Elements of Set Theory

By Enderton

Shao Hong

Contents

Definitions and Theorems

0.1 Axioms

1. **Axiom of Extensionality**

$$\forall A \forall B[(x \in A \iff x \in B) \implies A = B]$$

2. **Empty Set Axiom**

$$\exists \varnothing \forall x(x \notin B)$$

This can actually be derived from other axioms already; The Axiom of Infinity guarantees the existence of a set, A, thus by using a Subset Axiom, we can construct the empty set, $\varnothing$, as $x \in \varnothing \iff (x \in A \wedge x \neq x)$

3. **Pairing Axiom / Axiom of Pairing**
For any sets u, v, there exists a set B containing (only) u, v.

$$\forall u \forall v \exists B \forall x[x \in B \iff (x = u \vee x = v)]$$

4. **Union Axiom / Axiom of Union**

$$\forall A \exists B \forall x[x \in B \iff \exists b(b \in A \wedge x \in b)]$$

5. **Power Set Axiom**

$$\forall A \forall B \forall x(x \in B \iff x \subseteq A)$$

where we define $\subseteq$ as $\forall x \forall A(x \subseteq A \iff \forall y(y \in x \implies y \in A))$

6. **Axiom Schema of Specifiation / Subset Axioms**:

$$\forall t_1, \ldots, t_k \forall A \exists B \forall x(x \in B \iff [x \in A \wedge \varphi(t_1, \cdots, t_k, A)])$$

Extra Stuff for the Axiom Schema of Specifiation.

7. **Axiom of Infinity / Infinity Axiom**

$$\exists A[\varnothing \in A \wedge \forall a(a \in A \implies a^+ \in A)]$$

8. **Axiom Of Choice / Choice Axiom**

   (a) First Form: For all relations R, there exists a function F such that $F \subseteq R$ and $\operatorname{dom} F = \operatorname{dom} R$.

   (b) Second Form: The Cartesian product of nonempty sets is always nonempty. That is, if H is a function with domain I and if $H(i) \neq \varnothing$, then there exists a function f with domain I such that $(\forall i \in I) f(i) \in H(i)$.
   I think we can also state this more formally as;

$$\forall I \forall H \forall A \left[(H \colon I \to A \wedge H(i) \neq \varnothing) \implies \exists f \left(f \colon I \to \bigcup_{i \in I} H(i) \wedge f(i) \in H(i) \right) \right]$$

   Equivalently, we can also say that for any set X of nonempty sets, there exists a choice function f that is defined on X and maps each set of X to an element of the set:

$$\forall X \left(\varnothing \notin X \implies \exists f \left[f \colon X \to \bigcup X \wedge \forall A(A \in X \implies f(A) \in A) \right] \right)$$

   .

9. **Axiom of Regularity / Regularity Axiom**

$$\forall A[A \neq \varnothing \implies \exists m(m \in A \wedge m \cap A = \varnothing)]$$

10. **Replacement Axioms / Axiom Schema of Replacement**

(Note to self: I haven't read the chapter that covers this yet, so I just slapped this in basically directly from EEOST)

For all formulas $\phi(x, y)$ not containing the B, the following is an axiom:

$$\forall t_1 \cdots \forall t_k \forall A \Big((\forall x \in A) \forall y_1 \forall y_2 \big([\phi(x, y_1) \wedge \phi(x, y_2)] \implies y_1 = y_2 \big) \\ \implies \exists B \forall y [y \in B \iff (\exists x \in A) \phi(x, y)] \Big)$$

0.2 Chapter 2 — Axioms and Operations

Theorem 2A. *There is no set to which every set belongs.*

Proof:

Let A be a set; we will construct a set not belonging to A. Let B be a set such that:

$$B = \{x \in A | x \notin x\}$$

We have, by the construction of B,

$$B \in B \iff (B \in A \wedge B \notin B)$$

Assume $B \in A$, then

$$B \in B \iff B \notin B$$

This statement is obviously a contradiction (always false) since if $B \in B$ is true, then $B \notin B$ which is $\neg(B \in B)$ must be false. Therefore, it must be the case that $B \notin A$.

Theorem 2B. *For any nonempty set A, there exists a unique set $\bigcap A$ such that for any $x \in \bigcap A$, x belongs to every member of A,*

$$\forall x \left[x \in \bigcap A \iff \forall \alpha (\alpha \in A \implies x \in \alpha \right]$$

Proof (that such a set exists) :

We are given that A is nonempty; let c be some fixed member of A. Then by a subset axiom there is a set $\bigcap A$ such that for any x,

$$x \in \bigcap A \iff x \in c \wedge \forall \alpha (\alpha \in A \wedge \alpha \neq c \wedge x \in \alpha) \\ \iff \forall \alpha (\alpha \in A \wedge x \in \alpha)$$

Uniqueness follows from extensionality

Definition. n-tuples

We define the 1-tuple $\langle x \rangle = x$

An ordered pair is defined in the following way:

$$\langle x, y \rangle := \{\{x\}, \{x, y\}\}$$

An n-tuple is defined recursively:

$$\langle x, y, z \rangle := \langle \langle x, y \rangle, z \rangle$$
$$\langle x_1, x_2, \cdots, x_n \rangle = \langle \langle x_1, x_2, \cdots, x_{n-1} \rangle, x_n \rangle$$

Or we could also define an n-tuple as a function (for all $n > 3$)

$$t : \{i \in \mathbb{N} | 1 \leqslant i \leqslant n\} \implies S$$

(Does not cause a contradiction cos we defined a 2-tuple, which are the elements of this set)
(Using this definition we also justify the definition of the 0-tuple as $\varnothing$, since the function $t \colon \varnothing \to S$ is the empty set, i.e. $t = \varnothing$)

Let an ordered pair, $p = \langle x, y \rangle$; the first coordinate, $\pi_1(p)$ can be extracted by:

$$\pi_1(p) = \bigcup \left(\bigcap p \right)$$

The second coordinate, $\pi_2(p)$, can be extracted similarly,

$$\pi_2(p) = \bigcup \left\{ x \in \bigcup p \middle| \left(\bigcup p \neq \bigcap p \right) \implies x \notin \bigcap p \right\}$$

0.3 Chapter 3 — Relations and Functions

Theorem 3A. *$\langle u, v \rangle = \langle x, y \rangle$ iff $u = x$ and $v = y$.*

Proof:

One direction is trivial; if $u = x$ and $v = y$, then $\langle u, v \rangle$ is the same thing as $\langle x, y \rangle$.
To prove the interesting direction, assume that $\langle u, v \rangle = \langle x, y \rangle$, i.e.,

$$\{\{u\}, \{u, v\}\} = \{\{x\}, \{x, y\}\}.$$

Then we have

$$\{u\} \in \{\{x\}, \{x, y\}\} \quad \text{and} \quad \{u, v\} \in \{\{x\}, \{x, y\}\}.$$

From the first of these we know that either

$$(a) \ \{u\} = \{x\} \quad \text{or} \quad (b) \ \{u\} = \{x, y\},$$

and from the second we know that either

$$(c) \ \{u, v\} = \{x\} \quad \text{or} \quad (d) \ \{u, v\} = \{x, y\}$$

First suppose (b) holds; then $u = x = y$. Then (c) and (d) are equivalent, and tell us that $u = v = x = y$. In this case the conclusion of the theorem holds. Similarly if (c) holds, we have the same situation.
There remains the case in which (a) and (d) hold, From (a) we have $u = x$. From (d) we get either $u = y$ or $v = y$. In the first case (b) holds; that case has already been considered. In the second case, we have $v = y$ as desired.

Lemma 3B. *If $x \in C$ and $y \in C$, then $\langle x, y \rangle \in \mathscr{P}\mathscr{P}(C)$.*

Proof:

As the following calculation demonstrates, the fact that the braces in $\{\{x\}, \{x, y\}\}$ are nested to a depth of 2 is responsible for the two applications of the power set operation:

$$\begin{array}{rcl} x \in C & \wedge & y \in C \\ \{x\} \subseteq C & \wedge & \{y\} \subseteq C \\ \{x\} \in \mathscr{P}C & \wedge & \{y\} \in \mathscr{P}C \\ \{\{x\}, \{x, y\}\} & \subseteq & \mathscr{P}C \\ \{\{x\}, \{x, y\}\} & \in & \mathscr{P}\mathscr{P}C \end{array}$$

Corollary 3C. *For any sets A and B, there is a set whose members are exactly the pairs $\langle x, y\rangle$ with $x \in A$ and $y \in B$.*

Proof:

From a subset axiom we can construct

$$\{w \in \mathscr{P}\mathscr{P}(A \cup B) | w = \langle x, y\rangle \wedge x \in A \wedge y \in B\}$$

Clearly this set contains only pairs of the desired sort; by the preceding lemma, it contains them all.

This corollary justifies our earlier definition of the Cartesian product, $A \times B$.

Definition. The Binary Cartesian Product

$$A \times B := \{\langle x, y\rangle \, | x \in A \wedge y \in B\} = \{w \in \mathscr{P}\mathscr{P}(A \cup B) | w = \langle x, y\rangle \wedge x \in A \wedge y \in B\}$$

Definition. Relations

A relation, B, is a set of ordered pairs,

$$\forall z[z \in R \iff \exists x \exists y(z = \langle x, y\rangle)]$$

An n-ary relation, N, is a set of n-tuples,

$$\forall z(z \in N) \iff \exists e_1, e_2, \cdots, e_n(z = \langle e_1, e_2, \cdots, e_n\rangle)$$

M is single-rooted iff for each $y \in \operatorname{ran} R$, there exists one unique x such that xMy. i.e.: M will have the following property

$$(x_1 My \wedge x_2 My) \iff x_1 = x_2$$

We define an n-ary relation on A to be a set of n-tuples with all components in A.
i.e. Let M be an n-ary relation on A, then

1. $\forall z(z \in M) \iff \exists e_1, e_2, \cdots, e_n(e_1, e_2, \cdots, e_n \in A \wedge z = \langle e_1, e_2, \cdots, e_n\rangle)$
2. $M \subseteq A^n$

Definition. We define the *domain* of R ($\operatorname{dom} R$), the *range* of R ($\operatorname{ran} R$)m and the *field* ($\operatorname{fld} R$) by

$$\begin{aligned} x \in \operatorname{dom} R &\iff \exists y \langle x, y\rangle \in R, \\ x \in \operatorname{ran} R &\iff \exists t \langle t, x\rangle \in R, \\ \operatorname{fld} R &= \operatorname{dom} R \cup \operatorname{ran} R \end{aligned}$$

Lemma 3D. *If $\langle x, y\rangle \in A$, then $x, y \in \bigcup\bigcup A$*

Proof:

We assume that $\{\{x\}, \{x, y\}\} \in A$. Consequently, $\{x, y\} \in \bigcup A$ since it belongs to a member of A. And from this we conclude that $x \in \bigcup\bigcup A$ and $y \in \bigcup\bigcup A$.

This lemma indicates how we can use subset axioms to construct the domain and range of R:

$$\begin{aligned} \operatorname{dom} R &:= \left\{x \in \bigcup\bigcup A \,\middle|\, \exists y \, \langle x, y\rangle \in R\right\} \\ \operatorname{ran} R &:= \left\{y \in \bigcup\bigcup A \,\middle|\, \exists x \, \langle x, y\rangle \in R\right\} \end{aligned}$$

Definition. Functions

A function is a relation F such that for all x in $\operatorname{dom} F$, there is only one y such that xFy.

Basically, a function is a relation with the key property that: If $\langle x, y\rangle \in F$ and $\langle x, g\rangle \in F$, then $y = g$, i.e. 1 output for every input (Single-valued).

An n-ary function is a an $(n+1)$-ary relation whose elements are $(n+1)$-tuples.
An n-ary operation is one is a function $O : S^n \to S$.

Definition. ICRI — Inverse, Composition, Restriction, Image

1. (a) The inverse (preimage) of F is the set / relation

$$F^{-1} = \{\langle y, x\rangle \mid xFy\}$$

2. (b) The composition of F and G is the set

$$F \circ G = \{\langle x, y\rangle \mid \exists t(xGt \wedge tFy)\}$$

3. (c) The restriction of F to A is the set

$$F \upharpoonright A = \{\langle x, y\rangle \mid xFy \wedge x \in A\}$$

(d) The image of A under F is the set

$$F[\![A]\!] = \operatorname{ran}(F \upharpoonright A) = \{y \mid (\exists x \in A)xFy\}$$

These operations are most commonly applied to functions, sometimes to relations, but can actually be defined for arbitrary sets A, F, and G. (By "arbitrary" sets, the author probably just mean relations)

Theorem 3E. *For a set F, $\operatorname{dom} F^{-1} = \operatorname{ran} F$ and $\operatorname{ran} F^{-1} = \operatorname{dom} F$. For a relation F, $(F^{-1})^{-1} = F$.*

Proof (Mine):

$$\begin{aligned}\operatorname{dom} F^{-1} &= \{y \mid \exists x(yF^{-1}x)\}\\ &= \{y \mid \exists x(xFy)\}\\ &= \operatorname{ran} F\end{aligned}$$

$$\begin{aligned}\operatorname{ran} F^{-1} &= \{x \mid \exists y(yF^{-1}x)\}\\ &= \{x \mid \exists y(xFy)\}\\ &= \operatorname{dom} F\end{aligned}$$

$$\begin{aligned}(F^{-1})^{-1} &= \{\langle x, y\rangle \mid yF^{-1}x\}\\ &= \{\langle x, y\rangle \mid xFy\}\\ &= F\end{aligned}$$

Theorem 3F. *For a set F, F^{-1} is a function iff F is single-rooted. A relation F is a function iff F^{-1} is single-rooted.*

Proof (Mine):

Assume that F is single-rooted first, i.e. $\forall x_1 \forall x_2[(x_1Fy \wedge x_2Fy) \implies x_1 = x_2]$.
This is identical to $\forall x_1 \forall x_2[(yF^{-1}x_1 \wedge yF^{-1}x_2) \implies x_1 = x_2]$. Therefore, F^{-1} is single-valued and hence a function.
Conversely, now let F^{-1} be a function, i.e. $\forall x_1 \forall x_2[(yF^{-1}x_1 \wedge yF^{-1}x_2) \implies x_1 = x_2]$.
Again, this is the same as $\forall x_1 \forall x_2[(x_1Fy \wedge x_2Fy) \implies x_1 = x_2]$. Which means F is indeed single-rooted.
Thus, it has been proven that, for a set F, F^{-1} is a function iff F is single-rooted.

Utilising Theorem 3E and the previous result, the relation $(F^{-1})^{-1} \overset{3E}{=} F$ is a function iff F^{-1} is single-rooted.
Wherefore, a relation F is a function iff F^{-1} is single-rooted.

Theorem 3G. *Assume that F is an injective function. If $x \in \operatorname{dom} F$, then $F^{-1}(F(x)) = x$. If $y \in \operatorname{ran} F$, then $F(F^{-1}(y)) = y$.*

Proof (Mine):

$$\begin{aligned} x \in \operatorname{dom} F \implies F^{-1}(F(x)) &= F^{-1}[\![\{y \mid xFy\}]\!] && \text{where } |\{y \mid xFy\}| = 1 \text{ since } F \text{ is a function} \\ &= \{x \mid yF^{-1}x \wedge xFy\} \\ &= x && \text{since } F^{-1} \text{ is a function by Theorem 3F} \end{aligned}$$

Thus, it is proven that if $x \in \operatorname{dom} F$, then $F^{-1}(F(x)) = x$.

$$\begin{aligned} y \in \operatorname{ran} F \implies F(F^{-1}(y)) &= F[\![\{x \mid yF^{-1}x\}]\!] && \text{where } |\{x \mid yF^{-1}x\}| = 1 \text{ since } F^{-1} \text{ is a function} \\ &= \{y \mid xFy \wedge yF^{-1}x\} \\ &= y && \text{since } F \text{ is a function} \end{aligned}$$

So, If $y \in \operatorname{ran} F$, then $F(F^{-1}(y)) = y$.

Proof (Enderton's):

Suppose that $x \in \operatorname{dom} F$; then $\langle x, F(x)\rangle \in F$ and $\langle F(x), x\rangle \in F^{-1}$.
Thus $F(x) \in \operatorname{dom} F^{-1}$. F^{-1} is a function by Theorem 3F, so $x = F^{-1}(F(x))$.
If $y \in \operatorname{ran} F$, then by applying the first part of the theorem to F^{-1} we obtain the equation $(F^{-1})^{-1}(F^{-1}(y)) = y$. But $(F^{-1})^{-1} = F$.

Theorem 3H. *Assume that F and G are functions. Then $F \circ G$ is a function, its domain is*

$$\{x \in \operatorname{dom} G \mid G(x) \in \operatorname{dom} F\}$$

and for x in its domain, $(F \circ G)(x) = F(G(x))$.

Proof (Mine):

$$\operatorname{dom}(F \circ G) = \operatorname{dom}\{\langle x, y\rangle \mid \exists t(xGt \wedge tFy)\} = \{x \mid \exists t \exists y(xGt \wedge tFy)\} = \{x \in \operatorname{dom} G \mid G(x) \in \operatorname{dom} F\}$$
$$(F \circ G)(x) = \{y \mid x(F \circ G)y\} = \{y \mid \exists t(xGt \wedge tFy)\} = F[\![\{t \mid xGt\}]\!] = F(G(x))$$

Theorem 3I. *For any sets F and G,*

$$(F \circ G)^{-1} = G^{-1} \circ F^{-1}$$

Theorem 3J. *Assume that $F\colon A \to B$, and that A is nonempty.*

(a) There exists a function $G\colon B \to A$ (a "left inverse") such that $G \circ F$ is the identity function I_A on A iff F is injective.
(b) There exists a function $H\colon B \to A$ (a "right inverse") such that $F \circ H$ is the identity function I_B on B iff F is surjective.

Theorem 3K. *The following will hold for any sets (relations)*

(a) The image of a union is the union of the images:

$$F[\![A \cup B]\!] = F[\![A]\!] \cup F[\![B]\!] \text{ and } F\left[\!\!\left[\bigcup \mathcal{A}\right]\!\!\right] = \bigcup\{F[\![A]\!] | A \in \mathcal{A}\}$$

(b) The image of an intersection is included in the intersection of the images:

$$F[\![A \cap B]\!] \subseteq F[\![A]\!] \cap F[\![B]\!] \text{ and } F\left[\!\!\left[\bigcap \mathcal{A}\right]\!\!\right] \subseteq \bigcap\{F[\![A]\!] | A \in \mathcal{A}\}$$

(c) The image of a difference / complement includes the difference / complement of the images:

$$F[\![A]\!] \backslash F[\![B]\!] \subseteq F[\![A \backslash B]\!]$$

Equality holds if F is single-rooted.

Corollary 3L. *For any function G and sets $A, B, \mathcal{A}$:*

$$G^{-1}\left[\!\left[\bigcup \mathcal{A}\right]\!\right] = \bigcup\{G^{-1}[\![A]\!] | A \in \mathcal{A}\},$$
$$G^{-1}\left[\!\left[\bigcap \mathcal{A}\right]\!\right] = \bigcap\{G^{-1}[\![A]\!] | A \in \mathcal{A}\} \quad \textit{for } A \neq \varnothing$$
$$G^{-1}[\![A \backslash B]\!] = G^{-1}[\![A]\!] \backslash G^{-1}[\![B]\!].$$

Definition. ${}^{A}B$
${}^{A}B$ is read "B-pre-A", it is the collection of functions F from A into B.
${}^{A}B = \{F | F \text{ is a funtion } \wedge F : A \implies B\}$. (Otherwise notated as B^A)

Since $F : A \to B$, $F \subseteq A \times B$, so $F \in \mathscr{P}(A \times B)$. Consequently, we can apply a subset axiom to $\mathscr{P}(A \times B)$ to construct the set of all functions from A into B.

Definition. Infinite Cartesian Products
Let I be an index set such that $i \in I$

$$\prod_{i \in I} X(i) := \left\{ f \colon I \to \bigcup_{i \in I} X(i) \,\middle|\, (\forall i \in I)[f(i) \in X(i)] \right\}$$

If there exists some i such that $X(i) = \varnothing$, then clearly $\prod\limits_{i \in I} X(i)$ is empty. Conversely, suppose that for all i, $X(i) \neq \varnothing$, then we use the Axiom of Choice to show that $\prod\limits_{i \in I} X(i)$ is nonempty.

Definition. R is an *equivalence relation* on A iff R is a binary relation on A that is reflexive on A, symmetric and transitive:

1. R is *reflexive* on A, i.e. xRx for all $x \in A$
2. R is *symmetric*, i.e. for all x, y; if xRy then yRx.
3. R is *transitive*, i.e. for all x, y, z; if xRy and yRz, then also xRz.

Theorem 3M. *If R is a symmetric and transitive relation, then R is an equivalence relation on* $\operatorname{fld} R$.

This theorem deserves a ***precautionary note****: If R is a symmetric and transitive relation on A, it does* not *follow that R is an equivalence relation on A. R is reflexive on* $\operatorname{fld} R$*, but* $\operatorname{fld} R$ *amy be a small subset of A.*

Definition. The set $[x]_R$ is defined by

$$[x]_R = \{t \,|\, xRt\}.$$

If R is an equivalence relation and $x \in \operatorname{fld} R$, then $[x]_R$ is called the *equivalence class* of x *modulo* R. If the relation R is fixed by the context, we may write just $[x]$.

The existence of the set $[x]_R$ is guaranteed by a subset axiom, since $[x]_R \subseteq \operatorname{ran} R$. Furthermore, we can construct a set of equivalence classes, such as $\{[x]_R \,|\, x \in A\}$, since this set is in $\mathscr{P}(\operatorname{ran} R)$

Lemma 3N. *Assume that R is an equivalence relation on A and that $x, y \in R$. Then*

$$[x]_R = [y]_R \quad \textit{iff} \quad xRy$$

Definition. A *partition* Π of a set A is a set of nonempty subsets of A that are disjoint and exhaustive, i.e.,

(a) No two different sets in Π have any common elements.
In other words, $(\forall x \in \Pi)(\forall y \in \Pi)(x \neq y \implies x \cap y = \varnothing)$.
Or more formally, $\forall x \forall y[x \in \Pi \wedge y \in \Pi \implies (x \neq y \implies x \cap y = \varnothing)]$.

(b) Each element of A is in some set of Π.
That is, $\forall x[x \in A \iff (\exists b \in \Pi)x \in b]$.
Or more formally, $\forall x[x \in A \iff \exists b(b \in \Pi \wedge x \in b)]$.

Theorem 3P. *Assume that R is an equivalence relation on A. Then the set $\{[x]_R \mid x \in A\}$ of all equivalence classes is a partition of A.*

Proof:

Each equivalence class $[x]_R$ is nonempty (because $x \in [x]_R$) and is a subset of A (because R is a binary relation on A). The main thing we must prove is that the collection of equivalence classes is disjoint, i.e., part (a) of the above definition is satisfied. So suppose that $[x]_R$ and $[y]_R$ have a common element t. Thus

$$xRt \quad \text{and} \quad yRt.$$

But then xRy and by Lemma 3N, $[x]_R = [y]_R$. (End of proof)

If R is an equivalence relation on A, then we can define the quotient set

$$A/R = \{[x]_R \mid x \in A\}$$

whose members are the equivalence classes. (The expression A/R is read "A modulo R.") We also have the natural map *(or* canonical map*) $\varphi\colon A \to A/R$ defined by*

$$\varphi(x) = [x]_R$$

for $x \in A$.

Definition. If R is an equivalence relation on A, then we can define the *quotient set*

$$A/R = \{[x]_R \mid x \in A\}$$

Definition. If R is an equivalence relation on A, then we can define the *natural map* (or *canonical map*)

$$\varphi\colon A \to A/R \qquad \varphi(x) = [x]_R$$

Definition. A function F is *compatible* with the relation R on A iff for all x and y in A

$$xRy \implies F(x)RF(y)$$

Theorem 3Q. *Assume that R is an equivalence relation on A and that $F\colon A \to A$. If F is compatible with R, then there exists a unique $\hat{F}\colon A/R \to A/R$ such that*

$$(\bigstar) \qquad \hat{F}([x]_R) = [F(x)]_R \quad \textit{for all } x \textit{ in } A.$$

If F is not compatible with R, then no such $\hat{F}$ exists. Analogous results apply to functions from $A \times A$ into A.

STheorem I. *The Universal Property of The Quotient Set: If X is a set and $\sim$ an equivalence relation on X, then the natural/canonical projection $\varphi\colon X \to X/\sim$ such that $\varphi(x) = [x]_\sim$ can be formed. For any other set Y and function $f\colon X \to Y$ that respects $\sim$, i.e (for all x and x') $x \sim x' \implies f(x) = f(x')$; there exists a unique function $\hat{F}\colon X/\sim \to Y$ such that $f = \hat{F} \circ \varphi$:*

$$\begin{array}{ccc} X & \xrightarrow{\quad f \quad} & Y \\ {\scriptstyle\varphi}\big\downarrow & \nearrow_{\hat{F}} & \\ X/\sim & & \end{array}$$

On the contrary, if f does not respect $\sim$, then there does not exist such a function $\hat{F}\colon X/\sim \to Y$ such that $f = \hat{F} \circ \varphi$.

Proof.

Definition. Let A be any set. A *linear ordering* on A (also called a *total ordering* on A) is a binary relation R on A (i.e., $R \subseteq A \times A$) meeting the following two conditions:

(a) R is a transitive relation; i.e., whenever xRy and yRz, then xRz.

(b) R satisfies trichotomy on A, by which we mean that for any x and y in A exactly one of the three alternatives

$$xRy, \quad x = y, \quad yRx$$

holds.

Me: Note: In this case I think this definition is specifically a ***strict*** *total order.*

Theorem 3R. *Let R be a linear ordering on A.*

*(i) There ix no x for which xRx (*Irreflexive*)*

*(ii) For distinct x and y in A, either xRy or yRx (but never both) (*Connected*).*

In fact, for a transitive relation on A, conditions (i) and (ii) are equivalent to trichotomy. A relation meeting condition (i) is called irreflexive*; one meeting condition (ii) is said to be* connected *on A.*
Instead of R, we favor the symbol $<$ for a linear ordering

(Even for a general relation, possibly without transitivity, I think (i)+(ii) should be equivalent to trichotomy)

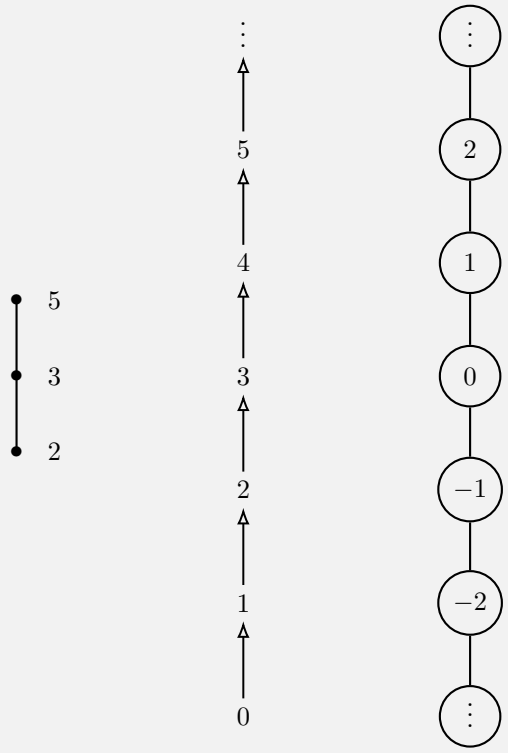
Fact. A linear ordering R can never lead us in circles, e.g., there cannot exist a circle such as

$$x_1Rx_2, \quad x_2Rx_3, \quad x_2Rx_4, \quad x_4Rx_5, \quad x_5Rx_1.$$

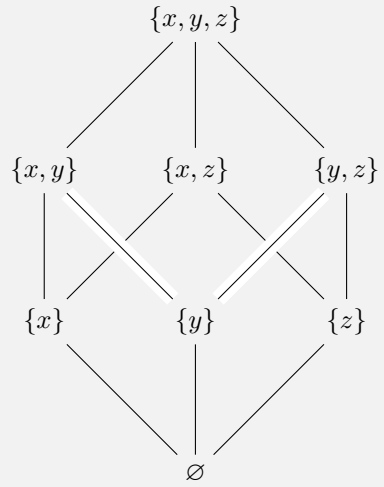
This is because if we had such a circle, then by transitivity x_1Rx_1, contradicting part (i) of the foregoing theorem.

Definition. Hasse Diagrams, illustration of a linear ordering:
We represent the members of A by dots, placing the dot for x below the dot for y whenever $x < y$. Then we add vertical lines to connect the dots. The resulting picture has the points of A stretched out along a line, in the correct order.

(The adjective "linear" reflects the possibility of drawing this picture.)



Hasse diagram of the set of all subsets of a three-element set, $\{x, y, z\}$, ordered by inclusion, (Partial-Order):



There are many ways to draw a Hasse diagram.

(E.g.: With arrow, without arrow, with circle as the node, just using the elements for the nodes, etc)

0.4 Chapter 4 — Natural Numbers

Definition. Von Neumann construction: We define the symbols $0, 1, 2, 3$ as

$$\begin{aligned} 0 &= \varnothing, \\ 1 &= \{0\} = \{\varnothing\}, \\ 2 &= \{0, 1\} = \{\varnothing, \{\varnothing\}\}, \\ 3 &= \{0, 1, 2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}. \end{aligned}$$

Definition. For any set a, its *successor* a^+ is defined by

$$a^+ = a \cup \{a\}.$$

In terms of the successor operation, the first few natural numbers can be characterized as

$$0 = \varnothing, \quad 1 = \varnothing^+, \quad 2 = \varnothing^{++}, \quad 3 = \varnothing^{+++}, \ldots$$

Which are all distinct sets.

Definition. A set A is said to be *inductive* iff $\varnothing \in A$ and it is "closed under successor," i.e.,

$$\forall a (a \in A \implies a^+ \in A).$$

Definition. A *natural number* is a set that belongs to every inductive set.

Theorem 4A. *There is a set whose members are exactly the natural numbers. (The set of all natural numbers is denoted by a lowercase Greek omega, ω.)*

In terms of classes, we have

$$\omega = \bigcap \{A \mid A \text{ is inductive}\}$$

but the class of all inductive sets is not a set.

Theorem 4B. *ω is inductive, and a subset of every other inductive set.*

Fact. Since ω is inductive, we know that $0 (= \varnothing)$ is in ω. It then follows that $1 (= 0^+)$ is in ω, as are $2 (= 1^+)$ and $3 (= 2^+)$. Thus $0, 1, 2$, and 3 are natural numbers.

Unnecessary extraneous objects have been excluded from ω, since ω is the smallest inductive set. This fact can also be restated as follows:

Induction Principle for ω: Any inductive subset of ω coincides with ω.

Theorem 4C. *Every natural number except 0 is the successor of some natural number.*

Self-Proof.

Definition. A *Peano system* is defined to be a triple $\langle N, S, e \rangle$ consisting of a set N, a function $S \colon N \to N$, and a member $e \in N$ such that the following three conditions are met:

(i) $e \notin \operatorname{ran} S$.

(ii) S is injective.

(iii) Any subset A of N that contains e and is closed under S equals N itself.

Theorem 4D. *$\langle \omega, \sigma, 0 \rangle$ is a Peano System.*
Where σ is the restriction of the successor operation to ω, i.e. $\sigma = \{\langle n, n^+ \rangle \mid n \in \omega\}$.

Self-Proof.

Definition. A set A is said to be a *transitive set* iff every member of a member of A is itself a member of A. We can state this equivalently in 4 ways: For all x;

$$x \in a \in A \implies x \in A, \tag{1}$$

$$\bigcup A \subseteq A, \tag{2}$$

$$a \in A \implies a \subseteq A, \tag{3}$$

$$A \subseteq \mathscr{P}A. \tag{4}$$

In the previous chapter we defined a transitive *relation* while we defined a transitive *set* here. These are not the same things. The context will make clear which sense of "transitive" is wanted.

Theorem 4E. *For a transitive set A,*

$$\bigcup (a^+) = a.$$

Theorem 4F. *Every natural number is a transitive set.*

Self-Proof.

Theorem 4G. *The set ω is a transitive set.*

Self-Proof.

Recursion Theorem on ω: *Let A be a set $a \in A$, and $F\colon A \to A$. Then there exists a unique function $h\colon \omega \to A$ such that*

$$h(0) = a,$$

and for every $n \in \omega$,

$$h(n^+) = F(h(n)).$$

The recursion theorem is in general false for systems not meeting the 3 conditions of Peano systems. So any correct proof of recursion absolutely must make use of conditions (i)-(iii).

Theorem 4H. *Let $\langle N, S, e\rangle$ be a Peano system. Then $\langle \omega, \sigma, 0\rangle$ is isomorphic to $\langle N, S, e\rangle$, i.e., there is a bijective function $h\colon \omega \to N$ in a way that preserves the successor operation*

$$h(\sigma(n)) = S(h(n))$$

and the zero element

$$h(0) = e.$$

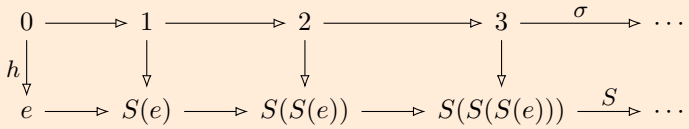


Fig. 18. Isomorphism of Peano Systems.

Self-Proof.

Theorem 4H shows that the number system we have constructed is, "to within isomorphism," the only system satisfying Peano's postulates.

Definition. A *binary operation* on a set A is a function from $A \times A$ into A.

Definition. *Addition* $(+)$ is the binary operation on ω such that for any m and n in ω,

$$m + n = A_m(n).$$

When written (explicitly) as a relation,

$$+ = \{\langle\langle m, n\rangle, p\rangle \mid m \in \omega \wedge n \in \omega \wedge p = A_m(n)\}.$$

Theorem 4I.

(A1) $$m + 0 = m,$$

(A2) $$m + n^+ = (m + n)^+.$$

Self-Proof.

Theorem 4J. *For natural numbers m and n,*

(M1) $$m \cdot 0 = 0,$$

(M2) $$m \cdot n^+ = m \cdot n + m.$$

Self-Proof.

Theorem 4K. *The following identities hold for all natural numbers.*

(1) Associative law for addition

$$m + (n + p) = (m + n) + p.$$

(2) Commutative law for addition

$$m + n = n + m.$$

(3) Distributive law

$$m \cdot (n + p) = m \cdot n + m \cdot p.$$

(4) Associative law for multiplication

$$m \cdot (n \cdot p) = (m \cdot n) \cdot p.$$

(5) Commutative law for multiplication

$$m \cdot n = n \cdot m.$$

Self-Proof.

Definition. For natural numbers m and n, we define m to be *less than* n iff $m \in n$.

Definition. We define

$$m \subseteq n \quad \text{iff} \quad (m \in n \vee m = n).$$

Lemma 4L. *(a) For any natural numbers m and n,*

$$m \in n \quad \textit{iff} \quad m^+ \in n^+.$$

(b) No natural number is a member of itself.

Self-Proof.

Trichotomy Law for ω *For any natural numbers m and n, exactly one of the three conditions*

$$m \in n, \quad m = n, \quad n \in m$$

holds.

Corollary 4M. *For any natural numbers m and n,*

$$m \in n \quad \textit{iff} \quad m \subset n$$

and

$$m \subseteq n \quad \textit{iff} \quad m \subseteq n.$$

Theorem 4N. *For any natural numbers m, n, and p,*

$$m \in n \iff m + p \in n + p.$$

If, in addition, $p \neq 0$, then

$$m \in n \iff m \cdot p \in n \cdot p.$$

Corollary 4P. *The following cancellation laws hold for m, n, and p in ω:*

$$m + p = n + p \implies m = n,$$
$$m \cdot p = n \cdot p \quad \textit{and} \quad p \neq 0 \implies m = n.$$

Self-Proof.

Well Ordering of ω *Let A be a nonempty subset of ω. Then there is some $m \in A$ such that $m \subseteq n$ for all $n \in A$.*

Note: *Such an m is said to be* least *in A. The theorem asserts that every nonempty subset of ω has a least element. The least element is always unique.*

Corollary 4Q. *There is no function $f : \omega \to \omega$ such that $f(n^+) \in f(n)$ for every natural number n.*

Self-Proof.

Strong Induction Principle for ω *Let A be a subset of ω, and assume that for every $n \in \omega$,*

if every number less than n is in A, then $n \in A$.

Then $A = \omega$.

Interesting Note: There seems, at first glance, that we are missing a critical assertion that $0 \in A$. However, in this particular form of the Strong Induction Principle for ω, it is actually completely unnecessary, because: Every number less than 0 is in A vacuously. Which means, by our Strong Induction Hypothesis, $0 \in A$! However, if we were to tweak our Strong Induction Hypothesis to the form below, then we certainly need the presumption that $0 \in A$:

if every number less than or equal to n is in A, then $n^+ \in A$.

In this form, we cannot deduce $0 \in A$ because $n^+ \neq 0$ for all natural n by Theorem 4D.

Self-Proof.

0.5 Chapter 5 — Construction of The Real Numbers

0.5.1 Integers

Definition. Define $\sim$ to be the relation on $\omega \times \omega$ for which

$$\langle m, n\rangle \sim \langle p, q\rangle \quad \text{iff} \quad m + q = p + n.$$

In more explicit (but less readable form), the above definition can be stated:

$$\sim = \{\langle\langle m, n\rangle, \langle p, q\rangle\rangle \mid m + q = p + n \text{ and all are in } \omega\}.$$

Theorem 5ZA. *The relation $\sim$ is an equivalence relation on $\omega \times \omega$.*

Self-Proof.

Definition. The set $\mathbb{Z}$ of *integers* is the set $(\omega \times \omega)/\sim$ of all equivalence classes of differences*.

*Where we call a pair of natural numbers $\langle m, n\rangle$ a *difference*; and an integer an equivalence class of differences

Lemma 5ZB. *If $\langle m, n\rangle \sim \langle m', n'\rangle$ and $\langle p, q\rangle \sim \langle p', q'\rangle$, then*

$$\langle m + p, n + q\rangle \sim \langle m' + p', n' + q'\rangle.$$

Self-Proof.

Definition. Define the addition operation, $+_{\mathbb{Z}}$ to be the binary operation on $\mathbb{Z}$ so that for all integers a and b,

$$a +_{\mathbb{Z}} b = [\langle m, p.n + q\rangle]$$

where $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$. Lemma 5ZB tells us that $+_{\mathbb{Z}}$ is a well-defined function.

Theorem 5ZC. *The operation $+_{\mathbb{Z}}$ is commutative and associative:*

$$a +_{\mathbb{Z}} b = b +_{\mathbb{Z}} a$$
$$(a +_{\mathbb{Z}} b) +_{\mathbb{Z}} c = a +_{\mathbb{Z}} (b +_{\mathbb{Z}} c)\,.$$

Theorem 5ZD. *(a) $0_{\mathbb{Z}}$ is an identity element for $+_{\mathbb{Z}}$:*

$$a +_{\mathbb{Z}} 0_{\mathbb{Z}} = a$$

for any a in $\mathbb{Z}$.

(b) Additive inverses exist: For any integer a, there is an integer b such that

$$a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}.$$

The inverse of a is denoted as $-a$. Then as the proof to Theorem 5ZD shows, $-[\langle m, n\rangle] = [\langle n, n\rangle]$.

Fact. Theorems 5ZC and 5ZD together say that $\mathbb{Z}$ wit the operation $+_{\mathbb{Z}}$ and the identity element $0_{\mathbb{Z}}$ is an *Abelian* group.

Inverses are unique. That is, if $a +_{\mathbb{Z}} b = 0_{\mathbb{Z}}$ and $a +_{\mathbb{Z}} b' = 0_{\mathbb{Z}}$, then $b = b'$. To prove this, observe that

$$b = b +_{\mathbb{Z}} (a +_{\mathbb{Z}} b') = (b +_{\mathbb{Z}} a) +_{\mathbb{Z}} b' = b'.$$

(This proof works in any Abelian group.)

Definition. Inverses provide us with a subtraction operation, which we define by the equation

$$b - a = b +_{\mathbb{Z}} (-a).$$

Lemma 5ZE. *If* $\langle m, n\rangle \sim \langle m', n'\rangle$ *and* $\langle p, q\rangle \sim \langle p', q'\rangle$, *then*

$$\langle mp + nq, mq + np\rangle \sim \langle m'p' + n'q' + m'q' + n'p'\rangle.$$

Definition. Define the multiplication operation, $\cdot_{\mathbb{Z}}$ to be the binary operation on $\mathbb{Z}$ so that for all integers a and b,

$$a \cdot_{\mathbb{Z}} b = [\langle mp + nq, mq + np\rangle]$$

where $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$ (and here we write as usual, mp in place of $m \cdot p$). Lemma 5ZE tells us that $\cdot_{\mathbb{Z}}$ is a well-defined function.

Theorem 5ZF. *The multiplication operation* $\cdot_{\mathbb{Z}}$ *is commutative, associative, and distributive over* $+_{\mathbb{Z}}$*:*

$$a \cdot_{\mathbb{Z}} b = b \cdot_{\mathbb{Z}} a$$
$$(a \cdot_{\mathbb{Z}} b) \cdot_{\mathbb{Z}} c = a \cdot_{\mathbb{Z}} (b \cdot_{\mathbb{Z}} c)$$
$$a \cdot_{\mathbb{Z}} (b +_{\mathbb{Z}} c) = (a \cdot_{\mathbb{Z}} b) +_{\mathbb{Z}} (a \cdot_{\mathbb{Z}} c)$$

Self-Proof of Commutativity.

Theorem 5ZG. *(a) The integer* $1_{\mathbb{Z}}$ *is a multiplicative identity element:*

$$a \cdot_{\mathbb{Z}} 1_{\mathbb{Z}} = a$$

for any integer a.

(b) $0_{\mathbb{Z}} = 1_{\mathbb{Z}}$.

(c) Whenever $a \cdot_{\mathbb{Z}} b = 0_{\mathbb{Z}}$, *then either* $a = 0_{\mathbb{Z}}$ *or* $b = 0_{\mathbb{Z}}$.

Part (c) is sometimes stated: There are no "zero divisors" in $\mathbb{Z}$.

Self-Proof.

Fact. In algebraic terminology, we can say that $\mathbb{Z}$ together with $+_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$, $0_{\mathbb{Z}}$, and $1_{\mathbb{Z}}$ forms an *integral domain*. This means that:

(i) $\mathbb{Z}$ together with $+_{\mathbb{Z}}$ and $0_{\mathbb{Z}}$ forms an Abelian group (Theorems 5ZC and 5ZD.)

(ii) Multiplication is commutative and associative, and is distributive over addition (Theorem 5ZF)

(iii) $1_{\mathbb{Z}}$ is a multiplicative identity (different from $0_{\mathbb{Z}}$), and no zero divisors exist (Theorem 5ZG).

Lemma 5ZH. *If* $\langle m, n\rangle \sim \langle m', n'\rangle$ *and* $\langle p, q\rangle \sim \langle p', q'\rangle$, *then*

$$m + q \in p + n \quad \textit{iff} \quad m' + q' \in p' + n'.$$

Definition. Define the ordering relation $<_{\mathbb{Z}}$ on $\mathbb{Z}$ to be such that for all integers a and b,

$$a <_{\mathbb{Z}} b \quad \text{iff} \quad m + q \in p + n.$$

where m, n, p, and q are chosen so that $a = [\langle m, n\rangle]$ and $b = [\langle p, q\rangle]$.

Lemma 5ZH shows that this yields a well-defined relation $<_{\mathbb{Z}}$ on the integers.

Theorem 5ZI. *The relation $<_{\mathbb{Z}}$ is a linear ordering relation on the set of integers.*

Self-Proof.

Definition. An integer b is called *positive* iff $0_{\mathbb{Z}} <_{\mathbb{Z}} b$. It is easy to check that

$$b <_{\mathbb{Z}} 0_{\mathbb{Z}} \quad \text{iff} \quad 0_{\mathbb{Z}} <_{\mathbb{Z}} -b.$$

Thus, a consequence of trichotomy is the fact that for an integer b, exactly one of the three alternatives

$$b \text{ is positive}, \quad b \text{ is zero}, \quad -b \text{ is positive}$$

holds.

Theorem 5ZJ. *The following are valid for any integers a, b, and c:*

(a) $a <_{\mathbb{Z}} b \iff a +_{\mathbb{Z}} c <_{\mathbb{Z}} b +_{\mathbb{Z}} c$.

(b) If $0_{\mathbb{Z}} <_{\mathbb{Z}} c$, *then*

$$a <_{\mathbb{Z}} b \iff a \cdot_{\mathbb{Z}} c <_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c.$$

This shows that addition preserves order, as does multiplication by a positive integer.

Corollary 5ZK. *For any integers a, b, and c the cancellation laws hold:*

$$a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c \implies a = b,$$
$$a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} \ \& \ c \neq 0_{\mathbb{Z}} \implies a = b.$$

Self-Proof.

Fact. Although ω is not actually a subset of $\mathbb{Z}$, nonetheless $\mathbb{Z}$ has a subset that is "just like" ω. To make this precise, define the function $E\colon \omega \to \mathbb{Z}$ by

$$E(n) = [\langle n, 0\rangle].$$

(E.g.: $E(0) = 0_{\mathbb{Z}}$ and $E(1) = 1_{\mathbb{Z}}$.)
The following theorem, in algebraic terminology, says that E is an "isomorphic embedding" of the system $\langle \omega, +, \cdot, \in_\omega\rangle$ into the system $\langle \mathbb{Z}, +_{\mathbb{Z}}, \cdot_{\mathbb{Z}}, <_{\mathbb{Z}}\rangle$. That is, E is an injective function that preserves addition, multiplication, and order.

Theorem 5ZL. *E is injective, and satisfies the following properties for any natural numbers m and n:*

(a) $E(m+n) = E(m) +_{\mathbb{Z}} E(n)$.

(b) $E(mn) = E(m) \cdot_{\mathbb{Z}} E(n)$.

(c) $m \in n$ *iff* $E(m) <_{\mathbb{Z}} E(n)$.

Fact. We can now give a precise counterpart to our motivating guideline that the difference $\langle m, n\rangle$ should name $m - n$. For any m and n,

$$[\langle m, n\rangle] = E(m) - E(n).$$

Note. Henceforth, we will streamline our notation by omitting the subscript "$\mathbb{Z}$" on $+_{\mathbb{Z}}$, $\cdot_{\mathbb{Z}}$, $<_{\mathbb{Z}}$, $0_{\mathbb{Z}}$, $1_{\mathbb{Z}}$, etc. Furthermore, $a \cdot b$ will usually be written as just ab.

0.5.2 Rational Numbers

Definition. By a *fraction*, we mean an ordered pair of integers, the second component of which (call the *denominator*) is nonzero.

Definition. Define $\sim$ to be the binary relation on $\mathbb{Z} \times \mathbb{Z}'$ for which

$$\langle a, b\rangle \sim \langle c, d\rangle \quad \text{iff} \quad a \cdot d = c\dot{b}.$$

Definition. The set $\mathbb{Q}$ of *rational numbers* is the set $(\mathbb{Z}\times\mathbb{Z}')/\sim$ of all equivalence classes of fractions.

Theorem 5QA. *The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}'$.*

Self-Proof.

Lemma 5QB. *If $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$, then*

$$\langle ad + cb, bd\rangle \sim \langle a'd' + c'b', b'd'\rangle.$$

Note. We use the same symbol "$\sim$" that has been used for other equivalence relations, but as we only discuss one equivalence relation at a time, no confusion should result.

Definition. Define the binary operation $+_{\mathbb{Q}}$ on $\mathbb{Q}$ with

$$[\langle a, b\rangle] +_{\mathbb{Q}} [\langle c, d\rangle] = [\langle ad + cb, bd\rangle].$$

Note that $bd \neq 0$ since $b \neq 0$ and $d \neq 0$. Hence, $\langle ad + cb, bd\rangle$ is a fraction. Lemma 5QB tells us that the binary operation $+_{\mathbb{Q}}$ is well-defined.

Theorem 5QC. *(a) Addition $+_{\mathbb{Q}}$ is associative and commutative:*

$$(q +_{\mathbb{Q}} r) +_{\mathbb{Q}} s = q +_{\mathbb{Q}} (r +_{\mathbb{Q}} s),$$
$$r +_{\mathbb{Q}} s = s +_{\mathbb{Q}} r.$$

(b) $0_{\mathbb{Q}}$ is an identity element for $+_{\mathbb{Q}}$:

$$r +_{\mathbb{Q}} 0_{\mathbb{Q}} = r$$

for any r in $\mathbb{Q}$.

(c) Additive inverses exist: For any r in $\mathbb{Q}$ there is an s in $\mathbb{Q}$ such that $r +_{\mathbb{Q}} s = 0_{\mathbb{Q}}$.

Fact. The set $\mathbb{Q}$ with the binary operation $+_{\mathbb{Q}}$ on $\mathbb{Q}$ and the additive identity $0_{\mathbb{Q}} \in \mathbb{Q}$ together form the Abelian group $\langle \mathbb{Q}, +_{\mathbb{Q}}, 0_{\mathbb{Q}}\rangle$.

Fact. As in any Abelian group, the inverse of $r \in \mathbb{Q}$ here is unique; we denote it as $-r$. The proof of Theorem 5QC shows that $-[\langle a, b\rangle] = [\langle -a, b\rangle]$.

Lemma 5QD. *If $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c', d'\rangle$, then*

$$\langle ac, bd\rangle \sim \langle a'c', b'd'\rangle.$$

Definition. $\cdot_{\mathbb{Q}}$ is the binary operation on $\mathbb{Q}$ defined by

$$[\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle c, d\rangle] = [\langle ac, bd\rangle].$$

Lemma 5QD verifies that $\cdot_{\mathbb{Q}}$ is indeed well-defined.

Theorem 5QE. *Multiplication of rationals is associative, commutative, and distributive over addition:*

$$(p \cdot_{\mathbb{Q}} q) \cdot_{\mathbb{Q}} r = p \cdot_{\mathbb{Q}} (q \cdot_{\mathbb{Q}} r),$$
$$q \cdot_{\mathbb{Q}} r = r \cdot_{\mathbb{Q}} q,$$
$$p \cdot_{\mathbb{Q}} (q +_{\mathbb{Q}} r) = (p \cdot_{\mathbb{Q}} q) +_{\mathbb{Q}} (p \cdot_{\mathbb{Q}} r).$$

Fact. The new property that the rationals have (and that integers lack) is the existence of multiplicative inverses for nonzero (rational) numbers, as seen in Theorem 5QF.

Theorem 5QF. *For every nonzero r in $\mathbb{Q}$ there is a nonzero q in $\mathbb{Q}$ such that $r \cdot_{\mathbb{Q}} q = 1_{\mathbb{Q}}$.*

Theorem 5QG. *If r and s are nonzero rational numbers, then $r \cdot_{\mathbb{Q}} s$ is also nonzero.*

Self-Proof.

Enderton's (General) Proof.
Enderton's proof works for any field, since fields have multiplicative inverses for all their nonzero elements and $x \cdot 0 = 0$ in any commutative ring with identity.

Fact. The nonzero rationals with *multiplication* form an Abelian group, $\langle \mathbb{Q} - \{0_{\mathbb{Q}}\}, \cdot_{\mathbb{Q}}, 1_{\mathbb{Q}} \rangle$.

Fact. The proof of Theorem 5QF shows that

$$[\langle a, b \rangle]^{-1} = [\langle b, a \rangle].$$

Fact. (Multiplicative) Inverses provide us with a division operation. For a nonzero rational r we can define

$$s \div r = s \cdot_{\mathbb{Q}} r^{-1}.$$

Fact. The algebraic concept exemplified by the rational numbers is the concept of a *field*. To say that $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, 0_{\mathbb{Q}}, 1_{\mathbb{Q}} \rangle$ is a field means that it is an integral domain with the further property that multiplicative inverses exist. (Other examples of fields are provided by the real numbers and the complex numbers.) **Cool fact!** The method we have used to extend $\mathbb{Z}$ to $\mathbb{Q}$ can be applied to extend any integral domain to a field.

Fact. Since $[\langle a, b \rangle] = [\langle -a, -b \rangle]$, every rational number can be represented by some fraction with a positive denominator. (Recall that for nonzero integers b, either b or $-b$ is positive.)
(This fact is critical to define our linear ordering $<_{\mathbb{Q}}$.)

Lemma 5QH. *Assume that $\langle a, b \rangle \sim \langle a', b' \rangle$ and $\langle c, d \rangle \sim \langle c', d' \rangle$. Further assume that b, b', d, and d' are all positive. Then,*

$$ad < cb \quad \textit{iff} \quad a'd' = c'b'.$$

Self-Proof.

Definition. The linear ordering $<_{\mathbb{Q}}$ on $\mathbb{Q}$ is so that

$$[\langle a, b \rangle] <_{\mathbb{Q}} [\langle c, d \rangle] \quad \text{iff} \quad ad < cb$$

whenever b and d are positive. Again, the previous Lemma 5QH verifies that our linear ordering $<_{\mathbb{Q}}$ is well-defined.

Theorem 5QI. *The relation $<_{\mathbb{Q}}$ is a linear ordering on $\mathbb{Q}$.*

Self-Proof.

Definition. Call a rational number q *positive* iff $0_{\mathbb{Q}} <_{\mathbb{Q}} q$. Thus, $r <_{\mathbb{Q}} 0_{\mathbb{Q}}$ iff $0_{\mathbb{Q}} <_{\mathbb{Q}} -r$. Then as a consequence of trichotomy, for any rational number r, exactly one of three alternatives

$$r \text{ is positive}, \quad r \text{ is zero}, \quad -r \text{ is positive}$$

holds.

Definition. We define the *absolute value* $|r|$ of r by

$$|r| = \begin{cases} -r & \text{if } -r \text{ is positive,} \\ r & \text{otherwise.} \end{cases}$$

Then, $0_{\mathbb{Q}} \leq_{\mathbb{Q}} |r|$ for every r.

Theorem 5QJ. *Let r, s, and t be rational numbers.*

(a) $r <_{\mathbb{Q}} s$ *iff* $r +_{\mathbb{Q}} t <_{\mathbb{Q}} s +_{\mathbb{Q}} t$.

(b) If t is positive, then

$$r <_{\mathbb{Q}} s \quad \textit{iff} \quad r \cdot_{\mathbb{Q}} t <_{\mathbb{Q}} s \cdot_{\mathbb{Q}} t.$$

Fact. The two preceding theorems (5QI and 5QJ) state that $\langle \mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, 0_{\mathbb{Q}}, 1_{\mathbb{Q}}, <_{\mathbb{Q}} \rangle$ is an *ordered field.*

Theorem 5QK. *The following cancellation laws hold for any rational numbers.*

(a) If $r +_{\mathbb{Q}} t = s +_{\mathbb{Q}} t$, then $r = s$.

(b) If $r \cdot_{\mathbb{Q}} t = s \cdot_{\mathbb{Q}} t$ and t is nonzero, then $r = s$.

Enderton's (General) Proof.
(works in any Abelian group)

Fact. Although $\mathbb{Z}$ is not a subset of $\mathbb{Q}$, there exists an embedding function $E\colon \mathbb{Z} \to \mathbb{Q}$ with

$$E(a) = [\langle a, 1 \rangle].$$

Which gives us an isomorphic embedding in the sense that the following theorem holds:

Theorem 5QL. *E is an injective function from $\mathbb{Z}$ into $\mathbb{Q}$ satisfying the following conditions:*

(a) $E(a + b) = E(a) +_{\mathbb{Q}} E(b)$.

(b) $E(ab) = E(a) \cdot_{\mathbb{Q}} E(b)$.

(c) $E(0) = 0_{\mathbb{Q}}$ *and* $E(1) = 1_{\mathbb{Q}}$.

(d) $a < b$ *iff* $E(a) <_{\mathbb{Q}} E(b)$.

Fact. We also obtain the following relation between fractions and division:

$$[\langle a, b \rangle] = E(a) \div E(b).$$

Since $b \neq 0$, we have $E(b) \neq 0_{\mathbb{Q}}$, and so the indicated division is possible.

Note. Henceforth, we will simplify the notation by omitting the subscript "$\mathbb{Q}$" on $+_{\mathbb{Q}}$, $\cdot_{\mathbb{Q}}$, $0_{\mathbb{Q}}$, and so forth. Also, the product $r \cdot s$ will usually be written as just rs.

0.5.3 Real Numbers

Note. There are many methods to choose from for a successful construction of the real numbers, each with their own advantages.

Definition. Define a *Cauchy sequence* to be a function $s\colon \omega \to \mathbb{Q}$ such that $|s_m, s_n|$ is arbitrarily small for sufficiently large n; i.e.,

$$(\forall \text{ positive } \varepsilon \text{ in } \mathbb{Q})(\exists k \in \omega)(\forall m > k)(\forall n > k)|s_m - s_n| < \varepsilon.$$

Definition. Let C be the se of all Cauchy sequences. For r and s in C, we define r and s to be *equivalent* ($r \sim s$) iff $|r_n - s_n|$ is arbitrarily small for all sufficiently large n; i.e.,

$$(\forall \text{ positive } \varepsilon \text{ in } \mathbb{Q})(\exists k \in \omega)(\forall n > k)|r_n - s_n| < \varepsilon.$$

Fact. The quotient set $C/\sim$ is a suitable candidate for $\mathbb{R}$. [a]

[a] This approach of constructing $\mathbb{R}$ is due to Cantor.

Fact. The Cauchy sequence construction of $\mathbb{R}$ has the advantage of generality, since it can be used with an arbitrary metric space in place of $\mathbb{Q}$.

Definition. A *Dedekind cut* is a subset x of $\mathbb{Q}$ such that:

1. $\varnothing \neq x \neq \mathbb{Q}$
2. x is closed "downwards", i.e.,
$$q \in x \;\&\; r < q \implies r \in x.$$
3. x has no largest member.

Definition. We define the real numbers to be the set of all Dedekind cuts.

Fact. The Dedekind cut construction of $\mathbb{R}$ has the advantage of simplicity, in that it provides a simple definition of $\mathbb{R}$ and its ordering. But multiplication of Dedekind cuts is awkward and verification of the properties of multiplication is a tedious business.

Definition. The ordering on $\mathbb{R}$ is particularly simple. For x and y in $\mathbb{R}$, define

$$x <_{\mathbb{R}} y \quad \text{iff} \quad x \subset y.$$

In other words, $<_{\mathbb{R}}$ is the relation of being a proper subset: $<_{\mathbb{R}} = \{\langle x, y\rangle \in \mathbb{R} \times \mathbb{R} \mid x \subset y\}$.

Theorem 5RA. *The relation $<_{\mathbb{R}}$ is a linear ordering on $\mathbb{R}$.*

Self-Proof.

Definition. A real number* x is said to be an *upper bound* of a subset A of $\mathbb{R}$ iff $y \leq_{\mathbb{R}} x$ for every y in A.

*The upper bound x need not belong in A.

Definition. The set A is *bounded* (i.e. *bounded above*) iff there exists some upper bound of A.

Definition. A *least upper bound* of A is a upper bound that is less than any other upper bound.

Theorem 5RB. *Any bounded nonempty subset of $\mathbb{R}$ has a least upper bound in $\mathbb{R}$.*

Self-Proof.

Definition. For reals x and y, define:

$$x +_{\mathbb{R}} y = \{q + r \mid q \in x \ \& \ r \in y\}.$$

Lemma 5RC. *For real numbers x and y, the sum $x +_{\mathbb{R}} y$ is also in $\mathbb{R}$.*

Self-Proof.

Theorem 5RD. *Addition of real numbers is associative and commutative:*

$$(x_{\mathbb{R}} y) +_{\mathbb{R}} z = x +_{\mathbb{R}} (y +_{\mathbb{R}} z),$$
$$x + \mathbb{R} + y = y +_{\mathbb{R}} x.$$

Definition. The zero element of $\mathbb{R}$ is defined to be the set of negative rational numbers:

$$0_{\mathbb{R}} = \{r \in \mathbb{Q} \mid r < 0\}.$$

Theorem 5RE. *(a) $0_{\mathbb{R}}$ is a real number.*

(b) For any x in $\mathbb{R}$, we have $x +_{\mathbb{R}} 0_{\mathbb{R}} = x$.

Self-Proof.

Definition. Define the inverse of x to be

$$-x = \{r \in \mathbb{Q} \mid (\exists s > r) - s \notin x\}.$$

Theorem 5RF. *For every x in $\mathbb{R}$:*

(a) $-x \in \mathbb{R}$,

(b) $x +_{\mathbb{R}} (-x) = 0_{\mathbb{R}}$.

Self-Proof.

Fact. $\langle \mathbb{R}, +_{\mathbb{R}}, 0_{\mathbb{R}} \rangle$ is an Abelian group. As in any Abelian group, the cancellation laws hold.

Corollary 5RG. *For any real numbers,*

$$x +_{\mathbb{R}} z = y +_{\mathbb{R}} z \implies x = y.$$

Theorem 5RH. *For any real numbers,*

$$x <_{\mathbb{R}} y \iff x +_{\mathbb{R}} z <_{\mathbb{R}} y +_{\mathbb{R}} z.$$

Definition. We define the absolute value $|x|$ of a real number x to be

$$|x| = x \cup -x.$$

We want $|x|$ to be the larger of x and $-x$, as the larger one is always the nonnegative one. Since our ordering is inclusion, the larger of the two is just their union. Hence, explaining our definition of $|x|$ above.

Definition. (a) If x and y are nonnegative real numbers, then

$$x \cdot_{\mathbb{R}} y = 0_{\mathbb{R}} \cup \{rs \,|\, 0 \leq r \in x \;\&\; 0 \leq s \in y\}.$$

(b) If x and y are both negative real numbers, then

$$x \cdot_{\mathbb{R}} y = |x| \cdot_{\mathbb{R}} |y|.$$

(c) If one of the real numbers x and y is negative and one is nonnegative, then

$$x \cdot_{\mathbb{R}} y = -(|x| \cdot_{\mathbb{R}} |y|).$$

Theorem 5RI. *For any real numbers, the following holds:*

(a) $x \cdot_{\mathbb{R}} y$ *is a real number.*

(b) Multiplication is associative, commutative, and distributive over addition.

(c) $0_{\mathbb{R}} \neq 1_{\mathbb{R}}$ *and* $x \cdot_{\mathbb{R}} 1_{\mathbb{R}} = x$.

(d) For nonzero x *there is a nonzero real number* y *with* $x \cdot_{\mathbb{R}} y = 1_{\mathbb{R}}$.

(e) Multiplication by a positive number preserves order: If $0_{\mathbb{R}} <_{\mathbb{R}} z$, *then*

$$x <_{\mathbb{R}} y \iff x \cdot_{\mathbb{R}} z <_{\mathbb{R}} y \cdot_{\mathbb{R}} z.$$

Where we define $1_{\mathbb{R}} = \{r \in \mathbb{Q} \,|\, r < 1\}$.

Fact. The foregoing theorems show that, like the rationals, the reals (with $+_{\mathbb{R}}$, $\cdot_{\mathbb{R}}$, $0_{\mathbb{R}}$, $1_{\mathbb{R}}$, and $<_{\mathbb{R}}$) form an ordered field. But unlike the rationals, the reals have the least-upper-bound property.

Definition. An ordered field is said to be *complete* iff it has the least-upper-bound property.

Fact. It can be shown that any other complete ordered field is isomorphic to the ordered field of real numbers.

Definition. The correct embedding function E from $\mathbb{Q}$ into $\mathbb{R}$ assigns to each rational number r the corresponding real number

$$E(r) = \{q \in \mathbb{Q} \,|\, q < r\},$$

consisting of all smaller rationals.

Theorem 5RJ. *E is an injective function from $\mathbb{Q}$ into $\mathbb{R}$ satisfying the following conditions:*

(a) $E(r + s) = E(r) +_{\mathbb{R}} E(s)$.

(b) $E(rs) = E(r) \cdot_{\mathbb{R}} E(s)$.

(c) $E(0) = 0_{\mathbb{R}}$ *and* $E(1) = 1_{\mathbb{R}}$.

(d) $r < s$ *iff* $E(r) <_{\mathbb{R}} E(s)$.

0.5.4 Summaries

Definitions.

i⟩ *Integers* Let m, n, p, and q be natural numbers.

$$\begin{aligned}
[\langle m,n\rangle] \sim [\langle p,q\rangle] &\iff m+q=p+n,\\
[\langle m,n\rangle] +_{\mathbb{Z}} [\langle p,q\rangle] &= [\langle m+p,n+q\rangle],\\
-[\langle m,n\rangle] &= [\langle n,m\rangle],\\
[\langle m,n\rangle] \cdot_{\mathbb{Z}} [\langle p,q\rangle] &= [\langle mp+nq,mp+np\rangle],\\
[\langle m,n\rangle] <_{\mathbb{Z}} [\langle p,q\rangle] &\iff m+q\in p+n,\\
E(n) &= [\langle n,0\rangle].
\end{aligned}$$

ii⟩ *Rational numbers* Let a, b, c, and d be integers with $bd\neq 0$.

$$\begin{aligned}
\langle a,b\rangle \sim \langle c,d\rangle &\iff ad=cb,\\
[\langle a,b\rangle] +_{\mathbb{Q}} [\langle c,d\rangle] &= [\langle ad+cb,bd\rangle],\\
-[\langle a,b\rangle] &= [\langle -a,b\rangle],\\
[\langle a,b\rangle] \cdot_{\mathbb{Q}} [\langle c,d\rangle] &= [\langle ac,bd\rangle],\\
[\langle a,b\rangle] <_{\mathbb{Q}} [\langle c,d\rangle] &\iff ad<cb, \qquad \text{when } b \text{ and } d \text{ are positive},\\
E(a) &= [\langle a,1\rangle].
\end{aligned}$$

iii⟩ *Real numbers* A real number is a set x such that $\varnothing \subset x \subset \mathbb{Q}$, x is closed downwards, and x has no largest member.

$$\begin{aligned}
x <_{\mathbb{R}} y &\iff x\subset y,\\
x +_{\mathbb{R}} y &= \{q+r \mid q\in x \ \&\ r\in y\},\\
-x &= \{r\in\mathbb{Q} \mid (\exists s>r) - s\notin x\},\\
|x| &= x\cup -x,\\
|x| \cdot_{\mathbb{R}} |y| &= 0_{\mathbb{R}}\cup\{rs \mid 0\leq r\in |x| \ \&\ 0\leq s\in |y|\},\\
E(r) &= \{q\in\mathbb{Q} \mid q<r\}.
\end{aligned}$$

iv⟩ An *Abelian group* (in additive notation) is a triple[a] $\langle A,+,0\rangle$ consisting of a set A, a binary operation $+$ on A, and an element ("zero") of A, such that the following conditions are met:

1. $+$ is associative and commutative.
2. 0 is an identity element, i.e., $x+0=x$.
3. Inverses exist, i.e., $\forall x\exists y(x+y=0)$.

An Abelian group (in multiplicative notation) is a triple $\langle A,\cdot,0\rangle$ consisting of a set A, a binary operation $\cdot$ on A, and an element 1 of A, such that the following conditions are met:

1. $\cdot$ is associative and commutative.
2. 1 is an identity element, i.e., $x\cdot 1=x$.
3. Inverses exist, i.e., $\forall x\exists y(x\cdot y=1)$.

This is, of course, the same as the preceding definition.

v⟩ A *group* has the same definition, except that we do not require that the binary operation be commutative.

Fact. All the groups that we have considered have, in fact, been Abelian groups. But some of our results (e.g. the uniqueness of inverses) are correct in any group, Abelian or not.

vi⟩ A *commutative ring with identity* is a quintuple $\langle D, +, \cdot, 0, 1\rangle$ consisting of a set D, binary operations $+$ and $\cdot$ on D, and distinguished elements 0 and 1 of D, such that the following conditions are met:

1. $\langle D, +, 0\rangle$ is an Abelian group.
2. The operation $\cdot$ is associative, commutative, and distributive over addition.
3. 1 is a multiplicative identity $x \cdot 1 = x$ and $0 \neq 1$.

vii⟩ An *integral domain* is a commutative ring with identity with the additional property that there are no zero divisors:

4. If $x \neq 0$ and $y \neq 0$, then also $x \cdot y \neq 0$.

viii⟩ A *field* is a commutative ring with identity in which multiplicative inverses exists:

4'. If x is a nonzero element of D, then $x \cdot y = 1$ for some y.

Fact. Any field is also an integral domain, because condition 4' implies condition 4 (see the proof to Corollary 5QG).

ix⟩ An *ordered field* is a sextuple $\langle D, +, \cdot, 0, 1, <\rangle$ such that the following conditions are met:

1. $\langle D, +, \cdot, 0, 1\rangle$ is a field.
2. $<$ is a linear ordering on D.
3. Order is preserved by addition and multiplication by positive element (i.e. $0 < z$):

$$x < y \iff x + z < y + z.$$

If $0 < z$, then

$$x < y \iff x \cdot z < y \cdot z.$$

x⟩ We can define *ordered integral domain* or even *ordered commutative ring with identity* by adjusting the first condition.

xi⟩ A *complete ordered field* is an ordered field in which for every bounded nonempty subset of D there is a least upper bound.

Note. The constructions in this chapter can be viewed as providing an existence proof for such fields. The conditions for a complete ordered field are not impossible to meet, for we have constructed a field meeting them.

[a] It is also possible to define a group to be a pair $A, +$, since the zero element turns out to be uniquely determined. We have formulated these definitions to match the exposition in this chapter.

0.6 Cardinal Numbers and the Axiom of Choice

Definition. A set A is *equinumerous* to a set B (written $A \approx B$) iff there is a bijective function from A into B. A bijection from A into B is called a *one-to-one correspondence* between A and B.

Fact. For any set A we have $\mathscr{P}A \approx {}^{A}2$ *Self-Proof.*

Theorem 6A. *For any sets A, B, and C:*

(a) $A \approx A$.

(b) If $A \approx B$, then $B \approx A$.

(c) If $A \approx B$ and $B \approx C$, then $A \approx C$.

Self-Proof.

Theorem 6B. *(a) The set ω is not equinumerous to the set $\mathbb{R}$ of real numbers.*

(b) No set is equinumerous to its power set.

Self-Proof.

Fact. $\mathbb{R}$ is equinumerous to $\mathscr{P}\omega$.

Definition. A set is *finite* iff it is equinumerous to some natural number. Otherwise, it is *infinite*.

Pigeonhole Principle *No natural number is equinumerous to a proper subset of itself.*

Corollary 6C. *No finite set is equinumerous to a proper subset of itself.* *Self-Proof.*

Corollary 6D. *(a) Any set equinumerous to a proper subset of itself is infinite.*

(b) The set ω is infinite.

Self-Proof.

Corollary 6E. *Any finite set is equinumerous to a* unique *natural number.* *Self-Proof.*

Definition. For any set A we will define (in Chapter 7) a set $\operatorname{card} A$ in such a way that:

(a) For any sets A and B,

$$\operatorname{card} A = \operatorname{card} B \quad \text{iff} \quad A \approx B.$$

(b) For a finite set A, $\operatorname{card} A$ is the natural number n for which $A \approx n$.

Lemma 6F. *If C is a proper subset of a natural number n, then $C \approx m$ for some m less than n.* *Self-Proof.*

Corollary 6G. *Any subset of a finite set is finite.* *Self-Proof.*

0.7 Random Interesting Stuff

0.7.1 Logic

Definition. Some Common Logical Notations

$$\begin{aligned}
(\forall x \in A)P(x) &\iff \forall x[x \in A \implies P(x)] \\
(\exists x \in A)P(x) &\iff \exists x[x \in A \wedge P(x)]
\end{aligned}$$

$$\begin{aligned}
(\exists y \in B)(\forall x \in A)C(x,y) &\iff \exists y \forall x\big(y \in B \wedge [x \in A \implies C(x,y)]\big) \\
&\iff \exists y[y \in B \wedge \forall x(x \in A \implies C(x,y))]
\end{aligned}$$

$$\begin{aligned}
(\forall x \in A)(\exists y \in B)C(x,y) &\iff \forall x \exists y\big(x \in A \implies [y \in B \wedge C(x,y)]\big) \\
&\iff \forall x\big(x \in A \implies [\exists y \wedge C(x,y)]\big)
\end{aligned}$$

"$\varphi \wedge \forall x\psi \dashv\vdash \forall x(\varphi \wedge \psi)$ whenever x is not free in phi (and similarly for exists and implies though one direction there requires classical logic)"

Extra Stuff for the Axiom Schema of Specifiation:

The reason why we use an axiom schema instead of $\forall\varphi$ is that in first order logic (which is where ZFC resides), quantification over predicates, like φ, is not allowed. Note that while $\forall\varphi$ and $\exists\varphi$ is not allowed in FOL, $\forall x(\varphi(x))$ and $\exists x(\varphi(x))$ is allowed.

Indeed, the k here represents a natural number and that we can only involve a finite number of symbols/variables (in our case sets) $t_1, \ldots, t_k$ in our predicate φ, a wff. By definition, a wff is finite sequence of symbols, which is why we can't 'involve' an infinite number of variables in φ. Now, to make each subset axiom a sentence, we must quantify over al the symbols involved, which is why we have $\forall t_1, \ldots, t_k \forall A \exists B \forall x$.

The reason that being a sentence is so important, is that, otherwise, the wff kind of has no meaning. To be more specific, in any mathematical structure, a sentence is automatically true or false (E.g.: $\exists y \forall x(x + y = x)$). On the contrary, something like $\exists y(x + y = x)$ has no meaning unless you say what y is: If you have free variables in your formula, you need a variable assignment function to give the formula a truth value. While for sentences you don't need to speak of variable assignment functions. For an axiomatic system, we want to know if any given structure satisfies those axioms or not. E.g.: In axiomatic set theory, we are defining/constructing sets by saying what properties they must have. If you are using sentences, then the sets will be well-defined and you can assert whether or not something is a set. However, with a wff that is not a sentence, you can't say if a structure satisfies that axiom/property without a variable assignment.

Enderton's A Introduction To Mathematical Logic:

Definition. An *expression* is a finite sequence of symbols.

Definition. A *well-formed formula* (or simply formula or *wff*) is an expression that can be built up from the sentence symbols by applying some finite number of times the formula-building operations(on expressions) defined by the equations

$$\begin{aligned}\mathcal{E}_{\neg}(\alpha) &= (\neg\alpha)\\ \mathcal{E}_{\wedge}(\alpha,\beta) &= (a \wedge b)\\ \mathcal{E}_{\vee}(\alpha,\beta) &= (a \vee b)\\ \mathcal{E}_{\rightarrow}(\alpha,\beta) &= (a \rightarrow b)\\ \mathcal{E}_{\leftrightarrow}(\alpha,\beta) &= (a \leftrightarrow b)\end{aligned}$$

Definition. If no variable occurs free in the wff α (i.e., if $h(\alpha) = \varnothing$), then α is a sentence.

Wise words by Enderton: In applications of subset axioms we generally will not write out the formula itself. And this example shows why; "a is a one-element subset of s" is much easier to read than the legal formula. But in every case it will be possible (for a person with unbounded patience) to eliminate the English words and the defined symbols (such as $\varnothing, \cup$ and so forth) in order to arrive at a legal formula. The procedure for eliminating defined symbols is discussed further in the Appendix.

Quantifiers in Induction:

Question(s):

Its rather common to see notation for the inductive step like
"Assume that $A(n)$ is true for a $n \in \mathbb{N}$." This *seems* be translated formally, roughly as

$$[\exists n \in P(n)] \implies P(n+1)$$

Hmm notice what seems to be a potential issue. The inductive step is supposed to look something like

$$(\forall n \in \mathbb{N})[P(n) \implies P(n+1)]$$

For the former, there is a free variable (as it is unquantified). So, would that even make any sense or be a sentence?

Answers:

1. https://math.stackexchange.com/questions/2935730/what-quantifier-is-used-when-assuming-pn-for-some-n-in-the-induction-hypothes
2. https://discord.com/channels/268882317391429632/328208536029102081/1042833046694543520

Basically; the "for some" here does not actually represent the existential quantifier. It is moreso meant to represent an *arbitrary* pick for our choice of n.
By Universal Generalization, we know if $\vdash P(x)$ has been derived, then $\vdash \forall x P(x)$ can also be derived.
We can also look at Enderton's A Introduction to Mathematical Logic for this statement (Pg 117):

GENERALIZATION THEOREM: If $\Gamma \vdash \varphi$ and x does not occur free in any formula in Γ, then $\Gamma \vdash \forall x\, \varphi$.

Hence, the 'logic' is to prove the statement that $n \in \mathbb{N} \implies [P(n) \implies P(n+1)]$ is true, *without any assumptions* on what n is. Then, by Universal Generalization, we know that $\forall n\big(n \in \mathbb{N} \implies [P(n) \implies P(n+1)]\big)$ is true.

(Also, since the existential quantifier in the latter doesn't even extend to P(n+1) you are saying if P(n) is true for one natural number P(n+1) is true for every variable assignment to n i.e. every natural number greater than 0. While what we want in induction is as mentioned above)

0.7.2 Certain Enderton Proofs

Enderton's Proof of Corollary 5QG:

The preceding theorem (Theorem 5QF) provides us h rationals r' and s' for which $r \cdot_{\mathbb{Q}} r' = s \cdot_{\mathbb{Q}} s' = 1_{\mathbb{Q}}$. Hence

$$(r \cdot_{\mathbb{Q}} s) \cdot_{\mathbb{Q}} (r' \cdot_{\mathbb{Q}} s') = 1_{\mathbb{Q}}$$

by using commutative and associative laws. But this implies that $r \cdot_{\mathbb{Q}} s \neq_{\mathbb{Q}}$, because $0_{\mathbb{Q}} \cdot_{\mathbb{Q}} (r' \cdot s') = 0_{\mathbb{Q}} \neq 1_{\mathbb{Q}}$. ⊣

Enderton's Proof of Theorem 5QK:

We can prove this as a corollary of the preceding theorem (Theorem 5QJ), following our past pattern. But there is now a simpler option open to us. In part (a) we add $-t$ to both sides of the given equations, and in part (b) we multiply both sides of the given equation by t^{-1}. (This proof works in any Abelian group.) ⊣

Exercises

1.1 Axioms and Operations

1.1.1 Axioms and Operations

1.1.2 Arbitrary Unions and Intersections

Qns 6(a) ×

Show that:

$$\bigcup \mathbf{P}(\mathbf{A}) = \mathbf{A}$$

By the Powerset Axiom, $P(A)$ contains all subsets of A, i.e.

$$P(A) \iff \forall y(y \in P(A) \iff y \subseteq A)$$

And by the Union Axiom, $\bigcup P(A)$ contains all elements that can be found in any member of $P(A)$:

$$\forall x \left[x \in \bigcup P(A) \iff (\exists y \in P(A))x \in y\right]$$

Trivially, these same members of $P(A)$ are subsets of A. Thus,

$$\forall x \left[x \in \bigcup P(A) \iff (\exists y \subseteq A)x \in y\right]$$

By the definition of a subset that:

$$y \subseteq A \iff \forall x(x \in A \implies x \in A)$$

All elements of $\bigcup P(A)$ must be in A, vice versa as well,

$$\forall x \left[x \in \bigcup P(A) \iff x \in A\right]$$

So, by the Extensionality Axiom, since all elements of $\bigcup P(A) = A$, and vice versa, they must be equal sets

$$\bigcup P(A) = A$$

Q.E.D ■

Remarks (Big Check 1, 28/12/22): If that first part ($P(A) \iff \ldots$) highlighted in green is included, then that line is certainly wrong. "vice versa as well" the converse direction is actually not shown. Of course, the phrasing is not very good since I did this a long time ago when I was less familiar/accustomed to proofs.

Redo of proof: Assume $x \in \bigcup \mathscr{P}A$. By definition of the powerset and union, this implies the existence of some $a \subseteq A$ so $x \in a$. Immediately, we see that x must be in A. Conversely, suppose $x \in A$. Then, $x \in A \subseteq A$, meaning $x \in A \in \mathscr{P}A$. And hence, $x \in \bigcup \mathscr{P}A$. Wherefore, we can now conclude that $\bigcup \mathscr{P}A = A$.

Q.E.D. ■

Qns 6(b) ×

Show that:

$$\mathbf{A \subseteq P \bigcup A}$$

By the Union Axiom, $\bigcup A$ contains all elements that can be found in any member of A:

$$\forall x \left(x \in \bigcup A \iff (\exists a \in A) x \in a \right)$$

Let $X \in A$, then

$$\forall x \left(x \in X \implies x \in \bigcup A \right)$$

By the Powerset Axiom, $P \bigcup A$ contains all subsets of $\bigcup A$, i.e.

$$\forall X \left(X \in P \bigcup A \iff X \subseteq \bigcup A \right)$$

Therefore, since any and all elements of A is also an element of $P \bigcup A$, $A \subseteq P \bigcup A$
Q.E.D. ■

$A = P \bigcup A$ only when $A = \{\varnothing\}$

Remarks (Big Check 1, 28/12/22): There is conflict between what X represents. I should have used two distinct symbols there. Honestly, confusing to read. A number of improvements can be made; such as concluding that $X \subseteq A$ after the second line, writing $X \subseteq \bigcup A \implies X \in \mathscr{P} \bigcup A$ in the third line instead of using the biconditional (which is totally unnecessary), etc.

Redo of proof: Let $x \in A$. Then, for any $y \in x \in A$, $y \in \bigcup A$ immediately follows. Hence, x is clearly a subset of $\bigcup A$ since all its elements are also in $\bigcup A$. Consequently, $x \in \mathscr{P} \bigcup A$. Wherefore, as this holds true for any selection of $x \in A$, $A \subseteq \mathscr{P} \bigcup A$.

Q.E.D. ■

Qns 8 ✓

Show that: There exists no set to which every singleton belongs

Assume there exists a set S containing all singletons. Now, by the Axiom of Pairing: for all sets x, $\{x\}$ is also a set. And hence, $\{x\} \in S$. So, the set

$$\bigcup S = \{x | \{x\} \in S\}$$

is a set of all sets, $\bigcup S$. However, this contradicts Theorem 2A. Therefore, there exists no set of all singletons.

Improved/Edited on 17/11/22

Remarks (Big Check 1, 28/12/22): Ehh seems about right, however, I'm still not satisfied with the phrasing. So, let's redo this!

Redo of proof: Assume a set S of all singletons exists. It follows from the Union Axiom that $\bigcup S = \{x \,|\, \{x\} \in S\}$ is a set. However, $\bigcup S$ would be a set of all sets, because $\{x\}$ exists for any set x by the Axiom of Pairing. This is in clear contradiction with Theorem 2A which asserts that such a set cannot exist. Wherefore, it must be that a set of all singletons does not exist.

Q.E.D. ■

✓

Qns 10

Show that:

$$\textbf{Given a} \in \textbf{b}, \mathscr{P}(\textbf{a}) \in \mathscr{P}\left(\mathscr{P}\left(\bigcup \textbf{B}\right)\right)$$

With reference / help of the Appendix

Assume $a \in B$. Let $c \in \mathscr{P}(a)$, then $c \subseteq a$. Taking $x \in c$, by the definition of the subset this means that $x \in a$:

$$x \in c \implies x \in a$$

By the Union Axiom $x \in \bigcup B$:

$$a \in B \wedge x \in a \implies x \in \bigcup B$$

Since any $x \in c$ also means $x \in \bigcup B$, $c \subseteq B$.

$$\left(x \in c \implies x \in \bigcup B\right) \iff c \subseteq \bigcup B$$

Therefore, $c \in \mathscr{P}\left(\bigcup B\right)$.

$$c \subseteq B \implies c \in \mathscr{P}\left(\bigcup B\right)$$

So, by the definition of the subset, $\mathscr{P}(a) \in \mathscr{P}\left(\bigcup B\right)$

$$\left[c \in \mathscr{P}(a) \implies c \in \mathscr{P}\left(\bigcup B\right)\right] \iff \mathscr{P}(a) \subseteq \mathscr{P}\left(\bigcup B\right)$$

Thus, $\mathscr{P}(a) \in \mathscr{P}\left(\mathscr{P}\left(\bigcup B\right)\right)$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Again, the general direction the proof points towards is correct. However, once more, the phrasing has much room for improvement and there are a number of errors:

1. There should be brackets enclosing the green part.
2. To be more accurate, the universal quantifier should be added in the third line in front of $(x \in c \implies x \in \bigcup B)$.
3. Same thing with the second last line.
4. The capital B should all be replaced with small b.

Redo of proof: Assume $a \in b$ and let $c \in \mathscr{P}(a)$, i.e. $c \subseteq a$. Then, for any $x \in c$, $x \in a \in b$ holds true. Hence, $x \in \bigcup b$ follows. As a result, $c \subseteq \bigcup b$. In other words, $c \in \mathscr{P}(\bigcup b)$. Consequently $\mathscr{P}(a) \subseteq \mathscr{P}(\bigcup b)$. Wherefore, indeed we see that $\mathscr{P}(a) \in \mathscr{P}(\mathscr{P}(\bigcup b))$.

Q.E.D. ■

1.1.3 Algebra of Sets

Qns 11 ✓

Show that for any sets A and B,

$$A = (A \cap B) \cup (A \backslash B) \text{ and } A \cup (B \backslash A) = A \cup B$$

Proof:

$$\begin{aligned} x \in (A \cap B) \cup (A \backslash B) &\iff (x \in A \wedge x \in B) \vee (x \in A \wedge x \notin B) \\ &\iff x \in A \wedge (x \in B \vee x \notin B) \\ &\iff x \in A \end{aligned}$$

Thus, since $x \in (a \cap B) \cup (A \backslash B)$ iff $x \in A$, $(A \cap B) \cup (A \backslash B) = A$

$$\begin{aligned} x \in A \cup (B \backslash A) &\iff x \in A \vee (x \in B \wedge x \notin A) \\ &\iff (x \in A \vee x \in B) \wedge (x \in A \vee x \notin A) \\ &\iff x \in A \vee x \in B \\ &\iff x \in A \cup B \end{aligned}$$

So, since $x \in A \cup (B \backslash A)$ iff $x \in (A \cup B)$, $A \cup (B \backslash A) = A \cup B$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Seems ok.

Qns 12 ✓

Verify the following identity (one of De Morgan's Laws):

$$C \backslash (A \cap B) = (C \backslash A) \cup (C \backslash B)$$

Proof:

$$\begin{aligned} x \in C \backslash (A \cap B) &\iff x \in c \wedge (x \notin A \vee x \notin B) \\ &\iff (x \in C \wedge x \notin A) \vee (x \in C \wedge x \notin B) \\ &\iff x \in (C \backslash A) \vee x \in (C \backslash B) \\ &\iff x \in (C \backslash A) \cup (C \backslash B) \end{aligned}$$

Therefore, $C \backslash (A \cap B) = (C \backslash A) \cup (C \backslash B)$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Seems fine too.

Qns 13 ✓

Show that if $B \subseteq A$, then $C\backslash B \subseteq C\backslash A$

Proof:

Let there be 2 sets A and B such that $A \subseteq B$;

$$\begin{aligned} x \in (C\backslash B) &\iff x \in C \wedge x \notin B \\ &\implies x \in C \wedge x \notin A, \text{ since } x \notin B \implies x \notin A \\ &\implies x \in C\backslash A \end{aligned}$$

Thus, it follows that $C\backslash B \subseteq C\backslash A$

Q.E.D. ■

Qns 15

$$A + B := (A\backslash B) \cup (B\backslash A)$$

(a) ✓ Show that $A \cap (B + C) = (A \cap B) + (A \cap C)$
(b) Show that $A + (B + C) = (A + B) + C$

Proof:

(a) By definition;

$$\begin{aligned} x \in (A \cap B) + (A \cap C) &\iff x \in [(A \cap B)\backslash(A \cap C)] \cup [(A \cap C)\backslash(A \cap B)] \\ &\iff [(x \in A \wedge x \in B) \wedge (x \notin A \vee x \notin C)] \\ &\quad \vee [(x \in A \wedge x \in C) \wedge (x \notin A \vee x \notin B)] \end{aligned}$$

Since $x \notin A$ would mean that $(x \in A \wedge x \in B)$ and $(x \in A \wedge x \in C)$ are both false, therefore it means $x \notin (A \cap B) + (A \cap C)$. Thus, $x \in A$ in order for $x \in (A \cap B) + (A \cap C)$:

$$\begin{aligned} x \in (A \cap B) + (A \cap C) &\iff [(x \in A \wedge x \in B) \wedge x \notin C] \\ &\quad \vee [(x \in A \wedge x \in C) \wedge x \notin B] \\ &\iff x \in [A \cap (B\backslash C)] \cup [A \cap (C\backslash B)] \\ &\iff x \in A \cap (B + C) \end{aligned}$$

So, $A \cap (B + C) = (A \cap B) + (A \cap C)$

Q.E.D. ■

(b)

$$\begin{aligned} x \in A + (B + C) &\iff x \in A + [(B \backslash C) \cup (C \backslash B)] \\ &\iff x \in (A \backslash [(B \backslash C) \cup (C \backslash B)]) \cup ([(B \backslash C) \cup (C \backslash B)] \backslash A) \end{aligned}$$

$$\begin{aligned} x \in (A + B) + C &\iff x \in [(A \backslash B) \cup (B \backslash A)] + C \\ &\iff x \in ([(A \backslash B) \cup (B \backslash A)] \backslash C) \cup (C \backslash [(A \backslash B) \cup (B \backslash A)]) \end{aligned}$$

And observe that:

$$x \in (B \backslash C) \cup (C \backslash B) \iff (x \in B \wedge x \notin C) \vee (x \in C \wedge x \notin B)$$

$$\begin{aligned} x \notin (B \backslash C) \cup (C \backslash B) &\iff \neg[(x \in B \wedge x \notin C) \vee (x \in C \wedge x \notin B)] \\ &\iff (x \notin B \vee x \in C) \wedge (x \notin C \wedge x \in B) \\ &\iff (x \in B \wedge x \in C) \vee (x \notin B \wedge x \in C) \end{aligned}$$

Applying this onto our previous expansions of $A + (B + C)$ and $(A + B) + C$;

$$\begin{aligned} x \in A + (B + C) &\iff (x \in A \wedge [(x \in B \wedge x \in C) \vee (x \notin B \wedge x \in C)]) \\ &\quad \vee ([(x \in B \wedge x \notin C) \vee (x \in C \wedge x \notin B)] \wedge x \notin A) \\ &\iff (x \in A \wedge x \in B \wedge x \in C) \vee (x \in A \wedge x \notin B \wedge x \notin C) \\ &\quad \vee [(x \in B \wedge x \notin C) \wedge x \notin A] \vee [(x \in C \wedge x \notin B) \wedge x \notin A] \\ &\iff (x \in A \wedge x \in B \wedge x \in C) \vee (x \in A \wedge x \notin B \wedge x \notin C) \\ &\quad \vee (x \in B \wedge x \notin C \wedge x \notin A) \vee (x \in C \wedge x \notin B \wedge x \notin A) \end{aligned}$$

$$\begin{aligned} x \in (A + B) + C &\iff x \in ([(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)] \wedge x \notin C) \\ &\quad \vee (x \in C \vee [(x \in A \vee x \in B) \wedge (x \notin B \vee x \notin A)]) \\ &\iff ([(x \in A \wedge x \notin B) \wedge x \notin C] \vee [(x \in B \wedge x \notin A) \wedge x \notin C]) \\ &\quad \vee (x \in C \wedge x \in B \wedge x \in A) \vee (x \in C \wedge x \notin B \wedge x \notin C) \\ &\iff (x \in A \wedge x \notin B \wedge x \notin C) \vee (x \in B \wedge x \notin A \wedge x \notin C) \\ &\quad \vee (x \in C \wedge x \in B \wedge x \in A) \vee (x \in C \wedge x \notin A \wedge x \notin B) \end{aligned}$$

So, $A + (B + C) = (A + B) + C$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Yeah nope I'm not checking this. Proving this by a truth table (considering the cases of $x \in A$, $x \notin A$, etc) would be much easier and readable, but last time I wanted to mess around a lil lol.

Qns 19

Is $\mathscr{P}(A\backslash B)$ always equal to $\mathscr{P}(A)\backslash\mathscr{P}(B)$? Is it ever equal to $\mathscr{P}(A)\backslash\mathscr{P}(B)$?

1. ✓ Let's look at a simple counterexample; Let $A = \{1, 2, 3\}$ and $B = \{3\}$,

$$\mathscr{P}(A\backslash B) = \mathscr{P}(\{1, 2\}) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$$

$$\begin{aligned}\mathscr{P}(A)\backslash\mathscr{P}(B) &= \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\} \ \backslash \ \{\varnothing, \{3\}\} \\ &= \{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}\end{aligned}$$

Thus, $\mathscr{P}(A\backslash B)$ is not always equal to $\mathscr{P}(A)\backslash\mathscr{P}(B)$. Also, notice that for all powersets, they contain $\varnothing$. Therefore, $\mathscr{P}(A\backslash B)$ always contains the $\varnothing$ while $\mathscr{P}(A)\backslash\mathscr{P}(B)$ never contains $\varnothing$, meaning that the $\mathscr{P}(A\backslash B) \neq \mathscr{P}(A)\backslash\mathscr{P}(B)$ for all sets A and B. Remarks (Big Check 1, 28/12/22): Not bad, the phrasing has improved compared to previous parts. Still has room for improvement though, of course.

2. × Score: Wtf Let's look at another way of showing this:

Let $X \in \mathscr{P}(A\backslash B)$, then $X \subseteq A\backslash B$, and $x \in X \iff x \in A \wedge x \notin B$

Also, let $Y \in \mathscr{P}(A)\backslash\mathscr{P}(B)$, meaning that $Y \in \mathscr{P}(A) \wedge Y \notin \mathscr{P}(B)$. So,
$y \in Y \implies y \in A \iff y \in A \wedge (y \in B \vee y \notin B)$

Therefore, $\mathscr{P}(A\backslash B) \not\equiv \mathscr{P}(A)\backslash\mathscr{P}(B)$ since their elements are not necessarily the same; it can be the case that $y \in A \wedge y \in B$ while it is always the case that $x \in A \wedge x \notin B$.

$$\begin{aligned}\mathscr{P}(A\backslash B) = \mathscr{P}(A)\backslash\mathscr{P}(B) \text{ iff } &\forall X, Y[X \in \mathscr{P}(A\backslash B) \vee Y \in \mathscr{P}(A)\backslash\mathscr{P}(B)] \\ &\forall z(z \in X \vee z \in Y)(z \in A \wedge z \notin B)\end{aligned}$$

Thus, for $\mathscr{P}(A\backslash B)$ there must be no $z \in A \wedge z \in B$. For $\varnothing \in \mathscr{P}(A\backslash B)$, which is always the case, is it (vacuously) true that all the non-existent members of $\varnothing$ are in A and in B. So, it is never the case that $\mathscr{P}(A\backslash B) = \mathscr{P}(A)\backslash\mathscr{P}(B)$.

Remarks (Big Check 1, 28/12/22): The presentation is rather terrible, the unnecessary symbols obscure the key points and makes it significantly challenging to the reader to understand. The errors are stated below:

1. First line: brackets around $x \in A \wedge x \notin B$ (however, again, English words are superior in this context)
2. Second line: brackets again. And in addition, the use of the conditional and biconditional on a single line is rather confusing to read.
3. Second and Third line: Yeah idk wtf I was writing anymore...

Qns 21 ×

Show that $\bigcup(A \cup B) = \bigcup A \cup \bigcup B$.

Let $X \in A$ and $Y \in B$, $x \in X$ and $y \in Y$,

$$(X \in A)x \in X \implies x \in \bigcup A$$

$$(Y \in B)y \in Y \implies y \in \bigcup B$$

Therefore,

$$x, y \in \bigcup A \cup \bigcup B$$

Observe that:

$$X, Y \in A \cup B$$

Thus,

$$x, y \in \bigcup(A \cup B)$$

So, since for any elements of the members of A and B, they are in both $\bigcup A \cup \bigcup B$ and $\bigcup(A \cup B)$, by the Extensionality Axiom, they are equal sets and $\bigcup A \cup \bigcup B = \bigcup(A \cup B)$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Wtf is that notation on the first (mathmode) line; $(X \in A)x \in X$ and $(Y \in B)y \in Y$? That's only used when we have a quantifier. In this case the proper notation would be $x \in X \in A$ and $y \in Y \in B$. Again, the phrasing and presentation is quite terrible, making the proof difficult to read and understand. The starting assumption is also kinda strange, why not just start with assuming $x \in \bigcup(A \cup B)$, then later the converse?

Qns 22 ×

Show that for if A and B are nonempty sets, $\bigcap(A \cup B) = \bigcap A \cap \bigcap B$.

Assume A and B to be nonempty sets. Let $X \in A, Y \in B$, and $x \in X, y \in Y$,

$$X, Y \in A \cup B$$

$$\forall X, Y(z \in X \wedge z \in Y) \iff z \in \bigcap(A \cup B)$$

Also, observe that:

$$\forall X(x \in X) \iff x \in \bigcap A$$

$$\forall Y(y \in Y) \iff y \in \bigcap B$$

Thus,

$$\forall X, Y(z \in X \wedge z \in Y) \iff z \in \bigcap A \cap \bigcap B$$

So, since for any arbitrary z, as long as $\forall X, Y(z \in X \wedge z \in Y)$, then $z \in \bigcap(A \cup B)$ and $z \in \bigcap A \cap \bigcap$, therefore by the Extensionality Axiom, $\bigcap(A \cup B) = \bigcap A \cap \bigcap B$. As long as A and B are nonempty sets.

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Much of the same issue as my past answer to Qns 21. I get the *gist* is the line of reasoning I was going for but still terrible, if im being honest.

Qns 23 ×

Show that if B is nonempty, then $A \cup \bigcap B = \bigcap\{A \cup X | X \in B\}$.

Assume B is a nonempty set. Let $Y \in A$ and $X \in B$, $y \in Y$ and $x \in X$,

$$\forall X(x \in X) \iff x \in \bigcap B$$

$$z \in A \vee \forall X(z \in X) \iff z \in A \cup \bigcap B$$

Also, notice that

$$z \in A \vee z \in X \iff z \in A \cup X$$

Thus,

$$z \in A \vee \forall X(z \in X) \iff z \in \bigcap\{A \cup X | X \in B\}$$

So, since for any z, $z \in A \vee \forall X(z \in X)$ means that z is an element of both $A \cup \bigcap B$ and $\bigcap\{A \cup X | X \in B\}$, by the Extensionality Axiom, $A \cup \bigcap B = \bigcap\{A \cup X | X \in B\}$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Again, I get what I was trying to bring across. However, the issue again lies in the frankly terrible presentation of it.

Qns 24

(a) ✓ Show that if A is nonempty, then $\mathscr{P}\bigcap A = \bigcap\{\mathscr{P}(X) | X \in A\}$
(b) Show that $\bigcup\{\mathscr{P}(X) | X \in A\} \subseteq \mathscr{P}\bigcup A$

(a)

Let $X \in A$, $x \in X$, $y \in \mathscr{P}\bigcap A$, notice that:

$$x \in \bigcap A \iff \forall X(x \in X)$$

$$\begin{aligned} y \in \mathscr{P}\bigcap A &\iff y \subseteq \bigcap A \\ &\iff \forall x(x \in y \implies x \in \bigcap A) \\ &\iff \forall x, X(x \in y \implies x \in X) \end{aligned}$$

Thus,

$$\begin{aligned} \forall x, X(x \in y \implies x \in X) &\iff \forall X(y \subseteq X) \\ &\iff \forall X(y \in \mathscr{P}(X)) \\ &\iff y \in \bigcap\{\mathscr{P}(X) | X \in A\} \end{aligned}$$

So, since for any y, $y \in \mathscr{P}\bigcap A \iff y \in \bigcap\{\mathscr{P}(X) | X \in A\}$, $\mathscr{P}\bigcap A = \bigcap\{\mathscr{P}(X) | X \in A\}$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Well, its more readable than some of the previous ones but the presentation is still clunky at best. Also, in the first line, there's no need to state the definition of the Union Axiom.

(b) ×

Let $x \in X, X \in A$ and $y \in \bigcup\{\mathscr{P}(X)|X \in A\}$,

Then,

$$\begin{aligned} y \in \bigcup\{\mathscr{P}(X)|X \in A\} &\iff y \in \mathscr{P}(X) \\ &\iff y \subseteq X \\ &\iff x \in y \implies x \in X \end{aligned}$$

Using the fact that

$$\begin{aligned} x \in \bigcup A &\iff (X \in A)x \in X \\ &\iff x \in X \end{aligned}$$

It follows that:

$$\begin{aligned} y \in \bigcup\{\mathscr{P}(X)|X \in A\} &\iff x \in y \implies x \in \bigcup A \\ &\implies y \subseteq \mathscr{P}\bigcup A \end{aligned}$$

So, since $y \in \bigcup\{\mathscr{P}(X)|X \in A\} \implies y \in \mathscr{P}\bigcup A$, by the definition of the subset, $\bigcup\{\mathscr{P}(X)|X \in A\} \subseteq y \in \mathscr{P}\bigcup A$.

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Same issues again with presentation and stuff. We're missing the existential quantifiers and brackets. Also, in the last *mathmode line*, I'm pretty sure I meant to write $y \in \mathscr{P}\bigcup A$ instead of $y \subseteq \mathscr{P}\bigcup A$.

Qns 25 ✓

Is $A \cup \bigcup B$ always the same as $\bigcup\{A \cup X|X \in B\}$? If not, then under what conditions does the equality hold?

Let $z \in A \cup \bigcup B$ and $X \in B$,

Then,

$$\begin{aligned} z \in A \cup \bigcup B &\iff z \in A \vee z \in \bigcup B \\ &\iff z \in A \vee z \in X \\ &\iff z \in A \cup X \\ &\iff z \in \bigcup\{A \cup X|X \in B\} \end{aligned}$$

Thus, since for any z, $z \in A \cup \bigcup B \iff z \in \bigcup\{A \cup X|X \in B\}$, by the Extensionality Axiom, $A \cup \bigcup B$ is always the same as $z \in \bigcup\{A \cup X|X \in B\}$.

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Aside from the missing brackets and (two) existential quantifiers, the proof's general outline seems fine. But there's no need to say that "By the Extensionality Axiom…"

1.1.4 Epilogue

Qns 31

Let B be the set $\{\{1,2\},\{2,3\},\{1,3\},\{\varnothing\}\}$
(a) $\bigcup B$
(b) $\bigcap B$
(c) $\bigcap\bigcup B$
(d) $\bigcup\bigcap B$

(a) ✓ $\bigcup B = \{\varnothing, 1, 2, 3\}$
(b) ✓ $\bigcap B = \varnothing$
(c) ✓ $\bigcap\bigcup B = \varnothing$
(d) ✓ $\bigcup\bigcap B = \varnothing$

Qns 32

Let S be the set {{a}, {a, b}}. Evaluate and simplify:
(a) $\bigcup\bigcup S$
(b) $\bigcap\bigcap S$
(c) $\bigcap\bigcup S \cup (\bigcup\bigcup S \backslash \bigcup\bigcap S)$

(a) ✓ $\bigcup\bigcup S = \bigcup\{a,b\} = a \cup b$
(b) ✓ $\bigcap\bigcap S = \bigcap\{a\} = a$
(c) ✓ $\bigcap\bigcup S \cup (\bigcup\bigcup S \backslash \bigcup\bigcap S) = (a \cap B) \cup [(a \cup b)\backslash a] = (a \cap b) \cup (b \backslash a) = b$

Qns 33 ✓

With S as in the preceding exercise, evaluate $\bigcup(\bigcup S \backslash \bigcap S)$ with when $a \neq b$ and when a = b

$$\bigcup\left(\bigcup S \backslash \bigcap S\right) = \bigcup(\{a,b\}\backslash\{a\}) = \bigcup\{b\} = b$$

Therefore, when $a \neq b$, $\bigcup(\bigcup S \backslash \bigcap S) = \bigcup\{b\} = b$, and when $a = b$, $\bigcup(\bigcup S \backslash \bigcap S) = \varnothing$

Remarks (Big Check 1, 28/12/22): In order to claim $\bigcup(\{a,b\}\backslash\{a\}) = \bigcup\{b\}$, we are using the assumption that $a \neq b$. So it would have been good if that was explicitly stated. But yeah the final answers should be correct.

Qns 34 ✓

Show that $\{\varnothing, \{\varnothing\}\} \in \mathscr{P}\mathscr{P}\mathscr{P}\mathscr{P}(S)$ for every set S

Since all non-existent elements of $\varnothing$ are in any and all sets, it is true that $\varnothing$ is a subset of all sets. Thus, for any set S,

$$\varnothing \in \mathscr{P}\mathscr{P}(S)$$
$$\varnothing \in \mathscr{P}\mathscr{P}\mathscr{P}(S) \wedge \{\varnothing\} \in \mathscr{P}\mathscr{P}\mathscr{P}(S)$$

Meaning that $\mathscr{P}\mathscr{P}\mathscr{P}(S) = \{\varnothing, \{\varnothing\}, \cdots\}$. Therefore, $\{\varnothing, \{\varnothing\}\}$ is a subset of $\mathscr{P}\mathscr{P}\mathscr{P}(S)$:

$$\{\varnothing, \{\varnothing\}\} \in \mathscr{P}\mathscr{P}\mathscr{P}\mathscr{P}(S)$$

So, $\{\varnothing, \{\varnothing\}\} \in \mathscr{P}\mathscr{P}\mathscr{P}\mathscr{P}(S)$ for every set S.

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): The first sentence is unnecessary as $\varnothing$ begin a subset of any set is trivial enough. Again, use English words over symbols like $\wedge$. But the phrasing here isn't as horrendous as some previous questions. And it seems fine in general, albeit with a lot of room for improvement.

Qns 37 ✓

Show that for the following sets the equations hold:
(a) $(A \cup B)\backslash C = (A\backslash C) \cup (B\backslash C)$
(b) $A\backslash(B\backslash C) = (A\backslash B) \cup (A \cap C)$
(c) $(A\backslash B)\backslash C = A\backslash(B \cup C)$

(a) ✓

$$\begin{aligned} t \in (A \cup B)\backslash C &\iff t \notin C \wedge (t \in A \vee t \in B) \\ &\iff (t \in A \wedge t \notin C) \vee (t \in B \wedge t \notin C) \\ &\iff t \in (A\backslash C) \cup (B\backslash C) \end{aligned}$$

Therefore, $(A \cup B)\backslash C = (A\backslash C) \cup (B\backslash C)$

(b) ✓

$$\begin{aligned} t \in A\backslash(B\backslash C) &\iff t \in A \wedge t \notin (B\backslash C) \\ &\iff t \in A \wedge (t \notin B \vee t \in C) \\ &\iff (t \in A \wedge t \notin B) \vee (t \in A \wedge t \in C) \\ &\iff t \in (A\backslash B) \cup (A \cap C) \end{aligned}$$

Therefore, $A\backslash(B\backslash C) = (A\backslash B) \cup (A \cap C)$

(c) ✓

$$\begin{aligned} t \in (A \backslash B) \backslash C &\iff (t \in A \wedge t \notin B) \wedge t \notin C \\ &\iff t \in A \wedge (t \notin B \wedge t \notin C) \\ &\iff t \in A \backslash (B \cup C) \end{aligned}$$

Therefore, $(A \backslash B) \backslash C = A \backslash (B \cup C)$

Remarks (Big Check 1, 28/12/22): Would have been good to add the necessary brackets, even though it should be clear what is meant. Not really a big issue here tho.

Qns 38 ✓

Prove that the following are valid:
(a) $A \subseteq C \wedge B \subseteq C \iff A \cup B \subseteq C$
(b) $C \subseteq A \wedge C \subseteq B \iff C \subseteq A \cap B$

(a) ✓

$$\begin{aligned} A \cup B \subseteq C &\iff (t \in A \vee t \in B) \implies t \in C \\ &\iff (t \in A \implies t \in C) \wedge (t \in B \implies t \in B) \\ &\iff A \subseteq C \wedge B \subseteq C \end{aligned}$$

So, $A \subseteq C \wedge B \subseteq C \iff A \cup B \subseteq C$.

Remarks (Big Check 1, 28/12/22): We should have added for all t with some additional brackets. The transition from the first to second step should have shown some intermediary steps to be clearer as well. But overall, the gist is fine.

(b) ✓

$$\begin{aligned} C \subseteq A \wedge C \subseteq B &\iff (t \in C \implies t \in A) \wedge (t \in C \implies t \in B) \\ &\iff t \in C \implies (t \in A \wedge t \in B) \\ &\iff C \subseteq (A \cap B) \end{aligned}$$

So, $C \subseteq A \wedge C \subseteq B \iff C \subseteq A \cap B$.

Remarks (Big Check 1, 28/12/22): Same thing here as in part (a).

1.2 Relations and Functions

1.2.1 Ordered Pairs

1. ✓ Suppose that we attempted to generalise the Kuratowski definitions of ordered pairs to ordered triples by defining

$$\langle x, y, z\rangle^* = \{\{x\}, \{x, y\}, \{x, y, z\}\}$$

Show that this definition is unsuccessful by giving examples of objects u, v, w, x, y, z with

$$\langle x, y, z\rangle^* = \langle u, v, w\rangle^*$$

but with either $y \neq v$ or $z \neq w$ (or both).

Answer:

Example:

$$\begin{aligned}\langle 1, 2, 1\rangle &= \{\{1\}, \{1, 2\}, \{1, 2, 1\}\}\\ &= \{\{1\}, \{1, 2\}, \{1, 2\}\}\end{aligned}$$

$$\begin{aligned}\langle 1, 2, 2\rangle &= \{\{1\}, \{1, 2\}, \{1, 2, 2\}\}\\ &= \{\{1\}, \{1, 2\}, \{1, 2\}\}\end{aligned}$$

Therefore, $\langle 1, 2, 1\rangle = \langle 1, 2, 2\rangle$ by this definition. Through this definition, as long as $w = y \vee w = z$, then $\langle x, y, z\rangle = \langle u, v, w\rangle$. This is not what we want from the definition of an ordered triple, as we want an ordered triple in the form $\langle x, y, z\rangle = \langle u, v, w\rangle$ iff $x = u \wedge y = v \wedge z = w$.

Remarks (Big Check 1, 28/12/22): Would have been good to say something like "in spite of the fact that $1 \neq 2$ in the third coordinate." after "Therefore, ... by this definition". Still, a valid counterexample!

3. ✓ Show that

$$A \times \bigcup B = \bigcup\{A \times X | X \in B\}$$

Proof:

$$\begin{aligned}\langle x, y\rangle \in A \times \bigcup B &\iff x \in A \wedge y \in \bigcup B\\ &\iff \exists X \in B\,(x \in A \wedge y \in X)\\ &\iff \exists X \in B\,(\langle x, y\rangle \in A \times X)\\ &\iff \langle x, y\rangle \in \bigcup\{A \times X | X \in B\}\end{aligned}$$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Yeah seems fine, its just that I would prefer an additional bracket in the first line.

4. ✓ Show that there is no set to which every ordered pair belongs.

Suppose that there exists a set S to which every ordered pair belongs. Now, by the Union Axiom we have

$$\begin{aligned} x \in \bigcup\bigcup S &\iff \exists s \exists \gamma (s \in S \wedge \gamma \in s \wedge x \in \gamma) \\ &\iff \exists y \exists z [\{\{y\}, \{y, z\}\} \in S \wedge (x \in \{y\} \vee x \in \{y, z\})] \\ &\iff \exists y \exists z [\{\{y\}, \{y, z\}\} \in S \wedge (x = y \vee x = z)] \end{aligned}$$

By the Axiom of Pairing, given any sets y, z, there exists the sets $\{y\}, \{z\}, \{y, z\}$. So, this means that the existence of such a set S containing all ordered pairs means that there also exist a set $\bigcup\bigcup S$ containing all sets. However, this contradicts Theorem 2A (Russel's Paradox) that there must not be any set of all sets. Thence, there does not exist a set S to which every ordered pair belongs. :D

Remarks (Big Check 1, 28/12/22): Yeah the general idea is there. But the presentation could again be better. Like, there's no reason to use $x \in \bigcup\bigcup S$ instead of $\langle x, y\rangle \in \bigcup\bigcup S$. Also, the $\exists s \exists \gamma (s \in S \wedge \gamma \in s \wedge x \in \gamma)$ part is unnecessary. Hence, let us do a redo of the above proof.

Redo of proof (2 proofs):

1. Assume that there exists such a set S of all ordered pairs. Now, we construct the subset $S' = \{\langle x, x\rangle \mid \langle x, x\rangle \in S\}$. Notice that every $\langle x, x\rangle$ can be simplified to $\{\{x\}\}$, by definition. Therefore, S' is the set of all such $\{\{x\}\}$. By the Axiom of Pairing, the set $\{\{x\}\}$ exists iff $\{x\}$ does. Whence, we can conclude that $\bigcup S'$ is the set of all singletons. However, this is in clear contradiction to exercise 4 of chapter 2. Wherefore, it must be that no set of all ordered pairs exists.

2. Suppose there exists such a set S of all ordered pairs. Then, $\bigcup S$ is a set containing all $\{x\}$ and $\{x, y\}$, because by the Axiom of Pairing, $\langle x, y\rangle$ exists iff $\{x\}$ and $\{x, y\}$ do. We repeat this procedure once more; $\bigcup\bigcup S$ is our set of all sets, as by the Axiom of Pairing once more, $\{x\}$ and $\{x, y\}$ exists iff the sets x and y (that belong in $\bigcup\bigcup S$) do. However, this now contradicts Theorem 2A which states the nonexistence of a set of all sets. Wherefore, it must be that no such set of all ordered pairs exist.

Q.E.D. ■

5. ✓

(a) ✓ Assume A and B are given sets, and show that there exists a set C such that for any y,

$$y \in C \iff y = \{x\} \times B \text{ for some } x \text{ in } A$$

In other words, show that $\{\{x\} \times B | x \in A\}$ is a set.

(b) ✓ With A, B, and C as above, show that $A \times B = \bigcup C$

(a)

Let A and B be sets.

By Corollary 3C, $A \times B = \{\langle x, y\rangle \,| x \in A \wedge y \in B\}$ is a set.

By the Powerset Axiom, $\mathscr{P}(A \times B)$ is also a set.

For any given $x \in A$, $\{x\} \subseteq A$ by a subset axiom. This is just one possible selection of x out of possibly many in A; thus $\{x\} \times B \subseteq A \times B$ is also a set by another subset axiom.

$$\begin{aligned} r \in \{x\} \times B &\iff r = \langle x, y\rangle \wedge x \in A \wedge y \in B \\ &\implies r \in A \times B \end{aligned}$$

So, by a subset axiom on $\mathscr{P}(A \times B)$, $C = \{\{x\} \times B | x \in A\}$ is a set too.

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Rather than the mathmode part with symbols, nowadays I would probably prefer to write that in words. Also, after that part it would be nice to first explicitly state that $\{x\} \times B$ is a subset of $A \times B$, followed by the final conclusion. Otherwise, yeah looks ok to me.

(b)

$$\begin{aligned} y \in \bigcup C &\iff y \in \bigcup \{\{x\} \times B | x \in A\} \\ &\iff (\exists x \in A) y \in \{x\} \times B \\ &\iff y \in A \times B \end{aligned}$$

Q.E.D. ■

Remarks (Big Check 1, 28/12/22): Again, would prefer words. But seems fine.

1.2.2 Relations

6. × Show that a set A is a relation iff $A \subseteq \text{dom } A \times \text{ran A}$

Assume set A is a relation. We can expand dom $A \times$ ran A to help us:

$$\begin{aligned}\text{dom } A \times \text{ran } A &= \{\langle x, y\rangle \,|x \in \text{dom } A \wedge y \in \text{ran A}\} \\ &= \{\langle x, y\rangle \,|x \in \{x|\exists z_1(xAz_1)\} \wedge y \in \{y|\exists z_2(z_2Ay)\}\} \\ &= \{\langle x, y\rangle \,|\exists z_1 \exists z_2(xAz_1 \wedge z_2Ay_2)\}\end{aligned}$$

Thus,

$$\begin{aligned}\langle x, y\rangle \in A &\iff xAy \\ &\implies \langle x, y\rangle \in \{\langle x, y\rangle \,|\exists z_1 \exists z_2(xAz_1 \wedge z_2Ay_2)\} \\ &\text{(In this case, } x = z_2 \wedge y = z_1) \\ &\implies \langle x, y\rangle \in \text{dom } A \times \text{ran } A\end{aligned}$$

So, A being a relation implies $A \subseteq \text{dom } A \times \text{ran } A$.

The converse holds true rather simply; Suppose dom A and ran A are some sets, such that there is a set $A \subseteq \text{dom } A \times \text{ran } A$

$$\text{dom } A \times \text{ran A} = \{\langle x, y\rangle \,|x \in \text{dom } A \wedge y \in \text{ran A}\}$$

$$A \subseteq \text{dom } A \times \text{ran } A \iff [\eta \in A \iff (\eta \in \text{dom } A \times \text{ran } A \wedge \varphi)]$$

for some predicate φ.

Thus, A is obviously a set of ordered pairs and hence a relation.

Thence, a set A is a relation iff $A \subseteq$ dom $A \times$ ran A.

Remarks (Big Check 1, 28/12/22): Seems a bit of a mess tbh, presentation leaves much to be desired. Hence, we shall now do a redo of the above question.

Redo of proof:

Assume that the set A is a relation and $\langle x, y\rangle$ is some element of A. Clearly, $x \in \text{dom } A$ and $y \in \text{ran } A$ since xAy. Consequently, $\langle x, y\rangle$ is in $\text{dom } A \times \text{ran } A$. Which also means $A \subseteq \text{dom } A \times \text{ran } A$. Conversely, suppose $A \subseteq \text{dom } A \times \text{ran } A$. Since the Cartesian product $\text{dom } A \times \text{ran } A$ only contains ordered pairs by definition, the set A must also only have ordered pairs in it. Therefore, A is a relation. Wherefore, the set A is a relation iff $A \subseteq \text{dom } A \times \text{ran } A$.

Q.E.D. ■

8. ✓ Show that for any set $\mathscr{A}$:

$$\begin{aligned}\operatorname{dom}\bigcup\mathscr{A} &= \bigcup\{\operatorname{dom}\ R|R\in\mathscr{A}\}\\ \operatorname{ran}\bigcup\mathscr{A} &= \bigcup\{\operatorname{ran}\ R|R\in\mathscr{A}\}\end{aligned}$$

We can simplify $\operatorname{dom}\bigcup\mathscr{A}$ and $\bigcup\{\operatorname{dom}\ R|R\in\mathscr{A}\}$ into their respective logical expressions first:

$$\begin{aligned}x\in\bigcup\{\operatorname{dom}\ R|R\in\mathscr{A}\} &\iff \exists R(R\in\mathscr{A}\wedge x\in\operatorname{dom}\ R)\\ &\iff \exists R[R\in\mathscr{A}\wedge\exists t(\langle x,t\rangle\in R)]\\ &\iff \exists R\exists t(R\in\mathscr{A}\wedge\langle x,t\rangle\in R)\end{aligned}$$

$$\begin{aligned}x\in\operatorname{dom}\bigcup\mathscr{A} &\iff \exists t\left(\langle x,t\rangle\in\bigcup A\right)\\ &\iff \exists R\exists t(R\in\mathscr{A}\wedge\langle x,t\rangle\in R)\end{aligned}$$

Now it is simple to see that

$$x\in\operatorname{dom}\bigcup\mathscr{A}\iff x\in\bigcup\{\operatorname{dom}\ R|R\in\mathscr{A}\}$$

So, obviously, by the Axiom of Extensionality, $\operatorname{dom}\bigcup\mathscr{A}=\bigcup\{\operatorname{dom}\ R|R\in\mathscr{A}\}$.

The case of $\operatorname{ran}\bigcup\mathscr{A}=\bigcup\{\operatorname{ran}\ R|R\in\mathscr{A}\}$ is basically the same procedure, so I won't redo it again.

Remarks (Big Check 1, 28/12/22): Rather than writing two chains of biconditionals and then doing a conclusion, it is simpler to just write it down in one chain, i.e.:

$$\begin{aligned}x\in\bigcup\{\operatorname{dom}\ R|R\in\mathscr{A}\} &\iff \exists R(R\in\mathscr{A}\wedge x\in\operatorname{dom}\ R)\\ &\iff \exists R[R\in\mathscr{A}\wedge\exists t(\langle x,t\rangle\in R)]\\ &\iff \exists R\exists t(R\in\mathscr{A}\wedge\langle x,t\rangle\in R)\\ &\iff \exists t\left(\langle x,t\rangle\in\bigcup A\right)\\ &\iff x\in\operatorname{dom}\bigcup\mathscr{A}\end{aligned}$$

Which affected the coherency of the above proof.

1.2.3 n-ary relations

10. ✓ Show that an ordered 4-tuple is also an ordered m-tuple for every positive integer m less than 4.

Proof:

$$\langle \alpha, \beta, \gamma, \zeta \rangle = \langle \langle \alpha, \beta, \gamma, \zeta \rangle \rangle$$

This shows that a 4-tuple is also a 1-tuple.

$$\langle \alpha, \beta, \gamma, \zeta \rangle = \langle \langle \alpha, \beta, \gamma \rangle, \zeta \rangle$$

This shows that a 4-tuple is also a 2-tuple.

$$\langle \alpha, \beta, \gamma, \zeta \rangle = \langle \langle \langle \alpha, \beta \rangle, \gamma \rangle, \zeta \rangle = \langle \langle \alpha, \beta \rangle, \gamma, \zeta \rangle$$

This shows that a 4-tuple is also a 3-tuple

Thence, a 4-tuple is a m-tuple for every positive integer m less than 4.

1.2.4 Functions

11. × Prove the following version (for functions) of the extensionality principle: Assume that F and G are functions, $\operatorname{dom} F = \operatorname{dom} G$, and $F(x) = G(x)$ for all x in the common domain. Then $F = G$.

$\operatorname{dom} F = \operatorname{dom} G$ and $F(x) = G(x)$ for all x in the common domain means that:

$$\begin{aligned}
&\forall x(x \in \operatorname{dom} F \wedge x \in \operatorname{dom} G \implies F(x) = G(x)) \\
\iff &\forall x[x \in \operatorname{dom} F \wedge x \in \operatorname{dom} G \implies \exists y(xFy \iff xGy)] \\
\iff &\forall x[x \in \operatorname{dom} F \vee x \in \operatorname{dom} G \implies \exists y(xFy \iff xGy)], \text{ since } \operatorname{dom} F = \operatorname{dom} G \\
\iff &F = G
\end{aligned}$$

Thence, our proof is complete since we have shown $F = G$.

Remarks (Big Check 1, 28/12/22): Unnecessary use of symbols which make the proof very hard to read, and neither clear nor concise. Resultantly, we will redo this:

Redo of proof:

Assume that F and G are functions so that $\operatorname{dom} F = \operatorname{dom} G$ and $F(x) = G(x)$ for all x in their common domain. Consequently, we see that
$F = \{\langle x, y\rangle \mid x \in \operatorname{dom} F \ \&\ y = F(x)\} = \{\langle x, y\rangle \mid x \in \operatorname{ran} G \ \&\ y = G(x)\} = G$. Wherefore, we conclude that $F = G$.

Q.E.D. ■

14. Assume that f and g are functions.

(a) × Show that $f \cap g$ is a function.

(b) Show that $f \cup g$ is a function iff $f(x) = g(x)$ for every x in $(\operatorname{dom} f) \cap (\operatorname{dom} g)$.

(a) Let f, g be functions,

$$z \in f \cap g \iff (z \in f \wedge z \in g) \iff \exists x \exists y(z = \langle x, y\rangle \wedge xfy \wedge xgy)$$

So, $f \cap g$ certainly contains tuples (only). Assume that $f \cap g$ is not a function, i.e. $f \cap g$ is not single-valued. Now;

$$\begin{aligned}
&\exists x \exists y_1 \exists y_2[(\langle x, y_1\rangle \in f \cap g) \wedge (\langle x, y_2\rangle \in f \cap g)] \\
\iff &\exists x \exists y_1 \exists y_2[(\langle x, y_1\rangle \in f) \wedge (\langle x, y_2\rangle \in f) \wedge (\langle x, y_1\rangle \in g) \wedge (\langle x, y_2\rangle \in g)]
\end{aligned}$$

However, we initially let f, g be functions, and it is shown that our assumption that $f \cap g$ is not a function (more precisely, that $f \cap g$ is not single-valued) leads to a contradictory conclusion that f, g are not functions. So, by contradiction, $f \cap g$ must be (single-valued, and) a function (since we shown it contains tuples only and $f \cap g$ is indeed single-valued).

Remarks (Big Check 1, 28/12/22): Yeah this seems like quite an unnecessarily convoluted mess. Let's redo this.

Redo of proof:

Assume that f and g are functions. Clearly, $f \cap g$ must contain only ordered pairs, hence, it is a relation. Now, we need to check for single-valuedness. Suppose that $\langle x, y_1\rangle \in f \cap g$ and $\langle x, y_2\rangle \in f \cap g$ simultaneously. Then, it follows that $\langle x, y_1\rangle \in f$, $\langle x, y_2\rangle \in f$, $\langle x, y_1\rangle \in g$, and $\langle x, y_2\rangle \in g$. Consequently, since f and g are single-valued (as they are functions), $y_1 = y_2$. In other words, $f \cap g$ is a single-valued relation. Wherefore, $f \cap g$ is indeed a function.

Q.E.D. ■

(b) Let f, g be functions once again;

$$\forall x \forall y[\langle x, y\rangle \in f \cup g \iff (xfy \vee xgy)]$$

If $f \cup g$ is a function, it has to be single rooted, meaning that:

$$\begin{aligned}
&f \cup g \text{ is a function} \\
\iff &\big[\forall x \forall y_1 \forall y_2 \big([(xfy_1 \vee xgy_1) \wedge (xfy_2 \vee xgy_2)] \implies y_1 = y_2\big)\big] \\
\iff &\big[\big(\forall x \forall y_1 \forall y_2 [(xfy_1 \vee xgy_1) \wedge (xfy_2 \vee xgy_2)]\big) \implies y_1 = y_2\big] \\
&\text{Since } f, g \text{ are functions, meaning they are single-rooted and} \\
&\text{it is never the case that } (xfy_1 \wedge xfy_2) \text{ or } (xgy_1 \wedge xgy_2) \text{ is true;} \\
\iff &\big[\big(\forall x \forall y_1 \forall y_2 [(xfy_1 \wedge xgy_2) \vee (xfy_2 \vee xgy_1)]\big) \implies y_1 = y_2\big] \\
\iff &\big[\big(\forall x \forall y_1 \forall y_2 (x \in \text{dom } f \wedge x \in \text{dom } g \wedge [(xfy_1 \wedge xgy_2) \vee (xfy_2 \vee xgy_1)])\big) \implies y_1 = y_2\big] \\
\iff &\big[\big(\forall x \forall y_1 \forall y_2 (x \in \text{dom } f \cap \text{dom } g \wedge [(xfy_1 \wedge xgy_2) \vee (xfy_2 \vee xgy_1)])\big) \implies y_1 = y_2\big] \\
\iff &\big(\forall x (x \in \text{dom } f \cap \text{dom } g \implies [f(x) = g(x)])\big)
\end{aligned}$$

So, $f \cup g$ is a function iff $f(x) = g(x)$ for every x in $(\text{dom } f) \cap (\text{dom } g)$.

Remarks (Big Check 1, 28/12/22): Again, this is unnecessarily convoluted and quite an unreadable chunk of symbols. So, let's redo this too!

Redo of proof:

Assume that f and g are functions so that $f \cup g$ is also a function, and let $x \in (\text{dom } f) \cap (\text{dom } g)$. Then, we see that $\langle x, f(x)\rangle \in f$ and $\langle x, g(x)\rangle \in g$. Consequently, $\langle x, f(x)\rangle$ and $\langle x, g(x)\rangle$ are in $f \cup g$. So, since $f \cup g$ is a function, $f(x) = g(x)$ must hold true.

Conversely, now suppose f and g are functions such that $f(x) = g(x)$ for every x in $(\text{dom } f) \cap (\text{dom } g)$. Clearly, $f \cup g$ can only contain ordered pairs, and is hence, a relation. Now, we need to show that $f \cup g$ is single-valued. Let $\langle x, y_1\rangle$ and $\langle x, y_2\rangle$ be in $f \cup g$. When both ordered pairs belong to f or both belong to g, then $y_1 = y_2$ immediately, as f and g are functions. Consider the case that one belongs in f and the other in g. Accordingly, $f(x) = g(x)$ would mean that $y_1 = y_2$ by our supposition. In any case, we conclude that $y_1 = y_2$. In other words, $f \cup g$ is single-valued, thence it is a function.

Wherefore, $f \cup g$ is a function iff $f(x) = g(x)$ for every x in $(\text{dom } f) \cap (\text{dom } g)$.

Q.E.D. ■

1.2.5 Infinite Cartesian Products

31. ✓ Show that from the first form of the Axiom of Choice we can prove the second form, and conversely:

First Form: For any relation R there is a function $H \subseteq R$ with $\operatorname{dom} H = \operatorname{dom} R$

Second Form: For any set I and function H with domain I, if $H(i) \neq \varnothing$ for all $i \in I$, then $\prod_{i \in I} H(i) \neq \varnothing$.

The First Form Implies The Second:

Assume the first form of the AOC.
Let H be a function with domain I, the relation $R = I \times \bigcup_{i \in I} H(i)$, and $A = \{\langle i, y\rangle \,|\, iRy \wedge y \in H(i)\}$.
If $H(i) \neq \varnothing$ for all $i \in I$, $\operatorname{dom} A = I$.

If it isn't clear enough to the reader; Since $R = \left\{\langle i, y\rangle \,|\, i \in I \wedge y \in \bigcup_{i \in I} H(i)\right\}$,

$$\forall i \exists y \left[i \in I \implies y \in H(i) \subseteq \bigcup_{i \in I} H(i) \right] \iff \forall i \exists y (i \in I \implies [iRy \wedge y \in H(i)])$$

So $\operatorname{dom} A = \{i | \exists y (iAy)\} = \{i | iRy \wedge y \in H(i)\} = I$.

By the first form of the AOC, there exists a function $f \subseteq R$ with $\operatorname{dom} f = \operatorname{dom} A = I$.

Therefore, $\prod_{i \in I} H(i) = \left\{ f \colon I \to \bigcup_{i \in I} H(i) \,\middle|\, (\forall i \in I)[f(i) \in H(i)] \right\} \neq \varnothing$ since it contains at least the function f constructed above.

When $I = \varnothing$, $\bigcup_{i \in \varnothing} H(i) = \varnothing$. $\prod_{i \in I} H(i) = \left\{ \varnothing \colon \varnothing \to \varnothing \,\middle|\, (\forall i \in \varnothing)[f(i) \in H(i)] \right\} = \{\varnothing\} \neq \varnothing$, because $(\forall i \in \varnothing)[f(i) \in H(i)]$ is vacuously true.

The Second Form Implies The First:

Assume the second form of the AOC:

Again, let H be a function with domain I. Define the relation

$E = \left\{ \langle i, y\rangle \in I \times \bigcup_{i \in I} H(i) \,\middle|\, y \in H(i) \right\}$, such that $\operatorname{dom} E = I$. If $E \neq \varnothing$, then $I \neq \varnothing$, and for all $i \in I$, there exists a $y \in H(i)$ (i.e. $H(i) \neq \varnothing$). By the second form of the AOC, there exists a function $f \colon I \to \bigcup_{i \in I} H(i)$ such that for all $i \in I$, $f(i) \in H(i)$. Wherefore, $f \subseteq E$ (as the only difference between them is that f has the extra condition that it must be single-valued) and $\operatorname{dom} f = \operatorname{dom} E = I$.
In the case that $E = \varnothing$, it already is a function. $E \subseteq E$ and $\operatorname{dom} E = \operatorname{dom} E$. Hence, for all relations E, there exists a function f with $\operatorname{dom} f = \operatorname{dom} E$.

The definition of E above is done without loss of generality:

We shall show that it is equivalent to defining a relation $\mathfrak{E} \subseteq X \times Y$ and letting $\operatorname{dom} \mathfrak{E} = I$.
Define H to be the function (with domain I) such that, for all $i \in I$,
$y \in H(i) \iff i\mathfrak{E}y$. Thus, $i\mathfrak{E}y \iff y \in \bigcup_{i\in I} H(i)$ also.
Now,

$$\begin{aligned}
iEy &\iff \langle i, y\rangle \in I \times \bigcup_{i\in I} H(i) \wedge y \in H(i) \\
&\iff \langle i, y\rangle \in \left\{ \langle a, b\rangle \;\middle|\; a \in I \wedge b \in \bigcup_{i\in I} H(i) \wedge b \in H(i) \right\} \\
&\iff \langle i, y\rangle \in \left\{ \langle a, b\rangle \;\middle|\; a \in \operatorname{dom} \mathfrak{E} \wedge a\mathfrak{E}b \right\} \\
&\iff \langle i, y\rangle \in \{\langle a, b\rangle \mid a\mathfrak{E}b\} \\
&\iff i\mathfrak{E}y
\end{aligned}$$

Q.E.D. ■

Remarks (Big Check 1, 29/12/22): In the part for the first form implies the second, we already constructed a specific function f. Hence, we should have used another symbol in $\prod_{i\in I} H(i) = \left\{ f \colon I \to \bigcup_{i\in I} H(i) \;\middle|\; (\forall i \in I)[f(i) \in H(i)] \right\} \neq \varnothing$ instead. The presentation and choice of words has much room for improvement. The first elaboration box is kinda unnecessary, and the explanation there was hard to read. In addition, it could have been carefully woven to flow with the rest of the text instead. Similarly with the second elaboration box, what it was trying to bring across could have been incorporated into the portion above it. However, the general idea is there and it isn't so terrible as a whole that I'm getting a stroke reading it. Hence, I give it a bare ✓.

1.2.6 Equivalence Relations

35. ✓ Show that for any R and x, we have $[x]_R = R[\![\{x\}]\!]$

$$[x]_R = \{t|xRt\} = \{t|(\exists x \in \{x\})xRt\} = \text{ran}(R \upharpoonright \{x\}) = R[\![\{x\}]\!]$$

Q.E.D. ■

37. ✓ Assume that Π is a partition of a set A. Define the relation R_Π as follows:

$$xR_\Pi y \iff (\exists B \in \Pi)(x \in B \wedge y \in B)$$

Show tht R_Π is an equivalence relation on A. (This is a formalised version of the discussion at the beginning of this section.)

R_Π is reflexive (on A):

$$\begin{aligned}(\forall x \in A)(\exists B \in \Pi)(x \in B) &\iff (\forall x \in A)(\exists B \in \Pi)(x \in B \wedge x \in B) \\ &\iff (\forall x \in A)(xR_\Pi x)\end{aligned}$$

R_Π is symmetric:

$$\begin{aligned}xR_\Pi y &\iff (\exists B \in \Pi)(x \in B \wedge y \in B) \\ &\iff (\exists B \in \Pi)(y \in B \wedge x \in B) \\ &\iff yR_\Pi x\end{aligned}$$

R_Π is transitive:

$$(xR_\Pi y \wedge yR_\Pi z) \iff [(\exists B \in \Pi)(x \in B \wedge y \in B) \wedge (\exists C \in \Pi)(y \in C \wedge z \in C)]$$

Since Π is a partition of A, its elements are disjoint, i.e.: Iff $B \neq C$, $B \cap C = \varnothing$. Therefore, in order for $y \in B \wedge y \in C$, $B = C$;

$$\begin{aligned}(xR_\Pi y \wedge yR_\Pi z) &\iff [(\exists B \in \Pi)(x \in B \wedge y \in B) \wedge (\exists B \in \Pi)(y \in B \wedge z \in B)] \\ &\iff (\exists B \in \Pi)[(x \in B \wedge y \in B) \wedge (y \in B \wedge z \in B)] \\ &\iff (\exists B \in \Pi)[(x \in B \wedge y \in B \wedge z \in B)] \\ &\implies (\exists B \in \Pi)[(x \in B \wedge z \in B)] \\ &\implies xR_\Pi z\end{aligned}$$

So, since the relation R_Π on the set A satisfies all 3 properties of reflexivity, symmetry, and transitivity, R_Π is indeed an equivalence relation on A.

Q.E.D. ■

Remarks (Big Check 1, 29/12/22): Yeah should be correct. However, it would again have been nice to have more English words and explanations rather than symbols.

Self-Exercise 1. Let $F\colon A \to B$ and for points in A define

$$x \sim y \quad \text{iff} \quad F(x) = F(y).$$

The relation $\sim$ is an equivalence relation on A. There is a unique one-to-one function $\hat{F}\colon A/\!\sim \to B$ such that $F = \hat{F} \circ \varphi$ (where φ is the natural map as shown in Fig. 13) ($\varphi\colon A \to A/\!\sim$ and $\varphi(x) = [x]_\sim$). [Example from page 58-59].

Prove the existence of the unique $\hat{F}$.

First Edition:

Existance of $\hat{F}$:

By Lemma 3N, for all x, y; $x \sim y$ iff $[x]_\sim = [y]_\sim$. So, $[x]_\sim = [y]_\sim$ iff $F(x) = F(y)$. Wherefore, $F(x) \in \operatorname{ran} F$ iff $[x]_\sim \in A/\!\sim$.

Accordingly, we can define $\hat{F}([x]_\sim) = F(x)$ (for all x). By this definition, $\hat{F}$ is injective:

$$\begin{aligned} \hat{F}([x]_\sim) &= \hat{F}([y]_\sim) \\ F(x) &= F(y) \\ [x]_\sim &= [y]_\sim \end{aligned}$$

Next, $\varphi\colon A \to A/\!\sim$ is surjective (i.e. $\operatorname{ran}\varphi = A/\!\sim$); because for all equivalence classes $[x]_\sim \in A/\!\sim$, $x \in A = \operatorname{dom}\varphi$ such that $\varphi(x) = [x]_\sim$.

For even more details:

$$\begin{aligned} \forall z[z \in A/\!\sim \implies \exists x(x \in A \wedge z = [x]_\sim) &\implies \exists x(\langle x, [x]_\sim\rangle \in \varphi)] \\ \forall x[\langle x, [x]_\sim\rangle \in \varphi &\implies [x]_\sim \in A/\!\sim] \end{aligned}$$

It then follows that $[x]_\sim \in A/\!\sim \iff \langle x, [x]_\sim\rangle \in \varphi$. By definition, $\operatorname{ran}\varphi = A/\!\sim$.

As a result, by Theorem 3H $\operatorname{dom}(\hat{F} \circ \varphi) = \{x \in A \mid \varphi(x) \in A/\!\sim\} = A$ since $\operatorname{ran}\varphi = A/\!\sim$.

Thence, there exists a function $\hat{F}\colon A \to A/\!\sim$ such that $(\hat{F} \circ \varphi)\colon A \to B$ where $F = \hat{F} \circ \varphi$.

Uniqueness of $\hat{F}$:

Assume there exists another injective function $\tilde{G}\colon A/\!\sim \to B$ such that $F = \tilde{G} \circ \varphi$ and $\tilde{G} \neq \hat{F}$. In order for $\tilde{G} \neq \hat{F}$, there are three possible cases:

1. $\operatorname{dom}\tilde{G} \neq \operatorname{dom}\hat{F}$: Then this immediately contradicts our assumption that $\tilde{G}\colon A/\!\sim \to B$. Naturally, this is thus not possible.

2. $\operatorname{ran}\tilde{G} \neq \operatorname{ran}\hat{F}$ ($\hat{F}$ and $\tilde{G}$ are otherwise identical) : Consequently,

$$\begin{aligned} \operatorname{ran}(\tilde{G} \circ \varphi) &= \{t \mid \exists x[x(\tilde{G} \circ \varphi)t]\} \\ &= \{t \mid \exists x \exists y(x\varphi y \wedge y\tilde{G}t)\} \\ &= \{t \in \operatorname{ran}\tilde{G} \mid \varphi(x) \in \operatorname{dom}\tilde{G}\} \\ &= \operatorname{ran}\tilde{G} \neq \operatorname{ran}\hat{F} \end{aligned} \qquad \begin{aligned} F &= \hat{F} \circ \varphi \\ \operatorname{ran} F &= \operatorname{ran}(\hat{F} \circ \varphi) \\ &= \{t \in \operatorname{ran}\hat{F} \mid \varphi(x) \in \operatorname{dom}\hat{F}\} \\ &= \operatorname{ran}\hat{F} \end{aligned}$$

   This implies that $\operatorname{ran}(\tilde{G} \circ \varphi) \neq \operatorname{ran} F$. However, this would mean that $F \neq \tilde{G} \circ \varphi$. By contradiction, this is not possible either.

3. There exists some x such that $\tilde{G}([x]_\sim) \neq F(x)$ ($\hat{F}$ and $\tilde{G}$ are otherwise identical): By Theorem 3H, $\operatorname{dom}(\tilde{G} \circ \varphi) = A$, and for all $x \in A$, $(\tilde{G} \circ \varphi)(x) = G(\tilde{\varphi(x)}) = \tilde{G}([x]_\sim)$. Thus, (for all x)

$$\tilde{G}([x]_\sim) \neq F(x) \iff (\tilde{G} \circ \varphi)(x) \neq F(x)$$

   Simultaneously, by our assumption, $F = \tilde{G} \circ \varphi$. Thus is true iff, for all x, $F(x) = (\tilde{G} \circ \varphi)(x)$. These two statement cannot be true simultaneously. Hence, by contradiction, this case is impossible.

- ☐ All other cases are when multiple of the above situations are true simultaneously. Since we already shown above that none of them are true individually, all other cases described above are false too.
  (Although the above proof that 2. and 3. are false relies on $\operatorname{dom}\tilde{G} \neq \operatorname{dom}\hat{F}$, if that is not true, then from 1. it would already be false.)

As a result, there exists no injective function $\tilde{G}\colon A/\!\sim \to B$ such that $F = \tilde{G} \circ \varphi$ and $\tilde{G} \neq \hat{F}$.

So, the function $\hat{F}$ we have constructed is unique.

Q.E.D. ■

Remarks/AFI:

Existance of $\hat{F}$:

`"we can define` $\hat{F}([x]_\sim) = F(x)$ `(for all` x`)."` We do not actually construct the function $\hat{F}$ here. This is already assuming (without rigorous justification) that a function $\hat{F}$ with such a mapping exists, and hence, creating a circular argument technically. Instead, we construct the set of ordered pairs we use to define what is $\hat{F}$. See ***Revised, Second Edition***. After we construct it rigorously, yes we do indeed find that the claim $\hat{F}([x]_\sim) = F(x)$ is true under that construction. However, we cannot say $\hat{F}([x]_\sim) = F(x)$ without that rigorous construction.

Uniqueness of $\hat{F}$:

Should work fine. However; There's a simpler and more elegant way to do it. Simply assume $\hat{F} \circ \varphi = \tilde{G} \circ \varphi$ and show then show that $\hat{F} = \tilde{G}$! :D

Credit/Thanks to Neverbloom#6760 on the math discord for helping me check my work and give me feedback.

Revised, Second Edition:

Existance of $\hat{F}$: ✓

By Corollary 3C, the set $(A/\!\sim) \times \operatorname{ran} F$ exists. Using a subset axiom, for all sets $(A/\!\sim) \times \operatorname{ran} F$, there exists $\hat{F}\colon A/\!\sim \to B$ where

$$\begin{aligned}\hat{F} &= \{\langle a, b\rangle \mid a \in A/\!\sim \ \wedge\ b \in \operatorname{ran} F \wedge F(a) = b\} \\ &= \{\langle [x]_\sim, F(x)\rangle \mid x \in A\} && \text{as } \operatorname{dom} F = A\end{aligned}$$

This is indeed a function, because it is single-valued:

$$\begin{aligned}[x]_\sim &= [x']_\sim \\ x &\sim x' && \text{by Lemma 3N} \\ F(x) &= F(x') \\ \langle [x]_\sim, F(x)\rangle &= \langle [x']_\sim, f(x')\rangle \\ \hat{F}([x]_\sim) &= \hat{F}([x']_\sim)\end{aligned}$$

By this definition, $\hat{F}$ is injective:

$$\begin{aligned}\hat{F}([x]_\sim) &= \hat{F}([y]_\sim) \\ F(x) &= F(y) \\ x &\sim y \\ [x]_\sim &= [y]_\sim\end{aligned}$$

So, by Theorem 3H; $\operatorname{dom}(\hat{F} \circ \varphi) = \{x \in A \mid \varphi(x) \in A/\!\sim\} = A$. Lastly, by the same theorem, for all $x \in A$, $(\hat{F} \circ \varphi)(x) = \hat{F}(\varphi(x)) = \hat{F}([x]_\sim) = F(x)$.

Thence, there indeed exists an injective function $\hat{F}\colon A/\!\sim \to B$ such that $(\hat{F} \circ \varphi)\colon A \to B$ and $F = \hat{F} \circ \varphi$.

Uniquness of $\hat{F}$:

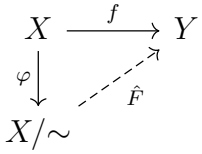
If there exists also an injective function $\tilde{G}\colon A/\!\sim \to B$ such that $(\tilde{G} \circ \varphi)\colon A \to B$ and $F = \tilde{G} \circ \varphi$, then $\hat{F} \circ \varphi = \tilde{G} \circ \varphi$.
Fact 1: For all $y \in A/\!\sim$, there exists an $x \in A$ such that $y = [x]_\sim = \varphi(x)$.

$$\begin{aligned}&&\hat{F} \circ \varphi &= \tilde{G} \circ \varphi \\ \text{For all } x \in A,\quad &&\hat{F}(\varphi(x)) &= \tilde{G}(\varphi(x)) && \text{by Theorem 3H} \\ &&\hat{F}([x]_\sim) &= \tilde{G}([x]_\sim) \\ \text{For all } y \in A/\!\sim,\quad &&\hat{F}(y) &= \tilde{G}(y) && \text{by Fact 1}\end{aligned}$$

Wherefore, $\hat{F} = \{\langle y, \hat{F}(y)\rangle \mid y \in A/\!\sim\} = \{\langle y, \tilde{G}(y)\rangle \mid y \in A/\!\sim\} = \tilde{G}$. Which means that the $\hat{F}$ we have constructed is indeed unique.

Remarks (Big Check 1, 29/12/22): There's an error in the part highlighted in green; it should probably be replaced with $(\exists x \in a)F(x) = b$, because the domain of F is A and *not* $A/\!\sim$. Then, for the reasoning in the next line we just have to add "and $A/\!\sim$ is a partition of A". Otherwise the proof looks good, the presentation is decent, tho not the best.

Self-Exercise 1.1: ✓ The Universal Property of The Quotient Set: If X is a set and $\sim$ an equivalence relation on X, then the natural/canonical projection $\varphi\colon X \to X/\!\sim$ such that $\varphi(x) = [x]_\sim$ can be formed. For any other set Y and function $f\colon X \to Y$ that respects $\sim$, i.e (for all x and x') $x \sim x' \implies f(x) = f(x')$; there exists a unique function $\hat{F}\colon X/\!\sim \to Y$ such that $f = \hat{F} \circ \varphi$:



On the contrary, if f does not respect $\sim$, then there does not exist such a function $\hat{F}\colon X/\!\sim \to Y$ such that $f = \hat{F} \circ \varphi$.

Self-Exercise 1 was a special case of this theorem, where we assumed that $x \sim x'$ iff $f(x) = f(x')$.

Prove the Universal Property of The Quotient Set.

Existance of φ:

By Corollary 3C, the set $X \times (X/\!\sim)$ exists. By the Axiom Schema of Specification, we construct the natural/canonical projection $\varphi\colon X \to X/\!\sim$:
Fact 1: For all $v \in X/\!\sim$, there exists an $x \in X$ such that $v = [x]_\sim$. (By defs.)

$$\begin{aligned} \varphi &= \{\langle u, v\rangle \mid u \in X \land v \in (X/\!\sim) \land v = [u]_\sim\} \\ \varphi &= \{\langle u, [u]_\sim\rangle \mid u \in X\} && \text{By Fact 1} \end{aligned}$$

Existance of $\hat{F}$:

Let $f\colon X \to Y$ be a function that respects $\sim$; By Corollary 3C, the set $(X/\!\sim) \times \operatorname{ran} F$ exists. Using a subset axiom on $(X/\!\sim) \times \operatorname{ran} F$, define the function $\hat{F}\colon X/\!\sim \to Y$ where

$$\begin{aligned} \hat{F} &= \{\langle a, b\rangle \mid a \in X/\!\sim \ \land\ b \in \operatorname{ran} f \land f(a) = b\} \\ &= \{\langle [x]_\sim, f(x)\rangle \mid x \in X\} && \text{as } \operatorname{dom} f = X \end{aligned}$$

This is indeed a function, because it is single-valued:

$$\begin{aligned} [x]_\sim &= [x']_\sim \\ x &\sim x' && \text{by Lemma 3N} \\ f(x) &= f(x') \\ \langle [x]_\sim, f(x)\rangle &= \langle [x']_\sim, f(x')\rangle \\ \hat{F}([x]_\sim) &= \hat{F}([x']_\sim) \end{aligned}$$

So, by Theorem 3H; $\operatorname{dom}(\hat{F} \circ \varphi) = \{x \in X \mid \varphi(x) \in X/\!\sim\} = X$. Lastly, by the same theorem, for all $x \in X$, $(\hat{F} \circ \varphi)(x) = \hat{F}(\varphi(x)) = \hat{F}([x]_\sim) = f(x)$.
Consequently, $f = \{\langle x, f(x)\rangle \mid x \in X\} = \{\langle x, (\hat{F} \circ \varphi)(x)\rangle \mid x \in X\} = (\hat{F} \circ \varphi)$

Thence, there indeed exists a function $\hat{F}\colon X/\!\sim \to B$ such that $(\hat{F} \circ \varphi)\colon X \to B$ and $f = \hat{F} \circ \varphi$.

Uniquness of $\hat{F}$:

If there also exists a function $\tilde{G}\colon X/\!\sim \to B$ such that $(\tilde{G}\circ\varphi)\colon X \to B$ and $f = \tilde{G}\circ\varphi$, then $\hat{F}\circ\varphi = \tilde{G}\circ\varphi$.

$$\begin{aligned} & & \hat{F}\circ\varphi &= \tilde{G}\circ\varphi & \\ \text{For all } x \in X, & & \hat{F}(\varphi(x)) &= \tilde{G}(\varphi(x)) & \text{by Theorem 3H} \\ & & \hat{F}([x]_\sim) &= \tilde{G}([x]_\sim) & \\ \text{For all } v \in X/\!\sim, & & \hat{F}(v) &= \tilde{G}(v) & \text{by Fact 1} \end{aligned}$$

Wherefore, $\hat{F} = \{\langle v, \hat{F}(v)\rangle \mid v \in X/\!\sim\} = \{\langle v, \tilde{G}(v)\rangle \mid v \in X/\!\sim\} = \tilde{G}$. Which means that the $\hat{F}$ we have constructed is indeed unique.

If f does not respect $\sim$, then there does not exist such a $\hat{F}$:

Assume that f does not respect $\sim$ and there still exists such a function $\hat{F}\colon X/\!\sim \to Y$ so that $f = \hat{F}\circ\varphi$. Note again that $f(x) = (\hat{F}\circ\varphi)(x) = \hat{F}(\varphi(x)) = \hat{F}([x]_\sim)$ (Theorem 3H). Then for all x and x' such that $x \sim x'$,

$$\begin{aligned} x &\sim x' & \\ [x]_\sim &= [x']_\sim & \text{by Lemma 3N} \\ \hat{F}([x]_\sim) &= \hat{F}([x']_\sim) & \\ f(x) &= f(x') & \end{aligned}$$

However, this contradicts our assumption that f does not respect $\sim$, i.e. that there exists some x and x' such that $x \sim x'$ and $f(x) \neq f(x')$. So, if f does not respect $\sim$, then there does not exist such a function $\hat{F}$ such that $f = \hat{F}\circ\varphi$.

Remarks (Big Check 1, 29/12/22): Actually since we claimed φ to be a function by writing $\varphi\colon X \to X/\!\sim$, it would have been good to verify that it is indeed a function. However, it is indeed pretty trivial. The part in green is just the same issue as before. Again, other than that the proof looks good, the presentation is decent, tho not the best.

40. ✓ Define an equivalence relation R on the set P of positive integers by

$$mRn \iff m \text{ and } n \text{ have the same number of prime factors.}$$

Is there a function $f\colon P/R \to P/R$ such that $f([n]_R) = [3n]_R$ for each n?

We define the function $F\colon P \to P$ such that $F(n) = 3n$. F is compatible with R. If mRn, then m and n have the same number of (unique) prime factors. Let this number be k. There are two cases to consider.

1. 3 is not a prime factor of m or n. Then $f(m) = 3m$ and $f(n) = 3n$ both have $k+1$ (unique) prime factors. As a result, $f(m)Rf(n)$ is true.
2. 3 is a prime factor of m and n. Then $f(m) = 3m$ and $f(n) = 3n$ have k (unique) prime factors. Hence, $f(m)Rf(n)$ holds again.

Indeed, we see that F is compatible with R.

Wherefore, by Theorem 3Q, the function $f\colon P/R \to P/R$ exists such that $f([n]_R) = [F(n)]_R = [3n]_R$.

41. ✓ Let $\mathbb{R}$ be the set of real numbers and define the relation Q on $\mathbb{R} \times \mathbb{R}$ by $\langle u, v\rangle Q\langle x, y\rangle$ iff $u + y = x + v$.

(a) ✓ Show that Q is an equivalence relation on $\mathbb{R} \times \mathbb{R}$.

(b) ✓ Is there a function $G\colon (\mathbb{R} \times \mathbb{R})/Q \to (\mathbb{R} \times \mathbb{R})/Q$ satisfying the equation

$$G([\langle x, y\rangle]_Q) = [\langle x + 2y, y + 2x\rangle]_Q?$$

(a) Q is Reflexive on $\mathbb{R} \times \mathbb{R}$:

For all $\langle u, v\rangle \in \mathbb{R} \times \mathbb{R}$, $u + v = v + u$ because addition of real numbers is commutative. Consequently, $\langle u, v\rangle Q\langle u, v\rangle$.

Q is Symmetric:

For all $\langle u, v\rangle, \langle x, y\rangle \in \mathbb{R} \times \mathbb{R}$; if $\langle u, v\rangle Q\langle x, y\rangle$, then $u + y = x + v$ is true. Hence, $x + v = u + y$ immediately holds, so does $\langle x, y\rangle Q\langle u, v\rangle$.

Q is Transitive:

For all $\langle u, v\rangle, \langle x, y\rangle, \langle a, b\rangle \in \mathbb{R} \times \mathbb{R}$: If $\langle u, v\rangle Q\langle x, y\rangle$ and $\langle x, y\rangle Q\langle a, b\rangle$ are true, it means that $u + y = x + v$ and $x + b = a + y$. So, by normal arithmetic on real numbers, $u + y = a + y - b + v$ thus $u + b = a + v$, meaning $\langle u, v\rangle Q\langle a, b\rangle$ is true.

Q is an equivalence relation on A since all three properties of an equivalence relation on a set have been proven true.

Remarks (Big Check 1, 29/12/22): $u + v = v + u$ tells us that $\langle u, v\rangle Q\langle v, u\rangle$. Which is not what we wanted. Actually we could simply say that $u + v = u + v$, after which $\langle u, v\rangle Q\langle u, v\rangle$ follows easily. Otherwise, looks good.

(b) Let $f\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ such that $f(\langle x, y\rangle) = \langle x + 2y, y + 2x\rangle$.
$\langle u, v\rangle Q\langle x, y\rangle$ implies

$$\begin{aligned} u + y &= x + v \\ 2v + 2x &= 2y + 2u \\ (u + y) + (2v + 2x) &= (x + v) + (2y + 2u) \\ (u + 2v) + (y + 2x) &= (x + 2y) + (v + 2u) \end{aligned}$$

As a result, $\langle u + 2v, v + 2u\rangle Q\langle x + 2y, y + 2x\rangle$, i.e. $f(\langle u, v\rangle)Qf(\langle x, y\rangle)$. which means that f is indeed compatible with Q.

Now, by Theorem 3Q, there exists a function $G\colon (\mathbb{R}\times\mathbb{R})/Q \to (\mathbb{R}\times\mathbb{R})/Q$ such that $G([\langle x,y\rangle]_Q) = [f(\langle x,y\rangle)]_Q = [\langle x+2y, y+2x\rangle]_Q$.

42. × State precisely the "analogous results" mentioned in Theorem 3Q. (This will require extending the concept of compatibility in a suitable way.)

Assume that R is an equivalence relation on $(A \times A) \times A$. Let the function $F\colon A \times A \to A$ be friendly with R, i.e. (for all $x, y, z, i, j, k \in A$):
$\langle\langle x, y\rangle, z\rangle R\langle\langle i, j\rangle, k\rangle \implies \langle\langle x, y\rangle, F(\langle x, y\rangle)\rangle R\langle\langle i, j\rangle, F(\langle i, j\rangle)\rangle$. Then, there exists a unique function $\hat{F}\colon ((A \times A) \times A)/R \to ((A \times A) \times A)/R$ such that

(★) $$\hat{F}([\langle\langle x, y\rangle, z\rangle]_R) = [\langle\langle x, y\rangle, F(\langle x, y\rangle)\rangle]_R$$

If F is not friendly / is hostile with R, then no such $\hat{F}$ exists.

Existance of $\hat{F}$:

Remarks: Not the most elegant extension of the results of Theorem 3Q by a long shot lol.

One that seems to be much better is as follows:
The analogous results are: Assume that R is an equivalence relation on A and that $F\colon A \times A \to A$. If F is compatible with R, then there exists a unique $\hat{F}\colon A/R \times A/R \to A/R$ such that

$$\hat{F}([x], [y]) = [F\langle x, y\rangle] \quad \text{for all } x \in A.$$

If F is not compatible with R, then no such $\hat{F}$ exists. Of course, we must extend the definition of compatibility. Note that we would like to have the following commutative diagram:

$$\begin{array}{ccc} A \times A & \xrightarrow{F} & A \\ \downarrow & & \downarrow \\ A/R \times A/R & \xrightarrow[\hat{F}]{} & A/R \end{array}$$

From this, we see that if $\langle x, y\rangle$ and $\langle u, v\rangle$ have the same image under $A \times A \to (A/R) \times (A/R)$, that is, $\langle [x], [y]\rangle = \langle [u], [v]\rangle$, then we also like $[F\langle x, y\rangle] = [F\langle u, v\rangle]$.
This suggests that we define that F is compatible with R if for any $x, y, u, v \in R$,

$$xRy \wedge uRv \implies F\langle x, y\rangle RF\langle u, v\rangle.$$

Remarks (Big Check 1, 29/12/22): Yeah is not really a great extension of Theorem 3Q. But hey we learn and bounce onto the next one.

1.2.7 Ordering Relations

43. ✓ Assume that R is a linear ordering on a set A. Show that R^{-1} is also a linear ordering on A.

R^{-1} is A Relation on A:

Since R is a linear ordering on A, $R \subseteq A^2$. As a result, for all z

$$\begin{aligned} z \in R^{-1} = \{\langle y, x\rangle \,|\, xRy\} &\implies \exists x \exists y \left(z = \langle y, x\rangle \in R^{-1}\right) \\ &\implies \langle x, y\rangle \in R \\ &\implies \langle x, y\rangle \in A^2 \end{aligned}$$

Which means that $R^{-1} \subseteq A^2$, and R^{-1} is also a relation on A.

R^{-1} is Transitive:

For all $x, y, z \in A$;

$$\begin{aligned} \left(zR^{-1}y \wedge yR^{-1}x\right) &\iff (xRy \wedge yRz) \\ &\implies xRz \qquad \text{by the transitivity of the linear order } R \\ &\implies zR^{-1}x \end{aligned}$$

R^{-1} Satisfies Trichotomy on A:

For all $x, y \in A$, since R is a linear ordering satisfying trichotomy on A; either xRy, $x = y$, or yRx (but never more than one). Consequently, we now have three cases to consider, that are only true one at a time and never true simultaneously.

i. xRy: Then $yR^{-1}x$.

ii. $x = y$: Then $y = x$.

iii. yRx: Then $xR^{-1}y$.

Therefore, for all $x, y \in A$; precisely one of $yR^{-1}x$, $y = x$, and $xR^{-1}y$ is true. So, R^{-1} satisfies trichotomy on A.

Wherefore, since R^{-1} is a relation on A which is transitive and satisfies trichotomy on A, R^{-1} is a linear ordering on the set A.

Remarks (Big Check 1, 29/12/22): Instead of saying $z \in R^{-1}$, we should just write $\langle y, x\rangle \in R^{-1}$. To be specific, we should conclude the first part by saying R^{-1} is a *binary* relation on A, not just any relation on A. The last part on showing that R^{-1} satisfies trichotomy on A could be more succinct and straight to the point. But ok I get the main arguments which are sound.

44. ✓ Assume that $<$ is a linear ordering on a set A. Assume that $f\colon A \to A$ and that f has the property that whenever $x < y$, then $f(x) < f(y)$. Show that f is one-to-one and that whenever $f(x) < f(y)$, then $x < y$.

f is an injective function:

If $f(x) = f(y)$, then as $x, y \in \operatorname{dom} f = A$ and $<$ satisfies trichotomy on A, one and only one of the following are true:

(i) $x < y$, implying $f(x) < f(y)$.

(ii) $x = y$, implying $f(x) = f(y)$.

(iii) $y < x$, implying $f(y) < f(x)$.

(i) and (iii) are impossible because they contradict our assumption that $f(x) = f(y)$. Hence, $x = y$ is the only possibility.
In other words, for all $x, y \in A$, if $f(x) = f(y)$, then $x = y$. f is now an injective function.

Whenever $f(x) < f(y)$, then $x < y$:

Assume $f(x) < f(y)$. Again, by the same reasons, exactly one of the following hold true;

(I) $x < y$, implying $f(x) < f(y)$.

(II) $x = y$, implying $f(x) = f(y)$.

(III) $y < x$, implying $f(y) < f(x)$.

In this case, (II) and (III) are false since they contradict our assumption that $f(x) < f(y)$. So, (I) where $x < y$ is the only possibility.
Wherefore, if $f(x) < f(y)$, then $x < y$.

In sum, our results for this question are that, for all $x, y \in A$,

1. $x < y$ iff $f(x) < f(y)$
2. $x = y$ iff $f(x) = f(y)$

45. ✓ Assume that $<_A$ and $<_B$ are linear orderings on A and B, respectively.
Define the binary relation $<_L$ on the Cartesian product $A \times B$ by:

$$\langle a_1, b_1\rangle <_L \langle a_2, b_2\rangle \quad \text{iff either} \quad a_1 <_A a_2 \quad \text{or} \quad (a_1 = a_2 \quad \& \quad b_1 <_B b_2)$$

Show that $<_L$ is a linear ordering on $A \times B$. (The relation $<_L$ is called a *lexicographic* ordering, being the ordering used in making dictionaries.)

$<_L$ is a Transitive Relation:

Whenever $\langle a_1, b_1\rangle <_L \langle a_2, b_2\rangle$ and $\langle a_2, b_2\rangle <_L \langle a_3, b_3\rangle$ is true, which is equivalent to $[a_1 <_A a_2 \quad \text{or} \quad (a_1 = a_2 \quad \& \quad b_1 <_B b_2)] \quad \text{and} \quad [a_2 <_A a_3 \quad \text{or} \quad (a_2 = a_3 \quad \& \quad b_2 <_B b_3)]$, there are 4 cases to consider:

1. $a_1 <_A a_2$ and $a_2 <_A a_3$: This implies than $a_1 <_A a_3$ by the transitivity of the linear ordering $<_A$. Therefore, $\langle a_1, b_1\rangle <_L \langle a_3, b_3\rangle$.
2. $a_1 <_A a_2 \quad \text{and} \quad (a_2 = a_3 \quad \& \quad b_2 <_B b_3)$: Then, $a_1 <_A a_3$. So, $\langle a_1, b_1\rangle <_L \langle a_3, b_3\rangle$.
3. $(a_1 = a_2 \quad \& \quad b_1 <_B b_2) \quad \text{and} \quad a_2 <_A a_3$: Again, $a_1 <_A a_3$. Hence, $\langle a_1, b_1\rangle <_L \langle a_3, b_3\rangle$.
4. $(a_1 = a_2 \quad \& \quad b_1 <_B b_2) \quad \text{and} \quad (a_2 = a_3 \quad \& \quad b_2 <_B b_3)$: Now, $(a_1 = a_3 \quad \& \quad b_1 <_B b_3)$ by the transitivity of the linear ordering $<_B$. Accordingly, $\langle a_1, b_1\rangle <_L \langle a_3, b_3\rangle$.

Consequently, we see that if $\langle a_1, b_1\rangle <_L \langle a_2, b_2\rangle$ and $\langle a_2, b_2\rangle <_L \langle a_3, b_3\rangle$ is true, then $\langle a_1, b_1\rangle <_L \langle a_3, b_3\rangle$ is true. In other words, $<_L$ is transitive.

$<_L$ satifies trichotomy on A:

For all $\langle a_1, b_1\rangle$ and $\langle a_2, b_2\rangle$ in the Cartesian product $A \times B$, there are 4 cases worth considering:

(I) $a_1 = a_2$ and $b_1 = b_2$: Then, by definition, $\langle a_1, b_1\rangle = \langle a_2, b_2\rangle$.

(II) $a_1 <_A a_2$ (whether $b_1 = b_2$, $b_1 <_B b_2$, or $b_2 <_B b_1$ is inconsequential): Immediately, $\langle a_1, b_1\rangle <_L \langle a_2, b_2\rangle$ is true.

(III) $a_1 = a_2$ and $b_1 <_B b_2$. Thus, $\langle a_1, b_1\rangle <_L \langle a_2, b_2\rangle$ again.

(IV) $a_2 <_A a_1$ (whether $b_1 = b_2$, $b_1 <_B b_2$, or $b_2 <_B b_1$ is inconsequential): It follows that $\langle a_2, b_2\rangle <_L \langle a_1, b_1\rangle$.

(V) $a_1 = a_2$ and $b_2 <_B b_1$. Similarly, we have $\langle a_2, b_2\rangle <_L \langle a_1, b_1\rangle$.

Wherefore, for all $\chi_1, \chi_2 \in A \times B$, one and only one of $\chi_1 = \chi_2$, $\chi_1 <_L \chi_2$, and $\chi_2 <_L \chi_1$ is true. i.e. $<_L$ satisfies trichotomy on A.

So, we conclude that $<_L$ is a linear ordering on the Cartesian product $A \times B$ — since the binary relation $<_L$ on $A \times B$ satisfies transitivity, and trichotomy on A.

1.2.8 Review Exercises

49. ✓ Find as many equivalence relations as you can on the set $\{0, 1, 2\}$.

- $\{\langle 0,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle\}$.
- $\{\langle 1,1\rangle, \langle 2,2\rangle, \langle 1,2\rangle, \langle 2,1\rangle, \langle 0,0\rangle\}$.
- $\{\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 1,1\rangle, \langle 2,2\rangle\}$.
- $\{\langle 0,0\rangle, \langle 0,2\rangle, \langle 2,0\rangle, \langle 2,2\rangle, \langle 1,1\rangle\}$.
- $\{\langle 0,0\rangle, \langle 0,1\rangle, \langle 1,0\rangle, \langle 1,1\rangle, \langle 0,2\rangle, \langle 2,0\rangle, \langle 2,2\rangle, \langle 1,2\rangle, \langle 2,1\rangle\}$.

52. ✓ Suppose that $A \times B = C \times D$. Under what conditions can we conclude that $A = C$ and $B = D$?

It must be that the sets A, B, C, D are nonempty.

Self-Exercise 2: × Prove that if the sets A, B, C, D are nonempty, and $A \times B = C \times D$; then $A = C$ and $B = D$.

Assume that $A \neq C$ or $B \neq D$, consider the following two cases. Then, there is some element that belongs in A but not in C, or in C but not in A. Now, suppose, without loss of generality, that exists $x \in A$ such that $x \notin C$. For this x and all $b \in B$, $\langle x, b\rangle \in A \times B$ by Lemma 3B but $\langle x, b\rangle \notin C \times D$ (See Details). However, this means $A \times B \neq C \times D$, contradicting our prior assumption that $A \times B = C \times D$. The same argument holds for $B \neq D$ as well. Therefore, $A \times B = C \times D$ must imply $A = C$ and $B = D$.

See Details:
By Lemma 3B

$$\begin{aligned}\forall x \forall y (x, y \in A \cup B \implies \langle x, y\rangle \in \mathscr{P}\mathscr{P}C) &\iff \forall x \forall y \big([(x \in A \vee x \in B) \wedge (y \in A \vee y \in B)] \\ &\qquad \implies \langle x, y\rangle \in \mathscr{P}\mathscr{P}C\big) \\ &\implies \forall x \forall y \big((x \in A \wedge y \in B) \implies \langle x, y\rangle \in \mathscr{P}\mathscr{P}C\big) \\ &\implies \forall x \forall y \big((x \in A \wedge y \in B) \implies \langle x, y\rangle \in A \times B\big)\end{aligned}$$

So, for the aforementioned x, indeed $\langle x, b\rangle \in A \times B$ for all $b \in B$.

While for Corollary 3C, since for this choice of x, it is not in C, thus $\langle x, b\rangle \notin C \times D$, even if $b \in D$.

Remarks (Big Check 1, 29/12/22): The presentation and phrasing of this has much room for improvement. Also, we can actually do a simple direct proof over here by showing that $A \subseteq C$ and $B \subseteq D$, then show $C \subseteq A$ and $D \subseteq B$ thereafter using the same procedure. Good try tho :D

58. ✓ Give an example to show that $F[\![F^{-1}[\![S]\!]]\!]$ is not always the same as S.

Let the function $F\colon \mathbb{R} \to \mathbb{R}_0^+$ such that, for all $x \in \mathbb{R}$, $F(x) = x^2$. Then, $F[\![F^{-1}[\![\mathbb{R}^-]\!]]\!] = \varnothing \neq \mathbb{R}^-$.

Self-Exercise 3.

i. × Prove that $S = F[\![F^{-1}[\![S]\!]]\!]$ iff $S \subseteq \operatorname{ran} F$.

ii. ✓ Prove that $S = F^{-1}[\![F[\![S]\!]]\!]$ iff $S \subseteq \operatorname{dom} F$.

i. First, notice the identity $F[\![F^{-1}[\![S]\!]]\!] = S \cap \operatorname{ran} F$

$$\begin{aligned} F[\![F^{-1}[\![S]\!]]\!] &= F[\![\{x \mid (\exists y \in S) y F^{-1} x\}]\!] \\ &= F[\![\{x \mid (\exists y \in S) x F y\}]\!] \\ &= \{y \mid y \in S \wedge x F y\} \\ &= \{y \in S \mid x F y\} \\ &= S \cap \operatorname{ran} F \end{aligned}$$

($\Longleftarrow$) Now, if $S \subseteq \operatorname{ran} F$, then $F[\![F^{-1}[\![S]\!]]\!] = F[\![\{x \mid (\exists y \in S) y F^{-1} x\}]\!] = S \cap \operatorname{ran} F = S$.

($\Longrightarrow$) Conversely, assume $S = F[\![F^{-1}[\![S]\!]]\!] = S \cap \operatorname{ran} F$. Consequently;

$$\forall y[(y \in S \wedge y \in \operatorname{ran} F) \iff y \in S] \implies \forall y[y \in S \implies y \in \operatorname{ran} F]$$

$S \subseteq \operatorname{ran} F$ as we wanted.

Thence, $S = F[\![F^{-1}[\![S]\!]]\!]$ iff $S \subseteq \operatorname{ran} F$.

ii. Let $F = G^{-1}$; now by part i. $S = G^{-1}\left[\!\left[\left(G^{-1}\right)^{-1}[\![S]\!]\right]\!\right]$ iff $S \subseteq \operatorname{ran} G^{-1}$. With Theorem 3E, we know that $G^{-1}\left[\!\left[\left(G^{-1}\right)^{-1}[\![S]\!]\right]\!\right] = G^{-1}[\![G[\![S]\!]]\!]$ and $\operatorname{ran} G^{-1} = \operatorname{dom} G$. By combining our results, $S = G^{-1}[\![G[\![S]\!]]\!]$ iff $S = \operatorname{dom} G$. Since G^{-1} and F were both chosen arbitrarily, so the statement is proven.

Remarks (Big Check 1, 29/12/22): The presentation here, especially for part i. is frankly terrible. Its hard to read and understand, obfuscated by a wall of symbols that at one point didn't even transition properly. Namely, it isn't clearly shown how we got from $F[\![\{x \mid (\exists y \in S) x F y\}]\!]$ to $\{y \mid y \in S \wedge x F y\}$. While the proof to part ii. is indeed better, its presentation still has lots of room for improvement.

1.3 Natural Numbers

1.3.1 Inductive Sets

Self-Proof of Theorem 4C: Prove Theorem 4C. ✓

0 Is Not The Successor of Any Natural Number:
(This part is not needed in the proof but just put it here for fun)

For all sets a, a is either empty or nonempty. So we have two cases to consider:

1. $a = \varnothing$. This implies that $a \cup \{a\} = \varnothing \cup \{\varnothing\} = \{\varnothing\} \neq \varnothing$.
2. $a \neq \varnothing$. Thus, there exists a set x such that $x \in a$. Thus $x \in a \cup \{a\}$ too. Which means $a \cup \{a\} \neq \varnothing$.

Consequently, there does not exist any set such that its successor is $\varnothing$, much less a natural number.

Remarks (Big Check 1, 28/12/22): Actually we can just consider an arbitrary set x, because then we know $\{x\}$ contains x and is hence nonempty. Consequently, this must mean that x^+ is nonempty. There's no need to split it casewise into $x = \varnothing$ and $x \neq \varnothing$.

Every Nonzero Natural Number is The Successor of Some Natural Number:

Now, we construct the inductive set ω' of natural numbers such that every nonzero natural number in ω' is the successor of some natural number, i.e.:

$$\forall x \Big(x \in \omega' \iff \big(x \in \omega \wedge (\exists y (y \in \omega \wedge y^+ = x) \vee x = \varnothing) \big) \Big)$$

By definition, $\varnothing \in \omega'$. Notice that for all x, $x \in \omega'$ implies $x^+ \in \omega'$:

$$x \in \omega' \implies x \in \omega \implies \big(x \in \omega \wedge x^+ \in \omega \big) \implies x^+ \in \omega'$$

As a result, ω' is an inductive subset of ω. Thence by the Induction Principle for ω; $\omega' = \omega$.

Wherefore, indeed every nonzero natural number is the successor of some natural number.

Remarks (Big Check 1, 29/12/22): There's no need to apply the Axiom Schema of Specification *that* explicitly. Using set builder notation is just as rigorous in this context. In fact, set builder notation is much more clear, concise, and straight to the point.

1. ✓ Show that $1 \neq 3$, i.e., that $\varnothing^+ = \varnothing^{+++}$.

We know that $1 = \varnothing^+ = \{\varnothing\}$ while $3 = \varnothing^{+++} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$. Hence, since there exists sets in 1 that are not in 3 — namely $\{\varnothing\}$ and $\{\varnothing, \{\varnothing\}\}$ — they are not equal.
(Because it is false that for all n, $n \in 1$ iff $n \in 3$.)

Remarks (Big Check 1, 29/12/22): This is quite the simple question but my answer here has much to be improved upon. Namely, for a question of such simplicity, it'll probably be good to add a bit more detail on the calculation of what the set 3 is, though its rather trivial. More importantly is the phrasing of the explanation, it should be clearly and more straight to the point.

1.3.2 Peano's Postulates

Self-Exercise 4: Prove that all inductive sets are infinite. ✓

Assume that there exists a finite inductive set A, i.e. it contains only n elements for some natural number n. Let the set x be in A.

Then: $x, x^+, x^{++}, \ldots, x^{\overbrace{+\cdots+}^{n \text{ times}}} \in A$. This means that there are (at least) $n+1$ elements in A. However, this contradicts with the fact that A contains only n elements. So, there does not exist some natural number n and inductive set A; such that we can say an A contains only n elements. Wherefore, all inductive sets are finite.

I think we may need to do the cardinality chapter first in order to create a proof that is fully satisfactory, both intuitively and rigorously; since the terms "finite", "infinite", and "cardinality" are defined there.

Remarks (Big Check 1, 29/12/22): Like what I said in my remarks after writing the above proof, I wasn't really satisfied with it. Mainly because of the handwavy notation used: $x^{\overbrace{+\cdots+}^{n \text{ times}}} \in A$. I think I now have an idea of how to rigorously prove this.

Redo of Proof:

Let S be an inductive set and x be. Oh wait wait wait. There's a simple and easy way to go about this proof that I just realised lmao.

Redo of Proof, V1.1:

Let S be an inductive set. By Theorem 4B, ω is a subset of every inductive set. Hence, let the identity function $I_\omega : \omega \to S$ so that $I_\omega(n) = n$. Clearly, I_ω must be injective; let $f(n) = f(n')$, then immediately, $n = n'$ by definition (since $f(n) = n$ and $f(n') = n'$). Wherefore, we know that $\operatorname{card} \omega \leq \operatorname{card} S$, and S must be infinite.

**Note: I'm doing this after Chapter 5 on the construction of the reals. So, I think this should correspond rigorously but I didn't quote any theorems here (since I haven't learnt them yet).*

Self-Proof of Theorem 4D: ✓

ω is inductive and hence closed under the successor operation. Which means that $\sigma : \omega \to \omega$.

(i) σ is a function:

Let $n_1 = n_2 \in \omega$. Then, $\sigma(n_1) = \sigma(n_2)$:

$$\begin{aligned} k \in \sigma(n_1) &\iff k \in n_1^+ \\ &\iff k \in n_1 \cup \{n_1\} \\ &\iff k \in n_1 \vee k = n_1 \\ &\iff k \in n_2 \vee k = n_2 \\ &\iff k \in n_2 \cup \{n_2\} \\ &\iff k \in n_2^+ \\ &\iff k \in \sigma(n_2) \end{aligned}$$

(ii) $0 \notin \operatorname{ran} \sigma$:

For all sets n, n is either empty or nonempty. So we have two cases to consider:

(a) $n = \varnothing$. This implies that $n \cup \{n\} = \varnothing \cup \{\varnothing\} = \{\varnothing\} \neq \varnothing$.

(b) $n \neq \varnothing$. Thus, there exists a set x such that $x \in n$. Thus $x \in n \cup \{n\}$ too. Which means $n \cup \{n\} \neq \varnothing$.

Consequently, there exists no set n such that $n^+ = \varnothing$, much less for $n \in \omega$.

(iii) σ is injective:

~~Assume there exists some $n, m \in \omega$ so that $n^+ = m^+$. Then, $n \cup \{n\} = m \cup \{m\}$. Which means that $n \in m$ or $n = m$. And $m \in n$ or $m = n$.~~
Ah yes, why couldn't I prove this after a couple hours? Because I needed the theorem from the next page. ***P a i n***. Giving some credit to myself, I did think of using the big union to arrive at Enderton's answer, however, I didn't delve that deep in it to derive all the theorems that allow me to rigorously state that. But, if I were to continue the above proof with usage of the Axioms Enderton has not covered, i.e. the Axiom of Regularity and the Axiom of Replacement, I probably could have arrived at a rigorous proof.

To quote Enderton; "We can now complete the proof of Theorem 4D; it remained for us to show that the successor operation on ω is one-to-one. If $m^+ = n^+$ for m and n in ω, then $\bigcup(m^+) = \bigcup(n^+)$. But since m and n are transitive sets, we have $\bigcup(m^+) = m$ and $\bigcup(n^+) = n$ by Theorem 4E. Hence $m = n$. "

(iv) By definition, any subset A of ω containing $\varnothing$ and which is closed under the successor operation is an inductive set. Therefore, by the Induction Principle for ω, $A = \omega$

Wherefore, since all 3 conditions are met, $\langle \omega, \sigma, 0 \rangle$ is indeed a Peano system.

Remarks (Big Check 1, 30/12/22): For the proof that σ is a function, there's no need to go such a lengthy route. We can simply say that $\sigma(n_1) = n_1^+ = n_1 \cup \{n_1\}$. And hence, by our assumption that $n_1 = n_2$, that is the same as $n_2 \cup \{n_2\} = n_2^+ = \sigma(n_2)$. While for the part on showing $0 \notin \operatorname{ran} \sigma$, its the same thing as in our Self-Proof of Theorem 4C; we have no need to split it casewise. And actually, we can simply quote Theorem 4C or our self-proof of it.

Self-Proof of Theorem 4F: ✓

Let the subset T of ω contain all transitive natural numbers, i.e.

$$T = \{n \in \omega \,|\, \forall k \forall m (k \in m \in n \implies k \in n)\}$$

Vacuously, $\varnothing \in T$. Now, for all n, if $n \in T$ then $n^+ \in T$:

$$\begin{aligned} n^+ = n \cup \{n\} &\implies \forall k \forall m \big[k \in m \in n^+ \iff (k \in m \in n \vee k \in m = n)\big] \\ &\implies \forall k \forall m \big[k \in m \in n^+ \implies k \in n \subseteq n^+\big] \\ &\implies \forall k \forall m \big[k \in m \in n^+ \implies k \in n^+\big] \end{aligned}$$

Therefore, the natural number n^+ is also transitive and hence in T.

Consequently, we know that the subset T of ω is an inductive set. By the Induction Principle for ω, $T = \omega$.

Wherefore, all natural numbers are transitive.

Remarks (Big Check 1, 30/12/22): Seems ok. However, the presentation for the inductive step could have been done much better. Instead of using only symbols, which makes the proof harder to parse, writing that down in words will probably have made it easier to understand and a significantly more enjoyable read.

s Self-Proof of Theorem 4G: ✓

Let the subset T of ω be as follows:

$$T = \{n \in \omega \,|\, \forall k (k \in n \implies k \in \omega)\}$$

Vacuously, $\varnothing \in T$. For all n, if $n \in T$, then $n^+ \in T$; because for all k:

$$\begin{aligned} k \in n^+ &\iff (k \in n \vee k = n) \\ &\implies k \in \omega \end{aligned}$$

Therefore, $n^+ \in T$. So, T is an inductive set. By the Induction Principle for ω, $T = \omega$ as desired. Which means that ω is indeed a transitive set — since for all k and n, $k \in n \in \omega$ implies $k \in \omega$.

Remarks (Big Check 1, 30/12/22): Yeah the general arguments are alright. The only thing is, again, that it would be better if more English was used over lines of symbols

2. ✓ Show that if a is a transitive set, then a^+ is also a transitive set.

For all a, if a is a transitive set, then for all sets b and c;

$$\begin{aligned} c \in b \in a^+ &\implies c \in b \in a \vee c \in b = a \\ &\implies c \in a \subseteq a^+ \\ &\implies c \in a^+ \end{aligned}$$

Therefore, a^+ is also a transitive set.

Remarks (Big Check 1, 30/12/22): Again, try to use more English over lines of symbols.

3.

(a) ✓ Show that if a is a transitive set, then $\mathscr{P}a$ is also a transitive set.

(b) ✓ Show that if $\mathscr{P}a$ is a transitive set, then a is also a transitive set.

(a) Assume a is a transitive set:

$$\begin{aligned} c \in b \in \mathscr{P}a &\implies c \in b \subseteq a \\ &\implies c \in a \\ &\implies c \subseteq a \qquad \text{by the assumption} \\ &\implies c \in \mathscr{P}a \end{aligned}$$

Therefore, $\mathscr{P}a$ is a transitive set.

(b) Conversely, now suppose $\mathscr{P}a$ is a transitive set:

$$\begin{aligned} (d \in c \in b \in \mathscr{P}a \implies d \in c \in \mathscr{P}a) &\implies (d \in c \in b \subseteq a \implies d \in c \subseteq a) \\ &\implies (d \in c \in a \implies d \in a) \end{aligned}$$

So, a is a transitive set.

Remarks (Big Check 1, 30/12/22): Again, more use of English over symbols would be good.

4. ✓ Show that if a is a transitive set, then $\bigcup a$ is also a transitive set.

Assume a is a transitive set:

$$\begin{aligned} c \in b \in \bigcup a &\implies \exists u(c \in b \in u \in a) \\ &\implies c \in b \in a \\ &\implies c \in \bigcup a \end{aligned}$$

Thus, we see that $\bigcup a$ is a transitive set indeed.

5. Assume that every member of $\mathscr{A}$ is a transitive set.

(a) ✓ Show that $\bigcup \mathscr{A}$ is a transitive set.

(b) ✓ Show that $\bigcap \mathscr{A}$ is a transitive set (assuming that $\mathscr{A}$ is nonempty).

(a)

$$\begin{aligned} c \in b \in \bigcup \mathscr{A} &\implies \exists a(c \in b \in a \in \mathscr{A}) \\ &\implies \exists a(c \in a \in A) \\ &\implies c \in \bigcup \mathscr{A} \end{aligned}$$

By definition, $\bigcup \mathscr{A}$ is a transitive set.

(b)

$$\begin{aligned} c \in b \in \bigcap \mathscr{A} &\implies \forall a(c \in b \in a \in \mathscr{A}) \\ &\implies \forall a(c \in a \in \mathscr{A}) \\ &\implies c \in \bigcap \mathscr{A} \end{aligned}$$

Indeed, we have that $\bigcap \mathscr{A}$ is a transitive set (assuming that $\mathscr{A}$ is nonempty).

6. ✓ Prove the converse to Theorem 4E: If $\bigcup(a^+) = a$, then a is a transitive set.

$$\begin{aligned}
\bigcup(a^+) &= a \\
\bigcup(a \cup \{a\}) &= a \\
\left(\bigcup a\right) \cup \left(\bigcup\{a\}\right) &= a \quad \text{by Exercise 21 of Chapter 2} \\
\left(\bigcup a\right) \cup a &= a
\end{aligned}$$

Hence, by extensionality:

$$\begin{aligned}
\forall x \left[x \in \left(\bigcup a\right) \cup a \iff x \in a\right] &\iff \forall x\big([\exists y(x \in y \in a) \vee x \in a] \iff x \in a\big) \\
&\implies \forall x\big([\exists y(x \in y \in a) \vee x \in a] \implies x \in a\big) \\
&\implies \forall x\big(\exists y(x \in y \in a) \implies x \in a\big) \\
&\implies \forall x\big(\forall y \neg(x \in y \in a) \vee x \in a\big) \\
&\implies \forall x \forall y\big(\neg(x \in y \in a) \vee x \in a\big) \\
&\implies \forall x \forall y\big(x \in y \in a \implies x \in a\big)
\end{aligned}$$

Wherefore, it should be clear that a is indeed a transitive set!
(Oh boi was that quite a few lines of elementary logic lol)

Remarks (Big Check 1, 30/12/22): There is an over reliance on symbols instead of English words here once more. Especially for the part after "Hence, by extensionality:", it was not a smooth read. Also, the transition from $\forall x\big([\exists y(x \in y \in a) \vee x \in a] \implies x \in a\big)$ to $\forall x\big(\exists y(x \in y \in a) \implies x \in a\big)$ was not really clear, rigorously speaking. (even though it makes sense 'intuitively')

1.3.3 Recursion On ω

7. ✓ Complete part 4 of the proof of the recursion theorem on ω.

Let S be the set on which h_1 and h_2 agree:

$$S = \{n \in \omega \,|\, h_1(n) = h_2(n)\}.$$

Where both functions $h_1 : \omega \to A$ and $h_2 : \omega \to A$ are such that $h_1(0) = h_2(0) = a$, and for all $n \in \omega$, $h_1(n^+) = F(h_1(n))$ as well as $h_2(n^+) = F(h_2(n))$. So, $\varnothing \in S$. Now, if $n \in S$, then $h_1(n) = h_2(n)$. Consequently, $h_1(n^+) = F(h_1(n)) = F(h_2(n)) = h_2(n^+)$. Which also means $n^+ \in S$. By definition, S is an inductive subset of ω. As a result, by the Induction Principle on ω, $S = \omega$. Hence, we conclude that the functions are identical:
$h_1 = \{\langle n, h_1(n)\rangle \,|\, n \in \omega\} = \{\langle n, h_2(n)\rangle \,|\, n \in \omega\} = h_2$.

Self-Proof of Theorem 4H: ✓

By the Recursion Theorem on ω, there exists a (unique) function $h : \omega \to N$ such that

1. $h(0) = e$
2. $h(n^+) = h(\sigma(n)) = S(h(n))$

h is injective:

Let set $T = \{n \in \omega \,|\, \forall k(h(n) = h(k) \implies n = k)\}$. In order for $h(n) = e$, either $n = 0$ or $n \neq 0$. Now, by condition (i) of Peano systems, $e \notin \operatorname{ran} S$. By Theorem 4C, for any natural $n \neq 0$, there exists another natural k with $k^+ = n$. For such nonzero n, $h(n) = h(k^+) = h(\sigma(k)) = S(h(k)) \neq e$. Thus, the only possibility for $h(n) = e$ is $n = 0$. So, $h(n) = h(k) = e$ implies $n = k = 0$. Which means $0 \in T$. If $n \in T$, then $n^+ \in T$ as seen in the following: First, notice that by Theorem 4D, $n^+ \neq 0$. So, $h(n^+) \neq e$:

$$\begin{aligned}
h(n^+) &= h(m) && \text{where } m \neq 0 \text{ since } h(m) \neq e \\
h(n^+) &= h(k^+) && \text{by Theorem 4C, where } k^+ = m \\
h(\sigma(n)) &= h(\sigma(k)) \\
S(h(n)) &= S(h(k)) \\
h(n) &= h(k) && \text{by condition (ii) of Peano systems} \\
n &= k && \text{by assumption} \\
n^+ &= k^+ = m
\end{aligned}$$

Hence, we see that $n^+ \in T$ whenever $n \in T$, as desired. By definition, this set T is now inductive. Consequently, by the Induction Principle for ω, $T = \omega$. i.e. $\forall n \forall k(h(n) = h(k) \implies n = k)$; h is an injective function.

h is surjective:

Notice that $\operatorname{ran} h \subseteq N$ and $h(0) = e \in \operatorname{ran} h$, by definition. If $n \in \operatorname{ran} h$, then there exists $k \in \omega$ so that $n = h(k)$. Then, $S(n) = S(h(k)) = h(\sigma(k)) \in \operatorname{ran} h$. So, $\operatorname{ran} h$ is closed under S. i.e. the subset $\operatorname{ran} h$ of N contains e and is closed under S. By condition (iii) of Peano systems, $\operatorname{ran} h = N$. Which means that h is indeed surjective.

We can now conclude that; Wherefore, there is a bijective function $h : \omega \to N$ in a way that preserves the successor operation

$$h(\sigma(n)) = S(h(n))$$

and the zero element

$$h(0) = e \qquad !\ :D$$

Q.E.D. ■

■ — refers to the part(s) I edited or added after reviewing my work, in order to improve it. **Note:* This was done before big check 1

9. ✓ Let f be a function from B into B, and assume that $A \subseteq B$. We have two possible methods for constructing the "closure[1]" C of A under f. First define C^* to be the intersection of the closed supersets of A:

$$C^* = \bigcap \{X \mid A \subseteq X \subseteq B \wedge f[\![X]\!] \subseteq X\}.$$

Alternatively, we could apply the recursion theorem to obtain the function h for which

$$\begin{aligned} h(0) &= A \\ h\big(n^+\big) &= h(n) \cup f[\![h(n)]\!]. \end{aligned}$$

Clearly, $h(0) \subseteq h(1) \subseteq \cdots$; define C_* to be $\bigcup \operatorname{ran} h$; in other words

$$C_* = \bigcup_{i \in \omega} h(i).$$

Show that $C^* = C_*$. [Suggestion: To show that $C^* \subseteq C_*$, show that $f[\![C_*]\!] \subseteq C_*$. To show that $C_* \subseteq C^*$, use induction to show that $h(n) \subseteq C^*$.]

Proof:

□ $C^* \subseteq C_*$

1. $A \subseteq C_* \subseteq B$:
   i. $\underline{A \subseteq C_*}$

$$\begin{aligned} x \in A &\implies (0 \in \omega \wedge x \in h(0) = A) \\ &\implies x \in \bigcup_{i \in \omega} h(i) \end{aligned}$$

   ii. $\underline{C_* \subseteq B}$

$$\begin{aligned} x \in \bigcup_{i \in \omega} h(i) &\iff \exists i (i \in \omega \wedge x \in h(i) \subseteq B) \\ &\implies x \in B \end{aligned}$$

   Thus, we know $A \subseteq C_* \subseteq B$.

2. $f[\![C_*]\!] \subseteq C_*$:

$$\begin{aligned} y \in f[\![C_*]\!] &\iff \exists x \left(x \in \bigcup_{i \in \omega} h(i) \wedge \langle x, y \rangle \in f \right) \\ &\iff \exists i \exists x (i \in \omega \wedge x \in h(i) \wedge \langle x, y \rangle \in f) \\ &\implies \exists i \left[i \in \omega \wedge y \in h\big(i^+\big) \right] && \text{by the construction of } h \\ &\implies y \in C_* \end{aligned}$$

   Now, it follows that

$$\begin{aligned} x \in C^* &\iff x \in \bigcap \{X \mid A \subseteq X \subseteq B \wedge f[\![X]\!] \subseteq X\} \\ &\iff \forall X \left[(A \subseteq X \subseteq B \wedge f[\![X]\!] \subseteq X) \implies x \in X \right] \\ &\implies x \in C_* && \text{as } A \subseteq C_* \subseteq B \text{ and } f[\![C_*]\!] \subseteq C_* \end{aligned}$$

   Which means, we successfully shown that $C^* \subseteq C_*$. We need only show $C_* \subseteq C^*$ after this.

□ $C_* \subseteq C^*$
Let the set $S = \{i \in \omega \mid h(i) \subseteq C^*\}$,

1. $0 \in S$:

$$\begin{aligned} x \in h(0) &\implies \forall X(A \subseteq X \implies x \in X) \\ &\implies \forall X\left[(A \subseteq X \subseteq B \wedge f[\![X]\!] \subseteq X) \implies x \in X\right] \\ &\implies x \in C^* \end{aligned}$$

   As $h(0) \subseteq C^*$, accordingly $0 \in S$.

2. If $i \in S$, then $i^+ \in S$:

   We first prove a small result

$$\begin{aligned} h(i) \subseteq C^* &\implies \forall X\big((A \subseteq X \subseteq B \wedge f[\![X]\!] \subseteq X) \implies [h(i) \subseteq X]\big) \\ &\implies \forall X\big((A \subseteq X \subseteq B \wedge f[\![X]\!] \subseteq X) \implies [f[\![h(i)]\!] \subseteq X]\big) \\ &\implies f[\![h(i)]\!] \subseteq C^* \end{aligned}$$

   As a result, the following holds true

$$\begin{aligned} y \in h\big(i^+\big) &\iff y \in h(i) \cup f[\![h(i)]\!] \\ &\iff y \in h(i) \vee y \in f[\![h(i)]\!] \\ &\implies y \in C^* \qquad\qquad \text{since } i \in S \text{ and } f[\![h(i)]\!] \subseteq C^* \end{aligned}$$

   Therefore, the subset S of ω is inductive, by definition. By the Induction Principle for ω, $S = \omega$. Consequently,

$$\begin{aligned} y \in C_* &\iff \exists i[i \in \omega \wedge y \in h(i)] \\ &\implies y \in C^* \end{aligned}$$

   Thence, $C_* \subseteq C^*$. Wherefore, since $C^* \subseteq C_*$ and $C_* \subseteq C^*$, so $C^* = C_*$ easily follows.

Remarks (Big Check 1, 30/12/22): Yeah it looks okay. Its just that, as usual, it'll be good if the explanations were done moreso in English than symbols.

[1] Wait, what even is the closure? The closure C of A under f is the smallest subset C of B so that $A \subseteq C$ and C is closed under f. L.A. e.g.: Let B be a vector space, A be a subset of B. Then, the closure C of A under $+$ and $\cdot$ would be what we call span A, which is a superset of A and a subset of B.

10. ✓ In Exercise 9, assume that B is the set of real numbers, $f(x) = x^2$, and A is the closed interval $\left[\frac{1}{2}, 1\right]$. What is the set called C^* and C_*?

The set C^* and C_* are $(0, 1]$.

11. ✓ In Exercise 9, assume that B is the set of real numbers, $f(x) = x - 1$, and $A = \{0\}$. What is the set called C^* and C_*?

The set C^* and C_* are the set of negative integers including 0, i.e. $\mathbb{Z}_0^-$.

Self-Exercise 5: Let the sets I, A and B be so that $A \subseteq B$, the function $f\colon \prod_{i\in I} B \to B$. We define the "$I$ product closure" C of A under f as follows:

$$C^* = \bigcap \left\{ X \;\middle|\; A \subseteq X \subseteq B \wedge f\left[\!\left[\prod_{i\in I} X\right]\!\right] \subseteq X \right\}$$

Alternatively, apply the recursion theorem to obtain the function $h\colon \omega \to \mathscr{P}B$ with

$$\begin{aligned} h(0) &= A \\ h\big(n^+\big) &= h(n) \cup f\left[\!\left[\prod_{i\in I} h(n)\right]\!\right] \end{aligned}$$

So,

$$C_* = \bigcup_{k\in\omega} h(k)$$

Prove or disprove $C^* = C_*$.

Answer 1: Counterexample with Proof by Contradiction: ×

Let $I = \omega$, $A = \{0, 1\}$, $B = \omega$, and

$$f(x) = \begin{cases} 1001 & \text{if } x = F \\ 2 \cdot [x(1) + x(2)] & \text{otherwise} \end{cases}$$

where $F = \{\langle n, 2n\rangle \mid n \in \omega\} \in \prod_{i\in\omega} \omega$

Assume $C^* = C_*$. It should be clear that from its definition, $C^* \subseteq X$, for all X such that $\{0, 1\} \subseteq X \subseteq \omega$ and $f[\![\prod_{i\in\omega} X]\!]$. As such, $f[\![\prod_{i\in\omega} C^*]\!] \subseteq C^*$:

$$\begin{aligned} y \in f\left[\!\left[\prod_{i\in\omega} C^*\right]\!\right] &\implies \forall X \left[\left(\{0,1\} \subseteq X \subseteq \omega \wedge f\left[\!\left[\prod_{i\in\omega} X\right]\!\right] \subseteq X\right) \implies y \in f\left[\!\left[\prod_{i\in\omega} X\right]\!\right]\right] \\ &\implies \forall X \left[\left(\{0,1\} \subseteq X \subseteq \omega \wedge f\left[\!\left[\prod_{i\in\omega} X\right]\!\right] \subseteq X\right) \implies y \in X\right] \\ &\implies y \in C^* \end{aligned}$$

Accordingly, by our assumption, $f[\![\prod_{i\in\omega} C_*]\!] \subseteq C_*$ also.

Let $S = \left\{n \in \omega \,\middle|\, \forall e\big(e \in h(n) \implies [e = 1 \vee \exists m(m \in \omega \wedge e = 2m)]\big)\right\}$. In English, S is the set of natural numbers n such that $h(n)$ contains only 1 and/or even (natural) numbers.

$0 \in S$ immediately by definition, because $h(0) = \{0, 1\}$ contains solely 1 and the even number 0. If $n \in S$, $n^+ \in S$ too: $e \in h(n^+)$ implies that $e \in h(n)$ or $e \in f\left[\!\left[\prod_{i\in I} h(n)\right]\!\right]$. In the first case, that $e \in h(n)$ easily satisfies the desired property as $n \in S$. As for the second case,

$$\begin{aligned} e \in f\left[\!\left[\prod_{i\in I} h(n)\right]\!\right] &\implies \exists g \left(g \in \prod_{i\in\omega} h(n) \wedge f(g) = e\right) \\ &\implies \exists g \left(g\colon \omega \to \bigcup_{i\in\omega} h(n) \wedge f(g) = e\right) \\ &\implies \exists g(g\colon \omega \to h(n) \wedge 2 \cdot [g(1) + g(2)] = e) \\ &\implies \exists m(m \in \omega \wedge e = 2m) && \text{since } h(n) \subseteq \omega, \text{ thus } g(1) + g(2) \in \omega \\ &\implies [e = 1 \vee \exists m(m \in \omega \wedge e = 2m)] \end{aligned}$$

Therefore, $n^+ \in S$ as the desired property holds true in both above cases. By definition, S is inductive. Using the Induction Principle for ω, $S = \omega$. Which also means that C_* is the set containing only 1 and even natural numbers.

We know $\operatorname{ran} F$ contains only even naturals as well (by def.). Hence, $F \in \prod_{i\in\omega} C_*$. However, $f(F) = 1001 \notin C_*$, because 1001 is not even. Consequently, $f[\![\prod_{i\in\omega} C_*]\!] \not\subseteq C_*$. This contradicts our previous claim, derived from our assumption, that $f[\![\prod_{i\in\omega} C_*]\!] \subseteq C_*$. Wherefore, it must be that $C^* \neq C_*$.

Remarks: We know that C_* is a set containing some even numbers. However, we have not shown the converse; that all even numbers are in C_*. Thus, we *cannot* conclude $F \in \prod_{i\in\omega} C_*$ yet. Proving this would be rather troublesome. So, in the second edition we tweak the example slightly:

✓✓ *Second Edition:* Let $I = \omega$, $A = \{0, 2\}$, $B = \omega$, and

$$f(x) = \begin{cases} 1001 & \text{if } x = F \\ x(1) + x(2) & \text{otherwise} \end{cases}$$

where $F = \{\langle n, 2n\rangle \mid n \in \omega\}$.
Assume $C^* = C_*$. It should be clear that from its definition, $C^* \subseteq X$, for all X such that $\{0, 1\} \subseteq X \subseteq \omega$ and $f[\![\prod_{i\in\omega} X]\!] \subseteq X$. As such, $f[\![\prod_{i\in\omega} C^*]\!] \subseteq C^*$:

$$\begin{aligned} y \in f\left[\!\left[\prod_{i\in\omega} C^*\right]\!\right] &\implies \forall X \left[\left(\{0,1\} \subseteq X \subseteq \omega \wedge f\left[\!\left[\prod_{i\in\omega} X\right]\!\right] \subseteq X\right) \implies y \in f\left[\!\left[\prod_{i\in\omega} X\right]\!\right]\right] \\ &\implies \forall X \left[\left(\{0,1\} \subseteq X \subseteq \omega \wedge f\left[\!\left[\prod_{i\in\omega} X\right]\!\right] \subseteq X\right) \implies y \in X\right] \\ &\implies y \in C^* \end{aligned}$$

Accordingly, by our assumption, $f[\![\prod_{i\in\omega} C_*]\!] \subseteq C_*$ also.

Let the set $S = \{n \in \omega \mid \forall e[e \in h(n) \implies \exists m(m \in \omega \wedge e = 2 \cdot m)]\}$. In English, S is the set of natural numbers n such that $h(n)$ contains only even (natural) numbers.

$0 \in S$ immediately, because $h(0) = \{0, 2\}$ indeed contains only the even numbers 0 and 2. If $n \in S$, then $n^+ \in S$ too: $e \in h(n^+)$ implies that $e \in h(n)$ or $e \in f[\![\prod_{i\in\omega} h(n)]\!]$. In the first case, $e \in h(n)$ easily satisfies the desired property as $n \in S$. As for the second case:

$$\begin{aligned} e \in f\left[\!\left[\prod_{i\in\omega} h(n)\right]\!\right] &\implies \exists g \left(g \in \prod_{i\in\omega} h(n) \wedge f(g) = e\right) \\ &\implies \exists g \left(g\colon \omega \to \bigcup_{i\in\omega} h(n) \wedge f(g) = e\right) \\ &\implies \exists g \left(g\colon \omega \to h(n) \wedge g(1) + g(2) = e\right) \\ &\implies \exists g \exists m_1 \exists m_2 \begin{pmatrix} g\colon \omega \to h(n) \ \wedge\ m_1 \in \omega \ \wedge\ m_2 \in \omega \\ \wedge\ g(1) = 2 \cdot m_1 \ \wedge\ g(2) = 2 \cdot m_2 \\ \wedge\ 2 \cdot m_1 + 2 \cdot m_2 = e \end{pmatrix} \quad \begin{array}{c}\text{since } n \in S,\ g(1) \text{ and } g(2) \\ \text{are even numbers}\end{array} \\ &\implies \exists m_1 \exists m_2 \left(2 \cdot (m_1 + m_2) = e\right) \\ &\implies \exists m(m \in \omega \wedge e = 2 \cdot m) \end{aligned}$$

Therefore, $n^+ \in S$ as the desired property holds true in both cases. By definition, S is inductive. Using the Induction Principle for ω, $S = \omega$. Which also means that C_* is the set containing only even numbers.

Now for the converse. Let the set $S' = \{k \in \omega \mid 2 \cdot k \in C_*\}$. By definition, $0 \in \omega$ as $2 \cdot 0 = 0 \in \{0, 2\} = h(0) \subseteq C_*$. Whenever $k \in \omega$, there exists some $n \in \omega$ so that $2 \cdot k \in h(n)$. As such, there also exists the function $G \in \prod_{i\in\omega} h(n)$ (by applying a subset axiom to $\omega \times h(n)$) with

$$G = \{\langle x, y\rangle \mid (x = 1 \implies y = 2 \cdot k) \wedge (x \in \omega \setminus \{1\} \implies y = 2)\}$$

because $2 \in h(n)$ for all $n \in \omega$. We shall do a quick proof of this small fact. Let the set $S'' = \{n \in \omega \mid 2 \in h(n)\}$. Then, $2 \in \{0, 2\} = h(0)$ by definition, meaning $0 \in S''$. If $n \in S''$, $n^+ \in S''$ since $h(n) \subseteq h(n^+) = h(n) \cup f[\![\prod_{i\in\omega} h(n)]\!]$. Thus, S'' is an inductive subset of ω. By the

Induction Principle for ω, $S'' = \omega$. Returning to the previous part,

$$\begin{aligned} f(G) \in f\left[\!\left[\prod_{i\in\omega} h(n)\right]\!\right] &\implies f(G) \in h\big(n^+\big) \\ &\implies G(1) + G(2) \in C_* \\ &\implies 2 \cdot k + 2 \in C_* \\ &\implies 2 \cdot (k+1) \in C_* \\ &\implies 2 \cdot \big(k^+\big) \in C_* \end{aligned}$$

Consequently, $k^+ \in S'$; S' is an inductive subset of ω. Using the Induction Principle for ω, $S' = \omega$. Which means that S contains all even (natural) numbers. Combined with what we previously proven, that C_* is the set containing only even numbers, we conclude that C_* is the set of all even numbers.

We know $\operatorname{ran} F$ contains only even naturals as well (by def.). Hence, $F \in \prod_{i\in\omega} C_*$. However, $f(F) = 1001 \notin C_*$, because 1001 is not even. Consequently, $f[\![\prod_{i\in\omega} C_*]\!] \nsubseteq C_*$. This contradicts our previous claim, derived from our assumption, that $f[\![\prod_{i\in\omega} C_*]\!] \subseteq C_*$. Wherefore, it must be that $C^* \neq C_*$.

Remarks (Big Check 1, 30/12/22): Once again, the general idea seems correct, however the presentation and phrasing here is suboptimal. It could be significantly clearer and easier to read with the aid of more English. Hence, I give this a ✓

Answer 2: Counterexample + Direct Proof: ×

Let $I = \omega$, $A = \{0, 1\}$, $B = \omega$, and

$$f(x) = \begin{cases} 1001 & \text{if } x = F \\ 2 \cdot [x(1) + x(2)] & \text{otherwise} \end{cases}$$

where $F = \{\langle n, 2n\rangle \mid n \in \omega\} \in \prod_{i\in\omega} \omega$.

Also let the set $T = \{n \in \omega \mid n \in C^*\}$. $0, 1 \in T$ since for all X; $\{0, 1\} \subseteq X$ implies $0, 1 \in X$. If $n \in T$, we shall see that $n^+ \in T$ as well. For all X such that $\{0, 1\} \subseteq X \subseteq \omega$, there exists $G \in \prod_{i\in\omega} X$ with

$$G(1) = n$$
$$G(2) = 1$$

because $1, n \in T$. Consequently, for all X,

$$\left(\{0, 1\} \subseteq X \subseteq \omega \wedge f\left[\!\left[\prod_{i\in\omega} X\right]\!\right] \subseteq X\right) \implies \forall g \left[g \in \prod_{i\in\omega} X \implies f(g) \in X\right]$$
$$\implies f(G) = 2(n + 1) = 2(n^+) \in X$$

Which means $2(n^+) \in C^*$. Hence, $n^+ \in T$ and T is inductive. By the Induction Principle for ω, $T = \omega$. In other words, C^* contains all even numbers. Now, for all X so that $\{0, 1\} \subseteq X \subseteq \omega$, $F \in \prod_{i\in\omega} X$. As a result, by the same logic as above, $1001 \in C^*$.

Let $S = \{n \in \omega \mid \forall e(e \in h(n) \implies [e = 1 \vee \exists m(m \in \omega \wedge e = 2m)])\}$. In English, S is the set of natural numbers n such that $h(n)$ contains only 1 and/or even (natural) numbers.

$0 \in S$ immediately by definition, because $h(0) = \{0, 1\}$ contains solely 1 and the even number 0. If $n \in S$, $n^+ \in S$ too: $e \in h(n^+)$ implies that $e \in h(n)$ or $e \in f\left[\!\left[\prod_{i\in I} h(n)\right]\!\right]$. In the first case, that $e \in h(n)$ easily satisfies the desired property as $n \in S$. As for the second case,

$$\begin{aligned} e \in f\left[\!\left[\prod_{i\in I} h(n)\right]\!\right] &\implies \exists g \left(g \in \prod_{i\in\omega} h(n) \wedge f(g) = e\right) \\ &\implies \exists g \left(g \colon \omega \to \bigcup_{i\in\omega} h(n) \wedge f(g) = e\right) \\ &\implies \exists g(g \colon \omega \to h(n) \wedge 2 \cdot [g(1) + g(2)] = e) \\ &\implies \exists m(m \in \omega \wedge e = 2m) && \text{since } h(n) \subseteq \omega, \text{ thus } g(1) + g(2) \in \omega \\ &\implies [e = 1 \vee \exists m(m \in \omega \wedge e = 2m)] \end{aligned}$$

Therefore, $n^+ \in S$ as the desired property holds true in both above cases. By definition, S is inductive. Using the Induction Principle for ω, $S = \omega$. Which also means that C_* is the set containing only 1 and even natural numbers.

We know $\operatorname{ran} F$ contains only even naturals as well (by def.). Hence, $F \in \prod_{i\in\omega} C_*$. However, $f(F) = 1001 \notin C_*$, because 1001 is not even. Consequently, $f\llbracket\prod_{i\in\omega} C_*\rrbracket \not\subseteq C_*$.

Wherefore, since $1001 \in C^*$ but $1001 \notin C_*$, $C^* \neq C_*$ is certain.

Remarks:

1. It should be quite clear that C^* does not contain all natural numbers.
2. If we use the set T as defined above, $2 \cdot (n^+) \in C^*$ does not necessarily mean $n^+ \in T$.
3. Similarly, even if we change the set T to be $\{n \in \omega \mid 2 \cdot n \in C^*\}$: our induction hypothesis that $n \in T$ will now mean $2 \cdot n \in C^*$. So, if we follow the above procedure, we would only arrive at $f(G) = 2 \cdot (2 \cdot n + 1)$. Which doesn't allow us to complete our inductive proof. Thus, we shall tweak the example slightly in the second edition:

✓✓ *Second Edition:* Let $I = \omega$, $A = \{0, 2\}$, $B = \omega$, and

$$f(x) = \begin{cases} 1001 & \text{if } x = F \\ x(1) + x(2) & \text{otherwise} \end{cases}$$

where $F = \{\langle n, 2n\rangle \mid n \in \omega\}$.
Also let the set $T = \{n \in \omega \mid 2 \cdot n \in C^*\}$. $0, 1 \in T$ since for all X; $\{0, 2\} \subseteq X$ implies $2 \cdot 0 = 0 \in X$ and $2 \cdot 1 = 2 \in X$. If $n \in T$, we shall see that $n^+ \in T$ as well. For all X such that $\{0, 1\} \subseteq X \subseteq \omega$, there exists a $G \in \prod_{i\in\omega} X$ with

$$G = \{\langle x, y\rangle \mid (x = 1 \implies y = 2 \cdot n) \wedge (x \in \omega \setminus \{1\} \implies y = 2)\}$$

because $1, n \in T$. Consequently, for all X,

$$\begin{aligned} \left(\{0, 2\} \subseteq X \subseteq \omega \wedge f\left[\!\left[\prod_{i\in\omega} X\right]\!\right] \subseteq X\right) &\implies \forall g\left[g \in \prod_{i\in\omega} X \implies f(g) \in X\right] \\ &\implies f(G) = 2 \cdot n + 2 = 2 \cdot n^+ \in X \end{aligned}$$

Which means that $2 \cdot n^+ \in C^*$. Hence, $n^+ \in T$ and T is an inductive subset of ω. By the Induction Principle for ω, $T = \omega$. In other words, C^* contains all even numbers. Now, for all X so that $\{0, 1\} \subseteq X \subseteq \omega$ and $f[\![\prod_{i\in\omega} X]\!] \subseteq X$, $F \in \prod_{i\in\omega} X$. As a result, by the same logic as above, $1001 \in C^*$.

Let the set $S = \{n \in \omega \mid \forall e[e \in h(n) \implies \exists m(m \in \omega \wedge e = 2 \cdot m)]\}$. In English, S is the set of natural numbers n such that $h(n)$ contains only even (natural) numbers.

$0 \in S$ immediately, because $h(0) = \{0, 2\}$ indeed contains only the even numbers 0 and 2. If $n \in S$, then $n^* \in S$ too: $e \in h(n^+)$ implies that $e \in h(n)$ or $e \in f[\![\prod_{i\in\omega} h(n)]\!]$. In the first case, $e \in h(n)$ easily satisfies the desired property as $n \in S$. As for the second case:

$$\begin{aligned} e \in f\left[\!\left[\prod_{i\in\omega} h(n)\right]\!\right] &\implies \exists g\left(g \in \prod_{i\in\omega} h(n) \wedge f(g) = e\right) \\ &\implies \exists g\left(g\colon \omega \to \bigcup_{i\in\omega} h(n) \wedge f(g) = e\right) \\ &\implies \exists g\,(g\colon \omega \to h(n) \wedge g(1) + g(2) = e) \\ &\implies \exists g \exists m_1 \exists m_2 \begin{pmatrix} g\colon \omega \to h(n) \ \wedge\ m_1 \in \omega \ \wedge\ m_2 \in \omega \\ \wedge\ g(1) = 2 \cdot m_1 \ \wedge\ g(2) = 2 \cdot m_2 \\ \wedge\ 2 \cdot m_1 + 2 \cdot m_2 = e \end{pmatrix} \quad \begin{array}{l}\text{since } n \in S,\ g(1) \text{ and } g(2) \\ \text{are even numbers}\end{array} \\ &\implies \exists m_1 \exists m_2\,(2 \cdot (m_1 + m_2) = e) \\ &\implies \exists m(m \in \omega \wedge e = 2 \cdot m) \end{aligned}$$

Therefore, $n^+ \in S$ as the desired property holds true in both cases. By definition, S is inductive. Using the Induction Principle for ω, $S = \omega$. Which also means that C_* is the set containing only even numbers.

Now for the converse. Let the set $S' = \{k \in \omega \mid 2 \cdot k \in C_*\}$. By definition, $0 \in \omega$ as $2 \cdot 0 = 0 \in \{0, 2\} = h(0) \subseteq C_*$. Whenever $k \in S'$, there exists some $n \in \omega$ so that $2 \cdot k \in h(n)$. As such, there also exists the function $G \in \prod_{i\in\omega} h(n)$ (by applying a subset axiom to $\omega \times h(n)$) with

$$G = \{\langle x, y\rangle \mid (x = 1 \implies y = 2 \cdot k) \wedge (x \in \omega \setminus \{1\} \implies y = 2)\}$$

because $2 \in h(n)$ for all $n \in \omega$. We shall do a quick proof of this small fact. Let the set $S'' = \{n \in \omega \mid 2 \in h(n)\}$. Then, $2 \in \{0, 2\} = h(0)$ by definition, meaning $0 \in S''$. If $n \in S''$, $n^+ \in S''$ since $h(n) \subseteq h(n^+) = h(n) \cup f[\![\prod_{i\in\omega} h(n)]\!]$. Thus, S'' is an inductive subset of ω. By the

Induction Principle for ω, $S'' = \omega$. Returning to the previous part,

$$\begin{aligned} f(G) \in f\left[\!\left[\prod_{i\in\omega} h(n)\right]\!\right] &\implies f(G) \in h\left(n^+\right) \\ &\implies G(1) + G(2) \in C_* \\ &\implies 2 \cdot k + 2 \in C_* \\ &\implies 2 \cdot (k+1) \in C_* \\ &\implies 2 \cdot \left(k^+\right) \in C_* \end{aligned}$$

Consequently, $k^+ \in S'$; S' is an inductive subset of ω. Using the Induction Principle for ω, $S' = \omega$. Which means that C_* contains all even (natural) numbers. Combined with what we previously proven, that C_* is the set containing only even numbers, we conclude that C_* is the set of all even numbers. As 1001 is not even, $1001 \notin C_*$.

Wherefore, since $1001 \in C^*$ but $1001 \notin C_*$, $C^* \neq C_*$ is certain.

Remarks (Big Check 1, 31/12/22): Same thing as before.

✓ Self-Exercise 5.1: **Find the condition(s)** such that $C^* = C_*$ is true iff those condition(s) are true.

$C^* = C_*$ iff $f[\![\prod_{i\in\omega} C_*]\!] \subseteq C_*$. *Proof:*

($\Longrightarrow$) It should be clear that from its definition, $C^* \subseteq X$, for all X such that $\{0,1\} \subseteq X \subseteq \omega$ and $f[\![\prod_{i\in\omega} X]\!]$. As such, $f[\![\prod_{i\in\omega} C^*]\!] \subseteq C^*$:

$$\begin{aligned} y \in f\left[\!\!\left[\prod_{i\in\omega} C^*\right]\!\!\right] &\Longrightarrow \forall X\left[\left(\{0,1\} \subseteq X \subseteq \omega \wedge f\left[\!\!\left[\prod_{i\in\omega} X\right]\!\!\right] \subseteq X\right) \Longrightarrow y \in f\left[\!\!\left[\prod_{i\in\omega} X\right]\!\!\right]\right] \\ &\Longrightarrow \forall X\left[\left(\{0,1\} \subseteq X \subseteq \omega \wedge f\left[\!\!\left[\prod_{i\in\omega} X\right]\!\!\right] \subseteq X\right) \Longrightarrow y \in X\right] \\ &\Longrightarrow y \in C^* \end{aligned}$$

Assume $C^* = C_*$ is true. Consequently, $f[\![\prod_{i\in\omega} C_*]\!] \subseteq C_*$ should hold.

($\Longleftarrow$) We know that $A \subseteq C_* \subseteq B$:

- $\underline{A \subseteq C_*}$:

$$\begin{aligned} x \in A &\Longrightarrow (0 \in \omega \wedge x \in h(0)) \\ &\Longrightarrow \exists k(k \in \omega \wedge x \in h(k)) \\ &\Longrightarrow x \in C_* \end{aligned}$$

- $\underline{C_* \subseteq B}$:

$$\begin{aligned} x \in C_* &\Longleftrightarrow \exists k(k \in \omega \wedge x \in h(k) \in \mathscr{P}B) \\ &\Longrightarrow x \in B \end{aligned}$$

Thus, we conclude that $A \subseteq C_* \subseteq B$, as desired.

Suppose that $f[\![\prod_{i\in\omega} C_*]\!] \subseteq C_*$ is true. As a result,

$$\begin{aligned} x \in C^* &\Longleftrightarrow x \in \bigcap\left\{X \,\middle|\, A \subseteq X \subseteq B \wedge f\left[\!\!\left[\prod_{i\in I} X\right]\!\!\right] \subseteq X\right\} \\ &\Longleftrightarrow \forall X\left[\left(A \subseteq X \subseteq B \wedge f\left[\!\!\left[\prod_{i\in I} X\right]\!\!\right] \subseteq X\right) \Longrightarrow x \in X\right] \\ &\Longrightarrow x \in C_* \qquad \text{as } A \subseteq C_* \subseteq B \text{ and } f\left[\!\!\left[\prod_{i\in\omega} C_*\right]\!\!\right] \subseteq C_* \end{aligned}$$

Hence, $C^* \subseteq C_*$. Now let the set $S = \{k \in \omega \mid h(k) \subseteq C^*\}$;

$$\begin{aligned} x \in h(0) &\Longrightarrow \forall X(A \subseteq X \Longrightarrow x \in X) \\ &\Longrightarrow \forall X\left[\left(A \subseteq X \subseteq B \wedge f\left[\!\!\left[\prod_{i\in\omega} X\right]\!\!\right] \subseteq X\right) \Longrightarrow x \in X\right] \\ &\Longrightarrow x \in C^* \end{aligned}$$

As $h(0) \subseteq C^*$, $0 \in S$.

If $k \in S$, $k^+ \in S$:

We first prove $f[\![\prod_{i\in I} h(i)]\!] \subseteq C^*$;

$$\begin{aligned} h(k) \subseteq C^* &\implies \forall X \left(\left(A \subseteq X \subseteq B \wedge f\left[\!\!\left[\prod_{i\in I} X \right]\!\!\right] \subseteq X \right) \implies [h(k) \subseteq X] \right) \\ &\implies \forall X \left(\left(A \subseteq X \subseteq B \wedge f\left[\!\!\left[\prod_{i\in I} X \right]\!\!\right] \subseteq X \right) \implies \left[f\left[\!\!\left[\prod_{i\in I} h(k) \right]\!\!\right] \subseteq X \right] \right) \\ &\implies f\left[\!\!\left[\prod_{i\in I} h(k) \right]\!\!\right] \subseteq C^* \end{aligned}$$

Therefore, the following is true

$$\begin{aligned} y \in h(k^+) &\iff y \in h(k) \cup f\left[\!\!\left[\prod_{i\in I} h(k) \right]\!\!\right] \\ &\iff y \in h(i) \vee y \in f\left[\!\!\left[\prod_{i\in I} h(k) \right]\!\!\right] \\ &\implies y \in C^* \qquad \text{since } k \in S \text{ and } f\left[\!\!\left[\prod_{i\in I} h(k) \right]\!\!\right] \subseteq C^* \end{aligned}$$

Accordingly, the set S is inductive, by definition. By applying the Induction Principle for ω, $S = \omega$. So, $C_* \subseteq C^*$:

$$\begin{aligned} y \in C_* &\iff \exists k[k \in \omega \wedge y \in h(k)] \\ &\implies y \in C^* \end{aligned}$$

Thence, we can conclude that; since $C^* \subseteq C_*$ and $C_* \subseteq C^*$, $C^* = C_*$.

Wherefore, $C^* = C_*$ iff $f[\![\prod_{i\in\omega} C_*]\!] \subseteq C_*$ as we claimed.

Now, there are various 'equivalent forms' of $f[\![\prod_{i\in I} C_*]\!] \subseteq C_*$. To be more accurate, $f[\![\prod_{i\in I} C_*]\!] \subseteq C_*$ holds iff at least one of the following does

1. $C_* \neq \varnothing$ and $A \neq \varnothing$, but $f\left[\!\!\left[\prod_{i\in I} C_* \right]\!\!\right] = \varnothing$, which is possible when AC is not assumed.
2. $f\left[\!\!\left[\prod_{i\in I} C_* \right]\!\!\right] \subseteq A$.
   i. $C_* = A = \varnothing$.
3. There exists a natural m so that $f\left[\!\!\left[\prod_{i\in I} C_* \right]\!\!\right] \subseteq f\left[\!\!\left[\prod_{i\in I} h(m) \right]\!\!\right]$.
   a. $I = \varnothing$.
   b. I is finite.
   c. There exists a natural m such that $C_* = h(m)$.

(Don't really feel like typing the proof of this out right now lol.)

Remarks (Big Check 1, 31/12/22): Note that we are trying to prove the general case here so $\{0, 1\}$ should be replaced with A and ω with I or B (depending on where ω is). I think that was a careless mistake where I got mixed up with the previous parts. Other than that error, the main issue would again be that the presentation could be considerably better and improved upon.

1.3.4 Arithmetic

Self-Proof of Theorem 4I: ✓✓
(A1)

$$m + 0 = A_m(0) = m$$

(A2)

$$m + n^+ = A_m\big(n^+\big) = A_m(n)^+ = (m + n)^+$$

Self-Proof of Theorem 4J: ✓✓
(M1)

$$m \cdot 0 = M_m(0) = 0$$

(M2)

$$m \cdot n^+ = M_m\big(n^+\big) = M_m(n) + m = m \cdot n + m$$

Self-Proof of Theorem 4K: ✓✓

(1) ✓✓ Let the set $S_1 = \{p \in \omega \,|\, \forall m \forall n[(m \in \omega \wedge n \in \omega) \implies m + (n + p) = (m + n) + p]\}$. When $p = 0$, $m + (n + 0) = m + n = (m + n) + 0$ by (A1), meaning $0 \in S_1$. If $p \in S_1$, $p^+ \in S_1$:

$$\begin{aligned} m + \big(n + p^+\big) &= m + (n + p)^+ && \text{(A2)} \\ &= [m + (n + p)]^+ && \text{(A2)} \\ &= [(m + n) + p]^+ && \text{since } p \in S_1 \\ &= (m + n) + p^+ && \text{(A2)} \end{aligned}$$

Thus, S_1 is an inductive subset of ω and by the Induction Principle for ω, $S_1 = \omega$. Which means that for all $m, n, p \in \omega$, $m + (n + p) = (m + n) + p$.

(2) ✓✓ Let the set $S_2 = \{n \in \omega \,|\, \forall m(m \in \omega \implies m + n = n + m)\}$ and the set $T_2 = \{m \in \omega \,|\, m + 0 = 0 + m\}$. Immediately, $0 + 0 = 0 + 0$ and $0 \in T_2$. If $m \in T_2$,

$$\begin{aligned} 0 + m^+ &= (0 + m)^+ && \text{(A2)} \\ &= (m + 0)^+ && \text{since } m \in T_2 \\ &= m^+ && \text{(A1)} \\ &= m^+ + 0 && \text{(A1)} \end{aligned}$$

Consequently, $m^+ \in T_2$. By the Induction Principle for ω, $T_2 = \omega$. i.e. $m + 0 = 0 + m$ for all $m \in \omega$; so $0 \in S_2$. Now assume $n \in S_2$; letting the set $T_2' = \{m \in \omega \,|\, m + n^+ = n^+ + m\}$:

$$\begin{aligned} 0 + n^+ &= (0 + n)^+ && \text{(A2)} \\ &= (n + 0)^+ && \text{as } n \in S_2 \\ &= n^+ && \text{(A1)} \\ &= n^+ + 0 && \text{(A1)} \end{aligned}$$

Accordingly, $0 \in T_2'$. Whenever $m \in T_2'$,

$$\begin{aligned} m^+ + n^+ &= \big(m^+ + n\big)^+ && \text{(A2)} \\ &= (n + m^+)^+ && \text{because } n \in S_2 \\ &= \Big[(n + m)^+\Big]^+ && \text{(A2)} \\ &= \Big[(m + n)^+\Big]^+ && \text{since } n \in S_2 \\ &= \big(m + n^+\big)^+ && \text{(A2)} \\ &= \big(n^+ + m\big)^+ && \text{as } m \in T_2' \\ &= n^+ + m^+ && \text{(A2)} \end{aligned}$$

As a result, $m^+ \in T_2'$. By the Induction Principle for ω, $T_2' = \omega$, and for all $m \in \omega$, $m + n^+ = n^+ + m$. Hence, $n^+ \in S_2$ follows and by the Induction Principle for ω, $S_2 = \omega$. We have successfully proven that for all $n, m \in \omega$; $m + n = m + n$.

(3) ✓✓ Let the set $S_3 = \{p \in \omega \mid \forall m \forall n[m, n \in \omega \implies m \cdot (n + p) = (m \cdot n) + (m \cdot p)]\}$. When $p = 0$,

$$\begin{aligned} m \cdot (n + 0) &= m \cdot n && \text{(A1)} \\ &= m \cdot n + 0 && \text{(A1)} \\ &= m \cdot n + m \cdot 0 && \text{(M1)} \end{aligned}$$

If $p \in S_3$;

$$\begin{aligned} m \cdot (n + p^+) &= m \cdot (n + p)^+ && \text{(A2)} \\ &= [m \cdot (n + p)] + m && \text{(M2)} \\ &= (m \cdot n + m \cdot p) + m && \text{since } p \in S_3 \\ &= m \cdot n + (m \cdot p + m) && \text{(1)} \\ &= m \cdot n + m \cdot p^+ && \text{(M2)} \end{aligned}$$

Therefore, we see that $p^+ \in S_3$ indeed. S_3 is now an inductive subset of ω. By the Induction Principle for ω, $S_3 = \omega$. Thence, for all $m, n, p \in \omega$, $m \cdot (n + p) = n \cdot n + m \cdot p$.

(4) ✓✓ Let the set $S_4 = \{p \in \omega \mid \forall m \forall n[m, n \in \omega \implies m \cdot (n \cdot p) = (m \cdot n) \cdot p]\}$. Since $m \cdot (n \cdot 0) = m \cdot 0 = 0 = (m \cdot n) \cdot 0$ by (M1), $0 \in S_4$. Whenever $p \in S_4$, $p^+ \in S_4$:

$$\begin{aligned} m \cdot \left(n \cdot p^+\right) &= m \cdot [(n \cdot p) + n] && \text{(M2)} \\ &= m \cdot (n \cdot p) + m \cdot n && \text{(3)} \\ &= (m \cdot n) \cdot p + m \cdot n && \text{as } p \in S_4 \\ &= (m \cdot n) \cdot p^+ && \text{(M2)} \end{aligned}$$

Therefore, we see that $p^+ \in S_4$ indeed. S_4 is now an inductive subset of ω. By the Induction Principle for ω, $S_4 = \omega$. In other words: For all $m, n, p \in \omega$; $m \cdot (n \cdot p) = (m \cdot n) \cdot p$.

(5) ✓✓ Let the set $S_5 = \{n \in \omega \mid \forall m(m \in \omega \implies m \cdot n = n \cdot m)\}$ and the set $T_5 = \{m \in \omega \mid m \cdot 0 = 0 \cdot m\}$. We see that $0 \cdot 0 = 0 \cdot 0$, so $0 \in T_5$. When $m \in T_5$,

$$\begin{aligned} 0 \cdot m^+ &= (0 \cdot m) + 0 && \text{(M2)} \\ &= (m \cdot 0) + 0 && \text{since } m \in T_5 \\ &= 0 + 0 && \text{(M1)} \\ &= 0 && \text{(A1)} \\ &= m^+ \cdot 0 && \text{(M1)} \end{aligned}$$

Thus, $m^+ \in T_5$; i.e. T_5 is an inductive subset of ω. By the Induction Principle for ω, $T_5 = \omega$. In other words, for all $m \in \omega$, $m \cdot 0 = 0 \cdot m$. Accordingly, $0 \in S_5$.
If $n \in S_5$, we shall see that $n^+ \in S_5$ as well: Let the set $T_5' = \{m \in \omega \mid m \cdot n^+ = n^+ \cdot m\}$. Notice that

$$\begin{aligned} 0 \cdot n^+ &= 0 \cdot n + 0 && \text{(M2)} \\ &= n \cdot 0 + 0 && \text{as } n \in S_5 \\ &= 0 + 0 && \text{(M1)} \\ &= 0 && \text{(A1)} \\ &= n^+ \cdot 0 && \text{(M1)} \end{aligned}$$

As a result, $0 \in T_5'$. Whenever $m \in T_5'$,

$$\begin{aligned}
m^+ \cdot n^+ &= m^+ \cdot n + m && \text{(M2)} \\
&= n \cdot m^+ + m && \text{because } n \in S_5 \\
&= (n \cdot m + n) + m && \text{(M2)} \\
&= (m \cdot n + n) + m && \text{because } n \in S_5 \\
&= m \cdot n + (n + m) && \text{(1)} \\
&= m \cdot n + (m + n) && \text{(2)} \\
&= (m \cdot n + m) + n && \text{(1)} \\
&= m \cdot n^+ + n && \text{(M2)} \\
&= n^+ \cdot m + n && \text{since } m \in T_5' \\
&= n^+ \cdot m^+ && \text{(M2)}
\end{aligned}$$

Consequently, $m^+ \in T_5'$ and T_5' is an inductive subset of ω. By the Induction Principle for ω, $T_5' = \omega$. i.e. For all $m \in \omega$, $m \cdot n^+ = n^+ \cdot m$. Wherefore, $n^+ \in S_5$ and S_5 is an inductive subset of ω. Once more, by the Induction Principle for ω, $S_5' = \omega$; For all $m, n \in \omega$, $m \cdot n = n \cdot m$.

Self-Exercise 6 — Generalising 'Arithmetical Functions': Prove that for all $i \in \omega$, there exists a unique function $G_i \colon \omega \to {}^{\omega}\omega$ so that

$$[G_0(m)](n) = A_m(n) \tag{1}$$

There exists some $c \in \omega$ such that $[G_i(m)](c) = m \quad \text{for all } m \in \omega$ (2)

If there exists some $j \in \omega$ with $i = j^+$, then:

There exists some $c' \in \omega$ for all $m \in \omega$ so $\left[G_{j^+}(m)\right](0) = c' \quad \text{and} \quad [G_j(m)](c') = m$ (3)

$$\left[G_{j^+}(m)\right]\left(n^+\right) = [G_j(m)]\Big(\left[G_{j^+}(m)\right](n)\Big) \tag{4}$$

We call functions mapping from ω to ${}^{\omega}\omega$ that satisfy conditions (2)-(4) as 'Natural Arithmetical unary Functions', or NAU-functions for short. (Yeah... coming up with names isn't my strong suit)

Proof: ✓

Existance of G_i for all $i \in \omega$

Let the set $S = \{k \in \omega \mid G_k \text{ exists}\}$.

$0 \in S$:

We know $[G_0(m)](n) = A_m(n)$ by definition, and $[G_0(m)](0) = A_m(0) = m$; meaning conditions (1) and (2) is satisfied. By Theorem 4D, 0 is not the successor of any natural number, so conditions (3) and (4) are not necessary to check (since the conditional statement above implicating them is immediately true already). By the construction of $A_m(n)$ (via the Recursion Theorem on ω), we know that for all $m \in \omega$, A_m is a function mapping from ω to ω, and thus indeed an element of ${}^{\omega}\omega$. G_0 is also a function: Let $m_1 = m_2 \in \omega$ and the set $T = \{n \in \omega \mid A_{m_1}(n) = A_{m_2}(n)\}$. Since $A_{m_1}(0) = m_1 = m_2 = A_{m_2}(0)$, $0 \in T$. When $n \in T$,

$$\begin{aligned} A_{m_1}\left(n^+\right) &= A_{m_1}(n)^+ \\ &= A_{m_2}(n)^+ \quad \text{as } n \in T \\ &= A_{m_2}\left(n^+\right) \end{aligned}$$

Which means that $n^+ \in T$ and the set T is an inductive subset of ω. By the Induction Principle for ω, $T = \omega$. As $A_{m_1}(n) = A_{m_2}(n)$ for all n in their common domain of $\operatorname{dom} A_{m_1} = \operatorname{dom} A_{m_2} = \omega$, $A_{m_1} = A_{m_2}$. Thus, G_0 is indeed a function; and $0 \in S$ holds true.

$k \in S$ implies $k^+ \in S$:

If $k \in S$, then we will see that $k^+ \in S$ must be true too: Notice that by our assumption that $k \in S$, for all $m \in \omega$ there indeed exists a function mapping from $\omega \to \omega$: namely $G_k(m) \in {}^{\omega}\omega$; and there is also some $c \in \omega$ (so that $[G_k(m)](c) = m$ for all $m \in \omega$). Hence all conditions for applying the Recursion Theorem on ω are satisfied. (For all $m \in \omega$) There now exists a (unique) function $h_m \colon \omega \to \omega$ where

$$\begin{aligned} h_m(0) &= c \\ h_m\left(n^+\right) &= [G_k(m)]\big(h_m(n)\big) \end{aligned}$$

We claim that h_m is our desired $G_{k^+}(m)$. Clearly, conditions (3) and (4) are satisfied by definition. Condition (2) is also satisfied as

$$\begin{aligned} h_m(1) &= [G_k(m)]\big(h_m(0)\big) \\ &= [G_k(m)]\big(c\big) \\ &= m \end{aligned}$$

Thence, h_m is the $G_{k^+}(m)$ we want indeed as conditions (2)-(4) are all satisfied. Lastly, we need to check that $G_{k^+} := \{\langle m, h_m\rangle \mid m \in \omega\}$ is a function. For all $m_1 = m_2 \in \omega$, $h_{m_1} = h_{m_2}$ because

from the Recursion Theorem on ω we know such a function is unique. Hence, $G_{k^+}(m_1) = G_{k^+}(m_2)$. Accordingly, G_{k^+} is a function.

Alternatively, we can give another proof that G_{k^+} is a function, by induction. Let the set $T' = \{n \in \omega \mid h_{m_1}(n) = h_{m_2}(n)\}$. By definition, $h_{m_1}(0) = c = h_{m_2}(n)$. Whenever $n \in T'$, $n^+ \in T'$ is also true:

$$\begin{aligned} h_{m_1}\left(n^+\right) &= \left[G_k(m_1)\right]\left(h_{m_1}(n)\right) \\ &= \left[G_k(m_2)\right]\left(h_{m_2}(n)\right) \quad \text{since } n \in T, \text{ and } G_k \text{ is a function as } k \in S_1 \\ &= h_{m_2}\left(n^+\right) \end{aligned}$$

As a result, T' is an inductive subset of ω and $T' = \omega$ by the Induction Principle for ω. So, since $h_{m_1}(n) = h_{m_2}(n)$ for all n in their common domain of $\omega = \operatorname{dom} h_{m_1} = \operatorname{dom} h_{m_2}$, thus $h_{m_1} = h_{m_2}$. Accordingly, $G_{k^+}(m_1) = G_{k^+}(m_2)$ and G_{k^+} is a function.

Which means that $k^+ \in S$ and S is an inductive subset of ω. By the Induction Principle for ω, $S = \omega$. Therefore, for all $i \in \omega$, such $G_i \colon \omega \to {}^{\omega}\omega$ (as described in the question) exists.

Uniqueness of each G_i for all $i \in \omega$

Let the set $T'' = \{i \in \omega \mid \forall G_i \forall G_i' (G_i \text{ and } G_i' \text{ are NAU-functions} \implies G_i = G_i')\}$. In other words, T'' is the set of all natural i so that the function G_i is unique. As aforementioned, for all $m \in \omega$, A_m is unique by its construction. Whence, $G_0(m) = A_m = G_0'(m)$ for all m in their common domain of $\omega = \operatorname{dom} G_0 = \operatorname{dom} G_0'$. Thus, $G_0 = G_0'$; and $0 \in T''$.

Assume $i \in T''$. Now let the set $T''' = \left\{n \in \omega \mid \forall m \left(m \in \omega \implies \left[G_{i^+}(m)\right](n) = \left[G_{i^+}'(m)\right](n)\right)\right\}$. By definition, there exists some $c' \in \omega$ for all $m \in \omega$ so $[G_i(m)](c') = [G_i'(m)](c') = m$ since $i \in T''$, and thus $\left[G_{i^+}(m)\right](0) = c' = \left[G_{i^+}'(m)\right](0)$. Accordingly, $0 \in T'''$. If $n \in T'''$, then

$$\begin{aligned} \left[G_{i^+}(m)\right]\left(n^+\right) &= \left[G_i(m)\right]\Big(\left[G_{i^+}(m)\right](n)\Big) \\ &= \left[G_i'(m)\right]\Big(\left[G_{i^+}'(m)\right](n)\Big) \quad \text{since } i \in T'' \text{ and } n \in T''' \\ &= \left[G_{i^+}'(m)\right]\left(n^+\right) \end{aligned}$$

Which means that $n^+ \in T'''$ and T''' is an inductive subset of ω. By the Induction Principle for ω, $T''' = \omega$. Therefore, for all $n \in \omega$ and $m \in \omega$, $\left[G_{i^+}(m)\right](n) = \left[G_{i^+}'(m)\right](n)$. We know the functions $G_{i^+}(m)$ and $G_{i^+}'(m)$ both have domain ω, on which they agree on, so $G_{i^+}(m) = G_{i^+}'(m)$ (for all $m \in \omega$). Applying the same principle, this G_{i^+} and G_{i^+}' both have a domain of ω, on which they agree on, thus $G_{i^+} = G_{i^+}'$. As a result, $i^+ \in T''$ and T'' is an inductive subset of ω. By the Induction Principle for ω, $T'' = \omega$. i.e. For all $i \in \omega$, the function G_i is indeed unique.

With this, now we can make our notation less awkward. We were previously forced to use not very nice notation in order to utilise the Recursion Theorem on ω in our proof. At last, we can introduce nicer notation instead of searing your eyes out.

1. First, let the function $\hat{G}_i = \{\langle\langle m, n\rangle, [G_i(m)](n)\rangle \mid m, n \in \omega\}$. We now prove our claim that it is a function: Let $\langle m_1, n_1\rangle = \langle m_2, n_2\rangle$. By definition, G_i is a function. So, $G_i(m_1) = G_i(m_2)$. G_i also maps from ω to ${}^{\omega}\omega$. i.e. $G_i(m_1) = G_i(m_2)$ is a function. Consequently, $[G_i(m_1)](n_1) = [G_i(m_2)](n_2)$. Which means that $\hat{G}_i(m_1, n_1) = \hat{G}_i(m_2, n_2)$. Indeed, we can conclude $\hat{G}_i$ is a function mapping from ω^2 to ω.

2. Secondly, let $G = \left\{\left\langle \langle i, m, n\rangle, \hat{G}_i(m, n)\right\rangle \,\middle|\, i, m, n \in \omega\right\}$. Suppose $\langle i_1, m_1, n_1\rangle = \langle i_2, m_2, n_2\rangle$. By uniqueness, which we proved earlier, $G_{i_1} = G_{i_2}$. We also know this is a function by definition, so $G_{i_1}(m_1) = G_{i_2}(m_2)$. Repeating the process, these are elements of ${}^{\omega}\omega$, and hence, functions. Necessarily, $[G_{i_1}(m_1)](n_1) = [G_{i_2}(m_2)](n_2)$. In other words, $\hat{G}_{i_1}(m_1, n_1) = \hat{G}_{i_2}(m_2, n_2)$; and so $G(i_1, m_1, n_1) = G(i_2, m_2, n_2)$. Indeed, G is now a function mapping from ω^3 to ω.

Sanity Check: Does this all make sense or we create some random functions?

1. Multiplication:

$$\begin{aligned} M_m(1) &= m && (2)\\ M_m(0) = 0 \quad &\text{and} \quad A_m(0) = m && (3)\\ M_m\left(n^+\right) &= M_m(n) + m \\ &= m + M_m(n) && \text{by Theorem 4K (2)} \\ &= A_m(M_m(n)) && (4) \end{aligned}$$

   Hence, $G_1(m) = M_m$ for all $m \in \omega$.

2. Exponentiation:

$$\begin{aligned} E_m(1) &= m && (2)\\ E_m(0) = 1 \quad &\text{and} \quad M_m(1) = m && (3)\\ E_m\left(n^+\right) &= E_m(n) \cdot m \\ &= m \cdot E_m(n) && \text{by Theorem 4K (5)} \\ &= M_m(E_m(n)) && (4) \end{aligned}$$

   Indeed, $G_2(m) = E_m$ for all $m \in \omega$.

3. Tetration:

$$\begin{aligned} T_m(1) &= m && (2)\\ T_m(0) = 1 \quad &\text{and} \quad E_m(1) = m && (3)\\ T_m\left(n^+\right) &= E_m(T_m(n)) && (4) \end{aligned}$$

   We see that $G_3(m) = T_m$ for all $m \in \omega$.

Ah yes, we are indeed sane still.

Exercises:

13. Let m and n be natural numbers such that $m \cdot n = 0$. Show that either $m = 0$ or $n = 0$. ✓

Assume $m \neq 0$ and $n \neq 0$. We shall show that $m \cdot n \neq 0$ in such cases. Let the set $S = \{k \in \omega \mid m \cdot k^+ \neq 0\}$. Since we know

$$\begin{aligned} m \cdot 0^+ &= m \cdot 0 + m && \text{(M2)} \\ &= 0 + m && \text{(M1)} \\ &= m + 0 && \text{by Theorem 4K (2)} \\ &= m && \text{(A1)} \\ &\neq 0 && \text{by assumption} \end{aligned}$$

thus $0 \in S$. If $k \in S$, then $k^+ \in S$. First let $T = \{p \in \omega \mid m + p \neq 0\}$. $m + 0 = m \neq 0$ by assumption, so $0 \in T$. When $p \in T$,

$$m + p^+ = (m + p)^+ \neq 0$$

because by Theorem 4D, 0 is not the successor of any natural number. Hence, $p^+ \in T$ and T is an inductive subset of ω. By the Induction Principle for ω, $T = \omega$; meaning the sum of any nonzero natural number with another natural number (possibly zero) is always nonzero. As such,

$$m \cdot k^{++} = m \cdot k^+ + m \neq 0 \quad \text{since } m \neq 0 \text{ by assumption}$$

Thence, $k^+ \in S$ and S is an inductive subset of ω. Again, by the Induction Principle for ω, $S = \omega$. Combined with the fact that for all nonzero $n \in \omega$, there exists some $k \in \omega$ such that $n = k^+$ by Theorem 4C; this means that for all nonzero $m, n \in \omega$, $m \cdot n \neq 0$. Taking the contrapositive of this conditional statement, we conclude that for all m, n; $m \cdot n = 0$ implies $m = 0$ or $n = 0$.

The converse is simple: Consider $n = 0$, then $m \cdot 0 = 0$ by (N1). If $m = 0$,

$$\begin{aligned} 0 \cdot n &= n \cdot 0 && \text{by Theorem 4K (5)} \\ &= 0 && \text{(M1)} \end{aligned}$$

Therefore, for all $m, n \in \omega$: If $m = 0$ or $n = 0$, then $m \cdot n = 0$.

Wherefore, we conclude that $m = 0$ or $n = 0$ iff $m \cdot n = 0$.

Remarks: Actually, instead of going the long route of proving $m + p \neq 0$ inductively and then concluding $m \cdot k^{++} = m \cdot k^+ + m \neq 0$ as a result, we can go a more direct path: By Theorem 4C, since $m \neq 0$, there exists some $\widehat{m} \in \omega$ so that $\widehat{m}^+ = m$. Consequently,

$$\begin{aligned} m \cdot k^{++} &= m \cdot k^+ + m \\ &= \widehat{m}^+ \cdot k^+ + \widehat{m}^+ \\ &= \left(\widehat{m}^+ \cdot k^+ + \widehat{m}\right)^+ \\ &\neq 0 && \text{by Theorem 4D} \end{aligned}$$

15. Complete the proof of part (1) of Thoerem 4K.

See Self-Proof of Theorem 4K.

16. Complete the proof of part (5) of Thoerem 4K.

See Self-Proof of Theorem 4K.

17. Prove that $m^{n+p} = m^n \cdot m^p$. ✓

Proof:

Let the set $S = \{p \in \omega \mid \forall m \forall n (n \in \omega \implies m^{n+p} = m^n \cdot m^p)\}$. We know

$$\begin{aligned}
m^{n+0} &= m^n && \text{(A1)} \\
&= m^n + 0 && \text{(A1)} \\
&= 0 + m^n && \text{by Theorem 4K (2)} \\
&= m^n \cdot 0 + m^n && \text{(M1)} \\
&= m^n \cdot 0^+ && \text{(M2)} \\
&= m^n \cdot 1 \\
&= m^n \cdot m^0 && \text{(E1)}
\end{aligned}$$

So, $0 \in S$. Suppose $p \in S$:

$$\begin{aligned}
m^{n+p^+} &= m^{(n+p)^+} && \text{(A2)} \\
&= m^{(p+n)^+} && \text{by Thoerem 4K (2)} \\
&= m^{p+n^+} && \text{(A2)} \\
&= m^{n^+ + p} && \text{by Thoerem 4K (2)} \\
&= m^{n^+} \cdot m^p && \text{as } p \in S \\
&= (m^n \cdot m) \cdot m^p && \text{(E2)} \\
&= m^n \cdot (m \cdot m^p) && \text{by Thoerem 4K (4)} \\
&= m^n \cdot (m^p \cdot m) && \text{by Thoerem 4K (5)} \\
&= m^n \cdot m^{p^+} && \text{(E2)}
\end{aligned}$$

Therefore, $p^+ \in S$. Now, S is an inductive subset of ω. Consequently, by the Induction Principle for ω, $S = \omega$. Wherefore, for all $m, n, p \in \omega$; $m^{n+p} = m^n \cdot m^p$.

1.3.5 Ordering on ω

Self-Proof of Lemma 4L: ✓

(a) ✓ Let the set $S = \{n \in \omega \,|\, \forall m\,[m \in \omega \implies (m \in n \iff m^+ \in n^+)]\}$. $m \in 0$ implies $m^+ \in 0^+$ is immediately vacuously true (for all natural m) since there exists no such $m \in 0$. Conversely,

$$m \in m^+ \in 0 \implies m \in 0 \quad \text{by Theorem 4F}$$

So, $m \in 0$ iff $m^+ \in 0^+$; meaning $0 \in S$. Whenever $n \in S$,

$$\begin{aligned} m \in n^+ &\implies m \in n \cup \{n\} \\ &\implies (m \in n \vee m = n) \\ &\implies \left(m^+ \in n^+ \vee m^+ = n^+\right) \quad \text{since } n \in S \\ &\implies m^+ \in n^+ \cup \left\{n^+\right\} \\ &\implies m \in n^{++} \end{aligned}$$

In addition,

$$\begin{aligned} m^+ \in n^{++} &\implies m \in n^+ \cup \left\{n^+\right\} \\ &\implies \left(m^+ \in n^+ \vee m^+ = n^+\right) \\ &\implies \left(m \in m^+ \in n^+ \;\vee\; m \in m^+ = n^+\right) \\ &\implies m \in n^+ \qquad \text{by Theorem 4F} \end{aligned}$$

Thus, $n^+ \in S$. Hence, S is an inductive subset of ω. By the Induction Principle for ω, $S = \omega$. Wherefore, for all $m, n \in \omega$: $m \in n$ iff $m^+ \in n^+$.

(b) ✓ Let the set $T = \{n \in \omega \,|\, n \notin n\}$. Since $\varnothing \notin \varnothing$ by definition, $0 \notin 0$ and therefore $0 \in T$. If $n \in T$: Assume $n^+ \in n^+$, then

$$\begin{aligned} n^+ \in n^+ &\implies n^+ \in n \cup \{n\} \\ &\implies \left(n^+ \in n \vee n^+ = n\right) \\ &\implies \left(n \in n^+ \in n \vee n \in n^+ = n\right) \\ &\implies n \in n \qquad \text{by Theorem 4F} \end{aligned}$$

However, $n \notin n$ since $n \in T$. Wherefore, by contradiction, $n^+ \notin n^+$. i.e. $n^+ \in T$, meaning T is an inductive subset of ω. By the Induction Principle for ω, $T = \omega$. Wherefore, for all $n \in \omega$: $n \notin n$.

Remarks: In part (a), for the $\impliedby$ direction, the simpler way is to first assume that $m^+ \in n^+$. Then we have $m \in m^+ \subseteq n$. Hence, by Theorem 4F, $m \in n$. In part (b) we could actually just have used part (a) to say $n \notin n \iff n^+ \notin n^+$ for the inductive step.

Self-Proof of Theorem 4N:

(i) Let the set $S = \{p \in \omega \,|\, \forall m \forall n[m, n \in \omega \implies (m \in n \iff m + p \in n + p)]\}$. We know that

$$m \in n \iff m + 0 \in n + 0 \quad \text{by (A1)}$$

Thus, $0 \in S$. Now, assume $p \in S$.

$$\begin{aligned} m \in n &\iff m + p \in n + p && \text{since } p \in S \\ &\iff (m + p)^+ \in (n + p)^+ && \text{by Lemma 4L (a)} \\ &\iff m + p^+ \in n + p^+ && \text{(A2)} \end{aligned}$$

So, $p^+ \in S$. i.e. S is an inductive subset of ω. Wherefore, by the Induction Principle for ω, $S = \omega$. Which means that for all $m, n, p \in \omega$: $m \in n$ iff $m + p \in n + p$.

(ii) Repeating a similar procedure; let the set $S' = \{p \in \omega \,|\, \forall m \forall n[(m, n \in \omega \wedge p \neq 0) \implies (m \in n \iff m \cdot p \in n \cdot p)\}$. $0 \in S'$ immediately holds true by the definition of a conditional statement. Suppose that $p \in S'$, then

$$\begin{aligned} m \in n &\iff m \cdot p \in n \cdot p && \text{since } p \in S' \\ &\iff m \cdot p + m \in n \cdot p + n && \text{by (i)} \\ &\iff m \cdot p^+ \in n \cdot p^+ && \text{(M2)} \end{aligned}$$

So, $p^+ \in S'$. i.e. S' is an inductive subset of ω. Wherefore, by the Induction Principle for ω, $S' = \omega$. Which means that for all $m, n, p \in \omega$: $m \in n$ iff $m \cdot p \in n \cdot p$.

Q.E.D. ■

Self-Proof of Corollary 4P:

If $m + p = n + p$, then neither $m + p \in n + p$ nor $n + p \in m + p$ are true by the Trichotomy Law for ω. Hence, utilising Theorem 4N, both $m \in n$ and $n \in m$ are false. Consequently, again with aid of the Trichotomy Law for ω, $m = n$ must be true since the other two options are provably false (as shown above).

Alternatively, if we prefer a presentation with symbols instead;

$$\begin{aligned} m + p = n + p &\implies (m + p \notin n + p \wedge n + p \notin m + p) && \text{by the Trichotomy Law for } \omega \\ &\implies (m \notin n \wedge n \notin m) && \text{by Theorem 4N} \\ &\implies m = n && \text{by the Trichotomy Law for } \omega \end{aligned}$$

Now, for multiplication, we repeat the above procedure similarly. Assume $m \cdot p = n \cdot p$ and $p \neq 0$. Then, it follows from the Trichotomy Law for ω, that $m \cdot p \notin n \cdot p$ and $n \cdot p \notin m \cdot p$. Using Theorem 4N, both $m \in n$ and $n \in m$ are certainly false. Wherefore, again with the Trichotomy Law for ω, we know $m = n$ holds true since the other two options are false.

Again, symbolically: Suppose $p \neq 0$, then

$$\begin{aligned} m \cdot p = n \cdot p &\implies (m \cdot p \notin n \cdot p \wedge n\dot{p} \notin m \cdot p) && \text{Trichotomy Law for } \omega \\ &\implies (m \notin n \wedge n \notin m) && \text{Theorem 4N} \\ &\implies m = n && \text{Trichotomy Law for } \omega \end{aligned}$$

Note that now we have proven the statement that

$$p \neq 0 \implies (m \cdot p = n \cdot p \implies m = n)$$

We can rewrite it equivalently into the desired form in Corollary 4P,

$$\begin{aligned}
[p \neq 0 \implies (m \cdot p = n \cdot p \implies m = n)] &\iff [\neg(p \neq 0) \vee (m \cdot p = n \cdot p \implies m = n)] \\
&\iff [\neg(p \neq 0) \vee [\neg(m \cdot p = n \cdot p) \vee m = n]] \\
&\iff [\neg\neg[\neg(p \neq 0) \vee \neg(m \cdot p = n \cdot p)] \vee m = n] \\
&\iff [\neg[p \neq 0 \wedge m \cdot p = n \cdot p] \vee m = n] \\
&\iff [(m \cdot p = n \cdot p \wedge p \neq 0) \implies m = n]
\end{aligned}$$

We can hence conclude that $(m \cdot p = n \cdot p \wedge p \neq 0) \implies m = n$ is true.

Q.E.D. ■

Self-Proof of Corollary 4Q: (Saw a bit of Enderton's proof but whatever)

Assume that there exists such a function $f : \omega \to \omega$ so that $f(n^+) \in f(n)$ for every natural number n. We see that for all $m \in \operatorname{ran} f$, there exists $n \in \operatorname{ran} f$ with $n \in m$.

$$\begin{aligned}
m \in \operatorname{ran} f &\implies \exists k(f(k) = m) \\
&\implies \exists k\left[f\left(k^+\right) \in f(k)\right] \qquad \text{by the definition of } f \\
&\implies \exists n[n \in \operatorname{ran} f \wedge n \in m]
\end{aligned}$$

Thus, we know that its negation — there exists $m \in \operatorname{ran} f$ for all $n \in \operatorname{ran} f$ so that $\neg(n \in m)$ — must be false. The last bit can be rewritten using the Trichotomy Law for ω as $m \subseteq n$. Whence, there does not exist a least element in $\operatorname{ran} f$, which is a subset of ω, by definition. Wherefore, by contradiction with the Well Ordering of ω, there indeed exists no such function.

Q.E.D. ■

Self-Proof of the Strong Induction Principle for ω:

Assume that the Strong Induction Principle for ω is false, i.e. there exists some $A \subseteq \omega$ so that for every n in ω, if every number less than n is in A, then $n \in A$. But suppose that, however, $A \neq \omega$.

By the Well Ordering of ω, we know that there exists some (natural) least element m of $\omega \setminus A$. Thus, for all natural $k \in m$, $k \notin \omega \setminus A$, lest there exist some $k \in \omega \setminus A$ with $k \in m$, which would mean m is not the least element of $\omega \setminus A$. So, for all natural $k \in m$, $k \in A$. However, by the Strong Induction Hypothesis — that for every $n \in \omega$, if every number less than n is in A, then $n \in A$ — we know that $m \in A$. This contradicts our previous fact that $m \in \omega \setminus A$. Wherefore, by contradiction, the Strong Induction Principle for ω certainly is true.

Q.E.D. ■

Exercises:

18. Simplify: $\in_\omega^{-1} [\![\{7,8\}]\!]$.

Answer:

$$\begin{aligned}\in_\omega^{-1} [\![\{7,8\}]\!] &= \{\langle m,n\rangle \,|\, m \in \{7,8\} \wedge n \in_\omega m\} \\ &= \{\langle 8,7\rangle, \langle 8,6\rangle, \ldots, \langle 8,0\rangle, \langle 7,6\rangle, \langle 7,5\rangle, \ldots, \langle 7,0\rangle\}\end{aligned}$$

20. Let A be a nonempty subset of ω such that $\bigcup A = A$. Show that $A = \omega$.

Proof:

Assume there exists some nonempty subset A of ω so that $\bigcup A = A$ but $A \neq \omega$. By the Well Ordering of ω, there exists some least element m of $\omega \setminus A$. There either exists some $k \in A$ with $m \in k$ or for all $k \in A$, $m \notin k$.

In the first case, $m \in k \in A$, so $m \in \bigcup A = A$. However, this contradicts our assumption that $m \in \omega \setminus A$.

As for the latter; first note there exists some $n \in \omega$ with $n^+ = m$ by Theorem 4C. In fact, more specifically $n \in A$, lest $n \in m$ for some $n \in \omega \setminus A$. Notice that for all $\widehat{k} \in A$, $\widehat{k} \subseteq n$: Suppose otherwise. Then, it is false that for all $\widehat{k} \in A$, $\widehat{k} \in n^+$. Thus, it is true that there exists $\widehat{k} \in A$ with $\widehat{k} \notin n^+$. By the Trichotomy Law for ω, $m = n^+ \subseteq \widehat{k}$. Since $m \notin A$ while $\widehat{k} \in A$, it must be that $m \in \widehat{k}$. However, this contradicts our presumption for this latter case, that for all $k \in A$, $m \notin k$. So, it must be true that for all $\widehat{k} \in A$, $n \subseteq \widehat{k}$. Again from the Trichotomy Law for ω, this means $n \notin \widehat{k}$. (Notice that this is the negation of there exists $\widehat{k} \in A$ with $n \in \widehat{k}$.) Consequently, $n \notin \bigcup A = A$. But this contradicts the fact we established earlier that $n \in A$.

Wherefore, since in both cases we arrive at a contradiction, it must be that for all nonempty subsets A of ω, if $\bigcup A = A$, then $A = \omega$.

Q.E.D. ■

26. Assume that $n \in \omega$ and $f : n^+ \to \omega$. Show that $\operatorname{ran} f$ has a largest element.

Proof:

We first construct the set of all natural numbers not smaller than or equal to some number in $\operatorname{ran} f$; i.e. $\omega \setminus (\operatorname{ran} f \cup \bigcup \operatorname{ran} f)$. By the Well Ordering of ω, there exists some least element m of $\omega \setminus (\operatorname{ran} f \cup \bigcup \operatorname{ran} f)$.

We know $\operatorname{ran} f$ is nonempty, because: for all $\kappa \in n^+$, there exists $k \in \operatorname{ran} f$. So, since $n^+ \neq 0 = \varnothing$ by Theorem 4D, there must exist some $k \in \operatorname{ran} f$. Since $\operatorname{ran} f \neq \varnothing$, $0 \in \operatorname{ran} f \cup \bigcup \operatorname{ran} f$:

Let the set $S = \{k \in \omega \,|\, 0 \subseteq k\}$. By definition, $0 \in S$. Suppose $k \in S$. If $k = 0$, $0 \in k^+$. When $0 \in k$, $0 \in k^+$. Thus, $k^+ \in S$ and S is an inductive subset of ω. By the Induction Principle for ω, $S = \omega$. As $\operatorname{ran} f \neq \varnothing$ (and is a subset of ω): Either $0 \in \operatorname{ran} f$. Or for all $k \in \operatorname{ran} f$ (of which there exists at least 1), $k \neq 0$ and $0 \in k \in \operatorname{ran} f$, so $0 \in \bigcup \operatorname{ran} f$. Regardless, $0 \in \operatorname{ran} f \cup \bigcup \operatorname{ran} f$ is true.

Consequently, $m \neq 0$ since $m \notin \operatorname{ran} f \cup \bigcup \operatorname{ran} f$. Therefore, there exists $\widetilde{n} \in \omega$ with $\widetilde{n}^+ = m$ by Theorem 4C. As $n \in m$, $m \in n$ is false by the Trichotomy Law for ω. As a result, $n \in \operatorname{ran} f \cup \bigcup \operatorname{ran} f$.

We claim that $\widetilde{n}$ is the largest element of $\operatorname{ran} f \cup \bigcup \operatorname{ran} f$. Assume otherwise. Then, it is false that for all $k \in \operatorname{ran} f \cup \bigcup \operatorname{ran} f$, $k \subseteq \widetilde{n}$. Accordingly, it is also that false for all $k \in \operatorname{ran} f \cup \bigcup \operatorname{ran} f$, $k \in \widetilde{n}^+$. It is then true that there exists $k \in \operatorname{ran} f \cup \bigcup \operatorname{ran} f$ with $k \notin \widetilde{n}^+$. By the Trichotomy Law for ω, $\widetilde{n}^+ \subseteq k$. In other words, $m \subseteq k$. Since $m \notin \operatorname{ran} f \cup \bigcup \operatorname{ran} f$, $m \in k$. Now, either $m \in k \in \operatorname{ran} f$ or $m \in k \in \bigcup \operatorname{ran} f$. In the latter, there exists $\widehat{k}$ such that $m \in k \in \widehat{k} \in \operatorname{ran} f$. By Theorem 4F, $m \in \widehat{k} \in \operatorname{ran} f$. Thence, in both cases, $m \in \bigcup \operatorname{ran} f$. Clearly, this contradicts the fact that $m \notin \operatorname{ran} f \cup \bigcup \operatorname{ran} f$. Whence, it must be that $\widetilde{n}$ is the largest element of $\operatorname{ran} f \cup \bigcup \operatorname{ran} f$.

It must be that $n \in \operatorname{ran} f$, because if it is in $\bigcup \operatorname{ran} f$, then there exists some $k \in \operatorname{ran} f$ such that $\widetilde{n} \in k$. By the Trichotomy Law for ω, $k \notin \widetilde{n}$. Which contradicts the established fact that $\widetilde{n}$ is the largest element of $\operatorname{ran} f \cup \bigcup \operatorname{ran} f$. Hence, $\widetilde{n} \in \operatorname{ran} f$ holds true.

Wherefore, $\widetilde{n}$ is indeed the largest element of $\operatorname{ran} f$.

Q.E.D. ■

27. Assume that A is a set, G is a function, and f_1 and f_2 map ω into A. Further assume that for each n in ω both $f_1 \restriction n$ and $f_2 \restriction n$ belong to $\operatorname{dom} G$ and

$$f_1(n) = G(f_1 \restriction n) \;\&\; f_2(n) = G(f_2 \restriction n).$$

Show that $f_1 = f_2$.

Proof:

Let the set $S = \{n \in \omega \mid f_1(n) = f_2(n)\}$. If every number less than n is in S, then for all $k \in n$: $f_1(k) = f_2(k)$. Hence, $f_1 \restriction n = \{\langle k, f_1(k)\rangle \mid k \in n\} = \{\langle k, f_2(k)\rangle \mid k \in n\} = f_2 \restriction n$. Consequently, $n \in S$ since $f_1(n) = G(f_1 \restriction n) = G(f_2 \restriction n) = f_2(n)$. By the Strong Inducion Principle for ω, $S = \omega$. Wherefore; $f_1 = \{\langle n, f_1(n)\rangle \mid n \in \omega\} = \{\langle n, f_2(n)\rangle \mid n \in \omega\} = f_2$.

Q.E.D. ■

1.4 Construction of The Real Numbers

*Note that from here on out, we will use Theorem 4K without stating it. (No real point to do so)

1.4.1 Integers

Self-Proof of Theorem 5ZA:

Clearly, by Thoerem 4K (2), we have $m+n=n+m$ for all natural m and n. Thus, $\langle m,n\rangle \sim \langle m,n\rangle$, and hence, $\sim$ is reflexive on $\omega\times\omega$. If $\langle m,n\rangle \sim \langle p,q\rangle$, then we know $m+q=p+n$ by definition. Which can be rewritten as $p+n=m+q$. Thus, $\langle p,q\rangle \sim \langle m,n\rangle$ immediately follows. So, $\sim$ is symmetric. Lastly, assume $\langle m,n\rangle \sim \langle p,q\rangle$ and $\langle p,q\rangle \sim \langle r,s\rangle$. In other words, $m+q=p+n$ and $p+s=r+q$. Whence,

$$\begin{aligned} m+q+p+s &= p+n+r+q \\ m+s &= r+n \qquad \text{by Corollary 4P} \end{aligned}$$

Consequently, $\langle m,n\rangle \sim \langle r+s\rangle$; meaning $\sim$ is transitive.

Wherefore, since the relation $\sim$ is reflexive on $\omega\times\omega$, symmetric, and transitive, $\sim$ indeed is an equivalence relation.

Q.E.D. ■

Self-Proof of Lemma 5ZB:

Assume that $\langle m,n\rangle \sim \langle m',n'\rangle$ and $\langle p,q\rangle \sim \langle p',q'\rangle$. Thus, we know that $m+n'=m'+n$ and $p+q'=p'+q$. Summing them up, we get that

$$\begin{aligned} m+n'+p+q' &= m'+n+p'+q \\ m+p+n'+q &= m'+p'+n+q \end{aligned}$$

Consequently, $\langle m+p,n+q\rangle \sim \langle m'+p',n'+q'\rangle$ by definition.

Q.E.D. ■

Self-Proof of Commutativity for Theorem 5ZF:

By definition, for any integers a and b, there exists natural numbers m, n, p, and q with $a=[\langle m,n\rangle]$ and $b=[\langle p,q\rangle]$. Therefore,

$$\begin{aligned} a\cdot_{\mathbb{Z}} b &= [\langle m,n\rangle]\cdot_{\mathbb{Z}}[\langle p,q\rangle] \\ &= [\langle mp+nq, mq+np\rangle] \\ &= [\langle pm+qn, pn+qm\rangle] \\ &= [\langle p,q\rangle]\cdot_{\mathbb{Z}}[\langle m,n\rangle] \\ &= b\cdot_{\mathbb{Z}} a. \end{aligned}$$

Which means that, the multiplication operation $\cdot_{\mathbb{Z}}$ is commutative indeed.

Q.E.D. ■

Self-Proof of Theorem 5ZG:

(a) By definition, for any integer a, there exists natural numbers m and n with $a=[\langle m,n\rangle]$. So,

$$\begin{aligned} a\cdot_{\mathbb{Z}} 1_{\mathbb{Z}} &= [\langle m,n\rangle]\cdot_{\mathbb{Z}}[\langle 1,0\rangle] \\ &= [\langle m\cdot 1+n\cdot 0, m\cdot 0+n\cdot 1\rangle] \\ &= [\langle m,n\rangle] \\ &= a \end{aligned}$$

Thus, as desired, the integer $1_{\mathbb{Z}}$ is the multiplicative identity.

(b) Since $0+0=0$ while $1+0=1$, we know $0+0 \neq 1+0$. Therefore, $\langle 0,0\rangle \sim \langle 1,0\rangle$ is false. Hence, it is indeed true that $0_{\mathbb{Z}} \neq 1_{\mathbb{Z}}$.

(c) Let $a \neq 0_{\mathbb{Z}}$ and $b \neq 0_{\mathbb{Z}}$. Then, there exists nonzero natural numbers m, n, p, and q such that $a = [\langle m,n\rangle]$ and $b = [\langle p,q\rangle]$. As a result,

$$\begin{aligned} a \cdot_{\mathbb{Z}} b &= [\langle m,n\rangle] \cdot_{\mathbb{Z}} [\langle p,q\rangle] \\ &= [\langle mp+nq, mq+np\rangle]. \end{aligned}$$

By exercise 13 of chapter 4, we know that mp, nq, mq, np are all nonzero. Whence, first notice that there exists $\alpha, \beta \in \omega$ with $\alpha^+ = nq$ and $\beta^+ = np$ by Theorem 4C. We now know that $\langle mp+\alpha^+, mq+\beta^+\rangle = [\langle (mp+\alpha)^+, (mq+\beta)^+\rangle]$ (by (A2)); where $(mp+\alpha)^+$ and $(mq+\beta)^+$ are certainly nonzero by Theorem 4D.

Consequently, we conclude that for all integers a and b; $a \cdot_{\mathbb{Z}} b \neq [\langle 0,0\rangle] = 0_{\mathbb{Z}}$. Taking the contrapositive of this conditional statement, we know that for all m and n, $a \cdot_{\mathbb{Z}} b = 0$ implies $a = 0_{\mathbb{Z}}$ or $b = 0_{\mathbb{Z}}$.

Q.E.D. ■

Remarks: Note that $[\langle m,m\rangle] = [\langle 0,0\rangle] = 0_{\mathbb{Z}}$! So, we actually have not proven that $a \cdot_{\mathbb{Z}} \neq 0_{\mathbb{Z}}$. Instead, what we could do is something like the following by Enderton:

Since $a \neq [\langle 0,0\rangle]$, we have $m \neq n$. So either $m \in n$ or $n \in m$. Similarly, either $p \in q$ or $q \in p$. This leads to a total of four cases, but in each case we have

$$mp+nq \neq mq+np$$

by Exercise 25 of Chapter 4. Hence, $a \cdot_{\mathbb{Z}} b \neq [\langle 0,0\rangle]$.

~~In my defense, it was 11 already. *Copes harder*~~

Self-Proof of Theorem 5ZI:

For all integers a and b, there exists natural numbers m, n, p, and q with $a = [\langle m,n\rangle]$ and $b = [\langle p,q\rangle]$ by definition. So, exactly one of the following is true by the Trichotomy Law for ω.

$$m+q = p+n, \quad m+q \in p+n, \quad \text{or} \quad p+n \in m+q.$$

Which also equivalently means that exactly one of the below options is true

$$[\langle m,n\rangle] = [\langle p,q\rangle], \quad [\langle m,n\rangle] <_{\mathbb{Z}} [\langle p,q\rangle], \quad \text{or} \quad [\langle p,q\rangle] <_{\mathbb{Z}} [\langle m,n\rangle].$$

Therefore, $<_{\mathbb{Z}}$ satisfies trichotomy on $\mathbb{Z}$ because one and only one of these are true:

$$a = b, \quad a <_{\mathbb{Z}} b, \quad \text{or} \quad b <_{\mathbb{Z}} a.$$

Also, for any integer c, there exists the natural numbers r, and s so $c = [\langle r,s\rangle]$. As a result, when $a <_{\mathbb{Z}} b$ and $b <_{\mathbb{Z}} c$, $m+q \in p+n$ and $p+s \in r+q$. Adding an s and an r respectively to each, we get that $m+q+s \in p+n+s$ and $p+s+n \in r+q+n$. By Theorem 4F, $m+q+s \in r+q+n$. Via Theorem 4N, we conclude that $m+s \in r+n$. i.e. $<_{\mathbb{Z}}$ is transitive since $[\langle m,n\rangle] <_{\mathbb{Z}} [\langle r,s\rangle]$.

Wherefore, since $<_{\mathbb{Z}}$ satisfies trichotomy on $\mathbb{Z}$ and is transitive, $<_{\mathbb{Z}}$ must be a linear ordering relation on $\mathbb{Z}$.

Q.E.D. ■

Self-Proof of Corollary 5ZK:

(a) Since $a +_{\mathbb{Z}} c = b +_{\mathbb{Z}} c$, thus we know that both $a +_{\mathbb{Z}} c <_{\mathbb{Z}} b +_{\mathbb{Z}} c$ and $b +_{\mathbb{Z}} c <_{\mathbb{Z}} a +_{\mathbb{Z}} c$ are by trichotomy (since $<_{\mathbb{Z}}$ is a linear ordering from Theorem 5ZI). Now, by Theorem 5ZJ (a), we know that the following are both false: $a <_{\mathbb{Z}} b$ and $b <_{\mathbb{Z}} a$. Wherefore, again by trichotomy, it must be that $a = b$.

(b) We apply a similar procedure as used in the above proof of (a). Assume $c \neq 0_{\mathbb{Z}}$ and $a \cdot_{\mathbb{Z}} c = b \cdot_{\mathbb{Z}} c$. Accordingly, by trichotomy, both $a \cdot_{\mathbb{Z}} c <_{\mathbb{Z}} b \cdot_{\mathbb{Z}} c$ and $b \cdot_{\mathbb{Z}} c <_{\mathbb{Z}} a \cdot_{\mathbb{Z}} c$ are false. Which then means $a <_{\mathbb{Z}} b$ and $b <_{\mathbb{Z}} a$ are false too by Theorem 5ZJ (b). Wherefore, utilising trichotomy one last time, it must be true that $a = b$.

Q.E.D. ■

Exercises:

3. Is there a function $H\colon \mathbb{Z} \to \mathbb{Z}$ satisfying the equation

$$H([\langle m, n\rangle]) = [\langle n, m\rangle]?$$

Answer:

We construct the set $H = \{\langle [\langle m, n\rangle], [\langle n, m\rangle]\rangle \mid m, n \in \omega\}$ by some applying a subset axiom to $\mathbb{Z} \times \mathbb{Z}$.

Now, we verify that it is a (well-defined) function. Let $\langle m, n\rangle \sim \langle p, q\rangle$, meaning $m + q = p + n$. Clearly, $n + p = q + m$, which means that $\langle n, m\rangle \sim \langle q, p\rangle$. Consequently, we see that

$$\begin{aligned} H([\langle m, n\rangle]) &= [\langle n, m\rangle] \\ &= [\langle q, p\rangle] \qquad \text{by the above fact} \\ &= H([\langle p, q\rangle]). \end{aligned}$$

Thence, it is indeed a function, which clearly also satisfies the given equation. Wherefore, such a function indeed exists (we just constructed one).

5. Give a formula for subtraction of integers:

$$[\langle m, n\rangle] - [\langle p, q\rangle] = ?$$

Answer:

By the definition given earlier about the subtraction of integers, namely that:

$$b - a = b +_{\mathbb{Z}} (-a) \quad \text{for any integers } a \text{ and } b,$$

we see that

$$\begin{aligned} [\langle m, n\rangle] - [\langle p, q\rangle] &= [\langle m, n\rangle] + (-[\langle p, q\rangle]) \\ &= [\langle m, n\rangle] +_{\mathbb{Z}} [\langle q, p\rangle] \\ &= [\langle m + p, q + n\rangle] \end{aligned}$$

So, our formula for the subtraction of integers is

$$[\langle m, n\rangle] - [\langle p, q\rangle] = [\langle m + p, q + n\rangle].$$

8. Prove parts (a), (b), and (c) of Theorem 5ZL.

Proof:

(a)

$$\begin{aligned} E(m) +_{\mathbb{Z}} E(n) &= [\langle m, 0\rangle] + [\langle n, 0\rangle] \\ &= [\langle m + n, 0\rangle] \\ &= E(m + n) \end{aligned}$$

(b)

$$\begin{aligned} E(m) \cdot_{\mathbb{Z}} E(n) &= [\langle m, 0\rangle] \cdot_{\mathbb{Z}} [\langle n, 0\rangle] \\ &= [\langle mn + 0 \cdot 0, m \cdot 0 + 0 \cdot n\rangle] \\ &= [\langle mn, 0\rangle] \\ &= E(mn) \end{aligned}$$

(c) Assume $m \in n$. Then, clearly $m + 0 \in n + 0$. Hence, $[\langle m, 0\rangle] <_{\mathbb{Z}} [\langle n, 0\rangle]$.

Consider the converse, first supposing that $[\langle m, 0\rangle] <_{\mathbb{Z}} [\langle n, 0\rangle]$. By definition, $m + 0 \in n + 0$. Which is simplified to $m \in n$, as desired.

Wherefore, we can now conclude that $m \in n$ iff $E(m) <_{\mathbb{Z}} E(n)$.

Q.E.D. ■

9. Show that

$$[\langle m, n\rangle] = E(m) - E(n)$$

for all natural numbers m and n.

Proof:

We see that

$$\begin{aligned} E(m) - E(n) &= [\langle m, 0\rangle] +_{\mathbb{Z}} (-[\langle n, 0\rangle]) \\ &= [\langle m, 0\rangle] +_{\mathbb{Z}} [\langle 0, n\rangle] \\ &= [\langle m + 0, 0 + n\rangle] \\ &= [\langle m, n\rangle] \end{aligned}$$

as desired.

Q.E.D. ■

1.4.2 Rational Numbers

Self-Proof of Theorem 5QA:

Reflexivity on $\mathbb{Z} \times \mathbb{Z}'$: Assume that $\langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z}'$. Then, it clearly holds that $a \cdot b = a \cdot b$. Which now means that $\langle a, b\rangle \sim \langle a, b\rangle$; i.e. $\sim$ is indeed reflexive on $\mathbb{Z} \times \mathbb{Z}'$.

Symmetry: Let $\langle a, b\rangle \sim \langle c, d\rangle$. It follows that $a \cdot d = c \cdot b$. Immediately, $c \cdot b = a \cdot d$ must hold true too. Thus, $\langle c, d\rangle \sim \langle a, b\rangle$ by definition; and so $\sim$ is symmetric.

Transitivity: Suppose that $\langle a, b\rangle \sim \langle c, d\rangle$ and $\langle c, d\rangle \sim \langle e, f\rangle$. This means that $a \cdot d = c \cdot b$ and $c \cdot f = e \cdot d$. Accordingly, $a \cdot d \cdot f = c \cdot b \cdot f$ and $c \cdot f \cdot b = e \cdot d \cdot b$. By Theroem 5ZF, $a \cdot f \cdot d = c \cdot b \cdot f$ and $c \cdot b \cdot f = e \cdot b \cdot d$. Consequently, $a \cdot f \cdot d = e \cdot b \cdot d$. By Corollary 5ZK (as $d \in \mathbb{Z}'$ is nonzero), $a \cdot f = e \cdot b$. Therefore, $\langle a, b\rangle \sim \langle e, f\rangle$. We can conclude that $\sim$ is transitive.

Wherefore, since the relation $\sim$ is reflexive on $\mathbb{Z} \times \mathbb{Z}'$, symmetric, and transitive, it is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}'$.

Q.E.D. ■

Self-Proof of Corollary 5QG:

Assume r and s are nonzero rational numbers, i.e. there exists the nonzero integers a, b, c, and d so that $r = [\langle a, b\rangle]$ and $s = [\langle c, d\rangle]$. Thus, $[\langle a, b\rangle] \cdot_{\mathbb{Z}} [\langle c, d\rangle] = [\langle ac, bd\rangle]$. Since a and c are nonzero, $ac \neq 0$ by the contrapositive of Theorem 5ZG (c). Consequently, $ac \cdot 1 \neq 0 \cdot bd$, lest $ac = 0$. Which implies that $\langle ac, bd\rangle \not\sim 0_{\mathbb{Q}}$. In other words, $r \cdot s$ is nonzero.

Q.E.D. ■

Self-Proof of Lemma 5QH:

By assumption, $\langle a, b\rangle \sim \langle a', b'\rangle$ and $\langle c, d\rangle \sim \langle c'd'\rangle$, where b, b', d, and d' are all positive. So, we know that $ab' = a'b$ and $cd' = c'd$. Then,

$$\begin{aligned}
ad < cb &\iff adb'd' < cbb'd' \\
&\iff ab'dd' < cd'bb' && \text{by Theorem 5ZF} \\
&\iff a'bdd' < c'dbb && \text{since } ab' = a'b \text{ and cd'=c'd} \\
&\iff a'd'bd < c'b'bd && \text{by Theorem 5ZF} \\
&\iff a'd' < c'b' && \text{by Theorem 5ZJ (b)}
\end{aligned}$$

Wherefore, indeed $ad < cd$ iff $a'd' < c'b'$.

Q.E.D. ■

Self-Proof of Thereom 5QI:

Trichotomy (on $\mathbb{Q}$): By Theroem 5ZI, exactly one of the following are true:

$$ad = cb, \quad ad < cb, \quad or \quad cb < ad.$$

Which means that one and only one of the below is true

$$r = s, \quad r < s, \quad or \quad s < r.$$

Thus, $<_{\mathbb{Q}}$ satisfies trichotomy on $\mathbb{Q}$.

Transitivity: Assume that $p <_{\mathbb{Q}} q$ and $q <_{\mathbb{Q}} r$. By definition, there exists the integers a, c, e, as well as the positive integers b, d, and e with $p = [\langle a, b\rangle]$, $q = [\langle c, d\rangle]$, and $r = [\langle e, f\rangle]$; such that $ad < cb$ and $cf < ed$. Consequently, we know that

$$adf < cbf \quad \text{and} \quad cfb < edb$$

by Theorem 5ZJ (b) (since b and f are nonzero). With Theorem 5ZF, we can rearrange the above (equivalently) as

$$afd < cbf \quad \text{and} \quad cbf < ebd.$$

Now, by Theorem 5ZI (transitivity of $<$), $afd < ebd$. Finally, utilising Theroem 5ZJ (b) (as d is nonzero), we conclude that $af < eb$. As a result, $p <_{\mathbb{Q}} r$ and transitivity holds.

Wherefore, we clearly see that $<_{\mathbb{Q}}$ must be a linear ordering on $\mathbb{Q}$.

Q.E.D. ■

Exercises:

11. Give a direct proof (not using Theorem 5QF) that if $r \cdot_{\mathbb{Q}} s = 0_{\mathbb{Q}}$, then either $r = 0_{\mathbb{Q}}$ or $s = 0_{\mathbb{Q}}$.

    Proof. See my Self-Proof of Corollary 5QG, as this is the contrapositive of Corollary 5QG.

12. Show that
$$r <_{\mathbb{Q}} 0_{\mathbb{Q}} \quad \text{iff} \quad 0_{\mathbb{Q}} <_{\mathbb{Q}} -r.$$

    Proof.

    Let r be a rational number. In other words, $r = [\langle a, b\rangle]$ for some integer a and nonzero integer b. Then,

$$\begin{aligned} r <_{\mathbb{Q}} 0_{\mathbb{Q}} &\iff a \cdot 1 < 0 \cdot b \\ &\iff a < 0 \\ &\iff a - a < -a \qquad \text{by Theorem 5ZD (b)} \\ &\iff 0 < -a \\ &\iff 0 \cdot b < -a \cdot 1 \\ &\iff 0 <_{\mathbb{Q}} r. \end{aligned}$$

    Thus, we have shown that indeed $r <_{\mathbb{Q}} 0_{\mathbb{Q}}$ iff $0_{\mathbb{Q}} <_{\mathbb{Q}} -r$.

    Q.E.D. ■

14. Show that the ordering of the rationals is dense, i.e., between any two rationals there is a third one:
$$p <_{\mathbb{Q}} s \implies \exists r(p <_{\mathbb{Q}} r <_{\mathbb{Q}} s).$$

    Proof.

    Let $p <_{\mathbb{Q}} s$. We can write $p = [\langle a, b\rangle]$ and $s = [\langle c, d\rangle]$ for some integers a, c, and positive integers b, d so that $ad < cb$.

    Now we construct the rational number $r = [\langle a + c, b + d\rangle]$. As addition (of integers) preserves order by Theorem 5ZJ, we see that
$$ab + ad < cb + ad \quad \text{and} \quad ad + cd < cb + cd.$$

    Consequently, we apply the commutative of integer addition from Theorem 5ZC to restate the above equivalently as
$$ab + ad < ad + cb \quad \text{and} \quad ad + cd < cb + cd.$$

    Hence, since for integers, multiplication distributes over addition by Theorem 5ZF;
$$a(b + d) < (a + c)b \quad \text{and} \quad (a + c)d < c(b + d).$$

    Wherefore, we can conclude that $p <_{\mathbb{Q}} r <_{\mathbb{Q}} s$ indeed.

    Q.E.D. ■

1.4.3 Real Numbers

Self-Proof of Theorem 5RA:

Transitivity: Let $x <_{\mathbb{R}} y$ and $y <_{\mathbb{R}} z$. We then know that $x \subset y$ and $y \subset z$ by definition. Thus, all elements of x are in y, and hence, in z too. In addition, (as $y \subset z$) there exists an element of z that is not in y, and so, not in x as well. Consequently, $x \subset z$, i.e. $x <_{\mathbb{R}} z$. Which means that $<_{\mathbb{R}}$ is transitive.

Trichotomy on $\mathbb{R}$: Assume that for real numbers x and y, there exists $r \in x$ with $r \notin y$ and there exists $q \in y$ so $q \notin x$. By the trichotomy of $<$ (Theorem 5QI), exactly one of

$$q < r, \quad q = r, \quad r < q$$

is true. We now evaluate them casewise using the fact that x and y are closed downwards:

1. When $q < r$, then $q \in x$.
2. If $q = r$, then immediately, they are elements of both x and y.
3. Whenever $r < q$, it follows that $r \in y$.

In any case, it contradicts our original assumption that $q \notin x$ and $r \notin y$. Therefore, it must be true that for all $r \in x$, $r \in y$, or for all $q \in y$, $q \in x$. In other words, either

$$x \subseteq y \quad \text{or} \quad y \subseteq x.$$

Which is the same as saying

$$x \subset y \quad \text{or} \quad x = y \quad \text{or} \quad y \subset x.$$

Now, we see that only one of the above holds true; lest $x \subset x$, $y \subset y$ or $x \subset y \subset x$, which implies $x \subset x$. Hence, $<_{\mathbb{R}}$ satisfies trichotomy on $\mathbb{R}$.

Wherefore, the relation $<_{\mathbb{R}}$ is indeed a linear ordering on $\mathbb{R}$.

Q.E.D. ■

Self-Proof of Theorem 5RB:

Let S be a bounded nonempty subset of $\mathbb{R}$, and U be the set of all upper bounds of S. We claim that $\bigcap U$ is a least upper bound in $\mathbb{R}$:

(a) Since S is nonempty, there exists one $x \in S$ that is itself nonempty by definition. Hence there is some $q \in x$. By definition, for all $x \in S$ and $b \in U$, $x \leq_{\mathbb{R}} b$. Which is the same as saying $x \subseteq b$. Thus, $q \in b$ for all $b \in U$. In other words, $q \in \bigcap U$; meaning $\bigcap U \neq \varnothing$. We also know, all upper bounds of S must be real numbers. That is, all of them are proper subsets of $\mathbb{Q}$. Therefore, $\bigcap U \subset \mathbb{Q}$ as well. In sum, we have shown that $\varnothing \neq \bigcap U \neq \mathbb{Q}$, and that $\bigcap U$ is a subset of $\mathbb{Q}$ in this paragraph.

(b) Now, (for any rational numbers p and q) if $q \in \bigcap U$ and $p < q$, then for all $b \in S$, $q \in b$ and $p < q$. Since b is real, it is closed downwards. Consequently, $p \in b$ (again, for all $b \in S$). Thence, $p \in \bigcap U$. We see that $\bigcap U$ is also closed downwards.

(c) Given any $r \in b \in U$, there must exist $q \in b$ with $r < q$ since the real numbers b have no largest element. Accordingly, this can be immediately rephrased into: for all $r \in \bigcap U$, there exists $q \in \bigcap U$ so that $r < q$. Whence, $\bigcap U$ is closed downwards.

As a result, we conclude that $\bigcap U$ is a real number. We need to lastly show that $\bigcap U$ is the *least* upper bound:

Clearly, for any $b \in U$, $\bigcap U \subseteq b$. Thereupon, we see that $\bigcap U \leq_{\mathbb{R}} b$ by definition. i.e. $\bigcap U$ is a (real) least upper bound of S.

Wherefore, any bounded nonempty subset S of $\mathbb{R}$ indeed has a least upper bound, $\bigcap U$ in $\mathbb{R}$.

Q.E.D. ■

Self-Proof of Lemma 5RC:

Let x and y be real numbers. We now verify that $x +_{\mathbb{R}} y$ is real:

(a) By definition, x and y are nonempty. So, let $q \in x$ and $r \in y$, of which there exists at least one such q and r respectively. Then, $r + q \in x +_{\mathbb{R}} y$ by definition, implying that $x +_{\mathbb{R}} y \neq \varnothing$. Clearly, $x +_{\mathbb{R}} y$ is a subset of $\mathbb{Q}$ since $\operatorname{ran} + \subseteq \mathbb{Q}$. We also know that x and y are proper subsets of $\mathbb{Q}$, meaning there exists some rational numbers s_1 not in x and s_2 not in y. Consequently, the rational number $s_1 + s_2$ is also not in $x +_{\mathbb{R}} y$. As desired, $x +_{\mathbb{R}} y \subset \mathbb{Q}$. In sum, $\varnothing \neq x +_{\mathbb{Q}} y \subset \mathbb{Q}$.

(b) Assume $q + r \in x +_{\mathbb{R}} y$ where $q \in x$ and $r \in y$, and the rational number b is less than $q + r$. It follows that $b - r < q$. Therefore, $b - r \in x$ since the real number x is closed downwards. Whence, $b - r + r = b$ is in $x +_{\mathbb{R}} y$. i.e. $x +_{\mathbb{R}} y$ is also closed downwards.

(c) Let $s \in x +_{\mathbb{R}} y$. By definition, there exists $q \in x$ and $r \in y$ with $s = q + r$. We know that the reals x and y have no largest member. Hence, there exists some $\widetilde{q} \in x$ and $\widetilde{r} \in y$ so $q < \widetilde{q}$ and $r < \widetilde{r}$. Furthermore, we see that $q + r < \widetilde{q} + r$ and $\widetilde{q} + r < \widetilde{q} + \widetilde{r}$. Finally, by the transitivity of $<$, $q + r < \widetilde{q} + \widetilde{r}$. Which means that we have just shown that for any element of $x +_{\mathbb{R}} y$, there exists another one greater than it in $x +_{\mathbb{R}} y$. In other words, $x +_{\mathbb{R}} y$ has no largest element.

Wherefore, $x +_{\mathbb{R}} y$ is in $\mathbb{R}$.

Q.E.D. ■

Remarks: This does not *immediately* mean that $s_1 + s_2 \notin x +_{\mathbb{R}} y$. Its still not clear that $s_1 + s_2$ *must* not be in $x +_{\mathbb{R}} y$. Actually, we need to add in one last part to complete our argument:

Consequently, for any $q \in x$ and $r \in y$, it must be that $q < s_1$ and $r < s_2$: Lest $s_1 \leq q$ but $s_1 \notin x$ or $s_2 \leq r$ but $s_2 \notin y$ (which would violate the fact that the reals x and y are closed downwards). Thus, $q + r < s_1 + r$ and $s_1 + r < s_1 + s_2$. By the transitivity of $<$ on $\mathbb{Q}$, $q + r < s_1 + s_2$. Thereupon, for all members $q + r$ of $x +_{\mathbb{R}} y$, $q + r \neq s_1 + s_2$, by trichotomy. Thence, $s_1 + s_2 \notin x +_{\mathbb{R}} y$ ...

Self-Proof of Theorem 5RE:

(a) (A) By definition, $0_{\mathbb{R}}$ contains only (negative) positive rational numbers, and thus, it is a subset of $\mathbb{Q}$. Notice that $-1 \in 0_{\mathbb{R}}$, meaning it is indeed nonempty. In sum, we proved $\varnothing \neq 0_{\mathbb{R}} \subset \mathbb{Q}$.

(B) If $q \in x$ and $r < q < 0$, by transitivity, we know $r < 0$ as well. Hence, $r \in x$. Therefore, x is closed downwards.

(C) Suppose $q \in 0_{\mathbb{R}}$. Then, $q < 0$. By Exercise 14 of the last section on rational numbers, there exists q' with $q < q' < 0$. As a result, $q' \in 0_{\mathbb{R}}$. i.e. We have shown that $0_{\mathbb{R}}$ has no largest member.

Since $0_{\mathbb{R}}$ is a subset of $\mathbb{Q}$ with the 3 above properties, it is a real number.

(b) i. $\underline{x +_{\mathbb{R}} 0_{\mathbb{R}} \subseteq x}$: Let $q \in x$ and $r \in 0_{\mathbb{R}}$. So, we know $r < 0$. Hence, $q + r < q$. Since x is a real number, it is closed downwards: $q + r \in x$. Thence, $x +_{\mathbb{R}} 0_{\mathbb{R}} \subseteq x$.

ii. $\underline{x \subseteq x +_{\mathbb{R}} 0_{\mathbb{R}}}$: Again, we assume $q \in x$. Since the real number x has no largest element, there must exist some $\widetilde{q} \in x$ with $q < \widetilde{q}$. Accordingly, $q - \widetilde{q} < 0$, implying that $q - \widetilde{q} \in 0_{\mathbb{R}}$. Consequently, $\widetilde{q} + (q - \widetilde{q}) = q \in x +_{\mathbb{R}} 0_{\mathbb{R}}$. In other words, $x \subseteq x +_{\mathbb{R}} 0_{\mathbb{R}}$.

Whence, we can conclude that $x +_{\mathbb{R}} 0_{\mathbb{R}} = x$.

Q.E.D. ■

Self-Proof of Theorem 5RF:

(a) As per normal, we need to verify the three properties of real numbers:

(A) Let $-s \in Q \setminus x$, of which there exists at least one since $x \subset \mathbb{Q}$. Then, $s - 1 < s$, and thus, $s - 1 \in -x$. As a result, $-x \neq \varnothing$. Consider $r' \in x$. As the real number x is nonempty, we have that there again is at least one such $r' \in x$. Subsequently, for any $\widetilde{s} > -r'$, we see that $-\widetilde{s} < r'$. Correspondingly, $-\widetilde{s} \in x$ since x is closed downwards. Resultantly, this means that $-r' \notin -x$ because there exists no $\widetilde{s} > -r'$ so that $-\widetilde{s} \notin x$. In other words, $-x \subset \mathbb{Q}$. In sum, it has been shown here that $\varnothing \neq x \subset \mathbb{Q}$.

(B) Assume $r \in -x$ and the rational number q is less than r. So, there must exist some $s > r$ with $-s \notin x$. Hence, $q < r < s$, and by transitivity, $s > q$. Thence, $q \in -x$. We see that $-x$ is closed downwards.

(C) We give two proofs that $-x$ has no largest member, first by contradiction and then directly:

V1. Suppose $-x$ has a largest element r^*. It follows from definition that there exists some $s > r^*$ with $-s \notin x$. Now, s must not be in $-x$; lest $s \in -x$ and $s > r^*$ — which would mean r^* is not the largest member of $-x$. However, we see that a contradiction is inevitable; because by Exercise 14 of this chapter — that states that the ordering of the rationals is dense — there exists q^* with $r^* < q^* < s$. Therefore, it is clear that $q^* \in -x$ and $r^* < q^*$ simultaneously. Whence, contradicting our assertion that $-x$ has a largest element r^*. Consequently, it must be that $-x$ has no largest element.

V2. Suppose $r \in -x$ again. Once more, we know there exists some $s > r$ with $-s \notin x$ by definition. Now, either $s \in -x$ or $s \notin -x$. Consider the former case of $s \in -x$: immediately we see that $s > r$ and $s \in -x$ simultaneously. In the latter case of $-s \notin x$, by Exercise 14 of this chapter (that proves that the ordering of rationals is dense), there exists some rational q with $r < q < s$. Therefore, $q \in x$ and $q > r$ again. In any case, it is clear that for any element of $-x$, there exists another larger one in $-x$. Whence, $-x$ has no largest element.

Since $-x$ is a subset of $\mathbb{Q}$ satisfying the 3 properties above, it certainly is a real number.

Q.E.D. ■

Exercises

16. In Lemma 5RC, show that $x +_{\mathbb{R}} y$ has no largest element.

    Proof:

    See Self-Proof of Lemma 5RC.

18. Assume that p is a positive rational number. Show that for any integer b there is some k in ω with
$$r < p \cdot E(E(k)).$$
(Here, k is in ω, $E(k)$ is the corresponding integer, and $E(E(k))$ is the corresponding rational.)

    Proof:

Notational note before we start: We shall include a subscript for addition, multiplication and ordering of integers and rationals. As well as for some specific integers like $0_{\mathbb{Z}}$ and $1_{\mathbb{Z}}$. While for natural numbers (and any operations on them), we will not.

We can write $r = [\langle a, b\rangle]$ and $q = [\langle c, d\rangle]$ for some integer a, positive integers b, c, and d. Repeating this procedure, we see that there exists natural numbers m, n, p, q, r, s, i, and j so
$$a = [\langle m, n\rangle], \quad b = [\langle p, q\rangle], \quad c = [\langle r, s\rangle], \quad \text{and} \quad d = [\langle i, j\rangle].$$
By the Trichotomy Law for ω, any natural number is either 0 or contains 0. Thus, $0 \subseteq mr + ns + ip + jq + 1$. Using Theorem 4N, that shows that $\in$ is preserved under addition of naturals, we arrive at two results:

{i} $(mr + ns + ip + jq) \ + \ 0 \ \in (mr + ns + ip + jq + 1)$, and

{ii} $(mr + ns + ip + jq + 1) \subseteq (mr + ns + ip + jq + 1) \ + \ (ms + nr + iq + jp)$

Therefore, since natural numbers are transitive sets by Theorem 4F, s
$$(mr + ns + ip + jq) + 0 \in (mr + ns + ip + jq + 1) + (ms + nr + iq + jp).$$
As a result, by the definition of the ordering on integers;
$$[\langle mr + ns + ip + jq,\ ms + nr + iq + jp\rangle] <_{\mathbb{Z}} [\langle mr + ns + ip + jq + 1,\ 0\rangle].$$
We now simplify each side of this inequality, starting from the left first:
$$\begin{aligned}[\langle mr + ns + ip + jq,\ ms + nr + iq + jp\rangle] &= [\langle mr + ns, ms + nr\rangle] +_{\mathbb{Z}} [\langle ip + jq, iq + jp\rangle] \\ &= [\langle m, n\rangle] \cdot_{\mathbb{Z}} [\langle r, s\rangle] +_{\mathbb{Z}} [\langle i, j\rangle] \cdot_{\mathbb{Z}} [\langle p, q\rangle] \\ &= ac +_{\mathbb{Z}} db.\end{aligned}$$
Similarly for the right, it is just $E(mr + ns + ip + jq + 1)$. Hence, we can rewrite our above inequality as
$$ac +_{\mathbb{Z}} db <_{\mathbb{Z}} E(mr + ns + ip + jq + 1).$$
To again utilise the fact that the ordering of integers is transitive, we notice two facts again:

{i} $(ac +_{\mathbb{Z}} db) \cdot 1_{\mathbb{Z}} <_{\mathbb{Z}} E(mr + ns + ip + jq + 1)$, and

{ii} $E(mr + ns + ip + jq + 1) <_{\mathbb{Z}} E(mr + ns + ip + jq + 1) \cdot bc$, because bc is a positive integer[2].

It follows that

$$(ac +_{\mathbb{Z}} db) \cdot 1_{\mathbb{Z}} <_{\mathbb{Z}} E(mr + ns + ip + jq + 1) \cdot bc.$$

Thence, by the definition of the linear ordering on the rationals,

$$[\langle ac + db, bc\rangle] <_{\mathbb{Q}} [\langle E(mr + ns + ip + jq + 1), 1_{\mathbb{Z}}\rangle].$$

Once more, we repeat the process of simplifying both sides, again starting from the left:

$$[\langle ac + db, bc\rangle] = [\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle d, c\rangle].$$

Then, as for the right, it is simply

$$[\langle E(mr + ns + ip + jq + 1), 1_{\mathbb{Z}}\rangle] = E(E(mr + ns + ip + jq + 1)).$$

Rewriting the inequality above, we get

$$[\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle d, c\rangle] <_{\mathbb{Q}} E(E(mr + ns + ip + jq + 1)).$$

Consequently, since multiplication of positive integers preserves the ordering of the rationals by Theorem 5QJ (b),

$$\begin{aligned} [\langle a, b\rangle] \cdot_{\mathbb{Q}} [\langle d, c\rangle] \cdot_{\mathbb{Q}} [\langle c, d\rangle] &<_{\mathbb{Q}} E(E(mr + ns + ip + jq + 1)) \cdot_{\mathbb{Q}} [\langle c, d\rangle] \\ [\langle a, b\rangle] &<_{\mathbb{Q}} [\langle c, d\rangle] \cdot_{\mathbb{Q}} E(E(mr + ns + ip + jq + 1)) \end{aligned}$$

This is just

$$r <_{\mathbb{Q}} p \cdot E(E(mr + ns + ip + jq + 1)).$$

Wherefore, there indeed exists a k in ω so that $r <_{\mathbb{Q}} p \cdot_{\mathbb{Q}} E(E(k))$; as we have just shown that $mr + ns + ip + jq + 1$ is one such k.

Q.E.D. ■

[2] I omit small details like proving that since b and c are positive integers, bc must be positive as well, as it would frankly be a waste of time.

19. Assume that p is a positive rational number. Show that for any real number x there is some rational q in x such that

$$p + q \notin x.$$

Proof:

Since x is real, we know $x \neq \mathbb{Q}$. Hence, the proper subset x of $\mathbb{Q}$ has an upper bound b in $\mathbb{Q} \setminus x$: Otherwise, there exists some $q \in x$ with $b \leq q$ but $b \notin x$, which either contradicts $q \in x$ or violates the fact that x is closed downwards. Then for any positive rational number p, $b < p + b$. Which means that $p + b \notin x$ because all rationals in x are strictly less than b.

Q.E.D. ■

20. Show that for any real number x, we have $0_{\mathbb{R}} \leq_{\mathbb{R}} |x|$.

Proof:

It is clear that for any real numbers x, either $x \geq_{\mathbb{R}} 0_{\mathbb{R}}$ or $x <_{\mathbb{R}} 0_{\mathbb{R}}$ — by the trichotomy of the linear ordering on $\mathbb{R}$ (Theorem 5RA). Hence, we consider them casewise:

$\underline{x \geq_{\mathbb{R}} 0}$: Then, by definition, $0_{\mathbb{R}} \subseteq x$. It follows that $0_{\mathbb{R}} \subseteq x \cup -x$. So, $0_{\mathbb{R}} \leq_{\mathbb{R}} |x|$.

$\underline{x <_{\mathbb{R}} 0_{\mathbb{R}}}$: Thus, since $-x$ is a real number (by Theorem 5RE), we see that

$$\begin{aligned} x +_{\mathbb{R}} (-x) &<_{\mathbb{R}} 0_{\mathbb{R}} +_{\mathbb{R}} (-x) && \text{as addition of reals preserves order by Theorem 5RH, so} \\ 0_{\mathbb{R}} &< -x && \text{because } -x \text{ is the additive inverse of } x \text{ be Theorem 5RF.} \end{aligned}$$

Consequently, $0_{\mathbb{R}} \subset -x$, and thereupon, $0_{\mathbb{R}} \subseteq x \cup -x$. Which means that $0_{\mathbb{R}} \leq_{\mathbb{R}} |x|$ holds.

Wherefore, in any case, we can conclude that $0_{\mathbb{R}} \leq_{\mathbb{R}} |x|$.

Q.E.D. ■

21. Show that if $x <_{\mathbb{R}} y$, then there is a rational number r with

$$x <_{\mathbb{R}} E(r) <_{\mathbb{R}} y.$$

Proof:

Assume that $x <_{\mathbb{R}} y$. Then, we immediately know that $x \subset y$. In other words there exists some s in y but not in x. This s must be an upper bound of x, lest there is some $q \in x$ with $s < q$ but $s \notin x$ — contradicting the fact that x is closed downwards. Since y has no largest element, $s < s'$ for some $s' \in y$. For all $q \in x$, $q < s < s'$. So, by transitivity, $q < s'$. Which shows that $s' \notin x$ — otherwise, s' would be the largest element of x — as well as that $x \subseteq E(s')$. Consequently, as $s \notin x$ but $s \in E(s')$, $x \subset E(s')$. Similarly, by reason of $s' \in y$; for any $r < s'$, $r \in y$ by virtue of y being closed downwards. In other words, $E(s') \subseteq y$. In addition, $s' \notin E(s')$. Whence, $E(s') \subset y$. Subsequently, we see that $x \subset E(s') \subset y$. Wherefore, we conclude that there indeed exists the rational number s' with

$$x <_{\mathbb{R}} E(s') <_{\mathbb{R}} y.$$

Q.E.D. ■

22. Assume that $x \in \mathbb{R}$. How do we know that $|x| \in \mathbb{R}$?

Proof:

Clearly, $|x|$ is a subset of $\mathbb{Q}$ by definition. As usual, we need to show the three properties of real numbers are satisfied, which we will do now:

(a) The real number x is nonempty by definition. So, $x \cup -x$ must be nonempty as well. By Theorem 5RA, the linear ordering on $\mathbb{R}$ is trichotomous. Thus, $x <_{\mathbb{R}} 0_{\mathbb{R}}$, $0_{\mathbb{R}} <_{\mathbb{R}} x$, or $x = 0_{\mathbb{R}}$ is true. We consider them casewise:

- ☐ When $x <_{\mathbb{R}} 0_{\mathbb{R}}$, let $-s \in 0_{\mathbb{R}} \setminus x$. At least one such $-s$ exists since $0_{\mathbb{R}} \subset x$. Consequently, $-s < 0$ and $0 < s$. Which means that for all $q \in x$, $q < 0 < s$. By Theorem 5RA, the linear ordering $<_{\mathbb{R}}$ is transitive. Therefore, $q < s$ and hence $q \in -x$. In other words, $x \subseteq -x$. Combined with the fact that the real number $-x$ is not $\mathbb{Q}$, it must be that $x \cup -x \neq \mathbb{Q}$ as well.
- ☐ If $0_{\mathbb{R}} <_{\mathbb{R}} x$, then
$$0_{\mathbb{R}} +_{\mathbb{R}} (-x) <_{\mathbb{R}} x +_{\mathbb{R}} (-x), \text{ so}$$
$$-x <_{\mathbb{R}} 0_{\mathbb{R}}.$$
Accordingly, $-x \subset -(-x)$ by the previous part. Now, recall that $\langle \mathbb{R}, +_{\mathbb{R}}, 0_{\mathbb{R}} \rangle$ is an Abelian group. As such, by PLemma A, $-(-x) = x$. As a result, $-x \subseteq x$. Thence, $x \cup -x \neq \mathbb{Q}$ because, again, the real number x is not $\mathbb{Q}$.

> **PLemma A.** *In any Abelian group $\langle A, +, 0 \rangle$, and for any $x \in A$, $x = -(-x)$.*
>
> *Proof:*
>
> $$\begin{aligned} x + (-x) &= 0 && \textit{by property 3} \\ [x + (-x)] + [-(-x)] &= -(-x) && \textit{by property 3} \\ x + \big((-x) + [-(-x)]\big) &= -(-x) && \textit{by property 1} \\ x + 0 &= -(-x) && \textit{by property 3} \\ x &= -(-x) && \textit{by property 2} \end{aligned}$$
>
> ♦

- ☐ Lastly, in the case that $x = 0_{\mathbb{R}}$; we see that $0_{\mathbb{R}} +_{\mathbb{R}} (-x)$, meaning $-x = 0_{\mathbb{R}}$. It is clear that $x \cup -x = 0_{\mathbb{R}} \neq \mathbb{Q}$.

In any case, $\varnothing \neq |x| \subset \mathbb{Q}$.

(b) Assume $q \in |x|$ and $r < q$. Immediately, either $q \in x$ or $q \in -x$. Since x and $-x$ are both real, they are closed downwards. Whence, in both cases, $r \in |x|$. That is, $|x|$ is also closed downwards.

(c) Finally, we need to prove $|x|$ has no largest element. Again, suppose that $q \in |x|$. By virtue of the reals x and $-x$ having no largest member, regardless of whether $q \in x$ or $q \in -x$, there exists some $r > q$ that is in the same set as q (i.e. in x or $-x$). Accordingly, $r \in |x|$ with $r > q$. Thereupon, $|x|$ has no largest element.

Wherefore, since $|x|$ is a subset of $\mathbb{Q}$ satisfying the 3 above properties, it is indeed a real number.

Q.E.D. ■

1.4.4 Cardinal Numbers and the Axiom of Choice

Self-Proof of $\mathscr{P}A \approx A$.

`Information provided:`

We define a one-to-one function H from $\mathscr{P}A$ onto ${}^{A}2$ as follows: For any subset B of A, $H(B)$ is the characteristic function of B, i.e., the function f_B from A into 2 for which

$$f_B(x) = \begin{cases} 1 & \text{if } x \in B, \\ 0 & \text{if } x \in A - B \end{cases}$$

Let $g \in {}^{A}2$ and define the sets $D_0 = \{x \in A \,|\, g(x) = 0\}$, and $D_1 = \{x \in A \,|\, g(x) = 1\}$. The sets D_0 and D_1 are disjoint, lest $g(x) = 0$ and $g(x) = 1$ simultaneously, which would violate the fact that the function g is single-valued. This combined with the fact that $D_0 \cup D_1 = A$ — because g has domain A in which $g(x) = 0$ or $g(x) = 1$ — means that $D_0 = A - D_1$. Consequently, we can write the mapping of g as

$$g(x) = \begin{cases} 1 & \text{if } x \in D_1 \\ 0 & \text{if } x \in A - D_1 \end{cases}$$

Accordingly, we notice that $H(D_1) = g(x)$. Hence, H is a surjective function.

Now assume that $H(B) = H(B')$. Then we immediately see that $f_B = f_{B'}$ are functions mapping from A into 2 so

$$f_B(x) = \left\{ \begin{array}{ll} 1 & \text{if } x \in B, \\ 0 & \text{if } x \in A - B. \end{array} \right\} = \left\{ \begin{array}{ll} 1 & \text{if } x \in B', \\ 0 & \text{if } x \in A - B'. \end{array} \right\} = f_{B'}(x).$$

Therefore, it is clear that $f_B(x) = 1$ iff $f_{B'}(x) = 1$; i.e.
$\{x \in A \,|\, f_B(x) = 1\} = \{x \in A \,|\, f_{B'}(x) = 1\}$ since both functions have domain A. However, by definition, the former is just B, while the latter is simply B'. That is:

$$B = \{x \in A \,|\, f_B(x) = 1\} = \{x \in A \,|\, f_{B'}(x) = 1\} = B'.$$

Thence, the function H is injective.

Wherefore, it now follows that H is a bijective function from $\mathscr{P}A$ to ${}^{A}2$. Which means that $\mathscr{P}A \approx {}^{A}2$. □

Self-Proof of Theorem 6A.

(a) Clearly, the identity map I_A provides us with such a bijection from A into A. When $a \in A$, $I_A(a) = a$. Thus, the identity map is surjective. Similarly, if $I_A(a) = I_A(a')$, then by definition, $I_A(a) = a$ and $I_A(a') = a'$. Accordingly, $a = a'$. We conclude that the identity map is also injective. Whence, A is equinumerous to itself.

(b) Assume that $A \approx B$. In other words, there exists a bijection $f\colon A \to B$. By Theorem 3F, f^{-1} is a function mapping from B into A because f is injective. Given any $a \in A$, $f(a)$ exists. Therefore, using Theorem 3G, we have that $f^{-1}(f(a)) = a$. We see that f^{-1} is surjective. Again, from the same theorem, for any b and b' in B such that $f(b) = f(b')$ — meaning $f(f^{-1}(b)) = f(f^{-1}(b))$ — we observe that $f(f^{-1}(b)) = b = f(f^{-1}(b')) = b'$. As a result, f^{-1} is injective. Thence, f^{-1} is a bijection from B into A; B is equinumerous to A.

(c) Now let $A \approx B$ and $B \approx C$. Immediately, there must exist some bijection $G_{AB} \colon A \to B$ and $\widetilde{G}_{BC} \colon B \to C$. Thus, we now construct the bijection $\overline{G}_{AC} \colon A \to C$ with $\overline{G}_{AC}(a) = \widetilde{G}_{BC}(G_{AB}(a))$.

Suppose $a = a'$. Hence, owing to the fact that G_{AB} is a function, $G_{AB}(a) = G_{AB}(a')$. By reason of $\widetilde{G}_{BC}$ also being a function, $\widetilde{G}_{BC}(G_{AB}(a)) = \widetilde{G}_{BC}(G_{AB}(a'))$. Consequently, $\overline{G}_{AC}(a) = \overline{G}_{AC}(a')$. i.e.: $\overline{G}_{AC}$ is a function.

If $c \in C$, then there is some $b \in B$ so $c = \widetilde{G}_{BC}(b)$ because $\widetilde{G}_{BC}$ is surjective. Similarly, as G_{AB} is surjective, $b = G_{AB}(a)$ for some $a \in A$. In sum, there exists an $a \in A$ such that $c = \widetilde{G}_{BC}(G_{AB}(a))$. By definition, $\overline{G}_{AC}(a) = c$. In other words, subjectivity is proven. Whenever $\overline{G}_{AC}(a) = \overline{G}_{AC}(a')$, $\widetilde{G}_{BC}(G_{AB}(a)) = \widetilde{G}_{BC}(G_{AB}(a'))$ by definition. Hence, since $\widetilde{G}_{BC}$ is injective, $G_{AB}(a) = G_{AB}(a')$. Repeating this once more, due to G_{AB} being injective, it must be that $a = a'$. We see that $\overline{G}_{AC}$ is injective.

Wherefore, $\overline{G}_{AC}$ is indeed a bijection from A into C. Which means that $A \approx C$.

□

Self-Proof of Theorem 6B.

(a) (N.A.) Mmm formalising decimals, specifically the part about showing every real number can be expressed as a decimal seems troublesome so nope. Interestingly, the argument is almost the same as that of (b).

(b) Assume that the function f maps S into its powerset. And let C be the subset of S so that $x \in C$ iff $x \notin f(x)$. Now, there either exists some $s \in S$ with $f(s) = C$ or there does not. Consider the case that there exists such a $s \in S$. Then, it follows that $s \in f(s)$ iff $s \in C$. By our construction of C, $s \in f(s)$ if and only if $s \notin f(s)$. However, this is clearly a contradiction. Consequently, it must be that there does not exist any such s. In other words, we have constructed a set C in the powerset of S but which is not in $\operatorname{ran} f$ for any function $f \colon S \to \mathscr{P}S$. Thence, showing that any $f \colon S \to \mathscr{P}S$ is never surjective. So, clearly there does not exist a bijection from S into $\mathscr{P}S$. Wherefore, S is not equinumerous to its powerset.

□

1. Show that the equation

$$f(m, n) = 2^m(2n + 1) - 1$$

defines a one-to-one correspondence between $\omega \times \omega$ and ω.

Proof. There are three criterion we need to check for, namely injectivity, surjectivity and that f is a (well-defined) function.

Surjectivity:

Let k be a natural number. By exercise 14 of Chapter 4, any natural number is either even or odd (but never both). Hence, we consider this casewise. First consider the much simpler case of k being even, which means $k = 2n$ for some natural n. Thus, $f(0, n) = 2^0(2n + 1) - 1 = 2n = k$. As for the latter case where k is odd, there is some natural n with $k = 2n + 1$. In other words, $k + 1 = 2n + 2 = 2(n + 1)$ is even. We now need the following lemma:

PLemma A. *Any nonzero even natural number can be written as* $2^i(2j+1)$ *for some naturals* $i \neq 0$ *and* j*, both less than* n*.*

Proof[a]*.* Let T be the set of naturals, n, so that if n is nonzero, then it can be written as $2^i(2j+1)$. Assume that for all $m \in n$, $m \in T$. If $n = 0$, $n \in T$ immediately holds. Suppose that n is nonzero. Then, consider n being odd, i.e. it can be written as some $2j+1$. Thus, $2n = 2^1(2j+1)$. When n is even, it is equivalent to some $2m^*$. Clearly $1 \subseteq m^* \in n$. Hence, $2m^*$ is expressible as some $2^i(2j+1)$. Which means that $2n = 2^{i+1}(2j+1)$. In any case, we see that $n \in T$. By the Strong Induction on ω, $T = \omega$. □

[a] We shall avoid stating "for some naturals..." to avoid unnecessarily cluttering up the proof. It should be clear to the reader which symbol represents what.

Utilising the above PLemma A, there are some natural numbers $i \neq 0$ and j (both less than n) for which $2n+2 = 2^i(2j+1)$. It follows that $k = 2n+1 = 2^i(2j+1) - 1 = f(i,j)$. Consequently, irregardless of whether k is even or odd, k is always in the range of f. Which means that f is surjective.

Injectivity:

Suppose that $f(m,n) = f(m',n')$. i.e. $2^m(2n+1) = 2^{m'}(2n'+1)$. And that T' is the set of natural numbers m so that for all natural m', $2^m(2n+1) = 2^{m'}(2n'+1)$ implies $m = m'$. Starting from $m = 0$ as usual, we see that $2^0(2n+1) = 2^{m'}(2n'+1)$ must mean $m = m'$, lest $m' \geq 1$ which would mean a natural number is both odd and even at the same time, contradicting exercise 14 of Chapter 4. Now, presume $m \in T$. Clearly $2^{m^+}(2n+1) = 2[2^m(2n+1)] = 2^{m'}(2n'+1)$ tells us that $m' \geq 1$, lest $m' = 0$; meaning a natural number is both even (left side) and odd (right side). Creating the same contradiction as above. Since $m' \geq 1$, there is a natural $\overline{m}$ with $m' = \overline{m}^+$. Accordingly, $2[2^m(2n+1)] = 2[2^{\overline{m}}(2n'+1)]$, and from the cancellation laws for natural numbers, we notice that $2^m(2n+1) = 2^{\overline{m}}(2n'+1)$. By our induction hypothesis, $m = \overline{m}$ again. In other words, $m^+ = m'$. Thereafter, by the cancellation laws, it follows that $2n+1 = 2n'+1$, and whence, $n = n'$. Resultantly, we have proven the injectivity of f.

Well-Definedness of f:

Lastly, we have the simplest part of our proof. Without pouring over minute details, if $m = m'$ and $n = n'$, then by virtue of addition, multiplication and exponentiation being functions, we can conclude that $2^m(2n+1) = 2^{m'}(2n'+1)$.

Wherefore, the bijection f defines a one-to-one correspondence between $\omega \times \omega$ and ω. □

3. Find a one-to-one correspondence between the open unit interval $(0,1)$ and $\mathbb{R}$ that takes rationals to rationals and irrationals to irrationals.

Proof. We define the bijection $f\colon (0,1) \to \mathbb{R}$ with

$$f(x) = \begin{cases} \frac{1}{1-x} - 2 & \text{if } \frac{1}{2} \leq x < 1, \\ 2 - \frac{1}{x} & \text{if } 0 < x < \frac{1}{2}. \end{cases}$$

By virtue of subtraction and division being functions, we easily see that f must be a function as we claimed. We now verify that it is injective, surjective, as well as maps rationals to rationals and irrationals to irrationals.

Injectivity:

Assume $f(x) = f(x')$. We first notice that both must be in either $\left[\frac{1}{2}, 1\right)$ or $\left(0, \frac{1}{2}\right)$. Otherwise, we can presume (without loss of generality) that $\frac{1}{2} \leq x < 1$ and $0 < x' < \frac{1}{2}$, in which case

$$\begin{aligned} \frac{1}{2} &\leq x & \text{and} \qquad x' &< \frac{1}{2} \\ 1 - x &\leq \frac{1}{2} & 2 &< \frac{1}{x'} \\ 0 &\leq \frac{1}{1-x} - 2 & 2 - \frac{1}{x'} &< 0. \end{aligned}$$

Clearly, this would mean that $f(x) \neq f(x')$, contradicting our assumption that $f(x) = f(x')$. Hence, we only need to consider the two cases below:

$$\begin{aligned} \frac{1}{1-x} - 2 &= \frac{1}{1-x'} - 2 \qquad \text{or} \qquad 2 - \frac{1}{x} = 2 - \frac{1}{x'} \\ \frac{1}{1-x} &= \frac{1}{1-x'} & \frac{1}{x'} &= \frac{1}{x} \\ 1 - x' &= 1 - x & x &= x' \\ x &= x' \end{aligned}$$

In any case, we see that $x = x'$. Consequently, f is indeed injective.

Surjectivity:

Let $y \in \mathbb{R}$. Then, there are two scenarios possible — either $y \geq 0$ or $y < 0$. For the former, observe that

$$\begin{aligned} y + 2 &\geq 2 \\ \frac{1}{2} &\geq \frac{1}{y+2} \\ -\frac{1}{y+2} &\geq -\frac{1}{2} \end{aligned}$$

This means two things:

$$\begin{aligned} -\frac{1}{y+2} &< 0 \qquad \text{and} \qquad 1 - \frac{1}{y+2} \geq \frac{1}{2} \\ 1 - \frac{1}{y+2} &< 1 \end{aligned}$$

Since $\frac{y+1}{y+2} = 1 - \frac{1}{y+2}$, thus $\frac{1}{2} \leq \frac{y+1}{y+2} < 1$. And so;

$$\begin{aligned} f\left(\frac{y+1}{y+2}\right) &= \frac{\left[2\left(\frac{y+1}{y+2}\right) - 1\right]}{\left[1 - \left(\frac{y+1}{y+2}\right)\right]} \\ &= \frac{2(y+1) - (y+2)}{(y+2) - (y+1)} \\ &= \frac{2y + 2 - y - 2}{y + 2 - y - 1} \\ &= \frac{y}{1} \\ &= y. \end{aligned}$$

Similarly for the latter, we find that $2 < 2 - y$, telling us that

$$0 < 2 - y \qquad \text{and} \qquad \frac{1}{2-y} < \frac{1}{2}$$
$$0 < \frac{1}{2-y}$$

Accordingly, we have that $0 < \frac{1}{2-y} < \frac{1}{2}$. Therefore,

$$\begin{aligned} f\left(\frac{1}{2-y}\right) &= 2 - \frac{1}{\left(\frac{1}{2-y}\right)} \\ &= 2 - (2-y) \\ &= y. \end{aligned}$$

Thence, irregardless of whether $y \geq 0$ or $y < 0$, there exists a x in $(0,1)$ such that $y = f(x)$. In other words, f is surjective.

Rationals To Rationals, Irrationals To Irrationals:

We claim that $x \in (0,1)$ is rational iff $f(x)$ is. When $\frac{p}{q} \in (0,1)$ where p and q are integers, then

$$\begin{aligned} f(x) &= \frac{1}{\left(1 - \frac{p}{q}\right)} - 2 \qquad \text{or} \qquad f(x) = 2 - \frac{1}{\left(\frac{p}{q}\right)} \\ &= \frac{q}{q-p} - 2 \qquad\qquad\qquad = 2 - \frac{q}{p} \\ &= \frac{2p-q}{q-p} \qquad\qquad\qquad = \frac{2p-q}{p} \end{aligned}$$

Either way, $f(x)$ is rational, as desired. Conversely, suppose $\frac{p}{q} \in \mathbb{R}$ for integers p and q. It follows that

$$\frac{\left(\frac{p}{q}+1\right)}{\left(\frac{p}{q}+2\right)} = \frac{p+q}{p+2q} \qquad \text{and} \qquad \frac{1}{\left(2 - \frac{p}{q}\right)} = \frac{q}{2-p}.$$

Both are easily seen to be rational. From the previous part we know that f maps these to $\frac{p}{q}$. As a result, we have shown $x \in (0,1)$ is rational iff $f(x)$ is. Correspondingly, $x \in (0,1)$ is irrational iff $f(x)$ is immediately holds. That is, f maps rationals to rationals and irrationals to irrationals.

Wherefore, this function $f\colon (0,1) \to \mathbb{R}$ is indeed the bijection we are looking for, with the property that it maps rationals to rationals and irrationals to irrationals. □

Self-Proof of Corollary 6C. Let S be some finite set and S' be a proper subset of S. It follows from definition that there exists a bijection $f\colon S \to n$ for some natural n. Clearly, $\operatorname{ran}(f \restriction S') \subset n$ and $S' \approx \operatorname{ran}(f \restriction S')$. By the Pigeonhole Principle, n is not equinumerous to $\operatorname{ran}(f \restriction S')$ since $\operatorname{ran}(f \restriction S')$ is a proper subset of n. Now utilising the contrapositive of Theorem 6A (c), it must be that $S \not\approx \operatorname{ran}(f \restriction S')$ because $n \approx S$ by definition. Consequently, using the same theorem a second time, we observe that as $S' \approx \operatorname{ran}(f \restriction S')$, $S \not\approx S'$ is certainly true. Hence, the finite set S is not equinumerous to any proper subset S' of itself. □

Self-Proof of Corollary 6D. (a) Taking the contrapositive of Corollary 6C, we clearly see that for any set S, if S is equinumerous to a proper subset of itself, then it is infinite.

(b) Let ε be the set of even natural numbers. Then, we see that there exists the bijection $f\colon \omega \to \varepsilon$ defined by $f(n) = 2n$. When $f(n) = f(n')$, $2n = 2n'$, and so, $n = n'$. Hence, f is indeed injective. If $2n \in \varepsilon$ for some natural n, then immediately, $f(n) = 2n$. Which means that f is surjective. Therefore, f bijects ω into ε as desired. Consequently, ω is equinumerous to ε. Wherefore, by part (a), since ε is a proper subset of ω yet $\omega \approx \varepsilon$ still, ω must be an infinite set.

□

1.5 Random Stuff

Self-Proof of Theorem 9T. Let S be a set of cardinality κ whose members are sets X of ordinals, so that $\bigcup S = \lambda$. Further suppose without loss of generality that each $X \in S$ is nonempty and pairwise disjoint. By AC, there exists a well-order $<$ on S. Now, define the lexicographic well-order $\sqsubset$ on λ by

$$\alpha_X \sqsubset \beta_Y \qquad \text{iff} \qquad X < Y \quad \text{or} \quad (X = Y \quad \& \quad \alpha_X \in \beta_Y).$$

We have the usual function E with domain λ given by $E(\alpha) = E[\![\operatorname{seg}\alpha]\!]$. By the injectivity of E, $\lambda \subseteq E[\![\lambda]\!]$ because $\lambda \preccurlyeq E[\![\lambda]\!]$. Furthermore since $\alpha \in \lambda$, we know $\operatorname{card}(E(\alpha)) = \operatorname{card}(\operatorname{seg}\alpha) < \lambda$. Thus, $E(\alpha) \in \lambda$ for every $\alpha \in \lambda$, so $E[\![\lambda]\!] \subseteq \lambda$. As such, $\lambda = E[\![\lambda]\!]$. Now define the function $G\colon S \to \lambda$ by $G(X) = \bigcup_{Y<X} E[\![Y]\!]$. $G(X)$ must never be λ, lest $\operatorname{card}(E[\![X]\!] \cup \bigcup_{Y<X} E[\![Y]\!]) = \lambda$. But since $\bigcup_{Y<X} E[\![Y]\!] \subset \lambda$, $\operatorname{card} E[\![X]\!] = \operatorname{card} X = \lambda$, a contradiction. Thence, $G(X) \in \lambda$ for every $X \in S$. We also see that G must be injective because: If $Y \neq X$, we can say wlog that $Y < X$ and that there is some α in X which isn't in Y. Accordingly, $E(\alpha) \in G(X)$ but $E(\alpha) \notin G(Y)$. Hence, $G(Y) \neq G(X)$. Lastly, notice that for any $E(\alpha)$, $\alpha \in X$ for some $X \in S$, so $E(\alpha) \in G(X)$. As a result, $\sup \operatorname{ran} G = \operatorname{ran} E = \lambda$. In other words, $\sup G[\![S]\!]$ is a set of ordinals $G(X)$ less than λ with supremum λ and cardinality $\operatorname{card} S = \kappa$. By the definition of cofinality, $\operatorname{cf}\lambda$ is indeed the least such κ. □