Chapter 1

MPI - lecture 4

1.1 Introduction and motivation

Searching for hidden similarities...

Let us consider this objects:

- the set $\mathbb{Z}$ of integers with the usual sum;
- the set of matrices $\mathbb{R}^{n,n}$ with the operation of matrix multiplication;
- the set of relations on a set A with the operation of relation composition;
- the set $\{0, 1, 2, 3\}$ with the multiplication $\pmod 4$;
- the set of finite automata with the operation of composition;
- the set of all colors with the operation "mixing";
- ...

What do they have in common?

Still the same structure!

All presented objects have the same structure. Indeed, they consist of two ingredients:

- A (finite or infinite) **set of objects**.
- A **binary operation** mapping two objects onto (exactly) one object (from the same set of objects).

Generally, we speak about a pair of: a set and a binary operation on it.

We will (mostly) use one of the following notations: $(M, \cdot)$ (multiplicative notation), $(M, +)$ (additive notation), or $(M, \circ)$ (general notation), where

- $M \neq \emptyset$ is a set,
- and for binary operation we have $\cdot : M \times M \to M$ (resp. $+ : M \times M \to M$, resp. $\circ : M \times M \to M$).

What is going on in algebra?

- The pair of "a set and a binary operation on it" could represent very different structures. We shall classify them by their properties.
- We are interested in properties of the binary operation:
  1. Is it associative?
  2. It is commutative?
  3. Are there some neutral elements for the binary operation?

Why are we doing this?

If we prove some statement for a general structure $(M, \cdot)$, where $\cdot$ is an associative operation, this statement is proved for all particular structures with an associative binary operation! A proof of this statement is reduced to a proof of associativity of the operation! We can understand a general structure as a **parent object**, from which particular structures **inherit** all its properties (see below).

Example of "inheritance" (1/4)

On the set of non-zero real numbers we prove the following (trivial) theorem:

Theorem 1. *For all $b, c \in \mathbb{R} \setminus \{0\}$, the equation $bx = c$ has solution $x = b^{-1}c$.*

Proof.

$$\begin{aligned} bx &= c && \text{[multiplication on the left by the inverse element } b^{-1}\text{]} \\ b^{-1}(bx) &= b^{-1}c && \text{[moving brackets due to associativity]} \\ (b^{-1}b)x &= b^{-1}c && \text{[for arbitrary } b \text{ we have } b^{-1}b = 1\text{]} \\ 1x &= b^{-1}c && \text{[for arbitrary } x \text{ we have } 1x = x\text{]} \\ x &= b^{-1}c \end{aligned}$$

□

What was fundamental for the proof: associativity, existence of (left) inverse element, existence of the neutral element.

Example of "inheritance" (2/4)

Let us consider a set M of all matrices $\mathbb{R}^{n,n}$ with the operation of matrix multiplication.

- Is the matrix multiplication associative? Yes. For $\forall\, A, B, C \in M$ we have $A(BC) = (AB)C$.
- Is there a neutral element? Yes. The identity matrix I_n has the property $I_n A = A$ valid for all $A \in M$.
- Is there an inverse matrix for all $A \in M$? No! We have to restrict ourselves to the set of regular matrices M_{reg}.

Example of "inheritance" (3/4)

We have everything needed to prove the theorem for matrices.

Theorem 2. *For all $B, C \in M_{reg}$, the equation $BX = C$ has solution $X = B^{-1}C$.*

Proof.

$$
\begin{array}{rcll}
BX & = & C & \text{[multiplication on the left by the inverse element } B^{-1}\text{]} \\
B^{-1}(BX) & = & B^{-1}C & \text{[moving brackets due to associativity]} \\
(B^{-1}B)X & = & B^{-1}C & \text{[for arbitrary } B \text{ we have } B^{-1}B = I_n\text{]} \\
I_n X & = & B^{-1}C & \text{[for arbitrary } C \text{ we have } I_n X = X\text{]} \\
X & = & B^{-1}C &
\end{array}
$$

□

What was fundamental for the proof: associativity, existence of (left) inverse element, existence of the neutral element.

Example of "inheritance" (4/4)

Suppose that we are given a pair $(M, \cdot)$ where the associativity law holds, for each element $b \in M$ there exists an inverse element, denoted by b^{-1}, and there exists a neutral element e. We will call such pair a group.

We have a general theorem.

Theorem 3. *For arbitrary elements b, c of a group $(M, \cdot)$, the equation $bx = c$ has solution $x = b^{-1}c$.*

Proof.

$$\begin{aligned} bx &= c && \text{[multiplication on the left by the inverse element } b^{-1}\text{]} \\ b^{-1}(bx) &= b^{-1}c && \text{[moving brackets due to associativity]} \\ (b^{-1}b)x &= b^{-1}c && \text{[for arbitrary } b \text{ we have } b^{-1}b = e\text{]} \\ ex &= b^{-1}c && \text{[for arbitrary } x \text{ we have } 1x = x\text{]} \\ x &= b^{-1}c \end{aligned}$$

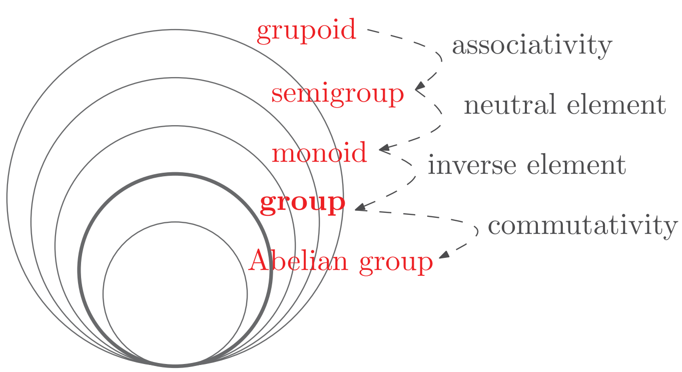
□

1.2 Hierarchy of sets with one binary operation

Introduction

Sets with one binary operation

We call an arbitrary pair "a set and a binary operation" a groupoid. Adding another requirements we get further notions.



Examples

- For the pair $(\mathbb{R} \setminus \{0\}, \cdot)$, the associative and commutative laws hold, the neutral element is 1 and the inverse element for b is $b^{-1} = 1/b$.

  It is an Abelian group.

- For the pair $(\mathbb{Z}, +)$ associative and commutative laws hold, the neutral element is 0 and the inverse element for b is $b^{-1} = -b$.

  It is an Abelian group.

- For the pair $(M_{\text{reg}}, \cdot)$ associativity law holds, the neutral element and the inverse exist, but the commutative law is not valid!

  It is a group, but not Abelian.

Mathematical analogy to Object-oriented programming

- We can consider the groupoid, monoid, etc., as mathematical (abstract) objects, for which a nonempty set and a binary operation with given properties are defined.
- For this abstract classes we can prove various statements (for example the theorem on solving linear equation for groups).
- If for some particular pair $(M, \cdot)$ we prove that it is a groupoid, monoid, etc., it means that it "inherits" all this statements and we need not prove it separately!
- This analogy could be employed in real programming: see, e.g., the mathematical open source software SageMath!

Definitions and elementary properties

Groupoid, semigroup, monoid, group

Definition 4. • *An ordered pair $(M, \circ)$, where M is an arbitrary nonempty set and $\circ$ is a binary operation on M, is called a groupoid.*

- *A groupoid $(M, \circ)$ such that $\circ$ is associative is called a semigroup.*
- *A semigroup $(M, \circ)$ such that there exists a neutral element e satisfying*

$$\forall\, a \in M \quad \textit{holds} \quad e \circ a = a \circ e = a$$

  is called a monoid.

- *A monoid* $(M, \circ)$ *such that for each* $a \in M$ *there exists an inverse element* $a^{-1} \in M$ *satisfying*

$$a^{-1} \circ a = a \circ a^{-1} = e$$

  is called a group.

- *Moreover, if* $\circ$ *is commutative, we say that a group* $(M, \circ)$ *is a commutative (Abelian) group.*

Set closed under the binary operation. What does it mean?

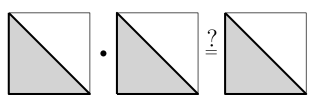
In the definition we require the binary operation $\circ$ to be a "binary operation on M".

This means that the result of a binary operation applied on two elements from M again belongs to M – we say that the **set** M **is closed under** $\circ$**.**

Example 5. *The pair* $(\mathbb{Z}_{-}, \cdot)$ *of negative integers with the usual multiplication is not even a groupoid, because it is not closed under the operation:* $(-1) \cdot (-1) = 1 \notin \mathbb{Z}_{-}$.

Whether the set is or is not closed under the binary operation need not be always obvious.

Example 6. *Let us consider the couple* $(M_{triang}, \cdot)$ *of lower triangular matrixes with the usual matrix multiplication. Is* M_{triang} *closed under the operation* $\cdot$*?*



Manual for classification of sets with binary operation

If we have a given pair "of the set and a binary operation" and we want to find out whether it is a groupoid, semigroup, monoid, (Abelian) group, we can proceed this way:

1. Is the set closed under the operation? If yes, it is a groupoid; if not, END.
2. Does the associativity law hold? If yes, it is a semigroup; if not, END.
3. Is there a neutral element? If yes, it is a monoid; if not, END.
4. Is there an inverse to each element? If yes, it is a group; if not, END.

5. Does the commutativity law hold? If yes, it is an Abelian group; if not, END.

Mostly “proofs” in these individual steps are very easy or obvious. Sometimes, they only seem obvious.

Groupoid, semigroup, monoid, group – examples (1/4)

Example 7. *Let us consider the groupoid* $(\mathbb{Q}, \circ)$*, where the binary operation* $\circ$ *is defined as the arithmetic mean:*

$$a \circ b = \frac{a+b}{2}.$$

Is this structure a semigroup / monoid / group?

In a semigroup, the associative law must hold. Let us claim that for this operation $\circ$ *the law* <u>*does not hold*</u>*, and let us prove it by a* <u>*counterexample*</u>*:*

$$(2 \circ -2) \circ 4 = 0 \circ 4 = 2 \quad \textit{but} \quad 2 \circ (-2 \circ 4) = 2 \circ 1 = \frac{3}{2}.$$

So, the associative law does not hold, and the structure is not a semigroup. It follows that $\mathbb{Q}$ *with this operation is neither a monoid nor a group.*

Groupoid, semigroup, monoid, group – examples (2/4)

Example 8. *Let us consider a groupoid* $(\mathbb{R}^+, \circ)$*, where the binary operation* $\circ$ *is defined as follows:*

$$a \circ b = \frac{a \cdot b}{a+b}.$$

- *Is* $(\mathbb{R}^+, \circ)$ *a semigroup?*
- *Is* $(\mathbb{R}^+, \circ)$ *a monoid?*

Groupoid, semigroup, monoid, group – examples (3/4)

Example 9. *Let us consider a groupoid* $(\mathbb{R}, \cdot)$*, where the binary operation is the usual multiplication of numbers.*

- *Is it a semigroup?*

- *Is it a monoid?*
- *Is it a group?*

Groupoid, semigroup, monoid, group – examples (4/4)

From the definition it follows that each group is a monoid, each monoid is a semigroup and each semigroup is a groupoid. Written in symbols we get:

$$\text{groupoid} \supset \text{semigroup} \supset \text{monoid} \supset \text{group} .$$

From the previous three examples we can be even more specific:

$$\text{groupoid} \supsetneq \text{semigroup} \supsetneq \text{monoid} \supsetneq \text{group} ,$$

because we have found a groupoid that is not a semigroup, a semigroup that is not a monoid, and a monoid that is not a group.

Uniqueness of neutral element

Theorem 10. *Given a monoid, there exists exactly one neutral element.*

Proof. Let $(M, \circ)$ be a monoid and e some neutral element (by definition we know that at least one exists!).

We prove by contradiction that e is the only neutral element.

By contradiction, assume that in the monoid there exists another neutral element $\overline{e}$ different from e. It holds that

$$\overline{e} = \overline{e} \circ e = e,$$

using the property of the neutral element from the definition. We get a contradiction with the statement that $\overline{e} \neq e$. □

Uniqueness of the inverse element

Theorem 11. *Given a group, each element has exactly one inverse element.*

Proof. Let $(G, \circ)$ be a group, a an arbitrary element of the group and a^{-1} one of its inverse elements (from the definition of a group we know that there exists at least one!). We prove *by contradiction* that a^{-1} is the only one.

By contradiction, assume that there exists another inverse element $\overline{a^{-1}}$ different from a^{-1}. Hence it holds that

$$\overline{a^{-1}} = \overline{a^{-1}} \circ e = \overline{a^{-1}} \circ \left(a \circ a^{-1}\right) = \left(\overline{a^{1}} \circ a\right) \circ a^{-1} = e \circ a^{-1} = a^{-1}$$

where e is the unique neutral element. Thus we get a contradiction with the assumption that $\overline{a^{-1}} \neq a^{-1}$. □

Cayley table

Cayley tables for finite groups

If the set M from the pair $(M, \circ)$ has a finite number of elements, its structure (with the given operation $\circ$) could be completely represented by the Cayley table.

Its onstruction of it is obvious from the following example.

Example 12. *Let us consider* $(\mathbb{Z}_4, +_4)$*, i.e., the set of numbers* $\{0, 1, 2, 3\}$ *with addition modulo* 4*. Since the set has* 4 *elements, the Cayley table has* 4 *rows and* 4 *columns:*

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

So, in the cell in row m *and column* n *we write the result of* $m +_4 n = m + n \ (mod\ 4)$*.*

For example the cell in row 2 *and column* 3 *is filled with* $2 + 3 \ (mod\ 4) = 1$*.*

What can be easily read from a Cayley table

Cayley table offers all information about a given set and operation. Some properties are very easy to read from the table; others with some difficulty:

- The set M is closed under the operation $\circ$ if all cells of the table contain elements from the set M only.
- The associativity law is difficult to read.
- The neutral element e is the one for which the corresponding row and column are just a copy of the first row and the first column of the table.

- The inverse element to the element a is the one corresponding to the row and column where the neutral element e is placed...

Cayley table and latin square (1/4)

Question: Is it possible to recognize whether a table is a Cayley table of a group? **Answer**: Almost.

Theorem 13. *The Cayley table of each group forms a latin square.*

- A latin square for a set M of n elements is a matrix $n \times n$ such that each row and column contains all elements of the set M.
- We prove the theorem by proving another one from which the statement of the original theorem follows directly.
- Unfortunately, not each Cayley table forming a latin square is a Cayley table of a group. Later we present a counterexample.

Cayley table and latin square (2/4)

Theorem 14. *In each group, we can divide uniquely. In other words: in each group $(G, \circ)$, for arbitrary $a, b \in G$ the equations*

$$a \circ x = b \quad \textit{and} \quad y \circ a = b$$

have only one solution.

Proof. Since we are in a group, each element has only one inverse.
The only solutions of the equations are $x = a^{-1} \circ b$ and $y = b \circ a^{-1}$. □

It is possible to prove that a group is a semigroup with a "unique division", i.e., the unique division guarantees the existence of a neutral element and inverse.

Cayley table and latin square (3/4)

Now we prove the theorem saying that the Cayley table of group is a latin square.

Proof. Proof by contradiction:

- Let us suppose that the table of some group $(G, \circ)$ is not a latin square.

- Hence in some row or column there is one element, denote it as b, repeated twice. WLOG[1], assume that it happens in row n and columns m_1 and m_2.

$\circ$	$\cdots$	m_1	$\cdots$	m_2	$\cdots$
$\vdots$		$\vdots$		$\vdots$	
n	$\cdots$	b	$\cdots$	b	$\cdots$
$\vdots$		$\vdots$		$\vdots$	

- It follows that the equation $n \circ x = b$ has two different solutions, namely m_1 and m_2, which is a **contradiction with the previous theorem**!

□

Cayley table and latin square (4/4)

- We have shown that the fact that a Cayley table is a latin square is a *necessary* condition for the given set and operation to be a group.
- The following example says it is not a *sufficient* condition.

Example 15. *Let us consider a set $M = \{a, b, c\}$ with operation given by the Cayley table:*

$\circ$	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

This table creates a latin square; in spite of it, it is not the table of a group (Why?!).

Cayley graph

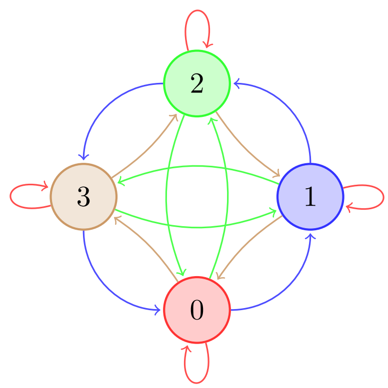
Cayley graph of a group

A finite Abelian group $G = (M, \circ)$ may be visualised by a Cayley graph with

- set of vertices V being the elements of G, i.e., $V = M$,

[1] Without Loss Of Generality

- set of directed edges E the set of (ordered) pairs (a, b) such that $a = c \circ b$ for some $c \in M$ (or, as we can see, for some $c \in N$ with N a subset of M).



If the group in question is not Abelian, we need to depict edges (a, b) for $a = b \circ c$ for some $c \in M$.