Definition der Kommutatorgruppe

Definition (6.6)

Sei G eine Gruppe. Für beliebige $g, h \in G$ bezeichnet man das Element $[g, h] = ghg^{-1}h^{-1}$ als den Kommutator von g und h. Bezeichnet $S = \{[g, h] \mid g, h \in G\}$ die Menge aller Kommutoren in G, so wird die Untergruppe $G' = \langle S \rangle$ die Kommutatorgruppe von G genannt.

Für alle $g, h \in G$ gilt jeweils

$$gh = [g, h]hg.$$

Die Bedeutung der Kommutatorgruppe

,

Satz (6.7)

Sei G eine Gruppe.

(i) Die Kommutatorgruppe G' ist ein Normalteiler von G.

(ii) Für einen beliebigen Normalteiler N von G gilt $N \supseteq G'$ genau dann, wenn die Faktorgruppe G/N abelsch ist.

Also ist G/G' die größte abelsche Faktorgruppe von G.

Man definiert rekursiv

- $G^{(0)} = G$
- $G^{(n+1)} = (G^{(n)})'$ für $n \in \mathbb{N}_0$

Die Untergruppen $G^{(n)}$ mit $n \geq 2$ werden die höheren Kommutatorgruppen von G genannt. Es gilt jeweils $G^{(n+1)} \trianglelefteq G^{(n)}$, und die Faktorgruppe $G^{(n)}/G^{(n+1)}$ ist abelsch.

Definition (6.8)

Eine Gruppe G wird auflösbar genannt, wenn $G^{(n)} = \{e\}$ für ein $n \in \mathbb{N}_0$ gilt.

Jede abelsche Gruppe G ist auflösbar, wegen $G^{(1)} = \{e\}$.

Definition der Subnormalreihen

Definition (6.9)

Eine Subnormalreihe für eine Gruppe G ist eine Folge von Untergruppen der Form

$$G = N_0 \supseteq N_1 \supseteq \dots \supseteq N_r = \{e\}$$

mit $r \in \mathbb{N}_0$, wobei für $0 \leq k < r$ jeweils $N_{k+1} \trianglelefteq N_k$ gilt. Die Faktorgruppen N_k/N_{k+1} bezeichnet man als Faktoren der Subnormalreihe. Sind alle Faktoren abelsch, dann spricht man von einer abelschen Subnormalreihe.

Proposition (6.10)

Jede endliche abelsche Gruppe besitzt eine Subnormalreihe mit zyklischen Faktoren von Primzahlordnung.

$\frac{\ldots}{|N_1|} = \frac{\ldots}{|N_1|} = \frac{\ldots}{(n/p)} = p$ ... Gruppe von Primzahlordnung

Beweis von Proposition 6.10

z.zg.: Jede endliche abelsche Gruppe G besitzt eine Subnormalreihe bestehend aus zyklischen Faktoren von Primzahlordnung.

Beweis durch vollst. Ind. über $n = |G|$.

Ind.-Anf. $n = 1$ Dann ist $G = \{e\}$. Hier erfüllt die Subnormalreihe $N_0 = G$ (Länge null) die Aussage.

Ind.-Schritt: Sei $n \in \mathbb{N}$, G abelsch von Ordnung n. Setze die Aussage für Gruppen der Ordnung $< n$ voraus.

Hauptsatz für endl. abelsche Gruppen $\Rightarrow \exists\, s \in \mathbb{N}$ und
$n_1, \dots, n_s > 1$, zyklische Gruppen C_j der Ordnung n_j
$(1 \le j \le s)$, so dass $G \cong C_1 \times \dots \times C_s$ ist. O.B.d.A.
gelte „$=$" statt „$\cong$". Sei p ein Primteiler von n_1 und
$g \in C_1$ ein Element mit $C_1 = \langle g \rangle$. $\operatorname{ord}(g) = n_1$, $p \mid n_1$
$\Rightarrow \operatorname{ord}(g^p) = \frac{n_1}{p}$ Setze $N_0 = G$, $N_1 = \langle g^p \rangle \times C_2 \times \dots \times C_s$
Dann ist N_1 eine abelsche Gruppe der Ordnung $\frac{n_1}{p} \cdot n_2 \cdot \ldots \cdot n_s = \frac{n}{p}$
$\frac{n}{p} < n$ Ind.-V. $\Rightarrow N_1$ besitzt eine Subnormalreihe
$N_1 \supseteq N_2 \supseteq \dots \supseteq N_r = \{e\}$, wobei N_k/N_{k+1} für $2 \le k < r$
zyklisch von Primzahlordnung. außerdem: $|N_0/N_1| = (N_0 : N_1)$
$= \frac{|N_0|}{|N_1|} = \frac{|G|}{|N_1|} = \frac{n}{(n/p)} = p$ Als Gruppe von Primzahlordnung

ist N_0/N_1 zyklisch. also: $N_0 \supseteq N_1 \supseteq \dots \supseteq N_r = \{e\}$ ist eine Subnormalreihe mit zykl. Faktoren von Primzahlordnung für G. $\square$

Auflösbarkeit und Subnormalreihen

Satz (6.11)

Für eine endliche Gruppe G sind die folgenden Eigenschaften äquivalent.

(i) Die Gruppe G ist auflösbar.

(ii) Sie besitzt eine abelsche Subnormalreihe.

(iii) Sie hat eine Subnormalreihe mit zyklischen Faktoren von Primzahlordnung.

Dabei ist die Äquivalenz „(i) $\Leftrightarrow$ (ii)“ auch für unendliche Gruppen gültig.

Beweis von Satz 6.11 (Rest)

z.zg.: Jede endliche Gruppe G, die eine abelsche Subnormalreihe besitzt, hat auch eine Subnormalreihe mit zyklischen Faktoren von Primzahlordnung.

Sei G eine endliche abelsche Gruppe und $G = N_0 \supseteq N_1 \supseteq \ldots \supseteq N_r = \{e\}$ eine abelsche Subnormalreihe. Sei $k \in \{0, \ldots, r-1\}$.
Nach Vor. gilt $N_{k+1} \trianglelefteq N_k$, und $\bar{G} = N_k / N_{k+1}$ ist eine endliche abelsche Gruppe. Prop. 6.10
$\Rightarrow$ Es existiert eine Subnormalreihe

$$\bar{G} = \bar{U}_0 \supseteq \bar{U}_1 \supseteq \dots \supseteq \bar{U}_s = \{e_{\bar{G}}\}$$

wobei jeweils $\bar{U}_{l+1} \trianglelefteq \bar{U}_l$, $\bar{U}_l / \bar{U}_{l+1}$ zyklisch von Primzahlordnung, für $0 \leq l < s$. Sei $\pi : N_k \to \bar{G}$ der kan. Epimorphismus. Dann sind $U_l = \pi^{-1}(\bar{U}_l)$ $(0 \leq l \leq s)$ Untergruppen von G, und es gilt

$$N_k = U_0 \supseteq U_1 \supseteq \dots \supseteq U_s = N_{k+1}$$

Auf Grund des Korr.-satzes gilt jeweils $U_{l+1} \trianglelefteq U_l$, und der Isom.-satz liefert $U_l / U_{l+1} \cong \bar{U}_l / \bar{U}_{l+1}$, jeweils für $0 \leq l < s$. Also ist auch U_l / U_{l+1} zyklisch von Prim-

abelsche
bnor-
zahl-

und

ue

$\ldots, r-1\}$.
N_k/N_{k+1}
rop. 6.10

zahlordnung. Fügt man nun $U_1, \ldots, U_{s-1}$ in die geg. Subnormalreihe zwischen N_k und N_{k+1} ein und verfährt so für jedes $k \in \{0, \ldots, r-1\}$, so erhält man insgesamt eine Subnormalreihe für G mit zyklischen Faktoren von Primzahlordnung. $\square$

<u>Bsp.</u> abelsche Subnormalreihe für S_4

$$S_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq \{id\}$$

Sei $C_2 = \langle (12)(34) \rangle$. Dann ist

$$S_4 \trianglerighteq A_4 \trianglerighteq V_4 \trianglerighteq C_2 \trianglerighteq \{id\}$$

eine Subnormalreihe mit zyklischen Faktoren von Primzahlordnung.

Ein weiteres Auflösbarkeitskriterium

Satz (6.12)

(i) Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.

(ii) Sei G eine Gruppe und $N \trianglelefteq G$. Unter diesen Voraussetzungen ist G auflösbar genau dann, wenn N und G/N beide auflösbar sind.

Die Auflösbarkeit der symmetrischen Gruppen

Satz (6.13)

Die Gruppen S_n und A_n sind auflösbar für $n \leq 4$, nicht auflösbar für $n \geq 5$.

Beweisskizze:

- Die Gruppe A_2 ist trivial, und A_3 ist zyklisch. Somit sind beide Gruppen auflösbar.
- Es gilt $V_4 \trianglelefteq A_4$. Daraus folgt, dass A_4 auflösbar ist.
- Für alle $n \geq 2$ ist S_n genau dann auflösbar, wenn A_n auflösbar ist, wegen $S_n/A_n \cong \{\pm 1\}$. Also ist S_n für $n \leq 4$ auflösbar.

Die Auflösbarkeit der symmetrischen Gruppen (Forts.)

- Es bleibt zu zeigen, dass A_n für $n \geq 5$ nicht auflösbar ist. Dafür wiederum genügt es zu überprüfen, dass $A_n' = A_n$ gilt.
- Weiter genügt es zu zeigen, dass A_n' alle 3-Zykel enthält (weil diese ein Erzeugendensystem von A_n bilden).
- Eine einfache Rechnung zeigt, dass jeder 3-Zykel aus Kommutator von 3-Zykeln dargestellt werden kann.

zeige: Jeder 3-Zykel in A_n $(n \geq 5)$ ist ein Kommutator von A_n

Seien $i, j, k, l, m \in M_n$ paarweise verschieden.

Sei $\sigma = (i\ j\ k)$, $\tau = (i\ l\ m)$. Dann gilt

$[\sigma, \tau] = \sigma \tau \sigma^{-1} \tau^{-1} = (i\ j\ k) \circ (i\ l\ m) \circ (i\ k\ j) \circ (i\ m\ l)$

$= (i\ j\ l)$ Da i, j, l in M_5 beliebig gewählt werden können, ist also jeder 3-Zykel ein Kommutator von A_n

Definition (7.1)

Sei G eine Gruppe und X eine Menge. Eine Gruppenoperation von G auf X ist eine Abbildung $\alpha : G \times X \longrightarrow X$ mit den Eigenschaften

$$\alpha(e_G, x) = x \qquad \text{und} \qquad \alpha(g, \alpha(h, x)) = \alpha(gh, x)$$

für alle $g, h \in G$ und $x \in X$, wobei e_G das Neutralelement der Gruppe bezeichnet.

An Stelle von $\alpha(g, x)$ verwendet man häufig auch die Infix-Schreibweise $g \cdot x$, wobei dann $\cdot$ das Symbol für die Gruppenoperation ist.

definierende Bedingungen einer Gruppen-operation $\circ : G \times X \to X$ in Infix-Schreibweise.

(i) $e_G \circ x = x \quad \forall x \in X$

(ii) $g \circ (h \circ x) = (gh) \circ x \quad \forall g, h \in G$ und $x \in X$

Beispiele für Gruppenoperationen:

(i) Für jedes $n \in \mathbb{N}$ ist eine Operation von S_n auf $M_n = \{1, 2, \dots, n\}$ geg. durch

$\circ : S_n \times M_n \to M_n, \ (\sigma, k) \mapsto \sigma(k)$

denn: Seien $\sigma, \tau \in S_n$ und $k \in M_n$. Dann gilt

$id \circ k = id(k) = k$. $\sigma \circ (\tau \circ k) = \sigma \circ (\tau(k)) =$

$\partial(\tau(k)) = (\partial \circ \tau)(k) = (\partial \circ \tau) \bullet k$

(ii) Seien $m, n \in \mathbb{N}$, K ein Körper, $G = GL_n(K)$, $X = K^n$.
Dann operiert G auf X durch $G \times X \to X$, $(A, v) \mapsto Av$.
denn: Seien $A, B \in G$ und $v \in X$. Dann gilt
$E_n \bullet v = E_n v = v$ und $A \bullet (B \bullet v) = A \bullet (Bv) = A(Bv)$
$= (AB)v = (AB) \bullet v$.

(iii) Sei K ein Körper, V ein K-Vektorraum. Dann operiert $G = K^\times$
auf $X = V$ durch $\bullet : G \times X \to X$, $(\lambda, v) \mapsto \lambda v$
denn: Seien $\lambda, \mu \in K^\times$ und $v \in V$. Dann gilt
$1_K \bullet v = 1_K v = v$ und $\lambda \bullet (\mu \bullet v) = \lambda \bullet (\mu v) = \lambda(\mu v)$
$= (\lambda \mu) v = (\lambda \mu) \bullet v$

Die Bahnen einer Gruppenoperation

Definition (7.2)

Sei G eine Gruppe, X eine Menge und $G \times X \to X$, $(g, x) \mapsto g \cdot x$ eine Gruppenoperation.

(i) Für jedes $x \in X$ nennt man $G(x) = \{g \cdot x \mid g \in G\}$ die Bahn von x.

(ii) Gibt es ein $x \in X$ mit $G(x) = X$, dann ist die Gruppenoperation transitiv.

(iii) Die Elemente $x \in X$ mit $G(x) = \{x\}$ heißen Fixpunkte der Gruppenoperation.

(iv) Eine Teilmenge $Y \subseteq X$ wird als G-invariant bezeichnet, wenn für alle $g \in G$ und $y \in Y$ auch $g \cdot y \in Y$ gilt.

Beispiele für die Bahnen einer Gruppenop.

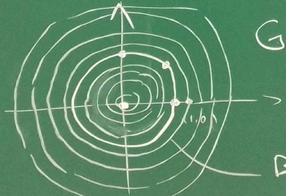
Bahn von $x \in X$: $G(x) = \{ g \cdot x \mid g \in G \}$

(1) $X = \mathbb{R}^2$, $G = SO(2) = \{ D_\alpha \mid \alpha \in \mathbb{R} \}$

wobei $D_\alpha = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$. Betrachte

die Operation $\cdot : G \times X \to X$, $(A, v) \mapsto Av$

$G((0,0)) = \{(0,0)\}$



Bahn $G((1,0))$

(2) $X = \mathbb{R}^2$, $G = GL_2(\mathbb{R})$ <u>Beh.</u>: Es gibt genau zwei Bahnen der Operation $\circ : G \times X \to X$, $(A, v) \mapsto Av$, nämlich $\{(0,0)\}$ und $\mathbb{R}^2 \setminus \{(0,0)\}$

Zeige zunächst: (i) $G((0,0)) = \{(0,0)\}$

(ii) $G((1,0)) = \mathbb{R}^2 \setminus \{(0,0)\}$

<u>zu (i)</u>

„$\supseteq$" Es gilt $E_2 \circ \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. $\Rightarrow \begin{pmatrix} 0 \\ 0 \end{pmatrix} \in G((0,0))$

„$\subseteq$" Sei $v \in G((0,0))$. $\Rightarrow \exists A \in GL_2(\mathbb{R})$ mit $v = A \circ \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$\Rightarrow v = A \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow v \in \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\}$

<u>zu (ii)</u> „$\subseteq$" Sei $v \in G((1,0))$ z.zg.: $v \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

$v \in G((1,0)) \Rightarrow \exists A \in GL_2(\mathbb{R})$ mit $A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = A \circ \begin{pmatrix} 1 \\ 0 \end{pmatrix} = v$

Ang. $v = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} = A^{-1} A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = A^{-1} v = A^{-1} \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ↯

"⊇" Sei $v \in \mathbb{R}^2 \setminus \{\binom{0}{0}\}$. zzg. $v \in G((1,0))$

gleichbed.: $\exists A \in GL_2(\mathbb{R})$ mit $A\binom{1}{0} = A \cdot \binom{1}{0} = v$

Wegen $v \neq \binom{0}{0}$ existiert ein $w \in \mathbb{R}^2$, so dass $\{v, w\}$ eine Basis von $\mathbb{R}^2$ ist. Sei A die Matrix mit den Spalten v, w. Dann gilt $A \in GL_2(\mathbb{R})$ und $A\binom{1}{0} = v$.

(3) Betrachte noch einmal die Operation von S_n auf M_n, für bel. $n \in \mathbb{N}$. Diese Operation ist transitiv, d.h. es gilt $S_n(1) = M_n$.

1. Fall: $n = 1$ $\quad 1 = id \circ 1 \in S_1(1) \Rightarrow S_1(1) = \{1\} = M_1$

2. Fall: $n \geq 2$ $\quad S_n(1) \subseteq M_n$ ist klar nach Def. der Bahn

"⊇" Sei $k \in M_n$. Fall $k = 1$: $1 = id\, 1 \in S_n(1)$

Fall $k > 1$: $(1\,k) \circ 1 = k \Rightarrow k \in S_n(1)$