2.2.4. Def Sea R un dominio entero.
(i.e. R es conmutativo con 1, sin divisores de cero) Entonces, R se llama un **anillo euclídeo** si R admite una función $d: R\setminus\{0\} \longrightarrow \mathbb{N}_0$ t.q.

$\forall a, b \in R\setminus\{0\}$ existen $q, r \in R$ con

- $a = qb + r$ y $r = 0$ ó $d(r) < d(b)$

2.2.5. Ejemplos

(1) $R = \mathbb{Z}$, $d(z) := |z|$ (valor absoluto)

$\rightsquigarrow$ $r < q$ no son únicos, por ejemplo

$a = 5$, $b = 2$

$$5 = \underbrace{2\cdot 2 + 1}_{q \quad r} = \underbrace{3\cdot 2 - 1}_{q' \quad r'}$$

(2) Sea K un campo,
$R := K[X]$ anillo de polinomios
$d : K[X] \setminus \{0\} \longrightarrow \mathbb{N}_0$, $f \mapsto \deg(f)$
d tiene la propiedad deseada por la última parte de Prp. 2.2.3.

(3) $R := \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$
el anillo de los enteros gaussianos.
$d : \mathbb{Z}[i] \longrightarrow \mathbb{N}_0$, $a + bi \mapsto a^2 + b^2$

le da a $\mathbb{Z}[i]$ la estructura de un anillo euclidiano

Dem. Podemos extender naturalmente d a
$d' : \mathbb{C} \longrightarrow \mathbb{R}_{\geq 0}$
$\Rightarrow d'(z \cdot w) = d'(z)\, d'(w)$ ya que $d'(z) = |z|^2$

Si tenemos $a, b \in \mathbb{Z}[i] \setminus \{0\}$, entonces

$\frac{a}{b} = p + qi$ para ciertos $p, q \in \mathbb{Q}$.

↑ división en $\mathbb{C}$

escojemos $m, n \in \mathbb{Z}$ t.q. $|p - m| \leq \frac{1}{2}$ y $|q - n| \leq \frac{1}{2}$

$\Rightarrow d'\left(\frac{a}{b} - (m + in)\right) = |p - m|^2 + |q - n|^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

y por eso

$$d\Big(\underbrace{a - \overbrace{(m + in)}^{q} b}_{r}\Big) = d'\left(\frac{a}{b} - (m + in)\right) d(b)$$

$$\leq \frac{1}{2} d(b) < d(b)$$

□

2.3. Ceros de Polinomios

2.2.1. Def. Sean $R \subset S$ anillos conmutativos con $1_S = 1_R$. Un tuplo $(r_1, \dots, r_n) \in S^n$ se llama **cero** de

$$f = \sum_{(i_1,\dots,i_n) \in I \subset \mathbb{N}_0^n} a_{i_1 i_2 \dots i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n} \in R[X_1, \dots, X_n]$$

(I finito)

si $f(r_1, \dots, r_n) := \sum_{(i_1,\dots,i_n) \in I} a_{i_1 \dots i_n} r_1^{i_1} r_2^{i_2} \dots r_n^{i_n} = 0 \in S$

2.3.2 Lema Sea R un anillo conmutativo con 1 y $f \in R[X]$. Si $r \in R$ es un cero de f, entonces existe $g \in R[X]$ con

$f = (x-\alpha)\,q$.

Dem. Si $f=0$, trivialmente podemos poner $q=0$ y $f = 0 = (x-\alpha)\cdot 0$ ✓

Si $f \neq 0$ existen por 2.3.3 (alg. div. con residuo) $q, r \in R[x]$ con

$1 \cdot f = q\,(x-\alpha) + r$

(coef. princ. $= 1$)

y $\deg(r) < \deg(x-\alpha) = 1$

$\Rightarrow r \in R$

$\Rightarrow 0 = f(\alpha) = q(\alpha-\alpha) + r$

$\Rightarrow r = 0 \Rightarrow f = q(x-\alpha)$ ✓

Obs. Usamos la siguiente observación sencilla: Para todo $r \in R$ tenemos un homomorfismo de anillos

$$ev_r : R[X] \longrightarrow R$$
$$f \longmapsto f(r)$$

que se llama homomorfismo de evaluación.

Tenemos por el Lema

$$\ker(ev_r) = R(X - r)$$

2.3.3. Prop. Sea R un dominio entero. Entonces cada $f \in R[X] \setminus \{0\}$ tiene a lo más $\deg(f)$ ceros diferentes.

Dem. Inducción / $\deg(f)$

$\deg(f) = 0 \Rightarrow f = r \in \mathbb{R} \setminus \{0\}$ no tiene ceros.

$\deg(f) = n+1$ Suponemos que cada polinomio g con $\deg(g) \leq n$ tiene a lo más $\deg(g)$ ceros.

Si $f \in \mathbb{R}[X]$ con $\deg(f) = n+1$ tiene un cero $a \in \mathbb{R}$, entonces por el Lema 2.3.2

$f = (X-a)\,g$

con $g \in \mathbb{R}[X]$ y $\deg(g) = n$ ($1_{\mathbb{R}}$ no es div. de cero)

Si $z \in \mathbb{R}$ es un cero de f, entonces

$0 = f(z) = (z-a)\,g(z) \in \mathbb{R}$

$\Rightarrow$ z es cero de $X-a$ ó z es cero de g.

($\mathbb{R}$ dom. de int.)

↑ única cero es a

↑ a lo más n ceros

□

2.3.4. Ejemplos

(1) Sea K un campo, $a_1, \dots a_n \in K$ con $a_i \neq a_j$ si $i \neq j$ y $b_1, \dots, b_n \in K$ arbitrarios, entonces

$$f := \sum_{i=1}^{n} b_i \frac{(X-a_1)\dots(\widehat{X-a_i})\dots(X-a_n)}{(a_i-a_1)\dots(\widehat{a_i-a_i})\dots(a_i-a_n)}$$

(en cada sumando omitimos el factor marcado con $\widehat{*}$)

es el único polinomio $h \in K[X]$ con $\deg(h) \leq n-1$ y $h(a_i) = b_i$ para $i = 1, 2, \dots, n$. (Ejercicio)

2) $f = X^2 + 1 \in \mathbb{R}[X]$ no tiene ceros en $\mathbb{R}$ pero $\pm i \in \mathbb{C}$ son ceros de f!

3) Polinomios en por lo menos dos indet. pueden tener una infinidad de ceros. Por ejemplo $f = X - Y \in \mathbb{R}[X,Y]$ tiene todo

$(r, r) \in \mathbb{R}^2$ ($\text{con } r \in \mathbb{R}$) como cero.

4) Si R tiene divisores de 0, 2.4.3 no es válido en general:

Sean $a, b \in R \setminus \{0\}$ con $a \cdot b = 0$, entonces $f = aX$ tiene grado 1 pero tiene por lo menos 2 ceros diferentes de 0!

2.3.5 Obs. Si R es un anillo finito, digamos $R = \{a_1, a_2, \dots, a_n\}$ entonces

$f := \prod_{i=1}^{n} (X - a_i) \in R[X] \setminus \{0\}$ pero

$f(a) = 0 \quad \forall a \in R$ Por eso, en general no se pueden identificar funciones polinomiales $R \to R$ con $R[X]$. Si R es un dominio entero infinito, no ocurre este problema!

§ 3. Ideales primos & ideales máximos

3.1. Ideales primos

3.1.1. Def. Sea R un anillo. Un ideal $I \subset R$ es *primo* si $I \neq 0$ y para $r, s \in R$ se tiene $r \cdot s \in I \Rightarrow r \in I$ ó $s \in I$.

3.1.2. Obs Un ideal $I \subsetneq R$ es primo sii $R \setminus I$ es cerrado bajo mult. i.e.

$$r, s \in R \setminus I \Rightarrow r \cdot s \in R \setminus I$$

3.1.3. Ejemplos

(0) Si R es un dominio entero, entonces $(0) = \{0\} \subset R$ es un ideal primo

(1) Si R es un dominio entero, entonces $(X) \subset R[X]$ es primo, pero $(X^2) \neq (X)$ no lo es.

($f \in (X) \iff f(0) = 0 \Rightarrow$ para $f, g \in R[X] \setminus (X)$ tenemos $f \cdot g \in R[X] \setminus (X)$!
$X \notin (X^2)$ pero $X^2 \in (X^2)$.)

(2) Si $m \in \mathbb{Z}_{\geq 1}$, entonces $m\mathbb{Z} \subset \mathbb{Z}$ es un ideal primo $\iff$ m es un número primo.

"$\Leftarrow$" Sean $k, l \in \mathbb{Z}$ con $k \cdot l \in m\mathbb{Z} \iff m \mid k \cdot l$
$\overset{m \text{ primo}}{\Longrightarrow}$ $m \mid l$ ó $m \mid k \iff k \in m\mathbb{Z}$ ó $l \in m\mathbb{Z}$.

"$\Rightarrow$" Si m no es primo, entonces existen $k, l \in \mathbb{Z}_{\geq 2}$ con $k \cdot l = m \Rightarrow \{k, l\} \cap m\mathbb{Z} = \emptyset$.
$k, l \neq m$

3.1.4. Prp. Sea R un anillo commutativo con 1. Entonces para un ideal $I \subset R$ son equiv.:

(1) I es ideal primo

(2) R/I es dominio entero

Dem. (1) $\Rightarrow$ (2) Claramente, R/I es un anillo commutativo con $1_{R/I} = 1 + I \neq 0_{R/I}$,

además, $(a+I)(b+I) = (0+I) \Rightarrow a \cdot b \in I$

hip. $\Rightarrow a \in I$ ó $b \in I$

$\Rightarrow (a+I = 0+I)$ ó $(b+I = 0+I)$ ✓

(2) $\Rightarrow$ (1) Por hip. $0 \neq 1_{R/I} \Rightarrow I \subsetneq R$.

Sean $a, b \in R$ con $a \cdot b \in I$

$\Rightarrow (a+I)(b+I) = (0+I) \Rightarrow a \in I$ ó $b \in I$ ✓

R/I dom. int.