Álgebra Moderna II: 15 mayo

Clase pasada: Unidades de $R_D = \mathbb{Z} + \mathbb{Z}\left(\frac{D+\sqrt{D}}{2}\right)$

Hoy: Repaso de definiciones y clarificación del material visto al momento.

Elemento primo p: p no es unidad &

$p \mid ab \Rightarrow p \mid a$ ó $p \mid b$.

Elemento irreducible r: r no es unidad &

$r = ab \Rightarrow$ a es unidad ó b es unidad.

Prop.- R un dominio entero.

$$p \neq 0 \text{ primo} \Rightarrow p \text{ irreducible}$$

Demostración: supongamos $p = ab$

$$\Rightarrow p \mid ab \Rightarrow p \mid a \text{ ó } p \mid b$$

si $p \mid a \Rightarrow c \cdot p = a$

$$\Rightarrow p = ab = c \cdot p \cdot b$$

$$\Rightarrow p(1 - cb) = 0$$

$\Rightarrow$ c es unidad y b es unidad

$\Rightarrow$ p irreducible. $\square$

¡El recíproco es falso!

Ejemplo: en $R = \mathbb{Z}[\sqrt{d}]$ con

d libre de cuadrados

y $d < -1$ $d \equiv 3 \pmod 4$

$$2\left(\frac{1-d}{2}\right) = (1-\sqrt{d})(1+\sqrt{d})$$

- 2 es irreducible
- 2 no es primo. (pues $2 \mid (1-\sqrt{d})(1+\sqrt{d})$

  pero $2 \nmid (1 \pm \sqrt{d})$.

Clase 14: Con este argumento concluimos que

R_D no es DFU $\left(\begin{matrix} d \equiv 3 \pmod 4 \\ \& \\ d < -1 \end{matrix}\right)$

$$\boxed{ab=0 \Rightarrow a=0 \text{ ó } b=0} \qquad \boxed{I=(a)}$$

$$\left\{\begin{matrix}\text{Todos los}\\ \text{anillos}\end{matrix}\right\} \supseteq \{\text{Dominios}\} \supseteq \{\text{DFU}\} \supseteq \{\text{DIP}\}$$

$$\cup\!\!\mid$$

$$\left\{\begin{matrix}\text{Dominios}\\ \text{Euclidianos}\\ \text{(DE)}\end{matrix}\right\}$$

$$\cup\!\!\mid$$

$$\{\text{Campos}\}$$

DE: existe una norma δ

$\forall\, a, b\neq 0$

$\exists\, q, r$ tal que

$a=bq+r$

$r=0$ ó $\delta(r)<\delta(b)$

<u>EJEMPLOS</u>:

$\mathbb{Z}\times\mathbb{Z}$

$\mathbb{Z}[\sqrt{d}]$

$d<-1$

$d\equiv 3 \pmod 4$

$\mathbb{Z}[x]$

$(x,2)$

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$

$\mathbb{Z}$

$\mathbb{R}$

Deuda:

Proposición: si R es DFU y $r \in R$ $(\neq 0)$ entonces, r es primo ssi r es irreducible.

Demostración: EJER

Ideales maximales & primos

Recordar: $M \leq R$ es un ideal maximal ssi $M \leq I \leq R \Rightarrow$
$I = M$ ó $I = R$

recordar M ideal maximal $\Longleftrightarrow$ R/M campo

Def.- $P \subsetneq R$ le llamamos ideal **primo** si $a \cdot b \in P$

$\Longrightarrow$ $a \in P$ ó $b \in P$.

Proposición: $p \in R$ es un elemento primo **ssi** (p) es un ideal primo.

Demostración: **EJER.**

Pregunta: si $I \subseteq R$ es un ideal primo ¿ $I = (p)$ para algún $p \in R$ primo ?