

Solutions to HW 5.

Addition

$$\begin{array}{ll} m + 0 & := m & \text{(Initial Condition for +)} \\ m + S(n) & := S(m + n) & \text{(Recurrence Relation (or Propagation Rule) for +)} \end{array}$$

Multiplication

$$\begin{array}{ll} m \cdot 0 & := 0 & \text{(Initial Condition for \cdot)} \\ m \cdot S(n) & := m \cdot n + m & \text{(Recurrence Relation for \cdot)} \end{array}$$

1. Prove that $m(n + k) = (mn) + (mk)$ holds for the natural numbers.

This is a proof by induction on k .

(Base Case: $k = 0$)

$$\begin{array}{ll} m(n + 0) & = mn & \text{(IC, +)} \\ & = mn + 0 & \text{(IC, +)} \\ & = mn + m0 & \text{(IC, \cdot)} \end{array}$$

(Inductive Step: Assume true for k , prove true for $S(k)$)

$$\begin{array}{ll} m(n + S(k)) & = mS(n + k) & \text{(RR, +)} \\ & = m(n + k) + m & \text{(RR, \cdot)} \\ & = (mn + mk) + m & \text{(IH)} \\ & = mn + (mk + m) & \text{(Associative Law, +)} \\ & = mn + mS(k) & \text{(RR, \cdot)} \end{array}$$

2. Prove that $m(nk) = (mn)k$ holds for the natural numbers.

This is a proof by induction on k .

(Base Case: $k = 0$)

$$\begin{array}{ll} m(n0) & = m0 & \text{(IC, \cdot)} \\ & = 0 & \text{(IC, \cdot)} \\ & = (mn)0 & \text{(IC, \cdot)} \end{array}$$

(Inductive Step: Assume true for k , prove true for $S(k)$)

$$\begin{array}{ll} m(n \cdot S(k)) & = m(nk + n) & \text{(RR, \cdot)} \\ & = m(nk) + mn & \text{(Distributive Law)} \\ & = (mn)k + mn & \text{(IH)} \\ & = (mn) \cdot S(k) & \text{(RR, \cdot)} \end{array}$$

3. Prove that $mn = nm$ holds for the natural numbers. (Some lemmas will be needed.)

Lemma 1. $0k = 0$.

Proof. This is a proof by induction on k .

(Base Case: $k = 0$)

$$00 = 0 \quad (\text{IC}, \cdot)$$

(Inductive Step: Assume true for k , prove true for $S(k)$)

$$\begin{aligned} 0 \cdot S(k) &= 0k + 0 && (\text{RR}, \cdot) \\ &= 0 + 0 && (\text{IH}) \\ &= 0 && (\text{IC}, +) \end{aligned}$$

Lemma 2. $1k = k$.

Proof. This is a proof by induction on k .

(Base Case: $k = 0$)

$$10 = 0 \quad (\text{IC}, \cdot)$$

(Inductive Step: Assume true for k , prove true for $S(k)$)

$$\begin{aligned} 1S(k) &= 1k + 1 && (\text{RR}, \cdot) \\ &= k + 1 && (\text{IH}) \\ &= S(k) && (\text{Law (a) of Addition: } S(n) = n + 1) \end{aligned}$$

Lemma 3. (Right distributivity) $(m + n)k = mk + nk$.

Proof. This is a proof by induction on k .

(Base Case: $k = 0$)

$$\begin{aligned} (m + n)0 &= 0 && (\text{IC}, \cdot) \\ &= 0 + 0 && (\text{IC}, +) \\ &= m0 + n0 && (\text{IC}, \cdot) \end{aligned}$$

(Inductive Step: Assume true for k , prove true for $S(k)$)

$$\begin{aligned} (m + n) \cdot S(k) &= (m + n)k + (m + n) && (\text{RR}, \cdot) \\ &= (mk + nk) + (m + n) && (\text{IH}) \\ &= mk + (nk + (m + n)) && (\text{Associative Law}, +) \\ &= mk + ((nk + m) + n) && (\text{Associative Law}, +) \\ &= mk + ((m + nk) + n) && (\text{Commutative Law}, +) \\ &= mk + (m + (nk + n)) && (\text{Associative Law}, +) \\ &= (mk + m) + (nk + n) && (\text{Associative Law}, +) \\ &= (m \cdot S(k)) + (n \cdot S(k)) && (\text{RR}, \cdot) \end{aligned}$$

Solution to the Problem.

Proof. We prove that $mn = nm$ by induction on n .

(Base Case: $n = 0$)

$$\begin{aligned} m0 &= 0 && (\text{IC}, \cdot) \\ &= 0m && (\text{Lemma 1}) \end{aligned}$$

(Inductive Step: Assume true for n , prove true for $S(n)$)

$$\begin{aligned} m \cdot S(n) &= mn + m && (\text{RR}, \cdot) \\ &= nm + m && (\text{IH}) \\ &= nm + 1m && (\text{Lemma 2}) \\ &= (n + 1)m && (\text{Lemma 3}) \\ &= S(n) \cdot m && (\text{Law (a) of Addition: } S(n) = n + 1) \end{aligned}$$