Solutions to selected exercises of Chapters 17 and 18

Bas Luttik

October 10, 2013

This document contains solutions to the following exercises in the book [1]:

17.7, 17.9(c), 17.10, 18.3(c), 18.4(c), 18.7, 18.8(b).

We **strongly** advise you to first try all these exercises by yourself, before looking at all at the solutions below. There is not a lot of variation possible in the way solutions to exercises should be written down. So if your solution in one way or another deviates from a solution below, then consider discussing the differences with your instructor.

The proofs below are given in textual form and contain the *minimum* amount of detail both with respect to the logic and reasoning involved, and with respect to the properties and definitions pertaining to sets, relations and mappings. Note that most applications of logical reasoning steps (i.e., the introduction and elimination rules discussed in Parts I and II of the book) are left implicit, but you should nevertheless be able to recognise where and how they are applied. For your convenience, there is also an appendix at the end of this document with very detailed logical derivations, following the methods of Parts I and II to the letter and being explicit about which rule is applied when. We encourage you to compare the proofs in textual form and the logical derivations, to make sure that you understand every step. At examinations you may give proofs about properties of sets, relations an mappings either in textual form, or as logical derivations.

17.7 In this exercise we consider the relation R on $\mathbb{Z}$ defined for $x, y \in \mathbb{Z}$ by

$$x \; R \; y \text{ if } x^2 - y^2 \text{ is a multiple of } 5 \; .$$

(Recall that $x^2 - y^2$ is a multiple of 5 if $x^2 - y^2 = k \cdot 5$ for some $k \in \mathbb{Z}$, i.e., if $\exists_k[k \in \mathbb{Z} : x^2 - y^2 = k \cdot 5]$.)

(a) To prove that the relation R is an equivalence relation, we need to prove it is reflexive, symmetric and transitive:

(i) R is reflexive: To prove that R is reflexive, we need to prove that $x \; R \; x$ for all $x \in \mathbb{Z}$. Let $x \in \mathbb{Z}$. Then $x^2 - x^2 = 0 = 0 \cdot 5$, and clearly $0 \in \mathbb{Z}$, so $x^2 - x^2$ is a multiple of 5, and hence xRx.

(ii) R is symmetric: To prove that R is symmetric, we need to prove, for all $x, y \in \mathbb{Z}$, that if $x \; R \; y$, then $y \; R \; x$. Let $x, y \in \mathbb{Z}$, and suppose $x \; R \; y$. Then, according to the definition of R, $x^2 - y^2$ is a multiple of 5, so there exists $k \in \mathbb{Z}$ such that $x^2 - y^2 = k \cdot 5$. Note that

$$y^2 - x^2 = -(x^2 - y^2) = -(k \cdot 5) = (-k) \cdot 5 \; ,$$

and since $k \in \mathbb{Z}$ also $-k \in \mathbb{Z}$. Hence, also $y^2 - x^2$ is a multiple of 5, and it follows that $y \; R \; x$.

(iii) R is transitive: To prove that R is transitive, we need to prove, for all $x, y, z \in \mathbb{Z}$, that if $x\ R\ y$ and $y\ R\ z$, then $x\ R\ z$. Let $x, y, z \in \mathbb{Z}$, and suppose $x\ R\ y$ and $y\ R\ z$. Then, according to the definition of R, $x^2 - y^2$ and $y^2 - z^2$ are both multiples of 5, so there exist $k \in \mathbb{Z}$ and $\ell \in \mathbb{Z}$ such that $x^2 - y^2 = k \cdot 5$ and $y^2 - z^2 = \ell \cdot 5$. Note that

$$x^2 - z^2 = -(x^2 - y^2) + (y^2 - z^2) = k \cdot 5 + \ell \cdot 5 = (k + \ell) \cdot 5 \ ,$$

and since both $k \in \mathbb{Z}$ and $\ell \in \mathbb{Z}$ it follows that also $(k + \ell) \in \mathbb{Z}$. Hence, also $x^2 - z^2$ is a multiple of 5, and it follows that $x\ R\ z$.

(b) We need to prove that $x \equiv_5 y$ implies $x\ R\ y$ for all $x, y \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}$ and suppose that $x \equiv_5 y$; we establish that $x\ R\ y$. Note that, according to the definition of $\equiv_5$, there exists $k \in \mathbb{Z}$ such that $x - y = k \cdot 5$, so

$$x^2 - y^2 = (x + y) \cdot (x - y) = (x + y) \cdot (k \cdot 5) = ((x + y) \cdot k) \cdot 5 \ ,$$

and, since $x, y \in \mathbb{Z}$ and also $k \in \mathbb{Z}$, we also get that $(x + y) \cdot k \in \mathbb{Z}$. Hence, $x^2 - y^2$ is a multiple of 5, and thereby we have established $x\ R\ y$.

(c) From part (b) of the exercise it immediately follows that R partitions $\mathbb{Z}$ into *at most* 5 classes: $K(0)$, $K(1)$, $K(2)$, $K(3)$ and $K(4)$. It may, however, be the case that some of these classes coincide. We investigate in which cases $K(x) = K(y)$ for$0 \leq x < y \leq 4$ (note that $K(x) = K(y)$ if, and only if, $x\ R\ y$):

- Since $0^2 - 1^2 = -1$ is not a multiple of 5, it follows that $\neg(0\ R\ 1)$, and hence $K(0) \neq K(1)$.
- Since $0^2 - 2^2 = -4$ is not a multiple of 5, it follows that $\neg(0\ R\ 2)$, and hence $K(0) \neq K(2)$.
- Since $0^2 - 3^2 = -9$ is not a multiple of 5, it follows that $\neg(0\ R\ 3)$, and hence $K(0) \neq K(3)$.
- Since $0^2 - 4^2 = -16$ is not a multiple of 5, it follows that $\neg(0\ R\ 4)$, and hence $K(0) \neq K(4)$.
- Since $1^2 - 2^2 = -3$ is not a multiple of 5, it follows that $\neg(1\ R\ 2)$, and hence $K(1) \neq K(2)$.
- Since $1^2 - 3^2 = -8$ is not a multiple of 5, it follows that $\neg(1\ R\ 3)$, and hence $K(1) \neq K(3)$.
- Since $1^2 - 4^2 = -15$ is a multiple of 5, it follows that $1\ R\ 4$, and hence $K(1) = K(4)$.
- Since $2^2 - 3^2 = -5$ is a multiple of 5, it follows that $2\ R\ 3$, and hence $K(2) = K(3)$.
- Since $2^2 - 4^2 = -12$ is not a multiple of 5, it follows that $2\ R\ 4$, and hence $K(2) \neq K(4)$.
- Since $3^2 - 4^2 = -7$ is not a multiple of 5, it follows that $3\ R\ 4$, and hence $K(3) \neq K(4)$.

We conclude that R partitions $\mathbb{Z}$ into three equivalence classes: $K(0)$, $K(1) = K(4)$ and $K(2) = K(3)$.

17.9 (c) To prove that $a\ R\ b \Leftrightarrow K(a) = K(b)$, it suffices to prove that the implication from left to right and the implication from right to left separately:

($\Rightarrow$) Suppose that $a\ R\ b$. We need to establish that $K(a) = K(b)$, and for this it suffices to show that $K(a) \subseteq K(b)$ and $K(b) \subseteq K(a)$.

First, consider an element $x \in K(a)$. Then from the definition of $K(a)$ it follows that $a\ R\ x$. Furthermore, since R is symmetric, from $a\ R\ b$ it follows that $b\ R\ a$. Since R is transitive, from $b\ R\ a$ and $a\ R\ x$ it follows that $b\ R\ x$. Hence, by the definition of $K(b)$, it follows that $x \in K(b)$. Thus, we have established that $K(a) \subseteq K(b)$. Next, consider an element $x \in K(b)$. Then from the definition of $K(b)$ it follows that $b\ R\ x$. Since R is transitive, from $a\ R\ b$ and $b\ R\ x$, it follows that $a\ R\ x$. Hence, by the definition of $K(a)$, it follows that $x \in K(a)$. Thus, we have established that $K(b) \subseteq K(a)$.

($\Leftarrow$) Suppose that $K(a) = K(b)$; we need to establish that $a\ R\ b$. To this end, note that $b \in K(b)$, and since $K(b) = K(a)$, it follows that $b \in K(a)$. Hence, from the definition of $K(a)$ it follows that $a\ R\ b$.

The proof is thereby complete.

17.10 (a) Suppose that $K(ab) = K(0)$. Then, according to Exercise 17.9(c), $ab \equiv_n 0$, so, by the definition of $\equiv_n$, ab is a multiple of n. It immediately follows that $n \mid ab$, and hence, since n is prime, by the hint in the exercise we get $n \mid a$ or $n \mid b$. This means that either a is a multiple of n or b is a multiple of n. So, by the definition of $\equiv_n$, $a \equiv_n 0$ or $b \equiv_n 0$, and hence $K(a) = K(0)$ or $K(b) = K(0)$. The proof is thereby complete.

(b) No, if n is not prime, then the implication does not hold. For a concrete counterexample, consider $n = 6$. Then $2 \cdot 3 \equiv_6 0$, so $K(2 \cdot 3) = K(0)$, but $2 \not\equiv_6 0$ and $3 \not\equiv_6 0$, so $K(2) \neq K(0)$ and $K(3) \neq K(0)$.

(More generally, if n is not prime, then there exist k and ℓ such that $1 < k, \ell < n$ and $n = k \cdot \ell$, and $K(k \cdot \ell) = K(0)$, but $K(k) \neq K(0)$ and $K(\ell) \neq K(0)$.)

18.3 (c) To prove that $f(S) \setminus f(T) \subseteq f(S \setminus T)$, let $y \in f(S) \setminus f(T)$; we prove that $y \in f(S \setminus T)$. From $y \in f(S) \setminus f(T)$ it follows, by the property of $\setminus$, that $y \in f(S)$ and $y \notin f(T)$. Hence, by the property of image, there exists $x \in S$ such that $f(x) = y$.

We now prove that $x \notin T$ by deriving a contraction from the assumption that $x \in T$. Note that from $x \in T$ it follows by the property of image $f(x) \in f(T)$, so $y \in f(T)$, which is in contradiction with the already established $y \notin f(T)$.

We have now established that $x \in S$ and $x \notin T$, so we may conclude, by the property of $\setminus$, that $x \in S \setminus T$. It follows, by the property of image, that $f(x) \in f(S \setminus T)$, so $y \in f(S \setminus T)$. The proof is thereby complete.

18.4 (c) We prove that $f^{\leftarrow}(U \setminus V) = f^{\leftarrow}(U) \setminus f^{\leftarrow}(V)$ with a calculation:

$$
\begin{array}{ll}
 & x \in f^{\leftarrow}(U \setminus V) \\
\overset{val}{=\!=} & \{\ \text{Property of source}\ \} \\
 & f(x) \in U \setminus V \\
\overset{val}{=\!=} & \{\ \text{Property of}\ \setminus\ \} \\
 & f(x) \in U \wedge \neg(f(x) \in V) \\
\overset{val}{=\!=} & \{\ \text{Property of source}\ (2\times)\ \} \\
 & x \in f^{\leftarrow}(U) \wedge \neg(x \in f^{\leftarrow}(V)) \\
\overset{val}{=\!=} & \{\ \text{Property of}\ \setminus\ \} \\
 & x \in f^{\leftarrow}(U) \setminus f^{\leftarrow}(V)\ .
\end{array}
$$

18.7 (a) To prove that $F(F^{\leftarrow}(B')) \subseteq B'$, let $y \in F(F^{\leftarrow}(B'))$; we establish that $y \in B'$. From $y \in F(F^{\leftarrow}(B'))$ it follows by the property of image that there exists $x \in F^{\leftarrow}(B')$ such that $F(x) = y$. Hence, by the property of source, $y = F(x) \in B'$.

(b) To prove that $F(F^{\leftarrow}(B')) = B'$ if F is a surjection, by part (a) of this exercise it remains to show that $B' \subseteq F(F^{\leftarrow}(B'))$ if F is a surjection. We consider $y \in B'$ and prove that $y \in F(F^{\leftarrow}(B'))$. Note that, since F is a surjection and $y \in B' \subseteq B$, there exists $x \in A$ such that $F(x) = y \in B'$. Hence, by the property of source, $x \in F^{\leftarrow}(B')$, so by the property of image, $y = F(x) \in F(F^{\leftarrow}(B'))$. The proof that $B' \subseteq F(F^{\leftarrow}(B'))$ is thereby complete, and we conclude that if F is a surjection, then $F(F^{\leftarrow}(B')) = B'$.

18.8 (b) To prove that $f(S\backslash T) = f(S)\backslash f(T)$, according to the definition of $=$ on sets we need to prove the two inclusions $f(S\backslash T) \subseteq F(S)\backslash f(T)$ and $f(S)\backslash f(T) \subseteq f(S\backslash T)$. Note that the second inclusion has already been proved earlier in this document, as the solution to Exercise 18.3(c), so it remains to prove the first inclusion.

To prove that $f(S\backslash T) \subseteq f(S)\backslash f(T)$, let $y \in f(S\backslash T)$. Then, by the (second) property of image, there exists $x \in S\backslash T$ such that $f(x) = y$. From $x \in S\backslash T$ it follows by the definition of $\backslash$ that $x \in S$ and $x \notin T$, and from $x \in S$ it follows by the (first) property of image that $f(x) \in f(S)$, and hence, since $f(x) = y$, that $y \in f(S)$. Therefore, to prove that $y \in f(S)\backslash f(T)$, by the property of $\backslash$ it now remains to prove that $y \notin f(T)$. To this end, suppose that $y \in f(T)$; we derive a contradiction. From $y \in f(T)$ it follows by the property of image that there exists $x' \in T$ such that $f(x') = y$.[1] Now, since $f(x) = y = f(x')$ and the mapping $f : A \to B$ is an injection, it follows that $x = x'$. Recall that we had already concluded that $x \notin T$, and now it also follows from $x' \in T$ that $x \in T$: a contradiction.

References

[1] Rob Nederpelt and Fairouz Kamareddine. *Logical Reasoning: A First Course*, volume 3 of *Texts in Computing*. King's College Publications, second revised edition edition, 2011.

[1] It is important to note that the property of image yields an element of T which f maps to y, but, at this point in the proof, it is not yet clear that this has to be x; for this, we need to use that f is an injection.

A Logical derivations

17.7 In this exercise we consider the relation R on $\mathbb{Z}$ defined for $x, y \in \mathbb{Z}$ by

$$x \; R \; y \text{ if } x^2 - y^2 \text{ is a multiple of } 5 \; .$$

(Recall that $x^2 - y^2$ is a multiple of 5 if $x^2 - y^2 = k \cdot 5$ for some $k \in \mathbb{Z}$, i.e., if $\exists_k[k \in \mathbb{Z} : x^2 - y^2 = k \cdot 5]$.)

(a) To prove that the relation R is an equivalence relation, we need to prove it is reflexive, symmetric and transitive:

(i) R is reflexive:

{ Assume: }

(1) **var** x; $x \in \mathbb{Z}$

{ Mathematics: }

(2) $x^2 - x^2 = 0 = 0 \cdot 5$

{ Mathematics: }

(3) $0 \in \mathbb{Z}$

{ $\exists^*$-intro (2) and (3): }

(4) $\exists_k[k \in \mathbb{Z} : x^2 - x^2 = k \cdot 5]$

{ Definition of R on (4): }

(5) $x \; R \; x$

{ $\forall_x$-intro on (1) and (5): }

(6) $\forall_x[x \in \mathbb{Z} : x \; R \; x]$

(ii) R is symmetric:

{ Assume: }

(1) **var** x; $x \in \mathbb{Z}$

{ Assume: }

(2) $x \; R \; y$

{ Definition of R on (2): }

(3) $\exists_k[k \in \mathbb{Z} : x^2 - y^2 = k \cdot 5]$

{ $\exists^*$-elim on (3): }

(4) Pick a k with $k \in \mathbb{Z}$ and $x^2 - y^2 = k \cdot 5$

{ Mathematics, using (4): }

(5) $y^2 - x^2 = -(x^2 - y^2) = -(k \cdot 5) = (-k) \cdot 5$

{ Mathematics, using (4): }

(6) $-k \in \mathbb{Z}$

{ $\exists^*$-intro on (5) and (6): }

(7) $\exists_\ell[\ell \in \mathbb{Z} : y^2 - x^2 = \ell \cdot 5]$

{ Definition of R on (7): }

(8) $y \; R \; x$

{ $\Rightarrow$-intro on (2) and (8): }

(9) $x \; R \; y \Rightarrow y \; R \; x$

{ $\forall$-intro on (1) and (9): }

(10) $\forall_{x,y}[x, y \in \mathbb{Z} : x \; R \; y \Rightarrow y \; R \; x]$

(iii) R is transitive:

{ Assume: }

(1) **var** $x, y, z;\ x, y, z \in \mathbb{Z}$

{ Assume: }

(2) $x\ R\ y \wedge y\ R\ z$

{ $\wedge$-elim on (2): }

(3) $x\ R\ y$

{ Definition of R on (3): }

(4) $\exists_k[k \in \mathbb{Z} : x^2 - y^2 = k \cdot 5]$

{ $\exists^*$-elim on (4): }

(5) Pick a k with $k \in \mathbb{Z}$ and $x^2 - y^2 = k \cdot 5$

{ $\wedge$-elim on (2): }

(6) $y\ R\ z$

{ Definition of R on (6): }

(7) $\exists_\ell[\ell \in \mathbb{Z} : y^2 - z^2 = \ell \cdot 5]$

{ $\exists^*$-elim on (7): }

(8) Pick an ℓ with $\ell \in \mathbb{Z}$ and $y^2 - z^2 = \ell \cdot 5$

{ Mathematics, using (5) and (8): }

(9) $x^2 - z^2 = (x^2 - y^2) + (y^2 - z^2) = k \cdot 5 + \ell \cdot 5 = (k + \ell) \cdot 5$

{ Mathematics, using (5) and (8): }

(10) $(k + \ell) \in \mathbb{Z}$

{ $\exists^*$-intro on (9) and (10): }

(11) $\exists_m[m \in \mathbb{Z} : x^2 - z^2 = m \cdot 5]$

{ Definition of R on (11): }

(12) $x\ R\ z$

{ $\Rightarrow$-intro on (2) and (12): }

(13) $(x\ R\ y \wedge y\ R\ z) \Rightarrow x\ R\ z$

{ $\forall$-intro on (1) and (13): }

(14) $\forall_{x,y,z}[x, y, z \in \mathbb{Z} : (x\ R\ y \wedge y\ R\ z) \Rightarrow x\ R\ z]$

(b) We first present the proof of the formula $\forall_{x,y}[x, y \in \mathbb{Z} : x \equiv_5 y \Rightarrow x\ R\ y]$ as a derivation in the style of Part II of the book, and then also present it in textual form.

{ Assume: }

(1) $\boxed{\textbf{var } x, y;\ x, y \in \mathbb{Z}}$

{ Assume: }

(2) $\boxed{x \equiv_5 y}$

{ Definition of $\equiv_5$ on (2): }

(3) $\exists_k[k \in \mathbb{Z} : x - y = k \cdot 5]$

{ $\exists^*$-elim on (3): }

(4) Pick a k with $k \in \mathbb{Z}$ and $x - y = k \cdot 5$

{ Mathematics, using (4): }

(5) $x^2 - y^2 = (x + y) \cdot (x - y) = (x + y) \cdot (k \cdot 5) = ((x + y) \cdot k) \cdot 5$

{ Mathematics, using (1) and (4): }

(6) $(x + y) \cdot k \in \mathbb{Z}$

{ $\exists^*$-intro on (5) and (6): }

(7) $\exists_\ell[\ell \in \mathbb{Z} : x^2 - y^2 = \ell \cdot 5]$

{ Definition of R on (7): }

(8) $x\ R\ y$

{ $\Rightarrow$-intro on (2) and (8): }

(9) $x \equiv_5 y \Rightarrow x\ R\ y$

{ $\forall$-intro on (1) and (9): }

(10) $\forall_{x,y}[x, y \in \mathbb{Z} : x \equiv_5 y \Rightarrow x\ R\ y]$

17.9 (c)

{ Assume: }

(1) $\boxed{a\ R\ b}$

{ Assume: }

(2) $\boxed{\textbf{var } x;\ x \in K(a)}$

{ Definition of $K(a)$ on (2) followed by Property of $\in$: }

(3) $x \in V$

{ Definition of $K(a)$ on (2) followed by Property of $\in$: }

(4) $a\ R\ x$

{ $\forall$-elim with a and b on 'R is symmetric': }

(5) $a\ R\ b \Rightarrow b\ R\ a$

{ $\Rightarrow$-elim on (5) and (1): }

(6) $b\ R\ a$

{ $\forall$-elim with b, a and x on 'R is transitive': }

(7) $(b\ R\ a \wedge a\ R\ x) \Rightarrow b\ R\ x$

{ $\wedge$-intro on (6) and (1): }

(8) $b\ R\ a \wedge a\ R\ x$

{ $\Rightarrow$-elim on (7) and (8): }

(9) $b\ R\ x$

{ Property of $\in$ on (3) and (9), followed by Definition of $K(b)$: }

(10) $x \in K(b)$

{ $\forall$-intro on (2) and (10): }

(11) $\forall_x[x \in K(a) : x \in K(b)]$

{ Definition of $\subseteq$ on (11): }

(12) $K(a) \subseteq K(b)$

{ Assume: }

(13) $\boxed{\textbf{var}\ x;\ x \in K(b)}$

{ Definition of $K(b)$ on (13) followed by Property of $\in$: }

(14) $x \in V$

{ Definition of $K(b)$ on (13) followed by Property of $\in$: }

(15) $b\ R\ x$

{ $\forall$-elim with b, a and x on 'R is transitive': }

(16) $(a\ R\ b \wedge b\ R\ x) \Rightarrow a\ R\ x$

{ $\wedge$-intro on (1) and (15): }

(17) $a\ R\ b \wedge b\ R\ x$

{ $\Rightarrow$-elim on (16) and (17): }

(18) $a\ R\ x$

{ Property of $\in$ on (3) and (18), followed by Definition of $K(a)$: }

(19) $x \in K(a)$

{ $\forall$-intro on (13) and (19): }

(20) $\forall_x[x \in K(b) : x \in K(a)]$

{ Definition of $\subseteq$ on (11): }

(21) $K(b) \subseteq K(a)$

{ $\wedge$-intro on (12) and (21): }

(22) $K(a) \subseteq K(b) \wedge K(b) \subseteq K(a)$

{ Definition of $=$ on (22): }

(23) $K(a) = K(b)$

{ $\Rightarrow$-intro on (1) and (23): }

(24) $a \; R \; b \Rightarrow K(a) = K(b)$

{ Assume: }

(25) $\boxed{K(a) = K(b)}$

{ Property of $\in$ on $b \in V$ and Definition of $K(b)$: }

(26) $b \in K(b)$

{ Property of $=$ on (25) and (26): }

(27) $b \in K(a)$

{ Definition of $K(a)$ on (26) followed by Property of $\in$: }

(28) $a \; R \; b$

{ $\Rightarrow$-intro on (25) and (28): }

(29) $K(a) = K(b) \Rightarrow a \; R \; b$

{ $\Leftrightarrow$-intro on (24) and (29): }

(30) $a \; R \; b \Leftrightarrow K(a) = K(b)$

17.10 (a) We first establish that, for all $n \in \mathbb{N}$,

$$n \mid x \overset{val}{=\!=} x \equiv_n 0 \qquad (*)$$

with a calculation:

$$\begin{array}{ll} & n \mid x \\ \overset{val}{=\!=} & \{ \text{ Definition of } \mid \} \\ & \exists_k[k \in \mathbb{Z} : x = k \cdot n] \\ \overset{val}{=\!=} & \{ \text{ Mathematics } \} \\ & \exists_k[k \in \mathbb{Z} : x - 0 = k \cdot n] \\ \overset{val}{=\!=} & \{ \text{ Definition of } \equiv_n \} \\ & x \equiv_n 0 \; . \end{array}$$

{ Assume: }

(1) $\boxed{K(ab) = K(0)}$

{ Exercise 17.9(c) on (1): }

(2) $a \cdot b \equiv_n 0$

{ $(*)$ on (2): }

(3) $n \mid ab$

{ Hint of the exercise on (3), using the assumed primality of n: }

(4) $n \mid a \vee n \mid b$

{ (*) on (4) (2×) }

(5) $a \equiv_n 0 \vee b \equiv_n 0$

{ Exercise 17.9(c) on (5) }

(6) $K(a) = K(0) \vee K(b) = K(0)$

{ $\Rightarrow$-intro on (1) and (6): }

(7) $K(ab) = K(0) \Rightarrow (K(a) = K(0) \vee K(b) = K(0))$

18.3 (c)

{ Assume: }

(1) $\boxed{\textbf{var } y;\ y \in f(S) \setminus f(T)}$

{ Property of $\setminus$ on (1): }

(2) $y \in f(S) \wedge \neg(y \in f(T))$

{ $\wedge$-elim on (2): }

(3) $y \in f(S)$

{ Property of image on (3): }

(4) $\exists_x[x \in S : f(x) = y]$

{ $\exists^*$-elim on (4): }

(5) Pick an x with $x \in S$ and $f(x) = y$

{ Assume: }

(6) $\boxed{x \in T}$

{ Property of image on (6): }

(7) $f(x) \in f(T)$

{ Leibniz on (5) and (7): }

(8) $y \in f(T)$

		{ $\wedge$-elim on (2): }
(9)		$\neg(y \in f(T))$
		{ $\neg$-elim on (9) and (8): }
(10)		`False`
	{ $\neg$-intro on (6) and (10): }	
(11)	$\neg(x \in T)$	
	{ $\wedge$-intro on (5) and (11): }	
(12)	$x \in S \wedge \neg(x \in T)$	
	{ Property of $\setminus$ on (12): }	
(13)	$x \in S \setminus T$	
	{ $\exists^*$-intro on (5) and (13): }	
(14)	$\exists_x[x \in S \setminus T : f(x) = y]$	
	{ Property of image on (14): }	
(15)	$y \in f(S \setminus T)$	
	{ $\forall$-intro on (1) and (16): }	
(16)	$\forall_y[y \in f(S) \setminus f(T) : y \in f(S \setminus T)]$	
	{ Definition of $\subseteq$ on (16): }	
(17)	$f(S) \setminus f(T) \subseteq f(S \setminus T)$	

18.7 (a)

{ Assume }

(1) **var** y; $y \in F(F^{\leftarrow}(B'))$

{ Property of image on (1): }

(2) $\exists_x[x \in F^{\leftarrow}(B') : F(x) = y]$

{ $\exists^*$-elim on (2): }

(3) Pick an x with $x \in F^{\leftarrow}(B')$ and $F(x) = y$

{ Property of source on (3): }

(4) $F(x) \in B'$

{ Leibniz on (2) and (4): }

(5) $y \in B'$

{ $\forall$-intro on (1) and (6): }

(6) $\forall_y[y \in F(F^{\leftarrow}(B')) : y \in B']$

{ Definition of $\subseteq$ on (6): }

(7) $F(F^{\leftarrow}(B')) \subseteq B'$

(b) Note that to prove that $F(F^{\leftarrow}(B')) = B'$ if F is a surjection, by part (a) of this exercise, it remains to show that $B' \subseteq F(F^{\leftarrow}(B'))$ if F is a surjection:

{ Assume: }

(1) $\boxed{F \text{ is a surjection}}$

  { Assume: }

(2) $\boxed{\textbf{var } y;\ y \in B'}$

    { Property of $\subseteq$ on $B' \subseteq B$ and (2): }

(3) $x \in B$

    { Property of surjection on (1) followed by $\forall$-elim with (3): }

(4) $\exists_x[x \in A : F(x) = y]$

    { $\exists^*$-elim on (4): }

(5) Pick an x with $x \in A$ and $F(x) = y$

    { Leibniz on (5) and (2): }

(6) $F(x) \in B'$

    { Property of source on (6): }

(7) $x \in F^{\leftarrow}(B')$

    { Property of image on (7): }

(8) $F(x) \in F(F^{\leftarrow}(B'))$

    { Leibniz on (5) and (8): }

(9) $y \in F(F^{\leftarrow}(B'))$

  { $\forall$-intro on (2) and (8): }

(10) $\forall_y[y \in B' : y \in F(F^{\leftarrow}(B'))]$

  { Definition of $\subseteq$ on (10): }

(11) $B' \subseteq F(F^{\leftarrow}(B'))$