

Teoría de Números : 29 agosto 2018

Clase pasada: Campos finitos

Hoy: Dado un anillo  $R$ , ¿podemos crear un campo a raíz de él?

$\left. \begin{array}{l} I \subseteq R \\ \text{ideal} \end{array} \right\} \hookrightarrow$  ¿Cuál es la relación entre los ideales de  $R$  y los de  $R/I$ ?

Bijección:

$\left. \begin{array}{l} \text{ideales } I \subseteq J \subseteq R \\ \text{de } R \text{ contenidos} \\ \text{a } I \end{array} \right\} \longrightarrow \left\{ \begin{array}{l} \text{ideales} \\ \bar{I} \subseteq \bar{R} = R/I \end{array} \right\}$

$J \longmapsto f(J) \subseteq \bar{R}$

$f^{-1}(\bar{J}) \longleftarrow \bar{J}$

Además,  $R/J \cong \bar{R}/\bar{J}$  isomorfismo de anillos <sup>k</sup>

\*  $f(J)$  es un ideal: si  $f(a), f(b) \in f(J)$   
con  $a, b \in J$ . Entonces

$$f(a) + f(b) = f(a+b) \in f(J)$$

\*  $f(a) \in f(J)$  &  $\bar{r} \in \bar{R}$

¿ es  $\bar{r}f(a) \in f(J)$

↳ observar  $f: R \rightarrow R/I$  es  
suprayectivo  $\Rightarrow$

$\exists c \in R$  tal que  $f(c) = \bar{r}$ .  $\Rightarrow$

$$\bar{r}f(a) = f(c \cdot a) \in f(J).$$

¡OJO! Si  $f: R \rightarrow R'$  no es suprayectivo,  
entonces  $f(J)$  no es necesario ideal.

EJER:  $\tilde{f}^{-1}(J)$  es un ideal de  $R$ . (8)

Por último,  $g \circ f = F$

$$R \xrightarrow{f} R/I = \bar{R} \xrightarrow{g} \bar{R}/\bar{J}$$

EJER: ¿Cuál es el  $\ker(F)$ ?

¿Es  $F$  suprayectivo?

↳ Concluir:  $R/I \cong \bar{R}/\bar{J}$

CONSECUENCIAS: ¿Cuándo es  $R/I$  un campo?



¿Cuándo  $\bar{R}$  tiene solo dos ideales?

( $\bar{R} \neq \{0\}$ )

Resp.  $\rightarrow$  Cuando existen solo dos ideales en  $R$   
conteniendo a  $I$ . ( $R \neq I$ )

(4)

Def. -  $I \subseteq R$  ideal se dice maximal  
si  $\nexists I \subset J$  ideal se tiene que  
 $J = R$ .

Pregunta: ¿Cuáles son los ideales maximales  
de  $\mathbb{Z}$ ,  $F[x]$ ,  $\mathbb{Z}[i]$ ?  
↑ campo

Propo. - 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 lo tanto:

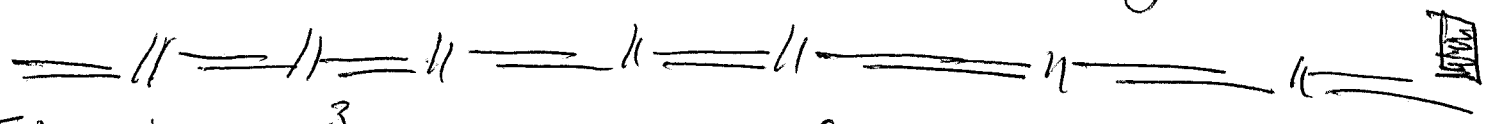
$\{\text{ideales}\} \longleftrightarrow \{\text{polinomios mónicos}\}$

$I_f \supset I_g \longleftrightarrow f \text{ divide a } g$   
i.e.  $g(x) = f(x)h(x)$

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

Si  $f(x)$  y  $g(x)$  polinomios  $\deg(f) \geq \deg(g)$

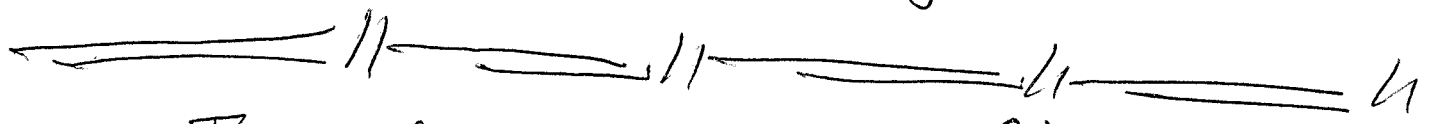
entonces,  $f(x) = g(x)q(x) + r(x)$   
↑  $\deg(r) < \deg(g)$



Ejemplo:  $x^3 + 2x^2 + 3x + 7 = f(x)$   
 $x^2 + x + 1 = g(x)$  }  $f - xg =$   
 $x^2 - 2x + 7$

$\Rightarrow q(x) = x + 1$   
 $r(x) = x + 6$   $\Rightarrow f - xg - q = x + 6$

¡ Este funciona en general !



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

$f(x) \mapsto f(c)$

¿ es  $ev$  homomorfismo de anillos ?

EJER:  $\text{Ker}(ev) = (x - c)$

(6)

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.

$C \in \mathbb{Z}$ ,

$$\begin{array}{c} \mathbb{Z}[x] \longrightarrow \mathbb{Z} \\ f(x) \longmapsto f(c) \end{array}$$

$$\ker(\epsilon_c) = ?$$

$$\mathbb{F}[x]$$