ANILLOS

Propiedades de anillos

- Elemento nulo (suma) : $a + 0_R = a$
- Elemento opuesto (suma) : $a + (-a) = 0_R$
- Asociativa del producto : $(ab)c = a(bc)$
- Distributiva (suma y producto) : $a(b+c) = ab + ac$

Anillos que son cuerpos (para el producto)

- Conmutativa del producto : $ab = ba$
- Anillo con identidad : $a \cdot 1_R = a \quad \forall a \in R \rightarrow$ tiene elemento neutro
- Anillo de división (inverso) : $a \cdot a^{-1} = a^{-1} \cdot a = 1_R \rightarrow$ tiene inverso

Subanillo

$S \subseteq R$ es subanillo si $\forall a, b \in S$

1) $a - b \in S$
2) $a \cdot b \in S$

DOMINIO DE INTEGRIDAD

Divisor de cero

Si $\forall r, s \in R^*$, $r \cdot s = 0_R$, r es divisor de cero. $\rightarrow$ C_R = múltiplos de los factores

D.I

Un anillo conmutativo, con identidad y sin divisores de cero se denomina dominio de integridad (DI).

Unidades

$\exists a^{-1} \in R$ tal que $a \cdot a^{-1} = 1_R$, U_R es grupo

U_R se compone de todos los elementos de R que tengan un inverso contenido en R tal que $a \cdot a^{-1} = 1_R$

1) Cuerpo $\Rightarrow$ D.I $\rightarrow$ Probamos que es cuerpo para demostrar que es D.I
2) D.I finito $\Rightarrow$ Cuerpo

Característica.

$C = \{ r \in \mathbb{N} : r \cdot a = 0_R \text{ para todo } a \in R \} \Rightarrow c(R) = \min(C)$

1) $|1_R| < \infty \Rightarrow c(R) = |1_R|$
2) $|1_R| = \infty \Rightarrow c(R) = 0$

La característica de todo D.I o cuerpo es 0 o un nº primo.

* Ningún producto cartesiano es D.I $\Rightarrow$ no es cuerpo tampoco
* La característica de un producto cartesiano es mcm (m,n) o máx orden de un elemento del grupo
* $\mathbb{Z}$ es D.I pero no es cuerpo
* Matrices $\begin{cases} U = \{ A \in \mathbb{R}^{n \times n} : \det(A) \neq 0 \} \\ C = \{ A \in \mathbb{R}^{n \times n} : \det(A) = 0 \} \end{cases}$

* Ningún $\mathbb{Z}_p$, para p primo tiene divisores de cero.
* Los divisores de cero de productos cartesianos son del tipo

$(a, b) : a \in C(\mathbb{Z}_x), b \in C(\mathbb{Z}_y)$

En caso de que $\mathbb{Z}_x$ ó $\mathbb{Z}_y$ no tengan divisores de cero, se pone (0,b) ó (a,0) con todos los números pertenecientes del grupo correspondiente en cada caso.

Caracterización

Sea $I \subseteq R$, I es ideal $\Leftrightarrow$

1) $\forall a,b \in S \Rightarrow a-b \in I$
2) $\forall a \in I, \forall r \in R \Rightarrow ar, ra \in I$

En $(\mathbb{Z},+,\cdot)$ todos los $n\mathbb{Z}$ son subanillos ideales

I es propio si $I \neq R$

$I_0 = \{0\}$ es trivial de R

I es principal si $\exists a \in R : I = (a)$

En $(\mathbb{Z},+,\cdot)$ todos los ideales son principales.

En $(\mathbb{Z},+,\cdot)$ el ideal $(p) = p\mathbb{Z}$ es maximal $\Leftrightarrow$ p es primo

Anillo cociente

$R/I = \{[r]_I = r+I : r \in R\} \Rightarrow$ I es ideal de $R \Leftrightarrow (R/I,+,\cdot)$ es anillo.

$R/I = \{r+I : r \in R\}$

Ideales maximales

I es maximal $\Leftrightarrow (R/I,+,\cdot)$ es cuerpo $\Leftrightarrow I \subseteq J \subseteq R$

Ideal generador o ideal mínimo

Es el $\mathrm{mcd}(a,b) = M$ (suma)

Es el producto $a \cdot b = M$ (producto)

HOMOMORFISMOS

Comprobación de homomorfismo

1) SUMA: $\varphi(a+b) = \varphi(a) + \varphi(b)$
2) PRODUCTO: $\varphi(ab) = \varphi(a) \cdot \varphi(b)$

Comprobación de isomorfismo

1) Para que sea biyectiva tiene que ser inyectiva
   $\Rightarrow \ker \varphi = \{0\}$
2) Suprayectiva $\forall b \in H, \exists a \in A$ tq $\varphi(a) = b$

Núcleo e imagen

- $\ker(\varphi) = \{r \in R : \varphi(r) = 0_S\} \rightarrow$ es ideal de R
- $\varphi(R) = \{\varphi(r) : r \in R\} \rightarrow$ es subanillo de S

$\left.\begin{array}{l}\\\\\end{array}\right\} \varphi : R \rightarrow S$

$(\mathbb{Z}_n, +_n, \cdot_n) \rightarrow (\mathbb{Z}_m, +_m, \cdot_m)$

Homomorfismo $\varphi([1]_n) = [k]_m$

1) De grupos $\Leftrightarrow n \cdot k \equiv 0 \bmod m$
2) De anillos $\Leftrightarrow k^2 \equiv k \bmod m$

Sea $(R,+,\cdot)$ un anillo con identidad $\Rightarrow$

- $c(R) = n > 0 \Rightarrow R$ contiene un subanillo $\cong$ a $\mathbb{Z}_n$
- $c(R) = 0 \Rightarrow R$ contiene un subanillo $\cong$ a $\mathbb{Z}$.

Th de isomorfía

$R/\ker\varphi \cong \varphi(R)$

ANILLOS DE POLINOMIOS

$(R,+,\cdot)$ un anillo.

Polinomio nulo → $a_0 = a_1 = \dots = a_n = 0_R \in R$

Grado de $f \in R[x]$ → $gr(f) = n$

$gr(f) = -\infty$ → nulo

$gr(f) \leq 0$ → constante

$(R,+,\cdot)$ es conmutativo y con unidad ⇒ $(R[x],+,\cdot)$ también.

Polinomio <u>mónico</u> → $cp(f) = a_n = 1_R \in R$

Se dice que <u>α es raíz</u> de $f \iff f(\alpha) = 0_R$

Si R es dominio de integridad ⇒ R[x] lo es y $gr(f \cdot g) = gr(f) + gr(g)$

Bezout

Algoritmo de la división → $mcd(f,g) = d$

IDEALES MAXIMALES

$(K,+,\cdot)$ cuerpo

Sea $f \in K[x]$ con grado $(f) = n$ ⇒ es irreducible ⇔ no puede ser expresado como producto de polinomios de grado estrictamente menor que f.

1) $\mathbb{C}[x] \iff gr(f) = 1$
2) $\mathbb{R}[x] \iff gr(f) = 1$ ó $gr(f) = 2$ y $b^2 - 4ac < 0$
3) $\mathbb{Q}[x] \iff$
   - Eisentein para p primo
   - Raíces racionales tq $\alpha = \frac{r}{s} \in \mathbb{Q}$, $r \mid a_0$, $s \mid a_n$
   - Irreducible en $\mathbb{Z}_p$, es decir, ⇔ es distinto al producto de dos irreducibles en $\mathbb{Z}_p$. ó no puede dividirse por un irreducible.
4) Los polinomios de grado 2 y 3 son irreducibles ⇔ no tienen raíces.

Teoremas

1) Resto: $x \in K[x]$ ⇒ $f(\alpha)$ es el resto de $f/x-\alpha$
2) Factor: $a \in K[x]$ es raíz ⇔ $x-\alpha \mid f$ en $K[x]$

Ideales en K[x]

- Sea $(K,+,\cdot)$ cuerpo ⇒ todo ideal de $(K[x],+,\cdot)$ es principal
- Sea $(K,+,\cdot)$ cuerpo ⇒ f es maximal si es irreducible en $K[x]$.

CUERPOS DE FRACCIONES

Cuerpo de fracciones

Sea $(D,+,\cdot)$ un dominio de integridad, se denomina al cuerpo

$Cf(D) = \{\frac{a}{b} : a,b \in D, b \neq 0_D\}$ es cuerpo y mínimo cuerpo que contiene un anillo isomorfo a D.

Extensiones de cuerpos

Sea $K \subseteq F$ ⇒ K es subcuerpo de F y F extensión de K.

El <u>mínimo subanillo</u> que contiene a un cuerpo y a un elemento α que no pertenece a es cuerpo, sino a su extensión es $K[\alpha] \subseteq F$

El <u>mínimo cuerpo</u> que contiene a un cuerpo y un elemento a que no pertenece a ese cuerpo, sino a su extensión, es $K(\alpha) = Cf(F[\alpha]) \subseteq F$.

Los cuerpos $(\mathbb{Q},+,\cdot)$ y $(\mathbb{Z}_p,+_p,\cdot_p)$ son cuerpos mínimos y si

- $c(D)=0 \Rightarrow D \subseteq \mathbb{Q}$
- $c(D)=p \Rightarrow D \subseteq \mathbb{Z}_p$

KRONECKER

Sea $(\mathbb{K},+,\cdot)$ y $h \in \mathbb{K}[x]$ un polinomio irreducible con $gr(h)>1 \Rightarrow$

1) Existe una extensión $\mathbb{F}$ de $\mathbb{K}$ donde h tiene una raíz
2) Si $\alpha \in \mathbb{F}$ es raíz de $h \Rightarrow \mathbb{K}(\alpha) \approx \mathbb{K}[x]/(h) \approx \mathbb{K}[\alpha]$

Además $\mathbb{K}[x]/(h)$ es cuerpo $\Leftrightarrow h$ es irreducible.

El $cf(\mathbb{Z})=\mathbb{Q}$ y cualquier anillo contenido en $\mathbb{Z}$ tiene como cuerpo de fracciones a $\mathbb{Q}$

BASES

α es algebraico sobre $\mathbb{K}$ si $f(\alpha)=0$ (es raíz de f) y entonces f es el polinomio mínimo mónico.

α es algebraico $\Leftrightarrow \mathbb{K}[\alpha]=\mathbb{K}(\alpha)$

Grado de extensión

Si $\alpha \in \mathbb{F}$ es algebraico sobre $\mathbb{K} \Rightarrow$ el grado del polinomio mínimo de α sobre $\mathbb{K}$ es $[\mathbb{K}(\alpha):\mathbb{K}]=n$ (grado del polinomio mínimo) y una base de $\mathbb{K}(\alpha)$ es $B=\{1,\alpha,\alpha^2,\dots,\alpha^{n-1}\}$.

Polinomios irreducibles

En $\mathbb{Z}_2[x] \rightarrow x^2+x+1$

En $\mathbb{Z}_3[x] \rightarrow \begin{cases} x^2+1 \\ x^2+x+2 \\ x^2+2x+2 \end{cases}$

3.1. ANILLOS Y SUBANILLOS

1. Estudiar conjuntos

a) $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ siendo $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} \,;\, a,b \in \mathbb{Q}\}$

- $(a+b\sqrt{2}) - (c+d\sqrt{2}) = a-c+(b-d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$
  $a,b,c,d \in \mathbb{Q} \Rightarrow a-c,\ b-d \in \mathbb{Q}$
- $(a+b\sqrt{2})(c-d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

} CARACTERIZAC. DE SUBANILLO

- $I = 1+0\sqrt{2} = 1 \in \mathbb{Q}[\sqrt{2}]$ CON IDENTIDAD
- ES CONMUTATIVO
- $a+b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$; $\frac{1}{a+b\sqrt{2}} \in \mathbb{R} \Rightarrow \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}$

$\Rightarrow$ ¿ $\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2} \in \mathbb{Q}$? | Para que esté en $\mathbb{Q}$ tienen que ser números racionales.

$a^2-2b^2 \neq 0$ ya que si $a^2-2b^2=0$ entonces $2 = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 \Rightarrow \sqrt{2}$ sería racional !!!

ES DE DIVISIÓN

b) $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ siendo $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbb{Z}\}$

Mismo razonamiento. Cuando todos nos da división.

c) $(S, +, \cdot)$ siendo $S = \{a+b\sqrt{2}+c\sqrt{3} : a,b,c \in \mathbb{Z}\}$

- $(a+b\sqrt{2}+c\sqrt{3}) - (d+e\sqrt{2}+f\sqrt{3}) = (a-d)+(b-e)\sqrt{2}+(c-f)\sqrt{3} \in S$
- $(a+b\sqrt{2}+c\sqrt{3})(d+e\sqrt{2}+f\sqrt{3}) = (ad+2be+3cf)+(ae+bd+3cf)\sqrt{2}+(af+cd)\sqrt{3}+$
  $+(bf+ce)\sqrt{6} \in S$ ES SUBANILLO

d) $(\mathbb{Z}[i], +, \cdot)$ siendo $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}] = \{a+bi : a,b \in \mathbb{Z}\}$

- $(a+bi) - (c+di) = (a-c)+(b-d)i \in \mathbb{Z}[i]$
- $(a+bi)(c+di) = (ac-bd)+(ad+bc)i \in \mathbb{Z}[i]$
- $I = 1+0i = 1$
  $1(a+bi) = 1a + (1b)i = a+bi$ ES DE IDENTIDAD

NO ES DE DIVISIÓN

↳ $a+bi \in \mathbb{Z}[i]$ $\frac{1}{a+bi} \in \mathbb{C}$

$$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i \Rightarrow (1+i)^{-1} = \frac{1}{2} - \frac{1}{2}i \in \mathbb{Z}[i]$$

e.) $(\mathbb{Z}_p[i], +_p, \cdot_p)$ siendo $\mathbb{Z}_p[i] = \mathbb{Z}_p[\sqrt{-1}] = \{a+bi : a, b \in \mathbb{Z}_p\}$

1. $(a+bi)+((c+di)+(e+fi)) = ((a+bi)+(c+di))+(e+fi)$
   Suma módulo p.
2. $[0]_p \in \mathbb{Z}_p[i]$ es neutro de $(\mathbb{Z}_p[i], +_p)$
3. $\forall a+bi \in \mathbb{Z}_p[i]$ $\exists -a-bi \in \mathbb{Z}_p[i]$ tq $(a+bi)+(-a-bi)=0$
4. $(a+bi)+(c+di) = (c+di)+(a+bi)$
5. $(a+bi)[(c+di)(e+fi)] = [(a+bi)(c+di)](e+fi)$
6. $(a+bi)[(c+di)+(e+fi)] = (a+bi)(c+di)+(a+bi)(e+fi)$

↳ Es anillo

↕ Ambos casos de la igualdad y si coinciden, cumple la prop.

- Conmutativo $(a+bi)(c+di) = (c+di)(a+bi)$
  (La suma también lo es)
- $I = 1 + [1]_p$ de identidad
- $a+bi \in \mathbb{Z}_p[i] \Rightarrow \frac{1}{a+bi} \in \mathbb{C} \Rightarrow \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$ ¿$\in \mathbb{Z}_p[i]$?
  Depende del valor de p.
  Si $a^2+b^2 \neq p$ = si pertenece

[Si $p \equiv 1 \bmod 4 \Rightarrow p = a^2+b^2 \Rightarrow$ NO ES DE DIVISIÓN
  Si $p \equiv 3 \bmod 4 \Rightarrow p \neq a^2+b^2 \Rightarrow$ SÍ ES DE DIVISIÓN

g.) $(T, +, \cdot)$ siendo $T = \{a+bi : a \in \mathbb{Z}, b \in 2\mathbb{Z}\}$

$L_0 = \{a+2bi : a, b \in \mathbb{Z}\}$

- $(a+2bi)-(c+2di) = (a-c)+2(b-d)i \in T$
- $(a+2bi)(c+2di) = ac-4bd+2(ad+bc)i \in T$

  } SUBANILLO

- T es subanillo de $\mathbb{C}$ que es conmutativo $\Rightarrow$ T conmutativo
- $1 = T_1 \in T$ tiene identidad $1(a+2bi) = a+2bi \in T$
- No es de división

$$\frac{1}{a+2b} \in \mathbb{C} \Rightarrow \frac{a-2bi}{a^2+4b^2} = \frac{a}{a^2+4b^2} - \frac{2b}{a^2+4b^2}i \notin T$$

2. $(\mathbb{Z}, \oplus, \odot)$ Anillo $\begin{cases} x \oplus y = x+y-k \\ x \odot y = x+y-mxy \end{cases}$ Conm.? Ass.? Dist.? Cuerpo?

- $x \oplus y = x+y-k$
  - 1. $x \oplus (y \oplus z) = x \oplus (y+z-k) = x+y+z-k-k = x+y+z-2k$
    $(x \oplus y) \oplus z = (x+y-k) \oplus z = x+y-k+z-k = x+y+z-2k$
  - 2. $x \oplus y = x+y-k$
    3. $y \oplus x = y+x-k$
    $\Big\} \; x \oplus y = y \oplus x$
  - 4. E neutro de $\oplus$ e: $x \oplus e = x$, $e = k$; $x+e-k = x$ $\Big\}$ $\boxed{e=k}$
  - 5. E. opuesto de a en $\oplus$: $a \oplus a' = k$, $a+a'-k = k$ $\Big\}$ $\boxed{a' = 2k-a}$

  Es ABELIANO

- $x \odot y = x+y-m$
  - 1. $(x \odot y) \odot z = (x+y-mxy) \odot z = x+y-mxy+z-mxz-myz+m^2xyz$
    $x \odot (y \odot z) = x \odot (y+z-myz) = x+y+z-myz-mxy-mxz+m^2xyz$
  - 2. $x \odot (y \oplus z) = x \odot (y+z-k) = x+y+z-k-mxy-mxz+mkx$
    $(x \odot y) \oplus (x \odot z) = (x+y-mxy) \oplus (x+z-mxz) = x+y-mxy+x+z-mxz-k =$
    $= x+y+z-k-mxy-mxz+x$

  Son iguales $\Leftrightarrow mkx = x \Leftrightarrow mk = 1 \Leftrightarrow \begin{cases} m=k=1 \\ m=k=-1 \end{cases}$

8. $(S, +_1, \cdot_1)$ y $(T, +_2, \cdot_2)$ anillos y $R = S \times T$ (anillo producto)

a) Si S y T son conmutativos $\Rightarrow$ R conmutativo

$(a,b)(c,d) = (a \cdot_1 c, b \cdot_2 d) = (c \cdot_1 a, d \cdot_2 b) = (c,d)(a,b)$

b) Si S y T tienen U. resp. $1_S \in S$ y $1_T \in T \Rightarrow$ R tiene U.

$1_S \times 1_T = (1_S, 1_T)$

c) Si S y T son cuerpos ¿R es cuerpo?

Aunque S y T sean cuerpos, va a haber elementos que a $S \times T$ no tenga inverso.

$a \neq 0_S$ $\qquad$ $1_{S \times T} = (1_S, 1_T)$

$(a, 0_T) \neq (0_S, 0_T)$

¿$\exists (b,c)$ tq $(a,0_T)(b,c) = (1_S, 1_T)$? $\Rightarrow$ NO, No existe.

3.2 DOMINIOS DE INTEGRIDAD

1. Unidades de los anillos

a) $(\mathbb{Z}, +, \cdot) \Rightarrow U_{\mathbb{Z}} = \{1, -1\}$

b) $(\mathbb{Z} \times \mathbb{Z}, +, \cdot) \Rightarrow \{(a,b) : a, b \in U_{\mathbb{Z}}\}$

$(1,1), (1,-1), (-1,1), (-1,-1)$

c) $(\mathbb{Z}_3, +_3, \cdot_3) \Rightarrow U_{\mathbb{Z}_3} = \{1, 2\}$

d) $(\mathbb{Q}, +, \cdot) \Rightarrow U_{\mathbb{Q}} = \{r \in \mathbb{Q} : r \neq 0\}$ → $(\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}, +, \cdot)$

e) $(\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}, +, \cdot) \Rightarrow U_{\mathbb{Z} \times \mathbb{Q} \times \mathbb{Z}} = \{(a,b,c) : a, c \in \{1,-1\}, b \in \mathbb{Q} : r \neq 0\}$

f) $(\mathbb{R}^{n \times n}, +, \cdot) \Rightarrow U_{\mathbb{Z}_4} = \{1, 3\}$

2. Divisores de cero y unidades anillo

a) $(\mathbb{Z}_{10}, +_{10}, \cdot_{10})$

$C_{10} = \{2, 4, 5, 6, 8\}$

$U_{10} = \{1, 3, 7, 9\}$

b) $(\mathbb{Z}_{12}, +_{12}, \cdot_{12})$

$C_{12} = \{1, 2, 3, 4, 6,$

$U_{12} = \{1, 5, 7, 11\}$

c) $(\mathbb{Z}_4 \times \mathbb{Z}_2, +_4 \times +_2, \cdot_4 \times \cdot_2)$

$U_{\mathbb{Z}_4 \times \mathbb{Z}_2} = \{(1,1)(2,2)(4,1)(5,1)(7,1)(8,1)\}$

$C_{\mathbb{Z}_4 \times \mathbb{Z}_2} = \{(a,0) : a \in \{1,2,3,\ldots 8\}\} \cup \{(0,1)(3,1)(6,1)\}$

↑ cuando es 0, todos divisores — ↑ cuando es 1, solo div. $\mathbb{Z}_4$.

d) $(P(X), \Delta, \cap)$, siendo $A \Delta B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

$0_{P(X)} = \emptyset$, $1_{P(X)} = X$

$\forall A \subset X, A \neq \emptyset, A \neq X \Rightarrow$ (complementario) $A^c \neq X, A^c \neq \emptyset \Rightarrow A \cap A^c \neq \emptyset$

$\Rightarrow A$ es un divisor de cero

La unidad es el total es $U_{P(X)} = \{X\}$

e) $(\mathbb{Z}_2^{2\times 2}, +, \cdot)$

$U_{\mathbb{Z}_2^{2\times 2}} = \{\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\1&1\end{pmatrix}\begin{pmatrix}1&0\\1&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\}$

$C_{\mathbb{Z}_2^{2\times 2}} = \{\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\1&1\end{pmatrix}\begin{pmatrix}1&0\\1&0\end{pmatrix}\begin{pmatrix}0&1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\1&1\end{pmatrix}\}$

↳ Al cuadrado $= \begin{pmatrix}0&0\\0&0\end{pmatrix} \Rightarrow$ DIVISORES

8.) $(\mathbb{R}^{n\times n}, +, \cdot)$

$U_{\mathbb{R}^{n\times n}} = \{A \in \mathbb{R}^{n\times n} : \det(A) = 0\}$

$C_{\mathbb{R}^{n\times n}} = \{A \in \mathbb{R}^{n\times n} : \det(A) = 0\}$

3. Dem todo dom no nulo de $(\mathbb{Z}_n, +_n, \cdot_n)$ es unidad o divisor de cero.

Cualquier dom $r \in \mathbb{Z}_n$, $r \neq 0$, $1 \leq r < n$

Se verifica que $mcd(r, n) = d$ y ocurre que:

a) $d = 1 \Rightarrow 1 = r \cdot k + n \cdot y \Rightarrow [1]_n = [r]_n \cdot [x]_n + [0]_n \Rightarrow$

$\Rightarrow [r]^{-1}_n = [x]_n \Rightarrow r$ es una unidad.

b) $d > 1 \Rightarrow n = d \cdot q_1$, $r = d \cdot q_2$ $\Rightarrow d \cdot q_1 \cdot q_2 = r \cdot q_1 = n \cdot q_2 = 0$ mod n

$\Rightarrow [r \cdot q_1]_n = [0]_n \Rightarrow [r]_n [q_1]_n = [0]_n \Rightarrow$ r tiene divisor de cero.

4. Encontrar dom. de un anillo no divisor de cero ni unidad.

En $(\mathbb{Z}, +, \cdot)$, $n = 2$ (el cual $\neq -1, 1$) no es divisor de 0 y tampoco unidad

Lo es un dominio de integridad.

Otras unidades son 1 y -1 y no tiene div. de cero.

5. a y $b \in \mathbb{R}$ en $(\mathbb{R}, +, \cdot)$, son divisores de cero pero $a+b$ no es ni div.

$(\mathbb{Z}_{10}, +_{10}, \cdot_{10})$

$a = 2$, $b = 5$ ambos son divisores de cero

pero $a + b = 7$ no es div. de cero, pero es unidad en $\mathbb{Z}_{10}$

6. Anillos $\Rightarrow$ dom. de integridad? cuerpos?

a) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$

Nada que sea producto cartesiano es un dominio de integridad $\Rightarrow$

$\Rightarrow$ no es cuerpo.

$(0,1) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ divisor de cero

$(0,1)(1,0) = (0,0)$

b) $(\mathcal{P}(\{a\}), \Delta, \cap)$, sea $A \Delta B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

$0_{\mathcal{P}(\{a\})} = \emptyset$ $\quad \mathcal{P}(\{a\}) = \{\emptyset, \{a\}\}$ solo contiene 2 elementos no es DI (cuerpo).

$1_{\mathcal{P}(\{a\})} = \{a\}$ y la otra $i^2 = 0$ es con INTEGRIDAD

Si es un cuerpo (todo elem que no sea 0 tiene elem inverso.)

$\forall x \in \mathcal{P}(\{a\})$ con $x \neq 0_{\mathcal{P}(\{a\})} = \emptyset$ resulta que $x = \{a\}$

$\{a\} \cap \{a\} = \{a\} = 1_{\mathcal{P}(\{a\})}$

c) $(\{a+bi : a, b \in \mathbb{Q}\}, +, \cdot)$

Probamos que es cuerpo $\Rightarrow$ Si (o es) $\Rightarrow$ es D.I

$a+bi \in \mathbb{Q}$ $a, b \in \mathbb{Q}$, $a+bi \neq 0 \Leftrightarrow a^2+b^2 \neq 0$

En $\mathbb{Q}$ $\frac{1}{a+bi} = \underbrace{\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2} i}_{*} \Rightarrow \frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \mathbb{Q} \Rightarrow * \in M$

$a, b \in \mathbb{Q}$, $a^2+b^2 \neq 0$

Como nos dieron, entonces ES CUERPO $\Rightarrow$ DI

- CONMUTATIVO ✓
- CON IDENTIDAD ✓
- DE DIVISIÓN ✓

d) $(\mathbb{Z} \times \mathbb{R}, +, \cdot)$

No DI $\Rightarrow$ NO es cuerpo.

e) $(\{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}, +_{10}, \cdot_{10})$

$\cdot_{10}$	2	4	(6)	8
2	4	8	2	[6]
4	8	[6]	4	2
(6)	2	4	[6]	8
8	[6]	2	8	4

Busco $i^2 = 1 \Rightarrow$ es 6 $\boxed{1^2 = 6}$

¿Es de div? Todos tienen inverso $\Rightarrow$ de división

$\boxed{\forall a - b = 6}$

7. El anillo conmutativo sin divisores de cero que no son integros.

- CONM.
- NO DIV 0
- NO D I
- DIV IDENT.

Sabemos que DI es anillo, conmutativo, íntegros y sin divisores de cero. Luego tenemos que encontrar, alguno anillo sin íntegros.

Ej: $(2\mathbb{Z}, +, \cdot)$

Cualquier $n\mathbb{Z}$, $n \neq 1$

8. Anillo $(R,+,\cdot)$ $\begin{cases} \text{IDEMPOTENTE } a^2=a \\ \text{NILPOTENTE } a^n=0 \end{cases}$ $\mathbb{Z}_3 \times \mathbb{Z}_6$

$U_{\mathbb{Z}_3\times\mathbb{Z}_6} = \{(1,1)(1,5)(2,1)(2,5)\}$ $\begin{cases} a=\{1,2,3,..\} \\ b=\{0,2,3,4\} \end{cases}$

$C_{\mathbb{Z}_3\times\mathbb{Z}_6} = \{(0,a)(1,5)(2,5)\}$

$a^2=a \Rightarrow a^2-a=0 \Leftrightarrow a(a-1)=0$ (I. compatible)

$I_{\mathbb{Z}_3}=\{0,1\}$
$I_{\mathbb{Z}_6}=\{0,1,3,4\}$ $\Big\} I_{\mathbb{Z}_3\times\mathbb{Z}_6}=\{(a,5): a\in\{0,1\}, b\in\{0,1,3,4\}\}$

$a^n=0 \Rightarrow a.a^{n-1}=0 \Rightarrow a$ es divisor de cero
$n>1$

$Nilp_{\mathbb{Z}_6\times\mathbb{Z}_6}=\{(0,0)\}$

9. Si $a\in R$ es nilpotente en anillo con id $(R,+,\cdot)$, probar 1_R-a es unidad

$(1-a)(1+a+..a^{n-1})$ siendo $a^n=0$, $n\geq 1$

$1+a+..a^{n-1}-a-a^2-..a^n = 1-a^n = 1$

$(1-a)^{-1}=(1+a+..a^{n-1})$

10. Característica de anillos:

a) $(\mathbb{Z},+,\cdot) \Rightarrow C(\mathbb{Z})=0$

b) $(\mathbb{Z}\times\mathbb{Z},+,\cdot) \Rightarrow C(\mathbb{Z}\times\mathbb{Z})=0$

c) $(\mathbb{Z}_3\times 3\mathbb{Z},+,\cdot) \Rightarrow C(\mathbb{Z}_3\times 3\mathbb{Z})=0$

d) $(\mathbb{Z}_3\times\mathbb{Z}_3,+,\cdot) \Rightarrow C(\mathbb{Z}_3\times\mathbb{Z}_3)=|1_{\mathbb{Z}_3\times\mathbb{Z}_3}|=3$

e) $(\mathbb{Z}_3\times\mathbb{Z}_4,+,\cdot) \Rightarrow C(\mathbb{Z}_3\times\mathbb{Z}_4)=12$

f) $(\mathbb{Z}_6\times\mathbb{Z}_{15},+,\cdot) \Rightarrow C(\mathbb{Z}_6\times\mathbb{Z}_{15})=mcm(6,15)$

g) $(\mathbb{Z}_m\times\mathbb{Z}_n,+,\cdot) \Rightarrow C(\mathbb{Z}_m\times\mathbb{Z}_n)=mcm(m,n)$

h) $(\{[0]_{12},[2]_{12},[4]_{12},[6]_{12},[8]_{12},[10]_{12}\},+_{12},\cdot_{12})$

$|0|=1 \quad |4|=3 \quad |8|=3$
$|2|=6 \quad |6|=2 \quad |10|=6$ $\quad C(R)=6$

11. $(R,+,\cdot)$ anillo conmutativo con id. Si $C(R)=p$ primo $\Rightarrow (x+y)^p=x^p+y^p$

Anillo con caract. $C(R)=4$ ej $(x+y)^4 \neq x^4+y^4$

$(x+y)^p=\binom{p}{0}x^p+\binom{p}{1}x^{p-1}y+..\binom{p}{p-1}xy^{p-1}+\binom{p}{p}y^p=\sum\binom{p}{k}x^k y^{p-k}$

$\binom{p}{k}=\frac{p!}{k!(p-k)!}=p\frac{(p-1)!}{k!(p-k)!}$, $0<k<p \Rightarrow 0<p-k<p$

Si p primo es múltiplo de $p \Rightarrow \binom{p}{k}\equiv 0 \bmod p$ si $\begin{cases} 0<k<p \\ p \text{ primo} \end{cases}$

$(x+y)^p=x^p+y^p \bmod p$ con p primo

En $\mathbb{Z}_4$ $\begin{cases} (1+3)^4=4^4=0 \\ 1^4+3^4=2 \end{cases} \neq 4$ se demuestra

3.4 HOMOMORFISMO DE ANILLOS

3. Det homomorfismos de anillos en cada caso:

a) Del anillo $(\mathbb{Z}_{20}, +_{20}, \cdot_{20})$ en el anillo $(\mathbb{Z}_{30}, +_{30}, \cdot_{30})$

$\varphi: \mathbb{Z}_{20} \longrightarrow \mathbb{Z}_{30}$ $\quad \begin{cases} 20\,a \equiv 0 \mod 30 \\ a^2 \equiv a \mod 30 \end{cases}$

$\varphi([1]_{20}) = [a]_{30}$

$a \in \{0, \cancel{3}, 5, \cancel{9}, \cancel{11}, 15, \cancel{18}, 21, \cancel{24}, \cancel{29}\}$

b) Del anillo $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$ en el anillo $(\mathbb{Z}, +, \cdot)$

$\varphi: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$

$\varphi((n,m)) = \varphi((n,0)+(0,m)) = \varphi((n,0)) + \varphi((0,m)) = n\varphi((1,0)) + m\varphi((0,1))$

$\varphi((1,0)) = \varphi((1,0)\cdot(1,0)) = \varphi((1,0))^2$ $\quad \begin{cases} \varphi((1,0)) = a \\ \varphi((0,1)) = b \end{cases}$

$a = a^2 \quad a(a-1) = 0$

$b = b^2 \quad b(b-1) = 0$ $\Rightarrow a, b \in \{0, 1\}$

$\varphi((1,1)) = \varphi((1,1)(1,1)) = \varphi((1,1))^2 \Rightarrow$

$a+b \qquad (a+b)^2 = a^2 + b^2 + 2ab$

$\Rightarrow$ ① $\varphi_1((a,b)) = a$

② $\varphi_2((a,b)) = b$

③ $\varphi_3((a,b)) = 0$

4. Dem único homomorfismo de anillos entre $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ y $(\mathbb{Z}[\sqrt{3}], +, \cdot)$ homom. nulo.

$\varphi = \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Z}[\sqrt{3}]$ homomorfismo de anillos

$a+b\sqrt{2} \qquad c+d\sqrt{3}$

$\varphi(a+b\sqrt{2}) = \varphi(a) + b\varphi(\sqrt{2}) = a\varphi(1) + b\varphi(\sqrt{2})$

$\varphi(1) = \varphi(1\cdot 1) = \varphi(1)^2 \Rightarrow \varphi(1) = a \Rightarrow a = a^2 \Rightarrow a \in \{0, 1\}$

$\varphi(\sqrt{2}) = c + d\sqrt{3}$

$\varphi(\sqrt{2}\cdot\sqrt{2}) = (c+d\sqrt{3})^2 = \varphi(2) = 2\varphi(1) = 2a$

$2a = c^2 + 3d^2 + 2cd\sqrt{3} \Rightarrow$ $\begin{cases} a = 0 \Rightarrow c^2 + 3d^2 = -2cd\sqrt{3} \Rightarrow \\ \Rightarrow c^2 + 3d^2 = 0 \Rightarrow c = d = 0 \\ a = 1 \Rightarrow 2 = c^2 + 3d^2 + 2cd\sqrt{3} \text{ !!!} \end{cases}$

$\Rightarrow \varphi(a+b\sqrt{2}) = 0$

5. Estudiar si pares de anillos son isomorfos

a) $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ y $H = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ (suma y prod)

$\varphi : \mathbb{Z}[\sqrt{2}] \longrightarrow \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \; a, b \in \mathbb{Z} \right\}$

$a + \sqrt{2}\, b \longrightarrow \varphi(a+b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \Rightarrow$ APLICACIÓN BIEN DEFINIDA

SUMA $\varphi((a+b\sqrt{2}) + (c+d\sqrt{2})) = \varphi((a+c) + \sqrt{2}(b+d)) = \begin{pmatrix} a+c & 2(b+d) \\ b+d & a+c \end{pmatrix}$

$\varphi(a+b\sqrt{2}) + \varphi(c+d\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + \begin{pmatrix} c & 2d \\ d & c \end{pmatrix} =$ → son iguales

PROD $\varphi((a+b\sqrt{2})(c+d\sqrt{2})) = \varphi((ac+2bd) + \sqrt{2}(ad+bc)) = \begin{pmatrix} ac+2bd & 2(ad+bc) \\ ad+bc & ac+2bd \end{pmatrix}$

$\varphi(a+b\sqrt{2})\varphi(c+d\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}\begin{pmatrix} c & 2d \\ d & c \end{pmatrix}$ → son iguales

SÍ ES HOMOMORFISMO DE ANILLOS.

- Para que sea biyectiva tiene que ser inyectiva

$\varphi(a+b\sqrt{2}) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \Leftrightarrow a = b = 0 \Rightarrow \ker \varphi = \{0\} \Rightarrow$ H es INYECTIVA

- SOBREYECTIVA: $\forall \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\} \in H, \; \exists (x+b\sqrt{2}) \in \mathbb{Z}[\sqrt{2}]$

y es tq $\varphi(a+b\sqrt{2}) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}$

SON ISOMORFOS

b) $(2\mathbb{Z}, +, \cdot)$ y $(3\mathbb{Z}, +, \cdot)$

NO ES UNITARIO

$\varphi : 2\mathbb{Z} \longrightarrow 3\mathbb{Z}$ homomorfismo de anillos

$\varphi(2) = 3a$

Se debería verificar: → $3a + 3a$

$\varphi(2+2) = \varphi(4) = \varphi(2) + \varphi(2) = 6a$

$\varphi(2 \cdot 2) = \varphi(4) = \varphi(2) \cdot \varphi(2) = 9a^2$ → $3a \cdot 3a$

$6a = 9a^2 \Leftrightarrow 6a - 9a^2 = 0$

$3a(2 - 3a) = 0 \Rightarrow \begin{cases} a = 0 \longrightarrow \text{este sí permite aplicación} \\ a = 2/3 \notin \mathbb{Z} \end{cases}$

$\varphi(2) = 0 \Rightarrow \varphi(2n) = 0 \; \forall n$ (hay homomorfismo)

NO SON ISOMORFOS

6. Dan homomorfismo de anillos $\Phi: \mathbb{Z} \to \mathbb{Z}_4$ x $\Phi(n) = [n]_4$, aplica dos cuadrados impares al mismo dom. Ninguno dan 11, 111, 1111, .. es cuadrado

$\Phi: \mathbb{Z} \to \mathbb{Z}_4$

$n \to \Phi(n) = [n]_4$

Sea $n \in \mathbb{Z} \Rightarrow n$ es un cuadrado impar $\Rightarrow n = (2k+1)^2 = 4k^2 + 4k + 1$,

$\varphi(n) = [4k^2 + 4k + 1]_4 = [1]_4$

Sea $n \in \mathbb{Z} \Rightarrow$ si es cuadrado par $\Rightarrow n = (2k)^2 = 4k^2$

$\varphi(n) = [4k^2]_4 = [0]_4$

Si queremos saber si 11, 111, 1111, ... no son cuadrados

$\varphi(11) = [11]_4 = [3]_4$

$\varphi(111) = [111]_4 = [100 + 11]_4 = [100]_4 + [11]_4 = [11]_4 = [3]_4$

$\varphi(1111) = [1111]_4 = [11 \cdot 100 + 11]_4 = [11]_4 = [3]_4$

$\vdots$

$\varphi(1..1) = [3]_4$

7. $\varphi: \mathbb{Z} \to \mathbb{Z}_5 \times \mathbb{Z}_{11}$ el homomorfismo de anillos $\Rightarrow \varphi(n) = ([n]_5, [n]_{11})$

a) Det ker(φ)

$\varphi: \mathbb{Z} \to \mathbb{Z}_5 \times \mathbb{Z}_{11}$, $\varphi(n) = ([n]_5, [n]_{11})$

$\varphi(n) = ([0]_5, [0]_{11}) \Leftrightarrow \begin{cases} n \equiv 0 \bmod 5 \\ n \equiv 0 \bmod 11 \end{cases}$ Como son primos entre sí $\Rightarrow (5 \text{ y } 11) \Rightarrow n = 5 \cdot 11 = 55 \cdot n$, $n \in \mathbb{Z}$

b) φ sobreyectiva?

$\forall a \in \mathbb{Z}_5, \forall b \in \mathbb{Z}_{11}, \exists n : \varphi(n) = (a, b)$

Dan que existe congruencia resolver el sistema)

$\begin{cases} n \equiv a \bmod 5 \\ a \equiv b \bmod 11 \end{cases}$ $n = 11a \cdot [11]_5^{-1} + 5b[5]_{11}^{-1} + 55k =$

$= 11a + 45b + 55k$

Lo $\varphi(11a + 45b + 55k) = (a, b)$

Si es sobreyectiva

→ calcular el inverso: $5b = 11k + 1$

$5(9) = 11 \cdot k + 1$ (9 es el inverso)

$45 = 11 \cdot 4 + 1$

$45 = 44 + 1$

c) $\varphi^{-1}([1]_5, [5]_{11}) \Rightarrow$ como b)

8. $R = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$ y $\varphi : R \to \mathbb{Z}$ tal que $\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \right) = a - b$

a) Ver que φ es homomorfismo de anillos

$\varphi : R \longrightarrow \mathbb{Z}$

$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \longrightarrow a - b$

SUMA $\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} + \begin{pmatrix} c & d \\ d & c \end{pmatrix} \right) = \varphi \begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix} = (a+c) - (b+d)$

$\varphi \begin{pmatrix} a & b \\ b & a \end{pmatrix} + \varphi \begin{pmatrix} c & d \\ d & c \end{pmatrix} = (a-b) + (c-d) = a + c - b - b$ // son iguales

PROD $\varphi\left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} c & d \\ d & c \end{pmatrix} \right) = \varphi \begin{pmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{pmatrix} = (ac+bd) - (ad+bc)$

$\varphi \begin{pmatrix} a & b \\ b & a \end{pmatrix} \varphi \begin{pmatrix} c & d \\ d & c \end{pmatrix} = (a-b)(c-d) = ac - bc - ad + bd$ ↗ son iguales

b) Det $\ker(\varphi)$

$\ker \varphi = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} : a \in \mathbb{Z} \right\}$

porque $a - a = 0$ (Imagen 0)

c) Ver que $R / \ker(\varphi)$ es isomorfismo a $\mathbb{Z}$

Por 1º th isomorfía

Si $\varphi : R \to S$ es homo. de anillos $\Rightarrow R / \ker \varphi \simeq \varphi(R)$

$\varphi : R \to \mathbb{Z}$ es homomorfismo $\Rightarrow R / \ker \varphi \simeq \varphi(R)$

¿$\varphi(R) = \mathbb{Z}$? (es suprayectiva?)

$\varphi \begin{pmatrix} a & b \\ b & a \end{pmatrix} = a - b \Rightarrow \forall n \in \mathbb{Z}$ Existe una imagen

sea n: $\varphi \begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} = n$, $\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \in R$

d) ¿Es $\ker(\varphi)$ un ideal maximal?

$R / \ker \varphi \simeq \mathbb{Z}$ que no es un cuerpo $\Rightarrow \ker \varphi$ no es ideal maximal