

# Álgebra I

Curso 2020/21



# Índice

<b>1</b>	<b>El lenguaje de los conjuntos</b>	<b>5</b>
1.1	Sobre la teoría axiomática de conjuntos . . . . .	6
1.1.1	Proposiciones y Demostraciones. . . . .	11
1.2	El conjunto producto cartesiano. Aplicaciones . . . . .	15
1.2.1	Imágenes directas e inversas . . . . .	19
1.3	Relaciones de equivalencia. Conjuntos cocientes. . . . .	21
<b>2</b>	<b>Anillos conmutativos</b>	<b>25</b>
2.1	Los anillos $\mathbb{Z}_n$ . . . . .	26
2.2	Generalidades . . . . .	28
2.3	Los anillos de enteros cuadráticos $\mathbb{Z}[\sqrt{n}]$ . . . . .	30
2.4	Múltiplos y potencias naturales . . . . .	32
2.5	Unidades. Cuerpos . . . . .	33
2.6	Múltiplos negativos y potencias de exponente negativo . . . . .	35
2.7	Los anillos de polinomios $A[x]$ . . . . .	37
2.8	Homomorfismos . . . . .	40
<b>3</b>	<b>Congruencias. Ideales y Cocientes</b>	<b>45</b>
3.1	El primer teorema de Isomorfía . . . . .	48
3.2	Operaciones con ideales . . . . .	49
<b>4</b>	<b>Divisibilidad en Dominios de Integridad</b>	<b>51</b>
4.1	Dominios de Integridad . . . . .	51
4.2	El cuerpo de fracciones de un DI . . . . .	53
4.3	Divisibilidad . . . . .	54



## Tema 4

# Divisibilidad en Dominios de Integridad

Ecuaciones sencillas, como  $ax = b$ , con  $a \neq 0$ , no son sencillas de resolver en el contexto de un anillo conmutativo arbitrario (a diferencia de las del tipo  $a + x = b$ , que siempre tiene solución única:  $x = b - a$ ). Si estamos en un cuerpo  $K$  (como  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{Z}_2$ , etc.), tal ecuación siempre tiene solución  $x = ba^{-1}$ , y esta es única. Pero, en general, puede no tener solución (por ejemplo,  $2x = 3$  en  $\mathbb{Z}$ ), y puede tener más de una (por ejemplo,  $2x = 2$  en  $\mathbb{Z}_6$ , tiene dos:  $x = 1$ ,  $x = 4$ ). En lo que sigue, nos centraremos en anillos conmutativos donde las ecuaciones  $ax = b$ , con  $a \neq 0$ , caso de tener solución, esta es única. Estos anillos son los “*Dominios de integridad*”, que presentamos a continuación.

### 4.1 Dominios de Integridad

Un anillo conmutativo no trivial ( $1 \neq 0$ ) es un Dominio de Integridad (DI, para acortar) si en él se verifica la “*propiedad cancelativa*”:

$$\text{Si } a \neq 0, \text{ entonces } ax = ay \Rightarrow x = y.$$

En adelante, los anillos serán supuestos no triviales.

**Proposición 4.1.1.** *Un anillo conmutativo  $A$  es un DI si y solo si el producto de elementos no nulos es no nulo, esto es, si*

$$a \neq 0 \wedge b \neq 0 \Rightarrow ab \neq 0,$$

*o, equivalentemente,*

$$ab = 0 \Rightarrow a = 0 \vee b = 0.$$

*Demostración.*

$\Rightarrow$ ) Si  $ab = 0$ , tendríamos que  $ab = a0$ . Si  $a \neq 0$  tendría que ser  $b = 0$ , al estar en un DI.

$\Leftarrow$ ) Supongamos  $ax = ay$ , con  $a \neq 0$ . Entonces  $a(x - y) = 0$  y será  $x - y = 0$ , es decir que  $x = y$ .

■

**Proposición 4.1.2.**

1. *Cualquier subanillo de un DI es un DI.*
2. *Todo cuerpo es un DI.*

*Demostración.*

1. Si la propiedad cancelativa se verifica para todos los elementos no nulos de un anillo, obviamente se verifica para los de un subanillo suyo.
2. Si  $A$  es cuerpo, todo elemento no nulo es unidad. Si  $a \neq 0$  y  $ax = ay$ , multiplicando por  $a^{-1}$ , obtenemos que  $a^{-1}ax = a^{-1}ay$ , de donde  $x = y$ .

■

EJEMPLOS.

1.  $\mathbb{Z}$ , que es un subanillo de  $\mathbb{Q}$  o de  $\mathbb{R}$ , es un DI. También los anillos  $\mathbb{Z}[\sqrt{n}]$ , que son todos subanillos de  $\mathbb{C}$ , son DI.
2. El anillo  $\mathbb{Z}_4$  no es un DI, pues  $2 \cdot 2 = 0$ .
3. Si  $A$  es un DI, en anillo de polinomios  $A[x]$  es in DI. Para ver esto, introduzcamos una terminología:

- Para un polinomio no nulo  $f(x) = \sum_{m \geq 0} a_m x^m$ , decimos que su “grado” es  $r$ , si  $a_r \neq 0$  y  $a_n = 0$  para todo  $n > r$ .

Si  $g(x) = \sum_{m \geq 0} b_m x^m$  es otro no nulo de grado, digamos  $s$ , entonces los coeficientes del producto en grados  $n > r + s$ ,  $\sum_{i+j=n} a_i b_j$  son todos nulos, pues  $i + j > r + s$  obliga a que bien  $i > r$  o bien  $j > s$ , o sea que  $a_i = 0$  o  $b_j = 0$  en todos los sumandos. Por otra parte, el coeficiente de grado  $r + s$  del producto es  $\sum_{i+j=r+s} a_i b_j = a_r b_s$ , pues si  $i < r$  entonces ha de ser  $j > s$  (para que sumen  $r + s$ ) y entonces  $b_j = 0$ .

Conclusión:

- En general

$$gr(fg) \leq gr(f) + gr(g).$$

Pero puede darse que  $gr(fg) < gr(f) + gr(g)$ : En  $\mathbb{Z}_6[x]$ , sea  $f(x) = 3 + 2x$  y  $g(x) = 3x$ . Entonces  $fg = x$  y  $gr(fg) = 1 < gr(f) + gr(g) = 1 + 1 = 2$ .

Ahora, si el anillo  $A$  es un DI, entonces el coeficiente en grado  $r + s$  de  $fg$  es  $a_r b_s \neq 0$ , pues  $a_r \neq 0$  y  $b_s \neq 0$ . Luego  $fg \neq 0$ , y concluimos que  $A[x]$  es un DI. Además, se da la igualdad

$$gr(fg) = gr(f) + gr(g)$$

para todos los polinomios no nulos  $f, g \in A[x]$ , siempre que  $A$  sea un DI.

Una observación interesante está dada en la siguiente

**Proposición 4.1.3.** *Si  $A$  es un DI finito, entonces es un cuerpo.*

*Demostración.* Sea  $a \in A$ ,  $a \neq 0$ . La aplicación  $f : A \rightarrow A$  definida por  $f(x) = ax$  es inyectiva, y por tanto biyectiva. Luego existe un  $x \in A$  tal que  $ax = 1$ . Esto es,  $a \in U(A)$ .

■

Hemos visto que todo subanillo de un cuerpo es un DI. La relación entre dominios de integridad y cuerpos es mucho más estrecha: todo DI es subanillo de un cuerpo, como vemos a continuación.

## 4.2 El cuerpo de fracciones de un DI

Sea  $A$  un DI. En el conjunto

$$A \times (A \setminus \{0\}) = \{(a, s) \mid a, s \in A, s \neq 0\}$$

establecemos la relación

$$(a, s) \sim (b, t) \Leftrightarrow at = bs.$$

Claramente es reflexiva y simétrica. Para ver que es transitiva, supongamos  $(a, s) \sim (b, t) \sim (c, u)$ , de manera que  $at = bs \wedge bu = ct$ . Entonces,  $atu = bsu = cts$ . Como  $t \neq 0$ , simplificando en la igualdad  $tau = tcs$ , y obtenemos que  $au = cs$ , así que  $(a, s) \sim (c, u)$ .

Consideremos el conjunto cociente  $A \times (A \setminus \{0\}) / \sim$  y denotaremos  $\frac{a}{s}$  a la clase de equivalencia del par  $(a, s)$  (esto es,  $\frac{a}{s} = \overline{(a, s)}$ ). Llamaremos a este elemento “*fracción de numerador  $a$  y denominador  $b$* ”. Entonces,

$$\frac{a}{s} = \frac{b}{t} \Leftrightarrow at = bs.$$

Al conjunto cociente  $A \times (A \setminus \{0\}) / \sim$  le denotaremos por  $\mathbb{Q}(A)$ . Así que

$$\mathbb{Q}(A) = \left\{ \frac{a}{s} \mid a, s \in A, a \neq 0 \right\}.$$

Definimos ahora en  $\mathbb{Q}(A)$  una suma y un producto por

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \quad \frac{a_1}{s_1} \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2},$$

que están bien definidas:

Si  $\frac{a_1}{s_1} = \frac{b_1}{t_1}$  y  $\frac{a_2}{s_2} = \frac{b_2}{t_2}$ , entonces

$$\frac{a_1 s_2 + a_2 s_1}{s_1 s_2} = \frac{b_1 t_2 + b_2 t_1}{t_1 t_2} \text{ y } \frac{a_1 a_2}{s_1 s_2} = \frac{b_1 b_2}{t_1 t_2},$$

pues

$$\begin{aligned} (a_1 s_2 + a_2 s_1) t_1 t_2 &= a_1 s_2 t_1 t_2 + a_2 s_1 t_1 t_2 = b_1 s_1 s_2 + b_2 s_1 s_2 t_1 = (b_1 t_2 + b_2 t_1) s_1 s_2 \text{ y} \\ a_1 a_2 t_1 t_2 &= b_1 s_1 b_2 s_2 = b_1 b_2 s_1 s_2. \end{aligned}$$

Así,  $\mathbb{Q}(A)$  resulta un anillo conmutativo, que además es un cuerpo:

- Su “cero” es  $\frac{0}{1}$  ( $= \frac{0}{s}$ , para cualquier  $s \neq 0$ ).
- El opuesto de una fracción  $\frac{a}{s}$  es  $-\frac{a}{s} = \frac{-a}{s} = \frac{a}{-s}$ .
- Su “uno” es  $\frac{1}{1}$  ( $= \frac{s}{s}$ , para cualquier  $s \neq 0$ ).
- Además, si  $\frac{a}{s} \neq \frac{0}{1}$ , entonces  $a \neq 0$  y  $\frac{s}{a} \in \mathbb{Q}(A)$  y se verifica que  $\frac{a}{s} \frac{s}{a} = \frac{as}{as} = \frac{1}{1}$ . Luego  $(\frac{a}{s})^{-1} = \frac{s}{a}$ .

Al cuerpo  $\mathbb{Q}(A)$  se le llama “el cuerpo de fracciones de  $A$ ”.

Por ejemplo, es claro que  $\mathbb{Q}(\mathbb{Z}) = \mathbb{Q}$  el cuerpo de los números racionales.

En  $\mathbb{Q}(A)$ , una fracción de denominador 1,  $\frac{a}{1}$  está unívocamente determinada por el numerador ( $\frac{a}{1} = \frac{b}{1} \Leftrightarrow a = b$ ), y la representaremos simplemente por el numerador. Esto es, ponemos  $a = \frac{a}{1}$ . De esta forma  $A \subseteq \mathbb{Q}(A)$  como un subanillo. Pero notemos que los elementos  $a$  de  $A$  pueden ser representados en  $\mathbb{Q}(A)$  por las diferentes fracciones equivalentes a  $\frac{a}{1}$ . Así, por ejemplo, en  $\mathbb{Q} = \mathbb{Q}(\mathbb{Z})$ ,  $-2 = \frac{-2}{1} = \frac{6}{-3}$ .

**Observación 4.2.1.** Si  $K$  es un cuerpo, entonces  $K = \mathbb{Q}(K)$ .

En efecto, para cualquier  $\frac{a}{s} \in \mathbb{Q}(K)$ , como  $s \neq 0$ ,  $s^{-1} \in K$  y, entonces,  $as^{-1} \in K$ . Pero  $as^{-1} = \frac{as^{-1}}{1} = \frac{a}{s}$ , luego  $\frac{a}{s} \in K$ .

Esto nos permite utilizar legítimamente la notación de fracciones en cualquier cuerpo:  $as^{-1} = \frac{a}{s}$ . Por ejemplo, en  $\mathbb{R}$ , tenemos que

$$\frac{1}{2} = 2^{-1}, \quad \frac{3}{2} = 3 \cdot 2^{-1}, \quad (\sqrt{2})^{-1} = \frac{1}{\sqrt{2}} = \frac{\sqrt{2}}{2}, \quad \frac{\sqrt{2}}{\sqrt{3}} = \sqrt{2}(\sqrt{3})^{-1}, \text{ etc.}$$

Por ejemplo, es fácil comprobar que todo elemento no nulo de  $\mathbb{Z}_5$  es una unidad, por ejemplo  $3^{-1} = 2$  así podremos escribir

$$2 \cdot 3^{-1} = \frac{2}{3} = 2 \cdot 4.$$

Y esto permite a su vez la siguiente regla operativa para las fracciones en cualquier cuerpo (en  $\mathbb{Q}(A)$ , en particular.)

$$\frac{\frac{a}{s}}{\frac{b}{t}} = \frac{a}{s} \left( \frac{b}{t} \right)^{-1} = \frac{a}{s} \frac{t}{b} = \frac{at}{bs}.$$

**Observación 4.2.2.** Si  $A \subseteq B$ , entonces  $\mathbb{Q}(A) \subseteq \mathbb{Q}(B)$ .

**Observación 4.2.3.** Si  $A \subseteq K$ , donde  $K$  es un cuerpo, entonces  $\mathbb{Q}(A) \subseteq \mathbb{Q}(K) = K$ . Así que, “ $\mathbb{Q}(A)$  es el menor cuerpo que contiene a  $A$ ”.

**Observación 4.2.4.** El cuerpo de fracciones de  $\mathbb{Z}[\sqrt{n}]$  es  $\mathbb{Q}[\sqrt{n}]$ . En efecto, sabemos que  $\mathbb{Q}[\sqrt{n}]$  es un cuerpo y  $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{Q}[\sqrt{n}]$ . Por tanto, el cuerpo de fracciones de  $\mathbb{Z}[\sqrt{n}]$  está contenido en  $\mathbb{Q}[\sqrt{n}]$ . Por otra parte, cualquier cuerpo que contenga a  $\mathbb{Z}[\sqrt{n}]$  contiene a  $\mathbb{Q}[\sqrt{n}]$ , pues al contener a  $\mathbb{Z}$  también contiene a  $\mathbb{Q} = \mathbb{Q}(\mathbb{Z})$ , y entonces a todo número de la forma  $a + b\sqrt{n}$  con  $a, b \in \mathbb{Q}$ , esto es, contiene a  $\mathbb{Q}[\sqrt{n}]$ . En particular, el cuerpo de fracciones de  $\mathbb{Z}[\sqrt{n}]$  contiene a  $\mathbb{Q}[\sqrt{n}]$ .

### 4.3 Divisibilidad

En lo que sigue  $A$  es un DI. El estudio de la ecuación  $ax = b$ , conduce de forma natural a estudiar la relación de “divisibilidad” entre elementos del anillo, que se establece como sigue.

**Definición 4.3.1.** Dados  $a, b \in A$ , decimos que “ $a$  divide a  $b$ ”, situación que representamos por “ $a|b$ ”, o que “ $a$  es un divisor de  $b$ ” o también que “ $b$  es un múltiplo de  $a$ ”, si existe un  $c \in A$  tal que  $ac = b$ .



Esto es,  $a|b$  si la ecuación  $ax = b$  tiene solución, la cual, si  $a \neq 0$ , será necesariamente única, pues  $A$  es un DI.

El caso  $a = 0$ , se discute de forma trivial:

$$0|b \Leftrightarrow b = 0.$$

Esto es, 0 solo es divisor del cero, o, en otras palabras, 0 es el único múltiplo del 0.

Notemos ahora que cuando  $a \neq 0$ , podemos expresar la relación  $a|b$  en términos de  $\mathbb{Q}(A)$ :

$$a|b \Leftrightarrow \frac{b}{a} \in A.$$

En efecto, si  $a|b$ , existirá un  $c \in A$  tal que  $ac = b$ , en cuyo caso  $\frac{b}{a} = \frac{ac}{a} = \frac{c}{1} = c \in A$ . Y recíprocamente, si  $\frac{b}{a} \in A$ , será  $\frac{b}{a} = c = \frac{c}{1}$  para algún  $c \in A$ , en cuyo caso  $b = ac$  y, por tanto,  $a|b$ .

Las siguientes son propiedades elementales de la relación de divisibilidad.

1. (Reflexiva)  $a|a$ .
2. (Transitiva)  $a|b \wedge b|c \Rightarrow a|c$ .
3. Si  $a|b$  y  $a|c$ , entonces  $a|(bx + cy)$ , para todo  $x, y \in A$ .
4. Si  $c \neq 0$ , entonces  $a|b \Leftrightarrow ac|ab$ .

**Observación 4.3.1.** Todos los elementos del anillo dividen a 0, esto es,  $a|0$  para todo  $a \in A$  (pues  $a0 = 0$ ).

**Observación 4.3.2.** Los *divisores de 1* son precisamente los elementos invertibles del anillo, es decir los elementos del conjunto  $U(A)$  de unidades de  $A$ .

EJEMPLOS.

1.  $U(\mathbb{Z}) = \{1, -1\}$ .
2.  $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$ .
3.  $U(A[x]) = U(A)$ . En efecto, es claro que  $U(A) \subseteq U(A[x])$ . Si  $f(x) = \sum_m a_m x^m \in U(A[x])$ , existirá  $g(x) = \sum_m b_m x^m \in A[x]$  tal que  $f(x)g(x) = 1$ . Pero entonces  $gr(f(x)) + gr(g(x)) = 0$ , así que  $gr(f(x)) = 0 = gr(g(x))$ . Esto es,  $f(x) = a_0 \in A$ ,  $g(x) = b_0 \in A$  y  $a_0 b_0 = 1$ . En particular  $f(x) = a_0 \in U(A)$ .
4.  $U(\mathbb{Z}[x]) = \{1, -1\}$ ,  $U(\mathbb{Q}[x]) = \mathbb{Q} - \{0\}$ ,  $U(\mathbb{Z}_3[x]) = \{1, 2\}$ , etc.

**Observación 4.3.3.** Las unidades del anillo son divisores de todos los elementos del anillo: Si  $u \in U(A)$ , entonces para todo elemento  $a$ , se tiene que  $a = a1 = (au^{-1})u$ , así que  $u|a$ . También ocurre que si multiplicamos cualquier elemento  $a$  por una unidad  $u$  el resultado  $ua$  es un divisor de  $a$ , pues  $a = (ua)u^{-1}$ . Así que, para cualquier elemento  $a$ , los elementos del conjunto

$$\{u, ua \mid u \in U(A)\}$$

son siempre divisores de  $a$ , les llamamos los “*divisores triviales*” de  $a$ . Por ejemplo, en  $\mathbb{Z}$ , los divisores triviales del 2 son  $\{1, -1, 2, -2\}$ . En el anillo  $\mathbb{Z}[i]$  de los enteros de Gauss, los divisores triviales de  $1 + i$  son

$$\{1, -1, i, -i, 1 + i, -1 - i, -1 + i, 1 - i\}.$$

**Observación 4.3.4.** Para cada elemento  $a$ , los divisores triviales de la forma  $ua$ , con  $u \in U(A)$ , se llaman “asociados” de  $a$ . Observar que, dada cualquier unidad  $u \in U(A)$ , tenemos que  $u^{-1} \in U(A)$  y  $b = ua \Leftrightarrow a = u^{-1}b$ . Por tanto un elemento  $b$  es asociado de un  $a$  si y solo si este  $a$  es asociado de  $b$ . Hablamos simplemente de que “ $a$  y  $b$  son asociados”.

Estos se pueden caracterizar como sigue.

**Proposición 4.3.2.** Para cualesquiera  $a, b \in A \setminus \{0\}$ , son equivalentes

1.  $a$  y  $b$  son asociados.
2.  $a/b \wedge b/a$ .

*Demostración.* Es claro que si  $a$  y  $b$  son asociados, cada uno es divisor del otro. Recíprocamente, supongamos que  $a$  y  $b$  se dividen mutuamente. Digamos que  $b = ua$  y que  $a = vb$ . Entonces  $a = uva$  y, como  $a \neq 0$ , es  $uv = 1$ . Luego  $u, v \in U(A)$  y  $a$  y  $b$  son asociados. ■

**Definición 4.3.3.** Un elemento  $a \in A$ , se dice que es “irreducible” si no es cero ni unidad y sus únicos divisores son los triviales, esto es, las unidades y sus asociados.

**Proposición 4.3.4.** Un elemento  $a \in A$ , no nulo ni unidad, es irreducible si y solo si se verifica que, dada cualquier factorización suya en producto de dos elementos entonces uno de los factores es una unidad (y entonces el otro un asociado); esto es:

$$a \text{ es irreducible} \Leftrightarrow a = bc, \text{ entonces } b \in U(A) \text{ o } c \in U(A).$$

*Demostración.*

- $\Rightarrow$ ) Supongamos que  $a = bc$  y que  $b, c \notin U(A)$ . Como  $b$  y  $c$  son divisores triviales, ambos serán asociados de  $a$ . Digamos que  $b = ua$  y que  $c = va$ , con  $u, v \in U(A)$ . Entonces  $a = uava = uva^2$ . Como  $a \neq 0$ , será  $1 = (uv)a$ , y concluimos que  $a$  es una unidad, lo que supone una contradicción.
- $\Leftarrow$ ) Supongamos que  $b|a$ . Será  $a = bc$  para un cierto  $c \in A$ . Entonces  $b \in U(A)$  o  $c \in U(A)$ . Si  $b \in U(A)$ ,  $b$  es un divisor trivial. Si  $b \notin U(A)$ , será  $c \in U(A)$ , y por tanto  $b$  un asociado de  $a$ . ■

EJERCICIOS.

1. Argumenta si los siguientes anillos son, o no, Dominios de Integridad:

$$\mathbb{Z}_8, \mathbb{Z}[\sqrt{2}], \mathbb{Z}_3, \mathbb{Z} \times \mathbb{Z}, \mathbb{Z}_6[x], \mathbb{Z}[i], \mathbb{Z}_5[x].$$

2. Es el anillo definido por el conjunto  $\mathbb{Z} \times \mathbb{Z}$  con las operaciones

$$(a, a') + (b, b') = (a + b, a' + b') \text{ y } (a, a')(b, b') = (ab, ab' + a'b),$$

un Dominio de Integridad?

3. ¿Es el anillo definido por el conjunto  $\mathbb{Z}$  de los números enteros con las operaciones  $a \oplus b = a + b - 1$  y  $a \otimes b = a + b - ab$  un Dominio de Integridad? integridad?
4. Se define el cuerpo  $\mathbb{Q}(x)$  como el cuerpo de fracciones del anillo  $\mathbb{Z}[x]$ , esto es  $\mathbb{Q}(x) = \mathbb{Q}(\mathbb{Z}[x])$ . Describe como son sus elementos y sus operaciones.

5. Demuestra que  $\mathbb{Z}[x]$  y  $\mathbb{Q}[x]$  tienen el mismo cuerpo de fracciones. Esto es,

$$\mathbb{Q}(\mathbb{Q}[x]) = \mathbb{Q}(x).$$

6. Sea  $A = \{\frac{m}{2^k} \in \mathbb{Q} \mid m \in \mathbb{Z} \text{ y } k \geq 0\}$ . Argumentar que

- (a)  $A$  es subanillo de  $\mathbb{Q}$ .
- (b)  $\mathbb{Z} \subsetneq A$ .
- (c) El cuerpo de fracciones de  $A$  es el mismo que el de  $\mathbb{Z}$ , o sea  $\mathbb{Q}$ .

7. Argumentar la veracidad o falsedad de las siguientes proposiciones referidas a elementos de un Dominio de Integridad

- (a)  $a \mid b \wedge a \nmid b \Rightarrow b \nmid b + c$ .
- (b)  $a \nmid b \wedge a \nmid c \Rightarrow a \nmid b + c$ .

8. ¿Es la relación “ser divisor de” una relación de orden entre los elementos de un DI?

9. En un Dominio de Integridad  $A$  establecemos la relación  $\sim$  diciendo que  $a \sim b$  si  $a$  es asociado con  $b$ .

- (a) Probar que  $\sim$  es una relación de equivalencia en  $A$ .
- (b) Sea  $A/\sim = \{\bar{a} \mid a \in A\}$ , el correspondiente conjunto cociente. Establecemos entre sus elementos la relación por la cual  $\bar{a} \leq \bar{b}$  si  $a$  es un divisor de  $b$  en el anillo  $A$ . ¿Está bien definida esa relación en  $A/\sim$ ? ¿Es una relación de orden?