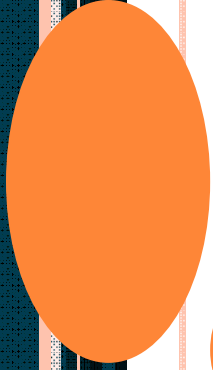
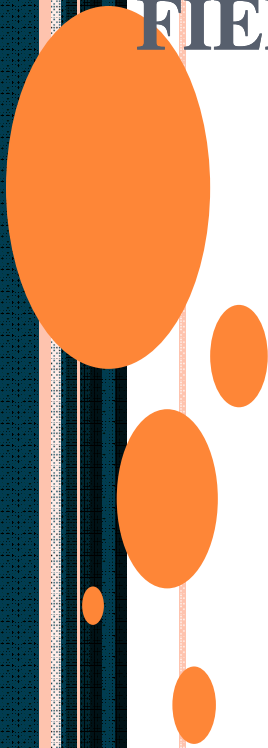


# DISCRETE STRUCTURE



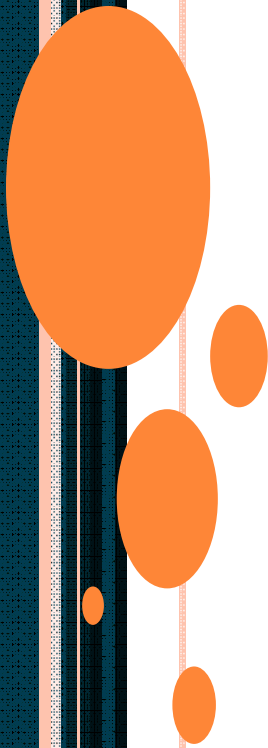
# LECTURE-20

## NORMAL SUB GROUP, CYCLIC GROUP ,INTEGRAL DOMAIN & FIELD



# TOPICS COVERED

- ❑ Introduction to Normal sub group
- ❑ Cyclic group
- ❑ Integral domain & field



# NORMAL SUBGROUPS

Let  $\langle H, \bullet \rangle$  be a subgroup of  $\langle G, \bullet \rangle$ . Then  $\langle H, \bullet \rangle$  is a normal subgroup if, for any  $a \in G$ , the left coset  $a \bullet H$  is equal to the right coset  $H \bullet a$

$\bullet$	$\alpha$	$\beta$	$\gamma$	$\delta$	$\varepsilon$	$\zeta$
$\alpha$	$\alpha$	$\beta$	$\gamma$	$\delta$	$\varepsilon$	$\zeta$
$\beta$	$\beta$	$\gamma$	$\alpha$	$\varepsilon$	$\zeta$	$\delta$
$\gamma$	$\gamma$	$\alpha$	$\beta$	$\zeta$	$\delta$	$\varepsilon$
$\delta$	$\delta$	$\zeta$	$\varepsilon$	$\alpha$	$\gamma$	$\beta$
$\varepsilon$	$\varepsilon$	$\delta$	$\zeta$	$\beta$	$\alpha$	$\gamma$
$\zeta$	$\zeta$	$\varepsilon$	$\delta$	$\gamma$	$\beta$	$\alpha$

$\langle H, \bullet \rangle$  is a normal subgroup where  $H = \{\alpha, \beta, \gamma\}$

e.g.  $\delta \bullet H = \{\delta \bullet \alpha, \delta \bullet \beta, \delta \bullet \gamma\} = \{\delta, \zeta, \varepsilon\}$

$H \bullet \delta = \{\alpha \bullet \delta, \beta \bullet \delta, \gamma \bullet \delta\} = \{\delta, \varepsilon, \zeta\}$

**Theorem:** In an Abelian group, every subgroup is a normal subgroup

## CYCLIC GROUP

- A group  $G$  is called cyclic if there exists an element  $g$  in  $G$  such that  $G = \langle g \rangle = \{ g^n \mid n \text{ is an integer} \}$ . Since any group generated by an element in a group is a subgroup of that group, showing that the only subgroup of a group  $G$  that contains  $g$  is  $G$  itself suffices to show that  $G$  is cyclic.



## EXAMPLE OF CYCLIC GROUP

- For example, if  $G = \{ g^0, g^1, g^2, g^3, g^4, g^5 \}$  is a group, then  $g^6 = g^0$ , and  $G$  is cyclic. In fact,  $G$  is essentially the same as (that is, isomorphic to) the set  $\{ 0, 1, 2, 3, 4, 5 \}$  with addition modulo 6. For example,  $1 + 2 \equiv 3 \pmod{6}$  corresponds to  $g^1 \cdot g^2 = g^3$ , and  $2 + 5 \equiv 1 \pmod{6}$  corresponds to  $g^2 \cdot g^5 = g^7 = g^1$ , and so on. One can use the isomorphism  $\chi$  defined by  $\chi(g^i) = i$ .



# CYCLIC GROUP

- For every positive integer  $n$  there is exactly one cyclic group (up to isomorphism) whose order is  $n$ , and there is exactly one infinite cyclic group (the integers under addition). Hence, the cyclic groups are the simplest groups and they are completely classified.
- The name "cyclic" may be misleading: it is possible to generate infinitely many elements and not form any literal cycles; that is, every  $g^n$  is distinct. (It can be said that it has one infinitely long cycle.) A group generated in this way is called an **infinite cyclic group**, and is isomorphic to the additive group of integer  $\mathbf{Z}$ .



# CYCLIC GROUP

- Furthermore, the circle group (whose elements are uncountable) is *not* a cyclic group—a cyclic group always has countable elements.
- Since the cyclic groups are abelians, they are often written additively and denoted  $\mathbf{Z}_n$ . However, this notation can be problematic for number theorists. The quotient notations  $\mathbf{Z}/n\mathbf{Z}$ ,  $\mathbf{Z}/n$ , and  $\mathbf{Z}/(n)$  are standard alternatives. We adopt the first of these here to avoid the collision of notation.
- One may write the group multiplicatively, and denote it by  $C_n$ , where  $n$  is the order (which can be  $\infty$ ). For example,  $g^2g^4 = g^1$  in  $C_5$ , whereas  $2 + 4 = 1$  in  $\mathbf{Z}/5\mathbf{Z}$ .
- Properties





# INTEGRAL DOMAINS AND FIELDS

$\langle A, \oplus, \bullet \rangle$  is an *integral domain* if it is a commutative ring with unity that also satisfies the following property;

$$\forall x, y \in A \quad x \bullet y = 0 \Rightarrow x = 0 \text{ or } y = 0$$

$\langle \mathbb{Z}, +, \times \rangle$  is also an integral domain

$\langle A, \oplus, \bullet \rangle$  is a *field* if:

- (1)  $\langle A, \oplus \rangle$  is an Abelian group
- (2)  $\langle A - \{0\}, \bullet \rangle$  is an Abelian group
- (3) The operation  $\bullet$  is distributive over the operation  $\oplus$

Example: The set of real numbers with respect to  $+$  and  $\times$  is a field.

$\langle \mathbb{Z}, +, \times \rangle$  is not a field. Why?



## A FIELD IS AN INTEGRAL DOMAIN

Let  $\langle A, \oplus, \bullet \rangle$  be a field then certainly  $\langle A, \oplus, \bullet \rangle$  is a commutative ring with unity. Hence, it only remains to prove that

$$\forall x, y \in A \quad x \bullet y = 0 \Rightarrow x = 0 \text{ or } y = 0$$

Now suppose  $x \bullet y = 0$  then if  $x=0$  the above holds. Consider the case then where  $x \neq 0$

Since  $\langle A - \{0\}, \bullet \rangle$  is an Abelian group then it must contain an inverse to  $x$ ,  $x^{-1}$ , for which the following holds

$$y = 1 \bullet y = (x^{-1} \bullet x) \bullet y = x^{-1} \bullet (x \bullet y) = x^{-1} \bullet 0$$

Now

$$a \bullet (0 \oplus 0) = a \bullet 0$$

$$\Rightarrow a \bullet 0 \oplus a \bullet 0 = a \bullet 0 \text{ (distributivity)}$$

$$\Rightarrow a \bullet 0 \oplus a \bullet 0 = a \bullet 0 \oplus 0 \text{ (0 is identity)}$$

$$\Rightarrow a \bullet 0 = 0 \text{ (cancellation laws for } \oplus)$$

Therefore  $y=0$  as required

# PROPERTIES

**Theorem:** if  $\langle A, \oplus, \bullet \rangle$  is a ring. Then

$$\forall x \in A \quad 0 \bullet x = x \bullet 0 = 0$$

**Proof:** as for previous argument

Let  $-x$  denote the inverse of  $x$  under  $\oplus$

**Theorem:** if  $\langle A, \oplus, \bullet \rangle$  is a ring then the following hold

$$(i) \quad (-x) \bullet y = x \bullet (-y) = -(x \bullet y)$$

$$(ii) \quad (-x) \bullet (-y) = x \bullet y$$

**Proof:** (i)

$$(x \oplus (-x)) \bullet y = 0 \bullet y \text{ (additive inverse)}$$

$$= 0 \text{ (by above theorem)}$$

$$\Rightarrow x \bullet y \oplus (-x) \bullet y = 0 \text{ (distributivity)}$$

$$\Rightarrow (-x) \bullet y = -(x \bullet y) \oplus 0 \text{ (division laws for } \oplus \text{)}$$

$$= -(x \bullet y) \text{ (additive identity)}$$



$$\begin{aligned}
 \text{(ii)} \quad & (-x) \bullet (-y) = -(x \bullet (-y)) \text{ (part(i))} \\
 & = (-(- (x \bullet y))) \text{ (part(i))} \\
 & = x \bullet y \text{ (double inverse)}
 \end{aligned}$$

for both (i) and (ii) the symmetric cases are proved similarly

**Theorem:** suppose that elements  $a, b$  and  $c$  of an integer domain satisfy  $a \bullet b = a \bullet c$  and  $a \neq 0$  then  $b=c$ .

**Proof:**

$$a \bullet b \oplus -(a \bullet c) = a \bullet c \oplus -(a \bullet c) = 0 \text{ (additive inverse)}$$

$$\text{Now } -(a \bullet c) = a \bullet (-c) \text{ (prev. theorem)}$$

$$\therefore a \bullet (b \oplus -c) = 0 \text{ (distributivity)}$$

$$\Rightarrow (b \oplus -c) = 0 \left( \begin{array}{l} \text{by defn. of integer domain} \\ \text{since } a \neq 0 \end{array} \right)$$

$$\Rightarrow b = 0 \oplus (-(-c)) \text{ (by devision law for } \oplus)$$

$$\Rightarrow b = c \text{ (double inverse)}$$



# APPLICATION & SCOPE OF RESEARCH

- Coding Theory
- Cryptography

