Algebra

1 Mengen

1.1 Operationen

$\|A\|$	Anzahl der Elemente von A (Mächtigkeit, Betrag, Kardinalität)
$\wp(A)$	Potenzmenge von X ($\rightarrow \|\wp(A)\| = 2^{\|A\|}$)
$A \subseteq B$	wenn jedes Element von A auch Element von B ist.
$A = B$	$\leftrightarrow (A \subseteq B$ und $B \subseteq A)$
$A \cup B$	$= \{x \mid x \in A$ oder $x \in B\}$ (Vereinigung)
$A \cap B$	$= \{x \mid x \in A$ und $x \in B\}$ (Schnitt)
$A \setminus B$	$= \{x \mid x \in A$ und $x \notin B\}$ (Differenz)
$A \vartriangle B$	$= (A \cup B) \setminus (A \cap B)$ (Symmetrische Differenz)
$A \times B$	$= \{(a,b) \mid a \in A, b \in B\}$ (Produkt)
$\overline{A}$	$= M \setminus A$ (mit $A \subseteq M$) (Komplement in M)
$\binom{A}{k}$	Menge aller k–elementigen Teilmengen von A $\Rightarrow \left\|\binom{A}{k}\right\| = \binom{\|A\|}{k}$

1.2 Gesetze

$\cup$, $\cap$ und $\vartriangle$ sind kommutativ und assoziativ.

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

$$A \cap \bigcup_{i \in I} B_i = \bigcup_{i \in I} (A \cap B_i) \qquad A \cup \bigcap_{i \in I} B_i = \bigcap_{i \in I} (A \cup B_i)$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \quad \overline{A \cap B} = \overline{A} \cup \overline{B} \quad {\scriptstyle (A,B \subseteq M)}$$

$$\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i} \quad \overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i} \quad {\scriptstyle (A_i \subseteq M)}$$

1.3 Eigenschaften

Zwei Mengen A und B heißen **gleichmächtig** (von gleicher **Kardinalität**), wenn es eine bijektive Abbildung (s. Abschnitt **??**) zwischen ihnen gibt. (Schreibweise: $A \sim B$)

Eine Menge A heißt **endlich**, wenn es ein $n \in \mathbb{N}$ gibt mit $A \sim \{1, 2, \cdots, n\}$.

Eine Menge A heißt **abzählbar**, wenn $A \sim \mathbb{N}$ gilt. Insbesondere sind $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ abzählbar, $\mathbb{R}$ und $\mathbb{C}$ sind nicht abzählbar (überabzählbar).

1.4 Graph

geg: Mengen V, $E \subseteq \binom{V}{2}$

(V, E) ist ein **schlichter Graph** mit **Eckenmenge** V und **Kantenmenge** E.

$(V, \binom{V}{2})$ ist ein **vollständiger Graph** mit Eckenmenge V.

1.5 Partition

Eine **Partition** (Klasseneinteilung) Π einer Menge M ist eine Menge mit den Eigenschaften:

- $\Pi \subseteq \wp(M) \setminus \{\varnothing\}$
- je zwei verschiedene Mengen aus Π sind disjunkt
- $\bigcup \Pi = M$

$\Rightarrow$ Jedes $m \in M$ ist Element von genau einer $T \in \Pi$.

2 Relationen

2.1 Definition

Eine (binäre) **Relation** auf einer Menge A ist $R \subseteq A \times A$.

Die Elemente von $A^n = A \times A \times \cdots \times A$ (n Faktoren) sind n–Tupel mit Elementen aus A. Teilmengen von A^n heißen **n–stellige Relationen** auf A.

Schreibweise: Für $(a, b) \in R$ schreibt man auch aRb oder $R(a, b)$.

Binäre Relationen nennt man auch **gerichtete Graphen** mit Eckenmenge A und Kantenmenge R (R besteht aus Paaren, nicht Mengen!).

2.2 Operationen

$R \circ Q$	$:= \{(a,c) \mid \exists(b \in A)(aRb \wedge bQc)\}$ $_{(R,Q \subseteq A \times A)}$ (Relationenprodukt)
R^{-1}	$:= \{(b,a) \mid aRb\}$ $_{(R \subseteq A \times A)}$
id_A, $\triangle_A$	$:= \{(a,a) \mid a \in A\}$ (Identische Relation auf A)

$(R^{-1})^{-1} = R$ $\qquad$ $(R \circ Q)^{-1} = Q^{-1} \circ R^{-1}$

2.3 Eigenschaften

Eine Relation $R = A \times A$ heißt

reflexiv:	$aRa \; \forall \, a \in A$, bzw. $\mathrm{id}_A \subseteq R$ (Hauptdiagonale vollst.)
irreflexiv:	$(a,a) \notin R \; \forall \, a \in A$, bzw. $\mathrm{id}_A \cap R = \varnothing$ (Hauptdiagonale leer)
symmetrisch:	$aRb \rightarrow bRa$, bzw. $R = R^{-1}$
antisymmetrisch:	$(aRb \wedge bRa) \Rightarrow a = b$, bzw. $R \cap R^{-1} \subseteq \mathrm{id}_A$
transitiv:	$(aRb \wedge bRc) \rightarrow aRc$, bzw. $R \circ R \subseteq R$
konnex:	$R \cup R^{-1} = A \times A$

2.4 Ordnung

Typen

Eine Relation $R \subseteq A \times A$ ist ein(e)

- **Ordnung** (Halbordnung, Partialordnung), wenn sie reflexiv, transitiv und antisymmetrisch ist (z. B. "kleiner-gleich").
- **strikte Ordnung**, wenn sie irreflexiv, transitiv und antisymmetrisch ist (z. B. "kleiner-als").
- **lineare Ordnung**, wenn sie eine konnexe Ordnungsrelation ist.
- **Wohlordnung**, wenn sie eine lineare Ordnung ist, bei der jede nichtleere Teilmenge der Grundmenge ein kleinstes Element hat (z. B. $\leq$-Relation auf $\mathbb{N}$).
- **Verband**, wenn jede zweielementige Teilmenge $a, b \in A$ ein Supremum $a \vee b$ und ein Infimum $a \wedge b$ hat.
- **Vollständiger Verband**, wenn jede Teilmenge von A ein Supremum und ein Infimum hat.

Symbolik

(A, R) mit $R \subseteq A \times A$ ist eine **geordnete Menge**.

Beliebtes **Symbol**: "$\leq$" (infix) für Ordnungsrelationen, "$<$" für die zugehörige strikte Ordnung $\leq \setminus \mathrm{id}$.

Spezielle Elemente

Sei $(M, \leq)$ eine geordnete Menge, $T \subseteq M$ und $t \in T$.

t ist ein **minimales Element** von T, wenn $(s \leq t \rightarrow s = t) \; \forall \, s \in T$.

t ist das **kleinste Element** von T, wenn $t \leq s \; \forall \, s \in T$.

$u \in M$ heißt **untere Schranke** von T, wenn $u \leq s \; \forall \, s \in T$.

Dual dazu definiert man **maximales Element**, **größtes Element** und **obere Schranke**.

Gibt es eine größte untere Schranke von T, heißt diese **Infimum** ($\inf T$, $\wedge T$).

Gibt es eine kleinste obere Schranke von T, heißt diese **Supremum** ($\sup T$, $\vee T$).

Wohlordnung als Beweisprinzip

Wenn man zeigen will, dass eine Aussage $S(n)$ für alle natürlichen Zahlen gilt, nutzt man aus, dass es, wenn überhaupt, ein kleinstes Gegenbeispiel geben müßte und zeigt dann, das sich aus dessen Existenz ein Widerspruch ergibt.

2.5 Transitive Hülle

Die **transitive Hülle** einer Relation A ist die kleinste transitive Relation, die A enthält.

$A^+ = \mathrm{tra}(A) = A \cup A^2 \cup A^3 \cup \ldots$ (bis höhere Potenzen keine neuen Einträge mehr liefern)

2.6 Äquivalenz

Ist eine Relation reflexiv, transitiv und symmetrisch, so ist sie eine **Äquivalenz**.

geg: Äquivalenzrelation Θ auf M, $m \in M$

Äquivalenzklasse von m bezügl. Θ: $[m]\Theta := \{n \in M | \; m \Theta n\}$

$\Rightarrow m \in [m]\Theta$ (da Θ refl.) $\quad n \in [m]\Theta \leftrightarrow m \in [n]\Theta$ (da Θ symm.) $\quad m \in [n]\Theta \rightarrow [m]\Theta \subseteq [n]\Theta$

Verschiedene Äquivalenzklassen sind disjunkt, d. h. $[m]\Theta \cap [n]\Theta \neq \varnothing \rightarrow [m]\Theta = [n]\Theta$.

$\Rightarrow$ Die Faktormenge $^{M}/_{\Theta} = \{[m]\Theta | \; m \in M\}$ ("M nach Theta") ist eine Partition von M.

3 Formaler Kontext

3.1 Definition

Ein **formaler Kontext** (G, M, I) besteht aus Mengen G und M und einer binären Relation $I \subseteq G \times M$.

$\Rightarrow$ Mathematische Repräsentation einer Kreuztabelle mit Gegenständen G und Merkmalen M.

3.2 Operationen

Sei $A \subseteq G$, $B \subseteq M$.

$A' := \{m \in M \big| \; (g, m) \in I \; \forall \, g \in A\}$ ($\Rightarrow$ Gemeinsame Merkmale der Gegenstände aus A)

$B' := \{g \in G \big| \; (g, m) \in I \; \forall \, m \in B\}$ ($\Rightarrow$ Alle Gegenstände, die die Merkmale B haben)

3.3 Gesetze

Für $A, A_1, A_2 \subseteq G$ und $B, B_1, B_2 \subseteq M$ gilt:

$A_1 \subseteq A_2 \to A_2' \subseteq A_1'$	$B_1 \subseteq B_2 \to B_2' \subseteq B_1'$
$A \subseteq A''$	$B \subseteq B''$
$A' = A'''$	$B' = B'''$
$(A_1 \cup A_2)' = A_1' \cap A_2'$	$(B_1 \cup B_2)' = B_1' \cap B_2'$

3.4 Begriff

Ein **formaler Begriff** von (G, M, I) ist ein Paar (A, B) mit $A \in G$, $B \in M$, $A' = B$ und $B' = A$. Die Menge aller Begriffe von (G, M, I) kann durch

$$(A_1, B_1) \leq (A_2, B_2) \leftrightarrow A_1 \subseteq A2 \qquad (\to B_2 \subseteq B_1)$$

geordnet werden. Sie bildet mit dieser Ordnung einen vollständigen Verband, den **Begriffsverband**.

$(A_1, B_1) \wedge (A_2, B_2) = (A_1 \cap A_2, (B_1 \cup B_2)'')$ (größter gemeinsamer Unterbegriff)

$(A_1, B_1) \vee (A_2, B_2) = ((A_1 \cup A_2)'', B_1 \cap B_2)$ (kleinster gemeinsamer Oberbegriff)

4 Abbildungen

4.1 Definition

Eine **Abbildung** von einer Menge A in eine Menge B ist ein Tripel (A, B, f), wobei f eine Relation ist, die folgende Bedingung erfüllt: Zu jedem Element $a \in A$ gibt es genau ein $b \in B$ mit $(a, b) \in f$. Man nennt A den **Definitionsbereich** (*domain*), B den **Wertebereich** (*codomain*) und f den **Graphen** der Abbildung. b ist das **Bild** von a unter Abbildung f.

Schreibweise: $f : A \to B$; für $(a, b) \in f$ schreibt man $f(a) = b$ oder $a \overset{f}{\mapsto} b$.

4.2 Eigenschaften

$f : A \to B$ heißt

injektiv: (*one-to-one*)	$\forall\, a_1, a_2 \in A, a_1 \neq a_2 \to f(a_1) \neq f(a_2) \quad \Rightarrow \lvert A\rvert \leq \lvert B\rvert$
surjektiv: (*onto*)	zu jedem $b \in B$ existiert ein $a \in A$ mit $f(a) = b \quad \Rightarrow \lvert A\rvert \geq \lvert B\rvert$
bijektiv:	f ist zugleich injektiv und surjektiv $\quad \Rightarrow \lvert A\rvert = \lvert B\rvert$

4.3 Operationen

B^A	Menge aller Abbildungen von A nach B. $\Rightarrow \left\lvert B^A \right\rvert = \lvert B\rvert^{\lvert A\rvert}$
$\mathrm{id}_A : A \to A$	**identische Abbildung** (Identität) von A mit $\mathrm{id}_A(a) = a \;\forall\, a \in A$
$f_{\mid T}(t)$	$:= f(t) \;\forall\, t \in T$ mit $T \subseteq A$ (**Einschränkung** von f auf T)
$f^{-1}(Y)$	$:= \{a \in A \mid f(a) \in Y\}$ mit $Y \subseteq B$ (**Urbildmenge** von Y unter f)
$(g \circ f)(a)$	$:= g(f(a)) \;\forall\, a \in A$ mit $f : A \to B$, $g : B \to C$ und $g \circ f : A \to C$ (**Komposition**)
$f(T)$	$:= \{f(t) \mid t \in T\}$ mit $T \subseteq A$ (**Bild** von T unter f)
$\mathrm{Im} f$	$:= f(A) = \{f(a) \mid a \in A\}$ (**Bild**)
$\ker f$	$:= \{(a_1, a_2) \mid a_1, a_2 \in A \wedge f(a_1) = f(a_2)\}$ (**Kern**)

4.4 Gesetze

Komposition: $\circ$ ist assoziativ, aber nicht kommutativ.

Schubfachprinzip: Ist $f : A \to B$ und $|A| > |\mathrm{Im} f|$, dann ist f nicht injektiv.

$\ker f$ ist eine Äquivalenzrelation auf A. $\left|{}^{A}/_{\ker f}\right| = |\mathrm{Im} f|$, denn $[a]\ker f \mapsto f(a)$ ist bijektiv.

$$\left.\begin{array}{l} f \text{ ist injektiv} \leftrightarrow \exists\, g : B \to A\ (g \circ f = \mathrm{id}_A) \\ f \text{ ist surjektiv} \leftrightarrow \exists\, g : B \to A\ (f \circ g = \mathrm{id}_B) \\ f \text{ ist bijektiv} \leftrightarrow \exists\, g : B \to A\ (g \circ f = \mathrm{id}_A \wedge f \circ g = \mathrm{id}_B) \end{array}\right\} g : \text{inverse Abbildung zu } f$$

5 Permutationen

5.1 Definition

Eine **Permutation** ist eine bijektive Abbildung einer Menge A auf sich selbst.

Die **symmetrische Gruppe** S_A oder $\mathrm{Sym}(A)$ ist die Menge aller Permutationen von A. Sie wird im Fall $A = \{1, 2, ..., n\}$ auch mit S_n bezeichnet.

5.2 Schreibweise

$A = \{a_1, a_2, \ldots, a_n\}$, $f : A \to A$, f ist Permutation auf A.

$$f = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ f(a_1) & f(a_2) & \cdots & f(a_n) \end{pmatrix}$$

Zyklenschreibweise:

$$f = \underbrace{\big(a_i\ f(a_i)\ f(f(a_i))\ \ldots\big)}_{1.Zyklus}\ \underbrace{\big(a_j\ f(a_j)\ f(f(a_j))\ \ldots\big)}_{2.Zyklus} \cdots$$

Einer-Zyklen werden weggelassen!

5.3 Gesetze

Die symmetrische Gruppe S_n hat $n!$ Elemente.

Die Hintereinanderausführung $g \circ f$ zweier Permutationen f und g ist wieder eine Permutation.

Die Ordnung einer Permutation ist das kgV der Längen aller Zyklen.

6 Algebraische Strukturen

6.1 Operation

Eine (**einsortige Operation** auf eine **Trägermenge** A der **Stelligkeit** $n \in \mathbb{N}$ ist eine Abbildung $f : A^n \to A$.

Stelligkeitsabbildung: $n = \sigma(f)$

6.2 Signatur

Eine **Signatur einsortiger Algebren** (auch **Rangalphabet**) $\Sigma := (\mathcal{F}, \sigma)$ besteht aus der Menge der **Operationssymbole** $\mathcal{F}$, sowie einer Abbildung $\sigma : \mathcal{F} \to \mathbb{N}$, die den Elmtenten aus $\mathcal{F}$ ihre **Stelligkeit** zuordnet.

Typ einer Algebra: Folge der Stelligkeiten der Operationen aus $\mathcal{F}$.

6.3 Unteralgebra

Sei $\underline{A} = (A, \mathcal{F})$ eine Algebra. Eine Teilmenge $U \subseteq A$ bildet eine **Unteralgebra** $(U, \mathcal{F})$ von $\underline{A}$, wenn sie unter den Operationen aus $\underline{A}$ **abgeschlossen** ist, d. h., wenn gilt:

$$\forall f \in \mathcal{F} : a_1, \ldots, a_{\sigma(f)} \in U \;\rightarrow\; f(a_1, \ldots, a_{\sigma(f)}) \in U$$

6.4 Typen

Binar (Gruppoid): Algebra vom Typ (2)

Halbgruppe: Gruppoid $(H, \circ)$ mit assoziativer Operation $\circ$

Es gilt das Potenzgesetz $x^a \circ x^b = x^{a+b}$

$< x >_H := \{x^n \big| n \in \mathbb{N}^+\}$ $(x \in H)$ ist die **durch x erzeugte** Unterhalbgruppe von H. Ist $\big| < x > \big|$ endlich, so heißt $\big| < x > \big|$ **Ordnung** des Elementes x (und aller anderen Elemente aus $< x >$).

Monoid: Halbgruppe mit neutralem Element

Gruppe: Algebra $(G, \cdot, ^{-1}, e)$ vom Typ $(2, 1, 0)$ mit:

- $(G, \cdot, e)$ ist ein Monoid
- $(\forall g \in G)\; g \cdot g^{-1} = g^{-1} \cdot g = e$

Durch $\cdot$ sind $^{-1}$ und e eindeutig bestimmt. $\rightarrow$ Definition der Gruppe durch eine Halbgruppe $(G, \cdot)$ mit bes. Eigenschaften (**Gruppenaxiome**):

- $(\forall g \in G)(\exists g^{-1} \in G)\; g \cdot g^{-1} = g^{-1} \cdot g = e$
- $(\exists e \in G)(\forall g \in G)\; e \cdot g = g \cdot e = g$

Es gilt: $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$

Eine Untergruppe $N \subseteq G$ mit $a \cdot N = N \cdot a \;\forall a \in G$ heißt **Normalteiler** von $\underline{G}$.

Ring: Algebra $(R, +, -, 0, \cdot)$ vom Typ $(2, 1, 0, 2)$, mit:

- $(R, +, -, 0)$ ist kommutative Gruppe (Abelsche Gruppe)
- $\cdot$ ist assoziativ und distributiv über $+$.

Es gilt: $\forall\, r \in R :\; r \cdot 0 = 0$

Wenn $a, b \in R \setminus \{0\} \;\wedge\; a \cdot b = 0 \;\rightarrow\; a$ und b sind **Nullteiler**.

Ring mit 1: Ring, bei dem es ein neutrales Element von $\cdot$ gibt.

Ein nullteilerfreier kommutativer Ring mit 1 heißt **Integritätsbereich**. In diesen gilt die Kürzungsregel: $a \cdot b = a \cdot c \;\wedge\; a \neq 0 \;\rightarrow\; b = c$

Körper: Ring mit Eins $(K, +, -, 0, \cdot, 1)$ für den gilt: $(K \setminus \{0\}, \cdot)$ ist eine Gruppe mit neutralem Element 1.

Jeder Körper ist Integritätsbereich.

Vektorraum: Abelsche Gruppe $\mathbb{V} = (V, +, -, \underline{0})$ (**Vektoren**) über einem Körper $\mathbb{K}$ (**Skalare**) ($\underline{0}$: **Nullvektor**). Es ist eine äußere Operation $\circ : K \times V \rightarrow V$ (**Skalarmultiplikation**) mit folgenden Eigenschaften definiert:

- $k_1 \circ (k_2 \circ v) = (k_1 \cdot k_2) \circ v$
- $k \circ (v_1 + v_2) = k \circ v_1 + k \circ v_2$
- $(k_1 + k_2) \circ v = k_1 \circ v + k_2 \circ v$
- $1 \circ v = v$ (1: neutrales Element von $\mathbb{K}$ bzgl $\cdot$)

6.5 Kongruenz

Sei $\underline{A} = (A, \circ)$ eine Algebra und $R \subseteq A \times A$ eine Äquivalenzrelation in A. R heißt **Kongruenzrelation**, wenn gilt:

$$\forall x_1, x_2, y_1, y_2 \in A : \quad x_1 R x_2 \wedge y_1 R y_2 \rightarrow (x_1 \circ y_1) R (x_2 \circ y_2)$$

Die Faktormenge ${}^{A}/_{R}$ bildet bzgl. repräsentantenweisen Rechnens die **Faktoralgebra** $({}^{A}/_{R}, \bullet)$ mit $[a_1]_R \bullet [a_2]_R := [a_1 \circ a_2]_R$ $(a_1, a_2 \in A)$.

7 Morphismen

Ein Morphismus ist eine Abbildung $f : A \rightarrow B$ zwischen strukturtragenden Mengen, die die Struktur der Mengen respektiert.

7.1 Definition

Seien $\underline{A} = (A, \circ)$ und $\underline{B} = (B, *)$ Algebren. $f : A \rightarrow B$ heißt **Homomorphismus**, wenn gilt:

$$\forall a_1, a_2 \in A : f(a_1 \circ a_2) = f(a_1) * f(a_2)$$

Isomorphismus: bijektiver Homomorphismus

Endomorphismus: wenn $A = B$

Automorphismus: bijektiver Endomorphismus

7.2 Gesetze

Seien $\underline{A_1} = (A_1, \circ)$ und $\underline{A_2} = (A_2, *)$ Algebren, $f : A_1 \rightarrow A_2$ Homomorphismus. Dann gilt:

- Ist $U_1 \subseteq A_1$ Unteralgebra von A_1, so ist $f(U_1)$ Unteralgebra von A_2.
- Ist $U_2 \subseteq A_2$ Unteralgebra von A_2, so ist $f^{-1}(U_2)$ Unteralgebra von A_1.

Homomorphiesatz für Halbgruppen:

Sei $f : H_1 \rightarrow H_2$ ein Halbgruppenhomomorphismus. Dann gilt: ${}^{H_1}/_{\ker f} \cong f(H_1)$.

Homomorphiesatz für Gruppen (Satz von Cayley):

Jede endliche Gruppe ist zu einer Permutationsgruppe isomorph, d. h., zu jeder endlichen Gruppe $\underline{G}$ $\exists n \in \mathbb{N}$, so dass $\underline{G}$ isomorph zu einer Untergruppe von $(S_n, \circ)$ ist. (Gilt sinngemäß auch für unendliche Gruppen).

7.3 Homomorphismen und Kongruenz

Natürlicher Homomorphismus

geg: Algebra $\underline{A} = (A, \circ)$, Kongruenzrelation R in A

$\Rightarrow$ Natürlicher Homomorphismus $\mathrm{nat}_R : A \rightarrow {}^{A}/_{R}$ mit $\mathrm{nat}_R(a) = [a]_R$

Kern

geg: Homomorphismus $f : A_1 \rightarrow A_2$

Die **Kongruenzklasse** $[a]_f := \{x \in A_1 \big| f(x) = f(a)\}$ $(a \in A_1)$ ist die größte Klasse von Elementen aus A_1, auf denen f konstant ist. Die dadurch erzeugte Kongruenzrelation ist $\ker f$.