304 Prove

(a) $\top$ is an invariant for specification S .

(b) $\bot$ is an invariant for specification S .

(c) Assertion A is an invariant for ok .

(d) $x+y = 5$ is an invariant for $(x{:=}\ x+1.\ \ y{:=}\ y-1)$ where the variables are x and y .

(e) $x\ge 0$ is an invariant for $x{:=}\ x+1$ where the variable is x .

(f)√ $y=x^2$ is an invariant for $(x{:=}\ x+1.\ \ y{:=}\ y + 2\times x - 1)$ where the variables are x and y .

(g) $a\times x^2 + b\times x + c = 0$ is an invariant for $(x{:=}\ a\times x + b.\ \ x{:=}\ -x/a)$ where the variable is x .

(h) $f = n!$ is an invariant for $(n{:=}\ n+1.\ \ f{:=}\ f\times n)$ where f and n are natural variables and $!$ is factorial.

After trying the question, scroll down to the solution.

(a) $\top$ is an invariant for specification S .

§	$\forall\sigma, \sigma'\cdot (\top\Rightarrow\top) \Leftarrow S$	base or identity
$=$	$\forall\sigma, \sigma'\cdot \top\Leftarrow S$	base
$=$	$\forall\sigma, \sigma'\cdot \top$	identity
$=$	$\top$	

I could have said that I'll work inside the quantifiers, like this:

	$(\top\Rightarrow\top) \Leftarrow S$	base or identity
$=$	$\top\Leftarrow S$	base
$=$	$\top$	

and that's what I'll do for most of the other parts of this question.

(b) $\bot$ is an invariant for specification S .

§	$(\bot\Rightarrow\bot) \Leftarrow S$	base
$=$	$\top\Leftarrow S$	base
$=$	$\top$	

(c) Assertion A is an invariant for ok .

§	$\forall\sigma, \sigma'\cdot (A\Rightarrow A') \Leftarrow ok$	
$=$	$\forall\sigma, \sigma'\cdot (A\Rightarrow A') \Leftarrow \sigma'=\sigma$	one-point law
$=$	$\forall\sigma\cdot (A\Rightarrow A)$	reflexive law
$=$	$\forall\sigma\cdot \top$	idempotent law
$=$	$\top$	

(d) $x+y = 5$ is an invariant for $(x{:=}\ x+1.\ \ y{:=}\ y-1)$ where the variables are x and y .

§	$(x+y = 5 \ \Rightarrow\ x'+y' = 5) \Leftarrow (x{:=}\ x+1.\ \ y{:=}\ y-1)$	replace final assignment
$=$	$(x+y = 5 \ \Rightarrow\ x'+y' = 5) \Leftarrow (x{:=}\ x+1.\ \ x'=x \wedge y'=y-1)$	substitution law
$=$	$(x+y = 5 \ \Rightarrow\ x'+y' = 5) \Leftarrow (x'=x+1 \wedge y'=y-1)$	context
$=$	$(x+y = 5 \ \Rightarrow\ x+1+y-1 = 5) \Leftarrow (x'=x+1 \wedge y'=y-1)$	arithmetic
$=$	$(x+y = 5 \ \Rightarrow\ x+y = 5) \Leftarrow (x'=x+1 \wedge y'=y-1)$	reflexive
$=$	$\top \Leftarrow (x'=x+1 \wedge y'=y-1)$	base
$=$	$\top$	

(e) $x\ge 0$ is an invariant for $x{:=}\ x+1$ where the variable is x .

§	$(x\ge 0 \Rightarrow x'\ge 0) \Leftarrow (x{:=}\ x+1)$	replace assignment
$=$	$(x\ge 0 \Rightarrow x'\ge 0) \Leftarrow x'=x+1$	context
$=$	$(x\ge 0 \Rightarrow x+1\ge 0) \Leftarrow x'=x+1$	connection (Galois)
$=$	$x \le x+1 \Leftarrow x'=x+1$	cancellation
$=$	$0\le 1 \Leftarrow x'=x+1$	order
$=$	$\top \Leftarrow x'=x+1$	base
$=$	$\top$	

(f)√ $y=x^2$ is an invariant for $(x:= x+1.\ y:= y + 2\times x - 1)$ where the variables are x and y.

§ $(y=x^2 \Rightarrow y'=x'^2) \Leftarrow (x:= x+1.\ y:= y + 2\times x - 1)$ replace last assignment

$= (y=x^2 \Rightarrow y'=x'^2) \Leftarrow (x:= x+1.\ x'=x \land y' = y + 2\times x - 1)$ substitution

$= (y=x^2 \Rightarrow y'=x'^2) \Leftarrow x'=x+1 \land y' = y + 2\times(x+1) - 1$ arithmetic

$= (y=x^2 \Rightarrow y'=x'^2) \Leftarrow x'=x+1 \land y' = y + 2\times x + 1$ context

$= (y=x^2 \Rightarrow (y + 2\times x + 1)=(x+1)^2) \Leftarrow x'=x+1 \land y' = y + 2\times x + 1$ arithmetic

$= (y=x^2 \Rightarrow (y + 2\times x + 1)=(x+1)^2) \Leftarrow x'=x+1 \land y' = y + 2\times x + 1$

arithmetic and cancellation

$= (y=x^2 \Rightarrow y=x^2) \Leftarrow x'=x+1 \land y' = y + 2\times x + 1$ reflexive, base

$= \top$

(g) $a\times x^2 + b\times x + c = 0$ is an invariant for $(x:= a\times x + b.\ x:= -x/a)$ where the variable is x.

§ $(a\times x^2 + b\times x + c = 0 \Rightarrow a\times x'^{\,2} + b\times x' + c = 0) \Leftarrow (x:= a\times x + b.\ x:= -x/a)$

replace final assignment

$= (a\times x^2 + b\times x + c = 0 \Rightarrow a\times x'^{\,2} + b\times x' + c = 0) \Leftarrow (x:= a\times x + b.\ x' = -x/a)$

substitution law

$= (a\times x^2 + b\times x + c = 0 \Rightarrow a\times x'^{\,2} + b\times x' + c = 0) \Leftarrow x' = -(a\times x + b)/a$ context

$= (a\times x^2 + b\times x + c = 0 \Rightarrow a\times(-(a\times x + b)/a)^2 + b\times(-(a\times x + b)/a) + c = 0)$

$\Leftarrow x' = -(a\times x + b)/a$ arithmetic

$= (a\times x^2 + b\times x + c = 0 \Rightarrow a\times x^2 + b\times x + c = 0) \Leftarrow x' = -(a\times x + b)/a$ reflexive, base

$= \top$

(h) $f = n!$ is an invariant for $(n:= n+1.\ f:= f\times n)$ where f and n are natural variables and $!$ is factorial.

§ $(f = n! \Rightarrow f' = n'!) \Leftarrow (n:= n+1.\ f:= f\times n)$ expand last assignment

$= (f = n! \Rightarrow f' = n'!) \Leftarrow (n:= n+1.\ f'=f\times n \land n'=n)$ substitution law

$= (f = n! \Rightarrow f' = n'!) \Leftarrow f'=f\times(n+1) \land n'=n+1$ context

$= (f = n! \Rightarrow f\times(n+1) = (n+1)!) \Leftarrow f'=f\times(n+1) \land n'=n+1$ definition of $!$

$= (f = n! \Rightarrow f\times(n+1) = n!\times(n+1)) \Leftarrow f'=f\times(n+1) \land n'=n+1$ cancellation

$= (f = n! \Rightarrow f = n!) \Leftarrow f'=f\times(n+1) \land n'=n+1$ reflexive, base

$= \top$