# Contents

# 1 First order logic

## 1.1 Basic concepts

- A **deduction** consists of a sequence of sentences or other deductions.

- There are two types of sentences: some are true or false, while others contain unknown quantities (free variables) and its truthness depends on the choice of those quantities. The first type are called **propositions**, the latter called **predicates**.

- For example, “we are all going to die some day”, or “the earth is flat”, is a proposition, “$x + 1 > 2$” is a predicate.

- When we add (“deduce”) a proposition in the deduction, we mean that if all the preceding propositions in its context is true, then this new proposition is true. When we add a predicate, we mean if its free variables are chosen so that all the preceding sentences are true, then it is true.

- For example, from “the square of any real number is non negative” and “2 is a real number” we can get “$2^2$ is non negative”, while from “the square of any real number is non negative” and “x is a real number” we can get “$x^2$ is non negative”

## 1.2 The elements of the first order language, and the rules for deduction

In what follows we use $A_1, A_2, \dots A_k \vdash B_1, B_2 \dots B_l$ to mean “$B_1, \dots B_l$ can be deduced from $A_1, \dots A_k$”. In other words, all $B_i$ are true if all $A_i$ are true. The deductions we will cover is called natural deduction because we are allowed to make new assumptions, i.e. change things on the left of $\vdash$ sign.

- Predicates and functions
  - $A(x)$ denotes a predicate which gives a truth value for any values of $x$. The truth value depends only on what $x$ is. $(a = b \vdash A(a) \iff A(b))$
  - $f(x)$ denotes a function which sends a value $x$ to another value. The result depends only on the value of $x$. $(a = b \vdash f(a) = f(b))$
  - The usual practice is to use upper case letters to denote propositions and predicates, lower case letters from the beginning of the alphabet (like a, b, c, f, g...) to denote functions or constants, and lower case letters from the end of the alphabet (w, x, y, z) to denote variables. However this is not followed at all time and the exact meaning of a letter should be determined by context.
- $\wedge$ And
  - To show $A \wedge B$, need to show that both $A$ and $B$ are true. $(A, B \vdash A \wedge B)$
  - If $A \wedge B$ is known to be true, then $A$ is true, $B$ is also true. $(A \wedge B \vdash A, B)$
  - Truth table:

    | $A$ | $B$ | $A \wedge B$ |
    |---|---|---|
    | T | T | T |
    | T | F | F |
    | F | T | F |
    | F | F | F |

- $\vee$ Or
  - To show $A \vee B$, one can either show $A$ is true, or show $B$ is true. $(A \vdash A \vee B;\ B \vdash A \vee B)$
  - If $A \vee B$ is known to be true, both $A$ and $B$ implies $C$, then $C$ is true. $(A \vee B, A \implies C, B \implies C \vdash C;\ A \vee B, (A \vdash C), (B \vdash C) \vdash C)$
  - Truth table:

    | $A$ | $B$ | $A \vee B$ |
    |---|---|---|
    | T | T | T |
    | T | F | T |
    | F | T | T |
    | F | F | F |

- $\neg$ Not, $\perp$ Contradiction
  - $A$ can be replaced by $\neg\neg A$ and vice versa. $(A \vdash \neg\neg A;\ \neg\neg A \vdash A)$
  - To show $\neg A$, one can assume $A$ and deduce a contradiction. (proof by contradiction) $((A \vdash \perp) \vdash \neg A)$

  - If $A$ and $\neg A$ are both known to be true, there must be a contradiction. $(A, \neg A \vdash \bot)$
  - If there is a contradiction, one can deduce anything from it. $(\bot \vdash A)$
  - Truth table:

    | $A$ | $\neg A$ |
    |---|---|
    | T | F |
    | F | T |

- $\implies$ Implies
  - To show $A \implies B$, assume $A$, try to deduce $B$ from it. $((A \vdash B) \vdash A \implies B)$
  - If $A \implies B$ is known to be true, and $A$ is true, then $B$ is also true. $(A \implies B, A \vdash B)$
  - Truth table:

    | $A$ | $B$ | $A \implies B$ |
    |---|---|---|
    | T | T | T |
    | T | F | F |
    | F | T | T |
    | F | F | T |

- $\iff$ If and only if
  - $A \iff B$ is the same as $(A \implies B) \wedge (B \implies A)$. $(A \iff B \vdash (A \implies B) \wedge (B \implies A)$; $A \iff B \vdash A \implies B, B \implies A$; $(A \implies B) \wedge (B \implies A) \vdash A \iff B$; $A \implies B, B \implies A \vdash A \iff B)$
  - $A \iff B$ is the same as $(A \wedge B) \vee (\neg A \wedge \neg B)$.
  - Truth table:

    | $A$ | $B$ | $A \iff B$ |
    |---|---|---|
    | T | T | T |
    | T | F | F |
    | F | T | F |
    | F | F | T |

- $\forall$ For all
  - To show $\forall x P(x)$, need to deduce $P(x)$, here the variable $x$ can not appear in any assumptions as a free variable, i.e. one can not assume anything on $x$. (for example, one can not say "assume $P(x)$, then $\forall x P(x)$") $(A(x) \vdash \forall x A(x))$
  - If $\forall x P(x)$ is known to be true, then $P(t)$ is true for any term $t$ that does not contain bounded variable in $P$. (for example, one can not say $\forall x \exists y P(x,y)$ implies $\exists y P(y,y)$) $(\forall x A(x) \vdash A(t))$
- $\exists$ Exists
  - To show $\exists x P(x)$, need to show that $P(t)$ is true for some $t$ that does not contain bounded variable in $P$. (for example, one can not say $\forall y P(y,y)$ implies $\exists x \forall y P(x,y)$) $(A(t) \vdash \exists x A(x))$

  - If $\exists x P(x)$, and the fact that $P(y)$ is true for some $y$ would induce $B$ (which does not contain $y$), then $B$ can be deduced. Here $y$ must be a distinct variable. (for example, if we know $\exists x A(x)$, we can not say "let $y$ be such that $A(y)$, then $A(y)$, then $\forall y A(y)$") $(\exists x A(x), (A(x) \vdash B) \vdash B)$

- $=$ Equals

  - $=$ satisfies the usual qualities one should expect, like $a = a$, if $a = b$, $b = c$ then $a = c$, if $a = b$ then $b = a$. $(\vdash t = t; t = s, s = r \vdash t = r; t = s \vdash s = t)$

Summary of the deduction rules: (Color: Creation of a symbol, Annihilation of a symbol)

- Predicate and Function: $a = b \vdash A(a) \iff A(b)$; $a = b \vdash f(a) = f(b)$
- $\wedge$: $A, B \vdash A \wedge B$; $A \wedge B \vdash A, B$
- $\vee$: $A \vdash A \vee B$; $B \vdash A \vee B$; $A \vee B, A \implies C, B \implies C \vdash C$; $A \vee B, (A \vdash C), (B \vdash C) \vdash C$
- $\neg$: $A \vdash \neg\neg A$; $\neg\neg A \vdash A$
- $\perp$: $(A \vdash \perp) \vdash \neg A$; $A, \neg A \vdash \perp$; $\perp \vdash A$
- $\implies$: $(A \vdash B) \vdash A \implies B$; $A \implies B, A \vdash B$
- $\iff$: $A \iff B \vdash (A \implies B) \wedge (B \implies A)$; $A \iff B \vdash A \implies B, B \implies A$; $(A \implies B) \wedge (B \implies A) \vdash A \iff B$; $A \implies B, B \implies A \vdash A \iff B$
- $\forall$: $A(x) \vdash \forall x A(x)$; $\forall x A(x) \vdash A(t)$
- $\exists$: $A(t) \vdash \exists x A(x)$; $\exists x A(x), (A(x) \vdash B) \vdash B$
- $=$: $\vdash t = t$; $t = s, s = r \vdash t = r$; $t = s \vdash s = t$

## 1.3 Examples for deduction in first order logic

Here we do not distinguish "$A$" and "$A$ is true", and sometimes just add "is true" to make the sentence more readable. In more formal treatment of logic however these two statements would need be distinguished.

All the results of the examples here can be used in HW or exams without needing to prove them yourself.

Indentations here are just to clarify the logical orders of the assumptions, you do not need to write proofs in lines or with indentations in HW or exams.

**Example 0** $(A \implies B) \iff (\neg B \implies \neg A)$
Proof strategy: This is an iff statement, so assume one side, try to deduce the other side, and vice versa. The negatives in the statement would need to be dealt with using double negatives or proof by contradiction.
Proof:

```
Assume $A \implies B$
  Suppose $\neg B$
    Suppose $A$
      Then $B$ must be true
      Contradiction
    Hence $\neg A$
  Hence $\neg B \implies \neg A$
Hence $(A \implies B) \implies (\neg B \implies \neg A)$
Assume $\neg B \implies \neg A$
  Suppose $A$
    Suppose $\neg B$
      Then $\neg A$
      Contradiction
    Hence $\neg\neg B$, i.e. $B$
  Hence $A \implies B$
So $(\neg B \implies \neg A) \implies (A \implies B)$
$(A \implies B) \iff (\neg B \implies \neg A)$
```

**Example 1** $A \vee \neg A$
Proof strategy: This is an or statement so one would need to show either $A$ or $\neg A$. However, in general neither proposition can be guaranteed to be true, so a possible way around it is to use proof by contradiction.
Proof:

```
Assume $\neg(A \vee \neg A)$
  Assume $A$ is true
    $A \vee \neg A$ is true
    This contradicts with the assumption
  Hence $\neg A$ is true
  Hence $A \vee \neg A$ is true
  Contradiction
Hence $\neg\neg(A \vee \neg A)$, i.e. $A \vee \neg A$.
```

### 1.3.1 One can define some of the 5 logical symbols $\neg, \wedge, \vee, \implies, \iff$ by the other symbols

**Example 2** $A \wedge B \iff \neg(A \implies \neg B)$
Proof:

```
Assume $A \wedge B$
  Assume further that $A \implies \neg B$
    From the first assumption, $A$ is true
    Hence $\neg B$ from the second assumption
    However also from the first assumption, $B$ is true
    Contradiction
  Hence $\neg(A \implies \neg B)$
Hence $A \wedge B \implies \neg(A \implies \neg B)$
Assume $\neg(A \implies \neg B)$
  Assume $\neg A$
    Further assume $A$ is true
      There is a contradiction
      Hence $\neg B$ is true
    Hence $A \implies \neg B$
    This contradicts with the assumption that $\neg(A \implies \neg B)$
  Hence $\neg\neg A$, i.e. $A$ is true
  Assume $\neg B$
    Further assume $A$
    Because $\neg B$ is already known to be true, we have $A \implies \neg B$
    A contradiction
  Hence $\neg\neg B$, i.e. $B$
  This implies $A \wedge B$
So $\neg(A \implies \neg B) \implies A \wedge B$
Hence $A \wedge B \iff \neg(A \implies \neg B)$
```

**Example 3** $A \vee B \iff (\neg A \implies B)$

```
Proof:
Assume $A \vee B$
  Assume $A$ is true
    Assume further that $\neg A$ is true
      There is a contradiction, hence $B$ is true
    Hence $\neg A \implies B$
  Hence $A \implies (\neg A \implies B)$
  Assume $B$ is true
    Assume $\neg A$ is true
    Because $B$ is already known to be true, $\neg A \implies B$
  Hence $B \implies (\neg A \implies B)$
Hence $A \vee B \implies B \implies (\neg A \implies B)$
Assume $\neg A \implies B$
  From example 1, we have $A \vee \neg A$
  Suppose $A$
    Then $A \vee B$
  So $A \implies A \vee B$
  Suppose $\neg A$
    Then $B$
    Hence $A \vee B$
  Hence $\neg A \implies A \vee B$
  Hence $(A \vee \neg A) \implies A \vee B$
```

```
 Hence $A \vee B$
Hence $(\neg A \implies B) \implies A \vee B$
Hence $A \vee B \iff (\neg A \implies B)$.
```

**Example 4** $(A \implies B) \iff \neg A \vee B$

```
Proof:
By Example 3, $\neg A \vee B \iff (\neg\neg A \implies B)$
Hence Example 4 follows, because $\neg\neg A$ is just $A$.
```

### 1.3.2 Negating a proposition

**Example 5** $\neg(A \wedge B) \iff (\neg A \vee \neg B)$

```
Proof: Assume $\neg(A \wedge B)$
 From Example 1, $A \vee \neg A$
 Suppose $A$
  Further suppose $B$
   Then $A \wedge B$, a contradiction
  Hence $\neg B$
  Hence $\neg A \vee \neg B$
 Hence $A \implies \neg A \vee \neg B$
 Suppose $\neg A$
  Hence $\neg A \vee \neg B$
 Hence $\neg A \implies \neg A \vee \neg B$
 Hence $(A \vee \neg A) \implies \neg A \vee \neg B$
 Hence $\neg A \vee \neg B$
$\neg(A \wedge B) \implies \neg A \vee \neg B$
Suppose $\neg A \vee \neg B$
 Suppose $A \wedge B$
  Then $A$ and $B$ are both true
  Suppose $\neg A$
   There is a contradiction
  So $\neg A$ implies a contradiction
  Suppose $\neg B$
   There is a contradiction
  So $\neg B$ implies a contradiction
  Hence $\neg A \vee \neg B$ implies a contradiction
  Hence there must be a contradiction
 Hence $\neg(A \wedge B)$
Hence $\neg A \vee \neg B \implies \neg(A \wedge B)$
$\neg(A \wedge B) \iff \neg A \vee \neg B$
```

**Example 6** $\neg(A \vee B) \iff (\neg A \wedge \neg B)$

```
Proof:
Suppose $\neg(A \vee B)$
 Suppose $\neg(\neg A \wedge \neg B)$
```

```
    From Example 5, we have $\neg\neg A \vee \neg\neg B$, i.e. $A \vee B$
    A contradiction
  Hence $\neg A \wedge \neg B$
Hence $\neg(A \vee B) \implies \neg A \wedge \neg B$
Suppose $\neg A \wedge \neg B$
  Suppose $A \vee B$
    Then $\neg\neg A \vee \neg\neg B$
    Then from Example 5, $\neg(\neg A \wedge \neg B)$
    Contradiction
  Hence $\neg(A \vee B)$
Hence $\neg A \wedge \neg B \implies \neg(A \vee B)$
Hence $\neg A \wedge \neg B \iff \neg(A \vee B)$
```

**Example 7** $\neg(A \implies B) \iff \neg B \wedge A$
Proof:

```
Suppose $\neg(A \implies B)$
  Then $\neg(A \implies \neg\neg B)$
  From Example 2, we have $A \wedge \neg B$
Hence $\neg(A \implies B) \implies A \wedge \neg B$
Suppose $\neg B \wedge A$
  From example 2, we have $\neg(A \implies \neg\neg B)$, i.e. $\neg(A \implies B)$
Hence $\neg B \wedge A \implies \neg(A \implies B)$
Hence $\neg(A \implies B) \iff \neg B \wedge A$
```

**Example 8** $\neg(A \iff B) \iff (\neg B \wedge A) \vee (\neg A \wedge B)$
Proof: This follows from Example 5 and Example 7.

**Example 9** $\neg\forall x P(x) \iff \exists x \neg P(x)$
Proof strategy: When we assume left hand side and try to deduce the right hand side, we need to prove an existence statement. This could be done by using examples, but such an example is not obvious, so we try proof by contradiction.
Proof:

```
Suppose $\neg\forall x P(x)$
  Further assume that $\neg\exists x \neg P(x)$
    Suppose for some $y$, $\neg P(y)$
      Then $\exists x \neg P(x)$
      Contradiction
    So $\neg\neg P(y)$, i.e. $P(y)$
    Hence $\forall x P(x)$
    Contradiction
  Hence $\exists x \neg P(x)$
Hence $\neg\forall x P(x) \implies \exists x \neg P(x)$.
Suppose $\exists x \neg P(x)$
  Let $y$ be such that $\neg P(y)$
  Suppose $\forall x P(x)$
```

  Then $P(y)$
  Contradiction
Hence $\neg\forall x P(x)$
Hence $\exists x\neg P(x) \implies \neg\forall x P(x)$
$\neg\forall x P(x) \iff \exists x\neg P(x)$

**Example 10** $\neg\exists x P(x) \iff \forall x\neg P(x)$
Proof:
Suppose $\neg\exists x P(x)$
 Suppose $P(y)$ for some $y$
  Then $\exists x P(x)$
  Contradiction
 Hence $\neg P(y)$
 Hence $\forall x P(x)$
Hence $\neg\exists x P(x) \implies \forall x P(x)$
Suppose $\forall x\neg P(x)$
 Suppose $\exists x P(x)$
  Let $y$ be such that $P(y)$
  By the prior assumption that $\forall x\neg P(x)$, we have $\neg P(y)$
  Contradiction
 Hence $\neg\exists x P(x)$
Hence $\forall x\neg P(x) \implies \neg\exists x P(x)$
$\neg\exists x P(x) \iff \forall x\neg P(x)$

### 1.3.3 Injections

**Example 11** $(\forall x\forall y\neg(x = y) \implies \neg(f(x) = f(y))) \implies (\forall x\forall y\neg(x = y) \implies \neg(f(f(x)) = f(f(y))))$
Proof:
Suppose $\forall x\forall y\neg(x = y) \implies \neg(f(x) = f(y))$
 Consider some $z$, $w$ so that $\neg(z = w)$
  Then by assumption, $\neg(z = w) \implies \neg(f(z) = f(w))$
  Hence $\neg(f(z) = f(w))$
  Also by assumption, $\neg(f(z) = f(w)) \implies \neg(f(f(z)) = f(f(w)))$
  Hence $\neg(f(f(z)) = f(f(w)))$
 Hence $\neg(z = w) \implies \neg(f(f(z)) = f(f(w)))$
Hence $\forall x\forall y\neg(x = y) \implies \neg(f(f(x)) = f(f(y)))$
$(\forall x\forall y\neg(x = y) \implies \neg(f(x) = f(y))) \implies (\forall x\forall y\neg(x = y) \implies \neg(f(f(x)) = f(f(y))))$

### 1.3.4 More tautologies in proposition logic

**Example 12** $((A \implies B) \wedge (B \implies C)) \implies (A \implies C)$
Proof:
Assume $((A \implies B) \wedge (B \implies C))$
 Then $A \implies B$

```
  Assume $A$
    Then because $A \implies B$, $B$ is true
    Also from the first assumption, $B \implies C$
    So $C$ is true
  So $A \implies C$
So $((A \implies B) \wedge (B \implies C)) \implies (A \implies C)$
```

**Example 13** $(A \wedge B) \wedge C \iff A \wedge (B \wedge C)$

```
Proof:
Assume $(A \wedge B) \wedge C$
  Then both $A \wedge B$ and $C$ are true
  Hence $A$, $B$, $C$ are all true
  Hence $B \wedge C$ is true
  So $A \wedge (B \wedge C)$ is true
This shows that $(A \wedge B) \wedge C \implies A \wedge (B \wedge C)$
Assume $A \wedge (B \wedge C)$
  Both $A$ and $B \wedge C$ are true
  $A$, $B$, $C$ are all true
  Hence $(A \wedge B)$ is true
  Hence $(A \wedge B) \wedge C$ is true
Hence $A \wedge (B \wedge C) \implies (A \wedge B) \wedge C$
```

**Example 14** $(A \vee B) \vee C \iff A \vee (B \vee C)$

```
Proof:
Assume $(A \vee B) \vee C$
  Assume $A \vee B$
    Assume $A$
      Then $A \vee (B \vee C)$
    Hence $A \implies A \vee (B \vee C)$
    Assume $B$
      Then $B \vee C$, which implies $A \vee (B \vee C)$
    Hence $B \implies A \vee (B \vee C)$
    Hence $A \vee (B \vee C)$
  Hence $A \vee C \implies A \vee (B \vee C)$
  Assume $C$
    Then $B \vee C$
    Hence $A \vee (B \vee C)$
  This implies that $A \vee (B \vee C)$ is true
Hence $(A \vee B) \vee C \implies A \vee (B \vee C)$
Assume $A \vee (B \vee C)$
  Assume $B \vee C$
    Assume $C$
      Then $(A \vee B) \vee C$
    Hence $C \implies A \vee (B \vee C)$
    Assume $B$
```

   Then $A \vee B$, which implies $(A \vee B) \vee C$
  Hence $B \implies (A \vee B) \vee C$
  Hence $(A \vee B) \vee C$
 Hence $B \vee C \implies (A \vee B) \vee C$
 Assume $A$
  Then $A \vee B$
  Hence $(A \vee B) \vee C$
 This implies that $(A \vee B) \vee C$ is true
Hence $A \vee (B \vee C) \implies (A \vee B) \vee C$
Together with the results of the first half, we get $(A \vee B) \vee C \iff A \vee (B \vee C)$

**Example 15** $A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C)$
Proof:
Suppose $A \vee (B \wedge C)$
 Assume $A$
  Then $A \vee B$, $A \vee C$ are both true
  So $(A \vee B) \wedge (A \vee C)$
 So $A \implies (A \vee B) \wedge (A \vee C)$
 Assume $B \wedge C$
  Then $B$ and $C$ are both true
  Hence $A \vee B$, $A \vee C$ are both true
  So $(A \vee B) \wedge (A \vee C)$
 So $B \wedge C \implies (A \vee B) \wedge (A \vee C)$
 So $(A \vee B) \wedge (A \vee C)$
This shows $A \vee (B \wedge C) \implies (A \vee B) \wedge (A \vee C)$
Suppose $(A \vee B) \wedge (A \vee C)$
 Then $A \vee B$ and $A \vee C$ are both true
 From Example 1, we have $A \vee \neg A$
 Suppose $A$ is true
  Then $A \vee (B \wedge C)$ is true
 Suppose $\neg A$ is true
  Since $A \vee B$ is known, we consider the two cases, which is when $A$ is true and when $B$ is true
  Suppose $A$ is true
   There is a contradiction, hence $B$
  Suppose $B$ is true, we get the same result
  Hence $B$ is true
  Do the same for $A \vee C$, we get that $C$ is true
  So $B \wedge C$ is true, which implies $A \vee (B \wedge C)$
 So $A \vee (B \wedge C)$
This shows that $(A \vee B) \wedge (A \vee C) \implies A \vee (B \wedge C)$
Hence $A \vee (B \wedge C) \iff (A \vee B) \wedge (A \vee C)$

**Example 16** $A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C)$
Proof:

```
Suppose $A \wedge (B \vee C)$
  Then $A$ is true
  And $B \vee C$ is true
  Suppose $B$ is true
    Then $A \wedge B$ is true, which implies $(A \wedge B) \vee (A \wedge C)$
  Hence $B \implies (A \wedge B) \vee (A \wedge C)$
  Suppose $C$ is true
    Then $A \wedge C$ is true, which implies $(A \wedge B) \vee (A \wedge C)$
  Hence $C \implies (A \wedge B) \vee (A \wedge C)$
  Hence $(A \wedge B) \vee (A \wedge C)$ is true
This shows that $A \wedge (B \vee C) \implies (A \wedge B) \vee (A \wedge C)$
Suppose $(A \wedge B) \vee (A \wedge C)$
  Suppose $A \wedge B$
    Then both $A$ and $B$ are true
    Hence $B \vee C$ is true
    Hence $A \wedge (B \vee C)$
  Suppose $A \wedge C$
    Then both $A$ and $C$ are true
    Hence $B \vee C$ is true
    Hence $A \wedge (B \vee C)$
  This shows that $A \wedge (B \vee C)$ is true
Hence $(A \wedge B) \vee (A \wedge C) \implies A \wedge (B \vee C)$
This shows that $A \wedge (B \vee C) \iff (A \wedge B) \vee (A \wedge C)$
```

## 1.4 A few more commonly seen logic symbols

- $a \neq b$ is short hand for $\neg(a = b)$
- $\nexists x P(x)$ is short hand for $\neg \exists x P(x)$
- $\exists! x P(x)$ means $(\exists x P(x)) \wedge (\forall x \forall y (P(x) \wedge P(y) \implies (x = y)))$

# 2 First order theory of natural numbers (First order Peano Arithmetics)

To remind ourselves and others that we are doing deduction in the universe of natural numbers, we replace $\forall x$ with $\forall x \in \mathbb{N}$, $\exists x$ with $\exists x \in \mathbb{N}$.

## 2.1 New symbols and rules

- We introduces 4 more symbols and 7 more rules associated to them. The symbols are: 0, $s(\cdot)$ (successor, intuitively, $s(n) = n + 1$), $+$, $\times$. Here 0 is a constant and the other 3 are functions.
- Rule 1: $s$ is an injection: $\forall x \in \mathbb{N} \forall y \in \mathbb{N} \neg(x = y) \implies \neg(s(x) = s(y))$
- Rule 2: 0 is the first natural number: $\neg \exists x \in \mathbb{N}(0 = s(x))$
- Rule 3: Mathematical induction: $(P(0) \wedge \forall \in \mathbb{N} x(P(x) \implies P(s(x)))) \implies \forall \in \mathbb{N} x P(x)$
- Rule 4: First rule for addition: $\forall x \in \mathbb{N} x + 0 = x$
- Rule 5: Second rule for addition: $\forall x \in \mathbb{N} \forall y \in \mathbb{N} x + s(y) = s(x + y)$
- Rule 6: First rule for multiplication: $\forall x \in \mathbb{N} x \times 0 = 0$
- Rule 7: Second rule for multiplication: $\forall x \in \mathbb{N} \forall y \in \mathbb{N} x \times s(y) = x \times y + x$

A shortened format for writing proofs using mathematical induction is:
(what needs to be proved is $\forall x \in \mathbb{N} P(x)$)
Induction on x
Prove $P(0)$
Suppose $P(x)$
...
$P(s(x))$
Hence by induction, $\forall x \in \mathbb{N} P(x)$.

The numbers are defined as $1 = s(0)$, $2 = s(s(0))$, .... $s(x)$ can also be written as $x + 1$.

## 2.2 Some examples

**Example 17** $1 + 2 = 3$
Proof:
$s(0) + s(s(0)) = s(s(0) + s(0)) = s(s(s(0) + 0)) = s(s(s(0))) = 3.$
Here we repeated use the properties of $=$ in logic and the rule 5 and 6 for natural numbers.

**Example 18** $\forall x \in \mathbb{N} \neg(x = s(x))$
Proof:
Induction on $x$.
Suppose $0 = s(0)$
 Then $\exists x \in \mathbb{N} 0 = s(x)$, which contradicts with rule 2
So $\neg(0 = s(0))$.
Suppose $\neg(x = s(x))$
 Suppose $(s(x) = s(s(x)))$
  Then by Rule 1, $x = s(x)$, a contradiction
 Hence $\neg(s(x) = s(s(x)))$
By induction, $\forall x \in \mathbb{N} \neg(x = s(x))$

## 2.3 Properties of arithmetics

The followings are true for all natural numbers $a.b, c \ldots$:

- $0 + a = a$
- $a + b = b + a$
- $(a + b) + c = a + (b + c)$
- $0 \times a = 0$
- $a \times b = b \times a$
- $(a \times b) \times c = a \times (b \times c)$
- $a \times (b + c) = a \times b + a \times c$
- $a + b = c + b \iff a = c$
- $a \times b = c \times b \iff (b = 0 \vee a = c)$
- $\ldots$

They can all be easily proven via mathematical induction.

**Example 19** $\forall x \in \mathbb{N} 0 + x = x$
Proof:
Induction on $x$
$0 + 0 = 0$
Suppose $0 + x = x$
$0 + s(x) = s(0 + x) = s(x)$
Hence by induction, the proposition is proved.

**Example 20** $\forall x \in \mathbb{N} \forall y \in \mathbb{N} x + y = y + x$
Proof:
Induction on $x$
$\forall y \in \mathbb{N} 0 + y = y = y + 0$ by Example 19
Suppose $\forall y \in \mathbb{N} x + y = y + x$
Induction on $y$
$s(x) + 0 = s(x) = 0 + s(x)$
Suppose $s(x) + y = y + s(x)$
$s(x) + s(y) = s(s(x) + y) = s(y + s(x)) = s(s(y + x)) = s(s(x + y))$, and $s(y) + s(x) = s(s(y) + x) = s(x + s(y)) = s(s(x + y))$, these two are the same
Hence by induction, $\forall y \in \mathbb{N} s(x) + y = y + s(x)$
By induction, the proposition is proved.

## 2.4 Divisibility and comparison

**Definition:** $a|b$ iff $\exists c \in \mathbb{N} b = a \times c$

**Definition:** $a \leq b$ iff $\exists c \in \mathbb{N} b = a + c$, $a \geq b$ iff $b \leq a$, $a < b$ iff $a \leq b$ and $a \neq b$, $a > b$ iff $b < a$.

**Definition:** The power function is defined as $m^0 = 1$ when $m \neq 0$, $m^{n+1} = m^n \times m$. The factorial function is defined as $0! = 1$, $(n+1)! = n!(n+1)$. The summation symbol is defined as $\sum_{i=a}^{a} f(i) = f(a)$, $\sum_{i=a}^{b+1} f(a) = \sum_{i=a}^{b} f(a) + f(b+1)$. The product symbol is defined as $\prod_{i=a}^{a} f(i) = f(a)$, $\prod_{i=a}^{b+1} f(a) = \prod_{i=a}^{b} f(a) \times f(b+1)$.

**Remark** Strictly speaking, the concept of functions in first order logic as described in the previous section must be defined everywhere, so if one wants to be completely rigorous one should extend those functions to where they are undefined, e.g. let $0^0 = 1$.

More properties:

- $a = b \vee a < b \vee a > b$
- $\neg(a < b \wedge a > b)$
- $(a \leq b \wedge b \leq c) \implies a \leq c$
- $a|b \implies a|b \times c$
- $a|b \wedge a > 0 \implies a \leq b$
- $c > 0 \implies (a < b \iff a + c < b + c \iff a \times c < b \times c)$
- ...

All these can be proven from the rules, definitions and the properties of × and + in the previous subsection.

## 2.5 Formal and informal proofs

Formal proofs: every step must be an assumption, or follows from prior steps using one of the prescribed rules (rules of first order logic, first order theory of natural numbers, etc).

Guideline for informal proofs:

- Write down enough steps so that a reader that is mathematically literate can fill in the rest and get a formal proof.
- For the current class, write down as much detail as the examples I do in class/put in lecture notes.
- When you're not sure, err on the side of more details.

Examples of formal vs informal proofs:

**Example 21** $\forall x \in \mathbb{N}(x = 0 \vee \exists y \in \mathbb{N} x = y + 1)$
Formal Proof:
Induction on $x$.
$0 = 0$
Which implies $0 = 0 \vee \exists y \in \mathbb{N} 0 = y + 1$
Suppose $x = 0 \vee \exists y \in \mathbb{N} x = y + 1$
$x + 1 = x + 1$
$\exists y \in \mathbb{N} x + 1 = y + 1$
$x + 1 = 0 \vee \exists y \in \mathbb{N} x + 1 = y + 1$
By induction, $\forall x \in \mathbb{N}(x = 0 \vee \exists y \in \mathbb{N} x = y + 1)$
Informal proof:
We prove it by induction on $x$. When $x = 0$, $0 = 0$. Suppose the statement $x = 0 \vee \exists y \in \mathbb{N} x = y + 1$ is known for some $x$, because $x + 1 = x + 1$ it is also true for $x + 1$. Hence it is true for all $x$.

**Example 22** $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(x \leq y \vee y \leq x)$
Informal Proof:
Induction on $x$. $0 \leq y$ for all $y$. Suppose this is known for some value $x$, then, for each $y$, either $x \leq y$ or $y \leq x$. In the latter case $y \leq x + 1$, while in the former case, let $z$ be such that $y = x + z$, then from the previous example $z = 0$ or $z \geq 1$. If $z = 0$ then $x = y$ and $y \leq x + 1$, while if $z \geq 1$ then $x + 1 \leq y$. Hence in all cases the statement is true for $x + 1$, the proposition is proved.
Formal Proof:

Firstly include the proofs of Example 19, Example 20, Example 21, and the associativity rule of addition.
Induction on $x$
By Example 19, $0 + y = y$
$0 \leq y \vee y \leq 0$
$\forall y \in \mathbb{N}(0 \leq y \vee y \leq 0)$
Now suppose $\forall y \in \mathbb{N}(x \leq y \vee y \leq x)$
$x \leq y \vee y \leq x$
Suppose $x \leq y$
$\exists z \in \mathbb{N}(x + z = y)$
By Example 21, $z = 0 \vee \exists w \in \mathbb{N} z = w + 1$
Suppose $z = 0$
$x = x + 0 = y$
$y + 1 = x + 1$
$y \leq x + 1$
$x + 1 \leq y \vee y \leq x + 1$
Suppose $\exists w \in \mathbb{N} z = w + 1$
Let $w$ be such that $z = w + 1$
$(x + 1) + w = x + (1 + w)$ by associativity rule of addition.
$1 + w = w + 1$ by Example 20.
$(x + 1) + w = x + (1 + w) = x + (w + 1) = x + z = y$
$x + 1 \leq y$
Hence $x + 1 \leq y \vee y \leq x + 1$
By $\vee$ rule, $x + 1 \leq y \vee y \leq x + 1$
Suppose $y \leq x$
$\exists z \in \mathbb{N} y + z = x$
Let $z$ be such that $y + z = x$
$y + (z + 1) = x + 1$
$y \leq x + 1$
$x + 1 \leq y \vee y \leq x + 1$
By $\vee$ rule again, $x + 1 \leq y \vee y \leq x + 1$
By induction, the Example is proved.

**Starting from now we will stop requiring that all deduction steps must follow the rules of first order logic or Peano arithmetics. In other words, we will freely use properties about numbers we learned in grade schools and in your previous classes.**

**Example 23** $\forall x \in \mathbb{N} \neg(\exists y \in \mathbb{N} x = 2y \wedge \exists y \in \mathbb{N} x = 2y + 1)$
Proof:
Suppose $\exists y \in \mathbb{N} x = 2y \wedge \exists y \in \mathbb{N} x = 2y + 1$
Let $z$ be such that $x = 2z$
Let $w$ be such that $x = 2w + 1$
(By Example 22) $z \leq w \vee w \leq z$
Suppose $z \leq w$

$\exists c \in \mathbb{N} w = z + c$

Let $c$ satisfy $w = z + c$

$2(z + c) + 1 = 2z$, hence $2c + 1 = 0$, contradiction.

Suppose $w \leq z$

$\exists c \in \mathbb{N} z = w + c$

Let $c$ satisfy $z = w + c$

$2w + 1 = 2(w + c)$, hence $1 = 2c$

Whether $c = 0$ or $c > 0$, there is a contradiction.

Hence $\neg \exists y \in \mathbb{N} x = 2y \wedge \exists y \in \mathbb{N} x = 2y + 1$

$\forall x \neg \exists y \in \mathbb{N} x = 2y \wedge \exists y \in \mathbb{N} x = 2y + 1$

## 2.6 Further examples on induction and proof writing

- Unless specified, in an informal proof you are allowed to use simple tautologies in first order logic (similar to the examples in this notes) as well as things you learn prior to this course (e.g. arithmetic, Euclidean geometry, calculus etc).
- Clearly distinguish comments ("we are going to show...", "This is because of ..."), assumptions ("suppose..", "Let x satisfy...") and other regular statements in the proof.
- It's never a bad idea to write more details, but the "details" have to be correct
- For now, it is recommended that you write down the reasoning of every step in parenthesis when writing proofs.

**Example 24** Problem 4 in Workshop 2:

Suppose $x^2 = 2y^2$

By Problem 3, $\exists x' \in \mathbb{N}(x = 2x')$

$4x'^2 = 2y^2$

$2x'^2 = y^2$

By Problem 3, $\exists y' \in \mathbb{N}(y = 2y')$

$\exists x' \in \mathbb{N} \exists y' \in \mathbb{N}(x'^2 = 2y'^2 \wedge x = 2x' \wedge y = 2y')$

$x^2 = 2y^2 \implies \exists x' \in \mathbb{N} \exists y' \in \mathbb{N}(x'^2 = 2y'^2 \wedge x = 2x' \wedge y = 2y')$

This indicate to us that we should try induction on $x$, because what happens to a larger $x$ can be reduced to what happens to a smaller $x$. Yet attempts of simple induction doesn't work. What is needed is first strengthen the proposition that needs to be proved then use induction, as follows:

Induction on $N$ to show that $\forall x \in \mathbb{N}((x \leq N) \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0))$

When $N = 0$, $x \leq N$ implies $x = 0$, hence this predicate is true. (here we used tautology $(A \implies C) \implies (A \implies (B \implies C))$, and the fact that $a \leq 0 \implies a = 0$)

Suppose $\forall x \in \mathbb{N}((x \leq N) \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0))$
 Suppose $\neg\forall x \in \mathbb{N}((x \leq N+1) \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0))$
  Then $\exists x \in \mathbb{N}((x \leq N+1) \wedge \exists y \in \mathbb{N}(x^2 = 2y^2) \wedge \neg(x = 0))$
  Let $x$, $y$ satisfy $x^2 = 2y^2$ and $x \neq 0$.
  Due to the earlier argument, $\exists x' \in \mathbb{N}(x = 2x')$, $\exists y' \in \mathbb{N}(y = 2y')$, and $x'^2 = 2y'^2$.
  Because $x' < x$, $x' \leq N$, a contradiction.
 Hence $\forall x \in \mathbb{N}((x \leq N+1) \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0))$
The Example is proved due to induction.

**Example 25, an example of recursive definition** $\forall n \in \mathbb{N}(2^n \geq 2n)$
Proof:
Induction on $n$
$2^0 = 1 \geq 0 = 2 \times 0$
Suppose $2^n \geq 2n$
 $2^{n+1} \geq 4n$
 We know $n = 0 \vee n \geq 1$
 Suppose $n = 0$
  $2^{n+1} = 2 \geq 2 = 2 \times (0+1)$
 Suppose $n \geq 1$
  $4n \geq 2(n+1)$, hence $2^{n+1} \geq 2(n+1)$
By induction, $\forall n \in \mathbb{N}(2^n \geq 2n)$

Generally, if one need to make use of recursive definitions (define a function using the same function, but acts on different values), one use mathematical induction.

## 2.7 The remainder theorem

**Example 26, Remainder theorem** $\forall x \in \mathbb{N}((x > 0) \implies (\forall y \in \mathbb{N}\exists! r \in \mathbb{N}\exists! q \in \mathbb{N} r < x \wedge y = xq + r))$
Proof:
Suppose $x > 0$
For existence: prove by induction on $y$
When $y = 0$, $0 = x \times 0 + 0$, so we can let $r = q = 0$
Suppose $\exists r \in \mathbb{N}\exists q \in \mathbb{N} r < x \wedge y = xq + r$
 We have $r + 1 < x$ or $r + 1 = x$
 Suppose $r + 1 < x$
  Then $r + 1 < x \wedge y + 1 = xq + r + 1$
  so $\exists r \in \mathbb{N}\exists q \in \mathbb{N} y + 1 = xq + r$
 Suppose $r + 1 = x$
  Then $0 < x \wedge y + 1 = x(q+1)$
  so $\exists r \in \mathbb{N}\exists q \in \mathbb{N} y + 1 = xq + r$
By induction, $\forall y \exists r \in \mathbb{N}\exists q \in \mathbb{N} r < x \wedge y = xq + r$
Now for uniqueness: suppose $xq + r = xq' + r'$, $r < x$, $r' < x$
$q = q'$ or $q < q'$ or $q > q'$

Suppose $q = q'$, then $xq = xq'$, hence $r = r'$, which shows uniqueness of both $q$ and $r$
If $q < q'$, let $q' = p + q$, so $r = xp + r'$. Because $p > 1$, $xp + r' > x$, a contradiction, hence uniqueness is also true in this case.
The situation for $q > q'$ is similar.

## 2.8 Alternatives to induction

We have an alternative presentation of induction:

**Example 27** (Any non empty set of natural numbers has a minimum element)
$(\exists x \in \mathbb{N} P(x)) \implies (\exists x \in \mathbb{N}(P(x) \wedge (\forall y \in \mathbb{N}(P(y) \implies x \leq y))))$.
Proof:
We prove the contrapositive.
Assume $\forall x \in \mathbb{N}(\neg P(x) \vee \exists y \in \mathbb{N}(P(y) \wedge y < x))$.
We will use induction on $x$ to prove $\forall x \in \mathbb{N} \neg \exists y \in \mathbb{N}(P(y) \wedge y < x)$
Suppose $\exists y \in \mathbb{N}(P(y) \wedge y < 0)$
Yet $\neg \exists y \in \mathbb{N}(y < 0)$
Contradiction
Hence $\neg \exists y \in \mathbb{N}(P(y) \wedge y < 0)$
Suppose $\neg \exists y \in \mathbb{N}(P(y) \wedge y < x)$
Suppose $\exists y \in \mathbb{N}(P(y) \wedge y < x + 1)$
Let $z$ be such that $P(z) \wedge z < x + 1$
Suppose $z < x$
$\exists y \in \mathbb{N}(P(y) \wedge y < x)$, a contradiction
Hence $z = x$
Because of the initial assumption, and that $P(z)$ is true, $\exists y \in \mathbb{N}(P(y) \wedge y < z)$
Hence $\exists y \in \mathbb{N}(P(y) \wedge y < x)$, a contradiction.
Hence $\neg \exists y \in \mathbb{N}(P(y) \wedge y < x + 1)$
By induction, $\forall x \in \mathbb{N} \neg \exists y \in \mathbb{N}(P(y) \wedge y < x)$
Hence $\forall x \in \mathbb{N} \neg P(x)$
The Example is proved.

An equivalent formulation of Example 27 is:

$$P(0) \wedge \forall n(\forall x((x < n) \implies P(x)) \implies P(n)) \implies \forall x P(x)$$

This provides an alternative proof of Example 24 and Example 26.

**Example 24** (alternative proof)
Suppose $x^2 = 2y^2$
By Problem 3, $\exists x' \in \mathbb{N}(x = 2x')$
$4x'^2 = 2y^2$
$2x'^2 = y^2$

By Problem 3, $\exists y' \in \mathbb{N}(y = 2y')$

$\exists x' \in \mathbb{N} \exists y' \in \mathbb{N}(x'^2 = 2y'^2 \wedge x = 2x' \wedge y = 2y')$

$x^2 = 2y^2 \implies \exists x' \in \mathbb{N} \exists y' \in \mathbb{N}(x'^2 = 2y'^2 \wedge x = 2x' \wedge y = 2y')$

Induction on $x$ to show that $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$

When $N = 0$, $x \leq N$ implies $x = 0$, hence this predicate is true. (here we used tautology $(A \implies C) \implies (A \implies (B \implies C))$, and the fact that $a \leq 0 \implies a = 0$)

Suppose $(x \leq N) \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$

Suppose $(N+1)^2 = 2y^2$

Due to the earlier argument, $\exists x' \in \mathbb{N}(N + 1 = 2x')$, $\exists y' \in \mathbb{N}(y = 2y')$, and $x'^2 = 2y'^2$.

Because $x' < N + 1$, $x' \leq N$, hence $x' = 0$ Hence $N + 1 = 2x' = 0$.

Hence $\forall x \in \mathbb{N}((x \leq N + 1) \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0))$

The Example is proved due to induction.

## 2.9 Primes

**Definition** A natural number $p$ is called “prime” iff $p > 1 \wedge (\forall f \in \mathbb{N} f|p \implies (f = 1 \vee f = p))$.

**Example 28** $\forall n \in \mathbb{N}((n > 1) \implies \exists p \in \mathbb{N}(Prime(p) \wedge p|n))$

Proof:

Suppose otherwise

Let $n$ be the smallest $n$ so that $(n > 1) \wedge \forall p \in \mathbb{N}(p|n \implies \neg Prime(p))$.

$n|n$

Hence $\neg Prime(n)$

Hence $\exists m \in \mathbb{N}((m|n) \wedge (m > 1) \wedge (m < n))$

Let $m$ satisfy $m|n \wedge m > 1 \wedge m < n$

Inductive hypothesis implies that $\exists p(Prime(p) \wedge p|m)$

Let $p'$ be a prime number that divides $m$

Then $p'|n$, a contradiction.

Hence $\forall n \in \mathbb{N}((n > 1) \implies \exists p \in \mathbb{N}(Prime(p) \wedge p|n))$

**Example 29** $\forall p \in \mathbb{N}(Prime(p) \implies \forall x \in \mathbb{N} \forall y \in \mathbb{N}(p|(xy) \implies (p|x \vee p|y)))$.

Suppose otherwise.

Let $p$ be the smallest prime number so that $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(p|(xy) \implies (p|x \vee p|y))$ is false.

Let $x$ be the smallest natural number so that $\exists y(p|(xy) \wedge \neg(p|x) \wedge \neg(p|y))$

Let $y$ be the smallest natural number so that $(p|(xy) \wedge \neg(p|x) \wedge \neg(p|y))$

Suppose $p \leq x$

Let $x = p + x'$

From Example 26, let $r, q$ satisfy $x'y = qp + r \wedge r < p$

Then $xy = (p + x')y = py + x'y = p(q + y) + r$

Hence $r = 0$, $p|(x'y)$

From Example 26, let $r', q'$ satisfy $x' = r' + q'p \wedge r' < p$

```
    Then $x = (q' + 1)p + r'$
    Hence $r' \neq 0$, $\neg(p|x')$
    By assumption, $\neg(p|y)$
    Contradiction with the minimality of $x$
  Hence $x < p$
  Similarly, $y < p$ (go through the same argument, with $x$ replaced with $y$)
  Let $xy = pk$
  Then $k < p$
  $k = 0 \lor k = 1 \lor k > 1$
  If $k = 0$
    $x = 0$ or $y = 0$, a contradiction because $p|0$
  If $k = 1$
    $xy = p \land x < p \land y < p$, a contradiction
  If $k > 1$
    From Example 27, Let $p'$ be a prime number such that $p'|k$
    By minimality of $p$, $p'|x \lor p'|y$
    Suppose $p'|x$
      Let $w$ satisfy $x = p'w$
        Then $p|wy$ and $w < x$
        Contradiction
    The case when $p'|y$ is the same.
(Here because "contradiction" doesn't have any variables, all assumptions made
in the various "let" statements are all eliminated)
Hence $\forall p \in \mathbb{N}(Prime(p) \implies \forall x \in \mathbb{N} \forall y \in \mathbb{N}(p|(xy) \implies (p|x \lor p|y)))$.
```

# 3 Sets

## 3.1 Definition of sets

The language of axiomatic set theory consists of the language of first order logic with an additional predicate $\in$. As in the case of natural numbers, we will also extend this language by introducing various shorthand notations for convenience.

Due to time constraint we will not do a rigorous treatment of axiomatic set theory. However, all examples we will do (and all mathematics you learned so far) can indeed be proved from the axioms and the deduction rules and it would be a good exercise to try doing that yourself.

Here is a commonly used set of axioms for set theory (all lower case Latin letters are sets, $\phi$ is a predicate)

- Extensionality: $\forall x \forall y (\forall z (z \in x \iff z \in y) \implies x = y)$
- Empty set: $\exists x \forall y \neg (y \in x)$.
- Transfinite induction: $\forall x (\forall y (y \in x \implies \phi(y)) \implies \phi(x)) \implies \forall x \phi(x)$
- Replacement: $\forall w_1 \dots \forall w_n \forall s (\forall x (x \in s \implies \exists ! y \phi(x, y, w_1, \dots w_n, s)) \implies \exists t \forall y (y \in t \implies \exists x \in s \phi(x, y, w_1, \dots w_n, s)))$, $\phi$ is a predicate.
- Pair: $\forall x \forall y \exists z (x \in z \wedge y \in z)$.
- Union: $\forall x \exists y \forall e (e \in y \iff \exists z (z \in x \wedge e \in z))$
- Infinity: $\exists x (\exists y (y \in x) \wedge \forall y (y \in x \implies \exists z (z \in x \wedge \forall w (w \in y \implies w \in z) \wedge \neg (y = z))))$
- Power set: $\forall x \exists y \forall z (\forall w (w \in z \implies w \in x) \iff z \in y)$
- Choice: $\forall z (\forall x (x \in z \implies \exists y (y \in z)) \implies \exists f \forall p (p \in f \implies \exists x \exists y \forall q (q \in p \implies q = x \vee \forall r (r \in q \implies r = x \vee r = y) \wedge x \in z \wedge y \in x)))$

In English, these axioms are

- Extensionality: Two sets are the same if they have the same elements.
- Empty set: There is an empty set.
- Transfinite induction: If a predicate being true for all elements of a set implies that it is true for the set, then it is true for all sets.
- Replacement: One can replace all elements of a set with other sets, and the result will be a set.
- Pair: There is a set consisting of two sets.
- Union: The union of a set of sets is a set.

- Infinity: This implies that $\mathbb{N}$ is a set.
- Power set: The power set of any set is a set.
- Choice: If there is a set of sets, one can define a function from it to the union of its members, such that every element get sends to one of its member. This is called a choice function.

We may discuss these axioms briefly at the end of the semester if we have some extra time. They WILL NOT be covered in the exams.

Instead of refering to the axioms, we understand sets intuitively as collections of mathematical objects that can be obtained via the various set-building operation and will just use this intuition for proofs, i.e. we will do "naive set theory". By transfinite induction $\forall x \neg x \in x$ so the collection of all sets is not a set. From now on, if unspecified, "function" always mean set theoretic function and not the "function" we saw in first order logic.

## 3.2 Basic concepts in set theory

By default almost all of mathematics is carried out within set theory, in other words, almost everything you have ever seen and will ever see in a math textbook is a set.

- $\emptyset$ is a set.
- $\mathbb{N}$ is a set. (In set theory, where we want to make sure everything is a set, it is often represented as $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}, \dots\}$, the existence of which is guaranteed by an axiom in ZFC)
- If $A$, $B$ are two sets, $x \in A \implies x \in B$, then we say $A$ is a subset of $B$, denoted as $A \subseteq B$.
- From a finite collection of values $x_1, \dots x_n$, there is a set consisting of them, denoted as $\{x_1, \dots x_n\}$.
- (Power) If $X$ is a set, the power set $P(X)$, which consists of all subsets of $X$, is a set.
- (Specification) If $X$ is a set, the collection of elements in $X$ that satisfy some predicate $\phi$, denoted as $\{x \in X : \phi(x)\}$, is a set.
- (Union) If $A$ is a set of sets, there is a set consisting of all the members of that are in some member of $A$, denoted as $\bigcup_{a \in A} a$ (or $\bigcup A$). When $A = \{B_1, \dots B_n\}$ we write it as $B_1 \cup \dots \cup B_n$.
- (Intersection) $A$ is a set of sets, $\bigcap_{a \in A} a$ (or $\bigcap A$) means $\{x \in \bigcup_{a \in A} a : \forall a \in A (x \in a)\}$. When $A = \{B_1, \dots B_n\}$ we write it as $B_1 \cap \dots \cap B_n$.
- (Exclusion) $A$ and $B$ are two sets, $A \backslash B$ means $\{x \in A : \neg(x \in B)\}$.

- (Product) Given any two sets $a$ and $b$, a pair $(a,b)$ is a set, such that $(a,b)=(a',b') \iff a=a' \wedge b=b'$. If $A$ and $B$ are two sets, there is a set consisting of ordered pairs of elements in $A$ and $B$, denoted as $A\times B$.
- (Relation) A relation between $A$ and $B$ is a subset of $A\times B$. $(a,b)\in R$ is also written as $aRb$
- (Function) If a relation $R$ between $A$ and $B$ satisfy that $\forall x\in A\exists! y\in B(x,y)\in R$, $R$ is called a function from $A$ to $B$, denoted as $R:A\to B$, and $xRy$ is written as $y=R(x)$. $A$ is called the domain, $B$ the codomain, $\{y\in B:\exists x\in A(x,y)\in R\}$ is called the range.
- (Injection, surjection, bijection) A function $f:A\to B$ is injective if $\forall x\in A\forall y\in A(f(x)=f(y)\implies x=y)$, surjective if $\forall x\in B\exists y\in A(f(y)=x)$, bijective if $\forall x\in B\exists! y\in A(f(y)=x)$
- (General Power sets) $B^A$ means $\{R\in P(A\times B):\forall x\in A\exists! y\in B(x,y)\in R\}$, i.e. the set of functions from $A$ to $B$.
- (General Product sets) If $A$ is a set of sets, $\prod_{a\in A} a$ means $\{f\in(\bigcup_{a\in A})^A : \forall a\in A(f(a)\in a)\}$, called the product of elements in $A$.
- (Axiom of Choice) $\forall A(\emptyset\neq A\wedge\neg(\emptyset\in A)\implies \emptyset\neq\prod_{a\in A} a)$
- (Transfinite induction) Let $A$ be a predicate, then $\forall x(\forall y\in x(A(y))\implies A(x))\implies \forall x A(x)$
- (Identity function) $X$ is a set, the identity function $id_X\in X^X$ is defined as $\forall x\in X(id_X(x)=x)$, or $id_X=\{(x,y)\in X\times X: x=y\}$
- (Inclusion function) $Y\subseteq X$, the inclusion function from $Y$ to $X$ is $i_{Y\to x}\in X^Y$, $\forall x\in Y(i_{Y\to x}(x)=x)$
- (Composition) $f\in Y^X$, $g\in Z^Y$, their composition, denoted as $g\circ f$, is defined as $g\circ f(x)=g(f(x))$, or $g\circ f=\{(x,z)\in X\times Z:\exists y\in Y((x,y)\in f\wedge(y,z)\in g)\}$.
- (Restriction) $f\in Y^X$, $X'\subseteq X$, the restriction of $f$ on $X'$, denoted as $f|_{X'}$, is $f\circ i_{X'\to X}$.
- $Y^X$ is also written as $Map(X,Y)$.

## 3.3 Some examples of proofs in set theory

The steps in blue are straightforward use of the deduction rules and are there for the sake of clarification, you can omit lines like that in your proofs.

**Example 30** $\emptyset^\emptyset = \{\emptyset\}$
Proof:
By definition, $\emptyset^\emptyset = \{f \in P(\emptyset \times \emptyset) : \forall x \in \emptyset \exists! y \in \emptyset (x, y) \in f\}$.
$\emptyset \times \emptyset = \emptyset$
Hence $P(\emptyset \times \emptyset) = \{\emptyset\}$.
By the definition of empty set, $x \in \emptyset$ is always false.
Hence $\forall x((x \in \emptyset) \implies \exists! y \in \emptyset (x, y) \in \emptyset)$ is always true
Hence $\emptyset$ satisfies the predicate $\forall x \in \emptyset \exists! y \in \emptyset (x, y) \in f$, and should be a member of $\emptyset^\emptyset$.
Hence $\emptyset^\emptyset = \{\emptyset\}$.

**Example 31** $\forall A \forall B \forall C (A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C))$
Proof:
Suppose $x \in A \backslash (B \cap C)$
 Then $x \in A \wedge \neg x \in (B \cap C)$
 Hence $x \in A \wedge \neg (x \in B \wedge x \in C)$
 Hence $(x \in A \wedge \neg x \in B) \vee (x \in A \wedge \neg x \in C)$ (due to tautology $P \wedge \neg (Q \wedge R) \iff (P \wedge \neg Q) \vee (P \wedge \neg R)$
 This implies that $x \in (A \backslash B) \cup (A \backslash C)$
Hence $x \in A \backslash (B \cap C) \implies x \in (A \backslash B) \cup (A \backslash C)$
The proof that $x \in (A \backslash B) \cup (A \backslash C) \implies x \in A \backslash (B \cap C)$ is similar.
Hence $A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C)$
$\forall C (A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C))$
$\forall B \forall C (A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C))$
$\forall A \forall B \forall C (A \backslash (B \cap C) = (A \backslash B) \cup (A \backslash C))$

**Example 32** The function $f : \mathbb{N} \to \mathbb{N}$, defined as $f(x) = x^2$, is an injection.
Proof strategy: check the definition for injection for $f$.
Proof:

```
Suppose $x \in \mathbb{N}$
 Suppose $y \in \mathbb{N}$
  Suppose $f(x) = f(y)$
   Then $x^2 = y^2$
   Suppose $x \neq y$
    Then $x < y \vee y < x$
    If $x < y$
     $x \geq 0 \wedge y > 0$
     Hence $x^2 \leq xy < y^2$
     Contradiction.
    Similarly, $y < x$ also leads to contradiction.
   Hence $x = y$
  Hence $f(x) = f(y) \implies x = y$
 Hence $y \in \mathbb{N} \implies f(x) = f(y) \implies x = y$
 $\forall y \in \mathbb{N} f(x) = f(y) \implies x = y$
$x \in \mathbb{N} \implies \forall y \in \mathbb{N} f(x) = f(y) \implies x = y$
```

$\forall x \in \mathbb{N} \forall y \in \mathbb{N} f(x) = f(y) \implies x = y$

Hence $f$ is an injection.

**Example 33** $\forall X \forall Y \forall f \in Y^X \forall x \in X \forall y \in X (x = y \implies f(x) = f(y))$

Remark: this is showing that set theoretic functions have similar properties as the functions in logic.

Proof:

Suppose $f \in Y^X$

Then $\forall x \in X \exists ! z \in Y (x, z) \in f$ (definition of function)

Suppose $x \in X$

Suppose $y \in X$

Then $\exists z \in Y ((x, z) \in f)$ (due to the second line)

Let $z \in Y$ satisfy $(x, z) \in f$, i.e. $z = f(x)$

Then $\exists w \in Y ((y, w) \in f)$ (due to the second line)

Let $w \in Y$ satisfy $(y, w) \in f$, i.e. $w = f(y)$

Then $(x, w) \in f$ (because $x = y$)

Hence $z = w$ (due to the "uniqueness" part in the second line)

Hence $f(x) = f(y)$

$\forall X \forall Y \forall f \in Y^X \forall x \in X \forall y \in X (x = y \implies f(x) = f(y))$ (use $\implies$ and $\forall$ rules 3 times, then $\forall$ rule twice, as in the last two examples)

**Example 34** (Currying) $\forall X \forall Y \forall Z \exists c \in ((Z^Y)^X)^{Z^{X \times Y}}$ ($c$ is a bijection )

Proof:

Define $c$ as $g = c(f) \iff \forall x \in X \forall y \in Y (f(x, y) = (g(x))(y))$

First we show that $\forall f \in Z^{X \times Y} \exists g \in (Z^Y)^X (g = c(f))$:

Suppose $f \in Z^{X \times Y}$

Suppose $x \in X$

Suppose $y \in Y$

$\exists ! z \in Z (f(x, y) = z)$ (because $f$ is a function from $X \times Y$ to $Z$)

$\forall y \in Y \exists ! z \in Z (f(x, y) = z)$

$f_x$ defined as $f_x(y) = f(x, y)$ is a function from $Y$ to $Z$

Because $f_x$ is defined using $f$ and $x$, it is unique as long as $f$ and $x$ are both fixed

$g(x) = f_x$ is a function from $X$ to $Z^Y$

$\forall f \in Z^{X \times Y} \exists g \in (Z^Y)^X (g = c(f))$

Next we show the uniqueness of $c(f)$:

Suppose $\forall x \in X \forall y \in Y (f(x, y) = (g(x))(y)) \wedge \forall x \in X \forall y \in Y (f(x, y) = (g'(x))(y))$

Suppose $x \in X$

Suppose $y \in Y$

$(g(x))(y) = f(x, y) = (g'(x))(y)$

$g(x) = g'(x)$ (because two sets are identical iff their members are identical)

$g = g'$

Next we show that $c$ is an injection:

Suppose $c(f) = c(f')$

Suppose $(x, y) \in X \times Y$
$f(x, y) = (c(f)(x))(y) = (c(f')(x))(y) = f'(x, y)$
Hence $f = f'$
Lastly we show that $c$ is a surjection:
Suppose $g \in (Z^Y)^X$
Let $f(x, y) = (g(x))(y)$
Then $g = c(f)$ by the definition of $c$
Hence $c$ is indeed a bijection.

**Example 35** $\forall X \forall Y \forall f \in Y^X(f \text{ is an injection } \implies \exists g \in Range(f)^X(g \text{ is a bijection} \wedge f = i_{Range(f) \to Y} \circ g$
Proof:
Let $g : X \to Range(f)$ be defined as $g(x) = f(x)$
Then $g$ is injection because $f$ is an injection
$g$ is a surjection because $Range(f) = \{y \in Y : \exists x \in X(y = f(x))\}$
And if $x \in X$, then $i_{Range(f) \to Y} \circ g(x) = i_{Range(f) \to Y}(g(x)) = i_{Range(f) \to Y}(f(x)) = f(x)$
(Here I skipped the tedious checks for being a function, for injectivity and for surjectivity as in the previous example, as those are straightforward use of the quantifier rules and the definition of function/injection/surjection)

## 3.4 More examples of proofs

Notations in set theory:

- Cartesian product, power, union
- Function, injection, surjection, composition, inclusion, identity
- $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{C}$

Note that "definitions of sets" are actually assumptions, which are eliminated in the end because of the set building axioms.

**Example 36** There is no function from $\mathbb{N}$ to $\mathbb{N}$ that sends $x$ to $x - 2$ ($\neg \exists f \in Map(\mathbb{N}, \mathbb{N}) \forall x \in \mathbb{N}(x = f(x) + 2)$)
Proof:
Suppose $\exists f \in Map(\mathbb{N}, \mathbb{N}) \forall x \in \mathbb{N}(x = f(x) + 2)$
Let $f$ satisfy $f \in Map(\mathbb{N}, \mathbb{N}) \wedge \forall x \in \mathbb{N}(x = f(x) + 2)$
Hence $\forall x \in \mathbb{N} \exists y \in \mathbb{N}(y = f(x))$
Hence $\exists y \in \mathbb{N}(y = f(1))$
Let $y$ satisfy $y \in \mathbb{N} \wedge y = f(1)$
Then $1 = y + 2$, contradiction. Hence $\neg \exists f \in Map(\mathbb{N}, \mathbb{N}) \forall x \in \mathbb{N}(x = f(x) + 2)$

**Example 37** There is a surjection from $P(\mathbb{N})$ to $\mathbb{N}$ $(\exists f \in Map(P(\mathbb{N},\mathbb{N}))(\forall x \in \mathbb{N}\exists y \in P(\mathbb{N})f(y)=x))$
Proof:
Let $f(x) = \begin{cases} 0 & x=\emptyset \\ m & m \in x \wedge \forall y \in x(y \geq m) \end{cases}$
Suppose $x \in P(\mathbb{N})$
If $x = \emptyset$
From the definition above, $f(x)=0$
$\exists! y(f(x)=y)$
If $x \neq \emptyset$
Then $\exists m \in \mathbb{N}(m \in x \wedge \forall y \in x(m \leq y))$ Let $m$ satisfy $(m \in x \wedge \forall y \in x(m \leq y))$
Suppose $m'$ also satisfy $(m' \in x \wedge \forall y \in x(m' \leq y))$
Then $m \leq m' \wedge m' \leq m$
Hence $m = m'$
$\exists! y(f(x)=y)$
Hence $f$ is a function.
Assume $x \in \mathbb{N}$
$f(\{x\}) = x$
Hence $f$ is a surjection.
The Example is proved.

**Example 38** $\exists S \in P(N)(0 \notin S \wedge \forall a \in S \forall b \in S(a<b \implies \exists m \in \mathbb{N} b = 2^m a))$
Proof:
Let $S = \{x \in \mathbb{N} : \exists m \in \mathbb{N} x = 2^m\}$
Suppose $m \in \mathbb{N}$
$2^m > 0$
Hence $0 \notin S$
Suppose $a \in S$
Suppose $b \in S$
Suppose $a < b$
Let $a = 2^m$
Let $b = 2^n$
Then $m < n$
$b = 2^{n-m}a$
Hence $\forall a \in S \forall b \in S(a < b \implies \exists m \in \mathbb{N} b = 2^m a)$
Hence $\exists S \in P(N)(0 \notin S \wedge \forall a \in S \forall b \in S(a<b \implies \exists m \in \mathbb{N} b = 2^m a))$

**Example 39** $\forall X(X \neq \emptyset \implies \exists f \in X^{P(X)} \forall x \in X \exists y \in P(X)(f(y)=x))$
Proof:
Assume $X \neq \emptyset$
Let $a$ satisfy $a \in X$

Let $f \in X^{P(X)}$ be $f(y) = \begin{cases} x & y = \{x\} \\ a & otherwise \end{cases}$
Suppose $x \in X$
Then $f(\{x\}) = x$
Hence $\forall x \in X \exists y \in P(X)(f(y) = x))$
$\forall X(X \neq \emptyset \implies \exists f \in X^{P(X)} \forall x \in X \exists y \in P(X)(f(y) = x))$

**Example 40** $\exists S \in P(\mathbb{N}) \forall a \in S \forall b \in S \exists k \in S(a = b + 2k \vee b = a + 2k)$
Proof:
Let $S = \{x \in \mathbb{N} : \exists k \in \mathbb{N} x = 2k\}$
Suppose $a \in S$
Suppose $b \in S$
Let $m$, $n$ satisfies $m \in \mathbb{N}$, $n \in \mathbb{N}$, $a = 2m$, $b = 2n$
If $m \leq n$
$b = a + 2(n - m) \wedge n - m \in \mathbb{N}$
If $m > n$
$a = b + 2(m - n) \wedge m - n \in \mathbb{N}$
Hence $\exists S \in P(\mathbb{N}) \forall a \in S \forall b \in S \exists k \in S(a = b + 2k \vee b = a + 2k)$

## 3.5 Cardinality

When $S$ is a finite set (there is a bijection from $S$ to some set of the form $\{n \in \mathbb{N} : n < M\}$), $\|S\|$ means the number of elements in $S$.

In general, $\|A\| = \|B\|$ iff there is bijection between $A$ and $B$, $\|A\| \leq \|B\|$ iff there is an injection from $A$ to $B$, or there is a surjection from $B$ to $A$.

Example 39 shows that $\|X\| \leq \|P(X)\|$.

**Example 41** (Cantor's theorem) There is no surjection from $X$ to $P(X)$. In other words, $\|P(X)\| > \|X\|$.
Proof:
Suppose otherwise, let $f$ be such an surjection.
Let $S = \{x \in X : x \notin f(x)\}$
Let $y \in X$ satisfies $f(y) = S$
Then $y \in f(y) \wedge y \notin f(y)$
Contradiction
Hence there is no surjection from $X$ to $P(X)$.

**Example 42** For any natural number $n$, there is no surjection from $\{x \in \mathbb{N} : x < n\}$ to $\{x \in \mathbb{N} : x < n + 1\}$
Proof:
Suppose otherwise

Let $m$ be the smallest natural number where there is such a surjection
Let $f$ be such a surjection
$m > 0$, because there is no surjection from $\emptyset$ to $\{0\}$.
If $f(m-1) = m$, then $g(x) = \begin{cases} 0 & f(x) = m \\ f(x) & otherwise \end{cases}$
If $f(m-1) < m$, let $a$ satisfies $f(a) = m$, then $g(x) = \begin{cases} f(m-1) & x = a \\ 0 & x \neq a \wedge f(x) = m \\ f(x) & otherwise \end{cases}$
In either case, $g$ is a surjection from $\{x \in \mathbb{N} : x < m-1\}$ to $\{x \in \mathbb{N} : x < m\}$
Contradiction.
Hence Example 42 is proved.

### 3.6 Equivalence class

A relation $R \subset X \times X$ is an equivalence relation if $(\forall x \in X (x,x) \in R) \wedge (\forall x \in X \forall y \in X (x,y) \in R \iff (y,x) \in R) \wedge (\forall x \in X \forall y \in X \forall z \in X((x,y) \in R \wedge (y,z) \in R \to (x,z) \in R))$

$id_X$ is an equivalence relation.

If $R$ is an equivalence relation, $X/R$ is defined as $\{S \in P(X) : \exists x \in X \forall y \in X((y \in S \iff (x,y) \in R)\}$. The elements in $X/R$ are called equivalence classes.

**Example 43** $R = \{(x,y) \in \mathbb{N} \times \mathbb{N} : 3|(x-y)\}$ is an equivalence relation. The proof is obvious.

**Example 44** $\bigcup X/R = X$
Proof:
Suppose $x \in \bigcup X/R$
Then $\exists C \in X/R(x \in C)$
Let $C$ be such an element in $X/R$ such that $x \in C$
Then $x \in X$ because $C \subset X$
Suppose $x \in X$
Then $[x] = \{y \in X : (x,y) \in R\} \in X/R$
Hence $x \in \bigcup X/R$

**Example 45** $\forall x \in X/R \forall y \in X/R(x = y \vee x \cap y = \emptyset)$
Proof:
Suppose $x = [a] \in X/R, y = [b] \in X/R, x \cap y \neq \emptyset$
Let $c \in x \cap y$
Then $(a,c) \in R$, $(b,c) \in R$

Hence $(a, b) \in R$

Suppose $z \in x$

Then $(a, z) \in R$

Hence $(b, z) \in R$

Hence $z \in y$

Hence $x \subseteq y$

Similarly, $y \subseteq x$

Hence $x = y$

$\forall x \in X/R \forall y \in X/R(x = y \vee x \cap y = \emptyset)$

## 3.7 Indcutively defined functions

**Example 46** $\exists f \in Map(\mathbb{N}, \mathbb{N})(f(0) = 1 \wedge \forall x \in \mathbb{N} f(x + 1) = (x + 1)f(x))$

Proof idea: define the value of $f$ on natural numbers one by one. In other words, create a number of "partially defined functions" and "glue" them together.

Proof:

Let $A = \{g \in P(\mathbb{N} \times \mathbb{N}) : (\forall y \in \mathbb{N}((0, y) \in g \iff y = 1)) \wedge (\forall x \in \mathbb{N} \forall y \in \mathbb{N}((x + 1, y) \in g \implies (\exists x \in \mathbb{N}((x, z) \in g) \wedge y = (x + 1)z)))\}$

Let $f = \bigcup A$

Now we show that $f$ is a function $(\forall x \in \mathbb{N} \exists! y \in \mathbb{N}(x, y) \in f)$ by induction on $x$

The case when $x = 0$ is because all elements $g$ in $A$ satisfies $\forall y \in \mathbb{N}(0, y) \in g \iff y = 1$

Suppose $\exists! y \in \mathbb{N}(x, y) \in f$

Let $y$ satisfies $(x, y) \in f$

Then because $f = \bigcup A$, there is some $g \in A$ such that $(x, y) \in g$

Let $g \in A \wedge (x, y) \in g$

Then $g \cup (x + 1, (x + 1)y) \in A$

Hence $\exists y \in \mathbb{N}(x + 1, y) \in f$

Suppose $(x + 1, z) \in f$

There is some $h \in A$, such that $(x + 1, z) \in h$

There is some $y' \in \mathbb{N}$ such that $(x, y') \in h \subset f$ and $z = (x + 1)y'$

The uniqueness of $y$ such that $(x, y) \in f$ implies that $y = y'$, hence $z = (x+1)y$

Hence $\exists! y \in \mathbb{N}(x + 1, y) \in f$

By induction, $f$ is a function from $\mathbb{N}$ to $\mathbb{N}$.

The fact that $f$ satisfies the two other assumptions $(f(0) = 1 \wedge \forall x \in \mathbb{N} f(x+1) = (x + 1)f(x))$ is obvious.

## 3.8 Bijection and inverse

**Example 47** $\forall X \forall Y \forall f \in Map(X, Y)((\exists g \in Map(Y, X) g \circ f = id_X \wedge f \circ g = id_Y) \implies f \text{ is a bijection})$

Proof:

Suppose $f \in Map(X, Y)$

Suppose $\exists g \in Map(Y, X) g \circ f = id_X \wedge f \circ g = id_Y$

Let $g \in Map(Y, X)$ satisfies $g \circ f = id_X \wedge f \circ g = id_Y$

Suppose $x, x' \in X,\ f(x) = f(x')$
$x = g(f(x)) = g(f(x')) = x'$
Hence $f$ is an injection.
Suppose $y \in Y$
$f(g(y)) = y \wedge g(y) \in X$
Hence $\exists x \in X(g(x) = y)$, hence $f$ is a surjection.
The example follows.

## 3.9 Review

| | |
|---|---|
| $\neg$ | Not |
| $\wedge$ | And |
| $\vee$ | Or |
| $\implies$ | Implies, if.. then.. |
| $\iff$ | if and only if |
| $=$ | equals |
| $\forall$ | For all |
| $\exists$ | There exists |
| $\in$ | belongs to, is a member of |
| $\mathbb{N}$ | the set of natural numbers |
| $\mathbb{Z}$ | the set of integers |
| $\mathbb{Q}$ | the set of rational numbers |
| $\mathbb{R}$ | the set of real numbers |
| $\emptyset$ | the empty set |
| $A \subseteq B$ | $A$ is a subset of $B$ |
| $P(X)$ | the set of subsets of $X$, power set<br>$y \in P(X) \iff y \subseteq X$ |
| $X \times Y$ | Cartesian product of $A$ and $B$.<br>The set of pairs between elements in $A$ and elements in $B$. |
| $\{a \in A : \psi(a)\}$ | the subset of $A$ consisting of elements satisfying predicate $\psi$. |
| $f$ is a relation between $A$ and $B$ | $f \in P(A \times B)$ |
| $f : A \to B$<br>$f$ is a function from $A$ to $B$ | $f \in P(A \times B) \wedge \forall x \in A \exists! y \in B((x, y) \in f)$<br>$A$ is called the domain and $B$ the codomain.<br>To check two functions are identical, show that they are the same on their domain. |
| $X^Y, Map(Y, X)$ | the set of functions from $Y$ to $X$<br>$\{f \in P(Y \times X) : \forall y \in Y \exists! x \in X((y, x) \in f)\}$ |
| $\forall a \in A$ | $\forall a(a \in A \implies$ |
| $\exists a \in A$ | $\exists a(a \in A \wedge$ |
| $f : \mathbb{R} \to \mathbb{R}$<br>$f(x) = \begin{cases} x & x < 0 \\ 1 & x \geq 0 \end{cases}$ | $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} :$<br>$(x < 0 \wedge y = x) \vee (x \geq 0 \wedge y = 1)\}$ |
| $Range(f)$, where $f \in B^A$ | $\{b \in B : \exists a \in A(f(a) = b)\}$ |

| | |
|---|---|
| $f : A \to B$ is injective | $\forall x \in A \forall x' \in A(f(x) = f(x') \implies x = x')$ |
| $f : A \to B$ is surjective | $\forall y \in B \exists x \in A(f(x) = y)$ |
| $f : A \to B$ is bijective | $\forall y \in B \exists ! x \in A(f(x) = y)$ |
| $\bigcap A$ | $x \in \bigcap A \iff \forall a \in A(x \in a)$ |
| $\bigcup A$ | $x \in \bigcup A \iff \exists a \in A(x \in a)$ |
| $A \cup B$ | $x \in A \cup B \iff (x \in A \vee x \in B)$ |
| $A \cap B$ | $x \in A \cap B \iff (x \in A \wedge x \in B)$ |
| $A \backslash B$ | $x \in A \backslash B \iff (x \in A \wedge x \notin B)$ |
| $R$ is an equivalence Relation on $X$ | $R \subseteq X \times X \wedge (\forall x \in X((x, x) \in R))$ $(\forall x \in X \forall y \in X((x, y) \in R \implies (y, x) \in R) \wedge$ $(\forall x \in X \forall y \in X \forall z \in X((x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R)$ |
| $[x]$, or $[x]_R$ | $\{y \in X : (x, y) \in R\}$. Here $R$ is an equivalence relation |
| $X/R$ | $\{S \in P(X) : \exists x \in X(S = [x]_R)\}$ |
| $\Vert X \Vert$ | number of elements in $X$ |
| $id_X$ | $\{(x, y) \in X \times X : x = y\}$ |
| $i_{Y \to X}$, where $Y \subseteq X$ | $\{(a, b) \in Y \times X : a = b\}$ |
| $g \circ f$, where $f : X \to Y$ $g : Y \to Z$ | $\{(x, z) \in X \times Z : \exists y \in Y((x, y) \in f \wedge (y, z) \in g)\}$ |
| $f : X \to Y$, $g = f^{-1}$ | $g \circ f = id_X \wedge f \circ g = id_Y$ |

- In $B = \{a \in A : \psi(a)\}$, $a$ is a bounded variable. This sentence is the same as $\forall a(a \in B \iff (a \in A \wedge \psi(a)))$.
- Although we write the proofs into steps we seldom come up with these steps in the same order as we write them. Always think of a strategy first before doing the writing.
- All deduction steps must happen in your mind, though the more obvious ones don't need to be written down

**Example 48** : (universal property of empty set)

$\forall X(X = \emptyset \iff \forall Y(Map(X, Y) \neq \emptyset))$

Proof:

Suppose $X = \emptyset$

Let $f = \emptyset$

Then $\forall x \in X \exists ! y \in Y(x, y) \in f$

Hence $f \in Map(X, Y)$, $Map(X, Y) \neq \emptyset$

Suppose $\forall Y(Map(X, Y) \neq \emptyset)$

Then $Map(X, \emptyset) \neq \emptyset$

Let $f \in Map(X, \emptyset)$

Then $f \subset X \times \emptyset = \emptyset$

Hence $f = \emptyset$

Hence $\forall x \in X \exists ! y \in \emptyset(x, y) \in \emptyset$

i.e. $(\neg(x \in X) \vee \exists! y \in \emptyset (x,y) \in \emptyset$
Hence $\neg(x \in X)$ because $\exists! y \in \emptyset (x,y) \in \emptyset$ is false
$X = \emptyset$

**Example 49** : (Universal property of surjection)
$\forall X \forall Y \forall f \in Map(X,Y)(f \text{ is a surjection } \iff \forall Z \forall g, g' \in Map(Y,Z)(g \circ f = g' \circ f \implies g = g')$
Proof: will show $\implies$, the other direction left as exercise.
Suppose $f$ is a surjection
Suppose $g, g' \in Map(Y,Z)$, $g \circ f = g' \circ f$
Suppose $y \in Y$
Let $x \in X$ such that $f(x) = y$ (by the definition of surjection)
Hence $g(y) = g(f(x)) = g'(f(x)) = g'(y)$
Hence $\forall y \in Y(g(y) = g'(y))$
$g = g'$

Some other examples of universal properties:

- $f = id_X$ iff $\forall Y \forall g \in Map(X,Y)(g \circ f = g)$
- $f : X \to Y$ is injection iff $\forall Z \forall g, g' \in Map(Z,X)(f \circ g = f \circ g' \implies g = g')$
- $Z = X \times Y$, $\pi_1 : Z \to X$ is $\pi_1((a,b)) = a$, $\pi_2 : Z \to Y$ is $\pi_2((a,b)) = b$, then $\forall W \forall h_1 \in Map(W,X) \forall h_2 \in Map(W,Y) \exists! h \in Map(W,Z)(h_1 = \pi_1 \circ h \wedge h_2 = \pi_2 \circ h)$

These statement are important in math and have fairly simple proofs, so it might be a good idea to prove them by yourself if you have time!

**Example 50** (The Quotient function)
$R$ is an equivalence relation on $X$, let $q : X \to X/R$ be defined as $x \mapsto [x]$, then $R = \{(a,b) \in X \times X : q(a) = q(b)\}$.
Proof:
Assume that $R$ is an equivalence relation on $X$ and $q : X \to X/R$ is $q(x) = [x]$
Suppose $(a,b) \in R$
Suppose $c \in q(a) = [a]$
Then $(a,c) \in R$
Hence $(b,c) \in R$
Hence $c \in [b] = q(b)$
Similarly, $c \in q(b) \implies c \in q(a)$
Hence $q(a) = q(b)$
$(a,b) \in \{(a,b) \in X \times X : q(a) = q(b)\}$
If $(a,b) \in \{(a,b) \in X \times X : q(a) = q(b)\}$
Since $(b,b) \in R$, $b \in [b] = q(b) = q(a) = [a]$
Hence $(a,b) \in R$

**Example 51** Let $A = \{n \in \mathbb{N} : n < 10\}$. Are the following relations equivalence relations?

- $R_1 = \{(a, b) \in P(\mathbb{N}) \times P(\mathbb{N}) : a \cap b \neq \emptyset\}$
- $R_2 = \{(a, b) \in P(\mathbb{N}) \times P(\mathbb{N}) : a \cap A = b \cap A\}$

Three conditions to check:

- $\forall x \in P(\mathbb{N})((x, x) \in R)$
- $\forall x \in P(\mathbb{N}) \forall y \in P(\mathbb{N})((x, y) \in R \implies (y, x) \in R)$
- $\forall x \in P(\mathbb{N}) \forall y \in P(\mathbb{N}) \forall z \in P(\mathbb{N})((x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R)$

It is evident that $R_1$ is not an equivalence relation and $R_2$ is an equivalence relation.

# 4 Numbers and Proofs in Calculus

**This section will not appear in the final exam.**

## 4.1 Natural Numbers, Integers and Rationals

- Natural Numbers
  - The existence of the set $\mathbb{N}$ is mandated by the Axiom of Infinity.
  - Natural numbers can be represented by sets, e.g.: $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$, $\ldots$, $n + 1 = n \cup \{n\}$
- Integers
  - $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\{((a, b), (c, d)) \in (\mathbb{N} \times \mathbb{N}) \times (\mathbb{N} \times \mathbb{N}) : a + d = b + c\}$
  - $[(a, b)] + [(c, d)] = [(a + c, b + d)]$
  - $[(a, b)] - [(c, d)] = [(a + d, b + c)]$
  - $[(a, b)] \times [(c, d)] = [(ac + bd, ad + bc)]$
  - $[(a, b)] \geq 0 \iff a \geq b$
  - $|[(a, b)]| = \begin{cases} a - b & a \geq b \\ b - a & a < b \end{cases}$
  - $\mathbb{N}$ is identified with a subset of $\mathbb{Z}$ via $n \mapsto [(n, 0)]$
- Rationals
  - $\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z}\backslash\{0\}))/\{((a, b), (c, d)) \in (\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})) \times (\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})) : ad = bc\}$
  - $[(a, b)] + [(c, d)] = [(ad + bc, bd)]$
  - $[(a, b)] - [(c, d)] = [(ad - bc, bd)]$
  - $[(a, b)] \times [(c, d)] = [(ac, bd)]$
  - $[(a, b)]/[(c, d)] = [(ad, bc)]$ (when $c \neq 0$)
  - $[(a, b)] \geq 0 \iff ab \geq 0$
  - $|[(a, b)]| = [(|a|, |b|)]$
  - $\mathbb{Z}$ is identified with a subset of $\mathbb{Q}$ via $n \mapsto [(n, 1)]$

## 4.2 Cauchy sequence, Reals

- A sequence of rational numbers is a function from $\mathbb{N}$ to $\mathbb{Q}$, $n \mapsto a_n$, denoted as $\{a_n\}$. Note that this notation doesn't mean a set consisting of all the $a_n$.
- $\{a_n\}$ is a sequence of rational numbers, $\{n_i\}$ a sequence of natural numbers such that $i < j \implies n_i < n_j$, then the composition of the two functions $i \mapsto n_i$ and $n \mapsto a_n$ is called a subsequence, denoted as $\{a_{n_i}\}$.

- A sequence of rational numbers is a Cauchy sequence, if

$$\forall M \in (\mathbb{N}\backslash\{0\})\exists N \in \mathbb{N}\forall n \in \mathbb{N}\forall n' \in \mathbb{N}((n > N \wedge n' > N)$$
$$\implies (|a_n - a_{n'}| < 1/M))$$

- Two Cauchy sequences $\{a_n\}$ and $\{b_n\}$ are said to have the same limit, if

$$\forall M \in (\mathbb{N}\backslash\{0\})\exists N \in \mathbb{N}\forall n \in \mathbb{N}((n > N) \implies (|a_n - b_n| < 1/M))$$

- Let $\mathcal{C}$ be the set of Cauchy sequences of rational numbers.
- Let $\mathcal{R} = \{(\{a_n\}, \{b_n\}) \in \mathcal{C} \times \mathcal{C} : \{a_n\}, \{b_n\}$ have the same limit$\}$
- $\mathbb{R} = \mathcal{C}/\mathcal{R}$
- Arithmetic in $\mathbb{R}$ can be defined element-wise.
- The embedding of $\mathcal{Q}$ into $\mathcal{R}$ is defined via $q \mapsto \{q_n\}$, where $\forall n \in \mathbb{N}(q_n = q)$.

**Example 52** The sequence $\{\frac{a_n}{n+1}\}$, where $a_n > 0$, $a_n^2 < 2(n+1)^2 < (a_n+1)^2$, is a Cauchy sequence.
Proof idea:
Suppose $n \in \mathbb{N}, m \in \mathbb{N}$, then $\frac{a_n+1}{n+1} \geq \frac{a_m}{m+1}$, $\frac{a_m+1}{m+1} \geq \frac{a_n}{n+1}$.
If $\frac{a_n}{n+1} < \frac{a_m}{m+1}$, then $\frac{a_n}{n+1} < \frac{a_m}{m+1} < \frac{a_n+1}{n+1}$, hence $|\frac{a_n}{n+1} - \frac{a_m}{m+1}| < \frac{1}{n+1}$
If $\frac{a_n}{n+1} > \frac{a_m}{m+1}$, similarly we get $|\frac{a_n}{n+1} - \frac{a_m}{m+1}| < \frac{1}{m+1}$
Hence, in the definition of Cauchy sequence, we need only to set $N = M$.
Proof:
Suppose $M \in \mathbb{N}\backslash\{0\}$
Let $N = M$
Suppose $n \in \mathbb{N}$, $n' \in \mathbb{N}$, $n > N$, $m > N$
If $\frac{a_n}{n+1} < \frac{a_m}{m+1}$
By assumption on $a_n$, $(\frac{a_m}{m+1})^2 < 2 < (\frac{a_n+1}{n+1})^2$
Hence $\frac{|\frac{a_n}{n+1} - \frac{a_m}{m+1}| < \frac{a_n+1}{n+1}}{\frac{a_n}{n+1} = \frac{1}{n+1} < \frac{1}{M}}$
The case when $\frac{a_n}{n+1} > \frac{a_m}{m+1}$ is similar
Hence $\{\frac{a_n}{n+1}\}$ is a Cauchy sequence.
The real number represented by this Cauchy sequence is called $\sqrt{2}$.

One can prove various elementary properties of the real numbers (e.g. $\forall x \in \mathbb{R}(x^2 \geq 0)$, or the ones listed in Section 7.1 of the textbook) from this definition. The proofs are mostly straightforward and will not be covered due to time constraint.

## 4.3 Limit

$a_n$ is a sequence of real numbers. Let $\mathbb{R}^+ = \{r \in \mathbb{R} : r > 0\}$ We say $\lim_{n\to\infty} a_n = b$, if $\forall \epsilon \in \mathbb{R}^+ \exists N \in \mathbb{N} \forall n \in \mathbb{N} (n > N \implies |a_n - b| < \epsilon)$

Together with the definitions

$$e^x = \lim_{n\to\infty} \sum_{k=0}^{n} x^k/k!$$

$$e^{it} = \cos t + i \sin t$$

You can now prove almost everything in a calculus textbook, which is a good exercise.

# 5 Final review

## 5.1 Basic concepts

- **Proposition and predicate** Which of the following is a proposition, which of the following is a predicate?
  - $x$ is a natural number.
  - Any natural number is a real number.
  - The set of natural numbers larger than 5.
- **Free and bounded variables** In the following sentences, which variables are free and which are bounded? What are their scopes?
  - $\forall y \in \mathbb{N}((y|x) \implies (y = 1 \lor y = x))$
  - $f$ is a function from $\mathbb{R}$ to $\mathbb{Z}$ defined as $f(n) = \begin{cases} \sum_{i=0}^{n^2}(i!) & n^2 \in \mathbb{Z} \\ 0 & \text{otherwise} \end{cases}$
- **Implication and contradiction**
  - $A \implies B \iff (\neg A \lor B)$: Saying that "if you do well in the final exam you will get an A" is the same as saying "you will either do badly in the final exam, or you will get an A".
  - $(A \vdash \perp) \vdash \neg A$: If every positive integer is an even number, then for any positive integer $n$, $n/2$ is a smaller positive integer. Hence there isn't a smallest positive integer, which contradicts with the fact that 1 is the smallest positive integer, hence there are positive integers that are odd.
- **For all rules**
  - If one can prove predicate $A(x)$ without assumption on $x$, then we know $\forall x A(x)$:<br>Suppose $x \in \mathbb{R}$<br>Suppose $x < 0$<br>$x^2 = (-x)^2 > 0$<br>hence $\forall x \in \mathbb{R}((x < 0) \implies (x^2 > 0))$
  - If one knows $\forall x A(x)$, then $A(t)$ if $t$ is a term without bounded variables in $A$:<br>We know $\forall x \in \mathbb{R}(x^2 \geq 0)$.<br>Suppose $x \in \mathbb{R}$<br>$x + 1 \in \mathbb{R}$<br>hence $(x + 1)^2 \geq 0$
- **Exists rules**

  - If we can prove $A(t)$, where $t$ does not contain any bounded variable in $A$, then we get $\exists x A(x)$:
    Suppose $x \in \mathbb{R}$
    $x < x + 1$
    $x + 1 \in \mathbb{R}$
    hence $\exists y \in \mathbb{R}(x < y)$.
  - If we know $\exists x A(x)$, and assuming $A(x)$ we can get some sentence $B$ that doesn't depend on $x$, then $B$ is true.
    If a student does well in the final they will get A.
    Suppose there exists some students who do well in the final
    Let $x$ be a student who does well in the final
    Then $x$ gets A
    Hence there are students who get A.

- **Cartesian product** If $A$ is the set of all triangles and $B$ is the set of all circles, an element in $A \times B$ consists of a pair, the first entry being a triangle, the second a circle.

- **Power set** If there are 10 students in a class, let $S$ be the set of all students. How many elements are there in $P(S)$? If $a$ is a student in the class, is $a \in P(S)$ true?

- **Union and intersection** Let $S$ be the set of 10 students as above. What is $\bigcap P(S)$? What is $\bigcup P(S)$?

- **Specification** Let $S$ be the set of 10 students as above. What is $\{x \in P(S) : ||x|| = 2\}$ (here $|| \cdot ||$ is the cardinality)?

- **Function** Let $X$ consists of all the finite closed intervals in $\mathbb{R}$. For example, $[0, 1] \in X$. Let $f \subset X \times \mathbb{R}$ be $\{(a, b) \in X \times \mathbb{R} : a$ has length $b\}$. Then $f$ is a function. Is it an injection? Is it a surjection?

- **Equivalence relation** Let $X$ be the same as above. Let $R = \{(a, b) \in X \times X : a, b$ has the same length$\}$.

- **Quotient** Let $X$ and $R$ as above, what is $X/R$? Show that there is a bijection from $X/R$ to $\{x \in \mathbb{R} : x \geq 0\}$.

- **Induction** Three equivalent formats:
  - $\forall S \in P(\mathbb{N})((0 \in S \wedge \forall x \in \mathbb{N}(x \in S \implies (x + 1) \in S)) \implies S = \mathbb{N})$
  - $\forall S \in P(\mathbb{N})(\forall x \in \mathbb{N}(\forall y \in \mathbb{N}(y < x \implies y \in S) \implies x \in S) \implies S = \mathbb{N})$
  - $\forall S \in P(\mathbb{N})((S \neq \emptyset) \implies \exists! x \in \mathbb{N}(x \in S \wedge \forall y \in S(x \leq y)))$

Common mistakes in proof writing:

- Not indicating which sentences are assumptions, which sentences are comments.

- Not eliminating all assumptions:
  Prove that the Riemann Hypothesis is true.
  “Proof”:
  Suppose the Riemann Hypothesis is true
  Hence the Riemann Hypothesis is true, q.e.d.

- Using values where a proposition or a predicate is needed.
  Prove that P is not NP.
  “Proof”:
  Assume 42.
  P is not NP.

- Confusing $a \in S$ with $a \subset S$. There are sets for which $a \in S \implies a \subset S$ (find one), but $a \subset S \implies a \in S$ is never true.

## 5.2 Proofs

### 5.2.1 Steps for writing proofs

1. Understand the problem
2. Come up with an overall strategy
3. Fill in the gaps, write down the proof

### 5.2.2 Some common strategies for proofs

**Implication** To prove $A \implies B$, one can assume $A$, then prove $B$.
Prove that $\forall x \in \mathbb{N}(x > 2 \implies 2x > 4)$
Assume $x > 2$
 Then $2x > 4$
Hence $x > 2 \implies 2x > 4$
Hence $\forall x \in \mathbb{N}(x > 2 \implies 2x > 4)$

**Iff** To prove $A \iff B$, assume $A$ then prove $B$, assume $B$ then prove $A$.
Prove that $\forall x \in \mathbb{N}(x > 2 \iff 2x > 4)$
Assume $x > 2$
 Then $2x > 4$
Assume $2x > 4$
 Then $x > 2$
Hence $x > 2 \iff 2x > 4$
Hence $\forall x \in \mathbb{N}(x > 2 \iff 2x > 4)$

**Prove by cases** Enumerate all possible cases and prove the statement for each.
Prove that $\forall x \in \mathbb{N}(2|x(x+1))$
If $\exists y \in \mathbb{N}(x = 2y)$
 $x(x+1) = 2y(x+1)$

Hence $2|x(x+1)$
If $\exists y \in \mathbb{N}(x = 2y+1)$
$x(x+1) = 2x(y+1)$
Hence $2|x(x+1)$
Hence $\forall x \in \mathbb{N}(2|x(x+1))$

**Prove by contraposition** To prove $A \implies B$, prove $\neg B \implies \neg A$.
If it rains the street will be wet, hence, if the street is dry it is not currently raining.

**Prove by contradiction** To prove $A$, assume $\neg A$ and reach a contradiction. If a student does well in the exam you will get an A, and a student X did not get an A. Suppose the student X did well in the exam, then X gets an A, contradiction, so X didn't do well in the exam.

**Prove statements with quantifiers** To prove $\forall x A(x)$, either use the creation of $\forall$, or use prove by contradiction and the elimination of $\exists$. Similarly for $\exists x A(x)$.

**Prove by mathematical induction** Three formats:

**Example 53** Prove that $\forall f \in Map(\mathbb{N},\mathbb{N})(\forall x \in \mathbb{N}(f(x+1) > f(x)) \implies \forall x \in \mathbb{N}(f(x) \geq x))$

**Proof 1** Suppose $f \in Map(\mathbb{N},\mathbb{N})$
Suppose $\forall x \in \mathbb{N}(f(x+1) > f(x))$
Induction on $x$ to show $\forall x \in \mathbb{N}(f(x) \geq x)$
$f(0) \geq 0$ because $f(0) \in \mathbb{N}$
Suppose $f(x) \geq x$
$f(x+1) \geq f(x) + 1 \geq x + 1$
Hence by induction, $\forall x \in \mathbb{N}(f(x) \geq x)$
$\forall f \in Map(\mathbb{N},\mathbb{N})(\forall x \in \mathbb{N}(f(x+1) > f(x)) \implies \forall x \in \mathbb{N}(f(x) \geq x))$

**Proof 2** Suppose $f \in Map(\mathbb{N},\mathbb{N})$
Suppose $\forall x \in \mathbb{N}(f(x+1) > f(x))$
Induction on $x$ to show $\forall x \in \mathbb{N}(f(x) \geq x)$
$f(0) \geq 0$ because $f(0) \in \mathbb{N}$
Suppose $\forall y \in \mathbb{N}((y \leq x) \implies f(y) \geq y)$
Then $f(x) \leq x$
$f(x+1) \geq f(x) + 1 \geq x + 1$
Hence by induction, $\forall x \in \mathbb{N}(f(x) \geq x)$
$\forall f \in Map(\mathbb{N},\mathbb{N})(\forall x \in \mathbb{N}(f(x+1) > f(x)) \implies \forall x \in \mathbb{N}(f(x) \geq x))$

```
**Proof 3** Suppose $f \in Map(\mathbb{N},\mathbb{N})$
 Suppose $\forall x \in \mathbb{N}(f(x+1) > f(x))$
  Suppose $\exists x \in \mathbb{N}(f(x) < x)$
   Let $x$ be the smallest such natural number
   Then $x > 0$ as otherwise $f(x) < 0$
   Hence $f(x-1) \geq x-1$
   Hence $f(x) \leq f(x-1)$, contradiction.
$\forall f \in Map(\mathbb{N},\mathbb{N})(\forall x \in \mathbb{N}(f(x+1) > f(x)) \implies \forall x \in \mathbb{N}(f(x) \geq x))$
```

A proof usually make use of multiple strategies:

**Example 54** Prove that $\forall f \in Map(\mathbb{N},\mathbb{Z})(\forall x \in \mathbb{N}(f(x) > 0) \implies \exists x \in \mathbb{N}(f(x+1) \geq f(x)))$

Proof:

```
1. Suppose $\forall x \in \mathbb{N}(f(x+1) < f(x))$
2.  Prove by induction on $x$ that $\forall x \in \mathbb{N} f(x) \leq f(0) - x$
3.  $f(0) \leq f(0) - 0$
4.  Suppose $f(x) \leq f(0) - x$
5.    $f(x+1) < f(x)$
6.    Hence $f(x+1) \leq f(x) - 1 \leq f(0) - (x+1)$
7.  By induction, $\forall x \in \mathbb{N}(f(x) \leq f(0) - x)$
8.  If $f(0) < 0$
9.    Then $\exists x \in \mathbb{N}(f(x) \leq 0)$
10.  If $f(0) \geq 0)$
11.   Then $f(f(0)+1) < 0$
12.    Hence $\exists x \in \mathbb{N}(f(x) \leq 0)$
13. Hence $\forall x \in \mathbb{N}(f(x) > 0) \implies \exists x \in \mathbb{N}(f(x+1) \geq f(x))$
14. $\forall f \in Map(\mathbb{N},\mathbb{Z})(\forall x \in \mathbb{N}(f(x) > 0) \implies \exists x \in \mathbb{N}(f(x+1) \geq f(x)))$
```

- Line 13: Prove by contraposition
- Line 7: Prove by induction
- Lines 8-11: Prove by cases
- Line 12: Prove using the creation of $\exists$
- Line 14: Prove using the creation of $\forall$
- …

## 5.3 More Examples

**Example 55** $\forall f \in Map(\mathbb{N},\mathbb{R})((\forall M \in \mathbb{N}\backslash\{0\}\exists N \in \mathbb{N}\forall n \in \mathbb{N}((n > N) \implies (|f(n)| < 1/M))) \implies (\forall M' \in \mathbb{N}\backslash\{0\}\exists N' \in \mathbb{N}\forall n' \in \mathbb{N}((n' > N') \implies (|f(2^{n'})| < 1/M'))))$

Proof:

Suppose $f \in Map(\mathbb{N}, \mathbb{R})$
Suppose $\forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall n \in \mathbb{N}((n > N) \implies (|f(n)| < 1/M))$
Suppose $M' \in \mathbb{N}\backslash\{0\}$
Then $\exists N \in \mathbb{N} \forall n \in \mathbb{N}((n > N) \implies (|f(n)| < 1/M'))$
Let $N$ satisfies $N \in \mathbb{N}$ and $\forall n \in \mathbb{N}((n > N) \implies (|f(n)| < 1/M'))$
Suppose $n' \in \mathbb{N}$, $n' > N$
Then $2^{n'} > N$
Hence $|f(2^{n'})| < 1/M'$
Hence $\forall n' \in \mathbb{N}((n' > N) \implies (|f(2^{n'})| < 1/M'))$
Hence $\exists N' \in \mathbb{N}((n' > N') \implies (|f(2^{n'})| < 1/M'))$
Hence $\forall M' \in \mathbb{N}\backslash\{0\} \exists N' \in \mathbb{N} \forall n' \in \mathbb{N}((n' > N') \implies (|f(2^{n'})| < 1/M'))$
Hence $\forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall n \in \mathbb{N}((n > N) \implies (|f(n)| < 1/M))) \implies (\forall M' \in \mathbb{N}\backslash\{0\} \exists N' \in \mathbb{N} \forall n' \in \mathbb{N}((n' > N') \implies (|f(2^{n'})| < 1/M')))$
$\forall f \in Map(\mathbb{N}, \mathbb{R})((\forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall n \in \mathbb{N}((n > N) \implies (|f(n)| < 1/M))) \implies (\forall M' \in \mathbb{N}\backslash\{0\} \exists N' \in \mathbb{N} \forall n' \in \mathbb{N}((n' > N') \implies (|f(2^{n'})| < 1/M'))))$

**Example 56** $\emptyset \notin \{\{\emptyset\}\}$
Proof:
Suppose $\emptyset \in \{\{\emptyset\}\}$
Then $\emptyset = \{\emptyset\}$
However, $\emptyset \notin \emptyset$ but $\emptyset \in \{\emptyset\}$
Contradiction
Hence $\emptyset \notin \{\{\emptyset\}\}$

**Example 57** For any set $X$, the function $f : Map(\{0\}, X) \to X$ defined by $f(g) = g(0)$ is an injection
Proof:
Suppose $f$ is the function defined above.
Suppose $g, g' \in Map(\{0\}, X)$
Suppose $f(g) = f(g')$
Then $g(0) = g'(0)$
Suppose $(a, b) \in g$
Then $a \in \{0\}$
Hence $a = 0$
Hence $b = g(0)$
Hence $(a, b) \in g'$
Similarly, $(a, b) \in g' \implies (a, b) \in g$
Hence $g = g'$
$f$ is an injection.
The example is proved.

**Example 58** $\forall f \in Map(\mathbb{R}, \mathbb{R})(\forall a \in \mathbb{R} \forall b \in \mathbb{R}(f(a) = f(b)) \implies \exists c \in \mathbb{R} \forall d \in \mathbb{R}(f(c) = d))$
Proof:

Suppose $f \in Map(\mathbb{R}, \mathbb{R})$
Suppose $\forall a \in \mathbb{R} \forall b \in \mathbb{R}(f(a) = f(b))$
Then $\forall b \in \mathbb{R}(f(0) = f(b))$
Hence $\exists c \in \mathbb{R} \forall d \in \mathbb{R}(f(c) = d)$
$\forall f \in Map(\mathbb{R}, \mathbb{R})(\forall a \in \mathbb{R} \forall b \in \mathbb{R}(f(a) = f(b)) \implies \exists c \in \mathbb{R} \forall d \in \mathbb{R}(f(c) = d))$

**Example 59** $\forall A(A \in P(P(\emptyset)) \implies A \subset P(P(\emptyset)))$
Proof:
Suppose $A \in P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$
Then $A = \emptyset$ or $A = \{\emptyset\}$, both are subsets of $P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$
Hence $\forall A(A \in P(P(\emptyset)) \implies A \subset P(P(\emptyset)))$

**Example 60** $\forall n \in \mathbb{N} \forall m \in \mathbb{N}((m \leq n \wedge m > 0) \implies m|n!)$
Proof:
Induction on $n$.
$m \in \mathbb{N} \wedge m \leq 0 \wedge m > 0$ is always false
Hence $\forall m \in \mathbb{N}((m \leq 0 \wedge m > 0) \implies m|0!)$
Suppose $\forall m \in \mathbb{N}((m \leq n \wedge m > 0) \implies m|n!)$
Suppose $m \in \mathbb{N}$, $m \leq n+1$, and $m > 0$
Then $m = n+1 \vee m \leq n$
If $m = n+1$
$(n+1)! = (n+1)n!$
Hence $m|(n+1)!$
If $m \leq n$
$(n+1)! = (n+1)n!$
By inductive hypothesis, $m|n!$
Hence $m|(n+1)!$
Hence $\forall m \in \mathbb{N}((m \leq n+1 \wedge m > 0) \implies m|(n+1)!)$
By inductive hypothesis this is proved.

**Example 61** $\forall A \forall B(\exists! x(x \in B) \implies \exists! f(f \in Map(A, B)))$
Proof:
Suppose $\exists! x(x \in B)$
Let $x$ be such that $x \in B$
Then $f = \{(a, b) \in A \times B : b = x\} \in Map(A, B)$ (check the definition of function)
Suppose $g \in Map(A, B)$
Suppose $a \in A$
Then $g(a) \in B$
Hence $g(a) = x = f(a)$
Hence $\forall a \in A(g(a) = f(a))$
Hence $\exists! f(f \in Map(A, B)))$
$\forall A \forall B(\exists! x(x \in B) \implies \exists! f(f \in Map(A, B)))$

**Example 62** Let $Y : Map(\mathbb{R}\times\mathbb{R},\mathbb{R})\times Map(\mathbb{R},\mathbb{R} \to Map(\mathbb{R},\mathbb{R})$ be $(Y(f,g))(z) = f(z,g(z))$. What is $Y(+,\sin)$?
Answer: $x \mapsto x + \sin x$.

**Example 63** $A = \{0,1\}$, write down $Map(A,A)/\{(f,g) \in Map(A,A) \times Map(A,A) : \exists h \in Map(A,A), h \text{ is a bijection}, g = h \circ f \circ h^{-1}\}$.
Answer: $\{\{id_A\},\{\{(0,1),(1,0)\}\},\{\{(0,1),(1,1)\},\{(0,0),(1,0)\}\}\}$.

**Example 64** $f : \mathbb{N} \to P(\mathbb{Z})$ satisfies $f(0) = \{0\}$, $\forall n \in \mathbb{N}\forall y \in f(n+1)\exists z \in f(n)(y \leq z+1)$. Show that $\forall n \in \mathbb{N}\forall y \in f(n)(y \leq n)$.

```
Proof:
Induction on $n$
Suppose $y \in f(0) = \{0\}$
  Then $y = 0$
  Hence $y \leq 0$
$\forall y \in f(0)(y \leq 0)$
Suppose $\forall y \in f(n)(y \leq n)$
  Suppose $y \in f(n+1)$
    Then $\exists z \in f(n)(y \leq z+1)$
    Let $z$ satisfies $z \in f(n)$ and $y \leq z+1$
    Then by inductive hypothesis, $z \leq n$
    Hence $y \leq n+1$
The statement follows due to induction.
```

## 5.4 Further readings

- Textbooks on mathematical logic:
  - Ebbinghaus, Flum and Thomas, Mathematical Logic
  - William Weiss, Set Theory
- Other books about logic that might be of interest:
  - Douglas Hofstadter, Gödel, Escher, Bach
  - Friedman, Eastlund, The Little Prover
  - Alain Badiou, Being and Event

# 6 Solutions for all problems in midterm, homework and workshop

## 6.1 True or false

### 6.1.1 Exams and practice exams

**1** $(\forall x(f(g(x)) = x)) \implies (\forall x(g(f(x)) = x))$
False, for example, in $\mathbb{N}$, $g(x) = x + 1$, $f(x) = x - 1$ if $x > 0$ and 0 if otherwise.

**2** $\forall x \exists y(P(x, y) \wedge Q(y)) \iff \exists y Q(y) \wedge \forall x \exists y P(x, y)$
False, because the $y$ in $\exists y Q(y)$ and the $y$ in $\forall x \exists y P(x, y)$ are different.

**3** $\forall x \in \mathbb{N} \exists y \in \mathbb{N}(y < x \wedge x < y^2)$
False, for example if $x = 0$, then there isn't any such $y$.

**4** $\forall x \in \mathbb{N} \exists y \in \mathbb{N}(x^3 = x + y \wedge (x + 1)|y)$
True, $x^3 - x = x(x + 1)(x - 1)$.

**5** Let $X$ be any set. Is it true that the union of the elements in the power set of $X$ is $X$?
Yes.
Suppose $x \in \bigcup P(X)$
$\exists A \in P(X)(x \in A)$ by the definition of union.
Let $A \in P(X)$ such that $x \in A$
Then $A \subset X$
Hence $x \in X$
Suppose $x \in X$
$x \in \{x\}$, $\{x\} \in P(X)$
Hence $x \in \bigcup P(X)$.

**6** Let $z : \mathbb{R}^{\mathbb{R}} \to P(\mathbb{R})$ be $z(f) = \{x \in \mathbb{R} : f(x) = 0\}$. Is $z$ an injection? Is $z$ a surjection?
Idea of the answer: $z$ is a function that sends every real-valued function over $\mathbb{R}$ to the set of its zeroes. It is evident that this is a surjection but not an injection.
Answer:
$z$ is not an injection, because if $f_1(x) = 2x$, $f_2(x) = 3x$, then $z(f_1) = z(f_2) = \{0\}$.
$z$ is a surjection, because if $S \subset \mathbb{R}$, let $f_S(x) = \begin{cases} 0 & x \in S \\ 1 & otherwise \end{cases}$. Then $z(f_s) = S$.

**7** $\forall f \in Map(\mathbb{N}, \mathbb{N})((\forall x \in \mathbb{N} f(x + 1) = (x + 1)f(x)) \implies \forall x \in \mathbb{N}(f(x) = x!))$
False, for example $f(x) = 0$ is also possible.

**8** $\forall n \in \mathbb{N} \forall S((S \subseteq \{y \in \mathbb{N} : y < n\} \wedge S \neq \emptyset) \implies \exists! m \in \mathbb{N}(m \in S \wedge \forall z \in \mathbb{N}(z \in S \implies z \leq m)))$
True. Any finite sets of natural numbers has a maximum.

**9** For any natural number $n$, the set $\{x \in \mathbb{N} : x^2 > n\}$ has a smallest element.
True. Any non empty set of natural numbers has a minimum.

**10** $\emptyset \in Map(\{\emptyset\}, \{\emptyset\})$
False by the definition of function.

**11** $\forall f \in Map(\{0,1\}, \{0,1\})(f \circ f = id_{\{0,1\}} \implies f = id_{\{0,1\}})$ False, $f$ can also be $0 \mapsto 1$, $1 \mapsto 0$.

### 6.1.2 Homework

**12** One of the following "proofs" in predicate logic is incorrect. Find the incorrect one and point out the line number of the step where there is a logical mistake.
*Proposition 1:* $\exists x \forall y P(x,y) \implies \forall y \exists x P(x,y)$
*Proof:*

1. Assume that $\exists x \forall y P(x,y)$.
2. Let $z$ be such that $\forall y P(z,y)$.
3. This assumption implies that the predicate $P(z,y)$, where $y$ is the free variable, must be always true.
4. Hence $\exists x P(x,y)$ is always true.
5. Because $y$ is a free variable in this predicate, $\forall y \exists x P(x,y)$ is true.
6. This shows that $\exists x \forall y P(x,y) \implies \forall y \exists x P(x,y)$.

*Proposition 2:* $\forall x \exists y P(x,y) \implies \exists y \forall x P(x,y)$
*Proof:*

1. Assume that $\forall x \exists y P(x,y)$.
2. This implies the predicate $\exists y P(x,y)$ is always true.
3. Suppose $P(x,z)$ is true for some $z$.
4. We must have $\forall x P(x,z)$.
5. Hence $\exists y \forall x P(x,y)$.
6. This shows that $\forall x \exists y P(x,y) \implies \exists y \forall x P(x,y)$.

Answer: The 3rd line of proposition 2 can not imply the 4th line, because $x$ is not arbitrary as in the 3rd line it is assumed that $x$ must satisfy $P(x,z)$.

**13** $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(x^2 + 2y = y^2 + 2x \implies x = y)$
For any natural numbers $x$ and $y$, if $x^2 + 2y = y^2 + 2x$ then $x = y$. This is false because for example if $x = 0$, $y = 2$.

**14** $\forall x \in \mathbb{N} \forall y \in \mathbb{N} \forall z \in \mathbb{N}(x = yz \implies (x \leq y^2 \vee x \leq z^2))$
If a natural number can be written as the product of two other numbers, it is no larger than the square of one of these two numbers. This is true.

**15** $(\exists x(A(x) \vee B(x))) \implies (\exists x A(x) \vee \exists x B(x))$.
If some $x$ satisfy predicate $A$ or $B$, then either there is some $x$ that satisfy $A$, or there is some $x$ that satisfy $B$. This is true (a tautology).

**16** $((\forall x P(x)) \implies Q) \implies ((\exists x \neg P(x)) \implies \neg Q)$
False. If everyone in the class get $B$ then the average grade will be $B$, but it doesn't follow that if some people get above or below $B$ the average can never be $B$.

**17** $(\forall x \exists y(P(x) \implies Q(y))) \implies (\exists y Q(y) \vee \forall x \neg P(x))$.
True.

### 6.1.3 Workshop

**18** 3 is an integer but not an even number
If $x$ is an integer, then $x$ is even implies $3x$ is even
Hence, if $X$ is an integer, then $x$ is not even implies $3x$ is not even
So $9 = 3 \times 3$ is not even
The conclusion is correct but the deduction is invalid. The third line doesn't follow from the second.

**19** For any integer $x$, $x^2$ can not be negative
Suppose $y^2 = -1$
Suppose $y$ is an integer
$y^2$ is not negative due to the first line of the deduction, but $y^2$ is negative due to assumption
Contradiction
Hence $y$ can not be an integer
So $y^2 = -1 \implies y$ is not an integer
This is a valid argument.

**20** $\forall x \exists y f(y) = x$
Let $z$ be such a $y$
Then $\forall x f(z) = x$
Answer: This is not valid. The "$\exists$" in $\exists y$ is not the first quantifier in the first line, hence it is not allowed to replace $y$ with $z$.

## 6.2 Tests on basic concepts

### 6.2.1 Exams and practice exams

**1** Find three functions $f, g, h$ from $\mathbb{R}$ to $\mathbb{R}$, such that $f$ is a bijection, $g$ is a injection but not a surjection, $h$ a surjection but not an injection, and $f \cap g \cap h = \emptyset$. Justify your answer.
Answer:
$f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : x = y\}$
$g = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = \arctan(x)\}$
$h = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = x^3 - x - 1\}$
The "justification" will not be graded very strictly.
$f$ is an injection because suppose $f(x) = f(y)$, because $f(x) = x$, $f(y) = y$, we have $x = y$
$f$ is a surjection because if $x \in \mathbb{R}$, $f(x) = x$, hence $\forall x \in \mathbb{R} \exists y \in \mathbb{R} f(y) = x$.
$g$ is an injection because the derivative of $g$ is greater than 0, hence mean value theorem implies that if $x \neq x'$, $g(x) \neq g(x')$.
$g$ is a not a surjection because $\arctan(x) < \pi/2$, hence $\nexists y \in \mathbb{R} g(y) = 3$.
$h$ is a surjection because of intermediate value theorem and the fact that $\lim_{x\to\infty} h(x) = \infty$, $\lim_{x\to-\infty} h(x) = -\infty$.
$h$ is not an injection because $h(0) = h(1) = 0$

**2** How many equivalence relations are there in the set $\{0, 1, 2\}$?
Answer: 5. $id_{\{0,1,2\}}$, $\{0, 1, 2\} \times \{0, 1, 2\}$, $id_{\{0,1,2\}} \cup \{(0, 1), (1, 0)\}$, $id_{\{0,1,2\}} \cup \{(0, 2), (2, 0)\}$, $id_{\{0,1,2\}} \cup \{(2, 1), (1, 2)\}$.

**3** Let $A = \{z \in \mathbb{N} : z < 10\}$. Let $R = \{(a, b) \in A \times A : \exists n \in \mathbb{N}(a = 2^n b \vee b = 2^n a)\}$. Write down the elements in $A/R$ (in other words, write down all equivalence classes in $A$ under $R$)
Answer: $\{0\}, \{1, 2, 4, 8\}, \{3, 6\}, \{5\}, \{7\}, \{9\}$

### 6.2.2 Homework

**4** What is $\emptyset^{(\emptyset^{(\emptyset^{\emptyset})})}$?
Answer: $\{\emptyset\}$.

**5** Write down:

- a relation which is not a function
- a function which is not a surjection
- a surjection which is not a bijection.

Answer: If $A = \{0, 1, 2\}$, $B = \{0, 1\}$. $A \times B$ is not a function. $\{(0, 1), (1, 1), (2, 1)\}$ is a function that is not a surjection, and $\{(0, 0), (1, 1), (2, 1)\}$ is a surjection that is not a bijection.

### 6.2.3 Workshop

**6** Write down the elements of the following sets: $P(P(P(\emptyset)))$, $\emptyset^{P(\emptyset)}$, $P(\emptyset)^{P(P(\emptyset))}$, $P(\emptyset) \times P(P(\emptyset))$.
Answer:
$P(P(P(\emptyset))) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$.
$\emptyset^{P(\emptyset)} = \emptyset$.
$P(\emptyset)^{P(P(\emptyset))} = \{\{(\emptyset, \emptyset), (\{\emptyset\}, \emptyset)\}\}$.
$P(\emptyset) \times P(P(\emptyset)) = \{(\emptyset, \emptyset), (\emptyset, \{\emptyset\})\}$.

**7** Let $X = \{1, 2\}$. How many elements are there in the set $\cup_{f \in X^X} f$?
Answer: $\cup_{f \in X^X} f = X \times X$ and has 4 elements.

**8** Write down two different equivalence relations $R_1$, $R_2$ in the set $A = \{0, 1, 2\}$, and the set $A/R_1$, $A/R_2$.
Answer: $R_1 = id_A$, $R_2 = id_A \cup \{(0, 1), (1, 0)\}$. $A/R_1 = \{\{0\}, \{1\}, \{2\}\}$, $A/R_2 = \{\{0, 1\}, \{2\}\}$.

**9** Write down two different bijections from $A$ to $A$, for the same $A$ in problem 1.
Answer: $f_1 = id_A$, $f_2 = \{(0, 1), (1, 0), (2, 2)\}$

**10** Let $f : \mathbb{Z} \to \mathbb{Z}$ be $f(x) = x+3$. Let $S = \{R \in P(\mathbb{Z}\times\mathbb{Z}) : R$ is an equivalence relation$\wedge$ $f \subseteq R\}$, $R_0 = \bigcap S$. What is $R_0$? How many elements are there in $\mathbb{Z}/R_0$?
Answer:
It is easy to see that $R' = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : 3|(x - y)\}$ is an equivalence relation and it contains $f$. Hence $R_0 \subset R'$. We need to show $R' \subset R_0$, or $\forall R \in S(R' \subset R)$.
$R' = \bigcup\{R^i\}$, where $R^i = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : y = x + 3i\}$, and $i$ is chosen among all integers.
One needs only to show that $\forall R \in S \forall i \in \mathbb{N}(R^i \in R \wedge R^{-i} \in R)$
Suppose $R \in S$
We will show $\forall i \in \mathbb{N}(R^i \in R \wedge R^{-i} \in R)$ by induction on $i$:
$R^0 = id_{\mathbb{Z}} \subset R$, because $R$ is an equivalence relation hence must contain identity (Because according to the definition of equivalence relation, $\forall x \in \mathbb{Z}((x, x) \in R)$)
Suppose $R^i \subset R$
Suppose $(a, b) \in R^{i+1}$
Then $(a, b - 3) \in R^i \subset R$, $(b - 3, b) \in f \subset R$
Hence $(a, b) \in R$
Suppose $R^{-i} \subset R$
Suppose $(a, b) \in R^{-i-1}$
Then $(a, b + 3) \in R^{-i} \subset R$, $(b, b + 3) \in f \subset R$
Hence $(a, b) \in R$
By induction, $\forall i \in \mathbb{N}(R^i \in R \wedge R^{-i} \in R)$
Hence $R' = R_0$, $\mathbb{Z}/R_0$ would have three elements due to remainder theorem.

**11** Let $A = \{n \in \mathbb{Z} : n^2 = 1\}$.

- Write down the elements of $A$.
- Write down the elements of $P(A)$.
- Write down the elements of $Map(A, A)$.
- Write down the elements of $id_A$.
- Write down the elements of $\{f \in Map(Map(A, A), A) : f(id_A) = 1\}$

Answer:

- $A = \{-1, 1\}$
- $P(A) = \{\emptyset, \{-1\}, \{1\}, \{-1, 1\}\}$
- $Map(A, A) = \{\{(-1, -1), (1, 1)\}, \{(-1, 1), (1, 1)\}, \{(-1, -1), (1, -1)\}, \{(-1, 1), (1, -1)\}\}$
- $id_A = \{(-1, -1), (1, 1)\}$
-

$$\begin{gathered}\{f \in Map(Map(A, A), A) : f(id_A) = 1\} = \\ \{\{(\{(-1,-1),(1,1)\},1),(\{(-1,1),(1,1)\},1),(\{(-1,-1),(1,-1)\},1),(\{(-1,1),(1,-1)\},1)\}, \\ \{(\{(-1,-1),(1,1)\},1),(\{(-1,1),(1,1)\},1),(\{(-1,-1),(1,-1)\},1),(\{(-1,1),(1,-1)\},-1)\}, \\ \{(\{(-1,-1),(1,1)\},1),(\{(-1,1),(1,1)\},1),(\{(-1,-1),(1,-1)\},-1),(\{(-1,1),(1,-1)\},1)\}, \\ \{(\{(-1,-1),(1,1)\},1),(\{(-1,1),(1,1)\},-1),(\{(-1,-1),(1,-1)\},1),(\{(-1,1),(1,-1)\},1)\}, \\ \{(\{(-1,-1),(1,1)\},1),(\{(-1,1),(1,1)\},-1),(\{(-1,-1),(1,-1)\},-1),(\{(-1,1),(1,-1)\},1)\}, \\ \{(\{(-1,-1),(1,1)\},1),(\{(-1,1),(1,1)\},1),(\{(-1,-1),(1,-1)\},-1),(\{(-1,1),(1,-1)\},-1)\}, \\ \{(\{(-1,-1),(1,1)\},1),(\{(-1,1),(1,1)\},-1),(\{(-1,-1),(1,-1)\},1),(\{(-1,1),(1,-1)\},-1)\}, \\ \{(\{(-1,-1),(1,1)\},1),(\{(-1,1),(1,1)\},-1),(\{(-1,-1),(1,-1)\},-1),(\{(-1,1),(1,-1)\},-1)\}\}\end{gathered}$$

**12** A function $g \in Map(\mathbb{N}, P(\mathbb{N})$ satisfies $g(0) = \emptyset$, $\forall n \in \mathbb{N}(g(n+1) = g(n) \cup \{m \in \mathbb{N} : n^2 < m \wedge m < (n+1)^2\})$. What is $g(3)$?
Answer: $g(3) = \{2, 3, 5, 6, 7, 8\}$.

## 6.3 Proofs

### 6.3.1 Exams and practice exams

**1** $(\forall y \neg(f(y) = y)) \implies \exists x \exists y(\neg(x = y))$
Proof:
Assume $(\forall y \neg(f(y) = y))$
$\neg(f(x) = x)$ (replace bounded variable $y$ with free variable $x$)
$\exists y \neg(x = y)$ (replace $f(x)$ with $y$, $\exists$ rule)
$\exists x \exists y(\neg(x = y))$
Hence $(\forall y \neg(f(y) = y)) \implies \exists x \exists y(\neg(x = y))$

**2** $(\exists x \forall y (f(y) = x)) \implies (\forall x \forall y (f(x) = f(y)))$

Proof:

Assume $\exists x \forall y (f(y) = x)$

Let $z$ satisfy $\forall y (f(y) = z)$

$f(y) = z$

$f(x) = z$

$f(x) = f(y)$

$\forall x \forall y (f(x) = f(y))$

Hence $(\exists x \forall y (f(y) = x)) \implies (\forall x \forall y (f(x) = f(y)))$

**3** $\forall x \in \mathbb{N} \forall y \in \mathbb{N} (x^3 = y \implies \exists z \in \mathbb{N} (y = x + 2z))$

Proof:

If $x = 0$

$x = 0 \leq 0 = x^3 = y$

If $x \geq 1$

$x = x \times 1 \times 1 \leq x^3 = y$

Hence $\forall x \in \mathbb{N} (x \leq x^3)$

Suppose $x^3 = y$

$x$ is even or odd

If $x$ is even

Let $c$ satisfy $x = 2c$

Let $d$ satisfy $c^3 = c + d$

Then $y = 8c^3 = x + 2(3c + 4d)$

$\exists z \in \mathbb{N} (y = x + 2z)$

If $x$ is odd

Let $c$ satisfy $x = 2c + 1$

Let $d$ satisfy $c^3 = c + d$

Then $y = 8c^3 + 12c^2 + 6c + 1 = x + 2(3c + 4d + 6c^2 + 3c)$

$\exists z \in \mathbb{N} (y = x + 2z)$

Hence $\forall x \in \mathbb{N} \forall y \in \mathbb{N} (x^3 = y \implies \exists z \in \mathbb{N} (y = x + 2z))$

The first 4 lines can be removed because $\forall x \in \mathbb{N} (x \leq x^3)$ is fairly obvious.

**4** $\exists c \in \mathbb{N} \forall n \in \mathbb{N} (3n \leq 2^n + c)$

Proof:

Induction on $n$ to show $3n \leq 2^n + 2$

$3 \times 0 = 0 \leq 3 = 2^0 + 2$

Suppose $3n \leq 2^n + 2$

Suppose $n \geq 2$

$3(n + 1) = 3n + 3 \leq 3n + 2^n \leq 2^n + 2 + 2^n = 2^{n+1} + 2$

Suppose $n = 0$

$3 \leq 4 = 2^1 + 2$

Suppose $n = 1$

$6 \leq 6 = 2^2 + 2$

Hence $3(n + 1) \leq 2^{n+1} + 2$ is true in all cases

By induction, $\forall n (3n \leq 2^n + 2)$

$\exists c \forall n (3n \leq 2^n + c)$

**5** $\forall x \in \mathbb{N}(f(x+1) = (x+1)f(x)) \implies \forall x \in \mathbb{N}(f(x) = x! \times f(0))$
Proof:
Assume $\forall x \in \mathbb{N}(f(x+1) = (x+1)f(x))$
Induction on $x$ to show that $\forall x \in \mathbb{N}(f(x) = x! \times f(0))$
$f(0) = 1 \times f(0) = 0!f(0)$
Suppose $f(x) = x!f(0)$
$f(x+1) = (x+1)f(x) = (x+1)x!f(0) = (x+1)!f(0)$
By induction, $\forall x \in \mathbb{N}(f(x) = x! \times f(0))$
$\forall x \in \mathbb{N}(f(x+1) = (x+1)f(x)) \implies \forall x \in \mathbb{N}(f(x) = x! \times f(0))$

**6** If $f : \mathbb{N} \to \mathbb{N}$ is a surjection, show that there is a subset $S$ of $\mathbb{N}$ such that $f \circ i_{S \to \mathbb{N}}$ is a bijection.
Proof:
Let $f : \mathbb{N} \to \mathbb{N}$ be a surjection
Let $S = \{x \in \mathbb{N} : \forall y \in \mathbb{N}(y < x \implies f(y) \neq f(x))\}$
First we show that $f \circ i_{S \to \mathbb{N}}$ is a surjection.
Suppose $x \in \mathbb{N}$
Surjectivity of $f$ implies that $\exists y \in \mathbb{N}(f(y) = x)$
Let $m$ be the smallest such $y$
The minimality of $m$ means that $z < m \implies f(z) \neq x = f(m)$ for all $z \in \mathbb{N}$
$m \in S$
Hence $f \circ i_{S \to \mathbb{N}}(m) = f(m) = x$
Now we show that $f \circ i_{S \to \mathbb{N}}$ is an injection.
Suppose $a \in S \wedge b \in S \wedge f \circ i_{S \to \mathbb{N}}(a) = f \circ i_{S \to \mathbb{N}}(b)$
Then $f(a) = f(b)$
Suppose $a < b$
Then $a < b \wedge f(a) = f(b)$
Then $b \notin S$
Contradiction
Similarly, $b < a$ will also lead to contradiction
Hence $a = b$.

**7** Show that there is an injection from $P(\mathbb{N})$ to $\{f \in \mathbb{N}^{\mathbb{N}} : f \text{ is an injection }\}$.
Hint: show that if $f : \mathbb{N} \to \mathbb{N}$ is a function, then $n \mapsto \sum_{i=0}^{n} f(i) + n$ is an injection.
Proof:
Suppose $f : \mathbb{N} \to \mathbb{N}$ is a function.
Suppose $n, n' \in \mathbb{N}$, $\sum_{i=0}^{n} f(i) + n = \sum_{i=0}^{n'} f(i) + n'$
Suppose $n < n'$
Then $\sum_{i=0}^{n} f(i) \leq \sum_{i=0}^{n'} f(i)$
Hence $\sum_{i=0}^{n} f(i) + n < \sum_{i=0}^{n'} f(i) + n'$
Contradiction.
Similarly, $n' < n$ will also lead to contradiction.

$n = n'$
$\sum_{i=0}^{n'} f(i) + n' \in \{f \in \mathbb{N}^{\mathbb{N}} : f \text{ is an injection }\}$
Let $c : P(\mathbb{N}) \to \mathbb{N}^{\mathbb{N}}$ be $c(S)(x) = \begin{cases} 1 & x \in S \\ 0 & x \notin S \end{cases}$.
Let $d : \mathbb{N}^{\mathbb{N}} \to \{f \in \mathbb{N}^{\mathbb{N}} : f \text{ is an injection }\}$ be $d(f)(n) = \sum_{i=0}^{n} f(i) + n$
Let $e = d \circ c$.
Suppose $e(S) = e(S')$
Suppose $x \in S$
If $x = 0$
$1 = c(S)(0) = e(S)(0) = e(S')(0) = c(S')(0)$
Hence $0 \in S'$.
If $x > 0$
Then $1 = c(S)(x) = e(S)(x) - e(S)(x-1) - 1 = e(S')(x) - e(S')(x-1) - 1 = c(S')(x)$
Hence $x \in S'$
Hence $\forall x(x \in S \implies x \in S')$
Similarly, $\forall x(x \in S' \implies x \in S)$
Hence $S = S'$.

Alternatively, with the concept of cardinality, you can simplify the proof as below:
Let $e : P(\mathbb{N}) \to \{f \in \mathbb{N}^{\mathbb{N}} : f \text{ is an injection }\}$ be $(e(S))(n) = \|\{z \in \mathbb{N} : z \leq n \wedge z \in S\}\| + n$.
First we show $e(S) \in \{f \in \mathbb{N}^{\mathbb{N}} : f \text{ is an injection }\}$, which shows that $e$ is well defined.
Suppose $e(S)(n) = e(S)(n')$
If $n < n'$
$\{z \in \mathbb{N} : z \leq n \wedge z \in S\} \subseteq \{z \in \mathbb{N} : z \leq n' \wedge z \in S\}$
Hence $\|\{z \in \mathbb{N} : z \leq n \wedge z \in S\}\| \leq \|\{z \in \mathbb{N} : z \leq n' \wedge z \in S\}\|$
Hence $e(S)(n) < e(S)(n')$, a contradiction.
Similarly, $n' < n$ will lead to contradiction, hence $n = n'$
Next we show that $e$ is an injection.
Suppose $e(S) = e(S')$
Suppose $x \in S$
If $x = 0$
$1 = \|\{0\}\| = \|\{z \in \mathbb{N} : z \leq 0 \wedge z \in S\}\| = e(S)(0) = e(S')(0) = 1$
$0 \in \{z \in \mathbb{N} : z \leq n \wedge z \in S'\}$, hence $0 \in S$.
If $x > 0$
$1 = \|\{x\}\| = \|\{z \in \mathbb{N} : z \leq x \wedge z \in S\} \backslash \{z \in \mathbb{N} : z \leq x-1 \wedge z \in S\}\| = \|\{z \in \mathbb{N} : z \leq x \wedge z \in S\}\| - \|\{z \in \mathbb{N} : z \leq x-1 \wedge z \in S\}\| = e(S)(x) - e(S)(x-1) - 1 = e(S')(x) - e(S')(x-1) - 1 = \|\{z \in \mathbb{N} : z \leq x \wedge z \in S'\}\| - \|\{z \in \mathbb{N} : z \leq x-1 \wedge z \in S'\}\| = \|\{z \in \mathbb{N} : z \leq x \wedge z \in S'\} \backslash \{z \in \mathbb{N} : z \leq x-1 \wedge z \in S'\}\|$
Hence $x \in S'$
Similarly, $x \in S' \implies x \in S$
Hence $S = S'$

**8** Prove that $m = \{(a, b) \in (P(\mathbb{N})\backslash\{\emptyset\}) \times \mathbb{Z} : b + 1 \in a \wedge (\forall c \in \mathbb{N}(c \in a \implies b < c))\}$ is a function.
Idea of the answer: $m$ is a function from $P(\mathbb{N})\backslash\{\emptyset\}$ to $\mathbb{Z}$, that sends every subset $a$ of $\mathbb{N}$ that is non empty to an integer $b$, such that $b+1$ is the smallest element in $a$. This is evidently a function. To show it we need to check the definition of function.
Answer:
Suppose $a \in P(\mathbb{N})\backslash\{\emptyset\}$
Then $\exists n \in \mathbb{N}(n \in a)$ (because the elements of $a$ are in $\mathbb{N}$, and $a$ has at least one element)
Let $e$ be the smallest natural number such that $e \in a$ (we learned before midterm 1, that if a predicate for natural numbers is true for some number, it must be true for a smallest number).
Then $e \in a \wedge \forall c \in \mathbb{N}(c \in a \implies e \leq c)$ (this is what "smallest" mean)
Hence $(e - 1) + 1 \in a \wedge \forall c \in \mathbb{N}(c \in a \implies e - 1 \leq c)$
$\exists b \in \mathbb{Z}((a, b) \in m)$ ($\exists$ rule, replace $e - 1$ with $b$. This finishes the "existence" part of the proof.)
Suppose $(a, b) \in m \wedge (a, b') \in m$
Then $b+1 \in a \wedge b'+1 \in a$, and $\forall c \in \mathbb{N}(c \in a \implies b < c) \wedge \forall d \in \mathbb{N}(d \in a \implies b' < d)$
Hence $b < b'+1$, $b' < b+1$ ($\forall$ rule, replace $c$, $d$ with $b'+1$, $b+1$ respectively)
Hence $b = b'$
Hence $\forall a \in P(\mathbb{N})\backslash\{\emptyset\}\exists! b \in \mathbb{Z}((a, b) \in m)$, i.e. $m$ is a function.

**9** Prove that $\forall S \in P(\mathbb{N})\forall T \in P(\mathbb{N})((\forall n \in \mathbb{N}(\{z \in \mathbb{N} : z < n\} \cap S = \{z \in \mathbb{N} : z < n\} \cap T)) \implies S = T)$
Idea of the answer: This is asking you to show that if two sets of natural numbers are different, they differ at some number that is smaller than some natural number $n$ (you see that by taking the contrapositive).
Answer:
Assume that $S \in P(\mathbb{N})$, $T \in P(\mathbb{N})$
Assume $x \in S$
$x \in \{z \in \mathbb{N} : z < x + 1\}$
Hence $x \in \{z \in \mathbb{N} : z < x + 1\} \cap S$
Hence $x \in \{z \in \mathbb{N} : z < x + 1\} \cap T$
Hence $x \in T$
Hence $x \in S \implies x \in T$
Similarly, one can show $x \in T \implies x \in S$
Hence $\forall S \in P(\mathbb{N})\forall T \in P(\mathbb{N})((\forall n \in \mathbb{N}(\{z \in \mathbb{N} : z < n\} \cap S = \{z \in \mathbb{N} : z < n\} \cap T)) \implies S = T)$

**10** Let $C$ be the set consisting of bijections from $A$ to $B$, $D$ be the set consisting of bijections from $B$ to $A$. Show that there is a bijection from $C$ to $D$. Hint: you may divide your proof into the following steps:

(i) For any $f \in C$, show that $\{(b, a) \in B \times A : b = f(a)\} \in D$. This means that $H(f) = \{(b, a) \in B \times A : b = f(a)\}$ is a function from $C$ to $D$.

(ii) Show that the $H$ defined above is an injection.

(iii) Show that the $H$ defined above is a surjection.

Answer: (You do not need to provide as much details)
Suppose $C, D$ and $H$ are as defined in the problem
(i)
Suppose $f \in C$
Let $g = \{(b, a) \in B \times A : (a, b) \in f\}$
Suppose $b \in B$
$\exists! a \in A((a, b) \in f)$ (because $f$ is a bijection)
Hence $\exists! a \in A((b, a) \in g)$
Hence $g$ is a function
Suppose $a \in A$
$\exists! b \in B((a, b) \in f)$ (because $f$ is a function)
Hence $\exists! b \in B((b, a) \in g)$
Hence $g$ is a bijection, $g \in D$
This shows that $H$ is a function
(ii)
Suppose $f, f' \in C$, $H(f) = H(f')$
Suppose $(a, b) \in f$
Then $(b, a) \in H(f) = H(f')$
Hence $(a, b) \in f'$
Hence $(a, b) \in f \implies (a, b) \in f'$
Similarly, one can show that $(a, b) \in f' \implies (a, b) \in f$
Hence $f = f'$
Hence $H$ is an injection
(iii)
Suppose $g \in D$
Due to the same argument in (i), $f = \{(a, b) \in A \times B : (b, a) \in g\} \in C$
Furthermore, by the definition of $H$, $H(f) = g$
Hence $H$ is a surjection.
This proves the problem

**11** . Show that $R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a^2 + 4b = b^2 + 4a\}$ is an equivalence relation. In other words, show that:

(i) $\forall x \in \mathbb{N}((x, x) \in R)$

(ii) $\forall x \in \mathbb{N} \forall y \in \mathbb{N}((x, y) \in R \implies (y, x) \in R)$

(iii) $\forall x \in \mathbb{N} \forall y \in \mathbb{N} \forall z \in \mathbb{N}((x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R)$

Answer:
Let $R = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a^2 + 4b = b^2 + 4a\}$ (i)
Suppose $x \in \mathbb{N}$

$x^2 + 4x = x^2 + 4x$
Hence $(x, x) \in R$
$\forall x \in \mathbb{N}((x, x) \in R)$
(ii)
Suppose $x, y \in \mathbb{N}$
Suppose $(x, y) \in R$
Then $x^2 + 4y = y^2 + 4x$
Hence $y^2 + 4x = x^2 + 4y$
Hence $(y, x) \in R$
$\forall x \in \mathbb{N}\forall y \in \mathbb{N}((x, y) \in R \implies (y, x) \in R)$
(iii)
Suppose $x, y, z \in \mathbb{N}$
Suppose $(x, y) \in R$, $(y, z) \in R$
Then $x^2 + 4y = y^2 + 4x$, $y^2 + 4z = z^2 + 4y$
Hence $x^2 - 4x = y^2 - 4y$, $y^2 - 4y = z^2 - 4z$
Hence $x^2 - 4x = z^2 - 4z$
$x^2 + 4z = z^2 + 4x$
Hence $(x, z) \in R$
$\forall x \in \mathbb{N}\forall y \in \mathbb{N}\forall z \in \mathbb{N}((x, y) \in R \wedge (y, z) \in R \implies (x, z) \in R)$
Hence $R$ is an equivalence relation.

**12** Prove that there are two different functions from $\mathbb{N}$ to $\{0, 1\}$, i.e. $\exists f \in Map(\mathbb{N}, \{0, 1\})\exists g \in Map(\mathbb{N}, \{0, 1\})(f \neq g)$.
Proof: The functions $f_0 : x \mapsto 0$ and $f_1 : x \mapsto 1$ are distinct as $f_0(0) = 0 \neq 1 = f(1)$.

**13** Prove that $R = \{(a, b) \in \mathbb{Q} \times \mathbb{Q} : a = b \vee a - b \in \mathbb{Z}\}$ is an equivalence relation.
Proof: $a = b$ implies $a - b = 0 \in \mathbb{Z}$, hence $R = \{(a, b) \in \mathbb{Q} \times \mathbb{Q} : a - b \in \mathbb{Z}\}$. Suppose $a \in \mathbb{Q}$, then $a = a$ hence $(a, a) \in R$. Suppose $a, b \in \mathbb{Q}$ and $(a, b) \in R$, then $b - a = -(a - b) \in \mathbb{Z}$, hence $(b, a) \in R$. Suppose $(a, b) \in R$, $(b, c) \in R$, then $a - c = (a - b) + (b - c) \in \mathbb{Z}$, hence $(a, c) \in R$.

**14** Prove that $\exists c \in \mathbb{N}\forall n \in \mathbb{N}(\sum_{i=0}^{n}(i^2) \leq n^3 + c)$.
Proof: Induction on $n$ to show $\forall n \in \mathbb{N}(\sum_{i=0}^{n} i^2 \leq n^3)$. $\sum_{i=0}^{0} i^2 = 0^2 = 0^3$. Suppose $\sum_{i=0}^{n} i^2 \leq n^3$, $\sum_{i=0}^{n+1} i^2 \leq n^3 + (n + 1)^2 \leq (n + 1)^3$

**15** Show that the function $z \in Map(Map(\mathbb{N}, \mathbb{N}), \mathbb{N})$ defined by $z(f) = f(0)$ is a surjection. i.e. $\forall z(z = \{(a, b) \in Map(\mathbb{N}, \mathbb{N}) \times \mathbb{N} : b = a(0)\} \implies \forall y \in \mathbb{N}\exists x \in Map(\mathbb{N}, \mathbb{N})(z(x) = y))$.
Proof: Suppose $n \in \mathbb{N}$, then $f_n : x \mapsto n$ is a function in $Map(\mathbb{N}, \mathbb{N})$ and $z(f_n) = n$

**16** Let $S$ be the set of bijections from $\mathbb{N}$ to $\mathbb{N}$. Show that the intersection of all the elements of $S$ is empty. i.e. $\forall S(S = \{f \in P(\mathbb{N} \times \mathbb{N}) : \forall x \in \mathbb{N}\exists! y \in$

$\mathbb{N}((x,y) \in f) \land \forall y \in \mathbb{N}\exists! x \in \mathbb{N}((x,y) \in f)\} \implies \bigcap S = \emptyset)$.

Proof: Let $f = id_{\mathbb{N}}$, $g(n) = \begin{cases} 2y & n = 2y+1 \\ 2y+1 & n = 2y \end{cases}$, then $f, g \in S$, hence $\bigcap S \subset f \cap g = \emptyset$.

### 6.3.2 Homework

**17** $((\forall x(f(x) = g(x))) \land (\forall x \exists y f(y) = x)) \implies (\forall x \exists y g(y) = x)$

Proof:

Assume $(\forall x(f(x) = g(x))) \land (\forall x \exists y f(y) = x)$

Then $\forall x \exists y f(y) = x$

Hence $\exists y f(y) = x$

Let $z$ be such that $f(z) = x$

From the first assumption, we also have $\forall x(f(x) = g(x))$

Hence $f(z) = g(z)$

So $g(z) = x$

$\exists y g(y) = x$

By the rule on $\exists$, $\exists y g(y) = x$

Because $x$ is free, $\forall x \exists y g(y) = x$

So $(\forall x(f(x) = g(x))) \land (\forall x \exists y f(y) = x) \implies \forall x \exists y g(y) = x$

**18** $\exists x(A(x) \implies \forall y B(x,y)) \implies (\exists x \neg A(x)) \lor (\forall y \exists x B(x,y))$

Answer:

Assume $\exists x(A(x) \implies \forall y B(x,y))$

Let $z$ satisfy $A(z) \implies \forall y B(z,y)$

From the example $(P \implies Q) \iff (\neg P \lor Q)$, we have $\neg A(z) \lor \forall y B(z,y))$

Suppose $\neg A(z)$

$\exists x \neg A(x)$

$(\exists x \neg A(x)) \lor (\forall y \exists x B(x,y))$

Hence $\neg A(z) \implies (\exists x \neg A(x)) \lor (\forall y \exists x B(x,y))$

Suppose $\forall y B(z,y))$

$B(z,y)$

$\exists x B(x,y)$

$\forall y \exists x B(x,y)$

Hence $(\exists x \neg A(x)) \lor (\forall y \exists x B(x,y))$

Hence $\forall y B(z,y)) \implies (\exists x \neg A(x)) \lor (\forall y \exists x B(x,y))$

So we have $(\exists x \neg A(x)) \lor (\forall y \exists x B(x,y))$

By $\exists$ rule, $(\exists x \neg A(x)) \lor (\forall y \exists x B(x,y))$ is always true

Hence $\exists x(A(x) \implies \forall y B(x,y)) \implies (\exists x \neg A(x)) \lor (\forall y \exists x B(x,y))$

**19** . $\forall x \in \mathbb{N} \forall y \in \mathbb{N} \forall z \in \mathbb{N}(x + y < x + z \implies y < z)$

Proof:

Suppose $x + y < x + z$ [Assumption 1]

By definition, this implies $x + y \leq x + z \land x + y \neq x + z$ [Definition of $<$]

Hence $x + y \leq x + z$ [$A \land B \vdash A$]

Hence $\exists c \in \mathbb{N}(x+y)+c = x+z$ [Definition of $\leq$]
Let $c$ satisfy $(x+y)+c = x+z$ [Assumption 2]
Then $y+c = z$ [$a+(b+c) = (a+b)+c$, $a+b = a+c \implies b = c$]
So $\exists c \in \mathbb{N}y+c = z$ [$A(t) \vdash \exists x A(x)$]
Hence $y \leq z$ by definition. [Definition of $\leq$]
[Assumption 2 eliminated because $\exists x A(x), (A(x) \vdash B) \vdash B$]
Suppose $y = z$ [Assumption 3]
Then $x+y = x+z$, a contradicton. [$a = b \vdash f(a) = a(b)$]
Hence $y \neq z$ [Proof by contradiction, Assumption 3 eliminated]
Together with the prior conclusion that $y \leq z$, we have $y < z$ [Definition of $<$]
Hence $x+y < x+z \implies y < z$ [$(a \vdash b) \vdash a \implies b$]
Hence $\forall x \in \mathbb{N}\forall y \in \mathbb{N}\forall z \in \mathbb{N}(x+y < x+z \implies y < z)$. [$A(x) \vdash \forall x A(x)$, Assumption 1 eliminated]

**20** $\forall x \in \mathbb{N}(\exists y \in \mathbb{N}(x = 2y) \vee \exists y \in \mathbb{N}(x = 2y+1))$
Proof:
Induction on $x$ [Mathematical induction]
When $x$ is 0, $0 = 2 \times 0$, hence the predicate is true. [$\forall x \in \mathbb{N}x \times 0 = 0$]
Suppose $\exists y \in \mathbb{N}(x = 2y) \vee \exists y \in \mathbb{N}(x = 2y+1)$ [Assumption 1, Inductive hypothesis]
Suppose we are in the case when $\exists y \in \mathbb{N}(x = 2y)$ [Assumption 2]
Let $y$ satisfy $x = 2y$ [Assumption 3]
Then $x+1 = 2y+1$ [$a = b \vdash f(a) = f(b)$]
Hence $\exists y \in \mathbb{N}(x+1 = 2y+1)$ [$A(t) \vdash \exists x A(x)$]
Therefore, $\exists y \in \mathbb{N}(x = 2y) \vee \exists y \in \mathbb{N}(x = 2y+1)$ is true in this case [$A \vdash A \vee B$]
[Assumption 3 eliminated because $\exists x A(x), (A(x) \vdash B) \vdash B$]
Suppose we are in the case when $\exists y \in \mathbb{N}(x = 2y+1)$ [Assumption 4]
Let $y$ satisfy $x = 2y+1$ [Assumption 5]
Then $x+1 = 2y+1+1 = 2y+2 \times 1 = 2(y+1)$ [$a = b \vdash f(a) = f(b)$, $a = b, b = c \vdash a = c$, $ab+ac = a(b+c)$]
Hence $\exists y \in \mathbb{N}(x+1 = 2y)$ [$A(t) \vdash \exists x A(x)$]
Therefore, $\exists y \in \mathbb{N}(x = 2y) \vee \exists y \in \mathbb{N}(x = 2y+1)$ is true in this case. [$A \vdash A \vee B$]
[Assumption 5 eliminated because $\exists x A(x), (A(x) \vdash B) \vdash B$]
Hence $\exists y \in \mathbb{N}(x = 2y) \vee \exists y \in \mathbb{N}(x = 2y+1)$ [$A \vee B, (A \vdash C), (B \vdash C) \vdash C$, Assumption 2, Assumption 4 eliminated]
Hence by induction, $\forall x \in \mathbb{N}(\exists y \in \mathbb{N}(x = 2y) \vee \exists y \in \mathbb{N}(x = 2y+1))$ [Mathematical induction, Assumption 1 eliminated]

**21** $\forall x \in \mathbb{N}(\exists y \in \mathbb{N}(x \times x = 2y) \implies \exists z \in \mathbb{N}(x = 2z))$
Proof:
Copy the proof of Problem 20 here.
Here we add a proof that $\forall r \in \mathbb{N}2r \neq 1$ since we need to use it later
Induction on $r$ to show $\forall r \in \mathbb{N}2r \neq 1$ [Induction]
$2 \times 0 = 0 \neq 1$ [Definition of $\times$]

Suppose $2r \neq 1$ [Inductive hypothesis, Assumption A]

Suppose $2(r+1) = 1$ [Assumption B]

Then $2r + 1 = 0$ [$a(b+c) = ab + ac$]

Contradicts with the rule that says 0 is the first natural number.

Hence $2(r+1) \neq 1$ [Proof by contradiction, Assumption B eliminated]

Hence by induction, $\forall r \in \mathbb{N} 2r \neq 1$[Induction, Assumption 0 eliminated]

Suppose $\exists y \in \mathbb{N}(x \times x = 2y)$ [Assumption 1]

Let $z$ be this $y$, i.e. $x^2 = 2z$ [Assumption 2]

Suppose further, that $\neg \exists y \in \mathbb{N}(x = 2y)$ [Assumption 3]

By the result in Problem 2, $\exists y \in \mathbb{N}(x = 2y) \vee \exists y \in \mathbb{N}(x = 2y + 1)$ [$\forall x A(x) \vdash A(t)$]

Suppose we are in the case $\exists y \in \mathbb{N}(x = 2y)$ [Assumption 4]

There is a contradiction [$A, \neg A \vdash \perp$]

Hence $\exists y \in \mathbb{N}(x = 2y + 1)$ in this case. [$\perp \vdash A$]

Suppose we are in the other case, then we also have $\exists y \in \mathbb{N}(x = 2y + 1)$ [Assumption 5]

Hence $\exists y \in \mathbb{N}(x = 2y + 1)$ [$A \vee B, (A \vdash C), (B \vdash C) \vdash C$, Assumption 4, Assumption 5 eliminated]

Let $y$ satisfies $x = 2y + 1$ [Assumption 6]

Then $x^2 = (2y+1)^2 = 2(2y^2 + 2y) + 1$ [Various laws regarding + and ×]

Hence $\exists y \in \mathbb{N} x^2 = 2y$ [$A(t) \vdash \exists x A(x)$]

Let $w$ satisfy $x^2 = 2w$ [Assumption 7]

Then $2w = 2z + 1$ [$a = b, b = c \vdash a = c$]

Hence $2z \leq 2w$ [Definition of $\leq$]

Which implies $z \leq w$ [$ac \leq bc \wedge c \neq 0 \implies a \leq b$]

$\exists r \in \mathbb{N} w = z + r$ [Definition of $\leq$]

$2z + 2r = 2z + 1$, hence $2r = 1$ [$a(b+c) = ab + ac$, $a + c = b + c \implies a = b$]

However from earlier in the proof, $2r \neq 1$ [$\forall x A(x) \vdash A(t)$]

Contradiction [$A, \neg A \vdash \perp$]

[Assumption 7, Assumption 6 eliminated because $\exists x A(x), (A(x) \vdash B) \vdash B$]

Hence $\exists y \in \mathbb{N}(x = 2y)$ [Proof by contradiction, $\neg\neg A \vdash A$, Assumption 3 eliminated]

[Assumption 2 eliminated because $\exists x A(x), (A(x) \vdash B) \vdash B$]

In conclusion, $\forall x \in \mathbb{N}(\exists y \in \mathbb{N}(x \times x = 2y) \implies \exists z \in \mathbb{N}(x = 2z))$ [$(A \vdash B) \vdash A \implies B$, Assumption 1 eliminated]

**22** $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0)$

Proof:

Copy the proof of Problem 21 here.

We will use induction on $N$ to show $\forall N \in \mathbb{N} \forall x \in \mathbb{N}((x \leq N) \implies \forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0))$. [Induction]

Suppose $x \leq 0$ [Assumption 1]

$x = 0$

Assume $x^2 = 2y^2$ [Assumption 2]

$x = 0$

Hence $x^2 = 2y^2 \implies x = 0$ [Assumption 2 eliminated]

Hence $\forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$

$x \leq 0 \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$ [Assumption 1 eliminated]

$\forall x \in \mathbb{N}((x \leq 0) \implies \forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0))$

Now suppose $\forall x \in \mathbb{N}((x \leq N) \implies \forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0))$. [Assumption 3, inductive hypothesis]

Suppose $x \leq N + 1$ [Assumption 4]

$x = N + 1 \vee x \leq N$

Suppose we are in the case when $x \leq N$ [Assumption 5]

By inductive hypothesis, $(x \leq N) \implies \forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0)$

Hence $\forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0)$ is true in this case.

Suppose we are in the case when $x = N + 1$ [Assumption 6]

Further suppose $x \times x = 2y \times y$ [Assumption 7]

$\exists z \in \mathbb{N}(x^2 = 2z)$

$\exists x' \in \mathbb{N}(x = 2x')$ due to the result of Problem 3.

$4x'^2 = 2y^2$

Hence $y^2 = 2x'^2$

$\exists z \in \mathbb{N}(y^2 = 2z)$

$\exists y' \in \mathbb{N}(y = 2y')$

Let $x'$, $y'$ satisfy $x = 2x'$, $y = 2y'$ respectively. [Assumption 8, 9]

Then $x'^2 = 2y'^2$

Suppose $x' = N + 1$ [Assumption 10]

Then $x = 2x' = 2N + 2 > N + 1$

Contradiction

Hence $x' \leq N$ [Assumption 10 eliminated]

Hence $\forall y \in \mathbb{N}(x' \times x' = 2y \times y \implies x' = 0)$

$x'^2 = 2y^2 \implies x' = 0$

Hence $x' = 0$

$x = 2x' = 0$

[Assumption 9, 8 eliminated]

$x^2 = 2y^2 \implies x = 0$ [Assumption 7 eliminated]

Hence $\forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$ is true in this case.

Hence $\forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$ [Assumption 6, Assumption 5 eliminated]

$(x \leq N + 1) \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$ [Assumption 4 eliminated]

$\forall x \in \mathbb{N}(x \leq N + 1) \implies \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$

By induction, $\forall N \in \mathbb{N} \forall x \in \mathbb{N}((x \leq N) \implies \forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0))$ [Assumption 3 eliminated]

$\forall x \in \mathbb{N}((x \leq N) \implies \forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0))$

$(x \leq N) \implies \forall y \in \mathbb{N}(x \times x = 2y \times y \implies x = 0))$

$N \leq N$

Hence $\forall y \in \mathbb{N}(N \times N = 2y \times y \implies N = 0))$

Hence $\forall x \in \mathbb{N} \forall y \in \mathbb{N}(x^2 = 2y^2 \implies x = 0)$.

**23** $(\exists x(A(x) \implies B) \wedge \forall x A(x)) \implies B$.
Proof:
Suppose $\exists x(A(x) \implies B) \wedge \forall x A(x)$
 Then $\exists x(A(x) \implies B)$
 And $\forall x A(x)$
 Let $x$ satisfy $A(x) \implies B$
 Then $A(x)$ is true because $\forall x A(x)$
 Hence $B$
Hence $(\exists x(A(x) \implies B) \wedge \forall x A(x)) \implies B$.

**24** $\forall x \in \mathbb{N} \exists y \in \mathbb{N}(2y = x(x+1))$
You can use the fact that $x$ is either even or odd, or use induction as follows:
Proof:
Induction on $x$
$2 \times 0 = 0 \times (0+1)$
Hence $\exists y \in \mathbb{N}(2y = 0(0+1))$
Suppose $\exists y \in \mathbb{N}(2y = x(x+1))$
 Let $y$ satisfy $2y = x(x+1)$
 Then $(x+1)((x+1)+1) = x(x+1) + 2(x+1) = 2(y+x+1)$
 Hence $\exists y \in \mathbb{N}(2y = (x+1)((x+1)+1))$
Hence by induction, $\forall x \in \mathbb{N} \exists y \in \mathbb{N}(2y = x(x+1))$

**25** $\forall n \in \mathbb{N}(1 + \sum_{k=0}^{n} k \cdot k!) = (n+1)!$
Proof:
Induction on $n$
$1 + \sum_{k=0}^{0} 0 \cdot 0! = 1 = (0+1)!$
Suppose $1 + \sum_{k=0}^{n} k \cdot k! = (n+1)!$
 $1 + \sum_{k=0}^{n+1} k \cdot k! = (n+1)! + (n+1) \cdot (n+1)! = (n+2) \cdot (n+1)! = ((n+1)+1)!$
Hence by induction, $\forall n \in \mathbb{N}(1 + \sum_{k=0}^{n} k \cdot k!) = (n+1)!$

**26** $\forall x \in \mathbb{N} \exists y \in \mathbb{N} \forall z \in \mathbb{N}((y \leq z) \implies (x \leq z^2))$
Proof:
$x = 0 \vee 1 \leq x$
If $x = 0$
 $x \leq x^2$
If $1 \leq x$
 $x = 1 \times x \leq x \times x = x^2$
Hence $x \leq x^2$ is always true.
If $x \leq z$
 $x \leq x^2 \leq z^2$
Hence $(x \leq z) \implies (x \leq z^2)$
$\forall z \in \mathbb{N}(x \leq z) \implies (x \leq z^2)$
$\exists y \in \mathbb{N} \forall z \in \mathbb{N}(x \leq z) \implies (x \leq z^2)$ (replacing the first $x$ with $y$)
$\forall x \in \mathbb{N} \exists y \in \mathbb{N} \forall z \in \mathbb{N}((y \leq z) \implies (x \leq z^2))$

**27** $\forall n \in \mathbb{N} \exists y \in \mathbb{N}(n^2 = 4y \vee n^2 = 4y + 1)$
Proof:
From Problem 20 above, $\forall n \in \mathbb{N}(\exists y \in \mathbb{N}(n = 2y) \vee \exists y \in \mathbb{N}(n = 2y + 1))$
$\exists y \in \mathbb{N}(n = 2y) \vee \exists y \in \mathbb{N}(n = 2y + 1)$
Suppose $\exists y \in \mathbb{N}(n = 2y)$
 $n^2 = 4y^2$
 $n^2 = 4y^2 \vee n^2 = 4y^2 + 1$
 $\exists y \in \mathbb{N}(n^2 = 4y \vee n^2 = 4y + 1)$ (replace $y^2$ with $y$)
Suppose $\exists y \in \mathbb{N}(n = 2y + 1)$
 $n^2 = (2y + 1)^2 = 4(y^2 + y) + 1$
 $n^2 = 4(y^2 + y) \vee n^2 = 4(y^2 + y) + 1$
 $\exists y \in \mathbb{N}(n^2 = 4y \vee n^2 = 4y + 1)$ (replace $y^2 + y$ with $y$)
Hence $\exists y \in \mathbb{N}(n^2 = 4y \vee n^2 = 4y + 1)$ is always true.
$\forall n \in \mathbb{N} \exists y \in \mathbb{N}(n^2 = 4y \vee n^2 = 4y + 1)$

**28** Prove the following: $(f(0) = 1 \wedge f(1) = 1 \wedge \forall n \in \mathbb{N}(f(n + 2) = f(n) + f(n + 1))) \implies \forall n \in \mathbb{N} \exists z \in \mathbb{N}(f(3n + 2) = 2z)$. Hint: use induction.
Proof:
Suppose $f(0) = 1 \wedge f(1) = 1 \wedge \forall n \in \mathbb{N}(f(n + 2) = f(n) + f(n + 1))$
 Induction on $n$
 $f(2) = f(1) + f(0) = 1 + 1 = 2$
 Hence $\exists z \in \mathbb{N}(f(2) = 2z)$
 Suppose $\exists z \in \mathbb{N}(f(3n + 2) = 2z)$
  $f(3(n + 1) + 2) = f(3n + 4) + f(3n + 3) = f(3n + 2) + 2f(3n + 3)$
  Let $z$ satisfy $f(3n + 2) = 2z$
  Then $f(3(n + 1) + 2) = 2(z + f(3n + 3))$
  Hence $\exists z \in \mathbb{N}(f(3(n + 1) + 2) = 2z)$
 By induction, $\forall n \in \mathbb{N} \exists z \in \mathbb{N}(f(3n + 2) = 2z)$
Hence $(f(0) = 1 \wedge f(1) = 1 \wedge \forall n \in \mathbb{N}(f(n + 2) = f(n) + f(n + 1))) \implies \forall n \in \mathbb{N} \exists z \in \mathbb{N}(f(3n + 2) = 2z)$

**29** $\forall X \forall Y \forall f \in Y^X((f \text{ is an injection } \wedge X \neq \emptyset) \implies \exists g \in X^Y \forall x \in X(g(f(x)) = x))$ (Hint: try to construct one such $g$)
Answer: (throughout the proof you can replace $y = f(x)$ with $(x, y) \in f$ if you wish, but keep in mind that $y = f(x)$ means $(x, y) \in f$.)
Assume $f \in Y^X$
 Assume $f$ is an surjection, and $X \neq \emptyset$
  Let $a \in X$
  Let $g : Y \to X$ be $\{(y, x) \in Y \times X : (x, y) \in f \vee (x = a \wedge \neg \exists x \in X((x, y) \in f))\}$
  We now show that $g$ is a function:
  Let $y \in Y$
  If $\neg \exists x \in X((x, y) \in f)$
   Then $(x, y) \in f$ is always false
   Hence $(y, x) \in g \iff x = a$
   Hence $\exists! x \in X((y, x) \in g)$

If $\exists x \in X((x,y) \in f)$
Then $\neg\exists x(y = f(x))$ is false
Hence $(y,x) \in g \iff (x,y) \in f$
Let $x$ satisfies $(x,y) \in f$
Then $(y,x) \in g$
If $(y,x') \in g$ for some $x' \in X$
Then $(x',y) \in f \wedge (x,y) \in f$
Hence $x = x'$ because $f$ is an injection
Hence $g \in X^Y$.
Suppose $x \in X$
Let $y \in Y$ satisfies $(x,y) \in f$
Then $(y,x) \in g$
Hence $\forall x \in X(g(f(x)) = x)$
Hence $\forall X \forall Y \forall f \in Y^X((f \text{ is an injection } \wedge X \neq \emptyset) \implies \exists g \in X^Y \forall x \in X(g(f(x)) = x))$

**30** Show that there is a bijection between the power set of $\mathbb{R}$ and the set of functions from $\mathbb{R}$ to $\{0,1\}$.

Answer: Let $c : P(\mathbb{R}) \to \{0,1\}^{\mathbb{R}}$ be $(c(S))(x) = \begin{cases} 1 & x \in S \\ 0 & x \notin S \end{cases}$

It is evident that $c$ is a function. Now we show that it is both an injection and a surjection.
Suppose $S, S' \in P(\mathbb{R})$ such that $c(S) = c(S')$
Suppose $x \in S$
Then $1 = c(S)(x) = c(S')(x)$
Hence $x \in S'$
Similarly, $x \in S' \implies x \in S$
Hence $c$ is an injection.
Suppose $f \in \{0,1\}^{\mathbb{R}}$
Let $Z = \{x \in \mathbb{R} : f(x) = 1\} \in P(\mathbb{R})$
Suppose $x \in \mathbb{R}$
If $x \in Z$
$(c(Z))(x) = 1 = f(x)$
If $x \notin Z$
$(c(Z))(x) = 0 = f(x)$
Hence $c(Z) = f$
Hence $c$ is a surjection.

**31** Show that for any set $X$, there is a bijection from $X$ to $Map(\{0\}, X)$ defined by $x \mapsto \{(0,x)\}$.
Answer:
Let $H$ be $x \mapsto \{(0,x)\}$.
Suppose $x \in X$
Suppose $a \in \{0\}$

$a = 0$
$(a, x) \in \{(0, x)\}$
Hence $\exists y \in X((a, y) \in \{0, x\})$
Suppose $(a, y) \in \{(0, x)\}$
Then $(a, y) = (0, x)$
Hence $y = x$
Hence $\exists! y \in X((a, y) \in \{(0, x)\})$
Hence $\{(0, x)\} \in Map(\{0\}, X)$
Hence $\forall x \in X \exists! f \in Map(\{0\}, X)(f = H(x))$
Hence $H$ is a function.
Suppose $x, x' \in X$
Suppose $H(x) = H(x')$
Then $\{(0, x)\} = \{(0, x')\}$
Hence $(0, x) = (0, x')$
$x = x'$
Hence $H$ is an injection.
Suppose $f \in Map(\{0\}, X)$
Suppose $a \in \{0\}$
Then $a = 0$
$H(f(0))(0) = f(0)$
Hence $f = H(f(0))$
Hence $H$ is a surjection.

### 6.3.3 Workshop

**32** $(\forall x(f(g(x)) = x)) \implies \forall x \exists y(f(y) = x)$
Answer:
Assume $\forall x(f(g(x)) = x)$
Then the predicate $f(g(x)) = x$ is always true
Hence $\exists y(f(y) = x)$
Because $x$ is free in the previous line, $\forall x \exists y(f(y) = x)$
So $(\forall x(f(g(x)) = x)) \implies \forall x \exists y(f(y) = x)$

**33** $\forall n \in \mathbb{N} \sum_{i=0}^{n} 2 = 2(n+1)$
Answer:
Induction on $n$
$\sum_{i=0}^{0} 2 = 2 = 2(0+1)$, hence it is true when $n$ is 0.
Suppose $\sum_{i=0}^{n} 2 = 2(n+1)$
$\sum_{i=0}^{n+1} 2 = 2(n+1) + 2 = 2((n+1)+1)$
Hence by induction, $\forall n \in \mathbb{N} \sum_{i=0}^{n} 2 = 2(n+1)$

**34** $\forall n \in \mathbb{N}(\sum_{i=0}^{n} 2^i) + 1 = 2^{n+1}$
Answer:
Induction on $n$
$(\sum_{i=0}^{0} 2^i) + 1 = 1 + 1 = 2^{0+1}$

Suppose $(\sum_{i=0}^{n} 2^i) + 1 = 2^{n+1}$
$(\sum_{i=0}^{n+1} 2^i) + 1 = 2^{n+1} + 2^{n+1} = 2^{(n+1)+1}$
Hence by induction, $\forall n \in \mathbb{N}(\sum_{i=0}^{n} 2^i) + 1 = 2^{n+1}$

**35** $\forall n \in \mathbb{N} \exists k \in \mathbb{N}(n \leq 2^k)$
Proof:
Induction on $n$ to show $\forall n \in \mathbb{N} n \leq 2^n$
$0 \leq 1 = 2^0$
Suppose $n \leq 2^n$
$n + 1 \leq 2^n + 1 \leq 2^n + 2^n = 2^{n+1}$
Hence by induction, $\forall n \in \mathbb{N} n \leq 2^n$
$n \leq 2^n$
$\exists k \in \mathbb{N} n \leq 2^k$
$\forall n \in \mathbb{N} \exists k \in \mathbb{N}(n \leq 2^k)$

**36** $\forall n \in \mathbb{N}((n > 1) \implies \exists k \in \mathbb{N}((k > 1) \wedge k|n \wedge \forall p \in \mathbb{N}(p|k \implies (p = 1 \vee p = k))))$ (Recall that $a|b$ means $\exists c \in \mathbb{N}(b = ac)$)
Proof:
See example 27 in lecture notes.

**37** $\forall n \in \mathbb{N} \exists k \in \mathbb{N}((n < k) \wedge \forall p \in \mathbb{N}(p|k \implies (p = k \vee p = 1)))$.
Proof:
$n! + 1 > 1$
From problem 2 above, $\exists k \in \mathbb{N}((k > 1) \wedge k|n! + 1 \wedge \forall p \in \mathbb{N}(p|k \implies (p = 1 \vee p = k)))$
Let $k$ satisfy $(k > 1) \wedge k|n \wedge \forall p \in \mathbb{N}(p|k \implies (p = 1 \vee p = k))$
Suppose $k \leq n$
Then $k|n!$
Hence $\neg k|n! + 1$ due to remainder theorem
Contradiction.
Hence $k > n$
$\exists k \in \mathbb{N}((n < k) \wedge \forall p \in \mathbb{N}(p|k \implies (p = k \vee p = 1)))$.
$\forall n \in \mathbb{N} \exists k \in \mathbb{N}((n < k) \wedge \forall p \in \mathbb{N}(p|k \implies (p = k \vee p = 1)))$.

**38** $\forall x P(x, f(x)) \implies \forall x \exists y P(x, y)$
Proof:
Suppose $\forall x P(x, f(x))$
$P(x, f(x))$
$\exists y P(x, y)$ (replacing $f(x)$ with $y$)
$\forall x \exists y P(x, y)$
Hence $\forall x P(x, f(x)) \implies \forall x \exists y P(x, y)$

**39** $\forall x \in \mathbb{N}(\exists y \in \mathbb{N}(y > 1 \wedge (y|x) \wedge y < x) \implies \exists y \in \mathbb{N}(y > 1 \wedge (y|x) \wedge y^2 \leq x))$
Proof:
Suppose $\exists y \in \mathbb{N}(y > 1 \wedge (y|x) \wedge y < x)$

Let $y$ satisfy $y > 1 \land (y|x) \land y < x$
Let $z$ satisfy $x = yz$
$z > 1$ (because $y < x = yz$)
$y \leq z \lor z \leq y$
If $y \leq z$
$y^2 \leq yz = x$
Hence $y > 1 \land (y|x) \land y^2 \leq x$
$\exists y \in \mathbb{N}(y > 1 \land (y|x) \land y^2 \leq x))$
If $z \leq y$
$z^2 \leq yz = x$
Hence $z > 1 \land (z|x) \land z^2 \leq x$
$\exists y \in \mathbb{N}(y > 1 \land (y|x) \land y^2 \leq x))$
Hence $\exists y \in \mathbb{N}(y > 1 \land (y|x) \land y < x) \implies \exists y \in \mathbb{N}(y > 1 \land (y|x) \land y^2 \leq x)$
$\forall x \in \mathbb{N}(\exists y \in \mathbb{N}(y > 1 \land (y|x) \land y < x) \implies \exists y \in \mathbb{N}(y > 1 \land (y|x) \land y^2 \leq x))$

**40** $\forall x \in \mathbb{N} \exists y \in \mathbb{N}((x \leq y) \land (3|(2^y + 1)))$
Hint: Calculate a few $2^y + 1$ for small $y$ and try to see the pattern.
Proof:
Induction on $x$
$(0 \leq 1) \land (3|2^1 + 1)$
Hence $\exists y \in \mathbb{N}((0 \leq y) \land (3|(2^y + 1)))$
Suppose $\exists y \in \mathbb{N}((x \leq y) \land (3|(2^y + 1)))$
Let $y$ satisfy $(x \leq y) \land (3|(2^y + 1))$
Then $x + 1 \leq y + 2$
Let $z$ satisfy $2^y + 1 = 3z$
Then $2^{y+2} + 1 = 4 \times 2^y + 1 = 2^y + 1 + 3 \times 2^y = 3(z + 2^y)$
Hence $3|2^{y+2} + 1$
Hence $\exists y \in \mathbb{N}((x + 1 \leq y) \land (3|2^y + 1))$ (replacing $y + 2$ with $y$)
By induction, $\forall x \in \mathbb{N} \exists y \in \mathbb{N}((x \leq y) \land (3|(2^y + 1)))$

**41** $\exists c \in \mathbb{N} \forall x \in \mathbb{N}(2^n \leq n! + c)$
Before writing down a proof, try a few $n$ and see that for $\forall x \in \mathbb{N}(2^n \leq n! + c)$ to be true, $c$ must be at least 2.
Proof:
Use induction to prove that $\forall x \in \mathbb{N}(2^n \leq n! + 2)$
$2^0 = 1 \leq 3 = 0! + 2$
Suppose $2^n \leq n! + 2$
If $n \geq 2$
$2 \leq n! \quad 2^{n+1} = 2 \times 2^n \leq 2(n! + 2) \leq 2n! + n! + 2 = 3n! + 2 \leq (n + 1)! + 2$
If $n = 0$
$2^{n+1} = 2 \leq 3 = (n + 1)! + 2$
If $n = 1$
$2^{n+1} = 4 \leq 4 = (n + 1)! + 2$
Hence $2^{n+1} \leq (n + 1)! + 2$ is true in all cases
By induction, $\forall x \in \mathbb{N}(2^n \leq n! + c)$

$\exists c \in \mathbb{N} \forall x \in \mathbb{N}(2^n \leq n! + c)$

**42** $(\forall x \exists y(f(x) = g(y))) \implies \forall x(\exists y(f(y) = x) \implies \exists y(g(y) = x))$
Proof:
Suppose $\forall x \exists y(f(x) = g(y))$
 Suppose $\exists y(f(y) = x)$
  Let $z$ satisfy $f(z) = x$
  $\exists y(f(z) = g(y))$ ($\forall$ rule, used on the first line of the proof)
  Let $y$ satisfy $f(z) = g(y)$
  Then $g(y) = x$
  $\exists y(g(y) = x)$
 $\exists y(f(y) = x) \implies \exists y(g(y) = x)$
 $\forall x(\exists y(f(y) = x) \implies \exists y(g(y) = x))$
$(\forall x \exists y(f(x) = g(y))) \implies \forall x(\exists y(f(y) = x) \implies \exists y(g(y) = x))$

**43** $\forall x \in \mathbb{N} \exists z \in \mathbb{N}(x^3 = x + 3z)$
Proof:
Induction on $x$
$0^3 = 0 + 3 \times 0$
$\exists z \in \mathbb{N}(0^3 = 0 + 3z)$
Suppose $\exists z \in \mathbb{N}(x^3 = x + 3z)$
 Let $z$ satisfy $x^3 = x + 3z$
 Then $(x + 1)^3 = x + 1 + 3(z + x + x^2)$
 Hence $\exists z \in \mathbb{N}(x^3 = x + 3z)$
$\forall x \in \mathbb{N} \exists z \in \mathbb{N}(x^3 = x + 3z)$

**44** Prove that $\forall f \in X^X((\forall x \in X \exists y \in X(f(f(y)) = x)) \implies (\forall x \in X \exists y \in X(f(y) = x)))$ (Hint: the rules about functions in first order logic apply to functions in set theory also)
Answer:
Suppose $f \in X^X$
 Suppose $\forall x \in X \exists y \in X(f(f(y)) = x)$
  Suppose $x \in X$
   Then $\exists y \in X(f(f(y)) = x)$
   Let $y$ satisfies $y \in X \wedge f(f(y)) = x$
   Then $\exists z \in X(f(y) \in z)$ (because $f \in X^X$)
   Let $z$ satisfies $z \in X \wedge f(y) = z$
   Then $f(z) = x$
   Hence $\exists y \in X(f(y) = x)$
  Hence $\forall x \in X \exists y \in X(f(y) = x)$
$\forall f \in X^X((\forall x \in X \exists y \in X(f(f(y)) = x)) \implies (\forall x \in X \exists y \in X(f(y) = x)))$

**45** Prove that for any set $X$, the function $f : X \to P(X)$ where $f(x) = \{y \in X : y \neq x\}$ is an injection.
Answer:

```
Suppose $x \in X$, $y \in X$
 Suppose $f(x) = f(y)$
  Then $x \notin f(x)$
  Hence $y \notin f(x)$
  Hence $\neg(y \neq x)$
  Hence $y = x$
Hence $\forall x \in X \forall y \in X(f(x) = f(y) \implies x = y)$
In other words, $f$ is indeed an injection.
```

**46** Show that $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = x^3$, is an injection.
Answer:

```
Suppose $x \in \mathbb{Z}$
 Suppose $y \in \mathbb{Z}$
  Suppose $f(x) = f(y)$
   Then $x^3 - y^3 = (x - y)(x^2 + xy + y^2) = (x - y)(3(x + y)^2 + (x - y)^2)/4 = 0$
   Hence $x - y = 0$, hence $x = y$.
$f$ is an injection.
```

**47** If a function $f : \mathbb{N} \to \mathbb{N}$ is a surjection, and for any $x, y \in \mathbb{N}$, $x < y$ implies $f(x) < f(y)$, then $f$ must be identity. (Hint: use induction)
Answer:

```
Assume $f : \mathbb{N} \to \mathbb{N}$ is an surjection and that $x < y$ implies $f(x) < f(y)$
 Induction on $n$ to show $\forall n \in \mathbb{N} f(n) = n$
 Suppose $f(0) > 0$
  Suppose $y \in \mathbb{N}$
   Then $y > 0$ or $y = 0$
   Hence $f(y) \geq f(0) > 0$
  Hence $\forall y \in \mathbb{N} f(y) > 0$
  $\neg\exists y \in \mathbb{N} f(y) = 0$, which contradicts with the assumption that $f$ is surjection.
 Hence $f(0) = 0$
 Suppose $f(n) = n$
  Suppose $f(n+1) > n+1$
   Suppose $y \in \mathbb{N}$
    Then $y \leq n$ or $y = n+1$ or $y > n+1$
    Hence $f(y) \leq n$ (when $y \leq n$) or $f(y) \geq f(n+1) > n+1$ (when $y \geq n+1$)
   Hence $\neg\exists y \in \mathbb{N} f(y) = n+1$, contradiction.
  Hence $f(n+1) \leq n+1$
  $f(n+1) = n+1$
 By induction, $f = id_{\mathbb{N}}$
And the proposition is proved.
```

**48** $\forall f \in \mathbb{N}^{\mathbb{N}} \forall n \in \mathbb{N} \exists M \in \mathbb{N} \forall x \in \mathbb{N}(x < n \implies f(x) < M)$. (Any function $f : \mathbb{N} \to \mathbb{N}$ sends any subset of the form $\{1, \ldots n\}$ to a subset of some $\{1, \ldots M\}$. Hint: induction.) Answer:

```
Suppose $f \in \mathbb{N}^{\mathbb{N}}$
```

Induction on $n$
Suppose $x \in \mathbb{N}$
$x < 0 \implies f(x) < 0$ is always true
Hence $\exists M \in \mathbb{N} \forall x \in \mathbb{N}(x < 0 \implies f(x) < M)$
Suppose $\exists M \in \mathbb{N} \forall x \in \mathbb{N}(x < n \implies f(x) < M)$
Let $M \in \mathbb{N}$ satisfies $\forall x \in \mathbb{N}(x < n \implies f(x) < M)$
Let $M'$ be the larger number between $M$ and $f(n) + 1$.
Suppose $x \in \mathbb{N}$, $x < n + 1$
Then $x < n$ or $x = n$
Hence $f(x) < M \leq M'$ (when $x < n$) or $f(x) < f(n)+1 \leq M'$ (when $x = n$)
Hence $\forall x \in \mathbb{N}(x < n + 1 \implies f(x) < M')$
$\exists M \in \mathbb{N} \forall x \in \mathbb{N}(x < n + 1 \implies f(x) < M)$
By induction, the problem is proved.

**49** $\forall a \in Map(\mathbb{N}, \mathbb{R})(\forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(m) - a(n)| < 1/M) \implies \forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(2^m) - a(2^n)| < 1/M))$
Proof:
Suppose $a \in Map(\mathbb{N}, \mathbb{R})$
Suppose $\forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(m) - a(n)| < 1/M)$
Suppose $M \in \mathbb{N}\backslash\{0\}$
Let $N$ satisfies $\forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(m) - a(n)| < 1/M)$
Assume $m, n \in \mathbb{N}$, $m > N$, $n > N$
Then $2^m > N$, $2^n > N$
Hence $|a(2^m) - a(2^n)| < 1/M$
Hence $\forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(2^m) - a(2^n)| < 1/M)$
$\exists N \in \mathbb{N} \forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(2^m) - a(2^n)| < 1/M)$
$\forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(2^m) - a(2^n)| < 1/M)$
$\forall a \in Map(\mathbb{N}, \mathbb{R})(\forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(m) - a(n)| < 1/M) \implies \forall M \in \mathbb{N}\backslash\{0\} \exists N \in \mathbb{N} \forall m \in \mathbb{N} \forall n \in \mathbb{N}((m > N \wedge n > N) \implies |a(2^m) - a(2^n)| < 1/M))$

**50** Let $A = \{n \in \mathbb{N} : n < 20\}$. Show that the relation $R = \{(a, b) \in A \times A : a = b \vee a + b = 20\}$ is an equivalence relation.
Proof:
Suppose $a \in A$
Then $a = a$, hence $(a, a) \in R$
Suppose $a, b \in A$, $(a, b) \in R$
Then $a = b$ or $a + b = 20$
In both cases $(b, a) \in R$
Suppose $a, b, c \in A$, $(a, b) \in R$, $(b, c) \in R$
If $a = b$
If $b = c$

```
      Then $a = c$, hence $(a, c) \in R$
    If $b + c = 20$
      Then $a + c = 20$, hence $(a, c) \in R$
  If $a + b = 20$
    If $b = c$
      Then $a + c = 20$, hence $(a, c) \in R$
    If $b + c = 20$
      Then $a = c$, hence $(a, c) \in R$
Hence $R$ is an equivalence relation.
```