CS201: DISCRETE COMPUTATIONAL STRUCTURES	**Semester III**

Module III

Lecturer: Jestin Joy *Class: CSE-B*

Syllabus: *Groups, definition and elementary properties, subgroups, Homomorphism and Isomorphism, Generators - Cyclic Groups, Cosets and Lagrange's Theorem Algebraic systems with two binary operations- rings, fields-sub rings, ring homomorphism*

Disclaimer: *These may be distributed outside this class only with the permission of the Instructor.*

Federal Institute of Science And Technology (FISAT)

Contents

3.1 Groups

Group is special type of Monoid that has applications in Mathematics, Physics,and Chemistry etc.

Definition 3.1 *A Group $(G, *)$ is a monoid ,with identity e, that has the additional property that for every element $a \in G$ there exists an element a' such that $a * a' = a' * a = e$.*

Thus a Group is a set together with operation * on G such that

1. For all a, b in G, the result of the operation, $a * b$, is also in G
2. $(a * b) * c = a * (b * c)$ for any elements$a, b,$and c in G.
3. There is a unique element$e$in G such that $a * e = e * a$ for any $a \in G$
4. For every $a \in G$, there is an element $a' \in G$, called inverse of a such that $a * a' = a' * a = e$

We shall write the product $a * b$ of the elements a and b in the group $(G, *)$ simply as ab ,and we shall also refer to $(G, *)$ simply as G. A Group is said to be Abelian if $ab = ba$ for all elements a and b in G.

Examples of Group include

- $(Z, +)$
- $(Q, +)$
- $(R, +)$
- $(C, +)$
- (Q^*, X) : Q^* is the set of non zero rationals and X is the multiplication operation

3.2 Subgroups

Given a group G under a binary operation $*$, a **subset** H of G is called a subgroup of G if H also forms a group under the operation $*$.

For the group $(Z_8, +)$, $(\{0, 4\}, +)$ and $(\{0, 2, 4, 6\}, +)$ are subgroups.

3.3 Isomorphism and Homomorphism

Let $(S, *)$ and $(T, *')$ be two groups . A function $f : S \to T$ is called an Isomorphism from $(S, *)$ to $(T, *')$ if it is a one-to-one correspondance (one-one and onto) from S to T ,and if

$$f(a * b) = f(a) *' f(b)$$

for all a, b in S.

Let $(S, *)$ and $(T, *')$ be two groups .A function$f : S \to T$ is called Homomorphism from $(S, *)$ to $(T, *')$ if

$$f(a * b) = f(a) *' f(b)$$

for all a and b in S.

3.4 Cyclic Group

Definition 3.2 *A group G is called cyclic if there is an element $x \in G$, such that for each $a \in G$,$a = x^n$ for some $n \in Z$.*

*Such an element x is called a **generator** of G.*

We may indicate that G is a cyclic group generated by x, by writing $G =< x >$.

Example: The group $H = (Z_4, +)$ is cyclic. Here, the operation is addition.

We can find that both 1 and 3 generate H. For the case of 3 ,we have

- 1 mod 4=1
- (1+1)mod 4=2
- (1+1+1)mod 4=3
- (1+1+1+1)mod 4=0

Since 1 generates all the elements of Z_4 we can say that 1 is a generator.

Like wise 3 is also a generator.

Therefore $H =< 1 >=< 3 >$

Example: Consider the multiplicative group , $U_9 = 1, 2, 4, 5, 7, 8$. Here we find that $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 7, 2^5 = 5, 2^6 = 1$.

So U_9 is a cyclic group of order 6 and $U_9 =< 2 >$.It is also true that $U_9 =< 5 >$ because

- 5^1 mod 9=5
- 5^2 mod 9=7
- 5^3 mod 9=8
- 5^4 mod 9=4
- 5^5 mod 9=2
- 5^6 mod 9=1

3.5 Cosets and Lagrange's Theorem

Let $(A, *)$ be an algebraic system , where $*$ is a binary operation.Let a be an element in A and H be a subset of A. The left coset of H with respect to a , which we shall denote aH is the set of elements $\{a * x \mid x \in H\}$.

Similarly the right coset of H with respect to a , which we shall denote Ha is the set of elements $\{x * a \mid x \in H\}$.

Example 1

Let $G = S_3$ and $H\{(1), (13)\}$. Then the left coset of H in G are:

$(1)H = H$

$(12)H = \{(12), (12)(13)\} = \{(12), (132)\} = (132)H$

$(13)H = \{(13), (1)\} = H$

$(23)H = \{(23), (23)(13)\} = |(23), (123) = (123)H$

Example 2:

Let $H = \{0, 3, 6\}$ in Z_9 under addition. In the case that the group operation is addition , we use the notation $a + H$ instead of aH . Then the cosets of H in Z_9 are:

$0 + H = \{0, 3, 6\} = 3 + H = 6 + H,$

$1 + H = \{1, 4, 7\} = 4 + H = 7 + H,$

$2 + H = \{2, 5, 8\} = 5 + H = 8 + H$

A subgroup H of a group G is normal in G if and only if $aH = Ha$ for all a in G; i.e., the sets of left and right cosets coincide.

3.5.1 Langrange's Theorem

Definition 3.3 *If G is a finite group of order n with H a subgroup of order m , then m divides n (or equivalently $|H| divides |G|$). Also the number of cosets is equal to $\frac{G}{H}$*

3.6 Algebraic Systems with two binary properties

3.6.1 Rings

Definition 3.4 *Let S be a non empty set with two binary operations $+$ and $*$.The structure $(S, +, *)$ is called a Ring if*

1. *$(S, +)$ is abelian*
2. *$(S, *)$ is a semigroup*
3. ** is distributive over +. That is for any $a, b, c \in S$*
   - $a * (b + c) = a * b + a * c$
   - $(b + c) * a = b * a + c * a$

Example: The set $Z_n = \{0, 1, ...n - 1\}$ under addition and multiplication modulo n is a commutative ring with unity 1.

- If * is commutative, then it is called **commutative ring**
- If * is a monoid. Then it is a **ring with identity**

3.6.2 Fields

Definition 3.5 *Suppose that F is a commutative ring with identity . We say that F is a Field if every **non-zero** element x in F has a multiplicative inverse.*

3.6.3 Field Properties

F has two binary operations; an addition $+$ and a multiplication $*$, and has two special elements denoted by 0 and 1, so that for all x, y and z in F.

1. $x + y = y + x$
2. $x * y = y * x$
3. $(x + y) + z = x + (y + z)$
4. $(x * y) * z = x * (y * z)$
5. $x + 0 = x$
6. $x * 1 = x$
7. $x * (y + z) = (x * y) + (x * z)$
8. $(y + z) * x = (y * x) + (z * x)$
9. For each x in F there is a unique element in F denoted by $-x$ so that $x + (-x) = 0$
10. For each $x \neq 0$ in F there is a unique element in F denoted by x^{-1} so that $x * x^{-1} = 1$

Example : $(Z_5, +, *)$,$(Z_7, +, *)$, where is + is modulo addition and * is modulo multiplication.

3.7 Subrings

Subsets of rings which are themselves rings are called **subrings**. So a non empty subset B of a ring A with respect to operation $+$ is a subring of A if and only if B satisfies all conditions needed for a ring.

3.7.1 Properties of Subrings

1. A subring of a commutative ring is a commutative ring.
2. A subring of a is a ring in its own right.

Example 2: $\{0, 2, 4\}$ is a subring of the ring Z_6, the integers modulo 6.

3.8 Ring Homomorphism

Definition 3.6 *A ring homorphism ϕ from a ring R to ring S is a mapping from R to S that preserves the two ring operations ; that is , for all a, b in R, $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ A ring homomorphism that is both one-to-one and onto is called ring isomorphism.*

An isomorphism is used to show that two rings are algebraically identical; a homomorphism is used to simplify a ring while retaining certain of its features.

Example 1:

For any positive integer n, the mapping $k \to k$ mod n is a ring homomorphism from Z to Z_n. This mapping is called the natural homomorphism from Z to Z_n.

try it now

A KTU STUDENTS PLATFORM

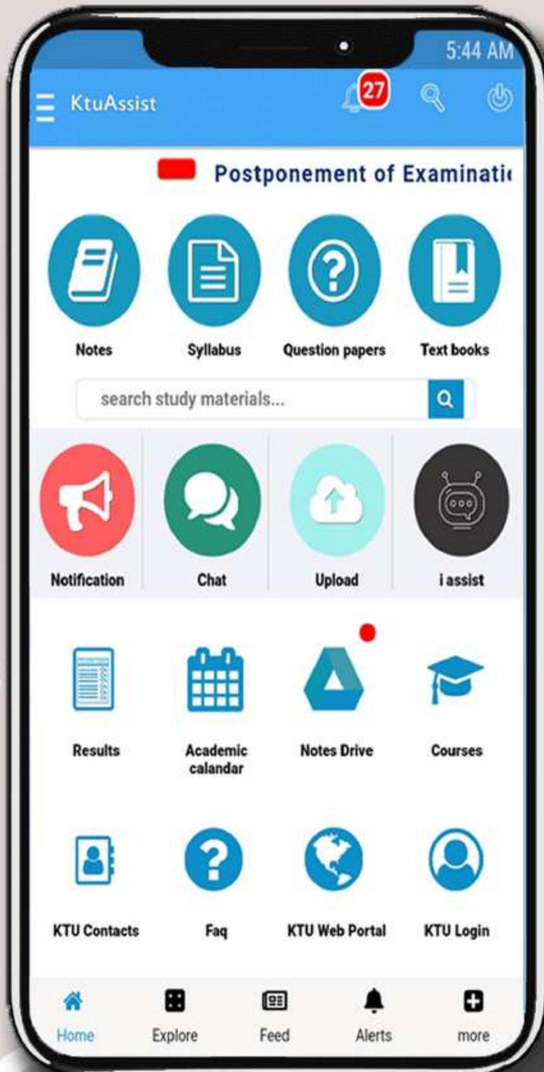
SYLLABUS

NOTES

TEXT BOOKS

QUESTION PAPERS

KTU NOTIFICATION



DOWNLOAD IT FROM GOOGLE PLAY

CHAT

CALENDAR

FAQ

LOGIN

MUCH MORE

DOWNLOAD APP

ktuassist.in

instagram.com/ktu_assist

facebook.com/ktuassist