Permutation Groups

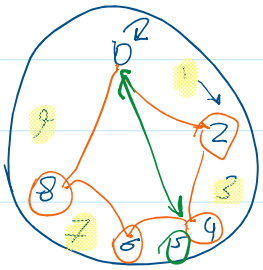
Wednesday, April 1, 2026 7:07 PM

Recall: cyclic groups

e.g. $\mathbb{Z}_{10} = \langle 1 \rangle$

divisors of 10: $d = 1, 2, 5, 10$

$\phi(5) = 4$ $\Rightarrow$ we have 4 elts of order 5



Note; safe prime

$p = 2q + 1$ where q is prime

$\mathbb{Z}_{23}^*$ is cyclic by primitive-root theorem $n = p, 2p, p^k, 2p^k$

it has $\phi(22) = 10$ generators.

Since $23 = 2 \cdot q + 1$ is safe prime, besides 1 and -1,

every other element is a generator, or of high order $\frac{|G|}{2}$

e.g. (homomorphism) $\theta: \mathbb{Z} \to \mathbb{Z}_{23}^*$, $\theta(a+b) = \theta(a) \cdot \theta(b)$

x	..	-3	-2	-1	0	1	2	3 ..	4	5	6
$\theta(x)$		6	12	1	2	4	8	16	9	18	

take $d \in \mathbb{Z}_{23}^*$, $d = 2$. $\theta(n) = 2^n \pmod{23}$

Proof let $a, b \in \mathbb{Z}$

then $\theta(a+b) = 2^{a+b}$

$= 2^a \cdot 2^b$

$= \theta(a) \cdot \theta(b)$.

§ 3. Permutation Groups

1] Def^n. Let $A = \{1, 2, \ldots, n\}$

a permutation π of A is a bijection from A to A

$$\pi : A \longrightarrow A$$

Here π is an ordered list of the elements in A

e.g. $\pi = [2\ 3\ 1]$

2] Notation

① $S(A)$ is the set of all permutations of A.

② If $|A| = n$, then $S_n = S(A)$.

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

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

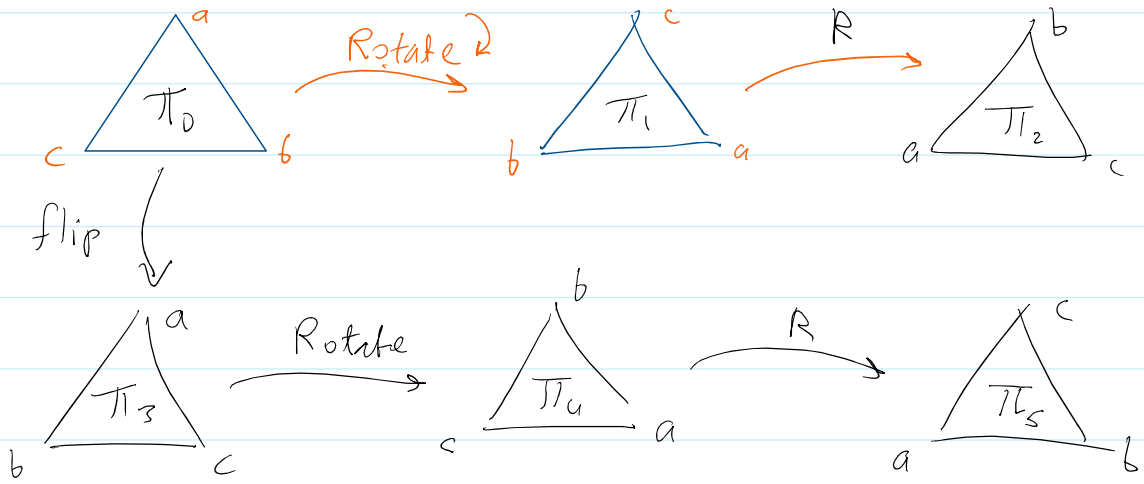
$$S_3 = \{[1\ 2\ 3], [1\ 3\ 2], [2\ 1\ 3], [2\ 3\ 1], [3\ 1\ 2], [3\ 2\ 1]\}$$

take $\pi = [2\ 1\ 3]$ as a function $\pi : A \to A$

defined by $\pi(1) = 2$, $\pi(2) = 1$, $\pi(3) = 3$

The null permutation $\pi_0 = [1\ 2\ 3]$, defined as $\pi_0(i) = i$

S_n known as the symmetric group on $A = \{1, 2, \ldots, n\}$



4] Proposition:

$(S_n, \circ)$ is a group with the operation of composition of functions, (called the symmetric group)

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

π_1 after π_2

5] Note: In $(S_n, \circ)$

$\pi_0 = [1\ 2\ \cdots\ n]$ is the identity.

The group is non-abelian for $n > 2$ since π_1 of π_2