Permutation Groups

Wednesday, October 15, 2025 9:47 AM

Missing

100 # 1, 7, 9, 10, 14,

+B # 118

200 # 1, 2, 7, 8, 9, 10, 17, 21, 22, 24

+B # 203, 218, 226, 220

+2B # 215

500 # 10/19 online

—

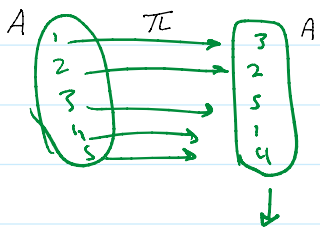
Recall: Groups

§ 3. Permution Groups

1] Def^n. Let $A = \{1, 2, \cdots, n\}$,
a permutation π of A is a bijection from A to A.

$$\pi : A \to A$$

i.e. π is an ordered list of the elements in A.



[3 2 5 1 4]

e.g. $A = \{1, 2, 3\}$

$\pi = [3 \ 1 \ 2]$

2] Notation:

$$S(A) = \{\pi \mid \pi \text{ is a permation of } A\}$$

if $|A| = n$, then $S(A) = S_n$

$$S_n = \{\pi \mid \pi \text{ is a permutation of } n \text{ elements}\}$$

3] e.g. For $n = 3$

$$S_3 = \{[1\ 2\ 3], [1\ 3\ 2], [2\ 1\ 3], [2\ 3\ 1], [3\ 1\ 2], [3\ 2\ 1]\}$$

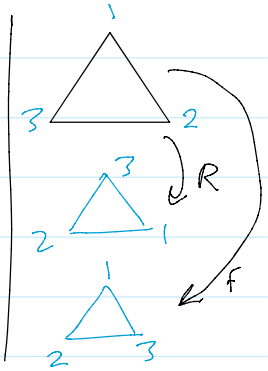
Let $\pi = [3 \ 1 \ 2]$. then $\pi : A \to A$ is a bijection

$$\pi(1) = 3, \quad \pi(2) = 1, \quad \pi(3) = 2$$

The null permutation $\pi_0 = [1\ 2\ 3]$, $\pi(x) = x$

4] Prop. $(S_n, \circ)$ is a group with the operation of function composition, $\pi_1 \circ \pi_2$ defined by

$$\pi_1 \circ \pi_2 (x) = \pi_1 (\pi_2 (x))$$



Here, S_n is a permutation group of A, a.k.a. the Symmetric group on A

5] Note: In $(S_n, \circ)$, the operation $\pi_1 \circ \pi_2$ means applying π_1 after π_2.

The identity element is the null permutation π_0.

6] e.g. π_a π_b

$$[1\ 3\ 2] \circ [2\ 1\ 3]$$

$$= [3\ 1\ 2]$$

$\pi_b \circ \pi_a$

$$[2\ 1\ 3] \circ [1\ 3\ 2]$$

$$= [2\ 3\ 1]$$

e.g. π_a π_b

in S_3, find ① $[1\ 3\ 2] \circ [3\ 2\ 1]$

$$= [2\ 3\ 1]$$

π_b π_a

② $[3\ 2\ 1] \circ [1\ 3\ 2]$

$= [3 \quad 1 \quad 2]$

$\therefore (S_n, \circ)$ is non-abelian

7] Prop. every $\pi \in S_n$ can be written a a product of disjoint cycles. The cycles are unique.

8]. e.g. S_6, $\pi = [1 \quad 4 \quad 6 \quad 5 \quad 2 \quad 3]$

$c_1 : \quad 1 \longrightarrow 1 \qquad (1)$

$c_2 : \quad 2 \longrightarrow 4 \longrightarrow 5 \longrightarrow 2 \qquad (2 \quad 4 \quad 5)$

$c_3 : \quad 3 \longrightarrow 6 \longrightarrow 3 \qquad (3 \quad 6)$

$\therefore \quad \pi = c_1 \circ c_2 \circ c_3 = (1) \circ (2 \quad 4 \quad 5) \circ (3 \quad 6)$

$$\pi(2) = c_1 \circ c_2 \circ c_3 (2) = c_1 \circ c_2 (2)$$
$$= c_1 (4)$$
$$= 4$$

$$\pi(3) = c_1 \circ c_2 \circ c_3 (3) = c_1 \circ c_2 (6)$$
$$= c_1 (6)$$
$$= 6$$

Review:

① Fermat Theorem

$$a^{p-1} \equiv 1 \pmod{p}$$

e.g. $4^{225} \pmod{13}$

$\equiv (4^{12})^{10} \cdot 4^{-15}$

$\equiv (1)^{10} \cdot (4^{12})^{-1} \cdot 4^{-3}$

$\equiv 1 \cdot 1 \cdot 4^{-3}$ by F.T.

$\equiv (2)^{-6} \equiv 2^{6}$

$= 2^4 \cdot 2^2$

$\equiv 3 \cdot 4 \equiv 12 \pmod{13}$

4^{225}

$\equiv 4^{-15} \equiv 4^{-3}$ by FT

$\equiv 2^{-6} \equiv 2^{6} = 2^4 \cdot 2^2$

$= 12$

② Cyclic Groups

$\mathbb{Z}_n^*$ is cyclic if

$n = 2, 4, p^k, 2p^k$

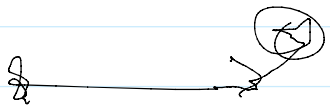
$\mathbb{Z}_{24}^*$ zero generators

$\mathbb{Z}_{18}^*$ $18 = 2 \cdot 3^2$. It is cyclic

It has $\phi(|\mathbb{Z}_{18}^*|)$ generators

$= \phi(6) = 2$ generators

③ Cyclic Groups Exer



Q2.

$A = \{1, 5, 7, 11\}$ $\quad x * y = xy \pmod{24}$

$\langle 5 \rangle = \{5, 1\}$

$\langle 7 \rangle = \{7, 1\}$

$\langle 11 \rangle = \{11, 1\}$

∴ no. generator $\Longrightarrow$ not cyclic

Q3. Is $\mathbb{Z}_n^*$ cyclic

$n = 6$ Yes $\Longrightarrow$ has $\phi(2) = 1$ generator

$n = 30 = 2 \cdot 3 \cdot 5$. no

$n = 32 = 2^5$ No, 2 is not odd.

Exer #2

Is $\mathbb{Z}_{125}^* \cong \mathbb{Z}_{250}^*$?

Soln

$|\mathbb{Z}_{125}^*| = \phi(125) = \phi(5^3) = 4 \cdot 5^2 = 100$

$$|\mathbb{Z}_{250}^*| = \phi(2 \cdot 125) = 100$$

both are cyclic for $125 = 5^3$, $250 = 2 \cdot 5^3$

$\therefore$ they are isomorphic

Proof:

Let $\langle \alpha \rangle = \mathbb{Z}_{125}^*$

$\langle \beta \rangle = \mathbb{Z}_{250}^*$

① define $\theta : \mathbb{Z}_{125}^* \longrightarrow \mathbb{Z}_{250}^*$ bijection by

$$\theta(\alpha^i) = \beta^i$$

Thus

x	α	α^2	α^{40}	α^{70}	$\alpha^{100} = 1$
$\theta(x)$	β	β^2	β^{40}	β^{70}	$\beta^{100} = 1$

②

$$\theta(\alpha^i \cdot \alpha^j) = \theta(\alpha^{i+j})$$

$$= \beta^{i+j}$$

$$= \beta^i \cdot \beta^j$$

$$= \theta(\alpha^i) \cdot \theta(\alpha^j)$$

$\therefore \theta$ is a homomorphic bijection

$\Rightarrow$ Isomorphism