376 Prove the following; quantifications are over *nat* unless stated otherwise.

(a) $\neg\exists i, j\cdot\ j\ne 0\ \land\ 2^{1/2} = i/j$ The square roots of 2 are irrational.

(b) $\forall n\cdot (\Sigma i\colon 0,..n\cdot 1)\ =\ n$

(c) $\forall n\cdot (\Sigma i\colon 0,..n\cdot i)\ =\ n\times(n-1)/2$

(d) $\forall n\cdot (\Sigma i\colon 0,..n\cdot i^2)\ =\ n\times(n-1)\times(2\times n - 1)/6$

(e) $\forall n\cdot (\Sigma i\colon 0,..n\cdot i^3)\ =\ (\Sigma i\colon 0,..n\cdot i)^2$

(f) $\forall n\cdot (\Sigma i\colon 0,..n\cdot 2^i)\ =\ 2^n - 1$

(g) $\forall n\cdot (\Sigma i\colon 0,..n\cdot i\times 2^i)\ =\ (n-2)\times 2^n + 2$

(h) $\forall n\cdot (\Sigma i\colon 0,..n\cdot (-2)^i)\ =\ (1 - (-2)^n) / 3$

(i) $\forall n\cdot n\ge 3\ \Rightarrow\ 2\times n^3 > 3\times n\times(n+1)$

(j) $\forall n\cdot n\ge 4\ \Rightarrow\ 3^n > n^3$

(k) $\forall n\cdot n\ge 4\ \Rightarrow\ n! > 2^n$ where ! is factorial

(l) $\forall n\cdot n\ge 10\ \Rightarrow\ 2^n > n^3$

(m) $\forall a, d\cdot \exists q, r\cdot d\ne 0\ \Rightarrow\ r<d\ \land\ a = q\times d + r$

(n) $\forall a, b\cdot a\le b\ \Rightarrow\ (\Sigma i\colon a,..b\cdot 3^i) = (3^b - 3^a)/2$

(o) $\forall n\cdot\ (n+1)^{nat} :\ nat\times n + 1$

(p) $\forall n\cdot (\Sigma i\colon 0,..n\cdot i\times(i+1))\ =\ (n-1)\times n\times(n+1)/3$

(q) $\forall n\cdot (\Sigma i\colon 0,..n\cdot (-1)^i \times i^2)\ =\ -(-1)^n \times (n-1) \times n / 2$

(r) $\forall n\cdot (\Sigma i\colon 0,..n\cdot 1/((i+1)\times(i+2)))\ =\ n/(n+1)$

After trying the question, scroll down to the solution.

(a) $\neg\exists i,j\cdot\ j{\ne}0\ \land\ 2^{1/2} = i/j$ The square root of 2 is irrational.

§ For this question only, I define f: $nat \rightarrow xnat$ so that $f\,n$ is the number of times that 2 is a factor of n .

$$f(2{\times}n)\ =\ 1 + f\,n$$
$$f(2{\times}n + 1)\ =\ 0$$

From that definition we easily see $f\,0 = \infty$, $f\,1 = 0$, $f\,2 = 1$, $f\,3 = 0$, $f\,4 = 2$, and so on. Now I need to prove a lemma:

$$f(x{\times}y)\ =\ f\,x + f\,y$$

The proof of the lemma uses induction.

if *even x*
then $\exists n\cdot\quad x = 2{\times}n$
$\land\quad f(x{\times}y)$
$=\ f(2{\times}n{\times}y)$ — use definition of f
$=\ 1 + f(n{\times}y)$ — either $n{\times}y = 2{\times}n{\times}y = 0$ and we apply a base case, or else $n{\times}y < 2{\times}n{\times}y$ and we use the induction hypothesis
$=\ 1 + f\,n + f\,y$ — use definition of f again
$=\ f(2{\times}n) + f\,y$
$=\ f\,x + f\,y$
else if *even y*
then by a similar proof $f(x{\times}y) = f\,x + f\,y$
else *odd x* $\land$ *odd y*
$\Rightarrow \exists n, m\cdot\quad x = 2{\times}n{+}1\ \land\ y = 2{\times}m{+}1$
$\land\quad f(x{\times}y)$
$=\ f(4{\times}n{\times}m + 2{\times}n + 2{\times}m + 1)$ — use definition of f
$=\ 0$ — use definition of f twice more
$=\ f(2{\times}n{+}1) + f(2{\times}m{+}1)$
$=\ f\,x + f\,y$ **fi fi**

Now the main theorem:

$\neg\exists i,j\cdot\ j{\ne}0\ \land\ 2^{1/2} = i/j$ — duality
$=\quad \forall i,j\cdot\ 2^{1/2} = i/j\ \Rightarrow\ j{=}0$ — square both sides of equation
$\Leftarrow\quad \forall i,j\cdot\ i^2 = 2{\times}j^2\ \Rightarrow\ j{=}0$

Now work inside the quantification, starting with the equation.

$i^2 = 2{\times}j^2$
$\Rightarrow\quad f(i^2) = f(2{\times}j^2)$ — now use the lemma
$=\quad 2{\times}(f\,i)\ =\ f\,2 + 2{\times}(f\,j)$
$=\quad 2{\times}(f\,i)\ =\ 1 + 2{\times}(f\,j)$ — we can't have an even number equal to an odd number
$=\quad f\,i = f\,j = \infty$
$=\quad i = j = 0$

(b) $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot\ 1)\ =\ n$

§ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot\ 1)\ =\ n$ — induction
$\Leftarrow\quad (\Sigma i{:}\ 0,..0\cdot\ 1) = 0\ \land\ \forall n\cdot (\Sigma i{:}\ 0,..n\cdot\ 1) = n\ \Rightarrow\ (\Sigma i{:}\ 0,..n{+}1\cdot\ 1)\ =\ n{+}1$ — sum over empty domain; divide domain of final sum; simplify
$=\quad \forall n\cdot (\Sigma i{:}\ 0,..n\cdot\ 1) = n\ \Rightarrow\ (\Sigma i{:}\ 0,..n\cdot\ 1){+}1\ =\ n{+}1$ — use antecedent as context then drop
$\Leftarrow\quad \forall n\cdot\ n{+}1\ =\ n{+}1$ — identity
$=\quad \top$

(c) $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i) = n\times(n-1)/2$

§ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i) = n\times(n-1)/2$ — induction

$\Leftarrow$ $(\Sigma i{:}\ 0,..0\cdot i) = 0\times(0-1)/2$

$\wedge$ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i) = n\times(n-1)/2 \;\Rightarrow\; (\Sigma i{:}\ 0,..n{+}1\cdot i) = (n+1)\times(n+1-1)/2$

sum over empty domain; divide domain of final sum; simplify

$=$ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i) = n\times(n-1)/2 \;\Rightarrow\; (\Sigma i{:}\ 0,..n\cdot i)+n = (n+1)\times n/2$

use antecedent as context, then drop antecedent

$\Leftarrow$ $\forall n\cdot n\times(n-1)/2 + n = (n+1)\times n/2$ — arithmetic

$=$ $\top$

(d) $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i^2) = n\times(n-1)\times(2\times n-1)/6$

(e) $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i^3) = (\Sigma i{:}\ 0,..n\cdot i)^2$

§ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i^3) = (\Sigma i{:}\ 0,..n\cdot i)^2$ — induction

$\Leftarrow$ $(\Sigma i{:}\ 0,..0\cdot i^3) = (\Sigma i{:}\ 0,..0\cdot i)^2$

$\wedge$ $(\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i^3) = (\Sigma i{:}\ 0,..n\cdot i)^2 \;\Rightarrow\; (\Sigma i{:}\ 0,..n{+}1\cdot i^3) = (\Sigma i{:}\ 0,..n{+}1\cdot i)^2)$

sum over empty domain; divide domain of final two sums into $0,..n$ and n

$=$ $0{=}0 \wedge (\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i^3) = (\Sigma i{:}\ 0,..n\cdot i)^2 \;\Rightarrow\; (\Sigma i{:}\ 0,..n\cdot i^3)+n^3 = ((\Sigma i{:}\ 0,..n\cdot i)+n)^2)$

use antecedent as context; drop antecedent

$\Leftarrow$ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i)^2+n^3 = ((\Sigma i{:}\ 0,..n\cdot i)+n)^2$ — arithmetic

$=$ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i)^2 + n^3 = (\Sigma i{:}\ 0,..n\cdot i)^2 + 2\times(\Sigma i{:}\ 0,..n\cdot i)\times n + n^2$ — subtract $(\Sigma i{:}\ 0,..n\cdot i)^2$

$=$ $\forall n\cdot n^3 = 2\times(\Sigma i{:}\ 0,..n\cdot i)\times n + n^2$ — use Lemma 295(c)

$=$ $\forall n\cdot n^3 = 2\times n\times(n-1)/2\times n + n^2$ — arithmetic

$=$ $\top$

(f) $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot 2^i) = 2^n - 1$

§ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot 2^i) = 2^n - 1$ — induction

$\Leftarrow$ $(\Sigma i{:}\ 0,..0\cdot 2^i) = 2^0 - 1$

$\wedge$ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot 2^i) = 2^n - 1 \;\Rightarrow\; (\Sigma i{:}\ 0,..n{+}1\cdot 2^i) = 2^{n+1} - 1$

sum over empty domain; divide domain of final sum; simplify

$=$ $0{=}1{-}1 \wedge \forall n\cdot (\Sigma i{:}\ 0,..n\cdot 2^i) = 2^n - 1 \;\Rightarrow\; (\Sigma i{:}\ 0,..n\cdot 2^i)+2^n = 2^{n+1} - 1$

use antecedent as context then drop it

$\Leftarrow$ $\forall n\cdot 2^n - 1 + 2^n = 2^{n+1} - 1$ — law of exponents, identity

$=$ $\top$

(g) $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i\times 2^i) = (n-2)\times 2^n + 2$

§ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i\times 2^i) = (n-2)\times 2^n + 2$ — induction

$\Leftarrow$ $(\Sigma i{:}\ 0,..0\cdot i\times 2^i) = (0-2)\times 2^0 + 2$

$\wedge$ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i\times 2^i) = (n-2)\times 2^n + 2 \;\Rightarrow\; (\Sigma i{:}\ 0,..n{+}1\cdot i\times 2^i) = (n+1-2)\times 2^{n+1} + 2$

sum over empty domain; divide domain of final sum; simplify

$=$ $\forall n\cdot (\Sigma i{:}\ 0,..n\cdot i\times 2^i) = (n-2)\times 2^n + 2 \;\Rightarrow\; (\Sigma i{:}\ 0,..n\cdot i\times 2^i) + n\times 2^n = (n+1-2)\times 2^{n+1} + 2$

use antecedent as context, then drop antecedent

$\Leftarrow$ $\forall n\cdot (n-2)\times 2^n + 2 + n\times 2^n = (n+1-2)\times 2^{n+1} + 2$ — law of exponents and simplify

$=$ $\top$

(h) $\forall n\cdot (\Sigma i: 0,..n\cdot (-2)^i) = (1-(-2)^n) / 3$

§ $\forall n\cdot (\Sigma i: 0,..n\cdot (-2)^i) = (1-(-2)^n) / 3$ induction

$\Leftarrow$ $(\Sigma i: 0,..0\cdot (-2)^i) = (1-(-2)^0) / 3$

$\wedge$ $(\forall n\cdot (\Sigma i: 0,..n\cdot (-2)^i) = (1-(-2)^n) / 3 \Rightarrow (\Sigma i: 0,..n+1\cdot (-2)^i) = (1-(-2)^{n+1}) / 3)$

$=$ $0=0$ reflexive, identity

$\wedge$ $(\forall n\cdot (\Sigma i: 0,..n\cdot (-2)^i) = (1-(-2)^n) / 3$ use this context in consequent

$\Rightarrow (\Sigma i: 0,..n\cdot (-2)^i) + (-2)^n = (1-(-2)\times(-2)^n) / 3)$

$=$ $\forall n\cdot (\Sigma i: 0,..n\cdot (-2)^i) = (1-(-2)^n) / 3$

$\Rightarrow (1-(-2)^n) / 3 + (-2)^n = (1-(-2)\times(-2)^n) / 3$ arithmetic

$=$ $\forall n\cdot (\Sigma i: 0,..n\cdot (-2)^i) = (1-(-2)^n) / 3$

$\Rightarrow \top$

$=$ $\top$

(i) $\forall n\cdot n\ge 3 \Rightarrow 2\times n^3 > 3\times n^2 + 3\times n$

(j) $\forall n\cdot n\ge 4 \Rightarrow 3^n > n^3$

(k) $\forall n\cdot n\ge 4 \Rightarrow n! > 2^n$ where ! is factorial

(l) $\forall n\cdot n\ge 10 \Rightarrow 2^n > n^3$

(m) $\forall a, d\cdot \exists q, r\cdot d\ne 0 \Rightarrow r<d \wedge a = q\times d + r$

(n) $\forall a, b\cdot a\le b \Rightarrow (\Sigma i: a,..b\cdot 3^i) = (3^b-3^a)/2$

(o) $\forall n\cdot (n+1)^{nat} : nat\times n + 1$

§ $\forall n\cdot (n+1)^{nat} : nat\times n + 1$ bunch-element conversion

$=$ $\forall n\cdot \forall m\cdot \exists i\cdot (n+1)^m = i\times n + 1$ induction on m

$\Leftarrow$ $\forall n\cdot (\exists i\cdot (n+1)^0 = i\times n + 1)$

$\wedge$ $(\forall m\cdot (\exists i\cdot (n+1)^m = i\times n + 1) \Rightarrow (\exists i\cdot (n+1)^{m+1} = i\times n + 1))$

In the first $\exists i$, generalize. In the last $\exists i$, rename i to j and then distribute outward.

$\Leftarrow$ $\forall n\cdot ((n+1)^0 = 0\times n + 1)$

$\wedge$ $(\forall m\cdot (\exists i, j\cdot (n+1)^m = i\times n + 1 \Rightarrow (n+1)^{m+1} = j\times n + 1))$

The base case disappears by arithmetic. The step case uses the law of exponents.

$=$ $\forall n, m\cdot \exists i, j\cdot (n+1)^m = i\times n + 1 \Rightarrow (n+1)^m\times(n+1) = j\times n + 1$

In the implication, use context.

$=$ $\forall n, m\cdot \exists i, j\cdot (n+1)^m = i\times n + 1 \Rightarrow (i\times n + 1)\times(n+1) = j\times n + 1$ arithmetic

$=$ $\forall n, m\cdot \exists i, j\cdot (n+1)^m = i\times n + 1 \Rightarrow i\times n^2 + i\times n + n = j\times n$

Split the domain of n into 0 and $nat+1$.

$=$ $(\forall m\cdot \exists i, j\cdot 1^m = 1 \Rightarrow 0+0+0 = 0)$

$\wedge$ $(\forall n: nat+1\cdot \forall m\cdot \exists i, j\cdot (n+1)^m = i\times n + 1 \Rightarrow i\times n^2 + i\times n + n = j\times n)$

The top conjunct disappears by arithmetic. In the bottom conjunct, divide by n .

$=$ $\forall n: nat+1\cdot \forall m\cdot \exists i, j\cdot (n+1)^m = i\times n + 1 \Rightarrow i\times n + i + 1 = j$

Generalize $\exists i$

$\Leftarrow$ $\forall n: nat+1\cdot \forall m\cdot \exists i, j\cdot (n+1)^m = i\times n + 1 \Rightarrow i\times n + i + 1 = i\times n + i + 1$

reflexivity, base, idempotence

$=$ $\top$

(p) $\forall n\cdot (\Sigma i: 0,..n\cdot i\times(i+1)) = (n-1)\times n\times(n+1)/3$

(q) $\forall n\cdot (\Sigma i\colon 0,..n\cdot (-1)^i \times i^2) = -(-1)^n \times (n-1) \times n / 2$

(r) $\forall n\cdot (\Sigma i\colon 0,..n\cdot 1/((i+1)\times(i+2))) = n/(n+1)$