L07

Tuesday, August 9, 2022 9:45 AM

* A ring is a set R with operations $+$ and $\circ$ such that

(0) R is closed under $+$ and $\circ$

(1) $(R, +)$ is a commutative ring.
(and we denote the "identity of $+$ operations by 0)

(2) $\circ$ is associative.

$$(a \circ b) \circ c = a \circ (b \circ c)$$

(3) The operation $\circ$ is distributive over $+$

That is $a \circ (b+c)$

$$= a \circ b + b \circ c$$

* A ring is commutative (or Abelian)

if $a \circ b = b \circ a$

* Example #1: $\mathbb{Z}^{m \times m}$ the integer matrices

is a Ring.

is a Ring.

Example #2: $\{0, 1, \cdots, m-1\}$ w. addition and multiplication under modulo m is a <u>commutative ring</u>

Example #3: The set of "binary polynomial" is a <u>commutative ring</u>

Fields.

Def'n: A Field F with $\bullet$ and $+$ must satisfy

① F is a <u>commutative group</u> with respect to $+$ (The identity of $+$ is denoted by 0)

② $F \setminus \{0\}$ is a <u>commutative group</u> under $\bullet$

③ The $\bullet$ and $+$ distribute:

$$a \bullet (b + c) = a \bullet b + a \bullet c$$

Summary

		Associativity	Identity	Inverse	Commutative	Distribue
Groups	$\cdot$	✓	✓	✓		
Commutative group	$\cdot$	✓	✓	✓	✓	
rings	$+$	✓	✓	✓	✓	
	$\cdot$	✓				✓
Commutative rings	$+$	✓	✓	✓	✓	
	$\cdot$	✓			✓	✓
Fields	$+$	✓	✓	✓	✓	
	$\cdot$	✓	✓	✓	✓	✓

Intuition: Groups $\Longrightarrow$ add or subtract

Rings $\Longrightarrow$ add, subtract, multiply

Fields $\Longrightarrow$ add, subtract, multiply, division

Example: $\mathbb{R}$: all real numbers.

$\mathbb{C}$: all complex numbers.

$\mathbb{Q}$: all rational numbers

$\mathbb{Z}$: all integers are NOT a field.

---

* Fields of finite order (finite # of elements) is of the main interest to us.

* They were discovered by Evariste Galois

* Denoted by $GF(q)$ where q is the <u>order</u> G: Galois