ALGEBRA I (LECTURE NOTES 2017/2018)
LECTURE 2 - OPERATIONS ON A SET, STRUCTURES WITH ONE BINARY OPERATION

PAVEL RŮŽIČKA

2.1. **Operation on a set.** In the previous section we defined an n^{th}-cartesian power of a set M as

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

We define the 0^{th} cartesian power of M to be equal to the one-element set $\{\emptyset\}$, i.e, $M^0 := \{\emptyset\}$. Now we can define for every $n \in \mathbb{N}_0$ an n-ary operation on a set M as a map $f\colon M^n \to M$. Of a particular interest in our course will be nulary, unary and binary operations. A nulary operation is determined by its image $f(\emptyset)$ and thus it can be understood as "picking an element from the set M" while an unary operation on the set M correspond to a map $M \to M$. Binary operations are by the definition maps $M \times M \to M$. A set equipped with operations is called an *algebra*. A *signature* is a sequence $\mathcal{I} = (I_0, I_1, \dots)$ of sets and an *algebra* $\boldsymbol{A}$ of a given signature $\mathcal{I}$ consists of a set A and a bunch of operations

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

i.e., f_i^j is an operation of arity j[1]. The operations are often subject various requirements which allow us define algebraic structures as groups, rings, vector spaces, etc. We will focus on these particular cases.

2.2. **Algebras with one binary operation.** It is customary to denote binary operations by symbols as $+, \cdot, *, \circ, \wedge, \vee$, etc. ... and write, for example, $a+b$ instead of $+(a, b)$ (that, is $a+b$ stands for the image of a pair $\langle a, b\rangle$). An algebra $\boldsymbol{A}$ with a single binary operation, say $\cdot$, is called a *grupoid*. We usually write the grupoid as pair $\boldsymbol{A} := (A, \cdot)$ of a set and the binary operation. Grupoids are far too general, but interesting classes of them are obtained by imposing additional properties on the operation.

Date: October 9, 2017.

[1]Note that j in f_i^j is an upper index, meaning the arity of j, not an exponent

A binary operation $\cdot$ is called *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:*

$$[(f \circ g) \circ h](m) = f(g(h(m)) = [f \circ (g \circ h)](m), \text{ for all } m \in M.$$

It follows that $\boldsymbol{F}$ is a semigroup. There is something more; I mean the identity map $1_M \colon M \to M$. Observe that $1_M \circ f = f \circ 1_M = f$, for all $f \in F$.

Such an element, say u, of a grupoid is called a *unit element* (or shortly a unit). In particular, an element l, resp. r, of a grupoid $\boldsymbol{G} := (G, \cdot)$ is a *left unit*, resp. *right unit* if $l \cdot a = a$, resp. $a \cdot r = r$, for all $a \in G$. An element $u \in G$ is a *unit* provided that it is both left and right unit. That is, u is the unit of the grupoid $\boldsymbol{G}$ if

$$a \cdot u = a = u \cdot a, \text{ for all } a \in G.$$

Lemma 2.1. *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 $l = l \cdot r = r$. □

Note that it can happen that a monoid has many distinct left units. Indeed, if $\boldsymbol{G} = (G, *)$ is such that $g * h = h$, for all $g, h \in G$, then every element of G is a left unit. Of course, the monoid $\boldsymbol{G}$ has no right unit unless G has at most one element.

A semigroup $\boldsymbol{A} = (A, \cdot)$ with a distinguished 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, an algebra with one unary and one nulary operation.

Example 2.2. *Let M be a set and let $R_b(M)$ denote the set of all binary relations on the set M. Then $\boldsymbol{R_b}(M) := (R_b(M), \circ, \Delta)$ is a monoid.*

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

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

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 table

$*$	a	b	c	d
a	b	c	c	d
b	c	a	c	a
c	a	a	c	b
d	b	b	c	c

represents a binary operation $*$ on a set $\{a, b, c, d\}$.

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.*

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. In other word, rows and columns of the table are permutations of L. Such tables are called *latin squares*. Here is an example of a latin square:

(2.1)

$*$	a	b	c	d	e
a	b	c	a	d	e
b	c	a	e	b	d
c	a	b	d	e	c
d	e	d	c	a	b
d	d	e	b	c	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 2.2. *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 (cf. Lemma 2.1) 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 unit and the table (2.1) determines a loop without an unit element.

Lemma 2.3. *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} will be called an *inverse* of g.

Proposition 2.4. *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 2.2 and 2.3 that each group has a unit element and inverses. 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. □

It follows from Proposition 2.4 that we can view groups as algebras with a asociative binary operation, a nulary operation (the unit) and a unary operation (the inverse map).

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