Mathematik 1 – Formeln und Beweise

Die natürlichen Zahlen

Peano-Axiome:

- 0 ist eine natürliche Zahl
- Jede natürliche Zahl n hat genau einen Nachfolger n^+
- Es gibt keine natürliche Zahl n mit $n^+ = 0$
- Falls 2 natürliche Zahlen den selben Nachfolger haben, dann sind diese Zahlen gleich
- Enthält eine Menge 0 und für jedes Element n aus dieser Menge ist auch n^+ Element dieser Menge, dann ist diese Menge die Menge der natürlichen Zahlen

Komplexe Zahlen

Moivre'sche Formel:

$(\cos\phi + i \cdot \sin\phi)^n = \cos(n\phi) + i \cdot \sin(n\phi)$ ... hergeleitet von Potenzierung komplexer Zahlen mit r = 1

Fundamentalsatz der Algebra: Jeder Gleichung n-ten Grades mit komplexen oder reellen Koeffizienten hat in C genau n Lösungen, wenn man mehrfache Lösungen entsprechend ihrer Vielfachheit zählt.

Modulo-Rechnung

Rechengesetze:

- $a \equiv b \bmod m$ à $a + c \equiv b + c \bmod m$ mit a, b, c aus Z und m aus N
- $a \equiv b \bmod m$ à $ac \equiv bc \bmod m$ mit a, b, c aus Z und m aus N
- $ac \equiv bc \bmod mc$ à $a \equiv b \bmod m$ mit a, b, c aus Z und m aus N
- $ac \equiv bc \bmod m$ à $a \equiv b \bmod m$, falls ggT(c, m) = 1
- $a \equiv b \bmod m$ $x \equiv y \bmod m$
  $mk = a – b$ $mg = y – x$ mit g, k aus Z
  $mk – a + b = 0$ $mg + x – y = 0$
  $mk – a + b = mg + x – y$
  $m(k – g) = a – b + x – y$
  $m(k – g) = (a + x) – (b + y)$
  à $a + x \equiv b + y \bmod m$

ISBN :

x-yyy-zzzzz-p
x ... Gruppe (nach Sprache, Region, etc.)
y ... Verlag
z ... Titel
p ... Prüfziffer

$10x_1 + 9x_2 + ... + 2x_9 + p \equiv 0 \mod 11$

Eigenschaften:

- jeder Fehler in einer Ziffer wird erkannt
- jede Vertauschung zweier Ziffern wird erkannt

Mengen

Potenzmenge

$|P(M)| = 2^{|M|}$

Beweis:

1. $M = \emptyset \Rightarrow P(M) = \{\emptyset\} \Rightarrow |P(M)| = 1 = 2^{|M|}$
2. n à n + 1

   $M = \{a_1, a_2, ..., a_{n+1}\}$

   $P(M) = \{A : A \subseteq \{a_1, a_2, ..., a_n\}\} \cup \{A : A = B \cup \{a_{n+1}\} \wedge B \subseteq \{a_1, a_2, ..., a_n\}\}$

   $|P(M)| = 2^n + 2^n = 2^{n+1}$

Äquivalenzrelationen

Eine Äquivalenzrelation und eine Partition (Klasseneinteilung) einer Menge entsprechen einander umkehrbar eindeutig.

Beweis:

Eigenschaften einer Äquivalenzrelation:

- (R)eflexivität
- (S)ymmetrie
- (T)ransitivität

Eigenschaften einer Partition

- $K_i \neq \emptyset \quad \forall i \in I$
- $K_i \cap K_j = \emptyset \quad \text{für} \quad i \neq j$
- $\bigcup\limits_{i \in I} K_i = A$

Äquivalenzrelation à Klasseneinteilung:

- $K(a) \neq \emptyset, \quad weil \quad (R) \Rightarrow a \in K(a) \quad \forall a \in A$
- $K(a) \cap K(b) \neq \emptyset \Rightarrow K(a) = K(b)$

  $man \quad wähle \quad ein \quad c \in K(a) \cap K(b)$

  $$\left.\begin{array}{l} a \in K(a) \wedge c \in K(a) \Rightarrow aRc \\ b \in K(b) \wedge c \in K(b) \Rightarrow bRc \end{array}\right\} aRb \xrightarrow{(T)} K(a) = K(b)$$

- $\bigcup\limits_{a \in A} K(a) \supseteq A, \quad weil \quad K(a) \supseteq a$

  $K(a) \subseteq A, \quad \forall a \in A \Rightarrow \bigcup\limits_{a \in A} K(a) \subseteq A$

  Somit: $\bigcup\limits_{a \in A} K(a) = A$

Klasseneinteilung à Äquivalenzrelation:

- (R) $a \in K(a) \quad \forall a \in A \Rightarrow aRa \quad \forall a$
- (S) $a \in K_i \quad \wedge \quad b \in K_i \Rightarrow b \in K_i \quad \wedge \quad a \in K_i$
- (T) $aRb, bRc \Rightarrow a \in K_i, b \in K_i, b \in K_j, c \in K_j$

  $\Rightarrow b \in K_i \cap K_j \xrightarrow{wegen \quad Eigenschaft \quad 2} K_i = K_j \Rightarrow a, c \in K_i \Rightarrow aRc$

Halbordnungsrelationen

- k ist das kleinste Element, wenn $k \leq a \forall a \in R$
- g ist das größte Element, wenn $g \geq a \forall a \in R$
- m ist ein minimales Element, wenn $\nexists a \in R : a < m$
- M ist ein maximales Element, wenn $\nexists a \in R : a > M$
- a ist unterer Nachbar von b, wenn gilt: $a < b \wedge \nexists c \in R : a < c < b$
- Vollordnung heißt: $a \leq b \vee b \leq a \quad \forall a, b \in R$

Abbildungen

- Injektiv: $f(a) = f(b) \Rightarrow a = b \quad d.h. \forall b \in B \exists \text{höchstens ein}\, a \in A : f(a) = b$
- Surjektiv: $\forall b \in B : \exists a \in A : f(a) = b$
- Bijektiv: $\forall b \in B : \exists | a \in A : f(a) = b$ à es existiert die Umkehrabbildung f^{-1}

Für eine Abbildung f: A à A, wobei A eine endiche Menge ist, sind diese 3 Begriffe gleichwertig (d.h. trifft eine Eigenschaft zu, sind auch die anderen wahr).

Beweis:

- Injektiv à Surjektiv:
$$\left.\begin{array}{l} f(A) \subseteq A \\ |f(A)| = |\{\underbrace{f(a_1), f(a_2), \ldots, f(a_n)}_{\text{alle verschieden}}\}| = |A| \end{array}\right\} f(A) = A \Rightarrow \text{surjektiv}$$
- Surjektiv à zusätzlich auch noch injektiv:
Angenommen *f* ist nicht injektiv:
$$\left.\begin{array}{l} \text{Nicht-Injektivität} \Rightarrow f(A) < |A| \\ \text{Surjektivität} \Rightarrow f(A) = |A| \end{array}\right\} \text{Widerspruch} \Rightarrow f \text{ muss injektiv sein}$$
- Bijektiv à Injektiv
ist wahr, laut Definition von *bijektiv*

Logik

- Eine *Aussage* ist ein Satz, dem einer der Wahrheitswerte *wahr* oder *falsch* zugeordnet werden kann.
- Eine *Aussagenvariable* kann einen dieser Werte (*wahr* oder *falsch*) annehmen.
- Ein *Prädikat* ist ein Satz der form $P(x_1, x_2, ..., x_n)$, wobei x_i aus einer geeigneten/beliebigen Grundmenge stammen können (nicht unbedingt aus der bool'schen Menge). Nach Belegung der Variablen geht das Prädikat in eine Aussage über (z.B. *P(x) : x ist gerade für x aus Z*).
- Eine *Formel der Aussagenlogik* ist ein Satz der Form $F(x_1, x_2, ..., x_n)$, wobei x_i Aussagenvariablen sind (also nur *wahr* oder *falsch* annehmen können). Eine Formel kann erfüllbar (für mindestens eine Belegung wahr), gültig (für alle Belegungen wahr) oder unerfüllbar (für alle Belegungen falsch) sein.
- Aussagen können mit Junktoren verknüpft werden und bilden neue Aussagen.
- Prädikate können durch Verwendung von Quantoren neue Ausdrücke bilden.

Kombinatorik

Regeln

- Summenregel: Hat man 2 Mengen mit n und m Elementen, so gibt es n + m Möglichkeiten ein Element aus einer Menge zu ziehen, falls die Mengen disjunkt sind
- Produktregel: Hat man 2 Mengen mit n und m Elementen, so gibt es n • m Möglichkeiten aus jeder Menge je ein Element zu ziehen.
- Gleichheitsregel: Gilt für zwei Mengen |A| = |B| (sie entsprechen einander umkehrbar eindeutig), so gibt es gleich viele Möglichkeiten ein Element aus A oder B zu ziehen.

Auswahlprobleme

- Permutation ohne Wiederholung (Anzahl der möglichen Anordnungen von Elementen): $P_n = n!$ Herleitung durch grafische Darstellung (Auswahlmöglichkeiten an der i-ten Stelle).
- Permutation mit Wiederholung (Elemente kommen mehrfach vor à Multimenge): $P_n^{k_1,\dots,k_n} = \frac{n!}{k_1!\cdot\ldots\cdot k_n!}$ (es fallen je k_i Permutationen zusammen, d.h. die Vertauschungsmöglichkeiten der gleichen Elemente sind uninteressant).
- Variation ohne Wiederholung (Auswahl von *k* aus *n* Elementen, wobei die Reihenfolge wichtig ist): $V_n^k = \frac{n!}{(n-k)!}$ Herleitung durch grafische Darstellung (Auswahlmöglichkeiten an der i-ten Stelle).
- Variation mit Wiederholung (Auswahl von *k* aus *n* Elementen, wobei die Reihenfolge wichtig ist und ein Element mehrfach gewählt werden darf): ${}^{W}V_n^k = n^k$ Herleitung durch grafische Darstellung (Auswahlmöglichkeiten an der i-ten Stelle). Beispiel: Toto.
- Kombination ohne Wiederholung (Auswahl von *k* aus *n* Elementen, wobei die Reihenfolge keine Rolle spielt. $C_n^k = \binom{n}{k}$. Herleitung über die Variation („Herausnehmen“ der Reihenfolge) Beispiel: Lotto.
- Kombination mit Wiederholung (Auswahl von *k* aus *n* Elementen, wobei ein Element mehrfach gewählt werden darf. ${}^{W}C_n^k = \binom{n+k-1}{k}$.

  Beweis:

  $$A = \{1,2,\dots,n\}$$

  $$C_n^k = |\{(a_1,a_2,\dots,a_k) : a_i \in A \wedge 1 \le a_1 < a_2 < \dots < a_n \le n\}| \ldots \textit{exakte Definition von "Reihenfolge ist egal"}$$

  $${}^{W}C_n^k = |\{(a_1,a_2,\dots,a_k) : a_i \in A \wedge 1 \le a_1 \le a_2 \le \dots \le a_n \le n\}|$$

  $$< \textit{wird wegen der Wiederholungsmöglichkeit zu} \le$$

  $$\Rightarrow \textit{Wiederherstellung des alten Musters von } C_n^k \textit{ durch zusätzliche Summanden}:$$

  $${}^{W}C_n^k = |\{(a_1,a_2,\dots,a_k) : a_i \in A \wedge 1 \le a_1 \le a_2 + 1 < a_3 + 2 < \dots < a_n \le n+k-1\}|$$

  $$\Rightarrow {}^{W}C_n^k = \binom{n+k-1}{k}$$

Inklusions-Exklusions-Prinzip (Siebformel)

Umwandlung von Fragestellungen der Art $|A \cup B \cup ... \cup C|$ in Ausdrücke mit $\cap$ (leichter zählbar).

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ I\neq\emptyset}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} A_i\right|$$

Beweis:

Für 2 Mengen: $|A \cup B| = |A| + |B| - |A \cap B|$ durch ein Venn-Diagramm

$$\left|\bigcup_{i=1}^{n+1} A_i\right| = \left|(\underbrace{\bigcup_{i=1}^{n} A_i}_{B}) \cup A_{n+1}\right| = |B| + |A_{n+1}| - |B \cap A_{n+1}| = |B| + |A_{n+1}| - |(\underbrace{\bigcup_{i=1}^{n} A_i}_{B}) \cap A_{n+1}| =$$

$$= |B| + |A_{n+1}| - |\bigcup_{i=1}^{n}(\underbrace{A_i \cap A_{n+1}}_{B_i})| = \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ I\neq\emptyset}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} A_i\right| + |A_{n+1}| - \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ I\neq\emptyset}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} B_i\right| =$$

$$= \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ I\neq\emptyset}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} A_i\right| + |A_{n+1}| - \sum_{\substack{I\subseteq\{1,2,\ldots,n,n+1\}\\ \{n+1\}\subset I}} (-1)^{|I|} \cdot \left|\bigcap_{i\in I} A_i\right| =$$

$$= \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ I\neq\emptyset}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} A_i\right| + |A_{n+1}| + \sum_{\substack{I\subseteq\{1,2,\ldots,n,n+1\}\\ \{n+1\}\subset I}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} A_i\right| =$$

$$= \sum_{\substack{I\subseteq\{1,2,\ldots,n\}\\ I\neq\emptyset}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} A_i\right| + \sum_{\substack{I\subseteq\{1,2,\ldots,n,n+1\}\\ \{n+1\}\subseteq I}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} A_i\right| =$$

$$= \sum_{\substack{I\subseteq\{1,2,\ldots,n+1\}\\ I\neq\emptyset}} (-1)^{|I|-1} \cdot \left|\bigcap_{i\in I} A_i\right| \qquad QED$$

<u>Binomialkoeffizient</u>

Verwendung beim Auflösen von Binomen: $(x + y)^n = (x + y)(x + y) \ldots (x + y)$.

Man kann aus jeder Klammer x oder y auswählen. Will man *k* Mal *x* (und daher *n-k* Mal *y*) wählen, so gibt es $P_n^{k,n-k} = \frac{n!}{k! \cdot (n-k)!} = \binom{n}{k}$ Möglichkeiten. Nun kann man aber *0* bis *n* mal *x* (und daher *n-0* bis *n-n=0* mal *y*) wählen. Daher ergibt sich:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Es gilt:

- $\binom{n}{k} = \binom{n}{n-k}, \quad weil\ \frac{n!}{k! \cdot (n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!}$
-

$$\binom{n}{k}+\binom{n}{k+1}=\binom{n+1}{k+1}, \quad weil\ \frac{n!}{k!\cdot(n-k)!}+\frac{n!}{(k+1)!\cdot(n-k-1)!}=\frac{\frac{n!(k+1)}{n-k}+n!}{(k+1)!(n-k-1)!}=$$

$$=\frac{\frac{n!k+n!+n!n-n!k}{n-k}}{(k+1)!(n-k-1)!}=\frac{(n+1)!}{(k+1)!(n-k)!}$$

- $(1+1)^n=2^n \Rightarrow \sum_{k=0}^{n}\binom{n}{k}=2^n$

Graphentheorie

Ein nicht-schlichter Graph benötigt eine Inzidenzabbildung, um einer Kante die Knoten zuzuordnen, die durch sie verbunden werden. Die Kantenmenge ist eine Auflistung der „Namen" der Kanten.

Gerichtet: $G=<V,E,f>$ mit $f:E\to V^2=\{(u,v):u,v\in V(G)\}$

Ungerichtet: $G=<V,E,f>$ mit $f:E\to\{\{u,v\}:u,v\in V(G)\}$

Ein schlichter Graph benötigt keine Inzidenzabblindung, da es keine Mehrfachkanten gibt. Die Kantenmenge ist direkt eine Menge von Mengen (ungerichtet) oder von 2-Tupeln (gerichtet). 2 adjazente (verbundene) Knoten sind inzident zur verbindenden Kante.

Handschlaglemma

Ungerichtet: $\sum_{v\in V}d(v)=2\cdot|E(G)|$

Gerichtet: $\sum_{v\in V}d^+(v)=\sum_{v\in V}d^-(v)=|E(G)|$

Beweis für ungerichtete Graphen nach E(G):

1. E(G) = 0 (keine Kanten). $\sum_{v\in V}d(v)=0$
2. Zusätzliche Kante einfügen: $|E(G_{neu})|=|E(G)|+1$

   Die Kante verbindet 2 Knoten à 2 Knotengrade werden um je 1 erhöht,

   also $\sum_{v\in V_{neu}}d(v)=\left(\sum_{v\in V}d(v)\right)+2$

$$\left(\sum_{v\in V}d(v)\right)+2=2\cdot(\underbrace{|E(G)|+1}_{E(G_{neu})})\Rightarrow\left(\sum_{v\in V}d(v)\right)+2=2\cdot|E(G)|+2\Rightarrow\sum_{v\in V}d(v)=2\cdot|E(G)|$$

Das ist wahr laut Induktionsvoraussetzung.

Beweis für gerichtete Graphen nach E(G):

1. E(G) = 0 (keine Kanten). $\sum_{v\in V}d^+(v)=\sum_{v\in V}d^-(v)=0$
2. Zusätzliche Kante einfügen: $|E(G_{neu})|=|E(G)|+1$

   Die Kante verbindet 2 Knoten à Ein Hin- und ein Weggrad wird erhöht

also $\sum_{v\in V_{neu}}d^+(v)=\left(\sum_{v\in V}d^+(v)\right)+1$ (für den Hingrad analog)

$$\left(\sum_{v\in V}d^+(v)\right)+1=\underbrace{|E(G)|+1}_{E(G_{neu})}\Rightarrow\sum_{v\in V}d^+(v)=|E(G)|$$

Das ist wahr laut Induktionsvoraussetzung.

Definitionen

- Kantenfolge: Beliebige Aneinanderreihung von Kanten (offen oder geschlossen)
- Kantenzug: Keine Kante darf mehr als ein Mal verwendet werden (alle Kanten paarweise verschieden)
- Weg: Keine Kante und kein Knoten darf öfter verwendet werden
- Kreis: Weg mit einer Ausnahme: Start- und Endknoten sind gleich

Es ist stets möglich:
Reduktion einer offenen *Kantenfolge* auf einen *Weg*
Reduktion eines geschlossenen *Kantenzuges* zu einem *Kreis*

Eulersche Linie

Ein Kantenzug, bei dem jede Kante *genau einmal* verwendet wird. Es existiert genau dann eine geschlossene Eulersche Linie in einem ungerichteten Graphen, wenn alle Knotengrade gerade sind.

Beweis:
Spezialfall: $|V(G)| = 1$ à alle Knotengrade (der eine Knotengrad) = 0: ein Knoten enthält eine eulersche Linie

Andernfalls: alle Knotengrade $\geq 2 \Rightarrow$ es existiert ein geschlossener Kantenzug, und somit ein Kreis (würde kein geschlossener Kantenzug existieren, müsste man irgendwo nicht mehr weiterkommen, was aber bedeuten würde, dass nicht alle Knotengrade gerade sind). Entfernen des Kreises aus dem Graphen: $G_1 = < V, E \setminus C_1 >$. Jeder Knotengrad wird um 2 reduziert à wieder gerade à Schritt wiederholbar bis $E_i = \emptyset$. Die Kreise können nun durchlaufen werden à geschlossene Eulersche Linie.

Umgekehrter Beweis: bei jedem Knotendurchlauf wird der Grad um 2 erhöht. Also: eulersche Linie à alle Knotengrade gerade

Offene Eulersche Linie: genau 2 Knoten haben einen ungeraden Grad.
Gerichteter Graph: Hin- und Weggrad aller Knoten sind gleich.

Typen von Graphen

- Wald: es existiert zwischen je zwei Knoten maximal ein Weg (kreisfrei)
- Baum: es existiert zwischen je zwei Knoten genau ein Weg (kreisfrei)
  Beweis:
  Baum à genau 1 Weg:
  angenommen es existieren 2 Wege von *v* nach *w*:
  $v_1, v_2, ..., v_i, v_{i+1}, ..., v_j, v_{j+1}, \dots v_k$
  $w_1, w_2, ..., w_i, w_{i+1}, ..., w_{j'}, w_{j'+1}, \dots w_{k'}$
  wobei $v_a = w_a$ für $a \leq i$ und "$a \geq j$" à Kreis: $v_i, v_{i+1}, \dots, v_j, w_{j'-1}, \dots, w_i = v_i$
  genau 1 Weg à Baum:

angenommen es ist kein Baum à es existiert ein Kreis $v_1, v_2, ..., v_{k-1}, v_1$
à 2 Wege: $v_1 v_{k-1}$
$v_1 v_2 ... v_{k-1}$

Es gilt in einem Baum: |V| = |E| + 1

Beweis: 1. |V| = 1, |E| = 0: 1 = 0 + 1 w.A.

2. |V| = n + 1, |E| = n

Entfernen eines Endknotens + Kante (existiert immer, da andernfalls alle Knotengrade $\geq 2 \Rightarrow$ es existiert ein Kreis $\Rightarrow$ kein Baum)

$|V \setminus \{v_1\}| = |E \setminus \{e_1\}| + 1$ ... laut Induktionsvoraussetzung

|V| - 1 = |E| - 1 + 1

|V| = |E| + 1 QED

- Gerüst: ein Teilgraph eines Graphen, der ein Baum ist und dieselben Knoten wie der ursprüngliche Graph hat
- Komplement: ein Graph G', für den gilt: (v,w) $\in E(G') \Leftrightarrow$ (v,w) $\notin E(G)$ für $w \neq v$ (analog für ungerichtete Graphen)
- Transitive Hülle: ein gerichteter Graph G^T, für den gilt: (v,w)$\in E(G^T) \Leftrightarrow \exists$gerichteter Weg von v nach w in G
- Transitive Reduktion: ein Graph G_R für den gilt: $G_R^T = G^T$ mit E_R ist minimal und $E_R \subseteq E$
- Wurzelbaum: ein Baum, bei dem ein Knoten als Wurzel bezeichnet wird (oben gezeichnet)
- Binärbaum: Ein Wurzelbaum, bei dem jeder Knoten genau 0 oder 2 Teilbäume
  Endknoten ... x, Innere Knoten ... m: es gilt: x =m + 1
  Beweis:
  $|V(G)| = m + x \qquad |V(G)| = |E(G)| + 1 \qquad |E(G)| = 2m$
  $\Rightarrow 2m + 1 = m + x$
  $m + 1 = x$

Kruskal-Algorithmus

1. $T_0 = \langle V, E_0 = \emptyset \rangle$, i=0
2. Man wähle aus $E \setminus E_i$ die Kante e mit der geringsten Bewertung, so dass $\langle V, E_i \cup \{e\} \rangle$ kreisfrei bleibt
3. i=i+1; Falls i = |V| - 1: Ende, sonst weiter bei Schritt 2

Dijkstra-Algorithmus

1. a=Startknoten; b = Endknoten; l(a) = 0, l(v) $= \infty\ \forall v \neq a$, U={a}, u = a
2. $l(v) = \min(l(v), l(u) + l(u,v)) \quad \forall v \in V : \{u,v\} \in E(G) \wedge v \notin U$
3. Man wähle einen Knoten $v \in V \setminus U$ mit l(v) ist minimal. u = v, U = U $\cup$ {v}
4. Falls u = b: Ende (l(u) = kürzester Weg; Weg kann durch rekursive Suche der Vorgänger o mit l(o) + l(o, u) = l(u) bestimmt werden), sonst weiter bei 2

Weitere Aufgaben der Graphentheorie

- Kritische Pfade in Netzplänen suchen
- Maximalen Datenfluss in Netzwerken bestimmen
- Prüfen ob ein Graph planar ist
- Feststellen wie viele verschiedene Frequenzen man in einem Funknetz braucht

Algebraische Strukturen

Typen von algebraischen Strukturen

- Gruppoid, falls die Struktur eine Operation hat und abgeschlossen ist (andernfalls ist es gar keine algebraische Struktur)
- Halbgruppe, falls außerdem die Operation assoziativ ist
- Monoid, falls außerdem ein neutrales Element existiert
- Gruppe, falls außerdem jedes Element ein inverses hat
- Abelsche Gruppe, falls außerdem die Operation kommutativ ist
- Ring, falls die Operationen + und * definiert sind, die Menge mit + eine kommutative Gruppe und mit * eine Halbgruppe bildet und * distributiv bezüglich + ist
- Integritätsring, wenn darüber hinaus * kommutativ ist, ein Einselement für * existiert und keine Nullteiler existieren
- Körper, falls darüber hinaus die Menge ohne das 0-Element mit * eine Gruppe bildet
- Verband, falls die Operationen $\cup$ und $\cap$ definiert sind, mit der Menge kommutative Halbgruppen bilden und die Verschmelzungsgesetze gelten
- Boolsche Algebra, falls darüber hinaus die Operatoren gegenseitig distributiv sind und die neutralen Elemente 0 (bezüglich $\cup$) und 1 (bezüglich $\cap$) sowie die Komplementbildung ($a' \cup a=1$, $a' \cap a=0$) definiert sind

Besondere algebraische Strukturen

- „Symmetrische Halbgruppe“: die Menge aller Abbildungen einer Menge auf sich selbst mit der Komposition als Operation
- „Freies Monoid“: die Menge aller endlichen Wörter, die aus Buchstaben einer bestimmten Menge bestehen sowie das Leerwort. Operation ist die Verkettung. Die Buchstabenmenge wird meist A genannt, die Wörtermenge A^*.
- „Symmetrische Gruppe“: die Menge aller bijektiven Abbildungen (=Permutationen) einer Menge auf sich selbst. Operation ist die Komposition. Abgekürzt mit S_i (wobei *i* die Anzahl der Elemente der Defintitions-(=Bild)-Menge ist).

Rechenregeln für Gruppen

- $(ab)^{-1} = b^{-1}a^{-1}$
- $(a^{-1})^{-1} = a$
- ac = bc à a = b (Kürzungsregel)

Untergruppen

Falls eine Teilmenge der ursprünglichen Menge gemeinsam mit der Operation wieder eine Gruppe bildet, dann heißt sie Untergruppe
$(\ \textit{falls} \quad U \subseteq G \quad \textit{und} \quad \langle U, \bullet \rangle \quad \textit{Gruppe, dann heißt } U \leq G\ )$

Wenn $\langle G, \bullet \rangle$ *Gruppe und* $U \subseteq G, U \neq \emptyset$, *dann gilt* :

$$U \leq G \overset{1}{\Leftrightarrow} \left\{ \begin{array}{l} a)\ a,b \in U \Rightarrow ab \in U \\ b)\ 1 \in U \\ c)\ a \in U \Rightarrow a^{-1} \in U \end{array} \right\} \overset{2}{\Leftrightarrow} a,b \in U \Rightarrow ab^{-1} \in U \overset{3}{\Leftrightarrow} U \leq G$$

Beweis:
1. a) ist erfüllt, weil U Gruppe und daher abgeschlossen
b) U ist Gruppe und hat daher Einselement. Angenommen 1_U ungleich 1_G:

$$\left.\begin{array}{l} 1_U \cdot 1_U = 1_U \\ 1_G \cdot 1_U = 1_U \end{array}\right\} 1_U \cdot 1_U = 1_G \cdot 1_U \Rightarrow 1_U = 1_G$$

c) U ist Gruppe und hat daher inverse Elemente. Angenommen $a^{-1}{}_U$ ungleich $a^{-1}{}_G$:

$$\left.\begin{array}{l} a_U \cdot a^{-1}{}_U = 1 \\ a_U \cdot a^{-1}{}_G = 1 \end{array}\right\} a_U \cdot a^{-1}{}_U = a_U \cdot a^{-1}{}_G \Rightarrow a^{-1}{}_U = a^{-1}{}_G$$

2. $a,b \in U \xrightarrow{c} b^{-1} \in U \xrightarrow{a} ab^{-1} \in U$

3. $U \neq \emptyset \Rightarrow \exists c \in U \xrightarrow{UG-Kriterium} cc^{-1} \in U \Rightarrow 1 \in U \Rightarrow 1c^{-1} \in U \Rightarrow c^{-1} \in U$
$a(b^{-1})^{-1} \in U \Rightarrow ab \in U \Rightarrow U \leq G$

Klasseneinteilung

$$aU = \{a \cdot u \mid u \in U\} ...Linksnebenklasse$$
$$\{aU \mid a \in G\} ...Linksnebenklassenzerlegung$$

Es gilt:
- LNK-Zerlegung = K_L = Partition von G
- Alle LNK sind gleich mächtig
- |G:U| (Index) ist die Anzahl der LNK und RNK

Satz von Lagrange

|G| = |G:U|•|U|
Beweis:
G = $a_1U \cup a_2U \cup ... \cup a_nU$
|G| = $|a_1U| \cup |a_2U| \cup ... \cup |a_{G:U}U|$ … da alle a_i disjunkt
|G| = |G:U|•|U| à |G:U| ist immer Teiler von |G|

Normalteiler

$aN = Na \quad \forall a \in G$ à K_L, K_R sind selbst Gruppen (N ist Normalteiler).
$K_L = K_R$ = G / N (Faktorgruppe)
Es gilt dann: (aN)(bN) = (ab)N, wobei (aN)(bN) paarweise durchgeführt wird („jedes mit jedem“)

Homomorphismus

Eine Abbildung $\phi : G \rightarrow H$ heißt Momomorphismus falls gilt:

$$\phi(a \underbrace{\cdot}_{in\ G} b) = \phi(a) \underbrace{\cdot}_{in\ H} \phi(b)$$

Ist die Abbildung auch bijektiv, dann heißt sie Isomorphismus.

ker ϕ = $\{ a \in G \mid \phi(a) = 1_H \}$ ker $\phi \leq G$
img ϕ = $\{ b \in H \mid \exists a \in G : \phi(a) = b\}$ $img \phi \leq H$

Der Kern des Homomorphismus ist ein Normalteiler von G und das Bild von ϕ ist isomorph zur Faktorgruppe (Homomorphiesatz):

$$G/\ker n\phi \cong img\ \phi$$

Neuetrales und inverse Elemente werden auf eben diese abgebildet.
Beweis:

$$\phi(\underbrace{a\cdot 1_G}_{a}) = \phi(a)\cdot\phi(1_G) = \phi(a) \Rightarrow \phi(1_G) = 1_H$$

$$\left.\begin{aligned}&\phi(\underbrace{a\cdot a^{-1}}_{1_G}) = \underbrace{\phi(a)\cdot\phi(a^{-1})}_{1_H}\\ &\phi(1_G) = 1_H\end{aligned}\right\}\phi(a^{-1})\ ist\ invers\ zu\ \phi(a)$$

<u>Erzeugende Elemente</u>

$\langle a\rangle = \{a^n \mid n\in Z\}$, weil $a^m a^{-n} = a^{m-n} \in \langle a\rangle$
Dies ist die von a erzeugte Untergruppe.
Ist $a\in G\ und\ ist\ G = \langle a\rangle,$ dann heißt G zyklisch und a das erzeugende Element von G.

Weiters gilt für endliche Gruppen:

$$\langle a\rangle = \{1, a^1, a^2, a^3, \ldots, a^{m-1}\}$$

$$a^m = 1 \qquad m = |G|$$

$$\langle a\rangle = \{1, a^1, a^2, a^3, \ldots, a^{r-1}\} \qquad r \ge 1$$

$$\langle a\rangle = \{1, a^1, a^2, a^3, \ldots, a^{m-1}\}$$

$$|\langle a\rangle| \mid |G|$$

$$r \mid |G| \qquad a^r = 1$$

$$a^{|G|} = a^{r\cdot|G:<a>|} = \left(a^r\right)^{|G:<a>|} = 1$$

Lineare Algebra

<u>Rechengesetze für Vektoren</u>

- $\vec{x}(\vec{y}+\vec{z}) = \vec{x}\vec{y} + \vec{x}\vec{z}$
- $\vec{x}(\lambda\vec{y}) = \lambda(\vec{x}\vec{y})$
- $\vec{x}\vec{y} = \vec{y}\vec{x}$
- $\vec{x}^2 \ge 0 \qquad \vec{x}^2 = 0 \Rightarrow \vec{x} = \vec{0}$

<u>Voraussetzung für folgende Beweise</u>

$$\|\vec{x}\|^2 = (\vec{x})^2$$

$$\left(\sqrt{x_1^{\ 2} + x_2^{\ 2} + \ldots + x_n^{\ 2}}\right)^2 = \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \ldots \\ x_n \end{pmatrix}$$

$$x_1^{\ 2} + x_2^{\ 2} + \ldots + x_n^{\ 2} = x_1^{\ 2} + x_2^{\ 2} + \ldots + x_n^{\ 2}$$

$$\Rightarrow QED$$

Orthogonalität zweier Vektoren

$$\|\vec{x} - \vec{y}\|^2 = \|\vec{x}\|^2 + \|\vec{y}\|^2 \qquad \textit{...Pythagoras}$$

$$(\vec{x} - \vec{y})^2 = (\vec{x})^2 + (\vec{y})^2$$

$$(\vec{x})^2 - 2\vec{x}\vec{y} + (\vec{y})^2 = (\vec{x})^2 + (\vec{y})^2$$

$$-2\vec{x}\vec{y} = 0$$

$$\left[\vec{x}\vec{y} = 0\right]$$

Winkel zwischen 2 Vektoren

$$\|\vec{x} - \vec{y}\|^2 = \|\vec{x}\|^2 + \|\vec{y}\|^2 - 2\|\vec{x}\| \cdot \|\vec{y}\| \cdot \cos\phi \qquad \textit{...Cosinussatz}$$

$$(\vec{x} - \vec{y})^2 = (\vec{x})^2 + (\vec{y})^2 - 2\|\vec{x}\| \cdot \|\vec{y}\| \cdot \cos\phi$$

$$\vec{x}^2 - 2\vec{x}\vec{y} + \vec{y}^2 = (\vec{x})^2 + (\vec{y})^2 - 2\|\vec{x}\| \cdot \|\vec{y}\| \cdot \cos\phi$$

$$-2\vec{x}\vec{y} = -2\|\vec{x}\| \cdot \|\vec{y}\| \cdot \cos\phi$$

$$\left[\cos\phi = \frac{\vec{x}\vec{y}}{\|\vec{x}\| \cdot \|\vec{y}\|}\right]$$

Dreiecksungleichung

$$\|\vec{x} + \vec{y}\| \le \|\vec{x}\| + \|\vec{y}\|$$

$$\|\vec{x} + \vec{y}\|^2 \le (\|\vec{x}\| + \|\vec{y}\|)^2 \qquad \textit{...Quadrieren}$$

$$(\vec{x} + \vec{y})^2 \le \vec{x}^2 + 2\|\vec{x}\| \cdot \|\vec{y}\| + \vec{y}^2$$

$$\vec{x}^2 + 2\vec{x}\vec{y} + \vec{y}^2 \le \vec{x}^2 + 2\|\vec{x}\| \cdot \|\vec{y}\| + \vec{y}^2$$

$$\vec{x}^2 + 2\cos\phi \cdot \|\vec{x}\| \cdot \|\vec{y}\| + \vec{y}^2 \le \vec{x}^2 + 2\|\vec{x}\| \cdot \|\vec{y}\| + \vec{y}^2 \qquad \textit{...Winkelformel einsetzen}$$

$$2\cos\phi \cdot \|\vec{x}\| \cdot \|\vec{y}\| \le 2\|\vec{x}\| \cdot \|\vec{y}\|$$

$$\cos\phi \le 1 \Rightarrow w.A.$$

$$= \quad wenn \quad \phi = 0$$

Vektorprodukt

$$\vec{x}\times\vec{y}=\begin{pmatrix}\begin{vmatrix}x_2 y_2\\ x_3 y_3\end{vmatrix}\\ -\begin{vmatrix}x_1 y_1\\ x_3 y_3\end{vmatrix}\\ \begin{vmatrix}x_1 y_1\\ x_2 y_2\end{vmatrix}\end{pmatrix}$$

- $\vec{x}\times\vec{y}=\vec{0}$, falls $\vec{x}=\vec{0}$ oder $\vec{y}=\vec{0}$ oder $\vec{x}$ und $\vec{y}$ parallel
  Andernfalls steht $\vec{x}\times\vec{y}$ normal auf $\vec{x}$ und auf $\vec{y}$, so dass ein Rechtssystem entsteht
- $\|\vec{x}\times\vec{y}\|$ ist der Flächeninhalt des von $\vec{x}$ und $\vec{y}$ aufgespannten Parallelogramms
- $\vec{x}\times\vec{y}=-\vec{y}\times\vec{x}$
  (vertauschen zweier Spalten → Vorzeichen der Determinanten ändert sich)
- $(\lambda\vec{x})\times\vec{y}=\vec{x}\times(\lambda\vec{y})=\lambda(\vec{x}\times\vec{y})$
- $\vec{x}\times(\vec{y}+\vec{z})=\vec{x}\times\vec{y}+\vec{x}\times\vec{z}$ (gilt auch von rechts)

Graßmannscher Entwicklungssatz: $(\vec{x}\times\vec{y})\times\vec{z}=(\vec{x}\vec{z})\vec{y}-(\vec{y}\vec{z})\vec{x}$
Lagrange'sche Identität: $(\vec{x}\times\vec{y})(\vec{z}\times\vec{u})=(\vec{x}\vec{z})(\vec{y}\vec{u})-(\vec{x}\vec{u})(\vec{y}\vec{z})$

Volumsberechnung eines Spats

$V=F\cdot h=\|\vec{x}\times\vec{y}\|\cdot\|\vec{z}\|\cdot\cos\phi$ *...ϕ ist der Winkel zwischen $\vec{x}\times\vec{y}$ und $\vec{z}$*

$V=\|\vec{x}\times\vec{y}\|\cdot\|\vec{z}\|\dfrac{(\vec{x}\times\vec{y})\vec{z}}{\|\vec{x}\times\vec{y}\|\cdot\|\vec{z}\|}$ *...Einsetzen der Winkelformel*

$V=(\vec{x}\times\vec{y})\vec{z}$

Lineare Unabhängigkeit

Vektoren sind genau dann linear unabhängig, wenn sie durch lineare Kombination nur dann $\vec{0}$ ergeben, wenn alle Faktoren 0 sind.

linear unabhängig → Faktoren sind 0, falls lineare Kombination den Nullvektor ergibt.
Angenommen nicht alle Faktoren sind 0:

$$\lambda_1 x_1+\lambda_2 x_2+\ldots+\lambda_n x_n=\vec{0}\quad mit\quad \lambda_1\neq 0$$

$$\lambda_1 x_1=-\lambda_2 x_2-\ldots-\lambda_n x_n$$

$$x_1=-\frac{\lambda_2}{\lambda_1}x_2-\ldots-\frac{\lambda_n}{\lambda_1}x_n\Rightarrow nicht\ \ linear\ \ unabhängig$$

Vektoren sind linear abhängig → es existieren Faktoren ungleich 0

$$x_1 = \lambda_2 x_2 + \ldots + \lambda_n x_n$$
$$-1 \cdot x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = \overset{r}{0}$$
$$1 \neq 0 \; w.A. \Rightarrow QED$$

<u>Rechengesetze für Matrizen</u>

- $(AB)^T = B^T A^T$
- $(AB)^{-1} = B^{-1} A^{-1}$
- $|A| \cdot |B| = |A \cdot B| \qquad ...\mathit{Multiplikationssatz} \quad \mathit{für} \quad \mathit{Deter}\min \mathit{anten}$

  $|A^T| = |A|$
- $|A| \neq 0 \Leftrightarrow \exists A^{-1}$ (A heißt invertierbar, nicht singular oder regulär)

  In diesem Fall gilt: $A^{-1} = \frac{1}{|A|}(A_{ik})^T$

  wobei A_{jk} die Determinante der Matrix ist, die durch Weblassen der i-ten Zeile und der j-ten Spalte entsteht (algebraisches Komlement)

<u>Gesetze bei der Determinantenberechnung</u>

- Vertauschen von 2 Zeilen oder Spalten ändert das Vorzeichen
  (daher „Nicht-Kommutativität" des Kreuzproduktes zweier Vektoren)
- Multiplikation einer Zeile oder Spalte ändert die Determinante um diesen Faktor
- Addition des Vielfachen einer Zeile oder Spalte ändert die Determinante nicht

<u>Lineare Gleichungssysteme</u>

Erlaubt ist jederzeit:

- Vertauschen zweier Zeilen (=Gleichungen)
- Vertauschen zweier Spalten (muss aber bei der Lösung berücksichtigt werden)
- Multiplikation zweier Zeilen mit einem Faktor ungleich 0
- Addition eines Vielfachen einer Zeile zu einer anderen

Mögliche Lösungsfälle:

- r < m mit d_{r+1} bis d_m ungleich 0 à keine Lösung
- r = n à eindeutige Lösung
- r < n à nach Streichen der unnötigen Zeilen existiert ein Lösungsraum mit n – r Dimensionen (unendlich viele Lösungen)