Operaciones de ideales

Facultad de Ciencias UNAM

Introducción

En esta sección introducimos una forma de sumar y multiplicar ideales. Veremos que esta suma y multiplicación gozan muchas de las propiedades que intuitivamente pensaríamos que gozan y también veremos que se llevan muy bien con los ideales generados introducidos en la sección anterior.

Suma y producto de ideales

Definición

Supongamos que R es un anillo y que I, J son ideales de R. Definimos la suma $I + J$, el producto IJ, y la n-esima potencia I^n (con $n \in \mathbb{Z}_{\geq 1}$ por

$$
\begin{aligned}
I + J &:= \{a + b \mid a \in I,\ b \in J\} \\
IJ &:= \{a_1 b_1 + \cdots + a_m b_m \mid m \in \mathbb{Z}_{\geq 1},\ a_k \in I,\ b_k \in J\} \\
I^n &:= \{\text{sumas finitas de elementos de la forma } a_1 a_2 \cdots a_n \mid a_k \in I\} \\
&= \left\{ \sum_{k=1}^{m} a_1^k a_2^k \cdots a_n^k \mid m \in \mathbb{Z}_{\geq 1},\ a_l^k \in I \right\}
\end{aligned}
$$

Observación

Supongamos que R es un anillo y que I, J son ideales de R.

- En general, el conjunto $\{ab \mid a \in I,\ b \in J\}$ no es cerrado bajo suma y por lo tanto, no es necesariamente un ideal.

  Por ejemplo, si $I \subset \mathbb{Z}[x]$ es el ideal que consiste de los polinomios cuyo 0-esimo coeficiente es par, entonces $x^2 + 4 \in^1 I^2$ pero $x^2 + 4 \notin^2 \{p(x)q(x) \mid p(x), q(x) \in I\}$.
- Para $n \in \mathbb{Z}_{\geq 2}$ pudimos haber definido inductivamente $I^1 := I$, $I^n := II^{n-1}$.
- Si $a_1, \ldots, a_n \in R$, entonces

$$R\{a_1, \ldots, a_n\} = Ra_1 + \cdots + Ra_n.$$

[1] Pues $x, 2 \in I$ y por lo tanto, $x^2, 4 \in I^2$.

[2] De lo contrario, existirían $p(x), q(x) \in I$ tales que $x^2 + 4 = p(x)q(x)$ y por lo tanto $\deg p(x) = \deg q(x) = 1$. Luego, $x^2 + 4 = (ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$ para algunas $a, c \in \mathbb{Z}$ y $b, d \in 2\mathbb{Z}$. Por lo tanto, $ac = 1$, $ad + bc = 0$ y $bd = 4$. Sin embargo, es fácil ver que no existen semejantes a, b, c, d.

Operaciones de ideales de $\mathbb{Z}$

Supongamos que $n, m \in \mathbb{Z} \setminus \{0\}$, entonces

- $n\mathbb{Z} + m\mathbb{Z} = \text{mcd}\{n, m\}\mathbb{Z}$:
  Recordemos que en la sección anterior vimos que $\text{mcd}\{n, m\}\mathbb{Z} = (n, m)$. Como $n\mathbb{Z} + m\mathbb{Z} = (n, m)$, obtenemos lo deseado.
- $n\mathbb{Z} \cdot m\mathbb{Z} = (n \cdot m)\mathbb{Z}$:
  $\subset$) Primero notemos que para toda $a \in n\mathbb{Z}$ y toda $b \in m\mathbb{Z}$ tenemos $ab \in (n \cdot m)\mathbb{Z}$. Como $(n \cdot m)\mathbb{Z}$ es un ideal, entonces las sumas finitas de elementos de esta forma también pertenecen a $(n \cdot m)\mathbb{Z}$. Por lo tanto, por definición de producto de ideales, $n\mathbb{Z} \cdot m\mathbb{Z} \subset (n \cdot m)\mathbb{Z}$.
  $\supset$) $x \in (m \cdot n)\mathbb{Z} \implies \exists k \in \mathbb{Z} \setminus \{0\}\ (x = k(n \cdot m)) \implies \exists k, k' \in \mathbb{Z} \setminus \{0\}\ (x = kn \cdot k'm)$ (poniendo $k' = 1$) $\implies x \in n\mathbb{Z} \cdot m\mathbb{Z}$.
- $n\mathbb{Z} \cap m\mathbb{Z} = \text{mcm}\{n, m\}\mathbb{Z}$:
  $x \in n\mathbb{Z} \cap m\mathbb{Z} \iff x$ es múltiplo común de n y $m \iff x$ es múltiplo de $\text{mcm}\{n, m\} \iff x \in \text{mcm}\{n, m\}\mathbb{Z}$.

La relación entre la suma y la unión

Proposición 1

Supongamos que R es un anillo y que I, J son ideales de R.

1. $I + J$ es el ideal de R mas chico que contiene a I y J. En otras palabras, $I + J = (I \cup J)$.
2. Si A, B son subconjuntos de R, entonces $(A \cup B) = (A) + (B)$.

Demostración.

1. Supongamos que I, J son ideales izquierdos y veamos que $I + J = R(I \cup J)$. Los casos en los que I, J son ideales izquierdos o bilaterales son análogos.
   $\subset$) Cualquier ideal que contenga a $I \cup J$ contiene a $I + J$.
   $\supset$) $I + J$ es un ideal que contiene a $I \cup J$.
2. Recordemos que $(A \cup B) = ((A) \cup (B))$ y por el inciso anterior tenemos $((A) \cup (B)) = (A) + (B)$.

La relación entre el producto y la intersección

Proposición 2

Supongamos que R es un anillo y que I, J son ideales de R.

1. IJ esta contenido en $I \cap J$.
2. IJ no necesariamente contiene a $I \cap J$.
3. Si R es conmutativo y $I + J = R$, entonces $IJ = I \cap J$.

Demostración

1. Como I y J son ideales, contienen a todos los elementos de la forma ab con $a \in I$, $b \in J$. Finalmente, como $I \cap J$ es un ideal, contiene a todas las sumas finitas de elementos de esta forma y por lo tanto, contiene a $I + J$.
2. $4\mathbb{Z} \cdot 6\mathbb{Z} = (4 \cdot 6)\mathbb{Z} = 24\mathbb{Z} \subsetneq 12\mathbb{Z} = \text{mcm}\{4, 6\}\mathbb{Z} = 4\mathbb{Z} \cap 6\mathbb{Z}$.
3. Sea $x \in I \cap J$. Como $I + J = R$, entonces existen $a \in I$ y $b \in J$ tales que $x = a + b$. Usando que $x \in I \cap J \subset I$, que $a \in I$, y que I es ideal, obtenemos $b = -a + (a + b) = -a + x \in I$. Análogamente, $a \in J$. Por lo tanto, $x = a + b \in I \cap J$.

$\square$

Aritmética de ideales

Proposición 3

Supongamos que R es un anillo. Si I, J, K son ideales de R, entonces

1. $I(J + K) = IJ + IK$.
2. $I \cap (J + K) = J + (I \cap K)$ si $J \subset I$.

Demostración.

1. Usando las definiciones,

$$
\begin{aligned}
&I(J+K) = \{a_1b_1 + \cdots + a_nb_n \mid a_i \in I,\ b_i \in J+K,\ n \in \mathbb{Z}_{\geq 1}\} = \\
&\{a_1(j_1+k_1) + \cdots + a_n(j_n+k_n) \mid a_i \in I,\ j_i \in J,\ k_i \in K,\ n \in \mathbb{Z}_{\geq 1}\} = \\
&\{a_1j_1 + a_1k_1 + \cdots + a_nj_n + a_nk_n \mid a_i \in I,\ j_i \in J,\ k_i \in K,\ n \in \mathbb{Z}_{\geq 1}\} = \\
&\{(x_1y_1 + \cdots + x_my_m) + (x_1'z_1 + \cdots + x_l'z_l) \mid \\
&\qquad\qquad x_i, x_i' \in I,\ y_i \in J,\ z_i \in K,\ m, l \in \mathbb{Z}_{\geq 1}\} = IJ + IK.
\end{aligned}
$$

   Justifiquemos la cuarta igualdad:
   $\subset$) Podemos poner $m = l = n$; $x_i = x_i' = a_i$; $y_i = j_i$; $z_i = k_i$.
   $\supset$) Podemos poner $n = m + l$; $a_i = x_i$ para $i = 1, \ldots, m$; $a_i = x_i'$ para $i = m+1, \ldots, m+l$; $j_i = 0$ para $i = 1, \ldots, m$; $j_{m+i} = y_i$ para $i = 1, \ldots, l$; $k_i = z_i$ para $k = 1, \ldots, m$; y $k_i = 0$ para $i = m+1, \ldots, m+l$.

2. Antes que nada, recordemos que $J + (I \cap K)$ es el ideal mas chico que contiene a $J \cup (I \cap K) = (J \cup I) \cap (J \cup K) =^3 I \cap (J \cup K)$. En particular, como $I \cap (J + K)$ contiene a $I \cap (J \cup K)$, entonces $J + (I \cap K) \subset I \cap (J + K)$. Para ver la otra inclusión, supongamos que $x \in I \cap (J + K)$. Queremos ver que $x = j + \alpha$ para algunas $j \in J$ y $\alpha \in I \cap K$. Por definición de x, sabemos que $x \in I$ y $x = j + k$ para algunas $j \in J$ y $k \in K$. En particular, como $j \in J \subset I$, entonces

$$k = -j + (j + k) = -j + x \in I$$

Por lo tanto $\alpha \coloneqq k$ cumple lo deseado.

$\square$

[3] Pues $J \subset I$.