Divisibilidad

Facultad de Ciencias UNAM

Introducción

En esta sección generalizamos conceptos de divisibilidad en $\mathbb{Z}$ a un anillo conmutativo arbitrario. Específicamente, generalizaremos los conceptos de máximo común divisor y mínimo común múltiplo.

Divisibilidad

Definición

Supongamos que R es un anillo conmutativo y que $a, b \in R$ con $b \neq 0$.

- Decimos que b **divide a** a **en** R si existe $r \in R$ tal que $a = br$. En este caso escribimos $b|a$ y también decimos que b **es un divisor de** a **en** R o que a **es un múltiplo de** b **en** R.
- Si R es un dominio entero y $b|a$, definimos $\frac{a}{b}$ como el único elemento en R tal que $b \cdot \frac{a}{b} = a$. Cabe recalcar que la unicidad es consecuencia de que R es dominio entero.

Comentario

Cabe recalcar que si el anillo R no esta especificado, la notación $b|a$ es ambigua. En efecto, en $\mathbb{Q}$, $2|3$ pues $2(3/2) = 3$ pero en $\mathbb{Z}$, $2 \nmid 3$ pues no existe $k \in \mathbb{Z}$ tal que $2k = 3$.

A pesar de esto, (por conveniencia) seguiremos ocupando la notación $b|a$, pero es importante tomar en cuenta que el concepto de divisibilidad depende del anillo en donde estemos considerando a los elementos.

De hecho, tomaremos todavía mas libertades: Cuando no haya ambigüedad, simplemente decimos que "b divide a a" en vez de "b divide a a en R".

Finalmente, notemos que el ejemplo al inicio ilustra que esta ambigüedad solo se presenta cuando consideramos el concepto de divisibilidad en un subanillo o en un anillo mas grande.

Observación

Supongamos que R es un dominio entero y que $a, b \in R$ con $b \neq 0$. Si $b|a$, entonces $\frac{a}{b}$ esta bien definido y para toda $c \in R$ tenemos que

$$c\frac{a}{b} = \frac{ca}{b}$$

pues por definición, $\frac{ca}{b}$ es la *única* $x \in R$ que satisface

$$bx = ca$$

y es claro que $c\frac{a}{b}$ también satisface esta igualdad.

Caracterización de divisibilidad en términos de ideales

Proposición 1

Supongamos que R es un anillo conmutativo y que $a, b \in R$ con $b \neq 0$. Son equivalentes:

1. $b|a$
2. $a \in (b)$
3. $(a) \subset (b)$

La demostración es muy sencilla y por eso se la dejamos al lector.

Máximo común divisor

Definición

Supongamos que R es un anillo conmutativo y que $d, x, y \in R$.

- Decimos que d es un **divisor común** de x y y si $d|x$ y $d|y$.
- Decimos que $d \in R \setminus \{0\}$ es un[1] **máximo común divisor** (abreviado **mcd**) de x y y si
  - d es divisor común de x y y.
  - Todo divisor común de x y y también es divisor de d. En otras palabras,

$$\forall d' \in R \left(\left(d'|x \quad \text{y} \quad d'|y \right) \implies d'|d \right).$$

- Supongamos que R tiene 1. Si el $1 \in R$ es mcd de x y y, decimos que x y y son **primos relativos**.

[1] A diferencia del máximo común divisor usual, en general no vamos a poder garantizar la unicidad.

Comentario

Es importante recordar que como el concepto de divisibilidad depende del anillo en donde estemos viendo a los elementos, el concepto de máximo divisor común también depende del anillo. Por ejemplo, seria mas preciso decir que $d \in R \setminus \{0\}$ es un máximo común divisor de x y y en R si

- d divide a x y y en R.
- Todo elemento que divide x y y en R también divide a d en R.

Con esto en mente, continuemos.

Caracterización de divisores comunes en términos de ideales

Proposición 2

Supongamos que R es un anillo conmutativo, que $x, y \in R \setminus \{0\}$, y que $d \in R$. Entonces

1. d es divisor común de x y y si y solo si $(x, y) \subset (d)$.
2. d es un mcd de x y y si y solo si
   - $(x, y) \subset (d)$
   - $\forall d' \in R \setminus \{0\} \left((x, y) \subset (d') \implies (d) \subset (d') \right)$

   En otras palabras, d es un mcd de x y y si y solo si d es generador del ideal principal mas chico que contiene a (x, y).

Demostración.

1. d es un divisor común de x y $y \iff$ [2] $x, y \in (d) \iff (x, y) \subset (d)$.
2. Por el inciso anterior, basta probar que la segunda condición del inciso 2 es equivalente a la segunda condición de la definición de máximo común divisor. Específicamente, basta probar

$$\forall d' \in R \left(\left(d' | x \quad \text{y} \quad d' | y \right) \implies d' | d \right). \tag{1}$$

$$\iff$$

$$\forall d' \in R \setminus \{0\} \left((x, y) \subset (d') \implies (d) \subset (d') \right)$$

   Sin embargo, demostrar esto es cuestión de simplemente reescribir (1) usando el inciso anterior y la caracterización de divisibilidad en términos de ideales.

□

Una consecuencia inmediata del inciso 2 es que si x y y tienen un máximo común divisor d, entonces (d) es el ideal principal mas chico que contiene a x y y. En particular, cualesquiera dos mcd de x y y generan el mismo ideal principal.

[2] Por la caracterización de divisibilidad.

Condiciones suficientes (pero no necesarias) para que un elemento sea un máximo común divisor

Proposición 3

Supongamos que R es un anillo conmutativo y que $d, x, y \in R \setminus \{0\}$.

1. $(x, y) = (d) \implies d$ es un máximo común divisor de x y y.
2. x y y tienen *algún* máximo común divisor $d \not\Longrightarrow (x, y) = (d)$.

Demostración.

1. Como $(x, y) \subset (d)$, entonces d es un divisor común de x y y. Por otro lado, si $d' \in R \setminus \{0\}$ es tal que $(x, y) \subset (d')$, entonces $(d) = (x, y) \subset (d')$. Por la caracterización, d es mcd de x y y.
2. Recordemos que en la sección 1.9 vimos que el ideal $(2, x)$ de $\mathbb{Z}[x]$ no es principal (es decir, no existe $d \in \mathbb{Z}[x]$ tal que $(2, x) = (d)$). Sin embargo, es fácil ver que el $1 \in \mathbb{Z}[x]$ es máximo común divisor de 2 y x.

"Unicidad" de mcd's en dominios enteros

Proposición 4

Supongamos que R es un dominio entero y $x, y \in R$. Si d y d' son mcd de x y y, entonces $d' = ud$ para alguna $u \in R$ invertible.

Demostración. Recordemos que en la sección 1.9 vimos que para cualesquiera $a, b \in R$, $(a) = (b)$ si y solo si $b = vu$ para alguna $v \in R$ invertible. Usando esto obtenemos lo deseado porque si d y d' son mcd de x y y, entonces $(d) = (x, y) = (d')$. $\square$

Mínimo común múltiplo

Definición

Supongamos que R es un anillo conmutativo.

- Si $e, x, y \in R$, decimos que e es un **múltiplo común** (abreviado **mcm**) de x y y si $x|e$ y $y|e$, es decir, e es múltiplo de x y e es múltiplo de y.
- Si $x, y \in R \setminus \{0\}$, decimos que $e \in R$ es un **mínimo común múltiplo** de x y y si
  - e es múltiplo común de x y y.
  - Todo múltiplo común de x y y también es múltiplo de e. En otras palabras,

$$\forall e' \in R \left(\left(x|e' \quad \text{y} \quad y|e' \right) \implies e|e' \right).$$

Caracterización de múltiplos comunes en términos de ideales

Proposición 5

Supongamos que R es un anillo conmutativo, que $x, y \in R \setminus \{0\}$, y que $e \in R$. Entonces

1. e es múltiplo común de x y y si y solo si $(e) \subset (x) \cap (y)$.
2. e es un mcm de x y y si y solo si
   - $(e) \subset (x) \cap (y)$
   - $\forall e' \in R \left((e') \subset (x) \cap (y) \implies (e') \subset (e) \right)$

   En otras palabras, e es un mcm de x y y si y solo si e es generador del ideal principal mas grande que esta contenido en $(x) \cap (y)$.

Demostración.

1. e es un múltiplo común de x y $y \iff x|e$ y $y|e \iff e \in (x)$ y $e \in (y)$ $\iff e \in (x) \cap (y) \iff (e) \subset (x) \cap (y)$.
2. Por el inciso anterior, basta probar que la segunda condición del inciso 2 es equivalente a la segunda condición de la definición de mínimo común múltiplo. Específicamente, basta probar

$$\forall e' \in R \left(\left(x|e' \quad \text{y} \quad y|e' \right) \implies e|e' \right) \tag{2}$$

$$\iff$$

$$\forall e' \in R \left((e') \subset (x) \cap (y) \implies (e') \subset (e) \right)$$

Sin embargo, demostrar esto es cuestión de simplemente reescribir (2) usando el inciso anterior y la caracterización de divisibilidad en términos de ideales.

□

“Unicidad” de mcm’s en dominios enteros

Proposición 6

Supongamos que R es un dominio entero y $x, y \in R$. Si e y e' son mcm de x y y, entonces $e' = ue$ para alguna $u \in R$ invertible.

Demostración. La demostración es análoga a la de “‘Unicidad’ de máximos comunes divisores en dominios enteros” pero usando la caracterización de mínimo común múltiplo en términos de ideales. □

Otra caracterización de los mcm's

Proposición 7

Supongamos que R es un anillo conmutativo y que $e, x, y \in R \setminus \{0\}$. Entonces, e es un mínimo común múltiplo de x y y si y solo si $(x) \cap (y) = (e)$.

Demostración.

$\Longrightarrow$) Supongamos que e es mcm de x y y. Entonces e es múltiplo común de x y y y por la caracterización de múltiplos comunes en términos de ideales, $(e) \subset (x) \cap (y)$. Para ver la otra inclusión, supongamos que $e' \in (x) \cap (y)$. Entonces $(e') \subset (x) \cap (y)$ y por la caracterización de mcm's en términos de ideales, esto implica que $(e') \subset (e)$. En particular, $e' \in (e)$ y por lo tanto, $(x) \cap (y) \subset (e)$.

$\Longleftarrow$) Es consecuencia de que e es un mcm de x y y si y solo si e es generador del ideal principal mas grande que esta contenido en $(x) \cap (y)$.

$\square$

Observación

La proposición anterior muestra una diferencia importante entre los mcd's y los mcm's. Específicamente, hasta antes de la proposición anterior, parecía que había una dualidad perfecta entre el mcm y el mcd:

1. e es un múltiplo común de x y y si y solo si $(e) \subset (x) \cap (y)$.
2. d es un divisor común de x y y si y solo si $(x, y) \subset (d)$.

y

3. e es un mcm de x y y si y solo si e es generador del ideal principal mas grande que esta contenido en $(x) \cap (y)$.
4. d es un mcd de x y y si y solo si d es generador del ideal principal mas chico que contiene a (x, y).

Pero en la proposición anterior, vimos que

5. e es un mcm de x y y si y solo si $(e) = (x) \cap (y)$.

y por lo tanto, tomando en cuenta los incisos (1)-(4), uno esperaría que

6. d es un mcd de x y y si y solo si $(d) = (x, y)$.

Sin embargo, como sabemos esto no es cierto. La razón por la que no podemos modificar la demostración de (5) para obtener una demostración de (6) es la siguiente:

Antes que nada, recordemos que las implicaciones "$\Longleftarrow$" de (5) y (6) son consecuencia inmediata de (3) y (4) respectivamente. Conversamente, las inclusiones $(e) \subset (x) \cap (y)$ y $(x, y) \subset (d)$ son consecuencia inmediata de (1) y (2).

Por lo tanto, para ver (5) resta probar que e mcm $\implies (x) \cap (y) \subset (e)$ y de manera análoga, para ver (6) restaría probar que d mcd $\implies (d) \subset (x, y)$ pero como ya sabemos, esto no es cierto.

Para ver porque e mcm $\implies (x) \cap (y)$ pero d mcd $\not\Longrightarrow (d) \subset (x, y)$ recordemos las caracterizaciones de mcm y mcd en términos de ideales.

e es un mcm de x y y si y solo si

7. $(e) \subset (x) \cap (y)$
8. $\forall e' \in R \left((e') \subset (x) \cap (y) \implies (e') \subset (e) \right)$

y d es un mcd de x y y si y solo si

9. $(x, y) \subset (d)$
10. $\forall d' \in R \setminus \{0\} \left((x, y) \subset (d') \implies (d) \subset (d') \right)$

Ahora si, la razón por la que $(x) \cap (y) \subset (e)$ es cierto y $(d) \subset (x, y)$ no es porque

- Si tomamos $e' \in (x) \cap (y)$ o equivalentemente, $(e') \subset (x) \cap (y)$, podemos inmediatamente hacer uso de (8) para obtener $e \in (e') \subset (e)$.
- En contraste, si tomamos $d' \in (d)$, no podemos usar (10) de la misma manera en la que ocupamos (8).

Cabe recalcar que las dualidades (1) :: (2) y (3) :: (4) se ven todavía mas bonitas si ocupamos la igualdad $(x, y) = (x) + (y)$.

Otras propiedades básicas de divisibilidad

Proposición 8

Supongamos que R es un anillo conmutativo y que $a, b, c \in R$ con $b \neq 0 \neq c$.

1. $b|a \implies cb|ca$
2. $c|b$ y $b|a \implies c|a$.
3. $b|a \implies \frac{b}{d}|\frac{a}{d}$ para todo $d \in R$ tal que $d|a$ y $d|b$.

La demostración es muy sencilla y por eso se la dejamos al lector.

Dividir por el máximo común divisor

Proposición 9

Supongamos que R es dominio entero con 1 y que $a, b \in R \setminus \{0\}$. Si d es un mcd de a y b, entonces el $1 \in R$ es un mcd de $\frac{a}{d}$ y $\frac{b}{d}$.

Demostración. Como obviamente el 1 es divisor común de cualesquiera dos elementos, resta probar la segunda condición de los mcd's de $\frac{a}{d}$ y $\frac{b}{d}$. Para esto, considera las siguiente cadena de implicaciones.

$$
\begin{aligned}
d' \mid \frac{a}{d} \text{ y } d' \mid \frac{b}{d} &\implies dd' \mid a \text{ y } dd' \mid b && \text{(multiplicando por } d\text{)} \\
&\implies dd' \mid d && (d \text{ es mcd de } a \text{ y } b) \\
&\implies d' \mid 1 && \text{(dividiendo por } d\text{)}
\end{aligned}
$$

En resumen, todo divisor común de $\frac{a}{d}$ y $\frac{b}{d}$ es divisor del 1. En otras palabras, el $1 \in R$ satisface la segunda condición de los mcd de $\frac{a}{d}$ y $\frac{b}{d}$. $\square$

Observación

Terminamos esta sección generalizando el concepto de máximo común divisor a una cantidad finita de elementos. Cabe recalcar que todas las propiedades que vimos del máximo común divisor también son satisfechas por esta generalización. La verificación de este hecho es muy sencilla, y por eso se la dejamos al lector.

El máximo común divisor de mas de dos elementos

Definición

Supongamos que R es un anillo conmutativo y que $d, x_1, \ldots, x_n \in R$.

- Decimos que d es un **divisor común de** $x_1, \ldots, x_n$ si $d|x_i$ para toda $i \in \{1, \ldots, n\}$.
- Decimos que $d \in R \setminus \{0\}$ es un **máximo común divisor de** $x_1, \ldots, x_n$ si
  - d es divisor común de $x_1, \ldots, x_n$.
  - Todo divisor común de $x_1, \ldots, x_n$ también es divisor de d. En otras palabras,

$$\forall d' \in R \left(d'|x_i \text{ para toda } i \implies d'|d \right)$$

- Supongamos que R tiene 1. Si el $1 \in R$ es mcd de $x_1, \ldots, x_n$, decimos que $x_1, \ldots, x_n$ son **primos relativos** .