Homework 2 Solutions

Exercise 1.5.11

Part (3)

(1) $(\forall x \text{ in } Z)[(A(x) \to R(x)) \vee T(x)]$	
(2) $(\exists x \text{ in } Z)[T(x) \to P(x)]$	
(3) $(\forall x \text{ in } Z)[A(x) \wedge \neg P(x)]$	
(4) $T(a) \to P(a)$	(2), Existential Instantiation
(5) $A(a) \wedge \neg P(a)$	(3), Universal Instantiation
(6) $\neg P(a)$	(5), Simplification
(7) $\neg T(a)$	(4), (6), Modus Tollens
(8) $(A(a) \to R(a)) \vee T(a)$	(1), Universal Instantiation
(9) $A(a) \to R(a)$	(7), (8), Modus Tollendo Ponens
(10) $A(a)$	(5), Simplification
(11) $R(a)$	(9), (10), Modus Ponens
(12) $(\exists x \text{ in } Z)[R(x)]$	(11), Existential Generalization

Exercise 1.4.1

Part (4)

We know L is true from the third premise, and combined with the first premise this gives M. Then $M \vee N$ is true, and therefore $L \to K$. We already know that L is true, and thus K must be true as well.

Part (6)

We are given that $\neg D$ is true, and therefore $\neg D \vee A$ is true, which lets us conclude $\neg\neg C$. This is the same as C, which gives $\neg A$, which in turn yields $B \to \neg C$. But we already know that C is true, and therefore B must be false.

Exercise 2.2.6

Theorem. *Let a, b, c, m and n be integers. If $a|b$ and $a|c$ then $a|(bm + cn)$.*

Proof. Suppose that $a|b$ and $a|c$. Then there must exist integers r and s so that $b = ar$ and $c = as$. Then $bm + cn = arm + asn = a(rm + sn)$, so $a|(bm + cn)$ as well. $\square$

Here is a two-column proof of the same theorem:

(1) $a \mid b$	
(2) $a \mid c$	
(3) $(\exists x \text{ in } \mathbb{Z})(ax = b)$	(1), Definition of Divides
(4) $(\exists x \text{ in } \mathbb{Z})(ax = c)$	(2), Definition of Divides
(5) $ar = b$	(3), Existential Instantiation
(6) $as = c$	(4), Existential Instantiation
(7) $arm = bm$	(5), Multiplying by m
(8) $asn = cn$	(6), Multiplying by n
(9) $arm + asn = bm + cn$	(7), (8), Addition of equations
(10) $a(rm + sn) = bm + cn$	(9) Distributive Law
(11) $(\exists x \text{ in } \mathbb{Z})(ax = bm + cn)$	(10), Existential Generalization
(12) $a \mid (bm + cn)$	(11), Definition of Divides

Exercise 2.2.7

Theorem. *Let a, b, c, and d be integers. If $a \mid b$ and $c \mid d$ then $ac \mid bd$.*

Proof. Suppose that $a \mid b$ and $c \mid d$, and let u and v be integers so that $b = au$ and $d = cv$. Then $bd = aucv = (ac)(uv)$, which proves that $ac \mid bd$. □

Here is a two-column proof of the same theorem:

(1) $a \mid b$	
(2) $c \mid d$	
(3) $(\exists x \text{ in } \mathbb{Z})(ax = b)$	(1), Definition of Divides
(4) $(\exists x \text{ in } \mathbb{Z})(cx = d)$	(2), Definition of Divides
(5) $au = b$	(3), Existential Instantiation
(6) $cv = d$	(4), Existential Instantiation
(7) $(au)(cv) = bd$	(5), (6), Multiplication of equations
(8) $(ac)(uv) = bd$	(7), Associativity and Commutativity
(9) $(\exists x \text{ in } \mathbb{Z})[(ac)x = bd]$	(8), Existential Generalization
(10) $ac \mid bd$	(9), Definition of Divides