ALGEBRA

(A handbook for final exam preparation)

CONTENTS

1 Introduction

When writing this handbook, our intention was to provide the students with a selection of theoretical notions and solved exercise helpful in the preparation of the algebra subject of the final exam. Each of the main chapters – **Chapters 2, 3 and 4** – details one topic from the corresponding curricula.

For better support the students, we tried to produce a self-included theoretical part of reasonable length for this material. Yet, there are some completions the reader may consider useful. They can be found in the references. For instance, the last chapter uses some basic properties concerning the determinant or the rank of a matrix (only some of them listed at the beginning of the chapter). The students were supposed to know them from high school for matrices with number field entries. The general case do not differ much from the high school studied cases for the properties we are going to use here. However, if the reader wants a detailed presentation of the general case, it can be found in [3, Chapter VI]. On the other hand, the section 4.3 is quite poor in theoretical results. Our approach was to insist on the describing the most common algorithms used for solving systems of linear equations. For additional information, see [2, Chapter 3].

Except, maybe, for the considered lists of exercises, this material looks pretty much like the first year courses which refer to the discussed topics. Yet some slight changes concerning the notations or the order some results succeed may appear. The theoretical part is a mixture between the Romanian version of this handbook, based on [1] and [3] and the English Algebra course [2]. A hint for the reader who needs hints for solving the proposed exercises – which are listed in in the sections **Exercises** – is that all the exercises (solved or proposed) were taken from [5].

I thank **Septimiu Crivei**, **Ioan Purdea** and **Simion Breaz** for their support. One can say that this handbook is a joint work since, in order to produce the final version of this handbook in due time, we used some source files of [1], [2], [3] and [5]. The most obvious resemblance (or identity, sometimes) one can notice is with [5] and it concerns most of the theoretical issues presented here. My contribution stands mainly in organizing this handbook to serve its purpose and to look like an autonomous material. Of course, I do not exclude the possibility that some typewriting errors occur. I only hope they do not turn into mathematical errors. However, we invite the students to cooperate with us in finding and repairing these errors.

Cosmin Pelea

2 Groups, rings and fields

2.1 Groups

Definition 2.1. By a **binary operation** on a set A we understand a map

$$\varphi : A \times A \to A\,.$$

Since all the operations considered in this section are binary operations, we briefly call them **operations**. Usually, we denote operations by symbols like $*$, $\cdot$, $+$, and the image of an arbitrary pair $(x, y) \in A\times A$ is denoted by $x*y$, $x\cdot y$ (multiplicative notation), $x + y$ (additive notation), respectively.

Examples 2.2. a) The usual addition and multiplication are operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, but not on the set of irrational numbers.
b) The usual subtraction is an operation on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, but not on $\mathbb{N}$.
c) The usual division is an operation on $\mathbb{Q}^*, \mathbb{R}^*$, $\mathbb{C}^*$, but not on $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{N}^*$ or $\mathbb{Z}^*$.

Definitions 2.3. Let $*$ be an operation on A. We say that:
i) $*$ is **associative** if

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3),\ \forall a_1, a_2, a_3 \in A;$$

ii) $*$ is **commutative** if

$$a_1 * a_2 = a_2 * a_1,\ \forall a_1, a_2 \in A.$$

iii) $e \in A$ is an **identity element** for $*$ if

$$a * e = e * a = a,\ \forall a \in A.$$

When using the multiplicative or additive notation, an identity element e is usually denoted by 1 or 0, respectively.

Definitions 2.4. Let $(A, \cdot)$ be a monoid. A groupoid is called **semigroup** if its operation is associative. A semigroup $(A, *)$ is called **monoid** if it has an **identity element**. A groupoid, semigroup, monoid with a commutative operation is called **commutative groupoid**, **commutative semigroup**, **commutative monoid**, respectively.

Remarks 2.5. a) In a groupoid $(A, *)$ there exists at most an identity element.

Indeed, if an identity element does not exist, the statement is, obviously, true. If e and f are identity elements then, seeing each of them as an identity element, we have

$$e * f = f \text{ şi } e * f = e.$$

Hence $e = f$.
b) From a) one deduces that a monoid has a unique identity element.

In the next part of this section we prefer to use the multiplicative notation.

Definition 2.6. Let $(A, \cdot)$ be a groupoid with an identity element 1. An element $a \in A$ **has an inverse** if there exists an element $a' \in A$ such that

$$a \cdot a' = a' \cdot a = e.$$

We say that a' is an **inverse** for a.

Remarks 2.7. a) In any monoid $(A, \cdot)$ there exists at least an element which have an inverse, e.g. the identity element 1 (whose inverse is, of course, 1).
b) Let $(A, \cdot)$ be a monoid. If an inverse element for $a \in A$ does exist, then it is unique.

Indeed, if we suppose that a has $a_1, a_2 \in A$ as inverses, then we may compute the product $a_1 \cdot a \cdot a_2$ in two ways as

$$a_1 \cdot (a \cdot a_2) = a_1 \cdot 1 = a_1,$$

$$(a_1 \cdot a) \cdot a_2 = 1 \cdot a_2 = a_2$$

and we obtain $a_1 = a_2$.

The unique inverse of an element a of a monoid $(A, \cdot)$ is denoted by a^{-1}. When using the multiplicative notation, this notation changes into $-a$ and this element is usually called **the opposite of** a.

Definition 2.8. A groupoid $(A, \cdot)$ is called **group** if it is a monoid in which every element has an inverse. If the operation is commutative as well, the structure is called **commutative** or **Abelian group**.

Examples 2.9. a) $(\mathbb{N}, +)$ and $(\mathbb{Z}, \cdot)$ are commutative monoids, but they are not groups.
b) $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ are commutative monoids, but they are not groups since 0 has no inverse.
c) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ are Abelain groups.
d) Let $\{e\}$ be a single element set and let $\cdot$ be the only operation on $\{e\}$, defined by $e \cdot e = e$. Then $(\{e\}, \cdot)$ is an abelian group, called the **trivial group**.
e) Let M be a set, and $M^M = \{f \mid f : M \to M\}$. If $\circ$ is the usual map composition, then $(M^M, \circ)$ is a monoid. The identity function $1_M : M \to M$, $1_M(x) = x$ is its identity element and the invertible elements are the bijective functions.
f) Let $(G, \cdot)$ and $(G', \cdot)$ be groups with identity elements 1 and $1'$ respectively. Define on $G \times G'$ the operation $\cdot$ by

$$(g_1, g_1') \cdot (g_2, g_2') = (g_1 \cdot g_2, g_1' \cdot g_2')\,,\ \forall (g_1, g_1'), (g_2, g_2') \in G \times G'\,.$$

Then $(G \times G', \cdot)$ is a group, called the **direct product** of the groups G and G'. The identity element is $(1, 1')$ and the inverse of an element $(g, g') \in G \times G'$ is (g^{-1}, g'^{-1}). If $(G, \cdot)$ and $(G', \cdot)$ are both commutative, then $(G \times G', \cdot)$ is commutative.

The example can be easily generalized for n groups.

Remarks 2.10. a) From Remark 2.7 b) one deduces that in a group, each element has a unique inverse element.
b) The group definition can be rewritten: A groupoid $(A, \cdot)$ is a **group** if and only if it follows the following conditions:

(i) $(a_1 \cdot a_2) \cdot a_3 = a_1 \cdot (a_2 \cdot a_3)$, $\forall a_1, a_2, a_3 \in A$ ($\cdot$ is associative);
(ii) $\exists 1 \in A$, $\forall a \in A :\ a \cdot 1 = 1 \cdot a = a$ (there exists an identity element for $\cdot$);
(iii) $\forall a \in A$, $\exists a^{-1} \in A :\ a \cdot a^{-1} = a^{-1} \cdot a = 1$ (all the elements of A have inverses).

If $(A, \cdot)$ is a semigroup, then the operation $\cdot$ is associative, so for any $a \in A$ and $n \in \mathbb{N}^*$, we may define a^n as follows: $a^1 = a$, and if $n > 1$, then

$$a^n = a^{n-1} \cdot a = \underbrace{a \cdot \cdots \cdot a}_{n \text{ factors}}.$$

If $(A, \cdot)$ is a monoid and $a \in A$, we may define

$$a^0 = 1.$$

If, in addition, a has an inverse, and $n \in \mathbb{N}^*$, then we may define

$$a^{-n} = (a^{-1})^n.$$

If we work in additive notation, instead of a^n we write na.

One can easily check that in a group we have the following:

Proposition 2.11. (Some standard properties of group computation)
Let $(G, \cdot)$ be a group. The following properties hold:
1) For any $a, b \in G$,

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

$$ab = ba \Leftrightarrow (ab)^{-1} = a^{-1}b^{-1}.$$

2) For any $a, b \in G$ and any $m, n \in \mathbb{Z}$,

$$a^m a^n = a^{m+n}, \ (a^m)^n = a^{mn},$$

$$ab = ba \Rightarrow (ab)^n = a^n b^n.$$

3) **(Cancellation laws)** For any $a, x, y \in G$,

$$ax = ay \Rightarrow x = y,$$

$$xa = ya \Rightarrow x = y.$$

4) For any $a, b \in G$, each of the equations $ax = b$ and $ya = b$ has a unique solution in G ($x = a^{-1}b$ and $y = ba^{-1}$, respectively).

Corollary 2.12. If $(G, \cdot)$ is a group, then for any $a \in G$ the maps $t_a : G \to G$, $t_a(x) = ax$ and $t'_a : G \to G$, $t'_a(x) = xa$ are bijections.

Definitions 2.13. Let (A, φ) be a grupoid and $B \subseteq A$. We say that B is a **subgrupoid** of (A, φ) or that B **is closed under** φ if

$$b_1, b_2 \in B \Rightarrow \varphi(b_1, b_2) \in B.$$

If B is closed under φ, one can define an operation on B as follows:

$$\varphi' : B \times B \to B, \ \varphi'(b_1, b_2) = \varphi(b_1, b_2).$$

We call φ' the **operation induced** by φ on B or, briefly, the **induced operation**. Most of the time, we denote it also by φ.

Remarks 2.14. a) Let (A, φ) be a groupoid, $B \subseteq A$ closed under φ and let φ' be the induced operation on B. If φ is associative or commutative, then φ' is associative or commutative, respectively. So any subgroupoid B of a semigroup (A, φ) is a semigroup with respect to the induced operation, that is why a subgroupoid of a semigroup is called **subsemigroup**.
b) Let φ_1 and φ_2 be operations on A, let $B \subseteq A$ be closed under φ_1 and φ_2, and let φ_1' and φ_2' be the operations induced by φ_1 and φ_2 on B, respectively. If φ_1 is distributive with respect to φ_2, i.e.

$$\varphi_1(a_1, \varphi_2(a_2, a_3)) = \varphi_2(\varphi_1(a_1, a_2), \varphi_1(a_1, a_3)), \forall a_1, a_2, a_3 \in A,$$

then φ_1' is distributive with respect to φ_2'.
c) The existence of an identity element is not always preserved by induced operations. For instance, $\mathbb{N}^*$ is a subgroupoid of $(\mathbb{N}, +)$, but $(\mathbb{N}^*, +)$ has no identity element.

Example 2.15. Let M be a nonempty set and let us consider the monoid $(M^M, \circ)$ from Example 2.9 e). Then $S_M = \{f : M \to M \mid f \text{ is bijective}\}$ is closed under $\circ$ and the identity map 1_M is bijective, i.e. $1_M \in S_M$, hence $(S_M, \circ)$ is a monoid. Since any bijective map f has an inverse f^{-1} with respect to map composition, $(S_M, \circ)$ is a group. This group is called the **symmetric group of** M.

Definition 2.16. Let $(G, \cdot)$ be a group. A subset $H \subseteq G$ is called a **subgroup of** G if:
i) H is closed under the operation of $(G, \cdot)$, that is,

$$\forall x, y \in H\,, \quad x \cdot y \in H\,;$$

ii) H is a group with respect to the induced operation.

We denote by $H \leq G$ the fact that H is a subgroup of G.

Examples 2.17. a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are subgroups of $(\mathbb{C}, +)$, $\mathbb{Z}$, $\mathbb{Q}$ are subgroups of $(\mathbb{R}, +)$ and $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$.
b) $\mathbb{Q}^*$, $\mathbb{R}^*$ are subgroups of $(\mathbb{C}^*, \cdot)$ and $\mathbb{Q}^*$ is a subgroup of $(\mathbb{R}^*, \cdot)$.
c) $\mathbb{N}$ is a subsemigroup of $(\mathbb{Z}, +)$ which is not a subgroup.
d) Every non-trivial group $(G, \cdot)$ has two subgroups, namely $\{1\}$ and G. Any other subgroup of $(G, \cdot)$ is called **proper subgroup**.

Remarks 2.18. a) Any subgroup is a nonempty set.

This is a straightforward consequence of ii).
b) If H is a subgroup of the group $(G, \cdot)$, then the identity element of $(H, \cdot)$ coincides the identity element of $(G, \cdot)$.

Indeed, if e and 1 are the identity elements of H and G, respectively and $h \in H \subseteq G$, then we have in G:

$$eh = h = 1h.$$

Applying the left cancellation law for h in G we get $e = 1$.
c) If H is a subgroup of the group $(G, \cdot)$ and $h \in H$, then the inverse of h in $(H, \cdot)$ is the same as the inverse of h in $(G, \cdot)$.

Indeed, if h' and h^{-1} are inverses for h in H and G, respectively, from b) we deduce

$$h'h = e = 1 = h^{-1}h.$$

Applying the left cancellation law in G to the extreme members of this chain of equalities G we get $h' = h^{-1}$.

The following characterization theorem provides us with two easy ways to check if a subset of a group is a subgroup.

Theorem 2.19. (Teorema de caracterizare a subgrupului)
Let $(G, \cdot)$ be a group and $H \subseteq G$. The following statements are equivalent:
1) H is a subgroup of $(G, \cdot)$.
2)The following conditions hold for H:
α) $H \neq \emptyset$;
β) $h_1, h_2 \in H \Rightarrow h_1h_2 \in H$;
γ) $h \in H \Rightarrow h^{-1} \in H$.
3) The following conditions hold for H:
α) $H \neq \emptyset$;
δ) $h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H$.

Proof. 1) $\Rightarrow$ 2). From Remark 2.18 a) one deduces α), and β) and i) coincide; γ) follows directly from Remark 2.18 c).
2) $\Rightarrow$ 3). Using 2), we have:

$$h_1, h_2 \in H \Rightarrow h_1, h_2^{-1} \in H \Rightarrow h_1h_2^{-1} \in H.$$

Hence δ) holds.
3) $\Rightarrow$ 1). Taking $h_1 = h_2$ in δ) it follows that $1 \in H$. Let us consider an arbitrary $h \in H$ and let us apply δ) to $h_1 = 1$ and $h_2 = h$. We deduce that $h^{-1} \in H$. Using this and δ) we have:

$$h_1, h_2 \in H \Rightarrow h_1, h_2^{-1} \in H \Rightarrow h_1(h_2^{-1})^{-1} = h_1h_2 \in H.$$

So the operation of $(G, \cdot)$ induces an operation on H. The induced operation is, of course, associative and the above considerations help us conclude that H is a subgroup of $(G, \cdot)$. □

Remark 2.20. The condition α) can be replaced in Theorem 2.19 by the fact that $1 \in H$, and, most of the time, this is what we check in order to show that $H \neq \emptyset$.

Examples 2.21. a) The subset $H = \{z \in \mathbb{C} \mid |z| = 1\}$ of $\mathbb{C}^*$ is a subgroup of $(\mathbb{C}^*, \cdot)$.

Indeed, $H \neq \emptyset$ since $1 \in H$, so α) holds for H. Using the following properties of the absolute value

$$|z_1z_2| = |z_1| \cdot |z_2| \text{ and } |z^{-1}| = |z|^{-1}$$

we have

$$z_1, z_2 \in H \Rightarrow |z_1| = 1,\ |z_2| = 1 \Rightarrow |z_1z_2| = 1 \Rightarrow z_1z_2 \in H$$

and

$$z \in H \Rightarrow |z| = 1 \Rightarrow |z^{-1}| = 1 \Rightarrow z^{-1} \in H.$$

Hence β) and γ) also hold for H. Thus $H \leq (\mathbb{C}^*, \cdot)$.
b) Let us consider $n \in \mathbb{N}$. The set $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ of the integers which are multiples of n is a subgroup of $(\mathbb{Z}, +)$ since $n\mathbb{Z} \neq \emptyset$ and the difference of two multiples of n is a multiple of n. Thus α) and δ) hold for $n\mathbb{Z}$ or, equivalently, $n\mathbb{Z} \leq (\mathbb{Z}, +)$.

Let us remind that for a finite set X, we denote by $|X|$ the number of elements in the set X.

Theorem 2.22. (Lagrange Theorem) Let G be finite group and $H \leq G$. Then $|H|$ divides $|G|$.

Proof. Let $\rho_H \subseteq G \times G$ be the relation defined by

$$x \rho_H y \Leftrightarrow y \in xH,$$

where $xH = \{xh \mid h \in H\} \subseteq G$. We notice that

$$x \rho_H y \Leftrightarrow x^{-1} y \in H.$$

First, we show that ρ_H is an equivalence relation on G. The relation ρ_H is reflexive since

$$\forall x \in G,\ x^{-1}x = 1 \in H \ \Leftrightarrow\ \forall x \in G,\ x\rho_H x.$$

If $x\rho_H y$ and $y\rho_H z$ then $x^{-1}y \in H$ and $y^{-1}z \in H$. It follows that

$$(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$$

hence $x\rho_H z$. So ρ_H is transitive. The relation ρ_H is also symmetric since if $x\rho_H y$, i.e. $x^{-1}y \in H$, then $(x^{-1}y)^{-1} = y^{-1}x \in H$, i.e. $y\rho_H x$.

For any $x \in G$

$$\rho_H\langle x\rangle = \{y \in G \mid x\rho_H y\} = \{y \in G \mid x^{-1}y \in H\} = \{y \in G \mid y \in xH\} = xH.$$

We choose exactly one element from each of the different (and disjoint) classes

$$H, xH, yH, \ldots$$

and we get a subset $X \subseteq G$. The quotient set, i.e. the partition determined by ρ_H is

$$G/\rho_H = \{\rho_H\langle x\rangle \mid x \in X\} = \{xH \mid x \in X\},$$

hence

$$G = \bigcup_{x \in X} \rho_H\langle x\rangle = \bigcup_{x \in X} xH.$$

For any $x, y \in X$, $x \neq y$ we have $xH \bigcap yH = \emptyset$. Moreover, for any $x \in X$, the map $t_x : H \to xH$, $t_x(h) = xh$ is bijective, so $|H| = |xH|$. Then

$$|G| = \sum_{x \in X} |xH| = \underbrace{|H| + \cdots + |H|}_{|X| \text{ terms}} = |X||H|,$$

which concludes the proof. □

Definition 2.23. Let $(G, *)$, $(G', \perp)$ be two groups. A map $f : G \to G'$ is called **homomorphism** if

$$f(x_1 * x_2) = f(x_1) \perp f(x_2),\ \forall\ x_1, x_2 \in G.$$

A bijective homomorphism is called **isomorphism**. A homomorphism of $(G, *)$ into itself is called **endomorphism** of $(G, *)$. An isomorphism al lui $(G, *)$into itself is called **automorphism** of $(G, *)$. If there exists an isomorphism $f : G \to G$, we say that the groups $(G, *)$ and $(G', \perp)$ are isomorphic and we denote this by $G \simeq G'$ or $(G, *) \simeq (G', \perp)$.

Example 2.24. (a) Let $(G, \cdot)$ and $(G', \cdot)$ be groups and let $f : G \to G'$ be defined by $f(x) = 1'$, $\forall x \in G$. Then f is a homomorphism, called the **trivial homomorphism**.
(b) Let $(G, \cdot)$ be a group. Then the identity map $1_G : G \to G$ is an automorphism of G. This shows that $\simeq$ is reflexive.
(c) Let $(G, \cdot)$ be a group and let $H \leq G$. Define $i : H \to G$ by $i(x) = x$, $\forall x \in H$. Then i is a homomorphism, called the **inclusion homomorphism**.
(d) Let $n \in \mathbb{N}$ and define $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = nx$, $\forall x \in \mathbb{Z}$. Then f is an endomorphism of the group $(\mathbb{Z}, +)$.
(e) The groups $(\mathbb{R}, +)$ and $(\mathbb{R}_+^*, \cdot)$ are isomorphic. An isomorphism is $f : \mathbb{R} \to \mathbb{R}_+^*$ defined by $f(x) = e^x$, $\forall x \in \mathbb{R}$.
(f) The map $f : \mathbb{C}^* \to \mathbb{R}^*$, $f(z) = |z|$ is a group homomorphism from $(\mathbb{C}^*, \cdot)$ into $(\mathbb{R}^*, \cdot)$ since $f(z_1 z_2) = |z_1 z_2| = |z_1| \cdot |z_2| = f(z_1) f(z_2)$.
(g) The map $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$ (where $\overline{z}$ is the conjugate of z) is an automorphism of the group $(\mathbb{C}, +)$ and $f^{-1} = f$. Its restriction to $\mathbb{C}^*$ is an automorphism of $(\mathbb{C}^*, \cdot)$.
(h) For any group $(G, \cdot)$, the map $f : G \to G$, $f(x) = x^{-1}$ is bijective. The map f is an automorphism of $(G, \cdot)$ if and only if $(G, \cdot)$ is an Abelian group.

Let us come back to the multiplicative notation.

Theorem 2.25. Let $(G, \cdot)$ and $(G', \cdot)$ be groups, and let 1 and $1'$, respectively, be the identity element of $(G, \cdot)$ and $(G', \cdot)$, respectively. If $f : G \to G'$ is a group homomorphism, then:
(i) $f(1) = 1'$;
(ii) $[f(x)]^{-1} = f(x^{-1})$, $\forall x \in G$.

Proof. (i) We have $\forall x \in G$, $1 \cdot x = x \cdot 1 = x$, so that $f(1 \cdot x) = f(x \cdot 1) = f(x)$. Since f is a homomorphism, it follows that

$$f(1) \cdot f(x) = f(x) \cdot f(1) = f(x)\,,$$

whence we get $f(1) = 1'$ by multiplying by $(f(x))^{-1}$.
(ii) Let $x \in G$. Since $x \cdot x^{-1} = x^{-1} \cdot x = 1$, f is a homomorphism and $f(1) = 1'$, it follows that $f(x) \cdot f(x^{-1}) = f(x^{-1}) \cdot f(x) = 1'$. Hence $[f(x)]^{-1} = f(x^{-1})$. □

Theorem 2.26. Let $f : G \to G'$ be a group isomorphism. Then $f^{-1} : G' \to G$ is again a group isomorphism.

Proof. Clearly, f^{-1} is bijective. Now let $x', y' \in G'$. By the surjectivity of f, there exist $x, y \in G$ such that $f(x) = x'$ and $f(y) = y'$. Since f is a homomorphism, it follows that

$$f^{-1}(x' \cdot y') = f^{-1}(f(x) \cdot f(y)) = f^{-1}(f(x \cdot y)) = x \cdot y = f^{-1}(x') \cdot f^{-1}(y')\,.$$

Therefore, f^{-1} is an isomorphism. □

Corollary 2.27. a) If $(G, \cdot) \simeq (G', \cdot)$ then $(G', \cdot) \simeq (G, \cdot)$, hence $\simeq$ is symmetric.
b) An homomorphism $f : G \to G'$ is isomorphism if and only if there exists a homomorphism $g : G \to G'$ such that $g \circ f = 1_G$ şi $f \circ g = 1_{G'}$.

Theorem 2.28. Let $f : G \to G'$ and $g : G' \to G''$ be group homomorphisms (isomorphisms). Then $g \circ f : G \to G''$ is a group homomorphism (isomorphism).

Proof. For any $x_1, x_2 \in G$ we have

$$(g\circ f)(x_1x_2) = g(f(x_1x_2)) = g(f(x_1)f(x_2)) = g(f(x_1))\cdot g(f(x_2)) = (g\circ f)(x_1)\cdot(g\circ f)(x_2),$$

thus $g \circ f$ is a group homomorphism. The map composition of two bijective function is a bijective function, thus if f and g are isomorphisms, then $g \circ f$ is an isomorphism. □

Corollary 2.29. a) If $(G, \cdot) \simeq (G', \cdot)$ and $(G', \cdot) \simeq (G'', \cdot)$ then $(G, \cdot) \simeq (G'', \cdot)$, i.e. $\simeq$ is transitive.
b) Let $(G, \cdot)$ be a group and let us denote by $End(G, \cdot)$ and $Aut(G, \cdot)$ the set of its endomorphisms and automorphisms, respectively. Then $End(G, \cdot)$ is a subgroupoid of $(G^G, \circ)$ and $(End(G, \cdot), \circ)$ is a monoid. The set $Aut(G, \cdot)$ is closed in $(End(G, \cdot), \circ)$, it contains the identity element 1_G (see Example 2.24 (b)). According to Corollary 2.27, each element of $Aut(G, \cdot)$ has an inverse, thus $(Aut(G, \cdot), \circ)$ is a group.

For a map $f : A \to B$, $X \subseteq A$ and $Y \subseteq B$, we denote

$$f(X) = \{f(x) \mid x \in X\} \text{ and } \overset{-1}{f}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Theorem 2.30. Let $f : G \to G'$ be a group homomorphism and let $H \leq G$ and $H' \leq G'$. Then $f(H) \leq G'$ and $\overset{-1}{f}(H') \leq G$.

Proof. Since $1 \in H$ and $1' = f(1)$, we have $1' \in f(H)$. Now let $x', y' \in f(H)$. Then there exist $x, y \in H$ such that $f(x) = x'$ and $f(y) = y'$. It follows that

$$x'{y'}^{-1} = f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H),$$

hence $x'{y'}^{-1} \in f(H)$. Therefore, $f(H) \leq G'$.

Let us prove the second part. Since $f(1) = 1' \in H'$, we have $1 \in \overset{-1}{f}(H')$. Now let $x, y \in \overset{-1}{f}(H')$. Then there exist $x', y' \in H'$ such that $f(x) = x'$ and $f(y) = y'$. But since $H' \leq G'$ and f is a group homomorphism, we have

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} = x'{y'}^{-1} \in H'\,.$$

Hence $xy^{-1} \in \overset{-1}{f}(H')$. Consequently, $\overset{-1}{f}(H') \leq G$. □

Definition 2.31. Let $f : G \to G'$ be a group homomorphism. Then the set

$$\mathrm{Ker} f = \{x \in G \mid f(x) = 1'\}$$

is called the **kernel** of the homomorphism f.

By applying the second part of the previous theorem to the trivial subgroup $\{1'\}$ of G' we have:

Corollary 2.32. $\mathrm{Ker} f = \{x \in G \mid f(x) = 1'\}$ is a subgroup of G.

Theorem 2.33. Let $f : G \to G'$ be a group homomorphism. Then f is injective if and only if $\mathrm{Ker} f = \{1\}$.

Proof. $\Rightarrow$ Suppose that $\mathrm{Ker} f = \{1\}$. Let $x, y \in G$ be such that $f(x) = f(y)$. Then $f(x)(f(y))^{-1} = 1'$, whence it follows that $f(xy^{-1}) = 1'$, that is, $xy^{-1} \in \mathrm{Ker} f = \{1\}$. Hence $x = y$. Therefore, f is injective.
$\Leftarrow$ Suppose that f is injective. Clearly, $\{1\} \subseteq \mathrm{Ker} f$. If $x \in \mathrm{Ker} f$ then $f(x) = 1' = f(1)$, hence $x = 1$. Thus $\mathrm{Ker} f \subseteq \{1\}$ and $\mathrm{Ker} f = \{1\}$. □

2.2 Exercises with solution

1) Let M be a set, let $\mathcal{P}(M)$ be the set of its subsets and let us consider the **simmetric difference** $\triangle$, i.e. for $X, Y \subseteq M$, $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$. Show that $(\mathcal{P}(M), \triangle)$ is a group.

Solution: Let $C(X) = C_M X = M \setminus X$. We have

$$X \triangle Y = [X \cap C(Y)] \cup [Y \cap C(X)]. \tag{1}$$

In order to prove that $\triangle$ is associative, we show that

$$C(X \triangle Y) = (X \cap Y) \cup [C(X) \cap C(Y)]. \tag{2}$$

This results from (1), de Morgan laws and from distributivity of $\cap$ with respect to $\cup$ as follows:

$$\begin{aligned} C(X \triangle Y) &= C(X \cap C(Y)) \cap C(Y \cap C(X)) = [C(X) \cup Y] \cup [C(Y) \cup X] \\ &= \{[C(X) \cup Y] \cap C(Y)\} \cup \{[C(X) \cup Y] \cap X\} \\ &= [C(X) \cap C(Y)] \cup [Y \cap C(Y)] \cup [C(X) \cup X] \cup [Y \cap X] \\ &= [C(X) \cap C(Y)] \cup \emptyset \cup \emptyset \cup (X \cap Y) = (X \cap Y) \cup [C(X) \cap C(Y)]. \end{aligned}$$

Using (1) and (2) we deduce

$$\begin{aligned} &(X \triangle Y) \triangle Z = [(X + Y) \cap C(Z)] \cup [C(X + Y) \cap Z] \\ =&\{[(X \cap C(Y)) \cup (Y \cap C(X))] \cap C(Z)\} \cup \{[(X \cap Y) \cup (C(X) \cap C(Y))] \cap Z\} \\ =&[X \cap C(Y) \cap C(Z)] \cup [Y \cap C(X) \cap C(Z)] \cup [X \cap Y \cap Z] \cup [C(X) \cap C(Y) \cap Z] \\ =&(X \cap Y \cap Z) \cup [X \cap C(Y) \cap C(Z)] \cup [C(X) \cap Y \cap C(Z)] \cup [C(X) \cap C(Y) \cap Z]. \end{aligned}$$

One finds the same result when computing $X \triangle (Y \triangle Z)$. Hence $\triangle$ is associative.

From the definition of $\triangle$ it is easy to notice that $\triangle$ is commutative, that the empty set is the identity element and that $X\triangle X = \emptyset$, i.e. the opposite of X with respect to $\triangle$ is X. Thus $(\mathcal{P}(M), \triangle)$ is an Abelian group.

2) Let $G = (-1, 1)$, $x, y \in G$ and

$$(*) \qquad x * y = \frac{x+y}{1+xy}\,.$$

Show that:
i) the equality $(*)$ defines an operation $*$ on G and $(G, *)$ is an Abelian group;
ii) there exists an isomorphism $f : \mathbb{R}_+^* \to G$ between the multiplicative group of positive real numbers $(\mathbb{R}_+^*, \cdot)$ and $(G, *)$ which has the form $f(x) = \dfrac{\alpha x - 1}{x+1}$.
Solution: i) If $x, y \in G$ then $x * y \in G$ since

$$x * y = -1 + \frac{(x+1)(y+1)}{1+xy} \quad \text{and} \quad x * y = 1 - \frac{(x-1)(y-1)}{1+xy}\,.$$

So $*$ is an operation on G. From (1) one easily deduces the commutativity of $*$. The associativity results as follows:

$$\begin{aligned}(x * y) * z &= \frac{x+y}{1+xy} * z = \frac{x+y+z+xyz}{xy+xz+yz+1}\,,\\ x * (y * z) &= x * \frac{y+z}{1+yz} = \frac{x+y+z+xyz}{xy+xz+yz+1}\,.\end{aligned}$$

Let us assume that e is the identity element. Then $x * e = x$ for any $x \in G$, i.e.

$$\frac{x+e}{1+xe} = x,\ \forall x \in G.$$

It follows that $e = 0$. Hence, if an identity element exists, it must be 0. Since $x * 0 = x$, for any $x \in G$, we deduce that 0 is, indeed, the identity element. If x' is the inverse of $x \in G$ then $x * x' = 0$ which leads us to $x' = -x \in G$. So, if x has an inverse element, this must be $-x$. Conversely, one can easily check that $-x$ is, indeed, the inverse of any $x \in G$ with respect to $*$. Thus $(G, *)$ is an Abelian group.
ii) Since the image of the identity element through a group homomorphism is the identity element, $f(1) = 0$, which implies $\alpha = 1$. Hence

$$(**) \qquad f(x) = \frac{x-1}{x+1}\,.$$

Since

$$\begin{aligned}\frac{x-1}{x+1} > -1 &\Leftrightarrow \frac{2x}{x+1} > 0\,,\\ \frac{x-1}{x+1} < +1 &\Leftrightarrow \frac{-2}{x+1} < 0\,,\end{aligned}$$

$f(x) \in G$ for any $x \in \mathbb{R}_+^*$; this shows that the equality $(**)$ defines a map $f : \mathbb{R}_+^* \to G$. The map f is bijective since the equation $f(x) = y$ has a unique solution $x = \dfrac{1+y}{1-y} \in \mathbb{R}_+^*$. Easy computation shows that

$$f(x_1x_2) = \frac{x_1x_2 - 1}{x_1x_2 + 1} = f(x_1) * f(x_2)\,,$$

i.e. f is a homomorphism. Thus f is an isomorphism.

3) Let $(G,\cdot)$ be a finite group and $\emptyset \neq H \subseteq G$. Show that H is a subgroup of G if and only if H is closed under the multiplication of $(G,\cdot)$.

Solution: If $H \leq G$ then, obviously, H is closed in $(G,\cdot)$.

Let us take an arbitrary $h \in H$. If H is closed in $(G,\cdot)$, than the image of each restriction of each translation with h to H is in H. Therefore we can consider the maps

$$t_h, t'_h : H \to H,\ t_h(x) = hx,\ t'_h(x) = xh.$$

If $x_1, x_2 \in H$ and $t_h(x_1) = t_h(x_2)$, i.e. $hx_1 = hx_2$, using the cancellation laws, this equality leads us in G to $x_1 = x_2$. Hence t_h is injective, and, since H is finite, t_h is also bijective.

The surjectivity of t_h leads us to the existence of $e \in H$ for which $h = t_h(e) = he$. Then, in G, we have $1h = eh$. Using, again, the cancellation laws, we get $1 = e \in H$. Since t_h is surjective, există $h' \in H$ cu proprietatea că

$$1 = t_h(h') = hh' \Rightarrow hh^{-1} = 1 = hh' \Rightarrow h^{-1} = h' \in H.$$

But $h \in H$ is an arbitrary element, so the characterization theorem for subgroups helps us conclude that $H \leq G$.

4) Show that the only group homomorphism from $(\mathbb{Q},+)$ into $(\mathbb{Z},+)$ is the trivial one.

Solution: Let $f : \mathbb{Q} \to \mathbb{Z}$ be a homomorphism, an arbitrary $x \in \mathbb{Q}$ and $f(x) = a \in \mathbb{Z}$. For any $n \in \mathbb{N}^*$ we have

$$a = f(x) = f\left(n \cdot \frac{x}{n}\right) = f\Bigg(\underbrace{\frac{x}{n} + \cdots + \frac{x}{n}}_{n \text{ terms}}\Bigg) = \underbrace{f\left(\frac{x}{n}\right) + \cdots + f\left(\frac{x}{n}\right)}_{n \text{ terms}} = n \cdot f\left(\frac{x}{n}\right),$$

and since $f\left(\frac{x}{n}\right) \in \mathbb{Z}$, we deduce that $a = 0$ (being a multiple of any $n \in \mathbb{N}^*$), hence $f(x) = 0$ for any $x \in \mathbb{Q}$.

5) Find all the automorphisms of the group $(\mathbb{Z},+)$.

Solution: Let $f : \mathbb{Z} \to \mathbb{Z}$ be an endomorphism of $(\mathbb{Z},+)$. If $x \in \mathbb{N}^*$, then

$$f(x) = f(\underbrace{1 + 1 + \cdots + 1}_{x \text{ terms}}) = xf(1)$$

and $f(-x) = -f(x)$. Obviously, $f(0) = 0 = f(1) \cdot 0$, so,

$$f(x) = f(1) \cdot x,\ \forall x \in \mathbb{Z}.$$

If f is an automorphism, since f is surjective, there exists $a \in \mathbb{Z}$ such that $1 = f(1) \cdot a$. It follows that $f(1)$ divides 1, which means that $f(1) \in \{-1, 1\}$. If $f(1) = 1$, then $f = 1_{\mathbb{Z}}$ which is, of course, an automorphism of $(\mathbb{Z},+)$, and if $f(1) = -1$, then f is

$$-1_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z},\ (-1_{\mathbb{Z}})(x) = -x$$

for which one easily can show that it is an automorphism of $(\mathbb{Z},+)$.

Thus the automorphisms of $(\mathbb{Z},+)$ are $1_{\mathbb{Z}}$ and $-1_{\mathbb{Z}}$.

2.3 Rings and fields

Definition 2.34. Let R be a set. A structure $(R, +, \cdot)$ with two operations is called:
(1) **ring** if $(R, +)$ is an Abelian group, $(R, \cdot)$ is a semigroup and the distributive laws hold (that is, $\cdot$ is distributive with respect to $+$).
(2) **unitary ring** if $(R, +, \cdot)$ is a ring and there exists a multiplicative identity element.

Definition 2.35. Let $(R, +, \cdot)$ be e unital ring. An element $x \in R$ which has an inverse $x^{-1} \in R$ is called **unit**. The ring $(R, +, \cdot)$ is called **division ring** if it is a unitary ring, $|R| \geq 2$ and any $x \in R^*$ is a unit. A commutative division ring is called **field**.

Definition 2.36. Let $(R, +, \cdot)$ be a ring. An element $x \in R^*$ is called **zero divisor** if there exists $y \in R^*$ such that

$$x \cdot y = 0 \text{ or } y \cdot x = 0.$$

We say that R is an **integral domain** if $R \neq \{0\}$, R is unitary, commutative and has no zero divisors.

Remarks 2.37. (1) Notice that $x \in R^*$ is not a zero divisor iff

$$y \in R\,,\ x \cdot y = 0 \text{ or } y \cdot x = 0 \ \Rightarrow\ y = 0\,.$$

(2) A ring R has no zero divisors if and only if

$$x, y \in R\,,\ x \cdot y = 0 \Rightarrow x = 0 \text{ or } y = 0\,.$$

(3) $(R, +, \cdot)$ is a division ring if and only if it satisfies the following conditions:
i) $(R, +)$ is an Abelian group;
ii) R^* is closed in $(R, \cdot)$ and $(R^*, \cdot)$ is a group;
iii) $\cdot$ is distributive with respect to $+$.
(4) Every field has no zero divisor. Moreover, every field is an integral domain.

Examples 2.38. (a) $(\mathbb{Z}, +, \cdot)$ is an integral domain, but it is not a field. Its units are -1 and 1.
(b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are fields.
(c) Let $\{0\}$ be a single element set and let both $+$ and $\cdot$ be the only operation on $\{0\}$, defined by $0 + 0 = 0$ and $0 \cdot 0 = 0$. Then $(\{0\}, +, \cdot)$ is a commutative unitary ring, called the **trivial ring** (or **zero ring**). The multiplicative identity element is, of course, 0, hence we can write $1 = 0$. As matter of fact, this equality characterize the trivial ring.
(d) Let R be a set and $m, n \in \mathbb{N}^*$. A map

$$A : \{1, \ldots, m\} \times \{1, \ldots, n\} \to R$$

is called $m \times n$ **matrix with entries in** R. When $m = n$, one says that A is a **square matrix**. For all $i = 1, \ldots, m$ and $j = 1, \ldots, n$ we denote $A(i, j)$ by $a_{ij} (\in R)$; we can write A as a rectangular array with m rows and n columns such that the element from the i-th row and j-th column is the image of (i, j):

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ldots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

We also write $A = (a_{ij})$. We denote the set of $m \times n$ matrices with entries in R by $M_{m,n}(R)$, or by $M_n(R)$ when $m = n$. If $(R, +, \cdot)$ is a ring, the $+$ from R induces an operation $+$ on $M_{m,n}(R)$ as follows: if $A = (a_{ij})$ and $B = (b_{ij})$ are $m \times n$ matrices, then

$$A + B = (a_{ij} + b_{ij}).$$

One can easily check that this (matrix) addition is associative, commutative, the matrix $O_{m,n}$ with all entries 0 is its identity element and each $A = (a_{ij})$ from $M_{m,n}(R)$ has an opposite matrix $-A = (-a_{ij})$.

The term **matrix multiplication** is used for the partial operation defined on

$$\bigcup\{M_{m,n}(R) \mid (m,n) \in \mathbb{N}^* \times \mathbb{N}^*\}$$

as follows: if $A = (a_{ij}) \in M_{m,n}(R)$ and $B = (b_{ij}) \in M_{n,p}(R)$, then

$$AB = (c_{ij}) \in M_{m,p}, \text{ cu } c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}, \ (i,j) \in \{1,\dots,m\} \times \{1,\dots,p\}.$$

If we take $m = n = p$, hence we work with $n \times n$ square matrices $\cdot$ becomes an operation as in Definition 2.1, operation which is associative and distributive with respect to $+$. Thus $(M_n(R), +, \cdot)$ is a ring, called the **ring of matrices $n \times n$ with entries in R** If R has a multiplicative identity, then $M_n(R)$ has a multiplicative identity. This is

$$I_n = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

If $n \geq 2$ and $R \neq \{0\}$ then $M_n(R)$ is not commutative and it has zero divisors. Indeed, if $a, b \in R^*$, one can multiply the non-zero matrices

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \dots & b \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

both sides for showing these facts.

If R is a unitary ring, the units of $M_n(R)$ are the elements of

$$GL_n(R) = \{A \in M_n(R) \mid \exists B \in M_n(R) : AB = BA = I_n\}.$$

$GL_n(R)$ is closed under the matrix multiplication, it preserves the identity of $(M_n(R), \cdot)$ and $(GL_n(R), \cdot)$ is a group called the **general linear group over R**. One knows that if R is one of the number fields ($\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$) then $A \in M_n(R)$ is invertible if and only if $\det A \neq 0$. Thus,

$$GL_n(\mathbb{C}) = \{A \in M_n(\mathbb{C}) \mid \det A \neq 0\},$$

and similarly one can define $GL_n(\mathbb{R})$ and $GL_n(\mathbb{Q})$.

(e) Let $n \in \mathbb{N},\ n \geq 2$. The Division Algorithm in $\mathbb{Z}$ gives us a partition of $\mathbb{Z}$ in classes determined by the remainders one can find when dividing by n :

$$\{n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}\},$$

where $r+n\mathbb{Z} = \{r+nk \mid k \in \mathbb{Z}\}$ $(r \in \mathbb{Z})$. We use the following notations

$$\widehat{r} = r+n\mathbb{Z}\ (r \in \mathbb{Z}) \text{ şi } \mathbb{Z}_n = \{n\mathbb{Z}, 1+n\mathbb{Z}, \dots, (n-1)+n\mathbb{Z}\} = \{\widehat{0}, \widehat{1}, \dots, \widehat{n-1}\}.$$

Let us notice that for $a, r \in \mathbb{Z}$,

$$\widehat{a} = \widehat{r} \Leftrightarrow a+n\mathbb{Z} = r+n\mathbb{Z} \Leftrightarrow a-r \in n\mathbb{Z} \Leftrightarrow n|a-r.$$

The operations

$$\widehat{a}+\widehat{b} = \widehat{a+b},\quad \widehat{a}\,\widehat{b} = \widehat{ab}$$

are well defined, i.e. if one considers another representatives a' and b' for the classes $\widehat{a}$ and $\widehat{b}$, respectively, the operations provide us with the same results. Indeed, from $a' \in \widehat{a}$ şi $b' \in \widehat{b}$ it follows that

$$n|a'-a,\ n|b'-b \Rightarrow n|a'-a+b'-b \Rightarrow n|(a'+b')-(a+b) \Rightarrow \widehat{a'+b'} = \widehat{a+b}$$

and

$$a' = a+nk,\ b' = b+nl\ (k,l \in \mathbb{Z}) \Rightarrow a'b' = ab+n(al+bk+nkl) \in ab+n\mathbb{Z} \Rightarrow \widehat{a'b'} = \widehat{ab}.$$

One can easily check that the operations $+$ and $\cdot$ are associative and commutative, $+$ has $\widehat{0}$ as identity element, each class $\widehat{a}$ has an opposite in $(\mathbb{Z}_n, +)$, $-\widehat{a} = \widehat{-a} = \widehat{n-a}$, $\cdot$ has $\widehat{1}$ as identity element and $\cdot$ is distributive with respect to $+$. Thus, $(\mathbb{Z}_n, +, \cdot)$ is a unitary ring, called $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring, called the **residue-class ring modulo** n.

Since $\widehat{2} \cdot \widehat{3} = \widehat{0}$, both $\widehat{2}$ and $\widehat{3}$ are zero divisors in the ring $(\mathbb{Z}_6, +, \cdot)$. Thus $(\mathbb{Z}_n, +, \cdot)$ is not a field in the general case. Actually, $\widehat{a} \in \mathbb{Z}_n$ is a unit if and only if $(a, n) = 1$. Thus $(\mathbb{Z}_n, +, \cdot)$ is a field if and only if n is a prime number.

Remark 2.39. If $(R, +, \cdot)$ is a ring, then $(R, +)$ is a group and $(R, \cdot)$ is a semigroup, so that we may talk about multiples and positive powers of elements of R.

Definition 2.40. Let $(R, +, \cdot)$ be a ring, let $x \in R$ and let $n \in \mathbb{N}^*$. Then we define

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ terms}},\ 0 \cdot x = 0\,,\ (-n) \cdot x = -n \cdot x\,,$$

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ factors}}.$$

If R is a unitary ring, then we may also consider $x^0 = 1$. If R is a division ring, then we may also define negative powers of nonzero elements x by

$$x^{-n} = (x^{-1})^n\,.$$

Remark 2.41. Notice that in the definition $0 \cdot x = 0$, the first 0 is the integer zero and the second 0 is the zero element of the ring R, i.e., the identity element of the additive group $(R, +)$.

Clearly, the first computational properties of a ring $(R, +, \cdot)$ are the properties of the group $(R, +)$ and of the semigroup $(R, \cdot)$. Some relationship properties between the two operations are given in the following result.

Theorem 2.42. Let $(R, +, \cdot)$ be a ring and let $x, y, z \in R$. Then:
(i) $x \cdot (y - z) = x \cdot y - x \cdot z$, $(y - z) \cdot x = y \cdot x - z \cdot x$;
(ii) $x \cdot 0 = 0 \cdot x = 0$;
(iii) $x \cdot (-y) = (-x) \cdot y = -x \cdot y$.

Proof. (i) We have

$$x \cdot (y - z) = x \cdot y - x \cdot z \Leftrightarrow x \cdot (y - z) + x \cdot z = x \cdot y \Leftrightarrow x \cdot (y - z + z) = x \cdot y \,,$$

the last equality being obviously true. Similarly, $(y - z) \cdot x = y \cdot x - z \cdot x$.
(ii) $x \cdot 0 = x \cdot (y - y) = x \cdot y - x \cdot y = 0$. Similarly, $0 \cdot x = 0$.
(iii) We have

$$x \cdot (-y) = -x \cdot y \Leftrightarrow x \cdot (-y) + x \cdot y = 0 \Leftrightarrow x \cdot (-y + y) = 0 \Leftrightarrow x \cdot 0 = 0 \,,$$

the last equality being true by (ii). □

Definition 2.43. Let $(R, +, \cdot)$ be a ring and $A \subseteq R$. Then A is a **subring of** R if:
(1) A is closed under the operations of $(R, +, \cdot)$, that is,

$$\forall x, y \in A \,,\ x + y \,,\ x \cdot y \in A \,;$$

(2) $(A, +, \cdot)$ is a ring.

Remarks 2.44. (a) If $(R, +, \cdot)$ is a ring and $A \subseteq R$, then A is a subring of R if and only if A is a subgroup of $(R, +)$ and A is closed in $(R, \cdot)$.

This follows directly from subring definition and Remark 2.14 b).
(b) A ring R may have subrings with or without (multiplicative) identity, as we will see in a forthcoming example.

Using Remark 2.44 (a) and the characterization theorem for subgroups, one can easily prove the following **characterization theorem for subrings**:

Theorem 2.45. Let $(R, +, \cdot)$ be a ring and $A \subseteq R$. The following conditions are equivalent:
1) A is a subring of $(R, +, \cdot)$.
2) The following conditions hold for A:
α) $A \neq \emptyset$;
β) $\alpha_1, \alpha_2 \in A \Rightarrow a_1 - a_2 \in A$;
γ) $\alpha_1, a_2 \in A \Rightarrow a_1 a_2 \in A$.
3) The following conditions hold for A:
α) $A \neq \emptyset$;
β') $a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A$;
β'') $a \in A \Rightarrow -a \in A$;
γ) $a_1, a_2 \in A \Rightarrow a_1 a_2 \in A$.

Definition 2.46. Let $(K,+,\cdot)$ be a field and let $A \subseteq K$. Then A is called a **subfield of K** if:
(1) A is closed under the operations of $(K,+,\cdot)$, that is,

$$\forall x, y \in K\,,\ x+y\,,\ x\cdot y \in K\,;$$

(2) $(A,+,\cdot)$ is a field.

Remarks 2.47. (a) From (2) it follows that for a subfield A, we have $|A| \geq 2$.
(b) If $(K,+,\cdot)$ is a field and $A \subseteq K$, then A is a subfield if and only if A is a subgroup of $(K,+)$ and A^* is a subgroup of $(K^*,\cdot)$.
(c) f $(K,+,\cdot)$ is a field and $A \subseteq K$, then A is a subfield if and only if A is a subring of $(K,+,\cdot)$, $|A| \geq 2$ and for any $a \in A^*$, $a^{-1} \in A$.

Next result provide us with a **characterization theorem for subfields**.

Theorem 2.48. Let $(K,+,\cdot)$ be a field and $A \subseteq K$. The following conditions are equivalent: 1) A is a subfield of $(K,+,\cdot)$.
2) The following conditions hold for A:
α) $|A| \geq 2$;
β) $a_1, a_2 \in A \Rightarrow a_1 - a_2 \in A$;
γ) $a_1, a_2 \in A;\ a_2 \neq 0 \Rightarrow a_1 a_2^{-1} \in A$;
3) The following conditions hold for A:
α) $|A| \geq 2$;
β') $a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A$;
β'') $a \in A \Rightarrow -a \in A$;
γ') $a_1, a_2 \in A \Rightarrow a_1 a_2 \in A$;
γ'') $a \in A;\ a \neq 0 \Rightarrow a^{-1} \in A$.

Proof. It follows from Remark 2.47 and Theorem 2.19. □

Examples 2.49. (a) Every non-trivial ring $(R,+,\cdot)$ has two subrings, namely $\{0\}$ and R, called the **trivial subrings**.
(b) $\mathbb{Z}$ is a subring of $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$, $\mathbb{Q}$ is a subfield of $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$, $\mathbb{R}$ is a subfield of $(\mathbb{C},+,\cdot)$.
(c) If $n \in \mathbb{N}$, then $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a subring of $(\mathbb{Z},+,\cdot)$. Indeed, $0 = n\cdot 0 \in n\mathbb{Z}$, and since for any $x, y \in n\mathbb{Z}$, there exist $k, l \in \mathbb{Z}$ such that $x = nk$ and $y = nl$, we have $x - y = n(k-l) \in n\mathbb{Z}$ and $x \cdot y = n(nkl) \in n\mathbb{Z}$. One notices that the ring induced on $2\mathbb{Z}$ by the operations of $(\mathbb{Z},+,\cdot)$ has no multiplicative identity.
(d) The set $\mathbb{Z}[i] = \{x + iy \mid x, y \in \mathbb{Z}\}$ of Gauss integers is a subring of $(\mathbb{C},+,\cdot)$. Thus $(\mathbb{Z}[i],+,\cdot)$ is a ring, called the **ring of Gauss integers**.

Definition 2.50. Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings and $f : R \to R'$. Then f is called a **(ring) homomorphism** if

$$f(x+y) = f(x) + f(y)\,,\ \forall x, y \in R$$

$$f(x\cdot y) = f(x)\cdot f(y)\,,\ \forall x, y \in R.$$

The notions of **(ring) isomorphism**, **endomorphism** and **automorphism** are defined as usual.

Remark 2.51. If $f : R \to R'$ is a ring homomorphism, then the first condition from its definition tells us that f is a group homomorphism between $(R, +)$ and $(R', +)$. Then f takes the identity element of $(R, +)$ to the identity element of $(R', +)$, that is, $f(0) = 0'$ and we also have $f(-x) = -f(x)$, for any $x \in R$ (see Theorem 2.25). But in general, even if R and R' have identities, denoted by 1 and $1'$ respectively, in general it does not follow that a ring homomorphism $f : R \to R'$ has the property that $f(1) = 1'$.

We denote by $R \simeq R'$ the fact that two rings R and R' are isomorphic.

Examples 2.52. (a) Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be rings and let $f : R \to R'$ be defined by $f(x) = 0'$, $\forall x \in R$. Then f is a homomorphism, called the **trivial homomorphism**. Notice that if R and $R' \neq \{0'\}$ have identities, we do not have $f(1) = 1'$.
(b) Let $(R, +, \cdot)$ be a ring. Then the identity map $1_R : R \to R$ is an automorphism of R.
(c) Let $(R, +, \cdot)$ be a ring and let $A \leq R$. Define $i : A \to R$ by $i(x) = x$, $\forall x \in A$. Then i is a homomorphism, called the **inclusion homomorphism**.
(d) The map $f : \mathbb{R} \to M_2(\mathbb{R})$, $f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ is a ring homomorphism between the rings $(\mathbb{R}, +, \cdot)$ and $(M_2(\mathbb{R}), +, \cdot)$.
(e) More general, if R is a ring and $n \in \mathbb{N}^*$, the map $f : R \to M_n(R)$,

$$f(a) = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a \end{pmatrix}$$

is an injective ring homomorphism.
(f) Let us take $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$ (where $\overline{z}$ is the complex conjugate of z). Since

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},\ \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} \text{ and } \overline{\overline{z}} = z,$$

f is an automorphism of $(\mathbb{C}, +, \cdot)$ and $f^{-1} = f$.

Definition 2.53. Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be rings with identity elements 1 and $1'$ respectively and let $f : R \to R'$ be a ring homomorphism. Then f is called a **unitary homomorphism** if $f(1) = 1'$.

Theorem 2.54. *Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be rings with identity elements 1 and $1'$ respectively and let $f : R \to R'$ be a unitary ring homomorphism. If $x \in R$ has an inverse element $x^{-1} \in R$, then $f(x)$ has an inverse and $f(x^{-1}) = [f(x)]^{-1}$.*

Proof. Since $xx^{-1} = 1 = x^{-1}x$, we have

$$f(x)f(x^{-1}) = 1' = f(x^{-1})f(x)$$

which completes the proof. □

Remark 2.55. Any non-zero homomorphism between two fields is a unitary homomorphism.

Indeed, if $(K,+,\cdot)$ and $(K',+,\cdot)$ are fields and $f: K \to K'$ is a non-zero homomorphism, there exists $x_0 \in K$ such that $f(x_0) \neq 0$. Since $1 \cdot x_0 = x_0$,

$$f(1)f(x_0) = f(x_0) = 1' f(x_0),$$

multiplying both extreme members by the inverse of $f(x_0)$, we get $f(1) = 1'$.

2.4 Exercises with solution

1) Let M be a set and $\mathcal{P}(M) = \{X \mid X \subseteq M\}$. We consider on $\mathcal{P}(M)$ the operations $+$ and $\cdot$ defined by:

$$X + Y = (X \setminus Y) \cup (Y \setminus X) \text{ şi } X \cdot Y = X \cap Y.$$

Show that:
i) $(\mathcal{P}(M),+,\cdot)$ is commutative unitary ring;
ii) if $|M| \geq 2$ than any $X \in \mathcal{P}(M) \setminus \{\emptyset, M\}$ is a zero divisor;
iii) $(\mathcal{P}(M),+,\cdot)$ is a field if and only if $|M| = 1$.

Solution: i) One notices that $X+Y$ is the symmetric difference of X and Y, so the solved exercise 1) of the previous section tells us that $(\mathcal{P}(M),+)$ is an Abelian group. Using the set intersection properties, one deduces that $\cdot$ is associative, commutative and M is its identity element. Hence $(\mathcal{P}(M),\cdot)$ is a commutative monoid.

Let us prove the distributivity of $\cdot$ with respect to $+$. Indeed,

$$\begin{aligned}
X \cdot Y + X \cdot Z &= (X \cap Y) + (X \cap Z) \\
&= [(X \cap Y) \cap C(X \cap Z)] \cup [(X \cap Z) \cap C(X \cap Y)] \\
&= [X \cap Y \cap (C(X) \cup C(Z))] \cup [X \cap Z \cap (C(X) \cup C(Y))] \\
&= [X \cap Y \cap C(X)] \cup [X \cap Y \cap C(Z)] \cup [X \cap Z \cap C(X)] \cup [X \cap Z \cap C(Y)] \\
&= \emptyset \cup [X \cap Y \cap C(Z)] \cup \emptyset \cup [X \cap Z \cap C(Y)] \\
&= [X \cap Y \cap C(Z)] \cup [X \cap Z \cap C(Y)] = X \cap [(Y \cap C(Z)) \cup (Z \cap C(Y))] \\
&= X \cdot (Y + Z),
\end{aligned}$$

Thus $(\mathcal{P}(M),+,\cdot)$ is a unitary commutative ring. Its additive identity is $\emptyset$, and its multiplicative identity is M.
ii) In this ring, for any $X \subseteq M$, $X^2 = X$, or, equivalently, $X(X-1) = 0$, which means for us $X(X+M) = \emptyset$. This shows that any $X \in \mathcal{P}(M) \setminus \{\emptyset, M\}$ is a zero divisor.
iii) From ii) it follows that $(\mathcal{P}(M),+,\cdot)$ has no zero divisors if and only if $P(M) = \{\emptyset, M\}$, i.e. $|M| \leq 1$. If $|M| = 0$ then $M = \emptyset$ and $(\mathcal{P}(M),+,\cdot)$ is the trivial ring, and if $|M| = 1$ then $(\mathcal{P}(M),+,\cdot)$ is isomorphic to $(\mathbb{Z}_2,+,\cdot)$, thus $(\mathcal{P}(M),+,\cdot)$ is a field.

2) Let $(R,+,\cdot)$ be a ring and $a, b \in R$. Show that:
a) $(a+b)^2 = a^2 + 2ab + b^2 \Leftrightarrow ab = ba \Leftrightarrow a^2 - b^2 = (a-b)(a+b)$;
b) if $ab = ba$, then for any $n \in \mathbb{N}^*$,

$$\begin{aligned}
(a+b)^n &= C_n^0 a^n + C_n^1 a^{n-1} b + \cdots + C_n^{n-1} a b^{n-1} + C_n^n b^n; \\
a^n - b^n &= (a-b)\left(a^{n-1} + a^{n-2} b + \cdots + a b^{n-2} + b^{n-1}\right); \\
a^{2n+1} + b^{2n+1} &= (a+b)\left(a^{2n} - a^{2n-1} b + \cdots - a b^{2n-1} + b^{2n}\right).
\end{aligned}$$

Solution: a) If $(a+b)^2 = a^2+2ab+b^2$ then $a^2+ab+ba+b^2 = a^2+ab+ab+b^2$. Applying the cancellation laws in the group $(R,+)$ we deduce that $ab = ba$. From $a^2-b^2 = (a-b)(a+b)$ it follows that $a^2-b^2 = a^2+ab-ba-b^2$, so $0 = ab-ba$, i.e. $ab = ba$. If $ab = ba$ the other equalities result by easy computations.
b) If a and b commute, then any natural exponent powers of a and b commute. Let us prove by way of induction on n the first equality. For $n = 1$ the statement is, obviously true. Let us assume that the equality holds for n. Then

$$\begin{aligned}(a+b)^{n+1} = (a+b)^n(a+b) = (C_n^0a^n + C_n^1a^{n-1}b + \cdots + C_n^{n-1}ab^{n-1} + C_n^nb^n)a \\ + (C_n^0a^n + C_n^1a^{n-1}b + \cdots + C_n^{n-1}ab^{n-1} + C_n^nb^n)b \\ = C_n^0a^{n+1} + (C_n^1 + C_n^0)a^nb + \cdots + (C_n^{n-1} + C_n^n)ab^n + C_n^nb^{n+1}.\end{aligned}$$

Since $C_n^0 = C_n^n = 1$ and $C_n^k + C_n^{k-1} = C_{n+1}^k$ for any $n \in \mathbb{N}^*$ and $1 \leq k \leq n$, we have

$$(a+b)^{n+1} = C_{n+1}^0a^{n+1} + C_{n+1}^1a^nb + \cdots + C_{n+1}^nab^n + C_{n+1}^{n+1}b^{n+1},$$

which ends the induction step and the proof.

The other equalities result by simply computing the right side product.

3) Let $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$ and $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\}$. Show that:
i) $\mathbb{Z}[\sqrt{2}]$ is a subring of $(\mathbb{R},+,\cdot)$ which contains 1;
ii) $\mathbb{Q}(\sqrt{2})$ is a subfield of $(\mathbb{R},+,\cdot)$;
iii) $S_1 = \{a+b\sqrt[3]{2} \mid a,b \in \mathbb{Z}\}$ is not a subring of $(\mathbb{R},+,\cdot)$;
iv) $S_2 = \{a+b\sqrt[3]{2} \mid a,b \in \mathbb{Q}\}$ is not a subfield of $(\mathbb{R},+,\cdot)$.
Solution: i) Obviously, $\mathbb{Z}[\sqrt{2}] \neq \emptyset$. For any $u = a+b\sqrt{2}$, $u' = a'+b'\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ $(a,a',b,b' \in \mathbb{Z})$ we have:

$$u-u' = (a-a') + (b-b')\sqrt{2} \in \mathbb{Z}[\sqrt{2}],\ uu' = (aa'+2bb') + (ab'+a'b)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$$

and $1 = 1+0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Hence $\mathbb{Z}[\sqrt{2}]$ is a subring and $1 \in \mathbb{Z}[\sqrt{2}]$.
ii) Obviously, $|\mathbb{Q}(\sqrt{2})| \geq 2$. As in i) one shows that for any $u,u' \in \mathbb{Q}(\sqrt{2})$ one has $u-u', uu' \in \mathbb{Q}(\sqrt{2})$. Let $u = a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $u \neq 0$. This means that $a,b \in \mathbb{Q}$ and $a^2-2b^2 \neq 0$. So,

$$u^{-1} = \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Thus $\mathbb{Q}(\sqrt{2})$ is a subfield.
iii) Let $u = \sqrt[3]{2}$. Obviously, $u \in S_1$. Let us show that $u^2 \notin S_1$. Assume by contradiction that $u^2 \in S_1$. Then $u^2 = a+bu$ cu $a,b \in \mathbb{Z}$. Therefore $u^3 = au+bu^2$, and

$$2 = au + b(a+bu) = ab + (a+b^2)u.$$

But u is an irrational number, hence $ab = 2$ and $a+b^2 = 0$, system which has no solution in $\mathbb{Z}$. Thus S_1 is not closed under $\cdot$ and, consequently, S_1 is not a subring of $(\mathbb{R},+,\cdot)$.
iv) One can show as in iii) that $u = \sqrt[3]{2} \in S_2$, but $u^2 \notin S_2$.

4) Find all the automorphisms of the field $\mathbb{Q}(\sqrt{2})$.

Solution: Let us consider that $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ is an automorphism. Since nonzero field automorphisms are unitary homomorphisms, $f(1) = 1$.

If $m, n \in \mathbb{N}^*$ then $f\left(\frac{m}{n}\right) = f\left(\underbrace{\frac{1}{n} + \cdots + \frac{1}{n}}_{m \text{ terms}}\right) = mf\left(\frac{1}{n}\right)$. It follows that

$$1 = f(1) = f\left(\frac{n}{n}\right) = nf\left(\frac{1}{n}\right),$$

so $f\left(\frac{1}{n}\right) = \frac{1}{n}f(1) = \frac{1}{n}$, $f\left(\frac{m}{n}\right) = \frac{m}{n}f(1) = \frac{m}{n}$, and $f\left(-\frac{m}{n}\right) = -f\left(\frac{m}{n}\right) = -\frac{m}{n}$. Therefore, $f(x) = x$ for any $x \in \mathbb{Q}$. We also have $(\sqrt{2})^2 = 2$. Hence $[f(\sqrt{2})]^2 = 2$ which means that $f(\sqrt{2}) \in \{-\sqrt{2}, \sqrt{2}\}$. Thus $f \in \{f_1, f_2\}$, where $f_1(a + b\sqrt{2}) = a + b\sqrt{2}$ and $f_2(a + b\sqrt{2}) = a - b\sqrt{2}$. Clearly, f_1 is an automorphism, since $f_1 = 1_{\mathbb{Q}(\sqrt{2})}$. From $f_2 \circ f_2 = 1_{\mathbb{Q}(\sqrt{2})}$, one deduces that f_2 is bijective and $f_2^{-1} = f_2$. One can easily check that f_2 is a homomorphism. Thus f_2 is also an automorphism. Finally, one can say that the automorphisms of the field $\mathbb{Q}(\sqrt{2})$ are f_1 and f_2.

5) Show that the only nonzero endomorphism of the field $(\mathbb{R}, +, \cdot)$ is $1_{\mathbb{R}}$.

Solution: Let f be an endomorphism of $(\mathbb{R}, +, \cdot)$. Then $(f(1))^2 = f(1)$, so $f(1) = 1$ or $f(1) = 0$, case when f is zero. One can show as in the previous exercise that $f(x) = x$ for any $x \in \mathbb{Q}$.

Let us an arbitrary $x \in \mathbb{R}$, $x > 0$. Then $f(x) = f((\sqrt{x})^2) = (f(\sqrt{x}))^2 \geq 0$. Assuming by contradiction that $f(x) = 0$, since $x \neq 0$, we have

$$1 = f(1) = f\left(x \cdot \frac{1}{x}\right) = f(x) \cdot f\left(\frac{1}{x}\right) = 0 \cdot f\left(\frac{1}{x}\right) = 0,$$

which is absurd. Hence our assumption is wrong and

$$x \in \mathbb{R},\ x > 0 \ \Rightarrow\ f(x) > 0.$$

This leads us to the fact that f is strictly increasing (hence, also, injective). Indeed, if $x, y \in \mathbb{R}$ and $x < y$ then $f(y) - f(x) = f(y - x) > 0$, i.e. $f(x) < f(y)$.

Finally, let us show that $f(a) = a$ for any $a \in \mathbb{R} \setminus \mathbb{Q}$. Assume by contradiction that $f(a) \neq a$. Of course, this means that either $a < f(a)$ or $a > f(a)$. Let us take the first case (the second will lead us to a contradiction in the same way). It follows that there exists a rational number $b \in \mathbb{Q}$ such that $a < b \leq f(a)$. But then, since f is strictly increasing, $f(a) < f(b) = b$, which is absurd. Hence our assumption was wrong.

Thus $f(x) = x$, for any $x \in \mathbb{R}$, i.e. $f = 1_{\mathbb{R}}$.

2.5 Exercises

1) Let $x, y \in \mathbb{R}$ and $x * y = xy - 5x - 5y + 30$. Is $(\mathbb{R}, *)$ a group? What about $(\mathbb{R} \setminus \{5\}, *)$?

2) Let $(G, \cdot)$ be a group and $a, b \in G$ such that $ab = ba$. Show that

$$a^m b^n = b^n a^m,\ \forall m, n \in \mathbb{Z}.$$

3) Let $(G, \cdot)$ be a group and $f, g : G \to G$, $f(x) = x^{-1}$, $g(x) = x^2$. Show that:

i) f is bijective;

ii) f is an automorphism if and only if $(G, \cdot)$ is Abelian;
iii) g is a homomorphism if and only if $(G, \cdot)$ is Abelian.
4) Show that $H \subseteq \mathbb{Z}$ is a subgroup of $(\mathbb{Z}, +)$ if and only if there exists a unique $n \in \mathbb{N}$ such that $H = n\mathbb{Z}$.
5) Let $n \in \mathbb{N},\ n \geq 2$. Show that there exists only one group homomorphism from $(\mathbb{Z}_n, +)$ into $(\mathbb{Z}, +)$.
6) Show that if $f : \mathbb{Q} \to \mathbb{Q}$ is an endomorphism of $(\mathbb{Q}, +)$ then

$$f(x) = f(1) \cdot x,\ \forall x \in \mathbb{Q},$$

i.e. f is a translation of $(\mathbb{Q}, \cdot)$. Show that any translation of $(\mathbb{Q}, \cdot)$ is an endomorphism of $(\mathbb{Q}, +)$. Determine the automorphisms of $(\mathbb{Q}, +)$.
7) Let $a \in \mathbb{Z}$. Show that $\widehat{a} \in \mathbb{Z}_n$ is a unit of the ring $\mathbb{Z}_n$ if and only if $(a, n) = 1$. Using this equivalence, prove that $(\mathbb{Z}_n, +, \cdot)$ is a field if and only if n is a prime number.
8) a) Solve the equations

$$\widehat{4}x + \widehat{5} = \widehat{9} \text{ and } \widehat{5}x + \widehat{5} = \widehat{9}$$

in $\mathbb{Z}_{12}$, and the equation $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} X = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ in $M_2(\mathbb{C})$.
b) Find all the solutions of the system $\begin{cases} \widehat{3}x + \widehat{4}y = \widehat{11} \\ \widehat{4}x + \widehat{9}y = \widehat{10} \end{cases}$ in $\mathbb{Z}_{12}$.
9) A number $d \in \mathbb{Z}$ is a **square-free integer** if $d \neq 1$ and the only square number which divides d is 1. Let d be a square-free integer. Show that:
i) $\sqrt{d} \notin \mathbb{Q}$;
ii) $a, b \in \mathbb{Q},\ a + b\sqrt{d} = 0 \ \Rightarrow\ a = b = 0$;
iii) $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ is a subring of $(\mathbb{C}, +, \cdot)$ which contains 1;
iv) $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is a subfield of $(\mathbb{R}, +, \cdot)$.
10) Show that the only nonzero field homomorphism from $(\mathbb{Q}, +, \cdot)$ into $(\mathbb{C}, +, \cdot)$ is the inclusion homomorphism $i : \mathbb{Q} \to \mathbb{C},\ i(x) = x$.

3 Vector spaces

3.1 Vector spaces, subspaces, linear maps

Let $(K, +, \cdot)$ be a field. Throughout this chapter this condition on K will always be valid.

Definition 3.1. A **vector space over** K (or a K**-vector space**) is an abelian group $(V, +)$ together with an external operation

$$\cdot : K \times V \to V\,, \quad (k, v) \mapsto k \cdot v\,,$$

satisfying the following axioms:
(L_1) $k \cdot (v_1 + v_2) = k \cdot v_1 + k \cdot v_2$;
(L_2) $(k_1 + k_2) \cdot v = k_1 \cdot v + k_2 \cdot v$;
(L_3) $(k_1 \cdot k_2) \cdot v = k_1 \cdot (k_2 \cdot v)$;
(L_4) $1 \cdot v = v$,
for any $k, k_1, k_2 \in K$ and any $v, v_1, v_2 \in V$.

In this context, the elements of K are called **scalars**, the elements of V are called **vectors** and the external operation is called **scalar multiplication**. Sometimes a vector space is also called **linear space**.

We denote the fact that V is a vector space over K either by ${}_KV$ or by $(V, K, +, \cdot)$, since for a given field K, the addition on V and the external operation are the operations that determine the vector space structure of V.

Remark 3.2. Notice that in the definition of a vector space appear four operations, two denoted by the same symbol $+$ and two denoted by the same symbol $\cdot$. Of course, they are not the same, but we to denote them identically for the sake of simplicity of writing. The nature of the elements involved when using these symbols tells us which is the operation. More precisely, if $+$ appears between two vectors, then it is the addition from V, if it appears between two scalars, it is the addition from K; if $\cdot$ appears between a scalar and a vector, then it is the scalar multiplication, otherwise, it appears between to scalars, hence it is the multiplication from K.

Examples 3.3. (a) Let V_2 be the set of all vectors (in the classical sense) in the plane with a fixed origin O. Then V_2 is a vector space over $\mathbb{R}$ (or a *real vector space*), where the addition is the usual addition of two vectors by the parallelogram rule and the external operation is the usual scalar multiplication of vectors by real scalars.

If we consider two coordinate axes Ox and Oy in the plane, each vector in V_2 is perfectly determined by the coordinates of its ending point. Therefore, the addition of vectors and the scalar multiplication of vectors by real numbers become:

$$(x, y) + (x', y') = (x + x', y + y'),$$

$$k \cdot (x, y) = (k \cdot x, k \cdot y),$$

for any $k \in \mathbb{R}$ and any $(x, y), (x', y') \in \mathbb{R} \times \mathbb{R}$. Thus, $(\mathbb{R}^2, \mathbb{R}, +, \cdot)$ is a vector space.

Similarly, one can consider the real vector space V_3 of all vectors in the space with a fixed origin. Moreover, a further generalization is possible, as we may see in the following example.

(b) Let $n \in \mathbb{N}^*$. Define

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n),$$

$$k \cdot (x_1, \dots, x_n) = (kx_1, \dots, kx_n),$$

for any $(x_1, \dots, x_n), (y_1, \dots, y_n) \in K^n$ and for any $k \in K$. Then $(K^n, K, +, \cdot)$ is a vector space, called the **canonical vector space**.

For $n = 1$, we get that ${}_KK$ is a vector space. Hence, as far as the classical numerical fields are concerned, ${}_\mathbb{Q}\mathbb{Q}$, ${}_\mathbb{R}\mathbb{R}$ and ${}_\mathbb{C}\mathbb{C}$ are vector spaces.

(c) If $V = \{0\}$ is a single element set, then we know that there is a unique structure of an abelian group for V, namely that one defined by $0 + 0 = 0$. Then we can define a unique scalar multiplication, namely $k \cdot 0 = 0$, for any $k \in K$. Thus, V is a vector space, called the **zero (null) vector space** and denoted by $\{0\}$.

(d) Let A be a subfield of the field K. Then K is a vector space over A, where the addition and the scalar multiplication are just the addition and the multiplication of elements in the field K. In particular, ${}_\mathbb{Q}\mathbb{R}$, ${}_\mathbb{Q}\mathbb{C}$ and ${}_\mathbb{R}\mathbb{C}$ are vector spaces.

(e) $(K[X], K, +, \cdot)$ is a vector space, where the addition is the usual addition of polynomials and the scalar multiplication is defined as follows: if $f = a_0 + a_1X + \cdots + a_nX^n \in K[X]$,

$$kf = (ka_0) + (ka_1)X + \cdots + (ka_n)X^n,\ forallk \in K\,.$$

(f) Let $m, n \in \mathbb{N}$, $m, n \geq 2$. Then $(M_{mn}(K), K, +, \cdot)$ is a vector space, where the operations are the usual addition and scalar multiplication of matrices.
(g) Let A be a non-empty set. Denote

$$K^A = \{f \mid f : A \to K\}\,.$$

Then $(K^A, K, +, \cdot)$ is a vector space, where the addition and the scalar multiplication are defined as follows: for any $f, g \in K^A$, for any $k \in K$, we have $f + g \in K^A$, $kf \in K^A$, where

$$(f + g)(x) = f(x) + g(x)\,,\ (kf)(x) = kf(x)\,, \forall x \in A\,.$$

As a particular case, we obtain the vector space $(\mathbb{R}^{\mathbb{R}}, \mathbb{R}, +, \cdot)$ of real functions of a real variable.
(h) Let K be a field. The group $(M_{m,n}(K), +)$ of the $m \times n$ matrices over K is a K-vector space with the scalar multiplication

$$\alpha(a_{ij}) = (\alpha a_{ij})\ (\alpha \in K,\ (a_{ij}) \in M_{m,n}(K)).$$

Let us notice that for $n \times n$ square matrices, besides the K-vector space structure, $M_n(K)$ also has a ring structure (see Example 2.38 d)). Moreover, there is a certain compatibility between the scalar multiplication and the matrix multiplication

$$\alpha(A\,B) = (\alpha A)B = A(\alpha B),\ \forall \alpha \in K,\ \forall A, B \in M_n(K).$$

(i) If V_1 and V_2 are K-vector spaces, the Cartesian product $V_1 \times V_2$ is a K- vector space with the operations defined by

$$(x_1, x_2) + (x_1', x_2') = (x_1 + x_1', x_2 + x_2'),\ \alpha(x_1, x_2) = (\alpha x_1, \alpha x_2)$$

for any $(x_1, x_2), (x_1', x_2') \in V_1 \times V_2$ and $\alpha \in K$. This vector space is called the **direct product** of ${}_KV_1$ and ${}_KV_2$.

Next we give some computation rules in a vector space. Notice that we denote by 0 both the zero scalar and the zero vector.

Theorem 3.4. Let V be a vector space over K. Then for any $k, k', k_1, \ldots, k_n \in K$ and for any $v, v', v_1, \ldots, v_n \in V$ we have:
(i) $k \cdot 0 = 0 \cdot v = 0$;
(ii) $k(-v) = (-k)v = -kv$;
(iii) $k(v - v') = kv - kv'$;
(iv) $(k - k')v = kv - k'v$;
(v) $(k_1 + \cdots + k_n)v = k_1v + \cdots + k_nv$;
(vi) $k(v_1 + \cdots + v_n) = kv_1 + \cdots + kv_n$.

Proof. (i) Since

$$k \cdot 0 + k \cdot v = k(0 + v) = kv\,,$$

we get $k \cdot 0 = 0$. Since

$$0 \cdot v + k \cdot v = (0 + k)v = kv\,,$$

we get $0 \cdot v = 0$.
(ii) We have

$$kv + k(-v) = k(v - v) = k \cdot 0 = 0\,,$$

whence $k(-v) = -kv$. Also,

$$kv + (-k)v = (k - k)v = 0 \cdot v = 0\,,$$

whence $(-k)v = -kv$.
(iii) By computing

$$k(v - v') + kv' = k(v - v' + v') = kv\,,$$

we obtain $k(v - v') = kv - kv'$.
(iv) By computing

$$(k - k')v + k'v = (k - k' + k')v = kv\,,$$

we obtain $(k - k')v = kv - k'v$.
(v) and (vi) can be proved by way of induction on n. □

Theorem 3.5. Let V be a vector space over K and let $k \in K$ and $v \in V$. Then

$$kv = 0 \Leftrightarrow k = 0 \text{ or } v = 0\,.$$

Proof. $\Rightarrow$ Assume $kv = 0$. Suppose that $k \neq 0$. Then k is invertible in the field K and we have

$$kv = 0 \Rightarrow k \cdot v = k \cdot 0 \Rightarrow v = 0\,.$$

$\Leftarrow$ This is Theorem 3.4 (i). □

Definition 3.6. Let V be a vector space over K and let $S \subseteq V$. Then S is a **subspace** of V if:
(1) S is closed with respect to the addition of V and to the scalar multiplication, that is,

$$\forall x, y \in S\,, \quad x + y \in S\,,$$

$$\forall k \in K\,,\ \forall x \in S\,,\ kx \in S\,.$$

(2) S is a vector space over K with respect to the induced operations of addition and scalar multiplication.

We denote by $S \leq_K V$ the fact that S is a subspace of the vector space V over K.

Remarks 3.7. 1) Actually, the second condition in the definition is almost superfluous. If $S \neq \emptyset$, then by the stability of S in V with respect to the addition and the scalar multiplication, it follows immediately that S is a vector space with respect to the induced operations. Of course, the second condition implies the fact that $S \neq \emptyset$ since ${}_KS$ is build on the abelian group $(S, +)$ determined by the induced addition.
2) The previous remark shows that $S \leq_K V$ if and only if $S \leq (V, +)$ and $kx \in S$ for any $x \in S$ and any $k \in K$.

Hence we have the following **characterization theorem for subspaces**.

Theorem 3.8. Let V be a vector space over K and let $S \subseteq V$. The following conditions are equivalent:
1) $S \leq_K V$.
2) The following conditions hold for S:
α) $S \neq \emptyset$;
β) $\forall x, y \in S\,,\ x + y \in S$;
γ) $\forall k \in K\,,\ \forall x \in S\,,\ kx \in S\,.$
3) The following conditions hold for S:
α) $S \neq \emptyset$;
δ) $\forall k_1, k_2 \in K\,,\ \forall x, y \in S\,,\ k_1x + k_2y \in S\,.$

Proof. 1) $\Leftrightarrow$ 2) is a straightforward corollary of the Remark 3.7 1).
3) $\Rightarrow$ 2) Taking $k_1 = k_2 = 1$ and $k_2 = 0$ and applying δ), we get β) and γ), respectively.
2) $\Rightarrow$ 3) Let $k_1, k_2 \in K$ and $x, y \in S$. We apply γ) to get $k_1x, k_2y \in S$ and then β to get $k_1x + k_2y \in S$. □

Remark 3.9. (1) Notice that Remark 3.7 2) allows us to replace α) in the previous theorem with $0 \in S$.
(2) If $S \leq_K V$, $k_1, \dots, k_n \in K$ and $x_1, \dots, x_n \in S$ then $k_1x_1 + \dots + k_nx_n \in S$.

Examples 3.10. (a) Every non-zero vector space V over K has two subspaces, namely $\{0\}$ and V. They are called the **trivial subspaces**. If a vector space has only trivial subspaces, it is called a **simple vector space**.
(b) Let

$$S = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}\,,$$
$$T = \{(x, y, z) \in \mathbb{R}^3 \mid x = y = z\}\,.$$

Then S and T are subspaces of the real vector space $\mathbb{R}^3$. More generally, the subspaces of $\mathbb{R}^3$ are the trivial subspaces, the lines containing the origin and the planes containing the origin.
(c) Let $n \in \mathbb{N}$ and let

$$K_n[X] = \{f \in K[X] \mid \deg f \leq n\}\,.$$

Then $K_n[X]$ is a subspace of the polynomial vector space $K[X]$ over K.
d) Let $I \subseteq \mathbb{R}$ be an interval. The set $\mathbb{R}^I = \{f \mid f : I \to \mathbb{R}\}$ is a $\mathbb{R}$-vector space with respect to the following operations

$$(f + g)(x) = f(x) + g(x),\ (\alpha f)(x) = \alpha f(x)$$

with $f, g \in \mathbb{R}^I$ and $\alpha \in \mathbb{R}$. The subsets

$$C(I, \mathbb{R}) = \{f \in \mathbb{R}^I \mid f \text{ continuous on } I\},\ D(I, \mathbb{R}) = \{f \in \mathbb{R}^I \mid f \text{ derivable on } I\}$$

are subspaces of $\mathbb{R}^I$ since they are nonempty and

$$\alpha, \beta \in \mathbb{R},\ f, g \in C(I, \mathbb{R}) \Rightarrow \alpha f + \beta g \in C(I, \mathbb{R});$$

$$\alpha, \beta \in \mathbb{R},\ f, g \in D(I, \mathbb{R}) \Rightarrow \alpha f + \beta g \in D(I, \mathbb{R}).$$

Theorem 3.11. Let I be a nonempty set, V be a vector space over K and let $(S_i)_{i\in I}$ be a family of subspaces of V. Then $\bigcap_{i\in I} S_i \leq_K V$.

Proof. For each $i \in I$, $S_i \leq_K V$, hence $0 \in S_i$. Then $0 \in \bigcap_{i\in I} S_i \neq \emptyset$. Now let $k_1, k_2 \in K$ and $x, y \in \bigcap_{i\in I} S_i$. Then $x, y \in S_i$, $\forall i \in I$. But $S_i \leq_K V$, for any $i \in I$. It follows that $k_1x + k_2y \in S_i$, for any $i \in I$, hence $k_1x + k_2y \in \bigcap_{i\in I} S_i$. Now by Theorem 3.8, we have $\bigcap_{i\in I} S_i \leq_K V$. □

Remark 3.12. In general, the union of two subspaces is not a subspace.

Indeed, $S = \{(a, 0) \mid a \in \mathbb{R}\}$ and $T = \{(0, b) \mid b \in \mathbb{R}\}$ are subspaces of ${}_{\mathbb{R}}\mathbb{R}^2$, but $S \cup T$ is not a subspace of ${}_{\mathbb{R}}\mathbb{R}^2$, since $(1, 0) \in S \subseteq S \cup T$, $(0, 1) \in T \subseteq S \cup T$ and $(1, 0) + (0, 1) = (1, 1) \notin S \cup T$.

At this point, as we did for the previous algebraic structures, we are interested how to complete a given subset of a vector space to a subspace in a minimal way. This is the motivation for the following definition.

Definition 3.13. Let V be a vector space and let $X \subseteq V$. Then we denote

$$\langle X\rangle = \bigcap\{S \leq_K V \mid X \subseteq S\}$$

and we call it the **subspace generated by** X or the **subspace spanned by** X. Here X is called the **generating set** of $\langle X\rangle$.

If $X = \{x_1, \dots, x_n\}$, we denote $\langle x_1, \dots, x_n\rangle = \langle\{x_1, \dots, x_n\}\rangle$.

Remarks 3.14. (1) Actually, $\langle X\rangle$ is the smallest subspace of V (with respect to $\subseteq$) which contains X.
(2) Notice that $\langle\emptyset\rangle = \{0\}$.
(3) If V is a K-vector space, then:
(i) If $S \leq_K V$ then $\langle S\rangle = S$.
(ii) If $X \subseteq V$ then $\langle\langle X\rangle\rangle \subseteq \langle X\rangle$.
(iii) If $X \subseteq Y \subseteq V$ then $\langle X\rangle \subseteq \langle Y\rangle$.

Definition 3.15. A vector space V over K is called **finitely generated** if there exist $n \in \mathbb{N}$ and $x_1, \dots, x_n \in V$ such that $V = \langle x_1, \dots, x_n\rangle$. Then we call the set $\{x_1, \dots, x_n\}$ a **system of generators** for V.

Definition 3.16. Let V be a K-vector space. A finite sum of the form

$$k_1x_1 + \cdots + k_nx_n\,,$$

with $k_1, \dots, k_n \in K$ and $x_1, \dots, x_n \in V$, is called a **linear combination** of the vectors $x_1, \dots, x_n$.

Let us show how the elements of a generated subspace look like.

Theorem 3.17. Let V be a vector space over K and let $\emptyset \neq X \subseteq V$. Then

$$\langle X\rangle = \{k_1x_1 + \cdots + k_nx_n \mid k_i \in K\,,\ x_i \in X\,, i = 1, \dots, n\,,\ n \in \mathbb{N}^*\}\,,$$

that is, the set of all finite linear combinations of vectors of V.

Proof. We prove the result in 3 steps, by showing that

$$L = \{k_1x_1 + \cdots + k_nx_n \mid k_i \in K\,,\ x_i \in X\,, i = 1, \dots, n\,,\ n \in \mathbb{N}^*\}$$

is a subspace of V, L contains X and it is the smallest subspace which has this property.
(i) We choose $n = 1$ and $k_1 = 1$ to show that $X \subseteq L$.
(ii) $L \neq \emptyset$ since $X \subseteq L$ and $X \neq \emptyset$. Now let $k, k' \in K$ and $v, v' \in L$. Then $v = \sum_{i=1}^{n} k_ix_i$ and $v' = \sum_{j=1}^{m} k'_jx'_j$ for some $k_1, \dots, k_n, k'_1, \dots, k'_m \in K$ and $x_1, \dots, x_n, x'_1, \dots, x'_m \in X$. Hence

$$kv + k'v' = k\sum_{i=1}^{n} k_ix_i + k'\sum_{j=1}^{m} k'_jx'_j = \sum_{i=1}^{n}(kk_i)x_i + \sum_{j=1}^{m}(k'k'_j)x'_j \in L\,,$$

since it is a finite linear combination of vectors of X. Now by Theorem 3.8, we have $L \leq_K V$.
(iii) Let us suppose that $S \leq_K V$ and $X \subseteq S$. Let $k_1, \dots, k_n \in K$ and $x_1, \dots, x_n \in X$. Since $X \subseteq S$ and $S \leq_K V$, it follows by Theorem 3.8 that $k_1x_1 + \cdots + k_nx_n \in S$. Hence $L \subseteq S$.

Thus, by Remark 3.14 (1), we have $\langle X \rangle = L$. □

Corollary 3.18. Let V be a vector space over K and $x_1, \dots, x_n \in V$. Then

$$\langle x_1, \dots, x_n \rangle = \{k_1x_1 + \cdots + k_nx_n \mid k_i \in K\,,\ x_i \in X\,, i = 1, \dots, n\}\,.$$

Remark 3.19. Notice that a linear combination of linear combinations is again a linear combination.

Examples 3.20. Consider the canonical real vector space $\mathbb{R}^3$ (see Example 3.3). Then

$$\langle (1,0,0), (0,1,0), (0,0,1) \rangle = \{k_1(1,0,0) + k_2(0,1,0) + k_3(0,0,1) \mid k_1, k_2, k_3 \in \mathbb{R}\} =$$

$$= \{(k_1,0,0) + (0,k_2,0) + (0,0,k_3) \mid k_1, k_2, k_3 \in \mathbb{R}\} = \{(k_1,k_2,k_3) \mid k_1, k_2, k_3 \in \mathbb{R}\} = \mathbb{R}^3\,.$$

Hence $\mathbb{R}^3$ is generated by the three vectors $(1,0,0), (0,1,0), (0,0,1)$.

If $S, T \leq_K V$, the smallest subspace of V which contains the union $S \cup T$ is $\langle S \cup T \rangle$. We will show that this subspace is the sum of the given subspaces.

Definition 3.21. Let V be a vector space over K and let $S, T \leq_K V$. Then we define the **sum** of the subspaces S and T as the set

$$S + T = \{s + t \mid s \in S\,,\ t \in T\}\,.$$

If $S \cap T = \{0\}$, then $S + T$ is denoted by $S \oplus T$ and is called the **direct sum** of the subspaces S and T.

Examples 3.22. Consider the canonical real vector space $\mathbb{R}^2$. Then $\mathbb{R}^2 = S \oplus T$, where $S = \{(x,0) \mid x \in \mathbb{R}\}$ and $T = \{(0,y) \mid y \in \mathbb{R}\}$.

Theorem 3.23. Let V be a vector space over K and let $S, T \leq_K V$. Then

$$S + T = \langle S \cup T \rangle\,.$$

Proof. First, let $v = s + t \in S + T$, for some $s \in S$ and $t \in T$. Then $v = 1 \cdot s + 1 \cdot t$ is a linear combination of vectors $s, t \in S \cup T$, hence $v \in \langle S \cup T \rangle$. Thus,

$$S + T \subseteq \langle S \cup T \rangle .$$

Now let $v \in \langle S \cup T \rangle$. Then

$$v = \sum_{i=1}^{n} k_i v_i = \sum_{i \in I} k_i v_i + \sum_{j \in J} k_j v_j \, ,$$

where $I = \{i \in \{1, \dots, n\} \mid v_i \in S\}$ and $J = \{j \in \{1, \dots, n\} \mid v_j \in T \setminus S\}$. But the first sum is a linear combination of vectors of S, hence it belongs to S, whereas the second sum is a linear combination of vectors of T, hence it belongs to T. So $v \in S + T$ and consequently

$$\langle S \cup T \rangle \subseteq S + T.$$

Thus, $S + T = \langle S \cup T \rangle$. □

Remarks 3.24. (1) One can also prove the previous theorem by showing that $S+T \leq_K V$, $S \cup T \subseteq S + T$, and $S + T$ is the smallest subspace of V which has this property. Actually, a more general result can be proved: if $S_1, \dots, S_n$ are subspaces of a K-vector space V then $S_1 + \dots + S_n = \langle S_1 \cup \dots \cup S_n \rangle$.
(2) Moreover, if $X_i \subseteq V$ $(i = 1, \dots, n)$, then $\langle X_1 \cup \dots \cup X_n \rangle = \langle X_1 \rangle + \dots + \langle X_n \rangle$.

Indeed, $X_i \subseteq X_1 \cup \dots \cup X_n$ implies $\langle X_i \rangle \subseteq \langle X_1 \cup \dots \cup X_n \rangle$ $(i = 1, \dots, n)$ and we have $\langle X_1 \cup \dots \cup X_n \rangle \supseteq \langle X_1 \rangle + \dots + \langle X_n \rangle$. Since $X_i \subseteq \langle X_i \rangle \subseteq \langle X_1 \rangle + \dots + \langle X_n \rangle$ $(i = 1, \dots, n)$, we have $X_1 \cup \dots \cup X_n \subseteq \langle X_1 \rangle + \dots + \langle X_n \rangle$, hence

$$\langle X_1 \cup \dots \cup X_n \rangle \subseteq \langle \langle X_1 \rangle + \dots + \langle X_n \rangle \rangle = \langle X_1 \rangle + \dots + \langle X_n \rangle .$$

Definition 3.25. Let V and V' be vector spaces over K. The map $f : V \to V'$ is called a **(vector space) homomorphism** or a **linear map** (or a **linear transformation**) if

$$f(x + y) = f(x) + f(y) \, , \; \forall x, y \in V \, ,$$

$$f(kx) = kf(x), \;\; \forall k \in K, \; \forall x \in V \, .$$

The notions of **(vector space) isomorphism**, **endomorphism** and **automorphism** are defined as usual.

We will mainly use the name *linear map* or, more precisely, *K-linear map.*

Remarks 3.26. (1) Notice that, when defining a linear map, we consider vector spaces over the same field K.
(2) If $f : V \to V'$ is a K-linear map, then the first condition from its definition tells us that f is a group homomorphism between $(V, +)$ and $(V', +)$. Then we have $f(0) = 0'$ and $f(-x) = -f(x)$, for any $x \in V$ (see Theorem 2.25).

We denote by $V \simeq V'$ the fact that two vector spaces V and V' are isomorphic and

$$Hom_K(V, V') = \{f : V \to V' \mid f \text{ is a } K\text{-linear map}\} \, ,$$

$$End_K(V) = \{f : V \to V \mid f \text{ is a } K\text{-linear map}\} \, .$$

Theorem 3.27. Let V and V' be vector spaces over K and $f : V \to V'$. Then f is a linear map if and only if

$$f(k_1v_1 + k_2v_2) = k_1f(v_1) + k_2f(v_2)\,,\ \forall k_1, k_2 \in K,\ \forall v_1, v_2 \in V.$$

Proof. Let $k_1, k_2 \in K$ and $v_1, v_2 \in V$. Then

$$f(k_1v_1 + k_2v_2) = f(k_1v_1) + f(k_2v_2) = k_1f(v_1) + k_2f(v_2)\,.$$

Conversely, if we choose $k_1 = k_2 = 1$ and then $k_2 = 0$, we get the two conditions from the definition of a linear map. □

One can easily prove by way of induction the following:

Corollary 3.28. If $f : V \to V'$ is a linear map, then

$$f(k_1v_1 + \cdots + k_nv_n) = k_1f(v_1) + \cdots + k_nf(v_n),\ \forall v_1, \ldots, v_n \in V, \forall k_1, \ldots, k_n \in K.$$

Examples 3.29. (a) Let V and V' be K-vector spaces and let $f : V \to V'$ be defined by $f(x) = 0'$, for any $x \in V$. Then f is a K-linear map, called the **trivial linear map**.
(b) Let V be a vector space over K. Then the identity map $1_V : V \to V$ is an automorphism of V.
(c) Let V be a vector space and $S \leq_K V$. Define $i : S \to V$ by $i(x) = x$, for any $x \in S$. Then i is a K-linear map, called the **inclusion linear map**.
(d) Let us consider $\varphi \in \mathbb{R}$. The map

$$f : \mathbb{R}^2 \to \mathbb{R}^2,\ f(x, y) = (x\cos\varphi - y\sin\varphi, x\sin\varphi + y\cos\varphi),$$

i.e. the plane rotation with the rotation angle φ, is a linear map.
(e) If $a, b \in \mathbb{R}$, $a < b$, $I = [a, b]$, and $C(I, \mathbb{R}) = \{f : I \to \mathbb{R} \mid f \text{ continuous on } I\}$, then

$$F : C(I, \mathbb{R}) \to \mathbb{R},\ F(f) = \int_a^b f(x)dx$$

is a linear map.

As in the case of group homomorphisms, we have the following:

Theorem 3.30. (i) Let $f : V \to V'$ and $g : V' \to V''$ be K-linear maps (isomorphisms). Then $g \circ f : V \to V''$ is a K-linear map (isomorphism).
(ii) Let $f : V \to V'$ be an isomorphism of vector spaces over K. Then $f^{-1} : V' \to V$ is again an isomorphism of vector spaces over K.

Proof. (i) If $v_1, v_2 \in V$ and $k_1, k_2 \in K$, then

$$(g \circ f)(k_1v_1 + k_2v_2) = g(f(k_1v_1 + k_2v_2)) = g(k_1f(v_1) + k_2f(v_2)) =$$

$$= k_1g(f(v_1)) + k_2g(f(v_2)) = k_1(g \circ f)(v_1) + k_2(g \circ f)(v_2)$$

hence $g \circ f$ is a liniar map.
(ii) We have to check that

$$f^{-1}(k_1v_1' + k_2v_2') = k_1f^{-1}(v_1') + k_2f^{-1}(v_2'),\ \forall\ v_1', v_2' \in V',\ \forall k_1, k_2 \in K.$$

If we denote $f^{-1}(v_i') = v_i,\ i = 1,2$ then $f(v_1) = v_1',\ f(v_2) = v_2'$, hence

$$k_1 v_1' + k_2 v_2' = k_1 f(v_1) + k_2 f(v_2) = f(k_1 v_1 + k_2 v_2).$$

Thus,

$$f^{-1}(k_1 v_1' + k_2 v_2') = k_1 v_1 + k_2 v_2 = k_1 f^{-1}(v_1') + k_2 f^{-1}(v_2'),$$

which completes the proof. □

Definition 3.31. Let $f : V \to V'$ be a K-linear map. Then the set

$$\text{Ker} f = \{x \in V \mid f(x) = 0'\}$$

is called the **kernel** of the K-linear map f and the set

$$\text{Im} f = \{f(x) \mid x \in V\}$$

is called the **image** of the K-linear map f.

Theorem 3.32. Let $f : V \to V'$ be a K-linear map. Then we have

1) $\text{Ker} f \leq_K V$ and $\text{Im} f \leq_K V'$.

2) f is invective if and only if $\text{Ker} f = \{0\}$.

Proof. 1) Since $f(0) = 0'$, we have $0 \in \text{Ker}\, f$ and $0' \in \text{Im} f$. If $x_1, x_2 \in \text{Ker}\, f$ and $k_1, k_2 \in K$ then

$$f(k_1 x_1 + k_2 x_2) = k_1 f(x_1) + k_2 f(x_2) = k_1 0' + k_2 0' = 0'$$

hence $k_1 x_1 + k_2 x_2 \in \text{Ker}\, f$. Thus $\text{Ker}\, f \leq_K V$.

If $x_1', x_2' \in \text{Im}\, f$ and $k_1, k_2 \in K$ then there exist $x_1, x_2 \in V$ such that $f(x_1) = x_1'$ and $f(x_2) = x_2'$. Therefore

$$f(k_1 x_1' + k_2 x_2') = k_1 f(x_1) + k_2 f(x_2) = f(k_1 x_1 + k_2 x_2) \in \text{Im} f\,.$$

Thus $\text{Im}\, f \leq_K V$.

2) Since

$$f(x_1) = f(x_2) \Leftrightarrow f(x_1 - x_2) = 0 \Leftrightarrow x_1 - x_2 \in \text{Ker}\, f$$

and

$$x_1 = x_2 \Leftrightarrow x_1 - x_2 = 0$$

the implication

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2$$

holds if and only if $\text{Ker}\, f = \{0\}$. □

Theorem 3.33. Let $f : V \to V'$ be a K-linear map and let $X \subseteq V$. Then

$$f(\langle X \rangle) = \langle f(X) \rangle\,.$$

Proof. Let us assume $X \neq \emptyset$. By Theorem 3.17 we have

$$\langle X \rangle = \{k_1x_1 + \cdots + k_nx_n \mid k_i \in K\,,\ x_i \in X\,, i = 1, \ldots, n\,,\ n \in \mathbb{N}^*\}\,,$$

Since f is a K-linear map, it follows by Theorem 3.27 that

$$f(\langle X \rangle) = \{f(k_1x_1 + \cdots + k_nx_n) \mid k_i \in K\,,\ x_i \in X\,, i = 1, \ldots, n\,,\ n \in \mathbb{N}^*\} =$$

$$= \{k_1f(x_1) + \cdots + k_nf(x_n) \mid k_i \in K\,,\ x_i \in X\,, i = 1, \ldots, n\,,\ n \in \mathbb{N}^*\} = \langle f(X) \rangle\,.$$

If $X = \emptyset$, the conclusion trivially holds. □

Theorem 3.34. Let V and V' be vector spaces over K. For any $f, g \in Hom_K(V, V')$ and for any $k \in K$, we consider $f + g, k \cdot f \in Hom_K(V, V')$,

$$(f + g)(x) = f(x) + g(x),\ \forall x \in V\,,$$

$$(kf)(x) = kf(x),\ \forall x \in V\,.$$

The above equalities define an addition and a sclar multiplication on $Hom_K(V, V')$ and $Hom_K(V, V')$ is a vector space over K.

Proof. Let $k \in K$ and $f, g \in Hom_K(V, V')$.

Let us prove first that $f + g, kf \in Hom_K(V, V')$. Let $k_1, k_2 \in K$. Then:

$$(f+g)(k_1x+k_2y) = f(k_1x+k_2y)+g(k_1x+k_2y) = k_1f(x)+k_2f(y)+k_1g(x)+k_2g(y) =$$

$$= k_1(f(x) + g(x)) + k_2(f(y) + g(y)) = k_1(f + g)(x) + k_2(f + g)(y)\,.$$

We also have:

$$(kf)(k_1x + k_2y) = kf(k_1x + k_2y) = k(k_1f(x)) + k(k_2f(y)) = (kk_1)f(x) + (kk_2)f(y) =$$

$$= k_1(kf(x)) + k_2(kf(y))\,.$$

Therefore, $f + g, kf \in Hom_K(V, V')$.

It is easy to check that $(Hom_K(V, V'), +)$ is an abelian group, where the identity element is the trivial linear map $\theta : V \to V'$ defined by $\theta(x) = 0'$, for any $x \in V$ and any element $f \in Hom_K(V, V')$ has a symmetric $-f \in Hom_K(V, V')$ defined by $(-f)(x) = -f(x)$, $\forall x \in V$.

Checking the axioms of the vector space for $Hom_K(V, V')$ reduces by the definitions of operations to the axioms for the vector space ${}_KV'$. □

Corollary 3.35. If V is a K-vector space, then $End_K(V)$ is a vector space over K.

Remarks 3.36. a) Let V be a K-vector space and let $End(V, +)$ be the set of the endomorphisms of its additive group $(V, +)$. From Theorem 3.30 one deduces that $End_K(V)$ is a subgroupoid of $(End(V, +), \circ)$ and from Example 3.29 (b) it follows that $(End_K(V), \circ)$ is a monoid. Moreover, the endomorphism composition $\circ$ is distributive with respect to endomorphism addition $+$, thus $End_K(V)$ also has a unitary ring structure, $(End_K(V), +, \circ)$.

b) The set $Aut_K(V)$ is a subgroup of the automorphism group $(Aut(V, +), \circ)$ of $(V, +)$.

3.2 Exercises with solution

1) Can one organize a finite set as a vector space over an infinite field?

Solution: Let V be a finite set and K be an infinite field. If V has only one element, there exists (a unique) K-vector space structure on V, the zero vector space.

If $|V| \geq 2$, assuming by contradiction that there exists a K-vector space structure on V and taking $x \neq 0$, one deduces that $t'_x : K \to V$, $t'_x(\alpha) = \alpha x$ is an injective map since

$$\alpha_1, \alpha_2 \in K,\ t'_x(\alpha_1) = t'_x(\alpha_2) \Rightarrow \alpha_1 x = \alpha_2 x \Rightarrow (\alpha_1 - \alpha_2)x = 0 \overset{x \neq 0}{\Rightarrow} \alpha_1 - \alpha_2 = 0 \Rightarrow \alpha_1 = \alpha_2.$$

Hence $|K| \leq |V|$, which is absurd. Thus there is no K-vector space structure on V in this case.

2) Let V be a K-vector space, $S \leq_K V$ and $x, y \in V$. We denote $\langle S, x\rangle = \langle S \cup \{x\}\rangle$. Show that if $x \in V \setminus S$ and $x \in \langle S, y\rangle$ then $y \in \langle S, x\rangle$.

Solution: From $x \in \langle S, y\rangle$ it results that there exist $s_1, \dots, s_n \in S$ and $\alpha_1, \dots, \alpha_n, \alpha \in K$ such that

$$x = \alpha_1 s_1 + \dots + \alpha_n s_n + \alpha y.$$

Assuming by contradiction that $\alpha = 0$ would imply $x = \alpha_1 s_1 + \dots + \alpha_n s_n \in S$ which contradicts our hypothesis. So, $\alpha \neq 0$ is a unit in K and

$$y = -\alpha^{-1}\alpha_1 s_1 - \dots - \alpha^{-1}\alpha_n s_n + \alpha^{-1} x \in \langle S, x\rangle.$$

3) If V is a K-vector space, $V_1, V_2 \leq_K V$ and $V = V_1 \oplus V_2$, we say that V_i $(i = 1, 2)$ is a **direct summand** of V. Show that the property of a subspace of being a direct summand is transitive.

Solution: Let V_1, V_2, V_3, V_4 be subspaces of K-vector space V such that $V = V_1 \oplus V_2$ and $V_1 = V_3 \oplus V_4$. Then $V = V_1 + V_2 = V_3 + V_4 + V_2$. Moreover, if $v_3 \in V_3 \cap (V_4 + V_2)$, there exists $v_4 \in V_4$, $v_2 \in V_2$ such that $v_3 = v_4 + v_2$. Hence $v_2 = v_3 - v_4 \in V_3 + V_4 = V_1$, which implies $v_2 \in V_1 \cap V_2 = \{0\}$. So, $v_2 = 0$ and $v_3 = v_4 \in V_3 \cap V_4 = \{0\}$. Thus, $V_3 \cap (V_4 + V_2) = \{0\}$ and we deduce that $V = V_3 \oplus (V_4 + V_2)$, which means that V_3 is a direct summand of V.

4) Is there any $\mathbb{R}$-linear map $f : \mathbb{R}^3 \to \mathbb{R}^2$ such that

$$f(1, 0, 3) = (1, 1) \text{ and } f(-2, 0, -6) = (2, 1)?$$

Solution: No, since $f(-2, 0, -6) \neq (-2)f(1, 0, 3)$. Indeed, $f(-2, 0, -6) = (2, 1)$ and $(-2)f(1, 0, 3) = (-2)(1, 1) = (-2, -2)$.

3.3 Bases. Dimension

Definition 3.37. Let V be a vector space over K. We say that the vectors $v_1, \dots, v_n \in V$ are (or the set of vectors $\{v_1, \dots, v_n\}$ is):

(1) **linearly independent** in V if for any $k_1, \dots, k_n \in K$,

$$k_1 v_1 + \dots + k_n v_n = 0 \Rightarrow k_1 = \dots = k_n = 0\,.$$

(2) **linearly dependent** in V if they are not linearly independent, that is,

$$\exists k_1, \ldots, k_n \in K \text{ not all zero, such that } k_1v_1 + \cdots + k_nv_n = 0\,.$$

More generally, an infinite set of vectors of V is said to be:

(1) **linearly independent** if any finite subset is linearly independent.

(2) **linearly dependent** if there exists a finite subset which is linearly dependent.

Remarks 3.38. (1) A set consisting of a single vector v is linearly dependent if and only if $v = 0$.

(2) As an immediate consequence of the definition, we notice that if V is a vector space over K and $X, Y \subseteq V$ such that $X \subseteq Y$, then:

(i) If Y is linearly independent, then X is linearly independent.

(ii) If X is linearly dependent, then Y is linearly dependent. Thus, every set of vectors containing the zero vector is linearly dependent.

Theorem 3.39. Let V be a vector space over K. Then the vectors $v_1, \ldots, v_n \in V$ are linearly dependent iff one of the vectors is a linear combination of the others, that is,

$$\exists j \in \{1, \ldots, n\},\ \exists \alpha_i \in K:\ v_j = \sum_{\substack{i=1\\ i\neq j}}^{n} \alpha_i v_i.$$

Proof. Since $v_1, \ldots, v_n \in V$ are linearly dependent, there exist $k_1, \ldots, k_n \in K$ not all zero, say $k_j \neq 0$, such that $k_1v_1 + \cdots + k_nv_n = 0$. But this implies

$$-k_jv_j = \sum_{\substack{i=1\\ i\neq j}}^{n} k_iv_i$$

and further,

$$v_j = \sum_{\substack{i=1\\ i\neq j}}^{n} (-k_j^{-1}k_i)v_i\,.$$

Now choose $\alpha_i = -k_j^{-1}k_i$ for each $i \neq j$ to get the conclusion.

Conversely, if there exists $j \in \{1, \ldots, n\}$ such that

$$v_j = \sum_{\substack{i=1\\ i\neq j}}^{n} \alpha_i v_i$$

for some $\alpha_i \in K$, then

$$(-1)v_j + \sum_{\substack{i=1\\ i\neq j}}^{n} \alpha_i v_i = 0\,.$$

Since there exists such a linear combination equal to zero and the scalars are not all zero, the vectors $v_1, \ldots, v_n$ are linearly dependent. □

Examples 3.40. (a) $\emptyset$ is linearly independent in any vector space.

(b) Let V_2 be the real vector space of all vectors (in the classical sense) in the plane with a fixed origin O. Recall that the addition is the usual addition of two vectors by the parallelogram rule and the external operation is the usual scalar multiplication of vectors by real scalars. Then:

(i) one vector v is linearly dependent in $V_2 \Leftrightarrow v = 0$;

(ii) two vectors are linearly dependent in $V_2 \Leftrightarrow$ they are collinear;

(iii) three vectors are always linearly dependent in V_2.

(c) Let V_3 be the real vector space of all vectors (in the classical sense) in the space with a fixed origin O. Then:

(i) one vector v is linearly dependent in $V_3 \Leftrightarrow v = 0$;

(ii) two vectors are linearly dependent in $V_3 \Leftrightarrow$ they are collinear;

(iii) three vectors are linearly dependent in $V_3 \Leftrightarrow$ they are coplanar;

(iv) four vectors are always linearly dependent in V_3.

(d) If K is a field and $n \in \mathbb{N}^*$, then the vectors

$$(1,0,0,\dots,0),(0,1,0,\dots,0),\dots,(0,0,0,\dots,1)$$

from K^n are linearly independent in the K-vector space K^n.

(e) Let K be a field and $n \in \mathbb{N}$. Then the vectors $1, X, X^2, \dots, X^n$ are linearly independent in the vector space $K_n[X] = \{f \in K[X] \mid \deg f \leq n\}$ over K and, more generally, the vectors $1, X, X^2, \dots, X^n, \dots$ are linearly independent in the K-vector space $K[X]$.

We are going to define a key notion concerning vector spaces, namely *basis*, which will perfectly determine a vector space. We will discuss *only the case of finitely generated vector spaces.* This is why, till the end of the chapter, *by a vector space we will understand a finitely generated vector space.* However, many results from the next part hold for arbitrary vector spaces.

Definition 3.41. Let V be a vector space over K. By a **list of vectors** in V we understand an n-tuple $(v_1, \dots, v_n) \in V^n$ for some $n \in \mathbb{N}^*$.

Definition 3.42. Let V be a vector space over K. An n-tuple $B = (v_1, \dots, v_n) \in V^n$ is called a **basis** of V if:

(1) B is a system of generators for V, that is, $\langle B \rangle = V$;

(2) B is linearly independent in V.

Theorem 3.43. Let V be a vector space over K. A list $B = (v_1, \dots, v_n)$ of vectors in V is a basis of V if and only if each vector $v \in V$ can be uniquely written as a linear combination of the vectors $v_1, \dots, v_n$, i.e.

$$\forall v \in V,\ \exists k_1, \dots, k_n \in K :\ v = k_1 v_1 + \dots + k_n v_n .$$

Proof. Let us assume that B is a basis of V. Hence B is linearly independent and $\langle B \rangle = V$. The second condition assures us that every vector $v \in V$ can be written as a linear combination of the vectors of B. Let us suppose now that $v = k_1 v_1 + \dots + k_n v_n$ and $v = k_1' v_1 + \dots + k_n' v_n$ for some $k_1, \dots, k_n, k_1', \dots, k_n' \in K$. It follows that

$$(k_1 - k_1')v_1 + \dots + (k_n - k_n')v_n = 0 .$$

By the linear independence of B, we must have $k_i = k_i'$ for each $i \in \{1, \dots, n\}$. Thus, we have proved the uniqueness of writing.

Conversely, let us assume that every vector $v \in V$ can be uniquely written as a linear combination of the vectors of B. Then clearly, $V = \langle B \rangle$. If $k_1, \dots, k_n \in K$ and $k_1 v_1 + \dots + k_n v_n = 0$, since this way of writing 0 is unique, we have

$$k_1 v_1 + \dots + k_n v_n = 0 \cdot v_1 + \dots + 0 \cdot v_n \Rightarrow k_1 = \dots = k_n = 0\,,$$

hence B is linearly independent. Consequently, B is a basis of V. □

Definition 3.44. Let V be a vector space over K, $B = (v_1, \dots, v_n)$ a basis of V and $v \in V$. Then the scalars $k_1, \dots, k_n \in K$ from the unique writing of v as a linear combination

$$v = k_1 v_1 + \dots + k_n v_n$$

of the vectors of B are called the **coordinates of** v **in the basis** B.

Examples 3.45. (a) $\emptyset$ is basis for the zero vector space.
(b) If K is a field and $n \in \mathbb{N}^*$, then the list $E = (e_1, \dots, e_n)$ of vectors of K^n, where

$$e_1 = (1, 0, 0, \dots, 0), e_2 = (0, 1, 0, \dots, 0), \dots, e_n = (0, 0, 0, \dots, 1)$$

is a basis of the canonical vector space K^n over K, called the **standard basis**. Indeed, we saw that E is linearly independent and each vector $(x_1, \dots, x_n) \in K^n$ can be written as a linear combination of the vectors of E,

$$(x_1, \dots, x_n) = x_1 e_1 + \dots + x_n e_n.$$

Notice that the coordinates of a vector in the standard basis are just the components of the vector, fact that is not true in general.

In particular, if $n = 1$, the set $\{1\}$ is a basis of the canonical vector space K over K. For instance, $\{1\}$ is a basis of the vector space $\mathbb{C}$ over $\mathbb{C}$.
(c) Consider the canonical real vector space $\mathbb{R}^2$. We already know a basis of $\mathbb{R}^2$, namely the standard basis $((1, 0), (0, 1))$. But it is easy to show that the list $((1, 1), (0, 1))$ is also a basis of $\mathbb{R}^2$. Therefore, a vector space may have more than one basis.
(d) Let V_3 be the real vector space of all vectors (in the classical sense) in the space with a fixed origin O. Any 3 vectors which are not coplanar form a basis of V_3; e.g. the three pairwise orthogonal *unit vectors* $\overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k}$.
(e) The sets $S = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}$ and $T = \{(x, y, z) \in \mathbb{R}^3 \mid x = y = z\}$ are subspaces of ${}_{\mathbb{R}}\mathbb{R}^3$. As a matter of fact, $S = \langle (1, 0, -1), (0, 1, -1) \rangle$ and $T = \langle (1, 1, 1) \rangle$. Since the two generators of S are linearly independent, they form a basis of S. The only generator of T is clearly linearly independent, hence it forms a basis of T.
(f) Since for any $z \in \mathbb{C}$, there exist the uniquely determined real numbers $x, y \in \mathbb{R}$ such that $z = x \cdot 1 + y \cdot i$, the list $B = (1, i)$ is a basis of the vector space $\mathbb{C}$ over $\mathbb{R}$ (see Theorem 3.43). The coordinates of a vector $z \in \mathbb{C}$ in the basis B are just its real and its imaginary part.
(g) Let K be a field and $n \in \mathbb{N}$. Then the list $B = (1, X, X^2, \dots, X^n)$ is a basis of the vector space $K_n[X] = \{f \in K[X] \mid \deg f \leq n\}$ over K, because each vector (polynomial) $f \in K_n[X]$ can be uniquely written as a linear combination

$$f = a_0 \cdot 1 + a_1 \cdot X + \dots + a_n \cdot X^n$$

($a_0, \dots, a_n \in K$) of the vectors of B (see Theorem 3.43). In this case, the coordinates of a vector $f \in K_n[X]$ in the basis B are just its coefficients as a polynomial.
(h) Let K be a field. The list

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right)$$

is a basis of the vector space $M_2(K)$ over K. More generally, let $m, n \in \mathbb{N}$, $m, n \geq 2$ and consider the matrices $E_{ij} = (a_{kl})$, where

$$a_{kl} = \begin{cases} 1 & \text{if } k = i \text{ and } l = j \\ 0 & \text{otherwise} \end{cases}.$$

The list consisting of all matrices E_{ij} is a basis of the K-vector space $M_{mn}(K)$ and the coordinates of a vector $A \in M_{mn}(K)$ in the above basis are the entries of A.
(i) If V_1 and V_2 are K-vector spaces and $B_1 = (x_1, \dots, x_m)$ and $B_2 = (y_1, \dots, y_n)$ are bases for V_1 and V_2, respectively, then $((x_1, 0), \dots, (x_m, 0), (0, y_1), \dots, (0, y_n))$ is a basis for the direct product $V_1 \times V_2$.

Theorem 3.46. Every vector space has a basis.

Proof. Let V be a vector space over K. If $V = \{0\}$, then it has the basis $\emptyset$.

Now let $\{0\} \neq V = \langle B \rangle$, where $B = (v_1, \dots, v_n)$. If B is linearly independent, then B is a basis and we are done. Suppose that the list B is linearly dependent. Then by Theorem 3.39, there exists $j_1 \in \{1, \dots, n\}$ such that

$$v_{j_1} = \sum_{\substack{i=1 \\ i \neq j_1}}^{n} k_i v_i$$

for some $k_i \in K$. It follows that $V = \langle B \setminus \{v_{j_1}\} \rangle$, because every vector of V can be written as a linear combination of the vectors of $B \setminus \{v_{j_1}\}$. If $B \setminus \{v_{j_1}\}$ is linearly independent, it is a basis and we are done. Otherwise, there exists $j_2 \in \{1, \dots, n\} \setminus \{j_1\}$ such that

$$v_{j_2} = \sum_{\substack{i=1 \\ i \neq j_1, j_2}}^{n} k'_i v_i$$

for some $k'_i \in K$. It follows that $V = \langle B \setminus \{v_{j_1}, v_{j_2}\} \rangle$, because every vector of V can be written as a linear combination of the vectors of $B \setminus \{v_{j_1}, v_{j_2}\}$. If $B \setminus \{v_{j_1}, v_{j_2}\}$ is linearly independent, then it is a basis and we are done. Otherwise, we continue the procedure. If all the previous intermediate subsets are linearly dependent, we get to the step $V = \langle B \setminus \{v_{j_1}, \dots, v_{j_{n-1}}\} \rangle = \langle v_{j_n} \rangle$. If v_{j_n} were linearly dependent, then $v_{j_n} = 0$, hence $V = \langle v_{j_n} \rangle = \{0\}$, contradiction. Hence v_{j_n} is linearly independent and thus forms a single element basis of V. □

Remarks 3.47. (1) We have proved the existence of a basis of a vector space. As we saw in Example 3.45 (c) such a basis not necessarily unique.
(2) In the proof of Theorem 3.46 we saw that if B is an n-elements set which generates V one can successively eliminate elements from B in order to find a basis for V. It follows that any basis of V has at most n vectors. Later we will prove even a stronger result, namely if a vector space has a basis of n elements, then all its bases have n elements.

Theorem 3.48. i) Let $f : V \to V'$ be a K-linear map and let $B = (v_1, \dots, v_n)$ be a basis of V. Then f is determined by its values on the vectors of the basis B.
ii) Let $f, g : V \to V'$ be K-linear maps and let $B = (v_1, \dots, v_n)$ be a basis of V. If $f(v_i) = g(v_i)$, for any $i \in \{1, \dots, n\}$, then $f = g$.

Proof. i) Let $v \in V$. Since B is a basis of V, there exists $k_1, \dots, k_n \in K$ uniquely determined such that $v = k_1v_1 + \dots + k_nv_n$. Then

$$f(v) = f(k_1v_1 + \dots + k_nv_n) = k_1f(v_1) + \dots + k_nf(v_n)\,,$$

that is, f is determined by $f(v_1)$, ..., $f(v_n)$.
ii) Let $v \in V$. Then $v = k_1v_1 + \dots + k_nv_n$ for some $k_1, \dots, k_n \in K$, hence

$$f(v) = f(k_1v_1 + \dots + k_nv_n) = k_1f(v_1) + \dots + k_nf(v_n) = k_1g(v_1) + \dots + k_ng(v_n) = g(v)\,.$$

Therefore, $f = g$. □

Remark 3.49. From the previous theorem one deduces that *given two K-vector spaces V, V', a basis B of V and a function $f' : B \to V'$, there exists a unique linear map $f : V \to V'$ which extends f' (i.e. $f|_B = f'$ or, equivalently, $f(x_i) = f'(x_i)$, $i = 1, \dots, n$),* result also known as **universal property of vector spaces**.

Theorem 3.50. Let $f : V \to V'$ be a K-linear map. Then:
(i) f is injective if and only if for any X linearly independent in V, $f(X)$ is linearly independent in V'.
(ii) f is surjective if and only if for any X system of generators for V, $f(X)$ is a system of generators for V'.
(iii) f is bijective if and only if for any X basis of V, $f(X)$ is a basis of V'.

Proof. (i) Let $X = (v_1, \dots, v_n)$ be a linearly independent list of vectors in V and let $k_1, \dots, k_n \in K$ be such that $k_1f(v_1) + \dots + k_nf(v_n) = 0$. Since f is a K-linear map, we deduce $f(k_1v_1 + \dots + k_nv_n) = f(0)$. By the injectivity of f we get $k_1v_1 + \dots + k_nv_n = 0$. But since X is linearly independent in V, we have $k_1 = \dots = k_n = 0$. Therefore, $f(X)$ is linearly independent in V'.

Conversely, let $x, y \in V$ with $x \neq y$. Then the non-zero vector $x - y$ is linearly independent, hence $f(x - y)$ is linearly independent by hypothesis. So, $f(x - y) \neq 0$ and thus, $f(x) \neq f(y)$. Thus f is injective.
(ii) Let X be a system of generators for V. Then $\langle X \rangle = V$. By Theorem 3.33 and the surjectivity of f we have:

$$\langle f(X) \rangle = f(\langle X \rangle) = f(V) = V'\,,$$

that is, $f(X)$ is a system of generators for V'.

Conversely, V is, clearly, a system of generators for V. By hypothesis, it follows that $f(V)$ is a system of generators for V'. Hence $\langle f(V) \rangle = V'$. Now by Theorem 3.33, we get $f(\langle V \rangle) = V'$, that is, $f(V) = V'$. Hence f is surjective.
(iii) It follows by (i) and (ii). □

Recall that we consider only finitely generated vector spaces. Let us begin with a very useful lemma, that will be often implicitly used.

Lemma 3.51. Let V be a K-vector space and let $Y = \langle y_1, \dots, y_n, z\rangle$. If $z \in \langle y_1, \dots, y_n\rangle$, then $Y = \langle y_1, \dots, y_n\rangle$.

Proof. The generated subspace Y is the set of all linear combinations of the vectors $y_1, \dots, y_n, z$ (see Theorem 3.17). Since $z \in \langle y_1, \dots, y_n\rangle$, z is a linear combination of the vectors $y_1, \dots, y_n$. It follows that every vector in Y can be written as a linear combination only of the vectors $y_1, \dots, y_n$. Consequently, $Y = \langle y_1, \dots, y_n\rangle$. □

Let us now discuss a key theorem for proving that any two bases of a vector space have the same number of elements. But it is worth mentioning that it has a much broader importance in Linear Algebra.

Theorem 3.52. (Steinitz, The Exchange Theorem) Let V be a vector space over K, let $X = (x_1, \dots, x_m)$ be a linearly independent list of vectors of V and $Y = (y_1, \dots, y_n)$ a system of generators of V ($m, n \in \mathbb{N}^*$). Then $m \le n$ and m vectors of Y can be replaced by the vectors of X in order to obtain a system of generators for V.

Proof. We prove this result by way of induction on m. Let us take $m = 1$. Then clearly $m \le n$. Since Y is a system of generators for V, we have $x_1 = \sum_{i=1}^{n} k_i y_i$ for some $k_1, \dots, k_n \in K$. The list $X = \{x_1\}$ is linearly independent, hence $x_1 \ne 0$. It follows that there exists $j \in \{1, \dots, n\}$ such that $k_j \ne 0$. Then

$$y_j = k_j^{-1} x_1 - \sum_{\substack{i=1\\ i\ne j}}^{n} k_j^{-1} k_i y_i\,,$$

that is, y_j is a linear combination of the vectors $y_1, \dots, y_{j-1}, x_1, y_{j+1}, \dots, y_n$. Hence, in any linear combination of $y_1, \dots, y_n$, the vector y_j can be expressed as a linear combination of the other vectors and x_1. Therefore, we have

$$V = \langle y_1, \dots, y_n\rangle = \langle y_1, \dots, y_{j-1}, x_1, y_{j+1}, \dots, y_n\rangle\,.$$

Thus, we have obtained again a system of n generators for V containing x_1.

Let us assume that the statement holds for a list with $m-1$ linearly independent vectors of V ($m \in \mathbb{N},\ m \ge 2$) and let us prove it for the linearly independent list $X = (x_1, \dots, x_m)$. Then $(x_1, \dots, x_{m-1})$ is also linearly independent in V. By the induction step hypothesis, we have $m - 1 \le n$. If necessary, we can reindex the elements of Y and we have

$$V = \langle x_1, \dots, x_{m-1}, y_m, \dots, y_n\rangle\,.$$

Assume by contradiction that $m - 1 = n$. Then from $V = \langle x_1, \dots, x_{m-1}\rangle$ it follows that $x_m \in \langle x_1, \dots, x_{m-1}\rangle$, which is absurd since X is linearly independent in V. Thus $m - 1 < n$ or, equivalently, $m \le n$.

We have $x_m \in V = \langle x_1, \dots, x_{m-1}, y_m, \dots, y_n\rangle$, hence

$$x_m = \sum_{i=1}^{m-1} k_i x_i + \sum_{i=m}^{n} k_i y_i$$

for some $k_1, \dots, k_n \in K$. The list X being linearly independent in V, it follows that there exists $m \le j \le n$ such that $k_j \ne 0$ (otherwise, $x_m = \sum_{i=1}^{m-1} k_i x_i$ and the list X

would be linearly dependent in V). For simplicity of writing, assume that $j = m$. It follows that

$$y_m = k_m^{-1}x_m - \sum_{i=1}^{m-1} k_m^{-1}k_ix_i - \sum_{i=m+1}^{n} k_m^{-1}k_iy_i \,.$$

Thus, $y_m \in \langle x_1, \dots, x_m, y_{m+1}, \dots, y_n\rangle$. Therefore, we have

$$V = \langle x_1, \dots, x_{m-1}, y_m, \dots, y_n\rangle = \langle x_1, \dots, x_m, y_{m+1}, \dots, y_n\rangle \,.$$

Thus, we have obtained again a system of generators for V, where m vectors of the list Y have been replaced by the vectors of the list X. This completes the proof. □

Theorem 3.53. Any two bases of a vector space have the same number of elements.

Proof. Let V be a vector space over K and let $B = (v_1, \dots, v_m)$ and $B' = (v_1', \dots, v_n')$ be bases of V. Since B is linearly independent in V and B' is a system of generators for V, we have $m \leq n$ by Theorem 3.52. Since B is a system of generators for V and B' is linearly independent in V, we have $n \leq m$ by the same Theorem 3.52. Hence $m = n$. □

Definition 3.54. Let V be a vector space over K. Then the number of elements of any of its bases is called the **dimension of** V and is denoted by $\dim_K V$ or simply by $\dim V$.

Examples 3.55. Using the bases given in Examples 3.45, one can easily determine the dimension of those vector spaces.
(a) If $V = \{0\}$, V has the basis $\emptyset$ and $\dim V = 0$.
(b) Let K be a field and $n \in \mathbb{N}^*$. Then $\dim_K K^n = n$. In particular, $\dim_{\mathbb{C}} \mathbb{C} = 1$.
(c) $\dim_{\mathbb{R}} \mathbb{C} = 2$.
(d) $S = \{(x, y, z) \in \mathbb{R}^3 \mid x + y + z = 0\}$ and $T = \{(x, y, z) \in \mathbb{R}^3 \mid x = y = z\}$ are subspaces of ${}_{\mathbb{R}}\mathbb{R}^3$ with $\dim S = 2$ and $\dim T = 1$. More general, the subspaces of $\mathbb{R}^3$ are $\{(0, 0, 0)\}$, any line containing the origin, any plane containing the origin and ${}_{\mathbb{R}}\mathbb{R}^3$. Their dimensions are 0, 1, 2 and 3, respectively.
(e) Let K be a field and $n \in \mathbb{N}$. Then $\dim K_n[X] = n + 1$.
(f) Let K be a field. Then $\dim M_2(K) = 4$. More generally, if $m, n \in \mathbb{N}$, $m, n \geq 2$, then $\dim M_{mn}(K) = m \cdot n$.
(g) If V_1 and V_2 are K-vector spaces and $B_1 = (x_1, \dots, x_m)$ and $B_2 = (y_1, \dots, y_n)$ are bases for V_1 and V_2, respectively, then $\dim(V_1 \times V_2) = m + n = \dim V_1 + \dim V_2$.

Theorem 3.56. Let V be a vector space over K. Then the following statements are equivalent:

(i) $\dim V = n$;
(ii) The maximum number of linearly independent vectors in V is n;
(iii) The minimum number of generators for V is n.

Proof. (i)⇒(ii) Assume $\dim V = n$. Let $B = (v_1, \dots, v_n)$ be a basis of V. Since B is a system of generators for V, any linearly independent list in V must have at most n elements by Theorem 3.52.
(ii)⇒(i) Let $B = (v_1, \dots, v_m)$ be a basis of V and let $(u_1, \dots, u_n)$ be a linearly independent list in V. Since B is linearly independent, we have $m \leq n$ by hypothesis. Since B

is a system of generators for V, we have $n \leq m$ by Theorem 3.52. Hence $m = n$ and consequently $\dim V = n$.
(i)$\Rightarrow$(iii) Assume $\dim V = n$. Let $B = (v_1, \ldots, v_n)$ be a basis of V. Since B is a linearly independent list in V, any system of generators for V must have at least n elements by Theorem 3.52.
(iii)$\Rightarrow$(i) Let $B = (v_1, \ldots, v_m)$ be a basis of V and let $(u_1, \ldots, u_n)$ be a system of generators for V. Since B is a system of generators for V, we have $n \leq m$ by hypothesis. Since B is linearly independent, we have $m \leq n$ by Theorem 3.52. Hence $m = n$ and consequently $\dim V = n$. □

Theorem 3.57. Let V be a vector space over K with $\dim V = n$ and $X = (u_1, \ldots, u_n)$ a list of vectors in V. Then X is linearly independent in V if and only if X is a system of generators for V.

Proof. Let $B = (v_1, \ldots, v_n)$ be a basis of V.

Let us assume that X is linearly independent. Since B is a system of generators for V, we know by Theorem 3.52 that n vectors of B, i.e., all the vectors of B, can be replaced by the vectors of X and we get another system of generators for V. Hence $\langle X \rangle = V$. Thus, X is a system of generators for V.

Conversely, let us suppose that X is a system of generators for V. Assume by contradiction that X is linearly dependent. Then there exists $j \in \{1, \ldots, n\}$ such that

$$u_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i u_i$$

for some $k_i \in K$. It follows that $V = \langle X \rangle = \langle u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n \rangle$. This contradicts the fact that the minimum number of generators for V is n (see Theorem 3.56). Thus our assumption must have been false. So X is linearly independent. □

Theorem 3.58. Any linearly independent list of vectors in a vector space can be completed to a basis of the vector space.

Proof. Let V be a K-vector space, let $B = (v_1, \ldots, v_n)$ be a basis of V and $(u_1, \ldots, u_m)$ be a linearly independent list in V. Since B is a system of generators for V, we know by Theorem 3.52 that $m \leq n$ and m vectors of B can be replaced by the vectors $(u_1, \ldots, u_m)$ obtaining again a system of generators for V, say $(u_1, \ldots, u_m, v_{m+1}, \ldots, v_n)$. But by Theorem 3.57, this is also linearly independent in V and consequently a basis of V. □

Remark 3.59. The completion of a linearly independent list to a basis of the vector space is not unique.

Example 3.60. The list (e_1, e_2), where $e_1 = (1, 0, 0)$ and $e_2 = (0, 1, 0)$, is linearly independent in the canonical real vector space $\mathbb{R}^3$. It can be completed to the standard basis of the space, namely (e_1, e_2, e_3), where $e_3 = (0, 0, 1)$. On the other hand, since $\dim_{\mathbb{R}} \mathbb{R}^3 = 3$, in order to obtain a basis of the space it is enough to add to our list any vector v_3 for which (e_1, e_2, v_3) is linearly independent (see Theorem 3.57). For instance, we may take $v_3 = (1, 1, 1)$.

Corollary 3.61. Let V be a vector space over K and $S \leq_K V$. Then:

(i) Any basis of S is a part of a basis of V.

(ii) $\dim S \leq \dim V$.

(iii) $\dim S = \dim V \Leftrightarrow S = V$.

Proof. (i) Let $(u_1, \dots, u_m)$ be a basis of S. Since the list is linearly independent, it can be completed to a basis $(u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ of V by Theorem 3.58.

(ii) follows from (i).

(iii) Assume that $\dim S = \dim V = n$. Let $(u_1, \dots, u_n)$ be a basis of S. Then it is linearly independent in V, hence it is a basis of V by Theorem 3.57. Thus, if $v \in V$, then $v = k_1 u_1 + \dots + k_n u_n$ for some $k_1, \dots, k_n \in K$, hence $v \in S$. Therefore, $S = V$. □

Remark 3.62. For the equivalence (iii) from the previous corollary the fact that we are working in a finitely generated space is essential.

Theorem 3.63. Let V and V' be vector spaces over K. Then

$$V \simeq V' \Leftrightarrow \dim V = \dim V' .$$

Proof. $\Rightarrow$. Let $f : V \to V'$ be a K-isomorphism. If $(v_1, \dots, v_n)$ is a basis of V, then by Theorem 3.50, $(f(v_1), \dots, f(v_n))$ is a basis of V'. Hence $\dim V = \dim V'$.

$\Leftarrow$. Assume that $\dim V = \dim V' = n$. Let $B = (v_1, \dots, v_n)$ and $B' = (v'_1, \dots, v'_n)$ be bases of V and V' respectively. We know by Theorem 3.48 that a K-linear map $f : V \to V'$ is determined by its values on the vectors of the basis B. Define $f(v_i) = v'_i$, for any $i \in \{1, \dots, n\}$. Then it is easy to check that f is a K-isomorphism. □

Corollary 3.64. Any vector space V over K with $\dim V = n (\in \mathbb{N}^*)$ is isomorphic to the canonical vector space K^n over K.

Remark 3.65. Corollary 3.64 is a very important structure result, saying that, up to an isomorphism, any finite dimensional vector space over K is, actually, the canonical vector space K^n over K. Thus, we have an explanation why we have used so often this kind of vector spaces: not only because the operations are very nice and easily defined, but they are, up to an isomorphism, the only types of finite dimensional vector spaces.

We end this section with some important formulas involving vector space dimension.

Theorem 3.66. Let $f : V \to V'$ be a K-linear map. Then

$$\dim V = \dim(\mathrm{Ker} f) + \dim(\mathrm{Im} f) .$$

Proof. Let $(u_1, \dots, u_m)$ be a basis of the subspace $\mathrm{Ker} f$ of V. Then by Corollary 3.61, it can be completed to a basis $B = (u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ of V. We are going to prove that $B' = (f(v_{m+1}), \dots, f(v_n))$ is a basis of $\mathrm{Im} f$.

First, we prove that B' is linearly independent in $\mathrm{Im} f$. Let us take $k_{m+1}, \dots, k_n \in K$. By the K-linearity of f we have:

$$\sum_{i=m+1}^{n} k_i f(v_i) = 0 \Rightarrow f\Big(\sum_{i=m+1}^{n} k_i v_i \Big) = 0 \Rightarrow \sum_{i=m+1}^{n} k_i v_i \in \mathrm{Ker} f .$$

Since $(u_1, \dots, u_m)$ is a basis of Ker$f$, there exist $k_1, \dots, k_m \in K$ such that

$$\sum_{i=m+1}^{n} k_i v_i = \sum_{i=1}^{m} k_i u_i \,,$$

that is,

$$\sum_{i=1}^{m} k_i u_i - \sum_{i=m+1}^{n} k_i v_i = 0 \,.$$

But $B = (u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ is a basis of V, hence it follows that $k_i = 0$, for any $i \in \{1, \dots, n\}$. Therefore, B' is linearly independent in Imf.

Let us now show that B' is a system of generators for Imf. Let $v' \in$ Imf. Then $v' = f(v)$ for some $v \in V$. Since B is a basis of V, there exist $k_1, \dots, k_n \in K$ such that

$$v = \sum_{i=1}^{m} k_i u_i + \sum_{i=m+1}^{n} k_i v_i \,.$$

By the K-linearity of f and the fact that $u_1, \dots, u_m \in$ Ker$f$, it follows that

$$v' = f(v) = f\Big(\sum_{i=1}^{m} k_i u_i + \sum_{i=m+1}^{n} k_i v_i\Big) = \sum_{i=1}^{m} k_i f(u_i) + \sum_{i=m+1}^{n} k_i f(v_i) = \sum_{i=m+1}^{n} k_i f(v_i) \,.$$

Hence B' is a system of generators for Imf.

Therefore, B' is a basis of Imf and consequently,

$$\dim V = n = m + (n - m) = \dim(\mathrm{Ker} f) + \dim(\mathrm{Im} f) \,.$$

□

Corollaries 3.67. a) Let V be a K-vector space and let S, T be subspaces of V. Then

$$\dim S + \dim T = \dim(S \cap T) + \dim(S + T).$$

Indeed, $f : S \times T \to S + T$, $f(x, y) = x - y$ is a surjective linear map with the kernel $\mathrm{Ker}\, f = \{(x, x) \mid x \in S \cap T\}$. Hence,

$$\dim(S \times T) = \dim(\mathrm{Ker}\, f) + \dim(S + T).$$

Since $g : S \cap T \to \mathrm{Ker}\, f$, $g(x) = (x, x)$ is an isomorphism, we have

$$\dim(\mathrm{Ker}\, f) = \dim(S \cap T),$$

and by Example 3.55 g) we have $\dim(S \times T) = \dim S + \dim T$, which completes the proof of the statement.

b) If V is a K-vector space and $S, T \leq_K V$, then

$$\dim(S + T) = \dim S + \dim T \Leftrightarrow S + T = S \oplus T.$$

c) Let V be a K-vector space and $f \in End_K(V)$. The following statements are equivalent:

(i) f is injective;
(ii) f is surjective;
(iii) f is bijective.

Of course, it is enough to show that (i)$\Leftrightarrow$ (ii).

(i)$\Rightarrow$(ii) If f is injective, then $\mathrm{Ker}f = \{0\}$ by Theorem 3.32, hence $\dim(\mathrm{Ker}f) = 0$. By Theorem 3.66, it follows that $\dim(\mathrm{Im}f) = \dim V$. But $\mathrm{Im}f \leq_K V$, so $\mathrm{Im}f = V$ by Corollary 3.61.

(ii)$\Rightarrow$(i) Let us assume that f is surjective. Since $\mathrm{Im}f = V$, it follows by Theorem 3.66 that $\dim(\mathrm{Ker}f) = 0$, whence $\mathrm{Ker}f = \{0\}$. By Theorem 3.32, f is injective.

3.4 Exercises with solution

1) Let $n \in \mathbb{N}$ and $f_n : \mathbb{R} \to \mathbb{R}$, $f_n(x) = \sin^n x$. Show that $L = \{f_n \mid n \in \mathbb{N}\}$ is a linearly independent subset of the $\mathbb{R}$-vector space $\mathbb{R}^{\mathbb{R}}$.

Solution: L is linearly independent if and only if for any $n_1, \dots, n_k \in \mathbb{N}$ mutually different, the vectors $f_{n_1}, \dots, f_{n_k}$ are linearly independent. Let us take $\alpha_1, \dots, \alpha_k \in \mathbb{R}$ arbitrary such that $\alpha_1 f_{n_1} + \dots + \alpha_k f_{n_k} = \theta$ (θ is the zero map). It follows that

$$\forall x \in \mathbb{R},\ \alpha_1 \sin^{n_1} x + \dots + \alpha_k \sin^{n_k} x = 0.$$

We deduce that for the polynomial

$$p = \alpha_1 X^{n_1} + \dots + \alpha_k X^{n_k} \in \mathbb{R}[X]$$

any number $t(= \sin x) \in [-1, 1]$ is a root, hence it has infinitely many roots. This is possible only if $p = 0$, so $\alpha_1 = \dots = \alpha_k = 0$.

2) Let $p \in \mathbb{N}$ be a prime number. Show that the usual addition and multiplication determine a $\mathbb{Q}$-vector space structure on $V = \{a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \mid a, b, c \in \mathbb{Q}\}$ and find a basis and the dimension of ${}_{\mathbb{Q}}V$.

Solution: V is a subspace of ${}_{\mathbb{Q}}\mathbb{R}$ generated by $\{1, \sqrt[3]{p}, \sqrt[3]{p^2}\}$. We show that $1, \sqrt[3]{p}, \sqrt[3]{p^2}$ are linearly independent. If $a, b, c \in \mathbb{Q}$ and $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0$. Multiplying this equality by $\sqrt[3]{p}$, we get $a\sqrt[3]{p} + b\sqrt[3]{p^2} + cp = 0$. We eliminate $\sqrt[3]{p^2}$ from the two equalities and we have $(ab - c^2p) + (b^2 - ac)\sqrt[3]{p} = 0$. Since $\sqrt[3]{p} \notin \mathbb{Q}$, we must have $ab - c^2p = 0 = b^2 - ac$. Assuming by contradiction that $a \neq 0$ we have $c = \dfrac{b^2}{a}$, hence $ab - \dfrac{b^4}{a^2}p = 0$, i.e. $p = \dfrac{b^3}{a^3}$. This implies $\sqrt[3]{p} = \dfrac{b}{a} \in \mathbb{Q}$, which is absurd. Thus $a = 0$, and, consequently, $b = c = 0$. It means that $(1, \sqrt[3]{p}, \sqrt[3]{p^2})$ is a basis of ${}_{\mathbb{Q}}V$ and $\dim_{\mathbb{Q}} V = 3$.

3) Let V be a K-vector space whose dimension is 3 and let V_1, V_2 be two different subspaces, both having the dimension 2. Show that the dimension of $V_1 \cap V_2$ is 1. Which is the geometric meaning of this situation when $K = \mathbb{R}$, $V = \mathbb{R}^3$?

Solution: From $V_1 \neq V_2$ and $\dim V_1 = \dim V_2$ it follows that $V_2 \nsubseteq V_1$. Hence,

$$V_1 \subsetneqq V_1 + V_2 \subseteq V,$$

which implies $\dim(V_1 + V_2) = 3$ and

$$\dim(V_1 \cap V_2) = \dim V_1 + \dim V_2 - \dim(V_1 + V_2) = 1.$$

In $\mathbb{R}^3$ this means that the intersection of two distinct planes which contain the origin is a line which contains the origin.

4) Let V be a K-vector space whose dimension is $n \in \mathbb{N}^*$ and let V_1, V_2 be subspaces of V. Sho that if $\dim V_1 = n-1$ and $V_2 \nsubseteq V_1$ then

$$\dim(V_1 \cap V_2) = \dim V_2 - 1 \text{ and } V_1 + V_2 = V.$$

Solution: Since $V_2 \nsubseteq V_1$, we have $V_1 \cap V_2 \subsetneqq V_2$, so $\dim(V_1 \cap V_2) < \dim V_2$, or, equivalently, $\dim V_2 - \dim(V_1 \cap V_2) \geq 1$. Then

$$n = \dim V \geq \dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim(V_1 \cap V_2) \geq n - 1 + 1 = n.$$

Therefore, $\dim(V_1 + V_2) = n = \dim V$, thus $V = V_1 + V_2$. Finally, we have

$$\dim(V_1 \cap V_2) = \dim V_1 + \dim V_2 - \dim(V_1 + V_2) = n - 1 + \dim V_2 - n = \dim V_2 - 1.$$

3.5 Exercises

1) Show that the Abelian group $(\mathbb{R}_+^*, \cdot)$ is an $\mathbb{R}$-vector space with respect to the scalar multiplication $*$ defined by

$$\alpha * x = x^\alpha,\ \alpha \in \mathbb{R},\ x \in \mathbb{R}_+^*$$

and that this vector space is isomorphic to the $\mathbb{R}$-vector space defined on $\mathbb{R}$ by the usual addition and multiplication.

2) Let V be a K-vector space, let $\alpha, \beta, \gamma \in K$ and $x, y, z \in V$ such that $\alpha\gamma \neq 0$ and $\alpha x + \beta y + \gamma z = 0$. Show that $\langle x, y \rangle = \langle y, z \rangle$.

3) In the $\mathbb{R}$-vector space $\mathbb{R}^\mathbb{R} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ one considers

$$(\mathbb{R}^\mathbb{R})_i = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is odd}\},\ (\mathbb{R}^\mathbb{R})_p = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ is even}\}.$$

Show that $(\mathbb{R}^\mathbb{R})_i$ and $(\mathbb{R}^\mathbb{R})_p$ are subspaces of $\mathbb{R}^\mathbb{R}$ and $\mathbb{R}^\mathbb{R} = (\mathbb{R}^\mathbb{R})_i \oplus (\mathbb{R}^\mathbb{R})_p$.

4) Let V be a $\mathbb{R}$-vector space and $v_1, v_2, v_3 \in V$. Show that v_1, v_2, v_3 are linearly independent if and only if the vectors $v_2 + v_3, v_3 + v_1, v_1 + v_2$ are linearly independent.

5) Show that in the $\mathbb{R}$-vector space $M_2(\mathbb{R})$ the matrices

$$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},\ E_2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix},\ E_3 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ E_4 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

form a basis and find the coordinates of the matrix $A = \begin{pmatrix} -2 & 3 \\ 4 & -2 \end{pmatrix}$ in this basis.

6) Find $a \in \mathbb{R}$ such that the vectors $v_1 = (a, 1, 1)$, $v_2 = (1, a, 1)$, $v_3 = (1, 1, a)$ form a basis of the real vector space $\mathbb{R}^3$.

7) In the $\mathbb{Q}$-vector space $\mathbb{Q}^3$ one considers the vectors

$$a = (-2, 1, 3),\ b = (3, -2, -1),\ c = (1, -1, 2),\ d = (-5, 3, 4),\ e = (-9, 5, 10).$$

Prove that $\langle a, b \rangle = \langle c, d, e \rangle$.

8) In the $\mathbb{R}$-vector space $\mathbb{R}^4$ one considers the subspaces:

a) $S = \langle u_1, u_2, u_3 \rangle$, with $u_1 = (1, 2, 2, 1, -2)$, $u_2 = (2, 3, 1, 0)$, $u_3 = (1, 2, 2, -3)$,
$T = \langle v_1, v_2, v_3 \rangle$, with $v_1 = (1, 1, 1, 1)$, $v_2 = (1, 0, 1, -1)$, $v_3 = (1, 3, 0, -3)$;

b) $S = \langle u_1, u_2\rangle$, with $u_1 = (1, 2, 1, 0)$, $u_2 = (-1, 1, 1, 1)$,
$T = \langle v_1, v_2\rangle$, with $v_1 = (2, -1, 0, 1)$, $v_2 = (1, -1, 3, 7)$;
c) $S = \langle u_1, u_2\rangle$, with $u_1 = (1, 1, 0, 0)$, $u_2 = (1, 0, 1, 1)$,
$T = \langle v_1, v_2\rangle$, with $v_1 = (0, 0, 1, 1)$, $v_2 = (0, 1, 1, 0)$;
d) $S = \langle u_1, u_2, u_3\rangle$, with $u_1 = (1, 2, -1, -2)$, $u_2 = (3, 1, 1, 1)$, $u_3 = (-1, 0, 1, -1)$,
$T = \langle v_1, v_2\rangle$, with $v_1 = (-1, 2, -7, -3)$, $v_2 = (2, 5, -6, -5)$.
Find a basis and the dimension for each of the spaces S, T, $S + T$ and $S \cap T$.

4 Matrices and linear maps. Systems of linear equations

For a better understanding of this section, we recommend the reader to remind the basics concerning the determinant of a matrix and the rank of a matrix. In order to support their effort, we list here some of the properties which will be used in our further discussions.

Let K be a field, $A = (a_{ij}) \in M_n(K)$, $n \geq 2$, $d = \det A$, let d_{ij} be the minor of a_{ij} and $\alpha_{ij} = (-1)^{i+j} d_{ij}$ be the cofactor of a_{ij}.
1) The determinant of A and the deteriminant of its transpose matrix ${}^tA$ are equal.
2) If the matrix B results from A by multiplying each element of a row (column) of A by an element $\alpha \in K$ then $\det(B) = \alpha \det(A)$.
3) If A has two equal rows (columns), then $\det(A) = 0$.
4) If B results from A after permuting two rows (columns) of A then $\det(B) = -\det(A)$.
5) If a row (column) of A consists only of 0, then $\det(A) = 0$.
6) If B results from A after adding to its i-th row (column) its j-th row (column) multiplied by an element from K $(i \neq j)$, then $\det B = \det A$.
7) If a row (column) of A is a linear combination of the other rows (columns) of A, then $\det A = 0$.
8) If $A, B \in M_n(K)$ then $\det(AB) = \det(A) \cdot \det(B)$.
9) **(the cofactor expansion of $\det(A)$ along its i-th row)**

$$\det(A) = a_{i1}\alpha_{i1} + a_{i2}\alpha_{i2} + \cdots + a_{in}\alpha_{in},\ \forall i \in \{1, \ldots, n\}.$$

10) **(the cofactor expansion of $\det(A)$ along its j-th column)**

$$\det A = a_{1j}\alpha_{1j} + a_{2j}\alpha_{2j} + \cdots + a_{nj}\alpha_{nj},\ \forall j \in \{1, \ldots, n\}.$$

11) If $i, k \in \{1, \ldots, n\}$, $i \neq k$, then

$$a_{i1}\alpha_{k1} + a_{i2}\alpha_{k2} + \cdots + a_{in}\alpha_{in} = 0.$$

12) If $j, k \in \{1, \ldots, n\}$, $j \neq k$ then

$$a_{1j}\alpha_{1k} + a_{2j}\alpha_{2k} + \cdots + a_{nj}\alpha_{nk} = 0.$$

Using the above properties, we can deduce the following:

Theorem 4.1. A matrix $A = (a_{ij}) \in M_n(K)$ is invertible if and only if $d = \det(A) \neq 0$. If this is the case, then

$$A^{-1} = d^{-1} \cdot A^*.$$

Proof. If A is invertible, i.e. there exists $A^{-1} \in M_n(K)$ such that

$$A^{-1} \cdot A = I_n = A \cdot A^{-1},$$

according to 8), we have

$$\det(A^{-1}) \cdot \det(A) = 1,$$

hence $d \neq 0$.

Conversely, let us consider $d \neq 0$. Let us take the matrix $A^* = {}^t(\alpha_{ij})$ (called the **adjugate** or the **(classical) adjoint**) of A. From 9), 10), 11) and 12) it follows

$$A^* \cdot A = d \cdot I_n = A \cdot A^*.$$

Hence, if $d \neq 0$ then A has an inverse matrix equal to $A^{-1} = d^{-1} \cdot A^*$. □

The previous properties also allow us to connect the rank of a matrix with the dimension of the subspace generated by its rows (columns).

Theorem 4.2. If $A \in M_{m,n}(K)$, and $r_1^A, \ldots, r_m^A \in K^n$ and $c_1^A, \ldots, c_n^A \in K^m$ are the rows and the columns of A, respectively, then

$$\operatorname{rank} A = \dim\langle r_1^A, \ldots, r_m^A\rangle = \dim\langle c_1^A, \ldots, c_n^A\rangle.$$

where $\langle r_1^A, \ldots, r_m^A\rangle$ is the subspace of K^n generated by $r_1^A, \ldots, r_m^A$ and $\langle c_1^A, \ldots, c_n^A\rangle$ is the subspace of K^m generated by $c_1^A, \ldots, c_n^A$.

Proof. Let $r = \operatorname{rank} A$. The matrix A has an $r \times r$ nonzero minor. To simplify the notations, we consider that such a minor is

$$d = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} \\ a_{21} & a_{22} & \ldots & a_{2r} \\ \vdots & \vdots & & \vdots \\ a_{r1} & a_{r2} & \ldots & a_{rr} \end{vmatrix} \neq 0$$

Since any $(r+1) \times (r+1)$ minor is zero, the $(r+1) \times (r+1)$ determinant

$$D_{ij} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} & a_{1j} \\ a_{21} & a_{22} & \ldots & a_{2r} & a_{2j} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{r1} & a_{r2} & \ldots & a_{rr} & a_{rj} \\ a_{i1} & a_{i2} & \ldots & a_{ir} & a_{ij} \end{vmatrix}$$

obtained by adding to d the i-th row and the j-th column of A is) $(1 \leq i \leq m, r < j \leq n)$, i.e. $D_{ij} = 0$. The cofactor expansion of D_{ij} along its $r+1$-th row gives us

$$a_{i1}d_1 + a_{i2}d_2 + \cdots + a_{ir}d_r + a_{ij}d = 0,$$

where the cofactors $d_1, d_2, \ldots, d_r$ do not depend on the added row. It follows that

$$a_{ij} = -d^{-1}d_1 a_{i1} - d^{-1}d_2 a_{i2} - \cdots - d^{-1}d_r a_{ir}$$

for $i = 1, 2, \ldots, m$ and $j = r+1, \ldots, n$. Therefore,

$$c_j^A = \alpha_1 c_1^A + \alpha_2 c_2^A + \cdots + \alpha_r c_r^A \text{ for } j = r+1, \ldots, n,$$

where $\alpha_k = -d^{-1}d_k$, $1 \leq k \leq r$. This means that c_j^A is a linear combination $c_1^A, c_2^A, \ldots, c_r^A$. Thus, $\dim\langle c_1^A, \ldots, c_n^A\rangle \leq r$. If we had $\dim\langle c_1^A, \ldots, c_r^A\rangle < r$ then it would results that each of the columns $c_1^A, \ldots, c_r^A$ is a linear combination of the other columns, hence $d = 0$, which is absurd. Thus $\dim\langle c_1^A, \ldots, c_1^A\rangle = r$. Since we also have, $\operatorname{rank} A = \operatorname{rank}\ {}^tA$ we conclude that $\dim\langle r_1^A, \ldots, r_n^A\rangle = r$. □

Corollary 4.3. a) The rank of A is equal to the maximum number of linearly independent rows (columns) of A.
b) If an $r \times r$ determinant d is nonzero, and an $(r+1) \times (r+1)$ determinant D obtained from d by adding it a row and a column is zero, then the added row (column) is a linear combination of all the other rows (columns) of D.

Remarks 4.4. a) The previous theorem is also valid for any finite dimensional vector space: *the dimension of the subspace generated by m vectors of an n-dimensional vector space ${}_KV$ is equal to the rank of the $m \times n$ matrix A whose rows are the coordinates of these vectors in a certain basis B of V.*

This can be easily shown by using the isomorphism between V and K^n which transforms B into the standard basis. Obviously, this isomorphism transforms the given m vectors into $r_1^A, \ldots, r_m^A$.
b) n vectors in an n-dimensional vector space are linearly dependent if and only if the determinant of the matrix formed with their coordinates as rows (or as columns) is zero.

4.1 The matrix of a linear map

First, we define the matrix of a vector in a basis of a vector space. For certain reasons, it is presented as a column-matrix, but it must be said that this is rather a convention than a constraint. Of course, if one changes the convention, the form of the next notions and results must be properly changed.

Definition 4.5. Let V be a K-vector space, $v \in V$ and $B = (v_1, \ldots, v_n)$ a basis of V. If $v = k_1v_1 + \cdots + k_nv_n$ $(k_1, \ldots, k_n \in K)$ is the unique writing of v as a linear combination of the vectors of the basis B, then the **matrix of the vector** v in the basis B is

$$[v]_B = \begin{pmatrix} k_1 \\ \vdots \\ k_n \end{pmatrix}$$

Definition 4.6. Let $f : V \to V'$ be a K-linear map, $B = (v_1, \ldots, v_n)$ a basis of V and $B' = (v_1', \ldots, v_m')$ a basis of V'. Then we can uniquely write the vectors in $f(B)$ as linear combinations of the vectors of the basis B', say

$$\begin{cases} f(v_1) = a_{11}v'_1 + a_{21}v'_2 + \cdots + a_{m1}v'_m \\ f(v_2) = a_{12}v'_1 + a_{22}v'_2 + \cdots + a_{m2}v'_m \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ f(v_n) = a_{1n}v'_1 + a_{2n}v'_2 + \cdots + a_{mn}v'_m \end{cases}$$

for some $a_{ij} \in K$. Then the **matrix of the K-linear map** f in the pair of bases (B, B') (or, simply, in the bases B and B') is the matrix whose columns consist of the coordinates of the vectors of $f(B)$ in the basis B', that is,

$$[f]_{BB'} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

If $V = V'$ and $B = B'$, then we simply denote $[f]_B = [f]_{BB'}$.

Remarks 4.7. (1) We complete the matrix of a linear map by columns. This is also a part of the convention we mentioned at the beginning of this section.
(2) As we will see next, the matrix of a linear map depens on the map, on the considered bases, but also by the order of the elements in each basis.

Examples 4.8. a) Consider the $\mathbb{R}$-linear map $f : \mathbb{R}^4 \to \mathbb{R}^3$ defined by

$$f(x, y, z, t) = (x + y + z, y + z + t, z + t + x)\,,\ \forall(x, y, z, t) \in \mathbb{R}^4\,.$$

Let $E = (e_1, e_2, e_3, e_4)$ and $E' = (e'_1, e'_2, e'_3)$ be the standard bases in $\mathbb{R}^4$ and $\mathbb{R}^3$ respectively. Since

$$\begin{cases} f(e_1) = f(1, 0, 0, 0) = (1, 0, 1) = e'_1 + e'_3 \\ f(e_2) = f(0, 1, 0, 0) = (1, 1, 0) = e'_1 + e'_2 \\ f(e_3) = f(0, 0, 1, 0) = (1, 1, 1) = e'_1 + e'_2 + e'_3 \\ f(e_4) = f(0, 0, 0, 1) = (0, 1, 1) = e'_2 + e'_3 \end{cases}$$

it follows that the matrix of f in the bases E and E' is

$$[f]_{EE'} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

b) Let $\mathbb{R}_n[X]$ be the $\mathbb{R}$ - vector space of the polynomials with the degree at most n and real coefficients. The map

$$\varphi : \mathbb{R}_3[X] \to \mathbb{R}_2[X],\ \varphi(a_0 + a_1X + a_2X^2 + a_3X^3) = a_1 + 2a_2X + 3a_3X^2$$

(which associates a polynomial f its formal derivative f') is a linear map. Let us write the matrix of φ in the pair of basis $B = (1, X, X^2, X^3)$, $B' = (1, X, X^2)$, and then in the pair of basis $B = (1, X, X^2, X^3)$, $B'' = (X^2, 1, X)$. We have

$$\begin{aligned}\varphi(1) &= 0\cdot 1 + 0\cdot X + 0\cdot X^2 = 0\cdot X^2 + 0\cdot 1 + 0\cdot X\\ \varphi(X) &= 1\cdot 1 + 0\cdot X + 0\cdot X^2 = 0\cdot X^2 + 1\cdot 1 + 0\cdot X\\ \varphi(X^2) &= 0\cdot 1 + 2\cdot X + 0\cdot X^2 = 0\cdot X^2 + 0\cdot 1 + 2\cdot X\\ \varphi(X^3) &= 0\cdot 1 + 0\cdot X + 3\cdot X^2 = 3\cdot X^2 + 0\cdot 1 + 0\cdot X\end{aligned}$$

thus,

$$[\varphi]_{B,B'} = \begin{pmatrix} 0 & 1 & 0 & 0\\ 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 3\end{pmatrix} \text{ and } [\varphi]_{B,B''} = \begin{pmatrix} 0 & 0 & 0 & 3\\ 0 & 1 & 0 & 0\\ 0 & 0 & 2 & 0\end{pmatrix}.$$

c) Let K be a field, $m, n \in \mathbb{N}^*$ and $A \in M_{m,n}(K)$. If E is the standard basis of K^n and E' is the standard basis of K^m, and one writes the vectors of K^n and K^m as columns, one can easily show that

$$f_A : K^n \to K^m,\ f_A(x) = Ax$$

is a linear map and $[f_A]_{E,E'} = A$.

Theorem 4.9. Let $f : V \to V'$ be a K-linear map, $B = (v_1, \ldots, v_n)$ a basis of V, $B' = (v'_1, \ldots, v'_m)$ a basis of V' and $v \in V$. Then

$$[f(v)]_{B'} = [f]_{BB'} \cdot [v]_B\,.$$

Proof. Let $[f]_{BB'} = (a_{ij}) \in M_{mn}(K)$. Let $v = \sum_{j=1}^n k_j v_j$ and $f(v) = \sum_{i=1}^m k'_i v'_i$ for some $k_i, k'_i \in K$. On the other hand, using the definition of the matrix of f in the bases B and B', we have

$$f(v) = f\Big(\sum_{j=1}^n k_j v_j\Big) = \sum_{j=1}^n k_j f(v_j) =$$

$$= \sum_{j=1}^n k_j \Big(\sum_{i=1}^m a_{ij} v'_i\Big) = \sum_{i=1}^m \Big(\sum_{j=1}^n a_{ij} k_j\Big) v'_i\,.$$

But the writing of $f(v)$ as a linear combination of the vectors of the basis B' is unique, hence we must have

$$k'_i = \sum_{j=1}^n a_{ij} k_j$$

for every $i \in \{1, \ldots, m\}$. Therefore, $[f(v)]_{B'} = [f]_{BB'} \cdot [v]_B$. □

For a K-linear map $f : V \to V'$ the dimension $\dim(\mathrm{Im} f)$ is also called **the rank of** f. We denote it by $\mathrm{rank}(f)$. The rank of a linear map and the rank of its matrix in a pair of bases are strongly connected.

Theorem 4.10. Let $f : V \to V'$ be a K-linear map. Then

$$\mathrm{rank}(f) = \mathrm{rank}[f]_{BB'}\,,$$

where B and B' are arbitrary bases of V and V' respectively.

Proof. Let $B = (v_1, \dots, v_n)$ and $[f]_{BB'} = A$. By Theorem 3.33 and Remark 4.4 a), we have

$$\mathrm{rank}(f) = \dim(\mathrm{Im} f f) = \dim f(V) = \dim f(\langle v_1, \dots, v_n \rangle) = \dim\langle f(v_1), \dots, f(v_n)\rangle =$$

$$= \mathrm{rank}(\ {}^tA) = \mathrm{rank}(A) = \mathrm{rank}[f]_{BB'}\,.$$

Now take some other bases $B_1 = (u_1, \dots, u_n)$ of V and B_1' of V' and denote $[f]_{B_1B_1'} = A_1$. It follows that

$$\mathrm{rank}([f]_{B_1B_1'}) = \mathrm{rank}(A_1) = \mathrm{rank}(\ {}^tA_1) = \dim\langle f(u_1), \dots, f(u_n)\rangle = \dim(\mathrm{Im} f f) =$$

$$= \dim\langle f(v_1), \dots, f(v_n)\rangle = \mathrm{rank}[f]_{BB'}\,.$$

□

Remark 4.11. (1) Notice that the rank of a linear map does not depend on the pair of bases in which we write its matrix.
(2) Also notice that, considering matrices of a linear map in different pairs of bases, their ranks are the same. Some other connection between matrices of a linear map in different pairs of bases will be discussed in the next part of this section.

Example 4.12. Consider the $\mathbb{R}$-linear map $f : \mathbb{R}^4 \to \mathbb{R}^3$ defined by

$$f(x, y, z, t) = (x + y + z, y + z + t, z + t + x)\,,\ \forall (x, y, z, t) \in \mathbb{R}^4\,.$$

Let $E = (e_1, e_2, e_3, e_4)$ and $E' = (e_1', e_2', e_3')$ be the canonical bases in $\mathbb{R}^4$ and $\mathbb{R}^3$ respectively. We have seen in Example 4.8 a) that $[f]_{EE'} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$. Since

$$\begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{vmatrix} = 1 \neq 0\,,$$

it follows by Theorem 4.2 that $\mathrm{rank}(f) = \mathrm{rank}[f]_{EE'} = 3\,.$

We continue this section by presenting one of the key results in Linear Algebra, connecting linear maps and matrices.

Theorem 4.13. Let V, V' and V'' be vector spaces over K with $\dim V = n$, $\dim V' = m$ and $\dim V'' = p$ and let B, B' and B'' be bases of V, V' and V'' respectively. If $f, g \in Hom_K(V, V')$, $h \in Hom_K(V', V'')$ and $k \in K$, then

$$[f + g]_{BB'} = [f]_{BB'} + [g]_{BB'}\,,\ [kf]_{BB'} = k \cdot [f]_{BB'}\,,$$

$$[h \circ f]_{BB''} = [h]_{B'B''} \cdot [f]_{BB'}\,.$$

Proof. Let us consider $[f]_{BB'} = (a_{ij}) \in M_{mn}(K)$, $[g]_{BB'} = (b_{ij}) \in M_{mn}(K)$ and $[h]_{B'B''} = (c_{ki}) \in M_{pm}(K)$. We have

$$f(v_j) = \sum_{i=1}^{m} a_{ij} v_i'\,, \quad g(v_j) = \sum_{i=1}^{m} b_{ij} v_i'\,, \quad h(v_i') = \sum_{k=1}^{p} c_{ki} v_k''$$

for any $j \in \{1, \ldots, n\}$ and for any $i \in \{1, \ldots, m\}$.

Then for any $k \in K$ and for any $j \in \{1, \ldots, n\}$ we have

$$(f+g)(v_j) = f(v_j) + g(v_j) = \sum_{i=1}^{m} a_{ij} v'_i + \sum_{i=1}^{m} b_{ij} v'_i = \sum_{i=1}^{m} (a_{ij} + b_{ij}) v'_i \,,$$

$$(kf)(v_j) = kf(v_j) = k \cdot (\sum_{i=1}^{m} a_{ij} v'_i) = \sum_{i=1}^{m} (ka_{ij}) v'_i \,,$$

hence $[f+g]_{BB'} = [f]_{BB'} + [g]_{BB'}$ and $[kf]_{BB'} = k \cdot [f]_{BB'}$.

Finally, for any $j \in \{1, \ldots, n\}$ we have

$$(h \circ f)(v_j) = h(f(v_j)) = h(\sum_{i=1}^{m} a_{ij} v'_i) = \sum_{i=1}^{m} a_{ij} h(v'_i) = \sum_{i=1}^{m} a_{ij} (\sum_{k=1}^{p} c_{ki} v''_k) =$$

$$= \sum_{k=1}^{p} \sum_{i=1}^{m} (c_{ki} a_{ij}) v''_k \,,$$

hence $[h \circ f]_{BB''} = [h]_{B'B''} \cdot [f]_{BB'}$. □

Theorem 4.14. Let V and V' be vector spaces over K with $\dim V = n$ and $\dim V' = m$ and let B and B' be bases of V and V' respectively. Then the map

$$\varphi : Hom_K(V, V') \to M_{mn}(K)$$

defined by

$$\varphi(f) = [f]_{BB'} \,, \ \forall f \in Hom_K(V, V')$$

is an isomorphism of vector spaces.

Proof. Let us prove first that φ is bijective.

Let $f, g \in Hom_K(V, V')$ such that $\varphi(f) = \varphi(g)$. Then $[f]_{BB'} = [g]_{BB'} = (a_{ij})$ and

$$f(v_j) = a_{1j} v'_1 + a_{2j} v'_2 + \cdots + a_{mj} v'_m = g(v_j) \,, \ \forall j \in \{1, \ldots, n\}.$$

Then $f = g$ by Theorem 3.48. Thus, φ is injective.

Now let $A = (a_{ij}) \in M_{mn}(K)$, seen as a list of column-vectors $(a^1, \ldots, a^n)$, where $a^j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$. Consider $B = (v_1, \ldots, v_n)$ and $B' = (v'_1, \ldots, v'_m)$ and define a K-linear map $f : V \to V'$ on the basis of the domain by

$$f(v_j) = a_{1j} v'_1 + \cdots + a_{mj} v'_m \,,$$

for any $j \in \{1, \ldots, n\}$. Then

$$\varphi(f) = [f]_{BB'} = (a_{ij}) = A \,.$$

Thus, φ is surjective.

The proof is completed by Theorem 4.13. □

Remark 4.15. The extremely important isomorphism given in Theorem 4.14 allows us to work with matrices instead of linear maps, which is much simpler from a computational point of view.

As we saw in Remark 3.36 a), $(End_K(V), +, \circ)$ is a unitary ring.

Theorem 4.16. *Let V be a vector space over K with $\dim V = n$ and let B be a basis of V. Then the map*

$$\varphi : End_K(V) \to M_n(K)$$

defined by

$$\varphi(f) = [f]_B\,,\ \forall f \in End_K(V)$$

is an isomorphism of vector spaces and of rings.

Proof. It follows by Theorem 4.13 and Theorem 4.14. □

Corollary 4.17. *Let V be a vector space over K, B is an arbitrary basis of V and $f \in End_K(V)$. Then*

$$f \in Aut_K(V) \Leftrightarrow \det[f]_B \neq 0\,.$$

Proof. By Remark 3.36 b) and Theorems 4.16, $f \in Aut_K(V)$ (i.e. f is a unit in the ring $(End_K(V), +, \circ)$) if and only if $[f]_B$ is a unit in $(M_n(K), +, \cdot)$. According to Remark 4.4 b), this means that $\det[f]_B \neq 0$. □

Definition 4.18. Let $f \in End_K(V)$ and let $B = (v_1, \dots, v_n)$ and $B' = (v'_1, \dots, v'_n)$ be bases of V. Then we can write

$$\begin{cases} v'_1 = t_{11}v_1 + t_{21}v_2 + \cdots + t_{n1}v_n \\ v'_2 = t_{12}v_1 + t_{22}v_2 + \cdots + t_{n2}v_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ v'_n = t_{1n}v_1 + t_{2n}v_2 + \cdots + t_{nn}v_n \end{cases}$$

for some $t_{ij} \in K$. Then the matrix $(t_{ij}) \in M_n(K)$, having as columns the coordinates of the vectors of the basis B' in the basis B, is called the **transition matrix from** B **to** B' and is denoted by $T_{BB'}$.

Remarks 4.19. 1) Sometimes the basis B is referred to as the "old" basis and the basis B' is referred to as the "new" basis.
2) The j-th column of $T_{BB'}$ $(j = 1, \cdots, n)$ consists of the coordinates of $v'_j = 1_V(v'_j)$ in the basis B, hence $T_{BB'} = [1_V]_{B'B}$.

Theorem 4.20. *Let $f \in End_K(V)$ and let $B = (v_1, \dots, v_n)$ and $B' = (v'_1, \dots, v'_n)$ be bases of V. Then the transition matrix $T_{BB'}$ is invertible and its inverse is the transition matrix $T_{B'B}$.*

Proof. Since $T = T_{BB'}$ is the transition matrix from the basis B to the basis B' we have

$$v'_j = \sum_{i=1}^{n} t_{ij}v_i\,,$$

for any $j \in \{1, \dots, n\}$. Denote $S = (s_{ij}) \in M_{mn}(K)$ the transition matrix from the basis B' to the basis B. Then

$$v_i = \sum_{k=1}^{n} s_{ki} v'_k \,,$$

for any $i \in \{1, \dots, n\}$. It follows that

$$v'_j = \sum_{i=1}^{n} t_{ij} (\sum_{k=1}^{n} s_{ki} v'_k) = \sum_{k=1}^{n} (\sum_{i=1}^{n} s_{ki} t_{ij}) v'_k \,.$$

By the uniqueness of writing of each v'_j as linear combination of the vectors of the basis B', it follows that

$$\sum_{i=1}^{n} s_{ki} t_{ij} = \begin{cases} 1 & \text{if } k = j \\ 0 & \text{if } k \neq j \end{cases} ,$$

that is, $S \cdot T = I_n$.

Similarly, one can show that $T \cdot S = I_n$. Thus, T is invertible and its inverse is S. □

Theorem 4.21. Let $f \in End_K(V)$, let $B = (v_1, \dots, v_n)$ and $B' = (v'_1, \dots, v'_n)$ be bases of V and let $v \in V$. Then

$$[v]_B = T_{BB'} \cdot [v]_{B'} \,.$$

Proof. Let $v \in V$ and let us write v in the two bases B and B'. Then $v = \sum_{i=1}^{n} k_i v_i$ and $v = \sum_{j=1}^{n} k'_j v'_j$ for some $k_i, k'_j \in K$. Since $T_{BB'} = (t_{ij}) \in M_n(K)$, we have

$$v'_j = \sum_{i=1}^{n} t_{ij} v_i \,,$$

for any $j \in \{1, \dots, n\}$. It follows that

$$v = \sum_{j=1}^{n} k'_j (\sum_{i=1}^{n} t_{ij} v_i) = \sum_{i=1}^{n} (\sum_{j=1}^{n} t_{ij} k'_j) v_i \,.$$

By the uniqueness of writing of v as a linear combination of the vectors of the basis B, it follows that

$$k_i = \sum_{j=1}^{n} t_{ij} k'_j \,,$$

hence $[v]_B = T_{BB'} \cdot [v]_{B'}$. □

Remark 4.22. Usually, we are interested in computing the coordinates of a vector v in the new basis B', knowing the coordinates of the same vector v in the old basis B and the transition matrix from B to B'. Then by Theorem 4.21, we have

$$[v]_{B'} = T_{BB'}^{-1} \cdot [v]_B = T_{B'B} \cdot [v]_B \,.$$

Example 4.23. Consider the bases $E = (e_1, e_2, e_3)$ and $B = (v_1, v_2, v_3)$ of the canonical real vector space $\mathbb{R}^3$, where E is the canonical basis and $v_1 = (0, 1, 1)$, $v_2 = (1, 1, 2)$, $v_3 = (1, 1, 1)$. Let us determine the transition matrices from E to B and viceversa.

Since

$$\begin{cases} v_1 = \phantom{e_1 + {}} e_2 + e_3 \\ v_2 = e_1 + e_2 + 2e_3 \\ v_3 = e_1 + e_2 + e_3 \end{cases}$$

it follows that

$$T_{EB} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix}.$$

Further, we get

$$\begin{cases} e_1 = -v_1 \phantom{{}- v_2} + v_3 \\ e_2 = v_1 - v_2 + v_3 \\ e_3 = \phantom{v_1 - {}} v_2 - v_3 \end{cases}$$

hence

$$T_{BE} = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}.$$

Recall that we must have $T_{BE} = T_{EB}^{-1}$, so that we could have obtained T_{BE} by computing the inverse of the matrix T_{EB}.

Let us consider now the vector $u = (1, 2, 3)$. Clearly, its coordinates in the canonical basis E are 1, 2 and 3. By Theorem 4.21, it follows that

$$[u]_B = T_{BE} \cdot [u]_E = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Hence the coordinates of u in the basis B are 1, 1 and 0.

Theorem 4.24. Let $f \in End_K(V)$ and let B and B' be bases of V. Then

$$[f]_{B'} = T_{BB'}^{-1} \cdot [f]_B \cdot T_{BB'}\,.$$

Proof. Let us denote $T = T_{BB'}$. For every $v \in V$, by Theorems 4.9 and 4.21, we have

$$[f(v)]_B = [f]_B \cdot [v]_B = [f]_B \cdot T \cdot [v]_{B'}\,.$$

We also have

$$[f(v)]_B = T \cdot [f(v)]_{B'} = T \cdot [f]_{B'} \cdot [v]_{B'}\,.$$

Then the equality

$$[f]_B \cdot T \cdot [v]_{B'} = T \cdot [f]_{B'} \cdot [v]_{B'}$$

yields two ways of writing the vector v as linear combinations of the vectors of the basis B'. Since we must have the equality of the corresponding scalars, $[f]_B \cdot T = T \cdot [f]_{B'}$. Therefore, $[f]_{B'} = T^{-1} \cdot [f]_B \cdot T$. □

Example 4.25. Consider the bases $E = (e_1, e_2, e_3)$ and $B = (v_1, v_2, v_3)$ of the canonical real vector space $\mathbb{R}^3$, where E is the canonical basis and $v_1 = (0, 1, 1)$, $v_2 = (1, 1, 2)$, $v_3 = (1, 1, 1)$. Also let $f \in End_{\mathbb{R}}(\mathbb{R}^3)$ be defined by

$$f(x, y, z) = (x + y, y - z, z + x)\,,\ \forall (x, y, z) \in \mathbb{R}^3\,.$$

Let us determine the matrix of f in the basis E and in the basis B.

Since

$$\begin{cases} f(e_1) = (1, 0, 1) = e_1 + e_3 \\ f(e_2) = (1, 1, 0) = e_1 + e_2 \\ f(e_3) = (0, -1, 1) = -e_2 + e_3 \end{cases}$$

we get $[f]_E = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix}$. Using Theorem 4.24 and the transition matrices T_{EB} and T_{BE}, that we have determined in Example 4.23, we have

$$[f]_B = T_{EB}^{-1} \cdot [f]_E \cdot T_{EB} = T_{BE} \cdot [f]_E \cdot T_{EB} =$$

$$= \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -3 & -2 \\ 1 & 4 & 2 \\ 0 & -2 & 0 \end{pmatrix}.$$

It is worth to be mentioned that we could have reached the same result using the definition of the matrix of a linear map and expressing the vectors $f(v_1)$, $f(v_2)$ and $f(v_3)$ as linear combinations of the vectors v_1, v_2 and v_3 of the basis B.

Remark 4.26. It is possible to establish a more general result than Theorem 4.24, namely to consider linear maps between different vector spaces and to take two bases in each of the vector spaces. Thus, we have the following theorem whose proof gives the reader another way to approach Theorem 4.24.

Theorem 4.27. Let $f \in Hom_K(V, V')$, let B_1 and B_2 be bases of V and let B'_1 and B'_2 be bases of V'. Then

$$[f]_{B_2 B'_2} = T_{B'_1 B'_2}^{-1} \cdot [f]_{B_1 B'_1} \cdot T_{B_1 B_2}\,.$$

Proof. As in Remark 4.19 2), $T_{B_1 B_2} = [1_V]_{B_2 B_1}$ and $T_{B'_1 B'_2} = [1_{V'}]_{B'_2 B'_1}$. Of course, $T_{B'_1 B'_2}^{-1} = [1_{V'}]_{B'_1 B'_2}$. Applying Theorem 4.13 to the equality $f = 1_{V'} \circ f \circ 1_V$, we have

$$[f]_{B_2 B'_2} = [1_{V'}]_{B'_1 B'_2} \cdot [f]_{B_1 B'_1} \cdot [1_V]_{B_2 B_1},$$

hence the expected conclusion. □

4.2 Exercises with solution

1) Let $B = ((1, 2), (-2, 1))$ and $B' = ((1, -1, 0), (-1, 0, 1), (1, 1, 1))$. Show that B, and B' are bases in the $\mathbb{R}$-vector spaces $\mathbb{R}^2$ and $\mathbb{R}^3$, respectively, and determine the matrix of the linear map $f : \mathbb{R}^2 \to \mathbb{R}^3$, $f(x, y) = (x + y, 2x - y, 3x + 2y)$ in the pair of bases (B, B').

Solution: Since the rank of the matrix formed with the pairs from B is 2, and the rank of the matrix formed with the vectors of B' is 3, B is a basis of $\mathbb{R}^2$ and B' is a basis of $\mathbb{R}^3$. The columns of the matrix $[f]_{B,B'} = (a_{ij}) \in M_{3,2}(\mathbb{R})$ are given by the equalities

$$\begin{aligned} (3,0,7) = f(1,2) &= a_{11}(1,-1,0) + a_{21}(-1,0,1) + a_{31}(1,1,1), \\ (-1,-5,-4) = f(-2,1) &= a_{12}(1,-1,0) + a_{22}(-1,0,1) + a_{32}(1,1,1), \end{aligned}$$

hence by the systems

$$\begin{cases} a_{11} - a_{21} + a_{31} = 3 \\ -a_{11} \quad\quad + a_{31} = 0 \\ \quad\quad a_{21} + a_{31} = 7 \end{cases} \text{ and } \begin{cases} a_{12} - a_{22} + a_{32} = -1 \\ -a_{12} \quad\quad + a_{32} = -5 \\ \quad\quad a_{22} + a_{32} = -4 \end{cases}$$

which have the solutions $\left(\frac{10}{3}, \frac{11}{3}, \frac{10}{3}\right)$ and $\left(\frac{5}{3}, -\frac{2}{3}, -\frac{10}{3}\right)$, respectively. Thus,

$$[f]_{B,B'} = \begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ \frac{11}{3} & -\frac{2}{3} \\ \frac{10}{3} & -\frac{10}{3} \end{pmatrix}.$$

Another solution: The transition matrix from the standard basis E' of $\mathbb{R}^3$ to B' is $T = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, and the matrix of f in the bases B, E' is

$$[f]_{B,E'} = \begin{pmatrix} 3 & -1 \\ 0 & -5 \\ 7 & -4 \end{pmatrix},$$

(its columns are the coordinates of $f(1,2)$ and $f(-2,1)$ in the standard basis baza E', i.e. $f(1,2)$ and $f(-2,1)$) hence,

$$[f]_{B,B'} = T^{-1}[f]_{B,E'} = \begin{pmatrix} \frac{10}{3} & \frac{5}{3} \\ \frac{11}{3} & -\frac{2}{3} \\ \frac{10}{3} & -\frac{10}{3} \end{pmatrix}.$$

2) Let $f : \mathbb{R}^3 \to \mathbb{R}^4$ be the R-linear map defined on the standard basis as follows:

$$f(e_1) = (1,2,3,4),\ f(e_2) = (4,3,2,1),\ f(e_3) = (-2,1,4,1).$$

Determine:
i) $f(v)$ when $v \in \mathbb{R}^3$;
ii) the matrix of f in the standard bases;
iii) a basis for each of the $\mathbb{R}$-spaces $\operatorname{Im} f$ and $\operatorname{Ker} f$.

Solution: i) $f(x_1,x_2,x_3) = x_1 f(e_1) + x_2 f(e_2) + x_3 f(e_3)$.

ii) The matrix of f in the standard bases is the matrix whose columns are $f(e_1)$, $f(e_2)$ and $f(e_3)$, respectively, i.e.

$$\begin{pmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{pmatrix}.$$

iii) $\operatorname{Im} f = f(\langle e_1, e_2, e_3 \rangle) = \langle f(e_1), f(e_2), f(e_3) \rangle$, so,

$$\dim(\operatorname{Im} f) = \operatorname{rank} \begin{pmatrix} 1 & 4 & -2 \\ 2 & 3 & 1 \\ 3 & 2 & 4 \\ 4 & 1 & 1 \end{pmatrix} = 3,$$

therefore $f(e_1)$, $f(e_2)$ and $f(e_3)$ form a basis in $\operatorname{Im} f$. Then

$$\dim(\operatorname{Ker} f) = \dim \mathbb{R}^3 - \dim(\operatorname{Im} f) = 3 - 3 = 0,$$

hence $\operatorname{Ker} f = \{(0,0,0)\}$ and $\emptyset$ is a basis in $\operatorname{Ker} f$.

3) Let V, V' be $\mathbb{R}$-vector spaces, $B = (v_1, v_2, v_3)$ be a basis in V, $B' = (v_1', v_2', v_3')$ be a basis in V' and $f : V \to V'$ be the linear map for which

$$[f]_{B,B'} = \begin{pmatrix} 0 & -1 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{pmatrix}.$$

Determine:
i) the dimension and a basis for each of the spaces $\operatorname{Im} f$ and $\operatorname{Ker} f$;
ii) $[f]_{B,E'}$ when $V' = \mathbb{R}^3$, $v_1' = (1,0,0)$, $v_2' = (0,1,1)$, $v_3' = (0,0,1)$ and E' is the standard basis of $\mathbb{R}^3$;
iii) $f(x)$ for $x = 2v_1 - v_2 + 3v_3$, under the circumstances of ii).

Solution: i) We remind that the columns of $[f]_{B,B'}$ give us the coordinates of the vectors $f(v_1)$, $f(v_2)$ and $f(v_3)$, respectively in B', i.e.

$$f(v_1) = v_2',\ f(v_2) = -v_1' + v_3' \text{ and } f(v_3) = 5v_1' - 5v_3'.$$

Then $\dim(\operatorname{Im} f) = \operatorname{rank}[f]_{B,B'} = 2$, and a 2×2 minor of $[f]_{B,B'}$ can be taken from the first 2 columns (and the first 2 rows), therefore $f(v_1)$ and $f(v_2)$ form a basis in $\operatorname{Im} f$. Furthermore,

$$\dim(\operatorname{Ker} f) = \dim V - \dim(\operatorname{Im} f) = 3 - 2 = 1,$$

and, since the columns 2 and 3 of $[f]_{B,B'}$ are proportional, we have

$$f(v_3) = -5f(v_2) \Leftrightarrow f(v_3 - 5v_2) = 0 \Leftrightarrow v_3 - 5v_2 \in \operatorname{Ker} f.$$

Thus $v_3 - 5v_2$ forms a basis in $\operatorname{Ker} f$.
ii) The transition matrix T from the standard basis E' to B' is the matrix whose columns are $v_1',\ v_2',\ v_3'$, and

$$[f]_{B,B'} = T^{-1}\,[f]_{B,E'} \ \Leftrightarrow\ [f]_{B,E'} = T\,[f]_{B,B'}.$$

iii) Since the columns of $[f]_{B,E'}$ contain the coordinates of $f(v_1)$, $f(v_2)$, $f(v_3)$ in the standard basis E', they will be exactly the vectors $f(v_1)$, $f(v_2)$, $f(v_3)$ of $\mathbb{R}^3$, and

$$f(x) = f(2v_1 - v_2 + 3v_3) = 2f(v_1) - f(v_2) + 3f(v_3).$$

We recommend the reader to complete the solution with the missing computations.

4) Let $f \in End_{\mathbb{Q}}(\mathbb{Q}^4)$ with the matrix in the standard basis

$$\begin{pmatrix} 1 & 2 & 1 & 2 \\ 3 & 2 & 3 & 2 \\ -1 & -3 & 0 & 4 \\ 0 & 4 & -1 & -3 \end{pmatrix}.$$

Find a basis and the dimension for each of the $\mathbb{Q}$-spaces $\operatorname{Ker} f$ and $\operatorname{Im} f$.

Solution: Let $E = (e_1, e_2, e_3, e_4)$ be the standard basis of ${}_{\mathbb{Q}}\mathbb{Q}^4$. The given matrix is $[f]_E$ and its columns are $f(e_1)$, $f(e_2)$, $f(e_3)$, $f(e_4)$. For finding a basis and the dimension of $\operatorname{Im} f$ we compute the rank of $[f]_E$, carefully watching from which columns we "cut" a nonzero minor which gives us $\operatorname{rank}[f]_E$. We find that $\dim(\operatorname{Im} f) = 3$ and a possibility for a 3×3 nonzero minor is to take the first 3 rows and the first 3 columns. So, $(f(e_1), f(e_2), f(e_3))$ is a basis of $\operatorname{Im} f$ and $\dim(\operatorname{Ker} f) = 4 - 3 = 1$. For finding a basis for $\operatorname{Ker} f$ we can notice that $7(c_1 - c_3) = c_2 - c_4$ (c_i denotes the i-th column of $[f]_E$, i.e. $f(e_i)$) and we continue as in the previous exercise, or we can use Theorem 4.9 as follows:

$$(x_1, x_2, x_3, x_4) \in \operatorname{Ker} f \Leftrightarrow [f]_e \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Leftrightarrow \begin{cases} x_1 + 2x_2 + x_3 + 2x_4 = 0 \\ 3x_1 + 2x_2 + 3x_3 + 2x_4 = 0 \\ -x_1 - 3x_2 \qquad + 4x_4 = 0 \\ \qquad +4x_2 - x_3 - 3x_4 = 0 \end{cases}.$$

The solution set of this system is

$$\{(7\alpha, -\alpha, -7\alpha, \alpha) \in \mathbb{Q}^4 \mid \alpha \in \mathbb{Q}\} = \{\alpha(7, -1, -7, 1) \mid \alpha \in \mathbb{Q}\} = \langle (7, -1, -7, 1) \rangle,$$

hence the vector $(7, -1, -7, 1)$ is a linearly independent (i.e. nonzero) generator of $\operatorname{Ker} f$, thus it forms a basis of $\operatorname{Ker} f$.

4.3 Systems of linear equations

Let K be a field. A **system of m linear equations with n unknowns** $x_1, \dots, x_n$ is

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \qquad (S)$$

where $a_{ij}, b_i \in K$ ($i = 1, \dots, m$, $j = 1, \dots, n$). The elements $a_{ij} \in K$ ($i = 1, \dots, m$, $j = 1, \dots, n$) are called **coefficients** and $b_i \in K$ ($j = 1, \dots, n$) are called **constant terms**.

The matrix $A = (a_{ij}) \in M_{mn}(K)$ is called the **matrix of the system** (S). Let us denote $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$. Then the system (S) can also be written:

$$A \cdot x = b \tag{S}$$

The matrix

$$\bar{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

is called the **augmented matrix of the system** (S).

By Theorem 4.14, there exists a bijective correspondence between K-linear maps and matrices. Thus, since $A \in M_{mn}(K)$, there exists $f_A \in Hom_K(K^n, K^m)$ such that $[f_A]_{EE'} = A$, where E and E' are the standard bases in K^n and K^m, respectively (see Remark 4.8 c)). If one considers $x \in K^n$ and $b \in K^m$, by Theorem 4.9, we have

$$[f_A(x)]_{E'} = [f_A]_{EE'} \cdot [x]_E = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = [b]_E \,.$$

It follows that $f_A(x) = b$. Thus, the system (S) can be written as:

$$f_A(x) = b \tag{S}$$

Remarks 4.28. (1) Thus, for a linear system of equations we have three equivalent forms, namely: the classical one with coefficients and unknowns, the one using matrices and the one using the corresponding linear map.
(2) We have denoted by x and b first column-matrices and then row-matrices to get nicer results, without using any transposed matrices.

Definition 4.29. An element $x^0 \in M_{n1}(K)$ ($x^0 \in K^n$) is called a **solution** of (S) if

$$A \cdot x^0 = b \quad \text{(or, equivalently, } f_A(x^0) = b) \,.$$

The system (S) is called **consistent** if it has at least one solution. Otherwise, the system (S) is **inconsistent**. Two **systems** of linear equations with n unknowns are **equivalent** if they have the same solution set.

If $b = 0$, then the system (S) is called a **homogeneous system of linear equations** and it has the following three equivalent forms:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = 0 \end{cases} \tag{S_0}$$

$$A \cdot x = 0 \tag{S_0}$$

$$f_A(x) = 0 \tag{S_0}$$

Denote the solution sets of (S) and (S_0) by

$$S = \{x^0 \in M_{n1}(K) \mid A \cdot x^0 = b\} = \{x^0 \in K^n \mid f_A(x^0) = b\}\,,$$

$$S_0 = \{x^0 \in M_{n1}(K) \mid A \cdot x^0 = 0\} = \{x^0 \in K^n \mid f_A(x^0) = 0\}\,.$$

Theorem 4.30. The solution set S_0 of the homogeneous linear system of equations (S_0) is a subspace of the canonical vector space K^n over K and

$$\dim S_0 = n - \operatorname{rank}(A)\,.$$

Proof. Since

$$S_0 = \{x^0 \in K^n \mid f_A(x^0) = 0\} = \operatorname{Ker} f_A$$

and the kernel of a linear map is always a subspace of the domain vector space, it follows that $S_0 \leq K^n$. Now by Theorems 3.66 and 4.10, it follows that

$$\dim S_0 = \dim(\operatorname{Ker} f_A) = \dim K^n - \dim(\operatorname{Imf} f_A) = n - \operatorname{rank}(f_A) = n - \operatorname{rank}(A)\,.$$

□

Remark 4.31. If $(c^1, \dots, c^l)$ is a basis of the subspace S_0, then every $x \in S_0$ can be uniquely written as

$$x = k_1 c^1 + \cdots + k_l c^l$$

for some $k_1, \dots, k_l \in K$.

Theorem 4.32. If $x^1 \in S$ is a particular solution of the system (S), then

$$S = x^1 + S_0 = \{x^1 + x^0 \mid x^0 \in S_0\}\,.$$

Proof. Since $x^1 \in S$, we have $Ax^1 = b$.

First, let $x^2 \in S$. Then

$$Ax^2 = b \Rightarrow Ax^2 = Ax^1 \Rightarrow A(x^2 - x^1) = 0 \Rightarrow x^2 - x^1 \in S_0 \Rightarrow x^2 \in x^1 + S_0\,.$$

Conversely, let $x^2 \in x^1 + S_0$. Then there exists $x^0 \in S_0$ such that $x^2 = x^1 + x^0$. It follows that $Ax^2 = A(x^1 + x^0) = Ax^1 + Ax^0 = b + 0 = b$ and consequently $x^2 \in S$.

Therefore, $S = x^1 + S_0$. □

Remarks 4.33. (1) By Theorem 4.32, if x^1 is a (particular) solution of (S), then every $x \in S$ can be uniquely written as

$$x = x^1 + k_1 c^1 + \cdots + k_l c^l$$

for some $k_1, \dots, k_l \in K$. This is called the *general solution* of the system (S).
(2) By Theorem 4.32, the general solution of the system (S) can be obtained by knowing the general solution of the homogeneous system (S_0) and a particular solution of (S).

Next, we are going to see when a linear system of equations has a solution.

Remarks 4.34. (1) The system (S) is consistent if and only if $b \in \mathrm{Im} f_A$.
(2) Any homogeneous linear system of equations is consistent, having at least the zero (trivial) solution.

Theorem 4.35. The system (S_0) has a non-zero solution if and only if $\mathrm{rank}(A) < n$.

Proof. By Theorem 4.30, we have

$$S_0 = \mathrm{Ker} f_A \neq \{0\} \Leftrightarrow \dim S_0 \neq 0 \Leftrightarrow n - \mathrm{rank}(A) \neq 0 \Leftrightarrow \mathrm{rank}(A) < n\,.$$

□

Corollary 4.36. If $A \in M_n(K)$, then

$$S_0 = \{0\} \Leftrightarrow \mathrm{rank}(A) = n \Leftrightarrow \det(A) \neq 0\,.$$

Definition 4.37. If $A \in M_n(K)$ and $\det(A) \neq 0$, then the system (S) is called a **Cramer system**.

So, Cramer system is a system

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n = b_n \end{cases}$$

with $A = (a_{ij}) \in M_n(K)$, $b_1, \dots, b_n \in K$ and $d = \det(A) \neq 0$

Theorem 4.38. A Cramer system has a unique solution. This solution is given by the so called **Cramer's rule** (or **Cramer's formulas**) which says that if d_j is the determinant obtained from d by replacing its j-th column by b (the column of constant terms), then

$$\begin{cases} x_1 = d_1 \cdot d^{-1} \\ x_2 = d_2 \cdot d^{-1} \\ \vdots \\ x_n = d_n \cdot d^{-1} \end{cases}$$

Proof. The matrix of a Cramer system is an invertible matrix $A \in M_n(K)$. Then we deduce that $x = A^{-1}b$ is the unique solution. More precisely,

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A^{-1} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = d^{-1} \cdot A^* \cdot \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = d^{-1} \cdot \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix},$$

which leads us to the expected formulas. □

Corollary 4.39. A homogeneous Cramer system has only the zero solution.

As for the consistency of the general linear systems, we have the following result.

Theorem 4.40. (Kronecker-Capelli) The linear system (S) is consistent if and only if $\operatorname{rank}(\bar{A}) = \operatorname{rank}(A)$.

Proof. Let $(e_1, \ldots, e_n)$ be the standard basis of the canonical vector space K^n over K and denote by $a^1, \ldots, a^n$ the columns of the matrix A. Then using Theorem 4.4, we have

$$(S) \text{ is consistent } \Leftrightarrow \exists x^0 \in K^n : \ f_A(x^0) = b \Leftrightarrow b \in \operatorname{Im} f_A \Leftrightarrow b \in f_A(\langle e_1, \ldots, e_n \rangle) \Leftrightarrow$$

$$\Leftrightarrow b \in \langle f_A(e_1), \ldots, f_A(e_n) \rangle \Leftrightarrow b \in \langle a^1, \ldots, a^n \rangle \Leftrightarrow \langle a^1, \ldots, a^n, b \rangle = \langle a^1, \ldots, a^n \rangle \Leftrightarrow$$

$$\Leftrightarrow \dim \langle a^1, \ldots, a^n, b \rangle = \dim \langle a^1, \ldots, a^n \rangle \Leftrightarrow \operatorname{rank}(\bar{A}) = \operatorname{rank}(A)\,.$$

□

Let us consider that $\operatorname{rank}(A) = r$. Based on how one can determine the rank of a matrix one can restate the previous theorem as follows:

Theorem 4.41. (Rouché) Let d_p be a nonzero $r \times r$ minor of the matrix A. The system (S) is consistent if and only if all the $(r+1) \times (r+1)$ minors of $\overline{A}$ obtained by completing d_p with a column of constant terms and the corresponding row are zero (if such $(r+1) \times (r+1)$ minors exist).

We call the unknowns corresponding to the the entries of d_p **main unknowns** and the other unknowns **side unknowns**.

We end this section by presenting two algorithms for solving arbitrary systems of linear equations.

1. Based on Rouché Theorem. We use the notations from Rouché Theorem.

Let us consider that we have the minor d_p of A. For simplicity reasons, we consider that this minor was "cut" from the first r rows and the first r columns of A. If one finds a nonzero $(r+1) \times (r+1)$ minor which completes d_p as in Rouché Theorem, then (S) is inconsistent and the algorithm ends. If $r = m$ or all the Rouché Theorem $(r+1) \times (r+1)$ minor completions of d_p are 0, then (S) is consistent. One considers only the r equations which determined the rows of d_p. Since $\operatorname{rank} \overline{A} = \operatorname{rank} A = r$, Corollary 4.3 b) tells us that all the other equations are linear combinations" of these r equations, hence S is equivalent to

$$\begin{cases} a_{11}x_1 + x_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + x_{22}x_2 + \cdots + a_{2n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{r1}x_1 + x_{r2}x_2 + \cdots + a_{rn}x_n = b_r \end{cases} \tag{$*$}$$

If $n = r$, i.e. all the unknowns are main unknowns, then $(*)$ is a Cramer system. The Cramer's rule gives us its unique solution, hence the unique solution of (S).

Otherwise, $n > r$, and $x_{r+1}, \ldots, x_n$ are side unknowns. We can assign them arbitrary "values" from K $\alpha_{r+1}, \ldots, \alpha_n$, respectively. Then $(*)$ becomes

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r = b_1 - a_{1,r+1}\alpha_{r+1} - \cdots - a_{1n}\alpha_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2r}x_r = b_2 - a_{2,r+1}\alpha_{r+1} - \cdots - a_{2n}\alpha_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rr}x_r = b_r - a_{r,r+1}\alpha_{r+1} - \cdots - a_{rn}\alpha_n \end{cases} \tag{$**$}$$

The determinant of the matrix of $(**)$ is $d_p \neq 0$, hence we can express the main unknowns using the side unknowns, by solving the Cramer system $(**)$.

2. Gaussian elimination provides us with an algorithm for studying the consistency of a linear system (S) as well as for solving it. It is based on the fact that certain elementary operations on the equations of (S) (or, more precisely, on the matrix $\overline{A}$) lead us to equivalent systems.

By an **elementary operation on the rows (columns)** of a matrix we understand one of the following:

(1) the interchange of two rows (columns).

(2) multiplying a row (column) by a non-zero element from K.

(3) multiplying a row (column) by an element from K and adding the result to another row (column).

The purpose is to successively use elementary operations on the rows of the augmented matrix $\overline{A}$ of (S) in order to bring it to an echelon form B. This procedure corresponds to a partial elimination of some unknowns to get an equivalent system which can be easier solved. If we manage to do this, then B is the augmented matrix of such an equivalent system.

A matrix $A \in M_{mn}(K)$ is in an **echelon form** with $r \geq 1$ non-zero rows if:

(1) the rows $1, \ldots, r$ are non-zero and the rows $r+1, \ldots, m$ consists only of 0;

(2) if $N(i)$ is the number of zeros at the beginning of the row i ($i \in \{1, \ldots, r\}$), then

$$0 \leq N(1) < N(2) < \cdots < N(r)\,.$$

An r non-zero rows echelon form with $N(i) = i - 1$, for any $i \in \{1, \ldots, r\}$ is called **trapezoidal form**.

As we will see in the solution of Exercise (with solution) 2), one can easily work very well with the echelon form for solving a linear system. Yet, if we manage to get to a trapezoidal form, some information on the given system can be easily red from this. E.g. the rank of $\overline{A}$ is (the rank of B which is) the number of the nonzero elements on the diagonal of B and these nonzero elements on the diagonal of B provide us with the main unknowns. Yet, finding the trapezoidal form is not always possible by using only row elementary operations (see, again, Exercise (with solution) 2)). Sometimes, we have to interchange two columns of the firs n columns, hence columns corresponding to the matrix of a certain equivalent system. This is, obviously, allowed since this means that we commute the two corresponding terms in each equation of this system.

If, during this algorithm, one can find a row for which all the elements are 0, except for the last one, which is $a \in K^*$, then (S) is inconsistent since it is equivalent to a system which contains the equality $0 = a$ which is not possible. Otherwise, B gives us an equivalent system of the form

$$\begin{cases} a'_{11}x_1 + a'_{12}x_2 + \cdots + a'_{1,r-1}x_r + a'_{1r}x_r + a'_{1,r+1}x_{r+1} + \cdots + a'_{1n}x_n = b'_1 \\ \qquad a'_{22}x_2 + \cdots + a'_{2,r-1}x_r + a'_{2r}x_r + a'_{2,r+1}x_{r+1} + \cdots + a'_{2n}x_n = b'_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \qquad\qquad a'_{r-1,r-1}x_{r-1} + a'_{r-1,r}x_r + a'_{r-1,r+1}x_{r+1} + \cdots + a'_{r-1,n}x_n = b'_{r-1} \\ \qquad\qquad\qquad a'_{rr}x_r + a'_{r,r+1}x_{r+1} + \cdots + a'_{rn}x_n = b'_r \end{cases}$$

(possibly with the unknowns succeeding in a different way, not as in (S), if we permuted columns) The main unknowns $x_1, \dots, x_r$ can be easily computed starting from the last equation of this system.

4.4 Exercises with solution

1) Solve in $\mathbb{R}^3$ the following system

$$\begin{cases} x_1 + x_2 + 2x_3 = -1 \\ 2x_1 - x_2 + 2x_3 = -4 \\ 4x_1 + x_2 + 4x_3 = -2. \end{cases}$$

Solution: **I) ... using Gaussian elimination:**
The augmented matrix of the system is

$$\overline{A} = \left(\begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 2 & -1 & 2 & -4 \\ 4 & 1 & 4 & -2 \end{array}\right)$$

Subtracting row 2 from row 1 multiplied by 2, fact denoted by $r_2 - 2r_1$, and subtracting from row 3 row 1 multiplied by 4 we get the matrix

$$\overline{A}_1 = \left(\begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 0 & -3 & -2 & -2 \\ 0 & -3 & -4 & 2 \end{array}\right)$$

The row operation $r_3 - r_2$ leads us to the echelon form:

$$\overline{A}_2 = \left(\begin{array}{ccc|c} 1 & 1 & 2 & -1 \\ 0 & -3 & -2 & -2 \\ 0 & 0 & -2 & 4 \end{array}\right)$$

Hence the given system is equivalent to

$$\begin{cases} x_1 & +x_2 & +2x_3 & = -1 \\ & -3x_2 & -2x_3 & = -2 \\ & & -2x_3 & = 4 \end{cases}$$

Thus the given system has a unique solution; the last equation leads us to $x_3 = -2$, the second to $x_2 = 2$, and the first to $x_1 = 1$. So, the solution is $(1, 2, -2)$.

If in $\overline{A}_2$ we continue the row operations as follows

$$\overline{A}_2 \underset{r_1+r_3}{\overset{r_2-r_3}{\sim}} \begin{pmatrix} 1 & 1 & 0 & 3 \\ 0 & -3 & 0 & -6 \\ 0 & 0 & -2 & 4 \end{pmatrix} \overset{r_1+\frac{1}{3}r_2}{\sim} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & -3 & 0 & -6 \\ 0 & 0 & -2 & 4 \end{pmatrix}$$

one says that we used **Gauss-Jordan elimination**. This gives us the equivalent system:

$$\begin{cases} x_1 = 1 \\ -3x_2 = -6 \\ -2x_3 = 4 \end{cases}$$

The solution results right away.

II) ... using Rouché Theorem:

The systems matrix determinant is

$$\begin{vmatrix} 1 & 1 & 2 \\ 2 & -1 & 2 \\ 4 & 1 & 4 \end{vmatrix} = 6.$$

So, we are dealing with a Cramer system. Hence, the system is consistent, it has a unique solution, and this solution is given by Cramer's formulas. We let the reader find the solution this way.

2) Solve in $\mathbb{R}^4$ the system

$$\begin{cases} 3x_1 + 4x_2 + x_3 + 2x_4 = 3 \\ 6x_1 + 8x_2 + 2x_3 + 5x_4 = 7 \\ 9x_1 + 12x_2 + 3x_3 + 10x_4 = 13 \end{cases}$$

Solution: **I) ... using Gaussian elimination:**

We write the augmented matrix and we apply the mentioned elementary operations

$$\overline{A} = \left(\begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 6 & 8 & 2 & 5 & 7 \\ 9 & 12 & 3 & 10 & 13 \end{array}\right) \underset{r_3-3r_1}{\overset{r_2-2r_1}{\sim}} \left(\begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 4 & 4 \end{array}\right)$$

$$\overset{r_3-4r_2}{\sim} \left(\begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

This shows that the given system is equivalent to

$$\begin{cases} 3x_1 + 4x_2 + x_3 \quad +2x_4 \quad = 3 \\ \qquad\qquad\qquad\qquad x_4 \quad = 1 \end{cases}$$

Here, x_1, x_4 are main unknowns and the solution set is:

$$\left(\frac{1}{3}(1 - 4\alpha - \beta), \alpha, \beta, 1\right) \text{ cu } \alpha, \beta \in \mathbb{R}.$$

Remark: If one wants to continue the algorithm in order to obtain a trapezoidal form, one has to permute columns. E.g., permutinc c_2 and c_4 we get the trapezoidal form

$$\left(\begin{array}{cccc|c} 3 & 4 & 1 & 2 & 3 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Consequently, when we write the corresponding equivalent system, the unknowns succession (in each equation) is x_1, x_4, x_3, x_2, hence the system appears as follows

$$\begin{cases} 3x_1 \quad +2x_4 \quad +x_3 + 4x_2 = 3 \\ \qquad\quad x_4 \qquad\qquad\quad = 1 \end{cases}$$

One can easily notice that this system is consistent and it is to find its solution set.

II) ... using Rouché Theorem: We have

$$\begin{vmatrix} 1 & 2 \\ 2 & 5 \end{vmatrix} = 1 \text{ and } \begin{vmatrix} 3 & 1 & 2 \\ 6 & 2 & 5 \\ 9 & 3 & 10 \end{vmatrix} = \begin{vmatrix} 4 & 1 & 2 \\ 8 & 2 & 5 \\ 12 & 3 & 10 \end{vmatrix} = 0$$

(since $c{+}1 = 4c_2$). Therefore, we can consider $d_p = \begin{vmatrix} 1 & 2 \\ 2 & 5 \end{vmatrix}$. We can uniquely complete it with a constant terms column $\begin{vmatrix} 1 & 2 & 3 \\ 2 & 5 & 7 \\ 3 & 10 & 13 \end{vmatrix}$ and this determinant is 0 since column 3 is the sum of the first two columns. Thus the system is consistent, and it is equivalent to

$$\begin{cases} x_3 + 2x_4 = 3 - 3x_1 - 4x_2 \\ 2x_3 + 5x_4 = 7 - 6x_1 - 8x_2 \end{cases}$$

Here x_1, x_2 are side unknowns. We consider them parameters, and finding x_3 and x_4 from the above system is now an easy exercise.

3) Solve in $\mathbb{R}^3$ the system

$$\begin{cases} x_1 + x_2 - 3x_3 = -1 \\ 2x_1 + x_2 - 2x_3 = 1 \\ x_1 + x_2 + x_3 = 3 \\ x_1 + 2x_2 - 3x_3 = 1 \end{cases}$$

Solution: **I) ... using Gaussian elimination:**

$$\overline{A} = \left(\begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 2 & 1 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 2 & -3 & 1 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 1 & 0 & 2 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 4 & 5 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & -3 & -1 \\ 0 & -1 & 4 & 3 \\ 0 & 0 & 4 & 4 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

The last row leads us to $0 \cdot x_4 = 1$, which is absurd. Thus the system is inconsistent.

II) ... using Rouché Theorem:

Avem $d_p = \begin{vmatrix} 1 & 1 & -3 \\ 2 & 1 & -2 \\ 1 & 1 & 1 \end{vmatrix} = -4 \neq 0$; the unique way to complete it with a constant terms column is $\begin{vmatrix} 1 & 1 & -3 & -1 \\ 2 & 1 & -2 & 1 \\ 1 & 1 & 1 & 3 \\ 1 & 2 & -3 & 1 \end{vmatrix} = -4$ which is not zero, hence the system is inconsistent.

4) Discuss on the real parameter α the consistency of the following system in $\mathbb{R}^4$, then

solve it:

$$\left\{\begin{array}{l} 2x_1 - \ \ x_2 + 3x_3 + \ \ 4x_4 = \ \ 5 \\ 4x_1 - 2x_2 + 5x_3 + \ \ 6x_4 = \ \ 7 \\ 6x_1 - 3x_2 + 7x_3 + \ \ 8x_4 = \ \ 9 \\ \alpha x_1 - 4x_2 + 9x_3 + 10x_4 = 11 \end{array}\right. .$$

Solution: **I) ... using Gaussian elimination:**
Starting with the augmented matrix we successively find the matrices

$$\begin{pmatrix} 2 & -1 & 3 & 4 & 5 \\ 4 & -2 & 5 & 6 & 7 \\ 6 & -3 & 7 & 8 & 9 \\ \alpha & -4 & 9 & 10 & 11 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ -2 & 4 & 5 & 6 & 7 \\ -3 & 6 & 7 & 8 & 9 \\ -4 & \alpha & 9 & 10 & 11 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ 0 & 0 & -1 & -2 & -3 \\ 0 & 0 & -2 & -4 & -6 \\ 0 & \alpha-8 & -3 & -6 & -9 \end{pmatrix}$$

$$\sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ 0 & -2 & -1 & 0 & -3 \\ 0 & -4 & -2 & 0 & -6 \\ 0 & -6 & -3 & \alpha-8 & -9 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ 0 & -2 & -1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \alpha-8 & 0 \end{pmatrix}$$

$$\sim \begin{pmatrix} -1 & 2 & 3 & 4 & 5 \\ 0 & -2 & -1 & 0 & -3 \\ 0 & 0 & 0 & \alpha-8 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} -1 & 2 & 4 & 3 & 5 \\ 0 & -2 & 0 & -1 & -3 \\ 0 & 0 & \alpha-8 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

hence the system is always consistent.
1) If $\alpha \neq 8$, we get the equivalent system:

$$\left\{\begin{array}{rcl} -x_2 + 2x_4 + 4x_1 + 3x_3 &=& 5 \\ -2x_4 \qquad\quad - \ x_3 &=& -3 \\ (\alpha-8)x_1 \qquad\quad &=& 0 \end{array}\right. .$$

Its solution set is

$$S = \left\{ \left(0, -2 + 2x_3, x_3, \frac{3}{2} - \frac{x_3}{2}\right) \mid x_3 \in \mathbb{R} \right\}.$$

2) If $\alpha = 8$, the system is equivalent to

$$\left\{\begin{array}{rcl} -x_2 + 2x_4 + 4x_1 + 3x_3 &=& 5 \\ -2x_4 \qquad\quad - \ x_3 &=& -3 \end{array}\right. ,$$

which has the solution set

$$S = \left\{ \left(x_1, -2 + 4x_1 + 2x_3, x_3, \frac{3}{2} - \frac{x_3}{2}\right) \mid x_1, x_3 \in \mathbb{R} \right\}.$$

II) ... using Rouché Theorem:
We have $\begin{vmatrix} -1 & 3 \\ -2 & 5 \end{vmatrix} = 1,$

$$\begin{vmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \\ 6 & -3 & 7 \end{vmatrix} = \begin{vmatrix} -1 & 3 & 4 \\ -2 & 5 & 6 \\ -3 & 7 & 8 \end{vmatrix} = \begin{vmatrix} -1 & 3 & 4 \\ -2 & 5 & 6 \\ -4 & 9 & 10 \end{vmatrix} = 0 \text{ and } \begin{vmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \\ \alpha & -4 & 9 \end{vmatrix} = \alpha - 8.$$

1) If $\alpha = 8$, then we can consider $d_p = \begin{vmatrix} -1 & 3 \\ -2 & 5 \end{vmatrix}$. We can complete it two ways with constant terms columns:

$$\begin{vmatrix} -1 & 3 & 5 \\ -2 & 5 & 7 \\ -3 & 7 & 9 \end{vmatrix} = \begin{vmatrix} -1 & 3 & 5 \\ -2 & 5 & 7 \\ -4 & 9 & 11 \end{vmatrix} = 0,$$

hence the system is consistent. To get the solution set, we have to solve a system of 2 linear equations with 2 unknowns, which will be the reader's task.

2) If $\alpha \neq 8$, we take $d_p = \begin{vmatrix} 2 & -1 & 3 \\ 4 & -2 & 5 \\ \alpha & -4 & 9 \end{vmatrix}$. The only way to complete it with a constant terms column gives us a zero minor, hence the system is consistent, equivalent to

$$\begin{cases} 2x_1 - \ x_2 + 3x_3 = \ 5 - 4x_4 \\ 4x_1 - 2x_2 + 5x_3 = \ 7 - 6x_4 \\ \alpha x_1 - 4x_2 + 9x_3 = 11 - 10x_4 \end{cases},$$

system which can be solved with Cramer's rule.

Let us notice that in the considered cases, we have different types of consistency: in the first case we have 2 side unknowns and in the second case we have only one.

5) Discuss on the real parameter α the consistency of the following system in $\mathbb{R}^3$, then solve it:

$$\begin{cases} \alpha x_1 + \ x_2 + \ x_3 = 1 \\ x_1 + \alpha x_2 + \ x_3 = 1 \\ x_1 + \ x_2 + \alpha x_3 = 1 \end{cases}.$$

Solution: **I) ... using Gaussian elimination:**
We successively obtain the equivalent matrices:

$$\begin{pmatrix} \alpha & 1 & 1 & 1 \\ 1 & \alpha & 1 & 1 \\ 1 & 1 & \alpha & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 1 & \alpha & 1 & 1 \\ \alpha & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 0 & \alpha - 1 & 1 - \alpha & 0 \\ 0 & 1 - \alpha & (1-\alpha)(1+\alpha) & 1 - \alpha \end{pmatrix}$$

$$\sim \begin{pmatrix} 1 & 1 & \alpha & 1 \\ 0 & \alpha - 1 & 1 - \alpha & 0 \\ 0 & 0 & (1-\alpha)(2+\alpha) & 1 - \alpha \end{pmatrix} = B.$$

1) If $\alpha = -2$ then

$$B = \begin{pmatrix} 1 & 1 & -2 & 1 \\ 0 & -3 & 3 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix},$$

hence the system is inconsistent.
2) If $\alpha \neq 2$ then the system is consistent.
2.1) If $\alpha = 1$ then

$$B = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

the system is consistent, equivalent to the equation $x_1 + x_2 + x_3 = 1$, and the solution set is $S = \{(1 - x_2 - x_3, x_2, x_3) \mid x_2, x_3 \in \mathbb{R}\}$.
2.2) If $\alpha \in \mathbb{R} \setminus \{-2, 1\}$ then the system is consistent, it has a unique solution which can be found by solving the equivalent system

$$\left\{ \begin{array}{rrr} x_1 + & x_2 + & \alpha x_3 = 1 \\ & (\alpha-1)x_2 + & (1-\alpha)x_3 = 0 \\ & & (1-\alpha)(2+\alpha)x_3 = 1-\alpha \end{array} \right. .$$

The systems solution set is $\left(\frac{1}{2+\alpha}, \frac{1}{2+\alpha}, \frac{1}{2+\alpha}\right)$.

II) ... using Rouché Theorem:

The system's matrix determinant is $\begin{vmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{vmatrix}$. We add all the rows to the first one, we get the factor $\alpha + 2$, and the left determinant can be easily computed

$$\begin{vmatrix} \alpha & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{vmatrix} = (\alpha+2) \begin{vmatrix} 1 & 1 & 1 \\ 1 & \alpha & 1 \\ 1 & 1 & \alpha \end{vmatrix} = (\alpha+2)(\alpha-1)^2.$$

1) If $\alpha \in \mathbb{R} \setminus \{-2, 1\}$, the system is consistent, with a unique solution, provided by Cramer's rule.
2) If $\alpha = 1$, all the equations become

$$x_1 + x_2 + x_3 = 1,$$

which can be solved as we previously saw.
3) If $\alpha = -2$, we take $d_p = \begin{vmatrix} -2 & 1 \\ 1 & -2 \end{vmatrix}$. The only way to complete it with a constant terms column gives us the minor $\begin{vmatrix} -2 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & 1 \end{vmatrix} = 9 \neq 0$ hence the system is inconsistent.

4.5 Exercises

1) Let $\varphi \in \mathbb{R}$. Show that the plane rotation with rotation angle φ, i.e. the map

$$f : \mathbb{R}^2 \to \mathbb{R}^2,\ f(x, y) = (x \cos\varphi - y \sin\varphi, x \sin\varphi + y \cos\varphi),$$

is an automorphism of the real vector space $\mathbb{R}^2$. Find the matrix of f in the standard basis of $\mathbb{R}^2$.
2) Show that the maps $f : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (x, -y)$ (the symmetry with respect to Ox) and $g : \mathbb{R}^2 \to \mathbb{R}^2$, $f(x, y) = (-x, y)$ (the symmetry with respect to Oy) are automorphisms of the real space $\mathbb{R}^2$. Find the matrices of f, g, $f - g$, $f + 2g$ and $g \circ f$ in the standard basis.
3) Show that the vector lists (v_1, v_2, v_3) and (v_1', v_2', v_3') with

$$v_1 = (1, 2, 1), v_2 = (2, 3, 3), v_3 = (3, 7, 1) \text{ and } v_1' = (3, 1, 4), v_2' = (5, 2, 1), v_3' = (1, 1, -6)$$

are bases for the real vector space $\mathbb{R}^3$ and find the connection between the coordinates of a given vector in these bases.

4) Let $B = (v_1, v_2, v_3, v_4)$ be a basis of the $\mathbb{R}$-vector space $\mathbb{R}^4$, let us consider

$$u_1 = v_1,\ u_2 = v_1 + v_2,\ u_3 = v_1 + v_2 + v_3,\ u_4 = v_1 + v_2 + v_3 + v_4$$

and let $f \in End_{\mathbb{R}}(\mathbb{R}^4)$ with

$$[f]_B = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 3 & 0 & -1 & 2 \\ 2 & 5 & 3 & 1 \\ 1 & 2 & 1 & 3 \end{pmatrix}.$$

Show that $B' = (u_1, u_2, u_3, u_4)$ is a basis of $\mathbb{R}^4$ and determine the matrix $[f]_{B'}$.

5) Let V be a real vector space, $B = (v_1, v_2, v_3)$ a basis of V, let us consider

$$u_1 = v_1 + 2v_2 + v_3,\ u_2 = v_1 + v_2 + 2v_3,\ u_3 = v_1 + v_2$$

and let $f \in End_{\mathbb{R}}(V)$. Show that $B' = (u_1, u_2, u_3)$ is a basis of V and determine the matrix $[f]_B$ knowing that

$$[f]_{B'} = \begin{pmatrix} 1 & 1 & 3 \\ 0 & 5 & -1 \\ 2 & 7 & -3 \end{pmatrix}.$$

6) Let $f \in End_{\mathbb{Q}}(\mathbb{Q}^4)$ with the matrix in the standard basis equal to

$$\begin{pmatrix} 0 & 1 & 2 & 3 \\ -1 & 2 & 1 & 0 \\ 3 & 0 & -1 & -2 \\ 5 & -3 & -1 & 1 \end{pmatrix}.$$

Determine a basis and the dimension for each of the vector spaces $\operatorname{Ker} f$, $\operatorname{Im} f$, $\operatorname{Ker} f + \operatorname{Im} f$ and $\operatorname{Ker} f \cap \operatorname{Im} f$.

7) Let $K = \mathbb{R}$. Check the equality $S = x^1 + S_0$ from Theorem 4.32 for the linear system

$$\begin{cases} 2x_1 + x_2 - x_3 - x_4 + x_5 = 1 \\ x_1 - x_2 + x_3 + x_4 - 2x_5 = 0 \\ 3x_1 + 3x_2 - 3x_3 - 3x_4 + 4x_5 = 2 \end{cases}$$

and find a basis for the solution subspace of the associated homogeneous system.

8) Discuss on the real parameters $\alpha,\ \beta,\ \gamma,\ \lambda$ the consistency of the following systems, then solve them:

$$a) \begin{cases} 5x_1 - 3x_2 + 2x_3 + 4x_4 = 3 \\ 4x_1 - 2x_2 + 3x_3 + 7x_4 = 1 \\ 8x_1 - 6x_2 - x_3 - 5x_4 = 9 \\ 7x_1 - 3x_2 + 7x_3 + 17x_4 = \alpha \end{cases} \text{(in } \mathbb{R}^4\text{)},\ b) \begin{cases} x_1 + x_2 + x_3 = 1 \\ \alpha x_1 + \beta x_2 + \gamma x_3 = \lambda \\ \alpha^2 x_1 + \beta^2 x_2 + \gamma^2 x_3 = \lambda^2 \end{cases} \text{(in } \mathbb{R}^3\text{)}.$$

References

[1] S. Breaz, T. Coconeţ, C. Conţiu, *Lecţii de algebră*, Ed. Eikon, Cluj-Napoca, 2010.

[2] S. Crivei, *Basic Abstract Algebra*, Ed. Casa Cărţii de Ştiinţă, Cluj-Napoca, 2002

[3] I. D. Ion, N. Radu, *Algebră*, Editura Didactică şi Pedagogică, Bucureşti, 1991.

[4] I. Purdea, I. Pop, *Algebră*, Ed. Gil, Zalău, 2003.

[5] I. Purdea, C. Pelea, *Probleme de algebră*, Ed. Eikon, Cluj-Napoca, 2008.