Reading Questions 7

page 45: Definition 2.27

page 45: Example 2.28

1. Let a be an element of a group. Then $a^{-2} = a^{-1}a^{-1}$. T
2. Let a be an element of a group. Then $a^0 = 1$. F
3. Let $a = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}$ be an element in $\mathrm{GL}(2, Z_3)$. Compute a^2. $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$ $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$

Section 2.3 Cyclic Groups and the Order of an Element (Part 1)

Cyclic Groups

P 1. Let $G = (Z_5)^\times$ and $a = 2$. Compute a^3a^2.

P 2. Let $G = Z_5$ and $a = 2$. Compute a^3a^2.

P 3. Let G be a group such that $a \in G$. Let $m \in \mathbb{Z}$ and $n = 0$. Prove $a^m a^n = a^{m+n}$.

P 4. Let G be a group such that $a \in G$. Let $m, n \in \mathbb{Z}$. Prove that $\underline{(a^n)^{-1} = a^{-n}}$.

P 5. Show that $(Z_7)^\times$ is cyclic by finding a generator for the group.

P 6. Determine if S_4 is cyclic.

Def: Let $a \in (G, \cdot)$. Then $a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{-times}}$

lem: Let G be a group such that $a \in G$. Let $m, n \in \mathbb{Z}$.

Then

(1) $a^m a^n = a^{m+n}$

(2) $(a^n)^{-1} = a^{-n}$

(3) $(a^m)^n = a^{mn}$.

pf: (1) proof by cases.

$(m, n > 0)$

$$a^m a^n = \underbrace{\underbrace{a \cdot \cdots \cdot a}_{m\text{-times}} \cdot \underbrace{a \cdot \cdots \cdot a}_{n\text{-times}}}_{m+n\text{ - times}}$$

$$= a^{m+n}$$

$(m, n < 0)$

$$a^m a^n = a^{-1 \cdot |m|} \; a^{-1 \cdot |n|}$$

$$= \underbrace{\underbrace{a^{-1} \cdot \cdots a^{-1}}_{|m|\text{-times}} \; \underbrace{a^{-1} \cdot \cdots \cdot a^{-1}}_{|n|\text{-times}}}_{|m|+|n|\text{ - times}}$$

$$= (a^{-1})^{|m|+|n|} \qquad (\text{by } 3)$$

$$= a^{-|m|-|n|}$$

$$= a^{m+n}$$

$(m < 0, \; n > 0)$

Assume $|m| > n$

$$a^m a^n = a^{-1 \cdot |m|} \; a^n$$

$$= \underbrace{a^{-1} \cdot \cdots a^{-1}}_{|m|\text{-times}} \; \underbrace{a \cdots a}_{n\text{-times}}$$

$$= \underbrace{a^{-1} \cdots a^{-1}}_{|m|-n} \; \underbrace{e \cdots e}_{n\text{-times}}$$

$$= (a^{-1})^{|m|-n} = a^{-|m|+n}$$

$$= a^{m+n}$$

$(n = 0)$ Try

Thm: Let $(G, \cdot)$ be a group such that $a \in G$.

Let $H = \{ a^k : k \in \mathbb{Z} \} = \{ \dots, a^{-2}, a^{-1}, a^0, a^1, a^2, \dots \}$.

Then $(H, \cdot)$ is an abelian group.

pf: Let $a \in G$ and $k, l \in \mathbb{Z}$.

(closure) Then $a^k a^l = a^{k+l}$ ← by previous lem $k+l \in \mathbb{Z}$

$\in H$.

(associativity) follows from G

(identity) $\underline{a^k \cdot a^0} = a^{k+0} = \underline{a^k} = a^{0+k} = \underline{a^0 \cdot a^k}$

a^0 - identity

(inverse) $a^k a^{-k} = a^{k-k} = a^0 = e$

similarly $a^{-k} a^k = e$

(commutivity) $a^k a^l = a^{k+l} = a^{l+k} = a^l a^k$

$\square$

Def: Let $(G, \cdot)$ be a group such that $a \in G$ and

$G = \{ a^k : k \in \mathbb{Z} \}$.

Then G is cyclic (cyclic group) and a is a generator of G. Also $G = \langle a \rangle$.

Ex: $(\mathbb{Z}_3, +)$ is cyclic and 1 is a generator.

$\mathbb{Z}_3 = \langle 1 \rangle$.

$$\mathbb{Z}_3 = \{1^0, 1^1, 1^2\} = \{\overset{0 \cdot 1}{\overset{\shortparallel}{0}}, 1, 1+1\}$$

$$= \{0, 1, 2\} = \langle 1 \rangle$$

$$1^3 = 1+1+1 = 2+1 = 3 \equiv 0$$

Ex: D_{2n} where $n > 4$ is not cyclic since

D_{2n} is not abelian.

Def: $\langle a \rangle := \{a^k : k \in \mathbb{Z}\}$

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 $|\langle a \rangle| = k$.

$$a^{k+1} = a^k a^1$$

$$= e \cdot a = a$$