Linear Algebra with Application

(LAWA 2021)

Lecture 1

Francesco Dolce
francesco.dolce@fjfi.cvut.cz

February 17th, 2021

Let us start by fixing some notation and giving some basic example.

1 Numerical sets

We denote by $\mathbb{N}$ the set of *natural numbers*, that is

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\},$$

and with $\mathbb{Z}$ the set of *integers*

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}.$$

Two important subsets of $\mathbb{Z}$ are the sets $\mathbb{Z}^+$ of *positive integers* and $\mathbb{Z}^-$ of *negative integers*:

$$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}, \quad \text{and} \quad \mathbb{Z}^- = \{-1, -2, -3, \ldots\}.$$

We can also use the notations Z_0^+ and $\mathbb{Z}_0^-$ to denote respectively the sets of *non-negative integers* and the one of *non-positive integers*, that is:

$$\mathbb{Z}_0^+ = \{0, 1, 2, 3, \ldots\} \quad \text{and} \quad \mathbb{Z}_0^- = \{0, -1, -2, -3, \ldots\}.$$

Note that $Z_0^+ = \mathbb{Z}^+ \cup \{0\} = \mathbb{N}$.

Other important numerical sets are the set of *rational numbers* $\mathbb{Q}$ defined us

$$\mathbb{Q} = \left\{\frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0\right\} = \left\{0, \frac{1}{2}, -\frac{3}{5}, \dots\right\}$$

and the one of *real numbers* $\mathbb{R}$ (a formal definition is beyond the scope of this course)

$$\mathbb{R} = \left\{0, 1, -5, \frac{7}{4}, \sqrt{2}, \pi, e, \dots\right\}.$$

The last numerical set we will consider is the set of *complex numbers* $\mathbb{C}$ defined us

$$\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\},$$

where i is called the *imaginary unit* and satisfies $i^2 = -1$.

We have the following chain of inclusions:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

2 Algebraic structures with one operation

A *binary operation* on a set M is a map f from the cartesian product $M \times M$ to M, that is

$$\begin{aligned} f:\quad & M \times S \to M \\ & (x, y) \mapsto f(x, y). \end{aligned}$$

Example 1 The *sum* on $\mathbb{N}$ is the binary operation defined as

$$\begin{aligned} +:\quad & \mathbb{N} \times \mathbb{N} \to \mathbb{N} \\ & (a, b) \mapsto +(a, b) \end{aligned} .$$

Instead of $+(a, b)$, we usually denote the image of the sum by $a + b$. For istance, instead of $+(2, 3) = 5$ we will write $2 + 3 = 5$.

Some sets, when equipped with a binary operation (or more than one), have particular properties. According to which properties are satisfied, we use different names. In this section we consider the main algebraic structures equipped with just one binary operation.

2.1 Groupoids

Let us consider a set M and a binary operation $\circ : M \times M \to M$.

The pair $(M, \circ)$ is called a *groupoid* whenever the set M is *closed under* the operation $\circ$. That is, we have

$$\forall\, a, b \in M \quad a \circ b \in M.$$

Example 2 The pair $(\mathbb{N}, +)$ is a groupoid, since for every two natural numbers a, b one has $a + b \in \mathbb{N}$.

On the other hand, if we consider the set $M = \{0, 1, 2, \ldots, 9\}$, we have that M is not closed under the sum, since, for instance, $2 + 9 \notin M$.

Exercise 3 Find an infinite subset $S \subset \mathbb{N}$ such that $(S, +)$ is not a groupoid.

2.2 Semigroups

A groupoid $(M, \circ)$ is called a *semigroup* if the operation $\circ$ is *associative*, that is if

$$\forall\, a, b, c \in M \quad (a \circ b) \circ c = a \circ (b \circ c).$$

Example 4 The set $\mathbb{N}$ with the usual *multiplication* is a semigroup, since for every $a, b, c \in \mathbb{N}$ one has $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. The same is not true if we consider the *exponentiation* as binary operation. Indeed

$$\left(2^3\right)^2 = 64 \neq 512 = 2^{(3^2)}.$$

2.3 Monoids

A semigroup $(M, \circ)$ is called a *monoid* whenever there exists a *neutral element*, that is an element $e \in M$ such that

$$\forall\, a \in M \;\; a \circ e = e \circ a = e.$$

Note that in the definition we want e to be a neutral element both on the left and on the right. In some tricky case we could have a *left neutral element* but no *right neutral element*, or viceversa, or we could have both but distinct.

Example 5 The set $\mathbb{N}$ provided with the sum is a monoid. A neutral element is the element $0 \in \mathbb{N}$.

Proposition 6 *The neutral element of a monoid is unique.*

Proof. Let $(M, \circ)$ be a monoid and e some neutral element (from the 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 e' different from e. It holds that

$$e' = e' \circ e = e,$$

using the property of the neutral element from the definition. We get a contradiction with the statement that $e' \neq e$. ■

2.4 Groups

Let us consider a monoid $(M, \circ)$ with neutral element e. We say that an element $a \in M$ is *invertible*, whenever there exists another element $b \in M$ such that $a \circ b = e = b \circ a$. Such an element is called an *inverse* of a and it is usually denoted $-a$ (whenever we use the additive notation) or a^{-1} (whenever we use the multiplicative notation). Note that, again, we consider an inverse as both a *left inverse* and a *right inverse*.

A monoid $(M, \circ)$, with neutral element e, is called a *group* if every element is invertible, that is if

$$\forall\, a \in M\ \exists\, a^{-1} \in M \text{ such that } \quad a \circ a^{-1} = e \text{ and } a^{-1} \circ a = e.$$

Exercise 7 The monoid $(\mathbb{Z}, +)$ is a group, since the inverse of any element $a \in \mathbb{Z}$ is $-a$. On the other hand $(\mathbb{N}, +)$ is not a group since, for istance, the element $2 \in \mathbb{N}$ has no inverse.

Example 8 Find an infinite subset $S \subset \mathbb{Z}$ such that $(S, +)$ is a monoid but not a group.

Proposition 9 *Each element of a group has exactly one inverse.*

Proof. Let $(M, \circ)$ be a group, a an arbitrary element of the group and a^{-1} one of its inverse elements (from the definition we know that there exists at least one!) Let us suppose, by contradiction, that there exists another element $\bar{a}$, different from a^{-1} such that $\bar{a} \circ a = e = a \circ \bar{a}$, where e is the neutral element of the group. Hence, it holds that

$$\bar{a} = \bar{a} \circ e = \bar{a} \circ (a \circ a^{-1}) = (\bar{a} \circ a) \circ a^{-1} = e \circ a^{-1} = a^{-1},$$

contradicting the fact that $\bar{a} \neq a^{-1}$. ∎

A group $(M, \circ)$ is called *Abelian*, or *commutative*, if its elements commute, that is if

$$\forall\, a, b \in M \quad a \circ b = b \circ a.$$

Example 10 Both the additive group $(\mathbb{Q}, +)$ and the multiplicative group $(\mathbb{Q}, \cdot)$ are Abelian. The first has neutral element 0, while the second has neutral element 1.

A very important example of non Abelian group will be given later in this course.

3 Algebraic structures with two operations

Let us now consider triplets $(M, +\cdot)$, with M a nonempty set and $+, \cdot$ two binary operations on M.

3.1 Rings

We say that a triplet $R = (M, +, \cdot)$ is a *ring* if the following hold:

- $(M, +)$ is an Abelian group;
- $(M, \cdot)$ is a monoid;
- both left and right *distributive laws* hold, i.e. $\forall\, a, b, c \in M$ we have
  - $a \cdot (b + c) = a \cdot b + a \cdot c$ and
  - $(b + c) \cdot a = b \cdot a + c \cdot a$.

We respect the standard convention that multiplication has a higher priority than addition, so we can write $a \cdot b + a \cdot c$ instead of $(a \cdot b) + (a \cdot c)$.

Moreover, when it is clear from the context we replace $\cdot$ by the simple juxstaposition, that is we write ab instead of $a \cdot b$.

Example 11 Both the triplets $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Q}, +, \cdot)$ are rings. On the other hand the triplet $(\mathbb{N}, +, \cdot)$ is not a ring since $(\mathbb{N}, +)$ is not a group.

Example 12 The triplet $(\{0\}, +, \cdot)$, with $0 + 0 = 0$ and $0 \cdot 0 = 0$ is a ring called the *trivial ring*.

We say that a ring $R = (M, +, \cdot)$ is a *commutative ring* whenever $\cdot$ is commutative. The group $(M, +)$ is called the *additive group* of R, while the monoid $(M, \cdot)$ is the *multiplicative monoid* of R.

The neutral element of the additive group is called the *zero element* of the ring, and it is denoted by 0, and the inverse element of $a \in M$ is denoted by $-a$. We can also define the *subtraction* of two elements $a, b \in M$ by

$$a - b := a + (-b).$$

Proposition 13 *Let $(M, +, \cdot)$ be a ring. Left and right distributive laws hold for the subtraction, that is:*

$$\forall\, a, b, c \in M \quad a(b - c) = ab - ac \quad \text{and} \quad (a - b)c = ac - bc.$$

Proof. Let us prove the left distributive law, the right one being proved symmetrically. Since the distributive law hold for the sum, we have

$$ac + a(b - c) = a(c + b - c) = ab.$$

Thus, by subtracting ac to both members, we have

$$a(b - c) = ab - ac.$$

■

Example 14 The set of polynomials with real coefficients $\mathbb{R}[x]$ is a ring. The zero element is the zero polynomial $p(x) = 0$. We will talk more of this example later in the course.

3.2 Integral domains

Let $(M, +, \cdot)$ be a ring. Two non-zero elements $a, b \in M$ are called *zero divisors* if $a \cdot b = 0$.

A commutative ring without zero divisors is called an *integral domain.*

Example 15 The ring $(\mathbb{Z}, +, \cdot)$ is an integral domain. On the other hand the ring $(\mathbb{Z}_6, +_6, \cdot_6)$, where the sum and the product are defined *modulo* 6, is not an integral domain, since $2, 3 \neq 0$ but $2 \cdot_6 3 = 0$.

3.3 Fields

A ring $(M, +, \cdot)$ is a *field* if $(M \setminus \{0\}, \cdot)$ is an Abelian group. This group is called the *multiplicative group* of the field.

Example 16 The ring of integers $(\mathbb{Z}, +, \cdot)$ is not a field, since $(\mathbb{Z} \setminus \{0\}, \cdot)$ misses some inverse elements.

On the other hand, $(\mathbb{Q}, +, \cdot)$ is a field. Moreover, this is the smallest number field with the common arithmetical operations.

Example 17 The smallest field is the so-called *trivial field* $(\{0, 1\}, +, \cdot)$, with operations

$$0 + 0 = 0, \quad 0 + 1 = 1, \quad 1 + 0 = 1, \quad 1 + 1 = 0,$$

and

$$0 \cdot 0 = 0, \quad 0 \cdot 1 = 0, \quad 1 \cdot 0 = 0, \quad 1 \cdot 1 = 1.$$

Proposition 18 *Each field is an integral domain.*

Proof. Since the multiplicative group $(M \setminus \{0\}, \cdot)$ is closed under multiplication, for all non-zero elements $a, b \in M$ it holds that their product $a \cdot b \in M \setminus \{0\}$ is again non-zero. ■