Ideales generados

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos el concepto de ideal generado. Naturalmente, este juega el mismo rol en teoría de anillos, que el concepto de grupo generado en la teoría de grupos. Sin embargo, veremos que la existencia de las dos operaciones y la no (necesaria) conmutatividad de la multiplicación, requieren un poquito mas de cuidado.

La intersección arbitraria de ideales es un ideal

Proposición 1

Supongamos que R es un anillo. Si $\{I_\alpha\}_{\alpha\in\mathcal{A}}$ es una familia de ideales izquierdos de R, entonces $I := \bigcap_{\alpha\in\mathcal{A}} I_\alpha$ es un ideal izquierdo de R.
Mas aun, si en el enunciado anterior cambiamos "izquierdo" por "derecho" o "bilateral", el enunciado sigue siendo cierto.

Demostración. Supongamos que $r \in R$ e $i \in I$. Por definición, $i \in I_\alpha$ para toda $\alpha \in \mathcal{A}$. Como I_α es ideal, entonces $ri \in I_\alpha$ para toda $\alpha \in \mathcal{A}$. Por lo tanto, $ri \in \bigcap_{\alpha\in\mathcal{A}} I_\alpha$. Es decir, I es un ideal izquierdo de R. □

Ideales generados

Definición

Supongamos que R es un anillo y $A \subset R$ es un subconjunto de R. El *ideal izquierdo de R generado por A*, denotado RA es el ideal izquierdo de R mas chico que contiene a A. El *ideal derecho de R generado por A*, denotado AR es el ideal derecho de R mas chico que contiene a A. El *ideal bilateral de R generado por A*, denotado RAR es el ideal bilateral de R mas chico que contiene a A. Específicamente,

$$RA := \bigcap \{I \subset R \mid I \text{ es un ideal izquierdo de } R \text{ y } A \subset I\}$$

$$AR := \bigcap \{I \subset R \mid I \text{ es un ideal derecho de } R \text{ y } A \subset I\}$$

$$(A) := \bigcap \{I \subset R \mid I \text{ es un ideal bilateral de } R \text{ y } A \subset I\}$$

Una caracterización del ideal generado

Proposición 2

Supongamos que R es un anillo. Si $A \subset R$ es un subconjunto de R, entonces

$$RA = \left\{ r_1 a_1 + \cdots + r_n a_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}_{\geq 1} \right\}$$
$$AR = \left\{ a_1 r_1 + \cdots + a_n r_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}_{\geq 1} \right\}$$
$$(A) = \left\{ r_1 a_1 r_1' + \cdots + r_n a_n r_n' \mid r_i, r_i' \in R,\ a_i \in A,\ n \in \mathbb{Z}_{\geq 1} \right\}$$

Demostración. Veamos la primera igualdad. Las otras dos son análogas.
$\subset$) $\left\{ r_1 a_1 + \cdots + r_n a_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}_{\geq 1} \right\}$ es un ideal izquierdo que contiene a A.
$\supset$) Todo ideal izquierdo que contiene a A contiene a $\left\{ r_1 a_1 + \cdots + r_n a_n \mid r_i \in R,\ a_i \in A,\ n \in \mathbb{Z}_{\geq 1} \right\}$. $\square$

Ideales principales e ideales finitamente generados

Definición

Supongamos que R es un anillo.

- Un *ideal izquierdo principal de* R es un ideal de la forma $R\{a\}$, donde $a \in R$. En este caso escribimos $Ra := R\{a\}$. De manera análoga, definimos los *ideales derechos principales de* R y los *ideales bilaterales principales*. En estos casos escribimos $aR := \{a\}R$ y $(a) := (\{a\})$.
- Un *ideal izquierdo finitamente generado* es un ideal de la forma $R\{a_1, \ldots, a_n\}$, donde $a_1, \ldots, a_n \in R$. De manera análoga, definimos los *ideales derechos finitamente generados* y los *ideales bilaterales finitamente generados*. Finalmente, introducimos la siguiente notación: $(a_1, \ldots, a_n) := (\{a_1, \ldots, a_n\})$.

Observación

- Supongamos que R es un anillo. Entonces, el ideal 0 es principal: $0 = (0_R)$. Mas aun, si R tiene 1, entonces R también es principal: $R = R1 = 1R = (1)$.
- Si el anillo R no esta especificado, la notación (A) es ambigua. En efecto, el ideal principal (2) de $\mathbb{Z}$ (generado por el numero 2 en $\mathbb{Z}$) es simplemente $2\mathbb{Z}$, pero el ideal principal (2) de $\mathbb{Q}$ es todo $\mathbb{Q}$, pues $1 = \frac{1}{2} \cdot 2 \in (2)$.
- Si R es un anillo conmutativo y $a \in R$, entonces $(a) = \{ras \mid r, s \in R\}$. Sin embargo, si R no es conmutativo, el conjunto $\{ras \mid r, s \in R\}$ no es necesariamente cerrado bajo suma.
- Si R es un anillo conmutativo y $a, b \in R$, entonces $b \in (a)$ si y solo si $b = ra$ para alguna $r \in R$. En otras palabras, $b \in (a)$ si y solo si b **es un múltiplo de** a o a **divide a** b. Mas aun, es fácil verificar que $b \in (a)$ si y solo si $(b) \subset (a)$. Por lo tanto la relación (en términos de contención) entre dos ideales parece capturar algunas propiedades de la aritmética de anillos conmutativos.

Los ideales de $\mathbb{Z}$

Primero notemos que para toda $n \in \mathbb{Z}$ tenemos $n\mathbb{Z} = \mathbb{Z}n = (n) = (-n)$. Ahora bien, recordemos que como (1) todos los subgrupos aditivos de $\mathbb{Z}$ son los $n\mathbb{Z}$, con $n \in \mathbb{Z} \setminus \{0\}$ y (2) todos los $n\mathbb{Z}$ son ideales de $\mathbb{Z}$, entonces todos los ideales de $\mathbb{Z}$ son los $n\mathbb{Z}$. Por otro lado, supongamos que $m, n \in \mathbb{Z}_{\geq 1}$. Entonces

- m divide a n si y solo si $n\mathbb{Z} \subset m\mathbb{Z}$:
  $m|n \iff \exists k \in \mathbb{Z}\ (n = mk) \iff n \in m\mathbb{Z} \iff$ [1] $n\mathbb{Z} \subset m\mathbb{Z}$.
- $(\text{mcd}\{m, n\}) = (m, n)$:
  Antes que nada, recordemos que podemos escribir $\text{mcd}\{m, n\}$ como combinación lineal de m y n en $\mathbb{Z}$. Específicamente, sabemos que existen $a, b \in \mathbb{Z}$ tales que $\text{mcd}\{m, n\} = am + bn$. Entonces,
  $x \in (\text{mcd}\{m, n\}) \iff \exists k \in \mathbb{Z}\ (x = k \cdot \text{mcd}\{m, n\}) \iff \exists k \in \mathbb{Z}\ (x = k(am + bn)) \iff x \in (m, n)$

[1] La implicación "$\Longrightarrow$" es porque $n\mathbb{Z}$ es el ideal mas chico que contiene a n y $m\mathbb{Z}$ es un ideal.

Ideales generados e intersecciones/uniones

Supongamos que R es un anillo y $A, B \subset R$ son subconjuntos de R. Entonces,

1. $(A \cap B) \subset^{2} (A) \cap (B)$ pero la igualdad no es necesariamente cierta: considera los siguientes ideales principales de $\mathbb{Z}$ $(\{2\} \cap \{3\}) = 0$ pero $(2) \cap (3) =^{3} (6)$.
2. $(A) \cup (B) \subset^{4} (A \cup B)$, pero la igualdad no es necesariamente cierta: considera los siguientes ideales principales de $\mathbb{Z}$ $5 \notin (2) \cup (3)$ pero $5 \in \mathbb{Z} = (1) = (\text{mcd}\{2,3\}) =^{5} (2,3) = (\{2\} \cup \{3\})$.
3. $((A) \cup (B)) = (A \cup B)$: La inclusión "$\subset$" es consecuencia inmediata del inciso anterior. La inclusión "$\supset$" es consecuencia inmediata de que $A \cup B \subset^{6} ((A) \cup (B))$.

---

[2] $A \cap B \subset A, B \implies A \cap B \subset (A), (B) \implies (A \cap B) \subset (A), (B)$.

[3] Pronto veremos que en general, $(n) \cap (m) = (\text{mcm}\{n, m\})$.

[4] $A, B \subset A \cup B \implies A, B \subset (A \cup B) \implies (A), (B) \subset (A \cup B)$.

[5] En la siguiente diapositiva veremos que en general, $(m, n) = (\text{mcd}\{m, n\})$.

[6] Pues $A \subset (A) \subset ((A) \cup (B))$ y $B \subset (B) \subset ((A) \cup (B))$

Un ideal izquierdo principal de $M_n(R)$

Supongamos que R es un anillo y $n \in \mathbb{Z}_{\geq 1}$. Recordemos un poco de notación que introdujimos en la sección 1.7.

- Sea $E^n_{pq} = (a_{ij})_{ij} \in M_n(R)$ tal que $a_{pq} = 1$ y $a_{ij} = 0$ si $(i,j) \neq (p,q)$. Entonces, para toda $p, q, r \in \{1, \ldots, n\}$ tenemos $E^n_{pq} \cdot E^n_{qr} = E^n_{pr}$.
- Para cada $k \in \{1, \ldots, n\}$ sea $C^n_k \subset M_n(R)$ el conjunto de todas las matrices que solo tienen entradas no nulas en la k-esima columna. Recordemos que demostramos que C^n_j es un ideal izquierdo de $M_n(R)$ pero *no* es un ideal derecho de $M_n(R)$.

Veamos que $C^n_k = M_n(R)E^n_{mk}$ para cada $m \in \{1, \ldots, n\}$. Primero notemos que como podemos escribir cada $A \in C^n_k$ como una suma de matrices de la forma αE^n_{ik} donde $\alpha \in R$ y $i \in \{1, \ldots, n\}$, entonces basta demostrar que $\alpha E^n_{ik} \in M_n(R)E^n_{mk}$ para toda $\alpha \in R$ y $i \in \{1, \ldots, n\}$. Sin embargo, esto es consecuencia de la siguiente igualad $\alpha E^n_{ik} = (\alpha E^n_{im})(E^n_{mk})$. Por lo tanto, C^n_k es un ideal izquierdo principal de $M_n(R)$ generado por E^n_{mk}, donde $m \in \{1, \ldots, n\}$.

Ideales principales de anillos de funciones

Sea $I := \{f \in \mathbb{R}^{[0,1]} \mid f(\frac{1}{2}) = 0\}$ el ideal de $R^{[0,1]}$. Si $g : \mathbb{R} \to [0,1]$ es tal $g(\frac{1}{2}) = 0$ y $g(x) = 1$ si $x \neq \frac{1}{2}$, entonces $f = f \cdot g$ para toda $f \in I$. Por lo tanto, $I = (g)$. De hecho, cualquier función que sea cero en $\frac{1}{2}$ y distinta de cero en $[0,1] \setminus \{\frac{1}{2}\}$ genera a I.

Sin embargo, si $J := \{f \in \mathcal{C}\left([0,1]\right) \mid f(\frac{1}{2}) = 0\}$ es el ideal de $\mathcal{C}([0,1])$, entonces J no es ni siquiera finitamente generado. Desafortunadamente, la demostración requiere técnicas de análisis y por eso la omitimos.

$R[x]/(x) \cong R$

Proposición 3

Supongamos que R es un anillo conmutativo. Entonces

1. $(x) = \{\text{los polinomios con constante} = 0\}$.
2. $R[x]/(x) \cong R$.

Demostración.

1. $\subset$) Es fácil verificar que $\{\text{los polinomios con constante} = 0\}$ es un ideal de $R[x]$ y como $x \in \{\text{los polinomios con constante} = 0\}$, entonces $(x) \subset \{\text{los polinomios con constante} = 0\}$.

   $\supset$) Supongamos que $p(x)$ tiene constante $= 0$. Es decir, $p(x) =^{7} \sum_{i=1}^{n} a_i x^i$ para algunas $a_i \in R$ y $n \in \mathbb{Z}_{\geq 1}$. Entonces

$$p(x) = \sum_{i=1}^{n} a_i x^i = \left(\sum_{i=1} a_i x^{i-1} \right) x \in (x).$$

[7] Este polinomio tiene termino constante $= 0$ porque estamos empezando la suma en $i = 1$.

2. Supongamos que $\varphi : R[x] \to R$ es tal que

$$p(x) \mapsto p(0) = \text{el termino constante de } p(x)$$

Entonces φ es un homomorfismo suprayectivo y

$$\ker \varphi = \{\text{los polinomios con constante} = 0\} = (x)$$

donde la ultima igualdad se cumple por el inciso anterior. Finalmente, por el primer teorema de isomorfismos

$$R[x]/(x) = R[x]/\ker \varphi \cong \operatorname{im} \varphi = R.$$

□

Un ideal no principal de $\mathbb{Z}[x]$

Veamos que el ideal $(2, x)$ de $\mathbb{Z}$ (generado por los polinomios 2 y x) *no* es principal. Por definición

$$(2, x) = \{2p(x) + xq(x) \mid p(x), q(x) \in \mathbb{Z}[x]\}$$

y por lo tanto, el 0-esimo coeficiente de todo polinomio en $(2, x)$ es un entero par. En particular, $(2, x)$ es un ideal propio. Ahora si, veamos que $(2, x)$ no es principal, suponiendo lo contrario. Es decir, existe $a(x) \in \mathbb{Z}[x]$ tal que $(2, x) = (a(x))$. Como $2 \in (2, x) = (a(x))$, entonces existe $p(x) \in \mathbb{Z}[x]$ tal que $2 = p(x)a(x)$. Entonces[8] $a(x)$ y $p(x)$ son polinomios constantes y como 2 es primo, entonces $a(x), p(x) \in \{\pm 1, \pm 2\}$. En caso de que $a(x)$ fuera ± 1, $(a(x)) = (2, x)$ no seria propio. Por lo tanto, $a(x) = \pm 2$. Como $x \in (2, x) = (a(x))$, entonces existe $q(x) \in \mathbb{Z}[x]$ tal que $x = 2q(x)$. Pero entonces, $q(x) = \frac{1}{2}x$, contradiciendo $q(x) \in \mathbb{Z}[x]$.

[8] De nuevo ocupando que $\deg p(x)q(x) = \deg p(x) + \deg q(x)$ y que $\deg p(x) = 0$ si y solo si $p(x)$ es constante.

Ideales principales en dominios enteros

Proposición 4

Supongamos que R es un dominio entero. Si $a, b \in R$, entonces

$$(a) = (b) \iff a = ub \text{ para alguna } u \in R \text{ invertible.}$$

Demostración.
$\Longrightarrow$) $(a) = (b) \implies a \in (b)$ y $b \in (a) \implies a = ub$ y $b = va$ para algunas $u, v \in R \implies a = ub = u(va) = (uv)a \implies$ [9] $1 = uv$. Análogamente, $vu = 1$. Por lo tanto, u es invertible y como $a = ub$, obtenemos lo deseado.
$\Longleftarrow$) $a = ub$ para alguna $u \in R$ invertible $\implies a \in (b) \implies$ [10] $(a) \subset (b)$. De manera análoga, ocupando la igualdad $b = u^{-1}a$ obtenemos $(b) \subset (a)$. Por lo tanto, $(a) = (b)$. □

[9] Recordemos que en un domino podemos cancelar factores no nulos
[10] Recordemos que (a) es el ideal mas chico que contiene a a.

Anillos que solo tienen ideales triviales

Proposición 5

Supongamos que R es un anillo con 1.

1. Los únicos ideales izquierdos[11] de R son los triviales $\iff$ R es un anillo con división. En particular,
   - "$\Longleftarrow$" implica que los únicos ideales de un campo son los triviales.
   - "$\Longrightarrow$" implica que que si R es conmutativo y sus únicos ideales izquierdos son los triviales, entonces R es un campo.
2. Los únicos ideales bilaterales de R son los triviales $\not\Longrightarrow$ R es un anillo con división.

[11] Podemos cambiar "izquierdos" por "derechos".

Demostración.

1. $\Longrightarrow$) Supongamos que $a \in R \setminus \{0\}$. En particular, $Ra \neq 0$ y por lo tanto, la hipótesis implica que $Ra = R$. En particular, como $1 \neq 0$, entonces existe $b \in R \setminus \{0\}$ tal que $ba = 1$. Por lo tanto, $Rb = R$. En particular, existe $c \in R \setminus \{0\}$ tal que $cb = 1$. Luego,

$$a = 1a = (cb)a = c(ba) = c1 = c$$

Por lo tanto, $ab = 1$ y $ba = 1$. Es decir, todo elemento de R es invertible.
$\Longleftarrow$) Supongamos que $I \neq 0$ es un ideal izquierdo de R. Queremos ver que $I = R$. Recordemos que basta ver que $1_R \in I$. Como $I \neq 0$, existe $a \in I$ distinta de 0. Como R es un anillo con división, existe a^{-1}. Por lo tanto, como I es ideal, $1_R = a^{-1}a \in I$.

2. Antes de presentar el contraejemplo, veamos porque el argumento que ocupamos en el inciso anterior no funciona en este caso: Para obtener el inverso de $a \in R \setminus \{0\}$, ocupábamos la igualdad $Ra = R$ (o $aR = R$) para encontrar $b \in R \setminus \{0\}$ tal que $ba = 1$ o $ab = 1$. Sin embargo, con las hipótesis que tenemos en este caso, tenemos la igualdad $RaR = R$. Por lo tanto, si procediéramos de la misma manera, obtendríamos $r, s \in R \setminus \{0\}$ tales que $ras = 1$. Por obvias razones, ya no podemos continuar de la misma manera.

   Ahora si, veamos el contraejemplo. Para esto, supongamos que F es un campo. Demostraremos que $M_n(F)$ cumple lo deseado. Para esto, recordemos la siguiente notación: Sea $E^n_{pq} = (a_{ij})_{ij} \in M_n(F)$ tal que $a_{pq} = 1$ y $a_{ij} = 0$ si $(i, j) \neq (p, q)$. Una cuenta directa demuestra que E^n_{11} no es invertible y por lo tanto, $M_n(R)$ no tiene división. Resta ver que los únicos ideales bilaterales de $M_n(F)$ son los triviales. Para esto, ocuparemos el siguiente lema.

Lema. Si R es un anillo conmutativo, entonces todo ideal bilateral de $M_n(R)$ es de la forma $M_n(I)$ donde I es un ideal bilateral de R.

Demostración del lema. Antes que nada, fijemos $n \in \mathbb{Z}_{\geq 0}$ y denotemos $E_{pq} \coloneqq E^n_{pq}$. Ocuparemos la siguiente igualdad: Si $A = (a_{ij})_{ij} \in M_n(R)$, entonces

$$E_{kl}AE_{pq} = a_{lp}E_{kq} \text{ para toda } k, l, p, q \in \{1, \ldots, n\} \tag{1.9.1}$$

Ahora bien, sea J un ideal bilateral de $M_n(R)$, necesitamos encontrar un ideal bilateral I de R tal que $J = M_n(I)$. Veamos que
$I \coloneqq \{r \in R \mid rE_{11} \in J\}$ cumple lo deseado. Para ver que I es un ideal bilateral, supongamos que $r \in R$ y $\alpha \in I$, entonces

$$(ra)E_{11} = (rE_{11})(aE_{11}) \in J.$$

Donde la igualdad es consecuencia de una cuenta directa y la pertenencia es consecuencia de que J es ideal. Por lo tanto, $ra \in I$. Análogamente $ar \in I$.

Resta probar que $J = M_n(I)$:

$\subset$) Supongamos que $A = (a_{ij})_{ij} \in J$. Usando (1.9.1) obtenemos $a_{ij}E_{11} = E_{1i}AE_{j1}$ para toda $i, j \in \{1, \ldots, n\}$. Luego, como $A \in J$ y J es ideal bilateral, entonces $E_{1i}AE_{j1} \in J$. Por lo tanto, $a_{ij}E_{11} \in J$. Pero por definicion de I, entonces $a_{ij} \in I$. En otras palabras, todas las entradas de J son elementos de I, es decir, $J \in M_n(I)$.

$\supset$) Supongamos que $A \in M_n(I)$. Es claro que podemos escribir a A como una suma de matrices de la forma αE_{ij} con $\alpha \in I$ y $i, j \in \{1, \ldots, n\}$. Por lo tanto, (como J es ideal) basta probar que $\alpha E_{ij} \in J$ para toda $\alpha \in I$ y toda $i, j \in \{1, \ldots, n\}$:
Si $\alpha \in I$, entonces (por definicion) $\alpha E_{11} \in J$. Luego, (por (1.9.1)) $\alpha E_{ij} = E_{i1}(\alpha E_{11})E_{1j} \in^{12} J$ para toda $i, j \in \{1, \ldots, n\}$. Por lo tanto, $\alpha E_{ij} \in J$ para toda $\alpha \in I$ y toda $i, j \in \{1, \ldots, n\}$.
Fin del lema.

[12] Pues $\alpha E_{11} \in J$ y J es ideal

Usando que los únicos ideales bilaterales de un campo son los triviales, el lema implica que los únicos ideales de $M_n(F)$ son $M_n(0)$ y $M_n(F)$, es decir, los triviales.

En resumen, si F es un campo, entonces $M_n(F)$ solo tiene ideales bilaterales triviales, *pero* $M_n(F)$ no tiene división.

□

Por otro lado, recuerda que en el lema 1.6.7 demostramos el siguiente resultado.

Supongamos que F y F' son campos. Si $\varphi : F \to F'$ es un homomorfismo de anillos tal que $\varphi(1_F) = 1_{F'}$, entonces φ es inyectiva.

Finalizamos esta sección usando la proposición anterior para obtener una generalización de este resultado.

Los homomorfismos de anillos no triviales con dominio igual a un campo son inyectivos

Corolario 6

Supongamos que F es un campo y R es un anillo. Si $\varphi : F \to R$ es un homomorfismo de anillos no trivial, entonces φ es inyectivo.

Demostración. Como φ es un homomorfismo de anillos no trivial, entonces $\ker \varphi \neq F$. Pero como $\ker \varphi$ es un ideal de F, entonces[13] $\ker \varphi = 0$. Por lo tanto, φ es inyectiva. □

[13] Los únicos ideales de un campo son los triviales