Veremos propiedades de los elementos de un anillo 9/10/24

Definición: sea R anillo. Un elemento $\overset{0}{\neq} a \in R$ se dice divisor de cero a izquierda (derecha) si $\exists b \in R$, $b \neq 0$ tal que $ab = 0$ (resp. $ba = 0$)

Si a es divisor de cero a izquierda y a derecha, entonces se dice que a es divisor de cero

Ejemplos:

1) En $\mathbb{Z}_n$, si n no es primo, tomamos $d | n \Rightarrow \bar{d}$ es un divisor de cero en $\mathbb{Z}_n$

2) En $M_n(R)$, $n > 1$ tomamos $A = \begin{pmatrix} 0 \cdots 0 \\ * \end{pmatrix} \neq 0$ $B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & & \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \neq 0$ si $1_R \neq 0$

Luego $BA = 0$ $\therefore$ A es divisor de cero a derecha

Notar que si tomamos A de cierta forma para que $AB \neq 0$ no implica que A no sea divisor de cero a izquierda

Definición: un anillo conmutativo con identidad $1 \neq 0$ se dice un dominio íntegro (o de integridad) si no posee divisores de 0

Ejemplos:

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ son dominios de integridad

2) $\mathbb{Z}_n$ es dominio de int. $\Leftrightarrow$ n es primo

Observemos que $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

divisores de cero en $\mathbb{Z}_n$ son las clases de los divisores de n pero si n es primo $\Rightarrow \nexists$ div. de cero.

3) $\mathbb{Z}[x]$, $\mathbb{Z}[x_1, \dots, x_k]$, etc son dominios de integridad

↳ polinomios con coefs. en $\mathbb{Z}$ y variables x_i

$0 \neq 1 \in R$ si $0 = na = (n \cdot 1)a$ $\Rightarrow n \cdot 1 = 0$ $\not\Rightarrow n = 0$ por ejemplo $\mathbb{Z}_p$

$p \neq 0$ pero $p \cdot 1 = 0$.

Definición: sea $\mathcal{R}$ un anillo con identidad y sea $a \in \mathcal{R}$ ($a \neq 0$). Se dice que a es:

inversible a izquierda $\iff \exists\, b \in \mathcal{R}$ tal que $ba = 1$

inversible a derecha $\iff \exists\, b \in \mathcal{R}$ tal que $ab = 1$

inversible si lo es a izquierda y a derecha

Un anillo D con $1 \neq 0$ donde todo elemento es inversible se llama un anillo de división;

Si además D es conmutativo, D se dice un cuerpo

Observación: si $a \in \mathcal{R}$ es inversible $\Rightarrow$ el inverso a izquierda de a coincide con su inverso a derecha y está unívocamenle determinado por a

Notación: a^{-1}

Demostración:

$b \cdot a = 1$ y $a \cdot c = 1$ entonces $b = b \cdot 1 = b \cdot (a \cdot c) = (ba)c = 1 \cdot c = c \Rightarrow b = c$

Esto también implica la segunda afirmación

Definición: el conjunto de los elementos inversibles en un anillo $\mathcal{R}$ (con $1 \neq 0$) se llama el grupo de unidades de $\mathcal{R}$

Notación: $\mathcal{R}^{\times}$ ó $\mathcal{R}^{*}$ ó $\mathcal{U}(\mathcal{R})$

Esto es un grupo con el producto de $\mathcal{R}$

Ejemplos:

1) $\mathbb{Z}_n^{\times} = \{ \bar{k} \in \mathbb{Z}_n \mid (k, n) = 1 \}$

2) $\mathbb{Z}^{\times} = \{ \pm 1 \}$

3) $\mathbb{Q}^{\times} = \mathbb{Q} - \{0\}$ (válido en cualquier cuerpo)

4) $(M_n(\mathbb{R}))^{\times} = GL(n, \mathbb{R})$

5) $\underset{\substack{\downarrow \\ \text{endomorfismos}}}{\mathrm{End}}(\mathbb{Z}) = \{ f : \mathbb{Z} \to \mathbb{Z},\ f \text{ homo} \}$

$(f+g)(x) = f(x) + g(x)$

$(f \cdot g)(x) = (f \circ g)(x) = f(g(x))$ $\quad \forall x \in \mathbb{Z}$

$0 \equiv x \longmapsto 0 \quad \forall x \in \mathbb{Z}$

$\Rightarrow \mathrm{End}(\mathbb{Z})^{\times} = \mathrm{Aut}(\mathbb{Z}) = \{ \pm id \}$

TEOREMA: sea R anillo con $1 \neq 0$ y característica $n > 0$, entonces si R no tiene divisores de $0 \Rightarrow n$ es primo.

Demostración:

Sea $n = \min\{k \in \mathbb{N} \mid k \cdot 1 = 0\}$

Si $n = m \cdot l$, $1 < m$, $l < m$ $\Rightarrow$ $(n \cdot 1) = (m \cdot 1) \cdot (l \cdot 1) = 0$

$\Rightarrow m \cdot 1 = 0$ ó $l \cdot 1 = 0$ contradicción por la minimalidad de n

$\therefore n$ es primo $\square$

Observación: sea R anillo sin divisores de cero y $a, b, c \in R$

$$\left.\begin{array}{lll} a \text{ izq.} & ab = ac & \Rightarrow b = c \\ a \text{ der.} & ba = ca & \Rightarrow b = c \end{array}\right\} a(b-c) = 0 \underset{a \neq 0}{\Rightarrow} b - c = 0 \Rightarrow b = c$$ $\square$

TEOREMA: sea R anillo, entonces R es isomorfo a un subanillo de un anillo S con 1

Demostración:

Sea $S = R \times \mathbb{Z}$ como grupo abeliano

$(a, m)(b, m) = (ab + mb + ma, mn)$ $\forall a, b \in R$, $m, n \in \mathbb{Z}$

Entonces S es un anillo con identidad $1 = (0, 1) \neq 0 = (0, \dots, 0)$

Sea $\varphi: R \to S$, $\varphi(a) = (a, 0)$ monomorfismo de anillos $\square$

Sea R anillo y una colección de ideales (resp. a izq/der) de R $\{I_j\}_{j \in \Lambda}$

- $\bigcap_{j \in \Lambda} I_j$ es un ideal (resp. a izq/der) de R
- $X \subseteq R$, $(X) = \bigcap_{\substack{I \text{ ideal} \\ X \subseteq I}} I$ es un ideal generado por X
- Un ideal $(\{x\})$ (generado por un sólo elemento) $(x \in R)$ se dice principal y se denota (x)

Definición: un dominio de integridad tal que todos sus ideales son principales se dice un dominio de ideales principales

Ejemplos: $\mathbb{Z}$, $\mathbb{Z}_n$

En el caso de polinomios, la minimalidad se ve en el grado de ellos

TEOREMA DE ISOMORFISMO

Sea R anillo, $I, J \subseteq R$ ideales:

1) Si $\varphi: R \longrightarrow S$ homo de anillos $R/_{\ker \varphi} \cong \operatorname{Im} \varphi$ (φ induce un iso de anillos)

2) $I+J/_J \cong I/_{I \cap J}$ es iso de anillos

si un ideal contiene a la identidad $\Rightarrow$ ese ideal es todo el anillo

3) Si $I \subseteq J \Rightarrow J/_I$ es ideal de $R/_I$ y $\dfrac{R/I}{J/I} \cong R/_J$ como anillos

Demostración:

Se reduce a probar que los iso de grupos abelianos correspondientes son efectivamente de anillos □

Definición: sea R anillo. Un ideal P de R tal que $P \neq R$ se dice primo si para cualquier par de ideales I, J de R vale que:

$$IJ \subseteq P \Rightarrow I \subseteq P \text{ ó } J \subseteq P$$

donde $IJ = \left\{ \sum_{i=1}^{r} a_i b_i \;\middle|\; r \in \mathbb{N},\ a_i \in I,\ b_i \in J \right\}$

TEOREMA: sea $P \subsetneq R$ ideal tal que para todo $a, b \in R$ se cumple que $ab \in P \Rightarrow a \in P$ ó $b \in P$. Entonces P es primo

Si R es conmutativo, vale la recíproca.

Demostración:

Sean $I, J \subseteq R$ ideales tales que $IJ \subseteq P$

Supongamos que $I \not\subseteq P \Rightarrow \exists a \in I$ tal que $a \notin P$

$\forall b \in J$ se tiene $ab \in IJ \subseteq P$

$\Rightarrow$ Como $a \notin P$ resulta que $b \in P$ $\therefore$ $J \subseteq P$ pues $\forall b \in J$ tenemos $b \in P$

Así P resulta ser primo (por hipótesis $P \neq R$)

Supongamos ahora que R es conmutativo y P es un ideal primo

Sean $a, b \in R$, $ab \in P$

$I = (a)$, $J = (b)$ $\Rightarrow$ Como $ab \in P$ se tiene $(ab) \subseteq P$

Además $IJ = (a)(b) \subseteq (ab)$ → aquí usamos que R es conmutativo

$(a) = \{ra + \underbrace{na}_{(n \cdot 1)a \text{ si } 1 \in R} \mid r \in R, n \in \mathbb{Z}\}$ → (Ejercicio: probarlo)

$r \in R$, si R no tiene a 1 $\Rightarrow$ (a) no tendría a "a" lo cual no puede ocurrir

Como P es primo $\Rightarrow$ $I = (a) \subseteq P$ ó $J = (b) \subseteq P$

$\Rightarrow$ $a \in P$ ó $b \in P$ $\square$

Ejemplo:

1) Si $R = \mathbb{Z}$ todo ideal es principal

$P = (p) \neq \mathbb{Z} \iff p \neq \pm 1$

$I = (a)$, $J = (b)$ ideales de $\mathbb{Z}$

$IJ = (ab) \subseteq P = (p) \iff p \mid ab \Rightarrow p \mid a$ ó $p \mid b \iff p$ primo

el ideal de p está formado por todos los múltiplos de p — p primo

2) $R \neq 0$ anillo sin divisores de cero $\Rightarrow \{0\}$ es un ideal primo

$ab \in \{0\} \Rightarrow a = 0$ ó $b = 0$

Si R es un anillo conmutativo $\Rightarrow$ es dominio de integridad $\iff \{0\}$ es ideal primo