Integral Domain = commutative ring R with $1 \in R$ s.t. there are no zero divisors

↓

i.e. $\nexists$ no $a \in R$ and $b \in R$ $a \neq 0, b \neq 0$ s.t. $a \cdot b = 0$.

$\mathbb{Z}$ 6.

$2 \cdot 3 = 6 = 0$

Theorem The characteristic of an integral domain is either zero or prime.

Proof: Let D be int. Domain, $\text{char}(D) = n \neq 0$

If n is not Prime

$n = ab \quad 1 < a < n \quad , \quad 1 < b < n$

Suppose $n \cdot 1 = 0 \Rightarrow (ab) \cdot 1 = 0$

$\Rightarrow (a \cdot 1)(b \cdot 1) = 0$

$\Rightarrow ab = 0$ But D is an integral Domain

$\Rightarrow$ either $a = 0$ or $b = 0$

$\Rightarrow a \cdot 1 = 0$ or $b \cdot 1 = 0$

$\Rightarrow \text{char}(D) < n$, this is a contradiction of $\text{char}(D) = n$.

$\Rightarrow$ either n is prime or 0.

Ring Homomorphisms + Ideals

Let R, S be rings. A ring homomorphism is a map $\phi : R \to S$ s.t. . Let $a, b \in R$

- $\phi(a+b) = \phi(a) + \phi(b)$
- $\phi(ab) = \phi(a) \cdot \phi(b)$ $\forall a, b \in R$.

If ϕ is 1-1 and onto $\Rightarrow$ ϕ is an isomorphism.

Def For any ring homomorphism $\phi : R \to S$ define:

$$\ker \phi = \{ r \in R \mid \phi(r) = 0 \}$$

Ex for any $n \in \mathbb{Z}$ we may define a ring hom.

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$
$$a \mapsto a \pmod n$$

$$\phi(a+b) = a+b \pmod n$$
$$= (a \bmod n) + (b \bmod n)$$
$$= \phi(a) + \phi(b)$$

$$\phi(ab) = ab \pmod n = (a \bmod n)(b \bmod n)$$
$$= \phi(a)\,\phi(b)$$

$\ker(\phi) = n\mathbb{Z}$ also write as

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

Ex | Fix $\alpha \in [a,b] \subseteq \mathbb{R}$

$$\phi_\alpha : C[a,b] \longrightarrow \mathbb{R}$$
$$f \longmapsto f(\alpha)$$

$$\phi_\alpha(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g)$$

$$\phi_\alpha(fg) = (fg)(\alpha) = f(\alpha)\,g(\alpha) = \phi_\alpha(f) \cdot \phi_\alpha(g).$$

Prop | Let $\phi : R \to S$ be a ring homomorphism.

- If R is commutive then $\phi(R)$ is commutive
- $\phi(0_R) = 0_S$
- Suppose $1_R \in R$. If ϕ is onto then $1_S \in S$ and $\phi(1_R) = 1_S$.
- If R is a feild and $\phi(R) \neq \{0\}$ then $\phi(R)$ is a feild.

Proof | Home work.

Def | An ideal I in a ring R is:

- I is a subring of R
- If $a \in I$, $r \in R \Rightarrow ar \in I$ and $ra \in I$
  $\Rightarrow$ that is $rI \subseteq I$ and $Ir \subseteq I$.

Ex | $\{0\}$ and R are always ideals of R

$n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Remark Let R be a ring with identity $1 \in R$

If I is an ideal and $1 \in I$

$\Rightarrow$ $I = R$ since for $r \in R$ $1 \cdot r = r \in I$ since I is an ideal.

Ex Let R be a commutative ring with $1 \in R$. For any $a \in R$

$$\langle a \rangle = \{ ar \mid r \in R \} \text{ — Principal ideal in } R$$

subring

- $\langle a \rangle$ is non-empty since $0 = a0 \in \langle a \rangle$ and $a = a \cdot 1 \in \langle a \rangle$
- $\langle a \rangle$ is closed under add., take $ar, ar' \in \langle a \rangle$ then $ar + ar' = a(\underbrace{r + r'}_{\in R}) \in \langle a \rangle$
- If $ar \in \langle a \rangle \Rightarrow$ as $-ar = a(-r) \in \langle a \rangle$.
- For any $ar \in \langle a \rangle$ pick $s \in R$

$$s(ar) = a\underbrace{sr}_{\in R} \in \langle a \rangle.$$

$\langle a \rangle$ is an ideal of R.

- An integral Domain where every ideal is Principal is called a principal ideal Domain P.I.D.

Theorem $\mathbb{Z}$ is a principal ideal domain.

Proof: • $\{0\} = \langle 0 \rangle$ is a principle ideal.

Let I to be any non-zero ideal in $\mathbb{Z}$

$\Rightarrow$ There is some positive $m > 0$ $m \in \mathbb{Z}$ s.t. $m \in I$

By the well ordering principle $\Rightarrow$ $\exists$ a least positive integer $n \in I$.

Choose an arbitrary $a \in I$. By the division algorithm $\exists\ q, r \in \mathbb{Z}$ s.t.

$n \in I$ since $n \in I$.

$$a = nq + r \quad \text{where} \quad 0 \leq r < n$$

$\in I$ since $a, nq \in I$.

$$\Rightarrow \quad r = a - nq$$

Note r is positive and $r < n$

$\Rightarrow$ $r = 0$ since n is the positive integer in I

$\therefore$ $a = nq$ $\forall\ a \in I$

$\Rightarrow$ $I = \langle n \rangle$. ∎