Definition der Untergruppen

Definition (2.3)

Sei $(G, \cdot)$ eine Gruppe. Eine Teilmenge $U \subseteq G$ wird Untergruppe von G genannt, wenn e_G in U liegt und für alle $a, b \in U$ auch die Elemente $a \cdot b$ und a^{-1} in U liegen.

Existenz und Eindeutigkeit der erzeugten Untergruppe

Satz (2.6)

Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge. Dann gibt es eine eindeutig bestimmte Untergruppe U von G mit den folgenden Eigenschaften.

(i) $U \supseteq S$

(ii) Ist V eine weitere Untergruppe von G mit $V \supseteq S$, dann folgt $V \supseteq U$.

Beide Bedingungen lassen sich zusammenfassen in der Aussage, dass U die kleinste Untergruppe von G ist, die S als Teilmenge enthält.

Definition der erzeugten Untergruppe $\langle S \rangle$

Definition (2.7)

Die Untergruppe U aus Satz (2.6) wird die von S erzeugte Untergruppe genannt und mit $\langle S \rangle$ bezeichnet. Ist V eine beliebige Untergruppe von G, dann wird jede Teilmenge T von G mit $V = \langle T \rangle$ ein Erzeugendensystem von V genannt.

Zyklische und endlich erzeugte Gruppen

Definition (2.8)

Eine Gruppe G wird zyklisch genannt, wenn ein $g \in G$ mit $G = \langle g \rangle$ existiert. Existiert eine endliche Teilmenge $S \subseteq G$ mit $G = \langle S \rangle$, dann nennt man G eine endlich erzeugte Gruppe.

Die Elemente von endlich erzeugten Untergruppen

Satz (2.9)

Sei G eine Gruppe und $S \subseteq G$ eine Teilmenge.

(i) Die Elemente von $\langle S \rangle$ sind gegeben durch

$$\langle S \rangle = \{g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r} \mid r \in \mathbb{N}_0, g_1, \ldots, g_r \in S, \varepsilon_k \in \{\pm 1\} \text{ für } 1 \leq k \leq r\}.$$

(ii) Sei S endlich, $S = \{g_1, \ldots, g_m\}$ für ein $m \in \mathbb{N}_0$, und setzen wir voraus, dass jedes Element der Menge S mit jedem anderen vertauschbar ist. Dann gilt

$$\langle S \rangle = \{g_1^{e_1} \cdot \ldots \cdot g_m^{e_m} \mid e_k \in \mathbb{Z} \text{ für } 1 \leq k \leq m\}.$$

Beweis von Satz 2.9, nur Teil (i)

Sei $U = \{ g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r} \mid r \in \mathbb{N}_0, \varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}, g_1, \ldots, g_r \in S \}$

zu überprüfen (1) $U \leq G$ (d.h. U ist Untergp. von G)

(2) $U \supseteq S$ (3) $V \leq G, V \supseteq S \Rightarrow V \supseteq U$

zu (1) z.zg. (1.1) $e_G \in U$ (1.2) $\forall g, h \in U: gh, g^{-1} \in U$

zu (1.1) Per Konvention ist e_G in G das Produkt der Länge 0,
d.h. man erhält $e_G \in U$ für $r = 0$.

zu (1.2) Seien $g, h \in U \Rightarrow \exists r, s \in \mathbb{N}_0, \varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}$,

zu (1.1) Es konvergiert (x_n) in G $\Leftrightarrow$ (x_n) ist Cauchy-Folge,

d.h. man erhält $e_G \in U$ für $r = 0$.

$\varepsilon_1, \dots, \varepsilon_s \in \{\pm 1\}$, $g_1, \dots, g_r \in S$, $h_1, \dots, h_s \in S$ mit $g = g_1^{\varepsilon_1} \circ \dots \circ g_r^{\varepsilon_r}$ und $h = h_1^{\eta_1} \circ \dots \circ h_s^{\eta_s} \Rightarrow g \cdot h = k_1^{\delta_1} \circ \dots \circ k_t^{\delta_t}$ mit $t = r + s$, $k_i = g_i$ für $1 \le i \le r$, $k_i = h_{i-r}$ für $r+1 \le i \le r+s$, $\delta_i = \varepsilon_i$ für $1 \le i \le r$, $\delta_i = \eta_{i-r}$ für $r+1 \le i \le r+s \Rightarrow gh \in U$

$g^{-1} = (g_1^{\varepsilon_1} \circ \dots \circ g_r^{\varepsilon_r})^{-1} = g_r^{-\varepsilon_r} \circ \dots \circ g_1^{-\varepsilon_1}$ (müsste streng genommen durch vollst. Ind. über r bewiesen werden) $\Rightarrow g^{-1} \in U$

(2) Sei $g \in S$. Setze $r = 1$, $g_1 = g$, $\varepsilon_1 = 1 \Rightarrow g = g_1^{\varepsilon_1}$

$\Rightarrow g \in U$

(3) zzg: Untergr. V mit $V \supseteq S$ $\Rightarrow U \subseteq V$. Sei $g \in U$.

$\Rightarrow \exists r \in \mathbb{N}_0, g_1, \dots, g_r \in S, \varepsilon_1, \dots, \varepsilon_r \in \{\pm 1\}$ mit $g = g_1^{\varepsilon_1} \circ \dots \circ g_r^{\varepsilon_r}$

Für $1 \leq i \leq s$ gilt $g_i \in V$ (wg. $S \subseteq V$).

$g_i \in V, V \leq G \Rightarrow g_i^{\varepsilon_i} \in V$, für $1 \leq i \leq s$

Aus $V \leq G$ folgt weiter $g_1^{\varepsilon_1} g_2^{\varepsilon_2} \in V$, $g_1^{\varepsilon_1} g_2^{\varepsilon_2} g_3^{\varepsilon_3} \in V$

... und schließlich $g = g_1^{\varepsilon_1} \cdot \ldots \cdot g_r^{\varepsilon_r}$. □

=

w

Zum

setz

Sei

drei

2

Zu 1.

↑. S

Zu 2.

Zyklische Gruppen

Folgerung (2.10)

(i) Ist G eine Gruppe und $g \in G$, dann gilt $\langle g \rangle = \{g^e \mid e \in \mathbb{Z}\}$.

(ii) Jede zyklische Gruppe ist abelsch.

Beweis von Folgerung 2.10

zu (i) bereits in der letzten Vl. erledigt

zu (ii) geg. zyklische Gruppe G, z.zg.: G ist abelsch

G zyklisch $\overset{(i)}{\Rightarrow} \exists g \in G$ mit $G = \langle g \rangle = \{ g^e \mid e \in \mathbb{Z} \}$

Seien nun $a, b \in G$, z.zg.: $ab = ba$

s.o. $\Rightarrow \exists e, f \in \mathbb{Z}$ mit $a = g^e$, $b = g^f$

$\Rightarrow ab = g^e \cdot g^f = g^{e+f} = g^{f+e} = g^f \cdot g^e$

$= ba.$

□

Def

ist

(Dies

von

Bsp

⇒

Bem:

Gilt s

Bew:

valenz

denn: „

„⇐" An

Erzeugendensysteme der S_n

Vorbemerkungen:

- Der Träger $\operatorname{supp}(\sigma)$ eines Elements $\sigma \in S_n$ ist die Menge aller $j \in M_n$ mit $\sigma(j) \neq j$.
- Seien $\sigma, \tau \in S_n$ mit $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \varnothing$. Dann sind die Elemente σ und τ vertauschbar, d.h. es gilt $\sigma \circ \tau = \tau \circ \sigma$.

Satz (2.11)

Sei $n \in \mathbb{N}$ beliebig.

(i) Die Transpositionen bilden ein Erzeugendensystem von S_n.

(ii) Die 3-Zykel bilden ein Erzeugendensystem von A_n.

Def Der Träger eines Elements $\sigma \in S_n$ ist definiert durch $\operatorname{supp}(\sigma) = \{ i \in M_n \mid \sigma(i) \neq i \}$.

(Dies sind genau die Elemente, die in einer Darstellung von σ als Produkt disjunkter Zykel vorkommen.

Bsp: $\sigma = (1\,2\,4)(3\,7) \in S_7$

$\Rightarrow \operatorname{supp}(\sigma) = \{1, 2, 3, 4, 7\}$.)

Bem: Sei $n \in \mathbb{N}$, und seien $\sigma, \tau \in S_n$.

Gilt $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = \emptyset$, dann gilt $\sigma \circ \tau = \tau \circ \sigma$.

Bew: Vorbem. Für jedes $k \in M_n$ gilt die Äquivalenz $k \notin \operatorname{supp}(\sigma) \iff \sigma(k) \notin \operatorname{supp}(\sigma)$

denn: „$\Rightarrow$" $k \notin \operatorname{supp}(\sigma) \Rightarrow \sigma(k) = k \Rightarrow \sigma(k) \notin \operatorname{supp}(\sigma)$

„$\Leftarrow$" Ang. $\sigma(k) \notin \operatorname{supp}(\sigma)$ und $k \in \operatorname{supp}(\sigma)$

□

$\sigma(k) \notin \mathrm{supp}(\sigma) \Rightarrow \sigma(\sigma(k)) = \sigma(k)$

$k \in \mathrm{supp}(\sigma) \Rightarrow \sigma(k) \neq k$

$\Rightarrow k$ und $\sigma(k)$ sind zwei versch. Elt., die beide auf $\sigma(k)$ abgebildet werden $\lightning$ zur Injektivität von σ

ε_3
$g_3 \in V$

$\square$

Zum Nachweis von $\sigma \circ \tau = \tau \circ \sigma$ unter der Voraussetzung $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$

Sei $i \in M_n$, z.zg.: $(\sigma \circ \tau)(i) = (\tau \circ \sigma)(i)$

drei mögl. Fälle: 1. $i \in \mathrm{supp}(\sigma)$, $i \notin \mathrm{supp}(\tau)$

2. $i \notin \mathrm{supp}(\sigma)$, $i \in \mathrm{supp}(\tau)$ 3. $i \notin \mathrm{supp}(\sigma) \cup \mathrm{supp}(\tau)$

zu 1. l.S.: $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i)$

r.S.: $(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \sigma(i)$

$\uparrow$ $i \in \mathrm{supp}(\sigma)$
s.o.
$\Rightarrow \sigma(i) \in \mathrm{supp}(\sigma)$
$\rightarrow \sigma(i) \notin \mathrm{supp}(\tau)$

zu 2. analog zu 1.

Abschluss des Nachweises von $\sigma \circ \tau = \tau \circ \sigma$
unter der Voraussetzung $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \varnothing$:

zu 3. In diesem Fall gilt $(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = i$ und ebenso $(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \tau(i) = i$.

Beweis von Satz 2.11

zu (i) Es genügt z.Zg., dass jedes Element aus S_n als Produkt von Transpositionen darstellbar ist (denn dann ist klar, das jedes $\sigma \in S_n$ in $\langle S \rangle$ liegt, wobei S die Menge der Transp. bezeichnet) Beweis durch vollst. Ind. über $|\mathrm{supp}(\sigma)|$

Ind-Anf.: $|\mathrm{supp}(\sigma)| = 0 \Rightarrow \mathrm{supp}(\sigma) = \emptyset \Rightarrow \sigma = id$

Die Identität ist Produkt von 0 Transpositionen.

Ind-Schritt: Sei $m \in \mathbb{N}_0$ und $\sigma \in S_n$ mit $|\mathrm{supp}(\sigma)| = m+1$.
Setze die Aussage für m voraus. Sei $i \in \mathrm{supp}(\sigma)$ und setze $\tau = (i\ \sigma(i)) \circ \sigma$. Dann gilt $\mathrm{supp}(\tau) \subseteq \mathrm{supp}(\sigma) \setminus \{i\}$
(denn: Sei $k \in \mathrm{supp}(\tau)$, d.h. $\tau(k) \neq k$. Da $i, \sigma(i)$ in $\mathrm{supp}(\sigma)$ liegen, folgt $k \in \mathrm{supp}(\sigma)$. Ang. $k = i$. $\Rightarrow \tau(k) = \tau(i) =$

$(i_{\sigma(i)} \circ \sigma)(i) = (i_{\sigma(i)})(\sigma(i)) = i = k$ ↯ zu $k \in \operatorname{supp}(\tau)$)

Es folgt $|\operatorname{supp}(\tau)| \leq m$ Widerspruch $\Rightarrow \exists\, \tau_1, \ldots, \tau_r$ $(r \in \mathbb{N}_0)$ mit $\tau = \tau_1 \circ \ldots \circ \tau_r$ $\Rightarrow \sigma = (i_{\sigma(i)})^{-1} \circ \tau = (i_{\sigma(i)}) \circ \tau_1 \circ \ldots \circ \tau_r$, d.h. σ ist Produkt von Transp.

zu (ii) siehe Skript

Zweielementige Erzeugendensysteme von S_n

Proposition (2.12)

Für jedes $n \in \mathbb{N}$ ist die Menge $\{\sigma, \tau\}$ bestehend aus den beiden Elementen $\sigma = (1\ 2\ \ldots\ n)$ und $\tau = (1\ 2)$ ein Erzeugendensystem von S_n. Ist n eine ungerade Primzahl, dann wird S_n sogar von jeder zweielementigen Menge bestehend aus einem n-Zykel und einer Transposition erzeugt.

Beweis von Prop. 2.12. zur 1. Teilaussage

z.zg. $S_n = \langle \sigma, \tau \rangle$, wobei $\sigma = (1\,2 \ldots n)$, $\tau = (1\,2)$

$= \langle (1\,0), \tau \rangle$

wichtige allgemeine Rechenregel: Für jedes $\rho \in S_n$ und jede k-elem. Teilmenge $\{a_1, \ldots, a_k\} \subseteq M_n$ $(2 \leq k \leq n)$ gilt $\rho \circ (a_1\, a_2 \ldots a_k) \circ \rho^{-1} = (\rho(a_1) \ldots \rho(a_k))$

Die analoge Regel gilt auch für Elemente, die aus mehreren Zyklen zusammengesetzt sind, z.B.

$\rho \circ (1\,2\,3) \circ (4\,5) \circ \rho^{-1} = (\rho(1)\, \rho(2)\, \rho(3)) \circ (\rho(4)\, \rho(5))$

$\dots = (p(a_1) \dots p(a_k))$

Die analoge Regel gilt auch für Elemente, die aus

Anwendung auf die Elemente σ, τ von oben $\rightarrow$

$\sigma \circ \tau \circ \sigma^{-1} = (\sigma(1)\ \sigma(2)) = (2\ 3)$

$\sigma^2 \circ \tau \circ \sigma^{-2} = (3\ 4)$, allgem. $\sigma^{k-1} \circ \tau \circ \sigma^{1-k} = (k\ k+1)$

für $1 \leq k \leq n-1$

$[(1\,2), (2\,3), (3\,4) \dots (n-1\ n) \in \langle \sigma, \tau \rangle]$

weiter: $(2\ 3) \circ (1\ 2) \circ (2\ 3)^{-1} = (1\ 3)$

$(3\ 4) \circ (1\ 3) \circ (3\ 4)^{-1} = (1\ 4)$

Insgesamt erhält man durch Konjugation der Transp. der Form $(k\ k+1)$ mit anderen Transpositionen jede Transposition aus S_n (Details siehe Skript) $\rightarrow$ Die Menge S der Transp. von S_n ist in $\langle \sigma, \tau \rangle$ enthalten. $\langle \sigma, \tau \rangle \leq S_n$, $S \subseteq \langle \sigma, \tau \rangle \rightarrow \langle S \rangle \leq \langle \sigma, \tau \rangle$

Prop. 2.11(1) $\Rightarrow S_n \leq \langle \sigma, \tau \rangle \Rightarrow S_n = \langle \sigma, \tau \rangle$

Links- und Rechtsnebenklassen einer Untergruppe

Definition (2.13)

Sei $(G, \cdot)$ eine Gruppe und U eine Untergruppe. Eine Teilmenge von G, die mit einem geeigneten $g \in G$ in der Form

$$gU \quad = \quad \{gu \mid u \in U\}$$

geschrieben werden kann, wird Linksnebenklasse von U genannt. Ebenso bezeichnet man die Teilmengen der Form $Ug = \{ug \mid u \in U\}$ mit $g \in G$ als Rechtsnebenklassen von U.

Im Folgenden bezeichnet G/U für die Menge der Links- und $U\backslash G$ die Menge der Rechtsnebenklassen von U.