04 November 2020 09:04

4, 5, 6, 7 → Whole syllabus

Unit-4 Group

Unit-5 → Ring, field → 1 lec

Unit-6 → G.F. → 1 lect

5 Assignments

$\boxed{\text{7 quiz}}$ → best five

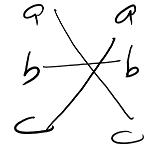
Permutation groups :- $S = \{a, b, c\}$. $\phi : S \to S$: bijective function

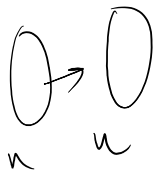
n elements.

↳ one-to-one mappings.

$\phi : S \to S$

$$\phi = \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \Rightarrow$$





$\Rightarrow n!$

$S = \{a, b\}$ ϕ_1 ϕ_2.

$S = \{a, b\}$, $p_1 = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$ $p_2 = \begin{pmatrix} a & b \\ a & b \end{pmatrix}$

Δ	p_1	p_2
p_1	p_2	
p_2	p_1	

Δ - (right) Composition of permutations.

$p_i \Delta p_j =$

$\circ \to$ (left) Composition of permutations.

$p_i \Delta p_j = p_j \circ p_i$ for $j = 1, 2$

$(p_i \Delta p_j) a = (p_j \circ p_i) a = p_j(p_i(a)) \to$

$(p_i \Delta p_j) b = (p_j \circ p_i) b = p_j(p_i(b)) \to$

$(p_2 \Delta p_1) a = (p_1 \Delta p_2) a = p_1(p_2(a)) = p_1(a) = b$

$(p_2 \Delta p_1) b = p_2(p_1(b)) = p_2(b) = a$

$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \approx p_1$

(1) Δ, $\circ \to$ Associative

(2) identity $\to p_2$ w.r.t. Δ.

(3) Inverse should exist

$\{a, b\}$ $\{1, 2\}$

$\langle S_2, \Delta \rangle \to$

$\langle S_3, \Delta \rangle \to$

$\langle S_4, \Delta \rangle \to$

$\{S_3, \Delta\}$ +1

$S = \{a, b, c\}$

$S_3 = \{p_1, p_2 \to p_6\}$

$p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$p_i \Delta p_j \neq p_j \Delta p_i \to$

Δ	p_1	p_2	p_3	p_4	p_5
p_1	–	–	–		
p_2	–	–	–		
p_3	–	–	– p_4		
	–	–	–		
p_6	–				

→ Abelian group → Yes

– ~~X~~ ~~(3)~~

$p_3 \Delta p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \Delta \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$= p_4$

$p_3 \Delta p_5 = p_4$

$\{S_n, \Delta\} \to$ order $\to n!$ →

degree $\to n$.

$S = \{a, b, c\} \Rightarrow 3$

$S_3 = \{p_1 - p_6\} \Rightarrow 6$

$a \in G \to$ a^n for some n

$\langle Z_m, +_m \rangle \to$ generator

[0] [1] [2] [3]

$m=5$, $\langle Z_5, +_5 \rangle \to$ [1] [2] [3] [4]

$m=6$ $\langle Z_6, +_6 \rangle \to$ [1] [5] only.

$G \to \{4\}$

$S \to 2$
[1]

Sub-group:- $\langle G, * \rangle$ $S \subseteq G$

i) $e \in S$, e is the identity element of $\langle G, * \rangle$

ii) $a \in S$ then $a^{-1} \in S$.

iii) for $a, b \in S$, then $a * b \in S$

then $\langle S, * \rangle$ is called subgroup of $\langle G, * \rangle$.

$\langle G, * \rangle \longrightarrow$ trivial subgroups $\langle \{e\}, * \rangle$

$\langle G, * \rangle$

proper subgroups.

A subset $S \neq \phi$ of G is a subgroup of $\langle G, * \rangle$, if

for any $a, b \in S$, $a * b^{-1} \in S$

---

e_G. $\langle G, * \rangle$, $\langle H, \Delta \rangle$ e_H.

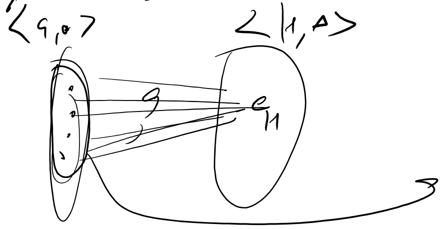
$g : G \to H$ iff

$$g(a * b) = g(a) \Delta g(b) \quad - (1).$$ → preserve the identity, inverses & subgroups

$$g(e_G) = e_H$$

$$g(a^{-1}) = [g(a)]^{-1}$$

Kernal :-



→ Kernal → Set of all elements of G. Which are mapped to e_H.

G = 20

Fact: not every subset of a set is a subgroup.

problem: find all the subsets which can qualify to become subgroups.

Relationship.

Subgroups $\Leftarrow$ group

$\Downarrow$

Lagrange's theorem.

Subgroup.

Let $\langle G, * \rangle$ $\langle H, * \rangle$

Equiv. R. is called left coset relation w.r.t. $\langle H, * \rangle$

left coset relation modulo H.

S.t for any $a, b \in G$, $a \equiv b \pmod{H}$ iff $b^{-1} * a \in H$ $\Rightarrow$ Equivalence Relation??

Reflexive $a \equiv a \pmod{H}$

$a^{-1} * a \in H$. $a^{-1} * a = e \in H$. $a \equiv a \pmod{H}$

Symmetric $a \equiv b \pmod{H}$ $b \equiv a \pmod{H}$

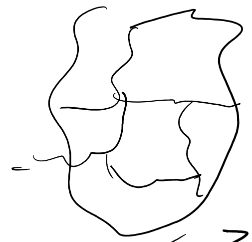
$b^{-1} * a \in H$. $(b^{-1} * a)^{-1} = (a^{-1} * b) \in H \Rightarrow b \equiv a \pmod{H}$

Transitive

04 November 2020 09:45

Equiv. R.

The Equivalence relation R partition the set G. into Equivalence Classes



For any $a \in G$.

$$[a] = \{x \in G \mid x \equiv a \pmod H\}$$
$$= \{x \in G \mid a^{-1} + x \in H\}$$
$$= \{a + h \mid h \in H\}$$

$a^{-1} + x = h$
$x = a + h$

$\langle Z_5, +_5 \rangle$

$$[a] = \{a + h \mid h \in H\}$$

Def^n - Let $\langle H, + \rangle$ $a \in G$,

$a \rightarrow$ representative element of G.

$$aH = \{a + h \mid h \in H\}$$

$\rightarrow$ the left coset of H in G. determined by the elem $a \in G$.

$$Ha = \{h + a \mid h \in H\}$$

Lagrange's theorem :-> Subgroup ← group

$|G| = 48$

1, 2, 3, 4, 6, 8, 12, 24, 48

The order of a subgroup of a finite group divides the order of a group.

$$\text{index } k = \frac{|G|}{|H|}$$

→ $|G| = 17$

Normal Subgroups :-> $\langle H, * \rangle$ of $\langle G, * \rangle$. Every subgroup of an abelian group is normal.

if $gH = Hg$

left coset = Right coset

04 November 2020 09:56

Algebraic System

↪ Ring

Field

and Integral domain

Error Correcting Codes.

Group codes → H/w.

fast adders → Digital Logic }

Unit-6 { Generating functions

Recurrence Relation } Kenneth Rosen }