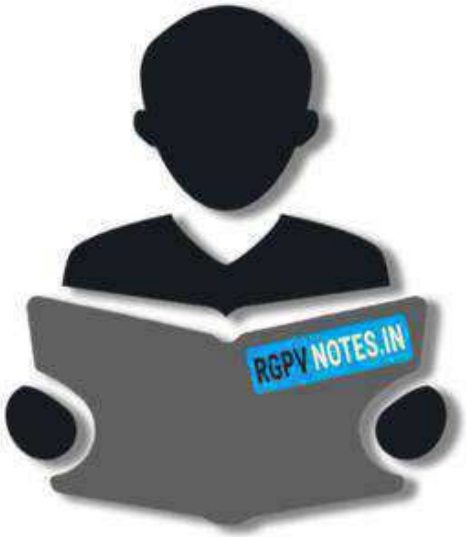

RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Discrete Structure**

Subject Code: **CS-302**

Semester: **3rd**

Subject Notes
CS301 - Discrete Structures

UNIT-2

Group Theory is a branch of mathematics and abstract algebra that defines an algebraic structure named as **Group**. Generally, a group comprises of a set of elements and an operation over any two elements on that set to form a third element also in that set. In 1854, Arthur Cayley, the British Mathematician, gave the modern definition of group for the first time −

"**A set of symbols all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a group. These symbols are not in general convertible [commutative], but are associative.**"

Any set of elements in a mathematical system may be defined with a set of operators and a number of postulates.

Algebric Structure

an algebraic structure is a set (called carrier set or underlying set) with one or more finitary operations defined on it that satisfies a list of axioms.

A binary operator defined on a set of elements is a rule that assigns to each pair of elements a unique element from that set. For example, given the set A={1,2,3,4,5}

, we can say o is a binary operator for the operation c=aob, if it specifies a rule for finding c for the pair of (a,b), such that a,b,c∈A.

Properties of Algebric Structure

The **postulates** of a mathematical system form the basic assumptions from which rules can be deduced. The postulates are −

1. **Closure-** A set is closed with respect to a binary operator if for every pair of elements in the set, the operator finds a unique element from that set.

Example

Let A={0,1,2,3,4,5,…}

This set is closed under binary operator into (∗) , because for the operation $c=a*b$, for any $a,b\in A$, the product $c\in A$.

The set is not closed under binary operator divide (÷) , because, for the operation $c=a\div b$, for any $a,b\in A$, the product c may not be in the set A. If a=7,b=2, then c=3.5. Here $a,b\in A$ but $c\notin A$

2. **Associative Laws -** A binary operator ⊗ on a set A is associative when it holds the following property −

$$(x\otimes y)\otimes z=x\otimes(y\otimes z)$$, where $x,y,z\in A$

Example

Let A={1,2,3,4} The operator plus (+) is associative because for any three elements, $x,y,z\in A$, the property $(x+y)+z=x+(y+z)$ holds.

The operator minus (−) is not associative since

$$(x-y)-z\neq x-(y-z)$$

3. **Commutative Laws -** A binary operator ⊗ on a set A is commutative when it holds the following property −

$$x\otimes y=y\otimes x$$, where $x,y\in A$

Example

Let A={1,2,3,4} The operator plus (+) is commutative because for any two elements, $x,y\in A$, the property $x+y=y+x$ holds.

The operator minus (−) is not associative since

$$x-y\neq y-x$$

4. **Distributive Laws -** Two binary operators ⊗ and ⊛ on a set A, are distributive over operator ⊛

when the following property holds −

$$x \otimes (y \circledast z) = (x \otimes y) \circledast (x \otimes z)$$, where $x,y,z \in A$

Example

Let $A=\{1,2,3,4\}$ The operators into ($*$) and plus (+) are distributive over operator + because for any three elements, $x,y,z \in A$, the property $x*(y+z)=(x*y)+(x*z)$ holds.

However, these operators are not distributive over $*$ since

$x+(y*z) \neq (x+y)*(x+z)$

5. **Identity Element -** A set A has an identity element with respect to a binary operation ⊗ on A, if there exists an element $e \in A$, such that the following property holds −

$$e \otimes x = x \otimes e$$, where $x \in A$

Example

Let $Z=\{0,1,2,3,4,5,\ldots\}$ The element 1 is an identity element with respect to operation $*$ since for any element $x \in Z$,

$1*x=x*1$

On the other hand, there is no identity element for the operation minus (−)

6. **Inverse -** If a set A has an identity element e with respect to a binary operator ⊗, it is said to have an inverse whenever for every element $x \in A$, there exists another element $y \in A$, such that the following property holds −

$$x \otimes y = e$$

Example

Let $A=\{\cdots -4,-3,-2,-1,0,1,2,3,4,5,\ldots\}$ Given the operation plus (+) and $e=0$, the inverse of any element x is $(-x)$ since $x+(x)=0$

Semigroup

A finite or infinite set 'S' with a binary operation 'o' (Composition) is called semigroup if it holds following two conditions simultaneously −

i. **Closure** − For every pair $(a,b) \in S, (aob)$ has to be present in the set S

ii. **Associative** − For every element $a,b,c \in S, (aob)oc=ao(boc)$ must hold.

Example

The set of positive integers (excluding zero) with addition operation is a semigroup. For example, $S=\{1,2,3,\ldots\}$

Here closure property holds as for every pair $(a,b) \in S, (a+b)$ is present in the set S. For example, $1+2=3 \in S$]

Associative property also holds for every element $a,b,c \in S, (a+b)+c=a+(b+c)$. For example, (1+2)+3=1+(2+3)=5

Monoid

A monoid is a semigroup with an identity element. The identity element (denoted by e or E) of a set S is an element such that $(aoe)=a$, for every element $a \in S$. An identity element is also called a **unit element**. So, a monoid holds three properties simultaneously − **Closure, Associative, Identity element**.

Example

The set of positive integers (excluding zero) with multiplication operation is a monoid. $S=\{1,2,3,\ldots\}$

1. Here closure property holds as for every pair $(a,b) \in S, (a \times b)$ is present in the set S. [For example, $1 \times 2=2 \in S$ and so on]
2. Associative property also holds for every element $a,b,c \in S, (a \times b) \times c=a \times (b \times c)$ [For example, $(1 \times 2) \times 3=1 \times (2 \times 3)=6$ and so on]
3. Identity property also holds for every element $a \in S, (a \times e)=a$ [For example, $(2 \times 1)=2, (3 \times 1)=3$ and so on]. Here identity element is 1.

Group

A group is a monoid with an inverse element. The inverse element (denoted by I) of a set S is an element such that $(aoI)=(Ioa)=a$, for each element $a \in S$. So, a group holds four properties simultaneously –

i) Closure, ii) Associative, iii) Identity element, iv) Inverse element.

The order of a group G is the number of elements in G and the order of an element in a group is the least positive integer n such that an is the identity element of that group G.

Examples

The set of *N*×*N* non-singular matrices form a group under matrix multiplication operation.

1. The product of two *N*×*N* non-singular matrices is also an *N*×*N*
2. non-singular matrix which holds closure property.
3. Matrix multiplication itself is associative. Hence, associative property holds.
4. The set of *N*×*N* non-singular matrices contains the identity matrix holding the identity element property.

As all the matrices are non-singular they all have inverse elements which are also nonsingular matrices. Hence, inverse property also holds.

Abelian Group

An abelian group G is a group for which the element pair $(a,b) \in G$ always holds commutative law. So, a group holds five properties simultaneously –

i) Closure, ii) Associative, iii) Identity element, iv) Inverse element, v) Commutative.

Example

The set of positive integers (including zero) with addition operation is an abelian group. *G*={0,1,2,3,…}

1. Here closure property holds as for every pair $(a,b) \in S, (a+b)$ is present in the set S. [For example, $1+2=2 \in S$ and so on]
2. Associative property also holds for every element $a,b,c \in S, (a+b)+c=a+(b+c)$ [For example, (1+2)+3=1+(2+3)=6 and so on]
3. Identity property also holds for every element $a \in S, (a \times e)=a$ [For example, (2×1)=2,(3×1)=3 and so on]. Here, identity element is 1.
4. Commutative property also holds for every element $a \in S, (a \times b)=(b \times a)$ [For example, (2×3)=(3×2)=3
5. Inverse Property also holds for every element a • b = b • a = e [For example 0+1 = 1+0 =1]

Properties of Groups

1. If G is a group with binary operation ∗, then the left and right cancellation laws hold in G. that is, a ∗b=a ∗c implies b=c, and b ∗a=c ∗a implies b=c for all a, b, c ∈G.

Proof - Suppose a * b = a * c. Then there exists an inverse of a' to a. Apply this inverse on the left,

a' * (a * b) = a' *(a * c)

By the associatively law,

(a' * a) * b = (a' * a) * c

Since a' is the inverse of a, a' * a =e, we have

e * b = e * c

By the definition of e,

b = c

Similarly for the right cancellation

2. If G is a group with binary operation ∗, and if a and b are any elements of G, then the linear equations a ∗ x=b and y ∗ a=b have unique solutions x and y in G.

Proof: First we show the existence of at least one solution by just computing that a' ∗ b is a solution of a ∗ x=b. Note that

a * (a' * b) = (a *a') * b, associative law,

=e * b, definition of a',

=b, property of e.

Thus x= a' ∗ b is a solution a ∗ x=b. In a similar fashion, y=b ∗ a' is a solution of y ∗ a=b.
To show uniqueness of y, we assume that we have two solutions, y_1 and y_2, so that y_1 ∗a=b and y_2 ∗a=b. Then y_1 ∗a=y_2 ∗a, and by Theorem 4.15, y_1=y_2. The uniqueness of x follows similarly.

3. In a group G with binary operation ∗, there is only one element e in G such that

$$e * x = x * e = x$$

for all x ∈G. Likewise for each a ∈G, there is only one element a' in G such that

$$a' * a = a * a' = e$$

Cyclic Group and Subgroup

A **cyclic group** is a group that can be generated by a single element. Every element of a cyclic group is a power of some specific element which is called a generator. A cyclic group can be generated by a generator 'g', such that every other element of the group can be written as a power of the generator 'g'.

Example

The set of complex numbers {1,−1,*i*,−*i*} under multiplication operation is a cyclic group.

Solution- There are two generators – *I* and –*i* as *i*1=*i*,*i*2=−1,*i*3=−*i*,*i*4=1 and also (–*i*)1=−*i*,(–*i*)2=−1,(–*i*)3=*i*,(–*i*)4=1 which covers all the elements of the group. Hence, it is a cyclic group.

Note − A **cyclic group** is always an abelian group but not every abelian group is a cyclic group. The rational numbers under addition is not cyclic but is abelian.

A **subgroup** H is a subset of a group G (denoted by *H*≤*G*) if it satisfies the four properties simultaneously − **Closure, Associative, Identity element**, and **Inverse**.

A subgroup H of a group G that does not include the whole group G is called a proper subgroup (Denoted by *H*<*G*). A subgroup of a cyclic group is cyclic and a abelian subgroup is also abelian.

Example

Let a group *G*={1,*i*,−1,−*i*}

Then some subgroups are *H*1={1},*H*2={1,−1}, This is not a subgroup − *H*3={1,*i*} because that (*i*)−1=−*i* is not in *H*3

Coset

Given H ≤ G, a left coset of H in G is a subset of G of the form gH = {gh|h∈ H} for some g ∈ G. Similarly a right coset of H in G is a subset of G of the form Hg = {hg|h∈ H} for some g ∈ G. Notice since g = eg = ge that g ∈ Hg and g ∈gH.

Example Suppose G = Σ $_3$, H =< (1, 2) >= {e,(1, 2)} and g = (1, 3). Then a simple computation shows that gH = {(1, 3),(1, 2, 3)} while Hg = {(1, 3),(1, 3, 2)} and sogH 6= Hg. Thus we see that for a fixed element g, the left cosetgH may be different from the right coset Hg in general.

Multiplying elements and sets Of course, the expression gH does not make immediate sense from the group axioms. What it means, by definition, is gH = {gh | h ∈ H} .

To put this another way, the golden rule is this: if you know that f ∈gH, then you can conclude that there is some h ∈ H so that f = gh.

Applying the golden rule Consider G = S4 and H = {id,(1, 2)}. If g = (2, 3, 4), thengH = {(2, 3, 4),(2, 3, 4)(1, 2)} = {(2, 3, 4),(1, 3, 4, 2)}. Now let f = (3, 4, 2, 1)—this is an element of gH. Which h ∈ H satisfies f = gh?

Or

if g = (1, 3)(2, 4), then gH = {(1, 3)(2, 4),(1, 4, 2, 3)}. If you let f = (1, 4, 2, 3), which h ∈ H satisfies f = gh this time?

compute the two cosets g1H ⊂ S4 and g2H ⊂ S4 for H = {id,(1, 2, 3, 4),(1, 3)(2, 4),(1, 4, 3, 2)} and g1 = (1, 3, 2), g2 = (1, 2, 3, 4).

Factor Group

If N is a normal subgroup of G, then the group of left cosets of N in G is called the factor group of G determined by N. It will be denoted by G/N.

Example Let N be a normal subgroup of G. If a ∈G, then the order of aN in G/N is the smallest positive integer n such that $a^n \in N$.

Permutations Group

A permutation of a set X is a function σ : X → X that is one-to-one and onto, i.e., a bijective map.

Example

A = {1,2,3}

There are six permutations for this set, namely

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

Normal Subgroup

A normal subgroup is a subgroup which is invariant under conjugation by members of the group of which it is a part. In other words, a subgroup H of a group G is normal in G if and only if gH = Hg for all g in G; i.e., the sets of left and right cosets coincide.

gH = Hg

Homomorphism

Definition: A group homomorphism ϕ : G → G0 is an isomorphism if ϕ is a bijection. If there is an isomorphism between G and G0 we say G and G0 are isomorphic. This is denoted by G ∼= G0 .

Given a homomorphism ϕ : G → G0 there are subgroups of each that can indicate to us whether ϕ is injective or surjective. Definition. Let ϕ : G → G0 be a homomorphism. Define ker(ϕ) = {g ∈ G : ϕ(g) = eG0}. This is called the kernel of ϕ. Define im(ϕ) = {ϕ(g) : g ∈ G}. This is called the image of ϕ. We usually use the notation ϕ(G) for im(G).

Example If ϕ : GL2(R) → R\{0} is given by ϕ(A) = det(A) then ker(ϕ(A)) = SL2(R) and im(ϕ) = R\{0}.

Theorem Letϕ : G → G0 be a homomorphism. Then 1.ker(ϕ) is a subgroup of G, and ϕ is injective if and only if ker(ϕ) = eG. 2. im(ϕ) is a subgroup of G0 , and ϕ is surjective if and only if im(ϕ) = G0 (or equivalently, ϕ(G) = G0).

Proof. If a, b ∈ker(ϕ), then ϕ(ab−1) = ϕ(a)ϕ(b) −1 = eG0(eG0) −1 = eG0 so by the Subgroup Test, ker(ϕ) is a subgroup.

Now if ker(ϕ) = {e} then ϕ(a) = ϕ(b) =⇒ϕ(ab−1) = e =⇒ ab−1 = e =⇒ a = b.

Moreover, if ϕ is injective, then

ϕ(a) = e =⇒ϕ(a) = ϕ(e) =⇒ a = e, so ker(ϕ) = {e}.

Isomorphism

The homomorphism ϕ : G → G0 is an isomorphism if and only if there exists a homomorphism ψ : G0 → G such that ϕ ◦ ψ = ψ ◦ ϕ are identity maps on their respective groups.

Proof : Define ψ(a) to be the unique pre-image of a under ϕ. Since ϕ is a bijection, this is well defined and ϕ ◦ ψ = ψ ◦ ϕ are identity maps between their respective groups. One needs to check ψ is indeed a homomorphism, but this effectively comes for free since ϕ is one.

Example and standard result on Group

Integers Z with addition

(G1) a, b ∈ Z =⇒ a + b ∈ Z

(G2) (a + b) + c = a + (b + c)
(G3) the identity element is 0 as a + 0 = 0 + a = a and 0 ∈ Z
(G4) the inverse of a ∈ Z is −a as a + (−a) = (−a) + a = 0 and −a ∈ Z (G5) a + b = b + a

The set Zn of congruence classes modulo n with addition
(G1) [a], [b] ∈ Zn ⟹ [a] + [b] = [a + b] ∈ Zn
(G2) ([a] + [b]) + [c] = [a + b + c] = [a] + ([b] + [c])
(G3) the identity element is [0] as [a] + [0] = [0] + [a] = [a]
(G4) the inverse of [a] is [−a] as [a] + [−a] = [−a] + [a] = [0]
(G5) [a] + [b] = [a + b] = [b] + [a]

The set Gn of invertible congruence classes modulo n with multiplication
A congruence class [a]n ∈ Zn belongs to Gn if gcd(a, n) = 1.
(G1) [a]n, [b]n ∈Gn ⟹gcd(a, n) = gcd(b, n) = 1 ⟹gcd(ab, n) = 1 ⟹ [a]n[b]n = [ab]n ∈Gn
(G2) ([a][b])[c] = [abc] = [a]([b][c])
(G3) the identity element is [1] as [a][1] = [1][a] = [a]
(G4) the inverse of [a] is [a] −1 by definition of [a] −1
(G5) [a][b] = [ab] = [b][a]

Permutations S(n) with composition (= multiplication)
(G1) π and σ are bijective functions from the set {1, 2, . . . , n} to itself ⟹ so is πσ
(G2) (π σ)τ and π(σ τ) applied to k, 1 ≤ k ≤ n, both yield π(σ(τ (k))).
(G3) the identity element is id as π id = id π = π
(G4) the inverse of π is π −1 by definition of the inverse function (G5) fails for n ≥ 3 as (as (1 2)(2 3) = (1 2 3) while (2 3)(1 2) = (1 3 2).

Ring
The definition of a ring: A structure (R, +, ·) is a ring if R is a non-empty set and + and · are binary operations:
+: R × R → R, (a, b) 7→ a + b · : R × R → R, (a, b) 7→ a · b
such that
Addition: (R, +) is an abeliangroup, that is,
(A1) associativity: for all a, b, c ∈ R we have a + (b + c) = (a + b) + c
(A2) zero element: there exists 0 ∈ R such that for all a ∈ R we have a + 0 = 0 + a = a
(A3) inverses: for any a ∈ R there exists −a ∈ R such that a + (−a) = (−a) + a = 0
(A4) commutativity: for all a, b ∈ R we have a + b = b + a

Multiplication:
(M1) associativity: for all a, b, c ∈ R we have a · (b · c) = (a · b) · c

Addition and multiplication together (D) for all a, b, c ∈ R,
a · (b + c) = a · b + a · c and (a + b) · c = a · b + b · c.
We sometimes say 'R is a ring', taken it as given that the ring operations are denoted + and ·. As in ordinary arithmetic we shall frequently suppress · and write ab instead of a · b

Special types of rings: definitions. Assume (R; +, ·) is a ring. We say R is a commutative ring if its multiplication · is commutative, that is,
(M4) Commutativity: a · b = b · a for all a, b ∈ R. We say R is a ring with 1 (or ring with identity) if there exists an identity for multiplication, that is,
(M2) identity element: there exists 1 ∈ R such that for all a ∈ R we have a · 1 = 1 · a = a.

Examples of rings

Number systems

(1) All of Z, Q, R and C are commutative rings with identity (with the number 1 as the identity).

(2) N is NOT a ring for the usual addition and multiplication. These are binary operations and we do have a zero element, namely 0, so axiom (A2) holds. However (A3) (existence of additive inverses) fails: there is no n ∈ N for which 1 + n = 0, for example.

(3) Consider the set of even integers, denoted 2Z, with the usual addition and multiplication. This is a commutative ring without an identity. To verify that (M2) fails it is not sufficient just to say that the integer 1 does not belong to 2Z. Instead we argue as follows. Suppose for contradiction that there were an element e ∈ 2Z such that n·e = n for all n ∈ 2Z. In particular 2e = 2, from which we deduce that e would have to be 1. Since 1 ∈/ 2Z we have a contradiction.

Matrix rings Under the usual matrix addition and multiplication Mn(R) and Mn(C), are rings with 1, but are not commutative (unless n = 1). If we restrict to invertible matrices we no longer have a ring, because there is then no zero for addition.

PolynomialsPolynomials, with real coefficients, form a commutative ring with identity under the usual addition and multiplication; we denote this by R[x].

Modular arithmetic Binary arithmetic on {0, 1} (see 1.2(4)) gives us a 2-element commutative ring with identity. More generally we get a commutative ring with identity if we consider addition and multiplication mod n on {0, 1, . . . , n − 1}.

Calculational rules for rings.

Assume that (R; +, ·) is a commutative ring.

Let a, b, c ∈ R.

(i) If a + b = a + c then b = c.

(ii) If a + a = a then a = 0.

(iii) −(−a) = a.

(iv) 0a = 0.

(v) −(ab) = (−a)b = a(−b). Assume in addition that R has an identity 1 Then

(vi) (−1)a = −a.

(vii) If a ∈ R has a multiplicative identity a −1 then ab = 0 implies b = 0.

Field

A field is a ring in which the elements, other than the identity element for addition, and the multiplication operator, also form a group.

- There are only two kinds of finite fields. One kind is the field formed by addition and multiplication modulo a prime number.
- The other kind of finite field has a number of elements that is a power of a prime number.
- The addition operator consists of multiple independent additions modulo that prime. The elements of the field can be thought of as polynomials whose coefficients are numbers modulo that prime. In that case, multiplication is polynomial multiplication, where not only the coefficients modulo that prime, but the polynomials are modulo a special kind of polynomial, known as a primitive polynomial. All finite fields, but particularly those of this second kind, are known as Galois fields.
- A commutative ring which has more than one element such that every non-zero element of S has a multiplicative inverse in S is called a field.

The ring of even integers is a subring of the ring of integers. Let •> and Å , ¤ > be rings. A mapping of g : R® S is called a ring homomorphism from and Å ,¤ > if for any a, b, Î R g(a + b) = g(a) Å g(b) and g(a • b) = g(a) ¤ g(b).

Standard results

If R is a ring and a, b, c, d ∈ R, evaluate (a + b)(c + d).

Solution: $(a + b)(c + d) = a(c + d) + b(c + d)$
by distributive law
$= (ac + ad) + (bc + bd)$
$= ac + ad + bc + bd$

Prove that if a, b ∈ R, then $(a + b)^2 = a^2 + ab + ba + b^2$ where by x^2 we mean xx.
Solution: $(a + b)^2 = (a + b)(a + b) = a(a + b) + b(a + b) = a^2 + ab + ba + b^2$ Note that if R is not a commutative ring ab 6= ba.
If in a ring R every $x ∈ R$ satisfies $x^2 = x$,prove that R must be commutative (A ring in which $x^2 = x$ for all elements is called a Boolean ring).
Solution: Let x, y ∈ R. Then $(x + y)^2 = (x + y)(x + y) = x^2 + xy + yx + y^2$ Since $x^2 = x$ and $y^2 = y$ we have $x + y = x + xy + yx + y$. Hence $xy = −yx$. But for every $x ∈ R$ $(−x) = (−x)^2 = (−x)(−x) = x^2 = x$. Hence $−yx = yx$ i.e. we obtain $xy = yx$.

Prove that any field is an integral domain.
Solution: Let a 6= 0 and b be two elements in the field F and ab = 0. Since F is a field and a 6= 0. we have $a −1 ∈$ F. Hence $a −1ab = a −10 = 0$. So we obtain b = 0. Hence there exists no zero divisor in F.

If U is an ideal of R and $1 ∈ U$, prove that U = R.
Solution: Since for any $r ∈ R$ and $u ∈ U$, $ru∈ U$ we have for any $r ∈ R$, $r1 = r ∈ U$. Hence R = U.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in