Skript LAAG

Stefan E. Schmidt

LaTeX: Maximilian Marx
Jens Zumbrägel

TU Dresden
Wintersemester 2013/14

Version vom 26.07.2014

Inhaltsverzeichnis

„Wenn Leute nicht glauben, dass Mathematik einfach ist, dann nur deshalb, weil sie nicht begreifen, wie kompliziert das Leben ist.“

(– John von Neumann)

0 Grundlegende Bemerkungen

Wir unterscheiden

Axiome, unbewiesene Grundaussagen in einem „strengen Setup“,

Postulate, unbewiesene Aussagen, von denen man in einer bestimmten Situation („Kontext“) ausgeht,

Definitionen, exakte Begriffsfindungen, die helfen, eine exakte Sprache zu entwickeln (Präzisierung, Makrobildung),

Theoreme, Aussagen, die in einem Kontext beweisbar sind (besitzen Beweise),

Propositionen, kleinere, (oft aus Axiomen) abgeleitete Aussagen, und

Hypothesen, unbewiesene Vermutungen.

Mittels *Abduktion* stellen wir Hypothesen und Axiome auf. Ausgehend von Hypothesen und Axiomen finden wir mittels *Deduktion* zu Theoremen, und ausgehend von Beispielen und Modellen gelangen wir über *Induktion* zu Theoremen.

Ein berühmtes Postulat im Kontext des Anschauungsraums ist das *euklidische Parallelen-Postulat*: Zu jedem Punkt p und jeder Gerade h, die nicht durch p verläuft, gibt es eine zu h parallele Gerade durch p. Erst im 19. Jahrhundert wurde gezeigt, dass das Parallelen-Postulat nicht für die offene Kreisscheibe gilt (ein Modell für die hyperbolische Geometrie).

Für zwei Aussagen A und B sind unter anderem folgende Fragen interessant:

A **wahr?** Ist die Aussage A wahr?

$\mathrm{A} \Rightarrow \mathrm{B}$ **wahr?** Ist „A impliziert B“ (aus A folgt B) wahr?

$\mathrm{A} \Leftrightarrow \mathrm{B}$ **wahr?** Ist „A ist gleichbedeutend mit B“ wahr?

Es gilt: Ist A wahr, und $\mathrm{A} \Rightarrow \mathrm{B}$ wahr, so ist B wahr. Uninteressant (aber richtig): Ist A unwahr, dann ist $\mathrm{A} \Rightarrow \mathrm{B}$ wahr.

Ist B unwahr, und $\mathrm{A} \Rightarrow \mathrm{B}$ auch unwahr. Dann kann A dennoch wahr sein.

0.1 Theorem
Seien A *und* B *zwei Aussagen,* B *unwahr, und* $\mathrm{A} \Rightarrow \mathrm{B}$ *wahr. Dann ist* A *unwahr.* □

Beweis
Angenommen, A ist wahr. Dann folgt aus $\mathrm{A} \Rightarrow \mathrm{B}$ ist wahr bereits, dass B wahr ist. ■

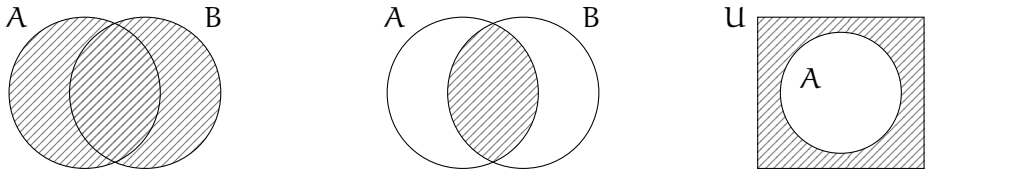
1 Mengen und Abbildungen

1.1 Mengen und Aussagenlogik

1.1 Definition (Menge, Georg Cantor, 19. Jahrhundert)
Eine *Menge* (engl. "Set") ist eine ungeordnete Zusammenfassung von wohlunterschiedenen Objekten (unseres Denkens) zu einem Ganzen. □

Aussagenlogische Seite: Moderne Aussagenlogik begründet durch Gottlob Frege (Jena, 19. Jahrhundert). Notation:

$\forall$	„für alle“	$\subseteq$	„ist Teilmenge von“
$\exists$	„es gibt“	$\wedge$	„und“
$\mid$	„so dass“, „mit“	$\vee$	„oder“
$\{\}$	„Menge“	$\neg$	„nicht“
$\in$	„Element von“	$:=$	„definiert als“



Vereinigungsmenge $A \cup B$ Schnittmenge $A \cap B$ Komplementmenge $A^c = U \setminus A$

Illustration von Mengenkonstruktionen mittels *Venn-Diagrammen*

1.2 Definition (Vereinigungsmenge)
Seien A und B Mengen. Dann ist

$$A \cup B := \{x \mid x \in A \vee x \in B\},$$

die *Vereinigungsmenge* von A und B, die Menge aller Elemente x mit der Eigenschaft, dass x Element von A oder x Element von B ist. □

1.3 Definition (Schnittmenge)
Seien A und B Mengen. Dann ist

$$A \cap B := \{x \mid x \in A \wedge x \in B\},$$

die *Schnittmenge* von A und B, die Menge aller Elemente x mit der Eigenschaft, dass x Element von A und x Element von B ist. □

1.4 Definition (Komplementmenge)
Sei $A \subseteq U$ Menge. Dann ist

$$A^c := U \setminus A := \{x \mid x \notin A\},$$

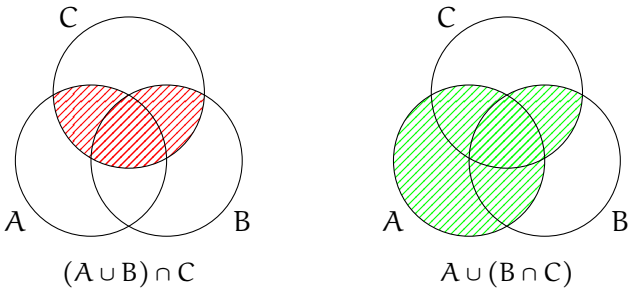
das *Komplement* von A in U, die Menge mit der Eigenschaft, dass x kein Element von A ist. □

Ist $\mathcal{M}$ Menge von Mengen, so ist

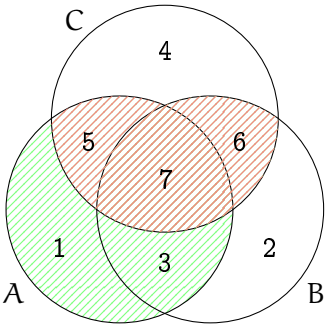
$$\bigcap \mathcal{M} := \{x \mid \forall A \in \mathcal{M} : x \in A\}$$
$$\bigcup \mathcal{M} := \{x \mid \exists A \in \mathcal{M} : x \in A\}$$

Es gilt nicht:

$$(A \cup B) \cap C \stackrel{?}{=} A \cup (B \cap C)$$



Wir konstruieren ein Gegenbeispiel:



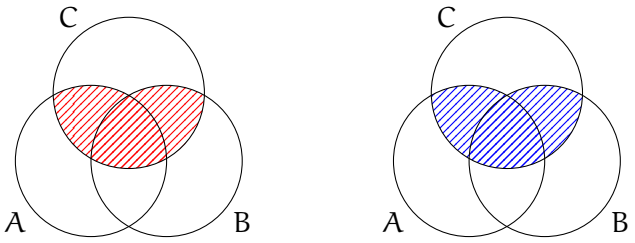
Mit $A = \{1, 3, 5, 7\}$, $B = \{2, 3, 6, 7\}$ und $C = \{4, 5, 6, 7\}$ ist

$$(A \cup B) \cap C = \{5, 6, 7\}, \quad \text{aber} \quad A \cup (B \cap C) = \{1, 3, 5, 6, 7\}.$$

Offenbar klappt also das Umklammern bei gemischten Ausdrücken mit $\cup$ und $\cap$ nicht. Klappt denn wenigstens Distributivität?

$$(A \cup B) \cap C \stackrel{?}{=} (A \cap C) \cup (B \cap C)$$

In unserem Beispiel gilt $A \cap C = \{5, 7\}$, $B \cap C = \{6, 7\}$ und $(A \cap C) \cup (B \cap C) = \{5, 6, 7\}$, sowie auch $(A \cup B) \cap C = \{5, 6, 7\}$. Dies legt nahe, dass die Aussage tatsächlich gilt, aber wie beweisen wir das?



$(A \cup B) \cap C$ $(A \cap C) \cup (B \cap C)$

Sieht gut aus, jetzt wollen wir es wirklich zeigen. Dazu müssen wir erstmal klären, was Gleichheit von Mengen eigentlich ist.

1.5 Definition (Teilmengenrelation)
Seien A, B Mengen. Dann schreiben wir $A \subseteq B$ und sagen „A ist enthalten in B“, wenn

$$\forall x \in A : \ x \in B$$

gilt, das heißt wenn jedes Element x von A auch ein Element von B ist. □

Eine äquivalente Formulierung ist

$$A \subseteq B \quad \Leftrightarrow \quad \forall x : x \in A \Rightarrow x \in B.$$

1.6 Definition (Gleichheit von Mengen)
Sind A und B Mengen, so ist $A = B$ genau dann, wenn

$$A \subseteq B \ \wedge \ B \subseteq A$$

gilt, das heißt wenn

$$\forall x : x \in A \Leftrightarrow x \in B$$

gilt, also genau dann, wenn für jedes x stets x genau dann ein Element von A ist, wenn x ein Element von B ist. □

1.7 Beispiel

1. Sei $A = \{\text{Ball}, \text{Schläger}\}$, und $B = \{\text{Ball}, \text{Würfel}, \text{Schläger}\}$. Dann ist $A \subseteq B$.
2. Sei $A = \{1, 1, 2, 3\}$, und $B = \{1, 2, 3, 2, 3\}$. Dann ist $A = B$. □

Nun zeigen wir das Distributivgesetz für $\cup$ and $\cap$.

Beweis
Wir zeigen

$$(A \cup B) \cap C \ = \ (A \cap C) \cup (B \cap C).$$

Dazu zeigen wir zunächst

$$(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C).$$

Sei $x \in (A \cup B) \cap C$. Dann gilt:

$$\begin{aligned}
& x \in A \cup B \ \wedge \ x \in C \\
\Rightarrow \ & (x \in A \vee x \in B) \wedge x \in C \\
\underline{\Rightarrow} \ & (x \in A \wedge x \in C) \vee (x \in B \wedge x \in C) \\
\Rightarrow \ & x \in A \cap C \ \vee \ x \in B \cap C \\
\Rightarrow \ & x \in (A \cap C) \cup (B \cap C).
\end{aligned}$$

An der Stelle „$\underline{\Rightarrow}$“ haben wir eine Regel der elementaren Aussagenlogik benutzt: Sind p, q, r Aussagen, so gilt $(p \vee q) \wedge r \ \Rightarrow \ (p \wedge r) \vee (q \wedge r)$.

Sei jetzt umgekehrt $x \in (A \cap C) \cup (B \cap C)$. Dann gilt:

$$\begin{aligned}
& x \in A \cap C \ \vee \ x \in B \cap C \\
\Rightarrow \ & (x \in A \wedge x \in C) \vee (x \in B \wedge x \in C) \\
\underline{\Rightarrow} \ & (x \in A \vee x \in B) \wedge x \in C \\
\Rightarrow \ & x \in A \cup B \ \wedge \ x \in C \\
\Rightarrow \ & x \in (A \cup B) \cap C.
\end{aligned}$$

An der Stelle „$\underline{\Rightarrow}$“ haben wir wieder eine Regel der Aussagenlogik benutzt, nämlich $(p \wedge r) \vee (q \wedge r) \ \Rightarrow \ (p \vee q) \wedge r$.

Logisch exakter aufgeschrieben:

$$\begin{aligned}
\forall x : \big(x \in (A \cup B) \cap C \ & \Leftrightarrow \ x \in A \cup B \ \wedge \ x \in C \\
& \Leftrightarrow \ (x \in A \vee x \in B) \wedge x \in C \\
& \underline{\Leftrightarrow} \ (x \in A \wedge x \in C) \vee (x \in B \wedge x \in C) \\
& \Leftrightarrow \ x \in A \cap C \ \vee \ x \in B \cap C \\
& \Leftrightarrow \ x \in (A \cap C) \cup (B \cap C) \big)
\end{aligned}$$

■

1.8 Definition (Leere Menge)
Die *leere Menge* ist eine Menge, die kein Element enthält. □

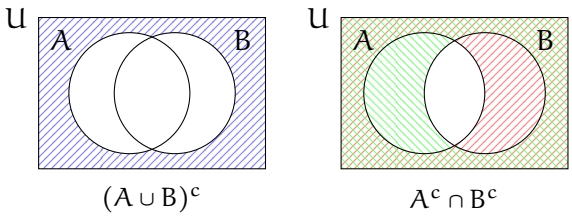
1.9 Axiom (Existenz der leeren Menge)
Die leere Menge existiert, und wird mit $\varnothing =: \{\}$ bezeichnet. □

Seien A und B Mengen. Dann ist $A \setminus B := \{x \mid x \in A \wedge x \notin B\}$, die *Differenzmenge* von A und B, die Menge aller Elemente x mit der Eigenschaft, dass x Element von A und x kein Element von B ist.

1.10 Proposition (Weitere Rechenregeln für Mengen)
Sei U eine Menge, und seien $A, B, C \subseteq U$. Dann gilt:

1. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$
2. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
3. $A \cup B = B \cup A$ und $A \cap B = B \cap A$
4. $\varnothing \cup A = A = A \cup \varnothing$
5. $(A \cup B)^c = A^c \cap B^c$
6. $(A \cap B)^c = A^c \cup B^c$
7. $(A^c)^c = A$
8. $A \cup B = (A^c \cap B^c)^c$
9. $A \cap B = (A^c \cup B^c)^c$
10. $\varnothing^c = U$
11. $\varnothing \cap A = \varnothing$
12. $A \subseteq B \Leftrightarrow A \cup B = B$
13. $A \setminus B = A \cap B^c$
14. Zerlegung von U in acht Teile.
    $U = (A \cap B \cap C) \cup (A \cap B \cap C^c) \cup (A \cap B^c \cap C) \cup (A^c \cap B \cap C) \cup (A \cap B^c \cap C^c) \cup (A^c \cap B \cap C^c) \cup (A^c \cap B^c \cap C) \cup (A^c \cap B^c \cap C^c)$
15. $(A \setminus B) \cup (B \setminus C) \cup (C \setminus A) = (B \setminus A) \cup (C \setminus B) \cup (A \setminus C)$ □

5. und 6. sind die *De Morganschen Regeln*.



$(A \cup B)^c$ $A^c \cap B^c$

Illustration von Regel 5.

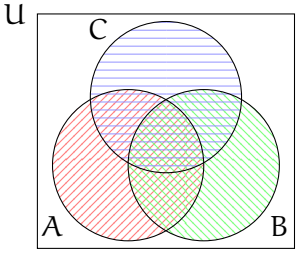


Illustration von Regel 14.

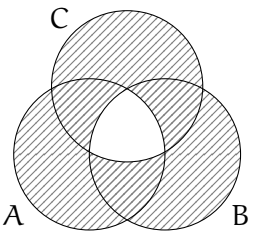


Illustration von Regel 15.

1.11 Proposition
Sei U Menge und seien $A, B \subseteq U$. Dann gilt:

1. $A \subseteq B \Leftrightarrow A \cap B^c = \varnothing$
2. $A \subseteq B^c \Leftrightarrow B \subseteq A^c$ □

$A \subseteq B$ $\qquad$ $A \cap B = \varnothing$

Spezielle Situationen (Prop. 1.11)

Beweis

1. $A \subseteq B \Leftrightarrow \forall x : x \in A \Rightarrow x \in B \Leftrightarrow \nexists x : x \in A \wedge x \notin B$
   $\Leftrightarrow \nexists x : x \in A \wedge x \in B^c \Leftrightarrow \nexists x : x \in A \cap B^c \Leftrightarrow A \cap B^c = \varnothing$

2. Es gilt $A \subseteq B^c \Leftrightarrow A \cap B = \varnothing$ ("missing link") $\Leftrightarrow B \subseteq A^c$, denn:

$$\begin{aligned} A \subseteq B^c &\Leftrightarrow \forall x : x \in A \Rightarrow x \in B^c \\ &\Leftrightarrow \nexists x : x \in A \wedge x \notin B^c \\ &\Leftrightarrow \nexists x : x \in A \wedge x \in B \quad (\text{denn } \forall x \in U : x \in B \Leftrightarrow x \notin B^c) \\ &\Leftrightarrow A \cap B = \varnothing. \end{aligned}$$

■

1.12 Postulat
Ist A Menge, so ist der „Container" aller Teilmengen von A ebenfalls eine Menge, die sogenannte *Potenzmenge* von A, die wir mit 2^A (auch $\mathfrak{P}(A)$) bezeichnen. □

Es ist $2^A := \{B \mid B \subseteq A\}$. Wegen $A \subseteq A$ folgt stets $A \in 2^A$ und $\varnothing \in 2^A$.

1.13 Postulat
Ist A Menge, so gilt $A \notin A$. □

1.14 Warnung (Russel)
Der „Container" aller Mengen ist selbst keine Menge. Denn wäre der „Container" $\mathcal{C}$ aller Mengen eine Menge, so würde $\mathcal{C} \in \mathcal{C}$ gelten. Dies ist ein Widerspruch zu unserem Postulat. □

1.15 Definition (Endliche Menge)
Eine Menge ist *endlich*, wenn sie nur endlich viele Elemente besitzt (zunächst „wackelige" Definition). Ist n die Anzahl der Elemente einer endlichen Menge X, so schreiben wir $\#X = n$, oder auch $|X| = n$, und sagen, dass X eine n-elementige Menge ist. □

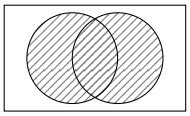
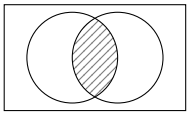
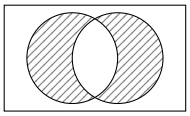
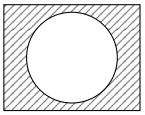
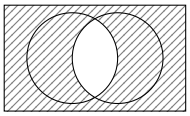
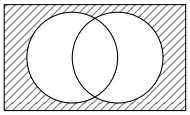
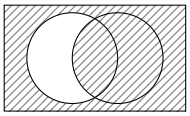
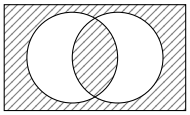
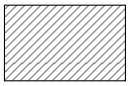
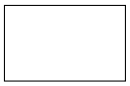
1.16 Beispiel
Ist $n \in \mathbb{N}$ und ist A eine n-elementige Menge, so gilt

$$\#(2^A) = 2^{\#A}.$$

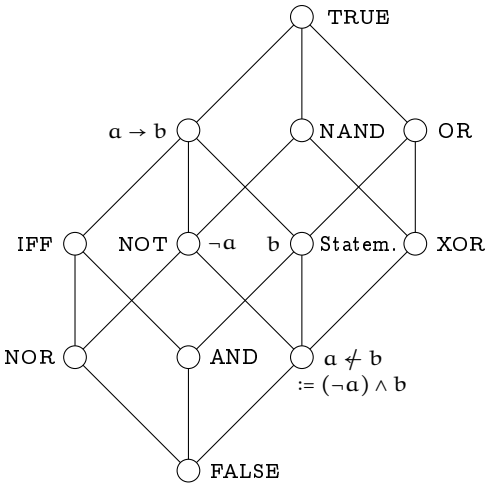
□

1.17 Bemerkung
Die Menge $2^{\mathbb{N}}$ ist unglaublich groß, und sogar echt größer als $\mathbb{N}$. Tatsächlich ist für jede Menge A stets 2^A echt größer als A. □

Mehr zu Aussagen Zentrale Symbole für syntaktische/formale Aussagen „mit Bild“.

$\vee$	OR	oder, Diskunktion	$a \vee b$	
$\wedge$	AND	und, Konjunktion	$a \wedge b$	
$\oplus := \dot{\vee}$	XOR	entweder-oder	$a \dot{\vee} b := (a \vee b) \wedge \neg(a \wedge b)$	
$\neg$	NOT	nicht, Negation	$\neg a$	
$\uparrow$	NAND	“Sheffer Stroke”	$a \uparrow b := \neg(a \wedge b)$	
$\downarrow$	NOR		$a \downarrow b := \neg(a \vee b)$	
$\rightarrow, \Rightarrow$	IF-THEN	Implikation	$(a \rightarrow b) := (\neg a) \vee b$	
$\leftrightarrow, \Leftrightarrow$	IFF	logische Äquivalenz	$(a \leftrightarrow b) := (a \wedge b) \vee \neg(a \vee b)$	
$\top, \mathcal{T}$	TRUE	Tautologie		
$\bot, \mathcal{F}$	FALSE	Widerspruch		

Übung: NXOR := NOT XOR = IFF



Hierarchisches Diagramm

Eine Menge hat oft die Form $S := \{s \mid s \text{ hat Eigenschaft } E\}$, wobei E eine bestimmte Eigenschaft ist. Zum Beispiel ist $B := \{x \mid x \text{ ist Säugetier}\}$ eine Menge. Besser ist es jedoch, eine Menge U von Dingen (beziehungsweise Lebewesen) vorzugeben. Dann ist $\{x \in U \mid x \text{ ist Säugetier}\}$ eine Menge. Eine solche Menge U wird *Universum* oder *Kontext* genannt.

1.18 Bemerkung (Quantoren)
Quantoren helfen dabei, mathematische Aussagen kompakt aufzuschreiben. Sie erlauben es, aus einer Aussage über ein konkretes Objekt eine Aussage über die Beschaffenheit jener Objekte, für die diese Aussage wahr ist, zu konstruieren. Die wichtigsten sind der

Existenzquantor $\exists$, der die Aussage „es gibt ein Objekt, dass diese Aussage erfüllt“ konstruiert, und der

Allquantor $\forall$, der die Aussage „jedes Objekt erfüllt diese Aussage“ konstruiert. □

1.19 Beispiel (Quantoren)
Seien $A := \{\text{Ball}, \text{Auto}, \text{Stift}\}$, $B := \{x \in U \mid x \text{ ist Säugetier}\}$. Dann gilt:

- $\forall a \in A: \ a \notin B$
  gelesen als: Für jedes Element a aus der Menge A gilt: a ist kein Element aus der Menge B.
- $\exists a \in A: \ a$ hat „Räder“
  gelesen als: Es gibt ein Element a aus A, für das gilt: a hat Räder.
- $\exists b \in B \ \forall a \in A: \ b$ besitzt a
  gelesen als: Es gibt ein Element b aus B, für das gilt: Für jedes Element a aus A gilt: Das Element b besitzt das Element a.
- $\forall a \in A \ \exists b \in B: \ b$ besitzt a
  gelesen als: Für alle Elemente a in A gilt: Es gibt ein Element b aus B, für das gilt: Das Element b besitzt das Element a. □

1.2 Abbildungen

Abbildungen begegnen uns z. B. bei Daten-Tabellen („Buchhalter“):

	Fläche (Tsd. km^2)	Bevölkerung (# in Mill.)	Bevölk.-dichte (#/km^2)
Deutschland	357	80	224
Ägypten	1000	84	84
Israel	22	8	364
Jordanien	89	6	67
Libanon	10	5	500
Syrien	186	22,5	121
Irak	438	31	71
Iran	1648	77	47

1.20 Definition (Abbildung)
Eine *Abbildung* ("map") f besteht aus zwei Mengen X und Y und einer Abbildungsvorschrift, die jedem Element $x \in X$ genau ein Element $y \in Y$ zuordnet. Wir schreiben dafür $x \overset{f}{\mapsto} y$.

Die Menge X heißt *Definitionsbereich* („Ausgangsmenge", "domain") und die Menge Y heißt *Wertebereich* („Zielmenge", "codomain"). Demgemäß schreiben wir für f auch $f : X \to Y$, $x \overset{f}{\mapsto} y$ beziehungsweise $f : X \to Y$, $x \mapsto fx$, oder einfach $f : X \to Y$, und sagen „Abbildung von X nach Y". Andere Schreibweisen für $x \overset{f}{\mapsto} y$ sind

- $f(x) := fx := y$ (wir sagen „f von x"), oder
- $xf := y$ bzw. $x^f := y$ (wir sagen „x unter f"). □

Auch üblich sind die Schreibweisen $X \overset{f}{\to} Y$, $x \mapsto fx$ und $X \overset{f}{\to} Y$ (bei Diagrammen). Man schreibt auch $f : \operatorname{dom} f \to \operatorname{cod} f$, $x \overset{f}{\mapsto} y$.

1.21 Beispiel
Wir betrachten folgende Mengen:

positive natürliche Zahlen $\mathbb{N}_+ := \{1, 2, 3, \dots\}$,

natürliche Zahlen $\mathbb{N} := \{0, 1, 2, \dots\}$,

ganze Zahlen $\mathbb{Z} := \{\dots, -2, -1, 0, 1, 2, \dots\}$,

rationale Zahlen $\mathbb{Q} := \left\{\frac{z}{n} \mid z \in \mathbb{Z} \wedge n \in \mathbb{N}_+\right\}$, und

reelle Zahlen $\mathbb{R}$.

Beispiele für Abbildungen sind

1. $f : \mathbb{N} \to \mathbb{N},\ n \mapsto 2n$,
2. $g : \mathbb{Z} \to \mathbb{Z},\ z \mapsto z^3$, und
3. $h : \mathbb{Q} \to \mathbb{Q},\ q \mapsto q^2$. □

1.22 Bemerkung
Sei $f : X \to Y$ eine Abbildung. Ist $D \subseteq X$, so heißt

$$fD := f[D] := \{fx \mid x \in D\} := \{y \in Y \mid \exists x \in D : fx = y\}$$

das *Bild* von D unter f. Wir nennen $\operatorname{Im} f := f[X]$ das *Bild* ("Image") von f.

Für $C \subseteq Y$ sei

$$f^{-1}C := f^{-1}[C] := \{x \in X \mid fx \in C\} = \{x \in X \mid \exists y \in C : fx = y\}$$

die *Urbildmenge* von C unter f. □

1.23 Definition (Injektivität, Surjektivität, Bijektivität)
Eine Abbildung $f : X \to Y$ heißt

injektiv, falls für $x_1, x_2 \in X$ stets $fx_1 = fx_2 \Rightarrow x_1 = x_2$ gilt,

surjektiv, falls $fX = Y$ gilt, und

bijektiv, falls f injektiv und surjektiv ist. □

Für formale Beweise ist folgendes „nützlich“: Seien X und Y Mengen. Dann ist $f : X \to Y$, $x \mapsto fx$ eine Abbildung, falls gilt:

f **wohldefiniert:** $\forall x_1, x_2 : (x_1 = x_2 \Rightarrow fx_1 = fx_2)$ („f ist rechtseindeutig“), und

f **linkstotal:** $\forall x \in X \; \exists y \in Y : fx = y$.

Ist f nur wohldefiniert, aber nicht linkstotal, so heißt f *partielle Abbildung.*
Weiter gilt:

f **injektiv:** $\forall x_1, x_2 \in X : (fx_1 = fx_2 \Rightarrow x_1 = x_2)$ („f ist linkseindeutig“),

f **surjektiv:** $\forall y \in Y \; \exists x \in X : fx = y$ („f ist rechtstotal“),

und f heißt bijektiv, falls f injektiv und surjektiv ist. Eine injektive Abbildung nennen wir auch *Injektion*, eine surjektive Abbildung auch *Surjektion* und eine bijektive Abbildung auch *Bijektion.*

Kombinatorische Fragen:

1. Wie viele Abbildungen gibt es von $\{1, 2, 3, 4, 5\}$ nach $\{a, b, c, d\}$?
2. Wie viele Permutationen hat $\{1, 2, 3, 4, 5\}$?

Idee: Wo kann die 1 hin abgebildet werden? $1 \mapsto a$, $1 \mapsto b$, $1 \mapsto c$, und $1 \mapsto d$ sind möglich. Unabhängig davon kann die 2 ebenfalls auf jedes der Elemente aus B abgebildet werden. Entsprechendes gilt für jedes Element aus A.
Insgesamt gilt: $\#B^A := 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 = 4^5 = \#B^{\#A}$.

1.24 Definition
Seien A, B Mengen. Die Menge aller Abbildungen von A nach B sei mit B^A bezeichnet. □

1.25 Proposition
Sind A, B endliche Mengen, so gilt:

$$\#\left(B^A\right) = \#B^{\#A}.$$ □

1.26 Definition
Ist $f : X \to X$ eine Bijektion, so heißt f *Permutation.* Mit $\mathrm{Bij}(X, X) =: \mathrm{Perm}\, X =: \mathrm{Sym}\, x$ bezeichnen wir die Menge aller Bijektionen von X nach X. Speziell sei $\Sigma_n := \mathrm{Sym}_n := \mathrm{Perm}\,\{1, \ldots, n\}$. □

Zurück zur Frage: $\#\,\mathrm{Sym}_5 = \#\,\mathrm{Perm}\,\{1, 2, 3, 4, 5\} = ?$
„Sehen, wie der Hase läuft.“ Bestimme $\#\,\mathrm{Sym}_n$ für $n = 1, 2, \ldots$.
Für $n = 1$ geht nur $1 \mapsto 1$, also $\#\,\mathrm{Sym}_1 = 1$.

Für $n = 2$ gibt es $\begin{smallmatrix}1&2\\1&2\end{smallmatrix}$ und $\begin{smallmatrix}1&2\\2&1\end{smallmatrix}$, also $\#\operatorname{Sym}_2 = 2 = 1 \cdot 2$.

Für $n = 3$ haben wir $\begin{smallmatrix}1&2&3\\1&2&\underline{3}\end{smallmatrix}$, $\begin{smallmatrix}1&2&3\\1&\underline{3}&2\end{smallmatrix}$, $\begin{smallmatrix}1&2&3\\\underline{3}&1&2\end{smallmatrix}$, und $\begin{smallmatrix}1&2&3\\2&1&\underline{3}\end{smallmatrix}$, $\begin{smallmatrix}1&2&3\\2&\underline{3}&1\end{smallmatrix}$, $\begin{smallmatrix}1&2&3\\\underline{3}&2&1\end{smallmatrix}$, also $\#\operatorname{Sym}_3 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 6$.

Entsprechend findet man $\#\operatorname{Sym}_4 = 6 \cdot 4 = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Allgemein gilt $\#\operatorname{Sym}_n = n!$.

1.3 Inzidenzstrukturen

- Notation: Für $n \in \mathbb{N}_+ = \{1, 2, 3, \dots\}$ sei $[n] := \{1, 2, \dots, n\}$ (beliebte Notation in Ungarn, dem „Königreich“ der Kombinatorik und der diskreten Mathematik), und $\underline{n} := \{0, 1, \dots, n-1\}$.

- Paare, n-Tupel, kartesisches Produkt „naiv“: Ein Paar (a, b) ist geordnet, das heißt $(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$ (mögliche Mengenkonstruktion: $(a, b) := \{a, \{a, b\}\}$). Entsprechend für 3-Tupel (a, b, c) geordneter Elemente, das heißt $(a, b, c) = (a', b', c') \Leftrightarrow a = a' \wedge b = b' \wedge c = c'$. Allgemein ist für $n \in \mathbb{N}_+$ stets $(a_1, \dots, a_n)$ ein n-Tupel geordneter Elemente $a_1, a_2, \dots, a_n$. Auch hier ist $(a_1, \dots, a_n) = (b_1, \dots, b_n) \Leftrightarrow \forall i \in [n] : a_i = b_i$.

  Sind A, B Mengen, so heißt $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$ das *kartesische Produkt* von A mit B. Achtung: Falls $A \neq B$, $A \neq \varnothing$, $B \neq \varnothing$ gilt, so ist $A \times B \neq B \times A$.

  Entsprechend sei für Mengen $A_1, \dots, A_n$ auch $A_1 \times \cdots \times A_n := \{(a_1, \dots, a_n) \mid \forall i \in [n] : a_i \in A_i\}$ das kartesische Produkt. Wir definieren $A^2 := A \times A$, und $A^n := A \times \cdots \times A$ (n-mal) das n-fache kartesische Produkt von A.

  Übung: Ist A endliche Menge, so ist $\#(A^n) = (\#A)^n$.

Nun folgt ein erstes Konstruktionshighlight.

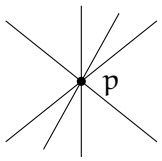
1.27 Definition (Inzidenzstruktur)
Ein Tripel $\mathcal{I} = (P, B, I)$ bestehend aus Mengen P, B, I mit $I \subseteq P \times B$ (das heißt „I ist binäre Relation auf (P, B)“) heißt *Inzidenzstruktur*. Wir nennen P Menge von *Punkten*, B Menge von *Blöcken* und I die *Inzidenzrelation*. □

Wir benutzen die Konvention und Sprechweise: $pIB :\Leftrightarrow (p, b) \in I$ („p inzidiert mit b“, oder lax: „p liegt auf b“) für alle $p \in P$ und alle $b \in B$. Entsprechend schreiben wir $p \not I b :\Leftrightarrow (p, b) \notin I$ („p inzidiert nicht mit b“, oder lax: „p liegt nicht auf b“).

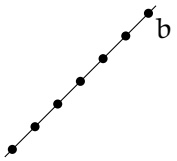
p liegt auf b p liegt nicht auf b

Sinn-Bilder

Ist $p \in P$, so ist $pI := \{b \in B \mid pIb\}$ die Menge aller Blöcke, die mit dem Punkt p inzidieren.
Ist $b \in B$, so ist $Ib := \{p \in P \mid pIb\}$ die Menge aller Punkte, die mit Block b inzidieren.



pI



Ib

Sinn-Bilder

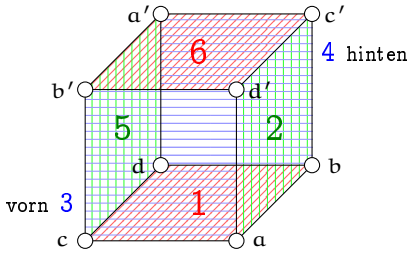
1.28 Beispiel (Formaler Kontext)
Business: FCA – "Formal Concept Analysis". Hier wird „Punkt" als „Gegenstand" interpretiert, „Block" wird interpretiert als „Merkmal", und „Inzidenz" wird interpretiert als „Gegenstand hat Merkmal".

Sei $\mathcal{I} = (P, B, I)$ Inzidenzstruktur (beziehungsweise „formaler Kontext") mit $P = \{\text{Ball}, \text{Kugel}, \text{Gummibär}\}$ und $B = \{\text{rund}, \text{elastisch}, \text{essbar}\}$. Darstellung der Inzidenzrelation I durch Kreuztabelle:

	rund	elastisch	essbar
Ball	×	×	·
Kugel	×	·	·
Gummibär	·	×	×

Offenbar gilt $\text{Ball}\,I\,\text{rund}$ und $\text{Gummibär}\,I\,\text{essbar}$. Es ist $\text{Ball}\,I = \{\text{rund}, \text{elastisch}\}$ und $I\,\text{rund} = \{\text{Ball}, \text{Kugel}\}$. □

1.29 Beispiel (Geometrisches Beispiel „Würfel")
Sei $\mathcal{I} = (P, B, I)$ mit $P = \{a, b, c, d, a', b', c', d'\}$ und $B = \{1, 2, 3, 6, 5, 4\}$ wie im Bild.



Wir erhalten als zugehörige Kreuztabelle:

	1	2	3	6	5	4
a	×	×	×	·	·	·
a'	·	·	·	×	×	×
b	×	×	·	·	·	×
b'	·	·	×	×	×	·
c	×	·	×	·	×	·
c'	·	×	·	×	·	×
d	×	·	·	·	×	×
d'	·	×	×	×	·	·

Schöner ist vielleicht die folgende Beschreibung von I:

$$\begin{aligned} aI &= \{1,2,3\} & a'I &= \{6,5,4\} \\ bI &= \{1,2,4\} & b'I &= \{6,5,3\} \\ cI &= \{1,3,5\} & c'I &= \{6,4,2\} \\ dI &= \{1,5,4\} & d'I &= \{6,2,3\} \end{aligned}$$

□

Beobachtung: Zu jeder Inzidenzstruktur $\mathcal{I} = (P, B, I)$ gehören zwei Abbildungen, die „mengenwertig“ sind:

1. $P \to 2^B$, $p \mapsto pI$ („Büschelabbildung“, „p-te Zeile der Kreuztabelle zu $\mathcal{I}$“), und
2. $B \to 2^P$, $b \mapsto Ib$ („Spurabbildung“, „b-te Spalte der Kreuztabelle zu $\mathcal{I}$“).

1.30 Proposition
Seien P und B Mengen und

$$\rho : 2^{P\times B} \to (2^B)^P, \quad I \mapsto \rho I \text{ mit } \rho I : P \to 2^B,\ p \mapsto pI.$$

Also ist $p(\rho I) := pI$ für alle $p \in P$. Sei weiterhin

$$\lambda : 2^{P\times B} \to (2^P)^B, \quad I \mapsto I\lambda \text{ mit } I\lambda : B \to 2^P,\ b \mapsto Ib.$$

Also ist $(I\lambda)b := Ib$ für alle $b \in B$. Dann sind ρ und λ Bijektionen:

$$(2^B)^P \xleftarrow{\ \rho\ } 2^{P\times B} \xrightarrow{\ \lambda\ } (2^P)^B$$

„Büschelsicht“ „Tabellensicht“ „Punktesicht“

Dies sind also gleichwertige Sichtweisen (Beschreibungsweisen). □

1.4 Charakterisierung von $\mathbb{N}$ und Induktionsprinzip

Die Menge $\mathbb{N}$ der natürlichen Zahlen ist bestimmt durch

1. $0 \in \mathbb{N}$,
2. $s : \mathbb{N} \to \mathbb{N} \setminus \{0\}$, $n \mapsto n+1$ („Nachfolger von n“) ist injektiv,
3. für alle $X \in 2^{\mathbb{N}}$ mit $0 \in X$ und $\forall n \in \mathbb{N} : (n \in X \Rightarrow n+1 \in X)$ gilt bereits $X = \mathbb{N}$.

Prinzip (Induktionsprinzip)
Sei $A(n)$ Aussage für jedes $n \in \mathbb{N}$. Ist dann $A(0)$ wahr und es gilt

$$\forall n \in \mathbb{N} :\ (A(n) \text{ wahr } \Rightarrow\ A(n+1) \text{ wahr}),$$

so ist $A(n)$ für jedes $n \in \mathbb{N}$ wahr. □

Begründung: Sei $X := \{n \in N \mid A(n) \text{ wahr}\}$. Dann folgt $X = \mathbb{N}$ (mit 3.).

Mengenkonstruktivismus: Zermelo-Fraenkel-Mengenlehre („Aufbau aus dem Nichts“). Modell von $\mathbb{N}$ wie folgt: $0 := \varnothing$, $1 := \{\varnothing\}$, $n+1 := \{0, \ldots, n\}$.

1.5 Interpretationen von Abbildungen

Sei $a : P \to S$ eine Abbildung. Unterschiedliche Interpretationen („hohe Expressivität“):

1. a ist „bipartite Zerlegung“:
   Beispiel: P Menge von Personen, S Menge von Orten, $p \overset{a}{\mapsto} s$ ordnet jeder Person p ihren Geburtsort s zu.

2. a ist „Transformation“:
   Zum Beispiel Projektion eines Fotos auf eine Leinwand („Darstellende Geometrie“), oder, falls $P = S$: etwa P Punktmenge des Anschauungsraums, a ist eine Drehung.

3. a ist eine „Familie“ von Elementen aus S indiziert durch P:
   Wir nennen P dann auch „Indexmenge“ zu a. Schreibweise: $(ap)_{p\in P} := a$ (manchmal wird S „vergessen“). Oft setzt man $a_p := ap = a(p)$ und folglich $(a_p)_{p\in P} = a$.

4. a als „Datenvektor“.
   Beispiel: a wie in 1., $P = \{\text{Fritz}, \text{Hans}, \text{Lisa}\}$, $S = \{\text{Berlin}, \text{Hamburg}, \text{Dresden}\}$, und

p	a_p
Fritz	Berlin
Hans	Hamburg
Lisa	Dresden

   Für $n \in \mathbb{N}_+$ sei $(a_1, \ldots, a_n) \in S^n$. Setze $P := [n] = \{1, \ldots, n\}$ und $a : P \to S$, $p \mapsto a_p$. Dann wird a mit $(a_1, \ldots, a_n)$ identifiziert. Entsprechend wird S^n mit $S^{[n]}$ identifiziert.

   „Zeile“

p	1	2	…	n
a_p	a_1	a_2	…	a_n

   oder „Spalte“

p	a_p
1	a_1
2	a_2
…	…
n	a_n

   S^n ist naiv definiert als die Menge aller n-Tupel mit Werten in S,

   $$S^n := \{(s_1, \ldots, s_n) \mid s_1, \ldots, s_n \in S\}.$$

   $S^P := \{f \mid f : P \to S \text{ Abbildung}\}$, das heißt S^P ist die Menge aller Abbildungen von P nach S. Also ist $S^{[n]} = \{f \mid f : [n] \to S \text{ Abbildung}\}$.

   $f =$

p	1	2	…	n
fp	$f1$	$f2$	…	fn

   $\equiv (f1, f2, \ldots, fn)_S$

   also $(f1, \ldots, fn)_S := (fp)_{p\in[n]} := f$. (Oft lax $(f1, \ldots, fn) := f$, „vergisst S“.)

   Also n-*Tupel über* S ist Abbildung von $[n]$ nach S.

5. modern: a als *Fuzzy-Teilmenge* von P über S (gemessen).
   ap „Ausprägung von p bezüglich a“, „Grad der Unschärfe von p bezüglich a“, bzw. ap ist der „Grad der Mitgliedschaft von p in a.“ (Lotfi A. Zadeh, fuzzy – „unscharf“)

Beispiel: $S = [0,1] := \{x \in \mathbb{R} \mid 0 \le x \le 1\}$. $a(\text{Fritz}) = \frac{3}{7}$ („Fritz geht an 3 von 7 Tagen in eine Kneipe“).

1.6 Mehr zu Abbildungen

Schreibweisen Sei $f : A \to B$ Abbildung.

1. Ist f injektiv ($fx_1 = fx_2 \Rightarrow x_1 = x_2$), dann schreiben wir auch $f : A \rightarrowtail B$ (französische Notation, Bourbaki) oder $f : A \hookrightarrow B$ (englische Notation).
2. Ist f surjektiv ($\forall y \in B\ \exists x \in A : fx = y$), dann schreiben wir $f : A \twoheadrightarrow B$.
3. Ist f bijektiv (also injektiv und surjektiv), so schreiben wir auch $f : A \xrightarrow{\sim} B$ bzw. $A \xrightarrow[f]{\sim} B$ (englische Notation) oder $f : A \rightarrowtail\!\!\!\!\twoheadrightarrow B$ (französische Notation, weniger üblich).

Wir sagen, A ist *gleichmächtig* zu B, falls eine bijektive Abbildung $f : A \to B$ existiert, und schreiben dafür auch $A \simeq B$ beziehungsweise $A \cong B$.

Einschränkung, Gleichheit, Inklusion, Identität Seien $f : A \to B$, $g : C \to D$ Abbildungen.

1. g heißt *Einschränkung* von f (und f *Fortsetzung* von g), falls gilt:

$$C \subseteq A \ \wedge\ D \subseteq B \ \wedge\ \forall x \in C :\ gx = fx.$$

   Dann schreiben wir $g \sqsubseteq f$ (oder $f \sqsupseteq g$) und setzen $f \mid (C \to D) := g$. Gilt zusätzlich $B = D$, so heißt g die Einschränkung von f auf C und wir setzen $f|C := g$ (auch $f|_C := f|C$).

2. Es sei:

$$\begin{aligned} f = g \ &:\Leftrightarrow\ f \sqsubseteq g \ \wedge\ g \sqsubseteq f \\ &\Leftrightarrow A = C \ \wedge\ B = D \ \wedge\ \forall x \in A :\ fx = gx. \end{aligned}$$

3. Gilt $A \subseteq B$ und $f : A \to B$, $x \mapsto x$, so nennen wir f die *Inklusion* (Inklusionsabbildung) von A nach B und setzen $\mathrm{id}_{A,B} := f$. Gilt überdies $A = B$, so heißt f die *Identität* auf A und wir setzen $\mathrm{id}_A := f$.

Verkettung von Abbildungen

1.31 Definition
Seien A, B, C Mengen, sowie $f : A \to B$ und $g : B \to C$ Abbildungen. Dann ist

$$g \circ f : A \to C, \quad a \mapsto g(fa)$$

wieder eine Abbildung, die sogenannte *kontravariante Verkettung* von f mit g.

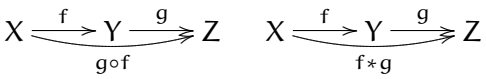
Entsprechend heißt

$$f * g : A \to C, \quad a \mapsto (af)g$$

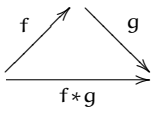
die *kovariante Verkettung* von f mit g. □

Es gilt also (Diagrammsicht):

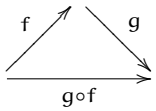
$$g \circ f = f * g$$



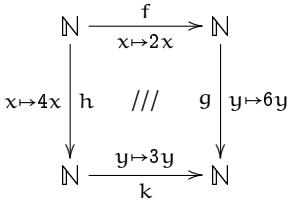
naive Sicht, kovariant, „f vor g“



clevere Sicht, kontravariant, „g nach f“



Rechengesetze in $\mathbb{N}$ Beispiel für ein „kommutierendes Diagramm“ (s. u.):



Hier gilt $f * g = h * k$ (naiv, kovariant) bzw. $g \circ f = k \circ h$ (clever, kontravariant).
Als intuitiv gegeben: $n + (m + 1) := (n + m) + 1$, $n \cdot (m + 1) := n \cdot m + n$.
Es ergeben sich die Rechengesetze:

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

Assoziativität $\cdot$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

Kommutativität, $a + b = b + a$, $a \cdot b = b \cdot a$, und

Distributivität, $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$.

Addition und Multiplikation natürlicher Zahlen kann als Verkettung von Abbildungen (als „Transformationen“ bzw. „Aktionen“) gesehen werden:

1.32 Proposition
Für jedes $n \in \mathbb{N}$ seien folgende Abbildungen erklärt:

- $\tau_n : \mathbb{N} \to \mathbb{N}$, $x \mapsto n + x$ („Verschiebung (Translation) um n nach nechts“), und
- $\sigma_n : \mathbb{N} \to \mathbb{N}$, $x \mapsto n \cdot x$ („Streckung um Faktor n im Nullpunkt“).

Dann gilt für alle $m, n \in \mathbb{N}$:

1. $\tau_n \circ \tau_m = \tau_{n+m}$
   „erst um m, dann um n verschieben, ist das Gleiche wie um $n + m$ verschieben“,
2. $\sigma_n \circ \sigma_m = \sigma_{n \cdot m}$
   „erst um m, dann um n strecken, ist das Gleiche, wie um $n \cdot m$ zu strecken“ □

Beweis

1. Für jedes $x \in \mathbb{N}$ gilt:

$$x \overset{\tau_m}{\longmapsto} m + x \overset{\tau_n}{\longmapsto} n + (m + x), \qquad \tau_n \circ \tau_m = \tau_m * \tau_n$$

   Wegen $n + (m + x) = (n + m) + x$ (Assoziativgesetz $+$) folgt $(\tau_n \circ \tau_m)x = \tau_{n+m}x$ für alle $x \in \mathbb{N}$, das heißt $\tau_n \circ \tau_m = \tau_{n+m}$.

2. Für alle $x \in \mathbb{N}$ gilt:

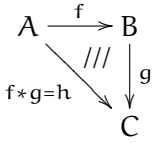
$$\begin{aligned}
(\sigma_n \circ \sigma_m)x &= \sigma_n(\sigma_m x) && \text{Definition } \circ \\
&= \sigma_n(m \cdot x) && \text{Definition } \sigma_n \\
&= n \cdot (m \cdot x) && \text{Definition } \sigma_m \\
&= (n \cdot m) \cdot x && \text{Assoziativgesetz } \cdot \\
&= \sigma_{n \cdot m} x, && \text{Definition } \sigma_{n \cdot m}
\end{aligned}$$

   also $\sigma_n \cdot \sigma_m = \sigma_{n \cdot m}$. ∎

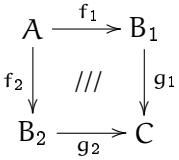
Kommutierende Diagramme Business: “Diagram Chasing”.

1.33 Definition (Kommutierende Diagramme von Abbildungen)

1. Seien $f : A \to B$, $g : B \to C$ und $h : A \to C$ Abbildungen. Dann bildet $((f, g), h)$ ein *kommutierendes Dreieck*, falls $f * g = h$ (das heißt $g \circ f = h$) gilt:



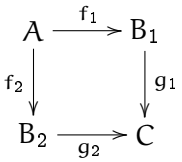
2. Seien $f_1 : A \to B_1$, $f_2 : A \to B_2$, $g_1 : B_1 \to C$ und $g_2 : B_2 \to C$ Abbildungen. Dann bildet $((f_1, g_1), (f_2, g_2))$ ein *kommutierendes Quadrat*, falls $f_1 * g_1 = f_2 * g_2$ (das heißt $g_1 \circ f_1 = g_2 \circ f_2$) gilt:



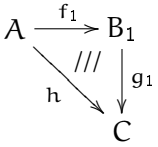
□

1.34 Bemerkung

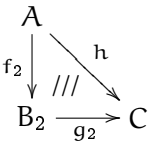
Vier Abbildungen



bilden genau dann ein kommutierendes Quadrat, wenn es eine Abbildung $h : A \to C$ gibt, so dass sowohl

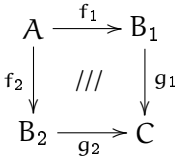


als auch



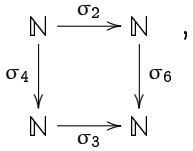
kommutierende Dreiecke bilden. □

Beweis
Sei



kommutierendes Quadrat, das heißt $f_1 * g_1 = f_2 * g_2$. Dann erfüllt $h := f_1 * g_1$, dass $((f_1, g_1), h)$ und $((f_2, g_2), h)$ kommutierende Dreiecke sind. Seien umgekehrt $((f_1, g_1), h)$ und $((f_2, g_2), h)$ kommutierende Dreiecke, das heißt $f_1 * g_1 = h$ und $f_2 * g_2 = h$, dann ist folglich $f_1 * g_1 = f_2 * g_2$, also ist $((f_1, g_1), (f_2, g_2))$ kommutierendes Quadrat. ■

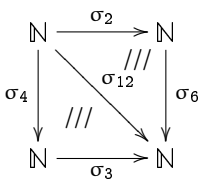
1.35 Beispiel
Sei $\sigma_n : \mathbb{N} \to \mathbb{N}$, $x \mapsto n \cdot x$ „Streckung um n im Nullpunkt“, dann ist



ein kommutierendes Quadrat wegen

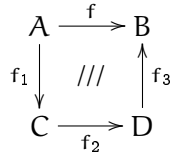
$$\sigma_3 \circ \sigma_4 = \sigma_{3 \cdot 4} = \sigma_{12} = \sigma_{6 \cdot 2} = \sigma_6 \circ \sigma_2.$$

Also sind die zugehörigen kommutierenden Dreiecke:



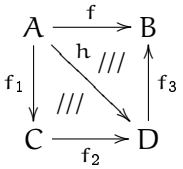
□

Anderer Typ kommutierender Diagramme:



bedeute $f = f_1 * f_2 * f_3$.

Zerlegung in kommutierende Dreiecke:



wobei $((f_1, f_2), h)$ und $((h, f_3), f)$ kommutierende Dreiecke sind. Dabei ist $h := f_1 * f_2$, denn dann gilt:

$$f = f_1 * f_2 * f_3 = (f_1 * f_2) * f_3 = h * f_3 \quad \text{und} \quad h = f_1 * f_2.$$

1.7 Äquivalenz und Ordnung

Rückblick: $\mathcal{I} = (P, B, I)$ ist Inzidenzstruktur, falls P, B, I Mengen mit $I \subseteq P \times B$ sind. Dann heißt I Inzidenzrelation bezüglich (P, B). pIb „Ball ist rund“.

1.36 Definition
Ist A Menge und $R \subseteq A \times A$, das heißt $R \in 2^{A \times A}$, so nennen wir R *binäre Relation* auf A. (Dies ist eine andere Situation als üblich für Inzidenzstrukturen, wo oft $P \cap B = \varnothing$ gilt.) Das Paar $\mathcal{A} := (A, R)$ nennen wir dann *binäres Relat*. Wir schreiben aRb für $(a, b) \in R$.

$\mathcal{A}$ **reflexiv:** $\forall x \in A : xRx$,

$\mathcal{A}$ **symmetrisch:** $\forall x, y \in A : xRy \Leftrightarrow yRx$,

$\mathcal{A}$ **transitiv:** $\forall x, y, z \in A : xRy \wedge yRz \Rightarrow xRz$,

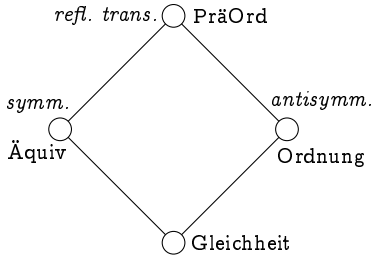
$\mathcal{A}$ **antisymmetrisch:** $\forall x, y \in A : xRy \wedge yRx \Rightarrow x = y$.

- $\mathcal{A}$ heißt *Präordnung* („prägeordnete Menge“, „R ist Präordnung auf A“), falls $\mathcal{A}$ reflexiv und transitiv ist (Beispiel: Studenten nach Notenspiegel ordnen),
- $\mathcal{A}$ heißt *Äquivalenz* („R ist Äquivalenzrelation auf A“), falls $\mathcal{A}$ symmetrische Prärordnung ist
  – d. h. $\mathcal{A} = (A, R)$ Äquivalenz ist reflexiv, symmetrisch und transitiv,
- $\mathcal{A}$ heißt *Ordnung* („geordnete Menge“, „R ist Ordnungsrelation auf A“), falls $\mathcal{A}$ antisymmetrische Prärordnung ist
  – d. h. $\mathcal{A} = (A, R)$ Ordnung ist reflexiv, antisymmetrisch und transitiv.

$\operatorname{diag} A := \{(x, x) \mid x \in R\}$ ist eine Äquivalenzrelation auf A, die auch als *Gleichheitsrelation* auf A bezeichnet wird. □

Kreuztabelle („formaler Kontext"):

	reflexiv	transitiv	symmetr.	antisymm.
Präordnung	×	×		
Äquivalenz	×	×	×	
Ordnung	×	×		×



Ordnungsdiagramm (↑ allgemeiner, ↓ spezieller)

Warnung: In der Soziologie und bei Herrn Schuricht wird Ordnung als strikte Ordnung definiert. Ein binäres Relat $\mathcal{A} = (A, R)$ heißt *strikte Ordnung*, falls $\mathcal{A}$ transitiv und *irreflexiv* ist, das heißt $\forall x \in A : x \not R x$ (oder: $\operatorname{diag} A \cap R = \varnothing$).

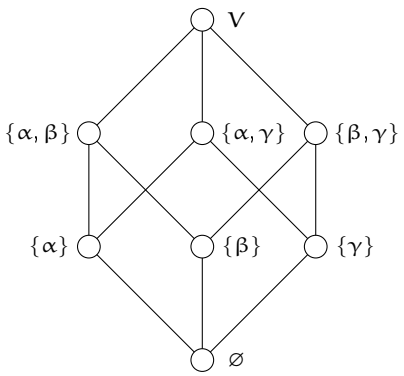
1.37 Definition
Ein binäres Relat $\mathcal{A} = (A, R)$ heißt *total geordnet*, falls $\mathcal{A}$ Ordnung mit $\forall x, y \in A : xRy \vee yRx$ („linear geordnet") ist. □

1.38 Beispiel

- $(\mathbb{N}, \leq)$ ist linear geordnet,
- $(\mathbb{Z}, \leq)$ ist linear geordnet,
- $(\mathbb{R}, \leq)$ ist linear geordnet, aber
- $(\mathbb{N} \times \mathbb{N}, \leq)$ mit $(n_1, n_2) \leq (n_1', n_2') :\Leftrightarrow n_1 \leq n_1' \wedge n_2 \leq n_2'$ ist nicht total geordnet (denn $(1,0) \not\leq (0,1) \not\leq (1,0)$). □

Für eine Menge U ist $(2^U, \subseteq) =: 2^U$ eine geordnete Menge, der *Potenzmengenverband*.

1.39 Beispiel
$U = \{\alpha, \beta, \gamma, \delta\}$, $V := U \setminus \{\delta\} = \{\alpha, \beta, \gamma\}$.

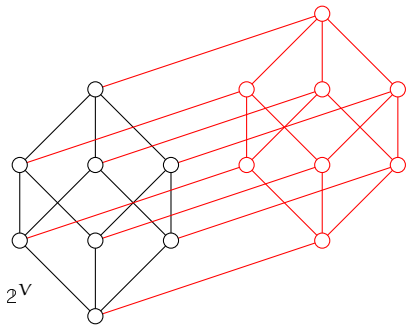


Ordnungsdiagramm (auch Hasse-Diagramm) von 2^V

Dann ist

$$2^U = \{X \in 2^U \mid \delta \notin X\} \cup \{X \in 2^U \mid \delta \in X\},$$

wobei $\{X \in 2^U \mid \delta \in X\} = \{X \cup \{\delta\} \mid X \in 2^V\}$.



Ordnungsdiagramm von 2^U

Hasse-Diagramm zu 2^U für $U = \{\alpha, \beta, \gamma, \delta\}$, „Helmut Hasse — Hamburg“. □

Sei $\operatorname{Eq} A$ die Menge aller Äquivalenzrelationen (“equivalence relation”) auf A und $\operatorname{Ord} A$ die Menge aller Ordnungsrelationen auf A.

Ein wichtiges Beispiel für eine Äquivalenzrelation ist folgendes.

1.40 Definition (Kern einer Abbildung)
Sei $f : A \to B$ eine Abbildung. Dann heißt

$$\ker(f) := \{(x, y) \in A \times A \mid fx = fy\}$$

der *Kern* (“kernel”) von f. Dieser ist eine Äquivalenzrelation auf A. □

1.41 Proposition
Sind A, B Mengen, so ist für $f \in B^A$ stets $\ker(f) \in \operatorname{Eq} A$. □

Beweis

„reflexiv“ $(x, x) \in \ker f$ für alle $x \in A$, da $fx = fx$.

„transitiv“ Ist $(x, y) \in \ker f$ und $(y, z) \in \ker f$, so ist $(x, z) \in \ker f$, da dann $fx = fy$ und $fy = fz$, also $fx = fz$ gilt.

„symmetrisch“ Ist $(x, y) \in \ker f$, so ist auch $(y, x) \in \ker f$, da dann $fx = fy$, also $fy = fx$ gilt. ■

Sei für eine Menge A die (durch $\subseteq$) geordnete Menge aller Äquivalenzrelationen auf A mit $\mathbb{E}\mathrm{q}\, A := (\operatorname{Eq} A, \subseteq)$ bezeichnet. Dann ist $\operatorname{diag} A \subseteq R \subseteq A \times A$ für alle $R \in \operatorname{Eq} A$, also ist $\operatorname{diag} A$ die kleinste Äquivalenzrelation auf A, und $A \times A$ ist die größte Äquivalenzrelation auf A.

Äquivalenzrelationen und Partitionen

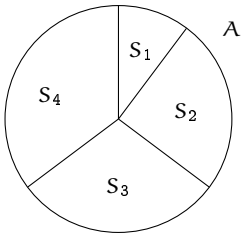
1.42 Definition (Äquivalenzklassen)
Ist $\mathcal{R} = (A, R)$ eine Äquivalenz, so ist $[x]R := \{y \in A \mid xRy\}$ die zu $x \in A$ gehörige *Äquivalenzklasse* von $\mathcal{R}$. Weiter bezeichnen wir mit $A/R := \{[x]R \mid x \in A\}$ die Menge aller Äquivalenzklassen von $\mathcal{R}$ bzw. von R (lax). □

Es ist also $A/R \subseteq 2^A$.
Quantoren: $\forall$ „für alle“, $\exists$ „es gibt mindestens ein“, $\exists!$ „es gibt genau ein“.

1.43 Definition (Partition)
Eine Teilmenge $\mathcal{S}$ von 2^A heißt *Partition* von A, falls gilt:

1. $\forall x \in A\ \exists! S \in \mathcal{S} :\ x \in S$,
2. $\varnothing \notin \mathcal{S}$.

Gilt nur 1., so heißt $\mathcal{S}$ eine schwache Partition von A. □



$\{S_1, S_2, S_3, S_4\} = \mathcal{S}$ zerlegt A

Sei $\operatorname{Part} A$ die Menge aller Partitionen von A.

1. Ist $R \in \operatorname{Eq} A$, so ist $A/R \in \operatorname{Part} A$.
2. Ist $\mathcal{S} \in \operatorname{Part} A$, so ist $R_{\mathcal{S}} := \{(x, y) \in A \mid \exists S \in \mathcal{S} : x, y \in S\} \in \operatorname{Eq} A$.
3. Die Abbildung
$$\Phi : \operatorname{Eq} A \to \operatorname{Part} A, \quad R \mapsto A/R$$
ist eine Bijektion mit $\Psi : \operatorname{Part} A \to \operatorname{Eq} A$, $\mathcal{S} \mapsto R_{\mathcal{S}}$ als inverser Abbildung.

1.8 Mehr zu Inzidenzstrukturen

1.44 Proposition (Doppelte Abzählung)
Ist $\mathcal{I} = (P, B, I)$ endliche Inzidenzstruktur (das heißt P und B endliche Mengen), so gilt: $\{\{p\} \times pI \mid p \in P\}$ und $\{Ib \times \{b\} \mid b \in B\}$ sind Partitionen von I, und man hat

$$\sum_{p \in P} \#(pI) = \#I = \sum_{b \in B} \#(Ib).$$ □

1.45 Definition (taktische Konfiguration)
Sei $\mathcal{I} = (P, B, I)$ eine endliche Inzidenzstruktur, und sei $v_{\mathcal{I}} := \#P$, $b_{\mathcal{I}} := \#B$ und seien $\rho_{\mathcal{I}} : P \to \mathbb{N}$, $p \mapsto \#(pI)$, $\kappa_{\mathcal{I}} : B \to \mathbb{N}$, $b \mapsto \#(Ib)$. Dann heißt $\mathcal{I}$ *taktische Konfiguration*, falls $\rho_{\mathcal{I}}$ und $\kappa_{\mathcal{I}}$ konstante Abbildungen sind. □

Für eine taktische Konfiguration $\mathcal{I} = (P, B, I)$ sei $r_{\mathcal{I}} := \#(pI)$ für $p \in P$ und $k_{\mathcal{I}} := \#(Ib)$ für $b \in B$. Dann gilt:

$$v_{\mathcal{I}} \cdot r_{\mathcal{I}} = b_{\mathcal{I}} \cdot k_{\mathcal{I}},$$

denn $v_{\mathcal{I}} \cdot r_{\mathcal{I}} = \sum_{p \in P} r_{\mathcal{I}} = \sum_{p \in P} \#(pI) = \#I = \sum_{b \in B} \#(Ib) = \sum_{b \in B} k_{\mathcal{I}} = b_{\mathcal{I}} \cdot k_{\mathcal{I}}$.

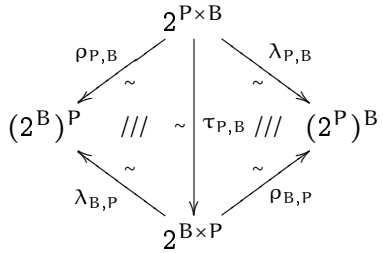
Wir nennen $(v_{\mathcal{I}}, r_{\mathcal{I}}; b_{\mathcal{I}}, k_{\mathcal{I}})$ „Parameterquadrupel“ zur taktischen Konfiguration $\mathcal{I}$.

1.46 Definition (duale Inzidenzstruktur)
Sei $\mathcal{I} = (P, B, I)$ eine Inzidenzstruktur. Dann ist die *duale Inzidenzstruktur* zu $\mathcal{I}$ definiert als $\mathcal{I}^d := (B, P, I^d)$, wobei $I^d := \{(b, p) \subseteq B \times P \mid pIb\}$ ist („alte Blöcke als neue Punkte“, „alte Punkte als neue Blöcke“), also $bI^d p :\Leftrightarrow pIb$.

Weitere übliche Notationen: $I^{op} := I^{-1} := I^{tr} := I^d$ (“opposite relation”, “inverse relation”, “transpose relation”, “duale relation”). □

1.47 Proposition
Ist $\mathcal{I} = (P, B, I)$ taktische Konfiguration mit Parametertupel $(v_{\mathcal{I}}, r_{\mathcal{I}}; b_{\mathcal{I}}, k_{\mathcal{I}})$, dann ist I^d ebenfalls eine taktische Konfiguration, mit $(b_{\mathcal{I}}, k_{\mathcal{I}}; v_{\mathcal{I}}, r_{\mathcal{I}})$ als Parameterquadrupel. □

Übersicht: Inzidenzstrukturen zu Mengen P und B.



Hierbei ist für $I \in 2^{P\times B}$ (das heißt $I \subseteq P \times B$) stets

$$I\rho_{P,B} : P \to 2^B,\ p \mapsto pI \quad \text{Büschelabbildung zu I bezüglich } (P, B),$$
$$\lambda_{P,B} I : B \to 2^P, b \mapsto Ib \quad \text{Spurabbildung zu I bezüglich } (P, B),$$
$$\tau_{P,B} : 2^{P\times B} \to 2^{B\times P},\ I \mapsto I^d = I^{tr}.$$

1.9 Datenmatrizen

Mathematische Modellierung von Tabellen als „Datenmatrizen“:

	Größe	Alter	Gewicht
Peter	groß	jung	mittel
Paul	riesig	mittel	schwer
Gabi	mittel	jung	leicht
Mandy	klein	alt	mittel

Als Datenmatrix modellieren:

$$\begin{aligned} P &:= \{\text{Peter, Paul, Gabi, Mandy}\} \\ Q &:= \{\text{Größe, Alter, Gewicht}\} \\ S &:= \{\text{groß, riesig, mittel, klein, jung, alt, schwer, leicht}\} \end{aligned}$$

(Die Anordnung ist Sache des Buchhalters, unwichtig für Zuordnung.)
Vorstellung: $\alpha : P \times Q \to S$ Tabelle ist Abbildungstabelle. Zum Beispiel:

$$\begin{aligned} \alpha(\text{Peter, Größe}) &= \text{groß} \\ \alpha(\text{Mandy, Alter}) &= \text{alt} \\ \alpha(\text{Paul, Gewicht}) &= \text{schwer} \end{aligned}$$

α ist die Datenmatrix zur Tabelle zu (P, Q).

1.48 Definition
Eine *Datenmatrix* zu einem Mengenpaar (P, Q) über einer Menge S ist definiert als Abbildung $\alpha : P \times Q \to S$. Wir sagen auch, α ist eine „$P \times Q$–Matrix“ über S. □

1.49 Bemerkung
(P, Q, α) kann als Fuzzy-Inzidenzstruktur aufgefasst werden, beziehungsweise als *mehrwertige Inzidenzstruktur* (auch „mehrwertiger formaler Kontext“). □

Zu $p \in P$ heißt die Abbildung $\alpha(p, \cdot) \to S$, $q \mapsto \alpha(p, q)$ die p-te *Zeile* von α („$\cdot$“ salopp für Platzhalter). Entsprechend heißt zu $q \in Q$ die Abbildung $\alpha(\cdot, q) : P \to S$, $p \mapsto \alpha(p, q)$ die q-te *Spalte* von α.
Zum Beispiel:

$\alpha(\text{Mandy}, \cdot) : Q \to S$

Größe	Alter	Gewicht
klein	alt	mittel

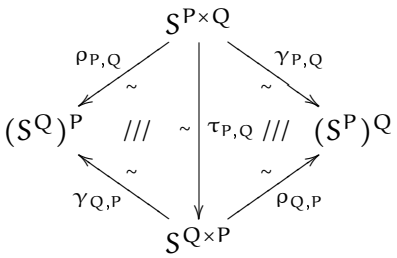
$\alpha(\cdot, \text{Größe})$:

Peter	groß
Paul	riesig
Gabi	mittel
Mandy	klein

Sei $r_\alpha : P \to S$, $p \mapsto \alpha(p, \cdot)$ (“row map”) die *Zeilenabbildung* zu α, und sei $c_\alpha : Q \to S$, $q \mapsto \alpha(\cdot, q)$ (“column map”) die *Spaltenabbildung* zu α (r “row”, Zeile, c “column”; Spalte). Zu $\alpha \in S^{P \times Q}$ (das heißt $\alpha : P \times Q \to S$ Abbildung) sei

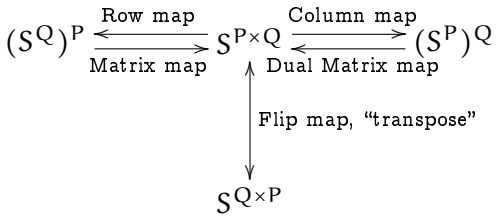
$$\alpha^T : Q \times P \to S, \quad (q, p) \mapsto \alpha(p, q)$$

die *Transponierte* zu α. (Achtung: $\alpha(q, p)$, $q \in Q$, $p \in P$ Syntaxblödsinn.)
Übersicht zu Datenmatrizen zu Mengenpaar (P, Q) über Menge S:



Hierbei ist $\rho_{P,Q} : S^{P\times Q} \to (S^Q)^P$, $\alpha \mapsto r_\alpha$, und $\gamma_{P,Q} : S^{P\times Q} \mapsto (S^P)^Q$, $\alpha \mapsto c_\alpha$, sowie $\tau_{P,Q} : S^{P\times Q} \to S^{Q\times P}$, $\alpha \mapsto \alpha^T$.

Sichtweisen von Datenmatrizen im Überblick Seien P, Q, S Mengen. Dann haben wir folgendes Zusammenspiel:



Erläuterungen zum Diagramm:

1. Für Datenmatrix $\alpha \in S^{P\times Q}$ schreiben wir auch $\alpha =: (\alpha(p,q))_{(p,q)\in P\times Q}$. Dann ist:
   a) $r_\alpha \in (S^Q)^P$ mit $r_\alpha := (\alpha(p,\cdot))_{p\in P}$ die "ROW-MAP of α", Zeilenabbildung zu α,
   b) $c_\alpha \in (S^P)^Q$ mit $c_\alpha := (\alpha(\cdot,q))_{q\in Q}$ die "COLUMN-MAP of α", Spaltenabbildung zu α,
   c) $\alpha^T \in S^{Q\times P}$ mit $\alpha^T := (\alpha(p,q))_{(q,p)\in Q\times P}$ die "TRANSPOSE of α", Transponierte zu α.

2. Für „Familie von Datenvektoren" $u \in (S^Q)^P$ schreiben wir auch $u = (up)_{p\in P}$ und $u = \big(((up)q)_{q\in Q}\big)_{p\in P}$, wobei $up = ((up)q)_{q\in Q}$ Datenvektor von p (zu u). Dann ist:
   a) $\mu_u \in S^{P\times Q}$ mit $\mu_u := ((up)q)_{(p,q)\in P\times Q}$ die "MATRIX-MAP of u",
   b) $\mu_u^T \in S^{Q\times P}$ mit $\mu_u^T := ((up)q)_{(q,p)\in Q\times P}$ die "DUAL-MATRIX-MAP of u",
   c) $u^\sigma \in (S^P)^Q$ mit $u^\sigma := (((up)q)_{p\in P})_{q\in Q}$ der "SWAP of u".

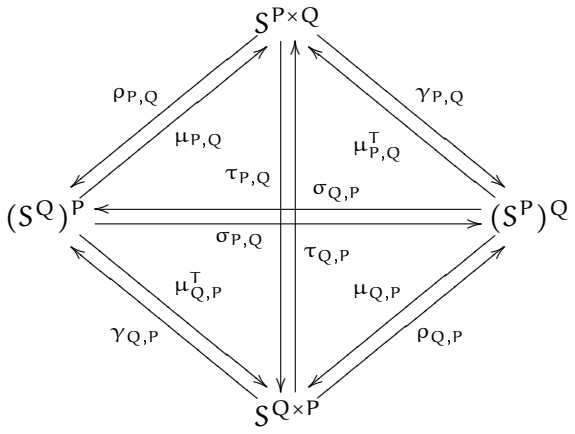
   Anmerkung: $\mu_u^T = (\mu_u)^T$.

Beispiel: $(u\,\text{Peter})\,\text{Geburtsort} = \text{Dresden} - \text{SWAP} - (u^\sigma\,\text{Geburtsort})\,\text{Peter} = \text{Dresden}$. Also gilt:

1. Ist $\alpha \in S^{P\times Q}$, dann
$$(r_\alpha p)q = (c_\alpha q)p = \alpha^T(q,p) = \alpha(p,q)$$
   für alle $p \in P$, $q \in Q$.

2. Ist $u \in (S^Q)^P$, dann
$$\mu_u(p,q) = \mu_u^T(q,p) = (u^\sigma q)p = (up)q$$
   für alle $p \in P$, $q \in Q$.

"Grand view":



1.10 Binäre Relate als Inzidenzstrukturen und als Netzwerke

Sei $\mathcal{R} = (A, R)$ binäres Relat, das heißt R ist binäre Relation auf A (also $R \in 2^{A\times A}$, das heißt $R \subseteq A \times A$).

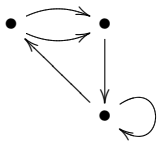
Sicht I: als Inzidenzstruktur Wir sagen $\mathcal{IR} := (A, A, R)$ ist „$\mathcal{R}$ als Inzidenzstruktur", $aR := \{b \in A \mid aRb\}$, $Ra := \{b \in A \mid bRa\}$.

Beispiel: R „erachtet als Freund": aR Menge derjenigen, die a als Freund erachtet, Ra Menge derjenigen, die a als Freund erachten.

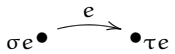
Darstellung durch Kreuztabelle: Beispiel $\mathcal{R} = (A, R)$ mit $A = \{a, b, c\}$ und $R = \{(a, b), (b, c), (c, a), (c, c)\}$ hat folgende Darstellung (als Kreuztabelle zu $\mathcal{R}$):

	a	b	c
a		×	
b			×
c	×		×

Sicht II: als Netzwerk Mathematische Beschreibung von Pfeildiagrammen:



e Kante, σe Anfangspunkt "source of e" , τe Endpunkt "target of e".

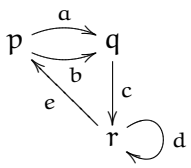


1.50 Definition (gerichtetes Netzwerk)
Ein (gerichtetes) *Netzwerk* (bzw. gerichteter *Multigraph*) ist definiert als Quadrupel $\mathcal{N} := (V, E, \sigma, \tau)$ bestehend aus Mengen V, E und Abbildungen $\sigma, \tau \in V^E$ (das heißt σ, τ sind Abbildungen von E nach V).

Die Abbildung $\rho : E \to V \times V$, $e \mapsto (\sigma e, \tau e)$ heißt die *Strukturabbildung* von $\mathcal{N}$. □

Interpretation: V Menge von *Knoten* ("vertices", "nodes"), E Menge von *Kanten* bzw. *Pfeilen* ("edges", "arrows"), σ "source map", τ "target map", für e Kante ist σe „Anfangsknoten der Kante e", τe „Endknoten der Kante e".

Formale Beschreibung des obigen Beispiels:



$V := \{p, q, r\}$, $E := \{a, b, c, d, e\}$,

x	a	b	c	d	e
σx	p	p	q	r	r
τx	q	q	r	r	p

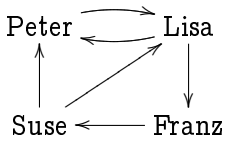
x „variable Kante"

$\mathcal{N}$ heißt *einfach*, falls ρ injektiv ist. Nicht einfach: • ⇄ •, einfach: • ⇄ •.

Ist $\mathcal{R} = (A, R)$ binäres Relat, so ist $\mathcal{NR} := (A, R, \sigma, \tau)$ mit $\sigma : R \to A$, $(p, q) \mapsto p$ und $\tau : R \to A$, $(p, q) \mapsto q$ einfaches Netzwerk. Wir sagen „$\mathcal{NR}$ ist $\mathcal{R}$ als Netzwerk (Graph)".

Es ist pR die „Menge der OUT-Knoten zu p bezüglich $\mathcal{NR}$ beziehungsweise $\mathcal{R}$", und Rp die „Menge der IN-Knoten p bezüglich $\mathcal{NR}$ beziehungsweise $\mathcal{R}$".

1.51 Beispiel
Sei xRy „x bewundert y". $\mathcal{R}$ als Netzwerk $\mathcal{NR}$:



$R\,\text{Lisa} = \{\text{Peter}, \text{Suse}\}$ IN-Knoten zu Lisa, $\text{Lisa}\,R = \{\text{Peter}, \text{Franz}\}$.

$\mathcal{R}$ als Inzidenzstruktur $\mathcal{IR}$:

	Peter	Lisa	Franz	Suse
Peter		×		
Lisa	×		×	
Franz				×
Suse	×	×		

□

1.52 Beispiel
Beispiel für eine Äquivalenzrelation als Inzidenzstruktur und zugehörige Partition: Sei $R := \ker f$ für $f : [6] \to \{a, b, c\}$, $f1 = f2 = a$, $f3 = f4 = f5 = b$, $f6 = c$. $\mathcal{R} = (A, R)$ ist Äquivalenz und $\mathcal{IR}$ hat folgende Kreuztabelle:

	1	2	3	4	5	6
1	×	×				
2	×	×				
3			×	×	×	
4			×	×	×	
5			×	×	×	
6						×

$A/R = \{S_1, S_2, S_3\}$ mit $S_1 = \{1,2\}$, $S_2 = \{3,4,5\}$, $S_3 = \{6\}$. Es ist $\Phi : \operatorname{Eq} A \xrightarrow{\sim} \operatorname{Part} A$, $R \mapsto A/R$, und $\Psi : \operatorname{Part} A \xrightarrow{\sim} \operatorname{Eq} A$, $\mathcal{S} \mapsto R_{\mathcal{S}}$ mit $R_{\mathcal{S}} := \bigcup \{S \times S \mid S \in \mathcal{S}\}$. □

1.11 Folgen und Abzählung

Wiederholung: $A \simeq B :\Leftrightarrow A \cong B$ („A gleichmächtig zu B“) $:\Leftrightarrow \exists f : A \to B$ Bijektion

1.53 Definition
Eine Menge A heißt endlich, falls ein $n \in \mathbb{N}$ mit $A \simeq [n]$ existiert. Dann ist n eindeutig und wird als *Anzahl* bzw. *Mächtigkeit* von A bezeichnet. Schreibweise $\#A := n$. □

Ist $f : [n] \to A$ Abbildung, so heißt f *endliche Folge* in A; üblich $(f_i)_{i \in [n]} = f$. Eine Abbildung $f : \mathbb{N} \to A$ heißt (unendliche) *Folge* in A; üblich $(f_i)_{i \in \mathbb{N}} := f$.

Schreibweisen: $(f_i)_{i=1,\dots,n} := (f_i)_{i \in [n]}$ und $(f_i)_{i=1,2,\dots} := (f_i)_{i \in \mathbb{N}}$.

Eine Bijektion $\alpha : [n] \to A$ heißt *Abzählung* bzw. *Nummerierung* von A. Für $\alpha : [n] \to A$, $i \mapsto a_i$ wird häufig lax $A = \{a_1, \dots, a_n\}$ geschrieben (ist aber leicht missverständlich).

Es heißt A *abzählbar unendlich*, falls $A \simeq \mathbb{N}$. Eine Bijektion $\alpha : \mathbb{N} \to A$, $i \mapsto a_i$ heißt *Abzählung* von A, $\alpha =: (a_i)_{i \in \mathbb{N}} =: (a_1, a_2, \dots)$. (Der Buchhalter spricht.)

- Die Menge aller Folgen in A ist $A^{\mathbb{N}}$.
- „Duales“ Konzept: Natürliche Multimengen.
  Was ist eine (natürliche) Multimenge? „Gemüsemathe“. Ist A Menge (von Gemüsesorten zum Beispiel), so heißt $\alpha \in \mathbb{N}^A$ *Multimenge* zu A.

  Die Menge aller natürlichen Multimengen zu A ist $\mathbb{N}^A$.

2 Algebraische Operationen

„Wir rechnen – konkret und abstrakt.“

2.1 Summation

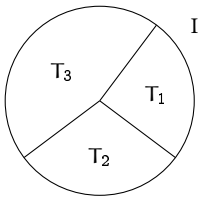
Σ Sigma sei Summationssymbol.

2.1 Definition (endliche Summation)
Sei M eine Menge. *Endliche Summation* über M ist eine Vorschrift Σ, die für jede endliche Menge I („Indexmenge“) eine Abbildung $\Sigma : M^I \to M$ induziert derart, dass für alle $\alpha \in M^I$ gilt

1. $\sum \alpha = \alpha i$ falls $I = \{i\}$,
2. $\sum \alpha = \sum \beta$ falls J endliche Menge, $f : I \to J$ Abbildung und $\beta : J \to M$, $j \mapsto \sum \alpha|_{f^{-1}j}$. □

Sloppy: Hierbei sei $f^{-1}j := f^{-1}\{j\} = \{i \in I \mid fi = j\}$.

Insbesondere gilt für jede Partition $\mathcal{T} \in \operatorname{Part} I$ und $\beta : \mathcal{T} \to M$, $T \mapsto \sum \alpha|_T$, dass $\sum \alpha = \sum \beta$ ist (wo $\alpha \in M^I$). „Summe der Teilsummen, also $\sum \beta$, ist die Gesamtsumme $\sum \alpha$.“



Zugehöriges $f : I \to \mathcal{T}$ ist $i \mapsto T$ mit $i \in T$, das heißt $f = \pi_{\mathcal{T}}$ ist Partitionsabbildung.

2.2 Notation
Für $\alpha \in M^I$ setzen wir $\sum_{i \in I} \alpha i := \sum \alpha$ und $\sum_{i=1}^{n} \alpha i := \sum_{i \in [n]} \alpha i$ für $I = [n]$ mit $n \in \mathbb{N}_+$. □

„Addition“: $x + y := \sum \alpha$ mit $\alpha : [2] \to M$, $1 \mapsto x$, $2 \mapsto y$.
$0 := \sum \alpha$ für $\alpha : \varnothing \to M$, leere Summation.
Es gilt (Übung):

1. $0 + a = a + 0$,
2. $a + b = b + a$,
3. $a + (b + c) = (a + b) + c$.

Also sei $\mathcal{T} \in \operatorname{Part} I$ und $\alpha \in M^I$. Dann ist für $\beta : \mathcal{T} \to M$, $T \mapsto \sum \alpha|_T$ stets $\sum \alpha = \sum \beta$, das heißt wegen $\sum_{i\in I} \alpha i := \sum \alpha$ und $\beta T = \sum \alpha|_T =: \sum_{i\in T} \alpha i$ und $\sum_{T\in\mathcal{T}} \beta T := \sum \beta$ gilt

$$\sum_{i\in I} \alpha i = \sum \alpha = \sum \beta = \sum_{T\in\mathcal{T}} \beta T = \sum_{T\in\mathcal{T}} \sum_{i\in T} \alpha i,$$

das heißt die Gesamtsumme ($\sum_{i\in I} \alpha i$) ist die Summe der Teilsummen ($\sum_{i\in T} \alpha i$ ist Teilsumme von α auf $T \in \mathcal{T}$) ("nested summation", „Doppelsumme").

2.3 Beispiel (Summation auf $\mathbb{N}$)
$\mathbb{N}_{add} := (\mathbb{N}, +, 0)$ natürliche Zahlen mit Addition, $\mathbb{N}_{mult} := (\mathbb{N}, \cdot, 1)$ natürliche Zahlen mit Multiplikation, $\mathbb{N} := (\mathbb{N}, +, \cdot, 0, 1)$ natürliche Zahlen mit Addition und Multiplikation.

0. Für $\alpha : \varnothing \to \mathbb{N}$ sei $\sum \alpha := 0$.

1. Sei $\alpha : \{1\} \to \mathbb{N}$ Abbildung. Dann sei $\sum \alpha := \alpha 1$.

2. Sei $I = I_0 \cup \{i_1\}$ endliche Menge mit $i_1 \notin I_0$ und sei $\alpha : I \to \mathbb{N}$ Abbildung. Dann sei $\sum \alpha := (\sum \alpha|I_0) + \alpha i_1$.

Dann ist Σ Summation auf $\mathbb{N}$ (Summation, wie wir sie kennen).

Insbesondere ist für $\alpha : [n+1] \to \mathbb{N}$ mit $n \in \mathbb{N}_+$ stets $\sum \alpha = \sum_{i=1}^{n+1} \alpha i = \sum_{i=1}^{n} \alpha i + \alpha(n+1)$. □

2.2 Multimengen

2.4 Definition (Multimenge)
Eine *natürliche Multimenge* über einer Menge M ist eine Abbildung von M nach $\mathbb{N}$. □

Für eine Menge M ist also $\mathbb{N}^M$ die Menge der (natürlichen) Multimengen zu M.

Ist beispielsweise M ein Warensortiment (Angebot), so ist $\alpha \in \mathbb{N}^M$ ein „Warenkorb" und αx ist die Anzahl der Ware x im Korb α („der Vorrat von x in α").

2.5 Beispiel
Sei $M = \{\text{Apfel, Birne, Zitrone, Banane}\}$.

x	Apfel	Birne	Zitrone	Banane
αx	5	3	2	0
βx	2	7	1	9
$(\alpha+\beta)x$	7	10	3	9

Lokale Addition, „komponentenweise Addition". □

Sind α und β Warenkörbe aus M (das heißt $\alpha, \beta \in \mathbb{N}^M$), so sei die *Summe* von α und β erklärt als

$$\alpha + \beta : M \to \mathbb{N}, \quad x \mapsto \alpha x + \beta x,$$

das heißt $(\alpha+\beta)x = \alpha x + \beta x$ für alle $x \in M$.

Natürliche Ordnung auf Multimengen $(\mathbb{N}, +, 0)$ ist *natürlich geordnet* via

$$x \leq y \iff \exists z \in \mathbb{N} : x + z = y.$$

Also $x \leq x + z$, „Dazu-Addieren ist mehr (oder gleich viel)“.

Wir schreiben $(\mathbb{N}, +, 0, \leq)$, + Addition, 0 Null, $\leq$ Ordnung.

Warnung: $(\mathbb{Z}, +, 0)$ ist nicht natürlich geordnet. Denn $0 < 1$, aber $1 + (-1) = 0$, „Dazu-Addieren kann weniger sein“. (Beispiel: Erbe antreten.)

$(\mathbb{N}^M, +, 0_M)$ mit $0_M : M \to \mathbb{N}, x \mapsto 0$ „Nullabbildung“, leere Multimenge zu M, ist ebenfalls natürlich geordnet via

$$\alpha \leq_M \beta \iff \exists \gamma \in \mathbb{N}^M : \alpha + \gamma = \beta,$$

wobei $\alpha \leq_M \beta :\Leftrightarrow \forall x \in M : \alpha x \leq \beta x$ komponentenweise geordnet für alle $\alpha, \beta \in \mathbb{N}^M$ (Dominanzordnung).

2.6 Beispiel
Sei $M = \{\text{Apfel}, \text{Birne}, \text{Zitrone}, \text{Banane}\}$.

x	Apfel	Birne	Zitrone	Banane
αx	2	5	3	1
βx	4	7	8	1

Dann ist $\alpha x \leq \beta x$ für alle $x \in \{\text{Apfel}, \text{Birne}, \text{Zitrone}, \text{Banane}\}$, also $\alpha \leq \beta$. □

$(\mathbb{N}, \leq)$ ist linear geordnet (das heißt $\forall x, y \in \mathbb{N} : x \leq y \vee y \leq x$). Für $a, b \in \mathbb{N}$ sei $a \wedge b := \min\{a, b\}$ das Minimum von a und b, das heißt (Fallunterscheidungsklammer)

$$a \wedge b := \begin{cases} a & \text{falls } a \leq b, \\ b & \text{falls } b < a, \end{cases}$$

und sei $a \vee b := \max\{a, b\}$ das Maximum, also

$$a \vee b := \begin{cases} b & \text{falls } a \leq b, \\ a & \text{falls } b < a. \end{cases}$$

Dann seien $\alpha \wedge \beta : M \to \mathbb{N}$, $x \mapsto \alpha x \wedge \beta x$ der “Meet” (Schnitt) von α und $\beta \in \mathbb{N}^M$, und $\alpha \vee \beta : M \to \mathbb{N}$, $x \mapsto \alpha x \vee \beta x$ der “Join” (Verbindung) von α und β.

Andere Sprechweisen: $\alpha \wedge \beta$ heißt das Infimum (verallgemeinert „Durchschnitt“ von Mengen) von α und β in $(\mathbb{N}^M, \leq_M)$, und $\alpha \vee \beta$ heißt das Supremum (verallgemeinert „Vereinigung“) von α und β in $(\mathbb{N}^M, \leq_M)$.

Bemerkung:

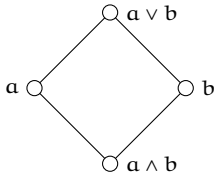
$$\alpha \leq \beta \iff \alpha \vee \beta = \beta \iff \alpha \wedge \beta = \alpha.$$

2.7 Beispiel
Sei wieder $M = \{\text{Apfel}, \text{Birne}, \text{Zitrone}, \text{Banane}\}$.

x	Apfel	Birne	Zitrone	Banane
αx	5	3	2	0
βx	2	7	1	9
$(\alpha + \beta)x$	7	10	3	9
$(\alpha \vee \beta)x$	5	7	2	9
$(\alpha \wedge \beta)x$	2	3	1	0

□

Master-Formel Kontext: Garrett Birkhoff (Harvard, nahe MIT) begründet Ende 1920er, Anfang 1930er die Verbandstheorie ("Lattice Theory"). Das *Supremum* $a \vee b := \sup\{a, b\}$ sei die kleinste obere Schranke von a und b in geordneter Menge $\mathbb{P} = (P, \leq_{\mathbb{P}})$; entsprechend sei das *Infimum* $a \wedge b := \inf\{a, b\}$ die größte untere Schranke von a und b. $\vee, \wedge$ verallgemeinern Konzepte aus Logik, Geometrie, Arithmetik, Ordnungstheorie.



Sei $a : I \to \mathbb{N}^M$ eine Familie von Multimengen zu M, das heißt $a = (a_i)_{i \in I}$ mit $a_i \in \mathbb{N}^M$. Dann seien $\bigvee a$ und $\bigwedge a$ in $\mathbb{N}^M$ definiert durch

$$\bigvee a : M \to \mathbb{N}, \quad x \mapsto \max\{(a_i)x \mid i \in I\}$$

falls I endlich ($= 0$ für $I = \varnothing$), oder $\{(a_i)x \mid i \in I\}$ beschränkt für jedes $x \in M$, sowie

$$\bigwedge a : M \to \mathbb{N}, \quad x \mapsto \min\{(a_i)x \mid i \in I\}$$

für $I \neq \varnothing$. (Also $\bigvee$ verallgemeinert $\bigcup$, und $\bigwedge$ verallgemeinert $\bigcap$.) Wir nennen $\bigvee a =: \sup a$ Join bzw. Supremum von a, $\bigwedge a =: \inf a$ Meet bzw. Infimum von a.

2.8 Satz („Master-Formel")
Sei M Menge und $\alpha, \beta \in \mathbb{N}^M$. Dann gilt:

$$(\alpha \vee \beta) + (\alpha \wedge \beta) = \alpha + \beta.$$

□

Die Probe für Beispiel 2.7 klappt.

BEWEIS
Für alle $x \in M$ gilt:

$$\begin{aligned}((\alpha \vee \beta) + (\alpha \wedge \beta))x &= (\alpha \vee \beta)x + (\alpha \wedge \beta)x \\ &= (\alpha x) \vee (\beta x) + (\alpha x) \wedge (\beta x) \\ &= \begin{cases} \beta x + \alpha x & \text{falls } \alpha x \leq \beta x \\ \alpha x + \beta x & \text{falls } \beta x < \alpha x \end{cases} \\ &= \alpha x + \beta x \\ &= (\alpha + \beta)x. \end{aligned}$$

■

Anwendung (Ausblick): Seien $a, b \in \mathbb{N}_+$ und sei $\mathrm{ggT}(a,b) := a \vee_{\mathcal{T}} b$ der größte gemeinsame Teiler von a und b und sei $\mathrm{kgV}(a,b) =: a \wedge_{\mathcal{T}} b$ das kleinste gemeinsame Vielfache von a und b. Dann folgt:

$$\mathrm{kgV}(a,b) \cdot \mathrm{ggT}(a,b) = a \cdot b.$$

Für eine Multimenge $\alpha \in \mathbb{N}^M$ sei der *Support* (Träger) von α gegeben durch

$$\operatorname{supp} \alpha := \{x \in M \mid \alpha x \neq 0\}$$

(„Menge der Warensorten, die α im Angebot hat“). Es heißt α eine *endliche Multimenge*, falls $\operatorname{supp} \alpha$ endlich ist. Sei $\mathbb{N}^{(M)}$ die Menge der endlichen Multimengen. Für $\alpha \in \mathbb{N}^{(M)}$ bezeichne

$$\#\alpha := \sum \alpha := \sum \alpha|_{\operatorname{supp} \alpha}$$

die *Anzahl* von α, das heißt $\#\alpha = \sum_{x \in M : \alpha x \neq 0} \alpha x$ („Warenanzahl im Warenkorb α“).

2.9 Beispiel
Betrachte:

x	Apfel	Birne	Zitrone	Banane
αx	5	3	2	0

dann ist $\operatorname{supp} \alpha = \{\text{Apfel}, \text{Birne}, \text{Zitrone}\}$ und $\sum \alpha = 5 + 3 + 2 = 10$. □

Es gilt für $\alpha, \beta \in \mathbb{N}^{(M)}$ stets $\alpha + \beta \in \mathbb{N}^{(M)}$ und

$$\#(\alpha + \beta) = \#\alpha + \#\beta.$$

Folglich (Master-Formel anwenden) gilt:

$$\#(\alpha \vee \beta) + \#(\alpha \wedge \beta) = \#\alpha + \#\beta.$$

Für endliche Mengen $A, B \in 2^M$ verallgemeinert dies die Formel

$$\#(A \cup B) + \#(A \cap B) = \#A + \#B.$$

2.3 Monoide und Gruppen

2.10 Definition (Monoid)

1. $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}})$ heißt *Monoid*, falls

$$*_{\mathbb{M}} : M \times M \to M, \quad (x, y) \mapsto x *_{\mathbb{M}} y$$

eine Abbildung ist („2-stellige *Verknüpfung* bzw. *Operation* auf M"), also $x *_{\mathbb{M}} y := *_{\mathbb{M}}(x, y)$, und $1_{\mathbb{M}} \in M$ ist derart, dass gilt:

(Ass) $(x *_{\mathbb{M}} y) *_{\mathbb{M}} z = x *_{\mathbb{M}} (y *_{\mathbb{M}} z)$ für alle $x, y, z \in M$, und

(Neutr) $x *_{\mathbb{M}} 1_{\mathbb{M}} = x = 1_{\mathbb{M}} *_{\mathbb{M}} x$ für alle $x \in M$.

2. Das Monoid $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}})$ heißt *kommutativ*, falls gilt: $\forall x, y \in M : x *_{\mathbb{M}} y = y *_{\mathbb{M}} x$. Für den kommutativen Fall verwenden wir oft $\mathbb{M} = (M, +, 0)$ als Notation, zum Beispiel $\mathbb{N}_{\text{add}} = (\mathbb{N}, +, 0) = (\mathbb{N}, *_{\mathbb{N}_{\text{add}}}, 1_{\mathbb{N}_{\text{add}}})$.

3. $\mathbb{M}$ bildet eine *Gruppe*, falls

$$\forall x \in M \ \exists y \in M : \ x *_{\mathbb{M}} y = 1_{\mathbb{M}} = y *_{\mathbb{M}} x.$$

Es ist y eindeutig bestimmt durch x und wir setzen $x^{-1} := y$ und nennen es das Inverse zu x in $\mathbb{M}$. Dann: $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}}, \cdot^{-1})$ *ist* eine Gruppe.

4. Ist $\mathbb{M} = (M, +, 0)$ ein kommutatives Monoid, so heißt $\mathbb{M}$ *natürlich geordnet*, falls durch

$$x \leq_{\mathbb{M}} y \quad :\Leftrightarrow \quad \exists z \in M : \ x + z = y$$

auf M eine Ordnungsrelation $\leq_{\mathbb{M}}$ definiert ist. □

Beispiele von Monoiden

0. Abbildungsmonoide: Sei P Menge, dann ist $\mathbb{M}\text{aps}\, P := (P^P, \circ, \text{id}_P)$ ein Monoid, welches das (kontravariante) volle *Abbildungsmonoid* auf P heißt.

$$P \xrightarrow{f} P \xrightarrow{g} P \qquad (g \circ f) \qquad\qquad P \xrightarrow{\text{id}_P} P, \quad x \mapsto x$$

1. $(2^T, \cup, \varnothing)$ und $(2^T, \cap, T)$ sind natürlich geordnete Monoide.

2. $\mathbb{N}_{\text{add}} := (\mathbb{N}, +, 0)$ ist natürlich geordnetes kommutatives Monoid, das *additive* Monoid der natürlichen Zahlen.

3. $\mathbb{N}_{\text{mult}} := (\mathbb{N}, \cdot, 1)$ ist natürlich geordnetes kommutatives Monoid, das *multiplikative* Monoid der natürlichen Zahlen.

4. Für $n \in \mathbb{N}_+$ ist $T_n := (\underline{n}, +^n, 0)$ ein natürlich geordnetes kommutatives Monoid, falls

$$x +^n y := \begin{cases} x + y & \text{für } x + y < n, \\ n - 1 & \text{sonst,} \end{cases}$$

für alle $x, y \in \underline{n}$. Es heißt T_n die n-te *Truncation* (Abschneidung) von $\mathbb{N}_{\text{add}}$.

5. Für $n \in \mathbb{N}_+$ bildet $C_n := (\underline{n}, +_n, 0)$ eine kommutative Gruppe, falls

$$x +_n y := \begin{cases} x + y & \text{für } x + y < n, \\ x + y - n & \text{sonst,} \end{cases}$$

für alle $x, y \in \underline{n}$. Es heißt C_n die *zyklische Gruppe* zu $\mathbb{N}_{\text{add}}$ modulo n.

2.4 Kommutative Monoide

Sei $\mathbb{A} = (A, +, 0)$ ein kommutatives Monoid. Zu $n \in \mathbb{N}$ und $a \in A$ definiere

$$n \cdot a := a + \cdots + a \quad (n\text{-fach}),$$

das heißt $\tilde{a} : [n] \to A$, $i \mapsto a$, dann $n \cdot a := \sum \tilde{a}$. Zum Beispiel $2 \cdot a := a + a$, $3 \cdot a := a + a + a$.

Multimengen und Monoide

- $(\mathbb{N}^M, +, 0_M) =: \mathbb{N}^M_{\text{add}}$ ist kommutatives, natürlich geordnetes Monoid aller natürlichen Multimengen zu M,
- $(\mathbb{N}^{(M)}, +, 0_M) =: \mathbb{N}^{(M)}_{\text{add}}$ ist kommutatives, natürlich geordnetes Monoid aller endlichen natürlichen Multimengen zu M.

Sei M Menge. Dann sei

$$\delta^M : M \to \mathbb{N}^{(M)}, \quad m \mapsto \delta^M_m \quad \text{mit} \quad \delta^M_m : M \to \mathbb{N}, \quad x \mapsto \begin{cases} 1 & \text{falls } x = m, \\ 0 & \text{sonst,} \end{cases}$$

die *Dirac-Einbettung* von M in $\mathbb{N}^{(M)}_{\text{add}}$ (δ^M heißt auch „Dirac-Basis“, „Standardbasis“). Abbildung δ^M interpretiert $m \in M$ als „elementare“ Multimenge δ^M_m, also $\operatorname{supp} \delta^M_m = \{m\}$.

2.11 Beispiel
Sei $M = \{\text{Apfel}, \text{Birne}, \text{Zitrone}, \text{Banane}\}$, z. B. Apfel $\overset{\delta^M}{\mapsto} \delta^M_{\text{Apfel}}$.

x	Apfel	Birne	Zitrone	Banane
δ^M_{Apfel}	1	0	0	0
δ^M_{Banane}	0	0	0	1

Sei $\alpha \in \mathbb{N}^M$ gegeben durch:

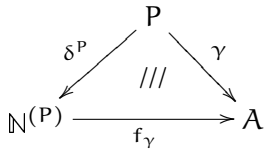
x	Apfel	Birne	Zitrone	Banane
αx	5	3	2	0

dann ist $\alpha = 5 \cdot \delta^M_{\text{Apfel}} + 3 \cdot \delta^M_{\text{Birne}} + 2 \cdot \delta^M_{\text{Zitrone}}$.

(Zu $\alpha \in \mathbb{N}^M$ und $n \in \mathbb{N}$ definieren wir $n \cdot \alpha$ durch $(n \cdot \alpha)x := n \cdot \alpha x$ für alle $x \in M$.) □

2.12 Theorem
Sei $\mathbb{A} = (A, +, \vec{0})$ kommutatives Monoid, sei $\gamma : P \to A$ Abbildung (also $\gamma = (\gamma p)_{p\in P}$ Familie in A). Dann existiert genau eine Abbildung $f_\gamma : \mathbb{N}^{(P)} \to A$ mit

1. $f_\gamma(\alpha + \beta) = f_\gamma\alpha + f_\gamma\beta$ *für alle* $\alpha, \beta \in \mathbb{N}^{(P)}$,
2. $f_\gamma(0_P) = \vec{0}$, *und*
3. $f_\gamma \circ \delta^P = \gamma$, *das heißt:*



□

Beweis

1. Für $\alpha \in \mathbb{N}^{(P)}$ ist stets

$$\alpha = \sum_{p\in P} \alpha p \cdot \delta^P_p := \sum_{p\in \operatorname{supp}\alpha} \alpha p \cdot \delta^P_p,$$

denn für alle $q \in P$ gilt $\alpha q = \sum_{p\in P} \alpha p \cdot \delta^P_p(q)$, und $\delta^P_p(q) = 1$ genau für $q = p$.
Setzt man $\alpha \odot \delta^P : P \to \mathbb{N}^{(P)}$, $p \mapsto \alpha p \cdot \delta^P_p$, dann gilt $\alpha = \sum \alpha \odot \delta^P$.

2. Angenommen, wir haben f_γ wie oben gefunden. Wie sieht f_γ dann aus?

$$\begin{aligned} f_\gamma\alpha &= f_\gamma\Big(\sum_{p\in P} \alpha p \cdot \delta^P_p\Big) \\ &= \sum_{p\in P} \alpha p \cdot f_\gamma(\delta^P_p) \\ &= \sum_{p\in P} \alpha p \cdot \gamma p \qquad (\text{denn } (f_\gamma \circ \delta^P)p = \gamma p) \\ &= \sum \alpha \odot \gamma \end{aligned}$$

für $\alpha \odot \gamma : P \to A$, $p \mapsto \alpha p \cdot \gamma p$.

3. Konstruktion von f_γ (via 2.): Sei $f_\gamma : \mathbb{N}^{(P)} \to A$, $\alpha \mapsto \sum \alpha \odot \gamma$, das heißt

$$f_\gamma\alpha := \sum_{p\in P} \alpha p \cdot \gamma p := \sum_{p\in \operatorname{supp}\alpha} \alpha p \cdot \gamma p.$$

(Also ist $f_\gamma\alpha$ die „gewichtete Summe“ (mit Elementen aus $\mathbb{N}$) von $(\gamma p)_{p\in P}$.)
Es ist $f_\gamma(\alpha + \beta) = f_\gamma\alpha + f_\gamma\beta$, denn $f_\gamma(\alpha + \beta) = \sum(\alpha + \beta) \odot \gamma = \sum(\alpha \odot \gamma + \beta \odot \gamma) = \sum \alpha \odot \gamma + \sum \beta \odot \gamma = f_\gamma\alpha + f_\gamma\beta$. In der Tat ist $(\alpha + \beta) \odot \gamma = \alpha \odot \gamma + \beta \odot \gamma$, da

$$\begin{aligned} ((\alpha + \beta) \odot \gamma)p &= (\alpha + \beta)p \cdot \gamma p \\ &= (\alpha p + \beta p) \cdot \gamma p \\ &\overset{=}{=} \alpha p \cdot \gamma p + \beta p \cdot \gamma p \\ &= (\alpha \odot \gamma)p + (\beta \odot \gamma)p \\ &= (\alpha \odot \gamma + \beta \odot \gamma)p, \end{aligned}$$

wobei „$\overset{!}{=}$“ wegen $(n+m)\cdot a = n\cdot a + m\cdot a$, für $m,n\in\mathbb{N}$ und $a\in A$, gilt.

Es ist $f_\gamma(0_P) = \vec{0}$, denn $f_\gamma(0_P) = \sum_{p\in P} 0_P(p)\cdot\gamma p = \vec{0}$, da $0\cdot a := \vec{0}$.

Es ist schließlich $f_\gamma \circ \delta^P = \gamma$, denn $(f_\gamma\circ\delta^P)p = f_\gamma(\delta^P_p) = \sum_{q\in P}\delta^P_p(q)\cdot\gamma q = \gamma p$. ∎

2.13 Beispiel (siehe Blatt 9, Ü4)
Sei $P = \{\text{Dime}, \text{Quarter}, \text{Dollar}\}$ und $\gamma : P \to \mathbb{N}$ mit

$$\text{Dime} \mapsto 10\ (\text{Cent}),\quad \text{Quarter} \mapsto 25\ (\text{Cent}),\quad \text{Dollar} \mapsto 100\ (\text{Cent})$$

(hier $\mathbb{A} = (\mathbb{N}, +, 0)$). Dann ist $f_\gamma\alpha = \sum_{p\in P}\alpha_p\cdot\gamma p = \alpha_{\text{Dime}}\cdot 10 + \alpha_{\text{Quarter}}\cdot 25 + \alpha_{\text{Dollar}}\cdot 100$ für $\alpha\in\mathbb{N}^P$ (schreibe hier $\alpha_p := \alpha p$). □

Sei $\mathbb{A} = (A, +, \vec{0})$ kommutatives Monoid und sei $A^{(P)} := \left\{\eta\in A^P \mid \operatorname{supp}\eta \text{ endlich}\right\}$, wobei $\operatorname{supp}\eta := \left\{p\in P \mid \eta p \neq \vec{0}\right\}$. Für $\eta\in A^{(P)}$ sei dann vereinbart $\sum\eta := \sum\eta|\operatorname{supp}\eta$.

Wir nennen $f_\gamma : \mathbb{N}^{(P)} \to A$ aus Theorem 2.12, also

$$f_\gamma\alpha = \sum \alpha\odot\gamma = \sum_{p\in P}\alpha p\cdot\gamma p,$$

die *Linearkombinationsabbildung* zu $\gamma : P\to A$ bezüglich $\mathbb{A}$ über $\mathbb{N} := (\mathbb{N}, +, \cdot, 0, 1)$.

Anmerkung: γp heißt manchmal „abstrakter Vektor“, $f_\gamma\alpha$ ist also mit $\mathbb{N}$ gewichtete Summe „abstrakter Vektoren“. $\mathbb{A}$ muss noch erkundet werden („Pfadfinderprinzip“).

2.14 Definition
Sei $\gamma : P\to A$ Abbildung und sei $f_\gamma : \mathbb{N}^{(P)}\to A$ die Linearkombinationsabbildung zu γ bezüglich $\mathbb{A}$ über $\mathbb{N}$.

Ist f_γ surjektiv, so heißt γ *erzeugend* für $\mathbb{A}$ über $\mathbb{N}$ bzw. γ *erzeugt* $\mathbb{A}$ über $\mathbb{N}$.

Ist f_γ injektiv, so heißt γ *unabhängig* für $\mathbb{A}$ über $\mathbb{N}$.

Ist f_γ bijektiv, so heißt γ *Basis* von $\mathbb{A}$ über $\mathbb{N}$. □

2.15 Beispiel
δ^P ist Basis von $\mathbb{N}^{(P)}_{\text{add}}$ über $\mathbb{N}$:

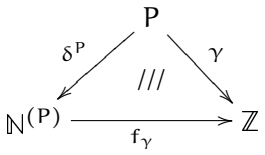
δ^P erzeugt, da für $\alpha\in\mathbb{N}^P$ stets gilt $\alpha = \sum_{p\in P}\alpha p\cdot\delta^P_p$.

δ^P unabhängig, da für $\alpha,\beta\in\mathbb{N}^P$ stets gilt:

$$(\alpha =)\sum\alpha\odot\delta^P = \sum\beta\odot\delta^P (= \beta)\ \Rightarrow\ \alpha = \beta.$$

Kurzum: $f_{\delta^P} = \mathrm{id}_{\mathbb{N}^{(P)}}$. □

2.16 Beispiel
Sei $\mathbb{A} = (\mathbb{Z}, +, 0)$ und $P = \{+,-\}$, sowie $\gamma : P\to\mathbb{Z}$, $+\mapsto 1$, $-\mapsto -1$. Für $\alpha\in\mathbb{N}^P$ sei $\alpha_p := \alpha p$ für alle $p\in P$.

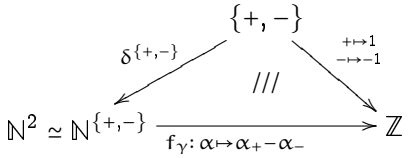


Dann ist $f_\gamma \alpha = \sum_{p \in P} \alpha_p \cdot \gamma p = \alpha_+ \cdot 1 + \alpha_- \cdot (-1)$, das heißt

$$f_\gamma \alpha = \alpha_+ - \alpha_-.$$

$\alpha : \{+,-\} \to \mathbb{N}$, also α_+ mein „Haben“ (Bank oder sonst wo), α_- mein „Soll“ (bei Freunden, Investitionen), dann ist $f_\gamma \alpha = \alpha_+ - \alpha_-$ „Haben minus Soll“, tatsächlicher Besitz (elementare Aktuarsmathematik). Beispiel: $\alpha_+ = 5000$, $\alpha_- = 6500$, dann $f_\gamma \alpha = -1500$.

Situation:



Es ist γ ist erzeugend, aber nicht unabhängig. □

2.17 Definition
Sei f_γ wie oben. Dann heißt

$$\langle \gamma \rangle_{\mathbb{A}} := \operatorname{Im} f_\gamma = f_\gamma(\mathbb{N}^{(P)}) = \left\{ \sum_{p \in P} \alpha p \cdot \gamma p \mid \alpha \in \mathbb{N}^{(P)} \right\}$$

das *Erzeugnis* von γ in $\mathbb{A}$ über $\mathbb{N}$. □

Was ist das Erzeugnis in den Beispielen?

1. Das Erzeugnis von γ in $\mathbb{A}$ über $\mathbb{N}$ im Beispiel 2.13 (Dime, Quarter, Dollar) ist

$$\langle \gamma \rangle_{\mathbb{N}_{add}} = \{0, 10\} \cup \{5 \cdot n \mid n \in \mathbb{N} : n \geq 4\} = \cdot\mathbb{N} \setminus \{5, 15\}.$$

2. Im Beispiel 2.16 (Aktuar) mit $\mathbb{A} = \mathbb{Z}_{add} = (\mathbb{Z}, +, 0)$ ist $\langle \gamma \rangle_{\mathbb{Z}_{add}} = \mathbb{Z}$. Denn sei für $n \in \mathbb{N}$: $\alpha_n : P \to \mathbb{N}$, $+ \mapsto n, - \mapsto 0$, und $\beta_n : P \to \mathbb{N}$, $+ \mapsto 0, - \mapsto n$. Dann ist

$$f_\gamma(\alpha_n) = n \cdot 1 + 0 \cdot (-1) = n \quad \text{und} \quad f_\gamma(\beta_n) = 0 \cdot 1 + n \cdot (-1) = -n.$$

   Also γ erzeugt $\mathbb{Z}$ (über $\mathbb{N}$).

Der Kern einer Abbildung $f : A \to B$ war definiert als $\ker f := \{(t, x) \in A \times A \mid ft = fx\}$. Was ist $\ker f_\gamma$?

1. Im Beispiel 2.13:
   $(\alpha, \beta) \in \ker f_\gamma \Leftrightarrow \alpha_{Dime} \cdot 10 + \alpha_{Quarter} \cdot 25 + \alpha_{Dollar} 100 = f_\gamma \alpha = f_\gamma \beta = \beta_{Dime} \cdot 10 + \beta_{Quarter} \cdot 25 + \beta_{Dollar} 100$. Mit $W\alpha := f_\gamma \alpha$ (Wert von α) ist $(\alpha, \beta) \in \ker f_\gamma \Leftrightarrow W\alpha = W\beta$, das heißt gleicher Wert.

2. Im Beispiel 2.16:
   $(\alpha, \beta) \in \ker f_\gamma \Leftrightarrow W\alpha = W\beta \Leftrightarrow f_\gamma \alpha = f_\gamma \beta$, wobei $W\alpha := f_\gamma \alpha = \alpha_+ - \alpha_-$ (Wert von α, tatsächlicher Besitz von α), das heißt $\alpha_+ - \alpha_- = \beta_+ - \beta_-$, also $\alpha_+ + \beta_- = \beta_+ + \alpha_-$. In der Tat ist (wird noch erläutert)

$$\mathbb{N}_{add}^P / \ker f_\gamma \simeq \mathbb{Z}_{add}.$$

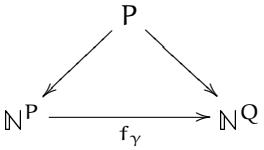
2.18 Beispiel
Sei $P := \{\text{Dime}, \text{Dollar}\}$, $Q := \{\text{Nickel}, \text{Quarter}\}$ und sei $\gamma : P \to \mathbb{N}^Q$ gegeben durch

$$\text{Dime} \mapsto 2\delta^Q_{\text{Nickel}} \quad \text{und} \quad \text{Dollar} \mapsto 10\delta^Q_{\text{Nickel}} + 2\delta^Q_{\text{Quarter}}.$$

Dann ist die Linearkombinationsabbildung $f_\gamma : \mathbb{N}^P \to \mathbb{N}^Q$, $\alpha \mapsto \sum_{p\in P} \alpha_p \cdot \gamma p$, also

$$\begin{aligned} f_\gamma \alpha &= \alpha_{\text{Dime}} \cdot \gamma\text{Dime} + \alpha_{\text{Dollar}} \cdot \gamma\text{Dollar} \\ &= \alpha_{\text{Dime}} \cdot 2\delta^Q_{\text{Nickel}} + \alpha_{\text{Dollar}} \cdot \left(10\delta^Q_{\text{Nickel}} + 2\delta^Q_{\text{Quarter}}\right) \\ &= \left(2\alpha_{\text{Dime}} + 10\alpha_{\text{Dollar}}\right)\delta^Q_{\text{Nickel}} + 2\alpha_{\text{Dollar}} \cdot \delta^Q_{\text{Quarter}}. \end{aligned}$$

Zum Beispiel sei $\alpha_{\text{Dime}} = 3$, $\alpha_{\text{Dollar}} = 5$, dann also $f_\gamma \alpha = (2\cdot 3 + 10\cdot 5)\delta^Q_{\text{Nickel}} + 2\cdot 5 \cdot \delta^Q_{\text{Quarter}} = 56\delta^Q_{\text{Nickel}} + 10\delta^Q_{\text{Quarter}}$.



Hier ist $\gamma : P \to \mathbb{N}^Q$ Abbildung, also $\gamma \in (\mathbb{N}^Q)^P$. Die zugehörige Datenmatrix ist $\mu_\gamma : P \times Q \to \mathbb{N}$, $(p, q) \mapsto (\gamma p)q$.

Es ist $\gamma\text{Dime} = 2\delta^Q_{\text{Nickel}}$, also $(\gamma\text{Dime})\text{Nickel} = 2$, $(\gamma\text{Dime})\text{Quarter} = 0$, und $\gamma\text{Dollar} = 10\delta^Q_{\text{Nickel}} + 2\delta^Q_{\text{Quarter}}$, also $(\gamma\text{Dollar})\text{Nickel} = 10$, $(\gamma\text{Dollar})\text{Quarter} = 2$.

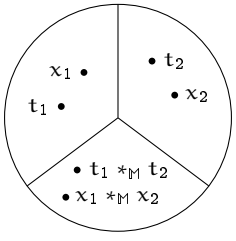
	Nickel	Quarter
Dime	2	0
Dollar	10	2

Es ist γ unabhängig in $\mathbb{N}^Q_{\text{add}}$ über $\mathbb{N}$, da f_γ injektiv ist (Übung); aber γ ist nicht erzeugend, da f_γ nicht surjektiv ist (Übung). □

2.5 Kongruenzrelationen und Morphismen

2.19 Definition
Sei $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}})$ Monoid. Dann ist Θ *Kongruenzrelation* auf $\mathbb{M}$, falls Θ Äquivalenzrelation auf M derart, dass für alle $t_1, t_2, x_1, x_2 \in M$ gilt:

$$t_1 \Theta x_1 \wedge t_2 \Theta x_2 \;\Rightarrow\; t_1 *_{\mathbb{M}} t_2 \,\Theta\, x_1 *_{\mathbb{M}} x_2.$$ □



Veranschaulichung: M/Θ ist zugehörige Partition

Dann ist

$$*_{\mathbb{M}/\Theta} : (M/\Theta) \times (M/\Theta) \to M/\Theta, \quad ([t]\Theta, [x]\Theta) \mapsto [t *_{\mathbb{M}} x]\Theta$$

wohldefiniert und assoziativ, und $\pi_{M/\Theta} : M \to M/\Theta$, $x \mapsto [x]\Theta$ erfüllt

$$\pi_{M/\Theta}(t *_{\mathbb{M}} x) = \pi_{M/\Theta}(t) *_{\mathbb{M}/\Theta} \pi_{M/\Theta}(x)$$

für alle $t, x \in M$. Außerdem sei $1_{\mathbb{M}/\Theta} := [1_{\mathbb{M}}]\Theta = \pi_{M/\Theta}(1_{\mathbb{M}})$. Dann ist $1_{\mathbb{M}/\Theta} *_{\mathbb{M}/\Theta} [x]\Theta = [x]\Theta = [x]\Theta *_{\mathbb{M}/\Theta} 1_{\mathbb{M}/\Theta}$. Somit ist $\mathbb{M}/\Theta := (M/\Theta, *_{\mathbb{M}/\Theta}, 1_{\mathbb{M}/\Theta})$ ein Monoid.

Sei $\varphi := \pi_{M/\Theta}$. Dann ist also $\varphi : M \to M/\Theta$ Abbildung mit

1. $\forall t, x \in M: \ \varphi(t *_{\mathbb{M}} x) = \varphi t *_{\mathbb{M}/\Theta} \varphi x$
   „Bild der Verknüpfung ist Verknüpfung der Bilder“, und

2. $\forall x \in M : \varphi(1_{\mathbb{M}}) = 1_{\mathbb{M}/\Theta}$
   „Bild des neutralen Elements ist neutrales Element des Bildes“.

2.20 Definition
Sind $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}})$, $\mathbb{A} = (A, *_{\mathbb{A}}, 1_{\mathbb{A}})$ Monoide, so ist ein *Morphismus* (bzw. *Monoidmorphismus* oder *Homomorphismus*) von $\mathbb{M}$ nach $\mathbb{A}$ eine Abbildung $\varphi : M \to A$ mit

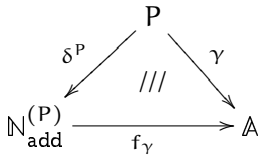
1. $\forall t, x \in M: \ \varphi(t *_{\mathbb{M}} x) = \varphi t *_{\mathbb{A}} \varphi x$, und

2. $\varphi(1_{\mathbb{M}}) = 1_{\mathbb{A}}$.

Wir verwenden die Schreibweise $\varphi : \mathbb{M} \to \mathbb{A}$. Es heißt φ *Isomorphismus* von $\mathbb{M}$ nach $\mathbb{A}$, falls φ bijektiver Morphismus ist, Schreibweise $\varphi : \mathbb{M} \xrightarrow{\sim} \mathbb{A}$. □

2.21 Beispiel

1. $\mathbb{A} = (A, +, \vec{0})$ sei kommutatives Monoid, $\gamma : P \to A$ sei Abbildung (aufgefasst als Familie $\gamma = (\gamma p)_{p \in P}$). Dann ist die Linearkombinationsabbildung f_γ ein Morphismus von $\mathbb{N}_{\text{add}}^{(P)}$ nach $\mathbb{A}$.



   Denn für alle $\alpha, \beta \in \mathbb{N}^{(P)}$ ist

$$\begin{aligned} f_\gamma(\alpha + \beta) &= \sum_{p \in P} (\alpha + \beta)p \cdot \gamma p \\ &= \sum_{p \in P} (\alpha p + \beta p) \cdot \gamma p \\ &= \sum_{p \in P} \alpha p \cdot \gamma p + \sum_{p \in P} \beta p \cdot \gamma p \\ &= f_\gamma \alpha + f_\gamma \beta, \end{aligned}$$

   und $f_\gamma(0_P) = \sum_{p \in P} 0_P(p) \cdot \gamma p = \sum_{p \in P} \vec{0} = \vec{0}$.

2. Ist Θ Kongruenzrelation auf einem Monoid $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}})$, so ist $\pi_{M/\Theta}$ Morphismus von $\mathbb{M}$ nach $\mathbb{M}/\Theta$.

3. Ist φ Isomorphismus eines Monoids $\mathbb{M}$ in ein Monoid $\mathbb{A}$, so ist $\varphi^{-1} : \mathbb{A} \to \mathbb{M}$ ebenfalls ein Isomorphismus.

4. Sei $n \in \mathbb{N}_+$ und $T_n := (\underline{n}, +^n, 0)$ mit $x +^n y := (x + y) \wedge (n - 1)$ für alle $x, y \in \underline{n}$ (das heißt T_n ist das "Truncation"-Monoid zu n). Dann ist

$$\varphi : \mathbb{N} \to \underline{n}, \quad x \mapsto x \wedge (n - 1)$$

ein Morphismus von $\mathbb{N}_{\text{add}}$ nach T_n. □

2.22 Bemerkung
Ist $\varphi : \mathbb{M} \to \mathbb{A}$ Monoidmorphismus, so ist $\ker \varphi$ Kongruenzrelation auf $\mathbb{M}$. □

Beweis
Seien $t_1, t_2, x_1, x_2 \in M$ mit $(t_1, x_1), (t_2, x_2) \in \ker \varphi$ (das heißt $t_1 \Theta x_1 \wedge t_2 \Theta x_2$ für $\Theta := \ker \varphi$). Dann ist also $\varphi t_1 = \varphi x_1$ und $\varphi t_2 = \varphi x_2$, und folglich gilt:

$$\begin{aligned} \varphi(t_1 *_{\mathbb{M}} t_2) &= \varphi t_1 *_{\mathbb{A}} \varphi t_2 \\ &= \varphi x_1 *_{\mathbb{A}} \varphi x_2 = \varphi(x_1 *_{\mathbb{M}} x_2), \end{aligned}$$

woraus $(t_1 *_{\mathbb{M}} t_2, x_1 *_{\mathbb{M}} x_2) \in \ker \varphi$ folgt. ■

Anmerkung: Jede Abbildung $\varphi : A \to B$ hat folgende „Zerlegung"

$$\varphi = \mathrm{id}_{\varphi A, B} \circ \tilde{\varphi} \circ \pi_{A/\ker \varphi},$$

wobei $\tilde{\varphi} : A/\ker \varphi \to \operatorname{Im} \varphi$, $[x]\ker \varphi \mapsto \varphi x$ bijektiv ist ($\operatorname{Im} \varphi := \varphi A$).

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle \pi_{A/\ker\varphi}}\downarrow & /\!/\!/ & \uparrow{\scriptstyle \mathrm{id}_{\varphi A,B}} \\ A/\ker\varphi & \xrightarrow{\tilde{\varphi}} & \operatorname{Im}\varphi \end{array}$$

Analog sei $\varphi : \mathbb{M} \to \mathbb{A}$ Monoidmorphismus. Dann hat φ Zerlegung in Monoidmorphismen

$$\varphi = \mathrm{id}_{\varphi M, A} \circ \tilde{\varphi} \circ \pi_{M/\ker \varphi}$$

und $\tilde{\varphi} : \mathbb{M}/\ker \varphi \to \mathbb{I}\mathrm{m}\, \varphi$ ist sogar Isomorphismus, wobei $\mathbb{I}\mathrm{m} := \mathbb{A}|\varphi M$ die Einschränkung von $\mathbb{A}$ auf φM bezeichne.

$$\begin{array}{ccc} \mathbb{M} & \xrightarrow{\varphi} & \mathbb{A} \\ {\scriptstyle \pi_{M/\ker\varphi}}\downarrow & /\!/\!/ & \uparrow{\scriptstyle \mathrm{id}_{\varphi M,A}} \\ \mathbb{M}/\ker\varphi & \xrightarrow{\tilde{\varphi}} & \mathbb{I}\mathrm{m}\,\varphi \end{array}$$

Dazu fehlt noch eine kleine Definition:

2.23 Definition
Sei $\mathbb{M} = (M, *_M, 1_M)$ Monoid und $U \subseteq M$, dann bildet U *Untermonoid* von $\mathbb{M}$ falls

1. $\forall x, y \in U : \; x *_{\mathbb{M}} y \in U$, und
2. $1_{\mathbb{M}} \in U$.

Die *Einschränkung* von $\mathbb{M}$ auf U sei $\mathbb{M}|U := (U, *_{M|U}, 1_{\mathbb{M}})$ mit $*_{M|U} := *_{\mathbb{M}}|(U^2 \to U)$. □

Ist $U \subseteq M$, so sei $\mathrm{id}_{U,M} : U \to M, x \mapsto x$ die identische Einbettung von U in M. Bildet U Untermonoid eines Monoids $\mathbb{M}$, so ist $\mathbb{M}|U$ wieder ein Monoid und $\mathrm{id}_{U,M} : \mathbb{M}|U \to \mathbb{M}$ ist Morphismus, die *identische Einbettung* von $\mathbb{M}|U$ in $\mathbb{M}$.

Sind $\mathbb{M}$ und $\mathbb{A}$ isomorph (das heißt, es gibt ψ Isomorphismus von $\mathbb{M}$ nach $\mathbb{A}$), so schreiben wir auch $\mathbb{M} \simeq \mathbb{A}$. Es ist

$$\tilde{\varphi} : \mathbb{M}/\ker\varphi \xrightarrow{\sim} \mathbb{I}\mathrm{m}, \quad [x]\ker\varphi \mapsto \varphi x$$

ein Isomorphismus. Also Ergebnis:

$$\mathbb{M}/\ker\varphi \;\simeq\; \mathbb{I}\mathrm{m}\,\varphi.$$

Mengenkerne

2.24 Definition
Seiem $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}})$, $\mathbb{L} = (L, *_{\mathbb{L}}, 1_{\mathbb{L}})$ Monoide und sei φ Morphismus von $\mathbb{M}$ nach $\mathbb{L}$. Dann heißt

$$\mathrm{Ker}\,\varphi := [1_{\mathbb{M}}]\ker\varphi = \{x \in M \mid \varphi x = 1_{\mathbb{L}}\} = \varphi^{-1}\{1_{\mathbb{L}}\}$$

der *Mengenkern* von φ.

Zur besseren Unterscheidung nennen wir $\ker\varphi := \{(t, x) \in M \times M \mid \varphi t = \varphi x\}$ auch den *relationalen Kern* von φ. □

Beispiel-Warnung: Für

$$\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \quad (x_1, x_2) \mapsto 2x_1 + 5x_2$$

gilt $\mathrm{Ker}\,\varphi = \{(0,0)\}$ (da $\varphi^{-1}0 = \{(0,0)\}$), aber $[10]\ker\varphi = \{(0,2),(5,0)\}$ ist nicht aus $\mathrm{Ker}\,\varphi$ konstruierbar!

Notation: Für $U, W \in 2^M$ und $t \in M$ sei

$$U *_{\mathbb{M}} W := \{u *_{\mathbb{M}} w \mid u \in U \wedge w \in W\}$$
$$t *_{\mathbb{M}} U := \{t\} *_{\mathbb{M}} U = \{t + u \mid u \in U\}$$
$$U *_{\mathbb{M}} t := U *_{\mathbb{M}} \{t\} = \{u + t \mid u \in U\}$$

($U *_{\mathbb{M}} W$ heißt „Komplexprodukt“ bzw. „Minkowski-Produkt“ von U mit W).

Beispiel: $\{1,2,3\} + \{4,5\} = \{1+4, 1+5, 2+4, 2+5, 3+4, 3+5\}$, $7 + \{1,8,9\} = \{7+1, 7+8, 7+9\}$.

2.25 Proposition
Bildet $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}})$ eine Gruppe und ist Θ Kongruenzrelation von $\mathbb{M}$, so gilt für $U := [1_{\mathbb{M}}]\Theta := \{x \in M \mid x \Theta 1_{\mathbb{M}}\}$ und $t \in M$ stets

$$t *_{\mathbb{M}} U = [t]\Theta = U *_{\mathbb{M}} t.$$

□

Beweis
Wegen Symmetrie genügt es, $t *_{\mathbb{M}} U = [t]\Theta$ zu zeigen.

Sei $x \in t *_{\mathbb{M}} U$. Dann gibt es $u \in U$ mit $x = t *_{\mathbb{M}} u$. Also ist $t^{-1} *_{\mathbb{M}} x = u \in U = [1_{\mathbb{M}}]\Theta$, das heißt $t^{-1} *_{\mathbb{M}} x \,\Theta\, 1_{\mathbb{M}}$. Folglich (wegen $t \,\Theta\, t$) ist $x = t *_{\mathbb{M}} (t^{-1} *_{\mathbb{M}} x) \,\Theta\, t * 1_{\mathbb{M}} = t$, also $x \in [t]\Theta$.

Sei umgekehrt $x \in [t]\Theta$, das heißt $x \,\Theta\, t$. Wegen $t^{-1} \,\Theta\, t^{-1}$ folgt (da Θ Kongruenzrelation) stets $t^{-1} *_{\mathbb{M}} x \,\Theta\, t^{-1} *_{\mathbb{M}} t = 1_{\mathbb{M}}$. Also ist $t^{-1} * x \in [1_{\mathbb{M}}]\Theta = U$, woraus $x = t *_{\mathbb{M}} (t^{-1} * x) \in t *_{\mathbb{M}} U$ folgt. ∎

Anwendung: Sei $\mathbb{M} \xrightarrow{\varphi} \mathbb{L}$ Morphismus, wobei $\mathbb{M} = (M, *_{\mathbb{M}}, 1_{\mathbb{M}})$ und $\mathbb{L} = (L, *_{\mathbb{L}}, 1_{\mathbb{L}})$ Gruppen bilden. Für $t \in M$ ist dann stets

$$t *_{\mathbb{M}} \operatorname{Ker}\varphi \;=\; [t]\ker\varphi \;=\; \operatorname{Ker}\varphi *_{\mathbb{M}} t.$$

Denn: Setze $U := [1_{\mathbb{M}}]\ker\varphi = \operatorname{Ker}\varphi$ in obige Gleichung ein.

Also gilt hier: $\operatorname{Ker}\varphi$ bestimmt bereits $\ker\varphi$.

2.6 Lösung von Gleichungen

> „I think mathematicians should be more explicit about their thought processes.“
>
> *(– Timothy Gowers)*

(Aus “Gowers's Weblog” (gowers.wordpress.com), “The exchange lemma and Gaussian elimination”.)

Seien A, B Mengen und sei $f : A \to B$ Abbildung. Aufgabe: Löse für $b \in B$ die Gleichung

$$fx = b,$$

das heißt bestimme die “Lösungsmenge”

$$L(fx = b) := \{t \in A \mid ft = b\},$$

das heißt $L(fx = b) = f^{-1}\{b\}$ (kann leicht sein, kann aber auch sehr schwer sein).

Das “Makro” $\ker(f)$ ist definiert als die Menge aller Paare $(a, c) \in A \times A$ mit $fa = fc$,

$$\ker(f) \;=\; \{(a, c) \in A \times A \mid fa = fc\}$$

und heißt der Kern von f; dies ist eine Äquivalenzrelation auf A.

2.26 Beispiel
Sei A Menge von Personen, B Menge von Orten und f ordne jeder Person ihren Geburtsort zu, das heißt Person x wird ihr Geburtsort fx zugeordnet.

Person a ist “äquivalent” zu Person c, falls $fa = fc$ gilt, das heißt falls a und c den gleichen Geburtsort haben. Die “Lösungsmenge” $L(fx = \text{Dresden})$ ist die Menge aller Personen, die in Dresden geboren sind. □

2.27 Beispiel
Betrachte das Gleichungssystem

$$x_1 \cdot 3 + x_2 \cdot 5 = 17$$
$$x_1 \cdot 4 + x_2 \cdot 1 = 12$$

(mit $x = (x_1, x_2)$), also

$$f(x) := (x_1 \cdot 3 + x_2 \cdot 5, x_1 \cdot 4 + x_2 \cdot 1) \quad \text{und} \quad b := (17, 12)$$

und gesucht ist $L(fx = b)$.

Hier fehlen noch A und B! Das heißt f ist nur Vorschrift ohne Definitionsbereich und ohne Wertebereich.

Also sei $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q} \times \mathbb{Q}$ und $x \mapsto fx$ wie oben, $fx = b$ ist „lineares Gleichungssystem“.□

Ist $f : A \to B$ Abbildung und ist $a \in A$ mit $fa = b$, das heißt a ist eine Lösung der Gleichung $fx = b$, dann gilt

$$L(fx = b) = [a]\ker(f).$$

Denn $L(fx = b) = \{t \in A \mid ft = b\} = \{t \in A \mid ft = fa\} = [a]\ker\varphi$.

Für $f : A \to B$ Abbildung, $b \in B$, gilt also:

$$L(fx = b) = \{t \in A \mid ft = b\} = f^{-1}\{b\}$$
$$= \begin{cases} [a]\ker(f) & \text{falls } a \in A \text{ existiert mit } fa = b, \\ \varnothing & \text{sonst.} \end{cases}$$

Lösung von Gleichungen bei Morphismen „Einrenken“ durch den Algebraiker.

Es bilden $\mathbb{A} = (A, *_{\mathbb{A}}, 1_{\mathbb{A}})$ und $\mathbb{B} = (B, *_{\mathbb{B}}, 1_{\mathbb{B}})$ Gruppen und sei $f : \mathbb{A} \to \mathbb{B}$ ein Morphismus (das heißt $f(x *_{\mathbb{A}} y) = fx *_{\mathbb{B}} fy$, $f(1_{\mathbb{A}}) = 1_{\mathbb{B}}$). Sei $b \in B$ und ist $a \in A$ mit $fa = b$, so gilt („homogen“)

$$L(fx = b) = [a]\ker f = a *_{\mathbb{A}} \operatorname{Ker} f = a *_{\mathbb{A}} L(fx = 1_{\mathbb{B}}),$$

wobei $\operatorname{Ker} f := [1_{\mathbb{A}}]\ker f = \{t \in A \mid ft = f1_{\mathbb{A}} = 1_{\mathbb{B}}\}$ und $[a]\ker f := \{t \in A \mid ft = fa\}$.

Insbesondere ist $\ker f$ aus $\operatorname{Ker} f$ rekonstruierbar via

$$\ker f = \{(t, x) \in A \times A \mid t *_{\mathbb{A}} \operatorname{Ker} f = x *_{\mathbb{A}} \operatorname{Ker} f\}.$$

Wichtiger Spezialfall: Es bilden $\mathbb{A} = (A, +, 0_{\mathbb{A}})$ und $\mathbb{B} = (B, +, 0_{\mathbb{B}})$ kommutative Gruppen und sei $\varphi : \mathbb{A} \to \mathbb{B}$ ein Morhpismus. Dann genügt es zur Bestimmung der Lösungsmenge $L(\varphi x = b)$ für $b \in B$, *eine* Lösung zu finden, das heißt ein $a \in A$ mit $\varphi a = b$ zu bestimmen, und außerdem für die *homogene Gleichung* $\varphi x = 0_{\mathbb{B}}$ die Lösungsmenge $L(\varphi x = 0_{\mathbb{B}}) = \operatorname{Ker}\varphi$ zu ermitteln, denn es gilt:

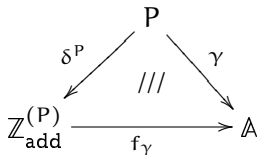
$$L(\varphi x = b) = a + \operatorname{Ker}\varphi = a + L(\varphi x = 0_{\mathbb{B}}),$$

also spezielle Lösung plus homogene Lösungsmenge.

2.7 Kommutative Gruppen

Situation: $\mathbb{A} = (A, +, 0)$ bildet kommutative Gruppe (das heißt „abelsche“ Gruppe) und P sei Menge. Wir nennen $\mathbb{Z}^{(P)}$ die Menge der endlichen „ganzzahligen Multimengen“.

2.28 Satz
Zu $\gamma : P \to A$ Abbildung existiert genau ein Morphismus $f_\gamma : \mathbb{Z}^{(P)}_{\mathrm{add}} \to \mathbb{A}$ mit $f \circ \delta^P = \gamma$.



□

Hierbei ist

$$\delta^P : P \to \mathbb{Z}^{(P)}_{\mathrm{add}}, \quad p \mapsto \delta^P_p \quad \text{wo} \quad \delta^P_p : P \to \mathbb{Z}, \quad q \mapsto \begin{cases} 1 & \text{falls } q = p, \\ 0 & \text{sonst,} \end{cases}$$

“Standardbasis“, “Dirac-Basis” zu $\mathbb{Z}^{(P)}_{\mathrm{add}}$ über $\mathbb{Z} := (\mathbb{Z}, +, \cdot, 0, 1)$ (interpretiert jedes $p \in P$ als Multimenge δ^P_p).

2.29 Beispiel
Sei $P = [3] = \{1, 2, 3\}$, $\mathbb{Z}^P \equiv \mathbb{Z}^3$, $\delta^P_1 \equiv (1, 0, 0)$, $\delta^P_2 \equiv (0, 1, 0)$, $d^P_3 \equiv (0, 0, 1)$, also:

x	1	2	3
$\delta^P_1 x$	1	0	0

x	1	2	3
$\delta^P_2 x$	0	1	0

x	1	2	3
$\delta^P_3 x$	0	0	1

□

Wir nennen f_γ die *Linearkombinationsabbildung* zu γ bezüglich $\mathbb{A}$ über $\mathbb{Z} = (\mathbb{Z}, +, \cdot, 0, 1)$,

$$f_\gamma \lambda := \lambda * \gamma := \sum_{p \in P} \lambda p \cdot \gamma p$$

für $\lambda \in \mathbb{Z}^{(P)}$. Zu $a \in A$ („abstrakter Vektor“) ist λ Koordinatenvektor, falls $\lambda * \gamma = a$.

Konsequenz: Sind f und g Morphismen von $\mathbb{Z}^{(P)}_{\mathrm{add}}$ nach $\mathbb{A}$ mit

$$f \circ \delta^P = g \circ \delta^P, \quad \text{das heißt} \quad \forall p \in P : \ f(\delta^P_p) = g(\delta^P_p).$$

Dann gilt bereits $f = g$.

Denn für $\lambda = \sum_{p \in P} \lambda p \cdot \delta^P_p$ ist stets

$$\begin{aligned} f\lambda &= f\Big(\sum_{p \in P} \lambda p \cdot \delta^P_p \Big) = \sum_{p \in P} f(\lambda p \cdot \delta^P_p) \\ &= \sum_{p \in P} \lambda p \cdot f(\delta^P_p) = \sum_{p \in P} \lambda p \cdot g(\delta^P_p) \\ &= \ldots = g\lambda, \end{aligned}$$

da f und g Morphismen sind.

2.30 Beispiel (Blatt 11 Ü4)
Sei $P := [2]$ und $\alpha \in \mathbb{Z}^{P\times P}$ tabellarisch wie folgt gegeben:

	1	2
1	3	4
2	2	3

Zur ROW-MAP $\gamma := r_\alpha$ bestimme die Koordinatenabbildung $f_\gamma : \mathbb{Z}^P \to \mathbb{Z}^P$, $\lambda \mapsto \lambda * \gamma$, und finde ein $\beta \in \mathbb{Z}^{P\times P}$ derart, dass für $\eta := r_\beta$ die Abbildung f_η zu f_γ invers ist.

Es gilt

$$f_\eta \circ f_\gamma = \mathrm{id}_{\mathbb{Z}^P} \iff f_\eta \circ \gamma = \delta^P,$$

wegen $f_\gamma \circ \delta^P = \gamma$ und der obigen Konsequenz.

Vorgehen: Finde $\eta : P \to \mathbb{Z}^P$, $p \mapsto \eta_p := \eta p$ mit $f_\eta \circ \gamma = \delta^P$ und definiere $\beta : P \times P \to \mathbb{Z}$, $(p, q) \mapsto (\eta_p)q$.

Ausführung: $f_\eta \circ \gamma = \delta^P$ bedeutet für jedes $p \in P$ ist

$$\alpha(p,1)\cdot\eta_1 + \alpha(p,2)\eta_2 = \alpha(p,\cdot) * \eta = \gamma p * \eta = f_\eta(\gamma p) = (f_\eta \circ \gamma)p = \delta^P_p,$$

das heißt

$$3\eta_1 + 4\eta_2 = \delta^P_1,$$
$$2\eta_1 + 3\eta_2 = \delta^P_2.$$

„$3\cdot$“ erste Gleichung und „$4\cdot$“ zweite Gleichung liefert $9\eta_1 + 12\eta_2 = 3\delta^P_1$ und $8\eta_1 + 12\eta_2 = 4\delta^P_2$, also (voneinander abziehen)

$$\eta_1 = 3\delta^P_1 - 4\delta^P_2.$$

„$2\cdot$“ erste Gleichung und „$3\cdot$“ zweite Gleichung gibt $6\eta_1 + 8\eta_2 = 2\delta^P_1$, $6\eta_1 + 9\eta_2 = 3\delta^P_2$, also

$$\eta_2 = -2\delta^P_1 + 3\delta^P_2.$$

Damit ist β die folgende Matrix:

	1	2
1	3	-4
2	-2	3

□

3 Rechenbereiche, Moduln und Vektorräume

3.1 Rechenbereiche

3.1 Definition
Ein *Rechenbereich* bzw. *Semiring* ist ein Quintupel $\mathbb{S} := (S, +, \cdot, 0, 1)$ derart, dass $\mathbb{S}_{\text{add}} := (S, +, 0)$ kommutatives Monoid und $\mathbb{S}_{\text{mult}} := (S, \cdot, 1)$ Monoid ist, sowie folgende Rechenregeln gelten:

Distributivgesetze $\forall x, y, z \in S: \ (x+y)\cdot z = (x\cdot z) + (y\cdot z) \ \wedge \ x\cdot(y+z) = (x\cdot y) + (x\cdot z)$
Vereinbarung „Punktrechnung vor Strichrechnung“: $x\cdot y + x\cdot z := (x\cdot y) + (x\cdot z)$, also $(x+y)\cdot z = x\cdot z + y\cdot z \ \wedge \ x\cdot(y+z) = x\cdot y + x\cdot z$,

Null-Absorption $\forall x \in S: \ x\cdot 0 = 0 = 0\cdot x$, und

Reichhaltigkeit $1 \neq 0$.

Es heißt $+$ die *Addition* und $\cdot$ die *Multiplikation* in $\mathbb{S}$, entsprechend heißt $\mathbb{S}_{\text{add}}$ das *additive Monoid* und $\mathbb{S}_{\text{mult}}$ das *multiplikative Monoid* von $\mathbb{S}$; außerdem nennen wir 0 „die Null von $\mathbb{S}$“ und 1 „die Eins von $\mathbb{S}$“.

Spezialisierungen:

1. $\mathbb{S}$ heißt *kommutativ*, falls $\mathbb{S}_{\text{mult}}$ kommutativ ist.

2. $\mathbb{S}$ heißt *Ring*, falls $\mathbb{S}_{\text{add}}$ eine Gruppe bildet, das heißt zu jedem $x \in S$ existiert genau ein $y \in S$ mit $x + y = 0$; setze dann $-x := y$, $-x$ heißt das *additive Inverse* von x in $\mathbb{S}$ (Notation: $t - x := t + (-x)$).

3. $\mathbb{S}$ heißt *Divisionsring*, falls $(S \setminus \{0\}, \cdot, 1)$ eine Gruppe bildet und $\mathbb{S}$ Ring ist. Also existiert hier zu jedem $x \in S \setminus \{0\}$ genau ein $y \in S \setminus \{0\}$ mit $x\cdot y = 1 = y\cdot x$; setze dann $x^{-1} := y$. Für $t, x \in S \setminus \{0\}$ sei $t\backslash x := t^{-1}\cdot x$ und $x/t := x\cdot t^{-1}$.

4. $\mathbb{S}$ heißt Körper (“field”), falls $\mathbb{S}$ kommutativer Divisionsring ist. Hier bezeichnet $x : t = \frac{x}{t} = t^{-1}\cdot x = x\cdot t^{-1}$ die Division „x geteilt durch t“ (für $t, x \in S \setminus \{0\}$). (Vier Grundrechenarten $+$, $\cdot$, $-$, $:$.)

5. $\mathbb{S}$ heißt *Semikörper* (“semifield”), falls $\mathbb{S}$ kommutativer Semiring und $(S \setminus \{0\}, \cdot, 1)$ eine Gruppe bildet. □

Notation: $\underline{n} := \{0, 1, \ldots, n-1\}$, $[n] := \{1, \ldots, n\}$.

3.2 Beispiel

1. Fall $S = \{0,1\} = \underline{2}$ (kleinster Fall). Verknüpfungstabellen

$+$	0	1
0	0	1
1	1	?

$\cdot$	0	1
0	0	0
1	0	1

$$1+1 = \begin{cases} 0 & ? \\ 1 & ? \\ 2 & ? \end{cases}$$

Fall 1:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\mathrm{GF}\,2 := \mathbb{Z}_2 := \mathbb{S}$ heißt „$\mathbb{Z}$ modulo 2“ (interpretiere $+$ als XOR), “Galois field 2”.

Fall 2:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

$\mathbb{B}_2 := \mathbb{S}$ heißt 2-elementiger boolescher Semiring (interpretiere $+$ als OR).

2. $\mathbb{N} := (\mathbb{N}, +, \cdot, 0, 1)$ der Semiring der natürlichen Zahlen,
3. $\mathbb{Z} := (\mathbb{Z}, +, \cdot, 0, 1)$ Ring der ganzen Zahlen,
4. $\mathbb{Q} := (\mathbb{Q}, +, \cdot, 0, 1)$ Körper der rationalen Zahlen,
5. $\mathbb{R} := (\mathbb{R}, +, \cdot, 0, 1)$ Körper der reellen Zahlen,
6. $\mathbb{C} := (\mathbb{C}, +, \cdot, 0, 1)$ Körper der komplexen Zahlen,
7. $\mathbb{H} := (\mathbb{H}, +, \cdot, 0, 1)$ Divisionsring (Schiefkörper) der *Hamiltonschen Quaternionen*,
8. Oktaven fallen raus (nicht mehr distributiv)...,
9. $\mathbb{Z}_n := (\underline{n}, +_n, \cdot_n, 0, 1)$ ist der Ring „$\mathbb{Z}$ modulo n“ (für $n \in \mathbb{N}$ mit $n \geq 2$). Hier ist $x +_n y := [x+y]_n$ und $x \cdot_n y := [x \cdot y]_n$, wobei zu $z \in \mathbb{N}$ die Zahl $[z]_n$ definiert ist als das eindeutig bestimmte $r \in \underline{n}$, zu dem es ein $t \in \mathbb{N}$ mit $z = r + t \cdot n$ gibt (wobei $+$ und $\cdot$ aus $\mathbb{N}$ genommen werden), also r ist der Rest von z geteilt durch n.

   Anmerkung: Ist n Primzahl, so ist $\mathbb{Z}_n$ ein Körper.

   Ist $n = k \cdot l$ mit $k, l \in \mathbb{N} \setminus \{0,1\}$, so gilt $k \cdot_n l = 0$, also ist dann $\mathbb{Z}_n$ kein Körper.

10. $\mathrm{Trunc}_n := (\underline{n}, +^n, \cdot^n, 0, 1)$ für $n \in \mathbb{N} \setminus \{0,1\}$ und $x +^n y := (x+y) \wedge (n-1)$ und $x \cdot^n y := (x \cdot y) \wedge (n-1)$ (wobei $\wedge$ Minimum) für alle $x, y \in \underline{n}$ ist ein Semiring, der sogenannte n-te *Truncation Semiring* ($\mathrm{Trunc}_2 = \mathbb{B}_2$).
11. „Der (reelle) tropische Semiring“ (“tropical geometry”), in der Optimierung wichtig: $\mathbb{R}_{\mathrm{trop}} := (\mathbb{R} \cup \{\infty\}, +_{\mathrm{trop}}, \cdot_{\mathrm{trop}}, 0_{\mathrm{trop}}, 1_{\mathrm{trop}})$ mit $x +_{\mathrm{trop}} y := x \wedge y := \min\{x, y\}$ (in $(\mathbb{R}, \leq)$), $x \cdot_{\mathrm{trop}} y := x + y$ (in $\mathbb{R}_{\mathrm{add}}$), für alle $x, y \in \mathbb{R} \cup \{\infty\}$, und $0_{\mathrm{trop}} := \infty$, $1_{\mathrm{trop}} := 0$.
12. „Der (reelle) arktische Semiring“ $\mathbb{R}_{\mathrm{arc}} := (\mathbb{R} \cup \{-\infty\}, +_{\mathrm{arc}}, \cdot_{\mathrm{arc}}, 0_{\mathrm{arc}}, 1_{\mathrm{arc}})$ mit $x +_{\mathrm{arc}} y := x \vee y := \max\{x, y\}$ (in $(\mathbb{R}, \leq)$), $x \cdot_{\mathrm{arc}} y := x + y$ (in $\mathbb{R}_{\mathrm{add}}$), für alle $x, y \in R \cup \{-\infty\}$, und $0_{\mathrm{arc}} := -\infty$, $1_{\mathrm{arc}} := 0$.

    $\mathbb{R}_{\mathrm{trop}}$ und $\mathbb{R}_{\mathrm{arc}}$ sind Semikörper.

13. $\mathbb{S}_{\text{Fuzzy}} := ([0,1], \vee, \wedge, 0, 1)$ (Lotfi Zadeh, UC Berkeley) "Fuzzy Semiring", wobei $\vee$ Maximum und $\wedge$ Minimum.

14. $\mathbb{S}_{\text{prob}} := ([0,1], \vee, \cdot, 0, 1)$ „probabilistischer Semiring".

15. $\overline{\mathbb{R}}_{\geq 0} := ([0,\infty], +, \cdot, 0, 1)$, wobei $+$ und $\cdot$ wie in $\mathbb{R}$. □

3.3 Definition
Seien $\mathbb{S} = (S, +, \cdot, 0, 1)$ und $\mathbb{T} = (T, +, \cdot, 0, 1)$ Semiringe. Dann heißt φ *Morphismus* von $\mathbb{S}$ nach $\mathbb{T}$ (*Semiring-Morphismus*), falls $\varphi : S \to T$ Abbildung derart, dass $\varphi : \mathbb{S}_{\text{add}} \to \mathbb{T}_{\text{add}}$ Morphismus und $\varphi : \mathbb{S}_{\text{mult}} \to \mathbb{T}_{\text{mult}}$ Morphismus, das heißt für alle $x, y \in S$ gilt:

$$\varphi(x+y) = \varphi x + \varphi y \qquad \varphi 0 = 0$$
$$\varphi(x \cdot y) = \varphi x \cdot \varphi y \qquad \varphi 1 = 1$$ □

3.4 Beispiel
Sei $n \in \mathbb{N}$, $n \geq 2$ und $\text{Trunc}_n = (\underline{n}, +^n, \cdot^n, 0, 1)$ mit $x +^n y := (x+y) \wedge (n-1)$, $x \cdot^n y := (x \cdot y) \wedge (n-1)$. Dann ist

$$\varphi : \mathbb{N} \to \underline{n}, \quad x \mapsto x \wedge (n-1)$$

Morphismus von $\mathbb{N}$ nach Trunc_n. Speziell für $n = 2$ ist $\mathbb{N} \xrightarrow{\varphi} \mathbb{B}_2$ Morphismus in den 2-elementigen booleschen Semiring. □

3.5 Beispiel
Es ist $\psi : \mathbb{N} \to \underline{n}$, $x \mapsto [x]_n$ (Rest von x geteilt durch n) Morphismus von $\mathbb{N}$ nach $\mathbb{Z}_n$. □

3.2 Projektionen

Was ist eine Projektion (im Kontext von Gruppen)?

Bilde $\mathbb{M} = (M, +, 0)$ eine Gruppe. Ein Morphismus φ von $\mathbb{M}$ in sich heißt *Endomorphismus*. Es ist φ *idempotent*, falls $\varphi^2 := \varphi \circ \varphi$ gleich φ ist, das heißt $\varphi(\varphi x) = \varphi x$ gilt für alle $x \in M$. Eine *Projektion* ist definiert als idempotenter Endomorphismus.

Es heißt $U \subseteq M$ *Normalteiler* von $\mathbb{M}$, falls U Untergruppe von $\mathbb{M}$ bildet und $t + U = U + t$ für alle $t \in M$ gilt.

1. Sei φ ein Endomorphismus von $\mathbb{M}$.

   $\operatorname{Im}\varphi := \varphi M$ bildet Untergruppe von $\mathbb{M}$, denn $\varphi t + \varphi x = \varphi(t+x) \in \operatorname{Im}\varphi$, $0 = \varphi 0 \in \operatorname{Im}\varphi$, $-\varphi x = \varphi(-x) \in \operatorname{Im}\varphi$ (da $\varphi x + \varphi(-x) = \varphi(x + (-x)) = \varphi 0 = 0$ folgt $\varphi(-x) = -\varphi x$).

   $\ker\varphi$ ist Kongruenzrelation (Vorlesung), also $\operatorname{Ker}\varphi$ Normalteiler (Blatt 11 Ü1).

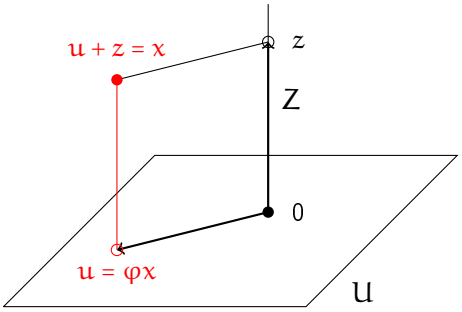
2. Extrem verschiedene Situation zur Projektion:

$$\varphi^2 = 0 \Leftrightarrow \forall x : \varphi(\varphi x) = 0 \Leftrightarrow \forall x : \varphi x \in \operatorname{Ker}\varphi \Leftrightarrow \operatorname{Im}\varphi \subseteq \operatorname{Ker}\varphi.$$

3. Sei U Untergruppe und Z Normalteiler von M.

   Vorbereitung: Für $\psi : U \times Z \to M$, $(u,z) \mapsto u+z$ gilt $\operatorname{Im}\psi = U+Z$ (da $U+Z = \{u+z \mid u \in U \wedge z \in Z\}$), also ψ surjektiv genau dann, wenn $U+Z = M$. Es ist ψ injektiv genau dann, wenn $U \cap Z = \{0\}$, denn: Sei ψ injektiv und $t \in U \cap Z$, dann folgt $\psi(t,0) = t = \psi(0,t)$, also $(t,0) = (0,t)$ und $t = 0$. Sei umgekehrt $U \cap Z = \{0\}$ und $\psi(u,z) = \psi(u',z')$, also $u+z = u'+z'$, dann ist $t := (-u')+u = z'+(-z) \in U \cap Z = \{0\}$, somit $t = 0$, und $(u,z) = (u',z')$.

   Anwendung: Sei $U \oplus Z = M$ (das heißt $U+Z = M$ und $U \cap Z = \{0\}$). Projiziere M mittels Z auf U, das heißt $\pi_{Z,U} := \varphi$ via $\varphi : M \to U$, $\psi(u,z) = u+z \mapsto u$ (da ψ bijektiv), das heißt $\varphi x := u$ für $x = \psi(u,z) = u+z$.



Idee der Projektion $\pi_{Z,U}$

   „Ausbeute“:

   - φ ist *idempotent*, das heißt $\varphi^2 = \varphi$ (da $u+z \overset{\varphi}{\mapsto} u \overset{\varphi}{\mapsto} u$),
   - $\operatorname{Ker}\varphi = Z$ (da $u+z \overset{\varphi}{\mapsto} 0 \Leftrightarrow u = 0$) und $\operatorname{Im}\varphi = U$ (da $u+z \overset{\varphi}{\mapsto} u \Rightarrow \operatorname{Im}\varphi = U$),
   - $0 = 0+0 \overset{\varphi}{\mapsto} 0$, das heißt $\varphi 0 = 0$,
   - $x = \psi(u,z) = u+z$, $x' = \psi(u',z') = u'+z'$, also gibt es $z'' \in Z : z+u' = u'+z''$ (da $Z+u' = u'+Z$, Z Normalteiler), also $\varphi(x+x') = \varphi(u+z+u'+z') = \varphi(u+u'+z''+z') = u+u' = \varphi x + \varphi x'$.

   Also $\pi_{Z,U} = \varphi$ ist Projektion (definiert als idempotenter Endomorphismus) mit $\operatorname{Ker}\varphi = Z$ und $\operatorname{Im}\varphi = U$.

   Außerdem ist $\{\varphi x\} = (x+Z) \cap U$ (da $x = u+z \Rightarrow x+Z = u+Z \overset{\varphi}{\mapsto} \{u\} = \{\varphi x\}$). Anwendung: Für jedes $X \in 2^M$ ist $(X+Z) \cap U = \varphi X$.

4. Sei φ Projektion von M. Dann ist $Z := \operatorname{Ker}\varphi$ Normalteiler und $U := \operatorname{Im}\varphi$ Untergruppe von M. Behauptung: $U \oplus Z = M$.

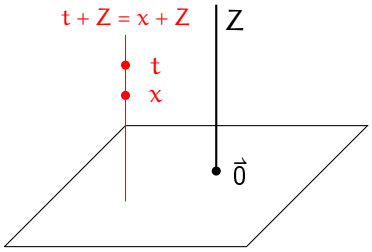
   Subtraktionstrick: $a = (a+(-b))+b$, $a = b+((-b)+a)$. Let's go for it!

   - $M = U+Z$: Begründung: Für $x \in M$ setze $u := \varphi x$ und $z := (-\varphi x)+x$, also $x = u+z$ und $u \in \operatorname{Im}\varphi = U$ und $z \in \operatorname{Ker}\varphi = Z$, da $\varphi z = \varphi((-\varphi x)+x) = \varphi(-\varphi x)+\varphi x = -\varphi(\varphi x)+\varphi x = -\varphi x+\varphi x = 0$, das heißt $x = u+z \in U+Z$.
   - $U \cap Z = \{0\}$: Denn sei $t \in U \cap Z$; da $t \in U = \operatorname{Im}\varphi$ gibt es $x \in M$ mit $t = \varphi x$, also $t = \varphi x = \varphi^2 x = \varphi(\varphi x) = \varphi t$, aber $\varphi t = 0$, da $t \in Z = \operatorname{Ker}\varphi$, also $t = \varphi t = 0$. Das heißt $t \in U \cap Z \Rightarrow t = 0$, also $U \cap Z = \{0\}$.

Es ist $\varphi = \pi_{Z,U}$, denn $\varphi(u+z) = \varphi u + \varphi z = u$ für $u \in U$, $z \in Z$.

3.6 Beispiel (Projektion im Anschauungsraum)
Anschauungsraum modelliert via $\mathbb{M} = (\mathbb{R}^3, +, \vec{0})$, wobei $\vec{0} = (0,0,0)$. Es sei Z die z-Achse und U sei die x-y-Ebene. Dann ist $\Theta_Z := \{(t,x) \in M \times M \mid t + Z = x + Z\}$ Kongruenzrelation zu Z in $\mathbb{M}$, und M/Θ_Z ist Partition von M in Parallelbüschel von Graden. Bezeichnet $\mathbb{U}$ die durch U in $\mathbb{M}$ induzierte Untergruppe, so gilt

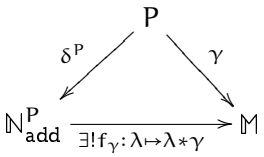
$$\mathbb{U} \simeq \mathbb{M}/Z = \mathbb{M}/\Theta_Z.$$



Addition auf $\mathbb{M}/Z$: Sei $[x] := [x]\Theta_Z = x + Z$ für $x \in M$. Für $x, y \in M$ sei $u, v \in U$ mit $[x] \cap U = \{u\}$, $[y] \cap U = \{v\}$, dann ist $([x] + [y]) \cap U = [x+y] \cap U = \{u+v\}$. □

3.3 Moduln über Semiringen

Wir hatten: Sei f Morphismus von $\mathbb{N}^P_{add}$ nach $\mathbb{M}$ (kommutatives Monoid, P endliche Menge), dann gilt $f = f_\gamma$ für $\gamma := f \circ \delta^P$.



Es ist f_γ die Linearkombinationsabbildung.

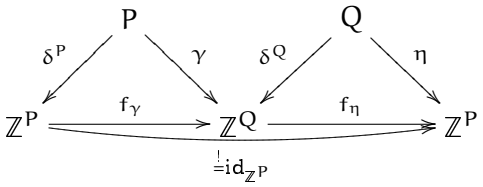
Für jedes $\lambda \in \mathbb{N}^P$ ist $\lambda * \gamma := \sum_{p \in P} \lambda p \cdot \gamma p$, wobei λp „Skalar“, γp „abstrakter Vektor“. Zum Beispiel für $P = [3]$ ist $\lambda * \gamma = \lambda 1 \cdot \gamma 1 + \lambda 2 \cdot \gamma 2 + \lambda 3 \cdot \gamma 3 = \lambda_1\gamma_1 + \lambda_2\gamma_2 + \lambda_3\gamma_3$ (auch üblich als Notation).

Es gilt $f \circ \delta^P = g \circ \delta^P \Rightarrow f = g$, für f, g Morphismen von $\mathbb{N}^P_{add}$ nach $\mathbb{M}$.

Entsprechendes gilt für Morphismen von $\mathbb{Z}^P_{add}$ nach $\mathbb{A}$ (kommutative Gruppe).

Anwendung: Für $M = \mathbb{Z}^Q$ und $\gamma : P \to \mathbb{Z}^Q$, $\eta : Q \to \mathbb{Z}^P$ gilt $f_\eta \circ \gamma = \delta^P \Leftrightarrow f_\eta \circ f_\gamma = \mathrm{id}_{\mathbb{Z}^P}$, denn $(f_\eta \circ f_\gamma) \circ \delta^P = f_\eta \circ (f_\gamma \circ \delta^P) = f \circ \gamma$ und $\mathrm{id}_{\mathbb{Z}^P} \circ \delta^P = \delta^P$. Ist also $(f_\eta \circ \gamma)p = \delta^P_p$ für alle $p \in P$, wobei $(f_\eta \circ \gamma)p = f_\eta(\gamma p) = (\gamma p) * \eta = \sum_{q \in Q} (\gamma p)q \cdot \eta q$, also $\sum_{q \in Q} (\gamma p)q \cdot \eta q = \delta^P_p$ für alle $p \in P$, dann ist $f_\eta \circ f_\gamma = \mathrm{id}_{\mathbb{Z}^P}$.

Speziell für $\gamma = r_\alpha$ mit $\alpha \in \mathbb{Z}^{P\times Q}$ ist dann $\sum_{q\in Q} \alpha(p,q)\cdot \eta q = \delta^P_p \Leftrightarrow f_\eta \circ f_\gamma = \mathrm{id}_{\mathbb{Z}^P}$.



3.7 Beispiel
Sei $P = [3]$. Ist $\alpha(p,1)\cdot\eta 1 + \alpha(p,2)\cdot\eta 2 + \alpha(p,3)\cdot\eta 3 = \delta^P_p$ für alle $p \in [3]$, dann gilt $f_\eta \circ f_\gamma = \mathrm{id}_{\mathbb{Z}^P}$. □

Konstruktion: Sei $\mathbb{M} = (M, +, 0)$ ein kommutatives Monoid und sei $\mathrm{End}\,\mathbb{M}$ die Menge aller Endomorphismen von $\mathbb{M}$. Dann ist

$$\mathbb{E}\mathrm{nd}^\circ\,\mathbb{M} := (\mathrm{End}\,\mathbb{M}, +, \circ, \vec{0}, \mathrm{id}_M)$$

mit $\varphi + \psi : M \to M$, $x \mapsto \varphi x + \psi x$, und $\psi \circ \varphi$ kontravariante Verkettung von φ mit ψ, sowie $\vec{0} : M \to \mathbb{M}$, $x \mapsto 0$, ein Semiring, der *kontravariante Endomorphismen-Semiring*.

Entsprechend ist $\mathbb{E}\mathrm{nd}^*\,\mathbb{M} := (\mathrm{End}\,M, +, *, \vec{0}, \mathrm{id}_M)$ der *kovariante Endomorphismen-Semiring*, wobei $\varphi * \psi$ kovariante Verkettung.

3.8 Beispiel (Semiring-Isomorphismen)

1. $\mathbb{E}\mathrm{nd}^\circ\,\mathbb{N}_{\mathsf{add}} \xrightarrow{\sim} \mathbb{N}$, $\varphi \mapsto \varphi 1$
2. $\mathbb{E}\mathrm{nd}^\circ\,\mathbb{Z}_{\mathsf{add}} \xrightarrow{\sim} \mathbb{Z}$, $\varphi \mapsto \varphi 1$. □

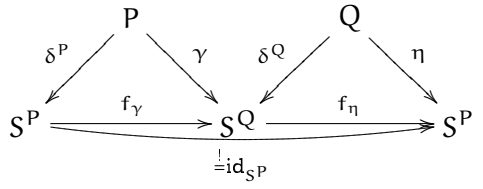
3.9 Definition („Moduln über Semiringen“)
$\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ heißt *(linksseitiger) Semiring-Modul*, falls $\mathbb{M} = (M, +, \vec{0})$ kommutatives Monoid, $\mathbb{S} = (S, +, \cdot, 0, 1)$ Semiring und $\sigma : S\times M \to M$ Abbildung derart, dass $r_\sigma : S \to M^M$, $s \mapsto \sigma(s, \cdot)$ Morphismus von $\mathbb{S}$ nach $\mathbb{E}\mathrm{nd}^\circ\,\mathbb{M}$ bildet.

Ist $\mathbb{S}$ Körper, so heißt $\mathcal{M}$ *Vektorraum*. □

Notation: $sx := s\cdot x := \sigma(s,x)$, „skalare Multiplikation“ des Skalars s mit dem abstrakten Vektor x.

Regeln: $s\cdot(x_1+x_2) = s\cdot x_1 + s\cdot x_2$, $(s_1+s_2)\cdot x = s_1\cdot x + s_2\cdot x$, $s_2\cdot(s_1\cdot x) = (s_2\cdot s_1)\cdot x$, $0\cdot x = \vec{0}$, $s\cdot\vec{0} = \vec{0}$, $1\cdot x = x$ für alle $s_1, s_2, s \in S$ und $x_1, x_2, x \in M$.

Anwendung (ersetze $\mathbb{Z}$ durch $\mathbb{S}$): $f_\eta\circ\gamma = \delta^P \Leftrightarrow f_\eta\circ f_\gamma = \mathrm{id}_{S^P}$, denn $(f_\eta\circ f_\gamma)\circ\delta^P = f\circ\gamma$ und $\mathrm{id}_{S^P}\circ\delta^P = \delta^P$. Also $(f_\eta\circ\gamma)p = \sum_{q\in Q}(\gamma p)q\cdot\eta q = \delta^P_p$ für alle $p \in P$ impliziert $f_\eta\circ f_\gamma = \mathrm{id}_{S^P}$. Speziell für $\gamma = r_\alpha$ mit $\alpha \in S^{P\times Q}$ gilt $\sum_{q\in Q}\alpha(p,q)\cdot\eta q = \delta^P_p \Leftrightarrow f_\eta\circ f_\gamma = \mathrm{id}_{S^P}$.



3.10 Beispiel
Sei $\mathbb{S}$ Semiring, P Menge. Dann ist $\mathrm{Mod}(\mathbb{S}, P) := (\mathbb{S}_{add}^{(P)}, \mathbb{S}, \sigma)$ mit $\sigma : S \times S^{(P)} \to S^{(P)}$, $(s, x) \mapsto sx$, wobei $sx : P \to S$, $p \mapsto s \cdot xp$, ein Semiring-Modul. □

3.11 Definition
Seien $\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ und $\mathcal{M}' = (\mathbb{M}', \mathbb{S}, \sigma')$ Semiring-Moduln. Dann heißt eine Abbildung $f : M \to M'$ eine *lineare Abbildung* von $\mathcal{M}$ nach $\mathcal{M}'$, falls

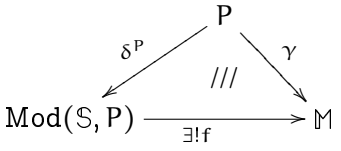
1. $f(\sum \alpha) = \sum f \circ \alpha$, das heißt $f(\sum_{i \in I} \alpha i) = \sum_{i \in I} f(\alpha i)$, für alle $\alpha \in M^I$, I endlich, und
2. $f\sigma(s, x) = \sigma'(s, fx)$, das heißt $f(s \cdot x) = s \cdot fx$, für alle $s \in S$, $x \in M$. □

3.12 Bemerkung
Seien $\mathcal{M}$, $\mathcal{M}'$ und $f : M \to M'$ wie oben. Dann sind folgende Bedingungen äquivalent:

1. f ist lineare Abbildung von $\mathcal{M}$ nach $\mathcal{M}'$,
2. $f(x + y) = fx + fy$ und $f(s \cdot x) = s \cdot fx$ für alle $x, y \in M$ und $s \in S$,
3. f ist Morphismus von $\mathbb{M}$ nach $\mathbb{M}'$ mit $f \circ (r_\sigma s) = (r_{\sigma'} s) \circ f$ für alle $s \in S$,
4. $f(\lambda *^\sigma \gamma) = \lambda *^{\sigma'} (f \circ \gamma)$ für alle $\lambda \in S^{(I)}$ und $\gamma \in M^I$ mit beliebiger Indexmenge I – hierbei sei $S^{(I)} := \{\lambda \in S^I \mid \mathrm{supp}\,\lambda \text{ ist endlich}\}$, $\mathrm{supp}\,\lambda := \{i \in I \mid \lambda i \neq 0\}$ und $\lambda *^\sigma \gamma := \sum_{i \in I} \sigma(\lambda i, \gamma i) := \sum_{i \in \mathrm{supp}\,\lambda} \sigma(\lambda i, \gamma i)$.

Bedingung 4. schreibt man auch als $f(\lambda * \gamma) = \lambda * (f \circ \gamma)$ bzw. $f(\sum_{i \in I} \lambda i \cdot \gamma i) = \sum_{i \in I} \lambda i \cdot f(\gamma i)$. □

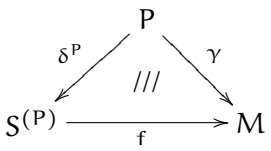
3.13 Theorem
Ist $\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ *Semiring-Modul, so existiert zu jedem* $\gamma : P \to M$ *genau eine lineare Abbildung* f *von* $\mathrm{Mod}(\mathbb{S}, P)$ *nach* $\mathcal{M}$ *mit* $f \circ \delta^P = \gamma$. *Setze* $f_\gamma := f$.



□

Beweis

1. Konstruktion von f: Es ist $f : S^{(P)} \to M$, $\lambda \mapsto \lambda * \gamma$ mit $\lambda * \gamma := \sum_{p \in P} \lambda p \cdot \gamma p$ lineare Abbildung von $\mathrm{Mod}(\mathbb{S}, P)$ nach $\mathcal{M}$ mit $f \circ \delta^P = \gamma$, wobei $\delta^P : P \to S^{(P)}$, $p \mapsto \delta_p^P$ und $\delta_p^P : P \to S$, $q \mapsto \begin{cases} 1 & \text{falls } q = p, \\ 0 & \text{sonst.} \end{cases}$



2. Eindeutigkeit: Sei g lineare Abbildung von $\mathrm{Mod}(\mathbb{S}, P)$ nach $\mathcal{M}$ mit $g \circ \delta^P = \gamma$. Für jedes $\lambda \in S^{(P)}$ ist dann

$$g\lambda = g(\sum \lambda p \cdot \delta_p^P) = \sum \lambda p \cdot g(\delta_p^P) = \sum \lambda p \cdot \gamma p = \lambda * \gamma = f\lambda,$$

da $\lambda = \sum_{p \in P} \lambda p \cdot \delta_p^P$ und $g(\delta_p^P) = (g \circ \delta^P)_p = \gamma p$. ∎

3.14 Definition
Sei $\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ Semiring-Modul, P Menge und sei $\gamma \in M^P$ „Familie (abstrakter) Vektoren“ aus $\mathcal{M}$. Dann heißt

1. γ *unabhängig* in $\mathcal{M}$, falls f_γ injektiv ist,
2. γ *erzeugend* bezüglich $\mathcal{M}$, falls f_γ surjektiv ist,
3. γ *Basis* von $\mathcal{M}$, falls f_γ bijektiv ist. □

3.15 Bemerkung
Für jeden Semiring $\mathbb{S}$ und jede Menge P ist δ^P Basis von $\mathrm{Mod}(\mathbb{S}, P)$, genannt *Standardbasis* bzw. *Dirac-Basis*.

Denn für $\lambda \in S^{(P)}$ gilt stets $(\sum_{p \in P} \lambda p \cdot \delta_p^P)q = \sum_{p \in P} \lambda p \cdot \delta_p^P(q) = \lambda q$ für alle $q \in P$, also $\sum_{p \in P} \lambda p \cdot \delta_p^P = \lambda$, und somit

$$f_{\delta^P}(\lambda) = \lambda * \delta^P = \sum_{p \in P} \lambda p \cdot \delta_p^P = \lambda = \mathrm{id}_{S^{(P)}}(\lambda).$$

Folglich ist $f_{\delta^P} = \mathrm{id}_{S^{(P)}}$ eine Bijektion und damit δ^P eine Basis. □

3.4 Elementare Transformationen

Sei $\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ Modul über einem Ring (das heißt $\mathcal{M}$ ist Semiring-Modul und $\mathbb{S}$ ist Ring) und sei P endliche Menge. $\eta \in M^P$ heißt „elementar Transformierte“ zu $\gamma \in M^P$ bezüglich $\mathcal{M}$, falls eine der drei folgenden Eigenschaften gilt:

1. „Elementar-Addition“: Es existieren $p', p'' \in P$ mit $p' \neq p''$ und $s \in S$ mit

$$\eta : P \to M, \quad p \mapsto \begin{cases} \gamma p' + s \cdot \gamma p'' & \text{falls } p = p', \\ \gamma p & \text{sonst,} \end{cases}$$

das heißt Addition des s-fachen von $\gamma p''$ zu $\gamma p'$: $\eta p' = \gamma p' + s \cdot \gamma p''$.

3.16 Beispiel
Sei $P = [3]$, $\gamma \equiv (\gamma 1, \gamma 2, \gamma 3)$, $\mathbb{S} = \mathbb{Z}$, $s := -5$, $p' = 2$, $p'' = 3$, dann $\eta \equiv (\eta 1, \eta 2, \eta 3) = (\gamma 1, \gamma 2 - 5\gamma 3, \gamma 3)$. □

2. „reguläre Elementar-Streckung“: Es existiert $p' \in P$ und ein in $\mathbb{S}_{\mathrm{mult}}$ invertierbares $s \in S$ mit

$$\eta : P \to M, \quad p \mapsto \begin{cases} s \cdot \gamma p' & \text{falls } p = p', \\ \gamma p & \text{sonst,} \end{cases}$$

das heißt skalare Multiplikation von $\gamma p'$ mit s, also „s-Streckung von $\gamma p'$“: $\eta p' = s \cdot \gamma p'$.

3.17 Beispiel
Sei $P = [2]$, $\mathbb{S} = \mathbb{R}$, $\gamma = (\gamma 1, \gamma 2)$, $p' = 1$, $s = \frac{1}{2}$, dann $\eta = (\frac{1}{2} \cdot \gamma 1, \gamma 2)$. □

3. „Switching“, Vertauschung: Es existieren $p', p'' \in P$ mit $p' \neq p''$ mit

$$\eta : P \to M, \quad p \mapsto \begin{cases} \gamma p'' & \text{falls } p = p', \\ \gamma p' & \text{falls } p = p'', \\ \gamma p & \text{sonst,} \end{cases}$$

das heißt Vertauschung von $\gamma p'$ und $\gamma p''$: $\eta p' = \gamma p''$, $\eta p'' = \gamma p'$.

3.18 Beispiel
Sei $P = [4]$, $\mathbb{S} = \mathbb{N}$, $p' = 1$, $p'' = 3$, $\gamma = (\gamma 1, \gamma 2, \gamma 3, \gamma 4)$ und $\eta = (\gamma 3, \gamma 2, \gamma 1, \gamma 4)$. □

Bemerkung: Ist η elementar Transformatierte zu γ, so ist auch γ elementar Transformatierte zu η. Da:

1. Seien $p', p'' \in P$, $p' \neq p''$ und $s \in S$ mit $\eta p' = \gamma p' + s \cdot \gamma p''$, sowie $\eta p = \gamma p$ falls $p \neq p'$. Dann $\gamma p' = \eta p' - s \cdot \gamma p'' = \eta p' + (-s) \cdot \eta p''$ und $\gamma p = \eta p$ falls $p \neq p'$, das heißt γ ist elementar Transformatierte zu η.

2. Sei $p' \in P$ und $s \in S$ mit s^{-1} existiert (das heißt $s \cdot s^{-1} = 1 = s^{-1} \cdot s$) und $\eta p' = s \cdot \gamma p'$, sowie $\eta p = \gamma p$ falls $p \neq p'$. Dann $\gamma p' = (s^{-1}) \cdot \eta p'$, sowie $\gamma p = \eta p$ falls $p \neq p'$, also ist γ elementar Transformatierte zu η.

3. Seien $p', p'' \in P$ mit $p' \neq p''$ und $\eta p' = \gamma p''$, $\eta p'' = \gamma p'$, sowie $\eta p = \gamma p$ sonst. Dann $\gamma p' = \eta p''$, $\gamma p'' = \eta p'$, sowie $\gamma p = \eta p$ sonst. Also ist γ elementar Transformatierte zu η.

Beobachtung: Ist γ Basis von $\mathcal{M}$ und η elementar Transformatierte zu γ (bezüglich $\mathcal{M}$), so ist auch η Basis von $\mathcal{M}$, das heißt f_γ bijektiv genau dann, wenn f_η bijektiv ist.

Zusatz-Definition: Ist $\mathbb{M} = \mathbb{S}_{\text{add}}^{Q}$ für endliche Menge Q, so heißt $\beta \in S^{P \times Q}$ *elementare Zeilenumformung* von $\alpha \in S^{P \times Q}$ (bzw. „elementar Zeilen-Transformatierte“ zu α) über $\mathbb{S}$, falls $\eta := r_\beta$ (ROW-MAP zu β) elementar Transformierte zu $\gamma := r_\alpha$ (ROW-MAP zu α) bezüglich $\mathrm{Mod}(\mathbb{S}, Q)$ ist.

3.19 Beispiel
Sei $P = Q = [3]$, $\mathbb{S} = \mathbb{Z}$ und sei $\alpha \in S^{P \times Q}$ wie folgt:

α	1	2	3
1	1	-1	3
2	3	2	0
3	0	3	1

Elementar-Addition mit $p' = 2$, $p'' = 1$ und $s = 2$, also $\eta 2 = \gamma 2 + 2 \cdot \gamma 1$. Es ist $\gamma 1 = (1, -1, 3)$, $\gamma 2 = (3, 2, 0)$, $\gamma 3 = (0, 3, 1)$, also $\eta 1 = \gamma 1 = (1, -1, 3)$,

$\eta 2 = \gamma 2 + 2 \cdot \gamma 1 = (3,2,0) + 2 \cdot (1,-1,3) = (3+2, 2+(-2), 0+6) = (5,0,6)$, $\eta 3 = \gamma 3 = (0,3,1)$, und somit:

β	1	2	3
1	1	-1	3
2	5	0	6
3	0	3	1

„Praktiker“, algorithmische Seite:

$$\begin{bmatrix} 1 & -1 & 3 \\ 3 & 2 & 0 \\ 0 & 3 & 1 \end{bmatrix} \overset{\gamma 2+2\cdot\gamma 1}{\rightsquigarrow} \begin{bmatrix} 1 & -1 & 3 \\ 5 & 0 & 6 \\ 0 & 3 & 1 \end{bmatrix} \overset{\eta 3+3\cdot\eta 1}{\rightsquigarrow} \begin{bmatrix} 1 & -1 & 3 \\ 5 & 0 & 6 \\ 3 & 0 & 10 \end{bmatrix}$$

„Zeile $2 + 2 \cdot$ Zeile $1 \mapsto$ Zeile 2“, „Zeile $3 + 3 \cdot$ Zeile $1 \mapsto$ Zeile 3“

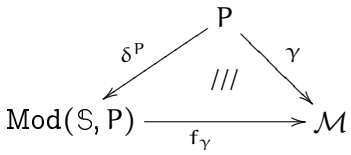
„zeilenweise“ Gauß-Elimination bei $(1,2)$, Spalte 2 enthält überall 0 (wird eliminiert) außer bei $(1,2)$. □

3.5 Lineare Abbildungen und Datenmatrizen

Was wissen wir bereits?

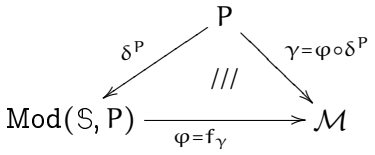
Sei $\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ Semiring-Modul, P Menge. Zu jedem $\gamma : P \to M$ existiert genau eine lineare Abbildung $f : \mathrm{Mod}(\mathbb{S}, P) \to \mathcal{M}$ mit $f \circ \delta^P = \gamma$.

1. „Existenz“: Ist $\gamma \in M^P$, so ist die Linearkombinationsabbildung zu γ bezüglich $\mathcal{M}$ gegeben durch $f_\gamma : S^{(P)} \to M$, $\lambda \mapsto \lambda * \gamma := \sum_{p \in P} \lambda p \cdot \gamma p$. Es ist f_γ lineare Abbildung von $\mathrm{Mod}(\mathbb{S}, P)$ nach $\mathcal{M}$ mit $f_\gamma \circ \delta^P = \gamma$:



   $\mathrm{Mod}(\mathbb{S}, P) = (\mathbb{S}^P_{\mathrm{add}}, \mathbb{S}, \sigma)$, $\sigma(s,x) := s \cdot x$, $(s \cdot x)p := s \cdot xp$, der „frei P-erzeugte Modul über $\mathbb{S}$“, P-faches Coprodukt von $\mathbb{S}_{\mathrm{add}}$. Sehr sloppy: $\mathbb{S}^{(P)} := \mathrm{Mod}(\mathbb{S}, P)$.

2. „Eindeutigkeit“: Ist φ lineare Abbildung von $\mathrm{Mod}(\mathbb{S}, P)$ nach $\mathcal{M}$, so ist φ bereits Linearkombinationsabbildung zu $\gamma := \varphi \circ \delta^P$ bezüglich $\mathcal{M}$, das heißt $\varphi = f_\gamma$ für $\gamma := \varphi \circ \delta^P$:



3. Sind φ und ψ lineare Abbildungen von $\mathrm{Mod}(\mathbb{S}, P)$ nach $\mathcal{M}$, so folgt aus $\varphi \circ \delta^P = \psi \circ \delta^P$ bereits $\varphi = \psi$. Denn: $\varphi = f_\gamma = \psi$ für $\gamma := \varphi \circ \delta^P = \psi \circ \delta^P$ nach 2.

Keine Angst vor Matrizen! $W^{P \times Q}$ Menge der $P \times Q$-Daten-Matrizen über W, typisch $P = [m]$, $Q = [n]$, $W = S$, $\mathbb{S} = (S, +, \cdot, 0, 1)$ Semiring, zum Beispiel $S = \mathbb{R}$.

Beispiel für eine 3×2-Matrix ($m = 3$, $n = 2$) über $\mathbb{R}$:

	1	2
1	3,71	4,5
2	$\sqrt{2}$	$\frac{1}{3}$
3	7	11

Sei $\mathbb{S} = (S, +, \cdot, 0, 1)$ Semiring und seien P, Q, T endliche Mengen. Sind $\lambda, \nu \in S^T$, so sei $\lambda * \nu := \sum_{t \in T} \lambda t \cdot \nu t$ die *Elementarfaltung* von λ mit ν.

3.20 Definition (Matrizenmultiplikation)
Sei α $P \times T$-Matrix, β $T \times Q$-Matrix, dann sei $\alpha * \beta$ $P \times Q$-Matrix definiert durch

$$(\alpha * \beta)(p, q) := \sum_{t \in T} \alpha(p, t) \cdot \beta(t, q) = r_\alpha p * c_\beta q,$$

Matrizenmultiplikation (p-te Zeile, q-te Spalte). □

Wir kennen schon für Semiring-Modul $\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ und endliche Menge P: Zu $\lambda \in S^P$ „Koordinatenvektor“ und $\gamma \in M^P$ Familie abstrakter Vektoren aus $\mathcal{M}$ ist

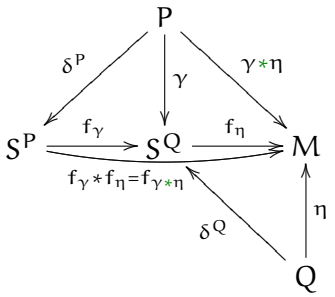
$$\lambda * \gamma := \sum_{p \in P} \lambda p \cdot \gamma p \in M$$

die *Faltung* bzw. *Linearkombination* von λ mit γ, also ein abstrakter Vektor aus $\mathcal{M}$. Gilt $\lambda * \gamma = \nu \in M$, so heißt λ auch Koordinatenvektor von ν zu γ bezüglich $\mathcal{M}$.

Faltung von Vektorfamilien Sei $\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ Semiring-Modul. Für endliche Mengen P und Q sei $\gamma \in (S^Q)^P$ Familie „konkreter Vektoren“ aus S^Q, sowie $\eta \in M^Q$ Familie „abstrakter Vektoren“ aus M. Die *Faltung* der Vektorfamilie γ mit der Familie η ist

$$\gamma * \eta := \delta^P * f_\gamma * f_\eta = f_\eta \circ f_\gamma \circ \delta^P \in M^P$$

($*$ kovariante Verkettung von Abbildungen, $\circ$ kontravariant). Damit ist $f_{\gamma * \eta} = f_\gamma * f_\eta$.



Also $\gamma * \eta = \gamma * f_\eta \in M^P$, das heißt $(\gamma * \eta)p = f_\eta(\gamma p) = \gamma p * \eta = \sum_{q \in Q} (\gamma p)q \cdot \eta q$.
Für $\alpha \in S^{P \times Q}$ sei $\gamma := r_\alpha$, das heißt $(\gamma p)q = \alpha(p, q)$. Dann gilt:

$$(r_\alpha * \eta)p = \sum_{q \in Q} \alpha(p, q) \cdot \eta q.$$

Fall $M = S^R$, $\beta \in S^{Q\times R}$, für $\eta := r_\beta$ gilt dann

$$(r_\alpha * r_\beta)p = \sum_{q\in Q} \alpha(p,q)\cdot\beta(q,\cdot) =: r_{\alpha*\beta}p,$$

das heißt $\alpha * \beta := m(r_\alpha * r_\beta)$.

Zusammenfassung: $\mathcal{M} = (\mathbb{M}, \mathbb{S}, \sigma)$ Semiring-Modul, P, Q, T endliche Mengen.

1. Zu $\lambda \in S^P$, $\gamma \in M^P$ ist $\lambda * \gamma := \sum_{p\in P} \lambda p \cdot \gamma p$ Linearkombination von λ mit γ.
2. Zu $\gamma \in (S^Q)^P$, $\eta \in M^P$ ist $\gamma*\eta := \delta^P * f_\gamma * f_\eta = \gamma * f_\eta = f_\eta \circ \gamma$, und es gilt $(\gamma*\eta)p = \gamma p * \eta$, sowie $f_{\gamma*\eta} = f_\gamma * f_\eta$.
3. Zu $\alpha \in S^{P\times T}$, $\beta \in S^{T\times Q}$ ist $\alpha * \beta := m(r_\alpha * r_\beta)$ das Matrixprodukt, $r_{\alpha*\beta} = r_\alpha * r_\beta$.

3.21 Bemerkung
Zu $\alpha \in S^{P\times Q}$ setze $f_\alpha := f_{r_\alpha}$, die zu α zugehörige lineare Abbildung von S^P nach S^Q, das heißt von $\mathrm{Mod}(\mathbb{S}, P)$ nach $\mathrm{Mod}(\mathbb{S}, Q)$. Dann gilt

$$f_{\alpha*\beta} = f_\alpha * f_\beta. \qquad \square$$

Beweis
Sei $\gamma := r_\alpha$ und $\eta := r_\beta$. Dann ist $r_{\alpha*\beta} = r_\alpha * r_\beta = \gamma * \eta$, also ist $f_{\alpha*\beta} = f_{r_{\alpha*\beta}} = f_{\gamma*\eta} = f_\gamma * f_\eta = f_\alpha * f_\beta$. ∎

Anwendung: $*$ ist assoziativ, denn $f_{(\alpha*\alpha')*\alpha''} = f_{\alpha*\alpha'} * f_{\alpha''} = (f_\alpha * f_{\alpha'}) * f_{\alpha''} = f_\alpha * (f_{\alpha'} * f_{\alpha''}) = f_\alpha * f_{\alpha'*\alpha''} = f_{\alpha*(\alpha'*\alpha'')}$, also $(\alpha * \alpha') * \alpha'' = \alpha * (\alpha' * \alpha'')$.
Es gilt $f_\alpha = f_\beta \Rightarrow \alpha = \beta$, da $\delta^P * f_\alpha = \delta^P * f_{r_\alpha} = r_\alpha$, also $f_\alpha = f_\beta \Rightarrow r_\alpha = r_\beta \Rightarrow \alpha = \beta$.

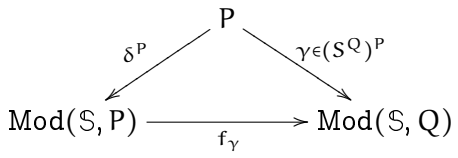
Lineare Abbildungen vs Matrizen Abstrakt: $\mathcal{M} \xrightarrow{f} \mathcal{N}$ lineare Abbildung zwischen Semiring-Moduln, zum Beispiel Vektorräume.

Halb-Konkret: $\mathrm{Mod}(\mathbb{S}, P) \xrightarrow{f} \mathcal{M}$ lineare Abbildung von konkret nach abstrakt.

Konkret: $\mathrm{Mod}(\mathbb{S}, P) \xrightarrow{f} \mathrm{Mod}(\mathbb{S}, Q)$ lineare Abbildung, P, Q endliche Mengen, zum Beispiel $P = [m]$, $Q = [n]$, etwa $P = [3]$, $Q = [4]$.

Zu $\gamma \in (S^Q)^P$ ist der MATRIX-MAKER $m\gamma \in S^{P\times Q}$ definiert durch $(m\gamma)(p,q) := (\gamma p)q \in S$, für $p \in P$, $q \in Q$. Zu $\alpha \in S^{P\times Q}$ ist die ROW-MAP $r_\alpha \in (S^Q)^P$ definiert durch $(r_\alpha p)q := \alpha(p,q) \in S$, für $p \in P$, $q \in Q$. Es gilt $r_{m\gamma} = \gamma$ und $m(r_\alpha) = \alpha$.

1. Sei $\mathbb{S}$ Semiring, P, Q endliche Mengen. Betrachte:



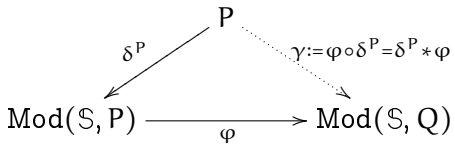
Hierbei ist $f_\gamma : \lambda \mapsto \lambda * \gamma := \sum_{p\in P} \lambda p \cdot \gamma p \in S^Q$ Linearkombinationsabbildung zu γ.

Was ist die zu f_γ gehörige Datenmatrix?

Antwort: Der MATRIX-MAKER tut es! Es ist $\alpha := m\gamma \in S^{P\times Q}$ die zu f_γ gehörige Datenmatrix. Notation $f_\alpha := f_\gamma$, das heißt $f_{m\gamma} = f_\gamma$.

2. Sei $\varphi : \mathrm{Mod}(\mathbb{S}, P) \to \mathrm{Mod}(\mathbb{S}, Q)$ lineare Abbildung. Was ist die zu φ gehörige Datenmatrix?

   Antwort: Klappt schon mit 1., wenn man Folgendes beachtet: Mir fehlt das γ.



   Dann ist $\varphi = f_\gamma = f_{\delta^P * \varphi}$. Also ist

$$\alpha := m\gamma = m(\delta^P * \varphi),$$

   das heißt $\alpha(p, q) = ((\varphi \circ \delta^P)p)q = (\varphi\delta^P_p)q$ für alle $p \in P$, $q \in Q$, die zu φ gehörige Datenmatrix.

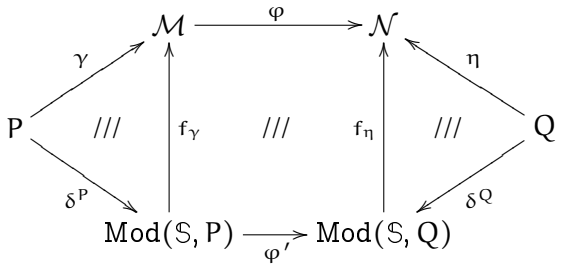
3. Seien $\mathcal{M}$ und $\mathcal{N}$ Semiring-Moduln über $\mathbb{S}$. Was ist die zu einer linearen Abbildung $\varphi : \mathcal{M} \to \mathcal{N}$ gehörige Matrix?

   Antwort: Geht nicht im Allgemeinen!

   Aber: Ist $\gamma \in M^P$ Basis von $\mathcal{M}$ und $\eta \in N^Q$ Basis von $\mathcal{N}$, so ist $\varphi' := f_\gamma * \varphi * f_\eta^{-1}$ lineare Abbbildung von $\mathrm{Mod}(\mathbb{S}, P)$ nach $\mathrm{Mod}(\mathbb{S}, Q)$, und es sei

$$m(\varphi; \gamma, \eta) := m(\delta^P * \varphi') = m(\delta^P * f_\gamma * \varphi * f_\eta^{-1})$$

   die zu $(\varphi; \gamma, \eta)$ gehörige Matrix.



4. Umgekehrt (rein konstruktiv): Sei $\mathbb{S}$ ein Semiring und P, Q endliche Mengen. Was ist die lineare Abbildung zu einer Matrix $\alpha \in S^{P\times Q}$?

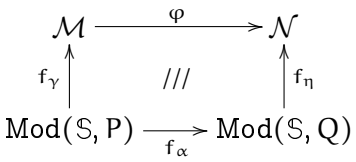
   Antwort: $f_\alpha := f_{r_\alpha}$, das heißt

$$f_\alpha : S^P \to S^Q, \quad \lambda \mapsto \lambda * \alpha,$$

   wobei $\lambda * \alpha := \lambda * r_\alpha$ (Koordinatenvektor mal Datenmatrix, Faltung), $\lambda * \alpha = \sum_{p\in P} \lambda p \cdot \alpha(p, \cdot) \in S^Q$, das heißt $(\lambda * \alpha)q = \sum_{p\in P} \lambda p \cdot \alpha(p, q)$ für alle $q \in Q$.

5. Sei $\alpha \in S^{P\times Q}$ und $\gamma \in M^P$ Basis eines Semiring-Moduls $\mathcal{M}$ (über Semiring $\mathbb{S}$), sowie $\eta \in N^Q$ Basis eines Semiring-Moduls $\mathcal{N}$ (über $\mathbb{S}$). Was ist die hierzu gehörige lineare Abbildung φ von $\mathcal{M}$ nach $\mathcal{N}$?

   Antwort:



   das heißt $\varphi := f_\gamma^{-1} * f_\alpha * f_\eta$.

Sei $\mathcal{M}$ Semiring-Modul, dann sei $\operatorname{End}\mathcal{M}$ die Menge der Endomorphismen von $\mathcal{M}$, das heißt die Menge der linearen Abbildungen von $\mathcal{M}$ nach $\mathcal{M}$. Es ist $\mathbb{E}\mathrm{nd}^*\,\mathcal{M} := (\operatorname{End}\mathcal{M}, +, *, \vec{0}, \mathrm{id})$ ein Semiring, der *covariante Endomorphismen-Semiring* zu $\mathcal{M}$, wo $(\varphi+\psi)x := \varphi x + \psi x$ und $*$ covariante Verkettung.

Für Semiring $\mathbb{S}$ und endliche Menge P sei weiter $\mathrm{Mat}_P\,\mathbb{S} := (S^{P\times P}, +, *, 0, I)$ mit $\alpha + \beta : P\times P \to S,\ (p,q) \mapsto \alpha(p,q) + \beta(p,q)$, und

$$\alpha * \beta : P\times P \to S, \quad (p,q) \mapsto \sum_{t\in P} \alpha(p,t)\cdot\beta(t,q),$$

sowie $0 : P\times P \to S,\ (p,q) \mapsto 0$, und

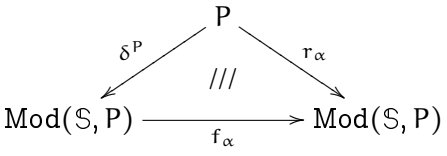
$$I := m\delta^P : P\times P \to S, \quad (p,q) \mapsto \begin{cases} 1 & \text{für } p = q, \\ 0 & \text{sonst,} \end{cases}$$

der *Matrizen-Semiring* der $P\times P$-Matrizen über $\mathbb{S}$.

3.22 Theorem
Sei $\mathbb{S}$ Semiring und P endliche Menge. Dann haben wir einen Isomorphismus

$$\mathbb{E}\mathrm{nd}(\mathbb{S}, P) \xrightarrow{\sim} \mathrm{Mat}_P\,\mathbb{S}, \quad \varphi \mapsto m(\delta^P * \varphi), \quad \alpha \mapsto f_\alpha.$$ □

Beweis
Es ist $f_{\alpha+\beta} = f_\alpha + f_\beta$ und $f_{\alpha*\beta} = f_\alpha * f_\beta$. Außerdem gilt $m(\delta^P * f_\alpha) = m(r_\alpha) = \alpha$, sowie $f_{m(\delta^P*\varphi)} = \varphi$, denn $\delta^P * f_{m(\delta^P*\varphi)} = r_{m(\delta^P*\varphi)} = \delta^P * \varphi$.



■

Kurzes Review

Multimengen Zu $\alpha, \beta \in \mathbb{N}^{(P)}$ sei $\alpha + \beta : P \to \mathbb{N}$, $\alpha p + \beta p$ (Addition der „konkreten Vektoren“ α und β aus $\mathrm{Mod}(\mathbb{N}, P) = (\mathbb{N}_{\mathrm{add}}^{(P)}, \mathbb{N}, \sigma)$, hier σ “for free”, zum Beispiel $5 \cdot \alpha := \alpha+\alpha+\alpha+\alpha+\alpha$), $\alpha \vee \beta : P \to \mathbb{N}$, $p \mapsto \alpha p \vee \beta p := \max\{\alpha p, \beta p\}$, $\alpha \wedge \beta : P \to \mathbb{N}$, $p \mapsto \alpha p \wedge \beta p := \min\{\alpha p, \beta p\}$.

	Tomate	Kartoffel	Zwiebel
α	3	4	1
β	1	100	200
$\alpha + \beta$	$3 + 1 = 4$	$4 + 100 = 104$	$1 + 200 = 201$
$\alpha \vee \beta$	$3 \vee 1 = 3$	$4 \vee 100 = 100$	$1 \vee 200 = 200$
$\alpha \wedge \beta$	$3 \wedge 1 = 1$	$4 \wedge 100 = 4$	$1 \wedge 200 = 1$

Allgemein Sei $\mathbb{S}$ Semiring (Beispiel $\mathbb{S} = \mathbb{N} = (\mathbb{N}, +, \cdot, 0, 1)$), P Menge. Semiring-Modul mit Standardbasis δ^P über $\mathbb{S}$ ist $\mathrm{Mod}(\mathbb{S}, P)$, der P-fache Semiring-Modul (Coprodukt von $\mathbb{S}_{\mathrm{add}}$), „der Standardmodul zu P über $\mathbb{S}$“, frei P-erzeugter Semiring-Modul über $\mathbb{S}$.

Es ist $\mathrm{Mod}(\mathbb{S}, P) := (\mathbb{S}_{\mathrm{add}}^{(P)}, \mathbb{S}, \sigma)$ mit $\sigma : S \times S^{(P)} \to \mathbb{S}^{(P)}$, $(s, \alpha) \mapsto s \cdot \alpha$, wobei $s \cdot \alpha : P \to S$, $p \mapsto s \cdot \alpha p$; $\alpha + \alpha = 2 \cdot \alpha$ – Verdoppelung des Warenkorbes α (auch fast “for free”) ist Konstruktion. Zum Beispiel $\mathbb{R}^n$ (sloppy), das heißt $\mathbb{R}^n := \mathrm{Mod}(\mathbb{R}, [n])$, oft $n \in \{1, 2, 3\}$.

$$\frac{1}{2}(5, 7, 11) \in \mathbb{R}^3 \qquad \frac{1}{2}\begin{pmatrix} 5 \\ 7 \\ 11 \end{pmatrix} \text{ Standard}$$

$$2 \cdot (5, 7, 11) = (2 \cdot 5, 2 \cdot 7, 2 \cdot 11)$$

$$\frac{1}{2} \cdot (5, 7, 11) = (\frac{1}{2} \cdot 5, \frac{1}{2} \cdot 7, \frac{1}{2} \cdot 11)$$

Beispiel-Aufgabe (Theorie): Begründe $s \cdot (\alpha + \beta) = s \cdot \alpha + s \cdot \beta$.

Beweis: Für beliebiges $p \in P$ gilt: $(s \cdot (\alpha+\beta))p = s \cdot (\alpha+\beta)p = s \cdot (\alpha p + \beta p) = s \cdot \alpha p + s \cdot \beta p = (s \cdot \alpha)p + (s \cdot \beta)p = (s \cdot \alpha + s \cdot \beta)p$ (denn $(\alpha + \beta)p := \alpha p + \beta p$, $(s \cdot a)p := s \cdot \alpha p$).

Kerne und Partitionen Sei $f : A \to B$ Abbildung, $\ker f := \{(t, x) \in A \times A \mid ft = fx\} \in \mathrm{Eq}\, A$, $A/\ker f$ Partition der Äquivalenzklassen, $[t]\Theta := t\Theta := \{x \in A \mid t\Theta x\}$ $((t, x) \in \Theta)$, $\Theta \in \mathrm{Eq}\, A$. Beispiel für $A = [6] = \{1, \ldots, 6\}$, $\Theta \in \mathrm{Eq}\, A$, $A/\Theta = \{\{1, 2\}, \{3\}, \{4, 5, 6\}\} \in \mathrm{Part}\, A$.

Θ	1	2	3	4	5	6
1	×	×				
2	×	×				
3			×			
4				×	×	×
5				×	×	×
6				×	×	×