Linear Algebra

Bachelor Applied Artificial Intelligence (AAI-B2)

André Herzwurm

TH Rosenheim, SoSe 2022

Literature

S. Axler, *Linear Algebra Done Right*, Springer, 3rd Edition, 2015.

G. Fischer, *Lineare Algebra*, Springer, 18. Auflage, 2014. (German)

J. Liesen, V. Mehrmann, *Linear Algebra*, Springer, 2015.

Contents

Chapter I

Algebraic Structures

In this chapter we introduce the notion of groups and fields. We also present simple examples and elementary properties of groups and fields.

1 Groups

In the sequel let G be a non-empty set.

Definition 1. A map

$$*\colon G \times G \to G$$

is called *operation* on G. An operation is *associative* if[1]

$$\forall\, a, b, c \in G\colon (a * b) * c = a * (b * c),$$

and *commutative* if

$$\forall\, a, b \in G\colon a * b = b * a.$$

Notation: Brackets may be dropped in case of an associative operation with multiple elements. Depending on the context we may also write $a + b$, $a \cdot b$, ab etc. instead of $a * b$.

Definition 2. A set G with an operation $*$ is called *group* if $*$ is associative and there exists $e \in G$ such that

$$\forall\, a \in G\colon e * a = a \tag{1}$$

and

$$\forall\, a \in G\ \exists\, a' \in G\colon a' * a = e. \tag{2}$$

Furthermore, a group is called *commutative (abelian)* if $*$ is commutative.

Notation: We sometimes write $(G, *)$ to emphasize the operation $*$.

[1] In a definition one typically uses "if" instead of "iff" (if and only if).

Example 3.

(i) Additive groups:

a) $(\mathbb{N}_0, +)$ is not a group since (2) does not hold.

b) $(\mathbb{Z}, +)$ is a commutative group with $e = 0$ and

$$\forall\, m \in \mathbb{Z}\colon \big(-m \in \mathbb{Z} \ \wedge\ (-m) + m = 0\big).$$

Clearly, $+$ is associative and commutative and

$$\forall\, m, n \in \mathbb{Z}\colon m + n \in \mathbb{Z}.$$

c) $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are commutative groups.

(ii) Multiplicative groups:

a) $(\mathbb{Z}, \cdot)$ is not a group since (2) does not hold. In particular, we have

$$\forall\, m \in \mathbb{Z}\colon m \cdot 0 = 0 \neq 1.$$

b) $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a commutative group with $e = 1$ and

$$\forall\, q \in \mathbb{Q} \setminus \{0\}\colon \big(1/q \in \mathbb{Q} \setminus \{0\} \ \wedge\ 1/q \cdot q = 1\big).$$

Clearly, $\cdot$ is associative and commutative and

$$\forall\, q_1, q_2 \in \mathbb{Q} \setminus \{0\}\colon q_1 \cdot q_2 \in \mathbb{Q} \setminus \{0\}.$$

c) $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are commutative groups.

(iii) $G = \{0, 1\}$ together with

$*$	0	1
0	0	1
1	1	0

is a commutative group. See `Exercise` 0.1.

Definition 4. Let $*$ be an operation on G and let $\varnothing \neq G' \subseteq G$ satisfy

$$\forall\, a, b \in G'\colon a * b \in G'.$$

Then the operation $*'\colon G' \times G' \to G'$, defined by $a *' b = a * b$, is called the *induced operation* on G'.

Henceforth we do not distinguish between $*$ and $*'$.

1.1 Permutations

Notation: The set of mappings from a set X to a set Y is denoted by Y^X.

Proposition 5. Let $X \neq \varnothing$ and

$$G = \{f \in X^X : f \text{ bijective}\}.$$

G together with function composition $\circ$ is a group. Moreover, G is not commutative if $|X| \geq 3$.

Definition 6. G from Proposition 5 is called the *symmetric group* of the set X. Its elements are called *permutations*.

1.2 Elementary Properties of Groups

In the sequel let G be a group.

Lemma 7. Let $e \in G$ satisfy (1) and (2) and let $a, a' \in G$. Then we have

(i) $a'a = e \Rightarrow aa' = e$,

(ii) $ae = a$.

Proof. ad (i): According to (2) there exists $a'' \in G$ such that

$$a''a' = e.$$

Using (1) we obtain

$$aa' = eaa' = a''a'aa' = a''ea' = a''a' = e.$$

ad (ii): Let $a' \in G$ such that $a'a = e$. From part (i) we get

$$ae = aa'a \overset{\text{(i)}}{=} ea = a. \qquad \square$$

Proposition 8. There exists a unique $e \in G$ satisfying (1) and (2).

Proof. Let (1) and (2) be satisfied for $e = e_1$ and $e = e_2$. Then we have $e_1e_2 = e_2$ and $e_2e_1 = e_1$. Lemma 7.(i) shows $e_2e_1 = e_2$ and hence $e_1 = e_2e_1 = e_2$. $\square$

Definition 9. $e \in G$ satisfying (1) and (2) is called the *neutral element* of G.

In the sequel let e be the neutral element of G.

Proposition 10. For every $a \in G$ there exists a unique $a' \in G$ such that $a'a = e$.

Proof. Let $a', a'' \in G$ such that $a'a = a''a = e$. Lemma 7.(i) shows $aa' = e$. Using Lemma 7.(ii) we obtain

$$a'' \overset{\text{(ii)}}{=} a''e = a''aa' = ea' = a'.$$

Cf. `Exercise` 0.2. $\square$

Definition 11. For $a \in G$ the element $a' \in G$ satisfying $a'a = e$ is called the *inverse element* of a.
Notation: $a' = a^{-1}$, $a' = 1/a$, or $a' = -a$.

Lemma 12. For $a, b, c \in G$ we have

(i) $ab = ac \Rightarrow b = c$,

(ii) $ba = ca \Rightarrow b = c$,

(iii) $(a^{-1})^{-1} = a$,

(iv) $(ab)^{-1} = b^{-1}a^{-1}$,

(v) $e^{-1} = e$,

(vi) $\exists_1 x \in G\colon ax = b$.

Proof. See `Exercise` 0.3. □

1.3 Subgroups

Definition 13. $G' \subseteq G$ is a *subgroup* of G if the following conditions hold:

(i) $G' \neq \varnothing$,

(ii) $\forall\, a, b \in G'\colon ab \in G'$,

(iii) $\forall\, a \in G'\colon a^{-1} \in G'$.

Remark 14. (i) Every subgroup G' of G satisfies $e \in G'$.
(Proof: Choose $a \in G'$. Then we obtain $a^{-1} \in G'$ and $e = aa^{-1} \in G'$.)

(ii) $\{e\}$ and G are the smallest and the largest subgroup of G, respectively, i.e., every subgroup G' of G satisfies $\{e\} \subseteq G' \subseteq G$.

Example 15. (i) $G' = \mathbb{Z}$ is a subgroup of $G = \mathbb{Q}$ w.r.t. the addition.

(ii) $G' = \{q \in \mathbb{Q}\colon q > 0\}$ is a subgroup of $G = \mathbb{Q} \setminus \{0\}$ w.r.t. the multiplication.

(iii) Let G be the symmetric group of X. For $X_0 \subseteq X$ put

$$G' = \{f \in G\colon \forall\, x \in X_0\colon f(x) = x\}.$$

Then G' is a subgroup of G.

Proposition 16. Every subgroup of G (together with the induced operation) is a group with neutral element e.

Proof. `Exercise`. □

Lemma 17. Let G_1 and G_2 be subgroups of G. Then $G_1 \cap G_2$ is a subgroup of G.

Proof. Note that $e \in G_1 \cap G_2$. Let $a, b \in G_1 \cap G_2$. Then we have $ab \in G_i$ and $a^{-1} \in G_i$ for $i = 1, 2$ since the G_i are subgroups of G. This shows $ab \in G_1 \cap G_2$ and $a^{-1} \in G_1 \cap G_2$. □

Example 18. $G_1 = \{2k \colon k \in \mathbb{Z}\}$ and $G_2 = \{3k \colon k \in \mathbb{Z}\}$ are subgroups of $G = \mathbb{Z}$ w.r.t. the addition. We have $G_1 \cap G_2 = \{6k \colon k \in \mathbb{Z}\}$.
Note that $-2, 3 \in G_1 \cup G_2$, but $(-2) + 3 = 1 \notin G_1 \cup G_2$. Thus $G_1 \cup G_2$ is not a subgroup of G, cf. `Exercise` 0.4.

2 Fields

Definition 1. A set K together with two operations

$$\begin{aligned} +&\colon K \times K \to K \quad \textit{(addition)} \\ \cdot&\colon K \times K \to K \quad \textit{(multiplication)} \end{aligned}$$

is a *field* if the following conditions hold:

(i) $(K, +)$ is a commutative group.

(ii) Let 0 be the neutral element in $(K, +)$. For $K^* = K \setminus \{0\}$ we have

$$\forall\, a, b \in K^* \colon a \cdot b \in K^*,$$

and $(K^*, \cdot)$ is a commutative group.

(iii) $\forall\, a, b, c \in K \colon \big(a \cdot (b + c) = a \cdot b + a \cdot c \wedge (a + b) \cdot c = a \cdot c + b \cdot c\big)$ (*distributivity*).

Notation: The neutral element and the inverse element of $a \in K$ in $(K, +)$ are denoted by 0 and $-a$, respectively. The neutral element in $(K^*, \cdot)$ is denoted by 1. The inverse element of $a \in K^*$ is denoted by a^{-1} or $1/a$.
We often write ab instead of $a \cdot b$ and $a - b$ instead of $a + (-b)$ for $a, b \in K$, and a/b instead of $a \cdot b^{-1}$ for $a \in K$ and $b \in K^*$.
Convention: $\cdot$ has precedence over $+$.

Remark 2. Per definition we have $0 \neq 1$ in every field.

Example 3. (i) $\mathbb{Q}$ with the usual operations $+$ and $\cdot$ is a field.

(ii) $K = \{0, 1\}$ with the addition according to Example 3.(iii) and the multiplication given by

$\cdot$	0	1
0	0	0
1	0	1

is a field. Note that $1 + 1 = 0$ in this case.

2.1 Elementary Properties of Fields

In the sequel let K be a field.

Lemma 4. For $a, b, c \in K$ we have

(i) $0 \cdot a = a \cdot 0 = 0$,

(ii) $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$,

(iii) $a \cdot (-b) = (-a) \cdot b = -(ab)$,

(iv) $(-a) \cdot (-b) = ab$,

(v) $a \cdot b = a \cdot c \wedge a \neq 0 \Rightarrow b = c$,

(vi) $a \neq 0 \Rightarrow (\exists_1 x \in K : a \cdot x = b)$.

Proof. See *Analysis I.* □

Remark 5. Due to Lemma 4.(i) the multiplication is associative and commutative on $K = K^* \cup \{0\}$ and

$$\forall\, a \in K : 1 \cdot a = a.$$

Note that 0 does not have an inverse element w.r.t. the multiplication.

2.2 Pointwise Addition and Multiplication of Functions

In the sequel let $X \neq \varnothing$.

Definition 6. *Addition* and *multiplication* on K^X are defined as follows: For $f, g \in K^X$ and $x \in X$ we put

$$(f + g)(x) = f(x) + g(x)$$

and

$$(f \cdot g)(x) = f(x) \cdot g(x).$$

Terminology: pointwise addition (or sum) and pointwise multiplication (or product) of functions, respectively.

Lemma 7.

(i) $(K^X, +)$ is a commutative group with neutral element $0 \in K^X$.

(ii) The multiplication is associative and commutative on K^X, and for $1 \in K^X$ we have

$$\forall\, f \in K^X : 1 \cdot f = f.$$

(iii) Distributivity holds.

(iv) For all $f \in K^X$ we have

$$\big(\exists\, g \in K^X \colon g \cdot f = 1\big) \Leftrightarrow \big(\forall\, x \in X \colon f(x) \neq 0\big).$$

Proof. `Exercise`. □

Notation: $f - g$ instead of $f + (-g)$ for $f, g \in K^X$ and f/g instead of $f \cdot h$ for $f \in K^X$ and $g \in K^X$ provided that $g(x) \neq 0$ and $h(x) = (g(x))^{-1}$ for all $x \in X$.