

# Chapter 1 Algebraic Structures

## §0 Notation

Commonly used symbols (in the order in which they appear):

$\in$	"is a member of" or "is in"	$\text{iff} = \text{if and only if}$
$\notin$	"is not a member of"	$\cong$ isomorphic to
$\Rightarrow$ or $\leadsto$	"implies" or "it follows"	
$\wedge$	logical "and"	
$\vee$	logical "or"	
$\equiv$	equal by def.	
$\equiv$	identically equal	
$\exists$	there exists	
$\exists!$	there exists one and only one	
$\square$	end of proof	

## §1 Sets and Mappings

### 1.1 Sets

Consider a well-organized collection of well-defined, distinct objects that can be real or imagined.

Example: (1) Coins, cars, numbers, letters, pieces of cloth

def. 1: (a) A set  $M$  is defined by any property that each of the objects does or does not possess. If  $m$  is an object that has the property we say " $m$  is a member of  $M$ " or " $m$  is in  $M$ " and write  $m \in M$ . Otherwise we write  $m \notin M$ .

(b) The set with no members is called empty set or

example: (2) All blue pieces of cloth form a set  $M_{bc}$ .

notation: (1)  $\exists$  if a set  $M$  has elements  $m_1, m_2, \dots$ , we write  $M = \{m_1, m_2, \dots\}$

(2)  $\exists$  if  $p$  is the property that characterizes  $M$ , we write

$$M = \{m; m \text{ has property } p\}$$

example: (3) Number sets:  $\mathbb{N} = \{1, 2, 3, \dots\}$  natural numbers

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \text{ integers}$$

$$\mathbb{Q} = \{p/q; p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\} \text{ rational}$$

remark: (1) We often have an intuitive understanding of these number sets formally defining them is tricky (see, e.g., Russell 1993) ditto for the real numbers  $\mathbb{R}$  (for a definition, see van der Waerden 1991).

(2) The objects themselves can be sets, although this can lead to problems that we will ignore (see Problem #1).

problem 1:  
Russell's Paradox

def. 2: (a) let  $A$  and  $B$  be sets.  $A$  is called a subset of  $B$  ( $A \subseteq B$ ) if  $a \in A$  implies  $a \in B$  ( $a \in A \Rightarrow a \in B$ )

(b)  $A$  and  $B$  are called equal ( $A = B$ ) if  $A \subseteq B \wedge B \subseteq A$

(c)  $A$  is called a proper subset of  $B$  if  $A \subseteq B \wedge A \neq B$

(d)  $\emptyset$  is a subset of any set. ( $\emptyset \subseteq A$ )

remark: (3) Graphic representation of  $A \subseteq B$ :

$$(4) A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$$

Graphical proof:



def. 3: let  $A$  and  $B$  be sets. We define

(a) The union of  $A$  and  $B$ :  $A \cup B := \{x; x \in A \vee x \in B\}$

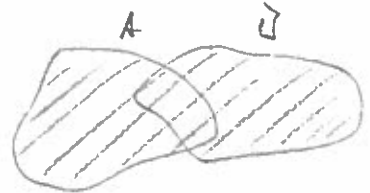
(b) The intersection:  $A \cap B := \{x; x \in A \wedge x \in B\}$

(c) The difference:  $A \setminus B := \{x; x \in A \wedge x \notin B\}$

also the complement of  $B$  in  $A$ .

remark: (5) Graphically,

$A \cup B =$



$A \cap B =$

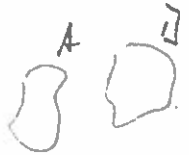


$A \setminus B =$



note 2:  
distribution property  
of  $\cap$  and  $\cup$

def. 4: Two sets for which  $A \cap B = \emptyset$  are called disjoint

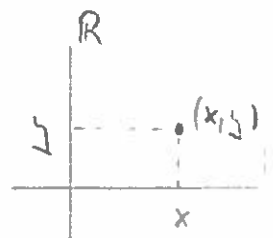


def. 5: let  $X, Y$  be sets and consider ordered pairs  $(x, y)$  when  $x \in X$  and  $y \in Y$ . Then the cartesian product of  $X$  and  $Y$  is defined as

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

remark: (6)  $X=Y$  is possible. E.g.,

$\mathbb{R} \times \mathbb{R} \equiv \mathbb{R}^2 \equiv \mathbb{R}_2$  is a dybrenic representation of the cartesian plane.



1.2 Mappings

def. 1: (a) let  $X, Y$  be sets. let  $\varphi$  be

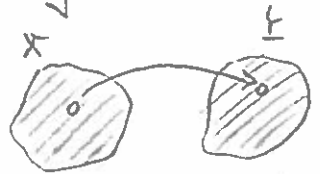
a prescription that associates

with every  $x \in X$  one and only one  $y = \varphi(x) \in Y$ . Then  $\varphi$  is called a mapping, from  $X$  to  $Y$ .

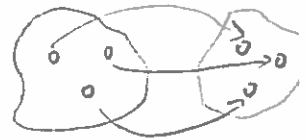


(b)  $y = \varphi(x)$  is called image of  $x$  under  $\varphi$ , and  $x$  is called the pre-image of  $y$ . We write  $x \mapsto y$  or  $\varphi: x \mapsto y$ .

(c)  $\exists$ ! every  $y \in Y$  has at least one pre-image in  $X$ , the mapping is called surjection. We write  $Y = \varphi(X)$  and sometimes say " $\varphi$  maps  $X$  onto  $Y$ ".



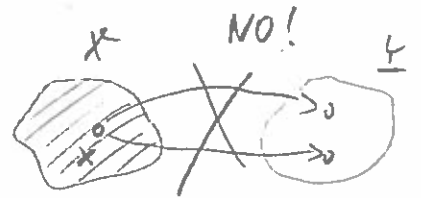
(d)  $\exists$ ! every image  $y \in Y$  has only one pre-image the mapping is called injection or one-to-one.



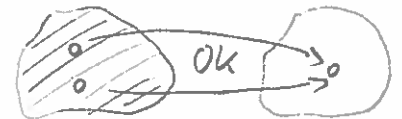
(e) A mapping that is both surjective and injective is called bijection.

(f) Let  $X$  be a set and let a bijective mapping  $\varphi: \mathbb{N} \rightarrow X$  exist. Then  $X$  is called countable.

Remark: (1) No pre-image can have more than one image, and every  $x \in X$  must be the pre-image of some image  $y \in Y$ .



(2) An image can have more than one pre-image.



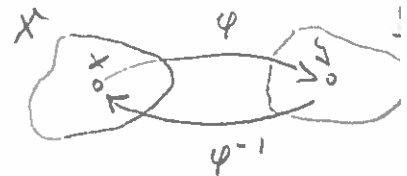
Example: (1)  $X = Y = \mathbb{R}$ .  $x \mapsto |x|$  is not a mapping, but

$X = \{x; x \in \mathbb{R} \wedge x \geq 0\}$ ,  $Y = \mathbb{R}$ ,  $x \mapsto |x|$  is a mapping.

Remark: (2)  $\exists$ !  $\varphi: X \rightarrow Y$  is bijective, then

$\exists$ ! mapping  $\varphi^{-1}: Y \rightarrow X$  and that

if  $\varphi: x \mapsto y$  then  $\varphi^{-1}: y \mapsto x$ .  $\varphi^{-1}$  is called the inverse of  $\varphi$ . This is intuitively plausible, but requires a proof (which we skip).



9/26/16

problem 3:  
mapping

problem 4:

probabilistic  
mapping

def. 2: let  $X = \mathbb{Z}$ . The mapping  $\varphi: x \mapsto x$  is called the identity on  $X$  and denoted by  $\text{id}_X$  or  $\mathbb{1}_X$ .

remark: (4)  $\mathbb{1}_X$  is obviously bijective and its own inverse.

(5)  $\exists!$   $f: X \rightarrow \mathbb{Z}$  on number sets, mappings  $f: X \rightarrow \mathbb{Z}$  are called functions and we will write  $y = f(x)$ . For functions the prohibition from remark (3) is sometimes relaxed ("univalent" functions).

def. 3: let  $X$  be a set and  $I$  a nonempty set called index set. The images  $x_i$  of any mapping  $\varphi: i \in I \mapsto x_i \in X$  are called a system of subsets of  $X$  that are indexed or labeled by  $I$ .

remark: (6) Often  $I$  is  $\mathbb{N}$ , or a subset of  $\mathbb{N}$ , but that's not necessary and  $I$  does not even have to be countable.

example: (7) Writing is an example of indexing with  $I = \mathbb{N}$ .

(8) Consider rotations  $g$  in the Cartesian plane. Label each  $g$  by its rotation angle  $\alpha$ . Then  $I = [0, 2\pi[$  and  $\varphi: \alpha \in I \mapsto g_\alpha$ .

remark: (7) The labeled objects can themselves be sets  $X_i$ .

(8) Indexing lets us generalize the concepts of intersection and union:

$$\bigcap_{i \in I} X_i := \{x; x \in X_i \forall i \in I\}$$



$$\bigcup_{i \in I} X_i := \{x; x \in X_i \text{ for at least one } i \in I\}$$



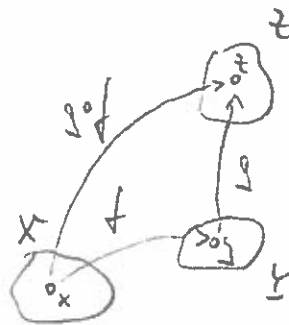
as well as the Cartesian product, e.g.  $\mathbb{N} \times \mathbb{N} = \mathbb{N}^2 = \{(x, y) \mid x, y \in \mathbb{N}\}$

def. 4: let  $f: X \rightarrow Y$  and  $g: Y \rightarrow Z$  be mappings.

Then the prescription  $x \mapsto g(f(x)) \forall x \in X$

defines a mapping  $g \circ f: X \rightarrow Z$  called

the composition of  $f$  and  $g$ . We say " $g$  after  $f$ " or " $g$  follows  $f$ ".



proposition 1: Associativity of composition of mappings

let  $f_1, f_2, f_3$  be mappings  $f_i: X_i \rightarrow X_{i+1}$  ( $i=1,2,3$ )

then 
$$f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1$$

proof: let  $x \in X_1 \rightarrow (f_3 \circ (f_2 \circ f_1))(x) = f_3((f_2 \circ f_1)(x)) = f_3(f_2(f_1(x)))$

$$\text{and } ((f_3 \circ f_2) \circ f_1)(x) = (f_3 \circ f_2)(f_1(x)) = f_3(f_2(f_1(x)))$$

This holds for all  $x \in X_1 \rightarrow$  the mappings are identical.

remark: (9) In general, the composition of mappings is not commutative,  $f \circ g \neq g \circ f$ .

example: (4)  $f: \mathbb{R} \rightarrow \mathbb{R}$ ,  $g: \mathbb{R} \rightarrow \mathbb{R}$  with  $f(x) = x+1$ ,  $g(x) = x^2$ .

$$\rightarrow (f \circ g)(x) = f(g(x)) = x^2 + 1$$

$$(g \circ f)(x) = g(f(x)) = (x+1)^2 = x^2 + 1 + 2x \neq x^2 + 1$$

## 1.2 Ordered sets

def. 1: let  $X$  be a set. An order on  $X$  is a relation  $x \sim y$  ("x is related to y") between ordered pairs  $(x, y) \in X \times X$

and let (i)  $x \sim x \forall x \in X$  ("reflexivity")

(ii)  $(x \sim y \wedge y \sim x) \rightarrow x = y$

(iii)  $(x \sim y \wedge y \sim z) \rightarrow x \sim z$  ("transitivity")

(iv) Either  $x \sim y$  or  $y \sim x \nexists (x, y) \in X \times X$ , then the order is called linear.

remark: (1) Orders are often denoted by  $\leq$  instead of  $\sim$ .

example: (1) "n divides m" is an order on  $\mathbb{N}$ . It is not linear (e.g., 3 does not divide 5).

(2) The relation "person 1 is the mother of person 2" is not an order (not reflexive).

(3) The ordinary "less or equal than" relation on  $\mathbb{N}$ ,  $\mathbb{Z}$ ,  $\mathbb{Q}$ , or  $\mathbb{R}$  is a linear order.

def. 2: a) Let  $X$  be a set with an order  $\leq$ , and let  $\underline{t} \subseteq X$ .

Let  $b \in X$  have the property

$$y \leq b \quad (b \leq y) \quad \forall y \in \underline{t}$$

Then  $b$  is called an upper (lower) bound of  $\underline{t}$  and  $\underline{t}$  is said to be bounded above (below) by  $b$ .

b) Let  $\mathcal{B}$  be the set of upper (lower) bounds of  $\underline{t}$ , and let  $c \in \mathcal{B}$  have the property

$$c \leq b \quad (b \leq c) \quad \forall b \in \mathcal{B}$$

Then  $c$  is called least upper (greatest lower) bound or supremum (infimum) of  $\underline{t}$ .

remark: (2) The supremum, if it exists, may or may not be an element of  $\underline{t}$ .

example: (4)  $X = \mathbb{R}$ ,  $\underline{t} = [0, 1[ \subset \mathbb{R}$ . Then  $\sup \underline{t} = 1 \notin \underline{t}$ .

## 1.4 The natural numbers, and the principle of mathematical induction

The natural numbers  $N$  can be defined by Peano's

axioms: (1)  $1 \in N$

(2) For every  $n \in N$  there is a unique successor  $n^+ \in N$

(3)  $n^+ \neq 1 \quad \forall n \in N$  (i.e., 1 is not the successor of any natural number)

(4)  $n^+ = m^+ \rightarrow n = m$  (i.e., every number is the successor of one and only one number, or it is not the successor of any number)

(5) Let  $M \subseteq N$  and let

(a)  $1 \in M$

(b)  $n \in M \rightarrow n^+ \in M$

then  $M = N$ .

remark: (1)  $n^+$  is usually denoted by  $n+1$ , we will:  $1+1=2, 2+1=3$ , etc and the successor property induces  $N$  with a order:  $n \leq n^+ \leq n^+$

(2) Axiom (5) is called "principle of mathematical induction"

If a statement  $S$  is true for  $n=1$ , and if one can show

that " $S$  is true for  $n=m$ " implies " $S$  is true for  $n=m^+$ "

then  $S$  is true for all  $n \in N$ .

example: proposition:  $\sum_{k=1}^n k = \frac{1}{2} n(n+1)$

proof by induction: let  $n=1 \rightarrow 1 = \frac{1}{2} 1 \cdot 2 = 1 \quad \checkmark$

suppose  $\sum_{k=1}^m k = \frac{1}{2} m(m+1) \rightarrow \sum_{k=1}^{m+1} k = \frac{1}{2} m(m+1) + (m+1) = \frac{1}{2} (m+1)(m+2)$

Problem 6

Works for  $n!$



ok 7  
 (duals  
 - here some  
 else  
 week 1  
 1st (1, 2, 3, 4)  
 7/28/16

remark: (2) Induction also works for statements that are true for all  $N \ni n \geq n_0 > 1$ , since  $\exists$  an obvious isomorphism between  $\{n_0, n_0+1, n_0+2, \dots\}$  and  $N$ .

## 12 Groups

### 2.1 The definition of a group

def. 1: Let  $G \neq \emptyset$  be a set. Let  $\text{then } \overset{\text{be}}{\text{a mapping}} \varphi: G \times G \rightarrow G$  that assigns to every ordered pair  $(a, b)$  with  $a, b \in G$  an element of  $G$  that we denote by  $a \vee b$ .

remark: " $\vee$ " is used to denote the mapping, i.e.,  $\varphi(a, b) = a \vee b$ .  
 It is not to be confused with the logical operator "or".

Let  $\vee$  have the following properties

(i)  $a \vee b \in G \quad \forall a, b \in G$  (closure; this is already implied by what we said above)

(ii)  $(a \vee b) \vee c = a \vee (b \vee c) \quad (\text{associativity})$   
 $\equiv a \vee b \vee c$

(iii)  $\exists e \in G: e \vee a = a \quad \forall a \in G$  (existence of a neutral element)

(iv)  $a \in G \rightarrow \exists a^{-1} \in G: a^{-1} \vee a = e$  (existence of an inverse)

The  $G$  is called a group under the operation  $\vee$ , and we write  $(G, \vee)$ .

If, in addition,

(v)  $a \vee b = b \vee a \quad \forall a, b \in G$

the  $G$  is called an abelian group, and  $\vee$  is called commutative.