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.

Wie in § 1 ausgeführt, erhält man somit durch Einschränkung eine Verknüpfung $\cdot_U$ auf U.

Proposition (2.4)

Das Paar $(U, \cdot_U)$ ist eine Gruppe.

Existenz und Eindeutigkeit der erzeugten Untergruppe

Proposition (2.5)

Sei $(G, \cdot)$ eine Gruppe, und sei $(U_i)_{i \in I}$ eine Familie von Untergruppen von G. Dann ist auch $U = \bigcap_{i \in I} U_i$ eine Untergruppe von G.

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

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

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.

Sei $k \in M_n$. z.zg. $(\sigma \circ \tau)(k) = (\tau \circ \sigma)(k)$

Beweis von Folgerung 2.10 (ii)

Sei G eine zyklische Gruppe z.zg: G ist abelsch

Seien $a, b \in G$. z.zg: $a \cdot b = b \cdot a$

G zyklisch $\Rightarrow \exists g \in G$ mit $G = \langle g \rangle \overset{2.10\,(i)}{=} \{g^e \mid e \in \mathbb{Z}\}$

$a, b \in G \Rightarrow \exists e, e' \in \mathbb{Z}$ mit $a = g^e$, $b = g^{e'}$

$\Rightarrow a \cdot b = g^e \cdot g^{e'} = g^{e+e'} = g^{e'+e} = g^{e'} \cdot g^e = b \cdot a$ $\square$

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.

Bem: Sind $\sigma, \tau \in S_n$ mit $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$, dann gilt $\sigma \circ \tau = \tau \circ \sigma$

Vorweg: Ist $\sigma \in S_n$ und $k \in M_n$, dann gilt

$$k \in \mathrm{supp}(\sigma) \iff \sigma(k) \in \mathrm{supp}(\sigma)$$

„$\Rightarrow$" Ang. $k \in \mathrm{supp}(\sigma)$ und $\sigma(k) \notin \mathrm{supp}(\sigma)$ $\Rightarrow$
$\sigma(k) \neq k$ und $\sigma(\sigma(k)) = \sigma(k) \Rightarrow k$ und $\sigma(k)$ werden beide auf $\sigma(k)$ abgebildet, und $\sigma(k) \neq k$ $\lightning$ zur Injektivität

„$\Leftarrow$" Ang $\sigma(k) \in \mathrm{supp}(\sigma)$, aber $k \notin \mathrm{supp}(\sigma)$.
Das ist unmöglich, da $\sigma(k) = k$ wegen $k \notin \mathrm{supp}(\sigma)$ gilt.

Seien nun $\sigma, \tau \in S_n$ mit $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$
Sei $k \in M_n$. z.zg.: $(\sigma \circ \tau)(k) = (\tau \circ \sigma)(k)$

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

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

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

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

$(\tau \circ \sigma)(k) = \tau(k)$ (mit $k \notin \mathrm{supp}(\sigma)$)

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

3. Fall: $k \in \mathrm{supp}(\sigma)$, $k \notin \mathrm{supp}(\tau)$

4. Fall: $k \in \mathrm{supp}(\sigma)$, $k \in \mathrm{supp}(\tau)$

ist ausgeschlossen, da $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \emptyset$

Beweis von Satz 2.11

zu (i) Sei $T \subseteq S_n$ die Menge der Transpositionen ($=2$-Zykel) in S_n. z.zg.: $S_n = \langle T \rangle$

Überprüfe: S_n besitzt die definierenden Eigenschaften von $\langle T \rangle$, im Einzelnen

(1) S_n ist Untergruppe von S_n (klar)

(2) $S_n \supseteq T$ (klar)

(3) Sei U eine bel. Untergruppe von S_n mit $U \supseteq T$. Dann folgt $U \supseteq S_n$ (äquivalent: $U = S_n$).

genügt z.zg.: Jedes $\sigma \in S_n$ kann als Produkt von Transpositionen geschrieben

werden. (Wegen $U \supseteq T$ enthält U dann auch alle Produkte von Transpositionen aus der zu zeigenden Aussage folgt damit $U \supseteq S_n$)

Sei $\sigma \in S_n$. Beweise die Aussage durch vollst. Induktion über $m = |\mathrm{supp}(\sigma)|$.

Ind.-Anf. $m = 0$: Vor.: $|\mathrm{supp}(\sigma)| = 0$

$\Rightarrow \mathrm{supp}(\sigma) = \emptyset \Rightarrow \sigma = id$

$\Rightarrow \sigma$ ist Produkt von null Transpositionen.

Ind.-Schritt: Sei $m \in \mathbb{N}$. Setze die Aussage für m voraus. Ann.: $|\mathrm{supp}(\sigma)| = m+1 \Rightarrow \mathrm{supp}(\sigma) \neq \emptyset$

$\exists\, i \in \mathrm{supp}(\sigma)$. Setze $\tau = (i\ \sigma(i)) \circ \sigma$

Sei $\sigma \in S_n$. Beweise die Aussage durch

Beh.: $\mathrm{supp}(\tau) \subseteq \mathrm{supp}(\sigma) \setminus \{i\}$

Sei $k \in \mathrm{supp}(\tau)$. Ang. $k \notin \mathrm{supp}(\sigma)$

$\Rightarrow k \notin \{i, \sigma(i)\}$ (denn s.o. $\Rightarrow \sigma(i) \in \mathrm{supp}(\sigma)$)

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

$= k \Rightarrow k \notin \mathrm{supp}(\tau)$ ↯ zur Vor.

also: $\mathrm{supp}(\tau) \subseteq \mathrm{supp}(\sigma)$

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

$= i \Rightarrow i \notin \mathrm{supp}(\tau)$

also: $\mathrm{supp}(\tau) \subseteq \mathrm{supp}(\sigma) \setminus \{i\}$.

Aus der Beh. folgt $|\mathrm{supp}(\tau)| \leq |\mathrm{supp}(\sigma)| - 1$

$= (m+1) - 1 = m \Rightarrow$ Ind.-V. anwendbar auf

$\tau \Rightarrow \exists r \in \mathbb{N}_0$, Transp. $\tau_1, \dots, \tau_r \in T$ mit

$\tau = \tau_1 \circ \dots \circ \tau_r$. $\tau = (i \; \sigma(i)) \circ \sigma \Rightarrow$

$\sigma = (i \; \sigma(i))^{-1} \circ \tau = (i \; \sigma(i)) \circ \tau_1 \circ \dots \circ \tau_r$

$\leftarrow (i \; \sigma(i))^2 = id$

$\Rightarrow \sigma$ ist darstellbar als Produkt von Transpositionen.

zu (ii) Sei D die Menge der 3-Zyklen in S_n

Beh: $\langle D \rangle = A_n$

zu überprüfen: (1) A_n ist Untergr. von S_n (bekannt)

(2) $A_n \supseteq D$

(3) U Untergr. von S_n mit $U \supseteq D \Rightarrow U \supseteq A_n$

zu (2) bekannt: σ k-Zyklus $\Rightarrow \operatorname{sgn}(\sigma) = (-1)^{k-1}$

insbesondere also: $\sigma \in D \Rightarrow \operatorname{sgn}(\sigma) = (-1)^{3-1} = +1$

$\Rightarrow \sigma \in A_n$

zu (3) genügt z.Zg.: Jedes $\sigma \in A_n$ ist Produkt von 3-Zyklen (denn U enthält all diese Produkte) Sei $\sigma \in A_n$.

Teil (i) $\Rightarrow \exists$ Transp. $\tau_1, \dots, \tau_r$ mit $\sigma = \tau_1 \circ \dots \circ \tau_r$

$+1 = \operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1) \cdot \dots \operatorname{sgn}(\tau_r) = (-1)^r \Rightarrow r$ ist gerade

Es genügt somit zu zeigen: Jedes Produkt von zwei Transpositionen ist Produkt von 3-Zyklen. $(*)$ $i \neq j$, $k \neq l$

Seien $i, j, k, l \in M_n$ $^{(*)}$ zeige: $(ij) \circ (kl)$ ist Produkt v. 3-Zyklen

1. Fall: $\{i, j\} \cap \{k, l\} = \emptyset$ dann gilt $(ij) \circ (kl) = (ikj) \circ (ikl)$

2. Fall: $\{i, j\} \cap \{k, l\}$ ist einelementig, o.B.d.A. $j = l$

$\Rightarrow (ij) \circ (kl) = (ij) \circ (kj) = (ijk)$

3. Fall: $\{i, j\} = \{k, l\} \Rightarrow (ij) \circ (kl) = (ij) \circ (ij) = \mathrm{id}$ □

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.

Zum Beweis von Prop. 2.12, erster Teil.

Beh: $S_n = \langle \sigma, \tau \rangle$, wobei $\sigma = (1\,2\,\dots\,n)$, $\tau = (1\,2)$.

Es reicht zu zeigen, dass $\langle \sigma, \tau \rangle$ alle Transpositionen enthält; denn dann folgt $S_n = \langle \sigma, \tau \rangle$ aus Prop. 2.11. Vorrende dafür die Rechenregel

$$\rho \circ (1\,2) \circ \rho^{-1} = (\rho(1)\ \rho(2)) \quad \forall\, \rho \in S_n.$$

$$\sigma \circ (1\,2) \circ \sigma^{-1} = (\sigma(1)\ \sigma(2)) = (2\,3) \in \langle \sigma, \tau \rangle$$

$$\sigma^2 \circ (1\,2) \circ \sigma^{-2} = (\sigma^2(1)\ \sigma^2(2)) = (3\,4) \in \langle \sigma, \tau \rangle$$

$$(2\,3) \circ (1\,2) \circ (2\,3)^{-1} = (1\,3) \in \langle \sigma, \tau \rangle$$

Rest siehe Skript. □

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.

Beispiel für eine Zerlegung einer Gruppe in die Linksnebenklassen einer Untergruppe

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

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

Linksnebenklassen:

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

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

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

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

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

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

$\Rightarrow S_3/U = \{\{id, (12)\}, \{(13), (123)\}, \{(23), (132)\}\}$

Für die Menge der Rechtsnebenklassen von U gilt $U \backslash S_3 = \{\{id, (12)\}, \{(13), (132)\}, \{(23), (123)\}\}$

Gleichmächtigkeit der Linksnebenklassen

Lemma (2.14)

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

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

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

Beweis von Lemma 2.14:

geg.: Gruppe G, Untergruppe $U \leq G$ und $g \in G$.

Beh.: Die Abbildung $\tau_g^l : U \to G$, $u \mapsto gu$ definiert eine Bijektion zwischen U und $gU = \{gu \mid u \in U\}$. Überprüfe:

(1) $\tau_g^l(U) \subseteq gU$ (d.h. τ_g^l ist Abb. $U \to gU$)

(2) τ_g^l ist injektiv

(3) τ_g^l ist (als Abb. $U \to gU$) surjektiv.

zu (1) Sei $u \in U \Rightarrow \tau_g^l(u) = gu \in gU$.

zu (2) Seien $u, v \in U$ mit $\tau_g^l(u) = \tau_g^l(v)$

$\Rightarrow gu = gv \Rightarrow g^{-1}gu = g^{-1}gv \Rightarrow$

$eu = ev \Rightarrow u = v$

zu (3) Sei $h \in gU \Rightarrow \exists u \in U$ mit $h = gu$

$\Rightarrow \tau_g^l(u) = gu = h.$ □