Introduction to Discrete Structures

Dr. Pascal Hitzler
http://www.pascal-hitzler.de/

EGR 199, Fall Quarter 2011
Wright State University, Dayton, OH, U.S.A.

Team: Adila Alfa Krisnadhi
Kylyn Magee
Kunal Sengupta
Cong (Joshua) Wang

[version: 11/10/2011 – final]

Contents

References

[1] Apostolos Doxiadis, Christos H. Papadimitriou, Alecos Papadatos, and Annie Di Donna. *Logicomix: An Epic Search for Truth.* Bloomsbury USA, 2009.

[2] Judith L. Gersting. *Mathematical Structures for Computer Science.* W.H. Freeman and Company, New York, 6th edition, 2007.

[3] Seymour Lipschutz and Marc Lipson. *Discrete Mathematics.* Schaum's Outline Series. McGraw-Hill, New York, 3rd edition, 2007.

This manuscript, together with the explanations given in class, is the sole reference for all course material. There is no textbook (or at least none I was able to find) which covers all topics exactly as we do them in this class. However, most of the material is contained in any book on *Discrete Mathematics* (or similar titles), in very similar form.

For the class, I will use [3] as much as possible, however this is not a required book. If you want to make a bigger investment already, you could get [2], which is used in the class *Discrete Mathematics*.

I use the margin to indicate which part of the manuscript was covered in which lecture session, using dates (American format—month first :). E.g., Chapter 1 below was started on 8th of September 2011.

This manuscript will evolve throughout the quarter while I fix typos and expand (and probably rearrange) material. However, changes will only be made to *future* material—parts of the manuscript which have already been covered in previous lecture session can be considered fixed. The version/date of the overall manuscript can be found on the front page.

If you find mistakes or typos in this manuscript, please let me know.

1 Sets

9/8/11

1.1 Definition
A *set* is a collection of objects, called the *elements* or *members* of the set (or *contained in* the set). If X is a set, then we write $a \in X$ to state that a is a member of X, and we write $a \notin X$ to state that a is not a member of X.

Usually (but not always) we will use uppercase letters to denote sets.

1.2 Remark
Note, that objects cannot occur multiple times in a set, i.e. $\{a\} = \{a, a\}$. It is not forbidden to write $\{a, a\}$, but it is the same as $\{a\}$.

1.3 Remark
Definition 1.1 is an informal definition. This causes some problems (more about this later). With more background in mathematics, it is possible to do a bit better, but this is out of scope for this lecture. However, in the end we have to start somewhere, and will not be able to completely remove the necessity to appeal to intuition.

1.4 Notation

$$X = \{2, 4, 6, 8\} = \{x \mid x \text{ is an even integer between 1 and 9}\}$$

Sometimes

$$\{x : x \text{ is an even integer between 1 and 9}\}$$

is used.

The text after the |-symbol must not be ambiguous. E.g., writing something like

$$\{x \mid x > -7 \text{ and } x < 5 \text{ or } x \text{ even}\}$$

does not constitute a well-defined set.

We read a comma as *and*:

$$\{x \mid x > -7, x < 5\} = \{x \mid x > -7 \text{ and } x < 5\} = \{x \mid -7 < x < 5\}$$

$\emptyset$ is the *empty set*, the set containing no element.

Be careful with the use of the ellipsis $\ldots$: What is $\{1, \ldots, 9\}$? $\{3, 5, 7, \ldots\}$? *If you use it, it's your responsibility that the reader does not misunderstand it.*

9/13/11

1.5 Example
We will use the following four sets throughout the class.

$\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$	the *non-negative integers* or *natural numbers*
$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$	the *integers*
$\mathbb{Q} = \left\{\frac{n}{k} \mid n \in \mathbb{Z}, 0 \neq k \in \mathbb{Z}\right\}$	the *rational numbers*
$\mathbb{R}$	the *real numbers*

Note, however, that we do not know yet what numbers *are*. We will continue to use them because we are familiar with them, but will discuss this in more depth later.

$$\begin{aligned}
\{x \mid x^2 = 4\} &= \{-2, 2\} \\
\{y \mid y \text{ is a card suit}\} &= \{\spadesuit, \heartsuit, \diamondsuit, \clubsuit\} \\
\{x \mid x \text{ is a string of } a\text{'s of length 1, 2, or 3}\} &= \{a, aa, aaa\} \\
\{2x \mid x \in \mathbb{N}\} = \{0, 2, 4, 6, 8, \ldots\} &= \{x \mid x \text{ is an even natural number}\} \\
\{n \in \mathbb{Z} \mid -2 \leq n < 2\} &= \{-2, -1, 0, 1\} \\
\sqrt{2} &\in \{x \mid x \in \mathbb{R}, x \notin \mathbb{Q}\}
\end{aligned}$$

Sets can also contain sets. E.g.,

$$\{X \mid X \text{ contains exactly 2 natural numbers}\} = \{\{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 3\}, \ldots\}.$$

This set can also be written, e.g., as

$$\{\{m, n\} \mid m, n \in \mathbb{N}, m \neq n\}.$$

Note: A statement like "$m, n \in \mathbb{N}$" is a (commonly used) abuse of notation. It actually means "$m \in \mathbb{N}$ and $n \in \mathbb{N}$."

Exercise 1
Give all elements of each of the following sets (without duplicates). Justify your answers.

(a) $A = \{x \mid \sqrt{x} \in \mathbb{N}, x < 10\}$

(b) $\{\{k, n\} \mid k, n \in A\}$

Exercise 2
Give all elements of each of the following sets (without duplicates). Justify your answers.

(a) $B = \{x \mid x \in \{\☺, \spadesuit\} \text{ or } x = 3^2\}$

(b) $\{y^2 \mid y \in B \text{ and } y \in \mathbb{N}\}$

Exercise 3
Give all elements of each of the following sets (without duplicates). Justify your answers.

(a) $C = \{x \mid x < 5, x > 7\}$

(b) $\{z \mid z = C\}$

Exercise 4 (no hand-in)
Give all elements of each of the following sets (without duplicates). Justify your answers.

(a) $A = \{x \in \mathbb{N} \mid -2 < x \leq 3\}$

(b) $B = \{x \in \mathbb{Z} \mid -3 < x \leq 2\}$

(c) $C = \{y \in \mathbb{N} \mid 4 \leq y^2 < 17\}$

(d) $D = \{x \mid x \in A \text{ or } x \in B\}$

(e) $E = \{x \mid x \in B \text{ and } x \in C\}$

(f) $F = \{x \mid x \in D \text{ and } x \in C\}$

(g) $E = \{y \mid y \in A \text{ or } y \in E\}$

1.6 Remark
Let us return to Remark 1.3, where we indicated that a naive notion of set may lead to problems. Let us assume for a moment that we were very much at liberty what we do with sets.

Then we could define the following set $\mathcal{X}$, as the "set of all sets."

$$\mathcal{X} = \{A \mid A \text{ is a set}\} \tag{1}$$

Now, since we naively assume that $\mathcal{X}$ is a set, we actually have that $\mathcal{X}$ contains itself:

$$\mathcal{X} \in \mathcal{X}$$

That sounds peculiar and strange. How could a set contain itself? We probably don't really want that. So let us look at a (presumably) "safe" selection of members of $\mathcal{X}$, defined as follows.

$$\mathcal{Y} = \{A \in \mathcal{X} \mid A \notin A\} \tag{2}$$

The intention would be that $\mathcal{Y}$ is the set consisting exactly of those sets which do not contain themselves. This sounds like a reasonable notion, doesn't it?

Let's have a closer look. In fact, let's try to answer the question whether $\mathcal{Y}$ contains itself. In other words, is $\mathcal{Y} \in \mathcal{Y}$? There are two possible answers, yes and no. Let's look at both possibilities in turn.

(yes) If $\mathcal{Y} \in \mathcal{Y}$ (i.e., $\mathcal{Y}$ were contained in $\mathcal{Y}$), then by (2) we obtain that $\mathcal{Y} \notin \mathcal{Y}$, which is impossible. So the "yes"-answer doesn't make sense.

(no) If $\mathcal{Y} \notin \mathcal{Y}$ (i.e., $\mathcal{Y}$ were *not* contained in $\mathcal{Y}$), then by (2) we obtain that $\mathcal{Y} \in \mathcal{Y}$, which is impossible. So the "no"-answer doesn't make sense either.

Looks like we're in trouble. Something must be wrong with our argumentation. But how to fix this?

The argumentation just presented is known as *Russell's Paradox*[1] (or *Russell's Antinomy*). When it was presented in 1901, it shook the foundations of mathematics.

The solution to Russell's Paradox adopted in mathematics is to define in a more precise way which collections actually constitute sets, and which collections do not constitute sets. We will not discuss this in detail here—we can safely leave this to the mathematicians. With the more precise definition in place, neither $\mathcal{X}$ nor $\mathcal{Y}$ above are actually sets, and the paradox vanishes.

So how do we know what is a set and what is not? Luckily, most collections we encounter in computer science (and even in mathematics) *are* sets. As a rule of thumb, we have to be careful when forming a "collection of all sets, which ...". If you avoid this formulation, and rather talk about a "set of all numbers, which ..." or "set of all Java programs, which ..." or "set of all sets *of real numbers*, which ...." When in doubt, ask your local mathematician. We will also return to this point later when we can make things a bit more precise.

1.7 Definition
Given two sets A and B, we say that A *is a subset of* B (A *is included in* B) if every element of A is also an element of B. We write $A \subseteq B$ in this case. The $\subseteq$-relation(ship) is called the *set inclusion ordering* (sometimes *subset inclusion ordering*).

We write $A \subsetneqq B$ if $A \subseteq B$ and $A \neq B$. We write $A \not\subseteq B$ if A is not a subset of B.

1.8 Remark
Sometimes, the symbol "$\subset$" is used, and it depends on the context if it means $\subseteq$ or $\subsetneqq$. Because of this ambiguity, it is best to avoid it.

Sometimes, in particular in books, $\subsetneq$ is used instead of $\subsetneqq$.

1.9 Remark
It is common practice to cross out symbols like $=$, $\in$, $\subseteq$ to state that the relation(ship) does *not* hold: $\neq$, $\notin$, $\not\subseteq$. Likewise, such symbols are often "flipped:" $B \supseteq A$ is written instead of $A \subseteq B$, etc. We will also use these practices in the future without further comment.

[1]Bertrand Arthur William Russell, 1872–1970. British philosopher, logician, mathematician (amongst others). A humorous and entertaining—and excellent—account of the events surrounding Russell's Paradox and its impact on the world of mathematics and science, can be found in the comic [1].

1.10 Example
Consider the sets

$$A = \{a\}$$
$$B = \{a, b\}$$
$$C = \{a, c\}$$
$$D = \{a, b, c, d\}.$$

Then $A \subseteq B \subseteq D$ and $A \subseteq C \subseteq D$. However, both $B \nsubseteq C$ and $C \nsubseteq B$.

Exercise 5
Order the following sets by set inclusion:

$$A = \{x \mid \sqrt{x} \in \mathbb{N}, x < 10\}$$
$$B = \{x^2 \mid x \in \mathbb{Z}, |x| < 4\}$$
$$C = \{x^3 \mid x \in \mathbb{N}, x < 3\}$$
$$D = \mathbb{Q}$$

Justify your answers.

Exercise 6
Consider the following sets:

H	the set of all humans
C	the set of all children
D	the set of all daughters
P	the set of all parents
A	the set of all aunts

Order these sets by set inclusion. Justify your answers.

Exercise 7
Determine all sets $B \subseteq \{a, b\}$ which satisfy the requirement

$$B \not\supseteq \{a\}.$$

Justify your answer.

1.11 Proposition
For all sets A, B, C, the following hold.

i) $A \subseteq A$

ii) If $A \subseteq B$ and $B \subseteq A$, then $A = B$.

iii) If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

1.12 Remark
For all integers x, y, z, the following hold.

i) $x \leq x$

ii) If $x \leq y$ and $y \leq x$, then $x = y$.

iii) If $x \leq y$ and $y \leq z$, then $x \leq z$.

1.13 Remark
For any two integers x and y, we always have $x \leq y$ or $y \leq x$ (or even both). However, for two sets A and B it can happen, that neither $A \subseteq B$ nor $B \subseteq A$ holds. See Example 1.10.

1.14 Remark
A practical way to avoid trouble with Russell's Paradox is the following. Whenever talking about sets, you fix a (big) set U, called the *universe* (of discourse), which contains everything you need for your current discussion. All "sets" in your discussion will then be subsets of U. In this case, you do not have to worry about Russell's Paradox, provided the universe U is really a set.

Whenever sets are discussed, there is an underlying universe. In many cases, however, the universe is not explicitly given (or even mentioned). The reason for this is that the exact universe for a discussion is usually of little consequence, as long as it is "big enough" and really contains everything that's needed for the discussion.

1.15 Definition
Let U be a universe $A \subseteq U$, and $B \subseteq U$. Then define the following.

$A \cap B = \{x \in U \mid x \in A \text{ and } x \in B\}$	the *intersection* of A and B
$A \cup B = \{x \in U \mid x \in A \text{ or } x \in B\}$	the *union* of A and B
$A \setminus B = \{x \in U \mid x \in A \text{ and } x \notin B\}$	the *difference* of A and B
$A^{\mathsf{c}} = U \setminus A = \{x \in U \mid x \notin A\}$	the *complement* of A
$A \times B = \{(x, y) \mid x \in A \text{ and } y \in B\}$	the (*Cartesian*[2]) *product* of A and B

Example

$$\{2, 3\} \cap \{3, 4\} = \{3\}$$
$$\{2, 3\} \cup \{3, 4\} = \{2, 3, 4\}$$
$$\{2, 3\} \setminus \{3, 4\} = \{2\}$$

[2]Named after René Descartes, 1596–1650, French philosopher and mathematician.

1.16 Remark
We use brackets "(" and ")" in the usual way, e.g. to distinguish $(A \cup B) \cap C$ from $A \cup (B \cap C)$.

1.17 Remark
A sentence like "Let U be a universe $A \subseteq U$, and $B \subseteq U$." is often phrased (abusing language and notation) in ways such as "Let U be a universe and A, B be sets." If the universe doesn't matter much, it may even be stated as "Let A, B be sets."

1.18 Remark
Strictly speaking, a notation such as $\{x \in U \mid x \notin A\}$ is a (common) abuse of notation. Correct is $\{x \mid x \in U \text{ and } x \notin A\}$. We will also follow this practice.

1.19 Remark
With respect to the definition of the Cartesian product just given, note that we do not *formally* know yet what *pairs* are. We will rectify this later.

Exercise 8
Let $U = \{n \in \mathbb{N} \mid n < 10\}$, $A = \{0, 1, 2, 3\}$, $B = \{3, 4, 5\}$. Give all elements of each of the following sets.

(a) $A \cup B$

(b) $(A \cup B)^{\mathsf{c}}$

Exercise 9
Let $U = \{n \in \mathbb{N} \mid n < 10\}$, $A = \{0, 1, 2, 3\}$, $B = \{3, 4, 5\}$. Give all elements of each of the following sets.

(a) $A \cap B$

(b) $(A \cap B)^{\mathsf{c}} \setminus (A \cup B)$ – explain how you arrived at the solution.

Exercise 10
Let $U = \{n \in \mathbb{N} \mid n < 10\}$, $A = \{0, 1, 2, 3\}$, $B = \{3, 4, 5\}$. Give all elements of each of the following sets.[3]

(a) $A \times B$

(b) $(A \cap B) \times B$ – explain how you arrived at the solution.

1.20 Remark
Relationships between sets can be depicted informally using Venn diagrams.[4] Examples are given in Figure 1. Note, however, that the use of Venn diagrams is limited. For example, products cannot be depicted. An argument or proof is usually incomplete when it only consists of a Venn diagram.

[3] Corrected part (a) after grading.
[4] Named after John Venn, 1834–1923, British logician and philosopher.

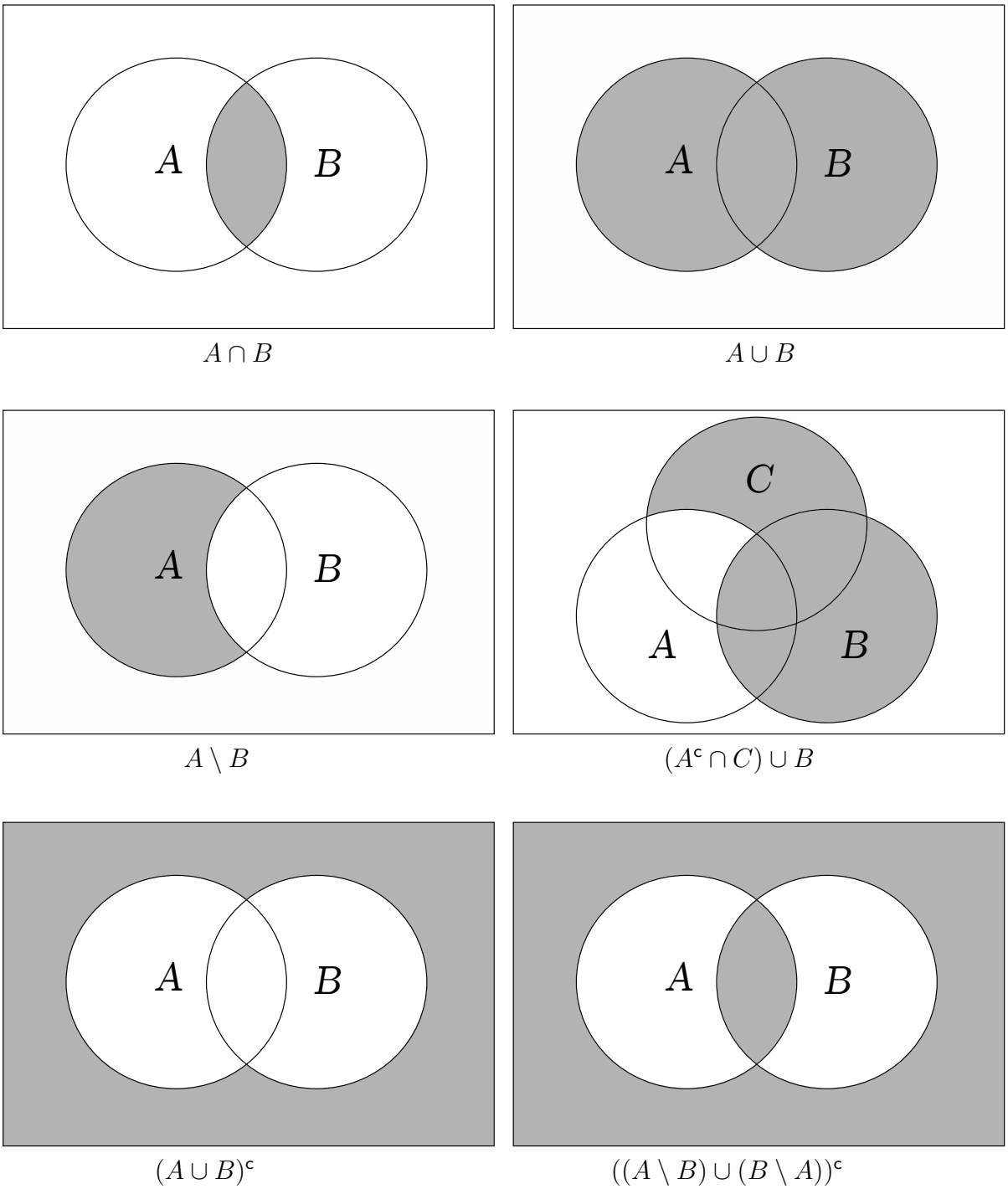

Figure 1: Examples of Venn diagrams

1.21 Definition
Two sets A and B are said to be *disjoint* if $A \cap B = \emptyset$, i.e., if they have an empty intersection; in other words, if they do not have any common element.

Exercise 11
(a) Make a Venn diagram depicting the set $(A^{\mathsf{c}} \cup B) \cap C$.

(b) Determine all elements of the set

$$(\mathbb{Q} \setminus (\mathbb{Z} \setminus \mathbb{N}))^{\mathsf{c}} \cap \left\{-2, 2, \sqrt{2}, \frac{7}{2}\right\},$$

where the universe is $U = \mathbb{R}$.
Justify your answers.

1.22 Proposition
Let U be a universe and A, B, C be sets. Then the following hold.

$A \cap A = A$	$A \cup A = A$	idempotency
$A \cap B = B \cap A$	$A \cup B = B \cup A$	commutativity
$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$	associativity
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	distributivity
$A \setminus B = A \cap B^{\mathsf{c}}$		difference
$(A^{\mathsf{c}})^{\mathsf{c}} = A$		involution
$(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$	$(A \cup B)^{\mathsf{c}} = A^{\mathsf{c}} \cap B^{\mathsf{c}}$	de Morgan's Laws[5]

Proof: We give two example proofs.

We first show the de Morgan Law $(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$. To do this, we show two things: (1) $(A \cap B)^{\mathsf{c}} \subseteq A^{\mathsf{c}} \cup B^{\mathsf{c}}$ and (2) $A^{\mathsf{c}} \cup B^{\mathsf{c}} \subseteq (A \cap B)^{\mathsf{c}}$.

(1) Let $a \in (A \cap B)^{\mathsf{c}}$. Then a is not an element of $A \cap B$, i.e., either a is not in A or a is not in B. Hence we have either $a \in A^{\mathsf{c}}$ or $a \in B^{\mathsf{c}}$ (or both), and consequently $a \in A^{\mathsf{c}} \cup B^{\mathsf{c}}$. Since this argument holds for all $a \in (A \cap B)^{\mathsf{c}}$, we have shown that $(A \cap B)^{\mathsf{c}} \subseteq A^{\mathsf{c}} \cup B^{\mathsf{c}}$.

(2) Let $a \in A^{\mathsf{c}} \cup B^{\mathsf{c}}$. Then $a \in A^{\mathsf{c}}$ or $a \in B^{\mathsf{c}}$ (or both). Consequently, a is not in A or not in B, and thus it is not possible that it is in both A and B. Hence, a is not in $A \cap B$, and thus $a \in (A \cap B)^{\mathsf{c}}$. Since this argument holds for all $a \in A^{\mathsf{c}} \cup B^{\mathsf{c}}$, we have shown that $A^{\mathsf{c}} \cup B^{\mathsf{c}} \subseteq (A \cap B)^{\mathsf{c}}$

This completes the proof of the correctness of the de Morgan Law $(A \cap B)^{\mathsf{c}} = A^{\mathsf{c}} \cup B^{\mathsf{c}}$.

As another example, we show that the Involution property $(A^{\mathsf{c}})^{\mathsf{c}} = A$ holds. We obtain $(A^{\mathsf{c}})^{\mathsf{c}} = U \setminus A^{\mathsf{c}} = U \setminus (U \setminus A) = U \setminus \{x \in U \mid x \notin A\} = \{x \in U \mid x \notin \{x \in U \mid x \notin A\}\} = \{x \in U \mid x \in A\} = A$. ■

[5]Named after Augustus de Morgan, 1806–1871, British mathematician and logician.

1.23 Remark
The "calculus" described in Proposition 1.22 is called *the algebra of sets*.

1.24 Remark
Because of associativity, we can write $A \cap B \cap C$ and $A \cup B \cup C$ without brackets: it doesn't make a difference how the brackets are set.

1.25 Example
We show $(A \setminus B) \cap C = A \cap (C \setminus B)$ by applying the equations in Proposition 1.22:

$$\begin{aligned}
(A \setminus B) \cap C &= (A \cap B^{\mathsf{c}}) \cap C && \text{(difference)} \\
&= A \cap (B^{\mathsf{c}} \cap C) && \text{(associativity)} \\
&= A \cap (C \cap B^{\mathsf{c}}) && \text{(commutativity)} \\
&= A \cap (C \setminus B) && \text{(difference)}
\end{aligned}$$

1.26 Example
We show $(A \cap B)^{\mathsf{c}} \cup C = A^{\mathsf{c}} \cup (B \setminus C)^{\mathsf{c}}$ by applying the equations in Proposition 1.22:

$$\begin{aligned}
(A \cap B)^{\mathsf{c}} \cup C &= (A^{\mathsf{c}} \cup B^{\mathsf{c}}) \cup C && \text{(de Morgan)} \\
&= A^{\mathsf{c}} \cup (B^{\mathsf{c}} \cup C) && \text{(associativity)} \\
&= A^{\mathsf{c}} \cup (B^{\mathsf{c}} \cup (C^{\mathsf{c}})^{\mathsf{c}}) && \text{(involution)} \\
&= A^{\mathsf{c}} \cup (B \cap C^{\mathsf{c}})^{\mathsf{c}} && \text{(de Morgan)} \\
&= A^{\mathsf{c}} \cup (B \setminus C)^{\mathsf{c}} && \text{(difference)}
\end{aligned}$$

Exercise 12
Show the following for all sets A and B, by applying the equations from Proposition 1.22.

(a) $(A^{\mathsf{c}} \cap B^{\mathsf{c}})^{\mathsf{c}} = A \cup B$

(b) $A \setminus (B \setminus C) = (A \cap B^{\mathsf{c}}) \cup (A \cap C)$

09/22/11

1.27 Example
We show that A and A^{c} are disjoint.

$$\begin{aligned}
A \cap A^{\mathsf{c}} &= A \setminus A && \text{(difference)} \\
&= \{x \in U \mid x \in A \text{ and } x \notin A\} \\
&= \emptyset
\end{aligned}$$

1.28 Example
We show $U^{\mathsf{c}} = \emptyset$:

$$\begin{aligned}
U^{\mathsf{c}} &= U \setminus U && \text{(difference)} \\
&= \emptyset && \text{(see Example 1.27)}
\end{aligned}$$

We show $\emptyset^{\mathsf{c}} = U$:

$$\begin{aligned}
U &= (U^{\mathsf{c}})^{\mathsf{c}} && \text{(involution)} \\
&= \emptyset^{\mathsf{c}} && \text{(shown above)}
\end{aligned}$$

1.29 Example
We show $A \cup A^{\mathsf{c}} = U$.

$$\begin{aligned} A \cup A^{\mathsf{c}} &= (A^{\mathsf{c}})^{\mathsf{c}} \cup A^{\mathsf{c}} && \text{(involution)} \\ &= (A^{\mathsf{c}} \cap A)^{\mathsf{c}} && \text{(de Morgan)} \\ &= \emptyset^{\mathsf{c}} && \text{(Exercise 1.27)} \\ &= U && \text{(Exercise 1.28)} \end{aligned}$$

1.30 Example

$$A \cap U = \{x \in U \mid x \in A \text{ and } x \in U\} = \{x \in U \mid x \in A\} = A$$

$$\begin{aligned} A \cup \emptyset &= (A^{\mathsf{c}})^{\mathsf{c}} \cup (\emptyset^{\mathsf{c}})^{\mathsf{c}} && \text{(involution, twice)} \\ &= (A^{\mathsf{c}} \cap \emptyset^{\mathsf{c}})^{\mathsf{c}} && \text{(de Morgan)} \\ &= (A^{\mathsf{c}} \cap U)^{\mathsf{c}} && \text{(Example 1.28)} \\ &= (A^{\mathsf{c}})^{\mathsf{c}} && \text{(see above)} \\ &= A && \text{(involution)} \end{aligned}$$

$$A \cup U = \{x \in U \mid x \in A \text{ or } x \in U\} = \{x \in U \mid x \in U\} = U$$

$$\begin{aligned} A \cap \emptyset &= (A^{\mathsf{c}})^{\mathsf{c}} \cap (\emptyset^{\mathsf{c}})^{\mathsf{c}} && \text{(involution, twice)} \\ &= (A^{\mathsf{c}} \cup \emptyset^{\mathsf{c}})^{\mathsf{c}} && \text{(de Morgan)} \\ &= (A^{\mathsf{c}} \cup U)^{\mathsf{c}} && \text{(Example 1.28)} \\ &= (U)^{\mathsf{c}} && \text{(see above)} \\ &= \emptyset && \text{(Example 1.28)} \end{aligned}$$

09/27/11

Exercise 13
Show, using the equations from Proposition 1.22:

$$U = A \cup ((B^{\mathsf{c}} \cap A) \cup (B \cap A))^{\mathsf{c}}.$$

[Hint: if you find this difficult, you may be able to get inspiration from working through Examples 1.34 to 1.36.]

1.31 Definition
Given any set X, the *power set* $\mathcal{P}(X)$ of X is defined as the set of all subsets of X.

1.32 Remark
Another very common notation for the power set of a set X is to write 2^X instead of $\mathcal{P}(X)$.

1.33 Example

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

Exercise 14
(a) Determine the number of elements of $\mathcal{P}(\{1, 2, 3, 4\})$.

(b) Determine the number of elements of $\mathcal{P}(\mathcal{P}(\emptyset))$.
Justify your answers.

Further Examples

These examples have not been discussed in class. They remain in the manuscript for you to read and study yourself.

1.34 Example
We show $(A \cap B)^c \cup B = U$.

$$\begin{aligned}
(A \cap B)^c \cup B &= (A^c \cup B^c) \cup B && \text{(de Morgan)} \\
&= A^c \cup (B^c \cup B) && \text{(associativity)} \\
&= A^c \cup (B \cup B^c) && \text{(commutativity)} \\
&= A^c \cup U && \text{(Example 1.29)} \\
&= U && \text{(Example 1.30)}
\end{aligned}$$

1.35 Example
We show $(A \cap B) \cup (A \cap B^c) = A$.

$$\begin{aligned}
(A \cap B) \cup (A \cap B^c) &= (A \cup (A \cap B^c)) \cap (B \cup (A \cap B^c)) && \text{(distributivity)} \\
&= (A \cup A) \cap (A \cup B^c) \cap (B \cup A) \cap (B \cup B^c) && \text{(distributivity, twice)} \\
&= A \cap (A \cup B^c) \cap (B \cup A) \cap U && \text{(idempotency, Ex. 1.29)} \\
&= A \cap (A \cup B^c) \cap (A \cup B) && \text{(commutativity, Ex. 1.30)} \\
&= A \cap (A \cup (B^c \cap B)) && \text{(distributivity)} \\
&= A \cap (A \cup \emptyset) && \text{(Exercise 1.27)} \\
&= A \cap A && \text{(Exercise 1.30)} \\
&= A && \text{(involution)}
\end{aligned}$$

Note there's also a simpler solution. Do you see it?

1.36 Example
We show $(A \cap B^c) \cup (A^c \cap B) \cup (A \cap B) = A \cup B$.

$$\begin{aligned}
(A \cap B^c) \cup (A^c \cap B) \cup (A \cap B) &= (A \cap B^c) \cup (A^c \cap B) \cup (A \cap B) \cup (A \cap B) && \text{(idempot.)} \\
&= (A \cap B) \cup (A \cap B^c) \cup (B \cap A) \cup (B \cap A^c) && \text{(commut.)} \\
&= (A \cap (B \cup B^c)) \cup (B \cap (A \cup A^c)) && \text{(distribut.)} \\
&= (A \cap U) \cup (B \cap U) && \text{(Ex. 1.29)} \\
&= A \cup B && \text{(Ex. 1.30)}
\end{aligned}$$

2 Functions and Relations

We have defined the Cartesian product of sets using a notion of *pair*. But we did not give a formal definition of *pair*. Can we found the notion of *pair* in set theory?

2.1 Definition
A *pair*[6] is a set $\{\{a\},\{a,b\}\}$, written (a,b), where $a,b \in U$.

2.2 Example

$$\begin{aligned}(a,\{b\}) &= \{\{a\},\{a,\{b\}\}\}\\ (\emptyset,a) &= \{\{\emptyset\},\{\emptyset,a\}\}\\ (\{b\},\{b\}) &= \{\{\{b\}\}\}\end{aligned}$$

Exercise 15
(a) Write $\{\{a\}\}$ as pair.

(b) Write the pair $(\{a,b\},\{a\})$ in set notation.

(c) Write the set of pairs $\{(a,b),(a,c)\}$ in set notation.

2.3 Proposition
$(a,b) = (c,d)$ if, and only if, $a = c$ and $b = d$.

Proof: We first prove the "if"-part. Let $a = c$ and $b = d$. Then $\{a\} = \{c\}$ and $\{a,b\} = \{c,d\}$. Hence $\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}$, i.e., $(a,b) = (c,d)$. This concludes the "if"-part.

We now prove the "only if"-part. Let $(a,b) = (c,d)$. Then by Defintion 2.1 we have

$$\{\{a\},\{a,b\}\} = \{\{c\},\{c,d\}\}. \tag{3}$$

We distinguish two cases.

1. If $\{a\} = \{c,d\}$, then $a = c = d$ and from (3) we obtain $\{\{a\},\{a,b\}\} = \{\{a\}\}$. This implies that $a = b$, and hence $a = b = c = d$. We have shown $a = c$ and $b = d$ as required.
2. If $\{a\} = \{c\}$ (but not $\{a\} = \{c,d\}$, then by definition 2.1 we have $\{\{a\},\{a,b\}\} = \{\{a\},\{a,d\}\}$. Since $\{a\} = \{c,d\}(= \{a,d\})$—and thus also $a = d$—have been excluded, we obtain $\{a,b\} = \{a,d\}$ and in particular $b = d$. From $\{a\} = \{c\}$ we also obtain $a = c$, as required.

All possible cases lead to the desired conclusion. ■

[6] Due to Kazimierz Kuratowski, 1896–1980, Polish mathematician and logician.

2.4 Definition
Let A, B be sets. A (*binary*) *relation* R from A to B is a subset of $A \times B$. In this case, we call A the *domain* of R, denoted $\mathrm{dom}(R)$, and we call B the *range* of R, denoted $\mathrm{ran}(R)$.[7] We can use the notation $R(a, b)$ to indicate $(a, b) \in R$.

2.5 Remark
Relations are simply sets of pairs. Explicit mention of domain and range is often omitted, if they are inconsequential.

If A and B are sets, then every $R \subseteq A \times B$ is a relation from A to B. By another abuse of notation, a phrase such as "let $R \subseteq A \times B$" is often shorthand for "let R be a relation from A to B."

So what about all this abuse of notation? It seems arbitrary and wild, but it actually isn't. With some practice, some things are self-evident and do not need explicit mention. And, in fact, avoiding explicit mention of self-evident things often makes mathematics easier to read. However, there is a danger in there, because misunderstandings may happen. In the end, it's an author's responsibility to make sure that all necessary details are given. When in doubt, be verbose and formal.

2.6 Example
Let A be a set. Then "$=$" (*equality*) is a relation on A (meaning, a relation from A to A). Formally, $= \subseteq A \times A$. Equality is usually written in *infix* notation, i.e., all of the following mean the same: $a = a$ (infix notation), $=(a, a)$ (*prefix* notation), $(a, a) \in =$ (set notation).

2.7 Example
$\leq \subseteq \mathbb{Z} \times \mathbb{Z}$ is a relation, the "less than or equal" ordering on the integers:

$$\leq = \{(m, n) \mid m \leq n\}.$$

It is usually written infix.

2.8 Example
Let A be a set. $\subseteq$ (set inclusion) is a relation on $\mathcal{P}(A)$:

$$\subseteq = \{(B, C) \mid B \subseteq C \subseteq A\}$$

It is usually written infix.

2.9 Example
Let A be a set. $\in \subseteq A \times \mathcal{P}(A)$ (the membership relation) is a relation from A to $\mathcal{P}(A)$:

$$\in = \{(x, X) \mid x \in A, X \subseteq A\}.$$

It is usually written infix.

2.10 Example
$\{(a,b),(a,c),(a,e),(b,a),(b,e)\}$ is an example for a relation from $\{a,b,c,d\}$ to $\{a,b,c,e,f\}$.

2.11 Example
Let H be the set of all humans and C be the set of all cars. Then *owner-of* is a relation from H to C, where we have *owner-of*(a,b) if and only if a is a human who owns car b.

Exercise 16
Write the statement $\{a\} \subseteq \{a,b\}$

(a) in prefix form,

(b) in the form $\ldots \in \subseteq$ (with $\ldots$ appropriately filled in). Set notation is expected.

2.12 Definition
A relation R on a set A is called

i) *reflexive*, if $(a,a) \in R$ for all $a \in A$.

ii) *symmetric*, if $(a,b) \in R$ whenever $(b,a) \in R$.

iii) *antisymmetric*, if $a = b$ whenever $(a,b) \in R$ and $(b,a) \in R$.

iv) *transitive*, if $(a,c) \in R$ whenever $(a,b) \in R$ and $(b,c) \in R$.

2.13 Example

- Equality is reflexive, symmetric, antisymmetric and transitive.
- The "less than or equal"-ordering on integers is reflexive, antisymmetric and transitive, but not symmetric.
- The "less than"-ordering "$<$" on integers is transitive and antisymmetric, but neither reflexive nor symmetric. To see that it is antisymmetric, we have to show the following: *Whenever* $m < n$ *and* $n < m$*, then* $m = n$*.* And indeed this is the case, because it can never happen that $m < n$ and $n < m$ for two $m, n \in \mathbb{Z}$.
- The set inclusion ordering is reflexive, antisymmetric and transitive, but not symmetric.
- The membership relation from a set A to $\mathcal{P}(A)$ has differing domain and range, and thus is neither reflexive, nor symmetric, nor antisymmetric, nor transitive.

Exercise 17
For each of the following relations, determine whether it is reflexive, symmetric, antisymmetric, transitive. Justify your answers.

[7] The definitions of domain and range of relations are different in [3]. We follow [2] in what is the commonly used definition.

(a) The *proper set inclusion* "$\subsetneq$."

(b) The relation $\{(a,a),(a,c),(a,d),(b,b),(b,c),(c,c),(c,a),(c,b),(d,a),(d,d)\}$ on the set $\{a,b,c,d\}$ with four elements.

2.14 Definition
A (*total*) *function* (or *mapping*) f from A to B (written $f : A \to B$) is a relation from A to B which satisfies the following requirement: For each $a \in A$ there exists exactly one b such that $(a,b) \in f$. We denote this unique b by $f(a)$ in this case, and we call b the (*output*) *value* of f under (or *with input value*) a. We also say that a *is mapped to* or *maps to* b.

2.15 Remark
Note that each function comes with a domain and a range, and if you change any of them you obtain a different function. For example, the function mapping each natural number x to x^2 (with domain $\mathbb{N}$ and range $\mathbb{N}$) is different from the function mapping each integer x to x^2 (with domain $\mathbb{Z}$ and range $\mathbb{N}$).

2.16 Example
Let $A = \{0,1,2,3\} \subseteq \mathbb{N}$. We want to define the function which squares the input value. There are different, equivalent, ways how to do this.

- $f : A \to \mathbb{N} : k \mapsto k^2$. Note the different types of arrows: "$\to$" is used between domain and range, while "$\mapsto$" is used between input and output value. If domain and range are clear from the context (or inconsequential), then we can simply write $f : k \mapsto k^2$.
- $f : A \to \mathbb{N} : f(n) = n^2$.
- $f : A \to \mathbb{N} : 0 \mapsto 0; 1 \mapsto 1; 2 \mapsto 4; 3 \mapsto 9$. I.e., we can choose to explicitly give the output for each input value, using the $\mapsto$-arrow. This form is rarely used because it is difficult to read.
- $f : A \to \mathbb{N} : f(n) = \begin{cases} 0 & \text{if } n = 0 \\ 1 & \text{if } n = 1 \\ 4 & \text{if } n = 2 \\ 9 & \text{if } n = 3 \end{cases}$
  or similar definitions by cases.
- $f : A \to \mathbb{N}$ with $f = \{(0,0),(1,1),(2,4),(3,9)\}$. This form is rarely used because it is difficult to read. However, it is closest to our definition of *functions* as special types of relations.

Other notations can be derived from these, e.g., by writing the set in the last example in other formats.

10/11/11

Exercise 18
Let $A = \{2,4,6\}$. Write the following functions in the notation $f : A \to \mathbb{N} : n \mapsto \ldots$, with "..." filled in appropriately. Justify your answers.

(a) $\{(k, m) \mid k \in A, m = 2k\}$

(b) $\{\{\{2\}, \{1, 2\}\}, \{\{4\}, \{2, 4\}\}, \{\{6\}, \{3, 6\}\}\}$

Exercise 19
Is the relation $\not\subseteq$ reflexive? symmetric? antisymmetric? transitive? Justify your answers.

Exercise 20
Consider the function $f : \mathbb{N} \to \mathbb{N} : n \mapsto n^2$ as a relation on $\mathbb{N}$. Is it reflexive? symmetric? antisymmetric? transitive? Justify your answers.

2.17 Example
$f : (\mathbb{N} \times \mathbb{N}) \to \mathbb{N} : (k, n) \mapsto k + n$ is a function whose input values are pairs. We call such a function a *binary* function. By abuse of language, we say that f has two input values.

$f : ((\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \to \mathbb{N} : ((k, n), m) \mapsto \frac{k+m}{n+1}$ is a *ternary* function, i.e., a function with three input values. We can also write it as $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (k, n, m) \to \frac{k+m}{n+1}$. Is is common to write $\mathbb{N}^3$ for $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$.

Similarly, functions of higher arity (*n-ary functions* with n input values) can be defined.

2.18 Definition
A *partial function* f from A to B (written $f : A \to B$) is a relation from A to B which satisfies the following requirement: For each $a \in A$ there exists *at most* one b such that $(a, b) \in f$. We denote this unique b by $f(a)$ in this case. We furthermore write $f(a) = \perp$ if there is no pair of the form $(a, \cdot) \in f$.

2.19 Example
The partial function $f : \mathbb{R} \to \mathbb{R} : x \mapsto \frac{1}{x}$ is not total, since 0 is not mapped to any element of $\mathbb{R}$.

2.20 Remark
Every total function is also a partial function.

2.21 Remark
When mathematicians talk about "functions," they usually mean total functions, and they explicitly say "partial function" if they don't require it to be total. In some areas (including some areas of Computer Science), partial functions are more important, and in this case the notion "function" is often reserved for partial functions, while it is explicitly stated if a function is total. We will follow the convention used in Mathematics.

2.22 Definition
A funtion $f : A \to B$ is called *injective* (or *one-to-one*) if, whenever $a \neq b$, then als $f(a) \neq f(b)$. It is called *surjective* (or *onto*) if for every $b \in B$ there is an $a \in A$ with $f(a) = b$. It is called *bijective* if it is injective and surjective.

2.23 Remark
Intuitively, $f : A \to B$ is injective if "no two input values have the same output value." It is surjective if "the complete range is used by the function." It is injective if "it constitutes a bidirectional one-to-one mapping between domain and range."

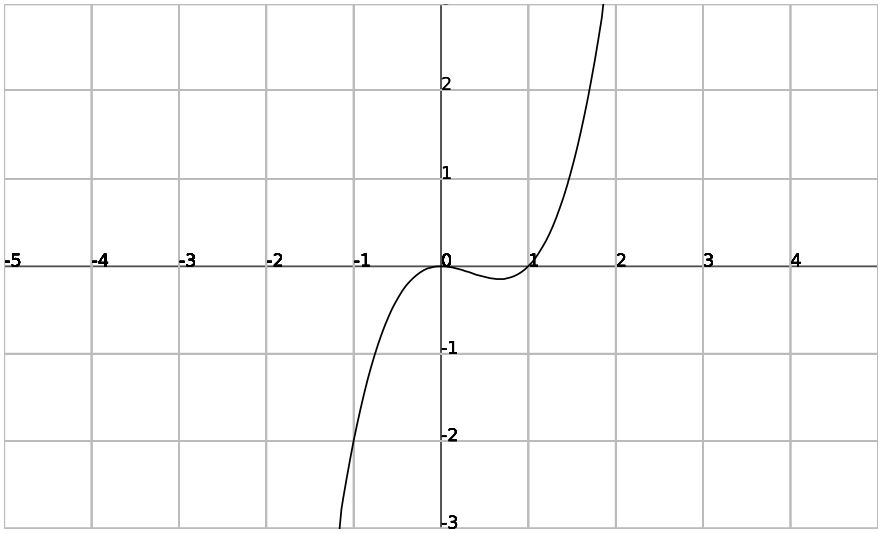

Figure 2: $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^3 - x^2$

2.24 Remark
An equivalent (and more common) definition of injectivity is as follows: A function $f : A \to B$ is *injective* if, whenever $f(a) = f(b)$, then also $a = b$.

2.25 Example

- $f : \mathbb{R} \to \mathbb{R} : x \mapsto 2^x$ is injective but not surjective.
- $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^3 - x^2$ (see Figure 2) is surjective but not injective.
- $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^3$ is injective and surjective (and thus bijective).
- $f : \mathbb{R} \to \mathbb{R} : x \mapsto x^2$ is neither injective nor surjective.

Exercise 21
Determine for each of the following functions whether it is injective, surjective, bijective. Justify your answers.

(a) $g : \{a, b, c\} \to \{d, e, f\}$ with $g = \{(a, d), (b, e), (c, f)\}$.

(b) $h : \{a, b, c\} \to \{d, e, f, h\}$ with $h = \{(a, d), (b, e), (c, f)\}$.

(c) $g : \{a, b, c\} \to \{d, e\}$ with $g = \{(a, d), (b, e), (c, d)\}$.

Exercise 22
Let $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x \geq 0\}$. Determine for each of the following functions whether it is injective, surjective, bijective. Justify your answers.

(a) $f : \mathbb{R} \to \mathbb{R}^+ : x \mapsto x^2$.

(b) $f : \mathbb{R}^+ \to \mathbb{R}^+ : x \mapsto x^2$.

2.26 Definition
Two sets A and B are said to be *of the same cardinality* if there is a bijective function $f : A \to B$. We write $|A| = |B|$ or $A \equiv B$ in this case.

A set A is said to be *of lower cardinality* than a set B if there is an injection $f : A \to B$. We write $|A| \leq |B|$ or $A \preceq B$ in this case.

A set A is said to be *of strictly lower cardinality* than a set B if if it is of lower cardinality but not of the the same cardinality. We write $|A| < |B|$ or $A \prec B$ in this case.

2.27 Example

$$\begin{aligned} \{a, b, c\} &\equiv \{1, 2, 3\} \\ \{a, b\} &\preceq \{1, 2, 3, 4\} \\ \{a, b, c, d\} &\preceq \mathbb{N} \end{aligned}$$

2.28 Proposition
The relation "$\preceq$" is reflexive, antisymmetric, and transitive.

2.29 Example
Let $2\mathbb{N} = \{2n \mid n \in \mathbb{N}\} = \{0, 2, 4, 6, \dots\}$ be the set of even natural numbers. Then $|2\mathbb{N}| = |\mathbb{N}|$.

To see why this is the case, consider the function $f : \mathbb{N} \to 2\mathbb{N} : n \mapsto 2n$. This function is a bijection, which shows that $\mathbb{N}$ and $2\mathbb{N}$ are of the same cardinality.

2.30 Definition
A set A is said to be *infinite* (or *of infinite cardinality*) if there is a proper subset $B \subsetneq A$ with $|B| = |A|$.

A set is said to be *finite* (or *of finite cardinality*) if it is not infinite.

A set A is said to be *countable* (or *of countable cardinality*) if $|A| \leq |\mathbb{N}|$.

A set is said to be *countably infinite* (or *of countably infinite cardinality*) if it is infinite and countable.

A set is said to be *uncountable* (or *of uncountable cardinality*) if it is not countable.

10/13/2011

2.31 Example
$\mathbb{N}$ is inifinite, as seen in Example 2.29. It is therefore countably infinite.

$|\mathbb{Z}| = |\mathbb{N}|$, because the following function is a bijection:

$$f : \mathbb{N} \to \mathbb{Z} : n \mapsto \begin{cases} \frac{n}{2} & \text{if } n \in 2\mathbb{N} \\ -\frac{n+1}{2} & \text{if } n \notin 2\mathbb{N} \end{cases}$$

2.32 Theorem
$|\mathbb{N}| = |\mathbb{Q}|$

Proof: See the lecture. The proof is based on *Cantor's first diagonalization principle*.[8] ■

[8]Named after Georg Ferdinand Ludwig Philipp Cantor, 1845–1918, German mathematician.

2.33 Theorem
$\mathcal{P}(\mathbb{N})$ is not countable. In other words, $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$.

Proof: *Assume* $\mathcal{P}(\mathbb{N})$ is countable.[9] Then there is a bijection $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$. Define the set $D = \{n \in \mathbb{N} \mid n \notin f(n)\} \subseteq \mathbb{N}$. Since f is a bijection, there must be some $d \in \mathbb{N}$ such that $f(d) = D$.

Is $d \in D$? If it were, then by definition of D we obtain $d \notin f(d) = D$ which is impossible. If it were not, then again by definition of D we obtain $d \in D$ which is impossible.

So, if we assume that $\mathcal{P}(\mathbb{N})$ is countable, then we arrive at an impossible situation (called a *contradiction*). The assumption "$\mathcal{P}(\mathbb{N})$ is countable" therefore must be refuted. This completes the proof that $\mathcal{P}(\mathbb{N})$ is not countable. ■

2.34 Remark
The proof of Theorem 2.33 is based on *Cantor's second diagonalization principle*, often referred to simply as *diagonalization*. Diagonalization is of central importance in studying the limits of computation.

Exercise 23
A relation R on a set X is called *linear* if, for any $x, y \in X$ with $x \neq y$, we have $(x, y) \in R$ or $(y, x) \in R$.

(a) Is set inclusion "$\subseteq$" linear? Justify your answer.

(b) Is the $\leq$-relation on $\mathbb{R}$ linear? Justify your answer.

10/18/2011

3 Boolean[10] Algebra / Propositional Logic

3.1 Definition
Let **P** be a countably infinite set. We call the elements of **P** *propositional variables* (or *Boolean variables*), and will usually denote them by letters $p, q, r, \ldots$.

3.2 Remark
Intuitively, we think of a Boolean variable as something which is either *true* or *false*. They stand for statements like "Mary is in the library" or "Socrates is dead." This intuition leads us into the realm of logic and artificial intelligence.

Alternatively, we can think of Boolean variables to stand for "power on" or "power off"—this intuition leads us into the realm of hardware (circuit) design.

3.3 Definition
We define (*propositional*) *formulas* recursively as follows.

[9] Proper use of English would probably demand the wording "Assume $\mathcal{P}(\mathbb{N})$ *were* countable." However, this would prompt us to use the conditional everywhere in the proof, which would be rather awkward. It is thus common practice to use the present tense in such proofs.

[10] Named after George Boole, 1815–1864, English mathematician and philosopher.

- Every $p \in \mathbf{P}$ is a formula (called an *atomic* formula).
- If F is a formula, then $\neg F$ is a formula.
- If F, G are formulas, then $(F \vee G)$ and $(F \wedge G)$ are formulas.
- nothing else is a formula.

$(F \vee G)$ is called the *disjunction* of F and G (pronounced "F or G"). $(F \wedge G)$ is called the *conjunction* of F and G (pronounced "F and G").

We denote the set of all formulas by $\mathbf{F}$.

The symbols $\vee$, $\wedge$, $\neg$ are called *connectives*.

3.4 Example
All of the following are formulas:
$(p \vee q)$
$((p \wedge q) \vee r)$
$\neg\neg\neg p$
$\neg(p \vee \neg r) \wedge r$

3.5 Example
None of the following are formulas:
$(p \vee q\wedge)$
$(p \wedge q \vee r)$
$\neg \vee \neg p$
$\neg(p \vee \neg r) \wedge r\neg$

Exercise 24
Which of the following are formulas? Justify your answers.
$r \vee p \wedge p$
$r \vee (p \wedge r)$
$\neg r \vee p\neg$
$((p \wedge p) \wedge (p \wedge p))$

3.6 Definition
Let $\mathbb{T} = \{0, 1\}$. We call it the set of *truth values*: *false*, and *true*, respectively.

An *assignment* is a function $\mathcal{A} : \mathbf{P} \to \mathbb{T}$.

Given an assignment $\mathcal{A}$, we extend it to $\mathcal{A}' : \mathbf{F} \to \mathbb{T}$.

1. $\mathcal{A}'(p) = \mathcal{A}(p)$ for each $p \in \mathbf{P}$
2. $\mathcal{A}'(F \wedge G) = \begin{cases} 1, & \text{if } \mathcal{A}'(F) = 1 \text{ and } \mathcal{A}'(G) = 1 \\ 0, & \text{otherwise} \end{cases}$
3. $\mathcal{A}'(F \vee G) = \begin{cases} 1, & \text{if } \mathcal{A}'(F) = 1 \text{ or } \mathcal{A}'(G) = 1 \\ 0, & \text{otherwise} \end{cases}$

4. $\mathcal{A}'(\neg F) = \begin{cases} 1, & \text{if } \mathcal{A}'(F) = 0 \\ 0, & \text{otherwise} \end{cases}$

[From now on, drop distinction between $\mathcal{A}$ and $\mathcal{A}'$.]

3.7 Example
Let $\mathcal{A}(p) = \mathcal{A}(q) = 1$ and $\mathcal{A}(r) = 0$.

$$\begin{aligned} \mathcal{A}(\neg(p \wedge q) \vee \neg r) &= \begin{cases} 1, & \text{if } \mathcal{A}(\neg(p \wedge q)) = 1 \text{ or } \mathcal{A}(\neg r) = 1 \\ 0, & \text{otherwise} \end{cases} \\ &= \begin{cases} 1, & \text{if } \mathcal{A}(p \wedge q) = 0 \text{ or } \mathcal{A}(r) = 0 \\ 0, & \text{otherwise} \end{cases} \\ &= \begin{cases} 1, & \text{if } \mathcal{A}(p) = 0 \text{ or } \mathcal{A}(q) = 0 \text{ or } \mathcal{A}(r) = 0 \\ 0, & \text{otherwise} \end{cases} \\ &= 1 \end{aligned}$$

Exercise 25
Do the calculation from Example 3.7 for the formula $\neg(r \vee \neg p) \vee \neg q$ and the values $\mathcal{A}(r) = 1$ and $\mathcal{A}(p) = \mathcal{A}(q) = 0$.

3.8 Remark
The same thing can be expressed via *truth tables*.

$\mathcal{A}(F)$	$\mathcal{A}(G)$	$\mathcal{A}(F \wedge G)$
0	0	0
0	1	0
1	0	0
1	1	1

$\mathcal{A}(F)$	$\mathcal{A}(G)$	$\mathcal{A}(F \vee G)$
0	0	0
0	1	1
1	0	1
1	1	1

$\mathcal{A}(F)$	$\mathcal{A}(\neg F)$
0	1
1	0

3.9 Example
Determining the truth values of formulas using truth tables:

$\mathcal{A}(p)$	$\mathcal{A}(q)$	$\mathcal{A}(r)$	$\mathcal{A}(p \wedge q)$	$\mathcal{A}(\neg(p \wedge q))$	$\mathcal{A}(\neg r)$	$\mathcal{A}(\neg(p \wedge q) \vee \neg r)$
0	0	0	0	1	1	1
0	0	1	0	1	0	1
0	1	0	0	1	1	1
0	1	1	0	1	0	1
1	0	0	0	1	1	1
1	0	1	0	1	0	1
1	1	0	1	0	1	1
1	1	1	1	0	0	0

Exercise 26
Make the truth table for the formula from Exercise 25.

3.10 Remark
The truth value of a formula is uniquely determined by the truth values of the propositional variables it contains as subformulas.

3.11 Definition
Two Formulas F and G are (*semantically*) *equivalent* (written $F \equiv G$) if for every assignment $\mathcal{A}$ we have $\mathcal{A}(F) = \mathcal{A}(G)$.

3.12 Example
$p \vee q \equiv q \vee p$.

We can show that this equivalence holds by looking at the truth table for both formulas:

$\mathcal{A}(p)$	$\mathcal{A}(q)$	$\mathcal{A}(p \vee q)$	$\mathcal{A}(q \vee p)$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	1

3.13 Example
$p \vee \neg p \equiv q \vee \neg q$.

This can also be shown via truth table.

$\mathcal{A}(p)$	$\mathcal{A}(q)$	$\mathcal{A}(\neg p)$	$\mathcal{A}(\neg q)$	$\mathcal{A}(p \vee \neg p)$	$\mathcal{A}(q \vee \neg q)$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	1	1
1	1	0	0	1	1

3.14 Example
$(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$.

This can also be shown via truth table.

$\mathcal{A}(p)$	$\mathcal{A}(q)$	$\mathcal{A}(r)$	$\mathcal{A}(q \wedge r)$	$\mathcal{A}((p \vee (q \wedge r)))$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	1
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

$\mathcal{A}(p)$	$\mathcal{A}(q)$	$\mathcal{A}(r)$	$\mathcal{A}(p \vee q)$	$\mathcal{A}((p \vee r))$	$\mathcal{A}(((p \vee q) \wedge (p \vee r)))$
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	1	0	0
0	1	1	1	1	1
1	0	0	1	1	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	1	1

3.15 Theorem
The following hold for all formulas F, G, and H.

$F \wedge F \equiv F$	$F \vee F \equiv F$	idempotency
$F \wedge G \equiv G \wedge F$	$F \vee G \equiv G \vee F$	commutativity
$(F \wedge G) \wedge H \equiv F \wedge (G \wedge H)$	$(F \vee G) \vee H \equiv F \vee (G \vee H)$	associativity
$F \wedge (G \vee H) \equiv (F \wedge G) \vee (F \wedge H)$	$F \vee (G \wedge H) \equiv (F \vee G) \wedge (F \vee H)$	distributivity
$\neg\neg F \equiv F$		involution
$\neg(F \wedge G) \equiv \neg F \vee \neg G$	$\neg(F \vee G) \equiv \neg F \wedge \neg G$	de Morgan's Laws

Proof: Straightforward using truth tables. ■

3.16 Remark
Theorem 3.15 is very similar to Proposition 1.22.

We will sometimes omit brackets when it cannot cause confusion. E.g., we will write $p \vee q \vee r$. However, a statement like $p \vee q \wedge r$ is *not* allowed because it is ambiguous:

$\mathcal{A}(p)$	$\mathcal{A}(q)$	$\mathcal{A}(r)$	$\mathcal{A}((p \vee q) \wedge r)$	$\mathcal{A}(p \vee (q \wedge r))$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	1
1	0	1	1	1
1	1	0	0	1
1	1	1	1	1

3.17 Example
We can now use the equalities from Theorem 3.15 to do calculations with formulas.

$\neg(F \wedge \neg G) \vee G \equiv \neg F \vee \neg\neg G \vee H$	de Morgan
$\equiv \neg F \vee G \vee G$	involution
$\equiv \neg F \vee G$	idempotency

Exercise 27
Show the following for all formulas F and G, by applying the equalities from Theorem 3.15: $\neg(\neg F \wedge \neg G) \equiv (G \vee F)$

Exercise 28 (no hand-in)
Show the following for all formulas F, G and H, by applying the equalities from Theorem 3.15:

$$(((G \vee H) \wedge F) \vee (F \wedge G)) \equiv F \wedge (G \vee H)$$

3.18 Remark
Define $F \uparrow G = \neg(F \wedge G)$—pronounced "$F$ nand G." Then we can express negation, disjunction, and conjunction using only "$\uparrow$", as follows.

$$\begin{aligned} \neg F &\equiv \neg(F \wedge F) \equiv F \uparrow F \\ F \vee G &\equiv \neg(\neg F \wedge \neg G) \equiv \neg F \uparrow \neg G \equiv (F \uparrow F) \uparrow (G \uparrow G) \\ F \wedge G &\equiv \neg\neg(F \wedge G) \equiv \neg(F \uparrow G) \equiv (F \uparrow G) \uparrow (F \uparrow G). \end{aligned}$$

This means that we don't need three symbols ($\neg$, $\vee$, $\wedge$)—one symbol ($\uparrow$) is enough.

Exercise 29
Define $F \downarrow G = \neg(F \vee G)$ ("nor"). Express negation, disjunction and conjunction using only "$\downarrow$".

3.19 Remark
Exclusive or can be expressed as $(F \vee G) \wedge \neg(F \wedge G)$.

Exercise 30
Show $(F \vee G) \wedge \neg(F \wedge G) \equiv (F \wedge \neg G) \vee (G \wedge \neg F)$.

3.20 Remark
The following connectives are commonly used as short notations. They are called *implication* and *equivalence*, respectively.

$$\begin{aligned} F \to G &= \neg F \vee G \\ F \leftrightarrow G &= (F \to G) \wedge (G \to F) \end{aligned}$$

3.21 Remark

$$\begin{aligned} F \to G &\equiv \neg F \vee G && \text{by definition} \\ &\equiv \neg F \vee \neg\neg G && \text{involution} \\ &\equiv \neg\neg G \vee \neg F && \text{commutativity} \\ &\equiv \neg G \to \neg F && \text{by definition} \end{aligned}$$

The equivalence $F \to G \equiv \neg G \to \neg F$ is called *contraposition*.

Exercise 31
Show $F \to (G \to H) \equiv (F \wedge G) \to H$.

4 Numbers

10/25/2011

So far, we have *used* numbers, but we have not defined them.

What are natural numbers? Let's define them recursively.

4.1 Definition (Peano axioms[11])
The following *axioms* define the natural numbers.

1. There is a natural number, denoted by 0.
2. Every natural number n has another natural number as *successor*, denoted by $S(n)$.
3. There is no natural number whose successor is 0.
4. If two natural numbers have the same successor, then they are identical.
5. If a set X contains 0, and for every natural number n also its successor $S(n)$, then the natural numbers are a subset of X.

The set of all natural numbers is denoted by $\mathbb{N}$.

4.2 Remark
The above definition still doesn't tell us what 0 or S are. Intuitively, 0 stands for *zero* and $S(n)$ stands for $n + 1$. In the following, we will use the notation $S(n)$ and $n + 1$ interchangeably.

4.3 Remark
We can rephrase the statements from Definition 4.1 as follows.

1. $0 \in \mathbb{N}$.
2. If $n \in \mathbb{N}$ then $n + 1 \in \mathbb{N}$.
3. There is no $n \in \mathbb{N}$ with $n + 1 = 0$.
4. If $n + 1 = m + 1$ then $n = m$. (In other words, S is injective.)
5. For any set X, if
   (1) $0 \in X$ and
   (2) for every $n \in X$ we have $n + 1 \in X$,
   then $\mathbb{N} \subseteq X$.

We omit redundant brackets and write, e.g., $0 + 1 + 1$ instead of $(0 + 1) + 1$.
We can now *define* addition and multiplication.

[11] Giuseppe Peano, Italian mathematician and logician, 1858–1932.

4.4 Definition
$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (a binary function, called *addition*, written infix) is defined recursively as follows. For all $n, m \in \mathbb{N}$ we define:

$$\begin{aligned} n + 0 &= n \\ n + S(m) &= S(n + m) \end{aligned}$$

4.5 Example
According to the definition just given we can calculate, for example:

$$\begin{aligned} (0+1+1+1)+(0+1+1) &= S(S(S(0))) + S(S(0)) \\ &= S(\quad S(S(S(0))) + S(0) \quad) \\ &= S(S(\quad S(S(S(0))) + 0 \quad)) \\ &= S(S(S(S(S(0))))) \\ &= 0+1+1+1+1+1 \end{aligned}$$

4.6 Definition
$\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (a binary function, called *multiplication*, written infix) is defined recursively as follows. For all $n, m \in \mathbb{N}$ we define:

$$\begin{aligned} n \cdot 0 &= 0 \\ n \cdot S(m) &= (n \cdot m) + n \end{aligned}$$

For convenience, we agree on the precedence of multiplication over addition, i.e., $m + n \cdot k$ is read as $m + (n \cdot k)$.

4.7 Example

$$\begin{aligned} (0+1)\cdot(0+1+1) &= S(0) \cdot S(S(0)) \\ &= (S(0) \cdot S(0)) + S(0) \\ &= (\quad (S(0) \cdot 0) + S(0) \quad) + S(0) \\ &= (\quad 0 + S(0) \quad) + S(0) \\ &= S(0+0) + S(0) \\ &= S(0) + S(0) \\ &= S(\quad S(0) \quad) \\ &= S(S(0)) \\ &= 0+1+1 \end{aligned}$$

Exercise 32
Calculate $(0+1+1)\cdot(0+1)$ using the equations in Definitions 4.4 and 4.6 only.

4.8 Definition
For convenience, we introduce the following symbols, called *digits*:

$$\begin{aligned} 0 &= 0 & 5 &= 4+1 \\ 1 &= 0+1 & 6 &= 5+1 \\ 2 &= 0+1+1 & 7 &= 6+1 \\ 3 &= 0+1+1+1 & 8 &= 7+1 \\ 4 &= 3+1 & 9 &= 8+1 \end{aligned}$$

4.9 Remark
It is now possible to show the following *laws of arithmetic* for all $k, m, n \in \mathbb{N}$.

$$\begin{aligned} n+0 &= n & n \cdot 1 &= n && \text{(unit laws)} \\ n+m &= m+n & n \cdot m &= m \cdot n && \text{(commutativity)} \\ k+(m+n) &= (k+m)+n & k \cdot (m \cdot n) &= (k \cdot m) \cdot n && \text{(associativity)} \\ k \cdot (m+n) &= (k \cdot m) + (k \cdot n) & & && \text{(distributivity)} \end{aligned}$$

10/27/2011

4.10 Remark
The Peano axioms are the most common way of formally introducing the natural numbers. However, it is possible to even go a step further and base the natural numbers in set theory. To do this, we only have to explain, using set theory, what 0 and S are, and then show that the Peano axioms are met.

We do this as follows. Note that in set theory everything is a set, so each natural number will be a set.

- We set $0 = \emptyset$. I.e., we *identify* 0 with the emptyset.
- For every natural number n, we set $S(n) = n \cup \{n\}$.

As sets, the natural numbers thus look as follows:

$$\begin{aligned} 0 &= \emptyset \\ 1 &= 0 \cup \{0\} = \{\emptyset\} \\ 2 &= 1 \cup \{1\} = 0 \cup \{0\} \cup \{0 \cup \{0\}\} = \{\emptyset, \{\emptyset\}\} = \{0, 1\} \\ 3 &= 2 \cup \{2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\} \\ 4 &= 3 \cup \{3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} = \{0, 1, 2, 3\} \end{aligned}$$

etc.

In this notation, we have $n = \{k \in \mathbb{N} \mid k < n\}$ for each $n \in \mathbb{N}$. Also, for each $n \in \mathbb{N}$ we have that n is a set of exactly n elements.

Exercise 33
Write the natural number 5 in set notation (not using any digits or the symbols S or $+$).

4.11 Definition
A list[12] $a_k a_{k-1} \dots a_0$ of digits represents a natural number n which is computed as follows:

$$n = ((\dots(a_k \cdot (9+1) + a_{k-1}) \cdot (9+1) + \dots) \cdot (9+1) + a_0)$$

This means, in particular, that $9 + 1 = 10$, i.e., we can rewrite this as follows:

$$n = ((\dots(a_k \cdot 10 + a_{k-1}) \cdot 10 + \dots) \cdot 10 + a_0)$$

4.12 Example

$$43562 = (((4 \cdot 10 + 3) \cdot 10 + 5) \cdot 10 + 6) \cdot 10 + 2$$

4.13 Definition
Using *exponents* (not defined here, but known from high school[13]), we can also write this as follows:

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_0$$

The representation just introduced is called the *decimal notation*.

4.14 Example

$$4259 = 4 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 9$$

4.15 Definition
Writing expressions like

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_0$$

is rather tedious. The following is a shortcut notation, called the *sum* notation:

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \qquad (= a_0 \cdot 10^0 + a_1 \cdot 10^1 + \dots + a_k \cdot 10^k)$$

Sometimes a notation like $\sum_{i=0}^{k} a_i \cdot 10^i$ is used.

The sum symbol $\sum_{i=5}^{9}$ can be read like a loop in a programming language. The $i = 5$ beneath the $\sum$-symbol initializes the "counter" i to 5. The 9 on top of the $\sum$-symbol is the (inclusive) exit criterion: i starts with 5 and runs to (including) 9. The value behind the $\sum$-symbol is added for each such i.

[12] What is a *list* of digits? This can also be defined easily using set theory: Let's first take a special symbol, say [], which stands for the *empty list*. Then we can define recursively:

- [] is a list of digits.
- If a is a digit and L a list of digits, then the pair (a, L) is a list of digits.

Lists are common data structures in Computer Science. If (a, L) is a (non-empty) list, then a is called the *head* of this list, while L is called the *tail* of this list.

[13] As a reminder: For all $k, n \in \mathbb{N}$, we have $n^0 = 1$, $n^1 = n$ and $n^{k+1} = n \cdot n^k$.

4.16 Example

$$\sum_{i=0}^{4} i = 0 + 1 + 2 + 3 + 4 = 10$$

$$\sum_{k=4}^{6} (k - 3) = (4 - 3) + (5 - 3) + (6 - 3) = 6$$

$$\sum_{i=1}^{5} 2 = 10$$

Exercise 34
Calculate the following.

(a) $\sum_{n=2}^{4} n^2$

(b) $\sum_{m=0}^{3} 2 \cdot m$

Exercise 35
Calculate the following.

(a) $5 \cdot \sum_{n=2}^{2} n^3$

(b) $\sum_{m=0}^{3} 3$

Exercise 36 (no hand-in)
Calculate the following.

$$\sum_{i=0}^{3} \left(\sum_{k=0}^{i} k \right)$$

4.17 Definition
The decimal notation using lists $a_k a_{k-1} \ldots a_0$, i.e.

$$a_k a_{k-1} \ldots a_0 = \sum_{i=0}^{k} a_i \cdot 10^i \qquad (= a_0 \cdot 10^0 + a_1 \cdot 10^1 + \ldots + a_k \cdot 10^k)$$

uses *base* 10. We indicate this (sometimes) by writing the number with a subscript 10, e.g., 1235_{10}. If a subscript is missing, we assume base 10 is used.

4.18 Definition
The *binary notation* uses base 2. In this case we use only 2 digits, namely 0 and 1 (called *binary digits*). In this case, a list $a_k a_{k-1} \ldots a_0$ of binary digits stands for the number

$$n = \sum_{i=0}^{k} a_i \cdot 2^i \qquad (= a_0 \cdot 2^0 + a_1 \cdot 2^1 + \ldots + a_k \cdot 2^k).$$

We indicate a binary number by a subscript 2.

4.19 Example
Calculate conversion from binary to decimal *from right to left.*

$$1011_2 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 = 1 + 2 + 0 + 8 = 11_{10}$$
$$100_2 = 0 \cdot 2^0 + 0 \cdot 2^1 \cdot 1 \cdot 2^2 = 0 + 0 + 4 = 4_{10}$$

Exercise 37
Convert 1100_2 and 11_2 to decimal notation.

4.20 Example
To calculate conversion from decimal to binary, *repeatedly divide by* 2*, keep only the integer value and note the remainders from right to left to obtain the result.*

11_{10} divided by 2 is 5_{10} with remainder $1(= a_0)$
5_{10} divided by 2 is 2_{10} with remainder $1(= a_1)$
2_{10} divided by 2 is 1_{10} with remainder $0(= a_2)$
1_{10} divided by 2 is 0_{10} with remainder $1(= a_3)$

The result is $a_3a_2a_1a_0 = 1011_2$.

26_{10} divided by 2 is 13_{10} with remainder $0(= a_0)$
13_{10} divided by 2 is 6_{10} with remainder $1(= a_1)$
6_{10} divided by 2 is 3_{10} with remainder $0(= a_2)$
3_{10} divided by 2 is 1_{10} with remainder $1(= a_3)$
1_{10} divided by 2 is 0_{10} with remainder $1(= a_4)$

The result is $a_4a_3a_2a_1a_0 = 11010_2$.

Exercise 38
Convert 17_{10} and 16_{10} to binary notation.

4.21 Definition
For any $n \in \mathbb{N}$ we can establish an *n-ary notation* (with base n). For this we need n digits. It is customary to use letters for digits standing for 10_{10} and higher. E.g., the 16-ary notation (called *hexadecimal notation*) uses the digits 0 to 9 as usual, and additionally the digits $\mathrm{A} = 10_{10}$, $\mathrm{B} = 11_{10}$, $\mathrm{C} = 12_{10}$, $\mathrm{D} = 13_{10}$, $\mathrm{E} = 14_{10}$, $\mathrm{F} = 15_{10}$. We use the base as subscript as before, i.e. $9\mathrm{AFD3}_{16}$ is a hexadecimal number. 11/01/2011

A number $m \in \mathbb{N}$ is expressed in n-ary notation by a list $a_k a_{k-1} \ldots a_0$ of (suitable) digits, where

$$a_k a_{k-1} \ldots a_0 = \sum_{i=0}^{k} a_i \cdot n^i \qquad (= a_0 \cdot n^0 + a_1 \cdot n^1 + \ldots + a_k \cdot n^k)$$

4.22 Example
Conversion from hexadecimal to decimal.

$$\begin{aligned} 4\mathrm{AF}_{16} &= \mathrm{F}_{16} \cdot 16^0_{10} + \mathrm{A}_{16} \cdot 16^1_{10} + 4_{16} \cdot 16^2_{10} \\ &= (15_{10} \cdot 1_{10}) + (10_{10} \cdot 16_{10}) + 4_{10} \cdot 256_{10} \\ &= 15_{10} + 160_{10} + 1024_{10} \\ &= 1199_{10} \end{aligned}$$

Exercise 39
Convert ABC_{16} and 1010_{16} to decimal notation.

4.23 Example
Conversion from decimal to hexadecimal.

$$\begin{aligned} 286_{10} \text{ divided by 16 is } 17_{10} \text{ with remainder } 14_{10} = \mathrm{E}_{16} (= a_0) \\ 17_{10} \text{ divided by 16 is } 1_{10} \text{ with remainder } 1 (= a_1) \\ 1_{10} \text{ divided by 16 is } 0_{10} \text{ with remainder } 1 (= a_2) \end{aligned}$$

The result is $a_2 a_1 a_0 = 11\mathrm{E}_{16}$.

Exercise 40
Convert 1024_{10} to hexadecimal notation.

Exercise 41 (no hand-in)
Convert 172_8 to decimal notation.

Exercise 42 (no hand-in)
Convert 172_{10} to notation using base 7.

4.24 Example
Conversion between binary and hexadecimal notations is actually very simple. It further helps to have the binary notation for the hexadecimal digits in mind:

$0 = 0$	$4 = 100_2$	$8 = 1000_2$	$\mathrm{C} = 1100_2$
$1 = 1$	$5 = 101_2$	$9 = 1001_2$	$\mathrm{D} = 1101_2$
$2 = 10_2$	$6 = 110_2$	$\mathrm{A} = 1010_2$	$\mathrm{E} = 1110_2$
$3 = 11_2$	$7 = 111_2$	$\mathrm{B} = 1011_2$	$\mathrm{F} = 1111_2$

When starting from a hexadecimal number, simply expand each digit separately into binary notation:

3	A	B	8	E_{16}
11	1010	1011	1000	1110_2

So $3AB8E_{16} = 111010101110001110_2$.

When converting from binary to hexadecimal, group the binary digits in groups of four (starting from the right), then convert each group separately.

$$\begin{array}{ccccc} & & 1011001000011111101_2 & & \\ 101 & 1001 & 0000 & 1111 & 1101_2 \\ 5 & 9 & 0 & F & D_{16} \\ & & 590FD_{16} & & \end{array}$$

Exercise 43
Convert ABC_{16} and 1010_{16} to binary notation.

Exercise 44
Convert 1100_2 and 11_2 to hexadecimal notation.

exam material stops here

Integers, Rationals, Reals

[Back to decimal notation for the following.]

4.25 Definition
We can define the set $\mathbb{Z}$ of *integers* as follows.[14]

- $\mathbb{N} \subseteq \mathbb{Z}$
- For each $x \in \mathbb{Z}$ there exists a unique $y \in \mathbb{Z}$ such that $x + y = 0$. We write y as $-x$ in this case (and call it the *inverse* (*with respect to addition*; *additive inverse*) of x). We abbreviate $x + (-y)$ as $x - y$.
- $\mathbb{Z}$ is as small as possible.

4.26 Example
The inverse of 5 is -5. Writing $7 - 3$ is a shortcut notation for $7 + (-3)$.

11/03/2011

4.27 Proposition
For $\mathbb{Z}$, the following hold.

- Both addition and multiplication are associative, commutative, and have units.
- The distributive law $x \cdot (y + z) = x \cdot y + x \cdot z$ holds for all $x, y, z \in \mathbb{Z}$.
- Every $x \in \mathbb{Z}$ has an additive inverse $-x$.

So what about multiplicative inverses? If we furthermore force the existence of multiplicative inverses, then this gives rise to the rational numbers.

[14] The integers—and also the rationals and reals—can also be defined entirely using set theory, but we will not cover this here.

4.28 Definition
We can define the set $\mathbb{Q}$ of *rational numbers* as follows.

- $\mathbb{Z} \subseteq \mathbb{Q}$
- For each $x \in \mathbb{Q}$ there exists a unique $y \in \mathbb{Q}$ such that $x \cdot y = 1$. We write y as $\frac{1}{x}$ in this case (and call it the *inverse* (*with respect to multiplication*; *multiplicative inverse*) of x). We abbreviate $x \cdot \frac{1}{y}$ as $\frac{x}{y}$ or as $x : y$.
- $\mathbb{Q}$ is as small as possible.

4.29 Example
The multiplicative inverse of -4 is $-\frac{1}{4}$. The multiplicative inverse of $\frac{3}{4} = 3 \cdot \frac{1}{4}$ is $\frac{1}{3} \cdot 4 = \frac{4}{3}$.

4.30 Proposition
For $\mathbb{Q}$, the following hold.

- Both addition and multiplication are associative, commutative, and have units.
- The distributive law $x \cdot (y + z) = x \cdot y + x \cdot z$ holds for all $x, y, z \in \mathbb{Q}$.
- Every $x \in \mathbb{Q}$ has an additive inverse $-x$, and every $x \in \mathbb{Q} \setminus \{0\}$ has a multiplicative inverse $\frac{1}{x}$.

rest of section skipped

4.31 Remark
We can recover the usual decimal notation for rationals as follows: Two lists of digits joined by a dot, written $a_k a_{k-1} \dots a_0 . b_1 b_2 \dots b_m$, denote a rational number n as follows.

$$n = \left(\sum_{i=0}^{k} a_i \cdot 10^i \right) + \left(\sum_{j=1}^{m} b_j \cdot \frac{1}{10^j} \right)$$

Using negative exponents (where x^{-n} stands for $\frac{1}{x^n}$), we can also write this as

$$n = \left(\sum_{i=0}^{k} a_i \cdot 10^i \right) + \left(\sum_{j=1}^{m} b_j \cdot 10^{-j} \right).$$

Note, however, that this notation does not cover all rational numbers: The fraction $\frac{1}{3}$ is not expressible in this way. To cover all rational numbers, we also have to allow representations of the form

$$a_k a_{k-1} \dots a_0 . b_1 b_2 \dots b_m \overline{c_1 c_2 \dots c_l}$$

which stands for the number

$$n = \left(\sum_{i=0}^{k} a_i \cdot 10^i \right) + \left(\sum_{i=1}^{m} b_i \cdot 10^{-i} \right) + \left(\sum_{i=0}^{\infty} \left(10^{-m+i \cdot l} \cdot \sum_{j=1}^{l} c_j \cdot 10^{-j} \right) \right).$$

It obviously needs a formal proof that this form of representation is meaningful and exhaustive for $\mathbb{Q}$. But this is out of scope for this lecture.

4.32 Example

$$314.159 = 3 \cdot 10^2 + 1 \cdot 10^1 + 4 \cdot 10^0 + \frac{1}{10} + \frac{5}{10^2} + \frac{9}{10^3}$$
$$\frac{169}{75} = 2.25\overline{3} = 2 \cdot 10^0 + \frac{2}{10} + \frac{5}{10^2} + \frac{3}{10^3} + \frac{3}{10^4} + \frac{3}{10^5} + \frac{3}{10^6} + \dots$$

4.33 Remark
The decimal representation of rational numbers is not unique since, e.g., $0.\overline{9} = 1$.

4.34 Definition
Given $k, n \in \mathbb{N}$ with $n \neq 0$, we say that k *is divisible by* n if $\frac{k}{n} \in \mathbb{N}$. In this case, we call n a *divisor* of k.

By $D(k)$ we denote the set of all divisors of k, i.e.

$$D(k) = \left\{ n \in \mathbb{N} \setminus \{0\} \mid \frac{k}{n} \in \mathbb{N} \right\}.$$

4.35 Example

$$D(1) = \{1\}$$
$$D(2) = \{1, 2\}$$
$$D(6) = \{1, 2, 3, 6\}$$
$$D(10) = \{1, 2, 5, 10\}$$

Exercise 45
Determine $D(0)$ and $D(12)$.

4.36 Definition
A number $p \in \mathbb{N} \setminus \{0, 1\}$ is called a *prime number* if $D(p) = \{1, p\}$. We denote the set of prime numbers by $\mathbb{P}$.

4.37 Remark
A number $p \in \mathbb{N}$ is a prime number if and only if $|D(p)| = 2$.

4.38 Remark

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 15, 17, 19, 23, 29, 31, 37, \dots\}$$

4.39 Theorem (Fundamental Theorem of Arithmetic[15])
Every $n \in \mathbb{N} \setminus \{0\}$ can be written as a unique product (up to the ordering of the factors) of prime numbers. This product is called the *prime factorization* of n.

[15]This goes back to the ancient Egyptians, more than 3,500 years ago.

4.40 Example

$$12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$$
$$28 = 2 \cdot 2 \cdot 7 = 2^2 \cdot 7$$
$$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$$

Exercise 46
Determine the prime factorizations of the numbers 112, 128, 86, and 17.

4.41 Theorem
$|\mathbb{P}| = |\mathbb{N}|$, i.e., the set of all prime numbers is countably infinite.

Proof:[16] It suffices to show that for each $p \in \mathbb{P}$ there exists a $q \in \mathbb{P}$ with $p < q$.

So let $p \in \mathbb{P}$ be any prime number. We need to show that there is a larger prime number.

Denote the n-th prime number (in ascending order) by p_n, i.e., $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc. Then there is a k with $p = p_k$. Now consider the number

$$r = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1,$$

which is divisible by 1 and by r, but not divisible by any of the prime number $p_1, \ldots, p_k$.

We consider two cases.

(1) If r is a prime number, then this completes the proof since $r > p$ as required.

(2) If r is not a prime number, then by Theorem 4.39 it must be divisible by a prime number $q > p$, which also completes the proof. ■

4.42 Theorem
There is no $x \in \mathbb{Q}$ with $x^2 = 2$.

Proof: We give a proof by contradiction. Assume there is $x = \frac{p}{q} \in \mathbb{Q}$ with $x^2 = 2$.

We can assume without loss of generality that $p, q \in \mathbb{N}$ and that at least one of p and q is odd: If both are even, then repeatedly reduce the fraction $\frac{p}{q}$ by 2 (i.e., divide both p and q by 2) until this condition is satisfied.

Then we have

$$2 = \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2}$$

and hence

$$2 \cdot q^2 = p^2.$$

Consequently, p^2 must be even, which implies that p must be even (since squares of odd numbers are always odd).

Therefore, there exists $k \in \mathbb{N}$ with $p = 2 \cdot k$, and we obtain

$$2 \cdot q^2 = p^2 = (2 \cdot k)^2 = 2 \cdot 2 \cdot k^2$$

[16] Euclid (of Alexandria), ca. 300 BC, Greek mathematician, the "Father of Geometry."

and therefore

$$q^2 = 2 \cdot k^2,$$

which means that q is even.

We have just shown that both p and q are even, which contradicts our earlier statement that one of p and q must be odd.

Hence, there can be no $x \in \mathbb{Q}$ with $x^2 = 2$. ■

So how can we define the real numbers? Since we defined the rationals by "adding fractions" to the integers, can we do the same to define the reals, i.e., "add square roots" to the rational numbers to define the reals?

It turns out that defining the real numbers is much more complicated, but discussing this is out of scope for this lecture. We thus take a "pragmatic" approach to defining the reals, which is not as mathematically concise.

In decimal notation, real numbers can be written as two lists of digits joined by a dot, where the first list is finite, and the second list is infinite (i.e., a *sequence*):

$$a_k a_{k-1} \ldots a_0 . b_1 b_2 b_3 b_4 \ldots$$

Such a real number r can be understood as the result of the (infinite) sum

$$r = \left(\sum_{i=0}^{k} a_k \right) + \left(\sum_{j=1}^{\infty} b_j \cdot 10^{-j} \right) = \left(\sum_{i=0}^{k} a_k \right) + \frac{b_1}{10} + \frac{b_2}{10^2} + \frac{b_3}{10^3} + \ldots .$$

It clearly requires further explanations why it makes sense to form such infinite sums (and what it means), but we will leave this to the mathematicians.

Recall that this representation is not unique, e.g., $0.999999\ldots = 1.0000\ldots$.

4.43 Example

$$\begin{aligned} \pi &= 3.1415926535\ldots \\ \sqrt{2} &= 1.4142135\ldots \\ \frac{5}{4} &= 1.25000000\ldots = 1.24999999\ldots \end{aligned}$$

11/03/2011

5 Lists and Trees

5.1 Definition

Given a set X, we can recursively define *lists* over X, as follows.

- λ is a list, called the *empty list*.
- If $a \in X$ and L is a list, then the pair (a, L) is a list.

If (a, L) is a (non-empty) list, then a is called the *head* of this list, while L is called the *tail* of this list. We denote the set of all lists over X by $\mathbb{L}_X$.

5.2 Example
The following are lists over $\mathbb{N}$.

$$(1, (2, (4, (3, \lambda))))$$
$$(5, (4, (3, (2, \lambda))))$$
$$(0, \lambda)$$
$$\lambda$$

5.3 Notation
If

$$(a_1, (a_2, (a_3, (\ldots (a_{k-1}, (a_k, \lambda)) \ldots))))$$

is a list, then we can also write this list as

$$[a_1, a_2, a_3, \ldots, a_{k-1}, a_k].$$

5.4 Example

$$(1, (2, (4, (3, \lambda)))) = [1, 2, 4, 3]$$
$$(5, (4, (3, (2, \lambda)))) = [5, 4, 3, 2]$$
$$(0, \lambda) = [0]$$
$$\lambda = \lambda$$

Exercise 47
Convert the lists $[3, 4, 3]$ and $(6, (5, \lambda))$ into the (respective) other notation, as just introduced.

5.5 Definition
We define the following functions.

$$\text{head} : \mathbb{L}_X \to X : (h, L) \mapsto h$$
$$\text{tail} : \mathbb{L}_X \to \mathbb{L}_X : (h, L) \mapsto L$$
$$\text{cons} : X \times \mathbb{L}_X \to \mathbb{L}_X : (a, L) \mapsto (a, L)$$

5.6 Example

$$\text{head}([2, 6, 7]) = 2$$
$$\text{tail}([2, 6, 7]) = [6, 7]$$
$$\text{cons}(3, [2, 6, 7]) = [3, 2, 6, 7]$$

Exercise 48
Determine head($[6, 8, 3, 4]$), tail($[3]$) and cons$(5, \lambda)$.

5.7 Definition
We define recursively the function length : $\mathbb{L}_X \to \mathbb{N}$:

$$\begin{aligned} \text{length}(\lambda) &= 0 \\ \text{length}(\text{cons}(h, T)) &= 1 + \text{length}(T) \end{aligned}$$

5.8 Example

$$\begin{aligned} \text{length}([a, b, c, d]) &= 1 + \text{length}([b, c, d]) \\ &= 1 + 1 + \text{length}([c, d]) \\ &= 1 + 1 + 1 + \text{length}([d]) \\ &= 1 + 1 + 1 + 1 + \text{length}(\lambda) \\ &= 4 \end{aligned}$$

Exercise 49
Determine length$([a, a, a])$.

5.9 Remark
length : $\mathbb{L}_X \to \mathbb{N}$ is surjective, but not injective.

5.10 Definition
We define recursively the function $\circ : \mathbb{L}_X \times \mathbb{L}_X \to \mathbb{L}_X$ (written infix, and called the *concatenation* or *append* function):

$$\begin{aligned} \lambda \circ L &= L \\ (h, T) \circ L &= \text{cons}(h, T \circ L) \end{aligned}$$

5.11 Example

$$\begin{aligned} [1, 2] \circ [a, b, c] &= (1, [2] \circ [a, b, c]) \\ &= (1, (2, \lambda \circ [a, b, c])) \\ &= (1, (2, [a, b, c])) \\ &= [1, 2, a, b, c] \end{aligned}$$

Exercise 50
Determine $[a, b, a] \circ [a, a, b]$.

5.12 Definition
We define recursively the function reverse : $\mathbb{L}_X \to \mathbb{L}_X$:

$$\begin{aligned} \text{reverse}(\lambda) &= \lambda \\ \text{reverse}(\text{cons}(h, T)) &= \text{reverse}(T) \circ [h] \end{aligned}$$

5.13 Example

$$\begin{aligned}\text{reverse}([a,b,c]) &= \text{reverse}([b,c]) \circ [a] \\ &= (\text{reverse}([c]) \circ [b]) \circ [a] \\ &= ((\text{reverse}(\lambda) \circ [c]) \circ [b]) \circ [a] \\ &= ((\lambda \circ [c]) \circ [b]) \circ [a] \\ &= ([c] \circ [b]) \circ [a] \\ &= [c,b] \circ [a] \\ &= [c,b,a]\end{aligned}$$

Exercise 51
Determine reverse($[a]$).

5.14 Remark
reverse : $\mathbb{L}_X \to \mathbb{L}_X$ is injective and surjective, and thus bijective.

Exercise 52
Give a recursive definition for the function aggsum : $\mathbb{L}_{\mathbb{N}} \to \mathbb{N}$ which calculates the sum of all the numbers occuring in the list. E.g., aggsum$([3,6,3,2]) = 14$.

5.15 Remark
The concatenation function "$\circ$" is associative and has a (left and right) unit λ, but it is not commutative, and there are no inverses other than for λ.

end of lecture material

5.16 Definition
A *multiset* (or *bag*) M is a pair (X, m), where X is a set and $f : X \to \mathbb{N} \setminus \{0\}$ is a function. For each $x \in X$, $f(x)$ is called the *multiplicity* of x in M.

5.17 Notation
We indicate multisets by the notation $\langle a_0, a_1, a_2, \ldots, a_n \rangle$, where $a_1, \ldots, a_n \in X$. If an element a_i occurs multiple times, then the number of occurrences is the multiplicity $m(a_i)$ of a_i. Note that the order of appearance of elements in this notation is irrelevant. The *empty multiset* $(\emptyset, \emptyset)$ is denoted by μ.

5.18 Example
The multiset

$$(\{a,c,d\}, \{(a,2),(c,1),(d,3)\})$$

can be written as

$$\langle a,a,c,d,d,d \rangle$$

or also as

$$\langle a,c,d,d,d,a \rangle$$

or

$$\langle d,a,a,d,d,c \rangle$$

etc.

Exercise 53
Give the multiplicity of each of the elements in the multiset

$$\langle 0, 1, 1, 2, 2, 2, 2, 3, 3\rangle.$$

5.19 Definition
The following function mset2set maps multisets to sets.

$$\text{mset2set}((X, m)) = X.$$

5.20 Example

$$\text{mset2set}(\langle a, a, c, d, d, d\rangle) = \{a, c, d\}$$

5.21 Definition
The following function adds an element a to a multiset (X, m).

$$\text{msetadd}(a, (X, m)) = (X \cup \{a\}, m'),$$

where

$$m' : X \cup \{a\} \to \mathbb{N} : x \mapsto \begin{cases} m(x) & \text{if } x \neq a \\ m(a) + 1 & \text{if } x = a \in X \\ 1 & \text{if } x = a \notin X \end{cases}$$

5.22 Example

$$\begin{aligned} \text{msetadd}(b, \langle a, a, c, d, d, d\rangle) &= \langle a, a, b, c, d, d, d\rangle \\ \text{msetadd}(a, \langle a, a, c, d, d, d\rangle) &= \langle a, a, a, c, d, d, d\rangle \end{aligned}$$

5.23 Definition
The following function "$\sqcup$" (written infix) defines *multiset union* of two multisets.

$$\begin{aligned} \mu \sqcup M &= M \\ \text{msetadd}(a, N) \sqcup M &= N \sqcup \text{msetadd}(a, M) \end{aligned}$$

5.24 Example

$$\begin{aligned} \langle a, a, b\rangle \sqcup \langle a, c, d, d\rangle &= \text{msetadd}(a, \langle a, b\rangle) \sqcup \langle a, c, d, d\rangle \\ &= \langle a, b\rangle \sqcup \text{msetadd}(a, \langle a, c, d, d\rangle) \\ &= \langle a, b\rangle \sqcup \langle a, a, c, d, d\rangle \\ &= \langle b\rangle \sqcup \text{msetadd}(a, \langle a, a, c, d, d\rangle) \\ &= \langle b\rangle \sqcup \langle a, a, a, c, d, d\rangle \\ &= \mu \sqcup \text{msetadd}(b, \langle a, a, a, c, d, d\rangle) \\ &= \mu \sqcup \langle a, a, a, b, c, d, d\rangle \\ &= \langle a, a, a, b, c, d, d\rangle \end{aligned}$$

5.25 Definition
The following recursively defined function maps lists to the multiset of their elements.

$$\begin{aligned}\text{list2mset}(\lambda) &= \mu \\ \text{list2mset}(\text{cons}(h, T)) &= \text{msetadd}(h, \text{list2mset}(T))\end{aligned}$$

5.26 Example

$$\begin{aligned}\text{list2mset}([a,b,c,a]) &= \text{msetadd}(a, \text{list2mset}([b,c,a])) \\ &= \text{msetadd}(a, \text{msetadd}(b, \text{list2mset}([c,a]))) \\ &= \text{msetadd}(a, \text{msetadd}(b, \text{msetadd}(c, \text{list2mset}([a])))) \\ &= \text{msetadd}(a, \text{msetadd}(b, \text{msetadd}(c, \text{msetadd}(a, \text{list2mset}(\lambda))))) \\ &= \text{msetadd}(a, \text{msetadd}(b, \text{msetadd}(c, \text{msetadd}(a, \mu)))) \\ &= \text{msetadd}(a, \text{msetadd}(b, \text{msetadd}(c, \langle a \rangle))) \\ &= \text{msetadd}(a, \text{msetadd}(b, \langle a, c \rangle)) \\ &= \text{msetadd}(a, \langle a, b, c \rangle) \\ &= \langle a, a, b, c \rangle\end{aligned}$$

Exercise 54
Determine list2mset($[a, a, b, d, d, d]$).

Exercise 55
Determine mset2set(list2mset($[a, a, b, d, d, d]$)).

5.27 Definition
Given a set X, we can recursively define *binary trees* over X, as follows.

- τ is a binary tree, called the *empty tree*.
- If $r \in X$ and T_1 and T_2 are binary trees, then the triple (a, T_1, T_2) is a binary tree.

If $T = (r, T_1, T_2)$ is a (non-empty) binary tree, then r is called the *root* of the tree, while T_1 and T_2 are called the *left* and *right subtrees* of T. If T_1 (respectively, T_2) is non-empty, then its root is called the *left* (respectively, *right*) *successor* (or *child*) of r.

5.28 Definition
We define the following functions on trees over X as follows, where the first results in a multiset of trees over X, and the second results in a multiset of elements of X.

$$\begin{aligned}\text{subtrees}(\tau) &= \mu \\ \text{subtrees}((r, T_1, T_2)) &= \langle (r, T_1, T_2) \rangle \sqcup \text{subtrees}(T_1) \sqcup \text{subtrees}(T_2)\end{aligned}$$

$$\begin{aligned}\text{nodes}(\tau) &= \mu \\ \text{nodes}((r, T_1, T_2)) &= \langle r \rangle \sqcup \text{nodes}(T_1) \sqcup \text{nodes}(T_2)\end{aligned}$$

Given a tree T, we call subtrees(T) the multiset of *subtrees* of T, and we call nodes(T) the multiset of all *nodes* of T.

The multiset of all *leaves* of of a tree is defined as follows.

$$\begin{aligned}
\text{leaves}(\tau) &= \mu \\
\text{leaves}((r, \tau, \tau)) &= \langle r \rangle \\
\text{leaves}((r, T_1, T_2)) &= \text{leaves}(T_1) \sqcup \text{leaves}(T_2) \qquad \text{if } T_1 \neq \tau \text{ or } T_2 \neq \tau
\end{aligned}$$

5.29 Example
For

$$T = (5, (3, (1, \tau, \tau), (4, \tau, \tau)), (9, (7, \tau, (8, \tau, \tau)), (12, (10, \tau, \tau), \tau)))$$

we have

$$\begin{aligned}
\text{nodes}(T) &= \langle 5, 3, 1, 4, 9, 7, 8, 12, 10 \rangle \\
\text{subtrees}(T) &= \langle T, (3, (1, \tau, \tau), (4, \tau, \tau)), \\
&\qquad (1, \tau, \tau), (4, \tau, \tau) \rangle \\
&\qquad (9, (7, \tau, (8, \tau, \tau)), (12, (10, \tau, \tau), \tau)) \\
&\qquad (7, \tau, (8, \tau, \tau)), (8, \tau, \tau) \\
&\qquad (12, (10, \tau, \tau), \tau), (10, \tau, \tau) \rangle
\end{aligned}$$

The leaves of T are $1, 4, 8, 10$.

5.30 Example
Arithmetic expressions can be understood as trees:

$$\begin{aligned}
x \cdot (5 + y) &= (\cdot, (x, \tau, \tau), (+, (5, \tau, \tau), (y, \tau, \tau))) \\
-(x + z) &= (-, (+, (x, \tau, \tau), (z, \tau, \tau)), \tau)
\end{aligned}$$

Expressions from the algebra of sets can be understood as trees:

$$(M \cup N^{\mathsf{c}}) \cap (N \cup A)^{\mathsf{c}} = (\cap, (\cup, (M, \tau, \tau), (\mathsf{c}, (N, \tau, \tau), \tau)), (\mathsf{c}, (\cup, (N, \tau, \tau), (A, \tau, \tau)), \tau))$$

Note, that the leaves are the sets occurring in the expression.

Logical formulas can be understood as trees:

$$(p \vee \neg q) \wedge p = (\wedge, (\vee, (p, \tau, \tau), (\neg, (q, \tau, \tau), \tau)), (p, \tau, \tau))$$

Note that the leaves are the boolean variables occurring in the expression.

Exercise 56
Write the following as trees: $((A^{\mathsf{c}})^{\mathsf{c}})^{\mathsf{c}} \cap A, \quad 1 + (1 + 1), \quad (1 + 1) + 1$

5.31 Definition
We define the following two functions, which assign natural numbers to trees.

$$\begin{aligned} \mathrm{size}(\tau) &= 0 \\ \mathrm{size}((r, T_1, T_2)) &= 1 + \mathrm{size}(T_1) + \mathrm{size}(T_2) \end{aligned}$$

$$\begin{aligned} \mathrm{depth}(\tau) &= 0 \\ \mathrm{depth}((r, T_1, T_2)) &= 1 + \max\{\mathrm{depth}(T_1), \mathrm{depth}(T_2)\} \end{aligned}$$

For the latter, $\max A$, for a finite $A \subseteq \mathbb{N}$, denotes the largest number in the set A.

5.32 Example

$$\begin{aligned} &\mathrm{size}((\cdot,(x,\tau,\tau),(+,(5,\tau,\tau),(y,\tau,\tau)))) \\ &\quad = 1 + \mathrm{size}((x,\tau,\tau)) + \mathrm{size}((+,(5,\tau,\tau),(y,\tau,\tau))) \\ &\quad = 1 + (1 + \mathrm{size}(\tau) + \mathrm{size}(\tau)) + (1 + \mathrm{size}((5,\tau,\tau)) + \mathrm{size}((y,\tau,\tau))) \\ &\quad = 1 + (1 + 0) + (1 + (1 + \mathrm{size}(\tau) + \mathrm{size}(\tau)) + (1 + \mathrm{size}(\tau) + \mathrm{size}(\tau))) \\ &\quad = 1 + (1 + 0 + 0) + (1 + (1 + 0 + 0) + (1 + 0 + 0)) \\ &\quad = 5 \end{aligned}$$

$$\begin{aligned} &\mathrm{depth}((\cdot,(x,\tau,\tau),(+,(5,\tau,\tau),(y,\tau,\tau)))) \\ &\quad = 1 + \max\{\mathrm{depth}((x,\tau,\tau)), \mathrm{depth}((+,(5,\tau,\tau),(y,\tau,\tau)))\} \\ &\quad = 1 + \max\{1 + \max\{\mathrm{depth}(\tau), \mathrm{depth}(\tau)\}, 1 + \max\{\mathrm{depth}((5,\tau,\tau)), \mathrm{depth}((y,\tau,\tau))\}\} \\ &\quad = 1 + \max\{1 + \max\{0, 0\}, 1 + \max\{\mathrm{depth}((5,\tau,\tau)), \mathrm{depth}((y,\tau,\tau))\}\} \\ &\quad = 1 + \max\{1 + 0, 1 + \max\{\mathrm{depth}((5,\tau,\tau)), \mathrm{depth}((y,\tau,\tau))\}\} \\ &\quad = 1 + \max\{1, 1 + \max\{1 + \max\{\mathrm{depth}(\tau), \mathrm{depth}(\tau)\}, 1 + \max\{\mathrm{depth}(\tau), \mathrm{depth}(\tau)\}\} \\ &\quad = 1 + \max\{1, 1 + \max\{1 + \max\{0, 0\}, 1 + \max\{0, 0\}\}\} \\ &\quad = 1 + \max\{1, 1 + \max\{1 + 0, 1 + 0\}\} \\ &\quad = 1 + \max\{1, 1 + \max\{1, 1\}\} \\ &\quad = 1 + \max\{1, 1 + 1\} \\ &\quad = 1 + \max\{1, 2\} \\ &\quad = 1 + 2 \\ &\quad = 3 \end{aligned}$$

Exercise 57
Determine $\mathrm{size}(((A^{\mathsf{c}})^{\mathsf{c}})^{\mathsf{c}} \cap A)$ and $\mathrm{depth}(((A^{\mathsf{c}})^{\mathsf{c}})^{\mathsf{c}} \cap A)$.

5.33 Definition
The following defines a function which associates with each tree a *list* of its nodes. The function is called *depth-first traversal*.

$$\begin{aligned} \mathrm{dft}(\tau) &= \lambda \\ \mathrm{dft}((r, T_1, T_2)) &= [r] \circ \mathrm{dft}(T_1) \circ \mathrm{dft}(T_2) \end{aligned}$$

5.34 Example

$$\begin{aligned}
&\mathrm{dft}((1,(2,(3,\tau,\tau),(4,\tau,\tau)),(5,(6,\tau,\tau),(7,\tau,\tau))))\\
&\qquad = [1]\circ\mathrm{dft}((2,(3,\tau,\tau),(4,\tau,\tau)))\circ\mathrm{dft}((5,(6,\tau,\tau),(7,\tau,\tau)))\\
&\qquad = [1]\circ[2]\circ\mathrm{dft}((3,\tau,\tau))\circ\mathrm{dft}((4,\tau,\tau))\circ[5]\circ\mathrm{dft}((6,\tau,\tau))\circ\mathrm{dft}((7,\tau,\tau))\\
&\qquad = [1]\circ[2]\circ[3]\circ\mathrm{dft}(\tau)\circ\mathrm{dft}(\tau)\circ[4]\circ\mathrm{dft}(\tau)\circ\mathrm{dft}(\tau)\circ\\
&\qquad\qquad\qquad\qquad\circ[5]\circ[6]\circ\mathrm{dft}(\tau)\circ\mathrm{dft}(\tau)\circ[7]\circ\mathrm{dft}(\tau)\circ\mathrm{dft}(\tau)\\
&\qquad = [1,2,3]\circ\lambda\circ\lambda\circ[4]\circ\lambda\circ\lambda\circ[5,6]\circ\lambda\circ\lambda\circ[7]\circ\lambda\circ\lambda\\
&\qquad = [1,2,3,4,5,6,7]
\end{aligned}$$

Exercise 58
Calculate

$$\mathrm{dft}((\cdot,(x,\tau,\tau),(+,(5,\tau,\tau),(y,\tau,\tau)))).$$

5.35 Definition
The following defines another function which associates with each tree a *list* of its nodes. The function is called *breadth-first traversal*.

$$\begin{aligned}
\mathrm{bft}(T) &= \mathrm{bftL}([T])\\
\mathrm{bftL}(\lambda) &= \lambda\\
\mathrm{bftL}(\mathrm{cons}(\tau,L)) &= \mathrm{bftL}(L)\\
\mathrm{bftL}(\mathrm{cons}((r,T_1,T_2),L)) &= [r]\circ\mathrm{bftL}(L\circ[T_1,T_2])
\end{aligned}$$

5.36 Example

$$\begin{aligned}
&\mathrm{bft}((1,(2,(4,\tau,\tau),(5,\tau,\tau)),(3,(6,\tau,\tau),(7,\tau,\tau))))\\
&\qquad = \mathrm{bftL}([(1,(2,(4,\tau,\tau),(5,\tau,\tau)),(3,(6,\tau,\tau),(7,\tau,\tau)))])\\
&\qquad = [1]\circ\mathrm{bftL}([(2,(4,\tau,\tau),(5,\tau,\tau)),(3,(6,\tau,\tau),(7,\tau,\tau))])\\
&\qquad = [1]\circ[2]\circ\mathrm{bftL}([(3,(6,\tau,\tau),(7,\tau,\tau))]\circ[(4,\tau,\tau),(5,\tau,\tau)])\\
&\qquad = [1,2]\circ[3]\circ\mathrm{bftL}([(4,\tau,\tau),(5,\tau,\tau)]\circ[(6,\tau,\tau),(7,\tau,\tau)])\\
&\qquad = [1,2,3]\circ[4]\circ\mathrm{bftL}([(5,\tau,\tau)]\circ[(6,\tau,\tau),(7,\tau,\tau)]\circ[\tau,\tau])\\
&\qquad = [1,2,3,4]\circ[5]\circ\mathrm{bftL}([(6,\tau,\tau),(7,\tau,\tau)]\circ[\tau,\tau]\circ[\tau,\tau])\\
&\qquad = [1,2,3,4,5]\circ[6]\circ\mathrm{bftL}([(7,\tau,\tau)]\circ[\tau,\tau]\circ[\tau,\tau]\circ[\tau,\tau])\\
&\qquad = [1,2,3,4,5,6]\circ[7]\circ\mathrm{bftL}([\tau,\tau]\circ[\tau,\tau]\circ[\tau,\tau]\circ[\tau,\tau])\\
&\qquad = [1,2,3,4,5,6,7]
\end{aligned}$$

Exercise 59
Calculate

$$\mathrm{bft}((\cdot,(x,\tau,\tau),(+,(5,\tau,\tau),(y,\tau,\tau)))).$$