Vortragsskript
Einführung in die Algebra

TeamTUM - Das Wettbewerbsteam Mathematik

Technische Universität München
Fakultät für Mathematik

Vortragender: Vu Phan Thanh
Datum: 26.11.12

Inhaltsverzeichnis

1. Halbgruppe, Monoid, Gruppe

Definition 01: **Verknüpfung**

Eine Verknüpfung $\circ$ auf einer Menge M ist eine Abbildung (Abgeschlossenheit)

$$\circ : \ M \times M \to M, \quad (a, b) \mapsto a \circ b$$

Die Verknüpfung $\circ$ heißt assoziativ, falls $\forall a, b, c \in M : \ (a \circ b) \circ c = a \circ (b \circ c)$, und kommutativ, falls $\forall a, b \in M : \ a \circ b = b \circ a$

Definition 02: **Halbgruppe**

Sei M eine Menge und $\circ$ eine assoziative Verknüpfung, dann heißt das Paar $(M, \circ)$ Halbgruppe. (*Notation:* Wir schreiben ab statt $a \circ b$ und sagen Halbgruppe M)

Definition 03: **(Links-/Rechts-)Neutralelement**

Ein Element e einer Halbgruppe M heißt linksneutral, falls $\forall m \in M : \ em = m$, rechtssneutral, falls $\forall m \in M : \ me = m$, und neutral, falls e sowohl linksneutral, als auch rechtsneutral ist

Satz 1: **Eindeutigkeit des Neutralelement**

Besitzt eine Halbgruppe M ein linksneutrales Element e und ein rechtsneutrales Element e', so gilt $e = e'$ und diese stellen somit das eindeutige Neutralelement in der Halbgruppe M dar. *Beweis:* Es gilt: $e' = ee' = e$

Definition 04: **Monoid**

Eine Halbgruppe M, welches ein Neutralelement $e \in M$ besitzt, heißt Monoid. Insbesondere ist das Neutralelement e gemäß *Satz 1* eindeutig.

Definition 05: **(Links-/Rechts-)Inverses**

Seien x, y zwei Elemente eines Monoids M, für welche $xy = e$ (Neutralelement e) gilt. Dann heißt x Linksinverses zu y bzgl. e, y heißt Rechtsinverses zu x bzgl. e, ist gar $xy = e = yx$, so heißt x Inverses zu y bzgl. e und umgekehrt.

Satz 2: **Eindeutigkeit des Inversen**

Besitzt ein Element x des Monoids M ein Linksinverses y und ein Rechtsinverses y', so gilt $y = y'$, somit besitzt insbesondere jedes Element $x \in M$ höchstens ein Inverses aus der Halbgruppe M. *Beweis:* Es gilt: $y = ye = yxy' = ey' = y'$

Definition 06: **Gruppe**

Sei G eine Menge und $\circ$ eine Verknüpfung, dann heißt das Paar $(G, \circ)$ Gruppe, falls folgende Axiome erfüllt sind:
1. Die Verknüpfung $\circ$ ist assoziativ, (somit ist G eine Halbgruppe)
2. Es existiert ein Element $e \in G$, sodass
a) e ein linksneutrales Element in der Halbgruppe G ist
b) jedes Element $g \in G$ besitzt ein Linksinverses bzgl. e

Eine Gruppe G mit einer kommutativen Verknüpfung heißt abelsche Gruppe

Satz 3: **Charakterisierung der Gruppe**

Eine Gruppe G ist ein Monoid (mit Neutralelement e), in der jedes Element $g \in G$ ein eindeutiges Inverses bzgl. e besitzt. (Dieses wird mit g^{-1} bezeichnet.)

2. Untergruppe

Definition 01: **Untergruppen**

Sei G eine Gruppe und $H \subseteq G$ eine Teilmenge eben dieser.
Dann heißt H eine Untergruppe von G, falls gilt:
1. Ist $a, b \in H$, dann ist auch $ab \in H$ (Abgeschlossenheit)
2. H zusammen mit der eingeschränkten Verknüpfung von G auf H
(also $\circ : \ H \times H \to H, \ \ (a, b) \mapsto a \circ b$) wiederum eine Gruppe

Satz 1: **Charakterisierung von Untergruppen**

Eine Teilmenge H einer Gruppe G ist genau dann eine Untergruppe von G, wenn
1. $H \neq \varnothing$ und 2. $a, b \in H \Rightarrow ab^{-1} \in H$

Satz 2: **Schnitt von Untergruppen**

Sei $(H_i)_{i \in I}$ eine Familie von Untergruppe von G mit Indexmenge I, dann ist folgender Schnitt ebenfalls eine Untergruppe von G

$$\bigcap_{i \in I} H_i \subseteq G$$

Definition 02: **Erzeugte Untergruppen**

Sei S eine beliebige Teilmenge einer Gruppe G, dann heißt die kleinste Untergruppe von G, die S enthält, die von S erzeugte Untergruppe $\langle S \rangle$. Sie ist gegeben durch folgenden Schnitt aller Unntergruppen H, die Obermengen von S sind:

$$\langle S \rangle = \bigcap_{S \subseteq H \subseteq G} H \subseteq G$$

Eine Gruppe G heißt endlich erzeugt, wenn es eine endliche Teilmenge $S \subseteq G$ gibt, welches die ganze Gruppe erzeugt, also $\langle S \rangle = G$. Existiert gar eine einelementige Teilmenge $S = \{g\}$, die G erzeugt, so nennt man $G = \langle S \rangle = \{g^n | n \in \mathbb{Z}\}$ zyklisch.

3. Gruppenordnung und Elementordnung

Definition 01: **Gruppenordnung**

Mit der Ordnung $ord(G) = |G|$ einer Gruppe G bezeichnet man die Anzahl der Elemente in dieser. Ist die Anzahl endlich, so ist $ord(G) \in (N)$, ansonsten setzt man $ord(G) = \infty$

Definition 02: **Elementordnung**

Die Ordnung eines Gruppenelements $g \in G$ wird definiert als die Anzahl der Elemente in der von g erzeugten Untergruppe $\langle g \rangle = \langle \{g\} \rangle = \{g^n \mid n \in \mathbb{Z}\}$.
Offensichtlich gilt also: $ord(g) = ord(\langle g \rangle) = min\{k \in \mathbb{N} \setminus \{0\} \mid g^k = e\}$,
somit ist $ord(g)$ auch Teiler aller ganzen Zahlen k, für die $g^k = e$ gilt.

Folgende Sätze sind Folgerungen aus dem ***Satz von Lagrange***

Satz 1: **Ordnung von Untergruppen**

Sei H eine Untergruppe einer endlichen Gruppe G,
dann ist $ord(H)$ ein Teiler von $ord(G)$.

Satz 2: **Ordnung von Gruppenelementen**

Sei g ein Element einer endlichen Gruppe G, dann ist $ord(g)$ ein Teiler von $ord(G)$, da $\langle g \rangle$ eine Untergruppe von G ist. Insbesondere folgt, dass $g^{ord(G)} = e$.

Satz 3: **Gruppen mit Primzahlordnung**

Sei G eine Gruppe mit Primzahlordnung, dann besitzt G nur die beiden trivialen Untergruppen $\{e\}$ und G. Zudem erzeugt jedes Element $g \in G \setminus \{e\}$ die gesamte zyklische Gruppe, also $\langle g \rangle = G$. Insbesondere ist G somit abelsch.

4. Symmetrische und Alternierende Gruppe

Definition 01: **Symmetrische Gruppe**

Sei M eine Menge, dann ist $Sym(M) = \{f : \ M \to M \mid f \text{ bijektiv}\} \subseteq Abb(M, M)$, die Menge der bijektiven Abbildungen, mit der Komposition/Verkettung von eben diesen Abbildungen als Verknüpfung $\circ$ die sog. Symmetrische Gruppe.
Hierbei handelt es sich tatsächlich um eine Gruppe, da Kompositionen von Abbildungen stets assoziativ wirken, die Identitätsabbildung $(id : \ M \to M, \quad m \mapsto m)$ als Neutralelement dient und bijektive Abbildungen wiederum ihre bijektive Umkehrabbildungen als Inverses besitzen.

Ist die Menge $M = [n] = 1, 2, 3, ..., n$, so bezeichnet man kurz $S_n = Sym([n])$. Man nennt S_n auch Permutationsgruppe. Für ein Element $\sigma \in S_n$ kann man explizit schreiben:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Insbesondere sieht man am folgendem Beispiel, dass S_n i.A. nicht abelsch ist:

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

Definition 02: **Zykel**

Seien $i_1, i_2, \dots, i_l \in [n]$ (mit $1 \leq j \leq l$) paarweise verschieden. Dann ist der l-Zykel $\sigma \in S_n$ definiert durch

$$\sigma(x) = \begin{cases} x, & x \notin \{i_1, i_2, \dots, i_l\} \\ i_1, & x = i_l \\ i_{j+1} & x = i_j \text{ für } 1 \leq j \leq l-1 \end{cases}$$

Man schreibt solche l-Zykel-Permutation dann auch als „Tupel“ $\sigma = (i_1 i_2 \dots i_l)$.
Eine 2-Zykel-Permutation bezeichnet man auch als Transposition.

Satz 1: **Produkt disjunkter Zykel**

Jede Permutation $\sigma \in S_n$ lässt sich als Produkt von s paarweise disjunkten Zykeln $(a_{i1}, \ldots, a_{ir_i})$ schreiben, man erhält also:

$$\sigma = \prod_{i=1}^{s} (a_{i1}, \ldots, a_{ir_i})$$

Disjunkte Zykel kommutieren miteinander, deshalb kann man $r_1 \leq r_2 \leq \ldots \leq r_s$ anordnen und das Tupel $(r_1, r_2, \ldots, r_s)$ heißt dann Permutationstyp von σ.

Definition 03: **Signum**

Das Signum ist eine Abbildung (sogar ein *Gruppenhomomorphismus*), die den Permutationen $\sigma \in S_n$ einer „Parität“ aus $\{-1, 1\}$ zuordnet. Dazu betrachtet man die Folge $\sigma(1), \sigma(2), \ldots, \sigma(n)$. Ein Fehlstand in dieser Folge liegt vor, wenn für $i < j$ dennoch $\sigma(i) > \sigma(j)$ gilt $(i, j \in [n])$. Die Gesamtanzahl dieser Fehlstände über alle möglichen Paare (i, j) sei k. Dann wird das Signum wie folgt erklärt:

$$sign: \ S_n \to \{-1, 1\}, \quad \sigma \mapsto sign(\sigma) = (-1)^k$$

Das Signum kann man auch mit folgender Formel berechnen:

$$sign(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Ist die Anzahl der Fehlstände von σ gerade, also $sign(\sigma) = 1$, so nennt man die Permutation σ gerade, analog bezeichnet man die Permutation σ als ungerade, wenn $sign(\sigma) = -1$.

Satz 2: **Signum von Transpositionen**

Jede Transposition $\tau \in S_n$ ist ungerade, also $sign(\tau) = -1$

Definition 04: **Alternierende Gruppe**

Die Alternierende Gruppe A_n ist die Teilmenge der Symmetrischen Gruppe S_n, in der alle geraden Permutationen aus S_n liegen, also

$$A_n = \{\sigma \in S_n \mid sign(\sigma) = 1\} \subseteq S_n$$

Hierbei handelt es sich tatsächlich um eine Gruppe.

(Die Gruppe A_n kann auch als Kern des Gruppenhomomorphismus $sign$ erklärt werden und ist dadruch automatisch eine Untergruppe des S_n)