Construcción de los números enteros.

Teorema (4.3.1)

Existe un dominio entero simplemente ordenado $(D, \oplus, \odot, <', \mathbf{0}, \mathbf{1})$ con la propiedad de: $\forall x \in D$, se cumple una y sólo una de los siguientes:

i) $\exists\, n \in P \ \ni\ x = n\mathbf{1}$.

ii) $x = \mathbf{0}$.

iii) $\exists\, m \in P \ \ni\ x = -m\mathbf{1}$.

Dem:

Sea $(P, S_c, +, \cdot, <, 1)$ el sistema de los números naturales. En el conjunto:

$$P \times P = \{(n,m) : n \in P \text{ y } m \in P\}$$

definimos la relación $\sim$ como sigue:

1) $\forall\, (n,m), (p,q) \in P \times P$.

$$(n,m) \sim (p,q) \Leftrightarrow n+q = p+m$$

Como $\sim$ es una relación, $\sim \subset (P\times P) \times (P \times P)$. Probaremos que $\sim$ es de equivalencia.

2) $\sim$ es reflexiva: $\forall\ (n,m) \in P \times P$:

$$n+m = n+m$$

por tanto, $\forall\ (n,m) \in P \times P$: $(n,m) \sim (n,m)$.

3) $\sim$ es simétrica: $\forall\, (n,m), (p,q) \in P \times P$:

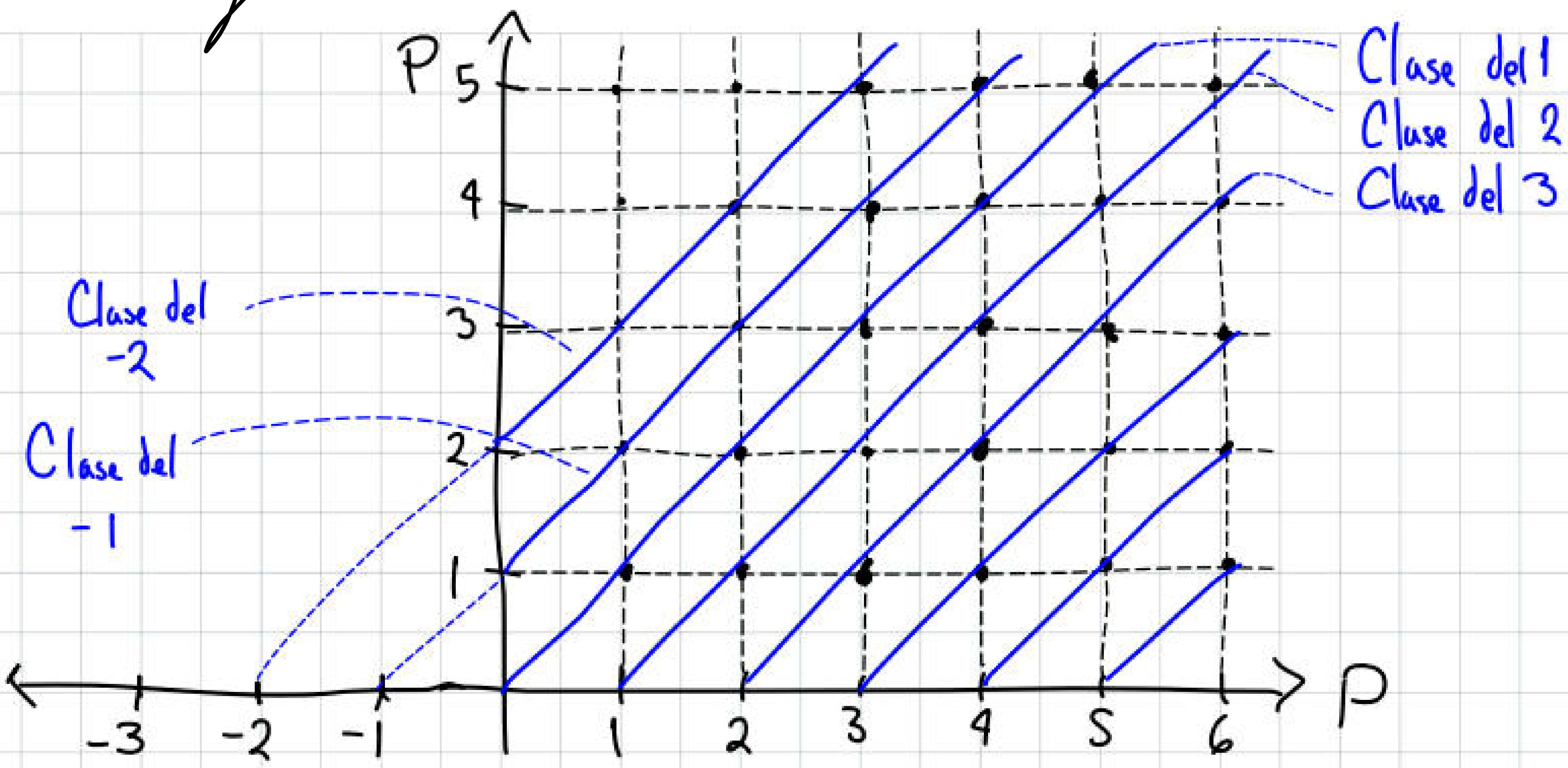
$$(n,m) \sim (p,q) \Rightarrow n+q = p+m \Rightarrow p+m = n+q \Rightarrow (p,q) \sim (n,m)$$

4) $\sim$ es transitiva.

Sean $(n,m), (p,q), (r,s) \in P \times P$, $(n,m) \sim (p,q)$ y $(p,q) \sim (r,s)$

$$\begin{aligned}
&\Rightarrow n+q = p+m \quad y \quad p+s = r+q \\
&\Rightarrow n+q+p+s = p+m+r+q \\
&\Rightarrow n+s+(p+q) = r+m+(p+q) \\
&\Rightarrow n+s = r+m \\
&\Rightarrow (n,m) \sim (r,s)
\end{aligned}$$

Por (2), (3) y (4), $\sim$ es rel. de equivalencia.



Ahora, definimos las siguientes operaciones binarias en $P \times P$:

$\forall (n,m),(p,q) \in P \times P$,

5) $(n,m) \uplus (p,q) = (n+p, m+q)$.

6) $(n,m) * (p,q) = (np+mq, nq+mp)$.

También definimos la sig relación $<$ en $P \times P$:

7) $\forall (n,m),(p,q) \in P \times P$,

$$(n,m) < (p,q) \Leftrightarrow n+q < m+p$$

Probaremos ahora que la relación $\sim$ es compatible con respecto a $\uplus$, $*$ y $<$, es decir, probaremos que $\forall (n,m),(p,q),(n',m'),(p',q') \in P \times P$, se cumplen las propiedades (8), (9) y, (10) siguientes:

8) $[(n,m) \sim (n',m') \text{ y } (p,q) \sim (p',q')] \Rightarrow (n,m) \uplus (p,q) \sim (n',m') \uplus (p',q')$.

En efecto:

$$\begin{aligned}
& (n,m) \sim (n',m') \quad \text{y} \quad (p,q) \sim (p',q') \\
\Rightarrow \;& n+m' = n'+m \quad \text{y} \quad p+q' = p'+q \\
\Rightarrow \;& n+m'+p+q' = n'+m+p'+q \\
\Rightarrow \;& n+p+m'+q' = n'+p'+m+q \\
\Rightarrow \;& (n+p, m+q) \sim (n'+p', m'+q') \\
\Rightarrow \;& (n,m) \uplus (p,q) \sim (n',m') \uplus (p',q')
\end{aligned}$$

9) $(n,m) \sim (n',m')$ y $(p,q) \sim (p',q') \Rightarrow (n,m) * (p,q) \sim (n',m') * (p',q')$

En efecto, observemos que:

$$(n,m) * (p,q) = (np+mq, nq+mp)$$

Y que:

$$(n',m')*(p',q')=(n'p'+m'q',\ n'q'+m'p')$$

así que debemos probar que:

$$(np+mq,\ nq+mp)\sim(n'p'+m'q',\ n'q'+m'p')$$

es decir, que:

$$np+mq+n'q'+m'p'=n'p'+m'q'+nq+mp$$

Procederemos con la prueba:

$$(n,m)\sim(n',m') \quad y \quad (p,q)\sim(p',q')$$
$$\Rightarrow n+m'=n'+m \quad y \quad p+q'=p'+q$$

y por tanto:

$$np+m'p=n'p+mp$$
$$n'q+mq=nq+m'q$$
$$n'p+n'q'=n'p'+n'q$$
$$m'p'+m'q=m'p+m'q'$$

Nota: los que no están en rojo no se cancelan.

por tanto, aplicando ley de la cancelación:

$$np+mq+n'q'+m'p'=mp+nq+n'p'+m'q'$$

por tanto:

$$(np+mq)+(n'q'+m'p')=(n'p'+m'q')+(nq+mp)$$
$$\Rightarrow (np+mq,\ nq+mp)\sim(n'p'+m'q',\ n'q'+m'p')$$

por tanto:

$$(n,m)*(p,q)\sim(n',m')*(p',q')$$

10) $[(n,m)<(p,q) \ y \ (n,m)\sim(n',m') \ y \ (p,q)\sim(p',q')]\Rightarrow(n',m')<(p',q')$.

En efecto:

$$(n,m)<(p,q) \ y \ [(n,m)\sim(n',m') \ y \ (p,q)\sim(p',q')]$$
$$\Rightarrow n+q<m+p \ y \ [n+m'=n'+m \ y \ p+q'=p'+q]$$
$$\Rightarrow n+q+n'+m+p+q'<m+p+n+m'+p'+q$$
$$\Rightarrow (n'+q')+(n+m+p+q)<(m'+p')+(n+m+p+q)$$
$$\Rightarrow n'+q'<m'+p'$$
$$\Rightarrow (n',m')<(p',q')$$

Con $[n,m]$ denotaremos la clase de equivalencia de (n,m) bajo $\sim$, es decir:

$$\begin{aligned}[n,m] &= C_{\sim}(n,m)\\ &= \{(p,q)\in P\times P : (p,q)\sim(n,m)\}\\ &= \{(p,q)\in P\times P : p+m=n+q\}\end{aligned}$$

Sea $D = P\times P/_{\sim} = \{[n,m] : (n,m)\in P\times P\}$

Puesto que $\sim$ es compatible con respecto a $\uplus$, $*$, entonces $\uplus$ y $*$ inducen las siguientes operaciones binarias $\oplus$ y $\odot$ en D:

11) $[n,m]\oplus[p,q] = [(n,m)\uplus(p,q)]$
$$= [n+p, m+q]$$

12) $[n,m]\odot[p,q] = [(n,m)*(p,q)]$
$$= [np+mq, nq+mp]$$

Análogamente, como $\sim$ es compatible con $<$, entonces $<$ induce la siguiente relación $<'$ en D:

13) $[n,m] <' [p,q] \Leftrightarrow (n,m) < (p,q) \Leftrightarrow n+q < m+p$.

Buscamos ahora $\mathbf{0}$ y $\mathbf{1}$ en D, para luego demostrar que:
$$(D,\oplus,\odot,<',\mathbf{0},\mathbf{1})$$
es un dominio entero simplemente ordenado.

14) Definimos $\mathbf{0}=[1,1]$. Es claro que $\forall x\in D$:
$$x\oplus\mathbf{0}=x$$

$x=[p,q]$. Luego: $x\oplus\mathbf{0} = [p,q]\oplus[1,1]$
$$= [p+1,q+1]$$

Buscamos ahora el 1, queremos: $[p,q]\in D$ tal que $\forall [n,m]\in D$:
$$[n,m]\odot[p,q] = [n,m]$$
$$\Leftrightarrow [np+mq, nq+mp] = [n,m]$$
$$\Leftrightarrow (np+mq, nq+mp)\sim(n,m)$$
$$\Leftrightarrow np+mq+m = n+nq+mp$$
$$\Leftrightarrow np+m(q+1) = n(q+1)+mp \quad \ldots \quad (a)$$

Veamos 2 casos, si $n\neq m$, entonces:

$$m<n \text{ o } n<m$$

por tanto:

$$\exists\, u\in P \text{ tal que } n=m+u.$$

o

$$\exists\, v\in P \text{ tal que } m=n+v.$$

Aplicando a), es claro que:

$$(m+u)p+m(q+1)=(m+u)(q+1)+mp$$

o

$$np+(n+v)(q+1)=n(q+1)+(n+v)p$$

entonces:

$$\cancel{mp}+up+\cancel{mq}+\cancel{m}=\cancel{mq}+\cancel{m}+uq+u+\cancel{mp}$$

o:

$$\cancel{np}+\cancel{nq}+\cancel{n}+vq+v=\cancel{nq}+\cancel{n}+\cancel{np}+vp$$

entonces:

$$up=u(q+1) \text{ o } v(q+1)=vp$$

en ambos casos:

$$p=q+1.$$

por tanto, si $n\neq m$, entonces:

$$[n,m]\odot[q+1,q]=[n,m]$$

Si $n=m$, entonces:

$$\begin{aligned}[n,m]\odot[q+1,q]&=[n,n]\odot[q+1,q]\\&=[n(q+1)+nq,\ nq+(q+1)n]\\&=[1,1]\\&=[n,n]\\&=[n,m]\end{aligned}$$

En resumen, $\forall [n,m]\in D$,

$$[n,m]\odot[q+1,q]=[n,m]$$

por tanto, definimos:

15) Definimos $\mathbf{1}=[2,1]$

y se cumple que $\forall\, x\in D$,

$$x\odot \mathbf{1}=x$$

Probaremos ahora que:

$$(D,\oplus,\odot,<',\mathbf{0},\mathbf{1})$$

es un dominio entero simplemente ordenado, es decir, que satisface las siguientes catorce condiciones:

16) $\mathbf{0}\neq\mathbf{1}$.

17) $\forall\, x,y\in D,\ x\oplus y=y\oplus x$.

18) $\forall\, x,y,z\in D,\ x\oplus(y\oplus z)=(x\oplus y)\oplus z$.

19) $\forall\, x\in D,\ x\oplus\mathbf{0}=x$.

20) $\forall\, x,y\in D, \exists\ u\in D$ tal que: $x\oplus u=y$.

21) $\forall\, x,y\in D,\ x\odot y=y\odot x$.

22) $\forall\, x,y,z\in D,\ x\odot(y\odot z)=(x\odot y)\odot z$.

23) $\forall\, x\in D,\ x\odot\mathbf{1}=x$.

24) $\forall\, x,y,z\in D,\ x\odot(y\oplus z)=x\odot y\oplus x\odot z$.

25) $\forall\, x,y\in D$, si $x\odot y=\mathbf{0}$, entonces $x=\mathbf{0}$ o $y=\mathbf{0}$.

26) $\forall\, x,y\in D$, se cumple una y sólo una de las siguientes.

a) $x<'y$.

b) $x=y$.

c) $y<'x$.

27) $\forall\, x,y,z\in D$, si $x<'y$ y $y<'z$, entonces $x<'z$.

28) $\forall\, x,y,z\in D,\ x<'y\Rightarrow x\oplus z<'y\oplus z$.

29) $\forall\, x,y,z\in D$, si $x<'y$ y $\mathbf{0}<'z$, entonces $x\odot z<'y\odot z$.

Prueba de cada inciso.

16) Como $1+1\neq 2+1$, entonces $(1,1)\not\sim(2,1)$, por tanto $[1,1]\neq[2,1]$ y así $\mathbf{0}\neq\mathbf{1}$.

17) $\forall\,[m,n],[p,q]\in D,\ [m,n]\oplus[p,q]=[m+p,n+q]=[p+m,q+n]=[p,q]\oplus[m,n].\ \Delta$

18) $\forall [m,n],[p,q],[r,s]\in D$, $[m,n]\oplus([p,q]\oplus[r,s]) = [m,n]\oplus([p+r,q+s])$
$= [m+(p+r), n+(q+s)] = [(m+p)+r, (n+q)+s] = [m+p, n+q]\oplus[r,s] =$
$([m,n]\oplus[p,q])\oplus[r,s]$.

19)

20) Sean $[n,m],[p,q]\in D$, queremos $[l,K]\in D$ tal que:
$$[n,m]\oplus[l,K] = [p,q]$$
bastará probar que dado $[n,m]\in D$, $\exists [c,d]\in D$ tal que:
$$[n,m]\oplus[c,d] = [1,1]$$
pues en tal caso elegimos
$$[l,K] = [c,d]\oplus[p,q]$$
y se cumple que:
$$\begin{aligned}[n,m]\oplus[l,K] &= [n,m]\oplus([c,d]\oplus[p,q])\\ &= ([n,m]\oplus[c,d])\oplus[p,q]\\ &= [1,1]\oplus[p,q]\\ &= [p,q]\oplus[1,1]\\ &= [p,q].\end{aligned}$$
Probaremos la existencia del $[c,d]$
$$\begin{aligned}&[n,m]\oplus[c,d] = [1,1]\\ \Leftrightarrow\ &[n+c, m+d] = [1,1]\\ \Leftrightarrow\ &(n+c, m+d)\sim(1,1)\\ \Leftrightarrow\ &n+c+1 = 1+m+d\\ \Leftrightarrow\ &n+c = m+d\\ \Leftrightarrow\ &c+n = m+d\\ \Leftrightarrow\ &(c,d)\sim(m,n)\\ \Leftrightarrow\ &[c,d] = [m,n].\end{aligned}$$
Así que, dado $[n,m]\in D$ $\exists [m,n]\in D$ tal que:

$$[n,m]\oplus[m,n]=[1,1]$$

Por notación:

$$[n,m]=-[m,n].$$

21)

Finalmente, resta probar que:

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

i) $\exists\ n\in P \ni x=n\mathbf{1}$.

ii) $x=\mathbf{0}$.

iii) $\exists\ m\in P \ni x=-m\mathbf{1}$.

Afirmamos que:

$$n\mathbf{1}=[n+1,1]$$

es decir, que:

$$n(2,1)=[n+1,1]$$

En efecto, procederemos por inducción sobre n:

a) Si $n=1$:

$$\begin{aligned}1\mathbf{1}&=1[2,1]\\&=[2,1]\\&=[1+1,1]\end{aligned}$$

b) Suponemos el resultado cierto para n, i.e, suponemos que:

$$n\mathbf{1}=[n+1,1]$$

c) Probemos que el resultado es cierto para $n+1$:

$$\begin{aligned}(n+1)\mathbf{1}&=n\mathbf{1}\oplus\mathbf{1}\\&=[n+1,1]\oplus[2,1]\\&=[(n+1)+2,1+1]\\&=[(n+1)+1+1,1+1]\\&=[((n+1)+1)+1,1+1]\end{aligned}$$

y como $(((n+1)+1)+1,1+1)\sim((n+1)+1,1)$, en efecto:

$$((n+1)+1)+1+1=(n+1)+1+1+1$$
$$((n+1)+1)+1+1=((n+1)+1)+1+1$$

así:

$$(n+1)\mathbf{1}=[(n+1)+1,1]$$

Sea ahora $x=[p,q]\in D$, entonces $p,q\in P$ y por tanto, se cumple una y sólo una de las sig:

i) $\exists\ n\in P \ \text{m}\ p=q+n$.

ii) $p=q$.

iii) $\exists\ m\in P\ \text{m}\ q=p+m$.

Entonces, se cumple una y sólo una de:

i) $\exists\ n\in P\ \text{m}\ p+1=n+1+q$.

ii) $p=q$

iii) $\exists\ m\in P\ \text{m}\ p+m+1=1+q$.

Entonces, se cumple una y ...

i) $\exists\ n\in P\ \text{m}: (p,q)\sim(n+1,1)$

ii) $p=q$.

iii) $\exists\ m\in P$ tal que: $(p,q)=(1,m+1)$

Entonces...

i) $\exists\ n\in P\ \text{m}\ [p,q]=[n+1,1]$.

ii) $[p,q]=[1,1]=\mathbf{0}$.

iii) $\exists\ m\in P\ \text{m}\ [p,q]=[1,m+1]$

Por tanto:

i) $\exists\ n\in P$ tal que: $[p,q]=n\mathbf{1}$.

ii) $[p,q]=\mathbf{0}$.

iii) $\exists\ m\in P\ \text{m}\ [p,q]=-[m+1,1]=-m\mathbf{1}$.

q.e.d.

obs: Sea $(D,+,\cdot,<,0,1)$ un dominio entero simplemente ordenado. Definimos:

$$D^{-}=\{x\in D: -x\in D^{+}\}.$$

donde:

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

Por tanto:

$$D^{-}=\{x\in D\mid -x<'0\}$$

para el dominio entero $(D,\oplus,\odot,<',\mathbf{0},\mathbf{1})$ del teorema anterior, dado $x\in D$ se cumple uno y sólo uno de:

i) $\exists\ n\in P\ \text{m}\ x=n\mathbf{1}$.

ii) $x=0$.

iii) $\exists\, m\in P \ni x=-m1$.

afirmamos que

$$D^+=\{n1 \mid n\in P\}$$

En efecto:

$$\begin{aligned}[p,q]\in D^+ &\Leftrightarrow 0<'[p,q]\\ &\Leftrightarrow [1,1]<'[p,q]\\ &\Leftrightarrow (1,1)<'(p,q)\\ &\Leftrightarrow 1+q<1+p\\ &\Leftrightarrow q<p.\\ &\Leftrightarrow \exists\, n\in P \ni \ p=q+n.\\ &\Leftrightarrow [p,q]=[q+n,q]\end{aligned}$$

Puesto que:

$$\begin{aligned}&q+n+1=n+1+q \Leftrightarrow\\ &(q+n,q)\sim(n+1,1)\\ \Leftrightarrow\ &[q+n,q]=[n+1,1] \quad \ldots (2)\end{aligned}$$

Por tanto:

$$[p,q]=[n+1,1]$$

Entonces $0<'[p,q]\Leftrightarrow [p,q]=[n+1,1]=n1$. En consecuencia:

$$D^-=\{-n1 : n\in P\}$$

Puesto que:

$$(P,+,\cdot,<,1)\cong(D^+,\oplus,\odot,<',1),$$

entonces D^+ está bien ordenado por $\leqslant'$, pues P está bien ordenado por $\leqslant$.

Teorema (4.3.2)

Existe un dominio entero simplemente ordenado:

$$(\mathbb{Z},+,\cdot,<,0,1)$$

tal que:

i) $(P, +, \cdot, <, 1)$ es un subsistema de $(\mathbb{Z}, +, \cdot, <, 1)$
ii) $\forall x \in \mathbb{Z}$, se cumple una y sólo una de: $x \in P$ ó $x = 0$ ó $-x \in P$.

Dem:

Sea:

$$(D, \oplus, \odot, <', \mathbf{0}, 1)$$

el dominio entero del teorema (4.3.1). Por el teorema (1.2.5) sabemos que:

$$(P, +, \cdot, <, 1) \cong (D^+, \oplus, \odot, <', 1)$$

donde:

$$D^+ = \{n1 \mid n \in P\}$$

Puesto que $(D^+, \oplus, \odot, <', 1)$ es un subsistema de $(D, \oplus, \odot, <', 1)$, entonces por el teorema (2.3.3) existe un sistema

$$(\mathbb{Z}, +, \cdot, <, 1)$$

que contiene como subsistema a:

$$(P, +, \cdot, <, 1)$$

y tal que:

$$(\mathbb{Z}, +, \cdot, <, 1) \cong (D, \oplus, \odot, <', 1)$$

Sea $H: \mathbb{Z} \to D$ el isomorfismo entre $(\mathbb{Z}, \dots)$ y $(D, \dots)$. Si tomamos $0 \in \mathbb{Z}$ al único elemento tal que $H(0) = \mathbf{0}$, entonces:

$$(\mathbb{Z}, +, \cdot, <, 0, 1) \cong (D, \oplus, \odot, <', \mathbf{0}, 1)$$

En consecuencia, $(\mathbb{Z}, +, \cdot, 0, 1)$ es un dominio entero simplemente ordenado que contiene como subsistema a $(P, +, \cdot, <, 1)$.

Por otro lado, como:

$$\begin{aligned} H(x) \oplus H(-x) &= H(x + (-x)) \\ &= H(0) \\ &= \mathbf{0} \end{aligned}$$

Entonces: $H(-x) = -H(x)$. Por tanto, $\forall x \in \mathbb{Z}$ se cumple una y sólo una de:

1. $H(x) \in D^+$.

2. $H(x)=0$.

3. $-H(x)=H(-x)\in D$

Es decir, $\forall x\in\mathbb{Z}$ se cumple una y sólo una de: $x\in P$ ó $x=0$ ó $-x\in P$.

obs: puesto que:

$$(D^+,<')\cong(P,<)$$

entonces:

$$x\in P\iff H(x)\in D^+\iff 0<'H(x)\iff 0<x\iff x\in\mathbb{Z}^+.$$

entonces:

$$\mathbb{Z}^+=P.$$

nota: el siguiente teorema afirma que $(\mathbb{Z},+,\cdot,<,0,1)$ es único sobre isomorfismos.

Teorema (1.3.3) (caracterización de los enteros)

Sean:

$$(D,+,\cdot,<,0,1)\quad y\quad (D',\oplus,\odot,<',0',1')$$

dominios enteros simplemente ordenados. Si D^+ y D'^+ están bien ordenados por $\leq$ y $\leq'$, respectivamente, entonces:

$$(D,+,\cdot,<,0,1)\cong(D',\oplus,\odot,<',0',1')$$

Dem:

Demostración: Ejercicio [Ver: McCoy, Introduction to modern algebra, 3^{rd} edition, pag 69, 70, 71].

Algunas propiedades de los enteros

Def. Sean $a,b \in \mathbb{Z}$. Decimos que b divide a a ó que a es divisible por b ó que b es un factor de a ó que a es un múltiplo de b, si existe $q \in \mathbb{Z}$ tal que: $a = bq$.

notación: para decir que b divide a a, escribiremos $b|a$. La expresión $b \nmid a$ significa que b no divide a a.

Observemos que:

$$b|a \Leftrightarrow \exists q \in \mathbb{Z} \text{ tal que } a = bq.$$

$$b \nmid a \Leftrightarrow \forall q \in \mathbb{Z},\ a \neq bq.$$

Proposición (4.4.2)

Si $a = bq$ y $b \neq 0$, entonces q es único.

Dem:

Teorema (4.4.3)

i) $b|b \ \forall b \in \mathbb{Z}$.

ii) $b|0,\ \forall b \in \mathbb{Z}$.

iii) $0|a \Leftrightarrow a = 0$.

iv) $1|a,\ \forall a \in \mathbb{Z}$.

v) $b|1 \Leftrightarrow b = \pm 1$.

vi) $b|a$ y $a|b \Rightarrow a = \pm b$.

vii) $b|a$ y $a|c \Rightarrow b|c$.

viii) $b|a \Rightarrow b|ac,\ \forall c \in \mathbb{Z}$.

ix) $b|a$ y $b|c \Rightarrow b|a+c$ y $b|a-c$.

x) $b|a$ y $b|c \Rightarrow b|ar+cs$ y $b|ar-cs$, $\forall\, r,s \in \mathbb{Z}$.

xi) $b|a \Leftrightarrow b|-a \Leftrightarrow -b|a \Leftrightarrow -b|-a$.

xii) $b|a \Leftrightarrow b\,|\,|a| \Leftrightarrow |b|\,|\,a \Leftrightarrow |b|\,|\,|a|$.

Dem:

Teorema (4.4.5)

Si $a,b \in \mathbb{Z}$ y $b \neq 0$, entonces existen $q,r \in \mathbb{Z}$, únicos, tales que:

$$a = bq + r \text{ y } 0 \leq r < |b|.$$

Dem: