Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 8

Homomorphie- und Isomorphiesatz

Satz 1. *(Homomorphiesatz) Seien G, Q und H Gruppen, es sei $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus und $\psi : G \longrightarrow Q$ ein surjektiver Gruppenhomomorphismus. Es sei vorausgesetzt, dass*

$$\ker \psi \subseteq \ker \varphi$$

ist. Dann gibt es einen eindeutig bestimmten Gruppenhomomorphismus

$$\tilde{\varphi} : Q \longrightarrow H$$

derart, dass $\varphi = \tilde{\varphi} \circ \psi$ ist. Mit anderen Worten: das Diagramm

$$\begin{array}{ccc} G & \longrightarrow & Q \\ & \searrow & \downarrow \\ & & H \end{array}$$

ist kommutativ.

Beweis. Für jedes Element $u \in Q$ gibt es mindestens ein $g \in G$ mit $\psi(g) = u$. Wegen der Kommutativität muss

$$\tilde{\varphi}(u) = \varphi(g)$$

gelten. Das bedeutet, dass es maximal ein $\tilde{\varphi}$ geben kann. Wir haben zu zeigen, dass durch diese Bedingung eine wohldefinierte Abbildung gegeben ist. Seien also $g, g' \in G$ zwei Urbilder von u. Dann ist

$$g'g^{-1} \in \ker \psi \subseteq \ker \varphi$$

und daher ist $\varphi(g) = \varphi(g')$. Die Abbildung ist also wohldefiniert. Wegen $\tilde{\varphi}(e_Q) = \varphi(e_G) = e_H$ geht das neutrale Element auf das neutrale Element. Seien $u, v \in Q$ und seien $g, h \in G$ Urbilder davon. Dann ist gh ein Urbild von uv und daher ist

$$\tilde{\varphi}(uv) = \varphi(gh) = \varphi(g)\varphi(h) = \tilde{\varphi}(u)\tilde{\varphi}(v) .$$

D.h. φ ist ein Gruppenhomomorphismus. □

Die im vorstehenden Satz konstruierte Abbildung heißt *induzierte Abbildung* oder *induzierter Homomorphismus* und entsprechend heißt der Satz auch *Satz vom induzierten Homomorphismus*.

Korollar 2. *Seien G und H Gruppen und sei $\varphi : G \longrightarrow H$ ein surjektiver Gruppenhomomorphismus. Dann gibt es eine kanonische Isomorphie*

$$\tilde{\varphi} : G/\ker \varphi \longrightarrow H .$$

Beweis. Wir wenden Satz 8.1 auf $Q = G/\ker\varphi$ und die kanonische Projektion $q : G \longrightarrow G/\ker\varphi$ an. Dies induziert einen Gruppenhomomorphismus

$$\tilde{\varphi} : G/\ker\varphi \longrightarrow H$$

mit $\varphi = q \circ \tilde{\varphi}$, der surjektiv ist. Sei $[x] \in G/\ker\varphi$ und $[x] \in \ker\tilde{\varphi}$. Dann ist

$$\tilde{\varphi}([x]) = \varphi(x) = e_H\,,$$

also $x \in \ker\varphi$. Damit ist $[x] = e_Q$, d.h. der Kern von $\tilde{\varphi}$ ist trivial und nach Lemma 5.11 ist $\tilde{\varphi}$ auch injektiv. □

Satz 3. *Seien G und H Gruppen und sei $\varphi : G \longrightarrow H$ ein Gruppenhomomorphismus. Dann gibt es eine kanonische Faktorisierung*

$$G \xrightarrow{q} G/\ker\varphi \xrightarrow{\theta} U \xhookrightarrow{\iota} H\,,$$

wobei q die kanonische Projektion, θ ein Gruppenisomorphismus und U eine Untergruppe von H ist.

Beweis. Dies folgt aus Korollar 8.2 angewandt auf die Bildgruppe $U = \operatorname{bild}\varphi \subseteq H$. □

Satz 4. *(Isomorphiesatz für Restklassengruppen) Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler mit der Restklassengruppe $Q = G/N$. Es sei $H \subseteq G$ eine weiterer Normalteiler in G, der N umfasst. Dann ist das Bild $\overline{H}$ von H in Q ein Normalteiler und es gilt die kanonische Isomorphie*

$$G/H \cong Q/\overline{H}\,.$$

Beweis. Für die erste Aussage siehe Aufgabe 7.7. Damit ist die Restklassengruppe $Q/\overline{H}$ wohldefiniert. Wir betrachten die Komposition

$$q \circ \theta : G \longrightarrow Q \longrightarrow Q/\overline{H}\,.$$

Wegen

$$\begin{aligned}\ker q \circ \theta &= \{x \in G :\ q \circ \theta(x) = e\}\\ &= \{x \in G :\ q(x) = xN \in \ker\theta\}\\ &= \{x \in G :\ xN \in \overline{H}\}\\ &= \{x \in G :\ xH \in \overline{H}\}\\ &= H\end{aligned}$$

ist $\ker q \circ \theta = H$. Daher ergibt Korollar 8.2 die kanonische Isomorphie

$$G/H \longrightarrow Q/\overline{H}.$$

□

Kurz gesagt ist also

$$G/H = (G/N)/(H/N)\,.$$

Permutationsgruppen

Seien M_1, M_2, M_3, M_4 Mengen und es seien Abbildungen

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} M_3 \xrightarrow{\varphi_3} M_4$$

gegeben. Dann ist es egal, ob man die Hintereinanderschaltung der drei Abbildungen als $\varphi_3 \circ (\varphi_2 \circ \varphi_1)$ oder als $(\varphi_3 \circ \varphi_2) \circ \varphi_1$ auffasst. Das ist die natürliche Assoziativität für Abbildungen.

Definition 5. Sei M eine beliebige Menge. Dann ist die Menge

$$\mathrm{Abb}\,(M) = \mathrm{Abb}\,(M, M)$$

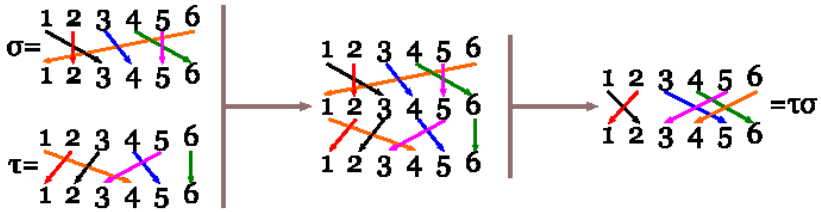
der Abbildungen von M in sich mit der Hintereinanderschaltung von Abbildungen als Verknüpfung und mit der Identität als neutralem Element ein Monoid, das man das *Abbildungsmonoid* zu M nennt.

Definition 6. Zu einer Menge M nennt man die Menge

$$\mathrm{Aut}\,(M) = \mathrm{Perm}\,(M) = \{\varphi : M \longrightarrow M : \varphi \text{ bijektiv}\}$$

der bijektiven Selbstabbildungen die *Automorphismengruppe* oder die *Permutationsgruppe* zu M.

Für eine endliche Menge $I = \{1, \ldots, n\}$ schreibt man auch $S_n = \mathrm{Perm}\,(I)$. Wir werden uns hauptsächlich auf endliche Permutationsgruppen beschränken. Eine endliche Permutation kann man bspw. mit einer (vollständigen) Wertetabelle beschreiben.



Lemma 7. *Sei M eine endliche Menge mit n Elementen. Dann besitzt die Permutationsgruppe* $\mathrm{Perm}\,(M) \cong S_n$ *genau $n!$ Elemente.*

Beweis. Es sei $M = \{1, \ldots, n\}$. Für die 1 gibt es n mögliche Bilder, für 2 gibt es noch $n-1$ mögliche Bilder, für 3 gibt es noch $n-2$ mögliche Bilder, usw. Daher gibt es insgesamt

$$n(n-1)(n-2)\cdots 2 \cdot 1 = n!$$

mögliche Permutationen. □

Lemma 8. *Sei M eine Menge und $N \subseteq M$ eine Teilmenge. Dann gibt es eine natürliche injektive Abbildung*

$$\mathrm{Perm}\,(N) \longrightarrow \mathrm{Perm}\,(M),\ \sigma \longmapsto \tilde{\sigma},$$

wobei $\tilde{\sigma}$ auf N gleich σ und auf $M \setminus N$ die Identität ist. Mittels dieser Abbildung ist $\mathrm{Perm}\,(N)$ *eine Untergruppe von* $\mathrm{Perm}\,(M)$.

Beweis. Offenbar ist die Abbildung wohldefiniert. Sie ist injektiv, da aus $\tilde{\sigma} = \tilde{\tau}$ sofort folgt, dass $\sigma = \tau$ ist. Die Abbildung liefert eine Bijektion zwischen $\mathrm{Perm}\,(N)$ und der Menge der Permutationen auf M, die $M \setminus N$ fest lassen. Diese Permutationen bilden eine Untergruppe. □

Bemerkung 9. Das vorstehende Lemma besagt bei $M = \{1, \ldots, n\}$ und $N = \{1, \ldots, n-1\}$, dass $S_{n-1} \subseteq S_n$ eine Untergruppe ist. Diese Untergruppe ist bei $n \geq 3$ kein Normalteiler. Sie hat den Index n, woraus sich erneut durch Induktion ergibt, dass die Permutationsgruppe S_n die Ordnung $n!$ besitzt.

Permutationsgruppen tauchen in vielen unterschiedlichen Situationen auf, und zwar häufig dann, wenn man sich die Wirkungsweise einer Gruppe auf einem geometrischen Objekt anschaut, wie im folgenden Beispiel (Zykel und Transposition werden sofort definiert).

Beispiel 10. Wir betrachten die Gruppe der eigentlichen Bewegungen an einem Würfel. Für eine fixierte Raumdiagonale W betrachten wir die Untergruppe H derjenigen Bewegungen, die diese Raumdiagonale in sich überführen. Das sind einerseits die drei Drehungen um diese Achse um $0, 120, 240$ Grad, andererseits aber auch die drei Halbdrehungen um diejenigen Kantenmittelpunktsachsen, deren Kanten nicht an den Ecken von W anliegen. Diese drei Halbdrehungen führen ebenfalls W in sich über, wobei allerdings die Eckpunkte vertauscht werden.

Es seien B, G und R die drei anderen Raumdiagonalachsen. Dann definiert jede Bewegung aus H eine Permutation der Menge $\{B, G, R\}$. Die beiden Dritteldrehungen definieren dabei die beiden Zykel $\langle B, G, R\rangle$ und $\langle B, R, G\rangle$, und die drei Halbdrehungen definieren jeweils eine Transposition. Damit ist H isomorph zu S_3 und somit ist S_3 eine Untergruppe der Würfelgruppe.

Zykeldarstellung für Permutationen

Sei M eine endliche Menge, $\sigma \in \mathrm{Perm}\,(M)$ eine Permutation und $x \in M$. Dann kann man die Folge

$$\sigma^0(x) = \mathrm{id}\,(x) = x,\ \sigma^1(x) = \sigma(x),\ \sigma^2(x),\ \sigma^3(x) \ldots$$

betrachten. Da M endlich ist, gibt es eine Wiederholung $\sigma^i(x) = \sigma^j(x)$ mit $i < j$. Durch Multiplikation mit σ^{-i} sieht man, dass es ein minimales $k \in \mathbb{N}_+$ gibt mit $\sigma^k(x) = \sigma^0(x) = x$, und dass alle $\sigma^j(x)$ für $j, 1 \leq j < k$, verschieden sind. Ist $y = \sigma^j(x)$, so durchläuft auch $\sigma^i(y)$ dieselbe Teilmenge aus M.

Definition 11. Sei M eine endliche Menge und σ eine Permutation auf M. Man nennt σ einen *Zykel der Ordnung* r, wenn es eine r-elementige Teilmenge $Z \subseteq M$ gibt derart, dass σ auf $M \setminus Z$ die Identität ist und σ die Elemente

aus Z zyklisch vertauscht. Wenn $Z = \{z, \sigma(z), \sigma^2(z), \ldots, \sigma^{r-1}(z)\}$ ist, so schreibt man einfach

$$\sigma = \langle z, \sigma(z), \sigma^2(z), \ldots, \sigma^{r-1}(z) \rangle .$$

Dabei kann man statt z jedes andere Element aus Z als Anfangsglied nehmen. Die Menge Z heißt auch der *Wirkungsbereich* des Zykels, und die (geordnete) Auflistung heißt die *Wirkungsfolge* des Zykels.

Definition 12. Eine *Transposition* auf einer endlichen Menge M ist eine Permutation auf M, die genau zwei Elemente miteinander vertauscht und alle anderen Elemente unverändert lässt.

Eine Transposition ist also ein besonders einfacher Zykel mit der Zyklendarstellung $\langle x, y \rangle$, wenn die Transposition die Punkte x und y vertauscht.

Lemma 13. *Jede Permutation auf einer endlichen Menge M kann man als Produkt von Transpositionen schreiben.*

Beweis. Wir beweisen die Aussage durch Induktion über die Anzahl der Menge M. Für $\#(M) = 1$ ist nichts zu zeigen, sei also $\#(M) \geq 2$. Die Identität ist das leere Produkt aus Transpositionen. Sei also σ nicht die Identität, und sei $\sigma(x) = y \neq x$. Es sei τ die Transposition, die x und y vertauscht. Dann ist y ein Fixpunkt von $\sigma\tau$, und man kann $\sigma\tau$ auffassen als eine Permutation auf $M' = M \setminus \{y\}$. Nach Induktionsvoraussetzung gibt es dann Transpositionen τ_j auf M' mit $\sigma\tau = \prod_j \tau_j$ auf M'. Dies gilt dann auch auf M, und daher ist $\sigma = \prod_j \tau_j \tau$. □

Satz 14. *Sei M eine endliche Menge und σ eine Permutation auf M. Dann gibt es eine Darstellung*

$$\sigma = \sigma_1 \cdots \sigma_k ,$$

wobei die σ_i Zykel der Ordnung ≥ 2 sind mit disjunkten Wirkungsbereichen. Dabei ist die Darstellung bis auf die Reihenfolge eindeutig.

Beweis. Es sei F die Fixpunktmenge von σ und es seien $Z_1, \ldots, Z_k$ diejenigen Teilmengen von M mit mindestens zwei Elementen derart, dass σ die Elemente aus jedem Z_i zyklisch vertauscht. Dann ist M die disjunkte Vereinigung aus F und den Z_i. Zu $i, 1 \leq i \leq k$ sei σ_i der Zykel auf M, der auf $M \setminus Z_i$ die Identität ist und auf Z_i mit σ übereinstimmt. Wir behaupten

$$\sigma = \sigma_1 \cdots \sigma_k .$$

Um dies einzusehen, sei $x \in M$ beliebig. Bei $x \in F$ ist x ein Fixpunkt für alle σ_i und daher kommt links und rechts wieder x raus. Sei also x kein Fixpunkt der Permutation. Dann gehört $x \in Z_i$ für genau ein i. Für alle $j \neq i$ ist x ein Fixpunkt von σ_j. Da $y = \sigma(x)$ ebenfalls zu Z_i gehört, ist auch y ein Fixpunkt von σ_j für alle $j \neq i$. Wendet man daher die rechte Seite auf x an, so wird x auf x abgebildet bis man zu σ_i kommt. Dieses bildet x auf y ab und die

folgenden σ_j bilden y auf y ab, so dass die rechte Seite insgesamt x auf y schickt und daher mit σ übereinstimmt. □

Aufgrund von diesem Satz können wir allgemein eine Zyklendarstellung für eine beliebige Permutation definieren.

DEFINITION 15. Sei M eine endliche Menge und σ eine Permutation auf M. Es seien $Z_1, \ldots, Z_k$ die Wirkungsbereiche der Zyklen von σ mit $n_i = \#(Z_i)$. Es sei $x_i \in Z_i$ und $Z_i = \{x_i, \sigma(x_i), \ldots, \sigma^{n_i-1}(x_i)\}$. Dann nennt man

$$\langle x_1, \sigma(x_1), \ldots, \sigma^{n_1-1}(x_1)\rangle\langle x_2, \sigma(x_2), \ldots, \sigma^{n_2-1}(x_2)\rangle \cdots \langle x_k, \sigma(x_k), \ldots, \sigma^{n_k-1}(x_k)\rangle$$

die Zyklendarstellung von σ.

Diese Schreibweise ist wie in Satz 8.14 zu verstehen, dass also σ das Produkt der k Zykel ist, die jeweils durch ihre Wirkungsfolge angegeben werden.

Abbildungsverzeichnis