Group Theory

Recap

Power of an element, Subgroup

Subgroup generated by an element

Website : https://www.goclasses.in/

Groups

Definition. A **group** is a set G, together with a binary operation $*$, that satisfies the following axioms:

(G1: closure)
for all elements g and h of G, $g * h$ is an element of G;

(G2: associativity)
$(g * h) * k = g * (h * k)$ for all $g, h, k \in G$;

(G3: existence of identity)
there exists an element $e \in G$, called the **identity** (or **unit**) of G, such that $e * g = g * e = g$ for all $g \in G$;

(G4: existence of inverse)
for every $g \in G$ there exists an element $h \in G$, called the **inverse** of g, such that $g * h = h * g = e$.

The group $(G, *)$ is said to be **commutative** (or **Abelian**) if it satisfies an additional axiom:

(G5: commutativity) $g * h = h * g$ for all $g, h \in G$.

Basic properties of groups

- The identity element is unique.
- The inverse element is unique.
- $(g^{-1})^{-1} = g$. In other words, $h = g^{-1}$ if and only if $g = h^{-1}$.
- $(gh)^{-1} = h^{-1}g^{-1}$.
- $(g_1 g_2 \dots g_n)^{-1} = g_n^{-1} \dots g_2^{-1} g_1^{-1}$.
- **Cancellation properties**: $gh_1 = gh_2 \implies h_1 = h_2$ and $h_1 g = h_2 g \implies h_1 = h_2$ for all $g, h_1, h_2 \in G$.

Indeed, $gh_1 = gh_2 \implies g^{-1}(gh_1) = g^{-1}(gh_2)$
$\implies (g^{-1}g)h_1 = (g^{-1}g)h_2 \implies eh_1 = eh_2 \implies h_1 = h_2$.
Similarly, $h_1 g = h_2 g \implies h_1 = h_2$.

Equations in groups

Theorem Let G be a group. For any $a, b, c \in G$,

- the equation $ax = b$ has a unique solution $x = a^{-1}b$;
- the equation $ya = b$ has a unique solution $y = ba^{-1}$;
- the equation $azc = b$ has a unique solution $z = a^{-1}bc^{-1}$.

Powers of an element

Let g be an element of a group G. The positive **powers** of g are defined inductively:

$$g^1 = g \quad \text{and} \quad g^{k+1} = g \cdot g^k \quad \text{for every integer} \quad k \geq 1.$$

The negative powers of g are defined as the positive powers of its inverse: $g^{-k} = (g^{-1})^k$ for every positive integer k.
Finally, we set $g^0 = e$.

Theorem Let g be an element of a group G and $r, s \in \mathbb{Z}$. Then

(i) $g^r g^s = g^{r+s}$,
(ii) $(g^r)^s = g^{rs}$,
(iii) $(g^r)^{-1} = g^{-r}$.

Next, we introduce the concept of integral exponents of elements in a group. The concept plays an important role in the theory of cyclic groups.

Definition 14.2

For any $a \in G$ we define

$$\begin{aligned} a^0 &= e \\ a^n &= a^{n-1}a, \quad for\ n \geq 1 \\ a^{-n} &= (a^{-1})^n \quad for\ n \geq 1. \end{aligned}$$

Given $r \in \mathbb{Z}$ and $a \in G$, we write

$$a^r = \begin{cases} a * a * \cdots * a \ \ (r \text{ times}), & \text{if } r > 0 \\ e, & \text{if } r = 0 \\ a^{-1} * a^{-1} * \cdots * a^{-1} \ \ (-r \text{ times}), & \text{if } r < 0 \end{cases}$$

If $n > 0$ is an integer, we abbreviate $\underbrace{a * a * a * \cdots * a}_{n \text{ times}}$ by a^n. Thus $a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * a^{-1} * \cdots * a^{-1}}_{n \text{ times}}$

Theorem 14.4

Let a be an element of a group G and m and n denote integers. Then

(i) $a^n a^{-n} = e$.
(ii) $a^m a^n = a^{m+n}$
(iii) $(a^m)^n = a^{mn}$.

Subgroups

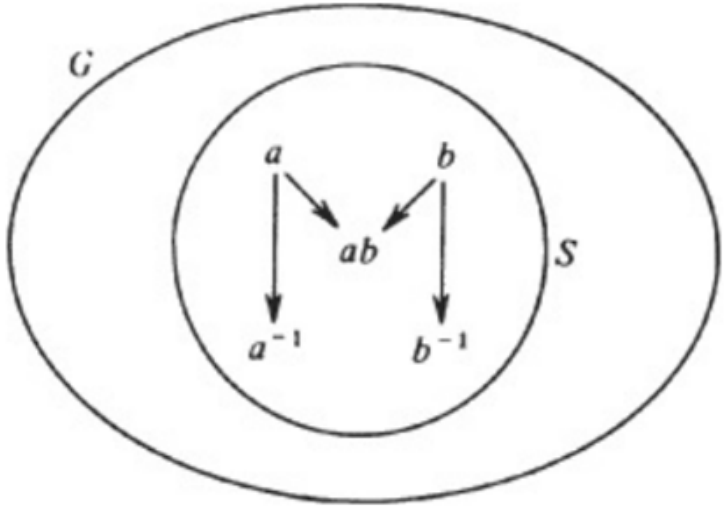
Definition. *Let $(G, *)$ be a group. A **subgroup** of G is a subset $H \subset G$ such that*

1. $e \in H$
2. $x, y \in H \Rightarrow x * y \in H$
3. $x \in H \Rightarrow x^{-1} \in H$

"Subgroup of Group G" is a Subset which is also a group under same Operation.

A subgroup is naturally a group under the induced binary operation. It clearly has the same identity element.

Let G be a group, and S a nonempty subset of G. It may happen (though it doesn't have to) that the product of every pair of elements of S is in S. If it happens, we say that S is *closed with respect to multiplication*. Then, it may happen that the inverse of every element of S is in S. In that case, we say that S is *closed with respect to inverses*. If both these things happen, we call S a *subgroup* of G.



Example 2.1: *Examples of subgroups.*

1. Both $\{1\}$ and G are subgroups of the group G. Any other subgroup is said to be a *proper subgroup*. The subgroup $\{1\}$ consisting of the identity alone is often called the *trivial subgroup*.

2. If a is an element of the group G, then

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, a^4, \ldots\}$$

are all the powers of a. This is a subgroup and is called the *cyclic subgroup* generated by a.

Note: Group $(G, *)$; $a \in G$

$\langle a \rangle$ = Subgroup of G generated by a

= Smallest Subgroup of G Containing a

$\langle a \rangle = \{ a^n \mid n \in Z \}$

Notations:

Subgroup $\leq$

H is subgroup of G $\equiv$ $H \leq G$

Subgroup

$\langle a \rangle$ = subgroup generated by a.

Group G, $|G|$ = order of G = Cardinality of G

$|G| = o(G) =$ order of Group G

number of elements in G.

Q: Group $(G, *)$; let $a \in G$

$\bar{a}^1 = a$ then $a = e$?

Ans: No.

for $e \Rightarrow \boxed{\bar{e}^1 = e}$

But $\boxed{a = \bar{a}^1} \not\Rightarrow a = e$

If $a = \bar{a}^1$ then

$a^2 = a \cdot a$

$= a \cdot \bar{a}^1 = e$

$(\{1, 3, 5, 7\}, \otimes_8) = U_8$

e

$e^{-1} = e$

$1^{-1} = 1$; $3^{-1} = 3$; $5^{-1} = 5$; $7^{-1} = 7$

$5^{-1} = 5$

$3^2 = 3 \otimes_8 3 = 1 = e$

$5 = e$

Q : Let G be a group. Let a $\in$ G and a is inverse of itself. Then what is $< a >$?

Q : Let G be a group. Let a $\in$ G and a is inverse of itself. Then what is $\langle a \rangle$?

$\bar{a}^1 = a$ Given. $a^2 = a \cdot a = a \cdot \bar{a}^1 = e$

$\langle a \rangle = \{ a^0 = e, a^1 = a, \bar{a}^1 = a, a^2 = e, a^3 = a, \bar{a}^2 = e, \bar{a}^3 = a, \ldots \}$

$(G, *)$; $a \in G$

$\bar{a}^1 = a$

means

$\bar{a}^2 = (\bar{a}^1)^2 = a^2 = e$

$a^3 = (a^2) \cdot a = e \cdot a = a$

$\bar{a}^3 = (\bar{a}^1)^3 = a^3 = a$

$a^2 = e$

$\bar{a}^2 = e$

$a^3 = a$

$(G, *)$, $a \in G$, $\bar{a}^1 = a$

$\langle a \rangle = \{a, e\}$

$\langle e \rangle = \{e\}$

Q : Let G be a group which can be generated by an element "a" which is inverse of itself.

Then what is order of G?

$(G, *)$; group

$\langle a \rangle = G$

$\bar{a}^1 = a$ given

a is Generator of G

$\langle a \rangle = G$

$G = \{a, e\}$

$|G| \leq 2$;

$|G| = 1$ or 2

$a^{-1} = a$

$\langle a \rangle = \{a, e\}$

$G = (\{e\}, *)$

$G = (\{e, a\}, *)$

Q: Group $(G, *)$; $a \in G$

$\langle a \rangle = G$; $\bar{a}^1 = a$

then How many such Non-Isomorphic Groups possible? $\Rightarrow$ 2 (each is Abelian)

Ans: 2 — Group of order 1 $\Rightarrow$ 1
Group of order 2 $\Rightarrow$ 1

Group Theory

Next Topic

Order of an Element

(Size of Subgroup generated by an element)

Website : https://www.goclasses.in/

The order of a finite group is the number of its elements.

If a group is not finite, one says that its order is infinite.

The order of an element of a group (also called period length or period) is the order of the subgroup generated by the element.

$\varphi : (\{1, -1, i, -i\}, \times) = G \Rightarrow \langle i \rangle = G$

$\langle -i \rangle = G$

order of $G = 4 = |G|$

order of $1 = |\langle 1 \rangle| = |\{1\}| = 1$

order of $-1 = |\langle -1 \rangle| = |\{-1, 1\}| = 2$

order of $i = |\langle i \rangle| = 4$; $|-i| = 4$

Note: Group $(G, *)$; $a \in G$

order of a $= |\langle a \rangle|$

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

order of a

Q: $U_{10} = \{1, 3, 7, 9\}, \otimes_{10}$

e

$|U_{10}| = 4$

$|1| = |e| = |\langle e \rangle| = |\{e\}| = 1$

$|3| = |\langle 3 \rangle| = |\{1, 3, 9, 7\}| = 4 \Rightarrow$ 3 is Generator

$G = (\{1, 3, 7, 9\}, \otimes_{10})$

$3^3 = (3 \times 3 \times 3) \bmod 10$

$= 7$

$3^{-1} = 7 \; ; \; 7^{-1} = 3$

$3^{-1} = (3 \times y) \bmod 10$

$= 1$

$\langle 7 \rangle = \langle 3 \rangle = \{1, 3, 7, 9\}$

$|7| = 4$

So 7 is Generator

$|9| = |\{1, 9\}|$

$\bar{9}^1 = 9$

$|9| = 2$

$9 =$ NoT Generator

$e^{-1} = e$

$\Downarrow$

$\langle e \rangle = \{e\}$

$\bar{a}^1 = a$

$\Downarrow$

$\langle a \rangle = \{a, e\}$

$G : (G, *)$ group ; $a \in G$; $a^{-1} = a$

$|\langle a \rangle| = ?$

$|\langle a \rangle| \leq 2$

$\begin{cases} a = e & |\langle a \rangle| = 1 \\ a \neq e & |\langle a \rangle| = 2 \end{cases}$

Observation:

$\{0, 1, 2, \cdots, 9\}$

Ex: $(Z_{10}, \oplus_{10})$

$e = 0$

① $\langle 0 \rangle = \{0^0 = 0^e\}$ $\quad \langle e \rangle = \{e\}$

$\langle 0 \rangle = \{0^n \mid n \in Z\}$

Note: In Number Theory $= 0^0 =$ UnDefined

In Group : $0^0 = e$

Generator

(2) $\langle 1 \rangle = \{1^0 = 0, 1^1 = 1, 1^2 = 2, 1^3 = 3, 1^4 = 4, 1^5 = 5, 1^6 = 6, 1^7 = 7, 1^8 = 8, 1^9 = 9, 1^{10} = 0; 1^{11}, 1^{12} \ldots$ nothing new

$\langle 1 \rangle = Z_{10}$

$1^{10} = e$

$\bar{1}^1 = 1^9 = 9$

(2) $\langle 2 \rangle = \{ 2^n \mid n \in Z \} = \{ 2^0, 2^1, 2^2, 2^3, \ldots, 2^{-1}, 2^{-2}, 2^{-3}, \ldots \}$

$\langle 2 \rangle = \{ 2^0 = 0 = e ; 2^1 = 2 ; 2^2 = 4 ; 2^3 = 6 ; 2^{-1}, 2^4 = 8 ; 2^5 = 0 = e ; 2^6 = 2 ; 2^7 = 4 ; 2^8 = 6 \ldots$ nothing new

Not Positive

$2^5 = e \Rightarrow 2^4 \cdot 2 = e \Rightarrow 2^{-1} = 2^4 = 8$

$2^{-2} = (2^{-1})^2 = (2^4)^2 = 2^8 = (2^5 \cdot 2^3) = e \cdot 6 = 6$

$2^3 = 8$ ✗

$2^3 = 2 \oplus_{10} 2 \oplus_{10} 2 = (2+2+2) \bmod 10 = 6$

$\langle 2 \rangle = \{2, 4, 6, 8, e\}$

order of $2 = 5$

2 = Not Generator

$\langle 3 \rangle = \{$

$3^1 = 3,\ 3^2 = 6,\ 3^3 = 9,$

$3^4 = 2,\ 3^5 = 5;\ 3^6 = 8;\ 3^7 = 1;$

$3^8 = 4;\ 3^9 = 7;\ 3^{10} = 0 = e$ $\}$

smallest +ve int

$3^5 = (3^4) \cdot 3 = 2 \cdot 3 = (2+3) \bmod 10 = 5$

$\langle 3 \rangle = Z_{10}^{*}$ $\quad$ 3 = Generator

$|3| = |\langle 3 \rangle| = 10$

$|3|$ = Smallest positive integer n such that $3^n = e$

$\langle a \rangle = \{a^1, a^2, \ldots, a^{r-1}, a^r = e\}$

a^{-1}

Order of $a = r$

smallest +ve integer

Note:

Not positive

$\langle a \rangle = \{ a^0 = e, a^1 = a, a^2 = b, a^3 = e, a^4 = a, \ldots \}$

↑ smallest positive power

$a^5 = b$

$a^6 = e$

$a^7 = a$

$a^8 = b \ldots$

$a^6 = a^3 \cdot a^3 = e \cdot e = e$

$a^5 = a^3 \cdot a^2 = e \cdot a^2 = a^2 = b$;

Note: In Group

$ba = e \Rightarrow b = \bar{a}^1$

In Group:

$a^5 = e \Rightarrow \bar{a}^1 = a^4$

$a^4 \cdot a = e \Rightarrow \bar{a}^1 = a^4$

Note: In Group if $ba = e$

working as a^{-1}

$ba = e$

$\underline{b^{-1}(ba)} = b^{-1}e$

e

$a = b^{-1}$

$b = a^{-1}$

Note: Group $(G, *)$; $a \in G$; $a \neq e$

$\langle a \rangle = \{ a^0 = e ; a^1 = a ; a^2 = b ; a^3 = e \}$

$a^3 = e$

$a^{-1} = a^2$

a^{-1}, a^{-2}

a^{-1}

a^2

$a^4 = a$

nothing new

$a^4 = a$

a^5, a^6, ... Nothing new

Order of an Element Definitions:

Group $(G, *)$ $\quad$ $a \in G$

1. If $a = e$ $\quad$ $|e| = 1$
2. $a \neq e$ then $|a| = |\langle a \rangle|$

$|a| =$ smallest +ve n such that $a^n = e$

$|a| = |\langle a \rangle| =$ Smallest Positive n ; $a^n = e$

If $|a| = 5$ means;

$\langle a \rangle = \{ a^1 = a, a^2 = b, a^3 = c, a^4 = d, a^5 = e \}$

Identity

a^{-1}

$Q : (\{1, -1, i, -i\}, \times)$

$|i| = \{i^1, i^2, i^3, i^4, \ldots\}$

$i \quad -1 \quad -i \quad -1$

$i^{-1} = -i = i^3$

$i^4 = e = 1$

$|i| = 4$

$|i| =$ Smallest $+ve$ n

$i^n = 1$

$n = 4$

$|i| = 4 = |\langle i \rangle|$

Definition 1: order of a = size of subgroup generated by a

= |⟨a⟩|

Definition 2

12 Order of an Element : The order of an element $a \in G$ is the least positive integers n such that

$$a^n = e \text{ , where e is the identity of G.}$$

Example : Let G = {1, –1. i, –i}. Then G is a multiplicative group.

Now $1^1 = 1 \Rightarrow 0(1) = 1$

$(-1)^1 = 1$, $(-1)^2 = 1 \Rightarrow 0(-1) = 2$, $i^1 = I$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1 \Rightarrow o(i) = 4$

$(-i)^1 = -i$, $(-i)^2 = -1$, $(-i)^3 = i$, $(-i)^4 = 1 \Rightarrow 0(-i) = 4$

Note:

If $|a| = n$ then $a^{-1} = a^{n-1}$

$|a| = n$ means $a^n = e$

Smallest +ve integer

Order of an element

Let g be an element of a group G. We say that g has **finite order** if $g^n = e$ for some positive integer n.

If this is the case, then the smallest positive integer n with this property is called the **order** of g and denoted $o(g)$.

Otherwise g is said to have the **infinite order**, $o(g) = \infty$.

Q: $(Z, +)$ — Infinite Group

$\langle 2 \rangle = \{ 2^1 = 2, 2^2 = 4, 2^3 = 6, 2^4 = 8, \ldots \}$

$2^0 = 0, 2^{-1} = -2, 2^{-2} = -4, \ldots$

$\langle 2 \rangle = 2Z$

$|2| = \infty$

Smallest +ve n such that $2^n = 0$? No such n

NOTE: ① If there is No positive integer n such that $a^n = e$ then we will say that order of a is Infinite.

So, a can generate ∞ number of elements.

(2) If $a^n = e$ → smallest +ve integer

$\langle a \rangle = \{ a^1, a^2, \ldots, a^{n-1}, a^n = e \}$

$a^{n-1} \rightarrow a^{-1}$

$a^n = e \rightarrow a^0$

③ for infinite Groups, Take Care.

$\langle a \rangle = \{ a^n \mid n \in Z \}$

$|a| =$ smallest +ve integer (n)

$a^n = e$

$(Z, +)$ – Group

$|0| = 1$

$a \neq 0$

$|a| = \infty$

$\langle a \rangle = aZ$

NOTE: In Infinite Group if order of an element can be finite or infinite.

Note: In finite Group;

order of every element is finite.

Order (group theory)

In group theory, a branch of mathematics, the term **order** is used in two closely-related senses:

- The order of a group is its cardinality, i.e., the number of its elements.
- The order, sometimes **period**, of an element a of a group is the smallest positive integer m such that $a^m = e$ (where e denotes the identity element of the group, and a^m denotes the product of m copies of a). If no such m exists, a is said to have infinite order. All elements of finite groups have finite order.

The order of a group G is denoted by $\text{ord}(G)$ or $|G|$ and the order of an element a by $\text{ord}(a)$ or $|a|$.

Example 6.3. The orders of the elements of $\mathbb{Z}_{10}$ (under addition modulo 10) are 1, 10, 5, 10, 5, 2, 5, 10, 5, 10 respectively.

|0| |1| |2| |3| |4| |9|

Generators: 1, 3, 7, 9

Group Theory

Next Topic

Cyclic Group

Group that can be generated by a single element

Website : https://www.goclasses.in/

Cyclic Group:

Group that can be generated by a single element.

or

Group with at least one generator.

Ex: $(\{1,3,5,7\}, \otimes_8)$ — Cyclic Group?

$\langle 1 \rangle = \{1\}$ $\quad |1| = 2$

$\langle 3 \rangle = \{1, 3\}$ $\quad |3| = 2$

$\langle 7 \rangle = \{1, 7\}$ $\quad |7| = 2$

No

$7^2 = 1$

$5^2 = 1 : e$

Ex: $(\{1, 2, 3, 4\}, \times_5)$ → Cyclic Group? Yes

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

$\langle 2 \rangle = \{2, 4, 3, 1\}$

3, 2 = Generator

$2^{-1} = 3$

2^{-1}

$|2| = 2^{4} = 1$

$2^4 = 16 \bmod 5 = 1$

$2^3 = 8 \bmod 5 = 3$

13 Cyclic group : If in a group G there exist an element $a \in G$ such that every element $x \in$ G is of the form a^m, where m is some integer. Then G is a cyclic group and a is called the generator of G.

Example $G = \{1, -1, i, -i\}$

$= \{i^4, i^2, i, i^3\} = \{i, i^2, i^3, i^4\}$

Then G is a cyclic group generated by i.

Note : There may be more than one generators of any cyclic group.

$(Z_n, \oplus_n)$ —— Cyclic Group ?

Generator = 1 iff $n \geq 2$

$Z_1 = \{0\} \Rightarrow$ Cyclic — generator = 0

$Z_2 = \{0, 1\} \Rightarrow$ Cyclic → generator = 1

Cyclic Groups and Generators

Some groups have an interesting property:

all the elements in the group can be obtained by repeatedly applying the group operation to a particular group element. If a group has such a property, it is called a cyclic group and the particular group element is called a generator. A trivial example is the group Z_n, the additive group of integers modulo n. In Z_n, 1 is always a generator:

$1 \equiv 1 \bmod n$

$1+1 \equiv 2 \bmod n$

$1+1+1 \equiv 3 \bmod n$

...

$1+1+1+...+1 \equiv n \equiv 0 \bmod n$

If a group is cyclic, then there may exist multiple generators. For example, we know Z_5 is a cyclic group. The element 1 is a generator for sure. And if we take a look at 2, we can find:

$2 \equiv 2 \bmod 5$

$2+2 \equiv 4 \bmod 5$

$2+2+2 \equiv 6 \equiv 1 \bmod 5$

$2+2+2+2 \equiv 8 \equiv 3 \bmod 5$

$2+2+2+2+2 \equiv 10 \equiv 0 \bmod 5$

So all the group elements $\{0,1,2,3,4\}$ in Z_5 can also be generated by 2. That is to say, 2 is also a generator for the group Z_5.

NOTE :

Not every element in a group is a generator. For example, the identity element in a group will never be a generator. No matter how many times you apply the group operator to the identity element, the only element you can yield is the identity element itself. For example, in Z_n, 0 is the identity element and $0+0+...+0 \equiv 0 \bmod n$ in all cases.

Cyclic groups

A group $(G, \cdot, e)$ is called *cyclic* if it is generated by a single element g. That is if every element of G is equal to

$$g^n = \begin{cases} gg\ldots g\ (n \text{ times}) & \text{if } n > 0 \\ e & \text{if } n = 0 \\ g^{-1}g^{-1}\ldots g^{-1}\ \ (|n| \text{ times}) & \text{if } n < 0 \end{cases}$$

Example 9.1. *$\mathbb{Z}$ is cyclic. It is generated by 1.*

Example 9.2. *$\mathbb{Z}_n$ is cyclic. It is generated by 1.*

Note: Cyclic Group means $\exists$ generator g.

Cyclic Group G

$$G = \langle g \rangle = \{g^0, g^{\pm 1}, g^{\pm 2}, g^{\pm 3}, \cdots\}$$

$$= \{g^0, g^1, g^{-1}, g^2, g^{-2}, \cdots\}$$

Q: Group of nth roots of unity is a cyclic group? (operation = mul)

Yes

$\{1\} \Rightarrow$ generator $g = 1$

$\{1, -1\} \Rightarrow g = -1$

$\{1, -1, i, -i\}$

$g = i, -i$

$\{1, \omega, \omega^2\} \Rightarrow g = \omega, \omega^2$

n^{th} Roots of unity :

$$\{1, \theta, \theta^2, \theta^3, \ldots, \theta^{n-1}\} \Rightarrow \text{Cyclic Group}$$

Generator $= \theta$

Q: Every Zn is a cyclic group? Yes.

Operation = $\oplus_n$

$Z_9 = \{1^0, 1^1, 1^2, 1^3, \ldots, 1^8\}$

$= \{0, 1, \ldots, 8\}$

Q: Every U_n is a cyclic group? — $\otimes_n$ operation

No

$(\{1, 2, 3, 4\}, \otimes_5) = U_5 = \text{cyclic}$

$U_8 =$ Not cyclic

Let $\mathbb{Z}_7^*$ be the set of nonzero elements in $\mathbb{Z}_7$ regarded as a group using (modular) multiplication. Show that it is cyclic by finding a generator.

Ans:

$\mathbb{Z}_7^* = U_7$

Operation = $\otimes_7$

cyclic

Generator $g =$

$U_7 = \{1, 2, 3, 4, 5, 6\}$, $\otimes_7$

Generators:

$2^{-1} = 4$ $\quad |4| = 3$

$|1| = 2$

$6^2 = 36 \bmod 7 = 1$

$\langle 1 \rangle = \{1\}$ $\quad |2| = 3$ so 2, 4 is not Generator

$|2| = 2^{(h?)} = 1$ $\quad 3$

$\langle 2 \rangle = \{2, 4, 1\}$

$|3| = 3^{6} = 1$ — smallest true integer

$3^{5} = 243 \bmod 7 = 5$

$3^{6} = 3^{5} * 3 = 5 * 3 = 15 \bmod 7 = 1$

$|3| = 6$ ⟹ 3 is the generator.

$3^{-1} = 5 \Rightarrow$ 3, 5 are Generators.

$|G| = 2$

$6^2 = 36 \bmod 7 = 1$

Q: finite Group G $|G| = n$

$\forall a$, $a^n = ? = e$

$\forall a$, $\boxed{a^n = e}$

Note

$U_7 = \{1, 2, 3, 4, 5, 6\}, \otimes_7$

$|U_7| = 6$

$1^6 = 1$

$2^6 = 1$

$3^6 = 1$

$4^6 = 1$

$5^6 = 1$

$6^6 = 1$

Generators = 3, 5

U_7 = cyclic group

Q: Every Cyclic Group is Abelian?

Ans: Yes.

Cyclic Group "G" means ∃ generator (g)

$$G = \langle g \rangle = \{ g^0, g^1, g^2, g^3, \ldots, g^{-1}, g^{-2}, \ldots \}$$

Cyclic Group G

g = generator

$G = \{ g^n \mid n \in Z \}$

$a, b \in G$; $a = g^m$, $b = g^p$

$ab = ba$? yes

$g^m g^p = g^p g^m$

$g^{p+m} = g^{p+m}$

So Every Cyclic Group is Abelian.

Q: Every Abelian Group is Cyclic?

Ans: No.

Ex: $(U_8, \otimes_8) = \{1, 3, 5, 7\}, \otimes_8$

Abelian

Not Cyclic

Q: Order of Smallest Group that is NOT Cyclic ?

Ans: 4

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Generator = a, b ← Cyclic? Yes.

$a^1 = a$; $a^2 = b$; $a^3 = a^2 a = ba = e$

Q: Order of Smallest Group that is Not Cyclic but Abelian?

Ans: 4

3.2.2 Cyclic groups

If g is an element of a group G, we define the powers g^n of G (for $n \in \mathbb{Z}$) as follows: if n is positive, then g^n is the product of n factors g; $g^0 = 1$; and $g^{-n} = (g^{-1})^n$. The usual laws of exponents hold: $g^{m+n} = g^m \cdot g^n$ and $g^{mn} = (g^m)^n$.

A *cyclic group* is a group C which consists of all the powers (positive and negative) of a single element. If C consists of all the powers of g, then we write $C = \langle g \rangle$, and say that C is *generated by* g.

Proposition 3.11 *A cyclic group is Abelian.*

Proof Let $C = \langle g \rangle$. Take two elements of C, say g^m and g^n. Then

$$g^m \cdot g^n = g^{m+n} = g^n \cdot g^m.$$

Let $C = \langle g \rangle$. Recall the *order* of g, the smallest positive integer n such that $g^n = 1$ (if such n exists – otherwise the order is infinite).

Q: If e is the Generator then

$G = 1 \Rightarrow$ Trivial Group

$|G| = 1$ $(G = \{e\}, *)$

4.4.22 Group Theory: GATE CSE 2009 | Question: 22 top

For the composition table of a cyclic group shown below:

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

Which one of the following choices is correct?

A. a, b are generators
B. b, c are generators
C. c, d are generators
D. d, a are generators

4.4.22 Group Theory: GATE CSE 2009 | Question: 22 top

For the composition table of a cyclic group shown below:

$c^1 = d$

$e = a$; e can never be the Generator

$b^1 = b$; $b^2 = bb = a = e$ so $|b| = 2$

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

Which one of the following choices is correct?

A. a, b are generators
B. b, c are generators
C. c, d are generators
D. d, a are generators

so b is not Gen.

$\langle b \rangle = \{a, b\}$

$c^1 = c$; $c^2 = cc = b$; $c^3 = c^2 c = bc = d$; $c^4 = bb = a = e$

$\{e, x, y, z\}$ — Cyclic Group

$x^{-1} = x$ $y^{-1} = z$

Generators: y, z

$\{e, x, y, z\}$ — Not cycle

$\forall a, \quad a^{-1} = a$

3. List all of the elements in each of the following subgroups.

(a) The subgroup of $\mathbb{Z}$ generated by 7

(b) The subgroup of $\mathbb{Z}_{24}$ generated by 15

(g) The subgroup generated by 3 in $U(20)$

(h) The subgroup generated by 5 in $U(18)$

(i) The subgroup of $\mathbb{R}^*$ generated by 7

(j) The subgroup of $\mathbb{C}^*$ generated by i where $i^2 = -1$

(k) The subgroup of $\mathbb{C}^*$ generated by $2i$

(l) The subgroup of $\mathbb{C}^*$ generated by $(1+i)/\sqrt{2}$

(m) The subgroup of $\mathbb{C}^*$ generated by $(1+\sqrt{3}\,i)/2$

3. List all of the elements in each of the following subgroups.

(a) The subgroup of $\mathbb{Z}$ generated by 7

(b) The subgroup of $\mathbb{Z}_{24}$ generated by 15

(g) The subgroup generated by 3 in $U(20)$

(h) The subgroup generated by 5 in $U(18)$

(i) The subgroup of $\mathbb{R}^*$ generated by 7

(j) The subgroup of $\mathbb{C}^*$ generated by i where $i^2 = -1$

(k) The subgroup of $\mathbb{C}^*$ generated by $2i$

(l) The subgroup of $\mathbb{C}^*$ generated by $(1+i)/\sqrt{2}$

(m) The subgroup of $\mathbb{C}^*$ generated by $(1+\sqrt{3}\,i)/2$

R^* = Non Zero Reals

C^* = Non Zero Complex numbers.

(a) $(Z, +)$

$\langle 7 \rangle = 7Z$

$\langle n \rangle = nZ$

$\langle 0 \rangle = \{0\}$

$|7| = \infty$

$|n| = \infty \; ; \; n \neq 0$

(b) $(Z_{24}, \oplus_{24})$

$15^2 = (15+15) \bmod 24$

15 ⇒ Not Generator

$\langle 15 \rangle = \{ 15^1, 15^2 = 6, 15^3 = 21, 15^4 = 12, 15^5 = 3, 15^6 = 18, 15^7 = 9, 15^8 = 0 \}$

$|15| = 8$

$15^4 = 15^2 \cdot 15^2 = 6 \cdot 6 = (6+6) \bmod 24 = 12$

$15^3 = (15^2)^6 \cdot 15 = (6+15) \bmod 24 = 21$

$\langle 15 \rangle = \{15, 6, 21, 12, 3, 18, 9, 0\}$

$|\langle 15 \rangle| = 8$; $5^{8} = 0$

$8 \rightarrow$ smallest +ve int.

(9) U_{20} ; $\langle 3 \rangle = ?$ operation = $(\times)_{20}$

$\langle 3 \rangle = \{ 3^1 = 3, 3^2 = 9, 3^3 = 7 ; 3^4 = 1 \}$ smallest +ve int

$3^{-1} = e$

$3^4 = 3^3 \cdot 3^1 = 7 \cdot 3 = 21 \bmod 20 = 1$

$|3| = 4$

$|U_{20}| = |\{1, 3, 7, 9, 11, 13, 17, 19\}| = 8$

U_{20} → 3 is NOT Generator

Hw: Is U_{20} a Cyclic Group?

(i) $(R^*, \times)$ $\quad \langle 7 \rangle = ?$ $\quad 7^{-1} = \frac{1}{7}$

$$\langle 7 \rangle = \{7^0 = 1, 7^1 = 7, 7^2 = 49, 7^3, 7^4, \ldots\}$$
$$7^{-1} = \frac{1}{7}, 7^{-2} = \frac{1}{49}, \ldots$$

$$\langle 7 \rangle = \{7^n \mid n \in Z\}$$

$|7| = \infty$

7 = Not generator

$(R^*, \times)$ — Cyclic Group? No

No g such that $\forall a$, $g^n = a$; for some n.

No Generator

$$(1+i)^2 = 1 + 2i + i^2 = 2i$$

$$(a+b)^2 = a^2 + 2ab + b^2$$

(1) $(C, C^*, \times)$ $\left\langle \frac{1+i}{\sqrt{2}} \right\rangle$ mul

$\left(\frac{1+i}{\sqrt{2}}\right)^0 = 1$; $\left(\frac{1+i}{\sqrt{2}}\right)^1 = \frac{1+i}{\sqrt{2}}$

$\left(\frac{1+i}{\sqrt{2}}\right)^2 = \frac{2i}{2} = i$

$$\left(\frac{1+i}{\sqrt{2}}\right)^3 = \left(\frac{1+i}{\sqrt{2}}\right) i = \frac{i-1}{\sqrt{2}}$$

$$\left(\frac{1+i}{\sqrt{2}}\right)^4 = i \cdot i = -1$$

$$\left(\frac{1+i}{\sqrt{2}}\right)^8 = 1 = e$$

$$\left|\frac{1+i}{\sqrt{2}}\right| = 8$$

$(C^*, \times)$ — ∞ Group

$\left|\frac{i+1}{\sqrt{2}}\right| = 8$

$\left\langle \frac{i+1}{2} \right\rangle = \{ \alpha, \alpha^2 = i, \alpha^3, \alpha^4 = -1, \alpha^5, \ldots, \alpha^8 = 1 \}$

α