Structures

An algebraic structure is a set + operation (internal law)

$A : S \times S \to S$, $(x,y) \to x * y$ — set

+ associativity $\forall x,y,z \in S \quad (x*y)*z = x*(y*z)$ — semigroup

+ neutral element. $\exists e \in S$ s.t. $x*e = e*x = x$ + unique — monoid

ex. $(\mathcal{M}_n(\mathbb{R}), \cdot), (\mathbb{Z}_7, \cdot), (A^A, \circ)$

+ invertability $\forall x \in S: \exists x' \in S : x*x' = e$ — group

ex: $(\mathbb{Z}, +), (\mathcal{M}_n(\mathbb{R}), \cdot), (\mathbb{Z}^2, +), (\mathbb{Z}_7^*, \cdot)$

+ commutativity $\forall x, y \in S : \quad x*y = y*x$ — abelian group

R - set ; $+, \cdot$ are operations on R

$(R, +)$ - abelian group

$(R, \cdot)$ - semigroup

+ distributivity $\forall x,y,z \in R : \quad x(y+z) = xy + xz$

$(y+z)\cdot x = yx + zx$ — $(R, +, \cdot)$ ring

+ "$\cdot$" has a neutral element ex: $(\mathcal{M}_n(\mathbb{R}), +, \cdot), (\mathbb{Z}, +, \cdot), (\mathbb{Z}_6, +, \cdot)$ — unital ring

+ "$\cdot$" has every el. invertable $\forall x \in R, x \neq 0 \ \exists x' \in R \quad x' \cdot x = x \cdot x' = e$

+ "$\cdot$" commutative — division ring

$\Rightarrow$ field ex: $(\mathbb{Z}_n, +, \cdot)$ for n prime, $(\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot), (\mathbb{Q}, +, \cdot)$

Thm Euclidean division

K - field

$f, g \in K[x]$, $g \neq 0$

$\exists\, q, r \in K[x]$ with $\deg r < \deg g$ s.t. $f = g \cdot q + r$

Relations, functions, equivalence relations & partitions

$\mathcal{r} = (A, B, R)$ a triple where A, B are sets and

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

A - domain, B - codomain, R - graph of the relation $\mathcal{r}$

$A = B \Rightarrow \mathcal{r}$ is **homogeneous**

$\mathcal{r}(X) = \{b \in B \mid \exists\, x \in X : x \mathcal{r} b\}$ ⟶ the class of X with respect to $\mathcal{r}$ $(X \subseteq A)$

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

↳ a homogeneous relation called the inequality relation

every function is a relation

$f : A \to B \iff G_f = \{(x,y) \in A \times B \mid y = f(x)\}$, (A, B, G_f) - relation

* A relation $\mathcal{r} = (A, B, R)$ is a function $\iff \forall a \in A : |\mathcal{r}\langle a \rangle| = 1$

↳ for every element in A there is one element in the codomain

* A homogeneous relation $\mathcal{r} = (A, A, R)$ is called:

1) reflexive (r) : $\forall x \in A,\ x \mathcal{r} x$

2) transitive (t) : $x, y, z \in A$, $x \mathcal{r} y$ and $y \mathcal{r} z \Rightarrow x \mathcal{r} z$

3) symmetric (s) : $x, y \in A$, $x \mathcal{r} y \Rightarrow y \mathcal{r} x$

↳ it is called an equivalence relation if $\mathcal{r}$ has all properties (r, t, s)

ex: the equality relation $\mathcal{r} = (A, A, \Delta_A)$

$\Delta_A = \{(a,a) \mid a \in A\}$

$x \equiv y \pmod{n} \iff n \mid (x - y)$

$x \mathcal{r}_{\mathcal{P}} y \iff \exists\, i \in I : x, y \in A_i$ (relation associated to the partition $\mathcal{P}$)

ex: $\mathcal{R} = (A, A, R) \in E(A)$

$A/\mathcal{R} = \{ \mathcal{R}<a> \mid a \in A \} = \{ \{1,2\}, \{1,2\}, \{3\} \}$

$\mathcal{R}<1> = \{1, 2\}$

$\mathcal{R}<2> = \{1, 2\}$

$\mathcal{R}<3> = \{3\}$

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

Operations (composition law)

$(A, \cdot) \rightarrow$ "$\cdot$" is an operation on set A

Let $\gamma : A \times A \rightarrow A$ $B \subseteq A$. B is stable subset if $\forall x, y \in B$ $\gamma(x,y) \in B$

* associativity & commutativity „pass on" in a stable subset, but the identity element & the inverse DO NOT transfer

Groups

$(G, \cdot)$ - group $\Leftrightarrow$
- "$\cdot$" - operation
- "$\cdot$" - associative
- "$\cdot$" - has neutral element

all elements in A are invertable

Subgroups

$H \subseteq G$ is a subgroup of G if $(H, \cdot)$ - group

$H \leq G \Leftrightarrow$

1) $H \neq \emptyset$ $1 \in H$
2) $\forall x, y \in H : x \cdot y \in H$
3) $\forall x \in H \ \exists x^{-1} \in H$

$\Leftrightarrow \forall x, y \in H : x \cdot y^{-1} \in H$

$(\mathbb{Z}, -)$ is not a semigroup because "$-$" is not associative on $\mathbb{Z}$

$GL_n(\mathbb{R}) = \{ A \in \mathcal{M}_n(\mathbb{R}) \mid \det(A) \neq 0 \}$, $(GL_n(\mathbb{R}), \cdot)$ - group general linear group of rank n

* Klein's group ?

ex: $n\mathbb{Z} = \{ n \cdot x \mid x \in \mathbb{Z} \} \leq (\mathbb{Z}, +) \quad \forall n \in \mathbb{N}$

Proof: $n\mathbb{Z} = \{ n \cdot k \mid k \in \mathbb{Z} \} \neq \emptyset$

Let $x, y \in n\mathbb{Z} \Rightarrow x = n \cdot k$, $y = n \cdot l$, $k, l \in \mathbb{Z}$

$\Rightarrow x - y = n \cdot (k - l) \in n\mathbb{Z}$

$SL_n(\mathbb{R}) = \{ A \in \mathcal{M}_n(\mathbb{R}) \mid \det A = 1 \}$

$SL_n(\mathbb{R}) \leq (GL_n(\mathbb{R}), \cdot)$

Rings

$(R, +, \cdot)$ - ring $\Leftrightarrow$ $(R, +)$ - abelian group; $(R, \cdot)$ - semigroup; $\cdot$ distributive

Subrings

$S \subseteq R$ is a subring $(S \leq R)$ if $(S, +, \cdot)$ is a ring

$S \leq R \Leftrightarrow$!

1) $S \neq \emptyset$ $(0 \in S)$ → subgroup of $(R, +)$
2) $(S, +)$ subgroup of R
   $\forall x, y \in S, \ x - y \in S$
3) $(S, \cdot) \leq (R, \cdot)$
   $\forall x, y \in S, \ x \cdot y \in S$

If $(R, +, \cdot)$ - field, to check if S is a subfield you only need to add $\forall x \in S, x \neq 0 : x^{-1} \in S$

$S \leq R \Leftrightarrow$!

1) $|S| \geq 2$ $(0, 1 \in S)$
2) $\forall x, y \in S \quad x - y \in S$
3) $\forall x, y \in S, y \neq 0 \quad x \cdot y \in A$

ex: $(\mathbb{Z}, +, \cdot)$ unitary ring, not field

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

$n\mathbb{Z} \leq (\mathbb{Z}, +, \cdot) : n\mathbb{Z} \neq \emptyset \quad (0 \in n\mathbb{Z})$

$\forall x, y \in n\mathbb{Z} \quad x - y \in n\mathbb{Z}$

$\forall x, y \in n\mathbb{Z}, \quad x = n \cdot k \quad y = n \cdot l \Rightarrow x \cdot y = n(nkl) \in n\mathbb{Z}$

Group Homomorphisms

Let $(G, \cdot)$ and $(G', \odot)$ groups and $f: G \to G'$. f is a:

1) homomorphism if $f(x \cdot y) = f(x) \odot f(y)$
2) isomorphism if is bijective

Thm If $f: G \to G'$ homomorphism:

1) $f(1) = 1'$ (identity element in G')
2) $(f(x))^{-1} = f(x^{-1}) \quad \forall x \in G$

ex: $f: \mathbb{Z} \to \mathbb{Z}$ $f(x) = nx$ homomorphism for $(\mathbb{Z}, +)$

$f: \mathbb{Z} \to \mathbb{Z}_n$ $f(x) = \hat{x}$ —— 11 —— $(\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$

$f: GL_n(\mathbb{R}) \to \mathbb{R}^*$ $f(A) = \det A$ homo for $(GL_n(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$

Ring Homomorphism

$f: (R, +, \cdot) \to (R^*, \oplus, \odot)$

1) ring homomorphism if $\forall x, y \in R$:
$$f(x+y) = f(x) \oplus f(y)$$
$$f(x \cdot y) = f(x) \odot f(y)$$
2) isomorphism if bijective

ex: $f: \mathbb{Z} \to \mathbb{Z}_n$ $f(x) = \hat{x}$ $(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot)$

↳ if $(R, +, \cdot)$ & $(R', +, \cdot)$ rings with identity el. 1 & $1'$ and $f: R \to R'$ homo.

⇒ f is unitary if $\boxed{f(1) = 1'}$

Remark if R & R' are rings $(\exists 1, 1')$ and $f(1) = 1'$ ⇒ unital ring homo

if R & R' are fields & $f: R \to R'$ (field homo) ⟺ $f: R \to R'$ ring homo

Vector spaces

K – field

A K-vector space is an abelian group $(V,+)$ together with an external operation (e.g. $\cdot : V \times V \to V$)

$k \in K$, $v \in V$

$$\odot : K \times V \longrightarrow V \qquad (k,v) \mapsto k \cdot v$$

that satisfy the axioms:

(L1) $k \odot (v_1 \oplus v_2) = k \odot v_1 \oplus k \odot v_2$ — distributivity kinda

(L2) $(k_1 + k_2) \odot v = k_1 \odot v \oplus k_2 \odot v$ — distributivity on the right

(L3) $(k_1 \cdot k_2) \odot v = k_1 \odot (k_2 \odot v)$ — associativity

(L4) $1 \cdot v = v$ — neutral element

→ they involve elements taken from diff. sets

⇒ for a vector space you need
1) an abelian group
2) a field
3) an external operation that satisfies the axioms

ex: 1) the usual vectors in the plane with a fixed origin O $(\mathbb{R}^2, \mathbb{R}, +, \cdot)$ def. as $(x,y) \in \mathbb{R} \times \mathbb{R}$

2) the canonical vectorspace over K

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

for $K = \mathbb{Z}_2$, $\mathbb{Z}_2^n$ is a vectorspace over $\mathbb{Z}_2$

3) $V = \{e\}$: $e + e = e$, $k \cdot e = e$ ⇒ V is the zero vectorspace : $\{0\}$

4) $\mathbb{R}$ – v.s. over $\mathbb{Q}, \mathbb{R}$
$\mathbb{C}$ – v.s over $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

5) $(K[x], K, +, \cdot)$

6) $K^A = \{f \mid f : A \to K\}$ ⇒ $(K^A, K, +, \cdot)$ v.s. : $(f+g)(x) = f(x) + g(x)$
$(kf)(x) = k f(x)$

Subspaces

Let V be a vector space over K and $S \subseteq V$. 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) $\forall k \in K,\ \forall v \in S,\ kv \in S$

$S \leq_K V$ – S is a subspace of the vectorspace V

* every S is a subgroup of $(V,+)$ hence S must contain 0

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

e.g. for $S = \{(x,y,z) \in \mathbb{R}^3 \mid x+y+z = 0\}$, show that $S \leq \mathbb{R}^3$

- $(0,0,0) \in S \neq \emptyset$
- Let $k_1, k_2 \in K$ & $v_1 = (x_1, y_1, z_1)$, $v_2 = (x_2, y_2, z_2) \in S$

$$\Rightarrow k_1 v_1 + k_2 v_2 = k_1(x_1, y_1, z_1) + k_2(x_2, y_2, z_2) =$$

$$= (k_1 x_1, k_1 y_1, k_1 z_1) + (k_2 x_2, k_2 y_2, k_2 z_2) \in \mathbb{R}^3$$

and $(k_1 x_1 + k_2 x_2) + (k_1 y_1 + k_2 y_2) + (k_1 z_1 + k_2 z_2) = k_1 \underbrace{(x_1 + y_1 + z_1)}_{0} + k_2 \underbrace{(x_2 + y_2 + z_2)}_{0}$

$$= 0 \Rightarrow k_1 v_1 + k_2 v_2 \in S$$

* a plane (x,y,z) passing through the origin is not a subspace of $\mathbb{R}^3$ over $\mathbb{R}$
* $\{f \in K[X] \mid \deg(f) = n\}$ is not a subspace of $K[X]$ over K
* $\mathbb{R}^I = \{f \mid f : I \to \mathbb{R}\}$ $I \subseteq \mathbb{R}$ where $(f+g)(x) = f(x) + g(x)$, $(kf)(x) = k f(x)$ $\forall x \in I$

$C(I, \mathbb{R}) = \{f \in \mathbb{R}^I \mid f \text{ cont. on } I\}$

$D(I, \mathbb{R}) = \{f \in \mathbb{R}^I \mid f \text{ deriv. on } I\}$

are subspaces of $\mathbb{R}^I$

We denote $S(V)$ the set of all subspaces of V

Thm Let V be a vector space over K and $(S_i)_{i \in I}$ be a family of subspaces

$$\bigcap_{i \in I} S_i \in S(V)$$

* the union of 2 subspaces does not automatically mean that it results another subspace (e.g. $S = \{(x,0)\}$ $T = \{(0,y)\}$ but $(1,0) + (0,1) \notin S \cup T$)

Generated subspace

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

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

and we call it the subspace generated by X. Here X is called the generating set of $\langle X \rangle$. If $X = \{v_1, \dots, v_n\} \Rightarrow \langle v_1, \dots, v_n \rangle = \langle \{v_1, \dots, v_n\} \rangle$

(1) $\langle X \rangle$ is the smallest subspace of V

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

(3) $S \leq V \Rightarrow \langle S \rangle = S$

Def A vector space is finitely generated if $\exists\, v_1 \dots v_n \in V$ s.t.

$V = \langle v_1, \dots, v_n \rangle$, the set $\{v_1, \dots, v_n\}$ is the system of generators

Def Let V v.s. and $v_1, \dots, v_n \in V$. A finite sum $k_1 v_1 + \dots + k_n v_n$ where $k_i \in K$ is called a linear combination of vectors $v_1, \dots, v_n$

Thm Characterization of the generated subspace

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

$\langle X \rangle = \{ k_1 v_1 + \dots + k_n v_n \mid k_i \in K, v_i \in X \}$ is set of all finite linear comb of vectors of X

e.g. 1) canonical vector-space $\mathbb{R}^3$ $\langle (1,0,0), (0,1,0), (0,0,1) \rangle = \{ k_1(1,0,0) + k_2(0,1,0) + k_3(0,0,1) \mid k_1, k_2, k_3 \in \mathbb{R} \}$

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

↳ generated by 3 vectors $\Rightarrow$ finitely generated

2) $S \leq_K \mathbb{R}^3$ $S = \{ (x,y,z) \in \mathbb{R}^3 \mid x - y - z = 0 \} = \{ (y+z, y, z) \mid y, z \in \mathbb{R} \} = \{ y(1,1,0) + z(1,0,1) \mid y, z \in \mathbb{R} \}$

$= \langle (1,1,0), (1,0,1) \rangle$

Sum of subspaces

Def Let V be v.s. over K and $S, T \leq V$. We define the sum of the subspaces S and T as

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

If $S \cap T = \{0\}$ then $S + T$ is the direct sum of the subspaces S and T

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

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

Linear Maps

Let V and V' be vector spaces over the same field K

A function $f: V \to V'$ is called:

(1) K-linear map if

$$f(v_1+v_2) = f(v_1)+f(v_2)$$
$$f(kv) = kf(v)$$

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

(2) isomorphism if it is bijective

(3) endomorphism if $V = V'$

(4) automorphism if it is bijective and $V = V'$

Properties:

f - group homomorphism $\Rightarrow$ $f(0) = 0'$

$f(-v) = -f(v)\ \forall v \in V$

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

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

$\mathrm{Aut}_K(V) = \{ f: V \to V \mid f \text{ is bijective} \}$

Characterization of linear maps

Thm Let V and V' vector spaces over K and $f: V \to V'$

f is a K-linear map $\Leftrightarrow$ $f(k_1v_1 + k_2v_2) = k_1f(v_1) + k_2f(v_2)\ \forall k_1,k_2 \in K,\ \forall v_1, v_2 \in V$

e.g. $f: \mathbb{R}^2 \to \mathbb{R}$ $\quad f(x,y) = x+y$ is a linear map but $f(x,y) = xy$ is Not

$$f(k_1(x_1,y_1) + k_2(x_2,y_2)) = f(k_1x_1+k_2x_2, k_1y_1+k_2y_2)$$
$$= (k_1x_1+k_2x_2)+(k_1y_1+k_2y_2) =$$
$$= k_1(x_1+y_1) + k_2(x_2+y_2) = k_1f(x_1,y_1) + k_2f(x_2,y_2)$$

Thm (i) Let $f: V \to V'$ be an isomorphism of vector spaces over K

$f^{-1}: V' \to V$ also isomorphic over K

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

Kernel and image of a linear map

Let $f: V \to V'$ be a k-linear map:

$$\operatorname{Ker} f = \{ v \in V \mid f(v) = 0' \} \qquad \operatorname{Im} f = \{ f(v) \mid v \in V \}$$

Thm Let $f: V \to V'$ be a k-linear map.

$$\operatorname{Ker} f \leq V \quad \text{and} \quad \operatorname{Im} f \leq V'$$

Thm Let $f: V \to V'$ be a k-linear map:

$$\operatorname{Ker} f = \{0\} \iff f \text{ is injective}$$

$\{0\}$ ← aici nu ii subspace?

Thm Let $f: V \to V'$ a k-linear map. $X \subseteq V$

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

Linear independence

Definition

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

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

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

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

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

Approach: you are in a vector space & to show if a set of vectors is (in)dependent compute the sum $k_1 v_1 + \ldots + k_n v_n$ and come to a conclusion

(1) A set consisting of a single vector v is linearly dependent $\iff$ $v = 0$. ← remember this

Theorem

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

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

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

(i) one vector v is linearly dependent in $V_2 \iff v = 0$;
(ii) two vectors are linearly dependent in $V_2 \iff$ they are collinear;
(iii) three vectors (or more) are always linearly dependent in V_2.

$k_1 v_1 + k_2 \cdot v_2 = 0$ with $k_2 \neq 0$

(v_1, v_2 linearly dependent)

$\Rightarrow v_2 = \underbrace{-k_2^{-1} \cdot k_2}_{\alpha} v_1$ (when we talk about vectors this just means that they are COLINEAR)

$\Rightarrow$ if two vectors are colinear $\iff$ the vectors are linearly dependent

ex:

(b) If K is a field and $n \in \mathbb{N}^*$, then the vectors $e_1 = (1, 0, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, 0, 0, \ldots, 1) \in K^n$ are linearly independent in the canonical vector space K^n over K. In order to show that, let $k_1, \ldots, k_n \in K$ be such that

$$k_1 e_1 + k_2 e_2 + \cdots + k_n e_n = 0 \in K^n.$$

Then we have

$$k_1(1, 0, 0, \ldots, 0) + k_2(0, 1, 0, \ldots, 0) + \cdots + k_n(0, 0, 0, \ldots, 1) = (0, \ldots, 0),$$

Show that $e_1, e_2, \ldots e_n$ are linearly independent in the canonical vector space K^n over K:

Let $k_1, \ldots k_n \in K$ be such that $k_1 e_1 + \ldots + k_n e_n = 0 \in K$

$\Rightarrow (k_1, 0, \ldots, 0) + (0, k_2, \ldots, 0) + \ldots + (0, 0, \ldots, k_n) = (0, \ldots, 0) \in K^n$

$\Rightarrow (k_1, k_2, \dots, k_n) = (0, \dots, 0) \in K^n$

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

Hence $e_1, \dots e_n$ are linearly independent

Definition 2.7.1 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, $\langle B \rangle = V$.

Theorem 2.7.2 *Every vector space has a basis.*

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

Now let $V = \langle B \rangle \neq \{0\}$, 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 by Theorem 2.6.3, $\exists j_1 \in \{1, \dots, n\}$ 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 $k_i' \in K$. It follows that $V = \langle B \setminus \{v_{j_1}, v_{j_2}\} \rangle$, because every vector of V can be written as a linear combination of the vectors of $B \setminus \{v_{j_1}, v_{j_2}\}$. If $B \setminus \{v_{j_1}, v_{j_2}\}$ is linearly independent, then it is a basis and we are done. Otherwise, we continue the procedure. If all the previous intermediate subsets are linearly dependent, we get to the step

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

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

Remark 2.7.3 We are going to see that a vector space may have more than one basis.

Let us give now a characterization theorem for a basis of a vector space.

Theorem 2.7.4 *Let V be a vector space over K. A list $B = (v_1, \dots, v_n)$ of vectors in V is a basis of V if and only if every vector $v \in V$ can be uniquely written as a linear combination of the vectors $v_1, \dots, v_n$, that is,*

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

for some unique $k_1, \dots, k_n \in K$.

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

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

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

$\boxed{\Longleftarrow}$ Assume that every vector $v \in V$ can be uniquely written as a linear combination of the vectors of B. Then clearly, $V = \langle B \rangle$. For $k_1, \dots, k_n \in K$, we have by the uniqueness of writing

$$k_1 v_1 + \cdots + k_n v_n = 0 \Longrightarrow k_1 v_1 + \cdots + k_n v_n = 0 \cdot v_1 + \cdots + 0 \cdot v_n \Longrightarrow$$

$$\Longrightarrow k_1 = \cdots = k_n = 0\,,$$

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

Definition 2.7.5 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*.

(b) Consider the canonical real vector space $\mathbb{R}^2$. We already know a basis of $\mathbb{R}^2$, namely the canonical basis $((1,0),(0,1))$. But it is easy to show that the list $((1,1),(0,1))$ is also a basis of $\mathbb{R}^2$. Therefore, a vector space may have more than one basis.

Also, note that $\{e_1\}$ is linearly independent, but not a system of generators, while the list $(e_1, e_2, e_1 + e_2)$ is a system of generators, but not linearly independent. Hence none of the two lists is a basis of the canonical real vector space $\mathbb{R}^2$.

Theorem 2.7.7 *Let $f : V \to V'$ be a K-linear map and let $B = (v_1, \ldots, v_n)$ be a basis of V. Then f is determined by its values on the vectors of the basis B.*

Proof. Let $v \in V$. Since B is a basis of V, $\exists! k_1, \ldots, k_n \in K$ such that $v = k_1 v_1 + \cdots + k_n v_n$. Then

$$f(v) = f(k_1 v_1 + \cdots + k_n v_n) = k_1 f(v_1) + \cdots + k_n f(v_n)\,,$$

that is, f is determined by $f(v_1), \ldots, f(v_n)$. □

Corollary 2.7.8 *Let $f, g : V \to V'$ be K-linear maps and let $B = (v_1, \ldots, v_n)$ be a basis of V. If $f(v_i) = g(v_i)$, $\forall i \in \{1, \ldots, n\}$, then $f = g$.*

Proof. Let $v \in V$. Then $v = k_1 v_1 + \cdots + k_n v_n$ for some $k_1, \ldots, k_n \in K$, hence

$$f(v) = f(k_1 v_1 + \cdots + k_n v_n) = k_1 f(v_1) + \cdots + k_n f(v_n) = k_1 g(v_1) + \cdots + k_n g(v_n) = g(v)\,.$$

Theorem 2.7.9 *Let $f : V \to V'$ be a K-linear map, and let $X = (v_1, \ldots, v_n)$ 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'.

Proof. We have $f(X) = (f(v_1), \ldots, f(v_n))$.

(*i*) Let $k_1, \ldots, k_n \in K$ be such that

$$k_1 f(v_1) + \cdots + k_n f(v_n) = 0'.$$

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

$$f(k_1 v_1 + \cdots + k_n v_n) = f(0),$$

whence by the injectivity of f we get

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

But since X is linearly independent in V, we have $k_1 = \cdots = k_n = 0$. Hence $f(X)$ is linearly independent in V'.

(*ii*) Since X is a system of generators for V, we have $\langle X \rangle = V$. By the surjectivity of f we have:

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

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

(*iii*) This follows by (*i*) and (*ii*). □

Theorem 2.8.2 (Steinitz Theorem, Exchange Theorem) *Let V be a vector space over K, $X = (x_1, \ldots, x_m)$ a linearly independent list of vectors of V and $Y = (y_1, \ldots, y_n)$ 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.

Theorem 2.8.4 *Any two bases of a vector space have the same number of elements.*

Proof. Let V be a vector space over K and let $B = (v_1, \ldots, v_m)$ and $B' = (v'_1, \ldots, v'_n)$ be bases of V. Since B is linearly independent in V and B' is a system of generators for V, we have $m \leq n$ by Theorem 2.8.2. Since B is a system of generators for V and B' is linearly independent in V, we have $n \leq m$ by the same Theorem 2.8.2. Hence $m = n$. □

Definition 2.8.5 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 $\dim V$.

Theorem 2.8.8 *Let V be a vector space over K. Then the following statements are equivalent:*
(i) $\dim V = n$.
(ii) The maximum number of linearly independent vectors in V is n.
(iii) The minimum number of generators for V is n.

Proof. $(i) \implies (ii)$ Assume that $\dim V = n$. Let $B = (v_1, \ldots, v_n)$ be a basis of V. Then B is a list of n linearly independent vectors in V. Since B is a system of generators for V, any linearly independent list in V must have at most n elements by Theorem 2.8.2.

$(ii) \implies (i)$ Assume (ii). Let $B = (v_1, \ldots, v_m)$ be a basis of V and let $(u_1, \ldots, u_n)$ be a linearly independent list in V. Since B is linearly independent, we have $m \leq n$ by hypothesis. Since B is a system of generators for V, we have $n \leq m$ by Theorem 2.8.2. Hence $m = n$ and consequently $\dim V = n$.

$(i) \implies (iii)$ Assume that $\dim V = n$. Let $B = (v_1, \ldots, v_n)$ be a basis of V. Then B is a system of n generators for V. Since B is a linearly independent list in V, any system of generators for V must have at least n elements by Theorem 2.8.2.

$(iii) \implies (i)$ Assume (iii). Let $B = (v_1, \ldots, v_m)$ be a basis of V and let $(u_1, \ldots, u_n)$ be a system of generators for V. Since B is a system of generators for V, we have $n \leq m$ by hypothesis. Since B is linearly independent, we have $m \leq n$ by Theorem 2.8.2. Hence $m = n$ and consequently $\dim V = n$. □

Theorem 2.8.9 *Let V be a vector space over K with $\dim V = n$ and $X = (u_1, \ldots, u_n)$ a list of vectors in V. Then*

$$X \text{ is linearly independent in } V \iff X \text{ is a system of generators for } V\,.$$

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

$\boxed{\implies}$ Assume that X is linearly independent. Since B is a system of generators for V, we know by Theorem 2.8.2 that n vectors of B, that is, all the vectors of B, can be replaced by the vectors of X and we get another system of generators for V. Hence $\langle X \rangle = V$. Thus, X is a system of generators for V.

$\boxed{\impliedby}$ Assume that X is a system of generators for V. Suppose that X is linearly dependent. Then $\exists j \in \{1, \ldots, n\}$ such that

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

for some $k_i \in K$. It follows that

$$V = \langle X \rangle = \langle u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n \rangle\,.$$

But the minimum number of generators for V is n by Theorem 2.8.8, which is a contradiction. Therefore, X is linearly independent. □