§3.6 Permutation Groups

Shaoyun Yi

MATH 546/701I

University of South Carolina

Summer 2021

Review for §3.5

- Every subgroup of a cyclic group G is cyclic.
- Let G be a cyclic group. $\begin{cases} \text{i) If } G \text{ is infinite, then } G \cong \mathbf{Z}. \\ \text{ii) If } |G| = n < \infty, \text{ then } G \cong \mathbf{Z}_n. \end{cases}$
- i) Any two infinite cyclic groups are isomorphic to each other.
  ii) Two finite cyclic groups are isomorphic $\Leftrightarrow$ they have the same order.
- Subgroups of $\mathbf{Z}$: For any $0 \neq m \in \mathbf{Z}$, $\langle m \rangle = m\mathbf{Z} \cong \mathbf{Z} = \langle 1 \rangle = \langle -1 \rangle$.
  $\bullet\ m\mathbf{Z} \subseteq n\mathbf{Z} \Leftrightarrow n|m$ $\quad \bullet\ m\mathbf{Z} = n\mathbf{Z} \Leftrightarrow m = \pm n$
- Subgroups of $\mathbf{Z}_n$: For any $d|n$, $d\mathbf{Z}_n = \langle [d] \rangle \rightsquigarrow$ **subgroup diagram**
  i) $d = (k, n)$: $\langle [k] \rangle = \langle [d] \rangle$ & $|\langle [k] \rangle| = |\langle [d] \rangle| = n/d$.
  ii) $\mathbf{Z}_n = \langle [k] \rangle \Leftrightarrow [k] \in \mathbf{Z}_n^\times \Leftrightarrow (k, n) = 1$.
  iii) If $d_1|n$ and $d_2|n$, then $\langle [d_1] \rangle \subseteq \langle [d_2] \rangle \Leftrightarrow d_2|d_1$.
  iii)′ If $d_1|n$ and $d_2|n$ and $d_1 \neq d_2$, then $\langle [d_1] \rangle \neq \langle [d_2] \rangle$.
- $\mathbf{Z}_n \cong \mathbf{Z}_{p_1^{\alpha_1}} \times \mathbf{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbf{Z}_{p_m^{\alpha_m}} \rightsquigarrow$ Euler's totient function $\varphi(n)$
- Let G be a *finite abelian* group. Let N be the **exponent** of G.
  $N = \max\{o(a) \colon a \in G\}$. In particular, G is cyclic $\Leftrightarrow N = |G|$.
- For small n, check $\mathbf{Z}_n^\times$ cyclic or not without using *primitive root thm*.

Review for §2.3

- A **permutation** $\sigma\colon S \to S$ is one-to-one and onto. Write $\sigma \in \mathrm{Sym}(S)$
- $\mathrm{Sym}(S)$ is a group under $\circ$. S_n is the **symmetric group** of degree n.
- $|S_n| = n!$
- Cycle of length k: $\sigma = (a_1 a_2 \cdots a_k)$ has order k.
- Disjoint cycles are commutative.
- $\sigma \in S_n$ can be written as a *unique* product of disjoint cycles.
- The order of σ is the **lcm** of the orders of its disjoint cycles.
- A **transposition** is a cycle $(a_1 a_2)$ of length two.
- $\sigma \in S_n$ can be written as a product of transpositions. (NOT unique)
- Even permutation & Odd permutation
- A cycle of odd length is even. & A cycle of even length is odd.

Cayley's Theorem

Any subgroup of the symmetric group $\mathrm{Sym}(S)$ is called a **permutation group**.

Every group G is isomorphic to a permutation group.

Proof: Given $a \in G$, define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$. To show $\lambda_a \in \mathrm{Sym}(G)$.

- λ_a is one-to-one: If $\lambda_a(x_1) = \lambda_a(x_2)$, then $x_1 = x_2$. [Why?]
- λ_a is onto: For any $x \in G$, we have $\lambda_a(a^{-1}x) = a(a^{-1}x) = x$. $\square$

This implies that $\phi : G \to \mathrm{Sym}(G)$ defined by $\phi(a) = \lambda_a$ is well-defined.

To show $G_\lambda := \phi(G)$ is a subgroup of $\mathrm{Sym}(G)$.

i) Closure: For any $\lambda_a, \lambda_b \in G_\lambda$ with $a, b \in G$, to show $\lambda_a \lambda_b \in G_\lambda$.

$$\lambda_a\lambda_b(x) = \lambda_a(\lambda_b(x)) = \lambda_a(bx) = a(bx) = (ab)x = \lambda_{ab}(x) \quad \text{for all } x \in G.$$

ii) Identity λ_e: $\lambda_a\lambda_e = \lambda_{ae} = \lambda_a \quad \& \quad \lambda_e\lambda_a = \lambda_{ea} = \lambda_a$.

iii) Inverses $\lambda_{a^{-1}}$: $\lambda_a\lambda_{a^{-1}} = \lambda_e \quad \& \quad \lambda_{a^{-1}}\lambda_a = \lambda_e$. $\square$

Define $\phi\colon G \to G_\lambda$ by $\phi(a) = \lambda_a$ (well-def., onto). To show ϕ is an isomorphism.

1) For all $x \in G$, $\phi(a) = \phi(b) \rightsquigarrow \lambda_a(x) = \lambda_b(x) \rightsquigarrow ax = bx \rightsquigarrow a = b$.

2) For any $a, b \in G$, we have $\phi(ab) = \lambda_{ab} = \lambda_a\lambda_b = \phi(a)\phi(b)$. $\square$

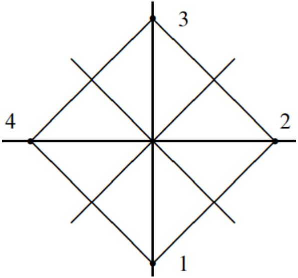
Thus $G \cong G_\lambda$, where G_λ is a permutation group. [Why?] $\square$

Example: Rigid Motions of a Square

A **rigid motion** is a change in position where the distance between points is preserved and figures remain congruent (having the same size and shape)

- Translation (slide) • Reflection (flip) • Rotation (turn) • A combination of these

Each rigid motion determines a permutation of the vertices of the square. There are a total of eight rigid motions of a square. [Why?] $(4 \cdot 2 = 8)$



(1234) counterclockwise rotation through 90°

$(13)(24)$ counterclockwise rotation through 180°

(1432) counterclockwise rotation through 270°

(1) counterclockwise rotation through 360°

(24) flip about vertical axis

(13) flip about horizontal axis

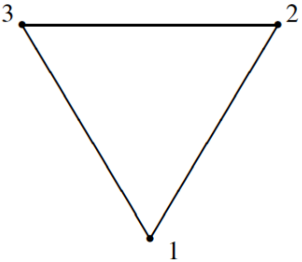
$(12)(34)$ flip about diagonal

$(14)(23)$ flip about diagonal

We do not obtain all $(4! = 24)$ elements of S_4 as rigid motions. e.g., (12)

Example: Rigid Motions of an Equilateral Triangle

The rigid motions of an equilateral triangle yield the group S_3.



(123) counterclockwise rotation through 120°

(132) counterclockwise rotation through 240°

(1) counterclockwise rotation through 360°

(23) flip about vertical axis

(13) flip about angle bisector

(12) flip about angle bisector

Recall: Another notion for describing S_3 in §3.3

$$S_3 = \{e, a, a^2, b, ab, a^2b\}, \quad \text{where } a^3 = e,\ b^2 = e,\ ba = a^2b = a^{-1}b.$$

Another notion for describing Rigid Motions of a Square

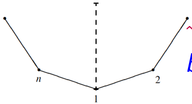
Let $a = (1234)$ and $b = (24)$. It can be shown that $ba = a^3b$.

$S = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e, b^2 = e, ba = a^3b = a^{-1}b$.

Rigid Motions of a Regular Polygon (n-gon)

There are $2n$ rigid motions of a regular n-gon.

Proof: There are n choices of a position in which to place first vertex A, and then two choices for second vertex since it must be adjacent to A. $\square$



a is a counterclockwise rotation about the center through $(360/n)^\circ$

$\rightsquigarrow$ a is the cycle $(123\cdots n)$ of length n and has order n.

b is a flip about the line of symmetry through position number 1.

$\rightsquigarrow$ b is the product of $(2n)(3\ n-1)\cdots$ and has order 2.

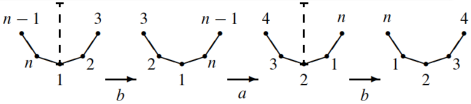
Consider the set $S = \{a^k, a^k b \mid 0 \leq k < n\}$ of rigid motions with $|S| = 2n$.

- a^k for $0 \leq k < n$ are all distinct. [Why?]
- $a^k b$ for $0 \leq k < n$ are all distinct.
- $a^k \neq a^j b$ for all $0 \leq k, j < n$ since a^k does not flip the n-gon.

$$S = \{a^k, a^k b \mid 0 \leq k < n\}, \quad \text{where } a^n = e,\ b^2 = e,\ ba = a^{-1}b.$$

To show $ba = a^{-1}b \iff bab = a^{-1}$

a^{-1}: clockwise rotation through $(360/n)^\circ$



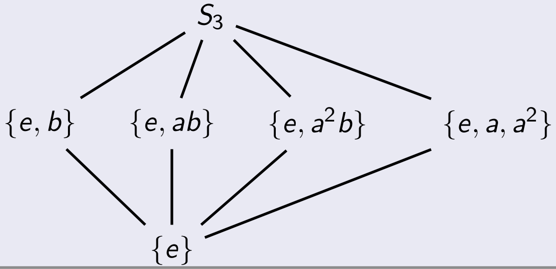
Dihedral Group D_n ($n \geq 3$)

Let $n \geq 3$ be an integer. The group of rigid motions of a regular n-gon is called the nth **dihedral group**, denoted by D_n. Note that $|D_n| = 2n$.

$$D_n = \{a^k, a^k b \mid 0 \leq k < n\}, \quad \text{where } a^n = e,\ b^2 = e,\ ba = a^{-1}b.$$

- We will not list all subgroups of S_n ($n \geq 4$) since there are too many.
- The "simple" subgroups of S_n: cyclic subgroup generated by $\sigma \in S_n$.
- The dihedral group D_n is one important example of subgroups of S_n.
- The alternating group A_n is another one important example. (soon!)

Every proper subgroup of $D_3 = S_3$ is cyclic. [Why?] Its subgroup diagram



Subgroups of D_4

$D_4 = \{e, a, a^2, a^3, b, ab, a^2b, a^3b\}$, where $a^4 = e$, $b^2 = e$, $ba = a^{-1}b = a^3b$.

The possible orders of proper subgroups of D_4 are 1, 2, or 4. [Why?]

I. Two special subgroups: $\{e\}$ (trivial subgroup) & D_4 (non-cyclic)

II. The cyclic subgroups:
   i) $a^4 = e$: $\langle a \rangle = \langle a^3 \rangle = \{e, a, a^2, a^3\}$ & $\langle a^2 \rangle = \{e, a^2\}$ (Note that $2|4$.)
   ii) Each of the elements b, ab, a^2b, a^3b has order 2. (Check it!)

III. **Q:** Are there proper subgroups of D_4 that are not cyclic? **A:** Yes.

If H is a non-cyclic proper subgroup, then $H \cong \mathbf{Z}_2 \times \mathbf{Z}_2$.

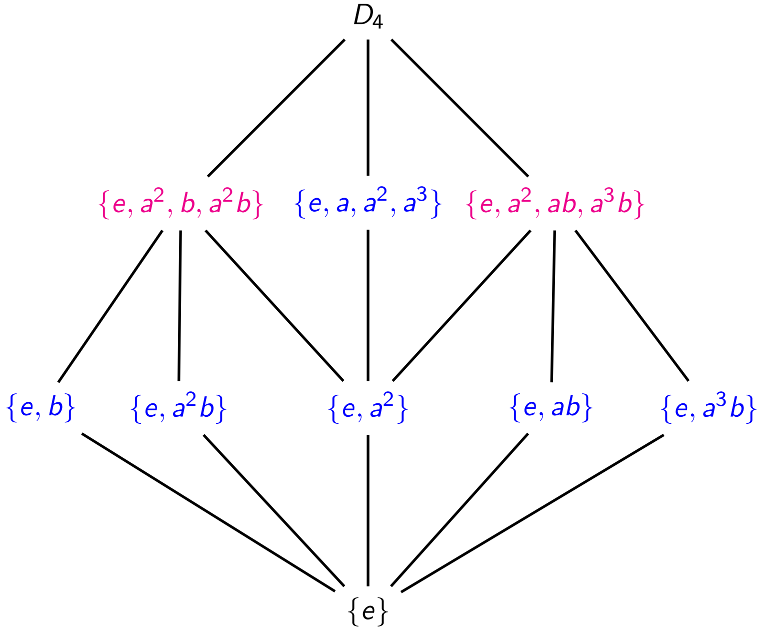
Proof: $|H| = 4$ and any non-identity element of H has order 2. $\square$

Say $H = \{e, x, y, xy\}$, and so $yx = xy$ since H is abelian.

Consider all possible pairs of elements of order 2 to find all such H's.

1) $H_1 = \{e, a^2, b, a^2b\}$: $ba^2 = \cdots = a^2b$ ✓
2) $H_2 = \{e, a^2, ab, a^3b\}$: $(ab)a^2 = \cdots = a^3b$ ✓

Subgroup Diagram of D_4



Alternating Group A_n $(n \geq 2)$

The set of all even permutations of S_n is a subgroup of S_n.

Proof: $(|S_n| < \infty)$ Nonempty: (1) Closure: If σ and τ are even, so is $\tau\sigma$.

The set of all even permutations of S_n is called the **alternating group** A_n.
$|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$. This is the largest possible cardinality for a proper subgroup.

Proof: Let O_n be the set (not a subgroup) of odd permutations in S_n. So

$$S_n = A_n \bigsqcup O_n \quad \rightsquigarrow |S_n| = |A_n| + |O_n|.$$

i) For each odd permutation $\sigma \in O_n$, the permutation $(12)\sigma$ is even. If σ and τ are two distinct odd permutations, then $(12)\sigma \neq (12)\tau$. Thus, $|A_n| \geq |O_n|$. [Why?]

ii) Similarly, we can show that $|O_n| \geq |A_n|$.

iii) Therefore, $|A_n| = |O_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$. □

e.g., $S_3 = \{(1), (12), (13), (23), (123), (132)\} \rightsquigarrow A_3 = \{(1), (123), (132)\}$

Example: List all the Elements of A_4 with $|A_4| = 12$.

The **decomposition type** of a permutation σ in S_n is the list of all the cycle lengths involved in a decomposition of σ into disjoint cycles.

$\rightsquigarrow$ Possible decomposition types of permutations of S_4:

I. a single cycle of length $1, 2, 3$ or 4

II. two disjoint cycles of length 2

$\rightsquigarrow$ Only single cycles of length 1 or 3 and two disjoint cycles of length 2 could possibly be even. Note that the single cycle of length 1 is just (1).

i) single cycle of length 3: Choose any three of the numbers $1, 2, 3, 4$:

$$\binom{4}{3} = \text{Four choices:} \quad 123, \quad 124, \quad 134, \quad 234.$$

For each choice, there are **two** ways to make a cycle.

$$(123),\ (132), \quad (124),\ (142), \quad (134),\ (143), \quad (234),\ (243).$$

ii) two disjoint cycles of length 2: Choose any two of the $\#$s $1, 2, 3, 4$:

$$\binom{4}{2} = \text{Six choices:} \quad 12, \quad 13, \quad 14, \quad 23, \quad 24, \quad 34.$$

$\rightsquigarrow$ **Three** different products of two disjoint transpositions. [Why?]

$$(12)(34), \quad (13)(24), \quad (14)(23).$$

$\rightsquigarrow$ $A_4 = \{(1), (123), (132), \ldots, (234), (243), (12)(34), (13)(24), (14)(23)\}$

The Converse of Lagrange's Theorem is False

Recall that $A_4 = \{(1), (123), (132), \ldots, (234), (243), (12)(34), (13)(24), (14)(23)\}$
In particular, every non-identity element of A_4 has order 2 or 3. [Why?]

A_4 has no subgroup of order 6.

Proof by contradiction: Suppose that H is a subgroup of order 6 in A_4.

H must contain an element of order 2.

Proof: If not, $\{h, h^{-1}\} \in H$ with $h \neq h^{-1}$ for any $h \neq e$ & $\{e, e^{-1}\} = \{e\}$.
$\rightsquigarrow$ H has an odd number of elements, which is impossible. $\square$

H must contain an element of order 3.

Proof: If not, assume that every non-identity element of H has order 2.
Let $x, y \in H$ with $x \neq y$ and $o(x) = o(y) = 2$. So $o(xy) = 2$ since $xy \in H$ and $xy \neq e$ [Why?]. And then $xy = yx$ since $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.
$\rightsquigarrow$ $\{e, x, y, xy\}$ is a subgroup of H of order 4, a contradiction. [Why?] $\square$
$\rightsquigarrow$ H must contain an element (abc) and $(ab)(cd)$ for distinct a, b, c, d.
Then H contains $(abc)(ab)(cd) = (acd)$ and $(ab)(cd)(abc) = (bdc)$.
$\rightsquigarrow$ H has **six** elements of order 3 since $(acb), (adc), (bcd) \in H$. [Why?] $\square$

Two Examples

$$A_4 \not\cong S_3 \times \mathbf{Z}_2$$

Proof: A_4 has no subgroup of order 6, but $S_3 \times \mathbf{Z}_2$ does (e.g., $S_3 \times \{[0]_2\}$)

$$S_4 \not\cong A_4 \times \mathbf{Z}_2$$

Proof: The largest possible order of an element in S_4 is 4. [Why?]

Recall that the possible decomposition types of permutations of S_4 are

I) a single cycle of length $1, 2, 3$ or 4

II) two disjoint cycles of length 2

And so the possible decomposition types of permutations of A_4 are

i) a single cycle of length 1 or 3

ii) two disjoint cycles of length 2

It follows that there is an element of order 6 in $A_4 \times \mathbf{Z}_2$. [Why?]

However, S_4 has no element of order 6. Thus $S_4 \not\cong A_4 \times \mathbf{Z}_2$. $\square$