Ideales y anillos cociente

Facultad de Ciencias UNAM

Introducción

Supongamos que $\phi : (G, \bullet) \to (G', \bullet')$ es un homomorfismo de grupos. En álgebra moderna 1 vimos que si identificamos a los elementos de G que tienen la misma imagen bajo ϕ, obtenemos un grupo isomorfo a la imagen de ϕ. Específicamente, el primer teorema de isomorfismos (de grupos) nos dice que $G/\ker\phi \cong \operatorname{im}\phi$, donde

1. $G/\ker\phi := \{g \bullet \ker\phi \mid g \in G\}$.
2. $g \bullet \ker\phi$ es la clase de equivalencia de g inducida por la relación $x \sim y \iff \phi(x) = \phi(y)$ o equivalentemente, $x \sim y \iff x - y \in \ker\phi$. De hecho, recordemos que de esta manera, $g \bullet \ker\phi = \{g \bullet x \mid x \in \ker\phi\}$.
3. La operación $\circ$ en $G/\ker\phi$ esta dada por

$$(g \bullet \ker\phi) \circ (h \bullet \ker\phi) := (g \bullet h) \bullet \ker\phi$$

Naturalmente, queríamos generalizar la construcción anterior cambiando cada "$\ker\phi$" por un subgrupo arbitrario "N". Sin embargo, la *única* razón por la que la operación esta bien definida es que $\ker\phi$ satisface la siguiente propiedad:

$$\forall x \in G,\ \forall k \in \ker\phi \left(xkx^{-1} \in \ker\phi\right) \tag{1}$$

Por eso, introducíamos el concepto de subgrupo normal[1]. El objetivo de esta sección es encontrar una construcción análoga para anillos.

[1] Recordemos que la operación en el cociente G/N esta bien definida si y solo si N es normal.

Discusión

Supongamos que R es un anillo y que I es un subgrupo aditivo de R. Como $(R, +_R)$ es un grupo abeliano, $R/I = \left\{r +_R I \mid r \in R\right\}$ es un grupo abeliano con la operación $+$ dada por

$$(r +_R I) + (r' +_R I) = (r +_R r') + I.$$

para toda $r, r' \in R$. Nos gustaría definir una multiplicación en R/I para convertirlo en un anillo. El candidato obvio es

$$(r +_R I) \times (r' +_R I) \coloneqq (r \times_R r') +_R I$$

para toda $r, r' \in R$. Sin embargo, como veremos mas adelante, en general esta operación no está bien definida. Por eso, preguntamos ¿hay una condición para análoga a (1) para anillos? En otras palabras, ¿podemos encontrar condiciones suficientes y necesarias sobre I para que $\times$ este bien definida?

En lo que sigue, omitimos el subíndice de las operaciones de R porque no hay ambigüedad acerca de qué tipo de elementos estamos operando.

Trabajemos de adelante para atrás. Es decir, supongamos que $\times$ esta bien definida. Como para toda $r, r' \in R$ y $\alpha, \alpha' \in I$ (siempre) tenemos

$$r + I = (r + \alpha) + I \quad \text{y} \quad r' + I = (r' + \alpha') + I,$$

entonces el hecho de que $\times$ este bien definida implica que podemos multiplicar estas ecuaciones para obtener

$$(r \times r') + I = \big((r + \alpha) \times (r' + \alpha')\big) + I$$

para toda $r, r' \in R$ y $\alpha, \alpha' \in I$. En particular, si $\alpha = 0 = r'$, entonces

$$I = \big(r \times \alpha'\big) + I$$

Por lo tanto, $r \times \alpha' \in I$ para toda $r \in R$ y $\alpha' \in I$. De manera análoga, poniendo $\alpha' = 0 = r$ obtenemos que $\alpha \times r' \in I$ para toda $r' \in R$ y $\alpha \in I$.

Veamos que estas son las condiciones suficientes que buscamos. Específicamente, supongamos que I es subgrupo aditivo de R tal que

$$\forall r \in R \, \forall \alpha \in I \, (\alpha \times r \in I \quad \text{y} \quad r \times \alpha \in I) \tag{2}$$

y veamos que $\times$ esta bien definida. Supongamos que $r, r', \rho, \rho' \in R$ son tales que

$$r + I = \rho + I \quad \text{y} \quad r' + I = \rho' + I$$

Entonces,

$$\rho = r + \alpha \quad \text{y} \quad \rho' = r' + \alpha' \text{ para algunas } \alpha, \alpha' \in I$$

Queremos ver que

$$(r \times r') + I = \big((r + \alpha) \times (r' + \alpha')\big) + I.$$

Esto es si y sólo si

$$(r \times r') + I = \big((r \times r') + (r \times \alpha') + (\alpha \times r') + (\alpha \times \alpha')\big) + I,$$

y esto es si y sólo si

$$I = \big((r \times \alpha') + (\alpha \times r') + (\alpha \times \alpha')\big) + I,$$

y esto es si y sólo si

$$(r \times \alpha') + (\alpha \times r') + (\alpha \times \alpha') \in I.$$

Pero como I satisface (2), esto es cierto. En resumen, acabamos de demostrar que la multiplicación en el cociente R/I esta bien definida si y sólo si I es un subgrupo aditivo tal que

$$\forall r \in R \; \forall \alpha \in I \, (\alpha \times r \in I \quad \text{y} \quad r \times \alpha \in I)$$

Por eso, introducimos la siguiente definición.

Ideales

Definición

Supongamos que R es un anillo e I es un subgrupo aditivo de R.

- Decimos que I es un **ideal izquierdo** de R si
$$\forall r \in R\, \forall \alpha \in I\, (r \times \alpha \in I)\,.$$
- Decimos que I es un **ideal derecho** de R si
$$\forall r \in R\, \forall \alpha \in I\, (\alpha \times r \in I)\,.$$
- Decimos que I es un **ideal** de R si I es un ideal izquierdo y derecho de R. Cuando es conveniente, a los ideales también les llamamos **ideales bilaterales**.

Observación

- Obviamente, ideal $\implies$ subanillo, pero subanillo $\not\Longrightarrow$ ideal: Por ejemplo, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ pero no es un ideal de $\mathbb{Q}$.
- Para anillos conmutativos, las nociones ideal izquierdo, ideal derecho, e ideal coinciden.
- El kernel de cualquier homomorfismo de anillos es un ideal (c.f. proposición 1.6.4).
- Si R tiene 1 y queremos ver que un subconjunto I de R es ideal, basta demostrar que I es (1) cerrado bajo suma y (2) cerrado bajo multiplicación por todos los elementos de R (no solo los de I). La razón por la que no hace falta ver que I es cerrado bajo resta[2] es que por (2), para toda $a \in I$ tenemos $(-1)a = -a \in I$. Usando (1), tendremos que $b - a \in I$ para toda $a, b \in I$. Es decir, I es un subgrupo aditivo de R.

[2] Recordemos que un ideal es un subgrupo aditivo.

La necesidad del concepto de ideal

Resumimos la discusión inicial en la siguiente proposición.

Proposición 1

Supongamos que R es un anillo e I es un subgrupo aditivo de R. Sean $+$ y $\times$ las operaciones en R/I dadas por

$$(r +_R I) + (s +_R I) := (r +_R s) +_R I$$
$$(r +_R I) \times (s +_R I) := (r \times_R s) +_R I$$

Son equivalentes:

1. I es un ideal bilateral.
2. $\times$ esta bien definida.
3. $(R/I, +, \times)$ es un anillo.

Anillos cociente

Definición

Supongamos que R es un anillo y que I es un ideal bilateral de R. El cociente R/I con las operaciones de la proposición anterior es un anillo llamado el **anillo cociente** R **modulo** I.

Notación

Cuando no haya ambigüedad respecto al ideal I, a veces escribimos

$$\overline{r} := r + I$$

para toda $r \in R$. Con esta notación, las operaciones en R/I se escriben de la siguiente manera.

$$\overline{r} + \overline{s} = \overline{r + s}$$
$$\overline{r} \times \overline{s} = \overline{r \times s}$$

Antes de seguir, cabe recalcar que si I es un ideal izquierdo ó derecho, pero *no* es bilateral, entonces la multiplicación en el cociente *no* esta bien definida. En lo que sigue, damos un ejemplo de esta situación.

Un ideal de $R[x]$

Supongamos que R es un anillo. Sea I el conjunto de todos los polinomios sobre R tales que su 0-esimo coeficiente y su 1-esimo coeficiente son cero. En otras palabras,

$$I := \left\{ a_n x^n + a_{n-1} x^{n-1} + \cdots + a_3 x^3 + a_2 x^2 \mid n \in \mathbb{Z}_{\geq 2} \text{ y } a_i \in R \right\}.$$

I es un ideal de $R[x]$:

Claramente es cerrado bajo suma. Para ver que es cerrado bajo multiplicación basta notar que el producto de dos elementos en I va a ser un polinomio que se ve de la siguiente manera

$$c_{n+m} x^{n+m} + c_{n+m-1} x^{n+m-1} + \cdots + c_5 x^5 + c_4 x^4$$

Por otro lado, notemos que si $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x]$, entonces

$$p(x) + I = (a_1 x + a_0) + I$$

Por lo tanto, un conjunto de representantes de R/I esta dado por los polinomios de la forma $ax + b$, es decir, los polinomios de grado 1.

Finalmente, notemos que si R tiene 1, entonces en R/I tenemos

$$\overline{x} \cdot \overline{x} = \overline{1x} \cdot \overline{1x} = \overline{1x^2} = 0.$$

Por lo tanto, R/I tiene divisores de 0 (independientemente de si R tenga divisores de 0 o no).

Ideales no bilaterales

Supongamos que R es conmutativo y que tiene 1. Para toda $k \in \{1, \ldots, n\}$ sea $C_k^n \subset M_n(R)$ el conjunto de todas las matrices que solo tienen entradas no nulas en la k-esima columna. Es claro que C_k^n es un subgrupo aditivo de $M_n(R)$. Usando la definición de multiplicación de matrices, también es fácil ver que C_k^n es un ideal izquierdo. Sin embargo, C_k^n *no* es ideal derecho. Por ejemplo, veamos el caso $n = 3$, $k = 1$.

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

En general, supongamos que $n \in \mathbb{Z}_{\geq 1}$ y $k \in \{1, \ldots, n\}$ son arbitrarios. 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 $E^n_{pq} \cdot E^n_{qr} = E^n_{pr}$. Por ejemplo, la ecuación anterior se puede escribir como

$$E^3_{31} \cdot E^3_{12} = E^3_{32}$$

Usando esto, notemos que si $r \neq k$, entonces $E^n_{1k} \in C^n_k$ pero $E^n_{1k} \cdot E^n_{kr} = E^n_{1r} \notin C^n_k$. Por lo tanto, C^n_k *no* es un ideal derecho.

De manera análoga, si $F_k \subset M_n(R)$ es el conjunto de todas las matrices que solo tienen entradas no nulas en la k-esima fila, entonces F_k es un ideal derecho, pero *no* es un ideal izquierdo.

Finalmente, veamos que la multiplicación en $M_n(R)/C_k^n$ no esta bien definida. De nuevo, veamos el caso $n = 3$, $k = 1$. Necesitamos encontrar $A, A', B, B' \in M_n(R)$ tales que $\overline{A} = \overline{A'}$ y $\overline{B} = \overline{B'}$ pero $\overline{A \cdot B} \neq \overline{A' \cdot B'}$. Sean

$$A := E_{31}^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad A' := E_{21}^3 = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \text{y}$$

$$B = B' := E_{12}^3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Como $\overline{X} = \overline{Y}$ si y solo si $X - Y \in C_k^3$, entonces $\overline{A} = \overline{A'}$ y $\overline{B} = \overline{B'}$. Por otro lado, usando la identidad de la diapositiva anterior, obtenemos $A \cdot B = E_{32}^3$ y $A' \cdot B' = E_{22}^3$. En particular, $A \cdot B - A' \cdot B' \notin C_k^3$. Por lo tanto, $\overline{A \cdot B} \neq \overline{A' \cdot B'}$. La generalización al caso $n \in \mathbb{Z}_{\geq 1}$ y $k \in \{1, \ldots, n\}$ arbitrarios es sencilla y por eso se la dejamos al lector.

Los ideales triviales

Supongamos que R es un anillo.

- Claramente, los subanillos 0 y R son ideales. A estos anillos les llamamos los **ideales triviales** y si I es un ideal distinto de R, decimos que I es un **ideal propio**.
- Si I es un ideal de R, entonces

$$I = R \iff 1_R \in I.$$

$S/I \cong S$ si $I \cap S = 0$.

Proposición 2

Supongamos que R es un anillo y S es un subanillo de R. Si I es un ideal de R tal que $S \cap I = 0$, entonces $S/I \cong S$, donde $S/I := \{s + I \mid s \in S\}$.

Demostración. Supongamos que $S \cap I = 0$. Recordemos que la proyección canónica $\pi : S \to S/I$ es un homomorfismo suprayectivo. Por lo tanto, para ver que $S \cong S/I$, basta probar que π es inyectiva. Para esto, veamos que $\ker \pi = 0$. Supongamos que $a \in \ker \pi$. Entonces $\pi(a) = 0$ o en otras palabras, $a + I = I$. Pero esto es si y solo si $a \in I$. Finalmente, como a también esta en S, $a \in S \cap I = 0$. Es decir, $a = 0$ y $\ker \pi = 0$. $\square$

La imagen inversa de un ideal bajo un homomorfismo

Proposición 3

Supongamos que $\varphi : R \to R'$ es un homomorfismo de anillos. Si J es un ideal de R', entonces $\varphi^{-1}(J)$ es un ideal de R.

En particular, cuando R es un subanillo de R' y φ es la inclusión $R \hookrightarrow R'$, entonces $J \cap R = \varphi^{-1}(J)$ es un ideal de R. En palabras, la intersección de un subanillo y un ideal es un ideal del subanillo.

Demostración. Sean $a, b \in \varphi^{-1}(J)$ y $r \in R$. Entonces, $\varphi(a), \varphi(b) \in J$ y

$$\varphi(a-b) = \varphi(a) - \varphi(b) \in J \quad \text{y} \quad \varphi(a \times r) = \varphi(a) \times \varphi(r) \in J$$

y análogamente, $\varphi(r \times a) \in J$ (donde las pertenencias se cumplen porque J es un ideal de R'). En otras palabras, $a - b \in \varphi^{-1}(J)$, $a \times r \in \varphi^{-1}(J)$ y $r \times a \in \varphi^{-1}(J)$. Es decir, $\varphi^{-1}(J)$ es un ideal de R.

La imagen directa de un ideal bajo un homomorfismo suprayectivo

Proposición 4

Supongamos que $\varphi : R \to R'$ es un homomorfismo de anillos. Si φ es suprayectiva e I es un ideal de R, entonces $\varphi(I)$ también es un ideal de R'.

Mas aun, la suprayectividad es necesaria. Es decir, existen R, R' anillos, φ no suprayectiva, e I ideal de R tales que $\varphi(I)$ no es un ideal de R'.

Demostración. Sean $x, y \in \varphi(I)$ y $r' \in R'$. Entonces, $x = \varphi(a)$ y $y = \varphi(b)$ para algunas $a, b \in I$ y (como φ es suprayectiva) existe $r \in R$ tal que $r' = \varphi(r)$. Por lo tanto,

$$x + y = \varphi(a) + \varphi(b) = \varphi(a + b) \in \varphi(I)$$
$$x \times r' = \varphi(a) \times \varphi(r) = \varphi(a \times r) \in \varphi(I)$$

y análogamente, $r' \times x \in \varphi(I)$ (donde las pertenencias se cumplen porque I es un ideal de R). Por lo tanto, $\varphi(I)$ es un ideal de R. $\square$

Ideales e isomorfismos de anillos

Proposición 5

Supongamos que $\varphi : R \to R'$ es un isomorfismo de anillos. Si I es un ideal de R, entonces

$$R/I \cong R'/\varphi(I).$$

Demostración. Antes que nada, notemos que como φ es isomorfismo, en particular es φ suprayectivo. Por la proposición anterior, esto implica que $\varphi(I)$ es un ideal de R' y por lo tanto, el cociente $R'/\varphi(I)$ esta bien definido.

Sea

$$\begin{aligned}\Phi : R/I &\to R'/\varphi(I)\\ a+I &\mapsto \varphi(a)+\varphi(I).\end{aligned}$$

Veamos que

- Φ *esta bien definida y es inyectiva*:

$$\begin{aligned} a+I=b+I &\iff a-b\in I\\ &\iff \varphi(a-b)\in\varphi(I) && \text{(pues } \varphi \text{ es iso)}\\ &\iff \varphi(a)-\varphi(b)\in\varphi(I)\\ &\iff \varphi(a)+\varphi(I)=\varphi(b)+\varphi(I)\end{aligned}$$

- Φ *es suprayectiva*: Esto es consecuencia inmediata de la definición de Φ y de que ϕ es suprayectiva.

□