Retomando ❗: Sea $I \subseteq R$ ideal

$\exists$ un homomorfismo de anillos

$f: R \longrightarrow R'$ cuyo kernel es I.

Tomemos $R' = \{r+I \mid r \in R\}$ clases laterales con $(+, 0)$.

$= R/I$

Afirmación: R/I es un anillo.

1) I es subgrupo de R. Entonces R/I grupo cociente (R conmut)

2) $(r+I)(r'+I) = r \cdot r' + \cancel{rI}^{I} + \cancel{r'I}^{I} + \cancel{I \cdot I}^{I}$

$= r \cdot r' + I \in R/I$.

Esta es la multiplicación en R/I

Por tanto, $f: R \longrightarrow R/I$ donde
$r \longmapsto r+I$

$\ker(f) = I \subseteq R$.

EJER: Verificar $f: R \longrightarrow R/I$, donde $I \subseteq R$ ideal, es un homomorfismo de anillos.

EJEMPLOS: - Si $I = \{0\}$ entonces $R/I = R$.

& $I = \ker\left(R \longrightarrow R/I = R\right)$
$a \longmapsto a$

- $I = R = \{\ker R \longrightarrow \{0\} = R/R\}$

¿ Puede un anillo tener sólo dos ideales $(\{0\}, R)$?

Propo - Si R tiene sólo un ideal, $R = \{0\}$.

R tiene dos ideales $\Longleftrightarrow$ R es campo.
$(0, R)$

↑
anillo donde todo $a \in R \setminus \{0\}$ tiene inverso multiplicativo.

Demostración: Primera parte EJER

Segunda parte, $\Leftarrow$) Asumamos R campo & $I \neq 0$ ideal. (Debemos mostrar que $I = R$)

$a \in I$ con $a \neq 0$.

entonces $\exists\ \bar{a}' = r$ en R.

Por tanto $1 = \bar{a}' \cdot a \in I$, Luego

$b \cdot 1 = b \in I$ para todo $b \in R$

$\Rightarrow$ $I = R$.

Ahora, $\Rightarrow$ Sea $a \in R$ $a \neq 0$ & $\langle a \rangle = I$ ideal principal.

Como R tiene solo 2 ideales $I = R$. Observar $1 \in R$ entonces

$\exists\ b \in I$ tal que $b \cdot a = 1$.

Por lo tanto Cualquier $a \neq 0$ en R tiene inverso. R campo.

$R = \mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\}$

$I = (0), (1), (2)$

$\| \quad$ Todos los ideales

$\{0,2\}$

$R = \mathbb{Z}/n\mathbb{Z}$ tiene un ideal (d) si $d \mid n$

$R = \mathbb{Z}/p^k\mathbb{Z}$ $\quad (1) \supsetneq (p) \supset (p^2) \supset \cdots \supset (p^k) = (0)$

Cadena descendiente de ideales

¡ # finito de ideales !

$\mathbb{Z} = R$ tiene una infinidad de ideales distintos.

$I_n = n\mathbb{Z} = (n)$ para cada $n \geq 0$

$$I_n \supseteq I_{n'} \iff n \text{ divide } n'$$

$R/I_n = \mathbb{Z}/n\mathbb{Z}$

Estos son todos los ideales de $\mathbb{Z}$.

Otro ejemplo donde conocemos todos los ideales es:

Sea F un campo. $R = F[x]$

$$= \{a_0 + \cdots + a_m x^m \mid a_i \in F\}$$

$p(x) \in R$ es mónico si $a_m = 1$.

Propos. Cualquier ideal $I \subseteq R = F[x]$ es principal. Es decir, $I = (f)$ donde f es el polinomio mónico de menor grado en I.

Por tanto

$$\{\text{ideales}\} \longleftrightarrow \{\text{polinomios mónicos}\}$$

$$I_f \supset I_g \iff f \text{ divide al polinomio } g$$

$$\text{i.e. } g(x) = f(x)q(x)$$

Demostración de la proposición: Análogo al algoritmo de la división en $\mathbb{Z}$: ↓

si f y g polinomios $\deg(f) \geq \deg(g)$

entonces, $f(x) = g(x)q(x) + r(x)$

$\deg(r) < \deg(g)$

Ejemplo: $x^3+2x^2+3x+7 = f(x)$

$x^2+x+1 = g(x)$

$f - xg = x^2+2x+7$

$\Rightarrow f - xg - g = x+6$

$\Rightarrow q(x) = x+1$

$r(x) = x+6$

¡Esto funciona en general!

EJER

Ahora, si $I \neq 0$, considerar $f \in I$ de grado mínimo.

Escalando f, podemos pensarlo mónico.

Sea $h(x) \in I$ distinto de f.

entonces, $h = g(x) f(x)$ & $r(x) \equiv 0$

$\Rightarrow h \in (f)$ debido al algoritmo de la división.

∎

$c \in F$. Considerar $F[x] \xrightarrow{ev} F$

$f(x) \longmapsto f(c)$

EJER: ev es un homomorfismo de anillos.

$\ker(ev) \leq F[x]$ ideal.

EJER: $\ker(ev) = (x-c)$

Corolario: si $f(c)=0$, entonces

$$f(x)=(x-c)\,g(x)$$

Corolario: si $f \in F[x]$ de grado n, entonces f tiene a lo más n raíces.

Ejemplo de un ideal que no es principal

$R = F[x,y]$ & F = Campo.

$$= \left\{ \sum_{\substack{i=1 \\ j=1}} a_{ij} x^i y^j \;\middle|\; a_{ij} \in F \right\} = \{ a_{0,0} + a_{1,0}x + a_{0,1}y + a_{1,1}xy + \dots \}$$

Considerar $h : R \longrightarrow F$ homomorfismo de anillos.

$f \longmapsto f(0,0)$

$I = \ker(h)$ no es generado por un elemento.

$$I = (x,y) = \{ rx + r'y \mid r, r' \in R \}$$

— Cualquier grupo G . . .

$$\{e\} \hookrightarrow G$$

— Cualquier anillo conmutativo .

$$\begin{array}{ccc} & i & \\ \mathbb{Z} & \longrightarrow & R \\ 0 & \longmapsto & 0 \\ 1 & \longmapsto & 1 \\ n = 1+\cdots+1 & \longmapsto & \underset{R}{1}+\cdots+\underset{R}{1} = n_R \end{array}$$

homomorfismo de anillos.

por tanto $\ker i = (n)$ para algún $n \in \mathbb{Z}$.

si R es un campo: $(*)$

$$n = \begin{cases} 0 \\ p \text{ - primo.} \end{cases}$$ Invariante de un campo.