144 Let x be an integer variable. Prove the refinement

(a) $x'=0 \ \Leftarrow\ $ **if** $x=0$ **then** ok **else** $x:= x-1.\ x'=0$ **fi**

(b) $P \ \Leftarrow\ $ **if** $x=0$ **then** ok **else** $x:= x-1.\ t:= t+1.\ P$ **fi**

where $P \ = \ x'=0 \ \land$ **if** $x\ge 0$ **then** $t' = t+x$ **else** $t'=\infty$ **fi**

After trying the question, scroll down to the solution.

(a) $x'=0 \;\Leftarrow\; \textbf{if } x=0 \textbf{ then } ok \textbf{ else } x:=x-1.\; x'=0 \textbf{ fi}$

§ By Cases. First case:

$x=0 \land ok \;\Rightarrow\; x'=0$ expand ok
$= \quad x=0 \land x'=x \land t'=t \;\Rightarrow\; x'=0$ context
$= \quad x=0 \land x'=x \land t'=t \;\Rightarrow\; x=x$ reflexive
$= \quad x=0 \land x'=x \land t'=t \;\Rightarrow\; \top$ base
$= \quad \top$

Last case:

$x\ne 0 \land (x:=x-1.\; t:=t+1.\; x'=0)$ substitution twice
$= \quad x\ne 0 \land x'=0$ specialization
$\Rightarrow \quad x'=0$

(b) $P \;\Leftarrow\; \textbf{if } x=0 \textbf{ then } ok \textbf{ else } x:=x-1.\; t:=t+1.\; P \textbf{ fi}$
where $P \;=\; x'=0 \land \textbf{if } x\ge 0 \textbf{ then } t'=t+x \textbf{ else } t'=\infty \textbf{ fi}$

§ By Parts, and part (a) proved one part, so we just have to prove

$\textbf{if } x\ge 0 \textbf{ then } t'=t+x \textbf{ else } t'=\infty \textbf{ fi} \;\Leftarrow\; \textbf{if } x=0 \textbf{ then } ok \textbf{ else } x:=x-1.\; t:=t+1.\; P \textbf{ fi}$

And we prove it by Cases. First case:

$x=0 \land ok \;\Rightarrow\; \textbf{if } x\ge 0 \textbf{ then } t'=t+x \textbf{ else } t'=\infty \textbf{ fi}$ expand ok
$= \quad x=0 \land x'=x \land t'=t \;\Rightarrow\; \textbf{if } x\ge 0 \textbf{ then } t'=t+x \textbf{ else } t'=\infty \textbf{ fi}$ context
$= \quad x=0 \land x'=x \land t'=t \;\Rightarrow\; \textbf{if } 0\ge 0 \textbf{ then } t=t+0 \textbf{ else } t'=\infty \textbf{ fi}$ reflexive, case base
$= \quad x=0 \land x'=x \land t'=t \;\Rightarrow\; t=t$ reflexive
$= \quad x=0 \land x'=x \land t'=t \;\Rightarrow\; \top$ base
$= \quad \top$

Last case:

$x\ne 0 \land (x:=x-1.\; t:=t+1.\; \textbf{if } x\ge 0 \textbf{ then } t'=t+x \textbf{ else } t'=\infty \textbf{ fi})$ substitution twice
$= \quad x\ne 0 \land \textbf{if } x-1\ge 0 \textbf{ then } t'=t+1+x-1 \textbf{ else } t'=\infty \textbf{ fi}$ simplify
$= \quad x\ne 0 \land \textbf{if } x>0 \textbf{ then } t'=t+x \textbf{ else } t'=\infty \textbf{ fi}$ context: $x\ne 0 \Rightarrow (x>0 = x\ge 0)$
$= \quad x\ne 0 \land \textbf{if } x\ge 0 \textbf{ then } t'=t+x \textbf{ else } t'=\infty \textbf{ fi}$ specialization
$\Rightarrow \quad \textbf{if } x\ge 0 \textbf{ then } t'=t+x \textbf{ else } t'=\infty \textbf{ fi}$