

## Lecture 12. More algebra: Groups, semigroups, monoids, strings, concatenation.

### CONTENTS

1. Properties of operations and special elements.....	1
1.1. Properties of binary operations.....	1
1.2. Special elements.....	2
2. Groups.....	3
2.1. Definitions and examples .....	3
2.2. Subgroups.....	4
3. Semigroups and monoids. Strings over some alphabet, concatenation.....	5
Homework 12.....	5

**Reading:** Chapter 9: 9.2, 9.3, pp. 248 –250, Chapter 10, pp. 255 –274, Chapter 16, pp. 431-435 of PtMW.

## 1. Properties of operations and special elements

### 1.1. Properties of binary operations.

In the previous lectures we considered properties of some operations : operations on sets, operations of Boolean algebra. Here we repeat certain of these properties in a more abstract way and consider some other useful properties.

Let us consider a binary operation  $\circ$  on some set  $A$ , i.e. a mapping  $A \times A \rightarrow A$ . We will use an infix notation for  $\circ$ . [Note<sup>1</sup>]

An operation  $\circ$  is *associative* iff for all  $a, b, c$  in  $A$ ,  $(a \circ b) \circ c = a \circ (b \circ c)$ . Set theoretic intersection and union are associative, as are Boolean operations  $\wedge$  and  $\vee$ . Operations of addition and multiplication on numbers are associative. Functional composition is associative. Examples of non-associative operations are division and subtraction on real numbers and set-theoretic difference on sets.

An operation  $\circ$  is *commutative* iff for all  $a, b$  in  $A$ ,  $a \circ b = b \circ a$ . Set theoretic intersection and union, Boolean operations  $\wedge$  and  $\vee$ , addition and multiplication on numbers are commutative. Some non-commutative operations are subtraction, division, set-theoretic difference and function composition.

An operation  $\circ$  is *idempotent* iff for all  $a$  in  $A$ ,  $a \circ a = a$ . Set theoretic intersection and union are idempotent, as are Boolean operations  $\wedge$  and  $\vee$ . But most of the operations we have considered are not: addition, multiplication, subtraction, division and function composition are not idempotent operations.

For two binary operations  $\circ_1$  and  $\circ_2$  both on  $A$ ,  $\circ_1$  *distributes over*  $\circ_2$  iff for all  $a, b, c$  in  $A$ ,  $a \circ_1 (b \circ_2 c) = (a \circ_1 b) \circ_2 (a \circ_1 c)$ . We have seen that set-theoretic union distributes over intersection and vice versa. But, although arithmetic multiplication distributes over addition  $(a \times (b + c)) = (a \times b) + (a \times c)$ , addition does not distribute over multiplication, since in general,  $(a + (b \times c)) \neq (a + b) \times (a + c)$ .

---

<sup>1</sup> The operator symbol for a group is usually written as a small circle at a mid-height level, higher than the letter ‘o’ but lower than the degree symbol  $^\circ$ . We have not found that symbol in Word’s symbol repertory, so we are just using the letter o in a smaller font,  $\circ$ .

## 1.2. Special elements.

The next notions are special properties which certain members of a set may have with respect to some operation defined on the set.

Given a set  $A$  and a binary operation  $\circ$  on  $A$ , an element  $e_l$  is a *left identity element* of  $\circ$  iff for all  $a$  in  $A$ ,  $e_l \circ a = a$ . Similarly,  $e_r$  in  $A$  is a *right identity element* of  $\circ$  iff for all  $a$  in  $A$ ,  $a \circ e_r = a$ . The notation  $1_l$  and  $1_r$  also used for identity elements: the operation  $\circ$  is considered metaphorically as multiplication, and “1” is a traditional symbol for an identity element when there is only one (“multiplication”) operation.

As we saw in Lectures 1-3, for a function  $F: A \rightarrow B$  and the operation of function composition  $\circ$ , identity functions  $id_B$  and  $id_A$  are respectively a left and right identity elements:  $id_B \circ F = F$  and  $F \circ id_A = F$ . Subtraction defined on the set of integers and zero has a right identity element, namely zero itself, since for all  $n$ ,  $n - 0 = n$ . But there is no left identity element, i.e. there is no element  $m$  in the set such that for all  $n$ ,  $m - n = n$ .

For commutative operations, every left identity element is also a right identity element [prove it as an exercise!]. An element that is both a right and a left identity element is called *two sided identity* or simply an *identity element*. While commutativity of an operation is a sufficient condition for every right or left identity to be two sided, it is not a necessary condition; a two-sided identity may exist for some operations that are not commutative. An example of this is found in the operation of composition of functions defined on some set of functions  $\mathbf{F} = \{F, G, H, \dots\}$  each being a function in a set  $A$ . If  $id_A$  is one of these functions, it is a two-sided identity, since for each  $F \in \mathbf{F}$ ,  $id_A \circ F = F \circ id_A = F$ . But the operation of composition of functions is not in general commutative. For addition, the two-sided identity is 0, but for arithmetic multiplication it is 1, since for all  $n$ ,  $n + 0 = 0 + n = n$  and  $n \times 1 = 1 \times n = n$ . Given some collection of sets, the identity element for intersection is  $U$ , the universal set, and for union it is the empty set  $\emptyset$  (verify!).

Given a set  $A$  and a binary operation  $\circ$  on  $A$  with a two-sided identity element  $e$ , a given element  $a$  in  $A$  is said to have a *right inverse*  $a_r$  iff  $a \circ a_r = e$ . A given element  $a$  in  $A$  is said to have a *left inverse*  $a_l$  iff  $a_l \circ a = e$ . If  $a^{-1}$  is both a left and a right inverse of  $a$ , i.e.  $a^{-1} \circ a = a \circ a^{-1} = e$ , then  $a^{-1}$  is called a *two-sided inverse* of  $a$ . When the term ‘inverse’ is used without further qualification, we mean that it is two-sided. Note the inverses are always paired in the following way:  $b$  is a right inverse of  $a$  iff  $a$  is a left inverse of  $b$ , since both statements followed from  $a \circ b = e$ . One should observe also that the question of the existence of an inverse can be raised with respect to *each* element in the set on which the operation is defined. In contrast, an identity element, if it exists, is defined for the operation as a whole. To illustrate, let addition be defined in the set  $Z$  of all positive and negative integers and zero. As we have seen, 0 is the two-sided identity element for this operation. Consider now the number 3, and let us ask if it has an inverse in  $Z$ . Is there an element  $z$  in  $Z$  that when added to 3 yields 0? The number  $-3$  is such an element, and furthermore, it is both a right and a left inverse, since  $3 + (-3) = (-3) + 3 = 0$ . From this it also follows that 3 is a two-sided inverse of  $-3$ . For addition, every number of  $Z$  has an inverse, since to each integer  $z$ , except 0, there corresponds an integer  $-z$ , such that  $z + (-z) = 0$ . The number 0 is its own inverse, since  $0 + 0 = 0$ .

## 2. Groups

### 2.1. Definitions and examples

A *group*  $G$  is an algebra with a carrier  $G$  and a single binary operation  $\circ$  on  $G$ . To be a group,  $G$  must satisfy the following conditions, the group axioms:

G1: The operation  $\circ$  is associative.

G2:  $G$  contains an identity element.

G3: Each element in  $G$  has an inverse element.

We can consider several signatures for groups:  $\Omega_G = \{\circ\}$ ,  $\Omega_G = \{\circ, 1\}$  and

$\Omega_G = \{\circ, 1, \theta\}$ .  $1$  is a 0-ary operation (constant) which marks an identity element (we show later that in any group there exists a unique identity element). For the signatures  $\Omega_G$  and  $\Omega_G$  we can rewrite the axiom G2 as G2':

G2':  $1 \circ x = x \circ 1 = 1$ .

The operation  $\theta$  in the signature  $\Omega_G = \{\circ, 1, \theta\}$  is a unary operation of "taking the inverse", i.e. the operation with the axiom G3':

G3':  $x \circ \theta x = \theta x \circ x = 1$ .

Traditionally instead of  $\theta x$  write  $x^{-1}$  and axioms for groups (in the signature  $\Omega_G$ ) are usually written as

G1'':  $(x \circ y) \circ z = x \circ (y \circ z)$ .

G2'':  $1 \circ x = x \circ 1 = 1$ .

G3'':  $x \circ x^{-1} = x^{-1} \circ x = 1$ .

The advantage of this third signature  $\Omega_G$  is that now all of the group axioms can be written directly in terms of operator symbols found in the signature. Now all the axioms can be written with free variables, which we understand as universally quantified. With the simpler signatures, we require 'existence axioms' as well: there exists an identity element; there exist inverses. With the fuller signatures, the existence claims are in effect put into the signature, although we still need the axioms to tell us what sorts of things are being claimed to exist – what properties something must have to be an identity element, or to be an inverse. (Note that certain notations are traditionally tied to certain such properties: "1", "0",  $x^{-1}$ , etc., have traditional meanings.)

Note that the binary operation  $\circ$  does not have to be commutative. A group whose binary operation is commutative is a *commutative* or *Abelian group*.

### Examples.

- a. The positive rational numbers with multiplication form a group: first of all, it is an algebra: the product of any two positive rationals is a unique positive rational; multiplication is associative; 1 is an identity element (of multiplication) and every positive rational  $p/q$  has an inverse:  $(p/q)^{-1} = q/p$ . Furthermore, this group is Abelian since multiplication is commutative.

- b. The set  $Z$  of all positive and negative integers and zero with the binary operation of addition forms a group with 0 as an identity element. Of course,  $x^{-1} = -x$  here.
- c. The set of all even integers under addition forms a group but the set of all odd integers does not, since it does not contain an identity element, and it is not closed under addition (i.e. it is not even an algebra).
- d. The integers  $\{0,1,2,3\}$  form a group with the binary operation of addition modulo 4 and 0 as an identity element. [Exercise: how do we define inverse element in this group?].
- e. The algebra considered earlier of ‘symmetries of the square’ is a group (PtMW, Ch. 10, pp. 256-258). [Are all of its subalgebras also subgroups? Try this as an exercise. Does it matter with respect to which of our three group signatures we ask this question?]

From the group axioms it is not difficult to prove the following elementary statements (they are given in PtMW and we number them here in the same way):

Theorem 10.1. *In any group, the equations  $x \circ a = b$  and  $a \circ y = b$  have unique solutions  $x = b \circ a^{-1}$  and  $y = a^{-1} \circ b$  respectively.*

Corollary 10.1. *A group has only one identity element.*

Corollary 10.2. *A group has only one inverse  $a^{-1}$  for each element  $a$ .*

Theorem 10.2. *A group with 4 or fewer elements must be commutative.*

The proofs are given in PtMW [but they are recommended as optional exercises].

## 2.2. Subgroups.

We define a subgroup  $G'$  of a group  $G$  as a subalgebra of  $G$  which is itself a group. Note that if we consider groups as algebras in the signature  $\Omega_G$ , any subalgebra of group in this signature will be a group. [Exercise: but what if we just used the signature  $\Omega_G$  ?]

### Examples.

- a. The group of even integers with addition is a proper subgroup of the group of all integers with addition.
- b. The subgroups of the group of ‘symmetries of the square’ were considered earlier.
- c. The set of all non-negative integers with addition a subalgebra of the group of all integers with addition (considered as algebra in the signature  $\Omega_G$ ). But it is not a subgroup because it is not itself a group: it is associative, and has an identity element 0, but all of the members of its carrier except 0 lack inverses.

Theorem 10.3. *The intersection  $G' \cap G''$  of two subgroups  $G'$  and  $G''$  of a group  $G$  is itself a subgroup of  $G$ .*

*Proof:*

The proof is trivial if we consider groups as algebras in the signature  $\Omega_G$ . Subgroups are subalgebras and the intersection of subalgebras is a subalgebra in which all the group axioms hold.

### **3. Semigroups and monoids. Strings over some alphabet, concatenation.**

[Read pp.262-263 and pp.431-435 of PtMW]

#### **Homework13.**

1. There are quite a number of good questions in the handout, and theorems whose proofs you could try. Try some of those.
2. Show that no Boolean algebra can be a group (with one of its operations, e.g.  $\cup$ , as the group operation.) If it helps, first show it for a specific Boolean algebra – pick your favorite one – and that should give you ideas about how to show that no Boolean algebra could be a group. [This is very similar to questions 2e,f in PtMW, p. 271]
3. Try parts or all of question 5, PtMW, p. 272.
4. PtMW pp 272-3, question 8.
5. PtMW pp 273, question 9.
6. Read about integral domains in PtMW, and then (with just minimal reading) you can try the nice mathematical induction questions 13a,b on p. 274.