SOLUTIONS TO THE EXAMPLE PROBLEM SET 2

(1) Prove with derivations that the following formula is a tautology.

$$\exists x[\forall y[P(x) \Rightarrow Q(y)]] \Rightarrow (\forall u[P(u)] \Rightarrow \exists v[Q(v)])$$

{Assume}

(1) $\boxed{\exists x[\forall y[P(x) \Rightarrow Q(y)]]}$

{Assume}

(2) $\boxed{\forall u[P(u)]}$

{$\exists *$-elim. on (1)}

(3) Pick a with $\forall y[P(a) \Rightarrow Q(y)]$

{$\forall$-elim. on (3)}

(4) $P(a) \Rightarrow Q(a)$

{$\forall$-elim. on (2)}

(5) $P(a)$

{$\Rightarrow$-elim. on (4) and (5)}

(6) $Q(a)$

{$\exists$-intro on (6)}

(7) $\exists v[Q(v)]$

{$\Rightarrow$-intro on (2) and (7)}

(8) $\forall u[P(u)] \Rightarrow \exists v[Q(v)]$

{$\Rightarrow$-intro on (1) and (8)}

$\exists x[\forall y[P(x) \Rightarrow Q(y)]] \Rightarrow (\forall u[P(u)] \Rightarrow \exists v[Q(v)])$

2 Check whether the following propositions always hold. If so, give a proof; if not give a counterexample.

(a) $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$

This statement holds since

$$
\begin{aligned}
X \in \mathcal{P}(A) \cap \mathcal{P}(B) &\overset{val}{=} X \in \mathcal{P}(A) \wedge X \in \mathcal{P}(B) \\
&\overset{val}{=} X \subseteq A \wedge X \subseteq B \\
&\underset{(*)}{\overset{val}{=}} X \subseteq A \cap B \\
&\overset{val}{=} X \in \mathcal{P}(A \cap B)
\end{aligned}
$$

where the equivalence marked by (*) is the following set property:

(*) $X \subseteq A \wedge X \subseteq B \Leftrightarrow X \subseteq A \cap B$.

We give a proof of (*): $\leftrightarrow$ flag-proof would also be suitable

$\boxed{\Rightarrow}$ Assume $X \subseteq A$ and $X \subseteq B$. let $x \in X$. Then from $X \subseteq A$ we have $x \in A$, and from $X \subseteq B$ we have $x \in B$, so $x \in A \cap B$. We have shown $X \subseteq A \cap B$.

$\boxed{\Leftarrow}$ Assume $X \subseteq A \cap B$. Let $x \in X$. Then from $X \subseteq A \cap B$, we get $x \in A \cap B$, so $x \in A$ and $x \in B$. In particular, $x \in A$, showing $X \subseteq A$. Let again $x \in X$. Then from $X \subseteq A \cap B$ we have $x \in A \cap B$, so (again) $x \in A$ and $x \in B$. ... B, showing $X \subseteq B$.

(b) $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$

This proposition does not always hold.

Here is a counter-example.

Let $A = \{a\}$ and $B = \{b\}$.

Then $\mathcal{P}(A) = \{\emptyset, \{a\}\}$ and $\mathcal{P}(B) = \{\emptyset, \{b\}\}$.

$$A \cup B = \{a, b\}$$

$$\begin{aligned} \mathcal{P}(A \cup B) &= \{\emptyset, \{a\}, \{b\}, \{a, b\}\} \\ &\neq \{\emptyset, \{a\}, \{b\}\} \\ &= \mathcal{P}(A) \cup \mathcal{P}(B). \end{aligned}$$

3. Prove that a relation R is transitive if and only if $R^2 \subseteq R$. Use this then to show that the transitive closure of a transitive relation R is R itself.

This is a somewhat lengthy task.
We show several things. Let $R \subseteq A \times A$.

(1) R is transitive iff $R^2 \subseteq R$.

Recall that

$$R^2 = \{(x,z) \in A \times A \mid \exists y\, [y \in A : (x,y) \in R \wedge (y,z) \in R]\}$$

($\Rightarrow$) Let R be a transitive relation and let $(x,z) \in R^2$.
Let $y \in A$ be such that $(x,y) \in R$ and $(y,z) \in R$.
(This y exists since $(x,z) \in R^2$.)
Then from $(x,y) \in R$, $(y,z) \in R$ and R is transitive, we get $(x,z) \in R$. Hence we have shown $R^2 \subset R$ under the assumption that R is transitive.

($\Leftarrow$) Assume now that $R^2 \subseteq R$.
Let $x,y,z \in A$ be such that $(x,y) \in R$ and $(y,z) \in R$. Then from the definition of R^2, we get $(x,z) \in R^2$, and from $R^2 \subseteq R$ we get further $(x,z) \in R$ showing that R is transitive.

(2) If R is transitive, then
$R^+ = R$.

Recall that $R^+ = \bigcup_{n \geq 1} R^n$.

Since $R = R^1$, it is clear that $R \subseteq R^+$.

For the opposite inclusion, we need two simpler properties (lemmas), that we'll prove separately.

(*) $\forall n \, [n \geq 1 : R^n \subseteq R]$

(**) If $\{A_i \mid i \in I\}$ is a family of sets and A is a set such that $\forall i \, [i \in I : A_i \subseteq A]$, then $\bigcup_{i \in I} A_i \subseteq A$.

Once we get (*) and (**), we proceed as follows.
We consider the family $\{B_i \mid i \in I\}$ where $I = \{n \in \mathbb{N} \mid n \geq 1\}$ given by
$$B_n = R^n.$$
From (*) we have $\forall i \, [i \in I : B_i \subseteq R]$.
Then from (**) we get
$$\bigcup_{i \in I} B_i = \bigcup_{n \geq 1} R^n \subseteq R.$$

It remains to prove (*) and (**).

We prove (*) by induction on $n \geq 1$.

<u>Base</u>: <u>$n=1$</u>, the statement holds since $R^1 = R \subseteq R$.

<u>Inductive hypothesis</u>: Assume $R^n \subseteq R$.

<u>Inductive step</u>: Consider R^{n+1}.

By definition $R^{n+1} = R^n \circ R$.

From the inductive hypothesis we have $R^n \subseteq R$.

Now from a simple property

(***) Let R, S, T be relations on a set A, then

if $R \subseteq S$, then $R \circ T \subseteq S \circ T$.

[called monotonicity of relation composition]

we get, from $R^n \subseteq R$ and $R \subseteq R$, that

$$R^n \circ R \subseteq R \circ R = R^2 \underset{\boxed{\blacktriangle}}{\subseteq} R.$$

Hence $R^{n+1} \subseteq R$.

The inclusion marked by $\boxed{\blacktriangle}$ holds since by assumption R is transitive, so it amounts to using (1): if R is transitive, then $R^2 \subseteq R$.

Hence, if we prove (***), the proof of (*) will be completed.

For (***):

Let R, S, T be relations on a set A and assume $R \subseteq S$.

Let $(x,z) \in R \circ T$. This means that there is a $y \in A$ such that $(x,y) \in R$ and $(y,z) \in T$.

From $(x,y) \in R$ and $R \subseteq S$, we get
$(x,y) \in S$.

Hence $(x,y) \in S$ and $(y,z) \in T$.
But this means that $(x,z) \in S \circ T$, and completes the proof of (***).

Finally, it remains to show (**).
Let $\{A_i \mid i \in I\}$ be a family of sets with the property that $\forall i[i \in I : A_i \subseteq A]$ where A is a set.
Let $x \in \bigcup_{i \in I} A_i$. This means, by definition, that there exists an index, say $j \in I$, such that
$x \in A_j$. From $\forall i[i \in I : A_i \subseteq A]$ we have that in particular for $j \in I$, $A_j \subseteq A$.
From $x \in A_j$ and $A_j \subseteq A$, we get $x \in A$.
Hence, we have proven $\bigcup_{i \in I} A_i \subseteq A$.

This completes the proof. ∎

4 Let $f: A \to B$ be given. Show that

(a) f is injective iff for any two functions $g_1, g_2 : C \to A$ it holds that

$$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2$$

(b) f is surjective iff for any two functions $g_1, g_2 : B \to C$ it holds that

$$g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2 .$$

(a) $\boxed{\Rightarrow}$ Let f be injective.

Let $g_1, g_2 : C \to A$ be two functions such that $f \circ g_1 = f \circ g_2$.

Let $x \in C$. Then from the assumption on g_1 and g_2 we get that

$f(g_1(x)) = f \circ g_1(x) = f \circ g_2(x) = f(g_2(x))$.

Now from the assumption that f is injective and from $f(g_1(x)) = f(g_2(x))$ we get

$$g_1(x) = g_2(x).$$

Since x was arbitrary and g_1 and g_2 have the same domain and codomain, we have that

$$g_1 = g_2.$$

$\boxed{\Leftarrow}$ Assume that for any two functions

$g_1, g_2 : C \to A$ it holds that

$$f \circ g_1 = f \circ g_2 \Rightarrow g_1 = g_2.$$

We want to show that f is injective.

Let $x, y \in A$ be such that $f(x) = f(y)$.

Consider the two constant functions

$g_x : C \to A$ and $g_y : C \to A$ where C is any nonempty set

[one could also take just a singlton $C = \{*\}$]

defined by $g_x(c) = x$, $g_y(c) = y$ for all $c \in C$.

Then we have that $f \circ g_x = f \circ g_y$, since for all $c \in C$

$$f \circ g_x(c) = f(g_x(c)) = f(x) = f(y) = f(g_y(c)) = \\ = f \circ g_y(c).$$

Hence, from the assumption, we get

$$g_x = g_y.$$

But this shows that (taking any $c \in C$)

$x = g_x(c) = g_y(c) = y$, and hence we have shown that f is injective.

(b) $\boxed{\Rightarrow}$ Let f be surjective.

Let $g_1, g_2 : B \to C$ be two functions such that

$$g_1 \circ f = g_2 \circ f.$$

Let $y \in B$. Since f is surjective, there exists an $x \in A$ s.t. $f(x) = y$. Then we have

$$g_1(y) = g_1(f(x)) = g_1 \circ f(x) = g_2 \circ f(x) = g_2(f(x)) = g_2(y)$$

which shows (since $y \in B$ was arbitrary and g_1, g_2 have the same domain and codomain) that $g_1 = g_2$.

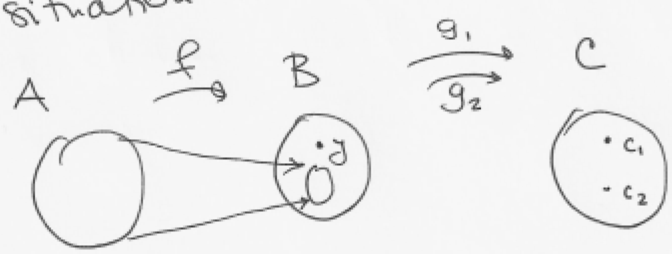
$\boxed{\Leftarrow}$ Assume that for any two functions $g_1, g_2 : B \to C$ it holds that

$$g_1 \circ f = g_2 \circ f \Rightarrow g_1 = g_2. \quad (*)$$

Assume that f is not surjective (towards a contradiction).

Then we will construct two functions g_1, g_2 for which $(*)$ does not hold.

The situation is



f is not surjective, there exists $y \in B$

s.t. $y \notin f(A)$ i.e.

$y \neq f(x)$ for all $x \in A$.

Let $C = \{c_1, c_2\}$ and define

$g_1 : B \to C$, $g_2 : B \to C$ by

$g_1(x) = c_1$, for all $x \in B$ and

$$g_2(x) = \begin{cases} c_1, & x \neq y \\ c_2, & x = y \end{cases}$$

Then we have that

$g_1 \circ f = g_2 \circ f$, since for any $x \in A$, $f(x) \neq y$, so

$$g_1 \circ f(x) = g_1(f(x)) = c_1 = g_2(f(x)) = g_2 \circ f(x).$$

But obviously $g_1 \neq g_2$,

(namely $g_1(y) = c_1 \neq c_2 = g_2(y)$)

which contradicts (*). $\blacksquare$

5 $A^B = \{f \mid f : B \to A\}$.

What is the cardinality of A^B if

$A = \{0,1,2,3,4\}$ and $B = \{a,b,c\}$?

Well, the cardinality is $125 = 5^3$.

To give a function $f : B \to A$ means to specify $f(a), f(b), f(c) \in \{0,1,2,3,4\}$

There are ~~three~~ five possibilities for $f(a)$,
five for $f(b)$, and
five for $f(c)$.

They can be combined in any possible way, so the total number of functions is $5 \cdot 5 \cdot 5 = 5^3$.

Prove that $\{0,1\}^{\mathbb{N}}$ is nondenumerable.

$\{0,1\}^{\mathbb{N}}$ is the set of all functions from $\mathbb{N}$ to $\{0,1\}$.

Equivalently, it is the set of all infinite sequences (of 0's and 1's).
$(a_i \mid i \in \mathbb{N})$ with $a_i \in \{0,1\}$

The proof that this is nondenumerable is given in the Book, page 311-312, please read it there.