First Partial Exam (theory)

A. ALGEBRAIC STRUCTURES

1. Relations:

A triple $r = (A, B, R)$, where A, B are sets and

$$R \subseteq A \times B = \{(a, b) \mid a \in A, b \in B\},$$

is called a *(binary) relation*.
The set A is called the *domain*, the set B is called the *codomain* and the set R is called the *graph* of the relation r.
If $A = B$, then the relation r is called *homogeneous*.

Recall that a relation $r = (A, B, R)$ is called *homogeneous* if $A = B$.

Definition

A homogeneous relation $r = (A, A, R)$ on A is called:
(1) *reflexive* (r) if: $\forall x \in A,\ x\, r\, x$.
(2) *transitive* (t) if: $x, y, z \in A,\ x\, r\, y$ and $y\, r\, z \Longrightarrow x\, r\, z$.
(3) *symmetric* (s) if: $x, y \in A,\ x\, r\, y \Longrightarrow y\, r\, x$.
A homogeneous relation $r = (A, A, R)$ is called an *equivalence relation* if r has the properties (r), (t) and (s).

2. Operations:

Definition

By an *operation* (or *composition law*) on a set A we understand a function

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

Usually, we denote operations by symbols like $\cdot$, $+$, $*$, so that $\varphi(x, y)$ is denoted by $x \cdot y$, $x + y$, $x * y$, $\forall (x, y) \in A \times A$. We denote by $(A, \cdot)$ the fact that "$\cdot$" is an operation on a set A.

Definition

Let "$\cdot$" be an operation on an arbitrary set A.
(1) *Associative law*: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $\forall x, y, z \in A$.
(2) *Commutative law*: $x \cdot y = y \cdot x$, $\forall x, y \in A$.
(3) *Identity law*: $\exists e \in A$ such that $\forall a \in A,\ a \cdot e = e \cdot a = a$. In this case, e is called an *identity element*.
(4) *Inverse law*: $\forall a \in A, \exists a' \in A$ such that $a \cdot a' = a' \cdot a = e$, where e is the identity element. In this case, a' is called an *inverse element for* a.

Lemma

Let "$\cdot$" be an operation on a set A.
(i) If there exists an identity element in A, then it is unique.
(ii) Assume further that the operation "$\cdot$" is associative and has identity element e and let $a \in A$. If an inverse element for a does exist, then it is unique.

3. Groups:

Definition

Let "$\cdot$" be an operation on a set A. Then $(A, \cdot)$ is called a:
(1) *semigroup* if the associative law holds.
(2) *monoid* if it is a semigroup with identity element.
(3) *group* if it is a monoid in which every element has an inverse.

If the operation is commutative as well, then the structure is called *commutative*. A commutative group is also called an *abelian group* (after the name of N. H. Abel).

Remark

We denote by 1 the identity element of a group $(G, \cdot)$ and by x^{-1} the inverse of an element $x \in G$. In case of an additive group $(G, +)$, the identity element is denoted by 0, while the inverse of an element $x \in G$ is called the *symmetric* of x and is denoted by $-x$.

- power in groups:

Let $(G, \cdot)$ be a semigroup, let $x \in G$ and let $n \in \mathbb{N}^*$. Then we may use the associative law and define

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

If $(G, \cdot)$ is a monoid, then we may also define $x^0 = 1$.
If $(G, \cdot)$ is a group, then we may also define $x^{-n} = (x^{-1})^n$.

If the operation is "+", then x^n becomes nx.

- examples:

(a) The operation "$-$" defined on $\mathbb{Z}$ is not associative.

(b) $(\mathbb{N}^*, +)$ is a semigroup, but not a monoid.

(c) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ are monoids, but not groups.

(d) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ and $(\mathbb{C}^*, \cdot)$ are groups.

(e) Let X be a non-empty set. By a *word on* X of length n we understand a string of n elements from X for some $n \in \mathbb{N}$. The word of length 0 is called the *void word* and is denoted by e. On the set X^* of words on X consider the operation "$\cdot$" given by concatenation. Then $(X^*, \cdot)$ is a monoid with identity element e, called the *free monoid* on the set X.

(f) 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*.

(g) Let $n \in \mathbb{N}$, $n \geq 2$. Then $(\mathbb{Z}_n, +)$ is an abelian group, called the *group of residue classes modulo n*. The addition is defined by

$$\widehat{x} + \widehat{y} = \widehat{x + y}, \quad \forall \widehat{x}, \widehat{y} \in \mathbb{Z}_n.$$

(h) Let $n \in \mathbb{N}$ with $n \geq 2$. Denote by $M_{m,n}(\mathbb{R})$ the set of $m \times n$-matrices with entries in $\mathbb{R}$ and by $M_n(\mathbb{R})$ the set of $n \times n$-matrices with entries in $\mathbb{R}$. Then $(M_{m,n}(\mathbb{R}), +)$ is an abelian group and $(M_n(\mathbb{R}), \cdot)$ is a monoid.
Denote by $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ the set of invertible $n \times n$-matrices with real entries. Then $(GL_n(\mathbb{R}), \cdot)$ is a group, called the *general linear group of rank n*.

(i) Let M be a set and let $S_M = \{f : M \to M \mid f \text{ is bijective}\}$. Then $(S_M, \circ)$ is a group, called the *symmetric group of* M. The identity element is the identity map 1_M and the inverse of an element f (which is a bijection) is the inverse function f^{-1}.
If $|M| = n$, then S_M is denoted by S_n, and the group $(S_n, \circ)$ is in fact the *permutation group* of n elements.

(j) Let $K = \{e, a, b, c\}$ and define an operation "$\cdot$" on K by the following table:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Then $(K, \cdot)$ is an abelian group, called *Klein's group*. It may be viewed as the group of geometric transformations of a rectangle:
- e is the identical transformation,
- a is the symmetry with respect to the horizontal symmetry axis,
- b is the symmetry with respect to the vertical symmetry axis,
- c is the symmetry with respect to the center of the circumscribed circle.

The product $x \cdot y$ is defined by performing first y and then x.

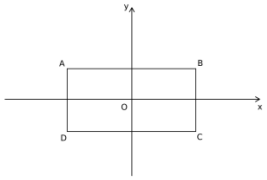

Figure: Klein's group.

4. Rings:

Definition

Let R be a set. A structure with two operations $(R, +, \cdot)$ is called a:
(1) *ring* if $(R, +)$ is an abelian group, $(R, \cdot)$ is a semigroup and the *distributive laws* hold:

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad \forall x, y, z \in R,$$
$$(y + z) \cdot x = y \cdot x + z \cdot x, \quad \forall x, y, z \in R.$$

(2) *unitary ring* if $(R, +, \cdot)$ is a ring and there is an identity element with respect to "$\cdot$".
(3) *division ring* (or *skew field*) if $(R, +)$ is an abelian group, $(R^*, \cdot)$ is a group and the distributive laws hold.
(4) *field* if it is a commutative division ring.
The ring $(R, +, \cdot)$ is called *commutative* if "$\cdot$" is commutative.

- power in rings:

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

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ times}},$$
$$0 \cdot x = 0,$$
$$(-n) \cdot x = -n \cdot x,$$
$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}.$$

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

- examples:

(a) $(\mathbb{Z},+,\cdot)$ is a unitary ring, but not a field.

(b) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$ are fields.

(c) Let $\{e\}$ be a single element set and let both "$+$" and "$\cdot$" be the only operation on $\{e\}$, defined by $e+e=e$ and $e\cdot e=e$. Then $(\{e\},+,\cdot)$ is a commutative unitary ring, called the *trivial ring*.

(d) Let $n\in\mathbb{N}$, $n\geq 2$. Then $(\mathbb{Z}_n,+,\cdot)$ is a commutative unitary ring, called the *ring of residue classes modulo n*. The addition and the multiplication are defined by

$$\widehat{x}+\widehat{y}=\widehat{x+y}\,,\quad \widehat{x}\cdot\widehat{y}=\widehat{x\cdot y}\,,\quad \forall \widehat{x},\widehat{y}\in\mathbb{Z}_n.$$

Note that $(\mathbb{Z}_n,+,\cdot)$ is a field if and only if n is prime.

(e) Let $(R,+,\cdot)$ be a commutative unitary ring. Then $(R[X],+,\cdot)$ is a commutative unitary ring, called the *polynomial ring over R in the indeterminate X*, where the operations are the usual addition and multiplication of polynomials.

(f) Let $n\in\mathbb{N}$, $n\geq 2$ and let $(R,+,\cdot)$ be a ring. Then $(M_n(R),+,\cdot)$ is a ring, called the *ring of matrices $n\times n$ with entries in R*, where the operations are the usual addition and multiplication of matrices.

(g) Let M be a non-empty set and let $(R,+,\cdot)$ be a ring. Define on the set

$$R^M=\{f\mid f:M\to R\}$$

two operations by: $\forall f,g\in R^M$, we have $f+g:M\to R$, $f\cdot g:M\to R$, where

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

$$(f\cdot g)(x)=f(x)\cdot g(x)\,,\quad \forall x\in M\,.$$

5. Subgroups:

Definition

Let $(G,\cdot)$ be a group and let $H\subseteq G$. Then H is called a *subgroup* of G if:
(i) H is a stable subset of $(G,\cdot)$.
(ii) $(H,\cdot)$ is a group.

- characterization of subgroups:

Let $(G,\cdot)$ be a group and let $H\subseteq G$. Then

$$H\leq G\Leftrightarrow\begin{cases}H\neq\emptyset\ (1\in H)\\ \forall x,y\in H,\ x\cdot y\in H\\ \forall x\in H,\ x^{-1}\in H.\end{cases}\Leftrightarrow\begin{cases}H\neq\emptyset\ (1\in H)\\ \forall x,y\in H,\ x\cdot y^{-1}\in H.\end{cases}$$

In case of an additive group $(G,+)$, the conditions become:
- $\forall x,y\in H,\ x+y\in H$.
- $\forall x\in H,\ -x\in H$.
- $\forall x,y\in H,\ x-y\in H$.

- examples:

(a) Every non-trivial group $(G,\cdot)$ has two subgroups, namely $\{1\}$ and G, called the *trivial subgroups*.

(b) $\mathbb{Z}$ is a subgroup of $(\mathbb{Q},+)$, $(\mathbb{R},+)$ and $(\mathbb{C},+)$, $\mathbb{Q}$ is a subgroup of $(\mathbb{R},+)$ and $(\mathbb{C},+)$, $\mathbb{R}$ is a subgroup of $(\mathbb{C},+)$.

(c) The set

$$n\mathbb{Z}=\{nx\mid x\in\mathbb{Z}\}$$

is a subgroup of $(\mathbb{Z},+)$ for every $n\in\mathbb{N}$.

(d) The set

$$H=\{z\in\mathbb{C}\mid |z|=1\}$$

is a subgroup of the group $(\mathbb{C}^*,\cdot)$, called the *circle group*. But it is not a subgroup of the group $(\mathbb{C},+)$.

(e) The set

$$U_n=\{z\in\mathbb{C}\mid z^n=1\}\quad (n\in\mathbb{N}^*)$$

is a subgroup of the group $(\mathbb{C}^*,\cdot)$, called the *group of n^{th} roots of unity*. Its elements are the following:

$$\varepsilon_k=\cos\frac{2k\pi}{n}+i\sin\frac{2k\pi}{n},\quad k\in\{0,\dots,n-1\}.$$

(f) Consider the general linear group $(GL_n(\mathbb{R}),\cdot)$ of rank n, where $GL_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \det(A)\neq 0\}$ $(n\in\mathbb{N},\ n\geq 2)$ and denote

$$SL_n(\mathbb{R})=\{A\in M_n(\mathbb{R})\mid \det(A)=1\}.$$

Then $SL_n(\mathbb{R})$ is a subgroup of $(GL_n(\mathbb{R}),\cdot)$, called the *special linear group of rank n*.

6. Subrings & subfields:

Definition

Let $(R,+,\cdot)$ be a ring and let $A \subseteq R$. Then A is called a *subring* of R if:
(i) A is a stable subset of $(R,+,\cdot)$.
(ii) $(A,+,\cdot)$ is a ring.

Theorem

Let $(R,+,\cdot)$ be a ring and let $A \subseteq R$. Then

$$A \text{ is a subring of } R \iff \begin{cases} A \neq \emptyset \ (0 \in A) \\ \forall x,y \in A,\ x-y \in A \\ \forall x,y \in A,\ x \cdot y \in A. \end{cases}$$

Definition

Let $(K,+,\cdot)$ be a field and let $A \subseteq K$. Then A is called a *subfield* of K if:
(i) A is a stable subset of $(K,+,\cdot)$.
(ii) $(A,+,\cdot)$ is a field.

Theorem

Let $(K,+,\cdot)$ be a field and let $A \subseteq K$. Then

$$A \text{ is a subfield of } K \iff \begin{cases} |A| \geq 2 \ (0,1 \in A) \\ \forall x,y \in A,\ x-y \in A \\ \forall x,y \in A \text{ with } y \neq 0,\ x \cdot y^{-1} \in A. \end{cases}$$

- examples:

(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 $(\mathbb{C},+,\cdot)$.

(c) $\mathbb{Q}$ is a subfield of $(\mathbb{R},+,\cdot)$ and $(\mathbb{C},+,\cdot)$, while $\mathbb{R}$ is a subfield of $(\mathbb{C},+,\cdot)$.

(d) The set

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$$

is a subring of $(\mathbb{Z},+,\cdot)$ for every $n \in \mathbb{N}$. Note that $n\mathbb{Z}$ does not have identity for $n \geq 2$.

(e) The set

$$\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$$

is a subring of the field $(\mathbb{C},+,\cdot)$, but not a subfield. It is called the *ring of Gauss integers*.

7. Homomorphisms:

Definition

Let $(G,\cdot)$, $(G',\cdot)$ be groups and $f : G \to G'$. Then f is called a:
1. *group homomorphism* if $f(x \cdot y) = f(x) \cdot f(y)$, $\forall x,y \in G$.
2. *group isomorphism* if it is a bijective group homomorphism.

Theorem

Let $f : G \to G'$ be a group homomorphism. Then:
(i) $f(1) = 1'$.
(ii) $(f(x))^{-1} = f(x^{-1})$, $\forall x \in G$.

Definition

Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be rings and $f : R \to R'$. Then f is called a:
1. *ring homomorphism* if $\forall x,y \in R$ we have
$$f(x+y) = f(x)+f(y),$$
$$f(x \cdot y) = f(x) \cdot f(y).$$
2. *ring isomorphism* if it is a bijective ring homomorphism.

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

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

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 $f(1) = 1'$.

Unitary ring homomorphisms

Definition

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 *unitary* if $f(1) = 1'$.

Theorem

Let $(R,+,\cdot)$ and $(R',+,\cdot)$ be unitary rings with identity elements 1 and $1'$ respectively, and let $f : R \to R'$ be a ring homomorphism.
(i) If f is surjective, then f is unitary.
(ii) If f is a ring isomorphism, then f is unitary.
(iii) If f is unitary and $x \in R$ has an inverse element $x^{-1} \in R$, then $f(x)$ has an inverse and

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

B. VECTOR SPACES

Definition

A *vector space over K* (or a *K-vector space*) is an abelian group $(V,+)$ together with a so-called *external operation* or *scalar multiplication*

$$\cdot : K \times V \to V\,, \quad (k,v) \mapsto k \cdot v \quad (\text{or simply } kv)\,,$$

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 every $k, k_1, k_2 \in K$ and every $v, v_1, v_2 \in V$.
The elements of K are called *scalars* and the elements of V are called *vectors*.
Sometimes a vector space is also called a *linear space*.

We usually denote a vector space V over K by ${}_KV$ or $(V, K, +, \cdot)$.

(1) In the definition of a vector space there are present four operations (3 by our definition), two denoted by the same symbol "$+$" and two denoted by the same symbol "$\cdot$". Of course, they are not the same, but we use the convention to denote them identically for the sake of simplicity of writing.

(2) The axioms (L_1) and (L_2) look like some distributive laws and the axiom (L_3) looks like an associative law, but they are not, since the involved elements are not taken from the same set.

(3) We have defined a *left vector space*. It is also possible to define a *right vector space* by considering an external operation

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

satisfying some similar axioms, but on the right hand side.

- basic properties:

Let V be a vector space over K. Then $\forall k, k' \in K$ and $\forall v, v' \in V$:
(i) $k \cdot 0 = 0 \cdot v = 0$.
(ii) $k(-v) = (-k)v = -kv$.
(iii) $k(v - v') = kv - kv'$.
(iv) $(k - k')v = kv - k'v$.

in

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

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

1. Subspaces:

Definition

Let V be a vector space over K and let $S \subseteq V$. Then S is a *subspace* of V if:
(i) $S \neq \emptyset$.
(ii) $\forall v_1, v_2 \in S$, $v_1 + v_2 \in S$.
(iii) $\forall k \in K$, $\forall v \in S$, $kv \in S$.

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

Notice that every subspace S of a vector space V over K is a subgroup of the additive group $(V,+)$, hence S must contain 0.

- characterization of subspaces:

Theorem

Let V be a vector space over K and let $S \subseteq V$. Then

$$S \leq V \iff \begin{cases} S \neq \emptyset \quad (0 \in S) \\ \forall k_1, k_2 \in K\,,\ \forall v_1, v_2 \in S\,,\ k_1 v_1 + k_2 v_2 \in S\,. \end{cases}$$

- examples:

(a) Every non-zero vector space V over K has two subspaces, namely $\{0\}$ and V. They are called the *trivial subspaces*.

(b) Let us show that

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

are subspaces of the canonical real vector space $\mathbb{R}^3$ [...].
Note that S is a plane passing through the origin. For instance, the plane

$$\{(x,y,z) \in \mathbb{R}^3 \mid x+y+z = 1\}$$

is not a subspace of $\mathbb{R}^3$ over $\mathbb{R}$.
Note that T is a line passing through the origin.

(c) More generally, the only subspaces of $\mathbb{R}^3$ are $\{(0,0,0)\}$, any line containing the origin, any plane containing the origin and $\mathbb{R}^3$.

(d) Let $n \in \mathbb{N}$ and let

$$K_n[X] = \{f \in K[X] \mid \text{degree}(f) \leq n\}.$$

Then $K_n[X]$ is a subspace of the polynomial vector space $K[X]$ over K. Note that the set $\{f \in K[X] \mid \text{degree}(f) = n\}$ is not a subspace of $K[X]$ over K.

(e) Let $I \subseteq \mathbb{R}$ be an interval. We have seen that

$$\mathbb{R}^I = \{f \mid f : I \to \mathbb{R}\}$$

is a real vector space, where the addition and the scalar multiplication are defined as follows: $\forall f, g : I \to \mathbb{R}$, $\forall k \in K$, we have $f+g : I \to \mathbb{R}$, $kf : I \to \mathbb{R}$, where

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

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 $\mathbb{R}^I$, because they are nonempty and we have:

$$\forall k_1, k_2 \in \mathbb{R}, \forall f, g \in C(I,\mathbb{R}),\ k_1 f + k_2 g \in C(I,\mathbb{R}),$$

$$\forall k_1, k_2 \in \mathbb{R}, \forall f, g \in D(I,\mathbb{R}),\ k_1 f + k_2 g \in D(I,\mathbb{R}).$$

2. Intersection of subspaces:

For a vector space V over K, we denote by $S(V)$ the set of all subspaces of V. Sometimes, this set is denoted by $S_K(V)$ if we like to emphasize the field K.

Theorem

Let V be a vector space over K and let $(S_i)_{i \in I}$ be a family of subspaces of V. Then $\bigcap_{i \in I} S_i \in S(V)$.

3. Generated subspaces:

Definition

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

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

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 $X = \{v_1, \ldots, v_n\}$, we denote $\langle v_1, \ldots, v_n \rangle = \langle \{v_1, \ldots, v_n\} \rangle$.

(1) $\langle X \rangle$ is the "smallest" (with respect to inclusion) subspace of V containing X.

(2) $\langle \emptyset \rangle = \{0\}$.

(3) If $S \leq V$, then $\langle S \rangle = S$.

Definition

A vector space V over K is called *finitely generated* if $\exists v_1, \dots, v_n \in V$ $(n \in \mathbb{N})$ such that

$$V = \langle v_1, \dots, v_n \rangle.$$

Then the set $\{v_1, \dots, v_n\}$ is called a *system of generators for* V.

Definition

Let V be a vector space over K and $v_1, \dots, v_n \in V$ $(n \in \mathbb{N})$. A finite sum of the form

$$k_1 v_1 + \cdots + k_n v_n,$$

where $k_i \in K$ $(i = 1, \dots, n)$, is called a (finite) *linear combination* of the vectors $v_1, \dots, v_n$.

- characterization of the generated subspaces:

Theorem

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

$$\langle X \rangle = \{k_1 v_1 + \cdots + k_n v_n \mid k_i \in K,\ v_i \in X, i = 1, \dots, n,\ n \in \mathbb{N}^*\},$$

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

- examples:

(a) Consider the canonical real vector space $\mathbb{R}^3$. Then

$$\begin{aligned}&\langle (1,0,0), (0,1,0), (0,0,1) \rangle \\ &= \{k_1(1,0,0) + k_2(0,1,0) + k_3(0,0,1) \mid k_1, k_2, k_3 \in \mathbb{R}\} \\ &= \{(k_1,0,0) + (0,k_2,0) + (0,0,k_3) \mid k_1, k_2, k_3 \in \mathbb{R}\} \\ &= \{(k_1, k_2, k_3) \mid k_1, k_2, k_3 \in \mathbb{R}\} = \mathbb{R}^3.\end{aligned}$$

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

(b) Consider the canonical vector space $\mathbb{Z}_2^3$ over $\mathbb{Z}_2$. Similarly as above, we have:

$$\langle (\widehat{1},\widehat{0},\widehat{0}), (\widehat{0},\widehat{1},\widehat{0}) \rangle = \{(k_1, k_2, \widehat{0}) \mid k_1, k_2 \in \mathbb{Z}_2\} \neq \mathbb{Z}_2^3.$$

Hence $\mathbb{Z}_2^3$ is not generated by the two vectors $(\widehat{1},\widehat{0},\widehat{0})$ and $(\widehat{0},\widehat{1},\widehat{0})$. But it is generated by $(\widehat{1},\widehat{0},\widehat{0})$, $(\widehat{0},\widehat{1},\widehat{0})$ and $(\widehat{0},\widehat{0},\widehat{1})$, hence it is finitely generated.

(c) Consider the subspace

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

of the canonical real vector space $\mathbb{R}^3$. Let us write it as a generated subspace. Expressing $x = y + z$, we have:

$$\begin{aligned}S &= \{(y+z, y, z) \mid y, z \in \mathbb{R}\} = \{(y,y,0) + (z,0,z) \mid y, z \in \mathbb{R}\} \\ &= \{y(1,1,0) + z(1,0,1) \mid y, z \in \mathbb{R}\} = \langle (1,1,0), (1,0,1) \rangle.\end{aligned}$$

Alternatively, one may express y or z by using the other two components and get other writings of S as a generated subspace, namely $S = \langle (1,1,0), (0,-1,1) \rangle = \langle (1,0,1), (0,1,-1) \rangle$. We see that S is finitely generated.

4. Sum of subspaces:

Definition

Let V be a vector space over K and let $S, T \leq V$.
We define the *sum* of the subspaces S and T as the set

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

Theorem

Let V be a vector space over K and $S, T \leq V$. Then
$S + T = \langle S \cup T \rangle$, *hence* $S + T \leq V$.

- direct sum of subspaces:

Definition

Let V be a vector space over K and let $S, T \leq V$.
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.

Theorem

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

$$V = S \oplus T \iff \forall v \in V, \exists! s \in S, t \in T \ : v = s + t.$$

5. Linear maps:

Definition

Let V and V' be vector spaces over the same field K. A function $f : V \to V'$ is called:
(1) *(K-)linear map* (or *(vector space) homomorphism* or *linear transformation*) if

$$f(v_1 + v_2) = f(v_1) + f(v_2), \quad \forall v_1, v_2 \in V,$$
$$f(kv) = kf(v), \quad \forall k \in K, \forall v \in V.$$

(2) *isomorphism* if it is a bijective K-linear map.
(3) *endomorphism* if it is a K-linear map and $V = V'$.
(4) *automorphism* if it is a bijective K-linear map and $V = V'$.

- properties of linear maps:

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 the groups $(V, +)$ and $(V', +)$. Then we have $f(0) = 0'$ and $f(-v) = -f(v)$, $\forall v \in V$.

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

$$\mathrm{Hom}_K(V, V') = \{f : V \to V' \mid f \text{ is } K\text{-linear}\},$$
$$\mathrm{End}_K(V) = \{f : V \to V \mid f \text{ is } K\text{-linear}\},$$
$$\mathrm{Aut}_K(V) = \{f : V \to V \mid f \text{ is bijective } K\text{-linear}\}.$$

Theorem

Let V and V' be vector spaces over K and $f : V \to V'$. Then f is a K-linear map $\iff f(k_1v_1 + k_2v_2) = k_1f(v_1) + k_2f(v_2), \forall k_1, k_2 \in K, \forall v_1, v_2 \in V$.

Theorem

(i) 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.
(ii) Let $f : V \to V'$ and $g : V' \to V''$ be K-linear maps. Then $g \circ f : V \to V''$ is a K-linear map.

- Kernel and image of a linear map:

Definition

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

$$\mathrm{Ker}\, f = \{v \in V \mid f(v) = 0'\}$$

is called the *kernel* (or the *null space*) of the K-linear map f and the set

$$\mathrm{Im}\, f = \{f(v) \mid v \in V\}$$

is called the *image* (or the *range space*) of the K-linear map f.

Theorem

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

$$\mathrm{Ker} f \leq V \text{ and } \mathrm{Im} f \leq V'.$$

Theorem

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

$$\mathrm{Ker}\, f = \{0\} \iff f \text{ is injective}.$$

Theorem

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. If $X = \emptyset$, then we have:

$$f(\langle \emptyset \rangle) = f(\{0\}) = \{f(0)\} = \{0'\} = \langle \emptyset \rangle = \langle f(\emptyset) \rangle.$$

If $X \neq \emptyset$, use

$$\langle X \rangle = \{k_1v_1 + \cdots + k_nv_n \mid k_i \in K,\ v_i \in X,\ i = 1, \ldots, n,\ n \in \mathbb{N}^*\}\ [...].$$

Theorem

Let V and V' be vector spaces over K. Consider on $\mathrm{Hom}_K(V, V')$ the operations: $\forall f, g \in \mathrm{Hom}_K(V, V')$ and $\forall k \in K$, $f + g, k \cdot f \in \mathrm{Hom}_K(V, V')$, where

$$(f + g)(v) = f(v) + g(v),$$
$$(kf)(v) = kf(v)$$

$\forall v \in V$. Then $\mathrm{Hom}_K(V, V')$ is a vector space over K.

Corollary

Let V be a vector space over K. Then $\mathrm{End}_K(V)$ is a vector space over K.

6. Linear independence:

Definition

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 every $k_1, \dots, k_n \in K$,

$$k_1 v_1 + \cdots + k_n v_n = 0 \Longrightarrow k_1 = \cdots = k_n = 0\,.$$

(2) *linearly dependent* in V if they are not linearly independent, that is, $\exists k_1, \dots, k_n \in K$ not all zero such that

$$k_1 v_1 + \cdots + k_n v_n = 0\,.$$

(1) A set consisting of a single vector v is linearly dependent $\Longleftrightarrow$ $v = 0$.

(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.

(3) More generally, an infinite set of vectors of V is called *linearly independent* if any finite subset is linearly independent, and *linearly dependent* if there exists a finite subset which is linearly dependent.

- linear dependence:

Let V be a vector space over K. Then the vectors $v_1, \dots, v_n \in V$ are linearly dependent if and only if one of the vectors is a linear combination of the others, that is, $\exists j \in \{1, \dots, n\}$ such that

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

for some $\alpha_i \in K$, where $i \in \{1, \dots, n\}$ and $i \neq j$.

- linear dependence in K^n:

Theorem

Let $n \in \mathbb{N}$, $n \geq 2$.
(i) Two vectors in the canonical vector space K^n are linearly dependent $\Longleftrightarrow$ their components are respectively proportional.
(ii) n vectors in the canonical vector space K^n are linearly dependent $\Longleftrightarrow$ the determinant consisting of their components is zero.

7. Basis:

Definition

Let V be a vector space over K. A list of vectors $B = (v_1, \dots, v_n) \in V^n$ is called a *basis* of V if:
(i) B is linearly independent in V;
(ii) B is a system of generators for V, that is, $\langle B \rangle = V$.

- existence of basis and proof:

Theorem

Every vector space V over K has a basis.

Proof. If $V = \{0\}$, then it has the basis $\emptyset$.
Now let $V = \langle B \rangle \neq \{0\}$, 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 $\exists j_1 \in \{1, \dots, n\}$ 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, $\exists j_2 \in \{1, \dots, n\} \setminus \{j_1\}$ such that $v_{j_2} = \sum_{\substack{i=1 \\ i \neq j_1, j_2}}^{n} k_i' v_i$ for some $k_i' \in K$. Then $V = \langle B \setminus \{v_{j_1}, v_{j_2}\} \rangle$, 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

$$V = \langle B \setminus \{v_{j_1}, \dots, v_{j_{n-1}}\} \rangle = \langle v_{j_n} \rangle.$$

• If v_{j_n} were linearly dependent, then $v_{j_n} = 0$, hence we have $V = \langle v_{j_n} \rangle = \{0\}$, contradiction. Hence v_{j_n} is linearly independent and thus forms a single element basis of V. □

We shall see that a vector space may have more than one basis.

- coordinates of a vector in a basis:

Definition

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 $k_1, \dots, k_n \in K$ appearing in the unique writing of v as a linear combination

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

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

- bases and linear maps:

Theorem

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.

Proof. [...]

Corollary

Let $f, g : V \to V'$ be K-linear maps and let $B = (v_1, \dots, v_n)$ be a basis of V. If $f(v_i) = g(v_i)$, $\forall i \in \{1, \dots, n\}$, then $f = g$.

Theorem

Let $f : V \to V'$ be a K-linear map, and let $X = (v_1, \dots, v_n)$ be a list of vectors in V.
(i) If f is injective and X is linearly independent in V, then $f(X)$ is linearly independent in V'.
(ii) If f is surjective and X is a system of generators for V, then $f(X)$ is a system of generators for V'.
(iii) If f is bijective and X is a basis of V, then $f(X)$ is a basis of V'.

8. Dimension:

Definition

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 $\dim V$.

If $V = \{0\}$, then V has the basis $\emptyset$ and $\dim V = 0$.

Theorem

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

Proof. [...]

Theorem (Steinitz Theorem, Exchange Theorem)

Let V be a vector space over K, $X = (x_1, \dots, x_m)$ a linearly independent list of vectors of V and $Y = (y_1, \dots, y_n)$ a system of generators of V. Then:
(i) $m \leq n$.
(ii) m vectors of Y can be replaced by the vectors of X obtaining again a system of generators for V.

- characterization of dimension:

Theorem

Let V be a vector space over K. The following are equivalent:
(i) $\dim V = n$.
(ii) The maximum no. of linearly independent vectors in V is n.
(iii) The minimum no. of generators for V is n.

Proof. $(i) \Longrightarrow (ii)$ Assume that $\dim V = n$. Let $B = (v_1, \dots, v_n)$ be a basis of V. Then B is linearly independent in V. Since B is a system of generators for V, any linearly independent list in V must have at most n elements by Steinitz Theorem.

$(ii) \Longrightarrow (i)$ Assume (ii). 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 Steinitz Theorem. Hence $m = n$ and consequently $\dim V = n$.

Theorem

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

Corollary

Let V be a vector space over K and $S \leq V$. Then:
(i) Any basis of S is a part of a basis of V.
(ii) $\dim S \leq \dim V$.
(iii) $\dim S = \dim V \iff S = V$.

- decomposition theorem:

Theorem

Let V be a vector space over K and let $S \leq V$. Then there exists $\overline{S} \leq V$ such that $V = S \oplus \overline{S}$. In particular,

$$\dim V = \dim S + \dim \overline{S}.$$

Proof. Let $(u_1, \dots, u_m)$ be a basis of S. Then it can be completed to a basis $B = (u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ of V. We consider

$$\overline{S} = \langle v_{m+1}, \dots, v_n \rangle$$

and we prove that $V = S \oplus \overline{S}$ [...]. □

- complement of a subspace:

Definition

Let V be a vector space over K and $S \leq V$. Then a subspace $\overline{S}$ of V such that

$$V = S \oplus \overline{S}$$

is called a *complement of S in V*.

Note that a subspace may have more than one complement.

Consider the subspace $S = \langle e_1, e_2 \rangle$ of the canonical real vector space $\mathbb{R}^3$, where $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$. Then clearly (e_1, e_2) is a basis of S.

It can be completed to a basis of $\mathbb{R}^3$, with the vector $e_3 = (0, 0, 1)$ or with the vector $v_3 = (1, 1, 1)$. Following the proof of the above theorem, a complement in V of the subspace $S = \langle e_1, e_2 \rangle$ is $\langle e_3 \rangle$ or $\langle v_3 \rangle$.

- *First Dimension Theorem*:

Definition

Let $f : V \to V'$ be a K-linear map. Then:
(1) $\dim(\mathrm{Ker} f)$ is called the *nullity* of f, and is denoted by $\mathrm{null}(f)$.
(2) $\dim(\mathrm{Im} f)$ is called the *rank* of f, and is denoted by $\mathrm{rank}(f)$.

Theorem (First Dimension Theorem)

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

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

In other words, $\dim V = \mathrm{null}(f) + \mathrm{rank}(f)$.

- *Second Dimension Theorem:*

Theorem (Second Dimension Theorem)

Let V be a vector space over K and let S, T be subspaces of V. Then

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

Corollary

Let V be a vector space over K, and let S and T be subspaces of V such that $V = S \oplus T$. Then

$$\dim V = \dim S + \dim T.$$

- dimension theorems:

Theorem

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

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

Proof. $\boxed{\Longrightarrow}$ If $f : V \to V'$ is a K-isomorphism and $B = (v_1, \dots, v_n)$ is a basis of V, then one shows that $B' = f(B) = (f(v_1), \dots, f(v_n))$ is a basis of V'. [...]
$\boxed{\Longleftarrow}$ If $B = (v_1, \dots, v_n)$ and $B' = (v'_1, \dots, v'_n)$ are bases of V and V' respectively, define a function $f : V \to V'$ in the following way. For every $v = k_1 v_1 + \cdots + k_n v_n \in V$ (where $k_1, \dots, k_n \in K$ are uniquely determined), define $f(v) = k_1 v'_1 + \cdots + k_n v'_n$. One proves that f is a K-isomorphism. [...]