Lecture 25: $(R, +, \cdot)$ is called a ring if

(1) $(R, +)$ is an abelian group

(2) $(R, \cdot)$ is a semi-group

(3) Distributive laws hold (connect both the binary operations)

$$\left.\begin{aligned} a\cdot(b+c) &= a\cdot b + a\cdot c \\ (a+b)\cdot c &= a\cdot c + b\cdot c \end{aligned}\right\} \forall\, a, b, c \in R$$

The binary operations $+$ and $\cdot$ are called addition and multiplication, respectively.

We say that the ring $(R, +, \cdot)$ has identity if R has an identity element with respect to the multiplication. We call R to be commutative if R is commutative with respect to the multiplication operation in R.

Ex: (i) $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity 1.

(ii) $(2\mathbb{Z}, +, \cdot)$ is a commutative ring without identity element.

Definition: Let R be a ring with identity 1. $x \in R$ is called a unit if x has inverse in R with respect to the multiplication. That is, x is called a unit if $\exists\, y \in R$ such that $x \cdot y = 1 = y \cdot x$.

$U(R) :=$ set of all the units in R.

Ex: Prove that $U(R)$ is a group with respect to the multiplication in R.

Definition: Let $(R, +, \cdot)$ be a ring. $S \subseteq R$ is called a subring if $(S, +, \cdot)$ is itself a ring.

__Ex:__ It is easy to check that a subset S of a ring $(R, +, \cdot)$ is a subring of R if

$$a-b,\ a\cdot b \in S \quad \forall\, a, b \in S.$$

__Example 1:__ $M_n(\mathbb{R})$ = set of all the $n \times n$ real matrices is a ring under matrix addition and multiplication. It is non-commutative and the identity is the identity matrix. Also, the group of units in $M_n(\mathbb{R})$ is the set of all the non-singular matrices in $M_n(\mathbb{R})$.

<u>Some remarks:</u> Let S be a subring of a ring R.

(1) S may be commutative but not R.

<u>Example:</u> $R = M_n(\mathbb{R})$, $n \geq 2$. Then R is non-commutative. But $S = \left\{ \begin{pmatrix} a & & 0 \\ & a & \\ & & \ddots \\ 0 & & & a \end{pmatrix} : a \in \mathbb{R} \right\}$, the set of all the diagonal matrices in R is a commutative subring of R.

(2) S may not have identity even if R has.

<u>Example:</u> $R = \mathbb{Z}$ and $S = 2\mathbb{Z}$.

(3) S may have identity, even if R does not have.

<u>Example:</u> Let $R = \mathbb{Z} \times 2\mathbb{Z}$. Then R is a ring under the following operations:

$$(a, b) + (c, d) = (a+c, b+d)$$

$$(a, b) \cdot (c, d) = (a \cdot c, b \cdot d).$$

Clearly, $R = \mathbb{Z} \times 2\mathbb{Z}$ does not have identity element.

However, $S = \{(a, 0) : a \in \mathbb{Z}\}$ is a subring of R with identity element $(1, 0)$.

(4) S and R may both have identity elements, but they are different.

<u>Example</u>: Let $R = M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}$

Then, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of R.

We first find a subring of R which does not contain $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Let $S = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{R} \right\}$.

<u>Ex</u>: Prove that S is a ring under matrix addition and multiplication. That is, S is a subring of R.

Now, let $\begin{pmatrix} e & e \\ e & e \end{pmatrix} \in S$ be an identity element of S.

Then, $\begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} e & e \\ e & e \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix} \quad \forall\, a \in \mathbb{R}$

$\therefore \quad 2ae = a \quad \forall\, a \in \mathbb{R} \Rightarrow e = \frac{1}{2}.$

Thus, $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$ is the identity element of S

which is different from the identity element of R.

§ <u>Division ring</u>: $(R,+,\cdot)$ is called a division ring if every non-zero element of R has inverse under multiplication. That is, $R-\{0\}$ is a group under multiplication.

§ <u>Field</u>: A commutative division ring is called a field. That is, $(R,+,\cdot)$ is a field if $R-\{0\}$ is a commutative group under multiplication.

<u>Example:</u> $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ are all fields. Here, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the set of rational, real, complex numbers respectively.

§ Example of a division ring which is not a field:

Let $R = \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} : u, v \in \mathbb{C} \right\}$.

For $u \in \mathbb{C}$, $\bar{u}$ is the conjugate of u.

Clearly, R is a ring with respect to addition and multiplication of matrices. Note that the entries of the matrices in R are complex numbers. It is easy to check that R is not commutative.

Again, let $\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ be non-zero in R. Then its inverse is given by

$$\frac{1}{u\bar{u}+v\bar{v}}\begin{pmatrix}\bar{u} & -v\\ \bar{v} & u\end{pmatrix}.$$

Hence, R is a division ring. Since R is not commutative, so R is not a field.

<u>Example</u>: For $n \geq 2$, let $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$
Then, $\mathbb{Z}_n$ is a ring under addition and multiplication modulo n.
We have $\mathbb{Z}_n$ is a field $\Leftrightarrow$ n is a prime.
Thus, for each prime p, $\mathbb{Z}_p$ is a finite field. #