3.10.2019

Algebra Course 1

Linear Algebra

Structure : Chapter 1 - Preliminaries
Chapter 2 - Vector spaces
Chapter 3 - Matrices and Linear Sistems
Chapter 4 - Coding Theory - introduction

Bibliography

1. N. Both, S. Crivei
„Culegere de probleme de algebră"
Lito UBB, Cluj, 1996

2. G. Călugăreanu, „Lecții de algebră liniară", Lito UBB, Cluj 1995

Courses
3. S. Crivei, „Basic abstract algebra"
Casa ~~Editurii~~ Cărții de Știință, Cluj,
2002, 2003

4. G. Gilbert, L. Gilbert - „Elements of modern algebra, PWS Kent,
Boston 1992

Chapter 4 * 5. W. J. Gilbert, W. K Nicholson -
„Modern algebra with Applications"
John Wiley, 2004

6. I Purdea, C. Pelea - „Probleme de algebră"

Seminar : - min. attendance : 75%

- bonus points - up to 0.5p (5x0.1p)
- bonus projects - course : up to 1p (5x0.2p)

Exam

Partial exam 1: Week 8

Partial exam 2: Week 14

Final grade:

$$G = 1 + \underset{4p}{P_1} + \underset{5p}{P_2} + \underset{\text{bonus}}{B}$$

Chapter 1 Preliminaries

1 Relations

Def By a (binary) relation we mean a triple:

$r = (A, B, R)$, where A, B are sets and $R \subseteq A \times B$

A — domain, B — codomain, R — graph; $A \times B = \{(a,b) \mid a \in A, b \in B\}$

if $A = B$ then r is called homogeneous

Def Let $r = (A, B, R)$ be a relation and $X \subseteq A$

then $r(X) \overset{not}{=} \{b \in B \mid \exists x \in X : (x, b) \in R\}$

called the relation class of X with respect to R

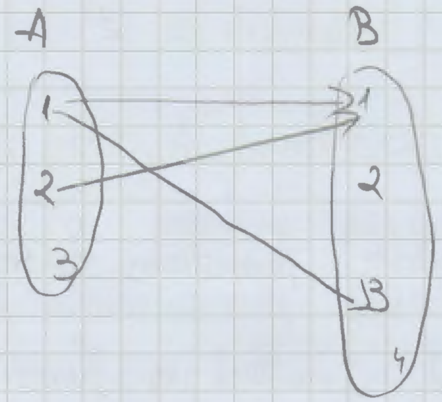
if $X = \{x\}$ then we denote $r\langle x\rangle \overset{not}{=} r(\{x\}) =$
$= \{b \in B \mid (x, b) \in R\}$

Notation $(a, b) \in R \equiv a \; r \; b$

Remark: In case of relations defined on finite sets we may use diagrames to picture that

$r = (A, B, R)$ $\quad A = \{1, 2, 3\}$ $\quad B = \{1, 2, 3, 4\}$

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



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

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

Ex a) $r = (C, P, R)$

C – the set of children

P – the set of parents

$R = \{(c,p) \in C \times P \mid c \text{ is a child of } p\}$

b) $r = (\mathbb{R}, \mathbb{R}, R)$

$R = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$

c) divisibility of – on $\mathbb{N}, \mathbb{Z}$

paralelism – $\parallel$, $\perp$ on lines, $\equiv$ $\sim$ on Δ

d) $\varnothing(A, B, \varnothing)$ – the void relation

$u = (A, B, A \times B)$ – the universal relation

e) $\delta_A = (A, A, \Delta_A)$

$\Delta_A = \{(a,a) \mid a \in A\}$ – the equality relation

f) Every function is a relation

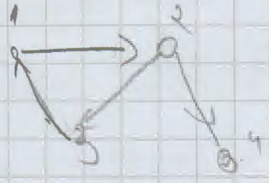
$f: A \to B \rightsquigarrow (A, B, G_f)$

where $G_f = \{(a, f(a)) \mid a \in A\}$

g) Every directed graph is a relation

V – set of vertices

T - set of vertices; E - set of edges -> (V, V, E)



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

$E = \{(1,2), (2,3), (2,4), (3,1)\}$

$\boxed{2}$ Functions – how do we relate functions to relations?

Def: A relation $r = (A, B, R)$ is called a function if ~~for elem~~ $\forall a \in A$, $|r\langle a\rangle| = 1$

number of elem $r\langle a\rangle$

$f : A \to B$

$\forall a \in A \quad |f\langle a\rangle| = 1$

this unique elem. will be $f(a)$

Ex – relation that is not a function, check Remark

Homework: recall: injective, surjective, bijective

$\boxed{3}$ Equivalence relations and partitions

Def Equivalence relations

$r = (A, A, R)$ is called an equivalence relation if it take the following 3 properties

(r) reflexivity: $\forall a \in A$, $a \, r \, a$

(t) transitivity: $a, b, c \in A$ with $a \, r \, b$ and $b \, r \, c$, we have $a \, r \, c$

(s) symetry $\forall a, b \in A$ with $a \, r \, b$, we have $b \, r \, a$

Notation $E(A)$ – the set of equivalence relations on a set A

a. $\delta_A = (A, A, \Delta_A) \in E(A)$ equality

b. $\equiv$ of triangles is ~~an~~ equivalence relation on a set of Δ

<u>Def</u> Let $A \neq \emptyset$ be a set

By a ~~partion~~ partition on A we mean a family $(A_i)_{i\in I}$ of non-empty subsets of A such that:

- $\bigcup_{i\in I} A_i = A$
- $\forall\, i,j \in I,\ i \neq j$, we have $A_i \cap A_j = \emptyset$

Notation: $P(A)$ the set of all partitions on a set A

<u>Ex</u> (a) $A = \{1,2,3,4\}$

$\{A_1, A_2, A_3\}$ is a partition of A if:

$A_1 = \{1,2\}$

$A_2 = \{3\}$

$A_3 = \{4\}$

(b) O - the set of odd integers

E - the set of even integers

$\{O, E\}$ is a partition of $\mathbb{Z}$

(c) $\{\{x\} \mid x \in \mathbb{Z}\}$ - is a partition of $\mathbb{Z}$

Theorem:

(1) Let r be $r \in E(A)$

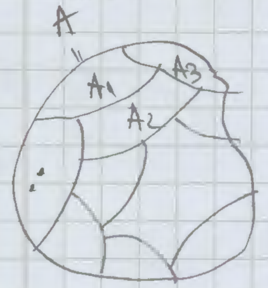
Denote $A/r \overset{not}{=} \{r\langle a\rangle \mid a \in A\}$ - the quotion set of a by r

then $A/r \in P(A)$

(2) Let $\pi = (A_i)_{i\in I} \in P(A)$. Define a relation r_π on A by

def

$x, y \in A \ , \ x \, r_{\bar{\pi}} \, y \overset{\text{def}}{\iff} \exists \, i \in I : x, y \in A_i$



Then $r_{\bar{\pi}}$ is an equivalent relation on set A

$r_{\bar{\pi}} \in E(A)$

(3) There exists a bijection

$F : E(A) \to P(A) \ , \quad F(r) = A/r$

with inverse

$G : P(A) \to E(A) \ , \ G(\bar{\pi}) = r_{\bar{\pi}}$

10.10.2019

Course 2

$\boxed{4}$ Operations (composition law)

Definition : by an operation or composition law on a set A we mean a function

$f : A \times A \to A$

Example : "+" is an operation on all numerical sets

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

"$-$" is an op. on $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

"$\cdot$" is an op on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

"$/$" is an op on $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$

Definition: Let $(A, \cdot)$ be a set together with an operation

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

(Commutative law) $\forall a, b \in A \quad a \cdot b = b \cdot a$

(Identity law) $\exists \, e \in A$ s.t $a \cdot e = e \cdot a = a$

(Symmetric law) For any a from A exists a' from A such that a*a'=a'*a=e, where exists e from A identity element

Lemma: Let $(A, \cdot)$

(i) The identity element is unique

(ii) Assume that " $\cdot$ " is associative and $a \in A$ has a symmetric. Then a has a unique symmetric

Definition let $(A, \cdot)$ and $B \subseteq A$

Then B is called a stable subset (B is closed under " $\cdot$ " in A) is $\forall b_1, b_2 \in B$, $b_1 \cdot b_2 \in B$

Another point of view

$\varphi : A \times A \to A$, $B \subseteq A$ stable subset

$\forall b_1, b_2 \in B$, $\varphi(b_1, b_2) \in B$

$\Rightarrow \varphi' = \varphi|_{B \times B} : B \times B \to B \Rightarrow \varphi|_{B \times B}$ is an op. on B

Remark: Assoc. law, commutative law transfer to stable subsets (they are defined by using only the quantifier $\forall$)

ex $(\mathbb{Z}, +)$, $\mathbb{N} \subseteq \mathbb{Z}$ is a stable subset

$\boxed{5}$ Groups and rings

Definition let $(A, \cdot)$

Then it is called:

(i) semigroup if " $\cdot$ " associative

(ii) monoid if " $\cdot$ " associative and $\exists$ identity elem.

(iii) group if " $\cdot$ " associative

$\exists$ identity elem.

all elem. are symmetrical

have a symmetric (inverse

If "$\cdot$" is also commutative, we have a commutative semigroup, monoid, group

A commutative group is also called <u>abelian</u>.

Remark: The identity elem. will usually be denoted by 1 and the inverse of an elem. $a \in A$ will usually be denoted by a^{-1}.

Examples: (a) "$-$" is ~~not~~ associative on $\mathbb{Z}$

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

(c) $(\mathbb{N}, +)$ is a monoid but not a group

(d) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ are groups.

$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ are groups

(e) Let $A = \{e\}$ be a single-elem. set

exists unique $\exists!$ op on A defined by $e \cdot e = e$

$(\{e\}, \cdot)$ is a group called the trivial group

(f) Let $n \in \mathbb{N}$, $n \geq 2$. Then

$(\mathbb{Z}_n, +)$ is an abelian group

where $\forall \hat{x}, \hat{y} \in \mathbb{Z}_n$,

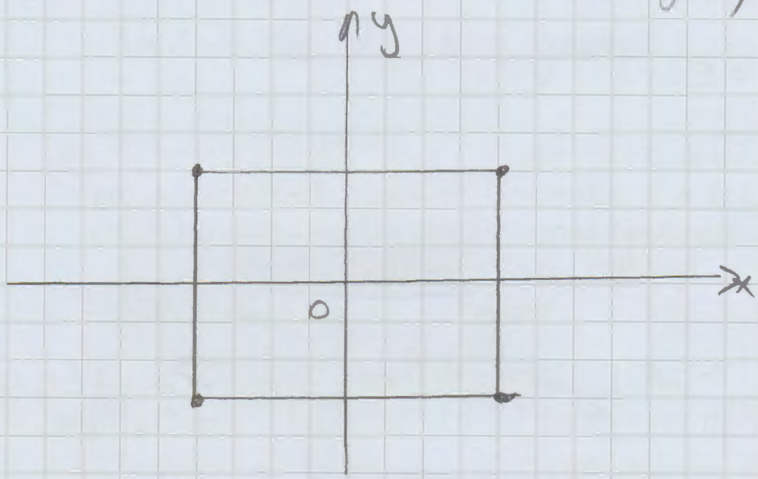
$$\hat{x} + \hat{y} = \widehat{x+y}$$

This is called - the group of residue classes modulo n

(g) Let $K = \{e, a, b, c\}$ and consider the operation given by 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

$\Rightarrow$ $(K, \cdot)$ is an abelian group Klein's group



Definition let $(A, +, \cdot)$ (a set A together with 2 op denoted by "$+$", "$\cdot$")

Then it is called a:

(i) Ring if $\begin{cases} (A,+) \text{ is an abelian group} \\ (A,\cdot) \text{ is a semigroup} \\ \forall a,b,c \in A \quad a\cdot(b+c) = a\cdot b + a\cdot c \\ \qquad\qquad\qquad (b+c)\cdot a = b\cdot a + c\cdot a \end{cases}$

(distributive laws)

(ii) unitary ring (ring with identity)

if $(A,+,\cdot)$ ring where $(A,\cdot)$ monoid

we denote by 1 the identity elem)

exp $\to$ (iii) division ring (or skew field)

if $\begin{cases} (A,+) \text{ abelian group (w. identity 0)} \\ (A^*, \cdot) \text{ group } (A^* = A \text{ without the identity elem}) \\ \qquad\qquad\qquad A \setminus \{0\} \\ \text{Distributive laws} \end{cases}$

(iv) field (comp comutativ) if

it is a commutative division ring

Ex (a) $(\mathbb{Z}, +, \cdot)$ is a commutative unitary ring

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

(c) Let $A = \{e\}$ be a single elem set

we define $e + e = e$

$e \cdot e = e$

$\Rightarrow (\{e\}, +, \cdot)$ is a commutative unitary ring called a trivial ring

(d) Let $n \in \mathbb{N}$, $n \geq 2$. we define on $\mathbb{Z}_n$ the op

$$\hat{x} + \hat{y} = \widehat{x+y} \qquad \forall \hat{x}, \hat{y} \in \mathbb{Z}_5$$
$$\hat{x} \cdot \hat{y} = \widehat{x \cdot y}$$

then $(\mathbb{Z}_n, +, \cdot)$ is a commutative unitary ring

(note that $(\mathbb{Z}_n, +, \cdot)$ field $\Leftrightarrow$ n prime)

(e) Let $(R, +, \cdot)$ be a commutative unitary ring != {0}

Then $(R[X], +, \cdot)$ is a commutative unitary ring

polynomials with coefficients in R

(f) Let $(R, +, \cdot)$ be a ring, $n \geq 2$ $n \in \mathbb{N}$

Then $(M_n(R), +, \cdot)$ is a ring

$\boxed{6}$ Subgroups and subrings

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

Then $H \subseteq G$ is called a subgroup (denote $H \leq G$) if

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

Theorem The following are equivalent for a group $(G, \cdot)$ and $H \leq G$

(1) $H \leq G$

(2) i) $H \neq \emptyset$ $(1 \in H)$

(2) i) H != null set, (1 belongs to H)
ii) For any x, y from H, x*y^-1 is also in H

(3) (i) H stable subset

(ii) $(H, \cdot)$ is a group

<u>ex</u>: (a) Let $(G, \cdot)$ be a group. Then $\{1\}$ and G are subgroups of $(G, \cdot)$

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

Definition Let $(R, +, \cdot)$ be a ring

Then $A \subseteq R$ is called a subring (denoted $A \leq R$) if

$$\begin{cases} A \neq \emptyset & (0 \in A) \\ \forall x, y \in A, & x - y \in A \\ \forall x, y \in A, & x \cdot y \in A \end{cases}$$

Let $(K, +, \cdot)$ be a field. Then $A \subseteq K$ is a subfield (denoted $A \leq K$) if

$$\begin{cases} |A| \geq 2 & (0, 1 \in A) \\ \forall x, y \in A, & x - y \in A \\ \forall x, y \in A \text{ with } y \neq 0, & x \cdot y^{-1} \in A \end{cases}$$

Theorem: Let $(R, +, \cdot)$ be a ring (field). Then $A \subseteq R$ is a subring (subfield) if:

(i) A stable subset of $(R, +, \cdot)$

(ii) $(A, +, \cdot)$ ring (field)

Example (a) Let $(R, +, \cdot)$ be a ring. Then $\{0\}$, R are subrings of $(R, +, \cdot)$

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

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

(c) $2\mathbb{Z} \overset{\text{not}}{=} \{2k \mid k \in \mathbb{Z}\}$ is a subring of $(\mathbb{Z}, +, \cdot)$ without identity

HW - recall group/ring homo morphism (isomorphism)

Course 3 17. 10-2019

Chapter 2: Vector spac

1 Basic definition, examples and properties

Def Let $(K, \oplus, \cdot)$ be a field

By a K-vector space (or K-linear space, or vector spac over K) we mean: an abelian group $(V, \oplus)$ together with so-called "external operation"

+ not the same

$$\varphi : K \times V \to V$$

$$\varphi(k, v) \overset{not}{=\!=} k \cdot v \quad ! \text{ not-commutative}$$

satisfying the axioms:

$(L1)$ $k \cdot (v_1 + v_2) = k \cdot v_1 + k \cdot v_2$

$(L2)$ $(k_1 + k_2) \cdot v = k_1 v + k_2 \cdot v$

(L_3) $(k_1 \cdot k_2) \cdot v = k_1 \cdot (k_2 \cdot v)$

(L_4) $1 \cdot v = v$

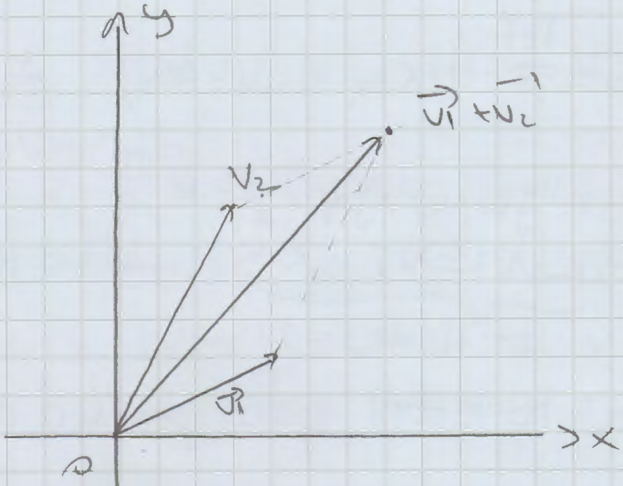
$\forall\, k, k_1, k_2 \in K,\ \forall\, v, v_1, v_2 \in V$

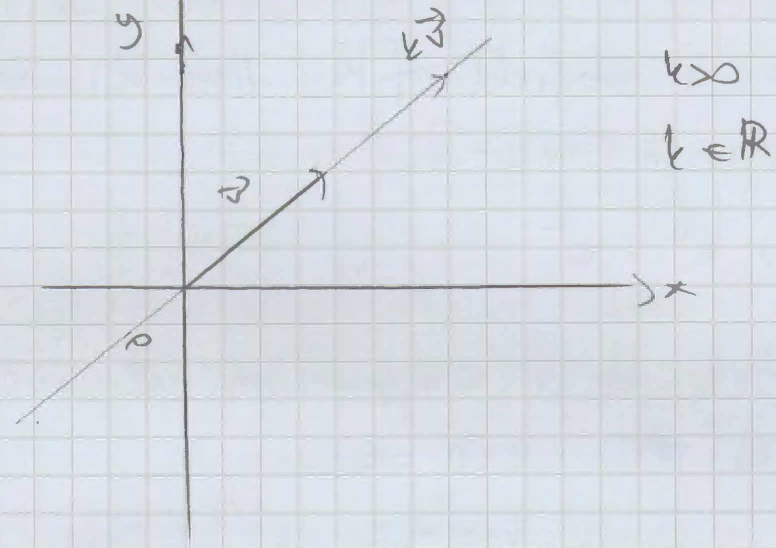
The elements of V are called vectors and the elem of K are called <u>scalars</u>.

Notation ${}_K V$ (or $(V, K, +, \cdot)$)

left K vect spaces

<u>Ex</u> (a) Let V_2 be the set of all vectors (from Physics) in plane having the origin in a fixed point O of the plane





$$\left.\begin{array}{l}\vec{v_1} \longleftrightarrow (x_1; y_1) \\ \vec{v_2} \longleftrightarrow (x_2; y_2)\end{array}\right\} \Rightarrow \vec{v_1}+\vec{v_2} \longleftrightarrow (x_1+x_2, y_1+y_2)$$

$$\vec{v} \longleftrightarrow (x,y) \Rightarrow k\cdot\vec{v} \longleftrightarrow (k\cdot x, k\cdot y)$$

$V_2 \longleftrightarrow \mathbb{R}\times\mathbb{R} \overset{\text{not}}{=} \mathbb{R}^2$; V_2 is an $\mathbb{R}$ vector space

Similarly, the set V_3 of all vectors in space having the origin in a fixed point O form an $\mathbb{R}$-vector space

(b) Let K be a field and $n\in\mathbb{N}^*$. We define

- $(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) \overset{\text{def}}{=}$

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

• $k \cdot (x_1, \dots, x_n) \overset{def}{=} (k \cdot x_1, \dots, k \cdot x_n)$

$\forall (x_1, \dots, x_n), (y_1, \dots, y_n) \in K^n$ ← V dif'ni'tie

(where $K^n = \underbrace{K \times K \times \dots \times K}_{n \text{ times}}$), $\forall k \in K$

Then K^n is a K-vector space, called the canonical K-vector space

(c) Let A be a subfield of K. Then K is an A-vector space (the op are the same ; "+")

eg. ${}_{\mathbb{Q}}\mathbb{R}$, ${}_{\mathbb{R}}\mathbb{C}$, ${}_{\mathbb{Q}}\mathbb{C}$

(d) Let $V = \{e\}$ be a single-elem. set and K a field. We define: $e + e = e$

$k \cdot e = e$, $\forall k \in K$

Then $V = \{e\}$ is a K-vector space, called the trivial K vector space, and we denote it by $\{0\}$

(e) Let $m, n \in \mathbb{N}$ $m, n \geq 2$

Define on $M_{m,n}(K)$

(the set of all matrices $m \times n$ with entries in K) the usual addition and multiplication by a scalar

Then $M_{m,n}(K)$ is a K-vector space

(f) Let $K[x]$ be the set of all polynomials with coefficients in a field K. Define on $K[x]$ the usual addition and scalar multiplication

Then $K[x]$ is a K vector-space

<u>Theorem</u> Let V be a K-vector space. Then:

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

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

(iii) $k \cdot (v - v') = kv - k \cdot v'$ $\quad \forall k, k_1, k_2 \in K$

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

Proof (i) • $k \cdot 0 + k \cdot v \overset{L_4}{=} k \cdot (0 + v) =$

$= k \cdot v$

$k \cdot 0 + k \cdot v = k \cdot v \quad | -k \cdot v$

$k \cdot 0 = 0$

• $0 \cdot v + k \cdot v \overset{L_2}{=} (0 + k) \cdot v = k \cdot v$

$0 \cdot v + k \cdot v = k \cdot v \quad | -k \cdot v$

$0 \cdot v = 0$

(ii) • $k \cdot (-v) + k \cdot v \overset{L_1}{=} k(-v + v) = k \cdot 0 \overset{(i)}{=} 0$

$k \cdot (-v) + k \cdot v = 0 \quad | -k \cdot v$

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

• $(-k) \cdot v + k \cdot v = (-k + k) \cdot v = 0 \cdot v \overset{(i)}{=} 0.$

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

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

(iii) $k \cdot (v - v') + k \cdot v' \overset{L_1}{=} k(v - v' + v') = k \cdot v$

$k \cdot (v - v') + k \cdot v' = k \cdot v$

$k(v - v') = k \cdot v - k \cdot v'$

(iv) Similarly

Theorem 2 Let V be a K-vector space and $v \in V, k \in K$

Then $k \cdot v = 0 \iff k = 0$ or $v = 0$

(no 0 divisors)

proof „$\Leftarrow$" By theorem 1

„$\Rightarrow$" Assume that $k \cdot v = 0$

if $k=0$, then we are done

assume $k \neq 0 \Rightarrow \exists k^{-1} \in K$

$k \cdot v = 0 \quad | \cdot k^{-1}$

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

$(k^{-1} \cdot k) \cdot v = 0$ by theorem 1 and L_3

$1 \cdot V = 0$

$\overset{L(4)}{\Longrightarrow} \quad V = 0$

[2] Subspaces

<u>Def</u> Let V be a K vector space and $S \subseteq V$

Then S is called a subspace of $_K V$ iff

$$\begin{cases} S \neq \emptyset \\ \forall v_1, v_2 \in S \quad v_1 + v_2 \in S \\ \forall k \in K, \forall v \in S, k \cdot v \in S \end{cases} \quad \text{not } S \leq_K V$$

Theorem Let V be a K-vector space and $S \subseteq V$

Then S is a subspace of $V \Leftrightarrow$

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

$\Leftrightarrow$ $\begin{cases} S \text{ is a stable subset of } V \text{ w.r.sp to "+" \& "}\cdot\text{" } \\ \text{scalars} \\ S \text{ is a } K\text{-vector space} \end{cases}$

Example: (a) Let V be a K-vectorspace. Then $\{0\}$ and V are subspaces of V

(b) Consider the real vector space V_2

Its subspaces are the following:

$\begin{cases} \bullet \ \{0\} \\ \bullet \ \text{any line passing through (the origin) } O \\ \bullet \ V_2 \end{cases}$

The subspaces of V_3:

$\begin{cases} \bullet \ \{0\} \\ \bullet \ \text{Any line passing through } O \\ \bullet \ \text{any plane passing through } O \\ \bullet \ V_3 \end{cases}$

(c) Let $n \in \mathbb{N}$ Denote

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

Then $K_n[x] \leq_K K[x]$

Theorem Let V be a K-vector space 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 • $0 \in \bigcap_{i \in I} S_i$

Let $k_1, k_2 \in K$ and $v_1, v_2 \in \bigcap_{i \in I} S_i \Rightarrow \left. \begin{array}{l} v_1, v_2 \in S_i, \ \forall i \in I \\ S_i \leq_K V \end{array} \right\} \Rightarrow$

th

$\Rightarrow k_1 \cdot v_1 + k_2 \cdot v_2 \in S_i \quad \forall i \in I \Rightarrow k_1 \cdot v_1 + k_2 \cdot v_2 \in \bigcap_{i \in I} S_i$

Hence set intersection Si, i from I <= kV (intersection = reversed U)

Rk: The union of subspaces is <u>NOT</u> a subspace in general

- for instance, take the union of 2 lines passing through O in V_2

24. 10. 2019

<u>Course 4</u>

<u>General problem</u> $V \to K$ v.s. X vectors in V

Given a set of vectors X in a K vector space V, complete it in a minimal way with some other vectors in order to get a subspace of V

<u>Def</u>: Let V be a K-vector space and $X \subseteq V$

Then, we denote

$$\langle X \rangle \overset{not}{=} \bigcap \{ S \leq_K V \mid X \subseteq S \}$$

Note that $\langle X \rangle \leq_K V$ because it is an intersection of subspaces of V. Also, note that $\langle X \rangle$ is the "smallest" (with respect to inclusion) subspace of V containing X

$\langle X \rangle$ - the subspace generated by X. In this setting, X is called a generating set for $\langle X \rangle$.

If $V = \langle X \rangle$ for some $X \subseteq V$, then V is said to be generated by X

If X is finite, then V is called finitely generated

When $X = \{ a \}$, then we denote $\langle a \rangle = \langle \{ a \} \rangle$

$X = \{ v_1, \dots, v_n \}$ $\quad \langle v_1, \dots, v_n \rangle = \langle \{ v_1, \dots, v_n \} \rangle$

Remark: $<\emptyset> = \{0\}$

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

$$<X> = \{ k_1 \cdot v_1 + \dots + k_n \cdot v_n \mid k_1, \dots, k_n \in K, \; v_1, \dots, v_n \in X, \; n \in \mathbb{N}^* \}$$

- the set of all finite linear combinations of vectors from X $(k_1 \cdot v_1 + \dots + k_n \cdot v_n)$

Proof: Denote $L = \{ k_1 \cdot v_1 + \dots + k_n \cdot v_n / k_1, \dots, k_n \in K, v_1, \dots, v_n \in X, n \in \mathbb{N}^* \}$

In order to show that $<X> = L$, it is enough to prove that L is the smallest subspace of V containing X.

Step 1: $L \leq_K V$

- $L \neq \emptyset$, because $\exists\, v \in X \neq \emptyset$ and $0 = 0 \cdot v \in L$
- Let $k, k' \in K$ and $v, v' \in L$.

We prove that $k \cdot v + k' \cdot v' \in L$

We have $v = \sum_{i=1}^{n} k_i \cdot v_i$, $v' = \sum_{j=1}^{m} k_j' \cdot v_j$

$\Rightarrow k \cdot v + k' \cdot v' = \sum_{i=1}^{n} (k \cdot k_i) \cdot v_i + \sum_{j=1}^{m} (k' \cdot k_j') \cdot v_j \in L$

Hence $L \leq_K V$

Step 2: $X \subseteq L$

We have $\forall v \in X \neq \emptyset$

$v = 1 \cdot v \in L$

Hence $X \subseteq L$

Step 3: We show that if $S \leq_K V$ with $X \subseteq S$, then $L \subseteq S$

Let $S \leq_K V$ with $X \leq S$

$\Rightarrow \forall v_1, \ldots, v_n \in X, \forall k_1, \ldots k_n \in K$,
we have $k_1 \cdot v_1 + \ldots + k_n \cdot v_n \in S$ because $S \leq_K V$

Hence any finite linear combination of vectors from X belongs to S

$\Rightarrow L \subseteq S$

Corollary: Let V be a K-vector space and $v_1, \ldots, v_n \in V$

Then $\langle v_1, \ldots, v_n \rangle = \{ k_1 v_1 + \ldots + k_n v_n \mid k_1, \ldots, k_n \in K \}$

Example: Consider the canonical (real) vector space $\mathbb{R}^3$ and $v_1 = (1,0,0)$
$v_2 = (0,1,0)$
$v_3 = (0,0,1)$

$\Rightarrow \langle v_1, v_2, v_3 \rangle = \{ k_1 \cdot v_1 + k_2 v_2 + k_3 \cdot v_3 \mid k_1, k_2, k_3 \in \mathbb{R} \}$

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

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

Hence $\mathbb{R}^3$ is a finitely generated $\mathbb{R}$-vector space

General problem:

Decompose a vector space into subspaces

Def Let V be a K vector-space and $S,T \leq_K V$

Then $S+T \overset{not}{=} \{ s+t / s\in S,\ t\in T \}$

is called the sum of S and T

Theorem Let V be a K-vector space and $S,T \leq_K V$

Then $S+T = \langle S \cup T \rangle$ In particular, $S+T$ is a subspace of V $(S+T \leq_K V)$

Proof: $\boxed{\subseteq}$ Let $v \in S+T \Rightarrow v = s+t$ for some $s\in S$ and $t \in T$

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

$\boxed{\supseteq}$ Let $v \in \langle S \cup T \rangle$ Then $v = \sum_{i=1}^{n} k_i \cdot v_i$ for some

$v_i \in S \cup T$

Denote $I = \{ i \in \{1,\dots,n\} / v_i \in S \}$, $J = \{1,\dots,n\} \setminus I$

$v = \underbrace{\sum_{i\in I} k_i \cdot \underset{\underset{S}{\cap}}{v_i}}_{\underset{S}{\cap}} + \underbrace{\sum_{j\in J} k_j \cdot \underset{\underset{T}{\cap}}{v_j}}_{\underset{T}{\cap}} \in S+T$ (we've used $S,T \leq_K V$)

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

Then we denote $V = S \oplus T$ if $V = S+T$ and $S\cap T = \{0\}$

In this case, we say that V is the <u>direct sum</u> of S,T

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

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

Proof: $\boxed{\Longrightarrow}$ Suppose that $V = S \oplus T \Rightarrow$

$\Rightarrow V = S + T$ and $S \cap T = \{0\}$

$\Rightarrow \forall v \in V$, $\exists s \in S$ and $t \in T$ such that $v = s + t$

For uniqueness, assume that $\exists s' \in S$ and $t' \in T$ such that
$v = s' + t'$

$$\Rightarrow s + t = s' + t' \Rightarrow \underbrace{s - s'}_{\in S} = \underbrace{t' - t}_{\in T} \in S \cap T = \{0\}$$

$$\Rightarrow \begin{cases} s = s' \\ t = t' \end{cases}$$

$\boxed{\Longleftarrow}$ suppose that $\forall v \in V, \exists! s \in S, t \in T$ s.t
$v = s + t$

We show that $S \cap T = \{0\}$

let $v \in S \cap T$

$$v = \underset{\in S}{v} + \underset{\in T}{0} = \underset{\in S}{0} + \underset{\in T}{v} \xrightarrow{\text{unigness}} v = 0 \Rightarrow S \cap T = \{0\}$$

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

$$\forall (x, y) \in \mathbb{R}^2, (x, y) = \underset{\in S}{(x, 0)} + \underset{\in T}{(0, y)} \in S + T$$

$S \cap T = \{(0, 0)\}$

Using the theorem: $\forall (x, y) \in \mathbb{R}^2$, $\exists!$ $s \in S$ and $t \in T$
s.t $(x, y) = s + t$

$(x, y) = (a, 0) + (0, b)$

$(x, y) = (a, b)$

3 Linear maps

Definition: Let V and V' be K vector spaces. Then $f: V \to V'$ is called a K-linear map if:

$$\begin{cases} \forall v_1, v_2 \in V,\ f(v_1+v_2) = f(v_1) + f(v_2) \\ \forall k \in K,\ \forall v \in V,\ f(k \cdot v) = k \cdot f(v) \end{cases}$$

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

- isomorphism if it is bijective
- endomorfism if $V = V'$
- automorfism if $V = V'$ and f bijective

Notation

- We denote $V \simeq V'$ if $\exists$ isomorphism between V and V'
- $End_K(V)$ - the set of all endomorphisms of V
- $Aut_K(V)$ - the set of all automorphisms of V

Remark. Every K-linear map $f: V \to V'$ is a group homomorphism between the abelian groups $(V, +)$ and $(V', +)$

$\Rightarrow f(0) = 0'$ and $f(-v) = -f(v)$ $\forall v \in V$

Theorem $f: V \to V'$ is a K-linear map $\Leftrightarrow \forall k_1, k_2 \in K$, $\forall v_1, v_2 \in V$ $f(k_1 v_1 + k_2 v_2) = k_1 f(v_1) + k_2 f(v_2)$

Example: Let $S \leq_K V$. Then $i: S \to V$, $i(u) = u$ is a K linear map called the inclusion K-linear map

Course 5

Recall:

Definition: Let $f: V \to V'$ be a function beetwen K-vector spaces V and V'. Then f is called a K-linear map if $\forall v_1, v_2 \in V$, $f(v_1+v_2) = f(v_1) + f(v_2)$

$\forall k \in K, \forall v \in V, f(k \cdot v) = k \cdot f(v)$

$\Leftrightarrow \forall k_1, k_2 \in K, \forall v_1, v_2 \in V, f(k_1 v_1 + k_2 v_2) = k_1 f(v_1)+k_2 f(v_2)$

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

$\mathrm{Ker} f \overset{not}{=} \{ v \in V \mid f(v) = 0' \}$ is called the kernel (nucleul) of f

$\mathrm{Im} f \overset{not}{=} \{ f(v) \mid v \in V \}$ is called the image of f

Theorem: Let $f: V \to V'$ be a K-linear map. Then $\mathrm{Ker} f \leq V$ and $\mathrm{Im} f \leq V'$

Proof: • $0 \in \mathrm{Ker} f$, because $f(0) = 0'$

• Let $k_1, k_2 \in K$ and and $v_1, v_2 \in \mathrm{Ker} f$

We show that $k_1 v_1 + k_2 v_2 \in \mathrm{Ker} f$

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

$= k_1 \cdot 0' + k_2 \cdot 0' = 0'$

Hence $\mathrm{Ker} f \leq V$

• $0' = f(0) \in \mathrm{Im} f$

• Let $k_1, k_2 \in V$ and $v_1', v_2' \in \mathrm{Im} f$

We have $k_1 \cdot v_1' + k_2 \cdot v_2' = k_1 \cdot f(v_1) + k_2 \cdot f(v_2)$ for some

for some v1, v2 in V (because v1', v2' in Im f)

$= f(k_1 \cdot v_1 + k_2 \cdot v_2) \in \operatorname{Im} f$

Hence $\operatorname{Im} f \leq V'$

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

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

$\boxed{14}$ Linear independence and basis

$f(x)$

Definition : Let V be a K-vector space and $v_1, \dots, v_m \in V$. Then $v_1, \dots, v_m$ are called <u>linearly independent</u> (or $\{v_1, \dots v_m\}$ is linearly independent) if for every $k_1, \dots, k_m \in K$ s.t.

$$k_1 v_1 + \dots + k_m v_m = 0 \quad \text{we must have } k_1 = \dots = k_m = 0$$

The vectors $v_1, \dots, v_m \in V$ are called <u>linearly dependent</u> if they are not linearly independent, that is, $\exists k_1, \dots k_m \in K$ <u>not</u> all zero such that

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

Theorem Let V be a K-vector space and $v_1, \dots, v_m \in V$. Then $v_1, \dots, v_m$ are linearly dependent $\Leftrightarrow$

$\exists \ j \in \{1, \dots, m\}$ s.t.

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

Proof: $\boxed{\Longrightarrow}$ Assume that $v_1, \dots, v_m$ are linearly dependent $\Rightarrow \exists \ k_1, \dots, k_m \in K$ <u>not</u> all zero. such that $k_1 \cdot v_1 + \dots + k_m \cdot v_m = 0 \Rightarrow \exists \ j \in \{1, \dots, m\}$ s.t. $k_j \neq 0$ and

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

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

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

$\boxed{\Leftarrow}$ Assume that $\exists j \in \{1, \dots, n\}$ s.t.

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

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

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

This is a linear combination of ~~the~~ $v_1, \dots, v_n$ equal to 0 but not all scalars are $0 \Rightarrow v_1, \dots, v_n$ lin. dependent

Theorem: let $n \in \mathbb{N}$, $n \geq 2$

(i) 2 vectors in the canonical vector space K^n are linearly dependent $\Leftrightarrow$ if their components are respectively proportional

(ii) n vectors in ${}_K K^n$ are linearly dependent $\Leftrightarrow$ if the determinant consisting of their components is zero

Proof: (i) let $v_1, v_2 \in K^n$, say $v_1 = (x_{11}, x_{21}, \dots x_{n1})$
$v_2 = (x_{12}, x_{22}, \dots, x_{n2})$

$\overset{Th}{\Rightarrow}$ one of them is a linear combination of the Other one say $v_1 = k \cdot v_2$

$$(x_{11}, \dots x_{n1}) = k \, (x_{12}, \dots x_{n2})$$

$$\Rightarrow \begin{cases} x_{11} = kx_2 \\ \dots \quad \dots \\ x_{n1} = k \, x_{n2} \end{cases}$$

(ii) Let $\begin{cases} v_1 = x_{11}, \dots, x_{n1} \\ v_2 = x_{12}, x_{22}, \dots, x_{n2}) \\ \vdots \\ v_n = (x_{1n}, x_{2n}, \dots x_{nn}) \end{cases}$

$v_1, \dots, v_n$ are linearly dependent in K^n

$\Leftrightarrow$ $k_1, \dots, k_n \in K$ not all zero s.t.

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

$k_1 (x_{11}, x_{21}, \dots, x_{n1}) + \dots + k_n (x_{1n}, x_{2n}, \dots x_n) = (0, \dots 0) \in K^n$

$\Leftrightarrow \exists \, k_1, \dots k_n \in K$ not all zero s.t

$$(S) \begin{cases} k_1 \cdot x_{11} + \dots + k_n x_{1n} = 0 \\ \dots \\ k_1 x_{1n} + \dots + k_n x_{nn} = 0 \end{cases}$$

$\Leftrightarrow$ determinant of (S) is zero

<u>Examples</u> (a) Consider the real vector space V_2

- v linearly dependent $\Leftrightarrow v = 0$
- v_1, v_2 linearly dependent $\Leftrightarrow v_1, v_2$ are collinear
- any 3 vect in K are linearly dependent

Consider ${}_{\mathbb{R}}V_3$

- v linearly dependent $\Leftrightarrow$ $v = 0$
- v_1, v_2 $\Leftrightarrow v_1, v_2$ col.
- v1, v2, v3 <=> v1,v2, v3 are in the same plane

• any 4 (or more) vectors in V_3 are linearly dependent

(b) Consider ${}_K K^n$. Let

$e_1 = (1, 0, \dots, 0)$
$e_2 = (0, 1, \dots, 0)$ $\quad \in K^n$
$\dots$
$e_n = (0, 0, \dots, 1)$

let $k_1, \dots, k_n \in K$ s.t.
$k_1 e_1 + \dots + k_n e_n = 0$
$\Rightarrow k_1(1, \dots, 0) + k_2(0, 1, \dots, 0) + \dots + k_n(0, \dots, 1) = (0, \dots, 0) \in K^n$
$\Rightarrow k_1 = \dots = k_n = 0$
Hence $e_1, \dots, e_n$ are linearly independent

c) Let ${}_K M_2(K)$ Then

$E_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ $E_2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ ..

are linearly independent

(d) Let ${}_K K_n[X] = \{ f \in K[X] \mid \deg(f) \leq n \}$

Then $1, X, X^2, \dots X^n$ are l. independent

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

Theorem: Any vector space has (at least) a basis

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

are called the coord. of v in the basis B

Proof: $\boxed{\Rightarrow}$ Assume that B is a basis of V

$\Rightarrow \begin{cases} B \text{ is l. independent in } V \\ V = \langle B \rangle \end{cases}$

$\Downarrow$

$\forall v \in V, \exists \, k_1,\dots,k_n \in K$ s.t. $v = k_1 v_1 + \dots + k_n v_n$ (1)

- for uniqueness, suppose that we also have
  $v = k_1' \cdot v_1 + \dots + k_n' v_n$ (2)

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

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

$\xRightarrow[\text{independent}]{B \text{ is linearly}} \begin{cases} k_1 - k_1' = 0 \\ \vdots \\ k_n - k_n' = 0 \end{cases} \Rightarrow k_i = k_i', \forall i \in \{1,\dots,n\}$

$\boxed{\Leftarrow}$ Assume that $\forall v \in V, \exists! \, k_1,\dots,k_n \in K$ s.t.
$v = k_1 \cdot v_1 + \dots + k_n \cdot v_n$

$\Rightarrow V = \langle B \rangle$

We prove that B is linearly independent

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

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

but $0 = 0 \cdot v_1 + \dots + 0 \cdot v_n$

Uniqueness of writing 0 as a linear comb

but 0=0*v1+...+0*vn

$\Rightarrow k_1 = \ldots = k_m = 0$

Hence B is linearly independent and so B is a basis of V

<u>Examples</u> (a) Consider ${}_K K^n$ (canonical)

Then $E = (e_1, \ldots, e_n)$ is a basis of ${}_K K^n$,

where $\begin{cases} e_1 = (1, 0, \ldots 0) \\ \ldots \\ e_n = (0, \ldots, 1) \end{cases}$

E is linearly independent and K^n is generated by E

($K^n = \langle E \rangle$) because $\forall (x_1, \ldots, x_n) \in K^n$, $v = x_1 e_1 + \ldots + x_n e_n$

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

(b) Consider ${}_{\mathbb{R}}V_2$ ($\simeq {}_{\mathbb{R}}\mathbb{R}^2$)

$\begin{cases} \vec{i} = (1, 0) \\ \vec{j} = (0, 1) \end{cases}$ form a basis of ${}_{\mathbb{R}}V_2$

Consider ${}_{\mathbb{R}}V_3$

$(\vec{i}, \vec{j}, \vec{k})$ basis of ${}_{\mathbb{R}}V_3$, where $\vec{i} = (1, 0, 0)$, $\vec{j} = (0, 1, 0)$, $\vec{k} = (0, 0, 1)$

(c) Consider ${}_K M_2(K)$

(E_1, E_2, E_3, E_4) is a basis of $M_2(K)$

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

(d) Consider ${}_K K_n[X]$

$(1, X, X^2, \ldots X^n)$ is a basis of ${}_K K_n[X]$

because $\forall f \in K_n[X]$, $\exists!\, a_0, \ldots, a_n \in K$ s.t.

f = a0*1+a1*x+...+anx^n

Course 6

Partial exam
21^{st} Nov. 2019
13. 50
Courses 1-6
Seminars 1-7
4p → 1p theory
→ 3p ex

5 Dimension

Theorem (STEINITZ)
Let V be a K-vector space
$X=(x_1,\dots,x_m)$ be a linearly independent list in V,
$Y=(y_1,\dots,y_n)$ be a system of generators for V. Then

- $m \le n$
- m vectors from Y may be replaced by the vectors of X obtaining again a syst. of generators for V.

Corollary. Any 2 basis of K-vector space have the same number of vectors (we consider finitely generated K-vector spaces)

Proof. Let $B=(v_1,\dots,v_m)$, $B'=(v_1',\dots,v_n')$ be basis of a K vector space

$\left.\begin{array}{l} B \text{ is linearly independent} \\ B' \text{ is a system of generators} \end{array}\right\} \xRightarrow{\text{Steinitz}} m \le n$

$\left.\begin{array}{l} B' \text{ is linearly independent} \\ B \text{ is a system of generators} \end{array}\right\} \xRightarrow{\text{Steinitz}} n \le m$

Hence $n=m$

Definition: By the dimension of a K-vector space V, we mean the number of vectors of any of its bases

Notation $\dim_K V$

Examples:

(a) Consider the trivial K vector space $V = \{0\}$

Then $\emptyset$ is a basis of V so $\dim_K V = 0$

(b) Consider ${}_{\mathbb{R}}V_3$ ($\underset{\mathbb{R}}{\simeq} \mathbb{R}^3$)

Its subspaces are:

- V_3 : $\dim_{\mathbb{R}} V_3 = 3$

(a basis is $\vec{i}, \vec{j}, \vec{k}$)

- any plane passing through 0

$\rightarrow \dim_{\mathbb{R}} V_3 = 2$

- any line passing through 0

$\rightarrow \dim_{\mathbb{R}} V_3 = 1$

- $\{0\}$ $\rightarrow \dim_{\mathbb{R}} \{0\} = 0$

(c) Consider the canonical K-vector K^n. It has the canonical basis $E = (e_1, \dots, e_n)$, where $e_1 = (1, 0, \dots, 0)$

$\dots\dots$

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

$\Rightarrow \dim_K K^n = n$

(d) $\dim_K M_{m,n}(K) = m \cdot n$

(e) $\dim_K K_n[X] = n+1$ (a basis is $(1, X, X^2, \dots, X^n)$)

Theorem Let V be a K-vect space. The following are equivalent

(i) $\dim_K V = n$

(ii) The maximum number of linearly independent vectors in V is n

(iii) The minimum number of vectors of a system of generators for V is n.

Proof: $\boxed{(i) \Rightarrow (ii)}$ Suppose that $\dim_K V = n$

So V has a basis $B = (v_1, \dots, v_n)$

$\Rightarrow \exists$ linearly independent list with n vectors, namely B

Let $X = (x_1, \dots, x_m)$ be a linearly independent list in V

View B as a system of generators for V

$\xRightarrow{\text{Steinitz}} m \leq n$

$\boxed{(ii) \Rightarrow (i)}$ Suppose that the max. number of linearly independent vectors in V is n

Consider a basis $B = (v_1, \dots, v_m)$ of $V \Rightarrow \dim_K V = m$

$$\left.\begin{array}{l} \text{View } B \text{ as linearly independent list} \xRightarrow[\text{hypothesis}]{} m \leq n \\ \text{View } B \text{ as a system of generators} \xRightarrow[\text{Steinitz}]{} n \leq m \end{array}\right\} \Rightarrow m = n$$

$\boxed{(i) \Leftrightarrow (iii)}$ Homework

Theorem. Let V be a K-vector space with $\dim_K V = n$. Let $X = (u_1, \dots, u_n)$ be a list in V. Then X is linearly independent in $V \Leftrightarrow X$ is a system of generators for V

Proof. $\boxed{\Rightarrow}$ Suppose that X is linearly independent in V

Let $B = (v_1, \dots, v_n)$ be a basis of $V \Rightarrow B$ is a system of generators for V

Steinitz $\Longrightarrow$ n vectors from B (so all of them) may be replaced by the vectors of X obtaining again a system of generators

$\Rightarrow$ X is a system of generators for V

$\boxed{\Longleftarrow}$ Suppose that X is a system of generators

Assume that X is linearly dependent

$\Rightarrow \exists\, j \in \{1, \dots, n\}$ s.t. $\boxed{u_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i \cdot u_i}$

We have $V = \langle X \rangle = \langle u_1, \dots, u_n \rangle \overset{!}{=}$

$\overset{!}{=} \langle u_1, \dots, u_{j-1}, u_{j+1}, \dots, u_n \rangle \Rightarrow$

$\Rightarrow V$ has a system of generators with $n-1$ vectors

But $\dim_K V = n \Rightarrow$ the min. number of vectors in a syst. of generators for V is n

$\Rightarrow$ contradiction. Hence X is linearly independent

<u>Corollary</u> n vectors in the canonical K-vector space K^n form a basis $\Leftrightarrow$ they are linearly independent

$\Leftrightarrow$ the det. of their components is non-zero

<u>Theorem</u>: Let V be a K vector space, and $S \leq_K V$

(i) Any linearly independent list in V can be completed to a basis of V

(ii) Any basis of S can be completed o a basis of V

(iii) $\dim_K S \leq \dim_K V$

(iv) $\dim_K S = \dim_K V \Leftrightarrow S = V$

Proof: (i) Let $X = (u_1, \dots, u_m)$ be a linearly independent list in V. Let $B = (v_1, \dots, v_n)$ be a basis of V

Steinitz $\Rightarrow m \leq n$ and m vectors from B can be replaced by those from X obtaining again a system of generators for V.

By reordering them if necessary, let us assume that the first m vectors from B are replaced by those of X. $\Rightarrow (u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ is a system of generators

$\left.\begin{array}{l} \\ \text{but } \dim_K V = n \end{array}\right\} \Rightarrow (u_1, \dots, u_m, v_{m+1}, \dots, v_n)$ is

linearly independent in V $\Rightarrow$ it is a basis of V

<u>Corollary</u> Let V be a K v.s. and $S \leq_K V$
Then $\exists\, \bar{S} \leq_K V$ s.t. $V = S \oplus \underset{\substack{\uparrow \\ \text{complement of } S}}{\bar{S}}$

Proof: Let $B = (u_1, \dots, u_m)$ be a basis of S
$B' = (v_1, \dots, v_n)$ be a basis of V

Complete B as a basis of V
$(u_1, \dots, u_m, v_{m+1}, \dots, v_n)$

Then $\bar{S} = \langle v_{m+1}, \dots, v_n \rangle$ [...]

<u>Theorem</u> Let V and V' be K v.s. Then $V \simeq V' \Leftrightarrow$
$\dim_K V = \dim_K V'$

Corollary. Let V be a K.v.s. with $\dim_K V = n$

Then $V \simeq K^n$

$\boxed{6}$ Dimension formulas

Theorem (1^{st} dimension formula)

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

$\dim_K V = \dim_K \operatorname{Ker} f + \dim_K \operatorname{Im} f$.

Theorem (2^{nd} dimension formula)

Let V be a K.v.s., $S, T \leq_K V$

Then $\dim_K S + \dim_K T = \dim_K (S+T) + \dim_K (S \cap T)$