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

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

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.

Höhere Kommutatorgruppen und Auflösbarkeit

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

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

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.

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.

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.

Zusatz:

Ist G ein inneres semidirektes Produkt von $U \leq G$ und $N \trianglelefteq G$, so ist G genau dann auflösbar, wenn N und U beide auflösbar sind. Dies folgt wegen $G/N = (UN)/N \cong U$ aus Satz 6.12.

Beweis von Satz 6.12

gg.: Gruppe G, $U \leq G$, $N \trianglelefteq G$

zu (i) Beh: Ist G auflösbar, dann auch U.

Für jedes $n \in \mathbb{N}_0$ gilt $U^{(n)} \leq G^{(n)}$, denn:

Die Menge der Kommutatoren von U ist enthalten in der Menge der Kommutatoren von G. Daraus folgt $U' \leq G'$.

Damit folgt $\forall n \in \mathbb{N}_0: U^{(n)} \leq G^{(n)}$ durch vollst. Ind.

Da G auflösbar ist, gilt $G^{(n)} = \{e\}$ für ein $n \in \mathbb{N}_0$.

$\underrightarrow{U^{(n)} \leq G^{(n)}}$ $U^{(n)} = \{e\}$ $\Rightarrow$ U ist auflösbar

zu (ii) z.zg.: G ist auflösbar $\iff$ $N, G/N$ sind auflösbar

„$\Rightarrow$" Die Auflösbarkeit von N folgt aus (i).

Sei $\bar{G} = G/N$ und $\pi: G \to \bar{G}$ der kanonische Epimorphismus

Beh.: $\bar{G}' = \pi(G')$

Sei $S \subseteq G$ die Menge der Kommutatoren in G und $\bar{S} \subseteq \bar{G}$ die Menge der Kommutatoren in $\bar{G}$. Dann gilt $\pi(S) = \bar{S}$, denn:

„$\subseteq$" Für jedes $[g,h] \in S$ (mit $g,h \in G$) gilt $\pi([g,h]) = \pi(ghg^{-1}h^{-1}) = \pi(g)\pi(h)\pi(g)^{-1}\pi(h)^{-1} = [\pi(g),\pi(h)] \in \bar{S}$

„$\supseteq$" Sei $[gN, hN] \in \bar{S}$, mit $g,h \in G$. Dann ist $[gN,hN] = [\pi(g),\pi(h)] \overset{\text{s.o.}}{=} \pi([g,h]) \in \pi(S)$

Daraus folgt: $\bar{S} \subseteq \pi(S) \subseteq \pi(G') \overset{\pi(G') \text{ Untergr. von } \bar{G}}{\Longrightarrow} \bar{G}' = \langle \bar{S} \rangle \subseteq \pi(G')$

ebenso: $\pi(S) \subseteq \bar{S} \Rightarrow S \subseteq \pi^{-1}(\bar{S}) \subseteq \pi^{-1}(\bar{G}')$

$\pi^{-1}(\bar{G})$ Untergruppe von G $\Rightarrow$ $G' = \langle S \rangle \subseteq \pi^{-1}(\bar{G}')$

Insgesamt erhalten wir $\pi(G') = \bar{G}'$. ($\Rightarrow$ Beh)

Durch vollst. Ind. folgt $\pi(G^{(n)}) = \bar{G}^{(n)} \quad \forall n \in \mathbb{N}_0$.

Da G auflösbar ist, gilt $G^{(n)} = \{e\}$ für ein $n \in \mathbb{N}_0 \Rightarrow \bar{G}^{(n)} = \pi(\{e\}) = \{\bar{e}\} \Rightarrow$

$\bar{G} = G/N$ ist auflösbar

„$\Leftarrow$" Vor.: G/N und N sind auflösbar $\Rightarrow$

$\exists n \in \mathbb{N}_0$ mit $\bar{G}^{(n)} = \{\bar{e}\}$ und $N^{(n)} = \{e\}$

$\bar{G}^{(n)} = \{\bar{e}\} \overset{s.o.}{\Rightarrow} \pi(G^{(n)}) = \{\bar{e}\} \Rightarrow$

$\forall g \in G^{(n)} : \pi(g) = \bar{e} \Rightarrow \forall g \in G^{(n)} : gN = N$

$\rightarrow \forall g \in G^{(n)} : g \in N \Rightarrow G^{(n)} \leq N \Rightarrow$

$G^{(2n)} = (G^{(n)})^{(n)} \leq N^{(n)} = \{e\} \Rightarrow G^{(2n)} = \{e\}$

$\Rightarrow$ G ist auflösbar. $\square$

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.

(G̅')

Beh.: Im Fall $n \geq 5$ ist jeder 3-Zyklel als Kommutator von 3-Zyklen darstellbar.

Beh)

Seien k, l, m, n, p fünf verschiedene Elemente von $\Pi_n = \{1, 2, \ldots, n\}$. Sei $\sigma = (k\ l\ m)$ und $\tau = (k\ n\ p)$. Dann ist

$$[\sigma, \tau] = \sigma \circ \tau \circ \sigma^{-1} \circ \tau^{-1} =$$

$$(k\ l\ m) \circ (k\ n\ p) \circ (m\ l\ k) \circ (p\ n\ k)$$

$$= (k\ l\ n)(m)(p) = (k\ l\ n)$$

$\in \mathbb{N}_0$.

$\Rightarrow$

e ∤

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.

Beispiele für Gruppenoperationen:

i) $G = S_n$, $X = M_n = \{1, 2, \dots, n\}$

Dann ist durch $\sigma \circ k = \sigma(k)$ eine Operation von S_n auf M_n definiert.

ii) $G = GL_2(\mathbb{R})$, $X = \mathbb{R}^2$

Dann ist $A \circ v = Av$ (Matrix-Vektor-Produkt) eine Operation von $GL_2(\mathbb{R})$ auf $\mathbb{R}^2$ definiert.

iii) K Körper, V K-Vektorraum, $G = GL(V)$ = Gruppe der bij. linearen Abb. $V \to V$, $X = V$

Dann ist $\circ$ gegeben durch $\varphi \circ v = \varphi(v)$ für $\varphi \in G$, $v \in V$ eine Operation von $GL(V)$ auf 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.

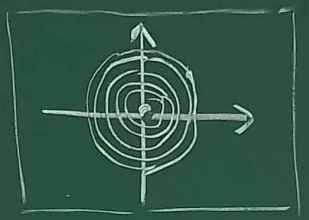
(ii) Gibt es ein $x \in X$ mit $G(x) = X$, dann ist die Gruppenoperation transitiv.

(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 Bahnen.

(i) Betrachte die Operation von $SO(2) = \left\{ \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix} \mid \alpha \in \mathbb{R} \right\}$ auf $\mathbb{R}^2$ geg durch $A \cdot v = Av$. Dann haben die Bahnen der Operation die Form



$0_{\mathbb{R}^2} = (0,0)$ ist der einzige Fixpunkt der Operation

(ii) $G = S_n \ (n \geq 2)$, $X = M_n$

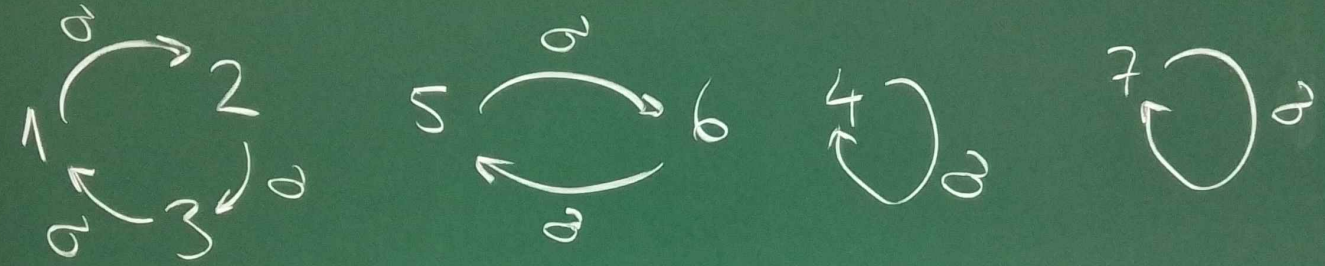
Betrachte wieder die Operation geg durch $\sigma \circ k = \sigma(k)$

Dann gilt $G(1) = X$, d.h. die Operation ist transitiv

(grund: $1 = id \circ 1 \Rightarrow 1 \in G(1)$ Für $2 \leq k \leq n$ gilt $k = (1\,k) \circ 1$ und somit ebenfalls $k \in G(1) \Rightarrow G(1) = \{1, 2, \ldots, n\} = M_n = X$)

(iii) Betrachte die Operation der Untergruppe $U = \langle \sigma \rangle \leq S_7$ mit $\sigma = (123)(56)$ auf $X = M_7$, geg durch $\tau \circ k = \tau(k)$ $\forall \tau \in U, k \in X$

Dann sind die Bahnen der Operation gegeben durch $\{1,2,3\}, \{5,6\}, \{4\}, \{7\}$.



Zerlegung einer Menge in Bahnen

Proposition (7.3)

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

(i) Die Menge $\mathcal{B} = \{G(x) \mid x \in X\}$ der Bahnen ist eine Zerlegung von X.

(ii) Eine Teilmenge $Y \subseteq X$ ist genau dann G-invariant, wenn Y eine Vereinigung von Bahnen der Operation ist.

Beweis von Proposition 7.3 (i)

z.zg.: $\mathcal{B} = \{ G(x) \mid x \in X \}$ ist eine Zerlegung der Menge X

Zu überprüfen: (i) $\emptyset \notin \mathcal{B}$ (ii) $\bigcup_{B \in \mathcal{B}} B = X$

(iii) $\forall x, y \in X : G(x) \cap G(y) \neq \emptyset \Rightarrow G(x) = G(y)$

Zu (i) Sei $B \in \mathcal{B} \Rightarrow \exists x \in X : B = G(x)$

$\Rightarrow x = e \cdot x \in G(x) \Rightarrow B \neq \emptyset$

Zu (ii) nur „$\supseteq$" zu zeigen Sei $x \in X$. $\overset{\text{s.o.}}{\Rightarrow} x \in G(x)$

Wegen $G(x) \in \mathcal{B}$ folgt $x \in \bigcup_{B \in \mathcal{B}} B$.

Zu (iii) Seien $x, y \in X$ und $z \in G(x) \cap G(y)$.

z.zg.: $G(x) = G(y)$ Beh.: $G(z) = G(x)$

(Genauso erhält man $G(z) = G(y)$, insgesamt folgt dann $G(x) = G(z) = G(y)$.)

Wegen $z \in G(x)$ gilt $z = g \circ x$ für ein $g \in G$.

„$\subseteq$" Sei $z_1 \in G(z)$. $\Rightarrow \exists\, h \in G$ mit $z_1 = h \circ z$

einsetzen $\Rightarrow z_1 = h \circ (g \circ x) = (hg) \circ x \in G(x)$

„$\supseteq$" $z = g \circ x \Rightarrow g^{-1} \circ z = g^{-1} \circ (g \circ x) = (g^{-1} g) \circ x$

$= e \circ x = x$ Sei nun $z_2 \in G(x)$. $\Rightarrow \exists\, h_2 \in G$:

$z_2 = h_2 \circ x \overset{s.o.}{=} h_2 \circ (g^{-1} \circ z) = (h_2 g^{-1}) \circ z \in G(z)$ $\square$