Algebra für Informationssystemtechniker

Prof. Dr. Ulrike Baumann

Fachrichtung Mathematik

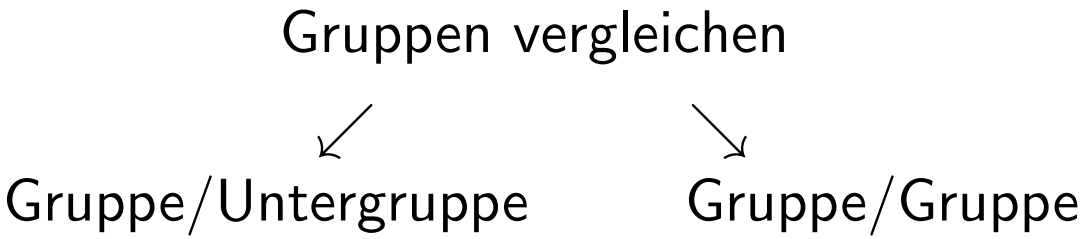
Institut für Algebra

www.math.tu-dresden.de/∼baumann

Ulrike.Baumann@tu-dresden.de

04.06.2018

11. Vorlesung



- Nebenklassenzerlegungen

  Satz von Lagrange

  Beispiel aus der Codierungstheorie

- Isomorphie von Gruppen

  Satz von Cayley

  Wichtige endliche Gruppen

Zyklische Gruppen

- Zu jeder Teilmenge T einer (endlichen) Gruppe gibt es eine kleinste Untergruppe, die T enthält. Man nennt sie die **von T erzeugte Untergruppe** $\langle T \rangle$.

  $\langle T \rangle$ besteht aus
  - dem neutralen Element
  - allen Elementen von T
  - allen Elementen, die man daraus durch wiederholtes Anwenden der Gruppenoperation und der Inversenbildung gewinnen kann.

  Ist $T = \{a\}$, schreibt man auch $\langle T \rangle = \langle a \rangle$.

- Gruppen, die von einem einzigen Element erzeugt werden, nennt man **zyklisch**.

- Sei G eine Gruppe und $a \in G$.
  Die **Ordnung des Elements** a von G ist die Mächtigkeit der von a erzeugten zyklischen Untergruppe $\langle a \rangle$.

Nebenklassen

- Ist U eine Untergruppe der Gruppe G und $g \in G$, dann nennt man
$$g \circ U = \{g \circ u \mid u \in U\}$$
eine (Links-)**Nebenklasse** von U in G.

- Analog kann man Rechtsnebenklassen von U in G definieren.

- Je zwei Nebenklassen $a \circ U$ und $b \circ U$ von U in G sind entweder gleich oder disjunkt.

- Jede Nebenklasse von U in G hat die Mächtigkeit $|U|$.

Satz von Lagrange

- Sei G eine endliche Gruppe und U eine Untergruppe von G. Der **Index** $[G : U]$ von U in G ist die Anzahl der Nebenklassen von U in G.

- **Satz von Lagrange:**

  Ist U eine Untergruppe einer endlichen Gruppe G, dann gilt:

$$[G : U] = \frac{|G|}{|U|}$$

- Folgerungen
  - Die Ordnung einer Untergruppe ist ein Teiler der Ordnung der Gruppe.
  - Ist G eine Gruppe von Primzahlordnung p, dann hat G genau zwei Untergruppen.

Beispiel: Fehlerkorrektur im Standardfeld

- $((\mathbb{Z}_2)^n, +)$ ist eine Gruppe.
- $(\mathcal{C}, +)$ sei eine Untergruppe von $((\mathbb{Z}_2)^n, +)$.

Wähle in der Nebenklassenzerlegung
$(\mathbb{Z}_2)^n = a_1 + \mathcal{C} \cup a_2 + \mathcal{C} \cup \ldots \cup a_s + \mathcal{C}$ von $((\mathbb{Z}_2)^n, +)$ für a_i solche Vektoren in den Nebenklassen aus, die minimales Gewicht haben (*Klassenanführer*).

Beispiel: $|(\mathbb{Z}_2)^5| = 2^5 = 4 \cdot 8 = |\mathcal{C}| \cdot s$

00000	01101	10111	11010
00001	01100	10110	11011
00010	01111	10101	11000
00100	01001	10011	11110
01000	00101	11111	10010
10000	11101	00111	01010
00011	01110	10100	11001
00110	01011	10001	11100

Decodieren: Korrigiere $y \in a_i + \mathcal{C}$ zum Codewort $c = y + a_i$.

y wird zu dem Codewort c korrigiert (steht in der ersten Zeile!), das in der gleichen Spalte wie y steht.

Isomorphie von Gruppen

- Eine Gruppe $(G_1, \circ_1, (^{-1})_1, e_1)$ heißt zu einer Gruppe $(G_2, \circ_2, (^{-1})_2, e_2)$ **isomorph**, wenn es eine bijektive Abbildung $f : G_1 \to G_2$ mit

  (1) $f(a \circ_1 b) = f(a) \circ_2 f(b)$ für alle $a, b \in G_1$
  (2) $f(a^{-1}) = f(a)^{-1}$ für alle $a \in G_1$
  (3) $f(e_1) = e_2$

  gibt. Die Abbildung f heißt **Isomorphismus**.

- Die Isomorphie von Gruppen ist eine Äquivalenzrelation. Man kann von zueinander isomorphen Gruppen sprechen.

- Gruppen sind zueinander isomorph, wenn sie sich nur in der Bezeichnung der Elemente unterscheiden (isomorphe Gruppen sind Gruppen mit gleicher Struktur).

Isomorphieklassen von Gruppen

- Anzahl der Isomorphieklassen für Gruppen mit $n \leq 18$ Elementen:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5

- Es gibt bis auf Isomorphie genau eine Gruppe mit p Elementen, wenn p eine Primzahl ist.

- Satz von Cayley:

  Jede endliche Gruppe mit n Elementen ist zu einer Untergruppe der symmetrischen Gruppe S_n isomorph.

Wichtige endliche Gruppen

- Zyklische Gruppe Z_n der Ordnung n:

$$\begin{aligned} Z_n &= \langle d \mid d^n = e \rangle \\ &= \{e, d, d^2, \ldots, d^{n-1}\} \end{aligned}$$

  Z_n ist abelsch.

- Diedergruppe D_n der Ordnung $2n$ ($n > 2$):

$$\begin{aligned} D_n &= \langle d, s \mid d^n = e,\ s^2 = e,\ s \circ d = d^{-1} \circ s \rangle \\ &= \{e, d, \ldots, d^{n-1}, s, d \circ s, d^2 \circ s, \ldots, d^{n-1} \circ s\} \end{aligned}$$

  Die Diedergruppe D_n ist die Symmetriegruppe des regelmäßigen n-Ecks.

  D_n ist nichtabelsch.