Polyhedral Description Conversion upto symmetries

Jayant Apte
ASPITRG

Outline:Part-I

- Basic Terminology
  - Symmetry and Rigid Motions
  - Groups
  - Properties of Groups
  - Cyclic Groups
  - Permutations/Symmetry Group
  - Dihedral Group
  - Cosets and Lagrange's Theorem
  - Isomorphisms and Caylay's Theorem
  - Group Actions and Orbits
  - Fixed point sets and stabilizers

Outline:Part-II

- ?

A simple example

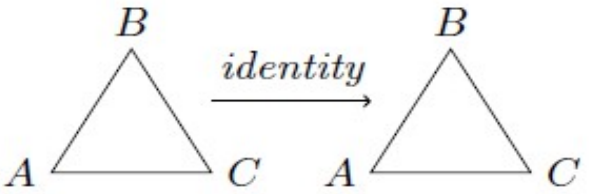
- Let $S = \{1, 2, 3\}$
- $\pi : S \to S$ given as: $\pi(1) = 2, \pi(2) = 1, \pi(3) = 3.$
- This is a bijective map.
- For any set S bijective map like $\pi : S \to S$ is called **permutation** of S.

Rigid Motions and Symmetry

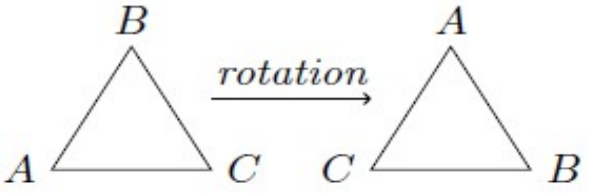
- A **rigid motion** of that 2-D geometric figure
  is a map from the plane to itself preserving the arrangement
  of sides and vertices as well as its distances and angles

- Rigid motions of a 2-D geometric figure is a way
  of characterizing its symmetries

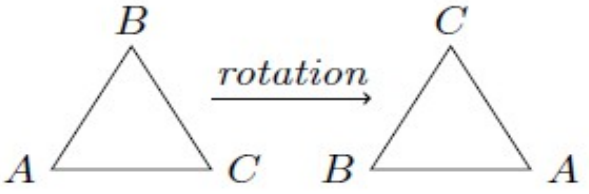
Rigid Motions of an equilateral triangle



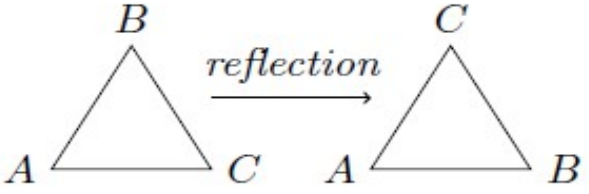
$$id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$



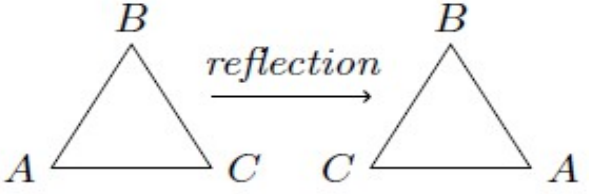
$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$



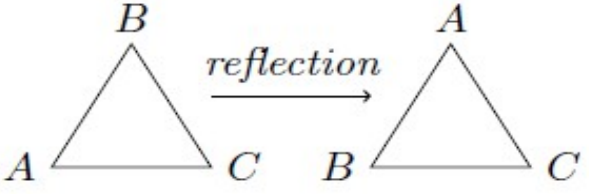
$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$



$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$



$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$



$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Figure Credits: Judson, Thomas W. Abstract Algebra: Theory and Applications. Boston, MA: PWS Pub., 1994. Print.

The Caylay Table for symmetries of equilateral triangle

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Figure Credits: Judson, Thomas W. Abstract Algebra: Theory and Applications. Boston, MA: PWS Pub., 1994. Print.

Group

- A **binary operation** or **law of composition** on set G is a function $G \times G \to G$ that assigns every pair $(a, b) \in G$ a unique element $a \circ b$, or ab in G is called composition of a and b.

- A **group** $(G, \circ)$ is a set G together with a law of composition $(a, b) \mapsto a \circ b$ satisfying axioms:
  1. operation is **associative**
  2. $\exists$ **identity element**
  3. $\exists$ **inverse element**

Group

- **Order** of group G is $|G|$. Group is **finite** if its order is finite, else it is **infinite**
- If the composition operation is **commutative** then the group is **abelian**.

Examples of groups

- Set of integers under addition as operation is called $\mathbb{Z}$, set of integers *modulo* n is called $\mathbb{Z}_n$ and is also a group under *modulo* n addition
- Denote $\mathbb{M}_2$ to be set of all 2×2 matrices under matrix multiplication
- **General linear group:** $GL_2(\mathbb{R}) \subset \mathbb{M}_2$ and has all invertible 2×2 matrices under matrix multiplication.

Properties of Groups

- Unique identity element
- Unique inverse for every element
- $\forall a \in G, (a^{-1})^{-1} = a$
- $(ab)^{-1} = b^{-1}a^{-1} \quad \forall a, b \in G$
- $\forall a, b \in G \; ax = b$ and $xa = b$ have unique solution $x \in G$

Properties of Groups

- **Left and right cancellation laws:** $ba = ca \Rightarrow b = c$ and $ab = ac \Rightarrow b = c$
- Exponent notation(esp. for multiplication operator) for repetitive operations, inverse operation etc.
    1. $g^m g^n = g^{m+n}$
    2. $(g^m)^n = g^{mn}$
    3. $(gh)^n = (h^{-1}g^{-1})^{-n} \forall n \in \mathbb{Z}$
- For abelian G, $(gh)^n = g^n h^n$

Subgroups

- A **subgroup** H of G is is a subset closed under operation of group G
- **Trivial** if $H = \{e\}$
- **Proper** if $H \subsetneq G$
- Denoted as $H \leq G$ (general) and $H < G$(proper)

Cyclic Subgroups and Cyclic Groups

- One element of group determines entire subset of group/subgroup then that subgroup is called cyclic subgroup.
- The subgroup generated by $a \in G$ is denoted by $< a >$
- Elements in this subgroup are $a \circ a, a \circ a \circ a, ...$
- For any $a \in G$, $< a >$ is called **cyclic subgroup** of G.
- If $\exists a \in G : G =< a >$ we call G a **cyclic group** with generator a

Examples

- Set of integer powers of 2 is a cyclic subgroup of group of positive rationals $\mathbb{Q}^+$ under ordinary multiplication
- $3\mathbb{Z}$ is cyclic subgroup of $\mathbb{Z}$, $3\mathbb{Z} =< 3 >$

Properties of Cyclic Groups

- cyclic $\Rightarrow$ *abelian*
- Let $G =< a >$ and G has order n. then $a^k = e$ iff $k \bmod n = 0$
- Every subgroup of cyclic group is cyclic
- If $b \in G, b = a^k$ where $G =< a >$ is cyclic of order n, then b is generator of a cyclic subgroup of G of order $\frac{n}{gcd(k,n)}$
- Hence if a to be generator of cyclic group G of n elements then $a = b^k$ for some other gererator b of G for k that is relatively prime to n

Permutation Group/Symmetry Group

- Group of permutations of elements of set X is called S_X
- When $X = \{1, 2, 3..., n\}$ it is denoted by S_n: **permutation group on n letters**
- The underlying set for S_n is the **set of ways of permuting** $\{1, 2, 3, ..., n\}$

Disjoint Cycle Notation

- We can refer to a permutation σ as
  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$
- Or we can use the **disjoint cycle notation** as$(\ 4321)$
- (4321) $4 \mapsto 3, 3 \mapsto 2, 2 \mapsto 1, 1 \mapsto 4$
- σ above is described with with just one cycle.
- As a minimal representation, we need cycles to be disjoint
- $\therefore$ (4321) is trivially valid
- Some permutations may consist of more than one cycle

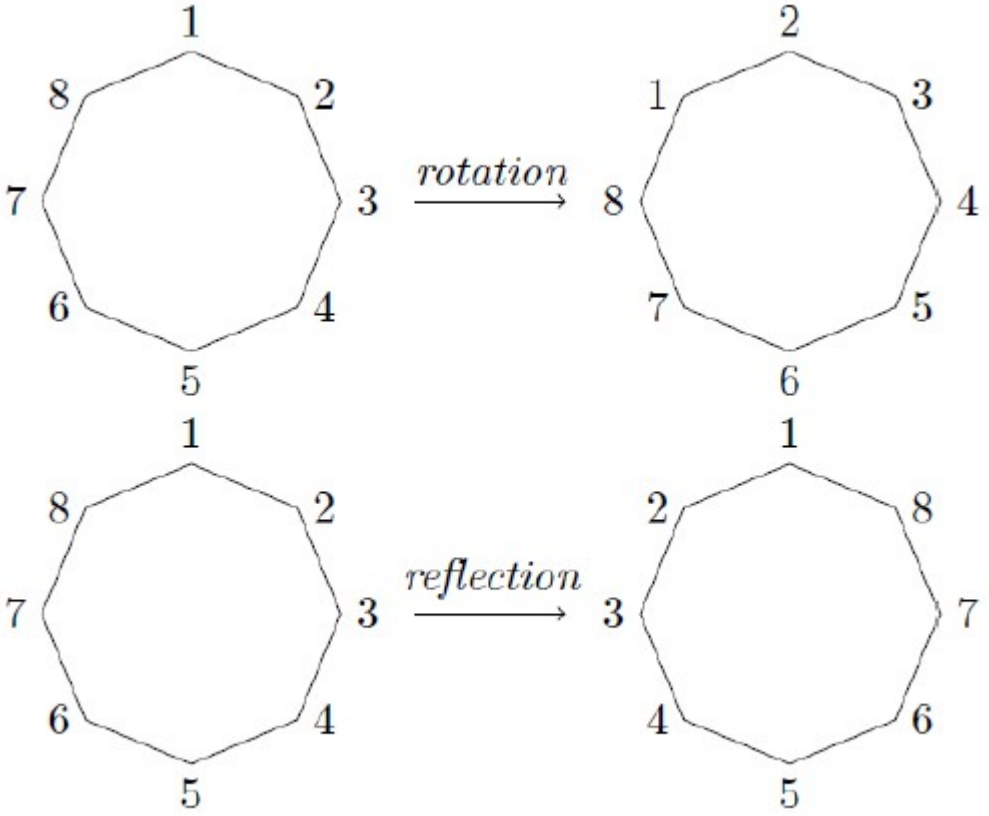
Transposition

- Example: (135)(27) is minimal because cycles are disjoint but (135)(347) reduces to (13475)
- **Transposition** is disjoint cycle representation with each cycle having only 2 elements
- number of cycles in transposition representation of id is even(intuitive)
- a permutation is **even** if it can be represented as even number of transpositions otherwise it is **odd**
- Set of all even permuatations A_n is a subgroup of S_n and its order is $n!/2$ = number of odd permutations

Dihedral Groups

- The dihedral group denoted by D_n is a group associated with a regular n-gon.
- **Rotations** We denote $\frac{360^\circ}{n}$ rotation of an n-gon by r, $2 \times \frac{360^\circ}{n}$ rotation by r^2 and so on. Hence rotation r generates all other rotations
- **Reflections** We define a reflection of n-gon by the vertex it leaves fixed: odd number of vertices:
- $r^n = id, s^2 = id, srs = r^{-1}$
- The group of rigid motions of a cube is S_4

Example: D_8


1
2
3
4
5
6
7
8
rotation
2
3
4
5
6
7
8
1
1
2
3
4
5
6
7
8
reflection
1
8
7
6
5
4
3
2

Cosets

- For any $g \in G$ and H $\leq G$ the set $gH = \{gh : h \in H\}$ is called **left coset** of H with **representative** g
- Similarly, $Hg = \{hg : h\}$ is the right coset
- **Example:** Let $H \leq \mathbb{Z}_6$ and $H = \{0, 3\}$ then 6 elements of G give following 6 cosets:

1. $0 + H = \{0, 3\}$
2. $1 + H = \{1, 4\}$
3. $2 + H = \{2, 5\}$
4. $3 + H = \{0, 3\}$
5. $4 + H = \{1, 4\}$
6. $5 + H = \{2, 5\}$

Cosets

- Only 3 of these cosets are unique. They are:
  $\{0,3\}, \{1,4\}, \{2,5\}$
- Further,$\{0,3\} \cup \{1,4\} \cup \{2,5\} = \mathbb{Z}_6$
- This leads to following theorem:
  For any $H \leq G$, left cosets of H in G partition G
  OR
  The group G is disjoint union of left cosets of H in G
- Number of left cosets=number of right cosets

Cosets

- For $H \leq G$ ***Index*** of H in G is number of left(right) cosets of H in G denoted by $[G : H]$
- ***Theorem(Lagrange):*** Let G be a finite group and let $H \leq G$. Then $|G|/|H| = [G : H]$ is the number of distinct cosets of H in G. Hence, if H is a subgroup of G then, number of elements in H must divide number of elements in G.
- **Converse is not true**

Double Cosets

- Generalize the notion of cosets
- Let H and K be subgroups of group G.
- An (H, K)-***double coset*** is a set of the form HxK for some $x \in G$. Here HxK is defied as:

  $HxK = \{hxk | h \in H and k \in K\}$

- $(H, \{id\})$-double cosets are the right cosets of H and $\{id\}, H$-double cosets are the left cosets of H
- Set of all (H, K)-double cosets is denoted as $H \backslash G / K$

Double Cosets

- $H\backslash G/K$ partitions G
- (H, K)-double cosets for given H, K need not be of same cardinality
- **Example:** If G is S_3, $H =< (1,2) >$ and $K =< (1,3) >$, then the two resulting (H, K)-double cosets are $\{e, (1,2), (1,3), (1,3,2)\}$ and {(2,3),(1,2,3)}

Isomorphisms

- Two groups $(G, \circ)$ and $(H, \cdot)$ are ***isomorphic*** $(G \cong H)$ if $\exists$ bijective map $\phi : G \to H$ preserving group operation. ϕ is then called an ***isomorphism***.
- **Example:** $\mathbb{Z}_4 \cong \langle i \rangle$
- ***Theorem(Caylay):*** Every group is isomorphic to a group of permutations(err, but we don't know the isomorphism ϕ)
- Calay's theorems it important to find an isomorphism of the group G that we want to study to a group that we know a lot about(S_n or matrix groups)
- **Example:** $\mathbb{Z}_3$ is isomorphic with $G = \{(0), (012), (021)\}$

Automorphisms

- If instead ϕ is $\phi : G \to G$ and its bijective, we call it ***automorphism***
- **Example:** $\phi : \mathbb{R} \to \mathbb{R}$ s.t. $\phi(x) = e^x$ is an automorphism between $(R, +)$ and itself

Group Actions

- **A left action** of G on X is a map $G \times X \mapsto X$ given by $(g, x) \mapsto gx$ where,

  1. $ex = x \ \ \forall x \in X$
  2. $(g_1 g_2)x = g_1(g_2 x), \forall x \in X$ and $\forall g_1, g_2 \in G$

- If conditions 1 and 2 are satisfied we call X as the ***G-set*** (That is same as saying G 'can act' on X)

- Every group trivially acts on every set through the map $(g, x) \mapsto x$

- **Example:** $GL_2(\mathbb{R})$ acting on $X = \mathbb{R}^2$ via matrix-vector multiplication. We can verify that condition 1 is satisfied with $e = I_2$ and condition 2 is satisfied because matrix multiplication is associative.

G-equivalence

- **G-equivalence:** If G acts on a set X and $x, y \in X$, then x is said to be G-***equivalent*** to y if $\exists g \in G$ s.t. $gx = y$. We denote G-***equivalence*** of x and y as $x \sim_G y$
- One can check that G-***equivalence*** is an equivalence relation by verifying its reflexive, symmetry and transitive properties

Orbits

- Each G-equivalent partition of X so formed is called ***orbit*** of X under G.
- We denote each orbit by a representative. e.g. orbit containing X is called $\mathcal{O}_x$
- **Example:** $G = \{(1), (123), (45), (123)(45), (132)(45)\}$ and $X = \{1, 2, 3, 4, 5\}$
- X is a G-set
- The orbits are:

  1. $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}_3 = \{1, 2, 3\}$ and
  2. $\mathcal{O}_4 = \mathcal{O}_5 = \{4, 5\}$

Fixed point sets

- ***Fixed point set*** X_g of $g \in G$ is the set $\{x | x \in X_g$ if $x \in X$ and $gx = x\}$
- **Example:** $X = \{1, 2, 3, 4, 5, 6\}$ and suppose G is permutation group given by permutations $\{(1), (12)(3456), (35)(46), (12)(3654)\}$
- Fixed point sets in X are:

  1. $X_{(1)} = X$
  2. $X_{(35)(46)} = \{1, 2\}$
  3. $X_{(12)(3456)} = X_{(12)(3654)} = \phi$

Stabilizer Subgroup

- Subgroup of G, denoted as G_x that fixes given x called ***stabilizer subgroup***
- **Example:** $X = \{1, 2, 3, 4, 5, 6\}$ and suppose G is permutation group given by permutations $\{(1), (12)(3456), (35)(46), (12)(3654)\}$
- The stabilizer subgroups are:

  1. $G_1 = G_2 = \{(1), (35)(46)\}$
  2. $G_3 = G_4 = G_5 = G_6 = \{(1)\}$