Elementare Gruppentheorie

Simon Lentner

Algebra und Zahlentheorie, Universität Hamburg

simon.lentner@uni-hamburg.de

9.4.2018

Definition

Eine **Gruppe** $(G, \circ)$ *besteht aus*

Daten:

- *Menge von Dingen* G.
- *Art* $\circ$, *zwei Dinge* $a, b \in G$ *zu neuem Ding* $a \circ b \in G$ *zu kombinieren.*

Axiomen:

- $(a \circ b) \circ c = a \circ (b \circ c)$
- *Es gibt ein neutrales Ding* e *mit* $e \circ b = b \circ e = b$
- *Es gibt immer ein inverses Ding* $\bar{b}$ *mit* $b \circ \bar{b} = \bar{b} \circ b = e$

Definition

Eine **Gruppe** $(G, \circ)$ *besteht aus*

Daten:

- *Menge von Dingen* G*.*
- *Art* $\circ$*, zwei Dinge* $a, b \in G$ *zu neuem Ding* $a \circ b \in G$ *zu kombinieren.*

Axiomen:

- $(a \circ b) \circ c = a \circ (b \circ c)$
- *Es gibt ein neutrales Ding* e *mit* $e \circ b = b \circ e = b$
- *Es gibt immer ein inverses Ding* $\bar{b}$ *mit* $b \circ \bar{b} = \bar{b} \circ b = e$

Zusätzlich heißt die Gruppe

- **endlich**, wenn es nur endlich viele Dinge in G gibt.
- **kommutativ**, wenn immer $a \circ b = b \circ a$.

Definition

Die **Gruppe** $(\mathbb{Z}, +)$ *besteht aus*

Daten:

- *Menge aller ganzen Zahlen.*
- *Art, zwei Zahlen zu einer neuen ganzen Zahl* $a + b$ *zu addieren.*

Axiome:

- $(a + b) + c = a + (b + c)$
- *Es gibt die neutrale* 0 *mit* $0 + b = b + 0 = b$
- *Es gibt immer die* $-b$ *mit* $b + (-b) = (-b) + b = 0$

Die Gruppe ist kommutativ und unendlich.

Definition

Die **Gruppe** $(\mathbb{Q}, +)$ *besteht aus*

Daten:

- *Menge aller Brüche.*
- *Art, zwei Brüche zu einem neuen Bruch* $a + b$ *zu addieren.*

Axiome:

- $(a + b) + c = a + (b + c)$
- *Es gibt die neutrale* 0 *mit* $0 + b = b + 0 = b$
- *Es gibt immer die* $-b$ *mit* $b + (-b) = (-b) + b = 0$

Die Gruppe ist kommutativ und unendlich.

Definition

Die **Gruppe** $(\mathbb{R}, +)$ *besteht aus*

Daten:

- *Menge aller reeller Zahlen.*
- *Art, zwei Zahlen zu einer neuen Zahl* $a + b$ *zu addieren.*

Axiome:

- $(a + b) + c = a + (b + c)$
- *Es gibt die neutrale* 0 *mit* $0 + b = b + 0 = b$
- *Es gibt immer die* $-b$ *mit* $b + (-b) = (-b) + b = 0$

Die Gruppe ist kommutativ und unendlich.

Definition

Die **Gruppe** $(\mathbb{R}$ *ohne* $\{0\}, \cdot)$ *besteht aus*

Daten:

- *Menge aller Zahlen außer* 0.
- *Art, zwei Zahlen zu einer neuen Zahl* $a \cdot b$ *zu multiplizieren*

Axiome:

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- *Es gibt die neutrale* 1 *mit* $1 \cdot b = b \cdot 1 = b$
- *Es gibt immer die Zahl* $\frac{1}{b}$ *mit* $b \cdot \frac{1}{b} = \frac{1}{b} \cdot b = 1$

Die Gruppe ist kommutativ und unendlich.

Definition

Die **Zyklische Gruppe** $(\mathbb{Z}_n, +)$ *für eine feste Zahl* n *besteht aus*

Daten:

- *Menge aller ganzen Zahlen* $\{0, 1, \ldots n-1\}$.
- *Art, zwei Zahlen zu einer neuen Zahl* $a+b$ *zu addieren, modulo* n

Axiome:

- $(a+b)+c = a+(b+c)$
- *Es gibt die neutrale* 0 *mit* $0+b = b+0 = b$
- *Es gibt immer die* $-b$ *mit* $b+(-b) = (-b)+b = 0$

Die Gruppe ist kommutativ und endlich von Größe n.

Beispiel: $\mathbb{Z}_{12}$ Uhr, $\mathbb{Z}_7$ Wochentage

Definition

Die **Permutations-Gruppe** $(\mathbb{S}_n, \circ)$ *für eine feste Zahl n besteht aus:*
Daten:

- *Menge aller Permutationen von n Symbolen, z.B.*

$$(\approx, \ominus, \Omega, \mathbb{m}) \overset{b}{\leftarrow} (\ominus, \Omega, \mathbb{m}, \approx)$$

- *Art, zwei Operationen hineineinander-auszuführen $a \circ b$, z.B.*

$$(\approx, \ominus, \mathbb{m}, \Omega) \overset{a}{\leftarrow} (\approx, \ominus, \Omega, \mathbb{m}) \overset{b}{\leftarrow} (\ominus, \Omega, \mathbb{m}, \approx)$$

Axiome:

- $(a \circ b) \circ c = a \circ (b \circ c)$
- *Es gibt Nichst-Tun:* $(\ominus, \Omega, \mathbb{m}, \approx) \overset{e}{\leftarrow} (\ominus, \Omega, \mathbb{m}, \approx)$
- *Es gibt immer Rückgängig-Machen einer Permutation:*
  $(\ominus, \Omega, \mathbb{m}, \approx) \overset{\bar{b}}{\leftarrow} (\approx, \ominus, \Omega, \mathbb{m}) \overset{b}{\leftarrow} (\ominus, \Omega, \mathbb{m}, \approx)$

Die Gruppe ist **nicht** *kommutativ und endlich von Größe n!.*

sowie die *geraden Permutationen* $\mathbb{A}_n$ als Teilmenge. Anwendung z.B. auf Rubick-Würfel, Konstruierbarkeit etc.

Definition

Die **Zopf-Gruppe** $(\mathbb{B}_n, \circ)$ *für eine feste Zahl n besteht aus*

Daten:

- *Menge aller Zöpfe in n Strägen bis auf "Zurechtzupfen"*
- *Art, zwei Zöpfe hineineinander-zuflechten* $a \circ b$, *z.B*

Axiome:

- $(a \circ b) \circ c = a \circ (b \circ c)$
- *Es gibt den trivialen Zopf*

- *Es gibt immer den Rückwärts-Zopf*

Die Gruppe ist nicht-kommutativ und unendlich.

Definition

Die **Dreh-Gruppe** $(\mathrm{O}_n, \circ)$ *für eine feste Zahl n besteht aus*

Daten:

- *Menge aller Drehungen und Spiegelungen in n Dimensionen*
- *Art, zwei Drehungen hintereinander-auszuführen*

Axiome:

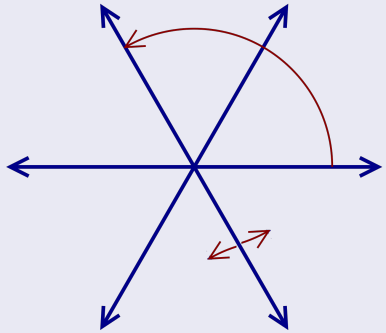
- $(a \circ b) \circ c = a \circ (b \circ c)$
- *Es gibt Nichst-Tun*
- *Es gibt immer Rückgängig-Machen einer Drehung*

Die Gruppe ist für $n \neq 1$ *nicht-kommutativ und unendlich.*

Definition

Die **Spiegelungs-Gruppe** $(\mathrm{A}_2, \circ), \circ)$ *besteht aus*
Daten:

- *Menge der folgenden Spiegelungen und Drehungen in 2 Dimensionen*



- *Art, zwei Drehungen hintereinander-auszuführen:* **Bleibt in** A_2**!**

Axiome:

- $(a \circ b) \circ c = a \circ (b \circ c)$
- *Es gibt Nichst-Tun*
- *Es gibt immer Rückgängig-Machen einer Drehung*

Die Gruppe ist nicht-kommutativ und **endlich** *von der Größe* 6.

Klassifikation aller endlichen (Weyl-) Spiegelungsgruppen (1890)
A_n, B_n, C_n, B_n und G_2, F_4, E_6, E_7, E_8

Philosophische Zwischenfolie

Mathematik als Lehre von Konsequenzenbäumen
Axiome als verschiedene Brillen (weniger als Annahmen)
Beispiel: Reelle Zahlen als Gruppe, Körper, Topologie, Ordnung,...

Sinnvolle Axiomensystems

- wirken fast trivial (bei richtiger Sicht)
- haben aber hochgradig nichttriviale Konsequenzen (zwischen Chaos und Banalität)
- Treten häufig auf

Philosophische Zwischenfolie

Wie kann ich überhaupt **alle Möglichkeiten klassifizieren?**
("die noch unbekannte Spezies deduzieren." Man lernt Strukturtheorie):

Merkmale finden mit überschaubaren Ausprägungen ("klassifiziert")
aber mit starken Konsequenzen für das unbekannte Objekt.
Alle Ausprägungen nachverfolgen, dann weitere Merkmale finden.
Letztlich die Lösungen konstruieren oder ausschließen.

Beispiel: Platonische Körper. Später: Gruppen.

(auch z.B. Aristoteles' Rhethorik, Schopenhauer's Grundregungen etc.)

Klassifikation: Alle möglichen Gruppen verstehen

Struktur einer *beliebigen* Gruppe verstehen.
Gruppen in unzerlegbare (=einfache) Gruppen zerlegen.

Klassifikation: Alle möglichen Gruppen verstehen

Struktur einer *beliebigen* Gruppe verstehen.
Gruppen in unzerlegbare (=einfache) Gruppen zerlegen.

Theorem (Folklore, Stoff für Mathematik Lehramt)

Jede endliche **kommutative** *Gruppe*
ist das Produkt von zyklischen Gruppen.

Klassifikation: Alle möglichen Gruppen verstehen

Struktur einer *beliebigen* Gruppe verstehen.
Gruppen in unzerlegbare (=einfache) Gruppen zerlegen.

Theorem (Folklore, Stoff für Mathematik Lehramt)

Jede endliche **kommutative** *Gruppe*
ist das Produkt von zyklischen Gruppen.

Theorem (Feit-Thompson (1963) 250 Seiten)

Jede endliche Gruppe von **ungerader Größe**
kann in zyklische Gruppen zerlegt werden.

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p
- Gerade Permutationen $\mathbb{A}_n$ für $n \geq 5$

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p
- Gerade Permutationen $\mathbb{A}_n$ für $n \geq 5$
- Drehgruppe $\mathrm{O}_n(\mathbb{Z}_p)$ in Räumen $\mathbb{Z}_p^n$ statt $\mathbb{R}^n$

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p
- Gerade Permutationen $\mathbb{A}_n$ für $n \geq 5$
- Drehgruppe $\mathrm{O}_n(\mathbb{Z}_p)$ in Räumen $\mathbb{Z}_p^n$ statt $\mathbb{R}^n$
- ...und andere geometrische Lie-Gruppen über $\mathbb{Z}_p$ klassifiziert durch ihre endliche Spiegelungsgruppen

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p
- Gerade Permutationen $\mathbb{A}_n$ für $n \geq 5$
- Drehgruppe $\mathrm{O}_n(\mathbb{Z}_p)$ in Räumen $\mathbb{Z}_p^n$ statt $\mathbb{R}^n$
- ...und andere geometrische Lie-Gruppen über $\mathbb{Z}_p$ klassifiziert durch ihre endliche Spiegelungsgruppen
- 26 Sporadische Gruppen, z.B.

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p
- Gerade Permutationen $\mathbb{A}_n$ für $n \geq 5$
- Drehgruppe $\mathrm{O}_n(\mathbb{Z}_p)$ in Räumen $\mathbb{Z}_p^n$ statt $\mathbb{R}^n$
- ...und andere geometrische Lie-Gruppen über $\mathbb{Z}_p$ klassifiziert durch ihre endliche Spiegelungsgruppen
- 26 Sporadische Gruppen, z.B.
  - Mathieu (1873) M_{24} mit Größe 244823040 permutiert 24 Symbole

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p
- Gerade Permutationen $\mathbb{A}_n$ für $n \geq 5$
- Drehgruppe $\mathrm{O}_n(\mathbb{Z}_p)$ in Räumen $\mathbb{Z}_p^n$ statt $\mathbb{R}^n$
- ...und andere geometrische Lie-Gruppen über $\mathbb{Z}_p$
  klassifiziert durch ihre endliche Spiegelungsgruppen
- 26 Sporadische Gruppen, z.B.
  - Mathieu (1873) M_{24} mit Größe 244823040
    permutiert 24 Symbole
  - Conway (1968) Co_1 mit Größe 4157776806543360000
    Drehungen des 24-dimensionalen Leech-Kugelpackung, enthält drei E_8

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p
- Gerade Permutationen $\mathbb{A}_n$ für $n \geq 5$
- Drehgruppe $\mathrm{O}_n(\mathbb{Z}_p)$ in Räumen $\mathbb{Z}_p^n$ statt $\mathbb{R}^n$
- ...und andere geometrische Lie-Gruppen über $\mathbb{Z}_p$
  klassifiziert durch ihre endliche Spiegelungsgruppen
- 26 Sporadische Gruppen, z.B.
  - Mathieu (1873) M_{24} mit Größe 244823040
    permutiert 24 Symbole
  - Conway (1968) Co_1 mit Größe 4157776806543360000
    Drehungen des 24-dimensionalen Leech-Kugelpackung, enthält drei E_8
  - Fischer, Griess (1976) $\mathbb{M}$ mit 53-stelliger Größe
    Symmetrien einer 24-dimensionalen Quantenfeldtheorie

Was sind die endlichen unzerlegbaren Gruppen?

- Zyklische Gruppe $\mathbb{Z}_p$ für Primzahl p
- Gerade Permutationen $\mathbb{A}_n$ für $n \geq 5$
- Drehgruppe $\mathrm{O}_n(\mathbb{Z}_p)$ in Räumen $\mathbb{Z}_p^n$ statt $\mathbb{R}^n$
- ...und andere geometrische Lie-Gruppen über $\mathbb{Z}_p$
  klassifiziert durch ihre endliche Spiegelungsgruppen
- 26 Sporadische Gruppen, z.B.
  - Mathieu (1873) M_{24} mit Größe 244823040
    permutiert 24 Symbole
  - Conway (1968) Co_1 mit Größe 4157776806543360000
    Drehungen des 24-dimensionalen Leech-Kugelpackung, enthält drei E_8
  - Fischer, Griess (1976) $\mathbb{M}$ mit 53-stelliger Größe
    Symmetrien einer 24-dimensionalen Quantenfeldtheorie

Theorem (Viele Forscher (1832-2002) ca. 15000 Seiten)

Das sind alle endlichen einfachen (=unzerlegbaren) Gruppen.