Diskrete Strukturen

gehalten von Prof. Dr. Gerhard Hiß

im WS 07/08

Diese Mitschrift ist
ein Gemeinschaftsprojekt von
http://wiki.infostudium.de/
Rev. 67

Inhaltsverzeichnis

Vorwort

Dieses Dokument ist nur für den RWTH-internen Gebrauch gedacht.

Literatur

1. M. Aigner, Diskrete Mathematik, Vieweg
2. A. Steger, Diskrete Strukturen, Band 1, Springer
3. G. Z. S. Teschl, Mathematik für Informatiker, Band 1, Springer
4. E. Zerz. Mathematische Grundlagen, Skript

1 Einführung in die Sprache der Mathematik

§ 1 Aussagen

Mathematische Aussagen sind sprachliche Ausdrücke (inkl. Symbolen), denen man einen eindeutigen Wahrheitswert, wahr (w) oder falsch (f) zuordnen kann.

(1.1) Beispiele:

1. $2+3=5$ (w)
2. Alle Punkte auf einem Kreis haben den gleichen Abstand zum Mittelpunkt. (w)
3. Jede ganze gerade Zahl größer als 2 ist Summe zweier Primzahlen. (?)
4. Jede reelle Zahl ist Quadrat einer reellen Zahl. (f)
5. Es gibt eine ganze Zahl, deren Quadrat gleich ihrem Doppelten ist. (w, denn $2^2 = 2 \cdot 2$)

"Aachen ist schön" und "die Mensa-Preise sind zu hoch" sind keine Aussagen.

Zu jeder Aussage gibt es ein "Gegenteil", die *Verneinung*.

A: Aussage, Verneinung von A: $\neg A$

Wahrheitstafel

A	$\neg A$
w	f
f	w

Beispiele für Verneinungen:

1. Verneinung von (1.1)(1): $2+3 \neq 5$
2. Verneinung von (1.1)(4): Es gibt eine reelle Zahl, die nicht Quadrat einer reellen Zahl ist.

Zwei Aussagen A und B können zu einer neuen Aussage verknüpft werden. Zwei wichtige *Verknüpfungen* sind:

1. "A und B", auch geschrieben "$A \wedge B$"
2. "A oder B", auch geschrieben "$A \vee B$"

Wahrheitstafel

A	B	$A \wedge B$	$A \vee B$	$A \oplus B$
w	w	w	w	f
w	f	f	w	w
f	w	f	w	w
f	f	f	f	f

$\oplus := (A \wedge \neg B) \vee (\neg A \wedge B)$; “xor”, “exclusives oder”, “entweder oder”

Zwei weitere wichtige Verknüpfungen:

1. $A \Rightarrow B$, “wenn A, dann B” (*Implikation*)
2. $A \Leftrightarrow B$, “genau dann A, wenn B” (*Äquivalenz*)

Wahrheitstafel

A	B	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	w	w
w	f	f	f
f	w	w	f
f	f	w	w

Wenn $A \Rightarrow B$ wahr ist, sagen wir auch: “A impliziert B”, oder “aus A folgt B”.

Wenn $A \Leftrightarrow B$ wahr ist, sagen wir auch: “A ist äquivalent zu B”, oder “A gilt genau dann, wenn B gilt”.

In mathematischen Beweisen zeigt man oft:

1. A ist wahr
2. $A \Rightarrow B$ ist wahr

Beispiel

A: Es regnet.

B: Die Straße ist nass.

$A \Rightarrow B$: Wenn es regnet, ist die Straße nass.

Verknüpfungen von Aussagen, die immer den Wahrheitswert w liefern, heißen *Tautologien*.

Beispiel

1. $(A \wedge (A \Rightarrow B)) \Rightarrow B$

A	B	$A \Rightarrow B$	$A \wedge (A \Rightarrow B)$	$(A \wedge (A \Rightarrow B)) \Rightarrow B$
w	w	w	w	w
w	f	f	f	w
f	w	w	f	w
f	f	w	f	w

2. $A \vee \neg A$
3. $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$ (De Morgan'sches Gesetz)
4. $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ (De Morgan'sches Gesetz)
5. $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$

Tautologien helfen bei Beweisen. So kann man z.B. zeigen, dass $\neg B \Rightarrow \neg A$ wahr ist. Damit ist dann auch $A \Rightarrow B$ wahr.

Z.B.: Wenn die Straße nicht nass ist, dann regnet es nicht.

§ 2 Mengen

(1.2) Definition (nach Cantor, 1895)

Eine *Menge* ist eine Zusammenfassung von bestimmten und wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen. □

Führt bei Leichtsinn zu Widersprüchen:

Barbier von Kreta: "Ich rasiere alle Männer meines Dorfes, die sich nicht selbst rasieren."

Gehört der Barbier zur Menge der Männer, die er rasiert?

Die Objekte, die zu einer Menge gehören, nennen wir *Elemente*.

Schreibweise: $x \in M$, wenn x ein Element der Menge M ist, andernfalls $x \notin M$.

Für zwei Mengen M,N gilt:

$M = N \Leftrightarrow$ Jedes $x \in M$ ist Element von N, und jedes $y \in N$ ist Element von M.

Beschreiben von Mengen

Aufzählen: $\{1,3,17\} \underbrace{=}_{\text{Reihenfolge unwichtig}} \{3,17,1\} \underbrace{=}_{\text{jedes Element ist nur einmal in der Menge}} \{1,3,17,1,3\}$

Beschreiben: $\mathbb{N} \underbrace{:=}_{\text{Definiert das Symbol auf der Seite des Doppelpunktes}}$ Menge der *natürlichen Zahlen* = $\{1,2,3,4,..\}$

$\mathbb{Z} :=$ Menge der *ganzen Zahlen* = $\{...,-2,-1,0,1,2,...\}$

$\mathbb{Q} :=$ Menge der *rationalen Zahlen*

$\mathbb{R} :=$ Menge der *reellen Zahlen*

Aussondern: M Menge, E Eigenschaft (die ein $x \in M$ hat oder nicht). Dann ist $\{x \in M | x$ hat die Eigenschaft E$\}$ eine Menge.

z.B.: $\{z \in \mathbb{Z} | z$ ist ungerade $\}$ Menge der ungeraden ganzen Zahlen.

(1.3) Definition (Konstruktion von Mengen aus Mengen)

M, N Mengen:

1. $N \subseteq M :\Leftrightarrow$ [Für alle $x \in N$ gilt: $x \in M$] N ist *Teilmenge* von M. M ist *Obermenge* von N.
   Es gilt: M = N $\Leftrightarrow [N \subseteq M$ und $M \subseteq N]$
2. $M \cap N := \{x \in M \,|\, x \in N\} \quad (= \{x \in N \,|\, x \in M\})$ *Durchschnitt* von M und N.
3. $M \cup N := \{x \,|\, x \in M$ oder $x \in N\}$ *Vereinigung* von M und N.
4. $M \setminus N := \{x \in M \,|\, x \notin N\}$ *Differenzmenge*
5. $M \times N := \{(x,y) \,|\, x \in M, y \in N\}$ *Kartesisches Produkt* von M und N.
   (x,y) ist geordnetes Paar, d.h. $(x,y) = (x',y') \Leftrightarrow [x = x', y = y']$
6. $P(M) = Pot(M) := \{S \,|\, S \subseteq M\}$ *Potenzmenge* von M.
   $M = \{1,2\}$, $P(M) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
   Allgemein gilt: Hat M n Elemente, dann hat $P(M)$ 2^n Elemente. ($n \in \mathbb{N}_0 := \mathbb{N} \cup \{0\}$)
7. $\emptyset :=$ *leere Menge* (die Menge, die keine Elemente hat)

Sei M Menge.

M heißt *endlich*, wenn M nur endlich viele Elemente besitzt.

Wir schreiben $|M|$ für die Anzahl der Elemente von M. (#M)

$|M| = \infty$ heißt: M ist nicht endlich.

Neue Form von Aussagen, nämlich

"Für alle $x \in M$ gilt $A(x)$"	gesprochen
$\forall x \in M : A(x)$	geschrieben

" Es existiert ein $x \in M$, für das $A(x)$ gilt "	gesprochen
$\exists x \in M : A(x)$	geschrieben

$A(x)$: mathematische Aussage, deren Wahrheitswert von $x \in M$ abhängt.

Beispiel

$x > 5$ keine Aussage
Aussagenform: $x \in \mathbb{Z}$

w für $x = 7$, f für $x = 3$

$\exists x \in \mathbb{Z} : x > 5$ w
$\forall x \in \mathbb{Z} : x > 5$ f

$\forall$: *Allquantor*
$\exists$: *Existenzquantor*

(1.4) Beispiele (vgl. 1.1)

(4) $\forall x \in \mathbb{R}\, \exists y \in \mathbb{R} : x = y^2$ f
(5) $\exists x \in \mathbb{Z} : x^2 = 2x$ w

Verneinungen

$\neg(\forall x \in M : A(x)) \Leftrightarrow \exists x \in M : \neg A(x)$

z.B.: $\forall x \in \mathbb{R} : x^2 > 0$ f
Verneinung: $\exists x \in \mathbb{R} : x^2 \leq 0$ w

$\neg(\exists x \in M : A(x)) \Leftrightarrow \forall x \in M : \neg A(x)$

§ 3 Abbildungen

(1.5) Definition

Seien M, N Mengen. Eine *Abbildung f von M nach N* ist eine Vorschrift, die jedem $x \in M$ genau ein Element aus N zuordnet. Dieses wird mit f(x) bezeichnet.

Schreibweise: $f : M \to N, x \mapsto f(x)$

M heißt *Definitionsmenge* von f,
N heißt *Wertemenge* von f (auch Bildbereich oder Wertebereich).

Sei $x \in M, y = f(x)$.

y heißt das *Bild von x unter* f,
x heißt ein *Urbild von y unter* f.

(1.6) Beispiele

1. $f : \mathbb{N} \to \mathbb{R}, i \mapsto i^2$

   Eine Abbildung $f : \mathbb{N} \to N$ heißt *Folge in N*.
   Andere Schreibweise für Folgen: $a_1, a_2, a_3, \ldots$ oder $(a_i)_{i \in \mathbb{N}} \quad (a_i \in N)$, wobei a_i für den Wert der Abbildung an $i \in \mathbb{N}$ steht. Obige Folge kann auch geschrieben werden als: $1, 4, 9, \ldots$ (oder $(i^2)_{i \in \mathbb{N}}$)
2. Die Addition in $\mathbb{Z}$ ist die Abbildung $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a,b) \mapsto a+b$.
3. Sei M eine Menge.

   $id_M : M \to M, x \mapsto x$ heißt die *Identität* auf M.
4. M: Menge von Glasperlen. F: Menge von Farben.

   $f : M \to F, p \mapsto$ Farbe von p
5. A: Menge der Anwesenden

   $J : A \to \mathbb{N}, P \mapsto$ Geburtsjahr von P

(1.7) Definition und Beispiel (n-Tupel)

Sei M eine Menge (z.B. $M = \mathbb{R}$)

1. Sei $n \in \mathbb{N}$. Wir setzen $\underline{n} := \{1, 2, \ldots, n\} \subseteq \mathbb{N}$
   z.B. $\underline{4} = \{1, 2, 3, 4\}$
2. Ein *n-Tupel* mit Werten in M ist eine Abbildung $t : \underline{n} \to M$

   Ähnliche Schreibweise wie für Folgen:

   $t_1, \ldots, t_n$ meist mit Klammern
   $(t_1, \ldots, t_n)$ mit $t_i := t(i)$

z.B.: $t : \underline{4} \to \mathbb{R}$,
$t(1) = 0, t(2) = \sqrt{3}, t(3) = -\frac{1}{2}, t(4) = \pi$ wird geschrieben als $(0, \sqrt{3}, -\frac{1}{2}, \pi)$.
M^n := Menge aller n-Tupel mit Werten in M $= \{(t_1, \ldots, t_n) | t_i \in M \forall 1 \leq i \leq n\}$. □

(1.8) Definition (Eigenschaften von Abbildungen)

Sei $f : M \to N$ eine Abbildung.

1. Für $X \subseteq M$ sei $f(X) := \{f(x) | x \in X\} = \bigcup_{x \in X} \{f(x)\} \subseteq N$.
   $f(X)$ heißt das *Bild von X unter f*.
2. Für $Y \subseteq N$ sei $f^{-1}(Y) := \{x \in M | f(x) \in Y\} \subseteq M$
   $f^{-1}(Y)$ heißt das *Urbild von Y unter f*. Die Menge $f^{-1}(\{y\}) \quad (y \in N)$ heißt die *Faser von f*.
3. f heißt *surjektiv*, falls $f(M) = N$. ("alle mind. 1 mal")
   f heißt *injektiv*, falls gilt: Sind $x, x' \in M$ mit $f(x) = f(x')$, dann ist $x = x'$. ("alle max. 1 mal")
   f heißt *bijektiv*, wenn f injektiv und surjektiv ist. □

(1.9) Beispiele

1. $f : \mathbb{Z} \to \mathbb{Z}, z \mapsto 2z$ ist injektiv, aber nicht surjektiv.
   $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist bijektiv.
2. $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ ist weder injektiv noch surjektiv.
   $f(\mathbb{R}) = \mathbb{R}_{\geq 0} := \{x \in \mathbb{R} | x \geq 0\}$
   $f_1 : \mathbb{R} \to \mathbb{R}_{\geq 0}, x \mapsto x^2$ ist surjektiv.
   Fasern von $f_1 : f_1^{-1}(\{y\}) = \{-\sqrt{y}, \sqrt{y}\}$
3. Vgl. (1.6) (4): M Glasperlen, F Farben.
   f: $M \to$ F, $p \mapsto$ Farbe von p.
   $f^{-1}(\{\text{rot}\})$ = Menge der roten Perlen in M.
   f ist injektiv, falls zu jeder Farbe aus F höchstens eine Perle dieser Farbe in M gibt.

(1.10) Definition (Zusammenfügen von Abbildungen)

Seien L, M, M', N Mengen mit $M \subseteq M'$, $g : L \to M'$ und $f : M \to N$ eine Abbildung mit $g(L) \subseteq M$

Dann heißt die Abbildung $f \circ g : L \to N, x \mapsto (f \circ g)(x) := f(g(x))$ die *Komposition von f mit g*.

// Ein hübsches Bild □

(1.11) Beispiele

$f : \mathbb{R}_{\geq 0} \to \mathbb{R}, x \mapsto \sqrt{x}$
$g : \mathbb{R} \to \mathbb{R}, x \to (x-3)^2$

$f \circ g : \mathbb{R} \to \mathbb{R}, x \mapsto \sqrt{(x-3)^2} = |x-3|$ □

(1.12) Bemerkung (Umkehrabbildung)

Sei $f : M \to N$ bijektiv. Dann besitzt f eine *Umkehrabbildung*. Dies ist die Abbildung $g : N \to M$ mit $g \circ f = id_M$ und $f \circ g = id_N$. Die Umkehrabbildung g ist bijektiv und durch f eindeutig bestimmt. Sie wird mit f^{-1} bezeichnet.

f bijektiv, $y \in N \quad [f : M \to N]$
$f^{-1}(\{y\}) = \{x\} \forall x \in N$
f^{-1}Umkehrabbildung : $f^{-1}(y) = x$

(1.21) Beispiele

1. $f : \mathbb{R} \to \mathbb{R}, x \mapsto 2x$ ist bijektiv,
   $f^{-1} : \mathbb{R} \to \mathbb{R}, x \mapsto \frac{1}{2}x$ ist die Umkehrabbildung.
2. $f : \mathbb{R}_{\geq 0} \to R_{\geq 1}, x \to x^2 + 1$ ist bijektiv,
   $f^{-1} : \mathbb{R}_{\geq 1} \to R_{\geq 0} x \mapsto \sqrt{x-1}$ ist die Umkehrabbildung. □

Grenzfälle und Konventionen

Sei M eine Menge.

- Es existiert genau eine Abbildung $f : \varnothing \mapsto M$.
  - f ist injektiv, aber nicht surjektiv außer $M = \varnothing$.
  - f ist bijektiv für $M = \varnothing$.
- Ist $M \neq \varnothing$, dann existiert keine Abbildung $f : M \mapsto \varnothing$

§ 4 Relationen

M, N Mengen.

(1.21) Definition

1. Eine Teilmenge $R \subseteq M \times N$ heißt *Relation zwischen M und N* oder *Relation auf M*, falls $N = M$.
   Schreibweise: $xRy :\Leftrightarrow (x,y) \in R$.
2. Eine Relation auf M, d.h. $R \subseteq M \times M$, heißt

   (R) *reflexiv*, falls also $(x,x) \in R \; \forall x \in M$.

   (S) *symmetrisch*, falls gilt: $(x,y) \in R \Rightarrow (y,x) \in R$.

   (A) *antisymmetrisch*, falls gilt $(x,y) \in R$ und $(y,x) \in R \Rightarrow x = y$.

   (T) *transitiv*, falls gilt $(x,y) \in R$ und $(y,z) \in R \Rightarrow (x,z) \in R$.
3. Eine Relation, die (R),(S),(T) erfüllt, heißt *Äquivalenzrelation*.
4. Eine Relation, die (R),(A),(T) erfüllt heißt *(Halb-)Ordnung*. □

(1.22) Beispiele

(A) aus der Mathematik

(1) $M = \mathbb{R}$

- R = "<" $[(x,y) \in R :\Leftrightarrow x < y]$ < ist transitiv, nicht reflexiv, nicht symmetrisch.
- R = "$\leq$" ist (R),(A),(T) also Ordnung.
  "$\leq$" ist sogar eine Totalordnung, d.h. $\forall a,b \in \mathbb{R}$ gilt $a \leq b$ oder $b \leq a$, d.h. je zwei Elemente von $\mathbb{R}$ sind bzgl. "$\leq$" vergleichbar.

(2) M = P(N) $[\{S|S \subseteq N\}]$

R = "$\subseteq$" (Inklusion) ist Ordnung, aber keine Totalordnung:
$\{1\},\{2\} \in P(\{1,2\})$, aber $\{1\} \not\subseteq \{2\}$ und $\{2\} \not\subseteq \{1\}$.

(3) Sei $f : M \to N$ Abbildung

- f ist Relation zwischen M und N, $\{(x,f(x))|x \in M\} \subseteq M \times N$.
- R_f definiert durch $xR_fx' :\Leftrightarrow f(x) = f(x')$ ist Äquivalenzrelation auf M.

(4) "=" ist Äquivalenzrelation auf M (zu $R = \{(x,x)|x \in M\}$)

(5) $M = \mathbb{Z}$

- "$\equiv_2$" ("kongruent modulo 2 zu...") definiert durch $x \equiv_2 y :\Leftrightarrow x - y$ gerade ist Äquivalenzrelation auf $\mathbb{Z}$. (0 ist gerade.)
- "|" definiert durch $x|y$ ("x teilt y") $:\Leftrightarrow \exists z \in \mathbb{Z} : xz = y$ erfüllt (R), (T).

(B) aus dem täglichen Leben

(1) Menge der Anwesenden
$xEy :\Leftrightarrow x$ hat das gleiche Elternpaar wie y.
$xGy :\Leftrightarrow x$ hat das gleiche Geburtsdatum wie y [Tag + Monat].

(2) M Menge von Glasperlen [vgl. (1.6)(4) u. (1.8)(2)]
$xCy :\Leftrightarrow x$ hat die gleiche Farbe wie y.

E,G,C sind Äquivalenzrelationen □

Äquivalenzrelationen fassen Elemente einer Menge unter einem "Gesichtpunkt" zusammen.

(1.23) Definition (Äquivalenzklasse)

Sei R eine Äquivalenzrelation auf M. Für $x \in M$ heißt $C_x := \{y \in M | xRy\}$ eine *Äquivalenzklasse* von R.
M/R := Menge aller Äquivalenzklassen ($\subseteq P(M)$). □

(1.24) Beispiele (vgl. (1.22)

(1) $f : M \to N$ Abbildung, R_f aus (1.22)(A)(3).
$x \in M : C_x = \{x' \in M | f(x) = f(x')\} = f^{-1}(\{f(x)\})$.
M/R_f : Menge der nicht-leeren Fasern von f.

(2) R: "=" $x \in M, C_x = \{x\}$.
$M/_= \quad = \{\{x\} | x \in M\}$.

(3) $M = \mathbb{Z}$, "$\equiv_2$"
$C_0 = \{y \in \mathbb{Z} | y \text{ gerade}\}$
$C_1 = \{y \in \mathbb{Z} | 1 - y \text{ gerade}\} = \{y \in \mathbb{Z} \mid y \text{ ungerade}\}$

(4) M = Menge der Anwesenden
R = E: Äquivalenzklassen: "Geschwistermenge"
R = G: $C_{\text{Hiß}} = \{y \in M \mid y \text{ hat am 27.7. Geburtstag}\}$.

(5) M = Menge von Glasperlen
R = C: Äquivalenzklasse einer Perle p: $\{y \in M | y \text{ hat die gleiche Farbe wie } p\}$. □

(1.25) Definition (Partition)

Eine *(Mengen-)Partition* von M besteht aus einer Menge P nicht-leerer Teilmengen von M (d.h. $P \subseteq P(M)$) mit:

(1) $M = \bigcup_{C \in P} C$ (jedes $x \in M$ liegt in einem $C \in P$)

(2) Sind $C, C' \in P$ mit $C \neq C'$, dann ist $C \cap C' = \emptyset$ (jedes $x \in M$ liegt in höchstens einen $C \in P$)

Die Elemente aus P heißen *Teile der Partition*.

Beispiel

$M = \mathbb{Z}, \equiv_2$
C_0 = gerade Zahlen
C_1 = ungerade Zahlen
$P = C_0, C_1$

(1) $C_0 \cup C_1 = \mathbb{Z}$.
(2) $C_0 \cap C_1 = \emptyset$.

(1.26) Satz

1. Sei R eine Äquivalenzrelation auf M. Dann ist M/R eine Partition von M.

   Partition von M: $P \subseteq P(M)$ mit

   (1) $\bigcup_{C \in P} C = M$

   (2) $C, C' \in P, \quad C \neq C' \Rightarrow C \cap C' = \emptyset$

   $R \subseteq M \times M$ Relation $xRy : (x,y) \in R$

   (R) $xRx \quad \forall x \in R$

   (S) $xRy \quad \Rightarrow \forall x, y \in R$

   (T) xRy und $yRz \quad \Rightarrow xRz \forall x, y, z \in R$

   R Äquivalenzrelation, $x \in M$.

   $C_x := \{y \in M | xRy\}$ Äquivalenzklasse

   $M/R := \{C_x | x \in M\}$.

2. (Umkehrung von (1)) Sei P eine Partition von M. Dann existiert eine Äquivalenzrelation R auf M mit $M/R = P$.

Beweis:

a) M/R ist Partition von M:
(a) $x \in M \underbrace{\Rightarrow}_{(R)} xRx \underbrace{\Rightarrow}_{Def.} x \in C_x$. Damit $M = \bigcup_{x \in M} C_x$.
(b) Zu zeigen: $x, y \in M$ mit $C_x \neq C_y \Rightarrow C_x \cap C_y = \emptyset$.
Beweis durch Kontraposition:
$C_x \cap C_y \neq \emptyset \Rightarrow C_x = C_y$
Sei $z \in C_x \cap C_y \quad \underbrace{\Rightarrow}_{Def.} \quad xRz$ und $yRz \quad \underbrace{\Rightarrow}_{(S)} \quad xRz$ und $zRy \quad \underbrace{\Rightarrow}_{(T)} \quad xRy$.

Sei $x' \in Cx \underbrace{\Rightarrow}_{Def.} xRx' \underbrace{\Rightarrow}_{(S)} x'Rx \underbrace{\Rightarrow}_{(T)} x'Ry \underbrace{\Rightarrow}_{(S)} yRx' \underbrace{\Rightarrow}_{Def.} x' \in C_y$.

Damit ist gezeigt: $C_x \subseteq c_y$. Analog $C_y \subseteq C_x$. Zusammen: $C_x = C_y$.

b) Sei P Partition von M.

Definiere $R \subseteq M \times M$ durch $(x,y) \in R :\Leftrightarrow$ Es ex. $C \in P$ mit $x \in C$ und $y \in C$.

Dann ist R eine Äquivalenzrelation auf M:

(R) Sei $x \in M, C \in P$ mit $x \in C$ [(1.25)(1)] $\Rightarrow (x,x) \in R$

(S) Sei $(x,y) \in R \Rightarrow (y,x) \in R$ [Def.]

(T) Seien $x,y,z \in M$ mit $(x,y) \in R$ und $(y,z) \in R$.

$\Rightarrow$ Es ex. $C, C' \in P$ mit $x,y \in C$ und $y,z \in C'$

$\Rightarrow y \in C \cap C' \underbrace{\Rightarrow}_{(1.25)(2)} C = C'$

$\Rightarrow (x,z) \in R$ [Def.]

Sei $x \in M, C \in P$ mit $x \in C \quad \Rightarrow \quad \underbrace{C_x}_{\text{Äquivalenzklasse von x bzgl. R}} = C$

Damit: M/R = P

□

§ 5 Einige Beweisprinzipien

(A)

Direkter Beweis (von Aussagen der Form “A => B”)

(B)

Indirekter Beweis

↙ ↘

Beweis durch Kontraposition Widerspruchsbeweis

(C)

Beweis durch vollständige Induktion.

zu (C):

Beruht auf folgender Eigenschaft von $\mathbb{N}$:
(I) Sei $A \subseteq \mathbb{N}$. Dann gilt: Ist $1 \in A$ und ist für jedes $n \in A$ auch $n+1 \in A$, dann ist $A = \mathbb{N}$.

Behauptungen der Form “Für alle $n \in \mathbb{N}$ gilt $A(n)$” lassen sich nach folgendem Schema (*“vollständige Induktion”*) beweisen:

Induktionsanfang:

Zeige: $A(1)$ ist wahr

Induktionsschritt:

Annahme/Induktionsvorraussetzung: $A(n)$ ist wahr.

Zeige: $A(n+1)$ ist wahr. Dann gilt $A(n)$ für alle $n \in \mathbb{N}$, denn die Menge $A := \{n \in \mathbb{N} | A(n) \text{ ist wahr}\}$ erfüllt die Vorraussetzungen von (I), ist also gleich $\mathbb{N}$.

(1.27) Satz (Induktionsbeweis-Beispiel)

Für alle $n \in \mathbb{N}$ ist $\underbrace{\sum_{i=1}^{n} i}_{1+2+3+\ldots+n} = \frac{1}{2}n(n+1)$.

Beweis: Induktion über n:

$n = 1$: Linke Seite: $\sum_{i=1}^{1} i = 1$

Rechte Seite: $\frac{1}{2} \cdot 1 \cdot (1+1) = 1$

$n \to n+1$: Annahme: $\sum_{i=1}^{n} i = \frac{1}{2}n(n+1)$.

$\Rightarrow \sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n+1)$

$= \frac{1}{2} \cdot n \cdot (n+1) + (n+1) = \underbrace{(\frac{1}{2}n+1)}_{\frac{1}{2}(n+2)}(n+1)$

$= \frac{1}{2}(n+1)(n+2)$. □

zu (A):

Direkter Beweis für "$A \Rightarrow B$":

Wir nehmen an, dass A wahr ist und folgern daraus, dass B wahr ist. Dann ist auch $A \Rightarrow B$" wahr:

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

(1.28) Satz (Direkter Beweis-Beispiel)

Für alle $n \in \mathbb{N}$ gilt:

n ungerade $\Rightarrow n^2$ ungerade $\quad (A(n) \Rightarrow B(n))$

Beweis: Sei n ungerade [Annahme]. Dann ex. $k \in \mathbb{N}$ mit $n = 2k-1$.

Dann ist $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = \underbrace{2(2k^2-2k)}_{\text{ungerade}} + 1$

Also ist n^2 ungerade. □

zu (B):

Beweis durch Kontraposition. Beruht auf der Tautologie: $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$.

Um zu zeigen: "$A \Rightarrow B$" ist wahr zeigen wir stattdessen: "$\neg B \Rightarrow \neg A$" ist wahr.

(1.29) Satz (Kontrapositionsbeweis-Beispiel)

Für alle $n \in \mathbb{N}$ gilt: n^2 gerade $\Rightarrow n$ gerade.

Beweis: Wir zeigen $\underbrace{\neg(n \text{ gerade})}_{n \text{ ungerade}} \Rightarrow \underbrace{\neg(n^2 \text{ gerade})}_{n^2 \text{ ungerade}}$

Die behauptete Aussage folgt aus (1.28). □

zu (B):

Beweis durch Widerspruch: Um zu zeigen: "A ist wahr" zeigen wir $\neg A \Rightarrow (B \wedge \neg B)$ " ist wahr. Da "$B \wedge \neg B$" falsch ist (das ist der Widerspruch) ist $\neg A$ falsch, d.h. A ist wahr.

(1.30) Satz (Widerspruchsbeweis-Beispiel)

$\sqrt{2} \notin \mathbb{Q}$ [Aussage A]

Beweis: Annahme: $\sqrt{2} \in \mathbb{Q}$ [Aussage $\neg A$]

$\Rightarrow$ Es ex. $m,n \in \mathbb{N}$ mit $\sqrt{2} = \frac{m}{n}$ und $\underbrace{[m \text{ ungerade oder } n \text{ ungerade}]}_{[\text{Aussage B}]}$

$\Rightarrow 2n^2 = m^2$ (mal n und Quadrieren)

$\Rightarrow m^2$ gerade (Def. von gerade)

$\Rightarrow m$ gerade (Satz (1.29))

$\Rightarrow$ Es ex. $k \in \mathbb{N}$ mit $m = 2k$

$\Rightarrow 2n^2 = (2k^2) = 4k^2$

$\Rightarrow n^2 = 2k^2$ (durch 2 geteilt)

$\Rightarrow n^2$ ist gerade

$\Rightarrow n$ gerade (Satz 1.29)

$\Rightarrow \underbrace{m \text{ gerade und } n \text{ gerade}}_{[\text{Aussage } \neg B]} \lightning$

Also ist die Aussgae $\neg A$ falsch, d.h. $A(\sqrt{2} \notin \mathbb{Q})$ wahr. $\square$

2 Kombinatorik

Bestimmung von Anzahlen, z.B.: Wie viele verschiedene Lottoergebnisse gibt es?

§ 1 Permutationen und Kombinationen

Sei A endliche Menge, $|A| = n \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

(2.1) Definition (Permutation)

Sei $k \in \mathbb{N}_0$, $k \leq n$.

Eine "Auswahl" von k Elementen aus A, wobei es auf die Reihenfolge ankommt, heißt *k-Permutation* (oder *Variation* oder *geordnete Auswahl*) aus A. *Permutation von A* = n-Permutation aus A. □

Beispiele:

$A = \underline{5} = \{1,2,3,4,5\}$

$(4,3,2), (4,2,3), (3,5,1)$ sind (verschiedene) 3-Permutationen

$(1,3,2,5,4), (1,4,5,3,2)$ sind Permutationen

Mathematisch:

k-Permutation: k-Tupel $(a_1, \ldots, a_k) \in A^k$ mit $a_i \neq a_j$ falls $i \neq j$.

(2.2) Definition (Fakultät)

Für $n \in \mathbb{N}$ sei $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ *(n-Fakultät)*

Konvention: $0! = 1$

Beispiele:

$5! = 120$; $6! = 720$

(2.3) Bemerkung (Anzahl Permutationen)

$k \in \mathbb{N}, k \leq n$.

(1) Die *Anzahl der k-Permutationen aus A* ist $\frac{n!}{(n-k)!} = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)$.

(2) Anzahl der Permutationen von A ist $n!$

Beweis:

(2) folgt aus (1) mit $k = n$.

(1) Für die Auswahl einer k-Permutation gibt es

an Position 1: n Möglichkeiten,
an Position 2: $n-1$ Möglichkeiten,
$\vdots$
an Position k: $n-k+1$ Möglichkeiten.

Zusammen: $n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$. □

Beispiel für das Beweisverfahren:

2-Permutationen aus $\{1,2,3,4\}$:

1	2	1	3	1	4	3
2	1	2	3	2	4	3
3	1	3	2	3	4	3
4	1	4	2	4	3	$3 \Rightarrow \Sigma 12 = 4 \cdot 3$ Stück

Eine Permutation von A ist eine Anordnung von A. Es gibt $n!$ viele davon.

(2.4) Definition (Kombination)

Sei $k \in \mathbb{N}, k \leq n$. Eine "Auswahl" von k Elementen aus A wobei es **nicht** auf die Reihenfolge ankommt, heißt eine *k-Kombination* (oder *ungeordnete Auswahl*) aus A.

$$\{4,3,2\} = \{3,2,4\}, \{3,5,1\} \quad \text{3-Kombinationen}$$

Mathematisch: k-Kombination aus A: k-elementige Teilmenge von A.

(2.5) Bemerkung (Anzahl Kombinationen)

$k \in \mathbb{N}, k \leq n$.

Die *Anzahl der k-Kombinationen aus A* (= Anzahl der k-elementigen Teilmengen von A) ist:

$$\frac{n!}{k!(n-k)!}$$

Beweis:

Jede k-Kombination liefert durch Anordnen der Elemente k! k-Permutationen.

x: gesuchte Anzahl $\Rightarrow x \cdot k! = \frac{n!}{(n-k)!} \Rightarrow x = \frac{n!}{k!(n-k)!}$ □

(2.6) Beispiel (Lotto)

$n = 49, k = 6$ (Lotto)

Ein ausgefüllter Lottoschein ist eine 6-Kombination aus $\underline{49}$. Gesamtzahl davon:

$$\frac{49!}{6!43!} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13.983.816$$

(2.7) Bemerkung (Ziehen mit Zurücklegen)

Sei $k \in \mathbb{N}, k \leq n$.

Die Anzahl der Möglichkeiten, k Elemente aus A auszuwählen, wobei jedes Element mehrfach vorkommen kann ("Ziehen mit Zurücklegen") ist

$$n^k$$

falls es auf die Reihenfolge ankommt, und

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

falls es **nicht** auf die Reihenfolge ankommt.

Beweis:

Mit Reihenfolge: Bei jedem der k Züge hat man n Möglichkeiten. [Eine solche "Auswahl" ist ein Element aus A^k.]

Ohne Reihenfolge:

1. Schritt: Nummeriere die Elemente aus A : $a_1, a_2, a_3, \ldots, a_n$.
2. Schritt: Nach dem Umsortieren besteht eine Auswahl aus der Folge:

$$(*)\ \underbrace{a_1, a_1, \ldots, a_1}_{s_1\text{-Stück}}, \underbrace{a_2, \ldots, a_2}_{s_2\text{-Stück}}, \ldots, \underbrace{a_n, \ldots, a_n}_{s_n\text{-Stück}}$$

Also: $s_i \in \mathbb{N}_0$: Anzahl der a_i in Auswahl. Es gilt: $s_1 + s_2 + \ldots + s_n = k$.

Wir kodieren eine Auswahl (*) durch ein binäres Wort (=0,1-Folge).

$$(**)\ \underbrace{111\ldots1}_{s_1 \text{ Einsen}}\,0\,\underbrace{111\ldots1}_{s_2 \text{ Einsen}}\,0\ldots\underbrace{111\ldots1}_{s_n \text{ Einsen}}$$

Die Nullen stehen an den Übergängen $a_i \to a_{i+1}$.

Das binäre Wort (**) besteht aus k Einsen und n-1 Nullen, es hat also die Gesamtlänge $n+k-1$.

Jedes solche Wort ist durch die $n-1$ Positionen (innerhalb von $\{1,...,n+k-1\}$) eindeutig bestimmt.

Es gibt also genau $\frac{(n+k-1)!}{(n-k)!k!} = \frac{(n+k-1)!}{k!(n-1)!}$ solcher Wörter.

□

§ 2 Binomialkoeffizienten

(2.8) Definition (Binominalkoeffizient)

Seien $k, n \in \mathbb{N}_0$, $k \leq n$. Dann heißt $\binom{n}{k} := \frac{n!}{k!(n-k)!}$ der *Binomialkoeffizient "n über k"*.

$\binom{n}{0} = \frac{n!}{0!n!} = 1$

$\binom{n}{n} = \frac{n!}{n!0!} = 1$

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

(2.9) Satz (Binomischer Lehrsatz)

Für $n \in \mathbb{N}$ und $a, b \in \mathbb{R}$ gilt:

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + ... + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$$

Beweis

Kombinatorisch:

$$(a+b)^n = (a+b)(a+b)\dots(a+b) \quad \text{[n Faktoren (a+b)]}$$

Ausmultiplizieren der rechten Seite:

Jeder Term enthält genau einen Faktor, a und b, aus jedem der n Faktoren (a+b). Jeder Term ist also von der Form $a^{n-k}b^k$, hier sind aus n Faktoren $(a+b)$ genau k b's gewählt worden.

Es gibt genau $\binom{n}{k}$ Möglichkeiten, k solche b's auszuwählen (2.5). Also kommt der Term $a^{n-k}b^k$ genau $\binom{n}{k}$ mal vor. □

(2.10) Satz

Seien $k, n \in \mathbb{N}_0$, $k \leq n$. Dann gilt:

1. $\binom{n}{k} = \binom{n}{n-k}$.
2. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ für $k \geq 1$.
3. $\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i} = \binom{m+n}{k}$ für $m \in \mathbb{N}_0$. (Van der mondsche Identität)

Beweis:

(1), (2) Nachrechnen.

(3) Kombinatorisch:

Seien $A = \underline{n} = \{1, \dots, n\}, \quad B = \{n+1, \dots, n+m\}$

Anzahl der k-elementigen Teilmengen von $A \cup B = n+m$ mit i Elementen aus B ist $\binom{m}{i}\binom{n}{k-i}$.

□

$n, k \in \mathbb{N}_0, k \leq n$

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

$0! = 1$

$\binom{n}{n} = 1 = \binom{n}{0}$

$[\binom{n}{k} = 0$, falls $k > n]$

$\binom{n}{k}$ = Anzahl der k-elementigen Teilmengen einer n-elementigen Menge

(2.11) Satz

Sei A eine endliche Menge mit $|A| = n \in \mathbb{N}_0$. Dann ist $|P(A)| = 2^n$.

Beweis:

Die Anzahl der k-elementigen Teilmengen von A ist $\binom{n}{k}$, $0 \leq k \leq n$.

$\Rightarrow |P(A)| = \sum_{k=0}^{n} \binom{n}{k} = (1+1)^n = 2^n.$ □

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

(2.10)(2): $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

(2.12) Definition (Pascalsches Dreieck)

Dies ist das Dreieck von Zahlen:

n																						
0							$\binom{0}{0}$										1					
1				$\binom{1}{0}$				$\binom{1}{1}$							1		1					
2			$\binom{2}{0}$			$\binom{2}{1}$			$\binom{2}{2}$					1		2		1				
3	$\binom{3}{0}$			$\binom{3}{1}$			$\binom{3}{2}$			$\binom{3}{3}$			1		3		3		1		
	$\dots$											1		4		6		4		1	

"Jede Zahl ist die Summe der zwei dadrüber stehenden Zahlen."

§ 3 Kombinatorische Beweisprinzipien

Sei A eine endliche Menge.

(2.13) Bemerkung (Summenregel)

Seien $A_1,\ldots,A_l \subseteq A$ mit $A_i \cap A_j = \emptyset$ für $i \neq j$, und $A = \bigcup_{i=1}^{l} A_i$.

[A ist die **disjunkte** Vereinigung der A_i, oder $\{A_1,....,A_l\}$ ist eine Partition von A.]

Dann ist $|A| = |\bigcup_{i=1}^{l} A_i| = \sum_{i=1}^{l} |A_i|$.

Beweis:

Klar. Diese Regel haben wir z.B. im Beweis von (2.11) verwendet. □

(2.14) Definition (Produktregel)

Seien $A_1,\ldots,A_l$ endliche Mengen und $A = A_1 \times A_2 \times \ldots \times A_l$ $(= \{(a_1,\ldots,a_l) | a_i \in A_i, 1 \leq i \leq l\})$.

Dann ist $|A| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_l|$

Beweis:

Klar. Dies haben wir z.B. beim Beweis von (2.7) (mit Reihenfolge) verwendet $(|A^k| = |A|^k)$. □

$\bigcup_{i=1}^{l} A_i$, wenn die A_i nicht disjunkt wird ?

(2.15) Satz (Inklusions-/Exklusions-Prinzip)

1. Sei $A = A_1 \cup A_2 \quad \Rightarrow \quad |A| = |A_1| + |A_2| - |A_1 \cap A_2|$.
   [In $|A_1| + |A_2|$ wird jedes Element aus $A_1 \cap A_2$ doppelt gezählt.]
2. Sei $A = A_1 \cup A_2 \cup A_3 \quad \Rightarrow \quad |A| = (|A_1| + |A_2| + |A_3|) - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) + (|A_1 \cap A_2 \cap A_3|)$.
   Die Elemente aus $A_1 \cap A_2 \cap A_3$ werden zunächst 3 mal gezählt, danach 3 mal abgezogen, zum Schluss einmal addiert.

3. Sei $A = \bigcup_{i=1}^{l}$. Dann gilt: $|A| = |\bigcup_{i=1}^{l} A_i| = \sum_{k=1}^{l} (-1)^{k-1} \sum_{1 \le i_1 \le i_2 \le \ldots \le i_k \le l} |\bigcap_{j=1}^{k} A_{ij}|$.

$|\bigcup_{i=1}^{l} A_i| = \sum_{k=1}^{l} (-1)^{k-1} \sum_{\substack{J \subseteq \underline{l}, \\ |J|=k}} |\bigcap_{j \in J} A_j|$.

Beweis:

Sei $a \in A$.

Links wird a genau einmal gezählt. Angenommen, a liegt in genau $m\,(1 \le m \le l)$ der Mengen A_i, deren Nummern die Menge M bilden.

Ist $J \subseteq \underline{l}$, $|J| = k$, dann ist $a \in \bigcap_{j \in J} A_j \Leftrightarrow J \subseteq M$. In diesem Fall ist $k = |J| \le m$.

In $\sum_{\substack{J \subseteq \underline{l}, \\ |J|=k}} |\bigcap_{j \in J} A_j|$ wird a also genau $\binom{m}{k}$ mal gezählt.

Auf der rechten Seite wird a also genau $\sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k}$ mal gezählt.

Aus dem Binomischen Lehrsatz folgt: $0 = (1-1)^m = \sum_{k=0}^{m} \binom{m}{k} 1^{m-k} (-1)^k = 1 - \sum_{k=0}^{m} \binom{m}{k} (-1)^{k-1}$

$\Rightarrow \sum_{k=1}^{m} (-1)^{k-1} \binom{m}{k} = 1$, d.h. a wird auch rechts genau einmal gezählt. □

(2.16) Beispiel

Sei $A = \{n \in \mathbb{N} | n \le 100, 2|n \text{ oder } 3|n \text{ oder } 5|n\} = A_2 \cup A_3 \cup A_5$ mit $A_i := \{n \in \mathbb{N} | n \le 100, i|n\}$.

$|A_i| = \lfloor \frac{100}{i} \rfloor$ (Für $x \in \mathbb{R}$ sei $\lfloor x \rfloor = max\{z \in \mathbb{Z} | z \le x\}$.)

$A_2 \cap A_3 = A_6$, da eine ganze Zahl genau dann durch 2 **und** durch 3 teilbar ist, wenn sie durch 6 teilbar ist.

Analog: $A_2 \cap A_5 = A_{10}, A_3 \cap A_5 = A_{15}, A_2 \cap A_3 \cap A_5 = A_{30}$.

Also: $|A_2 \cup A_3 \cup A_5| = |A_2| + |A_3| + |A_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}| = 50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$.

(2.17) Bemerkung (Schubfachprinzip)

Seien A, B endliche Mengen. Dann gilt: Ist $f : A \to B$ eine Abbildung, und $|A| > |B|$,

dann ex. $b \in B$ mit $\underbrace{|f^{-1}(\{b\})|}_{=\{a \in A | f(a)=b\}} \geq 2$.

[Unter den genannten Vorraussetzungen ex. $b \in B$, und $a_1, a_2 \in A$ mit $a_1 \neq a_2$ und $f(a_1) = f(a_2) = b$.]

(2.18) Beispiel

In jeder Menge von 13 Personen gibt es zwei, die im gleichen Monat Geburtstag haben.

§ 4 Permutationen

Sei A endliche Menge mit $|A| = n$. Wir schreiben $A = \{a_1, a_2, \ldots, a_n\}$

(2.19) Definition (Permutation)

Eine bijektive Abbildung $\pi : A \to A$ heißt *Permutation von A*

$$S_A := \{\pi : A \to A | \ \pi \text{ ist Permutation}\}$$

Schreibweise (vorläufig):

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ \pi(a_1) & \pi(a_2) & \ldots & \pi(a_n) \end{pmatrix}$$

Das n-Tupel $(\pi(a_1), \pi(a_2), \ldots, \pi(a_n))$ enthält jedes Element von A genau ein mal, es ist also eine n-Permutation im Sinne von Definition (2.1).

Beispiel für $A = \underline{n} = \underline{11}$:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 3 & 6 & 2 & 7 & 4 & 1 & 9 & 11 & 10 \end{pmatrix} \text{ (*)}$$

Für $A = \underline{n}$ schreiben wir $S_n := S_A$.

(2.20) Bemerkung

$|S_A| = |S_n| = n!$

Beweis: Dies folgt aus (2.3)(2). □

(2.21) Bemerkung (Komposition)

Die *Komposition* (vgl. Def. (1.9)) von Bijektionen ist wieder eine Bijektion.

Schreibweise: Sei $\pi \in S_A$

$\pi^2 := \pi \circ \pi$, $\pi^3 := \pi \circ \pi \circ \pi$, ...

Konvention: $\pi^0 := id_A \in S_A$

(2.22) Beispiele

1. Berechnung von $\pi \circ \psi \in S_n$: $\pi \circ \psi(1) = \pi(\psi(1))$

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}}_{\pi} \circ \underbrace{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}}_{\psi} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

2. $\pi(1) = 2, \quad \pi^2(1) = \pi(\pi(1)) = \pi(2) = 3, \quad \pi^3(1) = \pi(3) = 1$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

3. π die Permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 3 & 6 & 2 & 7 & 4 & 1 & 9 & 11 & 10 \end{pmatrix}$ (*) aus Def. 2.19

$$(1 \quad 5 \quad 2 \quad 8) \circ (3) \circ (4 \quad 6 \quad 7) \circ (9) \circ (10 \quad 11)$$

(Bild eines 4-Zykel-Kreises) (Bild eines 1-Zykel-Kreises) .....

(2.23) Definition und Bemerkung (Träger, Zykel)

1. Sei $1 \leq k \leq n$.

   Ein k-Zykel von S_n ist eine Permutation $\sigma \in S_n$ mit: Es ex. $i_1, i_2, \ldots, i_k \in \underline{n}$

   (paarweise verschieden) mit $\sigma(i_j) = i_{j+1}, 1 \leq j < k$ und $\sigma(i_k) = i_1$.

   Grafik: $i_k \to i_1 \to i_2 \to .... \to i_k$

   und $\sigma(l) = l \forall\, l \in \underline{n} \backslash \{i_1, \ldots, i_k\}$.

   Die Menge $\{i_1, \ldots, i_k\}$ heißt der *Träger von* σ, geschrieben T_σ.
2. Ein *Zykel* von S_n ist ein k-Zykel von S_n für ein $1 \leq k \leq n$.
3. Sei $\pi \in S_n$. Dann ex. Zykeln $\sigma_1, \ldots, \sigma_l$ von S_n mit paarweise disjunkten Trägern, wir sagen: disjunkte Zykeln mit $\pi = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_l$.
4. Seien $\sigma_1, \sigma_2 \in S_n$ disjunkte Zykel, dann ist $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

Beweis:

(3) Verfahren wie (2.22)(3):
In der Folge 1, $\pi(1), \pi^2(1), \ldots, \pi^n(1)$ stehen zwei gleiche Einträge (Schubfachprinzip), etwa $\pi^k(1) = \pi^l(1)$ mit $l > k$

$$\Rightarrow \pi^k(\pi^{l-k}(1)) = \pi^k(1) \overset{\pi^k \text{injektiv}}{\Rightarrow} \pi^{l-k}(1) = 1$$

Sei m minimal mit $\pi^m = 1 \quad (m \geq 0)$

$$\Rightarrow T_{\sigma_1} := \{1, \pi(1), \pi^2(1), \ldots, \pi^{m\cdot 1}(1)\} \text{ ist der Träger eines m-Zykels } \sigma_1.$$

Definiere σ_2 analog auf $\underline{n} \backslash T_{\sigma_1}$, falls $T_{\sigma_1} \neq \underline{n}$. Erhalte $\sigma_1, \ldots, \sigma_l$.

Weil die Träger der σ_i paarweise disjunkt sind, gilt $\pi = \sigma_1 \circ \ldots \circ \sigma_l$

(4) Selbst.

Schreibweise für Zykel:

$(i_1, i_2, \ldots, i_k) :=$ Grafik: $i_k \to i_1 \to i_2 \to .... \to i_k$

$$(3 \quad 2 \quad 1 \quad 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

Permutation aus (2.19):

$$(1 \quad 5 \quad 2 \quad 8)(3)(4 \quad 6 \quad 7)(9)(10 \quad 11)$$

Zykel der Länge 1 werden **oft** weggelassen.

$$(1 \quad 5 \quad 2 \quad 8)(4 \quad 6 \quad 7)(10 \quad 11) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 3 & 6 & 2 & 7 & 4 & 1 & 9 & 11 & 10 \end{pmatrix}$$

(2.24) Definition (Transposition)

Ein 2-Zykel heißt *Transposition*. Ist $(i \;\; j) = \tau$ eine Transpositon, dann sagen wir: τ vertauscht die Ziffern i und j.

- $\pi \in S_n$ ist Produkt (bzgl. "$\circ$") von Zykeln
- Ein Zykel ist Produkt von Transpositionen z.B. $(1\ 2\ 3\ 4) = (3\ 4) \circ (2\ 4) \circ (1\ 4)$
- Eine TP (Transposition) ist Produkt von TPs benachbarter Ziffern

z.B. $(1\ 4) = (3\ 4) \circ (2\ 3) \circ (1\ 2) \circ (2\ 3) \circ (3\ 4)$

$\Rightarrow \pi$ ist Produkt von TP benachbarter Ziffern.

(2.25) Satz

1. Sei $\sigma = (i_1 \ \ i_2 \ \ \dots \ \ i_k)$ ein k-Zykel, $k \geq 2$. Dann ist σ ein Produkt von TPs.
2. Sei $\tau \in S_n$ eine TP. Dann ist τ ein Produkt (einer ungeraden Anzahl) von TPs benachbarter Ziffern.
3. Jedes $\pi \in S_n$ ist ein Produkt von TPs benachbarter Ziffern.

Beweis:

1. Induktion über k. $\quad k = 2. \quad \surd$
   Sei $k > 2. \Rightarrow (i_1 \ \ i_2 \ \ \dots \ \ i_k) = (i_2 \ \ i_3 \ \ \dots \ \ i_k) \circ (i_1 \ \ i_k)$.
   Fertig mit Induktion.
2. Sei $\tau = (i \ \ j)$ mit $j > i$ Induktion über $j - i$. $\quad j - i = \underline{1}. \surd$
   Sei $j - i > \underline{1}. \Rightarrow (i \ \ j) = (j-1 \ \ j) \circ (i \ \ j-1) \circ (j-1 \ \ j)$.
   Fertig mit Induktion.
3. Folgt aus (2.23)(3), sowie den Teilen (1) und (2).

□

(2.26) Definition (Fehlstandspaar/Signum)

Sei $\pi \in S_n$.

(1) Ein Paar (i, j) mit $1 \leq i < j \leq n$ heißt *Fehlstandspaar von* π (FSP), wenn gilt: $\pi(i) > \pi(j)$.

(2) $sgn(\pi) := (-1)^{|\text{FSB von } \pi|}$ heißt das *Signum von* π ($sgn(\pi) \in \{1, -1\} \subseteq \mathbb{Z}$).

□

(2.27) Beispiele

(1) $\pi = id$ hat kein FSP $\Rightarrow sgn(id) = 1$.

(2) $\tau = (i \ \ i+1)$ hat genau **ein** FSP nämlich $(i, i+1) \Rightarrow sgn(\tau) = -1$.

□

(2.28) Satz (Produktsatz)

Seien $\sigma, \pi \in S_n$. Dann gilt: $sgn(\pi \circ \sigma) = sgn(\pi) \cdot sgn(\sigma)$.

Beweis:

Klar für $n = 1$. Sei also $n \geq 2$.

1. Fall: $\sigma = (i \;\; i+1)$. $\quad (1 \leq i < n)$

   $\overset{(2.27)(2)}{\Rightarrow} sgn(\sigma) = -1$.

   $$\pi \circ \sigma = \pi \circ (i \;\; i+1) = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & i+2 & \dots & n \\ \pi(1) & \dots & \pi(i-1) & \pi(i+1) & \pi(i) & \pi(i+2) & \dots & \pi(n) \end{pmatrix}$$

   Es gilt:

   (a) (k,i), $k < i$ FSP von $\pi \Leftrightarrow (k, i+1)$ FSP von $\pi \circ \sigma$

   (b) (i,k), $k > i+1$ FSP von $\pi \Leftrightarrow (i+1,k)$ FSP von $\pi \circ \sigma$

   (c),(d) analog für $i+1$ statt i.

   (e) $(i, i+1)$ FSP von $\pi \Leftrightarrow (i, i+1)$ kein FSP von $\pi \circ \sigma$.

   Aus (a)-(e) folgt: $|\{\text{FSP von } \pi\}| = |\{\text{FSP von } \pi \circ \sigma\}| \pm 1$

   $\Rightarrow sgn(\pi \circ \sigma) = -sgn(\pi) = sgn(\pi) \cdot sgn(\sigma)$.

2. Fall: $\sigma = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_l$, $l \geq 1$, wobei $\tau_j, 1 \leq j \leq l$ eine TP benachbarter Ziffern ist.

   Induktion über l:

   $l = 1$: 1. Fall

   $l > 1$: Setze $\sigma' = \tau_1 \circ \ldots \circ \tau_{l-1}$

   Dann ist $\sigma = \sigma' \circ \tau_l$.

Es gilt:

$$\begin{aligned} sgn(\pi \circ \sigma) &= sgn((\pi \circ \sigma') \circ \tau_l) \\ &= sgn(\pi \circ \sigma') \cdot sgn(\tau_l) && \text{(1. Fall)} \\ &= sgn(\pi) \cdot sgn(\sigma') \cdot sgn(\tau_l) && \text{(Induktion)} \\ &= sgn(\pi) \cdot sgn(\sigma' \circ \tau_l) && \text{(1. Fall)} \\ &= sgn(\pi) \cdot sgn(\sigma). \end{aligned}$$

(2.29) Beispiel

Sei $\pi \in S_n$ ein k-Zykel.

Dann gilt: $sgn(\pi) = \begin{cases} 1, & k \text{ ungerade } (k \geq 2) \\ -1, & k \text{ gerade} \end{cases}$

Beweis:

Sei $\pi = (i_1 \ \ldots \ i_k)$. Nach (2.25)(3) ist $\sigma = (i_{k-1} \ i_k) \circ (i_{k-2} \ i_k) \circ \ldots \circ (i_1 \ i_k)$.

Die Behauptung folgt aus (2.28) und (2.27)(2) □

Signum $\rightsquigarrow$ Determinante

§ 5 Stirling Zahlen

(2.30) Definition (Stirling-Zahlen erster Art (s))

Seien $k \in \mathbb{N}_0$.

Wir setzen $s_{0,0} := 1$, $s_{0.k} := 0$ für $k > 0$, und

$$s_{n,k} := |\{\pi \in S_n | \ \pi \text{ ist ein Produkt von genau k disjunkten Zykeln wie in (2.23)(3)}\}|$$

für $n > 0$. 1-Zykeln werden dabei mitgezählt. Die Zahlen $s_{n,k}$ heißen *Stirling-Zahlen erster Art*.

(2.31) Satz (Rekursive Berechnung)

Seien $n, k \in \mathbb{N}_0$.

(1) $s_{n,k} = 0$ für $k > n$; $\sum_{k=1}^{n} s_{n,k} = n!$

(2) (*Stirling-Dreieck* erster Art): Für $k \leq n$ gilt: $s_{n,k} = s_{n-1,k-1} + (n-1) \cdot s_{n-1,k}$

Beweis:

(1) Klar.

(2) Sei $\pi \in S_n$ ein Produkt von genau k Zykeln. π entsteht aus $\sigma \in s_{n-1}$ auf eine von 2 Arten:

1. $\pi = \sigma \circ (n)$, σ ist Produkt von genau $k-1$ Zykeln
   Anzahl: $S_{n-1,k-1}$
2. σ ist Produkt von genau k Zykeln, π entsteht aus σ durch Einfügen von n in einen dieser Zykel:
   $$(i_1 \ i_2 \ \ldots \ i_l) \qquad l \text{ Möglichkeiten}$$
   Anzahl: $(n-1) \cdot s_{n-1,k}$

□

$n=4$	$k=3$ (1)(2)(3)
(1)(2 3)(4)	(1 4)(2)(3)
(1 2)(3)(4)	(1)(2 4)(3)
(1 3)(2)(4)	(1)(2)(3 4)

n						
0				1		
1			0		1	
2		0		1		1
3	0		2		3		1

Erinnerung (1.25) und Ergänzung:

Sei A Menge: $A_1, \ldots, A_k \subseteq A$. $\{A_1, ...A_k\}$ heißt *k-Partition* von A, falls gilt:

(1) $\bigcup_{i=1}^{k} A_i = A$

(2) $A_i \neq \emptyset$, $1 \leq i \leq k$, und $A_i \cap A_j = \emptyset$ für $i \neq j$.

(2.32) Definition (Stirling-Zahlen zweiter Art (S))

Seien $n,k \in \mathbb{N}_0$: Wir setzen $S_{0,0} := 1$ und für $(n,k) \neq (0,0)$ sei $S_{n,k}$ = Anzahl der k-Partitionen von $\underline{n}$.

Die Zahlen $S_{n,k}$ heißen *Stirling-Zahlen zweiter Art (S)*.

(2.33) Satz

Seien $n,k \in \mathbb{N}_0$.

(1) $S_{n,0} = 0$ für $n > 0$ und $S_{n,k} = 0$ für $k > 0$.

(2) Für $k \leq n$ gilt: $S_{n,k} = S_{n-1,k-1} + k \cdot S_{n-1,k}$

Beweis:

Selbst.

3 Graphentheorie

§ 1 Grundbegriffe

(3.1) Definition (Graph, Knoten, Kante)

Ein (*ungerichteter*) $G = G(V,E)$ besteht aus einer endlichen Menge V von *Knoten* (engl.: vertex) und einer Menge E von *Kanten* (engl.: edge) $\{u,v\}$ mit $u \neq v \in V$.

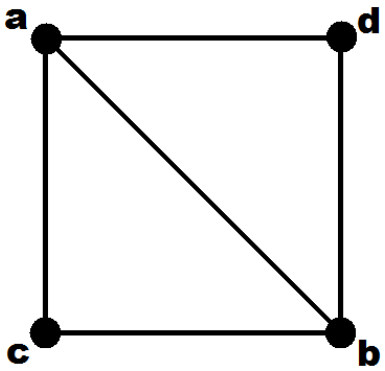
Mathematisches Modell für eine Kante zwischen den Knoten u,v:
Die zweielementige Teilmenge $\{u,v\} = \{v,u\} \subseteq V$.

Schreibweise für Kanten: $uv = vu$. u,v heißen die *Endknoten* der Kante uv.

Bildliche Darstellung $(\dagger)$:

$V = \{a,b,c,d\}$

$E = \{\{a,d\},\{a,c\},\{a,b\},\{c,b\},\{b,d\}\}$



(3.2) Definition (Teilgraph)

Sei $G = G(V,E)$ ein Graph. Der Graph $G' = G(V',E')$ heißt *Teilgraph* von G, wenn gilt: $V' \subseteq V, E' \subseteq E$.

Gilt $E' = E \cap \{\{u,v\} | u \neq v \in V'\}$, dann heißt G' ein *induzierter Teilgraph* von G und wird mit $G[V']$ bezeichnet.

□

Photo 2 Teilgraph von $(\dagger)$

Induzierter Teilgraph von $(\dagger)$

(3.3) Bemerkung (Graphvariationen)

Gelegentlich ist der Begriff "Graph" etwas allgemeiner gefasst und lässt z.B. zu:

1. *Schlingen*: Kanten, die einen Knoten mit sich selbst verbinden
   $\{v,v\} = \{v\}$ E enthält auch einelementige Mengen.
2. *Mehrfachkanten*: Mehr als eine Kante zwischen zwei Knoten.
   $\{u,v\}$ kommt mehrfach in E vor: E ist Multimenge.
3. *Gerichtete Kanten*: Kanten, die in eine Richtung zeigen.
   $(u,v) \in V \times V$ liegt in E □

Im Folgenden sei $G = G(V,E)$ wie in Definition (3.1) (ohne Schlingen, ohne Mehrfachkanten, ohne gerichtete Kanten).

(3.4) Definition (adjazent, inzident, Grad)

1. $u,v \in V$ heißen *adjazent* oder *benachbart* wenn $uv \in E$.
   $\Gamma(v) := \{u \in V | u \neq v, u,v \text{ adjazent}\}$
   Menge der Nachbarn von v.
2. Zwei Kanten mit einem gemeinsamen Endknoten heißen *inzident*.
   $v \in V$ und $e \in E$ heißen inzident, wenn v ein Endknoten von e ist.
3. Sei $v \in V$. Der *Grad von v*, geschrieben $deg(v)$, ist die Anzahl der mit v inzidenten Kanten.

□

(3.5) Bemerkung

$$\sum_{v \in V} deg(v) = 2|E| \, .$$

Beweis:

Sei $e = uv \in E, u \neq v$.

e trägt den Wert 1 zu $deg(v)$ und den Wert 1 zu $deg(u)$, also insgesamt den Wert 2 zu $\sum_{v \in V} deg(v)$.

□

(3.6) Korollar

Sei $V_u := \{v \in V | deg(v) \text{ ungerade}\}$. Dann ist $|V_u|$ gerade.

Beweis:

Sei $V_g := V \backslash V_u$

$\Rightarrow \sum_{v \in V_g} deg(v)$ gerade

$\Rightarrow \sum_{v \in V_u} deg(v) = 2|E| - \sum_{v \in V_g} deg(v)$ gerade

$\Rightarrow |V_u|$ gerade, da die Summe einer ungeraden Anzahl ungerader Zahlen ungerade ist. □

(3.7) Definition (Kantenzug, Pfad)

1. Ein *Weg w* (oder *Kantenzug*) *der Länge l in G* ist eine Folge $w = (v_0, v_1, \ldots, v_l)$ von Knoten mit $v_i v_{i+1} \in E \; \forall \; 0 \leq i < l$.

   v_0, v_l heißen die *Anfangs-* bzw. *Endknoten* von w und w heißt und ein v_0 - v_l - Weg.
2. Ein Weg $(v_0, v_1, \ldots, v_l)$ heißt *Pfad der Länge l in G*, falls alle $v_i, 0 \leq i \leq l$ paarweise verschieden sind. [v_0 - v_l - Pfad]
3. Sei $l \geq 3$. Ein *Kreis der Länge l in G* ist ein Weg $(v_0, v_1, \ldots, v_l)$ mit $v_l = v_0$, sodass $(v_1, \ldots, v_l)$ ein Pfad ist. [v_0-Kreis].

□

(a,d,b,a,c) ist ein Weg der Länge 4 aber **kein** Pfad.

(a,d,b,c) ist ein a-c-Pfad.

(a,d,b,c,a) ist ein a-Kreis der Länge 4.

(3.8) Definition und Bemerkung (Zusammenhangskomponente)

1. G heißt *zusammenhängend*, wenn für alle $u \neq v \in V$ ein u-v-Pfad existiert.

   Sonst heißt G *unzusammenhängend*.
2. Wir definieren die Relation $\sim$ auf V wie folgt:

   $u \sim v :\Leftrightarrow u = v$ oder $u \neq v$ und es existiert ein u-v-Pfad. Dann ist $\sim$ eine Äquivalenzrelation auf V.

   Seien $V_1, \ldots, V_k$ die Äquivalenzklassen von V. Dann heißen die induzierten Teilgraphen $G[V_i], 1 \leq i \leq k$, die *Zusammenhangskomponenten von G*.

Beweis:

$\sim$ ist Äquivalenzrelation:

(R): $\surd$

(S): Sei $u \sim v, u \neq v$, und sei $(u = u_0, u_1, \ldots, u_l = v)$ ein u-v-Pfad. Dann ist $(u_l, u_{l-1}, \ldots, u_1, u_0)$ ein v-u-Pfad.

(T): Sei $u \sim v, v \sim x, u \neq v \neq x \neq u$ (sonst trivial)

$\Rightarrow$ Es existiert ein u-x-Weg

$\Rightarrow$ Es existiert ein u-x-Pfad

(Ein Kreis in einem u-x-Weg kann weggelassen werden.)

Test auf Zusammenhang:

Breadth-First-Algorithmus. (Breitensuche)

Datenstrukturen für Graphen?

Zunächst: Nummeriere die Knoten, $V = \{v_1, ..., v_n\}$.

Im nächsten Schritt: Nehme $V = \underline{n} = \{1, ..., n\}$ an (identifiziere einen Knoten mit seiner Nummer).

(3.9) Definition (Datenstrukturen für Graphen)

Sei $V = \{1, \ldots, n\}$.

1. Die *Adjazenzmatrix von G* ist die 0-1-Matrix
   $A = (a_{ij})_{1 \leq i,j \leq n}$ mit $a_{ij} = \begin{cases} 1, & ij \in E, \\ 0, & \text{sonst.} \end{cases}$
2. Die *Adjazenzliste* speichert zu jedem Knoten die Liste seiner Nachbarn:
   $[[1, \Gamma(1)], [2, \Gamma(2), \ldots, [n, \Gamma(n)]]$

□

Photo

Matrix:
$$\begin{matrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{matrix}$$

Liste: $[[1, [2, 4]], [2, [1, 3, 4]], [3, [2]], [4, [1, 2]]$

(3.10) Algorithmus (Breadth-First-Search (BFS), Breitensuche)

Eingabe: Graph $G = G(V,E)$, $s \in V$.

Ausgabe: Listen $d[v]$, $pred[v]$, $v \in V$.

```
for all v ∈ V do begin
   if v = s then d[v] ← v else d[v] ← ∞;
   pred[v] ← nil;
end
Q ← [ ];  // leere Liste
Insert(Q,s);  // hängt s an das Ende von Q

while not IsEmpty(Q) do begin
  v ← Dequeue(Q);  // vorderstes Element von Q entfernen
  for all u ∈ Γ(v) do
       if d[u] = ∞ then begin
          d[u] ← d[v] + 1;
          pred[u] ← v;
          Insert(Q,u);
       end
end
```

□

(3.11) Bemerkung

Notation wie im Algorithmus (3.10).

1. d[v] ist die Länge eines kürzesten s-v-Pfades.

   Falls kein s-v-Pfad in G existiert, ist $d[v] = \infty$.
2. G ist genau dann zusammenhängend, wenn $d[v] \neq \infty \; \forall \; v \in V$.

Beweis:

1. (a) Für $v \in V \setminus \{s\}$ mit $d[v] \neq \infty$ gilt: $d[v] = d[pred[v]] + 1 \geq 1$.
   $\Rightarrow (s, \ldots, pred[pred[v]], pred[v], v)$ ist ein s-v-Pfad der Länge $d[v]$.
   (b) Zu jedem Zeitpunkt gilt für die Einträge $u_1, \ldots, u_l$ von Q in Alg, (3.10):
   $d[u_1] \leq d[u_2] \leq \ldots \leq d[u_l] \leq d[u_1] + 1$
   (c) Für $u, v \in V$ mit $d[u] \neq \infty \neq d[v]$ und $uv \in E$ gilt: $d[v] \leq d[u] + 1$.
   (Wurde $d[v]$ beim Durchlaufen von $\Gamma(u)$ gesetzt, dann ist $d[v] = d[u] + 1$. Andernfalls war $d[v]$ hier schon gesetzt, also beim Durchlaufen von $\Gamma(x)$ mit $d[x] \leq d[u]$; damit $d[x] = d[x] + 1 \leq d[u] + 1$.)

(d) Sei $(u_0, u_1, \ldots, u_k)$ mit $u_0 = s$, $u_k = v$ ein s-v-Pfad.
$\Rightarrow d[v] = d[u_k] \leq d[u_{k-1}] + 1 \leq \ldots \leq d[u_0] + k = k$.

2. G zusammenhängend $\Leftrightarrow$ Die Äquivalenzklasse von s bzgl. v aus (3.8) ist V. Die Behauptung folgt aus (1).

□

§ 2 Hamiltonkreise und Eulertouren

G = G(V,E) sei ein Graph.

(3.12) Definition (Hamiltonkreis)

Ein Kreis $(v_0, v_1, \ldots, v_n)$ in G heißt *Hamiltonkreis*, falls $V = \{v_1, \ldots, v_n\}$ und $|V| = n$.

(3.13) Beispiel (Traveling Salesman Problem (TSP))

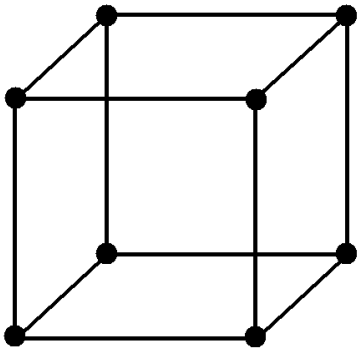
Ein Vertreter (Handlungsreisender) will n Städte besuchen und seine Rundreise möglichst effizient organisieren.

Modell: Graph $G = G(V,E)$

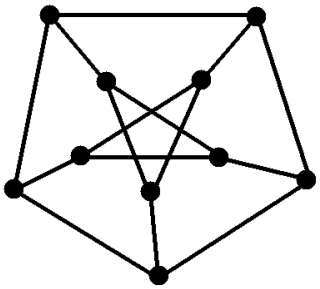
Knoten: $V = \{s_1, \ldots, s_n\}$ Städte

Kanten: $s_i s_j \in E :\Leftrightarrow$ Es ex. eine direkte Flugverbindung zwischen s_i und s_j. Es ex. genau dann eine *Rundreise* durch alle Städte, in der jede Stadt genau einmal besucht wird, wenn ein Hamiltonkreis in $G(V,E)$ ex. □

(3.14) Beispiel



Hamiltonkreis



kein Hamiltonkreis

(3.15) Satz

Gilt in G die Bedingung

$$(*) \qquad deg(u) + deg(v) \geq |V| \forall u \neq v \text{ in } V \text{ mit } uv \notin E,$$

dann ex. in G ein Hamiltonkreis.

Beweis:

Durch Widerspruch.

Angenommen, es ex. $G = G(V,E)$, der (*) erfüllt, aber keinen Hamiltonkreis enthält. Unter allen solchen mit festem $|V|$ wähle einen, mit $|E|$ maximal.

Seien $x \neq y \in V$ mit $xy \notin E$ (somit ex. Hamiltonkreis)

Sei $G' = G(V, E \cup \{xy\})$ $\overset{|E| \text{ max.}}{\Rightarrow}$ G' hat Hamiltonkreis, der "durch xy geht".

Sei $w = (y, v_1, \ldots, v_n)$ dieser Hamiltonkreis mit $x = v_1$ und $y = v_n$.

Setze:

$S := \{v_i | 1 \leq i \leq n, xv_{i+1} \in E\}$

$T := \{v_i | 1 \leq i \leq n, yv_{i+1} \in E\}$

$\Rightarrow v_n \in S \cup T$, d.h. $|S \cup T| < n$.

$|S| = deg(x), |T| = deg(y)$, d.h. $|S| + |T| \geq n$ wegen (*) $\Rightarrow S \cap T \neq \emptyset$

Sei $v_i \in S \cap T$ $\Rightarrow (v_1, v_2, \ldots, v_i, v_n, v_{n-1}, \ldots, v_{i+1}, v_1)$ ist Hamiltonkreis in G. $\lightning$ □

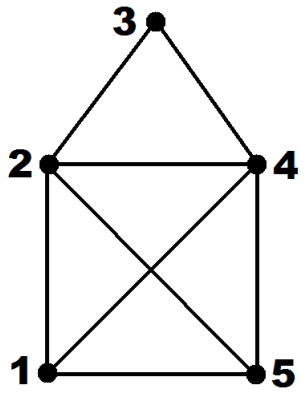
(3.16) Definition (Eulerweg/-tour)

Ein *Eulerweg* in G ist ein Weg $w = (v_0, v_1, \ldots, v_m)$ mit $E = \{v_i v_i + 1 \,|\, 0 \leq i \leq m\}$ und $|E| = m$.

Ist w ein Eulerweg mit $v_0 = v_m$, dann heißt w *Eulertour*.

□

(3.17) Beispiel (Das Haus vom Nikolaus)



$(1,2,4,1,5,4,3,2,5)$ ist ein Eulerweg, **keine** Eulertour. □

(3.18) Bemerkung

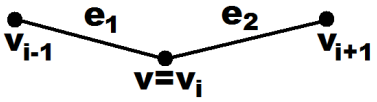
Sei $w = (v_0, v_1, \ldots, v_m)$ ein Eulerweg in G. Dann ist $deg(v)$ gerade $\forall v \in V \backslash \{v_0, v_m\}$.

1. Ist $v_0 = v_m$, d.h. w ist eine Eulertour, dann ist $deg(v_0)$ gerade.
2. Ist $v_0 \neq v_m$, dann sind $deg(v_0)$ und $deg(v_m)$ ungerade.

Beweis:

Jedes v_i kommt in w i.A. mehrfach vor, aber $V = \{v_0, v_1, \ldots, v_m\}$. Sei $v \in V \backslash \{v_0, v_m\}$.

Dann ist $v = v_i$ für ein $1 \leq i \leq m-1$.



e_1, e_2 sind zwei verschiedene Kanten an v_i

Ist $v = v_j$ für ein $1 \leq j \leq m-1$ mit $i \neq j$, dann sind $v_j - 1v, vv_{j+1}, v_{i-1}v, vv_{i+1}$ vier verschiedene Kanten, die mit v inzident sind, etc.

Beweis für $v = v_0 = v_m$ und $v = v_0 \neq v_m$ analog. □

(3.19) Bemerkung

Sei G zusammenhängend und $k = (v_0, v_1, \ldots, v_{m-1}, v_m)$ ein Kreis in $G(v_m = v_0)$.

Dann ist auch $G(V, E \backslash \{v_i v_{i+1}\}) \forall 0 \leq i < m$ zusammenhängend.

Beweis:

Sei $v \in V$.

Ist w ein v_i-v-Pfad in G, der über die Kante v_iv_{i+1} läuft, kann der Teilweg v_iv_{i+1} durch $(v_i, v_{i-1}, \ldots, v_0, v_{m-1}, \ldots, v_{i+1})$ ersetzt werden. □

(3.20) Bemerkung

Sei G zusammenhängend.

1. Sei $deg(v)$ gerade $\forall v \in V$. Dann besitzt G eine Eulertour.
2. Seien $x \neq y \in V$ mit $deg(x)$, $deg(y)$ ungerade und $deg(v)$ gerade $\forall\, v \in V \backslash \{x,y\}$. Dann besitzt G einen Eulerweg von x nach y.

Beweis:

1. Sei $w = (v_0, v_1, \ldots, v_k)$ ein Weg maximaler Länge in G, der keine Kante mehrfach enthält.

   $\Rightarrow$ Alle mit v_k inzidenten Kanten liegen auf w.

   $\Rightarrow v_0 = v_k$, $deg(v_k)$ gerade

   Angenommen, w ist keine Eulertour.

   G zusammenhängend $\overset{\Rightarrow}{}$ Es ex. $e \in E \backslash \{v_iv_{i+1} |\ 0 \leq i < k\}$ mit e inzident zu einem $v_i, 0 \leq i < k$

   Sei $e = uv_i$

   Dann ist $uv_i\, v_{i+1} \ldots v_k\, v_1 \ldots v_i$ länger als w und enthält keine Kante mehrfach. $\lightning$
2. **1. Fall:** $xy \notin E$

   Betrachte $G' = G(V, E \cup \{xy\})$. G' erfüllt die Vorraussetzung von (1) $\Rightarrow$ G' besitzt Eulertour.

   Lässt man darin die Kante xy weg, erhält man einen Eulerweg von x nach y.

   2. Fall: $xy \in E$

   Ist $deg(x) = deg(y) = 1$, dann G = o—o $\surd$

   Sei o.B.d.A $deg(y) > 1$. Betrachte $G' := G(V, E \backslash \{xy\})$

   Ist G' zusammenhängend, verwende (1).

Sei G' nicht zusammenhängend, und sei H die Zusammenhangskomponente von G', die y enthält. H erfüllt (1), und enthält damit eine Eulertour.

x ist kein Knoten von H, sonst wäre G' zusammenhängend.

Sei $e = yz$ in dieser Eulertour. $\Rightarrow z \neq x$.

Setze $G'' := G(V, E \backslash \{e\})$

Nach (3.19) ist G'' zusammenhängend, d.h. G'' erfüllt (2)

$\overset{\text{Induktion}}{\Rightarrow}$ G'' besitzt Eulerweg von x nach z

$\Rightarrow$ G besitzt Eulerweg von x nach y. □

(3.21) Algorithmus (Fleury)

Eingabe: Zusammenhängender Graph $G = G(V,E)$ mit $deg(v)$ gerade $\forall\, v \in V$.

Ausgabe: Liste $W = [v_0, v_1, \ldots, v_m]$, so dass $(v_0, \ldots, v_m)$ eine Eulertour in G ist.

Wähle $v_0 \in V_i$

```
w ← [v_0];
v ← v_0;
while not IsEmpty(E) do begin
  if Γ(v) = {v'}
  then v ← v \ {v}
  else wähle v' ∈ Γ(v), so dass G(V,E \ {v v'}) zusammenhängend ist;
  Insert(W,v');
  E ← E \ {v v'};
  v ← v';
end.
```

□

(3.22) Bemerkung

Der Algorithmus (3.21) terminiert mit einer Eulertour von G.

Beweis:

Folgt aus (3.20) bzw. dem Beweis von (3.20) (2). □

(3.23) Beispiel

w

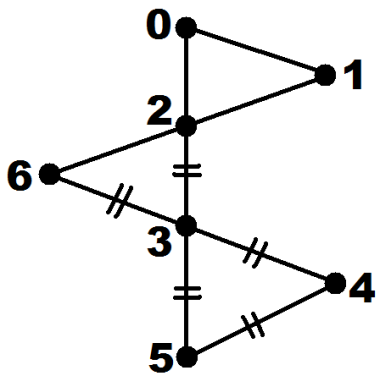
[2]

[2,3] 6 ist jetzt verboten! [2,3,5]

[2,3,5,4]

[2,3,5,4,3]

[2,3,5,4,3,6]



□

§ 3 Bäume

$G = G(V,E)$ sei ein Graph, $v \neq \emptyset$.

(3.23) Definition (Wald/Blatt)

G heißt *Wald*, falls G keine Kreise enthält. Ein zusammenhängender Wald heißt *Baum*.

Ist G ein Baum und $v \in V$ mit $deg(v) = 1$, dann heißt v *Blatt*.

(3.24) Bemerkung

Sei G ein Baum mit $|V| > 1$ und sei $w = (v_0, v_1, \ldots, v_m)$ ein Pfad maximaler Länge. Dann sind v_0, v_m Blätter und $v_0 \neq v_m$.

Beweis:

Ist v_0 kein Blatt, dann existiert $v \in \Gamma(v_0)$ mit $v \neq v_1$. Wäre $v = v_i$ für ein $2 \leq i \leq m$, dann gäbe es einen Kreis in G. Damit wäre $(v, v_0, v_1, \ldots, v_m)$ ein längerer Pfad als w ↯

Analog: v_m ist Blatt.

Ist $v_0 = v_m$, dann ist $m = 0$ und $V = \{v_0\}$. □

(3.25) Satz

Sei G zusammenhängend. Dann gilt: G ist Baum $\Leftrightarrow |E| = |V| - 1$.

Beweis:

"⇒" Induktion über $|V|$.

$|v| = 1$. Sei $|V| > 1$ und $v \in V$ ein Blatt von G.

Sei $\Gamma(v) = \{v'\}$.

$\Rightarrow G(V\backslash\{v\}, E\backslash\{vv'\})$ ist Baum (zusammenhängend und kreisfrei)

$\overset{\text{Induktion}}{\Rightarrow} |E| - 1 = (|V| - 1) - 1$, d.h. $|E| = |V| - 1$. // <– bitte überprüfen

"⇐" Induktion über $|V|$. $|V| = \surd$

Sei $|V| > 1$.

Angenommen, $deg(v) > 1 \forall v \in V$.

$\overset{(3.5)}{\Rightarrow} \sum_{v\in V} deg(v) = 2|E| = 2|V| - 2 < 2|V| = \sum_{v\in V} 2 \leq \sum_{v\in V} deg(v)$ ↯

Also existiert in G ein $v \in V$ mit $deg(v) = 1$. Sei $\Gamma(v) = \{v'\}$ und $G' = G(V\backslash\{v\}, E\backslash\{v\,v'\})$

$\Rightarrow G'$ ist zshgd. und $|E| - 1 = (|V| - 1) - 1$

$\overset{\text{Induktion}}{\Rightarrow} G'$ ist Baum

$\Rightarrow G$ ist Baum.

□

(3.26) Definition (Spannbaum)

Ein Teilgraph $G' = G(V', E')$ von G heißt *Spannbaum* (Gerüst, spanning tree) von G, falls G' ein Baum mit $V' = V$ ist.

(3.27) Bemerkung

G besitzt Spannbaum $\Leftrightarrow$ G ist zusammenhängend.

Beweis:

"⇒" Ein Baum ist zusammenhängend.

"⇐" Folgt aus (3.19): Ist $(v_0, v_1, \ldots, v_m)$ ein Kreis in G, dann ist $G(V, E\backslash\{v_0v_1\})$ zusammenhängend.

Durch sukzessives Weglassen von Kanten aus Kreisen erhält man einen Spannbaum. □

Breadth-First-Search-Algorithmus (3.10)

Erinnerung: Algorithmus (3.10) (BFS):

Eingabe: $G = G(V, E)$, $s \in V$

Ausgabe: $d[v], pred[v], v \in V$

```
for all v ∈ V do begin
  if v=s then d[v] <- 0 else d[v] <- ∞;
  pred[v] <- nil;
end
Q <- [];
Insert(Q,s);
while not IsEmpty(Q) do begin
  v <- Dequeue(Q);
  for all u <- Γ(v) do
    if d[u] = ∞ then begin
      d[u] <- d[v]+1;
      pred[u] <- v;
      Insert(Q,u);
    end
end
```

(3.28) Bemerkung

Sei G zusammenhängend.

Nach BFS auf G bilden die Kanten $\{v pred[v] | v \in V \backslash \{s\}\}$ einen Spannbaum T von G, so dass gilt:

Für alle $v \in V \backslash \{s\}$ ist der (eindeutig bestimmte) s-v-Pfad in T ein kürzester s-v-Pfad in G.

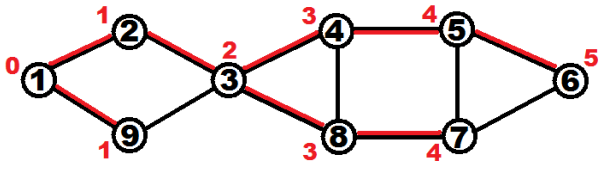
Beweis:

Nach (3.11) ist $d[v] \neq \infty \forall v \in V$ und $d[v]$ ist die Länge eines kürzsten s-v-Pfades in G.

$(s, \ldots, pred[pred[v]], pred[v], v)$ ist ein s-v-Pfad der Länge $d[v]$ in T $\Rightarrow$ T ist zusammenhängend.

Da T nach Definition genau $|V| - 1$ Kanten hat, ist T ein Baum. □

(3.29) Beispiel (Graph mit Breitdurchlauf)



rot: d[v], schwarz: v pred[v]

§ 4 Gewichtete Graphen

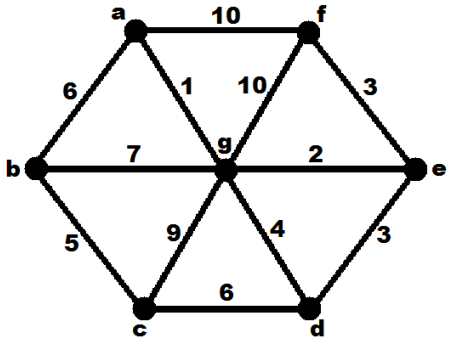
$G = G(V,E)$ Graph.

(3.30) Definition (gewichteter Graph/Gewicht)

G heißt *gewichteter Graph*, falls eine Abbildung $w : E \to \mathbb{R}_{\geq 0}$ definiert ist. ($\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} | x \geq 0\}$.)

In diesem Fall heißt $\sum_{e \in E} w(e)$ das *Gewicht* von G. □

(3.31) Beispiel



(3.32) Definition

Sei: G zusammenhängender gewichteter Graph. Ein *minimaler Spannbaum* von G ist ein Spannbaum von minimalen Gewicht (unter allen Spannbäumen). □

(3.33) Lemma

Ist $|V| > |E| + 1$, dann ist G nicht zusammenhängend.

Beweis:

Wäre G zusammenhängend, dann hätte G einen Spannbaum $T = G(V,E') \Rightarrow |E| \geq |E'| = |V| - 1 > |E|$↯ □

(3.34) Algorithmus (Kruskal)

Eingabe: $G = G(V,E), w : E \to \mathbb{R}_{\geq 0}$, G zusammenhängend.

Ausgabe: $F \subseteq E$ mit $G(V,F)$ ist minimaler Spannbaum von G.

Q $\leftarrow Sort(E,w)$; [sortiere Kanten nach aufst. Gewichten]

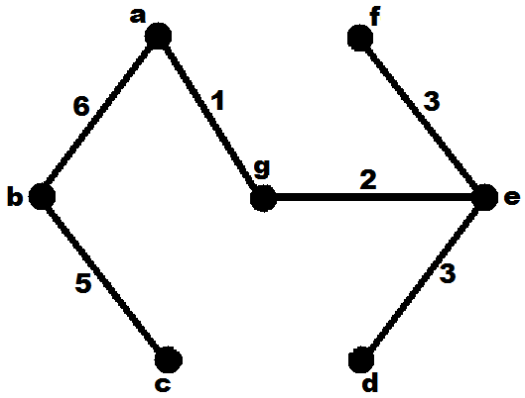
```
F ← [];
while |F| < |V|-1 do
  uv ← Dequeue(Q); //jeweils leichteste Kante
  if u, v in verschiedenen Zusammenhangs-Komponenten von G(V,F)
  then Insert(F,uv);
```

□

(3.35) Beispiel

G Graph aus (3.31):

Q	w	
ag	1	x
eg	2	x
ed	3	x
ef	3	x
dg	4	
bc	5	x
ab	6	x
cd	6	
bg	7	
cg	9	
af	10	
ag	10	



(3.36) Satz

Kruskals Algorithmus terminiert mit einem minimalen Spannbaum von G.

Beweis:

$|F| < |V| - 1 \overset{(3.33)}{\Rightarrow} G(V,F)$ nicht zusammenhängend.

In jedem Schritt ist $G(V,F)$ ein Wald, denn beim Hinzufügen von uv zu F werden zwei Bäume zu einem Baum vereinigt.

Da G zusammenhängend, existiert $uv \in E$, so dass u, v in verschiedenen Komponenten von $G(V,F)$ liegen.

Damit: Algorithmus (3.34) terminiert mit $|F| = |V| - 1$.

Danach: $G(V,F)$ ist Wald und $|F| = |V| - 1 \overset{(3.25)}{\Rightarrow} G(V,F)$ ist Baum, also Spannbaum.

Angenommen: $G(V,F)$ ist nicht minimal.

Sei $G(V,F')$ Spannbaum von minimalen Gewicht und unter allen solchen einer mit $|F \cap F'|$ maximal.

F ist nach Gewicht sortiert (nach Konstr.).

Sei $e \in F$ die erste Kante mit $e \notin F'$, $e = uv$. Sei F_0 die Menge der Kanten vor der Aufnahme von e.

$G(V, F' \cup \{e\})$ enthält einen Kreis k, $k = (u = u_1, u_2, \ldots, u_{m-1} = v, u_m = u)$

Sei $f = u_i\, u_{i+1}$ die letzte Kante aus F, die auf k liegt und sei F_1 die Menge der Kanten vor der Aufnahme von f.

u_i, u_{i+1} liegen in verschiedenen Komponenten der $G(V,F_1)$, bei allen anderen Kanten auf k, die in F liegen sind die Endknoten in der gleichen Komponente von $G(V,F_1)$

$\Rightarrow$ es existiert $e' = u_j u_{j+1}$ in k mit $e' \notin F$ und u_j, u_{j+1} in verschiedenen Komponenten

$\Rightarrow u_j, u_{j+1}$ in verschiedenen Komponenten von $G(V,F_1)$
$F_0 \subseteq F_1$ in verschiedenen Komponenten von $G(V,F_0)$

$\Rightarrow w(e) \leq w(e')$ (sonst hätte der Algorithmus e' genommen)

Sei $F'' := (F' \cup \{e\}) \backslash \{e'\}$

$\overset{w(e) \leq w(e')}{\Rightarrow} F''$ ist zusammenhängend (3.19), also Baum (3.25)

$\Rightarrow F''$ ist minimaler Spannbaum von G und $|F \cap F''| > |F \cap F'|$ $\quad \lightning$. $\square$

4 Modulare Arithmetik

§ 1 Gruppen, Ringe und Körper

(4.1) Definition (Verknüpfung, algebraische Struktur)

Eine *Verknüpfung* auf einer Menge M ist eine Abbildung $M \times M \to M$.

Eine *algebraische Struktur* ist eine Menge auf der eine oder mehrere Verknüpfungen definiert sind. □

$$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}\,(a,b) \mapsto a+b \text{ ist Verknüpfung.}$$

Das Abbildungssysmbol ist das $+$-Zeichen, das zwischen die Argumente gestellt wird.

Polnische Notation: $+a,b$

(4.2) Definition (Gruppe, abelsch, kommutativ)

Eine Menge G heißt *Gruppe*, wenn eine Verknüpfung $\star : G \times G \to G$, $(x,y) \mapsto x \star y$ definiert ist, so dass gilt:

(1) $(x \star y) \star z = x \star (y \star z) \;\; \forall\, x,y,z \in G$ (AG)

(2) Es ex. $e \in G$ mit $e \star x = x = x \star e \;\; \forall\, x \in G$

(3) Für alle $x \in G$ ex. $x' \in G$ mit $x \star x' = e = x' \star x$.

Gilt zusätzlich:

(4) $x \star y = y \star x \;\; \forall\, x \in G$, dann heißt G *abelsch* oder *kommutativ*.

(4.3) Bemerkung

Sei $(G, \star)$ eine Gruppe.

(a) Das Element e aus (4.2)(2) heißt *das neutrale Element von G* (es ist eindeutig bestimmt)

(b) Sei $x \in G$. Das Element x' aus (4.2)(3) ist durch x eindeutig bestimmt. Es heißt das zu x inverse Element.

(c) Ist G *abelsch*, dann schreiben wir oft $+$ für $\star, 0$ für $e, -x$ für x'.

(d) Oft schreiben wir G "multiplikativ", d.h. $\cdot$ oder kein Zeichen für $\star$, 1 für e und x^{-1} für x'.

(4.4) Beispiele

(1) $(\mathbb{Z},+)$ ist eine abelsche Gruppe.

$(\mathbb{N},+)$ ist keine Gruppe $(0 \notin \mathbb{N})$

$(\mathbb{N}_0,+)$ ist keine Gruppe ((4.2)(3) fehlt)

(2) $\mathbb{R}_{>0},\cdot)$ ist eine Gruppe

$(\mathbb{R}_{\geq 0},\cdot)$ ist keine Gruppe (0 hat kein Inverses)

(3)

$$vgl.(2.19)$$

$S_n = \{\pi : \underline{n} \to \underline{n} \mid \pi \text{ ist bijektiv}\}$ $(\underline{n} = 1,\ldots,n)$ die Menge der Permutationen von $\underline{n}$ ist eine Gruppe bzgl. der Verknüpfung:

$\circ : S_n \times S_n \to S_n, (\pi,\sigma) \mapsto \pi \circ \sigma$

$\circ$: Komposition von Abbildungen

Nach (2.21) ist $\pi \circ \sigma \in S_n$ für $\pi,\sigma \in S_n$

Neutrales Element: $id_{\underline{n}}$

Assoziativgesetz (4.2)(1): Gilt allgemein für Komposition von Abbildung

<– unübersichtliches Diagramm –> $h \circ (g \circ f)(x) = h(g \circ f(x)) = h(g(f(x))$

$(f \circ g) \circ f\ (x) = (h \circ g)(f(x)) = h(g(f(x))$

Inverses Element eines k-Zykels:

$(i\ i_2\ \ldots\ i_k)^{-1} = (i_k\ i_{k-1}\ \ldots\ i_2\ i_1)$

$(1\ 3\ 5\ 2)^{-1} = (2\ 5\ 3\ 1)$

$(1\ 3\ 5\ 2)(2\ 5\ 3\ 1) = (1)(2)(3)(4)(5).$

$|S_n| = n!$

S_n ist nicht abelsch für $n \geq 3$.

In diesem Fall liegen $(1\ 2),(2\ 3)$ in S_3 und $(1\ 2) \circ (2\ 3) = (1\ 2\ 3) \neq (1\ 3\ 2) = (2\ 3) \circ (12)$. $\square$

(4.5) Definition (Untergruppe)

Sei $(G,\star)$ eine Gruppe und $H \subseteq G$. H heißt *Untergruppe* von G, geschrieben $H \leq G$, wenn gilt:

(1) $e \in H$.

(2) Für $x,y \in H$ ist auch $x \star y \in H$. (H ist abgeschlossen bzgl. $\star$)

In diesem Fall ist H mit der Verknüpfung $\star$ selbst eine Gruppe.

[$x \in H, x' \in G$ mit $x \star x' = e \Rightarrow x' \star (x \star x') = x' \star e$?]

(4.6) Beispiele

(1) Sei $G = \mathbb{Z}$ mit $+$:

Für $n \in \mathbb{Z}$ sei $n\mathbb{Z} := \{n\ z | z \in \mathbb{Z}\}$. $n\mathbb{Z} := \{n\ z | z \in \mathbb{Z}\}$ ist n-er-Reihe.

Für $n = 3$:

$3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$ die 3er Reihe.

Dann ist $n\mathbb{Z} \leq \mathbb{Z}$:

(4.5)(1): $e = 0,\ 0 = n \cdot 0 \in n\mathbb{Z}$

(4.5)(2): $nz + ny = n(z+y) \in n\mathbb{Z}$

Später: Alle Untergrupppen von $(\mathbb{Z}, +)$ sind von dieser Form.

(2) $G = S_n$ mit $\circ$:

$H = \{\pi \in S_n | \pi(n) = n\}$. Dann ist $H \leq G$:

(1) e in $id_{\underline{n}}$ lässt n fest $\Rightarrow id_{\underline{n}} \in H$

(2) Seien $\sigma, \pi \in H \Rightarrow$

$\sigma \circ \pi(n) = \sigma(\pi(n)) = \sigma(n) = n \Rightarrow \sigma \circ \pi \in H$ "H ist Stabilisator von n".

(3) $G = R_{\geq 0}$ mit $\cdot$:

$\mathbb{Q}_{>0} \leq G : 1 \in \mathbb{Q}_{>0}, xy \in \mathbb{Q}_{>0}\ \ \forall\, x, y \in \mathbb{Q}_{>0}$

$\{10^z | z \in \mathbb{Z}\} < \mathbb{Q}_{>0}$

$R_{<0}$ keine Untergruppe von $(\mathbb{R}\ \{0\}, \cdot)$.

□

(4.8) Definition (Ring, kommutativ)

Eine Menge R heißt *Ring*, wenn auf R zwei Verknüpfungen $+$: $R \times R \to R$ und $\cdot : R \times R \to R$ definiert sind, so dass gilt:

(1) $(R, +)$ ist abelsche Gruppe

(2) $(x \cdot y) \cdot z = x \cdot (y \cdot z)\ \ \forall\, x, y, z \in R$ (AG)

(3) Es existiert $1 \in R$ mit $1 \cdot x = x = x \cdot 1\ \ \forall\, x \in R$.

(4) $\left.\begin{array}{c} x \cdot (y+z) = x \cdot y + x \cdot z \text{ und} \\ (x+y) \cdot z = x \cdot z + y \cdot z\ \forall\, x, y, z \in R \end{array}\right\}$ ("Distributivgesetz")

Gilt zusätzlich:

(5) $x \cdot y = y \cdot x\ \ \forall\, x, y \in R$, dann heißt R *kommutativ*.

□

(4.9) Beispiel

$(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring

Q Division: $\frac{1}{5} : 2 = \frac{1}{5} \cdot \frac{1}{2}$

$\frac{1}{2} = 2^{-1}$

(4.10) Definition (invertierbar, Einheit)

Sei R ein Ring. $x \in R$ heißt *invertierbar*, oder *Einheit*, wenn ein $x' \in R$ existiert mit $x \cdot x' = 1 = x' \cdot x$.

In diesem Fall ist x' eindeutig durch x bestimmen und wir schreiben x^{-1} für x'.

$R^\star : \{x \in R | x \text{ ist Einheit } \}$. □

(4.11) Beispiel

$\mathbb{Z}^\star = \{1, -1\}$.

(4.12) Bemerkung (Einheitsgruppe)

Sei R Ring. Dann ist $(R^\star, \cdot)$ eine Gruppe; deshalb heißt $R^\star$ auch die *Einheitsgruppe* von R.

Beweis:

Sind $x, y \in R^\star$, dann auch $x \cdot y$: $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot \underbrace{y \cdot y^{-1}}_{1} \cdot x^{-1} = x \cdot x^{-1} = 1$

$\Rightarrow \cdot : R^\star \times R^\star \to R^\star$ ist definiert.

AG: Folgt aus (4.8)(2).

$1 \in R^\star$, das Inverse zu $x \in R^\star$ ist x^{-1}. □

(4.13) Definition (Körper)

Eine Menge K mit zwei Verknüpfungen $+, \cdot$ heißt *Körper* (engl. field), wenn $(K, +, \cdot)$ ein kommutativer Ring ist mit $1 \neq 0$ und es gilt: $K^\star = K \backslash \{0\}$.

(Jedes von 0 verschiedene Element aus K ist eine Einheit.)

(4.14) Beispiele

$(\mathbb{Q},+,\cdot),(\mathbb{R},+,\cdot)$.

Weitere Beispiele später.

§ 2 Restklassenringe

(4.15) Definition (teilt, Vielfaches, Primzahl, zusammengesetzt)

(1) Seien $a,b \in \mathbb{Z}$.

a teilt b, geschrieben $a|b :\Leftrightarrow \exists c \in \mathbb{Z}$ mit $ac = b$.

In diem Fall sagen wir auch: b ist ein *Vielfaches* von a.

(2) Sei $p \in \mathbb{Z}$

p heißt *Primzahl*, falls gilt:

(a) $p \neq 1,-1$

(b) $a|p \Rightarrow a \in \{1,-1,p,-p\}$. $\mathbb{P} := \{p \in \mathbb{N} | p \text{ ist } \textit{Primzahl}\}$ (Menge aller positiven Primzahlen.)

(3) Falls $a \in \mathbb{Z}$, $a \neq 0,1,-1$ keine Primzahl ist, nennen wir a *zusammengesetzt*.

(4.16) Bemerkung

(1) $a|0 \ \forall\, a \in \mathbb{Z}$

$0|a$ nur für $a = 0$.

(2) $a|a$ und $a|-a \ \forall\, a \in \mathbb{Z}$

(3) Seien $a,b,c \in \mathbb{Z}$. Dann gilt:

(a) $a|b \Rightarrow a|-b$ und $-a|b$

(b) $a|b$ und $b|c \Rightarrow a|c$

(c) $a|b$ und $b|a \Rightarrow b = \pm a$

(d) $a|b \Rightarrow a|bc$

(e) $a|b$ und $a|c \Rightarrow a|b+c$

(4) Sei $p \in \mathbb{Z}$. Dann gilt p Primzahl $\Leftrightarrow -p$ Primzahl. (Deshalb Beschränkung auf $\mathbb{P} \subseteq \mathbb{N}$)

Beweis

Aussagen folgen aus Definition der Teilbarkeit und den Axiomen von $\mathbb{Z}$.

Als Beispiel beweise ich (3)(c):

Seien $c,d \in \mathbb{Z}$ mit $ac = b$ und $bd = \pm a$.

$\Rightarrow a = bd = (ac)d = a(cd) \quad \Rightarrow \quad a(1-cd) = 0$

1. Fall $a = 0 \Rightarrow b = ac = 0 = a$

2. Fall $a \neq 0 \Rightarrow 1 = cd = 0$, d.h. $cd = 1$

$\Rightarrow c \in \mathbb{Z}^\star$, d.h. $c = \pm 1$

$\Rightarrow b = ac = \pm a$. □

—-

zu (4.6)(3): $G = S_n$

$H = \{\pi \in G | \pi(n) = n\}$

$\sigma, \pi \in H$

$\pi^{-1} \in H : \pi^{-1}(n) = n$?

$$\pi(n) = n \Rightarrow \underbrace{\pi^{-1}(\pi(n)) = \pi^{-1}(n)}_{\underbrace{\pi^{-1} \circ \pi(n)}_{id_{\underline{n}}}}$$

—-

Schreibweise: $x \in \mathbb{R}$

$\lfloor x \rfloor := max\{z \in \mathbb{Z} | z \leq x\}$ größte ganze Zahl $\leq x$

$\lceil x \rceil := min\{z \in \mathbb{Z} | z \geq x\}$ kleinste ganze Zahl $\geq x$

(4.17) Bemerkung (Division mit Rest in $\mathbb{Z}$)

Seien $a, b \in \mathbb{Z}, b \neq 0$.

Dann existieren eindeutig bestimmte $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$.

Beweis

Existenz:

Setze $q := \begin{cases} \lfloor a/b \rfloor, & \text{falls } b > 0 \\ \lceil a/b \rceil, & \text{falls } b < 0 \end{cases}$

und $r := a - qb. \quad \Rightarrow \quad a = qb + r$ und $0 \leq r < |b|$.

Eindeutigkeit:

Sei $qb + r = a = q'b + r'$

mit $q, q', r, r' \in \mathbb{Z}$ und $0 \leq r, r < |b|$

$\Rightarrow (q - q')b = r - r \quad \xRightarrow{(4.16)(3)} \quad b|r' - r \quad \Rightarrow \quad |b||r' - r$

$\Rightarrow r' - r = 0$, denn $|r' - r| < |b| \quad \Rightarrow \quad q = q'$, denn $b \neq 0$.

(4.18) Definition

(1) Sei $n \in \mathbb{N} (0 \notin \mathbb{N})$.

mod $n : \mathbb{Z} \to \mathbb{N}_0$ ist die Abbildung die definiert ist durch $z \bmod n := r$, falls $z = qn + r$ mit $q, r \in \mathbb{Z}, 0 \leq r < n$.

(2) Definieren Relation auf $\mathbb{Z}$ für jedes $n \in \mathbb{N}_0$ durch:

$x \equiv y (\text{mod } n) :\Leftrightarrow n|x - y$.

(4.19) Beispiel

(1) $n = 7$:

$8 \bmod 7 = 1$

$-8 \bmod 7 = 6$

$21 \bmod 7 = 0$

$-3 \bmod 7 = 4$

(2) $\underline{n=0:}$

$x \equiv y(\text{mod } 0) \Leftrightarrow 0|x-y \Leftrightarrow x=y$

$\underline{n=1:}$

$x \equiv y(\text{mod } 1) \Leftrightarrow 1|x-y$

also: $\forall x,y \in \mathbb{Z} : x \equiv y(\text{mod } 1)$

$\underline{n=7:}$

$8 \equiv 1(\text{mod } 7)$

$-8 \equiv 6(\text{mod } 7)$

$21 \equiv 0(\text{mod } 7)$

$-3 \equiv 4(\text{mod } 7)$

(4.20) Bemerkung (Restklassen mod n)

(1) Für $n \in \mathbb{N}_0$ ist $\equiv \pmod n$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Die Äquivalenzklassen heißen *Restklassen modulo n*.

(2) Sei $n \in \mathbb{N}$. Dann gilt $\forall x,y \in \mathbb{Z}$:

$x \equiv y(\text{mod } n) \Leftrightarrow x \text{ mod } n = y \text{ mod } n$

(3) Sei $n \in \mathbb{N}_0$.

Für $x \in \mathbb{Z}$ sei C_x die Äquivalenzklasse von x bezüglich $\equiv \pmod n$. Dann ist $C_x = x+n\mathbb{Z} := \{x+nz | z \in \mathbb{Z}\} \subseteq \mathbb{Z}$

[z.B. $\underline{n=0:}\ x+0\mathbb{Z} = \{x\}$

$\underline{n=1:}\ x+1\mathbb{Z} = \mathbb{Z}$

$$\underline{n=2:}\ x+2\mathbb{Z} = \begin{cases} 2\mathbb{Z}, & \text{falls } x \text{ gerade} \\ 1+2\mathbb{Z}, & \text{falls } x \text{ unerade} \end{cases}$$

(4) Sei $n \in \mathbb{N}_0, x,x',y,y' \in \mathbb{Z}$ mit $x \equiv x'(\text{mod } n)$ und $y \equiv y'(\text{mod } n)$. Dann gilt:

$(x+y) \equiv (x'+y')(\text{mod } n)$ und $(xy \equiv (x'y')(\text{mod } n)$.

Beweis

(1) Folgt aus (4.16)

(2) "$\Rightarrow$" $n|x-y$

$x = q_1 n + r_1, y = q_2 n + r_2 \Rightarrow x-y = (q_1-q_2)n + (r_1-r_2)$

$\overset{(4.16)(3)(d)}{\Rightarrow}\ n|r_1-r_2 \overset{|r_1-r_2|<n}{\Rightarrow} r_1 = r_2$, d.h. $x \text{ mod } n = y \text{ mod } n$.

"$\Leftarrow$" $x = q_1 n + r,\ y = q_2 n + r$

$\Rightarrow x-y = (q_1-q_2)n$, d.h. $n|x-y$.

(3) Sei $y \in \mathbb{Z}$. Dann gilt:

$x \equiv y (\text{mod } n) \Leftrightarrow n|x-y$

$\Leftrightarrow$ es ex. $z \in \mathbb{Z}$ mit $x-y=zn$

$\Leftrightarrow$ es ex. $z \in \mathbb{Z}$ mit $y=x+(-z)n$

$\Leftrightarrow y \in x+n\mathbb{Z}$.

(4.21) Definition und Bemerkung (Restklassenring mod n)

Sei $n \in \mathbb{Z}$.

(1) Für $x \in \mathbb{Z}$ schreiben wir $\overline{x} := x+n\mathbb{Z}$ (Notation hängt von n ab.)

$\mathbb{Z}/n\mathbb{Z} := \{\overline{x}/x \in \mathbb{Z}\}$ Menge aller Restklassen modulo n.

Es ist $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ und $|\mathbb{Z}/n\mathbb{Z}| = n$

(2) Durch $\overline{x}+\overline{y} := \overline{x+y}$ und $\overline{x} \cdot \overline{y} := \overline{xy}$

Für $x, y \in \mathbb{Z}$ wird $\mathbb{Z}/n\mathbb{Z}$ zu einem kommutativen Ring, dem *Restklassenring modulo n*.

(Nach (4.20)(4) sind diese Def. repräsentanten-unabhängig: $\overline{x} = \overline{x'}$

(z.B. $n > 7, x = 8, x' = 1 : \overline{8} = \overline{1}$

$y = 4, y' = -3 : \overline{4} = \overline{-3}$

$x+y = 12, x'+y' = -2 : \overline{12} = \overline{-2}$).)

Beweis

(1) Nach (4.20)(2) ist $\overline{x} = \overline{x \bmod n} \Rightarrow \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

für $r \neq r', 0 \leq r, r' < n$ gilt $r \bmod n = r, r' \bmod n = r'$, also $r \bmod n \neq r' \bmod n$, d.h. $\overline{r} \neq \overline{r'}$.

(2) Rechengesetze folgen aus denen von $\mathbb{Z}$.

$\overline{0} = 0+n\mathbb{Z} = n\mathbb{Z}$ ist das neutrale Element bzgl +

$\overline{1} = 1+n\mathbb{Z}$ ist das neutrale Element bzgl. $\cdot$

$\overline{-x} = -x+n\mathbb{Z}$ ist das zu x inverse El. bzgl. +

□

Restklassenarithmetik = Rechnen in $\mathbb{Z}/n\mathbb{Z}$

$\overline{x}+\overline{y} = \overline{x \bmod n} + \overline{y \bmod n} = \overline{x \bmod n + y \bmod n} = \overline{(x \bmod n + y \bmod n) \bmod n}$.

$\overline{x} \cdot \overline{y} = (xy) \bmod n$

(4.22) Beispiele

(1) $\underline{n=2:}$ $\overline{0} = 2\mathbb{Z} =$ Menge der geraden Zahlen

$\overline{1} = 1 + 2\mathbb{Z} =$ Menge der ungeraden Zahlen

$\overline{0} + \overline{1} = \overline{0+1} = \overline{1}$ gerade + ungerade = ungerade

$\overline{1} + \overline{1} = \overline{1+1} = \overline{0}$ ungerade + ungerade = gerade

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

"binäre Addition"

XOR	F	W
F	F	W
W	W	F

XOR (vgl. Kap I, § 1)

(2) $\underline{n=7:}$ $\overline{3} + \overline{5} = \overline{8} = \overline{1}$

$\overline{3} - \overline{5} = \overline{3} + \overline{-5} = \overline{-2} = \overline{5}$

$\overline{6} \cdot \overline{5} = \overline{30} = \overline{2}$ oder

$\overline{6} \cdot \overline{5} = \overline{1} \cdot \overline{5} = \overline{-5} = \overline{2}$

$\overline{6}^{100000}$

||

$\overline{-1}^{100000} = (-(\overline{1}))^{100000} = ((-(\overline{1}))^2)^{50000} = \overline{1}^{50000} = \overline{1}.$

(3) $\underline{n=6:}$

$\overline{3} \cdot \overline{2} = \overline{3 \cdot 2} = \overline{6} = \overline{0}.$

Aber $\overline{3} \neq \overline{0}$, $\overline{2} \neq \overline{0}$.

[Einheiten in $\mathbb{Z}/n\mathbb{Z}$]

Alternative Schreibweise: $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$

§ 3 Der euklidische Algorithmus

(4.23) Definition (größte gemeinsame Teiler (ggT))

Seien $x,y \in \mathbb{Z}$. Ist $(x,y) = (0,0)$, dann sei $ggT(x,y) = 0$.

Für $(x,y) \neq (0,0)$ sei $ggT(x,y) = max\{d \in \mathbb{Z} |\ d|x \bmod d|y\}$

$ggT(x,y) \in \mathbb{N}_0$ heißt der *größte gemeinsame Teiler von x und y*.

(4.24) Bemerkung

(1) Seien $x,y \in \mathbb{Z}$. Dann gilt:
   (a) $ggT(x,y) = ggT(y,x)$.
   (b) $ggT(x,y) = ggT(|x|,|y|)$.
   (c) $ggT(0,y) = |y|$.

(2) Seien $m,n \in \mathbb{N}$ mit $m \leq n$ und $m \nmid n$. Dann ist $ggT(m,n) = ggT(n \bmod m, m)$.

Beweis

(1) Klar.

(2) Sei $r := n \bmod m$ (wegen $m \nmid n$ ist $r \neq 0$).
   Dann gilt für $d \in \mathbb{Z}$ wegen $n = qm + r$: $\quad d|n$ und $d|m \Leftrightarrow d|r$ und $d|m$

□

(4.25) Algorithmen (Euklidischer Algorithmus)

Eingabe: $m,n \in \mathbb{N}, m \leq n$.

Ausgabe: $ggT(m,n)$.

```
func EUKLID(m,n)
if m|n then return m
else return EUKLID(n mod m,m).
```

□

$ggT(0,n) = n$

$ggT(m,n) = m$, falls $m|n$

$x,y \in \mathbb{Z}, \quad ggT(x,y) = \max\{\alpha \in \mathbb{Z} |\ \alpha|x \text{ und } \alpha|y\}$

$x = y = 0 \quad ggT(x,y) = 0$

(4.26) Beispiel

$m = 91, n = 168$

		$\lfloor \frac{n}{m} \rfloor$
$91, 168$	$168 \bmod 91 = 77$	1
$77, 91$	$91 \bmod 77 = 14$	1
$14, 77$	$77 \bmod 14 = 7$	5
$7, 14 \rightarrow$	$7 \mid 14 \Rightarrow ggT(91, 168) = 7$	

□

$m, n \in \mathbb{N}, d = ggT(m,n)$, dann ex. $x, y \in \mathbb{Z}$ mit $d = mx + ny$.

z.B.: $-1001 + 1008 = 7$

$91 \cdot (-11) + 168 \cdot 6$

$[n \bmod m = n - \lfloor \frac{n}{m} \rfloor \cdot m]$

(4.27) Algorithmus (Erweiterter Euklidischer Algorithmus)

Eingabe: $m, n \in \mathbb{N}$ mit $m \leq n$.

Ausgabe: $x, y \in \mathbb{Z}$ mit $ggT(m,n) = mx + ny$.

```
func E_EUKLID(m,n)
if m|n then return (1,0)
else (x',y' ⟵ E_EUKLID(n mod m,m);
      x ← y' - x' ⌊ n/m⌋;
      y ← x';
      return (x,y);
```

□

(4.28) Bemerkung (Terminierung des Algorithmus)

Der Algorithmus (4.27) terminiert mit (x,y) für das gilt: $ggT(m,n) = mx+ny$.

Beweis

Bei jedem rekursiven Aufruf von E_EUKLID ist m+n kleiner als vorher. $\rightsquigarrow$ Terminierung

Aussage klar, falls $m|n$

Sei also $m \nmid n$

$\overset{Induktion}{\Rightarrow} ggT(n \bmod m, m) = (n \bmod m)x' + my'.$

$\overset{(4.24)(2)}{\Rightarrow} ggT(m,n) = ggT(n \bmod m, m) = (n - \lfloor \frac{n}{m} \rfloor \cdot m)x' + my' = m \cdot \underbrace{x}_{=y'-x'\lfloor \frac{n}{m} \rfloor} + n \underbrace{y}_{=x'}.$ □

(4.29) Beispiel (vgl. (4.26))

$m = 91, n = 168$

m	n	x'	y'	$\lfloor \frac{n}{m} \rfloor$	
91	168	-11	6	1	$-11 = -5 - 6 \cdot 1$
77	91	6	-5	1	$6 = 1 - (-5) \cdot 1$
14	77	-5	1	5	$-5 = 0 - 1 \cdot 5$
7	14	1	0		

$-11 \cdot 91 + 6 \cdot 168 = -1001 + 1008 = 7.$ □

Einheiten in $\mathbb{Z}|n\mathbb{Z}$

$n \in \mathbb{N} : \mathbb{Z}|n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

$\ldots, 1-2n, 1-n \quad 1, 1+n, 1+2n, \ldots = \underbrace{1+n\mathbb{Z}}_{(n+1)+n\mathbb{Z}}$

(4.30) Satz

Sei $n \in \mathbb{N}$. Dann gilt für $x \in \mathbb{Z}$: $\quad \overline{x} \in (\mathbb{Z}|n\mathbb{Z})^* \Leftrightarrow ggT(x,n) = 1$.

Beweis

"$\Rightarrow$" Indirekt.

Angenommen: $\exists a \in \mathbb{N}, a \neq 1$ mit $a|x$ und $a|n$.

Sei $n = ab$ mit $0 < b < n$, d.h. $\overline{b} \neq \overline{0}$.

Aus $n|xb$ folgt $\overline{x} \cdot \overline{b} = \overline{xb} = \overline{0}$ in $\mathbb{Z}|n\mathbb{Z}$

$\overline{x} \in (\mathbb{Z}|n\mathbb{Z})^*$, d.h. $\exists x' \in \mathbb{Z}$ mit $\overline{x'} \cdot \overline{x} = \overline{1}$

$\Rightarrow \overline{0} = \overline{x'} \cdot \overline{0} = \overline{x'} \cdot (\overline{x} \cdot \overline{b}) = (\overline{x'} \cdot \overline{x}) \cdot \overline{b} = \overline{1} \cdot \overline{b} = \overline{b}$ $\quad \lightning$

"$\Leftarrow$" Seien $a, b \in \mathbb{Z}$ mit $1 = xa + nb$ (4.27)

$\Rightarrow \overline{1} = \overline{x} \cdot \overline{a} + \overline{n} \cdot \overline{b} = \overline{x} \cdot \overline{a} = \overline{a} \cdot \overline{x}$, d.h. $\overline{x} \in (\mathbb{Z}|n\mathbb{Z})^*$. $\square$

Das zu $\overline{x}$ inverse Element in $(\mathbb{Z}|n\mathbb{Z})^*$ kann mittels EEA berechnet werden.

(4.31) Korollar

Sei $n \in \mathbb{N}$. Dann: $\mathbb{Z}|n\mathbb{Z}$ Körper $\Leftrightarrow n \in \mathbb{P}$.

Beweis

$\mathbb{Z}|nZ$ Körper $\Leftrightarrow \overline{0} \neq \overline{1}$ und $(\mathbb{Z}|n\mathbb{Z})^* \overset{(4.13)}{=} \{\overline{1}, \ldots, \overline{n-1}\} \overset{(4.30)}{\Leftrightarrow} n > 1$ und $ggT(K,n) = 1 \ \ \forall 1 \leq n \leq n-1 \Leftrightarrow n \in \mathbb{P}$.

Ist $p \in \mathbb{P}$, dann setzen wir $\mathbb{F}_p := \mathbb{Z}|p\mathbb{Z}, \mathbb{F}_p$: Körper mit p Elementen.

$p = 2$, $\mathbb{F}_2 = \{\overline{0}, \overline{1}\} = \{0,1\}$

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

$+$	0	1
0	0	1
1	1	0

(4.32) Definition (Eulersche φ-Funktion)

Für $n \in \mathbb{N}$ sei $\varphi(n) := |(\mathbb{Z}|n\mathbb{Z})^*| = |\{K | 0 \leq K \leq n-1, ggT(K,n) = 1\}|$

φ heißt die *Eulersche φ-Funktion*.

(4.33) Bemerkung

1. $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)\ \forall m,n \in \mathbb{N}$ mit $ggT(m,n) = 1$.
2. $\varphi(p^k) = p^{k-1}(p-1)\ \ \forall p \in \mathbb{P}, k \in \mathbb{N}$

Beweis

1. Folgt aus der eindeutigen Primfaktorzerlegung in $\mathbb{Z}$.
2. Für $m \in \mathbb{N}$ gilt: $ggT(m, p^k) \neq 1 \Leftrightarrow p|n$.
   $\{j | 0 \leq j \leq p^k, p|j\} = \{0, 1 \cdot p, 2 \cdot p, \ldots, (p^{k-1}-1)p\}$
   Auswahl: $p^{k-1} \quad \Rightarrow \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

□

(4.34) Beispiel

$\varphi(20) = \varphi(4)\varphi(5) = 2 \cdot 4 = 8$
$\varphi(675) = \varphi(27 \cdot 25) = 3^2 \cdot 2 \cdot 5 \cdot 4 = 360$ □

(4.35) Satz (Kleiner Satz von Fermat)

Sei $p \in \mathbb{P}, a \in \mathbb{Z}$ mit $p \nmid a$. Dann ist $a^{p-1} \equiv 1 (\text{mod } p)$ (oder: $\overline{a^{p-1}} = \overline{a}^{p-1} = \overline{1}$ in $\mathbb{F}_p$).

Beweis

[Steger, Kap 5, Satz 3.18]

Beispiel

$p = 7, a = 3, 3^6 = 729 = 1 + 104 \cdot 7$.
$p = 11, a = 2, 2^{10} = 1024 = 1 + 93 \cdot 11$.

(4.36) Definition ((endliche) Ordnung)

Sei G eine Gruppe, $g \in G$. Existiert $K \in \mathbb{N}$ mit $g^K = 1$, dann sagen wir: g hat *endliche Ordnung* und $|g| := min\{K \in \mathbb{N} \,|\, g^K = 1\}$ heißt *die Ordnung von g*. □

(4.37) Satz

Sei G eine endliche Gruppe (z.B. $G = (\mathbb{Z}|n\mathbb{Z})^*$). Dann hat jedes $g \in G$ endliche Ordnung und es gilt: $|g|\,|\,|G|$.

Beweis

[Steger, Kap. 5, Kor. 5.71]. □

§ 4 Das RSA-Kryptosystem

Public Key

Zwei Schlüssel K_o: öffentlich, K_p: privat (geheim)

1. Jeder kommt K_o, kann damit Nachrichten verschlüsseln, da nur der Besitzer von K_p entschlüsseln kann.
2. Eine *verschlüsselte Nachricht*, die mit K_o entschlüsselt werden kann, muss vom Besitzer mit K_p verschlüsselt worden sein. ($\rightarrow$ Signatur)

(4.38) Beispiel (RSA-Kryptosystem)

(1) Einrichtung des Systems

1. Wähle (Kaufe) geeignete Primzahlen $p,q \in \mathbb{P}, p \neq q$ groß (ca.: 100-150 Dezimalstellen)
2. Berechne $n = p \cdot q$ (leicht)
3. Wähle (geeignetes) $a \in \mathbb{N}$ mit $ggT(a, \varphi(n)) = 1$
   Berechne (mit EEA) $b \in \mathbb{N}$ mit $ab \equiv 1 (\text{mod } \varphi(n))$
4. Publiziere (z.B. auf Homepage)
   $K_o := (n,a)$
5. Halte $K_p := b$ geheim.

(2) Verschlüsseln

Verschlüssele Zahlen aus $\{0,1,...,n-1\}$

Das Verschlüsseln ist die Abb. $e_{K_o} : \{0,1,...,n.1\}$

$\rightarrow \{0,...,n-1\} x \mapsto x^a \text{ mod } n$

(3) Entschlüsseln

Das Entschlüsseln ist die Abb.

$d_{K_p} : \{0,...,n-1\} \to 0,...,n-1$

$x \mapsto x1b \bmod n.$

(4) Korrektheit

Beh.: $\forall x \in \{0,...,n-1\}$ gilt

$d_{K_p}(e_{K_o}(x)) = x \bmod e_{K_o}(d_{K_p}(x) = x.$

(4.39) Beispiel

$p = 3, q = 11$

$n = pq = 33, \varphi(n) = 2 \cdot 10 = 20$

$a = 2, b = 7$

Klartext

$x = 13$

Geheimtext

$x^a \bmod 33 = 13^3 \bmod 33$

$13^2 = 169, 169 \equiv 4 (\bmod 33)$

$13 \cdot 4 = 52, 52 \equiv 19 (\bmod 33)$

$\Rightarrow 13^3 \bmod 33 = 19$

$19^7 \bmod 33 : 19 \equiv (-14) (\bmod 33)$

$14^2 = 196, 196 \equiv (-2) (\bmod 33)$

$\Rightarrow 19^7 \equiv (-14) \cdot (-2)^3 \equiv 14 \cdot 8 \equiv 112 \equiv 13 (\bmod 33)$

$\Rightarrow 19^7 \bmod 33 = 13 \ \ [19^7 = 893.871.739].$ □

Korrektheit

Beh.: $\forall x \in \{0,...,n-1\}$ gilt:

$d_{K_p}(e_{K_p}(x)) = x = e_{K_o}(d_{K_p}(x))$

Beweis: Wegen der Symmetrie zwischen a und b, genügt es, die 1. Aussage zu beweisen.

Für $x \in \{0,...,n-1\}$ ist $e_{K_o}(x) \equiv x^a (\text{mod } n)$

und $d_{K_p}(x) \equiv x^b (\text{mod } n)$ ((4.20)(2))

$\Rightarrow d_{K_p}(d_{K_o}(x)) \equiv x^{ab} (\text{mod } n)$

$[(x^a \text{ mod } n)^b \text{ mod } n]$

Es genügt zu zeigen: $x^{ab} \equiv x (\text{mod } n)$

Haben

$ab \equiv 1 (\text{mod } \varphi(n))$, d.h

$\varphi(n) | ab-1$

$\varphi(n) = (p-1)(q-1)$ (4.33)

Sei $c \in \mathbb{Z}$ mit $ab = \varphi(n)c + 1 = (p-1)(q-1)+1$

Im Folgenden bezeichne $\overline{x}$ (für $x \in \mathbb{Z}$) die Restklasse von x modulo p,

d.h. $\overline{x} = x + p\mathbb{Z} \in \mathbb{Z}|p\mathbb{Z}$

Damit gilt:

$x^{ab} = \overline{x}^{ab} = \overline{x}(\overline{x}^{p-1})^{(q-1)c} = \overline{x}$

(denn $\overline{x}^{p-1} = \overline{1}$ falls $p \nmid x$ [4.35], und $\overline{x} = 0$, falls $p|x$)

$\overset{(4.20)}{\underset{(4.18)}{\Longrightarrow}} x^{ab} \equiv x (\text{mod } p)$, d.h. $p | x^{ab} - x$

Analog: $q | x^{ab} - x$

$\overset{p \neq q}{\underset{p,q \in \mathbb{P}}{\Longrightarrow}} p \cdot q | x^{ab} - x, d.h. x^{ab} \equiv x (\text{mod } n).$ □

(4.40) Bemerkung (Angriffe auf RSA)

$p,q,n=qp,a,b$ wie in (4.38)

1. Wäre $\varphi(n)$ bekannt: $n \approx 10^{25}$

b könnte mit EEA (4.27) aus $a \bmod \varphi(n)$ bestimmt werden

2. Wäre p bekannt (oder q)

$\varphi(n)=(p-1)(q-1)$ wäre bekannt

Also: Kann n faktorisiert werden, ist das System gebrochen.

Umgekehrt: Ist $\varphi(n)$ bekannt, kann n faktorisiert werden.

$n-\varphi(n)+1=p+q$

$n=pq$

$\Rightarrow p$ ist Lösung von $x^2-(n-\varphi(n)+1)x+n=0$ □

§ 5 Polynome

Hier: K Körper

(4.41) Definition

1. Ein Polynom über K in der *Vorbestimmten* (oder *Variablen*) X ist ein Ausdruck der Form
   $f=\sum_{i=0}^{n} a_i X^i$
   mit a_i $inK \forall 0 \leq i \leq n$.
   Ist $a_n \neq 0$ heißt $deg(f) := n$ der Grad von f und der höchste Koeffizient von f
2. Zwei Polynome $f=\sum_{i=0}^{n} a_i X^i$ und $g=\sum_{i=0}^{n} b_i X^i$ sind gleich $:\Leftrightarrow a_i=b_i \forall 0 \leq i \leq n$.
3. $K[X] :=$ Menge der Polynome über K.
   Beispiele: $K=\mathbb{R}: -2+X-\frac{1}{3}X^2+X^3\ -2\cdot X^0X^0=1$
   $K=\mathbb{F}_2: 1+X+X^2$
   $K=\mathbb{R}$: Polynom = Polynomfkt.
   $f:\mathbb{R}\to\mathbb{R}, x\mapsto -2+x-\frac{1}{3}x^2+x^3$
   $K=\mathbb{F}_2: \mathbb{F}_2\to\mathbb{F}_2, x\mapsto \underbrace{1+x+x^2}_{=1 \forall x\in F_2}$

(4.42) Bemerkung

1. Seien $f,g \in K[X]$,
   $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{i=0}^{n} b_i X^i$. Definiere
   $f+g := \sum_{i=0}^{n} (a_i + b_i) X^i$, und
   $f \cdot g := \sum_{i=0}^{2n} c_i X^i$ mit
   $c_i = \sum_{k=0}^{i} a_k b_{i-k}$
2. Durch $+, \cdot$ wird $K[X]$ ein komm. Ring, der *Polynomring in X über K*.

□

(4.43) Bemerkung

Seien $0 \neq f,g \in K[X]$

(1) $deg(f+g) \leq \max\{deg(f), deg(g)\}$ □

Betrachte K als Teilmenge von $K[X]$, in dem $a \in K$ mit dem "konstanten Polynome" $a \cdot 1 = a \cdot X^0$ identifiziert wird.

(4.44) Bemerkung

$K[X]* = K* = K \backslash \{0\}$

Beweis:

Sei $f \in K[X]*, g \in K[X]$ mit $f \cdot g = 1$

$\underset{(4.43)}{\Longrightarrow} 0 = deg(1) = deg(f \cdot g) = deg(f) + deg(g)$

$\Rightarrow deg(f) = 0$, d.h. $f \in K*$. □

(4.45) Satz (Division mit Rest im K[X])

Seien $f,g \in K[X], g \neq 0$

Dann ex. eindeutig bestimmmte $q,r \in K[X]$ mit $f = q \cdot g + r$

und $r = 0$ oder $deg(r) < deg(g)$

Beweis: Existenz (algorithmisch):

$f = 0$ Setze $q = r = 0$.

Sei $f \neq 0$, a_m bzw. b_n die höchsten Koeffizieten von f bzw. g

Ist $m < n$, setze $q = 0, r = f$

Ist $m \geq n$, setze $f_1 := f - \frac{a_m}{b_n} X^{m-n} g$

$\Rightarrow f_1 = 0$ oder $deg(f_1) < deg(f)$

$\xRightarrow[\text{Induktion}]{} \exists q_1, r \in K[X]$ mit $f_1 = q_1 g + r$

und $r = 0$ oder $deg(r) < deg(g)$

$\Rightarrow q := q_1 + \frac{a_m}{b_n} X^{m-n}$ und r erfüllen die Beh.

Eindeutigkeit: Analog zu (4.17). □

$f = 2, g = 3, q = \frac{2}{3}, r = 0$

$3 = \frac{2}{3} \cdot 3 + 0$

Beispiel: $f = X^3 - \frac{1}{3}X^2 + X - 2, g = X^3 + 3$

$$\begin{array}{l} \left(X^3 - \frac{1}{3}X^2 + X - 2 \right) \div \left(X^2 + 3 \right) = X - \frac{1}{3} + \frac{-2X-1}{X^2+3} \\ \underline{-X^3 \qquad -3X} \\ \qquad -\frac{1}{3}X^2 - 2X - 2 \\ \qquad \underline{\frac{1}{3}X^2 \qquad +1} \\ \qquad\qquad -2X - 1 \end{array}$$

$$\Rightarrow X^3 - \tfrac{1}{3}X^2 + X - 2 = (X^2+3)\underbrace{(X - \frac{1}{3})}_{q} - \underbrace{2X-1}_{r}$$

$f \bmod g := r$

Euklidischer Alg. u. EEA funktionieren im $K[X] \rightarrow ggT(f,g)$ berechnen und $ggT(f,g) = f \cdot h + g \cdot k$ mit $h, k \in K[X]$

Restklassenarithmetik (vgl. (4.20),(4.21))

$f \in K[X], \overline{g} := g + fK[X]$ Restklasse modulo f.

$$\begin{array}{rcl} K[X]/fK[X] & := & \{\overline{g} | g \in K[X]\} \\ & & \quad || \\ & & \{\overline{g} | g \in K[X], deg(g) < deg(f)\} \end{array}$$

$\{\mathbb{Z}|n\mathbb{Z}\} = \{\overline{0}, ..., \overline{n-1}\} \quad (\mathbb{Z}/p\mathbb{Z})$

$\rightsquigarrow$ endliche Körper

(4.46) Beispiel

$K = \mathbb{F}_2 = \{0,1\}$

$f = 1 + X + X^2$

$\mathbb{F}_4 = \{0,1,x,1+x\}$

(= Restklasse der Polynome von Grad < 2)

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	1	0	

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	
$1+x$	0	$1+x$		

$X + X = 1 \cdot X + 1 \cdot X = (1+1) \cdot X = 0 \cdot X = 0$

$X^2 = (X^2 + X + 1) + \underbrace{X+1}_{Rest}$

$X(1+X) = X^2 + X = (X^2 + X + 1) + \underbrace{1}_{Rest}$

$\Rightarrow \mathbb{F}_4$ ist Körper mit 4 Elementen

[$\mathbb{Z}|4\mathbb{Z}$ ist kein Körper ! (4.31)]

$2^8 = 256 \mathbb{F}_{2^8}$ □

(4.47) Beispiel (Die RWTH-ID)

[Bunsen - Müller]

Jedes Mitglied der RWTH $\rightarrow$ RWTH-ID

1. Bedingungen:
   - leicht zu merken
   $\rightsquigarrow$ Folge von Ziffern + Buchstaben
   ohne I,J,O,V $\rightsquigarrow$ 32 Symbole
   - großer Vorrat an Nummern
   $\rightsquigarrow$ 5 Symbole, $32^5 > 30$ Mio.

- sicher gegen Vertippen

$$\left.\begin{array}{c}\text{falsches Symbol}\\ \text{Symboldreher}\end{array}\right\} \text{sollen erkannt werden}$$

$\rightsquigarrow$ Check-Symbol $\rightsquigarrow$ 6 Symbole

$\rightsquigarrow 32^6$ Nummern

Idee: Auswahl von 32^5 zulässige Nummern

2. Zulässige Nummern

- Tabelle: 32 Symbole $\overrightarrow{bij}\mathbb{F}_2^5$

$0 \leftrightarrow 00000, z \leftrightarrow 11111$

- Folge aus 6 Symbolen, z.B. SL8BRX

$\rightsquigarrow$ Bitfolge $a_0a_1....a_{29}$

$\rightsquigarrow f := \sum_{i=0}^{29} a_iX^i \in \mathbb{F}_2[X], deg(f) < 30$

Setze $g := 1+X+X^5 \in \mathbb{F}_2[X]$

Definition: $f \in \mathbb{F}_2[X]$ gehört zu zulässigen Nummer $:\Leftrightarrow f = gh$ mit $h \in F_2[X], deg(h) < 25$

3. Codierung

Folge von 5 Symbolen, z.B. L8BRX

$\rightsquigarrow$ Bitfolge $a_0a_1...a_{24}$

$\rightsquigarrow f_0 := \sum_{i=0}^{24} a_iX^i$

$\rightsquigarrow r := X^5 \cdot f_0 \bmod g$

$\rightsquigarrow f := r + X^5 \cdot f_0\ [\ \underbrace{\overbrace{00000}^{b_o...b_5} a_0a_1...a_{24}}_{\hat{=}X^5\cdot f_0}\ ]$

$\Rightarrow f$ gehört zu einer zulässigen Nummer

$\rightarrow$ RWTH-ID, z.B. SL8BRX

4. Fehlerkennung

6 Symbole $\rightarrow \hat{f} \in \mathbb{F}_2[X], deg(\hat{f}) < 30$

$g|\hat{f}$ korrekt $g \nmid \hat{f}$ $\quad \hat{f}$ keine RWTH-ID

$\star$ falsches Symbol

$\Rightarrow \hat{f} = f + X1k \cdot h$ mit $k \in \{0,5,10,...25\}$

$deg(h) < 5$

$\Rightarrow g \nmid \hat{f}$, d.h. dieser Fehler wird erkannt

$\star$ Symbol-Dreher: ähnlich

□

§ 5 Boolsche Algebren

(4.48) Definition (vgl. (4.2))

1. Eine Menge M mit einer Verknüpfung $\star$ heißt *Halbgruppe*, wenn gilt
   (AG), $(x\star y)\star z = x\star(y\star z)\forall x,y,z \in M$
2. Eine Halbgruppe $(M,\star)$ heißt *Monoid*, wenn ein $e \in M$ mit $e\star x = x = x\star e \quad \forall x \in M$
   (Neutrales Element)
3. Eine Halbgruppe oder ein Monoid $(M,\star)$ heißt abelsch, wenn $x\star y = y\star x \ \ \forall x \in M$ gilt. □

(4.49) Beispiele

1. Ist $(G,\star)$ Gruppe, dann auch Halbgruppe und Monoid.
2. $(\mathbb{N},+)$ ist Halbgruppe, $(\mathbb{N}_0,+)$ ist Monoid.
3. Ist $(R,+,\cdot)$ ein Ring (siehe (4.8)), dann ist $(R,\cdot)$ ein Monoid

(4.50) Beispiele

Sei $\emptyset \neq A$ eine endliche Menge. (ein "Alphabet")

1. Ein Wort der Länge n über $A(n \in \mathbb{N})$ ist eine Folge $w = (a_1,...,a_n)$ mit $a_i \in A \ \ \forall 1 \leq i \leq n$.
   In diesem Kontext schreibt man oft:
   $w = a_1a_2...a_n$.
   [z.B. $A = \{a,b,.....,Z,0,1,.....,+,;,....\}$ Informatik]
   $W(A)$:= Menge aller Wörter über A
2. $W(A)\times W(A) \to W(A)$,
   $(w_1,w_2) \mapsto w_1,w_2$ (Hintereinanderhängen, Konkatenation) ist eine assoziative Verknüpfung
   [(Informatik, Studentin) → InformatikStudentin]
   $W(A)$: Worthalbgruppe über A
3. Das leere Wort über A ist die leere Folge der Länge 0 und wird mit ε bezeichnet
   $A* := W(A)\cup\{\varepsilon\}$ ist ein Monoid (mit Konkatenation).

□

(4.51) Definition (Eine algebraische Struktur)

$(S, \oplus, \odot,)$, wobei $\oplus$, $\odot$ Verknüpfungen auf S sind und $: S \to S$ eine Abb., heißt Boolsche Algebra, wenn gilt:

(B1) $(S, \oplus)$ ist abelsches Monoid mit neutralem Element. 0

(B2) $(S, \odot)$ ———- ‖ ——————

(B3) $a \oplus \bar{a} = 1 \; \forall a \in S$

$a \odot \bar{a} = 0 \; \forall a \in S$

(B4) Distributivgesetze, d.h.

$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ und

$a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c) \; \forall a, b, c \in S.$ □

(4.52) Beispiel

(1) $S = \{0, 1\}$, wobei $0, 1$ den Wahrheitswerten F bzw. W entsprechen, und $\oplus, \odot,$ durch die Wahrheitstafeln der von $\vee, \wedge, \neg$ festgelegt sind.

(vgl. Kap I, § 1)

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

a	$\neg a$
0	1
1	0

Die Axiome folgen aus diesen Wahrheitstafeln

$(\{0, 1\}, \vee, \wedge, \neg)$ heißt auch Schaltalgebra.

(2) Sei M Menge, $S = P(M)$ die Potenzmenge von M (vgl. (1.3)).

$\oplus := \cup, \odot = \cap, : x \to \bar{x} := M \backslash x$ (Komplement)

Neutrales Element bzgl. $\cup : \emptyset$

$\cap : M$

$(P(M), \cup, \cap,)$ Potenzmengenalgebra □

Rechenregeln:

(4.53) Satz

Sei $(S, \oplus, \odot,)$ Boolsche Algebra. Dann gelten:

(1) Idempotenz: $a \oplus a = a, a \odot a = a \ \ \forall a \in S$

(2) Einselement : $a \oplus 1 = 1, a \odot 0 = 0 \ \ \forall \in S$

(3) Absorption: $a \oplus (a \odot b) = a, a \odot (a \oplus b) = a \forall a, b \in S$

(4) Kürzen: $\forall a, b, c \in S$ gilt:

$[(a \oplus b = a \oplus c)$ und $(\bar{a} \oplus b = \bar{a} \oplus c)] \Leftrightarrow b = a$

$(a \odot b = a \odot c)$ und $(\bar{a} \odot b = \bar{a} \odot c)] \Leftrightarrow b = c$

(5) Eindeutiges Komplement: $\forall a, b \in S$ gilt:

$[(a \oplus b = 1)$ und $(a \odot = 0)] \Leftrightarrow b = \bar{a}$

(6) Involution: $\overline{(\bar{a})} = a \quad \forall a \in S$

(7) Konstante: $\bar{0} = 1, \bar{1} = 0$

(8) De-Morgan-Regeln: $\forall a, b \in S$ gilt:

$\overline{a \dot{+} b} = \bar{a} \odot \bar{b}$ und $\overline{a \odot b} = \bar{a} \oplus \bar{b}$.

Beweis: (Exemplarisch)

Axiome u. Aussagen snd symmetrisch in $\oplus$ und $\odot$

$\rightsquigarrow$ Es genügt, von jedem Regelpaar nur eine zu zeigen.

(1) $a = a \oplus 0 = a \oplus (a \odot \bar{a}) = (a \oplus a) \odot (a \oplus \bar{a})$ B1 B3 B4 $= (a \oplus a) \odot 1 = a \oplus a$ B2

(2) $a \oplus 1 = a \oplus (a \oplus \bar{a}) = (a \oplus a) \oplus \bar{a} = a \oplus \bar{a} = 1.$

(3) $a \oplus (a \odot b) = (a \odot a) \oplus (a \odot b) = a \odot (1 \oplus b)$ B2 B4 $= a \odot 1 = a$ (2) B2

(4.54) Definition

Sei $B := \{0,1\}$ und $(B, \vee, \wedge, \neg)$ die Schaltalgebra.

$F_n(B) := \{f \,|\, B^n \to B\} f \in F_n(B)$ heißt Boolsche Funktion

Für $f, g \in F_n(B)$ seien

$f \vee g : B^n \to B, f \vee g(a_1, ..., a_n) := f(a_1, ..., a_n) \vee g(a_1, ..., a_n) \in \{0,1\} \in \{0,1\}$

$f \wedge g : B^n \to B, f \wedge (a_1, ..., a_n) := f(a_1, ...a_n) \wedge g(a_1, ..., a_n)$

$\neg f : B^n \to B, \neg f(a_1, ..., a_n) := \neg(f(a_1, ..., a_n))$.

Dadurch wird $(F^n(b), \vee, \wedge, \neg)$ eine Boolsche Algebra. □

(4.55) Definition

Sei $n \in \mathbb{N}$, und $x_1, ...x_n$ Variablen

Boolsche Polynome (oder Formeln) in $x_1, ..., x_n$ werden rekursiv def. durch:

(P1) $x_1, ..., x_n, 0, 1$ sind Boolsche Polynome

(P2) Sind p, q Boolsche Polynome, dann auch $(p) \wedge (q), (p) \vee (q), \neg(p)$

[Boolsche Polynome sind Element von $W(A)$ mit $A = \{x_1, ..., x_n, 0, 1, \vee, \wedge, \neg, (,)\}$]

P_n : Menge der Boolsche Polynome in $x_1, ..., x_n$ □

$x_1 \wedge x_2 \neq x_2 \wedge x_1$

(4.56) Definition

$\Phi : P_n \to F_n(B)$ sei wie folgt def.: Sei $p \in P_n, \Phi(P) : B^n \to B$

$(a_1, ...a_n) \mapsto p(a_1, ..., a_n)$, wobei $p(a_1, ..., a_n) \in \{0,1\}$

aus p durch Einsetzen von a_i für $x_i (1 \leq .... \leq i)$ entsteht.

[Klammern zuerst, oder Vorrangregeln]

$\Phi(P)$ heißt *Boolsche Polynomfunktion*. □

(4.57) Beispiele

(1) $p = (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$

$p(0,0) = (0 \wedge 1) \vee (1 \wedge 0) = 0 \vee 0 = 0$

$p(1,0) = (1 \wedge 1) \vee (0 \wedge 0) = 1 \vee 0 = 1$

$p(0,1) = (0 \wedge 0) \vee (1 \wedge 1) = 0 \vee 1 = 1$

$p(1,1) = (1 \wedge 0) \vee (0 \wedge 1) = 0 \vee 0 = 0$

(2) Wegen (4.53)(3) (Absorption) gilt:

$a_1 \vee (a_1 \wedge a_2) = a_1 \quad \forall a_1, a_2 \in \{0,1\}$

$\Rightarrow x_1 \vee (x_1 \wedge x_2), x_1$ liefern die gleiche Polynomfunktion. □

(4.58) Definition

(1) Wir schreiben für $p, q \in P_n : p \sim q :\Leftrightarrow \Phi(p) = \Phi(q)$

$\sim$ ist Äquivalenzrelation auf P_n ((1.22)(3))

(2) Normalformenproblem: Gesucht ist $N_n \subseteq P_n$ mit:

$\forall p \in \mathbb{P}_n \; \exists$ genau ein $q \in N_n$ mit $p \sim q$

(N_n ist ein Repräsentatensystem).

Die Elemente von N_n heißen *Normalenformen*. □

Konvention:

Für $a \in \{0,1\}$ sei $a' := a, a^0 := \neg a$

für $x_i \in \{x_1, ..., a_n\}$ sei $x_i' := x_i, x_i^0 := \neg x_i$

(4.59) Satz

Die Boolsche Polynome der Form

$q := \bigvee a_{i_1}, ...a_{i_n} \wedge x_1^{i_1} \wedge x_2^{i_2} \wedge .... \wedge x_n^{i_n} \; (i_1, ..., i_n) \in B^n$

mit $a_{i_1}, ..., a_{i_n} \in \{0,1\} \forall (i_1, ..., i_n) \in B^n$

bilden eine Menge von Normalformen, die disjunktiven Normalformen (DNF)

Beweis: Es gilt. $0^1 = 1^0 = 0, 0^0 = 1^1 = 1$

Damit gilt für $(k_1, ..., k_n) \in B^n$:

$q(k_1, ..., k_n) = \bigvee_{(i_1,...,i_n) \in B^n} a_{i_a}, ..., a_{i_n} \wedge k_1^{i_1} \wedge ... \wedge k_1^{i_n}$

// ab hier fehler bereinigen!

$$= \begin{cases} 0, & \text{falls } (i_1 \text{ falls } (i_1 ...., i_n) \neq \\ 1, & \text{sonst} \end{cases}$$

$= a$.....

$\Rightarrow q$ beschreibt genau die Polynomfkt mit Werten $a_{k_1}, ...a_{k_n}$ für $(k_1, ..., k_n) \in B^n$. $\square$

Index