Álgebra Moderna II, Lunes 27 Feb

Última clase: R anillo conmutativo

$f: \mathbb{Z} \longrightarrow R$ homomorfismo de anillos

$1+\cdots+1 = n1 \longrightarrow 1_R+\cdots+1_R$

$f(-n) = -f(n)$

$\ker(f) = (n)$ para algún $n \geq 0$

$(n) \leq \mathbb{Z}$ ideal

si $R = \{0\}$, entonces $\ker(f) = \mathbb{Z}$

si $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, entonces $\ker(f) = (0)$

Prop. si R es un campo, entonces

$$\ker(f) = \begin{cases} 0 \\ p\mathbb{Z} \quad p \text{ primo} \end{cases}$$

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

y $n = a \cdot b$ $a, b > 0$ más aún,

$a > 1$ $b > 1$.

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

$\|$

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

entonces $f(a)$ ó $f(b)$ es cero

$\Rightarrow$ $f(a) = 0$ ó $f(b) = 0$

$\Rightarrow$ $a \in \ker(f)$ contradicción.

Def: $\ker(f)$ es llamada la característica del campo.

TEOREMA (GALOIS) Sea F un campo finito entonces $|F| = p^t$ para algún primo p.

Demostración: Consideramos

$$f : \mathbb{Z} \longrightarrow F \qquad \text{homomorfismo de anillos}$$
$$1 \longmapsto 1_F$$
$$n \longmapsto \underbrace{1_F + \cdots + 1_F}_{n}$$

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

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

$$\overline{f} : \mathbb{Z}/p\mathbb{Z} \longrightarrow F \qquad \left(\begin{array}{c}1^{er} \text{ teorema de} \\ \text{isomorfismo} \\ \text{en grupos}\end{array}\right)$$

Portanto F es un espacio vectorial sobre $\mathbb{Z}/p\mathbb{Z}$, y

Como F es finito, su dimensión sobre $\mathbb{Z}/p\mathbb{Z}$ es finita. Por lo tanto

$$|F| = p^f \text{ para algún primo } p.$$

$\blacksquare$

COROLARIO: $F \cong (\mathbb{Z}/p\mathbb{Z})^f$ como espacio vectorial

donde F es cualquier campo finito.

Pregunta (más adelante en el curso)

para cada f, ¿existe un campo F de cardinalidad p^f? con p primo

EJER: Exhibir un campo de cardinalidad 4.

EJER: Exhibir un campo de ~~8~~ 9 elementos. 49 elementos.

EJER:

---

cociente de anillos: $I \subseteq R$ ideal.

$\pi: R \longrightarrow R/I = \overline{R}$ homomorfismo suprayectivo.

¿Existe una relación entre los ideales de R y los de $\overline{R}$?

Biyección:

$$\left\{\begin{array}{l}\text{ideales } I \subseteq J \subseteq R \\ \text{de } R \text{ conteniendo } I\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Ideales} \\ \overline{I} \subseteq \overline{R}\end{array}\right\}$$

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

$$\overline{f}^{-1}(\overline{J}) \longmapsto \overline{J}$$

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

$f(J)$ es un ideal: Si

$f(a), f(b) \in f(J)$ $\quad a, b \in J$. Entonces

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

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

¿es $\bar{r} \cdot f(a) \in f(J)$?

↳ Observar $f: R \longrightarrow R/I = \bar{R}$ es

suprayectivo

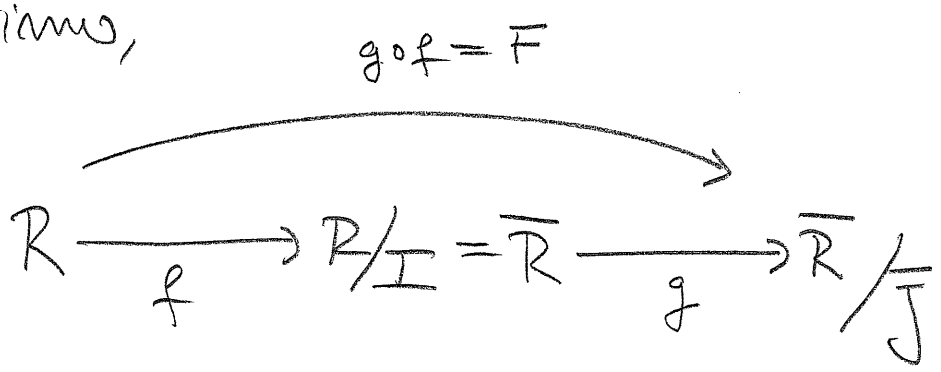
entonces $\bar{r} = f(c)$ para algún $c \in R$.

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

PRECAUCIÓN: si $g: R \longrightarrow R'$ no es suprayectivo, entonces $g(R)$ no es necesariamente un ideal.

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

Por último,



EJER:

¿ Cuál es el $\ker(F)$?

¿ Es F suprayectivo ?

Conclusión: $R/J \cong \bar{R}/\bar{J}$.

CONSECUENCIAS: ¿ Cuándo es $R/I = \bar{R}$ un campo ?

↕

Cuando $\bar{R}$ tiene solo dos ideales: $(\bar{R} \neq \{0\})$

↕

Cuando solo existen dos ideales conteniendo I en R. (R, I)

$\updownarrow$

$I \subseteq R$ es un ideal maximal de R.

EJER: ¿Cuales son los ideales maximales de $\mathbb{Z}$ & $F[x]$?

↑ campo.

CREAR RELACIONES EN UN ANILLO R.

$a \in R$

Si deseamos un anillo $\overline{R}$ que sea la imagen de R y donde $\bar{a} = 0$, entonces hacemos $\overline{R} = R/(a)$

Más aún, si deseamos un anillo donde $\bar{a}_1 = \dots = \bar{a}_k = 0$