CLASES 3 y 4 (reescritura)

(A) PRODUCTO DE DOS ANILLOS

<u>Definición</u> Dados dos anillos A y A' se define el anillo $A\times A'$

como $A\times A' = \{(a,a') : a\in A \; a'\in A'\}$

Ej Con las operaciones $(a,a')\cdot(b,b') = (ab, a'b')$

$(a,a')+(b,b') = (a+b, a'+b')$

$0_{A\times A'} = (0_A, 0_{A'})$

$1_{A\times A'} = (1_A, 1_{A'})$

$A\times A'$ es un anillo

Propiedad (1) $\pi_1 : A\times A' \to A$ y $\pi_2 : A\times A' \to A$ dadas por

$\pi_1(a,a') = a \; ; \; \pi_2(a,a') = a'$ son morfismos de anillos

② Si (B, p_1, p_2) es otro anillo y morfismos de anillos tales que se colocan en ese diagrama

$$\begin{tikzcd}
B \arrow[r, "\alpha"] \arrow[rr, bend left, "p_2"] \arrow[dr, bend right, "p_1"'] & A \times A' \arrow[r, "\pi_2"] \arrow[d, "\pi_1"] & A' \\
 & A &
\end{tikzcd}$$

$\exists!\ \alpha$: los diagramas con una flecha ↻ conmutan

Eso quiere decir que $p_2 = \pi_2 \alpha$; $p_1 = \pi_1 \alpha$.

<u>Dem</u> ① Ejercicio ② Defino $\alpha(b) = (p_1(b), p_2(b))$

Es claramente morfismo y si hacemos $(\pi_1 \alpha)(b) = \pi_1(p_1(b), p_2(b))$

$= p_1(b)$.

Unicidad si tenemos $\beta : B \to A$: y que tiene la misma propiedad que α. o sea $\pi_2 \beta = p_2$ y $\pi_1 \beta = p$ se tiene que si $\beta(b) = (u(b), v(b))$

se tiene que $v(b) = p_2(b)$ y $u(b) = p_1(b)$ lo que implica que

$$\beta(b) = (p_1(b), p_2(b)) = \alpha(b) \qquad \boxtimes$$

(B) OPERACIONES CON IDEALES BILATERALES

① Ideal generado Si A es un anillo y $X \subset A$ un subconjunto se llama ideal generado por X y se denota como $\langle X \rangle$ al siguiente ideal $\langle X \rangle = \bigcap \{ I \subset A : I \text{ ideal } X \subset I \}$

Observación. Más abajo probaremos que la intersección de una familia arbitraria de ideales, es un ideal.

(2) Sean I y J ideales bilaterales de A

- $I.J = \{\sum i.j \;:\; i \in I \; j \in J\}$ es un ideal
- $I+J = \{i+j \;:\; i \in I \; j \in J\} \subset A$ es un ideal.

Dem $a(i+j) = ai + aj = i' + j'$ o sea que $A.(I+J) \subset I+J$

$(i+j) + (i'+j') = (i+i') + (j+j') \in I+J$

Luego $(I+J)$ es cerrado con respecto a la suma

Luego $I+J$ es un ideal.

IJ si tomamos como antes $\{i.j : i \in I \; j \in J\}$ no es un ideal luego tomamos $\left\{\sum_{s=1}^{n} i_s j_s : i_s \in I \; j_s \in J\right\}$

que es el ideal generado por el conjunto en rojo arriba.

- Si $\{I_t : t \in X\}$ X conjunto de índices

  $\bigcap \{I_t : t \in X\}$ es un ideal.

<u>Dem</u> Ejercicio

Una propiedad importante de los ideales

- Los conjuntos $\{0\}$ y A son ideales de A.

  $I \subset A$ ideal $\quad I = A \longleftrightarrow 1 \in I$. Si $1 \in I$ $\quad a \cdot 1 = a \in I \; \forall a$

TEOREMA CHINO DE LOS RESTOS.

<u>Prop.</u> Si $I \subset \mathbb{Z}$ es un ideal $\Rightarrow \exists\, m \in \mathbb{Z}$: $I = \langle m \rangle$

O sea todo ideal de $\mathbb{Z}$ es de la forma $\{ n \in \mathbb{Z} : m \mid n \}$

para algún m. ($a \mid b$ en $\mathbb{Z}$ si existe $c \in \mathbb{Z}$: $ca = b$)

<u>Dem</u> Sea I ideal y sea $m = \min\{ i > 0 : i \in \mathbb{Z} \}$

(el mínimo siempre existe)

Sea ahora un entero $z \in I$: $\underbrace{m < z}_{z > 0}$ $\Rightarrow$ divido y

tengo q y r: $z = qm + r$ con $r < m$ ó $r = 0$.

$r < m$ es absurdo pues m era el mínimo. Luego $r = 0$ y $m \mid z$

si $\underset{\substack{\cap \\ I}}{z} < 0$ tomo $-z > 0$ $\quad -z \in I \Rightarrow -z = mp \Rightarrow z = (-p)m$

En $\mathbb{N}$ existe mcd y el mcm.

$$\text{mcd}(a,b) = \max\{c : c \mid a \text{ y } c \mid b\}$$

$$\text{mcm}(a,b) = \min\{c : a \mid c \text{ y } b \mid c\}$$

En $\mathbb{Z}$ decimos que $m \mid n$ si $\exists$ entero r $\quad mr = n$

es claro que si $m \mid n \Rightarrow m \mid -n$ porque $mr = n \Rightarrow$

$m(-r) = n.$

Entonces en $\mathbb{Z}$ $\quad mcd(a,b) = \max\{c>0 : c|a \text{ y } c|b\}$

lo mismo para $\quad mcm(a,b) = \min\{c>0 : a|c \text{ y } b|c\}$

Si $u,v \in \mathbb{Z}$ y $u|v \Rightarrow u\,p = v \Rightarrow aup = av$

$\Rightarrow \langle v\rangle \subseteq \langle u\rangle$. Luego $c|a$ y $c|b \Rightarrow \langle a\rangle \subset \langle c\rangle, \langle b\rangle \subseteq \langle c\rangle$

Propiedad $\quad \langle mcd(a,b)\rangle = \langle a\rangle + \langle b\rangle$

$$\langle mcm(a,b)\rangle = \langle a\rangle \cap \langle b\rangle$$

Obs $\quad a$ y b son primos entre si si no tienen divisores en común y eso quiere decir que $mcd(a,b)=1 \Leftrightarrow \langle a\rangle + \langle b\rangle = \mathbb{Z}$

Teorema (chino de los restos)

Sean a y b dos enteros primos entre sí y sean u y v enteros cualesquiera $\Rightarrow$ existe x : $x \equiv u \pmod a$ y $x \equiv v \pmod b$

(eso quiere decir que $a \mid x-u$ y que $b \mid x-v$)

además si x' es otra solución $\Rightarrow ab \mid x-x'$.

O sea x es único modulo ab.

Expresión en términos de ideales. $\langle a\rangle + \langle b\rangle = \langle \operatorname{mcd}(a,b)\rangle$

Luego a y b enteros: $\langle a\rangle + \langle b\rangle = \mathbb{Z}$. Sea $I = \langle a\rangle$ y $J \langle b\rangle$

Sean $I, J \subseteq \mathbb{Z}$ ideales: $I + J = \mathbb{Z}$

Sean u y v cualesquiera $\exists\, x$: $x \equiv u \pmod a$

$x \equiv v \pmod b$

$[x]_I = [u]_I \qquad [x]_J = [v]_J$

Consideremos $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}/I \times \mathbb{Z}/J$

$x \rightsquigarrow ([x]_I, [x]_J)$

$\forall$ elemento en $\mathbb{Z}/I \times \mathbb{Z}/J \quad [u]_I, [v]_J$

Sea $\xi = ([u]_I, [v]_J) \in \mathbb{Z}/_I \times \mathbb{Z}/_J$ elemento genérico existe

$x \in \mathbb{Z}$: $\phi(x) = ([x]_I, [x]_J) = ([u]_I, [v]_J)$

i.e. $\exists\, x \in \mathbb{Z} : \phi(x) = \xi$. O sea ϕ es sobre.

Primera parte del tchr

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/_I \times \mathbb{Z}/_J \quad \text{es sobre si } I + J = \mathbb{Z}$$

Segunda parte del tchr otra solución x' es tal que $ab \mid x - x'$.

$[x]_{\langle ab\rangle} = [x']_{\langle ab\rangle}$. Si x y x' son tales que $\phi(x) = \phi(x')$

$\Rightarrow [x]_{\langle ab\rangle} = [x']_{\langle a,b\rangle}$

Sea $y = x - x'$. Sabemos que $\begin{cases} [x]_I = [x']_I \text{ o sea } y \in I \\ [x]_J = [x']_J \text{ o sea } y \in J \end{cases}$

y queremos probar que $[x]_{\langle ab\rangle} = [x']_{\langle ab\rangle}$ o sea $y \in \langle ab\rangle = IJ$

Queremos probar que si $I + J = \mathbb{Z} \Rightarrow IJ = I \cap J$

Es claro que $IJ \subset I$ $IJ \subset J$ $\Rightarrow$ $IJ \subseteq I \cap J$.

Now if $a \in I \cap J$ and write $1 = i + j$ $\quad a = ai + aj \in \underbrace{IJ + IJ}_{= IJ}$

Conclusión: usando ideales hemos formulado el tchr.

Teorema chino de los restos en general.

Sea A un anillo cualquiera I, J ideales biláteros : $I + J = A$. Entonces $A/_{I \cap J} \cong A/_{I} \times A/_{J}$

Dem. Sea $\phi : A \longrightarrow A/_I \times A/_J$ $\quad \phi(x) = ([x]_I, [x]_J)$

1. ϕ morfismo de grupos $\quad \phi(x)\phi(y) = ([x]_I, [x]_J)\cdot([y]_I, [y]_J)$

$= ([x]_I \cdot [y]_I, [x]_J \cdot [y]_J) = ([xy]_J, [xy]_J) = \phi(xy).$

2. Sobreyectivo. Si tenemos $([u]_I, [v]_J)$ buscamos

$x : [x]_I = [u]_I$ y $[x]_J = [v]_J$. Como $I + J = R$

$\exists\, i \in I, j \in J : i + j = 1$. Sea $x = uj + vi$,

$$[uj+vi]_I = [uj]_I = [uj+ui]_I = [u]_I$$

$$[uj+vi]_J = [vi]_J = [vi+vj]_J = [v]_J$$

$$\phi : A \longrightarrow A/I \times A/J \qquad \ker\phi = \{ a\in A : a \in I\cap J \} = I\cap J$$

<u>Teorema general</u> R un anillo y K un ideal bilátero

$\alpha : R \longrightarrow S$: $\ker\alpha = K \Rightarrow$

$$\begin{tikzcd} R \arrow[r, "\alpha"] \arrow[d] & S \\ R/K \arrow[ur, "\hat{\alpha}"'] & \end{tikzcd}$$

$\hat{\alpha}([r]_K) = \alpha(r)$ esa definición para que tenga sentido tiene que pasar que $[r]_K = [r']_K \Rightarrow \alpha(r) = \alpha(r')$

o sea si $r - r' \in K \Rightarrow \alpha(r - r') = 0$ se necesita que

$K \subset \operatorname{Ker} \alpha$

$\hat{\alpha}$ inyectiva $\quad \hat{\alpha}([r]_K) = 0$ i.e $\alpha(r) = 0 \quad \Rightarrow [r]_K = 0$

i.e $r \in K$. O sea $\operatorname{Ker} \alpha \subset K$ que también es cierto

$\boxtimes$