DIDACTICA DE LA DIVISIBILIDAD

Antonio González Carlomán

1.- Relación de orden por multiplicación

En el conjunto N de los naturales definimos la relación

$R = \{(x,y) \mid \exists_{x'}(x.x'=y)\}$ $(x'=\frac{y}{x})$

y tal relación es de orden normal

Ya que:

1º.- Es reflexiva

$\forall_x(xRx)$ (el universo es N)

Demostración:

$\forall_x(xRx) \Leftrightarrow \forall_x \exists_{x'}(x.x'=x) \Leftrightarrow \forall_x (x.1=x)$

2º.- Es antisimétrica

$xRy \wedge yRx \Rightarrow x=y$

Demostración:

$xRy \wedge yRx \Rightarrow \exists_{x'}(x.x'=y) \wedge \exists_{y'}(y.y'=x) \Rightarrow \exists_{x',y'}(x.x'=y \wedge x.x'.y'=x) \Rightarrow \exists_{x',y'}(x.x'=y \wedge x'.y'=1) \Rightarrow \exists_{x',y'}(x.x'=y \wedge x'=1 \wedge y'=1) \Rightarrow x=y$

3º.- Es transitiva

$xRy \wedge yRz \Rightarrow xRz$

Demostración:

$xRy \wedge yRz \Rightarrow \exists_{x'}(x.x'=y) \wedge \exists_{y'}(y.y'=z) \Rightarrow \exists_{x',y'}(x.x'.y'=z) \Rightarrow \exists_{x''}(x.x''=z) \Rightarrow xRz$

Para no confundir esta relación de orden normal con la ordenación $\leqslant$ tal que:

$x \leqslant y \Leftrightarrow \exists_{x'}(x+x'=y)$ (orden por suma)

usaremos un signo distinto de "$\leqslant$" que sustituye a R, tal signo podría ser "$\leqslant'$"; pero, siguiendo la costumbre, convenimos que sea el signo "$|$", es decir:

$x|y \Leftrightarrow \exists_{x'}(x.x'=y)$

Para no confundir con el lenguaje común los dos órdenes normales $\leqslant$ y $|$, todavía convenimos lo siguiente:

Si se cumple $a|b$, lo leeremos en vez de "a anterior al elemento b" o "b posterior al elemento a" por "a divide al elemento b" o "b es múltiplo del elemento a"

También convenimos en representar la sección inferior normal del elemento a mediante el orden $|$ por $a^{\cdot}=\{x|x|a\}$ (léase divisores de a), y la sección superior normal del elemento a mediante el orden $|$ por $a_{\cdot}=\{x|a|x\}$ (léase múltiplos de a)

Propiedades:

Siendo $a,b,c,d \in N$, se cumplen:

1.1.- $a^{\cdot}=b^{\cdot} \Rightarrow a=b$

En efecto:

$a^{\cdot}=b^{\cdot} \Rightarrow a \in b^{\cdot} \wedge b \in a^{\cdot} \Rightarrow a|b \wedge b|a \Rightarrow a=b$

1.2.- $a_{\cdot}=b_{\cdot} \Rightarrow a=b$

En efecto:

$a^{\cdot}=b^{\cdot} \Rightarrow a \in b^{\cdot} \wedge b \in a^{\cdot} \Rightarrow b|a \wedge a \not| b \Rightarrow a=b$

1.3.- El número 1 es elemento ínfimo

$\forall_x(1|x)$ $\quad$ $(\forall_x(\frac{x}{1}= x))$

En efecto:

$\forall_x(1|x) \Leftrightarrow \forall_x \exists_{x'}(1.x'=x) \Leftrightarrow \forall_x(1.x=x)$

1.4.- El número 0 es elemento universal

$\forall_x(x|0)$ $\quad$ $(\forall_x(\frac{0}{x}=0))$

En efecto:

$\forall_x(x|0) \Leftrightarrow \forall_x \exists_{x'} (x.x'=0) \Leftrightarrow \forall_x(x.0=0)$

1.5.- Siendo $a \neq 0$

$b|a \Rightarrow b \leqslant a$

En efecto:

$b|a \overset{1}{\Rightarrow} \quad b.b'=a \Rightarrow b \leqslant b.b' \wedge b.b'=a \Rightarrow b \leqslant a$

1.- $b'=\frac{a}{b}$

1.6.- Siendo $a \neq 0$

$b > a \Rightarrow b \nmid a$ (b no divide al elemento a)

En efecto:

Por contrarreciprocidad de 1.5 y ser $\leqslant$ orden total

1.7.- $a|b \wedge a|c \Rightarrow a|b+c$ $\quad$ (si $a|b$ y $a|c$, $\frac{b}{a}+\frac{c}{a}=\frac{b+c}{a}$)

En efecto:

$a|b \wedge a|c \Rightarrow a.a' = b \wedge a.a'' = c \Rightarrow a.(a'+a'') = b+c \overset{1}{\Rightarrow} a.a''' = b+c \Rightarrow a|b+c$

1.- $a'+a'' = a'''$

1.8.- Siendo $c \leq b$

$a|b \wedge a|c \Rightarrow a|b-c$ (si $a|b$ y $a|c$, $\frac{b}{a} - \frac{c}{a} = \frac{b-c}{a}$)

En efecto:

$a|b \wedge a|c \Rightarrow a.a' = b \wedge a.a'' = c \Rightarrow a.(a'-a'') = b-c \Rightarrow a.a''' = b-c \Rightarrow a|b-c$

1.9.- $a|a.b$ ($\frac{a.b}{a} = b$)

En efecto:

$a|a.b \Leftrightarrow a.b = a.b$

1.10.- Isotonía particular respecto a la multiplicación

$a|b \Rightarrow a.c|b.c$ (si $a|b$, $\frac{b}{a} = \frac{b.c}{a.c}$)

En efecto:

$a|b \Rightarrow a.a' = b \Rightarrow a.c.a' = b.c \Rightarrow a.c|b.c$

1.11.- Isotonía general respecto a la multiplicación

$a|b \wedge c|d \Rightarrow a.c|b.c \wedge b.c|b.d \Rightarrow a.c|b.d$

1.12.- Regularidad respecto a la multiplicación

Siendo $c \neq 0$

$a.c|b.c \Rightarrow a|b$ (si $a.c|b.c$, $\frac{b.c}{a.c} = \frac{b}{a}$)

En efecto:

$a.c|\, b.c \rightarrow a.c.a' = b.c \rightarrow a.a'.c = b.c \rightarrow a.a' = b \rightarrow a|\, b$

1.13.- El orden $\nmid$ no es total

$$\neg \Psi_{x,y}(x|\, y \ V\ y|\, x)$$

En efecto:

$a>1 \rightarrow a \nmid a+1 \wedge a+1 \nmid a$

Ya que:

a) $a>1 \rightarrow a \nmid a+1$

Demostrémoslo en forma contrarrecíproca

$a|\, a+1 \rightarrow a \leq 1$

Demostración:

$a|\, a+1 \rightarrow a|\, a+1 \wedge a|\, a \overset{1}{\rightarrow} a|\, 1 \overset{2}{\rightarrow} a \leq 1$

1. Por 1.8
2. Por 1.5

b) $a>1 \rightarrow a+1 \nmid a$

Demostración:

$a>1 \rightarrow a+1>a \overset{1}{\rightarrow} a+1 \nmid a$

1.- Por 1.6

1.14.- El orden | es supsemirreticular (A.I-VII-10.6)

Dados dos elementos cualesquiera $a,b \in N$, existe un elemento, que representaremos por M(a,b), que es mínimo entre los mayorantes del conjunto {a,b} (que es múltiplo común de a y b, y divisor de cualquier múltiplo común de a y b)

$a \mid M(a,b)$, $b \mid M(a,b)$ y $a \mid c \wedge b \mid c \Rightarrow M(a,b) \mid c$

En efecto:

a) Si $a=0$ ó $b=0$, $M(a,b)=0$

Demostración:

$a \mid M(a,b)$ $(a \mid 0)$, $b \mid M(a,b)$ $(b \mid 0)$ y además

$a \mid c \wedge b \mid c \Rightarrow c=0 \Rightarrow 0 \mid c \Rightarrow M(a,b) \mid c$

b) Si $a \neq 0$ y $b \neq 0$, $M(a,b)$ coincide con el mínimo respecto al orden $\leqslant$ del conjunto no vacío $a^{\cdot} \cap b^{\cdot} - \{0\}$ $(a.b \in a^{\cdot} \cap b^{\cdot} - \{0\})$

Demostración:

$a \mid M(a,b)$, $b \mid M(a,b)$ y además

$a \mid c \wedge b \mid c \overset{1}{\Rightarrow} c \in a^{\cdot} \cap b^{\cdot} \wedge c = M(a,b).c' + r \wedge r < M(a,b) \overset{2}{\Rightarrow} c = M(a,b).c' \Rightarrow M(a,b) \mid c$

1.- Siendo c' y r respectivamente cociente y resto entero por defecto de c entre $M(a,b)$

2.- Al dividir los elementos a y b al elemento c y al elemento $M(a,b).c'$, entonces a y b dividen al elemento r(1.8); luego, por ser $r \in a^{\cdot} \cap b^{\cdot}$ y definición de $M(a,b)$, sería $r=0$

A este elemento $M(a,b)$, evidentemente único, le llamamos mínimo común múltiplo de a y b

1.15.- El orden $\mid$ es infsemirreticular (A.I-VII-10.7)

Dados dos elementos cualesquiera $a,b \in N$, existe un elemento, que representaremos por $D(a,b)$, que es máximo entre los minorantes del conjunto $\{a,b\}$ (que es divisor común de a y b, y múltiplo de cualquier divisor común de a y b)

$D(a,b) \mid a$, $D(a,b) \mid b$ y $c \mid a \wedge c \mid b \Rightarrow c \mid D(a,b)$

En efecto:

a) Si $a=0$ y $b=0$, $D(a,b)=0$

Demostración:

$D(a,b)|a \quad (0|0)$, $D(a,b)|b \quad (0|0)$ y además

$c|a \wedge c|b \Rightarrow c|0 \Rightarrow c|D(a,b)$

b) Si $a\neq 0$ ó $b\neq 0$, $D(a,b)$ coincide con el máximo respecto al orden $\leqslant$ del conjunto no vacío y mayorado $a^{\cdot}\cap b^{\cdot}$ ($1\in a^{\cdot}\cap b^{\cdot}$ y a ó b lo mayoran respecto a $\leqslant$)

Demostración:

$D(a,b)|a$, $D(a,b)|b$ y además

$c|a \wedge c|b \overset{1}{\Rightarrow} M(c,D(a,b))|a \wedge M(c,D(a,b))|b \overset{2}{\Rightarrow} M(c,D(a,b)) \leqslant D(a,b) \wedge D(a,b) \leqslant M(c,D(a,b)) \Rightarrow M(c,D(a,b))=D(a,b) \Rightarrow c|D(a,b)$

1.- Por ser a y b múltiplos comunes de c y $D(a,b)$

2.- Por definición de $D(a,b)$ y por 1.5 $(D(a,b)|M(c,D(a,b)))$

A este elemento $D(a,b)$, evidentemente único, le llamamos máximo común divisor de a y b

Si $D(a,b)=1$, diríamos que a y b son primos entre sí

1.16.- El orden $|$ es reticular (A.I-VII-10.8)

En efecto:

Por 1.14 y 1.15

1.17.- $a.D(b,c)=D(a.b,a.c)$

En efecto:

1º.- Si $a=0$

$a.D(b,c)=0.D(b,c)=0=D(0,0)=D(0.b,0.c)=D(a.b,a.c)$

2º.- Si $a\neq 0$

a) $a.D(b,c)\mid D(a.b,a.c)$

Demostración:

Sabemos que $D(b,c)\mid b$, $D(b,c)\mid c$ y además

$D(b,c)\mid b \wedge D(b,c)\mid c \overset{1}{\Rightarrow} a.D(b,c)\mid a.b \wedge a.D(b,c)\mid a.c \Rightarrow a.D(b,c)\mid D(a.b,a.c)$

1.- Por 1.10

b) $D(a.b,a.c)\mid a.D(b,c)$

Demostración:

Sabemos que $a\mid a.b$, $a\mid a.c$ y además

$a\mid a.b \wedge a\mid a.c \Rightarrow a\mid D(a.b,a.c) \Rightarrow a.a'=D(a.b,a.c) \Rightarrow a.a'=D(a.b,a.c)\wedge a.a' \mid a.b \wedge a.a' \mid a.c \overset{1}{\Rightarrow} a.a'=D(a.b,a.c)\wedge a'\mid b\wedge a'\mid c \Rightarrow a.a'=D(a.b,a.c)\wedge a'\mid D(b,c) \Rightarrow a.a'=D(a.b, a.c)\wedge a.a'\mid a.D(b,c) \Rightarrow D(a.b,a.c)\mid a.D(b,c)$

1.- Por 1.12

1.18.- $a\mid b.c \wedge D(a,b)=1 \Rightarrow a\mid c$

Si un número divide a un producto de dos factores y es primo con uno de ellos, divide al otro factor

En efecto:

$a\mid b.c \wedge D(a,b)=1 \overset{1}{\Rightarrow} a\mid a.c \wedge a\mid b.c \wedge D(a.c,b.c)=c \Rightarrow a\mid c$

1.- Por 1.17

1.19.- $D(a,b).a'=a \wedge D(a,b).b'=b \Rightarrow D(a',b')=1$

Los cocientes de dividir dos números entre su máximo común divisor son primos entre sí

En efecto:

$D(a,b).a'=a \wedge D(a,b).b'=b \Rightarrow D(D(a,b).a',\ D(a,b).b')=D(a,b) \overset{1}{\Rightarrow} D(a,b).D(a',b')=D(a,b) \Rightarrow D(a',b')=1$

1.- Por 1.17

1.20.- $M(a,b).D(a,b)=a.b$

En efecto:

1º.- Si $a=0$ ó $b=0$

$M(a,b).D(a,b)=0.D(a,b)=0=a.b$

2º.- Si $a \neq 0$ y $b \neq 0$

a) $M(a,b).D(a,b) \mid a.b$

Demostración:

Sabemos que $a \mid a.(b:D(a,b))$, $b \mid (a:D(a,b)).b$ y además

$a \mid a.(b:D(a,b)) \wedge b \mid (a:D(a,b)\}.b \Rightarrow a \mid (a.b):D(a,b) \wedge b \mid (a.b):D(a,b) \Rightarrow M(a,b) \mid (a.b):D(a,b) \Rightarrow M(a,b).D(a,b) \mid a.b$

b) $a.b \mid M(a,b).D(a,b)$

Demostración:

Sabemos que $a.(M(a,b):a)=b \cdot (M(a,b):b)$ y además

$a.(M(a,b):a)=b.(M(a.b):b) \Rightarrow D(a,b).(a:D(a,b)).(M(a,b):a)=D(a,b).(b:D(a,b)).(M(a,b):b) \Rightarrow (a:D(a,b)).(M(a,b):a)=(b:D(a,b)).(M(a,b):b) \overset{1}{\Rightarrow} a:D(a,b) \mid M(a,b):b \Rightarrow a \mid (M(a,b):b).D(a,b) \Rightarrow a.b \mid M(a,b).D(a,b)$

1.- Por 1.18 y 1.19

1.21.- $a=b.c+d \Rightarrow D(a,b)=D(b,d)$

En efecto:

$a=b.c+d \overset{1}{\Rightarrow} \forall_x (x|\ a \wedge x|\ b \leftrightarrow x|\ b \wedge x|\ d) \Rightarrow \forall_x (x|\ D(a,b) \leftrightarrow x|\ D(b,d)) \Rightarrow \forall_x (x \in D(a,b) \overset{\cdot}{\leftrightarrow} x \in D(b,d)\overset{\cdot}{)} \Rightarrow D(a,b) \overset{\cdot}{=} D(b,d) \overset{\cdot}{\overset{2}{\Rightarrow}} D(a,b)=D(b,d)$

1.- Por 1.7, 1.8 y 1.9

2.- Por 1.1

1.22.- $c|\ a.b \Leftrightarrow \exists_{x,y} (c=x.y \wedge x|\ a \wedge y|\ b)$

En efecto:

1º.- $c|\ a.b \Rightarrow \exists_{x,y} (c=x.y \wedge x|\ a \wedge y|\ b)$

Demostración:

a) Si $c=0$

$c|\ a.b \Rightarrow 0|\ a.b \Rightarrow 0=a.b \Rightarrow c=a.b \wedge a|\ a \wedge b|\ b \Rightarrow \exists_{x,y} (c=x.y \wedge x|\ a \wedge y|\ b)$

b) Si $c \neq 0$

$c|\ a.b \Rightarrow \exists_{x,y} (c=x.y \wedge x=D(c,a) \wedge x.y|\ x.(a:x).b) \overset{1}{\Rightarrow} \exists_{x,y} (c=x.y \wedge x=D(c,a) \wedge y|\ (a:x).b) \overset{2}{\Rightarrow} \exists_{x,y} (c=x.y \wedge x|\ a \wedge y|\ b)$

1.- Por 1.12, ya que $x \neq 0$

2.- Por 1.18, ya que $D(a:x,y)=1$ (1.19)

2º.- $\exists_{x,y} (c=x.y \wedge x|\ a \wedge y|\ b) \Rightarrow c|\ a.b$ (1.11)

1.23.- $D(c,b)=1 \Rightarrow D(a.c,b)=D(a,b)$

En efecto:

Supuesto $D(c,b)=1$

$D(a.c,b) :=D(a,b) :$ (1.1)

Demostración:

$x\in D(a.c,b) :\Leftrightarrow x|\ D(a.c,b)\Leftrightarrow x|\ a.c\wedge x|\ b\Leftrightarrow \exists_{y,z}\ (x=y.z\wedge y|\ a\wedge z|\ c)\wedge x|\ b\overset{1}{\Leftrightarrow}\exists_{y,z}$ --- $(x=y.z\wedge y|\ a\wedge z=1)\wedge x|\ b\Leftrightarrow x|\ a\wedge x|\ b\Leftrightarrow x|\ D(a,b)\Leftrightarrow x\in D(a,b) :$

1.- Por lo supuesto, ya que $z|\ c$ y $z|\ b$; luego $z|\ D(c,b)$

1.24.- $D(b,c)=1\Rightarrow D(a,b.c)=D(a,b).D(a,c)$

En efecto:

Supuesto $D(b,c)=1$

$D(a,b.c) :=(D(a,b).D(a,c)) :$

Ya que:

a) $x\in D(a,b.c) :\Rightarrow x\in(D(a,b).D(a,c)) :$

Demostración:.

$x\in D(a,b.c) :\Rightarrow x|\ D(a,b.c)\Rightarrow x|\ a\wedge x|\ b.c\Rightarrow x|\ a\wedge\exists_{y,z}(x=y.z\wedge y|\ b\wedge z|\ c)\Rightarrow\exists_{y,z}(x=y.z$ - $\wedge\ y|\ a\wedge y|\ b\wedge\ z|\ a\wedge z|\ c)\Rightarrow\ \exists_{y,z}(x=y.z\wedge y|\ D(a,b)\wedge\ z|\ D(a,c))\overset{1}{\Rightarrow}\ x|\ D(a,b).D(a,c)\Rightarrow$ - $x\in(D(a,b).D(a,c)) :$

1.- Por 1.11

b) $x\in(D(a,b).D(a,c)) :\Rightarrow x\in D(a,b.c) :$

Demostración:

$x\in(D(a,b).D(a,c)) :\Rightarrow x|\ D(a,b).D(a,c)\Rightarrow\exists_{y,z}(x=y.z\wedge y|\ D(a,b)\wedge\ z|\ D(a,c))\Rightarrow\exists_{y,z}$ $(x=y.z\wedge\ y|\ a\wedge y|\ b\wedge z|\ c\wedge z|a)\Rightarrow\ \exists_{y,z}(x=y.z\wedge\ y|\ z.(a:z)\wedge\ y|\ b\wedge z|\ c)\overset{1}{\Rightarrow}\ \exists_{y,z}(x=y.z\wedge$ $y|\ a:z\wedge x|\ b.c)\Rightarrow x|\ a\wedge x|\ b.c\Rightarrow x|\ D(a,b.c)\Rightarrow x\in D(a,b.c) :$

1.- Por 1.18, ya que $D(y,z)=D(b,c)=1$

1.25.- $a.M(b,c)=M(a.b,a.c)$

En efecto:

$a.M(b,c) \overset{1}{=} a.((b.c):D(b,c))=(a.b.c):D(b,c)=(a.b.a.c):(a.D(b,c)) \overset{2}{=} ((a.b).-(a.c)):D(a.b,a.c)=M(a.b,a.c)$

1.- Por 1.20

2.- Por 1.17

2.- Inducción del orden reticular | a operaciones con estructura reticular.

El orden reticular | en N (1.16), induce unas operaciones con estructura reticular en N(A.I-X-7) que son las operaciones internas binarias μ y δ definidas de la siguiente manera:

Dados cualesquiera $a,b \in N$

$a\mu b=M(a,b)$

$a\delta b=D(a,b)$

Se cumplirían entonces (A.I-X-5), siendo $a,b,c \in N$

A_1.- $a\mu a=a$	A'_1.- $a\delta a=a$
A_2.- $a\mu b=b\mu a$	A'_2.- $a\delta b=b\delta a$
A_3.- $a\mu(b\mu c)=(a\mu b)\mu c$	A'_3.- $a\delta(b\delta c)=(a\delta b)\delta c$
A_4.- $a\mu(a\delta b)=a$	A'_4.- $a\delta(a\mu b)=a$

Propiedades:

Aparte de las propiedades anteriores se cumplirían, siendo $a,b,c \in N$, las siguientes:

2.1.- La estructura reticular es distributiva (A.I-X-9.1)

1.- $a\mu(b\delta c) = (a\mu b)\delta(a\mu c)$

2.- $a\delta(b\mu c) = (a\delta b)\mu(a\delta c)$

En efecto:

Demostración de 1-

$a\mu(b\delta c) \overset{1}{=} a\delta b\delta c.a'\mu(b'\delta c') \overset{2}{=} a\delta b\delta c.a'.(b'\delta c') \overset{3}{=} a\delta b\delta c.\ a'.(b':a'\delta b')\delta c' \overset{4}{=} -$
$a\delta b\delta c.a'.(b':a'\delta b')\delta(c':a'\delta c') \overset{5}{=} a\delta b\delta c.(a'.b':a'\delta b')\delta(a'.c':a'\delta c') \overset{6}{=} a\delta b\delta c.$
$(a'\mu b')\delta(a'\mu c') \overset{7}{=} (a\mu b)\delta(a\mu c)$

1.- Por 1.17 y 1.25, siendo $a=(a\delta b\delta c).a'$, $b=(a\delta b\delta c).b'$ y $c=(a\delta b\delta c)c'$ (suponemos que . separa más fuerte que δ y μ)

2.- Por 1.20, ya que $a'\delta b'\delta c'=1$, pues $a\delta b\delta c=(a\delta b\delta c).(a'\delta b'\delta c')$

3.- Por ser $(a'\delta b')\delta c'=1$ (1.23)

4.- Por ser $(b':a'\delta b')\delta(a'\delta c') \overset{*}{=} b'\delta(a'\delta c')=a'\delta b'\delta c'=1$ (1.23)
* Por ser $(a'\delta b')\delta(a'\delta c')=a'\delta b'\delta c'=1$

5.- Por 1.17

6.- Por 1.20

7.- Por 1.17 y 1.25

Demostración de 2.-

$a\delta(b\mu c)=a\delta b\delta c.a'\delta(b'\mu c') \overset{1}{=} a\delta b\delta c.a'\delta(b'\delta c'.b''\mu c'') \overset{2}{=} a\delta b\delta c.a'\delta(b''.c'') \overset{3}{=} a\delta b$
$\delta c.\ a'\delta b''.a'\delta c'' \overset{4}{=} a\delta b\delta c.((a'\delta b'')\mu(a'\delta c'') \overset{5}{=} a\delta b\delta c.(a'\delta((b'\delta c').b''))\mu(a'\delta$
$((b'\delta c').c''))= a\delta b\delta c.(a'\delta b')\mu(a'\delta c')=(a\delta b)\mu(a\delta c)$

1.- Por 1.25, siendo $b'=(b'\delta c').b''$ y $c'=(b'\delta c').c''$

2.- Por ser $a'\delta(b'\delta c')=1$(1.23) y $b''\delta c''=1$ (1.20)

3.- Por ser $b''\delta c''=1$ (1.24)

4.- Por ser $(a'\delta b'')\delta(a'\delta c'')= a'\delta(b''\delta c'')=a'\delta 1=1$ (1.20)

5.- Por ser $a'\delta(b'\delta c')=1$(1.23)

2.2.- La estructura reticular tiene elemento ínfimo (A-I-X-9.2)

$1 \mu a = a$ (A.I-X-9.2.1)

$1 \delta a = 1$ (A.I-X-9.2.2)

En efecto:

Ya que el retículo tiene al elemento 1 como ínfimo (1.3)

2.3.- La estructura reticular tiene elemento universal (A.I-X-9.3)

$a \mu 0 = 0$ (A.I-X-9.3.1)

$a \delta 0 = a$ (A.I-X-9.3.2)

En efecto:

Ya que el retículo tiene al elemento 0 como universal (1.4)

2.4.- No simetrización en μ salvo el 1

$a \mu b = 1 \Rightarrow a = 1 \Lambda b = 1$

En efecto:

$a \mu b = 1 \Rightarrow a \mid 1 \Lambda b \mid 1 \Rightarrow (a \mid 1 \Lambda 1 \mid a) \Lambda (b \mid 1 \Lambda 1 \mid b) \Rightarrow a = 1 \Lambda b = 1$

2.5.- No simetrización en δ salvo el 0

$a \delta b = 0 \Rightarrow a = 0 \Lambda b = 0$

En efecto:

$a \delta b = 0 \Rightarrow 0 \mid a \Lambda 0 \mid b \Rightarrow (0 \mid a \Lambda a \mid 0) \Lambda (0 \mid b \Lambda b \mid 0) \Rightarrow a = 0 \Lambda b = 0$

3.- Números primos

Dado un conjunto natural N, llamamos números primos de él a los pertenecientes al conjunto P siguiente:

$P=\{x|\ x^{\cdot}=\{1,x\}\}$ (los que sólo son divisibles por si mismo y por 1)

Los números no pertenecientes al conjunto P (no primos)les llamamos compuestos.

Evidentemente $1\in P$ y $0\notin P$

Propiedades:

Siendo $a,b,c,m,n\in N$, se cumplen

3.1.- $P-\{1\}\neq\emptyset$

En efecto:

$2\in P-\{1\}$, pues $2^{\cdot}=\{1,2\}$

Ya que:

$x\in 2^{\cdot}\Rightarrow x|\ 2\Rightarrow x|\ 2\wedge x\leq 2\Rightarrow x=1\vee x=2\Rightarrow x\in\{1,2\}$

3.2.- $a\in P\wedge a\nmid b\Rightarrow a\delta b=1$

En efecto:

$a\in P\wedge a\nmid b\Rightarrow a^{\cdot}=\{1,a\}\wedge a\notin b^{\cdot}\Rightarrow a^{\cdot}\cap b^{\cdot}=\{1\}\Rightarrow a\delta b=1$

3.3.- Siendo $a\in P$

$a|\ b.c\Rightarrow a|\ b\vee a|\ c$

En efecto:

$a|\ b.c\overset{1}{\Rightarrow}\exists_{x,y}(a=x.y\wedge x|\ b\wedge y|\ c\wedge(x=a\ \vee\ x=1))\Rightarrow\exists_{x,y}(a=x.y\wedge x|\ b\wedge x=a)\vee\exists_{x,y}(a=x.y\wedge y|\ c\wedge x=1)\Rightarrow a|\ b\ \vee\ a|\ c$

1.- Por 1.22 y cumplirse que $x|\ a$

3.4.- Siendo $a,b \in P$, $a \neq 1$ y $n \neq 0$

$$a \mid b^n \Rightarrow a = b$$

En efecto:

Demostrémoslo por inducción particular sobre n en el conjunto $N-\{0\}$ que tiene a 1 como mínimo

1º.- Si $n=1$, $a \mid b^n \Rightarrow a \mid b \overset{1}{\Rightarrow} a=b$

1.- Por ser $b \in P$ y $a \neq 1$

2º.- Si se cumple la propiedad para $n=m$, $(m \neq 0)$ entonces se cumple para $n=m^+$

Demostración:

$a \mid b^{m^+} \Rightarrow a \mid b^m . b \Rightarrow a \mid b^m \ V \ a \mid b \Rightarrow a=b \ V \ a=b \Rightarrow a=b$

3.5.- Siendo $a,b \in P$, $a \neq 1$, $n \neq 0$ y $m \neq 0$

$$a^n \mid b^m \Rightarrow a=b \wedge n \leqslant m$$

En efecto:

a) $a^n \mid b^m \Rightarrow a=b$

Demostración:

$a^n \mid b^m \Rightarrow a \mid a^n \wedge a^n \mid b^m \Rightarrow a \mid b^m \Rightarrow a=b$

b) $a^n \mid b^m \Rightarrow n \leqslant m$

Demostración:

$a^n \mid b^m \overset{1}{\Rightarrow} a^n \leqslant b^m \wedge a=b \Rightarrow a^n \leqslant a^m \overset{2}{\Rightarrow} n \leqslant m$

1.- Por 1.5

2.- Por II-5.7 y II-5.9

3.6.- $a\notin P\Rightarrow\exists_x(x\in P-\{1\}\wedge x|\ a)$

En efecto:

$a\notin P\Rightarrow a\dot{-}\{1,a\}\neq\emptyset\Rightarrow b=\min.(a\dot{-}\{1,a\})\overset{1}{\Rightarrow} b\in P-\{1\}\wedge b|\ a\Rightarrow\exists_x(x\in P-\{1\}\wedge x|\ a)$

1.- Si $b\notin P-\{1\}$, entonces $b\dot{-}\{1,b\}\neq\emptyset$, $\min.(b\dot{-}\{1,b\})\in a\dot{-}\{1,a\}$ y $\min.(b\dot{-}\{1,b\})<b$, lo cual es imposible.

3.7.- $\forall_x(x\in P-\{1\}\wedge x^2\leq a\rightarrow x\nmid a)\Rightarrow a\in P$

En Efecto:

Demostrémoslo en forma contrarrecíproca

$a\notin P\Rightarrow\exists_x(x\in P-\{1\}\wedge x^2\leq a\wedge x|\ a)$

Demostración:

$a\notin P\overset{1}{\Rightarrow}\exists_x(x\in P-\{1\}\wedge x.(a:x)=a\wedge x\leq a:x)\Rightarrow\exists_x(x\in P-\{1\}\wedge x^2\leq a\wedge x|\ a)$

1.- Siendo x el mínimo número primo distinto de 1 que divide al número compuesto a, y a:x un número compuesto o primo distinto de 1

3.8.- El conjunto P es infinito

En efecto:

Si P fuese finito ($P\neq\emptyset$), entonces existiría un $n\in N-\{0\}$ y una biyección $\alpha:n^{<}\rightarrow P$(I-6.2.8), y puesto que $\forall_{x<n}(\alpha_x<1+\prod_{x<n}\alpha_x)$, sería $1+\prod_{x<n}\alpha_x\notin P$ y además

$$1+\prod_{x<n}\alpha_x\notin P\Rightarrow\exists_y(y\in P-\{1\}\wedge y|\ 1+\prod_{x<n}\alpha_x)\overset{1}{\Rightarrow}\exists_y(y\in P-\{1\}\wedge y|\ \prod_{x<n}\alpha_x\wedge y|\ 1+\prod_{x<n}\alpha_x)$$
$$\overset{2}{\Rightarrow}\exists_y(y\neq 1\wedge y|\ 1)\Rightarrow\exists_y(y\neq 1\wedge y=1)$$

1.- Por ser y primo, y es un elemento de la familia $(\alpha_x)_{x<n}$

2.- Por 1.8

luego se cumpliría $\exists_y\ (y\neq 1 \wedge y=1)$ lo cual es imposible

3.9.- El conjunto P es isomorfo al N

En efecto:

Por I-6.2.5.1

En adelante mencionaremos este isomorfismo mediante la biyección $p:N\to P$, y al conjunto P de números primos mediante la familia $(p_x)_{x\in N}$

4.- Familias primas

Dado un conjunto natural N y el conjunto P de sus números primos, llamamos familias primas a las familias del tipo $(\alpha_x^{\alpha' x})_{x<a'}$ en que $a'\in N-\{0\}$, α es un monomorfismo de $a'^{<}$ en $P-\{1\}$ y α' una aplicación de $a'^{<}$ en $N-\{0\}$

Propiedades:

4.1.- Siendo $b\in P-\{1\}$, $m\neq 0$ y $(\alpha_x^{\alpha' x})_{x<a'}$ una familia prima

$$b^m \mid \prod_{x<a'} \alpha_x^{\alpha' x} \Rightarrow \exists_{x<a'}(b^m \mid \alpha_x^{\alpha' x})$$

En efecto:

Demostrémoslo por inducción particular sobre a' en el conjunto $N-\{0\}$ que tiene a 1 como mínimo

1º.- Si $a'=1$, $b^m \mid \prod_{x<a'} \alpha_x^{\alpha' x} \Rightarrow b^m \mid \alpha_0^{\alpha' 0} \Rightarrow \exists_{x<a'}(b^m \mid \alpha_x^{\alpha' x})$

2º.- Si se cumple la propiedad para $a'=s$ $(s\neq 0)$, entonces se cumple para $a'=s^+$

Demostración:

$$b^m \mid \prod_{x<s^+} \alpha_x^{\alpha'x} \Rightarrow b^m \mid \prod_{x<s} \alpha_x^{\alpha'x} \cdot \alpha_s^{\alpha's} \overset{1}{\Rightarrow} b^m \mid \prod_{x<s} \alpha_x^{\alpha'x} \vee b^m \mid \alpha_s^{\alpha's} \Rightarrow \exists_{x<s} (b^m \mid \alpha_x^{\alpha'x}) \vee b^m \mid \alpha_s^{\alpha's} \Rightarrow \exists_{x<s^+} (b^m \mid \alpha_x^{\alpha'x})$$

1.- Por 3.3, $b \mid \prod_{x<s} \alpha_x^{\alpha'x}$ ó $b \mid \alpha_s^{\alpha's}$ pero no a los dos simultáneamente, ya que la aplicación α de $a'^{<}$ en N es inyectiva; luego b^m es primo con uno de los dos factores (1.18)

4.2.- Descomposición de un número en factores primos

Siendo $a \in N-\{0,1\}$, existe una familia prima $(\alpha_x^{\alpha'x})_{x<a'}$ y solamente una tal que $a = \prod_{x<a'} \alpha_x^{\alpha'x}$

En efecto:

1.- Existencia

Demostrémoslo por inducción general sobre a en el conjunto $N-\{0,1\}$ que tiene a 2 como mínimo

1º.- Siendo a=2, $a=2=2^{1} \overset{1}{=} \prod_{x<a'} \alpha_x^{\alpha'x}$

1.- En que $a'=1$, $\alpha_0=2$ y $\alpha'_0=1$

2º.- Siendo $a \neq 2$ $(2<a)$; si se cumple la propiedad para cualquier $b<a$ tal que $2<b$, entonces se cumple para a

Demostración:

a) Si $a \in P$

$$a \overset{1}{=} \prod_{x<a'} \alpha_x^{\alpha'x}$$

1.- Siendo $a'=1$, $\alpha_0=a$ y $\alpha'_0=1$

b) Si $a \notin P$

$$a \overset{1}{=} b.c = \prod_{x<b'} \beta_x^{\beta'x} . c \overset{2}{=} \prod_{x<a'} \alpha_x^{\alpha'x}$$

1.- En que c es el mayor número primo que divide al número a y por -

lo tanto $b<a$

2.- En que

a) Si $c\nmid b$, $a'=b'$, $\forall_{x<b'}(\alpha_x=\beta_x)$, $\forall_{x<b'-1}(\alpha'_x=\beta'_x)$ y $\alpha'_{a'-1}=1+\beta'_{a'-1}$

b) Si $c\nmid b$, $a'=b'+1$, $\forall_{x<b'}(\alpha_x=\beta_x \wedge \alpha'_x=\beta'_x)$, $\alpha_{b'}=c$ y $\alpha'_{b'}=1$

2.- Unicidad

Siendo $(\beta_x^{\beta'x})_{x<b'}$ una familia prima

$$\prod_{x<a'} \alpha_x^{\alpha'x} = \prod_{x<b'} \beta_x^{\beta'x} \Rightarrow a'=b' \wedge \forall_{x<a'} (\alpha_x=\beta_x \wedge \alpha'_x=\beta'_x)$$

Ya que:

a) $\prod_{x<a'} \alpha_x^{\alpha'x} = \prod_{x<b'} \beta_x^{\beta'x} \Rightarrow a'=b'$

Demostración:

$$\prod_{x<a'} \alpha_x^{\alpha'x} = \prod_{x<b'} \beta_x^{\beta'x} \Rightarrow \prod_{x<a'} \alpha_x^{\alpha'x} = \prod_{x<b'} \beta_x^{\beta'x} \wedge (a'=b' \vee a'<b' \vee b'<a') \overset{1}{\Rightarrow} a'=b'$$

1.- Si $a'<b'(b'<a')$, entonces existiría algun divisor primo de $\prod_{x<b'} \beta_x^{\beta'x}$ ($\prod_{x<a'} \alpha_x^{\alpha'x}$) que no lo sería de su igual $\prod_{x<a'} \alpha_x^{\alpha'x}$ ($\prod_{x<b'} \beta_x^{\beta'x}$)

b) $\prod_{x<a'} \alpha_x^{\alpha'x} = \prod_{x<b'} \beta_x^{\beta'x} \Rightarrow \forall_{x<a'}(\alpha_x=\beta_x \wedge \alpha'_x=\beta'_x)$

Demostrémoslo por inducción particular sobre a' en el conjunto $N-\{0\}$ que tiene a 1 como mínimo

1º.- Si $a'=1$, $\prod_{x<a'} \alpha_x^{\alpha'x} = \prod_{x<b'} \beta_x^{\beta'x} \Rightarrow \alpha_o^{\alpha'o} = \beta_o^{\beta'o} \Rightarrow \alpha_o=\beta_o \wedge \alpha'_o=\beta'_o \Rightarrow \forall_{x<a'}$ -- $(\alpha_x=\beta_x \wedge \alpha'_x=\beta'_x)$

2º.- Si se cumple la propiedad para $a'=n$, entonces se cumple para $a'=n^+$

Demostración:

$$\prod_{x<n^+} \alpha_x^{\alpha'x} = \prod_{x<n^+} \beta_x^{\beta'x} \Rightarrow \prod_{x<n} \alpha_x^{\alpha'x} \cdot \alpha_n^{\alpha'n} = \prod_{x<n} \beta_x^{\beta'x} \cdot \beta_n^{\beta'n} \overset{1}{\Rightarrow} \prod_{x<n} \alpha_x^{\alpha'x} = \prod_{x<n} \beta_x^{\beta'n} \wedge \alpha_n^{\alpha'n}$$

$$= \beta_n^{\beta'n} \Rightarrow \forall_{x<n}(\alpha_x = \beta_x \wedge \alpha'_x = \beta'_x) \wedge (\alpha_n = \beta_n \wedge \alpha'_n = \beta'_n) \Rightarrow \forall_{x<n^+} (\alpha_x = \beta_x \wedge \alpha'_x = \beta'_x)$$

1.- $\alpha_n(\beta_n)$ es el número primo máximo que divide al número a

4.3.- Siendo $(\alpha_x^{\alpha'x})_{x<a'}$ y $(\beta_x^{\beta'x})_{x<b'}$ familias primas

$$\prod_{x<a'} \alpha_x^{\alpha'x} \mid \prod_{y<b'} \beta_y^{\beta'y} \Leftrightarrow \forall_{x<a'} \exists_{y<b'} (\alpha_x = \beta_y \wedge \alpha'_x \leq \beta'_y)$$

En efecto:

a) $$\prod_{x<a'} \alpha_x^{\alpha'x} \mid \prod_{y<b'} \beta_y^{\beta'y} \Rightarrow \forall_{x<a'} \exists_{y<b'} (\alpha_x = \beta_y \wedge \alpha'_x \leq \beta'_y)$$

Demostración:

$$\prod_{x<a'} \alpha_x^{\alpha'x} \mid \prod_{y<b'} \beta_y^{\beta'y} \Rightarrow \forall_{x<a'} (\alpha_x^{\alpha'x} \mid \prod_{y<b'} \beta_y^{\beta'y}) \overset{1}{\Rightarrow} \forall_{x<a'} \exists_{y<b'} (\alpha_x^{\alpha'x} \mid \beta_y^{\beta'y})$$

$$\overset{2}{\Rightarrow} \forall_{x<a'} \exists_{y<b'} (\alpha_x = \beta_y \wedge \alpha'_x \leq \beta'_y)$$

1.- Por 4.1

2.- Por 3.5

b) $$\forall_{x<a'} \exists_{y<b'} (\alpha_x = \beta_y \wedge \alpha'_x \leq \beta'_y) \Rightarrow \prod_{x<a'} \alpha_x^{\alpha'x} \mid \prod_{y<b'} \beta_y^{\beta'y}$$

Demostración:

$$\forall_{x<a'} \exists_{y<b'} (\alpha_x = \beta_y \wedge \alpha'_x \leq \beta'_y) \overset{1}{\Rightarrow} \forall_{x<a'} \exists_{y<b'} (\alpha_x = \beta_y \wedge \alpha'_x \leq \beta'_y \wedge \prod_{x<a'} \alpha_x^{\alpha'x} \cdot \prod_{x<a'} \alpha_x^{\beta'y - \alpha'x} \mid \prod_{y<b'} \beta_y^{\beta'y}) \Rightarrow \prod_{x<a'} \alpha_x^{\alpha'x} \mid \prod_{y<b'} \beta_y^{\beta'y}$$

1.- Por III-3.23.1

4.4.- Siendo $(\alpha_x^{\alpha'x})_{x<a'}$ y $(\beta_x^{\beta'x})_{x<b'}$ familias primas; si $(\gamma_x^{\gamma'x})_{x<c'}$ es la familia prima cuyas bases son las distintas bases comunes o no comunes a las dos anteriores y cuyos correspondientes exponentes son el mayor de los correspondientes a las bases comunes o el correspondiente a

la base no común, entonces

$$\prod_{x<c'} \gamma_x^{\gamma' x} = \prod_{x<a'} \alpha_x^{\alpha' x} \mu \prod_{x<b'} \beta_x^{\beta' x}$$

En efecto:

a) $\prod_{x<a'} \alpha_x^{\alpha' x} \mid \prod_{x<c'} \gamma_x^{\gamma' x}$ y $\prod_{x<b'} \beta_x^{\beta' x} \mid \prod_{x<c'} \gamma_x^{\gamma' x}$

b) Siendo $n \in N$

$$\prod_{x<a'} \alpha_x^{\alpha' x} \mid n \wedge \prod_{x<b'} \beta_x^{\beta' x} \mid n \Rightarrow \prod_{x<c'} \gamma_x^{\gamma' x} \mid n$$

Demostración:

Por la construcción de $(\gamma_x^{\gamma' x})_{x<c'}$ y por 4.3

4.5.- Siendo $(\alpha_x^{\alpha' x})_{x<a'}$ y $(\beta_x^{\beta' x})_{x<b'}$ familias primas con alguna base común; si $(\varepsilon_x)_{x<e'}$ es la familia prima cuyas bases son las distintas bases comunes a los dos anteriores y cuyos correspondientes exponentes son el menor de los correspondientes a las bases comunes, entonces

$$\prod_{x<e'} \varepsilon_x^{\varepsilon' x} = \prod_{x<a} \alpha_x^{\alpha' x} \delta \prod_{x<b'} \beta_x^{\beta' x}$$

En efecto:

a) $\prod_{x<e'} \varepsilon_x^{\varepsilon' x} \mid \prod_{x<a'} \alpha_x^{\alpha' x}$ y $\prod_{x<e'} \varepsilon_x^{\varepsilon' x} \mid \prod_{x<b'} \beta_x^{\beta' x}$

b) Siendo $m \in N$

$$m \mid \prod_{x<a'} \alpha_x^{\alpha' x} \wedge m \mid \prod_{x<b'} \beta_x^{\beta' x} \Rightarrow m \mid \prod_{x<e'} \varepsilon_x^{\varepsilon' x}$$

Demostración:

Por la construcción de $(\varepsilon_x^{\varepsilon' x})_{x<e'}$ y por 4.3