Reading Questions 8

page 48: Definition 2.39

page 49: Example 2.41

1. The order of an element in a group G is the number elements in the group. F
2. Let G be a cyclic group such that a is a generator for G. Then the order of G is the order of a. T
3. What is the order of the identity element in a group? 1

Section 2.3 Cyclic Groups and the Order of an Element (Part 2)

Order of an Element

P 1. Find the order of (123) in S_4.

P 2. Find the order of $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ in $\mathrm{GL}(2, Z_2)$.

P 3. Let G be a group such that $a, b \in G$. Prove that $o(aba^{-1}) = o(b)$.

P 4. Let G be a group such that $a, b \in G$. Prove that $o(ba) = o(ab)$.

Recall:

Thm: Let G be a group of finite order such that $a \in G$. Then there exists a smallest positive integer k such that $a^k = e$ and $|\langle a \rangle| = k$.

Def: $k :=$ order of a

denoted by $o(a) = |\langle a \rangle| = k$

Ex: The order of 2 in $(\mathbb{Z}_5, +)$ is 5.

$\langle 2 \rangle = \{ 2^0 = 0,\ 2^1 = 2,\ 2^2 = 2+2 = 4,\ 2^3 = 2+2+2 = 1,\ 2^4 = 2^3 \cdot 2 = 1+2 = 3$

$2^5 = 2^4 \cdot 2 = 3+2 = 5 = 0 \}$
identity

$= \{0, 2, 4, 1, 3\} = \mathbb{Z}_5 \Rightarrow (\mathbb{Z}_5, +)$ is cyclic

Moreover $o(2) = 5$

Ex: The order of 3 in $\mathbb{Z}_6$ is 2.

$\langle 3 \rangle = \{3^0 = 0, 3^1 = 3\}$ $3^2 = 3+3 = 6 \equiv 0$

$= \{0, 3\}$

$\langle 2 \rangle = \{0, 2, 4\} = \langle 4 \rangle$ $o(2) = 3$

$\langle 1 \rangle = \langle 5 \rangle = \mathbb{Z}_6$

Prop: Let G be a group such that $a \in G$. Assume $O(a) = m$ and $a^k = e$ where m and k are positive integers. Then m divides k.

pf: We know m is the smallest positive integer in which $a^m = e$. ($O(a) = m$). Hence $m \leq k$.

Now $k = qm + r$ where $r, q \in \mathbb{Z}$ and $0 \leq r < m$ by DA.

So $a^k = a^{qm+r} = a^{qm} \cdot a^r = (a^m)^q \cdot a^r = (e)^q \cdot a^r = e \cdot a^r = a^r$.

Since $a^k = e$ it follows that $a^r = e$. Also $0 \leq r < m$ and m is the smallest positive integer in which $a^m = e$.

Hence $r = 0 \Rightarrow k = qm \Rightarrow m$ divides k.

Thm: Let G be a group such that $a \in G$. Then

$$o(a) = o(a^{-1}).$$

check

$\langle a \rangle = \langle a^{-1} \rangle$

pf: WTS $a^k = e \Rightarrow$ (1) $(a^{-1})^k = e$

(2) k is the smallest

$$(a^{-1})^k = a^{(-1)(k)} = a^{(k)(-1)} = (a^k)^{-1} = (e)^{-1} = e$$

Let $o(a^{-1}) = l$. Then $l \leq k$.

Now $(a^{-1})^l = e \Rightarrow a^{-l} = e$

$\Rightarrow (a^l)^{-1} = e$

$\Rightarrow (a^l)^{-1} \cdot a^l = e \cdot a^l$

$\Rightarrow e = a^l$.

Hence $l \geq o(a) = k \Rightarrow l = k$.

$\therefore o(a) = o(a^{-1})$.