ABSTRACT ALGEBRA 16SCCMM12

Unit - I

① If $G = \{a+b\sqrt{2} / a, b \in Z\}$. Then G is a group under usual addition.

Let $a+b\sqrt{2}$ and $c+d\sqrt{2} \in G$.

Then $(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2} \in G$.

WKT, The usual addition is associative.

$0 = 0 + 0\sqrt{2} \in G$.

is the identity element.

$-a-b\sqrt{2}$ is the inversed of $a+b\sqrt{2}$.

Hence G is a group.

② Define Permutation

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

$A = \{1, 2, 3, 4\}$, $f: A \to A$ given by

$f(1) = 2$, $f(2) = 1$, $f(3) = 4$, $f(4) = 3$

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

③ Define Abelian group

A group G is said to be abelian if $ab = ba$ for all $a, b \in G$.

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

Scanned with CamScanner

④ If G be a group. Let $a, b \in G$. Then $(ab)^{-1} = b^{-1}a^{-1}$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$$
$$= aea^{-1}$$
$$= aa^{-1}$$
$$= e$$

Similarly,

$$(b^{-1}a^{-1})(ab) = e$$

Hence $(ab)^{-1} = b^{-1}a^{-1}$

⑤ Define Transposition

A cycle of length two is called a transpo-sition. Thus a transposition $(a_1 a_2)$ interchange the symbols a_1 and a_2 and leaves all the other elements fixed.

Unit - II

① Define Improper Subgroup

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

② Any cyclic group is abelian

Let $G = \langle a \rangle$ be a cyclic group

Let $x, y \in G$. Then $x = a^r$ and $y = a^s$ for some r, s

Hence $xy = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = yx$

$\therefore G$ is abelian.

Scanned with CamScanner

③ State Lagrange's theorem

Let G be a finite group of order n and H be any subgroup of G. Then the order of H divides the order of G.

④ Define Left and Right Cosets

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 H.

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

⑤ State Fermat's theorem

Let p be a Prime number and a be any integer relatively Prime to p. Then $a^{p-1} \equiv 1 \pmod{p}$.

Unit - III

① Define Normal Subgroup

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

② Define Isomorphism

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

(i) f is a bijection

(ii) $f(xy) = f(x) f(y)$, for all $x, y \in G$.

Scanned with CamScanner

③ If $f: G \to G'$ be an isomorphism. If G is abelian Then G' is also abelian.

Let $a', b' \in G'$. Then there exists $a, b \in G$.

$\exists$ $f(a) = a'$ and $f(b) = b'$.

Now, $a'b' = f(a) f(b)$
$= f(ab)$
$= f(ba)$
$= f(b) f(a)$
$= b'a'$

Hence G' is abelian.

④. Define inner automorphism

The automorphism $\phi_a : G \to G$ defined by

$\phi_a(x) = axa^{-1}$, $\phi_a(y) = aya^{-1}$, for all $x, y \in G$.

$\phi_a(x) = \phi_a(y) \Rightarrow axa^{-1} = aya^{-1}$
$\Rightarrow x = y$ (by Cancellation law)

is called an inner automorphism.

⑤ Define Kernel

Let $f: G \to G'$ be a homomorphism. Let $K = \{x \mid x \in G, f(x) = e'\}$. Then K is called the kernel of f and is denoted by $\ker f$.

Scanned with CamScanner

Unit - IV

① Define isomorphism

Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be two rings.

A bijection $f: R \to R'$ is called an isomorphism if

(i) $f(a+b) = f(a) + f(b)$

(ii) $f(ab) = f(a) f(b)$ for all $a, b \in R$.

② Define field:

A commutative skew field is called a field.

In otherwise a field is a system $(F, +, \cdot)$ satisfying the following conditions

(i) $(F, +)$ is an abelian graub.

(ii) $(F - \{0\}, \cdot)$ is an abelian group.

(iii) $a \cdot (b+c) = a \cdot b + a \cdot c$ for all $a, b, c \in F$.

③ Integral domain

A commutative ring with identity having no zero-divisors is called in integral domain.

Thus an integral domain $ab = 0 \Rightarrow$ either $a = 0$ or $b = 0$.

or equivalently $ab = 0$ and $a \neq 0 \Rightarrow b = 0$;

or $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$.

Scanned with CamScanner

④ Define Subring

A non-empty subset S of a ring $(R, +, \cdot)$ is called a subring if S itself is a ring under the same operations as in R.

⑤ Define 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 a 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 Prime ideal

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

② Define Kernel

The Kernel K of a homomorphism f of a ring R to a ring R' is defined by $\{a / a \in R$ and $f(a) = 0\}$.

Scanned with CamScanner

③ Define ~~domain~~ Euclidean domain

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

(i) For any two non-zero elements $a, b \in R$, $d(a) \leq d(ab)$.

(ii) $a, b \in R$, $\exists\, q, r \in R$ such that $a = qb + r$ either $r = 0$ or $d(r) < d(b)$.

④ 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 $\exists$ $M \subseteq U \subseteq R$ then either $U = M$ or $U = R$. i.e) there is no proper ideal of R properly containing M.

⑤ Define Homomorphism of ring

Let R and R' be rings. A function $f: R \to R'$ is called a homomorphism if

(i) $f(a+b) = f(a) + f(b)$

(ii) $f(ab) = f(a)\, f(b)$ for all $a, b \in R$.

Scanned with CamScanner