

My set theory exercises

Evgeny Markin

2023

Contents

1	Introduction	4
1.1	Elementary Set Theory	4
1.1.1	4
1.1.2	4
1.1.3	4
1.1.4	5
1.1.5	5
1.1.6	5
1.1.7	5
1.1.8	5
1.1.9	6
1.2	Logical Notation	6
1.3	Predicates and Quantifiers	7
1.4	A Formal Language for Set Theory	7
1.4.1	7
1.4.2	7
1.4.3	7
1.4.4	7
1.4.5	8
1.4.6	8
1.4.7	8
1.4.8	8
1.5	The Zermelo-Fraenkel Axioms	9
1.5.1	9
1.5.2	9
1.5.3	9
1.5.4	9
1.5.5	10
1.5.6	10
1.5.7	10

1.5.8	10
1.5.9	11
1.5.10	11
2 Basic Set-Building Axioms and Operations	12
2.1 The First Six Axioms	12
2.2 Operations on Sets	14
2.2.1	15
2.2.2	15
2.2.3	15
3 Relations and Functions	17
3.1 Ordered Pairs in Set Theory	17
3.1.1	17
3.1.2	17
3.1.3	18
3.1.4	18
3.2 Relations	18
3.2.1	18
3.2.2	19
3.3 Functions	21
3.4 Order Relations	24
3.5 Congruence and Preorder	29
4 The Natural Numbers	31
4.1 Inductive Sets	31
4.2 The Recursion Theorem on ω	33
4.3 Arithmetic on ω	35
4.4 Order on ω	39
5 On the Size of Sets	44
5.1 Finite Sets	44
5.2 Countable Sets	51
5.3 Uncountable Sets	54

Useful things

I think that it is pretty straightforward to define some function based on axioms that we get. For example pairing axiom allows us to define $PA : S \times S \rightarrow S$ by

$$PA(u, v) = \{u, v\}$$

same goes for union axiom

$$UA(u) = \{\text{elements of elements of } U\}$$

Later some other function might be defined in the same manner.

In logic notation, I denote tautology as 'true' and contradiction as 'false'

There is a rule that I've used

$$a \wedge (b \vee \neg a) \Leftrightarrow (a \wedge b) \vee (a \wedge \neg a) \Leftrightarrow (a \wedge b) \vee (\text{false}) \Leftrightarrow a \wedge b$$

which I don't remember seeing in the book, but it's pretty useful.

Sometimes I use \oplus to denote xor.

I also denote ${}^B A$ as A^B , because it's more convinient.

Chapter 1

Introduction

1.1 Elementary Set Theory

Let A, B, C be

1.1.1

If $a \notin A \setminus B$ and $a \in A$, show that $a \in B$

Because $a \notin A \setminus B$, we follow that $x \in B$ or $x \notin A$. Since $x \in A$, we follow that $x \in B$, as desired.

1.1.2

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

Let $c \in C \setminus B$. Then we follow that $c \in C$ or $c \notin B$. Since $A \subseteq B$, we follow that $c \notin B$ implies that $c \notin A$. Thus we follow that $c \in C \setminus B$ implies that $c \in C \setminus A$. Therefore $C \setminus B \subseteq C \setminus A$.

1.1.3

Suppose $A \setminus B \subseteq C$. Show that $A \setminus C \subseteq B$.

Suppose that $a \in A \setminus C$. Then we follow that $a \in A$ and $a \notin C$.

Given that $A \setminus B \subseteq C$ and $A \not\subseteq C$, we follow that $a \notin A \setminus B$. Thus $a \notin A$ or $a \in B$. Since $a \in A$, we follow that $a \in B$. Thus

$$a \in A \setminus C \rightarrow a \in B$$

$$A \setminus C \subseteq B$$

as desired.

1.1.4

Suppose $A \subseteq B$ and $A \subseteq C$. Show that $A \subseteq B \cap C$

Suppose that $a \in A$. Then we follow that $a \in B$ and $a \in C$. Thus $a \in B \cap C$. Therefore we follow that $A \subseteq B \cap C$.

1.1.5

Suppose $A \subseteq B$ and $B \cap C = \emptyset$. Show that $A \subseteq B \setminus C$

Suppose that $a \in A$. Then we follow that $a \in B$ and since $B \cap C = \emptyset$, we follow that $a \notin C$. Thus $a \in B \setminus C$ by definition. Therefore $A \subseteq B \setminus C$.

1.1.6

Show that $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$. Suppose that $a \in A \setminus (B \setminus C)$. Then we follow that $a \in A$ and $a \notin B \setminus C$. Thus $a \notin B$ and $a \in C$. Thus we follow that $a \in A \setminus B$ or $a \in C$. Thus $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$ as desired.

1.1.7

Let $P(x)$ be the property $x > \frac{1}{x}$. Are the assertions $P(2)$, $P(-2)$, $P(\frac{1}{2})$, $P(\frac{-1}{2})$ true or false

$$2 > \frac{1}{2} \rightarrow P(2) = \text{true}$$

$$-2 < \frac{-1}{2} \rightarrow P(-2) = \text{false}$$

last two are reversed.

1.1.8

Show that each of the following sets can be expressed as an interval

$$a) (-3, 3)$$

$$b) (-3, \infty)$$

$$c) (-3, 3)$$

all of them follow from order properties of real numbers.

1.1.9

Express the following sets as truth sets

$$A = \{1, 4, 9, 16, 25, \dots\} \iff A = \{x \in N : x = y^2 \text{ for some } y \in N\}$$

$$B = \{\dots, -15, -10, -5, 0, 5, \dots\} \iff A = \{x \in N : x = 5y \text{ for some } y \in N\}$$

Rest are also trivial, not gonna go deep here

1.2 Logical Notation**1.2.1**

Using truth tables, show that $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$

P	Q	$P \Rightarrow Q$	$\neg(P \Rightarrow Q)$	$\neg Q$	$P \wedge \neg Q$
false	false	true	false	true	false
false	true	true	false	false	false
true	false	false	true	true	true
true	true	true	false	false	false

from this we can see that they are equivalent.

Following 4 exercises are the same as this one, so I'm skipping them

1.2.5

Show that $(P \Rightarrow Q) \wedge (P \Rightarrow R) \Leftrightarrow P \Rightarrow (Q \wedge R)$, using logic laws

$$(P \Rightarrow Q) \wedge (P \Rightarrow R) \Leftrightarrow (\neg P \vee Q) \wedge (\neg P \vee R) \Leftrightarrow \neg P \vee (R \wedge Q) \Leftrightarrow P \Rightarrow (R \wedge Q)$$

Laws used:

$$CL \rightarrow DIST \rightarrow CL$$

1.2.6

Show that $(P \Rightarrow R) \vee (Q \Rightarrow R) \Leftrightarrow (P \wedge Q) \Rightarrow R$, using logic laws

$$\begin{aligned} (P \Rightarrow R) \vee (Q \Rightarrow R) &\Leftrightarrow (\neg P \vee R) \vee (\neg Q \vee R) \Leftrightarrow \neg P \vee R \vee \neg Q \vee R \Leftrightarrow (\neg Q \vee \neg P) \vee R \Leftrightarrow \\ &\Leftrightarrow \neg(Q \wedge P) \vee R \Leftrightarrow (Q \wedge R) \Rightarrow R \end{aligned}$$

Laws used:

$$CL \rightarrow ASC \rightarrow ID, ASC \rightarrow DML \rightarrow CL$$

1.2.7

Show that $P \Rightarrow (Q \Rightarrow R) \Leftrightarrow (P \wedge Q) \Rightarrow R$, using logic laws

$$P \Rightarrow (Q \Rightarrow R) \Leftrightarrow \neg P \vee (Q \Rightarrow R) \Leftrightarrow \neg P \vee (\neg Q \vee R) \Leftrightarrow (\neg P \vee \neg Q) \vee R \Leftrightarrow \neg(P \wedge Q) \vee R \Leftrightarrow (P \wedge Q) \Rightarrow R$$

Laws used:

$$CL \rightarrow CL \rightarrow ASC \rightarrow DML \rightarrow CL$$

1.2.8

Show that $(P \Rightarrow Q) \Rightarrow R$ and $P \Rightarrow (Q \Rightarrow R)$ are not logically equivalent

We're gonna show that $q \wedge w \Leftrightarrow false$

$$\begin{aligned} ((P \Rightarrow Q) \Rightarrow R) \wedge (P \Rightarrow (Q \Rightarrow R)) &\Leftrightarrow (\neg(\neg P \vee Q) \vee R) \wedge (\neg P \vee (\neg Q \vee R)) \Leftrightarrow \\ &\Leftrightarrow ((P \wedge \neg Q) \vee R) \wedge (\neg P \vee \neg Q \vee R) \Leftrightarrow ((P \wedge Q) \wedge (\neg P \vee \neg Q)) \vee R \Leftrightarrow \\ &\Leftrightarrow ((P \wedge Q) \wedge \neg(P \wedge Q)) \vee R \Leftrightarrow false \vee R \Leftrightarrow false \end{aligned}$$

1.3 Predicates and Quantifiers**1.4 A Formal Language for Set Theory****1.4.1**

What does the formula $\exists x \forall y (x \notin y)$ say in English?

There exists x such that for every y we've got that x is not in y . In other words, there exists an empty set.

1.4.2

What does the formula $\forall y \exists x (y \notin x)$ say in English?

For every y there exists set x such that y is not in x .

1.4.3

What does the formula $\forall y \exists x (x \notin y)$ say in English?

For every y there exists x such that x is not in y .

1.4.4

What does the formula $\forall y \neg \exists x (x \notin y)$ say in English?

For every y there does not exist an x such that x is not in y .

1.4.5

What does the formula $\forall z \exists x \exists y (x \in y \wedge y \in z)$ say in English?

For every z there exists x and y such that x is in y and y is in z

1.4.6

Let $\phi(x)$ be a formula. What does $\forall z \forall y ((\phi(x) \wedge \phi(y)) \rightarrow z = y)$

For every z and y , $\phi(x)$ and $\phi(y)$ implies that $z = y$.

1.4.7

Translate each of the following into the language of set theory.

(a) x is the union of a and b

$$\forall (y \in x)(y \in a \vee y \in b)$$

(b) x is not a subset of y

$$\exists (z \in x)(z \notin y)$$

(c) x is the intersection of a and b

$$\forall (y \in x)(y \in a \wedge y \in b)$$

(d) a and b have no elements in common

$$\forall (x \in a) \forall (y \in b)(x \neq y)$$

1.4.8

Let a , b , C and D be sets. Show that the relationship

$$y = \begin{cases} a & \text{if } x \in C \setminus D \\ b & \text{if } x \notin C \setminus D \end{cases}$$

$$((x \in C \wedge x \notin D) \rightarrow (y = a)) \wedge ((x \notin C \setminus D) \rightarrow (y = b))$$

1.5 The Zermelo-Fraenkel Axioms

1.5.1

Let u, v, w be sets. By pairing axiom, the sets $\{u\}$ and $\{v, w\}$ exist. Using the pairing and union axioms, show that the set $\{u, v, w\}$ exists.

By pairing axiom we've got that

$$PA(u, u) = \{u\}$$

$$PA(v, w) = \{v, w\}$$

thus

$$PA(\{u\}, \{v, w\}) = \{\{u\}, \{v, w\}\}$$

and therefore by union axiom we follow that

$$UA(\{\{u\}, \{v, w\}\}) = \{u, v, w\}$$

as desired.

1.5.2

Let A be a set. Show that the pairing axiom implies that the set $\{A\}$ exists

$$PA(A, A) = \{A, A\}$$

which by extension axiom is equal to $\{A\}$, as desired.

1.5.3

Let A be a set. The pairing axiom implies that the set $\{A\}$ exists. Using the regularity axiom, show that $A \cap \{A\} = \emptyset$. Conclude that $A \notin A$.

Since $\{A\} \neq \emptyset$, we follow that there exists x such that $x \in \{A\}$ and $x \cap \{A\} = \emptyset$. Since A is the only element of $\{A\}$, we follow that $A \cap \{A\} = \emptyset$, as desired.

1.5.4

For sets A, B , the set $\{A, B\}$ exists by the pairing axiom. Let $A \in B$. Using the regularity axiom, show that $A \cap \{A, B\} = \emptyset$, and thus $B \notin A$.

$\{A, B\}$ consists of sets A and B , thus it is not empty and therefore there exists $x \in \{A, B\}$ such that $x \in \{A, B\} \wedge x \cap \{A, B\} = \emptyset$. For B we've got that $B \in \{A, B\}$. Since $A \in B$ and $A \in \{A, B\}$, we can follow that $A \in (B \cap \{A, B\})$. By pairing axiom we follow that the element with desired property must exist, and given that the only other choice is A , we conclude that $A \cap \{A, B\} = \emptyset$. Therefore we can follow that $B \notin A$, as desired.

1.5.5

Let A, B, C be sets. Suppose that $A \in B$ and $B \in C$. Using the regularity axiom, show that $C \notin A$.

This is an expansion of previous exercise. We can follow that

$$B \in \{A, B, C\} \wedge B \in C \Rightarrow B \in C \cap \{A, B, C\} \Rightarrow C \cap \{A, B, C\} \neq \emptyset$$

$$A \in \{A, B, C\} \wedge A \in B \Rightarrow A \in B \cap \{A, B, C\} \Rightarrow B \cap \{A, B, C\} \neq \emptyset$$

thus the only other choice is A , and therefore $A \cap \{A, B, C\} = \emptyset$. Therefore $C \notin A$, as desired.

1.5.6

Let A, B be sets. Using the subset and power set axioms, show that the set $\mathcal{P}(A) \cap B$ exists.

Because set A exists we follow that $\mathcal{P}(A)$ exists. By setting $\phi(x) : x \in B$ and subset axiom we follow that there exists a subset of $\mathcal{P}(A)$ such that $x \in S \Leftrightarrow x \in \mathcal{P}(A) \wedge x \in B$. Thus we follow by Extensionality axiom that $S = \mathcal{P}(A) \cap B$. Thus $\mathcal{P}(A) \cap B$ exists.

1.5.7

Let A, B be sets. Using the subset axiom, show that the set $A \setminus B$ exists.

$$\phi(x) : \neg x \in B$$

thus by subset axiom

$$x \in S \Leftrightarrow x \in A \wedge \neg x \in B$$

thus $A \setminus B$ exists.

1.5.8

Show that no two of the sets $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}$ are equal to each other.

I had a little confusion with this one at first because I thought that every set has empty set in it, which is false. Every set has an empty set as a subset, but it might be so that empty set is not in the set itself.

$$\emptyset \notin \emptyset \wedge \emptyset \in \{\emptyset\} \Rightarrow \emptyset \neq \{\emptyset\}$$

$$\emptyset \notin \emptyset \wedge \emptyset \in \{\emptyset, \{\emptyset\}\} \Rightarrow \emptyset \neq \{\emptyset, \{\emptyset\}\}$$

$$\{\emptyset\} \notin \{\emptyset\} \wedge \{\emptyset\} \in \{\emptyset, \{\emptyset\}\} \Rightarrow \{\emptyset\} \neq \{\emptyset, \{\emptyset\}\}$$

all of the implication follow from extensionality axiom.

1.5.9

Let A be a set with no elements. Show that for all x , we have that $x \in A$ if and only if $x \in \emptyset$. Using the extensionality axiom, conclude that $A = \emptyset$.

Suppose that $\neg x \in A$. Then we follow that x is an element, therefore $\neg x \in \emptyset$. Thus

$$\neg x \in A \Rightarrow \neg x \in \emptyset \iff x \in \emptyset \Rightarrow x \in A$$

Suppose that $\neg x \in \emptyset$. Then we follow that x is an element. Thus $\neg x \in A$. Thus

$$\neg x \in \emptyset \Rightarrow \neg x \in A \iff x \in A \Rightarrow x \in \emptyset$$

thus we follow that

$$x \in \emptyset \Leftrightarrow x \in A$$

thus by extensionality axiom we follow that

$$\emptyset = A$$

which gives us nice follow-up that

$$\emptyset = \{\}$$

1.5.10

Let $\phi(x, y)$ be the formula $\forall z(z \in y \Leftrightarrow z = x)$ which asserts that $y = \{x\}$. For all x the set $\{x\}$ exists. So $\forall x \exists! y \phi(x, y)$. Let A be a set. Show that the collection $\{\{x\} : x \in A\}$ is a set.

We know that A is a set and therefore $\mathcal{P}(A)$ is also a set. Thus by subset axiom there exists a set

$$\exists S(x \in S \Leftrightarrow x \in \mathcal{P}(A) \wedge \exists(y \in A)(\phi(x, y)))$$

which is precisely our collection.

Chapter 2

Basic Set-Building Axioms and Operations

2.1 The First Six Axioms

Prove the following theorems, where A, B, C, D are sets.

2.1.1

$$A \subseteq B \rightarrow (A \subseteq A \cup B \wedge A \cap B \subseteq A)$$

$$\begin{aligned} & \forall x(x \in A \rightarrow x \in B) \rightarrow ((\forall x(x \in A \Rightarrow x \in A \vee x \in B)) \wedge (\forall(x \in A \wedge x \in B \Rightarrow x \in A))) \Leftrightarrow \\ & \Leftrightarrow \forall x(x \in A \rightarrow x \in B) \rightarrow ((\forall x(\neg x \in A \vee x \in A \vee x \in B)) \wedge (\forall(\neg(x \in A \wedge x \in B) \vee x \in A))) \Leftrightarrow \\ & \Leftrightarrow \forall x(x \in A \rightarrow x \in B) \rightarrow ((\forall x(\text{true} \vee x \in B)) \wedge (\forall(\neg x \in A \vee \neg x \in B \vee x \in A))) \Leftrightarrow \\ & \Leftrightarrow \forall x(x \in A \rightarrow x \in B) \rightarrow (\text{true} \wedge (\forall(\text{true} \vee \neg x \in B))) \Leftrightarrow \\ & \Leftrightarrow \neg \forall x(x \in A \rightarrow x \in B) \vee (\text{true} \wedge \text{true}) \Leftrightarrow \\ & \Leftrightarrow \neg \forall x(x \in A \rightarrow x \in B) \vee \text{true} \Leftrightarrow \\ & \text{true} \end{aligned}$$

2.1.2

$$A \subseteq B \wedge B \subseteq C \rightarrow A \subseteq C$$

$$\begin{aligned} & (\forall x(x \in A \Rightarrow x \in B)) \wedge (\forall x(x \in B \Rightarrow x \in C)) \rightarrow \forall x(x \in A \Rightarrow x \in C) \Leftrightarrow \\ & \Leftrightarrow (\forall x(\neg x \in A \vee x \in B)) \wedge (\forall x(\neg x \in B \vee x \in C)) \rightarrow \forall x(\neg x \in A \vee x \in C) \Leftrightarrow \\ & \Leftrightarrow (\forall x((\neg x \in A \vee x \in B) \wedge (\neg x \in B \vee x \in C))) \rightarrow \forall x(\neg x \in A \vee x \in C) \Leftrightarrow \\ & \Leftrightarrow (\forall x((\neg x \in A \wedge (\neg x \in B \vee x \in C)) \vee (x \in B \wedge (\neg x \in B \vee x \in C)))) \rightarrow \forall x(\neg x \in A \vee x \in C) \Leftrightarrow \\ & \Leftrightarrow (\forall x(\neg x \in A \wedge (\neg x \in B \vee x \in C)) \vee ((x \in B \wedge \neg x \in B) \vee (x \in B \wedge x \in C))) \rightarrow \forall x(\neg x \in A \vee x \in C) \Leftrightarrow \\ & \Leftrightarrow (\forall x((\neg x \in A \wedge \neg x \in B) \vee (\neg x \in A \wedge x \in C) \vee (x \in B \wedge x \in C))) \rightarrow \forall x(\neg x \in A \vee x \in C) \Leftrightarrow \dots \end{aligned}$$

So this thing is tedious as hell and should be left to computers.

Suppose that $x \in A$. Then we follow by $A \subseteq B$ that $x \in B$. Thus by $B \subseteq C$ we follow that $x \in C$. Therefore $x \in A \rightarrow x \in C$. Therefore $A \subseteq C$, as desired.

2.1.3

$$B \subseteq C \Rightarrow A \setminus C \subseteq A \setminus B$$

Suppose that $x \in A \setminus C$. Then we follow that $x \in A$ and $x \notin C$. Therefore $x \in A$ and $x \notin B$ since $B \subseteq C$. Thus $x \in A \setminus B$. Therefore we follow that $B \subseteq C$ implies that $A \setminus C \subseteq A \setminus B$, as desired.

2.1.4

$$C \subseteq A \wedge C \subseteq B \iff C \subseteq A \cap B$$

Suppose that $x \in C$. Then we follow that $x \in A$ and $x \in B$. Thus $x \in A \cap B$. Therefore $C \subseteq A \cap B$. Thus we follow that $C \subseteq A \wedge C \subseteq B \Rightarrow C \subseteq A \cap B$

Suppose that $x \in C$. Then we follow that $x \in A \cap B$. Thus $x \in A$ and $x \in B$. Therefore $C \subseteq A \wedge C \subseteq B$. Therefore $C \subseteq A \cap B \Rightarrow C \subseteq A \wedge C \subseteq B$ thus we follow that

$$C \subseteq A \wedge C \subseteq B \iff C \subseteq A \cap B$$

as desired.

2.1.5

There exists an x such that $x \notin A$

Suppose that there does not exist x such that $x \notin A$. Then we follow that every set is a member of A , which is impossible.

2.1.6

$$A \cap B = B \cap A$$

$$x \in A \cap B \iff x \in A \wedge x \in B \iff x \in B \wedge x \in A \iff x \in B \cap A$$

2.1.7

$$A \cup B = B \cup A$$

$$x \in A \cup B \iff x \in A \vee x \in B \iff x \in B \vee x \in A \iff x \in B \cup A$$

2.1.8

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

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

2.1.31

$$A \subseteq \mathcal{P}(\cup(A))$$

Let $x \in A$. Then we follow that $x \subseteq \cup(A)$. Thus $x \in \mathcal{P}(\cup(A))$. Thus $A \subseteq \mathcal{P}(\cup(A))$.

2.1.32

Let $C \in F$. Then $\mathcal{P}(C) \in \mathcal{P}(\mathcal{P}(\cup F))$

Suppose that $C \in F$. Then we follow that $C \subseteq \cup F$. Therefore $C \in \mathcal{P}(\cup F)$. Thus $\mathcal{P}(C) \in \mathcal{P}(\mathcal{P}(\cup F))$.

the rest of the exercises for this section are more of the same.

2.2 Operations on Sets

Prove the following theorems

2.2.1

Let A be a set and $F \neq \emptyset$. Then

$$A \setminus \cap F = \cup \{A \setminus C : C \in F\}$$

$x \in A \setminus \cap F \Leftrightarrow x \in A \wedge x \notin \cap F \Leftrightarrow x \in A \wedge \neg x \in \cap F \Leftrightarrow x \in A \wedge \neg(\forall(C \in F)(x \in C)) \Leftrightarrow$
 $\Leftrightarrow x \in A \wedge \exists(C \in F)(x \notin C) \Leftrightarrow \exists(C \in F)(x \notin C \wedge x \in A) \Leftrightarrow \exists(C \in F)(x \in A \setminus C) \Leftrightarrow x \in \cup \{A \setminus C : C \in F\}$
 which seems to hold.

2.2.2

Let A, F be sets. Then $A \cup (\cup F) = \cup \{A \cup C : C \in F\}$

$$\begin{aligned} x \in A \cup (\cup F) &\Leftrightarrow x \in A \vee x \in \cup F \Leftrightarrow x \in A \vee (\exists C \in F)(x \in C) \Leftrightarrow \\ &\Leftrightarrow (\exists C \in F)(x \in A) \vee \exists(C \in F)(x \in C) \Leftrightarrow \\ &\Leftrightarrow \exists(C \in F)(x \in A \vee x \in C) \Leftrightarrow \exists(C \in F)(x \in A \cup C) \Leftrightarrow x \in \cup \{A \cup C : C \in F\} \end{aligned}$$

Where we've used the fact that

$$x \in A \Leftrightarrow x \in A \wedge \text{true} \Leftrightarrow x \in A \wedge (\exists C \in F)(\text{true}) \Leftrightarrow (\exists C \in F)(x \in A \wedge \text{true}) \Leftrightarrow (\exists C \in F)(x \in A)$$

don't know if we can use it, but I used it anyways.

2.2.3

Let A, F be sets. Then $A \cap (\cup F) = \cup \{A \cap C : C \in F\}$

$$\begin{aligned} x \in A \cap (\cup F) &\Leftrightarrow x \in A \wedge x \in \cup F \Leftrightarrow x \in A \wedge (\exists C \in F)(x \in C) \Leftrightarrow \\ &\Leftrightarrow \exists(C \in F)(x \in A \wedge x \in C) \Leftrightarrow \exists(C \in F)(x \in A \cap C) \Leftrightarrow x \in \cup \{A \cap C : C \in F\} \end{aligned}$$

2.2.5

Let A and F be sets. Then there exists a unique set ϵ such that for all Y we have that $Y \in \epsilon$ if and only if $Y = A \cap C$ for some $C \in F$.

$\cup F$ exists by union axiom, $A \cap (\cup F)$ exists by subset axiom. Thus $\mathcal{P}(A \cap (\cup F))$ exists by power axiom. Since $Y = A \cap C \Rightarrow Y \subseteq A \cap (\cup F)$, we follow that Y is a subset of $\mathcal{P}(A \cap (\cup F))$, which exists by subset axiom. By extensionality axiom we follow that the set is unique.

2.2.12

If F and G are nonempty sets, then

$$\cap(F \cup G) = \cap(F) \cap \cap(G)$$

$$\begin{aligned} x \in \cap(F \cup G) &\Leftrightarrow (\forall C \in F \cup G)(x \in C) \Leftrightarrow (\forall C \in F)(x \in C) \wedge (\forall C \in G)(x \in C) \Leftrightarrow \\ &\Leftrightarrow x \in \cap(F) \wedge x \in \cap(G) \Leftrightarrow x \in (\cap(F)) \cap (\cap(G)) \end{aligned}$$

2.2.14

Let F be a nonempty set. Then

$$\mathcal{P}(\cap(F)) = \cap\{\mathcal{P}(C) : C \in F\}$$

$$\begin{aligned} x \in \mathcal{P}(\cap(F)) &\Leftrightarrow x \subseteq \cap(F) \Leftrightarrow (\forall y \in x)(y \in \cap(F)) \Leftrightarrow (\forall y \in x)(\forall(C \in F)(y \in F)) \Leftrightarrow \\ &\forall(C \in F)((\forall y \in x)y \in F) \Leftrightarrow \forall(C \in F)(x \subseteq C) \Leftrightarrow \forall(C \in F)(x \in \mathcal{P}(C)) \Leftrightarrow x \in \cap\{\mathcal{P}(C) : C \in F\} \end{aligned}$$

Chapter 3

Relations and Functions

3.1 Ordered Pairs in Set Theory

3.1.1

Define $\langle a, b, c \rangle = \langle \langle a, b \rangle, c \rangle$ for any sets a, b, c . Prove that this yields an ordered tuple; that is, prove that if $\langle x, y, z \rangle = \langle a, b, c \rangle$, then $x = a$, $y = b$, $z = c$.

Suppose that

$$\langle x_1, x_2, x_3 \rangle = \langle y_1, y_2, y_3 \rangle$$

then we follow that

$$\langle \langle x_1, x_2 \rangle, x_3 \rangle = \langle \langle y_1, y_2 \rangle, y_3 \rangle$$

from which we get that $\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle$ and $x_3 = y_3$. From $\langle x_1, x_2 \rangle = \langle y_1, y_2 \rangle$ we get that $x_1 = y_1$ and $x_2 = y_2$. In total we get that

$$\langle \langle x_1, x_2 \rangle, x_3 \rangle = \langle \langle y_1, y_2 \rangle, y_3 \rangle \Rightarrow x_1 = y_1 \wedge x_2 = y_2 \wedge x_3 = y_3$$

Thus we follow that given construction defines an ordered tuple, as desired.

3.1.2

Prove that $(A \cup B) \times C = (A \times C) \cup (B \times C)$

$$x \in (A \cup B) \times C \Leftrightarrow x = \langle y, z \rangle \wedge y \in A \cup B \wedge z \in C \Leftrightarrow x = \langle y, z \rangle \wedge (y \in A \vee y \in B) \wedge z \in C$$

$$\Leftrightarrow (x = \langle y, z \rangle \wedge z \in C) \wedge (y \in A \vee y \in B) \Leftrightarrow$$

$$\Leftrightarrow (x = \langle y, z \rangle \wedge z \in C \wedge y \in A) \vee (x = \langle y, z \rangle \wedge z \in C \wedge y \in B) \Leftrightarrow$$

$$\Leftrightarrow (x \in A \times C) \vee (x \in B \times C) \Leftrightarrow x \in (A \times C) \cup (B \times C)$$

as desired.

3.1.3

Prove that $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$

$$\begin{aligned}
 x \in (A \setminus B) \times C &\Leftrightarrow x = \langle y, z \rangle \wedge y \in A \setminus B \wedge z \in C \Leftrightarrow x = \langle y, z \rangle \wedge (y \in A \wedge y \notin B) \wedge z \in C \\
 &\Leftrightarrow (x = \langle y, z \rangle \wedge z \in C) \wedge (y \in A \wedge y \notin B) \Leftrightarrow \\
 &\Leftrightarrow x = \langle y, z \rangle \wedge z \in C \wedge y \in A \wedge y \notin B \Leftrightarrow \\
 &\Leftrightarrow (x = \langle y, z \rangle \wedge y \in A \wedge z \in C) \wedge (x \neq \langle y, z \rangle \vee y \notin B \vee z \notin C) \Leftrightarrow \\
 &\Leftrightarrow (x = \langle y, z \rangle \wedge y \in A \wedge z \in C) \wedge (x \neq \langle y, z \rangle \vee y \notin B \vee z \notin C) \Leftrightarrow \\
 &\Leftrightarrow (x = \langle y, z \rangle \wedge y \in A \wedge z \in C) \wedge \neg(x = \langle y, z \rangle \wedge y \in B \wedge z \in C) \Leftrightarrow \\
 &\Leftrightarrow (x \in A \times C) \wedge \neg(x \in B \times C) \Leftrightarrow x \in (A \times C) \setminus (B \times C)
 \end{aligned}$$

Used a biconditional defined in "useful things"

3.1.4

Prove that

$$(\cup F) \times C = \cup \{A \times C : A \in F\}$$

$$\begin{aligned}
 x \in (\cup F) \times C &\Leftrightarrow x = \langle y, z \rangle \wedge y \in (\cup F) \wedge z \in C \Leftrightarrow x = \langle y, z \rangle \wedge (\exists A \in F)(y \in A) \wedge z \in C \Leftrightarrow \\
 &\Leftrightarrow (\exists A \in F)(y \in A \wedge x = \langle y, z \rangle \wedge z \in C) \Leftrightarrow (\exists A \in F)(x \in A \times C) \Leftrightarrow \\
 &\Leftrightarrow x \in \cup \{A \times C : A \in F\}
 \end{aligned}$$

3.2 Relations**3.2.1**

Explain why the empty set is a relation

Relation is defined to be a set of ordered pairs. That is, for every $x \in R$, x is an ordered pair. Since we haven't got any elements in the emptyset, we follow that the logical statement is true and therefore emptyset is a relation.

Other way to see it is to assume that it is not a relation. Then we follow that emptyset has an element that is not an ordered pair. Since emptyset does not have any elements, we follow that we have a contradiction.

3.2.2

Prove items 1-3 of Theorem 3.2.7

$$x \in \text{dom}(R^{-1}) \Leftrightarrow \exists y(\langle x, y \rangle \in R^{-1}) \Leftrightarrow \exists y(\langle y, x \rangle \in R) \Leftrightarrow x \in \text{ran}(R)$$

$$x \in \text{ran}(R^{-1}) \Leftrightarrow \exists y(\langle y, x \rangle \in R^{-1}) \Leftrightarrow \exists y(\langle x, y \rangle \in R) \Leftrightarrow x \in \text{dom}(R)$$

$$\begin{aligned} x \in (R^{-1})^{-1} &\Leftrightarrow \exists y \exists z (\langle y, z \rangle \in (R^{-1})^{-1}) \wedge x = \langle y, z \rangle \Leftrightarrow \exists y \exists z (\langle z, y \rangle \in (R^{-1})) \wedge x = \langle y, z \rangle \Leftrightarrow \\ &\Leftrightarrow \exists y \exists z (\langle y, z \rangle \in R) \wedge x = \langle y, z \rangle \Leftrightarrow x \in R \end{aligned}$$

3.2.4

$$\text{dom}(R) = \{0, 1, 2, 3, 4\}$$

$$\text{ran}(R) = \{0, 1, 2, 3, 4\}$$

$$R \circ R = \{\langle 0, 2 \rangle, \langle 0, 3 \rangle, \langle 0, 0 \rangle, \langle 0, 3 \rangle, \langle 0, 4 \rangle, \langle 1, 0 \rangle, \langle 1, 3 \rangle, \langle 1, 4 \rangle, \langle 1, 3 \rangle, \langle 1, 2 \rangle, \langle 2, 1 \rangle,$$

$$\langle 2, 2 \rangle, \langle 2, 3 \rangle, \langle 2, 2 \rangle, \langle 2, 4 \rangle, \langle 3, 3 \rangle, \langle 3, 2 \rangle, \langle 4, 4 \rangle\}$$

$$R[\{1\}] = \{\langle 1, 2 \rangle, \langle 1, 3 \rangle\}$$

$$R^{-1}[\{1\}] = \{\langle 1, 0 \rangle\}$$

$$R[\{1\}] = \{2, 3\}$$

$$R^{-1}[\{1\}] = \{0\}$$

3.2.5

Suppose that R is a relation. Prove that $R|(A \cup B) = (R|A) \cup (R|B)$ for any sets A, B

$$\begin{aligned} x \in R|(A \cup B) &\Leftrightarrow (\exists y \in A \cup B)(\exists z \in \text{ran}(R))(\langle y, z \rangle \in R \wedge x = \langle y, z \rangle) \Leftrightarrow \\ &\Leftrightarrow (\exists y \in A)(\exists z \in \text{ran}(R))(\langle y, z \rangle \in R \wedge x = \langle y, z \rangle) \vee (\exists y \in B)(\exists z \in \text{ran}(R))(\langle y, z \rangle \in R \wedge x = \langle y, z \rangle) \Leftrightarrow \\ &\Leftrightarrow x \in R|A \vee x \in R|B \Leftrightarrow x \in (R|A \cup R|B) \end{aligned}$$

thus

$$R|(A \cup B) = (R|A) \cup (R|B)$$

as desired.

3.2.6

Let R be a relation. Prove that $\text{fld}(R) = \bigcup \bigcup R$.

$$\begin{aligned} x \in \text{fld}(R) &\Leftrightarrow x \in \text{dom}(R) \vee x \in \text{ran}(R) \Leftrightarrow (\exists z \in R)(\exists y)(z = \langle x, y \rangle \vee z = \langle y, x \rangle) \Leftrightarrow \\ &\Leftrightarrow (\exists z \in R)(\exists y)(z = \{\{x\}, \{x, y\}\} \vee z = \{\{y\}, \{y, x\}\}) \Leftrightarrow (\exists z \in R)(x \in \bigcup z) \Leftrightarrow x \in \bigcup \bigcup R \end{aligned}$$

3.2.7

Let R and S be two relations and let A, B, C be sets. Prove that $R[A]$, $R^{-1}[B]$, $R[C]$ and $R \circ S$ are sets.

Given that R and S are relation, we follow that both of them are sets, $\bigcup \bigcup R$ and $\bigcup \bigcup S$ are sets and $\text{dom}(R), \text{ran}(R), \text{dom}(S), \text{ran}(S)$ are sets. Thus we follow that $R[A]$ is a subset of R , which is a set; $R^{-1}[B]$ and $R[C]$ are subsets of $\bigcup \bigcup R$, and $R \circ S$ are subsets of a set $\text{dom}(R) \times \text{ran}(S)$, which is a set.

3.2.8

Let R be a relation and G be a set. Prove that $\{R[C] : C \in G\}$ is a set. Prove that if G is nonempty, then $\{R[C] : C \in G\}$ is also nonempty

If R is a relation, then $\text{ran}(R)$ is a set. Therefore $\mathcal{P}(\text{ran}(R))$ is a set. Thus for any set C , $R[C] \subseteq \text{ran}(R)$, therefore $R[C] \in \mathcal{P}(\text{ran}(R))$. Thus $\{R[C] : C \in G\}$ is a subset of $\mathcal{P}(\mathcal{P}(\text{ran}(R)))$, which is a set.

Suppose that G is nonempty. Then we follow that there exists $C \in G$. Thus $R[C]$ is a set. Thus $R[C] \in \{R[C] : C \in G\}$. Therefore $\{R[C] : C \in G\}$ is nonempty.

3.2.10

Let R be a relation on A . Prove that R is symmetric if and only if

$$R^{-1} \subseteq R$$

In forward direction: Suppose that R is symmetric. Let $y \in R^{-1}$. We follow that there exists u, v such that $y = \langle u, v \rangle$. Thus $\langle v, u \rangle \in R$ by the definition. Since R is symmetric, we follow that $\langle u, v \rangle \in R$. Therefore $y \in R \Rightarrow y \in R$, as desired.

In reverse direction: Suppose that $R^{-1} \subseteq R$. Let $y \in R$. Then we follow that there exists u, v such that $y = \langle u, v \rangle$. Thus $\langle v, u \rangle \in R^{-1}$. Since $R^{-1} \subseteq R$, we follow that $\langle v, u \rangle \in R$. Thus we follow that $\langle u, v \rangle \in R \Rightarrow \langle u, v \rangle \in R$. Thus R is symmetric by definition, as desired.

3.2.19

Prove item (2) of Theorem 3.2.8

$$R[\bigcup G] = \bigcup R[C] : C \in G$$

$$\begin{aligned} x \in R[\bigcup G] &\Leftrightarrow (\exists y \in \bigcup G)(\langle y, x \rangle \in R) \Leftrightarrow (\exists C \in G)(y \in C \wedge \langle y, x \rangle \in R) \Leftrightarrow \\ &\Leftrightarrow (\exists C \in G)(x \in R[C]) \Leftrightarrow x \in \bigcup R[C] : C \in G \end{aligned}$$

3.2.20

Prove item (4) of Theorem 3.2.8

$$\begin{aligned} x \in R[\bigcap G] &\Leftrightarrow (\exists y \in \bigcap G)(\langle y, x \rangle \in R) \Leftrightarrow \exists y(\forall C \in G)(y \in C \wedge \langle y, x \rangle \in R) \Rightarrow \\ &\Rightarrow (\forall C \in G)(\exists y \in C)(\langle y, x \rangle \in R) \Leftrightarrow (\forall C \in G)(x \in R[C]) \Leftrightarrow x \in \bigcap \{R[C] : C \in G\} \end{aligned}$$

3.2.22

Let R and S be single-rooted relations. Prove that $R \circ S$ is single-rooted

Suppose that $\langle x, y \rangle \in R \circ S$. Then we follow that there exists $z \in \text{fld}(R)$ such that $\langle x, z \rangle \in S$ and $\langle z, y \rangle \in R$. Suppose that there exists $\langle x', y \rangle \in R \circ S$ such that $x \neq x'$. Then we follow that there exists $j \in \text{fld}(R)$ such that $\langle x', j \rangle \in S$ and $\langle j, y \rangle \in R$. If $j = z$, then we follow that $\langle x', z \rangle \in S \wedge \langle x, z \rangle \in S \wedge x \neq x'$. Thus we conclude that S is not single rooted, which is a contradiction. If $j \neq z$, then we follow that

$$\langle j, y \rangle \in R \wedge \langle z, y \rangle \in R \wedge j \neq z$$

thus R is not single-rooted, which is also a contradiction. Therefore we conclude that if $\langle x', y \rangle \in R \circ S$, then $x' = x$. Therefore we follow that $R \circ S$ is single rooted, as desired.

3.3 Functions**3.3.1**

Prove Lemma 3.3.5 and Lemma 3.3.13

Suppose that F and G are functions such that $\text{dom}(F) = \text{dom}(G)$. Lemma 3.3.5 states that $F = G$ iff $F(x) = G(x)$ for every $x \in \text{dom}(F)$. If $F = G$, then

$$F(x) = y \Leftrightarrow \langle x, y \rangle \in F \Leftrightarrow \langle x, y \rangle \in G \Leftrightarrow G(x) = y$$

thus $F(x) = G(x)$ for every $x \in \text{dom}(F)$.

Now suppose that $F(x) = G(x)$ for every $x \in \text{dom}(F)$. Then we follow that

$$z \in F \Leftrightarrow z = \langle x, y \rangle \wedge F(x) = y \Leftrightarrow z = \langle x, y \rangle \wedge G(x) = y \Leftrightarrow z \in G$$

as desired.

Lemma 3.3.13 states that a function F is one-to-one if and only if F is single-rooted.

Suppose that F is one-to-one and F is not single rooted. Then we follow that there exists $x, y \in F$ such that $x = \langle u, w \rangle \in F, y = \langle j, w \rangle \in F$. Then we follow that $F(u) = w = F(j)$, which is a contradiction.

Proof of converse is extremely simular.

3.3.2

Let F be a function and let $A \subseteq B \subseteq \text{dom}(F)$. Prove that $F[A] \subseteq F[B]$.

$$x \in F[A] \Leftrightarrow x = \langle u, v \rangle \wedge u \in A \wedge \langle u, v \rangle \in F \Rightarrow x = \langle u, v \rangle \wedge u \in B \wedge \langle u, v \rangle \in F \Leftrightarrow x \in F[B]$$

3.3.5

Let $g : C \rightarrow D$ be a one-to-one function, $A \subseteq C$ and $B \subseteq C$. Prove that if $A \cup B = \emptyset$, then $g[A] \cap g[B] = \emptyset$.

Suppose that $A \cap B = \emptyset$ and $g[A] \cap g[B] \neq \emptyset$. Then we follow that there exists $x \in g[A] \cap g[B]$. Thus

$$x \in g[A] \wedge x \in g[B] \Leftrightarrow (\exists y \in A)(\langle y, x \rangle \in g) \wedge (\exists z \in B)(\langle z, x \rangle \in g)$$

since g is one-to-one, we follow that $z = y$. Thus there exists $z \in A \cap B$, therefore $A \cap B \neq \emptyset$, which is a contradiction.

3.3.9

Suppose that $F : X \rightarrow Y$ is a function. Prove that if $C \subseteq Y$ and $D \subseteq Y$, then $F^{-1}[C \cap D] = F^{-1}[C] \cap F^{-1}[D]$.

Since F is a function, we follow that F^{-1} is a single-rooted relation. Thus we follow that

$$F^{-1}[C \cap D] = F^{-1}[C] \cap F^{-1}[D]$$

as desired.

3.3.10

Let F, G be functions from A to B . Suppose $F \subseteq G$. Prove that $F = G$.

Suppose that $x \in A$. Then we follow that

$$(\exists y \in B)(\langle x, y \rangle \in F) \Rightarrow (\exists y \in B)(\langle x, y \rangle \in G)$$

Thus we follow that for every $x \in A$ (where $\text{dom}(F) = A = \text{dom}(G)$)

$$F(x) = G(x)$$

thus by the lemma 3.3.5 we follow that

$$F = G$$

as desired.

3.3.11

Let C be a set of functions. Suppose that for all f and g in C , we have either $f \subseteq g$ or $g \subseteq f$.

(a) Prove that $\cup C$ is a function

Firstly, since C is a set of sets of ordered pairs, we follow that $\cup C$ is a set of ordered pairs, and therefore it is a relation. Suppose that $x \in \cup C$. Then we follow that there exist $f \in C$ such that $x \in f$ and $x = \langle u, v \rangle$. Suppose that there exists $y \in \cup C$, such that $y = \langle u, v' \rangle$, where $u' \neq u$. Since $y \in \cup C$, we follow that there exists $g \in C$ such that $y \in g$. Because $u' \neq u$, we follow that $g \neq f$. Therefore either $g \subset f$, or $f \subset g$. In both cases we follow that we can't have the case that $u' \neq u$. Thus we follow that for $x, y \in \cup C$, whenever the first part of the x is equal to the first part of y , we follow that the last parts are also equal. Thus we follow that $\cup C$ is a single-valued relation, and therefore it is a function.

3.3.13

Assume $f : A \rightarrow B$ is onto B . Let $C \subseteq B$. Prove that $f[f^{-1}[C]] = C$

$$\begin{aligned} x \in f[f^{-1}[C]] &\Leftrightarrow (\exists y \in f^{-1}[C])(f(y) = x) \Leftrightarrow (\exists z \in C)(\langle y, z \rangle \in f \wedge f(y) = x) \Leftrightarrow \\ &\Leftrightarrow (\exists z \in C)(f(y) = z \wedge f(y) = x) \Leftrightarrow (\exists z \in C)(x = z) \Leftrightarrow x \in C \end{aligned}$$

this notation may be a bit sloppy, but the result is derived faithfully.

3.3.15

Let $f : A \rightarrow B$ be a one-to-one function. Define $G : \mathcal{P}(A) \rightarrow \mathcal{P}(B)$ by $G(X) = f[X]$, for each $X \in \mathcal{P}(A)$. Prove that G is one-to-one.

Let $X_1, X_2 \in \mathcal{P}(A)$ be such that $G(X_1) = G(X_2)$. Then we follow that

$$f[X_1] = f[X_2]$$

thus

$$x \in X_1 \Leftrightarrow (\exists y \in f[X_1])(\langle x, y \rangle \in f) \Leftrightarrow (\exists y \in f[X_2])(\langle x, y \rangle \in f) \Leftrightarrow x \in X_2$$

thus we follow that $X_1 = X_2$. Therefore $G(X_1) = G(X_2) \rightarrow X_1 = X_2$, thus G is one-to-one, as desired.

3.3.21

Let $\langle A_i : i \in I \rangle$ be an indexed function with nonempty terms. Prove that there is an indexed function $x_i : i \in I$ is that $x_i \in A_i$ for all $i \in I$, using theorem 3.3.24

Let C be defined as

$$C = \text{ran}(A)$$

then by theorem 3.3.24 we follow that there exists a function $H : C \rightarrow \cup C$ such that

$$H(A_i) \in A_i$$

define $x = H \circ A$. Then we follow that

$$x(i) = H(A(i)) = H(A_i) \in A_i$$

thus we have the desired function.

3.4 Order Relations**3.4.1**

Define a relation \preceq on the set of integers Z by $x \preceq y$ if and only if $x \leq y$ and $x + y$ is even for all $x, y \in Z$. Prove that \preceq is a partial order on Z

Suppose that $x, y \in Z$. Poset requirements of \leq are going to be omitted.

Then we follow that

$$x + x = 2x$$

, therefore we've got symmetry. If $x \leq y$, $y \leq z$, $x + y$ is even and $y + z$ is even, then we follow that $x + y + y + z$ is even, therefore $x + z - 2y$ is also even. Antisymmetry follows from \leq .

Then answer the following questions about the poset (Z, \preceq)

(a) Is $S = \{1, 2, 3, 4, 5, 6, \dots\}$ a chain in Z

No, since $1 + 2 = 3$ is not even, we follow that $1 \not\preceq 2 \wedge 2 \not\preceq 1$.

(b) Is $S = \{1, 3, 5, 7, \dots\}$ a chain in Z ?

Suppose that $x, y \in Z$. Then we follow that there exist $m, n \in Z$ such that

$$x = 2m + 1$$

$$y = 2n + 1$$

thus

$$x + y = 2m + 2n + 2$$

thus $x + y$ is even for all cases. Since \preceq is a total order, we follow that S is indeed a chain in Z .

(c) Does the set $S = \{1, 2, 3, 4, 5\}$ have a lower bound or an upper bound?

No, since we've got both odd and even numbers in S , we follow that there is no $x \in Z$ such that $x + s$ is even for all $s \in S$, thus there does not exist an element such that $x \preceq s$ or $s \preceq x$ for all $s \in S$

(d) Does $S = \{1, 2, 3, 4, 5\}$ have any maximal or minimal elements?

Yes, 1, 2 are minimal elements and 4, 5 are maximal elements.

3.4.2

Prove Lemma 3.4.5

Suppose that (A, \preceq) is a poset and let \prec be the strict order corresponding to \preceq . Let $x, y, z \in A$. Then we follow that:

(1)

Since $x = x$, we follow that $x \not\prec x$ by definition of a strict order

(2)

Suppose that $x \prec y$. Then we follow that $x \preceq y$ and $y \neq x$. Thus by antisymmetry of \preceq we follow that $y \not\preceq x$, and therefore $y \not\prec x$ by definition.

(3)

Suppose that $x \prec y$ and $y \prec z$. Therefore we follow that $x \preceq y$ and $y \preceq z$, which gives us that $x \preceq z$. Suppose that $x = z$. Then we follow that $z \preceq y$ and thus $z = y$, which is a contradiction. Thus we follow that $x \preceq z$ and $x \neq z$, therefore $x \prec z$, as desired.

(4)

If $x = y$ then $x \not\prec y$ and $y \not\prec x$ by definition of strict order

Both $x \prec y$ and $y \prec x$ imply that $x \neq y$, and by case (2) we follow that for given $x, y \in A$ only one of $x = y$, $x \prec y$ or $y \prec x$ hold.

3.4.3

Find the greatest lower bound of the set $S = \{15, 20, 30\}$ in the poset $(A, |)$, where $A = \{n \in \mathbb{N} : n > 0\}$. Now find the least upper bound of S .

5 and 60 (gcd and lcm) respectively.

3.4.4

Let (A, \preceq) be a poset and let $S \subseteq A$. Suppose that b is the largest element of S . Prove that b is also the least upper bound of S .

Suppose that s is an upper bound of S . Then from the definition of the lower bound we follow that $x \prec s$ for every $x \in A$. Since $b \in S$ we follow that $b \prec s$. Thus b is the least upper bound (can't we just call it supremum?) of A by definition.

3.4.11

Let (B, \preceq') be a poset. Suppose $h : A \rightarrow B$ is an injective function. Define the relation \preceq on A by $x \preceq y$ if and only if $h(x) \preceq' h(y)$, for all $x, y \in A$. Prove that \preceq is a partial order.

Let $x, y, z \in A$. Since h is a function, we follow that $x = x$ implies that $h(x) = h(x)$, therefore $h(x) \preceq' h(x)$, thus $x \preceq x$. Thus we've got reflexivity.

If $x \preceq y$ and $y \preceq z$ we follow that $h(x) \preceq' h(y)$ and $h(y) \preceq' h(z)$, from which we follow that $h(x) \preceq' h(z)$ and therefore $x \preceq z$.

Suppose that $x \preceq y$ and $y \preceq x$. Then we follow that $h(x) \preceq' h(y)$ and $h(y) \preceq' h(x)$. Thus $h(y) = h(x)$. Because h is one-to-one, we follow that this implies that $x = y$. Thus we've got antisymmetry. Therefore \preceq is indeed a poset.

3.4.12

Let (B, \preceq') be a totally ordered. Suppose $h : A \rightarrow B$ is an injective function. Define the relation \preceq on A by $x \preceq y$ if and only if $h(x) \preceq' h(y)$, for all $x, y \in A$. Prove that \preceq is a partial order.

We follow that \preceq is a poset from previous exercise. Suppose that $x, y \in A$. then we follow that $h(x) \preceq' h(y) \vee h(y) \preceq' h(x)$. Thus $x \preceq y \vee y \preceq x$. Therefore \preceq is a total order.

3.4.14

Analogous to 4

3.4.14

Let \preceq be a partial order of A . Let $C \subseteq A$. Show that \preceq_C is a partial order on C . Show that if \preceq is a total order on A , then \preceq_C is a total order on C .

Everything follows directly from definitions.

3.4.17

Let \preceq be a partial order on A . Show that $\text{fld}(\preceq) = A$.

For every $x \in A$ we've got that $x \preceq x$, thus we follow that $\langle x, x \rangle \in \preceq$, thus $x \in \text{fld}(\preceq)$. Thus $A \subseteq \text{fld}(\preceq)$. Since $\text{fld}(\preceq) \subseteq A$ we follow that $A = \text{fld}(\preceq)$, as desired.

3.4.18

Let C be a set where each $\preceq \in C$ is a partial order on its field. Suppose that for any \preceq, \preceq' in C either $\preceq \subseteq \preceq'$ or $\preceq' \subseteq \preceq$

(a) Show that for every \preceq, \preceq' in C if $\preceq \subseteq \preceq'$, then $\text{fld}(\preceq) \subseteq \text{fld}(\preceq')$

Suppose that $\preceq \subseteq \preceq'$. Then we follow that $\text{fld}(\preceq) = \bigcup \preceq$ and $\text{fld}(\preceq') = \bigcup \preceq'$. Suppose that

$$x \in \text{fld}(\preceq)$$

then we follow that there exists y such that $\langle x, y \rangle \in \preceq$ or $\langle y, x \rangle \in \preceq$. Since $\preceq \subseteq \preceq'$, we follow that $\langle x, y \rangle \in \preceq'$ or $\langle y, x \rangle \in \preceq'$. Thus $x \in \text{fld}(\preceq')$. Thus $x \in \text{fld}(\preceq) \Rightarrow x \in \text{fld}(\preceq')$, as desired.

(b) Let \preceq^C be the relation $\bigcup C$ with field $\bigcup \{\text{fld}(\preceq) : \preceq \in C\}$. Prove that \preceq^C is a partial order on its field

Since $\preceq^C = \bigcup C$ we follow that if $x \in \bigcup \{\text{fld}(\preceq) : \preceq \in C\}$, then there exists $\preceq' \in C$ such that $x \in \text{fld}(\preceq')$. Thus, by the fact that \preceq' is a partial order, we follow that $\langle x, x \rangle \in \preceq'$. Thus $\langle x, x \rangle \in \bigcup C$, and therefore $\langle x, x \rangle \in \preceq^C$. Thus \preceq^C is reflexive.

Suppose that $x, y, z \in \bigcup \{\text{fld}(\preceq) : \preceq \in C\}$. Then we follow that there exist $\preceq_x, \preceq_y, \preceq_z$ such that

$$x \in \text{fld}(\preceq_x)$$

and so on. From the description of C we follow that $\preceq_x \subseteq \preceq_y$ or $\preceq_y \subseteq \preceq_x$, which in any case means that there exists \preceq_{xy} (equal to either of them) such that

$$\{x, y\} \subseteq \text{fld}(\preceq_{xy})$$

same goes for \preceq_z and \preceq_{xy} , which means that there exists \preceq' such that

$$\{x, y, z\} \subseteq \text{fld}(\preceq')$$

Since \preceq' is a partial order, we follow that if $x \preceq' y$ and $y \preceq' z$ implies that $x \preceq' z$, therefore $\langle x, z \rangle \in \preceq'$, and therefore $\langle x, z \rangle \in \preceq^C$, thus the relation is transitive.

Now let's go back a bit and focus on \preceq_{xy} . We follow that if $x \preceq_{xy} y$ and $y \preceq_{xy} x$, then by antisymmetry of \preceq_{xy} we follow that $x = y$. Thus we've got the antisymmetry of \preceq^C .

Thus \preceq^C satisfies all requirements of a poset, as desired.

3.4.19

Let (A, \preceq) and (B, \preceq') be posets. Define the relation \preceq_l on $A \times B$ by

$$\langle a, b \rangle \preceq_l \langle x, y \rangle \iff a \prec x \vee (a = x \wedge b \preceq' y)$$

for all $\langle a, b \rangle$ and $\langle x, y \rangle$ in $A \times B$.

(a) Prove that \preceq_l is a partial order on $A \times B$

Let $a \in A$ and $b \in B$. Then we follow that $b \preceq' b$ and $a = a$, thus

$$\langle a, b \rangle \preceq_l \langle a, b \rangle$$

If for some $a_1, a_2, a_3 \in A$ and $b_1, b_2, b_3 \in B$ it is true that

$$\langle a_1, b_1 \rangle \preceq_l \langle a_2, b_2 \rangle$$

and

$$\langle a_2, b_2 \rangle \preceq_l \langle a_3, b_3 \rangle$$

then we follow that

$$a_1 \prec a_2 \vee (a_1 = a_2 \wedge b_1 \preceq' b_2)$$

and

$$a_2 \prec a_3 \vee (a_2 = a_3 \wedge b_2 \preceq' b_3)$$

If $a_1 = a_2 = a_3$, then we follow that $b_1 \preceq' b_2$ and $b_2 \preceq' b_3$, from which we follow that $b_1 \preceq b_3$ and therefore $\langle a_1, b_1 \rangle \preceq \langle a_3, b_3 \rangle$.

If $a_1 \neq a_2$ and $a_2 = a_3$ then we follow that $a_1 \prec a_2$, thus $a_1 \prec a_3$, therefore $\langle a_1, b_1 \rangle \preceq_l \langle a_3, b_3 \rangle$. Similar case holds if $a_1 = a_2$ and $a_2 \neq a_3$

If $a_1 \neq a_2$ and $a_2 \neq a_3$, then we follow that $a_1 \prec a_2$ and $a_2 \prec a_3$, from which we follow that $a_1 \preceq a_3$. If $a_1 = a_3$, then we follow that $a_1 \neq a_2$, which is a contradiction. Thus $a_1 \neq a_3$. Thus $a_1 \prec a_3$. Therefore $\langle a_1, b_1 \rangle \preceq_l \langle a_3, b_3 \rangle$

Thus we follow that $\langle a_1, b_1 \rangle \preceq_l \langle a_3, b_3 \rangle$ for all a_1, a_3 , thus we've got the transitive condition.

Now suppose that $\langle a_1, b_1 \rangle \preceq_l \langle a_2, b_2 \rangle$ and $\langle a_2, b_2 \rangle \preceq_l \langle a_1, b_1 \rangle$. If $a_1 \neq a_2$, then we follow that $a_1 \prec a_2$ and $a_2 \prec a_1$, which is not possible, thus we conclude that $a_1 = a_2$. Thus we follow that $b_1 \preceq' b_2$ and $b_2 \preceq' b_1$, from which we follow that $b_1 = b_2$. Thus $\langle a_1, b_1 \rangle \preceq_l \langle a_2, b_2 \rangle$ and $\langle a_2, b_2 \rangle \preceq_l \langle a_1, b_1 \rangle$, then we follow that $\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle$. Thus we've got antisymmetry.

Now we can follow that \preceq_l satisfies all of the conditions of poset, as desired.

(b) Suppose that both \preceq and \preceq' are total orders on their respective sets. Prove that \preceq_l is a total order on $A \times B$.

Suppose that $\langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in A \times B$ are arbitrary. It follow that $a_1 \preceq a_2$ or $a_2 \preceq a_1$. Thus $a_1 \prec a_2 \vee a_2 \prec a_1 \vee a_1 = a_2$. We also follow that $b_1 \preceq' b_2$ or $b_2 \preceq' b_1$. This it can be shown that

$$\langle a_1, b_1 \rangle \preceq_l \langle a_2, b_2 \rangle$$

or

$$\langle a_2, b_2 \rangle \preceq_l \langle a_1, b_1 \rangle$$

as desired.

3.5 Congruence and Preorder

3.5.1

Let \sim be an equivalence relation on A . Let $f : A \rightarrow A/\sim$ be defined by

$$f(x) = [x]$$

for all $x \in A$. Show that the function f is one-to-one if and only if each equivalence class in A/\sim is a singleton.

In forward direction: Suppose that

$$f(x) = [x]$$

is one-to-one. Suppose that $x, y \in [x]$. Then we follow that $f(x) = f(y)$. Thus by the fact that f is one-to-one we follow that $x = y$. Thus $[x]$ is a singleton.

In reverse direction: Suppose that each $[x]$ is a singleton. Then we follow that if $x \neq y$, then $f(x) \neq f(y)$. Therefore f is one-to-one, as desired.

3.5.2

Prove theorem 3.5.6

Let \sim be an equivalence relation on A and let $f : A \times A \rightarrow A$.

Suppose that there exists a function $\hat{f} : A/\sim \times A/\sim \rightarrow A/\sim$ such that $\hat{f}([x], [y]) = [f(x, y)]$ then we follow that if $x \sim w$ and $y \sim z$, then $[x] = [w]$ and $[y] = [z]$, thus

$$\hat{f}([x], [y]) = [f(x, y)] = \hat{f}([w], [z]) = [f(w, z)]$$

thus we follow that $[f(x, y)] = [f(w, z)]$, therefore $f(x, y) \sim f(w, z)$. Thus we follow that $x \sim w$ and $y \sim z$ implies that $f(x, y) \sim f(w, z)$, therefore f is congruent with \sim .

If $x \sim w$ and $y \sim z$ implies that $f(x, y) \sim f(w, z)$, then we follow that we can construct a relation \hat{f} by

$$\hat{f} = \{ \langle [x], [y] \rangle, [f(x, y)] \mid x, y \in A \}$$

if $[x] = [w]$ and $[y] = [z]$, then we follow that $x \sim w$ and $y \sim z$, therefore $f(x, y) \sim f(w, z)$, therefore $[f(x, y)] = [f(w, z)]$. Thus this relation is a function, as desired.

3.5.3

Prove theorem 3.5.7

Suppose that \sim is an equivalence relation on A and R is a relation on A .

If there exists a relation \hat{R} on A/\sim such that $\hat{R}([x], [y]) \iff R(x, y)$ then we follow that if xRy for some $x, y \in A$ then $\hat{R}([x], [y])$. If there exist $w, z \in A$ such that $x \sim w$ and $y \sim z$, then $[x] = [w]$ and $[y] = [z]$, therefore $\hat{R}([w], [z])$ and thus wRz . Thus we follow that xRy iff wRz . Thus R is congruent with \sim .

If R is congruent with \sim , then we can create a relation \hat{R} by

$$\hat{R} = \{ \langle [x], [y] \rangle : \langle x, y \rangle \in R \}$$

that will satisfy the desired conditions.

3.5.4

Prove lemma 3.5.9

Let (A, \preceq) be a preordered set and let \sim be the relation on A defined by

$$a \sim b \iff a \preceq b \wedge b \preceq a$$

Then we follow that for $a \in A$ $a \preceq a$ by reflexivity of \preceq , therefore $a \sim a$ and thus \sim is reflexive.

If $a, b, c \in A$ such that $a \sim b$ and $b \sim c$, then we follow that

$$a \preceq b \wedge b \preceq c \Rightarrow a \preceq c$$

$$c \preceq b \wedge b \preceq a \Rightarrow c \preceq a$$

thus $a \sim c$. Therefore \sim is transitive.

Suppose that $x \sim y$. Then we follow that $x \preceq y$ and $y \preceq x$. Thus we follow that $y \sim x$, therefore \sim is symmetric. Thus \sim is an equivalence relation, as desired.

3.5.5

Prove lemma 3.5.10

Suppose that (A, \preceq) is a preordered set. Let \sim be the derived equivalence relation on A . Suppose that $a, b, c, d \in A$ are such that $a \sim c$ and $b \sim d$.

If $a \preceq b$ then we follow that $b \preceq d$ by $b \sim d$, therefore $a \preceq d$ by transitive property. From $a \sim c$ we derive that $c \preceq a$, therefore we follow that $c \preceq d$. Similar implication hold for reverse case. Thus we follow that \preceq is congruent with \sim .

Chapter 4

The Natural Numbers

4.1 Inductive Sets

4.1.1

Let I and J be inductive sets. Prove that $I \cap J$ is also inductive.

Since I and J are both inductive, we follow that $\emptyset \in I$ and $\emptyset \in J$, thus $\emptyset \in I \cap J$.

Suppose that $x \in I \cap J$. Then we follow that $x \in I$ and $x \in J$. Since both of them are inductive, we follow that $x^+ \in I$ and $x^+ \in J$, therefore $x^+ \in I \cap J$. Thus we've got that

$$\emptyset \in I \cap J \wedge (\forall x \in I \cap J)(x^+ \in I \cap J)$$

thus we follow that $I \cap J$ is inductive, as desired.

4.1.2

Prove that if A is a transitive set, then A^+ is also a transitive set.

Suppose that A is transitive. That means that $(\forall x \in A)(x \subseteq A)$. By definition, $A^+ = A \cup \{A\}$. Now let $y \in A^+$. We follow that $y = A \vee y \in A$. If $y = A$, then we follow that $y \subseteq A^+$. If $y \in A$, then we follow that $y \subseteq A$ by the fact that A is transitive, therefore $y \subseteq A^+$. Thus we've got that

$$(\forall y \in A^+)(y \subseteq A^+)$$

thus we follow that A^+ is a transitive set, as desired.

4.1.3

Prove that if A is a transitive set if and only if $A \subseteq \mathcal{P}(A)$.

Suppose that A is transitive. Then we follow that $(\forall x \in A)(x \subseteq A)$. Thus if $x \in A$, then $x \subseteq A$ and therefore $x \in \mathcal{P}(A)$. Thus we follow that $A \subseteq \mathcal{P}(A)$.

If $A \subseteq \mathcal{P}(A)$, then we follow that if $x \in A$, then $x \in \mathcal{P}(A)$ and therefore $x \subseteq A$. Thus A is transitive.

4.1.6

Prove Proposition 4.1.9

4.1.9 states that

$$\bigcup(A \cup B) = (\bigcup A) \cup (\bigcup B)$$

$$\begin{aligned} x \in \bigcup(A \cup B) &\Leftrightarrow (\exists C \in A \cup B)(x \in C) \Leftrightarrow (\exists C \in A)(x \in C) \vee (\exists C \in B)(x \in C) \Leftrightarrow \\ &\Leftrightarrow x \in \bigcup A \vee x \in \bigcup B \Leftrightarrow x \in (\bigcup A) \cup (\bigcup B) \end{aligned}$$

4.1.7

Prove that $n \neq n^+$ for all $n \in \omega$

This is true in general by regularity axiom, but let's apply some induction. Let

$$I = \{n \in \omega : n \neq n^+\}$$

$0 \neq \{0\}$, since $0 \in \{0\}$ and $0 \notin 0$ (because it is an empty set). Thus $0 \in I$.

Suppose that $n \in I$. Then we follow that $n \neq n^+$. Suppose that $n^+ = (n^+)^+$. Then we follow by 4.1.12 that $n = n^+$, which is a contradiction, because $n \in I$. Thus we follow that $n \in I \Rightarrow n^+ \in I$, therefore I is inductive, therefore $I = \omega$, as desired.

4.1.8

Prove that $n^+ \not\subseteq n$ for all $n \in \omega$

Suppose that $n^+ \subseteq n$. Since $n^+ = n \cup \{n\}$, we follow that $n \subseteq n^+$. Thus by double inclusion we've got that $n^+ = n$, which contradicts previous exercise.

4.1.9

Prove that for all $m \in \omega$ and all $n \in \omega$, if $m \in n$, then $n \not\subseteq m$.

Let

$$I = \{n \in \omega : m \in n \Rightarrow n \not\subseteq m\}$$

Since $m \in 0 \Leftrightarrow m \in \emptyset$ is always false, we follow that 0 is vacuously in I .

Let $n \in I$. Let $m \in \omega$ be such that $m \in n^+$. Thus $m \in n \cup \{n\}$. Thus $m \in n \vee m = n$.

If $m \in n$, then we follow that $n \not\subseteq m$, thus $(\exists y \in n)(y \notin m)$. Thus $(\exists y \in n \cup \{n\})(y \notin m)$. Therefore $n^+ \not\subseteq m$.

If $m = n$, then we follow that $n^+ \not\subseteq n$ by exercise 4.1.8. Thus we conclude that $n \in I \Rightarrow n^+ \in I$. Therefore I is inductive and thus $I = \omega$, as desired.

4.1.10

Conclude from exercise 9 that $n \notin n$ for all $n \in \omega$.

Suppose that $n \in n$. Then we follow by previous exercise that $n \not\subseteq n$, which is bonkers.

4.1.11

Let A be a set and suppose that $\bigcup A = A$. Prove that A is transitive and for all $x \in A$ there is a $y \in A$ such that $x \in y$.

Let $x \in A$ be arbitrary. Then we follow that $x \subseteq \bigcup A$ and thus $x \subseteq A$. Thus we follow that A is transitive, as desired.

Suppose that $x \in A$ and suppose that for all $y \in A$ we've got that $x \notin y$. Then we follow that $(\forall y \in A)(x \notin y)$. Thus

$$(\forall y \in A)(x \notin y) \Leftrightarrow \neg(\exists y \in A)(x \in y) \Leftrightarrow x \notin \bigcup A \Leftrightarrow x \notin A$$

which is a contradiction.

4.2 The Recursion Theorem on ω

How would one modify the proof of Theorem 4.2.1 in order to establish the following:

Theorem. Let A be a set and let $a \in A$. Suppose that $f : \omega \times A \rightarrow A$ is a function. Then there exists a unique function $h : \omega \rightarrow A$ such that

$$h(0) = a$$

$$h(n^+) = f(n, h(n))$$

We can define S and h in normal fashion, then prove that $\langle 0, a \rangle \in h$ and $\langle n, u \rangle \in h$ will imply that $\langle n^+, f(n^+, h(n)) \rangle \in h$, thus concluding the proof of claim 1.

Proof of claim 2 for the base case will not be altered. (IH) Will be modified in notation.

Proof of uniqueness does not depend on the domain of the functions and is true in general.

4.2.2

Let $a \in A$ and $f : A \rightarrow A$ be a function such that $a \notin \text{ran}(f)$. Suppose that $h : \omega \rightarrow A$ satisfies

$$(1) h(0) = a$$

$$(2) h(n^+) = f(h(n))$$

Assume that h is one-to-one and onto A . Prove that f is one-to-one.

Suppose that f is not one-to-one. Then we follow that there exist $x \neq y \in A$ such that $f(x) = f(y)$. Since h is onto, we follow that there exist $x', y' \in \omega$ such that $h(x') = x$ and $h(y') = y$. Since $x \neq y$ we follow that $h(x') \neq h(y')$ and therefore $x' \neq y'$ because h is a function.

Thus we follow that $x'^+ \neq y'^+$. Because h is one-to-one we follow that

$$h(x'^+) \neq h(y'^+)$$

thus

$$f(h(x')) \neq f(h(y'))$$

$$f(x) \neq f(y)$$

which is a contradiction. Thus we follow that f is one-to-one.

4.2.3

Let A be a set and let $a \in A$. Suppose that $f : A \rightarrow A$ satisfies

$$a \in f(a)$$

$$(\forall x, y \in A)(x \in y \rightarrow f(x) \in f(y))$$

Let $h : \omega \rightarrow A$ be states as in theorem 4.2.1. Prove that $h(n) \in h(n^+)$ for all $n \in \omega$.

We follow that $h(0) = a$ and $h(n^+) = f(h(n))$. For base case we've got that $h(0) = a \in f(a) = h(0^+) = h(1)$. Let I be defined as a subset of ω such that $m \in I$ implies that $h(m) \in h(m^+)$. Base case gives us that $0 \in I$. Suppose that $n \in I$. Then we follow that

$$h(n) \in h(n^+)$$

Since $h(n), h(n^+) \in A$, we follow that

$$f(h(n)) \in f(h(n^+))$$

by definition of h we follow that

$$h(n^+) \in h((n^+)^+)$$

thus $n^+ \in I$. Thus we follow that I is an inductive set. Since $I \subseteq \omega$, we follow that $I = \omega$, as desired.

4.2.4

Let $F : A \rightarrow A$ be a function and let $y \in A$.

(a) Prove that the class $S = \{B : B \subseteq A, y \in B, F[B] \subseteq B\}$

From this definition we follow that $B \in S \Rightarrow B \subseteq A$. Thus $B \in S \Rightarrow B \in \mathcal{P}(A)$. Thus $S \subseteq \mathcal{P}(A)$. Since A is a set we follow that its power set is a set, therefore the subset of a power set is also a set.

(b) Show that S is nonempty

We follow that $A \subseteq A$ by basic properties, $y \in B$ by the given restraints, and $F[B] \subseteq A$ since $F : A \rightarrow A$, and therefore $\text{ran}(F) \subseteq A$. Thus we follow that $A \in S$, therefore S is nonempty.

(c) Let $C = \bigcap S$. Prove that $y \in C$ and $F[C] \subseteq C$.

We follow that

$$(\forall B \in S)(y \in B)$$

from definition of S . Suppose that $y \in F[C]$. Then we follow that because $R[\bigcap G] \subseteq \bigcap \{R[C] : C \in G\}$ for any relation, we follow that

$$y \in \bigcap \{F[B] : B \in S\}$$

$$(\forall B \in S)(y \in F[B])$$

Since for every B we've got that $F[B] \subseteq B$, therefore we can follow that

$$(\forall B \in S)(y \in B)$$

thus $y \in \bigcap S$. Thus $y \in F[C] \Rightarrow y \in C$. Thus $F[C] \subseteq C$, as desired.

(d) Prove that for all $B \subseteq A$, if $y \in B$ and $F[B] \subseteq B$, then $C \subseteq B$

If $y \in B$ and $F[B] \subseteq B$, then we follow that $B \in S$. Since $C = \bigcap S$, we follow that $(\forall x \in C)(x \in C \rightarrow x \in B)$. Thus $C \subseteq B$, as desired.

(e) Prove that $y \in F[C]$ if and only if $F[C] = C$

If $F[C] = C$, then we follow that since $y \in C$, then $y \in F[C]$.

For C we've got that $F[C] \subseteq C$. Thus $F[F[C]] \subseteq C$. Thus if $y \in F[C]$, then $F[C]$ satisfies requirements presented in the previous point, and thus $C \subseteq F[C]$. By double inclusion we follow that $F[C] = C$, as desired.

4.3 Arithmetic on ω **Note**

Although not explicitly, but we've started to use the associative and commutative properties of addition pretty liberally at this point. To be more precise, we explicitly define the notation of several pluses in a row to be left-associative (e.g.

$$a_1 + a_2 + a_3 = (a_1 + a_2) + a_3 = A(A(a_1, a_2), a_3)$$

is one such example). Associative and distributive properties guarantee us that the order in which the functions are applied does not matter, and thus the notation is justified.

The order of operations of addition and multiplication is followed from the properties, that are proven in the chapter, and we follow that

$$a \cdot b + c = (a \cdot b) + c = A(M(a, b), c)$$

thus the usual rules of order of operations applies.

In general, all of the operations are defined in terms of functions, and the usual notation of addition and multiplication is nothing but a syntactic sugar. If in doubt, one can prove that the usual notation makes sense pretty easily.

4.3.1

Let $m \in \omega$. Suppose that $m + n = 0$. Prove that $m = n = 0$.

Suppose that $n \neq 0$. Then we follow that there exists j such that $j^+ = n$. Thus

$$m + n = m + j^+ = (m + j)^+ \neq 0$$

thus we get the contradiction.

4.3.2

Let $m \in \omega$ and $n \in \omega$. Show that if $m \cdot n = 0$, then $m = 0$ or $n = 0$.

Suppose that $m \neq 0$ and $n \neq 0$. Then we follow that there exist $n_p \in \omega$ such that $n = n_p^+$. Thus

$$m \cdot n = m \cdot n_p^+ = m \cdot n_p + m$$

Since $m \neq 0 \in \omega$ and $m \cdot n_p^+ \in \omega$, we follow from previous exercise that $m \cdot n_p = 0$ and $m = 0$, which contradicts the assumptions that $m \neq 0$.

4.3.3

Let $m \in \omega$ and $n \in \omega$. Prove that for all $p \in \omega$, if $m + p = n + p$, then $m = n$.

Let

$$I = \{a \in \omega : (\forall m, n \in \omega)(m + a = n + a \Rightarrow m = n)\}$$

If $p = 0$, then $m + 0 = m$, $n + 0 = n$, thus $m + 0 = n + 0$ implies that $m = n$. Thus $0 \in I$.

(IH) Suppose that p is such that $m + p = n + p$. Suppose that $m + p^+ = n + p^+$. Then

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

thus we follow that $p \in I$ implies that $p^+ \in I$. Thus I is inductive, and therefore $I = \omega$.

4.3.4

Prove that for all $n \in \omega$, the inequality $0 \cdot n = 0$ holds.

Suppose that I is the set such that $I = \{n \in \omega : 0 \cdot n = 0\}$. Since $0 \cdot 0 = 0$, we follow that $0 \in I$. Suppose that $0 \cdot n = 0$. Then we follow that

$$0 \cdot n^+ = 0 \cdot n + 0 = 0 + 0 = 0$$

Thus $n \in I \rightarrow n^+ \in I$. Thus $I = \omega$, as desired.

4.3.5

Prove that for all $m \in \omega$ and $n \in \omega$, we have that $m^+ \cdot n = m \cdot n + n$

Suppose that

$$I = \{n \in \omega : (\forall m \in \omega)(m^+ \cdot n = (m \cdot n) + n)\}$$

We follow from $M1$ that $m^+ \cdot 0 = 0$ and $(m \cdot 0) + 0 = m \cdot 0 = 0$ from $A1$ and $M1$. Thus $0 \in I$

Suppose that $n \in I$. Then we follow that

$$\begin{aligned} m^+ \cdot n^+ &= m^+ \cdot n + m^+ = m \cdot n + n + m^+ = m \cdot n + n + m + 1 = \\ &= m \cdot n + m + n + 1 = m \cdot n + m + n^+ = m \cdot n^+ + n^+ \end{aligned}$$

where theorems used are

$$M2 \Rightarrow IH \Rightarrow 4.3.4 \Rightarrow 4.3.4 \Rightarrow 4.3.10 \Rightarrow 4.3.4 \Rightarrow M2$$

4.3.6

Let $n \in \omega$. Prove theorem 4.3.13

Let

$$I = \{n \in \omega : n \cdot m = m \cdot n\}$$

We follow that $0 \cdot n = n \cdot 0 = 0$ from the previous exercises/theorems in the chapter. Thus $0 \in I$.

Suppose that $n \cdot m = m \cdot n$. Then for n^+ we've got that

$$n^+ \cdot m = n \cdot m + m = m \cdot n + m = m \cdot n^+$$

where we've used previous exercise, IH , and $M2$ respectively. Thus we follow that $n \in I \Rightarrow n^+ \in I$, thus $I = \omega$, as desired.

4.3.7

Prove that if $n \in \omega$, then n is either even or odd (details of definition of evenness in the exercise)

Let

$$I : \{n \in \omega : (\exists k \in \omega : n = 2 \cdot k + 1 \vee n = 2 \cdot k)\}$$

Since $0 = 2 \cdot 0$, we follow that $0 \in I$.

Suppose that $n \in I$. Then we follow that n is even or odd (or both, we don't know yet).

If n is even, then we follow that $n = 2 \cdot k$. Thus $n^+ = n + 1 = 2 \cdot k + 1$. Thus n^+ is odd, therefore $n^+ \in I$.

If n is odd, then we follow that $n = 2 \cdot k + 1$. Thus $n^+ = n + 1 = 2 \cdot k + 1 + 1 = 2 \cdot k + 2 = 2 \cdot k^+$. Thus we follow that $n^+ \in I$.

Thus we follow that $n \in I \Rightarrow n^+ \in I$, thus $I = \omega$, as desired.

4.3.8

Let $I = \{n \in \omega : \neg((\exists k, j \in \omega)(n = 2 \cdot k \wedge n = 2 \cdot j + 1))\}$ Prove that I is inductive. Conclude that no natural number is both odd and even.

Let $I = \{n \in \omega : \neg((\exists k, j \in \omega)(n = 2 \cdot k \wedge n = 2 \cdot j + 1))\}$

We've shown earlier that 0 is even. Suppose that 0 is odd. Then we follow that

$$0 = 2 \cdot k + 1 = (2 \cdot k)^+$$

which is a contradiction.

Suppose that $n \in I$. Then we follow that

$$\neg((\exists k, j \in \omega)(n = 2 \cdot k \wedge n = 2 \cdot j + 1))$$

thus

$$\begin{aligned} \neg((\exists k, j \in \omega)(n^+ = (2 \cdot k)^+ \wedge n^+ = (2 \cdot j + 1)^+)) &\Leftrightarrow \\ \Leftrightarrow \neg((\exists k, j \in \omega)(n^+ = 2 \cdot k + 1 \wedge n^+ = 2 \cdot j + 2)) &\Leftrightarrow \\ \Leftrightarrow \neg((\exists k, j \in \omega)(n^+ = 2 \cdot k + 1 \wedge n^+ = 2 \cdot j^+)) &\Leftrightarrow \\ \Leftrightarrow \neg((\exists k, l \in \omega)(n^+ = 2 \cdot k + 1 \wedge n^+ = 2 \cdot l)) \end{aligned}$$

(i've changed a variable under the quantifier for avoid confusion, which does not change the meaning) thus $n \in I \Rightarrow n^+ \in I$. Thus I is inductive, and $I = \omega$. Therefore every natural number is either odd or even, but not both.

4.3.9

Prove for all $m, n, k \in \omega$ that $m^{n+k} = m^n \cdot m^k$,

Let

$$I = \{k \in \omega : (\forall m, n \in \omega)(m^{n+k} = m^n \cdot m^k)\}$$

We follow that if $k = 0$ then

$$E(m, n + k) = E(m, n + 0) = E(m, n) = E(m, n) \cdot 1 = E(m, n) \cdot E(m, k)$$

thus we follow that $0 \in I$.

Suppose that $k \in I$. We follow that for k^+ we've got

$$E(m, n + k^+) = E(m, n + k) \cdot m = E(m, n) \cdot E(m, k) \cdot m = E(m, n) \cdot E(m, k^+)$$

thus we follow that $k \in I \Rightarrow k^+ \in I$. Thus we follow that $I = \omega$, as desired.

4.4 Order on ω **Note**

I'm using the symbol \leq instead of "in or equal" because it's more convinient. Theorems in the chapter provide us with the equivalence of two, and therefore the justification for this notation.

4.4.1

Let $n \in \omega$. Show that $1 \leq n^+$

We know that for every $n \in \omega$, $0 \leq n$. Thus $0 \leq n \Rightarrow 0^+ \leq n^+ \Leftrightarrow 1 \leq n^+$, as desired.

4.4.2

Let $m, n \in \omega$. Show that if $m \in n^+$, then $m \leq n$.

Suppose that $m \in n^+$. We follow that

$$m \in n^+ \Leftrightarrow m \in n \cup \{n\} \Leftrightarrow m \in n \vee m = n \Leftrightarrow m \leq n$$

4.4.3

Let $n, a \in \omega$. Show that if $n \in a$, then $n^+ \leq a$

Suppose that $n \in a$. We know that one of $n^+ = a$, $n^+ \in a$ or $a \in n^+$ holds. Suppose that $a \in n^+$. We follow that

$$a \in n \cup \{n\} \Leftrightarrow a \in n \vee a = n$$

If $a \in n$, then we've got that $n \in a$ and $a \in n$, which is impossible. If $a = n$, then $n \in n$, which is also not good. Thus we follow that $a \in n^+$ is impossible. Thus we follow that $n^+ \in a$ or $n^+ = a$. In other words, $n \leq a$, as desired.

4.4.4

Let I be inductive and let $a \in \omega$. Prove that $\{n \in I : n \in a \vee a \subseteq n\}$ is inductive

Let

$$Q = \{n \in I : n \in a \vee a \subseteq n\}$$

We follow that $0 \in Q$ since 0 is in every inductive set (by virtue of being a natural number), and by trichotomy property $0 \in a$ or $a \leq 0 \Leftrightarrow a \subseteq 0$.

Suppose that $q \in Q$. Since $Q \subseteq I$, we follow that $q \in I$, and because I is inductive, we follow that $q^+ \in I$ as well. We also follow that $q \in a \vee a \subseteq q$.

If $a \subseteq q$, then we follow that $a \subseteq q \cup \{q\}$, therefore $a \subseteq q^+$, and thus $q \in Q$.

Suppose that $q \in a$. Then we follow that since $a \in \omega \rightarrow a \subseteq \omega$, we follow that $q \in \omega$. Therefore $q^+ \in \omega$, and we've got by trichotomy that either $q^+ \in a$, $q^+ = a$ or $a \in q^+ \Leftrightarrow a \subset q^+$. Thus we follow that $q^+ \in a \vee a \subseteq q^+$, therefore $q^+ \in Q$.

Thus we can conclude that $0 = \emptyset \in Q$ and $q \in Q \Rightarrow q^+ \in Q$. Thus Q is inductive, as desired.

4.4.5

Let $m, n \in \omega$. Suppose that $m \leq n$. Prove that $\max(m, n) = n$.

From the chapter we follow that $\max(m, n) = m \cup n$. Since $m \leq n$, we follow that $m \subseteq n$. Thus $\max(m, n) = m \cup n = n$, as desired.

4.4.6

Let $m, n \in \omega$. Prove that for all $p \in \omega$ if $m \in n$, then $m + p \in n + p$

Let

$$I = \{p \in \omega : (\forall m, n \in \omega)(m \in n \Rightarrow m + p \in n + p)\}$$

Since $m + 0 = m$ and $n = n + 0$, we follow that $m \in n \Leftrightarrow m + 0 \in n + 0$.

Suppose that $p \in I$. Then we follow that

$$m \in n \Leftrightarrow m + p \in n + p \Leftrightarrow (m + p)^+ \in (n + p)^+ \Leftrightarrow m + p^+ \in n + p^+$$

thus $p^+ \in I$. Thus $I = \omega$, as desired.

4.4.7

Let $m, n \in \omega$. Prove that for all $p \in \omega$, if $m + p \in n + p$, then $m \in n$

In previous exercise we've got only biconditionals, thus we get the reverse case as well

4.4.8, 4.4.9

let $m, n \in \omega$. Prove that for all $p \in \omega$ $m \in n \Leftrightarrow m \cdot p^+ \in n \cdot p^+$

Let

$$I = \{p \in \omega : (\forall m, n \in \omega)(m \in n \Leftrightarrow m \cdot p^+ \in n \cdot p^+)\}$$

We first follow that if $p = 0$, then

$$m \cdot 0^+ \in n \cdot 0^+ \Leftrightarrow (m \cdot 0 + m) \in (n \cdot 0 + n) \Leftrightarrow (0 + m) \in (0 + n) \Leftrightarrow m \in n$$

thus $0 \in I$.

Suppose that $p \in I$. Then we follow that

$$m \in n \Leftrightarrow m \cdot p^+ \in n \cdot p^+$$

$m \in n$ if and only if $m + a \in n + a$ by previous exercise. Thus

$$m \in n \Leftrightarrow m + m \cdot p^+ \in n + m \cdot p^+$$

and also

$$m \cdot p^+ \in n \cdot p^+ \Leftrightarrow m \cdot p^+ + n \in n \cdot p^+ + n$$

by commutativity we follow that

$$m \cdot p^+ \in n \cdot p^+ \Leftrightarrow n + m \cdot p^+ \in n \cdot p^+ + n$$

thus

$$\begin{aligned} m \in n &\Leftrightarrow (m + m \cdot p^+ \in n + m \cdot p^+) \wedge (n + m \cdot p^+ \in n \cdot p^+ + n) \Leftrightarrow \\ &\Leftrightarrow (m + m \cdot p^+ \in n + m \cdot p^+) \wedge (n + m \cdot p^+ \in n \cdot p^+ + n) \Rightarrow \\ &m + m \cdot p^+ \in n \cdot p^+ + n \Leftrightarrow m \cdot (p^+)^+ \in n \cdot (p^+)^+ \end{aligned}$$

thus $m \in n \Rightarrow m \cdot (p^+)^+ \in n \cdot (p^+)^+$.

Let $m, n \in \omega$ be such that $m \cdot (p^+)^+ \in n \cdot (p^+)^+$. By trichotomy we follow that $m \in n$, $n \in m$ or $m = n$.

If $m = n$, then we follow that

$$n \cdot (p^+)^+ = m \cdot (p^+)^+ \in n \cdot (p^+)^+$$

which is a contradiction.

If $n \in m$, then we follow by implication that

$$n \cdot (p^+)^+ \in m \cdot (p^+)^+$$

and since $m \cdot (p^+)^+ \in n \cdot (p^+)^+$, we follow that $n \cdot (p^+)^+ \in n \cdot (p^+)^+$, which is also bad. Thus we follow that $m \cdot (p^+)^+ \in n \cdot (p^+)^+ \Rightarrow m \in n$. By including the implication we follow that

$$m \cdot (p^+)^+ \in n \cdot (p^+)^+ \Leftrightarrow m \in n$$

and therefore $p^+ \in I$. Thus $I = \omega$, as desired.

4.4.10

Use Theorem 4.4.11 and Theorem 4.4.9 to prove Corollary 4.4.12

Suppose that $m + p = n + p$. If $m \in n$, then we follow that $m + p \in n + p$, which is not the case. If $n \in m$, then we follow that $n + p \in m + p$, which is also not the case. Thus we follow that $m = p$. Thus $m + p = n + p \Leftrightarrow m = n$ (reverse case is trivial)

Suppose that $p \neq 0$ and we've got that $m \cdot p = n \cdot p$. Since $p \neq 0$, we follow that $p = j^+$ for some $j \in \omega$.

We follow that $m \in n$ and $n \in m$ are both impossible, because they would imply that $m \cdot p \in n \cdot p$ and $n \cdot p \in m \cdot p$, which are not the case. Thus we follow that

$$(\forall p \in (\omega \setminus 0))(m \cdot p = n \cdot p \Leftrightarrow m = n)$$

where reverse case is once again trivial.

4.4.11

Let $m \in \omega$. Prove that $m \in m + p^+$ for all $p \in \omega$.

We know that $m \in m^+$ for all $m \in \omega$. Thus we follow that for any $p \in \omega$ we've got that $m + p \in m^+ + p \Leftrightarrow m + p \in m + p^+$. We also can follow that for every $p \in \omega$ we've got that $m \leq m + p$ (can't find the exact reference, but it is easily followed by induction). Thus by transitive property we can follow that $m \in m + p^+$, as desired.

4.4.12

Let $m \in \omega$. Prove that for all $n \in \omega$, if $m \in n$ then $m + p^+ = n$ for some $p \in \omega$.

Let

$$I = \{j \in \omega : j \in m \vee (\exists p \in \omega)(j = m + p^+)\}$$

We follow that $0 \in m$, therefore $0 \in I$.

Suppose that $n \in I$. Then we follow that $n \in m \vee (\exists p \in \omega)(j = m + p^+)$. If $n \in m$, then we follow that $n^+ \in m \vee n^+ = m \Leftrightarrow n^+ \in m \vee n^+ = m + 0$. Thus we follow that if $n \in m$, then $n^+ \in I$.

If $(\exists p \in \omega)(n = m + p^+)$, then we follow that $n^+ = (m + p^+)^+ = m + (p^+)^+$. Since $p^+ \in \omega$, we follow $n^+ \in I$ as well.

Thus we can conclude that $n \in I \Rightarrow n^+ \in I$. Thus I is inductive, and since it is a subset of ω , we follow that $I = \omega$. Thus we follow that our initial $n \in I$. Thus $n \in m \vee (\exists p \in \omega)(n = m + p^+)$. Because $m \in n$, we follow by trichotomy that $n \notin m$, thus $(\exists p \in \omega)(n = m + p^+)$, as desired.

4.4.13

Combination of previous two exercises into one biconditional.

4.4.18

Prove for all $n \in \omega$, if $f : n \rightarrow \omega$, then $\text{ran}(f) \subseteq k$ for some $k \in \omega$.

Let

$$I = \{n \in \omega : (\forall f)(\exists k \in \omega)(f : n \rightarrow \omega \Rightarrow \text{ran}(f) \subseteq k)\}$$

We follow that if $f : 0 \rightarrow \omega$, then $\text{dom}(f) = \emptyset$, thus $f = \emptyset$, therefore $\text{ran}(f) = \emptyset = 0 \subseteq 0$. Thus $0 \in I$.

Suppose that $n \in I$. Let $f : n^+ \rightarrow \omega$. Then we follow that there exists $f|n : n \rightarrow \omega$, and thus $(\exists k \in \omega)(\text{ran}(f|n) \subseteq k)$. Since $n^+ = n \cup \{n\}$, we follow that

$$\text{ran}(f) = f[n^+] = f[n] \cup f[\{n\}] = f[n] \cup f(n) \subseteq k \cup f(n)$$

Since $f : n^+ \rightarrow \omega$, we follow that $f(n) \in \omega$. Thus $k \cup f(n) \in \omega$, thus there exists $j = k \cup f(n) \in \omega$ such that $f : n^+ \rightarrow \omega \Rightarrow \text{ran}(f) \subseteq j$. Thus we follow that $n^+ \in I$. Thus $n \in I \Rightarrow n^+ \in I$, therefore $I = \omega$, as desired.

Chapter 5

On the Size of Sets

Because of chapter 4'th construction of natural numbers and their ordering I think that we're justified to use basic number theory and some properties of the natural numbers, since it follows directly from the proven facts. One can argue even that we're justified to use \mathbb{Z} in general, but until the need arises I will refrain from doing so.

5.1 Finite Sets

5.1.1

In our proof of Theorem 5.1.3, under the case that $k \in m$, we did not show that the function g is one-to-one. Complete the proof by proving that g is one-to-one.

We need to prove that

$$g(a) = \begin{cases} k & \text{if } f(a) = m \\ f(a) & \text{if } f(a) \neq m \end{cases}$$

is one-to-one.

Suppose that $a_1, a_2 \in A$ are such that $a_1 \neq a_2$. Suppose that $f(a_1) \neq m$. Then we follow that if $f(a_2) \neq m$, then we've got that $f(a_1) \neq f(a_2)$ by the fact that f is injective, thus $g(a_1) = f(a_1) \neq f(a_2) = g(a_2)$ as well. If $f(a_2) = m$, then we follow that $g(a_2) = k$. Thus we follow that $f(a_1) = g(a_1) \in \text{ran}(f)$ and $g(a_2) = k \notin \text{ran}(f)$. Thus we follow that $g(a_1) \neq g(a_2)$.

Since f is injective, we can follow that $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$, thus we follow that the case when $f(a_1) = f(a_2) = m$ can't happen. Thus we follow that $a_1 \neq a_2 \Rightarrow g(a_1) \neq g(a_2)$, therefore g is injective, as desired.

5.1.2

Suppose that the set B is finite and $A \subseteq B$. Prove that A is finite.

We follow that there exists $n \in \omega$ $|B| = n$. Thus we follow that there exists $f : B \rightarrow n$, that is injective. Since f is injective and $A \subseteq B$, we follow that $f|_A$ is also one-to-one. Thus we follow that A is finite, as desired.

5.1.3

Let A and B be two finite sets, and let $f : A \rightarrow B$ be one-to-one. Prove that $|A| \leq |B|$.

Given that A and B are finite, we follow that there exist natural numbers $n = |A|$ and $m = |B|$. We can also follow that there exist bijections $h : A \rightarrow n$ and $g : B \rightarrow m$. Because h is a bijection, we follow that $h^{-1} : n \rightarrow A$ is also a bijection. Thus we follow that $g \circ f \circ h^{-1} : n \rightarrow m$ is a composition of injective functions, and therefore it's injective as well. Thus we follow that $|n| \leq m$, therefore

$$|A| \leq |B|$$

$$|A| \leq |B|$$

as desired.

5.1.4

Prove theorem 5.1.7

Let A and B be finite. Let $n = |A|$ and $m = |B|$. We follow that there exist bijections $f : A \rightarrow n$ and $g : B \rightarrow m$.

Thus we follow that if there exists a bijection $h : A \rightarrow B$, then we follow that $g \circ h \circ f^{-1} : n \rightarrow m$ is a bijection. Thus $g \circ h \circ f^{-1} : n \rightarrow m$ is injective and $(g \circ h \circ f^{-1} : n \rightarrow m)^{-1}$ is injective, thus we follow that $n \geq m$ and $m \geq n$, thus by antisymmetry we've got that $n = m$ and $|A| = |B|$.

If $|A| = |B|$, then we follow that $f : A \rightarrow |A|$ and $g : B \rightarrow |B|$ are bijections, and thus $g^{-1} \circ f : A \rightarrow B$ is also a bijection.

5.1.5

Let $n \in \omega$ and let $f : n \rightarrow A$. Prove that $f[n]$ is finite.

Let us firstly prove a theorem (which I'm sure that it was proven in the book before, but I can't find it) assuming for a moment that n is a general set.

If $f : n \rightarrow A$ is a function, then there exists an injective function g such that $g \subseteq f^{-1}$.

Suppose that $y \in f[n]$. Then we follow that there exists a nonempty set

$$A_y = \{x \in n : \langle x, y \rangle \in f\}$$

Thus we can define an indexed function $\langle A_y : y \in f[n] \rangle$, from which by axiom of choice we follow that there exists a function g such that

$$g(y) \in A_y$$

Thus we follow that $g : f[n] \rightarrow n$. From a definition of A_y we can follow that $g \subseteq f^{-1}$. Suppose that $n_1 \neq n_2 \in f[n]$. We follow that because f is a function, there does not exist $x \in n$ such that $f(x) = n_1$ and $f(x) = n_2$. Thus $g(n_1) \neq g(n_2)$. Thus we follow that $n_1 \neq n_2 \Rightarrow g(n_1) \neq g(n_2)$. Therefore g is injective, as desired.

By provided theorem we can follow that there exists an injective function g from $f[n]$ to n . Thus we follow that $f[n]$ is finite by definition.

5.1.6

Let A be finite and let $f : A \rightarrow \omega$. Prove that $\text{ran}(f) \subseteq k$, for some $k \in \omega$.

Since A is finite, we follow that there exists a bijection $g : A \rightarrow n$ for some $n \in \omega$. Thus we follow that $g^{-1} : n \rightarrow A$ is also a bijection. We now follow that $f \circ g^{-1} : n \rightarrow \omega$ is a function with a finite domain, and because g^{-1} is a bijection, we follow that $\text{ran}(f \circ g^{-1}) = \text{ran}(f)$. By exercise 4.4.18 we follow that there exists $k \in \omega$ such that $\text{ran}(f \circ g^{-1}) \subseteq k$. Thus we follow that $\text{ran}(f) \subseteq k$ for some $k \in \omega$, as desired.

5.1.7

Suppose that $f : A \rightarrow n$ is a bijection, where $n \in \omega$. Prove that $|A| = n$.

Since f is a bijection, we follow that it is injective. Thus we follow that A is finite. Let $|A| = m$. We follow that there exists a bijection $g : A \rightarrow m$ and thus $g^{-1} : m \rightarrow A$ is also a bijection. Thus

$$f \circ g^{-1} : m \rightarrow n$$

is also a bijection. Thus we follow that $|n| = |m|$. Therefore $n = m$, and thus $|A| = n$, as desired.

5.1.8

Let $f : \omega \times \omega \rightarrow \omega$ be defined by $f(i, j) = 2^i \cdot 3^j$. Prove that f is one-to-one. Prove that if $i < m$ and $j < n$, then $f(i, j) \leq f(m, n)$.

I think that at this point we're kind of justified to use the normal stuff from the number theory, such as divisibility and whatnot (given the fact that we've justified all of the normal things such as \cdot), and deduce from it that given function is indeed one-to-one. The fact that $i < m$ and $j < n$ follows easily from induction on i and then by induction on j .

5.1.9

Prove that $p : \omega \times \omega \rightarrow \omega$ defined by

$$p(i, j) = 2^i(2j + 1) - 1$$

is one-to-one and onto ω . Prove that if $i \in M$ and $j \in n$, then $p(i, j) < p(m, n)$.

Suppose that $i, j, i', j' \in \omega$ and $i > i', j > j'$. Then we follow that

$$p(i, j) - p(i', j') = 2^i(2j + 1) - 2^{i'}(2j' + 1) = 2^i 2j + 2^i - 2^{i'} 2j' - 2^{i'} =$$

from which we follow that $2^i > 2^{i'}$ because exponentiation function is strictly increasing for bases greater than 1. We can also follow that $j > j'$ implies that $2j > 2j'$, and because we've seen earlier that $2^i > 2^{i'}$, we follow that $2^i 2j > 2^{i'} 2j'$. Thus we follow that

$$i > i' \wedge j > j' \Rightarrow p(i, j) > p(i', j')$$

and

$$i = i' \wedge j > j' \Rightarrow p(i, j) > p(i', j')$$

$$i > i' \wedge j = j' \Rightarrow p(i, j) > p(i', j')$$

thus we follow that

$$\langle i, j \rangle \neq \langle i', j' \rangle \Rightarrow p(i, j) \neq p(i', j')$$

thus the function is injective.

Now suppose that $n \in \omega$. Then we follow that

$$2^i(2j + 1) - 1 = n$$

$$2^i(2j + 1) = n + 1$$

we follow that since $n + 1 > 0 \Rightarrow n \in \mathbb{Z}^+$, there exist a finite set of prime divisors $P = \{p_1, p_2, \dots, p_q\}$ and set of powers $K = \{k_1, \dots, k_l\}$ such that

$$n + 1 = \prod p_l^{k_l}$$

from which we follow that we can set i to be the power of 2 in case that $2 \in P$, or 0 in case that $2 \notin P$ to get

$$n + 1 = 2^i \prod_{P \setminus 2} p_j^{k_j}$$

since $2 \notin P \setminus 2$, we follow that $\prod_{P \setminus 2} p_j^{k_j}$ is an odd number, and thus there exists j such that $2j + 1 = \prod_{P \setminus 2} p_j^{k_j}$. Thus we follow that

$$n + 1 = 2^i(2j + 1)$$

$$n = 2^i(2j + 1) - 1$$

thus we follow that $p(i, j)$ is a surjective function. Thus p is bijective, as desired.

5.1.10

Prove that there exists a one-to-one function $f : \omega \rightarrow \omega \times \omega$ that is onto $\omega \times \omega$

Take a function from previous exercise and take its inverse. We follow that because it is a bijection, then its inverse is a function and a bijection, thus we've got the desired function, as desired.

5.1.11

Suppose that A and B are finite disjoint sets. Prove that $A \cup B$ is finite.

We follow that since both of them are finite, we've got that there exist bijections $f : |A| \rightarrow A$ and $g : |B| \rightarrow B$. Thus we follow that we can relation $h : |A| + |B| \rightarrow A \cup B$ by

$$h(x) = \begin{cases} x < |A| \Rightarrow f(x) \\ x \geq |A| \Rightarrow g(x - |A|) \end{cases}$$

(I've used a bit of a notation abuse here, but the principle is pretty clear) We follow that if $x \in |A| + |B|$, then $x < |A| \oplus x \geq |A|$. Thus we follow that $h(x)$ is a well-defined function. Now suppose that $x, y \in |A| + |B| \wedge x \neq y$. If $x, y < |A|$ or $x, y \geq |A|$, then we follow that

$$\langle h(x), h(y) \rangle = \langle f(x), f(y) \rangle \oplus \langle h(x), h(y) \rangle = \langle g(x), g(y) \rangle$$

from which we follow that $h(x) \neq h(y)$. If $x < |A|$ and $y \geq |A|$ (or vice-versa), then we follow that $x \in A$ and $y \in B$, and since A and B are disjoint, we follow that $x \neq y$. Thus we can conclude that $x \neq y \Rightarrow h(x) \neq h(y)$, and therefore the function is injective.

Now suppose that $x \in A \cup B$. If $x \in A$, we follow that there exists $n \in |A| \Rightarrow n \in |A| + |B|$ such that $h(n) = f(n) = x$. If $x \in B$, we follow that there exists $n \in |B|$ such that $g(n) = x$. $n \in |B|$ implies that $n + |A| \in |A| + |B|$, and thus there exists $k = n + |A| \in |A| + |B|$ such that

$$h(k) = g(n + |A| - |A|) = g(n) = x$$

thus we follow that $x \in A \cup B \Rightarrow (\exists k \in |A| + |B|)(h(k) = x)$. Thus we follow that h is surjective.

Thus we follow that $h : |A| + |B| \rightarrow A \cup B$ is bijective, and since $|A| + |B| \in \omega$, we follow that $A \cup B$ is finite, as desired.

By setting $A = A'$ and $B = B' \setminus A$, we can conclude that union of two arbitrary finite sets A', B' is finite as well.

5.1.12

Let A be an infinite set and B be a finite set. Prove that $A \setminus B$ is infinite.

Suppose that $A \setminus B$ is finite. Then we follow that $A \setminus B$ and B are disjoint sets, thus $(A \setminus B) \cup B$ is finite by previous exercise. Since

$$(A \setminus B) \cup B = A \cup B$$

we follow that $A \cup B$ is finite. Thus $A \subseteq A \cup B$ is finite as well, which is a contradiction.

5.1.13

Let $k \in \omega$. Suppose that $|A| = k^+$ and $a \in A$. Prove that $|A \setminus \{a\}| = k$.

One of the implications of exercise 5.1.12 is that if A and B are finite and disjoint, then $|A \cup B| = |A| + |B|$. Applying this thing to our exercise we follow that

$$|A| = |A \setminus \{a\} \cup \{a\}| = k^+$$

Without providing trivial proof we gonna state here that

$$|\{a\}| = 1$$

thus we conclude that

$$|A \setminus \{a\}| + |\{a\}| = k^+$$

$$|A \setminus \{a\}| + 1 = k + 1$$

$$|A \setminus \{a\}| = k$$

as desired.

5.1.14

Suppose taht $|K| = k$, $|N| = n$, and $f : K \rightarrow N$ is onto N where $k, n \in \omega$. Show that there is a function $g : k \rightarrow n$ that is onto

We follow that there exist bijections $h : k \rightarrow K$ and $j' : n \rightarrow N$. Since j' is a bijection we're justified to define bijection $j : N \rightarrow n; j = j'^{-1}$. Thus we can define $g : k \rightarrow n$ by

$$g = j \circ f \circ h$$

since all of the j, f, h are surjective, we follow that g is surjective as well, as desired.

5.1.15

Suppose that A and B are finite. Prove that $A \cup B$ is finite.

GOTO last paragraph of 5.1.12

5.1.16

Let $n \in \omega$. Suppose that $f : n \rightarrow A$ is onto A . Prove that A is finite.

We follow that since f is surjective, there exists injective $g : A \rightarrow n$ such that $g \subseteq f^{-1}$. Thus we follow that A is finite, as desired.

5.1.17

Let A be finite set. Prove that there exists an $f : n \rightarrow A$ that is onto A for some $n \in \omega$.

We know that there exists a bijection $f : |A| \rightarrow A$, thus concluding the exercise.

5.1.18

Suppose that $f : A \rightarrow B$ is onto B where A is finite. Prove that B is finite.

Since A is finite, we follow that there exists a bijection $g : |A| \rightarrow A$. Thus there exists a surjective function $f \circ g : |A| \rightarrow B$, which by 5.1.16 means that B is finite, as desired.

5.1.19

Let $n \in \omega$ and $\{A_i : i \in n\}$ be such that A_i is finite for all $i \in n$. Prove, by induction, that $\bigcup_{i \in n} A_i$ is finite.

Let

$$I = \{n \in \omega : \bigcup_{i \in n} A_i \text{ is finite}\}$$

(we can make a more formal definition here, but it'll be a bit cumbersome).

We follow that if $n = 0$, then $\{A_i : i \in n\} = \emptyset$, thus we follow that

$$\bigcup_{i \in n} A_i : i \in n = \emptyset$$

thus

$$|\bigcup_{i \in n} A_i : i \in n| = 0$$

thus we follow that $0 \in I$.

Suppose now that $n \in I$. Then we follow that $\bigcup_{i \in n} A_i$ and A_{n+} are finite, thus $\bigcup_{i \in n+} A_i$ is finite as well. Thus we've got the desired conclusion.

5.1.20

Suppose that A and B are finite sets. Prove that $A \times B$ is finite.

We follow that $\mathcal{P}(A)$ is finite, $\mathcal{P}(B)$ is also finite, thus $\mathcal{P}(A) \cup \mathcal{P}(B)$ is finite, therefore $\mathcal{P}(\mathcal{P}(A) \cup \mathcal{P}(B))$ is finite, and since $A \times B \subseteq \mathcal{P}(\mathcal{P}(A) \cup \mathcal{P}(B))$, we follow that $A \times B$ is finite as well.

5.1.21

Prove Corollary 5.1.11

Suppose that $G : \omega \rightarrow A$ is one-to-one. Suppose that A is finite. Then we follow that there exists a bijection $f : A \rightarrow |A|$. Therefore we follow that $f \circ G : \omega \rightarrow |A|$ is injective,

and thus ω is a finite, which is a contradiction. Thus we follow that A is not finite (i.e. infinite), as desired.

5.1.22

Let $\langle A_i : i \in I \rangle$ be an indexed function where I is a finite set and $A_i \neq \emptyset$. Without using AoC prove by induction on $|I|$ that there is an indexed function $\langle x_i : i \in I \rangle$ such that $x_i \in A_i$ for all $i \in I$.

Define W to be the set, for which the conditions hold.

We follow that if $|I| = 0$, then $I = \emptyset$, thus $\langle A_i : i \in I \rangle = \emptyset$, and therefore \emptyset is an indexed function $\langle x_i : i \in I \rangle$ as well, thus $i \in W$.

Suppose that $n \in W$. We follow that we can have I' such that $|I'| = n + 1$ and indexed function $\langle A_i : i \in I' \rangle$. Since I' is finite, we follow that there exists a bijection $f : n + 1 \rightarrow I'$, therefore there exists an element $f(0) \in I'$. Define $a = f(0)$. We can follow that $|I' \setminus \{a\}| = n$. We follow that for

$$\langle A_i : i \in I' \setminus \{a\} \rangle$$

there exists

$$\langle x_i : i \in I' \setminus \{a\} \rangle$$

Let us now look at $A_{\{a\}}$. We follow that since $A_{\{a\}} \neq \emptyset$ we can follow that there exists $b \in A_{\{a\}}$. Define a function $h : I' \rightarrow \bigcup_{i \in I'} A_i$ by

$$h(x) = \begin{cases} x = a \Rightarrow b \\ x \neq a \Rightarrow \langle x_i : i \in I' \setminus \{a\} \rangle \end{cases}$$

then we follow that h is the desired indexed function, and thus $n^+ \in W$. Therefore $W = \omega$, as desired.

5.1.23

Modify the proof of Theorem 5.1.14 to show that if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$.

Not gonna provide it, but we can follow that by making definition of I a bit more strict and following the same logic for the argument.

5.2 Countable Sets

5.2.1

Let $A = \{4, 8, 12, 16, \dots\}$ and let $B = \{n \in \mathbb{Z} : n < -25\}$. Define a bijection $f : A \rightarrow \omega$ and define a bijection $g : B \rightarrow \omega$.

$$\begin{aligned} f(x) &= x/4 - 1 \\ g(x) &= -n + 26 \end{aligned}$$

5.2.2

Let A and B be as in Exercise 1. Define an injection $h : A \cup B \rightarrow \omega$.

Because A and B are disjoint we can set

$$h(x) = \begin{cases} x = 2x \Rightarrow f^{-1}(x/2) \\ x = 2x + 1 \Rightarrow g^{-1}((x - 1)/2) \end{cases}$$

5.2.3

Show that the set of negative integers Z^- is countable

We can define $f : Z^- \rightarrow \omega$ by $f(x) = -x - 1$, which will be a bijection between Z^- and ω . Thus we conclude that Z^- is countable.

5.2.4

Conclude from Exercise 3 that set of integers Z is countable.

We can follow that sets Z^-, N are both countable, thus $Z^- \cup N = Z$ is countable as well.

5.2.5

Let $p : \omega \times \omega \rightarrow \omega$ be one-to-one. Using p , show that the set of positive rationals is countable. Conclude that the set of negative rationals is countable and the set of rationals is countable.

We can define an injection from Q^+ to $\omega \rightarrow \omega$ by

$$h(m/n) = \langle m, n \rangle$$

where m/n is in the lowest possible terms. From exercise 5.1.9 we follow that there exists an injection p from $\omega \times \omega$ to ω . Thus we conclude that $p \circ h$ is an injection from Q^+ to ω , thus Q^+ is countable.

Because we can define a bijection from Q^+ to Q^- by $f(x) = -x$ we follow that Q^+ is countable as well. Thus we follow that $Q^+ \cup Q^- \cup \{0\} = Q$ is a countable union of countable sets, and therefore is countable as well, as desired.

5.2.6

Let A and B be two countably infinite sets. Prove that there exists a bijection $f : A \rightarrow B$.

Since A and B are both countably infinite we follow that there exist bijections $h : A \rightarrow \omega$ and $g : B \rightarrow \omega$. Thus if we set $f = g^{-1} \circ h$ we get the desired bijection.

5.2.7

Let A and B be countable sets. Prove that $A \times B$ is countable.

We follow that there exist injections $f : A \rightarrow \omega$ and $g : B \rightarrow \omega$. Thus we can define an injection $p' : A \times B \rightarrow \omega \rightarrow \omega$ by

$$p'(x, y) = \langle f(x), g(y) \rangle$$

which we can plug into bijective $p : \omega \times \omega \rightarrow \omega$ to get injective $p \circ p' : A \times B \rightarrow \omega$, which proves that $A \times B$ is countable.

5.2.8

Let A be a set. Suppose that $f : \omega \rightarrow A$ is onto A . Prove that A is countable

We follow that there exists an injective function $g \subseteq f^{-1} : A \rightarrow \omega$, which proves that A is countable, as desired.

5.2.9

Let A be a nonempty countable set. Prove that there exists an $f : \omega \rightarrow A$ that is onto A .

Because A is nonempty, we follow that there exists $a \in A$. We follow that there exists an injection $f : A \rightarrow \omega$, therefore we can define a surjective function $h : \omega \rightarrow A$

$$h(x) = \begin{cases} x \in \text{ran}(f) \Rightarrow f^{-1}[\{x\}] \\ x \notin \text{ran}(f) \Rightarrow a \end{cases}$$

as desired.

5.2.10

Suppose that $f : A \rightarrow B$ is onto B where A is countable. Prove that B is also countable.

If $A = \emptyset$, then we follow that B is also an empty set, therefore B is countable.

If A is not empty, then we follow by previous exercise that there exists a surjective $g : \omega \rightarrow A$. Thus we follow that

$$f \circ g : \omega \rightarrow B$$

is surjective, therefore by exercise 5.2.8 we follow that B is countable, as desired.

5.2.11

Let A be an infinite set and let $C = \mathcal{P}(A) \setminus \{\emptyset\}$. By AoC there exists a function $g : C \rightarrow A$ such that $g(B) \in B$ for all $B \in C$. One can show that there is a function $h : \omega \rightarrow A$ such that

$$(\forall n \in \omega)(h(n) = g(A \setminus h[n]))$$

Prove that $h : \omega \rightarrow A$ is one-to-one

Suppose that $x < y \in \omega$ and $h(x) = h(y)$. We follow that $x \in y$, therefore

$$h(x) = h(y) = g(A \setminus h[y]) \in A \setminus h[y]$$

Since $x \in y$ we follow that $h(x) \in h[y]$, therefore we have a contradiction.

5.3 Uncountable Sets**5.3.1**

Let A be uncountable. Prove that $A \times B$ is uncountable for any nonempty set B .

Let $b \in B$. Define a function $f : A \rightarrow A \times B$ by

$$f(a) = \langle a, b \rangle$$

We follow that for $x, y \in A$

$$f(x) = f(y) \Rightarrow \langle x, b \rangle = \langle y, b \rangle \Rightarrow x = y$$

thus we follow that f is injective. Therefore we conclude that $A \times B$ is uncountable, as desired.

5.3.2

Let A be uncountable and B be countable. Prove that $A \setminus B$ is uncountable.

Suppose that $A \setminus B$ is countable. Then we follow that $A = A \setminus B \cup B$ is a countable union of countable sets, therefore it is countable as well, which is a contradiction.

5.3.3

Prove that the set of irrationals $R \setminus Q$ is uncountable.

R is uncountable, Q is countable, thus by previous exercise we follow this conclusion.

5.3.4

Suppose that A is uncountable and $A \subseteq B$. Prove that B is uncountable.

We follow that since $A \subseteq B$ we've got an injection $f : A \rightarrow B$ which is a restricted identity on A . Thus we follow that B is uncountable, as desired.

5.3.5

Prove that ω^ω is uncountable

We follow that $\{0, 1\}^\omega$ is a subset of ω^ω and because the former is uncountable, we follow by previous exercise that ω^ω is uncountable.

5.3.6

Suppose that A is uncountable. Prove that $\mathcal{P}(A)$ is uncountable.

Let us define a function $f : A \rightarrow \mathcal{P}(A)$

$$f(x) = \{x\}$$

this function is clearly injective, thus $\mathcal{P}(A)$ is uncountable, as desired.

5.3.7

Let $A \neq \emptyset$. Prove that if B is uncountable, then B^A is uncountable.

Let $a \in A$ and define $f : B \rightarrow B^A$ to be so that $f(b)$ is a function such that

$$(\forall a' \in A)((f(a))(a') = b$$

(i.e. it sends every a to value b). We follow that f is injective, thus we follow that B^A is uncountable.