CS250: Discrete Math for Computer Science

L13: Number Theory: Divisibility

Vocabulary of Number Theory, $\Sigma_{\#\text{thy}}$

$$\Sigma_{\#\text{thy}} \overset{\text{def}}{=} (\leq^2 \text{ [infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

Vocabulary of Number Theory, $\Sigma_{\#\mathrm{thy}}$

$$\Sigma_{\#\mathrm{thy}} \stackrel{\mathrm{def}}{=} (\leq^2 \text{ [infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ $\in$ World$[\Sigma_{\#\mathrm{thy}}]$; for now, **concentrate on $\mathbf{Z}$.**

Vocabulary of Number Theory, $\Sigma_{\#thy}$

$$\Sigma_{\#thy} \stackrel{\text{def}}{=} (\leq^2 \text{[infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ $\in$ $\mathrm{World}[\Sigma_{\#thy}]$; for now, **concentrate on Z**.

Definition x **divides** y $(x|y)$ iff $\exists z\, (x \cdot z = y)$.

Vocabulary of Number Theory, $\Sigma_{\#\mathrm{thy}}$

$$\Sigma_{\#\mathrm{thy}} \stackrel{\mathrm{def}}{=} (\leq^2 \text{[infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ $\in$ World[$\Sigma_{\#\mathrm{thy}}$]; for now, **concentrate on Z**.

Definition x **divides** y $(x|y)$ iff $\exists z\,(x \cdot z = y)$.

Examples: $3|6$, $2|6$, $4 \not| 6$, $1|1$, $1|2$, $1|3$

Vocabulary of Number Theory, $\Sigma_{\#thy}$

$$\Sigma_{\#thy} \stackrel{\text{def}}{=} (\leq^2 \text{ [infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ $\in$ $\mathrm{World}[\Sigma_{\#thy}]$; for now, **concentrate on Z.**

Definition x **divides** y $(x|y)$ iff $\exists z\, (x \cdot z = y)$.

Examples: $3|6$, $2|6$, $4 \not| 6$, $1|1$, $1|2$, $1|3$

Proposition $\forall y\, (1|y)$

Vocabulary of Number Theory, $\Sigma_{\#\text{thy}}$

$$\Sigma_{\#\text{thy}} \stackrel{\text{def}}{=} (\leq^2 \text{[infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ $\in$ $\text{World}[\Sigma_{\#\text{thy}}]$; for now, **concentrate on Z**.

Definition x **divides** y $(x|y)$ iff $\exists z\ (x \cdot z = y)$.

Examples: $3|6$, $2|6$, $4 \not| 6$, $1|1$, $1|2$, $1|3$

Proposition $\forall y\ (1|y)$

Proof.
Let $y_0 \in \mathbf{Z}$ be **arbitrary**

$\square$

Vocabulary of Number Theory, $\Sigma_{\#thy}$

$$\Sigma_{\#thy} \stackrel{\text{def}}{=} (\leq^2 \text{[infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ $\in$ $\mathrm{World}[\Sigma_{\#thy}]$; for now, **concentrate on Z**.

Definition x **divides** y $(x|y)$ iff $\exists z\,(x \cdot z = y)$.

Examples: $3|6$, $2|6$, $4 \not| 6$, $1|1$, $1|2$, $1|3$

Proposition $\forall y\,(1|y)$

Proof.
Let $y_0 \in \mathbf{Z}$ be **arbitrary**

$1 \cdot y_0 = y_0$ Axiom for $\mathbf{Z}$: 1 is identity for $\cdot$

$\square$

Vocabulary of Number Theory, $\Sigma_{\#\text{thy}}$

$$\Sigma_{\#\text{thy}} \stackrel{\text{def}}{=} (\leq^2 \text{[infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R} \in \text{World}[\Sigma_{\#\text{thy}}]$; for now, **concentrate on Z**.

Definition x **divides** y $(x|y)$ iff $\exists z\,(x \cdot z = y)$.

Examples: $3|6$, $2|6$, $4 \not| 6$, $1|1$, $1|2$, $1|3$

Proposition $\forall y\,(1|y)$

Proof.

Let $y_0 \in \mathbf{Z}$ be **arbitrary**

$1 \cdot y_0 = y_0$	Axiom for **Z**: 1 is identity for $\cdot$
$\exists z\,(1 \cdot z = y_0)$	$\exists$-i

$\square$

Vocabulary of Number Theory, $\Sigma_{\#\text{thy}}$

$$\Sigma_{\#\text{thy}} \stackrel{\text{def}}{=} (\leq^2 \text{ [infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ $\in$ World[$\Sigma_{\#\text{thy}}$]; for now, **concentrate on Z**.

Definition x **divides** y $(x|y)$ iff $\exists z\, (x \cdot z = y)$.

Examples: $3|6$, $2|6$, $4 \not| 6$, $1|1$, $1|2$, $1|3$

Proposition $\forall y\, (1|y)$

Proof.
Let $y_0 \in \mathbf{Z}$ be **arbitrary**

$1 \cdot y_0 = y_0$	Axiom for **Z**: 1 is identity for $\cdot$
$\exists z\, (1 \cdot z = y_0)$	$\exists$-i
$1\|y_0$	Def. of **divides**

$\square$

Vocabulary of Number Theory, $\Sigma_{\#\text{thy}}$

$$\Sigma_{\#\text{thy}} \stackrel{\text{def}}{=} (\leq^2 \text{[infix]}; 0, 1, +^2\text{[infix]}, \cdot^2\text{[infix]})$$

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ $\in$ $\text{World}[\Sigma_{\#\text{thy}}]$;   for now, **concentrate on Z.**

Definition x **divides** y $(x|y)$ iff $\exists z\,(x \cdot z = y)$.

Examples: $3|6$, $2|6$, $4 \not| 6$, $1|1$, $1|2$, $1|3$

Proposition $\forall y\,(1|y)$

Proof.

Let $y_0 \in \mathbf{Z}$ be **arbitrary**

$1 \cdot y_0 = y_0$	Axiom for **Z**: 1 is identity for $\cdot$
$\exists z\,(1 \cdot z = y_0)$	$\exists$-i
$1 \| y_0$	Def. of **divides** $\|$
$\forall y\,(1\|y)$	$\forall$-i, since y_0 was **arbitrary**

$\square$

$x|y \quad \hookrightarrow \quad \exists z\,(x \cdot z = y)$

Proposition 1. $\forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

Proof.

Let $x_0, y_0, z_0 \in \mathbf{Z}$ be **arbitrary** s.t. $x_0|y_0 \wedge x_0|z_0$

$\square$

$x|y \quad \hookrightarrow \quad \exists z\,(x \cdot z = y)$

Proposition 1. $\forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

Proof.

Let $x_0, y_0, z_0 \in \mathbf{Z}$ be **arbitrary** s.t. $x_0|y_0 \wedge x_0|z_0$

$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$ Def. of **divides** $|$

$\square$

$x|y \quad \hookrightarrow \quad \exists z\,(x \cdot z = y)$

Proposition 1. $\forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

Proof.

Let $x_0, y_0, z_0 \in \mathbf{Z}$ be **arbitrary** s.t. $x_0|y_0 \wedge x_0|z_0$

$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$ — Def. of **divides** $|$

$(x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0)$ — **hypothesis**

$\square$

Proposition 1. $\forall xyz\,(x|y \wedge x|z \;\to\; x|(y+z))$

Proof.

Let $x_0, y_0, z_0 \in \mathbf{Z}$ be **arbitrary** s.t. $x_0|y_0 \wedge x_0|z_0$

$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$ Def. of **divides** $|$

$(x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0)$ **hypothesis**

$(x_0 \cdot (u_0 + v_0) = y_0 + z_0)$ **Z** distributive

$\square$

Proposition 1. $\forall xyz\,(x|y \wedge x|z \;\to\; x|(y+z))$

Proof.

Let $x_0, y_0, z_0 \in \mathbf{Z}$ be **arbitrary** s.t. $x_0|y_0 \wedge x_0|z_0$

$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	Def. of **divides** $\vert$
$(x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0)$	**hypothesis**
$(x_0 \cdot (u_0 + v_0) = y_0 + z_0)$	**Z** distributive
$\exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i

$\square$

$x|y \quad \hookrightarrow \quad \exists z\,(x \cdot z = y)$

Proposition 1. $\forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

Proof.

Let $x_0, y_0, z_0 \in \mathbf{Z}$ be **arbitrary** s.t. $x_0|y_0 \wedge x_0|z_0$

$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	Def. of **divides** $\vert$
$(x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0)$	**hypothesis**
$(x_0 \cdot (u_0 + v_0) = y_0 + z_0)$	$\mathbf{Z}$ distributive
$\exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i
$x_0\vert(y_0 + z_0)$	Def. of **divides** $\vert$

$\square$

Proposition 1. $\forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

Proof.

Let $x_0, y_0, z_0 \in \mathbf{Z}$ be **arbitrary** s.t. $x_0|y_0 \wedge x_0|z_0$	
$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	Def. of **divides** $\mid$
$(x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0)$	**hypothesis**
$(x_0 \cdot (u_0 + v_0) = y_0 + z_0)$	$\mathbf{Z}$ distributive
$\exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i
$x_0|(y_0 + z_0)$	Def. of **divides** $\mid$
$x_0|(y_0 + z_0)$	$\exists$-e

$\square$

Proposition 1. $\forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

Proof.

Let $x_0, y_0, z_0 \in \mathbf{Z}$ be **arbitrary** s.t. $x_0|y_0 \wedge x_0|z_0$	
$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	Def. of **divides** $\mid$
$(x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0)$	**hypothesis**
$(x_0 \cdot (u_0 + v_0) = y_0 + z_0)$	$\mathbf{Z}$ distributive
$\exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i
$x_0|(y_0 + z_0)$	Def. of **divides** $\mid$
$x_0|(y_0 + z_0)$	$\exists$-e
$\forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$	$\forall$-i

$\square$

$x|y \quad \hookrightarrow \quad \exists z\,(x \cdot z = y)$

Γ_{Z} is the set of axioms in Epp that we use about **Z**.

$x|y \quad \hookrightarrow \quad \exists z\,(x \cdot z = y)$

Γ_Z is the set of axioms in Epp that we use about **Z.**

Prop. 1 $\quad \Gamma_Z \vdash \forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

$x|y \quad \hookrightarrow \quad \exists z\,(x \cdot z = y)$

Γ_Z is the set of axioms in Epp that we use about **Z**.

Prop. 1 $\quad \Gamma_Z \vdash \forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

1	$x_0 \mid y_0 \wedge x_0 \mid z_0$	
2	$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0$	
4	$x_0 \cdot (u_0 + v_0) = y_0 + z_0$	Γ_Z, 3
5	$\exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i, 4
6	$x_0 \mid (y_0 + z_0)$	$\hookrightarrow$, 5
7	$x_0 \mid (y_0 + z_0)$	$\exists$-e, 2, 3–6

1	$\quad\quad x_0 \mid y_0 \wedge x_0 \mid z_0$	
2	$\quad\quad \exists uv\,(x_0 \cdot u = y_0 \ \wedge\ x_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$\quad\quad\quad\quad x_0 \cdot u_0 = y_0 \ \wedge\ x_0 \cdot v_0 = z_0$	
4	$\quad\quad\quad\quad x_0 \cdot (u_0 + v_0) = y_0 + z_0$	Γ_Z, 3
5	$\quad\quad\quad\quad \exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i, 4
6	$\quad\quad\quad\quad x_0 \mid (y_0 + z_0)$	$\hookrightarrow$, 5
7	$\quad\quad x_0 \mid (y_0 + z_0)$	$\exists$-e, 2, 3–6
8	$x_0 \mid y_0 \wedge x_0 \mid z_0 \ \rightarrow\ x_0 \mid (y_0 + z_0)$	$\boxed{\phantom{\rightarrow\text{-i}}}$, 1–7

1	$\quad x_0 \mid y_0 \wedge x_0 \mid z_0$	
2	$\quad \exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$\qquad x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0$	
4	$\qquad x_0 \cdot (u_0 + v_0) = y_0 + z_0$	Γ_Z, 3
5	$\qquad \exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i, 4
6	$\qquad x_0 \mid (y_0 + z_0)$	$\hookrightarrow$, 5
7	$\quad x_0 \mid (y_0 + z_0)$	$\exists$-e, 2, 3–6
8	$x_0 \mid y_0 \wedge x_0 \mid z_0 \;\rightarrow\; x_0 \mid (y_0 + z_0)$	$\boxed{}$, 1–7

iClicker 13.1 Is line 8 correct and if so, using what ND rule?

A: No **B: Yes, Γ_Z** **C: Yes, $\rightarrow$-i** **D: Yes, $\forall$-i**

1	$x_0 \vert y_0 \wedge x_0 \vert z_0$	
2	$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0$	
4	$x_0 \cdot (u_0 + v_0) = y_0 + z_0$	Γ_Z, 3
5	$\exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i, 4
6	$x_0 \vert (y_0 + z_0)$	$\hookrightarrow$, 5
7	$x_0 \vert (y_0 + z_0)$	$\exists$-e, 2, 3–6
8	$x_0 \vert y_0 \wedge x_0 \vert z_0 \;\rightarrow\; x_0 \vert (y_0 + z_0)$	$\rightarrow$-i, 1–7
9	$\forall z\,(x_0 \vert y_0 \wedge x_0 \vert z \;\rightarrow\; x_0 \vert (y_0 + z))$	$\boxed{\phantom{\forall\text{-i}}}$, 8

1	$\quad x_0 \mid y_0 \wedge x_0 \mid z_0$	
2	$\quad \exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$\qquad x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0$	
4	$\qquad x_0 \cdot (u_0 + v_0) = y_0 + z_0$	Γ_Z, 3
5	$\qquad \exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i, 4
6	$\qquad x_0 \mid (y_0 + z_0)$	$\hookrightarrow$, 5
7	$\quad x_0 \mid (y_0 + z_0)$	$\exists$-e, 2, 3–6
8	$x_0 \mid y_0 \wedge x_0 \mid z_0 \;\rightarrow\; x_0 \mid (y_0 + z_0)$	$\rightarrow$-i, 1–7
9	$\forall z\,(x_0 \mid y_0 \wedge x_0 \mid z \;\rightarrow\; x_0 \mid (y_0 + z))$	$\boxed{}$, 8

iClicker 13.2 Is line 9 correct and if so, using what ND rule?

A: No **B: Yes, Γ_Z** **C: Yes, $\rightarrow$-i** **D: Yes, $\forall$-i**

Prop. 1 $\Gamma_Z \vdash \forall xyz\,(x|y \wedge x|z \;\rightarrow\; x|(y+z))$

1	$x_0 \mid y_0 \wedge x_0 \mid z_0$	
2	$\exists uv\,(x_0 \cdot u = y_0 \;\wedge\; x_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0 \;\wedge\; x_0 \cdot v_0 = z_0$	
4	$x_0 \cdot (u_0 + v_0) = y_0 + z_0$	Γ_Z, 3
5	$\exists w\,(x_0 \cdot w = y_0 + z_0)$	$\exists$-i, 4
6	$x_0 \mid (y_0 + z_0)$	$\hookrightarrow$, 5
7	$x_0 \mid (y_0 + z_0)$	$\exists$-e, 2, 3–6
8	$x_0 \mid y_0 \wedge x_0 \mid z_0 \;\rightarrow\; x_0 \mid (y_0 + z_0)$	$\rightarrow$-i, 1–7
9	$\forall xyz\,(x \mid y \wedge x \mid z \;\rightarrow\; x \mid (y+z))$	$\forall$-i, 8

Prop. 2 $\Gamma_Z \vdash \forall xyz\,(x|y \;\rightarrow\; x|(y \cdot z))$

Prop. 2 $\Gamma_Z \vdash \forall xyz\,(x|y \;\rightarrow\; x|(y \cdot z))$

1	$x_0 \| y_0$	
2	$\exists u\; x_0 \cdot u = y_0$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0$	
4	$y_0 \cdot z_0 = y_0 \cdot z_0$	$\boxed{}$

Prop. 2 $\Gamma_Z \vdash \forall xyz\,(x|y \rightarrow x|(y \cdot z))$

1	$x_0 \| y_0$		
2	$\exists u\; x_0 \cdot u = y_0$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0$	
4	$y_0 \cdot z_0 = y_0 \cdot z_0$	$\boxed{}$

iClicker 13.3 Is line 4 correct and if so, using what ND rule?

A: No **B: Yes, Γ_Z** **C: Yes, $=$-i** **D: Yes, $=$-e**

Prop. 2 $\Gamma_Z \vdash \forall xyz\,(x|y \;\rightarrow\; x|(y \cdot z))$

1	$\quad \mid \quad \mid\; \underline{x_0 \mid y_0}$		
2	$\quad \mid \quad \mid\; \exists u\; x_0 \cdot u = y_0$		$\hookrightarrow$, 1
3	$\quad \mid \quad \mid \quad \mid\; \underline{x_0 \cdot u_0 = y_0}$		
4	$\quad \mid \quad \mid \quad \mid\; y_0 \cdot z_0 = y_0 \cdot z_0$		$=$-i
5	$\quad \mid \quad \mid \quad \mid\; (x_0 \cdot u_0) \cdot z_0 = y_0 \cdot z_0$		$=$-e, 3, 4
6	$\quad \mid \quad \mid \quad \mid\; x_0 \cdot (u_0 \cdot z_0) = y_0 \cdot z_0$		Γ_Z, 5
7	$\quad \mid \quad \mid \quad \mid\; \exists w\, (x_0 \cdot w = y_0 \cdot z_0)$		$\exists$-i, 6
8	$\quad \mid \quad \mid \quad \mid\; x_0 \mid (y_0 \cdot z_0)$		$\hookrightarrow$, 7

Prop. 2 $\Gamma_Z \vdash \forall xyz\,(x|y \rightarrow x|(y \cdot z))$

1	$\quad\quad \underline{x_0 \mid y_0}$	
2	$\quad\quad \exists u\, x_0 \cdot u = y_0$	$\hookrightarrow$, 1
3	$\quad\quad\quad\quad \underline{x_0 \cdot u_0 = y_0}$	
4	$\quad\quad\quad\quad y_0 \cdot z_0 = y_0 \cdot z_0$	$=$-i
5	$\quad\quad\quad\quad (x_0 \cdot u_0) \cdot z_0 = y_0 \cdot z_0$	$=$-e, 3, 4
6	$\quad\quad\quad\quad x_0 \cdot (u_0 \cdot z_0) = y_0 \cdot z_0$	Γ_Z, 5
7	$\quad\quad\quad\quad \exists w\,(x_0 \cdot w = y_0 \cdot z_0)$	$\exists$-i, 6
8	$\quad\quad\quad\quad x_0 \mid (y_0 \cdot z_0)$	$\hookrightarrow$, 7
9	$\quad\quad x_0 \mid (y_0 \cdot z_0)$	$\exists$-e, 2, 3–8
10	$x_0 \mid y_0 \rightarrow x_0 \mid (y_0 \cdot z_0)$	$\rightarrow$-i, 1–9
11	$\forall xyz\,(x|y \rightarrow x|(y \cdot z))$	$\forall$-i, 10

Prop. 3 $\Gamma_Z \vdash \forall xyz\,(x|y \wedge y|z \rightarrow x|z)$

1	$x_0\|y_0 \wedge y_0\|z_0$	
2	$\exists uv\,(x_0 \cdot u = y_0 \wedge y_0 \cdot v = z_0)$	$\hookrightarrow$, 1
3	$x_0 \cdot u_0 = y_0 \wedge y_0 \cdot v_0 = z_0$	
4	$y_0 \cdot v_0 = y_0 \cdot v_0$	$=$-i
5	$(x_0 \cdot u_0) \cdot v_0 = y_0 \cdot v_0$	$=$-e, 3, 4
6	$x_0 \cdot (u_0 \cdot v_0) = y_0 \cdot v_0$	Γ_Z, 5
7	$x_0 \cdot (u_0 \cdot v_0) = z_0$	$=$-e, 3, 6
8	$\exists u\, x_0 \cdot u = z_0$	$\exists$-i, 7
9	$x_0\|z_0$	$\hookrightarrow$, 8
10	$x_0\|z_0$	$\exists$-e, 2, 3–9
11	$x_0\|y_0 \wedge y_0\|z_0 \rightarrow x_0\|z_0$	$\rightarrow$-i, 1–10
12	$\forall xyz\,(x\|y \wedge y\|z \rightarrow x\|z)$	$\forall$-i, 11