Lineare Algebra und Diskrete Strukturen

Jan Pangritz

30. Januar 2017

Inhaltsverzeichnis

0.1 Grundlagen

0.1.1 Begriffe

1. Axiom := Ein Axiom ist ein Grundsatz einer Theorie, einer Wissenschaft oder eines axiomischen Systems, der innerhalb dieses Systems nicht begründet oder deduktiv abgeleitet werden kann.
2. Satz := Ein Satz fasst eine wichtige logische korrekte Aussage zusammen.
3. Beweis := Der Beweis klärt auf, warum eine Aussage korrekt ist. Ohne Beweis bleibt eine Formulierung nur eine Behauptung oder Hypothese.
4. Lemma := Ein Lemma oder Hilfssatz ist in der Regel ein Satz von minderer Bedeutung.
5. Korollar := Eine direkte Folgerung aus dem Ergebnis des Satzes, aber ohne Beweis.
6. Definition := Sinnvolle, vollständige, präzise und nicht reduzierbare Festlegung eines Begriffes.
7. Zuweisung := Bei der asymmetrischen Zuweisung "J := Jan"wird der Doppelpunktseite die andere Seite zugewiesen; es ist eine Abkürzung. Beim symmetrischen Gleichsetzen "A = B" handelt es sich um eine Aussage.

1 Aussagenlogik

Beispiel

1. $A_1 := [22 + 9 = 30]$
2. $A_2 := [7 > 4]$
3. $A_3 :=$ [Mathe ist klasse]
4. $\neg A :=$ nicht A
5. $A \wedge B :=$ A und B
6. $A \vee B :=$ A oder B
7. $A \Rightarrow B :=$ Aus A folgt B
8. A⇔B := A gilt genau dann, wenn B gilt

   Eine Aussage ist ein sprachliches Gebilde von dem wir eindeutig entscheiden können ob es wahr oder falsch ist (W/F, 1/0)

   Keine Aussage: A_7= [Diese Aussage ist falsch.]

Definition 1.2

Seien A und B zwei Aussagen. Der Wahrheitswert der Aussagen:
$\neg A, A \wedge B, A \vee B, A \Rightarrow B, A \Leftrightarrow B$ und $A = B$
ist durch die folgende <u>Wahrheitstabelle</u> festgelegt:

A	B	¬A	¬B	A∧B	A∨B	A ⇒B	A⇔B
0	0	1	1	0	0	1	1
0	1	1	0	0	1	1	0
1	0	0	1	0	1	0	0
1	1	0	0	1	1	1	1

Bemerkung

1. Die Definition ist induktiv. Das heißt wenn A, B und C Aussagen sind, dann ist auch $(A \vee B) \vee C$ eine Aussage
2. Klammerung regelt die Reihenfolge. Die Stärke der Bindungen nimmt mit nachstehender Reihenfolge ab: $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$

1.1 Tautologien

Definition 1.3

Eine Aussage, die unabhängig von den Wahrheitswerten der in ihr enthaltenen Aussagen stets wahr ist, heißt allgemeingültig oder Tautologie.

Beispiel

$B \vee \neg B$	B	$\neg B$
1	0	1
1	1	0

Satz 1.4

Seien A,B und C Aussagen, dann sind folgende Aussagen Tautologien:

1. Kettenschluss $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$
2. Induktiver Beweis $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
3. Beweis der Äquivalenz $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$

Beweis 1.5

A	B	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

□

Definition 1.6

Eine natürliche Zahl heißt gerade, falls es eine natürliche Zahl k gibt, sodass $n = 2k$

Definition 1.7

Sei n eine natürliche Zahl. Ist n gerade, so ist n^2 auch gerade.

Beweis 1.8

1. $A_1 = n$ ist gerade
2. $A_2 = 2$ teilt n
3. $A_3 = 2$ teilt n^2
4. $A_4 = 2\ n^2$ ist gerade
5. $A_5 := A_1 \Leftrightarrow A_2$ (1,2 Def 1.4)
6. $A_6 := A_2 \Leftrightarrow A_3$ (2,3 $(2k)^2 = 2 * (2k^2)$)
7. $A_7 := A_3 \Leftrightarrow A_4$ (3,4 Def 1.4)
8. $A_8 := A_1 \Leftrightarrow A_3$ (5,6 Kettenschluss)
9. $A_9 := A_1 \Leftrightarrow A_4$ (7,8 Kettenschluss) □

Satz 1.9

Sei n eine natürlich Zahl. Ist n^2 gerade , so ist n gerade.

Beweis induktiv

Angenommen n ist ungerade, dann existiert eine Zahl mit $n = 2m + 1$ und $n^2 = (m + 1)^2$

$4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$ also ist n^2 ungerade. □

Satz 1.10

Sei n eine natürliche Zahl. Die Zahl n ist ungerade genau dann, wenn n^2 ungerade ist.

Lemma

A,B und C sind Aussagen genau dann, wenn gilt

1.1.1 Assoziativ-Gesetz

1. $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$
2. $(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$

1.1.2 Distributivgesetz

3 $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$

4 $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$

1.1.3 De Morgansche Regel

5 $\neg(A \wedge B) \Leftrightarrow (\neg A) \vee (\neg B)$

6 $\neg(A \vee B) \Leftrightarrow (\neg A) \wedge (\neg B)$

2 Mengenlehre

2.1 Mengen

Eine formale Beschreibung aller Mengen ist sehr schwer, daher nutzen wir die Charakterisierung von Cantor: "Eine Menge ist eine Zusammenfassung bestimmter, wohl unterschiedener Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen. Die Objekte, die hier zusammengefasst werden, werden auch Elemente genannt. "

Schreibweisen

- Eine Menge mit Elementen $m_1, m_2, ..., m_n : M := \{m_1, m_2, ..., m_n\}$
- m ist Element von M (m ist in M enthalten) : $m \in M$
- Ein Element n ist nicht Element von M $(n \notin M) := \neg(n \in M)$
- $m \in M$ für $i = 1, 2, ..., n$

Achtung!

- Ein Karton voller Tüten enthält keine Gummibärchen, sondern nur Tüten, die Gummibären sind in den Tüten.
- Ein Kasten voller leerer Bierflaschen ist voll.
- Die Russel'sche Antinomie, Cantor's Problem "Dieser Satz enthelt drei Fähler" Wahr oder Falsch? - Nicht entscheidbar!
- Analoges Beispiel:

  $M : \{N : N \notin N\}$

  Hier folgt $(M \in M) \Leftrightarrow (M \notin M)$.
- " Der Dorfbarbier rasiert alle Männer des Dorfes, die sich nicht selber rasieren."
  Wer rasiert den Barbier?

  Dazu b := Barbier, M:= {Männer, die sich nicht selber rasieren}.
  Ob b ∈ M ist nicht entscheidbar.

Beispiel 1.11

1. $\mathbb{N} := \{1, 2, 3, ...\}$ Natürliche Zahlen
2. $\mathbb{N}_0 := \{0, 1, 2, ..\}$ Natürliche Zahlen einschließlich 0
3. $\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\}$ Ganze Zahlen
4. $\mathbb{Q} := \{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N}\}$ Rationale Zahlen
5. $\mathbb{R}$:= Reelle Zahlen.
6. $\mathbb{C}$:= Komplexe Zahlen. Fundamentale Rollen bei Drehungen (Strömen) und bei Lösungen algebraischer Gleichungen z.B. hat x^2 Nullstellen?, Umfang eines Kreises.

2.2 Aufzählungen und Bereiche

$A := \{\sqrt{2}, \sqrt{3}\}, B :=$ { Cäsar,Cleopatra }

Eine Menge kann Mengen enthalten:
$M : \{A, B\} = \{\{\sqrt{2}, \sqrt{3}\},$ { Cäsar,Cleopatra }}

Achtung

$\sqrt{2} \notin M$ aber $(\sqrt{2} \in A) \wedge (A \in M)$

Wie können eine Aussage von einer Variablen abhängig machen: z.B.
$A(x) := [x \leq 3]$

Für $x \in \mathbb{N}$ ist also die Menge L aller x, für die $A(x)$ wahr ist.
$L := \{x \in \mathbb{N} : A(x)\} = \{1, 2, 3\}$

Definition 1.12 (Quantoren)

Sei M eine Menge, und $A(x)$ eine von $x \in M$ abhängige Aussage.

Wir definieren die Quantoren, $\forall, \exists, \exists!$, über den Wahrheitswert von $A(x)$

1. $(\forall x \in M : A(x))$ ist wahr $\Leftrightarrow$ für alle $x \in M$ ist $A(x)$ wahr
2. $(\exists x \in M : A(x))$ ist wahr $\Leftrightarrow$ gibt es ein $x \in M$ so dass $A(x)$ wahr ist
3. $(\exists! x \in M : A(x))$ ist wahr $\Leftrightarrow$ es gibt genau ein $x \in M$ so dass $A(x)$ wahr ist

   $[A(x) = 1 \wedge A(y) = 1 \Rightarrow x = y]$

Beispiel 1.13

Sei M := $\{1, 2, 3, 4, 5\}$

1. $\forall x \in M : x \leq 5$
2. $\exists x \in M : x \leq 3$
3. $\exists! x \in M : x \leq 1$

Bemerkung

1. $\neg[\forall x \in M : A(x)] \Leftrightarrow [\exists x \in M : \neg A(x)]$
   $\neg[\exists x \in M : A(x)] \Leftrightarrow [\forall x \in M : \neg A(x)]$
2. Die Quantoren sind nicht kommutativ. $S := \{\text{Studis}\}, B := \{\text{Biere}\}$, dann ist:
   "Es gibt ein Bier für alle Studis" i.a. nicht dasselbe wie "Für alle Studis gibt es ein Bier"
   $[\exists b \in B : \forall s \in S, \ldots] \neq [\forall s \in S \exists b \in B \ldots]$
3. $[\exists! x \in M : A(x)] \Leftrightarrow [\forall x \in M : A(x) \wedge (A(x) = A(y) \Rightarrow x = y)]$

Definition 1.14

1. M ist Teilmenge von N: $(M \subseteq N) := (\forall x \in M : x \in N)$
2. M ist echte Teilmenge von N: $(M \subset N) \wedge (\exists x \in M : x \notin N)$
3. M und N sind gleich : $(M = N) := [(M \subseteq N) \wedge (N \subseteq M)]$
4. $|M|$ bezeichnet die Anzahl der Elemente von M und heißt Mächtigkeit von M
5. $\varnothing$ bezeichnet die leere Menge.
6. Die Potenzmenge $P(N)$ ist die Menge aller Teilmengen von N
   $P(N) = \{M : M \subseteq N\}$

Beispiel 1.15

1. Offensichtlich gilt $|\varnothing| = 0$
2. Um die Teilmengen Bezeichnung $M \subseteq N$ nachweisen, wird für ein beliebiges $x \in M$ gezeigt, dass $x \in N : x \in M \Rightarrow x \in N$.
3. Für beliebige Mengen M gilt $\varnothing \subseteq M \wedge ; M \subseteq M$
4. Abkürzend schreiben wir $[A \subseteq B \subseteq C] \leftarrow [(A \subseteq B) \wedge (B \subseteq C)]$
5. Für die Zahlenbereiche gilt: $\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
6. Es kommt nicht auf die Reihenfolge oder Wiederholung der Elemente an:
   $\{1, 2, 3\} = \{2, 1, 3\} = \{1, 1, 2, 2, 3, 3\}$
7. Für die Potenzmenge $P(\{1, 2, 3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$
   Offensichtlich gilt $1 \in \{1, 2, 3\}$ aber
   $1 \notin P(\{1, 2, 3\}), \{1\} \in P(\{1, 2, 3\}), \{1\} \neq \{\{1\}\}$
8. $M := \{\varnothing\}; P(M) = \{\varnothing, \{\varnothing\}\}$
9. In der Literatur auch $\subset$ für $\subseteq$ und $\supset$ für $\supseteq$.

2.3 Mengenalgebra

Definition 1.16

Seien M,N Mengen. Folgende Mengen werden definiert.

1. Vereinigung von M und N: $M \cup N := \{x : x \in M \vee x \in N\}$
2. Durchschnitt von M und N: $M \cap N := \{x : x \in M \wedge x \in N\}$
3. Differenz von M und N: $M \setminus N := \{x : x \in M \wedge x \notin N\}$

4. Komplement von M: $\overline{M} := \{x : x \notin M\}$
5. Komplement von M in X: $\overline{M^X} := \{x \in X : x \notin M\}$
6. M und N heißen Disjunkt, falls $M \cap N = \varnothing$

   Hilfreich: Assoziation $\cup$ und $\vee$ bzw. $\cap$ und $\wedge$.

Lemma 1.17

Seien L,M,N Mengen. Es gilt:

Assoziativgesetz:

1. $(L \cap M) \cap N = L \cap (M \cap N)$
2. $(L \cup M) \cup N = L \cup (M \cup N)$

Distributivgesetze:

3. $L \cap (M \cup N) = (L \cap M) \cup (L \cap N)$
4. $L \cup (M \cap N) = (L \cup M) \cap (L \cup N)$

De Morgansche Regeln:

5. $\overline{(M \cap N)} = \overline{M} \cup \overline{N}$
6. $\overline{(M \cup N)} = \overline{M} \cap \overline{N}$

Kompliment : $\overline{(\overline{M})} = M$

Beweis

Wir zeigen exemplarisch 3, der Rest als Übung:

1. $L \cap (M \cup N) = \{x : x \in L \cap (M \cup N)\}$
   $= \{x : (x \in L) \wedge (x \in M \cup N)\}$
   $= \{x : (x \in L \wedge (x \in M \vee x \in N)\}$
   $\overset{Lemma 1.10}{=} \{x : (x \in L \wedge x \in M) \vee (x \in L \wedge x \in N)\}$
   $= \{x : x \in (L \cap M) \vee x \in (L \cap N)\}$
   $= \{x : x \in (L \cap M) \vee (L \cap N]\} = (L \cap M) \cup (L \cap N)$ □

2.3.1 Vereinigung und Durchschnitt von Mengen

Sei X eine Menge von Mengen, $M \in X$ eine Menge.

1. $\bigcup_x = \bigcup_{M \in X} M = \{x : \exists M \in X : x \in M\}$
2. $\bigcap_x = \bigcap_{M \in X} M = \{x : \forall M \in X : x \in M\}$

3. Kann man die Mengen abzählen(endlich), $X = \{M_1, M_2, ..., M_n\}$ folgt
$\bigcup_x = \bigcup\limits_{i=1}^{n} M_i = M_1 \cup M_2 \cup ... \cup M_n$

Beispiel 1.18

Sei $M_1 = \{1, 2, 3\}, M_2\{1, 4\}, M_3\{1, 5\}, I = \{1, 2, 3\}, X = \{M_1, M_2, M_3\} = \{M_i : i \in I\}$
$\bigcup_x = \bigcup_{i \in I} M_i = (M_1 \cup M_2) \cup M_3 = \{1, 2, 3, 4, 5\}$
$\bigcap_x = \bigcap_{i \in I} M_i = M_1 \cap (M_2 \cap M_3) = \{1\}$

Satz 1.19 Verallgemeinerte De Morgansche Regeln

Für eine Menge X von Mengen gilt:

1. $\overline{\bigcup_{M \in X}} = \bigcup_{M \in X} \overline{M}$
2. $\overline{\bigcap_{M \in X}} = \bigcap_{M \in X} \overline{M}$

Beweis zu 1

$\overline{\bigcup_{M \in X} M} = \{x : x \notin \bigcup_{M \in X} M\} =$
$= \{x : \forall M \in X : x \notin M\}$
$= \{x : \forall M \in X : x \in \overline{M}\}$
$= \{x : x \in \bigcap_{M \in X} \overline{M}\}$
$= \bigcap_{M \in X} \overline{M}$ □

Definition 1.20

Eine Menge X ist von Mengen heißt paarweise disjunkt(pwd.),

wenn gilt:

$\forall M, N \in X : M \cap N \neq \varnothing \Rightarrow M = N$

Definition 1.21

Eine Menge X von Mengen heißt eine Partition einer Menge P, falls

1. $\forall M \in X : M \neq \varnothing \land M \subseteq P$
2. Die Menge X ist pwd.
3. $P = \bigcup_X$

Beispiel 1.22

$X = \{G, U\}$ ist Partition von $\mathbb{N}_0$

Beispiel 1.23

Veranschaulichen wir Partition durch Venn Diagramm:

Definition 1.24

Seien M,N Mengen. Die Menge

$M \times N = \{(a, b) : a \in M \land b \in N\}$

heißt das kartesische Produkt von M und N

Die Elemente(a,b) heißen auch (geordnete) Paare oder 2- Tupel. Wir definieren weiter:

$\varnothing \times N := \varnothing$

$M \times \varnothing := \varnothing$

$[(a, b) = (c, d)] := [a = c \land b = d]$

Achtung : $(a \neq b) \Rightarrow (a, b) \neq (b, a)$

Beispiel 1.25

$M = \{1, 2, 3\}$
$N = \{x, y\}$
$M \times N = \{(1, x), (2, x), (3, x), (1, y), (2, y), (3, y)\}$
$N \times M = \{(x, 1), (y, 1), (x, 2), (y, 2), (x, 3), (y, 3)\}$

Satz 1.26

Seien M,N,L,O Mengen: Dann gilt

1. $(L \cap M) \times N = (L \times N) \cap (M \times N)$,
2. $L \times (M \cap N) = (L \times N) \cap (M \times N)$,
3. $(L \cup M) \times N = (L \times N) \cup (M \times N)$,
4. $L \times (M \cup N) = (L \times M) \cup (L \times N)$,
5. $(L \times M) \cap (N \times O) = (L \cap N) \times (M \cap O)$
6. $(L \times M) \cup (N \times O) \subseteq (L \cup N) \times (M \cup O)$
7. $\overline{L} \times \overline{M} \subseteq \overline{L \times M}$

Beweis

Hier exemplarisch 1, der Rest als Übung.

$(L \cap M) \times N = \{(x, y) : x \in L \cap M \wedge y \in N\}$
$= \{(x, y) : x \in L \wedge x \in M \wedge y \in N\}$
$= \{(x, y) : (x \in L \wedge y \in N) \wedge (x \in M \wedge y \in N)\}$
$= \{(x, y) : (x, y) \in L \times N \wedge (x, y) \in M \times N\}$
$= \{(x, y) : (x, y) \in (L \times N) \cap (M \times N)\} = (L \times N) \cap (M \times N)$ □

Definition 1.27

Seien $M_1, ..., M_n$ Mengen. Die Menge $M_1 \times M_2 \times ... \times M_n := \{(x_1, x_2, ..., x_n) : \forall i = 1, 2, ..., n : x_i \in M_i\}$ heißt das kartesische Produkt der Mengen $M_1, ..., M_n$, Die Elemente $(x_1, x_2, ..., x_n)$ heißen n-Tupel. Zwei Tupel heißen gleich, falls alle Einträge gleich sind.

$[x = y] := [\forall i = 1, .., n : x_i = y_i]$ wobei
$x = (x_1, x_2, ..., x_n)$ und $y = (y_1, y_2, ..., y_n)$

Falls $M_i = M_j \forall i, j \in \{1, ..., n\}$ Schreiben wir kürzer
$M^n := M \times M \times ... \times M(\text{n-Mal}), (M = M_i)$

Bemerkung

1. $M_1 \times (M_2 \times M_3) \neq_{(\text{i.A})} (M_1 \times M_2) \times M_3$ Also nicht assoziativ, da:

   Für $x_i \in M : (x_1, (x_2, x_3)) \neq ((x_1, x_2), x_3)$,da $x_3 \neq (x_1, x_2)$

2. $[M_1 = M_2 = M_3] := [M_1 = M_2 \wedge M_2 = M_3]$

Beispiel

Der "Abbildungsraum" $\mathbb{R}^3 = \{(x, y, z) : x, y, z \in \mathbb{R}\}$

1. Jeder Punkt (x, y, z) ist durch die Koordinaten x,y,z eindeutig bestimmt

2. Achtung: $(1, 0, 0) \neq (0, 1, 0) \wedge (1, 0, 0) \neq (0, 0, 1)$ aber
   $\{1, 0, 0\} = \{0, 1, 0\} = \{0, 0, 1\} = \{0, 1\}$

3 Abbildungen

Definition 1.29

Seien D, W Mengen. Eine Abbildung (oder Funktion) f ist eine Vorschrift, die jedem $x \in D$ genau ein $y \in W$ zuordnet. Dabei heißt D der Definition- (Urbild-) Bereich und W der Werte- (Bild-) Bereich von f.

$f : D \to W : x \in D \mapsto f(x) = y \in W$

Beispiel

$D = \{1, 2, 3, 4, 5\}$
also $f(1) = f(2) = a$
$f(3) = b$
$f(4) = f(5) = c$

$W = \{a, b, c, d\}$

Beweis

Zur Beschreibung einer Abbildung gehören Definitionsbereich, Wertebereich und Abbildungsvorschrift.
□

Definition 1.31

Sei$f : D \to W$ eine Abbildung

1. Für $M \subseteq D$ heißt $f(M) := \{f(x) : x \in M\}$ das Bild von M unter f
2. Insbesondere heißt Bild $f(x) := f(D) \subseteq W$ das Bild von f
3. Für $N \subseteq W$ heißt $f^{-1}(N) := \{x \in D : f(x) \in N\} \subseteq D$ das Urbild von N unter f
4. Die Menge Graph $(f) := \{(x, f(x)) : x \in D\} \subseteq D \times W$ heißt Graph von f.

Beispiel 1.32

1. Seien $a, b \in \mathbb{R}, a < b$, wie üblich
   $[a, b] := \{x \in \mathbb{R} : a \leq x \wedge x \leq b\}$ Abgeschlossenes Intervall.
   $(a, b) := \{x \in \mathbb{R} : a < x \wedge x < b\}$ offenes Intervall.
   $[a, b) := \{x \in \mathbb{R} : a \leq x \wedge x < b\}$ halboffenes Intervall.
   $(a, b] := \{x \in \mathbb{R} : a < x \wedge x \leq b\}$ halboffenes Intervall.
2. $f : [-2, 2] \to [0, 4], f(x) := x^2$

- $M := [1,2], f(M) = \{f(x) : x \in [1,2]\} = \{y : 1 \leq y \leq 4\} = [1,4]$
  $f^{-1}(f(M)) = [1,2] \cup [-2,-1] \supset M$
- $N := \{y : y \leq 1\}, f^{-1}(N) = [-1,1], f(f^{-1}(N)) = [0,1] \subset N = [-\infty, 1]$

Definition 1.33

Die Abbildung $f_1 : D_1 \to W_1$ und $f_2 : D_2 \to W : 2$
heißen gleich falls:

1. $D_1 = D_2$
2. $W_1 = W_2$
3. $\forall x \in D_1 : f_1(x) = f_2(x)$.

Definition 1.34

Sei $f : D \to W$ eine Abbildung. Die Abbildung heißt

1. surjektiv, falls $\text{Bild}(f) = W$
2. injektiv, falls $\forall x_1, x_2 \in D : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$
3. bijektiv, eineindeutig falls f surj und inj.

Definition 1.36

Sei $f : D \to W$ eine bijektive Abbildung. Dann heißt $g : W \to D$ mit $y \mapsto g(y) = x$, so dass $f(x) = y$ die Umkehrabbildung von f oder eine zu f inverse Abbildung

Bemerkung

1. Nur falls f bijektiv ist, ist die Umkehrabbildung definiert und eindeutig definiert:
   Seien dazu g und h zwei Umkehrabbildungen von f. Die Eindeutigkeit zeigen wir durch Nachweis $g = h$:
   Offensichtlich gilt $g : W \to D \wedge h : W \to D$ und daher stimmen Definition- und Werte- Bereich überein. Für beliebige $y \in W$ gibt es genau ein $x \in D$ mit $f(x) = y$, denn f ist bijektiv.

   Aus der Definition der Umkehrabbildung folgt $g(y) = x \wedge h(y) = x \Rightarrow g(y) = h(y)$ Damit folgt $g = h$ $\square$
2. Die Umkehrabbildung von f wird mit f^{-1} bezeichnet.
3. Die inverse Abbildung f^{-1} ist leicht mit der Urbildmenge $f^{-1}(N)$ zu verwechseln.
   zum Beispiel gilt für

$f: \mathbb{R} \to \mathbb{R}, f(x) = x^2$ und $N = \{4\} : f^{-1}(N) = f^{-1}(\{4\}) = \{-2, 2\}$
aber $f^{-1}(4)$ existiert nicht.

4. Für bijektive Abbildung $f : D \to W$ und $y \in W$ gilt $\{f^{-1}(y)\} = f^{-1}(\{y\})$

Definition 1.37

1. Seien $f : X \to Y$ und $y : Y \to Z$ Abbildungen. Dann heißt die Abbildung $g \circ f : X \to Z, x \mapsto (g \circ f)(x) := g(f(x))$ die Komposition oder Hintereinanderausführung von f und g.
2. Die identische Abbildung id_X einer Menge X ist definiert durch $id_X : X \to X, x \mapsto id_X(x) := x$

bem. Selbst wenn $f \circ g$ und $g \circ f$ definiert sind , gilt i.a. $f \circ g \neq g \circ f$!

Beispiel 1.38

$f : R \to \mathbb{R}, x \mapsto f(x) = 1 + x^2$ und $g : \mathbb{R} \to \mathbb{R}, x \mapsto g(x) = 1 + x$.
$f \circ g(x) = f(g(x)) = f(1 + x) = 1 + (1 + x)^2 = 2 + 2 + x^2$
$\neq g \circ f(x) = g(f(x)) = g(1 + x^2) = 1 + (1 + x^2) = 2 + x^2$ falls $x \neq 0$
$\Rightarrow g \circ f \neq f \circ g$

Satz 1.39

Seien $f : X \to Y, g : Y \to Z$ Abbildungen. Dann gilt :

1. f und g sind $A \Rightarrow g \circ f$ ist A, $A \in \{inj, suj, bij\}$
2. $g \circ f$ injektiv $\Rightarrow$ f inj.; g $\circ f$ surj $\Rightarrow$ g suj.
3. f,g bij.$\Rightarrow (g \circ f)^{-1} = f^{-1} \circ g^{-1}$
4. f bij.$\Rightarrow$
   a) $f^{-1} bij$
   b) $(f^{-1})^{-1} = f$
   c) $f \circ f^{-1} = id_Y$
   d) $f^{-1} \circ f = id_X$

Beweis

<u>zu 1.1</u>

Wir zeigen: $f, ginj \Rightarrow g \circ finj$.
Seien $x_1, x_2 \in X$ beliebig, so dass

$g \circ f(x_1) = g \circ f(x_2) \overset{Def 1.37.1}{\Leftrightarrow} g(f(x_1)) = g(f(x_2))$
$\Leftrightarrow$ (g inj.)$f(x_1) = f(x_2)$
$\Leftrightarrow$ (f inj.) $x_1 = x_2$

Da $x_1, x_2 \in X$ beliebig. folgt$\forall x_1, x_2 \in X : g \circ f(x_1) = g \circ f(x_2) \Rightarrow x_1 = x_2$, d.h $g \circ f$ inj.

zu 1.2

Wir zeigen f, g surj$\Rightarrow$ $g \circ f$ surj.
Da g surj, gibt es ein $y \in Y$ mit $g(y) = z$ und $z \in Z$
Da f surj, gibt es ein $x \in X$ mit $f(x) = y$

Zusammenfassung:

$g \circ f(x) = g(f(x)) = g(y) = z$
da $z \in Z$ beliebig, gilt:
$\forall z \in Z \exists x \in Z : g \circ f(x) = z$
d.h $g \circ f$ ist surj.

1.3

folgt aus 1.1 und 1.2 □

zu 2.1

$g \circ f$ injektiv impliziert

Für beliebiges $x_1, x_2 \in X$ folgt $g \circ f(x_1) = g \circ f(x_2) \Rightarrow x_1 = x_2$

Also $f(x_1) = f(x_2) \Rightarrow g(f(x_2)) = g(f(x_1)) \Rightarrow f \circ f(x_1) = g \circ f(x_2) \Rightarrow x_1 = x_2 \Rightarrow$ f inj. □

zu 2.2

$g \circ f$ surjektiv impliziert

Für beliebiges $z \in Z$ gibt es ein $x \in X$ mit $g \circ f(x) = z$ Für $y := f(x)$ gilt:

$g(y) = g(f(x)) = g \circ f(x) = z$ damit gibt es für jedes $z \in Z$ ein $y \in Y$ mit $g(y) = z \Rightarrow g$ suj. □

zu 3

Nach 1.3 folgt aus f, g bij das $g \circ f$ bij. und mit der Definition der Komposition folgt:

$(g \circ f)^{-1} : Z \to X, g^{-1} : Z \to Y, f^{-1} : Y \to X,$
$f^{-1} \circ g^{-1} : Z\ X$, das heißt Definition- und Werte-Bereiche von $(g \circ f)^{-1}$ und $f^{-1} \circ g^{-1}$ stimmt überein.

Für beliebige $z \in Z$ gibt es ein $y \in Y$ und $x \in X$ mit $g(y) = z$ und $f(x) = y$
das heißt $g \circ f(x) = z$ und deshalb ist $(g \circ f)^{-1}(z) = x$

Weiter gilt: $(f^{-1} \circ g^{-1})(z) = f^{-1}(g^{-1}(z)) = f^{-1}(y) = x$

Das heißt für alle $z \in Z$ gilt $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$
zusammen : $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ □

Definition 1.40

Eine Abbildung $f : D \to \mathbb{R}$ heißt

1. nach oben beschränkt $\Leftrightarrow [\exists c_1 \in \mathbb{R} \forall x \in D : f(x) \leq c_1]$
2. nach unten beschränkt $\Leftrightarrow [\exists c_2 \in \mathbb{R} \forall x \in D : f(x) \geq c_2]$
3. beschränkt $\Leftrightarrow$ [f nach oben beschränkt $\wedge$ f nach unten beschränkt]
4. Die Konstanten c_1 bzw. c_2 heißen obere bzw. untere Schranke.

Bemerkung

1. f beschränkt $\Leftrightarrow \exists c \in \mathbb{R} : |f(x)| \leq c]$
2. Analog zu obiger Definition nennen wir eine Menge $M \subseteq \mathbb{R}$ nach oben(bzw. unten) beschränkt, falls

   $\exists c_1 \in \mathbb{R} \forall x \in M : x \leq c_1$ bzw. $\exists c_2 \in \mathbb{R} \forall x \in M : x \geq c_2$
3. Jede nicht-leere nach oben (bzw. unten) beschränkte Menge $M \subseteq \mathbb{R}$ besitzt eine kleinste obere (bzw. größte untere) Schranke (ohne Beweis)

Definition 1.42

Sei$f : D \to \mathbb{R}$ eine Abbildung

1. Sei f nach oben beschränkt. Die kleinste obere Schranke $S \in \mathbb{R}$ heißt das Supremum von $f : S := sup\{f(x) : x \in D\}$
2. Sei f nach unten beschränkt. Die größte untere Schranke $s \in \mathbb{R}$ heißt das Infimum von f: $s := inf\{f(x)x \in D\}$
3. Gilt: $\exists z \in D \forall x \in D : f(z) \geq f(x)$, so heißt $M := f(z)$ das Maximum von f auf $D, M := \max\{f(x) : x \in D\}$ und z eine Maximalstelle.
4. Gilt: $\exists z \in D \forall x \in D : f(z) \leq f(x)$, so heißt $m := f(z)$ das Minimum von f auf $D, m := \min\{f(x) : x \in D\}$ und z eine Minimalstelle.

Korollar 1.43

$f : D \to \mathbb{R}$ eine Abbildung

1. Besitzt f ein Maximum in D gilt $\sup\{f(x), x \in D\} = \max\{f(x), x \in D\}$
2. Besitzt f ein Minimum in D gilt $\inf\{f(x), x \in D\} = \min\{f(x), x \in D\}$

Definition 1.45

Sei $I \subseteq \mathbb{R}, f : D \to \mathbb{R}$ heißt :

1. monoton (bzw. streng monoton) wachsend auf $I \subseteq D$ falls
   $\forall x_1, x_2 \in I : x_1 < x2 \Rightarrow f(x_1) \leq f(x_2)$ bzw. $f(x_1) < f(x_2)$
2. monoton (bzw. streng monoton) fallend auf $I \subseteq D$ falls
   $\forall x_1, x_2 \in I : x_1 < x2 \Rightarrow f(x_1) \geq f(x_2)$ bzw. $f(x_1) > f(x_2)$

4 Relation und Ordnungen

4.1 Allgemeine Relation

Beispiel 1.47

$Y = \{\text{Einwohner}\}, X = \{\text{Mutter}\} \subseteq Y$

$f : X \to Y$ ordne Mutter x Kind y zu $x \mapsto y$

Problem: Eine Mutter kann mehrere Kinder haben.

Dafür: Relation.

Definition 1.48

Sein X,Y Mengen.

Jede Teilmenge $R \subseteq X \times Y$ heißt Relation oder Korrespondenz zwischen X und Y. Falls X = Y heißt R auch Relation in X.
statt$(x, y) \in R$ schreiben wir kurz xRy .

Beispiel 1.49

1. $X = \{1, 2, 3\}, y = \{a, b, c, d\}$

x/y	a	b	c	d
1	$\bullet$			
2	$\bullet$	$\bullet$		
3			$\bullet$	$\bullet$

2. $R = \{(1, a), (2, a), (2, b), (3, c), (3, d)\} \subseteq X \times Y$
3. Mutter/Kind $R := \{(x, y) : x \text{ ist Mutter von y}\} \subseteq X \times Y$ ist eine Relation.

Definition 1.50

Die Relation R in X heißt

1. reflexiv, falls $\forall x \in X : xRx$
2. symmetrisch falls $\forall x, y \in X : xRy \Rightarrow yRx$
3. transitiv falls $\forall x, y, z \in X : xRy \wedge yRz \Rightarrow xRz$
4. antisymmetrisch falls $\forall x, y \in X : xRy \wedge yRx \Rightarrow x = y$

Beispiel und Bemerkungen 1.51

1. Begriffe nur für Relation R in X definiert.
2. Mutter/Kind jetzt mit $X = Y : R = \{(x, y) \in X^2 : x$ Mutter von y$\} \subseteq X^2$

2.1. $\neg$ reflexiv

2.2. $\neg$ symmetrisch

2.3. $\neg$ transitiv

2.4. antisymmetrisch

3. $R = \{(x, y) \in \mathbb{R}^2 : x \leq y\} \subseteq \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$

3.1. reflexiv

3.2. $\neg$ Symmetrisch

3.3. transitiv

3.4. antisymmetrisch

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

4.1. reflexiv

4.2. $\neg$ symmetrisch

4.3. $\neg$ transitiv

4.4. $\neg$ antisymmetrisch

Definition 1.52

Eine Relation $RinX$ heißt eine Halbordnung(-srelation) in X, falls R:

1. reflexiv
2. antisymmetrisch
3. transitiv

Eine Halbordnung R heißt Ordnung(-srelation) auf X, falls zu dem gilt:

$\forall x, y, \in X : xRy \vee yRx$

bsp $\{a, b\}, R = \{(a, a), (b, b)\} \subseteq X^2$

bsp.1 reflexiv,antisymmetrisch,transitiv $\Rightarrow$ Halbordnung

4. aber $\neg$ Ordnung, da $(a, b) \notin R \wedge (b, a) \notin R$

Beispiel 1.53

Sei $M \neq \varnothing, X := P(M), R := \{(A, B) \in X^2 : A \subseteq B\}$

Halbordnung, aber keine Ordnung(falls...)

Definition 1.54

Sei X eine Menge mit Halbordnung $\leq$. Ein Element $a \in T \subseteq X$ heißt

1. Maximales Element von T, falls $\forall x \in T : (a \leq x \Rightarrow a = x)$
2. minimales Element. von T, falls $\forall x \in T : (x \leq a \Rightarrow a = x)$
3. größtes Element oder ein Maximum von T , falls $\forall x \in T : x \leq a$
4. kleinstes Element oder ein Minimum von T, falls $\forall x \in T : a \leq x$

Bemerkung

Falls Max/Min existieren, so sind diese eindeutig bestimmt.

(sind a,b Minima folgt $a \leq b \wedge b \leq a \Rightarrow a = b$)

Beispiel 1.55

$T = \{\{a\}, \{b\}, \{a, b, c\}, \{a, b, c, d\}, \{b, d\}, \{c, e\}\}$ Mit Halbordnung $\leq$

1. Minimale Elemente : $\{a\}, \{b\}, \{c, e\}$
2. es gibt kein Minimum
3. Maximale Elemente :$\{a, b, c, d\}, \{c, e\}$
4. es gibt kein Maximum.

4.2 Äquivalenzrelation

Definition 1.56

Eine Relation R in X heißt Äquivalenzrelation in X, falls R reflexiv, symmetrisch und transitiv ist.

Für $x \in X$ heißt $[x]_R := \{y \in X : xRy\}$

die Äquivalenzklasse von x bzgl R. Ist der Bezug zu R klar , schreiben wir auch kurz $[x]$.

Bemerkung

In der Literatur auch folgende Schreibweise:

$xRy, x \sim\ y, x \sim_R\ y, x \equiv y, x \equiv_R y$

Beispiel 1.57

1. Sei $X = \mathbb{Q}$, die Relation $R = \{(x, y) \in \mathbb{Q}^2 : x = y\} \subseteq \mathbb{Q}^2$ ist Ä-Relation in $\mathbb{Q}$, mit z.B. $[\frac{1}{2}]_R = \{..., \frac{-2}{4}, \frac{-1}{2}, \frac{1}{2}, \frac{2}{4}, \frac{4}{8}, \frac{3}{6}, ...\}$
2. Im Keller stehen fünf Räder

   $K = \{A, B, F, D, E\}$

   A rot , 1 Gang

   B blau , 3 Gang

   F rot , 3 Gang

   D blau , 21 Gang

   E rot , 21 Gang

   Claudia findet Farben wichtig und wählt:

   $C := \{(x, y) \in K^2 : x$ gleichfarbig zu y$\} \subseteq K^2$

   Jan findet Gänge wichtig.

   $J := \{(x, y) \in K^2 : x$ hat so viele Gänge wie y$\} \subseteq K^2$

   C und J sind Ä-Relation

   $[A]_C = [F]_C = [E]_C = \{A, F, E\}$

   $[B]_C = [D]_C = \{B, D\}$

   $[A]_J = \{A\}$

   $[B]_J = [F]_J = \{B, F\}$

   $[D]_J = [E]_J = \{D, E\}$

Satz 1.58

Sei R Ä-Relation in X und $x, y \in X$. dann gilt:

1. $x \in [y] \Rightarrow [x] = [y]$
2. $[x] \cap [y] \neq \varnothing \Rightarrow [x] = [y]$
3. $[x] \neq [y] \Rightarrow [x] \cap [y] = \varnothing$

Beweis

Vorüberlegung: $[y] = \{x \in X : yRx\}$

$x \in [y] \Rightarrow yRx \Rightarrow xRy$

Zu 1. $x \in [y] \Rightarrow [x] = [y]$

1. $[x] \subseteq [y]$: Sei $x \in [y] \wedge z \in [x]$ bel. $\Rightarrow xRz \wedge yRx$

   $\Rightarrow zRx \wedge xRy \Rightarrow zRy \Rightarrow yRz \Rightarrow z \in [y]$

   Also : $\forall z \in X : z \in [x] \Rightarrow z \in [y]$ oder $[x] \subseteq [y]$

2. $[x] \supseteq [y]$: Sei $x \in [y] \wedge z \in [y]$ bel. $\Rightarrow yRx \wedge yRz$

   $\Rightarrow zRy \wedge Rx \Rightarrow zRx \Rightarrow xRz \Rightarrow z \in [x]$

   Also: $\forall z \in [y] : z \in [x]$ also $[y] \subseteq [x]$

   Zusammenfassung: $[x] = [y]$

zu 2. $[x] \cap [y] \neq \varnothing \Rightarrow [x] = [y]$

Sei $z \in [x] \cap [y] \Rightarrow z \in [x] \wedge z \in [y] \Rightarrow [z] = [y] \wedge [z] = [y] \Rightarrow [x] = [y]$

zu 3. $[x] \neq [y] \to [x] \cap [y] = \varnothing$

Folgen aus Satz 1.52 $((A \to B) \Leftrightarrow (\neg B \to \neg A))$ aus Teil 2. □

Satz 1.59

Sei X Menge.

1. Ist R Ä-Relation in X, so ist $\Sigma := \{[x]_R : x \in X\}$ eine Partition von X.
2. Ist Ω eine Partition von X, so ist $R := \{(x, y) \in X^2, \exists M \in \Omega : x, y \in M\}$ eine Ä-Relation in X.

Beweis

zu 1 Σ ist Partition von X

1. Sei $[x] \in \Sigma$ Da R refl. folgt: $x \in [x]$, d.h. $[x] \neq \varnothing$

   Weiter gilt: $[x] = \{y \in X : xRy\} \subseteq X$

2. Sein $[x], [y] \in \Sigma$ und angenommen $[x] \cap [y] \neq \varnothing \Rightarrow [x] = [y]$

   d.h die Klassen sind pwd.

3. Da $[x] \subseteq X$ gilt $\bigcup_{x \in X} [x] \subseteq X$

   Sei $x \in X$ bel. Es gilt $x \in [x]$ und daher $\bigcup_{x \in X} [x] \supseteq X$. Zusammen $X = \bigcup_{x \in X} [x]$

   Also ist Σ eine Partition von X.

zu 2 R ist Ä-Relation in X

1. $\bigcup_\omega = X \Rightarrow \forall x \in X \exists M \in \Omega : x \in M \Rightarrow (x,x) \in R \Rightarrow R$ ist reflexiv
2. Sei $(x,y) \in R \Rightarrow \exists M \in \Omega : x, y \in M \Rightarrow (y,x) \in R \Rightarrow R$ ist symmetrisch.
3. Sei $(x,y) \in R \wedge (y,z) \in R$

   $\Rightarrow (\exists M \in \Omega : (x,y) \in M) \wedge (\exists P \in \Omega : (y,z) \in P)$

   Da die Partition nur Mengen enthält, folgt aus $y \in M \wedge y \in P \Rightarrow P = M$ d.h $x, z \in M \Rightarrow (x,z) \in R$

   Da $x, y, z \in Z$ bel. folgt $xRy \wedge yRz \Rightarrow xRz$, d.h R ist transitiv.

   Zusammen folgt aus 1,2,3 R ist Ä-Relation. □

Definition 1.60

Sei R Ä-Relation in X und $x \in X$.

1. Jedes $y \in [x]$ heißt Repräsent der Ä-Klasse $[x]$
2. Die Quotientenmenge ist die Menge der Ä-Klassen.$X/R := \{[x] : x \in X\}$
3. Eine Menge $Y \subseteq X$ heißt Repräsentatensystem falls:

   $\forall [x] \in X/R : |Y \cap [x]| = 1$.

5 Zahlentheoretisches

5.1 Allgemeines

Zugrunde gelegt ist $\mathbb{Z}, a, b \in \mathbb{Z}$

Teiler $a|b(a$ teilt $b)$ falls $\exists g \in \mathbb{Z} : a * g = b$

Primzahl $p \in \mathbb{N}$ heißt prim, falls $p \notin \{1\}$ und $\forall q \in \mathbb{Z} : q|p \Rightarrow q \in \{\pm 1, \pm p\}$

Primfaktorzerlegung $a \in \mathbb{Z} \wedge a \neq 0 \Rightarrow a = \pm p_1, p_2 ... p_k$

$p_i \in \mathbb{N}$ prim pwd. , $q_i \in \mathbb{N}$

Gaus-Klammern

$\llcorner \lrcorner, \ulcorner \urcorner : \mathbb{R} \to \mathbb{Z}$

$\llcorner x \lrcorner := \max\{z \in \mathbb{Z} : z \leq x\}$

$\ulcorner x \urcorner := \min\{z \in \mathbb{Z} : z \geq x\}$

Größter gemeinsamer Teiler

$\mathrm{ggT}(a, b) = \max\{k \in \mathbb{N} : k|(a \wedge b)\}$

Kleinstes gemeinsames Vielfaches

$\mathrm{kgV}(a, b) = \min\{k \in \mathbb{N} : a|k \wedge b|k\}$

Beispiel 1.61

1. $2|4 \wedge \neg(2|5)$
2. 4 ist nicht prim: $2|4$ 5 prim : $x|5 \Rightarrow x \in \{\pm 1, \pm 5\}$
3. $a = 72 = 2 * 36 = 2 * 2 * 18 = 2 * 2 * 2 * 9 = 2 * 2 * 2 * 3 * 3 = 2^3 * 3^2$
4. $\llcorner 3,5 \lrcorner = 3, \ulcorner -3,4 \urcorner = -3, \llcorner -2,1 \lrcorner = -2$
5. $a = 12, b = 8$, positive Teiler von
   $a : \{1, 2, 3, 4, 6, 12\}$
   $b : \{1, 2, 4, 8\}$

   Teiler von a und b : $\{1, 2, 4\} \Rightarrow$ ggT $(12, 8) = 4$
6. $a = 3, b = 4$ positive Vielfache
   $a : 3, 6, 9, 12, 15, 18, ...$
   $b : 4, 8, 12, 16, ...$

   kgV (3,4) $= 12$

Satz 1.62 (Teilen mit Rest)

Seien $z \in \mathbb{Z}$ und $m \in \mathbb{N}$ Dann gibt es eindeutige Zahlen $q \in \mathbb{Z}$ und $r \in \{0, 1..., m-1\} \subseteq \mathbb{Z}$, sodass $z = m * q + r$

$20 = 3 * 6 + 2$

Ohne Beweis.

5.1.1 Euklidischer Algorithmus zur Berechnung des ggT's

Gesucht wird g = ggT(a, b), wobei $a, b \in \mathbb{N}, a \geq b$

Wir nutzen Division mit Rest und führen die Reste r_i und Faktoren q_i ein

Dabei ist

$r_{k-1} = q_k * r_k + r_{k+1}$

$r_{n-1} = q_n * r_n + 0$

$g =$ggT$(a, b) = r_n$

Beispiel 1.63

$a = 76, b = 42, a \geq b$

$r_0 := a = 76$

$r_1 := b = 42$

$r_{k+1} = q_k r_k + r_{k+1}$

Zur Begründung des Euklidischen Algorithmus

Ist $g = ggT(a, b)$, dann gibt es Zahlen c_0 und c_1, sodass $a = r_0 = c_o + g$ und $b - r_1 = c_1 * g$ also $r_2 = r_0 - q_1 r_1 = c_0 g - q_1 * c_1 * g = (c_0 - q_1 c_1) * g \Rightarrow g | r_2 \Rightarrow ... \Rightarrow g | r_n \Rightarrow g \leq r_n$

Weiter gilt $r_{n-1} = q_n r_n \Rightarrow r_{n-2} = (q_{n-1} q_n + 1) * r_n$ also $r_n | r_{n-1} \wedge r_n | r_{n-2}$ weiter $r_n | r_k$ für $k = 0, ..., n \Rightarrow r_n \leq g$

Zusammen: $r_n = g$

Erweiterter Euklidischer Algorithmus

Gegeben $a, b \in \mathbb{N}$

Gesucht: $g = ggT(a, b)$ und $s, t \in \mathbb{Z}$, sodass $g = sa + tb$

Euklidischer Algorithmus generiert eine Folge (r_k, q_k) mit $r_{k-1} = q_k r_k + r_{k+1}, r_{k+1} \leq r_k; k = 1, ..., n$

Hieraus kann die Faktorisierung bestimmt werden :

$g = r_n = r_{m-2} - q_{n-1} r_{n-1} = r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2} r_{n-2})$

$= (1 + q_{n-1}q_{n-2})r_{n-2} - q_{n-1}r_{n-3} = \alpha_{n-2}r_{n-2} + \beta_{n-2}r_{n-3}$

$= \alpha_{n-2}(r_{n-4} - q_{n-2}r_{n-3}) + \beta_{n-2}r_{n-3} =: \alpha_{n-2}r_{n-3} + \beta_{n-3}r_{n-4} = \alpha_0 r_0 + \beta_0 r_1$

Beispiel 1.64

$a = 99,\ b = 78$

1. $r_0 = q_1r_1 + r_2$ $99 = 1 * 78 + 21(A)$
2. $r_1 = q_2r_2 + r_3$ $78 = 3 * 21 + 15(B)$
3. $r_2 = q_3r_3 + r_4$ $21 = 1 * 15 + 6(C)$
4. $r_3 = q_4r_4 + r_5$ $15 = 2 * 6 + 3(D)$
5. $r_4 = q_5r_5 + r_6$ $6 = 2 * 3 + 0$ Also gilt $ggt(99, 78) = 3$

$ggt(a, b) = 3$

$\overset{(D)}{=} 15 - 2 * 6$

$\overset{(C)}{=} 15 - 2(21 - 1 * 15) = 3 * 15 - 2 * 21$

$\overset{(B)}{=} 3(78 - 3 * 21) - 2 * 21 = 3 * 78 - 11 * 21$

$\overset{(A)}{=} 3 * 78 - 11(99 - 1 * 78) = -11 * 99 + 14 * 78$

$s = -1 \land t = 14$

5.2 Kongruenzen

Definition 1.65

Sei $m \in \mathbb{N}$ und $x, y \in \mathbb{Z}$ gilt:

$m|(x - y)$, heißt $\underline{x \text{ kongruent zu y modulo m :}}$ $x \equiv y \bmod m$

Beispiel 1.66

1. $6 \equiv 4 \bmod 2$
2. $7 \equiv 1 \bmod 2 \Leftrightarrow x \in \{... - 3, -1, 1, 3, 5, ...\}$

   $y \equiv 0 \bmod 2 \Leftrightarrow y \in \{... - 4, -2, 0, 2, 4, ...\}$

   $y \equiv 4 \bmod 2 \Leftrightarrow y \equiv -2 \bmod 2 \Leftrightarrow y \equiv 0 \bmod 2$
3. $z \equiv 1 mod 4 \leftrightarrow z \in \{..., -7, -3, 1, 5, 9, ...\} = \{4 * p + 1, p \in \mathbb{Z}\}$

Satz 1.67

Sei $m \in \mathbb{N}$ und $x, y \in \mathbb{Z}$. Es gilt $x \equiv y \bmod m \Leftrightarrow x$ und y haben die Division durch m den selben Rest.

Bemerkung

Wie nutzen Satz 1.62 : $x = q_x m + r_x$ und $y = q_y * m + r_y$ wobei $q_x, q_y \in \mathbb{Z}$ und $r_x, r_y \in \{0, ..., m-1\}$ eindeutig bestimmt.

Es folgt

$x \equiv y \bmod m \Leftrightarrow m|(x-y) \Leftrightarrow m|q_x m + r_x - q_y m - r_y) \Leftrightarrow m|(r_x - r_y) \Leftrightarrow r_x = r_y$ □

Satz 1.68

Sei $m \in \mathbb{N}$ und $R := \{(x, y) \in \mathbb{Z}^2 : x =\equiv y \bmod m\} \subseteq \mathbb{Z}^2$

Die Menge R ist eine Äquivalenzrelation in $\mathbb{Z}$.

Beweis

Es ist R eine Relation in $\mathbb{Z}$ Sei $x, y, z \in \mathbb{Z}$ beliebig gewählt.

Reflexiv:

$m|(x-x) \Rightarrow x \equiv x \bmod m \Rightarrow xRx$. Da x beliebig folgt $\forall x \in \mathbb{Z} : xRx \Rightarrow R$ reflexiv.

1. Symmetrisch:

   $xRy \Leftrightarrow m|(x-y) \Leftrightarrow m|(y-x) \Leftrightarrow yRx$, da x, y beliebig $\Rightarrow \forall x, y \in \mathbb{Z} : xRy \Rightarrow yRx \Rightarrow R$ symmetrisch.

   Transitiv:

   $xRy \wedge yRz \Leftrightarrow (x \leq y \bmod m \wedge y \geq z \bmod m)$ Mit Satz 1.67
   Folgt $[x, y$ bei Division durch m denselben Rest$]$
   $\wedge[y, z$ bei Division durch m denselben Rest$]$
   also $[x, z$ bei Division durch m denselben Rest$] \Leftrightarrow x \equiv z \bmod m \Leftrightarrow xRz$

   Da x, y, z beliebig folgt $\forall x, y, z \in \mathbb{Z} : xRy \wedge yRz \Rightarrow xRz$ das heißt R ist transitiv.

   Zusammen R ist Äquivalenz-Relation. □

Definition 1.69

Sei $R := \{(x,y) \in \mathbb{Z}^2 : x \equiv y \text{ mod } m\}(m \in \mathbb{N})$ Die Äquivalenz-Klasse von $x \in \mathbb{Z}$ heißt Restklasse und wird mit $[x]_m$ bezeichnet.

$[x]_m = \{y \in \mathbb{Z} : x \equiv y \text{ mod } m\}$.

Die entsprechende Quotienten-Menge heißt $\mathbb{Z}_m := \mathbb{Z} \backslash Z$.

Beispiel 1.70

1. $m = 2 : \mathbb{Z}_2 = \{[0]_2, [1]_2\}$ mit $[0]_2 = \{0, \pm 2, \pm 4, ...\}[1]_2 = \{\pm 1, \pm 3, ...\}$
2. $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, 4, ...\}$ Modul m z.B.$m = 4$

   $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [-1]_4\}$

   $[0]_4 = \{4z : z \in \mathbb{Z}\}$

   $[1]_4 = \{4z + 1 : z \in \mathbb{Z}\}$

   $[2]_4 = \{4z + 2 : z \in \mathbb{Z}\}$

   $[-1]_4 = \{4z + 3 : z \in \mathbb{Z}\} = [3]_4$

   Sätze 1.59 und 1.68 implizieren $\mathbb{Z}[0]_2 \cup [1]_2$

   Allgemeiner :$\forall m \in \mathbb{N} : \mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}$ ist eine Partition von $\mathbb{Z}$

Satz 1.71

Sei $m \in \mathbb{N}, a, b, x, y \in \mathbb{Z}$ mit $a \equiv x \text{ mod } m$ und $b \equiv y \text{ mod } m$

Es gilt:

1. $a \pm b \equiv x \pm y \text{ mod } m$
2. $ab \equiv xy \text{ mod } m$
3. Sind p, q prim. $p \neq q, m = pq$ dann gilt

   $x \equiv y \text{ mod } m \Leftrightarrow [x] \equiv y \text{ mod } p \wedge x \equiv y \text{ mod } q]$

Beweis

Zu 1. Zu zeigen ist :

$m|(a \pm v - (x \pm y))$ Es gilt:

$a \equiv x \text{ mod } m \Rightarrow m|(x-a) \Rightarrow \exists p \in \mathbb{Z} : p * m = x - a$

$b \equiv y \bmod m \Rightarrow m|(y-b) \Rightarrow \exists q \in \mathbb{Z} : q * m = y - b$

$\Rightarrow (a-x) \pm (b-y) = pm \pm qm \Rightarrow m|((a-x) \pm (b-y)) \Rightarrow m|((a \pm b) - (x \pm y))$

2. Wir zeigen $m|(ab - xy) \Rightarrow ab, xy$ Div durch m denselben Rest $\Rightarrow ab \equiv xy \bmod m$

   Es gilt

   $a \equiv x \bmod m \Rightarrow m|(a-x) \Rightarrow m|(a-x)b$

   $b \equiv y \bmod m \Rightarrow m|(b-y) \Rightarrow m|(b-y)x$

   $\Rightarrow m|(a-x)b + (b-y)x = ab - xb + bx - xy$

   $-xb + bx = 0$

3. Wir zeigen die Äquivalenz durch zwei Implikationen:

   $" \Rightarrow " x \equiv y \bmod (p*q) \Rightarrow (q*p)|(x-y) \Rightarrow \exists k \in \mathbb{Z} : x - y = k * p * q$

   $\Rightarrow p|(x-y) \wedge q|(x-y) \Rightarrow$ Behauptung.

   $" \Leftarrow " [p|(x-y) \wedge q|(x-y)] \Rightarrow p, q$ zwei Faktoren der Primfaktorzerlegung von $x - y = p_1 * p_2 * p_3 * ... * p_w \Rightarrow (p*q)|(x-y) \Rightarrow$ Behauptung.

   Achtung:

   Voraussetzung p, q prim. ist wichtig:

   $4|16$ und $8|16$ aber $4 * 8 = 32 \nmid 16$ □

5.2.1 Dezimaldarstellung

$14365 = 1 * 10^4 + 4 * 10^3 + 3 * 10^2 + 6 * 10^1 + 5 * 10^0$

Korollar

Sei $x \in \mathbb{N}$ mit Dezimaldarstellung $x = \sum_{i=0}^{n} x_i 10^i, x_i \in \{0, ..., 9\}$ Dann ergibt : $9|x \Leftrightarrow 9|\sum_{i=1}^{n} x_i$

Beweis

Wir zeigen , dass x und $\sum x_i$ bei Div durch 9 denselben Rest haben, d.h $x \equiv \sum_{i=0}^{n} x_i \bmod 9$ Es gilt

$10 \equiv 1 \bmod 9 \overset{Satz 1.71}{\Rightarrow} 10^2 \equiv 1 \bmod 9$

$\Rightarrow x_i * 10^2 \equiv x_i \bmod 9 \Rightarrow (\sum x_i 10^2) \equiv (\sum x_i) \bmod 9$ □

5.3 Vollständige Induktion

5.3.1 Peano-Axiome

Für eine Menge N existiert eine Nachfolge-Abbildung $' : N \to N, n \mapsto n'$

1. $1 \in N$
2. $n \in N \Rightarrow n' \in N$
3. $n \in N \Rightarrow n' \neq 1$
4. $n, m \in N \Rightarrow (m' = n' \Rightarrow m = n)$
5. $[1 \in X \wedge \forall n \in N : n \in X \Rightarrow n' \in X] \Rightarrow [N \subseteq X]$

Die Menge mit $(1-5)$ ist eindeutig beschrieben und heißt die Menge der natürlichen Zahlen $\mathbb{N}$ Die Nachfolgeabbildung wird auch mit $+1$ gleichgesetzt: $n' = n + 1$

Für eine von $n \in \mathbb{N}$ abhängige Aussage $A(n)$ wird behauptet $B := [\forall n \in \mathbb{N} : A(n)]$ ist wahr.

5.3.2 Vollständige Induktion

Dazu: Beweisprinzip der vollständigen Induktion (wie Dominosteine).

1. Induktionsanfang (IA) : A(1) ist wahr.
2. Induktionsvoraussetzung (IV): Annahme : Für ein beliebiges aber festes $k \in \mathbb{N}$ gilt $A(k)$. Wichtig: k' ist konkret aber beliebig.

   [3'. Induktionsbehauptung : $A(k) \Rightarrow A(k+1)$]
3. Induktionsschluss (IS) : Wir zeigen $A(k) \Rightarrow A(k+1)$
4. Aus den Peano-Axiomen folgt $[A(1) \wedge \forall k \in \mathbb{N} : A(k) \Rightarrow A(k+1))] = [\forall n \in \mathbb{N} : A(n)] = B$

   Aus IA,IV,IS folgt B $\square$

Beispiel 1.73

1. $B = [\forall n \in \mathbb{N} : A(n)]$ mit $A(n) := [\sum\limits_{j=0}^{n} = \frac{n(n+1)}{2}$

   Beweis von B mit vollständiger Induktion (VI)

IA Für $n = 1$ gilt $A(1) = [\sum\limits_{j=0}^{1} j = \frac{1*(1+1)}{2}] = [0 + 1 = \frac{1*2}{2}]$ w.A.

IV Für ein beliebiges $k \in \mathbb{N}$ gilt $A(k) = [\sum\limits_{j=0}^{k} = \frac{k(k+1)}{2}]$

IS Wir zeigen $A(k+1) = [\sum\limits_{j=0}^{k+1} j = \frac{(k+1)((k+1)+1)}{2}]$ ist wahr:

$$\sum_{j=0}^{k+1} j = \sum_{j=0}^{k} j + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{(k+1)(k+1)+1}{2}$$

VI Aus IA,IV,IS folgt VI die Behauptung B. $\square$

Bemerkung

1. Kompakte Form: Mit vollständiger Induktion beweisen wir $B := [\forall n \in \mathbb{N} : A(n)]$

   IA : Wir zeigen $A(1)$

   IV: Annahme: Für ein beliebiges $k \in \mathbb{N}$ gilt $A(k)$

   IS: Schluss: $A(k) \Rightarrow A(k+1)$

   IV : IA,IV,IS $\Rightarrow B$, B ist wahr.

2. Man kann das Prinzip erweitern, indem $\mathbb{N}$ durch $n := \{z \in \mathbb{Z} : z \geq z_0\}$ ersetzt wird.

3. Man kann das Prinzip erweitern auf abzählbare Mengen A, d.h es gibt eine surjektive Abbildung $\mathbb{N} \to A$

   $f : \mathbb{N} \to \mathbb{Z}, n \mapsto \{n/2$, falls n gerade; $\frac{-(n+1)}{2}$, falls n ungerade

Beispiel 1.74

Wir zeigen $B := [\forall n \in \mathbb{N} : A(n)]$ wobei $A(n) = [\sum_{j=1}^{n}(2j-1) = n^2$

IA Wir zeigen $A(1) = [\sum_{j=1}^{1} = 1^2] = [2 - 1 = 1]$ w.A.

IV Für ein beliebiges $k \in \mathbb{N}$ gilt $A(k) = [\sum_{j=0}^{k}(2j-1) = k^2]$

IS $[A(k) \Rightarrow A(k+1)]$ ist wahr , da :

$$\sum_{j=1}^{k+1}(2j-1) = (2(k+1)-1) + \sum_{j=1}^{k}(2j-1) = (k+1)^2$$

Aus VI folgt: B ist wahr. □

Satz 1.75

Für alle $n \in \mathbb{N}$ und $x \geq -1$ gilt die Bernoulli-Ungleichung $(1+x)^n \geq 1 + nx$

Beweis

Mit VI beweisen wir $\forall n \in \mathbb{N} : A(n), A(n) := [(1+x)^n \geq 1 + nx]$.

IA Wir zeigen $A(1) : A(1) = [(1+x)^1 \geq 1 + 1 * x]$ w.A.

IV Für ein beliebiges $n \in \mathbb{N}$ gilt $A(n), A(n) = [(1+x)^n \geq 1 + n * x]$

IS Wir zeigen $(1+x)^{n+1} \geq 1 + (n+1)x$:

$(1+x)^{n+1} \geq (1+x)^n * (1+x)$ da $x \geq -1$

$\overset{VI}{\Leftrightarrow} 1+(n+1)x+nx^2 \geq 1+(n+1)x$

Mit VI folgt die Behauptung. $\square$

Definition 1.76

1. Sei $n \in \mathbb{N}_0$: Wir definieren die Fakultät:

   $0! := 1$ und $n! = n*(n-1)!$ für $n \in \mathbb{N}$

2. Seien $n, k \in \mathbb{N}_0$ mit $n \geq k$ Der Binominal-Koeffizient ist definiert durch $\binom{n}{k} := \frac{n!}{k!*(n-k)!}$ (sprich n über k)

Bemerkung

1. $n! = n*(n-1)! = n+(n-1)(n-2)! = ... = n(n-1)(n-2)*...*1*0! = \prod_{i=1}^{n} i$
2. $\binom{n}{0} = \binom{n}{n} = 1$ (nachrechnen!)
3. $\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$ Übungsaufgabe

5.3.3 Indexverschiebung

$\sum_{K=1}^{n} a_k = \sum_{K=m}^{n+m-1} a_{k-m+1} = a_1 + ... + a_n$

Satz 1.77 Binomischer Satz

Für $a, b \in \mathbb{R}$ und $n \in \mathbb{N}_0$ gilt:

$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

Beweis

Mittels VI beweisen wir die Aussage $\forall n \in \mathbb{N}_0 : A(n)$ mit $A(n) = [(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}]$

IA : Wir zeigen $A(0)$ ist wahr

$A(0) = [(a+b)^0 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{n-k}] = [1 = \binom{0}{0} a^0 + b^0]$

IV Für m beliebig $n \in \mathbb{N}_0$ gelte $A(n)$.

IS: Wir zeigen $A(n+1)$ ist wahr

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{k=0}^{n} \tbinom{n}{k} a^k b^{n-k}$$

$$= \sum_{k=0}^{n} \tbinom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \tbinom{n}{k} a^k b^{n-k+1}$$

$$= \sum_{k=1}^{n+1} \tbinom{n}{k-1} a^k b^{n-k+1} + \sum_{k=0}^{n} \tbinom{n}{k} a^k b^{n-k+1}$$

$$= \tbinom{n}{n} a^{n+1} b^0 + \sum_{k=1}^{n} [\tbinom{n}{k-1} + \tbinom{n}{k}] a^k b^{(n+1)-k} + \tbinom{n}{0} a^0 b^{n+1}$$

$$= \tbinom{n+1}{n+1} + \tbinom{n+1}{k} + \tbinom{n+1}{0}$$

$$= \sum_{k=0}^{n+1} \tbinom{k+1}{k} a^k b^{(n+1)-k}$$

Mit VI folgt die Behauptung $\forall n \in \mathbb{N}_0 : A(n)$. $\square$

z.B.

$(a+b)^0 = 1$
$(a+b)^1 = a+b$
$(a+b)^2 = 1 * a^3 + 2 * ab + 1 * b^2$
$(a+b)^3 = 1 * a^3 + 3 * a^2 * b + 3 * ab^2 + 1 * b^3$
$(a+b)^4 = 1 * a^4 + 4 * a^3 b + 6 * a^2 b^2 + 4 * a + b^3 + 1 * b^4$

6 Mengen und Folgen

Definition 1.78

Sei D eine Menge und $a : \mathbb{N} \to D$ eine Abbildung $n \mapsto a(n) := a_n \in D, (a_n)_{n\in\mathbb{N}}$ heißt die Folge in D. Die Menge Bild(a) $:= \{a_n, n \in \mathbb{N}\}$ heißt der Folge (a_n) unterliegende Menge.

Beispiel 1.79

$a_n := (-1)^n, b_n := (-1)^{n+1}$, Bild(a) $=\{\pm 1\} =$ Bild(b) Unterschiedliche Folgen können dasselbe Bild haben.

Definition 1.80

Eine nicht leere Menge D heißt abzählbar, wen es eine surjektive Abbildung $\Phi : \mathbb{N} \to D$ gibt. Die Menge heißt Überabzählbar wenn sie nicht abzählbar ist.

Beispiel 1.81

Abzählbare Mengen:

1. Endliche Mengen sind abzählbar: $M = \{m_0, ..., m_n\}$

   $a : \mathbb{N} \to M, a_j := m_{j-1}$ für $j = 1, ..., n, a_j := m_n$ falls $j > n$.

2. $\mathbb{N}$ ist abzählbar:$\Phi := id_{\mathbb{N}}$

3. $\mathbb{Z}$ ist abzählbar $a_0 := 0, a_{2k-1} := k, a_{2k} := -k, k \in \mathbb{N}$

Satz 1.82

Die Vereinigung abzählbar vieler abzählbarer Mengen ist abzählbar.

Beweis

$M_0 : x_{00}, x_{01}, x_{02}, x_{03}, x_{04}, x_{05}, ...$
$M_1 : x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15}, ...$
$M_2 : x_{20}, x_{21}, x_{22}, x_{23}, x_{24}, x_{25}, ...$
$M_3 : x_{30}, x_{31}, x_{32}, x_{33}, x_{34}, x_{35}, ...$
$M_4 : x_{40}, x_{41}, x_{42}, x_{43}, x_{44}, x_{45}, ...$
$x_{00}, x_{01}, x_{02}, x_{11}, x_{02}, x_{03} ... = y_0, y_1, y_2 ...$
Also $M = \{y_n : n \in \mathbb{N}\}$ Genannt: 2. Cantor'sches Diagonalisierungsverfahren □

Korollar 1.83

Die Menge $\mathbb{Q}$ ist abzählbar,

Beweis $A_n := \{\frac{k}{n}, k \in \mathbb{N}\}, b_n := \{-\frac{k}{n}, k \in \mathbb{N}\}$ sind abzählbar,

Somit auch $C_n = A_n \cup B_n \cup \{0\}$ und $\mathbb{Q} = \bigcup_{n \in \mathbb{N}} C_n$.

Satz 1.84

Die Menge $\mathbb{R}$ ist überabzählbar.

Beweis

Wir nutzen das 2. Cantor'sche Diagonalisierungverfahren um zu zeigen, dass das Intervall $(0,1)$ nicht abzählbar ist. Angenommen (0,1) $= \{a_n : n \in \mathbb{N}\}$, in Dezimaldarstellung:

$a_1 = 0, a_{11}, a_{12}, a_{13}, ...$
$a_2 = 0, a_{21}, a_{22}, a_{23}, ...$
$a_3 = 0, a_{31}, a_{32}, a_{33}, ...$

Wir definieren $c = 0, c_1, c_2, c_3, c_4...$ durch
$c_k =$
5 falls $a_{k,k} \neq 5$
4 falls $a_{k,k} = 5$
für $k \in \mathbb{N}$

Da $\mathbb{R}$ vollständig ist gilt $c \in (0,1)$ aber $c \neq a_n$ für alle $n \in \mathbb{N}$ Widerspruch... □

Korollar 1.85

Die Menge der irrationalen Zahlen ist überzählbar.

Beweis

Angenommen $\mathbb{R} \backslash \mathbb{Q}$ ist äbzählbar $\Rightarrow (\mathbb{R} \backslash \mathbb{Q}) \cup \mathbb{Q} = \mathbb{R}$ ist abzählbar Widerspruch. □

7 Gruppen und Körper

Beispiel 2.1

1. Mengen $\mathbb{N} =: G$ und Abbildung $\oplus : G \times G \to G, (a, b) \mapsto \oplus(a, b) =: a + b \in \mathbb{N}$
2. Menge $\mathbb{R} =: G$ und Abbildung $\odot : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a, b) \mapsto \odot(a, b) =: a * b = a, b \in \mathbb{R}$

7.1 Gruppen

Definition 2.2

Es sei G eine Menge und $\diamond$ eine Abbildung.

$\diamond : G \times G \to G,\ (a, b) \mapsto \diamond(a, b) =: a \diamond b.$

$G := \{f : \{1, 2, 3\} \to \{1, 2, 3\}, fby\}$

$a = [2, 1, 3], b = [1, 3, 2], c = [2, 3, 1], \diamond(a, b) = b \diamond a, a \diamond b = [2, 3, 1]$

Das Paar (G, $\diamond$) heißt Gruppe, falls die Gruppenaxiome (G1-G4) gelten:

G1 Vollständigkeit : $\forall a, b \in G : a \diamond b \in G$

G2 Assoziativität: $\forall a, b, c \in G : (a \diamond b) \diamond c = a \diamond (b \diamond c)$

G3 Neutrales Element : $\exists e \in G \forall a \in G : e \diamond a = a$

G4 Inversives Element $\forall a \in G \exists a' \in G : a' \diamond a = e$

Gilt zusätzlich (G5(Kommutativität $\forall a, b \in G : a \diamond b = b \diamond a$

heißt $(G, \diamond)$ abelsch (kommotativ).

Definition 2.3

1. Eine Gruppe $(G, \diamond)$ heißt endliche Gruppe, falls G nur endlich viele Elemente enthält.
2. Gelten nur $(G') \wedge (G2)$, so heißt $(G, \diamond)$ eine Halbgruppe.

Bemerkung

1. Oft abkürzend G oder $(G, \diamond, e)$ statt $(G, \diamond)$ und ab statt $a \diamond b$
2. $G \neq \varnothing$ wegen $(G3)$

Beispiel 2.4

1. $(\mathbb{Z}, +, 0), (\mathbb{R}, +, 0), (\mathbb{Q}\backslash\{0\}, ., 1)$ Gruppen
2. $(\mathbb{N}, +), (\mathbb{Z}, *)$ sind keine Gruppen wegen $(G4)$
3. $(\mathbb{Q}\backslash\{0\}, /)$

G1 Für beliebige $a, b \in \mathbb{Q}$ gilt $a/b \in \mathbb{Q}$ denn $a, b \in \mathbb{Q}, b \neq 0$ und $a/b \neq 0$, da $a \neq 0 \rightarrow (G1)$

G2 $100, 20, 5 \in \mathbb{Q}\backslash\{0\}$ aber $(100/20)/5 = 5/5 = 1$

$\neq 100/(20/5) = 100/4 = 25$ also gilt nicht $(G2)$

G3 Für $e := 1$ gilt $1 \in \mathbb{Q}\backslash\{0\} \wedge \forall a \in \mathbb{Q}\backslash\{0\} : 1/a \neq a$ Mit $a = 2 \in \mathbb{Q}\backslash\{0\}$ folgt $1/2 \neq 2$ d.h e ist kein neutrales Element.

G4 sinnlos ohne (G3)

Beispiel 2.5

$\mathbb{Z}_2 = \{[0], [1]\}, [a] \oplus [b] =: [a + b]$

$[0] \oplus [0] = [0], [0] \oplus [1] = [1], [1] \oplus [0] = [1], [1] \oplus [1] = [0]$

$\oplus$	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

G1 $\forall a, b \in \mathbb{Z}_2 a \diamond b \in \mathbb{Z}_2$

G2 Brutalst-Mögliches Nachrechnen:

$([0] \oplus [0]) \oplus [0] = [0] \oplus [0] = [0] = [0] + [0] = [0] + ([0] + [0])$ richtig

$([0] \oplus [0]) \oplus [1] = [0] \oplus [1] = [1] = [0] + [1] = [0] + ([0] + [1])$ richtig

$([0] \oplus [1]) \oplus [0] =$

G3 $[0] \in \mathbb{Z}_2 \wedge [0] \oplus [0] = [0] \wedge [0] \oplus [1] = [1]$

G4 $[0]$ ist invers zu $[0][0] \oplus [0] = [0]$,

$[1]$ ist invers zu $[1][1] \oplus [1] = [0]$,

G1-G4 $\rightarrow (\mathbb{Z}_2, \oplus)$ Gruppen.

G5 : $[0] \oplus [1] = [1] \oplus [0] \rightarrow \mathbb{B}$ ist ablsch. , $\mathbb{B} := \mathbb{Z}_a$

Beispiel 2.6

Die Menge $\mathbb{R}^n$ mit der Verknüpfung $+$ ist eine abelsche Gruppe

$$\mathbb{R}^n = \{x := \begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix} : x_j \in \mathbb{R}, j = 1, ..., n\}, + : \mathbb{R}^n x \mathbb{R}^n \rightarrow \mathbb{R}^n, (x, y) \rightarrow (x + y) := \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ ... \\ x_n + y_n \end{pmatrix}$$

G1 Klar

G2 folgt aus der Assoziation in $\mathbb{R}$

G3 Das neutrale Element ist $0 := (0, ..., 0)$

G4 Eine zu $x = \begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix}$ inverses Element ist $x' = \begin{pmatrix} -x_1 \\ ... \\ -x_n \end{pmatrix} =: -x \rightarrow$

G5 Folgt aus Kommutativ-Gesetzt in $\mathbb{R}$

Beispiel 2.7

[Komplexe Zahlen, wird fortgeführt]

$G = \mathbb{R}^2 = \{\binom{x_1}{x_2} : x_1, x_2 \in \mathbb{R}\}$ mit der Verknüpfung $\odot : \mathbb{R}^2 x \mathbb{R}^2 \rightarrow^2, \binom{x_1}{x_2} \odot \binom{y_1}{y_2} := \binom{x_1y_1 - x_2y_2}{x_1y_2 + x_2y_1} \in \mathbb{R}^2$

Dann ist $\mathbb{R}^2 \backslash \{0\}$ eine abelsche Gruppe: Übung!

Beispiel 2.8

Die Symmetrische Differenz von Mengen

X eine Menge

$\triangle : P(x)xP(x) \rightarrow P(x), (M, N) \rightarrow M \triangle N := (M \cup N) \backslash (M \cap N)$ ist abelsche Gruppe, Übung.

Satz 2.9.1

Sei $(G, \diamond)$ eine Gruppe mit einem neutralen Element e. Es gilt:

1. $\forall a \in G : a \diamond e = a$, d.h neutrales Element vertauscht in der Abbildung.
2. $\exists! e \in G : \forall a \in G : e \diamond a = a$, d.g neutrales Element eindeutig bestimmt.
3. Ist $a' \in G$ ein inverses zu a $\in G$, dann gilt : $a \diamond a' = e$, IE vertauscht!
4. $\forall a \in G : \exists! a' \in G : a \diamond a = e$, d..h IE eindeutig bestimmt.

Beweis

Sei $a \in G$ beliebig, a' ein beliebig Inverses zu a, e ein beliebig NE, sodass $a' \diamond a = e'$

zu 3: Da G eine Gruppe ist, gilt es ein zu a' inverses Element $a'' \in G$ sodass $a'' \diamond a' = e'$

Unter Verwendung der Gruppenmaxime rechnen wir nach $a \diamond a' = e' \diamond (a \diamond a')$ (e' ist NE)

$= (a'' \diamond a') \diamond (a \diamond a')$ ($e' = a'' \diamond a'$) =($a'' \diamond ((a' \diamond a) \diamond a')$ Assoziativ

$a'' \diamond (e' \diamond a')$ ($e' = a' \diamond a$)

$a'' \diamond a'$ (e' NE)

e' ($e' = a'' \diamond a'$)

Also kommutiert das inverse

Zu 1 $a \diamond e' = a \diamond (a' \diamond a)$ $(e' = a' \diamond a)$

$= (a \diamond a') \diamond a$ $(assoziativ)$

$= e' \diamond a$ (wegen Teil 3 $e' = a \diamond a'$)(e' ist NE)

Also kommutiert ein neutrales Element.

zu 2:

Wir zeigen: sind e, e' neutrale Elemente, folgt $e = e'$

$e' = e \diamond e'$ (e ist NE)

$= e$ (e' ist NE und Teil).

zu 4:

Seien $a, a', a'' \in \mathbb{G}$ mit $a' \diamond a = e \wedge a''a = e$

Wir zeigen : $a' = a''$: $a'' = a'' \diamond e$ (e ist NE und Teil 1)

=$a'' \diamond (a \diamond a')$ $(e = a' \diamond a = a \diamond a'$ Teil 3)

=$a'' \diamond a) \diamond a'$ Assoziativ-Gesetzt

$= e \diamond a'$ (a'' IE:$a'' \diamond a = e$)

a' (e ist NE) □

Satz 2.9.2

Rechtfertigt den Sprachgebrauch das <u>neutrale Element</u> bzw. das <u>inverse Element</u> nachträglich.

Gruppen sind die algebraischen Strukturen, in denen Wir Gleichungen lösen können.

Satz 2.10

Gegeben eine Menge $G \neq \varnothing$ und eine Abbildung $\diamond : GxG \to G$

Folgende Aussagen sind Äquivalent:

1. $(G, \diamond)$ ist Gruppe.
2. Es gilt das Assoziativ-Gesetz $(G2) \wedge \forall a, b \in G \exists! x \in G \exists! y \in G : x \diamond a = b \wedge a \diamond y = b$

Beweis

1. $\to 2)$: Offenbar gilt $(G2)$ weiter gilt für beliebig $a, b \in G, x \diamond a = b \to x = b \diamond a$‘ und $a \diamond y = b \to y = a' \diamond b$

   Lösung der Gleichung existieren, zu zeigen beleibt die Eindeutigkeit.

   Seien also $u, v \in G$ mit $u \diamond a = b \wedge a \diamond v = b$ Dann folgt : $u = u \diamond e = u \diamond (a \diamond a') = (u \diamond a) \diamond a' = b \diamond a' = x$ bzw. $v = e \diamond v = (a' \diamond a) \diamond v = a' \diamond (a \diamond v) = a' \diamond b = y$, d-h Lösung eindeutig. $\square$

Beweis

$2 \to 1$: $(G1)$ und $(G2)$ gelten nach Voraussetzung. zu zeigen: $(G3)$ und $(G4)$

Wähle $b \in G$ und setze $a = b$ in "$x \diamond a = b$" : $\exists! x \in G$ mit $x \diamond a = a$.

Wir machen den Ansatz $e := x$. Für beliebiges $b \in G$ folgt mit $a \diamond y = b$ und $x \diamond a = b$

$e \diamond b = e \diamond (a \diamond y) = (e \diamond a) \diamond y = a \diamond y = b$ und damit gilt $(G3)$

Wir setzen in den Gleichung $b := e$ dann folgt : $\forall a \in G, \exists! x \in G : x \diamond a = e$, also ist x invers zu a, und damit gilt $(G4)$

Zusammen $(G1 - G4)$ und also G Gruppe. $\square$

8 Vektoren und Matrizen

Definition 2.11

Ein Schema der Gestalt: A:= $\begin{pmatrix} a_{1,1} & a_{1,1} \\ a_{2,1} & a_{2,2} \end{pmatrix}$, $a_{i,j} \in \mathbb{R}, i, j \in \{1, 2\}$ heißt eine 2x2 Matrix, $a_{i,j}$ eine Komponente oder Eintrag von $A, i, j \in \{1, 2\}$ Die Menge 2x2 Matrizen bezeichnen wir mit:

$\mathbb{R}^{2,2} := \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} : a_{i,j} \in \mathbb{R}, i, j \in \{1.2\}$

Im Gegensatz zu Vektoren $x \in \mathbb{R}^2$(Tupel aus dem $\mathbb{R}^2$) werden Matrizen mit großen latainischen Buchstaben (A,B,...) abgekürzt.

Auf der Menge $\mathbb{R}^{2,2}$ definieren wir folgende Abbildung:

1. Addition von Matrizen. $\oplus : \mathbb{R}^{2,2} x \mathbb{R}^{2,2} \to \mathbb{R}^{2,2}$,
   $\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \oplus \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix} := \begin{pmatrix} a_{1,1} + b_{1,1} & a_{1,2} + b_{1,2} \\ a_{2,1} + b_{2,1} & a_{2,2} + b_{2,2} \end{pmatrix}$
2. Skalarmultiplikation :

   $\mathbb{R} x \mathbb{R}^{2,2} \to \mathbb{R}^{2,2}, \lambda * \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{1,2} & b_{2,2} \end{pmatrix} := \begin{pmatrix} \lambda * b_{1,1} & \lambda * b_{1,2} \\ \lambda * b_{1,2} & \lambda * b_{2,2} \end{pmatrix}$
3. Vektormultiplikation:

   $* : \mathbb{R}^{2,2} x \mathbb{R}^2 \to \mathbb{R}^2 \begin{pmatrix} b_{1,1} & b_{2,1} \\ b_{1,2} & b_{2,2} \end{pmatrix} * \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} := \begin{pmatrix} x_1 * b_{1,1} + x_2 * b_{1,2} \\ x_1 * b_{1,2} + x_2 * b_{2,2} \end{pmatrix}$
4. Matrizenmultiplikation:

   $* : \mathbb{R}^{2,2} x \mathbb{R}^{2,2} \to \mathbb{R}^{2,2} : \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{pmatrix} * \begin{pmatrix} b_{1,1} & b_{2,1} \\ b_{1,2} & b_{2,2} \end{pmatrix}$
   $= \begin{pmatrix} a_{1,1} * b_{1,1} + a_{1,2} * b_{2,1} & a_{1,1} * b_{1,2} + a_{1,2} * b_{2,2} \\ a_{2,1} * b_{1,1} + a_{2,2} * b_{1,2} & a_{2,1} * b_{1,2} + a_{2,2} * b_{2,2} \end{pmatrix}$

Lemma 2.12

Seien $A, B, C \in \mathbb{R}^{2,2}, x, y \in \mathbb{R}^2$ Es gilt:

1. $A * (x + y) = (A * x) + (A * y)$
2. $(A \oplus B) * x = (A * x) + (B * x)$
3. $(A \odot B) * x = A * (B * x)$
4. $(A \oplus B) \odot C = (A \odot C) \oplus (B \odot C)$

5. $(A \odot B) \odot C = A \odot (B \odot C)$
6. Mit der Einheitsmatrix $E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ gilt $E \odot A = A \odot E = A$
7. Die Matrizenmultiplikation ist nicht Kommutativ!

Beweis

Zu 7:

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \odot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \odot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \qquad \square$$

Beispiel 2.13

Addition von Matrizen-Gruppen

Mit der Nullmatrix $0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{R}^{2,2}$ als Neutrales Element bildet $(\mathbb{R}^{2,2}, \oplus, 0)$ eine abelsche Gruppe (Nachrechnen!)

Beispiel 2.14

Das Tripel $(\mathbb{R}^{2,2}, \odot, E)$ ist keine Gruppe!

Problematisch sind die Inversen.

Sei z.B. $A = \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix}$ Gesucht ein $A' = \begin{pmatrix} a'_{1,1} & a'_{1,2} \\ a'_{2,1} & a'_{2,2} \end{pmatrix} \in \mathbb{R}^{2,2}$ mit $A' \odot A = E$

Es gilt:

$$A' * A = \begin{pmatrix} a'_{1,1} & a'_{1,2} \\ a'_{2,1} & a'_{2,2} \end{pmatrix} \odot \begin{pmatrix} 0 & 1 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & a'_{1,1} + 2 * a'_{1,2} \\ 0 & a'_{2,1} + 2 * a'_{2,2} \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Allgemeiner stellt sich die Frage, welche Matrizen haben Inverse? $\begin{pmatrix} a'_{1,1} & a'_{1,2} \\ a'_{2,1} & a'_{2,2} \end{pmatrix} \odot \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = \begin{pmatrix} a'_{1,1} * a_{1,1} + a'_{2,1} * a_{2,1} & a'_{1,1} * a_{1,2} + a'_{1,2} * a_{2,2} \\ a'_{2,1} * a_{1,1} + a'_{2,2} * a_{2,2} & a'_{2,1} * a_{1,2} + a'_{2,2} * a_{2,2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$a'_{1,1} * a_{1,1} + a'_{2,1} * a_{2,1} = 1 | * a_{2,2} \rightarrow a'_{1,1} * a_{1,1} * a_{2,2} + (a'_{1,2} * a_{2,1} * a_{2,2} = a_{2,2}(A)$

$a'_{1,1} * a_{1,2} + a'_{1,2} * a_{2,2} = 0 | * a_{2,1} \rightarrow a'_{1,1} * a_{1,2} * a_{2,1} + a'_{1,2} * a_{2,1} * a_{2,2} = 0(B)$

$a'_{2,1} * a_{1,1} + a'_{2,2} * a_{2,2} = 0 | A - B \rightarrow a'_{1,1} * (a_{1,1} * a_{2,2} - a_{1,2} * a_{2,1} = a_{2,2}$

$a'_{2,1} * a_{1,2} + a'_{2,2} * a_{2,2} = 1$

$a'_{1,1} = \frac{1}{det} a'_{2,2}$

$a'_{1,2} = \frac{1}{det} a'_{1,2}$

$a'_{2,1} = \frac{1}{det} a'_{2,1}$

$a'_{2,2} = \frac{1}{det} a'_{1,1}$

Mit Analogen Argumenten folgt det $= a_{1,1} * a_{2,2} - a_{1,2} * a_{2,1} \neq 0$

Da $x * 0 = b$(x bel.)

Lemma 2.15

Sei $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$ mit det $:= a_{1,1} * a_{2,2} - a_{1,2} * a_{2,1} \neq 0$ und $A' := \frac{1}{det} \begin{pmatrix} a_{1,1} & -a_{1,2} \\ -a_{2,1} & a_{2,2} \end{pmatrix}$

Damit gilt : $A' \odot A = A \odot A = A \odot A' = E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Beweis: Nachrechnen !

Für $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ gilt det $?1 * 4 - 2 * 3 = -2 \neq 0$ und $A' = \frac{1}{2} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$

Definition 2.16

Als Generalized Linear Group über $\mathbb{R}$ bezeichnen wir die Menge $GL_2(\mathbb{R}) := \{ \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \in \mathbb{R}^{2,2}$ det : $a_{2,2} a_{1,1} - a_{2,1} * a_{2,1} \neq 0\}$

Satz 2.17

$GL_2(\mathbb{R}), \odot, E)$ ist eine nicht abelsche Gruppe.

9 Abbildung und Permutation

Aussage

Sei $M \neq \varnothing$, Abbildung $(M, R) := \{f : M \to \mathbb{R}\}$

$\oplus$: Abbildung $(M, \mathbb{R}) x$ Abbildung $(M, \mathbb{R} =\to$ Abbildung $(M, \mathbb{R})$

$(f, x) \to f \oplus g$ wobei $f \oplus g : M \to \mathbb{R}$ mit $f \oplus g(x) := f(x) + g(x)$

Die Nullabbildung $O : M \to \mathbb{R}, O(x) := 0$ ist das Neutrale Element von (Abbildung$(M, \mathbb{R}), \oplus)$

und das Inverse zu $f \in$ Abbildung $(M, \mathbb{R})$ ist $-f : M \to \mathbb{R}, (-f)(x) := -f(x)$.

(Abbildung $(M, \mathbb{R}) \oplus, 0)$ ist Abelsche Gruppe.

Spezialfälle:

Polynome von Höchstens n mit reellen Koeffizienten:

$\Pi_n(\mathbb{R}) := \{p : \mathbb{R} \to \mathbb{R} p(x) = \sum_{j=0}^{n} a_j x^j, a_j \in \mathbb{R}, j = 0, \ldots, n\}$

$\Pi_n \subseteq$ Abbildung $(\mathbb{R}, \mathbb{R})$, Add.

$\Pi_n(\mathbb{R}) \ni p, q : (p \oplus q)(x) = p(x) + q(x) = \sum a_j x^j + \sum b_j x^j$

$\Pi_n(\mathbb{R}) \ni 0, \sum 0 x^j$

$= \sum (a_j + b_j) * x^j$

$= 0 f$ alle $x \in \mathbb{R}$, d.h Nullpolynom.

Satz 2.18 (Symmetrische Gruppe)

Sei $M \neq \varnothing$ und $S(M) := \{f : M \to M, f$ bijektiv$\}$

$\circ : S(M) x S(M) \to S(M), f - g(x) := f(g(x))$

Dann ist $(S(M), \circ, id_M)$ eine nicht-abelsche Gruppe und wird als Symmetrische Gruppe bezeichnet.

Satz 2.18

(Sym. Gruppen)

Sei $M \neq \varnothing$ eine Menge und $S(M) := \{f : M \to M, f$ bij $\}$

$\circ : S(M) x S(M), f \circ g(x) := f(g(x)) f$ alle $x \in M$.

Dann ist $(S(M), \circ, id_m)$ eine i.a. nict abelsche Gruppe und wird als Symmetrische Gruppe bezeichnet

Beweis

Wir nur Skizziert (Übung); Kernelement Satz 1.39:

(G1) $f, g \in S(M) \to f \circ g \in S(M)$

(G2) $(h \circ g) \circ f(x) = h \circ g(f(x)) = h \circ (g \circ f)(x) = f \circ (g \circ f(x) = f$ alle $x \in M$

(G3) $id_M : M \to M, id_M bij$, d.h.$id_M \in S(M), id_M \circ f = f$

(G4) Zu $f \in S(M)$ existiert $f^{-1} \in S(M), f^{-1} \circ f = dm_m$

$S(M)$ nicht abelsch:

$M := \{0, 1\}, f, g : M \to M, f(x) := 1 - x, g(x) := x^2$

$f \circ g(x) = f(g(x)) - 1 - x^2 = g \circ f(x) = (1 - x)^2 = 1 - 2x + x^2$

Permutation bilden wichtigen Spezialfall, hier $M := M_n := \{1, \ldots, n\} M_3 = \{1, 2, 3\}$

$S_n := S(M_n) := \{f : M_n \to M_n, f \text{ bij } \} S_3$

$f : M_3 \to M_3, f(1) = a, f(2) = b, f(3) = c, \begin{pmatrix} 1 & 2 & 3 \\ a & b & c \end{pmatrix}, [a, b, c]$

So hat $3! = 6$ Elemente, die sog. Permutation

$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$

$M_3 = \{1, 2, 3\}$

S_3

$$f_2 \circ f_2 = f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$f_3 \circ f_3 = f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$$f_4 \circ f_5 = f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

$f_5 \circ f_4 ? f_1$, Inverses Kommutieren!

$$f_6 \circ f_6 = f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \circ f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = f_1$$

Auch S_3 ist nicht abelsch:

$$f_3 \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = f_2$$

$$\neq f_4 \circ f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = f_6$$

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	$\bullet$	$\bullet$	$\bullet$	$\bullet$
f_3	f_3	$\bullet$	f_1	$\bullet$	f_2	$\bullet$
f_4	f_4	$\bullet$	f_6	$\bullet$	f_1	$\bullet$
f_5	f_5	$\bullet$	$\bullet$	f_1	$\bullet$	$\bullet$
f_6	f_6	$\bullet$	$\bullet$	$\bullet$	$\bullet$	f_1

$\square$

10 Rechnen in Gruppen, endliche Gruppe, Untergruppen

Lemma 2.19

(Kürzungsregeln)

In einer Gruppe $(G, \diamond)$ gilt:

$\forall a, b, c \in G : a \diamond b = a \diamond c \leftrightarrow b = c$

Beweis

Zu $'' \rightarrow''$ $.b = e \diamond b = (a' \diamond a) \diamond b = a' \diamond (a \diamond c) = (a' \diamond a) diamond c = e \diamond c = c$

zu $'' \leftarrow''$ folgt unmittelbar durch Verkettung mit a □

Lemma 2.20

In einer Gruppe $(G, \diamond)$ gilt :

1. $\forall a \in G : (a') = a$
2. $\forall a, b, \in G : (a \diamond b)' = b' \diamond a'$

Beweis

zu 1. Nach Satz 2.9.4 existiert zu jedem $a \in G$ genau ein Inverses $a' \in G$ und zu $a' \in G$ genau ein Inverses $(a')' \in G$ Mit Satz 2.9.3 $a \diamond a' = e = (a')' \diamond a' \rightarrow$ (Lemma 2.19)$a = (a')'$

zu 2: $(b' \diamond a') \diamond (a \diamond b) = b' \diamond (a' \diamond (a \diamond b)) = b' \diamond ((a' \Diamond a) \diamond b)$

$= b' \diamond (e \diamond b) = b' \diamond b = e$ Also $(a \diamond b)' = b' \diamond a$. □

Definition 2.21

Sei $(G, \diamond, e)$ eine Gruppe: Für $a \in G$ def. wir:

1. $a^0 = e$
2. $a^k := a \diamond a^{k-1}$ für $k \in \mathbb{N}$
3. $a^{-k} := (a')^k$ für $k \in \mathbb{N}$

Das Element $a^k, k \in \mathbb{Z}$ heißt die kte Potenz von $a \in G$

Lemma 2.22

Sei $(G\diamond, e)$ eine Gruppe, $a \in G$ und $k \in \mathbb{N}$. Es gilt

1. $a \diamond a^{k-1} = a^{k-1} \diamond a$,
2. $a^{-k} = (a')^k = (a^l)'$

Beweis

Mit VI

1. $\forall k \in \mathbb{N} : A(k), A(k) := [a^k = a \diamond a^{k-1} = a^{k-1} \diamond a]$

IA Für $k = 1, a^1 = a \diamond a^0 = a \diamond e = a = e \diamond a)a^0 \diamond a\surd$

IV Für ein beliebiges $k \in \mathbb{N}$ gelte $A(k)$

IS Wir zeigen $A(k+1)$ ist wahr: $a^{k+1} = a \diamond a^k = a \diamond (a^{k-1} \diamond a) = (a \diamond a^{k-1}) \diamond a = a^k \diamond a$

VI folgt aus IA,IV,IS.

2. $a^{-k} \diamond a^k = (a')^k \Diamond a^k ?((a')^{k-1} \diamond a') \diamond (a \diamond a^{k-1}) = (a')^{k-1} \diamond (a' \diamond a) \diamond a^{k-1} = (a')^{k1} \Diamond a^{k-1} = a' \diamond a = e$ □

Lemma 2.23

Sei$(G, \diamond, e)$ eine Gruppe, $a \in G, m, n \in \mathbb{Z}$ Es gilt:

1. $a^n \diamond a^m = a^{n+m}$
2. $(a^m)^n = a^{m*n}$

Beweis

zu 1. Sei $m \in \mathbb{Z}$ beliebig aber fest gewählt. MIt VI: $\forall n \in \mathbb{N}_0 : A(n), A(n) := [a^n \diamond a^m = a^{n+m}]$

IA Wir zeigen $A(0)$ ist wahr: $a^0 \diamond a^m = e \diamond a^m = a^m = a^{0+m}$

IV Für beliebiges $n \in \mathbb{N}_0$ gilt $A(n)$

IS Wir zeigen $A(n+1)$ ist wahr:

$a^{n+1} \diamond a^m = (a \diamond a^n) \diamond a^m a \diamond (a^n \diamond a^m) = a \diamond a^{m+n} = a^{n+m+1} = a^{(n+1)+m}$

Mit VI folgt Behauptung f alle $n \in \mathbb{N}_0$

Wir zeigen nun, dass für $n \in \mathbb{N}_0 : a^{-n} \diamond a^m = a^{-n+m}$

$a^{-n} \diamond = (a')^n \diamond (a')^{-m} = (a')^{n-m} = a^{-m+n}$

Zusammen folgt Behauptung 1. Teil 2 zur Übung. □

Beispiel 2.24

1. $(\mathbb{Q}\backslash\{0\}, *, 1)$

   $(5^2)^3 = (5*5)^3 = (5*5)*(5*5)*(5*5) = 5^6 = 5^{2*3} = 15625$

2. $(\mathbb{Z}, +, 0)$: Für $x \in \mathbb{Z} \to x' := -x$ und $(x')' = -(-x) = x$

   Google fasst du es nicht verstehst... -.-

Lemma 2.25

Für eine endliche Gruppe $(G, \diamond, e)$ gilt:

$\forall a \in G \exists n \in \mathbb{N} : a^n = e$

Beweis

Sei $a \in G$ beliebig. Da es nur endlich viele Elemente in G gibt, können nicht alle Potenzen von a verschieden sein, das heißt. $\exists p, q, \in \mathbb{N} : p \neq q \wedge a^p = a^q$

und ohne Einschränkung $p > q$ $\square$

Lemma 2.24

$a^{p-q} = a^p \diamond a^{-q} = a^q \diamond a^{-q} = a^{q-q} = a^0 = e$

Woraus mit $n := p - q$ folgt $n \in \mathbb{N} \wedge a^n = e$.$\square$

Definition 2.26

Die Anzahl der Elemente einer endlichen Gruppe G heißt die Ordnung von G oder Gruppenordnung. Für $a \in G$ heißt die kleinste Zahl $m \in \mathbb{N}$ mit $a^m = e$ die Ordnung von a bezüglich G

Beispiel 2.27

$M_3\{1, 2, 3\}$ und $S_3 = \{f : M_3 \to M_3, fby\}$

S_3 hat die Ordnung 6, f_4 hat die Ordnung $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$f_4 = e, f_4' = f_4$

$f_4^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$$f_4^3 = f_4^2 \circ f_4 = f_4 \circ f_4^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Definition 2.28

Sei $(G, \diamond, e)$ eine Gruppe und $H \subseteq G \vee H \neq \varnothing$.

Ist $(H, \diamond)$ eine Gruppe, dann heißt $(H, \diamond)$ eine Untergruppe von G.

Satz 2.29 (Untergruppenkriterium)

Die Menge $H \subseteq G$ ist genau dann U-Gruppe von $G = (G, \diamond, e)$ wenn:

1. $H \neq \varnothing$
2. $\forall a, b \in H : a \diamond b \in H$
3. $\forall a \in H : a' \in H \wedge a' \diamond a = e$

Beweis

$'' \Rightarrow''$ Klar!

$'' \Leftarrow''$

(G1) folgt aus 2

(G2) folgt aus (G2) für G.

(G3) Mit 1 folgt: $\exists a \in H$, mit 3 folgt $\exists a' \in H$ und mit ...

(G4) folgt aus 3. □

Lemma 2.30

Die Menge $H \subseteq G$ ist genau dann U-Gruppe von $G = (G, \diamond, e)$ mit G endlich, wenn:

1. $H \neq \varnothing$
2. $\forall a, b \in H : a \diamond b \in H$

Beweis

Wegen Satz 2.29 bleibt zu zeigen: $a \in H \Rightarrow a' \in H$

Sei $a \in H$ bel. mit $a \neq e$ mit der Ordnung m, d.h. $a^m = e$

Ist $m = 1$, gilt $a = e \wedge a' = e = a \in H$.

Andernfalls ist $m > 1$ und Teil 2 impliziert $a^p \in H$ für alle $p \in \mathbb{N}\not{}$.

Also gilt $a \diamond a^{m-1} \in H$. □

Lemma 2.31

Sei $(G, \diamond, e)$ eine endl. Gruppe und $a \in G$ mit Ordnung m. Die Menge $H(a) := \{a^n : n \in \mathbb{Z}\} \subseteq G$ ist eine endl. U-Gruppe von G der Ordnung m, $H(a) = e, a^1, ..., a^{m-1}$.

Beweis

1. Da $e = a^n$ ist $H(a) \neq \varnothing$
2. Seien $b, c \in H(a)$, d.h. es gibt Zahlen $p, q \in \mathbb{Z}$ mit $b = a^p \wedge c = a^{-q}$

   Damit folgt $b \diamond c = a^p \diamond a^{-q} = a^{p-q} \in H(a)$
   Lemma 2.30 impliziert: $H(a)$ ist U-Gruppe von G.

   Für bel. $n \in \mathbb{Z}$ gibt es eindeutig bestimmte Zahlen $p, r \in \mathbb{Z} : n = p * m + r \wedge r \in \{0, 1, ..., m-1\}$ daher gilt $a^n = a^{pm+r} = (a^m)^p \diamond a^r = e^p \diamond a^r = e \diamond a^r = a^r$, d.h. $H(a) = \{a^r, r \in \{0, 1, ..., m-1\}\}$ oder die Ordnung von H ist m. □

Definition 2.32

Sei G eine endl. Gruppe und $a \in G$. Die Menge $H(a) := \{a^n : n \in \mathbb{Z}\} \subseteq G$ heißt zyklische Gruppe von a.

Beispiel 2.33

S_3 hat Ordnung 6, f_4 hat Ordnung 3,
$H(f_4) = \{id_{M_3}, f_4, f_4^2\}$ ist U-Gruppe der S_3 der Ordnung 3.

Satz 2.34 (Satz von Lagrange)

Sei $(G, \diamond, e)$ endl. Gruppe und H U-Gruppe von G.

Dann teilt die Ordnung von H die Ordnung von G, $|G|/|H| \in \mathbb{N}$.

Beweis

Wir generieren eine Partition on G, wobei jedes Element der Partition genau m Elemente enthält, m die Ordnung von H. Aus den Eigenschaften der Partition folgt dann die Beh.

Wir zeigen $R := \{(a,b) \in G^2 : a \diamond b' \in H\}$ ist Äquivalenzrelation in G.

Refl.: $\forall a \in G : aRa \Leftrightarrow a \diamond a' = e \in H$. w.A.

Sym.: $\forall a, b \in G : aRb \Rightarrow bRa : aRb \Leftrightarrow a \diamond b' \in H \Leftrightarrow (a \diamond b')' = (b')' \diamond a' = b \diamond a' \Leftrightarrow bRa$

Trans.: $\forall a, b, c \in G : aRb \wedge bRc \Rightarrow aRc : aRb \wedge bRc \Leftrightarrow a \diamond b' \in H \wedge b \diamond c' \in H \Rightarrow a \diamond c' = a \diamond b' \diamond b \diamond c' \in H \Leftrightarrow aRc$

R ist Äquivalenzrelation

Bezeichne $[b]$ die Äquivalenzklasse zu $b \in G$ bel.

Nun gilt $x \in [b] \Leftrightarrow u := x \diamond b' \in H \Leftrightarrow x = u \diamond b$, d.h. $[b] = \{u \diamond b : u \in H\} =: H \diamond b$

Wir zeigen $|H \diamond b| = |H| = m$ durch Konstruktion einer bij. Abbildung $f : H \to H \diamond b$ mit $f(u) := u \diamond b$.

Es gilt f injektiv: $f(u) = f(v) \Leftrightarrow u \diamond b = v \diamond b \Leftrightarrow u = v$

f surjektiv: $\forall w \in H \diamond b \exists u \in H : u \diamond b = w$

Also ist f bij. und alle Mengen $H \diamond b$ haben m Elemente, $m = |H|$.

Aus der Partition $G = \bigcup_{b \in G} [b$ und der Endlichkeit von G folgt: es gibt ein $p \in \mathbb{N}$ mit $|G| = pm$, d.h. $|G| = p|H|$ bzw. $|G| \backslash |H| = p \in \mathbb{N}$ □

10.1 Restklassengruppen

Wiederholung: $\mathbb{N} \ni m$ Modul

Für $x, y \in \mathbb{Z} : x \equiv y \mod m$

$\Leftrightarrow m|(x-y)$

x, y bei Division durch m denselben Rest.

$23 = 3 * 7 + 2$

$23 = 1.12 + 11$

$\forall z \in \mathbb{Z} \exists ! p \in \mathbb{Z} \exists ! r \in \{0, \dots, m-1\} : z - p * m + r$

$[x]_m := \{y \in \mathbb{Z} : x \equiv \mod m\}$

$\mathbb{Z}_m := \{[m]_m : x \in \mathbb{Z}\} = \{[0]_m, \dots, [m-1]_m\}$

Satz 1.71: $a \equiv x \mod m \wedge b \equiv y \mod m$

$a \pm b \equiv x \pm y \mod m$

$a * b \equiv x * y \mod m$

Sind p, q, prim, $m = p * q$ dann gilt :

$x \equiv y \mod m \Leftrightarrow [x \equiv y \mod p \wedge x \equiv y \mod q]$

$\oplus : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, [a]_m \oplus [b]_m := [a+b]_m$

$\odot : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, [a]_m \odot [b]_m := [a*b]_m$

Satz 2.35

Für jedes $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, [0]_m, \oplus)$ eine endliche abelsche Gruppe der Ordnung m

Beispiel 2.36

1. $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$ hat Gruppentafel:

$\oplus$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[-2]_2$

$= [0]_2$

2. $(\mathbb{Z}_m, \odot)$ und $m = 3$

$\odot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

$[1]_3$ ist ein "NeutralesËlement
$[0]_3$ hat kein Inverses
$(\mathbb{Z}_3, 0)$ ist keine Gruppe

Aber mit $\mathbb{Z}_3^* := \mathbb{Z}_3 \backslash \{[0]_3\}$ ist $(\mathbb{Z}_3^*, \odot, [1]_3)$ ist eine Gruppe der Ordnung 2.

3. $(\mathbb{Z}_m^*, \odot)$ ist nicht für jede $m \in \ltimes$ eine Gruppe . Z.B. für $m = 4 : [2]_4 \in \mathbb{Z}_4^*$ aber $[2]_4 \odot [2]_4 ? [0]_4 \notin \mathbb{Z}_4^K$

Satz 2.37

Sei $p \in \mathbb{N}$ prim. Dann ist $(\mathbb{Z}_p^*, \odot)$ eine endliche abelsche Gruppe der Ordnung $p-1, \mathbb{Z}_p^* := \mathbb{Z}_p \backslash \{[0]_p\}$

Beweis

(GI) Seien $[a], [b] \in \mathbb{Z}_p^*$ beliebig, dann gilt $[a] \odot [b] = [a*b] \in \mathbb{Z}_p$

Angenommen $[a*b] = [0]$, dann gilt es ein $k \in \mathbb{Z}$ mit $a*b = k*p$, d.h $p|ab$

Da p prim folgt $p|a \vee p|b$

$\Rightarrow [a] = [0] \vee [b] = [0]$ ein Widerspruch zu $[a], [b] \in \mathbb{Z}_p^*$.

(G2) Für beliebigen $[a], [b], [c] \in \mathbb{Z}_p^*$ gilt: $([a] \odot [b]) \odot [c] = [a*b] \odot [c] = [a*b*c] = [a] \odot [b*c] = [a] \odot ([b] \odot [c]) \surd$

(G3) Zunächst gilt: $[1] \in \mathbb{Z}_p^*$; weiter gilt: $\forall [a] \in \mathbb{Z}_p^* : [1] \odot [a] = [1*a] = [a]$

(G4) Sei $[a] \in \mathbb{Z}_p^*$ beliebig. Da p prim folgt $p \nmid a$ und $ggT(a,p) = 1$

Der Euklidische Algorithmus garantiert Zahlen $x, y \in \mathbb{Z}$ mit $1 = ggT(a,p) = a * x + p * y$

Beispiel:

$ggT(16,3) = 1 = 1 * 16 - 5 * 3 \Rightarrow [1] * [16] = [1]$

Also $1 \equiv x * a \mod p \Rightarrow [1] = [xa] = [x] \odot [a] \Rightarrow [a]' = [x]$

Weiter gilt $[x] \neq [0]$ denn $[0] \odot [a] = [0] \neq [1]$, d.h $[x] \in \mathbb{Z}_p^*$

Ordnung $\mathbb{Z}_p^* = \{[1]_p, \ldots, [p-1]_p\} \Rightarrow |\mathbb{Z}_p^*| = p - 1,$ □

Bemerkung

Fermats letzter (großer) Satz: Sei $m \in \mathbb{N}$. Dann gilt f , alle $x, y, z \in \mathbb{Z}^* : x^n + y^n = z^n \Rightarrow n \leq 2$

Beweis John Wiles 1994

Mit Satz 2.37 gelingt aber der Beweis des *kleinen* Satzen von Fermat

Satz 2.38 (Kleiner Satz von Fermat)

Sei p prim und $a \in \mathbb{N}$. Dann gilt $a^p \equiv a \mod p$

Falls $p \nmid a$ gilt auch $a^{p-1} \equiv 1 \mod p$ (Hauptaussage)

Beweis

1. $p|a$

   d.h $a \equiv 0 \mod p \overset{Satz 1.71}{\Rightarrow} a^p \equiv 0 \mod p \wedge 0 \equiv a \mod p$ Zusammen $a^p \equiv a \mod p$

2. $p \nmid a$. Wir machen 5 Teilschritte:

2.1 Satz 2.37 garantiert $(\mathbb{Z}_p^*, \odot)$ ist abelsche Gruppe der Ordnung $p - 1$.

2.2 Lemma 2.31 garantiert : $H(a) := \{[a]_p^n : n \in \mathbb{Z}\}$ ist eine U-Gruppe von $\mathbb{Z}_p^*$

Sei $k := |H(a)|$, mit dem Satz von Lagrange folgt:

$|\mathbb{Z}_p^*| \backslash |H(a)| \in \mathbb{N} \Rightarrow k|(p-1) \Rightarrow \exists m \in \mathbb{N} : k * m = p - 1$

2.3 Wegen $|H(a)| = k$ gilt $[a^k]_p = ([a]_p)^k = [1]_p$

Also gilt: $a^k \equiv 1 \mod p$

2.4 Also folgt $[a^{p-1}]_p = ([a]_p)^{p-1} = \overset{(2.2)}{=} ([a]_p)^{km} = ([a_p]^k)^m \overset{(2.3)}{=} ([1]_p)^m = [1]_p \Rightarrow a^{p-1} = \equiv 1 \mod p$ (Hauptaussage)

2.5 Mit Satz 1.652 und (2.4) folgt $a^p \equiv a \mod p$ □

10.2 RSA-Kryptologie

10.2.1 Eine Anwendung von Fermats Kleiner Satz in der Kryptologie

Kryptologie mehr in $5

- Entwicklung von Methoden zur Kodierung von Nachrichten.
- "Kunst"der Entschlüsselung unbekannter Kodes

RSA : Rivest Shamir, Adleman 1978

10.2.2 Vorbreitung

1. Bestimmen zwei Primzahlen p, q groß, so dass ein Angreifer (NSA,KGB) selbst bei Kenntnis von $m = pq$ nicht die Faktoren bestimmen können.

   Beispiel: $p = 53, q = 61 \Rightarrow m = 3233$

2. Bestimme zwei Schlüssel $c, s \in \mathbb{N}$, sodass $cs \equiv 1 \mod (p-1)(q-1)$

   $(p-1)(q-1) = 3120 = 2^4 * 3 * 5 * 12$

   Beispiel $c = 77, s = 1013 \Rightarrow 78001 = 25 * 3120 + 1 \equiv 1 \mod 3120$

   Öffentlicher Schlüssel ist (m, c) bekannt für alle Nutzer. erlaubte Kodierung aber keine Dekodierung.

10.2.3 Kodierung

- Wähle eine Nachricht (Zahl w mit $0 \leq w < m$, sonst geeignet proportionieren)
- Kodewort $\hat{w} = w^c \mod m$ mit $0 \leq \hat{w} \leq m-1$ eindeutig bestimmt.

  Beispiel : $w = 10, \hat{w} \in [w^c]_m = [10^{77}]_{3233}, \hat{w} = 2560$

10.2.4 Dekodierung

Nun hat man $m, c, \hat{w}$. Wie bekomme ich w?

1. Für alle $a \in \{0, ..., m-1\}$, teste $a^c \equiv \hat{w} mod m$? Falls ja: $w = a$
   Prinzipiell OK, dauert aber ewig.

2. Falls du den privaten Schlüssel s besitzt.

   $w \equiv \hat{w}^S mod m$, eindeutig durch $0 \leq w < m$.
   Beispiel: $\hat{w}^S = 2560^{1013} \Rightarrow w = 10$, klappt immer!

   Richtigkeit der Entschlüsselung zeigt der folgende Satz

Satz 2.39

Seien $c, s, p, q, m, w \in \mathbb{N}_0$ die Zahlen gemäß RSA Algorithmus.

Ist w eine Nachricht und $\hat{w} \equiv w^c mod m$ mit $0 \leq \hat{w} < m$ die Kodierung von w, dann gilt $w \equiv \hat{w}^S mod m$ mit $0 \leq w < m$.

Beweis

Die Aussage folgt aus der noch zu beweisenden Behauptung $w \equiv w^{cs} mod m$

Wir zeigen:

(P) $w \equiv w^{cs} mod p \equiv (w^c)^s mod p$

zwei Fälle sind möglich

a) $p|w \Rightarrow p|w^{cs} \Rightarrow p|(w^{cs} - w) \Leftrightarrow w \equiv w^{cs} mod p$, d.h. (P) gilt.

b) $p \nmid w$ Nach Konstruktion RSA Alg. gilt $cs \equiv 1 mod (p-1)(q-1)$, also $\exists k \in \mathbb{Z} : cs = k * (p-1)(q-1) + 1$

Damit folgt:

$w^{cs} = w^{1+k(p-1)(q-1)} = w * w^{(p-1)k(q-1)} = w * \left(w^{p-1}\right)^{k(q-1)}$

Da $p \nmid w$, folgt aus dem kleinen Satz von Fermat: $w^{p-1} \equiv 1 mod p$

Weiter

$\left(w^{p-1}\right)^{k(q-1)} \equiv 1 mod p \Rightarrow w^{cs} \equiv w * 1 mod p$, d.h. (P) gilt.

(Q) $w \equiv w^{cs} mod q$ völlig analog.

Wegen $m = pq$ und p, q prim gilt mit Satz 1.71 3):

$w \equiv w^{cs} mod p \wedge w \equiv w^{cs} mod q \Leftrightarrow w^{cs} \equiv w mod pq \equiv w mod m.$ □

11Zahlenkörper (Körper)

Definition 2.40

Gegeben sei eine Menge $\mathbb{K}$ und die Abbildung:

1. $+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}, (a, b) = +(a, b) =: a + b$
2. $* : \mathbb{K} \times \mathbb{K} \to \mathbb{K}, (a, b) = *(a, b) =: a * b$

Das Tripel $(\mathbb{K}, +, *)$ heißt Körper (Zahlenkörper), falls

(K1) $(\mathbb{K}, +, 0)$ ist abelsche Gruppe.

(K2) $(\mathbb{K}^*, *, 1)$ ist abelsche Gruppe, $\mathbb{K}^* := \mathbb{K}\backslash\{0\}$

K3 es gelten die Distributivgesetze:

$\forall a, b, c \in \mathbb{K} : a * (b + c) = (a * b) + (a * c) \wedge (a + b) * c = (a * c) + (b * c)$

Schreibweisen: kurz $\mathbb{K}$ oder lang $(K, +, 0, *, 1)$

Bemerkung

1. $(\mathbb{K}, +, 0)$ heißt die additive Gruppe und $(\mathbb{K}, *, 1)$ die multiplikative Gruppe des Körpers.
2. (K1) $\wedge$ (K2) $\Rightarrow \{0, 1\} \in \mathbb{K} \wedge 0 \neq 1$.
3. Klammerkonvention: Punkt- vor Strichrechnung: $a + b * c = a + (b * c)$
4. Neutrale Elemente 0 für $+$ und 1 für $*$
Inverse Elemente für $a \in \mathbb{K} : -a$ für $+$ und a^{-1} für $*$ für $a \neq 0$.
Ggf. auch Spezialsymbole für das Rechnen mit Inversen:
$a + (-b) =: a - b$ bzw. $a * (b^{-1}) = a/b$

Beispiel 2.41

1. $(\mathbb{R}, +, *)$ ist Körper
2. $(\mathbb{Q}, +, *)$ ist Körper
3. $(\mathbb{Z}, +, *)$ ist kein Körper, da $z = 2 \in \mathbb{Z}$, aber $z^{-1} = \frac{1}{2} \notin \mathbb{Z}$
4. p prim, $(\mathbb{Z}_p, \oplus, \odot)$ ist Körper
5. $(\mathbb{B}, +, 0, *, 1)$ ist Körper mit $\mathbb{B} = \{0, 1\}$
6. $(\mathbb{C} := (\mathbb{R}^2, +, \binom{0}{0}, *, \binom{1}{0})$ ist Körper.

Lemma 2.42

Sei $(\mathbb{K}, +, 0, *, 1)$ ein Körper. Es gilt:

1. $\forall a \in \mathbb{K} : 0 * a = a * 0 = 0$
2. $\forall a, b \in \mathbb{K} : a * b = 0 \Leftrightarrow (a = 0 \vee b = 0)$

   Wegen der zweiten Aussage heißt ein Körper auch Nullteiler frei. Ist das Produkt null, muss einer der Faktoren null sein.

Beweis

1. $0 * a = (0 + 0) * a = 0 * a + 0 * a \Rightarrow 0 = 0 * a$
2. $\Leftarrow$ folgt aus Teil 1.

   $\Rightarrow$ Für $a, b \neq 0 \overset{(K2)}{\Rightarrow} a * b \neq 0$, vgl. Satz 1.5.2 indirekter Beweis. □

Bemerkung

1. Da $0 \neq 1$ folgt aus Lemma 2.42.1, dass 0 kein multiplikatives Inverses hat. D.h. "0^{-1}" existiert nicht, die Verwendung ist unsinnig, der Gebrauch falsch.

   $(\mathbb{K}, *)$ kann keine Gruppe sein!
2. Ist n nicht Prim folgt $(\mathbb{Z}_n^k, *)$ nicht Nullteiler frei!

Weitere Strukturen

1. Magma $(M, \diamond)$ mit (G1)
2. Halbgruppe $(M, \diamond)$ mit (G1) + (G2)
3. Monoid $(M, \diamond)$ mit (G1-3)
4. Ring $(M, +, *)$ mit (K1) und (K3), wobei $(M, *)$ Halbgruppe ist.
5. Integritätsbereich: Nullteiler freier Ring
6. Schiefkörper $(M, +, *)$ ist ein Ring, aber $(M^*, *)$ ist eine nicht notwendige abelsche Gruppe.

12Die komplexen Zahlen C

12.1 Die Grundmenge C und deren Elemente

Schreibweisen für komplexe Zahlen $z \in \mathbb{C}, \mathbb{C} = \mathbb{R}^2$

$z = \binom{x}{y} = \binom{x}{0} + \binom{0}{y} = x\binom{1}{0} + y\binom{0}{1} = x * 1 + y * \imath =: x + \imath y$

dabei bezeichnet 1 und i die reelle bzw imaginäre Richtung und i die imaginäre Einheit. Die Komponenten x bzw y heißen Realteil $\Re$ bzw. Imaginärteil $\Im$ von z.

$x = \Re(z), y = \Im(z)$. Ist einer der Summanden 0, lassen wir den Term einfach weg.

Für $z = x + \imath y \in \mathbb{C}$ bezeichnet $\overline{z} := x - \imath y = \Re(z) - \Im(z)\imath$ die zu $z \in \mathbb{C}$ konjugiert komplexe Zahl.

$r * e^{\varphi} := r * \cos\varphi * 1 + r * \sin\varphi * \imath = z$

12.2 Kartesische und Polarkoordinaten

Beispiel 2.43

$e^{\imath\frac{\pi}{2}} = \imath$

$e^{\imath 0} = 1$

$e^{\imath\pi} = -1$

$1 + \imath = \sqrt{2}e^{\imath\frac{\pi}{4}}$

- Die Länge (Betrag, Modul) von $z \in \mathbb{C}$ bezeichnen wir mit:

  $|z| := \sqrt{z * \overline{z}} = \sqrt{\Re(z)^2 + \Im(z)^2} = \sqrt{x^2 + y^2} \in \mathbb{R}_{\geq 0}$ falls $z = x + \imath y$
  - $z = 1 + \imath$
  - $\overline{z} = 1 - \imath$
  - $z\overline{z} = (1^2 + 1^2) + \imath(-1 + 1) = 2$
- Den Winkel (Phase, Argument) zwischen der reellen Achse und den durch z gegebenen Strahl bezeichnen wir mit $\arg(z)$

  $\arctan\frac{y}{x}$, $x > 0$
  $\arctan\frac{y}{x} + \pi$, $x < 0 \land y \geq 0$
  $\arctan\frac{y}{x} - \pi$, $x < 0 \land y < 0$
  $\frac{\pi}{2}$, $x = 0 \land y > 0$
  $-\frac{\pi}{2}$, $x = 0 \land y < 0$
  unbestimmt, $x = 0 \land y = 0$ (zwecks Eindeutigkeit definieren wir $\arg(z) = 0$ für $z = 0$.

  zusammen $=: \varphi := \arg(z) := \arctan 2(y, x)$
- Das Tupel (r, φ) mit $r = |z|$ und $\varphi = \arg(z)$ heißt die Polarkoordinaten von $z \in \mathbb{C}$ und das Tupel (x, y) mit $x = \Re(z)$ und $y = \Im(z)$ heißt die kartesischen Koordinaten von $z \in \mathbb{C}$

  $x = r\cos\varphi$ und $y = r\sin\varphi \Leftrightarrow r = \sqrt{x^2 + y^2}$ und $\varphi = \arctan 2(y, x)$ für $z \neq 0$

Addition in C

$$a + b = +(a, b) := \begin{pmatrix} a_1 + b_1 \\ a_2 + b_2 \end{pmatrix} = (a_1 + \imath a_2) + (b_1 + \imath b_2) = (a_1 + b_1) + \imath(a_2 + b_2)$$

"Wir addieren Real- und Imaginärteile"

Multiplikation in C

$$a * b = *(a, b) := \begin{matrix} a_1 * b_1 - a_2 * b_2 \\ a_1 * b_2 + a_2 * b_1 \end{matrix} = (a_1 + \imath a_2) * (b_1 + \imath b_2) = (a_1 * b_1 - a_2 * b_2) + \imath(a_1 * b_2 + a_2 * b_1)$$

Beispiel 2.44

$(2 + 3\imath) * (2 - \imath) = (2 * 2 - 3(-\imath)) + \imath(2(-\imath) + 3 * 2) = 7 + 4\imath$

Hieraus folgt z.B. $\imath^2 = (-1)$

Das ist ein fundamentaler Ansatz zur Lösung algebraischer Gleichungen.

Bemerkung

Setzen wir $\mathbb{R} \ := \{x + 0\imath, x \in \mathbb{R}\} \subset \mathbb{C}$, dann gilt für alle $z, w \in \mathbb{R}$:

$z + w = \Re(z) + \Re(w) + \imath(\Im(z) + \Im(w)) \in \mathbb{R}$

$z * w = [\Re(z) * \Re(w) - \Im(z) * \Im(w)] + \imath[\Re(z) * \Im(w) + \Im(z) * \Re(w)] \subset \mathbb{R}$

Also sind $(\mathbb{R}\ , +, 0, *, 1)$ und $(\mathbb{R}, *, +)$ strukturell dasselbe!

$\Rightarrow$ Wir unterscheiden im Folgenden $\mathbb{R}$ und $\mathbb{R}$ nicht mehr.

Es gilt $\Re(w) = \Re(\overline{w})$ und $\Im(w) = \Im(\overline{w}$

$w\overline{w} = \Re(w)^2 + \Im(w)^2$

Damit besitzt das multiplikative Inverse zu $w \in \mathbb{C}, w \neq 0$ die Darstellung:

$w^{-1} = \frac{\overline{w}}{w\overline{w}}$, denn $w\overline{w} = \frac{w\overline{w}}{w\overline{w}} = 1$

Für $w \neq 0$ und z mit $z = x + \imath y$ und $w = u + \imath v$

$\frac{z}{w} := z * w^{-1} = \frac{z\overline{w}}{w\overline{w}} = \frac{(xu+yv)+\imath(-xv+yu)}{u^2+v^2}$

Potenzen z^k für $k \in \mathbb{Z}$ sind durch Def 2.21 bereits festgelegt.
$z^0 := 1, z^k = z * z^{k-1}, k > 0, z^{-k} = (z^{-1})^k, k > 0$

In $\mathbb{C}$ gilt ein binomischer Satz analog zu Satz 1.77

Beispiel 2.45

$(1 + \imath)^{14} * (1 + \sqrt{3}\imath)^7 = (\sqrt{2}e^{\imath\frac{\pi}{4}})^{14} * (2e^{\imath\frac{\pi}{3}})^7 = \sqrt{2}^{14} * 2^7 * e^{\imath(\frac{7}{2}\pi + \frac{7}{3}\pi)} = 2^{14} * e^{-\imath\frac{\pi}{6}}$

Es gelten die Regeln von de Moivre:

a) $e^{\imath\varphi} * e^{\imath\psi} = e^{\imath(\varphi+\psi)}$

b) $(e^{\imath}\varphi)^n = e^{\imath n\phi}$

c) $e^{-\imath\varphi} = \frac{1}{e^{\imath\varphi}}$

Mit den Polarkoordinaten wird die Multiplikation in $\mathbb{C}$ besonders transparent:

Für $z = r * e^{\imath\varphi}$ und $w = s * e^{\imath\omega}$ gilt:

$z * w = (r * e^{\imath\varphi}) * (s * e^{\imath\omega}) = (r * s) * e^{\imath(\varphi+\omega)}$

$z^n = r^n * e^{\imath n\varphi}, n \in \mathbb{Z}$

$\frac{z}{w} = \frac{r}{s} * e^{i(\varphi-\omega)}, w \neq 0$

Man multipliziert die Beträge und addiert die Winkel.

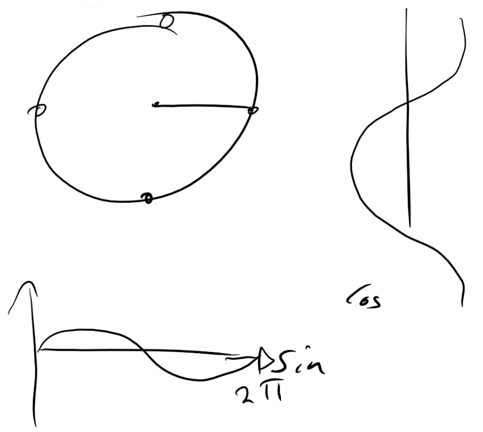
12.3 Schwingungen

$e^{i\varphi} * e^{i\psi} = (\cos\varphi + i\sin\varphi) * (\cos\psi + i\sin\psi)$

$= (\cos\varphi\cos\psi - \sin\varphi\sin\psi) + i(\cos\varphi\sin\psi + \sin\varphi\cos\psi)$

$\overset{Add.Th.}{=} \cos(\varphi+\psi) + i\sin(\varphi+\psi)$

$= e^{i(\varphi+\psi)}$



$e_k = e(k) = e^{i2\pi kt}$

12.4 Komplexe Wurzeln

Jede komplexe Lösung der Gleichung $z^n - a = 0, z, a \in \mathbb{C}, n \in \mathbb{N}$ heißt eine n-te Wurzel von $a \in \mathbb{C}$. Für $a = 1$ heißen die Lösunen komplexe Einheitswurzeln.

Satz 2.46

Sei $n \in \mathbb{N}$. Für die Lösungsmenge L der Gleichung $2^n = a$ gilt:

$L = \{z \in \mathbb{C} : z = w\mu_k, k = 0, ..., n-1\}, w = \sqrt[n]{|a|}e^{i\alpha n}, \mu_k = e^{i2\pi k/n}, a = r * e^{i\alpha}$

Beweis

Mit den Polardarstellungen $a = r * e^{i\alpha}$ und $z = s * e^{i\zeta}$ gilt $a = r * e^{i\alpha} = z^n = (s * e^{i\zeta})^n = s^n * e^{in\zeta} \Leftrightarrow$
$\begin{cases} s = \sqrt[n]{r} \\ \zeta = \frac{\alpha}{n} + \frac{2\pi j}{n} j \in \mathbb{Z} \end{cases}$

wobei die bijektive Abbildung $\sqrt[n]{\text{ffl}}, \mathbb{R}_{\geq 0} \leftarrow \mathbb{R}_{\geq 0}$

Für bel. $j \in \mathbb{Z}$ findet sich eine Darstellung $j = qn + k$

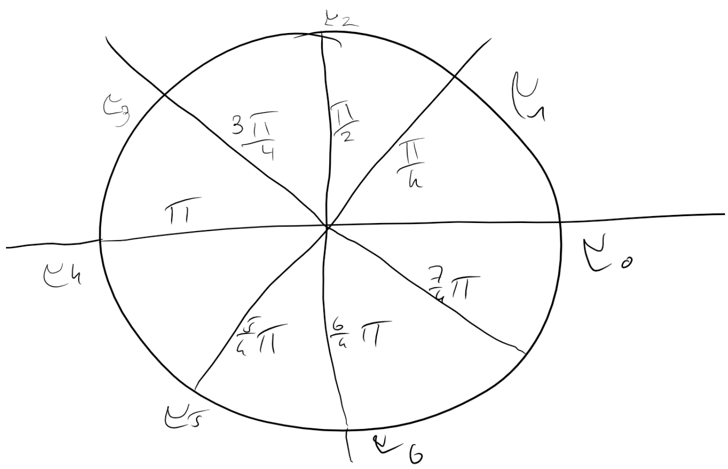
$z = s * e^{i(\frac{\alpha}{n} + \frac{2\pi j}{n})}$ mit $q \in \mathbb{Z}$ und $k \in \{0, ..., n-1\}$

$s * e^{i(\frac{\alpha}{n} + \frac{2\pi k}{n} + 2\pi q)}$

$s * e^{i(\frac{\alpha}{n} + \frac{2\pi k}{n})} * (e^{i2\pi})^n = s * e^{i(\frac{\alpha}{n} + \frac{2\pi k}{n})}$ und also sind die Mengen gleich. □

Speziell für die Einheitswurzeln gilt mit $\mu_k = e^{i\frac{k2\pi}{n}}$

$\sqrt[n]{1} := 1^{\frac{1}{n}} = \{\mu_0, ..., \mu_{n-1}\} = \{1, e^{i\frac{2\pi}{n}}, e^{i\frac{4\pi}{n}}, ..., e^{i\frac{(n-1)2\pi}{n}}$



13Vektorräume

Körper $(\mathbb{K}, +, 0, *, 1)$ vgl. Def. 2.40 $\alpha, \beta, \gamma \in \mathbb{K})$

Gruppe $(V, \oplus, 0)$

13.1 Definition des Vektorraums (VR) und Beispiele

Definition 3.1

Sei $\mathbb{K}$ Körper und $V \neq \varnothing$ eine Menge. Das Tripel $(V, \oplus, \odot)$ heißt ein $\mathbb{K}$-Vektorraum ($\mathbb{K}$-VR), falls mit den Abb.

$\oplus : V \times V \to V, (x, y) \mapsto \oplus(x, y) =: x \oplus y$

$\odot : \mathbb{K} \times V \to V, (\alpha, y) \mapsto \odot(\alpha, y) =: \alpha \odot y = \alpha * y$

die fünf VR-Axiome gelten:

V1 $(V, \oplus, 0)$ ist abelsche Gruppe

V2 $\forall \alpha, \beta \in \mathbb{K} \forall x \in V : (\alpha * \beta) \odot x = \alpha \odot (\beta \odot x)$

V3 $\forall x \in V : 1 \odot x = x$

V4 $\forall \alpha, \beta \in \mathbb{K} \forall x \in V : (\alpha + \beta) \odot x = (\alpha \odot x) \oplus (\beta \odot x)$

V5 $\forall \alpha \in \mathbb{K} \forall x, y \in V : \alpha \odot (x \oplus y) = (\alpha \odot x) \oplus (\alpha \odot y)$

Skalieren und Addieren ist damit sauber definiert.

Bemerkung

1. $\alpha, \beta \in \mathbb{K}$ heißen Skalare (i.A. griechische Buchstaben)
2. $x, y \in V$ heißen Vektoren (i.A. lateinische Buchstaben)
3. $\oplus$ Addition, Vektoraddition
4. $\odot$ Skalarmultiplikation
5. 0 (neutrales Element in V) heißt Nullvektor
6. $\alpha x := \alpha \odot x, \alpha x \oplus y := (\alpha \odot x) \oplus y$
7. Ist y' das Inverse von $y \in V$ bzgl. $\oplus$ (also $y \oplus y' = 0$), dann setzen wir $-y := y'$ und $x \oplus y' := x \oplus (-y)$

Beispiel 3.2

1. Mit $V := \mathbb{K}, \oplus := +, \odot := *$ ist $(V, \oplus, \odot)$ ein K-VR

2. $\mathbb{K}^n = \{x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_1, ..., x_n \in \mathbb{K}\}$ und $\begin{bmatrix} \mathbb{R}^n \text{ kommt mit Körper } \mathbb{R} \\ \mathbb{C}^n \text{ kommt mit Körper } \mathbb{C} \end{bmatrix}$

   $n \in \mathbb{N} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}, \alpha \odot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \alpha x_1 \\ \vdots \\ \alpha x_n \end{pmatrix} \Rightarrow (\mathbb{K}^n, \oplus, \odot)$

3. Polynome von Höchstgrad n mit reellen Koeffizienten $(\pi_n, \oplus, \odot)$

   $\pi_n := \{a : \mathbb{R} \to \mathbb{R}, a(x) = \sum\limits_{i=0}^{n} \alpha_i x^i, \alpha 0, \ldots, \alpha_n \in \mathbb{R}\}$

   $\oplus : \pi : nx\pi_n \to \pi_n(a \oplus b)(x) := \sum(\alpha_i + \beta_i)x^i$

   $\odot : \mathbb{R}x\pi_n \to \pi_n(\lambda \odot \alpha)(x) := \sum(\lambda\alpha i)x^i$

   $(\pi_, \oplus, \odot)$ ist $\mathbb{R}-$ VR. Für das neutrale Element gilt:

   $0(x) := \sum 0 * x^i$

Lemma 3.3

Sei $(V, \oplus, \odot)$ ein $\mathbb{K}$-VR. Es gilt:

1. $\forall \alpha \in \mathbb{K} \forall x \in V : \alpha \odot x = 0 \Leftrightarrow (\alpha = 0 \vee x = 0)$
2. $\forall x \in V : (-1) \odot x = -x$

   (Zweite Aussage möglicherweise als Klausuraufgabe)

Beweis zu Lemma 3.3.1

$'' \Leftarrow''$ Für $\alpha = 0 : 0 \odot x = (0 + 0) \odot x \overset{(V4)}{=} (o \odot x) + (0 \odot x) \overset{Satz 2.9}{\Leftrightarrow} 0 = 0 \odot x \checkmark$

n Für $x = 0 : \alpha \odot 0 = \alpha \odot (0 \oplus 0) \overset{(V5)}{=} \alpha \odot 0 \oplus \alpha \odot 0 \overset{Satz 2.9}{\Rightarrow} 0 = \alpha \odot 0 \checkmark$

$'' \Rightarrow''$ Sei nun $\alpha \odot x = 0$ Für $\alpha = 0$ ist nichts zu zeigen. Daher nun $\alpha \neq 0$

Da $\alpha \neq 0 \exists \alpha^{-1} \in \mathbb{K} : \alpha^{-1} * \alpha = 1$. Es folgt:

$0 \overset{(1)}{=} \alpha^{-1} \odot 0 = \alpha^{-1} \odot (\alpha \odot x) \overset{(V2)}{=} (\alpha^{-1} + \alpha) \odot x = 1 \odot x \overset{(V3)}{=} x$ $\square$

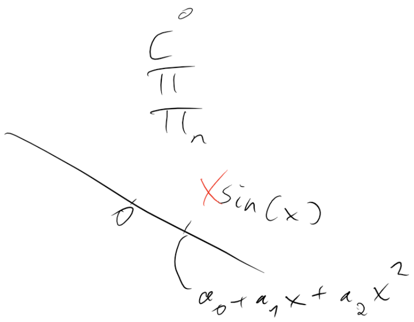
Definition 3.4

Sei $(V, \oplus, \odot)$ ein $\mathbb{K}$-VR. Die Menge W ist ein <u>Untervektorraum (U-VR) von V</u>, falls gilt:

1. $W \neq \varnothing$

   $W \subseteq V$

$(W, \oplus, \odot)$ ist ein $\mathbb{K}$-VR.



Satz 3.5 (U-VR Kriterium)

Sei V $\mathbb{K}$-VR, $W \neq \varnothing \wedge W \subseteq V$.

W ist U-BR von V genau dann wenn:

$\forall \alpha \in \mathbb{K} \forall x, y \in W : \alpha x + y \in W$ *

Beweis

$'' \Rightarrow ''$ 9 Aus der Vollst. von $\oplus : WxW \to W$ und $\odot : \mathbb{K}xW \to W$ folgt Behauptung.

$'' \Rightarrow ''$

1. $(V2 - V5)$ gelten f: alle $x \in V$ und damit auch $\forall w \in W \subseteq V$
2. Für (VI) : $(W, \oplus, \odot)$ ist abelsche Gruppe nutzen wir Untergruppenkriterium:
   a) $W \neq \varnothing \surd$
   b) $\forall x, y \in W : x \oplus y \in W$
   $\forall x \in W : -x \in W$

zu 2.1 gilt nach Voraussetzung.

zu 2.2 Für beliebiges $y \in W$ und $\alpha = 1 \in \mathbb{K}$ gilt $1 \odot y = y$, dann $y \in V$ und V erfüllt (V3)

Mit (*) folgt : $[\forall \alpha \in \mathbb{K} \forall x, y \in W : x \oplus 1 \odot y \in W] \Rightarrow [\forall x, y \in W : x \oplus y \in W]$

zu 2.3 Für ein beliebiges $x \in W$ und $\alpha = -1 \in \mathbb{K}$ folgt aus (*) $W \ni x \oplus (-1) \odot x \overset{Lemma 3.3}{=} x \oplus (-x) = 0$, also $0 \in W$

Zusammen:

$(W, \oplus, \odot)$ ist eine Untergruppe, dann V abelsch ist auch W abelsch.

3. Schließlich gilt: $\forall \alpha \in \mathbb{K} \forall x \in W : \alpha \odot x = 0 \oplus \alpha \odot x \overset{(*)}{\in} W$, d.h. $\odot : \mathbb{K}xW \to W$ $\square$

Beispiel 3.6

1. $V = \mathbb{R}^2, v \in \mathbb{R}^2, v \neq 0$

   $G := \{x \in V : x = \alpha \odot v, \alpha \in \mathbb{R}\}$ ist U-VR "Gerade in der Anschauungsebene"

2. $V = \mathbb{R}^3, v, w \in V, v \neq 0 \wedge w \neq 0$

   $E := \{x \in V : x = \alpha \odot v + \beta \odot w, \alpha, \beta \in \mathbb{R}\}$ ist U-VR

13.2 3.2 Basen eines K-VR

Definition 3.7

1. Sei V ein $\mathbb{R}$-VR, $v_1, \ldots, v_3 \in V$ und $\alpha_1, \ldots, \alpha_r \in \mathbb{K}$.

   $\alpha_1 \oplus v_1 \oplus \alpha_2 \oplus v_2 \oplus \cdots \oplus \alpha_r \odot v_r = \sum_{j=1}^{r} \alpha_j \odot v_j \in V$

   heißt Linearkombination des r-Tupels $(v_1, \ldots, v_r)$

2. Die Menge aller Lin.-Komb. von $(v_1, \ldots, v_r)$

   $\text{Spann}(v_1, \ldots, v_r) := \sum_{j=1}^{r} \mathbb{K} * v_j := \{\sum_{j=1}^{r} \alpha_j v_j, \alpha_1, \ldots, \alpha \in K\} \subseteq V$

   heißt die Lineare Hülle von $(v_1, \ldots, v_r)$ oder dem von den $v_1, \ldots, v_r$ aufgespannten Raum

   Falls $r = 0$, vereinbaren wir . spann$(\varnothing) := \{0\}$

3. Gilt $v = \text{spann}(v_1, \ldots, v_r)$ so heißt $(v_1, \ldots, v_r)$ ein erzeugendes System von V

   Wir sagen: V wird von den $v_1, \ldots, v_r$ aufgespannt.

Beispiel 3.8

Sei $V = \mathbb{R}^2, e_1 := \binom{1}{0} \wedge e_2 := \binom{0}{1}$

Jedes $x \in V$ besitzt die Darstellung : $x = \binom{x_1}{x_2} = \binom{x_1}{0} \oplus \binom{0}{x_2} = x_1 \odot \binom{0}{1} \oplus x_2 \odot \binom{0}{1}$

$= x_1 e_1 \oplus x_2 e_2 \in spann(e_1, e_2)$

$\forall x \in V : x \in \text{spann}(e_1, e_2) \wedge \text{spann}(e_1, e_2) \subseteq V \Rightarrow V = \text{spann}(e_1, e_2)$

$w_1 = \binom{1}{1} \wedge w_2 = \binom{0}{1} \wedge w_3 = \binom{17}{4}, x = \binom{x_1}{x_2} = \alpha w_1 \oplus \beta w_2 = \binom{\alpha}{\alpha} \oplus \binom{0}{\beta} = \binom{\alpha}{\alpha+\beta}$

falls $\alpha = x_1$ und $\beta = x_2 - x_1$

$q_1 = \binom{1}{0} \wedge q_2 = \binom{\frac{-1}{4}}{0}, \binom{x_1}{x_2} = \alpha q_1 \oplus \beta q_2 = \binom{\alpha - \frac{1}{4}\beta}{0} \Rightarrow x_2 = 0$

Lemma 3.9

Sei $V\mathbb{K}$-VR, $v_1, \dots, v_r \in V$.

1. spann$(v_1, \dots, v_r)$ ist U-VR von V
2. spann$(v_1, \dots, v_r)$ ist der kleinste U-VR von V, der $v_1, \dots, v_r$ enthält:

   Ist U: U-VR von V mit $v_1, \dots, v_r \in U$ dann gilt spann $(v_1, \dots, v_r) \subseteq U$.

Beweis

zu 1. Seien $x, y \in$ spann$(v_1, \dots, v_r)$, d.h $\exists \xi_1, \dots, \xi_r, \eta_1, \dots, \eta_r \in \mathbb{K}$

sodass $x = \sum\limits_{j=1}^{r} \xi_j v_j \wedge y = \sum \eta_j v_j$ mit Satz 3.5 und $\forall \alpha \in \mathbb{K} : x \oplus \alpha y = (\sum \xi_j v_j) + \alpha \odot (\sum \eta_j v_j) = \sum \xi : j + +\alpha \eta : j) v_j) v_j \in$spann$(v_1, \dots, v_j)$

folgt spann$(v_1, \dots, v_j($ ist U-VR von V.

zu 2 Sei U U-VR von V mit $v_j \in U, j = 1, \dots, r$. Dann folgt $\forall \xi_1, \dots, \xi_r \in \mathbb{K} \sum \xi_j v_j \in U$, d.h. spann$(v_1, \dots, v_r) \subseteq U$ □

Definition 3.10

Sei $V\mathbb{K}$-VR und $v_1, \dots, v_r \in V$ Das Tupel $(v_1, \dots, v_r)$ heißt Linear Unabhängig(l.u., lin. unabhg. ...) falls:

$$\sum_{j=1}^{r} \alpha_j v_j = 0 \Leftrightarrow \forall j = 1, \dots, r : \alpha_j = 0$$

Anderenfalls heißt $(v_1, \dots, v_r($ linear abhängig (l.a.,lin.abhäng.)

Wir sagen auch: Die Vektoren$v_1, \dots, v_r$ sind l.z. bzw l.a.

Konvention: $\varnothing$ ist l.u.

Beispiel 3.11

1. Sei $V = \mathbb{R}^2, v_1 = \binom{1}{2} \wedge v_2 = \binom{1}{1}$. Das Tupel (v_1, v_2) ist l.u.

   $\alpha_1 \odot v_1 \oplus \alpha_{\odot} v_2 = \alpha\binom{1}{2} \oplus \alpha_2 \binom{1}{1} = \binom{1*\alpha_1+1*\alpha_2}{2*\alpha_1+1+\alpha_2} = \binom{\alpha_1+\alpha_2}{2\alpha_1+\alpha_2} = \binom{0}{0} = 0$

   $\Leftrightarrow \alpha_1 = -\alpha_2 \wedge \alpha_1 = 0 \Leftrightarrow \alpha_1 = 0 \wedge \alpha_2 = 0$

2. Sei $V = \mathbb{R}^3, v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, v_2 = \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}, v_3 = \begin{pmatrix} -6 \\ -4 \\ -8 \end{pmatrix}$ Das Tupel (v_1, v_2, v_3) ist l.a.

$$\alpha_1 \odot v_1 \oplus \alpha_2 v_2 \oplus \alpha_3 \odot v_3 = \begin{pmatrix} \alpha_1 + 2\alpha_2 - 6\alpha_3 \\ \alpha_1 + \alpha_2 - 4\alpha_3 \\ \alpha_1 + 3\alpha_2 - 8\alpha_3 \end{pmatrix}$$

Für $\alpha_1 = 2, \alpha_2 = 2, \alpha_3 = 1$

$$\alpha_1 v_1 \oplus \alpha_2 v_2 \oplus \alpha_3 v_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ aber } \alpha_1 \neq 0$$

3. Seien $p_i \in \prod_2(\mathbb{R}), p_0(t) = 1, p_1(t) = t, p_2(t) = t^2$

   Angenommen $\alpha_0 \odot p_0 \oplus \alpha_1 \odot p_1 \oplus \alpha_2 \odot p_2 = 0 \in \prod_2(\mathbb{R})$,d.h. $\forall t \in \mathbb{R} : \alpha_0 * 1 + \alpha_1 * t + \alpha_2 * t^2 = 0 \in \mathbb{R}$

   Für die Wahl $t = 0$ folgt $\alpha_0 = 0$

   Für $t = \pm 1$ folgt $\pm\alpha, +\alpha_2 = 0 \Leftrightarrow \alpha_1 = 0 \wedge \alpha_2 = 0$

   Also ist (p_0, p_1, p_2) l.u.

Lemma 3.12

Sei $V\mathbb{K}$-VR und $v_j \in V, j = 1, \ldots, r$.

1. $(v_1, \ldots, v_r)$ l.a $\Leftrightarrow \exists i \in \{1, \ldots, r\} : v_i = \sum_{j=1}^{r} \alpha_j v_j j \neq u$
2. $\exists i, j \in \{1, \ldots, r\}$ mit $i \neq j \wedge v_i = v_j \Rightarrow (v_1, \ldots, v_r)$ l.a.
3. $\exists i \in \{1, \ldots, r\}$ mit $v_i = 0 \Rightarrow (v_1, \ldots, v_4)$ l.a.

Beweis

zu 1

$'' \Leftarrow''$ $\sum_{i \neq j} \alpha_j v_j - v_j = 0 \Leftrightarrow \sum \alpha_j v_j = 0$ mit $\alpha_1 = -1 \neq 0$ also l.a.

$'' \Rightarrow''$ l.a. impliziert:

$\sum \alpha_j v_j = 0 \wedge \neg(\forall j = 1, \ldots, r : \alpha_j = 0)$

d.h $\exists \in \{1, \ldots, r\} : \alpha_k \neq 0$, d.h es gibt ein mult.Inverses α_k^{-1}

$\alpha_k^{-1} \odot (\alpha_k \odot v_k \oplus \sum_{k \neq k} \alpha_j v_j) = 0 \Leftrightarrow v_k = \sum_{j \neq k} (-\alpha_k^{-1} \alpha_j) v_j$

zu 2 Mit $\alpha_k := 0$ für $k \neq i, j \wedge \alpha_i = \wedge \alpha_j :_= -1$

$\sum \alpha_p v_p = \alpha_i v_i \oplus \alpha_j v_j = v_i \ominus v_i = 0 \Rightarrow$ l.a.

zu 3 Mit $\alpha_k := 0 \forall k \leq i$ und $\alpha_i = 1 \neq 0$ folgt $\sum \alpha_p v_p = v_i = 0 \Rightarrow$l.a.

Beispiel 3.13

Sei $V = \mathbb{R}^3$

$x = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, v_1 = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, v_2 = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}, v_3 = \begin{pmatrix} -1 \\ 4 \\ 5 \end{pmatrix}$

Das Tupel (x, v_1, v_2, v_3) ist l.a:

$0x \ominus 3v_1 \oplus 2v_2 \oplus v_3 = 0$

Trotzdem lässt sich x nicht aus den v_j lin.kombinieren.

$-1 = \alpha_1 + 2\alpha_2 - \alpha_3$

$1 = 2\alpha_2 + \alpha_2 + 4\alpha_3$

$0 = 3\alpha_1 + 2\alpha_2 + 5\alpha_3$

Aufgelöst $\Rightarrow -3 = 0, 1 = 0$,Widerspruch.

Definition 3.14

Sei $V\mathbb{K}$-VK und $v_1, \ldots, v_r \in V$ Das Tupel $(v_1 m \ldots, v_r)$ heißt eine Basis von V, falls:

(BI) $(v_1, \ldots, v_r)$, l.u.

(B2) $(v_1, \ldots, v_r)$ ist Erzeugendensystem von V, d.g $V = \text{spann}(v_j, j = 1, \ldots, r)$

Sprechweisen: $(v_1, \ldots, v_r)$ bildet eine Basis von V bzw. $v_1, \ldots, v_r$ bilden eine Basis von V

Beispiel 3.15

Nach Bsp. 3.8 ist(v_1, v_2) l.u. $v_1 = \binom{1}{2}, v_2)\binom{1}{1} \forall x \in \mathbb{R}^2$ gilt :

$x = \binom{x_1}{x_2} = \alpha_1 v_1 \oplus \alpha_2 v_2 = \alpha_1 \binom{1}{2} \oplus \alpha_2 \binom{1}{1} = \binom{\alpha_1 + \alpha_2}{2\alpha_1 + \alpha_2}$

$\Leftrightarrow \binom{x_1 = \alpha_1 + \alpha_2}{x_2 = 2\alpha_1 + \alpha_2} \Leftrightarrow \binom{\alpha_1 = x_2 - x_1}{\alpha_2 = 2x_1 - x_2}$

d.h $\forall x \in \mathbb{R}^2 : x \in \text{spann}(v_1, v_2)$ d.h $\mathbb{R}^2 \subseteq \text{spann}(v_1, v_2)$

d.h (v_1, v_2) ist l.u. Erzeugendensystem. $\Rightarrow (v_1, v_2)$ ist Bases von $\mathbb{R}^2$

$e_1 = \binom{1}{0} \wedge e_2 = \binom{0}{1}, (e_1, e_2)$ ist Basis von $\mathbb{R}^2$

Satz 3.24

Sei V endl. erzeugter $\mathbb{K}$-VR. Sind $(v_1, \ldots, v_n)$ und $(w_1, \ldots, w_m)$ zwei Basen von V, dann gilt $m = n$

Beweis

Aus Lemma 3.23 folgt $m \leq n \wedge n \leq \Leftrightarrow m = n$ □

Definition 3.25

Sei V endl. erzeugter VR. Nach Satz 3.21 existiert eine endl. Basis, deren Anzahl von Elementen nach Satz 3.24 eindeutig ist.

Die eindeutige Anzahl der Elemente einer Basis von V heißt die Dimension von V und wird mit dim V bzw. $\dim(V)$ bezeichnet.

Lemma 3.26

V endl. erzeugter VR und $v_1, \ldots, v_m \in V$

Ist $m > \dim(V)$, so ist $(v_1, \ldots, v_m)$ l.a.

Beweis

Angenommen: $(v_1, \ldots, v_m)$ l.u., Satz 3.22 impliziert, dass $(v_1, \ldots, v_m)$ zu einer Basis von V ergänzt werden kann.

$m \leq \dim(V)$, ein Widerspruch! □

Beispiel 3.27

Wir betrachten den unendlich dimensionalen $\mathbb{R}$-VR

$V = \mathrm{Abb}([0,1], \mathbb{R})$, mit $\oplus$ und $\odot$ wie bei Abbildungen üblich.

Für $p \in \mathbb{N}$ sei $f_p : [0,1] \to \mathbb{R}$ mit $f_p(x) = \begin{cases} 1 & \text{für } x \in (\frac{1}{p+1}, \frac{1}{p}) \\ 0 & \text{sonst} \end{cases}$

Für $f := \sum_{j=1}^{n} \lambda_0 f_j$ gelte $f = 0$

Für $k \in \mathbb{N}$ setze $x_k := (\frac{1}{k} + \frac{1}{k+1}) * \frac{1}{2}$.

$f = 0 \Rightarrow 0 = 0(x_k) = f(x_k) = \sum_{j=1}^{n} \lambda_j f_j(x_k) = \lambda_k f_k(x_k) = \lambda_k$

d.h. die Vektoren $(f_1, \ldots, f_n)$ sind l.u. für beliebiges $n \in \mathbb{N}$

Nach Lemma 3.26: $\dim(V) \geq n \forall n \in \mathbb{N}$,

d.h V besitzt keine endliche Basis: $\dim(V) = \infty$ □

13.3 Normierte Vektorräume

Bemerkung

Motivation: Verallgemeinerung der Begriffe: Länge und Winkel im $\mathbb{R}^2$

Wichtige Fälle: $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$

Definition 3.28

Sei $V\mathbb{K}$-VR. Eine Abbildung $||*|| : V \to \mathbb{R}$ heißt Norm in V falls gilt:

(N1) Homogenität:

$\forall \lambda \in \mathbb{K}, \forall x \in V : ||\lambda x|| = |\lambda| ||x||$

(N2) Definitheit:

$\forall x \in V : ||x|| \geq 0 \land (||x|| = 0 \Leftrightarrow x = 0)$

(N3) Dreiecksungleichung:

$\forall x, y \in V : ||x + y|| \leq ||x|| + ||y||$

Ist $||*||$ eine Norm in CV, so heißt $(V, ||*||)$ (oder kurz V) ein normierter Vektorraum.

Lemma 3.29

Sei $V\mathbb{K}$-VR und $||*|| : V \to \mathbb{R}$ eine Abbildung mit (N1) und (N3). Dann gilt:

$[||x|| = 0 \Rightarrow x = 0] \Leftrightarrow [\forall x \in X : ||x|| \geq 0 \land (||x|| = 0 \Leftrightarrow x = 0)]$ (N2)

Beweis

$0 = ||0|| = ||x + (-1)x|| \leq ||x|| + |-1| * ||x|| = 2||x|| \Rightarrow 0 \leq ||x||$

Bemerkung

1. Norm $\hat{=}$ Vorstellung von Länge
2. Interpretation (N3): Der direkte Weg ist stets kürzer als ein Umweg.

Beispiel 3.30

1. Die p-Normen im $\mathbb{K}^n, n, p \in \mathbb{N}, ||*||_p : \mathbb{K}^n \to \mathbb{R}$
   a) $p = 2$, Euklidische Norm, 2-Norm.

   $$||x||_2 = \sqrt{\sum_{j=1}^{n} |x_j|^2} = \sqrt{|x_1|^2 + \cdots + |x_n|^2}$$

b) $p = 1$, Manhattan Norm oder 1-Norm.

$||x||_1 = \sum\limits_{j=1}^{n} |x_j| = |x_1| + \cdots + |x_2|$

c) Maximum oder ∞-Norm.

$p = \infty, ||x||_\infty = \max\{|x_j|, j = 1, \ldots, n\} = \max\{|x_1|, |x_2|, \ldots, |x_n|\}$

d) p-Norm $||x||_p = \sum\limits_{j=1}^{n} |x_j|^p)^{1/p} = \sqrt[p]{|x_1|^p + \cdots + |x_n|^p}$

2. Für $V = C^0 = \{f : [a, b] \to \mathbb{R}, f \text{ stetig }\}, || * ||_p : V \to \mathbb{R}$

   $||f||_p := (\int\limits_a^b |f(t)|^p dt)^{1/p}$

   $||f||_2 = \sqrt{\int\limits_a^b |f(t)|^2 dt}$

   $||f||_1 = \int\limits_a^b |f(t)| dt$

   $||f||_\infty = \max\{|f(t)|, a \leq t \leq b\}$

3. Seien $(U, || * ||_u)$ und $(W, || * ||_w)$ und $V := \{A : U \to W, A \text{ linear}\}$ (dazu später mehr)

   Dann ist $(V, || * ||_v)$ ein normierter VR mit $||A||_v := \sup\{||Ax||_w : ||x||_u = I\}$

   Bsp:

   $U = W = \mathbb{R}^2, || * ||_\infty), V = \{\alpha \in Abb/\mathbb{R}^{2,2}, \mathbb{R}^{2,2}) : \alpha(x) := Ax, A \in \mathbb{R}^{2,2}$. Dann gilt:

   $||A||_\infty = \sup\{||Ax||_\infty : ||x||_\infty = 1\}$.

   Es ist $(Ax)_j = a_{j,1}x_1 + +a_{j,2}x_2$ Für x mit $\max\{|x_1|, |x_2|\} = 1$ gilt:

   $\max\{|a_{j,1}x_1 + a_{j,2}x_2|\} \leq |a_{j,1}| + |a_{j,1}|$

   Wobei Gleichheit gilt, falls x mit $x_k := sign(a_{j,k})$ Also gilt:

   $(Ax)_j = \max\{|a_{1,1}| + |a_{1,2}| + |a_{2,2}|\}$ (Zeilensummennorm).

   $\left\|\begin{matrix} 1 & 2 \\ 3 & 4 \end{matrix}\right\|_\infty = \sup\{|1| + |2|, |3| + |4|\} = 7$

4. Die "Null-Norm" (Keine Norm!)

   $||x||_0 = \sqrt[0]{\sum x_j^0}$

   Zählen die nicht Null-Einträge einer Darstellung.

   $\neg$(N1) aber (N2) $\wedge$(N3)

Bemerkung

Wir zeigen exemplarisch, dass $|| * ||_\infty$ eine Norm auf $\mathbb{R}^2$ ist, $||x||_\infty = \max\{|x_1|, |x_2|\}$.

Sei $x \in \mathbb{R}$, und $x, y \in \mathbb{R}^2$ bel.

(N1) $||\lambda x||_\infty = ||\lambda \binom{x_1}{x_2}||_\infty = ||\binom{\lambda x_1}{\lambda x_2}||_\infty = \max\{|\lambda x_1|, |\lambda x_2|\}$

$= \max\{|\lambda||x_1|, |\lambda||x_2|\} = |\lambda| \max\{|x_1|, |x_2|\} = \lambda|||x||_\infty$

(N2) Aus $|x_1|, |x_2| \leq 0$ folgt $||x||_\infty = \max\{|x_1|, |x_2|\} \geq$

Weiter gilt $||0||_\infty = \max\{0, 0\} = 0$ und $||x||_\infty = \max\{|x_1|, |x_2|\} = 0 \Rightarrow |x_1| = |x_2| = 0 \Rightarrow x = 0$

(N3) $||x + y||_\infty = ||\binom{x_1}{x_2} \oplus \binom{y_1}{y_2}||_\infty = ||\binom{x_1+y_1}{x_2+y_2}||_\infty$

$\max\{|x_1+y_1|, |x_2+y_2|\} \leq \max\{|x_1|, |y_1|, |x_2|, |y_2|\} \leq \max\{|x_1|+|x_2|\}+\max\{|y_1|+|y_2|\} = ||x||_\infty+||y||_\infty$

Da λ, x, y bel. folgt die Beh.

13.4 Vektorräume mit Skalar-Produkt

13.4.1 Euklidische Vektorräume

Definition 3.31

Sei V ein $\mathbb{K}$-VR. Eine Abbildung $< *, * >: VxV \to \mathbb{K}$ heißt Skalarprodukt in V, falls

(SP1) Linearität: $\forall \lambda \in \mathbb{K} \forall x, y, z \in V :< \lambda x + y, z >= \lambda < x, y > + < y, z >$

(SP1) Symmetrie/Hemitisch: $\forall x, y \in V :< x, y >= \overline{< y, x >}$

(SP3) Definitheit: $\forall x \in V :< x, x >\geq 0 \wedge (< x, x >= 0 \Leftrightarrow x = 0)$

Ein $\mathbb{R}$-VR V mit Skalarprodukt $< *, * >$ heißt Euklidischer Vektorraum. Ein $\mathbb{C}$-VR mit Skalarprodukt $< *, * >$ heißt unitärer VR

Beispiel 3.32

1. $V = \mathbb{R}^n, < *, * >: \mathbb{R}^n x \mathbb{R}^n \to \mathbb{R}, < x, y >_2 =< \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} >:= \sum_{j=1}^{n} \overline{y_j} x_j$

   heißt Standart Skalarprodukt im $\mathbb{R}^n$

2. $V := C^0(\mathbb{C}, \mathbb{C}) := \{f : \mathbb{C} \to \mathbb{C} : f \text{ stetig}\}, < *, * >: C^0 x X^0 \to \mathbb{C}$.

   $< f, g >:= \int\limits_C \overline{g(z)} f(z) dt$ heißt Standart Skalarprodukt im $\mathbb{C}^0$

   $V := \{f : 0, 2\pi \overset{\mathbb{R}^n}{\to} \mathbb{C}\}, e_k(t) := e^{i \frac{2\pi}{n} kt}$

3. $V = \mathbb{R}^2, < *, * >$

$< \binom{x_1}{x_2}, \binom{y_1}{y_2} := x_1y_1 - x_1y_2 - x_2y_1 + 2x_2y_2$ Ist SP.

(SP1) Sei $\lambda \in \mathbb{R}, x, y, z \in \mathbb{R}^2$ bel.

$< \lambda x + y, z >=< \binom{\lambda x_1 + y_1}{\lambda x_2 + y_2}, \binom{z_1}{z_2} >$

$= (\lambda x_1, y_2)z_1 - (\lambda x_1 + y_1)z_2 - (\lambda x_2 + y_2)z_1 + 2(\lambda x_2 + y_2)z_2$

$\lambda(x_1z_2 - x_1z_2 - x_2z_1 + +2x_2z_2) + 2y_1z_1 - y_1z_2 - y_2z_1 - y_2z_1 + 2y_2z_2$

$\lambda < \binom{x_1}{x_2}, \binom{z_1}{z_2} > + < \binom{y_1}{y_2}, \binom{z_1}{z_2} >= \lambda < x, z > + < y, z >$.

(SP2) Für alle $x, y \in \mathbb{R}^2$ gilt $< x, z > - < \binom{x_1}{x_2}, \binom{z_1}{z_2} >= x_1z_2 - x_1z_2 - x_2z_1 + 2x_2z_2 = z_1x_1 - z_1x_2 - z_2x_1 + 2x_2z_2 - < \binom{z_1}{z_2}, \binom{x_1}{x_2} >=< z, x >$

$< x, x >=< \binom{x_1}{x_2}, \binom{x_1}{x_2} = x_1^2 - 2x_1, x_2 + 2x_2^2 = (x_1 - x_2)^2 + x_2^2 \geq 0$

und $< x, x >= 0 \Leftrightarrow x_1 - x_2 = 0 \wedge x_2 = 0 \Leftrightarrow x_1 = 0 \wedge x_2 = 0 \Leftrightarrow x = 0$

Lemma 3.33

Sei $(V, < *, * >)$ VR mit SP

Es gilt : $\forall x \in V :< 0, x >=< x, 0 >= 0$

Beweis

$< x, 0 > \overset{(SP2}{=} < 0, x >=< x - x, x > \overset{(SP1)}{=} < x, x > - < x, x >= 0$ □

Satz 3.34 (Couchy-Schwarze Ungleichung -CSU)

Sei $(V, < *, * >)$ ein VR mit SP. für alle $x, y \in V$ gilt $| < x, y > |^2 \leq< x, x >< y, y >$

Beweis

Für $y = 0$ folgt Behauptung aus Lemma 3.33.

Sei nun $y \neq 0 \Leftrightarrow< y, y >\neq 0$ Mit der klugen Wahl $\lambda = 0 \overset{(SP3)}{\leq} < x - \lambda y, x - \lambda y >$

$\overset{(SP1)}{=} < x, x - \lambda y > - \lambda < y, x - \lambda y > \overset{(SP2)}{=} \overline{< x - \lambda y, x >} - \lambda \overline{< x - \lambda y, y >} \overset{(SP1)}{=} \overline{< x, x >} - \lambda \overline{< y, x >} - \lambda(\overline{< x, y > - \lambda < y, y >})$

$\overset{(SP2)}{=} < x, x > - \overline{\lambda} < x, y > - \lambda \overline{< x, y >} + |\lambda|^2 < y, y >$

$=< x, x > - 2Re[\overline{\lambda} < x, y >] + |\lambda|^2 < y, y >$

$\Leftrightarrow 0 \leq< x, x > - 2Re[\frac{\overline{\overline{<x,y>}}}{<y,y>} < x, y >] + \frac{|<x,y>|^2}{<y,y>^2} < y, y >\leq< x, x > - 1\frac{|<x,y>|^2}{<y,y>^2}$

$| < x, y > |^2 \leq < x, x >< y, y >$ □

Satz 3.35

Jeder VR mit SP ist auch normierter VR: $|| * || : V \to \mathbb{R}, ||x|| := \sqrt{< x, x >}$.

Beweis

Wegen (SP2) gilt $\forall x \in V :< x, x >= \overline{< x, x >} \Rightarrow < x, x > \in \mathbb{R}$

Wegen (SP3) gilt $\forall x \in V :< x, x > \geq 0$ und damit ist

$||x|| = \sqrt{< x, x >}$ also positive Lösung der Gleichung $a^2 - b$ wohldefiniert.

(N1) Für alle $\lambda \in \mathbb{K}$ und $x \in V$ gilt :

$||\lambda x|| = \sqrt{< \lambda x, \lambda x} \overset{(SP1)}{=} \sqrt{\lambda < x, \lambda x >} \overset{(SP2)}{=} \sqrt{\lambda\overline{\lambda}\overline{< x, x >}} \overset{(SP2)}{=} |\lambda|\sqrt{< x, x >} = |\lambda|||x||-$

(N2) $\forall x \in V$ gilt $||x|| = \sqrt{< x, x >} \geq 0$ Weiter gilt: $||x|| = 0 \Leftrightarrow < x, x > \overset{(SP3)}{\Leftrightarrow} x = 0$

(N2) Folgt aus CSU: Für alle $x, y \in V$

$||x + y||^2 = < x + y, x + y > = <, x, > +2Re[< x, y >]+ < y, y >$

$\leq < x, x > +2| < x, y > |+ < y, y >$

$\leq ||x||^2 + 2||x||||y|| + ||y||^2 = (||x|| + ||y||)^2$

Beidseitige Wurzelbehandlung zeigt $\triangle$-Ungleichung.

Bemerkung

Für VR mit SP und induzierter Norm wird die CSU zu $| < x, y > | \leq ||x|| * ||y||$

Satz 3.36

Sei $(V, < *, * >)$ VR mit SP und induzierter Norm. $\forall x, y \in V : | < x, y > | = ||x|| * ||y|| \Leftrightarrow (x, y)$ l.a.

Beweis

$'' \Rightarrow ''$ aus $0 = < x, \lambda y, x + \lambda y >$ folgt $x + \lambda y = 0$, d.h (x, y) l.a.

$'' \Leftarrow ''$ Angenommen (x, y) l.a Ohne Einschränkung $x = \lambda y$ Damit gilt:

$| < x, y > | = | < \lambda y, y > \overset{(SP1)}{=} |\lambda| < y, y > = |\lambda|||y||||y||$

$= ||\lambda y||||y|| = ||x||||y||$, also Gleichheit in CSU.

Beispiel 3.37

Das Standart SP im $\mathbb{R}^n < x, y >_2 = \sum_{j=1}^{n} x_j y_j$

$||x||_2 = \sqrt{< x, x >_2} = \sqrt{|x|^2 + |x_2|^2 + \cdots + |x_n|^2}$

Mit Satz 3.35 folgt,dass $|| * ||_2$ eine Norm ist. Mit CSU:

$\sum_{j=1}^{n} x_j y_j)^2 \leq ($
$sum x_j^2)(\sum y_j^2)$

$-||x||||y|| \leq < x, y > \leq ||x||||y||$

$-1 \leq \frac{< x, y >}{||x||||y||} \leq 1$ falls $x, y \neq 0$

$\cos(\alpha)$

Korollar 3.38 (Satz von Pythagoras

Sei V ein VR mit SP. und induzierter Norm, dann gilt:

$\forall x, y \in V : ||x + y||^2 = ||x||^2 + ||y||^2 + 2Re[< x, y >]$

Beweis

$||x + y||^2 = < x + y, x + y > = < x, x > + < y, y > + 2Re[< x, y >]$ □