Teoría de Números : 29 agosto 2018

Clase pasada: Campos finitos

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

$I \subseteq R$ ideal } ↳ ¿Cuál es la relación entre los ideales de R y los de R/I?

↓

Biyección:

$$\left\{ \begin{array}{c} \text{ideales } I \subseteq J \subseteq R \\ \text{de } R \text{ conteniendo} \\ \text{a } I \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{ideales} \\ \overline{I} \subseteq \overline{R} = R/I \end{array} \right\}$$

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

$$\overline{f}^{-1}(\overline{J}) \longleftarrow\!\shortmid\ \overline{J}$$

Además, $R/J \cong \bar{R}/\bar{J}$ isomorfismo de anillos

* $f(J)$ 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 $f: R \longrightarrow R/I$ 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 $f: R \to R'$ no es suprayectivo, entonces $f(J)$ no es necesar ideal.

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

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: ¿Cuando es R/I un campo?

↕

¿Cuándo $\bar{R}$ tiene solo dos ideales? ($\bar{R}$ & 103)

Resp. ↳ Cuando existen solo dos ideales en R conteniendo a I. (R & I)

Def. – $I \subseteq R$ ideal se dice maximal si $\forall\, I \subsetneq J$ ideal se tiene que $J = R$.

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

F ← 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:

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

$$I_f \supseteq I_g \longleftrightarrow f \text{ divide a } g$$

ie. $g(x) = f(x)\,h(x)$

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

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

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

↑ $\deg(r) < \deg(g)$

Ejemplo: $\left.\begin{array}{l} x^3+2x^2+3x+7 = f(x) \\ x^2+x+1 = g(x) \end{array}\right\}$ $f - xg =$

$x^2 - 2x + 7$

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

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

$r(x) = x+6$ ¡ Esto funciona en general !

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

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

¿ es ev homomorfismo de anillos?

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.

$c \in \mathbb{Z}$,

$\mathbb{Z}[x] \longrightarrow \mathbb{Z}$

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

$\ker(ev) = ?$

EJER