CS201: DISCRETE COMPUTATIONAL STRUCTURES **Semester III**

Module III

Syllabus: ***Algebraic Systems:-*** *Groups, definition and elementary properties , subgroups, Homomprphism and Isomorphism , Generators -Cyclic groups , Cosets and Langrange'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.*

Contents

1.1 Groups

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

Definition and Elementary properties

Definition 1.1 *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 binary operation * on G such that

1. $a * b \in G$. (Closure of G under *)
2. $(a * b) * c = a * (b * c)$ for any elementsa, b,and c in G. (The associative Property)
3. There is a unique element e in G such that $a * e = e * a$ for any $a \in G$. (The existance of an Identity)

4. For every $a \in G$, there is an element $a^{'} \in G$, called inverse of a such that $a * a^{'} = a^{'} * a = e$.(The existance of Inverse)

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.

Example 1:

The set of integers Z , The set of rational numbers Q , and the set of Real numbers R are all groups under ordinary addition. In each case , the Identity is 0 and inverse of a is $-a$.

Example 2:

The set of integers under ordinary multiplication is not a group. Since the number 1 is the identity , property of inverse fails. For example, there is no integer b such that $5b = 1$.

Example 3:

The set Q^{+} of positive rationals is a group under ordinary multiplication. The inverse of any a is $1/a = a^{-1}$.

1.2 Subgroups

Definition 1.2 *Let H be a subset of a Group G such that*

- *The identity e of G belongs to H*
- *If a and b belong to H , then $ab \in H$*
- *If $a \in H$, then $a^{-1} \in H$*

Then H is called a subgroup of G.

For any element a, from a group we let $< a >$ denote the set $\{a^n | n \in Z\}$.

Let G be a group, and let a be any element of G. Then ,$< a >$ is a subgroup of G.

1.3 Isomorphism and Homomorphism

Let $(S, *)$ and $(T, *^{'})$ be two semigroups . A function $f : S \rightarrow T$ is called an Isomorphism from $(S, *)$ to $(T, *^{'})$ if it is a one-to-one correspondance 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 semigroups .An every-where defined function$f : S \rightarrow T$ is called Homomorphism from $(S, *)$ to $(T, *^{'})$ if $f(a * b) = f(a) *' f(b)$ for all a and b in S.

Iff is onto, we say that T is a homomorphic image of S.

1.4 Cyclic Group

Definition 1.3 *A group that has a generating set consisting of a single element is known as a Cyclic Group. 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: For the example of the rotation of geometric figures in the plane, the group $\{0, 60, 120, 180, 240, 300, \bigstar\}$ is a cyclic group.

Example: The group $H = (Z4, +)$ is cyclic. Here, the operation is addition ,so we have multiples instead of powers .

we find that both [1] and [3] generate H. For the case of [3] ,we have 1.[3]=[3], 2.[3](=[3]+[3])=[2], 3.[3]=[1], and 4.[3]=[0] .

Hence H=<[3]>=<[1]>.

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

1.5 Cosets and Lagrange's Theorem

Let $\{A, \bigstar\}$ be an algebraic system , where $\bigstar$ 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 $a\bigstar H$ is the set of elements $\{a\bigstar x \mid x \in H\}$.

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

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 $H = \{0, 3, 6\}$ inZ_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:

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

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

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

Langrange's Theorem

Definition 1.4 *If G is a finite group of order n with H a subgroup of order m , then m divides n.*

1.6 Algebraic Systems with two binary properties

1.6.1 Rings

Definition 1.5 *Let S be a non empty set with two binary operations $+$ and $*$ such that $(S, +)$ is an Abelian Group and $*$ is distributive over $+$.The structure $(S, +, *)$ is called a Ring if $*$ is associative. If $*$ is associative and commutative , we call $(S, +, *)$ a commutative ring. If $(S, *)$ is a monoid then $(S, +, *)$ is a ring with identity.*

Example: The set Z of integers under ordinary addition and multiplication is a commutative ring with unity 1 . The units of Z are 1 and -1.

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

1.6.2 Fields

Definition 1.6 *Suppose that F is a commutative ring with identity . We say that F is a Field if every nonzero element x in F has a multiplicative inverse.*

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 Fdenoted 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 :

For every prime p, Z_p , the ring of integers modulo p , is a field.

1.7 Subrings

A name can be given to the subsets of a ring which are themselves rings, just like in case of groups. So a non empty subset B of a ring A with respect to operation $+$ and is a subring of A if and only if B satisfies all conditions needed for a ring.

Definition 1.7 *Let be A ring and B a nonempty subset of A. Then $(B, +, *)$ is a subring of $(A, +, *)$ if and only if*

- $a + b \in B$, *for all* $a, b \in B$,
- $-a \in B$ *, for* $a \in B$,
- $a * b \in B$ *, for* $a, b \in B$

Properties of Subrings

1. Every ring has two trivial subrings: the ring itself and the set 0
2. A subring of a commutative ring is a commutative ring.
3. If A is a ring and Bi is an arbitrary collection of subrings of A, then Bi is a subring of A.

4. If A is a ring and B is a subset of A then, the intersection of all subrings of A that contains B , is a subring of A. It is called the subring generated by B.

5. A subring of a is a ring in its own right.

Example 1: $\{0\}$ and R are subrings of any ring $R.\{0\}$ is called the trivial subring of R.

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

1.8 Ring Homomorphism

Definition 1.8 *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.

Properties of Ring Homomorphism

1. For any $r \in R$ and any positive integer $n, \phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$
2. $\phi(A) = \{\phi(a)|a \in A\}$ is a subring of S.
3. If A is an ideal and ϕ is onto S , then $\phi(A)$ is an ideal.
4. $\phi^{-1}(B) = \{r \in R|\phi(r) \in B\}$ is an ideal of R.
5. If R is commutative , then $\phi(R)$ is commutative.
6. If R has a unity 1, $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S
7. ϕ is an isomorphism if and only if ϕ is onto and $Ker\phi = \{r \in R|\phi(r) = 0\} = \{0\}$
8. If ϕ is an isomorphism from R to S , then ϕ^{-1} is an isomorphism from S onto R.

Example 1:

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

Example 2:

The mapping $a + bi \longrightarrow a - bi$ is a ring isomorphism from complex numbers onto the complex numbers.