SRI BHARATHI ARTS & SCIENCE COLLEGE FOR WOMEN

KAIKKURICHI

Abstract Algebra

SUB CODE: 16SCCMM12

Unit - I

1) Define group.

A non-empty set G together with a binary operation $*: G \times G \to G$ is called a group. if the following conditions are satisfied.

(i) $*$ is associative (i.e.) $a*(b*c) = (a*b)*c \ \forall a,b,c \in G$.

(ii) $\exists$ an element $e \in G \ni: a*e = e*a = a \ \forall a \in G$.

(iii) For any element a in G $\exists$ an element $a' \in G \ni:$ $a*a' = a'*a = e$. a' is called the inverse of a.

2) Define Addition modulo & multiplication modulo.

let $Z_n = \{0, 1, 2, \dots, n-1\}$.

let $a, b \in Z_n$. let $a+b = qn + r$ where $0 \le r < n$.

we define $a \oplus b = r$.

let $ab = q'n + s$ where $0 \le s < n$.

we define $a \odot b = s$

The binary operations $\oplus$ and $\odot$ are called addition modulo n and multiplication modulo n respectively.

3) Define abelian.

A Group G is said to be abelian if $ab = ba \ \forall a, b \in G$.

A Group which is not abelian is called a non-abelian group.

ex: Z, Q, R and C usual addition are abelian groups.

4) Define Left identity & right identity.

Let $*$ be a binary operation defined on G.

An element $e \in G$ is called a left identity if $e * a = a \ \forall a \in G$.

2

e is called a right identity if $a * e = a \ \forall a \in G$.

eg: In N we define $a * b = a$. Here every element is a right identity.

5) Define permutation.

Let A be a finite set. A bijection from to itself is called a permutation of A.

For ex: if $A = \{1,2,3,4\}$ $f : A \to A$ given by $f(1) = 2$, $f(2) = 1$, $f(3) = 4$ and $f(4) = 3$ is a permutation of A.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

An element in the bottom row is the image of the element just above it in the upper row.

unit-II

1) Define Improper subgroup.

Let G be any group. Then $\{e\}$ and G are subgroup of G. They are called improper subgroups of G.

eg: $(Q,+)$ is a subgroup of $(R,+)$ ad $(R,+)$ is a subgroup of $(C,+)$.

2) Define cyclic group.

Let G be a group. Let $a \in G$. 3

Then $H = \{a^n / n \in Z\}$ is a subgroup of G.

H is called the cyclic group of G Generated by a and is denoted by $\langle a \rangle$.

ex: In $(Z, +)$, $\langle 2 \rangle = 2Z$ which is the group of even integers.

3) Define Left coset & right coset:

Let H be a subgroup of a group G. Let $a \in G$.

Then the set $aH = \{ah / h \in H\}$ is called the left coset of H defined by a in G.

||^{ly} $Ha = \{ha / h \in H\}$ is called the right coset of H defined by a.

4) Let $a \in R^*$. Let $H = \{a^n / n \in Z\}$. Then H is a subgroup of R^*.

Clearly H is non-empty.

Now, let $x, y \in H$.

Then $x = a^s$ and $y = a^t$ where $s, t \in Z$.

$\therefore xy^{-1} = a^s (a^t)^{-1} = a^{s-t} \in H$.

Hence H is a subgroup of R^*.

5) Let G be a group and H be a subgroup of G. Then

(i) $a \in H \Rightarrow aH = H$.

Let $a \in H$. We claim that $aH = H$.

Let $x \in aH$. Then $x = ah$ for some $h \in H$.

Now, $a \in H$ and $h \in H \Rightarrow ah = x \in H$.

Hence $aH \subseteq H$.

Let $x \in H$. Then $x = a(a^{-1}x) \in aH$.

Hence $H \subseteq aH$. Thus $H = aH$.

4

Conversely, let $aH = H$. Now $a = ae \in aH$.

$\therefore a \in H$.

unit - II

1) Define Normal subgroup.

A subgroup H of G is called a normal subgroup of G if $aH = Ha \; \forall \; a \in G$.

ex: For any group G, $\{e\}$ and G are normal subgroups.

2) Define quotient group.

let N be a normal subgroup of G. Then the group G/N is called the quotient group (factor group) of G modulo N.

Ex: $3z$ is a normal subgroup of $(z,+)$.

3) Define Isomorphism.

let G & G' be two groups. A map $f: G \to G'$ is called an isomorphism if

(i) f is a bijection.

(ii) $f(xy) = f(x)f(y) \; \forall \; x,y \in G$

4) Define inner automorphism.

The automorphism $\phi_a : G \to G$ defined in the inner is called an inner automorphism of the group G.

5) Define homomorphism.

A map f from a group G into a group G' is called a homomorphism if $f(ab) = f(a)f(b)$ $\forall$ $a, b \in G$.

ex: $f:(Z,+) \rightarrow (Z,+)$ defined by $f(x) = 2x$ is a homomorphism. For, $f(x+y) = 2(x+y) = 2x+2y = f(x)+f(y)$

Note that f is 1-1

5

Unit - IV

1) Define ring

A nonempty set R together with two binary operations denoted by '+' and '·' and called addition and multiplication which satisfy the following axioms is called a ring

(i) $(R,+)$ is an abelian group.

(ii) '·' is an associative binary operation on R.

(iii) $a\cdot(b+c) = a\cdot b + a\cdot c$ and $(a+b)\cdot c = a\cdot c + b\cdot c$ $\forall a,b,c \in R$

2) Define commutative.

A ring R is said to be commutative $ab = ba$ $\forall a,b \in R$.

ex: The familiar rings Z, Q, R are all commutative.

The following are examples of non-commutative rings.

3) Define unit:

let R be a ring with identity. An element $u \in R$ is called a unit in R if it has a multiplicative inverse in R. The multiplicative inverse of u is denoted by u^{-1}

for ex: $(Z,+,\cdot)$ and -1 are units.

4) Define skew field.

Let R be a ring with identity element. R is called a skew field or a division ring if every non-zero element in R is a unit. 6

For ex. For every non zero element $a \in R$, $\exists$ a multiplicative inverse $a^{-1} \in R \ni: aa^{-1} = a^{-1}a = 1$.

5) Define left & right ideal.

Let R be a ring. A non-empty subset of R is called a left ideal of R if

(i) $a, b \in I \Rightarrow a - b \in I$

(ii) $a \in I$ and $r \in R \Rightarrow ra \in I$.

I is called an right ideal of R if

(i) $a, b \in I \Rightarrow a - b \in I$

(ii) $a \in I$ and $r \in R \Rightarrow ar \in I$.

unit - V

1) Define maximal Ideal.

Let R be a ring. An ideal $M \neq R$ is said to be a maximal ideal of R if whenever U is an ideal of R $\ni$. $M \subseteq U \subseteq R$ then either $U = M$ or $U = R$. That is there is no proper ideal of R, properly containing M.

2) Define kernel.

The kernal K of a homomorphism f of a ring R to a ring R' is defined by

$\{a / a \in R$ and $f(a) = 0$.

3) Define field of quotients.

The field F which we have constructed above is called the field of quotients of D. 7

Th. If F and F' are isomorphic integral domains then their quotient fields are also isomorphic.

4) Define Euclidean domain.

Let R be a commutative ring without zero-divisors. R is called an Euclidean domain or an Euclidean ring if for every non-zero element $a \in R$ there is defined a non-negative integer $d(a)$ satisfying the conditions

For any two non-zero elements $a, b \in R$

$d(a) \leq d(ab)$.

For any two non-zero elements $a, b \in R$, there exists $q, r \in R$ ∋: $a = qb + r$ where either $r = 0$ or $d(r) < d(b)$

5) Define Prime Ideal.

Let R be a commutative ring. An ideal $P \neq R$ is called a prime ideal if $ab \in R \Rightarrow$ either $a \in P$ or $b \in P$.

ex. (3) is a prime ideal of Z

For $ab \in (3) \Rightarrow ab = 3n$ for some integer n.

$\Rightarrow 3 \mid ab$

$\Rightarrow 3 \mid a$ or $3 \mid b$

$\Rightarrow a \in (3)$ or $b \in (3)$ ∴ (3) is prime ideal

Scanned with CamScanner