7 October 2016 math.ubbcluj.ro/~crivei ; crivei@math.ubbcluj.ro

$G = 1 + T + E + S$ (HP, BP, HP)

1 — final grade (walk in); T — test; E — exam; S — seminar points

Ref.: 1. N. Both, S. Crivei - „Culegere de probleme de algebră" Lito UBB, C-N, 1976

- Structure of course

1. Preliminaries
2. Vector spaces
3. Matrices and linear systems
4. Introduction to coding theory

(1. + 2. — test)

Ref.: 1.

2. B. Călugăreanu - „Lecții de algebră liniară", Lito UBB, C-N, 1985
3. S. Crivei, „Basic Abstract Algebra", Coca Cărți de Știință, C-N, 2002-2003
4. S. Gilbert, L. Gilbert, „Elements of modern algebra", PWS Kent, Boston, 1992
5. W. J. Gilbert, W. K. Nicholson, „Modern algebra with applications", John Wiley, 2004

Chapter 1: PRELIMINARIES

1. RELATIONS

Def: A triple $r = (A, B, R)$ is called a (binary) relation, if A and B are sets and $R \subseteq A \times B = \{(a,b) \mid a \in A, b \in B\}$

A — the domain of r; B — the codomain of r; R — graph of r

⊛ If $A = B$, then r is called homogeneous

⊛ Let $X \subseteq A$. Then $r(X) \overset{\text{not}}{=} \{b \in B \mid \exists x \in X \text{ s.t. } (x,b) \in R\}$ — the relation class of X with respect to r

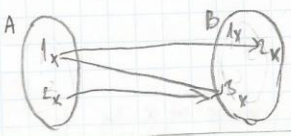
⊛ $(a,b) \in R$ can be written also $a \, r \, b$ ("a has a relation r to b")

⊛ We denote $r\langle x \rangle = r(\{x\})$

Ex.: a) Let $A = \{1,2\}$; $B = \{1,2,3\}$

$R = \{(1,2), (1,3), (2,3)\}$

$\Rightarrow r = (A, B, R)$



$r\langle 1 \rangle = \{2,3\}$

"

! not. for $r(\{1\})$

b) Let S be the set of all students

U the set of all universities

$R(S, U, R)$ where $R = \{(s,u) \in S \times U \mid s$ is a student of $U\}$

c) Let $r = (\mathbb{N}, \mathbb{N}, R)$ where $R = \{(a,b) \in \mathbb{N} \times \mathbb{N} \mid a = b\}$, that is $\{(a,a) \mid a \in \mathbb{N}\}$

Obs.: ! In general, $r = (A, A, R)$, where $R = \{(a,a) \mid a \in A\}$ is called the equality relation and is denoted by $\underset{r}{\delta_A} = \underset{R}{(A, A, \Delta_A)}$

d) $<, \leq, >, \geq, /$ $(\cdots)$ - relations

e) $\sim, \equiv$; for triangles $(\cdots)$

$\parallel, \perp$; for lines

f) Let $r = (A, B, R)$, $R \subseteq A \times B$ (a relation)

When $R = \emptyset$ then $\underline{0 = (A, B, \emptyset)}$ is called the void relation

When $R = A \times B$ then $\underline{u = (A, B, A \times B)}$ is called the universal relation

g) ! Every function is a relation (but not conversely: see ex. (a))

$f: A \to B$

$a \longmapsto f(a)$, $\forall a \in A$

$f = (A, B, \mathcal{F})$ where $\mathcal{F} = \{(a, f(a)) \mid a \in A\}$ the graph of f (G_f)

h) Every oriented graph is a relation

$V = \{1, 2, 3, 4\}$

(V, V, R), where $R = \{(1,2), (3,2), (4,3), (1,4)\}$

2. FUNCTIONS

Def.: A relation $r = (A, B, R)$, with $R \subseteq A \times B$ is called a function if $|r\langle a \rangle| = 1$, $\forall a \in A$

$f: A \to B$ $\quad a \longmapsto f(a)$

$X \subseteq A \Rightarrow f(X) = \{f(x), \mid x \in X\}$ - the image of x by f

Let A, b be sets with $|A| = m$, $|B| = n$ where $m, n \in \mathbb{N}^*$.

Denote $B^A = \{f : A \to B \mid f \text{ function}\}$

$|B^A| = m^n = |B|^{|A|}$

3. EQUIVALEN RELATIONS

Def.: A relation $r = (A, A, R)$ is called 1) (r) reflexive if $\forall a \in A$, $a \, r \, a$

2) (t) transitive if $a \, r \, b$ and $b \, r \, c \Rightarrow a \, r \, c$

3) (s) symmetric if $a \, r \, b \Rightarrow b \, r \, a$

$\Downarrow$

an (equivalence relation) [if it has (r), (t), (s)]

Ex.: "$=$", "$\equiv$", "r"

Denote by $E(A)$ the set of all equivalence relations on a set A.

4. PARTITIONS

Def.: Let $A \neq \emptyset$ be a set. A family $(A_i)_{i \in I}$ of non-empty subsets for A is called a partition of A if (i) $\bigcup_{i \in I} A_i = A$

(ii) $A_i \cap A_j = \emptyset$, $\forall i, j \in I$, $i \neq j$

Ex:

! no common elements

Ex.: (a) $A = \{1, 2, 3\}$; $A_1 = \{1, 2\}$, $A_2 = \{3\}$, $A_3 = \{4\}$

A_1, A_2, A_3, A_4 form a partition

(b) Partitions for $\mathbb{Z} \times \mathbb{Z}$: • $\mathbb{N}$, $\{$ neg. numbers$\}$

• $(\{x\})_{x \in \mathbb{Z}}$ "

! Every time we have a part. $\Rightarrow$ we have an eq-relation

Not.: $P(A)$ = the set of all partitions of the set A

Theorem: (1) Let $r \in E(A)$. Then $A/r \overset{not}{=} \{r\langle a \rangle \mid a \in A\} \in P(A)$.

(the quotient set of A by R)

(2) Let $\Pi = (A_i)_{i \in I} \in P(A)$. Then we define $x \, r_\Pi \, y \overset{def}{\Leftrightarrow} \exists \, i \in I, x, y \in A_i$. Then $r_\Pi \in E(A)$

related

13) $\exists$ bijection between $E(A)$ and $P(A)$

$F : E(A) \to P(A)$ bijective function

$F(R) = A/R$

with inverse $G : P(A) \to E(A)$

$G(\tilde{x}) = x\tilde{x}$

5. OPERATIONS

(Composition laws)

Def.: By an operation on a set A, we mean a function $\gamma : A \times A \to A$.

Ex.: "$\cdot$", "$+$" defines an operation on $\mathbb{N}, \mathbb{Z}, G, \mathbb{R}, \mathbb{C}$

"$-$" defines an operation on $\mathbb{Z}, G, \mathbb{R}, \mathbb{C}$

"$:$" does not define an operation on $\mathbb{N}, \mathbb{Z}, G, \mathbb{R}, \mathbb{C}$

Sometimes we denote operations by symbols like, "$*$", "$\top$", "$\perp$", etc

Def.: Let "$\cdot$" be an operation on a set A. (we denote this by $(A, \cdot)$)

- Associative law:

$\forall a,b,c \in A : a \cdot (b \cdot c) = (a \cdot b) \cdot c$

- Commutative law:

$\forall a,b \in A : a \cdot b = b \cdot c$

- Inverse law (Symetric)

$\forall a \in A : \exists a' \in A : a \cdot a' = e = a' \cdot a$

(e: identity element)

- identity element $\exists e \in A$ such that $\forall a \in A$, $a \cdot e = a$

Obs.! Let $(A, \cdot)$

i) If $\exists$ identity element, then it is unique. (we denote usualy by 1)

$a' \cdot a \cdot a'' = \begin{cases} a' \\ a \end{cases}$

ii) If "$\cdot$" is associative and $\exists$ identity element and a has an inverse, then, its inverse is unique (we denoted by a^{-1})

Def.: Let $(A,\cdot)$ and $B \subseteq A$. Then B is called a stable subset of A with respect to "$\cdot$": If $\forall a,b \in B$, $a \cdot b \in B$

- **Remark:** Associative Law and Commutative Law transfers to stable subset

Ex.: $\mathbb{Z}$ is a stable subset of $(\mathbb{Q},+)$ and $(\mathbb{Q},\cdot)$

6. GROUPS

Def.: Let $(A,\cdot)$. Then $(A,\cdot)$ is called a:

1. semigroup: if "$\cdot$" is associative
2. monoid: if "$\cdot$" associative and $\exists$ identity element
3. group: if "$\cdot$" associative, $\exists$ identity element, $\forall a \in A$ is inverse

If "$\cdot$" is commutative, a group $(A,\cdot)$ is called abelian

Ex.: (a) $(\mathbb{Z},\cdot)$ monoid
$(\mathbb{N},\cdot)$
$(\mathbb{R},\cdot)$
$(\mathbb{Q},\cdot)$

(b) $(\mathbb{N},+)$ monoid
$(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{C},+)$ groups

Def.: Let $(G,\cdot)$ be a group.

We may define $\forall x \in G$, $x^n = \begin{cases} \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}, & \text{for } n \in \mathbb{N}^* \\ 1, & \text{for } n = 0 \\ (x^{-1})^{-n}, & \text{for } n \in \mathbb{Z}, n < 0 \end{cases}$

Ex.: (a) Let $A = \{e\}$ be a single-element set. Then $(A,\cdot)$ is a group called a trivial group where $e \cdot e = e$

(b) Let $n \in \mathbb{N}$, $n \geq 2$, Denote by $\mathbb{Z}_n = \{\hat{0}, \hat{1}, \hat{2}, \ldots \hat{n-1}\}$ the set of residue classes modulo n

$\hat{x}$ = the set of all integers giving reminds x when divided by n

Note that $\mathbb{Z}_n$ is a partition of $\mathbb{Z}$.

Define $\forall \hat{x}, \hat{y} \in \mathbb{Z} \Rightarrow \hat{x} + \hat{y} = \widehat{x+y}$. Then $(\mathbb{Z}_n,+)$ is a group.

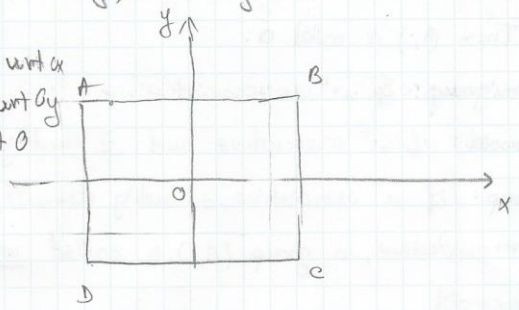
(c) Klein's group $(K,\cdot)$

$K = \{e, a, b, c\}$

$\circ$	e	a	b	c
a	e	b	c	d
b	b	e	c	b
c	c	e	e	a
d	d	b	a	e

Alternatively, we may see:

e-identity
a - symmetry with ox
b - symmetry with oy
c - symmetry with O
$x \cdot y =$



7. RINGS AND FIELDS

Def.: A triple $(A, +, \circ)$ where "+" and "$\circ$" are operations on A is called

① a ring if $(A, +)$ abelian group
$(A, \circ)$ semigroup
the distributive laws: $x \circ (y+z) = xy + xz$, $\forall x, y \in A$
$(y+z) \circ x = yx + zx$, $\forall x, y \in A$

② a division ring (or skew field) if $(A, +)$ abelian group
$(A^*, \circ)$ group
the distributive laws
where $A^* = A \setminus \{0\}$

③ field if it is a commutative field

④ integral domain if: $A \neq \{0\}$, A commutative, A unitary
(that is a ring with identity) and there are no zero divisors
$[x, y \in A,\ x \cdot y = 0 \Rightarrow x = 0 \text{ or } y = 0]$

Ex.: (a) $(\mathbb{Z}, +, \cdot)$ integral domain
(b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ fields
(c) Let $n \in \mathbb{N}$, $n \geq 2$. Then $(\mathbb{Z}_n, +, \cdot)$

(c) Let $n \in \mathbb{N}^*$, $n \geq 2$. Then $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring

where $\begin{cases} \hat{x}+\hat{y} = \widehat{x+y} \\ \hat{x}\cdot\hat{y} = \widehat{x\cdot y} \end{cases}$, $\forall \hat{x}, \hat{y} \in \mathbb{Z}_n$

Ex.: $\hat{2}\cdot\hat{3} = \hat{6}$, $\mathbb{Z}_6$

(c) Let $(A, +, \cdot)$ be a ring. Then $(M_n(A), +, \cdot)$ is a ring

$m=2$; $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = O_2$

d) Let $A(+,\cdot)$ be a commutative ring. Then $(A[X], +, \cdot)$ is a ring.

e) $(\{e\}, +, \cdot)$ trivial ring

8. SUBGROUPS AND SUBRINGS

Def: Let $(G, \cdot)$ be a group. Then $H \subseteq G$ is called a subgroup of G if $\begin{cases} H \neq \emptyset, & (e \in H) \\ \forall x, y \in H \Rightarrow x \cdot y \in H \\ \forall x \in H, \ x^{-1} \in H \end{cases}$

Not.: $H \leq G$

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

Ex.: (a) $\mathbb{Z}$ is a sub group of $(\mathbb{Q}, +)$, because $0 \in \mathbb{Z}$, $\forall x, y \in \mathbb{Z} \Rightarrow x + y \in \mathbb{Z}$ and $\forall x \in \mathbb{Z} \Rightarrow -x \in \mathbb{Z}$

(b) Any group $(G, \cdot)$ has the subgroups $\{1\}$ and G

Def.: Let $(R, +, \cdot)$ be a ring. Then $A \subseteq R$ is called a subring of A (denoted by $A \leq R$) if $\begin{cases} A \neq \emptyset \\ \forall x, y \in A, \ x - y \in A \\ \qquad\quad x \cdot y \in A \end{cases}$

Def.: Let $(K, +, \cdot)$ be a field. Then $A \subseteq K$ is called a subfield of K if $\begin{cases} |A| \geq 2, & (0, 1 \in A) \\ \forall x, y \in A \quad x - y \in A \\ \forall x, y \in A, \ y \neq 0, \ x \cdot y^{-1} \in A \end{cases}$

Ex.: (a) Any ring (field) has the subring (subfields) $\{0\}$ and R ($\mathbb{Z}_0$, $\mathbb{Q}$ and $\mathbb{R}$)

(b) $\mathbb{Z}$ is a subring of $(\mathbb{Q},+,\cdot)$

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

(d) $n\mathbb{Z} \overset{not}{=} \{n\cdot k \mid k\in\mathbb{Z}\}$ is a subring of $(\mathbb{Z},+,\cdot)$; $n\in\mathbb{N}$

$(2\mathbb{Z},+,\cdot)$ is a ring without identity

Recall: homomorfism, endomorfism, isomorfism, automorfism

- Project 1: Write a program to generate all partitions on a finite set (and count them).
- Project 2: Write a program to generate all associative operations (that is semigroups) on a finite set.

Ex.:

	a_1	a_2
a_1		
a_2		

Partial Exam 1: Week 7 (Friday 18.11.2016) . (4p)

10-12 (A-Z) Courses 1-6 (from 1-7)

Office hours hours 14:00 (Friday) C310

Cap 2: VECTOR SPACES

1. Definition. Examples. Basic properties

Let K be a field. $(K,+,\cdot)$

Def.: By a vector space over K (or K-vectorspace; K linear space) we mean an abelian group $(V,+)$ together with a so-called external operation (or scaler multiplication) $\gamma: K\times V\to V$, $\gamma(k,v) \overset{not}{=} k\cdot v$!

satisfying the axioms:

(L_1) $k\cdot(v_1+v_2) = kv_1 + kv_2$

(L_2) $(k_1+k_2)\cdot v = k_1v + k_2v$, $\forall v_1, v_2, v\in V$

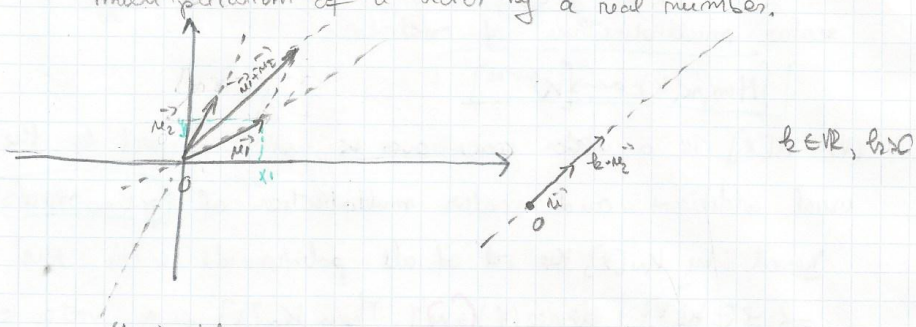
(L_3) $(k_1\cdot k_2)v = k_1\cdot(k_2\cdot v)$ $\forall k_1, k_2, k\in K$

(L_4) $1\cdot v = v$

(*) The elements of V are called vectors and the elements of K are called scalars.

• not. ${}_KV$ or $(V, K, +, \cdot)$

• Ex.: (a) Let V_2 be the set of all vectors (with the meaning from physics) from some place, having the origin in a fixed point, e.g. O. We can define the addition of two vectors and the scalar multiplication of a vector by a real number.



$k \in \mathbb{R}$, $k > 0$

$(V_2, +)$ abelian group
$\exists$ scalar multiplication (L_1) $k(L_2)$ hold
$\Rightarrow V_2$ is a vector space over K

Each vector of V_2 is perfectly described by the coordinates of its ending point.

• $\vec{u_1} \longleftrightarrow (x_1, y_1)$

• $\vec{u_2} \longleftrightarrow (x_2, y_2)$

• $\vec{u_1} + \vec{u_2} \longleftrightarrow (x_1+x_2, y_1+y_2)$

• $\vec{u} \longleftrightarrow (x, y)$

• $k\vec{u} \longleftrightarrow (kx, k\cdot y)$

$\Rightarrow \exists$ bijection (isomorphism) between V_2 and $\mathbb{R}^2 \overset{not}{=} \mathbb{R} \times \mathbb{R}$

$\Rightarrow$ ($\mathbb{R}^2$ is a vector space over $\mathbb{R}$)

$\Rightarrow$ similarly, one can show that the set V_3 of all vectors in space having a fixed origin define a vector space over K. ($V_3 \langle\cong\rangle \mathbb{R}^3$)

(b) Let $n \in \mathbb{N}^*$. Define $(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1+y_1, \dots, x_n+y_n)$

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

$\forall (x_1, \dots x_n), (y_1, \dots y_n) \in K^n$, $\forall k \in K$

⇒ then K^n is a vector space over K, called the canonical vector space.

(c) Let $\{e\}$ be a single element set. Consider the only possible $e+e=e$ and the only scalar multiplication $k \cdot e = e$, $\forall k \in K$

That $\{e\}$ is a vector space over K, called the trivial vector space and we denote it by $\{0\}$.

(d) Let $m, n \in \mathbb{N}$, $m, n \geq 2$. Then $M_{m,n}(K)$ is a vector space over K with respect to the usual addition of matrices and scalar multiplication of matrices.

$[M_{m,n}(K)$ ans $K^{m \cdot n}]$

(e) $K[X]$ is a vector space over K, with respect to the usual addition and scalar multiplication of polynomials.

Denote by $K_n[X]$ the set of all polinomials with the $= \{f \in K[X] \mid \text{degree}(f) \in \mathbb{N}\}$. Then $K_n[X]$ is a vector space over K.

↑ otherwise we don't have an operation

$[K_n[X]$ ans $K^{n+1}]$

(f) Let $A \neq \emptyset$ be a set. Consider $K^A = \{f : A \to K \mid f \text{ function}\}$

Define $\forall f, g \in K^A$, $\forall k \in K$

$f+g \in K^A$, $(f+g)(x) = f(x)+g(x)$

$k \cdot f \in K^A$, $(k \cdot f)(x) = k \cdot f(x)$, $\forall x \in A \Rightarrow K^A$ is a vector over K

- Proprieties:

Theorem: Let V be a vector space over K. Then:

(i) $k \cdot 0_V = 0_V = 0_K \cdot v$

(ii) $k(-v) = -kv = (-k) \cdot v$

(iii) $k(v_1 - v_2) = kv_1 - kv_2$

(iv) $(k_1 - k_2)v = k_1 \cdot v - k_2 \cdot v$ $\forall k_1, k_2, k \in K$, $v, v_1, v_2 \in V$

Proof: (i) $k \cdot v = k(0+v) = k \cdot 0 + k \cdot v \mid + (-kv)$

$\Leftrightarrow 0 = k \cdot 0$

$k \cdot v = (0+k)v = 0 \cdot v + k \cdot v \mid + (-k \cdot v)$

$\Leftrightarrow 0 = 0 \cdot v$

(ii) $k \cdot (u_1 - u_2) + k \cdot u_2 =$

$= k(u_1 - u_2 + u_2)$

$= k(u_1 + 0) = k \cdot u_1 \;| + (-k \cdot u_2)$

$\Rightarrow k \cdot (u_1 - u_2) = k u_1 - k u_2$

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

$$k \cdot u = 0 \iff k = 0 \text{ or } u = 0$$

Proof: ($\Rightarrow$) Assume $k \cdot u = 0$. If $k = 0$ we are done.

$$\text{If } k \neq 0, \quad k^{-1} \cdot (k \cdot u) = k^{-1} \cdot 0$$

$$\Leftrightarrow (k^{-1} \cdot k) \cdot u = 0$$

$$\Leftrightarrow 1 \cdot u = 0 \Leftrightarrow u = 0$$

($\Leftarrow$) This follows by the previous Theorem (i)

2. SUBSPACES

Def.: Let V be a vector space over K and $S \subseteq V$.

Then S is called a subspace of V if $\begin{cases} S \neq \emptyset \quad (0 \in S) \\ \forall u_1, u_2 \in S, \; u_1 + u_2 \in S \\ \forall k \in K, \; u \in S, \; k \cdot u \in S \end{cases}$

not. $S \leq_K V$ Obs.! Any subspace is a subgroup.

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

$$S \leq_K V \iff \begin{cases} S \neq 0 \\ \forall k_1, k_2 \in K, \; \forall u_1, u_2 \in S, \; k_1 \cdot u_1 + k_2 \cdot u_2 \in S \end{cases}$$

Ex.: (a) A vector space V over K has the subspaces $\{0\}$ and V.

(b) The subspaces of the $\mathbb{R}$ vector space V_2 are the following ones:

- $\{0\}$
- any line passing through 0
- V_2

Lecture 4: General problem:

Given a set X of vectors in a vector space over K. Find the smallest subspace of V containing X.

Lemma: Let V be a vector space over K and $X \leq V$ for $i \in I$. If X_i is a subspace for V, $X_i \leq_K V$, $\forall i \in I$, then their intersections are also a subspace,

$$\bigcap_{i \in I} X_i \leq_K V$$

Proof: • $\forall i \in I$, $X_i \leq V \Rightarrow \forall i \in I$, $0 \in V_i \Rightarrow 0 \in \bigcap_{i \in I} X_i$

• Let $k_1, k_2 \in K$ and $v_1, v_2 \in \bigcap_{i \in I} X_i$

$\Rightarrow v_1, v_2 \in X_i$, $\forall i \in I$

$X_i \leq_K V$, $\forall i \in I$

$\Rightarrow k_1 v_1 + k_2 v_2 \in X_i$, $\forall i \in I$

$\Rightarrow k_1 v_1 + k_2 v_2 \in \bigcap_{i \in I} X_i$ Hence $\bigcap_{i \in I} X_i \leq_K V$

Def.: Let V be a vector space over K and $X \leq V$.

Denote $\langle X \rangle = \bigcap \{ S \leq_K V \mid X \subseteq S \}$ ($\leq_K V$ comma)

$\langle X \rangle$ is called the subspace of V generate by the set X and it is the smallest subspace of V containing X.

X is called generating set for $\langle X \rangle$

If $X = \{v_1, v_2, \dots v_n\}$ then we denote $\langle v_1, \dots v_n \rangle = \langle \{v_1, \dots v_n\} \rangle$

Remark: $\langle \emptyset \rangle = \{0\}$ (being a subspace is containing 0)
(Who is the smallest subspace of the empty set!)

Def.: Let V be a vector space over K. Then V is called finitely generated if $\exists v_1, \dots, v_n \in V$ such that $V = \langle v_1, \dots, v_n \rangle$. In what follows, we should only refer to finitely generated vector spaces.

An expression of the form $k_1 v_1 + \dots + k_n v_n$ with $k_1, \dots k_n \in K$ and $v_1, \dots v_n \in V$, is called a linear combination of $v_1, \dots, v_n$

Theorem: Let V be a vector space and $\emptyset \neq X \subseteq V$.

Then! $\langle X \rangle = \{ k_1 v_1 + \dots + k_n v_n \mid k_1, \dots k_n \in K, v_1, \dots v_n \in V \in X, n \in \mathbb{N}^* \}$

that is a set of all finite linear combinations of vectors from K.

Corollary: Let V be a vector space over K and $v_1, \dots v_m \in V$.

Then! $\langle v_1, \dots v_m \rangle = \{ k_1 v_1 + \dots + k_m v_m \mid k_1, \dots k_m \in K \}$

Example: Consider the canonical vector space $\mathbb{R}^3$ over $\mathbb{R}$. Compute the subspace generated of $\langle v_1, v_2, v_3 \rangle$, where $v_1 = (1,0,0)$, $v_2 = (0,1,0)$, and $v_3 = (0,0,1)$

$$\langle v_1, v_2, v_3 \rangle = \{ k_1 \cdot (1,0,0) + k_2 (0,1,0) + k_3 (0,0,1) \mid k_1, k_2, k_3 \in \mathbb{R} \}$$
$$= \{ (k_1, 0, 0) + (0, k_2, 0) + (0, 0, k_3) \mid k_1, k_2, k_3 \in \mathbb{R} \}$$
$$= \{ (k_1, k_2, k_3) \mid k_1, k_2, k_3 \in \mathbb{R} \} = \mathbb{R}^3$$

also we can say that $\mathbb{R}^3$ is finitely generated.

Def.: Let V be a vector space over K and $S, T \leq_K V$.

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

Then $S+T$ is called the sum of subspaces S, T.

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

Example: $\mathbb{R}^2 = S \oplus T$ where $S = \{ (x, 0) \mid x \in \mathbb{R} \}$
$T = \{ (0, y) \mid y \in \mathbb{R} \}$

Theoreme: Let V be a vector space over K and $S, T \leq_K V$. Then

$S+T = \langle S \cup T \rangle$, hence $S+T \leq_K V$.

Proof: (⊆) Suppose that $v \in S+T \Rightarrow v = s+t$, where $s \in S$, $t \in T$.

$v = 1 \cdot s + 1 \cdot t \in \langle S \cup T \rangle$

(⊇) Suppose that $v \in \langle S \cup T \rangle$

$\Rightarrow v = \sum_{i=1}^{n} k_i \cdot v_i$, where $k_1, \dots k_n \in K$, $v_1, \dots, v_n \in V$

$\Rightarrow v = \sum_{i \in I} k_i \cdot v_i + \sum_{j \in J} k_j \cdot v_j$, where $I = \{ i \in \{1, \dots, n\} \mid v_i \in S \}$, $J = \{1, \dots n\} \setminus I$

denote that: $(I \cup J = \{1, \dots, n\}) \xrightarrow[S \leq_K V]{(1)} v \in S+T$
$T \leq_K V$

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

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

3. LINEAR MAPS

Def.: Let $f: V \to V$ be a function between two vector spaces V and V over K.

Then f is called a K-linear map if:

- $f(v_1 + v_2) = f(v_1) + f(v_2)$ $\quad \forall v_1, v_2, v \in V$
- $f(k_i \cdot v) = k_i \cdot f(v)$ $\quad \forall k_i \in K$

A K-linear map $f: V \to V'$ is called:

- isomorphism if f is bijective
- endomorphism if $V = V'$
- automorphism if $V = V'$ and f bijective

Notation: $\mathrm{Hom}_K(V, V')$ - the set of all K-linear maps between V and V'

$\mathrm{End}_K(V)$ - the set of all endomorphisms of V

$\mathrm{Aut}_K(V)$ - the set of all automorphism of V

Theorem: Let $f: V \to V'$ be a function between two vectors spaces V, V' over K. Then f is a K-linear map $\Leftrightarrow$

$$f(k_1 v_1 + k_2 v_2) = k_1 \cdot f(v_1) + k_2 \cdot f(v_2),$$

$\forall k_1, k_2 \in K$, $v_1, v_2 \in V$

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

Then $\boxed{\mathrm{Ker}\, f} = \{v \in V \mid f(v) = 0'\}$ is called the kernel of f

and $\boxed{\mathrm{Im}\, f} = \{f(v) \mid v \in V\}$ is called the image of f.

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

Then: $\mathrm{Ker}\, f \leq_K V$ and $\mathrm{Im}\, f \leq_K V'$

Proof: • $0 \in \mathrm{Ker}\, f$, because $f(0) = 0'$. Not that f is a group homomorphism between the groups $(V, +)$ and $(V', +) \Rightarrow f(0) = 0'$)

• Let $k_1, k_2 \in K$ and $v_1, v_2 \in \mathrm{Ker}\, f \Rightarrow f(v_1) = 0'$, $f(v_2) = 0'$. We show that $k_1 \cdot v_1 + k_2 \cdot v_2 \in \mathrm{Ker}\, f$. We have $f(k_1 v_1 + k_2 v_2) = \underbrace{k_1 \cdot f(v_1)}_{0'} + \underbrace{k_2 f(v_2)}_{0'}$

$\Rightarrow k_1 v_2 + k_2 \cdot v_2 \in \mathrm{Ker}\, f$, Hence $\mathrm{Ker}\, f \leq_K V$

• $0' \in \mathrm{Im}\, f$, because $0' = f(0)$

• Let $k_1, k_2 \in K$ and $v_1', v_2' \in \mathrm{Im}\, f$. We show that $k_1 \cdot v_1' + k_2 v_2' \in \mathrm{Im}\, f$

(1) $\Rightarrow v_1' = f(v_1)$, $v_2' = f(v_2)$ for some $v_1, v_2 \in V$.

We have $k_1 \cdot v_1' + k_2 \cdot v_2' = k_1 \cdot f(v_1) + k_2 \cdot f(v_2) = f(k_1 v_1 + k_2 \cdot v_2) \in \mathrm{Im}\, f$

Hence $\mathrm{Im}\, f \leq_K V'$

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

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

2.h. Linear ~~ant~~ independence and basis

Def.: Let V be a vector space over K and $v_1, \dots v_n \in V$. Then $v_1, \dots v_n$ are called **linearly independent** ($\{v_1, \dots v_n\}$ is linear independent) if

$\forall k_1, k_2, \dots k_n \in K$ such that $k_1 v_1 + \dots + k_n v_n = \vec{0}$ we have $k_1 = \dots k_n = 0$

! Also $v_1, \dots v_n$ are called **linear dependent** if they are **not** linearly independent

$\exists k_1, \dots k_n \in K$ not all zero, such that $k_1 \cdot v_1 + \dots + k_n v_n = 0$

Remarks: (1) One vector $v \in V$ is linearly independent $\Leftrightarrow v \neq 0$

$\{ k \cdot v = 0 \Rightarrow k = 0$
$\uparrow$
$v \neq 0$

(2) Any set of vectors containing 0 is linearly dependent.

Theorem: Let V be a vector space over K and $v_1, \dots v_n \in V$. Then $v_1, \dots v_n$ are linearly dependent ($\Rightarrow$ one of them can be written as a linear combination of the others, that is, $\exists j \in \{1, \dots, n\}$ such that $v_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i \cdot v_i$!

Proof: ($\Rightarrow$) assume that $v_1, \dots v_n$ are linearly dependent

$\Rightarrow \exists k_1, \dots k_n \in K$ not all zero such that $k_1 \cdot v_1 + \dots k_n + k_n = 0$

$\Rightarrow \exists j \in \{1, \dots, n\}$ such that $k_j \neq 0$

$\Rightarrow k_1 v_1 + \dots k_{j-1} \cdot v_{j-1} + k_j \cdot v_j + k_{j+1} \cdot v_{j+1} + \dots + k_n v_n = 0$

$\Rightarrow k_j v_j = -\sum_{\substack{i=1 \\ i \neq j}}^{n} k_i \cdot v_i$

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

$\Rightarrow v_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} -k_j^{-1} \cdot k_i \cdot v_i$

($\Leftarrow$) Assume that $\exists j \in \{1, \dots, n\}$ such that $v_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i \cdot v_i$; ($v_1 = k_1 v_2 + k_3 v_3$)

$\Rightarrow -v_j + \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i \cdot v_i = 0$

$\Rightarrow \underbrace{(-1)}_{\neq 0} \cdot v_j + \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i \cdot v_i = 0$

$\Rightarrow v_1, \dots, v_n$ are linearly independent

Examples:

(a) Consider that real vector space V_2

- $v \in V_2$ is lin. dependent $\Leftrightarrow v = 0$
- $v_1, v_2 \in V_2$ are lin dependent $\Leftrightarrow$ $v_1, v_2 \in V$ are linear dependent $\Leftrightarrow$ v_1, v_2 collinear ($v_1 = k \cdot v_2$ or $v_2 = k v_1$)
- 3 or more vectors in V_2 are always linearly dependent

(b) Consider the canonical vector space K^n over K

Let $v_1 = (1, 0, 0, \dots 0)$

$v_2 = (0, 1, \dots 0)$

$\vdots$

$v_n = (0, 0, \dots n) \in K^n$

Let $k_1, \dots k_n \in K$ such that $k_1 \cdot v_1 + \dots + k_n v_n = 0$

$\Rightarrow k_1(1, 0, \dots 0) + k_2(0, 1, 0, \dots 0) + \dots + (k_n(a_0, \dots a_n)) = (0, 0, \dots, 0)$

$\Rightarrow (k_1, 0, \dots 0) + (0, k_2, \dots 0) + \dots + (0, \dots, k_n) = (0, 0 \dots, 0)$

$\Rightarrow (k_1, k_2, \dots k_n) = (0, 0, \dots 0)$

$\Rightarrow k_1 = k_2 = \dots = k_n = 0$

Hence $v_1, \dots v_n$ are linearly independent in K^n.

* **Theorem:** (i) Two vectors in K^n are linearly dependent ($\Leftrightarrow$) the components of the vectors are respectively proportional.

(ii) n vectors in $K^{(n)}$ are linearly dependent !

Proof: Clear: (ii) Let $v_1, \dots v_m \in K^n$ be linearly dependent

$\Rightarrow v_1 = (x_{11}, x_{21}, \dots x_{m1}) \in K^n$

$\dots$

$v_1 = (x_{1n}, x_{2m}, \dots x_{nm})$

(*) $k_1, \dots k_m \in K$ not all zero such that $k_1 v_1 + \dots + k_m \cdot v_m = 0$

$k_1 v_1 + \dots + k_m v_m = 0$

$k_1(x_{11}, x_{21}, \dots y_{m1}) + \dots + k_m(y_{1m}, x_{2n}, \dots y_{mn}) = (0, 0 \dots, 0) \in K^n$

$k_1 x_{11} + \dots + k_m y_{1m} = 0$

$\dots$ has a non zero sol by (*)

$k_n x_{i1} + \dots$

Def.2) By a list of vectors in a vector space V over K we mean an n-tuple $(v_1, \dots v_n)$ with $v_1, \dots v_n \in V$

Def.3) Let V be a vector space over K. A list of vectors $(v_1, \dots v_n)$ from V is called a basis of V if

(i) B is a linearly independent in V

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

Theorem: Every vector space has a basis (in general, not unique)

Proof: Case I: $V = \{0\}$ has bases $\emptyset$

Case II $\forall \neq \{0\}$, $\exists$ $B \neq \emptyset \subseteq V$ such that $V = \langle B \rangle$ ($\exists$ e.g. $B = V$)

If B is linearly indep., then B is a bases of V and we are done.

If B is linear dep., then $\exists j \in \{1, \dots, n\}$ such that v_j is a linear combination of the other vectors from B

$\Rightarrow V = \langle B \rangle = \langle v_1, \dots v_n \rangle = \langle v_1, \dots, v_{j-1}, \dots, v_n \rangle = \langle B \setminus \{v_j\} \rangle$

If $B \setminus \{v_j\}$ is lin. independent, then $B \setminus \{v_j\}$ is a base of V and we are done.

If $B \setminus \{v_j\}$ is lin. dependent, then we continue the algorithm.

If we don't finish the algorithm before, then we get to $V = \langle v_j \rangle_{j \in J}$, for some $J \in \{1, \dots, n\}$. Since $V \neq \{0\}$, $v_j \neq 0 \Rightarrow v_j$ is lin. indep.

$\Rightarrow \{v_j\}$ is a bases of V.

Theorem: Let V be a vector space over K and $B = (v_1, \dots, v_n)$ be a list of vectors from V. Then B is a basis of $V \Leftrightarrow \forall v \in V, \exists! k_1, \dots k_n \in K$ such that $v = k_1 v_1 + \dots + k_n v_n$

they are called the coordinates of v in basis B

Proof: $\Rightarrow$ Assume that B is a bases of $V \Rightarrow V = \langle B \rangle \Rightarrow$

$\Rightarrow \forall v \in V, \exists k_1, \dots, k_n \in K$ such that $v = k_1 \cdot v_1 + \dots + k_n v_n$ (1)

Uniqueness: suppose that we also have $v = k_1' v_1 + \dots + k_n' v_n$, $k_1', \dots k_n' \in K$ (2)

$(k_1 - k_1') v_1 + \dots + (k_n - k_n') v_n = 0$ (3)

(by subtracting (2) from (1))

B basis $\Rightarrow v_1, \dots v_n$ are lin. independent $\xrightarrow{(3)} k_1 - k_1' = \dots = k_n - k_n' = 0$

$\Rightarrow k_i = k_i' \quad \forall i \in \{1, \dots, n\}$

(2⇐) Assume that every vector of V can be uniquely written as a linear combination of the vectors from B. $\Rightarrow V = \langle B \rangle$

We will have to show that B is linearly independent in V

Let $k_1, \dots k_n \in K$ be such that

$$\left.\begin{array}{l} k_1 v_1 + \dots + k_n v_n = 0 \\ 0 \cdot v_1 + \dots + 0 \cdot v_n = 0 \end{array}\right\} \xrightarrow{\text{uniqueness}} k_1 = 0, \dots k_n = 0. \text{ Hence } B \text{ is lin. indep} \Rightarrow$$

$\Rightarrow B$ basis of V

Ex.: (a) Consider the real vectors space V_3. Then $(\vec{i}, \vec{j}, \vec{k})$ is a basis of V_3

(b) Consider the canonical vector space ${}_K K^n$

$$\begin{cases} e_1 = (1, 0, \dots 0) \\ e_2 = (0, 1, \dots 0) \\ \vdots \\ e_n = (0, \dots 1) \end{cases} \in K^n$$

Then $E = (e_1, \dots e_n)$ is a basis of ${}_K K^n$ because $\forall v = (x_1, \dots x_n) \in K^n$ can be uniquely written as: $v = x_1 e_1 + \dots + x_n e_n$

E is called the canonical basis of ${}_K K^n$.

Note that the coordinates of a vector in K^n in the canonical basis E coincide with its components.

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

$f \in K_n[X] \Rightarrow f = a_0 1 + a_1 X + \dots + a_n X^n$, $a_0, \dots a_n \in K$ (uniquely!)

$\Rightarrow (1, X, \dots X^n)$ is a basis of ${}_K K_n[X]$

(d) Let ${}_K M_2(K)$. Then a basis of ${}_K M_2(K)$ is:

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

In ${}_K M_{m,n}(K)$ we have a similar basis with $m \times n$ matrices (...)