1. **Formal definition for the notion of relations and functions, and re-formulation of the definition of surjectivity and injectivity.**

   (a) *Let $D, R, H$ be sets. The ordered triple $(D, R, H)$ is called a* **relation from** $D$ **to** $R$ *if $H \subset D \times R$.*

   (b) *Let $D, R$ be sets, and $H$ be a subset of $D \times R$. The relation $(D, R, H)$ is said to be a* **function from domain** $D$ **to range** $R$ **with graph** $H$ *if both of the statements $(E), (U)$ below hold:*

   $(E)$: *For any $t \in D$, there exists some $u \in R$ such that $(t, u) \in H$.*
   $(U)$: *For any $t \in D$, for any $u, v \in R$, if $(t, u) \in H$ and $(t, v) \in H$ then $u = v$.*

   *Where we refer to $(D, R, H)$ as $h$, we write $u = h(t)$ exactly when $(t, u) \in H$.*

   (c) *Let $D, R$ be sets, and $h : D \longrightarrow R$ be a function from $D$ to $R$ with graph $H$.*

   i. *$h$ is said to be* **surjective** *if the statement $(S)$ below holds:*
   $(S)$: *For any $u \in R$, there exists some $t \in D$ such that $(t, u) \in H$.*

   ii. *$h$ is said to be* **injective** *if the statement $(I)$ below holds:*
   $(I)$: *For any $u \in R$, for any $t, s \in D$, if $(t, u) \in H$ and $(s, u) \in H$ then $t = s$.*

2. **Definition for the notion of bijective function.**

   *Let $D, R$ be sets, and $h : D \longrightarrow R$ be a function from $D$ to $R$. $h$ is said to be* **bijective** *if $h$ is both surjective and injective.*

   **Remark.** Hence $h = (D, R, H)$ is a bijective function from $D$ to $R$ with graph $H$ iff all of the statements $(E), (U), (S), (I)$ below hold:

   $(E)$: *For any $t \in D$, there exists some $u \in R$ such that $(t, u) \in H$.*
   $(U)$: *For any $t \in D$, for any $u, v \in R$, if $(t, u) \in H$ and $(t, v) \in H$ then $u = v$.*
   $(S)$: *For any $u \in R$, there exists some $t \in D$ such that $(t, u) \in H$.*
   $(I)$: *For any $u \in R$, for any $t, s \in D$, if $(t, u) \in H$ and $(s, u) \in H$ then $t = s$.*

3. **Definition. (Notion of inverse function).**

   *Let $A, B$ be sets, and $f : A \longrightarrow B$, $g : B \longrightarrow A$ be functions. $g$ is said to be an* **inverse function** *of $f$ if both of the following statements hold:*

   (†) *For any $x \in A$, $(g \circ f)(x) = x$.*  (‡) *For any $y \in B$, $(f \circ g)(y) = y$.*

   **Definition. (Identity function.)**

   *Let $C$ be a set. Define the function $\mathsf{id}_C : C \longrightarrow C$ by $\mathsf{id}_C(z) = z$ for any $z \in C$. $\mathsf{id}_C$ is called the* **identity function** *on the set $C$.*

   **Theorem (1). (Re-formulation of the definition of inverse function.)**

   *Let $A, B$ be sets, and $f : A \longrightarrow B$, $g : B \longrightarrow A$ be functions. The statements below are logically equivalent:*

   $(\star_0)$ *$g$ is an inverse function of $f$.*
   $(\star_1)$ *$g \circ f = \mathsf{id}_A$ and $f \circ g = \mathsf{id}_B$ as functions.*
   $(\star_2)$ *$f$ is an inverse function of $g$.*
   $(\star_3)$ *For any $x \in A$, for any $y \in B$, ($y = f(x)$ iff $x = g(y)$).*

4. **Theorem (2). (Uniqueness of inverse function.)**

   *Let $A, B$ be sets, and $f : A \longrightarrow B$ be a function. $f$ has at most one inverse function.*

   **Theorem (3). (Necessary condition for existence of inverse function.)**

   *Let $A, B$ be sets, $f : A \longrightarrow B$ be a function. Suppose $f$ has an inverse function, say, $g : B \longrightarrow A$. Then each of $f, g$ is bijective.*

   **Question.** *Is the necessary condition sufficient as well? Why?*

   **Answer.** *Yes. Reason: Theorem (4).*

5. **Theorem (4). (Existence and Uniqueness of inverse function for a bijective function.)**

   *Let $A, B$ be sets, and $f : A \longrightarrow B$ be a function. Suppose $f$ is bijective. Then there exists some unique bijective function $g : B \longrightarrow A$ such that $g$ is the inverse function of $f$.*

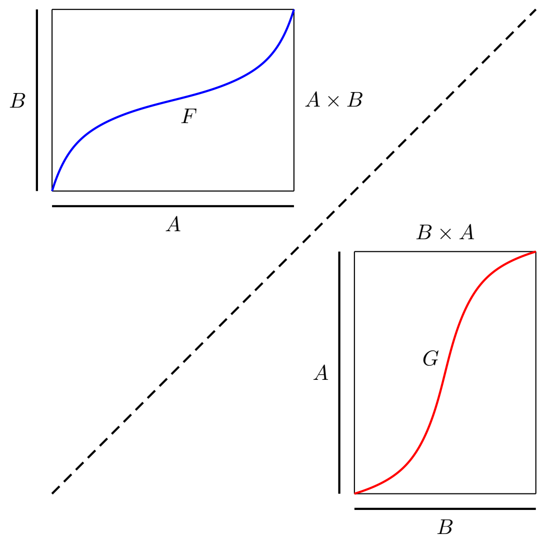
   **Convention on notations.** Because of the uniqueness of $g$ as the inverse function of a function $f$ (when such exists), we agree to write $g$ as $f^{-1}$.

6. **Proof of Theorem (4).**

Let $A, B$ be sets, and $f : A \longrightarrow B$ be a function. Suppose $f$ is bijective.

[Ask: How to write down an inverse function of $f$? What will its graph be?]

Denote by $F$ the graph of $f$. Define $G = \{(y, x) \mid x \in A \text{ and } y \in B \text{ and } (x, y) \in F\}$.




By definition, $G \subset B \times A$. Moreover, the statement ($\sharp$) holds:

($\sharp$): For any $t \in A$, for any $u \in B$, $((t, u) \in F$ iff $(u, t) \in G)$.

Define $g$ to be the ordered triple $(B, A, G)$. By definition, $g$ is a relation from $B$ to $A$ with graph $G$. [We verify that $g$ is a bijective function and $g$ is an inverse function of $f$.]

Since $f : A \longrightarrow B$ is a bijective function, the following statements hold:

$(E)$: For any $x \in A$, there exists some $y \in B$ such that $(x, y) \in F$.
$(U)$: For any $x \in A$, for any $y, z \in B$, if $(x, y) \in F$ and $(x, z) \in F$ then $y = z$.
$(S)$: For any $y \in B$, there exists some $x \in A$ such that $(x, y) \in F$.
$(I)$: For any $y \in B$, for any $x, w \in A$, if $(x, y) \in F$ and $(w, y) \in F$ then $x = w$.

Consider the relation $g = (B, A, G)$. [We are going to apply ($\sharp$).]

By $(S)$, the statement $(E')$ holds: for any $y \in B$, there exists some $x \in A$ such that $(y, x) \in G$.
By $(I)$, the statement $(U')$ holds: for any $y \in B$, for any $x, w \in A$, if $(y, x) \in G$ and $(y, w) \in G$ then $x = w$.
Therefore $g$ is a function from $B$ to $A$.
By $(E)$, the statement $(S')$ holds: for any $x \in A$, there exists some $y \in B$ such that $(y, x) \in G$.
Hence $g$ is a surjective function.
By $(U)$, the statement $(I')$ holds: for any $x \in A$, for any $y, z \in B$, if $(y, x) \in G$ and $(z, x) \in G$ then $y = z$.
Hence $g$ is an injective function. It follows that $g$ is a bijective function from $B$ to $A$.

[Ask: Is $g$ indeed an inverse function of $f$?]

Pick any $x \in A$, $y \in B$. Note that $y = f(x)$ iff $(x, y) \in F$ iff $(y, x) \in G$ iff $x = g(y)$. It follows from Theorem (1) that $g$ is an inverse function of $f$. By Theorem (2), $g$ is the unique inverse function of $f$.

7. **Theorem (5).**

*Let $A, B, C$ be sets and $f : A \longrightarrow B$, $g : B \longrightarrow C$ be bijective functions.*

*The statements below hold:*

(a) $f^{-1} \circ f = \mathsf{id}_A$ *and* $f \circ f^{-1} = \mathsf{id}_B$.
(b) *For any* $x \in A$, *for any* $y \in B$, $y = f(x)$ *iff* $x = f^{-1}(y)$.
(c) $f^{-1}$ *is a bijective function. Moreover,* $(f^{-1})^{-1} = f$.
(d) $g \circ f$ *is a bijective function. Moreover,* $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

**Remark.** The proof of Theorem (5) is left as an exercise.