Lineare Algebra

Skriptum zur Vorlesung von Prof. Dr. Victor Bangert
WS 2002/03 und SS 2003

Zur Einleitung: Lineare Gleichungssysteme

Wir untersuchen zunächst mit Methoden, die Sie vermutlich aus der Schule kennen, explizit einige kleine lineare Gleichungssysteme. Das Gleichungssystem I wird dabei sukzessive in "einfachere" Gleichungssysteme II, III, ... umgeformt. Die Umformungen sind so, daß sich die Lösungsmenge nicht ändert.

1) 1 Gleichung, 1 Unbekannte:

$$\begin{array}{lrl} \text{I} & 3x+5=9 & \mid -5 \\ \text{II} & 3x=4 & \mid :3 \\ \text{II} & x=\frac{4}{3} & \end{array}$$

Lösungsmenge $L_{\text{I}} = \{x \in \mathbb{R} \mid 3x+5=9\} = L_{\text{II}} = \{x \in \mathbb{R} \mid 3x=4\} = L_{\text{III}} = \left\{\frac{4}{3}\right\}$

2) 1 Gleichung, 2 Unbekannte:

$$\begin{array}{lrl} \text{I} & 2x+4y=8 & \mid :4 \mid -\frac{x}{2} \\ \text{II} & y=-\frac{x}{2}+2 & \end{array}$$

Betrachte geordnete Paare (x,y) mit $x \in \mathbb{R}, y \in \mathbb{R}$ und setze $\mathbb{R}^2 = \{(x,y) \mid x \in \mathbb{R} \text{ und } y \in \mathbb{R}\}$

$$L_I = \{(x,y) \in \mathbb{R}^2 \mid 2x+4y=8\} = L_{II} = \{(x, -\tfrac{x}{2}+2) \mid x \in \mathbb{R}\}$$

Es gibt unendlich viele Lösungen!

3) 2 Gleichungen, 2 Unbekannte:

$$\begin{array}{lrcll} \text{I} & 2x+4y & = & 8 & \mid \cdot\left(-\frac{3}{2}\right) \\ & 3x-6y & = & 4 & \leftarrow\mid \\ \text{II} & 2x+\ \ 4y & = & 8 & \\ & 0x-12y & = & -8 & \mid :(-12) \\ \text{III} & 2x+4y & = & 8 & \qquad 2x+\frac{8}{3}=8 \qquad 2x=\frac{16}{3} \qquad x=\frac{8}{3} \\ & y & = & \frac{2}{3} & \\ \text{IV} & x & = & \frac{8}{3} & \\ & y & = & \frac{2}{3} & \end{array}$$

$L_I = \{(x,y) \in \mathbb{R}^2 \mid (x,y) \text{ löst (I)}\} = \left\{\left(\frac{8}{3}, \frac{2}{3}\right)\right\}$, genau eine Lösung.

4) 2 Gleichungen, 2 Unbekannte:

$$\text{I} \qquad \begin{array}{rcl} 2x+4y &=& 8 \\ 3x+6y &=& 4 \end{array} \quad \left| \cdot\left(-\tfrac{3}{2}\right) \right. \quad \leftarrow|$$

$$\text{II} \qquad \begin{array}{rcl} 2x+4y &=& 8 \\ 0x+0y &=& -8 \end{array}$$

keine Lösung, $\quad L_I = \{(x,y) \in \mathbb{R}^2 \mid (x,y) \text{ erfüllt (I)}\} = \emptyset$

Geometrische Interpretation: Für eine Gleichung $ax + by = c$ mit $a \neq 0$ oder $b \neq 0$ (das wird im folgenden Abschnitt stets vorausgesetzt) ist die Lösungsmenge eine Gerade in der Ebene $\mathbb{R}^2$. (Für $b \neq 0$ etwa gegeben durch $y = -\frac{a}{b}x + \frac{c}{b}$). Zwei lineare Gleichungen mit zwei Unbekannten entsprechen also zwei Geraden und der Lösungsmenge des Gleichungssystems entspricht die Menge der Punkte, die auf jeder der beiden Geraden liegen. Im allgemeinen gibt es also genau eine Lösung des Gleichungssystems (= genau einen Schnittpunkt der beiden Geraden). Folgende Ausnahmefälle sind möglich:

a Verschiedene parallele Geraden ($\Rightarrow$ keine Lösung des Gleichungssystems)
b die beiden Geraden stimmen überein ($\Rightarrow$ unendlich viele Lösungen des Gleichungssystems, Lösungsraum durch einen reellen Parameter parametrisierbar).

Bemerkung: Zum Lösen haben wir nur die Grundrechenarten benützt. Sind die Koeffizienten (a, b etc.) rational (oder komplex), so liefert dieses Verfahren rationale (oder komplexe) Lösungen.

Gaußsches Eliminationsverfahren (überführt Gleichungssystem in äquivalentes in Stufenform $\rightarrow$ rekursiv auflösbar).

5) 3 Gleichungen mit 4 Unbekannten (genannt x_1, x_2, x_3, x_4).

$$\text{I} \qquad \begin{array}{rcrcrcrcr} 2x_1 &+& 4x_2 &+& 4x_3 &+& 6x_4 &=& 2 \\ 3x_1 &+& 7x_2 &+& 5x_3 &+& 9x_4 &=& 4 \\ x_1 &+& 3x_2 &-& x_3 &+& 5x_4 &=& 1 \end{array} \quad \left| \cdot\left(-\tfrac{3}{2}\right) \right. \quad \left| \cdot\left(-\tfrac{1}{2}\right) \right. \quad \leftarrow| \quad \leftarrow|$$

$$\text{II} \qquad \begin{array}{rcl} 2x_1 + 4x_2 + 4x_3 + 6x_4 &=& 2 \\ x_2 - x_3 &=& 1 \\ x_2 - 3x_3 + 2x_4 &=& 0 \end{array} \quad \left| (-1) \right. \quad \leftarrow|$$

$$\text{III} \qquad \begin{array}{rcrl} 2x_1 + 4x_2 + 4x_3 + 6x_4 &=& 2 & \text{III}_1 \\ x_2 - x_3 &=& 1 & \text{III}_2 \\ -2x_3 + 2x_4 &=& -1 & \text{III}_3 \end{array}$$

Gleichungssystem in Stufenform
("rekursiv ausflösbar")

Lösung: Wähle $x_4 = r \in \mathbb{R}$ beliebig

$$\begin{array}{lllllll} \mathrm{III}_3 & \Rightarrow & x_3 & = & x_4 + \frac{1}{2} & = & r + \frac{1}{2} \\ \mathrm{III}_2 & \Rightarrow & x_2 & = & x_3 + 1 & = & r + \frac{3}{2} \\ \mathrm{III}_1 & \Rightarrow & x_1 & = & -2x_2 - 2x_3 - 3x_4 + 1 & = & -7r - 3 \end{array}$$

$$\begin{array}{rcl} \mathbb{R}^4 & = & \{(x_1, x_2, x_3, x_4) \mid x_1 \in \mathbb{R}, x_2 \in \mathbb{R}, x_3 \in \mathbb{R}, x_4 \in \mathbb{R}\} \\ L_I & = & \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid (x_1, x_3, x_3, x_4) \text{ löst I}\} \\ & = & \{(-7r - 3, r + \frac{3}{2}, r + \frac{1}{2}, r) \mid r \in \mathbb{R}\} \text{ Parameterdarstellung des Lösungsraums} \end{array}$$

1. Zur Sprache der Mathematik

übliche Sprache + Fachausdrücke + mathematische Symbole

<u>Abkürzende logische Symbole</u>

(1.1) "$A \Rightarrow B$" bedeutet "aus Aussage A folgt Aussage B".
Beispiel: $x \in \mathbb{R} \Rightarrow x^2 \geq 0$
Andere sprachliche Formen:
"A impliziert B" oder
"A ist hinreichend für B"
"B ist notwendig für A"

(1.2) "$A \Leftrightarrow B$" bedeutet "$A \Rightarrow B$ und $B \Rightarrow A$".
Beispiel: $x \in \mathbb{R}$ und $3x \in \mathbb{Q} \Leftrightarrow x \in \mathbb{Q}$
Andere sprachliche Formen: "A und B sind äquivalent" oder "A gilt genau dann (dann und nur dann), wenn B gilt".

(1.3) "$\exists$" steht für "Es existiert (mindestens) ein ..."
Beispiel: "$\exists x \in \mathbb{R} : x^2 = 2$ steht für "Es existiert ein $x \in \mathbb{R}$, so daß $x^2 = 2$ gilt" (nämlich $x = \sqrt{2}$ oder $x = -\sqrt{2}$.

(1.4) "$\forall$" steht für "Für alle ..."
Beispiel: "$\forall x \in \mathbb{R} : x^2 \geq 0$" steht für "Für alle reellen Zahlen x gilt: $x^2 \geq 0$"

Schließlich: "oder" ist nicht ausschließend (im Gegensatz zu "entweder ... oder").
Die Aussage "Es gilt $1 + 1 = 2$ oder es gilt $1 - 1 = 0$" ist wahr.
Die Aussage "Entweder es gilt $1 + 1 = 2$ oder es gilt $1 - 1 = 0$" ist falsch.

(1.5) "$A := B$" steht für "A ist durch B definiert" oder "A ist nach Definition gleich B".

<u>Mengen und Abbildungen</u> (Georg Cantor 1845-1918)

Menge = Zusammenfassung von (mathematischen) Objekten (=Elementen)
"$x \in M$" steht für "x ist Element der Menge M",
"$x \notin M$" steht für "x ist nicht Element der Menge M".

Angabe von Mengen:

(1.6) Aufzählend, z.B. $M = \{1, 3, 5, 7\} (= \{1, 1, 3, 5, 7\})$

(1.7) Durch Angabe von Eigenschaften: Sei M eine Menge und $A(x)$ eine Aussage über die Elemente von M. Dann kann man eine Menge N definieren durch

$$N = \{x \mid x \in M \text{ und } A(x) \text{ ist wahr}\} = \{x \in M \mid A(x) \text{ ist wahr}\}$$

z.B. $\mathbb{Q} = \{x \in \mathbb{R} \mid \exists p \in \mathbb{Z}, \exists q \in \mathbb{N}, q \neq 0 : x = \frac{p}{q}\}$ Menge der rationalen Zahlen oder $M = \{x \in \mathbb{N} \mid x \text{ ist ungerade natürliche Zahl kleiner als } 9\}$.

Beispiele von Mengen:
$$\begin{aligned} \mathbb{N} &= \{x \in \mathbb{R} \mid x \text{ natürliche Zahl}\} = \{0, 1, 2, 3, \ldots\} \\ \mathbb{Z} &= \{x \in \mathbb{R} \mid x \text{ ganze Zahl}\} = \{0, 1, -1, 2, -2, \ldots\} \end{aligned}$$

Vielleicht kennen Sie schon $\mathbb{C} = \{x + iy \mid x \in \mathbb{R}, y \in \mathbb{R}\}$
$\emptyset$ die leere Menge (enthält kein Element)

(1.8) Def.: Eine Menge A heißt <u>Teilmenge einer Menge</u> B ("$A \subseteq B$"), falls jedes Element von A auch Element von B ist, d.h. falls gilt

$$x \in A \Rightarrow x \in B.$$

Beispiel: $\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

(1.9) Zwei Mengen A und B sind gleich ("$A = B$"), wenn A und B die selben Elemente enthalten, d.h. falls gilt

$$x \in A \Leftrightarrow x \in B$$

Oder: $A = B \Leftrightarrow A \subseteq B$ und $B \subseteq A$.

Beispiel: $\{x \mid x \text{ ungerade natürliche Zahl kleiner } 9\} = \{1, 3, 5, 7\}$

Konstruktionen mit Mengen A und B:

(1.10) <u>Schnittmenge</u> (Durchschnitt) $A \cap B$ <u>von</u> A <u>und</u> B:

$$x \in A \cap B \Leftrightarrow x \in A \text{ und } x \in B$$

<u>Vereinigung</u> $A \cup B$ <u>von</u> A <u>und</u> B:

$$x \in A \cup B \Leftrightarrow x \in A \text{ oder } x \in B$$

<u>Komplement</u> $A \setminus B$ <u>von</u> B <u>in</u> A (Differenzmenge von A und B)

$$x \in A \setminus B \Leftrightarrow x \in A \text{ und } x \notin B$$

(1.11) Rechenregeln (für Vereinigung, Durchschnitt, Komplement)

Sind A, B, C Mengen, so gilt:

(a)	$A \cup B$	$=$	$B \cup A$, $A \cap B = B \cap A$	"Kommutativgesetze"
(b)	$(A \cup B) \cup C$	$=$	$A \cup (B \cup C)$	"Assoziativgesetze"
	$(A \cap B) \cap C$	$=$	$A \cap (B \cap C)$	
(c)	$A \cap (B \cup C)$	$=$	$(A \cap B) \cup (A \cap C)$	"Distributivgesetze"
	$A \cup (B \cap C)$	$=$	$(A \cup B) \cap (A \cup C)$	
(d)	$A \setminus (B \cup C)$	$=$	$(A \setminus B) \cap (A \setminus C)$	"De Morgansche Regeln"
	$A \setminus (B \cap C)$	$=$	$(A \setminus B) \cup (A \setminus C)$	

Beweis von (c):
Sei $x \in A \cap (B \cup C) \Rightarrow x \in A$ und ($x \in B$ oder $x \in C$) $\Rightarrow$
($x \in A$ und $x \in B$) oder ($x \in A$ und $x \in C$) $\Rightarrow x \in (A \cap B) \cup (A \cap C)$

Sei $x \in (A \cap B) \cup (A \cap C) \Rightarrow$ ($x \in A$ und $x \in B$) oder ($x \in A$ und $x \in C$)
$\Rightarrow x \in A$ und ($x \in B$ oder $x \in C$) $\Rightarrow x \in A \cap (B \cup C)$

(1.12) Kartesische Produkt (benannt nach R. Descartes 1596-1650). Sind A, B Mengen, so ist das <u>kartesische Produkt</u> $A \times B$ <u>von</u> A <u>und</u> B die Menge aller geordneten Paare (a, b) mit $a \in A$ und $b \in B$.

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

Bem.: $(a, b) = (a', b') \Leftrightarrow a = a'$ und $b = b'$!

Bem.: $\mathbb{R} \times \mathbb{R} =: \mathbb{R}^2$

Allgemeiner: Sind $A_1, \ldots, A_n$ Mengen, so

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$$

Dabei gilt – per definitionem – $(a_1, \ldots, a_n) = (a'_1, \ldots, a'_n)$ genau dann, wenn $a_1 = a'_1$, ..., $a_n = a'_n$ gelten.

Bem.: $\underbrace{\mathbb{R} \times \ldots \times \mathbb{R}}_{n\text{-mal}} =: \mathbb{R}^n$. Ein Element $(a_1, \ldots, a_n) \in \mathbb{R}^n$ heißt <u>n-Tupel</u> von reellen Zahlen.

Exkurs: Nochmals lineare Gleichungssysteme

Das allgemeine lineare Gleichungssystem mit m Gleichungen und n Unbekannten:

$$\mathrm{I} \quad \begin{array}{lccccccc} I_1 & a_{11}x_1 & + & a_{12}x_2 & + \ldots + & a_{1n}x_n & = & b_1 \\ I_2 & a_{21}x_1 & + & a_{22}x_2 & + \ldots + & a_{2n}x_n & = & b_2 \\ \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ I_m & a_{m1}x_1 & + & a_{m2}x_2 & + \ldots + & a_{mn}x_n & = & b_m \end{array}$$

Gegeben sind die $a_{11}, \ldots, a_{mn}, b_1, \ldots, b_m$, gesucht die $x_1, \ldots, x_n$.

Lösungsmenge $L_I = \{(x_1, \ldots, x_n) \in \mathbb{R}^n \mid (x_1, \ldots, x_n)$ löst $I\}$

(1.13) Satz. *Sei $a_{11} \neq 0$ und sei I' das Gleichungssystem mit den Zeilen*

$$I'_1 = 1, I'_2 = I_2 - \frac{a_{21}}{a_{11}} I_1, \ldots, I'_m = I_m - \frac{a_{m1}}{a_{11}} I_1.$$

Dann gilt: $L_I = L_{I'}$

Beweis: Sei $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_n) \in L_I$. Dann erfüllt $\overline{x}$ die Gleichung I'_1 $(= I_1)$. Ist $2 \leq i \leq m$, so erfüllt $\overline{x}$ auch die Gleichung I_i, also auch $I'_i = I_i - \frac{a_{i1}}{a_{11}} I_1$. Also $x \in L_{I'}$.

Sei $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_n) \in L_{I'}$. Dann erfüllt $\overline{x}$ die Gleichung I_1 $(= I'_1)$.

Ist $2 \leq i \leq m$, so erfüllt $\overline{x}$ auch die Gleichung I'_i, also auch

$$I_i = I'_i + \frac{a_{i1}}{a_{11}} I_1.$$

Also $x \in L_I$.

(1.14) Definition. Das lineare Gleichungssystem I heißt homogen, falls $b_i = 0$ gilt für alle $i \in \{1, \ldots, m\}$.

Bemerkung: Ist I homogen, so ist $(0, \ldots, 0) \in \mathbb{R}^n$ Lösung von I.

Auf $\mathbb{R}^n$ definieren wir eine Addition durch

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n) \quad \text{(komponentenweise Addition)}$$

und eine Multiplikation mit reellen Zahlen $r \in \mathbb{R}$ durch

$$r(x_1, \ldots, x_n) := (rx_1, \ldots, rx_n)$$

(1.15) Satz. *Ist I ein homogenes lineares Gleichungssystem, so hat seine Lösungsmenge L_I folgende Eigenschaften:*

Ist $x = (x_1, \ldots, x_n) \in L_I$ *und* $y = (y_1, \ldots, y_n) \in L_I$, *so gilt* $x + y \in L_I$.
Ist $x = (x_1, \ldots, x_n) \in L_I$ *und* $r \in \mathbb{R}$, *so gilt* $rx \in L_I$.

Beweis: $x \in L_I$ und $y \in L_I \Rightarrow$ Für alle $i \in \{1, \ldots, m\}$ gelten: $a_{i1}x_1 + \ldots + a_{in}x_n = 0$ und $a_{i1}y_1 + \ldots + a_{in}y_n = 0$. Summiert man diese Gleichungen, so folgt

$$a_{i1}(x_1 + y_1) + \ldots + a_{in}(x_n + y_n) = 0 + 0 = 0$$

Also erfüllt $x+y = (x_1+y_1, \ldots, x_n+y_n)$ für alle $i \in \{1, \ldots, m\}$ die Gleichung I_i, d.h. $x+y \in L_I$.

Die 2. Behauptung folgt analog durch Multiplikation von I_i mit r.

Bemerkung: Besitzt ein homogenes lineares Gleichungssystem I eine Lösung $x \neq (0, \ldots, 0)$, so besitzt I nach (1.15) unendlich viele Lösungen $(\forall r \in \mathbb{R} : rx \in L_I)$.

Zu einem linearen Gleichungssystem I bezeichne I^{hom} das zugehörige homogene lineare Gleichungssystem, das sich nur dadurch von I unterscheidet, daß alle rechten Seiten von I durch 0 ersetzt werden.

(1.16) Satz. *Es existiere eine Lösung* $\overline{x} = (\overline{x}_1, \ldots, \overline{x}_n)$ *des linearen Gleichungssystems I. Dann gilt*

$$L_I = \{\overline{x} + x \mid x \in L_{I^{\text{hom}}}\}.$$

Ohne die Mengensprechweise drückte man die Aussage von (1.16) früher durch folgenden langen Satz aus: Die allgemeine Lösung eines linearen Gleichungssystems ist eine spezielle Lösung dieses Gleichungssystems plus die allgemeine Lösung des zugehörigen homogenen Gleichungssystems.

Beweis:

a) Sei $y \in L_I$. Wie zeigen: $y - \overline{x} \in L_{I^{\text{hom}}}$ (wobei $y - \overline{x} := y + (-1)\overline{x}$).

$$\{y, \overline{x}\} \subseteq L_I \Rightarrow \forall i \in \{1, \ldots, m\} \quad : \quad \begin{array}{l} a_{i1}y_1 + \ldots + a_{in}y_n = b_i \text{ und} \\ a_{i1}\overline{x}_1 + \ldots + a_{in}\overline{x}_n = b_i \end{array}$$

Subtraktion dieser Gleichungen liefert:

$$a_{i1}(y_1 - \overline{x}_1) + \ldots + a_{in}(y_n - \overline{x}_n) = b_i - b_i = 0$$

Also: $y - \overline{x} \in L_{I^{\text{hom}}}$. Wir nennen $y - \overline{x} =: x \in L_{I^{\text{hom}}}$ und erhalten $y = \overline{x} + x$ mit $x \in L_{I^{\text{hom}}}$.

b) Sei $x \in L_{I^{\text{hom}}}$. Dann gilt für alle $i \in \{1, \ldots, m\}$:

$$a_{i1}x_1 + \ldots + a_{in}x_n = 0$$

Wegen $y \in L_I$ gilt für alle $i \in \{1, \ldots, m\}$:

$$a_{i1}y_1 + \ldots + a_{in}y_n = b_i$$

Addition dieser Gleichungen liefert:

$$a_{i1}(x_1 + y_1) + \ldots + a_{im}(x_m + y_m) = b_i \quad (\text{für alle } i \in \{1, \ldots, m\})$$

also $y + x \in L_I$.

Zurück zur Mengenlehre:

Abbildungen zwischen Mengen

(1.17) Def.: Es seien M, N Mengen. Eine <u>Abbildung</u> $f : M \to N$ <u>von</u> M <u>nach</u> N ist eine Vorschrift, die jedem $x \in M$ genau ein Element $f(x) \in N$ zuordnet.

Beispiele:

a) $M = N = \mathbb{R}$, $f : \mathbb{R} \to \mathbb{R}$, $\forall x \in \mathbb{R} : f(x) := 3x^3 - x + 1$
b) $M = \mathbb{R}$, $N = \mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$, $\forall x \in \mathbb{R} : f(x) := e^x$.
c) $f : \mathbb{Z} \to \{0, 1\}$, $f(x) := \begin{cases} 0 & x \text{ gerade} \\ 1 & x \text{ ungerade} \end{cases}$
d) M Menge. $\text{id}_M : M \to M$, $\forall x \in M : \text{id}_M(x) := x$. "Identität von M".
e) $A \subseteq B$. $i : A \to B$, $\forall x \in A : i(x) := x$ "Inklusionsabbildung"

f) Seien $A_1, \ldots, A_n$ Mengen und $i \in \{1, \ldots, n\}$.
$p_i : A_1 \times \ldots \times A_n \to A_i, p_i(a_1, \ldots, a_n) := a_i$ "Projektion auf die i'te Komponente".
g) $+ : \mathbb{R}^2 \to \mathbb{R}$, $\forall (x, y) \in \mathbb{R}^2 : +(x, y) := x + y$

(1.18) Def.: Eine Abbildung $f : M \to N$ heißt

(a) injektiv, falls für alle $x \in M, y \in M$ gilt: $x \neq y \Rightarrow f(x) \neq f(y)$.
(b) surjektiv, falls für alle $y \in N$ ein $x \in M$ existiert, so daß $f(x) = y$ gilt.
(c) bijektiv, falls f injektiv und surjektiv is.

Von den obigen Beispielen ist a) surjektiv, aber nicht injektiv, während b) bijektiv ist.

(1.19) Def. (Komposition, Hintereinanderausführung) Seien A, B, C, D Mengen mit $B \subseteq C$ und $f : A \to B$, $g : C \to D$ Abbildungen. Dann ist $g \circ f : A \to D$ definiert durch: Für alle $x \in A$ ist $(g \circ f)(x) := g(\underbrace{f(x)}_{\in B})$.

Symbolisch: $\overbrace{A \xrightarrow{f} B \subseteq C \xrightarrow{g} D}^{g \circ f}$

Bem.: $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \Rightarrow h \circ (g \circ f) = (h \circ g) \circ f =: h \circ g \circ f$

Schreibweise: Ist $f : A \to B$ Abbildung und $C \subseteq A$, so bezeichne

$$f(C) := \{y \in B \mid \exists x \in C : f(x) = y\} \text{"Bild von } C \text{ unter } f\text{"}$$

Ist $D \subseteq B$, so bezeichne

$$f^{-1}(D) := \{x \in A \mid f(x) \in D\} \text{ "Urbild von } D \text{ unter } f\text{"}$$

Bem:

$f : A \to B$ surjektiv $\Leftrightarrow$ $f(A) = B$.
$f : A \to B$ injektiv $\Leftrightarrow$ Für alle $y \in B$ enthält $f^{-1}(\{y\})$ höchstens 1 Element.

(1.20) Rechenregeln: Sei $f : M \to N$ Abbildung, $A \subseteq M$, $B \subseteq M$. Dann gilt

(a) $f(A \cup B) = f(A) \cup f(B)$
(b) $f(A \cap B) \subseteq f(A) \cap f(B)$
(c) $f(M \setminus A) \supseteq f(M) \setminus f(A) \quad (\Leftrightarrow f(M) \setminus f(A) \subseteq f(M \setminus A))$
Für alle $C \subseteq N$, $D \subseteq N$ gilt:
(d) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$
(e) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$
(f) $f^{-1}(N \setminus C) = M \setminus f^{-1}(C)$

Beweis von (f):

$$\begin{gathered} x \in f^{-1}(N \setminus C) \Rightarrow x \in M \text{ und } f(x) \in N \setminus C \\ \Rightarrow x \in M \text{ und } f(x) \notin C \Rightarrow x \in M \setminus f^{-1}(C) \\ x \in M \setminus f^{-1}(C) \Rightarrow x \in M \text{ und } x \notin f^{-1}(C) \Rightarrow x \in M \text{ und } f(x) \notin C \\ \Rightarrow f(x) \in N \setminus f^{-1}(C) \end{gathered}$$

Beispiel zu (b):

$$\begin{gathered} f : \mathbb{R} \to \mathbb{R}, f(x) = x^2 \\ A = \{x \in \mathbb{R} \mid x < 0\}, B = \{x \in \mathbb{R} \mid x > 0\} \\ \Rightarrow A \cap B = \emptyset, \text{ aber } f(A) = f(B) = \{x \in \mathbb{R} \mid x > 0\} (=: \mathbb{R}_{>0}) \\ \text{d.h. } f(A) \cap f(B) = \mathbb{R}_{>0} \neq \emptyset. \end{gathered}$$

(1.21) Def.: Ist $f : M \to N$ Abbildung und $A \subseteq M$, so ist die <u>Einschränkung</u> (Restriktion) $f|A (= f|_A) : A \to N$ <u>von</u> f <u>auf</u> A definiert durch: Für alle $x \in A$ ist $(f|A)(x) = f(x)$.

Bemerkung: Bezeichnet $i : A \to M$ die Inklusion, so gilt $f|A = f \circ i$

(1.22) Fakt: Ist $f : M \to N$ bijektive Abbildung, so existiert genau eine Abbildung $f^{-1} : N \to M$, so daß $f^{-1} \circ f = \mathrm{id}_M$ gilt. Für diese Abbildung f^{-1} gilt auch $f \circ f^{-1} = \mathrm{id}_N$.

Vorsicht: Das Symbol f^{-1} wird in unterschiedlichen Bedeutungen verwendet!

Bew.: f bijektiv $\Leftrightarrow \forall y \in N$ ex. genau ein $x \in M : f(x) = y$.

Eindeutigkeit von f^{-1}: Gilt $f(x) = y$, so muß $\begin{aligned} f^{-1}(y) &= f^{-1}(f(x)) = (f^{-1} \circ f)(x) \\ &= \mathrm{id}_M(x) = x \text{ gelten.} \end{aligned}$

Definiere $f^{-1} : N \to M$ durch $f^{-1}(y) = x \Leftrightarrow y = f(x)$

(1.23) Def.: Seien M, N Mengen. Eine <u>Relation auf</u> (M, N) ist eine Teilmenge von $M \times N$. (Ist $M = N$, so spricht man von einer Relation auf M)

Schreibweise: Sei $R \subseteq M \times N$. Statt $(x, y) \in R$ schreibt man auch xRy.

Beispiele:

1) $\Delta_M = \{(x, x) \mid x \in M\}$ die <u>Diagonale</u> in $M \times M$.
2) Sei $f : M \to N$ Abbildung. Dann ist der <u>Graph von</u> f,
$$\text{graph } (f) := \{(x, f(x)) \mid x \in M\}$$
eine Relation auf (M, N). Bem.: $\Delta_M = \text{graph } (\mathrm{id}_M)$
3) Sei $M = N = \mathbb{R}$ und $R := \{(x, y) \in \mathbb{R}^2 \mid x = y^2\}$. Diese Relation ist nicht Graph einer Funktion $f : \mathbb{R} \to \mathbb{R}$.

(1.24) Def. Sei M Menge, $R \subseteq M \times M$ Relation auf M. Dann heißt

(a) R reflexiv $\Leftrightarrow \forall x \in M : xRx \quad (\Leftrightarrow \Delta_M \subseteq R)$
(b) R symmetrisch $\Leftrightarrow (\forall x, y \in M : xRy \Leftrightarrow yRx)$

(c) R transitiv $\Leftrightarrow (\forall x, y, z \in M : xRy$ und $yRz \Rightarrow xRz)$
(d) R Äquivalenzrelation $\Leftrightarrow R$ ist reflexiv, symmetrisch und transitiv

Bei Äquivalenzrelationen R schreibt man oft statt xRy: $x \sim_R y$ oder kurz $x \sim y$ (wenn klar ist, welches R gemeint ist).

Beispiele:

1) Auf $M = \mathbb{R}$ kennen wir die Relation "kleiner gleich", d.h.

$$R = \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$$

R ist reflexiv und transitiv, aber nicht symmetrisch. (Beweis?)

2) Sei $M = \mathbb{Z}$, $p \geq 2$ feste natürliche Zahl.

$$R := \{(m, n) \in \mathbb{Z}^2 \mid n - m \text{ ist durch } p \text{ teilbar}\}.$$

Wir zeigen: R ist eine Äquivalenzrelation

(a) $\forall m \in \mathbb{Z}$: $m \sim_R m$, da $m - m = 0$ durch p teilbar: $0 = 0 \cdot p$
(b) Es gelte $m \sim_R n \quad \Rightarrow \quad n - m$ durch p teilbar $\Rightarrow m - n$ durch p teilbar
$\Rightarrow \quad n \sim_R m$
(c) Es gelte $k \sim_R m$ und $m \sim_R n \Rightarrow \exists j \in \mathbb{Z}, l \in \mathbb{Z} : m - k = jp, n - m = lp$
$\Rightarrow n - k = (l + j)p$ und $l + j \in \mathbb{Z} \Rightarrow k \sim_R n$.

Langes Beispiel: Eine <u>Zerlegung</u> $\mathcal{M}$ <u>einer Menge</u> M, ist eine Menge $\mathcal{M}$, deren Elemente Teilmengen von M sind, so daß gilt:

(1) $A \in \mathcal{M}$, $B \in \mathcal{M} \Rightarrow A = B$ oder $A \cap B = \emptyset$.
(2) $\bigcup\limits_{A \in \mathcal{M}} A = M$. (wobei $\bigcup\limits_{A \in \mathcal{M}} A := \{x \mid \exists A \in \mathcal{M} : x \in A\}$)

Wir werden sehen, daß eine Äquivalenzrelation auf M im Grunde das gleiche ist, wie eine Zerlegung von M. Zunächst überlegen wir, wie wir aus einer Zerlegung eine Äquivalenzrelation erhalten: Zu einer Zerlegung $\mathcal{M}$ von M definieren wir die Relation

$$R = \{(x, y) \in M \times M \mid \exists A \in \mathcal{M} : \{x, y\} \subseteq A\}$$

Wir zeigen: R ist eine Äquivalenzrelation.

(a) Sei $x \in M$. Wir wollen zeigen, daß $(x, x) \in R$ gilt. Wegen (2) existiert ein $A \in \mathcal{M}$, so daß $x \in A$ gilt. Also gilt $\{x, x\}(= \{x\}) \subseteq A$, d.h. $(x, x) \in R$.
(b) $\{x, y\} \subseteq A \Leftrightarrow \{y, x\} \subseteq A$
(c) Es gelte $(x, y) \in R$ und $(y, z) \in R \Rightarrow \exists A \in \mathcal{M}$, $B \in \mathcal{M}$ mit $\{x, y\} \subseteq A$, $\{y, z\} \subseteq B$
$\Rightarrow y \in A \cap B$, d.h. $A \cap B \neq \emptyset \overset{(1)}{\Rightarrow} A = B \Rightarrow \{x, z\} \in A \Rightarrow (x, z) \in R$.

Bezeichnung: Sei $R \subseteq M \times M$ eine Äquivalenzrelation und $x \in M$. Dann heißt

$$\begin{aligned} [x]_R &:= \{y \in M \mid (x,y) \in R\} \text{ die Äquivalenzklasse von } x \text{ und} \\ M/R &:= \{[x]_R \mid x \in M\} \text{ die Menge der Äquivalenzklassen, die auch "}M \text{ modulo } R\text{"} \\ &\quad \text{genannt wird.} \end{aligned}$$

(1.25) Fakt: Sei $R \subseteq M \times M$ eine Äquivalenzrelation. Dann ist M/R eine Zerlegung von M.

Beweis: Offensichtlich ist jedes Element von M/R eine Teilmenge von M (nämlich eine Äquivalenzklasse). Wir zeigen, daß die Menge M/R die Eigenschaften (1) und (2) hat.

Zu (2): Offensichtlich gilt $\bigcup_{[x]_R \in M/R} [x]_R \subseteq M$. Sei umgekehrt $x \in M$. Die Reflexivität (a) von R besagt, daß $(x,x) \in R$ gilt, also $x \in [x]_R$. Damit $M \subseteq \bigcup_{[x]_R \in M/R} [x]_R$.

Zu (1): Wir zeigen, daß folgende Aussagen $(\alpha), (\beta), (\gamma)$ über Elemente $x \in M, y \in M$ äquivalent sind:

(α) $[x]_R \cap [y]_R \neq \emptyset$
(β) $x \sim y$
(γ) $[x]_R = [y]_R$

1. Schritt: $(\alpha) \Rightarrow (\beta)$: Sei $z \in [x]_R \cap [y]_R$, d.h. es gelten $x \sim z$ und $y \sim z$. Die Symmetrie und Transitivität von $\sim$ implizieren dann $x \sim y$.
2. Schritt: $(\beta) \Rightarrow (\gamma)$: Wegen der Symmetrie der Voraussetzung $x \sim y$ genügt es, $[y]_R \subseteq [x]_R$ zu zeigen. Sei $w \in [y]_R$, d.h. $y \sim w$. Unsere Voraussetzung $x \sim y$ ergibt zusammen mit $y \sim w$ und der Transitivität, daß $x \sim w$ gilt, d.h. $w \in [x]_R$.
3. Schritt: $(\gamma) \Rightarrow (\alpha)$: Wegen $x \in [x]_R$ folgt aus $[x]_R = [y]_R$, daß $[x]_R \cap [y]_R = [x]_R \neq \emptyset$ gilt.

Sind nun A und B Elemente von M/R, etwa $A = [x]_R$ und $B = [y]_R$ für Elemente x, y von M, so gilt wegen $(\alpha) \Leftrightarrow (\beta)$ entweder $A \cap B = \emptyset$ oder $A = B$. Das beweist (1).

Beispiel: Es sei nun wieder $p \in \mathbb{N}, p \geq 2$ und wir betrachten die Äquivalenzrelation auf $\mathbb{Z}$, die durch

$$m \sim n \Leftrightarrow n - m \text{ ist durch } p \text{ teilbar}$$

definiert ist, vgl. Bsp. 2 nach (1.24). Dann sind die Äquivalenzklassen von $\sim$ genau die Teilmengen von $\mathbb{Z}$, die aus den ganzen Zahlen bestehen, die bei Division (mit Rest) durch p, den gleichen Rest ergeben. Sie heißen deshalb auch die "Restklassen mod p". Es gibt genau p verschiedene solche Restklassen mod p, nämlich

$$\begin{array}{lcll} [0]_p & = & \{np \mid n \in \mathbb{Z}\} & \text{Rest 0 bei Division durch } p \\ [1]_p & = & \{np+1 \mid n \in \mathbb{Z}\} & \text{Rest 1 bei Division durch } p \\ & \vdots & & \\ [p-1]_p & = & \{np+(p-1) \mid n \in \mathbb{Z}\} & \text{Rest } p-1 \text{ bei Division durch } p \\ & = & \{np-1 \mid n \in \mathbb{Z}\} & \end{array}$$

Für diese Äquivalenzrelation ist folgende Bezeichnung gebräuchlich:

$$m \sim n \Leftrightarrow m \equiv n \pmod{p}$$