Examples : 1. The symmetric group S_3 is not cyclic, since it is not abelian.

2. The dihedral group D_4 is not cyclic, since it is not abelian.

Theorem 3.3 Let G be a finite cyclic group generated by a. Then $O(G) = n$ if and only if $O(a) = n$

Proof : Let $O(a) = n$. Then $a, a^2, \ldots, a^n (= e)$ are distinct elements of G, where e is the identity element in G.

So, $\{a, a^2, \ldots, a^n\} \subset G$ ... (i)

Again $G = \{a^k : k \in \mathbb{Z}\}$. Let p be an arbitrary element of G. Then $p = a^m$ for some integer m. By division algorithm, $\exists$ integers q and r such that $m = qn + r$ where $0 \le r < n$.

So, $p = a^m = a^{qn+r} = (a^n)^q a^r = e a^r = a^r$, since $a^n = e$.

So, $p \in \{a, a^2, \ldots, a^n (= e)\}$. $\therefore G \subset \{a, a^2, \ldots, a^n\}$ ... (ii)

From (i) and (ii) $G = \{a, a^2, \ldots, a^n (= e)\}$ and so $O(G) = n$

Conversely, let $O(G) = n$. Since G is a finite group, every element of G is of finite order. Let $O(a) = k$. So, $a, a^2, \ldots, a^k (= e)$ are distinct elements of G. Since G contains n elements, $k \le n$.

But k is not less than n, because by the previous argument, $O(a) = k \Rightarrow O(G) = k$, a contradiction. So, $k = n$.

So, $O(a) = n$.

Corollary 3.3.1 If $G = \langle a \rangle$ and $O(a) = n$, $G = \{a, a^2, \ldots, a^n (= e)\}$

Corollary 3.3.2 Let G be a cyclic group generated by a. Then G is infinite if and only if $O(a)$ is infinite

Theorem 3.4 A finite group G of order n is cyclic if and only if $\exists$ an element b in G such that $O(b) = n$

Proof : Let G be a finite cyclic group of order n. Let $G = \langle a \rangle$. So $O(a) = n$, by Theorem 3.3.

Scanned with CamScanner

Conversely, let $O(G) = n$ and $\exists$ an element b in G such that $O(b) = n$.
Since $O(b) = n$, the elements $b, b^2, \ldots, b^{n-1}, b^n (= e)$ are distinct elements of G
Since $O(G) = n$, $G = \{b, b^2, \ldots, b^{n-1}, b^n (= e)\}$
So, $G \subset \langle b \rangle = \{b^k : k \in \mathbb{Z}\}$. Since $b \in G$, $b^k \in G$ for any integer k
$\therefore \langle b \rangle \subset G$. Hence $G = \langle b \rangle = \{b^k : k \in \mathbb{Z}\}$

So, This shows that G is a cyclic group generated by b.

Examples: 1. $(\mathbb{Z}_n, +)$ is a group of order n and $\bar{1} \in \mathbb{Z}_n$ and $O(\bar{1}) = n$.
So, $(\mathbb{Z}_n, +)$ is a cyclic group of order n and $\bar{1}$ is a generator.

2. The symmetric group S_3 is not cyclic, since the order of S_3 is 6 and $\exists$ no element of order 6 in S_3

Theorem 3.4 Let G be a finite cyclic group of order $n (>1)$ generated by the element a. Then for a positive integer r, a^r is also a generator of the group if and only if r is less than n and prime to n.

Proof: Since $O(G) = n$, $O(a) = n$ and $G = \{a, a^2, \ldots, a^n (= e)\}$. Let a^r be a generator of the group. Then $1 \le r < n$.

Since a^r is a generator of G and $a \in G$, $a = (a^r)^k$ for some integer k

Hence $a^{rk-1} = e$. Since $O(a) = n$, n is a divisor of $rk-1$, by Theorem 2.7
So, $rk - 1 = sn$ for some integer s. So, $kr + sn = 1$ where k and s are integers and This implies $\gcd(r, n) = 1$. So, it follows that r is less than n and prime to n.

Conversely, let r be less than n and prime to n. Then $O(a^r) = n$. by Theorem 2.7. So a^r is a generator of G, by Theorem 3.3.

Corollary 3.4.1 The total number of generators of a finite cyclic group of order n is $\phi(n)$, where $\phi(1) = 1$ and $\phi(n) =$ the number of positive integers less than n and prime to n, for $n \ge 2$.

Examples: 1. The number of generators of the cyclic group $(\mathbb{Z}_p, +)$, where p is a prime is $p-1$ since $\phi(p) = p - 1$

Scanned with CamScanner

Theorem 3.5 Every subgroup of a cyclic group is cyclic.

Proof: Let G be a cyclic group generated by a and let H be a subgroup of G. We consider the following cases:

Case 1 $H = G$. So, H is a cyclic group.

Case 2 $H = \{e\}$ (e is the identity element in G). Since $e^n = e \ \forall n \in \mathbb{Z}$

$H = \{e^n : n \in \mathbb{Z}\}$. So, H is the cyclic group $\langle e \rangle$

Case 3 H is a proper subgroup of G other than $\{e\}$.

Then $\exists$ an $x \in H$ such that $x \neq e$. Since $x \in G$, $x = a^k$ for some integer $k \neq 0$. Since H is a subgroup, $x^{-1} \in H$, so $x^{-1} = a^{-k} \in H$

As $a^k, a^{-k} \in H$ for some integer $k \neq 0$, so, there is some positive integral power of a in H. Let m be the least positive integer such that $a^m \in H$. Such an m exists by well ordering property of $\mathbb{N}$.

We prove that a^m is a generator of H. So H should be cyclic.

Let $h \in H$. Then $h = a^p$ for some integer p. By division algorithm, $\exists$ integers q and r such that $p = qm + r$, $0 \leq r < m$.

Since H is a subgroup $a^m \in H \Rightarrow a^{-qm} \in H$. Also $a^p \in H$ and $a^{-qm} \in H \Rightarrow a^{p-qm} \in H$, i.e., $a^r \in H$. But $0 \leq r < m$ and $a^r \in H$ are both satisfied only if $r = 0$, because, otherwise, m fails to be the smallest positive integer such that $a^m \in H$.

So, $p = qm$ and therefore $a^p = a^{qm} = (a^m)^q$ where q is an integer. Hence $H = \langle a^m \rangle$

Corollary 3.5.1 A cyclic group of prime order has no non-trivial subgroup.

Corollary 3.5.2 Every non-trivial subgroup of an infinite cyclic group is infinite.

Scanned with CamScanner

Worked out exercises: 1. Find all subgroups of $(\mathbb{Z}, +)$

Solution: $(\mathbb{Z}, +)$ is a cyclic group with 1 as generator. Therefore every subgroup of $(\mathbb{Z}, +)$ is cyclic. Hence all subgroups of $(\mathbb{Z}, +)$ are given by the cyclic sub-groups generated by different elements of $\mathbb{Z}$.

The cyclic subgroup generated by the integer n is $(n\mathbb{Z}, +)$. So, all subgroups of $(\mathbb{Z}, +)$ are precisely $(n\mathbb{Z}, +)$, where n is an integer. Since the subgroups $(n\mathbb{Z}, +)$ and $(-n\mathbb{Z}, +)$ are identical, the totality of all the subgroups of $(\mathbb{Z}, +)$ are given by $(n\mathbb{Z}, +)$ where n is a non-negative integer.

2. Prove that $(\mathbb{Q}, +)$ is not cyclic

Proof: Suppose $(\mathbb{Q}, +)$ is cyclic. Then $\mathbb{Q} = \langle \frac{p}{q} \rangle$ for some $\frac{p}{q} \in \mathbb{Q}$, where p and q are relatively prime. Since $\frac{p}{2q} \in \mathbb{Q}$, $\exists\, n \in \mathbb{Z}$, $n \neq 0$ such that $\frac{p}{2q} = n\frac{p}{q}$. This implies $\frac{1}{2} = n \in \mathbb{Z}$, a contradiction. Thus, $\mathbb{Q}$ is not cyclic.

3. Let G be an infinite cyclic group generated by a. Show that

(i) $a^r = a^t$ if and only if $r = t$, where $r, t \in \mathbb{Z}$,

(ii) G has exactly two generators.

Proof: (i) Suppose $a^r = a^t$ and $r \neq t$. Let $r > t$. Then $a^{r-t} = e$. Thus, $o(a)$ is finite. As G is cyclic, so $o(G)$ would be finite by Theorem 3.3, a contradiction since G is an infinite cyclic group. So, $r = t$. The converse is straightforward.

(ii) Let $G = \langle b \rangle$ for some $b \in G$. Since $a \in G = \langle b \rangle$ and $b \in G = \langle a \rangle$, $a = b^r$ and $b = a^t$ for some $r, t \in \mathbb{Z}$

Thus $a = b^r = (a^t)^r = a^{tr}$. Hence, by (i) $tr = 1$. This implies either $t = r = 1$ or, $t = r = -1$. Thus, either $b = a$ or $b = a^{-1}$ now from (i) $a \neq a^{-1}$. So, G has exactly two generators.

Scanned with CamScanner

4. Let $G = \langle a \rangle$ be a cyclic group of order n, $n > 1$, and H be a proper subgroup of G. Then $H = \langle a^k \rangle$ for some integer k such that k divides n and $k > 1$. Furthermore, $o(H)$ divides n.

Proof: If $H = \{e\}$ then $H = \langle e^n \rangle$. Suppose $H \neq \{e\}$. Let k be the smallest positive integer such that $a^k \in H$. Then $H = \langle a^k \rangle$.

Now $\exists$ integers q and r such that $n = qk + r$, $0 \leq r < k$, and

$$a^r = a^{n-qk} = a^n a^{-qk} = a^{-qk} = \left((a^k)^{-1}\right)^q \in H.$$ The minimality of k implies $r = 0$. Hence $n = qk$ and so k divides n. Since $H \neq G$, $k > 1$. Next, we show that $o(H)$ divides n.

By Theorem 2.7, $o(a^k) = \frac{n}{\gcd(n,k)} = \frac{n}{k} = q$. So $o(H) = q$ by Theorem 3.3. Since $n = qk$, we have q divides n.

So $o(H)$ divides n.

4. Cosets. Let H be a subgroup of a group G and $a \in G$. The sets $aH = \{ah : h \in H\}$ and $Ha = \{ha : h \in H\}$ are called the left and right cosets of H in G, respectively.

If G is a commutative group, then $aH = Ha$. Observe that $eH = H = He$ (e being the identity element in G) and that

$a = ae \in aH$ and $a = ea \in Ha$

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

The left coset $0 + H = \{3n : n \in \mathbb{Z}\} = H$
The left coset $1 + H = \{3n+1 : n \in \mathbb{Z}\}$
The left coset $2 + H = \{3n+2 : n \in \mathbb{Z}\}$

There are three distinct left cosets of H. They are H, $1+H$ and $2+H$

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

Scanned with CamScanner

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

$\rho_1 H = \{\rho_1, \rho_5\}$ $\quad \rho_4 H = \{\rho_2, \rho_4\} = \rho_2 H$

$\rho_2 H = \{\rho_2, \rho_4\}$ $\quad \rho_5 H = \{\rho_1, \rho_5\} = \rho_1 H$

So there are three distinct left cosets of H. They are H, $\rho_1 H$ and $\rho_2 H$

Right cosets of H are given by

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

$H\rho_1 = \{\rho_1, \rho_4\}$ $\quad H\rho_4 = \{\rho_4, \rho_1\} = H\rho_1$

$H\rho_2 = \{\rho_2, \rho_5\}$ $\quad H\rho_5 = \{\rho_5, \rho_2\} = H\rho_2$

So, there are three distinct right cosets of H. They are H, $H\rho_1$ and $H\rho_2$

Theorem 4.1. Let G be a group and H be a subgroup of G. Then $aH = H = Ha$ for any $a \in H$

Proof: We prove $aH = H$ for all $a \in H$. Other part is similar.

Let $p \in aH \Rightarrow p = ah$ for some $h \in H$. Here $a \in H$, $h \in H$ and H is a subgroup. So, $p = ah \in H$. So, $aH \subset H$

Let $q \in H$, Since $a \in H$ and $q \in H$, $\exists$ a unique x in H such that $ax = q$. So $q \in H \Rightarrow q = ax$, for some $x \in H$

$\Rightarrow q \in aH$

So, $H \subset aH$ $\quad \therefore H = aH$

Theorem 4.2 Let G be a group and H be a subgroup of G. Let $a \in G - H$ Then $aH \cap H = \phi$

Proof: If possible, let $p \in aH \cap H$. Then $p \in H$ and $p \in aH$

Hence $p = ah$ for some $h \in H$ and $p = h'$ for some $h' \in H$

This implies $h' = ah$ and so, $a = h'h^{-1} \in H$, since H is a subgroup.

This contradicts that $a \in G - H$. So $aH \cap H = \phi$.

Theorem 4.3 Let G be a group and H be a subgroup of G. If $a, b \in G$ then either $aH = bH$ or $aH \cap bH = \phi$

Scanned with CamScanner