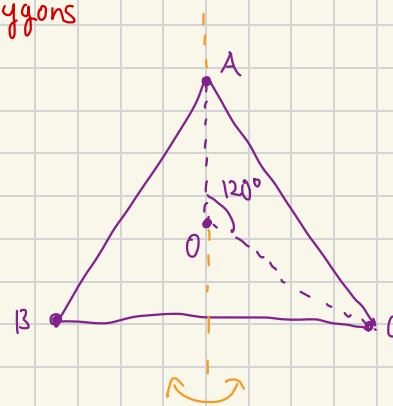
MAT301

Groups and Symmetries

Ex. polygons



rotate w.r.t. O by 120°

and the object appears unchanged

A B C ↦ C A B

doing nothing does not change it

Reflecting it also does not change it

A B C ↦ A C B

Each operation results in a permutation of vertices

Symmetric Group: The set of all permutations of n elements.

We label the elements $1, \dots, n$, and denote the set S_n

- Identity: 1 2 3 ↦ 1 2 3
- Transposition: 1 2 3 ↦ 1 3 2
- Cycle: 1 2 3 ↦ 3 1 2

A permutation is a way to order n objects. We codify them in "cycles"

- E.g. $n = 3$

$\begin{matrix}1&2&3\\1&2&3\end{matrix}$	$\begin{matrix}1&2&3\\1&3&2\end{matrix}$	$\begin{matrix}1&2&3\\3&2&1\end{matrix}$	$\begin{matrix}1&2&3\\2&1&3\end{matrix}$	$\begin{matrix}1&2&3\\2&3&1\end{matrix}$	$\begin{matrix}1&2&3\\3&1&2\end{matrix}$
$\mathbb{1}$					
$(1)(2)(3)$	$(1)(23)$	$(13)(2)$	$(12)(3)$	(123)	(132)

1 goes to 1

2 goes to 3
3 goes to 2

1 goes to 2
2 goes to 3
3 goes to 1

(cycle notation)

Ex. Sps we have 2 permutations

$\sigma = (12)(3456)$

$\varepsilon = (1654)(32)$

performed first

- σ first, ε second: $(1654)(32)(12)(3456)$

  $= (13)(26)(4)(5)$

- ε first, σ second: $(12)(3456)(1654)(32)$

  $= (13)(24)(5)(6)$

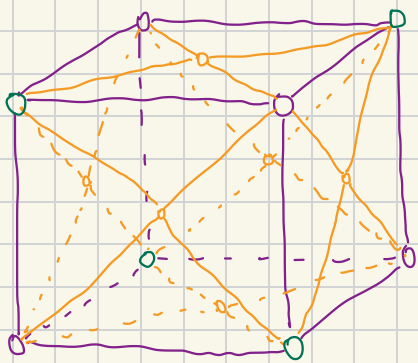
S_3 Multiplication Table

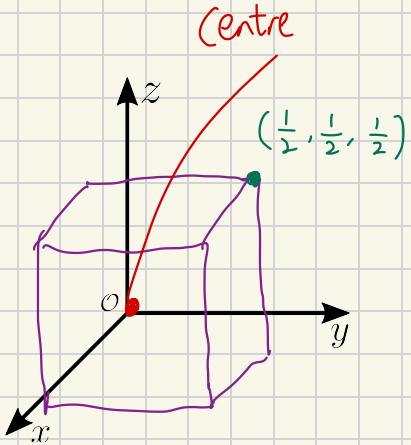
$\circ$	$\mathbb{1}$	(12)	(13)	(23)	(123)	(132)
$\mathbb{1}$						
(12)						
(13)						
(23)	(23)	(132)	(123)	$\mathbb{1}$	(13)	(12)
(123)						
(132)						

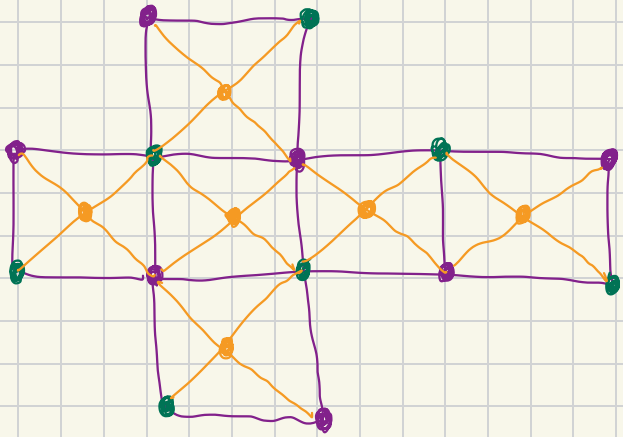
- Can write $(1\ 2\ 3) = (23)(13)$ 2 transpositions
- $\mathbb{1} = (12)(12) = (23)(23)$

Thm. The amount of transpositions needed to create a permutation preserves parity

Ex. Consider the following figure

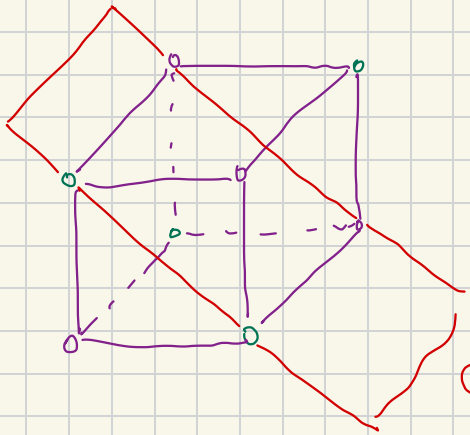




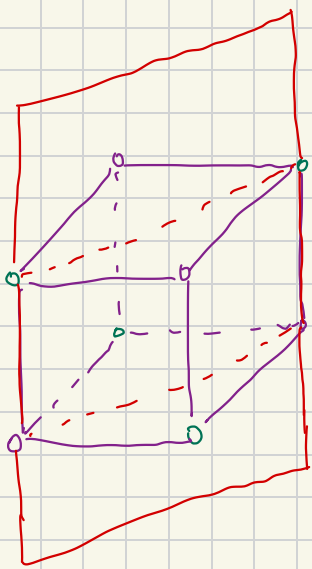


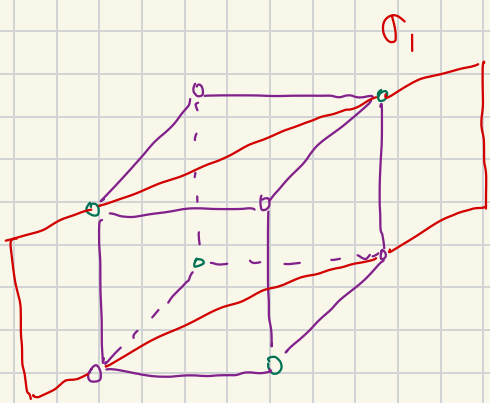
Question: find isometries that preserve the colouring of this object

Consider planes



A reflection on a plane preserves the colourings





- Each of those is a linear transformation, so they are induced by a matrix

Prop. If $S, T : \mathbb{R}^3 \to \mathbb{R}^3$ preserve the coloured cube and send the triangle to the same place, then $S = T$

Pf For three points b, θ, y:

$$Sb = Tb \qquad (S-T)b = 0$$

$$S\theta = T\theta \Rightarrow (S-T)\theta = 0$$

$$Sy = Ty \qquad (S-T)y = 0$$

And so b, θ, y are in the kernel of $S-T$.

Since b, θ, y (in. ind. $\dim \ker(S-T) = 3$

Because we are in $\mathbb{R}^3$, $S = T$. □

- Not only colour have to be same, $\mathbb{R}^3$ vectors also need to be same

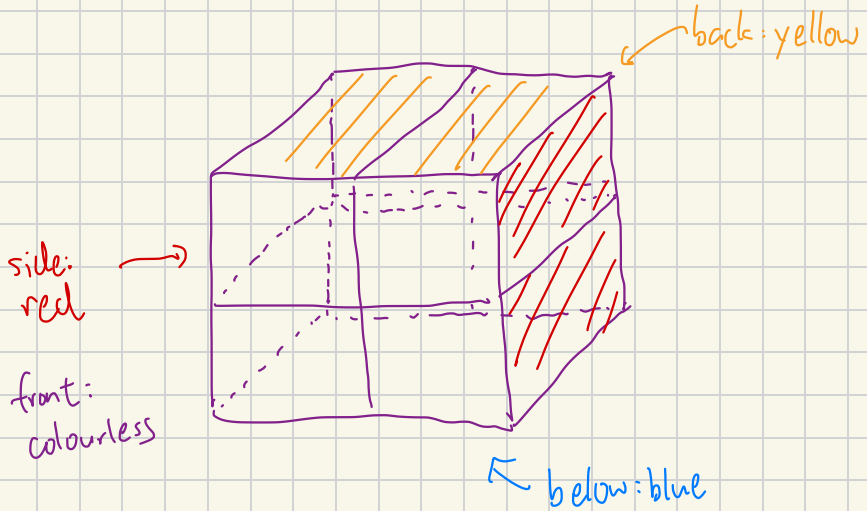
Def. A group is a pair $(G, \cdot)$ s.t. $G \times G \to G$ (multiplication) defined by $(a,b) \mapsto a \cdot b$ s.t. it satisfy the following:

- (identity) There exists an element $e \in G$ s.t. $e \cdot g = g \cdot e = g$
- (inverse) For each $g \in G$, there exists $h \in G$ s.t. $g \cdot h = h \cdot g = e$
- (associativity) For all $g, h, k \in G$, we have

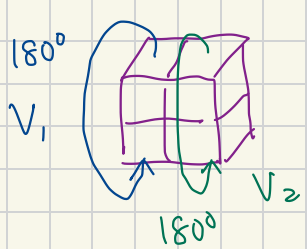
$(g \cdot h) \cdot k = g \cdot (h \cdot k)$

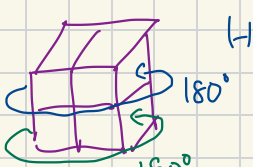
- If we also have $g \cdot h = h \cdot g$, then we call the group abelian or commutative

Ex. Consider the $2 \times 2 \times 1$ Rubik's cube (toy)

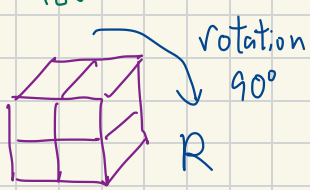


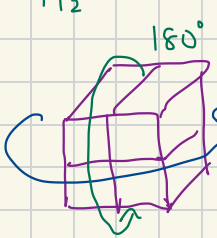
- Can do the following operations $V_1, V_2, H_1, H_2, V, H, R$





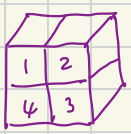
flip vertically V

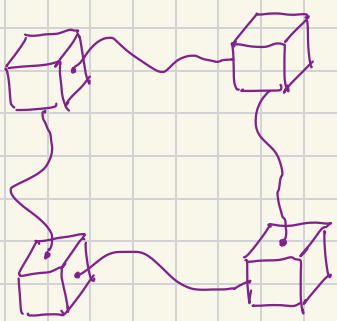




flip horizontally H

- $\underline{1} = V_1^2 = V_2^2 = H_1^2 = H_2^2 = V^2 = H^2 = R^4$
- Have redundancies
  - $V = V_1 V_2 = V_2 V_1$
  - $H = H_1 H_2 = H_2 H_1$
  - $RH_1 = V_1 R \Rightarrow H_1 = R^{-1} V_1 R$
- Consider the following.





1	2
4	3

location

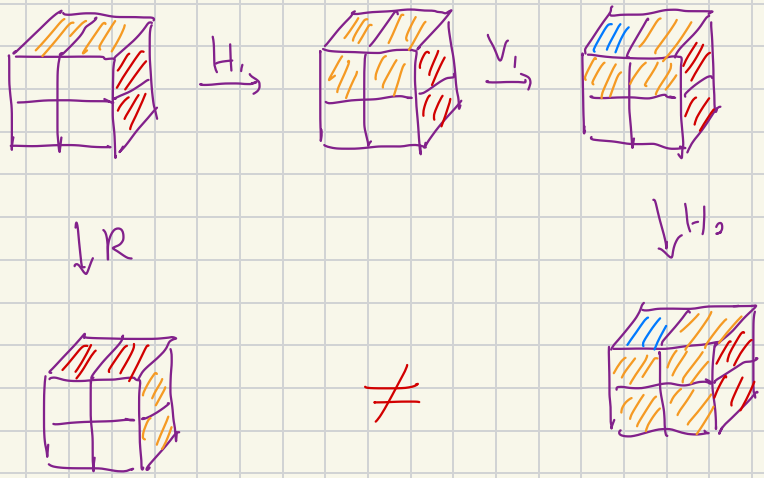
e.g. R $\begin{array}{|c|c|}\hline 1&2\\\hline 4&3\\\hline\end{array}$ $\rightarrow$ $\begin{array}{|c|c|}\hline 4&1\\\hline 3&2\\\hline\end{array}$ $(1\ 2\ 3\ 4)$

V_1 $\begin{array}{|c|c|}\hline 1&2\\\hline 4&3\\\hline\end{array}$ $\rightarrow$ $\begin{array}{|c|c|}\hline 4&2\\\hline 1&3\\\hline\end{array}$ $(1\ 4)$

$V_2 : (2\ 3)$ $H_1 : (1\ 2)$ $H_2 : (3\ 4)$

- Can verify $(1\ 2\ 3\ 4) = (3\ 4)(1\ 4)(1\ 2)$

but $R \neq H_2 V_1 H_1$!



- We have a group that is the one generated by the operations of the toy, have 2 models to understand the group
  1. The complete toy
  2. Location code (loses information)

  They codify information differently
- If we only have H_1, V_1, H_2, V_2, then the locations are believable. The group they generate is S_4
- Want to merge R w/ rest of the operations
  - Have $H_1R = RV_1$ and $H_2R = RV_2$

- Simplify the instruction

$$RV_1H_2RV_2H_1H_2RV_1H_2$$
$$= RV_1H_2RV_2H_1RV_2V_1H_2$$
$$= RV_1H_2RV_2RV_1V_2V_1H_2$$
$$= RV_1H_2RRH_2V_1V_2V_1H_2$$
$$= RV_1H_2V_1V_2H_1H_2H_2V_1V_2V_1H_2$$

- All elements of the group can be written as $X\sigma$ where $X = 1, R$ and $\sigma \in S_4$
- This writing is unique
  - Sps $X_1\sigma_1 = X_2\sigma_2$, then

    Case 1: $X_1 = X_2 = 1 \Rightarrow \sigma_1 = \sigma_2$

    Case 2: $X_1 = X_2 = R \Rightarrow R\sigma_1 = R\sigma_2 \Rightarrow \sigma_1 = \sigma_2$

    Case 3: $X_1 = 1, X_2 = R \Rightarrow \sigma_1 = R\sigma_2$

    by group theory axiom every element can be undone, so $R = \sigma_1\sigma_2^{-1}$, but $R \notin S_4$, so this cannot happen
- Can write as $(-1, \sigma) \in \{\pm 1\} \times S_4$
  - Multiplication: $(s_1, \sigma_1)(s_2, \sigma_2) = (s_1s_2, \sigma_1\sigma_2)$

Def. Let G be a group and $H \subseteq G$ a nonempty set. Then H is a subgroup of G if H w/ the operations of G is a group in itself

- In the Rubik's cube group, the element generated by V_1, H_1, V_2, H_2 are a subgroup

Def. Given an element $g \in G$, its order is the smallest positive number n s.t. $g^n = e$, in case it exists.

- E.g. $(\mathbb{Z}, +)$ is a group (infinite group). 0 has order 0, rest don't have order, i.e. $(-1) + (-1) + \cdots \neq 0$

Def. Let G be a group. The order of G, $|G|$, is its cardinality.

Def. Let G and H be groups and $\Phi : G \to H$. Φ is a homomorphism if $\Phi(g_1 \cdot g_2) = \Phi(g_1) \cdot \Phi(g_2)$

Def. A homomorphism is a

- monomorphism if it's injective
- epimorphism if it's surjective
- isomorphism if it's bijective

Def. Let $\Phi : G \to H$ be a homomorphism.

- The kernel of Φ is
$$\ker(\Phi)_H = \{g \in G : \Phi(g) = e_H\}$$
- The image of Φ is
$$\mathrm{Im}(\Phi) = \{\Phi(g) : g \in G\}$$

Ex. Consider $\mathrm{sgn} : S_n \to \{\pm 1\}$

- $$\ker(\mathrm{sgn}) = \left\{ \sigma \in S_n \;\middle|\; \begin{array}{l} \sigma \text{ needs an even \# of} \\ \text{transpositions to write} \end{array} \right\}$$
  - This is called the alternating group A_n
  - $A_4 = \{\mathbb{1}, (a,b)(c,d), (a,b,c)\}$
    $\hookrightarrow (b,c)(a,c)$

Def. Let G be a group and X a set. A group action on X by G, denoted $G \curvearrowright X$, is a map

$G \times X \to X$ defined by $(g, x) \mapsto g \cdot x$ s.t.

① $\mathbb{1} \cdot x = x$

② $h \cdot (g \cdot x) = (hg) \cdot x$

$g \cdot x \in X$, $hg \in G$

$h \cdot (g \cdot x) \in X$, $(hg) \cdot x \in X$

homomorphism

$G \to \sum(X)$

$\sum(X) = \{f : X \to X \mid f \text{ bijective}\}$

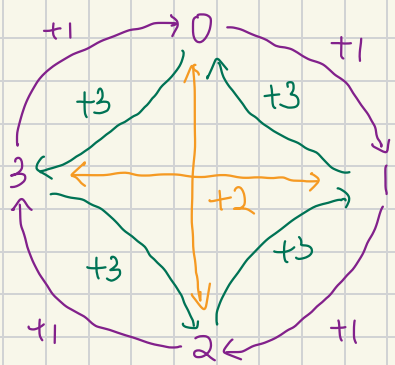
given $x \in X$, all the elements $g \cdot x$ are called the orbit of x

For every positive integer n, we consider the integers modulo n

- For $n = 3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

For $n = 4$.



Def. A cyclic group is a group G that has a generator (an element where repeatedly applying the operation

"generates" all elements of the group

Def. The group of integers modulo n is called the cyclic group of order n and denoted by C_n or $\mathbb{Z}/n\mathbb{Z}$

- The integers $\mathbb{Z}$ are cyclic, b/c $+1$ is the generator

$$\cdots \to -2 \xrightarrow{+1} -1 \xrightarrow{+1} 0 \xrightarrow{+1} 1 \xrightarrow{+1} \cdots$$

- Given a group G and element $g \in G$, we produce

$$\langle g \rangle = \{\cdots, g^{-2}, g^{-1}, g^0 = \mathbb{1}, g^1, g^2, \cdots\} \subseteq G$$

Prop. Let G be a group and $g \in G$.

① $\langle g \rangle$ is a subgroup of G $\cong$

② g has order m iff $\langle g \rangle$ is isomorphic to C_m

③ g has no order (infinite order) iff $\langle g \rangle$ is isomorphic to $\mathbb{Z}$

- Associativity follows from G
- Identity: $g^0 = \mathbb{1}$
- Inverse of g^n is g^{-n}
- Closed under operation $\bullet$: $g^n g^m = g^{n+m}$

- If g has order m, define $\Phi : C_m \to \langle g \rangle$ as $k \mapsto g^k$
  - Well-defined b/c if $a \equiv b \pmod m$ then $a = b + mt$, and so
    $$g^a = g^{b+mt} = g^b g^{mt} = g^b (g^m)^t = g^b 1^t = g^b$$
  - Homomorphism b/c $\Phi(a+b) = g^{a+b} = g^a g^b = \Phi(a)\Phi(b)$
  - Injective b/c assume $\Phi(b) = \Phi(a)$, then $g^a = g^b$, $g^{a-b} = 1$. Since $a, b \in \{0, \dots, m-1\}$, WLOG $a > b$, have $0 \le a-b \le m-1$, so $a-b = 0$, $a = b$
  - Surjective b/c $\langle g \rangle = \{g^0, \dots, g^{m-1}\}$. Take $k = 0, \dots, m-1$ produce all elements

Ex. Consider $C_6 = \{0, 1, 2, 3, 4, 5\}$

- $\langle 0 \rangle = \{0\} = C_1 \qquad \langle 1 \rangle = \langle 5 \rangle = C_6$

  $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\} \cong C_3$

  $\langle 3 \rangle = \{0, 3\} \cong C_2$

Ex. Consider S_3

- $\langle 1 \rangle = \{1\} = C_1$

$\langle (1,2) \rangle = \{ \mathbb{1}, (1,2) \} \cong C_2$

$\langle (1,2,3) \rangle = \{ \mathbb{1}, (1,2,3), (1,3,2) \} \cong C_3$

$\vdots$

- Cyclic Subgroups | # of them | # of generators

C_0	1	1
C_1	3	3
C_2	1	2

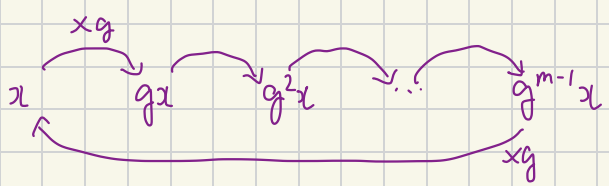
Def. A cyclic group of order $n \in \mathbb{Z}^+$ admits a generator of order n, i.e. $C_n = \{1, g, \dots, g^{n-1}\}$

Thm. Let p be a prime number and G be a group of order p. Then $G \cong C_p$

- To prove this, notice that $\exists g \in G$ s.t. $g \neq 1$. Let m be the order of G

  $C_m = \{1, g, \dots, g^{m-1}\} \subseteq G$

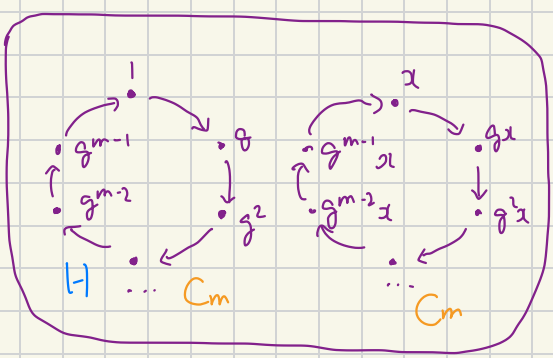
- Let $x \in G$ and multiply by g successively by the left



There is no repetition earlier. If $g^i x = g^j x$ for $0 \le i < j \le m-1$, then cancel x gives $g^i = g^j$

- Doing so, we see that G decomposes into cycles of size m. There must be a finite numbers of cycles, say k. Then $|G| = mk$
- Since $|G|$ is prime, $\{m, k\} = \{1, p\}$. The order m cannot be 1, so $m = p$, $k = 1$, i.e. 1 cycle of size p. Therefore $G = C_p$

From the step where we repeatedly apply G:



"multiply x by every element of C_m"

- H is a subgroup of G. Let $x \in G$
- Right: multiply every element of H by x

Ex. $S_3 = \{1, (12), (23), (13), (123), (132)\}$

- $H = \{1, (12)\}$ ⋮ not subgroups b/c no identity
- $H(23) = \{1(23), (12)(23)\} = \{(23), (123)\}$
- $H(13) = \{1(13), (12)(13)\} = \{(13), (132)\}$

Def. Given a group G and a subgroup H, define the coset of H as

- Right coset $Hx = \{hx \mid h \in H\}$ $H_1 \backslash G / H_2$
- Left coset $xH = \{xh \mid h \in H\}$

Denote by $H \backslash G$ the set of right cosets, and G/H the set of left cosets

Prop. Let G be a group and H a subgroup. Then

① All cosets have the same cardinality

② All left (right) cosets are disjoint

- To prove ①, multiplying by x is a bijection
- To prove ②, sps $xH \cap yH \neq \emptyset$, then we can write $xh_1 = yh_2$ w/ $h_1, h_2 \in H$. Then $y^{-1}x = h_2 h_1^{-1}$ so $y^{-1}x = h$ for some $h \in H$. Then $x = yh \in yH$. But for any $\tilde{h} \in H$, we can have

$xH \ni x\tilde{h} = (yh)\tilde{h} = y(h\tilde{h}) \in yH$, so $xH \subseteq yH$.

Changing roles, $yH \subseteq xH$. Therefore $xH = yH$.

Cor. Let $H \leq G$. Then

① $xH = yH$ iff $y^{-1}x \in H$

② $Hx = Hy$ iff $xy^{-1} \in H$

Thm. (Lagrange's) Let G be finite group and $H \leq G$.

Then $|H|$ divides $|G|$.

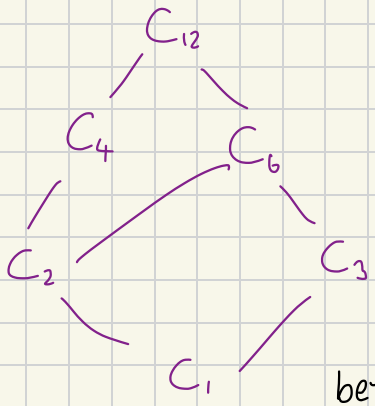
- To prove this, notice that G is the disjoint union of (left) cosets of G. Say there are k cosets, then $|G| = k|H| \Rightarrow |H| \mid |G|$

Ex. Consider $C_n = \mathbb{Z}/12\mathbb{Z} = \{0, 1, \ldots, 11\}$

- The divisors of 12 are

1	$\{0\}$
2	$\{0, 6\}$
3	$\{0, 4, 8\}$
4	$\{0, 3, 6, 9\}$
6	$\{0, 2, 4, 6, 8, 10\}$
12	$\{0, \ldots, 11\}$

- C_n has exactly one subgroup of each order dividing 12
- Can construct a subgroup map



Hasse diagram

Put an edge between H, H' if $|H|$ divides $|H'|$, only retain longest paths between every 2 nodes.

Def. Let G be a group and N be a subgroup. N is a normal subgroup of G if $\forall g \in G$, $gN = Ng$. Equivalently, $gNg^{-1} = N$. Denote $N \triangleleft G$

- G is a simple group if it has no normal subgroups

Ex. kernels are normal subgroups

- Let $x \in \ker\varphi$ and $g \in G$. Then $\varphi(gxg^{-1})$ $= \varphi(g)\varphi(x)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = 1$

Ex. A_n is normal in C_n

- b/c $A_n = \ker(\text{sgn})$

Let G be a group and N a normal subgroup. Construct G/N and pick two of them gN and hN. Construct a multiplication $gN \cdot hN := (gh)N$

Thm. G/N w/ the above product is a group iff N is normal. This is called the quotient group

- A_n is normal in S_n so S_n/A_n is a group
- A_n has 2 cosets, itself, and the odd permutation

	$\mathbb{1}A_n$	$(12)A_n$
$\mathbb{1}A_n$	A_n	$(12)A_n$
$(12)A_n$	$(12)A_n$	A_n

$S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$

- Notice the cosets $(12)A_n = (13)A_n$
- For $\text{sgn}: S_n \to \{1, -1\}$, notice $S_n/\ker(\text{sgn}) \cong \text{Im}(\text{sgn})$

Thm. (First Isomorphism) Let G be a group, $\varphi: G \to H$ a homomorphism. Then $G/\ker(\varphi) \cong \text{Im}(\varphi)$ and the isomorphism is $\tilde{\varphi}(x\ker\varphi) = \varphi(x)$

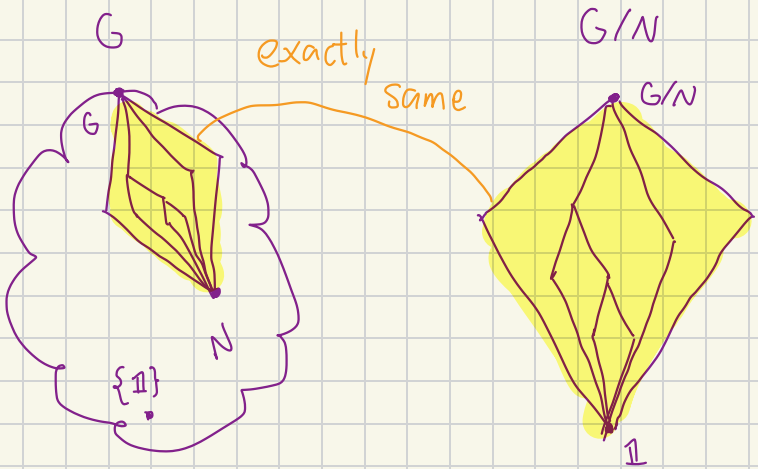
Thm. (Correspondence) Let G be a group and $N \triangleleft G$.

Then there is a correspondence

$$\{H \leq G \mid N \subseteq H \subseteq G\} \leftrightarrow \{\text{subgroup of } G/N\}$$

$$H \longrightarrow H/N$$

- Hasse diagram



Prop. Let G be a group and H a subgroup. Then H is normal in G iff there exists a homomorphism $\varphi: G \to K$ to some group K w/ $\ker\varphi = H$

Def. Let H be a subgroup of G. The cardinality of G/H is called the index of H in G and denoted by $[G:H]$

- If $H \leq G$ has index 2, then H is normal in G
  - Construct homomorphism whose kernel is H
  - $[G:H] = 2 \Rightarrow G = H \sqcup g_0 H$ for some $g_0 \in G$
  - Define a function $\varphi : G \to \{1, -1\}$ by

$$\varphi(g) = \begin{cases} 1, & \text{if } g \in H \\ -1, & \text{if } g \notin H \end{cases}$$

  - To show $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g) + \varphi(h)$:
    - $g, h \in H \Rightarrow gh \in H$
    - $g, h \notin H \Rightarrow gh \in H$
    - $g \in H, h \notin H \Rightarrow gh \notin H$

      This means $g \in H$, $h \in g_0 H$, and so $\exists t \in H$ s.t. $h = g_0 t$. Multiplying, $gh = g g_0 t$. Sps for contradiction that this $\in H$. Then $g_0 = \underbrace{g^{-1}}_{\in H}\underbrace{gh}_{\in H}\underbrace{t^{-1}}_{\in H} \Rightarrow g_0 \in H \not\in$
  - $\ker \varphi = \{g \in G \mid \varphi(g) = 1\} = \{g \in G \mid g \in H\}$
    $= H$

- D_n generated by R, S
  - $|D_n| = 2n$
  - $\{1, R, \ldots, R^{n-1}\} \cong C_n$
  - $[D_n : C_n] = 2 \Rightarrow \{1, R, \ldots, R^{n-1}\} \triangleleft D_n$
- If R is the $2\times2\times1$ Rubik's cube group
  - $|R| = 48$
  - $[R : S_4] = 2 \Rightarrow S_4 \triangleleft R$

Thm. Let p be prime and G be a group of p^2 elements. Then G is isomorphic to C_{p^2} or $C_p \times C_p$

- $(g_1, g_2) \times (g_3, g_4) = (g_1 g_3, g_2 g_4)$

Pf If G is cyclic, then $G \cong C_{p^2}$. Sps it's not cyclic. By Lagrange, the order of every element is in $\{1, p, p^2\}$. Since G is not cyclic, no element can have order p^2. Since only $\mathbb{1}$ has order 1, every nonidentity element has order p. The only intersection the C_p subgroups can have is $\mathbb{1}$. The count of C_ps is:

$$(\#C_p\text{s})\underbrace{(p-1)}_{\#\text{ generators}} + \underbrace{1}_{\mathbb{1}} = p^2 \Rightarrow \#C_p\text{s} = p+1$$

Let $P_1, P_2, \dots, P_{p+1}$ denote each C_p subgroup.

Take $g \in G$ and P_i to create $gP_ig^{-1} = P_j$

for $1 \le j \le p+1$. Call $\Phi(g) \in S_{p+1}$ s.t.

$gP_ig^{-1} = P_{\Phi(g)(i)}$. This creates a map $\Phi: G \to S_{p+1}$.

This is a homomorphism: pick $x, y \in G$, $\Phi(xy) = \Phi(x)\Phi(y)$

$(xy)P_i(xy^{-1}) = xyP_iy^{-1}x = xP_{\Phi(y)(i)}x^{-1} = P_{\Phi(x)(\Phi(y)(i))}$

Thus Φ must satisfy $p^2 = |\ker \Phi| \cdot |\operatorname{Im} \Phi|$.

If $|\ker \Phi| = 1$, then $|\operatorname{Im} \Phi| = p^2$. However

$|S_{p+1}| = (p+1)!$ and the image is a subgroup, but

$p^2 \nmid (p+1)!$ b/c by Lagrange. Thus $\ker \Phi$ is nontrivial.

There are elements $x \neq 1$ s.t. $xP_ix^{-1} = P_i \ \forall i$.

Sps $P_i \ni x$ and consider y a generator of P_i.

Then $xyx^{-1} = y^n$ for some n. Then $(xyx^{-1})(xyx^{-1})$

$= xy^2x^{-1} = y^ny^n = y^{2n}$. Continuing this gives $xy^kx^{-1} = y^{kn}$.

The powers of x: $1, x, \dots, x^{p-1}$ move the elements

as follows: $x^2yx^{-2} = x(xyx^{-1})x^{-1} = xy^nx^{-1} = (xyx^{-1})^n$

$= (y^n)^n = y^{n^2}$ $\quad (xyx^{-1})^2 = xyx^{-1}xyx^{-1} = xy^2x^{-1}$

Repeating this gives $x^kyx^{-k} = y^{n^k}$. Pick $k = p-1$,

then $x^{p-1} y x^{-(p-1)} = x^{-1} y x = y^{n^{p-1}} = y$ by Fermat's little theorem. Therefore $\exists x, y$ of order p in G that commute. Now define $\psi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \to G$ as $(m,n) \mapsto x^m y^n$. This is an isomorphism.

To show injectivity, let $x^m y^n = 1$, then $x^m = y^{-n}$, which is the intersection of C_p subgroups, therefore $x^m = y^{-n} = 1$, and so $m, n = 0$. To show homomorphism, $\psi(m_1 + m_2, n_1 + n_2) = x^{m_1+m_2} y^{n_1+n_2} = x^{m_1} y^{n_1} x^{m_2} y^{n_2}$ $= \psi(m_1, n_1)\psi(m_2, n_2)$ b/c x, y commute. Surjectivity is easy. This concludes that $G \cong C_p \times C_p$. □

Hasse Diagram of D_6

- 2 elements R, S generate everything
- They satisfy $R^6 = \mathbb{1}$, $S^2 = \mathbb{1}$, $SRS = R^5$
- Group elements: 1, R, R^2, R^3, R^4, R^5, S, SR, SR^2, SR^3, SR^4, SR^5 (same)
- Subgroups of prime order are all cyclic

- $(SR^i)(SR^i) = (SR^iS)R^i = (SRS)^iR^i = (R^5)^iR^i$

  $= R^{6i} = \mathbb{1}$

Order of Subgroup	Found	
12	self (all)	
6	cyclic (maybe other ones)	
4	none (maybe other ones)	
3	cyclic (all)	1 $\langle R^2 \rangle$
2	cyclic (all)	7 total
1	identity (all)	

- $\langle R^2 \rangle$ is normal b/c $g\langle R^2 \rangle g^{-1}$ is order 3, which can only be $\langle R^2 \rangle$
- If H normal in D_6 of order 6, then $\exists \phi : D_6 \to \{-1, 1\}$ w/ $\ker \phi = H$

  index is 2
- Let $x \in D_6$ w/ order m, $\phi(x)^m = 1$. If m odd then $\phi(x) = 1$. Then all elements of odd order are $\in \ker \phi$
  - Only odd element is $\langle R^2 \rangle$, order is 3
  - Now $\langle R^2 \rangle \leq H \leq D_6$

- Take coset of $\langle R^2 \rangle$ gives

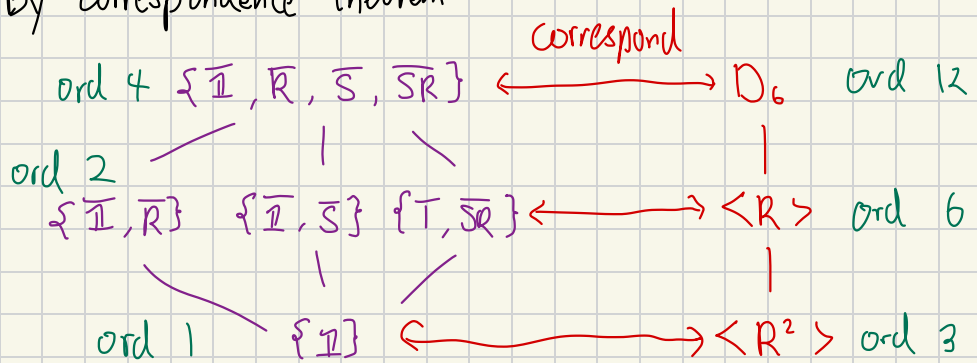
$\overline{1} = \{1, R^2, R^4\}$

$\overline{R} = R\{1, R^2, R^4\}$

$\overline{S} = S\{1, R^2, R^4\}$

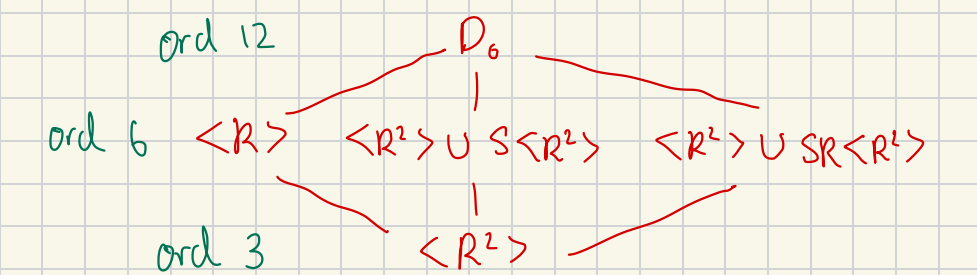
$\overline{SR} = SR\{1, R^2, R^4\}$

- By correspondence theorem



- By taking preimages

element	1	R	R^2	R^3	R^4	R^5	S	SR	SR^2	SR^3	SR^4	SR^5
coset	$\overline{1}$	$\overline{R}$	$\overline{1}$	$\overline{R}$	$\overline{1}$	$\overline{R}$	$\overline{S}$	$\overline{SR}$	$\overline{S}$	$\overline{SR}$	$\overline{S}$	$\overline{SR}$



- Now all order 6 elements are found

- Observe $C_2 \times C_2$ contains 3 elements of order 2
- Only 1 element of order 2 does not have S.

If some $H \leq D_6$ has $|H| = 4$, then at least 2 have an S: for SR^i, SR^j, $i \neq j$

$SR^i \cdot SR^j = (SRS)^i R^j = R^{5i+j} \in H$

must be $\langle R^3 \rangle$ ← third element of order 2

- $\langle R^3 \rangle \leq H \leq D_6$
- To make a correspondence, either
  1. Prove $\langle R^3 \rangle \triangleleft D_6$
  2. ✓ Verify the generators of D_6 conjugate $\langle R^3 \rangle$ to itself

- Check generator of $\langle R^3 \rangle$ since it's cyclic

$R \cdot R^3 \cdot R^{-1} = R^3$ $\quad$ $SR^3S^{-1} = R^3$

So $\langle R^3 \rangle \triangleleft D_6$

- Take the quotient gives 6 cosets

$\mathbb{1}$	R	R^2	R^3	R^4	R^5	S	SR	SR^2	SR^3	SR^4	SR^5
$\overline{\mathbb{1}}$	$\overline{R}$	$\overline{R^2}$	$\overline{\mathbb{1}}$	$\overline{R}$	$\overline{R^2}$	$\overline{S}$	$\overline{SR}$	$\overline{SR^2}$	$\overline{S}$	$\overline{SR}$	$\overline{SR^2}$

- This is S_3 b/c not cyclic or abelian

- Thus $\{\overline{\mathbb{I}}\} \leq H/\langle R^3\rangle \leq D_6/\langle R^3\rangle$

  and $|H/\langle R^3\rangle| = 4/2 = 2$

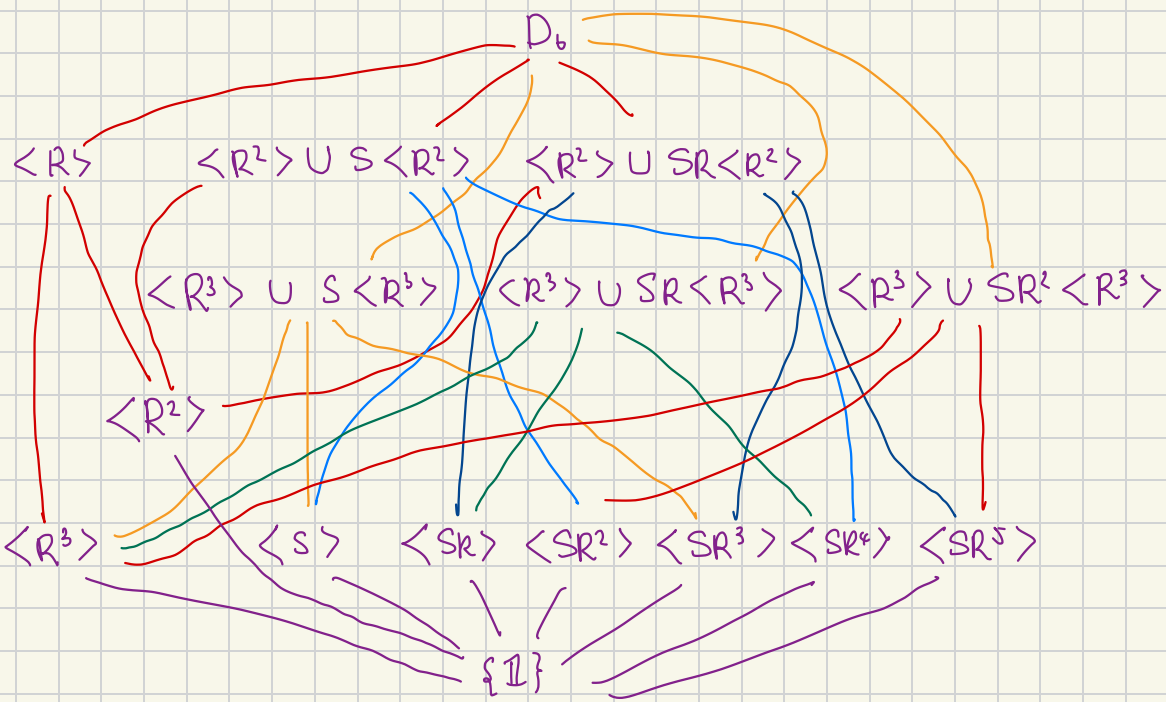
- 3 elements of order 2: $\overline{S}$, $\overline{SR}$, $\overline{SR^2}$

  $\overline{S} \leftrightarrow \{1, R^3, S, SR^3\}$

  $\overline{SR} \leftrightarrow \{1, R^3, SR, SR^4\}$

  $\overline{SR^2} \leftrightarrow \{1, R^3, SR^2, SR^5\}$

- Therefore



Def. Let G be a group and X a set. G acts on X if there is a map $G \times X \to X$ defined by

$(g, x) \mapsto g \cdot x$ that satisfy

① $1 \cdot x = x \quad \forall x \in X$

② $g \cdot (h \cdot x) = (gh) \cdot x$

- Associated to an action, there are 2 important constructions

① Given $x \in X$, the orbit of x is

$$O_x = \{g \cdot x \mid g \in G\}$$

② Given $x \in X$, the stabilizer of x is

$$Stab_x(G) = \{g \in G \mid g \cdot x = x\}$$

- Given a group G, we say G acts on itself by conjugation by defining $h^g = C_g(h) = ghg^{-1}$
  - $C_1(h) = 1h1^{-1} = h$
  - $C_g(C_h(k)) = C_g(hkh^{-1}) = ghkh^{-1}g^{-1} = ghk(gh)^{-1}$
    $= C_{gh}(k)$

Def. The orbits under conjugation is called conjugacy classes of G

- E.g. for S_3, the elements are 1, (12), (13), (23), (123), (132)

- For (12): $(12)^{-1} = (12)$

$(12) \overset{\text{act}}{\rightsquigarrow}$

$(12)\,\mathbb{1}\,(12) = \mathbb{1}$

$(12)(12)(12) = (12)$

$(12)(13)(12) = (23)$

$(12)(23)(12) = (13)$

$(12)(123)(12) = (132)$

$(12)(132)(12) = (123)$

- For (123): $(123)^{-1} = (132)$

$(123) \overset{\text{act}}{\rightsquigarrow}$

$(123)\,\mathbb{1}\,(132) = \mathbb{1}$

$(123)(12)(132) = (23)$

$(123)(13)(132) = (12)$

$(123)(23)(132) = (13)$

$(123)(123)(132) = (123)$

$(123)(132)(132) = (132)$

- The structure of the cycles is preserved, i.e. identity $\to$ identity, 2-cycle $\to$ 2-cycle, etc.

Thm. The conjugacy classes of S_n are classified by

cycle structure

- E.g. for S_4:

$(a)(b)(c)(d)$	(ab)	$(ab)(cd)$	(abc)	$(abcd)$
1 element	6	3	8	6

Let $G \in \mathbb{C}^{n \times n}$. E.g. for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, if it is diagonalizable, then there is a basis of eigenvectors v_1, v_2

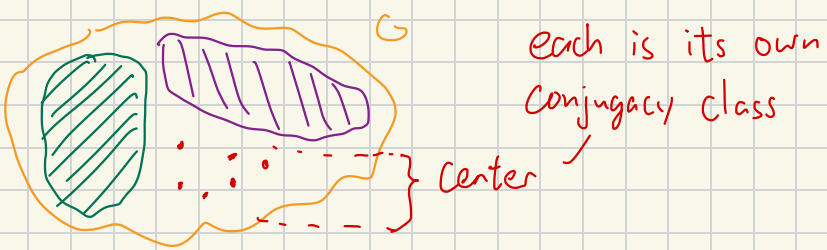
- Two bases: $(1,0), (0,1)$ in $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and v_1, v_2 in $\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$
- Find change-of-basis matrix Q where $Q \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} Q^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
- Q can be classified based on its shape, i.e. diagonal, upper-triangular, etc.
- For $C = ABA^{-1}$: B and C are conjugates, and A is the conjugating element
- Determinants of conjugates are preserved
  - Eigenvalues / eigenvectors are, but they are hard to compute

- Trace is also preserved, b/c it's the sum of eigenvalues (determinant being the product)
- For matrices nonstrictly larger than 3×3, trace + det is not enough to determine conjugates

Two observations about conjugation:

① If $x \in G$ is fixed by the conjugation, that means $gxg^{-1} = x \ \forall g \in G$, then x is in the center

② All conjugacy classes are disjoint



This gives the class equation

$$|G| = |Z(G)| + \sum_{x \notin Z(G)} |\text{Conj}(x)|$$

only one per class

Thm. (Orbit-Stabilizer) Let G be a finite group that act on X and $x \in X$. Then

$$|G| = |\text{Stab}_x(G)|\,|O_x|$$

this is a subgroup

all element of X reachable from x

all $g \in G$ s.t. $g \cdot x = x$

Moreover, $G/\text{Stab}_x(G) = O_x$

Pf Let $x \in X$ and $O_x = \{g \cdot x \mid g \in G\} = \{x_1, \ldots, x_k\}$

	Elements of g s.t. $g \cdot x = x_i$	
$x = x_1$	$g \cdot x = x$	(elements of $\text{Stab}_G(x)$)
x_2	$g \cdot x = x_2$	(a coset appears here)
$\vdots$		
x_k	$g \cdot x = x_k$	(a coset appears here)

If $h \in \text{Stab}_G(x)$, and $g \cdot x = x_2$, we can write gh and get $gh(x) = g(h \cdot x) = g \cdot x = x_2$.

Now the coset $g\,\text{Stab}_G(x)$ only has elements x, x_2

If a row contains $g, h \in G$, then they must be in the same coset of the stabilizer:

$g^{-1} \cdot (h \cdot x) = g^{-1} \cdot x^2 = x$, which means

$g^{-1}h \in \text{Stab}_G(x)$, which is sufficient to represent the same coset.

Then $|G| = |O_x| \cdot |\text{Stab}_G(x)|$.

□

Thm. (Cauchy) Let G be a finite group and p a prime w/ $p \mid |G|$. Then there exists an element $x \in G$ of order p.

- "Opposite direction" of Lagrange
- E.g. $|D_{15}| = 30 = 2 \times 3 \times 5$
- E.g. $|S_7| = 7! = 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$

Pf Sps we know the result for 2 cases:

① H is abelian

② $|H| < |G|$

Using class equation

$$|G| = |Z(G)| + \sum |\text{Conj}(x)|$$

b/c center is abelian (use ①)

$p \mid |G|$

- $p \mid |Z(G)|$ we're done
- $p \nmid |Z(G)|$

$$|G| = |\text{Conj}(x)| \, |\text{Stab}(x)|, \quad |\text{Stab}(x)| < |G|$$

If $p \mid |\text{Stab}(x)|$ we're done b/c we can use ②

If $p \nmid |Z(G)|$ and $p \nmid |\text{Stab}(x)|$, then we must have $p \mid |\text{Conj}(x)|$, but this, by class equation, means $p \mid |Z(G)|$ (since $p \mid |G|$) ↯

Def. If G is a group and $p \mid |G|$, then $H \leq G$ is a p-group if $|H| = p^k$, where p is a prime

- If $|G| = 20$ and H is a 2-group of G, then we must have $k \leq 2$

Def. Given $H \leq G$, we say that H is p-Sylow if

1. H is a p-group
2. For all p-groups N, we cannot have $H \lneq N$ (strict), i.e. H is maximal

Thm. If $|G| = p^a m$ where $p \nmid m$, then any p-Sylow group has size p^a

Thm. (Sylow I) If $|G| = p^a m$ where $p \nmid m$, then there is a subgroup $H \leq G$ w/ $|H| = p^a$.

Pf Consider the collection $X = \{A \subset G : |A| = p^a\}$.

Define group action $G \times X \to X$, $(g, A) \mapsto \{ga : a \in A\}$.

Want to find an element $A \in X$ s.t. $\text{Stab}_G(A)$ has size p^a. By orbit-stabilizer theorem

$|\text{Stab}_G(A)| \cdot |G \cdot A| = |G|$. We have to show that there is an A s.t. $|G \cdot A| = m$. Because $G \times X \to X$ is an action and orbits form a partition of X, we have $|X| = \sum_{\text{orbits}} |GA|$. On the other hand, $|X| = \binom{mp^a}{p^a} = \frac{(mp^a)!}{(p^a)!(mp^a - p^a)!}$

$= \frac{mp^a (mp^a - 1) \cdots (mp^a - p^a + 1)}{p^a (p^a - 1) \cdots (2)(1)} = m \frac{(mp^a - 1) \cdots (mp^a - p^a + 1)}{(p^a - 1) \cdots (2)(1)}$

$= m \binom{mp^a - 1}{p^a - 1}$. Now $p^a \nmid \binom{mp^a - 1}{p^a - 1}$ and $m \mid |X|$.

Thus there is an element A s.t. $|GA|$ has size m. Observe that the multiplication by g, $m_g : G \to G$ $h \mapsto gh$ and $m_g : X \to X$ $A \mapsto gA$ is bijection. Thus all orbits of elements of X have the same size. We claim that if $A \in X$ then $|GA| \mid |G|$. Then we have that $m \mid |GA|$, which implies that $|GA||\text{Stab}_G(A)| = p^a m$. therefore $p^a \mid \text{Stab}_G(A)$. Therefore $\text{Stab}_G(A)$ is a p-group of the correct size. □

Thm. (Sylow II)

① If H is a p-subgroup of G, then there is a p-Sylow subgroup $P \leq G$ s.t. $H \leq P$

② If P_1, P_2 are two p-Sylow subgroups, then $\exists g \in G$ s.t. $P_1 = g^{-1} P_2 g$

Thm (Sylow III) Let G be a group and $|G| = p^a m$ w/ $p \nmid m$. Let n_p denote the # of p-Sylow subgroups of G. Then

① $n_p \mid m$

② $n_p \equiv 1 \pmod p$

Lem. If $n_p = 1$ for some $p \mid |G|$, then that p-Sylow subgroup is normal in G.

Pf Conjugate $g^{-1} P g$ gives P. □

Ex. Consider a group G of size 20. Find the possibilities for n_2, n_5

- $n_2 = 1, 5$ b/c $n_2 \mid 5$ & $n_2 \equiv 1 \bmod 2$

- $n_5 = 1$ b/c $n_5 \mid 4$ & $n_5 \equiv 1 \bmod 5$

Lem. If $|G| = 2p^a$, then $|G|$ has a normal subgroup of order p^a

Pf $n_p \mid 2$ & $n_p \equiv 1 \bmod p$. must have $n_p = 1$ □

Lem. If $|G| = p^a q^b$ w/ p, q odd primes and $a < q-1$, $b < p-1$. Then all Sylow groups are normal.

We now know the following:

- If p is prime and $|G| = p$ then $G = C_p$
- If p is prime and $|G| = p^2$ then $G = C_{p^2}$ or $G = C_p \times C_p$
- If $p = 2$ and G is abelian w/ $|G| = 8$, then $G = C_8$, $G = C_4 \times C_2$, or $G = C_2 \times C_2 \times C_2$

Thm. Let p be a prime and $|G| = p^n$ w/ G abelian. Then $G = C_{p^{d_1}} \times \cdots \times C_{p^{d_k}}$ with $d_1 + \cdots + d_k = n$ and $d_1 \geq d_2 \geq \cdots \geq d_k \geq 1$

- E.g. if $|G| = p^3$, then we are looking for ways to

write 3 as a sum of positive integers

- $3 = 2+1 = 1+1+1$

  C_{p^3} $\quad C_{p^2} \times C_p$ $\quad C_p \times C_p \times C_p$

More general question: given n, find positive integers $d_1, \dots, d_k$ s.t. $d_1 + \cdots + d_k = n$ and $d_1 \geq d_2 \geq \cdots \geq d_k \geq 1$.

They are called partitions of n, denoted $p(n)$

Thm. Let G be an abelian group w/ $|G| = p_1^{d_1} \cdots p_k^{d_k}$.

Then $G = \underbrace{(C_{p_1^{\beta_1}} \times \cdots \times C_{p_1^{\beta_m}})}_{\text{correspond to a partition of } d_1} \times \cdots \times \underbrace{(C_{p_k^{\alpha_1}} \times \cdots \times C_{p_k^{\alpha_\ell}})}_{\text{of } d_k}$

Pf For each p_i there is a Sylow p_i-subgroup $S_i \leq G$ and $|S_i| = p_i^{d_i}$. Any other Sylow for p_i is conjugate to S_i, thus because of abelian, it does not change, which means S_i is unique. Having k Sylows $S_1, \dots, S_k$ we can write $\phi : S_1 \times \cdots \times S_k \to G$ $(s_1, \dots, s_k) \mapsto s_1 \cdots s_k$. If $s_1 \cdots s_k = s_1' \cdots s_k'$ then $\underbrace{(s_1')^{-1} s_1}_{S_1} = \underbrace{(s_2' \cdots s_k')(s_2 \cdots s_k)^{-1}}_{S_2 \times \cdots \times S_k}$. Since they have

trivial intersection, they are 1, therefore $S_1 = S_1'$, and so ϕ injective. Surjective is easy. □

Let p be prime. Then $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \ldots, p-1\}$ is isomorphic to C_p when we consider $+$ as operation. If it has a second operation $\times$ then it has more properties. but $\times$ does not make it a group (0 has no inverse)

- When we consider both $+, \times$ then this is a ring

Ex. Integer mod 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

group

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

not group

does not return to identity

does return to identity

Can restrict to only the invertible elements

×	1	3
1	1	3
3	3	1

This is a group! It's C_2.

Consider any n. this group is abelian & finite b/c multiplication is commutative. When is this cyclic?

Def. For $N \in \mathbb{Z}^+$, define

$$(\mathbb{Z}/N\mathbb{Z})^* = \{x \bmod N : \exists y \bmod N \text{ w/ } xy \equiv 1 \bmod N\}$$

- This is a finite abelian group

Consider p prime.

- When p is prime and $n \not\equiv 0 \pmod p$, we have $n^{p-1} \equiv 1 \pmod p$ by Fermat's little theorem.
  The inverse for n is n^{p-2}.
- Only 0 not invertible, this type of ring is a field
- Question. who is $(\mathbb{Z}/p\mathbb{Z})^*$?
- E.g. $p=7$

	1	2	3	4	5	6
inverse	1	4	5	2	3	6

  An abelian group of 6 elements must be C_6
  There must be a generator (3 and 5)
- E.g $p=17$. $(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \ldots, 16\}$.
  Possible abelian groups of order 16:
  C_{16}, $C_8 \times C_2$, $C_4 \times C_4$, $C_4 \times C_2 \times C_2$, $C_2 \times C_2 \times C_2 \times C_2$
  The existence of coordinates does not merge

appropriately w/ having inverses

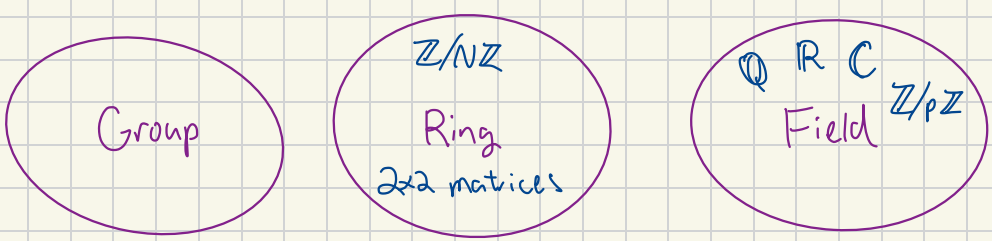
For example $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/6\mathbb{Z}$, by CRT

(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
↓	↓	↓	↓	↓	↓
0	4	2	3	1	5

they have 0 as a coordinate $\Rightarrow$ not invertible

Back to $\mathbb{Z}/17\mathbb{Z}$. 0 is the only noninvertible element, we can only put 0 in once, so we can only have 1 coordinate, and so $(\mathbb{Z}/p\mathbb{Z})^* = C_{16}$

Algebraic Structures



Operation +

Operation + with which it is abelian group

Operation X

A ring in which every nonzero element has a multiplicative inverse

- The set of invertible elements in a commutative ring form a group

- In a field, an equation of order n cannot have $>n$ solutions counted w/ multiplicity

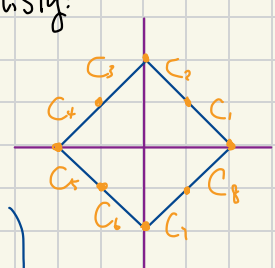
order	C_4	$C_2 \times C_2$
1	1	1
2	1	3
4	2	0

$x^2 = 1$ has more than 2 solutions $\Rightarrow$ not a field

Presentations and Isometries

Ex. Suppose we want to find a group G that is generated by 2 elements x, y which satisfy:

$x^4 = 1, \; y^2 = 1, \; yxy = x^3$



- Dihedral group D_4
- Define $R: \mathbb{R}^2 \to \mathbb{R}^2$ as $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

$S: \mathbb{R}^2 \to \mathbb{R}^2$ as $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Ex. Consider the following "groups"

- $G_1 = \langle x, y \rangle$
- $G_2 = \langle x, y, z \mid x^2 = y^2 = z^2 = (xy)^3 = (xz)^3 = (yz)^3 = 1 \rangle$

- $G_3 = \langle x, y, z \mid x^2 = y^2 = z^2 = (xy)^2 = (xz)^3 = (yz)^6 = 1 \rangle$

① I have $1, x, x^2, x^3, \ldots\ y, y^2, y^3, \ldots\ xy, xy^2, \ldots$

and weird stuff like $x^2yxyx^{-1}y^{-4}x$

① Consider $G_1' = \langle x, y \mid x^2 = y^2 = 1 \rangle$

Can be represented by a line

this group is infinite!

Start from 1, y: move to red dot

x: move to blue dot

Can be verified that $y^2 = x^2 = 1$

Can define $x : t \mapsto -t$ $\quad y : t \mapsto 2 - t$

Now we can compose x and y:

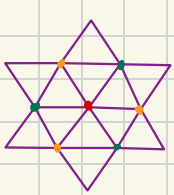
$(x \circ y)(t) = x(2-t) = t - 2$

$(x \circ x)(t) = x(-t) = t$ ✓

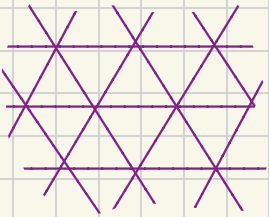
$(y \circ y)(t) = y(2-t) = 2 - 2 + t = t$ ✓

② Can be represented by triangles, where the chamber is the interior of a triangle

Applying x means move away from x, i.e. reflect on line yz



Analogous to y, z

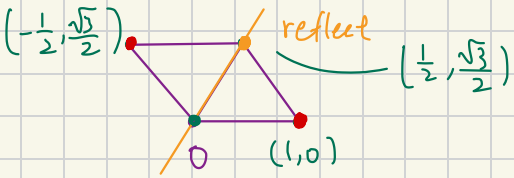


Given a chamber, there are different ways to move there

Some transformations reflect through a line that does not pass through the origin, which is not linear

$R\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$

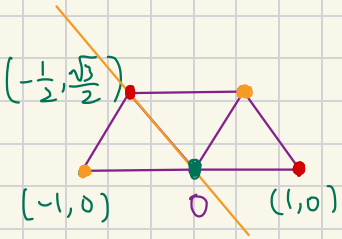
$R(1,0) = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$



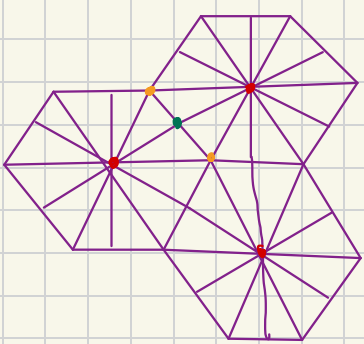
Another isometry:

$\tilde{Y}(-1,0) = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$

$\tilde{Y}\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$



(3)



Ex. $G = \langle a, b \mid a^{-1}ba = b^2, b^{-1}ab = a^2 \rangle$

- $ba = ab^2$, $ab = ba^2$
- $ba = abb = ba^2b \Rightarrow ab = 1$

- By symmetry $ba = 1$
- $1 = ba = ab^2 = ab \cdot b = 1 \cdot b = 1$
- By symmetry $a = 1$
- The group given by those rules is $\{1\}$

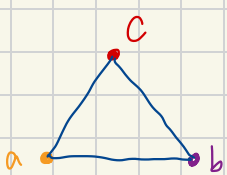
Determining whether a given group is $\{1\}$ is NP-complete

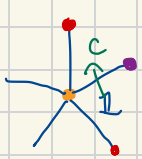
Def. A Coxeter group is a group that can be described by $G = \langle r_1, \dots, r_k \mid r_1^2 = \cdots = r_k^2 = 1, (r_i r_j)^{m_{ij}} = 1 \rangle_{i \neq j}$, where $2 \leq m_{ij} \leq \infty$

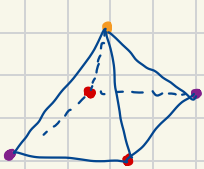
- E.g. $\langle a, b, c \mid a^2 = b^2 = c^2 = 1, (ab)^2 = (ac)^2 = (bc)^2 = 1 \rangle$

Algorithm to construct a group

- Our pieces are many equal triangles
- # pieces $= |G|$
- Apply c: jump away from c
- Since $bcbc = 1$:

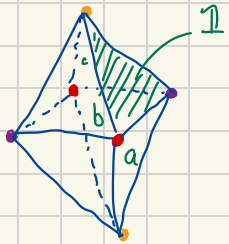




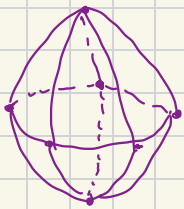


(fold the 4 triangles)

- Since we do this for all pairs:



This is an order 8 group, it's abelian. In fact, it is $C_2 \times C_2 \times C_2$

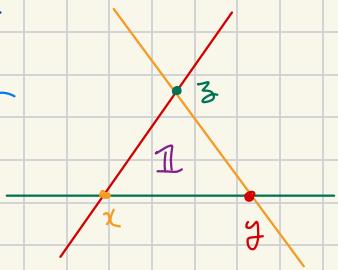


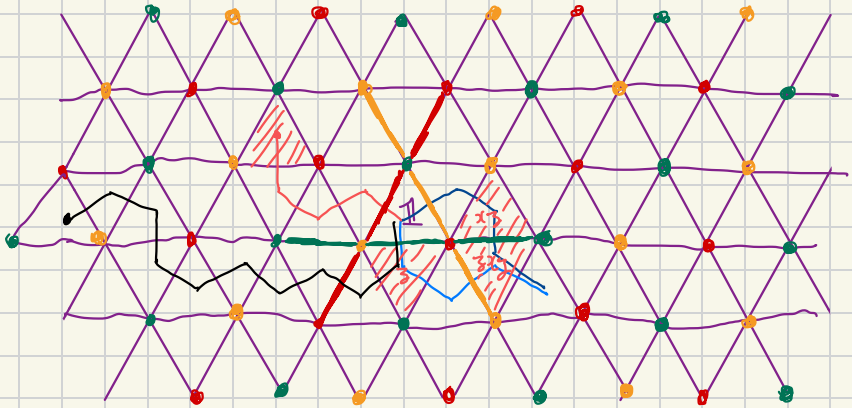
- This is a tessellation of a sphere

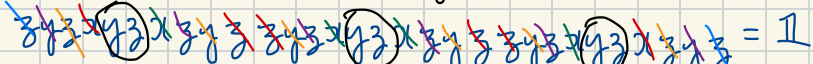
  Just like lattices is a tessellation of a plane

Prop. $G = \langle x, y, z \mid x^2 = y^2 = z^2 = (xy)^3 = (xz)^3 = (yz)^3 = 1 \rangle$ (the triangle pattern) coincides with the isometries of the plane $\mathbb{R}^2$

- A path can be represented by a sequence of x, y, zs, e.g. $yzxyzxyz$
  - We read them like functions, where each performs a reflection
- Consider a translation T in terms of the generator:
  - Try $T = xzxy$ (→ write path, ← trace chamber) —
  - Try $T = zxzy$ —
  - $xzxy = zxzy \Rightarrow xzx = zxz$
  - Try $T = yzxz$ —

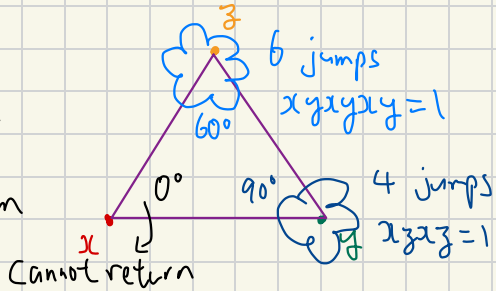




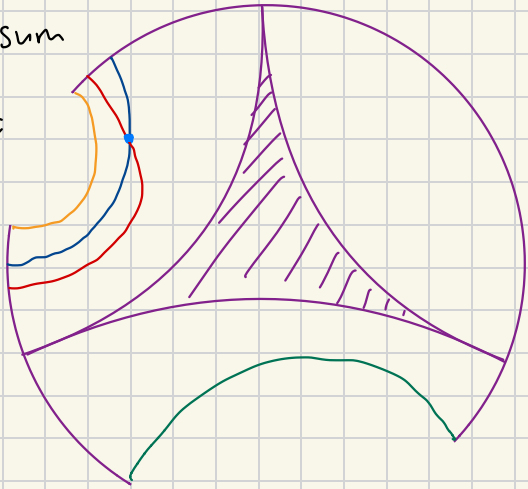
- Consider $w = zyzxyzxzyz$ —
  - This has order 3, b/c the destination is , a "rotated" version of start point , so when we trace the second w we go another direction
  - $w^3 =$  $= 1$ $(yz)^3 = 1$
- To determine what the possible orders are, we cannot use Lagrange b/c group has infinite order

Ex. Consider $G = \langle x, y, z \mid x^2 = y^2 = z^2 = (xy)^3 = (xz)^2 = 1 \rangle$

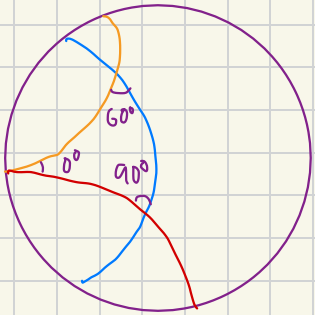
- yz has infinite order
- Triangles in this fashion don't necessarily have 180° angle sum



- Model for hyperbolic plane (Poincare disk model)
  - △ has 0° angle sum
  - L ∥ L, L ∥ L, but L ⋕ L
  - L ∥ L, L, L



- ∥H denotes hyperbolic
- Back to original example
- Upper half model



Postulate (Parallel). Given a line L and a point P not in L, there is a unique line through P parallel to L.

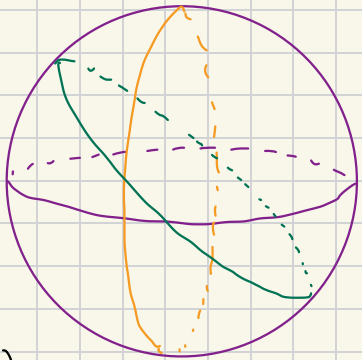
- Can break in 2 ways

  (S) There are no parallel lines to L through P

  (H) ∃ many ∃ ∃ ∃

- Spherical geometry satisfies (S)

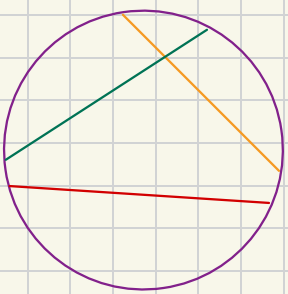
- Lines are called the great circles
- Any two great circles intersect



- Hyperbolic geometry satisfies (H1)

Klein model (a model of hyperbolic geometry)

- The lines are chords
- The model is not conformal (does not respect angles)



Different geometries differ in the sum of the angles in a triangle

Hyperbolic

$< \pi$

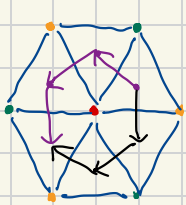
Euclidean

$= \pi$

Spherical

$> \pi$

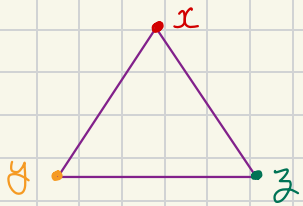
Path Translation



$yzy = zyz$

Coxeter group w/ 3 generators $G =$

$$\langle x, y, z \mid x^2 = y^2 = z^2 = (xy)^a = (yz)^b = (xz)^c = 1 \rangle$$



- $\angle x = \frac{360^\circ}{2b} = \frac{180^\circ}{b} = \frac{\pi}{b}$

  $\angle y = \frac{360^\circ}{2c} = \frac{180^\circ}{c} = \frac{\pi}{c}$

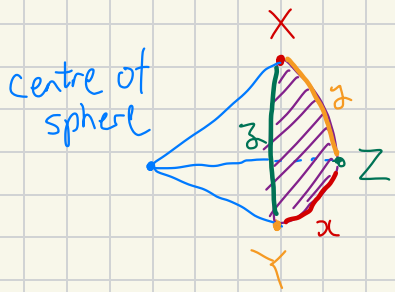
  $\angle z = \frac{360^\circ}{2a} = \frac{180^\circ}{a} = \frac{\pi}{a}$

- G is a tessellation of a plane if

  $$\frac{180^\circ}{a} + \frac{180^\circ}{b} + \frac{180^\circ}{c} = 180^\circ \iff \frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$$

- G is a tessellation of a sphere if

  $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} > 1$, in which case G is finite



can view the lines as arc lengths, which is equivalent to the respective angle

- Pythagorean theorem: $\cos(x) = \cos(y)\cos(z)$

- Law of sines. $\frac{\sin x}{\sin X} = \frac{\sin y}{\sin Y} = \frac{\sin z}{\sin Z}$

- Area of triangle: $X + Y + Z - \pi$

  assuming a unit sphere

- Area of unit sphere is 4π

- $$|G| = \frac{4\pi}{X+Y+Z-\pi} = \frac{4\pi}{\frac{\pi}{a}+\frac{\pi}{b}+\frac{\pi}{c}-\pi}$$

  $$= \frac{4\pi}{\frac{\pi(ab+bc+ac-abc)}{abc}} = \frac{4abc}{ab+bc+ac-abc}$$

- G is a tessellation of a hyperbolic plane if $\frac{1}{a}+\frac{1}{b}+\frac{1}{c} < 1$

- E.g. $a = b = c = \infty$, then the triangles have zero angle sum