SAMPLE PROOF

In the lecture on Jan 27 we discussed three possible proofs for the Problem below. The purpose of this document is to show how we can write up the second proof in complete sentences so that

- the logic of the proof is clear:
  in particular, we state the method(s) of proof — if different from 'direct proof' —, and state the assumption(s) and the desired conclusion(s);
- each step of the proof is properly justified:
  that is, in each step, we cite the
  - assumption(s),
  - definition(s),
  - theorem(s), and/or
  - statement(s) we have proved already (in the current proof)

  that we are using to make the deduction.

On the next page you will see the 'blackboard version' of the same proof, which has all these features, except that it does not use complete sentences.

Problem.
Let $f\colon A \to B$ and $g\colon B \to C$ be functions. Prove that if $g \circ f$ is injective, then so is f.

- This is a statement from part (5) of Theorem 2.5 from the handout "Background on Sets, Relations, and Functions" for the Jan 25 lecture. In the proof you may use any definitions and theorems from the last lecture which precede this statement.

Solution. Given the assumption of the problem:

(A1) $f\colon A \to B$ and $g\colon B \to C$ are arbitrary functions,

we want to show that "if $g \circ f$ is injective, then so is f". We will prove this statement by proving its contrapositive, which is:

"if f is not injective, then $g \circ f$ is not injective".

To this end, assume

(A2) f is not injective.

Our goal is to prove that $g \circ f$ is not injective. By assumption (A1), f is a function, so by the definition of injectivity in Def. 2.3[1] (applied to f) we get from assumption (A2) that there exist elements $a_1, a_2 \in A$ such that $a_1 \neq a_2$ and $f(a_1) = f(a_2)$. Here $f(a_1) = f(a_2) \in B$, and since g is a function $B \to C$ (see (A1) again), we get that $g(f(a_1)) = g(f(a_2))$. By the definition of $\circ$ in Def. 2.1 — as it applies to functions (cf. Thm. 2.5(1)) — we see that the left hand side of the last equality is $(g \circ f)(a_1)$, while the right hand side is $(g \circ f)(a_2)$. Thus, $(g \circ f)(a_1) = (g \circ f)(a_2)$. Since $a_1 \neq a_2$, the definition of injectivity (now applied to $g \circ f$) implies that $g \circ f$ is not injective. $\square$

[1] All definitions and theorems cited by number are from the handout "Background on Sets, Relations, and Functions" mentioned above.

Blackboard version of this proof from the Jan 27 lecture:

Second proof:

$\boxed{\text{DIRECT PROOF}}$

Assume: (A1) $f: A \to B$, $g: B \to C$ are arbitrary functions.

Want to show: If $g \circ f$ is injective, then f is injective.

to prove this:

$\boxed{\text{prove the contrapositive}}$, which is:

If f is not injective, then $g \circ f$ is not injective.

to prove this

Assume: (A2) f is not injective

Want to show: $g \circ f$ is not injective

Proof: Use (A2)

$\Downarrow$ def of inj. (for f)

there exist $a_1, a_2 \in A$ with $a_1 \neq a_2$ such that $f(a_1) = f(a_2)$.

Then

$$g(f(a_1)) = g(f(a_2))$$

by def of $\circ$

$$(g \circ f)(a_1) \overset{!}{=} (g \circ f)(a_2)$$

$\Downarrow$ def of inj. (for $g \circ f$)

$g \circ f$ is <u>not</u> injective