LECTURE 2
Operations on sets

PAVEL RŮŽIČKA

Abstract. We define an n-ary operation on a set M as a map from its n^{th} Cartesian power $M^n \to M$. An algebra is a set equipped with operations (possibly of various arities) subject to some relations. We focus on algebras with a single binary operation. We define grupoids, semigroups, monoids, loops, and groups.

We recall some basic properties of permutations. We proved that each permutation of a finite set decomposes uniquely (up to an ordering) as a product of independent cycles.

2.1. **Operations.** Recall that the n^{th}-Cartesian power of a set M is the set

$$M^n = \underbrace{M \times \cdots \times M}_{n\times}.$$

of all n-tuples of elements of the set M. We define the 0^{th} Cartesian power of M to be the one-element set: $M^0 := \{\emptyset\}$. For every positive integer n, an n-ary operation on the set M is a map $f\colon M^n \to M$.

We will be interested mainly in nulary, unary and binary operations. A nulary operation is determined by its image, $f(\emptyset)$, and so it can be understood as "picking an element from the set M". An unary operation corresponds to a map $M \to M$. Binary operations are maps $M \times M \to M$. Normally we denote binary operations by symbols as $+, \cdot, *, \circ, \wedge, \vee$, etc. and write, for example, $a + b$ instead of $+(a, b)$.

A set equipped with some operations is called an *algebra*. A *signature* (or *a similarity type*) is an infinite sequence $\mathcal{I} = \langle I_0, I_1, \dots \rangle$ of sets and an *algebra* $\boldsymbol{A}$ of a given signature $\mathcal{I}$ (or a given similarity type $\mathcal{I}$) consists of a set A and a bunch of operations

$$\{f_i^j\colon A^j \to A \mid j = 0, 1, \dots \text{ and } i \in I_j\}.$$

In particular, f_i^j is an operation of arity j for all $i \in I_j$. The operations are often subject to certain conditions, called axioms. This allow us to define algebraic structures as groups, rings, vector spaces, etc.

We denote algebras by bold letters $\boldsymbol{A}, \boldsymbol{B}, \dots$ while their underlying sets by capital letters $A, B, \dots$ We start studying algebras with one binary operation.

The Lecture and the tutorial took place in Malá strana, room S11, on October 9, 2018.

2.2. **Grupoids.** An algebra $\boldsymbol{A}$ with a single binary operation is called a *grupoid*. We usually write the grupoid as pair $\boldsymbol{A} := (A, \cdot)$ of a set and the binary operation, here denoted by $\cdot$. Grupoids are far too general, but interesting classe of algebras are obtained by imposing additional axioms.

A binary operation $\cdot$ is *associative* provided that

$$(a \cdot b) \cdot c = a \cdot (b \cdot c),$$

for all $a, b, c \in A$. A grupoid whose operation is associative is called a *semigroup*.

Example 2.1. *Let M be a set. We denote by F the set of all maps $M \to M$. We denote by $\circ$ the composition of maps from F. Then the pair $\boldsymbol{F} := (F, \circ)$ forms a grupoid. It is easy to see that the composition of maps is associative, indeed,*

$$[(f \circ g) \circ h](m) = f(g(h(m)) = [f \circ (g \circ h)](m),$$

for all $m \in M$. Therefore $\boldsymbol{F}$ is a semigroup.

There is something more, namely the identity map $1_M \colon M \to M$, in the example. Observe that $1_M \circ f = f \circ 1_M = f$, for all $f \in F$. Such an element is called a *unit*. Precisely, elements l and r of a grupoid $\boldsymbol{G} := (G, \cdot)$ are called a *left unit* and a *right unit* if $l \cdot a = a$ and $a \cdot r = a$, for all $a \in G$, respectively. An element $u \in G$ is a *unit* provided that

$$a \cdot u = a = u \cdot a,$$

for all $a \in \boldsymbol{G}$, i.e., if it is both left and right unit.

Lemma 2.2. *Let $\boldsymbol{G} = (G, \cdot)$ be a grupoid. If l is a left unit and r is a right unit of G then $l = r$. In particular, a unit element of a grupoid is unique.*

Proof. The statement follows readily from the equalities

$$l = l \cdot r = r.$$

□

Despite of the lemma, a monoid can have many distinct left (or right) units. For example, in a monoid $\boldsymbol{G} = (G, *)$ such that $g * h = h$, for all $g, h \in G$, every element a left unit. Note that such a monoid has no right unit unless it has only one element.

A semigroup $\boldsymbol{A} = (A, \cdot)$ with a unit element u is called a *monoid.* Note that the unit element can be viewed as a nulary operation on A and a monoid as an algebra of the signature $(1, 0, 1, 0, 0, \dots)$ (i.e, with a nulary and a binary operation).

Example 2.3. *Let $R_2(M)$ denote the set of all binary relations on a set M. The $\boldsymbol{R_2}(M) := (R_2(M), \circ, \Delta)$ is a monoid.*

Definition 2.4. Let $\boldsymbol{A} = (A, \cdot)$ be a grupoid. The operation $\cdot$ is called

- *left cancellative* if $a \cdot b = a \cdot c \implies b = c$, for all $a, b, c \in A$,
- *right cancellative* if $a \cdot c = b \cdot c \implies a = b$, for all $a, b, c \in A$,

- *left divisible* if an equation $a \cdot y = b$ in a variable y has a solution in A, for all $a, b \in A$,
- *right divisible* if an equation $x \cdot a = b$ in a variable x has a solution in A, for all $a, b \in A$.

A binary operation is *cancellative*, *divisible*, if it is both left and right cancellative, divisible, respectively.

A grupoid whose operation is both cancellative and divisible is called a *loop*.

Each binary operation (especially on a finite set) can be represented by a table. For instance, the following table represents a binary operation $*$ on a set $\{a, b, c, d\}$.

$\boldsymbol{*}$	$\boldsymbol{a}$	$\boldsymbol{b}$	$\boldsymbol{c}$	$\boldsymbol{d}$
$\boldsymbol{a}$	b	d	a	c
$\boldsymbol{b}$	a	c	b	d
$\boldsymbol{c}$	d	b	a	a
$\boldsymbol{d}$	c	a	d	d

Let $\boldsymbol{L} = (L, *)$ be loop on a set L. By the definition, the operation $*$ is both cancellative and divisible, hence each row and each column of the table of $*$ contains each element of L exactly once (cf. Exercise 2.1). That is, all rows and columns of the table are permutations of L. Such tables are called *latin squares*. Here is an example of a latin square:

d	a	c	b
b	c	a	d
a	b	d	c
c	d	b	a

A grupoid whose operation is associative, cancellative, and divisible is called a *group*. Thus groups are loops whose operation is associative, i.e, loops which are at the same time semigroups. While cancellativity and divisibility of a binary operation is easily seen from its table, it is not the case of associativity.

Let us explore some basic properties of groups.

Lemma 2.5. *A group has a (unique) unit element.*

Proof. Let $\boldsymbol{G} = (G, \cdot)$ be a group. It follows from the divisibility of $\cdot$ that for each $g \in G$, there are elements l_g and r_g such that

$$l_g \cdot g = g = g \cdot r_g.$$

Given a couple g, h of (not necessarily distinct) elements of G we get that

$$(g \cdot r_g) \cdot h = g \cdot h = g \cdot (l_h \cdot h).$$

Since the operation $\cdot$ is associative, we get that

$$(g \cdot r_g) \cdot h = (g \cdot l_h) \cdot h,$$

hence,

$$g \cdot r_g = g \cdot l_h,$$

due to the right cancellativity. The left cancellativity gives $r_g = l_h$. Therefore $u = r_g = l_h$ is the unique unit element of $\boldsymbol{G}$. □

Note that neither a semigroup nor a loop has to have a unit element. For example, the set of all positive integers with addition form a semigroup without a unit and the lattin square depicted above determines a loop with no unit element.

Lemma 2.6. *Let $\boldsymbol{G} = (G, \cdot)$ be a group with an unit element u. Then for each $g \in G$ there is a unique element g^{-1} such that*

$$g^{-1} \cdot g = u = g \cdot g^{-1}.$$

Proof. From the divisibility of $\cdot$ there are elements g^l and $g^r \in G$ such that $g^l \cdot g = u$ and $g \cdot g^r = u$. It suffices to show that they are equal. This follows from the following computation:

$$g^l = g^l \cdot u = g^l \cdot (g \cdot g^r) = (g^l \cdot g) \cdot g^r = u \cdot g^r = g^r.$$

We set $g^{-1} := g^l = g^r$. □

The element g^{-1} is called an *inverse* of g.

Proposition 2.7. *A semigroup $\boldsymbol{G} = (G, \cdot)$ is a group if and only if it has a unit element and each element of G has an inverse.*

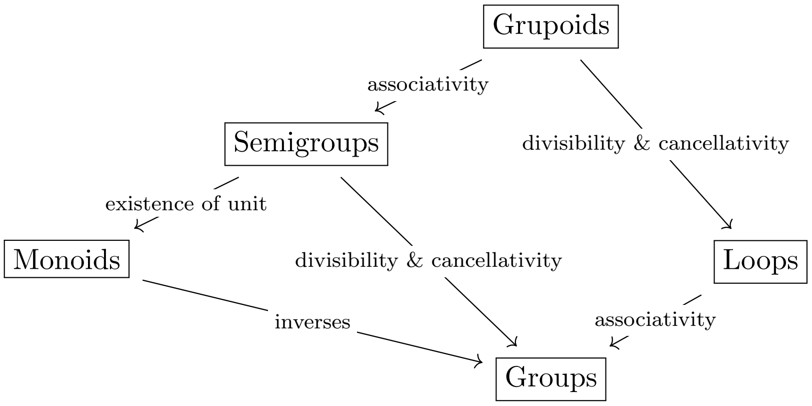
Proof. It follows from Lemmas 2.5 and 2.6, repectively, that each group has a unit element and each element of a group has a unique invers. Therefore it suffices to verify the ($\Leftarrow$) implication. Suppose that the semigroup $\boldsymbol{G}$ has a unit element u, and an inverse element g^{-1} for every $g \in G$. We show that the operation $\cdot$ is cancellative and divisible. Suppose that $g \cdot h = g \cdot k$, for some g, h, and k from G. Multiplying by g^{-1} on the left we get that

$$h = u \cdot h = (g^{-1} \cdot g) \cdot h = g^{-1} \cdot (g \cdot h) = g^{-1} \cdot (g \cdot k) = (g^{-1} \cdot g) \cdot k = u \cdot k = k,$$

which proves that $\cdot$ is left cancellative. The right cancellativity is proved similarly. It is straightforward to verify that the equations $g \cdot x = h$ (resp. $x \cdot g = h$) have a solution $g^{-1} \cdot h$ (resp. $h \cdot g^{-1}$). That is why the operation $\cdot$ is divisible. □

Recall that were defined as algebras of the signature $(0, 0, 1, 0, \dots)$. It follows from Proposition 2.7 that groups can be viewed as algebras with an associative binary operation, a nulary operation (the unit) and a unary operation (the inverse map), i.e, as algebras of the signature $(1, 1, 1, 0, \dots)$.

Here is the hierarchy of the defined algebras with a binary operation:



Permutations

A *permutation* of a finite set is a one-to-one map from the set onto itself. Observe that the permutations correspond to total orderings of the set.

Similarly as in the case of the composition of maps, we multiply permutations from left to right. That is, given permutations π and $\sigma \in S_n$ and $a \in \{1, 2, \dots, n\}$, we have that

$$(\sigma \cdot \pi)(a) = \sigma(\pi(a)).$$

We can write down permutations in several ways. The simplest one is to write a permutation $\pi\colon \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ as the sequence $\langle \pi(1), \dots, \pi(n) \rangle$. Another familiar way is to decompose a permutation into a product of independent cycles.

A *block* of a permutation π is the smallest non-empty subset of $\{1, 2, \dots, n\}$, say B, such that $\pi(B) \subseteq B$. We will us use the notation

$$\pi^k := \underbrace{\pi \cdot \cdots \cdot \pi}_{k\times}.$$

It follows from the minimality of B (with respect to inclusion) that

$$B = \{a, \pi(a), \pi^2(a), \dots\}, \tag{2.1}$$

for any $a \in B$. Since the blocks B are finite, starting with some positive integer $\leq n$, the elements in the list (2.1) will periodically repeat. Let k be the smallest positive integer such that there is $0 \leq l < k$ with $\pi^l(a) =$

$\pi^k(a)$. Then $l = 0$, indeed, otherwise $\pi^{l-1}(a) = \pi^{k-1}$ due to π being one-to-one. This would contradict the minimality of k. Therefore $\pi^k(a) = a$, $B = \{a, \pi(a), \dots, \pi^{k-1}(a)\}$, and $|B| = k$.

Lemma 2.8. *Let π be a permutation of the set $\{1, 2, \dots, n\}$. The blocks of π form a partition of $\{1, 2, \dots, n\}$.*

Proof. If $a \in \{1, 2, \dots, n\}$, then $\{a, \pi(a), \pi^2(a), \dots\}$ is a block of π. Therefore $\{1, 2, \dots, n\}$ is the union of all blocks of π.

Let A and B be blocks of π and suppose that $a \in A \cap B$. Then both A and B are given by (2.1), and so $A = B$. Therefore the blocks A and B are either disjoint or equal. The lemma readily follows. □

Let $\pi \in S_n$ be a permutation. The *support* of π is the set

$$\operatorname{supp} \pi := \{a \in \{1, 2, \dots, n\} \mid \pi(a) \neq a\}.$$

Permutations $\pi, \sigma \in S_n$ are called *independent* if $\operatorname{supp} \pi \cap \operatorname{supp} \sigma = \emptyset$. We say that permutations π and σ *commute* if $\pi \circ \sigma = \sigma \circ \pi$. Observe that independent permutations commute. Indeed, since π is one-to-one, $\pi(a) \neq a$, implies that $\pi^2(a) \neq \pi(a)$. Therefore $\pi(\operatorname{supp} \pi) = \operatorname{supp} \pi$. We infer that if $\pi, \sigma \in S_n$ are independent and $a \in \{1, 2, \dots, n\}$, then

$$\pi(\sigma(a)) = \sigma(\pi(a)) = \begin{cases} \pi(a) & \text{if } a \in \operatorname{supp} \pi; \\ a & \text{if } a \notin \operatorname{supp} \pi \cup \operatorname{supp} \sigma; \\ \sigma(a) & \text{if } a \in \operatorname{supp} \sigma. \end{cases}$$

A *cycle* is a permutation with at most one non-singleton block. More precisely, a *k-cycle* (for $2 \geq k$) is a cycle with the non-singleton block of size k. A *1-cycle* or a *trivial cycle* corresponds to the identity. Given a k-cycle γ with $2 \geq k$, we will use the notation

$$\gamma = (a, \gamma(a), \gamma^2(a), \dots, \gamma^{k-1}(a)),$$

where a is an element of $\operatorname{supp} \gamma$. By (a), where $a \in \{1, 2, \dots, n\}$ is arbitrary, we denote a trivial cycle.

Let $\pi \in S_n$ be a permutation and $B_1, \dots, B_m$ all non-trivial blocks of π. For each $j \in \{1, 2, \dots, m\}$ we pick an element $b_j \in B_j$ and we set

$$\gamma_j := (b_j, \pi(b_j), \dots, \pi^{|B_j|-1}(b_j)).$$

Since the blocks of π form a partition of the set $\{1, 2, \dots, n\}$ due to Lemma 2.8, the cycles $\gamma_1, \dots, \gamma_m$ are independent. It follows that

$$\pi = \gamma_1 \cdot \gamma_2 \cdot \dots \cdot \gamma_m. \tag{2.2}$$

The expression (2.2) is called the *decomposition* of the permutation π into the product of independent cycles. Since the cycles $\gamma_1, \gamma_2, \dots, \gamma_m$ are independent, we can freely change their order in (2.2). On the other hand, the set $\{\gamma_1, \gamma_2, \dots, \gamma_m\}$ is determined by the permutation π. It follows that

Theorem 2.9. *Every permutation has a unique (up to the order of cycles) decomposition into the product of independent cycles.*

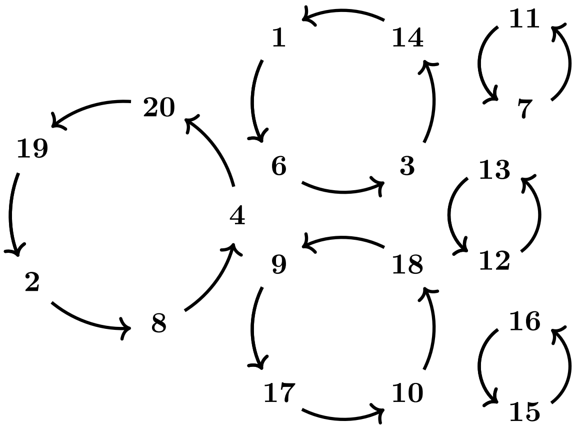
Example 2.10. *For example the permutation*

$$\langle 6, 8, 14, 20, 5, 3, 11, 4, 17, 18, 7, 13, 12, 1, 16, 15, 10, 9, 2, 19\rangle$$

decomposes as

$$(1, 6, 3, 14) \cdot (2, 8, 4, 20, 19) \cdot (7, 11) \cdot (9, 17, 10, 18) \cdot (12, 13) \cdot (15, 16).$$

The decomposition can be depicted as follows:



Let us write a pseudo-code of an algorithm that decomposes a permutation, say π, on a set $\{1, 2, \dots, n\}$ into a product of independent cyclic permutations:

Algorithm: Decomposition into cyclic permutations

```
procedure Decompose
input a permutation $\pi \in \boldsymbol{S_n}$
  $R \leftarrow \{1, 2, \dots, n\}$
loop A:
  until $R = \emptyset$ do
  $j \leftarrow \min R$
  $R \leftarrow R \setminus \{j\}$
  start a new cycle with $j$
  loop B:
  if $\pi(j) \in R$ do
    $R \leftarrow R \setminus \{j\}$
    $j \leftarrow \pi(j)$
    add $j$ to the cycle
    goto loop B
  close the cycle
  goto loop A
remove all cycles of length 1
close;
```

Exercises

Exercise 2.1. *Let $*$ be a binary operation on a set M. Prove that, given a table of $*$, the following holds true:*

(i) *The operation $*$ is left cancellative if and only if each element of M appears in each row of the table at most once;*
(ii) *The operation $*$ is right cancellative if and only if each element of M appears in each column of the table at most once;*
(iii) *The operation $*$ is left divisible if and only if each element of M appears in each row of the table at least once;*
(iv) *The operation $*$ is right divisible if and only if each element of M appears in each column of the table at least once.*

Exercise 2.2. *Let $*$ be a binary operation on a* **finite** *set M. Prove that the operation is left, right cancellative respectively if and only if it is left, right divisible. Show that this may not be true for an infinite M.*

Exercise 2.3 (A. G. Kuroš)**.** *A semigroup $\boldsymbol{G} = (G, \cdot)$ is a group if and only it has a right unit u and every element of $g \in \boldsymbol{G}$ has a right inverse, (i.e, an element g^{-1} such that $g \cdot g^{-1} = u$).*

Exercise 2.4. *A semigroup $\boldsymbol{G} = (G, \cdot)$ is a group if and only if it has a right unit u and its operation is left cancellative and left divisible.*

Exercise 2.5. *Prove that there are exactly $n!$ permutations on an n-element set.*

Exercise 2.6. *Let π be a permutation of the set $\{1, 2, \dots, n\}$. Write $a \sim_\pi b$ if there is $k \in \mathbb{N}_0$ such that $\pi^k(a) = b$. Prove that $\sim_\pi$ is an equivalence on the set $\{1, 2, \dots, n\}$ and that blocks of $\sim_\pi$ correspond to blocks of π.*

Exercise 2.7. *Recall that we compose permutations from right to left. Write a pseudo-code of an algorithm whose input is a sequence of (not necessarily independent) cycles and whose output is the decomposition of their product (in the given order) into a product of independent cycles.*