P.4. Example proofs

P.4.1. An inverse function to f exists if and only if f is bijective.—

Theorem P.4.1. — *Let $f\colon S \to T$ be a function. The inverse function to f exists if and only if f is bijective.*

Proof. —

$\Rightarrow$: Assume $f\colon S \to T$ has an inverse function $f^{-1}\colon T \to S$.
To show: (a) f is injective.
(b) f is surjective.
(a) Assume $s_1, s_2 \in S$ and $f(s_1) = f(s_2)$.
To show: $s_1 = s_2$.

$$s_1 = f^{-1}f(s_1)) = f^{-1}f(s_2)) = s_2.$$

So f is injective.
(b) Let $t \in T$.
To show: There exists $s \in S$ such that $f(s) = t$.
Let $s = f^{-1}(t)$.
Then

$$f(s) = f(f^{-1}(t)) = t.$$

So f is surjective.
So f is bijective.

$\Leftarrow$: Assume $f\colon S \to T$ is bijective.
To show: f has an inverse function.
We need to define a function $\varphi\colon T \to S$.
Let $t \in T$.
Since f is surjective there eists $s \in S$ such that $f(s) = t$.
Define $\varphi(t) = s$.
To show: (a) φ is well defined.
(b) φ is an inverse function to f.
(a) To show: (aa) If $t \in T$ then $\varphi(t) \in S$.
(ab) If $t_1, t_2 \in T$ and $t_1 = t_2$ then $\varphi(t_1) = \varphi(t_2)$.
(aa) This follows from the definition of φ.
(ab) Assume $t_1, t_2 \in T$ and $t_1 = t_2$.
Let $s_1, s_2 \in S$ such that $f(s_1) = t_1$ and $f(s_2) = t_2$.
Since $t_1 = t_2$ then $f(s_1) = f(s_2)$.
Since f is injective this implies that $s_1 = s_2$.
So $\varphi(t_1) = s_1 = s_2 = \varphi(t_2)$.
So φ is well defined.
(b) To show: (ba) If $s \in S$ then $\varphi(f(s)) = s$.
(bb) If $t \in T$ then $f(\varphi(t)) = t$.
(ba) This follows from the definition of φ.
(bb) Assume $t \in T$.
Let $s \in S$ be such that $f(s) = t$.
Then

$$f(\varphi(t)) = f(s) = t.$$

Notes of Arun Ram aram@unimelb.edu.au, Version: 7 April 2020

So $\varphi \circ f$ and $f \circ \varphi$ are the identity functions on S and T, respectively.
So φ is an inverse function to f.

□

P.4.2. An equivalence relation on S and a partition of S are the same data.—

Let S be a set.

- A *relation* $\sim$ *on* S is a subset $R_\sim$ of $S \times S$. Write $s_1 \sim s_2$ if the pair (s_1, s_2) is in the subset $R_\sim$ so that
$$R_\sim = \{(s_1, s_2) \in S \times S \mid s_1 \sim s_2\}.$$
- An *equivalence relation* on S is a relation $\sim$ on S such that
  (a) if $s \in S$ then $s \sim s$,
  (b) if $s_1, s_2 \in S$ and $s_1 \sim s_2$ then $s_2 \sim s_1$,
  (c) if $s_1, s_2, s_3 \in S$ and $s_1 \sim s_2$ and $s_2 \sim s_3$ then $s_1 \sim s_3$.

Let $\sim$ be an equivalence relation on a set S and let $s \in S$. The *equivalence class of* s is the set
$$[s] = \{t \in S \mid t \sim s\}.$$
A *partition of a set* S is a collection $\mathcal{P}$ of subsets of S such that
(a) If $s \in S$ then there exists $P \in \mathcal{P}$ such that $s \in P$, and
(b) If $P_1, P_2 \in \mathcal{P}$ and $P_1 \cap P_2 \neq \emptyset$ then $P_1 = P_2$.

Theorem P.4.2. —
(a) *If S is a set and let $\sim$ be an equivalence relation on S then*
$$\text{the set of equivalence classes of } \sim \qquad \text{is a partition of } S.$$
(b) *If S is a set and $\mathcal{P}$ is a partition of S then*
$$\text{the relation defined by} \qquad s \sim t \quad \text{if } s \text{ and } t \text{ are in the same } P \in \mathcal{P}$$
is an equivalence relation on S.

Proof. —
(a) To show: (aa) If $s \in S$ then s is in some equivalence class.
(ab) If $[s] \cap [t] \neq \emptyset$ then $[s] = [t]$.
(aa) Let $s \in S$.
Since $s \sim s$ then $s \in [s]$.
(ab) Assume $[s] \cap [t] \neq \emptyset$.
To show: $[s] = [t]$.
Since $[s] \cap [t] \neq \emptyset$ then there is an $r \in [s] \cap [t]$.
So $s \sim r$ and $r \sim t$.
By transitivity, $s \sim t$.
To show: (aba) $[s] \subseteq [t]$.
(abb) $[t] \subseteq [s]$.
(aba) Assume $u \in [s]$.
Then $u \sim s$.
We know $s \sim t$.
So, by transitivity, $u \sim t$.
Therefore $u \in [t]$.
So $[s] \subseteq [t]$.
(aba) Assume $v \in [t]$.

Then $v \sim t$.
We know $t \sim s$.
So, by transitivity, $v \sim s$.
Therefore $v \in [s]$.
So $[t] \subseteq [s]$.
So $[s] = [t]$.
So the equivalence classes partition S.

(b) To show: $\sim$ is an equivalence relation, i.e. that $\sim$ is reflexive, symmetric and transitive.
To show: (ba) If $s \in S$ then $s \sim s$.
(bb) If $s \sim t$ then $t \sim s$.
(bc) If $s \sim t$ and $t \sim u$ then $s \sim u$.
(ba) Since s and s are in the same S_α then $s \sim s$.
(bb) Assume $s \sim t$.
Then s and t are in the same S_α.
So $t \sim s$.
(bb) Assume $s \sim t$ and $t \sim u$.
Then s and t are in the same S_α and t and u are in the same S_α.
So $s \sim u$.
So $\sim$ is an equivalence relation.

□

P.4.3. Identities in a field. —

A *field* is a set $\mathbb{F}$ with functions

$$\begin{array}{ccc} \mathbb{F}\times\mathbb{F} & \longrightarrow & \mathbb{F} \\ (a,b) & \longmapsto & a+b \end{array} \qquad \text{and} \qquad \begin{array}{ccc} \mathbb{F}\times\mathbb{F} & \longrightarrow & \mathbb{F} \\ (a,b) & \longmapsto & ab \end{array}$$

such that

(Fa) If $a, b, c \in \mathbb{F}$ then $(a+b)+c = a+(b+c)$,
(Fb) If $a, b \in \mathbb{F}$ then $a+b = b+a$,
(Fc) There exists $0 \in \mathbb{F}$ such that

$$\text{if } a \in \mathbb{F} \quad \text{then} \quad 0+a = a \text{ and } a+0 = a,$$

(Fd) If $a \in \mathbb{F}$ then there exists $-a \in \mathbb{F}$ such that $a+(-a) = 0$ and $(-a)+a = 0$,
(Fe) If $a, b, c \in \mathbb{F}$ then $(ab)c = a(bc)$,
(Ff) If $a, b, c \in \mathbb{F}$ then

$$(a+b)c = ac+bc \qquad \text{and} \qquad c(a+b) = ca+cb,$$

(Fg) There exists $1 \in \mathbb{F}$ such that

$$\text{if } a \in \mathbb{F} \quad \text{then} \quad 1\cdot a = a \text{ and } a \cdot 1 = a,$$

(Fh) If $a \in \mathbb{F}$ and $a \neq 0$ then there exists $a^{-1} \in \mathbb{F}$ such that $aa^{-1} = 1$ and $a^{-1}a = 1$,
(Fi) If $a, b \in \mathbb{F}$ then $ab = ba$.

Proposition P.4.3. — *Let $\mathbb{F}$ be a field.*
(a) *If $a \in \mathbb{F}$ then $a \cdot 0 = 0$.*
(b) *If $a \in \mathbb{F}$ then $-(-a) = a$.*
(c) *If $a \in \mathbb{F}$ and $a \neq 0$ then $(a^{-1})^{-1} = a$.*
(d) *If $a \in \mathbb{F}$ then $a(-1) = -a$.*

(e) *If* $a, b \in \mathbb{F}$ *then* $(-a)b = -ab$.
(f) *If* $a, b \in \mathbb{F}$ *then* $(-a)(-b) = ab$.

Proof. —

(a) Assume $a \in \mathbb{F}$.

$$\begin{aligned} a \cdot 0 &= a \cdot (0+0), \quad \text{by (Fc)}, \\ &= a \cdot 0 + a \cdot 0, \quad \text{by (Ff)}. \end{aligned}$$

Add $-a \cdot 0$ to each side and use (Fd) to get $0 = a \cdot 0$.

(b) Assume $a \in \mathbb{F}$.
By (Fd),

$$-(-a) + (-a) = 0 = a + (-a).$$

Add $-a$ to each side and use (Fd) to get $-(-a) = a$.

(c) Assume $a \in \mathbb{F}$ and $a \neq 0$.
By (Fh),

$$(a^{-1})^{-1} \cdot a^{-1} = 1 = a \cdot a^{-1}.$$

Multiply each side by a and use (Fh) and (Fg) to get $(a^{-1})^{-1} = a$.

(d) Assume $a \in \mathbb{F}$.
By (Ff),

$$a(-1) + a \cdot 1 = a(-1+1) = a \cdot 0 = 0,$$

where the last equality follows from part (a).
So, by (Fg), $a(-1) + a = 0$.
Add $-a$ to each side and use (Fd) and (Fc) to get $a(-1) = -a$.

(e) Assume $a, b \in \mathbb{F}$.

$$\begin{aligned} (-a)b + ab &= (-a+a)b, \quad \text{by (Ff)}, \\ &= 0 \cdot b, \quad \text{by (Fd)}, \\ &= 0, \quad \text{by part (a)}. \end{aligned}$$

Add $-ab$ to each side and use (Fd) and (Fc) to get $(-a)b = -ab$.

(f) Assume $a, b \in \mathbb{F}$.

$$\begin{aligned} (-a)(-b) &= -(a(-b)), \quad \text{by (e)}, \\ &= -(-ab), \quad \text{by (e)}, \\ &= ab, \quad \text{by part (b)}. \end{aligned}$$

□

P.4.4. Identities in an ordered field. —

An *ordered field* is a field $\mathbb{F}$ with a total order $\leqslant$ such that

(OFa) If $a, b, c \in \mathbb{F}$ and $a \leqslant b$ then $a + c \leqslant b + c$,
(OFb) If $a, b \in \mathbb{F}$ and $a \geqslant 0$ and $b \geqslant 0$ then $ab \geqslant 0$.

Proposition P.4.4. — *Let* $\mathbb{F}$ *be an ordered field.*
(a) *If* $a \in \mathbb{F}$ *and* $a > 0$ *then* $-a < 0$.
(b) *If* $a \in \mathbb{F}$ *and* $a \neq 0$ *then* $a^2 > 0$.
(c) $1 \geqslant 0$.
(d) *If* $a \in \mathbb{F}$ *and* $a > 0$ *then* $a^{-1} > 0$.
(e) *If* $a, b \in \mathbb{F}$ *and* $a \geqslant 0$ *and* $b \geqslant 0$ *then* $a + b \geqslant 0$.

(f) *If* $a, b \in \mathbb{F}$ *and* $0 < a < b$ *then* $b^{-1} < a^{-1}$.

Proof. —

(a) Assume $a \in \mathbb{F}$ and $a > 0$.
Then $a + (-a) > 0 + (-a)$, by (OFb).
So $0 > -a$, by (Fd) and (Fc).

(b) Assume $a \in \mathbb{F}$ and $a \neq 0$.
Case 1: $a > 0$.
Then $a \cdot a > a \cdot 0$, by (OFb).
So $a^2 > 0$, by part (a).
Case 2: $a < 0$.
Then $-a > 0$, by part (a).
Then $(-a)^2 > 0$, by Case 1.
So $a^2 > 0$, by Proposition P.4.3 (f).

(c) To show: $1 \geqslant 0$.
$1 = 1^2 \geqslant 0$, by part (b).

(d) Assume $a \in \mathbb{F}$ and $a > 0$.
By part (b), $a^{-2} = (a^{-1})^2 > 0$.
So $a(a^{-1})^2 > a \cdot 0$, by (OFb).
So $a^{-1} > 0$, by (Fh) and Proposition P.4.3 (a).

(e) Assume $a, b \in \mathbb{F}$ and $a \geqslant 0$ and $b \geqslant 0$.

$$\begin{aligned} a + b &\geqslant 0 + b, && \text{by (OFa),} \\ &\geqslant 0 + 0, && \text{by (OFa),} \\ &= 0, && \text{by (Fc).} \end{aligned}$$

(f) Assume $a, b \in \mathbb{F}$ and $0 < a < b$.
So $a > 0$ and $b > 0$.
Then, by part (d), $a^{-1} > 0$ and $b^{-1} > 0$.
Thus, by (OFb), $a^{-1}b^{-1} > 0$.
Since $a < b$, then $b - a > 0$, by (OFa).
So, by (OFb), $a^{-1}b^{-1}(b - a) > 0$.
So, by (Fh), $a^{-1} - b^{-1} > 0$.
So, by (OFa), $a^{-1} > y^{-1}$.

□