Álgebra Moderna II, Lunes 20 Feb 2017

Homomorfismos de anillos $f: R \longrightarrow R'$

= $\boxed{R \text{ conmutativo en adelante}}$ =

1) homomorfismo de grupo $(+,0)$

2) $f(1_R) = 1_{R'}$ & $f(ab) = f(a)f(b)$

$\text{Ker}(f) = \{a \in R \mid f(a) = 0_{R'}\}$

↳ propiedades:

1) subgrupo de R $(+,0)$

2) $a, b \in \text{Ker}(f) \Rightarrow a \cdot b \in \text{Ker}(f)$

$\Updownarrow$

$f(a)f(b) = 0 \cdot 0 = 0$

Ker tiene una propiedad más fuerte:

si $a \in \operatorname{Ker}(f)$ y $b \in R \Rightarrow$

$$a \cdot b \in \operatorname{Ker}(f)$$
$$\Updownarrow$$
$$f(a) \cdot f(b) = 0 \cdot f(b) = 0.$$

Un subconjunto $I \subseteq R$ que es un subgp $(+)$ & es cerrado bajo la multiplicación de cualquier elemento de R, le llamamos <u>Ideal</u>.

<u>EJEMPLOS:</u> – Cualquier kernel de un homomorfismo

– $I = \{0\} \subseteq R$ $\qquad \{0\} = \ker\begin{pmatrix} R \longrightarrow R \\ a \longmapsto a \end{pmatrix}$

– $R = \ker 0 : R \longrightarrow \{0\}$

— dado $a \in R \setminus \{0\}$,

$I = \{ra \mid r \in R\}$ Ideal principal generado por a

Propo.— Cualquier ideal $I \subseteq R$ es el kernel de algún homomorfismo $f: R \longrightarrow R'$

Demostración: Sea $I \subseteq R$ ideal

$\pi: R \longrightarrow R/I := \{a + I \mid a \in R\}$ ← !

$\ker \pi = I$. ∎

Hecho: Todos los ideales $I \subseteq \mathbb{Z}$ son de la forma $I = \langle n \rangle$ para $n \in \mathbb{Z}$. (principales)

Demostración ①: los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$; Todos.

Demostración (2): $I \subseteq \mathbb{Z}$ ideal, & $a \in I$ el entero más pequeño de I.

Algoritmo de la división implica que $b = ra$ para cualquier

EJER: $b \in I$ y algún $r \in R$.

Por lo tanto $I = \langle a \rangle \subseteq \mathbb{Z}$.

¿Existen ideales que no sean generados por un elemento en R?

↳ ¿existen ideales que no sean principales?

EJER: Explorar los ideales de $R = \mathbb{Z} + \mathbb{Z}[i]$

Unidades de R: $a \in R$ tal que tiene un inverso multiplicativo.

$$\left\{\begin{matrix}\text{Todas las}\\ \text{Unidades}\\ \text{de } R\end{matrix}\right\} := R^* \subseteq R$$

gp de Unidades

No es un gp $(+)$

¡Es un grupo $(\cdot)$!

EJER: R^* es un grupo bajo la multiplicación.

EJEMPLOS: $R =$ Campo $\quad R^* = R \setminus \{0\}$

$\mathbb{Z}^* = \{-1, 1\}$ $\quad (\mathbb{Z}/n\mathbb{Z})^* =$ grupo abeliano con $\varphi(n)$ elements

$M_{n\times n}(F)^* = GL_n(F)$

Pregunta difícil: Dado un anillo R, ¿cuál es su grupo de unidades?