Teoría de Números: 27 agosto

clase pasada: ideales

Hoy: ideales & Campos

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

Propo Si $R$ tiene un solo ideal, $R=\{0\}$

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

Demostración:

- Primera parte EJER

- Segunda parte: $\Leftarrow$) Asumamos
$R$ campo & $I \neq 0$ ideal.

entonces, $a \in I$ $\bar{a}' \in R$ &
$a \cdot \bar{a}' = 1_R \in I$.

$\Uparrow$

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

Luego, $\underline{I = R}$.

Ahora, $\Rightarrow$) Sea $a \in R$ $a \neq 0$ & $\langle a \rangle = I$ ideal principal. Como $R$ tiene solo 2 ideales, $\Rightarrow$ $\underline{I = R}$

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

Por lo tanto cada $a \neq 0$ en $R$ tiene inverso. $\underline{R \text{ campo}}$ ∎

---

$R = \mathbb{Z}$, $I_n = \langle n \rangle$ ideales

$I_{n'} = \langle n' \rangle$ observar

$I_n \supset I_{n'} \iff n'$ divide $n$

$\Rightarrow \mathbb{Z}/n\mathbb{Z}$ tiene un ideal $\langle d \rangle$ si $d \mid n$.

- Cualquier grupo $G$

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

- Cualquier anillo conmutativo

$$\begin{aligned} \mathbb{Z} &\longrightarrow R \\ 0 &\longmapsto 0 \\ 1 &\longmapsto 1_R \end{aligned}$$

homomorfismo de anillos

$$n = 1+\cdots+1 \longmapsto 1_R+\cdots+1_R = n$$

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

AFIRMACIÓN:
Si $R$ es un campo, $\Rightarrow$

$$n = \begin{cases} 0 \\ p \text{ primo} \end{cases} \quad \Leftrightarrow \text{ invariante de un campo.}$$

Def Sea $n = \ker(i)$ con $i: \mathbb{Z} \longrightarrow R = \text{campo}$
$1 \longmapsto 1$
le llamamos característica de $R$

Demostración: Supongamos $\ker(i) = (n)$

y $n = a \cdot b$ $\quad a, b > 0$

$b > 1, \; a > 1$

entonces $i(a \cdot b) = 0$ en $R$.

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

$\Rightarrow \quad i(a) = 0 \quad$ ó $\quad i(b) = 0$

$\Rightarrow \; i(a) = 0 \;$ & $\; a \in \ker(i)$

Contradicción.

□

Teorema: (Galois) Sea $F$ un campo finito

entonces $|F| = p^k$ para algún primo $p$.

Demostración: $f: \mathbb{Z} \longrightarrow F$

homomorfismo de anillos

$1 \longmapsto 1_F$

$n \longmapsto 1 + + \cdots 1 = n$

Como $\mathbb{Z}$ es infinito $\Rightarrow \ker(f) \neq 0$.

Más aún, $\ker(f) = p\mathbb{Z}$ y $f$ induce

$$\bar{f} : \mathbb{Z}/p\mathbb{Z} \longrightarrow F$$

(1er teorema de isomorfismo en grupos)

Por tanto $F$ es un espacio vectorial sobre $\mathbb{Z}/p\mathbb{Z}$, Como $F$ es finito su dimensión sobre $\mathbb{Z}/p\mathbb{Z}$ es finita, entonces

$$|F| = p^k \quad \text{para algún primo } p \in \mathbb{Z}.$$

∎

<u>Coro:</u> $F \cong (\mathbb{Z}/p\mathbb{Z})^k$ como espacio vectorial.

donde $F$ es cualquier campo finito.

Pregunta: Para cada $k$, ¿existe un campo $F$ de cardinalidad $p^k$? con $p \in \mathbb{Z}$ primo

EJER: Exhibir un campo de 4, 9 & 49 elementos.