

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.

Beispiele für Erzeugendensysteme

(i) $G = (\mathbb{Z}, +)$ Beh. $S = \{1\}, T = \{-1\}$ sind Erzeugendensysteme von G , d.h. $G = \langle S \rangle = \langle T \rangle$

klar: G ist Untergruppe von G , $G \supseteq S$ und $G \supseteq T$

Sei V eine bel. Untergruppe von G mit $V \supseteq S$.

z.zg. $V \supseteq G$ Sei $a \in G$, zu überprüfen: $a \in V$

$$V \supseteq S \Rightarrow 1 \in V \Rightarrow a \cdot 1 \in V \Rightarrow a \in V$$

Sei nun V eine bel. Untergruppe von G mit $V \supseteq T$

z.zg. $V \supseteq G$ Sei $a \in G$, zu überprüfen: $a \in V$

$$V \supseteq T \Rightarrow -1 \in V \Rightarrow (-a) \cdot (-1) \in V \Rightarrow a \in V$$

Sei Untergruppe von G mit $V \neq \{$
z.zg. $V \geq G$ Sei $a \in G$, zu überprüfen: $a \in V$

iii) $G = (\mathbb{Z}, +)$ Beh. $S_1 = \{2, 3\}$ ist Erzeugendensystem
von G , d.h. es gilt $G = \langle S_1 \rangle$

klar: G ist Untergr. von G , $G \geq S_1$

Sei V eine Untergr. von G mit $V \geq S_1$, z.zg. $V \geq G$

Sei $a \in G$, überprüfe: $a \in V$

$$\begin{array}{l} S_1 \subseteq V \Rightarrow 2, 3 \in V \xrightarrow[\text{von } G]{V \text{ Untergr.}} 3 + (-2) = 1 \in V \\ \xrightarrow[\text{von } G]{V \text{ Untergr.}} a \cdot 1 \in V \Rightarrow a \in V \end{array}$$

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.

Satz (2.9)

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

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

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

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

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

Beweis von Satz 2.9, nur (ii)

geg. Gruppe G , $S = \{g_1, \dots, g_m\} \subseteq G$

mit $m \in \mathbb{N}$, es gilt $g_i g_j = g_j g_i$

$\forall i, j \in \{1, \dots, m\}$

Beh. $\langle S \rangle = \{g_1^{e_1} \cdot \dots \cdot g_m^{e_m} \mid e_1, \dots, e_m \in \mathbb{Z}\}$

Bezeichne die Menge auf der rechten Seite der Gleichung mit U , zu überprüfen:

(1) U ist Untergruppe von G

(2) $U \supseteq S$

(3) Ist V eine beliebige Untergr. von G
mit $V \geq S$, dann folgt $V \geq U$.

zu (1) überprüfe (1.1) $e_G \in U$

(1.2) $\forall a, b \in U: ab \in U, a^{-1} \in U$

zu (1.1) klar, da $e_G = g_1^0 \cdot \dots \cdot g_m^0$

zu (1.2) Seien $a, b \in U \Rightarrow \exists e_j, f_j \in \mathbb{Z}$

für $1 \leq j \leq m$ mit $a = g_1^{e_1} \cdot \dots \cdot g_m^{e_m}$ und

$b = g_1^{f_1} \cdot \dots \cdot g_m^{f_m} \Rightarrow ab = (g_1^{e_1} \cdot \dots \cdot g_m^{e_m}) \cdot$

$(g_1^{f_1} \cdot \dots \cdot g_m^{f_m}) = g_1^{e_1+f_1} \cdot \dots \cdot g_m^{e_m+f_m} \Rightarrow ab \in U$

$\uparrow$ g_j vertauschen
 $a^{-1} = (g_1^{e_1} \cdot \dots \cdot g_m^{e_m})^{-1} = (g_m^{e_m})^{-1} \cdot \dots \cdot (g_1^{e_1})^{-1}$

$$= g_m^{-e_m} \cdot \dots \cdot g_1^{-e_1} = g_1^{-e_1} \cdot \dots \cdot g_m^{-e_m} \in U$$

↑ Vertauschbarkeit

zu (2) Sei $j \in \{1, \dots, m\}$. Definiere $e_j = 1$ und $e_i = 0$ für $i \in \{1, \dots, m\} \setminus \{j\}$. Dann gilt $g_j = g_1^{e_1} \cdot \dots \cdot g_m^{e_m} \Rightarrow g_j \in U$

zu (3) Sei V eine beliebige Untergr. von G

mit $V \supseteq S$. z.zg. $V \supseteq U$. Sei $a \in U$, z.zg.

$a \in V$ $a \in U \Rightarrow \exists e_1, \dots, e_m \in \mathbb{Z}$ mit $a = g_1^{e_1} \cdot \dots \cdot g_m^{e_m}$

$S \subseteq V \Rightarrow g_1, \dots, g_m \in V \xrightarrow[V \text{ Untergr. von } G]{V \text{ Untergr.}} g_1^{e_1} \cdot \dots \cdot g_m^{e_m} \in V$

$\xrightarrow[V \text{ Untergr.}]{V \text{ Untergr. von } G} g_1^{e_1} \cdot \dots \cdot g_m^{e_m} \in V \Rightarrow a \in V$ □

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.

Vorbemerkungen:

- Der **Träger** $\text{supp}(\sigma)$ 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 $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$. 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 .

Beweis von Satz 2.11, nur (ii)

Sei $T \in S_n$ die Menge der 3-Zykel in S_n .

Beh. $A_n = \langle T \rangle$ zu überprüfen:

(1) A_n ist Untergr. von S_n (ist bekannt)

(2) $A_n \geq T$

(3) Ist V eine bel. Untergr. von S_n mit $V \geq T$,
dann folgt $V \geq A_n$

zu (2) Da 3 ungerade, hat jedes 3-Zykel positives
Signum $\Rightarrow T \subseteq A_n$

(3) Ist V eine bel. Unterg. von S_n mit $V \supseteq T$,
dann folgt $V \supseteq A_n$.

zu (3) Sei V Unterg. von S_n mit $V \supseteq T$. Sei $\sigma \in A_n$.
z.zg. $\sigma \in V$. Es reicht z.zg., dass σ Produkt von
3-Zykeln ist, dann die 3-Zykel liegen wegen $T \subseteq V$
alle in V , somit auf Grund der Unterg.eigenschaft
von V auch σ als Produkt von 3-Zykeln.

Teil (i) $\rightarrow \sigma$ kann als Produkt $\tau_1 \circ \dots \circ \tau_r$ von Transpositionen
 $\tau_i \in S_n$ dargestellt werden. bekannt: $\text{sgn}(\tau_i) = -1 \quad \forall i$
 $\Rightarrow \text{sgn}(\sigma) = (-1)^r \quad \sigma \in A_n \Rightarrow \text{sgn}(\sigma) = 1$

Also muss r gerade sein. Es reicht somit zu zeigen, dass
jedes Produkt von zwei Transpositionen als Produkt von
3-Zykeln dargestellt werden kann.

Seien also $\tau, \tau' \in S_n$ Transpositionen

1. Fall: $|\text{supp}(\tau) \cap \text{supp}(\tau')| = 2$

$\Rightarrow \exists i, j \in M_n, i \neq j$ mit $\tau = \tau' = (i j)$

$\Rightarrow \tau \circ \tau' = (i j) \circ (i j) = \text{id}$

$\Rightarrow \tau \circ \tau'$ ist Produkt von null 3-Zykeln

2. Fall: $|\text{supp}(\tau) \cap \text{supp}(\tau')| = 1$

$\Rightarrow \exists i, j, k \in M_n$, alle verschieden, mit

$\tau = (i j), \tau' = (i k) \Rightarrow \tau \circ \tau' =$

$(i j) \circ (i k) = (i k j)$

$\Rightarrow \tau \circ \tau'$ ist 3-Zykel

3. Fall: $|\text{supp}(\tau) \cap \text{supp}(\tau')| = 0$

Seien $i, j, k, l \in M_n$, alle verschieden,
mit $\tau = (i j)$, $\tau' = (k l)$. Dann gilt

$$(i k j) \circ (i k l) = (i j)(k l)$$

$\Rightarrow \tau \circ \tau'$ ist Produkt von zwei 3-Zyklen.



Seien $\sigma, \tau \in S_n$ ($n \in \mathbb{N}$) mit
 $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$.

z.zg.: $\sigma \circ \tau = \tau \circ \sigma$

Vorbereitung: Ist $i \in \text{supp}(\sigma)$, dann gilt
auch $\sigma(i) \in \text{supp}(\sigma)$.

denn: Ang. $i \in \text{supp}(\sigma)$, $\sigma(i) \notin \text{supp}(\sigma)$

$$i \in \text{supp}(\sigma) \Rightarrow \sigma(i) \neq i$$

$$\sigma(i) \notin \text{supp}(\sigma) \Rightarrow \sigma(\sigma(i)) = \sigma(i), \text{ aber}$$

$$\sigma(i) \neq i \quad \Downarrow \text{ zur Injektivität von } \sigma$$

Nachweis von $\sigma \circ \tau = \tau \circ \sigma$

Sei $k \in M_n$ zu überprüfen: $(\sigma \circ \tau)(k) = (\tau \circ \sigma)(k)$

1 Fall: $k \notin \text{supp}(\sigma)$, $k \notin \text{supp}(\tau)$

Dann gilt $(\sigma \circ \tau)(k) = \sigma(k) = k$ und

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

2 Fall: $k \in \text{supp}(\sigma)$, $k \notin \text{supp}(\tau)$

Dann gilt $(\sigma \circ \tau)(k) = \sigma(k)$ und

$(\tau \circ \sigma)(k) = \sigma(k)$, denn: Ang. $\sigma(k) \in \text{supp}(\tau)^{(*)}$

3. Fall: $k \in \text{supp}(\sigma)$, $k \in \text{supp}(\tau)$ ausgeschlossen
wegen $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$ (**)

(*) denn sonst läge (Voraussetzung) $\sigma(k)$ in $\text{supp}(\sigma)$ und
 $\text{supp}(\tau) \nrightarrow$ zu (**)

Zweielementige Erzeugendensysteme von S_n

Proposition (2.12)

Für jedes $n \in \mathbb{N}$ ist die Menge $\{\sigma, \tau\}$ bestehend aus den beiden Elementen $\sigma = (1\ 2\ \dots\ n)$ 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.

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

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

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 .

Beispiel für eine Zerlegung einer Gruppe in die Linksnebenklassen einer Untergruppe

$$G = S_3 = \{ \text{id}, (12), (13), (23), (123), (132) \}$$

$$U = \langle (12) \rangle = \{ \text{id}, (12) \}$$

Linksnebenklassen von U in G :

$$\text{id} \circ U = \{ \text{id} \circ \text{id}, \text{id} \circ (12) \} = \{ \text{id}, (12) \}$$

$$(12) \circ U = \{ (12) \circ \text{id}, (12) \circ (12) \} = \{ (12), \text{id} \}$$

$$(13) \circ U = \{ (13) \circ \text{id}, (13) \circ (12) \} = \{ (13), (123) \}$$

$$(23) \circ U = \{(23) \circ \text{id}, (23) \circ (12)\} = \{(23), (132)\}$$

$$(123) \circ U = \{(123) \circ \text{id}, (123) \circ (12)\} = \{(123), (13)\}$$

$$(132) \circ U = \{(132), (23)\}$$

Menge der Linksnebenklassen insgesamt:

$$\{\text{id}, (12)\}, \{(123), (13)\}, \{(132), (23)\}$$

ebenso überprüft man: Die Menge der Rechtsnebenklassen der Form $U \circ \sigma, \sigma \in S_3$ ist gegeben durch

$$\{\text{id}, (12)\}, \{(123), (23)\}, \{(132), (13)\}$$

Lemma (2.14)

Sei G eine Gruppe, U eine Untergruppe von G und $g \in G$ ein beliebiges Element. Dann sind die Abbildungen

$$\tau_g^\ell : U \rightarrow gU, \quad h \mapsto gh \quad \text{und} \quad \tau_g^r : U \rightarrow Ug, \quad h \mapsto hg$$

jeweils bijektiv. Ist U endlich, dann gilt also $|U| = |gU| = |Ug|$ für alle $g \in G$.

Beweis von Lemma 2.14, nur (i).

geg. G Gruppe, U Untergruppe, $g \in G$

Ziel: Nachweis der Bijektivität von

$$\tau_g^l: U \rightarrow gU, h \mapsto gh$$

(1) Injektivität: Seien $h, h' \in U$ mit $\tau_g^l(h) = \tau_g^l(h')$
 $\Rightarrow gh = gh' \Rightarrow g^{-1}gh = g^{-1}gh' \Rightarrow eh = eh'$
 $\Rightarrow h = h'$

(2) Surjektivität: Sei $k \in gU \Rightarrow \exists h \in U$ mit $k = gh$
 $\Rightarrow k = \tau_g^l(h)$ □