Correction of error in result 7 of previous page (page-12) :

Upto (So, $p \circ q \in H$) is correct. After that cross out or delete the next portion and write this :

Let $p \in H \Rightarrow p \circ g = g \circ p$ for all $g \in G$

Hence $p^{-1} \circ (p \circ g) \circ p^{-1} = p^{-1} \circ (g \circ p) \circ p^{-1}$

or, $(p^{-1} \circ p) \circ (g \circ p^{-1}) = (p^{-1} \circ g) \circ (p \circ p^{-1})$

or, $e \circ (g \circ p^{-1}) = (p^{-1} \circ g) \circ e$ (e is the identity element in G)

or, $g \circ p^{-1} = p^{-1} \circ g$ for all $g \in G$.

So, $p^{-1} \in H$

So, $p \in H \Rightarrow p^{-1} \in H$

Hence H is a subgroup of G.

Cyclic subgroups generated by an element :

Let (G, o) be a group a be an element in G. Let H be the subset of G defined by $H = \{a^n : n \in \mathbb{Z}\}$

[Here we define $a^0 = e$, e is the identity element in G.

and $a^n = \overbrace{a \circ a \circ \cdots \circ a}^{n \text{ times}}$ when n is a positive integer

and if $n = -m$ where m is a positive integer

then $a^n = \overbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}^{m \text{ times}}$]

So Here H is the subset of G containing all integral powers of a

H is non-empty as $a \in H$

Let $p, q \in H$. Then $p = a^r$, $q = a^s$ for some integers r and s

Now $p \circ q = a^{r+s} \in H$, since $r+s$ is an integer

Also $p^{-1} = a^{-r} \in H$, since $-r$ is an integer

So, $p, q \in H \Rightarrow p \circ q \in H$

and $p \in H \Rightarrow p^{-1} \in H$

So H is a subgroup of G. This subgroup is denoted by $\langle a \rangle$. $\langle a \rangle$ is also a commutative subgroup of G. Let $p, q \in \langle a \rangle \Rightarrow p = a^r$, $q = a^s$, r, s are integers

Now $p \circ q = a^r \circ a^s = a^{r+s}$ and $q \circ p = a^s \circ a^r = a^{s+r}$

Since r and s are integer, $r+s = s+r$. So, $p \circ q = q \circ p$

So $\langle a \rangle$ is a commutative subgroup of G.

Example: Let $G = \{1, -1, i, -i\}$. Then G is a group with respect to complex multiplication.

Here $\langle 1 \rangle = \{1\}$

$\langle i \rangle = \{1, -1, i, -i\} = G$ as $i^2 = -1$, $i^3 = -i$, $i^4 = 1$

$\langle -1 \rangle = \{1, -1\}$

$\langle -i \rangle = \{1, -1, i, -i\} = G$.

Ring: Definition: A non-empty set R is to form a ring with respect to two binary operations denoted by '+' and '.' defined on it, if the following conditions are satisfied:

(1) $(R, +)$ is a commutative group,

(2) $(R, \cdot)$ is a semigroup and

(3) for any three elements $a, b, c \in R$,

$a \cdot (b+c) = a \cdot b + a \cdot c$ (left distributive law)

and $(b+c) \cdot a = b \cdot a + c \cdot a$ (right distributive law)

Therefore a non-empty set R, with respect to two binary operations denoted by '+' and '.' defined on it, is a ring if

(i) $a+b \in R$ for all $a, b \in R$,

(ii) $a+(b+c) = (a+b)+c$ for all a, b, c in R,

(iii) there exists an element, denoted by 0, in R such that $a+0 = 0+a = a$ for all $a \in R$,

(iv) for each element a in R there exists an element, denoted by $-a$ in R such that $a+(-a) = (-a)+a = 0$,

(v) $a+b = b+a$ for all a, b in R,

(vi) $a \cdot b \in R$ for all a, b in R,

(vii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in R,

(viii) $a \cdot (b+c) = a \cdot b + a \cdot c$ and $(b+c) \cdot a = b \cdot a + c \cdot a$ for all a, b, c in R.

The ring R is denoted by $(R, +, \cdot)$ or R when no confusion arises regarding the underlying binary operations.

Note: Condition (i) to (v) gives $(R, +)$ a commutative group and (vi) and (vii) gives $(R, \cdot)$ is a semigroup and (viii) gives the two distributive laws.

R is said to be a commutative ring if $a.b = b.a$ for all a, b in R. In this case, the two distributive Laws state the same Thing and it is said to be the distributive law.

The additive identity element in R is called the zero element in R. An element e in R is said to be a multiplicative identity in R if $e.a = a.e = a$ for all a in R. R may or may not contain a multiplicative identity. If however, such an element exists in R, it is unique and it is said to be the unity in R and R is called a ring with unity. The unity is denoted by 1.

Examples 1. $(\mathbb{Z}, +, .)$ is a commutative ring with unity

2. $(\mathbb{R}, +, .)$ is a commutative ring with unity

3. $(\mathbb{Q}, +, .)$ is a commutative ring with unity

4. $(\mathbb{C}, +, .)$ is a commutative ring with unity

Note 1. Here $\mathbb{Z}$ is the set of all integers, $\mathbb{Q}$ is the set of all Rational numbers, $\mathbb{R}$ is the set of all Real numbers and $\mathbb{C}$ is the set of all Complex numbers.

2. '+' and '.' in 1 to 3 is usual addition and usual multiplication in Real numbers and '+' and '.' in 4 is complex number addition and multiplication.

5. $(2\mathbb{Z}, +, .)$ is a commutative ring. It is a ring without unity.

6. Let $M_2(\mathbb{R})$ be the set of all 2×2 real matrices. Let '+' be the matrix addition and '.' be the matrix multiplication. Then $(M_2(\mathbb{R}), +, .)$ is a ring with unity. $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the unity in the ring. This is a non-commutative ring.

Theorem 1: In a ring $(R, +, .)$

(i) $a.0 = 0.a = 0$ for all $a \in R$, 0 being the zero element in R,

(ii) $a.(-b) = (-a).b = -(a.b)$ for all $a, b \in R$

(iii) $(-a).(-b) = a.b$ for all $a, b \in R$.

Proof: (i) we have $a.0 = a.(0+0)$

$= a.0 + a.0$ (left distributive law)

Now $-(a\cdot 0) \in R$. Adding $-(a\cdot 0)$ to both sides we have

$-(a\cdot 0) + a\cdot 0 = -(a\cdot 0) + (a\cdot 0 + a\cdot 0)$

or, $0 = (-(a\cdot 0) + a\cdot 0) + a\cdot 0$ (additin is associative)

or, $0 = 0 + a\cdot 0$

or, $0 = a\cdot 0$

Likewise, $0\cdot a = (0+0)\cdot a$

$= 0\cdot a + 0\cdot a$ (right distributive Law)

$-(0\cdot a) \in R$. Adding $-(0\cdot a)$ to both sides and proceding as before we have $0 = 0\cdot a$

So, combining we have $a\cdot 0 = 0\cdot a = 0$ for all $a \in R$.

(ii) we have $(b + (-b)) = 0$

So, $a\cdot(b + (-b)) = a\cdot 0 = 0$ by (i)

or, $a\cdot b + a\cdot(-b) = 0$ (left distributive law)

$-(a\cdot b) \in R$. Adding $-(a\cdot b)$ to both sides we have

$-(a\cdot b) + (a\cdot b + a\cdot(-b)) = -(a\cdot b) + 0$

or, $(-(a\cdot b) + a\cdot b) + a\cdot(-b) = -(a\cdot b)$ (+ is associative)

or, $0 + a\cdot(-b) = -(a\cdot b)$

or, $a\cdot(-b) = -(a\cdot b)$

Again $a + (-a) = 0$

So, $(a + (-a))\cdot b = 0\cdot b = 0$ by (i)

or, $a\cdot b + (-a)\cdot b = 0$ (right distributive law)

$-(a\cdot b) \in R$. Adding $-(a\cdot b)$ to both sides and proceding as before we have $(-a)\cdot b = -(a\cdot b)$

Combining, we have $a\cdot(-b) = (-a)\cdot b = -(a\cdot b)$

(iii) Let $p = -a$ Then $p \in R$

$(-a)\cdot(-b) = p\cdot(-b)$

$= -(p\cdot b)$ by (ii)

$= -((-a)\cdot b)$

$= -(-(a\cdot b))$ by (ii)

$= a\cdot b$ (As $-(-a) = a$)

This completes the proof.