MANIPAL UNIVERSITY JAIPUR

INSPIRED BY LIFE

(University under Section 2(f) of the UGC Act)

B.TECH SECOND YEAR

ACADEMIC YEAR: 2020-2021

COURSE NAME: ENGINEERING MATHEMATICS-III

COURSE CODE : MA 2101

LECTURE SERIES NO : 36 (THIRTY SIX)

CREDITS : 3

MODE OF DELIVERY : ONLINE (POWER POINT PRESENTATION)

FACULTY : DR. VIVEK SINGH

EMAIL-ID : vivek.singh@Jaipur.manipal.edu

PROPOSED DATE OF DELIVERY: 19 OCTOBER 2020

MANIPAL UNIVERSITY JAIPUR

VISION

Global Leadership in Higher Education and Human Development

MISSION

- Be the most preferred University for innovative and interdisciplinary learning
- Foster academic, research and professional excellence in all domains
- Transform young minds into competent professionals with good human values

VALUES

Integrity, Transparency, Quality,
Team Work, Execution with Passion, Humane Touch

SESSION OUTCOME

" TO UNDERSTAND THE CONCEPT OF ODE AND THEIR APPLICATIONS AND SOLVE THE PROBLEM"

ASSIGNMENT

QUIZ

MID TERM EXAMINATION –I & II

END TERM EXAMINATION

ASSESSMENT CRITERIA'S

PROGRAM OUTCOMES MAPPING WITH CO1

[PO1]

ENGINEERING KNOWLEDGE: APPLY THE KNOWLEDGE OF MATHEMATICS, SCIENCE, ENGINEERING FUNDAMENTALS, AND AN ENGINEERING SPECIALIZATION TO THE SOLUTION OF COMPLEX ENGINEERING PROBLEMS.

Cosets

- If H is a subgroup of(G, *) and a $\in$ G then the set

Ha = { h * a | h $\in$ H} is called a **right coset** of H in G.

Similarly aH = {a * h | h $\in$ H} is called a **left coset** of H is G.

- ***Note:-*** 1) Any two left (right) cosets of H in G are either identical or disjoint.
- 2) Let H be a subgroup of G. Then the right cosets of H form a partition of G. i.e., the union of all right cosets of a subgroup H is equal to G.

  3) **Lagrange's theorem:** The order of each subgroup of a finite group is a divisor of the order of the group.
- 4) The order of every element of a finite group is a divisor of the order of the group.
- 5) The converse of the lagrange's theorem need not be true.

Example

- **Ex.** If G is a group of order p, where p is a prime number. Then the number of subgroups of G is
- a) 1 b) 2 c) $p - 1$ d) p
- Ans. b
- **Ex.** Prove that every subgroup of an abelian group is abelian.
- **Solution:** Let $(G, *)$ be a group and H is a subgroup of G.
- Let $a, b \in H$
- $\Rightarrow a, b \in G$ (Since H is a subgroup of G)
- $\Rightarrow a * b = b * a$ (Since G is an abelian group)
- Hence, H is also abelian.

State and prove Lagrange's Theorem

Lagrange's theorem: The order of each subgroup H of a finite group G is a divisor of the order of the group.

Proof: Since G is finite group, H is finite.

- Therefore, the number of cosets of H in G is finite.
- Let $Ha_1, Ha_2, \ldots, Ha_r$ be the distinct right cosets of H in G.
- Then, $G = Ha_1 \cup Ha_2 \cup \ldots, \cup Ha_r$
- So that $O(G) = O(Ha_1) + O(Ha_2) \ldots + O(Ha_r)$.
- But, $O(Ha_1) = O(Ha_2) = \ldots\ldots = O(Ha_r) = O(H)$
- $\therefore O(G) = O(H) + O(H) \ldots + O(H)$. (r terms)
- $= r \cdot O(H)$
- This shows that O(H) divides O(G).

Lagrange's Theorem

Statement: The order of each subgroup of a finite group is a divisor of the order of the group.

i.e., Let H be a subgroup of a finite group G and let

$o(G) = n$ and $o(H) = m$, then

$m \mid n$ (m divides n)

Since, $f : H \longrightarrow aH$ and $f : H \longrightarrow Ha$ is one-one and onto.

$\Rightarrow o(H) = o(H) = m$

Now, $G = H \cup Ha \cup Hb \cup Hc \cup \ldots$, where a,b,c,...$\in G$

$\Rightarrow \quad o(G) = o(H) + o(Ha) + o(Hb) + \ldots$

$\Rightarrow \quad n = m + m + m + m + \ldots +$ upto p terms (say)

$$\Rightarrow \quad n = mp$$

$\Rightarrow$ Order of the subgroup of a finite group is a divisor of the order of the group.

÷ ÷ ÷

× The converse of Lagrange's theorem is not true.

e.g.,

- Consider the symmetric group P_4 of permutation of degree 4. Then $o(P_4) = 4! = 24$ Let A_4 be the alternative group of even permutation of degree 4. Then, $o(A_4) = 24/2 = 12$. There exist no subgroup H of A_4, such that $o(H) = 6$, though 6 is the divisor of 12.

Cyclic Groups

OBJECTIVES:

Recall	Recall the meaning of cyclic groups
Determine	Determine the important characteristics of cyclic groups
Draw	Draw a subgroup lattice of a group precisely
Find	Find all elements and generators of a cyclic group
Identify	Identify the relationships among the various subgroups of a group

The notion of a "group," viewed only 30 years ago as the epitome of sophistication, is today one of the mathematical concepts most widely used in physics, chemistry, biochemistry, and mathematics itself.

- ALEXEY SOSINSKY , 1991

A *Cyclic Group* is a group which can be generated by one of its elements.

That is, for some a in **G**,

$\mathbf{G}=\{a^n \mid \mathbf{n}$ is an element of $\mathbf{Z}\}$

Or, in addition notation,

$\mathbf{G}=\{na \mid n$ is an element of $\mathbf{Z}\}$

This element a

(which need not be unique) is called a *generator* of **G**.

Alternatively, we may write $\mathbf{G}=\langle a\rangle$.

EXAMPLES

- The set of integers Z under ordinary addition is cyclic. Both 1 and –1 are generators. (Recall that, when the operation is addition, 1^n is interpreted as

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ terms}}$$

when n is positive and as

$$\underbrace{(-1) + (-1) + \cdots + (-1)}_{|n| \text{ terms}}$$

when n is negative.)

- The set $Z_n = \{0, 1, \ldots, n-1\}$ for $n \geq 1$ is a cyclic group under addition modulo n. Again, 1 and $-1 = n-1$ are generators.

  Unlike Z, which has only two generators, Z_n may have many generators (depending on which n we are given).

- $Z_8 = \langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle$.

To verify, for instance, that $Z_8 = \langle 3\rangle$, we note that $\langle 3\rangle = \{3, 3 + 3, 3 + 3 + 3, \ldots\}$ is the set $\{3, 6, 1, 4, 7, 2, 5, 0\} = Z_8$. Thus, 3 is a generator of Z_8. On the other hand, 2 is not a generator, since $\langle 2\rangle=\{0, 2, 4, 6\} \neq Z_8$.

- $U(10) = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^3, 3^2\} = \langle 3 \rangle$. Also, $\{1, 3, 7, 9\} = \{7^0, 7^3, 7^1, 7^2\} = \langle 7 \rangle$. So both 3 and 7 are generators for $U(10)$.
- Quite often in mathematics, a “nonexample” is as helpful in understanding a concept as an example. With regard to cyclic groups, U(8) serves this purpose; that is, U(8) is not a cyclic group. Note that U(8) = {1, 3, 5, 7}. But

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

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

$$\langle 5 \rangle = \{5, 1\}$$

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

so $U(8) \neq \langle a \rangle$ for any a in U(8).

With these examples under our belts, we are now ready to tackle cyclic groups in an abstract way and state their key properties.

Properties of Cyclic Groups

- **Theorem4.1** Criterion for $a^i = a^j$
  Let G be a group, and let a belong to G. If a has infinite order, then $a^i a^j$ if and only if $i=j$. If a has finite order, say, n, then $<a> = \{e, a, a^2, \ldots, a^{n-1}\}$ and $a^i a^j$ if and only if n divides $i - j$.

PROOF Let G be a cyclic group generated by g . Let a, b be elements of G. We want to show that $ab = ba$. Now,

$a = g^m$ and $b = g^n$ for some integers a and b. So,

$ab = g^m g^n = g^{m+n}$ and $ba = g^n g^m = g^{n+m}$. But $m+n = n+m$

(addition of integers is commutative).

So $ab = ba$. ∎

EXAMPLES

(i) $(Z, +)$ is a cyclic group because $Z = \langle 1 \rangle$.

(ii) $(\{na \mid n \in Z\}, +)$ is a cyclic group, where a is any fixed element of Z.

(iii) $(Z_n, +_n)$ is a cyclic group because $Z_n = \langle [1] \rangle$. ■

- **Corollary 1** $|a| = |\langle a \rangle|$

  For any group element a, $|a| = |\langle a \rangle|$.

- **Corollary 2** $a^k = e$ Implies That $|a|$ Divides k

  Let G be a group and let a be an element of order n in G. If $a^k = e$, *then n divides k.*

Theorem 4.1 and its corollaries for the case $|a| = 6$ are illustrated in Figure 4.1.

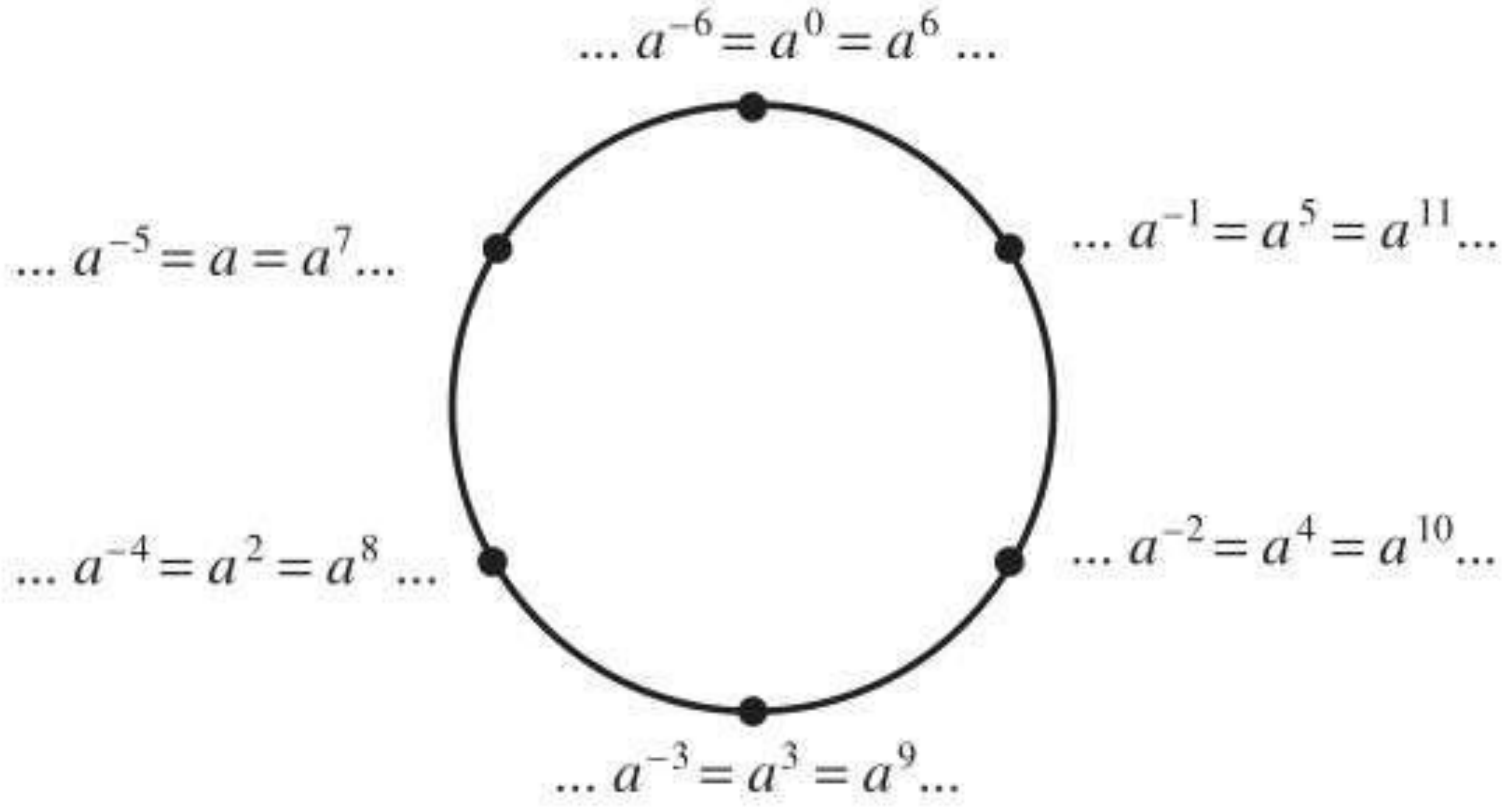


Figure 4.1

Theorem 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

- **Corollary 1** Orders of Elements in Finite Cyclic Groups

  In a finite cyclic group, the order of an element divides the order of the group.

- **Corollary 2** Criterion for $<a^i> = <a^j>$ and $|a^i| = |a^j|$

  Let $|a| = n$. Then $<a^i> = <a^j>$ if and only if $\gcd(n, i) = \gcd(n, j)$ and $|a^i| = |a^j|$ if and only if $\gcd(n, i)$ 5 $\gcd(n, j)$.

- **Corollary 3** Generators of Finite Cyclic Groups

  Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$ and $|a| = |\langle a^j \rangle|$ if and only if $\gcd(n, j) = 1$.

- **Corollary 4** Generators of Z_n

  An integer k in Z_n is a generator of Z_n if and only if $gcd(n, k) = 1$.

Classification of Subgroups of Cyclic Groups

Theorem 4.3

Fundamental Theorem of Cyclic Groups

- Every subgroup of a cyclic group is cyclic. Moreover, if |<a>| = n, then the order of any subgroup of <a> is a divisor of n; and, for each positive divisor k of n, the group <a> has exactly one subgroup of order k
- —namely, <$a^{n/k}$>.

Corollary Subgroups of Z_n

For each positive divisor k of n, the set <n/k> is the unique subgroup of Z_n of order k; moreover, these are the only subgroups of Z_n.

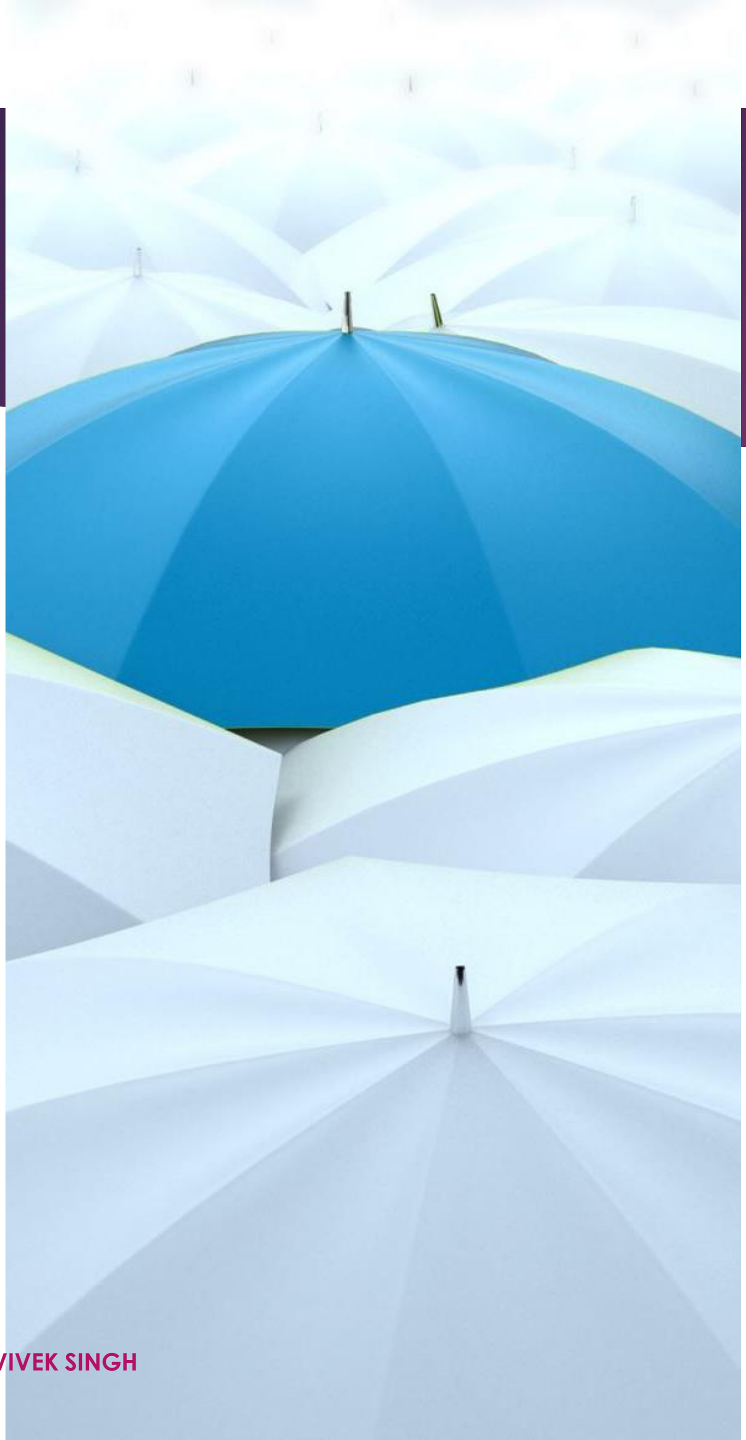
EXAMPLE The list of subgroups of *Z*30 is

- <1>= {0, 1, 2, . . . , 29} order 30,
- <2>= {0, 2, 4, . . . , 28} order 15,
- <3>= {0, 3, 6, . . . , 27} order 10,
- <5>= {0, 5, 10, 15, 20, 25} order 6,
- <6>= {0, 6, 12, 18, 24} order 5,
- <10>= {0, 10, 20} order 3,
- <15>= {0, 15} order 2,
- <30>= {0} order 1.

Theorem 4.4

Number of Elements of Each Order in a Cyclic Group

If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\varphi(d)$.



Corollary: Number of Elements of Order *d* in a Finite Group

- In a finite group, the number of elements of order d is divisible by φ (d).

The lattice diagram for Z_{30} is shown in Figure 4.2. Notice that <10> is a subgroup of both <2> and <5>, but <6> is not a subgroup of <10>.

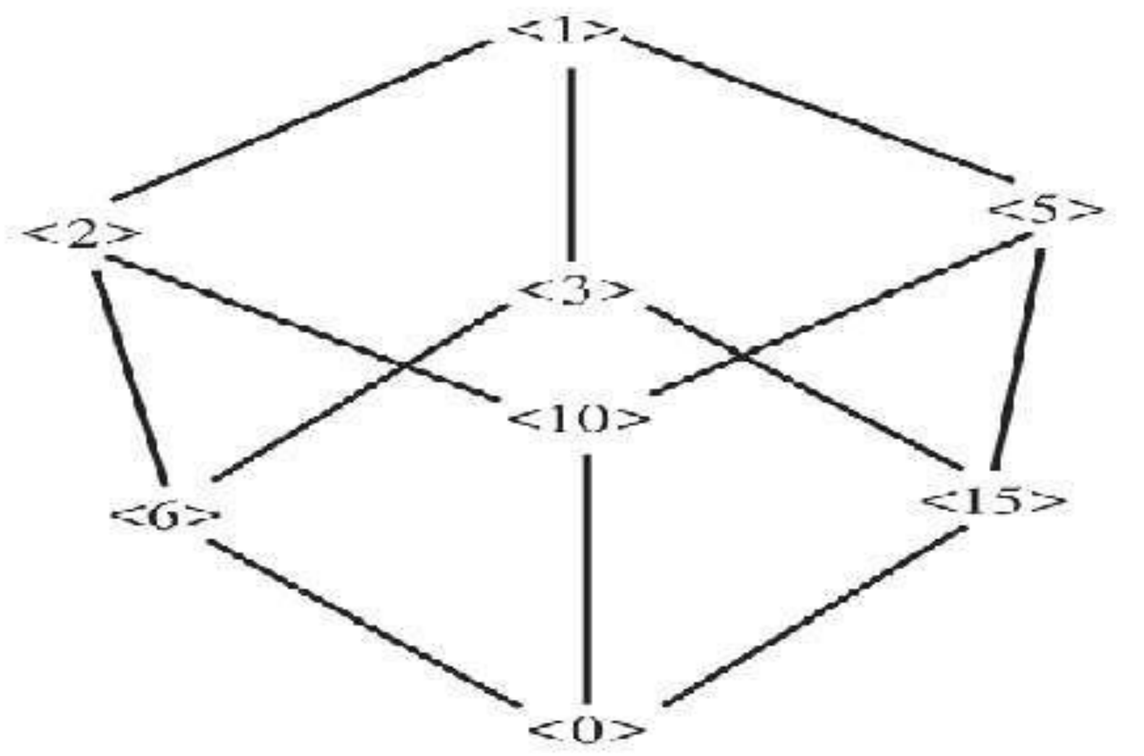


Figure 4.2 Subgroup lattice of Z_{30}.

THANK YOU

18

?

18