

# Linear Algebra – Lecture Notes

Lukas Prokop

winter term 2015

## Contents

<b>1 Set theory, logic and linear equations</b>	<b>5</b>	1.16 Remark about constructivism . . . . .	13
1.1 Axiomatic definition of a set . . . . .	5	1.16.1 $a^b$ is irrational with $a, b \in \mathbb{R}$ . . . . .	13
1.2 Notation for set theory . . . . .	5	1.17 Agreement . . . . .	13
1.3 Examples for custom sets . . . . .	7	1.18 Quantifiers . . . . .	13
1.4 Russell's paradoxon . . . . .	7	1.19 Proof using quantifiers . . . . .	15
1.5 Berrys paradoxon . . . . .	7	1.20 Negation with quantifiers . . . . .	15
1.6 Axiomatic system of Zermelo-Frauenkel . . . . .	7	1.21 Relation between set theory and boolean algebra . . . . .	15
1.7 Basics of logic . . . . .	7	<b>2 Power sets</b>	<b>17</b>
1.8 Gödel's incompleteness theorem . . . . .	9	<b>3 Relations of sets</b>	<b>17</b>
1.9 A correction . . . . .	9	<b>4 Solutions to linear equation systems</b>	<b>25</b>
1.10 Formal logic . . . . .	9	4.1 Substitution . . . . .	27
1.11 Definition . . . . .	9	4.2 Gauss-Jordan elimination algorithm . . . . .	33
1.12 Logical laws by DeMorgan . . . . .	9	<b>5 Vector spaces</b>	<b>35</b>
1.13 Proofs . . . . .	9	5.1 Properties . . . . .	35
1.14 Statement . . . . .	9	5.1.1 Addition . . . . .	35
1.14.1 Contraposition law . . . . .	11	5.1.2 Multiplication . . . . .	37
1.15 Proof by contradiction . . . . .	11	5.2 Applications . . . . .	37
1.15.1 $\sqrt{2}$ is irrational . . . . .	11		

5.2.1	Diagonals of a parallelogram . . . . .	37
5.2.2	Line crossing two points . . . . .	37
5.2.3	A layer can be defined by three points . . . . .	37
5.3	Algebraic structures . . . . .	37
5.3.1	Examples . . . . .	39
5.4	Compositions . . . . .	39
<b>6</b>	<b>Vector spaces</b>	<b>67</b>
6.1	Subspaces, linear independence and bases . . . . .	71
6.2	Construction of subspaces . . . . .	73
6.3	Revision . . . . .	77
6.4	Revision . . . . .	93
6.5	Summary for finite vector spaces . . . . .	99
6.6	Revision . . . . .	99
6.7	Representation of vector spaces . . . . .	99
<b>7</b>	<b>Construction of vector spaces</b>	<b>103</b>

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 unseres 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  $M$ :  $x \notin M$

### 1.2 Notation for set theory

Approaches for notations:

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

- $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$
- $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{N} \right\}$
- $\mathbb{R}$  = complex definition, see analysis
- $\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$
- $\{\} = \emptyset$  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, Zermelo 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  $\mathcal{P}(A) = \{B \mid B \subseteq A\}$

### 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**  $A \wedge B$  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**  $A \vee B$  is true, if  $A$  or  $B$  is true (latin "vel")

**Exclusive disjunction**  $A \dot{\vee} B$  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 ( $\neg(A \dot{\vee} B)$ )

**Implication / subjuction**  $A \implies B$  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

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

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, then  $n$  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

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

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

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

$$\begin{aligned} A^C &= \{x \in U \mid x \notin A\} \quad \text{“complement in } U, \text{ the universe”} \\ &= U \setminus A \end{aligned}$$

$$\begin{aligned} A \subseteq B &\Leftrightarrow \bigwedge_{x \in A} x \in B \\ &\Leftrightarrow \bigwedge_x (x \in A \implies x \in B) \end{aligned}$$

$$A = B \Leftrightarrow \bigwedge_x x \in A \Leftrightarrow x \in B$$

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

$$\bigcap_{i \in I} A_i = \left\{ x \mid \bigwedge_{i \in I} x \in A_i \right\} \quad \text{intersection of all } A_i$$

$$\bigcup_{i \in I} A_i = \left\{ x \mid \bigvee_i x \in A_i \right\} \quad \text{union of all } A_i$$

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

What happens at  $I = \emptyset$ ?

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

This is axiomatic:

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

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

$$\bigcap_{x \in \mathbb{R}} A_x = \left\{ y \mid \bigwedge_{x \in \mathbb{R}} y \in A_x \right\}$$

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



## 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  $(x, x) \in R$ )

**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 konnvexity 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:

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

$X/\sim = \{[x] \mid x \in X\}$  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  $x \sim y \xrightarrow{\text{symmetrical}} y \sim x$ . Hence  $y \sim x \wedge x \sim z \xrightarrow{\text{transitive}} y \sim z \implies z \in [y]$ . 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

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

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

**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  $X/\sim = \{[x] \mid x \in X\} \subseteq \mathcal{P}(X)$

- 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  $\bigwedge_{x,y \in X} [x] \cap [y] \neq \emptyset \implies [x] = [y] \iff x \sim y$ .

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

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

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

$$f : X \rightarrow Y$$

$$x \mapsto f(x)$$

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:

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

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

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

Remarks:

1. Domain and codomain are part of the definition of a function. A function is unambiguously defined by some graph:

□

- 2.

$$G_f = \{(x, f(x)) \mid x \in X\} \subseteq X \times Y$$

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

$$\bigwedge_{x \in X} \bigvee_{y \in Y} (x, y) \in G_f$$

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

Hence the domain and codomain must be equivalent.

4. The function  $\text{id}_X : X \rightarrow X$  is called “identity”.

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

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

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

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

6. Every function  $f : X \rightarrow \{0, 1\}$  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  $f : X \rightarrow Y$ . Then  $f|_A : A \rightarrow Y$  with  $a \mapsto f(a)$  is called *restriction of f to A*.

$f|_A$  is not defined outside  $A$ .

Let  $f : X \rightarrow Y$  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

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

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

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

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

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

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

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

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

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

Remark:

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

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

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

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

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.

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

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

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

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

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

Examples:

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

- $f : x \mapsto x^2$  in  $\mathbb{R} \rightarrow \mathbb{R}$  is not injective and not surjective. We have a restriction:

$$\tilde{f} : \mathbb{R}_0^+ \rightarrow \mathbb{R}_0^+$$

With this domain, the function is bijective.

- $f : x \mapsto x^3$  in  $\mathbb{R} \rightarrow \mathbb{R}$  is bijective.
- $f : A \mapsto A^C = X \setminus A$  in  $\mathcal{P}(X) \rightarrow \mathcal{P}(X)$ . 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  $f : X \rightarrow Y$  and  $g : Y \rightarrow Z$  be functions, the function

$$g \circ f : X \rightarrow Z$$

$$x \mapsto g(f(x))$$

is called composition of  $f$  and  $g$ .

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

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

Then

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

*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  $g \circ f(x_1) = g \circ f(x_2)$ . 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  $f : X \rightarrow Y$  is bijective, then  $f^{-1} : Y \rightarrow X$  and it holds that

$$f \circ f^{-1} = \text{id}_Y$$

$$f^{-1} \circ f = \text{id}_X$$

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:

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

with coefficients  $a_{ij}$ ,  $b_i \in \mathbb{R}$  for all  $i \in \{1, 2, \dots, n\}$  and  $j \in \{1, 2, \dots, n\}$ .  $x_1, x_2, \dots, x_n$  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  $(x_1, \dots, x_n)$ , which satisfies the equation.

The scheme

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

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;  $(0, 0, \dots, 0)$ .

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

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:

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

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

$$a_1 = 0, b \neq 0 \quad \text{no solution}$$

$$n = 2, m = 2$$

$$a_{1,1}x + a_{1,2}y = b_1$$

$$a_{2,1}x + a_{2,2}y = b_2$$

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.

$$x + y = 1$$

$$x - y = 2$$

We subtract the second from the first equation.

$$\begin{aligned} 0 - 2y &= 1 \\ \Rightarrow y &= -\frac{1}{2} \\ \Rightarrow x = 1 - y &= \frac{3}{2} \end{aligned}$$

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:

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

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 freedom.

**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:

$$\begin{aligned} -x + y + 2z &= 2 \\ 2y + 2z &= 2 \\ 5z &= 10 \end{aligned}$$

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

$$3x + 2y + z = 3$$

$$2x + y + z = 0$$

$$6x + 2y + z = 6$$

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

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.

$$( \ 0 \ 0 \ 2 \ 0 \mid 0 \ )$$

Therefore  $2x_3 = 0$ .

$$( \ 0 \ 0 \ 0 \ 0 \mid 0 \ )$$

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

## 5 Vector spaces

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

$$\left\{ a_1 a_2 \dots a_n \mid a_i \in \mathbb{R} \right\}$$

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

We define addition:

$$\begin{matrix} \vec{a} & \vec{b} & \vec{a} + \vec{b} \\ a_1 a_2 \dots a_n & + & b_1 b_2 \dots b_n := a_1 + b_1, a_2 + b_2, \dots, a_n + b_n \end{matrix}$$

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

$$\lambda \cdot \begin{matrix} \vec{a} \\ a_1 a_2 \dots a_n \end{matrix} := \begin{matrix} \vec{\lambda a} \\ \lambda a_1 \lambda a_2 \dots \lambda a_n \end{matrix}$$

Geometric interpretation for  $n = 1, 2, 3, \dots$ : 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**  $(A, B) \sim (A, B)$ ,  $\checkmark$

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

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

A vector is therefore an equivalence class of directed paths.

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

The set of vectors is in bijection with the set of 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 ( $M \neq N$ ).

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

$$= \overrightarrow{OA} - \frac{1}{2}(\overrightarrow{AB} + \overrightarrow{BC})$$

$$\begin{aligned} \overrightarrow{ON} &= \overrightarrow{OB} + \frac{1}{2}\overrightarrow{BD} \\ &= \overrightarrow{OA} + \overrightarrow{AB} + \frac{1}{2}\overrightarrow{BD} \\ &= \overrightarrow{OA} + \overrightarrow{AB} + \frac{1}{2}(\overrightarrow{BC} + \overrightarrow{CD}) \\ &= \overrightarrow{OA} + \overrightarrow{AB} + \frac{1}{2}(\overrightarrow{AD} + \overrightarrow{BA}) \\ &= \overrightarrow{OA} + \overrightarrow{AB} + \frac{1}{2}\overrightarrow{AD} - \frac{1}{2}\overrightarrow{AB} \\ &= \overrightarrow{OA} + \frac{1}{2}\overrightarrow{AB} + \frac{1}{2}\overrightarrow{AD} \\ &= \overrightarrow{OM} \end{aligned}$$

### 5.2.2 Line crossing two points

The line crossing two points  $P_1$  and  $P_2$  is defined as

$$\begin{aligned} &\left\{ \overrightarrow{OP_1} + t \cdot \overrightarrow{P_1P_2} \mid t \in \mathbb{R} \right\} \\ &= \left\{ \overrightarrow{OP_1} + t \cdot (\overrightarrow{OP_2} - \overrightarrow{OP_1}) \mid t \in \mathbb{R} \right\} \end{aligned}$$

### 5.2.3 A layer can be defined by three points

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

$$\left\{ \overrightarrow{OP_1} + s \cdot \overrightarrow{P_1P_2} + t \cdot \overrightarrow{P_1P_3} \mid s, t \in \mathbb{R} \right\}$$

## 5.3 Algebraic structures

A set  $M$  with a mapping  $\circ : M \times M \rightarrow M$  ( $(x, y) \mapsto x \circ y$ ) 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  $\circ$ :

$$\begin{aligned}\circ &= +, \cdot \\ x \circ y &= x + y \\ x \circ y &= x \cdot y\end{aligned}$$

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

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

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

$$a_1 \dots a_m \circ b_1 \dots b_n = a_1 \dots a_m b_1 \dots b_n$$

$A^*$  is the set of possible words.  $A^+$  is defined as  $A^* \setminus \{\varepsilon\}$  where  $\varepsilon$  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  $M = X^X = \{f : X \rightarrow X\}$  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<sup>1</sup>. The last two examples are not commutative; others are<sup>2</sup>

An element  $e \in M$  is called

**left-neutral if**

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

**right-neutral if**

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

<sup>1</sup>Assuming the first example uses addition.  $x^y$  is not associative.

<sup>2</sup>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.  $\varepsilon$  as neutral element
6. identity function acts as neutral element,  $\text{id} \circ f = f' = f \circ \text{id}$

Let  $(M, \circ)$  be a magma 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  $a_1, \dots, a_m$ , the invertible elements are  $\{\varepsilon\}$

6. The invertible elements are defined by any bijective mapping  $X \rightarrow X$ .

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.

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:

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

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

*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	$(M, \circ), \circ : M \times M \rightarrow M$
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.  $e \circ e = e \Rightarrow e$  is invertible  $\Rightarrow e \in G$

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

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

$$\stackrel{G1}{\Rightarrow} \text{associative}$$

$$\stackrel{G2}{\Rightarrow} \bigvee_e \bigwedge_x e \circ x = x$$

$$\stackrel{G3}{\Rightarrow} \bigvee_x \bigwedge_y y \circ x = e$$

Show that

i. A left-neutral element is right-neutral

ii. Left-inverse elements are also right-inverse

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

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

$$\begin{aligned}
 &\stackrel{G1}{=} z \circ (y \circ x) \circ y \\
 &= z \circ (e \circ y) \\
 &= z \circ y = e
 \end{aligned}$$

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

$$\begin{aligned}
 x \circ e &= x \circ (y \circ x) \stackrel{G1}{=} (x \circ y) \circ x = e \circ x \stackrel{G2}{=} x \\
 &\Rightarrow e \text{ is also right-neutral}
 \end{aligned}$$

□

□

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

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

**Corollary 1.**

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

$$S_X = \{f : X \rightarrow X \text{ bijective}\}$$

$(S_X, \circ)$  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  $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  bijective. Then  $\pi$  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  $f : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  is bijective.  $\Leftrightarrow f$  is injective.  $\Leftrightarrow f$  is surjective. This does not hold for infinite sets.

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

$$f(n) = 2n$$

is injective, but not surjective

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

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

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

$$|S_n| = n!$$

$S_3$  is non-commutative!

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

**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	$h$	$v$	$d_\pi$
id	id	$h$	$v$	$d_\pi$
$h$	$h$	id	$d_\pi$	$v$
$v$	$v$	$d_\pi$	id	$h$
$d_\pi$	$d_\pi$	$v$	$h$	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*

$$x \equiv y \pmod{n} \Leftrightarrow n \mid x - y$$

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

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

*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*

$$x \equiv x' \pmod{n} \quad (\text{ie. } [x]_n = [x']_n)$$

*and*

$$y \equiv y' \pmod{n} \quad (\text{ie. } [y]_n = [y']_n)$$

*then also  $x + y \equiv x' + y' \pmod{n}$  (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*

$$x \equiv x' \pmod{n}$$

*and*

$$y \equiv y' \pmod{n}$$

*then also  $x \circ y \equiv x' \cdot y' \pmod{n}$  (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  $x = x' \pmod{n}$  and  $y = y' \pmod{n}$ . 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:

$n \notin \mathbb{P}$

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

$$[n_1]_n \cdot [n_2]_n = [n_1 \cdot n_2]_n = [n]_n = [0]_n$$

$\Rightarrow [n_1]_n$  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.

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

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

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

therefore

$$\bigvee_k k \cdot x \equiv 0 \pmod{n}$$

$$\Rightarrow n \mid kx$$

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

$$\Rightarrow n \mid x$$

$$\Rightarrow [x]_n$$

$$\Rightarrow [0]_n$$

This is a contradiction.

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

*Proof.* Assume

$$\begin{aligned} \bigvee_{1 \leq k, l \leq n-1} [kx]_n &= [lx]_n \\ [kx]_n - [lx]_n &= [0]_n \\ [(k-l)x] &= [0]_n \\ \Rightarrow (k-l)x &\equiv 0 \pmod n \\ \Rightarrow n &\mid (k-l)x \\ \Rightarrow n &\mid k-l \vee n \mid x \end{aligned}$$

The second condition cannot hold.

$$\Rightarrow k-l=0$$

Requirement:  $[x]_n \neq [0]_n$ .

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

are all different.

$$\begin{aligned} \Rightarrow \bigvee_k [kv]_n &= [1]_n \\ \Rightarrow [k]_n &= [x]_n^{-1} \end{aligned}$$

$k$  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
2	2	4	0	2
3	3	0	3	0
4	4	2	0	4
4	5	4	3	2

□

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  $(\{\pm 1\}, \cdot)$

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

$$[0]_2 \rightarrow +1$$

$$[1]_2 \rightarrow -2$$

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

$$h : G_1 \rightarrow G_2$$

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

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

$$[0]_2 \mapsto +1$$

$$[1]_2 \mapsto -1$$

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

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

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

$$h_n : \mathbb{Z} \rightarrow \mathbb{Z}$$

$$h_n : x \mapsto n \cdot x$$

Is an endomorphism.

Show that

$$h_n(x + y) = h_n(x) + h_n(y)$$

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

No epimorphism for  $n \geq 2$ .

2.

$$g : \mathbb{Z} \rightarrow \mathbb{Z}$$

$$x \mapsto x + 1$$

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

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

$$4 \neq 3$$

3.

$$q_n : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_n, +)$$

$$a \mapsto [a]_n$$

Show that

$$q_n(a + b) = q_n(a) + q_n(b)$$

$$q_n(a + b) = [a + b]_n$$

$$= [a]_n + [b]_n$$

$$= q_n(a) + q_n(b)$$

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

$$[1]_n = q_n(1)$$

$$\vdots$$

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

*Epimorphism, but no isomorphism.*

4.

$$(\mathbb{R}^*, \cdot) \rightarrow (\{\pm 1\}, \cdot)$$

$$\mathbb{R}^* = \mathbb{R} \setminus \{0\}$$

$$\text{sign} : x \mapsto \text{sign}(x)$$

$$\text{sign}(x \cdot y) = \text{sign}(x) \cdot \text{sign}(y)$$

*is a group homomorphism and epimorphism, but no isomorphism.*

5.

$$h : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$$

$$x \mapsto -x$$

$$h(x+y) = -(x+y) = -x-y = h(x) + h(y)$$

*is homomorphism.*

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

6.

$$(\mathbb{R}^+ = ]0, \infty[, \cdot) \rightarrow (\mathbb{R}, +)$$

$$x \mapsto \log(x)$$

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

*Is a group homomorphism, epimorphism and isomorphism.*

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

*Let*

$$q : (G_1, \circ_1) \rightarrow (G_2, \circ_2)$$

$$h : (G_2, \circ_2) \rightarrow (G_3, \circ_3)$$

*be homomorphisms, then  $h \circ q : (G_1, \circ_1) \rightarrow (G_3, \circ_3)$  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  $G_1 \cong G_2$  is an equivalence relation.*

*Proof.* 1.

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

$$(h \circ g)(a \circ_1 b) = h(g(a \circ_1 b))$$

$$\stackrel{g \text{ is homomorphous}}{=} h(g(a) \circ_2 g(b))$$

$$\stackrel{h \text{ is homomorphous}}{=} h(g(a)) \circ_3 h(g(b))$$

$$= (h \circ g)(a) \circ_3 (h \circ g)(b)$$

2. To be worked through in the practicals.

3. To be worked through in the practicals.

□

**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  $h : G_1 \rightarrow G_2$  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.

$$h(e_1) = h(e_1) \circ e_2$$

$$h(e_1) = h(e_1 \circ e_1)$$

$$= h(e_1) \circ h(e_1)$$

$$h(e_1) \circ e_2 = h(e_1) \circ h(e_1)$$

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

2.

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

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

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.**

$$(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \quad \checkmark$$

$$(\mathbb{N}, +) \subseteq (\mathbb{Q}, +) \quad \nexists$$

$$(\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \quad \checkmark$$

$$(\mathbb{Q}, +) \subseteq (\mathbb{C}, +) \quad \checkmark$$

$n \in \mathbb{N}$  is fixed:

$$n \cdot \mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\} \leq \mathbb{Z}$$

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

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

**Theorem 15.**

$$S_n \leq S_{n+1}$$

$$S_n = \{f : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ is bijective}\}$$

$$S_{n+1} = \{f : \{1, \dots, n+1\} \rightarrow \{1, \dots, n+1\} \text{ is bijective}\}$$

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  $S_n \cong H$ .

$$H = \{f : \{1, \dots, n+1\} \rightarrow \{1, \dots, n+1\} \mid f \text{ is bijective}\} \\ \Rightarrow H \cong S_n$$

**Corollary 3.**

$$\mathbb{Z} \rightarrow n \cdot \mathbb{Z} \leq \mathbb{Z}$$

$$x \mapsto n \cdot x$$

is bijective.

$$\Rightarrow \mathbb{Z} \cong n \cdot \mathbb{Z}$$

$\Rightarrow \mathbb{Z}$  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.

$$h : G_1 \rightarrow G_2 \text{ is a homomorphism}$$

$$H_1 \leq G_1 \quad H_2 \leq G_2 \quad \text{are subgroups}$$

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:

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

$\Rightarrow$  choose  $z = x \circ_1 y \in H_1$  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  $h : G_1 \rightarrow G_2$  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  $R \times R \rightarrow R$ , 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  $(\mathbb{C}, +, \cdot)$ .

$$\mathbb{R}[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{N}_0, a_i \in \mathbb{R}\}$$

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  $a \cdot (1 \cdot x_+^0 \cdot \dots) = a$ ).

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

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

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:

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

□ “Es ändert nichts an dem Ganzen, aber sie haben ein besseres Gefühl.”  
(Franz Lehner)

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  $\bigvee_{y \in R} y \neq 0 \wedge x \cdot y = 0$ .  $R$  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  $h : R_1 \rightarrow R_2$  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.**

$$\begin{aligned} (\mathbb{Z}, +, \cdot) &\rightarrow (\mathbb{Z}_n, +, \cdot) \\ x &\mapsto [x]_n \end{aligned}$$

**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

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

*Proof.* One possible trivial ring is:

$$R = \{a\}$$

$$a + a := a \quad a \cdot a := a$$

3. Select  $a \notin \{0\}$ . Then

$$1 \cdot a = a$$

$$0 \cdot a = 0$$

$$\Rightarrow 1 \neq 0$$

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

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

$$\Rightarrow 0 = 1 \quad \nexists$$

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*

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

*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

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

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

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

**Corollary 5.**

$$\underbrace{\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})}_{\mathbb{N}_0} \subseteq \underbrace{\mathbb{R} \subseteq \mathbb{C}}_{\mathbb{N}_1}$$

*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  $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$  has  $n$  solutions.*

*Therefore  $\mathbb{C}$  is algebraically closed (but there exist transcendental 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  $\mathbb{Z}$ .  $\bar{z} = x - iy$  is called complex conjugate of  $z$ .  $i$  is defined as solution of the equation  $x^2 + 1 = 0$ .

*Geometrically, the real part is 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:

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

So geometrically this is rotation by  $\varphi$  with scaling by factor  $r$ .

From this the Eulerian equation follows<sup>3</sup>.

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

## 6 Vector spaces

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

- $V \times V \rightarrow V$   
 $(\lambda, \mu) \mapsto v \oplus \mu$
- $K \times V \rightarrow V$   
 $(\lambda, \mu) \rightarrow \lambda \odot v$

such that

1.  $(V, \oplus)$  is an abelian group.
2. associative law holds:

$$\bigwedge_{v \in V} \bigwedge_{\lambda \in K} \bigwedge_{\mu \in K} (\lambda \cdot \mu) \odot v = \lambda \odot (\mu \odot v)$$

3. distributive law holds:

$$\bigwedge_{\lambda \in K} \bigwedge_{v, w \in V} \lambda \odot (v \oplus w) = (\lambda \odot v) \oplus (\lambda \odot w)$$

---

<sup>3</sup>but can only be seen easily with the Taylor series expansion of  $e$

$$\bigwedge_{\lambda, \mu \in K} \bigwedge_{v \in V} (\lambda + \mu) \odot v = (\lambda \odot v) \oplus (\mu \odot v)$$

4. Furthermore,

$$\bigwedge_{v \in V} 1 \odot v = v$$

**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  $\odot$  (vector multiplication)

**Example 15.** 1.

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

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

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

- 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 multiplication is done component-wise.

3. Let  $X$  be an arbitrary set.

$$K^X = \{f : X \rightarrow K \mid f \text{ function}\}$$

$$(f + g)(x) := f(x) + g(x)$$

$$(\lambda f)(x) := \lambda(f(x))$$

$$\Rightarrow f + g, \lambda \cdot f \in K^X$$

*Proof.* (a) is a special case of (c) Specifically  $X = \{1, \dots, n\}$ . Every function  $f : \{1, \dots, n\} \rightarrow K$  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  $f : \{1, \dots, n\} \rightarrow K$  with

$$k \mapsto \varepsilon_k.$$

(d)

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

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.

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

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

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

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

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

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

$$\mathbb{R} = \mathbb{Q}^X$$

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  $K$ .

$$1. \bigwedge_{v \in V} 0 \cdot v = \underline{0}$$

□

$$2. \bigwedge_{\lambda \in K} \lambda \cdot \underline{0} = \underline{0}$$

$$3. \bigwedge_{v \in V} \bigwedge_{\lambda \in K} \lambda \cdot v = \underline{0} \Rightarrow \lambda = 0 \vee v = \underline{0}$$

$$4. \bigwedge_{v \in V} (-1) \cdot v = -v \text{ with } -v \text{ as neutral element in } (V, +)$$

*Proof.* 1. For the zero element it holds,

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

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

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.

$$\lambda v = 0 \Rightarrow \lambda = 0 \vee v = 0$$

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

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

*Proof.*

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

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  $\mathbb{Q}$ .

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

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

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

□

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

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

*Proof.*

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

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

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

3.  $V = \mathbb{R}^2$  with  $U = \{(x, y) \in \mathbb{R}^2 \mid x + y = 1\}$  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:

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

**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**

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

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

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

□

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

□

$$\begin{aligned} \bigwedge_{i \in I} a \in U_i \wedge b \in U_i &\xrightarrow{\text{all } U_i \text{ are subspaces}} \bigwedge_{i \in I} \lambda a + \mu b \in U_i \\ &\Rightarrow \lambda a + \mu b \in \bigcap_{i \in I} U_i \end{aligned}$$

□

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

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

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

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

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

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  $M$ :

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

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  $\lambda, a \in [\{a\}] \forall \lambda \in K$ .

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

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

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

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

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

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  $a_1, \dots, a_n \in V$ .

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

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

with  $\lambda_i \in K$ .

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

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

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

Construction of arbitrary finitely many vectors.

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

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

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

**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  $a \in M \Rightarrow a = 1 \cdot a \in L(M)$

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

$M \subseteq L(M)$ .  $L(M)$  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  $u = \lambda_1 a_1 + \dots + \lambda_m a_m$  with  $\lambda_i \in K$  and  $a_i \in M$ . Let  $v = \mu_1 b_1 + \dots + \mu_n b_n$  with  $\mu_i \in K, b_i \in M$ .

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

with

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

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

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

### 6.3 Revision

$$U \subseteq V \quad U \neq \emptyset$$

**(1)**  $U \neq \emptyset$

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

Therefore every linear combination is also in  $U$ .

$M \subseteq V$  subset

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

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

**Theorem 26.**

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

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

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

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  $L(M)$ .

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

Let  $v_1,$

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

$$\Rightarrow [M] = M$$

- ?? arbitrary ??

- Regarding notation: ?? ToDo content incomplete/incorrect

Notation:

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

ToDo content incomplete/incorrect

**Example 19.**

$$\begin{aligned} V &= \mathbb{R}^3 & K &= \mathbb{R} \\ M &= \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\} \\ [M] &= L(M) = \left\{ \lambda \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \mu \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \mid \lambda, \mu \in \mathbb{R} \right\} \\ &= \left\{ \begin{pmatrix} \lambda \\ \lambda \\ \lambda + \mu \end{pmatrix} \mid \lambda, \mu \in \mathbb{R} \right\} \\ &= \left\{ \begin{pmatrix} \lambda \\ \lambda \\ \mu' \end{pmatrix} \mid \lambda, \mu' \in \mathbb{R} \right\} \\ &= \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mid x_1 = x_2 \right\} \end{aligned}$$

**Example 20.**

$$\begin{aligned} V &= (\mathbb{Z}_3)^3 & K &= \mathbb{Z}_3 \\ V &= \left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mid x \in \mathbb{Z}_3 \right\} \\ |(\mathbb{Z}\mathbb{Z}_3)^3| &= 3^3 = 27 \\ M &= \left\{ \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \right\} \end{aligned}$$

$$\begin{aligned} L(M) &= \left\{ \lambda_1 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \lambda_3 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \mid \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}_3 \right\} \\ &= \left\{ \begin{pmatrix} \lambda_1 + \lambda_3 \\ \lambda_1 + \lambda_2 \\ \lambda_2 + \lambda_3 \end{pmatrix} \mid \lambda_2 \in \mathbb{Z}^3 \right\} \\ &= \left\{ \begin{pmatrix} \mu_2 \\ \mu_1 \\ \mu_2 \end{pmatrix} \mid \mu_1, \mu_2 \in \mathbb{Z}_3 \right\} = L\left( \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right) \end{aligned}$$

ToDo content incomplete/incorrect

$$\Rightarrow \text{vector } \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \text{ is useless}$$

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

**Remark 9.**

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

Let  $a \in L(M)$  then  $L(M) = L(M \cup \{a\})$ . Therefore linear hull does not increase.

ToDo content incomplete/incorrect

Let

$$w \in L(M \cup \{a\})$$

$$\Rightarrow \bigvee_{\lambda_1, \dots, \lambda_k} \bigvee_{\lambda_1, \dots, \lambda_k} w = \lambda_1 w_1 + \lambda_n w_n$$

ToDo content incomplete/incorrect

Case distinction:

**Case 1** all  $w \in M \Rightarrow w \in L(M)$



**Case 2** one of the  $w_i$  equals  $a$ . Wlog.  $w_1 = a$ . Therefore  $w_i \neq a$  for  $i \neq 1$ .

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

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

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  $(v_1, \dots, v_k) \in V$  is called linear independent, iff

$$\begin{aligned} \bigwedge_{\lambda_1, \dots, \lambda_n \in K} \lambda_1 v_1 + \lambda_2 v_2 + \dots + \lambda_n v_n &= 0 \\ \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_n &= 0 \end{aligned}$$

**Example 21.**

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

is linear independent.

$$\begin{aligned} \lambda_1 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \\ \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_1 \end{pmatrix} &= \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \\ \Rightarrow \lambda_1 = 0 \wedge \lambda_2 &= 0 \end{aligned}$$

**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!

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

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

**Theorem 27.** For a family  $(U_i)_{i \in I}$  mit an arbitrary index set  $I$  is called linear independent iff TODO content incomplete/incorrect

**Theorem 28.** A subset  $M \subseteq V$  is called linear independent if for every subfamily  $v_1, \dots, v_n$  every pairwise distinct  $v_i \in M$  are linear independent. A family  $(v_i)_{i \in I}$  is a mapping

$$\begin{aligned} f : I &\rightarrow V \\ i &\mapsto v_i \end{aligned}$$

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

**Theorem 29.** 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.** A one-tuple is linear dependent.

$$1 \cdot 0 = 0$$

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.

$$0 \cdot v_1 + 0 \cdot v_2 + \dots + 1 \cdot v_k + 0 \cdot v_{k+1} + \dots + 0 \cdot v_n = 0$$

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

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

$$\begin{aligned} 0v_1 + \dots + 0v_{k-1} + 1 \cdot v_k + 0 \cdot v_{k+1} \\ \dots (-1)v_l + 0v_{l+1} + \dots + 0 \cdot v_n = 0 \end{aligned}$$

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

$$\begin{aligned} \lambda_1 = 0 \quad \lambda_1 + \lambda_2 = 0 \\ \Rightarrow \lambda_1 - \lambda_2 = 0 \end{aligned}$$

**Corollary 14.**

$$V = K^n$$

**Corollary 12.** *If  $M \subseteq V$  is linear independent and  $N \subseteq M$ ,  $N$  is also linear independent. The unit vector is defined as*

**Corollary 13.**

$$\begin{aligned} (v_1, \dots, v_n) \text{ is linear independent} \\ \bigvee_{\lambda_1, \dots, \lambda_n \in K} \lambda_1 v_1 + \dots + \lambda_n v_n = 0 \\ \Rightarrow \bigvee_{k \in \{1, \dots, n\}} \bigvee_{\lambda_1, \dots, \lambda_n} v_l = \lambda_1 v_1 + \dots + \lambda_n v_n \end{aligned}$$

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

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

*where the 1 is given in row  $i$ .*

**Example 23.**

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

*are linear independent.*

$$\lambda_1 e_1 + \dots + \lambda_n e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

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

*then for all  $\lambda_i = 0$ .*

**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 independent. But*

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

**Theorem 30.** *Let  $v_1, \dots, v_n \in V$ . Then it holds equivalently,*

1.  $(v_1, \dots, v_n)$  is linear independent.
2.  $\bigwedge_{v \in L(\{v_1, \dots, v_n\})} \bigwedge_{\lambda_1, \dots, \lambda_n \in K} v = \lambda_1 v_1 + \dots + \lambda_n v_n$
3.  $\bigwedge_{k \in \{1, \dots, n\}} v_k \notin L(\{v_1, v_{k-1}, v_{k+1}, \dots, v_n\}) = \{v_1, \dots, v_{\hat{k}}, \dots, v_n\}$
4.  $\bigwedge_{k \in \{1, \dots, n\}} L(\{v_1, \dots, v_{k-1}v_{l+1}, \dots, v_n\}) \not\subset L(\{v_1, v_2, \dots, v_n\})$

*Proof.* Circle conclusion:  $1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 1$ .

For every  $v \in L(v_1, \dots, v_n)$ ,  $\bigwedge_{\lambda_1, \dots, \lambda_n} v = \lambda_1 v_1 + \dots + \lambda_n v_n$ . But is it unique?  
Assume  $v = \mu_1 v_1 + \dots + \mu_n v_n$ . Show that for all  $\lambda_i = \mu_i$ .

$$\Rightarrow v - v = \lambda_1 v_1 + \dots + \lambda_n v_n - (\mu_1 v_1 + \dots + \mu_n v_n)$$

$$0 = (\lambda_1 - \mu_1)v_1 + (\lambda_2 - \mu_2)v_2 + \dots + (\lambda_n - \mu_n)v_n$$

linear independence  $\Rightarrow \mu_1 - \mu = 0 \quad \lambda_n - \mu_n = 0$  Therefore for all,  $\lambda_i = \mu_i$ .

Assume

$$\bigvee_k U_k \in L(\{v_1, \dots, v_{\hat{k}}, \dots, v_n\})$$

$$\Rightarrow \bigvee_{\lambda_1, \dots, \lambda_n} v_k = \lambda_1 v_1 + \dots + \lambda_{n-1} v_{k-1} + 0 + \lambda_{k+1} v_{k+1} + \dots + \lambda_n v_n$$

$$\bigvee_{\lambda_1, \dots, \lambda_n} v_k = 0v_1 + \dots + 0v_{k-1} + 1 \cdot v_k + 0v_{k+1} + \dots + 0 \cdot v_n$$

So  $v_k$  has two different representations, this is a contradiction.

ToDo content incomplete/incorrect

Let  $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$ . Show that all  $\lambda_i = 0$ . Assume  $\bigwedge_k v_k = 0$ .

$$\Rightarrow \lambda$$

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).

$$\underbrace{[M]}_{\text{smallest subspace } \supseteq M} = \underbrace{L(M)}_{\text{set of all linear combinations}}$$

Conditions (from yesterday):

$$\Leftrightarrow \bigwedge_{v \in L(\{v_1, \dots, v_n\})} \bigvee_{\lambda_1, \dots, \lambda_n} v = \lambda_1 v_1 + \dots + \lambda_n v_n$$

$$\Leftrightarrow \bigwedge_k v_k \notin L(\{v_1, \dots, v_{\hat{k}}, \dots, v_n\})$$

$$\Leftrightarrow \bigwedge_{v \in L(M)} \bigvee_{n \in \mathbb{N}} \bigvee_{v_1, \dots, v_n \in M} \bigvee_{\lambda_1, \dots, \lambda_n} v = \lambda_1 v_1 + \dots + \lambda_n v_n$$

In general:  $M \subseteq V$  is called linear independent, if every subfamily of  $p_n$  different element is linear independent.

$$L(M) = V$$

**Definition 21.** • 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 10.** •  $(b_i)_{i \in I}$  is a basis of  $V$ . If

- every element is a linear combination of a finite subfamily  $b_{i_1}, \dots, b_{i_n}$ .
- every finite subfamily is linear independent.

- $(b_i)_{i \in \emptyset}$  is basis of  $\{0\}$ .
- if  $(b_1, \dots, b_n)$  is a basis of  $V$  then also every permutation  $(b_{i_1}, \dots, b_{i_n})$  (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  $(e_1, e_2, \dots, e_n)$  is

a basis of  $K^n$ ; specifically called canonical basis (or standard basis).

**Remark 11.**  $e_i$  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.**

$$K[X] := V = K^{\mathbb{N}_0} = \{(a_n)_{n \geq 0} \mid a_n \in K\}$$

Is the vector space of all sequences.

$$e_i = (0, \dots, 1, 0, \dots) \quad i \in \mathbb{N}_0$$

where 1 is given on the  $i$ -th position. If  $\sum \lambda_i e_i = (0, 0, \dots) \Rightarrow$  all  $\lambda_i = 0$  and  $(\lambda_0, \lambda_1, \dots) \Rightarrow (e_i)_{i \in \mathbb{N}_0}$  is linear independent.

Is not a basis, because 1 can never be reached.

$$(1, 1, 1, 1, \dots) \in \mathbb{R}^{\mathbb{N}_0}$$

$$\sum_{i=0}^n e_i = (1, 1, 1, \dots, 1, 0, 0, \dots) + (1, 1, 1, \dots)$$

for all  $n \in \mathbb{N}$ . In linear combinations only finitely many summands are allowed.

$L((e_i)_{i \in \mathbb{N}_0}) =$  vector space of all sequences  $(a_n)_{n \in \mathbb{N}_0}$  with arb. many  $a_n \neq 0$

is a subspace:  $(a_1, \dots, a_n, 0, \dots, 0) + (b_1, \dots, b_n, 0, \dots, 0)$ . Without loss of generality:  $m \leq n$ .

$$= (a_1 + b_1, \dots, a_m + b_m, b_{m+1}, \dots, b_n, 0, \dots, 0)$$

$(e_i)_{i \in \mathbb{Z}_0}$  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:

$$K[X] = \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{N}_0, a_i \in K\}$$

$$= (a_0 + a_1x + \dots + a_nx^n) + (b_0 + b_1x + \dots + b_nx^n)$$

$$= (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + b_nx^n$$

Without loss of generality

Instead of a unit vector  $e_i$  the formal polynomial  $x^i$  occurs.

$$\Rightarrow (x^n)_{n \geq 0} \text{ is a basis of } K[X]$$

$$\deg p(x) = \max \{i \mid a_i \neq 0\} = n$$

is the degree of the polynomial.

$$p(x) = a_0 + q_1x + q_2x^2 + \dots a_nx^n$$

$$\deg 0 := -\infty$$

Every formal polynomial  $p(x) = a_0 + a_1x + \dots + a_nx^n$  induces a polynomial function

$$K \rightarrow K$$

$$\xi \mapsto a_0 + a_1\xi + \dots + a_n\xi^n \in K$$

If  $K$  has infinite cardinality, then the polynomial function defines the formal polynomial uniquely.

**Theorem 31. Attention!** This does not hold if the field is finite!

*Proof.* There are  $|K^K| = |K|^{|K|}$  different functions of  $K \rightarrow K$ . For example for  $K = \mathbb{Z}_2$  there are  $2^2$  functions in  $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ .

$$\mathbb{Z}_2[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{N}_0, a_n \in \mathbb{Z}_2\}$$

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).  $\square$

Does  $K^{\aleph_0}$  have a basis? Does every vector space have a basis?

**Theorem 32.** *Every vector space has a basis.*

*Proof.* **Case 1**  $V$  is generated finitely.

Let  $(v_1, \dots, v_n)$  be a finite generating system. If  $(v_1, \dots, v_n)$  is linear independent, we are done. Otherwise we already know that (by a previous theorem)

$$\bigvee_{k \in \{1, \dots, n\}} v_k \in L(v_1, \dots, \hat{v}_k, v_n) \\ \Rightarrow L(v_1, \dots, v_n) = L(v_1, \dots, \hat{v}_k, \dots, v_n) = V$$

- 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 12.** *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 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 is 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 13.** *The axiom of choice is TODO content incomplete/incorrect of the other axioms of Zermelo-Fraenkel set theory (ZF). If ZF is contradiction-free, so is  $ZF + AC$ .*

**Theorem 33.** *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  $B$ :

$$\bigwedge_{v \in V} \bigvee_n \bigvee_{i_1, \dots, i_n} \bigvee_{\lambda_1, \dots, \lambda_n} v = \lambda_1 v_{i_1, 1} + \dots + \lambda_n b_{i_n}$$

3.  $B$  is a maximal linear independent family.
4.  $B$  is a minimal generating system.

**Remark 14.** *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 33.

We use circular reasoning (dt. Zirkelschluss).

1 → 2 Basis ⇒  $L(B) = V$

Let  $v \in V \Rightarrow \bigvee_{\lambda_1, \dots, \lambda_n} v = \lambda_1 b_{i_1} + \dots + \lambda_n b_{i_n}$ .

We need to show uniqueness of representation: Assume  $v = \mu_1 b_{j_1} + \mu_2 b_{j_2} + \dots + \mu_m b_{j_m}$ . We fill up the vectors such that  $m = n$  and  $j_k = i_k$ .

Therefore

$$v = \mu_1 \cdot b_{j_1} + \dots + \mu_n b_{i_n}$$

$$\Rightarrow 0 = v - v = \lambda_1 b_{i_1} + \dots + \lambda_n b_{i_n} - (\mu_1 b_{i_1} + \dots + \mu_n b_{i_n}) = (\lambda_1 - \mu_1) b_{i_1} + \dots + (\lambda_n - \mu_n) b_{i_n}$$

$$(b_i) \text{ are linear independent} \Rightarrow \bigwedge_{k \in \{1, \dots, n\}} \lambda_k = \mu_k.$$

2 → 1 From 2 it follows that  $L(B) = V$ . Show that it is linear independent.

Let  $\lambda_1 + b_{i_1} + \dots + \lambda_n b_{i_n} = 0$ . Condition 2 for the vector  $v = 0$  implies that it is the same representation like  $0b_{i_1} + \dots + 0b_{i_n} = 0$ . 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 → 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  $v = \lambda_1 b_{i_1} + \dots + \lambda_n b_{i_n}$ . Therefore  $\lambda_1 b_{i_1} + \lambda_2 b_{i_2} + \dots + \lambda_n b_{i_n} - v = 0$ . 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 → 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.

$$\Rightarrow \bigvee_{\lambda_0, \lambda_1, \dots, \lambda_n} \bigvee_{b_{i_1}, \dots, b_{i_n} \in B} \lambda_0 v + \lambda_1 b_{i_1} + \dots + \lambda_n b_{i_n} = 0$$

But not all  $\lambda_0, \dots, \lambda_n$  can be 0. If it would hold that  $\lambda_0 = 0$ , then  $\lambda_1 b_{i_1} + \dots + \lambda_n b_{i_n} = 0$ .

$$\Rightarrow \lambda_i = 0 \text{ because } B \text{ is linear independent}$$

Therefore  $\lambda_0$  cannot be 0.

$\lambda_i \neq 0 \Rightarrow$  division allowed.

$$\lambda_0 \cdot v = -\lambda_1 b_{i_1} - \dots - \lambda_n b_{i_n}$$

$$\Rightarrow v = -\frac{\lambda_1}{\lambda_0} b_{i_1} - \dots - \frac{\lambda_n}{\lambda_0} b_{i_n} \in L(B)$$

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

$$L(B \setminus \{b_{i_0}\}) = V$$

$$\Rightarrow b_{i_0} \in L(B \setminus \{b_{i_0}\})$$

$$\Rightarrow \bigvee_{\lambda_1, \dots, \lambda_n} \bigvee_{i_1, \dots, i_n \neq i_0} = \lambda_1 b_{i_1} + \dots + \lambda_n b_{i_n}$$

$$\Rightarrow \lambda_1 b_{i_1} + \dots + \lambda_n b_{i_n} - b_{i_0} = 0$$

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.

$$\begin{aligned}\lambda_1 b_1 + \dots + \lambda_n b_n &= 0 \\ \Rightarrow \lambda_i &= 0\end{aligned}$$

$v = 0$  has a unique representation as linear combination of the basis  $B$ .

**Theorem 34.** Let  $V$  be a vector space. Let  $B$  be a basis  $(b_i)_{i \in I} \subseteq V$ . Then the following statements are equivalent:

1.  $B$  is a basis.
2. Every  $v \in V$  has a unique representation as linear combination of  $B$ .
3.  $B$  is a maximal linear independent family.
4.  $B$  is a minimal generating system.

*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

$$\lambda_1 b_{i_1} + \dots + \lambda_n b_{i_n} = 0$$

There exists some  $k$  such that  $\lambda_k \neq 0$ .

$$\Rightarrow \lambda_k \cdot b_{i_k} = - \sum_{j \neq k} \lambda_j b_{i_j}$$

$$b_{i_k} = - \sum_{j \neq k} \frac{\lambda_j}{\lambda_k} b_{i_j}$$

$$\Rightarrow b_{i_k} \in L(B \setminus \{b_{i_k}\})$$

$$L(B \setminus \{b_{i_k}\}) = L(B \setminus \{b_{i_k}\}) \cup \{b_{i_k}\} = L(B) = V$$

$B \setminus \{b_{i_k}\}$  is also a generating system, but smaller. So  $B$  is not minimal.  $\square$

How can we construct/find bases?

**Theorem 35** (Exchange lemma). Let  $B = (b_1, \dots, b_n)$  be basis in vector space  $V$ . Let  $v \in V \setminus \{0\}$  with  $v \neq 0$ . Let

$$v = \sum_{i=1}^n \lambda_i \cdot b_i$$

If  $\lambda_k \neq 0$  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  $\mu_1, \dots, \mu_k \in K$ .

$$\mu_1 b_1 + \dots + \mu_{k-1} b_{k-1} + \mu_k v + \mu_{k+1} b_{k+1} + \dots + \mu_n b_n = 0$$

Show that all  $\mu_i = 0$ .

$$\begin{aligned}0 &= \sum_{i \neq k} \mu_i b_i + \mu_k v \\ &= \sum_{i \neq k} \mu_i b_i + \mu_k \left( \sum_{i=1}^n \lambda_i \cdot b_i \right) \\ &= \sum_{i \neq k} \mu_i b_i + \sum_{i \neq k} \mu_k \lambda_i b_i + \mu_k \lambda_k b_k \\ &= \sum_{j \neq k} (\mu_k + \mu_k \lambda_i) b_i + \mu_k \lambda_k b_k \\ &= \text{is linear combination of } B\end{aligned}$$

$$\mu_k \cdot \lambda_k = 0 \xrightarrow{\lambda_k \neq 0} \mu_k = 0$$

$$\Rightarrow \mu_i + \mu_k \lambda_i = 0 \Rightarrow \mu_i = 0 \text{ for all } i \neq k$$

$$\Rightarrow \forall \mu_i = 0$$

2.  $L(B') = V$ . It suffices to show that  $b_k \in L(B')$ .

Then it holds that

$$\begin{aligned} L(B') &= L(B' \cup \{b_k\}) \\ B' \cup \{b_k\} &= (B \setminus \{b_k\}) \cup \{b_k\} \cup \{v\} = B \cup \{v\} \\ &\Rightarrow L(B \cup \{v\}) \supseteq L(B) = V \quad \checkmark \\ v &= \sum_{i=1}^n \lambda_i b_i = \sum_{i \neq k} \lambda_i b_i + \lambda_k b_k \Rightarrow \lambda_k b_k = v - \sum_{i \neq k} \lambda_i b_i \\ \lambda_k \neq 0 &\Rightarrow b_k = \frac{1}{\lambda_k} v - \sum_{i \neq k} \frac{\lambda_i}{\lambda_k} b_i \in L(B') \end{aligned}$$

□

**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  $(v_1, \dots, v_n) \subseteq V$  be linear independent.*

*Then it holds that*

- $r \leq n$
- 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  $n \geq 1 = r = 1 \quad \checkmark$ .
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 it follows that  $(v_1, b_1, \dots, b_{k-1}, b_{k+1}, \dots, b_n)$  is a basis.

**induction step**  $r \rightarrow r + 1$

Let  $v_1, \dots, v_{r+1}$  be linear independent.

$\Rightarrow v_1, \dots, v_r$  is also linear independent

induction hypothesis  $\Rightarrow \bigvee_{j_1, \dots, j_{n-r}} (v_1, \dots, v_r, b_{j_1}, \dots, b_{j_{n-r}})$  is a basis

1.  $r \leq n$

We need to show that  $r + 1 \leq n$ .

We already know  $r \leq n$  and we need to exclude that  $r = n$ . In that case  $r + 1 \leq n$  holds (with  $r < n$ ).

Assume

$r = n \Rightarrow (v_1, \dots, v_r)$  is a basis

$\Rightarrow (v_1, \dots, v_r)$  is maximal linear independent family

$\Rightarrow (v_1, \dots, v_{r+1})$  is not linear independent

This is a contradiction to our assumption. So  $r < n \Rightarrow r + 1 \leq n$ .

2. We apply the exchange lemma to  $v_{r+1}$  and the basis  $(v_1, \dots, v_r, b_{i_1}, \dots, b_{i_{n-r}})$ . Let  $V_{r+1} = \sum_{i=1}^r \lambda_i v_i + \sum_{j=1}^{n-r} \mu_j b_{i_j}$  so either  $\lambda_i$  or some  $\mu_j \neq 0$ .

**Claim.** At least one  $\mu_j \neq 0$ . Otherwise  $v_1, \dots, v_{r+1}$  is not linear independent because otherwise  $v_{r+1} = \sum_{i=1}^r \lambda_i v_i$  would be linear combination of other  $v_i$ s.

Let  $\mu_k \neq 0$ . Then we have a new basis  $(v_1, \dots, v_{r+1}, b_{i_1}, \dots, b_{i_{k-1}}, b_{i_{k+1}}, \dots, b_{i_{n-r}})$ . So we remove  $b_{i_k}$ .

□

**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

$$\bigvee_{j_1, \dots, j_{n-r}} (b'_1, \dots, b'_r, b_{j_1}, \dots, b_{j_{n-r}}) \text{ is a basis}$$

$(b'_1, \dots, b'_r)$  is maximal linear independent family

$(b'_1, \dots, b'_r, b_{j_1}, \dots, b_{j_{n-r}})$  is also linear independent

$$\Rightarrow n - r = 0 \Rightarrow n = r$$

**Remark 15.**  $V$  has a basis.  $V$  is finitely generated.

*Proof.*  $\Rightarrow$  follows immediately.

$\Leftarrow$  use negative vectors until linear independent family remains.

**Definition 22.** 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.**

$$\dim R^3 = 3$$

$$\dim \emptyset = 0$$

$$\dim K^n = n$$

$$\dim K^m = |M|$$

$$\dim K[x] = \infty \dots \text{vector space of polynomials}$$

Remember that  $K[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{N} \text{ arbitrary}, a_i \in K\}$ .

$$\Rightarrow (x^n)_{n \in \mathbb{N}} \text{ is basis} \Rightarrow \dim K[x] = \infty$$

**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  $U$ .

$\Rightarrow (u_1, \dots, u_n)$  is linear independent in  $V$

$\Rightarrow (u_1, \dots, u_n)$  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 23.** 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  $\lambda_i$  are called coordinates of  $v$  with respect to  $B$ .

$$(v)_B := \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

is called coordinates vector of  $v$ .

The mapping

$$\Phi_B : V \rightarrow K^n$$

$$v \mapsto \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix}$$

is called coordinate mapping.

It follows immediately that  $\Phi_B$  is bijective.

**Example 28.**

$$V = R_3[x] = \{a_0 + a_1x + a_2x^2 + a_3x^3 \mid a_i \in \mathbb{R}\}$$

$$B = (1+x, 1-x, 1+x+x^2, x^2+x^3) \text{ is basis of } V$$

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).

$$\lambda_1(1+x) + \lambda_2(1-x) + \lambda_3(1+x+x^2) + \lambda_4(x^2+x^3) = 0$$

$$(\lambda_1 + \lambda_2 + \lambda_3) \cdot 1 + (\lambda_1 - \lambda_2 + \lambda_3)x + (\lambda_3 + \lambda_4)x^2 + \lambda_4x^3 = 0 \text{ (zero polynomial!!)}$$

$$\text{coefficient comparison} \Rightarrow \lambda_1 + \lambda_2 + \lambda_3 = 0$$

$$\Rightarrow \lambda_1 - \lambda_2 + \lambda_3 = 0$$

$$\Rightarrow \lambda_3 + \lambda_4 = 0$$

$$\Rightarrow \lambda_4 = 0$$

$$\text{coefficient comparison} \Rightarrow \lambda_1 + \lambda_2 = 0$$

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

$$\text{coefficient comparison} \Rightarrow 2\lambda_1 = 0$$

$$\Rightarrow \lambda_2 = 0$$

$\Rightarrow B$  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,

$$p(x) = \lambda_1(1+x) + \lambda_2(1-x) + \lambda_3(1+x+x^2) + \lambda_4(x^2+x^3)$$

$$= (\lambda_1 + \lambda_2 + \lambda_3) \cdot 1 + (\lambda_1 - \lambda_2 + \lambda_3) \cdot x + (\lambda_3 + \lambda_4)x^2 + \lambda_4x^3$$

Using coefficient comparison we get

$$\lambda_1 + \lambda_2 + \lambda_3 = 3$$

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

$$\lambda_3 + \lambda_4 = -3$$

$$\lambda_4 = 1$$

$$\lambda_3 = -3 - \lambda_4 = -4$$

$$\lambda_1 + \lambda_2 = 3 - (-4) = 7$$

$$\lambda_1 - \lambda_2 = 1 - (-4) = 5$$

$$2\lambda_1 = 12 \Rightarrow \lambda_1 = 6$$

$$\lambda_2 = 7 - \lambda_1 = 1$$

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:

$$\Phi_B(v) = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} \quad \Phi_B(w) = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix}$$

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  $B$ .  $v_1, \dots, v_k \in V$  are linear independent.

$$\Leftrightarrow \Phi_B(v_1) \dots \Phi_B(v_k) \text{ are linear independent in } K^n$$

## 7 Construction of vector spaces

**Remark 16.** We have already seen  $U, W \subseteq \text{subspaces} \Rightarrow U \cap W$  is subspace, but not  $U \cup W$ .

**Definition 24.**  $V$  is a vector space.  $U, W \subseteq V$  are subspaces. Then  $[U \cup W]$  is the sum of subspaces  $U$  and  $W$

$$=: U + W = \bigcap \{z \mid z \subseteq V, U \subseteq Z, W \subseteq Z\}$$

$$= L(U \cup W) = \left\{ \sum \lambda_i u_i + \sum \mu_j w_j \mid u_i \in U, w_j \in W \right\}$$

**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  $V = \mathbb{R}^4$ .

$$U = \left\{ \begin{pmatrix} \xi \\ \eta \\ \xi \\ \eta \end{pmatrix} \mid \xi, \eta \in \mathbb{R} \right\}$$

$$W = \left\{ \begin{pmatrix} \xi \\ \xi \\ \eta \\ \eta \end{pmatrix} \mid \xi, \eta \in \mathbb{R} \right\}$$

$$U + W = ?$$

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

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

$$U = L \left( \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right) = \left\{ \xi \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \eta \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \mid \xi, \eta \in \mathbb{R} \right\}$$

$$W = L \left( \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \right) = \left\{ \xi \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \eta \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \mid \xi, \eta \in \mathbb{R} \right\}$$

So... und jetzt ist das Alphabet aus! (Franz Lehner)

$$U + W = \{u + w \mid u \in U, w \in W\}$$

$$= \left\{ \xi \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \eta \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} + \chi \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + w \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \mid \xi, \eta, \chi, w \right\}$$

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

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

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:

$$\lambda \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} + \gamma \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} \lambda + \gamma \\ \mu + \gamma \\ \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \lambda = 0, \mu = 0 \Rightarrow \gamma = 0$$

$$\left( \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \right) \text{ is linear independent and basis of } U + W$$

$$\Rightarrow \dim(U + W) = 3$$

$$\dim U = 2 \quad \dim W = 2$$

**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.**

$$U \cap W = \left\{ \begin{pmatrix} \xi \\ \xi \\ \xi \\ \xi \end{pmatrix} \mid \xi \in \mathbb{R} \right\}$$

$$\dim(U \cap W) = 1$$

$$\text{Basis is } \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

$$\dim(U + W) = 2 + 2 - 1$$

**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  $U$  states 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  $v \in U \cap L(w_1, \dots, w_q) \subseteq U \cap W \Rightarrow v \in U \wedge v \in L(w_1, \dots, w_q)$ .

$$\Rightarrow \bigvee_{\lambda_1, \dots, \lambda_r, \mu_1, \dots, \mu_p} v = \sum_{i=1}^r \lambda_i v_i + \sum_{j=1}^p \mu_j u_j$$

$$\Rightarrow \bigvee_{\mu_1, \dots, \mu_q} v = \sum_{k=1}^q \mu_k w_k$$

$$v \in U \cap W \Rightarrow \bigvee_{\xi_1, \dots, \xi_r} v = \sum_{l=1}^r \xi_l v_l$$

Consider  $v$  in  $W$ :

$$0 = v - v = \sum_{k=1}^q \mu_k w_k - \sum_{l=1}^r \xi_l v_l$$

$(v_1, \dots, v_r, w_1, \dots, w_q)$  is basis of  $W$

$\Rightarrow$  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  $\lambda_i$ , all  $\mu_j$  and all  $\mu_k$  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  $\mu_1 = \dots = \mu_p = 0$ .

$(\mu_1, \dots, \mu_r, w_1, \dots, w_q)$  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.  $\square$

**Remark 17.** 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 25.** 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  $U \oplus W$ ).

**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  $v = 0$ .

$$u, u' \in U \quad w, w' \in W$$

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  $v = 0$ . □



## German keywords

Austauschlemma von Steinitz, 95  
Austauschlemma, 93  
Auswahlaxiom (axiom of choice), 89  
Dimension (Vektorraum), 97  
Einbettung, 55  
Endlich dimensional, 97  
Endomorphismus, 55  
Epimorphismus, 55  
Gruppenhomomorphismus, 55  
Hausdorff-Banach-Tarski Paradoxon, 89  
Homomorphismus, 55  
Isomorphismus, 55  
Koordinates eines Vektorraums, 99  
Siebformel, 107  
Unendlich dimensional, 97  
Vektorraumdimension, 97  
  
Minimales Erzeugendensystem, 89  
  
Zermelo-Fraenkel Mengenlehre (ZF), 89

## English keywords

Axiom of choice, 89

Coordinates, 99

Dimension of a vector space, 97

Embedding, 55

Endomorphism, 55

Epimorphism, 55

Exchange lemma, 93

Field embedding, 55

Finitely dimensional, 97

Group homomorphism, 55

Hausdorff-Banach-Tarski paradoxon, 89

Homomorphism, 55

Inclusion-exclusion principle, 107

Infinitely dimensional, 97

Isomorphism, 55

Minimal generating system, 89

Steinitz exchange lemma, 95

Zermelo-Fraenkel set theory (ZF), 89