8 Page 54

4.1 Fix some $k, m \in N$, we proceed by induction on n, for $n = 0$, $(k+m)+0 = k+(m+0)$ implies $k+m = k+m$ so we are done. Now assume (*) $(k+m)+n = k+(m+n)$ holds for n, then $(k+m)+(n+1) = [(k+m)+n]+1$ by 4.3, by induction hypothesis (*) it follows that $(k+m)+(n+1) = [k+(m+n)]+1$, hence 4.3 implies $[k+(m+n)]+1 = k+((m+n)+1) = k+(m+(n+1))$, thus $(k+m)+(n+1) = k+(m+(n+1))$, this completes the proof. since k, m were arbitrary the propositions holds for all $k, m, n \in N$.

4.2 We prove by induction on k, Let $k = 0$ then $m < n$ iff $m+0 < n+0$ trivially. Now assume that $m < n$ iff $m+k < n+k$ holds for k, we must prove that $m < n$ implies $m+(k+1) < n+(k+1)$. Assume $m < n$, then $m+k < n+k$ by induction hypothesis, exercise 2.2 (page 45) implies that $(m+k)+1 < (n+k)+1$, by previous exercise $m+(k+1) < n+(k+1)$, this completes the induction. the other side can be done by the fact that $S(n)$ is one-to-one.

4.3 We prove it by induction on m, if $m = 0$ then $0 \leq n$ iff there is some $k \in N$ such that $n = 0+k$, namely $k = n$. Let $m+1 \leq n$, since $m < m+1$ we have (*) $m < n$ and $m \leq n$, by induction hypothesis we get $n = m+k$ for some $k \in N$, $k \neq 0$ since otherwise we get $n = m$ which contradicts (*), hence $k = k'+1$ for some $k' \in N$, thus $n = m+k = m+(k'+1) = m+(1+k') = (m+1)+k'$ for some $k' \in N$, thus we are done.

4.4 We use parametric version of Recursion Theorem, let $P = A = N$ and $a : P \to N$ be such that $a(p) = 0$ for every $p \in P = N$ and $g : N \times N \times \times N \to N$ such that $g(p, x, n) = x + p$, then there is a function $\cdot$ such that $m \cdot 0 = \cdot(m, 0) = a(m) = 0$ for all $m \in N$ and $m \cdot (n+1) = \cdot(m, n+1) = g(m, \cdot(m, n), n) = \cdot(m, n) + m = m \cdot n + m$.

4.5 We should prove that $m \cdot n = n \cdot m$ for every $m, n \in N$. we proceed by induction on n, if $n = 0$ then $m \cdot 0 = 0$, we need to show that $0 = 0 \cdot m$ for all m, if $m = 0$ then $0 = 0 \cdot 0$, now assume that $0 = 0 \cdot m$ holds then $0 \cdot (m+1) = 0 \cdot m + 0$, by induction hypothesis we get $0 \cdot (m+1) = 0+0 = 0$, thus for every m we have $m \cdot 0 = 0 \cdot m$. Now assume that $m \cdot n = n \cdot m$ holds for n, we should prove (*) $m \cdot (n+1) = (n+1) \cdot m$ for all $m \in N$, we proceed by induction on m, if $m = 0$ it trivially holds. Now assume that (*) holds for m, we should prove that $(m+1) \cdot (n+1) = (n+1) \cdot (m+1)$. but we know that $(m+1) \cdot (n+1) = [(m+1) \cdot n] + (m+1) = [n \cdot (m+1)] + (m+1) =$

$= (n \cdot m + n) + (m+1)$

$= (n \cdot +m) + (n+1)$

$= (m \cdot n + m) + (n+1)$

$= (m \cdot (n+1)) + (n+1)$

$= (n+1) \cdot m + (n+1)$

$= (n+1) \cdot (m+1)$ and this completes the proof.

To prove that multiplication is distributive over addition we must show that $m \cdot (n+k) = m \cdot n + m \cdot k$. we proceed by induction on k, if $k = 0$ then $m \cdot (n+0) = m \cdot n$ on the other hand $m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$, thus $m \cdot (n+0) = m \cdot n + m \cdot 0$. Now assume that $m \cdot (n+k) = m \cdot n + m \cdot k$ holds for k, then $m \cdot (n + (k+1))$

$= m \cdot ((n+k)+1)$

$= m \cdot (n+k) + m$

$= (m \cdot n + m \cdot k) + m$ (by induction hypothesis)

$= m \cdot n + (m \cdot k + m)$

$= m \cdot n + m \cdot (k+1)$

this completes the induction.

To prove that it is associative we need to prove $(m \cdot n) \cdot k = m \cdot (n \cdot k)$ for all $m, n, k \in N$. Fix some $m, n \in N$, we proceed by induction on k, for $k = 0$, $(m \cdot n) \cdot 0 = m \cdot (n \cdot 0) = 0$ holds, since $m \cdot 0 = 0$. Assume that $(m \cdot n) \cdot k = m \cdot (n \cdot k)$ holds for k, then: $(m \cdot n) \cdot (k+1)$

$= (m \cdot n) \cdot k + m \cdot n$

$= m \cdot (n \cdot k) + m \cdot n$ by induction hypothesis

$= m \cdot ((n \cdot k) + n)$ by distributive property

$= m \cdot (n \cdot (k+1))$