

$$(2) \frac{\mathbb{Z}}{4\mathbb{Z}} = \{4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}.$$

$$(3) \frac{\mathbb{Z}}{2\mathbb{Z}} = \{2\mathbb{Z}, 1 + 2\mathbb{Z}\}.$$

Remark:

Let I be an ideal of R , the function $\pi: R \rightarrow R/I$ defined by $\pi(r) = r + I$, for all $r \in R$, is a ring epimorphism, it is called the natural epimorphism.

$$\begin{aligned}\pi(r_1 + r_2) &= \pi(r_1) + \pi(r_2) \\ \pi(r_1 \cdot r_2) &= \pi(r_1) \cdot \pi(r_2) \\ (r_1 \cdot r_2) \cdot I &= (r_1 + I) \cdot (r_2 + I)\end{aligned}$$

Remark: (Fund. Homo. Th. of rings) Let $f: R \rightarrow R'$ be a ring homomorphism, which is onto, then $\frac{R}{\ker f} \simeq R'$.

Proof: $g: \frac{R}{\ker f} \rightarrow R'$ (let $\ker f = k$) $g(r + k) = f(r)$

$$(1) r + k = r_1 + k \Leftrightarrow r - r_1 \in k$$

$$\Rightarrow f(r - r_1) = 0, f(r) - f(r_1) = 0 \Rightarrow f(r) = f(r_1)$$

$$\therefore g(r + k) = g(r_1 + k)$$

\therefore well defined

(2) g is homomorphism

$$g((r + k) + (r_1 + k)) = g(r + k) + g(r_1 + k)$$

$$g(r + r_1 + k) = f(r) + f(r_1)$$

$$\therefore f(r + r_1) = f(r) + f(r_1) \text{ (since } f \text{ is homo.)}$$

$\therefore g$ is homo.

(3) $g(r + k) = g(r_1 + k) \Rightarrow f(r) = f(r_1) \Rightarrow f(r) - f(r_1) = 0$ [since f is homomorphism]

$$f(r - r_1) = 0 \Rightarrow r - r_1 \in \ker f = k \Leftrightarrow r + k = r_1 + k \Rightarrow g \text{ is } (1 - 1)$$

(4) let $w \in R'$ since f is onto $\exists x \in R$, such that $f(x) = w$

$$g(x + k) = f(x) = w \Rightarrow g \text{ is onto.}$$

Example: Show that $\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n$

Solution: $f: \mathbb{Z} \rightarrow \mathbb{Z}_n, f(x) = \bar{x}$

$$\begin{aligned} f(x + y) &= \overline{x + y} = \bar{x} + \bar{y} = f(x) + f(y) \\ f(xy) &= \overline{xy} = \bar{x} \cdot \bar{y} = f(x) \cdot f(y) \end{aligned}$$

$\therefore f$ is homo.

Let $\bar{w} \in \mathbb{Z}_n \Rightarrow \exists w \in \mathbb{Z}$ such that $f(w) = \bar{w}$

$\therefore f$ is onto

by **F. H. Th.** $\frac{\mathbb{Z}}{\ker f} \simeq \mathbb{Z}_n$

$$\ker f = \{x \in \mathbb{Z} : f(x) = \bar{0}\} = \{x \in \mathbb{Z} : \bar{x} = \bar{0}\} = n\mathbb{Z}$$

$$\therefore \frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n.$$

Remark: The only nontrivial homo. from \mathbb{Z} to \mathbb{Z} is the identity.

Proof: $f: \mathbb{Z} \rightarrow \mathbb{Z}$ let $0 \neq n \in \mathbb{Z}$,

$$f(n) = \underbrace{f(1 + 1 + \dots + 1)}_{n \text{ times}} = \underbrace{f(1) + f(1) + \dots + f(1)}_{n \text{ times}}$$

[since f is homomorphism]

$$\begin{aligned} f(n) &= nf(1) \dots \dots \dots (*)\#(*) \\ f(n) &= f(n \cdot 1)\#(*) \\ f(n) \cdot 1 &= f(n) \cdot f(1) \Rightarrow f(1) = 1[\text{by } (*)]\#(*) \end{aligned}$$

$$\therefore f(n) = n$$

$\therefore f$ is identity.

Corollary (I): Let R be a ring and suppose that f, g a ring isomorphism, then $f = g: R \rightarrow Z$.

Proof: $f: R \rightarrow Z, g: R \rightarrow ZR \simeq Z$

$g^{-1}: Z \rightarrow R$ is a ring isomorphism

$$f \cdot g^{-1}: Z \rightarrow Z, \left(Z \xrightarrow{g^{-1}} R \xrightarrow{f} Z \right) \Rightarrow f \cdot g^{-1}: Z \rightarrow Z$$

$\therefore f \circ g^{-1} = I$ [by Remark]

$\therefore g = f$

Corollary (2): Let R be a ring and let $f, g: R \rightarrow Z$ be epimorphism then if $\ker f = \ker g$ then $f = g$.

Proof: by F. H. Th. $\frac{R}{\ker f} \simeq Z$ (f iso.) $\frac{R}{\ker g} \simeq Z$ (g* iso.) by coro.(1) $f^+ = g^*$

To prove that $f = g$

let $r \in R, f(r) = f'(r + \ker f)$

$\therefore f = g$.

Theorem: $Z_n \oplus Z_m \simeq Z_{nm}$ if and only if g.c. $d(n, m) = 1$.

Proof: we only have to show that $\frac{Z}{nz} \oplus \frac{Z}{mz} \simeq \frac{Z}{nmz}$ since by F. H. Th. $\frac{Z}{nz} \simeq Z_n$

and $Z_{nm} \simeq \frac{Z}{nmz}$

$$\phi: Z \rightarrow \frac{Z}{nz} \oplus \frac{Z}{mz}$$

$\phi(x) = (x + nZ, x + mZ) \forall x \in Z$ ϕ is a ring homo.?

ker

$$\phi = \{x \in Z: \phi(x) = (nZ, mZ)\} = \{x \in Z: (x + nZ, x + mZ) = (nZ, mZ)\}$$

$$= \{x \in Z: (x \in nZ, x \in mZ)\} = \{x \in Z: x \in nZ \cap mZ\} = nmZ \text{ since g.c.d}$$

$$(n, m)$$

$$= 1$$

$$\text{onto: Let } (a + nZ, b + mZ) \in \frac{Z}{nZ} \oplus \frac{Z}{mZ}$$

$$\text{g.c.d}(n, m) = 1 \Rightarrow \exists s, t \in Z$$

$$\Rightarrow S_n + t_m = 1$$

$$\begin{aligned} \phi(x) &= (x + nZ, x + mZ)\#(*) \\ &= (at_m + nZ, nS_n + mZ)\#(*) \\ &= (a + nZ, b + mZ)\#(*) \end{aligned}$$

$$a + nZ = at_m + nZ \Leftrightarrow a - at_m \in nZ \Leftrightarrow a(1 - t_m) \in nZ \Leftrightarrow aS_n \in nZ$$

$$\text{Similarly } bS_n + mZ = b + mZ \Leftrightarrow (b - bS_n) \in mZ \Leftrightarrow b(1 - S_n) \in mZ \Leftrightarrow$$

$$bt_m \in mZ$$

$\therefore \phi$ is onto.

Definition: A proper ideal M of a ring R is called maximal ideal if where ever I is an ideal of R with $M \subset I$, then $I = R$.

Example: In Z_6 the ideals are:

$$\{0\}, Z_6, \{\bar{0}, \bar{3}\}, \{\bar{0}, \bar{2}, \bar{4}\}$$

$$\{\bar{0}, \bar{3}\} \text{ is the maximal in } Z_6$$

$$\{\bar{0}, \bar{2}, \bar{4}\} \text{ is the maximal in } Z_6$$

Definition: A proper ideal P of a ring R is called a prime ideal if for all a, b in R with $a \cdot b \in P$ either $a \in P$ or $b \in P$.

Example:

$4Z$ is an ideal in Z , but not a prime ideal in Z . .1

$\{0\}$ is a prime ideal in Z .but not maximal. .2

$\{0\}$ is not a prime ideal in Z_6 .3

Definition: A commutative ring with identity is called an integral domain if it has no zero divisor.

Definition: A ring $(R, +, \cdot)$ is said to be field if $(R - \{0\}, \cdot)$ forms a commutative group (with identity 1).

Or

The field is commutative ring with identity in which each non-zero element has inverse under multiplication.

Remark: Every field is an integral domain.

Proof: Let R be a field and let $a, b \in R$ such that $a \cdot b = 0$

if $a \neq 0 \Rightarrow a$ has inverse say a^{-1} [since $a \in \text{field}$] $\Rightarrow a^{-1} \cdot a \cdot b = 0 \Rightarrow b = 0$
i.e., R is integral domain.

Remark: Let R be a commutative ring with identity then R is a field if and only if $\{0\}$ and R are the only ideals of R .

Proof: \Rightarrow let $I \neq 0$ be an ideal in R let $a \neq 0, a \in I$, but R is a field $\Rightarrow \exists a^{-1}$
and $a \cdot a^{-1} = 1 \in I$ [I ideal $a \in I, r \in R \Rightarrow ar \in I$] $\Rightarrow I = R$ [by remark]

\Leftarrow) let $a \neq 0, a \in R, \langle a \rangle$ is an ideal in R but $\langle a \rangle \neq \{0\} \Rightarrow \langle a \rangle = R$

$\therefore 1 \in R \Rightarrow 1 \in \langle a \rangle \Rightarrow 1 = r \cdot a$

Example: Q has ideals $\{0\}, Q$.

R has ideals $\{0\}, R$.

C has ideals $\{0\}, C$

Z has many ideals: Z_3, Z_5, Z_{2n+1} is field Z_2, Z_5, Z_{2n} is finite but not integral domain \Rightarrow not field.

Remark: Every finite integral domain is field.

Proof: Let $R = \{a_1, a_2, \dots, a_n\}$ be an integral domain and $0 \neq a_j \in R$

consider the set $S = \{a_1 a_j, a_2 a_j, \dots, a_n a_j\}$ all elements of S are distinct since if $a_\ell a_j = a_k a_j \Rightarrow a_\ell = a_k$!

Clearly $S \subseteq R$ and $R \subseteq S \Rightarrow S = R \Rightarrow 1 \in S$

$\Rightarrow 1 \in a_n a_j \Rightarrow a_j$ has inverse $\Rightarrow R$ is field.

Remark: Let R be an integral domain with only finite number of ideals in R then R is a field.

Proof: let $a \neq 0, a \in R, \langle a \rangle, \langle a^2 \rangle, \langle a^3 \rangle, \dots$, ideals in R but R has only finite number of ideals $\Rightarrow \exists k, \ell$ such that $k < \ell$ positive integers such that $\langle a^k \rangle = \langle a^\ell \rangle$

$\Rightarrow a^k \in \langle a^k \rangle = \langle a^\ell \rangle \Rightarrow a^k = r a^\ell$ for some $r \in R \Rightarrow a^k = r a^\ell = r a^{\ell-k} a^k$

R is integral domain \Rightarrow cancelation law is valid. $\Rightarrow 1 = r a^{\ell-k} \Rightarrow$ •

$$1 = (r a^{\ell-k-1}) a \text{ and } * 1 = a^{-1} a$$

$\therefore a^{-1} = r a^{\ell-k-1} \Rightarrow a^{-1}$ exists $\in R$

$\therefore R$ is a field.

Remark: if R is a field, then either f is $1 - 1$ or f is the zero homomorphism.

Proof: