Discrete Mathematics (CSA103)

Mathematical Logic: Propositional and Predicate Logic, Propositional Equivalences, Normal Forms, Predicates and Quantifiers, Nested Quantifiers, Rules of Inference.

Sets and Relations: Set Operations, Representation and Properties of Relations, Equivalence Relations, Partially Ordering. Counting,

Mathematical Induction and Discrete Probability: Basics of Counting, Pigeonhole Principle, Permutations and Combinations, Inclusion- Exclusion Principle, Mathematical Induction, Probability, Bayes Theorem.

Group Theory: Groups, Subgroups, Semi Groups, Product and Quotients of Algebraic Structures, Isomorphism, Homomorphism, Automorphism, Rings, Integral Domains, Fields, Applications of Group Theory.

Graph Theory: Simple Graph, Multigraph, Weighted Graph, Paths and Circuits, Shortest Paths in Weighted Graphs, Eulerian Paths and Circuits, Hamiltonian Paths and Circuits, Planner graph, Graph Coloring, Bipartite Graphs, Trees and Rooted Trees, Prefix Codes, Tree Traversals, Spanning Trees and Cut-Sets.

Boolean Algebra: Boolean Functions and its Representation, Simplifications of Boolean Functions.

Optimization: Linear Programming - Mathematical Model, Graphical Solution, Simplex and Dual Simplex Method, Sensitive Analysis; Integer Programming, Transportation and Assignment Models,

PERT-CPM: Diagram Representation, Critical Path Calculations, Resource Levelling, Cost Consideration in Project Scheduling.

Books Recommended:

- J.P. Trembley and R.P.Manohar, Discrete Mathematical Structures with Applications to Computer Science, McGraw Hill.
- Dornhoff and Hohn, Applied Modern Algebra, McMillan.
- N. Deo, Graph Theory with Applications to Engineering and Computer Science, PHI.
- C.L. Liu, Elements of Discrete Mathematics, McGraw-Hill.
- Rosen, Discrete Mathematics, Tata McGraw Hill.
- K.L.P. Mishra, N. Chandrasekaran, Theory of Computer Science: Automata, Languages and Computation, PHI.

Binary Operation: Let G be a non empty set then a function $* : G \times G \to G$ is called a binary operation on set G.

Algebraic Structure: Let G be a non empty set and $* : G \times G \to G$ be a binary operation on G then the pair $(G, *)$ is called an algebraic structure.

Quasi Group or Groupoid: A non empty set equipped with a binary operation is called a quasi group or groupoid.

Semi Group: A groupoid in which binary operation is associative is called a semi group.

Monoid: A semi group is said to be monoid if it has an identity element.

Group: Let G be a non empty set and $* : G \times G \to G$ be an operation on G, then the structure $(G, *)$ is said to be a group if it satisfies the following properties-

1. **Closure Property** $a * b \in G \ \forall \ a, b \in G$.
2. **Associativity** $a * (b * c) = (a * b) * c \ \forall \ a, b, c \in G$.
3. **Existence of Identity** $\exists \ e \in G$ such that $e * a = a * e = a \ \forall \ a \in G$.
4. **Existence of Inverse** $\exists \ b \in G$ such that $b * a = a * b = e \ \forall \ a \in G$.

Abelian Group: A group G is called a commutative group or an Abelian group if $b * a = a * b \ \forall \ a, b \in G$.

Examples:

- Let $G = \{1, -1\}$ then the structure $(G, \times)$ is a group. Which can be seen from the following composition table or Caley table:

$\times$	**1**	**-1**
1	1	-1
-1	-1	1

- Let $G = \{0, 1, 2, 3, 4\}$ then the structure $(G, +_5)$ is a group. Which can be seen from the following composition table or Caley table:

$+_5$	**0**	**1**	**2**	**3**	**4**
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Some more Examples:

- $(Z, +)$ is an Abelian group
- $(Q, , +)$ is an Abelian group
- $(R, , +)$ is an Abelian group
- Let $G = \{1, -1\}$ then the structure $(G, \times)$ is an Abelian group.

Subgroup: Let $(G, *)$ be a group and H be a non empty subset of G, then H is called subgroup of G if H itself is a group with respect to same binary operation $*$.

Example: Let $G = \{1, -1, i, -i\}$ then the structure $(G, \times)$ is a group. Consider $H = \{1, -1\}$ then the structure $(H, \times)$ is again a group. Hence, H is a subgroup of G.

Theorem: Let G be a group and H a non empty subset of G, then H is a subgroup of G iff $ab^{-1} \in H$ whenever $a, b \in H$.

Order of the element: Let G be a group and $a \in G$ then we say a is of the order (or period) r if r is the least positive integer such that $a^r = e$. It is denoted by $o(a)$.

Cyclic Groups: Let G be a group and $a \in G$ then $< a >= \{a^r : r \in Z\}$ is a subgroup of G called the cyclic subgroup generated by a.

Example: Let $G = \{1, -1, i, -i\}$ then the structure $(G, \times)$ is a group. Then one can see that $o(1) = 1, o(-1) = 2, o(i) = 4, o(-i) = 4$.

Coset: Let G be a group, $a \in G$ and H be a subgroup of G. Then the right coset Ha of H in G is defined as $Ha = \{ha : h \in H\}$. Similarly a left coset aH of H in G can be defined.

Cosets of of Subgroup: The index of subgroup H of a group G is defined as the number of distinct right (or left) cosets of H in G. It is denoted by $i_G(H)$ or $[G : H]$.

Normal Subgroup: A subgroup H of a group G is called a normal or invariant subgroup of G if its left coset equals its right coset, i.e, $aH = Ha \; \forall \; a \in G$.

Example: All subgroups of an abelian group are normal.

Simple Group: A group G having no proper normal subgroup is called simple.

Example: Let $G = \{0, 1, 2, 3, 4\}$ then $(G, +_5)$ is a simple group as its only subgroups are $\{0\}$ and G itself.

Quotient Group: Let H be a normal subgroup of G and then $G|H = \{$set of all right/left cosets of H in $G\}$ is a group, called the quotient group under the binary operation $Ha.Hb = Hab$ and $o(G|H) = o(G)/o(H)$.

Homomorphism: Let $(G, *)$ and (G', o) be two groups then a homomorphism $f : G \to G'$ is a mapping that preserves the group operations i.e, $f(a * b) = f(a)of(b)\ \forall\ a, b \in G$.

Example: Let $(\mathbb{R}, +)$ and $(\mathbb{R}, \times)$ be two groups then a map $f : (\mathbb{R}, +) \to (\mathbb{R}, \times)$ defined by $f(x) = e^x\ \forall\ x \in \mathbb{R}$ is a homomorphism.

Kernel: Let $f : G \to G'$ be a homomorphism then the set $kerf = \{x \in G : f(x) = e'\}$ is called the kernel of homomorphism, where e' is the identity of G'.

Range of Homomorphism: Let $f : G \to G'$ be a homomorphism then the set $R(f) = \{f(x) \in G' : x \in G\}$ is called the range of homomorphism.

Note:

1. $kerf$ is normal subgroup of G.
2. $R(f)$ is a subgroup of G'.

Isomorphism: A one-one onto homomorphism $f : G \to G'$ is called an isomorphism.

Example: TLet $(\mathbb{R}, +)$ and $(\mathbb{R}, \times)$ be two groups then a map $f : (\mathbb{R}, +) \to (\mathbb{R}, \times)$ defined by $f(x) = e^x \ \forall \ x \in \mathbb{R}$ is an isomorphism.

Automorphism: An isomorphism $f : G \to G$ is called an automorphism.

Example: A map $f : (G, \bullet) \to (G, \bullet)$ given by $f(x) = x^{-1}$ is an automorphism.

Fundamental Theorems of Homomorphism:

1. Every homomorphic image of a group is isomorphic to the quotient group induced by kernel of homomorphism i.e, If $f : G \to G'$ is a homomorphism then $G|kerf \cong f(G)$.
2. If H is a normal subgroup of G and K is another subgroup of G then $K|(H \cap K) \cong HK|H$.
3. Let H, K be normal subgroups of G such that K is normal subgroup of H then $G|H \cong \frac{(G|K)}{H|K}$.

Ring: A ring is the structure $(R, +, \bullet)$ where R is a nonempty set equipped with two binary operations $+, \bullet$ satisfying the following properties:

1. $(R, +)$ is an abelian group.
2. $\bullet$ is distributive over $+$, i.e,
   1. $a \bullet (b + c) = a \bullet b + a \bullet c$
   2. $(b + c) \bullet a = b \bullet a + c \bullet a$
3. $(a \bullet b) \bullet c = a \bullet (b \bullet c)$

Ring with unity: A ring $(R, +, \bullet)$ with multiplicative identity in it is called a ring with unity.

Example: The structure $(\mathbb{Z}, +, \times)$ is a ring with unity.

The structure $(\mathbb{Z}_4, +_4, \times_4)$ is a ring with unity.

Commutative Ring: A ring for which multiplication is commutative is called a commutative ring

Boolean Ring: A ring $(R, +, \bullet)$ is a Boolean ring if all its elements are idempotent. That is, $a \bullet a = a \ \forall \ a \in R$.

Zero Divisors: The non-zero elements $a, b \in R$ are called zero divisors if $a \bullet b = 0$.

Example: The ring $(\mathbb{Z}_8, +_8, \times_8)$ has zero divisors as $2 \times_8 4 = 0$. Hence, 2 and 4 are zero divisors.

Integral Domain: A commutative ring with unity is called an integral domain if it has no zero divisors.

Division Ring or Skew Field: A ring with at least two elements is called a division ring or skew field if all its non-zero elements form a group with respect to multiplication.

Field: An integral domain is called a field if its every non-zero element has multiplicative inverse in it.

OR

A commutative skew field is a field.

Examples:

1. $(\mathbb{Z}, +, \times)$ is an integral domain but not a field.
2. The set of all 2×2 matrices of the form

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

   forms a division ring or skew field which is not a field.
3. $(\mathbb{Q}, +, \times)$ is a field.
4. $(\mathbb{R}, +, \times)$ is a field.
5. $(\mathbb{C}, +, \times)$ is a field.
6. $(\mathbb{Z}_p, +_p, \times_p)$ is a field, where p is a prime.

Some Important Theorems:

- A ring R is without zero divisors if and only if the cancellation laws hold in R.
- Every field is an integral domain.
- Every finite integral domain is a field.
- A finite commutative ring without zero divisors is a field.

Applications of group theory: Group theory is a powerful tool for research in following areas

- Robotics
- Computer vision
- Computer graphics
- Medical image analysis

Further group theory is the ultimate theory for a analysis of symmetry.

Questions/Query ?