Segundo Tercio

① $(a \leq b \Rightarrow a \downarrow b = a) \wedge (a \geq b \Rightarrow a \downarrow b = b)$

② $(a \geq b \Rightarrow a \uparrow b = a) \wedge (a \leq b \Rightarrow a \uparrow b = b)$

Axiomas $\downarrow$ y $\uparrow$

$(\forall z : D \,|: z \leq a \downarrow b \equiv z \leq a \wedge z \leq b)$

$(\forall z : D \,|: a \uparrow b \leq z \equiv a \leq z \wedge b \leq z)$

Propiedades basicas $\uparrow$ y $\downarrow$

- Simetria $\downarrow$ $a \downarrow b = b \downarrow a$
- Simetria $\uparrow$ $a \uparrow b = b \uparrow a$
- Asociatividad $\downarrow$ $a \downarrow (b \downarrow c) \equiv (a \downarrow b) \downarrow c$
- Asociatividad $\uparrow$ $a \uparrow (b \uparrow c) = (a \uparrow b) \uparrow c$
- Idempotencia $\downarrow$ $a \downarrow a = a$
- Idempotencia $\uparrow$ $a \uparrow a = a$
- Proyección $\downarrow$ $a \leq b \equiv a \downarrow b = a$
- Proyección $\uparrow$ $a \leq b \equiv a \uparrow b = b$
- Cota inferior $a \downarrow b \leq a \wedge a \downarrow b \leq b$
- Cota superior $a \leq a \uparrow b \wedge b \leq a \uparrow b$
- Absorción de $\downarrow$ $a \downarrow (a \uparrow b) = a$
- Absorción de $\uparrow$ $a \uparrow (a \downarrow b) = a$
- Alternatividad $\downarrow$ $a \downarrow b = a \vee a \downarrow b = b$
- Alternatividad $\uparrow$ $a \uparrow b = a \vee a \uparrow b = b$
- contraposición $\downarrow$ $a \downarrow b \leq c \equiv a \leq c \vee b \leq c$
- contraposición $\uparrow$ $c \leq a \uparrow b \equiv c \leq a \vee c \leq b$
- caracterización $\uparrow$ $a \uparrow b = c \equiv a \leq c \wedge b \leq c \wedge (\forall z |: a \leq z \wedge b \leq z \Rightarrow c \leq z)$
- caracterización $\downarrow$ $a \downarrow b = c \equiv c \leq a \wedge c \leq b \wedge (\forall z |: z \leq a \wedge z \leq b \Rightarrow z \leq c)$
- $\uparrow$ domina a $\downarrow$ $a \downarrow b \leq a \uparrow b$
- Monotonía de $\downarrow$ $a \leq b \Rightarrow a \downarrow c \leq b \downarrow c$
- Monotonía de $\uparrow$ $a \leq b \Rightarrow a \uparrow c \leq b \uparrow c$
- ley de signos sobre $\downarrow$ $-(a \downarrow b) = -a \uparrow -b$
- ley de signos sobre $\uparrow$ $-(a \uparrow b) = -a \downarrow -b$
- Distributividad $\uparrow$ sobre $\downarrow$ $a \uparrow (b \downarrow c) = (a \uparrow b) \downarrow (a \uparrow c)$
- Distributividad $\downarrow$ sobre $\uparrow$ $a \downarrow (b \uparrow c) = (a \downarrow b) \uparrow (a \downarrow c)$
- Distribución $+$ sobre $\downarrow$ $c + (a \downarrow b) = c + a \downarrow c + b$
- Distribución $+$ sobre $\uparrow$ $c + (a \uparrow b) = c + a \uparrow c + b$
- Semidistribución de $\cdot$ sobre $\uparrow$ $c \geq 0 \Rightarrow c \cdot a \uparrow b = c \cdot a \uparrow c \cdot b$
- Semidistribución de $\cdot$ sobre $\downarrow$ $c \geq 0 \Rightarrow c \cdot a \downarrow b = c \cdot a \downarrow c \cdot b$

- Semimonotonía producto $a \leq a \uparrow b \Rightarrow c \cdot a \leq c \cdot a \uparrow b$
- Axioma cuantificado, sobre $\downarrow$ y $\uparrow$

$$(\downarrow x \mid R : E) \geq G \equiv (\forall x \mid R : E \geq G)$$
$$(\uparrow x \mid R : E) \leq G \equiv (\forall x \mid R : E \leq G)$$

- Teoremas de operatorias sobre $\downarrow$ y $\uparrow$
- $R[x := y] \Rightarrow (\downarrow x \mid R : E) \leq E[x := y]$

- Funciones piso y techo.

Ax. $\lfloor x \rfloor = (\uparrow z : \mathbb{Z} \mid z \leq x : z)$

$\lceil x \rceil = (\downarrow z : \mathbb{Z} \mid z \geq x : z)$

Axiomas.

$$(\forall z : \mathbb{Z} \mid : z \leq \lfloor x \rfloor \equiv z \leq x)$$
$$(\forall z : \mathbb{Z} \mid : z \geq \lceil x \rceil \equiv z \geq x)$$

Propiedades piso y techo

- $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$
- $\lceil x \rceil - 1 < x \leq \lceil x \rceil$
- $\lfloor k \rfloor = k = \lceil k \rceil$
- $-\lfloor -x \rfloor = \lceil x \rceil$
- $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

Valor Absoluto

Definición $|a| = a \uparrow -a$

- invariancia bajo $-$ $|a| = |-a|$
- desigualdad triangular $|a+b| \leq |a| + |b|$
- idempotencia. $||a|| = |a|$
- Valor absoluto de un producto $|a \cdot b| = |a| \cdot |b|$
- $|a| \leq b \equiv -b \leq a \leq b$
- $a \geq 0 \equiv |a| = a$
- $a \leq 0 \equiv |a| = -a$

Aritmetica multiplicativa.

① Divisibilidad $a \cdot | b \equiv (\exists z | : a \cdot z = b)$

- $a \cdot | a$ reflexividad
- Transitividad $a \cdot | b \wedge b \cdot | c \Rightarrow a \cdot | c$
- Antisimetrica $a \cdot | b \wedge b \cdot | a \Rightarrow a = b \vee a = -b$
- Multiplo de multiplos $a \cdot | b \Rightarrow a \cdot | b \cdot c$
- $a \cdot | 0$
- $1 \cdot | a$
- $0 \cdot | a \Rightarrow a = 0$
- $a \cdot | 1 \Rightarrow a = 1 \vee a = -1$
- $a > 1 \wedge a \cdot | b \Rightarrow \neg (a \cdot | b + 1)$
- Monotonia simple del producto $a \cdot | b \Rightarrow a \cdot c \cdot | b \cdot c$
- Monotonia doble del producto $a \cdot | b \wedge c \cdot | d \Rightarrow a \cdot c \cdot | b \cdot d$
- ley de signos $a \cdot | b = a \cdot | -b = -a \cdot | b$
- invariancia bajo valor absoluto $(a \cdot | |b| \equiv a \cdot | b) \wedge (|a| \cdot | b \equiv a \cdot | b)$
- Suma de multiplos $a \cdot | b \wedge a \cdot | c \Rightarrow a \cdot | b + c$
- divisibilidad indirecta $a \cdot | b \equiv (\forall z | : z \cdot | a \Rightarrow z \cdot | b)$
- divisibilidad indirecta $a \cdot | b \equiv (\forall z | : a \cdot | z \Leftarrow b \cdot | z)$
- divisores comunes $a = b \equiv (\forall z | : z \cdot | a \equiv z \cdot | b)$
- Multiplos comunes $a = b \equiv (\forall z | : a \cdot | z \equiv b \cdot | z)$

Maximo divisor Comun y Minimo multiplo común

Axioma. $(\forall z : z | : z \cdot | m \Downarrow n \equiv z \cdot | m \wedge z \cdot | n)$

$(\forall z : z | : m \Uparrow n \cdot | z \equiv m \cdot | z \wedge n \cdot | z)$

Propiedades.

- Simetría $a \Downarrow b = b \Downarrow a$

  $a \Uparrow b = b \Uparrow a$

- Asociatividad $a \Downarrow (b \Downarrow c) = (a \Downarrow b) \Downarrow c$

  $a \Uparrow (b \Uparrow c) = (a \Uparrow b) \Uparrow c$

- Idempotencia $a \Downarrow a = |a|$

  $a \Uparrow a = |a|$

- Absorción $a \Downarrow (b \Uparrow a) = |a|$

  $a \Uparrow (b \Downarrow a) = |a|$

Scanned by CamScanner

- Cotas inferiores y superiores
  ① $a \Downarrow b \cdot| a \ \wedge \ a \Downarrow b \cdot| b$
  ② $a \cdot| a \Uparrow b \ \wedge \ b \cdot| b \Uparrow a$
- Proyección
  ① $a \cdot| b \equiv a \Downarrow b = |a|$
  ② $a \cdot| b \equiv a \Uparrow b = |b|$
- Anulador
  ① $\perp \Downarrow a = \perp$
  ② $0 \Uparrow a = 0$
- Identidad
  ① $0 \Downarrow a = |a|$
  ② $\perp \Uparrow a = |a|$
- lema Bézout $ax + by = a \Downarrow b$
  ↳ $(\exists x, y : \mathbb{Z} \mid : a \Downarrow b = a \cdot x + b \cdot y)$ -> Nunca se demostró formalmente
- Monotonía sobre ·|
  ① $a \cdot| b \Rightarrow a \Downarrow c \cdot| b \Downarrow c$
  ② $a \cdot| b \Rightarrow a \Uparrow c \cdot| b \Uparrow c$
- distributividad de ·
  ① $c \geq 0 \Rightarrow c \cdot (a \Downarrow b) = c \cdot a \Downarrow c \cdot b$
  ② $c \geq 0 \Rightarrow c \cdot (a \Uparrow b) = c \cdot a \Uparrow c \cdot b$
- ley de signos
  ① $a \Downarrow -a = |a|$
  ② $a \Uparrow -a = |a|$
- invarianza sobre valor absoluto
  ① $a \Downarrow b = |a| \Downarrow |b|$
  ② $a \Uparrow b = |a| \Uparrow |b|$
- invarianza bajo suma.
  $a \Downarrow b = a \Downarrow (b-a) = a \Downarrow (b+a)$
- factorización $(a \Downarrow b) \cdot (a \Uparrow b) = |a \cdot b|$
- Distributividad mutua.
  ① $c \Downarrow (a \Uparrow b) = (c \Downarrow a) \Uparrow (c \Downarrow b)$
  ② $c \Uparrow (a \Downarrow b) = (c \Uparrow a) \Downarrow (c \Uparrow b)$
- Definición escolar
  ① $a \Downarrow b = (\uparrow k : \mathbb{Z} \mid k \cdot| a \wedge k \cdot| b : k)$
  ② $a \Uparrow b = (\downarrow k : \mathbb{Z} \mid k > 0 \wedge a \cdot| k \wedge b \cdot| k : k)$

- Algoritmo de la división $a \geq 0 \wedge b > 0 \Rightarrow (\exists q, r \mid 0 \leq r < b : a = q \cdot b + r)$
- Invariancia por residuo $a \Downarrow b = b \Downarrow (a \underline{mod} b)$ $\hookrightarrow a = b \cdot (a.div\, b) + a \underline{mod} b$
- Teo. Invariancia $a \Downarrow b = a \Downarrow (b + k \cdot a)$
- Representación en base b. $n = (+i \mid 0 \leq i \leq m : c_i \cdot b^i)$

Congruencias

Definición $a \overset{m}{=} b \equiv n \cdot \mid a - b$

Intuición $a \overset{m}{=} b \equiv a \underline{mod}\ m = b \underline{mod}\ m$

- Reflexiva. $a \overset{m}{=} a$
- Simetría $a \overset{m}{=} b \equiv b \overset{m}{=} a$
- Transitividad $a \overset{m}{=} b \wedge b \overset{m}{=} c \Rightarrow a \overset{m}{=} c$
- monotonía simple de + $a \overset{m}{=} b \Rightarrow a + c \overset{m}{=} b + c$
- monotonía doble de + $a \overset{m}{=} b \wedge c \overset{m}{=} d \Rightarrow a + c \overset{m}{=} d + b$
- monotonía simple de · $a \overset{m}{=} b \Rightarrow a \cdot c \overset{m}{=} b \cdot c$
- monotonía doble de · $a \overset{m}{=} b \wedge c \overset{m}{=} d \Rightarrow a \cdot c \overset{m}{=} b \cdot d$
- monotonía de potencias $a \overset{m}{=} b \Rightarrow a^n \overset{m}{=} b^n$
- Definición alternativa. $a \overset{m}{=} b \equiv a \underline{mod}\ m = b \underline{mod}\ m$
- Cancelación modular $a \cdot c \overset{m \cdot c}{=} b \cdot c \equiv a \overset{m}{=} b$, $c > 0$
- Teorema de leibniz para congruencias. $a \overset{m}{=} b \Rightarrow E[z := a] \overset{m}{=} E[z := b]$

Coprimidad

def $a \perp b \equiv a \Downarrow b = 1$

- $a \perp b \wedge a \cdot \mid b \cdot c \Rightarrow a \cdot \mid c$
- $a \perp b \wedge a \cdot \mid c \wedge b \cdot \mid c \Rightarrow a \cdot b \cdot \mid c$
- invariancia sobre congruencia $a \perp n \wedge a \overset{n}{=} b \Rightarrow b \perp n$

Scanned by CamScanner

Demostraciones propiedades básicas $\downarrow$ y $\uparrow$

① Simetría $\downarrow$ $a\downarrow b = b\downarrow a$

$a\downarrow b = b\downarrow a$

$\equiv$ < igualdad indirecta >

$(\forall z \mid: z \leq a\downarrow b \equiv z \leq b\downarrow a)$

$\equiv$ < Ax $\downarrow$ >

$(\forall z \mid: z \leq a \wedge z \leq b \equiv z \leq b \wedge z \leq a)$

$\equiv$ < conmutatividad de $(\wedge)$ y lógica >

true

② Simetría $\uparrow$ $a\uparrow b = b\uparrow a$

$a\uparrow b = b\uparrow a$

$\equiv$ < igualdad indirecta >

$(\forall z \mid: a\uparrow b \leq z \equiv b\uparrow a \leq z)$

$\equiv$ < Ax $\uparrow$ >

$(\forall z \mid: a \leq z \wedge b \leq z \equiv b \leq z \wedge a \leq z)$

$\equiv$ < conmutatividad $(\wedge)$ y lógica >

true

③ Asociatividad $\downarrow$ $a\downarrow(b\downarrow c) = (a\downarrow b)\downarrow c$, igual para el $\uparrow$

$a\downarrow(b\downarrow c) = (a\downarrow b)\downarrow c$

$\equiv$ < igualdad indirecta >

$(\forall z \mid: z \leq a\downarrow(b\downarrow c) \equiv z \leq (a\downarrow b)\downarrow c)$

$\equiv$ < Ax $\downarrow$ >

$(\forall z \mid: z \leq a \wedge z \leq b \wedge z \leq c \equiv z \leq a \wedge z \leq b \wedge z \leq c)$

$\equiv$ < lógica >

true

④ Idempotencia $\downarrow$ $a\downarrow a = a$, igual para $\uparrow$

$a\downarrow a = a$

$\equiv$ < igualdad indirecta >

$(\forall z \mid: z \leq a\downarrow a \equiv z \leq a)$

$\equiv$ < ax $\downarrow$ >

$(\forall z \mid: z \leq a \wedge z \leq a \equiv z \leq a)$

$\equiv$ < lógica >

true

⑤ Proyección $\uparrow$ $a \leq b \equiv a\uparrow b = b$, igual para $\downarrow$

Dem. transito

$a\uparrow b = b$

$\equiv$ < igualdad indirecta y Ax $\uparrow$ >

$(\forall z \mid: a \leq z \wedge b \leq z \equiv b \leq z)$

$\equiv$ < lógica >

$(\forall z \mid: b \leq z \Rightarrow a \leq z)$

$\equiv$ < desigualdad indirecta >

$a \leq b$

⑥ cota inferior $a{\downarrow}b \leq a \wedge a{\downarrow}b \leq b$

$a{\downarrow}b \leq a$

$\equiv$ < desigualdad indirecta >

$(\forall z |: z \leq a{\downarrow}b \Rightarrow z \leq a)$

$\equiv$ < Ax ↓ >

$(\forall z |: z \leq a \wedge z \leq b \Rightarrow z \leq a)$

$\equiv$ < logica >

true

$a{\downarrow}b \leq b$

$\equiv$ < desigualdad indirecta >

$(\forall z |: z \leq a{\downarrow}b \Rightarrow z \leq b)$

$\equiv$ < Ax ↓ >

$(\forall z |: z \leq a \wedge z \leq b \Rightarrow z \leq b)$

$\equiv$ < logica >

true

⑦ cota superior $a \leq a{\uparrow}b \wedge b \leq a{\uparrow}b$

$a \leq a{\uparrow}b$

$\equiv$ < desigualdad indirecta >

$(\forall z |: a{\uparrow}b \leq z \Rightarrow a \leq z)$

$\equiv$ < ax ↑ >

$(\forall z |: a \leq z \wedge b \leq z \Rightarrow a \leq z)$

$\equiv$ < logica >

true

$b \leq a{\uparrow}b$

$\equiv$ < desigualdad indirecta >

$(\forall z |: a{\uparrow}b \leq z \Rightarrow b \leq z)$

$\equiv$ < ax ↑ >

$(\forall z |: a \leq z \wedge b \leq z \Rightarrow b \leq z)$

$\equiv$ < logica >

true

⑧ Absorción ↓ $a{\downarrow}(a{\uparrow}b) = a$

Dem. Precedencia mutua

$a \leq a{\downarrow}(a{\uparrow}b)$

$\equiv$ < Ax ↓ >

$a \leq a \wedge a \leq a{\uparrow}b$

$\equiv$ < cota superior y logica >

true

$a{\downarrow}(a{\uparrow}b) \leq a$

$\equiv$ < cota inferior >

true

⑨ Absorción ↑ $a{\uparrow}(a{\downarrow}b) = a$

Dem. precedencia mutua

$a \leq a{\uparrow}(a{\downarrow}b)$

$\equiv$ < cota superior >

true

$a{\uparrow}(a{\downarrow}b) \leq a$

$\equiv$ < ax ↑ >

$a \leq a \wedge a \leq a{\downarrow}b$

$\equiv$ < cota inferior, logica >

true

(10) Alternatividad $\downarrow$ $a\downarrow b = a \vee a\downarrow b = b$, igual para $\uparrow$

$a\downarrow b = a \vee a\downarrow b = b$

$\equiv$ < igualdad indirecta, ax $\downarrow$ >

$(\forall z \mid : z \leq a \wedge z \leq b \equiv z \leq a) \vee (\forall z \mid : z \leq a \wedge z \leq b \equiv z \leq b)$

$\equiv$ < logica >

$(\forall z \mid : z \leq a \Rightarrow z \leq b) \vee (\forall z \mid : z \leq b \Rightarrow z \leq a)$

$\equiv$ < logica >

$(\forall z \mid : \neg z \leq a) \vee z \leq b \vee (\neg z \leq b) \vee z \leq a)$

$\equiv$ < logica >

true

(11) contraposición $\downarrow$ $a\downarrow b \leq c \equiv a \leq c \vee b \leq c$, igual para $\uparrow$

$a\downarrow b \leq c$

$\equiv$ < desigualdad indirecta, ax $\downarrow$ >

$(\forall z \mid : z \leq a \wedge z \leq b \Rightarrow z \leq c)$

$\equiv$ < logica >

$(\forall z \mid : (z \leq a \Rightarrow z \leq c) \vee (z \leq b \Rightarrow z \leq c))$

$\equiv$ < desigualdad indirecta >

$a \leq c \vee b \leq c$

(12) Caracterización $\uparrow$ $a\uparrow b = c \equiv a \leq c \wedge b \leq c \wedge (\forall z \mid : a \leq z \wedge b \leq z \Rightarrow c \leq z)$, igual $\downarrow$

$a \leq c \wedge b \leq c \wedge (\forall z \mid : a \leq z \wedge b \leq z \Rightarrow c \leq z)$

$\equiv$ < ax $\uparrow$ >

$a\uparrow b \leq c \wedge (\forall z \mid : a\uparrow b \leq z \Rightarrow c \leq z)$

$\equiv$ < desigualdad indirecta >

$a\uparrow b \leq c \wedge c \leq a\uparrow b$

$\equiv$ < Precedencia mutua >

$a\uparrow b = c$

(13) $\uparrow$ domina a $\downarrow$ $a\downarrow b \leq a\uparrow b$

$a\downarrow b$

$\leq$ < cota inferior >

a

$\leq$ < cota superior >

$a\uparrow b$

igual para ↑

(14) monotonía de $\downarrow$ $a \le b \Rightarrow a \downarrow c \le b \downarrow c$, igual para $\uparrow$

Dem. suposición de $a \le b$

$a \downarrow c \le b \downarrow c$

$\equiv$ <ax $\downarrow$>

$a \downarrow c \le b \ \wedge \ a \downarrow c \le c$

$\equiv$ <cota inferior>

$a \downarrow c \le b$

$\equiv$ <contraposición>

$a \le b \ \vee \ a \le c$

$\equiv$ <suposición $a \le b$, logica>

true

(15) ley de signos sobre $\downarrow$ $-(a \downarrow b) = -a \uparrow -b$, igual para $\uparrow$

$-(a \downarrow b) = -a \uparrow -b$

Por igualdad indirecta basta mostrar

$z \ge -(a \downarrow b) \equiv z \ge -a \uparrow -b$

$z \ge -(a \downarrow b)$

$\equiv$ <aritmetica>

$-z \le a \downarrow b$

$\equiv$ <ax $\downarrow$>

$-z \le a \ \wedge \ -z \le b$

$\equiv$ <aritmetica>

$-a \le z \ \wedge -b \le z$

$\equiv$ <ax $\uparrow$>

$-a \uparrow -b \le z$

(16) distributividad $\uparrow$ sobre $\downarrow$ $a \uparrow (b \downarrow c) = (a \uparrow b) \downarrow (a \uparrow c)$, igual para $\downarrow$ sobre $\uparrow$

$a \uparrow (b \downarrow c) = (a \uparrow b) \downarrow (a \uparrow c)$

Por igualdad indirecta, basta mostrar:

$a \uparrow (b \downarrow c) \le z \equiv (a \uparrow b) \downarrow (a \uparrow c) \le z$

$(a \uparrow b) \downarrow (a \uparrow c) \le z$

$\equiv$ <contraposición $\downarrow$>

$a \uparrow b \le z \ \vee \ a \uparrow c \le z$

$\equiv$ <Ax $\uparrow$>

$a \le z \wedge b \le z \ \vee \ a \le z \ \wedge \ c \le z$

$\equiv$ <logica>

$a \le z \ \wedge \ b \le z \vee c \le z$

$\equiv$ <contraposición $\downarrow$>

$a \le z \ \wedge \ b \downarrow c \le z$

$\equiv$ <Ax $\uparrow$>

$a \uparrow (b \downarrow c) \le z$

(17) distribución + sobre $\downarrow$, igual para $\uparrow$

$$c+(a\downarrow b) = c+a\downarrow c+b$$

por igualdad indirecta, basta mostrar:

$$z \leq c+a\downarrow b \equiv z \leq c+a\downarrow c+b$$

$z \leq c+a\downarrow b$

$\equiv \langle$ aritmetica $\rangle$

$z-c \leq a\downarrow b$

$\equiv \langle$ Ax $\downarrow \rangle$

$z-c \leq a \wedge z-c \leq b$

$\equiv \langle$ aritmetica $\rangle$

$z \leq a+c \wedge z \leq b+c$

$\equiv \langle$ Ax $\downarrow \rangle$

$z \leq a+c \downarrow b+c$

(18) $c \geq 0 \Rightarrow c\cdot a\uparrow b = c\cdot a \uparrow c\cdot b$

Se supone $c \geq 0$, basta mostrar

$c\cdot a\uparrow b = c\cdot a\uparrow c\cdot b$

$(\leq)$: $c\cdot a\uparrow b \leq c\cdot a\uparrow c\cdot b$

$\equiv \langle$ contraposición $\uparrow \rangle$

$c\cdot a\uparrow b \leq c\cdot a \vee c\cdot a\uparrow b \leq c\cdot b$

$\Leftarrow \langle$ suposición $c \geq 0$; semimonotonía $\cdot$ sobre $\leq \rangle$

$a\uparrow b \leq a \vee a\uparrow b \leq b$

$\equiv \langle$ contraposición $\uparrow \rangle$

$a\uparrow b \leq a\uparrow b$

$\equiv \langle$ reflexividad $\rangle$

true

$(\geq)$: $c\cdot a\uparrow c\cdot b \leq c\cdot a\uparrow b$

$\equiv \langle$ ax $\uparrow \rangle$

$c\cdot a \leq c\cdot a\uparrow b \wedge c\cdot b \leq c\cdot a\uparrow b$

$\Leftarrow \langle$ semimonotonía producto $\rangle$

$a \leq a\uparrow b \wedge b \leq a\uparrow b$

$\equiv \langle$ cota superior $\rangle$

true

(19) $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$

Dem.

$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$

$\equiv$ <aritmetica>

$\lfloor x \rfloor \leq x \;\wedge\; x < \lfloor x \rfloor + 1$

$\equiv$ <Axioma piso y $\neg$>

$\lfloor x \rfloor \leq \lfloor x \rfloor \;\wedge\; \neg(\lfloor x \rfloor + 1 \leq x)$

$\equiv$ <reflexividad y axioma piso>

$\neg(\lfloor x \rfloor + 1 \leq \lfloor x \rfloor)$

$\equiv$ <negación>

$\lfloor x \rfloor < \lfloor x \rfloor + 1$

$\equiv$ <matematicas>

true.

(20) $\lceil x \rceil - 1 < x \leq \lceil x \rceil$

Dem.

$\lceil x \rceil - 1 < x \leq \lceil x \rceil$

$\equiv$ <aritmetica>

$\lceil x \rceil - 1 < x \;\wedge\; x \leq \lceil x \rceil$

$\equiv$ <$\neg$> axioma techo>

$\neg(x \leq \lceil x \rceil - 1) \wedge (\lceil x \rceil \leq \lceil x \rceil)$

$\equiv$ <reflexividad> axioma techo>

$\neg(\lceil x \rceil \leq \lceil x \rceil - 1)$

$\equiv$ <$\neg$>

$\lceil x \rceil - 1 < \lceil x \rceil$

$\equiv$ <matematicas>

true

$z \geq \lceil x \rceil \equiv z \geq x$

$\lceil x \rceil \leq z \equiv x \leq z$

(21) $\lfloor k \rfloor = k = \lceil k \rceil$

Dem.

$\lfloor k \rfloor = k = \lceil k \rceil$

$\equiv$ ⟨reescribiendo⟩

$\lfloor k \rfloor = k \;\wedge\; k = \lceil k \rceil$

$\equiv$ ⟨igualdad indirecta⟩

$(z \leq \lfloor k \rfloor \equiv z \leq k) \;\wedge\; (z \geq k \equiv z \geq \lceil k \rceil)$

$\equiv$ ⟨Axioma piso y techo⟩

$(z \leq k \equiv z \leq k) \;\wedge\; (z \geq k \equiv z \geq k)$

$\equiv$ ⟨logica⟩

true

(22) $-\lfloor -x \rfloor = \lceil y \rceil$

Dem por igualdad indirecta. basta mostrar y cualquier entero z

$\lceil x \rceil \leq z \equiv -\lfloor -x \rfloor \leq z$

$\lceil x \rceil \leq z$

$\equiv$ ⟨Axioma techo⟩

$x \leq z$

$\equiv$ ⟨cambio signo⟩

$-z \leq -x$

$\equiv$ ⟨Axioma piso⟩

$-z \leq \lfloor -x \rfloor$

$\equiv$ ⟨cambio signo⟩

$-\lfloor -x \rfloor \leq z$

(23) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

Dem. Por igualdad indirecta basta mostrar y cualquier entero z

$z \leq \lfloor x + n \rfloor \equiv z \leq \lfloor x \rfloor + n$

$z \leq \lfloor x + n \rfloor$

$\equiv$ ⟨Ax piso⟩

$z \leq x + n$

$\equiv$ ⟨aritmetica⟩

$z - n \leq x$

$\equiv$ ⟨Axioma piso⟩

$z - n \leq \lfloor x \rfloor$

$\equiv$ ⟨aritmetica⟩

$z \leq \lfloor x \rfloor + n$

Scanned by CamScanner

(24) Invariancia bajo (-) $|a| = |-a|$

$|a| = |-a|$
$\equiv$ < def >
$a \uparrow -a = -a \uparrow -(-a)$
$\equiv$ < ley signos >
$a \uparrow -a = -a \uparrow a$
$\equiv$ < simetria y matematicas >
true

$|-a|$
$=$ < def >
$-a \uparrow -(-a)$
$=$ < ley signos, simetria $\uparrow$ >
$a \uparrow -a$
$=$ < Def >
$|a|$

(25) Desigualdad triangular

$|a+b| \leq |a| + |b|$

$|a| + |b|$
$=$ < def >
$a \uparrow -a + b \uparrow -b$
$=$ < distribucion (+) sobre $\uparrow$ >
$(a \uparrow -a) + b \uparrow -b + (a \uparrow -a)$
$=$ < distribución (+) sobre $\uparrow$ >
$(a+b \uparrow -a+b) \uparrow (-b+a \uparrow -a-b)$
$=$ < $a+b > -a+b$; $-b+a > -a-b$ >
$a+b \uparrow a-b$
$\geq$
$a+b \uparrow -(a+b)$
$=$ < def >
$|a+b|$

(26) idempotencia $||a|| = |a|$

$||a||$
$=$ < def >
$|a| \uparrow -|a|$
$=$ < def >
$(a \uparrow -a) \uparrow (-a \uparrow -(-a))$
$=$ < signos >
$(a \uparrow -a) \uparrow (a \uparrow -a)$
$=$ < idempotencia $\uparrow$ >
$a \uparrow -a$
$=$ < def >
$|a|$

Scanned by CamScanner

(27) Valor absoluto de un producto

$$|a \cdot b| = |a| \cdot |b|$$

$|a| \cdot |b|$

$= \langle def \rangle$

$a \uparrow -a \cdot b \uparrow -b$

$= \langle$ Semidistribución (·) sobre $\uparrow \rangle$

$(a \uparrow -a) \cdot b \uparrow (a \uparrow -a) \cdot -b$

$= \langle$ Semidistribución (·) sobre $\uparrow \rangle$

$(a \cdot b \uparrow -a \cdot b) \uparrow (a \cdot -b \uparrow a \cdot b)$

$= \langle$ idempotencia $\uparrow \rangle$

$a \cdot b \uparrow - a \cdot b$

$= \langle def \rangle$

$|a \cdot b|$

(28) $|a| \leq b \equiv -b \leq a \leq b$

$|a| \leq b$

$= \langle def \rangle$

$a \uparrow -a \leq b$

$\equiv \langle ax \uparrow \rangle$

$a \leq b \wedge -a \leq b$

$\equiv \langle$ cambio signo $\rangle$

$a \leq b \wedge -b \leq a$

$\equiv \langle$ reescribiendo $\rangle$

$-b \leq a \leq b$

(29) $a \geq 0 \equiv |a| = a$

$|a| = a$

$= \langle$ def ; igualdad indirecta ; cualquier $z \rangle$

$a \uparrow -a \leq z \wedge a \leq z$

$\equiv \langle AX \uparrow \rangle$

$a \leq z \wedge -a \leq z \wedge a \leq z$

$\equiv \langle$ logica $\rangle$

$-a \leq z \quad \wedge \quad \leq z$

$\equiv \langle$ cambio signo $\rangle$

$-a \geq -z$

$\Rightarrow \langle z = 0 \rangle$

$a \geq 0$

Supongo $a \geq 0$

basta mostrar

$|a| = a$

$|a|$

$= \langle def \rangle$

$a \uparrow -a$

$= \langle a > -a \rangle$

a

(30) Reflexividad $a \cdot | a$

$a \cdot | a$

$\equiv$ < def >

$(\exists z | : a \cdot z = a)$

$\Leftarrow$ < $z = 1$ >

$a \cdot 1 = a$

$\equiv$ < Reflexividad(=) >

true

(31) Transitividad $a \cdot | b \wedge b \cdot | c \Rightarrow a \cdot | c$

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

$\equiv$ < def , anidamiento >

$((\exists x, y | : a \cdot x = b \wedge b \cdot y = c) \Rightarrow a \cdot | c$

$\equiv$ < logica >

$((\forall x, y | : a \cdot x = b \wedge b \cdot y = c \Rightarrow a \cdot | c)$

basta mostrar

$a \cdot x = b \wedge b \cdot y = c \Rightarrow a \cdot | c$

$a \cdot x = b \wedge b \cdot y = c$

$\Rightarrow$ < particularizando $y = 1$ entonces $b = c$; reemplazando >

$a \cdot x = c$

$\Rightarrow$ < generalización >

$(\exists x | : a \cdot x = c)$

$\equiv$ < def >

$a \cdot | c$

(32) Antisimetría sobre $\mathbb{N}$

$a \cdot | b \wedge b \cdot | a \Rightarrow a = b \vee a = -b$

Dem.

$a \cdot | b \wedge b \cdot | a \Rightarrow a = b \vee a = -b$

$\equiv$ < def, anidamiento >

$(\exists x, y | : a \cdot x = b \wedge b \cdot y = a) \Rightarrow a = b \vee a = -b$

$\equiv$ < lógica >

$(\forall x, y | : a \cdot x = b \wedge b \cdot y = a \Rightarrow a = b \vee a = -b)$

---

basta mostrar

$a \cdot x = b \wedge b \cdot y = a \Rightarrow a = b \vee a = -b$

$$\boxed{\begin{array}{l} p \wedge q \Rightarrow p \vee q \\ \neg p \vee \neg q \vee p \vee q \equiv true \end{array}}$$

$a \cdot x = b \wedge b \cdot y = a$

$\Rightarrow$ < particularizando $x = 1$, $y = -1$ >

$a = b \wedge a = -b$

$\Rightarrow$ < lógica $p \wedge q \Rightarrow p \vee q$ >

$a = b \vee a = -b$

(33) Múltiplo de múltiplos

$a \cdot | b \Rightarrow a \cdot | b \cdot c$

$\equiv$ < def, lógica >

$(\forall x | : a \cdot x = b \Rightarrow a \cdot | b \cdot c)$

---

basta mostrar $a \cdot x = b \Rightarrow a \cdot | b \cdot c$

$a \cdot x = b$

$\Rightarrow$ < multiplicando por c >

$a \cdot (x \cdot c) = b \cdot c$

$\Rightarrow$ < generalizando >

$(\exists w | : a \cdot w = b \cdot c)$

$\equiv$ < def >

$a \cdot | b \cdot c$

(34) $a \cdot | 0$

dem.

$a \cdot | 0$

$\equiv$ <def>

$(\exists x \mid : a \cdot x = 0)$

$\Leftarrow$ < particularizando $x = 0$ >

$a \cdot 0 = 0$

$\equiv$ < matematicas >

true

(35) $1 \cdot | a$

dem.

$1 \cdot | a$

$\equiv$ <def>

$(\exists x \mid : 1 \cdot x = a)$

$\Leftarrow$ < particularizando $x = a$ >

$1 \cdot a = a$

$\equiv$ < reflexiva; multiplicando >

true

(36) $0 \cdot | a \Rightarrow a = 0$

dem.

$0 \cdot | a \Rightarrow a = 0$

$\equiv$ < def; logica >

$(\forall x \mid : 0 \cdot x = a \Rightarrow a = 0)$

—//—

∴ basta mostrar

$0 \cdot x = a \Rightarrow a = 0$

$0 \cdot x = a$

$\equiv$ < mat >

$0 = a$

$\equiv$ < def. fexiva >

$a = 0$

(37) $a \cdot | 1 \Rightarrow a = 1 \vee a = -1$

dem.

$a \cdot | 1 \Rightarrow a = 1 \vee a = -1$

$\equiv$ < def; logica >

$(\forall x \mid : a \cdot x = 1 \Rightarrow a = 1 \vee a = -1)$

—?—

basta mostrar

$a \cdot x = 1 \Rightarrow a = 1 \vee a = -1$

$a \cdot x = 1$

$\Rightarrow$ < particularización $x = 1$ >

$|a| = 1$

$\equiv$ < def absoluto >

$a = 1 \vee a = -1$

Scanned by CamScanner

(38) $a > 1 \wedge a \cdot | b \Rightarrow \neg(a \cdot | b + 1)$

Supongo $a > 1$, basta mostrar

$a \cdot | b \Rightarrow \neg(a \cdot | b + 1)$

$\equiv$ <def, logica>

$(\forall x |: a \cdot x = b \Rightarrow \neg(a \cdot | b + 1))$

—//—

basta mostrar

$a \cdot x = b \Rightarrow \neg(a \cdot | b + 1)$

Por contradicción $a \cdot x = b \Rightarrow a \cdot | b + 1$

$a > 1$ y tomando $a = 2$, $b = 8$, entonces

$2 \cdot x = 8 \Rightarrow 2 \cdot | 9$

$\equiv$ <matematicas>

false

(39) monotonía simple del producto $a \cdot | b \Rightarrow a \cdot c \cdot | b \cdot c$

Dem.

$a \cdot | b \Rightarrow a \cdot c \cdot | b \cdot c$

$\equiv$ <def; logica>

$(\forall x |: a \cdot x = b \Rightarrow a \cdot c \cdot | b \cdot c)$

—//—

basta mostrar

$a \cdot x = b \Rightarrow a \cdot c \cdot | b \cdot c$

$a \cdot x = b$

$\equiv$ <multiplicando por c>

$(a \cdot c) \cdot x = b \cdot c$

$\Rightarrow$ <generalizando>

$(\exists x |: (a \cdot c) \cdot x = b \cdot c)$

$\equiv$ <def>

$a \cdot c \cdot | b \cdot c$

Scanned by CamScanner

(40) Monotonía doble del producto $a \cdot | b \wedge c \cdot | d \Rightarrow a \cdot c \cdot | b \cdot d$

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

$\equiv$ < def; lógica >

$(\forall x, y |: a \cdot x = b \wedge c \cdot y = d \Rightarrow ac \cdot | bd)$

—— // ——

basta mostrar $a \cdot x = b \wedge c \cdot y = d \Rightarrow ac \cdot | bd$

$a \cdot x = b \wedge c \cdot y = d$

$\Rightarrow$ < multiplicando miembro a miembro >

$(ac)(xy) = (bd)$

$\Rightarrow$ < generalización existencial $w = xy$ >

$(\exists w |: (ac) w = bd)$

$\equiv$ < def >

$ac \cdot | bd$

(42) ley de signos $a \cdot | b = a \cdot | -b = -a \cdot | b$

$a \cdot | b = a \cdot | -b = -a \cdot | b$

$\equiv$ < reescribiendo >

$a \cdot | b = a \cdot | -b \wedge a \cdot | b = -a \cdot | b \wedge a \cdot | -b = -a \cdot | b$

Dem.

$a \cdot | b = a \cdot | -b$

—— // ——

$a \cdot | b$

$\equiv$ < def >

$(\exists x |: a \cdot x = b)$

$\equiv$ < monotonía simple producto (-1) >

$(\exists x |: a \cdot x = -b)$

$\equiv$ < def >

$a \cdot | -b$

Dem. $a \cdot | b = -a \cdot | b$

$a \cdot | b$

$\equiv$ < def, monotonía doble producto >

$(\exists x |: a \cdot x (-1) = b(-1))$

$\equiv$ < monotonía simple producto (-1) >

$(\exists x |: -a \cdot x = b)$

$\equiv$ < def >

$-a \cdot | b$

—— // ——

Dem. $a \cdot | -b = -a \cdot | b$

$a \cdot | -b$

$\equiv$ < def, monotonía doble producto (-1) >

$(\exists x |: -a \cdot x = b)$

$\equiv$ < def >

$-a \cdot | b$

(42) $(a\cdot|\,|b| \equiv a\cdot|b)$ invariancia sobre $|x|$

$|b| \begin{cases} b \\ -b \end{cases}$

$a\cdot|\,|b|$

$\equiv\langle$ def $|x|\rangle$

$a\cdot|b \wedge a\cdot|-b$

$\equiv\langle$ ley signos $\rangle$

$a\cdot|b \wedge a\cdot|b$

$\equiv\langle q\wedge q \equiv q\rangle$

$a\cdot|b$

(43) $a\cdot|b \wedge a\cdot|c \Rightarrow a\cdot|b+c$ Suma multiplos

Dem.

$a\cdot|b \wedge a\cdot|c \Rightarrow a\cdot|b+c$

$\equiv\langle$ def; anidamiento; logica $\rangle$

$(\forall x,y|: a\cdot x = b \wedge a\cdot y = c \Rightarrow a\cdot|b+c)$

——//——

basta mostrar $a\cdot x = b \wedge a\cdot y = c \Rightarrow a\cdot|b+c$

$a\cdot x = b \wedge a\cdot y = c$

$\Rightarrow\langle$ Sumando miembro a miembro $\rangle$

$a\cdot(x+y) = b+c$

$\Rightarrow\langle$ generalización existencial $\rangle$

$(\exists w|: a\cdot w = b+c)$

$\equiv\langle$ def $\rangle$

$a\cdot|b+c$

(44) divisibilidad indirecta $a\cdot|b \equiv (\forall z|: z\cdot|a \Rightarrow z\cdot|b)$

$z\cdot|a \Rightarrow z\cdot|b$

$\equiv\langle$ def; logica $\rangle$

$(\forall x|: z\cdot x = a \Rightarrow z\cdot|b)$

(48) Simetria $\Downarrow$, igual para $\Uparrow$

$a \Downarrow b = b \Downarrow a$

$\equiv$ < divisibilidad indirecta, generalización >

$z \cdot| a \Downarrow b \equiv z \cdot| b \Downarrow a$

$\equiv$ < ax $\Downarrow$ >

$z \cdot| a \wedge z \cdot| b \equiv z \cdot| b \wedge z \cdot| a$

$\equiv$ < conmutatividad y logica >

true

(49) Asociatividad $\Uparrow$, igual para $\Downarrow$

$a \Uparrow (b \Uparrow c) = (a \Uparrow b) \Uparrow c$

$\equiv$ < divisibilidad indirecta, generalización >

$a \Uparrow (b \Uparrow c) \cdot| z \equiv (a \Uparrow b) \Uparrow c \cdot| z$

$\equiv$ < Ax $\Uparrow$ >

$a \cdot| z \wedge b \cdot| z \wedge c \cdot| z \equiv a \cdot| z \wedge b \cdot| z \wedge c \cdot| z$

$\equiv$ < logica >

true

(50) Idempotencia $\Downarrow$, igual para $\Uparrow$

$a \Downarrow a = |a|$

$\equiv$ < divisibilidad indirecta >

$z \cdot| a \Downarrow a \equiv z \cdot| |a|$

$\equiv$ < def $|a| = a$; ax $\Downarrow$ >

$z \cdot| a \equiv z \cdot| a$

$\equiv$ < logica >

true

(51) Absorción $\Uparrow$, igual para $\Downarrow$

$a \Uparrow (b \Downarrow a) = |a|$

$\equiv$ < divisibilidad indirecta >

$a \Uparrow (b \Downarrow a) \cdot| z \equiv |a| \cdot| z$

$\equiv$ < def $|a|$; ax $\Uparrow$ >

$a \cdot| z \wedge b \Downarrow a \cdot| z \equiv a \cdot| z$

$\equiv$ < logica >

$a \cdot| z \Rightarrow b \Downarrow a \cdot| z$

$\equiv$ < desigualdad indirecta >

$b \Downarrow a \cdot| a$

$\equiv$ < cota $\Downarrow$ >

true

(52) cotas $\Downarrow$, igual para $\Uparrow$

$a \Downarrow b \cdot | a \quad \wedge \quad a \Downarrow b \cdot | b$

Dem.

$a \Downarrow b \cdot | a$
$\equiv$ < divisibilidad indirecta >
$z \cdot | a \Downarrow b \Rightarrow z \cdot | a$
$\equiv$ < ax $\Downarrow$ >
$z \cdot | a \wedge z \cdot | b \Rightarrow z \cdot | a$
$\equiv$ < logica >
true

//

$a \Downarrow b \cdot | b$
$\equiv$ < divisibilidad indirs ax $\Downarrow$ >
$z \cdot | a \wedge z \cdot | b \Rightarrow z \cdot | b$
$\equiv$ < logica >
true

(53) Proyección $\Uparrow$, igual $\Downarrow$

$a \cdot | b \equiv a \Uparrow b = |b|$

Dem,

$a \Uparrow b = |b|$
$\equiv$ < divisib. indire, ax $\Uparrow$ >
$a \cdot | z \wedge b \cdot | z \equiv |b| \cdot | z$
$\equiv$ < logica, def $|b|$ >
$b \cdot | z \Rightarrow a \cdot | z$
$\equiv$ < divisb. indirecta multiplos >
$a \cdot | b$

(54) Anulador $\Downarrow$

$\bot \Downarrow a = \bot$
$\equiv$ < divisib. idire, ax $\Downarrow$ >
$z \cdot | \bot \wedge z \cdot | a \equiv z \cdot | \bot$
$\equiv$ < logica >
$z \cdot | \bot \Rightarrow z \cdot | a$
$\equiv$ < divis. Indir >
$\bot \cdot | a$
$\equiv$ < teorema >
true

//

Anulador $\Uparrow$

$0 \Uparrow a = 0$
$\equiv$ < divis. Indir, ax $\Uparrow$ >
$0 \cdot | z \wedge a \cdot | z \equiv 0 \cdot | z$
$\equiv$ < logica >
$0 \cdot | z \Rightarrow a \cdot | z$
$\equiv$ < divis. indir >
$a \cdot | 0$
$\equiv$ < teorema >
true

(55) Identidad $\Downarrow$

$0 \Downarrow a = |a|$

$\equiv \langle$ divis. indir, ax $\Downarrow$, def $|a|$ $\rangle$

$z\cdot|0 \wedge z\cdot|a \equiv z\cdot|a$

$\equiv \langle$ lógica $\rangle$

$z\cdot|a \Rightarrow z\cdot|0$

$\equiv \langle$ divisib. indir $\rangle$

$a\cdot|0$

$\equiv \langle$ def '$\cdot|$' $\rangle$

true

Identidad $\Uparrow$

$1 \Uparrow a = |a|$

$\equiv \langle$ divis. ind, ax $\Uparrow$, def $|a|$ $\rangle$

$1\cdot|z \wedge a\cdot|z \equiv a\cdot|z$

$\equiv \langle$ lógica $\rangle$

$a\cdot|z \Rightarrow 1\cdot|z$

$\equiv \langle$ divis. indir $\rangle$

$1\cdot|a$

$\equiv \langle$ def '$\cdot|$' $\rangle$

true

(56) monotonía sobre $\cdot|$, $\Downarrow$

$a\cdot|b \Rightarrow a\Downarrow c \cdot| b\Downarrow c$

Dem. supongo $a\cdot|b \equiv a\cdot x = b$

$a\Downarrow c \cdot| b\Downarrow c$

$\equiv \langle$ ax $\Downarrow$ $\rangle$

$a\Downarrow c\cdot|b \wedge a\Downarrow c\cdot|c$

$\equiv \langle$ cota $\Downarrow$ $\rangle$

$a\Downarrow c\cdot|b$

$\equiv \langle$ hip. $a\cdot|b$; $a\Downarrow c\cdot|a$; cota $\Downarrow$ $\rangle$

true

$a\cdot|b \Rightarrow a\Uparrow c \cdot| b\Uparrow c$

Dem. supongo $a\cdot|b$

$a\Uparrow c \cdot| b\Uparrow c$

$\equiv \langle$ ax $\Uparrow$ $\rangle$

$a\cdot|b\Uparrow c \wedge c\cdot|b\Uparrow c$

$\equiv \langle$ cota $\Uparrow$ $\rangle$

$a\cdot|b\Uparrow c$

$\equiv \langle$ hip. $a\cdot|b$; $b\cdot|b\Uparrow c$; cota $\Uparrow$ $\rangle$

true

(57) Distributividad de $\cdot$

$c\geq 0 \Rightarrow c\cdot(a\Downarrow b) = c\cdot a \Downarrow c\cdot b$

Dem. supongo $c\geq 0$

$c\cdot(a\Downarrow b) = c\cdot a\Downarrow c\cdot b$

$\equiv \langle$ divisibilidad mutua $\rangle$

$c\cdot(a\Downarrow b)\cdot| c\cdot a\Downarrow c\cdot b$

$\equiv \langle$ Ax $\Downarrow$ $\rangle$

$c\cdot(a\Downarrow b)\cdot|c\cdot a \wedge c\cdot(a\Downarrow b)\cdot|c\cdot b$

$\equiv \langle$ monotonía, cota $\Downarrow$ $\rangle$

true

$c\geq 0 \Rightarrow c\cdot(a\Uparrow b) = c\cdot a\Uparrow c\cdot b$

Supongo $c\geq 0$, divisibilidad mutua basta mostrar.

$c\cdot a\Uparrow c\cdot b \cdot| c\cdot(a\Uparrow b)$

$\equiv \langle$ Ax $\Uparrow$ $\rangle$

$c\cdot a\cdot|c\cdot(a\Uparrow b) \wedge c\cdot b\cdot|c\cdot(a\Uparrow b)$

$\equiv \langle$ monotonía, cota $\Uparrow$ $\rangle$

true

(58) ley de signos $a \Downarrow -a = |a|$

$a \Downarrow -a = |a|$

$\equiv$ < divisibilidad mutua >

$|a| \cdot | a \Downarrow -a$

$\equiv$ < Ax $\Downarrow$ >

$|a| \cdot | a \wedge |a| \cdot | -a$

$\equiv$ < ley de signos sobre '$\cdot|$' ; reflexividad >

true

(59) Invarlancia sobre valor absoluto $\Uparrow$

$a \Uparrow b = |a| \Uparrow |b|$

$\equiv$ < divis. indirecta >

$a \Uparrow b \cdot| z \equiv |a| \Uparrow |b| \cdot| z$

$\equiv$ < Ax $\Uparrow$ >

$a \cdot| z \wedge b \cdot| z \equiv |a| \cdot| z \wedge |b| \cdot| z$

$\equiv$ < def $|a| = a$ ó $|a| = -a$ (igual b) >

$a \cdot| z \wedge b \cdot| z \equiv (a \cdot| z \vee -a \cdot| z) \wedge (b \cdot| z \vee -b \cdot| z)$

$\equiv$ < ley de signos, y logica >

true

(60) invariancia bajo suma

$a \Downarrow b = a \Downarrow (b-a) = a \Downarrow (b+a)$

Dem. $a \Downarrow b = a \Downarrow (b + k \cdot a)$ por divisibilidad mutua

(1) $a \Downarrow b \cdot| a \Downarrow (b + k \cdot a)$

$\equiv$ < ax $\Downarrow$ >

$a \Downarrow b \cdot| a \wedge a \Downarrow b \cdot| (b + k \cdot a)$

$\equiv$ < cota $\Downarrow$ >

$a \Downarrow b \cdot| (b + k \cdot a)$

$\Leftarrow$ < suma multiplos >

$a \Downarrow b \cdot| b \wedge a \Downarrow b \cdot| k \cdot a$

$\equiv$ < cota $\Downarrow$ >

$a \Downarrow b \cdot| k \cdot a$

$\Leftarrow$ < transitividad >

$a \Downarrow b \cdot| a \wedge a \cdot| k \cdot a$

$\equiv$ < cota, multiplo de multiplos >

true

(1·) $a \Downarrow (b + k \cdot a) \cdot| a \Downarrow b$

$\equiv$ < ax $\Downarrow$ >

$a \Downarrow (b + k \cdot a) \cdot| a \wedge a \Downarrow (b + k \cdot a) \cdot| b$

$\equiv$ < cota $\Downarrow$ >

$a \Downarrow (b + k \cdot a) \cdot| b$

$\Leftarrow$ < suma multiplos >

$a \Downarrow (b + k \cdot a) \cdot| b + k a \wedge a \Downarrow (b + k \cdot a) \cdot| b - k \cdot a$

$\equiv$ < cota $\Downarrow$; multiplo de multiplos; transitividad >

true

(61) factorización $(a \Downarrow b)\cdot(a \Uparrow b) = |a\cdot b|$

Dem. divisibilidad mutua

$|(a \Downarrow b)(a \Uparrow b)| \cdot | |ab|$

$\equiv$ < distribución de $\cdot$; def valor absoluto >

$(a \Downarrow b)a \Uparrow (a \Downarrow b)b \cdot | ab$

$\equiv$ < distribución de $\cdot$ >

$(a^2 \Downarrow ba) \Uparrow (ab \Downarrow b^2) \cdot | ab$

$\equiv$ < Ax $\Uparrow$ >

$a^2 \Downarrow ba \cdot | ab \wedge ab \Downarrow b^2 \cdot | ab$

$\equiv$ < cota $\Downarrow$ >

true

$|ab| \cdot | (a \Downarrow b)(a \Uparrow b)$

$\equiv$ < distribución $(\cdot)$; def valor absoluto >

$ab \cdot | (a \Uparrow b)a \Downarrow b(a \Uparrow b)$

$\equiv$ < distribución $(\cdot)$ >

$ab \cdot | (a^2 \Uparrow ba) \Downarrow (ba \Uparrow b^2)$

$\equiv$ < ax $\Downarrow$ >

$ab \cdot | a^2 \Uparrow ba \wedge ab \cdot | ba \Uparrow b^2$

$\equiv$ < cota $\Uparrow$ >

true

(62) invariancia por residuo $a \Downarrow b = b \Downarrow (a \underline{mod} b)$

dem. por divisibilidad indirecta

$z \cdot | a \Downarrow b$

$\equiv$ < Ax $\Downarrow$ >

$z \cdot | a \wedge z \cdot | b$

$\equiv$ < algoritmo de la división >

$z \cdot | b \cdot (a \underline{div} b) + a \underline{mod} b \wedge z \cdot | b$

$\equiv$ < Suma de multiplos, multiplo de multiplos >

$z \cdot | a \underline{mod} b \wedge z \cdot | b$

$\equiv$ < axioma $\Downarrow$ >

$z \cdot | b \Downarrow (a \underline{mod} b)$

(63) $a \overset{m}{=} a$ Reflexividad

$a \overset{m}{=} a$

$\equiv$ < def >

$m \cdot | a - a$

$\equiv$ < $a - a = 0$ y $x \cdot | 0$ >

true

Scanned by CamScanner

(64) Simetría $a \overset{m}{\equiv} b \equiv b \overset{m}{\equiv} a$

$a \overset{m}{\equiv} b$

$\equiv$ <def>

$m \cdot | a-b$

$\equiv$ < multiplicando x-1>

$-m \cdot | b-a$

$\equiv$ <def>

$b \overset{m}{\equiv} a$

(65) Transitividad $a \overset{m}{\equiv} b \wedge b \overset{m}{\equiv} c \Rightarrow a \overset{m}{\equiv} c$

$a \overset{m}{\equiv} b \wedge b \overset{m}{\equiv} c$

$\equiv$ <def>

$m \cdot | a-b \wedge m \cdot | b-c$

$\Rightarrow$ <suma multiplos>

$m \cdot | a-c$

$\equiv$ <def>

$a \overset{m}{\equiv} c$

6 (66) $a \overset{m}{\equiv} b \Rightarrow a+c \overset{m}{\equiv} b+c$

Suponemos $a \overset{m}{\equiv} b$

$a+c \overset{m}{\equiv} b+c$

$\equiv$ <def>

$m \cdot | a+c-b-c$

$\equiv$ <aritmetica>

$m \cdot | a-b$

$\equiv$ <sup>

true

(67) $a \overset{m}{\equiv} b \wedge c \overset{m}{\equiv} d \Rightarrow a+c \overset{m}{\equiv} b+d$

Dem.

$a \overset{m}{\equiv} b \wedge c \overset{m}{\equiv} d$

$\equiv$ < def >

$m \cdot | a-b \wedge m \cdot | c-d$

$\Rightarrow$ < suma multiplos >

$m \cdot | (a+c)-(b+d)$

$\equiv$ < def >

$a+c \overset{m}{\equiv} b+d$

(68) $a \overset{m}{\equiv} b \Rightarrow a \cdot c \overset{m}{\equiv} b \cdot c$

Sup. $a \overset{m}{\equiv} b$

$a \cdot c \overset{m}{\equiv} b \cdot c$

$\equiv$ < def >

$m \cdot | a \cdot c - b \cdot c$

$\equiv$ < sup y multiplo de multiplos >

true

(69) $a \overset{m}{\equiv} b \wedge c \overset{m}{\equiv} d \Rightarrow a \cdot c \overset{m}{\equiv} b \cdot d$

Supongo $m \cdot | a-b$, $m \cdot | c-d$ entonces

$m \cdot | a \wedge m \cdot | -b \wedge m \cdot | c \wedge m \cdot | -d$

Dem. $a \cdot c \overset{m}{\equiv} b \cdot d$

$a \cdot c \overset{m}{\equiv} b \cdot d$

$\equiv$ < def >

$m \cdot | a \cdot c - b \cdot d$

$\Leftarrow$ < suma multiplos >

$m \cdot | a \cdot c \wedge m \cdot | -b \cdot d$

$\equiv$ < sup >

true

Scanned by CamScanner

(70) $a \overset{m}{\equiv} b \Rightarrow a^n \overset{m}{\equiv} b^n$

Por inducción

Caso base $n=1$

$a^1 \overset{m}{\equiv} b^1 \Leftarrow a \overset{m}{\equiv} b \rightarrow$ True

Caso inductivo

$a^{n+1} \overset{m}{\equiv} b^{n+1} \Leftarrow a \overset{m}{\equiv} b$

$a \cdot a^n \overset{m}{\equiv} b \cdot b^n \Leftarrow a \overset{m}{\equiv} b$

$a \overset{m}{\equiv} b \Rightarrow a \overset{m}{\equiv} b \rightarrow$ True

(71) $a \cdot c \overset{m \cdot c}{\equiv} b \cdot c \equiv a \overset{m}{\equiv} b$

Dem.

$a \cdot c \overset{mc}{\equiv} bc$

$\equiv$ <def>

$m \cdot c \cdot | \, c \cdot (a-b)$

$\equiv$ <cancelación>

$m \cdot | \, a-b$

$\equiv$ <def>

$a \overset{m}{\equiv} b$

(72) $a \perp b \wedge a \cdot | \, b \cdot c \Rightarrow a \cdot | \, c$

$ax + by = 1$

$by = 1 - ax$

Supongo $a \perp b$, $a \cdot | \, bc$

Por lema Bézout $a \perp b = 1 = a \downarrow b = ax + by$ (x)

$a \cdot | \, c$

$\equiv$ <multiplicando por 1>

$a \cdot | \, c\,(ax + by)$

$\equiv$ <distributiva>

$a \cdot | \, cax + cby$

$\equiv$ <suma múltiplos; múltiplo de múltiplos>

true

(123) $a \perp b \wedge a \cdot | c \wedge b \cdot | c \Rightarrow a \cdot b \cdot | c$

supongo $a \perp b \wedge a \cdot | c \wedge b \cdot | c$

$a \perp b = 1 = ax + by$

dem. $a \cdot b \cdot | c$

$a \cdot b \cdot | c$

$\equiv$ < multiplicando por 1 >

$a \cdot b \cdot | \; axc + byc$

$\equiv$ < suma multiplos ; transitiva ; multiplo de multiplos >

true

(124) $a \perp n \wedge a \overset{n}{=} b \Rightarrow b \perp n$

Scanned by CamScanner

Aritmetica multiplicativa.

Ax. $a \cdot | b \equiv (\exists_z | : a \cdot z = b)$

Teo. $a \cdot | a$

$a \cdot | a$

$\equiv \langle Ax \rangle$

$(\exists_z | : a \cdot z = a)$

Testigo $z = 1$, entonces $a = a$

Teo. $a \cdot | b \wedge b \cdot | c \Rightarrow a \cdot | c$

$a \cdot | b \wedge b \cdot | c$

$\equiv \langle Ax \rangle$

$(\exists_z | : a \cdot z = b) \wedge (\exists_y | : b \cdot y = c)$ $(\exists_z | : a \cdot z = b \wedge b \cdot \cancel{z} = c)$

$\equiv$??

$a \cdot z = b$

$b \cdot z = c$

$a \cdot z \cdot z = c$

$a \cdot z = c$

Teo. $a \cdot | b \equiv a \cdot c \cdot | b \cdot c$

$a \cdot | b$

$\equiv \langle def \rangle$

$(\exists_z | : a \cdot z = b)$

$\Rightarrow \langle$ monotonía de $\exists$ y producto $\rangle$

$(\exists_z | : a \cdot c \cdot z = b \cdot c)$

$\equiv \langle def \rangle$

$a \cdot c \cdot | b \cdot c$

$P \Rightarrow P \wedge q$

p	q	p∧q	p∨q	p⇒p∧q	p⇒q
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	T
F	F	F	F	T	T

Teo. $a \cdot | b \cdot a \Leftarrow a \cdot | a$??

Supongo $a \cdot | a$

$a \cdot | b \cdot a$

$\equiv \langle def \rangle$

$(\exists_z | : a \cdot z = b \cdot a)$

$\Leftarrow \langle$ particularización $z = b \rangle$

$(\exists_b | : a \cdot b = b \cdot a)$

$\equiv \langle$ logica $\rangle$

true

Scanned by CamScanner

Teo. $a \mid b \Rightarrow a \mid b \cdot c$

$\equiv \langle def \rangle$

$(\exists z \mid : a \cdot z = b) \Rightarrow a \mid b \cdot c$

$\equiv \langle logica \rangle$

$(\exists z \mid : a \cdot z = b \Rightarrow a \mid b \cdot c)$

Dem. Transito.

$a \cdot z = b$

$\Rightarrow \langle leibniz \rangle$

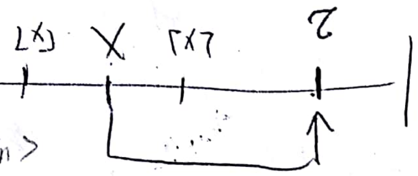
$(z \cdot c) = (b \cdot c)$

$\Rightarrow \langle generalizacion \rangle$

$(\exists w \mid a \cdot w = b \cdot c)$

$\equiv \langle def \rangle$

$a \mid b \cdot c$



$\lceil x \rceil \geq \lceil x \rceil$

$x \geq \lceil x \rceil$

$x \geq z \equiv \lceil x \rceil \geq z$

$\phi \wedge \psi \Rightarrow \phi$

$\neg\phi \vee \neg\psi \vee \phi$

Ax. $(\forall z : \mathbb{Z} \mid : z \mid m \Downarrow n \equiv z \mid m \wedge z \mid n)$

Ax. $(\forall z : \mathbb{Z} \mid : m \Uparrow n \mid z \equiv m \mid z \wedge n \mid z)$

Teo. $a \Downarrow b \mid a \wedge a \Downarrow b \mid b$

$a \Downarrow b \mid a$

$\equiv \langle Ax \rangle$

$(\exists x \mid : a \Downarrow b \cdot z = a)$??

$\Rightarrow \langle \ \rangle$??

$a \Downarrow b = a$

$z \mid a \Downarrow b \mid \Rightarrow z \mid a$

$z \mid a \wedge z \mid b \Rightarrow z \mid a$

$\equiv$ true

$p \wedge q \Rightarrow p$

$\neg p \vee q \vee p$

Teo. $b \mid a \equiv a \Uparrow b = |a|$

$\equiv$

$(\forall z \mid : |a| \mid z \equiv a \Uparrow b \mid z)$

$\equiv \langle def \rangle$

$(\forall z \mid : a \mid z \equiv a \mid z \wedge b \mid z)$

$\equiv \langle logica \rangle$

$(\forall z : a \mid z \Rightarrow b \mid z)$

$\equiv \langle div. \rangle$

$b \mid a$

$\phi \wedge \psi \equiv \phi$

$\equiv \phi \Rightarrow \psi$

$(z \mid a \Rightarrow z \mid b)$

$a \mid b$

$(h \Rightarrow \not\equiv)_L$

$\equiv$

$z > h$

① $a \uparrow b = c \equiv a \leq c \wedge b \leq c \wedge (\forall z \mid : a \leq z \wedge b \leq z \Rightarrow c \leq z)$

$a \leq c \wedge b \leq c \wedge (\forall z \mid : a \leq z \wedge b \leq z \Rightarrow c \leq z)$

$\equiv$ < def >

$a \uparrow b \leq c \wedge a \uparrow b \leq z \Rightarrow c \leq z$

$\equiv$ < desigualdad indirecta >

$a \uparrow b \leq c \wedge c \leq a \uparrow b$

$\equiv$ < precedencia mutua >

$a \uparrow b = c$

② $x \downarrow y = x \equiv x \uparrow y = y$

$x \uparrow y = y$

$\equiv$ < metodos indirectos >

$x \uparrow y \leq z \equiv y \leq z$

$\equiv$ < Axioma $\uparrow$ >

$x \leq z \wedge y \leq z \equiv y \leq z$

$\equiv$ < logica >

$y \leq z \Rightarrow x \leq z$

$\equiv$ < desigualdad indirecta >

$x \leq y$

$\equiv$ < $x \leq x \equiv true$; $a \wedge true \equiv a$ >

$x \leq y \wedge x \leq x$

$\equiv$ < Axioma $\downarrow$ >

$x \leq y \downarrow x$

$\equiv$ < $x \downarrow y \leq x \equiv true$; $a \wedge true \equiv a$ >

$x \leq y \downarrow x \wedge x \downarrow y \leq x$

$\equiv$ < precedencia mutua >

$y \downarrow x = x$

$x \downarrow y = x$

$\equiv$

$x \downarrow y \leq x \wedge x \leq x \downarrow y$

$\equiv$

$x \leq x \wedge x \leq y$

③ $x \downarrow y = x \vee x \downarrow y = y$

$x \downarrow y = x \vee x \downarrow y = y$

$\equiv$ < precedencia mutua >

$x \downarrow y \leq x \wedge x \leq x \downarrow y \vee x \downarrow y \leq y \wedge y \leq x \downarrow y$

$\equiv$ < cota $\downarrow$; axioma $\downarrow$ >

$x \leq x \wedge x \leq y \vee y \leq x \wedge y \leq y$

$\equiv$ < $x \leq x \equiv true$; $y \leq y \equiv true$ >

$y \leq y \vee y \leq x$

$\equiv$ < precedencia >

True

(4) $z < x \downarrow y \equiv z < x \wedge z < y$

$z < x \downarrow y$

$\equiv$ ⟨ aritmetica ⟩

$\neg(x \downarrow y \leq z)$

$\equiv$ ⟨ contraposición ⟩

$\neg(x \leq z \vee y \leq z)$

$\equiv$ ⟨ $\neg$ ⟩

$\neg(x \leq z) \wedge \neg(y \leq z)$

$\equiv$ ⟨ arItm ⟩

$z < x \wedge z < y$

(5) $a \downarrow b = b \downarrow a$

$z \leq a \downarrow b \equiv z \leq b \downarrow a$

$z \leq a \downarrow b$

$\equiv$

$z \leq a \wedge z \leq b$

$\equiv$

$z \leq b \downarrow a$

(6) $a \downarrow (a \uparrow b) = a$

$a \leq a \downarrow (a \uparrow b)$

$\equiv$

$a \leq a \wedge a \leq a \uparrow b$

$\equiv$

true

$a \downarrow (a \uparrow b) \leq a$

$\equiv$

true

(7) $a \downarrow b \leq a \wedge a \downarrow b \leq b$

$a \downarrow b \leq a$

$\equiv$

$z \leq a \downarrow b \Rightarrow z \leq a$

$\equiv$

$z \leq a \wedge z \leq b \Rightarrow z \leq a$

$\equiv$

true

$a \downarrow b \leq b$

$\equiv$

$z \leq a \wedge z \leq b \Rightarrow z \leq b$

$\equiv$

true

(8) $a \downarrow b = a \vee a \downarrow b = b$

$a \downarrow b = a \quad \vee \; a \downarrow b = b$

$\equiv$ < metodos indirectos >

$z \leq a \wedge z \leq b \equiv z \leq a \quad \vee \quad z \leq a \wedge z \leq b \equiv z \leq b$

$\equiv$

$z \leq a \Rightarrow z \leq b \quad \vee \quad z \leq b \Rightarrow z \leq a$

$\equiv$

$\neg(z \leq a) \vee z \leq b \quad \vee \quad \neg(z \leq b) \vee z \leq a$

$\equiv$

true

(9) $a \leq b \equiv a \downarrow b = a$

$a \downarrow b = a$

$\equiv$ < precedencia >

$a \downarrow b \leq a \quad \wedge \quad a \leq a \downarrow b$

$\equiv$ < cota sup $\downarrow$ >

$a \leq a \quad \wedge \quad a \leq b$

$\equiv$ < logica >

$a \leq b$

(10) $a \downarrow b \leq c \equiv a \leq c \vee b \leq c$

$a \downarrow b \leq c$

$\equiv$

$z \leq a \downarrow b \Rightarrow z \leq c$

$\equiv$

$z \leq a \wedge z \leq b \Rightarrow z \leq c$

$\equiv$

$z \leq a \Rightarrow z \leq c \quad \vee \quad z \leq b \Rightarrow z \leq c$

$\equiv$

$a \leq c \quad \vee \quad b \leq c$

$p \wedge q \Rightarrow r \equiv p \Rightarrow r \vee q \Rightarrow r$

$\neg p \vee \neg q \vee r \vee r$

$\neg p \vee r \quad \vee \quad \neg q \vee r$

$p \Rightarrow r \quad \vee \quad q \Rightarrow r$

(11) $c + (a \uparrow b) = c + a \uparrow c + b$

$c + (a \uparrow b) \leq z$

$\equiv$

$a \uparrow b \leq z - c$

$\equiv$

$a \leq z - c \quad \wedge \quad b \leq z - c$

$\equiv$

$a + c \leq z \quad \wedge \quad b + c \leq z$

$\equiv$

$a + c \uparrow b + c \leq z$

(12) $c \geq 0 \Rightarrow c(a \uparrow b) = ca \uparrow cb$

Supongo $c \geq 0$

$c(a \uparrow b) \leq ca \uparrow cb$

$\equiv$

$c(a \uparrow b) \leq ca \lor c(a \uparrow b) \leq cb$

$\Leftarrow$ <sup $c \geq 0$; semimonotonía $\cdot \leq$>

$a \uparrow b \leq a \lor a \uparrow b \leq b$

$\equiv$ <contrapositiva>

$a \uparrow b \leq a \uparrow b$

$\equiv$

true

$ca \uparrow cb \leq c(a \uparrow b)$

$\equiv$

$ca \leq c(a \uparrow b) \land cb \leq c(a \uparrow b)$

$\Leftarrow$ <semimonotonía $\cdot$>

$a \leq a \uparrow b \land b \leq a \uparrow b$

$\equiv$ <cota $\uparrow$>

true

(13) $-(a \downarrow b) = -a \uparrow -b$

$-(a \downarrow b) \leq z$

$\equiv$ <aritmética>

$-z \leq a \downarrow b$

$\equiv$ <ax>

$-z \leq a \land -z \leq b$

$\equiv$ <aritm>

$-a \leq z \land -b \leq z$

$\equiv$ <Ax>

$-a \uparrow -b$

(14) $a \downarrow b \leq a \uparrow b$

$a \downarrow b$

$\leq$

a

$\leq$

$a \uparrow b$

(15) $a \leq b \Rightarrow a \uparrow c \leq b \uparrow c$

$\equiv$ $a \uparrow c \leq b \uparrow c$

$\equiv$ <ax>

$a \leq b \uparrow c \land c \leq b \uparrow c$

$\equiv$ <cota>

$a \leq b \uparrow c$

$\equiv$

$a \leq b \lor a \leq c$

$\equiv$ <sup>

True

Scanned by CamScanner

(16) $\lceil x \rceil - 1 < x \leq \lceil x \rceil$

$\lceil x \rceil \leq z \equiv x \leq z$

$z \leq \lfloor x \rfloor \equiv z \leq x$

$\lceil x \rceil - 1 < x \quad \wedge \quad x \leq \lceil x \rceil$

$\equiv$ <Ax ; arith>

$\lceil x \rceil < x + 1 \quad \wedge \quad \lceil x \rceil \leq \lceil x \rceil$

$\equiv$

$\neg (x \leq \lceil x \rceil - 1)$

$\equiv$

$\neg (\lceil x \rceil \leq \lceil x \rceil - 1)$

$\equiv$

$\lceil x \rceil - 1 < \lceil x \rceil$

$\equiv$

true

(17) $\lfloor k \rfloor = k = \lceil k \rceil$

$\lfloor k \rfloor = k \quad \wedge \quad k = \lceil k \rceil$

$\equiv$ <igualdad indirecta>

$z \leq \lfloor k \rfloor \equiv z \leq k \quad \wedge \quad k \leq z \equiv \lceil k \rceil \leq z$

$\equiv$ <Ax>

true

(18) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$

$z \leq \lfloor x + n \rfloor \equiv z \leq \lfloor x \rfloor + n$

$z \leq \lfloor x + n \rfloor$

$\equiv$ <Ax>

$z \leq x + n$

$\equiv$ <arith>

$z - n \leq x$

$\equiv$ <Ax>

$z - n \leq \lfloor x \rfloor$

$\equiv$ <arith>

$z \leq \lfloor x \rfloor + n$

(19) $\frac{m}{n} = (\uparrow k : \mathbb{Z} \mid k \cdot n \leq m : k)$

$\frac{m}{n} = \lfloor \frac{m}{n} \rfloor$

$(\uparrow k : \mathbb{Z} \mid k \cdot n \leq m : k) = \lfloor \frac{m}{n} \rfloor$

$(\uparrow k : \mathbb{Z} \mid k \cdot n \leq m : k) \leq z$

$\equiv$ < Ax generalizado >

$(\forall_k : \mathbb{Z} \mid k \cdot n \leq m : k \leq z)$

(20) $n = \lfloor \sqrt{x} \rfloor \equiv n^2 \leq x < (n+1)^2$

$n^2 \leq x \wedge x < (n+1)^2$

$\equiv$ < mat >

$n \leq \sqrt{x} \wedge \sqrt{x} < n+1$

$\equiv$

$n \leq \lfloor x \rfloor \wedge \neg(n+1 \leq \sqrt{x})$

$\equiv$

$n \leq \lfloor x \rfloor \wedge \neg(n+1 \leq \lfloor x \rfloor)$

$\equiv$

$n \leq \lfloor x \rfloor \wedge \neg((n+1) \leq \lfloor x \rfloor + 1)$

$\equiv$

$n \leq \lfloor x \rfloor \wedge \neg(n \leq \lfloor x \rfloor)$

$\equiv$

$n \leq \lfloor x \rfloor \wedge \lfloor x \rfloor < n$

$n^2 + 2n + 1$

$n \leq \lfloor \sqrt{x} \rfloor \wedge \lfloor \sqrt{x} \rfloor \leq n$

$\equiv$

$n^2 \leq x \wedge \lfloor \sqrt{x} \rfloor \leq n+1$

$\equiv$

$n^2 \leq x \wedge \neg(n+1 < \lfloor \sqrt{x} \rfloor)$

$\equiv$

$n^2 \leq \lfloor x \rfloor \wedge \lfloor \sqrt{x} \rfloor \leq n+1$

$\equiv$

$n^2 \leq \lfloor x \rfloor \wedge$

(21) $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$

$z \leq \lfloor \sqrt{\lfloor x \rfloor} \rfloor$

$\equiv$

$z \leq \sqrt{\lfloor x \rfloor}$

$\equiv$

$z^2 \leq \lfloor x \rfloor$

$\equiv$

$z^2 \leq x$

$\equiv$

$z \leq \sqrt{x}$

$\equiv$

$z \leq \lfloor \sqrt{x} \rfloor$

(22) $f(-x) = -\lfloor x \rfloor$

(23) $\lfloor \frac{p}{q} \rfloor = \lceil \frac{m}{n} \rceil$

$z \leq \lfloor \frac{p}{q} \rfloor \equiv z \leq \lceil \frac{m}{n} \rceil$

$\lfloor \frac{5}{3} \rfloor = \lceil \frac{3}{7} \rceil$

(24) $|a-b| = a \uparrow b - a \downarrow b$

$a \uparrow b - (a \downarrow b)$

$= \langle$ ley signos $\rangle$

$a \uparrow b + -a \uparrow -b$

$= \langle$ distribución $\rangle$

$a + (-a \uparrow -b) \uparrow b + (-a \uparrow -b)$

$= \langle$ distribución $\rangle$

$(a - a \uparrow a - b) \uparrow (b - a \uparrow b - b)$

$= \langle$ mat $\rangle$

$a - b \uparrow b - a$

$= \langle$ def $\rangle$

$|a-b|$

$-(a \downarrow b) = -a \uparrow -b$

(25) $|a+b| \leq |a| + |b|$

$|a| + |b|$

$= \langle$ def $\rangle$

$|a \uparrow -a| + b \uparrow -b$

$= \langle$ distribución $\rangle$

$b + (a \uparrow -a) \uparrow -b + (a \uparrow -a)$

$=$

$(b + a \uparrow b - a) \uparrow (-b + a \uparrow -b - a)$

$= \langle b + a > b - a \; ; -b + a > -b - a)$

$b + a \uparrow -b + a$

$\geq$

$b + a \uparrow -(a+b)$

$= \langle$ def $\rangle$

$|a+b|$

$-(b+a) = -b - a$

$-b + a$

$-b - a = -(b+a)$

$a + b \uparrow -(a+b)$

(26) $||a|| = |a|$

$||a||$

= <def>

$|a|\uparrow|-a|$

= <def>

$a\uparrow -a \uparrow a\uparrow -a$

= <idempotencia>

$a\uparrow -a$

= <def>

$|a|$

(27) $|a \cdot b| = |a| \cdot |b|$

$|a| \cdot |b|$

= <def>

$a\uparrow -a \cdot b\uparrow -b$

= <semidist>

$(a\uparrow -a \cdot b)\uparrow(a\uparrow -a \cdot -b)$

= <semidis>

$(ab\uparrow -ab)\uparrow(-ab\uparrow ab)$

= <idemp>

$ab\uparrow -ab$

= def

$|a \cdot b|$

(28) $a \geq 0 \equiv |a| = a$

$a \geq 0 \Rightarrow |a| = a$

$|a| = a$

≡ <igualdad indirecta>

$|a| \leq z \equiv a \leq z$

≡ <def abs>

$a\uparrow -a \leq z \equiv a \leq z$

≡ <ax>

$a \leq z \wedge -a \leq z \equiv a \leq z$

≡ <logica>

$a \leq z \Rightarrow -a \leq z$

≡ <dem. indirecta>

$-a \leq a$

≡ <mat>

true

(29) $|a| = a\downarrow -a \equiv a \geq 0$

$|8| = 8\downarrow -8 \equiv a \geq 0$

$-8 \qquad 8 \geq 0$

Scanned by CamScanner

Nombre: Ana María Rincón Casallas

4,6

① (a) $a^2 \downarrow b^2 \leq a \cdot b$

Dem.

$a^2 \downarrow b^2 \leq a \cdot b$

$\equiv \langle$ contraposición $\rangle$

$a^2 \leq a \cdot b \vee b^2 \leq a \cdot b$

$\equiv \langle$ aritmetica $\rangle$

$a \leq b \vee b \leq a$

$\equiv \langle$ lógica ; $\cancel{\phi \vee \neg\phi \equiv true}$ $\rangle$ $\leq$ es lineal

true

(b) $(a \uparrow b) \cdot (a \downarrow b) = a \cdot b$

9/10

Dem. precedencia mutua

$(a \uparrow b) \cdot (a \downarrow b) \leq a \cdot b$

$\equiv \langle$ distributiva $\rangle$

$((a \downarrow b) \cdot a) \uparrow ((a \downarrow b) \cdot b) \leq a \cdot b$

$\equiv \langle$ distributiva $\rangle$

$(a^2 \downarrow ab) \uparrow (ab \downarrow b^2) \leq a \cdot b$

$\equiv \langle$ Ax. $\uparrow \rangle$

$a^2 \downarrow ab \leq ab \wedge ab \downarrow b^2 \leq ab$

$\equiv \langle$ cota $\downarrow \rangle$

true

//

$a \cdot b \leq (a \uparrow b)(a \downarrow b)$

$\equiv \langle$ distributiva $\rangle$

$a \cdot b \leq ((a \uparrow b) \cdot a) \downarrow ((a \uparrow b) \cdot b)$

$\equiv \langle$ distributiva $\rangle$

$a \cdot b \leq (a^2 \uparrow ab) \downarrow (ab \uparrow b^2)$

$\equiv \langle$ Ax $\downarrow \rangle$

$ab \leq a^2 \uparrow ab \wedge ab \leq ab \uparrow b^2$

$\equiv \langle$ cota $\uparrow \rangle$

true

② $\lceil x + n \rceil = n + \lceil x \rceil$

Dem. igualdad indirecta, basta mostrar

$\lceil x + n \rceil \leq z \equiv n + \lceil x \rceil \leq z$

—— // ——

$\lceil x + n \rceil \leq z$

10

$\equiv \langle$ Ax $\lceil x \rceil \rangle$

$x + n \leq z$

$\equiv \langle$ aritmetica $\rangle$

$x \leq z - n$

$\equiv \langle$ ax $\lceil x \rceil \rangle$

$\lceil x \rceil \leq z - n$

$\equiv \langle$ aritmetica $\rangle$

$n + \lceil x \rceil \leq z$

③ $a \cdot | b \equiv a \Uparrow b = b$

Dem.

$a \Uparrow b = b$

$\equiv$ < divisibilidad indirecta >

$(\forall z | : a \Uparrow b \cdot | z \equiv b \cdot | z)$

$\equiv$ < Ax $\Uparrow$ >

$(\forall z | : a \cdot | z \wedge b \cdot | z \equiv b \cdot | z)$

$\equiv$ < lógica >

$(\forall z | : b \cdot | z \Rightarrow a \cdot | z)$

$\equiv$ < divisibilidad indirecta >

$a \cdot | b$

8/10

⑤ $m^2 \perp n^2 \Rightarrow m \perp n$

Supongo $m^2 \perp n^2$

(*) $m^2 \perp n^2 \equiv m^2 \Downarrow n^2 = 1 = m^2 x + n^2 y$ < lema Bézout ; def >

$m \perp n$

$\equiv$ < def >

$m \Downarrow n = 1$

Basta mostrar, divisibilidad indirecta

$m \Downarrow n \cdot | 1 \wedge 1 \cdot | m \Downarrow n$

$\equiv$ < $1 \cdot | z$ >

$m \Downarrow n \cdot | 1$

$\equiv$ < (*) >

$m \Downarrow n \cdot | m^2 x + n^2 y$

$\Leftarrow$ $\cancel{\equiv}$ < Suma de multiplos >

$m \Downarrow n \cdot | m^2 x \wedge m \Downarrow n \cdot | n^2 y$

$\equiv$ < multiplo de multiplos ; cota $\Downarrow$ >

true

9/10

Scanned by CamScanner

Nombre: Ana María Rincón Casallas

⑥ $4 \cdot| m^2 - n^2$; $m = 2k+1$ y $n = 2l+1$, supongo m y n impares.

$4 \cdot| m^2 + n^2$

$\equiv$ <reemplazando m, n>

$4 \cdot| (2k+1)^2 - (2l+1)^2$

$\equiv$ <algebra, aritmetica>

$4 \cdot| 4(k^2 + k - l^2 - l)$

$\equiv$ <multiplo de multiplos>

true

10