

Einführung in die Mathematik für Informatiker, Cheatsheet

Tobias Kadenbach

26. Februar 2020

Inhaltsverzeichnis

1	Gruppen	2
1.1	Definition	2
1.2	Darstellung und abelsche Gruppen	2
1.3	Gruppenisomorphie	2
1.4	Erzeugendensystem	3
1.5	Einheitengruppen	3
1.6	Untergruppen	3
1.7	Linksnebenklassen	4
1.8	Ordnung eines Elements	4
2	Graphen	4
2.1	Komplementärer Graph	4
2.2	Bipartite Graphen	4
2.3	Bäume	4
2.4	Subgraph	5
2.4.1	Induzierter Subgraph	5
2.5	Brücken	5
2.6	Gelenkpunkte	5
2.7	Blockgraph	5
3	Satz von Euler Fermat	5

1 Gruppen

1.1 Definition

(G, \circ) ist eine Gruppe falls:

- abgeschlossen bzgl. \circ
- assoziativ
- neutrales Element mit $\exists e \in G \forall g \in G e \circ g = g \circ e = g$
- Inverse: $\forall g \in G \exists g^{-1} \in G g \circ g^{-1} = g^{-1} \circ g = e$

1.2 Darstellung und abelsche Gruppen

Eine mögliche Darstellung einer Gruppe ist eine sogenannte Gruppentafel dabei wird jedes Element der Gruppe in eine Zeile und eine Spalte geschrieben und anschließend werden so die Elemente der Gruppe mit der Gruppenoperation verbunden. Das ausfüllen erfolgt dabei nach dem Sudokuprinzip (in jeder Zeile und Spalte darf jedes Element nur exakt einmal vorkommen). Eine Gruppe wird auch abelsche genannt falls diese zur Hauptdiagonale symmetrisch ist.

1.3 Gruppenisomorphie

Eine Gruppe g ist Isomorph zu einer anderen Gruppe h wenn:

- h ist selber eine Gruppe
- es existiert ein Isomorphismus der jedem Element der Gruppe g ein Element der Gruppe h eindeutig zuordnet es muss gelten wenn $a \mapsto x$, $b \mapsto y$ und $c \mapsto z$ und gilt $a \circ b = c$, dann muss auch $x \circ y = z$ gelten.
- die Homomorphie Eigenschaft ist erfüllt ($h(a \circ b) = h(a) \circ h(b)$)

1.4 Erzeugendensystem

Ein Element einer Gruppe ist Erzeugendensystem wenn mit diesem Element und der Gruppeneoperation jedes Element der Gruppe erzeugt werden kann.

Beispiel:

$(\mathbb{Z}_n, +)$: $m \in \mathbb{Z}_n$ ist Erzeuger gleichbedeutend sind:

- m ist Einheit
- $\text{ggT}(m, n) = 1$

(\mathbb{Z}_n ist **zyklisch**, denn z.B. $\langle \{1\} \rangle = \mathbb{Z}_n$)

Die Anzahl an Erzeugern (o.a. Primitivwurzeln) lässt sich durch: $\phi(n)$ er-rechnen.

Beispiel:

$(\mathbb{Z}_{13}, +)$ hat $\phi(13) = 12$ Erzeuger.

1.5 Einheitengruppen

Einheiten Gruppen \mathbb{Z}_n^* enthalten nur die Einheiten der Gruppe \mathbb{Z}_n

Beispiel:

Eine Primitivwurzel von \mathbb{Z}_{13}^* finden:

n	1	2	3	4	5	6	7	8	9	10	11	12
2^n	2	4	8	$16 \equiv 3$	6	12	$24 \equiv 11$	$22 \equiv 9$	$18 \equiv 5$	10	$20 \equiv 7$	$14 \equiv 1$

1.6 Untergruppen

Sei (G, \circ) eine Gruppe $U \subset G$ ist eine Untergruppe von G falls:

- U ist abgeschlossen bzgl. \circ
- $e_G \in U$ (neutrales Element der Gruppe enthalten)
- $\forall u \in U : u^{-1} \in U$ (für jedes Element auch inverses enthalten)

Satz 1.1 (Satz von Lagrange) *Die Untergruppenordnung teilt die Gruppenordnung*

Beispiel:

\mathbb{Z}_{14}^* kann Untergruppen der Ordnung 1,2,3,6 haben da $|\mathbb{Z}_{14}^*| = 6$ Dabei ist:

- $\{1\}$ Untergruppe der Ordnung 1
- $\{1,13\}$ Untergruppe der Ordnung 2
- $\{1,9,11\}$ Untergruppe der Ordnung 3

1.7 Linksnebenklassen

U ist Linksnebenklasse von G falls $g \circ U = \{g \circ u | u \in U\}$

Beispiel für \mathbb{Z}_{14}^* :

$$1 \cdot U_2 = 1 \cdot 1, 1 \cdot 13 = U_2 \cdot 13$$

$$3 \cdot U_2 = 3 \cdot 1, 3 \cdot 13 = U_2 \cdot 11$$

$$5 \cdot U_2 = 5, 9 = U_2 \cdot 9$$

1.8 Ordnung eines Elements

$$\langle g \rangle = \{g, g \circ g, g \circ g \circ g\}$$

$$|\langle 1 \rangle| = |\{1\}| = 1 \Rightarrow 1 \text{ hat die Ordnung } 1$$

2 Graphen

2.1 Komplementärer Graph

Formel um die Knotenanzahl von \bar{G} zu berechnen: $\bar{G} = (V, \binom{V}{2} - E)$ also $\binom{n}{2} - |E|$

2.2 Bipartite Graphen

Ein Graph heißt bipartit falls man ihn mit genau zwei Farben so färben kann, dass nie zweimal die selbe Farbe nebeneinander auftritt. Ein Graph kann nicht bipartit sein wenn es ungerade Kreise in dem Graphen gibt.

2.3 Bäume

Ein Baum ist ein Graph der $T=(V,E)$ der keine Kreise hat und zusammenhängend ist.

2.4 Subgraph

Ein Graph $H=(W,F)$ heißt Subgraph von $G=(V,E)$, wenn $W \subseteq V$ und $F \subseteq E$.

2.4.1 Induzierter Subgraph

Ein induzierter Teilgraph entsteht, wenn beim Obergraphen ein oder mehrere Knoten samt dessen inzidenten ¹ Kanten entfernt werden.

2.5 Brücken

Subgraph $(\{u,v\}, \{\{u,v\}\})$ von G , so dass für die Zusammenhangskomponente H von u und v gilt: $(H, E(H) \setminus \{u,v\})$ nicht zusammenhängend.

2.6 Gelenkpunkte

Wenn man diesen Knoten entfernt so ist der Graph danach nicht mehr zusammenhängend.

2.7 Blockgraph

$$G_B = (V_B, E_B)$$

Knotenmenge $V_B = A \cup B$:

A: Menge der Gelenkpunkte

B: Menge der Blöcke

3 Satz von Euler Fermat

Seien $a, n \in \mathbb{N}$ und $\text{ggT}(a,n) = 1$ dann gilt:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Rechenbeispiel:

Berechnen Sie die letzten zwei Ziffern der Zahl 211^{1043} : Also $211^{1043} \bmod 100$ da 2 Stellen.

¹angrenzende