Ideales maximales

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos el concepto de ideal maximal. En principio podría parecer un concepto un poco arbitrario pues no esta en términos de la suma o de la multiplicación; de hecho, solo esta en términos de la relación "$\subset$" entre los ideales de un anillo. Sin embargo, pronto volverá evidente su importancia.

Ideales maximales

Definición

Supongamos que R es un anillo y que M es un ideal propio de R. Decimos que M es un **ideal maximal de** R si $M \neq R$ y el único ideal de R que contiene *propiamente* a M es R. En otras palabras, M es maximal si para todo $I \subset R$ se satisface la siguiente condición:

$$\big(I \text{ es ideal de } R \text{ y } M \subsetneqq I\big) \implies I = R.$$

Es importante mencionar que la propiedad "ser ideal maximal" depende del anillo en donde se considere el ideal. Por ejemplo, $4\mathbb{Z}$ no es un ideal maximal en $\mathbb{Z}$[1], pero $4\mathbb{Z}$ si es un ideal maximal en $2\mathbb{Z}$[2].

[1] Pues $4\mathbb{Z} \subsetneqq 2\mathbb{Z} \subsetneqq \mathbb{Z}$.

[2] Pues $4\mathbb{Z} \subsetneqq 2\mathbb{Z}$ y todos los ideales de $2\mathbb{Z}$ son de la forma $k2\mathbb{Z}$ (esto es consecuencia de que si I es ideal de $2\mathbb{Z}$, entonces es un subgrupo aditivo de $2\mathbb{Z}$ y por lo tanto, también es subgrupo aditivo de $\mathbb{Z}$; pero los subgrupos aditivos de $\mathbb{Z}$ son precisamente los $n\mathbb{Z}$).

Unos ejemplos

Sea $R := \mathbb{Z} + i\mathbb{Z} = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$. Entonces,

- $M := \{a + ib \in R \mid 3|a \text{ y } 3|b\}$ es un ideal maximal de R:

  Es fácil verificar que M es un ideal de R. Veamos que es maximal. Para esto, supongamos que N es un ideal de R tal que $M \subsetneq N$. Entonces existen $r, s \in \mathbb{Z}$ tales que $r + is \in N$ pero $3 \nmid r$ o $3 \nmid s$. En cualquier caso, tenemos[3] $3 \nmid t := r^2 + s^2 = (r - is)(r + is) \in N$ donde la pertenencia se cumple porque $r - is \in R$, $r + is \in N$ y N es ideal de R. Luego, como 3 es primo y $3 \nmid t$, entonces 3 y t son primos relativos. Entonces existen $u, v \in \mathbb{Z}$ tales que $u3 + vt = 1$. Pero $u3 + vt \in N$ porque $3 \in M \subset N$ y $t \in N$. Por lo tanto, $1 = u3 + vt \in N$ y $N = R$.

[3] Sin perdida de generalidad, supongamos que $3 \nmid r$. Haciendo las cuentas, es fácil verificar que al pasar a $\mathbb{Z}_3$, tenemos $[r^2]_3 = [1]_3$ y $[s^2]_3 \in \{[0]_3, [1]_3\}$. Usando esto, es fácil ver que $[r^2 + s^2]_3 \neq [0]_3$ y por lo tanto, $3 \nmid r^2 + s^2$.

- $I \coloneqq \{a + ib \in R \mid 5|a \text{ y } 5|b\}$ es un ideal *no* maximal de R:

  Es fácil verificar que I es un ideal. Veamos que no es maximal. Sea

  $$N \coloneqq \{x(2+i) \mid x \in R\}.$$

  Es fácil verificar que N es un ideal de R y como $5 = (2-i)(2+i)$, entonces $I \subset M$. Sin embargo, $N \neq R$. En efecto, de lo contrario, existirían $a, b \in \mathbb{Z}$ tales que $(a+ib)(2+i) = 1$. Distribuyendo y usando la igualdad en los complejos, obtendríamos las siguientes ecuaciones

  $$2a - b = 1 \text{ y } 2b + a = 0$$

  Resolviendo estas ecuaciones obtendríamos $a = \frac{5}{2}$ y $b = -\frac{1}{5}$, contradiciendo que $a, b \in \mathbb{Z}$. Por lo tanto, $N \neq R$ y como $I \subset N$, entonces I no es maximal.

Observación

Hay anillos que no tienen ideales maximales: Por ejemplo, considera $\mathbb{Q}$ con la suma usual pero con la multiplicación trivial. Es decir, $ab = 0$ para toda $a, b \in \mathbb{Q}$. De esta manera, los ideales del anillo $\mathbb{Q}$ coinciden con los subgrupos aditivos (usuales) de $\mathbb{Q}$. Por lo tanto, basta demostrar que el grupo aditivo $\mathbb{Q}$ no tiene subgrupos maximales. Para esto, supongamos que $H \neq 0$ es un subgrupo (aditivo) propio de $\mathbb{Q}$. Notemos que si $x \in \mathbb{Q} \setminus H$, entonces $H \subsetneqq H + (x)$. Por lo tanto, si demostramos que $H + (x) \neq \mathbb{Q}$, obtenemos lo deseado[4]. Para ver esto, sea $y \in H \setminus \{0\}$. Mas aun, sean $a, b \in \mathbb{Z}$ tales que $\frac{x}{y} = \frac{a}{b}$. Veamos que $\frac{x}{a} \notin H + (x)$. De lo contrario, existe $h \in H$ y $n \in \mathbb{Z}$ tales que $\frac{x}{a} = h + nx$. De donde,

$$x = a(h + nx) = ah + anx = ah + nax = ah + nby \in H$$

donde la ultima igualdad se cumple porque $\frac{x}{y} = \frac{a}{b}$, y la pertenencia se cumple porque $h, y \in H$ y $a, b, n \in \mathbb{Z}$.

[4]De esta manera, habremos demostrado que H esta propiamente contenido en un subgrupo (aditivo) propio de $\mathbb{Q}$.

Comentario

En la observacion anterior vimos que no todos los anillos tienen ideales maximales. Sin embargo, en la siguiente proposición veremos que esto no es cierto para anillos con 1, es decir, veremos que todos los anillos con 1 tienen ideales maximales. De hecho, veremos algo mas fuerte:

> *Si R es un anillo con 1 y I es un ideal propio de R, entonces existe un ideal maximal M_I de R tal que $I \subset M_I$.*

Para demostrar esto, necesitaremos el famoso *Lema de Zorn*[5]. Lamentablemente, la demostración no entra en los objetivos del curso y por eso, solamente enunciamos el resultado. Para esto, necesitaremos unas definiciones.

[5] Es interesante notar que es equivalente al axioma de elección

Definiciones para el Lema de Zorn

Definición

Un **conjunto parcialmente ordenado** es una pareja ordenada $(P, \preceq)$ donde P es un conjunto y $\preceq$ es una relación en P que es (1) reflexiva, (2) antisimétrica, y (3) transitiva. Mas aun, supongamos que $S \subset P$ es un subconjunto de P.

- Decimos que S es una **cadena** en P (respecto a $\preceq$) si para toda $x, y \in S$, $x \preceq y$ o $y \preceq x$.
- Decimos que $m \in S$ es **maximal** en S (respecto a $\preceq$) si no existe $s \in S \setminus \{m\}$ tal que $m \preceq s$.
- Decimos que $c \in S$ es una **cota superior** de S (respecto a $\preceq$) si para toda $s \in S$, $s \preceq c$.

Observación

- Si X es un conjunto y $\mathcal{F}$ es una familia de subconjuntos de X, entonces $(\mathcal{F}, \subset)$ es un conjunto parcialmente ordenado[6].
- Supongamos que R es un anillo y sea $\mathcal{F}$ el conjunto que consiste de todos los ideales de R. Entonces,

  $$I \text{ es un ideal maximal de } R \iff I \text{ es maximal en } \mathcal{F} \text{ (respecto a } \subset).$$

  Sin embargo, hay que tener cuidado: si $\mathcal{S} \subsetneqq \mathcal{F}$, puede existir $I \in \mathcal{S}$ tal que I es un elemento maximal en $\mathcal{S}$ (respecto a $\subset$) pero I no es ideal maximal de R. Por ejemplo, si $\mathcal{S} = \{(4), (5), (6)\}$, entonces cada uno de los elementos de $\mathcal{S}$ son maximales en $\mathcal{S}$ (respecto a $\subset$) pero solo (5) es un ideal maximal de $\mathbb{Z}$.

[6] Por supuesto, "$\subset$" es la inclusión usual de conjuntos.

El Lema de Zorn

Teorema 1

Supongamos que $(P, \preceq)$ es un conjunto parcialmente ordenado. Si toda cadena en P tiene una cota superior en P, entonces P contiene un elemento maximal.

Los anillos con 1 tienen ideales maximales

Proposición 2

Supongamos que R es un anillo con 1. Si I es un ideal propio de R, entonces existe un ideal maximal M_I de R tal que $I \subset M_I$.

Demostración. Supongamos que R es un anillo con 1 y que I es un ideal propio de R. Sea $\mathcal{S}$ el conjunto de todos los ideales propios de R que contienen a I. Entonces, $\mathcal{S}$ es no vació ($I \in \mathcal{S}$) y $\mathcal{S}$ con la inclusión usual de conjuntos "$\subset$" es un conjunto parcialmente ordenado. Como queremos usar el Lema de Zorn, supongamos que $\mathcal{C}$ es una cadena en $\mathcal{S}$. Veamos que $\mathcal{C}$ tiene una cota superior en $\mathcal{S}$. Naturalmente, definimos

$$J := \bigcup_{A \in \mathcal{C}} A$$

Por la forma en la que definimos J, debería ser claro que para ver que J es cota superior de $\mathcal{C}$ en $\mathcal{S}$, basta probar que $J \in \mathcal{S}$.

- J es un ideal de R.

  Subgrupo aditivo: Supongamos que $a, b \in J$. Por definición de J, existen $A, B \in \mathcal{C}$ tales que $a \in A$ y $b \in B$. Luego, como $\mathcal{C}$ es una cadena, entonces $A \subset B$ o $B \subset A$. En el primer caso (como A y B son ideales de R), $b - a \in B \subset J$; en el segundo, $b - a \in A \subset J$. Por lo tanto, (independientemente del caso) $b - a \in J$.

  Cerrado bajo multiplicación por elementos arbitrarios: Supongamos que $r \in R$ y $a \in J$. Por definición de J, existe $A \in \mathcal{C}$ tal que $a \in A$. Luego, como A es un ideal de R, entonces $ra \in A \subset J$. Por lo tanto, $ra \in J$.

- J es propio.

  Supongamos lo contrario. Entonces, $1 \in J$ y por lo tanto, por definición de J, existe $A \in \mathcal{C}$ tal que $1 \in A$. Contradiciendo el hecho de que A es un ideal propio[7] de R.

- J contiene a I.

  Por definición, todo $A \in \mathcal{C}$ contiene a I y por lo tanto, J también.

[7]Esto es consecuencia de que $A \in \mathcal{C} \subset \mathcal{S}$ y de la definición de $\mathcal{S}$

Por lo tanto, $J \in \mathcal{S}$ y acabamos de demostrar que toda cadena en $\mathcal{S}$ tiene una cota superior en $\mathcal{S}$. Entonces, podemos aplicarle el Lema de Zorn a $\mathcal{S}$ para obtener un elemento maximal $M_I \in \mathcal{S}$. Es decir, no existe ningún $K \in \mathcal{S}$ que contenga propiamente a M_I. Para ver que M_I es maximal, supón lo contrario y contradice el enunciado anterior usando que $I \subset$[8] M_I. Por lo tanto, para todo ideal propio I de R existe un ideal maximal M_I tal que $I \subset M_I$. □

[8]Pues $M_I \in \mathcal{S}$.

Una caracterización de los ideales maximales de un anillo conmutativo

Proposición 3

Supongamos que R es un anillo conmutativo con 1. Si M es un ideal de R, entonces

$$M \text{ es maximal} \iff R/M \text{ es un campo.}$$

Demostración. M es maximal $\iff$ no existe I ideal de R tal que $M \subsetneq I \subsetneq R$ $\iff$ [9] los únicos ideales de R/M son los triviales $\iff$ [10] R/M es un campo.

[9] Recordemos que el cuarto teorema de isomorfismos da una biyección entre los ideales de R que contienen a M y los ideales de R/M que son distintos de 0.

[10] Recordemos que un anillo conmutativo con 1 solo tiene ideales triviales si y solo si es un campo.

Observación

Cabe recalcar que en la demostración de la proposición anterior, solo ocupamos la conmutatividad de R en la "ida" del ultimo " $\iff$ ". Específicamente, solo la ocupamos en la implicación "los únicos ideales de R/M son los triviales $\implies R/M$ es un campo". Por lo tanto, tenemos la siguiente proposición:

Supongamos que R es un anillo (no necesariamente conmutativo). Si M es un ideal de R tal que R/M es un campo, entonces M es maximal.

Aplicaciones de la proposición anterior

- Supongamos que R es un anillo conmutativo con 1. Entonces, R es un campo si y solo si el subanillo 0 es maximal en R.
- Supongamos que $n \in \mathbb{Z}_{\geq 1}$. Por la proposición anterior,

  $$n\mathbb{Z} \text{ es maximal } \iff \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \text{ es un campo.}$$

  Sin embargo, ya sabemos que $\mathbb{Z}/n\mathbb{Z}$ es un campo si y solo si n es primo. Por lo tanto[11], los ideales maximales de $\mathbb{Z}$ son precisamente los $p\mathbb{Z}$ con p primo.
- Supongamos que A es un anillo conmutativo, X es un conjunto, $c \in X$, y $E_c : A^X \to A$ es tal que $f \mapsto f(c)$. Entonces, $\ker E_c = \{f \in A^X \mid f(c) = 0\}$ y por el primer teorema de isomorfismos, $A^X / \ker E_c \cong A$. Por lo tanto, $\ker E_c$ es un ideal maximal de A^X si y solo si A es un campo.

[11] Recordemos que los ideales de $\mathbb{Z}$ son precisamente los $n\mathbb{Z}$.

En particular, para toda $c \in [0,1]$, $\{f \in [0,1]^{\mathbb{R}} \mid f(c) = 0\}$ es un ideal maximal de $\mathbb{R}^{[0,1]}$. Mas aun, como

$$\mathcal{C}([0,1])/\{f \in \mathcal{C}([0,1]) \mid f(c) = 0\} \cong \mathbb{R}$$

entonces, $\{f \in \mathcal{C}([0,1]) \mid f(c) = 0\}$ es un ideal maximal de $\mathcal{C}([0,1])$.

- El ideal $(2, x)$ es maximal en $\mathbb{Z}[x]$ porque $\mathbb{Z}[x]/(2, x) \cong \mathbb{Z}_2$. En efecto, si $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_2$ es tal que $p(x) \mapsto [p(0)]_2$, entonces φ es un homomorfismo suprayectivo con kernel $(2, x)$.

  Mas aun, usando esto, vemos que el ideal (x) en $\mathbb{Z}[x]$ no es maximal porque $(x) \subsetneq$[12] $(2, x) \subsetneq \mathbb{Z}[x]$.

[12] La inclusión es propia porque $2 \notin (x)$.