Números Enteros

Dominios Enteros.

Def. Un sistema algebraico $(D,+,\cdot,0,1)$ se llama anillo conmutativo con identidad si 0 y 1 son elementos distinguidos de D, $+$ y $\cdot$ son operaciones binarias en D, y se satisfacen las condiciones siguientes:

i) $0 \neq 1$.
ii) $\forall x,y \in D$, $x+y=y+x$. (conmutatividad de $+$)
iii) $\forall x,y,z \in D$, $x+(y+z)=(x+y)+z$. (asociatividad de $+$)
iv) $\forall x \in D$, $x+0=x$. (identidad de $+$)
v) $\forall x,y \in D$ $\exists u \in D$ tal que $x+u=y$.
vi) $\forall x,y \in D$, $x\cdot y=y\cdot x$. (conmutatividad de $\cdot$)
vii) $\forall x,y,z \in D$, $x\cdot(y\cdot z)=(x\cdot y)\cdot z$ (asociatividad de $\cdot$)
viii) $\forall x \in D$, $x\cdot 1=x$ (identidad de $\cdot$)
ix) $\forall x,y,z \in D$, $x\cdot(y+z)=x\cdot y+x\cdot z$. (distributividad de $\cdot$ respecto a $+$)

Teorema (4.1.2)

[Unicidad de 0 y 1]. Sea $(D,+,\cdot,0,1)$ un anillo conmutativo con identidad, y sea $v \in D$.
i) Si $x+v=x$ $\forall x \in D$, entonces $v=0$.
ii) Si $x\cdot v=x$ $\forall x \in D$, entonces $v=1$.

Dem.

De (i). Si $x+v=x$ $\forall x\in D$, entonces, particularmente $0+v=0$, por tanto $v+0=0$. Como también, por (iv), $v+0=v$, entonces $v=0$.
De (ii): Si $x\cdot v=x$ $\forall x \in D$ entonces, particularmente $1\cdot v=1$, por tanto $v\cdot 1=1$. Como también, por (viii), $1\cdot v=v$, entonces $v=1$.

q.e.d

Teorema (4.1.3)

[Ley de cancelación]. Si $(D,+,\cdot,0,1)$ es un anillo conmutativo con identidad, entonces $\forall x,y,z \in D$:

$$x+y=x+z \Rightarrow y=z$$

Dem

Sean $x,y,z\in D$ tales que: $x+y=x+z$

Considerando a x y 0, por (v) existe $u\in D$ tal que $x+u=0$. Como:

$$x+y=x+z$$

Entonces:

$$u+(x+y)=u+(x+z)$$

por tanto:

$$(u+x)+y=(u+x)+z$$

por tanto:

$$(x+u)+y=(x+u)+z$$

en consecuencia:

$$0+y=0+z$$

por tanto:

$$y=z$$

q.e.d

Corolario (4.1.4)

Sea $(D,+,\cdot,0,1)$ un anillo conmutativo con identidad y sean $x,y\in D$. El elemento $u\in D$ tal que:

$$x+u=y$$

es único.

Dem

Si también existe $u'\in D$ tal que $x+u'=y$, entonces:

$$x+u'=x+u$$

por el teorema anterior:

$$u'=u$$

q.e.d

Def. Sea $(D,+,\cdot,0,1)$ un anillo conmutativo con identidad.

i) Dados $x,y\in D$, definimos $y-x$ como el único $u\in D$ tal que $x+u=y$, es decir:

$$x+u=y \iff u=y-x$$

ii) Para cada $x\in D$, definimos $-x\in D$ como $0-x$, es decir:

$$-x=0-x$$

obs: a cada par $x,y\in D$ se le asocia un único $y-x\in D$, y a cada $x\in D$ se le asosia un único $-x\in D$

Teorema (4.1.6)

Sea $(D,+,\cdot,0,1)$ un anillo commutativo con identidad. Entonces $\forall\, x,y,u\in D$:

i) $x+(-x)=0$.

ii) $x+u=0 \Rightarrow u=-x$.

iii) $y+(-x)=y-x$.

iv) $y=x \iff y-x=0$.

Dem:

(i) y (ii) son inmediatos de la definición.

De (iii): Puesto que:

$$\begin{aligned} x+(y+(-x)) &= (x+y)+(-x)\\ &= (y+x)+(-x)\\ &= y+(x+(-x))\\ &= y+0\\ &= y. \end{aligned}$$

Como $y-x\in D$ es único tal que:

$$x+(y-x)=y$$

entonces:

$$x+(y+(-x))=x+(y-x)$$

por ley de cancelación:

$$y+(-x)=y-x$$

De (iv): $y=x \iff x=y \iff x+0=y \iff 0=y-x \iff y-x=0$

q.e.d.

Teorema (4.1.7)

Sea $(D,+,\cdot,0,1)$ un anillo conmutativo con identidad. Entonces $\forall\, x \in D$:

$$x \cdot 0 = 0$$

Dem:

Aplicando (iv), tenemos que $\forall\, x \in D$:

$$\begin{aligned} x \cdot 0 + 0 &= x \cdot 0 \\ &= x \cdot (0+0) \\ &= x \cdot 0 + x \cdot 0 \end{aligned}$$

De donde se sigue por ley de cancelación que $x \cdot 0 = 0$.

q.e.d.

Teorema (4.1.8)

Sea $(D,+,\cdot,0,1)$ un anillo conmutativo con identidad. Entonces $\forall\, x,y \in D$:

i) $-x = (-1) \cdot x$

ii) $-(-x) = x$

iii) $x \cdot (-y) = -(x \cdot y)$

iv) $(-x) \cdot y = -(x \cdot y)$

v) $(-x) \cdot (-y) = x \cdot y$

UwU

Dem:

De (i): $\forall\, x \in D$,

$$\begin{aligned} x + (-1) \cdot x &= x \cdot 1 + x \cdot (-1) \\ &= x\,(1+(-1)) \\ &= x \cdot (1-1) \\ &= x \cdot 0 \\ &= 0 \end{aligned}$$

Como también $x + (-x) = 0$ y $-x$ es único con esta propiedad, entonces:

$$-x = (-1) \cdot x$$

De (ii): Como $x + (-x) = 0$, entonces $(-x) + x = 0$, entonces $x = 0 - (-x)$

$$= -(-x)$$

De (iii): $\forall\, x,y \in D$,

$$
\begin{aligned}
x\cdot y + x\cdot(-y) &= x\cdot y + x\cdot((-1)\cdot y)\\
&= x\cdot y + (x\cdot(-1))\cdot y\\
&= x\cdot y + ((-1)\cdot x)\cdot y\\
&= x\cdot y + (-1)\cdot(x\cdot y)\\
&= x\cdot y - (x\cdot y)
\end{aligned}
$$

Luego, por ley de cancelación, $x\cdot(-y) = -(x\cdot y)$.

De (iv): $\forall\, x,y \in D$:

$$
\begin{aligned}
(-x)\cdot y &= y\cdot(-x)\\
&= -(y\cdot x)\\
&= -(x\cdot y)
\end{aligned}
$$

De (v):

Para lo que sigue, $\mathbb{P}$ es el conjunto de los números naturales, junto con sus operaciones, relaciones y elemento distinguido.

Def. Sea S un conjunto y sean $+$ y $\cdot$ operaciones binarias en S. Sea $n \in \mathbb{P}$ y sean $x_1, x_2, \dots, x_n \in S$. Definimos:

i) $\sum_{k=1}^{n} x_k = (\dots((x_1+x_2)+x_3)+\dots)+x_n$

ii) $\prod_{k=1}^{n} x_k = (\dots((x_1 \cdot x_2)\cdot x_3)\cdot\dots)\cdot x_n$

obs: Si $+$ y $\cdot$ son asociativas, se pueden eliminar los paréntesis.

Def. Sea $(D, \oplus, \odot, \mathbf{0}, \mathbf{1})$ un anillo conmutativo con identidad, sean $x \in D$ y $n \in \mathbb{P}$. Definimos:

i) $1x = x$ y $(n+1)x = nx \oplus x$.

ii) $x^1 = x$ y $x^{n+1} = x^n \odot x$.

Nota: $\cdot$ y $+$ son operaciones en $\mathbb{P}$ y, $\odot$ y $\oplus$ lo son en el anillo.

Teorema (4.1.11)

Sea $(D, \oplus, \odot, \mathbf{0}, \mathbf{1})$ un anillo conmutativo con identidad. Si $x, y \in D$ y $m, n \in \mathbb{P}$, entonces:

i) $n\mathbf{0} = \mathbf{0}$.

ii) $nx = \overbrace{x \oplus x \oplus \dots \oplus x}^{n\text{-veces}}$.

iii) $(m+n)x = mx \oplus nx$.

iv) $n(x \oplus y) = nx \oplus ny$.

v) $(m \cdot n)x = m(nx)$.

vi) $n(x \odot y) = (nx) \odot y$.

vii) $n(-x) = -nx$.

viii) $n(x-y) = nx - ny$.

ix) $x^n = \underbrace{x \odot x \odot \dots \odot x}_{n\text{-veces}}$.

x) $x^{m+n} = x^m \odot x^n$.

xi) $x^{m \cdot n} = (x^m)^n$

xii) $0^n = 0$.

xiii) $1^n = 1$.

xiv) $(x \odot y)^n = x^n \odot y^n$

Demi:

De (i):

Def. Un sistema algebraico $(D,+,\cdot,0,1)$ se llama dominio entero, si es anillo conmutativo con identidad, que satisface la siguiente condición: $\forall x,y,z \in D$:

$$[x \neq 0 \ \text{y} \ x\cdot y = x\cdot z] \Rightarrow y = z.$$

Teorema (4.1.13)

Sea $(D,+,\cdot,0,1)$ un anillo conmutativo con identidad. Entonces $(D,+,\cdot,0,1)$ es un dominio entero, si y sólo si, $\forall x,y \in D$:

$$x\cdot y = 0 \Rightarrow x = 0 \ \text{o} \ y = 0.$$

Dem:

a) Suponemos primero que $(D,+,\cdot,0,1)$ es un dominio entero.

Sean $x,y \in D$ tales que $x\cdot y = 0$.

Si $x = 0$, nada hay que probar.

Si $x \neq 0$, entonces:

$$\begin{aligned} x\cdot y &= 0 \\ &= x\cdot 0 \end{aligned}$$

Por ser un dominio entero, aplica la ley de cancelación para el producto. Luego:

$$y = 0.$$

b) Suponemos ahora que $(D,+,\cdot,0,1)$ es un anillo conmutativo con identidad, tal que $\forall x,y \in D$:

$$x\cdot y = 0 \Rightarrow x = 0 \ \text{o} \ y = 0$$

Sean $x,y,z \in D$ tales que $x \neq 0$ y:

$$x\cdot y = x\cdot z$$

entonces $x \neq 0$ y

$$x\cdot y - x\cdot z = 0$$

entonces $x \neq 0$ y

$$x\cdot(y-z) = 0,$$

entonces $y - z = 0$, pues $x \neq 0$, por tanto $y = z$.

q.e.d

4.2 Dominios enteros ordenados.

Def. Un sistema algebraico $(D,+,\cdot,0,1)$ se llama dominio entero simplemente ordenado, si satisface las condiciones siguientes:

i) $(D,+,\cdot,0,1)$ es un dominio entero.

ii) $(D,<)$ es un conjunto simplemente ordenado ($<$ estricotómico y transitivo).

iii) $\forall x,y,z\in D,\ x<y \Rightarrow x+z<y+z$.

iv) $\forall x,y,z\in D,\ [x<y \text{ y } 0<z] \Rightarrow x\cdot z<x\cdot y$.

Def. Sea $(D,+,\cdot,0,1)$ un dominio entero simplemente ordenado.

i) Definimos D^+ como el conjunto:

$$D^+=\{x\in D: 0<x\}$$

ii) Si $(D',+,\cdot,0,1)$ es un subsistema de $(D,+,\cdot,0,1)$, decimos que $(D',+,\cdot,0,1)$ es un subdominio de $(D,+,\cdot,0,1)$.

Teorema (4.2.3)

Si $(D,+,\cdot,0,1)$ es un dominio entero simplemente ordenado, entonces $\forall x,y,z\in D$,

i) $x<y \Leftrightarrow y-x\in D^+$

ii) $x,y\in D^+ \Rightarrow x+y\in D^+$ y $x\cdot y\in D^+$.

iii) $\forall x\in D$ se cumple una y sólo una de las siguientes:

a) $x\in D^+$

b) $x=0$

c) $-x\in D^+$

iv) $x\neq 0 \Rightarrow x^2\in D^+$

v) $1\in D^+$

vi) $x\in D^+$ y $n\in P \Rightarrow nx\in D^+$ y $x^n\in D^+$.

vii) $x\cdot y\in D^+$ y $x\in D^+ \Rightarrow y\in D^+$.

viii) $x+z<y+z \Rightarrow x<y$

ix) $xz<yz$ y $0<z \Rightarrow x<y$.

Dem:

De (i):

$\Rightarrow$) $x<y \Rightarrow x+(-x)<y+(-x) \Rightarrow 0<y-x \Rightarrow y-x\in D^+$.

$\Leftarrow)$ $y-x \in D^+ \Rightarrow 0 < y-x \Rightarrow 0+x < (y-x)+x \Rightarrow x < x+(y-x) \Rightarrow x < y.$