Einführung in die Mathematik für Informatiker, Cheatsheet

Tobias Kadenbach

February 23, 2020

Contents

1 Gruppen

1.1 Definition

(G, ·) ist eine Gruppe falls:

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

1.2 Darstellung und abelsche Gruppen

Eine möglische Darstellung einer Gruppe ist eine sogenannte Gruppentafel dabei wir jedes Element der Gruppe in eine Zeile und eine Spalte geschrieben und anschließen 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 exisitiert ein Isomorphismus der jedem Element der Gruppe g ein Element der Gruppe h eineindeutig zuordnet es muss gelten wenn a $\mapsto$x , b $\mapsto$y und c $\mapsto$z und gilt a $\cdot$b = c, dann muss auch x $\cdot$y = z gelten.
- die Homomorphie Eigenschaft ist erfüllt (   )

1.4 Erzeugendensystem

Ein Element einer Gruppe ist Erzeugensystem wenn mit diesem Element und der Gruppneoperation jedes Element der Gruppe erzeugt werden kann.
Beispiel:
$(\mathbb{Z}_n, +)$: $m \in \mathbb{Z}_n$ ist Erzeuger gleichbedeutend sind:

- m ist Einheit
- ggt(m,n) = 1

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

Die Anzahl an Erzeugern lässt sich durch: $\phi(n)$ errechnen.
Beispiel:
$(\mathbb{Z}_{13}, +)$ hat $\phi(13) = 12$ Erzeuger.

2 Satz von Euler Fermat

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

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

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