Ideales primos

Facultad de Ciencias UNAM

Introducción

Una propiedad interesante del anillo $\mathbb{Z}$ es que hay una biyección natural entre los ideales de $\mathbb{Z}$ y los elementos de $\mathbb{Z}$ (dada por $n \leftrightarrow (n) = n\mathbb{Z}$). Como

$$m \in n\mathbb{Z} \iff \exists k \in \mathbb{Z} \text{ tal que } m = nk \iff n|m$$

es natural definir propiedades (sobre ideales arbitrarios) que estén inspiradas en propiedades de divisibilidad de los enteros. Por ejemplo, la propiedad de ser un numero primo. Con esto en mente, introducimos la siguiente definición.

Ideales primos

Definición

Supongamos que R es un anillo conmutativo y que P es un ideal propio de R. Decimos que P es un **ideal primo de** R si satisface la siguiente condición:

$$\forall a, b \in R\,(ab \in I \implies a \in I \text{ o } b \in I)$$

Es importante mencionar que la propiedad de "ser ideal primo" depende del anillo donde se considere el ideal. Por ejemplo, $6\mathbb{Z}$ no es un ideal primo en $\mathbb{Z}$[1], pero $6\mathbb{Z}$ es un ideal primo en $3\mathbb{Z}$[2].

[1] $2 \cdot 3 = 6 \in 6\mathbb{Z}$ pero $2 \notin 6\mathbb{Z}$ y $3 \notin 6\mathbb{Z}$.

[2] Procedamos por contrapuesta: supongamos que $k, l \in \mathbb{Z}$ son tales que $3k \notin 6\mathbb{Z}$ y $3l \notin 6\mathbb{Z}$. Como $6 = 3 \cdot 2$, esto implica que k y l son impares. Dejamos al lector verificar que si k y l son impares, $3k \cdot 3l \notin 6\mathbb{Z}$.

Observación

La noción de ideal primo generaliza la noción de numero primo en los enteros. En efecto, supongamos que $n \in \mathbb{Z}_{\geq 2}$. Por definición, el ideal $n\mathbb{Z}$ es primo si y solo si

$$\forall a, b \in \mathbb{Z}\,(ab \in n\mathbb{Z} \implies a \in n\mathbb{Z} \text{ o } b \in n\mathbb{Z})$$

Recordando que $m \in n\mathbb{Z}$ si y solo si $n|m$, podemos reescribir la condición anterior de la siguiente manera.

$$\forall a, b \in \mathbb{Z}\,\big(n|ab \implies n|a \text{ o } n|b\big)$$

Sin embargo, esto es equivalente a que n sea primo. Por lo tanto, $n\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ si y solo si n es primo.

En particular, los ideales primos no nulos en $\mathbb{Z}$ coinciden con los ideales maximales en $\mathbb{Z}$. Sin embargo, como pronto veremos, en general esto no es cierto.

Un ideal que *no* es primo

Sea

$$I := \left\{ f \in \mathcal{C}([0,1]) \mid f\left(\frac{1}{2}\right) = 0 \text{ y } f\left(\frac{1}{3}\right) = 0 \right\}.$$

Es fácil ver que I es un ideal de $\mathcal{C}([0,1])$. Veamos que I no es primo. Sean $f, g : [0,1] \to \mathbb{R}$ tales que

$$f(x) = x - \frac{1}{2} \quad \text{y} \quad g(x) = x - \frac{1}{3}$$

Claramente, $f \notin I$, $g \notin I$, pero $fg \in I$.

Una caracterización de los ideales primos de un anillo conmutativo

Proposición 1

Supongamos que R es un anillo conmutativo. Si P es un ideal de R, entonces

$$P \text{ es primo } \iff R/P \text{ es un dominio entero.}$$

En particular,

- un anillo conmutativo es un dominio entero si y solo si el ideal 0 es primo, y
- en general, los ideales primos no nulos no coinciden con los ideales maximales.

Demostración. Supongamos que R es un anillo conmutativo. Si P es un ideal de R, entonces

$$
\begin{aligned}
P \text{ es primo} &\iff \\
\forall a, b \in R\,(ab \in P &\implies a \in P \text{ o } b \in P) &\iff \\
\forall a, b \in R\,(ab + P = P &\implies a + P = P \text{ o } b + P = P) &\iff \\
\forall a, b \in R\,\big((a + P)(b + P) = P &\implies a + P = P \text{ o } b + P = P\big) &\iff \\
\forall x, y \in R/P\,(xy = 0 &\implies x = 0 \text{ o } y = 0) &\iff \\
R/P \text{ es un dominio entero} &
\end{aligned}
$$

□

Maximal $\Longrightarrow$ primo

Proposición 2

Supongamos que R es un anillo conmutativo con 1. Si I es un ideal maximal de R, entonces I es un ideal primo de R.

Demostración.

$$\begin{aligned} I \text{ es maximal} &\iff R/I \text{ es un campo} \\ &\Longrightarrow R/I \text{ es un dominio entero} \\ &\iff I \text{ es primo.} \end{aligned}$$

Primo $\not\Rightarrow$ maximal

El subanillo 0 de $\mathbb{Z}$ es primo pero no es maximal. Para ver un ejemplo menos chafa, recuerda que en la proposición 1.9.3. demostramos que para cualquier anillo, $R[x]/(x) \cong R$. Con esto en mente, notemos que

- El ideal (x) en $\mathbb{Z}[x]$ es primo porque $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ y $\mathbb{Z}$ es un dominio entero. Sin embargo, (x) no es maximal[3].
- En general, si R es un anillo conmutativo, entonces[4] tenemos que

$$(x) \text{ es primo en } R[x] \iff R \text{ es un dominio entero}$$

y

$$(x) \text{ es maximal en } R[x] \iff R \text{ es un campo.}$$

[3] Esto es consecuencia de la caracterización de ideales maximales en anillos conmutativos y de que $\mathbb{Z}$ no es campo.

[4] Usando el isomorfismo $R[x]/(x) \cong R$ y las caracterizaciones de ideales primos y maximales

Condiciones suficientes para que primo $\Longrightarrow$ maximal

Proposición 3

Supongamos que R es un anillo conmutativo.

1. Si R es finito y tiene 1, entonces todo ideal primo de R es maximal.
2. Si para toda $a \in R$ existe $n \in \mathbb{Z}_{>1}$ tal que $a^n = a$, entonces todo ideal primo de R es maximal.

Demostración.

1. Supongamos que P es un ideal primo de R. Usando la caracterización de ideales primos en anillos conmutativos y el hecho de que R es un anillo conmutativo finito con unidad, obtenemos que R/P es un dominio entero finito con unidad. Esto implica que R/P es un campo (recuerda que en la sección 1.5 vimos que "dominio entero finito con 1 $\implies$ campo"). Por lo tanto (por la caracterización de ideales maximales en anillos conmutativos), P es maximal.
2. Sea P un ideal primo de R. Entonces R/P es un dominio entero. Queremos ver que R/P es un campo. Para esto, sea $a + P \in R/P$ un elemento no nulo. En particular, $a \notin P$ y por hipótesis, existe $n \in \mathbb{Z}_{>1}$ tal que $a^n = a$. Pero

   $a^n = a \implies a^n - a = 0 \implies a(a^{n-1} - 1) = 0 \in^5 P \implies^6 a^{n-1} - 1 \in P \implies (a^{n-1} + 1) + P = P \implies (a + P)(a^{n-2} + P) = a^{n-1} + P = 1 + P$

   Por lo tanto, todo elemento no nulo de R/P tiene un inverso multiplicativo. Es decir, R/P es un campo.

[5] P es un ideal
[6] P es primo y $a \notin P$

Dos propiedades interesante de los ideales primos

Proposición 4

Supongamos que R es un anillo conmutativo y que P es un ideal primo de P.

1. Si P no tiene divisores de 0, entonces R es un dominio entero.
2. Si $A, B \subset R$ son subconjuntos de R, entonces

$$\{ab \mid a \in A,\ b \in B\} \subset P \implies A \subset P \text{ o } B \subset P$$

Demostración.

1. Supongamos que $a, b \in R$ son tales que $ab = 0$. Como P es ideal, entonces $ab = 0 \in P$. Mas aun, como P es primo, entonces $a \in P$ o $b \in P$. Sin perdida de generalidad, supongamos que $a \in P$. Pero entonces, $b = 0$: de lo contrario, $a \in P$ seria un divisor de cero, contradiciendo la hipótesis. De la misma manera, si suponemos $b \in P$, obtenemos $a = 0$. Por lo tanto, acabamos de demostrar que

$$\forall a, b \in R \, (ab = 0 \implies a = 0 \text{ o } b = 0)$$

   Es decir, R es un dominio. Finalmente, como es conmutativo, es un dominio entero.

2. Supongamos que $\{ab \mid a \in A,\ b \in B\}$ y que $B \not\subset P$. Entonces existe $b_0 \in B \setminus P$. Luego, para toda $a \in A$ tenemos $ab_0 \in P$. Pero como P es primo y $b_0 \notin P$, esto implica que $a \in P$ para toda $a \in A$. Es decir, $A \subset P$.

□

Ideales primos/maximales y homomorfismos de anillos

Proposición 5

Supongamos que $\varphi : R \to R'$ es un homomorfismo de anillos conmutativos.

1. Si P es un ideal primo de R', entonces $\varphi^{-1}(P)$ es un ideal primo de R o $\varphi^{-1}(P) = R$.
2. Si R y R' tienen unidad, φ es suprayectiva, y M es un ideal maximal de R', entonces $\varphi^{-1}(M)$ es un ideal maximal de R.

Demostración.

1. Supongamos que P es un ideal primo de R' y que $\varphi^{-1}(P) \neq R$. Para ver que $\varphi^{-1}(P)$ es primo, supongamos que $a, b \in R$ son tales que $ab \in \varphi^{-1}(P)$. Entonces, por definición, $\varphi(a)\varphi(b) = \varphi(ab) \in P$. Como P es primo, esto implica que $\varphi(a) \in P$ o $\varphi(b) \in P$. En otras palabras, $a \in \varphi^{-1}(P)$ o $b \in \varphi^{-1}(P)$.
2. Supongamos que M es un ideal maximal de R' y que φ es suprayectiva. Sea $\pi : R' \to R'/M$ la proyección canónica. Como φ es suprayectiva, el homomorfismo $\pi \circ \varphi : R \to R'/M$ también. Veamos que $\ker \pi \circ \varphi = \varphi^{-1}(M)$.

   $x \in \ker \pi \circ \varphi \iff \varphi(x) \in \ker \pi \iff \varphi(x) + M = M \iff$
   $\varphi(x) \in M \iff x \in \varphi^{-1}(M)$

   Por lo tanto, el primer teorema de isomorfismos implica $R/\varphi^{-1}(M) = R/(\ker \pi \circ \varphi) \cong R'/M$. Usando la caracterización de ideales maximales en un anillo conmutativo, obtenemos lo deseado.

□

Observación

- Una aplicación inmediata del primer inciso de la proposición anterior es la siguiente: si R es un subanillo de R' y φ es la inclusión $R \hookrightarrow R'$, entonces $P \cap R = \varphi^{-1}(P)$ es un ideal primo de R o $P \cap R = R$.
- La suprayectividad de φ en el segundo inciso de la proposición anterior es necesaria: (damos dos ejemplos)
  - Si R es un anillo, M es un ideal maximal de R, y $i : M \hookrightarrow R$ es la inclusión, entonces $i^{-1}(M) = M$ es la preimagen de un ideal maximal en R, pero no es maximal en M.
  - Si $i : \mathbb{Z} \hookrightarrow \mathbb{Q}$ es la inclusión usual, entonces $i^{-1}(\{0\}) = \{0\}$ es la preimagen de un ideal maximal en $\mathbb{Q}$ (recordemos que un anillo es un campo si y solo si el subanillo 0 es maximal) pero no es maximal en $\mathbb{Z}$.