PHYS 610 Mathematical Methods
F2022

Chapter 1 | Algebraic Structures

§0 Notation

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

$\in$	"is an element of" or "is in"	iff	= if and only if
$\notin$	"is not an element of"	$\equiv$	isomorphic to
$\Rightarrow$ or $\rightsquigarrow$	"implies" or "it follows"		
$\wedge$	logical "and"		
$\vee$	logical "or"		
$:=$	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

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

Example: (1) coins, cars, numbers, letters, pairs of shoes

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 an element of M" or "m is in M" and write $m \in M$. Otherwise we write $m \notin M$.

(b) The set with no elements is called empty set or null set and denoted by $\emptyset$.

example: (2) All blue pairs of shoes form a set M_{Sh}.

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

(2) 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

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

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

remark: (1) We assume an intuitive understanding of these number sets; formally defining them is tricky (see, e.g., Russell 1993) but not for the real numbers $\mathbb{R}$ (for a definition, see e.g. Walter 1991).

problem 1: Russell's Paradox

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

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 $A \subseteq B \wedge A \neq B$ ($A \subset B$)

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

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

(4) $A \subset B \wedge B \subset C \rightarrow A \subset C$

Graphical proof:

def. 3: Let A and B be sets. We define

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

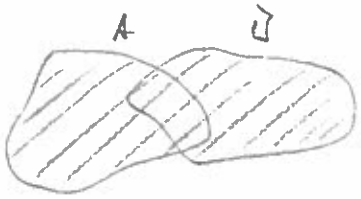
(b) The intersection $A \cap B := \{x ; x \in A \wedge x \in B\}$

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

also the complement of B in A.

remark: (5) Graphically,

$A \cup B$ =

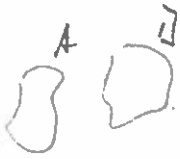


$A \cap B$ =

$A \setminus B$ =

rules 2: distributive property of $\cap$ and $\cup$

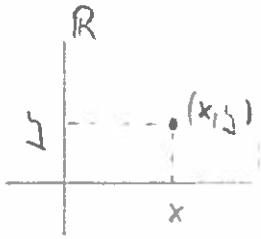
def. 4: Two sets for which $A \cap B = \emptyset$ are called disjoint



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

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

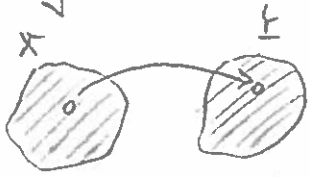
remark: (6) $X = Y$ is possible. E.g.,
$\mathbb{R} \times \mathbb{R} \equiv \mathbb{R}^2 \equiv \mathbb{R}_2$ is an algebraic representation of the cartesian plane.



1.2 Mappings

def. 1: (a) Let X, Y be sets. Let φ be a prescription that associates with any $x \in X$ one and only one $y = \varphi(x) \in Y$. Then φ is called a mapping from X to Y and we write $\varphi : X \to Y$

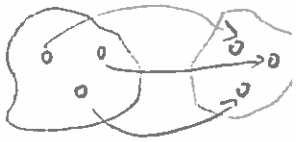
(b) $y = \varphi(x)$ is called image of x under φ, and x is called the pre-image of y. We will $x \overset{\varphi}{\mapsto} y$ or $\varphi : x \mapsto y$.



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

problem 3: mapping

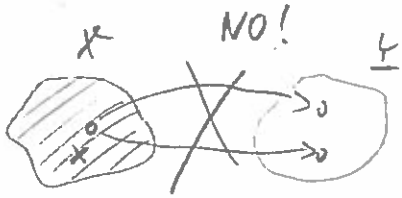
(d) If every image $y \in Y$ has only one pre-image the mapping is called injective or one-to-one.



problem 4: Cardinality mapping

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

(f) Let X be a set and let a bijective mapping $\varphi : \mathbb{N} \to X$ 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 $y \in Y$.

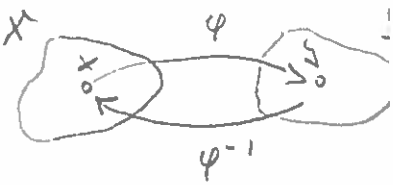
(2) An image can have more than one pre-image.

example: (1) $X = Y = \mathbb{R}$. $x \overset{\varphi}{\mapsto} \sqrt{x}$ is not a mapping, but

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

9/26/16

remark: (1) If $\varphi : X \to Y$ is bijective, then $\exists!$ mapping $\varphi^{-1} : Y \to X$ and that if $\varphi : x \mapsto y$ then $\varphi^{-1} : y \mapsto x$. φ^{-1} is called the inverse of φ. This is intuitively plausible, but requires a proof (which we skip).



def. 2 : Let $X = Y$. The mapping $\varphi : x \mapsto x$ is called the identity on X and denoted by id_X or $\mathbb{1}_X$.

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

(5) If X and Y are number sets, mappings $f : X \mapsto Y$ are called functions and we write $y = f(x)$. For functions the prohibition from remark (1) is sometimes relaxed ("multivalued" functions).

def. 3 : Let X be a set and $\mathcal{I}$ a second set called index set. Then the images x_i of any mapping $\varphi : i \in \mathcal{I} \mapsto x_i \in X$ are called a system of elements of X that are indexed or labeled by $\mathcal{I}$.

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

example : (2) Counting is an example of indexing with $\mathcal{I} = \mathbb{N}$.

(3) Consider rotations ρ in the cartesian plane. Label each ρ by its rotation angle α. Then $\mathcal{I} = [0, 2\pi[$ and $\varphi : \alpha \in \mathcal{I} \mapsto \rho_\alpha$.

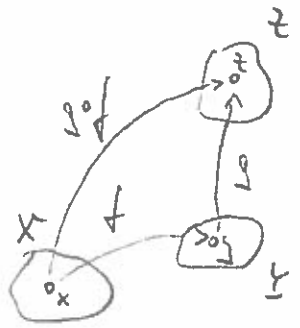
remark : (7) The labeled objects can themselves be sets X_i.

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

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

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

as well as the cartesian product, e.g. $\mathbb{R}^n = \mathbb{R} \cdot \mathbb{R} \cdot \ldots \cdot \mathbb{R} = \{ (x_1, x_2, \ldots, x_n) : x_i \in \mathbb{R} \}$



def. 4: Let $f: X \to Y$ and $g: Y \to Z$ be mappings. Then the prescription $x \mapsto g(f(x)) \ \forall x \in X$ defines a mapping $g \circ f : X \to Z$ 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 the mappings $f_i : X_i \to X_{i+1}$ $(i = 1, 2, 3)$

Then $$\boxed{f_3 \circ (f_2 \circ f_1) = (f_3 \circ f_2) \circ f_1}$$

proof: Let $x \in X_1$. $\rightsquigarrow \big(f_3 \circ (f_2 \circ f_1)\big)(x) = f_3\Big(\big(f_2 \circ f_1\big)(x)\Big) = f_3\big(f_2(f_1(x))\big)$

and $\big((f_3 \circ f_2) \circ f_1\big)(x) = \big(f_3 \circ f_2\big)\big(f_1(x)\big) = f_3\big(f_2(f_1(x))\big)$

This holds for all $x \in X_1$ $\rightsquigarrow$ The mappings are identical.

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

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

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

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

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

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

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

(iv) Either $x \sim y$ or $y \sim x$ $\forall (x,y) \in X \times X$, 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 $\mathbb{N}$. But 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.

Problem 5: Equivalence Relations

def 2: a) Let X be a set with an order $\leq$, and let $\underline{b} \subseteq X$. Let $b \in X$ have the property

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

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

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

$$c \leq b \ (b \leq c) \ \forall b \in \overline{\mathbb{B}}$$

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

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

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

1.4 The natural numbers, and the principle of mathematical induction

The natural numbers $\mathbb{N}$ can be defined by Peano's

axioms: (1) $\underline{1} \in \mathbb{N}$

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

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

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

(5) Let $\mathcal{M} \subseteq \mathbb{N}$ and let

(a) $\underline{1} \in \mathcal{M}$

(b) $n \in \mathcal{M} \Rightarrow n^+ \in \mathcal{M}$

Then $\mathcal{M} = \mathbb{N}$.

remark: (1) n^+ is usually denoted by $n+\underline{1}$, we will $1+1=2$, $2+1=3$, etc and the successor property endows $\mathbb{N}$ with an order: $n \leq n^+ \equiv n+$

(2) Axiom (5) is called "principle of mathematical induction" If a statement S is true for $n = \underline{1}$, 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 $n \in \mathbb{N}$.

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

proof by induction: Let $n = \underline{1} \Rightarrow \underline{1} = \frac{1}{2} \underline{1} \cdot \underline{2} = \underline{1}$ ✓

suppose $\sum_{k=1}^{n} k = \frac{1}{2} n(n+1)$ $\Rightarrow$ $\sum_{k=1}^{n+1} k = \frac{1}{2} n(n+1) + (n+1) = \frac{1}{2}(n+1)(n+$

Problem 6

Bounds for n!

...ch 7
... checks
... the same
... lar
week 1
...1 (1,2,3,4)
7/28/16

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

§2 Groups

2.1 The definition of a group

<u>def. 1</u>: Let $G \neq \emptyset$ be a set. Let there be a mapping $\varphi: G \times G \to G$ that assigns to every ordered pair (a,b) with $a, b \in G$ an element of G that we denote by $a \vee b$.

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

Let $\vee$ have the following properties

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

(ii) $(a \vee b) \vee c = a \vee (b \vee c) \equiv a \vee b \vee c$ (associativity)

(iii) $\exists\, e \in G: \; e \vee a = a \;\forall\, a \in G$ (existence of a <u>neutral element</u> e)

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

Then G is called a <u>group under the operation $\vee$</u>, and we write $(G, \vee)$.

If, in addition,

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

then G is called an abelian group, and $\vee$ is called <u>commutative</u>