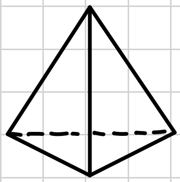
1 Introduction

GROUPS

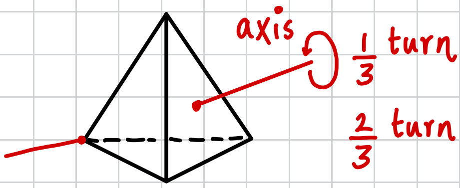
A group (loosely) is a set G together with a "rule" or binary operation that takes $g,h \in G$ and produces a new element $gh \in G$ satisfying certain axioms

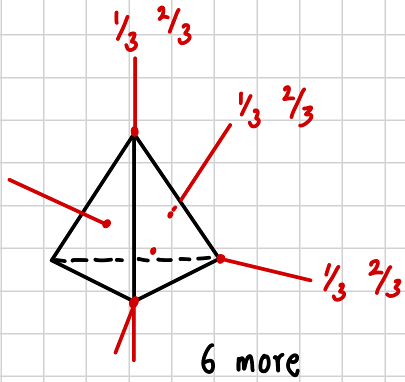
Examples of Groups

1) The group of rotational symmetries of regular tetrahedron



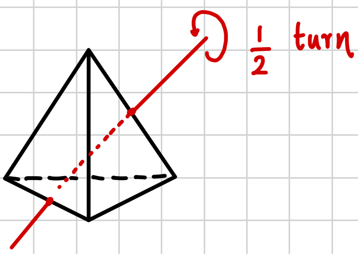
Symmetries are

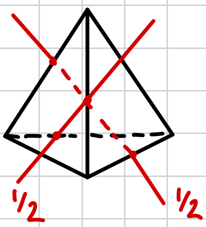




6 more

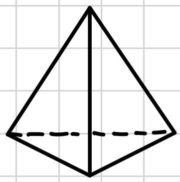
2 more



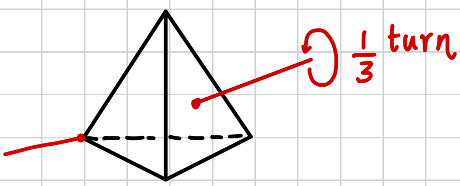


2 more

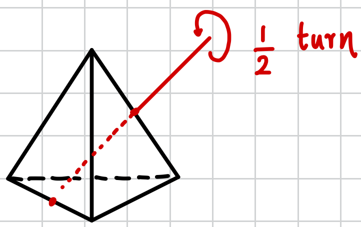
Finally do nothing



The rule takes the net effect of applying 2 rotations

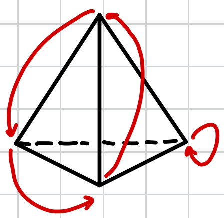


g

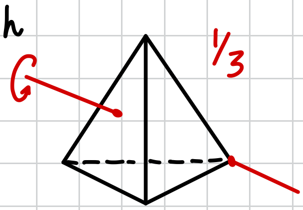


h

$\xrightarrow[\text{effect}]{\text{net}}$



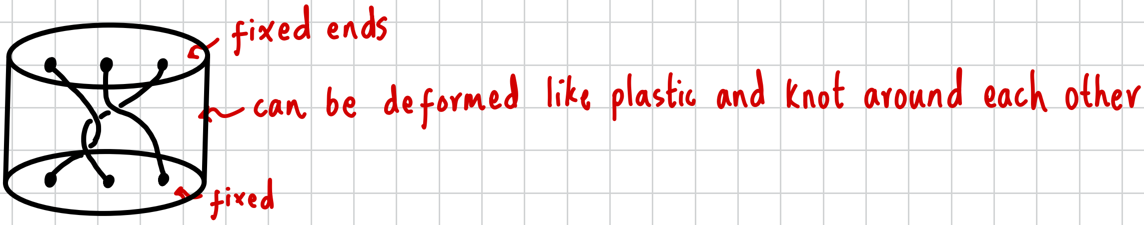
gh $\equiv$



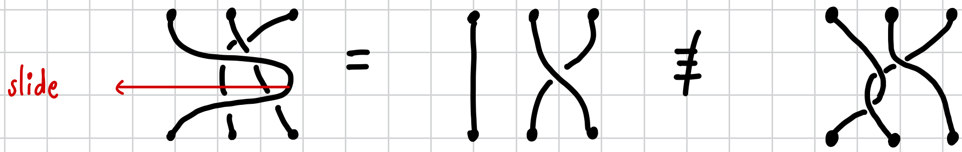
2) The n-stranded braid group

Elements: n-stranded braid

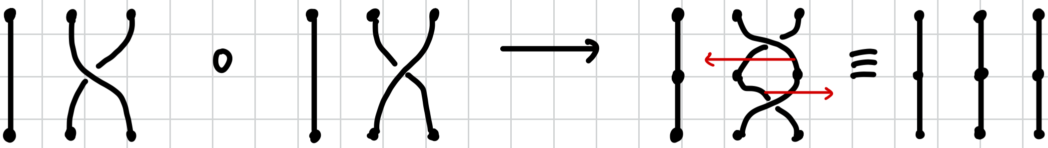
▸ $n=3$



> Two braids are the same if one can be deformed into the other without cutting



<u>The operation</u>: stick one on top of the other



Definition of a group

Definition Group

A group is a set G with binary operation

$$(g,h) \mapsto gh$$

such that

(1) Closure

$gh \in G$ is uniquely determined by g, h

(2) Associativity

$$g(hk) = (gh)k \quad \forall\, g,h,k \in G$$

(3) Existence of Identity

$\exists$ a $1_G \in G$ such that

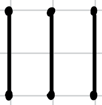
$$1_G g = g 1_G = g \qquad \forall g \in G$$

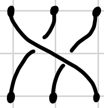
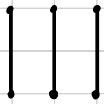
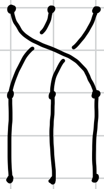
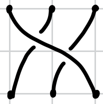
(4) Existence of Inverse

$\forall g \in G,\ \exists\, g^{-1} \in G$ s.t

$$g g^{-1} = g^{-1} g = 1_G$$

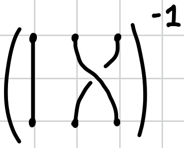
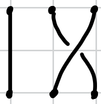
Example: In braid group

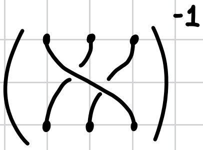
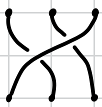
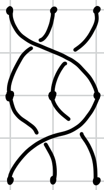
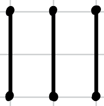
$1_G =$  as say

 $\circ$  $\equiv$  $\equiv$  $= g$

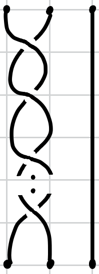
g $\quad$ 1_G $\quad$ $g1_G$

Inverse

-  $\equiv$ 

-  $=$  as  $=$ 

Notice also

 $\Longrightarrow$ the group is infinite

n- distinct elements

Notation: in a generic group G, write multiplicatively i.e.

$$gh \text{ for } g,h \in G$$

REVIEW OF GROUP THEORY

Symmetric group S_n

Let X be a non-empty set $X \neq \emptyset$ (often $X = [n] = \{1, \dots, n\}, n \in \mathbb{N}$)

We write I_X for the identity map $I_X : X \to X$. If $X = [n]$, we write I_n for $I_{[n]}$

Definition Symmetry

Let X be a set. A bijection $\sigma : X \to X$ is called a symmetry

We denote by S_X the set of all bijections from X to X.

$$S_X = \{\sigma : \sigma \text{ a symmetry of } X\}$$

If $X = [n]$, we write S_n for $S_{[n]}$

Notation: The binary operation represented by '$\circ$' is composition of a function

Proposition Symmetric Group

The pair $(S_X, \circ)$ is a group, the symmetric group on X

Cycle Notation

Definition Cycle

A cycle in S_n (of length $m \geq 2$)

$$\alpha = (a_1, \dots, a_m)$$

where $a_1, a_2, \dots, a_m \in \{1, \dots, n\}$ and $a_i \neq a_j$ for $i \neq j$

It is the bijection defined by

$$\alpha(a_1) = a_2 \quad \alpha(a_2) = a_3, \dots, \alpha(a_{m-1}) = a_m, \quad \alpha(a_m) = a_1$$

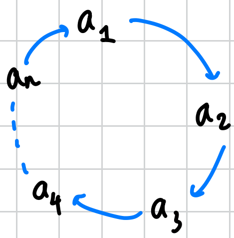
and

$$\alpha(x) = x \quad \forall x \in \{1, \dots, n\} \setminus \{a_1, \dots, a_m\}$$ fixes other elements

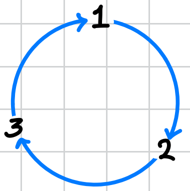
$m \leq n$

So

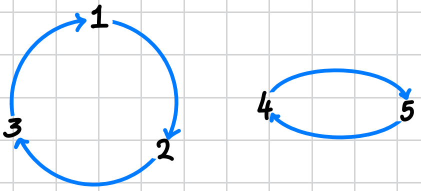
$\sigma = (a_1\, a_2 \cdots a_n)$ is



Example:

1) $\sigma =$ 

as $(1\ 2\ 3)$

2) $\tau =$ 

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

Note: Compose from right to left

e.g. if $\mu = (1\ 2)$

$$\tau\mu = (1\ 2\ 3)(4\ 5)(1\ 2) = (1\ 3)(4\ 5)$$

Subgroups

Definition Subgroups

Let G be a group. Let $H \subseteq G$.

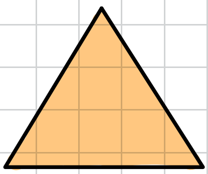
Then, H is a subgroup of G denoted $H \leq G$ if

(i) $a, b \in H \Rightarrow ab \in H$ — closure

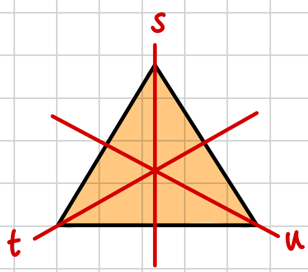
(ii) $a \in H \Rightarrow a^{-1} \in H$ — closure under inverse

(iii) $e \in H$ — contains identity $\Rightarrow H \neq \emptyset$

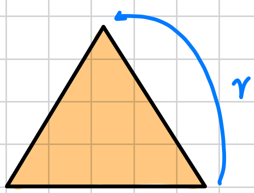
Example:

$G =$ symmetries of 

Operation: composition of symmetries



reflections s, t, u

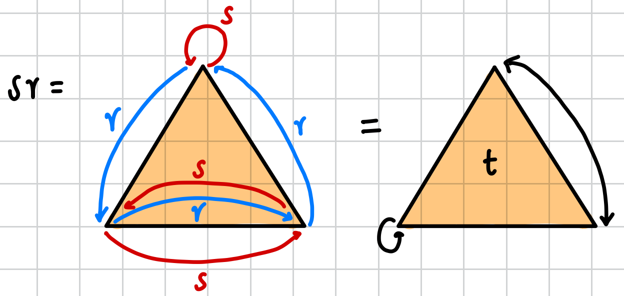


rotations $r, r^2, r^3 = I_G$

Then $G=\{I_G, r, r^2, s, t, u\}$

Symmetries are fns $\Longrightarrow$ compositions are right to left

Eg:



If $H=\{I_G, r, r^2\}$, then this set is self contained group of it's own

$\Longrightarrow$ H is a subgroup of G

$\Longrightarrow$ $H \leq G$

Looking at multiplication table

self contained

	1_G	r	r^2	s	t	u
1_G	1_G	r	r^2	s	t	u
r	r	r^2	1_G	u	s	t
r^2	r^2	1_G	r	t	u	s
s	s	t	u	1_G	r	r^2
t	t	u	s	r^2	1_G	r
u	u	s	t	r	r^2	1_G

Table for H

Cosets

Definition Left Coset

Let G be a group, $H \leq G$ and $a \in G$

The left coset with coset leader a is

$$aH = \{ah : h \in H\}$$

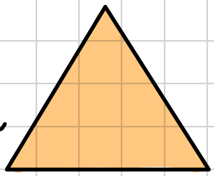
Note:

$$eH = \{eh : h \in H\} = \{h \in H\} = H$$

So H is a left coset

$\boxed{\text{'a' is called coset leader in } aH}$

Example:

$G = \text{Sym}$ 

$G =$

1_G	r	s
s	t	u

$\longleftarrow$ subgroup H

Consider $sH = \{s, sr, sr^2\} = \{s, t, u\}$ a (left) coset of H in G

$G =$

1_G	r	s
s	t	u

$=$

H
sH

$tH = \{t, tr, tr^2\} = \{t, u, s\} = sH$

Similarly $uH = tH = sH$, $rH = r^2H = H$ $\Longrightarrow$ $\boxed{\text{same coset can have different coset leaders}}$

Thus only 2 cosets of H in G, namely

$\underbrace{H = rH = r^2H}$ and $\underbrace{sH = tH = uH}$

different name for same coset

Definition Index

If $H \leq G$ then $[G:H]$ is the number of left cosets of H in G

$[G:H]$ is the **index** of H in G

In example above

H has index 2 in G $\Longrightarrow$ $[G:H] = 2$

Lagrange's Theorem

Theorem Lagrange's Theorem

Let G be finite group and $H \leq G$. Then the order of H divides order of G

$$|H| \mid |G|$$

Moreover

$$\frac{|G|}{|H|} = [G:H]$$

Proposition

$$sH = tH \iff t^{-1}s \in H$$

Proof:

Observe

$$sH = tH \iff t^{-1}sH = t^{-1}tH = H$$

$$\iff t^{-1}s \in H$$

$\blacksquare$

Order of $g \in G$

Let G be a group. For $a \in G$, $n \in \mathbb{N}$, we have

$$a^0 = e, \quad a^n = a \cdots\cdots a \quad \text{(n terms)}$$

$$a^{-n} = (a^{-1})^n = (a^n)^{-1}$$

Also $ee = e \implies e^{-1} = e$, we have

$$e^0 = e \quad ; \quad e^n = \underbrace{e \cdots\cdots e}_{n \text{ terms}} = e$$

$$(e^{-1})^n = e^n = e$$

i.e.

$$\boxed{e^z = e \quad \forall z \in \mathbb{Z}}$$

Consider the list $a \in G$

$$a (= a^1), a^2, a^3, \ldots$$

So either atleast one $a^i = e$ or no $a^i = e$

Definition order of element $a \in G$

Let G be a group. For any $a \in G$

The order of a written $o(a)$ is the least $n \in \mathbb{N}$ such that

$$a^n = e \quad \text{if such } n \in \mathbb{N} \text{ exists}$$

If no such n exists, then $o(a) = \infty$

Notation: use $o(g)$ or $|g|$

Example:

$G = \begin{array}{|c|c|c|} \hline 1_G & r & r^2 \\ \hline s & t & u \\ \hline \end{array} \quad \begin{array}{|c|c|c|} \hline 1 & 3 & 3 \\ \hline 2 & 2 & 2 \\ \hline \end{array}$ orders

Example: in S_n

$\sigma = (1\ 2\ 3\ 4) =$

$|\sigma| = 4$

Definition Disjoint Cycles

2 cycles are disjoint if they have no elements in common

$(a_1 \cdots a_m)$ and $(b_1 \cdots b_k)$ are disjoint if

$$\{a_1 \cdots a_m\} \cap \{b_1, \cdots, b_k\} = \emptyset$$

Proposition

Disjoint cycles commute i.e. $\alpha, \beta \in S_n$ are disjoint cycles then

$$\alpha\beta = \beta\alpha$$

Proposition

Let $\alpha \in S_n$, $\alpha \neq I_n$. Write

$$\alpha = \gamma_1 \gamma_2 \cdots \gamma_m$$

are disjoint. Suppose the length of γ_i is l_i for $1 \leq i \leq m$. Then

$$o(\alpha) = \operatorname{lcm}\{\ell_1, \dots, \ell_m\}$$

Example: in S_n

order of $(1\ 2)(3\ 4\ 5) = 6$

Example: Possible orders of elements of S_{10}

order	1	2	...	k	...	10
Eg	1_G	$(1\ 2)$		$(1\ 2 \cdots k)$		$(1\ 2 \cdots 10)$

(A) If $\text{lcm}\{n_1, n_2, \ldots, n_k\} = p^d$ where p prime then atleast one $n_i = p^d$

$\Rightarrow$ if $p^d \geq 10$, then $\nexists$ no $\sigma \in S_{10}$ with $|\sigma| = p^d$

This rules out orders 11, 13, 16, 17 and 19 (among orders b/w 10 and 20)

(B) If $\text{lcm} = p_1^{d_1} p_2^{d_2} \cdots p_m^{d_m}$ with $p_1, \ldots, p_m$ distinct primes, then to get a σ of this order, we require atleast

$$p_1^{d_1} + \cdots + p_m^{d_m}$$

distinct numbers

This rules out order 18 as $18 = 2 \cdot 3^2 \Rightarrow$ need $2 + 3^2 = 11 > 10$ numbers.

Hence we are left with

order	12	14	15	20	21
Eg	$(1\,2\,3)(4\,5\,6\,7)$	$(1\,2)(3\,4\,5\,6\,7\,8\,9)$	$(1\,2\,3)(4\,5\,6\,7\,8)$	$(1\,2\,3\,4)(5\,6\,7\,8\,9)$	$(1\,2\,3)(4\,5\,6\,7\,8\,9\,10)$

Now (A) rules out 23, 25, 27, 29

(B) rules out 22, 24, 26, 28

Finally

30
$(1\,2)(3\,4\,5)(6\,7\,8\,9\,10)$

Remarks:

1) g has order $1 \Rightarrow g^1 = 1_G$

$\Rightarrow g = 1_G$

2) If $g^n = 1_G$, at most we can say is

$$o(g) \mid n$$

Cyclic subgroups

Definition

Let G be a group, $a \in G$. We define

$$\langle a \rangle = \{a^z : z \in \mathbb{Z}\}$$

In '+' notation

$$\boxed{\langle a \rangle = \{za : z \in \mathbb{Z}\}}$$

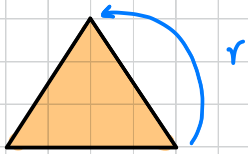
Definition Cyclic Subgroup

i) $\langle a \rangle$ is the cyclic subgroup generated by a

(ii) a group is cyclic if $G = \langle a \rangle$ for some $a \in G$. Then we say a generates G

Example:

$G = \text{Sym}$



$\langle r \rangle = \{r, r^2, r^3 = 1_G\}$

Lemma

For any $a \in G$, we have $\langle a \rangle$ is a commutative subgroup of G and

$$|\langle a \rangle| = o(a)$$

Proof:

If $o(a) = \infty$ then $a^i = a^j \implies i = j$

If $o(a) = \infty$ then if $i < j$ and $a^i = a^j \implies a^{j-i} = e$ contradiction ✗

So $\ldots a^{-2}, a^{-1}, e, a, a^2 \ldots$ are all distinct $\implies |\langle a \rangle| = \infty$

Since $a^i = a^j \implies a^{j-i} = e$, so if $j - i \neq 0$, we would say $o(a) \leq |j-i|$

Hence if $\boxed{o(a) = \infty, \ |\langle a \rangle| = \infty}$

If $o(a) = n \in \mathbb{N}$, then from remainder lemma, $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ and $e, a, a^2, \ldots, a^{n-1}$ are distinct

$$\boxed{\text{if } o(a) = n, \ |\langle a \rangle| = n \ \text{ and } \langle a \rangle = \{e, a^1, \ldots, a^{n-1}\}}$$

■

2. Group Actions

Definition of Group Actions

Definition Group Actions

Let G be a group, X be a set.

Say that G acts on X $\iff$ $\forall g \in G, \forall x \in X, \exists$ a uniquely determined

$$g * x \in X$$

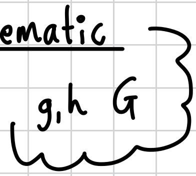
such that

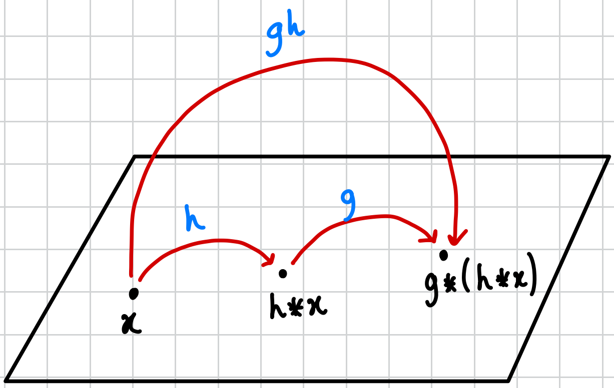
(A1) $1_G * x = x \qquad \forall x \in X$

(A2) $g * (h * x) = \underbrace{(gh)}_{\text{product in } G} * x \qquad \forall g, h \in G, x \in X$

Notation: $G \circlearrowright X$: G acts on X

Schematic





Remark: Group actions as functions

In a group action, each action is associated with a bijection

$$\sigma_g : X \to X; \quad \sigma_g(x) = g * x$$

Moreover we have $g^{-1} \in G$ which gives

$$\sigma_{g^{-1}} : X \to X, \quad \sigma_{g^{-1}}(x) = g^{-1} * x$$

Composing

$$\begin{aligned} \sigma_g(\sigma_{g^{-1}}(x)) &= \sigma_g(g^{-1} * x) \\ &= g * (g^{-1} * x) \\ &= (g g^{-1}) * x \qquad \text{A2} \end{aligned}$$

$$= 1_g * x$$

$$= x \qquad \text{A1}$$

i.e. $X \xrightarrow{\sigma_{g^{-1}}} X \xrightarrow{\sigma_g} X$ is the identity on X

Similarly $X \xrightarrow{\sigma_g} X \xrightarrow{\sigma_{g^{-1}}} X$

$\Rightarrow$ conclusion σ_g is a bijection

Examples of Group Actions

1) $G = S_n$

$X = \{1, 2, \dots, n\}$

Define

$$\underset{\in S_n}{\sigma} * \underset{\in X}{i} = \sigma(i) \leftarrow \text{image of } i \text{ under } \sigma$$

Checking axioms

(A1): $1_G * i = i$

(A2): $\tau * (\sigma * i) = \tau * (\sigma(i))$

$$= \tau(\sigma(i)) \underset{\text{defn of product in } S_n}{=} (\tau\sigma)(i) = (\tau\sigma) * i$$

Eg: S_4 and $X = \{1, 2, 3, 4\}$

$\sigma = (1\ 2\ 3\ 4)$ $\quad \sigma * 3 = 4$

$\sigma * 3 = 1$

2) $G = \mathbb{Z}$ under $+$

$X = \mathbb{R}$

Define $\mathbb{Z} \curvearrowright \mathbb{R}$ by

$$n * x = n + x$$

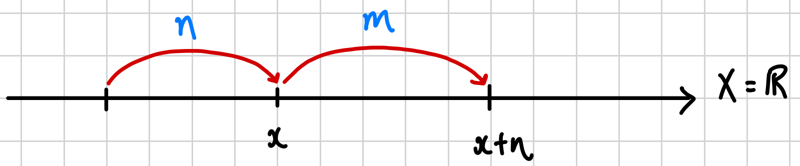
$\left(\begin{array}{l} gh \text{ becomes } n+m \\ 1_G \text{ becomes } 0 \\ g^{-1} \text{ becomes } -n \end{array}\right)$

Checking axioms

(A1): $0 * x = x$

(A2) $(n+m) * x = (n+m) + x$

$$= n + (m + x) = n + (m * x) = n * (m * x)$$

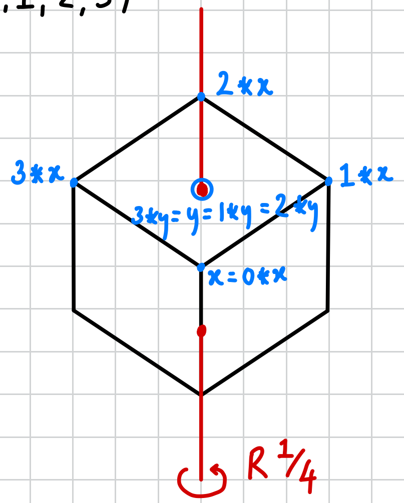


$\mathbb{Z}$ acts on $\mathbb{R}$ by translation

3) $G = \mathbb{Z}_n = \{0, 1, 2, 3, 4, \cdots n-1\}$ a group under + mod n

For $n=4$, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$

X = Cube



$\mathbb{Z}_4 \curvearrowright X$ by

$n * x = R^n(x)$

$\in \mathbb{Z}_4$ $\quad \in$ cube $\quad$ image of X under R^n

Eg: $2 * x = R^2(x)$

4) $G = GL(2, \mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid \det(A) \neq 0;$ invertible$\}$

A group under matrix multiplication.

Identity $= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

$X = \mathbb{R}^2 = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{R} \right\}$

Define $G \curvearrowright X$ by $\underset{GL(2,\mathbb{R})}{A} * \overset{\in \mathbb{R}^2}{\underline{v}} = A\underline{v}$ $\in \mathbb{R}^2$

<u>Checking axioms</u>:

(A1) $I_2 * \underline{v} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = \underline{v}$

(A2) $A * (B * \underline{v}) = A(B\underline{v}) = (AB)\underline{v} = (AB) * v$

5) G = any group

$X = G$ (G will act on itself)

Define $\underset{\in G}{g} * \underset{\in X = G}{x} = gxg^{-1}$ ← conjugation action

Check

(A1): $1_G * x = 1_G x 1_G^{-1} = x$

(A2): $g*(h*x) = g*(hxh^{-1})$

$= ghxh^{-1}g^{-1}$

$= (gh)x(gh)^{-1}$ $(gh)^{-1} = h^{-1}g^{-1}$

$= (gh)*x$

6) Any group G, $X = G$

$G \circlearrowright X$ via $g*x = gx$

both in G product in G

7) G a group and $H \leq G$

$X = G/H = \{aH \mid a \in G\}$

Then $G \circlearrowright X$ by

$$g * aH := (ga)H$$

<u>Well-defined</u>:

$a_1H = a_2H \iff a_2^{-1}a_1 \in H$

$\iff a_2^{-1}g^{-1}ga_1 \in H$

$\iff (ga_2)^{-1}ga_1 \in H$

$\iff (ga_1)H = (ga_2)H$

<u>Checking axioms</u>:

(A1) $1_G * aH = (1_G a)H = aH$

(A2) $g*(h*aH) = g*((ha)H)$

$= (g(ha)H) = (gh)*aH$

An equivalent definition of group action

Recall S_X = group of all bijections $X \to X$ (symmetric group on set X)

If G acts on X, then define

$$\theta : G \longrightarrow S_X$$

by $\theta(g) : X \to X$ is the map with

$$\theta(g)(x) = g * x$$

We saw on pg 10-11 that this is a bijection $X \to X$

The map $\theta(gh)$ is

$$\begin{aligned} \theta(gh)(x) &= (gh) * x \\ &= g * (h * x) \\ &= g * (\theta(h)x) \\ &= \theta(g)(\theta(h)x) \end{aligned}$$

i.e. $\theta(gh)$ the same map as $\underbrace{\theta(g)\theta(h)}_{\text{composition}}$

$$\Longrightarrow \theta \text{ is a homomorphism}$$

The converse is also true,

if $\theta : G \to S_X$ is a homomorphism, then $g * x = \theta(g)(x)$ is an action.

This leads to the following defn

Definition

Let G be a group and X be a set.

Say G **acts** on $X \iff \exists$ a homomorphism $\theta : G \longrightarrow S_X$

Orbits

Notation: Write gx for $g * x$

So we have

(A1) $1_G x = x \quad \forall x \in X$

(A2) $(gh)x = g(hx)$

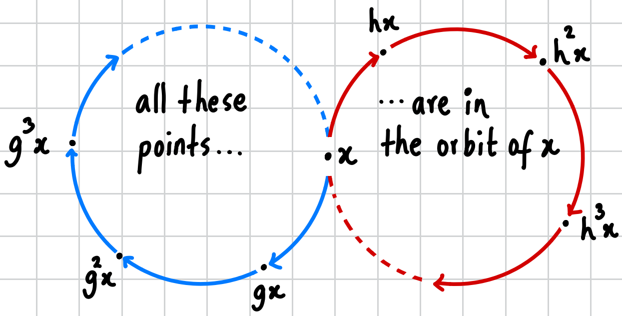
Definition Orbits

Let $G \curvearrowright X$.

Consider $x \in X$. The orbit of x denoted $G * x$ or $\mathrm{Orb}_G(x)$ is

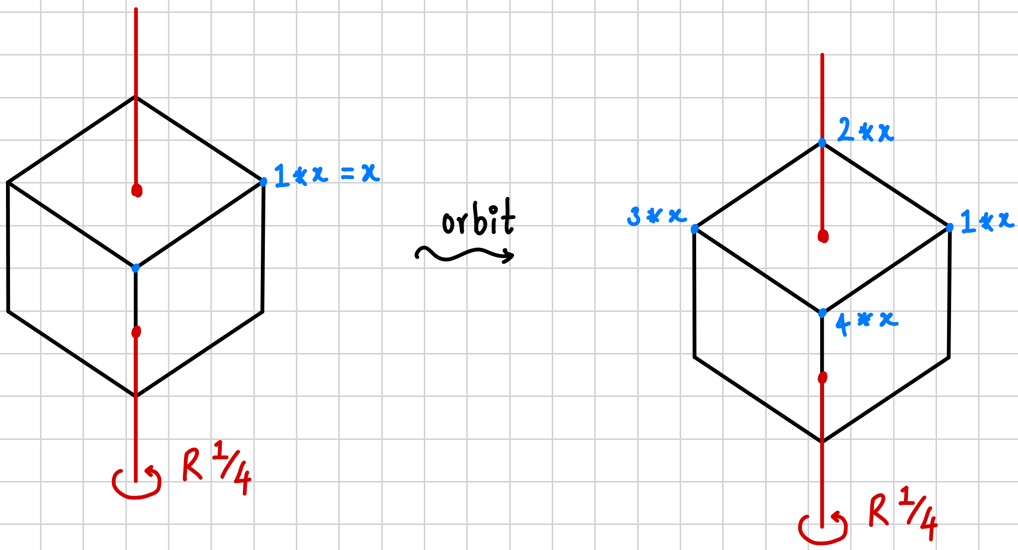
$$G * x = \{ g * x \mid g \in G \} \subseteq X$$

Schematic



Examples of orbits

1) $\mathbb{Z}_4 \curvearrowright$ Cube : action by rotation around fixed axis



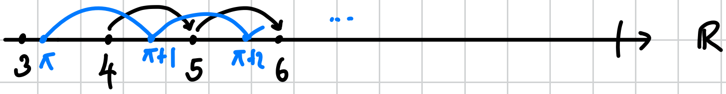
In fact this is (almost always) true for generic points on the cube

$$|\text{Orbit}| = 4$$

Exceptions: 2 pts where axis merges at top and bottom, $|\text{orbit}| = 1$

2) $\mathbb{Z} \curvearrowright \mathbb{R}$

$$n * r = n + r \quad n \in \mathbb{Z},\ r \in \mathbb{R}$$



$$\mathrm{Orb}_{\mathbb{Z}}(4) = \mathbb{Z} = \{4 + n \mid n \in \mathbb{Z}\}$$

$$\mathrm{Orb}_{\mathbb{Z}}(\pi) = \{\pi + n \mid n \in \mathbb{Z}\}$$

Properties of orbits

Lemma

$G \curvearrowright X$.

(i) $x \in G * x \quad \forall x \in X$

(ii) $y \in G * x \implies G * y = G * x$

(iii) $y \notin G * x \implies G * x \cap G * y = \phi$

Proof:

(i) $1_G * x \implies x \in G * x$

(ii) $y \in G * x \implies y = gx$ for some $g \in G$

If $z \in G * y \implies z = g'y$ for some $g' \in G$

$\implies z = g' * (g * x)$

$\implies z = (g'g) * x$

$\implies z \in G * x$

$\implies G * y \subseteq G * x$

If $z \in G * x \implies z = g'' * x$ for some $g'' \in G$

Now $y = g * x \implies g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = I_G x = x$

Thus $z = g''(g^{-1}y) = (g''g^{-1})y \implies z \in G * y$

$\implies G * y \subseteq G * x$

Hence $G * x = G * y$

(iii) Suppose $z \in G * x \cap G * y \Rightarrow z = g * x = h * y$ for some $g, h \in G$

$$\Rightarrow y = (h^{-1}g) * x$$

$$\Rightarrow y \in G * x$$ (contrapositive proven)

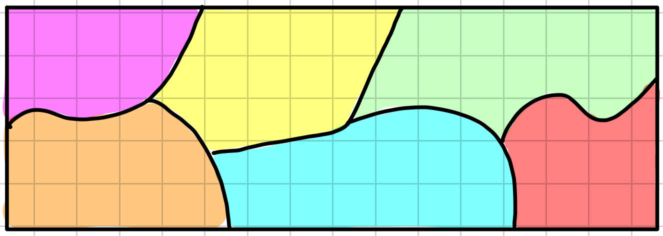
■

Note:

"Being in same orbit" is an equivalence relation

Moral: every element of X is contained in precisely one orbit, i.e. orbits partition X

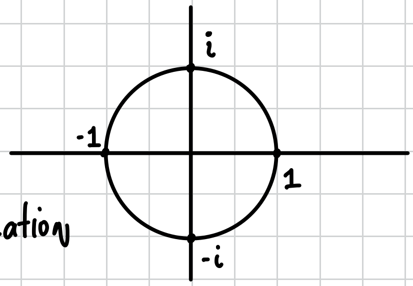
$X =$



Example:

$G = \{ z \in \mathbb{C} \mid |z| = 1 \}$

$= \{ e^{i\theta} \mid \theta \in \mathbb{R} \}$



Group operation is multiplication in $\mathbb{C}$

$$e^{i\theta} e^{i\phi} = e^{i(\theta+\phi)};$$

$\exists$ a homomorphism $(\mathbb{R}, +) \longrightarrow G$

$$\theta \longmapsto e^{i\theta}$$

Let $X = \mathbb{C}$ and $G \curvearrowright X$ by

$$e^{i\theta} * z = e^{i\theta} z$$

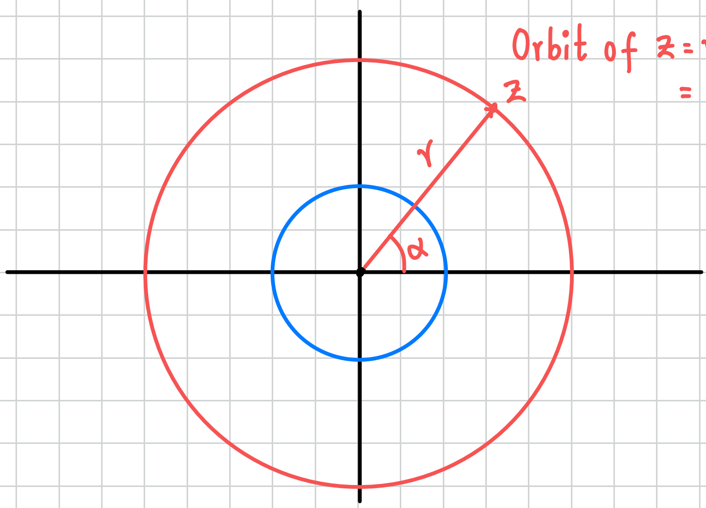
if $z = re^{i\varphi}$,

$$e^{i\theta} * z = re^{i(\theta+\varphi)}$$

Orbit of $0 = \{0\}$

Orbit of $1 = \{ e^{i\theta} \mid \theta \in \mathbb{R} \}$ = unit circle

Orbit of $z = re^{i\alpha}$ is $\{ re^{i(\alpha+\theta)} : \theta \in \mathbb{R} \}$ = circle of radius r in $\mathbb{C}$



Get one orbit for each $r \in \mathbb{R}_{\geq 0} = \mathbb{R}_0^+$

Example: If $G = X$ and action

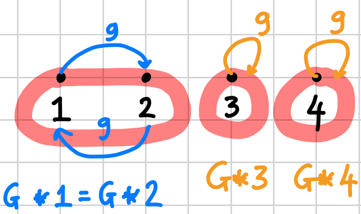
$$g * x = gxg^{-1}$$

The orbits are conjugacy classes in G

$$G * x = \{gxg^{-1} : g \in G\}$$

Example:

$$G = \{e, (1\,2)\} \leq S_4 \curvearrowright \{1,2,3,4\}$$



G has 3 orbits

S_4 has only 1 orbit

Transitivity

Definition

G acts on X transitively if $\exists$ precisely one orbit:

$\forall x \in X$, we have $G * x = X$.

Put another way, $\forall x, y \in X$, $\exists$ a $g \in G$ s.t

$$gx = y$$

Example: $G = S_n \curvearrowright \{1, 2, \dots, n\} = X$

Alfie Kashane

Finding orbit of 1: $\forall\, k \in X$, let $(1\,k) \in S_n$

Then $(1, k) * 1 = k \implies k \in$ orbit of 1

$\implies G * 1 = X$

$\implies$ action is transitive

Stabilizers

Definition Stabilizer

$G \curvearrowright X$, $x \in X$.

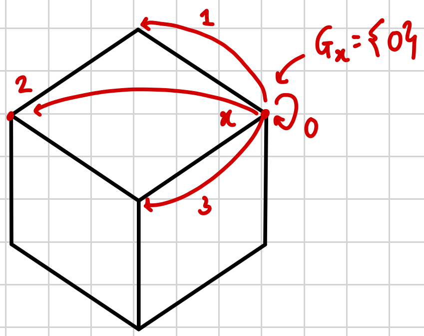
The stabilizer of x is

$$G_x = \mathrm{Stab}_G(x) = \{ g \in G \mid g * x = x \} \leq G$$

Note: When G acts on X:

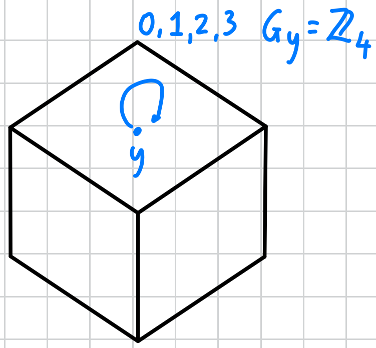
$$\left.\begin{array}{r} \text{orbits} \subseteq X \\ \text{stabilizers} \leq G \end{array}\right\} G \curvearrowright X$$

Example: $\mathbb{Z}_4 \curvearrowright$ Cube: action by rotation around fixed axis



Stabilizer of "generic point" fixes point

$\Longrightarrow$ trivial subgroup $\{1_G\}$



Stabilizer of one of the points where axis goes $= G$

Example: In example pg 17

$$\mathrm{Stab}_G(3) = \mathrm{Stab}_G(4) = G$$

$$\mathrm{Stab}_G(1) = \mathrm{Stab}_G(2) = \{e\}$$

Also have

$$\mathrm{Stab}_{S_4}(1) = \{e, (2\,3), (2\,4), (3\,4), (2\,3\,4), (2\,4\,3)\} \cong S_3$$

$$\mathrm{Stab}_{S_4}(2) = \{e, (1\,3), \dots \qquad\qquad \} \cong S_3$$

Lemma

$G \curvearrowright X$, $x \in X$

$$G_x \leq G$$

Proof:

(1): $1_G * x = x \Longrightarrow 1_G \in G_x \Rightarrow G_x \neq \emptyset$

(2) Suppose $g, h \in G_x$, then $(gh) * x = g * (h * x)$ (since $h \in G_x$)

$$= g * x$$

$$= x \qquad \text{since } g \in G_x$$

$$\Longrightarrow gh \in G_x$$

(3) Let $g \in G_x \Longrightarrow x = g * x$

$$\Longrightarrow g^{-1} * x = x$$

$$\Longrightarrow g^{-1} \in G_x$$

∎

Examples of Stabilizers

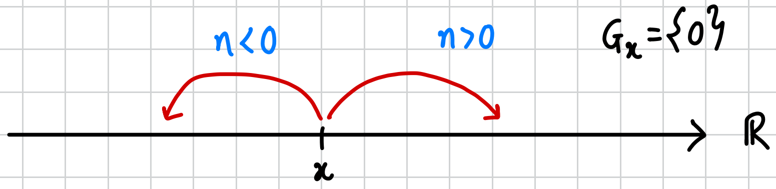
1) $G = S_4 \curvearrowright \{1, 2, 3, 4\} = X$

$$G_2 = \{\sigma \in S_4 \mid \sigma(2) = 2\}$$

$$= \{I_G, (1\,3)\,(1\,4), (3\,4), (1\,3\,4), (1\,4\,3)\} = S_Y \text{ for } Y = \{1, 3, 4\}$$

2) $\mathbb{Z} \curvearrowright \mathbb{R}$

$$x \overset{n}{\longmapsto} n+x = n * x$$



$G_x = \{0\}$

3) $GL(2,\mathbb{R}) \curvearrowright \mathbb{R}^2$

$$v \overset{A}{\longmapsto} Av = A * v$$

$G_v = \{A \in GL(2,\mathbb{R}) : Av = v\}$ = invertible 2x2 matrices having eigenvector v with eigenvalue 1.

4) $G \curvearrowright G$ by conjugation

$$g * x = g x g^{-1}$$

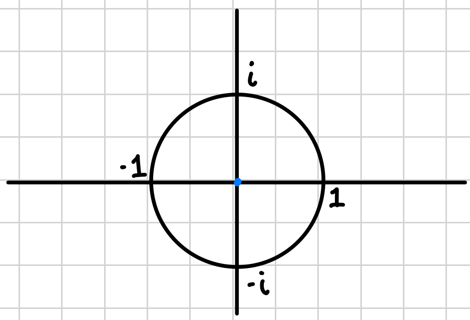
Then

$$G_x = \{g \in G \mid g x g^{-1} = x\}$$
$$= \{g \in G \mid gx = gx\}$$
$$= g \in G \text{ that commutes with } x$$

Example: $(\mathbb{R},+)$ acting on $\mathbb{C}$, $\mathbb{R} \curvearrowright \mathbb{C}$

$$\theta * z = e^{i\theta} z$$ (use hom $\mathbb{R} \to$ circle and action of circle)

Let $1 \in \mathbb{C}$, orbit



$\mathrm{stab}_{\mathbb{R}}(1) = \{2n\pi \mid n \in \mathbb{Z}\} \leq \mathbb{R}$

$\mathrm{stab}_{\mathbb{R}}(0) = \mathbb{R}$

$S_4 \curvearrowright \{1,2,3,4\}$

Orbit of $1 = \{1,2,3,4\}$

Stabilizer $= \{e, (2\,3), \cdots, (2\,4\,3)\} \cong S_3$

Theorem Orbit-Stabilizer Theorem

$G \curvearrowright X$ and $x \in X$. The map

$$G/G_x \longrightarrow G * x$$

cosets — orbits of X

$$gG_x \mapsto g * x$$

is a bijection.

Hence if G is finite

$$|G| = |G * x| \cdot |G_x|$$

Proof:

Call map ϕ so $\phi(gG_x) = g * x$

<u>Well-defined and one-to-one</u>:

$$\begin{aligned} gG_x = hG_x &\iff h^{-1}g \in G_x \\ &\iff (h^{-1}g) * x = x \\ &\iff g * x = h * x \\ &\iff \phi(gG_x) = \phi(hG_x) \end{aligned}$$

<u>Onto</u>: Given any $y \in G * x$; $y = g * x$ for some $g \in G$

$$\phi(gG_x) = g * x = y \implies \phi \text{ is onto}$$

Now if $|G| < \infty$, then

$$\left| G/G_x \right| = [G : G_x] = |G|/|G_x|$$

So $|G|/|G_x| = |G * x| \implies |G| = |G * x| \cdot |G|$ ∎

Corollary

Let G (finite) $\curvearrowright X$

Size of an orbit $|G * x|$ divides $|G|$.

$$|G * x| \mid |G|$$

Warmup:

$|G| = 25$, $|X| = 36 \Rightarrow G$ has a fixed point in X

$|G| = 25 \Rightarrow$ orbits of size 1, 5 or 25

X is partitioned by orbits

All ways to partition a set of size 36 into pieces of sizes 1, 5, 25 involve atleast one piece of size 1

$x \in X$ has orbit of size 1 $\Rightarrow g * x = x \quad \forall g \in G$

$\Rightarrow x$ is a fixed point

Counting orbits

2 extreme cases

1) Action is trivial $\Rightarrow g * x = x \quad \forall g \in G \; x \in X$

2) There is one orbit: the action of G is transitive on X

i.e. $\forall x, y \in X$. $\exists g \in G$ with $y = g * x$

$S_n \curvearrowright \{1, \dots, n\}$ is transitive

Theorem (Cauchy)

G a finite group and p a prime with $p \mid |G|$.

Then $\exists$ an element of order $p \in G$ (hence also a subgroup of size p (cyclic))

Proof:

Let $X = \{(x_1, \dots, x_p) \mid x_i \in G, \; x_1 \cdots x_p = 1_G\} \subseteq \underbrace{G \times \cdots \times G}_{p \text{ times}}$

There are $|G|$ choices for x_1. $|G|$ choices for x_2, ... $|G|$ choices for x_{p-1}

Then

$$x_1 \cdots x_p = 1_G \Rightarrow x_p = (x_1 \cdots x_{p-1})^{-1}$$

Can choose $x_1, \dots, x_{p-1}$ freely as long as

$$x_p = (x_1 \cdots x_{p-1})^{-1}$$

$\Rightarrow |X| = |G|^{p-1}$ which is divisible by p because $|G|$ is

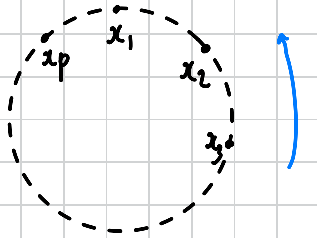
$p \mid |G| \Rightarrow p \mid |X|$

Let $\mathbb{Z}_p \curvearrowright X$

$\mathbb{Z}_p = \{0, 1, \cdots, p-1\}$ with $+$ mod p

$\mathbb{Z}_p \curvearrowright X$ by $m * (x_1, \cdots, x_p) := (x_{m+1}, \cdots, x_p, x_1, \cdots, x_m)$, $m \in \mathbb{Z}_p$

Let $\mathbb{Z}_p$ act on X by "cycling" tuples



$m \in \mathbb{Z}_p$ rotates by m

$\mathbb{Z}_p$ acts by rotation

Then by corollary 1 $\Rightarrow$ each orbit in X has size 1 or p

Have $(1_G, \cdots, 1_G) \in X$ and $m * (1_G, \cdots, 1_G) = (1_G, \cdots, 1_G)$ $\forall m \in \mathbb{Z}_p$

$\Longrightarrow$ orbit of $(1_G, \cdots, 1_G)$ has size 1

Suppose all other orbits have size p. Then $|X| = \sum$ sizes of orbits (orbits partition X)

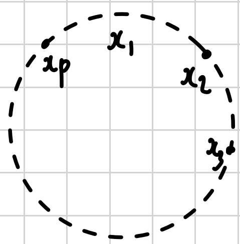
$$= \underbrace{1}_{\text{orbit of } (1_G, \cdots, 1_G)} + \underbrace{kp}_{\text{all other orbits}}$$

$\Longrightarrow |X| \equiv 1 \bmod p$ ※ since $p \mid |X|$

Contradiction $\Rightarrow \exists$ another orbit of size 1, i.e.

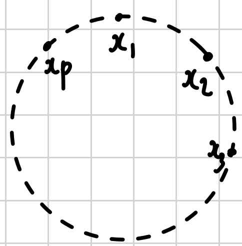
$(x_1, \cdots, x_p) \neq (1_G, \cdots, 1_G) \in X$ whose orbit is size 1

$\Longrightarrow m * (x_1, \cdots, x_p) = (x_1, \cdots, x_p)$ $\forall m$



$m \in \mathbb{Z}_p$ rotates by m

=



$\Longrightarrow x_1 = x_2 = \cdots = x_p = x$ (for example)

Thus $\exists\, x \neq 1_G$ s.t. $x^p = 1_G \Longrightarrow$ order of x divides p

$\Longrightarrow o(x) = 1$ or $o(x) = p$

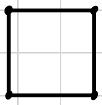
As $x \neq 1_G \implies o(x) = p$

Hence $H = \{x, x^2, \cdots, x^{p-1}, x^p = 1_G\} \leq G$ of size p exists

$\blacksquare$

3. How to Count

Example: Vertices of a square



square and we can color R B

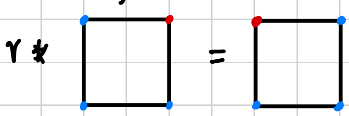
Question: How many different squares?? What if we are allowed to rotate?

Answer: $|X| = 2^4 = 16$

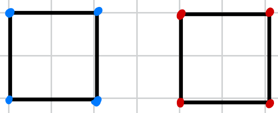
$X = \{\text{all possible colored squares}\}$

$G = \{1_G, r, r^2, r^3\}$ group of rotations

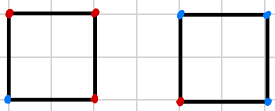
$G \curvearrowright X$ in "the obvious way"



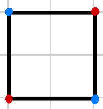
$\rightsquigarrow$ count orbits



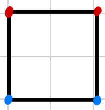
orbit of size 1 stabilizer size 4



two orbits of size 4, stabilizer of size 1



orbit of size 2, stabilizer of size 2 $(= \{1_G, \curvearrowright\pi\})$



orbit of size 4

$\rightsquigarrow$ get orbits of sizes $1+1+4+4+4+2=16$

We get 6 orbits in total

Fix

Definition

$G \curvearrowright X$

$\mathrm{Fix}(g) = \{x \in X \mid g * x = x\} \subseteq X$

Burnside Thm

Theorem Burnside Theorem

Let G be a finite group, X a finite set, $G \curvearrowright X$

$$\#\,\text{orbits} = \frac{1}{|G|} = \sum_{g \in G} |\text{Fix}(g)|$$

Proof:

Consider the set

$$Y = \{(g, x) : gx = x\} \subseteq G \times X$$

and count size of Y in 2 ways.

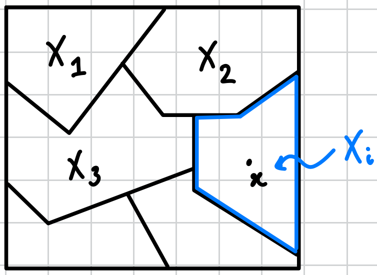
(1) For fixed g, there are $|\text{Fix}(g)|$ x's such that $gx = x$

Thus $|Y| = \sum_{g \in G} |\text{Fix}(g)|$

(2) For fixed x, there are $|G_x|$ g's s.t $gx = x$

Thus $|Y| = \sum_{x \in X} |G_x|$

orbits



Massaging this sum

Suppose $X_1, \dots, X_t$ are in orbits in X

Note: t is the number we want

$$|Y| = \sum_{x \in X} |G_x| = \sum_{i=1}^{t} \sum_{x \in X_i} |G_x|$$

orbits partition X

$$= \sum_{i=1}^{t} \sum_{x \in X_i} \frac{|G|}{|X_i|}$$

$x \in X_i$, then $|G| = |G \cdot x||G_x| \Rightarrow |G| = |X_i||G_x|$

$$= |G| \sum_{i=1}^{t} \sum_{x \in X_i} \frac{1}{|X_i|}$$

$$= |G| \sum_{i=1}^{t} \frac{|X_i|}{|X_i|} = |G| \sum_{i=1}^{t} 1 = |G| t$$

$$\Longrightarrow t = \#\,\text{orbits} = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

$\blacksquare$

Note

- $Fix(g) \subseteq X \quad G_x \leq G$
- Burnside Thm says

  #orbits = average # of fixed points

Example: pg 26 contd

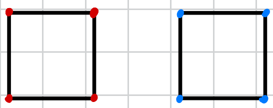
Counting orbits using burnside

$$\#\text{orbits} = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

(i) $g = 1_G$: have $Fix(1_G) = X$ always happens

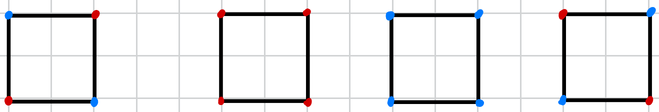
$$\implies |Fix(1_G)| = |X| = 2^4$$

(ii) $g = r$



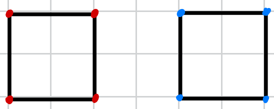
$$\implies |Fix(r)| = 2$$

(iii) $g = r^2$



$$\implies |Fix(r^2)| = 4$$

(iv) $g = r^3$

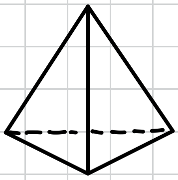


$$\implies |Fix(r^3)| = 2$$

Hence $\#\text{orbits} = \frac{1}{4}(2^4 + 2 + 2^2 + 2) = 6$

∎

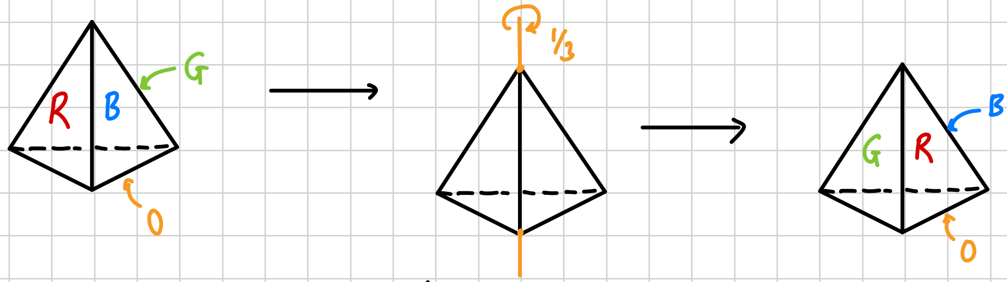
Example: Let $q \in \mathbb{Z}^{>0}$. How many ways can you color the faces of



using q colors

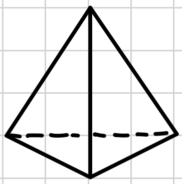
Naive attempt: q choices for each face $\Rightarrow q^4$ colored tetrahedra

problem:



are really the same, eventhough counted twice

Attempt #2: G = rotational symmetries of



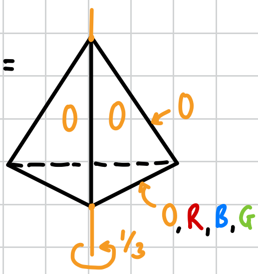
$X = \{$set of all possible painted tetrahedra$\}$

$G \curvearrowright X$ with a rotation, sending a painted tetrahedron to its image under rotation

Count # orbits

(i) $|Fix(1_G)| = |X| = q^4$ = naive answer

(ii) $g =$



top 3 must be same color - q possibilities

bottom - anything - q possibilities

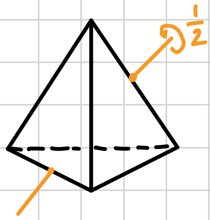
$\Rightarrow q^2$ possible fixed tetrahedra

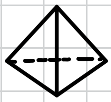
Similarly for other $1/3$ turns and there are 4 $1/3$ turns $\Rightarrow 4 \times q^2$

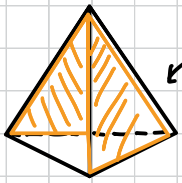
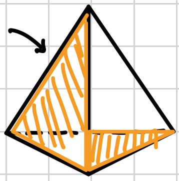
(iii) $g = 2/3$ rotation $= 1/3$ rotation in opposite direction

$\Rightarrow q^2$ fixed here as well

4 $2/3$ rotations $\Rightarrow 4 \times q^2$

(iv) $g =$ 

q^2 fixed 

 swapped by g 

q choices for pair $\quad\quad$ q choices for pairs

3 rotations like this $\Longrightarrow 3 \times q^2$

Thus

$$\# \text{ of painted tetrahedra} = \frac{1}{12}\left(q^4 + 11q^2\right)$$

Eg $q = 4$

$$\# = 36$$

4. Sylow Theory

Recall: Lagrange's Theorem

(1) **Theorem** Lagrange's Theorem

Let G be finite group and $H \leq G$. Then the order of H divides order of G

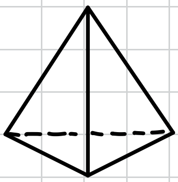
$$|H| \mid |G|$$

Moreover

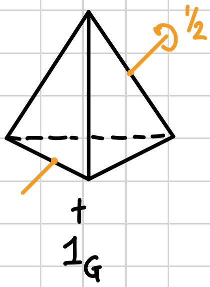
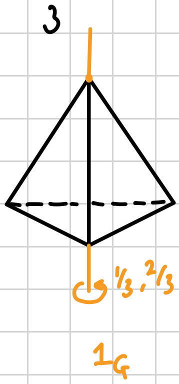
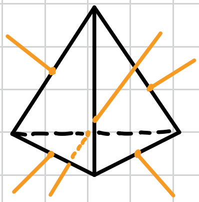
$$\frac{|G|}{|H|} = [G:H]$$

(2) Converse of Lagrange's Thm not true.

if $m \mid |G|$ then G has a subgroup of order m is NOT true

e.g. 1) G = rotations of  $\Longrightarrow |G| = 12$

with divisors

1	2	3	4	6	12
$\{1_G\}$				NONE	$\lvert G\rvert$

2) $G = S_5$, symmetric group

$|G| = 5! = 120$

So that $15 \mid |G|$ but NOT subgroup of order 15

(3) But (!) we do have a partial converse to Lagrange: Cauchy's Thm

p prime, if $p \mid |G|$, then G has prime subgroup of order p

Sylow p-subgroup

Definition Sylow p-subgroup

G be a finite group with

$$|G| = p^n \cdot m \quad \text{where } p \text{ prime}$$

and $\gcd(p,m)=1$. Then subgroup $H \leq G$ with

$$|H| = p^n$$

is called a Sylow p-subgroup of G

Example:

Suppose $|G| = 2^3 \cdot 5^2 \cdot 13$

then a subgroup of order

2^3 is a Sylow 2-subgroup

5^2 is a Sylow 5-subgroup

13 is a Sylow 13-subgroup

Sylow 1^{st} Theorem

Theorem Sylow's 1st Theorem

If G has order $p^n m$ with p prime and $\gcd(p,m)=1$, then

G has a Sylow p-subgroup

Proof:

Let $G \curvearrowright X$

X = set of all subsets of G having p^n elements.

Acts by $g \in G$, $A \in X$, then

$$g * A = gA = \{ga : a \in A\}$$

Then X has $\binom{|G|}{p^n} = \binom{p^n m}{p^n}$

"Ex:" p does not divide $\binom{p^n m}{p^n}$

$\Longrightarrow p$ does not divide $|X|$

Also X = disjoint union of orbits

$$\Longrightarrow |X| = \sum \text{size of orbits.}$$

<u>Conclusion</u>: $\exists$ an orbit whose size is NOT divisible by p

Call this orbit $A \in X$

By orbit-stabilizer theorem then says

$$p^n m = |G| = \underbrace{|G * A|}_{\text{orbit}}\,\underbrace{|G_A|}_{\text{stabilizer}}$$

$$p^n \mid |G| \Longrightarrow p^n \mid |G*A|\,|G_A|$$

$$\Longrightarrow p^n \mid |G_A| \qquad (*)$$

$$\Longrightarrow p^n \leq |G_A|$$

Now let $g \in G_A$ and $a \in A$. Then

$$gA = A$$

and in particular $ga \in A$. Thus

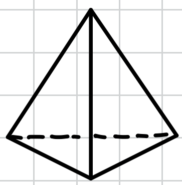
$$G_A a \subseteq A$$

Finally
$$|G_A| = |G_A a| \leq |A| = p^n \quad (*)$$

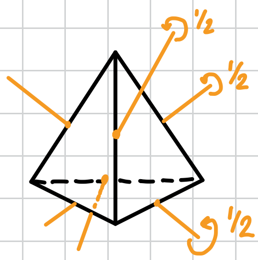
By $(*)$ and $(**)$

$$|G_A| = p^n$$

But $|G_A|$ is a subgroup. $\blacksquare$

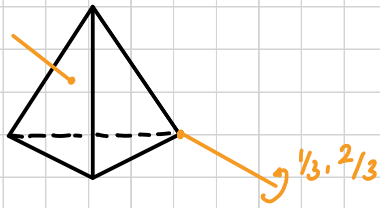
Example G = rotations of 

with $|G| = 2^2 \cdot 3$

$\Longrightarrow$ Sylow 2-subgroup order 2^2 

+ identity

Sylow 3 subgroup order 2



Example: S_5 has order $120 = 2^3 \cdot 3 \quad 5$

$\Rightarrow S_5$ has subgroup of order $2^3 = 8, 3, 5$

Note: S_5 does NOT have a subgroup of order 3.5 (prove!)

Sylow 2nd Theorem

Theorem Sylow 2nd Theorem

If P_1, P_2 are Sylow p-subgroups then $\exists$ a $g \in G$ s.t

$$P_2 = g P_1 g^{-1}$$

Sylow 3rd Theorem

Theorem Sylow's 3rd Theorem

Let N_p be the number of Sylow p-subgroups of G where $|G| = p^n m$. Then

(i) $N_p \equiv 1 \pmod p$

(ii) $N_p \mid m$

Proof:

(i) Let $X = \{H_1, \dots, H_{N_p}\} = \{\text{set of Sylow p-subgroups of } G\}$

$H_1 \curvearrowright X$;

$$h * H_j = h H_j h^{-1}$$

Exercise

(a) hH_jh^{-1} is also a Sylow p-subgroup

(b) Above is an action

(c) $K_j :=$ Stabilizer of H_j. Then $K_j = H_1 \cap H_j$

From Exercise

$$K_1 = H_1 \implies \text{stabilizer of } H_1 \text{ is just } H_1$$
$$\implies \text{orbit contains 1 element}$$

For $j \neq 1$ then $K_j = H_1 \cap H_j$ is a proper subgroup of H_1 where

$$|H_1| = p^n$$

Thus $|K_j| = p^k$ for some $k < n$

By orbit-stabilizer theorem

$$p^n = |H_1| = |K_j|\,|H_1 * H_j|$$

we get $p^n = p^k |H_1 * H_j|$ with $k < n$, so

$$p \mid |H_1 * H_j|$$

As X is the disjoint union of orbits. we have:

$$\begin{aligned} N_p &= \#\text{Sylow } p\text{-subgroups} \\ &= |X| \\ &= \sum \text{sizes of the orbits} \\ &= \underbrace{1}_{\text{orbit of } H_1} + \underbrace{Mp}_{\text{all other orbits have size } p} \equiv 1 \pmod p \end{aligned}$$

(ii) Use a group action

Let $G \curvearrowright X$

$$X = \{H_1, H_2, \dots, H_{n_p}\} = \{\text{set of Sylow-}p\text{-subgroups}\}$$

by:

$$g * H = gHg^{-1}$$

Makes sense? (show action)

Firstly is gHg^{-1} a Sylow p-subgroup. i.e. another element of X

(a) gHg^{-1} is a subgroup.

$$a, b \in gHg^{-1} \Rightarrow \left.\begin{array}{l} a = gh_1g^{-1} \\ b = gh_2g^{-1} \end{array}\right\} \Rightarrow ab = gh_1g^{-1}gh_2g^{-1}$$

$$h_i \in H \qquad = g\underbrace{h_1h_2}_{\in H}g^{-1} \in gHg^{-1}$$

$a^{-1} \in gHg^{-1}$

$e \in gHg^{-1}$

(b) Sylow

$$\underset{\text{order } p^n}{H} \xrightarrow{\text{bijection}} \underset{p^n \text{ elements}}{gH} \xrightarrow{\text{bijection}} \underset{\text{order } p^n}{gHg^{-1}} \quad \text{(prove)}$$

$\Rightarrow gHg^{-1}$ a Sylow p-subgroup.

(Also show (A1) and (A2) ....)

Now we have $G \curvearrowright X$. Then Sylow #2 $\Rightarrow$ action has 1 orbit, namely all of X transitive action

By orbit-stabilizer theorem, action has 1 orbit

$$|G| = p^n m = |G * H_1|\,|G_{H_1}| = |X|\,|G_{H_1}|$$

$\Rightarrow$ $|X|$ divides $p^n m$

Now consider $\gcd(|X|, p)$. Firstly

gcd divides $p \Rightarrow \gcd = 1$ or p

(a) $\gcd = p \Rightarrow p \mid |X|$ a contradiction since Sylow #3 (i) says

$$|X| = N_p \equiv 1 \pmod p \not\equiv 0 \pmod p$$

(b) Thus $\gcd = 1$

Note: $a \mid bc$ and $\gcd(a, b) = 1 \Rightarrow a \mid c$

$\Rightarrow |X| = N_p$ divides m ■

Theorem

H is a normal subgroup of G

$$\Updownarrow$$

$$gH = Hg$$

$$\Updownarrow$$

$$gHg^{-1} = H$$

Proof: Prove later

Observation: Suppose the number N_p of Sylow p-subgroups is equal to one.

Call the Sylow p-subgroup H, say

Then, for any g, we have gHg^{-1} is also a Sylow p-subgroup

But (!) there is only one such, so that

$$gHg^{-1} = H$$

$$\boxed{N_p = 1 \Longrightarrow H \text{ is normal}}$$

Example:

Suppose G has order 175.

$|G| = 5^2 \times 7$. Consider $N_5 = \#$ of Sylow 5-subgroups.

Sylow #3(ii) $\Longrightarrow N_5 \mid 7$

$\Longrightarrow N_5 = 1$ or 7

Sylow #3(i) $\Longrightarrow N_5 \equiv 1 \bmod 5$

$\Longrightarrow N_5 = 1$

Conclusion: G contains a normal subgroup with $5^2 = 25$ elements.

5. Conjugacy

Definition

Two elements $g_1, g_2 \in G$ are conjugates iff

$$g_2 = h g_1 h^{-1} \text{ for some } h \in G \qquad (*)$$

Notes:

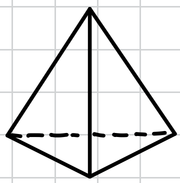
(1) $g_2 = h g_1 h^{-1} \implies h^{-1} g_2 h = g_1$

$\implies (h^{-1}) g_2 (h^{-1})^{-1}$

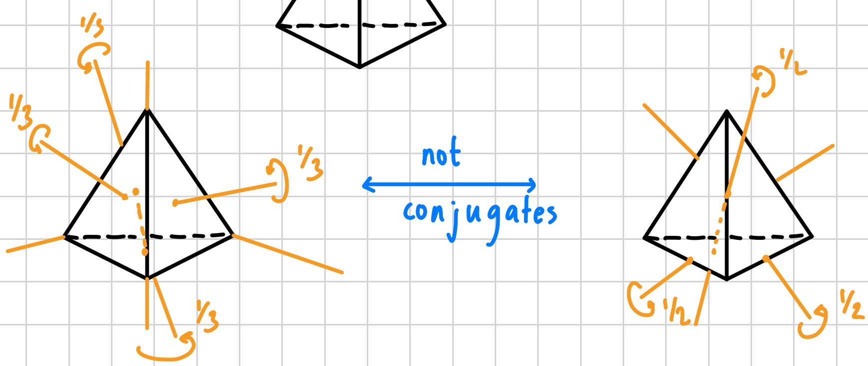
$\implies k g_2 k^{-1} = g_1$ for $k \in G$

(2) Intuitively conjugate elements have similar algebraic properties.

Example: G = rotations of



then



are all conjugates are all conjugates

Example:

$g_2 = h g_1 h^{-1}$ and $g_1^n = 1_G$

$$g_2^n = (h g_1 h^{-1})^n$$

$$= h g_1 \underbrace{h^{-1} \cdot h}\, g_1 \underbrace{h^{-1} \cdots h}\, g_1 h^{-1} \quad (n \text{ times})$$

$$= h g_1^n h^{-1}$$

$$= h h^{-1} = 1_G$$

Similarly $g_1 = h^{-1} g_2 h$ so that $g_2^n = 1_G \implies g_1^n = 1_G$

$\implies$ thus g_1 and g_2 have same order.

Example:

$G = GL(n, \mathbb{R})$

Then in linear algebra, an $A \in G$ is diagonalizable when

$$A = MDM^{-1}$$

for some M and D diagonal.

- A and D are conjugates (similar matrices)
- A and D represent the same linear map with different coordinates
- They have same eigenvalue, trace and determinant

Conjugacy class

Definition Conjugacy class

If $g \in G$, then conjugacy class of g is

$$g^G = \{hgh^{-1} : h \in G\}$$

the set of all conjugates of g

Centralizer

Definition Centralizer

The centraliser of g is

$$C_G(g) = \{h \in G \mid hgh^{-1} = g\}$$

Example: $G \curvearrowright G$ by conjugacy

$$h * g = hgh^{-1}$$

- orbit $= g^G$
- stabilizer $= C_G(g)$
- $\mathrm{Fix}(h) = \{g \in G \mid hgh^{-1} = g\} = C_G(h)$.

Hence

$$\boxed{\#\text{ conjugacy classes} = \frac{1}{|G|} \sum_{h \in G} |C_G(h)|}$$

Burnside thm

Example: G is Abelian (i.e. $gh = hg \ \forall g, h$)

Then

$$hgh^{-1} = hh^{-1}g = g$$

$$\Longrightarrow \quad g^G = \{g\} \text{ in an Abelian group}$$

Example: in any G

$$h1_G h^{-1} = 1_G \Longrightarrow 1_G^G = \{1_G\}$$

Conjugacy in S_n

Definition Cycle Structure

The **cycle structure** of a $\sigma \in S_n$ is a formal expression of the form

$$n_1 + n_2 + \cdots + n_k$$

where $n_i \in \mathbb{Z}^{>0}$ and $n_1 \geq n_2 \geq \cdots \geq n_k$ where if σ is written as a product of disjoint cycles, then there are cycles of length $n_1, n_2, \cdots n_k$ including cycles of length 1

Example:

1) $\sigma = (1\ 2\ 3)(4\ 5) \in S_5$ has cycle structure $3+2$
2) $\sigma = (1\ 2\ 3)(4\ 5) \in S_7$ has cycle structure $3+2+1+1$
3) $\sigma = (1\ 2\ 3\ 5)(2\ 4\ 3) = (1\ 2\ 4\ 3)$ has cycle structure $4+1$

Theorem

Two elements of S_n are conjugate

$$\Updownarrow$$

they have same cycle structure

Proof:

$(\Longrightarrow)$: Suppose $\tau = \mu \sigma \mu^{-1} \in S_n$

Consider

$$(a_1\ a_2 \cdots a_n)$$

a cycle of σ. Then

$$\boxed{\mu(a_1\ a_2 \cdots a_n)\mu^{-1} = (\mu(a_1)\ \mu(a_2) \cdots \mu(a_n))} \quad (*)$$

RHS: $\mu(a_i) \mapsto \mu(a_{i+1})$

LHS: $\mu(a_i) \overset{\mu^{-1}}{\longmapsto} a_i \overset{\sigma}{\longmapsto} a_{i+1} \overset{\mu}{\longmapsto} \mu(a_{i+1})$

Thus have expression above

Now write $\sigma = \sigma_1 \sigma_2 \cdots \sigma_\ell$ a product of disjoint cycles

$$\tau = \mu \sigma \mu^{-1} = \mu \sigma_1 \mu^{-1} \cdot \mu \sigma_2 \mu^{-1} \cdots \mu \sigma_\ell \mu^{-1}$$

By $(*)$ $\mu \sigma_i \mu^{-1}$ is a cycle of same length as σ_i

$\Longrightarrow \mu, \tau$ have same cycle structure

$(\Longleftarrow)$: Suppose σ, τ have same cycle structure.

$$n_1 + \cdots + n_k$$

$$\begin{array}{l} \sigma = (a_{11} \cdots a_{1n_1}) \cdots (a_{k1} \cdots a_{kn_k}) \\ \quad \mu \downarrow \\ \tau = (b_{11}, \cdots, b_{1n_1}) \cdots (b_{k1}, \cdots, b_{kn_k}) \end{array}$$

Then μ is a bijection $\in S_n$ with

$$\begin{tikzcd} a_{ij} \arrow[r, "\sigma"] \arrow[d, "\mu"'] & a_{ij+1} \arrow[d, "\mu"] \\ b_{ij} \arrow[r, "\tau"] & b_{i,j+1} \end{tikzcd} \quad \Longrightarrow \tau = \mu \sigma \mu^{-1}$$

Example: conjugacy in S_n

$n=5$

Cycle structure	e.g
$1+1+1+1+1$	1_{S_n}
$2+1+1+1$	$(1\,2)$
$2+2+1$	$(1\,2)(3\,4)$
$3+1+1$	$(1\,2\,3)$
$3+2$	$(1\,2\,3)(4\,5)$
$4+1$	$(1\,2\,3\,4)$
5	$(1\,2\,3\,4\,5)$

Every $\sigma \in S_n$ is conjugate to one of these seven.

Example: how many elements of S_6 are conjugate to $(1\,2)(4\,5)$?

Answer: τ is conjugate to $\sigma = (1\,2)(4\,5)$ exactly when $\tau = (a\,b)(c\,d)$ for $\{a,b,c,d\}$ distinct in $\{1,2,\dots,6\}$

Choose a,b,c,d in $\binom{6}{4}$ ways. Place them: $(-\,-)(-\,-)$

in fact $(a\,\underset{\uparrow}{-})(-\,-)$

b, c, d determine rest

$$\Longrightarrow 3\binom{6}{4} = 45$$

Counting conjugate elements

Question! How many elements of S_n are conjugate to some fixed $\sigma \in S_n$

Make S_n act on itself by conjugation; $S_n \circlearrowright S_n$ by

$$\mu * \sigma = \mu \sigma \mu^{-1}$$

Then orbits = conjugacy classes

stabilizers = centralizers

By orbit-stabilizer theorem

$$n! = |S_n| = \underbrace{|\sigma^{S_n}|}_{\text{conjugates of } \sigma} \; \underbrace{|C_{S_n}(\sigma)|}_{\text{all } \mu \text{ s.t } \mu\sigma\mu^{-1} = \sigma}$$

$$\Longrightarrow \# \text{ we want} = |\sigma^{S_n}| = \frac{n!}{|C_{S_n}(\sigma)|} \longleftarrow \text{ count this}$$

Write σ as a product of disjoint cycles s.t there are m_r cycles of length r

Then

$$\sigma = \cdots \underbrace{(a_{11} \cdots a_{1r}) \cdots (a_{m_r 1} \cdots a_{m_r r})}_{\text{The } r \text{ cycles}} \cdots \quad (*)$$

and

$$\mu\sigma\mu^{-1} = \cdots (\mu(a_{11}) \cdots \mu(a_{1r})) \cdots (\mu(a_{m_r 1}) \cdots \mu(a_{m_r r})) \cdots \quad (**)$$

We want to count the μ's s.t (**) = (*) i.e. $\mu \sigma \mu^{-1} = \sigma$

Need $(\mu(a_{11}) \cdots \mu(a_{1r}))$ to be one of the (**).

There are m_r choices for which one. Similarly $(\mu(a_{21}) \cdots \mu(a_{2r}))$ has $m_r - 1$ choices for matching up, ...

$$\Longrightarrow m_r! \text{ ways the } (**) \text{ can be matched with } (*)$$

Suppose $(\mu(a_{11}) \cdots \mu(a_{1r}))$ is matched with $(a_{i1} \cdots a_{ir})$, then either

$$\mu(a_{11}) = a_{i1} \text{ or } \mu(a_{11}) = a_{i2} \cdots\cdots \mu(a_{11}) = a_{ir}$$

i.e. r possibilities for $\mu(a_{11})$

As soon as this choice is made, the possibilities for the remaining $\mu(a_{ij})$ are completely determined.

This is the case for each r-cycle

$$(\mu(a_{i1}) \cdots \mu(a_{ir}))$$

of $\mu \sigma \mu^{-1}$ giving $m_r! r^{m_r}$ ways of the r-cycles of $\mu \sigma \mu^{-1}$ can equal the r-cycles of σ.

Conclusion: there are $m_r! r^{m_r}$ ways the r-cycles in (**) are equal to the r cycles in (*)

Let r vary to give

$$\prod_{r \geq 1} m_r! r^{m_r} \quad \mu\text{'s s.t } \mu \sigma \mu^{-1} = \sigma$$

$$\Longrightarrow \boxed{\#\text{ of conjugates of } \sigma = \frac{n!}{\prod_{r \geq 1} m_r! r^{m_r}}}$$

Note: If $m_r = 0$ then

$$m_r! r^{m_r} = 0! r^0 = 1$$

Example: $\sigma = (1\,2)(4\,5) \in S_6$

$$\Longrightarrow m_1 = 2, \quad m_2 = 2$$

$$\#\text{ conjugates of } \sigma = \frac{6!}{m_1! 1^{m_1} \times m_2! 2^{m_2}}$$

$$= \frac{6!}{2!\, 2!\, 2^2} = 45$$

6. Counting-Conjugacy

Recall if $G \curvearrowright X$, then by Burnside theorem

$$\#\text{orbits} = \frac{1}{|G|}\sum_{g\in G} |Fix(g)| \qquad \text{——— } (*)$$

Suppose now that $x \in X$ with $x \in Fix(g)$ so

$$g * x = gx = x$$

Consider

$$(hgh^{-1})(hx) = hg(x) = hx$$

i.e. $x \in Fix(g) \Rightarrow hx \in Fix(hgh^{-1})$

Conversely if $y \in Fix(hgh^{-1})$, i.e.

$$hgh^{-1}(y) = y \Rightarrow gh^{-1}(y) = h^{-1}y$$

i.e. $y \in Fix(hgh^{-1}) \Rightarrow h^{-1}(y) \in Fix(g)$

This gives

$$Fix(g) \underset{y \mapsto h^{-1}y}{\overset{x \mapsto hx}{\rightleftarrows}} Fix(hgh^{-1})$$

maps which are mutual inverses $\Rightarrow$ bijections

i.e. $\quad |Fix(g)| = |Fix(hgh^{-1})|$

Thus conjugate elements contribute the same summand to $(*)$

Thus

$$\boxed{\#\text{orbits} = \frac{1}{|G|}\sum_{\text{conjugacy classes}} |g^G|\,|Fix(g)|} \qquad \text{Polya Enumeration} \quad (**)$$

conjugacy class of g

Remark: $G = S_5$

$|G| = 5! = 120$ but G has only 7 conjugacy classes corresponding to the permutations of 5.

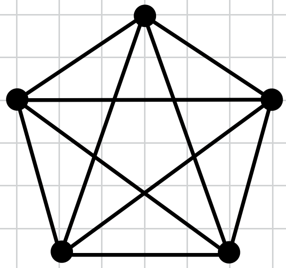
$(1+1+1+1+1,\ 2+1+1+1,\ \cdots)$

$\Rightarrow$ $(*)$ has 120 terms, $(**)$ has 7

Extended Example

A graph is a set of nodes/vertices connected by edges.

Convention: We won't allow multiple edges between vertices or loops

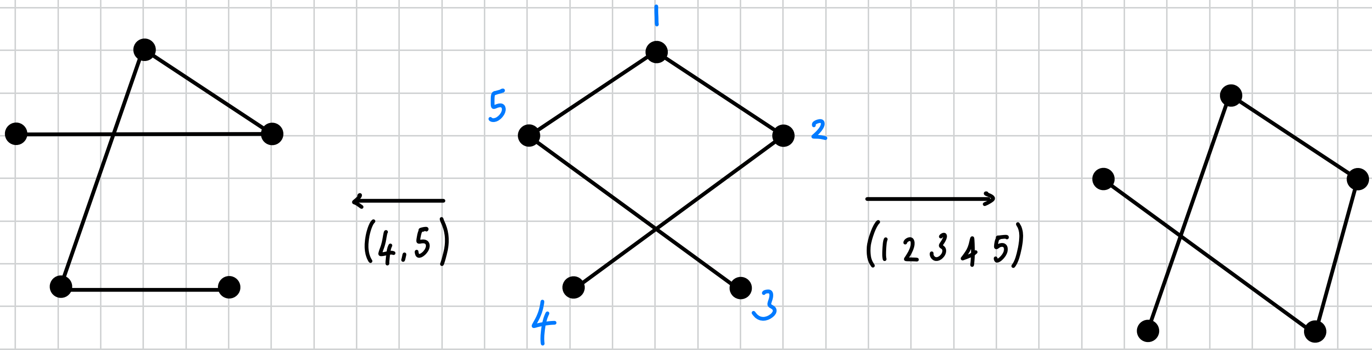


graph Γ

2 graphs Γ_1 and Γ_2 are isomorphic if $\exists$ a bijection f from vertices of Γ_1 to Γ_2 s.t

u and v are joined by an edge in Γ_1 $\iff$ $f(u)$ and $f(v)$ are joined by an edge in Γ_2

Example:



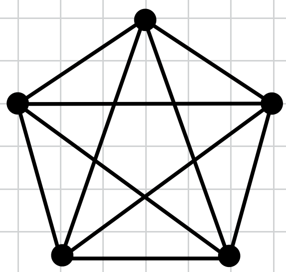
isomorphic to each other

Question: how many non-isomorphic graphs are there with 5 vertices

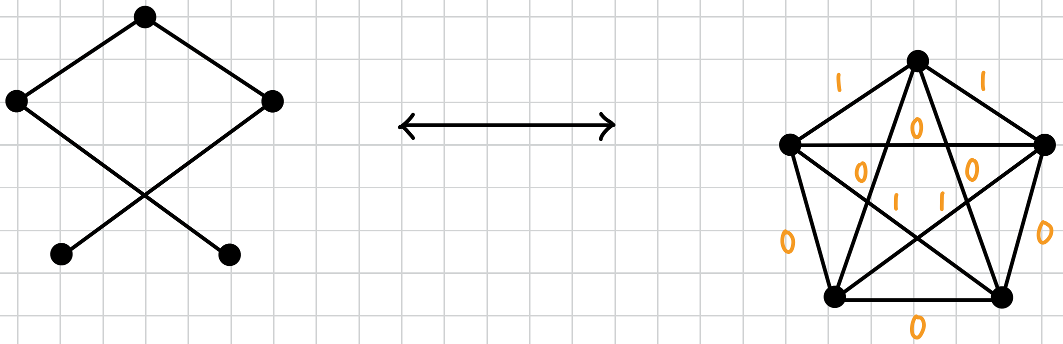
Alternate view:

Consider

Complete graph K_5



graphs on 5-vertices $\xleftrightarrow{1-1}$ colourings of edges of K_5 with 0, 1



Then Γ_1 isomorphic to Γ_2 $\Longleftrightarrow$ corresponding colorings of K_5 are isomorphic

Now let $S_5 \curvearrowright X$

$$X = \{\text{all possible edge colorings of } K_5\}$$

Then # non-isomorphic graphs = # orbits

Using Polya enumeration, list conjugacy classes in S_5

Table #1 (conjugacy in S_5)

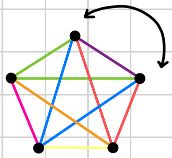
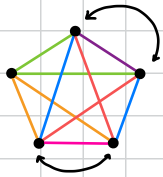
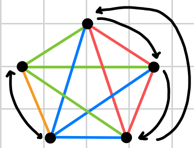
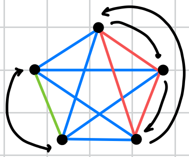
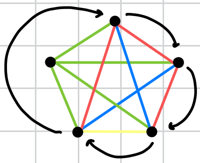
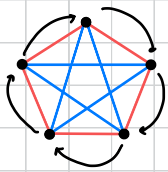
Partition of 5	example σ	$\lvert g^G \rvert = \frac{n!}{\prod_r m_r! \, r^{m_r}}$
1+1+1+1+1	1_{S_n}	1
2+1+1+1	(1 2)	10
2+2+1	(1 2)(3 4)	15
3+1+1	(1 2 3)	20
3+2	(1 2 3)(4 5)	20
4+1	(1 2 3 4)	30
5	(1 2 3 4 5)	24

<u>Reality check</u>: $G \curvearrowright G$ by conjugation

$$h * g = hgh^{-1}$$

Orbit of $g = \{h * g = hgh^{-1} : h \in G\}$

$\Longrightarrow$ $G =$ disjoint union of orbits/conjugacy classes

Example σ		$\lvert Fix(\sigma)\rvert$
1_G		$\lvert X\rvert = 2^{10}$
$(1\ 2)$	 edges the same color must have same 0,1-label	2^7 $\left(= 2^{\#\text{colors}}\right)$
$(1\ 2)(3\ 4)$		2^6
$(1\ 2\ 3)$		2^4
$(1\ 2\ 3)(4\ 5)$		2^3
$(1\ 2\ 3\ 4)$		
$(1\ 2\ 3\ 4\ 5)$		

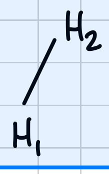
7. Subgroup Lattice

Definition. Subgroup Lattice

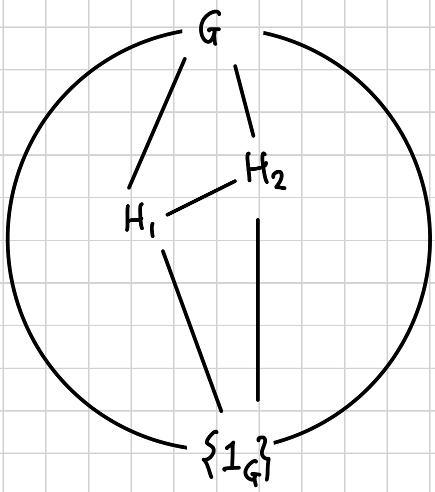
Let G be any group.

Then the subgroup lattice of G written $\mathcal{L}(G)$ is the set of all subgroups of G s.t

H_1 and $H_2 \leq G$ with $H_1 \subseteq H_2$, then in $\mathcal{L}(G)$ write:



Schematic



Example: $G = \mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$ with $+$ mod n

Then $H = \{1_G\} = \{0\}$ a subgroup

If $H \neq \{0\}$ then let $0 \neq k \in H$ be smallest

$$\Rightarrow k, k+k, k+k+k, \ldots \in H.$$

$$\Rightarrow k, 2k, 3k, \cdots \in H$$

$$\Rightarrow \{0, k, 2k, \ldots\} \subseteq H.$$

Now let $h \in H$ and divide with remainder

$$h = mk + r \qquad 0 \leq r < k$$

$\Rightarrow r = h - mk \in H$ by closure since $h \in H$, $mk \in H$

$\Rightarrow r \in H$

Since k smallest and $0 \leq r < k \Rightarrow r = 0 \Rightarrow h = mk$

Thus $H=\{0, k, 2k, \dots (s-1)k\}$ —— $(*)$

with $sk=n$.

<u>Conclusion</u>: If $H \leq \mathbb{Z}_n$, then H looks like $(*)$ with k dividing n, i.e. $k \mid n$

<u>$n=12$</u>

$\{0\}$

$\{0,6\} \cong \mathbb{Z}_2$

$\{0,4,8\} \cong \mathbb{Z}_3$

$\{0,3,6,9\} \cong \mathbb{Z}_4$

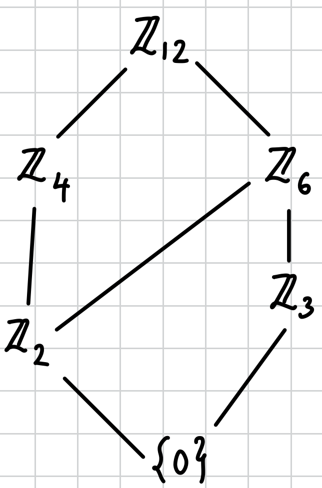
$\{0,2,4,6,8,10\} \cong \mathbb{Z}_6$

$\mathbb{Z}_{12}$

$$\begin{array}{c|cc} 0 & 0 & 6 \\ \hline 0 & 0 & 6 \\ 6 & 6 & 0 \end{array} \equiv \begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

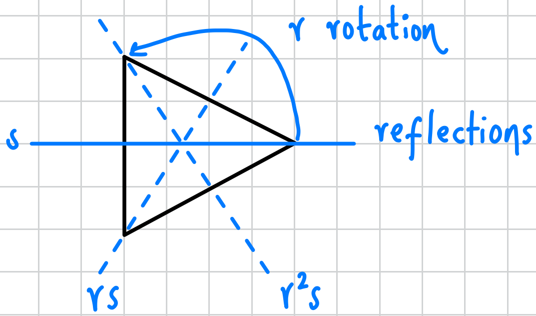
Note $\mathbb{Z}_3 \leq \mathbb{Z}_6$, $\mathbb{Z}_2 \leq \mathbb{Z}_4$.

$\mathcal{L}(\mathbb{Z}_{12})$



Example: Symmetries of equilateral triangle

$G=\{1_G, r, r^2, s, rs, r^2s\}$



Then $\{1_G\}$, $\{1_G, r, r^2\}$, $\{1_G, s\}$, $\{1_G, rs\}$, $\{1_G, r^2s\}$ and G subgroups

$\cong \mathbb{Z}_3$

Now let H be an arbitrary subgroup.

(1) Suppose $r \in H$ so that $\{1_G, r, r^2\} \subseteq H$

$$\Rightarrow 3 \leq |H| \leq 6$$

By Lagrange, $|H|$ divides $6 \Rightarrow |H| = 3$ or 6

$$\Rightarrow H = \{1_G, r, r^2\} \text{ or } G$$

(2) Suppose $s \in H$ and $r \notin H$. Then

$$\{1_G, s\} \subseteq H \Rightarrow |H| = 2, 3, 6$$

If $|H| = 2$, then $H = \{1_G, s\}$ and $|H| = 6$, then $H = G$

If $|H| = 3$, then the element of H that isn't 1_G or s cannot be r (hence r^2)

i.e. $H = \{1_G, s, rs\}$ or $H = \{1_G, s, r^2 s\}$.

If first, then $rs.s \in H \Rightarrow rs^2 = r \in H$

Similarly not second