Lecture 26 and Lecture 27. Oct 11 and Oct 14, 2022

Note Title 10/15/2022

Ex: We know that for a prime p, $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ is a field. Let $M_{2\times 2}(\mathbb{Z}_p)$ be the ring of all the 2×2 matrices with entries from $\mathbb{Z}_p$.

Show that $|U(M_{2\times 2}(\mathbb{Z}_p))| = (p^2-1)(p^2-p)$.

Definition: Let R be a ring. A non-zero element $x \in R$ is said to be a left zero divisor if $\exists$ a non-zero element $y \in R$ s.t. $xy = 0$.
Similarly, we define right zero divisor.

A zero divisor is an element of R which is both a left zero divisor and a right zero divisor.

Ex: In $\mathbb{Z}_6$, both 2 and 3 are zero divisors.

Ex: A ring R has no zero divisors if and only if the right and left cancellation laws (under multiplication) holds in R, that is, for $a, b, c \in R$ with $a \neq 0$ and

$$ab = ac \quad \text{or} \quad ba = ca \Rightarrow b = c.$$

Definition: A commutative ring R with identity and without any zero divisor is called an Integral Domain.

Example: ① Every field is an integral domain.

② $(\mathbb{Z}, +, \cdot)$ is an integral domain which is not a field.

(3) $(\mathbb{Z}_n, +, \cdot)$ is an integral domain $\Leftrightarrow$ n is prime.

<u>Theorem</u>: Every finite integral domain is a field.

<u>Proof</u>: Let R be a finite integral domain.

Since R is commutative with identity (being an ID), so to prove that R is a field, it is enough to prove that every $x \neq 0$ is a unit in R.

Let $x \in R$ and $x \neq 0$. Consider the elements:

$$x, x^2, x^3, \ldots\ldots$$

Since R is finite, so $\exists j > i$ such that $x^j = x^i$.

$$\Rightarrow x^i(x^{j-1} - 1) = 0.$$

Since R is an ID and $x \neq 0$, so $x^2 \neq 0$, $x^3 \neq 0$, $\dots$, $x^n \neq 0, \dots$

Thus, $x^i(x^{j-i}-1)=0 \Rightarrow x^{j-i}-1=0$ ($\because x^i \neq 0$ and R is an ID)

$\Rightarrow x^{j-i}=1 \Rightarrow x \cdot x^{j-i-1}=1$ ($\because j>i$, so $j-i-1 \geq 0$)

$\Rightarrow x^{j-i-1}$ is the inverse of x.

$\therefore x \in U(R)$. This proves that R is a field. #

<u>2nd proof</u>: Let $a \in R$ and $a \neq 0$.

We define $f: R \to R$ by $f(x) = ax$.

Let $f(x) = f(y)$. Then, $ax = ay \Rightarrow a(x-y)=0$.

Since $a \neq 0$ and R is an integral domain, so $x-y=0 \Rightarrow x=y$

Hence, f is one-to-one. Since R is finite, so f is onto.

As $1 \in R \Rightarrow \exists\, b \in R$ s.t. $f(b) = 1 \Rightarrow ab = 1$

$\therefore$ a is a unit.

This proves that R is a field.

Remark: For $n \geq 2$, $(\mathbb{Z}_n, +, \cdot)$ is an ID

$\Leftrightarrow$ n is a prime

$\Leftrightarrow$ $(\mathbb{Z}_n, +, \cdot)$ is a field.

Note Title 4/8/2021

Definition: (Characteristic of a ring): Let R be a ring.

The least positive integer n (if exists) such that $n \cdot a = 0 \quad \forall\, a \in R$ is called the characteristic of R.

If no such n exists, we say that the characteristic of R is zero.

Notation: We write $\text{char}(R)$ to denote characteristic of R.

Ex: • $\text{char}(\mathbb{Z}) = 0$

• $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = 0$

• $\text{char}(\mathbb{Z}_6) = 6 \qquad \text{Char}(\mathbb{Z}_n) = n.$

Theorem: Let R be a ring with identity 1_R. If the additive order of 1_R is infinite, then $\text{char}(R) = 0$. Otherwise, $\text{char}(R)$ is the additive order of 1_R.

Proof: Let $o(1_R) = \infty$ (w.r.t. $+$). Let 0_R be the additive identity.

Then $n 1_R \neq 0_R$ for all $n > 0$. Hence, $\text{char}(R) = 0$.

Let $o(1_R) = m$. Then, m is the smallest +ve integer such that
$$m 1_R = 0_R.$$

Let $x \in R$. Then
$$\begin{aligned} mx = m(1_R \cdot x) &= 1_R \cdot x + 1_R x + \cdots + 1_R \cdot x \\ &= (1_R + \cdots + 1_R) \cdot x \\ &= (m 1_R) \cdot x = 0_R \cdot x = 0. \end{aligned}$$

Thus, m is the smallest positive integer s.t. $mx = 0$ $\forall x \in R$.

$\therefore$ $\text{char}(R) = m$.

This completes the proof. #

__Example:__ $(\mathbb{Z}, +, \cdot)$ has identity 1.

Also, $o(1) = \infty$. Hence, $\mathrm{char}(\mathbb{Z}) = 0$.

__Example:__ $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. is a ring under addition modulo m and multiplication modulo m. The additive order of 1 is m, and hence

$\mathrm{Char}(\mathbb{Z}_m) = m$. #

Thm: Let R be an integral domain. Then, $\mathrm{char}(R)$ is either 0 or a prime.

Proof: If $\mathrm{char}(R) = 0$, there is nothing to prove.

Suppose that $\mathrm{char}(R) = n$. We need to prove that n is a prime number.

Consider a factorization of n, say, $n = mk$.

Then, $n \cdot 1 = 0 \Rightarrow mk \cdot 1 = 0 \Rightarrow (m \cdot 1) \cdot (k \cdot 1) = 0$

Since R is an integral domain, so either

$m \cdot 1 = 0$ or $k \cdot 1 = 0$

Since n is the least +ve integer such that $n.1=0$ and $1 \leq m, k \leq n$, so either $m=n$ or $k=n$.

This proves that n is a prime number. #.

§ Notation: Let R be a ring, and let I be a subset of R. For $a \in R$, define $aI = \{ax : x \in I\}$

$Ia = \{xa : x \in I\}$.

Definition (ideal): Let R be a ring and I be a subset of R. I is called a left ideal of R if (i) I is a subring of R (ii) $rx \in I$ $\forall r \in R, \forall x \in I$

Similarly, I is called a right ideal if

(i) I is a subring of R

(ii) $xr \in I \quad \forall\, x \in I$ and $\forall\, r \in R$.

A subset I of R that is both a left ideal and a right ideal is called an ideal of R.

(i) I is a subring

(ii) $xr,\ rx \in I \quad \forall\, x \in I,\ \forall\, r \in R$.

<u>Theorem:</u> Let I be a subset of a ring R. Then I is an ideal of R if (i) $a-b \in I \quad \forall\, a, b \in I$ (equivalently, $(I,+)$ is a subgroup of $(R,+)$).

(ii) $ra \in I$ and $ar \in I \quad \forall\, a \in I$ and $\forall\, r \in R$.

Ex: (i) The ideals of $(\mathbb{Z}, +, \cdot)$ are of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$.

(ii) Let $M_{2\times 2}(\mathbb{Z})$ be the ring of all the 2×2 matrices with integer entries.

In $M_{2\times 2}(\mathbb{Z})$, find a left ideal which is not a right ideal.

Also, find a right ideal which is not a left ideal.

#

Let I be an ideal of R.

$(I,+)$ is a subgroup of $(R,+)$

Since $(R,+)$ is abelian, so $(I,+)$ is a normal subgroup of $(R,+)$.

$(R/I,+)$ is an abelian group

$R/I = \{r+I : r \in R\}$ We define a multiplication in R/I as follows: $(r+I)\cdot(s+I) \coloneqq rs+I, \quad r,s \in R$

We prove that, if I is an ideal, then the multiplication of cosets is well defined.

Let $r+I = a+I$ and $s+I = b+I$, $r, s, a, b \in R$

<u>Claim:</u> $rs+I = ab+I$.

$$r+I = a+I \Rightarrow r-a \in I$$
$$s+I = b+I \Rightarrow s-b \in I.$$

Now, $$rs - ab = rs - rb + rb - ab$$
$$= \underbrace{r(s-b)}_{\in I} + \underbrace{(r-a)b}_{\in I}$$

Since $s-b \in I$ and I is an ideal, so $r(s-b) \in I$.
Similarly, $r-a \in I$
$\Rightarrow (r-a)b \in I$

$\therefore rs - ab \in I \Rightarrow rs+I = ab+I.$

Hence, given an ideal I of R, we have the following operations on $R/I = \{r + I \mid r \in R\}$.

Addition: $(r+I) + (s+I) = (r+s) + I$.

Multiplication: $(r+I)\cdot(s+I) = rs + I$.

Theorem: $R/I = \{r + I \mid r \in R\}$ is a ring w.r.t. the above two binary operations.

Ex: $\mathbb{Z}/n\mathbb{Z}$ is a ring under $(a+n\mathbb{Z}) + (b+n\mathbb{Z}) = (a+b) + n\mathbb{Z}$

$(a+n\mathbb{Z})\cdot(b+n\mathbb{Z}) = ab + n\mathbb{Z}$.

Clearly, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ is commutative with identity $1 + n\mathbb{Z}$.

Ex: $\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}, 1+6\mathbb{Z}, 2+6\mathbb{Z}, 3+6\mathbb{Z}, 4+6\mathbb{Z}, 5+6\mathbb{Z}\}$

$(2+6\mathbb{Z}) + (3+6\mathbb{Z}) = 5+6\mathbb{Z}$

$(2+6\mathbb{Z}) \cdot (3+6\mathbb{Z}) = 6+6\mathbb{Z} = 6\mathbb{Z}$, the zero of $\mathbb{Z}/6\mathbb{Z}$.

$\therefore$ $2+6\mathbb{Z}$ and $3+6\mathbb{Z}$ are zero divisors of $\mathbb{Z}/6\mathbb{Z}$.

#