Prof. Dr. H. Brenner **Osnabrück SS 2018**

Lineare Algebra und analytische Geometrie II

Vorlesung 44

In den folgenden Vorlesungen werden wir unsere Methoden um einige wesentliche Aspekte erweitern, indem wir insbesondere Äquivalenzrelationen in algebraischen Strukturen und Restklassenbildung besprechen. Diese Konstruktionen verlaufen für verschiedene algebraische Strukturen (Gruppen, Ringe, Vektorräume) nach dem gleichen Schema, so dass wir diese Konstruktion grundlegend für Gruppen besprechen.

Gruppen

Für ein Element $g \in G$ einer multiplikativ geschriebenen Gruppe G und $n \in \mathbb{N}$ schreibt man

$$g^n = g \cdots g$$

(n mal) und

$$g^n = (g^{-1})^{-n}$$

für $n \in \mathbb{Z}_-$. Aufgrund der Potenzgesetze, siehe Aufgabe 44.1, passt dies zusammen. Für Permutationen und invertierbare Matrizen haben wir schon mehrfach über die Ordnung gesprochen.

Definition 44.1. Sei G eine Gruppe und $g \in G$ ein Element. Dann nennt man die kleinste positive Zahl n mit $g^n = e_G$ die *Ordnung* von g. Man schreibt hierfür $\operatorname{ord}(g)$. Wenn alle positiven Potenzen von g vom neutralen Element verschieden sind, so setzt man $\operatorname{ord}(g) = \infty$.

Definition 44.2. Eine Gruppe G heißt *zyklisch*, wenn sie von einem Element erzeugt wird.

Das bedeutet, dass es ein Element $g \in G$ (einen *Erzeuger*) derart gibt, dass man jedes Element aus G als g^n mit einem $n \in \mathbb{Z}$ schreiben kann. Die Gruppe $(\mathbb{Z}, +, 0)$ ist zyklisch, wobei man 1 oder -1 als Erzeuger nehmen kann. Auch die Untergruppen von $\mathbb{Z}$ sind selbst wieder zyklisch, wie die folgende Aussage zeigt.

Satz 44.3. *Die Untergruppen von $\mathbb{Z}$ sind genau die Teilmengen der Form*

$$\mathbb{Z}d = \{kd \mid k \in \mathbb{Z}\}$$

mit einer eindeutig bestimmten nicht-negativen Zahl d.

Beweis. Siehe Aufgabe 44.2. □

Beispiel 44.4. Sei $n \in \mathbb{N}_+$ und betrachte auf

$$\mathbb{Z}/(n) = \{0, 1, \ldots, n-1\}$$

die Verknüpfung

$$a + b := (a+b) \mod n = \begin{cases} a+b, \text{ falls } a+b < n\,, \\ a+b-n, \text{ falls } a+b \geq n\,. \end{cases}$$

Mit dieser Verknüpfung liegt gemäß Aufgabe 44.14 eine Gruppe vor. Da man jedes Element als eine gewisse Summe der 1 mit sich selbst schreiben kann, liegt eine zyklische Gruppe vor.

Gruppenhomomorphismen

Gruppenhomomorphismen haben wir schon in der 18ten Vorlesung in Zusammenhang mit dem Signum einer Permutation erwähnt.

Definition 44.5. Seien $(G, \circ, e_G)$ und $(H, \circ, e_H)$ Gruppen. Eine Abbildung

$$\psi \colon G \longrightarrow H$$

heißt *Gruppenhomomorphismus*, wenn die Gleichheit

$$\psi(g \circ g') = \psi(g) \circ \psi(g')$$

für alle $g, g' \in G$ gilt.

Die Menge der Gruppenhomomorphismen von G nach H wird mit

$$\operatorname{Hom}(G, H)$$

bezeichnet. Lineare Abbildungen zwischen Vektorräumen sind insbesondere Gruppenhomomorphismen. Die folgenden beiden Lemmata folgen direkt aus der Definition.

Lemma 44.6. *Es seien G und H Gruppen und $\varphi \colon G \to H$ sei ein Gruppenhomomorphismus. Dann ist $\varphi(e_G) = e_H$ und $(\varphi(g))^{-1} = \varphi(g^{-1})$ für jedes $g \in G$.*

Beweis. Zum Beweis der ersten Aussage betrachten wir

$$\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G).$$

Durch Multiplikation mit $\varphi(e_G)^{-1}$ folgt $e_H = \varphi(e_G)$. Zum Beweis der zweiten Behauptung verwenden wir

$$\varphi\left(g^{-1}\right)\varphi(g) = \varphi\left(g^{-1}g\right) = \varphi(e_G) = e_H.$$

Das heißt, dass $\varphi(g^{-1})$ die Eigenschaft besitzt, die für das Inverse von $\varphi(g)$ charakteristisch ist. Da das Inverse in einer Gruppe nach Lemma 3.2 eindeutig bestimmt ist, muss $\varphi(g^{-1}) = (\varphi(g))^{-1}$ gelten. $\square$

Lemma 44.7. *Es seien F, G, H Gruppen. Dann gelten folgende Eigenschaften.*

(1) *Die Identität*

$$\mathrm{Id}\colon G \longrightarrow G$$

ist ein Gruppenhomomorphismus.

(2) *Sind* $\varphi : F \to G$ *und* $\psi : G \to H$ *Gruppenhomomorphismen, so ist auch die Hintereinanderschaltung* $\psi \circ \varphi\colon F \to H$ *ein Gruppenhomomorphismus.*

(3) *Ist* $F \subseteq G$ *eine Untergruppe, so ist die Inklusion* $F \hookrightarrow G$ *ein Gruppenhomomorphismus.*

(4) *Sei* $\{e\}$ *die triviale Gruppe. Dann ist die Abbildung* $\{e\} \to G$*, die* e *auf* e_G *schickt, ein Gruppenhomomorphismus. Ebenso ist die (konstante) Abbildung* $G \to \{e\}$ *ein Gruppenhomomorphismus.*

Beweis. Das ist trivial. □

Beispiel 44.8. Sei $d \in \mathbb{N}$ fixiert. Die Abbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z},\ n \longmapsto dn,$$

ist ein Gruppenhomomorphismus. Dies folgt unmittelbar aus dem Distributivgesetz. Für $d \geq 1$ ist die Abbildung injektiv und das Bild ist die Untergruppe $\mathbb{Z}d \subseteq \mathbb{Z}$. Bei $d = 0$ liegt die Nullabbildung vor. Bei $d = 1$ ist die Abbildung die Identität, bei $d \geq 2$ ist die Abbildung nicht surjektiv.

Beispiel 44.9. Sei $d \in \mathbb{N}_+$. Wir betrachten die Menge

$$\mathbb{Z}/(d) = \{0, 1, \ldots, d-1\}$$

mit der in Aufgabe 44.14 beschriebenen Addition, die damit eine Gruppe ist. Die Abbildung

$$\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/(d),$$

die eine ganze Zahl n auf ihren Rest bei Division durch d abbildet, ist ein Gruppenhomomorphismus. Sind nämlich $m = ad + r$ und $n = bd + s$ mit $0 \leq r, s < d$ gegeben, so ist

$$m + n = (a + b)d + r + s,$$

wobei allerdings $r + s \geq d$ sein kann. In diesem Fall ist

$$\varphi(m + n) = r + s - d$$

und das stimmt mit der Addition von r und s in $\mathbb{Z}/(d)$ überein. Diese Abbildungen sind surjektiv, aber nicht injektiv.

Beispiel 44.10. Zu einem Körper K und $n \in \mathbb{N}_+$ ist die Determinante

$$\det :\ \mathrm{GL}_n(K) \longrightarrow K^\times,\ M \longmapsto \det M,$$

ein Gruppenhomomorphismus. Dies beruht auf dem Determinantenmultiplikationssatz und Satz 16.11.

Beispiel 44.11. Die Zuordnung

$$S_n \longrightarrow \{1,-1\},\ \pi \longmapsto \operatorname{sgn}(\pi),$$

wobei S_n die Permutationsgruppe zu n Elementen bezeichnet, ist nach Satz 18.13 ein Gruppenhomomorphismus.

Lemma 44.12. *Sei G eine Gruppe. Dann entsprechen sich eindeutig Gruppenelemente $g \in G$ und Gruppenhomomorphismen φ von $\mathbb{Z}$ nach G über die Korrespondenz*

$$g \longmapsto (n \mapsto g^n) \text{ und } \varphi \longmapsto \varphi(1)\,.$$

Beweis. Sei $g \in G$ fixiert. Dass die Abbildung

$$\varphi_g\colon\ \mathbb{Z} \longrightarrow G,\ n \longmapsto g^n,$$

ein Gruppenhomomorphismus ist, ist eine Umformulierung der Potenzgesetze. Wegen $\varphi_g(1) = g^1 = g$ erhält man aus der Potenzabbildung das Gruppenelement zurück. Umgekehrt ist ein Gruppenhomomorphismus $\varphi\colon\ \mathbb{Z} \to G$ durch $\varphi(1)$ eindeutig festgelegt, da $\varphi(n) = (\varphi(1))^n$ für n positiv und $\varphi(n) = ((\varphi(1))^{-1})^{-n}$ für n negativ gelten muss. □

Man kann den Inhalt dieses Lemmas auch kurz durch $G \cong \operatorname{Hom}(\mathbb{Z}, G)$ ausdrücken. Die Gruppenhomomorphismen von einer Gruppe G nach $\mathbb{Z}$ sind schwieriger zu charakterisieren. Die Gruppenhomomorphismen von $\mathbb{Z}$ nach $\mathbb{Z}$ sind die Multiplikationen mit einer festen ganzen Zahl a, also

$$\mathbb{Z} \longrightarrow \mathbb{Z},\ x \longmapsto ax.$$

Gruppenisomorphismen

Definition 44.13. Seien G und H Gruppen. Einen bijektiven Gruppenhomomorphismus

$$\varphi\colon\ G \longrightarrow H$$

nennt man einen *Isomorphismus* (oder eine *Isomorphie*). Die beiden Gruppen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt.

Bijektive lineare Abbildungen sind insbesondere Gruppenisomorphismen.

Lemma 44.14. *Seien G und H Gruppen und sei*

$$\varphi\colon\ G \longrightarrow H$$

ein Gruppenisomorphismus. Dann ist auch die Umkehrabbildung

$$\varphi^{-1}\colon\ H \longrightarrow G,\ h \longmapsto \varphi^{-1}(h),$$

ein Gruppenisomorphismus.

Beweis. Dies folgt aus

$$\begin{aligned}\varphi^{-1}(h_1h_2) &= \varphi^{-1}\left(\varphi(\varphi^{-1}(h_1))\varphi(\varphi^{-1}(h_2))\right)\\ &= \varphi^{-1}\left(\varphi\left(\varphi^{-1}(h_1)\varphi^{-1}(h_2)\right)\right)\\ &= \varphi^{-1}(h_1)\varphi^{-1}(h_2).\end{aligned}$$

□

BEISPIEL 44.15. Betrachte die additive Gruppe der reellen Zahlen, also ($\mathbb{R}$, 0,+), und die multiplikative Gruppe der positiven reellen Zahlen, also ($\mathbb{R}_+$, $1, \cdot$). Dann ist die Exponentialabbildung

$$\exp\colon \mathbb{R} \longrightarrow \mathbb{R}_+,\, x \longmapsto \exp(x),$$

ein Gruppenisomorphismus. Dies beruht auf grundlegenden analytischen Eigenschaften der Exponentialfunktion. Die Homomorphieeigenschaft ist lediglich eine Umformulierung des Exponentialgesetzes

$$\exp(x+y) = e^{x+y} = e^x e^y = \exp(x)\exp(y).$$

Die Injektivität der Abbildung folgt aus der strengen Monotonie, die Surjektivität folgt aus dem Zwischenwertsatz. Die Umkehrabbildung ist der natürliche Logarithmus, der somit ebenfalls ein Gruppenisomorphismus ist.

Isomorphe Gruppen sind bezüglich ihrer gruppentheoretischen Eigenschaften als gleich anzusehen. Isomorphismen einer Gruppe auf sich selbst nennt man auch *Automorphismen*. Die Menge aller Automorphismen auf G bildet mit der Hintereinanderschaltung eine Gruppe, die man mit Aut G bezeichnet und die die *Automorphismengruppe* zu G nennt. Wichtige Beispiele für Automorphismen sind die sogenannten inneren Automorphismen.

DEFINITION 44.16. Sei G eine Gruppe und $g \in G$ fixiert. Die durch g definierte Abbildung

$$\kappa_g\colon G \longrightarrow G,\, x \longmapsto gxg^{-1},$$

heißt *innerer Automorphismus.*

Diese Abbildung κ_g heißt auch die *Konjugation* mit g. Wenn G eine kommutative Gruppe ist, so ist wegen $gxg^{-1} = xgg^{-1} = x$ die Identität der einzige innere Automorphismus. Der Begriff ist also nur bei nicht kommutativen Gruppen von Interesse.

LEMMA 44.17. *Ein innerer Automorphismus ist in der Tat ein Automorphismus. Die Zuordnung*

$$G \longrightarrow \operatorname{Aut} G,\, g \longmapsto \kappa_g,$$

ist ein Gruppenhomomorphismus.

Beweis. Es ist

$$\kappa_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \kappa_g(x)\kappa_g(y),$$

so dass ein Gruppenhomomorphismus vorliegt. Wegen

$$\kappa_g(\kappa_h(x)) = \kappa_g(hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = \kappa_{gh}$$

ist einerseits

$$\kappa_{g^{-1}} \circ \kappa_g = \kappa_{g^{-1}g} = \mathrm{id}_G,$$

so dass κ_g bijektiv, also ein Automorphismus, ist. Andererseits ist deshalb die Gesamtabbildung κ ein Gruppenhomomorphismus. □

Beispiel 44.18. Zu einer fixierten invertierbaren Matrix $B \in \mathrm{GL}_n(K)$ ist die Konjugation

$$\kappa_B\colon \mathrm{GL}_n(K) \longrightarrow \mathrm{GL}_n(K)\, ,\, M \longmapsto BMB^{-1},$$

gerade diejenige Abbildung, die der beschreibenden Matrix M zu einer linearen Abbildung bezüglich einer Basis die beschreibende Matrix bezüglich einer neuen Basis zuordnet.

Der Kern eines Gruppenhomomorphismus

Definition 44.19. Seien G und H Gruppen und sei

$$\varphi\colon G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann nennt man das Urbild des neutralen Elementes den *Kern* von φ, geschrieben

$$\mathrm{kern}\, \varphi = \varphi^{-1}(e_H) = \{g \in G \mid \varphi(g) = e_H\}\, .$$

Lemma 44.20. *Seien G und H Gruppen und sei*

$$\varphi\colon G \longrightarrow H$$

ein Gruppenhomomorphismus. Dann ist der Kern von φ eine Untergruppe von G.

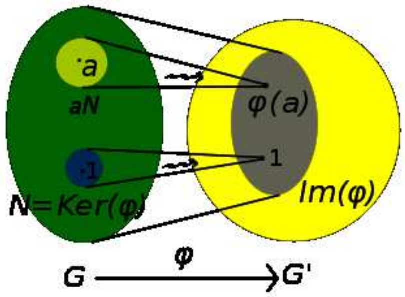
Beweis. Wegen $\varphi(e_G) = e_H$ ist $e_G \in \ker \varphi$. Seien $g, g' \in \ker \varphi$. Dann ist

$$\varphi(gg') = \varphi(g)\varphi(g') = e_H e_H = e_H$$

und daher ist auch $gg' \in \ker \varphi$. Der Kern ist also ein Untermonoid. Sei nun $g \in \ker \varphi$ und betrachte das inverse Element g^{-1}. Nach Lemma 44.6 ist

$$\varphi\left(g^{-1}\right) = (\varphi(g))^{-1} = e_H^{-1} = e_H,$$

also auch $g^{-1} \in \ker \varphi$. □



Wie für lineare Abbildungen gilt wieder das *Kernkriterium für die Injektivität.*

LEMMA 44.21. *Seien G und H Gruppen. Ein Gruppenhomomorphismus $\varphi : G \to H$ ist genau dann injektiv, wenn der Kern von φ trivial ist.*

Beweis. Wenn φ injektiv ist, so darf auf jedes Element $h \in H$ höchstens ein Element aus G gehen. Da e_G auf e_H geschickt wird, darf kein weiteres Element auf e_H gehen, d.h. $\ker \varphi = \{e_G\}$. Sei umgekehrt dies der Fall und sei angenommen, dass $g, \tilde{g} \in G$ beide auf $h \in H$ geschickt werden. Dann ist

$$\varphi\left(g\tilde{g}^{-1}\right) = \varphi(g)\varphi(\tilde{g})^{-1} = hh^{-1} = e_H$$

und damit ist $g\tilde{g}^{-1} \in \ker \varphi$, also $g\tilde{g}^{-1} = e_G$ nach Voraussetzung und damit $g = \tilde{g}$. □

Das Bild eines Gruppenhomomorphismus

LEMMA 44.22. *Seien G und H Gruppen und sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann ist das Bild von φ eine Untergruppe von H.*

Beweis. Sei $B := \operatorname{bild} \varphi$. Dann ist $e_H = \varphi(e_G) \in B$. Seien $h_1, h_2 \in B$. Dann gibt es $g_1, g_2 \in G$ mit $\varphi(g_1) = h_1$ und $\varphi(g_2) = h_2$. Damit ist $h_1 \cdot h_2 = \varphi(g_1) \cdot \varphi(g_2) = \varphi(g_1 \cdot g_2) \in B$. Ebenso gibt es für $h \in B$ ein $g \in G$ mit $\varphi(g) = h$. Somit ist $h^{-1} = (\varphi(g))^{-1} = \varphi(g^{-1}) \in B$. □

BEISPIEL 44.23. Betrachte die analytische Abbildung

$$\mathbb{R} \longrightarrow \mathbb{C},\, t \longmapsto e^{\mathrm{i}t} = \cos t + \mathrm{i} \sin t.$$

Aufgrund des Exponentialgesetzes (bzw. der Additionstheoreme für die trigonometrischen Funktionen) ist $e^{\mathrm{i}(t+s)} = e^{\mathrm{i}t}e^{\mathrm{i}s}$. Daher liegt ein Gruppenhomomorphismus von der additiven Gruppe $(\mathbb{R}, +, 0)$ in die multiplikative Gruppe $(\mathbb{C}^\times, \cdot, 1)$ vor. Wir bestimmen den Kern und das Bild dieser Abbildung. Für den Kern muss man diejenigen reellen Zahlen t bestimmen, für die

$$\cos t = 1 \text{ und } \sin t = 0$$

ist. Aufgrund der Periodizität der trigonometrischen Funktionen ist dies genau dann der Fall, wenn t ein ganzzahliges Vielfaches von 2π ist. Der Kern ist also die Untergruppe $2\pi\mathbb{Z}$. Für einen Bildpunkt gilt $\left|e^{\mathrm{i}t}\right| = \sin^2 t + \cos^2 t = 1$, so dass der Bildpunkt auf dem komplexen Einheitskreis liegt. Andererseits durchlaufen die trigonometrischen Funktionen den gesamten Einheitskreis, so dass die Bildgruppe der Einheitskreis mit der komplexen Multiplikation ist.

Abbildungsverzeichnis