DMA: Groups and friends

Jurij Volčič
Institut for Matematiske Fag

Outline

- Binary operations
- Groups, monoids, semigroups
- Homomorphisms, isomorphisms

Reading: KBR 9.1-9.2 and 9.4

Note: No class on Friday!

Binary operations

Def. A binary operation on a set A is an (everywhere defined) function $f\colon A \times A \to A$.

Notes:

- A binary operation on A assigns to each ordered pair $(a, b) \in A \times A$ a unique element of A.
- Use symbols such as $+$, $*$, $\circ$, $\odot$, instead of f.
- Infix-notation: $a * b$ instead of $*(a, b)$.

Examples of binary operations

Def. A binary operation on a set A is an (everywhere defined) function $A \times A \to A$.

Examples

- $+$ is a binary operation on $\mathbb{Z}$.
- $-$ is not a binary operation on $\mathbb{Z}^+$.
- $-$ is a binary operation on $\mathbb{Z}$.
- $/$ (division) is not a binary operation on $\mathbb{R}$.

Properties of binary operations

Def. We say that a binary operation $*$ on a set A is

- commutative if $a * b = b * a$ for all $a, b \in A$
- associative if $a * (b * c) = (a * b) * c$ for all $a, b, c \in A$

Examples

- $(\mathbb{Z}, +)$ is both commutative and associative.
- $(\mathbb{Z}, -)$ is neither commutative nor associative.
  For example, $5 - (4 - 3) \neq (5 - 4) - 3$

Tables for binary operations

For binary operations, we can represent this table as a grid.

Example:

$D_6 = \{1, 2, 3, 6\}$ with binary operation $\wedge$ (GCD).

$\wedge$	1	2	3	6
1	1	1	1	1
2	1	2	1	2
3	1	1	3	3
6	1	2	3	6

Groups

Def. A group $(A, *)$ consists of a set A and binary operation $*$ on A such that

1. **(Associativity)**: The operation $*$ is associative.
2. **(Identity Element)**: There exists $e \in A$ such that $e * a = a * e = a$ for all $a \in A$
3. **(Inverse)**: For each $a \in A$ there exists an $a' \in A$ such that $a * a' = a' * a = e$

Def. If the pair $(A, *)$ satisfies

- (1) then it is called a semigroup;
- (1) and (2) then it is called a monoid.

Examples

Examples

- $(\mathbb{Z}, +)$ is a group. The inverse of $a \in \mathbb{Z}$ is $-a$.
- The set of invertible $n \times n$ matrices is a group under the operation of matrix multiplication.
- Is $(\mathbb{N}, +)$ a group?
- Is $(\mathbb{N}_0, +)$ a group?
- Is $(\mathbb{R}, \cdot)$ a group?
- Is $(\mathbb{R}_{>0}, \cdot)$ a group?
- Is $(\mathbb{Z}, -)$ a group?
- The set of all permutations on $\{1, \ldots, n\}$ with composition is a group, denoted $(S_n, \circ)$.

How to check if $(A, *)$ is a semigroup/monoid/group?

Example. $(A, *) = (\mathbb{Z}, \min(\_,\_))$

- Is A closed under $*$? Yes
- Is $*$ associative? Yes,

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

$\Rightarrow$ $(A, *)$ is a semigroup

- Identity element?
- Is $(\mathbb{Z}, \min)$ a monoid/group?

Example: The multiplicative group $\mathbb{Z}_5^*$

Let $\mathbb{Z}_5^* = \{1,2,3,4\}$, where $\otimes$ is defined as

$$x \otimes y = (xy) \bmod 5$$

Then

$$2 \otimes 2 = 4,$$
$$2 \otimes 3 = 1$$
$$2 \otimes 4 = 3.$$

Fill in the table for $\otimes$

$\otimes$	1	2	3	4
1				
2				
3				
4				

$(\mathbb{Z}_5^*, \otimes)$ is a

- semigroup
- monoid (1 is the identity element)
- group?
    - What are the inverse elements?

Very popular examples

For $n \in \mathbb{N}$ let $\mathbb{Z}_n = \{0, \ldots, n-1\}$, and $\oplus$ is defined as

$$x \oplus y = (x + y) \bmod n$$

Then $(\mathbb{Z}_n, \oplus)$ is a group. Why?

For prime $p \in \mathbb{N}$ let $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$, and $\otimes$ is defined as

$$x \otimes y = (xy) \bmod p$$

Then $(\mathbb{Z}_p^*, \otimes)$ is a group. Why, and why ony for prime p?

Fermat's little theorem

Thm. If p is prime and a is not a multiple of p, then

$$a^{p-1} = 1 \bmod p.$$

In particular, a^{p-2} is the inverse of a in $\mathbb{Z}_p^*$.

Identity element

Thm. Let $(A, *)$ be a semigroup. There exists at most one identity element in A.

Proof. Let e and e' be two identity elements:

$$e * a = a = a * e$$
$$e' * a = a = a * e'$$

for all $a \in A$. In particular,

$$e = e * e' = e'$$

$\square$

Corollary. In a monoid/group there is a unique identity element.

Inverses (Theorems 9.4.1–4 from KBR)

Let $(G, *)$ be a group.

Thm. Every $a \in G$ has exactly one inverse[1].

Thm. Let $a, b, c \in G$.

1. If $a * b = a * c$ then $b = c$.
2. $(a^{-1})^{-1} = a$
3. $(a * b)^{-1} = b^{-1} * a^{-1}$

[1] We denote the inverse of a with a^{-1}.

Homomorphism

Def. A homomorphism from a semigroup $(G, *_G)$ to a semigroup $(H, *_H)$ is an everywhere defined function $f\colon G \to H$ such that for all $a, b \in G$

$$f(a *_G b) = f(a) *_H f(b)$$

Example. Let $f\colon \mathbb{Z} \to \mathbb{Z}_2$ be given by $f(k) = k \bmod 2$. The function f is a homomorphism from $(\mathbb{Z}, +)$ to $(\mathbb{Z}_2, \oplus)$, since for all $k, k' \in \mathbb{Z}$

$$\begin{aligned} f(k + k') &= (k + k') \bmod 2 \\ &= (k \bmod 2) \oplus (k' \bmod 2) \\ &= f(k) \oplus f(k') \end{aligned}$$

Isomorphism

Let $(G, *_G)$ and $(H, *_H)$ be semigroups.

Def. We say that $f : G \to H$ is an isomorphism if

1) f is a bijection and
2) f is a homomorphism from $(G, *_G)$ and $(H, *_H)$

Alternatively:

1') f is everywhere defined, surjective, and injective.
2') $f(a *_G b) = f(a) *_H f(b)$ for all $a, b \in G$.

Idea: Isomorphism between two mathematical structures means that they are "essentially the same".

Examples

- The groups $(S_2, \circ)$, $(\mathbb{Z}_2, \oplus)$, $(\mathbb{Z}_3^*, \otimes)$ are isomorphic:

$$\begin{aligned} f : S_2 &\to \mathbb{Z}_2, & f(12) &= 0 \bmod 2,\ f(21) = 1 \bmod 2 \\ g : \mathbb{Z}_2 &\to \mathbb{Z}_3^*, & g(i \bmod 2) &= 2^i \bmod 3 \end{aligned}$$

- Groups with the same size are not necessarily isomorphic, for example $(\mathbb{Z}_6, \oplus)$ and $(S_3, \circ)$. Why?

  $$(1,2) \circ (1,3) = (1,3,2) \neq (1,2,3) = (1,3) \circ (1,2)$$

- More challenging: if p is prime then $(\mathbb{Z}_p^*, \otimes)$ and $(\mathbb{Z}_{p-1}, \oplus)$ are isomorphic

Why do we like permutations?

$(S_n, \circ)$ is also called the **symmetric group** of degree n.

Thm. For every finite group $(G, *)$ there exists an injective homomorphism

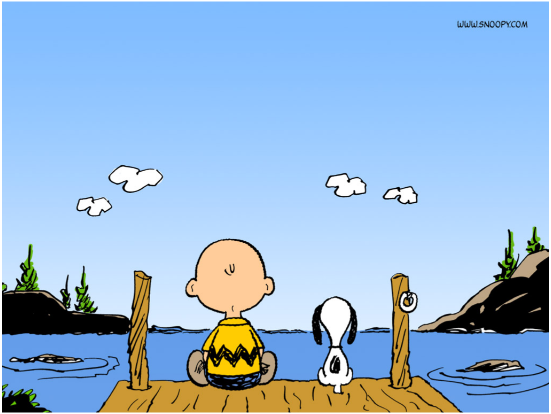
$$f : (G, *) \to (S_{|G|}, \circ).$$

Moral: a finite group can be “realized” with permutations (is a subgroup of the symmetric group)

What did we see today?

- Binary operations
- Group, monoid, and semigroup.
- How to check if $(A, *)$ is a group/monoid/semigroup.
- Isomorphism and homomorphism between two (semi)groups.

The end



It's been a pleasure having you as my students. Best of luck with the rest of your studies!