4. Groups and Symmetries

4.1 Cycles in Symmetric Groups

Symmetric groups (permutation groups) S_n consists of all bijections.

One way to express an element $\sigma \in S_n$ is to list the image of each number $1, 2, ..., n$ via σ as follows: $\sigma(1), ..., \sigma(n)$

$(a_1, ..., a_k)$ and $(b_1, ..., b_k)$ are disjoint if $a_1, ..., a_k, b_1, ..., b_k$ are all distinct.

Prop. Disjoint cycles commute.

Prop. Every $\sigma \in S_n$ can be written as a product of disjoint cycles in a unique way, up to reordering the cycles.

Pf. define an equivalence relation on $\{1, ..., n\}$ by $i \sim j$ if $\exists m \in \mathbb{Z}, j = \sigma^m(i)$.

$\sigma = ((a_1, \sigma(a_1), ..., \sigma^{m_1 - 1}(a_1)), \ldots, (a_k, \sigma(a_k), ..., \sigma^{m_k - 1}(a_k)))$

Write $\sigma \in S_n$ as a product of disjoint cycles, and we list the lengths of the cycles in an increasing order: $1 \leq n_1 \leq \ldots \leq n_r$ so that $n_1 + \ldots + n_r = n$. We define the cycle type of σ to be $(n_1, \ldots, n_r)$, or $n_1 + \ldots + n_r$.

Example: $\sigma = (123)(45) \in S_7$, cycle type is $(1, 1, 2, 3)$.

Lemma. $\sigma \in S_n$. $\sigma(a_1, ..., a_k)\sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))$.

Prop. Two elements in S_n are conjugate to each other $\iff$ they have the same cycle type.

Example: $\sigma = (12)(345) \in S_7$, $\sigma' = (34)(167) \in S_7$

Let $\tau(1) = 3, \tau(2) = 4, \tau(3) = 1, \tau(4) = 6, \tau(5) = 7, \tau(6) = 2, \tau(7) = 5$,

so $\tau = (13)(246)(57)$.

4.2 Signature Functions and Alternating Groups

Every $\sigma \in S_n$ can be written as a product of 2-cycles:

$(a_1, ..., a_k) = (a_1 a_k)(a_1 a_{k-1}) \ldots (a_1 a_2)$.

Now define a homomorphism $T : S_n \to GL_n(\mathbb{R})$ by sending the permutation $\sigma \in S_n$ to the $n \times n$ matrix whose j-th column is the unit vector $e_{\sigma(j)}$.

Example: $\sigma = (123)$. $T(\sigma) = [e_{\sigma(1)} e_{\sigma(2)} e_{\sigma(3)}] = [e_2 e_3 e_1] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

The signature function of S_n is defined to be

$sgn : S_n \xrightarrow{T} GL_n(\mathbb{R}) \xrightarrow{\det} \{\pm 1\}$

It is a surjective homomorphism.

If $sgn(\sigma) = +1$, we call it an even permutation.

If $sgn(\sigma) = -1$, we call it an odd permutation.

Prop. If $\sigma = (a_i a_j)$ is a 2-cycle, then $sgn(\sigma) = -1$.

If $\sigma = (a_1 ... a_k)$ is a k-cycle, then $sgn(\sigma) = (-1)^{k-1}$.

Example: $\sigma = (135)(24)(789) \in S_{10}$, $sgn(\sigma) = (-1)^{3-1}(-1)^{2-1}(-1)^{3-1} = -1$.

The normal subgroup of S_n defined by $A_n = \ker(sgn) = \{\sigma \in S_n | sgn(\sigma) = +1\}$ is called the alternating subgroup of n elements. It consists of all the even permutations in S_n.

By the First Isomorphism Theorem, $S_n/A_n \cong \{\pm 1\}$. In particular, $\frac{|S_n|}{|A_n|} = 2$, $|A_n| = \frac{S_n}{2} = \frac{n!}{2}$

- $A_1 = S_1 = \{id\}$
- When $n \geq 2$, $|A_n| = \frac{S_n}{2} = \frac{n!}{2}$.

  $A_2 = \{id\}$
- $A_3 = \{id, (123), (132)\}$
- $A_4 = \{id, (12)(34), (13)(24), (14)(23), (123), (132)\}$

  A normal group of A_4: $\{id, (12)(34), (13)(24), (14)(23)\} \cong K_4$

A group G is simple if it has no proper normal subgroups, i,e., its only normal subgroups are $\{1\}$ and G.

- A_n is simple for $n \geq 5$

4.3 Isometry on Euclidean Spaces

The dot product of two vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$ is $<\vec{u}, \vec{v}> = \vec{u}^T\vec{v}$.

The length of $\vec{v} \in \mathbb{R}^n$ is $|\vec{v}| =< \vec{v}, \vec{v} >$.

The distance of two vectors $\vec{u}, \vec{v} \in \mathbb{R}^n$ is the length $|\vec{u} - \vec{v}|$.

An isometry of $\mathbb{R}^n$ is a distance preserving map $f : \mathbb{R}^n \to \mathbb{R}^n$, i.e., for any $\vec{u}, \vec{v} \in \mathbb{R}^n$, $|f(\vec{u}) - f(\vec{v})| = |\vec{u} - \vec{v}|$.

Lemma. If f, g are isometries on $\mathbb{R}^n$, then $f \circ g$ is also an isometry on $\mathbb{R}^n$.

Each $\vec{a} \in \mathbb{R}^n$ induces a translation map: $t_{\vec{a}} : \mathbb{R}^n \to \mathbb{R}^n$, $\vec{u} \mapsto \vec{u} + \vec{a}$.

This is an isometry since $\vec{u}, \vec{v} \in \mathbb{R}^n$: $|t_{\vec{a}}(\vec{u}) - t_{\vec{a}}(\vec{v})| = |(\vec{u} + \vec{a}) - (\vec{v} + \vec{a})| = |\vec{u} - \vec{v}|$.

$T : \mathbb{R}^n \to \mathbb{R}^n$ is a linear operator if:

1. $\forall \vec{u}, \vec{v} \in \mathbb{R}^n, T(\vec{u} + \vec{v}) = T(\vec{u}) + T(\vec{v})$
2. $\forall c \in \mathbb{R}, \vec{u} \in \mathbb{R}^n, T(c\vec{u}) = cT(\vec{u})$

$T : \mathbb{R}^n \to \mathbb{R}^n$ is an orthogonal linear operator if it is a linear operator s.t. $\forall \vec{u}, \vec{v} \in \mathbb{R}^n$, $< T(\vec{u}), T(\vec{v}) >=< \vec{u}, \vec{v} >$.

A $n \times n$ invertible matrix A is orthogonal if $A^{-1} = A^T$. The set of all $n \times n$ orthogonal matrices forms a subgroup of $GL_n(\mathbb{R})$, called the orthogonal linear group $O_n(\mathbb{R})$.

Thm. $T : \mathbb{R}^n \to \mathbb{R}^n$ is a linear operator, and $A \in O_n(\mathbb{R})$ is its matirx. Then T is an orthogonal linear operator $\iff A$ is an orthogonal matrix.

Thm. The following conditions of a map $f : \mathbb{R}^n \to \mathbb{R}^n$ are equivalent:

1. f is an isometry that fixes $\vec{0}$.
2. f preserves the dot product.
3. f is an orthogonal linear operator.

4. Fix a standard basis $(e_1, ..., e_n)$ for $\mathbb{R}^n$, then $f(\vec{v}) = A\vec{v}$ for some $A \in O_n(\mathbb{R})$.

Cor. Every isometry $f : \mathbb{R}^n \to \mathbb{R}^n$ can be decomposed into $f = t_{\vec{a}} \cdot \phi$, where $t_{\vec{a}}$ is the translation along $\vec{a} = f(\vec{a})$, ϕ is an orthogonal linear operator.

Lemma. $\phi \cdot t_{\vec{a}} = t_{\phi(\vec{a})} \cdot \phi$

Cor. The set of all isometries on $\mathbb{R}^n$ with composition of functions form a group M_n, called the group of isometry on $\mathbb{R}^n$.

Cor. Let T_n be the set of translations on $\mathbb{R}^n$, O_n be the set of orthogonal linear operators on $\mathbb{R}^n$. Then O_n is a subgroup of M_n and T_n is a normal subgroup of M_n.

4.4 Isometry on the Plane

Lemma. The determinant of an orthogonal matrix is 1 or -1.

The kernel of $O_n(\mathbb{R})$: $SO_n(\mathbb{R}) = \{A \in O_n(\mathbb{R}) | \det(A) = 1\}$

When $n = 2$, by orthogonal $\to$ $a = d, b = -c$, by det=1 $\to$ $ad - bc = 1$ $\to$ $a^2 + c^2 = 1$

$SO_2(\mathbb{R}) = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$ for some $\theta \in \mathbb{R}$.

For any vector $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} R\cos(\alpha) \\ R\sin(\alpha) \end{bmatrix}$,

$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \begin{bmatrix} R\cos(\alpha) \\ R\sin(\alpha) \end{bmatrix} = \begin{bmatrix} R\cos(\alpha+\theta) \\ R\sin(\alpha+\theta) \end{bmatrix}$ — rotation of angle θ around origin

$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}$ — reflection with respect to x-axis

Thm. Let f be an isometry of the plane, then $f = t_{\vec{a}} \cdot \rho_\theta$ or $f = t_{\vec{a}} \cdot \rho_\theta \cdot r$,

where rotation $\rho_\theta = \begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix}$, reflection $r = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.

Thm. Every isometry of the plane has one of the following forms:

1. Translation along $\vec{a} \in \mathbb{R}^2$ — $t_{\vec{a}}$
2. Rotation through a nonzero angle about a point — $t_{\vec{a}}\rho_\theta$
3. Reflection along a line l — $t_{\vec{a}}\rho_\theta r$ with $\vec{a} \perp l$
4. Glide Reflection: reflection along a line l, followed by a translation along a nonzero vector parallel to l — $t_{\vec{a}}\rho_\theta r = t_{\vec{a}_1}(t_{\vec{a}_2}\rho_\theta r)$ with $\vec{a}_1 \parallel l$, $\vec{a}_2 \perp l$

The first two are orientation preserving and the last two are orientation reversing.

$t_{\vec{p}}\rho_\theta t_{-\vec{p}}$ is the rotation about $\vec{p}$ of angle θ.

$\rho_\theta r$ is the reflection along the line l through origin with angle $\frac{\theta}{2}$ to x-axis.

Lemma. The following identities hold:

- $t_{\vec{a}} + t_{\vec{b}} = t_{\vec{a}+\vec{b}}$
- $\rho_\alpha \cdot \rho_\beta = \rho_{\alpha+\beta}$, ${\rho_\theta}^{-1} = \rho_{-\theta}$
- $r^{-1} = r$ and $r^2 = id$
- $\rho_\theta t_{\vec{a}} = t_{\rho_\theta(\vec{a})} \rho_\theta$
- $r t_{\vec{a}} = t_{r(\vec{a})} r$
- $r \rho_\theta = \rho_{-\theta} r$ and $\rho_{-\theta} = r \rho_\theta r = r \rho_\theta r^{-1}$

4.5 Dihedral Groups

The dihedral group is the finite subgroup of O_2 defined by

$D_n = \{\rho_\theta^i r^j \in O_2 | 0 \leq i \leq n-1, 0 \leq j \leq 1\}$, where $\theta = \frac{2\pi}{n}$

Properties: $|D_n| = 2n$, $|\rho| = n$, $|r| = 2$

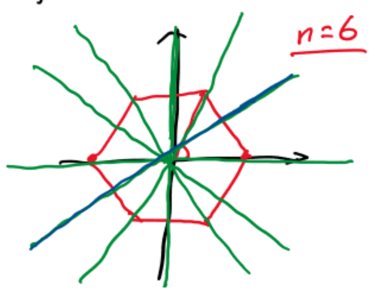
$<\rho>$ is a subgroup of index 2 in D_n, so it's a normal subgroup.

$\rho^i r = \rho_{i\theta} r$, it's the reflection along l, l passing through origin with angle $\frac{i\theta}{2}$

Geometrically, D_n is the group of symmetries for a regular n-gon.

ρ : rotation by $\theta = \frac{2\pi}{n}$

ρr : reflection along the blue line. with angle $\frac{\pi}{6}$.



We see each element of D_n permutes vertices of a polygon, and we can regard D_n as a subgroup of S_n in this sense.

In particular, when $n = 3$, $|D_3| = 2 \times 3 = 6$, $|S_3| = 6$, $D_3 \cong S_3$.

4.6 Group Actions

G is a group. X is a nonempty set. A group action of G on X is a function:

$G \times X \to X$

$(g, x) \mapsto g.x$

satisfying:

1. $1.x = x$ for any $x \in X$
2. $g_1.(g_2.x) = (g_1 g_2).x$ for any $g_1, g_2 \in G$, $x \in X$

Example: $G = S_n$ acts on $X = \{1, ..., n\}$ in a natural way: $\sigma \in S_n$ acts on $i \in X$ by $\sigma.i = \sigma(i)$

1. $id.i = id(i) = i$
2. $\sigma_1.(\sigma_2.i) = \sigma_1(\sigma_2(i)) = (\sigma_1 \cdot \sigma_2)(i) = (\sigma_1 \cdot \sigma_2).(i)$

Example: Any group G act on itself by left multiplication: $\forall g \in G, x \in G, g.x = gx$.

1. $1.x = x$
2. $g_1.(g_2.x) = g_1(g_2x) = (g_2g_2)x = (g_1g_2).x$

Prop. If G acts on X, then for any fixed $g \in G$

$\tau_g : X \to X$

$\tau_g(x) = g.x$

is a bijection.

Pf. To verify τ_g is bijective, we can verify $\tau_{g^{-1}} : X \to X$ is the inverse function of τ_g.

$\tau_g \cdot \tau_{g^{-1}}(x) = g.(g^{-1}.x) = (gg^{-1}).x = 1.x = x$

$\tau_{g^{-1}} \cdot \tau_g(x) = g^{-1}.(g.x) = (g^{-1}g).x = 1.x = x$

Example: If we want to define the action by right multiplication, we need $g.x = xg^{-1}$

- $1.x = x1 = x$
- $(g_1g_2).x = x(g_1g_2)^{-1} = (xg_2)^{-1}g_1^{-1} = g_1.(g_2.x)$

Example: G can act on itself by conjugation $g.x = gxg^{-1}$.

Example: The isometry group M_n acts on $\mathbb{R}_n$ by evaluation.

Example: $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication.

If G acts on X, and $x \in X$. The orbit of x is defined to be

$O(x) = \{y \in X | g.x = y \text{ for some } g \in G\}$

Lemma. The relation on X defined by $x \sim y$ if $y = g.x$ for some $g \in G$ is an equivalence relation, and each orbit is an equivalence class.

Pf. 1. $\forall x \in X, x \sim x$ since $1.x = x$

2. $x \sim y \to y = g.x \to g^{-1}.y = g^{-1}.(g.x) = (g^{-1}g).x = 1.x = x \to y \sim x$
3. $x \sim y, y \sim z \to y = g_1.x, z = g_2.y \to z = g_2.(g_1.x) = (g_1g_2).x \to x \sim z$

Cor. The orbits form a partition of X.

Example: G acts on itself. For any $x \in G$, $x = g.1$ for $g = x$, so $x \in O(1)$, so there's only one orbit.

Example: $GL_n(\mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication. There are two orbits: $\mathbb{R}^n \setminus \{0\}$ and $\{0\}$.

An action of G on X is transitive if there's only one orbit.

Prop. An action is transitive $\iff \forall x, y \in X, \exists g \in G, y = g.x$.

G acts on X. Define the stabilizer of $x \in X$ to be $G_x = \{g \in G : g.x = x\}$.

Prop. The stabilizer G_x is a subgroup of G.

Pf. 1. $\forall g_1, g_2 \in G_x$, $g_1.x = x$, $g_2.x = x$, $(g_1g_2).x = g_1.(g_2.x) = g_1.x = x \to g_1g_2 \in G_x$

2. $1.x = x \to 1 \in G_x$
3. $\forall g \in G$, $g.x = x$, $g^{-1}.x = g^{-1}.(g.x) = (gg^{-1}).x = 1.x = x \to g^{-1} \in G_x$

Example: G acts on itself by left multiplication, then for any $x \in G$, $G_x = \{g \in G, |g.x = x\} = \{g \in G|gx = x\} = \{1\}$

Example: G acts on itself by conjugation, then for any $x \in G$, $G_x = \{g \in G, |g.x = x\} = \{g \in G|gxg^{-1} = x\} = \{g \in G|gx = xg\} = N(G)$ — normalizer or centralizer of x

Prop. G acts on X, $g_1, g_2 \in G$, $x \in X$. Then $g_1.x = g_2.x \iff g_1 G_x = g_2 G_x$.

Pf. $g_1.x = g_2.x \iff g_2^{-1}.(g_1.x) = g_2^{-1}.(g_2.x) \iff (g_2^{-1}g_1).x = x \iff g_2^{-1}g_1 \in G_x \iff g_1 G_x = g_2 G_x$

4.7 Applications of Group Actions

Counting Formula, or Orbit-Stabilizer Theorem. G is a finite group acting on a set X. For each $x \in X$, let G_x be the stabilizer of x and $O(x)$ be the orbit of x. Then:

$|G| = |O(x)| \cdot |G_x|$

i.e. $|O(x)| = |G : G_x|$

Recall: $O(x) = \{y \in X|g.x = y \text{ for some } g \in G\}$, $G_x = \{g \in G : g.x = x\}$

Pf. Define $f : G/G_x \to O(x)$ by $f(gG_x) = g.x$.

By Prop, $f(g_1 G_x) = f(g_2 G_x) \iff g_1 G_x = g_2 G_x$, so f is well-defined and injective.

By definition of orbit, f is surjective.

So f is a bijection. By Lagrange Theorem, $\frac{|G|}{|G_x|} = |G/G_x| = |O(x)|$.

Example: D_n acts on V = the set of vertices of a regular n-gon. The action is transitive, since any v can be obtained from a fixed v_0 by a rotation ρ^k for some k. So for any $v \in V$, $O(v) = V$, $G_v = \frac{|D_n|}{|V|} = \frac{2n}{n} = 2$, and the two elements are identity and reflection along the line passing through v and the centre of the n-gon.

Prop. G is a finite group. H, K are subgroups of G. Then

$|HK| = \frac{|H| \times |K|}{|H \cap K|}$

Pf. $H \times K$ acts on G by $(h, k).g = hgk^{-1}$.

$O(1) = \{(h, k).1 \in G|(h, k) \in H \times K\} = \{hk^{-1} \in G|h \in H, k \in K\} = \{hk \in G|h \in H, k \in K\} = HK$.

$G_1 = \{(h, k) \in G \times K|(h, k).1 = hk^{-1} = 1\} = \{(h, k) \in H \times K|h = k\} = \{(g, g)|g \in H \cap K\}$, so $|G_1| = |H \cap K|$.

By Counting Formula, $|HK| = |O_1| = \frac{|H \times K|}{|G_1|} = \frac{|H| \times |K|}{|H \cap K|}$.

Thm. G is a group. X is a set. There's a one-to-one correspondence between G-actions on X and homomorphisms $G \to \mathrm{Per}(X)$, where $\mathrm{Per}(X)$ is the group of all bijections on X.

Pf. Given a group action of G on X, we have proved that for any $g \in G$, $\tau_g : X \to X$, $x \mapsto g.x$ is a bijection, so $\tau_g \in \mathrm{Per}(X)$. We define $F : G \to \mathrm{Per}(X)$, $g \mapsto \tau_g$. Since $F(g_1 g_2) = \tau_{g_1 g_2} = \tau_{g_1} \cdot \tau_{g_2} = F(g_1) \cdot F(g_2)$, F is a homomorphism.

Conversely, given a homomorphism $\phi : G \to \mathrm{Per}(X)$, we can define a G-action on X by $g.x = \phi(g)(x)$. It is a group action.

G can act on itself by conjugation: $g.x = gxg^{-1}$. $|O(x)| = 1 \iff x \in Z(G)$

Each orbit in this action is called a conjugacy class, denoted by C_x, so the above can be written as $C_x = \{x\} \iff x \in Z(G)$

$C_x = \{x\} \iff \forall g \in G, g.x = x \iff \forall g \in G, gxg^{-1} = x \iff \forall g \in G, gx = xg$

The stabilizer of x, denoted by $N(x)$, is called the normalizer or centralizer of x, $N(x) = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$.

Remark. More generally, for a subset S of a group G

Normalizer of S: $N(S) = \{g \in G | gSg^{-1} = S\}$

Centralizer of S: $N(x) = \{g \in G | \forall s \in S, gsg^{-1} = s\}$

By the counting formula, $|C_x| = \frac{|G|}{|N(x)|}$ if $|G| < \infty$. Also because the conjugacy classes form a partition of G, $|G|$ = sum of the cardinality of its conjugacy classes.

So we have:

Class Equation. G is a finite group, then

$|G| = |Z(G)| + \sum_{x \in S} |C_x| = |Z(G)| + \sum_{x \in S} \frac{|G|}{|N(x)|}$

where S is a set of representations of conjugacy classes (orbits) with at least two elements.

Cor. $1 \times 2 \times 3 = 1 + 2 + 3$.

Pf. Let $G = S_3$. Then $|S_3| = 1 \times 2 \times 3 = |Z(G)| + \sum_{x \in S} |C_x| = 1 + 2 + 3$ since $|C_{(123)}| = |\{(123), (132)\}| = 2$, $|C_{(12)}| = |\{(12), (13), (23)\}| = 3$.

Prop. If p is a prime number, then every group of order p^2 is abelian.

Cauchy's Theorem. If G is a finite group, and p is a prime number that divides $|G|$, then G has an element of order p.

Pf. Let $C_p =< a >$, the cyclic group of order G. C_p acts on

$Y = \{(g_1, ..., g_p) \in G \times ... \times G | g_1 ... g_p = 1\}$ by

$a.(g_1, ..., g_p) = (g_2, ..., g_p, g_1)$.

$|Y| = |G|^{p-1}$ since the last coordinate is determined by the first $n - 1$ coordinates.

$G_{(g_1, ..., g_p)} = G \iff g_1 = ... = g_p = g$ with $g^p = 1$.

Assume the only fixed point under this action is $(1, ..., 1)$, then since the size of each orbit divides $|C_p| = p$,

$np = |G|^{p-1} = |Y| = 1 + \sum |\text{other orbits}| = 1 + mp$ → contradiction

so there are some fixed point $(g, ..., g)$ other than $(1, ..., 1)$ and $g^p = 1$. Then $|g| = p$.

Fixed Point Theorem. G is a group acting on a set X. $|G| = p^k$ where p is a prime and $k > 0$. If $p \nmid |X|$, then there exists a fixed point $x \in X$ under this action, i.e. $g.x = x$ for any $g \in G$.

Pf. x is a fixed point $\iff O(x) = \{x\} \iff G_x = G$.

By Counting Formula, for any orbit $O(y)$, $|O(y)|$ divides $|G| = p^k$, so $|O(y)| = p^m, 0 \leq m \leq k$. Suppose the action has no fixed point, then $|O(y)| = p^m, 1 \leq m \leq k$.

$|X| = \sum |\mathrm{orbits}|$, LHS not divisible by p by assumption, RHS divisible by p → contradiction.