Discrete Structures (Monsoon 2021)

Ashok Kumar Das

Associate Professor
IEEE Senior Member
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad (IIIT Hyderabad)

E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashokkdas`
`https://sites.google.com/view/iitkgpakdas/`

Topic: **Ring and Field**

Ring and Field

Definition (Ring)

A ring R, sometimes denoted by $(R, \circ, *)$ is a set of elements with two binary operations, $\circ$ (e.g., ordinary addition) and $*$ (e.g., ordinary multiplication), such that for all $a, b, c \in R$ the following axioms are obeyed:

- **(A1-A5)** R is an abelian group under $\circ$.
- **(M1) Closure under $*$:** If $a, b \in R$, then $a * b \in R$.
- **(M2) Associativity of $*$:** $a * (b * c) = (a * b) * c$, for all $a, b, c \in R$.
- **(M3) Distributive Laws:**
  (i) Left Distributive Law: $a * (b \circ c) = (a * b) \circ (a * c)$, for all $a, b, c \in R$.
  (i) Right Distributive Law: $(a \circ b) * c = (a * c) \circ (b * c)$, for all $a, b, c \in R$.

Definition (Commutative Ring)

A ring $(R, \circ, *)$ is said to be *commutative* if it satisfies the following additional condition:

- **(M4) Commutative of $*$:** $a * b = b * a$, for all $a, b \in R$.

Ring and Field

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

Example

Let E denote the set of even integers, that is, $E = \{0, \pm 2, \pm 4, \pm 6, \cdots, \}$. Then, $(E, +, \times)$ is a commutative ring.

Example

Let M_n denote the set of all n-square ($n \times n$) matrices over the real numbers. Then, $(M_n, +, \times)$ is a commutative ring, where $+$ and $\times$ denote the ordinary matrix addition and multiplication, respectively.

Ring and Field

- **Problem:** Let $(R, +, \times)$ be a ring with identity, R is the set of real numbers. Using its elements, let us define another structure $(R', \oslash, \otimes)$, where $R' = R$ and for $a, b \in R$, $a \oslash b = a + b + 1$ and $a \otimes b = a \times b + a + b$.
  (i) Prove that $(R', \oslash, \otimes)$ is a ring.
  (ii) Is R' is a ring with identity? If so, which one is the multiplicative identity (under $\otimes$)?