1 Invertible functions

[readtex `set-theory/sections/02_functions/02_image-and-preimage.ftl.tex`]

Let u, v, w denote objects. Let x, y, z denote sets. Let f, g, h denote functions.

1.1 Definitions and basic properties

We call a function f *invertible* if there is a function g that undoes the operation of f, i.e. applying f after g and applying g after f each results in the identity function.

Definition 1.1. An inverse of f is a function g from $\mathrm{range}(f)$ to $\mathrm{dom}(f)$ such that

$$f(u) = v \iff g(v) = u$$

for all $u \in \mathrm{dom}(f)$ and all $v \in \mathrm{dom}(g)$.

Definition 1.2. f is invertible iff f has an inverse.

Lemma 1.3. Let g, g' be inverses of f. Then $g = g'$.

Proof. We have $\mathrm{dom}(g) = \mathrm{range}(f) = \mathrm{dom}(g')$.

Let us show that $g(v) = g'(v)$ for all $v \in \mathrm{range}(f)$. Let $v \in \mathrm{range}(f)$. Take $u = g'(v)$. Then $g(v) = u$ iff $f(u) = v$. We have $f(u) = v$ iff $g'(v) = u$. Thus $g(v) = g'(v)$. End.

Hence the thesis (by **??**). Indeed $\mathrm{dom}(g) = \mathrm{dom}(g')$. □

Definition 1.4. Let f be invertible. f^{-1} is the inverse of f.

Let f is involutory stand for f is the inverse of f. Let f is selfinverse stand for f is the inverse of f.

Proposition 1.5. Let f be a function from x onto y and g be a function from y onto x. Then g is the inverse of f iff $g \circ f = \mathrm{id}_x$ and $f \circ g = \mathrm{id}_y$.

Proof. Case g is the inverse of f. We have $\mathrm{dom}(g \circ f) = \mathrm{dom}(f) = x = \mathrm{dom}(\mathrm{id}_x)$. For all $u \in x$ we have $(g \circ f)(u) = g(f(u)) = u$. Hence $g \circ f = \mathrm{id}_x$.

We have $\mathrm{dom}(f \circ g) = \mathrm{dom}(g) = y = \mathrm{dom}(\mathrm{id}_y)$. For all $v \in y$ we have $(f \circ g)(v) = f(g(v)) = v$. Hence $f \circ g = \mathrm{id}_y$. End.

Case $g \circ f = \mathrm{id}_x$ and $f \circ g = \mathrm{id}_y$. Then $\mathrm{dom}(g) = y = \mathrm{range}(f)$ and $\mathrm{range}(g) = x = \mathrm{dom}(f)$. Let $u \in \mathrm{dom}(f)$ and $v \in \mathrm{dom}(g)$. If $f(u) = v$ then $g(v) = g(f(u)) = (g \circ f)(u) = \mathrm{id}_x(u) = u$. If $g(v) = u$ then $f(u) = f(g(v)) = (f \circ g)(v) = \mathrm{id}_y(v) = v$. Hence $f(u) = v$ iff $g(v) = u$. End. □

Proposition 1.6. Let f be an invertible function from x onto y. Then f^{-1} is an invertible function from y onto x such that $(f^{-1})^{-1} = f$.

Proof. f^{-1} is a function from y to x. Indeed $\mathrm{range}(f) = y$ and $\mathrm{dom}(f) = x$. f^{-1} is a function onto x. Indeed for any $u \in x$ we have $f^{-1}(f(u)) = u$. f^{-1} is the inverse of f. Thus $f \circ f^{-1} = \mathrm{id}_y$ and $f^{-1} \circ f = \mathrm{id}_x$. Therefore f is the inverse of f^{-1} (by 1.5). □

Proposition 1.7. Let f be an invertible function from x onto y. Then $f \circ f^{-1} = \mathrm{id}_y$ and $f^{-1} \circ f = \mathrm{id}_x$.

Proof. f^{-1} is a function from y onto x (by 1.6). f^{-1} is the inverse of f. Hence the thesis (by 1.5). □

Proposition 1.8. Let f be an invertible function from x onto y. Then ($f^{-1}(f(u)) = u$ for all $u \in x$) and ($f(f^{-1}(v)) = v$ for all $v \in y$).

Proof. Let us show that $f^{-1}(f(u)) = u$ for all $u \in x$. Let $u \in x$. Then $f^{-1}(f(u)) = (f^{-1} \circ f)(u) = \mathrm{id}_x(u) = u$. End.

Let us show that $f(f^{-1}(v)) = v$ for all $v \in y$. Let $v \in y$. Then $f(f^{-1}(v)) = (f \circ f^{-1})(v) = \mathrm{id}_y(v) = v$. End. □

Proposition 1.9. Let f be an invertible function from x onto y and g be an invertible function from y onto z. Then $g \circ f$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Proof. f^{-1} is a function from y onto x. g^{-1} is a function from z onto y. Take $h = f^{-1} \circ g^{-1}$. [prover vampire] Then h is a function from z onto x (by **??**). [prover eprover] $g \circ f$ is a function from x to z.

Let us show that $((g \circ f) \circ h) = \mathrm{id}_z$. We have $f \circ (f^{-1} \circ g^{-1}) = (f \circ f^{-1}) \circ g^{-1}$ (by **??**). Indeed $f \circ (f^{-1} \circ g^{-1})$ and $(f \circ f^{-1}) \circ g^{-1}$ are functions of z. $f \circ h$ is a function from z to y. Hence

$$\begin{aligned}
&(g \circ f) \circ h \\
&= g \circ (f \circ h) \\
&= g \circ (f \circ (f^{-1} \circ g^{-1})) \\
&= g \circ ((f \circ f^{-1}) \circ g^{-1}) \\
&= g \circ (\mathrm{id}_y \circ g^{-1}) \\
&= g \circ g^{-1} \\
&= \mathrm{id}_z .
\end{aligned}$$

End.

Let us show that $h \circ (g \circ f) = \mathrm{id}_x$. We have $(f^{-1} \circ g^{-1}) \circ g = f^{-1} \circ (g^{-1} \circ g)$ (by **??**). $g \circ f$ is a function from x to z. Hence

$$\begin{aligned} &h \circ (g \circ f) \\ &= (h \circ g) \circ f \\ &= ((f^{-1} \circ g^{-1}) \circ g) \circ f \\ &= (f^{-1} \circ (g^{-1} \circ g)) \circ f \\ &= (f^{-1} \circ \mathrm{id}_y) \circ f \\ &= f^{-1} \circ f \\ &= \mathrm{id}_x \,. \end{aligned}$$

End.

Thus h is the inverse of $g \circ f$ (by 1.5). Indeed $g \circ f$ is a function from x onto z and h is a function from z onto x. □

Proposition 1.10. Let f be an invertible function from x onto y and $a \subseteq x$. Then $f \restriction a$ is invertible and $(f \restriction a)^{-1} = f^{-1} \restriction f[a]$.

Proof. $f \restriction a$ is a function from a onto $f[a]$. Take $g = f^{-1} \restriction f[a]$. Then g is a function of $f[a]$.

Let us show that $a \subseteq \mathrm{range}(g)$. Let $u \in a$. Then $f(u) \in f[a]$. Hence $g(f(u)) = f^{-1}(f(u)) = u$. Thus u is a value of g. End.

Let us show that $\mathrm{range}(g) \subseteq a$. Let $u \in \mathrm{range}(g)$. Take $v \in f[a]$ such that $u = g(v)$. Take $w \in a$ such that $v = f(w)$. Then $u = (f^{-1} \restriction f[a])(v) = f^{-1}(v) = f^{-1}(f(w)) = w$. Hence $u \in a$. End.

Hence $\mathrm{range}(g) = a$. Thus g is a function onto a.

Let us show that $g((f \restriction a)(u)) = u$ for all $u \in a$. Let $u \in a$. Then $g((f \restriction a)(u)) = g(f(u)) = (f^{-1} \restriction f[a])(f(u)) = f^{-1}(f(u)) = u$. End.

Let us show that $((f \restriction a)(g(v))) = v$ for all $v \in f[a]$. Let $v \in f[a]$. Take $u \in a$ such that $v = f(u)$. We have $g(v) = g(f(u)) = (f^{-1} \restriction f[a])(f(u)) = f^{-1}(f(u)) = u$. Hence $(f \restriction a)(g(v)) = (f \restriction a)(u) = f(u) = v$. End.

Thus $g \circ (f \restriction a) = \mathrm{id}_a$ and $(f \restriction a) \circ g = \mathrm{id}_{f[a]}$. Therefore g is the inverse of $f \restriction a$. □

Proposition 1.11. Let f be an invertible function from x onto y and $b \subseteq y$. Then $f^{-}[b] = f^{-1}[b]$.

Proof. We have $f^{-1}[b] = \left\{ f^{-1}(v) \;\middle|\; v \in b \right\}$ and $f^{-}[b] = \{ u \in x \mid f(u) \in b \}$.

Let us show that $f^{-}[b] \subseteq f^{-1}[b]$. Let $u \in f^{-}[b]$. Take $v \in b$ such that $v = f(u)$. Then $f^{-1}(v) = f^{-1}(f(u)) = u$. Hence $u \in f^{-1}[b]$. End.

Let us show that $f^{-1}[b] \subseteq f^{-}[b]$. Let $u \in f^{-1}[b]$. Take $v \in b$ such that $u = f^{-1}(v)$. Then $f(u) = f(f^{-1}(v)) = v$. Hence $u \in f^{-}[b]$. End. $\square$

Corollary 1.12. Let f be an invertible function from x onto y and $v \in y$. Then $f^{-}[\{v\}] = \{f^{-1}(v)\}$.

Proof. $f^{-}[\{v\}] = f^{-1}[\{v\}]$. We have $f^{-1}[\{v\}] = \left\{ f^{-1}(w) \mid w \in \{v\} \right\}$. Hence $f^{-1}[\{v\}] = \{f^{-1}(v)\}$. $\square$

Proposition 1.13. Let f be a function from x onto y. f is invertible iff f is one to one.

Proof. Case f is invertible. Let $u, v \in x$. Assume $f(u) = f(v)$. Then $u = f^{-1}(f(u)) = f^{-1}(f(v)) = v$. End.

Case f is one to one. Define $g(v) =$ choose $u \in x$ such that $f(u) = v$ in u for $v \in y$. g is a function from y to x. For all $v \in y$ and all $u, u' \in x$ such that $f(u) = v = f(u')$ we have $u = u'$. Hence g is a function from y onto x. For all $u \in x$ we have $g(f(u)) = u$. For all $v \in y$ we have $f(g(v)) = v$. Hence g is the inverse of f. End. $\square$

Corollary 1.14. Let f be an invertible function from x onto y. Then f^{-1} is a bijection between y and x.

Proof. f^{-1} is a function from y onto x. f^{-1} is invertible. Hence f^{-1} is one to one. Thus f^{-1} is a function from y into x. Therefore f^{-1} is a bijection between y and x. $\square$

1.2 Involutions

A special case of invertible functions are *involutions*, i.e. functions which are self-inverse on their domain.

Definition 1.15. An involution on x is a selfinverse function f on x.

Proposition 1.16. id_x is an involution on x.

Proof. id_x is a function on x. We have $\mathrm{id}_x \circ \mathrm{id}_x = \mathrm{id}_x$. Hence id_x is selfinverse. $\square$

Proposition 1.17. Let f and g be involutions on x. Then $g \circ f$ is an involution on x iff $g \circ f = f \circ g$.

Proof. Case $g \circ f$ is an involution on x. Then $(g \circ f)^{-1} = f^{-1} \circ g^{-1} = f \circ g$. End.

Case $g \circ f = f \circ g$. $f \circ f$, $f \circ g$ and $f \circ g$ are functions on x. Hence

$$(g \circ f) \circ (g \circ f)$$

$$
\begin{aligned}
&= (g \circ f) \circ (f \circ g) \\
&= ((g \circ f) \circ f) \circ g \\
&= (g \circ (f \circ f)) \circ g \\
&= (g \circ \mathrm{id}_x) \circ g \\
&= g \circ g \\
&= \mathrm{id}_x \,.
\end{aligned}
$$

Thus $g \circ f$ is selfinverse. End. ☐

Corollary 1.18. Let f be an involutions on x. Then $f \circ f$ is an involution on x.

Proposition 1.19. Let f be an involution on x. Then f is a permutation of x.

Proof. f is an invertible function from x onto x. Hence f is a bijection between x and x. Thus f is a permutation of x. ☐