Clase 14: Ideales y cocientes, Ideales primos y maximales.

§ 27. Ideales

Cultura general: Kummer introdujo en 1844 el concepto de "número complejo ideal" debido a su interés en la ecuación de Fermat

$$x^n + y^n = z^n \quad \text{con } x, y, z \in \mathbb{Z}.$$

Sin embargo, Dirichlet le hizo notar que su argumento (y probablemente el de Fermat!) fallaba pues el anillo

$$\mathbb{Z}[\zeta] = \{a + b\zeta,\ a, b \in \mathbb{Z}\} \quad \text{con } \zeta = e^{\frac{2\pi i}{n}}$$

no es en general un anillo de factorización única (cf. $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ en $\mathbb{Z}$).

autom. normal!

Def: Sea A un anillo. Un subconjunto $I \subseteq A$ es un ideal de A si:

a) $(I, +)$ es un subgrupo de $(A, +)$, y

b) Para todo $a \in A$ y $b \in I$, se tiene que $ab \in I$.

Ejemplo emblemático: Sea $A = \mathbb{Z}$. Entonces, todo subgrupo de $(\mathbb{Z}, +)$ es de la forma $n\mathbb{Z}$ para cierto $n \in \mathbb{N}^{\geq 1}$ (Bézout).
Por otro lado, $I_n := n\mathbb{Z}$ es un ideal del anillo $\mathbb{Z}$. ✓

$\boxed{\text{Ejercicio}}$ Probar que si $\{I_j\}_{j\in J}$ es una familia arbitraria de ideales de A, entonces $\bigcap_{j\in J} I_j$ es un ideal de A.

Def/Ejemplo: Sea A un anillo y $S \subseteq A$ un subconjunto, definimos

$$\langle S \rangle := \bigcap_{\substack{S \subseteq I \\ I \text{ ideal de } A}} I = \Big\{ \sum_{\text{finita}} a_i s_i \ , \ a_i \in A \ , \ s_i \in S \Big\}$$

el ideal generado por S. En part, si $S = \{a_1, \dots, a_r\}$ conjunto finito, escribimos $\langle S \rangle =: \langle a_1, \dots, a_r \rangle$. Más aún, decimos que $I \subseteq A$ es un ideal principal si $\exists a \in A$ tal que $I = \langle a \rangle \overset{\text{def}}{=} \{ax, x \in A\}$.
Decimos que A es un dominio de ideales principales (DIP) si todo ideal de A es principal y A es un dominio.

Ejemplo (cf. MAT210 !): Usando división euclideana, se prueba que $\mathbb{Z}$ y $k[X]$ (con k cuerpo) son DIP.

$\boxed{\text{Ejercicio}}$ Probar que $k[X,Y]$ no es un DIP [Indicación: Considerar $I = \langle X, Y \rangle$]

⚠ Observación clave: (cf. construcción de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$)

siempre existe

Sea $I \subseteq A$ un ideal y consideremos el grupo abeliano cuociente $(A/I, +)$:

$$(a+I) + (b+I) \overset{\text{def}}{:=} (a+b+I) \quad (\text{i.e.}, \ [a]+[b] := [a+b])$$

Si $a' \in [a]$ (i.e., $a - a' = i_1 \in I$) y $b' \in [b]$ (i.e., $b - b' = i_2 \in I$)

$$\Rightarrow ab = (a'+i_1)(b'+i_2) = a'b' + \underbrace{a'i_2 + b'i_1 + i_1 i_2}_{\in I} \Rightarrow [ab] = [a'b']$$

Luego, $[a]\cdot[b] \overset{\text{def}}{:=} [ab]$ en A/I está bien definido !

Así, $\pi : A \twoheadrightarrow A/I$ es un morfismo de anillos sobreyectivo con $\ker(\pi) = I$

$$a \mapsto [a] := a + I := a \ (\text{mod } I)$$

Recíprocamente (Ejercicio), si $(I,+)$ es un subgrupo de $(A,+)$ y $\pi: A \to A/I$ es un morfismo de anillos $\Rightarrow$ I es un ideal de A. ■

Lema: Sea $\varphi: A \to B$ un morfismo de anillos y $J \subseteq B$ un ideal. Entonces, $\varphi^{-1}(J) \subseteq A$ es un ideal. En part, $\ker(\varphi) \subseteq A$ es un ideal.

Dem: Sea $a \in A$ y $b \in \varphi^{-1}(J)$ (ie, $\varphi(b) \in J$)

$\Rightarrow \varphi(ab) = \varphi(a)\underbrace{\varphi(b)}_{\in J \text{ ideal}} \in J$, ie, $ab \in \varphi^{-1}(J)$ ✓ ■

Teorema (propiedad universal del cociente): Sean A y B anillos, $I \subseteq A$ un ideal y $\varphi: A \to B$ morfismo de anillos tal que $\varphi(I) = \{0_B\}$ (ie, $I \subseteq \ker(\varphi)$). Entonces, $\exists!\ \hat{\varphi}: A/I \to B$ morfismo de anillos tal que

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & \arrow[d, phantom, "\circlearrowleft"] & B \\ & A/I \arrow[ur, "\exists!\hat{\varphi}"'] & \end{tikzcd}$$

es conmutativo, ie, $\varphi = \hat{\varphi} \circ \pi$ (ie, $\varphi(a) = \hat{\varphi}([a])\ \forall a \in A$)

Igual que para grupos!

■

Consecuencia: Tal como para grupos, la propiedad universal del cociente permite probar (verbatim!) el teorema del isomorfismo de Noether:

"Para todo $\varphi : A \to B$ morfismo de anillos, $A/_{\ker(\varphi)} \xrightarrow[\sim]{\hat{\varphi}} \mathrm{Im}(\varphi)$ es un isomorfismo"

Es natural preguntarse qué anillos son los análogos de los grupos simples:

Prop: Sea $A \neq \{0\}$ un anillo. Entonces, los únicos ideales de A son $\{0\}$ y A si y sólo si A es un cuerpo.

Dem: $(\Rightarrow)$ Sea $a \neq 0 \Rightarrow \langle 0 \rangle \subsetneq \langle a \rangle \overset{\text{Hip}}{\Longrightarrow} \langle a \rangle = A \ni 1$ y en part $\exists\, b \in A$ tq $ab = 1$ ✓

$\underset{\uparrow \text{ ideal}}{I} = A \Leftrightarrow 1 \in I$

$(\Leftarrow)$ Sea $I \neq \langle 0 \rangle$ ideal y sea $a \neq 0$ tq $a \in I$

$\overset{A \text{ cuerpo}}{\Longrightarrow} \exists\, a^{-1} a = 1 \overset{\text{def}}{\in} I \Leftrightarrow I = A$. ∎

Ejemplos:

① Sabemos que la preimagen de un ideal es un ideal. Sin embargo, en general, la imagen de un ideal no es un ideal: cuerpo!

$\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ inclusión y $I_n = n\mathbb{Z}$ ideal de $\mathbb{Z}$ con $n \geq 1 \Rightarrow \varphi(I_n) \subseteq \mathbb{Q}$
$\quad x \longmapsto x$ no es un ideal!

② Sea A un dominio y $a \in A$ fijo. Consideremos el morfismo de A-álgebras

$$ev_a : A[X] \twoheadrightarrow A, \quad f \longmapsto f(a). \qquad \text{"de evaluación"}$$

Por división euclideana de polinomios, si $f \in A[X]$ entonces

$$f(X) = q(X)(X-a) + r, \quad \text{con } r = f(a), \text{ i.e., } ev_a(f) = r$$

$$\Rightarrow \ker(ev_a) = \langle X-a \rangle \quad \text{y así} \quad A[X]/\langle X-a\rangle \cong A \quad \text{(Noether)}$$

$\boxed{\text{Ejercicio}}$ Probar que si $a_1, \ldots, a_n \in A$ (dominio), entonces $A[X_1, \ldots, X_n]/\langle X_1 - a_1, \ldots, X_n - a_n \rangle \cong A$.

Def: Un subconjunto $S \subseteq A$ es multiplicativo si:

"$1 \in S$ y si $a, b \in S$ entonces $ab \in S$"

Un ideal $\mathfrak{p}$ es primo si $A - \mathfrak{p}$ es multiplicativo, i.e.,

a) $1 \notin \mathfrak{p}$ $(\Leftrightarrow \mathfrak{p} \subsetneq A)$,

b) Si $ab \in \mathfrak{p}$ entonces $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$.

Más adelante interpretaremos esto geométricamente!

Lema: Sea $\varphi: A \to B$ un morfismo de anillos y $T \subseteq B$ subconjunto.

1) Si T multiplicativo, entonces $\varphi^{-1}(T) \subseteq A$ es multiplicativo.

2) Si $\varphi: A \twoheadrightarrow B$ es sobreyectivo y $\varphi^{-1}(T)$ multiplicativo, entonces T es multiplicativo.

Dem: Sea $S := \varphi^{-1}(T) \subseteq A$. Entonces:

① $1_A \in S$ pues $\varphi(1_A) = 1_B \in T$ ✓

Si $a, b \in S \Rightarrow \varphi(ab) = \underbrace{\varphi(a)}_{\in T} \underbrace{\varphi(b)}_{\in T} \in T$, i.e., $ab \in S$ ✓

② Si $1_A \in S \Rightarrow \varphi(1_A) = 1_B \in T$ ✓ Si $a, b \in S \Rightarrow \varphi(a), \varphi(b), \varphi(ab) \in T$

Como φ sobre: todo $t \in T$ es de la forma $t = \varphi(s)$ para cierto $s \in S$. ∎

Prop: Sea $\varphi: A \to B$ un morfismo de anillos y $\mathfrak{q} \subseteq B$ un ideal.

1) Si $\mathfrak{q}$ es primo, entonces $\varphi^{-1}(\mathfrak{q}) \subseteq A$ es primo.
2) Si $\varphi: A \twoheadrightarrow B$ es sobreyectivo y $\varphi^{-1}(\mathfrak{q})$ es primo, entonces $\mathfrak{q}$ es primo.

Dem: Aplicar el Lema anterior a $T := B - \mathfrak{q}$. ■

Como consecuencia, obtenemos el siguiente criterio (que usaremos siempre!):

Corolario: Sea $\mathfrak{p} \subsetneq A$ un ideal. Entonces,

$\mathfrak{p}$ es primo $\iff$ $A/\mathfrak{p}$ es un dominio de integridad.

Dem: Sea $\pi: A \twoheadrightarrow A/\mathfrak{p}$ sobre., con $\ker(\pi) = \mathfrak{p}$, i.e., $\pi^{-1}(\langle [0] \rangle) = \mathfrak{p}$.

Luego:

$\pi^{-1}(\langle [0] \rangle) = \mathfrak{p}$ primo $\iff \langle [0] \rangle \subseteq A/\mathfrak{p}$ es primo.

$\iff [1] \notin \langle [0] \rangle$ y $[ab] \in \langle [0] \rangle \Rightarrow [a] \in \langle [0] \rangle$ ó $[b] \in \langle [0] \rangle$ ■

Ejemplos:

Clase anterior

① $I_n = n\mathbb{Z} \subseteq \mathbb{Z}$ es primo $\iff$ $\mathbb{Z}/n\mathbb{Z}$ dominio entero $\iff$ n es primo ✓

② Si A es un dominio y $a \in A$, entonces $A[X]/\langle X-a\rangle \cong A$ ← dominio!

$\Rightarrow \mathfrak{p}_a := \langle X-a\rangle$ es un ideal primo de $A[X]$ ✓

Def: Un ideal $\mathfrak{m} \subseteq A$ es maximal si

a) $1 \notin \mathfrak{m}$ (ie, $\mathfrak{m} \subsetneq A$),

b) Para todo ideal $I \subseteq A$ tal que $\mathfrak{m} \subsetneq I$, se tiene que $I = A$

Más adelante lo interpretaremos geométricamente!

Ejemplo: Si A es un dominio, entonces $\langle X\rangle \subseteq A[X,Y]$ es primo (pues tenemos $A[X,Y]/\langle X\rangle \cong A[Y]$ dominio). Pero $\langle X\rangle \subsetneq \langle X,Y\rangle$ no es maximal.

Lema útil: $A \neq \{0\}$ es un cuerpo $\iff$ $\langle 0\rangle \subseteq A$ es un ideal maximal.

Dem: ($\Rightarrow$) Sea I ideal tq $\langle 0\rangle \subsetneq I$ y sea $a \in I$ no-nulo $\overset{A \text{ cuerpo}}{\Longrightarrow}$ $a^{-1}a = 1 \in I \Rightarrow I = A$

($\Leftarrow$) Sea $a \neq 0 \Rightarrow \langle 0\rangle \subsetneq \langle a\rangle$ y luego $\langle a\rangle = A \ni 1 \Rightarrow \exists b \in A$ tq $ab = 1$ ∎

$\boxed{\text{Ejercicio útil}}$ Sea k un cuerpo y $A \neq \{0\}$ un anillo. Probar que todo morfismo de anillos no-nulo $\varphi : k \hookrightarrow A$ es inyectivo.

Obs importante: Tal como para grupos, si $I \subseteq A$ es un ideal hay una correspondencia biyectiva (vía $\pi : A \twoheadrightarrow A/I$):

$$\left\{ \begin{matrix} \text{Ideales } J \subseteq A \\ \text{tal que } I \subseteq J \end{matrix} \right\} \xleftrightarrow[\sim]{1:1} \left\{ \begin{matrix} \text{Ideales} \\ K \subseteq A/I \end{matrix} \right\}$$

$$J \longmapsto J/I := \pi(J) = \{[b],\ b \in J\}$$

$$\pi^{-1}(K) \longleftarrow K$$

Además, se preservan inclusiones. En particular, $K \subseteq A/I$ maximal $\Leftrightarrow \pi^{-1}(K)$ maximal.

Corolario: Sea $\mathfrak{m} \subsetneq A$ un ideal. Entonces,

$$\mathfrak{m} \text{ es maximal} \iff A/\mathfrak{m} \text{ es un cuerpo}.$$

Dem: $\mathfrak{m} \subseteq A$ maximal $\underset{\substack{\pi : A \to A/\mathfrak{m} \\ \mathfrak{m} \mapsto 0}}{\iff}$ $\langle [0] \rangle \subseteq A/\mathfrak{m}$ maximal $\underset{\text{lema útil}}{\iff}$ $A/\mathfrak{m}$ cuerpo ■

Ejemplo importante: Sea k un cuerpo y $a = (a_1, \dots, a_n) \in k^n$. Entonces, $\mathfrak{m}_a := \langle X_1 - a_1, \dots, X_n - a_n \rangle \subseteq k[X_1, \dots, X_n]$ es maximal pues

$$k[X_1, \dots, X_n] / \mathfrak{m}_a \cong k \quad \text{es un cuerpo.}$$

Teorema (Krull, 1929): Todo anillo $A \neq \{0\}$ posee un ideal maximal. Además, todo ideal $I \neq A$ está contenido en algún ideal maximal.

Dem: Sea $I \subsetneq A$ un ideal y consideremos:
$\mathcal{P} = \{ J \subsetneq A \text{ ideal tq } I \subseteq J \}$. En part, $\mathcal{P} \neq \emptyset$ pues $I \in \mathcal{P}$ y además $\mathcal{P}$ es parcialmente ordenado resp. a la inclusión "$\subseteq$".

Dada una cadena $\mathcal{C} \subseteq \mathcal{P}$ (ie, $\forall J_1, J_2 \in \mathcal{C}$ se tiene que $J_1 \subseteq J_2$ ó $J_2 \subseteq J_1$)
$\Rightarrow J_{sup} := \bigcup_{J \in \mathcal{C}} J$ pertenece a $\mathcal{P}$ (pues $1 \notin J \ \forall J \in \mathcal{P}$) y es una cota superior de $\mathcal{C}$ (ie, $J \subseteq J_{sup} \ \forall J \in \mathcal{C}$) $\rightsquigarrow$ Lema de Zorn: $\exists \mathfrak{m} \in \mathcal{P}$ elemento maximal (ie, $\forall J \in \mathcal{P}$: si $\mathfrak{m} \subseteq J \Rightarrow \mathfrak{m} = J$) $\underset{\text{def}}{\Longrightarrow}$ $\mathfrak{m} \subsetneq A$ ideal maximal con $I \subseteq \mathfrak{m}$ ■