Algebra 18-3-2019

$U(10) = \{1,3,7,9\}$

φ

$\mathbb{Z}_4 = \{0,1,2,3\}$

(i) φ is bijective

(ii) $\varphi(x \cdot y) = \varphi(x) + \varphi(y)$

e.g. $\varphi(3 \cdot 9) = \varphi(7) = 3$

$\varphi(3) + \varphi(9) = 1 + 2 = 3 \neq 8$

Second example $U(12) = \{1,5,7,11\}$

$\mathbb{Z}_4 \Phi = \{0,1,2,3\}$. $\uparrow \varphi$?

$\varphi(x) = 5$

$\varphi(x+x) = \varphi(x) \cdot \varphi(x) = 5 \cdot 5 = 1$

$x=1$ $\varphi(2) = 1$ $\varphi(3) = \varphi(1+x+1) = 5 \cdot 5 \cdot 5 = 5$ ξ

Def. $(G_1, *_1)$ $(G_2, *_2)$

$\varphi : G_1 \to G_2$ is called isomorphism:

- φ is bijective
- $\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$

$(G_1, *_1) \cong (G_2, *_2)$

$U_{10} \cong \mathbb{Z}_4$, $U_{12} \stackrel{?}{\cong} \mathbb{Z}_4$

Theorem Let $(G, *)$ be a group of 4 elts.

then either $(G, *) \cong \mathbb{Z}_4$ or $(G, *) \cong U(12)$

Examples $(\mathbb{R}, +) \cong (\mathbb{R}_+, \cdot)$ $\varphi(x) = 2^x$

$\varphi(x+y) = 2^{x+y} = 2^x \cdot 2^y = \varphi(x) \cdot \varphi(y)$

$(\mathbb{Q},+) \xrightarrow{?} (\mathbb{Q}_+,\cdot)$ → exercise

Properties (i) $\varphi(e_1)=e_2$

$g_2 \in G_2$ let $\varphi(g_1)=g_2$

$g_2=\varphi(g_1)=\varphi(e_1 g_1)=\varphi(e_1)\cdot\varphi(g_1)=\underbrace{\varphi(e_1)}_{e_2}\cdot g_2$

(ii) $\varphi(g_1^{-1})=\varphi(g_1)^{-1}$

(iii) $|\varphi(g_1)|=|g_1|$

$U(12)=\{1,5,7,11\} \not\cong \mathbb{Z}_4=\{0,1,2,3\}$

orders: 1 2 2 2 vs 1 4 2 4

Theorem Let $(G,*)$ be a finite group, say $|G|=n$ then G is isomorphic to a subgroup of S_n.

"proof" $G=\{g_1,g_2,g_3,\dots,g_{n-1},g_n\}$

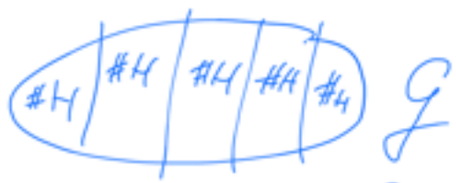
$\varphi(g_1)\in S_n$ $\begin{pmatrix} g_1 g_1, g_1 g_2, g_1 g_3, g_1 g_4, \dots g_1 g_{n-1}, g_1 g_n \\ = \begin{pmatrix} g_{i_1}, g_{i_2}, g_{i_3}, \dots g_{i_{n-1}}, g_{i_n} \end{pmatrix} \\ (i_1\ i_2\ i_3\ i_4 \dots i_{n-1}\ i_n) \end{pmatrix}$

Notion of coset

Let H be a subgroup of G, $|G|<\infty$ then $|H|$ divides $|G|$.

Corollary $|a|$ divides $|G|$.

because $H=\langle a\rangle$
the $|H|=|a|$



H subgroup of G
$a\in G \quad aH=\{ah \mid h\in H\}$

$G=(\mathbb{Z},+) \quad H=\{3k \mid k\in\mathbb{Z}\}=\langle 3\rangle$
$0.H=\{0+h \mid h\in H\}=\{3k \mid k\in\mathbb{Z}\}=H$
$1.H=\{1+h \mid h\in H\}=\{3k+1 \mid k\in\mathbb{Z}\}$
$2.H=\{2+h \mid h\in H\}=\{3k+2 \mid k\in\mathbb{Z}\}$
$3.H=0.H \; ; \; 4H=1.H$
$a.H=bH$ or $aH\cap bH=\emptyset$
$\bigcup aH=\mathbb{Z}$
$a\in G$

Properties
- $a\in aH \Rightarrow \bigcup_{a\in G} aH=G$
- $aH=bH \Leftrightarrow a\in bH \Leftrightarrow b\in aH$
- $aH=bH$ or $aH\cap bH=\emptyset$
  proof Let $aH\cap bH\neq\emptyset$, then:
  $x\in aH\cap bH$
  $x=ah_1=bh_2 \Rightarrow ah_1=bh_2$
  $\Rightarrow a=\underbrace{bh_2h_1^{-1}}_{\in H} \Rightarrow a\in bH$
  $\Rightarrow aH=bH$
- $\forall a\in G \quad |aH|=|H|$

proof of Lagrange: $G=\bigcup_1^N a_iH \Rightarrow |G|=\sum_1^N |a_iH|$

$a_i H \cap a_j H = \emptyset \quad i \neq j$ $\quad = \sum_{k=1}^{N} |H| = N \cdot |H|$.

$|H| = |G|/N \qquad N = |G|/|H|$

Corollary - $|G| = p \Rightarrow G$ is cyclic

- $a \in G \quad a^{|G|} = e$

$|a|$ divides $|G|$, say $|G| = k \cdot |a|$

$a^{|G|} = a^{k \cdot |a|} = (a^{|a|})^k = e^k = e$

($a^{|a|} = e$)

Application S is a finite set $S \neq \emptyset$

G is a group of permutations of S

$\varphi \in G \quad \varphi : S \to S$ bijective

ie S; $Stab_G(i) = \{\varphi \mid \varphi \in G, \varphi(i) = i\}$.

notice that $Stab_G(i)$ is a subgroup of G.

$\begin{matrix} 1&2&3&4 \\ 3&2&1&4 \end{matrix}$

$Orb_G(i) = \{\varphi(i) \mid \varphi \in G\}$.

Theorem $|Orb_G(i)| \cdot |Stab_G(i)| = |G|$.

$S = \{1,2,3,4,5,6\}$

$Orb_G(1) = \{1,2,3,4,5,6\} \to 6$

$Stab_G(1) = \{\begin{matrix}1&2&3&4&5&6 \\ 1&5&2&3&4&6 \\ 1&4&5&2&3&6\end{matrix} \to 4\} \Rightarrow 4 \cdot 6 = 24$

1 3 4 5 2 6 }