Cyclic group A group $(G,\circ)$ is said to be cyclic group if there exists an element $a \in G$ s.t.

$$G = \{a^n \mid n \in \mathbb{Z}\} \text{ i.e. } G = \langle a \rangle_\circ .$$

- a is said to be a generator of the cyclic group.
- Additive notation

$$G = \{na \mid n \in \mathbb{Z}\} = \langle a \rangle .$$

Examples

1. $(\mathbb{Z},+)$ cyclic, $-1, 1$ are generators.
2. $(\mathbb{Z}_4,+)$ cyclic, $[1],[3]$ generators.
3. $S = \{1, i, -1, -i\}$ cyclic, $i, -i$ generators
4. $S = \{1, -1\}$ cyclic generated by -1.
5. Klein's 4-group V not cyclic.
   - elements of V are e, a, b, c
   - none of $\langle e \rangle, \langle a \rangle, \langle b \rangle, \langle c \rangle$ equals V.

Theorem If a generates a cyclic group $(G,\circ)$, then $\bar{a}^1$ is also a generator of $(G,\circ)$.

proof Let $p \in G = \{a^n \mid n \in \mathbb{Z}\}$ & let $H = \{(\bar{a}^1)^n \mid n \in \mathbb{Z}\}$

$p \in G \Rightarrow p = a^r$ for some $r \in \mathbb{Z}$
$\Rightarrow p = (\bar{a}^1)^{-r}$, $-r \in \mathbb{Z}$.
$\Rightarrow p \in H \quad \therefore G \subseteq H$

$p \in H \Rightarrow p = (\bar{a}^1)^s$ for some $s \in \mathbb{Z}$
$= \bar{a}^s$, $-s \in \mathbb{Z}$
$\Rightarrow p \in G$
$\Rightarrow \therefore H \subseteq G$.

Theorem Every cyclic group is abelian.

Note. Every abelian group is not cyclic.

e.g. Klein's 4-group
abelian, but not cyclic.

$(G,\circ)$, $G = \langle a^n \rangle$.
$p, q \in G \Rightarrow p = a^r, q = a^s$
$r, s \in z$
$\Rightarrow p \circ q = a^{r+s} = a^{s+r} = q \circ p = a$

Example: The symmetric group S_3 is not abelian. So not cyclic.

Example: The dihedral group D_4 is not abelian. So not cyclic.

Theorem $(G,\circ)$ → finite cyclic group generated by a.
i.e. $G = \langle a \rangle$
Then $o(G) = o(a)$ & conversely.

(proof skip)

proof, let $o(a) = n$.
$\therefore a, a^2, \ldots, a^n (= e) \in G$.
all distinct
$\therefore \{a, a^2, \ldots, a^n\} \subset G$. — ①
let $p \in G = \{a^n \mid n \in z\}$
$\therefore p = a^m$ for some $m \in z$
$= a^{nq+r}$ for some r, $0 \le r < n$ (by division algm)
$= (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$, $0 \le r < n$
$\therefore p \in \{a, a^2, \ldots, a^n (= e)\}$
$\therefore G \subseteq \{a, a^2, \ldots, a^n\}$ — ②

Now $o(a) \mid o(a)$
$\Rightarrow k \mid n$ where $o(a) = k$
$\therefore n = kq$

• Conversely, let $O(G) = n$
Then since G is of finite order, $o(a) = k$ = finite
for $a \in G$, $a, a^2, \ldots, a^{k-1}, a^k (= e)$
$\therefore a, a^2, \ldots, a^k$ are all distinct elements of G
$\therefore k \le n$. But if $k < n$, then by previous case $O(a) = k (< n)$
$\therefore k = n = o(a) = o(a)$

① , ② $\Rightarrow G = \{a, a^2, \ldots, a^n\}$

Corollary: if $G = \langle a \rangle$ & $o(a) = n$, then $G = \{a, a^2, \ldots, a^n = e\}$

Theorem: (skip proof) Let $(G,\circ)$ be a cyclic group generated by a. Then G is infinite if and only if $o(a)$ is infinite.

Proof

- Let $o(a)$ be infinite
  $\Rightarrow \{a, a^2, \dots\}$ is an infinite set of distinct elements
  (i.e. if $a^r = a^s$ then $a^{r-s} = e \Rightarrow o(a)$ is finite $(\rightarrow\leftarrow)$.)
  But $\{a, a^2, \dots\} \subset G$
  $\Rightarrow o(G)$ is also infinite.
- Conversely, let $o(G)$ be infinite.
  if $o(a)$ is finite, then by the previous theorem,
  $o(G)$ is finite $(\rightarrow\leftarrow)$.

Hence $o(a)$ is infinite.

Theorem (skip proof) A finite group $(G,\circ)$ is cyclic of order n iff there is an element $b \in G$ s.t. $o(b) = n$.

Proof

- Let $(G,\circ)$ be a cyclic group of order n
  Then $G = \langle a \rangle$, $o(a) = n$
  $\Rightarrow o(G) = n$ (by previous theorem)
  $\therefore \exists\ b = a \in G$ s.t. $o(b) = n$.
- Conversely, let $\exists$ an element $b \in G$ s.t. $o(b) = n$ and $o(G) = n$.

As $o(b) = n$, $b, b^2, \dots, b^n (= e)$ are distinct elements of G
Also $o(G) = n \Rightarrow G = \{b, b^2, \dots, b^n\}$
$\therefore G \subset \{b^n \mid n \in \mathbb{Z}\}$ — (1)
Now $b \in G \Rightarrow b^0, b, b^{-1}, b^2, b^{-2}, \dots$ all $\in G$
$\therefore \{b^n \mid n \in \mathbb{Z}\} \subset G$ — (2)
(1), (2) $\Rightarrow G = \{b^n \mid n \in \mathbb{Z}\}$
$\Rightarrow G$ is cyclic group generated by b.

Examples:

1. $(\mathbb{Z}_n, +)$ cyclic generated by $[1]$ of order n.
   $[1] \in \mathbb{Z}_n$ has order n as $n[1] = [0]$
2. $(S, \cdot)$, $S = \{1, -1, i, -i\}$ is finite group of order 4
   $o(i) = 4$, so S is generated by i
3. $S_3 \to$ not cyclic as $o(S_3) = 6$, but no element in S_3 with order 6
4. $V \to$ not cyclic as $o(V) = 4$, but no element in V with order 4
5. $D_4 \to$ not cyclic as $o(D_4) = 8$, but no element of order 8 in D_4.

Theorem $(G, \circ)$ a finite cyclic gr. of order n, generated by a

Then a^r, r some +ve integer
↳ is also a generator of G iff $r < n$ & coprime to n

proof

$o(G) = n, a^n = e \Rightarrow G = \{a, a^2, \cdots, a^n (= e)\}$

- Let a^r be a generator of G. Then $a^r \in G$
  $\therefore 0 \le r < n$.
  Then $a = (a^r)^k$ for some integer k.
  $\Rightarrow a^{rk-1} = e \Rightarrow n \mid rk-1$ as $o(a) = n$.
  $\therefore rk - 1 = ns$ for some integer s
  $\Rightarrow rk + ns = 1 \Rightarrow \gcd(r, n) = 1$.
  $\therefore r < n$ & coprime to n.

Conversely, let $r < n$ and coprime to n

Then $o(a^r) = \frac{o(a)}{\gcd(r, o(a))} = \frac{n}{\gcd(r,n)} = n = o(G)$

$\Rightarrow a^r$ generates G.

Corollary The total no. of generators of a finite cyclic group of order n is $\phi(n)$.

$\phi(1) = 1$

$n \geq 2$, $\phi(n)$ = # of +ve integer $< n$ & coprime to n

Euler's totient fn

Example:

1. # of generators of the cyclic gr. $(S, \cdot)$ where $S = \{1, -1, i, -i\}$ is $\phi(4) = \phi(2^2) = 2^2\left(1 - \frac{1}{2}\right) = 2$

2. # of generators of the cyclic gr. of a prime order p is $\phi(p) = p - 1$.
   $\therefore$ each non-identity element of the gr. is a generator.

3. # of generators of the cyclic gr. $(\mathbb{Z}_2, +)$ is $\phi(2) = 1$.

Theorem Every subgroup of a cyclic group is cyclic.

Proof Let $(G, \circ)$ be a cyclic group generated by a and $(H, \circ)$ be a subgroup of G.

Every subgp. of an abelian gr. is abelian.

If $H = G$, then nothing to prove

We conside two cases.

Case I $H = \{e\}$.

Since $e^n = e \ \forall n \in \mathbb{Z}$, $H = \{e^n \mid n \in \mathbb{Z}\}$

$\Rightarrow H$ is the cyclic group generated by e

Case 2 Let H be a proper subset of G other than the trivial subgroup $\{e\}$.

Then $\exists$ an element $x \in H$ s.t. $x \neq e$

$\therefore x \in G$, $x = a^k$ for some integer $k \neq 0$.

As H is a subgroup of G, $x^{-1} \in H$

$\Rightarrow \bar{a}^k \in H$.

$\therefore a^k, \bar{a}^k$ both $\in H$ for some integer $k \neq 0$.

Therefore, there are some +ve integral powers of a in H.

Let m be the least +ve integer s.t. $a^m \in H$.
(by well ordering principle of the set of natural nos.)

Let $h \in H$

Then $h = a^p$ for some integer p as $h \in G = \langle a \rangle$ $(p \geq m)$

By division algm, $p = qm + r$, $0 \leq r < m$,
q, r unique +ve integers

As H is a subgroup, $a^m \in H \Rightarrow \bar{a}^{mq} \in H$

$a^p \in H$, $\bar{a}^{mq} \in H \Rightarrow a^{p-mq} \in H$

$\Rightarrow a^r \in H$

But $0 \leq r < m$ & $a^r \in H$ are both satisfied only if $r = 0$ because, otherwise m fails to be the smallest +ve integral power of a in H.

$\therefore p = qm \Rightarrow h = (a^m)^q$, q is an integer $\Rightarrow H = \langle a^m \rangle$.

Note 1 If a subgroup H of a finite group $G = \langle a \rangle$ of order n is generated by a^m, then $m \mid n$.

if $n = mq + r$, $0 \le r < m$, then $e = a^n = a^{mq} \circ a^r \Rightarrow a^r = a^{-mq} \in H$ $(\rightarrow\leftarrow)$ the minimality of m

Note 2 For a cyclic group G, the cyclic subgroups generated by different elements of G are the only subgroups of G.

$\rightarrow$ $H = \langle a^m \rangle$, m the least +ve int. s.t. $a^m \in H$

Theorem A cyclic group of prime order has no non-trivial subgroups.

proof. $(G, \circ)$ cyclic gr., $o(G) = p$, a prime.

$(H, \circ)$ a subgr. of $(G, \circ)$.

Then $(H, \circ)$ cyclic and $H = \langle a^m \rangle$, m being the least +ve integer s.t. $a^m \in H$.

$\because o(G) = p$, ~~and~~ $a^p = e \in H$

As $H = \langle a^m \rangle$ and $a^p \in H$, we must have $p = mk$, for some +ve integer k.

i.e. $m \mid p$

As p is prime, $m = 1$ or p.

$\Downarrow$ $\qquad$ $\Downarrow$

$H = G \qquad H = \{e\}$.

$\therefore (H, \circ)$ is either the trivial subgr. $\{e\}$ or the improper subgr. G.

Theorem Every non-trivial subgr. of an infinite cyclic gr. is infinite.

Proof $(G,\circ)$ infinite cyclic gr.

$G = \langle a \rangle$.

$(H,\circ)$ a non-trivial subgr. of $(G,\circ)$.

Then H is cyclic & $H = \langle a^m \rangle$, m is the least +ve integer s.t. $a^m \in H$

$o(a)$ infinite $\Rightarrow o(a)$ infinite $\Rightarrow o(a^m)$ infinite $\Rightarrow H$ infinite.

Theorem A cyclic gr. of finite order n has one and only one subgr. of order d for every +ve divisor d of n.

Proof $G = \langle a \rangle$ cyclic gr. of finite order n. $o(a) = o(G) = n$

Then $G = \{a, a^2, \cdots, a^n (= e)\}$.

- $\{e\}$ is the only subgr. of G of order 1
- G is the only subgr of G of order n.

$\therefore$ The theorem holds for the divisors 1 & n.

Let $1 < d < n$ be a +ve divisor of n i.e. $n = dm$ for some +ve int. m.

Now $a^m \in G$ and $o(a^m) = \dfrac{o(a)}{\gcd(m, o(a))} = \dfrac{n}{\gcd(m,n)} = \dfrac{n}{m} = d$ (as $m < n$)

$\therefore$ The cyclic gr. $H = \langle a^m \rangle$ is of order d.

Uniqueness Let K be another subgr. of G s.t. $o(K) = d$.

G cyclic $\Rightarrow K$ cyclic

Let b be the least +ve integer s.t. $a^b \in K$.

Then $K = \langle a^b \rangle$ and $(a^b)^d = e$.

By division algm, $p = mq + r$, $0 \le r < m \le p$, q, r unique

$\therefore pd = mqd + rd$ (assuming $p > m$; the case $m > p$ is similar)

$\Rightarrow a^{pd} = a^{mqd+rd}$

$\Rightarrow e = a^{rd}$ $(\because a^{md} = e$ as $H = \langle a^m \rangle$ & $o(H) = d)$.

$\Rightarrow r = 0$. as p is the least +ve int. s.t. $(a^p)^d = e$ & $r < p$

$\therefore p = mq$.

$\therefore \langle a^p \rangle \subseteq \langle a^m \rangle$

i.e. $K \subseteq H$.

$\because o(K) = o(H) \Rightarrow K = H$.

This proves that H is unique.

$Z_{13}^* = Z_{13} - \{0\}$ → mul. gp., cyclic → 12 elements

$Z_m - \{0\}$ → mul. gp. when m is prime → $m-1$ elements. $a^{m-1} = e$ is $\langle a \rangle$

$12 = 3 \times 2 \times 2$ → subgps of order 3, 2, 4, 6

Example: find all subgps. of the gp. $(Z, +)$.

Soln: $(Z, +)$ cyclic gp. generated by 1

$\therefore$ every subgp. of $(Z, +)$ is cyclic.

All subgps. of $(Z, +)$ are precisely $(mZ, +)$, when m is a non-negative integer ($(mZ, +)$, $(-mZ, +)$ identical)

Example: $(Q, +)$ non-cyclic.

Soln: if $(Q, +)$ is cyclic, let $Q = \langle a \rangle = \{ma \mid m \in Z\}$

$\frac{1}{2}a \in Q$ but $\frac{1}{2}a \notin \{ma \mid m \in Z\} \Rightarrow Q$ is not cyclic.

Example: $(R, +)$ non-cyclic o.w. if it is cyclic, its subgp. $(Q, +)$ will also be cyclic ($\rightarrow\leftarrow$)

n +ve integer.

Example: S = the set of n-th roots of unity

Show that $(S, \cdot)$ is cyclic.

Find all possible generators.

Solⁿ. $S = \{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$, $\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

S is a finite gr. w.r.to multiplication and $o(S) = n$.

n is the least +ve integer s.t.

$\alpha^n = 1$

$\Rightarrow o(\alpha) = n$

$x^n = 1 = \cos 0 + i\sin 0$

$x = \cos\frac{(0+2k\pi)}{n} + i\sin\frac{(0+2k\pi)}{n}$

$k = 0, 1, \cdots, n-1$

Thus S is a finite gr. containing n elements and $\alpha \in S$ with $o(\alpha) = n$.

$\Rightarrow (S, \cdot)$ is cyclic gr. generated by α.

generators α^r, where $\gcd(r, n) = 1$, $r \leq n$

Note. if $r < n$ and r is coprime to n, then a^r is a special root of $x^n - 1 = 0$.

So the possible generators of the cyclic gr. $(S, \cdot)$ are the special roots of the equn. $x^n - 1 = 0$.

Note. for each +ve integer n, there exists a cyclic gr. of order n.

Example: Let G be an abelian gr. of order 6 containing an element of order 3.
Prove that G is a cyclic gr.

Soln. $a \in G$, $o(a) = 3$.

As G is a finite gr. of even order, it must have an element, say, b of order 2.

$\therefore b \in G$ & $o(b) = 2$

$\because ab = ba$ & $o(a), o(b)$ are coprime,

$o(ab) = 6$.

$\therefore o(G) = 6$. & there exists an element of order 6 in G,

G is cyclic.

Example: Let G be an infinite cyclic gr. generated by a.
Prove that a and $\bar{a}^1$ are the only generators of the group.

Soln. G infinite cyclic gr.,

$\Rightarrow G = \langle a \rangle$.

Let b be a ~~generated by G~~ generator of G

$b \in G = \langle a \rangle \Rightarrow b = a^m$ for some integer m

$a \in G = \langle b \rangle \Rightarrow a = b^p$ for some integer p.

$\therefore a = b^p = a^{mp} \Rightarrow a^{mp-1} = e$, e being the identity element.

As $G = \langle a \rangle$ & $o(a)$ infinite, we get $o(a)$ infinite.

So $a^{mp-1} = e \Rightarrow mp = 1 \Rightarrow \begin{matrix} m=1, p=1 \\ \text{or} \\ m=-1, p=-1 \end{matrix} \Rightarrow \begin{matrix} b = a \\ \text{or} \\ b = \bar{a}^1 \end{matrix}$

e.g. $(\mathbb{Z}, +)$ infinite cyclic gr. generated by -1 & 1.
$(m\mathbb{Z}, +) \rightarrow$ infinite cyclic gr. generated by $-m, m$. (m +ve integer)

Example:

1. • (G,o) even order group. Then G contains an odd no. of elements of order 2
• Then $\#\, a \in G$ s.t. $o(a)=2$ is odd.

proof: Let $a \in G$
Then $o(a)=o(\bar{a}^1)$.

• $o(a)<3$ i.e. $o(a)=1$ or 2
$\Downarrow$
$a=\bar{a}^1$.

$\downarrow$ $a=e$, 1 least
$\Downarrow$
$\bar{e}^1=e$.
i.e.
$\bar{a}^1=a$

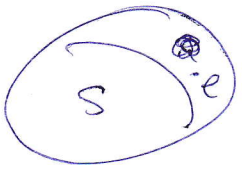
$\downarrow$ $a^2=e$, 2 least
$\Downarrow$
$a\circ a=e$
$\Downarrow$
$\bar{a}^1=a$

• $o(a)\geq 3$.
$\Downarrow$
$a, \bar{a}^1$ distinct elements of G $\rightarrow$ one pair of elements $(a,\bar{a}^1)$.

Now consider the set S of all such pairs $(x,\bar{x}^1)$.

$G-S \neq \phi$ as $o(e)=1$ & so $e \in G-S$

As $o(a)$ is even, $\exists$ even no. of elements in $G-S$ with order <3.



$o(s)$ even, order of each element in $S \geq 3$.

i.e. order 1 & order 2

Only one element e of order 1
$\Rightarrow$ odd no. of elements of order 2.

Note: In particular, G must contain at least one element of order 2.

2. Group $(G, \circ)$

$a, b \in G$ commutes & $o(a), o(b)$ are coprime.

Then $o(a \circ b) = o(a) \circ o(b)$.

Soln. Let $o(a) = m$, $o(b) = n$, $o(a \circ b) = k$.

$a \circ b = b \circ a \Rightarrow$

$\gcd(o(a), o(b)) = 1$

$(a \circ b)^k = (a \circ b) \circ (a \circ b) \circ \cdots \circ (a \circ b)$ (k times)

$= a \circ (b \circ a)(b \circ a) \circ \cdots \circ (b \circ a) b$

$= a \circ (a \circ b)$

Soln. Let $o(a) = m$, $o(b) = n$, $o(a \circ b) = k$.

$\therefore a^m = e$, $b^n = e$, $(a \circ b)^k = e$; $\gcd(m, n) = 1$.

$a \circ b = b \circ a \Rightarrow (a \circ b)^k = a^k \circ b^k$.

$\therefore (a \circ b)^k = e$

$\Rightarrow a^k \circ b^k = e$

$\Rightarrow a^k = b^{-k}$

$\Rightarrow a^{kn} = b^{-nk} = e \Rightarrow m \mid kn$ as $o(a) = m$

$\Rightarrow m \mid k$ as $\gcd(m, n) = 1$

$\Rightarrow a^{mk} = b^{-mk} = e \Rightarrow n \mid mk$ as $o(b) = n$

$\Rightarrow n \mid k$ as $\gcd(m, n) = 1$.

① $\therefore mn \mid k$ Since $\gcd(m, n) = 1$.

Also $(a \circ b)^{mn} = a^{mn} \circ b^{mn}$ as $a \circ b = b \circ a$

$= e \circ e = e$

② $\Rightarrow k \mid mn$ as $o(a \circ b) = k$

① & ② $\Rightarrow k = mn$.

$\therefore o(a \circ b) = o(a) \circ o(b)$.

$(a \circ b)^2 = (a \circ b)(a \circ b) = a \circ (b \circ a) \circ b = a \circ (a \circ b) \circ b = a^2 \circ b^2$

$(a \circ b)^3 = (a^2 \circ b^2)(a \circ b) = (a^2 \circ b^2) \circ (b \circ a) = a^2 \circ (b^3 \circ a) = a^2 \circ a \circ (b^3) = a^3 \circ b^3$.

$k = xm$

$k = yn$

$k^2 = xymn$.

$k = ?k'$ ($m = 3$, $n = 8$)

Comm

3. $(G, *)$ be a group.

$a \in G$ with $o(a) = 30$.

Find $o(a^{18})$.

Soln

$$o(a^{18}) = \frac{o(a)}{\gcd(18, o(a))} = \frac{30}{\gcd(18, 30)} = \frac{30}{6} = 5.$$

4. Find all elements of order 8 in the group $(Z_{24}, +)$.

$Z_{24} = \{[1], [2]$

$Z_{24} = \{[0], [1], [2], \ldots, [23]\}$.

$o([1]) = l$

$\Downarrow$

l is the least +ve integer s.t.

$l[1] = e = [0]$.

$\Downarrow$

$l = 24$.

$\therefore o([1]) = 24$.

Additive gr

order of perm formula

$$o(ma) = \frac{o(a)}{\gcd(m, o(a))}$$

Let $o([m]) = 8$; $0 \le m \le 23$

$\Downarrow$

$$o(m[1]) = 8 = \frac{o([1])}{\gcd(m, o([1]))}$$

i.e. $8 = \frac{24}{\gcd(m, 24)}$ 3

$\therefore \gcd(m, 24) = 3$.

$\Downarrow$

$m = 3, 6, 9, 12, 15, 18, 21$

× ×

i.e. $[3], [9], [15], [21]$.

Conjugate w.r. $(G,\circ)$ be a group & $a \in G$.

An element $b \in G$ is said to be a conjugate of a if $\exists$ an element $x \in G$ s.t. $b = x \circ a \circ x^{-1}$.

Example: Prove that any conjugate of a has the same order as that of a.

Deduce that $o(a \circ b) = o(b \circ a)$ for $a, b \in G$.

Soln: **Case I** $o(a) = m$ (finite). Let b be a conjugate of $a \in G$, $\in G$

$\therefore a^m = e$.

$\therefore \exists\, x \in G$ s.t. $b = x \circ a \circ x^{-1}$.

Now $b^m = (x \circ a \circ x^{-1})^m = (x \circ a \circ x^{-1}) \circ (x \circ a \circ x^{-1}) \circ \dots \circ (x \circ a \circ x^{-1})$

$= x \circ a^m \circ x^{-1}$

$= x \circ x^{-1}$

$= e$.

Claim $o(b) = m$, i.e. no int. $k < m$ s.t. $b^k = 1$.

↳ **proof** Let $k < m$ be a +ve integer s.t. $b^k = e$.

so $(x \circ a \circ x^{-1})^k = e$.

or $x \circ a^k \circ x^{-1} = e$.

$\Rightarrow a^k = x^{-1} \circ x = e$

$(\rightarrow\leftarrow)$ as $k < m$ & $o(a) = m$.

~~... not in the~~

$\therefore o(b) = m$.

Case 2 $o(a)$ ~~∞~~ infinite

Claim $o(b)$ infinite where $b = x \circ a \circ x^{-1}$.

↳ **proof** Let $o(b) = k$ (finite) $\Rightarrow (x \circ a \circ x^{-1})^k = e$.

$\Rightarrow x \circ a^k \circ x^{-1} = e$

$\Rightarrow a^k = e \Rightarrow o(a)$ finite $(\rightarrow\leftarrow)$.

Deduction $a \circ b = a \circ (b \circ a) \circ a^{-1} \Rightarrow o(a \circ b) = o(b \circ a)$

$\Rightarrow$ i.e. $a \circ b$ is a conjugate of $b \circ a$.

Cosets

Left cosets Let $(G,\cdot)$ be a gr. & $(H,\cdot)$ be a subgr. of G.

Let $a \in G$.

for all $h \in H$, $ah \in G$.

The subset $\{ah \mid h \in H\}$ in G is called a left coset of H & is denoted by aH.

- for different elements $b, c, \ldots$ in G, we get left cosets of H as $bH, cH, \ldots$
- for an additive gr. G, a left coset of H is denoted by $a+H$.

Examples.

1. $G = (\mathbb{Z}, +)$, $H = (3\mathbb{Z}, +)$

The left coset $0+H = \{3n \mid n \in \mathbb{Z}\} = H$

The left coset $1+H = \{3n+1 \mid n \in \mathbb{Z}\}$

The left coset $2+H = \{3n+2 \mid n \in \mathbb{Z}\}$

$\exists$ 3 distinct left cosets $\rightarrow$ H, $1+H$ & $2+H$.

2. $G = S_3$, $H = \{\rho_0, \rho_3\}$

The left cosets

$\rho_0 H = \{\rho_0, \rho_3\} = H$

$\rho_1 H = \{\rho_1, \rho_5\}$

$\rho_2 H = \{\rho_2, \rho_4\}$

$\exists$ 3 distinct left cosets $\rightarrow$ H, $\rho_1 H$, $\rho_2 H$.

$\rho_3 H = \{\rho_3, \rho_0\} = H$

$\rho_4 H = \{\rho_2, \rho_4\} = \rho_2 H$

$\rho_5 H = \{\rho_1, \rho_5\} = \rho_1 H$.

3. $G = S_3$, $H = \{\rho_0, \rho_1, \rho_2\}$.

$\rho_0 H = \{\rho_0, \rho_1, \rho_2\} = H$
$\rho_1 H = \{\rho_1, \rho_2, \rho_0\} = H$
$\rho_2 H = \{\rho_2, \rho_0, \rho_1\} = H$

$\rho_3 H = \{\rho_3, \rho_4, \rho_5\}$
$\rho_4 H = \{\rho_4, \rho_5, \rho_3\}$
$\rho_5 H = \{\rho_5, \rho_3, \rho_4\}$.

$\exists$ 2 distinct left cosets of H → H & $\{\rho_3, \rho_4, \rho_5\}$

Theorem Let G be a group and H be a subgroup of G. Let $h \in H$. Then $hH = H$.

proof:

- Let $p \in hH \Rightarrow p = hh_1$ for some $h_1 \in H$
  $\Rightarrow p \in H$ as $h \in H, h_1 \in H$ implies $hh_1 \in H$
  $\therefore hH \subseteq H$ — (1)

- Let $q \in H$.
  As $h \in H, q \in H$, $\exists$ a unique x s.t. $hx = q$
  $\Rightarrow q \in hH$
  $\therefore H \subseteq hH$ — (2)

~~$hH = \{hx : x \in H\}$~~.

(1), (2) $\Rightarrow hH = H$.

[i.e. H itself is a left coset of H]

Theorem $G \to$ group, $H \to$ subgr. of G.
If $a \in G \setminus H$ then $H \cap aH = \emptyset$.

proof:- if $p \in H \cap aH$ then $p = h_1$ for some $h_1 \in H$
& $p = ah_2$ for some $h_2 \in H \Rightarrow ah_2 = h_1 \Rightarrow a = h_1 h_2^{-1}$
$\in H$
$(\rightarrow\leftarrow)$

Theorem Any two left cosets of H in G are either identical or disjoint (They do not overlap)

i.e. $aH = bH$ or $aH \cap bH = \phi$ for $a, b \in G$.

Proof: $aH, bH \to$ two left cosets of H in G, $a, b \in G$.

Let $aH \cap bH \neq \phi$ & $p \in aH \cap bH$.

$\Rightarrow p \in aH, \; p \in bH$

$\Rightarrow p = ah_1 = bh_2$ for some $h_1, h_2 \in H$.

$\Rightarrow \boxed{a = bh_2h_1^{-1}, \; b = ah_1h_2^{-1}}$

Let $x \in aH \Rightarrow x = ah_3$ for some $h_3 \in H$

i.e. $x = bh_2h_1^{-1}h_3 \in bH$

So $aH \subseteq bH$ — (1)

Let $x \in bH \Rightarrow x = bh_4$ for some $h_4 \in H$

i.e. $x = ah_1h_2^{-1}h_4 \in aH$

So $bH \subseteq aH$ — (2)

(1), (2) $\Rightarrow aH = bH$.

$\therefore$ either $aH = bH$ or they are disjoint.

Theorem $G \to$ group, $H \to$ subgr of G; $a, b \in G$.

Then $aH = bH$ iff $a^{-1}b \in H$.

Theorem $G \to$ gr., $H =$ subgr., $a, b \in G$.

Then $b \in aH$ iff $a^{-1}b \in H$.

Define a relation ρ

$G \to$ gr., $H \to$ subgr. of G.

$a \rho b$ iff $a^{-1}b \in H$.

Theorem ρ is an equivalence relation.

Proof $a \rho a$ as $aa^{-1} \in H \ \forall a \in G$.

(Reflexive)

$a \rho b \Rightarrow a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H$ as H is a subgr. of G

$\Rightarrow b^{-1}a \in H$.

$\Rightarrow b \rho a \quad \forall a, b \in G$.

(Symmetric)

$a \rho b, b \rho c \Rightarrow a^{-1}b \in H, b^{-1}c \in H$

$\Rightarrow (a^{-1}b)(b^{-1}c) \in H$

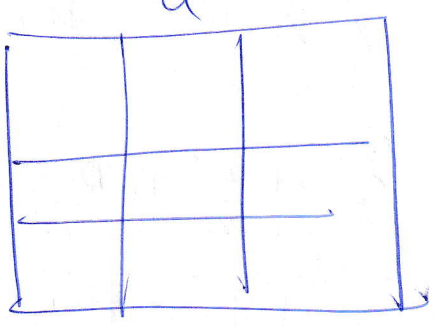
$\Rightarrow a^{-1}c \in H$

$\Rightarrow a \rho c \quad \forall a, b, c \in G$.

(Transitive).

So ρ is an equivalence relation.

Partition of G by the relation ρ



equivalence classes → Disj Cos

$Cl(a) = \{x \in G \mid a \rho x\}$

$= \{x \in G \mid a^{-1}x \in G\}$

$= \{x \in G \mid x \in aH\}$

$= aH$

Theorem Any two left cosets of H in a gr. G have the same cardinality.

ie. $|aH| = |bH| \quad \forall \; a, b \in G$.

proof: $aH, bH \to$ two left cosets of H in G, $a, b \in G$.

Define a mapping $f : aH \to bH$ by

$f(ah) = bh$ for every $h \in H$.

Claim 1 f is injective

proof $ah_1, ah_2 \in aH$

$f(ah_1) = f(ah_2) \Rightarrow bh_1 = bh_2$

$\Rightarrow h_1 = h_2$ by left cancellation law

$\Rightarrow ah_1 = ah_2$

So $ah_1 \neq ah_2 \Rightarrow f(ah_1) \neq f(ah_2)$.

$\Rightarrow f$ is injective.

Claim f is surjective.

proof let $bh \in bH$

Now $f(ah) = bh \Rightarrow ah$ is a preimage of bh.

So f is surjective.

Thus f is a bijection from aH to bH & So $|aH| = |bH|$

Lagrange's Theorem

If $G \to$ gr., $H \to$ Subgr. of G.

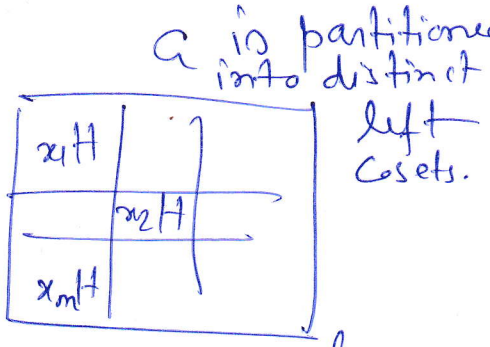
Then $o(H) \mid o(G)$.

proof: If $o(G) = n$

Consider the distinct left cosets of H in G.

$\to x_1H, x_2H, \ldots, x_mH$, $x_1, x_2, \ldots, x_m \in G$.

(As G is finite, # of distinct left cosets of H in G is also finite).



So $G = \bigcup_{i=1}^{m} x_iH$

Also each left coset has the same no. of elements.

H being itself a left coset ($eH = H$), each left coset has $o(H)$ elements.

$$\therefore |G| = m\,|x_iH|$$

$$o(G) = m \cdot o(H).$$

$$\Rightarrow \quad o(H) \mid o(G).$$

Note i) G finite gr. of order n $\not\Rightarrow$ for every +ve divisor d of n, G has a subgr. of order d

ii) G commutative gr. of order n $\Rightarrow$ for every +ve divisor d of n, G has a subgr. of order d

iii) G cyclic gr. of order n $\Rightarrow$ for every +ve divisor d of n, G has

Theorem Every gr. of prime order is cyclic.

proof. $G \to$ gr., $o(G) = p$, prime.

$\forall\ a \neq e \in G$ & $H = \langle a \rangle$, cyclic subgr. generated by a.

$o(H) > 1$.

By Lagrange's Theorem,

$o(H) \mid o(G) = p$.

$\Rightarrow o(H) = p$ as only divisors of p are 1 & p itself & $o(H) \neq 1$.

Corollary

Each non-identity element of a cyclic group G of prime order is a generator of G.

[G cyclic $\Rightarrow$ all its subgroups are cyclic

$\Rightarrow$ they are generated by the elements of G.

As each non-identity element of G generates G

G has no proper & non-trivial subgroup.]

Note order of a cyclic group may not be prime.

Example: $(\mathbb{Z}_n, +)$ cyclic group for all +ve integers n.

Theorem $G \to$ finite group, $a \in G$.

Then $o(a) \mid o(G)$.

proof: $\langle a \rangle \to$ cyclic subgr. of G generated by a

$o(\langle a \rangle) = o(a)$.

By Lagrange's Theorem, $o(\langle a \rangle) \mid o(G)$

$\Rightarrow o(a) \mid o(G)$.

Note $G \to$ finite gr. of prime order p.
$o(a) = p \ \forall\ a \neq e$ in G.

Theorem $G \xrightarrow{\text{finite}} \text{gr.}$, $a \in G$

Then $a^{o(a)} = e$.

[$o(a) \mid o(a) \Rightarrow o(a) = m \cdot o(a)$

$\Rightarrow a^{o(a)} = a^{m \cdot o(a)}$

$= \left(a^{o(a)}\right)^m$

$= e^m = e$.]

Note - In a finite group G, every element is of finite order.

- In an infinite group, the order of an element may be finite or infinite
- $\exists$ infinite groups every element of which is of finite order.

Example:

$S \to$ set of all n-th roots of unity $\forall\ n \in N$ → forms a group under multiplication

i.e. $S = \{ a \mid a^n = 1, n \in N \}$.

- $a, b \in S \Rightarrow a^p = 1, b^q = 1$ for some $p, q \in N$

$\Rightarrow (a^p)^q (b^q)^p = 1$

$\Rightarrow (ab)^{pq} = 1 \Rightarrow ab \in S$ (closure)

- Multiplication is associative in S
- $1 \in S$
- $a \in S \Rightarrow a^p = 1$ for some $p \in N \Rightarrow \left(\frac{1}{a}\right)^p = 1$

$\Rightarrow \frac{1}{a} \in S$

→ order of each element finite

→ but the group S is infinite.

Example:

(1) Every group of order < 6 is commutative.

Soln. $G \to$ group

$o(a) = 1 \to$ cyclic group generated by the identity element e

$\to$ Commutative

$o(a) = 2 \to$ prime order group $\to$ cyclic $\to$ Commutative

$o(a) = 3 \to$ .....

$o(a) = 5 \to$ .....

$o(a) = 4$

$a \in G$

$\Rightarrow o(a) \mid o(a) = 4$

$\Rightarrow o(a) = 1, 2$ or 4.

$\to$ Case 1 $\exists$ an element of order 4 in G

$\Rightarrow$ cyclic gr. of order 4

$\Rightarrow$ Commutative.

$\to$ Case 2 $\exists$ no element of order 4.

if $a \in G$, then $o(a) \mid o(a) = 4$

$\therefore o(a) = 1, 2$

$\begin{cases} o(a) = 1 \Rightarrow a = e, \text{ the identity element} \\ o(a) = 2 \Rightarrow \bar{a}^1 = a \end{cases}$

$\Leftarrow$ $\boxed{\bar{a}^1 = a \ \forall a \in G.}$

(S) [G has one element of order 1 (the identity element) & all the other elements have order = 2]

Hence (S) $a \in G, b \in G \Rightarrow a = \bar{a}^1, b = b^{-1}$

Thus $ab = \bar{a}^1 b^{-1} = (ba)^{-1} = ba$

as $ba \in G \Rightarrow (ba)^{-1} \in G$. $ba = (ba)^{-1}$

$\Rightarrow G$ is commutative

Example:

(2) A non-commutative group of order $2n$, where n is an odd prime, must have a subgroup of order n.

Soln: $G \to$ group, $o(G) = 2n$, n odd prime

$a \in G \Rightarrow o(a) \mid 2n$

$\Rightarrow o(a) = 1, 2, n$ or $2n$

No element of order n $\quad o(a) \neq 2n \to$ otherwise G will be cyclic generated by a & it will be commutative.

Only one element of order 1, the identity element $\quad o(a) = 1 \Rightarrow a = e \to$ only one element of order 1, the identity element

Order of each element cannot be 2 $\quad o(a) \neq 2 \to$ otherwise $a = a^{-1}$

Also $e = e^{-1}$

$\therefore$ if $a \in G$, $a = a^{-1}$

If $a \in G$, $b \in G$, then $ab \in G$,

$(ab)^{-1} = ab$,

$a^{-1} = a$, $b^{-1} = b$

$\therefore (ab)^{-1} = ab = a^{-1}b^{-1} = ba$

$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$

$\Rightarrow G$ is commutative.

$\therefore o(a) = n$ for some $a \in G$ & the cyclic subgroup $\langle a \rangle$ is a subgroup of G of order n.

Example:

(3) Every proper subgroup of a group of order 6 is cyclic

Sol^n: $G \to$ group, $o(G) = 6$.

$H \to$ proper subgroup of G.

As $o(H) \mid o(G) = 6$, so $o(H) = 1, 2, 3, 6$

$o(H) \neq 6$ as H is a proper subgroup of G.

- if $o(H) = 1$ then $H = \{e\} = \langle e \rangle \to$ cyclic
- if $o(H) = 2$ then H is prime order gr $\to$ cyclic
- if $o(H) = 3$ .....

Note Every proper subgroup of S_3 is cyclic.

Exponent of a group

$G \to$ finite group, each element of G is of finite order.

highest possible order of an element in G is called the exponent of G.

Example: $G \to$ abelian group.

~~Then (exponent of G) |~~

Then $o(a) \mid$ (exponent of G) $\forall\ a \in G$.

[exp. of $G = n$, $o(a) = m \Rightarrow m < n$; if $m \nmid n$, then $\text{lcm}(m,n) > n$.
G commutative $\Rightarrow \exists\ c \in G$ s.t. $o(c) = \text{lcm}(m,n) > n = \text{exp. of } G$ $(\to\leftarrow)$]

Note $G \to$ non-abelian group

$o(a)$ may not divide exponent of G for some $a \in G$.

↳ Example S_3 non-abelian, for ten element P_3, $o(P_3) \nmid$ (exponent of S_3)

Example:

(5) $G \rightarrow$ finite abelian group in which number of solutions of the equn. $x^n = e$ (e is the identity element) is at most n for every +ve integer n.

Prove that G is cyclic

Soln: let $O(G) = m$ and exponent of $G = m_1$

Then $m_1 \leq m$ ——— (1).

G abelian group and $m_1 =$ exp. of G

$\Rightarrow o(x) \mid m_1 \quad \forall x \in G$. i.e. $m_1 = o(x) \times t$ for some integer t

$\Rightarrow \forall x \in G, \quad x^{m_1} = (x^{o(x)})^t = e^t = e$.

As G has m elements,

# of Soln^{ns} of $x^{m_1} = e$ in G is m.

But by @ the given condition,

$x^{m_1} = e$ has at most m_1 Soln^{ns} in G

So $m \leq m_1$ ——— (2)

(1), (2) $\Rightarrow \quad m = m_1$

$\therefore \exists$ an element $c \in G$ s.t. $O(c) = m_1 = m$

$\Rightarrow \langle c \rangle = G \Rightarrow G$ is cyclic

Right Cosets

$G \to$ group, $a \in G$, $H \to$ Subgr. of G.

$\hookrightarrow Ha = \{ha \mid h \in H\}$

For different elements $a, b, c, \ldots$ in G

$\to$ the right cosets of H are

$Ha, Hb, Hc, \ldots$

for additive group $\to$ a right coset of H is denoted by $H+a$.

Example:

1) $G = (\mathbb{Z}, +)$, $H = (3\mathbb{Z}, +)$

$H+0 = \{3n \mid n \in \mathbb{Z}\} = H$

$H+1 = \{3n+1 \mid n \in \mathbb{Z}\}$ ⊃

$H+2 = \{3n+2 \mid n \in \mathbb{Z}\}$.

distinct

Three ~~different~~ right cosets $\to H, H+1, H+2$

2) $G = S_3$, $H = \{P_0, P_3\}$

$HP_0 = H$

$HP_1 = \{P_1, P_4\}$

$HP_2 = \{P_2, P_3\}$

distinct

$HP_3 = H$

$HP_4 = HP_1$

$HP_5 = HP_2$

Three ~~different~~ right cosets $\to H, HP_1, HP_2$

3) $G = S_3$, $H = \{\rho_0, \rho_1, \rho_2\}$

$H\rho_0 = \{\rho_0, \rho_1, \rho_2\} = H$
$H\rho_1 = \{\rho_1, \rho_2, \rho_0\} = H$
$H\rho_2 = \{\rho_2, \rho_0, \rho_1\} = H$
$H\rho_3 = \{\rho_3, \rho_5, \rho_4\}$
$H\rho_4 = \{\rho_4, \rho_3, \rho_5\}$
$H\rho_5 = \{\rho_5, \rho_4, \rho_3\}$

Two distinct right cosets → H, $\{\rho_3, \rho_4, \rho_5\}$

Theorem G gr., H Subgr. of G, $h \in H$
Thm $Hh = H$

Theorem G gr., H Subgr. of G, $a \in G \setminus H$
Thm $Ha \cap H = \phi$

Theorem Any two right cosets of H in G are either identical or distinct. (i.e. no overlapping).

Theorem H is a Subgr. of G, $a, b \in G$
Thm $b \in Ha \iff ba^{-1} \in H$

Theorem H is a Subgr. of G, $a, b \in G$.
Thm $Ha = Hb \iff ba^{-1} \in H$

Equivalent conditions for a Subgr. H of G & $a, b \in G$, Ha, Hb

i) $b \in Ha$
ii) $ba^{-1} \in H$
iii) $Ha = Hb$.

Equivalence relation

$a \rho b$ iff $ba^{-1} \in H$

Partion of G by ρ

Theorem $|Ha| = |Hb|$ $\forall a, b \in G$
right cosets Ha & Hb

Theorem Let H be a Subgroup of a group G.

# of distinct left cosets of H in G
$=$ # of distinct right cosets of H in G.

Proof Let L = the Set of all left cosets
R = the set of all right cosets.
$a \in G$

Define a mapping $f: L \to R$ by

$$f(aH) = Ha^{-1}, \quad aH \in L$$

Claim f is well defined in the sense that
if $xH = aH$ then $Hx^{-1} = Ha^{-1}$

proof $xH = aH \iff x \in aH \iff x^{-1}a \in H \iff x^{-1}(a^{-1})^{-1} \in H$
$\iff x^{-1} \in Ha^{-1}$
$\iff Ha^{-1} = Hx^{-1}$.

So f assigns a unique coset in R to a coset in L.

Claim f is injective.

proof Let $aH, bH \in L$ and
Now $aH \neq bH$

Now $f(aH) = f(bH) \Rightarrow Ha^{-1} = Hb^{-1} \Rightarrow aH = bH$
So $aH \neq bH \Rightarrow f(aH) \neq f(bH)$
$\Rightarrow f$ is injective.

Using equivalent conditions

H Subgr. of a gr. G
$a, b \in G$., aH, bH

i) $b \in aH$
ii) $a^{-1}b \in H$
iii) $aH = bH$.

Claim f is surjective. $f: L \to R$.

proof $\forall\ Ha \in R$.

The preimage of Ha is $a^{-1}H$ in L since

$$f(a^{-1}H) = H(a^{-1})^{-1} = Ha$$

$\Rightarrow$ f is surjective.

$\therefore$ f is bijective $\Rightarrow$ $|L| = |R|$.

Def (index)

The common cardinality of L, R is called the index of H in G & is denoted by $[G:H]$

Each subgroup H of G.

↓ yields distinct left cosets in G,

Say $x_1H, x_2H, \ldots, x_mH$

& $G = \bigcup_{i=1}^{m} x_iH$

$$o(G) = |x_1H| + |x_2H| + \cdots + |x_mH|$$

$= m \cdot |H|$ as any two left cosets have the same cardinality as that of coset H & $|H| = o(H)$.

Note: ~~$o(H)$~~

$$o(G) = m \cdot o(H)$$

$$= [G:H]\, o(H).$$

$$[G:H] = \frac{o(G)}{o(H)}.$$

Example:

1. $G = S_3$, $H = A_3$

   $[G:H] = 2 = \frac{o(G)}{o(H)}$

2. $G = (\mathbb{Z}, +)$, $H = (2\mathbb{Z}, +)$

   $[G:H] = 2$, both H, G infinite

3. $G = (\mathbb{R}, +)$, $H = (\mathbb{Z}, +)$

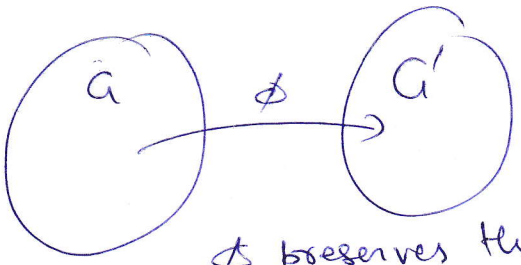
   $[G:H]$ infinite as $\exists$ infinitely many left cosets of H in G

Homomorphism

- $(G,\circ)$, $(G',*)$ two grs.

  $\phi : G \to G'$ is a homomorphism if

  $$\phi(a \circ b) = \phi(a) * \phi(b) \quad \forall\, a,b \in G.$$



ϕ preserves the algebraic structure of the systems.

- ϕ not only relates two elements $a,b \in G$ to two elements $a',b' \in G'$, but also relates $a \circ b \in G$ to $a' \circ b' \in G'$.

Monomorphism → a 1-to-1 homomorphism.

Epimorphism → onto homomorphism.

Isomorphism → both monomorphism & epimorphism

Automorphism → isomorphism from a group onto itself.

Example: $\phi : G \to G'$ $\quad (G,\circ)$, $(G',*)$ ← identity $e_{G'}$.

$$\boxed{\phi(a) = e_{G'}}$$

$\forall\, a,b \in G$, $\phi(a \circ b) = e_{G'} = e_{G'} * e_{G'} = \phi(a) * \phi(b)$

$\Rightarrow \phi$ is a homomorphism. → (always exists) trivial homomorphism from G to G'.

Example: $G = (\mathbb{Z}, +)$, $G' = (2\mathbb{Z}, +)$

$\phi : G \to G'$ defined by $\phi(a) = 2a$, $a \in G$.

Examine if ϕ is a homomorphism.

Soln: Let $a, b \in G$.

$$\phi(a+b) = 2(a+b) = 2a + 2b = \phi(a) + \phi(b)$$

So homomorphism.

Note: ϕ injective as well as surjective, so ϕ is an isomorphism.

Example: $G = (\mathbb{Z}, +)$

$\phi : G \to G$, $\phi(x) = x + 1$, $x \in G$.

Examine if ϕ is a homomorphism.

Soln: $x, y \in G$ $\quad \phi(x) = x + 1$

$\phi(y) = y + 1$

$$\phi(x+y) = x + y + 1 \neq \phi(x) + \phi(y) = x + y + 2$$

So not a homomorphism.

Note: Although ϕ is a bijection, ϕ does not satisfy the conditions for a group homomorphism

Example: $G = (\mathbb{Z}, +)$, $G' = (\mathbb{Z}_n, +)$.

$\phi : G \to G'$, $\phi(m) = [m]$, $m \in \mathbb{Z}$

($[m]$ = remainder of $m \pmod n$)

Examine if ϕ is a homomorphism.

Soln. $\forall\ p, q \in \mathbb{Z} \Rightarrow p+q \in \mathbb{Z}$.

$\phi(p) = [p]$, $\phi(q) = [q]$

$\phi(p+q) = [p+q] = [p] + [q] = \phi(p) + \phi(q)$

$\Rightarrow$ ϕ homomorphism.

Example: $G = S_3$, $G' = (\{1, -1\}, \cdot)$

$\phi : G \to G'$.

$$\phi(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is an even permutation in } S_3 \\ -1 & \text{if } \alpha \text{ is an odd permutation in } S_3 \end{cases}$$

Examine if ϕ is a homomorphism.

Soln. **Case I** α, β both even permutation $\Rightarrow$ $\alpha\beta$ also even.

$\phi(\alpha) = 1$, $\phi(\beta) = 1$, $\phi(\alpha\beta) = 1$

$\Rightarrow \phi(\alpha\beta) = \phi(\alpha)\,\phi(\beta)$.

case II α, β both odd permutations $\Rightarrow$ $\alpha\beta$ even

$\phi(\alpha) = -1$, $\phi(\beta) = -1$, $\phi(\alpha\beta) = 1 = \phi(\alpha)\,\phi(\beta)$

case III α odd, β even $\Rightarrow$ $\alpha\beta$ odd

$\therefore \phi(\alpha\beta) = -1 = \phi(\alpha)\,\phi(\beta)$.

$\therefore$ ϕ is homomorphism

Note: ϕ is not injective but surjective, so an epimorphism.

Theorem Let $(G,\circ)$ and $(G',*)$ be two groups and $\phi: G \to G'$ be a homomorphism. Then

(i) $\phi(e_G) = e_{G'}$

(ii) $\phi(a^{-1}) = \{\phi(a)\}^{-1} \quad \forall\, a \in G$

(iii) if $a \in G$ then $\phi(a^n) = \{\phi(a)\}^n$, n being an integer.

(iv) if $a \in G$ and $o(a)$ is finite, then $o(\phi(a))$ is a divisor of $o(a)$.

Rings

A non-empty set R is said to form a ring w.r.to two binary compositions, addition $(+)$ and multiplication $(\cdot)$ 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 $a,b,c \in R$ the left distributive law $a.(b+c) = a.b + a.c$ and the right distributive law $(b+c).a = b.a + c.a$ both hold.

Therefore, a non-empty set R is a ring with respect to two binary compositions $+$ and $\cdot$, if

(i) $a+b \in R \quad \forall\ a,b \in R$

(ii) $a+(b+c) = (a+b)+c \quad \forall\ a,b,c \in R$

(iii) $\exists$ an element, denoted by 0, in R s.t. $a+0 = a \quad \forall\ a \in R$

(iv) for each $a \in R$, $\exists\ (-a) \in R$ s.t. $a+(-a) = 0$.

(v) $a+b = b+a$

(vi) $a.b \in R \quad \forall\ a,b \in R$

(vii) $a.(b+c) = a.b + a.c$ and $(b+c).a = b.a + c.a \quad \forall\ a,b,c \in R$

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

- R is commutative ring if the multiplication is commutative.

Fields

A nontrivial ring R with unity is a field if it is commutative and each non-zero element of R is a unit.

Therefore, a non-empty set F forms a field w.r.to two binary compositions $+$ and $\cdot$, if

(i) $a+b \in F \ \forall\ a,b \in F$

(ii) $a+(b+c) = (a+b)+c \ \forall\ a,b,c \in F$.

(iii) $\exists$ an element, called the zero element and denoted by 0, in F such that $a+0=a \ \forall\ a \in F$.

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

(v) $a+b = b+a \ \forall\ a,b \in F$

(vi) $a.b \in F \ \forall\ a,b \in F$

(vii) $a.(b.c) = (a.b).c \ \forall\ a,b,c \in F$

(viii) $\exists$ an element, called the identity element and denoted by I, in F such that $a.I = a \ \forall\ a \in F$.

(ix) for each non-zero element $a \in F$, $\exists$ an element, denoted by $\bar{a}^1$, in F such that $a.(\bar{a}^1) = I$;

(x) $a.b = b.a \ \forall\ a,b \in F$

(xi) $a.(b+c) = a.b + a.c \ \forall\ a,b,c \in F$.

The field is denoted by $(F,+,\cdot)$ or by F.