Linear Algebra – Lecture Notes

Lukas Prokop

winter term 2015

Contents

This lecture took place on 5th of Oct 2015 (Prof. Franz Lehner).

Weekly schedule:

Mon	08:15–09:45	KF 06.01
Tue	08:15–09:45	TU P2
Tue	10:15	BE 01, Konversatorium
Wed	13:00–15:00	UE + Onlinekreuzesystem, Deadline 11:00
Mon, Tue, Thu	*	Tutorien

Exams:

1. VO-Prüfung (schriftlich, 3 Termine pro Semester, ohne Unterlagen)
2. 2 UE-Prüfungen (25.11, 27.01, 1 DIN A4 Blatt)

What is linear algebra?

- Arithmetics
- Geometry
- Analysis / infinitesimal computation

100 years ago, the following branch of mathematics was introduced:

- Algebra: abstract computational operations (fields, groups, rings, etc)
  - Linear algebra (branch of algebra, related to vector computations)

Mathematics is the search for statements of the structure: *If A, then B.*

1 Set theory, logic and linear equations

1.1 Axiomatic definition of a set

Georg Kantor (1869)

> Unter einer Menge verstehen wir eine Zusammenfassung von *bestimmten wohlunterschiedenen* Objekten unserer Anschauung oder unsres Denkens (welche die Objekte der Menge M genannt werden) zu einem Ganzen.
>
> We define a set as a combination of defined well-distinguishable objects of our perception and our minds (which are denoted set M) to a whole unit.

Hence for every object x one of these statements hold:

- x is part of M: $x \in M$
- x is not part of M: $x \in M$

1.2 Notation for set theory

Approaches for notations:

- Enumeration
  - $\{1, 2, 3\}$, $\{a, b, \text{teddy bear}, \text{lecture hall HS 06.01}\}$
  - Integers (in this lecture: without zero): $\mathbb{N} = \{0, 1, 2, \ldots\}$
  - $\{1, 2, 3, \ldots\}$: integers, end undetermined
  - $\{1, 2, \ldots, n\}$: integers from 1 to n
  - $\{x, y, \ldots, z\}$: general finite set
- Description
  - $\{1, 4, 9, 16, \ldots\}$
  - $\{n | n \text{ is square of an integer}\}$
  - $\left\{n | \text{there exists } k \in \mathbb{N} \text{ such that } n = k^2\right\} = \left\{k^2 | k \in \mathbb{N}\right\}$
- Defined set with shortcuts
  - $\mathbb{N}$

– $\mathbb{Z} = \{0, \pm1, \pm2, \ldots\}$
– $\mathbb{Q} = \left\{\frac{p}{q} | p \in \mathbb{Z}, q \in \mathbb{N}\right\}$
– $\mathbb{R}$ = complex definition, see analysis
– $\mathbb{C} = \{x + y \,|\, x, y \in \mathbb{R}\}$
– $\{\} = \emptyset$ as the empty set
– M. Bourbaki, “Elements of mathematics”

1.3 Examples for custom sets

“The set of all competent politicians” Not well-defined, opinion-based

“The set of all visible fix stars” Depends on definition of visibility, are tools allowed?, opinion-based

1.4 Russell’s paradoxon

Russell 1901, Zeromelo 1902

M = “the set of all sets” = “the set of all sets that does not contain itself”

1.5 Berrys paradoxon

M_{12} = set of all integers describable with at most 11 words
n is the smallest number not describable with at most 11 words

So n is not contained in M_{12}. But n itself is now described with 11 words. So it’s contained? Paradoxon.

1.6 Axiomatic system of Zermelo-Frauenkel

1. For all sets A, B it holds that $A = B$ iff $x \in A$ then also $x \in B$.
2. An empty set exists. Hence for all x it holds that $x \notin \emptyset$.
3. If A and B are sets, then also $\{A, B\}$.

4. If A and B are sets, then also the union of $A \cup B$ is a set.
5. An infinite set exists.
6. If A is a set, then also the power set $\mathcal{P}(A) = \{B | B \subseteq A\}$

1.7 Basics of logic

Aristoteles and Organon

Organon called the system “analytics”.

> A *statement* is a linguistic unit which is *true* or *false*.

Examples:

- Sokrates is a human.
- 7 is a prime number.
- 5 is an even number.
- There exists only one universe.

The last example has an unknown truth value. Constructivists: “Unknown means false”. Pragmatics: “Unknown means unknown”.

Other examples for unknown truth values:

- Today is monday.
- A. Gabalier has a beautiful voice.

Epimenides

> All crets are liars.

Russell:

> This statement is wrong.

1.8 Gödel's incompleteness theorem

Kurt Gödel (1930)

> In every formal system statements exist that are true, but not provable.

Example: "This statement is not provable."

1.9 A correction

Due to these contradictions:

> A *statement* is a linguistic unit for which it makes sense to ask: is it *true* or *false*?

1.10 Formal logic

Negation $\neg A$ means the truth value of A is inverted

Conjunction $A \land B$ is true, if A and B is true

Attention!

- Eating and drinking forbidden (actually: "no eating or drinking")
- Solutions for $x^2 = 1$: $x_1 = 1$ and $x_2 = -1$ ("actually: $x_1 = 1$ *or* $x_2 = -1$")

Disjunction $A \lor B$ is true, if A or B is true (latin "vel")

Exclusive disjunction $A \dot{\lor} B$ is true if A or B but not both are true (latin "out")

Equivalence $A \leftrightarrow B$ is true if both share the same truth value ($\neg(A \dot{\lor} B)$)

Implication / subjunction $A \implies B$ is true if A is false or A is true and B is false. A implies B. Deutsch: "A ist hinreichend für B. B ist notwendig für A."

1.11 Definition

Two logical statements are equivalent if for every variable assignment, the same truth value is evaluated $(P(A_1, \dots, A_n) \leftrightarrow Q(A_1, \dots, A_n))$.

1.12 Logical laws by DeMorgan

$$\neg(A \land B) \Leftrightarrow \neg A \lor \neg B$$

This lecture took place on 6th of Oct 2015 (Prof. Franz Lehner).

$$|\,\mathbb{N}\,| = \aleph_0$$

1.13 Proofs

A sentence is a statement of kind:

$$A \implies B$$

A is our requirement. B is our conclusion. A proof is showing that B holds under assumption of A.

1.14 Statement

> Let $n \in \mathbb{N}$ be odd, than n^2 is odd.

Proof:

A. n is even and $n \in \mathbb{N}$, hence there exists some $k \in \mathbb{N}_0$ such that $n = 2k + 1$

B. n^2 is odd, hence it holds that $l \in \mathbb{N}_0$ such that $n^2 = 2l + 1$

We know, $n = 2k + 1$

$$\Rightarrow n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1$$

with $l = 2k^2 + 2k$, statement B holds. Direct proof.

1.14.1 Contraposition law

$$A \implies B \Leftrightarrow \neg B \implies \neg A$$

A so-called "indirect proof".

If n^2 is even, than n is even.

A. n^2 is even

B. n is even

$\neg B$. n is odd

$\neg A$. n is odd

We already have shown,

$$\neg B \implies \neg A$$

hence also $A \implies B$ is true.

1.15 Proof by contradiction

$$A \vee \neg A$$

Tertium nondatur
hence if $\neg A$ is false, then A is true.

1.15.1 $\sqrt{2}$ is irrational

$$\sqrt{2} \notin \mathbb{Q}$$

Proof:

A. Let $x \in \mathbb{R}$ such that $x^2 = 2$ and $x > 0$ and let $\sqrt{2}$ be that number

B. $\sqrt{2} \notin \mathbb{Q}$

Assume $\neg B$ hence $\sqrt{2} \in \mathbb{Q}$. We find a contradiction.

$\sqrt{2} \in \mathbb{Q}$ then there exists some $p \in \mathbb{Z}, q \in \mathbb{N}$ such that $\sqrt{2} = \frac{p}{q}$.

Wlog (without loss of generality), we assume that the fraction is irreducible. Hence $\gcd(p, q) = 1$.

Therefore $\sqrt{2}$ has the following property.

$$\begin{aligned} \sqrt{2} &= \frac{p}{q} \\ (\sqrt{2})^2 &= 2 \\ \frac{p^2}{q^2} &= 2 \\ \Rightarrow p^2 &= 2q^2 \\ \Rightarrow p^2 &\text{ is even} \\ \Rightarrow p &\text{ is even} \end{aligned}$$

hence there exists some $k \in \mathbb{N}$ such that $p = 2k$

$$\begin{aligned} (2k)^2 &= 2q^2 \\ 4k^2 &= 2q^2 \\ 2k^2 &= q^2 \\ \Rightarrow q^2 &\text{ is even} \\ \Rightarrow q &\text{ is even} \end{aligned}$$

hence there is some $l \in \mathbb{N}$ such that $q = 2l$.

$$\sqrt{2} = \frac{2k}{2l}$$

is not reduced. This is contradictory to our original statement.

$$\begin{aligned}\gcd(p, q) &= \gcd(2k, 2l)\\ &\geq 2 \neq 1\end{aligned}$$

$\Rightarrow \neg B$ is wrong, so B is true.

1.16 Remark about constructivism

A few mathematicians deny "tertium non datur". For those $A \vee \neg A$ means that there is no proof for either statement.

1.16.1 a^b is irrational with $a, b \in \mathbb{R}$

Proof: We know that $\sqrt{2} \notin \mathbb{Q}$.

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2^{\in\mathbb{Q}}$$

case 1: $\sqrt{2}^{\sqrt{2}}$ is irrational $\Rightarrow$ choose $a = \sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}, b = \sqrt{2} \notin \mathbb{Q}, a^b \in \mathbb{Q}$

case 2: $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ choose $a = \sqrt{2} \notin \mathbb{Q}$ and $b = \sqrt{2} \notin \mathbb{Q}$ and $a^b \in \mathbb{Q}$.

With other means means that $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$.

1.17 Agreement

A *predicate* is an expression which depends on variable and by insertion of values, a statement is created.

$$P(n) \Leftrightarrow \; n \text{ is even}$$

is not a statement unless we define n.

$$P(2) \Leftrightarrow 2 \text{ is even}$$
$$P(3) \Leftrightarrow 3 \text{ is even}$$

1.18 Quantifiers

$$Q(n) \Leftrightarrow \big(P(n = 2k+1) \implies P(n^2 = 2l+1)\big)$$

hence the statement

$$Q(1) \wedge Q(2) \wedge Q(3) \wedge Q(4) \wedge Q(5) \dots$$

Notation:

$$\bigwedge_{n\in\mathbb{N}} Q(n) \;\text{ or }\; \forall n \in \mathbb{N} : Q(n)$$

So we can briefly write:

$$\bigwedge_{n\in\mathbb{N}} Q(n)$$

meaning for all $n \in \mathbb{N}$ it holds that "n is odd implies n^2 is odd".

$\bigwedge$ is called "all quantifier".

Analogously for $P(1) \vee P(2) \vee P(3) \vee \dots$ is true if there is some n such that $P(n)$ is true.

$$\bigvee_{n\in\mathbb{N}} P(n) \Leftrightarrow \exists n : P(n)$$

Variant:

$$\dot{\bigvee}_{x\in X} P(x)$$

there exists *exactly one* x such that $P(x)$ holds.

$$\exists! x \in X : P(x)$$

1.19 Proof using quantifiers

There exists some prime number:

- $\bigwedge_{n\in\mathbb{N}} n \in \mathbb{P}$ where $\mathbb{P}$ is the set of prime numbers.
- An integer is a prime number, if it does not have real divisor.

$$k \mid n = k \text{ divides } n \Leftrightarrow \bigvee_{l\in\mathbb{N}} k \cdot l = n$$

$$\bigwedge_{n\in\mathbb{N}} n \in \mathbb{P} \leftrightarrow \neg \bigvee_{k\in\mathbb{N}} (k > 1) \wedge (k < n) \wedge (k \mid n)$$

1.20 Negation with quantifiers

$$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$$

$$\neg \bigwedge_{x\in X} P(x) \Leftrightarrow \bigvee_{x\in X} \neg P(x)$$

1.21 Relation between set theory and boolean algebra

$$\begin{aligned} A \cap B &= \{x \mid x \in A \wedge x \in B\} \\ A \cup B &= \{x \mid x \in A \vee x \in B\} \\ A \triangle B &= \{x \mid x \in A \dot{\vee} x \in B\} && \text{“symbolic difference”} \\ A \setminus B &= \{x \mid x \in A \wedge x \notin B\} \end{aligned}$$

$$\begin{aligned} A^C &= \{x \in U \mid x \notin A\} && \text{“complement in } U\text{, the universe”} \\ &= U \setminus A \\ A \subseteq B &\Leftrightarrow \bigwedge_{x\in A} x \in B \\ &\Leftrightarrow \bigwedge_{x} (x \in A \implies x \in B) \\ A = B &\Leftrightarrow \bigwedge_{x} x \in A \Leftrightarrow x \in B \end{aligned}$$

Let A_i with $i \in I$ (where I is the index set) be sets than

$$\bigcap_{i\in I} A_i = \left\{ x \,\middle|\, \bigwedge_{i\in I} x \in A_i \right\} \qquad \text{intersection of all } A_i$$

$$\bigcup_{i\in I} A_i = \left\{ x \,\middle|\, \bigvee_{i} x \in A_i \right\} \qquad \text{union of all } A_i$$

$$\bigcap_{i\in I} A_i \cap \bigcap_{j\in J} A_j = \bigcap_{i\in I\cup J} A_i = \left\{ x \,\middle|\, \bigwedge_{i\in I\cup J} x \in A_i \right\}$$

What happens at $I = \emptyset$?

$$\bigwedge_{x\in\emptyset} P(x) \Leftrightarrow W \qquad \text{is always true}$$

This is axiomatic:

$$\bigwedge_{x\in\emptyset} P(x) \qquad \text{is always true}$$

$I = \mathbb{R}$, for every $x \in \mathbb{R}$ a set A_x is given

$$\bigcap_{x\in\mathbb{R}} A_x = \left\{ y \,\middle|\, \bigwedge_{x\in\mathbb{R}} y \in A_x \right\}$$

$$\bigvee_{x\in\emptyset} Q(x) \qquad \text{is always false}$$

2 Power sets

Let A be a set.

$$P(A) = 2^A = \{B \mid B \subseteq A\}$$

is called a "power set" of A.

$$P(\emptyset) = \{\emptyset\}$$
$$P(P(\emptyset)) = \{\emptyset, \{\emptyset\}\}$$

Let A, B be sets. The following set is called "cartesian product" (lat. renatus cartesius) (by René Descartes, 17th century)

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

Followingly,

$$A^2 = A \times A$$
$$A^n = \underbrace{A \times A \times \dots}_{n}$$
$$A \times B \times C = \{(a, b, c) \mid a \in A, b \in B, c \in C\}$$
$$A^n = \{(a_1, \dots, a_n) \mid a_i \in A\}$$
$$A^I = \{(a_i)_{i \in I} \mid a_i \in A\}$$

3ary tuples are called "triples". $(a_i)_{i \in I}$ is called family of elements (where I is an index set).

3 Relations of sets

A *relation* on a set is a subset

$$R \subseteq X \times X$$

Notation: xRy means x is in relation with y. Hence $(x, y) \in R$.

Example: X is the set of austrians. The relation is marriage. Be aware that every married couple occurs twice. Once as (x, y) and once as (y, x).

This lecture took place on 12th of Oct 2015 (Prof. Franz Lehner).

A relation of a set X is a subset $R \subseteq X \times X$. We denote xRy iff $(x, y) \in R$.

i	set	R
0	$X = \{\text{Austrian}\}$	"married"
1	$X = \{\text{Austrian}\}$	same location of birth
2	$X = \mathbb{R}$	$x \leq y$
3	X arbitrary	$x = y$
4	$X = \mathbb{N}$	$x \mid y$
5	$X = \mathbb{Z}$, defined $n \in \mathbb{N}$	$n \mid x - y$
6	$X = \{a, b, c\}$	$R = \{(a, a), (a, c), (b, b), (c, a), (c, c)\}$

i	reflexive	symmetrical	anti-sym.	transitive	konnex
0	false	true	false	false	false
1	true	true	false	true	false
2	true	false	true	true	true
3	true	true	true	true	false
4	true	false	true	true	false
5	true	true	false	true	false
6	true	true	false	true	false

Table 1: Examples for relations and their properties

A *relation* R operating on a set X is called

reflexive
: if $\bigwedge_{x \in X} xRx$ (hence $(x, x) \in \mathbb{R}$)

symmetrical
: if $\bigwedge_{x \in X} y \in X\,(xRy \implies yRx)$

anti-symmetrical
: if $\bigwedge_{x \in X} \bigwedge_{y \in X} (xRy \wedge yRx \implies x = y)$

transitive
: if $\bigwedge_{x \in X} \bigwedge_{y \in X} \bigwedge_{z \in X} (xRy \wedge yRz) \implies xRz$

konnvex
if $\bigwedge_{x\in X}\bigwedge_{y\in X}(xRy \vee yRx)$

A relation satisfying reflexivity, symmetry and transitivity is called *equivalence relation*. Examples 2, 4, 6 and 7 are equivalence relations.

A relation satisfying reflexivity, anti-symmetry and transitivity is called *order relation*. Examples 3, 4 and 5 are order relations.

A relation satisfying reflexivity, anti-symmetry, transitivity and konnvexivity is called *total order*. Example 2 is a total order.

Let $\sim$ be an equivalence relation operating on set X. For $x \in X$,

$$[x] = \{y \in X \mid x \sim y\}$$

is called equivalence class of x.

Examples:

- $[x] = \{y \mid y \text{ has the same location of birth}\}$
- $[x] = \{y \mid x = y\} = \{x\}$
- $[x] = \{y \mid n \mid x - y\} = \{y \mid x - y = q \cdot n\} = \{y \mid y = x - q \cdot n\} = \{x + k \cdot n \mid k \in \mathbb{Z}\}$
- $[a] = \{a, c\}, [b] = \{b\}, [c] = \{a, c\}$

${}^{X}\!/\!_{\sim} = \{[x] \mid x = X\}$ is called *factor set* or *quotient set*.

Examples:

- ${}^{X}\!/\!_{\sim} = \{\{\text{Graz}\}, \{\text{Linz}\}, \{\text{Wien}\}, \dots\}$
- ${}^{X}\!/\!_{\sim} = \{\{x\} \mid x \in X\}$
- $\mathbb{Z}\sim = \{[0], [1], [2], \dots, [n-1]\}$

$$n = 0 + 1 \cdot n \in [0]$$

$$0 = n - 1 \cdot n \in [n]$$

A *system of representatives* is a subset $S \subseteq X$ such that

$$\bigwedge_{[x]\in {}^{X}\!/\!_{\sim}} \dot{\bigvee}_{s\in S} s \in [x]$$

Examples:

- The mayor of a city.
- $S = X$
- $S = \{0, \dots, n-1\}$

Theorem 1. *Let $\sim$ be an equivalence relation operating on X. Then it holds that*

$$\bigwedge_{x,y\in X} (x \sim y \iff [x] = [y])$$

Proof: Let $x, y \in X$ be arbitrary elements such that $x \sim y$. Show that $[x] \subseteq [y] \wedge [y] \subseteq [x]$. It suffices to show that $[x] \subseteq [y]$ because x, y can be arbitrary.

Show $\bigwedge_{z\in[x]} z \in [y]$. Let $z \in [x] \implies x \sim z$. Furthermore $x \sim y \xrightarrow{symmetrical} y \sim x$. Hence $y \sim x \wedge x \sim z \xrightarrow{transitive} y \sim z \implies z \in [y]$. Hence $[x] \subseteq [y]$. Hence $[x] = [y]$.

If $[x] = [y]$, then $y \in [y]$ (because its reflexive) hence $y \in [x] \implies x \sim y$.

Let X be a set. A *partition* of X is a subset $Z \subseteq \mathcal{P}(X)$. Z is the set of subsets of X such that

- $\bigcup_{A=Z} A = X$
- $\bigwedge_{A,B\in Z} (A \neq B \implies A \cap B = \emptyset)$

$$\iff \bigwedge_{x\in X} \bigvee_{A\in Z} x \in A$$

Theorem 2. *Let X be a non-empty set.*

- *Let $\sim$ be an equivalence relation operating on X, then ${}^{X}\!/\!_{\sim}$ is a partition of X.*

- *Let $Z \subseteq \mathcal{P}(X)$ a partition of X. There is exactly one equivalence relation $\sim$ on X such that ${}^{X}\!/\!_{\sim} = Z$.*

Proof. Let $\sim$ be an equivalence relation on X. Then ${}^{X}\!/\!_{\sim} = \{[x] \,|\, x \in X\} \subseteq \mathcal{P}(x)$

- We need to show that $\bigcup_{x \in X} [x] = X$.

$$\begin{aligned} \bigwedge_{x \in X} x \sim y &\implies \bigwedge_{x \in X} x \in [x] \\ &\implies \bigwedge_{x \in X} x \in \bigcup_{y \in X} [y] \\ &\implies X \subseteq \bigcup_{y \in X} [y] \end{aligned}$$

- Furthermore we need to show that $\bigwedge_{x,y \in X} [x] \cap [y] \neq \emptyset \implies [x] = [y] \iff x \sim y$.

$$\begin{aligned} \text{Let } [x] \cap [y] \neg \emptyset & \bigvee_{z} z \in [x] \cap [y] \\ & \bigvee_{z} z \in [x] \wedge z \in [y] \\ \text{definition of equivalence class } &\implies x \sim z \wedge y \sim z \\ \text{symmetrical } &\implies \bigvee_{z} x \sim z \wedge z \sim y \\ &\xrightarrow{transitive} x \sim y \\ &\xrightarrow{theorem\ 1} [x] = [y] \end{aligned}$$

□

This lecture took place on 13rd of Oct 2015 (Prof. Franz Lehner).

A *function* (or mapping) between two sets X and Y

$$f : X \to Y$$

$$x \mapsto f(x)$$

is a relation assigning every element $x \in X$ some $f(x) \in Y$.

X is called domain and Y is called co-domain (also range or image). $f(x)$ is called image of x under f. We can find a symbolic expression for a function or explicitly enumerate all mappings possibilities.

Examples:

$$\begin{aligned} f_1 : \mathbb{R} &\to \mathbb{R} \\ x &\to x^2 \\ f_2 : \{0,1\} &\to \mathbb{R} \\ 0 &\to 11 & \to \pi \\ f_3 : \mathcal{P}(x) &\to \mathcal{P}(x) \\ A &\mapsto X \setminus A \end{aligned}$$

Let $\sim$ be an equivalence relation operating on set X.

$$\begin{aligned} f_4 : X &\to {}^{X}\!/\!_{\sim} \\ x &\mapsto [x] \\ f_5 : \mathbb{R} \times \mathbb{R} &\to \mathbb{R} \\ (x,y) &\mapsto x + y \end{aligned}$$

Remarks:

1. Domain and codomain are part of the definition of a function. A function is unambiguously defined by some graph:
2. $$G_f = \{(x, f(x)) \,|\, x \in X\} \subseteq X \times Y$$

   therefore a relation between X and Y such that every $x \in X$ occurs exactly once.

   $$\bigwedge_{x \in X} \dot{\bigvee}_{y \in Y} (x,y) \in G_f$$

3. Two functions $f : X \to Y$, $f : U \to V$ are equivalent iff $X = U$, $Y = V$ and $\bigwedge_{x\in X} f(x) = g(x)$.

   Hence the domain and codomain must be equivalent.

4. The function $\mathrm{id}_X : X \to X$ is called "identity".

5. Let $A \subseteq X$ be a subset.

$$\mathbb{1}_A = \chi_A : X \to \{0,1\}$$

$$x \to \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

   This function is called *indicator function of* A or *characteristic function of* A.

6. Every function $f : X \to \{0,1\}$ is the indicator function of a subset of X, namely $f = \mathbb{1}_A$ where $A = \{x \in X \mid f(x) = 1\}$.

Let $A \subseteq X$ be a subset of $f : X \to Y$. Then $f\mid_A: A \to Y$ with $a \mapsto f(a)$ is called *restriction* of f to A.

$f\mid_A$ is not defined outside A.

Let $f : X \to Y$ be a function defined for $B \subseteq Y$.

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\} \subseteq X$$

Therefore we define the domain function

$$f^{-1} : \mathcal{P}(Y) \to \mathcal{P}(X)$$

$f^{-1}(B)$ can be empty.

If $B = \{y\}$ then we write $f^{-1}(y)$ instead of $f^{-1}(\{y\})$.

$$f^{-1}(1) = f^{-1}(\{1\}) = \{+1, -1\}$$

$$f^{-1}(-1) = \emptyset$$

$$f(\{1,2\}) = \{1,4\}$$

$$f(\{+1,-1\}) = \{1\}$$

Analogously f indicates a function

$$\tilde{f} : \mathcal{P}(X) \to \mathcal{P}(Y)$$

$$A \mapsto f(A) = \{f(x) \mid x \in A\}$$

Remark:

$$f^{-1}(B) = \bigcup_{b\in B} f^{-1}(b)$$

A function $f : X \to Y$ is called *injective* iff

$$\bigwedge_{x_1,x_2\in X} (x_1 \neq x_2 \implies f(x) \neq f(x_2))$$

$$\iff \bigwedge_{x_1,x_2\in X} (f(x_1) = f(x_2) \implies x_1 = x_2)$$

A function is called *surjective* iff

$$\bigwedge_{y\in Y} \bigvee_{x\in X} f(x) = y$$

A function is called *bijective* iff a function is injective and surjective.

$$\bigwedge_{y\in Y} \dot{\bigvee}_{x\in X} f(x) = y$$

For a bijective function f^{-1} is called *inverse function.*

$$f^{-1} : Y \to X$$

$$y \mapsto \text{every distinct } x \text{ such that } f(x) = y$$

Be aware that $f^{-1}(y)$ sometimes means $f^{-1}(\{y\})$.

Examples:

- $f : x \mapsto 3x$ in $\mathbb{R} \to \mathbb{R}$ is injective and surjective. Therefore it is also bijective.

- $f : x \mapsto x^2$ in $\mathbb{R} \to \mathbb{R}$ is not injective and not surjective. We have a restriction:
$$\tilde{f} : \mathbb{R}_0^+ \to \mathbb{R}_0^+$$
With this domain, the function is bijective.
- $f : x \mapsto x^3$ in $\mathbb{R} \to \mathbb{R}$ is bijective.
- $f : A \mapsto A^C = X \setminus A$ in $\mathcal{P}(X) \to \mathcal{P}(X)$. Injective if $A \neq B$. Wlog $x \in A$, $x \notin B$
$$\Rightarrow x \notin A^C, x \in B^C \Rightarrow B^C \neq A^C$$
Surjective: Given $B \subseteq X$, find $A \subseteq X$ such that
$$f(A) = A^C = B$$
Yes, if $A = B^C$ that $A^C = (B^C)^C = B$. The inverse function is the function itself.

A function is called *involution* if its inverse function is the function itself.

Let $f : X \to Y$ and $g : Y \to Z$ be functions, the function

$$g \circ f : X \to Z$$
$$x \mapsto g(f(x))$$

is called composition of f and g.

Theorem 3. *Let $f : X \to Y$, $g : Y \to Z$ and $h : Z \to U$ be functions.*

$$X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} U$$

Then

$$h \circ (g \circ f) \overset{?}{=} (h \circ g) \circ f$$

Proof. $h \circ (g \circ f)$ and $(h \circ g) \circ f$ bounded from X to U.

$$(h \circ (g \circ f))(x) = h(g \circ f(x)) = h(g(f(x))) = h \circ g(f(x)) = (h \circ g) \circ f(x)$$

□

Theorem 4. *Let $X \xrightarrow{f} Y \xrightarrow{g} Z$ be functions. If f and g are injective/surjective or bijective, then $g \circ f$ has the same property.*

Proof. Let f, g be injective. So $g \circ f$ must also be injective.

Let $x_1, x_2 \in X$ such that $g \circ f(x_1) = g \circ f(x_1)$. We need to show $x_1 = x_2$.

$$g \circ f(x_1) = g \circ f(x_2)$$
$$\Rightarrow g(f(x(_1)) = g(f(x_2))$$
$$\Rightarrow y_1 = f(x_1), y_2 = f(x_2)$$
$$g(y_1) = g(y_2) \xrightarrow{g \text{ injective}} Y_1 = Y_2$$
$$\Rightarrow f(x_1) = f(x_2) \xrightarrow{f \text{ injective}} x_1 = x_2$$

□

Remarks:

1. If $f : X \to Y$ is bijective, then $f^{-1} : Y \to X$ and it holds that
$$f \circ f^{-1} = \mathrm{id}_Y$$
$$f^{-1} \circ f = \mathrm{id}_X$$
2. Let f, g be bijective, then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.
$$X \xrightarrow{f} Y \xrightarrow{g} Z$$
Is $g \circ f$ bijective? Is g or f bijective?

4 Solutions to linear equation systems

A linear equation system is an equation system of structure:

$$
\begin{aligned}
a_{1,1}x_1 + a_{1,2}x_2 + \ldots + a_{1,n}x_n &= b_1 \\
a_{2,1}x_1 + a_{2,2}x_2 + \ldots + a_{2,n}x_n &= b_2 \\
\vdots &= \vdots \\
a_{n,1}x_1 + a_{n,2}x_2 + \ldots + a_{n,n}x_n &= b_n
\end{aligned}
$$

with coefficients a_{ij}, $b_i \in \mathbb{R}$ for all $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, n\}$. $x_1, x_2, \ldots, x_n$ are the unknown variables.

$ax + b$ is linear whereas $ax^2 + bx + c$ is non-linear.

A particular solution of the equation system is an n-tuple $(x_1, \ldots, x_n)$, which satisfies the equation.

The scheme

$$
\begin{bmatrix}
a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\
a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\
\vdots & & \ddots & \vdots \\
a_{m,1} & a_{m,2} & \ldots & a_{m,n}
\end{bmatrix}
$$

is called matrix of the equation system.

The equation system is called homogeneous if all $b_i = 0$. A homogeneous system always has at least one solution; $(0, 0, \ldots, 0)$.

$$ax = b \implies x = \frac{b}{a}$$

Case distinction:

Case 1 with $a \neq 0$ $x = \frac{b}{a}$ has a distinct solution

Case 2 with $a = 0, b \neq 0$ has no solution

Case 3 with $a = 0, b = 0$ every x is a solution

Example 1. *Let $n = 2$ and $m = 1$.*

$$a_1x + a_2y = b$$

No distinct solution.

Case distinction:

$a_2 \neq 0$

$$y = \frac{-a_1x + b}{a_2}$$

x is arbitrary.

$a_2 = 0$

$$a_1x = b$$

y is arbitrary. Case distinction:

$a_1 \neq 0$ $x = \frac{b}{a_1}$

$a_1 = 0, b = 0$ $0 = 0 \implies \mathbb{R}$ *as solution*

$a_1 = 0, b \neq 0$ *no solution*

$$n = 2, m = 2$$

$$
\begin{aligned}
a_{1,1}x + a_{1,2}y &= b_1 \\
a_{2,1}x + a_{2,2}y &= b_2
\end{aligned}
$$

Case distinction:

Case 1 intersection between two lines (exactly one solution)

Case 2 two parallel lines (no solution)

Case 3 one line (infinite solution)

4.1 Substitution

Example 2. *Example for case 1.*

$$
\begin{aligned}
x + y &= 1 \\
x - y &= 2
\end{aligned}
$$

We subtract the second from the first equation.

$$0 - 2y = 1$$

$$\Rightarrow y = -\frac{1}{2}$$

$$\Rightarrow x = 1 - y = \frac{3}{2}$$

Distinct solution $(\frac{3}{2}, -\frac{1}{2})$.

Example 3. *Example for case 2.*

$$\begin{aligned} x + y &= 1 \\ 2x + 2y &= -1 \end{aligned}$$

We subtract equation two minus the first equation taken two times.

$$0 + 0 = -3$$

No solution.

Example 4. *Example for case 3.*

$$\begin{aligned} x + y &= 1 \\ 2x + 2y &= 2 \end{aligned}$$

We take the second equation minus two times the first equation.

$$0 + 0 = 0$$

$0 \cdot y = 0$ *is a solution for every possible* $y \in \mathbb{R}$. *Free variable* t *with* $y = t$.

$$x = 1 - y = 1 - t$$

Solution set:

$$\{(1 - t, t) \,|\, t \in \mathbb{R}\}$$

This lecture took place on 19th of Oct 2015 (Prof. Franz Lehner).

What if there are 2 unknown variables, but more equations?

Case 4 a solution, where only two lines intersect. But not all three at one time.

Case 5 Two equations are equivalent, but other equations are parallel or intersecting.

What if there are 3 unknown variables, but only one equation?

Case 6 No unique solution. Express one variable by others. Equation describes a layer.

What if there are three variables and two equations?

Case 7 Two layers intersect in one line

Case 8 Two layers are parallel

What if there are three variables and three equations?

Case 9 Intersection of three layers in one point

Or in general: point, line, layer, no solution or $\mathbb{R}^3$. On a line we have one degree of freedom whereas $\mathbb{R}^3$ gives us three degrees of freeedom.

Example

$$\begin{aligned} -x + y + 2z &= 2 \\ 3x - y + z &= 6 \\ -x + 3y + 4z &= 4 \end{aligned}$$

We use Gauss-Jordan elimination:

$$\begin{aligned} 2 + 3 \cdot 10 \cdot 2y - 7z &= 12 \\ 3 - 12y + 2z &= 2 \end{aligned}$$

The following equation system then has the same solution:

$$\begin{aligned} -x + y + 2z &= 2 \\ 2y + 7z &= 12 \\ 2y + 2z &= 2 \end{aligned}$$

We again use Gauss-Jordan elimination:

$$2 - 30 + 5z = 10$$

Therefore we derived:

$$-x + y + 2z = 2$$

$$2y + 2z = 2$$

$$5z = 10$$

Then $z = 2$, $y = -1$ and $x = 1$ follows.

Different notation (to save time & space, matrix notation):

$$\left(\begin{array}{ccc|c} -1 & 1 & 2 & 2 \\ 3 & -1 & 1 & 6 \\ -1 & 3 & 4 & 4 \\ \hline 0 & 2 & 7 & 12 \\ 0 & 2 & 2 & 2 \\ \hline & 0 & 5 & 10 \end{array}\right)$$

$$\left(\begin{array}{ccc|c} -1 & 1 & 2 & 2 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 5 & 10 \\ \hline -1 & 1 & 2 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{array}\right)$$

$$\left(\begin{array}{ccc|c} -1 & 1 & 0 & -2 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ \hline -1 & 0 & 0 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \\ \hline -x & 0 & 0 & -1 \\ 0 & y & 0 & -1 \\ 0 & 0 & z & 2 \end{array}\right)$$

Distinct solution.

Another example:

$$\begin{aligned} x + y + z &= 1 \\ x - 2z + 2z &= 2 \\ 4x + y + 3z &= 5 \end{aligned}$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 1 & -2 & 2 & 2 \\ 4 & 1 & 5 & 5 \\ \hline 0 & -3 & 1 & 1 \\ 0 & -3 & 1 & 1 \\ \hline 0 & 0 & 0 & 0 \end{array}\right)$$

We encountered a tautology $0 = 0$. We have two pivot rows left:

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 1 \\ 0 & -3 & 1 & 1 \\ \hline 1 & 4 & 0 & 0 \\ 0 & -3 & 1 & 1 \\ \hline x & +4y & & = 0 \\ 0 & -3y & +z & = 1 \end{array}\right)$$

y can be chosen arbitrarily. $y = t$ once y has been defined.

$$z = 1 + 3y = 1 + 3t$$

$$x = -4y = -4t$$

The solution set is given as:

$$\{(-4t, t, 1+3t) \mid t \in \mathbb{R}\}$$

This is a line in $\mathbb{R}^3$.

Example without solution

$$\begin{aligned} 3x + 2y + z &= 3 \\ 2x + y + z &= 0 \\ 6x + 2y + z &= 6 \end{aligned}$$

$$\left(\begin{array}{ccc|c} 3 & 2 & 1 & 3 \\ 2 & 1 & 1 & 0 \\ 6 & 2 & 4 & 6 \\ \hline -1 & -1 & 0 & -3 \\ -6 & -6 & 0 & -6 \\ \hline 0 & 0 & 0 & 12 \end{array}\right)$$

There is no solution to $0 = 12$. Therefore no solution is possible for the equation system.

4.2 Gauss-Jordan elimination algorithm

1. Write matrix
2. Find $a_{ij} \neq 0$ ("pivot element" which was not a pivot element before, i-th row = pivot row, j-th row = pivot column)
   (a) mark a_{ij}
   (b) subtract $\frac{a_{kj}}{a_{ij}}$ times i-th row from the k-th row for every $k \neq i$. In the j-th row a zero is created.
3. If no new pivot element can be found:
   (a) Delete all rows, which only have 0s on the left and right side
   (b) If there is a row which contains only 0s on the left side
      i. If right-hand side is not 0, NO SOLUTION!
      ii. If right-hand side is 0, apply back substitution meaning
      iii. Iterate over all pivot elements in reversed order and create 0 in corresponding pivot column
      iv. All columns which look like the pivot column, are assigned to free parameters
      v. those x_j, which are assigned to pivot columns, can be represented by the right side and free parameters

Example with 4 equations

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 1 & -2 & -3 \\ 2 & 3 & 4 & 5 & 6 \\ 1 & 1 & 1 & 1 & 1 \\ \hline 0 & -2 & -2 & -6 & -8 \\ 0 & -1 & -2 & -3 & -4 \\ 0 & -1 & -2 & -3 & -4 \end{array}\right)$$

First row is pivot row. First column is pivot column. 2nd row and 2nd column have not been pivot elements yet.

$$\left(\begin{array}{cccc|c} 0 & 0 & 2 & 0 & 0 \end{array}\right)$$

Therefore $2x_3 = 0$.

$$\left(\begin{array}{cccc|c} 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

We have found an equivalent system:

$$\left(\begin{array}{cccc|c} 1 & 2 & 3 & 4 & 5 \\ 0 & -1 & -2 & -3 & -4 \\ 0 & 0 & 2 & 0 & 0 \end{array}\right)$$

4 is a free parameter. Therefore we set $x_4 = t$. From $2x_3 = 0$, $x_3 = 0$ follows.

$$\left(\begin{array}{cccc|c} 1 & 2 & 0 & 4 & 5 \\ 0 & -1 & 0 & -3 & -4 \\ 0 & 0 & 1 & 0 & 0 \\ \hline 1 & 0 & 0 & -2 & -3 \\ 0 & -1 & 0 & -3 & -4 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

$$\begin{aligned} x_4 &= t \\ x_3 &= 0 \\ -x_2 - 3x_4 &= -4 \\ x_2 = 4 - 3x_4 &= 4 - 3t \\ x_1 - 2x_4 &= -3 \\ x_1 = -3 + 2x_4 &= -3 + 2t \end{aligned}$$

Solution set: $\{(-3 + 2t, 4 - 3t, 0, t) \,|\, t \in \mathbb{R}\}$

5 Vector spaces

A vector is an element of $\mathbb{R}^n$ ($\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R}$):

$$\left\{ a_1 a_2 v\vec{d}otsa_n \,\middle|\, a_i \in \mathbb{R} \right\}$$

Column vectors or n-tuples in $\mathbb{R}^n$.

We define addition:

$$\vec{a_1 a_2 \vdots a_n} + \vec{b_1 b_2 \vdots b_n} :- \vec{a_1 + b_1 a_2 + b_2 \vdots a_n + b_n}$$

Multiplication for $\lambda \in \mathbb{R}$:

$$\lambda \cdot \vec{a_1 a_2 \vdots a_n} :- \vec{\lambda a_1 \lambda a_2 \vdots \lambda a_n}$$

Geometric interpretation for $n = 1, 2, 3, \ldots$: For $n \leq 3$ we can think of n-tuples as points on lines, layers or within the room.

Let S be the set of all pairs of points (A, B). Consider it as directed path from A to B. Equivalence relation on S:

$$(A, B) \sim (A', B')$$

if (A', B') comes from (A, B) using a parallel translation.

Is parallel translation an equivalence relation?

reflexivity $(A, B) \sim (A, B)$, ✓

symmetry if $(A, B) \sim (A', B')$ then also $(A', B') \sim (A, B)$, inversed parallel translation, ✓

transitivity if $(A, B) \sim (A', B')$ and $(A', B') \sim (A'', B'')$, then $(A, B) \sim (A'', B'')$, composition of parallel translations, ✓

A vector is therefore an equivalence class of directed paths.

$$\overrightarrow{PQ} = [(P, Q)]$$

The set of vectors is in bijection with the set pof points. In every equivalence class there is one representative of structure $(0, A)$. $\overrightarrow{0A}$ is called position vector (dt. Ortsvektor) to A.

Addition of vectors (diagonal of a parallelogram)

Multiplication of vectors (stretching)

5.1 Properties

5.1.1 Addition

Commutativity law:

$$a + b = b + a$$

Associativity law:

$$a + (b + c) = (a + b) + c$$

Zero vector:

$$a + -a = 0$$

5.1.2 Multiplication

Associativity law:

$$\lambda \cdot (\mu \cdot a) = (\lambda \cdot \mu) \cdot a$$

Distributivity law:

$$(\lambda + \mu) \cdot a = \lambda a + \mu a$$

$$\mu \cdot (a + b) = \lambda a + \lambda b$$

5.2 Applications

5.2.1 Diagonals of a parallelogram

The diagonals of a parallelogram intersect exactly on the halfway of the whole diagonal. Hence we claim $|AS| = |SC|$ and $|BS| = |SD|$. Let M be the midpoint of $\overline{AC}$ and N be the midpoint of $\overline{BD}$. Then $M = N$ must hold.

Let's assume the opposite ($M \neq N$).

$$\overrightarrow{CM} = \overrightarrow{OA} + \frac{1}{2}\overrightarrow{AC}$$

$$= \overrightarrow{0A} - \frac{1}{2}\left(\overrightarrow{AB} + \overrightarrow{BC}\right)$$

$$\begin{aligned}
\overrightarrow{0N} &= \overrightarrow{0B} + \frac{1}{2}\overrightarrow{BD} \\
&= \overrightarrow{0A} + \overrightarrow{AB} + \frac{1}{2}\overrightarrow{BD} \\
&= \overrightarrow{0A} + \overrightarrow{AB} + \frac{1}{2}\left(\overrightarrow{BC} + \overrightarrow{CD}\right) \\
&= \overrightarrow{0A} + \overrightarrow{AB} + \frac{1}{2}\left(\overrightarrow{AD} + \overrightarrow{BA}\right) \\
&= \overrightarrow{0A} + \overrightarrow{AB} + \frac{1}{2}\overrightarrow{AD} - \frac{1}{2}\overrightarrow{AB} \\
&= \overrightarrow{0A} + \frac{1}{2}\overrightarrow{AB} + \frac{1}{2}\overrightarrow{AD} \\
&= \overrightarrow{0M}
\end{aligned}$$

5.2.2 Line crossing two points

The line crossing two points P_1 and P_2 is defined as

$$\left\{\overrightarrow{0P_1} + t \cdot \overrightarrow{P_1P_2} \,\middle|\, t \in \mathbb{R}\right\}$$

$$= \left\{\overrightarrow{0P_1} + t \cdot \left(\overrightarrow{0P_2} - \overrightarrow{0P_1}\right) \,\middle|\, t \in \mathbb{R}\right\}$$

5.2.3 A layer can be defined by three points

A layer can be defined by three points P_1, P_2 and P_3.

$$\left\{\overrightarrow{0P_1} + s \cdot \overrightarrow{P_1P_2} + t \cdot \overrightarrow{P_1P_3} \,\middle|\, s, t \in \mathbb{R}\right\}$$

5.3 Algebraic structures

A set M with a mapping $\circ : M \times M \to M$ $((x, y) \mapsto x \circ y)$ is called *Magma* or *algebraic structure*.

5.3.1 Examples

Examples for M:

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

Examples for mappings $\circ$:

$$\circ = +, \cdot$$
$$x \circ y = x + y$$
$$x \circ y = x \cdot y$$

1. Example $M = \mathbb{N}$ and $x \circ y = x^y$.
2. Example $M = \{\pm 1\}$ and $x \circ t = x \cdot y$.

	+1	-1
+1	+1	-1
-1	-1	+1

Table 2: composition table

3. Example $M = \mathcal{P}(X)$ and

$$A \circ B = \begin{cases} A \cap B \\ A \cup B \\ A \triangle B \end{cases}$$

4. Example $M = \{a, b, c, e\}$ and
5. Example $A = \{a, b, c, \dots\}$ where the set is the alphabet. Then $M = \{a_1, \dots, a_n \mid n \in \mathbb{N}, a_i \in A\}$ is the set of words. Then our composition is defined as
$$a_1 \dots a_m \circ b_1 \dots b_n = a_1 \dots a_m b_1 \cdot b_n$$
A^* is the set of possible words. A^+ is defined as $A^* \setminus \{\varepsilon\}$ where ε is the empty word.

	a	b	c	e
a	e	c	b	a
b	c	e	a	b
c	b	a	e	c
e	a	b	c	e

Table 3: composition table

6. Example $M = X^X = \{f : X \to X\}$ of an arbitrary set. $f \circ g$ is the composition (compute f after g).

5.4 Compositions

Let (M, a) be a Magma. The composition is called

associative if

$$\bigwedge_{x,y,z \in M} (x \circ y) \circ z = x \circ (y \circ z)$$

commutative if

$$\bigwedge_{x,y \in M} x \circ y = y \circ x$$

All examples above are associative[1]. The last two examples are not commutative; others are[2]

An element $e \in M$ is called

left-neutral if

$$\bigwedge_{x \in M} e \circ x = x$$

right-neutral if

$$\bigwedge_{x \in M} x \circ e = x$$

[1] Assuming the first example uses addition. x^y is not associative.
[2] Assuming the first example uses addition. x^y is not commutative.

A neutral element is left- and right-neutral.

Applied to the examples:

1. 0 acts as neutral element in addition. 1 is the neutral element of multiplication.
2. 1 is the neutral element
3. $A \cap B$ (X as neutral element), $A \cup B$ ($\emptyset$ as neutral element), $A \triangle B$ is left for the practicals
4. e as neutral element
5. ε as neutral element
6. identity function acts as neutral element, $\mathrm{id} \circ f = f' = f \circ \mathrm{id}$

Let $(M, \circ)$ be a magna with a neutral element e. Let $x \in M$, then $y \in M$ is called

left-inverse if $y \circ x = e$

right-inverse if $x \circ y = e$

An *inverse* element to x is left- and right-inverse simultaneously. x is *invertible* if an inverse element exists.

Applied to examples:

1. $(\mathbb{N}_0, +)$ has no inverse element. $(\mathbb{Z}, +)$ has an inverse element to x: $-x$. Same for $\mathbb{Q}$ and $\mathbb{R}$. $(\mathbb{N}, \cdot)$ has inverse element $\{1\}$. All non-zero elements in $(\mathbb{Q}, \cdot)$ are invertible.
2. $(\mathbb{Z}, \cdot)$ has inverse elements $\{\pm 1\}$.
3. $A \cap B = X$: inverse elements are $\{X\}$. $A \cup B = \emptyset$: inverse elements are $\{\emptyset\}$ $A \triangle B$ is left as an exercise.
4. All elements are invertible to themselves
5. For $a_1, \ldots, a_m$, the invertible elements are $\{\varepsilon\}$
6. The invertible elements are defined by any bijective mapping $X \to X$.

A *semigroup* is a magma with associative composition. A *monoid* is a semigroup with a neutral element. A group is a monoid where every element is invertible. An *abelian group* (or commutative group) is a semigroup, monoid or group with a commutative composition.

$\boxed{\text{Niels Henrik Abel (1802–1829)}}$

Examples:

1. $(\mathbb{N}, +)$ is a semi-group. $(\mathbb{N}_0, +)$ is a monoid. $(\mathbb{N}, \cdot)$ is a monoid. $(\mathbb{Z}, +)$ is a group. $(\mathbb{Z}, \cdot)$ is a monoid. $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group. $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are also groups. All of them are abelian.
2. is a group and abelian.
3. $(\mathcal{P}(X), \cap)$ and $(\mathcal{P}(X), \cup)$ are monoids. $(\mathcal{P}(X), \triangle)$ is an abelian group.
4. is an abelian group
5. $(A^+, \cdot$ is a semi-group (non-commutative). $(A^*, \circ$ is a monoid (non-commutative).
$$\mathbb{N} = A^t \text{ where } A = \{a\}$$
6. $(X^X, \circ)$ is a non-commutative monoid

Theorem 5. *A magma $(G, \circ)$ is a group iff*

G1 $\bigwedge_{x,y,z} (x \circ y) \circ z = x \circ (y \circ z)$ *"associative"*

G2 $\bigvee_{e \in G} \bigwedge_x e \circ x = x$ *"left-neutral element"*

G3 $\bigwedge_x \bigvee_y y \circ x = e$ *"left-inverse element"*

Neutral elements are necessarily right-neutral / right-inverse.

Proof. Show that

i. any left-neutral element is right-neutral

ii. left-inverse elements are right-inverse

ii. Let $x, y \in G$. y is left-inverse to x: $y \circ x = e$. Show that $x \circ y = e$.

$$x \circ y = e \circ (x \circ y) = (z \circ y) \circ (x \circ y)$$

From G3 it follows that

$$\bigvee_z z \circ y = e$$

From associativity it follows that $z \circ (y \circ x) \circ y \Rightarrow z \circ (e \circ z) \Rightarrow z \circ y = e$.

i. Let $x, y \in G$ with inverse elements x^{-1} and y^{-1}. Let $z = y^{-1} \circ x^{-1}$. Then,

$$\begin{aligned}(x \circ y) \circ z &= (x \circ y) \circ (y^{-1} \circ x^{-1}) \\ &= x \circ \underbrace{y \circ y^{-1}}_{e} \circ x^{-1} \\ &= x \circ e \circ x^{-1} \\ &= x \circ x^{-1} \\ &= e\end{aligned}$$

So $x \circ y$ is right-invertible (analogously left-invertible)

$$\Rightarrow x \circ y \in G$$

□

Theorem 6. *Let $(G, \cdot)$ be a group.*

1. *The neutral element is unique*
2. *Inverse elements are unique (therefore every element has exactly one inverse)*
3. *Equivalence laws:*

$$\bigwedge_{x,y,z \in G} x \circ z = y \circ z \implies x = z$$

$$\bigwedge_{x,y,z \in G} z \circ x = z \circ y \implies x = y$$

Proof. 1. Let e' be another neutral element:

$$e' \underbrace{=}_{e \text{ is neutral}} e' \circ e \underbrace{=}_{e' \text{ is neutral}} e$$

2. Let y, y' be two inverse elements to x

$$y \circ x = e = x \circ y$$

$$y' \circ x = e = x \circ y'$$

Show that $y = y'$:

$$y = y \circ e = y \circ (x \circ y') = (y \circ x) \circ y' = e \circ y' = y'$$

3. Let $x \circ z = y \circ z$. Let w be inverse to z: $z \circ w = e$.

$$(x \circ z) \circ w = (y \circ z) \circ w$$

$$x \circ (z \circ w) = y \circ (z \circ w)$$

$$x \circ e = y \circ e$$

$$x = y$$

□

- The unique inverse element of theorem 6 (2) of x is denoted with x^{-1}.
- Abelian groups are typically written additive. In $(G, +)$ the inverse element is denoted $-x$.

Theorem 7. *Let $(M, \cdot)$ be a monoid. Then $\{x \in M \mid x \text{ is invertible}\}$ is a group.*

Proof. Let $G = \{x \in M \mid x \text{ is invertible}\}$. Show that

1. If $x, y \in G$, then also $x \circ y \in G$.
2. Associativity is inherited from M.
3. A neutral element $e \in G$ exists.

Magma	$(M, \circ)$, $\circ : M \times M \to M$
Semigroup	+associative
Monoid	+neutral element e: $e \circ a = a = a \circ e$
Group	invertibility of all elements: $\bigwedge_x \bigvee_y x \circ y = e = y \circ x$

Table 4: Group theory cheatsheet

4. All elements are invertible in G.

Proof:

1. Let $x, y \in G$ with inverse x^{-1}, y^{-1}. Let $z = y^{-1} \circ x^{-1}$. Then it holds that

$$\begin{aligned}(x \circ y) \circ z &= (x \circ y) \circ (y^{-1} \circ x^{-1}) \\ &= x \circ y \circ y^{-1} \circ x^{-1} \\ &= x \circ e \circ x^{-1} \\ &= x \circ x^{-1} \\ &= e\end{aligned}$$

$x \circ y$ is right invertible (analogously: left invertible)

$$\Rightarrow x \circ y \in G$$

2. follows immediately

3. $e \circ e = e \implies e$ is invertible $\implies e \in G$

4. $x \in G \implies x^{-1} \in G$ because $x^{-1} \circ x = e \implies (x^{-1})^{-1} = x$

□

This lecture took place on 27th of Oct 2015 (Prof. Franz Lehner).

Theorem 8. *Let $(M, \circ)$ be a group.*

$$\begin{aligned}&\overset{G1}{\Rightarrow} \textit{associative} \\ &\overset{G2}{\Rightarrow} \bigvee_e \bigwedge_x e \circ x = x \\ &\overset{G3}{\Rightarrow} \bigvee_x \bigwedge_y y \circ x = e\end{aligned}$$

Show that

i. A left-neutral element is right-neutral

ii. Left-inverse elements are also right-inverse

Proof. ii. Let $x \in G \overset{G3}{\Rightarrow} \bigvee_y y \circ x = e$. Show that $x \circ y = e$.

$$\begin{aligned}x \circ y &\overset{G2}{=} e \circ (x \circ y) = (z \circ y) \circ (x \circ y) \\ &\overset{G3}{\Rightarrow} \bigvee_z z \circ y = e \\ &\overset{G1}{=} z \circ (y \circ x) \circ y \\ &= z \circ (e \circ y) \\ &= z \circ y = e\end{aligned}$$

i. Let $x \in G$, show that $x \circ e = x$. Let y be left-inverse to x. $e = y \circ x$.

$$x \circ e = x \circ (y \circ x) \overset{G1}{=} (x \circ y) \circ x = e \circ x \overset{G2}{=} x$$

$$\Rightarrow e \text{ is also right-neutral}$$

□

How do we construct groups? We select an associative $(M, \circ)$. $G = \{x \in M \,|\, x \text{ invertible}\}$ is a group.

Corollary 1.

$$(M, \circ) = (X^X, \circ) = \{f : X \to X\}$$

$$S_X = \{f : X \to X \ \textit{bijective}\}$$

$(S_X, \circ)$ *is a group ($\circ$ is composition of functions) and is called* symmetric group *over X or* permutation group *(if $|X| < \infty$).*

Corollary 2. *Let $X = \{1, \dots, n\}$. Let $\pi : \{1, \dots, n\} \to \{1, \dots, n\}$ bijective. Then π is typically written as scheme*

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \vdots & \vdots & \ddots & \vdots \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

is called permutation *(rearrangement).*

For finite sets $f : \{1, \dots, n\} \to \{1, \dots, n\}$ is bijective. $\Leftrightarrow$ f is injective. $\Leftrightarrow$ f is surjective. This does not hold for infinite sets.

$$f : \mathbb{N} \to \mathbb{N}$$

$$f(n) = 2n$$

is injective, but not surjective

$$S_2 = S_{\{1,2\}} = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$= \left\{ \begin{matrix} 1 & \mapsto & 2 \\ 1 & \mapsto & 2 \end{matrix}, \begin{matrix} 1 & \mapsto & 2 \\ 2 & \mapsto & 1 \end{matrix} \right\}$$

$$S_3 = S_{\{1,2,3\}} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \right\}$$

$$|S_n| = n!$$

S_3 is non-commutative!

$$\neg \bigwedge_{\pi, \phi \in S_3} \pi \circ \varphi = \varphi \circ \pi$$

Example 5.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Example 6. *Symmetry group of a rectangle: The group of motions, which keeps the rectangle invariant (ie. the rectangle is mapped to itself)*

- not *translation*
- *rotation*
- *mirroring*

Horizontal mirroring:

$$h \cong \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$$

Vertical mirroring:

$$V \cong \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$$

$$d_\pi \cong \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

Notes to create composition table:

$$v \circ h = \begin{pmatrix} A & B & C & D \\ D & C & B & A \\ C & D & A & B \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} = d_\pi$$

$$(v \circ h)^{-1} = d_\pi^{-1} = d_\pi$$

$$h^{-1} \circ v^{-1} = h \circ v$$

$$h \circ d_\pi = h \circ (h \circ v) = (h \circ h) \circ v = id \circ v = v$$

$\circ$	id	h	v	d_π
id	id	h	v	d_π
h	h	id	d_π	v
v	v	d_π	id	h
d_π	d_π	v	h	id

Table 5: Composition table for symmetry group of rectangles. The diagonal id represents that all elements are inverse to themselves. This table is symmetrical. Therefore this group is commutative.

Theorem 9. *Computations modulo n. The relation*

$$x \equiv y \mod n \Leftrightarrow n \mid x - y$$

is an equivalence relation on $\mathbb{Z}$. The equivalence classes

$$[x]_n = \{x + q \circ n \,|\, q \in \mathbb{Z}\}$$

are called residuo modulo classes *or* congruence classes modulo n.

A system of representatives is

$$\{0, \dots, n-1\}$$

Factor set:

$$\mathbb{Z}_n := \mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z} := \mathbb{Z}/\equiv_n$$

We define addition and multiplication

$$[x]_n + [y]_n := [x + y]_n$$

$$[x]_n \cdot [y]_n := [x \cdot y]_n$$

Are we allowed to define it like that? What about $[x]_n = [x + n]_n$? Does the definition not depend on the definition of the system of representatives?

Theorem 10. *(i) The addition on $\mathbb{Z}_n$ is well-defined if*

$$x \equiv x' \mod n \qquad (ie.\ [x]_n = [x']_n)$$

and

$$y \equiv y' \mod n \qquad (ie.\ [y]_n = [y']_n)$$

then also $x + y \equiv x' + y' \mod n$ (ie. $[x + y]_n = [x' + y']_n$).

$(\mathbb{Z}_n, +)$ is an abelian group with neutral element $[0]_n$ and inverse elements $-[x]_n = [-x]_n$.

(ii) The multiplication on $\mathbb{Z}_n$ is well-defined if

$$x \equiv x' \mod n$$

and

$$y \equiv y' \mod n$$

then also $x \circ y \equiv x' \cdot y' \mod n$ (ie. $[x \cdot y]_n = [x' \cdot y']_n$). $(\mathbb{Z}_n, \cdot)$ is a commutative matroid with neutral element $[1]_n$. $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]_n\}$ is a group if $n \in \mathbb{P}$

Proof. Let $x = x' \mod n$ and $y = y' \mod n$. Show that $x + y = x' + y'$ and $x \cdot y = x' \cdot y'$. $n \mid x - x'$ and $n \mid y - y'$. Show that

$$n \mid (x + y) - (x' + y') \text{ and } n \mid x \cdot y - x' \cdot y'$$

So for addition,

$$\bigvee_k x - x' = k \cdot n$$

$$\bigvee_l y - y' = l \cdot n$$

$$\begin{aligned} \Rightarrow (x + y) - (x' - y') &= x + y - x' - y' \\ &= x - x' + y - y' \\ &= k \cdot n + l \cdot n \\ &= (k + l) \cdot n \\ &= n \mid (x + y) - (x' + y') \end{aligned}$$

For multiplication,

$$\begin{aligned} x \cdot y &= (x' + kn) \cdot (y' + ln) \\ &= (x' \cdot y') + (k \cdot n \cdot y') + x' \cdot l \cdot n + k \cdot n \cdot l \cdot n \\ &= x' \cdot y' + n(R \cdot y' + l \cdot x' + k \cdot l \cdot n) \end{aligned}$$

$$xy - x'y' = \text{ multiple of } n$$
$$\Rightarrow n \mid xy - x'y'$$

□

Example 7. $(\mathbb{Z}_n, +)$ *is a group?*

- *We show G1:*

$$([x]_n + [y]_n) + [z]_n \stackrel{?}{=} [x]_n + ([y]_n + [z]_n)$$

$$[x+y]_n + [z]_n \stackrel{?}{=} [x]_n + [y+z]_n$$
$$\Rightarrow [(x+y)+z]_n = [x+(y+z)]_n$$

- *We show G2, by definition of $[0]_n$ as neutral element*

$$[x]_n + [0]_n = [x+0]_n = [x]_n$$

- *We show G3, by definition of $[-x]_n$ as neutral element*

$$[x]_n + [-x]_n = [x-x]_n = [0]_n$$

Analogously,

$$([x]_n \cdot [y]_n) \cdot [z]_n = [x]_n\,([y]_n \cdot [z]_n)$$
$$[x]_n \cdot [1]_n = [x1]_n = [x]_n$$

Therefore $[1]_n$ is the neutral element for multiplication

What is the inverse for multiplication? It is immediate, that $[0]_n$ has no inverse for multiplication.

$$[0]_n \cdot [x]_n = [0]_n \neq [1]_n$$

in $\mathbb{Z}_n \setminus \{[0]_n\}$?

Case distinction:

$n \notin \mathbb{P}$

$$\Rightarrow \bigvee_{1<n_1,n_2<n} n = n_1 \cdot n_2$$

$$[n_1]_n \cdot [n_2]_n = [n_1 \cdot n_2]_n = [n]_n = [0]_n$$
$$\Rightarrow [n_1]_n \textit{ has not inverse element!}$$

Assume

$$\bigvee_{[x]_n} [n_1]_n \cdot [x]_n = [1]_n$$

$$\Rightarrow [n_2] \cdot [n_1] \cdot [x]_n = [n_2]_n [1]_n$$
$$\Rightarrow [0]_n = [n_2]_n$$

This is a contradiction. No inverse can exist.

$n \in \mathbb{P}$ *Beforehand, for prime numbers p it holds that*

$$p \mid ab \Rightarrow p \mid a \vee p \mid b$$

Theorem 11. *We claim that every $[x]_n \neq [0]_n$ has an inverse.*

Proof.

$$V_X = \{[x], [2x], [3x], \ldots, [(n-1)x]\} \text{ multiples of } [x]_n$$

Then $[0]_n \notin V_x$. Assume

$$\bigvee_k [k \cdot x]_n = [0]_x$$

therefore

$$\bigvee_k k \cdot x \equiv 0 \mod n$$

$$\Rightarrow n \mid kx$$
$$\Rightarrow n \mid k \vee n \mid x$$
$$\Rightarrow n \mid x$$
$$\Rightarrow [x]_n$$
$$\Rightarrow [0]_n$$

This is a contradiction. □

Theorem 12. *All entries of V_X are different.*

Proof. Assume

$$\bigvee_{1\leq k,l\leq n-1} [kx]_n = [lx]_n$$

$$[kx]_n - [lx]_n = [0]_n$$

$$[(k-l)x] = [0]_n$$

$$\Rightarrow (k-l)x \equiv 0 \mod n$$

$$\Rightarrow n \mid (k-l)x$$

$$\Rightarrow n \mid k-l \vee n \mid x$$

The second condition cannot hold.

$$\Rightarrow k-l = 0$$

Requirement: $[x]_n \neq [0]_n$. □

$$\Rightarrow \{[x]_n, [2x]_n, \dots, [(n-1)x]\} \subseteq \{[1], [2], \dots, [n-1]\}$$

are all different.

$$\Rightarrow \bigvee_k : [kv]_n = [1]_n$$

$$\Rightarrow [k]_n = [x]_n^{-1}$$

k is constructed using the Euclidean algorithm.

Example 8.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 6: Composition table for $(\mathbb{Z}_5, +)$

In general $[x]_n$ is invertible iff $\gcd(x, n) = 1$.

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 7: Composition table for $(\mathbb{Z}_5, \cdot)$. Every row is a permutation of the first row. Every row (except 0) has a 1 element is therefore invertible.

·	1	2	3	4	
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
4	5	4	3	2	1

Table 8: Composition table for $(\mathbb{Z}_6, \cdot)$. 1 and 5 have a 1-element and is therefore invertible.

+	0	1
0	0	1
1	1	0

Table 9: Composition table for $(\mathbb{Z}_2, +)$

·	+1	-1
+1	+1	-1
-1	-1	+1

Table 10: Composition table for $(\{\pm 1\}, \cdot)$

$$h : \mathbb{Z}_2 \to \{\pm 1\}$$

$$[0]_2 \to +1$$
$$[1]_2 \to -2$$

The composition table of $\mathbb{Z}_2$ maps to composition table of $\{\pm 1\}$.

Therefore
$$h([x]+[y]) = h([x]) \cdot h([y]) \forall [x],[y]$$

Definition 1. *Let $(G_1, \circ)$ and $(G_2, \circ)$ be 2 groups. A map*

$$h : G_1 \to G_2$$

is called group-homomorphism if it holds that $\bigwedge_{x,y \in G_1} h(x \circ_1 y) = h(x) \circ_2 h(y)$.

This lecture took place on 3rd of November 2015 (Franz Lehner).

Definition 2. *Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be groups. A mapping $h : G_1 \to G_2$ is called group-homomorphism if $h(a \circ_1 b) = h(a) \circ_2 h(b)$ for all $a, b \in G_1$.*

Additionally

- *if h is injective, the mapping is called "field embedding".*
- *if h is surjective, the mapping is called "epimorphism".*
- *if h is bijective, the mapping is called "isomorphism".*
- *two groups are called isomorph, if there exists some isomorphism.*

Example 9. $\begin{array}{c|cc} (\mathbb{Z}_2,+) & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$ $G_1 = \mathbb{Z}_2, \circ_1 = +$ $\begin{array}{c|cc} (\{\pm 1\},\cdot) & +1 & -1 \\ \hline +1 & +1 & -1 \\ -1 & -1 & +1 \end{array}$ $G_2 = \{+1,-1\}, \circ_2 = \cdot$

$$h : \mathbb{Z}_2 \to \{\pm 1\}$$
$$[0]_2 \mapsto +1$$
$$[1]_2 \mapsto -1$$

preserves $h([a]+[b]) = h([a]) \cdot h([b])$ are isomorphic: $(\mathbb{Z}_2, +) \tilde{=} (\{\pm 1\}, \cdot)$.

Definition 3. *A homomorphism $G \to G$ is called* endomorphism. *An isomorphism $G \to G$ (bijective endomorphism) is called* automorphism.

Example 10. *1. $(\mathbb{Z}, +)$ with fixed $n \in \mathbb{N}$.*

$$h_n : \mathbb{Z} \to \mathbb{Z}$$
$$h_n : x \mapsto n \cdot x$$

Is an endomorphism.

Show that

$$\begin{aligned} h_n(x+y) &= h_n(x) + h_n(y) \\ n(x+y) &= n \cdot x + n \cdot y \end{aligned}$$

No epimorphism for $n \geq 2$.

2.

$$g : \mathbb{Z} \to \mathbb{Z}$$
$$x \mapsto x + 1$$

$$g(1+1) \stackrel{?}{=} 3$$
$$g(1) + g(1) \stackrel{?}{=} 1 + 1 + 1$$
$$4 \neq 3$$

3.

$$q_n : (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$$
$$a \mapsto [a]_n$$

Show that

$$\begin{aligned} q_n(a+b) &= q_n(a) + q_n(b) \\ q_n(a+b) &= [a+b]_n \\ &= [a]_n + [b]_n \\ &= q_n(a) + q_n(b) \end{aligned}$$

$$[0]_n = q_n(0) = q_n(n)$$

$$[1]_n = q_n(1)$$
$$\vdots$$
$$[n-1] = q_n(n-1)$$

Epimorphism, but no isomorphism.

4.
$$(\mathbb{R}^*, \cdot) \to (\{\pm 1\}, \cdot)$$

$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$
$$\text{sign} : x \mapsto \text{sign}(x)$$
$$\text{sign}(x \cdot y) = \text{sign}(x) \cdot \text{sign}(y)$$

is a group homomorphism and epimorphism, but no isomorphism.

5.
$$h : (\mathbb{Z}, +) \to (\mathbb{Z}, +)$$
$$x \mapsto -x$$
$$h(x+y) = -(x+y) = -x - y = h(x) + h(y)$$

is homomorphism.

It is surjective ($x = h(-x)$) and injective ($h(x) = h(y) \Rightarrow x = y$). Therefore it is an isomorphism.

6.
$$(\mathbb{R}^+ =]0, \infty[, \cdot) \to (\mathbb{R}, +)$$
$$x \mapsto \log(x)$$

$$\log(x \cdot y) = \log(x) + \log(y)$$

Is a group homomorphism, epimorphism and isomorphism.

Theorem 13. *1. The composition of homomorphisms is a homomorphism.*

Let
$$q : (G_1, \circ_1) \to (G_2, \circ_2)$$
$$h : (G_2, \circ_2) \to (G_3, \circ_3)$$

be homomorphisms, then $h \circ q : (G_1, \circ_1) \to (G_3, \circ_3)$ is a homomorphism.

2. The inverse mapping of an isomorphism is an isomorphism.

3. Isomorphism is an equivalence relation on the "set of all groups". Therefore on an arbitrary set of groups the relation $G_1 \tilde{=} G_2$ is an equivalence relation.

Proof. 1.
$$h \circ g(a \circ_1 b) = h \circ g(a) \circ_3 h \circ g(b)$$

$$\begin{aligned}
(h \circ g)(a \circ_1 b) &= h(g(a \circ_1 b)) \\
&\overset{\text{g is homomorphous}}{=} h(g(a) \circ_2 g(b)) \\
&\overset{\text{h is homomorphous}}{=} h(g(a)) \circ_3 h(g(b)) \\
&= (h \circ g)(a) \circ_3 (h \circ g)(b)
\end{aligned}$$

2. To be worked through in the practicals.

3. To be worked through in the practicals.

$\square$

Theorem 14. *Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be groups with a neutral element $e_1 \in G_1$ and $e_2 \in G_2$ and $h : G_1 \to G_2$ is a homomorphism. Then it holds that*

1. $h(e_1) = e_2$

2. $h(x^{-1}) = h(x)^{-1} \forall x \in G_1$

Proof. 1.

$$\begin{aligned}
h(e_1) &= h(e_1) \circ e_2 \\
h(e_1) &= h(e_1 \circ e_1) \\
&= h(e_1) \circ h(e_1) \\
h(e_1) \circ e_2 &= h(e_1) \circ h(e_1)
\end{aligned}$$

Cutback law in $G_2 \Rightarrow e_2 = h(e_1)$

2.
$$h(x^{-1}) = h(x)^{-1} \Leftrightarrow h(x) \circ h(x^{-1}) = e_2$$

$$h(x) \circ_2 h(x^{-1}) = h(x \circ_1 x^{-1}) \overset{\text{homomorphism}}{=} h(e_1) \overset{\text{bc (1)}}{=} e_2$$

Therefore $h(x^{-1}) \circ_2 h(x) = e_2$.
$\Rightarrow h(x^{-1})$ is left- and rightinverse to $h(x)$. $\Rightarrow h(x)^{-1} = h(x^{-1})$.

□

Definition 4. *A subgroup of a group $(G, \circ)$ is a non-empty subset $H \subseteq G$ such that*

1. $\bigwedge_{a,b \in H} a \circ b \in H$
2. $\bigwedge_{a \in H} a^{-1} \in H$

Notation: $H \leq G$.

Example 11.
$$(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \qquad \checkmark$$
$$(\mathbb{N}, +) \subseteq (\mathbb{Q}, +) \qquad \lightning$$
$$(\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \qquad \checkmark$$
$$(\mathbb{Q}, +) \subseteq (\mathbb{C}, +) \qquad \checkmark$$

$n \in \mathbb{N}$ is fixed:
$$n = \mathbb{Z} = \{n \cdot k \,|\, k \in \mathbb{Z}\} \leq \mathbb{Z}$$

1. $n \cdot k + n \cdot l = n \cdot (k + l) \in n \cdot \mathbb{Z}$
2. $-nk = n(-k) \in n \cdot \mathbb{Z}$

Theorem 15.
$$S_n \leq S_{n+1}$$

$$S_n = \{f : \{1, \ldots, n\} \to \{1, \ldots, n\} \text{ is bijective}\}$$
$$S_{n+1} = \{f : \{1, \ldots, n+1\} \to \{1, \ldots, n+1\} \text{ is bijective}\}$$

So $S_n \leq S_{n+1}$ cannot hold, right? S_n cannot be a subgroup.

Wrong, we interpreted it wrongfully: There is a subset $H \subseteq S_{n+1}$ which is a subgroup as by theorem 4 such that $S_n \tilde{=} H$.
$$H = \{f : \{1, \ldots, n+1\} \to \{1, \ldots, n+1\} \,|\, f \text{ is bijective}\}$$
$$\Rightarrow H \tilde{=} S_n$$

Corollary 3.
$$\mathbb{Z} \to n \cdot \mathbb{Z} \leq \mathbb{Z}$$
$$x \mapsto n \cdot x$$
is bijective.
$$\Rightarrow \mathbb{Z} \tilde{=} n \cdot \mathbb{Z}$$
$$\Rightarrow \mathbb{Z} \text{ is isomorphous to its own subgroup}$$

Remark 1. 1. *Let $H \leq G$ be a subgroup, then $e \in H$.*
Because with $H \neq \emptyset$, let $x \in H$. From the group definition it follows that $x^{-1} \in H$ and therefore $x \circ x^{-1} \in H$ with $x \circ x^{-1} = e$.

2. *$(H, \circ)$ is a group.*

Theorem 16. *Let $(G_1, \circ_1)$ and $(G_2, \circ_2)$ be groups.*
$$h : G_1 \to G_2 \text{ is a homomorphism}$$
$$H_1 \leq G_1 \qquad H_2 \leq G_2 \qquad \text{are subgroups}$$
Then it holds that

1. $h(H_1) \leq G_2$
2. $h^{-1}(H_2) \leq G_1$

Proof. 1. Let $h(H_1) \leq G_2$.
$$\Rightarrow \bigwedge_{u,v \in h(H_1)} u \circ_2 v \in h(H_1)$$
$$\Rightarrow \bigwedge_{x,y \in H_1} h(x) \circ h(y) \in h(H_1)$$
$$\Rightarrow \bigwedge_{x,y \in H_1} \bigvee_{z \in H_1} h(x) \circ h(y) = h(z)$$

h is a homomorphism:

$$\Rightarrow h(x) \circ_2 h(y) = h(x \circ_1 y)$$

$$\Rightarrow \text{choose } z = x \circ_1 y \in H_1 \text{ because } H_1 \leq G_1$$

2. Let $u \in h(H_1)$. We need to show that $u^{-1} \in h(H_1)$. Find $a \in H_1$ such that $u^{-1} = h(a)$. Let $b \in H_1$ with $h(b) = u$

$$\Rightarrow u^{-1} = h(b)^{-1} = h(b^{-1}) \in h(H_1)$$

then $b^{-1} \in H_1$.

□

Remark 2. *Always two* trivial subgroups *of a group G exist, namely*

$$H = G$$

$$H = \{e\}$$

One example which only has two trivial subgroups is $(\mathbb{Z}_p, +)$.

Definition 5. *Let $h : G_1 \to G_2$ be a homomorphism. Then $h^{-1}(\{e_2\})$ is a subgroup of G_1 and is called* kernel *of a homomorphism.*

$$\text{kernel}(h) = \{x \in G_1 \mid h(x) = e_2\}$$

$h(G_1) \leq G_2$ is a subgroup and is called image of h, *denoted* $\text{im}(h) = h(G_1)$.

Definition 6. *A* ring *is a tuple $(R, +, \cdot)$ with $R \neq \emptyset$ and $+, \cdot$ are combinations $R \times R \to R$, such that*

1. *$(R, +)$ is an abelian group ("additive group")*
2. *$(R, \cdot)$ is a semigroup ("multiplicative semigroup")*
3. *distributive laws hold*

$$(a + b) \cdot c = a \cdot c + b \cdot c$$
$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Examples include: $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$.

A ring is called commutative *if $(R, \cdot)$ is commutative. If $(R, \cdot)$ is a monoid, then $(R, +, \cdot)$ is a ring with a one-element. The neutral element with respect to $+$ is called zero-element.*

Inverse elements with respect to $+$ are denoted as $-x$. Inverse elements with respect to $\cdot$ are denoted as x^{-1}.

Example 12. *$(\mathbb{Z}, +, \cdot)$ is a commutative ring with a one-element. The same applies for $(\mathbb{Z}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$.*

$$\mathbb{R}[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{N}_0, a_i \in \mathbb{R}\}$$

is the ring of polynomials with respect to addition and multiplication (as we know it in $\mathbb{R}$). The one element with respect to multiplication is 1 *(because $a \cdot (1 \cdot x^0_+ 0 \cdot \ldots) = a$).*

$$(1 + x)^{-1} = \sum_{n=0}^{\infty} (-x)^n \notin \mathbb{R}[x]$$

$$(a_0 \cdot x^0)^{-1} = \frac{1}{a_0} x^0$$

Only constant polynomials are invertible.

Theorem 17. *$(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with a one-element.*

Proof. $(\mathbb{Z}_n, +)$ is a group. $(\mathbb{Z}_n, \cdot)$ is a monoid. They are commutative. We have already proven that.

What remains to show is the distributive law:

$$\begin{aligned}
&([a]_n + [b]_n) \cdot [c]_n \\
&\qquad = [a + b]_n \cdot [c]_n \\
&\qquad = [(a + b) \cdot c]_n \\
&\qquad = [a \cdot c + b \cdot c]_n \\
&\qquad = [a \cdot c]_n + [b \cdot c]_n \\
&\qquad = [a]_n \cdot [c]_n + [b]_n \cdot [c]_n
\end{aligned}$$

□

This lecture took place on 9th of Nov 2015 (Franz Lehner).

Definition 7. *Let $(R, +, \cdot)$ be a ring. An element $x \in R$ is called zero-divisor if $\bigvee_{y \in R} y \neq 0 \land x \cdot y = 0$. R is called zero-divisor-free if it does not contain zero-divisors.*

Theorem 18. $(\mathbb{Z}_n, +, \cdot)$ *is zero-divisor-free* $\Leftrightarrow n \in \mathbb{P}$

Definition 8. *Let $(R_1, +_1, \cdot_1)$ and $(R_2, +_2, \cdot_2)$ be rings. A mapping $h : R_1 \to R_2$ is called* ring homomorphism *if*

$$\bigwedge_{a,b \in R} h(a +_1 b) = h(a) +_2 h(b)$$

$$\bigwedge_{a,b \in R} h(a \cdot_1 b) = h(a) \cdot_2 h(b)$$

Example 13.

$$(\mathbb{Z}, +, \cdot) \to (\mathbb{Z}_n, +, \cdot)$$

$$x \mapsto [x]_n$$

Definition 9. *A field is a commutative ring $(K, +, \cdot)$ with 1 in which each element $a \in K \setminus \{0\}$ has an inverse element. Therefore $(K \setminus \{0\}, \cdot)$ is an abelian group.*

We denote $\frac{1}{x}$ instead of x^{-1}.

Example 14. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ *for* $p \in \mathbb{P}$, *not* $(\mathbb{Z}, +, \cdot)$.

Corollary 4.

1. *A field is zero-divisor-free (but not the opposite, $\mathbb{Z}$ as example)*
2. *The zero-element of a non-trivial ring cannot have an inverse*
3. *Let $|\,R\,| \geq 2$, then*

$$\underbrace{0}_{zero\ element} \neq \underbrace{1}_{one\ element}$$

> "Es ändert nichts an dem Ganzen, aber sie haben ein besseres Gefühl." (Franz Lehner)

Proof. One possible trivial ring is:

$$R = \{a\}$$

$$a + a \coloneqq a \qquad a \cdot a \coloneqq a$$

3. Select $a \not R \setminus \{0\}$. Then

$$1 \cdot a = a$$

$$0 \cdot a = 0$$

$$\Rightarrow 1 \neq 0$$

1. Let $a, b \in K \setminus \{a\}$. Assume $a \cdot b = 0$.

$$\Rightarrow 0 = a^{-1} \cdot 0 \cdot b^{-1} = a^{-1} \cdot (a \cdot b) \cdot b^{-1} = (a^{-1} \cdot a) \cdot (b \cdot b^{-1}) = 1 \cdot 1 = 1$$

$$\Rightarrow 0 = 1 \qquad ↯$$

2. Let a be inverse to 0.

$$\Rightarrow a \cdot 0 = 1$$

$$\Rightarrow a = 0$$

4.

$$\bigwedge_{a \in R} a \cdot 0 = 0$$

$$a \cdot 0 = a \cdot (0 + 0)$$

$$a \cdot 0 = a \cdot 0 + a \cdot 0$$

$$\Rightarrow a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$$

$$\Rightarrow a \cdot 0 = 0$$

□

Definition 10. (field extensions.) *The equation $x^2 - 2 = 0$ has no solution in $\mathbb{Q}$. We claim: $K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field. The proof will be provided in the practicals.*

So a field K with $\mathbb{Q} \subsetneq K \subsetneq \mathbb{R}$ is a field extension for $\mathbb{Q}$.

Definition 11. (complex numbers). *The equation $x^2 + 1 = 0$ has no solution in $\mathbb{R}$ because $x^2 > 0\ \forall x \in \mathbb{R}$. Assume some i exists with $i^2 = -1$ (therefore $i = \sqrt{-1}$) with*

$$\begin{aligned}(a+bi)+(c+di) &= a+c+(b+d)i\\ (a+bi)(c+di) &= ac+adi+bic+bdi^2\\ &= ac-bd+(ad+bc)i\end{aligned}$$

Then,

$$\begin{aligned}\frac{1}{a+bi} &= \frac{1}{a+bi}\cdot\frac{a-bi}{a-bi}\\ &= \frac{a-bi}{a^2-(bi)^2}\\ &= \frac{a-bi}{a^2+b^2}\end{aligned}$$

with $a^2 + b^2 \neq 0$ (does not hold for $a = b = 0$).

We define the complex numbers as $\mathbb{C} = \mathbb{R}^2$ with operations

$$\begin{aligned}(a,b)+(c,d) &\coloneqq (a+c,b+d)\\ (a,b)\cdot(c,d) &\coloneqq (ac-bd,ad+bc)\end{aligned}$$

We denote:

$$\begin{aligned}0 &= (0,0)\\ 1 &= (1,0)\\ i &= (0,1)\end{aligned}$$

Every $z \in \mathbb{C}$ has the structure $(a,b) = a\cdot 1 + b\cdot i$.

Theorem 19. *1. $(\mathbb{C}, +, \cdot)$ is a field (proof: provided in practicals).*

2. $\mathbb{C}$ contains $\mathbb{R}$ as subfield. Therefore

$$l : \mathbb{R} \to \mathbb{C}$$

$$x \mapsto x + 0\cdot i = (x, \circ)$$

$\mathbb{R}$ is identified with $l(\mathbb{R})$.

Corollary 5.

$$\underbrace{\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})}_{\aleph_0} \subseteq \underbrace{\mathbb{R} \subseteq \mathbb{C}}_{\aleph_1}$$

Also:

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R} \subseteq \mathbb{C}$$

Off topic: Peano curve.

Definition 12. (Fundamental theorem of algebra.) *In $\mathbb{C}$ every polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ has n solutions.*

Therefore $\mathbb{C}$ is algebraically closed (but there exist transcendal extensions).

Definition 13. (quaternions.) *$\mathbb{R}^4$ has a ring structure such that every element is invertible, but it is not commutative (division ring with elements called* quaternions*).*

Definition 14. *Let $z = x+iy$ be some element in $\mathbb{C}$. Then $\Re(z) = x$ (real part) and $\Im(z) = y$ (imaginary part) of $\mathbb{Z}$. $\overline{z} = x - iy$ is called complex conjugate of z. i is defined as solution of the equation $x^2 + 1 = 0$.*

Geometrically, the real part if represented on the x-axis and the imaginary part is quantified on the y-axis.

- *The addition of two complex numbers then geometrically corresponds to vector addition in $\mathbb{R}^2$.*

  Complex numbers in polar coordinates are defined with

$$x + iy = r(\cos\varphi + i\cdot\sin\varphi)$$

$$\Rightarrow r = \sqrt{x^2+y^2}$$

$$\Rightarrow \varphi = \arctan\frac{y}{x}$$

- *The multiplication looks like this:*

$$\begin{aligned}
&= (x_1 + iy_1) \cdot (x_2 + iy_2) \\
&= r_1(\cos\varphi_1 + i\sin\varphi_i) \cdot r_2(\cos\varphi_2 + i\sin\varphi_2) \\
&= r_1r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + i(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2)) \\
&= r_1r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2))
\end{aligned}$$

So geometrically this is rotation by φ with scaling by factor r.

From this the Eulerian equation follows[3]*.*

$$e^{i\varphi} = \cos\varphi + i\sin\varphi$$

6 Vector spaces

Definition 15. *Let $(K, +, \cdot)$ be a field. A vector space of K is a tuple $(V, \oplus, \circledcirc)$ if $V \neq \emptyset$.*

- $V \times V \to V$
  $(\lambda, \mu) \mapsto v \oplus \mu$
- $K \times V \to V$
  $(\lambda, \mu) \to \lambda \circledcirc v$

such that

1. *$(V, \oplus)$ is an abelian group.*
2. *associative law holds:*
$$\bigwedge_{v\in V}\bigwedge_{\lambda\in K}\bigwedge_{\mu\in K} (\lambda\cdot\mu)\circledcirc v = \lambda\circledcirc(\mu\circledcirc v)$$
3. *distributive law holds:*
$$\bigwedge_{\lambda\in K}\bigwedge_{v,w\in V} \lambda\circledcirc(v\oplus w) = (\lambda\circledcirc v)\oplus(\lambda\circledcirc w)$$
$$\bigwedge_{\lambda,\mu\in K}\bigwedge_{v\in V} (\lambda+\mu)\circledcirc v = (\lambda\circledcirc v)\oplus(\mu\circledcirc v)$$
4. *Furthermore,*
$$\bigwedge_{v\in V} 1\circledcirc v = v$$

[3] but can only be seen easily with the Taylor series expansion of e

Remark 3. *The elements of V are called* vectors*. The elements of K are called* scalars*. Furthermore we simplify notation:*

- *$+$ instead of $\oplus$ (vector addition)*
- *$\cdot$ instead of $\circledcirc$ (vector multiplication)*

Example 15. *1.*

$$K^n = \left\{ \begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix} \middle| \xi \in K \right\}$$

$$\textit{with} \begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix} + \begin{pmatrix}\eta_1\\ \vdots\\ \eta_n\end{pmatrix} = \begin{pmatrix}\xi_1+\eta_1\\ \vdots\\ \xi_n+\eta_n\end{pmatrix}$$

$$\textit{and } \lambda\cdot\begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix} = \begin{pmatrix}\lambda\xi_1\\ \vdots\\ \lambda\xi_n\end{pmatrix}$$

2.

$$K^{m\times n} = \left\{ \begin{pmatrix} a_{1,1} & \dots & a_{1,n}\\ \vdots & \ddots & \vdots\\ a_{m,1} & \dots & a_{m,n}\end{pmatrix} \middle| a_{i,j}\in K \right\}$$

is the so-called component notation. Addition and mutliplication is done component-wise.

3. Let X be an arbitrary set.

$$K^X = \{f : X \to K \quad \textit{function}\}$$

$$(f+g)(x) \coloneqq f(x) + g(x)$$

$$(\lambda f)(x) := \lambda(f(x))$$
$$\Rightarrow f+g, \lambda \cdot f \in K^X$$

Proof. **(a) is a special case of (c)** Specifically $X = \{1, \dots, n\}$. Every function $f : \{1, \dots, n\} \to K$ is uniquely defined by vector $\begin{pmatrix} f(1) \\ \vdots \\ f(n) \end{pmatrix}$. On the opposite site, every vector $\begin{pmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_n \end{pmatrix}$ is a function $f : \{1, \dots, n\} \to K$ with $k \mapsto \varepsilon_k$.

(d)

$$X = \mathbb{N} \qquad K^{\mathbb{N}} = \{(\varepsilon_n)_{n\in\mathbb{N}} \mid \varepsilon_i \in \mathbb{K}\}$$

is the space of all sequences.

□

Definition 16. *If $(K, +, \cdot)$ is a ring, the structure is called* module.

Corollary 6.

$$\lambda(u+v) = \lambda u + \lambda v$$
$$(\lambda + \mu)v = \lambda v + \mu v$$
$$1 \cdot v = v$$
$$(\lambda\mu)v = \lambda(\mu v)$$

Example 16. *Let $(K^n, +, \cdot)$ be a field.*

$$K^X = \{f : X \to K\}$$

$$\bigwedge_{x\in X} (f+g)(x) = f(x) + g(x)$$
$$\bigwedge_{x\in X} (\lambda f)(x) = \lambda f(x)$$

Corollary 7. *(e) $\mathbb{R}$ is a vector space over $\mathbb{Q}$. $(\mathbb{R}, +)$ is an abelian group.*

$$\cdot : \mathbb{Q} \times \mathbb{R} \to \mathbb{R}$$

$$(\lambda \in \mathbb{Q}, x \in \mathbb{R}) \mapsto \lambda \cdot x \in \mathbb{R}$$
$$\mathbb{R} = \mathbb{Q}^X$$

but $\mathbb{Q}$ is not *a vector space over $\mathbb{R}$.*

K has a zero element denoted 0. $(V, +)$ has a neutral element; also denoted 0. You should infer from context which one is meant. At the beginning we denote the neutral element of $(V, +)$ with $\underline{0}$.

Theorem 20. *This is a direct result following from the axioms. Let $(V, +, \cdot)$ be a vector space over K.*

1. $\bigwedge_{v\in\mathbb{V}} 0 \cdot v = \underline{0}$
2. $\bigwedge_{\lambda\in K} \lambda \cdot \underline{0} = \underline{0}$
3. $\bigwedge_{v\in V} \bigwedge_{\lambda\in K} \lambda \cdot v = \underline{0} \Rightarrow \lambda = 0 \vee v = \underline{0}$
4. $\bigwedge_{v\in V} (-1) \cdot v = -v$ *with $-v$ as neutral element in $(V, +)$*

Proof. 1. For the zero element it holds,

$$0 \cdot v = (0+0) \cdot v \underbrace{=}_{\text{distr. law}} 0 \cdot v + 0 \cdot v$$

but also $0 \cdot v + \underline{0} \Rightarrow 0 \cdot v + \underline{0} = 0 \cdot v + 0 \cdot v$. $\underline{0} = 0 \cdot v$.

2.

$$\lambda \cdot \underline{0} = \lambda(\underline{0} + \underline{0}) = \lambda\underline{0} + \lambda\underline{0}$$
$$\lambda \cdot \underline{0} = \lambda \cdot \underline{0} + \underline{0} \Rightarrow \underline{0} = \lambda \cdot \underline{0}$$

3.

$$\lambda v = 0 \Rightarrow \lambda = 0 \vee v = 0$$
$$A \to B \vee C \Leftrightarrow (\neg A \vee B \vee C) \Leftrightarrow \neg(A \wedge \neg B) \vee C \Leftrightarrow A \wedge \neg B \to C$$

We show: $(\lambda v = 0 \wedge \lambda \neq 0) \Rightarrow v = 0$.

Proof.

$$\lambda \cdot v = \underline{0} \Rightarrow \lambda^{-1}(\lambda \cdot v) = \lambda^{-1} \cdot \underline{0}$$

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

$$v = 1 \cdot v = \underline{0}$$

□

4. We need to show: $(-1) \cdot v + v = 0$

   Hence, $(-1) \cdot v$ is the additive inverse to v.

$$\begin{aligned}(-1) \cdot v + v &= (-1) \cdot v + 1 \cdot v \\ &= (-1+1) \cdot v \\ &= 0 \cdot v \\ &\xRightarrow{\text{first law}} \underline{0}\end{aligned}$$

□

6.1 Subspaces, linear independence and bases

Definition 17. *Let $(V, +, \cdot)$ be a vector space over K. A subset $U \subseteq V$ is called* subspace of V *if*

U1: $U \neq \emptyset$

U2: $\bigwedge_{u,v \in U} u + v \in U$

U3: $\bigwedge_{\lambda \in K} \bigwedge_{u \in U} \lambda u \in U$

Proof.

$$\bigwedge_{u \in U} -u \in U$$

Choose $\lambda = -1$ in subspace and multiply as in theorem 4. □

Corollary 8. *The* trivial *subspaces are $U = V$ and $U = \{0\}$.*

Theorem 21. *(subspace criterion.) Let $U \subseteq V$ be a subspace.*

$$\Leftrightarrow U \neq \emptyset \wedge \bigwedge_{\lambda,\mu \in K} \bigwedge_{u,v \in U} \lambda u + \mu v \in U$$

Proof. Let $\lambda, \mu \in K$ and $u, v \in U$.

$$\mathbf{U3} \Rightarrow \lambda u \in U \wedge \mu v \in U$$
$$\mathbf{U2} \Rightarrow \lambda u + \mu v \in U$$

So **U1** is immediate, **U2** follows with $\lambda = \mu = 1$ and **U3** follows with $v = 0$ and $\mu = 0$. □

Theorem 22. *Let $(V, +, \cdot)$ be a vector space. $U \subseteq V$ is a subspace. Then*

$$(U, +|_{U \times U}, \cdot|_{K \times U})$$

is a vector space.

Proof. Associativity and distributivity gets inherited. $(U, +)$ is a group.

$$-u = (-1) \cdot u \underbrace{\in}_{\mathbf{U3}} U$$

□

Example 17. *1. $\mathbb{R}$ is a vector space over $\mathbb{Q}$.*

$$\mathbb{Q} \subseteq \mathbb{R} \textit{ is a subspace}$$

2. $V = \mathbb{R}^2$ with $U = \{(x, y) \in R^2 \mid x + y = 0\} = \{(t, -t) \mid t \in \mathbb{R}\}$. Claim: U is a subspace.

Proof. **U1** $U \neq \emptyset$ because $(0, 0) \in U$.

$$\lambda, \mu \in \mathbb{R} \qquad u, v \in U$$

Show that $\lambda u + \mu v \in U$.

Proof.

$$u = (s, -s) \text{ for some element in } \mathbb{R}$$

$$v = (t, -t) \quad t \in \mathbb{R}$$

$$\begin{aligned}\lambda u + \mu v &= \lambda(s, -s) + \mu(t, -1)\\ &= (\lambda s - \mu t, \mu t, -\mu t)\\ &= (\lambda s + \mu t, -\lambda s - \mu t)\\ &= (r, -r) \text{ with } r = \lambda s + \mu t\\ &\subseteq U\end{aligned}$$

□

□

3. $V = \mathbb{R}^2$ with $U = \left\{(x, y) \in \mathbb{R}^2 \,\middle|\, x + y = 1\right\}$ is not a subspace. $U \neq \emptyset$.

$$(0, 1) \in U$$

$$(1, 0) \in U$$

$$(0, 1) + (1, 0) = (1, 1) \notin U$$

Remark 4. *A subspace always contains the zero-vector:*

$$U \neq \emptyset \Rightarrow \bigvee_u u \in U \overset{U3}{\Longrightarrow} \underline{0} = 0 \cdot u \in U$$

Remark 5. *What is the usual approach to find possible subspaces?*

- *Is $\underline{0} \in U$? If no, no subspace exists.*
- *Else yes, $U \neq \emptyset$*

We proceed with the subspace criterion.

6.2 Construction of subspaces

Theorem 23. *Let $(V, +, \cdot)$ be vector over K. Let I be an index set. Let $(U_i)_{i\in I}$ be a family of subspaces $U_i \subseteq V$. Then $\bigcap_{i\in I} U_i$ is a subspace.*

Proof. **U1**

$$\bigcap_{i\in I} U_i \neq \emptyset$$

$$\bigwedge_{i\in I} 0 \in U_i \Rightarrow 0 \in \bigcap_{i\in I} U_i = \left\{u \,\middle|\, \bigwedge_{i\in I} u \in U_i\right\}$$

$$\Rightarrow \bigcap_{i\in I} U_i \neq \emptyset$$

UR We need to show $\lambda, \mu \in K, a, b \in \bigcap_{i\in I} U_i$ then $\lambda a + \mu b \in \bigcap_{i\in I} U_i$.

$$\bigwedge_{i\in I} a \in U_i \wedge b \in U_i \xRightarrow{\text{all } U_i \text{ are subspaces}} \bigwedge_{i\in I} \lambda a + \mu b \in U_i$$

$$\Rightarrow \lambda a + \mu b \in \bigcap_{i\in I} U_i$$

□

Remark 6. *An equivalent statement for $U_1 \cup U_2$ does not hold! Unions of subspaces must not be subspaces.*

- $U_1 = \{(x, 0) \,|\, x \in \mathbb{R}\}$
- $U_2 = \{(0, y) \,|\, y \in \mathbb{R}\}$

$$u = (1, 0) \in U_1 \subseteq U_1 \cup U_2$$

$$v = (0, 1) \in U_2 \subseteq U_1 \cup U_2$$

$$u + v = (1, 1) \notin U_1 \cup U_2$$

To construct a new subspace from $U_1 \cup U_2$ we need to extend it.

Definition 18. *Let $(V, +, \cdot)$ be a vector space in K.*

$$M \subseteq V$$

The linear hull of M is the smallest subspace of V, which contains M:

$$[M] := \bigcap \{U \subseteq V \,|\, U \cup R \text{ such that } M \subseteq U\}$$

This is a subspace by theorem 23. For $M = 0$,

$$[\emptyset] = \{0\}$$

We also say $[M]$ is the subspace generated by *M.*

Remark 7. *$[M]$ is well-defined.*

At least one subspace exists which contains M:

$$U = V \Rightarrow [M] \neq \emptyset$$

Every subspace $U \subseteq V$ which contains M, contains also $[M]$ because M occurs in $M \subseteq U$ as intersection. Therefore $[M] \subseteq U$.

This construction is not constructive! We know that one smallest subspace exists, but don't know what it looks like.

There is no known method to determine whether the given vector $v \in V$ is in $[M]$ or not.

Example 18. *(second most simple case.)*

$$M = \{a\}$$

Case distinction:

Case 1: $a = 0$

$$[\{0\}] = \{0\}$$

Case 2: $a \neq 0$

*From **U1** it follows that $[\{a\}] \neq \emptyset$ because $0, a \in [\{a\}]$.*
*From **U3** it follows that $\lambda, a \in [\{a\}] \, \forall \lambda \in K$.*

$$K \cdot a := [\{a\}] = \{\lambda a \,|\, \lambda \in K\}$$

We look at a subfield: Let $u, v \in K \cdot a$ and $\lambda, \mu \in K$. Show that

$$\lambda u + \mu v \in K \cdot a$$

$$\bigwedge_{\alpha \in K} u = \alpha \cdot a \qquad \bigwedge_{\beta \in K} v = \beta \cdot a$$

$$\lambda u + \mu u = \lambda(\alpha \cdot a) + \mu(\beta \cdot a)$$

Associativity: $(\lambda \cdot \alpha) \cdot a + (\mu \cdot \beta) \cdot a$
Distributivity: $(\lambda \cdot \alpha + \mu \cdot \beta) \cdot a \in K \cdot a$

Using these laws the subfield is actually a plane. So we look at the more general case in the next theorem.

Theorem 24. *Let $(V, +, \cdot)$ be a vector space over K with $a_1, \ldots, a_n \in V$.*

A linear combination *of vectors $a_1, \ldots, a_n$ is a vector of structure*

$$\lambda_1 \cdot a_1 + \lambda_2 \cdot a_2 + \ldots + \lambda_n \cdot a_n$$

with $\lambda_i \in K$.

Let $\emptyset \neq M \subseteq V$, then a linear combination of M is a vector of structure

$$\lambda_1 \cdot a_1 + \lambda_2 \cdot a_2 + \ldots + \lambda_n \cdot a_n$$

with $a_i \in M$, $\lambda_i \in K$ and $n \in \mathbb{N}$.

Construction of arbitrary finitely many vectors.

$$L(M) = \{\lambda_1 a_1 + \ldots + \lambda_n a_n \,|\, n \in \mathbb{N}, a_i \in M, \lambda_i \in K\}$$

is the set of all linear combinations. We define $L(\emptyset) := \{0\} = [\emptyset]$.

$$L(\{a\}) \stackrel{!}{=} \{\lambda \cdot a \,|\, \lambda \in K\} = K \cdot a = [\{a\}]$$

Theorem 25. *Let $(V, +, \cdot)$ be a vector space over K.*

$$M \subseteq V \text{ as subset}$$

Then $[M] = L(M)$.

Proof. Show that,

- $[M] \subseteq L(M)$ therefore $L(M)$ is subspace which contains M.
- $L(M) \subseteq [M]$ therefore every subspace containing M, contains also $L(M)$.

We need to show $M \subseteq L(M)$. $L(M)$ is a subspace.

U1 $L(M) \neq \emptyset$ if $M = \emptyset \Rightarrow$ by definition. If $M \neq \emptyset \Rightarrow M \subseteq L(M)$.

$M \subseteq L(M)$. Let $a \in M \Rightarrow a = 1 \cdot a \in L(M)$

$$n = 1 \qquad a_1 = a \qquad \lambda_1 = 1$$

$M \subseteq L(M)$. $L(M)$ is a subspace.

Subfield: Let $u, v \in L(M)$ and $\lambda, \mu \in K$. Then also $\lambda u + \mu v \in L(M)$. Let $u = \lambda_1 a_1 + \ldots + \lambda_m a_m$ with $\lambda_i \in K$ and $a_i \in M$. Let $v = \mu_1 b_1 + \ldots + \mu_n b_n$ with $\mu_i \in K, b_i \in M$.

$$\begin{aligned}
\lambda u + \mu v &= \lambda(\lambda_1 a_1 + \ldots + \lambda_m a_m) + \mu(\mu_1 b_1 + \ldots \mu_n b_n) \\
&= \lambda\lambda_1 + \ldots + \lambda\lambda_m a_m + \mu\mu_1 b_1 + \ldots + \mu\mu_n b_n \\
&= v_1 c_1 + \ldots + v_{m+n} c_n \in L(M)
\end{aligned}$$

with

$$c_i = \begin{cases} a_i & i \leq m \in M \\ b_{i-m} & i \geq m+1 \end{cases}$$

$$v_i = \begin{cases} \lambda \cdot \lambda_i & i \leq i \leq n \\ \mu\mu_{i-m} & m+1 \leq i \leq m+n \end{cases}$$

□

This lecture took place on 16th of Nov 2015 (Franz Lehner).

6.3 Revision

$$U \subseteq V \qquad U \neq \emptyset$$

(1) $U \neq \emptyset$

(UR) $a, b \in U \to \lambda a + \mu b$

Therefore every linear combination is also in U.

$$M \subseteq V \text{ subset}$$

$$[M] = \text{ smallest vector space which contains } V := \bigcap_{U \subseteq V} U \supseteq \{0\}$$

$$L(M) = \{\lambda v_1 + \ldots + \lambda_n v_n \,|\, n \in \mathbb{N}, \lambda \in K, v_n \in M\}$$

Theorem 26.

$$[M] = L(M)$$

$$[M] \subseteq L(M)$$

$$L(M) \subseteq [M]$$

$\boxed{\text{ToDo content incomplete/incorrect}}$

Proof. It suffices to show, that every subspace U, which contains M, contains also $L(M)$. Every U in intersection $\bigcap_{M \subseteq U} U$ contains also $L(M)$.

$$\lambda_1, \ldots, \lambda_n \in K \Rightarrow L(M) \subseteq \bigcap_U U$$

Let v_1, □

Remark 8. *1. If $M \subseteq V$ is itself a subvector space*

$$\Rightarrow [M] = M$$

2. *especially for arbitrary subsets $M \subseteq V$*

$$[[M]] = [M]$$

3. *Regarding notation: The linear combination of $M \subseteq V$ is defined as,*

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n$$

where $n \in \mathbb{N}$ is finite. Equivalently (but shorter) we denote,

$$\sum_{a \in M} \lambda_a \cdot a$$

*If $\lambda_a = 0 \forall a \in M$, then the zero vector (*trivial *linear combination) is given, which is element of the linear hull of any vector space.*

Example 19.

$$V = \mathbb{R}^3 \qquad K = \mathbb{R}$$

$$M = \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

$$[M] = L(M) = \left\{ \lambda \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \mu \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \middle| \lambda, \mu \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} \lambda \\ \lambda \\ \lambda + \mu \end{pmatrix} \middle| \lambda, \mu \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} \lambda \\ \lambda \\ \mu' \end{pmatrix} \middle| \lambda, \mu' \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \middle| x_1 = x_2 \right\}$$

Example 20.

$$V = (\mathbb{Z}_3)^3 \qquad K = \mathbb{Z}_3$$

$$V = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \middle| x \in \mathbb{Z}_3 \right\}$$

$$\left| (\mathbb{Z}_3)^3 \right| = 3^3 = 27$$

$$M = \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\}$$

$$L(M) = \left\{ \lambda_1 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \lambda_3 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \middle| \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_3 \right\}$$

$$= \left\{ \begin{pmatrix} \lambda_2 + \lambda_3 \\ \lambda_1 + \lambda_2 \\ \lambda_2 + \lambda_3 \end{pmatrix} \middle| \lambda_2 \in \mathbb{Z}^3 \right\}$$

Let $\mu_2 = \lambda_2 + \lambda_3$ and $\mu_1 = \lambda_1 + \lambda_2$.

$$= \left\{ \begin{pmatrix} \mu_2 \\ \mu_1 \\ \mu_2 \end{pmatrix} \middle| \mu_1, \mu_2 \in \mathbb{Z}_3 \right\}$$

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

We omitted vector $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, because it is a linear combination of the others. Therefore we omit it.

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \in L\left(\left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\} \right)$$

Theorem 27. *Let $M \subseteq V$ subset. Let $a \in L(M)$ then $L(M) = L(M \cup \{a\})$. The linear hull does not grow, if the vector space is extended by an element of the linear hull.*

Proof. We need to show:

$$a \in L(M) \Rightarrow L(M) = L(M \cup \{a\})$$

- $L(M) \subseteq L(M \cup \{a\})$ holds trivially.
- It remains to show that $L(M \cup \{a\}) \subseteq L(M)$.
  In general, a linear combination w of $L(M \cup \{a\})$ is given by,

$$\bigvee_{\lambda_i \in K} \bigvee_{w_i \in M \cup \{a\}} w = \lambda_1 w_1 + \ldots + \lambda_k w_k \qquad i \in [1,k]$$

  For $a \in L(M)$ there exist $\mu_i \in K$ and $v_i \in M$ for $i \in [1,k]$ such that,

$$a = \mu_1 v_1 + \mu_2 v_2 + \ldots + \mu_k v_k$$

  In the linear combination of w, a occurs as w_i for some $i \in \mathbb{N}$. Without loss of generality, $w_1 = a$.

$$\begin{aligned} w &= \lambda_1 a + \lambda_2 w_2 + \ldots + \lambda_k w_k \\ &= \lambda_1 (\underbrace{\mu_1 v_1 + \ldots + \mu_n v_n}_{\text{all } \mu_i, v_i \in M}) + \underbrace{\lambda_2 w_2 + \ldots + \lambda_k w_k}_{\text{all } \lambda_i, w_i \in M} \\ &= (\lambda_1 \mu_1) v_1 + \ldots + (\lambda_1 \mu_n) v_n + \lambda_2 w_2 + \ldots + \lambda_k w_k \\ &\in L(M) \end{aligned}$$

  In other words, let $a \in M$, if $a \in L(M \setminus \{a\})$ then $L(M) = L(M \setminus \{a\})$.

$\square$

Question: Is there always a minimal generating system? Can we determine whether M is minimal?

Definition 19. *Let $(V, +)$ be a vector space over K. A tuple $(v_1, \ldots, v_k) \in V$ is called linear independent, iff*

$$\bigwedge_{\lambda_1, \ldots, \lambda_n \in K} \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n = 0$$

$$\Rightarrow \lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$$

Example 21.

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

is linear independent.

$$\lambda_1 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\Rightarrow \lambda_1 = 0 \wedge \lambda_2 = 0$$

Example 22.

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

is not linear independent!

$$\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\lambda_1 = 1 \qquad \lambda_2 = 1 \qquad \lambda_3 = -1$$

Theorem 28. *For a family $(U_i)_{i \in I}$ with an arbitrary index set I is called linear independent iff every finite subset is linear independent.*

Theorem 29. *A subset $M \subseteq V$ is called linear independent if for every subfamily $v_1, \ldots, v_n$ every pairwise distinct $v_i \in M$ are linear independent. A* family *$(v_i)_{i \in I}$ is a mapping*

$$f : I \to V$$

$$i \mapsto v_i$$

In comparison with sets elements are allowed to have duplicates. Every element has a fixed index. An n-tuple is a finite family: mapping $\{1, \ldots, n\} \to V$.

Theorem 30. *A rather informal statement: "The vectors $v_1, \dots, v_k$ are linear independent" iff the tuples $(v_1, \dots, v_n)$ are linear independent.*

Definition 20. $(v_i)_{i \in \emptyset}$ *is defined to be linear independent.*

Corollary 9. *The one-tuple* (0) *is linear dependent.*

$$1 \cdot 0 = 0$$

with 1 *as an arbitrary scalar. An* n*-tuple* v *is linear independent iff* $v \neq 0$*. If* $v \neq 0$ *and* $\lambda v = 0$*, then* $\lambda = 0$ *must hold.*

Corollary 10. *Let*

$$(v_1, \dots, v_n) \subseteq V$$

be a tuple. If $v_k = 0$ *for some* k*, then* $(v_1, \dots, v_k)$ *is linear dependent.*

$$0 \cdot v_1 + 0 \cdot v_2 + \ldots + 1 \cdot v_k + 0 \cdot k_{k+1} + \ldots + 0 \cdot v_n = 0$$

$$\lambda_1 = \begin{cases} 1 & i = k \\ 0 & i \neq k \end{cases}$$

Corollary 11. *If* $v_k = v_l$ *for some* $k \neq l$*, then* $(v_1, \dots, v_n)$ *is linear dependent.*

$$0v_1 + \ldots + 0v_{k-1} + 1 \cdot v_k + 0 \cdot v_{k+1}$$

$$\ldots (-1)v_l + 0v_{l+1} + \ldots + 0 \cdot v_n = 0$$

$$\lambda_1 = \begin{cases} 1 & i = k \\ -1 & i = l \\ 0 & \textit{else} \end{cases}$$

Corollary 12. *If* $M \subseteq V$ *is linear independent and* $N \subseteq M$*,* N *is also linear independent.*

Corollary 13.

$$(v_1, \dots, v_n) \textit{ is linear independent}$$

$$\Leftrightarrow \bigvee_{\lambda_1, \dots, \lambda_n \in K} \lambda_1 v_1 + \ldots + \lambda_n v_n = 0$$

$$\Rightarrow \bigvee_{k \in \{1, \dots, n\}} \bigvee_{\lambda_1, \dots, \lambda_n} v_l = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

Therefore one vector exists which can be represented using the other vectors.

Example 23.

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

are linear independent.

$$\lambda_1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \lambda_1 \\ \lambda_1 + \lambda_2 \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Example 24.

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

is linear dependent. But

$$\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

is linear independent.

$$\lambda_1 = 0 \qquad \lambda_1 + \lambda_2 = 0$$

$$\Rightarrow \lambda_1 - \lambda_2 = 0$$

Definition 21.

$$V = K^n$$

The unit vector is defined as

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

where the 1 *is given in row* i*.*

$(e_1, \dots, e_n)$ *is linear independent.*

$$\lambda_1 e_1 + \ldots + \lambda_n e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

then for all $\lambda_i = 0$.

Theorem 31. *Let $v_1, \dots, v_n \in V$. Then it holds equivalently,*

1. $(v_1, \dots, v_n)$ *is linear independent.*
2. $\bigwedge_{v \in L(\{v_1,\dots,v_n\})} \dot{\bigvee}_{\lambda_1,\dots,\lambda_n \in K} v = \lambda_1 v_1 + \ldots + \lambda_n v_n$
3. $\bigwedge_{k \in \{1,\dots,n\}} v_k \notin L(\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\}) = \{v_1, \dots, v_{\hat{k}}, \dots, v_n\}$
4. $\bigwedge_{k \in \{1,\dots,n\}} L(\{v_1, \dots, v_{\hat{k}}, \dots, v_n\}) \neq L(\{v_1, v_2, \dots, v_n\})$

Proof. Circle conclusion: $1 \to 2 \to 3 \to 4 \to 1$.

$1 \to 2$ For every $v \in L(v_1, \dots, v_n)$, $\bigwedge_{\lambda_1,\dots,\lambda_n} v = \lambda_1 v_1 + \ldots + \lambda_n v_n$. But is it unique? Assume $v = \mu_1 v_1 + \ldots + \mu_n v_n$. Show that for all $\lambda_i = \mu$.

$$\Rightarrow v - v = \lambda_1 v_1 + \ldots + \lambda_n v_n - (\lambda_1 v_1 + \ldots + \lambda_n v_n)$$

$$0 = (\lambda_1 - \mu_1) v_1 + (\lambda_2 - \mu_2) v_2 + \ldots + (\lambda_n - \mu_n) v_n$$

linear independence $\Rightarrow \mu_1 - \mu = 0 \qquad \lambda_n - \mu_n = 0$ Therefore for all, $\lambda_i = \mu_i$.

$2 \to 3$ Assume

$$\bigvee_k U_k \in L(\{v_1, \dots, v_{\hat{k}}, \dots, v_n\})$$

$$\Rightarrow \bigvee_{\lambda_1,\dots,\lambda_n} v_k = \lambda_1 v_1 + \ldots + \lambda_{n-1} N_{k-1} + 0 + \lambda_{k+1} v_{k+1} + \ldots + \lambda_n v_n$$

$$\bigvee_{\lambda_1,\dots,\lambda_n} v_k = 0 v_1 + \ldots + 0 v_{k-1} + 1 \cdot v_k + 0 v_{k+1} + 0 \cdot v_n$$

So v_k has two different representations, this is a contradiction.

$3 \to 4$ $\boxed{\text{TODO content incomplete/incorrect}}$ Let $\lambda_1 v_1 + \ldots + \lambda_n v_n = 0$. Show that all $\lambda_i = 0$. Assume $\bigwedge_k v_k = 0$.

$$\Rightarrow \lambda$$

$4 \to 1$ $\boxed{\text{TODO content incomplete/incorrect}}$

$$\Rightarrow v_k \in L(\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\})$$

$$\Rightarrow L(\{v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_n\}) = L(\{v_1, \dots, v_k, \dots, v_n\})$$

This is a contradiction to (4).

□

This lecture took place on 17th of November 2015 (Franz Lehner).

$$\underbrace{[M]}_{\text{smallest subspace} \supseteq M} = \underbrace{L(M)}_{\text{set of all linear combinations}}$$

In general: $M \subseteq V$ is called linear independent, if every subfamily of p_n different element is linear independent.

$$\Leftrightarrow \bigwedge_{v \in L(\{v_1,\dots,v_n\})} \dot{\bigvee}_{\lambda_1,\dots,\lambda_n} v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

$$\Leftrightarrow \bigwedge_k v_k \notin L(\{v_1, \dots, \hat{v_k}, \dots, v_n\})$$

$$\Leftrightarrow \bigwedge_{v \in L(M)} \bigvee_{n \in \mathbb{N}} \dot{\bigvee}_{v_1,\dots,v_n \in M} \bigvee_{\lambda_1,\dots,\lambda_n} v = \lambda_1 v_1 + \ldots + \lambda_n v_n$$

$$L(M) = V$$

Definition 22.
- *A family/set $S \subseteq V$ is called* generating system *if $V = [S] = L(S)$. "V is generated by S."*
- *V is called* finitely generated *if a finite generating system exists.*

- *A* basis *of a vectorspace V is a linear independent generating system. Therefore a family $B = (b_i)_{i\in I} \subseteq V$ such that $L(B) = V$, B is linear independent.*

Remark 9.
- *$(b_i)_{i\in I}$ is a basis of V, if*
  - *every element is a linear combination of a finite subfamily $b_{i_1}, \ldots, b_{i_n}$.*
  - *every finite subfamily is linear independent.*
- *$(b_i)_{i\in\emptyset}$ is basis of $\{0\}$.*
- *if $(b_1, \ldots, b_n)$ is a basis of V then also every permutation $(b_{i_1}, \ldots, b_{i_n})$ (addition is commutative).*

Example 25. *In K^n. Let $e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ be the unit vector, then $(e_1, e_2, \ldots, e_n)$ is a basis of K^n; specifically called* canonical basis *(or* standard basis*).*

Remark 10. *e_i is linear independent.*

$$\sum_{i=1}^{n} \lambda_i e_i = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

$$= 0 \Leftrightarrow \text{ all } \lambda_i = 0$$

Every vector is reachable by a linear combination of e_i.

Example 26.

$$K[X] \coloneqq V = K^{\mathbb{N}_0} = \{(a_n)_{n\geq 0} \,|\, a_n \in K\}$$

Is the vector space of all sequences.

$$e_i = (0, \ldots, 1, 0, \ldots) \qquad i \in \mathbb{N}_0$$

where 1 is given on the i-th position. If $\sum \lambda_i e_i = (0, 0, \ldots) \Rightarrow$ all $\lambda_i = 0$ and $(\lambda_0, \lambda_1, \ldots) \Rightarrow (e_i)_{i\in\mathbb{N}_0}$ is linear independent.

Is not a basis, because 1 can never be reached.

$$(1, 1, 1, 1, \ldots) \in \mathbb{R}^{\mathbb{N}_0}$$

$$\sum_{i=0}^{n} e_i = (1, 1, 1, \ldots, 1, 0, 0, 0, \ldots) + (1, 1, 1, \ldots)$$

for all $n \in \mathbb{N}$. In linear combinations only finitely many summands are allowed.

$$L\left((e_i)_{i\in\mathbb{N}_0}\right) = \text{ vector space of all sequences } (a_n)_{n\in\mathbb{N}_0} \text{ with arb. many } a_n \neq 0$$

is a subspace: $(a_1, \ldots, a_n, 0, \ldots, 0) + (b_1, \ldots, b_n, 0, \ldots, 0)$. Without loss of generality: $m \leq n$.

$$= (a_1 + b_1, \ldots, a_m + b_m, b_{m+1}, \ldots, b_n, 0, \ldots, 0)$$

$(e_i)_{i\in\mathbb{Z}_0}$ is a basis of $K[X]$; the vector space of polynomials and vector space of finite sequences.

We identify the vector space of finite sequences with the vector space of formal polynomials:

$$K[X] = \{a_0 + a_1 x + \ldots + a_n x^n \,|\, n \in \mathbb{N}_0, a_i \in K\}$$

$$\begin{aligned} &= (a_0 + a_1 x + \ldots + a_n x^n) + (b_0 + b_1 x + \ldots + b_n x^n) \\ &= (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + b_n x^n \end{aligned}$$

Without loss of generality

Instead of a unit vector e_i the formal polynomial x^i occurs.

$$\Rightarrow (x^n)_{n\geq 0} \text{ is a basis of } K[X]$$

$$\deg p(x) = \max\{i \,|\, a_i \neq 0\} = n$$

is the *degree of the polynomial.*

$$p(x) = a_0 + q_1 x + q_x x^2 + \ldots a_n x^n$$

$$\deg 0 \coloneqq -\infty$$

Every formal polynomial $p(x) = a_0 + a_1 x + \ldots + a_n x^n$ induces a polynomial function

$$K \to K$$

$$\xi \mapsto a_0 + a_1 \xi + \ldots + a_n \xi^n \in K$$

If K has infinite cardinality, then the polynomial function defines the formal polynomial uniquely.

Theorem 32. ***Attention!*** *This does not hold if the field is finite!*

Proof. There are $\left| K^K \right| = \left| K \right|^{\left| K \right|}$ different functions of $K \to K$. For example for $K = \mathbb{Z}_2$ there are 2^2 functions in $\mathbb{Z}_2 \to \mathbb{Z}_2$.

$$\mathbb{Z}_2[x] = \{a_0 + a_1 x + \ldots + a_n x^n \mid n \in \mathbb{N}_0, a_n \in \mathbb{Z}_2\}$$

There are 2^{n+1} polynomials of degree n. So they cannot be unique (no bijective function can exist to map 2^2 elements to 2^{n+1} elements). □

Does $K^{\mathbb{N}_0}$ have a basis? Does every vector space have a basis?

Theorem 33. *Every vector space has a basis.*

Proof. **Case 1** V is generated finitely.

Let $(v_1, \ldots, v_n)$ be a finite generating system. If $(v_1, \ldots, v_n)$ is linear independent, we are done. Otherwise we already know that (by a previous theorem)

$$\bigvee_{k \in \{1, \ldots, n\}} v_k \in L(v_1, \ldots, \hat{v_k}, v_n)$$

$$\Rightarrow L(v_1, \ldots, v_n) = L(v_1, \ldots, \hat{v_k}, \ldots, v_n) = V$$

- is this set linear independent, then this set is a basis.
- if not, then repeat this step.

Because originally only finitely many v_i were given, this algorithm must terminate after finitely many steps. The resulting system is linear independent and a generating system. Therefore the result is a basis.

This algorithm fails for V which are not generated finitely.

Every vector space has a basis iff you believe in the axiom of choice. □

Remark 11. *Whether every vector space has a basis depends on your faith in the Axiom of Choice (AC).*

The axiom of choice states: Let $(S_i)_{i \in I}$ be a family of non-empty sets. Then some $(x_i)_{i \in I}$ exist such that $\bigwedge_{i \in I} x_i \in S_i$.

Example 1:

$$(A)_{A \subseteq \mathbb{N}}$$

$(x_A)_{A \subseteq \mathbb{N}}$ such that $x_A = \min A$. A selection was made for every subset.

Example 2:

$$(A)_{A \subseteq \mathbb{R}}$$

$(x_A)_{A \subseteq \mathbb{R}}$ such that $x_A \in A \forall A$. Such a selection cannot be made.

Constructivists: You cannot state it explicitly, so it is not true.
General mathematicians: Well, we cannot state it, but just take one.

A consequence of the axiom of choice is the Hausdorff-Banach-Tarski paradox:

Consider a sphere in $\mathbb{R}^3$. Cut the sphere in 5 parts. Then you can move the parts such that two identical copies of the original sphere are created.

The Hausdorff-Banach-Tarski paradox is equivalent to the axiom of choice.

Constructivists do not believe in the axiom of choice and therefore the Hausdorff-Banach-Tarski paradox does not hold. The majority of mathematicians assume the axiom of choice, but following they need to accept the Hausdorff-Banach-Tarski paradox.

Remark 12. *The axiom of choice is independent of the other axioms of Zermelo-Fraenkel set theory (ZF). If ZF is contradiction-free, so is ZF + AC.*

Theorem 34. *Let V be a vector space over K*

$$B = (b_i)_{i \in I} \subseteq V$$

Then it holds equivalently, that

1. *B is a basis.*
2. *Every $v \in V$ can be represented uniquely as linear combination of B:*

$$\bigwedge_{v\in V} \bigvee_{n\in\mathbb{N}} \dot{\bigvee}_{i_1,\dots,i_n} \dot{\bigvee}_{\lambda_1,\dots,\lambda_n} v = \lambda_1 b_{i_1} + \ldots + \lambda_n b_{i_n}$$

3. *B is a maximal linear independent family.*
4. *B is a minimal generating system.*

Remark 13. *What does* minimal *mean?*

Minimal means no smaller generating system exists. Minimal does not mean, it is the smallest generating system.

Example:

$$\mathbb{R}^2 : \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

is a generating system. This is also a generating system:

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

is also a generating system.

Proof. We prove Theorem 34.

We use circular reasoning (dt. Zirkelschluss).

$1 \to 2$ Basis $\Rightarrow L(B) = V$

Let $v \in V \Rightarrow \bigvee_{\lambda_1,\dots,\lambda_n} v = \lambda_1 b_{i_1} + \ldots + \lambda_n b_{i_n}$.

We need to show uniqueness of representation: Assume $v = \mu_1 b_{j_1} + \mu_2 b_{j_2} + \ldots + \mu_m b_{j_m}$. We fill up the vectors such that $m = n$ and $j_k = i_k$.

Therefore

$$v = \mu_1 \cdot b_{j_1} + \ldots + \mu_n b_{i_n}$$

$\Rightarrow 0 = v - v = \lambda_1 b_{i_1} + \ldots + \lambda_n b_{i_n} - (\mu_1 b_{i_1} + \ldots + \mu_n b_{i_n}) = (\lambda_1 - \mu_1) b_{i_1} + \ldots + (\lambda_n - \mu_n) b_{i_n}$

(b_i) are linear independent $\Rightarrow \bigwedge_{k\in\{1,\dots,n\}} \lambda_k = \mu_k$.

$2 \to 1$ From 2 it follows that $L(B) = V$. Show that it is linear independent.

Let $\lambda_1 + b_{i_1} + \ldots + \lambda_n b_{i_n} = 0$. Condition 2 for the vector $v = 0$ implies that it is the same representation like $0 b_{i_1} + \ldots + 0 b_{i_n} = 0$. So have two representations of the vector $v = 0$. $\Rightarrow$ all $\lambda_k = 0$. Therefore B is linear independent and therefore a linear basis.

$1 \to 3$ From 1 it follows that B is linear independent. B maximal means that $\bigwedge_{v\in V\setminus B} B' = B \cup \{v\}$ is not linear independent any more.

Let $v \in V \setminus B$, but $L(B) = V$ there exists $\lambda_1, \dots, \lambda_n$ and $b_{i_1}, \dots, b_{i_n}$ such that $v = \lambda_1 b_{i_1} + \ldots + \lambda_n b_{i_n}$. Therefore $\lambda_1 b_{i_1} + \lambda_2 b_{i_2} + \ldots + \lambda_n b_{i_n} - v = 0$ Then a linear combination of $B \cup \{v\}$ is the coefficient of v. $-1 \neq 0$. $\Rightarrow B' \cup \{v\}$ is not linear independent.

$3 \to 4$ Let B be a maximal linear independent family.

1. Show that B is generating system and minimal.
   Every $v \in V$ is contained in $L(B)$. Let $v \in V$. Case distinction:
   - $v \in B \Rightarrow v \in L(B)$
   - $v \notin B$. From 3 it follows that $B \cup \{v\}$ is linear dependent.

$$\Rightarrow \bigvee_{\lambda_0,\lambda_1,\dots,\lambda_n} \bigvee_{b_{i_1},\dots,b_{i_n}\in B} \lambda_0 v + \lambda_1 b_{i_1} + \ldots + \lambda_n b_{i_n} = 0$$

But not all $\lambda_0, \dots, \lambda_n$ can be 0. If it would hold that $\lambda_0 = 0$, then $\lambda_1 b_{i_1} + \ldots + \lambda_n b_{i_n} = 0$.

$$\Rightarrow \lambda_i = 0 \text{ because } B \text{ is linear independent}$$

Therefore λ_0 cannot be 0.
$\lambda_i \neq 0 \Rightarrow$ division allowed.

$$\lambda_0 \cdot v = -\lambda_1 v_{i_1} - \ldots - \lambda_n b_{i_n}$$

$$\Rightarrow v = -\frac{\lambda_1}{\lambda_0} b_{i_1} + \ldots - \frac{\lambda_1}{\lambda_0} b_{i_n} \in L(B)$$

This holds for every $v \in V$, therefore $V = L(B)$.

- B is a minimal generating system. Assume $B' = B \setminus \{b_{i_0}\}$ is also generating system. Therefore

$$L(B \setminus \{b_{i_0}\}) = V$$
$$\Rightarrow b_{i_0} \in L(B \setminus \{b_{i_0}\})$$
$$\Rightarrow \bigvee_{\lambda_1,\dots,\lambda_n} \bigvee_{i_1,\dots,i_n \neq i_0} = \lambda 1 b_{i_1} + \ldots + \lambda_n b_{i_n}$$
$$\Rightarrow \lambda_n b_{i_1} + \ldots + \lambda_n b_{i_n} - b_{i_0} = 0$$

The coefficient of b_{i_0} is $\lambda_0 = -1 \neq 0$. This contradicts, because B is linear independent.

□

This lecture took place on 23rd of November 2015 (Franz Lehner).

6.4 Revision

A basis is a linear independent generating system.

$$\lambda_1 b_1 + \cdots + \lambda_n b_n = 0$$
$$\Rightarrow \lambda_i = 0$$

$v = 0$ has a unique representation as linear combination of the basis B.

Proof. We have already shown $1 \to 3 \to 4$. We prove $4 \to 1$.

Let B be a minimal generating system. Show that B is linear independent. Proof by contradiction.

Assume B is not linear independent. Then there are coefficients $(\lambda_1, \dots, \lambda_n) \neq (0, \dots, 0)$ such that

$$\lambda_1 b_{i_1} + \cdots + \lambda_n b_{i_n} = 0$$

There exists some k such that $\lambda_k \neq 0$.

$$\Rightarrow \lambda_k \cdot b_{i_k} = -\sum_{j \neq k} \lambda_k$$

$$b_{i_k} = -\sum_{j \neq k} \frac{\lambda_j}{\lambda_k} b_{i_j}$$
$$\Rightarrow b_{i_k} \in L(B \setminus \{b_{i_k}\})$$
$$L(B \setminus \{b_{i_k}\}) = L(B \setminus \{b_{i_k}\}) \cup \{b_{i_k}\} = L(B) = V$$

$B \setminus \{b_{i_k}\}$ is also a generating system, but smaller. So B is not minimal. □

How can we construct/find bases?

Theorem 35 (Exchange lemma). *Let $B = (b_1, \dots, b_n)$ be basis in vector space V. Let $v \in V \setminus \{0\}$. Let*

$$v = \sum_{i=1}^{n} \lambda_i \cdot b_i$$

If some $\lambda_k \neq 0$ then $B' = (b_1, \dots, b_{k-1}, v, b_{k+1}, \dots, b_n)$ is also a basis of V.

Proof. We need to show that

- B' is linear independent.
- B' is generating system.

1. Let $\mu_1, \dots, \mu_k \in K$.

$$\mu_1 b_1 + \ldots + \mu_{k-1} b_{k-1} + \mu_k v + \mu_{k+1} b_{k+1} + \cdots + \mu_n b_n = 0$$

Show that all $\mu_i = 0$.

$$\begin{aligned}
0 &= \sum_{i \neq k} \mu_i b_i + \mu_k v \\
&= \sum_{i \neq k} \mu_i b_i + \mu_k \left(\sum_{i=1}^{n} \lambda_i \cdot b_i \right) \\
&= \sum_{i \neq k} \mu_i b_i + \sum_{i \neq k} \mu_k \lambda_i b_i + \mu_k \lambda_k b_k \\
&= \sum_{i \neq k} (\mu_i + \mu_k \lambda_i) b_i + \mu_k \lambda_k b_k \\
&= \text{ is linear combination of B}
\end{aligned}$$

$$\mu_k \cdot \lambda_k = 0 \xRightarrow{\lambda_k \neq 0} \mu_k = 0$$
$$\Rightarrow \mu_i + \mu_k \lambda_i = 0 \Rightarrow \mu_i = 0 \text{ for all } i \neq k$$
$$\Rightarrow \forall \mu_i = 0$$

2. $L(B') = V$. It suffices to show that $b_k \in L(B')$.

   Then it holds that

$$L(B') = L(B' \cup \{b_k\})$$
$$B' \cup \{b_k\} = (B \setminus \{b_k\}) \cup \{b_k\} \cup \{v\} = B \cup \{v\}$$
$$\Rightarrow L(B \cup \{v\}) \supseteq L(B) = V \quad \checkmark$$

$$v = \sum_{i=1}^{n} \lambda_i b_i = \sum_{i \neq k} \lambda_i b_i + \lambda_k b_k \Rightarrow \lambda_k b_k = v - \sum_{i \neq k} \lambda_i b_i$$

$$\lambda_k \neq 0 \Rightarrow b_k = \frac{1}{\lambda_k} v - \sum_{i \neq k} \frac{\lambda_i}{\lambda_k} b_i \in L(B')$$

□

Theorem 36 (Steinitz exchange lemma)**.** *Let V be a vector space over a field K. Let $B = (b_1, \dots, b_n)$ be a basis. Let $(v_1, \dots, v_r) \subseteq V$ be linear independent with $r \leq n$.*

Then it holds that the following is a basis of V:

$$\bigvee_{i_1, \dots, i_{n+1} \in \{1, \dots, n\}} (v_1, \dots, v_r, b_{i_1}, \dots, b_{i_{n-r}})$$

Followingly $v_1, \dots, v_r$ can be exchanged as basis.

Proof. Complete induction over number of elements and using the exchange lemma.

induction base $r = 1$

1. Let (v_1) be linear independent. Then $v_1 \neq 0$. Then $B \neq \emptyset$. Then $n \geq 1$ where n is $|B|$. Because $r = 1$, $n = 1$.
2. Let $v_1 = \sum \lambda_i b_i \neq 0$. So there exists some k with $\lambda_k \neq 0$. From the exchange lemma 35 it follows that $(v_1, b_1, \dots, b_{k-1}, b_{k+1}, \dots, b_n)$ is a basis. ✓

induction step $r \to r + 1$

Let $v_1, \dots, v_{r+1}$ be linear independent.

$$\Rightarrow v_1, \dots, v_r \text{ is also linear independent}$$

$$\text{induction hypothesis} \Rightarrow \bigvee_{j_1, \dots, j_{n-r}} (v_1 \dots, v_r, b_{j_1}, \dots, b_{j_{n-r}}) \text{ is a basis}$$

1. It holds that $r \leq n$.

   We need to show that $r + 1 \leq n$, so we need to exclude that $r = n$. In that case $r + 1 \leq n$ holds (with $r < n$).

   Assume

$$r = n \Rightarrow (v_1, \dots, v_r) \text{ is a basis}$$
$$\Rightarrow (v_1, \dots, v_r) \text{ is maximal linear independent family}$$
$$\Rightarrow (v_1, \dots, v_{r+1}) \text{ is not linear independent}$$

   This is a contradiction to our assumption. So $r < n \Rightarrow r + 1 \leq n$.

2. By induction hypothesis V has a basis $(w_1, \dots, w_r, v_{i_1}, \dots, v_{i_{n-r}})$. The vector w_{r+1} can be written as

$$w_{r+1} = \sum_{i=1}^{r} \mu_i w_i + \sum_{j=1}^{n-r} \lambda_j v_{i_j}.$$

   At least one k satisfies $\lambda_k \neq 0$, otherwise $w_{r+1} \in \mathcal{L}(\{w_1, \dots, w_r\})$ in contradiction to the linear independence of $(w_1, \dots, w_{r+1})$. With the exchange lemma 35 we can replace v_{i_k} with w_{r+1}.

$$(w_1, \dots, w_{r+1}, v_{i_1}, \dots, v_{i_{k-1}}, v_{i_{k+1}}, \dots, v_{i_{n-r}})$$

   is therefore a basis.

□

Theorem 37. *Let V be a vector space over K.*

- *If V has a finite basis, then all bases are finite.*
- *For every two bases $(b_1, \dots, b_m)$ and $(b'_1, \dots, b'_n)$ it holds that $m = n$.*

Proof.
- Let $(b_1, \dots, b_n)$ be a finite basis of V. Let $(v_i)_{i \in I}$ be linear independent in V.

$$\Rightarrow \bigwedge_r v_{i_1}, \dots, v_{i_r} \text{ linear independent}$$

$$\Rightarrow r \leq n$$

$$\Rightarrow |\, I \,| \leq n$$

So every basis has at most n elements.

- Let $(b'_1, \dots, b'_r)$ be another basis $\Rightarrow$ maximal linear independent family $\Rightarrow$ $r \leq n$. From Steinitz' exchange lemma it follows that

$$\bigvee_{j_1, \dots, j_{n-r}} (b'_1, \dots, b'_r, b_{j_1}, \dots, b_{j_{n-r}}) \text{ is a basis}$$

$$(b'_1, \dots, b'_r) \text{ is maximal linear independent family}$$

$$(b'_1, \dots, b'_r, b_j, \dots, b_{j_{n-r}}) \text{ is also linear independent}$$

$$\Rightarrow n - r = 0 \Rightarrow n = r$$

□

Remark 14. *V has a basis. V is finitely generated.*

Proof. $\Rightarrow$ follows immediately.

$\Leftarrow$ use negative vectors until linear independent family remains. □

Definition 23. *Let V be a vector space over K. Assume V has a finite basis. Then the uniquely determinable number $n = \dim V$ is called dimension of the vector space. And V is called* finitely dimensional.

Otherwise $\dim V = \infty$. *V is called* infinitely dimensional.

Example 27.

$$\dim R^3 = 3$$

$$\dim \emptyset = 0$$

$$\dim K^n = n$$

$$\dim K^m = |\, M \,|$$

$$\dim K[x] = \infty \; \dots \textit{vector space of polynomials}$$

Remember that $K[x] = \{a_0 + a_1 x + \dots + a_n x^n \,|\, n \in \mathbb{N} \textit{ arbitrary}, a_i \in K\}$.

$$\Rightarrow (x^n)_{n \in \mathbb{N}} \textit{ is basis } \Rightarrow \dim K[x] = \infty$$

Theorem 38 (Basis extension theorem)**.** *(Steinitz' exchange lemma for finite vector spaces)*

Let V be a vector space with $\dim v = n < \infty$. Then every linear independent family $(v_1, \dots, v_r)$ can be extended to a basis.

Proof. Let $(b_1, \dots, b_n)$ be a basis. From Steinitz' exchange lemma it follows that $r \leq n$ and

$$\bigvee_{j_1, \dots, j_{n-r}} (v_1, \dots, v_r, b_{j_1}, \dots, b_{j_{n-r}})$$

is basis (maximal linear independent family). □

Theorem 39 (Basis selection theorem)**.** *If $(v_1, \dots, v_r)$ is a generating system of V (with $\dim V = n$). Then $r \geq n$ and $\bigvee_{j_1, \dots, j_n} (v_{j_1}, \dots, v_{j_n})$ is a basis of V.*

Proof. If $(v_1, \dots, v_r)$ is linear independent, then it is already a basis. If it is linear dependent, then

$$\bigvee_k v_k \in L(v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_r)$$

$$\Rightarrow L(v_1, \dots, v_r) = L(v_1, \dots, v_{k-1}, v_{k+1}, \dots, v_r) = V$$

We iterate this step until a linear independent family remains. □

6.5 Summary for finite vector spaces

In a finite generating vector space V

- every basis has the same number of elements ($\dim V = n$).
- every linear independent family has at most $\dim V$ elements.
- every generating system has at least $\dim V$ elements.

Theorem 40. *Let V be a vector space with $\dim V = n \in \mathbb{N}$. Let $v_1, \dots, v_n \in V$. Then the following statements are equivalent:*

1. *$(v_1, \dots, v_n)$ is basis.*
2. *$L(V_1, \dots, v_n) = V$*
3. *$(v_1, \dots, v_n)$ is linear independent.*

Proof. **1 to 2** follows immediately.

2 to 3

$$L(v_1, \dots, v_n) = V$$

From the basis extension theorem it follows that $v_{i_1}, \dots, v_{i_r}$ is a basis.

$$\dim V = n \Rightarrow r = n \Rightarrow i = 1, \dots, n$$

So we cannot remove any elements, so $(v_1, \dots, v_n)$ is already a basis.

3 to 1 Follows analogously with the basis extension theorem.

□

Theorem 41. *Let V be a vector space with $\dim V < \infty$ und $U \subseteq V$. Then it holds that,*

- $\dim U \leq \dim V$.
- $\dim U = \dim V \Leftrightarrow U = V$

Proof.
- U is finitely dimensional.

  Then every linear independent family in U is linear independent in V. Therefore $\leq \dim V$ elements.

  Let $v_1, \dots, v_r$ be basis of U.

$$\Rightarrow r \leq \dim V \quad \checkmark$$

- Let $n := \dim U = \dim V$. Let $(u_1, \dots, u_n)$ be basis of U.

$$\Rightarrow (u_1, \dots, u_n) \text{ is linear independent in } V$$

$$\Rightarrow (u_1, \dots, u_n) \text{ is basis of } V$$

  From Theorem 40 (3) it follows that $U = L(u_1, \dots, u_n) = V$.

□

6.6 Revision

- It will turn out that vector spaces with the same dimension are isomorphic.
- The dimension of a vector is the cardinality of every basis.
- It is also the maximal cardinality of a linear independent family.
- It is also the minimal cardinality of a generating system.

How do we find a basis?

- If a generating system is given, remove elements until it is linear independent.
- Otherwise add elements as long as the system remains linear independent.

6.7 Representation of vector spaces

This lecture took place on 24th of November 2015 (Franz Lehner).

Definition 24. *Let V be a vector space over K. Let $B = (b_1, \dots, b_n)$ be the basis of V. Then every $v \in V$ has a unique decomposition $v = \sum_{i=1}^{n} \lambda_i b_i$. The uniquely determinable coefficients λ_i are called* coordinates *of v with respect t B.*

$$(v)_B \coloneqq \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

is called coordinates vector *of v.*

The mapping

$$\Phi_B : V \to K^n$$

$$v \mapsto \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}$$

is called coordinate mapping.

It follows immediately that Φ_B is bijective.

Example 28.

$$V = R_3[x] = \left\{ a_0 + a_1 x + a_2 x^2 + a_3 x^3 \,\middle|\, a_i \in \mathbb{R} \right\}$$

$$B = (1 + x, 1 - x, 1 + x + x^2, x^2 + x^3) \text{ is basis of } V$$

To prove that B is a basis, it suffices to show that they are linear independent (because the dimension 4 reveals that 4 elements are required).

$$\lambda_1(1 + x) + \lambda_2(1 - x) + \lambda_3(1 + x + x^2) + \lambda_4(x^2 + x^3) = 0$$

$$(\lambda_1 + \lambda_2 + \lambda_3) \cdot 1 + (\lambda_1 - \lambda_2 + \lambda_3)x + (\lambda_3 + \lambda_4)x^2 + \lambda_4 x^3 = 0 \text{ (zero polynomial!)}$$

$$\begin{aligned}
\text{coefficient comparison} &\Rightarrow \lambda_1 + \lambda_2 + \lambda_3 = 0 \\
&\Rightarrow \lambda_1 - \lambda_2 + \lambda_3 = 0 \\
&\Rightarrow \lambda_3 + \lambda_4 = 0 \\
&\Rightarrow \lambda_4 = 0 \\
\text{coefficient comparison} &\Rightarrow \lambda_1 + \lambda_2 = 0 \\
&\Rightarrow \lambda_1 - \lambda_2 = 0 \\
\text{coefficient comparison} &\Rightarrow 2\lambda_1 = 0 \\
&\Rightarrow \lambda_2 = 0
\end{aligned}$$

$\Rightarrow$ B is linear independent $\wedge \,|\, B \,| = \dim V \Rightarrow B$ is basis (follows from Theorem 40).

Find the coordinates of the polynomial:

$$p(x) = 3 + x - 3x^2 + x^3 \text{ with respect to } B$$

Therefore we search for $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ such that,

$$p(x) = \lambda_1(1 + x) + \lambda_2(1 - x) + \lambda_3(1 + x + x^2) + \lambda_4(x^2 + x^3)$$

$$= (\lambda_1 + \lambda_2 + \lambda_3) \cdot 1 + (\lambda_1 - \lambda_2 + \lambda_3) \cdot x + (\lambda_3 + \lambda_4)x^2 + \lambda_4 x^3$$

Using coefficient comparison we get

$$\begin{aligned}
\lambda_1 + \lambda_2 + \lambda_3 &= 3 \\
\lambda_1 - \lambda_2 + \lambda_3 &= 1 \\
\lambda_3 + \lambda_4 &= -3 \\
\lambda_4 &= 1
\end{aligned}$$

$$\begin{aligned}
\lambda_3 &= -3 - \lambda_4 = -4 \\
\lambda_1 + \lambda_2 &= 3 - (-4) = 7 \\
\lambda_1 - \lambda_2 &= 1 - (-4) = 5
\end{aligned}$$

$$\begin{aligned}
2\lambda_1 &= 12 \Rightarrow \lambda_1 = 6 \\
\lambda_2 &= 7 - \lambda_1 = 1
\end{aligned}$$

So,

$$\Phi_B : \mathbb{R}_3[x] \Rightarrow \mathbb{R}^4$$
$$\Phi_B(p(x)) = \begin{pmatrix} 6 \\ 1 \\ -4 \\ 1 \end{pmatrix}$$

Theorem 42. *Let B be a basis of V. $v, w \in V$ with coordinates:*

$$\Phi_B(v) = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} \qquad \Phi_B(w) = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}$$

Then it holds that

$$\Phi_B(v+w) = \begin{pmatrix} \xi_1 + \eta_1 \\ \vdots \\ \xi_n + \eta_n \end{pmatrix} = \underbrace{\Phi_B(v) + \Phi_B(w)}_{\text{addition in } K^n}$$
$$\Phi_B(\lambda \cdot v) = \begin{pmatrix} \lambda \cdot \xi_1 \\ \vdots \\ \lambda \cdot \xi_n \end{pmatrix} = \lambda \cdot \Phi_B(v)$$

Example 29. *Let V be a vector space with basis B. $v_1, \ldots, v_k \in V$ are linear independent.*

$$\Leftrightarrow \Phi_B(v_1) \ldots \Phi_B(v_k) \text{ are linear independent in } K^n$$

7 Construction of vector spaces

Remark 15. *We have already seen $U, W \subseteq$ subspaces $\Rightarrow U \cap W$ is subspace, but not $U \cup W$.*

Definition 25. *V is a vector space. $U, W \subseteq V$ are subspaces. Then $[U \cup W]$ is the* sum of subspaces U and W

$$=: U + W = \bigcap \{z \mid z \subseteq V, U \subseteq Z, W \subseteq Z\}$$
$$= L(U \cup W) = \left\{ \sum \lambda_i u_i + \lambda \mu_i w_j \,\middle|\, u_i \in U, w_j \in W \right\}$$

Theorem 43.
$$U + W = \{u + w \mid u \in U, w \in W\}$$

Proof. Let $E := \{u + w \mid u \in U, w \in W\}$. The claim is that $[U \cup W] = E$.

We want to show that E is a subspace, $U \subseteq E, W \subseteq E$.

To show that E is a subspace, we show:

(UR) Let $v \in E, v' \in E, \lambda, \mu \in K$. Show that $\lambda \cdot v + \mu v' \in E$.

$$v \in E \Rightarrow \bigvee_{u \in U} \bigvee_{w \in W} v = u + w$$
$$v' \in E \Rightarrow \bigvee_{u' \in U} \bigvee_{w' \in W} v' = u' + w$$
$$\lambda v + \mu v' = \lambda(u + w) + \mu(u' + w')$$
$$= \underbrace{(\lambda u + \mu v')}_{\in U} + \underbrace{(\lambda w + \mu w')}_{\in W} \in E$$

$U \subseteq E$ is obvious. $u = u + 0 \in E$.
$W \subseteq E$: Every $w \in W$ is $w = 0 + w \in E$.

$[U \cup W] \supseteq E$ We need to show every subspace $Z \subseteq V$, which contains $U \cup W$, contains also E.

Let Z be a subspace. Let $v \in E$. Show that $v \in Z$.

$$v \in E \Rightarrow \bigvee_{u \in U} \bigvee_{w \in W} v = u + w$$
$$u \in U \subseteq Z \Rightarrow u \in Z$$
$$w \in W \subseteq Z \Rightarrow w \in Z$$
$$\Rightarrow u + w \in Z \text{ because } Z \text{ is subspace}$$

□

Example 30. *Let* $V = \mathbb{R}^4$.

$$U = \left\{ \begin{pmatrix} \xi \\ \eta \\ \xi \\ \eta \end{pmatrix} \middle| \xi, \eta \in \mathbb{R} \right\}$$

$$W = \left\{ \begin{pmatrix} \xi \\ \xi \\ \eta \\ \eta \end{pmatrix} \middle| \xi, \eta \in \mathbb{R} \right\}$$

$$U + W = ?$$

Determine the basis of $U + W$.

We guess the basis of U *is* $\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right)$. *We guess the basis of* W *is* $\left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right)$.

$$U = L\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right) = \left\{ \xi \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \eta \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \middle| \xi, \eta \in \mathbb{R} \right\}$$

$$W = L\left(\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right) = \left\{ \xi \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \eta \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \middle| \xi, \eta \in \mathbb{R} \right\}$$

So... und jetzt ist das Alphabet aus! (Franz Lehner)

$$\begin{aligned} U + W &= \{u + w \,|\, u \in U, w \in W\} \\ &= \left\{ \xi \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \eta \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \chi \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + w \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \middle| \xi, \eta, \chi, w \right\} \\ &= L\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right) \end{aligned}$$

$$1 \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} - 1 \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} - 1 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

The linear combination gives $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ $\Rightarrow$ *is not linear independent!*

$$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \in L\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right)$$

$\Rightarrow$ *linear hull stays the same, if we remove* $\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$

$$U + W = L\left(\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right)$$

Linear independence:

$$\lambda \begin{pmatrix}1\\0\\1\\0\end{pmatrix} + \mu \begin{pmatrix}0\\1\\0\\1\end{pmatrix} + \gamma \begin{pmatrix}1\\1\\0\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix}$$

$$\begin{pmatrix}\lambda+\gamma\\\mu+\gamma\\\lambda\\\mu\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\end{pmatrix} \Rightarrow \lambda = 0, \mu = 0 \Rightarrow \gamma = 0$$

$$\left(\begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\\0\end{pmatrix}\right) \textit{ is linear independent and basis of } U+W$$

$$\Rightarrow \dim(U+W) = 3$$

$$\dim U = 2 \qquad \dim W = 2$$

Theorem 44. *Let V be a vector space. $M, N \subseteq V$.*

$$L(M \cup N) = L(M) + L(N)$$

We will show this in the practicals.

Example 31.

$$U \cap W = \left\{ \begin{pmatrix}\xi\\\xi\\\xi\\\xi\end{pmatrix} \middle| \xi \in \mathbb{R} \right\}$$

$$\dim(U \cap W) = 1$$

$$\textit{Basis is } \begin{pmatrix}1\\1\\1\\1\end{pmatrix}$$

$$\dim(U+W) = 2 + 2 - 1$$

Theorem 45. *Let V be a vector space. $U, W \subseteq V$ are finite-dimensional subspaces. Then*

$$\dim(U+W) + \dim(U \cap W) = \dim U + \dim W$$

Theorem 46 (Inclusion-exclusion principle)**.** *In German, it is called Siebformel.*

$$|\, A \cup B \,| = |\, A \,| + |\, B \,| - |\, A \cap B \,|$$

$$|\, A \cup B \cup C \,| = |\, A \,| + |\, B \,| + |\, C \,| - |\, A \cap B \,| - |\, A \cap C \,| - |\, B \cap C \,| + |\, A \cap B \cap C \,|$$

*for $\dim(U + W + Z)$ the analogous equation is **wrong!***

Proof. Determine bases for all involved spaces.

Begin with the smallest space. Use the basis extension theorem. Let $v_1, \dots, v_r$ be basis of $U \cap W$. The basis extension theorem for U stats the $U \cap W$ is subspace of U.

$$\bigvee_{u_1,\dots,u_p} (v_1, \dots, v_r, u_1, \dots, u_p) \text{ is basis of } U$$

Analogously for W

$$\bigvee_{w_1,\dots,w_q} (v_1, \dots, v_r, w_1, \dots, w_q) \text{ is basis of } W$$

Therefore

$$U = L(\{v_1, \dots, v_r, u_1, \dots, u_p \,|\,)\}$$

$$W = L(v_1, \dots, v_r, w_1, \dots, w_q)$$

$$U + W = L(v_1, \dots, v_r, u_1, \dots, u_p, w_1, \dots, w_q)$$

Assume $v_1, \dots, v_r, u_1, \dots, u_p, w_1, \dots, w_q$ are linear independent.

$$\dim(U+W) = r + p + q$$

$$\dim(U) = r + p$$

$$\dim(W) = r - q$$

$$\dim(U \cap W) = r$$

$\Rightarrow$ the equation holds.

It remains to show that B is linear independent.

Intermediate step:

$$U \cap L(w_1, \dots, w_q) = \{0\}$$

Let $v \in U \cap L(w_1, \dots, w_q) \subseteq U \cap W \Rightarrow v \in U \wedge v \in L(w_1, \dots, w_q)$.

$$\Rightarrow \bigvee_{\lambda_1,\dots,\lambda_r,\mu,\dots,\mu_p} v = \sum_{i=1}^{r} \lambda_i v_i + \sum_{j=1}^{p} \mu_j u_j$$

$$\Rightarrow \bigvee_{\mu_1,\dots,\mu_q} v = \sum_{k=1}^{q} \mu_k w_k$$

$$v \in U \cap W \Rightarrow \bigvee_{\xi_1,\dots\xi_r} v = \sum_{l=1}^{r} \xi_l v_l$$

Consider v in W:

$$0 = v - v = \sum_{k=1}^{q} v_k w_k - \sum_{l=1}^{r} \xi_l v_l$$

$$(v_1, \dots, v_r, w_1, \dots, w_q) \text{ is basis of } W$$

$$\Rightarrow \text{ linear independence}$$

v in W is linear combination which results in 0. Therefore all coefficients are zero.

$$\Rightarrow v = 0$$

The last step remains: B is linear independent.

$$B = (v_1, \dots, v_r, u_1, \dots, u_p, w_1, \dots, w_q)$$

Let $(\lambda_i)_{i=1}^r, (\mu_j)_{j=1}^p, (\mu_k)_{k=1}^q \in K$.

$$\sum_{i=1}^{r} \lambda_i v_i + \sum_{j=1}^{p} \mu_j u_j + \sum_{k=1}^{q} \mu_k w_k = 0$$

Show that all λ_i, all μ_j and all μ_k are zero.

$$a := \underbrace{\sum_{i=1}^{r} \lambda_i v_i + \sum_{j=1}^{p} \mu_j u_j}_{\in U} + - \underbrace{\sum_{k=1}^{q} \mu_k w_k}_{\in L(w_1,\dots,w_q)}$$

$$\Rightarrow a \in U \cap L(w_1, \dots, w_q) = \{0\}$$

$$\Rightarrow a = 0 \Rightarrow \sum_{i=1}^{r} \lambda_i v_i + \sum_{j=1}^{p} \mu_j u_j = 0$$

$$\sum_{k=1}^{q} \mu_k w_k = 0$$

$v_1, \dots, v_r, u_1 \dots, u_p$ are bases in U $\Rightarrow$ linear independent.

From $0 \Rightarrow \sum_{i=1}^r \lambda_i v_i + \sum_{j=1}^p \mu_j u_j = 0$ it follows that $\lambda_1 = \dots = \lambda_r = 0$ and $\mu_1 = \dots = \mu_p = 0$.

$$(\mu_1, \dots, \mu_r, w_1, \dots, w_q) \text{ is basis in } W$$

So $\Rightarrow$ linear independence $\Rightarrow (w_1, \dots, w_q)$ is linear independent.

From $\sum_{k=1}^q \mu_k w_k = 0$ it follows that $\mu_1, \dots, \mu_q = 0$.

So the idea of this proof was to split B into two sums. We showed that their intersection is empty. Then we showed that they result in zero individually. □

Remark 16. *In this proof we have seen that every $v \in U + W$ has a unique representation $v = a + b + c$.*

$$U + W = \{u + w \mid u \in U, w \in W\}$$

$$a \in U \cap W = L(v_1, \dots, v_r)$$

$$b \in L(u_1, \dots, u_p)$$

$$c \in L(w_1, \dots, w_q)$$

The representation $v = u + w$ is not *unique with $u \in U, w \in W$ (unless $U \cap W = \{0\}$).*

$$v = \underbrace{(a + b)}_{\in U} + \underbrace{c}_{\in W} = \underbrace{b}_{\in U} + \underbrace{(a + c)}_{\in W}$$

Definition 26. *The sum $U+W$ of two subspaces is called* direct *if*

$$\bigwedge_{v\in U+W} \dot\bigvee_{u\in U} \dot\bigvee_{w\in W} v = u + w$$

If this holds, then we write $U\dot{+}W$ for the direct sum (or alternatively $U\oplus V$).

Theorem 47. *The sum $U+W$ is direct $\Leftrightarrow U\cap W=\{0\}$.*

Proof. Let $v\in U\cap W$.

$$\Rightarrow v = \underbrace{v}_{\in U} + \underbrace{0}_{\in W} = \underbrace{0}_{\in U} + \underbrace{v}_{\in W}$$

From the uniqueness of the decomposition it follows that $v=0$.

$$u,u'\in U \qquad w,w'\in W$$

We need to show that $u=u'$ and $w=w'$. Let $v\in U+W$ with the representation $v=u+w=u+w'$.

$$0 = v-v = u+w-(u'+w') = (u-u')+(w-w')$$

$$a := \underbrace{u'-u}_{\in U} = \underbrace{w-w'}_{\in W}$$

$$\Rightarrow a\in U\cap W=\{0\}$$

$$\Rightarrow a=0 \Rightarrow u'=u \wedge w=w'$$

Coefficient is zero, so $v=0$. □

This lecture took place on 30th of November 2015 (Franz Lehner).

Theorem 48.

$$\dim(U+W)=\dim(U)+\dim(W)-\dim(U\cap W)$$

If $U\cap W=\{0\}$ then the dimension is directly the sum $\dim(U)+\dim(W)$.

$$U+W=[U\cup W]=\{u+w \mid u\in U, w\in W\}$$

A sum is called direct if for all $u\in U+W$, the decomposition $u=u+w$ is unique.

Theorem 49. *The sum is direct if and only if $U\cap W=\{0\}$.*

Theorem 50. *Vector space V, $\dim(V)<\infty$. Then $U,W\subseteq V$ are subspaces.*

The following statements are equivalent:

- $V=U\dot{+}W$
- $V=U+W\wedge\dim(V)=\dim(U)+\dim(W)$
- $U\cap W=\{0\}\wedge\dim(V)=\dim(U)+\dim(W)$

Proof. **1 implies 2**

$$V=U\dot{+}W$$
$$\Rightarrow V=U+W\wedge U\cap W=\{0\} \text{ Theorem 47}$$
$$\xRightarrow{\text{Theorem 48}} \dim(U+W)=\dim(U)+\dim(W)$$

2 implies 3 We use theorem 48.

$$\dim(U+W)=\dim(U)+\dim(W)-\dim(U\cap W)$$
$$\Rightarrow \dim(V)=\dim(V)-\dim(U\cap W)$$
$$\dim(U+W)=\dim(V) \text{ because } U+W=V$$
$$\dim(U)+\dim(W)=\dim(V) \text{ is required}$$
$$\Rightarrow \dim(U\cap W)=0$$
$$\Rightarrow U\cap W=\{0\}$$

3 implies 1

$$U\cap W=\{0\}\wedge\dim(U)+\dim(W)=\dim(V)$$
$$\xRightarrow{\text{Theorem refsatz-4-5b}} \dim(U+W)=\dim(U)+\dim(W)-\dim(\{0\})$$
$$\dim(U+W)=\dim(U)+\dim(W)$$
$$U+W\subseteq V\wedge\dim(U+W)=\dim(V)\Rightarrow U+W=V$$

□

Example 32. *Consider $\mathbb{R}^2$. Let U be a subspace of dimension 1 which goes through $(0,0)$. Is there some $W \subseteq \mathbb{R}^2$ such that $\mathbb{R}^2 = U \dot{+} W$. Yes, this holds for all lines $W \neq U$ (with $\dim(W) = 1$) which go through $(0,0)$.*

Theorem 51. *Let V be a vector space with $\dim(V) < \infty$. Then it holds that*

$$\bigwedge_{U \subseteq V \text{ subspace}} \bigvee_{W \subseteq V \text{ subspace}} V = U \dot{+} W$$

W is called complementary space *of U.*

Remark 17.

1. *Complementary spaces are not uniquely defined!*
2. *If $\dim(V) = \infty$, then the question for existence of complementary spaces is difficult (depends on correctness of axiom of choice, covered in the complex analysis course)*

Proof. Let $u_1, \dots, u_n$ be basis of $U \subseteq V$. We use the basis extension theorem 38.

$$\Rightarrow \bigvee_{w_1, \dots, w_n \in V} (u_1, \dots, u_v, w_1, \dots, w_m) \text{ is basis of } V$$

Then $W = L(w_1, \dots, w_m)$ is a complementary space.

We need to show that $V = U \dot{+} W$. Therefore $V = U + W$ and $U \cap W = \{0\}$.

1. Let $u \in V$. Find $u \in U, w \in W$ such that $v = u + w$.

   B is basis

   $$\Rightarrow \bigvee_{\lambda_1, \dots, \lambda_m} \bigvee_{\mu_1, \dots, \mu_m} v = \underbrace{\lambda_1 u_1 + \dots + \lambda_r u_r}_{=u \in U} + \underbrace{\mu_1 w_1 + \dots + \mu_m w_m}_{=w \in W} = u + w \in U + W$$

2. Let $v \in U \cap W$.

   $$v \in U \Rightarrow \bigvee_{\lambda_1, \dots, \lambda_r} v = \lambda_1 u_1 + \dots + \lambda_r u_r$$

   $$v \in W \Rightarrow \bigvee_{\mu_1, \dots, \mu_m} v = \mu_1 w_1 + \dots + \mu_m w_m$$

   $$\Rightarrow 0 = v - v = \lambda_1 u_1 + \dots + \lambda_r u_r - \mu_1 w_1 - \dots - \mu_m w_m$$

   is linear combination of B, which results in 0. The basis is linear independent, therefore all $\lambda_i = 0$ and $\mu_j = 0$. Therefore $v = 0$.

□

Theorem 52. *Let V be a vector space. Let $U_1, \dots, U_m \subseteq V$ be subspaces. Then $U_1 + \dots + U_m = [U_1 \cup \dots \cup U_m]$ is the* sum of subspaces *and it holds that $U_1 + \dots + U_m = \{u_1 + \dots + u_m \mid u_i \in U_i\}$.*

The proof is provided in the practicals.

$$U_1 + (U_2 + U_3) = (U_1 + U_2) + U_3$$

Attention! *The inclusion-exclusion principle 46 does not hold for the dimension.*

Definition 27. *Let $U_1, \dots, U_m \subseteq V$ be subspaces. The sum $W = U_1 + \dots + U_m$ is called* direct*, if*

$$\bigwedge_{w \in W} \dot{\bigvee}_{u_1 \in U_1} \dots \dot{\bigvee}_{u_m \in U_m} w = u_1 + \dots + u_m$$

Therefore the decomposition must be unique. We denote:

$$W = U_1 \dot{+} U_2 \dot{+} \dots \dot{+} U_m$$

The resulting mapping

$$\pi_{\mathbb{R}} : W \to U_k$$
$$w \mapsto u_k$$

is called projection *on U_k.*

Theorem 53. *The characterization $U + W$ is direct $\Leftrightarrow U \cap W = \{0\}$ cannot be generalized. It does not suffices that $U_1 \cap \dots \cap U_m = \{0\}$*

Theorem 54. *Let V be a vectorspace. Let $U_1, \dots, U_m \subseteq V$ be subspaces with $U_i \neq \{0\}$.*

Then the sum $W = U_1 + \dots + U_m$ is direct. Therefore every family $(u_1, \dots, u_m)$ with $u_i \in U_i \setminus \{0\}$ is linear independent.

Proof. Proof direction $\Rightarrow$.

Let $u_i \in U_i \setminus \{0\}$. Show that if $\sum_{i=1}^m \lambda_i u_i = 0 \Rightarrow \lambda_i = 0 \forall i$.

Followingly therefore $\lambda_i = 0 \forall i$ and then $\lambda_i \cdot u_i = 0$. From $u_i \neq 0 \forall i$ it follows that, $\lambda_i = 0$.

Assume $\sum_{i=1}^m \lambda_i u_i = 0$.

$$\sum_{i=0}^m w_i \qquad w_i = \lambda_i u_i \in U_i$$

$\Rightarrow$ decomposition of vector 0 in components from U_i.

If the sum is direct, then the decomposition must be the same.

$$0 = 0 + 0 + \cdots + 0$$

□

Proof. Proof direction $\Leftarrow$.

Let $w \in W$ with $w = \sum_{i=1}^m u_i$. Show that the decomposition is unique.

Let $w = \sum_{i=1}^m w_i$ is a different decomposition. Show that all $u_i = u_i'$

$$0 = w - w = \sum_{i=1}^m (u_i - u_i')$$

Let

$$w_i = \begin{cases} u_i - u_i' & \text{if } u_i \neq u_i' \\ z_i \in U_i \setminus \{0\} & \text{arbitrary} \end{cases} \Rightarrow w_i \neq 0$$

Correspondingly

$$\lambda_i = \begin{cases} 1 & u_i \neq u_i' \\ 0 & u_i = u_i \end{cases}$$

$$\sum_{i=1}^m \lambda_i \cdot w_i = 0$$

$$= \sum_{\substack{i \\ u_i \neq u_i'}} u_i - u_i' + \sum_{\substack{i \\ u_i \neq u_i'}} 0 \cdot z_i = 0$$

$$w_i \text{ is linear indep.} \Rightarrow \lambda_i = 0 \forall i \Rightarrow \underbrace{\bigwedge_i}_{\lambda_i = 1 \text{ does not occur}} \qquad u_i = u_i'$$

□

> "Die Sache ist an sich klar. Nur wenn man sie niederschreibt, wird sie unklar." (Franz Lehner)

Theorem 55. *Let V be a vector space.* $\dim(V) < \infty$.

$$U_1, \ldots, U_m \subseteq V \textit{ are subspaces}, U_i \neq \{0\}$$

Then the following statements are equivalent:

1. $W = U_1 + \cdots + U_m$ *is direct.*
2. *For every choice of basis* $B_i \subseteq U_i$, $B_1 \cup \cdots \cup B_m$ *is basis of* W.
3. $\dim(W) = \sum_{i=1}^m \dim(U_i)$

Proof. 2 to 3 follows immediately.

1 to 2 Let $W = U_1 \dot{+} \ldots \dot{+} U_m$. Let $B_i = (U_{i,1}, \ldots, U_{i,\sqrt{i}})$ be basis of U_i for all i.

We need to show that $B_1 \cup \ldots B_m$ is basis of W. Therefore,

(a) $L(B_1 \cup \cdots \cup B_m) = W$

(b) $B_1 \cup \cdots \cup B_m$ is linear independent.

We prove those statements:

(a)

$$L(B_1 \cup \cdots \cup B_m) = L(B_1) + \cdots + L(B_m) = U_1 + \cdots + U_m = W$$

(b) $B_i \cup \dots \cup B_m$ is linear independent.

$$B_1 \cup \dots \cup B_m = \{b_{ij} \mid i \in \{1, \dots, m\}, j \in \{1, \dots, r_j\}\}$$

Let $\lambda_i \in K$ with $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, r_i\}$. Such that

$$\sum_{i=1}^{m} \sum_{j=1}^{r} \lambda_{ij} \mu_{ij} = 0$$

Show that all $\lambda_{ij} = 0$.
Let $w_i = \sum_{i=1}^{r} \lambda_{ij} u_{ij} \in U_i$.

$$\Rightarrow \sum_{i=1}^{m} w_i = 0$$

The sum of U_i is direct. Therefore the vector 0 has a unique decomposition. Therefore all $w_i = 0$.

$$\Rightarrow \sum_{j=1}^{r_i} = \lambda_{ij} u_{ij} = 0 \forall i$$

u_{ij} is basis of U_i. So it is linear independent. So $\lambda_{ij} = 0 \forall j \in \{1, \dots, r_i\}$.
This holds for every i

$$\Rightarrow \lambda_{ij} = 0 \qquad \forall i \forall j$$

3 implies 1 Let $B_i = (u_{i,1}, u_{i,2}, \dots, u_{i,r_i})$ be basis of U_i and $B = B_1 \cup \dots \cup B_m$ is basis of W.

Show that every $w \in W$ has a unique decomposition.

$$w = w_1 + \dots + w_m \text{ with } w_i \in U_i$$

Let $w = w_1' + \dots + w_m'$ be a different decomposition.

Let $w_i = \sum_{j=1}^{r_i} \lambda_{ij} u_{ij}$ be a decomposition of w_i in regards of basis B_i.

$$\begin{aligned} w_i' &= \sum_{j=1}^{r_i} \mu_{ij} u_{ij} \\ \Rightarrow w &= \sum_{i=1}^{m} \left(\sum_{j=1}^{r_i} \lambda_{ij} u_{ij} \right) \\ &= \sum_{i=1}^{m} \left(\sum_{j=1}^{r_i} \mu_{ij}, u_{ij} \right) \end{aligned}$$

Let (u_{ij}) be basis of W. Therefore all $\lambda_{ij} = \mu_{ij}$. Therefore $w_i = w_i'$ for all i. So the decomposition is unique.

□

Remark 18 (Special case)**.**

$$(b_1, \dots, b_m) \textit{ is basis of } W$$
$$\Leftrightarrow w = L(b_1) \dot{+} L(b_2) \dot{+} \dots \dot{+} L(b_m)$$

Theorem 56. *Let V, W be vector spaces over K.*
Given vector space X such that $X = V, W$. For example, $V = K[x]$ and $W = K^3$.
Then also

$$V \times W = \{(u, w) \mid u \in V, w \in W\}$$

with the operations

$$(v, w) + (v', w') = (v + v', w + w')$$
$$\lambda \cdot (v, w) = (\lambda v, \lambda w)$$

Given a vector space with vector 0 (which is $(0_v, 0_w)$) and an inverse element

$$-(v, w) = (-v, -w)$$

The product $V \times W$ (or denoted $V \oplus W$) is called direct product *or* outer sum *(but not $V \otimes W$ which is the tensor product).*

Theorem 57. *If* $\dim(V), \dim(W) < \infty$. *Then* $\dim(V \oplus W) = \dim(V) + \dim(W)$.

Proof. We are going to construct an appropriate basis. Let $(v_1, \dots, v_m)$ be a basis in V. Let $(w_1, \dots, w_n)$ be a basis in W.

Our claim is that $((u_1, 0), (u_2, 0), \dots, (u_m, 0), (0, w_1), (0, w_2), \dots, (0, w_n)) = B$ is a basis of $V \oplus W$.

Show that

1. B is linear independent.
2. $L(B) = V \oplus W$

Proof:

1. Let
$$\lambda_1, \dots, \lambda_{m+n} \in K \text{ such that } \sum_{i=1}^{m} \lambda_i (v_i, 0) + \sum_{j=1}^{n} \lambda_{m+j}(0, w_j) = (0, 0)$$
Show that all $\lambda_i = 0$.
$$= \sum_{i=1}^{m} (\lambda_i v_i, 0) + \sum_{j=1}^{n} (0, \lambda_{m+j} w_j)$$
$$= \left(\sum_{i=1}^{m} (\lambda_i v_i, 0) \right) + \left(0, \sum_{j=1}^{n} \lambda_{m+j} w_j \right)$$
$$= \left(\sum_{i=1}^{m} \lambda_i v_i, \sum_{j=1}^{n} \lambda_{m+j} w_j \right) \stackrel{?}{=} (0_v, 0_w)$$
$$\Rightarrow \sum_{i=1}^{m} \lambda_i v_i = 0_v \wedge \sum_{j=1}^{n} \lambda_{m+j} w_j = 0_w$$
$(v_1, \dots, v_m)$ is linear independent.
$$\Rightarrow \lambda_1 = \dots = \lambda_m = 0 \qquad \Rightarrow \lambda_{m+1} = \dots = \lambda_{m+n} = 0$$

2. Let $(v, w) \in V \oplus W$.
$$\rightsquigarrow \bigvee_{\lambda_i, \dots, \lambda_m} v = \sum_{i=1}^{m} \lambda_i v_i$$
$$\bigvee_{\mu_1, \dots, \mu_n} w = \sum_{j=1}^{n} \mu_j w_j$$
$$\begin{aligned} (v, w) &= \left(\sum_{i=1}^{m} \lambda_i v_i, \sum_{j=1}^{n} \mu_j w_j \right) \\ &= \left(\sum_{i=1}^{m} \lambda_i v_i, 0 \right) + \left(0, \sum_{j=1}^{n} \mu_j w_j \right) \\ &= \left(\sum_{i=1}^{m} \lambda_i (v_i, 0) + \sum_{j=1}^{n} \mu_j (0, w_j) \right) \in L(B) \end{aligned}$$
Every $(v, w) \in V \oplus W$ is in $L(B)$. $V \oplus W \subseteq L(B)$.

□

Remark 19. *Let* V_1 *and* V_2 *be vector spaces.*
$$V = V_1 \oplus V_2$$
Then we can identify V_1 *with the subspace*
$$U_1 = \{(v_1, 0) \mid v_1 \in V_1\} \subseteq V_1 \oplus V_2$$
analogously
$$V_2 \stackrel{\sim}{=} U_2 = \{(0, v_2) \mid v_2 \in V_2\} \subseteq V_1 \oplus V_2$$
and it holds that
$$V_1 \oplus V_2 = U_1 \dot{+} U_2$$

Theorem 58. *Let* I *be an index set. For every* $i \in I$, *let* V_i *be a vector space over* K.

Direct product:

$$\prod_{i\in I} V_i = \times_{i\in I} V_i = \{(v_i)_{i\in I} \mid v_i \in V_i \forall i\}$$

Direct outer sum:

$$\oplus_{i\in I} V_i = \{(v_i)_{i\in I} \mid v_i \in V_i \text{ and only finitely many } v_i \neq 0\}$$

They are vector spaces in regards of operations:

$$(v_i)_{i\in I} + (w_i)_{i\in I} = (v_i + w_i)_{i\in I} \qquad \lambda \cdot (v_i)_{i\in I} = (\lambda \cdot v_i)_{i\in I}$$

$$\oplus_{i\in I} V_i \subsetneq \prod_{i\in I} V_i \text{ if } I \text{ is infinite}$$

Example 33.

$$\mathbb{R}^{\mathbb{N}} = \prod_{n\in\mathbb{N}} \mathbb{R}$$

$$\begin{aligned}\oplus_{n\in\mathbb{N}}\mathbb{R} &= \left\{ (x_n)_{n\in\mathbb{N}} \,\middle|\, \bigvee_{n\in\mathbb{N}} \bigwedge_{n\geq n_0} x_n = 0 \right\} \\ &= \{(x_0, x_1, \dots, x_n, 0, \dots) \mid n \in \mathbb{N}, x_i \in \mathbb{R}\} \\ &\cong \mathbb{R}[x]\end{aligned}$$

In between there are many *other spaces (complex analysis discusses that).*

For example, $c_0 = \{(x_n) \mid \lim_{n\to\infty} x_n = 0\}$.

$$\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n$$

$$\lim_{n\to\infty} \lambda a_n = \lambda \lim_{n\to\infty} a_n$$

Because this holds, we have two operations for a vector space. This is actually a vector space (over the set of convergent sequences).

$$\mathbb{R}^{\mathbb{N}} := \oplus_{n\in\mathbb{N}}\mathbb{R} \subsetneq c_0 \subsetneq \mathbb{R}^{\mathbb{N}}$$

with

$$c = \{(x_n) \mid \lim x_n \text{ exists}\} = c_0 \oplus L((1,1,1,\dots)).$$

$$l^\infty = \left\{ (x_n)_{n\in\mathbb{N}} \,\middle|\, x_n \in \mathbb{R} \wedge \sup_n(|\, x_n \,|) < \infty \right\}$$

$$\mathbb{R}^{(\mathbb{N})} \subsetneq c_0 \subsetneq c \subsetneq l^\infty \subsetneq \mathbb{R}^{\mathbb{N}}$$

Every convergent sequence (x_n) *is uniquely representable as* $(y_n) + \lambda(1,1,1,\dots)$ *with* $(y_n) \in c_0$.

Remark 20.

$$(\mathbb{Z}_n, +)$$

Is a factor set $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

Factorization in regards of relation:

$$x \equiv_1 y \Leftrightarrow nx \mid -y \Leftrightarrow x - y \in n\mathbb{Z}$$

Let $(G, +)$ *be an abelian group.* $H \subseteq G$ *as subgroup. So this is a equivalence relation:*

$$x \equiv_H y \Leftrightarrow x - y \in H$$

Theorem 59 (Applied to vector spaces)**.** *Let* V *be a vector space over* K. $U \subseteq V$ *is a subspace.*

1. *The relation*

$$v \sim_u w \Leftrightarrow v - w \in U$$

   is an equivalence relation in V.

2. *The equivalence class of a vector* $v \in V$ *is*

$$[v]_u = \{w \mid w - v \in U\} = \{v + u \mid u \in U\} = v + U$$

   is called linear manifold *or* affine space.

   (Consider a vector v *and a line* U. $v + U$ *is the set of all lines parallel to* U *and going through* v.*)*

3.

$$\bigwedge_{v,v',w,w' \in V} v \sim_U v' \wedge w \sim_U w' \Rightarrow v + w \sim_U v' + w'$$

$$\bigwedge_{\lambda \in K} \bigwedge_{v,v' \in V} v \sim_U v' \Rightarrow \lambda v \sim_U \lambda v'$$

We therefore define

$\boxed{\text{TODO content incomplete/incorrect}}$

Proof. 1. **reflexive** $v \sim_U v \Leftrightarrow v - v \in U$

symmetrical $v \sim_U w \Leftrightarrow v - w \in U \Rightarrow w - v \in U \Rightarrow w \sim_U v$

transitive $v \sim_U w \wedge w \sim_U z \Rightarrow v - w \in U, w - z \in U$ and $v - z = (v - w) + (w - z) \in U$.

2. Follows immediately.

3.

$$v - v' \in U, w - w' \in U \Rightarrow v - v' + w - w' \in U$$

$$(v + w') - (v' + w')$$

Here we can see, that this will not work in non-commutative groups[4].

4. $v - v' \in U \Rightarrow \lambda v - \lambda v' = \lambda(v - v') \in U$

□

Theorem 60. *The set of equivalence classes* ${}^{V}\!/_{U}$*:*

$$^{V}\!/_{U} \coloneqq \left({}^{V}\!/_{\sim U}, +, \cdot\right)$$

with the operations

$$[v]_U + [w]_U \coloneqq [v + w]_U$$

$$[\Rightarrow v + U + w + U = (v + w) + U]$$

$$\lambda \cdot [v]_U \coloneqq [\lambda v]_U$$

$$[\Rightarrow \lambda \cdot (v + U) = \lambda v + U]$$

is a vector space with neutral element

$$[0]_U = U$$

and inverse element

$$-[v]_U = [-v]_U = -v + U$$

and is called factor space *or* quotient space.

Proof. The operations of Theorem 59 are well-defined. The distributive laws:

$$\begin{aligned} \lambda \cdot ([v]_U + [w]_U) &\overset{!}{=} \lambda[v]_U + \lambda[w]_U \\ &= \lambda \cdot [v + w]_U \\ &= [\lambda(v + w)]_U \\ &= [\lambda v + \lambda u]_U \\ &= [\lambda v]_U + [\lambda w]_U \\ &= \lambda[v]_U + \lambda[w]_U \end{aligned}$$

□

Example 34.

$$V = \mathbb{R}^3$$

$$U = \left\{ \begin{pmatrix} x \\ y \\ 0 \end{pmatrix} \middle| x, y \in \mathbb{R} \right\} = L\left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right)$$

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + U = \left\{ \begin{pmatrix} v_1 + x \\ v_2 + y \\ v_3 \end{pmatrix} \middle| x, y \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} x' \\ y' \\ v_3 \end{pmatrix} \middle| x, y \in \mathbb{R} \right\}$$

${}^{V}\!/_{U}$ *is the plane parallel to the x-y-plane.*

$$\left(\begin{pmatrix} 0 \\ 0 \\ z \end{pmatrix} + U \right) + \left(\begin{pmatrix} 0 \\ 0 \\ z \end{pmatrix} + U \right) = \left(\begin{pmatrix} 0 \\ 0 \\ z_1 + z_2 \end{pmatrix} + U \right)$$

$$^{V}\!/_{U} \cong \mathbb{R}$$

[4] We need at least the requirement of a normal divisor.

$$xHx^{-1} = H \quad \forall x \in G$$

Theorem 61. *Let* $\dim(V) < \infty$.

$$U \subseteq V \text{ is a subspace}$$

Then $\dim({}^{V}\!/\!_{U}) = \dim(V) - \dim(U)$.

Proof. Let $(u_1, \dots, u_r)$ be a basis of U. The basis extension theorem allows us to extend this set with $(w_1, \dots, w_n)$ such that $(u_1, \dots, u_r, w_1, \dots, w_n)$ is basis of V.

Claim: $\tilde{B} = (w_1 + U, w_2 + U, \dots, w_m + U)$ is basis of ${}^{V}\!/\!_{U}$.

These are exactly the equivalence classes of elements with basis of V, which are not mapped to $0 + U$ ($[0]_U$).

We need to prove that this is a basis:

1. Linear independence of $\tilde{B}$
2. $L(\tilde{B}) = {}^{V}\!/\!_{U}$

So,

1. Let $\lambda_1, \dots, \lambda_m \in K$ such that $\lambda_1(w_1 + U) + \dots + \lambda_m(w_m + U) = [0]_U$.

$$\lambda_1 w_1 + \dots + \lambda_m w_m + U = U$$

$$\Rightarrow \lambda_1 w_1 + \dots + \lambda_m w_m \in U$$

We know: $U \cap L(w_1, \dots, w_m) = \{0\}$. So,

$$\lambda_1 w_1 + \dots + \lambda_m w_m \cap L(w_1, \dots, w_m) = \{0\}$$

because the basis of U is linear independent of $L(w_1, \dots, w_m)$.

$$\Rightarrow \lambda_1 w_1 + \dots + \lambda_m w_m = 0$$

$$\Rightarrow \lambda_i = 0 \text{ because } (w_1, \dots, w_m) \text{ is linear independent (part of a basis)}$$

2. $L(\tilde{B}) \subseteq {}^{V}\!/\!_{U}$ is obvious.

Let $v + U \in {}^{V}\!/\!_{U}$

$$\Rightarrow v = \sum_{i=1}^{r} \lambda_i u_i + \sum_{i=1}^{m} \lambda_{r+i} w_i$$

Decomposition in regards of basis B of V.

$$v + U = \underbrace{\sum_{i=1}^{r} \lambda_i u_i}_{\in U} + \sum_{i=1}^{m} \lambda_{r+i} w_i + U$$

$$= \sum_{i=1}^{m} \lambda_{r+i} w_i + U$$

$$= \sum_{i=1}^{m} \lambda_{r+i} (w_i + U) \in L(\tilde{B})$$

□

7.1 Conclusion

What did we do in this section?

- $U + W$ (sums)
- $U \dot{+} W$ (direct sums)
- $V \oplus W, V \times W$ (outer sums)
- $\prod_{i \in I} V_i, \oplus_{i \in I} V_i$
- ${}^{V}\!/\!_{U}$

8 Linear mappings

Definition 28. *Let* V, W *be vector spaces over* K. *A mapping* $f : V \to W$ *is called* vector raum homomorphism *or* linear *if*

$$\bigwedge_{v,w \in V} f(v + w) = f(v) + f(w) \qquad \text{"additivity"}$$

$$\bigwedge_{\lambda \in K} \bigwedge_{v} f(\lambda v) = \lambda f(v) \qquad \text{“multiplicity”}$$

We denote:

$$\mathrm{Hom}(V, W) = \{f : V \to W \mid f \text{ is linear}\}$$

Theorem 62. *$f : V \to W$ is linear*

$$\Leftrightarrow \bigwedge_{\lambda,\mu \in K} \bigwedge_{v,w \in V} f(\lambda v + \mu w) = \lambda f(v) + \mu f(w)$$

$$\Leftrightarrow \bigwedge_{\lambda \in K} \bigwedge_{v,w \in V} f(\lambda v + w) = \lambda f(v) + f(w)$$

Example 35.

$$V = \mathbb{R} = W$$

Let $f : \mathbb{R} \to \mathbb{R}$ be linear. $x \mapsto k \cdot x$ with $k \in \mathbb{R}$ fixed.

As in high school: $f(x) = kx + d$.

Example 36.

$$id : V \to V$$

$$x \mapsto x$$

Example 37. *V with base $(b_1, b_2, \ldots, b_n)$.*

$$\bigwedge_{v \in V} \bigvee_{\lambda_1,\ldots,\lambda_n} v = \lambda_1 b_1 + \cdots + \lambda_n b_n$$

$$\Phi_B : V \to K^n \text{ is linear}$$

$$v \mapsto \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

To be discussed in the practicals.

This lecture took place on 7th of December 2015 (Franz Lehner).

Homomorphisms and vector spaces:

$$f(\lambda u + \mu v) = \lambda f(u) + \mu f(v)$$

$$f : V \to W$$

Example 38.

$$id{:}V \to V$$

$$v \mapsto v$$

Let V be a vector space. Let $B = (v_1, \ldots, v_n)$ be our basis.

$$v = \lambda_1 v_1 + \cdots + \lambda_n v_n$$

$$\Phi_B : V \to K^n$$

$$v \mapsto \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

In the practicals it is shown to be linear.

Remark 21. *Special case: Let $V = K^n$. Let $B = (e_1, \ldots, e_n)$ be your basis.*

$$\Phi_i : \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \mapsto \lambda_i$$

$$\Phi_i : (a + b) = \Phi_i \begin{pmatrix} a_1 + b_i \\ \vdots \\ a_n + b_n \end{pmatrix} = a_i + b_i = \Phi_i(a) + \Phi_i(b)$$

Remark 22. *Also:*

$$\Phi_i : V \to K$$

$$v \mapsto \lambda_i$$

Example 39.

$$V = K^X = \{f : X \to K\}$$

$$(f + g)(x) = f(x) + g(x)$$

$$(\lambda \cdot f)(x) = \lambda \cdot f(x)$$

Pointwise operations.

Let $x \in X$.

$$\Rightarrow \Phi_x : V \to K$$

$$f \mapsto f(x)$$

$$\Phi_x(\lambda f + \mu g) = (\lambda f + \mu g)(x) = \lambda f(x) + \mu g(x) = \lambda \Phi_x(f) + u \Phi_x(g)$$

Example 40.

$$\mathbb{R}[x] \to \mathbb{R}[x]$$
$$x^n \mapsto n \cdot x^{n-1}$$
$$\sum_{k=0}^{n} a_k x^k \mapsto \sum_{k=1}^{n} k \cdot a_k x^{k-1}$$

The derivation of $p(x) \to p'(x)$ is additive:

$$(p+q)(x) = p'(x) + q'(x)$$
$$(\lambda p)'(x) = \lambda \cdot p'(x)$$

Example 41.

$$\int_a^b : \mathbb{R}[x] \to \mathbb{R}$$
$$p(x) \mapsto \int_a^b p(x)\,dx \textit{ is linear.}$$

Example 42.

$$V = \mathbb{R}^2$$
$$T_{x_0} : x \mapsto x + x_0$$
$$x_0 = T_{x_0}(0) = T_{x_0}(0+0) = T_{x_0}(0) + T_{x_1}(0) = 2x_0 \quad \lightning$$

Translation in $\mathbb{R}^2$ is non-linear. It is only affine linear *(translation together with rotation).*

Example 43. *Rotation itself in $\mathbb{R}^2$ is linear.*

$$U_q : v = \textit{rotated vector } q \textit{ is linear}$$

Example 44.

$$A : \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 2x_1 \\ x_2 \end{pmatrix} \textit{ is linear}$$

Dilation is linear.

Example 45.

$$A(\lambda x + y) = \begin{pmatrix} 2(\lambda x_1 + y_1) \\ \lambda x_2 + y_2 \end{pmatrix} = \lambda \begin{pmatrix} 2x_1 \\ x_1 \end{pmatrix} + \begin{pmatrix} 2y_1 \\ y_2 \end{pmatrix} = \lambda A(x) + A(y) \textit{ is linear}$$

Example 46.

$$C = \{(x_n)_{n\in\mathbb{N}} \mid x_n \in \mathbb{R}, x_n \textit{ is convergent}\}$$
$$\lim_{n\to\infty}(x_n + y_n) = \lim_{n\to\infty} x_n + \lim_{n\to\infty} y_n$$
$$\lim_{n\to\infty}(\lambda x_n) = \lambda \cdot \lim_{n\to\infty} x_n$$
$$\Rightarrow \textit{ the mapping } \lim_{n\to\infty} c \to \mathbb{R}$$
$$(x_n)_{n\in\mathbb{N}} \mapsto \lim_{n\to\infty} x_n$$

is linear.

Example 47.

$$V = l^1 = \left\{ (\lambda_m) \,\middle|\, \sum_{n=1}^{\infty} |\,\lambda_n\,| < \infty \right\}$$
$$\sum_{n=1}^{\infty} |\,x_n + y_n\,| \le \sum_{n=1}^{\infty} |\,x_n\,| + \sum_{n=1}^{\infty} |\,y_n\,| < \infty$$
$$\sum_{n=1}^{\infty}(x_n + y_n) = \sum_{n=1}^{\infty} x_n + \sum_{n=1}^{\infty} y_n$$
$$\sum_{n=1}^{\infty} \lambda x_n - \lambda \cdot \sum_{n=1}^{\infty} x_n$$
$$\Rightarrow \sum_{n=1}^{\infty} : l^1 \to \mathbb{R} \textit{ is linear}$$
$$(x_n)_{n\in\mathbb{N}} \mapsto \sum_{n=1}^{\infty} x_n$$

Example 48.

$$V = U \dot{+} W \textit{ is the direct sum}$$
$$\bigwedge_v \dot{\bigvee}_{u\in\mathbb{U}} \dot{\bigvee}_{w\in W} v = u + w \textit{ is unambiguous}$$
$$\pi_U : V \to U \qquad \textit{“projections on } U\textit{”}$$
$$v \mapsto u$$
$$\pi_W : V \to W \qquad \textit{“projections on } W\textit{”}$$
$$v \mapsto w$$

Theorem 63. *Let V and W be vector spaces.*

$$f : V \to W \text{ is linear}$$

1. $f(0_v) = 0_w$
2. $\bigwedge_{v\in V} f(-v) = -f(v)$
3. *It holds that,*

$$\bigwedge_{n} \bigwedge_{\lambda_1,\dots,\lambda_n\in K} \bigwedge_{v_1,\dots,v_k\in V} f(\lambda_1 v_1 + \cdots + \lambda_n v_n) = \lambda_1 f(v_1) + \lambda_2 f(v_2) + \cdots + \lambda_n f(v_n)$$

Proof. We prove the first statement:

$$f(0_v) = f(0_v + 0_v) = f(0_v) + f(0_v)$$

$$0_w = f(0_v)$$

We prove the second statement.

$$f(-v) = f((-1)\cdot v) = (-1)\cdot f(v) = -f(v)$$

□

Definition 29. *Let V and W be vector spaces. Let $f : V \to W$. Homomorphism is an*

- epimorphism *if $f : V \to W$ and f is surjective.*
- monomorphism *if $f : V \to W$ and f is injective.*
- isomorphism *if $f : V \to W$ and f is bijective.*

Let $V = W$, then

- endomorphism *if $f : V \to V$.*
- automorphism *if $f : V \to V$.*

We also denote

$$\mathrm{Hom}(V, W) = \text{ homomorphism from } V \text{ to } W$$

$$\mathrm{End}(V) = \mathrm{Hom}(V, V)$$

$$\mathrm{Aut}(V) = \{f : V \to V \text{ automorphism}\}$$

Definition 30. *V and W are* isomorphic *$V \cong W$ if there exists isomorphism $f : V \to W$.*

V is called embeddable *in W if there exists some monomorphism $f : V \to W$. f is called* embedding.

Theorem 64. *Let U, V and W be vector spaces over K.*

$$f : U \to V \qquad g : V \to W \text{ is linear}$$

1. *$\Rightarrow g \circ f : U \to W$ is linear.*
2. *$\Rightarrow$ if $f : U \to V$ is isomorphism, then also $f^{-1} : V \to U$ is linear.*

Proof. We prove the first statement.

$$g \circ f(\lambda \cdot v + \mu w) \overset{!}{=} \lambda \cdot g \circ f(v) + \mu g \circ f(w)$$

$$\begin{aligned} g \circ f(\lambda \cdot v + \mu w) &= g(f(\lambda v + \mu w)) = g(\lambda f(v) + \mu f(w)) \\ &= \lambda \cdot g(f(v)) + \mu \cdot g(f(w)) = \lambda (g \circ f)(v) + \mu (g \circ f)(w) \end{aligned}$$

We prove the second statement.

$$f^{-1}(\lambda v + \mu w) = \underbrace{f^{-1}(\lambda f(f^{-1}(v))) + \mu \cdot f(f^{-1}(w))}_{f(\lambda \cdot f^{-1}(v) + \mu f^{-1}(w))}$$

$$f^{-1}(f(\lambda \cdot f^{-1}(v) + \mu f^{-1}(w))) = \lambda f^{-1}(v) + \mu f^{-1}(w)$$

□

Theorem 65. $\mathrm{Hom}(V, W)$ *with the operations $(f + g)(v) = f(v) + g(v)$ and $(\lambda f)(v) = \lambda \cdot f(v)$ is a vector space with 0-vector $0 : V \to W$ and $v \mapsto 0$.*

Proof. We need to prove that $\mathrm{Hom}(V,W)$ is a subspace of W^V. Therefore $f,g \in \mathrm{Hom}(V,W)$ is therefore

$$f+g \text{ and } \lambda \cdot f$$

Show that,

$$(\lambda\cdot f+\mu\cdot g)(\alpha v+\beta w) \overset{!}{=} \lambda\cdot(\lambda f+\mu g)(v)+\beta(\lambda f+\mu g)(w)$$

$$\begin{aligned}(\lambda f+\mu g)(\alpha v+\beta w) &= \lambda f(\alpha v+\beta w)+\mu g(\alpha v+\beta w)\\ f,g \text{ are linear } &= \lambda(\alpha f(v)+\beta f(w))+\mu(\alpha g(v)+\beta g(w))\\ &= \alpha\left(\alpha f(v)+\mu g(v)\right)+\beta(\lambda f(w)+\mu g(w))\\ &= \alpha(\lambda f+\mu g)(v)+\beta(\lambda f+\mu g)(w)\end{aligned}$$

$\Rightarrow (\mathrm{Hom}(V,W),+,\cdot)$ is a vector space over K. □

Theorem 66. *Let $V=W$, then $(\mathrm{End}(V),+,\circ)$ where $\circ$ denotes composition is a ring.*

Proof.
1. $(\mathrm{End}(V),+)$ is an abelian group ✓
2. $(\mathrm{End}(V),\circ)$ is a semi-group (sub-semigroup of $(V^V,\circ)$)
3. Distributive law is shown in the practicals.

□

Definition 31. *An* algebra *over a field K is a structure*

$$(A,+,\cdot,*)$$

$$+: A\times A\to A$$

$$\cdot: K\times A\to A$$

$$*: A\times A\to A$$

such that $(A,+,\cdot)$ is a vector space and $(A,+,*)$ is a ring.

Associativity holds,

$$\lambda(a*b)=(\lambda\cdot a)*b=a*(\lambda b)$$

Example 49.

$$A=\mathbb{R}[x]$$

$$(p+q)(x)=p(x)+q(x)$$

$$\lambda\cdot p(x)$$

$$(p*q)(x)=p(x)\cdot q(x)$$

also satisfies associativity.

Theorem 67. $(\mathrm{End}(V),+,\cdot,\circ)$ *is a non-commutative algebra.*

Proof. It only remains to show associativity. This is left for the practicals. □

8.1 Linear mappings and subspaces

Theorem 68. *Let V and W be vector spaces over K.*

$$f: V\to W \text{ is linear}$$

1. *if $V'\subseteq V$ is a subspace, then $f(V')\subseteq W$ is a subspace.*
2. *if $W'\subseteq W$ is a subspace, then $f^{-1}(W')\subseteq V$ is a subspace.*

Proof.
1. Let $w_1,w_2\in f(V)$ then also $\lambda_1 w_1+\lambda_2 w_2\in f(V')$. Let $w_1,w_2\in f(V')$.

$$\Rightarrow \bigvee_{v_1\in V'}\bigvee_{v_2\in V'} f(v_1)=w_1\wedge f(v_2)=w_2$$

$$\lambda_1 w_1+\lambda_2 w_2=\lambda_1 f(v_1)+\lambda_2 f(v_2)$$

$$f \text{ is linear} \Rightarrow f(\underbrace{\lambda_1 v_1+\lambda_2 v_2}_{\in V'})\in f(V')$$

2. Show that $v_1,v_2\in f^{-1}(W')$ then also $\lambda_1 v_1+\lambda_2 v_2\in f^{-1}(W')$. Show that if $f(v_1),f(v_2)\in W'$ then $f(\lambda_1 v_1+\lambda_2 v_2)\in W'$.

$$f(\lambda_1 v_2+\lambda_2 v_2)= \underbrace{\lambda_1\underbrace{f(v_1)}_{\in W'}+\lambda_2\underbrace{f(v_2)}_{\in W'}}_{\in W' \text{ because its a subspace}} \in W'$$

□

Theorem 69. *Let V and W be vector spaces over K.*

$$f : V \to W \text{ is linear}$$

$$(v_i)_{i \in I} \subseteq V$$

1. $f(L((v_i)_{i\in I})) = L((f(v_i))_{i\in I})$

$$M \subseteq V$$

$$f(L(M)) = L(f(M))$$

2. $(f(v_i))_{i\in I}$ *linear independent* $\Rightarrow (v_i)_{i\in I}$ *linear independent*

The inverse of the second statement does not hold (think about the zero-element).

Proof. 1.

$$w \in f(L((v_i)_{i\in I})) \Leftrightarrow \bigvee_{v \in L((v_i)_{i\in I})} w = f(v)$$

$$\Leftrightarrow \bigvee_m \bigvee_{i,\dots,i_n} \bigvee_{\lambda_1,\dots,\lambda_n} w = f(\lambda_1 v_{i,1} + \dots + \lambda_n v_{i,n})$$

$$\Leftrightarrow \bigvee_m \bigvee_{i,\dots,i_n} \bigvee_{\lambda_1,\dots,\lambda_n} w = \lambda_1 f(v_{i,1}) + \dots + \lambda_n f(v_{i,n})$$

$$\Leftrightarrow w \in L((f(v_i))_{i\in I})$$

2. Let $\lambda_1 v_{i,1} + \dots + \lambda_n v_{i,n} = 0 \overset{!}{\Rightarrow}$ all $\lambda_i = 0$.

$$f(\lambda_1, v_{i,1} + \dots + \lambda_n v_{i,n}) = 0_w$$

$$f \text{ linear} \Rightarrow \lambda_1 f(v_{i,1}) + \dots + \lambda_n f(v_{i,n}) = 0$$

$$f(v_i) \text{ linear independent} \Rightarrow \text{ all } \lambda_i = 0$$

□

Theorem 70. *Let V, W be vector spaces. Let $f : V \to W$ be linear.*

1. *f is surjective and $L(M) = V$, then $L(f(M)) = W$.*
2. *f is injective and $M \subseteq V$ is linear independent, then $f(M)$ is linear independent in W.*
3. *f is bijective and B is basis then B is basis of W.*

This lecture took place on 14th of December 2015 (Franz Lehner).

Proof. 1. If f is surjective and $L(M) = V$, then $L(f(M)) = W$. If f is surjective, then the image of the generating system is also a generating system.

$$L(f(M)) \overset{\text{Theorem 69}}{=} f(L(M)) = f(V) \overset{\text{surj.}}{=} W$$

2. Let $f(v_i) \in f(M)$. Let $\sum \lambda_i f(v_i) = 0$. Then $f(\sum \lambda_i v_i) = 0_W = f(0_V)$.

$$f \text{ inj.} \Rightarrow \sum \lambda_i v_i = 0_v$$

$$M \text{ is linear indep.} \Rightarrow \text{ all } \lambda_i = 0$$

3. If f is bijective and $B \subseteq V$ is basis, then $f(B)$ is basis.

□

Theorem 71. *Let $f : V \to W$ be linear.*

- *If f is injective, then $\dim V \le \dim W$.*
- *If f is surjective, then $\dim V \ge \dim W$.*
- *If f is bijective, then $\dim V = \dim W$.*

Proof. Let $(b_I)_{i\in I}$ be a basis of V.

1. If $\dim W = \infty$, we are done. $\dim W < \infty$, then from Theorem 70 it follows that, $(f(b_i))_{i\in I}$ is linear in W. $\dim W$ is given by maximal size of a linear independent family in W.

$$\Rightarrow \dim W \ge [I] = \dim V$$

2. If $\dim V = \infty$, we are done. If $\dim V < \infty \Rightarrow |\, I\,| < \infty$. From Theorem 70 (1) it follows that $(f(b_i))_{i\in I}$ generates W. $\dim W$ is given by maximal size of a linear independent family in W.
$$\Rightarrow \dim W \leq |\, I\,| = \dim V$$
3. Follows from the previous two items or directly from Theorem 70 (2).

□

Corollary 14. *If V and W are isomorphic (ie. if an isomorphism $f : V \to W$ exists), then $\dim V = \dim W$. Therefore the dimension of a vector space is an invariant.*

We show the inverse: If $\dim V = \dim W$, then isomorphism is given.

Theorem 72. *Abstract definition: "In the category of vector spaces, all objects are free."*

Given two vector spaces V and W. Let $(b_i)_{i\in I} \subseteq V$ be basis of V. $(w_i)_{i\in I} \subseteq W$ is arbitrary.

Then there exists a distinct linear mapping $f : V \to W$, such that $f(b_i) = w_i$ for all i.

Corollary 15. *Two linear mappings $f, g : V \to W$ are equal (ie. $\bigwedge_{v\in V} f(v) = g(v)$).*
$$\Leftrightarrow f|_B = g|_B \text{ for a basis of } V$$

Proof. A linear mapping with $f(b_i) = w_i$ and linear combination $v = \sum \lambda_i b_i$ must give
$$f(v) = f\left(\sum \lambda_i b_i\right) = \sum \lambda_i f(b_i) = \sum \lambda_i w_i$$
We therefore define
$$f(v) = \sum_{j=1}^{n} \lambda_j w_{ij}$$
If $v = \sum_{j=1}^{n} \lambda_j b_{ij}$ (decomposition in regards of basis).

This define a function $f : V \to W$. So for every decomposition in regards of the basis, this decomposition is distinct. Therefore f is well-defined.

We now need to show: f is linear.
$$v = \sum_{i=1}^{n} \alpha_j b_{ij} \qquad v = \sum_{j=1}^{n} \beta_j b_{ij}$$
Without loss of generality in both vectors we have the same basis vectors b_{ij} (in other case we extend them using zero coefficients).

$$\begin{aligned}
f(\lambda u + \mu v) &= f(\lambda \sum_{j=1}^{n} \alpha_j b_{ij} + \mu \sum_{j=1}^{n} \beta_j b_{ij}) \\
&= f(\sum_{j=1}^{n} (\lambda\alpha_j + \mu\beta_j)\, b_{ij}) \\
&= \sum_{j=1}^{n} (\lambda\alpha_j + \mu\beta_j)\, w_{ij} \\
&= \lambda \sum_{j=1}^{n} \alpha_j w_{ij} + \mu \sum_{j=1}^{n} \beta_j w_{ij} \\
&= \lambda f(u) + \mu f(v)
\end{aligned}$$

Therefore it is linear. But is it distinct?

Let $g : V \to W$ be linear with $g(b_i) = w_i$ for all i. We need to show that $g = f$. Therefore $g(v) = f(v)$ (for all $v \in V$). Let $v \in V \Rightarrow v = \sum_{j=1}^{n} \lambda_j b_{ij}$ be a decomposition in regards of the basis. Therefore $g(v) = g\left(\sum_{j=1}^{n} \lambda_j b_{ij}\right) = \sum_{j=1}^{n} \lambda_j g(b_{ij}) = \sum_{j=1}^{n} \lambda_j w_{ij} = f(v)$. □

Theorem 73. *Let V and W be finite-dimensional vector spaces. Then $V \cong W \Leftrightarrow \dim V = \dim W$.*

$$(\delta_x)_{x\in\mathbb{R}} \subseteq \mathbb{R}^{\mathbb{R}}$$
is linear independent, where
$$\delta_x(t) = \begin{cases} 1 & \text{if } t = x \\ 0 & \text{else} \end{cases}$$

Proof. **Proof** $\Rightarrow$ Let $f : V \to W$ be an isomorphism. Then from Theorem 71 (3) it follows that $\dim V = \dim W$.

Proof $\Leftarrow$ Let $(v_1, \dots, v_n)$ be a basis of V and $(w_1, \dots, w_n)$ be basis of W. Let $f : V \to W$ be a linear mapping from Theorem 72 for which $f(v_i) = w_i$ for all $1 \leq i \leq n$.

We need to show that f is bijective; injective and surjective.

Injectivity: Let $v, v' \in V$ with $f(v) = f(v')$. We need to show that $v = v'$.

$$\begin{aligned}
0 = f(v) - f(v') &= f\left(\sum_{i=1}^n \lambda_i v_i\right) - f\left(\sum_{i=1}^n \mu_i v_i\right) \\
&= \sum_{i=1}^n \lambda_i f(v_i) - \sum_{i=1}^n \mu_i f(v_i) \\
&= \sum_{i=1}^n \lambda_i w_i - \sum_{i=1}^n \mu_i w_i \\
&= \sum_{i=1}^n (\lambda_i - \mu_i) w_i = 0 \qquad \Rightarrow \lambda_i - \mu_i = 0 \quad \forall i \\
&\Rightarrow \text{all } \lambda_i = \mu_i \Rightarrow v = v'
\end{aligned}$$

Surjectivity: Let $w \in W$. We need to show that

$$\bigvee_{v \in V} f(v) = w$$

$(w_1, \dots, w_i)$ generates W. Therefore,

$$\bigvee_{\lambda_1, \dots, \lambda_n} w = \sum_{i=1}^n \lambda \cdot w_i$$

Then

$$f(v) = w \text{ for } v = \sum_{i=1}^n \lambda_i v_i \in V$$

$$f(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i f(v_i) = \sum_{i=1}^n \lambda_i w_i = w$$

We have shown that if $f : b_i \to w_i$ is extended to a linear mapping $f : V \to W$, then it holds that

1. if $(w_1, \dots, w_n)$ is linear independent, then f is injective.
2. if $L(w_1, \dots, w_n) = W$, then f is surjective.

$\square$

Corollary 16.

$$\dim V = n \Leftrightarrow V \cong K^n$$

Isomorphism: Let $(b_1, \dots, b_n)$ be a basis of V. Then,

$$f : V \to K^n$$

$$b_i \mapsto e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

with the 1 in the i-th row,

$$f\left(\sum_{i=1}^n \lambda_i b_i\right) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

is an isomorphism.

Corollary 17.

$$\mathrm{Hom}(V, W) \supsetneq \{0\} \ \textit{if } V, W \neq \{0\}$$

$\mathrm{Hom}(V, W)$ *is vector space (and ring, hence algebra).*

$$(\lambda f + \mu g)(v) = \lambda f(v) + \mu g(v)$$

It follows that $\dim \mathrm{Hom}(V, W) = \dim V \cdot \dim W$.

Theorem 74.

$$\dim \operatorname{Hom}(V,W) = \dim V \cdot \dim W$$

Proof. Every $f : V \to W$ is uniquely defined by the values of the basis of V. Let $(v_1, \dots, v_m)$ be a basis of V. Let $(w_1, \dots, w_n)$ be a basis of W.

Claim: The mapping $f_{ij} : V \to W$ such that

$$f_{ij}(v_k) = \begin{cases} w_j & \text{if } k = i \\ 0 & k \neq i \end{cases}$$

Is distinct according to Theorem 72. This is a basis of $\operatorname{Hom}(V,W)$. So we need to shown linear independence and that it is a generating system.

Let B such that,

$$B = (f_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \subseteq \operatorname{Hom}(V,W)$$

1. $$L(B) = \operatorname{Hom}(V,W)$$

   Let $f \in \operatorname{Hom}(V,W)$ be searched $\lambda_{ij} \in K$ such that $f = \sum_{i=1}^n \sum_{j=1}^n \lambda_{ij} f_j$.

   $$\bigwedge_h \bigvee_{\lambda_1,\dots,\lambda_n \in K} f(v_k) = \sum_{i=1}^n \lambda_{\alpha_j} w_j$$

   Decomposition of $f(v_k)$ in regards of the basis $(w_1, \dots, w_n)$.

   Claim:

   $$f = \sum_{i=1}^n \sum_{j=1}^n \alpha_{ij} f_{ij} = g$$

   To show that $f = g$ (hence $f(v) = g(v)$), it suffices to show that $f(v_k) - g(v_k)$ for all k (Theorem 72).

   $$g(v_k) = \left(\sum_{i=1}^n \sum_{j=1}^n \alpha_{ij} f_{ij} \right)(v_k)$$
   $$= \sum_{i=1}^n \sum_{j=1}^n \alpha_{ij} f_{ij}(v_k)$$

$$f_{ij}(v_k) = \begin{cases} w_j & \text{if } i = k \\ 0 & \text{if } i \neq k \end{cases}$$

$\Rightarrow = \sum_{j=1}^n \alpha_{k_j} w_j = f(v_k)$.

$$\Rightarrow g|_{\{v_1,\dots,v_m\}} = f|_{\{v_1,\dots,v_m\}}$$

$$\xRightarrow{\text{Theorem 72}} g = f$$

And finally we need to show linear independence.

Let $\lambda_{ij} \in K$ such that $\sum_{i=1}^n \sum_{j=1}^n \lambda_{ij} f_{ij} = 0$. Therefore $\sum_{i=1}^n \sum_{j=1}^n \lambda_{ij} f_{ij}(v) = 0$ for all $v \in V$. Show that for all $\lambda_{ij} = 0$.

$$0 = \sum_{i=1}^n \sum_{j=1}^n \lambda_{ij} f_{ij}(v_k)$$
$$= \sum_{j=1}^n \lambda_{kj} w_j = 0 \Rightarrow \bigwedge_j \in \{1, \dots, n\}\, \lambda_{kj} = 0$$

where

$$f_{ij}(v_k) = \begin{cases} w_j & i = k \\ 0 & i \neq k \end{cases}$$

so (w_j) are linear independent and this holds for all k. So,

$$\bigwedge_k \bigwedge_j \lambda_{kj} = 0$$

□

This lecture took place on 15th of December 2015 (Franz Lehner).

8.2 Revision

A factor set satisfies:

$$V/U \quad U \subseteq V \text{ is a subspace}$$
$$= \{v + U \mid v \in V\} = \{[v] \mid v \in V\}$$
$$v \sim_U v' \Leftrightarrow v - v' \in U \Leftrightarrow v \in V' + U$$
$$\dim(V/U) = \dim U = \dim V$$

Constructing a basis for V/U:

$$u_1, \dots, u_m \text{ is basis of } U \to \text{ extend to basis of } V$$
$$u_1, \dots, u_m, w_1, \dots, w_{n-m} \text{ is basis of } V$$
$$w_1 + U, \dots, w_{n-m} + U \text{ is basis of } V/U$$

Images and preimages of subspaces are subspaces.

Definition 32. *Let $f : V \to W$ be linear. The subspace*

$$\ker(f) := f^{-1}(\{0\}) = \{v \mid f(v) = 0\} \subseteq V$$

is called kernel *of the linear mapping f. The* image *of the linear mapping f is defined as*

$$\operatorname{im}(f) = f(V)$$

Example 50.

$$f : K^n \to K^n$$

Consider some fixed m.

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\operatorname{im}(f) = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_m \\ \vdots \\ 0 \end{pmatrix} \middle| X \in K \right\} \cong K^m$$

$$\ker(f) = \left\{ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x_{n+1} \\ \vdots \\ x_n \end{pmatrix} \middle| x_i \in K \right\} \cong K^{n-m}$$

In this example:

$$\ker(f) \dot{+} \operatorname{im}(f) = K^n$$
$$\dim \ker(f) + \dim \operatorname{im}(f) = \dim V$$

Theorem 75. *Let $f : V \to W$ be linear.*

- *f is surjective* $\Leftrightarrow \operatorname{im}(f) = W$
- *f is injective* $\Leftrightarrow \ker(f) = \{0_V\}$

Proof.
- Follows immediately.
- $\Rightarrow$: Let $v \in \ker(f) \Rightarrow f(v) = 0_W = f(0_V)$ and f is injective $\Rightarrow v = 0_v$.

  $\Leftarrow$: Let $v, v' \in V$ with $f(v) = f(v')$.

$$0 = f(v) - f(v') = f(v - v')$$
$$\Rightarrow v - v' \in \ker(f) = \{0\}$$
$$\Rightarrow v = v'$$

$\square$

Theorem 76 (homomorphism theorem)**.** *Let $g : V \to {}^{V}\!/_{U}$ be linear. $v \mapsto v + U$. Then it holds that:*

$$\tilde{f} : {}^{V}\!/_{\ker f} \to \operatorname{im}(f) \text{ is linear}$$

$$v + \ker(f) \mapsto f(v)$$

This gives an isomorphism.

Proof. We need to show,

1. Is it well-defined?
2. Is it linear?
3. Is it bijective?

1. So it must holds that $\tilde{f}(v + \ker(f))$ does not depend on the selection of the representative.

   So we need to show: If $v \sim_{\ker(f)} v'$ $(v - v' \in \ker(f))$ then $f(v) - f(v')$.

$$v - v' \in \ker(f) \Rightarrow f(v - v') = 0$$
$$\Rightarrow f(v) - f(v') = 0$$
$$\Rightarrow f(v) = f(v')$$

   Definition of $\tilde{f}(v + \ker(f))$ is consistent.

2.

$$\begin{aligned}\bigwedge_{v,v' \in V} \bigwedge_{\lambda,\mu \in K} &\tilde{f}(\lambda(v + \ker(f))) + \mu(v' + \ker(f)) \\ &= \tilde{f}((\lambda v + \mu v') + \ker f) \\ &= f(\lambda v + \mu v') \\ f \text{ is linear} \Rightarrow &= \lambda f(v) + \mu f(v') \\ &= \lambda \tilde{f}(v + \ker(f)) + \mu \tilde{f}(v' + \ker(f))\end{aligned}$$

3. $\tilde{f}$ is surjective? Let $w \in \operatorname{im}(f)$, choose $v \in V$ with $w = f(v) = \tilde{f}(v + \ker(f))$. Therefore $w \in \operatorname{im}(\tilde{f})$.

   $\tilde{f}$ is injective? We need to show that $\ker(\tilde{f}) = \{0 + \ker(f)\}$.

   Let $\tilde{f}(v + \ker(f)) = 0$. So $v \in \ker(f) \Rightarrow v + \ker(f) = \ker(f) = 0 + \ker(f)$.

□

Corollary 18. *Let $f : V \to W$ be linear. So $\dim V < \infty$. Then $\dim \ker(f) + \dim \operatorname{im}(f) = \dim V$.*

Proof.

$$\dim({}^{V}\!/_{\ker(f)}) \overset{\text{Theorem 61}}{=} \dim V - \dim \ker(f)$$

$$\tilde{f} : {}^{V}\!/_{\ker(f)} \to \operatorname{im}(f) \text{ is isomorphism}$$

$$\Rightarrow \dim({}^{V}\!/_{\ker(f)}) = \dim(\operatorname{im}(f))$$

□

Alternative, more comprehensible proof.

$$\ker(f) \subseteq V \text{ is subspace}$$

From Theorem 51 it follows that subspace $U \subseteq V$ exists such that $\ker(f) \dot{+} U = V$.

$$\dim U = \dim V - \dim \ker(f)$$

Claim. $f|_U : U \to \operatorname{im}(f)$ is bijective.
Claim. $f|_U$ is surjective.

Let $w \in \operatorname{im}(f)$

$$\Rightarrow \bigvee_{v \in V} f(v) = w$$

$$V = \ker(f) \dot{+} U \Rightarrow \dot{\bigvee}_{u \in U} \dot{\bigvee}_{v_0 \in \ker(f)} v = v_0 + u$$

$$w = f(v) = f(v_0) + f(U) \Rightarrow w \in f(U)$$

f_U: is bijective. We need to show that $\ker(f|_U) = \{0\}$.

$$\ker(f|_U) = \ker(f) \cap U = \{0\}$$

Is $\{0\}$, because $V = \ker(f)\dot{+}U$ is a direct sum. □

Remark 23. *Also the mapping*

$$U \to {}^{V}\!/_{\ker(f)}$$

$$u \mapsto u + \ker(f)$$

is an isomorphism.

The proof will be provided in the practicals.

Theorem 77.

$$\dim V = \dim W < \infty$$

$$f : V \to W \text{ is linear}$$

then it holds equivalently,

1. *f is a monomorphism*
2. *f is epimorphism*
3. *f is isomorphism*

Proof. 1. $\Leftrightarrow f$ is injective $\Leftrightarrow \ker f = \{0\}$

$$\Leftrightarrow \dim \ker(f) = 0$$

$$\xLeftrightarrow{\text{Corollary 18}} \dim \operatorname{im}(f) = \dim V = \dim W$$

$$\operatorname{im}(f) \subseteq W \text{ subspace}$$

and $\dim \inf(f) = \dim W$.

$$\Leftrightarrow \operatorname{im}(f) = W$$

$$\Leftrightarrow f \text{ is surjective}$$

$$\dim V = n \Leftrightarrow V \cong K^n$$

$$\text{basis } f_{i,j}, v_k \to \begin{cases} w_j & \text{if } k = i \\ 0 & \text{else} \end{cases}$$

Every $f : V \to W$ has the structure

$$f = \sum \alpha_{ij} f_{ij}$$

□

9 Matrix computations

We have already dealed with matrices when discussing linear mappings and linear equation systems.

Definition 33. *An $m \times n$ matrix over K is a number scheme:*

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

with m rows and n columns.

a_{ij} is the number of the i-th row and j-th column.

$$M_{m,n}(K) = K^{m \times n}$$

is the set of all $m \times n$ matrices. If $m = n$:

$$M_n(K) = K^{n \times n}$$

is called a quadratic matrix.

$z_i = (a_{i1}, a_{i2}, \dots, a_{in})$ is the i-th row vector. $s_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ is the j-th column vector.

The sequence $a_{11}, a_{22}, \dots, a_{kk}$ with $k = \min m, n$ is called main diagonal of A. If all entries are contained outside the main diagonal, A is called diagonal matrix.

$$A = \operatorname{diag}(a_{11}, a_{22}, \dots, a_{kk}) = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{kk} \end{bmatrix}$$

$I_n = \operatorname{diag}(1, \dots, 1)$ *is called* unit matrix.

$$= [\delta_{ij}]_{i,j \in 1,\dots,n}$$

Kronecker-δ:

$$\delta_{i,j} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{else} \end{cases}$$

If all entries outside the main diagonal are 0*, then A is called a* triangular matrix. *If all entries below the main diagonal are* 0*, then A is called an* lower triangular matrix. *If all entries above the main diagonal are* 0*, then A is called an* upper triangular matrix.

Matrix units *are defined as*

$$(E_{kl}^{(n)})_{ij} = \delta_{ki} \cdot \delta_{ej} = \begin{cases} 1 & \text{if } k = i \land l = j \\ 0 & \text{else} \end{cases}$$

Examples:

$$E_{11} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

$$E_{12} = \begin{pmatrix} 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

The transposed matrix of $A \in K^{m \times n}$ is denoted $A^t \in K^{n \times m}$ with entries:

$$(A^t)_{ij} = a_{ji}$$

So we mirror along the main diagonal.

$$(A^t)^t = A$$

Remark 24. *A column vector can be identified with a $1 \times n$ matrix. A row vector can be identified with a $n \times 1$ matrix.*

Theorem 78. $(K^{m \times n}, +, \cdot)$ *with*

$$[a_{ij}]_{i=1,\dots,m; j=1,\dots,n} + [b_{ij}]_{i=1,\dots,m; j=1,\dots,n} = [a_{ij} + b_{ij}]_{i=1,\dots,m; j=1,\dots,n}$$

$$\lambda [a_{ij}]_{i=1,\dots,m; j=1,\dots,n} = [\lambda a_{ij}]_{i=1,\dots,m; j=1,\dots,n}$$

Is a vector space of dimension $m \cdot n$ with basis $(E_{ij})_{i=1,\dots,m; j=1,\dots,n}$.

Remark 25.

$$K^{m \times n} \to K^{n \times m}$$
$$A \mapsto A^t$$

is a vector space isomorphism.

Definition 34. *Let $A = [a_{ij}]_{i=1,\dots,m; j=1,\dots,n} \in K^{m \times n}$.*

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n$$

is a column vector. Then

$$Ax = A \cdot x = \begin{pmatrix} \sum_{j=1}^n a_{1j} x_j \\ \sum_{j=1}^n a_{2j} x_j \\ \vdots \\ \sum_{j=1}^n a_{mj} x_j \end{pmatrix} \in K^m$$

This is called the product of the matrix A with the vector x.

So instead of a linear equation system with all entries listed explicitly, we will only write Ax in this section.

Example 51.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 \\ 4 \cdot 1 + 5 \cdot 2 + 6 \cdot 3 \end{pmatrix} = \begin{pmatrix} 14 \\ 32 \end{pmatrix}$$

Remark 26.

$$e_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$A \cdot e_k = s_k = k\text{-th column vector}$$

Theorem 79. *1. Let $A \in K^{m\times n}$. Then the mapping*

$$f_A : K^n \to K^m$$

$$x \to Ax$$

is linear.

2. For every $f \in \mathrm{Hom}(K^n, K^m)$ there exists a distinct matrix $A \in K^{m\times n}$ such that $f = f_A$.

$\boxed{\text{Namely the } k\text{-th column of } A = f(e_k) = A \cdot e_k}$.

3.

$$K^{m\times n} \to \mathrm{Hom}(K^n, K^m)$$

$A \mapsto f_A$ is an isomorphism.

This lecture took place on 11th of Jan 2016 (Franz Lehner).

9.1 Revision

We look at homomorphisms between vector spaces:

$$f : V \to W$$

$$+/\cdot : \mathrm{Hom}(V, W)$$

$$f(v + w) = f(v) + f(w)$$

$$f(\lambda w) = \lambda \cdot f(w)$$

Images and preimages of subspaces are subspaces. Especially,

$$\ker f = f^{-1}(\{0\})$$

$$\mathrm{im}\, f = f(V)$$

$$\dim\ker(f) + \dim\mathrm{im}(f) = \dim V$$

Every vector space has basis. Let $B \subseteq V$ be a basis

$$\bigwedge_{f:B\to W} \dot{\bigvee}_{\tilde{f}:V\to W} \tilde{f} \text{ linear} \wedge \tilde{f}\Big|_B = f$$

Followingly, if two mappings $f, g \in \mathrm{Hom}(V, W)$ are equivalent if and only if $f|_B = g|_B$.

If $\dim V < \infty$, $V \tilde{-} W \Leftrightarrow \dim V = \dim W$.

9.2 Matrix

$$A = \begin{bmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{bmatrix} \in K^{m\times n}$$

$$f_A : K^n \to K^m$$

$$f_A : x \mapsto A \cdot x = \begin{pmatrix} \sum_{j=1}^n a_{1,j}x_j \\ \sum_{j=1}^n a_{2,j}x_j \\ \vdots \\ \sum_{j=1}^n a_{mj}x_j \end{pmatrix}$$

Remark 27. $A \cdot e_k = s_k(A)$[5]

Theorem 80. *1. The mapping $f_A : K^n \to K^m$ is linear.*

[5] where s_k refers to the k-th column?

2. *For every $f \in \mathrm{Hom}(K^n, K^m)$ there is one unique matrix $A \in K^{m\times n}$, such that $f = f_A$. Therefore $f(x) = A \cdot x$ for all $x \in K^n$.*

3. *The mapping $K^{m\times n} \to \mathrm{Hom}(K^n, K^m)$ with $A \mapsto f_A$ is a homomorphism.*

Remark 28. *So linear mappings and matrices are semantically equivalent.*

Proof. We prove the three theorems.

1. Basic calculations.

2. Because of Remark 27 it must have a matrix with a column $s_k(A) = f(e_k)$, which satisfies $f = f_A$. Therefore it holds that $f(e_k) = f_A(e_k)$ and followingly, $f = f_A$ on the canonical basis from which $f = f_A$ on K^n follows.

   Basis of $\mathrm{Hom}(K^n, K^m)$? f_{ij} follows from Theorem 74:

$$f_{ij} : K^n \to K^m$$

$$e_k \mapsto \begin{cases} e_j & k = i \\ 0 & k \neq i \end{cases}$$

   which is equivalent to

$$s_k(H_{ij}) = \begin{cases} e_j & \text{if } k = i \\ 0 & \text{else} \end{cases}$$

$$H_{ij} = j \begin{bmatrix} \ddots & \dots & \ddots \\ \vdots & 1 & \vdots \\ \ddots & \dots & \ddots \end{bmatrix} = E_{ji}$$

   Basis of $K^{n\times m}$.

   We elaborate:

$$(f_{ij})_{\substack{i\in\{1,\dots,n\} \\ j\in\{1,\dots,m\}}}$$

   is basis of (K^n, K^m).

$$f_{ij} = f_{E_{ji}} \text{ where } E_{ji} = \text{ elementary matrix}$$

$$f = \sum \alpha_{ij} f_{ij} \in \mathrm{Hom}(K^n, K^m)$$

$$(E_{ji})_{\substack{i=1,\dots,n \\ j=1,\dots,m}} \text{ build basis in } K^{m\times n}$$

$$\Rightarrow f = f_{\sum \alpha_{ij} E_{ji}} = f_A$$

$$A = \sum \alpha_{ij} E_{ji}$$

The mapping

$$K^{m\times n} \to \mathrm{Hom}(K^n, K^m)$$

$$A \to f_A$$

is linear and build a basis (E_{ij}) maps to the basis (f_{ij}). Therefore it holds that

$$K^{m\times n} \overset{\sim}{-} \mathrm{Hom}(K^n, K^m)$$

□

Example 52.

$$f = id : K^n \to K^n$$

$$f(e_k) = e_k \to a = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} = I_n$$

$$f_{\lambda A + \mu B} = \lambda \cdot f_A + \mu \cdot f_B$$

Composition:

$$f_A \cdot f_B = f_C$$

$$K^p \to K^m \to K^n$$

Definition 35. *Let $A \in K^{n\times m}$ and $B \in K^{m\times p}$. Then the matrix $C := A \cdot B \in K^{n\times p}$ with $C_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj}$ for $i \in \{1, \dots, n\}, j \in \{1, \dots, p\}$ is the* product *of* A and B

$$A \cdot x = \begin{pmatrix} \sum_{k=1}^{m} a_{1k} \cdot x_k \\ \vdots \\ \sum_{k=1}^{m} a_{nk} \cdot x_k \end{pmatrix}$$

where $x \in K^m$. Therefore $s_j(C) = A \cdot s_j(B)$ is column of C; A times the j-th column of B.

Example 53.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} = \begin{pmatrix} 14 & 32 \\ 32 & 77 \end{pmatrix}$$

Use the schema,

$$\begin{array}{ccc|cc} & & & 1 & 4 \\ & & & 2 & 5 \\ & & & 3 & 6 \\ \hline 1 & 2 & 3 & 14 & 32 \\ 4 & 5 & 6 & 32 & 77 \end{array}$$

Remark 29. $A \cdot B \neq B \cdot A$.

$$A \cdot B = \begin{array}{cc|cc} & & 0 & 0 \\ & & 1 & 0 \\ \hline 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}$$

$$B \cdot A = \begin{array}{cc|cc} & & 0 & 1 \\ & & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}$$

Example 54.

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

$A^2 = A$ shows an idempotent property (infinitely many solutions).

Theorem 81.

$$f_A \circ f_B = f_{A \cdot B}$$

Proof. It suffices to check the basis.

$$f_A \cdot f_B(e_k) \overset{\text{Remark 27}}{=} A \cdot f_B(e_k)$$

$$= A \cdot s_k(B) \overset{\text{def. of } A\cdot B}{=} s_k(A \cdot B) = f_{A \cdot B}(e_k)$$

Alternative, more educational, proof: direct □

Corollary 19. *The matrix product is associative:*

$$A \in K^{n \times m} \quad B \in K^{m \times p} \quad C \in K^{p \times q}$$

$$\underbrace{\underbrace{(A \cdot B)}_{n \times p} \cdot C}_{n \times q} = \underbrace{A \cdot \underbrace{(B \cdot C)}_{m \times q}}_{n \times q}$$

Proof.

$$\begin{aligned} f_{A \cdot (B \cdot C)} &= f_A \circ f_{B \cdot C} \\ &= f_A \circ (f_B \circ f_C) \\ &= (f_A \circ f_B) \circ f_C \\ &= f_{A \cdot C} \circ f_C \\ &= f_{(A \cdot B) \circ C} \end{aligned}$$

□

Theorem 82. *1.*

$$\bigwedge_{A \in K^{n \times m}} \bigwedge_{B, C \in K^{m \times p}} A(B + C) = A \cdot B + A \cdot C$$

2.

$$\bigwedge_{A, B \in K^{n \times m}} \bigwedge_{C \in K^{m \times p}} (A + B) \cdot C = A \cdot C + B \cdot C$$

3.

$$\bigwedge_{\lambda \in K} \bigwedge_{A \in K^{n \times m}} \bigwedge_{B \in K^{m \times p}} \lambda(A \cdot B) - (\lambda A) \cdot BB = A \cdot (\lambda B)$$

4.

$$\bigwedge_{A \in K^{n \times m}} \bigwedge_{B \in K^{m \times p}} (A \cdot B)^T = B^T \cdot A^T$$

5.

$$\bigwedge_{A \in K^{n \times m}} I_n \cdot A = A = A \cdot I_m$$

Proof. 1. Immediate.

2. Immediate.

3. Immediate.

4.

$$\begin{aligned}\left((A\cdot B)^T\right)_{ij} &= (A\cdot B)_{ji}\\ &= \sum_{k=1}^{m} a_{jk}b_{ki}\\ &= \sum_{k=1}^{m} b_{ki}a_{jk}\\ &= \sum_{k=1}^{m} (B^T)_{ik}(A^T)_{kj}\\ &= \left(B^T\cdot A^T\right)_{ij}\end{aligned}$$

$$\Rightarrow \text{ for all } i,j: (A\cdot B)^T = B^T\cdot A^T$$

□

Corollary 20. *$(K^{n\times n}, +, \cdot_{scalar\ product}, \cdot_{matrix\ product})$ is a K-algebra*[6] *isomorphic to* $\mathrm{End}(K^n)$.

Definition 36. *A matrix $A\in K^{n\times n}$ is called* regular *if it is invertible hence if*

$$\bigvee_{B\in K^{n\times n}} A\cdot B = B\cdot A = I$$

A matrix which is not regular, is called singular.

Theorem 83. *A matrix $A\in K^{n\times n}$ has at most one inverse. If it exists, the inverse of A is denoted A^{-1}.*

[6] Scalar product is given with $K\times K^{n\times n}\to K^{n\times n}$

Proof. Let B and B' be two inverse matrices.

$$B = B\cdot I = B\cdot(A\cdot B') = (B\cdot A)\cdot B' = I\cdot B' = B'$$

□

Remark 30. *For finite-dimensional matrices it suffices to find either a left-inverse or a right-inverse matrix. For infinite-dimensional matrices this does not work any more.*

Theorem 84. *1. I_n is regular. $I_n\cdot I_n = I_n$*

2. $A,B\in K^{n\times n}$ is regular $\Rightarrow A\cdot B$ is regular.

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

3. $A\in K^{n\times n}$ is regular, then A^{-1} is also regular.

$$\left(A^{-1}\right)^{-1} = A$$

4. $A\in K^{n\times n}$ is regular, then A^T is regular with

$$\left(A^T\right)^{-1} = \left(A^{-1}\right)^T$$

5. A is regular if and only if $f_A: K^n\to K^n$ is automorphism,

$$(f_A)^{-1} = f_{A^{-1}}$$

Proof. 2.

$$(A\cdot B)\cdot(B^{-1}\cdot A^{-1}) = A\cdot(B\cdot B^{-1})\cdot A^{-1} = A\cdot I\cdot A^{-1} = A\cdot A^{-1} = I$$

Also it holds that

$$(B^{-1}\cdot A^{-1})\cdot(A\cdot B) = I$$

3. $A^{-1}\cdot A = I$. $A\cdot A^{-1} = I$. A^{-1} has A as inverse.

4. $A^T\cdot(A^{-1})^T = \left(A^{-1}\cdot A\right)^T = I^T = I$

5. $f_A\circ f_{A^{-1}} = f_{A\cdot A^{-1}} = f_I = \mathrm{id}$. So $f_A\circ f_B = \mathrm{id} \Leftrightarrow A\cdot B = I$

□

Example 55. *1.* $(\lambda \cdot I)^{-1} = \frac{1}{\lambda} I$

$$(\lambda \cdot A)^{-1} = \frac{1}{\lambda} \cdot A^{-1} \qquad (\lambda \neq 0)$$

2.

$$\begin{bmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_n \end{bmatrix} \cdot \begin{bmatrix} b_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & b_n \end{bmatrix} \stackrel{?}{=} \begin{bmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{bmatrix}$$

because

$$\begin{bmatrix} a_1 b_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_n b_n \end{bmatrix} = \begin{bmatrix} b_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & b_n \end{bmatrix} \begin{bmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_n \end{bmatrix}$$

If $\begin{bmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_n \end{bmatrix}$ *is regular* $\Leftrightarrow$ *all* $a_i \neq 0$

$$\begin{bmatrix} a_1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & a_n \end{bmatrix} = \begin{bmatrix} \frac{1}{a_1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \frac{1}{a_n} \end{bmatrix}$$

3. *Let* $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ *be bijective (hence it is a permutation).*

$$f : \underbrace{\{e_1, \dots, e_n\}}_{\text{canonical basis}} \to \{e_1, \dots, e_n\}$$

$$f(e_i) = e_\sigma(i)$$

German keywords

English keywords