## 3.2. Ideales máximos

**3.2.1 Def.** Sea $R$ un anillo. Un ideal $I < R$ se llama <u>máximo</u> si $I \neq R$ y si no existe ningún ideal $J$ con $I \subsetneq J \subsetneq R$

**3.2.2 Prop.** Sea $R$ un anillo conmutativo con 1. Entonces un ideal $I < R$ es máximo $\Longleftrightarrow$ $R/I$ es un campo.

**Dem.** Consideremos la proyección canónica $\pi : R \longrightarrow R/I$

Obviamente, $R/I$ es un anillo conmutativo con $1_{R/I} = 1_R + I$.
Por la correspondencia de ideales entre $R$ y $R/I$ (1.2.8.)
$I$ es máximo, si y solamente si $R/I$ solamente tiene los ideales triviales $\overline{0} = I$ y $R/I$.
$\Longleftrightarrow$ $R/I$ es un campo. $\square$

<u>3.2.3 Cor.</u> Si $R$ es un anillo conmutativo con 1, entonces

cada ideal $I < R$ máximo es un ideal primo.

<u>Dem.</u> Cada campo es un dominio entero.

## 3.2.4. Ejemplos

(1) Si $K$ es un campo, $\{0\}$ es el único ideal maximo

(2) $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$

$\Rightarrow (x^2+1) \subset \mathbb{R}[x]$ es máximo

De hecho tenemos un hom. de

anillos $\mathbb{R}[x] \xrightarrow{\varphi} \mathbb{C}$ ($i \in \mathbb{C}$ con $i^2 = -1$)

$f \longmapsto f(i)$

$$\begin{tikzcd}
\mathbb{R} \arrow[rr, hook] \arrow[dr, hook] & & \mathbb{C} \\
& \mathbb{R}[x] \arrow[ur] &
\end{tikzcd}$$

solo tenemos que ver que $\varphi$ sea suprayectivo (claro)

$\Rightarrow$ $\operatorname{Ker}(\varphi) = (x^2+1)$

"$\supseteq$" claro porque $\varphi(x^2+1) = -1+1 = 0$

"$\subseteq$" Sea $f \in \operatorname{Ker}(\varphi) \setminus \{0\}$

entonces tenemos la div.

un residuo en $\mathbb{R}[x]$

$$f = q\,(x^2+1) + r \quad \text{con}$$

$$\deg(r) < 2 = \deg(x^2+1).$$

Ahora $\varphi(r) = a + bi$

$$\begin{array}{c} \| \\ (r = a + bx) \end{array}$$

$\Rightarrow$ vemos

$$0 = \varphi(f) = f(i) = \overbrace{q(i)\,\cancelto{0}{(i^2+1)}}^{=0} + a + bi$$

$$\Rightarrow f = q\,(x^2+1) + 0$$

$$\Rightarrow f \in (x^2+1).$$

(3) En el anillo $\mathbb{Z}$, precisamente los ideales primos $I$ con $I \neq 0$ son máximos:

Si $0 \neq I \subset \mathbb{Z}$ es primo, entonces $I = p\mathbb{Z}$ para algún primo $p \in \mathbb{Z}_{\geq 2}$ $\Rightarrow$ $\mathbb{Z}/p\mathbb{Z}$ es un campo (dominio entero finito)

· El ideal $(0)$ es primo, pero no es máximo ya que ~~es~~ tenemos por ejemplo

$$(0) \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$$

(4) En $\mathbb{Z}$ cada ideal $I$ es de la forma $m\mathbb{Z}$ para algún $m \in \mathbb{Z}$.

Si un primo $p \mid m \Rightarrow$

$m\mathbb{Z} \subset p\mathbb{Z} \subset \mathbb{Z}$

$\therefore$ $I$ está contenido en un ideal máximo.

**3.2.5. Prop.** Sea $R$ un anillo conmutativo con $1 \neq 0$, entonces cada ideal $I \subset R$ está contenido en un ideal máximo.

Dem: Usamos el Lema de Zorn.
Cada conjunto parcialmente ordenado y inductivo tiene un elemento máximo
Aquí: $\mathcal{G} := \{ I' \subset R \text{ ideal} \mid I \subset I' \subsetneq R \}$ $\square$

# 4. Divisibilidad en dominios enteros

## 4.1. El campo de fracciones de un dominio entero

**4.1.1. Def.** Sea $R$ un dominio entero. Una pareja $(F, \iota)$ consistente de un campo $F$ y de un hom. injectivo de anillos (unitario) $\iota : R \longrightarrow F$ se llama __campo de fracciones__ de $R$ si cumple la siguiente propiedad universal:

$\forall$ homomorfismo injectivo de anillos

$$\begin{tikzcd} R \arrow[rr, hook, "\phi"] \arrow[dr, hook] & & K \\ & F \arrow[ur, dashed, "\psi"'] & \end{tikzcd}$$

con $K$ un campo

existe un único hom. de anillos (campos) $\psi$ que hace conmutar el diagrama.

<u>Obs.</u> El campo de fracciones es único, si existe.

<u>4.1.2. Prop.</u> Sea $R$ un dominio entero. Entonces consideramos

(1) $R \times (R \setminus \{0\})$ con la rel.

$(a,b) \sim (c,d) \Leftrightarrow ad = bc$

es una relación de equivalencia.

(2) Si denotamos con $\frac{a}{b}$ la clase de equivalencia de $(a,b) \in R \times (R \setminus \{0\})$

y con $\mathrm{Frac}(R)$ el conjunto de clases de equiv., entonces

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$$ y

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$$

son relaciones binarias bien definidas sobre $\mathrm{Frac}(R)$

(3) $(\mathrm{Frac}(R), +, \cdot)$ es un campo con $1_{\mathrm{Frac}(R)} = 1/1$ y

$0_{\mathrm{Frac}(R)} = 0/1$

(4) $c : R \longrightarrow \mathrm{Frac}(R)$

$r \longmapsto r/1$

es un hom. inyectivo de anillos y

$(\mathrm{Frac}(R), c)$ es "el" campo de fracciones de $R$.

Dem. (Ejercicio)

## 4.1.4. Ejemplos

(1) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$

(2) Si $K$ es un campo, entonces $\mathrm{Frac}(K[X]) =: K(X)$ es el campo de funciones racionales en una indeterminada $X$

## 4.2 Elementos primos y Elementos irreducibles

**4.2.1. Def.** Sea $R$ un dominio entero, $a, b \in R$.

$b \mid a \;:\Leftrightarrow\; a \in Rb$ ($b$ es un divisor de $a$)

**4.2.2. Obs.** Sea $R$ un dominio entero entonces

1) $1 \mid a \quad a \in R$

(2) $c \mid b$ , $b \mid a \Rightarrow c \mid a$

(3) $b \mid a_1$, $b \mid a_2, \ldots, b \mid a_n$ entonces

$b \mid (x_1 a_1 + x_2 a_2 + \ldots + x_n a_n)$

para todo $x_1, x_2, \ldots, x_n \in R$

(4) $b \mid 1 \Longleftrightarrow b \in R^*$ (unidad)

(5) $b \mid a \Longleftrightarrow bu \mid a \quad \forall u \in R^*$

(6) $(a) \subset (b) \Longleftrightarrow b \mid a$

(ejemplo en $\mathbb{Z}$ : $(6) \subset (2)$

porque $2 \mid 6$

( Ejercicio )

**4.3.4 Def.** Sea $R$ un dominio entero. Dos elementos $a, b \in R$ son <u>asociados</u> si existe una unidad $u \in R^*$ con $a = b \cdot u$

en este contexto se escribe

$a \sim b \iff a$ y $b$ son asociados

**4.2.4 Obs.** Sea $R$ un dominio entero entonces sigue de las definiciones

$a \sim b \iff (a) = (b) \iff a|b, b|a$

En part. $\sim$ es una rel. de equiv.

**4.2.5. Def.** Sea $R$ un dominio entero, entonces

(a) $p \in R$ es un **elemento primo** si vale

(i) $p \notin R^* \cup \{0\}$.

(ii) Si $a, b \in R$ con $p \mid a \cdot b$ $\Rightarrow$ $p \mid a$ ó $p \mid b$.

[ $(p)$ es un ideal primo ]

(b) $q \in R$ es un **elemento irreducible** si

(i) $q \notin R^* \cup \{0\}$

(ii) Si existen $a, b \in R$ con
$$q = a \cdot b \Longrightarrow a \in R^* \text{ o } b \in R^*$$

## 4.2. Ejemplos

1) Si $K$ es un campo entonces
$K = K^* \cup \{0\} \Rightarrow$ no hay
ni primos ni irreducibles.

2) En $\mathbb{Z}$ tenemos
$$a \sim b \Longleftrightarrow b \in \{-a, +a\}$$
$n \in \mathbb{Z}_{\geq 1}$ es primo $\Leftrightarrow$ irred.

(3) Si $K$ es un campo $a \in K^*$

$b \in K$ entonces

$aX + b \sim X + b/a$ es

irreducible:

$aX + b$ es de grado 1 $>$

$\Rightarrow aX + b = f \cdot g$ implica

$\deg(f) = 0$ o $\deg(g) = 0$

$\Rightarrow f \in (K[x])^*$ o $g \in (K[x])^*$,

(ojo! dependiendo de $K$,
puede haber pol. irred. en $K[x]$
con grado $\geq 2$ o no)