**3. Certain Elementary Theorems on Groups.**

**Definition(3-1):** Let $(G,\*)$ be a group, the integer powers of $a$, $a\in G$ is defined by:

1. $a^{n}=a\*a\*…\*a$ ($n$-times)
2. $a^{0}=e$
3. $a^{-n}=(a^{-1})^{n}, n\in Z^{+}$
4. $a^{n+1}=a^{n}\*a, n\in Z^{+}$

**Example(3-2):** In $(R,+)$, we have

$$3^{0}=0,$$

$$ 3^{2}=3+3=6, $$

$$ 3^{-3}=(3^{-1})^{3}=\left(-3\right)+\left(-3\right)+\left(-3\right)=-9$$

**Example(3-3):** In $(R,∙)$, we have

$2^{0}=1$,

$2^{3}=2∙2∙2=8$,

$$2^{-4}=(2^{-1})^{4}=(\frac{1}{2})^{4}=\frac{1}{2}∙\frac{1}{2}∙\frac{1}{2}∙\frac{1}{2}=\frac{1}{16}$$

**Example(3-4):** In $(G=\{1,-1,i,-i\},∙)$, we have

$i^{0}=1$,

$i^{2}=i∙i=-1$,

$$i^{-2}=(i^{-1})^{2}=(-i)^{2}=-i∙-i=-1$$

**Theorem(3-5):** Let $(G,\*)$ be a group and $a\in G,m,n\in Z$, then:

1. $a^{n}\*a^{m}=a^{n+m} ∀ n,m\in Z$ (**Homework)**
2. $(a^{n})^{m}=a^{nm} ∀ n,m\in Z^{+} $
3. $a^{-n}=(a^{n})^{-1} ∀ n\in Z^{+}$
4. $(a\*b)^{n}=a^{n}\*b^{n} ∀ n\in Z⟺G$ is an abelian group.

**Proof:** (2) let $P\left(m\right):(a^{n})^{m}=a^{nm}$

if $m=1⟹P\left(1\right):\left(a^{n}\right)^{1}=a^{n}=a^{n∙1}$

$⟹P(1)$ is a true.

Suppose that $P(k)$ is a true with $k\in Z^{+}, k\leq m$

$$⟹\left(a^{n}\right)^{k}=a^{nk}$$

We have to prove that $P(k+1)$ is a true

$$P\left(k+1\right):(a^{n})^{k+1}=a^{n(k+1)}$$

$$(a^{n})^{k+1}=(a^{n})^{k}\*(a^{n})^{1}$$

 $=a^{nk}\*a^{n}$

 $=a^{nk+n}$

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

$⟹P(k+1)$ is a true

By the principle of mathematical indication

$⟹P(m)$ is a true $∀ m\in Z^{+}$.

(3) if $n=1⟹P\left(1\right):\left(a^{-1}\right)^{1}=a^{-1}=(a^{1})^{-1}$

Suppose that if $n=k$ is a true

$$⟹P\left(k\right): \left(a^{-1}\right)^{k}=\left(a^{k}\right)^{-1}$$

We must prove $P(k+1)$ is a true

$$P\left(k+1\right):\left(a^{-1}\right)^{k+1}=\left(a^{k+1}\right)^{-1}$$

$$\left(a^{-1}\right)^{k+1}=\left(a^{-1}\right)^{k}\*\left(a^{-1}\right)^{1}$$

 $=\left(a^{k}\right)^{-1}\*\left(a^{1}\right)^{-1}$

 $=\left(a^{k+1}\right)^{-1}$

$⟹P(k+1)$ is a true

By the principle of mathematical indication

$⟹P(n)$ is a true $∀ n\in Z^{+}$.

(4) $\left(⟹\right) $if $n=2⟹\left(a\*b\right)^{2}=a^{2}\*b^{2}$

$$\left(a\*b\right)\*\left(a\*b\right)=a\*a\*b\*b$$

$$a\*\left(b\*a\right)\*b=a\*\left(a\*b\right)\*b$$

$$\left(b\*a\right)\*b=\left(a\*b\right)\*b$$

$$b\*a=a\*b$$

$⟹G$ is an abelian group

$(⟸)$ let $G$ be an abelian group and $P\left(n\right):(a\*b)^{n}=a^{n}\*b^{n}$

If $n=1⟹(a\*b)^{1}=a^{1}\*b^{1}$ is a true

Suppose that $P(k)$ is a true with $k\in Z^{+}, k\leq m$

$$\ni P\left(k\right):(a\*b)^{k}=a^{k}\*b^{k}$$

We must prove $P(k+1)$ is a true

$$P\left(k+1\right):(a\*b)^{k+1}=(a\*b)^{k}\*(a\*b)^{1}$$

 $=a^{k}\*b^{k}\*a^{1}\*b^{1}$

 $=(a^{k}\*b^{k})\*(b\*a)$

 $=a^{k}\*(b^{k}\*b)\*a$

 $=a^{k}\*a\*b^{k+1}$

 $=a^{k+1}\*b^{k+1}$

$⟹P(k+1)$ is a true $∀ n\in Z^{+}$.

**Definition(3-6):** (The order of a Group)

The number of elements of a group $G$ is called the order of $G$ and it is denoted by $\left|G\right|$ or $O(G)$. The group $G$ is called a finite if $\left|G\right|<\infty $ and an infinite group otherwise.

**Definition(3-7):** (The order of an element)

The order of an element $a$, $a\in G$ is the least positive integer $n$ such that $a^{n}=e$ where $e$ is the identity element of $G$. We denoted to order$ a$ by $\left|a\right|$ or $O(a)$. This means $\left|a\right|=n$ if $a^{n}=e, n\in Z^{+}$.

**Example(3-8):** $(Z,+)$ is an infinite group.

**Example(3-9):** The trivial group $G=\{0\}$, $\left|G\right|=1$, $G$ is the only group of order one.

**Example(3-10):** Find the order of $G$ and the order of their elements, where$ G=\{1,-1,i,-i\}$.

**Solution:** $\left|G\right|=4$and $\left|1\right|=1$, $\left|-1\right|=2$

$\left|i\right|=4$ and $\left|-i\right|=4$.

**Exercises:**

* Find the order of $(G=\left\{1,-1\right\},∙)$ and the order of their elements**.**
* Find the order of $(C\_{6},∙)$ and the order of their elements**.**
* Find the order of $(S\_{3},∘)$ and the order of their elements.
* Let $G=\{a,b,c,d\}$ be a set. Define a binary operation $\*$ on $G$ by the following table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| $$\*$$ | $$a$$ | $$b$$ | $$c$$ | $$d$$ |
| $$a$$ | $$a$$ | $$b$$ | $$c$$ | $$d$$ |
| $$b$$ | $$b$$ | $$c$$ | $$d$$ | $$a$$ |
| $$c$$ | $$c$$ | $$d$$ | $$a$$ | $$b$$ |
| $$d$$ | $$d$$ | $$a$$ | $$b$$ | $$c$$ |

Find the order of $G$ and their elements