Divisibilidad en Dominios de Integridad

Dominios de integridad

Un anillo conmutativo tq $1 \neq 0$ es D.I si se verifica la "propiedad cancelativa"

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

Proposición

A es DI $\Leftrightarrow$ el producto de elementos no nulos es no nulo:

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

$$\Updownarrow$$

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

Proposición

(1) Cualquier subanillo de un DI es un DI.

② Todo cuerpo es un DI.

↳ Todo elemento es unidad $\Rightarrow a \neq 0 \; \forall ax = ay \Rightarrow a^{-1} \cdot ax = a^{-1}ay$

$\Rightarrow x = y$.

[Ejemplos DI pag c].

Proposición

Si A es un DI finito $\Rightarrow$ A es cuerpo.

Demo:

Sea $a \in A$, $a \neq 0$. $f: A \to A$, $x \mapsto ax$ inyectiva y biyectiva pt.

Luego $\exists x \in A$ tq $ax = 1 \Rightarrow a \in U(A)$

Todo DI es subanillo de un cuerpo

El cuerpo de fracciones de un D.I

A DI. En $A \times (A \setminus \{0\}) = \{(a,s) / a, s \in A, s \neq 0\}$

se establece la relación $(a,s) \sim (b,t) \iff at = bs$

Es relación de equivalencia.

Sea el conjunto cociente $A \times (A \setminus \{0\}) / \sim$. Notaremos $\frac{a}{s}$ a la clase de equivalencia de (a,s) $\left(\frac{a}{s} = \overline{(a,s)}\right)$. Este elemento se denomina "fracción de numerador a y denominador s".

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

En conjunto cociente $A \times (A \setminus \{0\}) / \sim$ se denota por $Q(A)$

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

Suma

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

Producto

$$\frac{a_1}{s_1} \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$$

$Q(A)$ es un cuerpo:

- Su cero es $\frac{0}{1}$ $\left(= \frac{0}{s} \; ; s \neq 0 \right)$
- El opuesto de una fracción $\frac{a}{s}$ es $-\frac{a}{s} = \frac{-a}{s} = \frac{a}{-s}$
- Su "uno" es $\frac{1}{1}$ $\left(= \frac{s}{s}, \forall s \neq 0 \right)$
- Además, si $\frac{a}{s} \neq \frac{0}{1} \Rightarrow a \neq 0$, y $\frac{s}{a} \in Q(A)$ y se verifica que $\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{sa} = \frac{1}{1}$. Luego $\left(\frac{a}{s}\right)^{-1} = \frac{s}{a}$

$Q(A)$ = Cuerpo de fracciones de A

En $Q(A)$, $\frac{a}{1} = \frac{b}{1} \iff a = b$; $a = \frac{a}{1} \Rightarrow A \subseteq Q(A)$

Observación

Si K es un cuerpo, entonces $K = Q(K)$

Pues, $\forall \frac{a}{s} \in Q(K)$, como $s \neq 0$, $s^{-1} \in K$ y entonces $a \cdot s^{-1} \in K$

$$a \cdot s^{-1} = \frac{a \cdot s^{-1}}{1} = \frac{a}{s} \in K$$

Regla práctica para cualquier cuerpo (para los fracciones)

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

Observación

Si $A \subseteq B \Rightarrow \mathbb{Q}(A) \subseteq \mathbb{Q}(B)$

Observación

Si $A \subseteq K$, donde K es cuerpo, entonces $\mathbb{Q}(A) \subseteq \mathbb{Q}(K) = K$.

$\mathbb{Q}(A)$ es el menor cuerpo que contiene a A

Observación

El cuerpo de fracciones de $\mathbb{Z}[\sqrt{n}]$ es $\mathbb{Q}[\sqrt{n}]$. $\mathbb{Q}[\sqrt{n}]$ es un cuerpo y $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{Q}[\sqrt{n}]$. Por tanto, el cuerpo de fracciones de $\mathbb{Z}[\sqrt{n}] \subseteq \mathbb{Q}[\sqrt{n}]$. 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 todos números de la forma $a+b\sqrt{n}$, $a,b \in \mathbb{Q}$, es decir, contiene a $\mathbb{Q}[\sqrt{n}]$. El cuerpo de fracciones de $\mathbb{Z}[\sqrt{n}]$ contiene a $\mathbb{Q}[\sqrt{n}]$.

Divisibilidad

Definición (D.I)

Dados $a, b \in A$, decimos que "a divide a b", "$a|b$" ("a es divisor de b", o "b es múltiplo de a"), si $\exists\, c \in A$ tal que $\boxed{ac = b}$.

$a|b$ si $ax = b$ tiene solución, si $a \neq 0$. Será única, al ser $A = DI$.

$a|b \iff b = 0 \Rightarrow$ 0 solo es divisor de cero o cero es el único múltiplo de cero.

Cuando $a \neq 0 \Rightarrow a|b \iff \frac{b}{a} \in A$

Propiedades de la relación de divisibilidad.

Reflexiva $\Rightarrow a|a$

Transitiva $\Rightarrow a|b \wedge b|c \Rightarrow a|c$

Si $a|b$ y $a|c \Rightarrow a|(bx+cy)\ \forall x,y \in A$

Si $c \neq 0 \Rightarrow a|b \iff ac|ab$

Observación

Todos los elementos del anillo dividen a 0. Esto es, $a|0\ \forall a \in A$ pues $a0 = 0$

Observación

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

Observación

Las unidades del anillo son divisores de todos los elementos del anillo.

$\forall u \in U(A)$, $a = a.1 = a.(u^{-1}.u) = (au^{-1})u \Rightarrow \boxed{u|a}$

Además, $\forall a \in A$, $\{u, ua \mid u \in U(A)\}$. Los elementos de este conjunto son los llamados "divisores triviales" de a.

Observación

$\forall a \in A$, los divisores triviales de la forma ua con $u \in U(A)$ se llaman "asociados" de a.

$\forall u \in U(A)$, $u^{-1} \in U(A)$; $b = ua \iff a = u^{-1}b$

Por tanto, un elemento b es asociado de un a $\iff$ a es asociado con b.

Proposición

$\forall a, b \in A \setminus \{0\}$ son t.q:

1. a y b son asociados
2. $a \mid b$ y $b \mid a$

Definición

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

Proposición

Un elemento $a \in A$, no nulo, ni unidad, es irreducible si y sólo 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 es asociado):

a es irreducible $\iff$ $a = bc \Rightarrow b \in U(A)$ o $c \in U(A)$