

## 1. Elementary Mathematics

**Babylonian problem:** Find the solutions of  $xy = p$  and  $x + y = s$ , i.e.

$$x(s - x) = p.$$

We all prefer the the quadratic form

$$x^2 - sx + p = 0.$$

Equivalently, we have

$$\left(x - \frac{s}{2}\right)^2 = \frac{s^2}{4} - p.$$

**Question 1):** What are the properties of the numbers we have use in this calculation?

**Question 2):** What are the properties of the numbers we allow for the solution?

**Question 3):** What happens if  $s = \sqrt{2}$ ,  $p = 2$ , i.e.  $s^2/4 - p = -1$ ?

**Babylonian tower:** Lets assume that instead of speaking different languages the new penalty is to replace numbers by  $2 \times 2$  matrices. Here an original number  $a$  is replaced by the matrix

$$\hat{a} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Thus in question 3) we are lead to find all matrices  $b$  such that

$$b^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

**Problem:** Find all those solutions and discuss what you don't like about this new babylonian system of numbers!

In the following we should discuss

### What are numbers?

**Comment:** This sounds like a simple question, but it isn't. We will discuss this for  $\mathbb{N}$  and  $\mathbb{Z}$  and learn a lot on the way. However, the amount of time spent to do this for  $\mathbb{Z}$  convinced me that is better to stop after  $\mathbb{Z}$  and use a pragmatic approach (of the textbook) and accept the real numbers with its properties for the time being. This allows us to follow concrete problem and solutions and leave the worry of constructing the real numbers for the end of the class (see Appendix). By the way we will also learn two different approaches to mathematical research-the conceptual and the problem oriented approach.

## 2. The natural numbers and some set theory

**Question:** What are natural numbers?

**Intuitive answer:** An infinite set with the domino effect.

### 2.1. Some set theory.

The empty set  $\emptyset$  is a set and then also

$$\{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \dots$$

The natural numbers is the collection of all objects obtained by this procedure. In set theory we deal with sets, objects and the symbol

$$x \in X$$

which holds if  $x$  is an element in  $X$ .

**DEFINITION 2.1.** *Let  $X, Y$  be sets. We say that  $Y$  is contained in  $X$  (short  $Y \subset X$ ) if*

$$\forall y (y \in Y \Rightarrow y \in X)$$

*holds. (Every element in  $Y$  is an element of  $X$ ).*

### Some set theoretic axioms:

- i) Let  $X$  be a set and  $x$  be an object, then either  $x \in X$  or  $x \notin X$ .
- ii) Let  $X$  be set and  $P(y)$  be a property. Then

$$Y = \{x \in X : P(x)\}$$

is a set.

- iii) Let  $X$  be a set. Then the power set

$$P(X) = \{A : A \subset X\}$$

is a set.

- iv) Let  $X$  and  $Y$  be sets. Then the product set

$$X \times Y = \{(x, y) : x \in X, y \in Y\}$$

- v) Let  $X$  and  $Y$  be sets. Then there exists a set  $Z$  such that  $X \subset Z$  and  $Y \subset Z$ .

**Project:** Find Russell's paradox of naive set theory.

**Applications 1)** The intersection

$$X \cap Y = \{x \in X : x \in Y\}$$

and the difference

$$X - Y = X \setminus Y = \{x \in X : x \notin Y\}$$

is a set.

**2)** If  $X \subset Z$  and  $Y \subset Z$  are sets, then we may define the union

$$X \cup Y = \{x \in Z : x \in X \text{ or } x \in Y\}.$$

(This is independent of the choice of  $Z$ ).

**Project:** Assume that for every set  $X$  there exists a set  $X_\infty$  such that  $X \subset X_\infty$  and  $\infty \in X_\infty - X$ . Then the union  $X \cup Y$  can be constructed in  $X_\infty \times Y_\infty$ . Why?

## 2.2. Axioms for the natural numbers.

If we want to formulate our domino principle we have to use the a successor function:

**DEFINITION 2.2.** *The natural numbers are given by a set  $\mathbb{N}$ , an origin  $0 \in \mathbb{N}$  and a function  $\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$  with the following properties*

i)  $\text{succ} : \mathbb{N} \rightarrow \mathbb{N}$  is injective, i.e.

$$\forall x, y \in \mathbb{N} : x \neq y \Rightarrow \text{succ}(x) \neq \text{succ}(y),$$

ii) Every element in  $\mathbb{N} - \{0\}$  is a successor, i.e.

$$\forall x \in \mathbb{N} : x \neq 0 \Rightarrow \exists y \in \mathbb{N} \text{succ}(y) = x,$$

but 1 is not a successor,

iii) (Induction principle) Let  $A$  be a subset of  $\mathbb{N}$  such that  $0 \in A$  and

$$\forall x \in A : x \in A \Rightarrow \text{succ}(x) \in A,$$

Then  $A = \mathbb{N}$ .

**REMARK 2.3.** *i) and ii) does not imply iii). Let  $S = \mathbb{N} \cup \{\frac{1}{2} + x : x \in \mathbb{Z}\}$ . We define  $\text{succ}(x) = x + 1$ . Condition i) and ii) are satisfied. Let  $A = \mathbb{N}$ . Then condition iii) is satisfied, however  $A \neq S$ .*

**REMARK 2.4.** *We will have plenty of opportunity to practice the induction principle.*

**PROPOSITION 2.5.** *Let  $A \subset \mathbb{N}$  be a nonempty set. Then there exists a an element  $x \in A$  which has no predecessor in  $A$  (i.e. for no  $y \in A$  we have  $\text{succ}(y) = x$ ).*

PROOF. Let  $A \subset \mathbb{N}$  be a subset. Assume to the contrary that

$$\forall x \in A \exists y \in A : x = \text{succ}(y).$$

We show that  $A^c = \mathbb{N} \setminus A$  is  $\mathbb{N}$ . Since 1 has no predecessor, we now that  $1 \notin A$ . Now assume that  $x \notin A$ . We want to show  $\text{succ}(x) \notin A$ . Indeed, if  $\text{succ}(x) \in A$ , then we find  $y \in A$  such that  $\text{succ}(y) = \text{succ}(x)$ . This implies  $y = x$  and hence  $x \in A$ , a contradiction. ■

In the following we use  $\min(A)$  for the unique first element of a nonempty subset of  $A$ .

### 2.3. Functions.

A function  $f : X \rightarrow Y$  is an assignment which sends every element from  $X$  to some element  $f(x) \in Y$ .

Picture (forbidden arrows).

There are many ways to visualize functions! One way is to consider the graph

$$\text{graph}(f) = \{(x, f(x)) : x \in X\}.$$

(see page 13  $f(x) = e^x$ ,  $f(x) = \sin(x)$ ,  $f(x) = \arctan(x)$ .) In set theory the graph is used to explain what a function is, namely a subset  $gr \subset X \times Y$  such that

$$\forall x \in X, y \in Y, z \in Y : ((x, y) \in R \wedge (x, z) \in R \Rightarrow y = z).$$

(-logical operations)

**Remark:** In older textbooks only the relation between  $x$  and  $f(x)$  is assigned:  $\text{graph}(f_1) = \{(x, x^2) : x \in \mathbb{R}\}$  or  $\text{graph}(f_2) = \{(x^2, x) : x \in \mathbb{R}\}$ . In the second case  $f_2$  is defined on its natural domain  $\mathbb{R}_+$ .

**Project:** Explain the pictures in Example 5.34!

**Project:** The functional graph for the Penny problem on page 113.

DEFINITION 2.6. A function  $f : X \rightarrow Y$  is called surjective, if

$$\forall y \in Y \exists x \in X : f(x) = y.$$

A function is called injective if

$$\forall x_1, x_2 \in X (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

A function  $f : X \rightarrow Y$  is called is bijective if  $f$  is injective and surjective.

REMARK 2.7. A bijective function  $f : X \rightarrow Y$  admits an inverse  $f^{-1} : Y \rightarrow X$  defined by  $f^{-1}(f(x)) = x$ .

**Problem:** Let  $f$  be a bijective function. Show that

$$\text{graph}(f^{-1}) = \{(y, x) : (x, y) \in \text{graph}(f)\}.$$

One important feature of functions is their composition. If  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$ , then  $g \circ f : X \rightarrow Z$  is defined by composing arrows, i.e.

$$g \circ f = g(f(x)).$$

For functions  $f : X \rightarrow X$  we can also compose  $f$  with itself

$$f \circ f(x) = f(f(x)).$$

(see page 112). By induction we may define for  $k \in \mathbb{N}$

$$f^{(\text{succ}(k))}(x) = f \circ f^{(k)}(x).$$

(In short  $f^{(\text{succ}(k))} = f \circ f^{(k)}$ .)

### 3. The integers

On the natural numbers we may define

$$x + 1 = \text{succ}(x)$$

and  $f_k : \mathbb{N} \rightarrow \mathbb{N}$  by

$$f_k(x) = \text{succ}^{(k)}(x) = \underbrace{\text{succ}(\text{succ}(\cdots(\text{succ}(x))\cdots))}_{k \text{ times}}.$$

This leads to the more familiar notation

$$x + k = f_k(x).$$

The following Lemma will be proved later (project?) when we have more exercise in induction.

LEMMA 3.1. *i)  $x + k = k + x$  holds for all  $x, k \in \mathbb{N}$ .*

*ii)  $(x + k) + l = x + (k + l)$  holds for all  $x, k, l \in \mathbb{N}$ .*

DEFINITION 3.2. A function  $+: X \times X \rightarrow X$  (binary operation) is called associative if

$$+(+(a, b), c) = +(a, +(b, c))$$

holds for all  $a, b, c \in X$ . Such a function is called commutative if

$$+(a, b) = +(b, a)$$

holds for all  $a, b \in X$ .

I know, this reads much better in the form

$$(a + b) + c = a + (b + c) \quad \text{and} \quad a + b = b + c.$$

Binary operations can be extended to set-valued function:

LEMMA 3.3. *i) Let  $+$  :  $X \rightarrow X \rightarrow X$  be an associative function. Then the function  $\hat{+} : P(X) \times P(X) \rightarrow P(X)$  defined by*

$$A \hat{+} B = \{a + b : a \in A, b \in B\}$$

*is also an associative function.*

*ii) If  $+$  is commutative, so is  $\hat{+}$ .*

EXAMPLE 3.4.  $\{(0, x) : 0 \leq x \leq 1\} \hat{+} \{(x, 0) : 0 \leq x \leq 1\} = [0, 1] \times [0, 1]$ .

PROOF. i) Let  $A, B, C$  be sets. Let  $x \in (A \hat{+} B) \hat{+} C$ . Then there exists  $c \in C$  and  $y \in A \hat{+} B$  such that

$$x = y + c.$$

Now,  $y \in A \hat{+} B$  means that there is  $a \in A$  and  $b \in B$  such that

$$y = a + b.$$

By associativity we find

$$x = (a + b) + c = a + (b + c).$$

Thus  $z = b + c$  is an element in  $B \hat{+} C$  and  $a \in A$ . Hence

$$x \in A \hat{+} (\hat{B} + \hat{C}).$$

We have proved

$$(A \hat{+} B) \hat{+} C \subset A \hat{+} (B \hat{+} C).$$

Similarly, one shows

$$A \hat{+} (B \hat{+} C) \subset (A \hat{+} B) \hat{+} C.$$

ii) is an exercise. ■

**Key idea 1):** Let  $A_m = \{(x, x + m) : x \in \mathbb{N}\}$  and  $B_m = \{(x + m, x) : x \in \mathbb{N}\}$  be obtained from  $A_k$  by flipping the pairs. What is

$$A_m \hat{+} B_m ?$$

**Key idea 2):** Forget the  $m$  on the right hand side.

How? We say that  $(n, m)$  is equivalent to  $(k, l)$  if

$$n + l = m + k .$$

We use the notation  $(n, m) \sim (k, l)$ . Then we define the corresponding equivalence class (more on that subject later) as

$$[(n, m)] = \{(k, l) : (n, m) \sim (k, l)\} .$$

Note that

$$[(0, m)] = \{(x, x + m) : x \in \mathbb{N}\} = A_m$$

and

$$[(m, 0)] = \{(x + m, x) : x \in \mathbb{N}\} = B_m .$$

The new addition is now defined as

$$(3.1) \quad [(n, m)] + [(n', m')] = [(n + n', m + m')] .$$

Note in the situation above that  $(x + k, x + k)$  is equivalent to  $(x, x)$  and hence

$$[(n, 0)] + [(0, n)] = [(0, 0)] .$$

**THEOREM 3.5.** *Let  $\mathbb{Z} = \{[(n, m)] : n, m \in \mathbb{N}\}$  be the set of equivalence classes and  $e = [(0, 0)]$ . Then the operation  $+$  defined in (3.1) is well-defined. The triple  $(\mathbb{Z}, +, e)$  is a commutative group, i.e. satisfies the following axioms*

- i) (neutral element)  $e + x = e + x$  holds for all  $x \in \mathbb{Z}$ ;
- ii) (associativity)  $(x + y) + z = x + (y + z)$ ;
- iii) (inverse) There is an  $y \in \mathbb{Z}$  such that  $x + y = y + x = e$ ,
- (iv) (commutativity)  $x + y = y + x$  holds for all  $x, y \in \mathbb{Z}$ .

holds for all  $x, y, z \in \mathbb{Z}$ .

**PROOF.** We introduce  $f : P(\mathbb{N} \times \mathbb{N}) \rightarrow P(\mathbb{N} \times \mathbb{N})$  by

$$f(A) = \{y : \exists x \in A : x \sim y\} .$$

**Claim:**  $[(n, m)] + [(n', m')] = f([(n, m)] \hat{+} [(n', m')])$  holds for all  $n, m \in \mathbb{N}$ .

**Proof:** Let  $n, m, n', m' \in \mathbb{Z}$ . Let

$$(k, l) \in [(n + n', m + m')].$$

Then

$$(k, l) \sim (n + n', m + m') \in f([(n, m)] \hat{+} [(n', m')])$$

holds by definition. Conversely consider  $(k, l) \in f([(n, m)] \hat{+} [(n', m')])$ . This means we find  $(n_1, m_1) \sim (n, m)$  and  $(n_2, m_2) \sim (n', m')$  such that

$$(k, l) \sim (n_1 + n_2, m_1 + m_2).$$

This yields the following equalities

$$\begin{aligned} n_1 + n_2 + l &= m_1 + m_2 + k, \\ n_1 + m &= m_1 + n, \\ n_2 + m' &= m_2 + n' \end{aligned}$$

We obtain

$$\begin{aligned} m_1 + m_2 + m + m' + k &= m + m' + m_1 + m_2 + k = m + m' + n_1 + n_2 + l \\ &= n_1 + m + n_2 + m' + l = m_1 + n + m_2 + n' + l \\ &= m_1 + m_2 + (n + n' + l). \end{aligned}$$

We apply the cancellation property below and deduce

$$m + m' + k = n + n' + l.$$

This means  $(k, l) \in [(n + n', m + m')]$ . □

Using the claim we deduce from Lemma 3.3 that  $+$  is associative and commutative.

We have already seen that

$$[(n, m)] \hat{+} [(m, n)] = \{(x + n + m, x + n + m) : x \in \mathbb{N}\}$$

and hence

$$[(n, m)] + [(m, n)] = [(0, 0)].$$

This provides us with the desired inverse. ■

**LEMMA 3.6.** (*Cancellation property*) Let  $x, y, z \in \mathbb{N}$ . Then  $x + y = x + z$  implies  $y = z$ .

REMARK 3.7. *The relation  $\sim$  is what is called an equivalence relation.*

**Axioms of an equivalence relation**

- i) *(reflexivity)*  $x \sim x$ ,
- ii) *(symmetry)*  $x \sim y \Leftrightarrow y \sim x$ ,
- iii) *(transitivity)*  $x \sim y \wedge y \sim z \Rightarrow x \sim z$

*holds for all  $x, y, z$  in a set  $X$ . The transitivity iii) in our example  $((n, m) \sim (k, l)$  if  $n + l = m + k$ ) is again proved using the cancellation property.*