Vorlesungsmitschrift Mathematik I
WS 2001/2002 bei Prof. Dr. H. Upmeier

J.C. Hühn,
HuehnJ@Mathematik.Uni-Marburg.de

Herbst / Winter 2001

Inhaltsverzeichnis

1 Logik und Mengenlehre **3**
1.1 Grundlagen der Logik und der Mengenlehre . . . 3
1.1.1 Aussage . . . 3
1.1.2 Junktoren (Verknüpfungen) . . . 3
1.1.3 Junktoren-Kalkül . . . 3
1.1.4 Quantoren-Logik . . . 4
1.1.5 Satz de Morgan für Aussageformen . . . 4
1.2 Mengen und Teilmengen . . . 5
1.2.1 Mengen, naiv nach Cantor: . . . 5
1.2.2 Mengen <- -> Aussagen . . . 5
1.2.3 Teilmengenbeziehungen . . . 6
1.2.4 Tautologien (immer wahr) . . . 6
1.2.5 Teilmenge . . . 6
1.2.6 Durchschnitt . . . 6
1.2.7 Vereinigung . . . 7
1.2.8 Negation: Komplement M . . . 7
1.2.9 Relatives Komplement N/M . . . 7
1.2.10 Regeln für Teilmengen . . . 7
1.2.11 Kontraposition . . . 8
1.3 Mengen der natuerlichen Zahlen . . . 9
1.3.1 Teilmengen (endliche) . . . 9
1.3.2 Teilmengen (unendliche) . . . 9
1.3.3 Prinzip der vollständigen Induktion . . . 9
1.3.4 Beweis durch Induktion . . . 9
1.3.5 Anwedungs des Induktionsprinzips . . . 9
1.3.6 Binomialkoeffizient . . . 10
1.3.7 Gauss'sche Summenformel . . . 11
1.3.8 Definition durch Induktion . . . 11
1.3.9 endliche Mengen . . . 11
1.3.10 Singleton (Einermenge) . . . 12
1.3.11 Definition jeder einzelnen natürlichen Zahl $n \in \mathbb{N}$ . . . 12
1.4 Relationen und Funktionen . . . 13
1.4.1 Kartesisches Produkt . . . 13
1.4.2 Relationen . . . 14
1.4.3 Umkehrrelation . . . 16
1.4.4 Bildmenge und Urbildmenge . . . 19
1.5 Funktionen . . . 21
1.5.1 Überalldefiniertheit . . . 21
1.5.2 Surjektivität . . . 22
1.5.3 Eindeutigkeit . . . 22
1.5.4 Injektivität . . . 22
1.5.5 Funktion . . . 24
1.5.6 binäre Funktion . . . 26
1.5.7 charakteristische Funktion . . . 27
1.5.8 Eigenschaften von Funktionen . . . 27
1.5.9 Bijektivität von Funktionen . . . 28
1.6 Äquivalenzrelationen . . . 31
1.6.1 Definition der Äquivalenzrelation . . . 31

1.6.2 Quotientenmenge 33
1.6.3 Kanonische Projektion 34

2 Algebraische Strukturen **37**
2.1 Verknüpfungen und Halbgruppen 37
2.1.1 Halbgruppe 37
2.1.2 Neutrales Element 37
2.1.3 Äquivalenz-Klassen 39
2.1.4 Menge aller Äquivalenz-Klassen 39
2.1.5 Inverses Element 41
2.1.6 Gruppe 42
2.2 Permutations-Gruppen 42
2.2.1 Satz zur Permutationsgruppe 43
2.2.2 zyklische Permutation, k-Zykel 43
2.2.3 Gruppentafel, Matrix 45
2.2.4 Signum 47
2.3 Ringe und Körper 48
2.3.1 Satz von Jacobson 49
2.3.2 Matrizen-Ringe 49
2.3.3 Matrizen-Produkt 50
2.4 Gauss-Algorithmus 52
2.4.1 Zeilenreduktion 53
2.4.2 Invertierung von quadratischen Matrizen 54
2.5 Lineaere Gleichungssysteme 56
2.5.1 Homogenes lineares Gleichungssystem 56
2.5.2 Inhomogenes lineares Gleichungssytem 57
2.5.3 Allgemeine Lösung von inhomogenen Problemen 58
2.6 Untergruppen und Quotienten 59
2.6.1 Quotienten-Menge 61
2.6.2 Euklidscher Algorithmus (Division mit Rest) 61
2.7 Gruppen-Homomorphismen 64
2.7.1 Definition Homomorphismus 64
2.7.2 Definition Isomorphismus 64
2.7.3 Homomorphie-Satz 66
2.8 Ideale und Quotienten-Ringe 68
2.8.1 Definition Ideal 68

3 Vektorräume und lineare Abbildungen **71**
3.1 Vektorräume 71
3.1.1 Vektoren anschaulich 72
3.1.2 Quotienten-Raum 74
3.2 Lineare Abbildung 74
3.3 Lineare Unabhängigkeit | Basis 78
3.3.1 Proposition: Linearkombination 78
3.3.2 Defintion: lineare Unabhängigkeit 78
3.3.3 Linearer Aufspann (lineares Erzeugnis) 79
3.3.4 Definition: Erzeugenden-System 81
3.3.5 Methoden zur Basis-Konstruktion 82
3.3.6 Definition der Matrizen-Transposition 84
3.3.7 Orthogonales Komplement 86

3.3.8 Additionstheorem 89
3.4 Determinanten und Eigenwerte 90
3.4.1 Anwendung der Determinanten 90
3.4.2 Eigenwerte 90
3.4.3 Diagonalisierung von Matrizen 91

Anmerkung zur 1. kompletten Auflage im März 2002

Liebe(r) Mathematikbegeister(te) :-)
Diese Mitschrift beinhaltet einen Großteil der Tafelanschriebe der Vorlesung Mathematik 1 für Informatiker an der Philipps-Universität Marburg im Wintersemester 01 / 02 bei Herrn Professor Upmeier. Diese Mitschrift stellt nicht den Anspruch die komplette Vorlesung wiederzugeben, geschweige denn die Nummerierung der Vorlesung beizubehalten. Darüber möchte ich darauf hinweisen, dass sich vermutlich noch unzählige Fehler in diesem Dokument befinden. Wer einen Fehler findet, der darf ihn behalten oder mich (am besten per eMail) darüber informieren, so dass ich den Fehler für spätere korrigierte Fassungen entfernen kann.
Darüber hinaus möchte ich darauf hinweisen, dass die Weiterverwendung dieses Dokuments außer zu privaten Zwecke nur mit meiner ausdrücklichen Erlaubnis geschehen darf. Ganz besonders bedanken möchte ich mich bei Peter Geschel und Tim Dörnemann, die mir ihre Vorlesungsmitschriebe gerne zur Verfügung stellten, sowie bei allen, die mir hilfreich zur Seite standen.

Ich wünsche viel Spass beim Lernen der Linearen Algebra und hoffe dieses Mitschrift kann ein wenig behilflich sein
Jens

http://www.mathematik.uni-marburg.de/ huehnj/

Griechische Buchstaben

α	Alpha	β	Beta	γ	Gamma	δ	Delta
ϵ	Epsilon	ζ	Zeta	η	Eta	θ	Theta
ι	Iota	κ	Kappa	λ	Lambda	μ	My
ν	Ny	ξ	Xi	o	Omikron	π	Pi
ρ	Rho	σ	Sigma	τ	Tau	υ	Ypsilon
ϕ	Phi	χ	Chi	ψ	Psi	ω	Omega

Fraktur-Font

$\mathfrak{A}$	A	$\mathfrak{B}$	B	$\mathfrak{C}$	C	$\mathfrak{D}$	D
$\mathfrak{E}$	E	$\mathfrak{F}$	F	$\mathfrak{G}$	G	$\mathfrak{H}$	H
$\mathfrak{I}$	I	$\mathfrak{J}$	J	$\mathfrak{K}$	K	$\mathfrak{L}$	L
$\mathfrak{M}$	M	$\mathfrak{N}$	N	$\mathfrak{O}$	O	$\mathfrak{P}$	P
$\mathfrak{Q}$	Q	$\mathfrak{R}$	R	$\mathfrak{S}$	S	$\mathfrak{T}$	T
$\mathfrak{U}$	U	$\mathfrak{V}$	V	$\mathfrak{W}$	W	$\mathfrak{X}$	X
$\mathfrak{Y}$	Y	$\mathfrak{Z}$	Z				

1 Logik und Mengenlehre

1.1 Grundlagen der Logik und der Mengenlehre

1.1.1 Aussage

A entweder wahr (W)oder falsch (F)

Beispiele

- A = Sie sind leise (W)
- A = Seid leise! (Keine Aussage)
- A = Marburg ist schön (W)
- A = Marburg ist jung (F)

1.1.2 Junktoren (Verknüpfungen)

A, B Aussagen $\Rightarrow$ ($A \wedge B$), ($A \vee B$), $\overline{A}$ = $\neg\, A$

Wahrheitstafel

A	B	$A \wedge B$
W	W	W
W	F	F
F	W	F
F	F	F

A	B	$A \vee B$
W	W	W
W	F	W
F	W	W
F	F	F

A	$\neg A$
W	F
F	W

1.1.3 Junktoren-Kalkül

Seien A, B, C Aussagen
Dann gilt:

(i) Kommutativität: $A \wedge B \Leftrightarrow B \wedge A$, $A \vee B \Leftrightarrow B \vee A$
(ii)Assoziativität: $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$,
$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$
(iii)Idempotenz: $A \wedge A \Leftrightarrow A \Leftrightarrow A \vee A$
(iv)Distributivität: $(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$
$(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$
(v)de Morgan: $\overline{\overline{A}} = A$
$\overline{A \wedge B} = \overline{A} \vee \overline{B}$
$\overline{A \vee B} = \overline{A} \wedge \overline{B}$

Beweis durch Wahrheitstafeln

A	B	C	$A \wedge B$	$(\mathbf{A} \wedge \mathbf{B}) \vee \mathbf{C}$	$A \vee C$	$B \vee C$	$(\mathbf{A} \vee \mathbf{C}) \wedge (\mathbf{B} \vee \mathbf{C})$
W	W	W	W	W	W	W	W
W	W	F	W	W	W	W	W
W	F	W	F	W	W	W	W
W	F	F	F	F	W	F	F
F	W	W	F	W	W	W	W
F	W	F	F	F	F	W	F
F	F	W	F	W	W	W	W
F	F	F	F	F	F	F	F

1.1.4 Quantoren-Logik

All-Quantor $\forall x$, für alle x
Existenz-Quantor $\exists x$, es existiert mindestens ein x

(i) Sei $A(x)$ Aussageform $\Rightarrow$ Aussage: $\forall x A(x)$ wahr
$\Leftrightarrow A(x)$ wahr für alle $A(x)$
(ii)Sei $A(x)$ Aussageform $\Rightarrow$ Aussage: $\exists x A(x)$ wahr
$\Leftrightarrow A(x)$ wahr für mind. ein x$A(x)$

1.1.5 Satz de Morgan für Aussageformen

(i) $\overline{\forall x A(x)} = \neg(\forall x A(x)) = \exists x A(x)$
(ii)$\overline{\exists x A(x)} = \neg(\exists x A(x)) = \forall x A(x)$

Beweis

$\overline{Für\ alle\ x\ A(x)\ ist\ wahr}$ $\Leftrightarrow$ Für alle x gilt A(x) ist falsch
$\Leftrightarrow$ es gibt mind. ein x, so dass $\overline{A(x)}$ nicht gilt
$\Leftrightarrow$ es gibt mindestens ein x, so dass $\overline{A(x)}$ wahr ist
$\Leftrightarrow \overline{\exists x A(x)}$ wahr ist.
Also ist $\forall x A(x)$ wahr $\Leftrightarrow \exists x(A)x$ wahr. q.e.d.

Beispiel

x = Hochhäuser, Studenten, Autos, Sonnentage, Einwohner
$A(\,)$ = Marburg hat viele ( )

Dann gilt: $\forall x A(x)$ falsch (x = Sonnentage, Hochhäuser)
$\forall x A(x)$ wahr (x = Studenten)

Beispiel

$A = \forall x \exists y \forall z\ A(x,y,z) \Leftrightarrow$ für alle x gibt es ein y, so dass für alle z, $A(x,y,z)$ gilt.
Negation $\overline{A} = \overline{\forall x \exists y \forall z\ A(x,y,z)} = \exists y \forall y \exists z\ \overline{A(x,y,z)}$

1.2 Mengen und Teilmengen

1.2.1 Mengen, naiv nach Cantor:

Eine Menge M ist eine Zusammenfassung von wohlunterschiedenen Objekten (Elementen) zu einem Ganzen.
Formal

Elementbezeichnung: $\in$, $x \in M$ zweistelling

Mengenklammern: $\{:\}$

1.2.2 Mengen <- -> Aussagen

M Menge $\Rightarrow$ Aussageform $A(x) : x \in M$
$x \in M$ wahr oder falsch
Falls wahr, dann $x \in M$
Falls falsch, dann $x \notin M$

$A(x)$ Aussageform $\Rightarrow$ Menge $M = \{x : A(x)$ wahr$\}$
Also $x \in M \Leftrightarrow A(x)$ wahr
M, N Mengen $M = N \Leftrightarrow \forall x\ (x \in M \Leftrightarrow x \in N)$

Beispiel 1
M = { Marburg, Mathematik, Matrix }
$x \in M \Leftrightarrow x$ = Marburg oder x = Mathematik oder x = Matrix
x = Giessen $\notin M$

Beispiel 2
Pi = $\pi = 3.14\ldots$
M = Menge aller Ziffern $(0, 1, \ldots, 9)$, welche in π unendlich oft vorkommen. Unbekannt ob $0 \in M$

Beispiel 3

Variable $x = \begin{cases} Hochhäuser \\ Autos \\ Einwohner \\ Studenten \\ Sonnentage \end{cases}$

$A(x)$ = Marburg hat viele x (Aussageform)

zugehörige Menge:

M = $\{x : A(x)$ wahr $\}$

= { Autos, Einwohner, Studenten }

$x \in M \Leftrightarrow x$ = Autos, Einwohner, Studenten

$x \notin M \Leftrightarrow x$ = Hochhäuser, Sonnentage

Beispiel 4
x = Tage im Jahr 2000

$A(x)$ = Am Tage x scheint in Marburg die Sonne.
$M = \{x : A(x) \text{ wahr } \} = \{$ 4. Mai, 3. Juni, 4. Juli, 10. Oktober$\}$
M hat 4 Elemente.

1.2.3 Teilmengenbeziehungen

Aussagen A, B, C
Aussage $A \Rightarrow B := B \vee \overline{A}$ (unsymmetrisch)
enspricht: A impliziert B / wenn A, dann B

Wahrheitstafel

A	B	$A \Rightarrow B$
W	W	W
W	F	F
F	W	W
F	F	W

1.2.4 Tautologien (immer wahr)

reflexiv: $A \Rightarrow B$

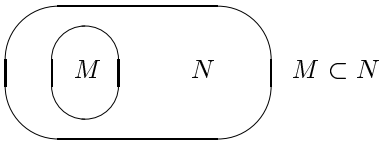
transitiv: $A \Rightarrow B \wedge B \Rightarrow C$, dann $A \Rightarrow C$

anti-symmetrisch: $A = B \wedge B = A$, dann $A \Leftrightarrow B$

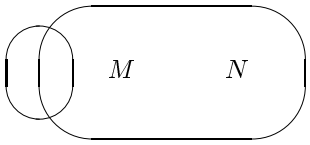
1.2.5 Teilmenge

Seien M, N Mengen
$M \subset N :\Leftrightarrow \forall x x \in M \Rightarrow x \in N$

Venn-Diagramm



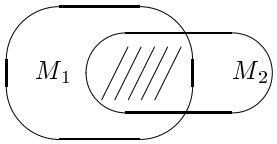
$M \subset N$



$$M \not\subset N \Leftrightarrow \overline{M \subset N}$$
$$\Leftrightarrow \overline{\forall x(x \in M \Rightarrow x \in N)}$$
$$\Leftrightarrow \exists x \overline{(x \in M \Rightarrow x \in N)}$$

1.2.6 Durchschnitt

M_1, M_2 Mengen
$M_1 \cap M_2 = \{x \in M_1 \wedge x \in M_2\}$
$x \in M_1 \cap M_2 \Leftrightarrow x \in M_1 \wedge x \in M_2$
Venn-Diagramm

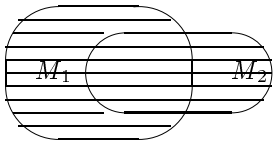


$M_1 \cap M_2$

1.2.7 Vereinigung

$M_1 \cup M_2 = \{x \in M_1 \vee x \in M_2\}$

Venn-Diagramm

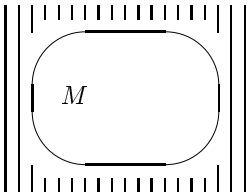


$M_1 \cup M_2$

1.2.8 Negation: Komplement M

$\overline{M} = \{x : x \in M\}$
$x \in \overline{M} \Leftrightarrow x \notin M$

Venn-Diagramm

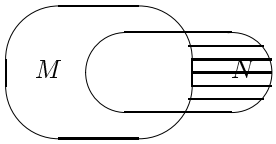


$\overline{M}$

1.2.9 Relatives Komplement N/M

$N/M = \{x : x \in N \wedge x \notin M\}$
$= N \cap \overline{M}$

Venn-Diagramm



$N \setminus M$

1.2.10 Regeln für Teilmengen

$M_1 \cap M_2 = M_2 \cap M_1$ ebenso $\cup$	kommutativ
$(M_1 \cap M_2) \cap M_3 = M_1 \cap (M_2 \cap M_3)$ ebenso $\cup$	assoziativ
$M \cap M = M = M \cup M$	idempotent
$(M_1 \cap M_2) \cup M_3 = (M_1 \cup M_3) \cap (M_2 \cup M_3)$	distributiv

Beweis: Distributivität
$(M_1 \cap M_2) \cup M_3 = (M_1 \cup M_3) \cap (M_2 \cup M_3)$

1. Schritt: $(M_1 \cap M_2) \cup M_3 \subset (M_1 \cup M_3) \cap (M_2 \cup M_3)$
z.z. $\forall x \in (M_1 \cap M_2) \cup M_3 \Rightarrow x \in (M_1 \cup M_3) \cap (M_2 \cup M_3)$
Sei $x \in (M_1 \cap M_2) \cup M_3 \Rightarrow x \in (M_1 \cap M_2) \vee x \in M_3$

IF $x \in M_1 \cap M_2 \Rightarrow x \in M_1 \wedge x \ \in M_2$

$\Rightarrow x \in M_1 \cup M_3 \wedge x \in M_2 \cup M_3$

$\Rightarrow x \in (M_1 \cup M_3) \cap x \in (M_2 \cup M_3)$

IF $x \in M_3$

$x \in M_3 \cup M_1 \wedge x \in M_3 \cup M_2$

$\Rightarrow x \in (M_1 \cup M_3) \cap x \in (M_2 \cup M_3)$

Da $x \in M$ beliebig, gilt $(M_1 \cap M_2) \subset M_3 (M_1 \cup M_3) \cap (M_2 \cup M_3)$.

2. Schritt: $(M_1 \cap M_2) \supset M_3 (M_1 \cup M_3) \cap (M_2 \cup M_3)$
z.z. $\forall x x \in (M_1 \cup M_3) \cap (M_2 \cup M_3) \Rightarrow \in (M_1 \cap M_2) \cup M_3$
Sei $x \in (M_1 \cup M_3) \cap (M_2 \cup M_3) \Rightarrow x \in (M_1 \cup M_3) \wedge x \in (M_2 \cup M_3)$

IF $x \in M_3 \Rightarrow x \in (M_1 \cap M_2) \cup M_3$

IF $x \notin M_3 \Rightarrow x \in M_1 \wedge x \in M_2$, da $x \in (M_1 \cup M_3) \cap (M_2 \cup M_3)$

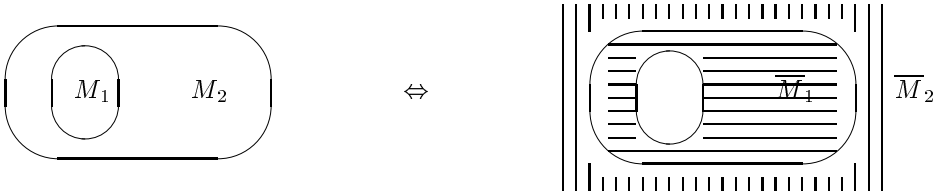
Also $x \in M_1 \cap M_2 \Rightarrow x \in (M_1 \cap M_2) \cup M_3$.
In beiden Fällen gilt $x \in (M_1 \cap M_2) \cup M_3$.
Da $x \in (M_1 \cup M_3) \cap (M_2 \cup M_3)$ beliebig war,
$(M_1 \cap M_2) \cup M_3 \subset (M_1 \cup M_3) \cap (M_2 \cup M_3)$.

1.2.11 Kontraposition

Aussagen:
$A \Rightarrow B$ genau dann, wenn $\overline{B} \Rightarrow \overline{A}$
aus A folgt B $\Leftrightarrow$ aus nicht B folgt nicht A

Mengen:
$M_1 \subset M_2 \Leftrightarrow \overline{M_2} \subset \overline{M_1}$

Venn-Diagramm



Beweis in zwei Schritten
$\Rightarrow$ z.z.: $M_1 \subset M_2 \Rightarrow \overline{M}_2 \subset \overline{M}_1$

Sei also $M_1 \subset M_2$, z.z.: $\overline{M}_2 \subset \overline{M}_1$
z.z.: $x\, in \overline{M}_2 \Rightarrow x \in \overline{M}_1$. Sei $x \in \overline{M}_2$
z.z.: $x \in \overline{M}_1$
Annahme: $x \notin \overline{M}_1 \Rightarrow x \in M_1 \Rightarrow x\, in M_2 \Rightarrow x \notin \overline{M}_2$
Also Annahme $x \notin \overline{M}_1$ falsch $\Rightarrow x \in \overline{M}_1$
Da $x \in \overline{M}_2 beliebig \Rightarrow \overline{M}_2 \subset \overline{M}_1$

"$\Leftarrow$" analog zu "$\Rightarrow$"

1.3 Mengen der natuerlichen Zahlen

$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$ unendlich viele Elemente

1.3.1 Teilmengen (endliche)

Ziffern: $\{0, 1, 2, 3, \ldots, 9\} \in \mathbb{N}, \quad \{0, 1\} \in \mathbb{N}$

1.3.2 Teilmengen (unendliche)

gerade Zahlen: $n \in \mathbb{N} \Leftrightarrow \exists m \in \mathbb{N}, n = 2m$

1.3.3 Prinzip der vollständigen Induktion

Sei $S \subset \mathbb{N}$ mit	$0 \in S$	Induktionsanfang
	$n \in S \Rightarrow n + 1 \in S$	Induktionsschritt

Dann gilt $S = \mathbb{N}$

1.3.4 Beweis durch Induktion

Sei $A(n)$ Aussage, die von $n \in \mathbb{N}$ abhängt.

Es gelte: (i) A(0) = wahr
(ii)wenn $A(n)$ wahr $\Rightarrow A(n + 1)$ wahr

Dann ist $A(n)$ wahr $\forall n \in \mathbb{N}$

1.3.5 Anwedungs des Induktionsprinzips

Sei $n \in \mathbb{N}, n \geq 0$
Fakultät: $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$

1.3.6 Binomialkoeffizient

$\binom{n}{m} = \frac{n!}{m!\cdot(n-m)!} \in \mathbb{N}$

Satz
Sei $0 < m \leq n \Rightarrow \binom{n}{m} = \binom{n}{m-1} + \binom{n+1}{m}$

Beweis

$$\begin{aligned}
\binom{n}{m} \cdot \binom{n}{m-1} &= \frac{n!}{m!\cdot(n-m)!} + \frac{n!}{(m-1)!\cdot(n-m+1)!} \\
&= \frac{n!}{(m-1)!\cdot m\cdot(n-m)!} + \frac{n!}{(m-1)!\cdot(n-m+1)\cdot(n-m)!} \\
&= \frac{n!}{(m-1)!\cdot(n-m)!} \cdot \left(\frac{1}{m} + \frac{1}{n-m+1}\right) \\
&= \frac{n!}{(m-1)!\cdot(n-m)!} \cdot \frac{n+1}{m\cdot(n-m+1)} \\
&= \frac{n!\cdot(n+1)}{(m-1)!\cdot m\cdot(n-m)!\cdot(n-m+1)} \\
&= \frac{(n+1)!}{m!\cdot(n+1-m)!} \\
&= \binom{n+1}{m}
\end{aligned}$$

Satz
$\forall n \in \mathbb{N}$ ist $n \cdot (n+1)$ gerade, daher durch 2 teilbar.

1. Beweis (Fallunterscheidung ohne Induktion)
Sei $n \in \mathbb{N}$ gegeben.

IF (Im Fall) n gerade $\Rightarrow \exists m \in \mathbb{N} : n = 2m$
$\Rightarrow n(n+1) = 2m(2m+1) = 2[m(2m+1)]$ gerade, da $m(2m+1) \in \mathbb{N}$
IF n ungerade $\Rightarrow \exists m \in \mathbb{N} : n = 2m+1$
$\Rightarrow n(n+1) = (2m+1)(2m+2) = (2m+1)(m+2)\cdot 2$ gerade,
da $(2m+1)(m+2) \in \mathbb{N}$
Beide Fälle ergeben die Behauptung.

2. Beweis (volständige Induktion für $n \geq 0$)

IV: Induktionsvoraussetzung: $A(n) = n(n+1)$ ist gerade

IA: Induktionsanfang $n = 0$: $0(0+1) = 0 gerade \Rightarrow A(0)$ wahr

IS: Induktionsschritt: $0 \leq n \rightarrow n+1$
Sei $A(n)$ wahr, daher $n(n+1)$ gerade. z.z.: $(n+1)(n+2)$ gerade
Nach IV gilt $\exists m \in \mathbb{N}\, n(n+1) = 2m$
$\Rightarrow (n+1)(n+2) \overset{=}{_{distr.}} (n+1)n + (n+1)2 \overset{=}{_{komm.}} n(n+1) + 2(n+1)$
$\overset{=}{_{IV}} 2m + 2(n+1) \overset{=}{_{distr.}} 2(m+n+1)$ gerade, da $(m+n+1) \in \mathbb{N}$
$\Rightarrow A(n+1)$ wahr $\Rightarrow A(n)$ wahr $\forall n \in \mathbb{N}$

1.3.7 Gauss'sche Summenformel

$0+1+2+3+4+5+\cdots+n=\sum_{k=0}^{n}k=\frac{n(n+1)}{2}\in\mathbb{N}$
$sum_{k=0}^{0}k=0$ leere Summe

Beweis durch Induktion

$Ind_{n\geq 0}\qquad A(n)=\sum_{k=0}^{n}k=\frac{n(n+1)}{2}$

IA: $n=0$: $A(0)=\sum_{k=0}^{0}k=\frac{0(0+1)}{2}=0$
IV: $\sum_{k=0}^{n}k=\frac{n(n+1)}{2}$
IS: $0\leq n\rightarrow n+1$
$\sum_{k=0}^{n+1}k=\sum_{k=0}^{n}k+\sum_{k=n+1}^{n+1}k=\sum_{k=0}^{n}k+n+1\underset{IV.}{=}\frac{n(n+1)}{2}+n+1$
$(n+1)(\frac{n}{2}+1)=(n+1)(\frac{n+2}{2})=\frac{(n+1)+(n+2)}{2}\qquad q.e.d.$

1.3.8 Definition durch Induktion

Sei $D(n)$ Definition, die von n abhängt.
Falls (i) $D(0)$ definiert (ii) wenn $D(n)$ definiert, dann $D(n+1)$ definiert.
Dann ist $D(n)\forall n\in\mathbb{N}$ definiert.
Definition
$0!:=1$ leeres Produkt. $(n+1)!:=(n+1)n!$. Dann ist $n!$ definiert $\forall n\in\mathbb{N}$.

Mulitplikations-Beispiel
Fakultät (factorial)
$6!=1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6=6\cdot 5!$
$1000!=1\cdot 2\cdot\ldots\cdot 1000=1000\cdot 999!$

Additions-Beispiel
$1+2+3+4+5+6=\sum_{k=1}^{5}(k)+6$

1.3.9 endliche Mengen

Definition
Sei M Menge
M endlich $\Leftrightarrow$ M enthält nur endlich viele Elemente.
$M=\underbrace{\{x_1,x_2,\ldots,x_n\}}_{\text{paarweise verschieden}}$
M hat n Elemente: $x_1\ldots x_n$
$|M|=n=\#M$, Anzahl der Elemente.

Satz
Seien $M_1\subset M_2$ Mengen. Dann gilt:

(i) M_2 endlich $\Rightarrow$ M_1 endlich $\wedge$ $|M_1|\leq|M_2|$
(ii) M_2 endlich, $|M_1|=|M_2|\Rightarrow M_1=M_2$

Beispiel endlicher Mengen
leere Menge $\emptyset := \{x : x \neq x\} = \{x : x \in x\} = \{\ \}$
Dann gilt $\emptyset$ endlich und $|\emptyset| = 0$

Satz
Jede Menge enthält $\emptyset$ als Teilmenge, daher: M Menge $\Rightarrow \emptyset \subset M$
Beweis
z.z.: $\emptyset \subset M$
z.z.: $x \in \emptyset \Rightarrow x \in M$

Kontraposition:
Sei $x \notin M$. $x \notin \emptyset$ immer wahr.
Da x beliebig $\Rightarrow \emptyset \subset M$

1.3.10 Singleton (Einermenge)

$\{a\} := \{x : x = a\}$
$x \in \{a\} \Leftrightarrow x = a$

Satz
$\{a\}$ unendlich und $|\{a\}| = 1$
Satz
$\{a\} \subset M \Leftrightarrow a \in M$
$\{a\} \cup \{b\} = \{a \cup b\}$, höchstens zwei Elemente, mindestens eins

Beweis
$\{a\} \cup \{b\} = \{x : x \in \{a\} \vee x \in \{b\}\} = \{x : x = a \vee x = b\} = \{a, b\}$

1.3.11 Definition jeder einzelnen natürlichen Zahl $n \in \mathbb{N}$

$0 := \emptyset$
Annahmem n sei definiert als Menge: $n + 1 = n \cup \{n\}$ (daher $n \in n \subset n + 1$)

Damit ist n definiert.

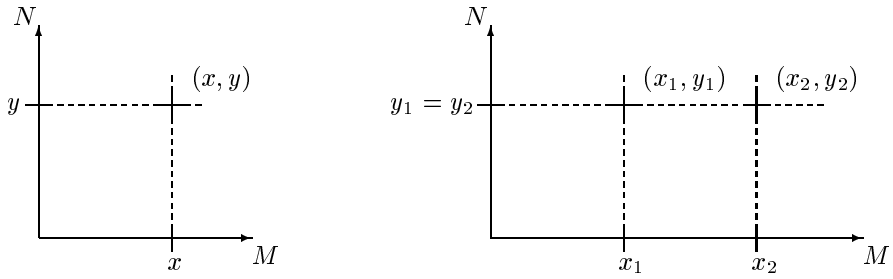
Beispiel
$0 = \{\ \}$
$1 := 0 \cup \{0\} = \{0\} = \{\{\}\}$
$2 := 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\}$
$3 := 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\}$
Satz

(i) n endliche Menge und $|n| = n$
(ii)Seien $m, n \in \mathbb{N}$ mit $m = \{0, 1, \ldots, m-1\}, n = \{0, 1, \ldots, n-1\}$
Dann gilt:
$m \subset n \Leftrightarrow m \in n$
$m \cup n = max(m, n)$ Maximum
$m \cap n = min(m, n)$ Minimum

1.4 Relationen und Funktionen

geordnetes Paar

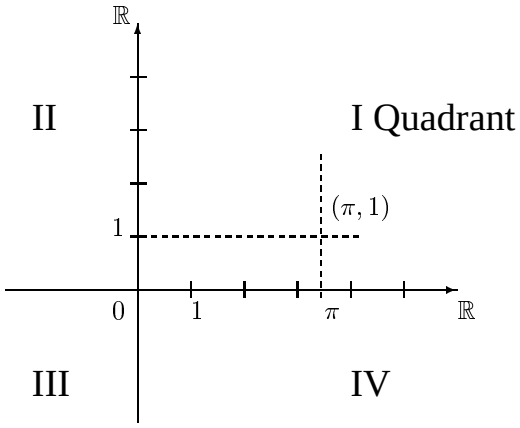
Seien M, N Mengen. $x \in M, y \in N$
$(x, y) := \{x, \{x, y\}\} = \{x\} \cup \{\{x, y\}\}$
Dann gilt $(x_1, y_1) = (x_2, y_2) \Leftrightarrow x_1 = x_2 \wedge y_1 = y_2$



1.4.1 Kartesisches Produkt

Definition
$M \times N := \{(x, y) : x \in M \wedge y \in N\}$ = Menge aller geordneten Paare
$\mathbb{R}$ = Zahlengerade; Menge aller reellen Zahlen. $\mathbb{R} \times \mathbb{R}$ = Ebene

$M = \mathbb{R}, N = \mathbb{R}$
$\Rightarrow M \times N = \mathbb{R}^2$



Satz
M, N endliche Mengen $\Rightarrow M \times N$ endliche Mengen und $|M \times N| = |M| \cdot |N|$

Beweis per Induktion
$n := |N|$ = Anzahl der Elemente von N

IA: $n = 0$ $\quad 0 = |N| \Rightarrow N = \emptyset$
$\Rightarrow$ es gibt keine zweite Koordinate in $M \times N$

$\Rightarrow M \times N = \emptyset$
$\Rightarrow |M \times N| = 0 = |M| \cdot 0 = |M| \cdot |N|$
Formel gilt für $|N| = 0$

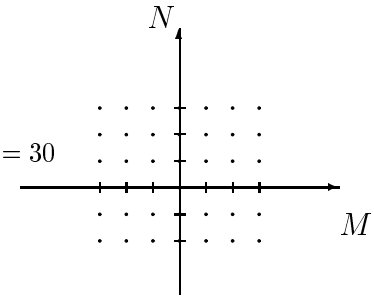
IA: $n = 1$ Sei $N = 1$ daher $N = \{y_0\} \Rightarrow M \times N = \{(x, y)|x \in M \wedge y \in N\}$
$= \{(x, y)|x \in M \wedge y = y_0\}$
$= \{(x, y_0)|x \in M\}$
$\Rightarrow |M \times N| = |M| \cdot |N| = |M| \cdot 1 = |M|$
Formel gilt für $|N| = 1$

IV: $|M \times N| = |M| \cdot |N| \quad \forall N\, |N| = n \wedge \forall M$

IS: $n \to n + 1$ z.z.: $|M \times N| = |M| \cdot |N|$ mit $|N| = n + 1$
Sei $|N| = n + 1 \Rightarrow N \neq \emptyset \Rightarrow \exists y_0 \in N$
$\Rightarrow |N \backslash \{y_0\}| = |N| - 1 = n + 1 - 1 = n$
$\Rightarrow M \times N = \{(x, y)|x \in M \wedge y \in N\}$
$= \{(x, y)|x \in M \wedge y \in N \wedge y \neq y_0\} \cup \{(x, y)|x \in M \wedge y \in N \wedge y = y_0\}$
$= \{(x, y)|x \in M \wedge y \in N \wedge y \neq y_0\} \cup \{(x, y_0)|x \in M\}$
$\Rightarrow |M \times N| = |M \times N \backslash \{y_0\}| + |M \times \{y_0\}|$
$\underset{IV}{=} |M| \cdot |N \backslash \{y_0\}| + |M|\}$
$= |M| \cdot n + |M| = |M| \cdot (n + 1) = |M| \cdot |N|$
Formel gilt auch für $|N| = n + 1$ Elemente

Beispiel:

$|M| = 6$
$|N| = 5$
$|M \times N| = |M| \cdot |N| = 6 \cdot 5 = 30$

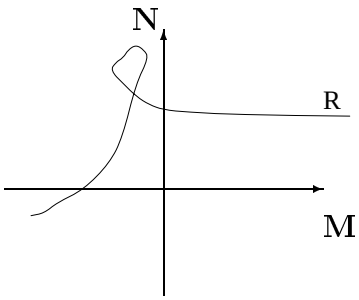


1.4.2 Relationen

Seien M, N Mengen
Betrachte $M \times N$

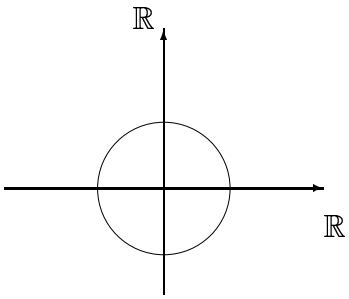
Relation $R \subset M \times N$
R Relation von M nach N
Relation = Menge geordneter Paare
$(x, y) \in R : x \in M \wedge y \in N$

graphische Darstellung



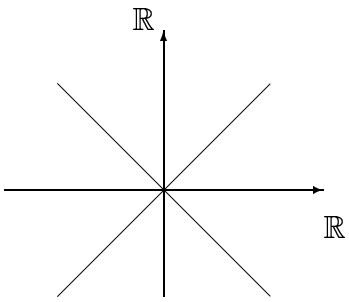
Beispiel 1: Kreis

$M = \mathbb{R} = N$
$R = \{(x, y) : x \in \mathbb{R} \wedge y \in \mathbb{R} : x^2 + y^2 = 1\}$



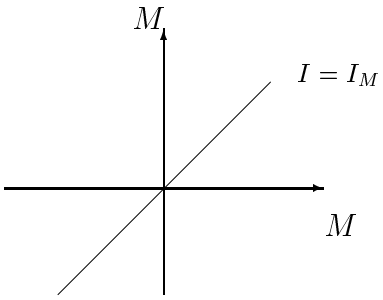
Beispiel 2: Kreuz

$S = \{(x, y) : x \in \mathbb{R} \wedge y \in \mathbb{R} : y = \pm x\} = \{(x, y) \in \mathbb{R} \times \mathbb{R} | y^2 = x^2\}$



Beispiel 3: Diagonale

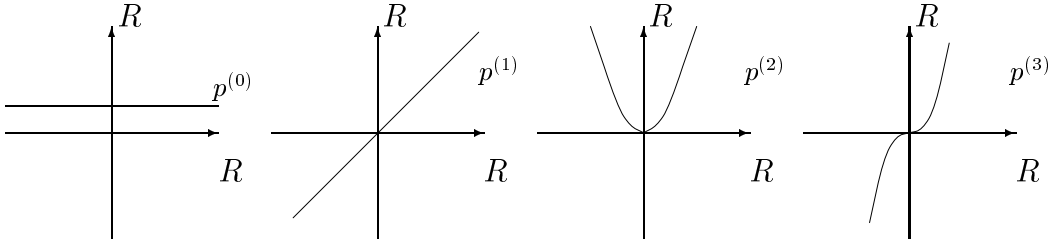
$I = \{(x,y)|xinM \wedge y \in M|x = y\} = \{(x,y) \in M \times M|x = y\}$
$= \{(x,x)|x \in M$



Beispiel 4: Potenzrelationen

$m \in \mathbb{N}$

$p(m) = \{(x,y)|x \in \mathbb{R} \wedge y \in \mathbb{R}|y = x^m\} = \{(x,y) \in \mathbb{R} \times \mathbb{R}|y = x^m\} = \{(x,x^m)|x \in \mathbb{R}\}$



1.4.3 Umkehrrelation

X, Y Mengen, Produktmengen $X \times Y \supset$ Relation

$X \times X \supset I = I_X = \{x_1, x_2 \in X \times X|x_1 = x_2\}$ Identität / Diagonale
$(x_1, x_2) \in I \Leftrightarrow x_1 = x_2$

Definition

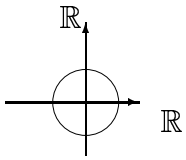
$X \times Y \supset R \Rightarrow Y \times X \supset R^{-1} := \{(y,x) \in Y \times X|(x,y) \in R\}$
$(y,x) \in R^{-1} \Leftrightarrow (x,y) \in R$, Inverse von R

$X \times Y \supset R, Y \times Z \supset S \Rightarrow X \times Z \supset S \circ R :=$
$\{(x,z) \in X \times Z|\exists y \in Y(x,y) \in R \wedge (y,z) \in S\}$

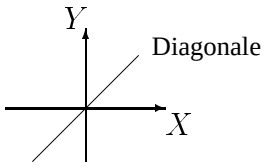
Produkt von R und S: Komposition von R und S:

$(x,z) \in S \circ R :\Leftrightarrow \exists y \in Y\, (x,y) \in S \wedge (y,z) \in R$

Beispiel 1: Kreis
$X = Y = Z = \mathbb{R}$
$C = \{(x,y) : x \in \mathbb{R} \wedge y \in \mathbb{R} : x^2 + y^2 = 1\}$
$C^{-1} = C$

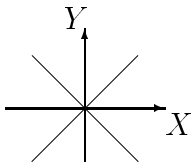


Beispiel 2: Gerade
$X = Y = \mathbb{R}$



Beispiel 3: Kreuz

Kreuz $S = \{(x,y) : x \in \mathbb{R} \wedge y \in \mathbb{R} : x^2 = y^2\}$
Potenz $P = P^{(2)} = \{(x,y) : x \in \mathbb{R} \wedge y \in \mathbb{R} : x = y^2\}$

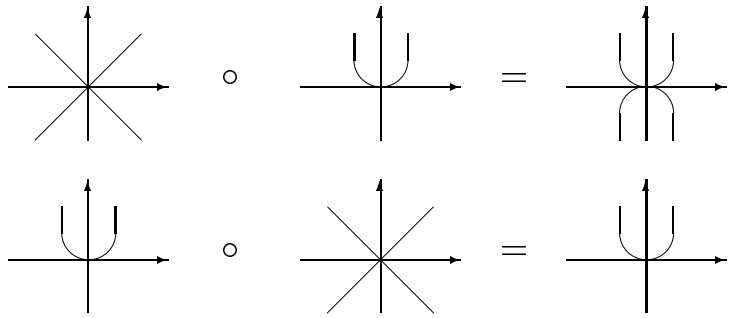


1. Behauptung: $\underbrace{P}_{y,z} \circ \underbrace{S}_{x,y} = \underbrace{P}_{x,z}$
Sei $(x,z) \in P \circ S \Rightarrow \exists y \in Y\, \underbrace{(x,y) \in S}_{x^2=y^2} \wedge \underbrace{(y,z) \in P}_{z=y^2} \Rightarrow x^2 = z$
$\Rightarrow (x,z) \in P$. Also $P \circ S \subset P$.
Sei $(x,z) \in P \Rightarrow z^2 = x$. Setze $y = x \Rightarrow y^2 = x^2 \wedge z = y^2$
$\Rightarrow (x,y) \in S \wedge (y,z) \in P \Rightarrow (x,z) \in P \circ S$. ($y = (-x)$ analog)

Beispiel 4: Kreuz

Kreuz $S = \{(x,y) : x \in \mathbb{R} \wedge y \in \mathbb{R} : x^2 = y^2\}$
Potenz $P = P^{(2)} = \{(x,y) : x \in \mathbb{R} \wedge y \in \mathbb{R} : x = y^2\}$

$S \circ P = \{(x,z) | z = \pm x^2\}$



Regeln für Inverses und Komposition

Seien R, S, T Relationen. Dann gilt:

(i) $T \circ (S \circ R) = (T \circ S) \circ R$ Assoziativität
(ii) $(S \circ R)^{-1} = R^{-1} \circ S^{-1}, R^{-1} = R$
(iii) $\left.\begin{array}{l} R \circ I_X = R \\ I_Y \circ R = R \end{array}\right\}$ neutral

Beweis zu (i)

"$\subset$" z.z.: $T \circ (S \circ R) \subset (T \circ S) \circ R$
Sei $(x, w) \in T \circ (S \circ R) \Rightarrow \exists z\, (x, z) \in S \circ R \wedge (z, w) \in T$
$\exists z\, \exists y\, ((x, y) \in R \wedge (y, z) \in S) \wedge (z, w) \in T$
$\underset{assoz.}{\Rightarrow} (x, y) \in R \wedge ((y, z) \in S \wedge (z, w) \in T)$
$\Rightarrow \exists Y (x, y) \in R \wedge (y, w) \in T \circ S$
$\Rightarrow (x, w) \in (T \circ S) \circ R$
Da (x, w) beliebig $\Rightarrow T \circ (S \circ R) \subset (T \circ S) \circ R$

"$\supset$" analog durch Umkehrung aller Schritte.

Bemerkung

$R \circ S$ nicht immer definiert, falls x, y, z verschieden sind:
$x = y = z \Rightarrow R \circ S, S \circ R$ wohldefiniert. $R \circ S \neq S \circ R$ im Allgemeinen.

Beweis zu (ii)

"$\subset$" z.z.: $(S \circ R)^{-1} \subset R^{-1} \circ S^{-1}$
Sei $(z, x) \in (S \circ R)^{-1} \Rightarrow (x, z)\, in S \circ R$
$\Rightarrow \exists y\, (x, y) \in R \wedge (y, z) \in S$
$\Rightarrow \exists y\, (y, x) \in R^{-1} \wedge (z, y) \in S^{-1}$
$\underset{Kommu.}{\Rightarrow} \exists y\, (y, x) \in S^{-1} \wedge (y, z) \in R^{-1}$
$\Rightarrow (z, x) \in R^{-1} \circ S^{-1}$
Da (z, x) beliebig $\Rightarrow (S \circ R)^{-1} \subset R^{-1} \circ S^{-1}$. Umkehrung "$\supset$" analog.

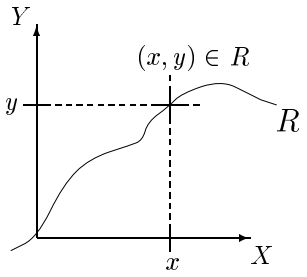
1.4.4 Bildmenge und Urbildmenge

Definition

Sei $R \subset X \times Y$
$x \in X \Rightarrow \{x\} \subset X$ Einermenge
$R\{x\} \subset Y$ Bildmenge von x

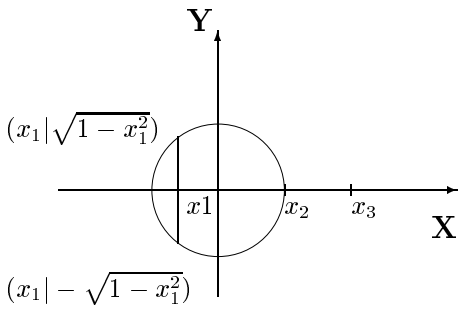
Ohne Mengenklammer: $y \in k\{x\} \Leftrightarrow (x, y) \in R$

Beispiel 1



$R\{x\} = \{y\}$ Einermenge

Beispiel 2



$R = \{(x, y) \in R \times R | x^2 + y^2 = 1\}$

$X = Y = R$

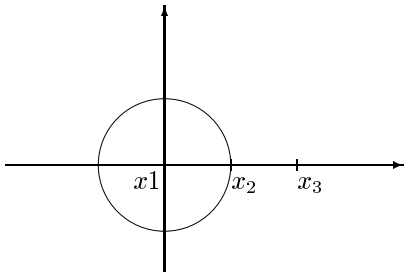
$R\{x_1\} = \{\sqrt{1 - x_1^2}| - \sqrt{1 - x_1^2}\}$
$R\{x_2\} = 0$
$R\{x_3\} = \emptyset$

Definition

Sei $R \subset X \times Y \qquad A \subset X$
Bildmenge von A:
$RA = R(A) := \{y \in Y | \exists x \in A | (x, y) \in R\}$
$R(A) \subset Y$

Definition ohne Mengenklammern:
$y \in R(A) \Leftrightarrow \exists x \in A (x, y) \in R$

Beispiel



$A = \{x_1, x_2, x_3\} = \{x_1\} \cup \{x_2\} \cup \{x_3\}$

$R(A) = \{y \in R | (x_1, y) \in R \vee (x_2, y) \in R \vee (x_3, y) \in R\}$

$= R\{x_1\} \vee R\{x_2\} \vee R\{x_3\}$
$= \{\sqrt{1-x_1^2}, -\sqrt{1-x_1^2}, 0\}$ Dreiermenge

Satz
$R \subset X \times Y, \quad S \subset Y \times Z, \quad A \subset X$
$\Rightarrow (S \circ R)(A) = S(\underbrace{R(A)}_{\subset Y}) \subset Z$

Beweis

"$\subset$" z.z.: $\Rightarrow (S \circ R)(A) \subset S(R(A)) \subset Z$
Sei $z \in (S \circ R)(A) \underset{Def.Bildmenge}{\Rightarrow} \exists x \in A\ (x, z) \in (S \circ R)$
$\underset{Def.Verkettung}{\Rightarrow} \exists y \in Y\ (x, y) \in R \wedge (y, z) \in S$
$\Rightarrow \exists y \in Y\ \exists x \in A\ (x, y) \in R \wedge (y, z) \in S$
$\Rightarrow \exists y \in Y\ \underbrace{y \in R(A)}_{\subset Y} \wedge (y, z) \in S$
$\Rightarrow z \in S(R(A))$
Da z beliebig $\Rightarrow (S \circ R)(A) \subset S(R(A)) \subset Z$. "$\supset$" analog.

Korrolar

$(S \circ R)\{x\} = S(R\{x\})$, wobei $\{x\}$ nicht immer Einermenge.

Beweis

A = {x}

Satz

$R \subset X \times Y$, $A, B \subset X$. Es gilt:

(i) $A \subset B \Rightarrow R(A) \subset R(B)$
(ii) $R(A \cup B) \Rightarrow R(A) \cup R(B)$
(iii) $R(A \cap B) \Rightarrow R(A) \cap R(B)$
(iv) $R(A \backslash B) \Rightarrow R(A) \backslash R(B)$

Beweis von (ii)

"$\subset$" z.z.: $R(A \cup B) \subset R(A) \cup R(B)$

Sei $y \in R(A \cup B) \underset{Def.Bildmenge}{\Rightarrow} \exists x \in A \cap B : (x,y) \in R$

IF: $x \in A \Rightarrow y \in R(A) \subset R(A) \cup R(B)$
$\Rightarrow y \in R(A) \cup R(B)$
IF: $x \in B \Rightarrow y \in R(B) \subset R(B) \cup R(A)$
$\Rightarrow y \in R(A) \cup R(B)$
Da y beliebig $\Rightarrow R(A \cup B) \subset R(A) \cup R(B)$

1.5 Funktionen

1.5.1 Überalldefiniertheit

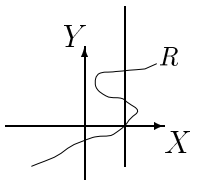
Seien X, Y Mengen, $R \subset X \times Y$ Relation

Definition
R überall definiert $:\Leftrightarrow \forall x \in X \quad R\{x\} \neq \emptyset \Leftrightarrow \forall x \in X \exists y \in Y \ (x,y) \in R$

Beispiel 1

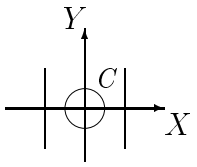
Jede Vertikale Gerade schneidet R.

R überall definiert



Beispiel 2

Kreis ist nicht überall definiert.



Satz

R ist überall defniniert $\Leftrightarrow I_X \subset R^{-1} \circ R$

Beweis

"$\Rightarrow$": Sei R überall definiert. z.z.: $I_X \subset R^{-1} \circ R$
Sei $(x_1, x_2) \in I_X \Rightarrow x_1 = x_2 =: x \in X \Rightarrow \exists y \in Y \ (x,y) \in R$
$\underset{Idemp.}{\Rightarrow} \exists y \in Y (x,y) \in R \wedge (x,y) \in R$
$\Rightarrow \exists y \in Y (y,x) \in R^{-1} \wedge (x,y) \in R$
$\Rightarrow (x,x) \in R^{-1} \circ R \Rightarrow I_X \subset R^{-1} \circ R.$
"$\Leftarrow$": Sei $I_X \subset R^{-1} \circ R$. z.z.: R überall definiert.
Sei $x \in X \Rightarrow (x,x) \in I_X \Rightarrow (x,x) \in R^{-1} \circ R$
$\underset{Def.Kompos.}{\Rightarrow} \exists y \in Y (x,y) \in R \wedge (y,x) \in R^{-1}$
$\Rightarrow \exists y \in Y (x,y) \in R \wedge (x,y) \in R$

$\Rightarrow \exists y \in Y (x, y) \in R \Rightarrow y \in R\{x\} \Rightarrow R$ überall definiert.

1.5.2 Surjektivität

Definition

$R \subset X \times Y$ surjektiv $\Leftrightarrow R^{-1} \subset Y \times X$ überall definiert
$\Leftrightarrow \forall y \in Y \exists x \in X\ (y, x) \in R^{-1}$
$\Leftrightarrow \forall y \in Y \exists x \in X\ (x, y) \in R$
$\overset{}{\underset{Satz für R^{-1}}{\Leftrightarrow}} I_Y \subset R \circ R^{-1}$

1.5.3 Eindeutigkeit

Definition

$R \subset X \times Y$ eindeutig $:\Leftrightarrow \forall x \in X |R\{x\}| = 1$. $R\{x\}$ hat höchstens ein Element.
$\Leftrightarrow \forall x \in X \forall y_1, y_2 \in Y\ (x, y_1) \in R \wedge (x, y_2) \in R \Rightarrow y_1 = y_2$

Satz

R eindeutig $\Leftrightarrow R \circ R^{-1} \subset I_Y$

Beweis

"$\Rightarrow$" Sei R eindeutig. z.z.: $R \circ R^{-1} \subset I_Y$
Sei $(y_1, y_2) \in R \circ R^{-1} \Rightarrow \exists x \in X (y_1, x) \in R^{-1} \wedge (x, y_2) \in R$
$\overset{}{\underset{Reindeutig}{\Rightarrow}} \exists x \in X (x, y_1) \in R \wedge (x, y_2) \in R \Rightarrow y_1 = y_2$
$\Rightarrow (y_1, y_2) \in I_Y \Rightarrow R \circ R^{-1} \subset I_Y$

"$\Leftarrow$" Sei $\circ R^{-1} \subset I_Y$. z.z.: R eindeutig
Sei $x \in X, y_1, y_2 \in Y$ mit $(x, y_1), (x, y_2) \in R$
z.z.: $y_1 = y_2 \qquad (x, y_1) \in R \wedge (x, y_2) \in R$
$\Rightarrow (x, y_1) \in R \wedge (y_2, x) \in R^{-1} \Rightarrow (y_1, y_2) \in R \circ R^{-1}$
$\overset{}{\underset{Vor.}{\Rightarrow}} (y_1, y_2) \in I_Y \Rightarrow y_1 = y_2$

1.5.4 Injektivität

Definition

R^{-1} eindeutig $\Leftrightarrow$ R injektiv
$\Leftrightarrow \forall y \in Y \forall x_1, x_2 \in X\ (y, x_1) \in R^{-1} \wedge (y, x_2) \in R^{-1} \Rightarrow x_1 = x_2$
$\Leftrightarrow \forall y \in Y \forall x_1, x_2 \in X\ (x_1, y) \in R \wedge (x_2, y) \in R$
$\Leftrightarrow \forall y \in Y\ |R^{-1}\{x\}| \leq 1$
$\overset{}{\underset{Satz für R^{-1}}{\Leftrightarrow}}$ R injektiv $\Leftrightarrow R^{-1} \circ R \subset I_X$

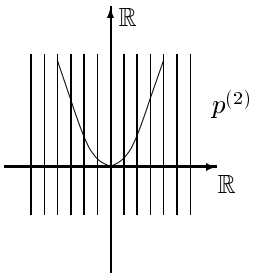
Übersicht

$R \subset X \times Y, :\ R^{-1} \subset Y \times X$

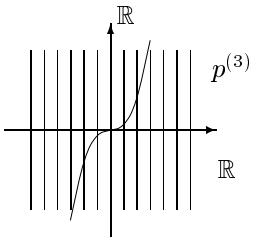
R überall definiert	$\Leftrightarrow$	$R^{-1} \circ R \supset I_X$
R eindeutig definiert	$\Leftrightarrow$	$R \circ R^{-1} \subset I_Y$
R injektiv definiert	$\Leftrightarrow$	$R^{-1} \circ R \subset I_X$
R surjektiv definiert	$\Leftrightarrow$	$R \circ R^{-1} \supset I_Y$

Graphisch

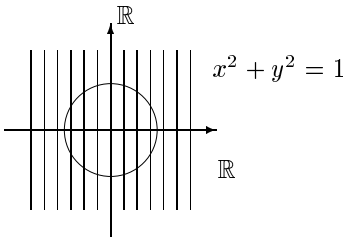
- Überalldefiniertheit $\Rightarrow$ jede vertikale Gerade schneidet R mindestens einmal.
  Bsp.: $R = P^{(2)} = \{(x, x^2) : x \in \mathbb{R}\}$



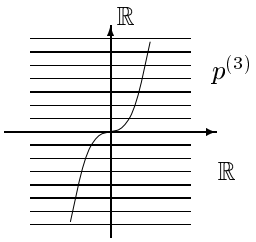
- Eindeutigkeit $\Rightarrow$ jede vertikale Gerade schneidet höchstens einmal.
  Bsp.: $R = P^{(3)} = \{(x, x^3) : x \in \mathbb{R}\}$



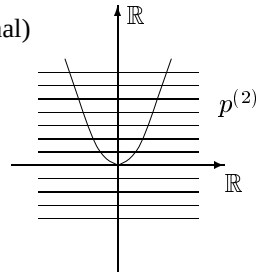
  Keine Eindeutigkeit beim Kreis



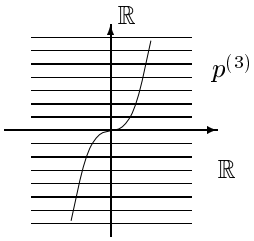
- Injektivität $\Rightarrow$ jede horizontale Gerade schneidet höchstens einmal.
  Bsp.: $R = P^{(3)} = \{(x, x^3) : x \in \mathbb{R}\}$



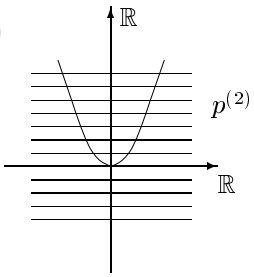
keine Injektivität (Horizontalen schneiden zweimal)



- Surjektivität $\Rightarrow$ jede horizontale Gerade schneidet mindestens einmal.
  Bsp.: $R = P^{(3)} = \{(x, x^3) : x \in \mathbb{R}\}$



keine Surjektivität (Horizontalen schneiden nicht)



1.5.5 Funktion

Definition

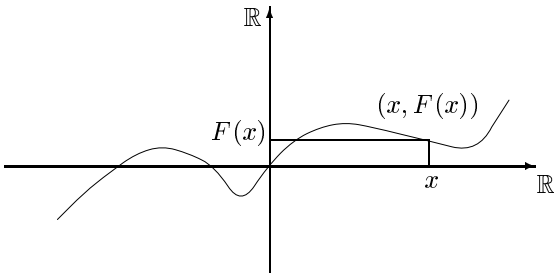
$F \subset X \times Y$ Funktion / Map von X nach Y
$\Leftrightarrow F$ überall definiert $\wedge$ F eindeutig
$\Leftrightarrow \forall x \in X \; |F\{X\}| = 1$

Definition des Funktionswertes

$F(x) \in Y$ mit $F\{x\} = \{F(x)\}$
Man schreibt $F : X \to Y, X \overset{F}{\to} Y$ für $F \subset X \times Y$ Funktion. $x \in X \to F(x) \in Y$

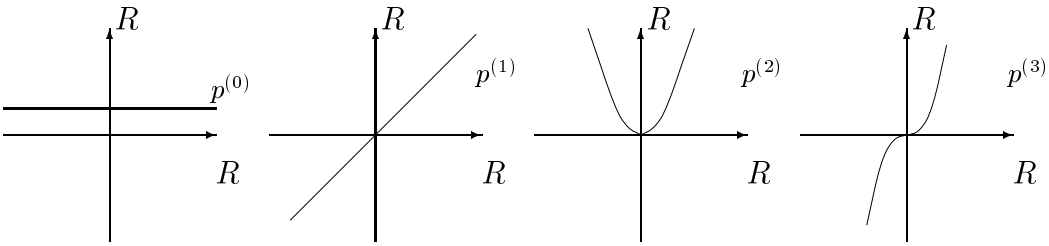
Graphisch

F Funktion $\Leftrightarrow$ jede vertikale Gerade hat genau einen Schnittpunkt.



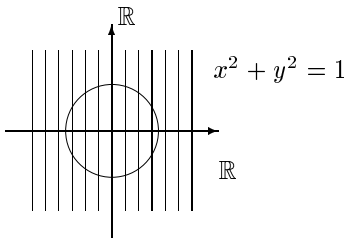
Beispiel 1

Jede Potenz $P^{(m)}$ ist Funktion von R nach R.
$P^{(m)} = \{(x, y) \in R \times R : y = x^m\}$ und $P^{(m)}(x) = x^m, P^{(m)}\{x\} = \{x^m\}$



Beispiel 2

Kreis keine Funktion.
$X = [-1, 1], Y \in \mathbb{R} \Rightarrow C \subset X \times Y$



Satz

Seien $F \subset X \times Y, G \subset Y \times X$ Relationen. Dann gilt:

(i) F überall definiert $\wedge$ G überall definiert $\Rightarrow$ $G \circ F$ überall definiert
(ii) F eindeutig $\wedge$ G eindeutig $\Rightarrow$ $G \circ F$ eindeutig
(iii) $F : X \to Y \wedge G : Y \to Z \Rightarrow G \circ F : X \to Z \wedge (G \circ F)(x) = G(F(x))$

Beweis

(i) Seien F, G überall definiert. z.z.: $G \circ F$ überall definiert.
Sei $x \in X \Rightarrow F\{x\} \neq \emptyset$
Sei $B \in Y, B \neq 0 \Rightarrow G(B) \neq 0$
$(G \circ F)\{x\} = G(\underbrace{F\{x\}}_{\neq 0}) \neq \emptyset$
Da x beliebig war, folgt F, G überall definiert.

(ii) Seien F, G eindeutig. z.z.: $G \circ F$ eindeutig.
Sei $x \in X \Rightarrow |F(x)| \leq 1$
$B \subset Y, |B| = 1 \Rightarrow |G(B)| \leq 1$
$\Rightarrow |(G \circ F)| = |G(\underbrace{F\{x\}}_{|F\{x\})| \leq 1}| \leq 1$

Satz

$X \overset{F}{\to} Y \overset{G}{\to} Z$ Funktionen $\Rightarrow X \overset{G \circ F}{\to}$ Funktionen
und $(G \circ F)(x) = G(F(x))$.

Beweis

$x \in X \Rightarrow F\{x\} = \{F(x)\}, y \in Y \Rightarrow G\{y\} = \{G(y)\}$
Setze $y := F(x) \Rightarrow G\{F(x)\} = \{G(F(x))\}$
$(G \circ F)\{x\} \overset{=}{_{Satz}} G(F(x)) = G(\{F(x)\}) = \{G(F(x))\}$
Da x beliebig $\Rightarrow G \circ F$ Funktion und $(G \circ F)\{x\} = G(F(x))$

Beispiel

$F(x) = x^2 + 3, \quad G(y) = \frac{1}{y+1}$
$\Rightarrow (G \circ F) = G(F(x)) = G(x^2 + 3) = \frac{1}{x^2+3+1}$

Definition
$Y^X =$ Menge aller Funktionen von X nach$Y$: $F : X \to Y \in Y^X$

Spezialfälle:

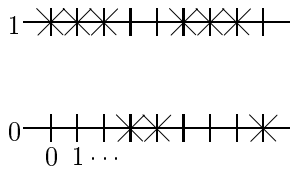
- $X = \mathbb{N}, Y$ Menge: $Y^{\mathbb{N}} = \{$ Funktionen von $\mathbb{N} \to Y\} = \{$ Folgen in $Y\}$
  $F \in Y^{\mathbb{N}}, \mathbb{N} \overset{F}{\to} Y$ also $n \mapsto F(n)$. $\quad F = (F(n))_{n \in \mathbb{N}}$ n-tes Folgenglied.
- $X = n = \{0, 1, \cdots, n-1\} \Rightarrow F : n \to Y \in Y^n$. n-Tupel
- $X = 2 = \{0, 1\} \Rightarrow F : 2 \to Y \in Y^2, F = (F(0), F(1))$
- X beliebig, $Y = 2 = \{0, 1\} \Rightarrow F : X \to 2 \in 2^X$. binäere Funktion

1.5.6 binäre Funktion

Definition
binäre Funktion auf $x \rightleftharpoons$ Teilmenge von X.
($2^X =$ Menge aller Teilmengen von X)

Beweis

Sei $F : X \to 2$. $X \times 2 =$ Zwei parallele Kopien von X.



$$\Rightarrow F^{-1}\{1\} = \{x \in X : F(x) = 1\} \subset X$$

1.5.7 charakteristische Funktion

$$\chi : X \to 2 \qquad \chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

Dann gilt:

(i) $\chi_A^{-1}(x) = A$ Gleichheit von Mengen
(ii) $\chi_{f^{-1}\{1\}} = f$ Gleichheit von Funktionen

Beweis

(i) Gleichheit von Mengen
"$\subset$" z.z.: $\chi_A^{-1}(x) \subset A$
Sei $x \in \chi_A^{-1}\{1\} \Rightarrow \chi_A(x) = 1 \Rightarrow x \in A$
Da x beliebig, $\chi_A^{-1}(x) \subset A$. "$\supset$" analog.

(ii) Gleichheit von Funktionen (alle Funktionswerte müssen gleich sein)
Sei $x \in X$. z.z.: $\chi_{f^{-1}\{1\}}(x) = f(x)$
IF: $f(x) = 1 \Rightarrow x \in f^{-1}\{1\} \Rightarrow \chi_{f^{-1}\{1\}}(x) = 1 = f(x)$
IF: $f(x) = 0 \Rightarrow x \notin f^{-1}\{1\} \Rightarrow \chi_{f^{-1}\{1\}}(x) = 0 = f(x)$
Da x beliebig, $\chi_{f^{-1}\{1\}}(x) = f(x)$

Prinzip der Funktionengleichheit

Seien $F, G : X \to Y$ Funktionen.
Dann gilt: $F = G \Leftrightarrow \forall x \in X F(x) = G(x)$.

Beispiel

2^2 = Potenzmenge von $2 = \{0, 1\}$
= Teilmengen von $\{0, 1\}$
= binäre Funktion $f : 2 \to 2$

4 Teilmengen von $2 = \{0, 1\}$: $\{0, 1\} \supset \emptyset, \{0\}, \{1\}, \{0, 1\}$

binäere Funktion:

x	$\chi_{\{\}}$	$\chi_{\{0\}}$	$\chi_{\{1\}}$	$\chi_{\{0,1\}}$
0	0	1	0	1
1	0	0	1	1

1.5.8 Eigenschaften von Funktionen

Sei $F : X \to Y$ Funktion
$F^{-1} : Y \to X$ Relation

Proposition

(i) $F\{x\} = \{F(x)\}$ Einermenge
(ii) $F^{-1}\{x\} = \{x \in X : F(x) = y\}$ Urbildmenge von Y

Beweis

(i) Definition von $F(x) \in Y$
(ii) $F^{-1}\{y\} = \{x \in X : (y, x) \in F^{-1}\}$
$= \{x \in X : (x, y) \in F\}$
$= \{x \in X : F(x) = y\}$

Proposition

(i) F injektiv $\forall x_1, x_2 \in X\, F(x_1) = F(x_2) \Rightarrow x_1 = x_2$
$\Leftrightarrow \forall x_1, x_2 \in X\, x_1 \neq x_2 \Rightarrow F(x_1) \neq F(x_2)$

(ii) F surjektiv $\forall y \in Y \exists x \in X\, F(x) = y$

1.5.9 Bijektivität von Funktionen

Definition

F bijektiv $\Leftrightarrow$ F injektiv $\wedge$ F surjektiv

Beweis

R Relation
(i) R injektiv $\Leftrightarrow \forall x_1, x_2 \in X\, \forall y \in Y\, (x_1, y) \in R \wedge (x_2, y) \in R \Rightarrow x_1 = x_2$
Sei $F \subset X \times Y$ Funktion
$y \in Y := F(x_1) = F(x_2)$
$\Rightarrow (x_1, y) = (x_1, F(x_1)) \in F \wedge (x_2, y) = (x_2, F(x_2)) \in F$
$\Rightarrow x_1 = x_2$

(ii) $R \subset X \times Y$ surjektiv $\Leftrightarrow \forall y \in Y \exists x \in X\, (x, y) \in R$
Sei $F \subset X \times Y$ Funktion, sei $y \in Y$
$\exists x \in X (x, y) \in F \Rightarrow y = F(x)$

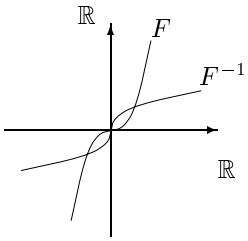
$F : X \to Y$ bijektiv $\Leftrightarrow$ F injektiv und surjektiv
$\Leftrightarrow \exists$ Umkehrfunktion $F^{-1} : Y \to X$ mit $F \circ F^{-1} = I_Y \wedge F^{-1} \circ F = I_X$

Schreibweise

$X \underset{F^{-1}}{\overset{F}{\rightleftarrows}} Y$ bijektive Funktion. $F^{-1}(F(x)) = x$ $F(F^{-1}(y)) = y$

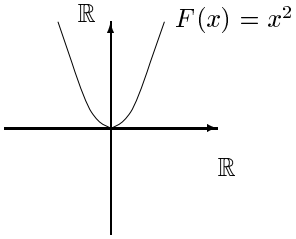
Beispiel 1

$X = \mathbb{R} = Y$ $R \overset{F=P^{(3)}}{\underset{\rightarrow}{}}$; $F(x) = x^3$
$\Rightarrow F$ bijektiv und $F^{-1} = \sqrt[3]{x}$



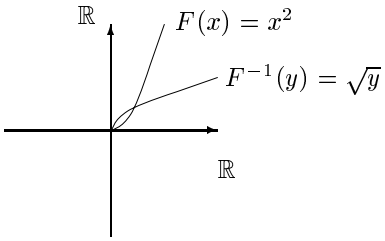
Beispiel 2

$X = \mathbb{R} = Y$ $R \overset{F=P^{(2)}}{\underset{\rightarrow}{}}$; $F(x) = x^2$
$\Rightarrow F$ nicht bijektiv, da $F(-1) = F(1) = 1$
(nicht surjektiv, da $(-1) \notin F(\mathbb{R})$)



Beispiel 2

$X = \mathbb{R}_+ = Y = \{x \in R : x \leq 0$ $F = P^{(2)}$
$F : \mathbb{R}_+ \to \mathbb{R}_+$ bijektiv



Proposition

$F \subset X \times Y; \quad A \subset X, B \subset Y$
$F^{-1} \subset Y \times X$ Umkehrrelation

Dann gilt:

(i) $F(A) = \{F(x); x \in A\}$
(ii) $F{-}1(B) = \{F^{-1}(y); y \in B\}$

Beweis

(i) F Relation

$$\begin{aligned} F(A) &= \{y \in Y; \exists x \in A; (x,y) \in F\} \\ &= \{y \in Y; \exists x \in A; F(x) = y\} \\ &= \{F(x); x \in A\} \end{aligned}$$

(i) F^{-1} Bildmenge der Relation F

$$\begin{aligned} F^{-1} &= \{\exists x \in X; y \in B; (y,x) \in F^{-1}\} \\ &= \{\exists x \in X; y \in B; (x,y) \in F\} \\ &= \{\exists x \in X; y \in B; F(x) = y\} \\ &= \{x \in X; F(x) \in B\} \end{aligned}$$

Proposition

Sei $F \subset X \times Y$ Funktion. $A \subset X; \quad B \subset Y$

(i) $A \subset F^{-1}(F(A))$ falls F injektiv
(ii) $B \subset F(F^{-1}(B))$ falls F surjektiv

Beweis

(i) Sei $x \in A \Rightarrow F(x) \in F(A) \Rightarrow x \in F^{-1}(F(A))$
(ii) Sei $y \in Y \Rightarrow F^{-1}(x) \in (F^{-1}(B) \Rightarrow y \in F(F^{-1}(B))$

Proposition

Sei $F : X \to Y$ mit Umkehrrelation $F^{-1} \subset Y \times X$
Dann gilt für $B_1, B_2 \subset Y$

(i) $F^{-1}(B_1 \cap B_2) = F^{-1}(B_1) \cap F^{-1}(B_2)$
(ii) $F^{-1}(B_1 \setminus B_2) = F^{-1}(B_1) \setminus F^{-1}(B_2)$

Beweis

(i) "$\subset$" gilt für Relation $R^{-1}(B_1 \cap B_2) \subset R^{-1}(B_1) \cap R^{-1}(B_2)$
"$\supset$" gilt nur für Funktionen
Sei $x \in F^{-1}(B_1) \cap F^{-1}(B_2)$
$\Rightarrow x \in F^{-1}(B_1) \wedge x \in F^{-1}(B_2)$
$\Rightarrow F(x) \in B_1 \wedge F(x) \in B_2$
$\Rightarrow F(x) \in (B_1 \cap B_2)$
$\Rightarrow x \in F^{-1}(B_1 \cap B_2)$
Da x belibieg, folgt $F^{-1}(B_1 \cap B_2) \supset F^{-1}(B_1) \cap F^{-1}(B_2)$

(ii) "$\supset$" gilt für Relation
"$\subset$" Sei $x \in F^{-1}(B_1 \setminus B_2)$
$\Rightarrow F(x) \in (B_1 \setminus B_2)$
$\Rightarrow F(x) \in B_1 \wedge F(x) \notin B_2$
$\Rightarrow x \in F^{-1}(B_1) \wedge x \notin F^{-1}(B_2)$
$\Rightarrow x \in F^{-1}(B_1) \setminus F{-}1(B_2)$
Da x belibieg, folgt $F^{-1}(B_1 \setminus B_2) \subset F^{-1}(B_1) \setminus F^{-1}(B_2)$

1.6 Äquivalenzrelationen

Sei X Menge
$R \subset X \times X$ Relation
$\Rightarrow R^{-1} \subset X \times X$ Umkehrrelation
$R \circ R \subset X \times X$ Verkettung
$I = I_X \subset X \times X$ Diagonale

Definition

(i) R reflexiv $\Leftrightarrow R \supset I$
$\Leftrightarrow \forall x \in X\ (x,x) \in R$

(ii) R symmetrisch $\Leftrightarrow R = R^{-1}$
$\Leftrightarrow \forall x,y \in X((x,y) \in R \Leftrightarrow (y,x) \in R)$

(iii) R transitiv $\Leftrightarrow R \supset R\circ$
$R \Leftrightarrow \forall x,y,z \in X((x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R)$

(iv) R antisymmetrisch $\Leftrightarrow R \cap R^{-1} \subset I$
$\Leftrightarrow \forall x,y \in X((x,y) \in R \wedge (y,x) \in R \Rightarrow x = y)$

1.6.1 Definition der Äquivalenzrelation

R Äquivalenz-Relation $\Leftrightarrow R$ reflexiv, symmetrisch, transitiv

$I \subset R = R^{-1} \supset R \circ R$

Man schreibt: $x \sim y$ für $(x,y) \in R$

Reflexivität: $x \sim x$
Symmetrie: $x \sim y \Leftrightarrow y \sim x$
Transitivität: $x \sim y \sim z \Rightarrow x \sim z$
Konsequenz: $x_1 \sim x_2 \sim x_3 \sim \cdots \sim x_n \Rightarrow x_1 \sim x_n$

Beispiel 1

$X = \mathbb{N}$, $R \subset \mathbb{N} \times \mathbb{N}$ Paritätsrelation, $m,n \in \mathbb{N}$

$m \sim n :\Leftrightarrow m - n$ gerade, durch 2 teilbar
$R = \{(m,n) \in \mathbb{N} \times \mathbb{N} | m - n \text{ gerade } \}$

Behauptung: "$\sim$" ist Äquaivalenzrelation

Beweis:

Reflexivität: $m \sim m$, da $m - m = 0$ gerade
Symmetrie: $m \sim n \Rightarrow m - n$ gerade $\Rightarrow n - m = -(m-n)$ gerade $\Rightarrow n \sim m$
Transitivität Sei $l \sim m \sim n \Rightarrow l - m$ gerade, $m - n$ gerade

$$\Rightarrow l - n = (l - m) + (m - n) \text{ gerade} \Rightarrow l \sim n$$

m, n haben gleiche Parität $\Leftrightarrow m \sim n$

Beispiel 2

$x = \{$ Menschen $\}, \quad x \sim y \Leftrightarrow x, y$ sind verwandt.

Definition

Sei $R \subset X \times X$ Äquivalenzrelation, $x \in X$

$$\begin{aligned} R\{x\} &= \{\exists y \in X | (x, y) \in R\} \subset X \\ &= \{\exists y \in X | x \sim y\} \end{aligned}$$

Äquivalenz-Klasse von x (”Familie von x”)
Hinweis: Wenn Äquivalenz-Klasse nicht disjunkt sind, dann sind sie gleich.

Proposition

$R\{x\} \neq \emptyset$
Beweis: R reflexiv $\Rightarrow (x, x) \in R, x \sim x \Rightarrow x \in R\{x\}$

Satz

R Äquivalenzrelation. Dann äquivalent

(i) $R\{x\} \subset R\{y\} \neq \emptyset$
(ii) $x \sim y$
(iii) $R\{x\} = R\{y\}$

Beweis per Ringschluss

$(i) \Rightarrow (ii)$ Sei $R\{x\} \cap R\{y\} \neq \emptyset$
z.z.: $x \sim y$
$\Rightarrow \exists z \in R\{x\} \cap R\{y\}$
$\Rightarrow z \in R\{x\} \wedge z \in R\{y\}$
$\Rightarrow z \sim x \wedge z \sim y \Rightarrow x \sim z \wedge z \sim y$
$\Rightarrow x \sim y$

$(ii) \Rightarrow (iii)$ Sei $x \sim y$
z.z.: $R\{x\} = R\{y\}$
”$\subset$” Sei $z \in R\{x\} \Rightarrow z \sim x$ (z.z.: $z \sim y$)
$\Rightarrow z \sim x \sim y \Rightarrow z \sim y$
Da z beliebig $R\{x\} \subset R\{y\}$
”$\supset$” $R\{y\} \subset R\{x\}$ analog, beziehungsweise $(y \sim x)$

$\underline{(iii) \Rightarrow (i)}$ Sei $R\{x\} = R\{y\}$
$\Rightarrow R\{x\} \cap R\{y\} = R\{x\} \neq \emptyset$

Man sagt:

Äquivalenz-Klasse $R\{x\}$ bilden Partitionen von X, daher verschiedene Äquivalenz-Klassen sind disjunkt. $y \in R\{x\}$ Repräsentanten von $R\{x\}$

Definition
$A, B \subset X$ sind disjunkt $\Leftrightarrow A \cap B = \emptyset$

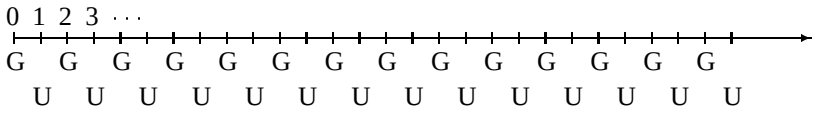
Beispiel: Paritätsrelation

$X = \mathbb{N}$ Paritätsrelation. $m \sim n \Leftrightarrow m - n$gerade

$\mathbb{N}\{0\}= \{m \in N : m \sim 0\}$ gerade Zahlen
$\mathbb{N}\{1\}= \{m \in N : m \sim 1\}$ ungerade Zahlen

$\mathbb{N}\{0\} \cap \mathbb{N}\{1\} = \emptyset$

U ungeraden Zahlen mit N{1} und G geraden Zahlen mit N{0}



1.6.2 Quotientenmenge

Sei $R \subset X \times X$ Äquivalenz-Relation
$R\{x\}, x \in X$ Äquivalenzklassen $A/B = A \cap B$

Definition $X/R = X/\sim$

$X/R =$ Menge aller Äquivalenz-Klassen
$X/R = \{R\{x\}|x \in X\}$
$x \in R\{x\} \in X/R, \quad R\{x\} \subset X$
(X/Rgesprochen als X modulo R)

Beispiel

$\mathbb{N}$ mit Parität $\sim$

$\mathbb{N}/\sim = \{N\{0\}|N\{1\}\} \hat{=} \{0, 1\}$
Zweiermenge mit $\{0, 1\}$ als Repräsentanten der geraden und ungeraden Zahlen. $\mathbb{N}/$ Parität $= 2$

Definition

Sei $R \subset X \times X$ Äquivalenz-Relation. $F : X \to YFunktion$

Man sagt: F wohldefiniert auf $X/R :\Leftrightarrow \forall x_1, x_2 \in X\ x_1 \sim x_2 \Rightarrow F(x_1) = F(x_2)$

In diesem Falle existiert $\tilde{F} : X/Y \to Y$ Abbildung.
$\tilde{F}(\underbrace{R\{x\}}_{Äqu-Klasse}) = F(\underbrace{x}_{Repräsentant})$

Beispiel

$X = \mathbb{N}$ mit Paritätsrelation. $\mathbb{N}/\sim$ = Zweiermenge
$F : \mathbb{N} \to \mathbb{Z} \quad F(n) := (-1)^n$

$\Rightarrow$ (i) F wohldefiniert auf $\mathbb{N}/\sim$
(ii)$\tilde{F}(\mathbb{N}\{0\}) = 1$
$\tilde{F}(\mathbb{N}\{1\} = (-1)$

Beweis

z.z.: $m \sim n \Rightarrow F(m) = F(n)$.
Sei $m \sim n \Rightarrow m - n$ gerade $\Rightarrow m - n = 2k | \exists k \in \mathbb{Z} \Rightarrow m = n + 2k$
$\Rightarrow F(m) = (-1)^m = (-1)^{n+2k} = (-1)^n * (-1)^{2k} = (-1)^n * ((-1)^2)^k = (-1)^n$
$= F(n)$
$\Rightarrow F$ wohldefiniert auf $\mathbb{N}/\sim$

induzierte Abbildung

$\tilde{F} : X/R \to Y$ definiert durch $\tilde{F}(R\{x\}) := F(x)$
Elementenweise: $R\{x\} \in X/R \mapsto F(x) \in Y$

1.6.3 Kanonische Projektion

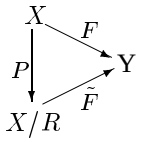
$P : X \to X/R$ surjektiv, $\forall y \in X/R \exists x \in XP(x) = y$ Elementweise: $x \in X \mapsto R\{x\} \in X/R \quad / \quad P(x) = R\{x\}$

(kanonische = natürliche)

Beweis

Sei $y \in X/R \Rightarrow y$ Äquivalenz-Klasse, $y \neq \emptyset \Rightarrow \exists x \in Y \Rightarrow y = R\{x\} = P(x)$
Da y beliebig $\Rightarrow P$ surjektiv.

Kommutatives Diagramm



daher $\tilde{F} \circ P = F$

$X \overset{\tilde{F} \circ P}{\rightarrow} Y \wedge X \overset{F}{\rightarrow} Y$

Beweis für $\tilde{F} \circ P = F$

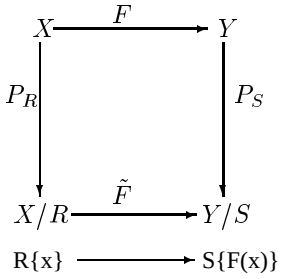
$\tilde{F} \circ P$ und F sind Abbildungen von $X \rightarrow Y$

Gleichheit $\tilde{F} \circ P$ und F elementweise:
Sei $x \in X$. z.z.: $(\tilde{F} \circ P)(x) = F(x)$
$(\tilde{F} \circ P)(x) = \tilde{F}(P(x)) = \tilde{F}(R\{x\}) = F(x)$
Da x beliebig $\Rightarrow \tilde{F} \circ P = F$

Definition

Sei $F : X \rightarrow Y$ und $R \subset X \times X, \quad S \subset Y \times Y$ Äquivalenz-Relation
Es gelte: $x_1 \tilde{R} x_2 \Rightarrow F(x_1) \tilde{S} F(x_2)$
$(x_1, x_2) \in R \Rightarrow (F(x_1), F(x_2) \in S$

Dann existiert induzierte Abbildung $\tilde{F} : X/R \rightarrow Y/S$



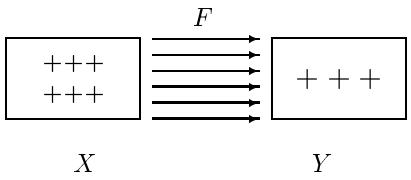
$P_S \circ F = \tilde{F} \circ P_R : X \rightarrow Y/S$

Beweis für $P_S \circ F = \tilde{F} \circ P_R$

Nach Voraussetzung ist $\tilde{F}(R\{x\}) := S\{F(x)\}$ wohldefiniert.
Das heisst, der Funktionswert ist unabhängig vom Repräsentanten.
z.z.: $P_S \circ F = \tilde{F} \circ P_R$, elementweise
Sei $x \in X$, dann gilt
$(\tilde{F} \circ P_R)(x) = \tilde{F}(P_R(x)) = \tilde{F}(R\{x\}) = S\{F(x)\} = P_S(F(x))$, da $P_S(y) = S\{y\}$
Da x beliebig $\Rightarrow \tilde{F} \circ P_R = P_S \circ F$

Beispiel für induzierte Abbildung bei Äquivalenz-Relation

Sei $F : X \rightarrow Y$ Abbildung



F surjektiv, aber nicht injektiv

Satz

(i) $F^{-1} \circ F \subset X \times X$ Äquivalenz-Relation
(ii) $x_1 \sim x_2 \Rightarrow F(x_1) = F(x_2)$
(iii) induzierte Abbildung $\tilde{F} : X/F^{-1} \circ F \to Y$
$(F^{-1} \circ F)\{x\} \mapsto F(x)$ injektiv

Beweis

(i) Übungsaufgabe
(ii) $x_1 \sim x_2 \Leftrightarrow x_1, x_2 \in F^{-1} \circ F$
$\Leftrightarrow \exists y \in Y\,(x_1, y) \in F \wedge (y, x_2) \in F^{-1}$
$\Leftrightarrow \exists y \in Y\,(x_1, y) \in F \wedge (x_2, y) \in F$
$\Leftrightarrow \exists y \in Y\; y = F(x_1) \wedge y = F(x_2)$
$\Leftrightarrow F(x_1) = F(x_2)$
(iii) Nach (ii) ist F auf $X/\sim$ wohldefiniert.
Sei $\tilde{F} : X/\sim \to Y$ induzierte Abbildung.

Äquivalenzklasse $(F^{-1} \circ F)\{x\} \mapsto F(x)$
z.z.: $\tilde{F}$ ist injektiv: z.z: $F(x_1) = F(x_2) \Rightarrow (F^{-1} \circ F\{x_1) = (F^{-1} \circ F)\{x_2\}$
Sei $F(x_1) = F(x_2) \Rightarrow x_1 \sim x_2 \overset{\Rightarrow}{_{Prop.}} (F^{-1} \circ F)\{x_1\} = (F^{-1} \circ F)\{x_2\}$
Da x_1, x_2 beliebig $\Rightarrow \tilde{F}$ injektiv.

Beispiel: Kanonische Projektion

Sei $R \subset X \times X$ Äquivalenz-Relation.
$X/\sim = \{R\{x\} : x \in X\}$ Quotienten-Menge.

Kanonische Projektion: $P : X \to X/\sim$ surjektiv
$x \mapsto R\{x\}$
$\underline{P(x) := R\{x\}}$

Satz
$P^{-1} \circ P = R$

Beweis

$(x_1, x_2) \in P^{-1} \circ P \Leftrightarrow P(x_1) = P(x_2) \Leftrightarrow R\{x_1\} = R\{x_2\}$
$\overset{\Leftrightarrow}{_{Prop.}} x_1 \sim x_2 \Leftrightarrow (x_1, x_2) \in R$

2 Algebraische Strukturen

2.1 Verknüpfungen und Halbgruppen

Sei P Menge. Produktmenge: $P \times P = P^2$ mit $(p, q) \in P^2$

Definition

Verknüpfung $P \times P \overset{*}{\to} P$; elementweise: $(x, y) \mapsto x * y$
Definiere: $x * y := *(x, y)$

Beispiel: Addition

$P = \mathbb{N} = \{0, 1, 2, 3, \cdots\}$
$\mathbb{N} \times \mathbb{N} \overset{+}{\to} \mathbb{N}$; elementweise: $(x, y) \mapsto x + y$
$x + y := +(x, y)$

Beispiel: Multiplikation

$\mathbb{N} \times \mathbb{N} \overset{\times}{\to} \mathbb{N}$; elementweise: $(m, n) \mapsto m \times n = m \cdot n = mn$
$m \times n := \times(m, n)$

2.1.1 Halbgruppe

Definition

Sei $(P, *)$ Menge mit Verknüpfung $P \times P \overset{*}{\to} P$
P Halbgruppe (semigroup) $\Leftrightarrow *$ ist assoziativ
$x, y, z \in P.$ $\quad (x * y) * z = x * (y * z)$

2.1.2 Neutrales Element

Definition

$o \in P$ mit Eigenschaft $\forall p \in P \; p * o = p = o * p$

Beispiel

Halbgruppe $(\mathbb{N}, +)$ $\quad o = 0 \quad p + 0 = p = 0 + p$

Halbgruppe $(\mathbb{N}, \times)$ $\quad o = 1 \quad p \times 1 = p = 1 \times p$

Kommutativgesetz

$(P, *)$ kommutativ (abelsch) $\Leftrightarrow \forall p, q \in P : \quad p * q = q * p$

Proposition

Das neutrale Element ist eindeutig.

Beweis

Seien $o_1, o_2 \in P$ neutrale Elemente. z.z.: $o_1 = o_2$.
Daher gilt: $o_1 = o_1 * o_2 = o_2$

Schreibweise

$(P, +, 0)$ Additive Halbgruppe
$(P, \times, 1)$ Multiplikative Halbgruppe

Satz

$(\mathbb{N}, +, 0)$ Additive Halbgruppe, kommutativ.
das heisst: $\forall a, b, c \in N\, (a + b) + c = a + (b + c)$
und $a + b = b + a$, sowie $a + 0 = a = 0 + a$

Satz

$(\mathbb{N}, \times, 1)$ Multiplikative Halbgruppe, kommutativ.
das heisst: $\forall a, b, c \in N\, (ab)c = a(bc)$
und $ab = ba$, sowie $a \cdot 1 = a = 1 \cdot a$

Definition

$(P, *)$ Halbgruppe, $Q \subset P$

(i) Q Unterhalbgruppe $\Leftrightarrow \forall q_1, q_2 \in Q\ q_1 * q_2 \in Q \qquad (Q * Q \subset Q)$
(ii) Q kürzbar (cancellation) $\Leftrightarrow \forall p_1, p_2 \in P\ \forall q \in Q\ \ p_1 * q = p_2 * q \Rightarrow p_1 = p_2$

Beispiel 1

$P = \mathbb{N}$, mit Addition +

Beh. $Q = P = \mathbb{N}$ kürzbar bezüglich +.
Bew. Seien $p_1, p_2 \in \mathbb{N}$ und $q \in \mathbb{N}$ mit $p_1 + q = +_2 + q \Rightarrow p_1 = p_2$

Beispiel 2

$P = \mathbb{N}$, mit Multiplikation $\times$

Dann: (i) $Q_1 = \mathbb{N}$ nicht kürzbar
(ii) $Q_2 = \mathbb{N}\backslash\{0\} = \{1, 2, 3, \cdots\}$ kürzbar

Bew: (i) Seien $p_1, p_2 \in \mathbb{N}, p_1 \neq p_2 \qquad q := 0 \in Q_1$
$\Rightarrow p_1 \times q = p_1 \times 0 = 0 = p_2 \times 0 = p_2 \times q$
0 nicht kürzbar
(ii) $Q_2 = \mathbb{N}\backslash\{0\}$, seien $p_1, p_2 \in \mathbb{N}$ und $q \in Q_2$ mit $p_1 \times q = p_2 \times q$

$\Rightarrow p_1 \times q = p_2 \times q \Rightarrow p_1 = p_2 \Rightarrow Q_2$ kürzbar

Satz

Sei $(P, *)$ kommutative Halbgruppe. Sei $Q \subset P$ Unterhalbgruppe und Q kürzbar.

Relation auf $P \times Q$ mit $(p,q) \in P \times Q$: $(p,q) \sim (p',q') :\Leftrightarrow p * q' = p' * q$
Dann ist $\sim$ Äquivalenz-Relation.

Beweis

reflexiv: z.z.:$(p,q) \sim (p,q) \quad \Rightarrow p * q = p * q$

symmetrie: Sei $(p,q) \sim (p',q')$. z.z.: $(p',q') \sim (p,q)$
$(p,q) \sim (p',q') \Rightarrow p * q' = p' * q \Rightarrow p' * q = p * q' \Rightarrow (p,q') \sim (p,q)$

transitiv: Sei $(p,q) \sim (p',q') \sim (p'',q'')$. z.z.. $(p,q) \sim (p'',q'')$
Da $(p,q) \sim (p',q') \Rightarrow p * q' = p' * q$
$(p',q') \sim (p'',q'') \Rightarrow p' * q'' = p'' * q'$
$\Rightarrow (p * q'') * q' \overset{=}{}_{assoz} p * (q'' * q') \overset{=}{}_{komm} p * (q' * q'')$
$= (p * q') * q'' \overset{=}{}_{Vor} (p' * q) * q'' \overset{=}{}_{komm} (q * p') * q''$
$\overset{=}{}_{assoz} q * (p' * q'') \overset{=}{}_{Vor} q * (p'' * q') \overset{=}{}_{assoz} (q * p'') * q'$
$(p * q'') * q' = (q * p'') * q' \Rightarrow p * q'' = q * p''$
$(p,q) \sim (p'',q'')$

Also $\sim$ Äquivalenz-Relation.

2.1.3 Äquivalenz-Klassen

Sei $(p,q) \in P \times Q$

$p \wr q = R\{(p,q)\} = \{(x,y) \in P \times Q | (x,y) \sim (p,q)\}$
$= \{(x,y) \in P \times Q | p * y = q * x\}$

$(x,y) \in p \wr q \Leftrightarrow p * y = q * x$

$$\boxed{\underbrace{x \wr y = p \wr q}_{Gleichheit\ in\ 2^P} \Leftrightarrow \underbrace{p * y = q * x}_{Gleichheit\ in\ P}}$$

2.1.4 Menge aller Äquivalenz-Klassen

$P \wr Q := \{p \wr q : (p,q) \in P \times Q\} = (P \times Q)/\sim$

Satz

$P \wr Q$ ist kommutative Halbgruppe mit Verknüpfung $(p_1 \wr q_1) * (p_2 \wr q_2) = p_1 * p_2 \wr q_1 * q_2$

Falls P neutrales Element o besitzt und $o \in Q \Rightarrow P \wr Q$ hat neutrales Element $o \wr o$

Beweis

(i) Die Verknüpfung ist wohldefiniert,
d.h. unabhängig von der Auswahl der Repräsentanten.
Sei $p_1 \wr q_1 = x_1 \wr y_1$ und $p_2 \wr q_2 = x_2 \wr y_2$. z.z.: $p_1 * p_2 \wr q_1 * q_2 = x_1 * x_2 \wr y_1 * y_2$

Nach Voraussetzung: $p_1 * y_1 = q_1 * x_1$ und $p_2 * y_2 = q_2 * x_2$

$(p_1 * p_2) * (y_1 * y_2) = p_1 * (p_2 * y_2) * y_2 = p_1 * (y_1 * p_2) * y_2$
$= (p_1 * y_1) * (p_2 * y_2) \underset{Vor.}{=} (q_1 * x_1) * (q_2 * x_2) = q_1 * (x_1 * q_2) * x_2$
$= q_1 * (q_2 * x_1) * q_2 = (q_1 * q_2) * (x_1 * x_2)$
$\Rightarrow p_1 * p_2 \wr q_1 * q_2 = x_1 * x_2 \wr y_1 * y_2$
$\Rightarrow P \wr Q$ besitzt Verknüpfung $P \wr Q \times P \wr Q \overset{*}{\rightarrow} P \wr Q$

(ii) $P \wr Q$, $*$ genütgt Assoziativgesetz und Kommutativgesetz
Zeige Kommutativ. z.z.: $(p_1 \wr q_1) * (p_2 \wr q_2) = (p_2 \wr q_2) * (p_1 \wr q_1)$
$(p_1 \wr q_1) * (p_2 \wr q_2) = (p_1 * p_2) \wr (q_1 \wr q2)$
$(p_2 * p_1) \wr (q_2 * q_1) = (p_2 \wr q_2) * (p_1 * q_1)$
Assoziativität analog.

(iii) neutrales Element $o \in Q$
Behauptung: $(p \wr q) * (o \wr o) = (p \wr q)$
Beweis: $(p \wr q) * (o \wr o) = (p * o) \wr (q * o) = p \wr q$

Beispiel 1

$(\mathbb{N}, +, 0)$ additive Halbgruppe (additiv immer kürzbar).
$P = \mathbb{N}, Q = \mathbb{N}$ Unterhalbgruppen.
$(m, n) \sim (p, q) \Leftrightarrow m + q = n + p \Leftrightarrow m - n = p - q$

Schreibweise $p \wr q =: p - q$
$\mathbb{Z} = N \wr N = \{p - q : p, q \in \mathbb{N}\}$
$=$ Menge der ganzen Zahlen

Nach Satz gilt: $\mathbb{Z}$ kommutative Halbgruppe.
$(p - q) + (m - n) = (p \wr q) + (m \wr n) = (p + m) \wr (q + n) = (p + m) - (q + n)$
übliche Addition ganzer Zahlen.

Beispiel 2

$(\mathbb{Z}, \times, 1)$ multiplikative Halbgruppe.
$P = \mathbb{Z}, \quad \mathbb{Z} \times Z \overset{\times}{\rightarrow} \mathbb{Z}; (a, b) \rightarrow ab$
$Q = \mathbb{Z} \backslash \{0\}$

Dann gilt: $Q \subset \mathbb{Z}$ Unterhalbgruppe (multiplikatativ), kürzbar.

$\Rightarrow$ Äquivalenz-Relation auf $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\})$
$(a,b) \sim (c,d) \Leftrightarrow ad = bc \Leftrightarrow \frac{a}{b} = \frac{c}{d}$
$\mathbb{Z} \wr \mathbb{Z}\backslash\{0\} =: \mathbb{Q} =$ Menge der rationalen Zahlen.
$a \wr b := \frac{a}{b} \quad a \wr b \in \mathbb{Q}; a \in \mathbb{Z}; b \in \mathbb{Z}\backslash\{0\}$

$\Rightarrow \mathbb{Q}$ multiplikative Halbgruppe mit Verknüpfung $\frac{a}{b} \times \frac{c}{d} = (a \wr b) \times (c \wr d) = ac \wr bd = \frac{ac}{bd}$
übliche Multiplikation rationaler Zahlen.

2.1.5 Inverses Element

Lemma

Sei $(P, *, o)$ Halbgruppe mit neutralem Element. $g \in P$ hat Inverses $x \in P$, falls $g * x = o = x * g$

Inverse sind eindeutig bestimmt.

Beweis

$g \in P$ mit Inversen x,y. z.z.: $x = y$

$g * x = o = x * g, \quad g * y = o = y * g$
$x = x * o = x * (g * y) = (x * g) * y = o * y = y$

Definition

$(P, *, o)$ Halbgruppe.
$\mathcal{G}(P) = \text{Inv}(P) = \{g \in P : g \text{ besitzt Inverses } g^- \in P\}$
$\Rightarrow g * g^- = o = g^- * g$

Beispiel 1: Addition (immer kommutativ)

$g^- = -g, \quad g + -g = 0 = (-g) + g$

$P = (\mathbb{N}, +, 0)$
$\mathcal{G}(\mathbb{N}, +) = \{0\} \qquad n + x = 0 \Rightarrow n = 0$
Also hat $n \in \mathbb{N}$ Inverses $x \in \mathbb{N}$

$P = (\mathbb{N}, +, 0) \Rightarrow \mathcal{G}(\mathbb{Z}, +) = \mathbb{Z}$
Beweis: $m - n = m \wr n \in \mathbb{Z}.$ inv: $-m \wr n = -(m - n) = n - m = n \wr m$

Beispiel 2: Multiplikation

$g^- \times g^{-1} = 1 = g^{-1} \times g^-$

$(\mathbb{N}, \times, 1)$
$\mathcal{G}(\mathbb{N}, x) = \{1\} \qquad m \times m^{-1} = 1 \Rightarrow m = 1$
(2 ist nicht invertierbar, da $\frac{1}{2} \notin \mathbb{N}$)

$\mathcal{G}(\mathbb{Z}, \times, 1) = \{\pm 1\} \qquad a, b \in \mathbb{Z}$ invertierbar $\Leftrightarrow a \times b = 1$

$\mathcal{G}(\mathbb{Q}, \times, 1) = \mathbb{Q} \backslash \{0\} \qquad p = \frac{a}{b} \in \mathbb{Q}$
$\frac{a}{b} \times \frac{b}{a} = 1$, falls $a \neq 0 \wedge b \neq 0$

Satz

(i) $g \in \mathcal{G}(P) \Rightarrow g^- \in \mathcal{G}(P) \wedge (g^-)^- = g$
(ii) $p, q \in \mathcal{G}(P) \Rightarrow p * q \in \mathcal{G}(P) \wedge (p * q)^- = p^- * q^-$
(iii) $\mathcal{G}(P)$ kürzbar

Beweis

(i) folgt aus Definition
(ii) $(p * q) * (q^- * p^-) = p * (q * q^-) * q^- = p * o * p^- = p * p^- = o$
$(p^- * q^-) * (p * q)$ analog
(iii) $q \in \mathcal{G}(P)$. z.z.: q kürzbar
$p_1 * q = p_2 * q \Rightarrow p_1 = p_1 * o = p_1 * (q * q^-) = (p_1 * q) * q^- = (p_2 * q) * q^-$
$= p_2 * (q * q^-) = p_2 * o = p_2$

2.1.6 Gruppe

Definition
$(G, *, o)$ Gruppe $:\Leftrightarrow$

(i) $(G, *, o)$ Halbgruppe
(ii) $\mathcal{G}(G) = G$ das heisst: $\forall g \in G \; \exists g^- \in G \; q * g^- = o = g^- * g$

Satz

$(P, *, o)$ Halbgruppe $\Rightarrow \mathcal{G}(P) Gruppe$

2.2 Permutations-Gruppen

X Menge
$2^{X \times X} = \{R \subset X \times X\}$ Halbgruppe bezüglich Komposition.
$R_1 \times R_2 \subset X \times X$, $R_1 * R_2 = R_1 \circ R_2 \subset X \times X$, $o = I = I_X \subset X \times X$

Satz

$(2^{X \times X}, \circ, I)$ Halbgruppe

Beweis

$R_1, R_2, R_3 \in 2^{X\times X} \Rightarrow (R_1 \circ R_2) \circ R_3 = R_1 \circ (R_2 \circ R_3)$ assoziativ

Satz

$X^X = \{X \overset{F}{\to} X\} \subset 2^{X\times X}$ Unterhalbgruppe

Beweis

$F_1, F_2 : X \to X \Rightarrow F_1 \circ F_2 : X \to X$
$I : X \to X$ Funktion $\Rightarrow F_1 \circ F_2 \in X^X, I \in X^X$

2.2.1 Satz zur Permutationsgruppe

$\mathcal{G}(2^{X\times X}) = \mathcal{G}(X^X) = \{X \overset{F}{\to}$ bijektiv $\}$ =: Permutationsgruppe

Beweis

$F \in X^X$ invertierbar $\Rightarrow \exists F^- : X \to X, F \circ F^- = I = F^- \circ F$
Permutationsgruppe von X = Menge aller Permutationen von X
Symmetrische Gruppe $\mathfrak{S}$ = Permuationsgruppe von X

Spezialfall

$X = n = \{1, 2, \cdots, n\}$ endliche Menge.
$\mathfrak{S}_n =$ Permutation (Umordnung) von n Objekten

$$\alpha \in \mathfrak{S}_n : \alpha = \frac{\begin{matrix}1&2&3&4&5&6\end{matrix}}{\begin{matrix}2&3&1&5&6&4\end{matrix}}$$

$\alpha(1) = 2, \alpha(2) = 3, \alpha(3) = 1, \cdots$

$$\alpha^{-1} = \frac{\begin{matrix}1&2&3&4&5&6\end{matrix}}{\begin{matrix}3&1&2&6&4&5\end{matrix}}$$

$$\beta = \frac{\begin{matrix}1&2&3&4&5&6\end{matrix}}{\begin{matrix}6&5&4&3&2&1\end{matrix}}$$

$$\alpha \circ \beta = \frac{\begin{matrix}1&2&3&4&5&6\end{matrix}}{\begin{matrix}4&6&5&3&2&1\end{matrix}} \neq \beta \circ \alpha = \frac{\begin{matrix}1&2&3&4&5&6\end{matrix}}{\begin{matrix}5&4&6&2&1&3\end{matrix}}$$

2.2.2 zyklische Permutation, k-Zykel

Definition

$i_1 \neq i_2 \neq \cdots \neq i_k$

$$\gamma = \overline{i_1 \cdots i_k} = \begin{matrix} i_1 & \longleftarrow & i_k \\ \downarrow & & \uparrow \\ i_2 & \longrightarrow & \cdots \end{matrix}$$

$\gamma = \overline{i_1 \cdots i_k} \in \mathfrak{S}_n, \qquad \gamma(j) = j \forall j \notin \{i_1, \cdots, i_k\}$
$\gamma(i_1) = i_2, \quad \gamma(i_2) = i_3, \quad \gamma(i_{k-1} = i_k, \quad \gamma(i_k) = i_1$

Beispiel

$\mathfrak{S}_6 \qquad \overline{1325} = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 3 & 5 & 2 & 4 & 1 & 6 \end{array}$

k-Zykel $\overline{i_1 \cdots i_k}$ und l-Zykel $\overline{j_1 \cdots j_l}$ heissen disjunkt
$:\Leftrightarrow \{i_1, \cdots i_k\} \cap \{j_1, \cdots, j_l\} = \emptyset$

Proposition

Disjunkte Zyklen kommutieren, d.h. $\{i_1, \cdots i_k\} \cap \{j_1, \cdots, j_l\} = \emptyset$
$\Rightarrow \{i_1, \cdots i_k\} \circ \{j_1, \cdots, j_l\} = \{j_1, \cdots, j_l\} \circ \{i_1, \cdots i_k\}$

Beweis durch Beispiel

$\mathfrak{S} : \overline{134} \circ \overline{25} = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 3 & 5 & 4 & 1 & 2 & 6 \end{array} = \overline{25} \circ \overline{134}$

Proposition

Nicht-disjunkte Zyklen kommutieren im Allgemeinen nicht

$\mathfrak{S}_5 : \overline{135} \circ \overline{25} = \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \hline 3 & 1 & 5 & 4 & 2 \end{array}$

$\mathfrak{S}_5 : \overline{25} \circ \overline{135} = \begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ \hline 3 & 5 & 2 & 4 & 2 \end{array}$

Satz

Jede Permutation von $\alpha \in \mathfrak{S}$ ist eindeutig als Produkt disjunkter Zyklen schreibbar.
$\alpha = \gamma_1, \cdots, \gamma_n$ disjunkte Zyklen, beliebig vertauschbar.

Beweis durch Algorithmus (ist konstruktiv)

1. Schritt Wähle erstes Objekt "1" und berechne "Bahn" von "1" unter α.
$i_1 = 1, i_2 = \alpha(1), i_3 = \alpha(i_2) = \alpha(\alpha(i_1))$ bis $i_1 = 1$ wieder erreicht wird.
$\Rightarrow \overline{i_1 \cdots i_k}$ k-Zykel

2. Schritt Wähle kleinstes Objekt $j \notin \{i_1, \cdots, i_k\}$ und berechne dessen Bahn von j_1
$j_1, j_2 = \alpha(j_1), j_3 = \alpha(j_2)$ bis j_1 wieder erreicht wird.
$\Rightarrow \overline{j_1, \cdots, j_l} \cap \overline{i_1, \cdots, i_k} = \emptyset$

Nach endlich vielen Schritten ($\leq n$) alle Elemente erfasst.

Beispiel

$\mathfrak{S}_{10} \ni \alpha = \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline 3 & 2 & 5 & 6 & 8 & 10 & 9 & 1 & 4 & 7 \end{array}$

$i_1 = 1$ $\quad$ $j_1 = 2$ $\quad$ $k_1 = 4$

$\overline{1358}$ $\quad$ $\cdot\ \not\overline{2}$ $\quad$ $\cdot\overline{46\,10\,79}$

$\Rightarrow \alpha = \overline{1358} \circ \overline{46\,10\,79}$

2.2.3 Gruppentafel, Matrix

Sei G endliche Gruppe, $G = \{g_1, \cdots, g_n\}$

$*$	g_1	g_2	$\cdots$	g_j	$\cdots$	g_n	
g_1	g_1	g_2	$\cdots$	$\vdots$	$\cdots$	g_n	
g_2	g_2	$g_2 * g_2$	$\cdots$	$\vdots$	$\cdots$	$g_2 * g_n$	
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	
g_i	$\cdots$	$\cdots$	$\cdots$	$g_i * g_j$	$\cdots$	$\cdots$	$i - te\ Zeile$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	
g_m	g_m	$\cdots$	$\cdots$	$g_i * g_j$	$\cdots$	$g_m * g_n$	
				$j - te\ Spalte$			

$\mathfrak{S}_2 = \{I, \tau\}$

$I = \dfrac{1\ \ 2}{1\ \ 2} = \overline{1} = \overline{2}$ $\qquad$ $\tau = \overline{12} = \dfrac{1\ \ 2}{2\ \ 1}$ $\qquad$ $\tau \circ \tau = I$

$\circ$	I	τ
I	I	τ
τ	τ	I

$\mathfrak{S}_n$ hat $n!$ Elemente

$\mathfrak{S}_3$ hat $3! = 6$ Elemente

$I = \dfrac{1\ \ 2\ \ 3}{1\ \ 2\ \ 3}$ $\qquad$ $\overline{12} = \dfrac{1\ \ 2\ \ 3}{2\ \ 1\ \ 3}$ $\qquad$ $\overline{13} = \dfrac{1\ \ 2\ \ 3}{3\ \ 2\ \ 1}$

$\overline{23} = \dfrac{1\ \ 2\ \ 3}{1\ \ 3\ \ 2}$ $\qquad$ $\overline{123} = \dfrac{1\ \ 2\ \ 3}{2\ \ 3\ \ 1}$ $\qquad$ $\overline{321} = \dfrac{1\ \ 2\ \ 3}{3\ \ 1\ \ 2}$

Schreiben: $I, \tau_1 = \overline{23}, \tau_2 = \overline{13}, \tau_3 = \overline{12}, \sigma = \overline{123}, \sigma^{-1} = \overline{321}$

Definition

In $\mathfrak{S}_n$ wähle $i \neq j \Rightarrow \overline{ij}$Transposition

$\tau = \overline{ij} \in \mathfrak{S}$ =

$\cdots$	i	$\cdots$	j	$\cdots$
$\cdots$	j	$\cdots$	i	$\cdots$

Charakterisiert: $\tau \neq I, \tau^2 = I$

Beispiel

$\mathfrak{S}_6 : \overline{13} = \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 3 & 2 & 1 & 4 & 5 & 6 \end{array}$

Definition

Zykel $\overline{i_0 \cdots i_n}$ hat Ordnung h
$\gamma = \overline{i_0 \cdots i_n} \Rightarrow N(\gamma) = h$
$\alpha \in \mathfrak{S} \Rightarrow \alpha = \gamma_1 \cdots \gamma_m$ Zerlegung in $m \geq 1$ disjunkte Zykel

totale Ordnung: $N(\alpha) = \sum_{i=1}^{m} N(\gamma_i) \in \mathbb{N}$

Beispiel

$N\tau = 1$

Propositon

γ Zykel der Ordnung $l \Rightarrow \gamma$ Produkt von l Transpositionen.

Beweis

$\gamma = \overline{i_0 \cdots i_l} = \overline{i_o i_1} \circ \overline{i_0 i_2} \circ \cdots \circ \overline{i_0 i_l}$ l Faktoren

Korollar

Sei $\alpha \in \mathfrak{S}_n$ beliebig
$\Rightarrow \alpha =$ Produkt von $N(\alpha)$ Transpositionen, Produkt nicht eindeutig

Beispiel

$\gamma = \overline{123} = \overline{13} \cdot \overline{12}$

Satz

Sei $\alpha \in \mathfrak{S}_n$, τ Transposition $\Rightarrow N(\tau \cdot \alpha) = N(\alpha) \pm 1$

Beweis

$\overline{i\, i_1 \cdots i_h} \cdot \overline{j\, j_1 \cdots j_k}$ (disjunkt) $= \overline{ij} \cdot \overline{i\, i_1 \cdots i_h\, j\, j_1 \cdots j_k}$ nicht disjunkt

$\Leftrightarrow \begin{array}{cccccccc} i & i_1 & i_{h-1} & i_h & j & j_1 & j_{k-1} & j_k \\ \hline i_1 & i_2 & i_h & i & j_1 & j_2 & j_k & j \end{array} = \begin{array}{cccccccc} i & i_1 & i_{h-1} & i_h & j & j_1 & j_{k-1} & j_k \\ \hline i_1 & i_2 & i_h & i & j_1 & j_2 & j_k & j \end{array}$

Also gilt auch (wegen $\overline{ij}^{\,2} = I$): $\overline{ij} \cdot \overline{i\, i_1 \cdots i_h} \cdot \overline{j\, j_1 \cdots j_k} = \overline{i\, i_1 \cdots i_h\, j\, j_1 \cdots j_k}$

IF i, j in verschiedenen α-Zyklen
$\Rightarrow \alpha = \overline{i\, i_1 \cdots i_h} \cdot \overline{j\, j_1 \cdots j_k} \cdot \gamma_3 \cdots \gamma_m$
$N(\alpha) = h + k + N(\gamma_3) + \cdots + N(\gamma_m)$
$\tau\alpha = \overline{ij} \cdot \overline{i\, i_1 \cdots i_h} \cdot \overline{j\, j_1 \cdots j_k} \cdot \gamma_3 \cdots \gamma_m = \cdot \overline{i\, i_1 \cdots i_h\, j\, j_1 \cdots j_k} \cdot \gamma_3 \cdots \gamma_m$

$N(\tau\alpha) = h + k + 1 + N(\gamma_3) + \cdots + N(\gamma_m)$

IF i, j im gleichen α-Zykel
$\overline{ij} \cdot \overline{i\, i_1 \cdots i_h\, j\, j_1 \cdots j_l} \cdot \gamma_2 \cdots \gamma_m$
$N(\alpha) = h + k + 1(\gamma_2) + \cdots + N(\gamma_m)$
$\tau\alpha = \overline{ij} \cdot \overline{i\, i_1 \cdots i_h\, j\, j_1 \cdots j_k} \cdot \gamma_2 \cdots \gamma_m = \overline{i\, i_1 \cdots i_h} \cdot \overline{j\, j_1 \cdots j_k} \cdot \gamma_2 \cdots \gamma_m$
$N(\tau\alpha) = h + k + 1 + N(\gamma_2) + \cdots + N(\gamma_m) = N(\alpha - 1)$

2.2.4 Signum

$\alpha = \tau_m \cdots \tau_1$ Produkt von Transpositionen (nicht notw. disjunkt)
$\Rightarrow -1^{N(\alpha)} = -1^m =: sgn(\alpha)$ Signum = Vorzeichen
(d.h. m und $N(\alpha)$ haben gleiche Parität)

Beweis per Induktion über $m \geq 0$

IA:$m = 1 \quad \alpha = \tau_1 = \overline{ij} \Rightarrow N(\alpha) = 1m$
$(\Rightarrow (-1)^{N(\alpha)} = -1 = (-1)^m \Rightarrow N(\alpha)$ und m haben gleiche Pariätät)
IV: $(-1)^{N(\alpha)} = (-1)^m$
IS: $1 \leq m \to m + 1$
$\alpha := \tau_{m+1}\, \tau_m \cdots \tau_1$
$\beta := \tau_m \cdots \tau_1, \quad \tau = \tau_{m+1} \Rightarrow \alpha = \tau \cdot \beta$
$\Rightarrow (-1)^{N(\beta)} = (-1)^m$
$\Rightarrow N(\alpha) = N(\tau\beta) = N(\beta) \pm 1$
$\Rightarrow (-1)^{N(\alpha)} = (-1)^{(N(\beta)\pm 1)} = -(-1)^{N(\beta)} = -(-1)^m = (-1)^{m+1}$
$\Rightarrow$ Formel gilt für α, d.h. für $m + 1$

Satz

sgn: $\mathfrak{S}_n \to \{\pm 1\}$
$\alpha \mapsto$ sgn$(\alpha) = (-1)^{N(\alpha)} = (-1)^m$

Dann gilt: sgn$(\alpha \cdot \beta) =$ sgn$(\alpha) \cdot$ sgn(β)

Beweis

$\alpha = \tau_m \cdots \tau_1$ m Transpositionen
$\beta = \sigma_n \cdots \sigma_1$ n Transpositionen

$\Rightarrow \alpha\beta = \tau_m \cdots \tau_1 \cdot \sigma_n \cdots \sigma_1$ m+n Transpositionen
$\Rightarrow$ sgn$(\alpha\beta) = (-1)^{m+n} = (-1)^m \cdot (-1)^n =sgn(\alpha) \cdot$sgn$(\beta)$

Beispiel

sgn$(\overline{ij}) = -1$

Definition

$\alpha \in \mathfrak{S}$ heisst gerade / ungerade $\Leftrightarrow$sgn$(\alpha) = 1 \backslash -1$

2.3 Ringe und Körper

Definition des Ringes

Sei R Menge mit zwei Verknüpfungen:
$R \times R \overset{+}{\to} R; (x, y) \mapsto x + y$ und
$R \times R \overset{\cdot}{\to} R; (x, y) \mapsto xy$

$(R, +, \cdot)$ Ring :$\Leftrightarrow$

(i) $(R, +, 0)$ abelsche Gruppe
(ii) $(R, \cdot)$ Halbgruppe
(iii) Distributivgesetze:
$(a + b) \cdot c = ac + bc$
$a \cdot (b + c) = ab + ac$

Definition

R unital :$\Leftrightarrow$ $(R, \cdot, o)$ hat neutrales Element

Definition

R kommutativ :$\Leftrightarrow$ $(R, \cdot)$ kommutativ

Definition

$\mathcal{G}(R) = \{a \in R : \exists$ Inverses $a^{-1} \in R$ mit $a \cdot a^{-1} = e = a^{-1} \cdot a\}$
multiplikative Gruppe (Einheitsgruppe von R)

Beispiel

$(\mathbb{Z}, +, \cdot, 0, 1)$ Ring, kommutativ, unital
$\Rightarrow \mathbb{Z}$ kein Körper (, da nicht alle außer 0 invertierbar)

Beispiel

$\mathbb{Q} = \mathbb{Z} \wr \mathbb{Z} \backslash \{0\} \ni \frac{p}{q} \neq 0, p, q \in \mathbb{Z} \Rightarrow \mathcal{G}(\mathbb{Q}) = \mathbb{Q} \backslash \{0\} \ni \frac{p}{q}$
$(\frac{p}{q})^{-1} = \frac{q}{p}$, da $p \neq 0 \neq q$
$\Rightarrow \mathbb{Z}$ Körper der rationalen Zahlen

Beispiel

$\mathbb{R} =$ reellen Zahlen
$\Rightarrow \mathbb{R}$ Körper, $\mathbb{R} \supset \mathbb{Q}$ Unterkörper

$(\mathbb{R}, +, 0, \cdot\ =)$ Ring

Proposition

$a \cdot 0 = 0 \forall a \in \mathbb{R}$

Beweis

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

Proposition

$a \cdot (-b) = -(ab) = (-a) \cdot b$

Beweis

z.z.: $a \cdot (-b) + ab = 0$
$a \cdot (-b) + ab = ab + a \cdot (-b) = a(b + (-b)) = a \cdot 0 = 0$

2.3.1 Satz von Jacobson

$(R, +, \cdot, 0, o)$ unitaler Ring, $a, b \in \mathbb{R}$
Es gelte $ab - o \in \mathcal{G}(R), d.h. (ab - o)^{-1} \in \mathbb{R}$.
$\Rightarrow ba - o \in \mathcal{G}(R)$ und $(ba - e)^{-1} = b(ab - o)^{-1}a - o$

Beweis

z.z.: $o = (ba - o)(b(ab - o)^{-1}a - o$
$(ba - o)(b(ab - o)^{-1}a - o = (ba)b(ab - o)^{-1}a - ba - b(ab - o)^{-1}a + o$
$= bab(ab - o)^{-1}a - b(ab - o)^{-1}a - ba + o = (bab - b)(ab - o)^{-1}a - ba + o$
$= b(ab - o)(ab - o)^{-1}a - ba + o = boa - ba + o = o$

z.z.: $o = [b(ab - o)^{-1}a - o](ba - o)$
$[b(ab - o)^{-1}a - o](ba - o) = b(ab - o)^{-1}a(ab - o) - o(ba - e)$
$= b(ab - o)^{-1}(aba - a) - ba + e = b(ab - o)^{-1}(ab - o)a - ba + e$
$= boa - ba + o = o$

2.3.2 Matrizen-Ringe

R Ring ($R = K$ Körper), $m, n \in \mathbb{N}\ m \geq 1 leqn$
$m = \{0, 1, \cdots, m - 1\}, n = \{0, 1, \cdots, n - 1\}$

$m \times n = \{(i, j) : i \in m \wedge j \in n\}$ Produktmenge

$R^{m \times n} = \{$ Abbildungen $A : m \times n \to R\}, m \times n \overset{A}{\to} R$

$(i, j) \mapsto A(i, j)$ Funktionswert von A in Paar (i, j)
bei Matrizen: $A_{(i,j)} = A_{ij} = A_i^j$

$$A = \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \vdots & \ddots & \vdots \\ A_{1m} & \dots & A_{nm} \end{pmatrix} \quad (m \times n)\text{-Matrize}$$

Beispiel

$R = \mathbb{Z}, \mathbb{Z}^{2\times 3} \ni A$

$$A = \begin{pmatrix} 4 & 3 & 2 \\ 0 & 1 & 7 \end{pmatrix} \quad (2 \times 3)\text{-Matrize}$$

$A_{13} = 2, \quad A_{22} = 1$

Beispiel

$$R = K = \mathbb{Q} \ni A = \begin{pmatrix} 3 \\ \frac{1}{12} \\ \frac{13}{14} \end{pmatrix}$$

Beispiel

$$K = \mathbb{R}\ \mathbb{R}^{3\times 3} \ni A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Proposition

$(R^{m\times n}, +)$ abelsche Gruppe, Koeffizientenweise

$$\begin{aligned} (A_{ij} + (B_{ij}) &:= (A_{ij} + B_{ij}) \\ -(A_{ij}) &:= (-A_{ij}) \\ 0 &:= (0) \text{ Nullmatrix} \end{aligned}$$

Beispiel

$$\begin{pmatrix} 0 & 1 & 3 \\ 4 & 1 & 7 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 8 & 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 3 \\ 12 & 2 & 6 \end{pmatrix}$$

$$- \begin{pmatrix} 3 & 2 \\ 1 & 0 \\ 4 & -9 \end{pmatrix} = \begin{pmatrix} -3 & -2 \\ -1 & 0 \\ -4 & 9 \end{pmatrix}$$

$$0_{4\times 5} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

2.3.3 Matrizen-Produkt

$$\begin{aligned} R^{m\times n} \times R^{n\times p} &\to R^{m\times p} \\ (A_{ij},\ B_{jk}) &\mapsto AB_{ik} \\ (AB)_{ik} &= \sum_{j=1}^{n} A_{ij} B_{jk} \end{aligned}$$

Beispiel

$$\begin{pmatrix} 2 & 4 \\ 0 & 3 \end{pmatrix} \times \begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix} = \begin{pmatrix} 2\cdot 3+4\cdot(-2) & 2\cdot 1+4\cdot 0 \\ 0\cdot 3+3\cdot(-2) & 0\cdot 1+3\cdot 0 \end{pmatrix} = \begin{pmatrix} -2 & 2 \\ -6 & 0 \end{pmatrix}$$

Satz: Identitäten für Matrizen-Produkte

(i) $(A+B)C = AC+BC$
$m\times n, m\times n \mapsto n\times p = m\times p, m\times p$
$A(B+C) = AB+AC$

(ii) Assoziativität
$(AB)C = A(BC)$

(iii) E_m Einheitsmatrix $= \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$
$E_m(A_{m\times m}) = (A_{m\times m}) = (A_{m\times m})E_m$

Beweis von (ii)

$((AB)C)_{il} = \sum_{k=1}^{p}(AB_{ik})C_{kl} = \sum_{k=1}^{p}[\sum_{j=1}^{n} A_{ij}B_{jk}]C_{kl}$
$= \sum_{j=1}^{n}\sum_{k=1}^{p} A_{ij}BjkC_{kl} = \sum_{k=1}^{p}\sum_{j=1}^{n} A_{ij}BjkC_{kl}$
$= \sum_{j=1}^{n}[\sum_{k=1}^{p} A_{ij}B_{jk}]C_{kl} = \sum_{j=1}^{n} A_{ij}(BC)_{jl} = (A(BC))_{il}$
$\Rightarrow (AB)C = A(BC)$

Spezialfall: $m = n$ quadratische Matrizen

$\Rightarrow (R^{n\times n}, +, \cdot)$ unitaler Ring mit Einselement $E = E_n$ $n\cdot E$, $n(n-1)$ Null

R kommutativ $\not\Rightarrow$ $R^{n\times n}$ kommutativ $(AB \neq BA)$

Definition
$GL_n(R) := \mathcal{G}(R^{n\times n}) = \{A \in R^{n\times n} : A^{-1} \in R^{n\times n} : AA^{-1} = E = A^{-1}A\}$
GL = general linear group

$\Rightarrow GL_n(R)$ Gruppe und $A, B \in GL_n(R) \Rightarrow AB \in GL_n(R) \wedge (AB)^{-1} = B^{-1}A^{-1}$

Satz

R kommutativ
Dann ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R^{2\times 2}$ invertierbar
$\Leftrightarrow ad-bc \in R$ invertierbar und $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$

Beweis durch Verifikation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ab-cd & ab-ba \\ cd-cd & cb-da \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix}$$
$$\Rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2$$

Analog $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{1}{ad-bc} = E_2$

Korollar

K Körper, $\mathcal{G}(K) = K \backslash \{0\}$
$GL_2(K) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K^{2\times 2} : ad - bc \neq 0\} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K^{2\times 2} : ad \neq bc\}$

Beispiel

$$\begin{pmatrix} 2 & 1 \\ -3 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 1 \\ 3 & 2 \end{pmatrix} \cdot \frac{1}{11} = \begin{pmatrix} \frac{4}{11} & \frac{-1}{11} \\ \frac{3}{11} & \frac{2}{11} \end{pmatrix}$$

Beispiel

$\begin{pmatrix} 2 & 1 \\ 6 & 3 \end{pmatrix}$ nicht invertierbar, da $2 \cdot 3 - 1 \cdot 6 = 0$

2.4 Gauss-Algorithmus

$A \in K^{m\times n}$

(i) Vertausche Zeile i mit Zeile j $(i \neq j)$

$$P^{i,j} = \begin{pmatrix} 0_{ii} & 1_{ji} & \dots & 0 \\ 1_{ij} & 0_{jj} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$ Transpositionsmatrix

$\Rightarrow A \mapsto P^{i,j}A$ vertauscht Zeile i und Zeile j

Beispiel $m = 2$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} & A_{1n} \\ A_{21} & A_{22} & A_{2n} \end{pmatrix} = \begin{pmatrix} A_{21} & A_{22} & A_{2n} \\ A_{11} & A_{12} & A_{1n} \end{pmatrix}$$

(ii) Multipliziere i-te Zeile mit $\alpha \in K \setminus \{0\}$

$$M^{i,\alpha} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \alpha_i & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$ Diagonalmatrix

$\Rightarrow \tilde{A} = M^{i,\alpha} \cdot A$

Beispiel $m = 2$

$$\begin{pmatrix} 1 & 0 \\ 0 & \alpha \end{pmatrix} \begin{pmatrix} A_{11} & A_{12} & A_{1n} \\ A_{21} & A_{22} & A_{2n} \end{pmatrix} = \begin{pmatrix} A_{11} & A_{12} & A_{1n} \\ \alpha \cdot A_{21} & \alpha \cdot A_{22} & \alpha \cdot A_{2n} \end{pmatrix}$$

(iii) Addiere α-fache von Zeile i zu Zeile $j \neq i$

$$T^{i,j,\alpha} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ \alpha_i & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

2.4.1 Zeilenreduktion

Definition

A heisst Zeilenreduziert (low-reduced)

$$\Leftrightarrow A = \left(\begin{array}{ccccccc} 0 & X & \vert 1_{1a} & X & 0 & X & 0 \\ 0 & X & 0 & X & \vert 1_{2b} & X & 0 \\ 0 & X & 0 & X & 0 & X & \vert 1_{3c} \end{array} \right) \text{ (X beliebig)}$$

Spalten a, b, c sind Pivot-Spalten.

Pivot-Spalten: $1 \leq j_1 < \dots < j_r \leq n$
k-te Pivot-Spalte $j_k = A_k^{jk} = 1 \qquad i \neq k \quad A_i^{jk} = 0$
Beispiel

$$A = \begin{pmatrix} 0 & \boxed{1} & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & \boxed{1} & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & \boxed{1} \end{pmatrix}$$

($\boxed{1}$ Pivot-Elemente)
pivotal: A^2, A^4, A^6 nicht-pivotal: A^1, A^3, A^5

Satz

Jede Matrix $A \in K^{m \times n}$ kann durch elementare Zeilenumformungen zeilenreduziert werden

Beweis durch Algorithmus

Typ (i) Vertausche zwei Zeilen $A_{j1} \leftrightarrow A_{i2}$
Typ (ii) Multipliziere i-te Zeile mit $\alpha \in K \setminus \{0\}$. $A_i \rightarrow \alpha A_i$
Typ (iii) Addiere ein vielfaches von einer Zeile zu einer anderen Zeile $A_i \rightarrow A_j + \alpha A_i; i \neq j$

Von links oben nach rechts unten
Schritt 1 Wähle erste Spalte $A^{j1} \neq 0$
(i) Finde i mit $A_i^{j1} \neq 0 \Rightarrow$ Typ 1 $A_1^{j1} \neq 0$
(ii) Typ 2 $\Rightarrow A_1^{j1} = 1$
(iii) Typ 3 $\Rightarrow A_i^{j1} = 0$ für $i > 1$

Nach Schritt 1 gilt: $A = \begin{pmatrix} 0 & 1 & X & X & X & X \\ 0 & 0 & X & X & X & X \\ 0 & 0 & X & X & X & X \end{pmatrix}$

Schritt 2 Wähle nächste Spalte A^{j2} mit $j_1 < j_2$ und $A_i^{j2} \neq 0$ für ein $i \geq 2$
(i) Finde $i \geq 2$ mit $A_i^{j2} \neq 0 \Rightarrow$ Typ 1 $A_2^{j2} \neq 0$
(ii) Typ 2 $\Rightarrow A_2^{j2} = 1$
(iii) Typ 3 $\Rightarrow A_i^{j2} = 0 \forall i \neq 2$

Nach Schritt 2 bleibt A^{j1} unverändert.
Nach Schritt 2 gilt: $A = \begin{pmatrix} 0 & 1 & Y & Y & 0 & X \\ 0 & 0 & Y & Y & 1 & X \\ 0 & 0 & Y & Y & 0 & X \end{pmatrix}$ (Y bekannt, aber nicht pivotal)

Schritt 3 Wähle nächste Spalte A^{j3} mit $j_2 < j_3$ und $A_i^{j3} \neq 0$ für ein $i \geq 3$
usw.

Beispiel

$$A = \begin{pmatrix} 2 & 3 & 4 & 2 & 1 \\ 1 & 0 & 3 & 4 & 2 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \in K^{3\times 5}, K = \mathbb{Q}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 3 & 4 & 2 \\ 2 & 3 & 4 & 2 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 2 & 4 & 1 \\ 0 & 3 & 2 & 2 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 3 & 2 & 2 & 1 \\ 0 & 0 & 2 & 4 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & 2 & 4 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & \frac{2}{3} & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & 1 & 2 & \frac{1}{2} \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & -2 & -\frac{1}{3} \\ 0 & 1 & 0 & -\frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & 1 & 2 & \frac{1}{2} \end{pmatrix}$$

Definition

Pivot-Spalten heisst Rang von A, d.h. Rang A = # Zeilen $\neq 0$ nach Reduktion

Beispiel

$A = \begin{pmatrix} 1 & 0 & 1 & 2 & -1 \\ 1 & 3 & 0 & 4 & 0 \\ 1 & 3 & 1 & 6 & -1 \end{pmatrix}$ hat Rang 2

2.4.2 Invertierung von quadratischen Matrizen

$$m = n \; A = \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \vdots & \ddots & \vdots \\ A_{1n} & \dots & A_{nn} \end{pmatrix}$$

$GL_n(K) = \{A \in K^{n\times n} : \exists A^{-1} \in K^{n\times n} : AA^{-1} = E = A^{-1}A$

Satz

Sei $A \in K^{n\times n}$

(i) A invertierbar $\Leftrightarrow$ Rang(A) =n (n Pivotspalten)
(ii) A^{-1} durch Zeilenreduktion: $(A, E) \Rightarrow (E, A^{-1})$

Beispiel

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 8 & 9 & 4 \\ 7 & 6 & 5 \end{pmatrix}$$

$$(A,E) = \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 8 & 9 & 4 & 0 & 1 & 0 \\ 7 & 6 & 5 & 0 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -7 & -20 & -8 & 1 & 0 \\ 0 & -8 & -16 & -7 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & -4 & -1 & 1 & -1 \\ 0 & -8 & -16 & -7 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 11 & 3 & -2 & 2 \\ 0 & 1 & -4 & -1 & 1 & -1 \\ 0 & 0 & -48 & -15 & 8 & -7 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & 11 & 3 & -2 & 2 \\ 0 & 1 & -4 & -1 & 1 & -1 \\ 0 & 0 & 1 & \frac{15}{48} & -\frac{8}{48} & \frac{7}{48} \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & 0 & -\frac{7}{16} & -\frac{1}{6} & \frac{19}{48} \\ 0 & 1 & 0 & \frac{5}{16} & \frac{1}{8} & -\frac{5}{12} \\ 0 & 0 & 1 & \frac{5}{16} & -\frac{1}{6} & \frac{7}{48} \end{pmatrix}$$

$\Rightarrow$ A hat Inverses $A^{-1} = \begin{pmatrix} 1 & 0 & 0 & -\frac{7}{16} & -\frac{1}{6} & \frac{19}{48} \\ 0 & 1 & 0 & \frac{5}{16} & \frac{1}{8} & -\frac{5}{12} \\ 0 & 0 & 1 & \frac{5}{16} & -\frac{1}{6} & \frac{7}{48} \end{pmatrix} \in \mathbb{Q}^{3\times 3}$

Satz

$m = n, A \in K^{n\times n}$
Dann $A \in Gl_n(K) \Leftrightarrow (A, E) \in K^{n\times 2n}$ hat die ersten n Spalten pivotal
$\Leftrightarrow$ Rang$(A, E) = n$ und Pivotal-Spalten sind die ersten n Spalten

In diesem Falle $(A, E) \Rightarrow (E, A^{-1})$

Beispiel

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in \mathbb{Z}^{3\times 3} \subset ratio^{3\times 3}$$

$$(A,E) = \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 4 & 5 & 6 & 0 & 1 & 0 \\ 7 & 8 & 9 & 0 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -3 & -6 & -4 & 1 & 0 \\ 0 & -6 & -12 & -7 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & -6 & -12 & -7 & 0 & 1 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{4}{3} & -\frac{1}{3} & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \end{pmatrix}$$

$\Rightarrow$ Pivot-Spalten $1, 2, 4$ (und nicht $1, 2, 3$) $\Rightarrow A$ nicht invertierbar.

2.5 Lineaere Gleichungssysteme

$m = \#$ Gleichunge, Zeile i = Gleichung i
$n = \#$ Unbekannte, Spalte j = Unbekannte j

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in K^{n\times 1} \text{ unbek., } x_j \in K, \quad A = \begin{pmatrix} A_1^1 & \dots & A_1^n \\ \vdots & \ddots & \vdots \\ A_m^1 & \dots & A_m^n \end{pmatrix} \in K^{m\times n} \text{ bek.}$$

2.5.1 Homogenes lineares Gleichungssystem

Definition

$$A_x = 0\,; \quad \begin{pmatrix} A_1^1 & \dots & A_1^n \\ \vdots & \ddots & \vdots \\ A_m^1 & \dots & A_m^n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

explizit m Gleichungen:
$A_1^1 x_1 \cdots A_1^n x_n = 0$
$A_2^1 x_1 \cdots A_2^n x_n = 0$
$\vdots$
$A_m^1 x_1 \cdots A_m^n x_n = 0$

Satz: Allgemeine Lösung des homogenen linearen Gleichungsystems $Ax = 0$

(i) Es gibt immer triviale Lösung:
$x_1 = 0, x_2 = 0, \cdots, x_n = 0$
(ii) nicht-triviale Lösung / allgeimeine Lösung
$Ax = 0 \Rightarrow$ Zeilenreduktion $A \sim \tilde{A}, \tilde{A}x = 0$

Sei $x_P =$ Spalte der Pivot-Variablen, $x_N =$ Spalte der Nicht-Pivot-Variablen.
$\Rightarrow x_N$ frei wählbar
$\Rightarrow x_P = -\tilde{A}_P^N x_N$, wobei $\tilde{A}_P^N =$ Teilmatrix von $\tilde{A}$ mit Spalten N und Zeilen P.

Beispiel

$A \in K^{3\times 7}$ drei Gleichungen, sieben Unbekannte

$$\tilde{A} = \begin{pmatrix} 1 & \tilde{A}_1^2 & 0 & \tilde{A}_1^4 & \tilde{A}_1^5 & 0 & \tilde{A}_1^7 \\ 0 & 0 & 1 & \tilde{A}_2^4 & \tilde{A}_2^5 & 0 & \tilde{A}_2^7 \\ 0 & 0 & 0 & 0 & 0 & 1 & \tilde{A}_3^7 \end{pmatrix}$$

Pivotal: $1, 3, 6$
N-Pivotal: $2, 4, 5, 7$

$$x_P = \begin{pmatrix} x_1 \\ x_3 \\ x_6 \end{pmatrix} \qquad x_N = \begin{pmatrix} x_2 \\ x_4 \\ x_5 \\ x_7 \end{pmatrix}$$

$$\Rightarrow x_2, x_4, x_5, x_7 \text{ frei wählbar. } \begin{pmatrix} x_1 \\ x_3 \\ x_6 \end{pmatrix} = \begin{pmatrix} \tilde{A}_1^2 & \tilde{A}_1^4 & \tilde{A}_1^5 & \tilde{A}_1^7 \\ 0 & \tilde{A}_2^4 & \tilde{A}_2^5 & \tilde{A}_2^7 \\ 0 & 0 & 0 & \tilde{A}_3^7 \end{pmatrix} \cdot \begin{pmatrix} x_2 \\ x_4 \\ x_5 \\ x_7 \end{pmatrix}$$

Korollar

frei-wählbare Parameter (Variablen)
= # nicht-Pivot-Spalten
= n − # Pivotspalten = n− Rang A
= # Ubekannten - Rang A

Speziell: Rang$(A) = n \Rightarrow$ nur triviale Lösung

2.5.2 Inhomogenes lineares Gleichungssytem

$A \in K^{m \times n}, x \in K^{n \times 1}, b \in K^{m \times 1}$

$$Ax = b \qquad \begin{pmatrix} A_1^1 & \dots & A_1^n \\ \vdots & \ddots & \vdots \\ A_m^1 & \dots & A_m^n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

explizit m Gleichungen:
$A_1^1 x_1 \cdots A_1^n x_n = b_1$
$A_2^1 x_1 \cdots A_2^n x_n = b_2$
$\vdots$
$A_m^1 x_1 \cdots A_m^n x_n = b_n$

Satz

Sei $Ax = b$ gegeben. $\Rightarrow$ erweiterte Matrix $(A, b) \in K^{m \times (n+1)}$

$(A, b) \Rightarrow (\tilde{A}, \tilde{b})$ zeilenreduziert

(i) $Ax = b$ hat Lösung $\Leftrightarrow$ b nicht pivotal
(ii) Falls b nicht pivotal
$\Rightarrow x_N =$ nicht-pivotal Variablen frei wählbar.
$x_P =$ pivotal
$x_P = -\tilde{b} - \tilde{A}_p x_N$

Beispiel

$2x_1 + x_2 + 3x_3 = 5$
$2x_1 + x_2 + 4x_3 = 6$

$4x_1 + 2x_2 + 5x_3 = 9$

Schritt 1 Matrixform

$$\begin{pmatrix} 2 & 1 & 3 \\ 2 & 1 & 4 \\ 4 & 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 5 \\ 6 \\ 9 \end{pmatrix}$$

Schritt 2 erweiterte Matrix

$$(A,b) = \left(\begin{array}{ccc|c} 2 & 1 & 3 & 5 \\ 2 & 1 & 4 & 6 \\ 4 & 2 & 5 & 9 \end{array}\right) \Rightarrow \left(\begin{array}{ccc|c} 2 & 1 & 3 & 5 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & -1 \end{array}\right)$$

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

Zusatzspalte nicht pivotal $\Rightarrow \exists$ Lösung

Allgemeine Lösung: $P = 1; 3$, $N = 2 \Rightarrow x_2$ frei wählbar

$$\begin{pmatrix} x_1 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ 0 \end{pmatrix} \cdot x_2$$

Schritt 3 $x_1 = 1 - \frac{1}{2}x_2$

$x_3 = 1$

$x_2 =$ frei wählbar

homogenes Problem

Lineares Gleichungssystem (lineares Problem)

Abbildung: $K^{m\times 1} \overset{A}{\leftarrow} K^{n\times 1}$, bzw. $Ax \leftarrow x$

allgemein:

$F : X \to Y$

$F^{-1}\{y\} = \{x \in X : F(x) = y\}$Urbildmenge

speziell:

$X = K^{n\times 1}, Y = K^{m\times 1}, F(x) = Ax$

$A^{-1}\{0\} = \{x \in K^{n\times 1} : Ax = 0\}, y = 0 \in K^{m\times 1}$

inhomogenes Problem

$Ax = B \in K^{m\times 1}$

inhomoge Lösung $x \in K^{n\times 1}$ mit $Ax = b$

Lösungsmenge $x \in A^{-1}\{b\}$

2.5.3 Allgemeine Lösung von inhomogenen Problemen

Satz

$Ax = b$ inhomogenes Problem $\Rightarrow (A,b) \in K^{m\times(n+1)}$ erweiterte Matrix

$\Rightarrow (A, b) \Rightarrow (\tilde{A}, \tilde{b})$

Dann gilt:

(i) $\exists$ inhomogene Lösung, d.h. $A^{-1}\{b\} = \emptyset$
$\Leftrightarrow$ Zusatzspalte nicht pivotal
(ii) Falls Zusatzspalte nicht pivotal $\Rightarrow$ allgemeine Lösung
nicht pivotal x_N frei wählbar. pivotal $x_P = \tilde{b} - \tilde{A}_P^N$

Korollar

(i) Zahl der freien Parameter in allgemeiner Lösung $= n-$ Rang(A)
(ii) Partikuläre Lösung $x_N = 0 \quad x_P = \tilde{b}$
(iii) Inhomogene Lösung = Homogene Lösung + Partikuläre Lösung

Beispiel

$x + 3y - z = 1$
$-y + 2z = \lambda$
$2x + 2y + 6z = 0$

Frage: Für welches λ existiert Lösung ?

$$\left(\begin{array}{ccc|c} 1 & 3 & -2 & 1 \\ & -1 & 2 & \lambda \\ 2 & 2 & 6 & 0 \end{array}\right) \Rightarrow \left(\begin{array}{ccc|c} 1 & 3 & -2 & 1 \\ & -1 & 2 & \lambda \\ 2 & 2 & 6 & 0 \end{array}\right) \Rightarrow \left(\begin{array}{ccc|c} 1 & 0 & 5 & 1+3\lambda \\ 0 & 1 & -2 & -\lambda \\ 0 & 0 & 0 & -2-4\lambda \end{array}\right)$$

d.h. Zusatzspalte pivotal $\Leftrightarrow -2 - 4\lambda \neq 0$
Zusatzspalte nicht pivotal $\Leftrightarrow -2 - 4\lambda = 0 \Leftrightarrow \lambda = -\frac{1}{2}$

$A^{-1}\{b\} \neq \emptyset \wedge \exists$ Lösung $\Leftrightarrow \lambda = -\frac{1}{2}$

2.6 Untergruppen und Quotienten

Sei $(G, *, o)$ Gruppe, nicht notw. kommutativ
$\forall g \in G \exists g^- \in G, g * g^- = o = g^- * g$

Definition

$H \subset G$ Untergruppe $\Leftrightarrow$

(i) $\forall h_1, h_2 \in H \Rightarrow h_1 * h_2 \in H \quad [H * H \subset H]$
(ii) $\forall h \in H$ gilt $h^- \in H$
(iii) $o \in H$

Beispiel

additive Gruppe $(\mathbb{Z}, +, 0)$
$G = \mathbb{Z}$, Sei $k \geq 2$ fest gewählt

$H = \mathbb{Z}k = k\mathbb{Z} =$ vielfache von k $= \{km : m \in \mathbb{Z}\} \ni 0, \pm k \pm 2k, \cdots$

Satz

$k\mathbb{Z} \subset \mathbb{Z}$ Untergruppe

Beweis

(i) Sei $km_1 \in k\mathbb{Z}, km_2 \in k\mathbb{Z}$
$km_1 + km_2 = k(m_1 + m_2) \in k\mathbb{Z}$
(ii) $-(km) = k(-m) \in k\mathbb{Z}$
(iii) $0 = k0 \in k\mathbb{Z}$

Satz

G Gruppe, H Untergruppe $\Rightarrow$ Äquivalenz-Relation auf G
$g_1 \sim g_2 \Leftrightarrow \boxed{g_1^- * g_2 \in H}$
$R = \{(g_1, g_2) \in G \times G | g_1^- * g_2 \in H\}$

Beweis

(i) reflexiv $g \sim g$, denn $g^- * g = o \in H$
(ii) symm. $g_1 \sim g_2 \Rightarrow g_1^- * g_2 \in H$
$\Rightarrow g_2^- * g_1 = (g_1^- * g_2)^- \in H$, da $H = H^- \Rightarrow g_2 \sim g_1$
(iii) trans. $g_1 \sim g_2 \sim g_3 \Rightarrow g_1^- * hg_2 \in H \ni g_2^- * g_3$

Beispiel

$(\mathbb{Z}, +) \sqsupset k\mathbb{Z}, k \geq 2$

Kongruenz mod $k\mathbb{Z}$ $\quad m \sim n \Leftrightarrow n - m = -m + n$ also $m - m$ durch k teilbar
$m \equiv n \mod k$

Satz

$(G, +)$ additive Gruppe, immer abelsch, $\quad H \sqsubset G$ Untergruppe

(i) $x, y \in H \Rightarrow x + y \in H$
(ii) $x \in H \Rightarrow -x \in H$
(iii) $0 \in H$

Kongruenz: $x \sim y$ kongruent $\mod H \Leftrightarrow -x + y = y - x \in H \Leftrightarrow x - y \in H$

Definition

G Äquivalenz-Klasse = Kongruenz-Klasse

$R \subset G \times G \qquad R\{g\} = \{g_1 \in G | g_1 \sim g\} = \{g_1 \in G | g_1^- * g \in H\} \in G$

Satz

Kongruenz-Klasse $R\{g\} = g * H = \{g * h : h \in H\}$ Restklasse

speziell $R\{0\} = o * H = H$

Beweis

"$\subset$" Sei $y \in R\{g\} \Rightarrow y \sim g \Rightarrow g \sim y$
$\Rightarrow h := g^- * y \in H \Rightarrow g * h = g * (g^- * y) = o * y$
$\Rightarrow y = g * h \in g * H$
Also $R\{g\} \subset g * H$

"$\supset$" Sei $y \in g * H \Rightarrow \exists h \in H, y = g * h$
$\Rightarrow g^- * y = g^- * (g * h) = o * h = h \in H$
$\Rightarrow y \sim g \Rightarrow y \in R\{g\}$
Also $g * H \subset R\{g\}$

2.6.1 Quotienten-Menge

$G/H = \{g * h | g \in G\}$ Menge der Kongruenz-Klassen

Satz

$\mathbb{Z}/k\mathbb{Z} = \{m + k\mathbb{Z} | m \in \mathbb{Z}\} = k = \{0, 1, \cdots, k-1\}$
$\mathbb{Z}/k\mathbb{Z} \ni 0 + k\mathbb{Z}, 1 + k\mathbb{Z}, k - 1 + k\mathbb{Z}$

Beispiel

$k = 2$, somit 2 Klassen: $0 + 2\mathbb{Z} : 1 + 2\mathbb{Z}$ (gerade und ungeraden ganzen Zahlen)

2.6.2 Euklidscher Algorithmus (Division mit Rest)

Sei $k \geq 2 : \forall p \in \mathbb{Z} \quad \exists q \in \mathbb{Z}\, \exists r \in k \quad (r \in \mathbb{Z} \quad 0 \leq r \leq k-1)$, so daß $\boxed{p = qk + r}$

Beweis

$M := \{n \in k\mathbb{Z} : n \leq p\}$ nach oben beschränkt durch p
z.z.: $M \neq \emptyset$, denn $-k|p| \in M \quad |p| = \begin{cases} p & p \geq 0 \\ -p & p < 0 \end{cases}$, denn $-k|p| \leq -|p| \leq p$
$\Rightarrow M \neq \emptyset$, nach oben beschränkt durch $p \overset{!}{\Rightarrow} \exists$ größtes Element $m \in M$

$\Rightarrow$ (i) $m = qk$ für $q \in \mathbb{Z}$, wegen $m \in k\mathbb{Z}$
$\Rightarrow$ (ii) $m \leq p$

Setze $r := p - m \geq 0 \Rightarrow p = m + r = qk + r$ Division mit Rest

Zeige $0 \leq r \overset{!}{<} k$, denn $(q+1)k = qk + k = m + k > m$
$\Rightarrow (q+1)k \notin M$, da m größtes Element von M
Da $(q+1)k \in k\mathbb{Z} \Rightarrow (q+1)k > p$
$\Rightarrow p = qk + r < (q+1)k = qk + k$
$\Rightarrow r = p - qk < k$

Satz

Gruppe $\mathbb{Z} \sqsupset k\mathbb{Z}$ Untergruppe
$\Rightarrow$ Kongruenz-Relation $\mod k\mathbb{Z} \qquad p \sim q \Leftrightarrow p - q \in k\mathbb{Z}$
$\Rightarrow$ Quotionentenmenge $\mathbb{Z}/k\mathbb{Z} \overset{F}{\leftarrow} K$ bijektiv
Klasse von $r = r + k\mathbb{Z} \hookleftarrow r$

d.h. alle Kongruenz-Klassen sind genau die folgenden: $k\mathbb{Z}, 1 + k\mathbb{Z}, 2 + k\mathbb{Z}, \cdots, (k-1) + k\mathbb{Z}$

Beweis

z.z.: F injektiv. Sei $F(r) = F(s)$, wobei $0 \leq r, s < k$
z.z.: $r = s$, Ohne Einschränkung $s \leq r$

$\Rightarrow 0 \leq r - s \leq r \leq k$
Nach Voraussetzung: $F(r) = r + k\mathbb{Z} = F(s) = s + k\mathbb{Z}$
$\Rightarrow r$ und s haben gleiche Äquivalenz-Klasse
$\Rightarrow r \sim s \Rightarrow r - s \in k\mathbb{Z}$ durch k teilbar
$0 \leq r - s < k \Rightarrow 0 = r - s \Rightarrow r = s$

z.z.: F surjektiv. Sei $A \in \mathbb{Z}/k\mathbb{Z}$ Äquivalenz-Klasse
z.z.: $\exists r \in K \quad A = F(r) = r + k\mathbb{Z}$
$A \neq \emptyset \Rightarrow \exists p \in A$ Repräsentant
$\Rightarrow$(nach Euklid) $\exists q \in Z \exists r \in k \quad p = qk + r$
$\Rightarrow p - r = qk \in k\mathbb{Z} \Rightarrow p \sim r$
$\Rightarrow A = p + k\mathbb{Z} = r + k\mathbb{Z} = F(r)$

Frage

$\mathbb{Z}/k\mathbb{Z} \overset{F^{-1}}{\rightarrow} k$ bijektiv
$A \mapsto F^{-1}(A)$

$F^{-1}(A) = min\{a : a \in A : a \geq 0\}$

Satz

Gruppe G abelsch, $G \sqsupset H$ Untergruppe
Kongruenz-Relation $g_1 \sim g_2 \Leftrightarrow g_1^- * g_2 \in H \ni g_2 * g_1^-$

$\Rightarrow G/H = \{g * H | g \in G\}$
$g * H := \{g * h : h \in H\}$ Äquivalenz-Klasse

G/H Gruppe abelsch mit Verknüpfung $(g_1 * H) * (g_2 * H) := (g_1 * g_2) * H$

Inverse $(g * H)^- = g^- * H$
Neutral $o * H = H \in G/H$

Beweis

z.z.: Verknüpfung wohldefiniert (d.h. unabhängig von Repräsentanten)
Sei $g_1 * H = y_1 * H \quad g_1 \sim y_1$
und $g_2 * H = y_2 * H \quad g_2 \sim y_2$

z.z.: $g_1 * g_2 \sim y_1 * y_2$
Da $g_1 \sim y_1 \Rightarrow g_1^- * y_1 \in H$ und $g_2 \sim y_2 \Rightarrow g_2^- * y_2 \in H$
$\Rightarrow (g_1 * g_2)^- * y_1 * y_2 = (g_2^- * g_1^-) * y_1 * y_2$
$= g_2^- (g_1^- * y_1) * y_2 = (g_1^- * y_1) * (g_2^- * y_2) \in H$
$\Rightarrow g_1 * g_2 \sim y_1 * y_2$ Verknüpfung wohldefiniert

$* : G/H \times G/H \to G/H$
$g_1 * H; g_2/astH \mapsto (g_1 * g_2) * H$

assoz. $((g_1 * H)(g_2 * H)) * (g_2 * H) = ((g_1 * g_2) * H) * (g_3 * H)$
$= (g_1 * g_2 * g_3) * H = (g_1 * H) * ((g_2 * g_3) * H)$
$(g_1 * H) * ((g_2 * H) * (g_3 * H))$
kommutativ analog
Neutral $(g * H) * H) = (g * H) * (o * H) = (g * o) * H = g * H$
Inverses $(g * H) * (g^- * H) = (g * g^-) * H = o * H = H$
Notation $G/H =$ Quotientengruppe von G und H
Multiplik. $G/H \ni gH = g \times H$
$gH = \{gh : h \in H\} \subset G$
$(g_1 H)(g_2 H) = (g_1 g_2)H$ (nur bei abelsch)
Additiv $G/H \ni g + H$
$g + h = \{g + h : h \in H\} \subset G$
$(g_1 + H) + (g_2 + H) := (g_1 + g_2) + H$
neutrales Element: $0 + H = H$
negative: $-(g + H) = (-g) + H$

Beispiel

$G = \mathbb{Z}$ abelsche additive Gruppe
$H = k\mathbb{Z} \sqsubset G$
$G/H = \mathbb{Z}/k\mathbb{Z} = \{r + k\mathbb{Z} : r \in k\}$

$\Rightarrow \mathbb{Z}/k\mathbb{Z}$ Quotienten-Gruppe
$\Rightarrow \mathbb{Z}/k\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \overset{\oplus}{\to} \mathbb{Z}/k\mathbb{Z}$

$(m + k\mathbb{Z}) \oplus (n + k\mathbb{Z}) := m + n + k\mathbb{Z}$
Konkret: $\mathbb{Z}/k\mathbb{Z} = k = \{0, 1, \cdots, k-1\}$

$r, s \in k \Rightarrow r \oplus s \in k$
$r \oplus s :=$ Additon von $r + s \mod k$, d.h. $r + s = qk + r \oplus s$

Satz

Die Menge $k = \{0, 1, \cdots, k-1\}$ ist abelsche Gruppe $k \times k \overset{\oplus}{\to} k$ definiert durch $r + s - (r \oplus s) \in k\mathbb{Z}$

Beispiel

$k = 2 \qquad k = \{0, 1\}$
$0 \oplus 0 = 0$
$0 \oplus 1 = 1 = 1 \oplus 0$
$1 \oplus 1 = 0$, denn $(1 + 1) - (1 + 1) = 2\dot{0} \in 2\mathbb{Z}$

2.7 Gruppen-Homomorphismen

Seien $(G, *)$ und $(G', *')$ Gruppen
$F : G \to G'$ Abbildung

2.7.1 Definition Homomorphismus

F Homomorphismus $:\Leftrightarrow \forall g_1, g_2 \in G \; F(\underbrace{g_1 * g_2}_{\in G}) = \underbrace{F(g_1)}_{\in G'} *' \underbrace{F(g_2)}_{\in G'}$

2.7.2 Definition Isomorphismus

F Isomorphismus $:\Leftrightarrow F$ Homomorphismus $\wedge$ F bijektiv
Notation: $G \overset{F}{\underset{\approx}{\to}} G'$

Beispiel 1

$G = \mathfrak{S}_n$ Permutation von $\{1, \cdots, n\}$
$\alpha \in \mathfrak{S}_n$
$sgn(\alpha) =$ Vorzeichen (Signum) = $(-1)^m$, falls $\alpha = \tau_1 \cdots \tau_m$ m Transpositionen
$G' = \{+1, -1\} = \{\pm 1\} = \mathcal{G}(\mathbb{Z}) = \mathcal{G}(\mathbb{Z}, \cdot)$
$\Rightarrow \mathfrak{S}_n \overset{sgn}{\to} \mathcal{G}(\mathbb{Z})$ Homomorphismus
$\alpha \mapsto sgn(\alpha)$, denn $sgn(\alpha \cdot \beta) = sgn(\alpha) \cdot sgn(\beta)$

sgn kein Isomorphismus, denn $\mathfrak{S}_n$ hat $n!$ Elemente
$G = \mathfrak{S}_n \quad G' = \{\pm 1\}$ hat zwei Elemente
$\Rightarrow$ sgn surjektiv, nicht injektiv

Beispiel 2

G Gruppe, abelsch $H \sqsubset G$ Untergruppe
$\Rightarrow$ Kongruenz-Relation $g_1 \sim g_2 \Leftrightarrow g_1^- * g_2 \in H$

Quotienten-Gruppe $G/H = \{g * H : g \in G\}$,
wobei $g * H = \{g * h : h \in H\}$ Kongruenz-Klasse

$\Rightarrow$ Kanonische Relation
$G \overset{P}{\underset{\rightarrow}{}} G/H; \qquad g \mapsto g * H$

P Homomorphismus
$P(g_1 * g_2) = (g_1 * g_2) * H = (g_1 * H) * (g_2 * H) = P(g_1) * P(g_2)$
P surjektiv, aber nicht injektiv

Proposition

(i) $G \underset{hom om.}{\overset{F}{\rightarrow}} G' \underset{hom om.}{\overset{F'}{\rightarrow}} G'' \Rightarrow G \underset{hom om.}{\overset{F' \circ F}{\rightarrow}} G''$
(ii) $G \underset{\approx}{\overset{F}{\rightarrow}} G' \Leftrightarrow G' \underset{\approx}{\overset{F^{-1}}{\rightarrow}} G$

Propositon

$G \underset{hom om.}{\overset{F}{\rightarrow}} G'$ (i) $F(o) = o'$
(ii) $F(g^-) = F(g)^-$

Beweis

(i) $F(o)^- *' F(o) = F(o)^- *' F(o * o)$
$= F(o)^- *' F(o *' F(o) = (F(o)^- *' F(o)) *' F(o) =$
$= o *' F(o) = F(o)$
(ii) a) $F(g^-) *' F(g) = F(g^- * g) = F(o) = o'$
b) $F(g) *' F(g^-) = F(g * g^-) = F(o) = o'$

Satz

$G \underset{hom om.}{\overset{F}{\rightarrow}} G$ (i) $\mathrm{Ker}(F) = F^-\{o'\} = \{g \in G : F(g) = o'\}$ UG von G
(ii) $\mathrm{Im}(F) = F(G) = \{F(g) : g \in G\} = \{g' \in G' : \exists g \in G : F(g) = g'\}$ UG von G'

Beweis

(i) a) $o \in Ker(F)$, denn $F(o) = o'$
b) $g^- \in Ker(F) \Rightarrow F(g^-) = F(g)^- = o'^- = o'$
c) $g_1, g_2 \in Ker(F) \Rightarrow F(g_1 * g_2) = F(g_1) *' F(g_2)$
$= o' *' o' = o' \Rightarrow g_1 * g_2 \in Ker(F)$

(ii) a) $o \in Im(F)$, denn $o = F(o)$
b) $g^- \in Im(F) \Rightarrow \exists g \in G\, g' = F(g)$
c) $g'_1, g'_2 \in Im(F) \Rightarrow \exists g_1, g_2 \in G\, g'_1 = F(g_1), g'_2 = F(g_2)$
$\Rightarrow g'_1 *' g'_2 = F(g_1) *' F(g_2) = F(g_1 * g_2) \in Im(F)$

Beispiel 1

$\mathfrak{S}_n \overset{sgn}{\to} \{\pm 1\} = \mathcal{G}(\mathbb{Z})$
$\Rightarrow Im(sgn) = \{\pm 1\} \qquad Ker(sgn) = \{\alpha \in \mathfrak{S}_n : sgn(\alpha) = 1\} = \{\alpha \in \mathfrak{S}_n : \alpha = \tau_1 \cdots \tau_{2m}\}$ gerade Zahl an Transpositionen
$\mathfrak{A}_n = Ker(sgn) \subset \mathfrak{S}$ alternierende Gruppe

Beispiel 2

$P : G \underset{\to}{} G/H$ d.h. $\qquad g \mapsto g * H$
$\Rightarrow Im(P) = G/H$ und $Ker(P) = H$

Beweis von $Ker(P) = H$

Sei $g \in Ker(P) \Rightarrow P(g) = o_{G/H} = H$, d.h. $g * H = o * H \Leftrightarrow g \sim o \Rightarrow g \in H$

2.7.3 Homomorphie-Satz

Sei $G \underset{homom.}{\overset{F}{\to}} G' \Rightarrow$

(i) F wohldefiniert auf $G/Ker(F)$
(ii) induzierte Abbildung $\tilde{F} : G/Ker(F) \to G'$ Homomorphismus
(iii) $G/Ker(F) \overset{F}{\underset{\approx}{\to}} F(g) = Im(F)$

Man sagt $G/Ker(F) \approx Im(F)$

Beweis

(i) $g_1 \sim g_2 \overset{!}{\Rightarrow} F(g_1) = F(g_2)$
Sei $g_1 \sim g_2 \Rightarrow g_1^- * g_2 \in Ker(F)$
$F(g_1) = F(g_1) *' o' = F(g_1) *' F(g_1^- * g_2)$
$= F(g_1) *' (F(g_1^-) *' F(g_2)) = (F(g_1) *' F(g_1^-)) *' F(g_2)$
$= F(g_1 * g_1^-) *' F(g_2) = F(o) *' F(g_2) = F(g_2)$

(ii) $\tilde{F}(g * Ker(F)) := F(g)$
$\tilde{F}((g_1 * Ker(F)) * (g_2 * Ker(F))) = \tilde{F}((g_1 * g_2) * Ker(F))$
$= F(g_1 * g_2) = F(g_1) * F(g_2) = \tilde{F}(g_1 * Ker(F)) *' \tilde{F}(g_2 * Ker(F))$

(iii) $\tilde{F}$ injektiv. Sei $\tilde{F}(g_1 * Ker(F)) = \tilde{F}(g_2 * Ker(F))$
z.z.: $g_1 * Ker(F) = g_2 * Ker(F)$
Nach Vorlesung gilt: $F(g_1) = F(g_2)$
$F(g_1^- * g_2) = F(g_1^-) *' F(g_2) = F(g_1)^- *' F(g_2)$
$\overset{=}{Vor.} F(g_1)^- *' F(g_1) = o')g_1^- * g_2 \in Ker(F)$
$\Rightarrow g_1 \sim g_2 \Rightarrow g_1 * Ker(F) = g_2 * Ker(F) \Rightarrow F$ injektiv

(iv) $\tilde{F}$ surjektiv. Sei $g' \in Im(F) \Rightarrow \exists g \in G : g' = F(g)$
$= \tilde{F}(g * Ker(F)) \Rightarrow g' \in Im(\tilde{F}) \Rightarrow F$ surjektiv

Satz

$\mathbb{Z}/k\mathbb{Z} \sqsubset \mathbb{Z}/l\mathbb{Z}$ Untergruppe, additiv
$x + k\mathbb{Z} \to mx + l\mathbb{Z} = mx + mk\mathbb{Z} = m(x + k\mathbb{Z})$

Beweis
$\mathbb{Z} \underset{hom.}{\overset{m}{\to}} \mathbb{Z} \overset{P}{\to} \mathbb{Z}/l\mathbb{Z} = \mathbb{Z} \underset{hom.}{\overset{F}{\to}} \to \mathbb{Z}/l\mathbb{Z}$

$F(x) = P(mx) = mx + l\mathbb{Z} \qquad mx + my = m(x + y) \Rightarrow$Homomorphismus
$x \in Ker(F) \Leftrightarrow F(x) = 0 = l\mathbb{Z} \overset{!}{=} mx + l\mathbb{Z}$
$\Rightarrow mx \in l\mathbb{Z} \Rightarrow \exists y \in \mathbb{Z} mx = ly = (mk)y = m(ky) \Rightarrow x = ky \Rightarrow x \in k\mathbb{Z}$

Also $Ker(F) = k\mathbb{Z}$
Homomorphie-Satz: $\tilde{F} : \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/l\mathbb{Z}$ injektiver Homomorphismus
$\Rightarrow \mathbb{Z}/k\mathbb{Z} \sqsubset \mathbb{Z}/l\mathbb{Z}$ vermöge $\tilde{F}(x + k\mathbb{Z}) = F(x) = mx + lz$

Beispiel

$k \in \mathbb{Z}, m \in \mathbb{Z}, l = mk$ Man schreibt k/l, k teilt l
$\mathbb{Z}/k\mathbb{Z} = k = \{0, 1, \cdots, k-1\}$ additive Gruppe, $i, j \in k \quad i \oplus j = i + j \mod k$
$6 = \{0, 1, 2, 3, 4, 5\} \ni 4 \qquad 4 \oplus 4 = 8 \mod 6 = 2$

Satz
$\mathbb{Z}/l\mathbb{Z} \sqsupset \mathbb{Z}/k\mathbb{Z} \Rightarrow (\mathbb{Z}/l\mathbb{Z})/(\mathbb{Z}/k\mathbb{Z}) \approx \mathbb{Z}/m\mathbb{Z}$
$x + l\mathbb{Z}) \oplus (\mathbb{Z}/k\mathbb{Z}) \mapsto x + m\mathbb{Z}$

Beweis
z.z.: $\mathbb{Z} \underset{hom.}{\overset{P}{\to}} \mathbb{Z}/m\mathbb{Z}, P(x) = x + m\mathbb{Z}$
Betr. P wohldefiniert auf $\mathbb{Z}/l\mathbb{Z} \qquad x \sim y \mod l\mathbb{Z}$
Bew. Sei $x \sim y \mod l\mathbb{Z} \Rightarrow x - y = lz = mkz \Rightarrow x - y \in m\mathbb{Z} \Rightarrow x \sim y \mod m\mathbb{Z}$
$\Rightarrow P(x) = x + m\mathbb{Z} = y + m\mathbb{Z} = P(y)$
$\Rightarrow$ induzierte Abbildung $\tilde{P} : \mathbb{Z}/l\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$
$\tilde{P}(x + l\mathbb{Z}) = x + m\mathbb{Z} \Rightarrow$ Homomorphismus
Beispiel
$12 = \{0, 1, \cdots, 11\} = \mathbb{Z}/12\mathbb{Z}$

$K = \left\{ \begin{array}{l} 3 \\ 6 \end{array} \right.$

$3 = \{0 \mapsto 0, 1 \mapsto 4, 2 \mapsto 8\} \quad 6 = \{0 \mapsto 0, 1 \mapsto 2, 2 \mapsto 4, 3 \mapsto 6, 4 \mapsto 8, 5 \mapsto 10\}$

Beispiel für Inverses: $H = (\mathbb{Z}/6\mathbb{Z}) \cdot 2 = \{0, 2, 3, 4, 6, 8, 10\}$ Untergruppe von 12
$8 \oplus 9 = 16 \mod 12 \equiv 4$
$10 \oplus 10 = 20 \mod 12 \equiv 8$

$-4 = -4 \mod 12 = 8$

Satz

$(\mathbb{Z}/l\mathbb{Z})/(\mathbb{Z}/k\mathbb{Z}) \approx \mathbb{Z}/m\mathbb{Z}$
genauer $(\mathbb{Z}/l\mathbb{Z})/m(\mathbb{Z}/k\mathbb{Z}) \ni (x + l\mathbb{Z}) \oplus m(\mathbb{Z}/l\mathbb{Z}) \to x + m\mathbb{Z}$
$\overset{\tilde{\tilde{P}}}{\underset{\approx}{\to}} \mathbb{Z}/m\mathbb{Z}$

Beweis

$\mathbb{Z} \underset{\to}{(} P)\mathbb{Z}/m\mathbb{Z} \qquad P(x) = x + m\mathbb{Z}$
$\Rightarrow P$ wohldefiniert auf $\mathbb{Z}/l\mathbb{Z}$, d.h. $x \sim y \mod l\mathbb{Z} \Rightarrow P(x) = P(y)$

$\Rightarrow$ induzierte Abbildung: $\mathbb{Z}/l\mathbb{Z} \overset{\tilde{P}}{\underset{\to}{}} \mathbb{Z}/m\mathbb{Z}$, d.h. $x + l\mathbb{Z} \mapsto x + m\mathbb{Z}$

Berechnen $Ker\tilde{P} \ni x + l\mathbb{Z}$
$\tilde{P}(x + l\mathbb{Z})x + m\mathbb{Z} \underset{=}{!} 0 = m\mathbb{Z}$
$x \in m\mathbb{Z}$, d.h. $x = my, y \in \mathbb{Z}$

$\Rightarrow x + l\mathbb{Z} = my + l\mathbb{Z} = my + mk\mathbb{Z} = mly + k\mathbb{Z}$
$\Rightarrow x + l\mathbb{Z} \in (\mathbb{Z}/k\mathbb{Z}) \sqsubset \mathbb{Z}/l\mathbb{Z}$
$\Rightarrow Ker\tilde{P} = m(\mathbb{Z}/k\mathbb{Z}$

$\Rightarrow$ Homomorphiesatz angewandt auf: $G = \mathbb{Z}/l\mathbb{Z}; G' = \mathbb{Z}/m\mathbb{Z}; F = \tilde{P}$
$G/KerF \overset{\tilde{F}}{\underset{\approx}{\to}} ImF$

$Ker\tilde{P} = m(\mathbb{Z}/k\mathbb{Z})$
$Im\tilde{P} = \mathbb{Z}/m\mathbb{Z}$, da P sujektiv
$(whole/l\mathbb{Z})/m(\mathbb{Z}/k\mathbb{Z}) \overset{\tilde{\tilde{P}}}{\underset{\approx}{\to}} \mathbb{Z}/m\mathbb{Z}$

$\tilde{\tilde{P}}((x + l\mathbb{Z}) \oplus m(\mathbb{Z}/k\mathbb{Z})) = \tilde{P}(x + l\mathbb{Z}) = x + m\mathbb{Z}$

2.8 Ideale und Quotienten-Ringe

Sei $(R, +, \cdot)$ Ring

2.8.1 Definition Ideal

$I \subset R$ heisst Ideal

(i) $I \subset (R, +)$ additive Untergruppe
(ii) $\forall a \in I, \forall b \in R \quad ab \in I \ni ba$
d.h.: $I + I \subset I \supset -I$
$R \times I \subset I \supset I \times R$

Beispiel

$R = (\mathbb{Z}, +, \cdot)$
$I = k\mathbb{Z} \sqsubset \mathbb{Z}$ additive Untergruppe

Notation

$I \triangleleft \mathbb{Z}$ Ideal
$\Rightarrow k\mathbb{Z} \triangleleft \mathbb{Z}$

Beweis

$kx + ky = k(x + y) \subset k\mathbb{Z}$ und $kx \in k\mathbb{Z}, y \in \mathbb{Z}$
$\Rightarrow (kx)y = k(xy) \in k\mathbb{Z} \ni y(kx)$

Proposition

Sei $I \triangleleft R, I \neq R, R \ni o$ unital
$\Rightarrow I \subset R \setminus \mathcal{G}(R)$, d.h. $I \cap \mathcal{G}(R) = \emptyset$

Insbesondere: $o \neq I$

Beweis

Widerspruchsannahme: $\exists a \in \mathcal{G}(R) \cap I$
$\Rightarrow \forall b \in R \quad b = bo = b(a^{-1}a) = \underbrace{ba^{-1}}_{\in R} \underbrace{a}_{\in I} \in I \Rightarrow b \in I \Rightarrow R = I$ Widerspruch

Corollar

$K K\ddot{o}rper, \mathcal{G}(K) = K \setminus \{0\}$
$\Rightarrow K$ hat einzige Ideale $I = \{0\}$ (Nullideal) und $I = K$

Ein Körper hat keine Ideale

Satz

$RingR \triangleright I$ Ideal
$\Rightarrow R/I$ additive Quotientengruppe ist Ring mit Produkt $(a + I) \odot (b + I) : ab + I$
Einselement: $o + I$

Beweis

(i) Produkt wohldefiniert: $a_1 \sim a_2 \mod I, b_1 \sim b_2 \mod I$
$\Rightarrow a_1 \times b_1 \sim a_2 \times b_2 \mod I$
$a_1 - a_2 \in I \ni b_1 - b_2 \Rightarrow a_1 \times b_1 - a_2 \times b_2 = \underbrace{(a_1 - a_2)}_{\in I} \times \underbrace{b_1}_{\in R} + \underbrace{a_2}_{\in R} \times \underbrace{(b_1 - b_2)}_{\in I} \in I$

(ii) Assoziativität und Distributivität werden repräsentantenweise gezeigt

Beispiel

$\mathbb{Z} \triangleright k\mathbb{Z} \Rightarrow \mathbb{Z}/k\mathbb{Z}$ Ring kommutativ, unital
$x + k\mathbb{Z} \odot y + k\mathbb{Z} := xy + k\mathbb{Z}$ (Multiplikation $\mod k$)

$k = 12 \quad (12, \oplus, \odot \qquad 6 \odot 8 = 48 \mod 12 \equiv 0$

Definition

$R \underset{hom om.}{\overset{F}{\to}} R'$ Ring-Homomorphismus $\Leftrightarrow$

(i) $(R,+) \underset{hom om.}{\overset{F}{\to}} (R',+) \qquad F(a+b) = F(a) +' F(b)$
$F(-a) = -F(a)$
$F(0) = 0'$
(ii) $F(a \times b) = F(a) \times' F(b)$
(iii) F unital $\Leftrightarrow (Fo) = o'$
(iv) F Ring-Isomorphismus $\Leftrightarrow F$ bijektiv

Proposition

$R \underset{hom om.}{\overset{F}{\to}} R' \underset{hom om.}{\overset{F'}{\to}} R'' \Rightarrow R \underset{hom om.}{\overset{F' \circ F}{\to}} R''$
$R \overset{F}{\underset{\approx}{\to}} R' \Rightarrow R' \overset{F^{-1}}{\underset{\not\sim}{\to}} R$

Proposition

$R \overset{F}{\underset{\to}{}} R'$ Ring-Homomorphismus

(i) $Ker(F) = F^{-1}\{0\} = \{\forall a \in R : F(a) = 0'\} \triangleleft R$ Ideal in K
(ii) $Im(F) \sqsubset R'$ Unterring, d.h. $a', b' \in Im(F) \Rightarrow a' \times b' \in Im(F)$

Beweis

(i) $a \in Ker(F), b \in R \Rightarrow F(ab) = F(a)F(b) = o'$
$F(b) = o'$
$\Rightarrow ab \in Ker(F) \ni ba \Rightarrow Ker(F)$ Ideal

(ii) $a', b' \in Im(F) \Rightarrow \exists a, b \in R, a' \in F(a), b' \in F(b)$
$\Rightarrow a' \cdot b' = F(a) \cdot F(b) = F(ab) \in Im(F)$

Homomorphie-Satz

$R \underset{homom.}{\overset{F}{\rightarrow}} R' \Rightarrow R/Ker(F) \overset{\tilde{F}}{\underset{\approx}{\rightarrow}} Im(F)$ Ring-Isom. $a + Ker(F) \mapsto F(a)$

Beweis

$\tilde{F}$ Gruppen-Isomorphismus bzgl. +

$\tilde{F}(a + Ker(F) \odot b + Ker(F)) = \tilde{F}(ab + Ker(F)) = F(ab) = F(a)F(b)$
$\tilde{F}(a + Ker(F)) \cdot \tilde{F}(b + Ker(F)) \Rightarrow \tilde{F}$ Ring-Isom.

3 Vektorräume und lineare Abbildungen

3.1 Vektorräume

Sei $(K, +, \cdot)$ Körper, d.h. K kommutativer, unitaler Ring.
Jedes $\alpha \in K, \alpha \neq 0$, hat Inverses $\frac{1}{\alpha}$. $\mathcal{G}(K) = K \setminus \{0\}$

Definition

$(V, +, \cdot)$ K-Vektorraum $:\Leftrightarrow$

(i) $(V, +)$ abelsche Gruppe
d.h. $\forall v, w \in V \; v + w \in V$
$-v \in V$
$0_V \in V$

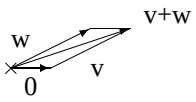
(ii) $K \times V \overset{\cdot}{\rightarrow} V$ Skalar-Multiplikation
$(\alpha, v) \mapsto \alpha v$
mit folgenden vier Eigenschaften:

a)	assoziativ:	$\alpha(\beta v) = (\alpha\beta)v$
b)	unital:	$1v = v$
c)	links-distr.:	$(\alpha + \beta)v = \alpha v + \beta v$
d)	rechts-distr.:	$\alpha(v + w) = \alpha v + \alpha w$

3.1.1 Vektoren anschaulich

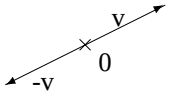
Vektor = Länge + Richtung

Summe



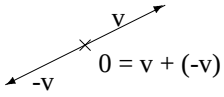
Negativ

$-v$ gleiche Länge wie v, aber umgekehrte Richtung



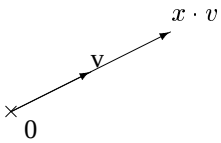
Null-Vektor

Länge $= 0$, Richtung beliebig



Skalar-Multiplikation

gleiche Richtung, x-fache LÄnge



Proposition

(i) $\forall \alpha \in K \ \alpha \cdot 0_V = 0_V$
(ii) $\forall v \in V \ \ 0_K \cdot v = 0_V$

Beweis

(i) $\alpha 0_V = \alpha 0_V + 0_V = \alpha 0_V + (\alpha 0_V - \alpha 0_V) = (\alpha 0_V + \alpha 0_V) - \alpha 0_V$
$= \alpha(0_V + 0_V) - \alpha 0_V = \alpha 0_V - \alpha 0_V = 0_V$
(ii) $0_K \cdot v = 0_K \cdot v + 0_V = 0_K + (0_K \cdot v - 0_K \cdot v)$

$$(0_K \cdot v + 0_K \cdot v) - 0_K \cdot v = (0_K + 0_K)v - 0_K \cdot v = 0_K$$

Korollar

$\alpha \in K, v \in V$
$-(\alpha v) = (-\alpha)v = \alpha(-v)$
Speziell: $\alpha = 1 \qquad -v = (-1)v$

Beispiel: Zeilen-Vektorraum

$V = K^n = K^{1\times n}$
Zeilen über $K = 1 \times n$-Matrizen über K
$v = (v_1, v_2, \cdots, v_n); v_i \in K$

Addition, komponentenweise

$$(v_1, v_2, \cdots, v_n) + (w_1, w_2, \cdots, w_n) := (v_1 + w_1, v_2 + w_2, \cdots, v_n + w_n)$$

Skalar-Multiplikation, komponentenweise

$$\alpha(v_1, v_2, \cdots, v_n) := (\alpha v_1, \alpha v_2, \cdots, \alpha v_n)$$

Beispiel

$n = 4$
$(2, -1, 0, 3) + (0, 3, 7, 2) = (2, 2, 7, 5)$
$5(2, -1, 0, 3) = (10, -5, 0, 15)$

Analog: Spalten-Vektorraum

$$K^{n\times 1} \ni \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \qquad v_i \in K$$

Definition

$V\, K-$Vektorraum, $U \subset V$
U Unterraum (linearer Teilraum) von $V :\Leftrightarrow$

(i) $(U, +)$ additive Untergruppe, d.h.:
$\forall u_1, u_2 \in U : u_1 + u_2 \in U$
$\forall u \in U : -u \in U$
$0_V \in U$
(i) $\forall \alpha \in K, \forall u \in U : \alpha u \in U$
kurz: $U + U \subset U$
$-U = U$
$kU \subset U$

Beispiel

$V = \mathbb{R}^2$ Ebene
$\Rightarrow V$ hat Unterräume U
$U = \{0\}$ Nullvektorraum, 0-dimensional
$U =$ Gerade durch Nullpunkt, 1-dimensional
$U =$ Ebene durch Nullpunkt, 2-dimensional

3.1.2 Quotienten-Raum

$VK-$Vektorraum, $U \subset V$ Unterraum
$\Rightarrow$ Quotientengruppe $V/U = \{v + U : v \in V\}$
$(v_1 + U) \oplus (v_2 + U) = (v_1 + v_2) + U$

$\Rightarrow V/U$ K-Vektorraum mit Skalarmultiplikation $\alpha(v + U) := \alpha v + U$

Beweis

z.z.: wohldefiniert
Sei $v_1 + U = v_2 + U \Rightarrow v_1 - v_2 \in U$
$\Rightarrow \alpha v_1 - \alpha v_2 = \alpha(v_1 - v_2) \in \alpha U \subset U$
$\Rightarrow \alpha v_1 + U = \alpha v_2 + U$

3.2 Lineare Abbildung

Definition

$V, WK-$Vektorräume, $F : V \to W$ Abbildung
F linear $:\Leftrightarrow$

(i) $F(v_1 + v_2) = F(v_1) + F(v_2)$ Gruppenhomomorphismus
(ii) $F(\alpha v) = \alpha F(v)$
(i) + (ii) $F(\alpha v_1 + \alpha v_2) = \alpha_1 F(v_1) + \alpha_2 F(v_2)$

Beispiel

Spalten-Vektorraum $V = K^{n\times 1} \ni \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \quad v_i \in K; \quad W = K^{m\times 1}$

$V = K^{n\times 1} \underset{linear}{\overset{A}{\to}} W = K^{m\times 1} \quad A \in K^{m\times n}$ feste Matrix $A = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix}$
$v \mapsto Av =: A(v)$
dh. jede Matrix definiert lineare ABbildung von Spaltenvektorräumen durch Links-Multiplikation

$$Av = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} =$$

$$\begin{pmatrix} A_1^1 v_1 & +\cdots+ & A_1^n v_n = \sum_i A_1^i v_i = w_i \\ \vdots & & \\ A_m^1 v_1 & +\cdots+ & A_m^n v_n = \sum_i A_m^i v_i = w_i \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_m \end{pmatrix}$$

Beispiel

Raum $\mathbb{R}^{3\times 1} \leftarrow \mathbb{R}^{2\times 1}$ *Ebene*
$\begin{pmatrix} u \\ v \\ w \end{pmatrix} \leftarrow \begin{pmatrix} x \\ y \end{pmatrix}$
$A = 3 \times 2$-Matrix $\begin{pmatrix} 3 & 0 \\ 1 & 1 \\ 4 & -3 \end{pmatrix} \in R^{3\times 2}$

$\mathbb{R}^{3\times 1} \underset{linear}{\overset{\mathbb{R}}{\leftarrow}} {}^{2\times 1}$
$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 1 & 1 \\ 4 & -3 \end{pmatrix} = \begin{pmatrix} 3x \\ x+y \\ 4x-3y \end{pmatrix}$$
$u = 3x$
$v = x + y$
$w = 4x - 3y$

Proposition

$U \underset{lin}{\overset{F}{\rightarrow}} V \underset{lin}{\overset{G}{\rightarrow}} W \Rightarrow V \underset{lin}{\overset{G\circ F}{\rightarrow}} W$

Beweis

$(G \circ F)(\alpha u) = G(F(\alpha u)) = G(\alpha F(u)) = \alpha G(F(u)) = \alpha (G \circ F)(u)$

Definition

$F : V \to W$ linearer Isomorphismus $V \underset{\approx}{\overset{F}{\rightarrow}} W :\Leftrightarrow$

(i) F linear
(ii) F bijektiv

Satz

Sei $F : V \to W$ lineare Abbildung
$\Rightarrow Ker(F) = F^{-1}\{0\} = \{v \in V : F(v) = 0_W\}$Unterraum von V
$\Rightarrow Im(F) = F(v) = \{w \in W : \exists v \in V : w = F(v)\} = \{F(v) : v \in V\}$ URaum von W

Beweis

z.z.: $v_1, v_2 \in Ker(F) \ni v, \alpha \in K$
$\Rightarrow v_1 + v_2 \in Ker(F) \ni \alpha v$

$F(v_1 + v_2) = F(v_1) + F(v_2) = 0_W + 0_W = 0_W$
$F(\alpha v) = \alpha F(v) = \alpha 0_W = 0_W$

$Im(F) = F(V) = \{F(v) : v \in V\} = \{w \in W : \exists v \in V : F(v) = w\}$

Behauptung: $Im(F) \subset W$ Unterraum
z.z.: $w_1 + w_2 \in Im(F) \ni w, \alpha \in K$
$\Rightarrow w_1 + w_2 \in Im(F) \ni \alpha w$

$w_1 = F(v_1), w_2 = F(v_2), w = F(v)$
$\Rightarrow w_1 + w_2 = F(v_1) + F(v_2) = F(v_1 + v_2) \in Im(F)$

$\alpha w = \alpha F(v) = F(\alpha v) \in Im(F)$

Homomorphie-Satz

$V \underset{lin}{\overset{F}{\rightarrow}} W \Rightarrow \tilde{F} : V/KerrightarrowIm(F)$, elementweise: $v + Ker(F) \mapsto F(v)$

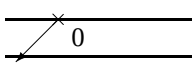
Beweis

Da $(V, +)$ abelsche Gruppe $\Rightarrow \tilde{F}$ Isomorphismus abelscher Gruppe
$\tilde{F}((v_1 + KerF) \oplus (v_2 + KerF))\tilde{F}((v_1 + v_2) + KerF) = F(v_1 + v_2) = F(v_1) + F(v_2) =$
$= \tilde{F}(v_1 + KerF) + \tilde{F}(v_2 + KerF)$

z.z.: $\tilde{F}$ linear : $\tilde{F}(\alpha(v + KerF) = \tilde{F}(\alpha v + KerF) =$
$F(\alpha v) = \alpha F(v) = \alpha \tilde{F}(v + KerF)$

Beispiel

Quotientenraum $V = \mathbb{R}^2$, $\quad U = X-$Achse $= \{\begin{pmatrix} x \\ 0 \end{pmatrix} : x \in \mathbb{R}\}$



$V/U \ni v + U$ Kongruenz-Klasse $= \{v + U : u \in U\}$ enthält v, parallel zu U

Beweis

$U = X-$Achse (horizontale Gerade durch 0)
$\Rightarrow$ Kongruenz-Klasse $v + U$ horizontalen Geraden
$\Rightarrow V/U \approx \{y-$Achse $\} =$ vertikale Gerade durch 0

genauer: $V/U \underset{\approx}{\rightarrow} \{y-\text{Achse}\}$, elementweise: $v+V \mapsto y$-Abstand von $v+U$

Satz

$A \in K^{m\times n}$ Matrix
$A = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix}$

lineare Abbildung $K^{m\times 1} \underset{linear}{\overset{\tilde{A}}{\leftarrow}} K^{n\times 1}$

$$\tilde{A}(v) = Av \leftarrow v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}$$

$\Rightarrow Ker\tilde{A} \subset K^{n\times 1}$ Unterraum

$Ker\tilde{A}$ besteht aus den homog. Lösungen $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ des homog. Problems $Ax = 0$

also $Ker\tilde{A} =$ homogener Lösungsraum

Beweis

$x \in Ker\tilde{A} \Leftrightarrow \tilde{A}(x) = 0 \Leftrightarrow Ax = 0 \Leftrightarrow x$ homogene Lsg

Frage: $Im\tilde{A}$?

Definition

$Im\tilde{A}$ = Spaltenraum von A

$A = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix}$

Spaltenvektoren von A:

$$\left.\begin{array}{l} A^1 = \begin{pmatrix} A_1^1 \\ A_2^1 \\ \vdots \\ A_m^1 \end{pmatrix} \\ \vdots \\ A^n = \begin{pmatrix} A_1^n \\ A_2^n \\ \vdots \\ A_m^n \end{pmatrix} \end{array}\right\} \in Im\tilde{A}$$

3.3 Lineare Unabhängigkeit | Basis

V K-Vektorraum, z.B: $V = \mathbb{R}^2$
m Vektoren $v_1, v_2, \cdots v_m \in V$

Spalte von Vektoren $\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} = V_.$

3.3.1 Proposition: Linearkombination

$K^m \xrightarrow[lin]{V_.} V$ elementweise: $(\alpha_1, \alpha_2, \cdots, \alpha_m) \mapsto \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m$
$= (\alpha_1, \alpha_2, \cdots, \alpha_m) \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix} \in V$

3.3.2 Defintion: lineare Unabhängigkeit

$v_1, \cdots, v_m \in V$ linear unabhängig
$\Leftrightarrow V_. : K^m \to V$ injektiv
$\Leftrightarrow KerV_. = V_.^{-1}\{0\} = \{0\}$ Nullzeile
$\Leftrightarrow \boxed{\forall \alpha_1, \cdots \alpha_m \quad \alpha_1 v_1 + ...\alpha_m v_m = 0_V \Rightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_m = 0}$

$v_1, \cdots, v_m \in V$ linear abhängig
$\Leftrightarrow V_.$ nicht injektiv
$\Leftrightarrow KerV_. \neq \{0\}$
$\Leftrightarrow \exists \alpha_1, \cdots, \alpha_m \neq 0 \Rightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_m = 0_V$

Beispiel 1

$m = 1 \quad V = v_1$
v linear unabhängig $\Leftrightarrow v \neq 0$

Beweis: Sei $v \neq 0$. Sei $\alpha \in K$ mit $\alpha v = 0_V$
Behauptung: $\alpha = 0$
Annahme: $\alpha \neq 0 \Rightarrow \frac{1}{\alpha} \in K \Rightarrow 0_V = \frac{1}{\alpha} 0_V$
$= \frac{1}{\alpha}(\alpha v) = (\frac{1}{\alpha}\alpha)v = 1v = v \Rightarrow v = 0_V$ Widerspruch!
Also: $\alpha = 0 \Rightarrow v$ linear unabhängig

Beispiel 2

$m = 2 \quad v, w \in V$

Proposition: v, w linear abhängig $\Leftrightarrow$ ein Vektor ist Vielfaches des anderens
d.h.: $v = \alpha w$ oder $w = \beta v$ (v, w sind colinear (in einer Geraden))

Beispiel 3
$m = 3 \quad u, v, w \in V$

u, v, w linear abhängig $\Leftrightarrow$ u, v, w co-planar (in Ebene durch den Nullpunkt)

3.3.3 Linearer Aufspann (lineares Erzeugnis)

$ImV_\cdot = \{\alpha_1 v_1 + \cdots + \alpha_m v_m | \alpha_1, \cdots \alpha_m$ beliebig $\}$
$=$ Menge aller Linearkombination und Unterraum von V

Notation

$ImV_\cdot =< v_1, \cdots, v_m >$ Aufspann von $v_1, \ldots, v_m$ (erzeugter Unterraum)

Definition

$< v_1, v_2, \cdots, v_m >:= \{\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m | \alpha_1, \alpha_2, \cdots, \alpha_m \in K\}$

$< v_1, v_2, \cdots, v_m > \supset \{v_1, v_2, \cdots, v_m\}$

Beispiel

$m = 1 \qquad < v >= Kv = \{\alpha v | \alpha \in K\} =$ Gerade auf der Vektor v liegt

Beispiel
$m = 3 \quad \mathbb{R}^3$

(e_1, e_2, e_3) Dreibein
Bemerkung: $e_1, \cdots, e_m$ linear unabhängig: $m-$Bein

Definition Einheitsvektoren

$V = K^m$

$e_1 = (1, 0, 0, \cdots, 0)$
$e_2 = (0, 1, 0, \cdots, 0)$
$e_3 = (0, 0, 1, \cdots, 0)$
$e_m = (0, 0, 0, \cdots, 1)$

$$e_\cdot = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_m \end{pmatrix} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$ Einheitsmatrix

Beweis 1

$$e_\cdot = \begin{pmatrix} e_1 \\ \vdots \\ e_m \end{pmatrix} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$ bijektiv

Beweis 2

Seien $\alpha_1, \alpha_2, \cdots, \alpha_m \in K$, so dass
$0 = \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_m e_m$
$= \alpha_1(1,0,\cdots,0) + \alpha_2(0,1,\cdots,0) + \cdots + \alpha_m(0,0,\cdots,1)$
$= (\alpha_1, 0, \cdots, 0) + (0, \alpha_2, \cdots, 0) + \cdots + (0,0,\cdots \alpha_m)$
$= (\alpha_1, \alpha_2, \cdots, \alpha_m) \stackrel{!}{=} (0,0,\cdots 0)$
$\Rightarrow \alpha_1 = 0, \alpha_2 = 0, \cdots, \alpha_m = 0 \Rightarrow$ linear abhängig

Definition

$< e_1 >=$ von e_1 erzeugte Gerade = x-Achse
$< e_2 >=$ von e_2 erzeugte Gerade = y-Achse
$< e_3 >=$ von e_3 erzeugte Gerade = z-Achse

$< e_1, e_3 >=$ von e_1, e_3 erzeugte Ebene = xz-Ebene
$< e_1, e_2, e_3 >=$ ganzer Vektorraum $V = xyz$-Raum

Beweis

Behauptung: $< e_1, e_3 >= xz$-Ebene
Beweis: $< e_1, e_3 > \exists$ Linearkombination von e_1, e_3
$\alpha_1 e_1 + \alpha_3 e_3 = x e_1 + z e_3, xz \in \mathbb{R}$
$= x(1,0,0) + z(0,0,1) = (x,0,0) + (0,0,z) = (x,0,z)$

Proposition

$v_1, \cdots, v_m$ linear abhängig $\Leftrightarrow \exists v_i$ als Linearkombination von $v_1, \cdots v_{i-1}; v_{i+1}, \cdots, v_m$

Beweis

"$\Rightarrow$"
Seien $v_1, v_2, \cdots, v_m$ linear abhängig
$\Rightarrow \exists(\alpha_1, \alpha_2, \cdots, \alpha_m) \in K^m$ mit $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m = 0_V$
und nicht alle $\alpha_i = 0$,d.h.: $(\alpha_1, \alpha_2, \cdots, \alpha_m) \neq (0,0,\cdots,0)$

OBDA: $\alpha_2 \neq 0$
Behauptung v_2 ist Linearkombiunation von $v_1, v_3, \cdots, v_m$
$0_V = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_m v_m$
$\Rightarrow 0_V - \alpha_1 v_1 - \alpha_3 v_3 - \cdots - \alpha_m v_m = \alpha_2 v_2$
Da $\alpha_2 \neq 0 \Rightarrow -\frac{\alpha_1}{\alpha_2} v_1 - \frac{\alpha_3}{\alpha_2} v_3 - \cdots - \frac{\alpha_m}{\alpha_2} v_m = v_2$
d.h. $v_2 = \beta_1 v_1 + \beta_3 v_3 + \cdots + \beta_m v_m$ wobei $\beta_i = -\frac{\alpha_i}{\alpha_2} \in K$

Mengen-Notation

$A = \{v_1, v_2, \cdots, v_m\}$
A Menge von Vektoren, endlich

Proposition

$A \subset V$; A linear abhängig $\Leftrightarrow \exists a \in A$ so dass $a \in < A \setminus \{a\} >$

3.3.4 Definition: Erzeugenden-System

$v_1, \cdots v_m$ Erzeugenden-System $\Leftrightarrow < v_1, \cdots, v_m >= V$
$\Leftrightarrow v_.$ surjektiv $\Leftrightarrow \forall v \in V \quad \exists \alpha_1, \cdots, \alpha_m \in K \quad v = \alpha_1 v_1 + \cdots \alpha_m v_m$

Jeder Vektor in V ist Linearkombination von $v_1, \cdots, v_m$

Beispiel

$\{v, w\} \subset < v, w >= \mathbb{R}^2$

Definition

$v_1, \cdots, v_m$ Basis $\Leftrightarrow$

(i) $v_1, \cdots, v_m$ linear unabhängig
(ii) $v_1, \cdots, v_m$ Erzeugenden-System

$\Leftrightarrow Ker V_. = \{0\} \wedge Im V_. = V$
$\Leftrightarrow v_.$ bijektiv $K \overset{V_.}{\underset{\approx}{\rightarrow}} V$
$\Leftrightarrow \forall v \in V \quad \exists_1 \alpha_1, \cdots, \alpha_m \in K \quad v = \alpha_1 v_1 + \cdots + \alpha_m v_m$

Beispiel

$V = K^n$ hat Basis $e_1, \cdots, e_n$ Einheitsvektoren mit eindeutiger Linearkombination
$K^n \ni (\alpha_1, \alpha_2, \cdots, \alpha_n) = v = \alpha_1 e_1 + \alpha_2 e_2 + \cdots \alpha_n e_n$

Definition

$A = \{v_1, \cdots, v_m\} \quad < A >=< v_1, \cdots, v_m > \quad A \ni a = v_1$
A linear abhängig $\Leftrightarrow \exists a \in A \quad a \in < A \setminus \{a\} >$

$dim V \leq n \Leftrightarrow$ Jede linear unabhängige Menge $A \subset V$ hat höchstens n Elemente (Vektoren)
$dim V \geq n \Leftrightarrow \exists$ linear unabhängige Menge $A \subset V, |A| > n$

Satz

Sei $A \subset V$ linear unabhängig $\Rightarrow \exists$ Basis $B \supset A$
d.h. jede linear unabhängige Menge von Vektoren kann zu einer Basis ergänzt werden

Corollar

Jeder Vektorraum hat Basis

Beispiel 1

$V = \mathbb{R}^2 \qquad A = \{v\}, v \neq 0$ linear unabhängig $\Rightarrow B = \{v_1, v_2\}$ Basis

Beispiel 2

$V = \mathbb{R}^3 \qquad A = \{v_1, v_2\} \sqsubset \mathbb{R}^3, \quad v_1, v_2$ linear unabhängig
$v_3 \notin < v_1, v_2 > \Rightarrow B = \{v_1, v_2, v_3\}$ Basis

Satz

A linear unabhängig, C Erzeugenden-System $\Rightarrow |A| \leq |C|$

Definition

$n =$ Zahl der Basisvektoren = Dimension von V

Standard-Beispiel

$V = K^n$
Standard-Basis e mit $|e| = n$ Basisvektoren $\Rightarrow dim K^n = n$

3.3.5 Methoden zur Basis-Konstruktion

$$A = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix} \in K^{m \times n}$$

Zeilenreduktion von A

$A_1 = (A_1^1, A_1^2, \cdots, A_1^n) \in K^n$ 1. Zeilenvektor
$\vdots$
$A_m = (A_m^1, A_m^2, \cdots, A_m^n) \in K^n$ m. Zeilenvektor

Definition

Zeilenraum von $A =< A_1, \cdots, A_m >=$ lineares Erzeugnis von $A_1, \cdots A_m$

Beispiel

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 3 & 4 & 1 \end{pmatrix} \in \mathbb{R}^{2 \times 3}$$

$A_1 = (1, 2, 0) \in real^3$
$A_2 = (3, 4, 1) \in real^3$

$< A_1, A_2 >= \alpha(1,2,0) + \beta(3,4,1) = (\alpha + 3\beta, 2\alpha + 4\beta, \beta)$ $\alpha, \beta \in \mathbb{R}$ beliebig
z.B. $\alpha = 1, \beta = 1:$ $(-2,-2,-1) \in < A_1, A_2 >$

Problem 1

Konstruire Basis des Zeilenraums und bestimme Dimension
(Dimension des Zeilenraums von $A = Rang(A)$)

Lösung

$K^{m\times n} \ni A \to$ Zeilenreduktion

$$\tilde{A} = \left(\begin{array}{cccccccc} 0 & X & \vert 1_{1a} & X & 0 & X & 0 \\ 0 & X & 0 & X & \vert 1_{2b} & X & 0 \\ 0 & X & 0 & X & 0 & X & \vert 1_{3c} \end{array}\right)$$

(i) Basis des Zeilenraums = Zeilen $\neq 0$ von $\tilde{A}$
(ii) Dimension des Zeilenraums von $A = Rang(A) = \#Zeilen \neq 0$ von $\tilde{A} = \#$ Pivotspalten

Beispiel

$u = (3,-6,9,0) \in real^4$
$v = (4,-6,8,-4) \in \mathbb{R}^4$
$w = (-2,-1,1,7) \in \mathbb{R}^4$

Finde Basis von $< u, v, w > \sqsubset \mathbb{R}^4$
Finde Dimension von $< u, v, w >$
Sind u, v, w linear unabhängig ?

Lösung:

$$A = \left(\begin{array}{cccc} 3 & 6 & 9 & 0 \\ 4 & -6 & 8 & -4 \\ -2 & -1 & 1 & 7 \end{array}\right) \in \mathbb{R}^{3\times 4}$$

$u = A_1, v = A_2, w = A_3$

Zeilenreduktion: $\tilde{A} = \left(\begin{array}{cccc} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array}\right)$

Basis des Zeilenraums von A = Basis von $< u, v, w >=< b_1, b_2, b_3 >=< \tilde{A}_1, \tilde{A}_2, \tilde{A}_3 >$
$b_1 = (1,0,0,3) \in \mathbb{R}^4$
$b_2 = (0,1,0,0) \in \mathbb{R}^4$
$b_3 = (0,0,1,1) \in \mathbb{R}^4$

Rang(A) = dim $< u, v, w >= 3 > \Rightarrow u, v, w$ linear unabhängig

Proposition

$A \in K^{m\times n} \Rightarrow ZeilenA_1, \cdots, A_m$ sind linear unabhängig $\Leftrightarrow Rang(A) = m$

Problem 2

Berechnen des homogenen Lösungsraums = Basis von Ker(A)

$$A = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix} \in K^{m \times n}$$

homogenes Problem:
$A_1^1 x_1 \cdots A_1^n x_n = 0$
$A_2^1 x_1 \cdots A_2^n x_n = 0$
$\vdots$
$A_m^1 x_1 \cdots A_m^n x_n = 0$

Finde Basis von $KerA$
$KerA = \{(x_1, \cdots, x_n) \in K^n | Ax = 0\}$ homogener Lösungsraum
Lösung:

$$A = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix} \Rightarrow \tilde{A} = \left(\begin{array}{ccccccc} 0 & X & \vert 1_{1a} & X & 0 & X & 0 \\ 0 & X & 0 & X & \vert 1_{2b} & X & 0 \\ 0 & X & 0 & X & 0 & X & \vert 1_{3c} \end{array}\right)$$

Allgemeine Lösung:
Nicht-pivot: x_N frei wählbar
pivot: $X_P = -\tilde{A}_P^N x_N$

Basis des Lösungsraums:
$X_N = (1, 0, \cdots, 0)$
$X_N = (0, 1, \cdots, 0)$
$\vdots X_N = (0, 0, \cdots, 1)$

Dimension des Lösungsraums = # Nicht-Pivot-Spalten = n - Rang(A)
n = # Spalten = # Pivot-Spalten (also Rang A) + # Nicht-Pivot-Spalten (also Ker A)

3.3.6 Definition der Matrizen-Transposition

(Spiegelung an der Diagonalen)

$$A = \begin{pmatrix} A_1^1 & A_1^2 & A_1^3 \\ A_2^1 & A_2^2 & A_2^3 \\ A_3^1 & A_3^2 & A_3^3 \end{pmatrix} \Rightarrow A^t = \begin{pmatrix} A_1^1 & A_2^1 & A_3^1 \\ A_1^2 & A_2^2 & A_3^2 \\ A_1^3 & A_2^3 & A_3^3 \end{pmatrix}$$

Eigenschaften

$(A + B)^t = A^t + B^t$
$(\alpha A)^t = \alpha A^t$
$(AB)^t = B^t A^t$

Satz

Basis des Lösungsraumes (Spalten) $v^{\cdot} = (v^1, \cdots, v^m)$

$$v^{\cdot} = \begin{pmatrix} -\tilde{A}_P^N \\ E_N^N \end{pmatrix}$$

Beispiel

$u + w = 0$
$-u - 2v - w + 2z = 0$
$2u + 2v + 5w + 3z = 0$
$u + 2v + 4w + 3z = 0$

$$\begin{pmatrix} u \\ v \\ w \\ z \end{pmatrix} \in K^{n\times 1}$$

Finde Basis des homogenen Lösungsraumes

Koeffizientenmatrix:

$$K^{4\times 4} \ni A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ -1 & -2 & -1 & 2 \\ 2 & 2 & 5 & 3 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

$$\Rightarrow \tilde{A} = \begin{pmatrix} 1 & 0 & 0 & -\frac{5}{3} \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & \frac{5}{3} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$ Dimension des Lösungsraumes = # N = 1

Basis des Lösungsraumes = 1 Vektor (weil nur 1 N)

$$v = \begin{pmatrix} -\frac{5}{3} \\ -1 \\ \frac{5}{3} \\ \boxed{1} \end{pmatrix} \qquad \boxed{1} \text{ wegen } E_1$$

Allgemeine Lösung: $X_N = z$ frei wählbar

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = - \begin{pmatrix} -\frac{5}{3} \\ -1 \\ \frac{5}{3} \end{pmatrix} z = \begin{pmatrix} \frac{5}{3}z \\ z \\ -\frac{5}{3}z \end{pmatrix}$$

$u = \frac{5}{3}z, v = z, w = -\frac{5}{3}$

$$\begin{pmatrix} u \\ v \\ w \\ z \end{pmatrix} = - \begin{pmatrix} -\frac{5}{3} \\ -1 \\ \frac{5}{3} \\ 1 \end{pmatrix} z = \begin{pmatrix} \frac{5}{3}z \\ z \\ -\frac{5}{3}z \\ z \end{pmatrix} = zV$$

Skalaprodukt in K^n

$x = (x_1, x_2, \cdots, x_n) \in K^n$
$y = (y_1, y_2, \cdots, y_n) \in K^n$

$$x \cdot y := xy^t = (x_1, \cdots, x_n) = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = x_1y_1 + \cdots x_ny_n$$

Bemerkung
Für Spalten $u, v \in K^{n\times 1}$

$$u \cdot v = u^t v = (u_1, \cdots, u_n) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Spezialfall: $x\dot{x} = x_1^2 + \cdots + x_n^2$

Länge: $||x|| = \sqrt{x_1^2 + \cdots + x_n^2} = \sqrt{x \cdot x}$
Spezialfall: Orthogonalität

$x, y \in K^n$
$x \perp y$ (senkrecht)
$\Leftrightarrow x \cdot y = 0 \Leftrightarrow x_1 y_1 + \cdots x_n y_n = 0$

3.3.7 Orthogonales Komplement

$< v_1, \cdots v_m >^{\perp} := \{x \in K^n | x \perp v_1, x \perp v_2 \cdots x \perp V_m\}$
$= \{x \in K^n | x \cdot v_1 = x \cdot v_2 = \cdots = x \cdot v_m = 0\}$ Unterraum von K^n

Beispiel

Finde eine Basis des Orthongal-Raumes der Vektoren
$u = (1, 8, 3, 6), v = (3, 0, 2, 2), w = (2, -8, -1, 6)$ im $\mathbb{R}^4$

Orthogonal-Raum $< u, v, w >^{\perp} \ni X$
$u \cdot x = 0, v \cdot x = 0, w \cdot x = 0$

$$u \cdot x \quad = 0 v \cdot x \quad = 0 w \cdot x \quad = 0 \qquad A = \begin{pmatrix} u \\ v \\ w \end{pmatrix} \begin{pmatrix} 1 & 8 & 3 & 6 \\ 3 & 0 & 2 & 2 \\ 2 & -8 & -1 & 6 \end{pmatrix}$$

$$\Rightarrow \tilde{A} \begin{pmatrix} 1 & 0 & \frac{3}{2} & 0 \\ 0 & 1 & \frac{7}{24} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Allgemeine Lösung:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_4 \end{pmatrix} = - \begin{pmatrix} \frac{3}{2} \\ \frac{7}{24} \\ 0 \end{pmatrix} x_3 = \begin{pmatrix} -\frac{3}{2} x_3 \\ -\frac{7}{24} x_3 \\ 0 \end{pmatrix}$$

$$< u, v, w >^{\perp} \ni x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} -\frac{3}{2} x_3 \\ -\frac{7}{24} x_3 \\ x_3 \\ 0 \end{pmatrix} = - \begin{pmatrix} \frac{3}{2} \\ \frac{7}{24} \\ 1 \\ 0 \end{pmatrix} x_3$$

Basisvektor $b = \begin{pmatrix} \frac{3}{2} \\ \frac{7}{24} \\ 1 \\ 0 \end{pmatrix} \in < u, v, w >^{\perp}$

Finde Einheitsvektor (Länge = 1) senkrecht auf u, v, w

$b \cdot b = ||b||^2 = (\frac{3}{2}, \frac{7}{24}, 1, 0) = \begin{pmatrix} \frac{3}{2} \\ \frac{7}{24} \\ 1 \\ 0 \end{pmatrix} = \frac{4}{9} + \frac{49}{9*64} + 1 = \frac{\sqrt{881}}{24}$

Einheitsvektor: $e \perp u, e \perp v, e \perp w, ||e|| = 1$

$e = \frac{b}{||v||} = \frac{\sqrt{881}}{24}(\frac{3}{2}, \frac{7}{24}, 1, 0)$

Satz zur Drehung von Vektoren um θ

$V = \mathbb{R}^2 \quad V \underset{linear}{\overset{R_\theta}{\leftarrow}} \quad R_\theta =$ Drehung um θ (Theta)

$R_\theta (u + v) = R_\theta u + R_\theta v$
$R_\theta (\alpha u) = \alpha R_\theta (u)$

Satz zur Matrix von R_θ

$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \in \mathbb{R}^{2\times 2}$

d.h. $R_\theta \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} \cos\theta v_1 + \sin\theta v_2 \\ -\sin\theta v_1 + \cos\theta v_2 \end{pmatrix}$

Proposition

$\theta_1, \theta_2 \in \mathbb{R} \Rightarrow R_{\theta_1} + R_{\theta_2} = R_{\theta_1 + \theta_2}$

Satz

Jeder $K-$Vektorraum V ist isomorph zu K^n

Beweis

Da V die Dimension n hat $\Rightarrow$ es existiert Basis $b = \{b^1, b^2, \cdots . b^n\} \subset V$ mit n Vektoren

$\Rightarrow K^{n\times 1} \underset{\approx}{\overset{b\cdot}{\rightarrow}} V$, d.h. $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \mapsto b^1\alpha_1 + \cdots + b^n\alpha_n = \sum_{j=1}^n b^j\alpha_j$ q.e.d.

Umkehrung des Isomorphismus $V \underset{\approx}{\overset{b\cdot^{-1}}{\rightarrow}} K^{n\times 1}$

$V \to V(b\cdot^{-1}) = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$

$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ = Komponenten von v bzgl. $(b^1, \cdots, b^n)$

Problem

Schreibe v als Komponenten bzgl. (e^1, r^2)

Lösung 1: Kartesiche Koordinaten

$$v = \begin{pmatrix} x \\ y \end{pmatrix} = xe^1 + ye^2$$

Lösung 2: Polarkoordinaten

$v = ||v|| \cos(\theta)e^1 + ||v|| \sin(\theta)e^2$
$\theta =$ Richtung von v
$||v|| =$ Länge von v

Satz

Jede lineare Abbildung $F : V \overset{F}{\underset{linear}{\leftarrow}} U$ lässt sich durch eine $(m \times n)$-Matrix darstellen, wobei $m = dimV, n = dimU$

Beweis

Sei $b^\cdot = (b^1, \cdots, b^n)$ Basis von V
Sei $a^\cdot = (a^1, \cdots, a^n)$ Basis von U

Definiere $(m \times n)$-Matrix $A = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix}$ wie folgt $\boxed{F\, a^j = \sum_{i=1}^m b^i A_i^j}$

Definition

$A = (A_i^j)$ heisst Koeffizienten-Matrix von F bzgl. Basen $a^\cdot = (a^1, \cdots, a^n)$ von V und $b^\cdot = (b^1, \cdots, b^n)$ von U.

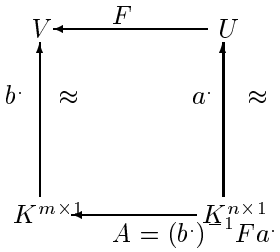
Beispiel

$V = U = \mathbb{R}^2$, Basis $e^\cdot = (e^1, e^2)$ Einheitsbasis, $F = R_\theta$

Koeffizienten-Matrix von R_θ
$R_\theta e^1 = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix} = \cos\theta e^1 + \sin\theta e^2$
$R_\theta e^2 = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} = -\sin\theta e^1 + \cos\theta e^2$

$\Rightarrow R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$

Formal



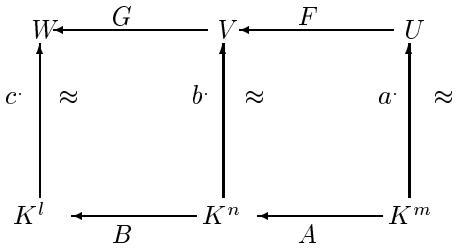
Proposition

U, V, W K-Vektorräume

$W \underset{linear}{\overset{G}{\leftarrow}} V \underset{linear}{\overset{F}{\leftarrow}} U$
$\Rightarrow W \underset{linear}{\overset{G\circ F}{\leftarrow}} U$

Beweis

Sei $a\cdot = (a^1, \cdots, a^n)$ Basis von U
Sei $b\cdot = (b^1, \cdots, b^n)$ Basis von V
Sei $c\cdot = (c^1, \cdots, c^n)$ Basis von W



$A = (b\cdot)^{-1} F a\cdot$ Koeffizienten-Matrix von F
$B = (c\cdot)^{-1} G b\cdot$ Koeffizienten-Matrix von G

$\Rightarrow BA = ((c\cdot)Gb\cdot)((b\cdot)^{-1}Fa\cdot)$
$= (c\cdot)^{-1} Gb\cdot (b\cdot)^{-1} Fa\cdot$
$= (c\cdot)^{-1} GFa\cdot = (c\cdot)^{-1}(GF)a\cdot$ = Koeffizienten-Matrix von GF

3.3.8 Additionstheorem

für $\sin\theta, cos\theta$

$\cos(\theta_1 + \theta_2) = \cos\theta_1 \cos\theta_2 - \sin\theta_1 \sin\theta_2$
$\sin(\theta_1 + \theta_2) = \sin\theta_1 \cos\theta_2 + \cos\theta_1 \sin\theta_2$

3.4 Determinanten und Eigenwerte

Definition

$U = V$

$A = \begin{pmatrix} A_1^1 & A_1^n \\ A_m^1 & A_m^n \end{pmatrix}$ und $A^t = \begin{pmatrix} A_1^1 & A_m^1 \\ A_1^n & A_m^n \end{pmatrix}$
$Det(A) \in K$
$Det(AB) = Det(A) \cdot Det(B)$

3.4.1 Anwendung der Determinanten

Satz

$A \in K^{n \times n}$ ist invertierbar, d.h. $A \in GL(n, K) \Leftrightarrow Det(A) \neq 0$

1. Anwendung

n Vektoren in K^n: $v^1, \cdots v^n \in K^{n \times 1}$ sind linear unabhängig
$\Leftrightarrow v^{\cdot} = (v^1, \cdots, v^n)$invertierar
$\Leftrightarrow Det(v^1, \cdots, v^n) \neq 0$

Ebenso für Zeilenvektoren $v_1, \cdots, v_n \in K^{1 \times n}$ sind linear unabhängig
$\Leftrightarrow Det(v_1, \cdots, v_n) \neq 0$

2. Anwendung

n Gleichungen mit n Unbekannten $A \in K^{n \times n}$, $Ax = 0$

$Ax = 0$ hat nicht-triviale Lösung $x \neq 0 \Leftrightarrow Det(A) = 0$

3.4.2 Eigenwerte

$A \in K^{n \times n}$, $E =$ Einheitsmatrix
$\lambda \in K$ Eigenwert von $A \Leftrightarrow \boxed{\exists v \in K^n, v \neq 0 : Av = \lambda v}$
$\Leftrightarrow$ Eigenraum (Raum aller Eigenvektoren) $Ker(\lambda E - A) \neq \{0\}$

λ Eigenwert $\Leftrightarrow$ Det$(\lambda E - A) = 0$
$\Leftrightarrow \lambda =$ Nullstelle von Det$(\lambda E - A)$ =charakteristisches Polynom

Beispiel

$A = \begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} \in \mathbb{R}^{2 \times 2}$

(i) Berechne Eigenwerte
(ii) Berechne Eigenvektoren

Schritt 1 $\text{Det}(\lambda E - A) = \begin{vmatrix} \lambda - 1 & -2 \\ -3 & \lambda - 2 \end{vmatrix} = \lambda^2 - 3\lambda - 4$

Schritt 2 $\text{Det}(\lambda E - A) = \lambda^2 - 3\lambda - 4 = 0 \Leftrightarrow \lambda_{1/2} = \frac{3}{2} \pm \sqrt{\frac{3}{4} + 4} = \frac{3}{2} \pm \frac{5}{2}$

Eigenwerte: $\lambda_1, \lambda_2 = -1; 4$

Schritt 3.1 Eigenvektoren zu $\lambda_1 = 4$

$Av = \lambda_1 v = 4v; v = \begin{pmatrix} x \\ y \end{pmatrix}$

$\begin{pmatrix} 1 & 2 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 4 \begin{pmatrix} x \\ y \end{pmatrix}$

$x + 2y = 4x, 3x + 2y = 4y$

$\Rightarrow A - 4E = \begin{pmatrix} -3 & 2 \\ 3 & -2 \end{pmatrix} \Rightarrow \overline{A - 4E} = \begin{pmatrix} 1 & -\frac{2}{3} \\ 0 & 0 \end{pmatrix}$

y beliebig, $x = \frac{2}{3}y$ Eigenvektor $v^1 = \begin{pmatrix} \frac{2}{3} \\ 1 \end{pmatrix}$

Schritt 3.1 Eigenvektoren zu $\lambda_2 = -1$

$\Rightarrow A - 4E = \begin{pmatrix} 2 & 2 \\ 3 & 3 \end{pmatrix} \Rightarrow \overline{A - 4E} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

y beliebig $\quad x = -y \Rightarrow v^2 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$

Basis der Eigenvektoren:

$v^{\cdot} = (v^1, v^2) = \begin{pmatrix} \frac{2}{3} & -1 \\ 1 & 1 \end{pmatrix}$

Satz

Sei $A \in K^{n \times n}$ mit Basis $v^{\cdot} = (v^1, \cdots, v^n)$ von Eigenvektoren

$\Rightarrow {v^{\cdot}}^{-1} A v^{\cdot} = \text{Diagonal-Matrix} = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}$

$A = v^{\cdot} \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix} {v^{\cdot}}^{-1}$

Satz

$A \in K^{n \times n}$ mit n verschiedenen Eigenwerten $\lambda_1, \cdots, \lambda_n$
$\Rightarrow A$ diagonalisierbar ($\exists$ Eigenbasis)

Satz

$A \in \mathbb{R}^{n \times n}, A^t = A$ symmetrische Basis
$\Rightarrow A$ hat n reelle Eigenwerte und A ist diagonalisierbar

3.4.3 Diagonalisierung von Matrizen

Sei $A \in K^{n \times n}$

Ziel

(i) Finde Basis des K^n aus Eigenvektoren zu A
$v^{\cdot} = ({}^1, \cdots, v^n)$ Basis
$Av^i = \lambda_i v^i$

(ii) $v^{\cdot\,-1} A v^{\cdot} = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}$

$$A = v^{\cdot} \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix} v^{\cdot\,-1}$$

Strategie

Schritt 1 Charakteristisches Polynom Det$(\lambda E - A)$ vom Grad n
Schritt 2 Finde Nullstellen Deat$(\lambda_k E - A) = 0 \quad 1 \leq k \leq n$
$\lambda k = k - ter$ Eigenwert
Schritt 3 Sei k fest gewählt $\Rightarrow \lambda_k$ bekannt.
Betrachte: linear homogenes Problem
$Av^k = \lambda_k v^k \quad v^k$ unbekannt
$(A = \lambda_k E)v^k = 0$
Lösung durch Zeilenreduktion $A - \lambda_k E \Rightarrow \overline{A - \lambda_k E}$
Schritt 4 $(v^1, \cdots, v^n)$ Basis von Eigenvektoren
Schritt 5 Invertiere $v^{\cdot} \Rightarrow v^{\cdot\,-1}$
aber falls $A^t = A \Rightarrow v^{\cdot\,-1} = v^{\cdot\,t}$

Definition

A symmetrisch $\Leftrightarrow A^t = A \Leftrightarrow$

(i) alle Eigenwerte reell $\lambda_1, \cdots, \lambda_n$
(ii) Basis aus Eigenvektoren $v^1, \cdots, v^n$
Orthonormalbasis: $||v^k|| = 1, v^i \cdot v^j = 0$
$(v^{\cdot})^{-1} = (v^{\cdot})^t$

Beispiel

$$A = \begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} = A^t$$

(i) Det$(\lambda E - A) = \begin{vmatrix} \lambda - 1 & 2 \\ 2\lambda - 4 & \end{vmatrix}$

(ii) $0 = \lambda^2 - 5\lambda = \lambda(\lambda - 5)$

$\lambda_1 = 0; \lambda_2 = 5$

(iii) $\lambda_1 = 0$

$$\begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

y beliebig, $x = 2y$

$v^1 = \begin{pmatrix} 2y & y \end{pmatrix} \quad ||v^1||^2 = (2y)^2 + y^2 = 5y^2 \Rightarrow y = \frac{1}{\sqrt{5}}$

$$v^1 = \begin{pmatrix} \frac{2}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} \end{pmatrix}$$

$\lambda_2 = 5$

$$\begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 5 \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 5x \\ 5y \end{pmatrix}$$

y beliebig, $x = -\frac{y}{2}$

$v^2 = \begin{pmatrix} -\frac{y}{2} & y \end{pmatrix} \quad ||v^2||^2 = (-\frac{y}{2})^2 + y^2 = \frac{y^2}{4} + y^2 = \frac{5}{4}y^2 \Rightarrow y = \frac{2}{\sqrt{5}}$

$$v^2 = \begin{pmatrix} -\frac{1}{\sqrt{5}} \\ \frac{2}{\sqrt{5}} \end{pmatrix}$$

$$v^{\cdot} = (v^1, v^2) = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 & -1 \\ 1 & 2 \end{pmatrix}$$

$$v^{\cdot -1} = (v^{\cdot})^t = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & -2 \\ -2 & 4 \end{pmatrix} = \begin{pmatrix} \frac{2}{\sqrt{5}} & -\frac{1}{\sqrt{5}} \\ \frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 5 \end{pmatrix} \begin{pmatrix} \frac{2}{\sqrt{5}} & \frac{1}{\sqrt{5}} \\ -\frac{1}{\sqrt{5}} & \frac{2}{\sqrt{5}} \end{pmatrix}$$