

Algebra

Vorlesungsmitschrift

Prof. Dr. Damaris Schindler

\LaTeX -Version von Ben Arnold und Niklas Sennewald

Mathematisches Institut
Georg-August-Universität Göttingen
Wintersemester 2020/21

Inhaltsverzeichnis

I. Gruppen	1
1.1. Gruppen und Gruppenhomomorphismen	1
1.2. Nebenklassen und Normalteiler	5
Definitionen	9
Dateien	11

Dieses Skript stellt keinen Ersatz für die Vorlesungsnotizen von Prof. Schindler dar und wird nicht nochmals von ihr durchgesehen. Beweise werden wir i.d.R. nicht übernehmen (weil das in \LaTeX einfach keinen Spaß macht). glhf

I. Gruppen

1.1. Gruppen und Gruppenhomomorphismen

Datei 1

Motivation: aus dem ersten Jahr kennen wir viele Gruppen, z.B. $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $\mathbb{Z}/m\mathbb{Z}$ für $m \in \mathbb{N}$, \mathbb{R}^n , S_n = Permutationen auf n Elemente, Funktionen $f : \mathbb{R} \rightarrow \mathbb{C}$ mit punktweiser Addition

erstes Ziel:

- Wiederholung Grundbegriffe von Gruppen
- erste Resultate zur Theorie endlicher Gruppen

Definition (Monoid)

Ein Monoid ist eine Menge M zusammen mit einer Verknüpfung $\circ : M \times M \rightarrow M$, die folgende Eigenschaften erfüllt:

- i) $\forall a, b, c \in M$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$
- ii) es gibt ein Einselement $e \in M$ mit $e \circ a = a = a \circ e \forall a \in M$

Bemerkung: $(\mathbb{N}_{\geq 0}, +)$, $(\mathbb{Q}_{\geq 0}, +)$ sind Monoide aber keine Gruppe.

Definition (Inverselemente)

Sei (M, \circ) ein Monoid und $a \in M$. Wir nennen b invers zu a / *inverses Element* zu a , falls $b \circ a = a \circ b = e$.

Bemerkung: Sind $b, b' \in M$ invers zu a , dann ist $b = b'$, denn $b = b \circ e = b \circ (a \circ b') = (b \circ a) \circ b' = e \circ b' = b'$

Beispiel: Im $(\mathbb{N}_{\geq 0}, +)$ ist 0 das einzige Element, das ein inverses Element hat.

Notation: Ist $a \in M$ und $b \in M$ invers zu a , so schreiben wir $b = a^{-1}$.

Definition (Gruppe)

Wir nennen ein Monoid (G, \circ) eine *Gruppe*, falls jedes $a \in G$ ein inverses Element $a^{-1} \in G$ besitzt.

Beispiel: $GL_n(\mathbb{R}) = \{A \in M_{n \times n}(\mathbb{R}) \mid \det(A) \neq 0, n \geq 0\}$ ist eine Gruppe unter Matrixmultiplikation. Für $n \geq 2$ gibt es Matrizen $A, B \in GL_n(\mathbb{R})$ mit $AB \neq BA$.

Definition (abelsche Gruppe)

Sei (G, \circ) eine Gruppe. G heißt *kommutativ* oder *abelsch*, falls gilt $a \circ b = b \circ a \forall a, b \in G$.

Beispiel: ① Die Gruppe aller Diagonalmatrizen in $GL_n(\mathbb{R})$

$$\left\{ A \in GL_n(\mathbb{R}) \mid A = \begin{pmatrix} \alpha_1 & & 0 \\ & \ddots & \\ 0 & & \alpha_n \end{pmatrix}, \alpha_1, \dots, \alpha_n \in \mathbb{R} \setminus \{0\} \right\}$$

ist eine kommutative Gruppe unter Matrixmultiplikation.

② $M_{n \times n}(\mathbb{R})$ ist eine abelsche Gruppe unter Addition von Matrizen mit neutralem Element $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix}$

Bemerkung: Sei I eine Indexmenge und $G_i, i \in I$, Gruppen. Dann ist $\prod_{i \in I} G_i$ wieder eine Gruppe unter der Verknüpfung $((g_i)_{i \in I}, (h_i)_{i \in I}) \mapsto (\underbrace{g_i h_i}_{\in G_i})_{i \in I}$ für $g_i, h_i \in G_i, i \in I$.

Beispiel: Für $m \in \mathbb{N}$ ist $\mathbb{Z}/m\mathbb{Z}$ eine Gruppe unter Addition. Wir können nach dieser Bemerkung daraus (endliche abelsche) Gruppen

$$\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \dots \times \mathbb{Z}/m_n\mathbb{Z}$$

für $m_1, \dots, m_n \in \mathbb{N}$ konstruieren.

Definition (Untermonoid, Untergruppe)

Sei M ein Monoid und $H \subseteq M$. Wir nennen H ein *Untermonoid*, falls $e \in H$ und gilt $a, b \in H \implies a \circ b \in H$. Sei G eine Gruppe. Eine Teilmenge $\emptyset \neq H \subseteq G$ heißt *Untergruppe* von G , falls gilt $\forall a, b \in H : a \circ b^{-1} \in H$.

Notation: Ist H eine Untergruppe von G , so schreibe auch $H \leq G$ und $H < G$ falls $H \neq G$.

Beispiel: ① Für eine beliebige Gruppe G sind $\{e\}$ und G stets Untergruppen von G .

② Sei $(G, \circ) = (\mathbb{Z}, +)$ und $m \in \mathbb{N}$. Dann ist $m \cdot \mathbb{Z} \subseteq \mathbb{Z}$ eine Untergruppe von \mathbb{Z}

und $m \cdot \mathbb{Z}_{\text{geq}0}$ ein Untermonoid von \mathbb{Z} .

© $(\mathbb{Z}, +)$ ist eine Untergruppe $(\mathbb{C}, +)$, $(\mathbb{Z}_{\text{geq}0}, +)$ ist Untermonoid von $(\mathbb{C}, +)$.

④ Sei \mathbb{K} ein Körper und $n \in \mathbb{N}$. Dann ist $SL_n(\mathbb{K}) = \{A \in Mat_{n \times n}(\mathbb{K}) \mid \det(A) = 1\}$ eine Untergruppe von $GL_n(\mathbb{K}) = \{A \in M_{n \times n}(\mathbb{K}) \mid \det(A) \neq 0\}$.

Bemerkung: Sei G eine Gruppe und $H_i, i \in I$ Untergruppen von G . Dann ist auch $\bigcap_{i \in I} H_i$ eine Untergruppe von G .

Datei 2

Definition (Gruppenhomomorphismus)

Seien G, G' Gruppen. Wir nennen eine Abbildung $\varphi : G \rightarrow G'$ *Gruppenhomomorphismus*, wenn gilt

$$\varphi(a \circ b) = \varphi(a) \circ \varphi(b) \quad \forall a, b \in G.$$

Bemerkung: Statt $a \circ b$ schreiben wir im Folgenden kürzer auch ab .

Lemma 1.1.1

Sei $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus und e bzw. e' die Einselemente von G bzw. G' . Dann gilt

$$(i) \quad \varphi(e) = e'$$

$$(ii) \quad \varphi(a^{-1}) = (\varphi(a))^{-1} \quad \forall a \in G$$

Beispiel: ① Sei G eine Gruppe und $g \in G$. Dann definiert die Abbildung

$$\begin{aligned} \varphi : \mathbb{Z} &\rightarrow G \\ n &\mapsto g^n \end{aligned}$$

einen Gruppenhomomorphismus. Wir setzen hier $g^0 := e$ und $g^{-m} := (g^{-1})^m$ für $m \in \mathbb{N}$. Jeder Gruppenhomomorphismus $\varphi : \mathbb{Z} \rightarrow G$ hat diese Form.

→ im Allgemeinen ist φ weder injektiv noch surjektiv!

$$\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, n \mapsto n \bmod m \quad \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}, n \mapsto (n, 0)$$

⑤ Seien $m, n \in \mathbb{N}, m < n$. Schreibe $\pi \in S_n$ in der Form $\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$.

Dann ist $\varphi : S_m \rightarrow S_n$,

$$\begin{pmatrix} 1 & \dots & m \\ \pi(1) & \dots & \pi(m) \end{pmatrix} \mapsto \begin{pmatrix} 1 & \dots & m & m+1 & \dots & n \\ \pi(1) & \dots & \pi(m) & \pi(m+1) & \dots & \pi(n) \end{pmatrix}$$

ein injektiver Gruppenhomomorphismus.

Definition (verschiedene Morphismen, Kern)

Ein Gruppenhomomorphismus $\varphi : G \rightarrow G'$ heißt *Isomorphismus/ Monomorphismus/ Epimorphismus*, falls φ bijektiv/injektiv/surjektiv ist.

Ein Gruppenhomomorphismus $\varphi : G \rightarrow G$ nennen wir auch *Endomorphismus* und falls φ bijektiv ist *Automorphismus*. Die Menge $\ker \varphi = \{g \in G \mid \varphi(g) = e'\} \subseteq G$ heißt *Kern von φ* und $\operatorname{im} \varphi = \varphi(G) \subseteq G'$ *Bild von φ* .

Notation: Gibt es einen Isomorphismus $\varphi : G \rightarrow G'$, so schreiben wir auch $G \cong G'$.

Bemerkung: Ⓐ Sei $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus. Dann sind $\varphi(G)$ und $\ker \varphi$ Untergruppen von G' bzw. G .

Ⓑ Seien $\varphi : G \rightarrow G'$ und $\psi : G' \rightarrow G''$ Gruppenhomomorphismen. Dann ist auch

$$\psi \circ \varphi : G \rightarrow G''$$

ein Gruppenhomomorphismus

Lemma 1.1.2

Sei $\varphi : G \rightarrow G'$ ein Gruppenhomomorphismus. Die Abbildung φ ist genau dann ein Isomorphismus, wenn es einen Gruppenhomomorphismus $\psi : G' \rightarrow G$ gibt mit $\psi \circ \varphi = \operatorname{id}_G$ und $\varphi \circ \psi = \operatorname{id}_{G'}$.

Beispiel: (i) Sei G eine Gruppe und $a \in G$. Dann ist $\varphi_a : G \rightarrow G, g \mapsto aga^{-1}$ ein Automorphismus von G . Schreibe $\operatorname{Aut}(G) = \{\varphi : G \rightarrow G \mid \varphi \text{ Automorphismus}\}$. Dann ist $\operatorname{Aut}(G)$ eine Gruppe unter Verknüpfung und

$$\begin{aligned} G &\rightarrow \operatorname{Aut}(G) \\ a &\mapsto \varphi_a \end{aligned}$$

ein Gruppenhomomorphismus.

(ii) Sei $n \in \mathbb{N}$ und E_n die Menge der n -ten Einheitswurzeln, d.h. $E_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$. Dann ist E_n eine Gruppe unter Multiplikation und für jedes $m \in \mathbb{N}$ ist die Abbildung

$$\begin{aligned} E_n &\rightarrow E_n \\ \zeta &\mapsto \zeta^m \end{aligned}$$

ein Endomorphismus von E_n .

- (iii) $\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R} \setminus \{0\}, \cdot), x \mapsto e^x$ ist ein Gruppenhomomorphismus mit $\ker \exp = \{0\}$, also ein Monomorphismus.

Notation: Für eine nichtleere Menge X schreibe

$$S_X := \{\sigma : X \rightarrow X \mid \sigma \text{ ist bijektiv}\}.$$

Dann ist S_X eine Gruppe unter Verkettung von Abbildungen.

Bemerkung: Ist $|X| = n < \infty$, dann gibt es einen Gruppenisomorphismus

$$S_X \cong S_n.$$

Satz 1.1.3 (Satz von Cayley)

Sei G eine Gruppe mit $|G| = n < \infty$. Dann ist G isomorph zu einer Untergruppe von S_n .

1.2. Nebenklassen und Normalteiler

Datei 3

Beispiel: Sei $(G, \cdot) = (\mathbb{Z}, +)$ und $m \in \mathbb{N}$. Wir definieren eine Äquivalenzrelation \sim auf \mathbb{Z} durch

$$\begin{aligned} a \sim b &\iff m \mid a - b \\ &\iff a - b \in m\mathbb{Z} \end{aligned}$$

Dann ist $a \in \mathbb{Z}$ die Menge $a + m\mathbb{Z} \subseteq \mathbb{Z}$ eine Äquivalenzklasse. $m\mathbb{Z} \subseteq \mathbb{Z}$ ist eine Untergruppe und jede Äquivalenzklasse von \sim hat die Form $a + m\mathbb{Z}$ für ein $a \in \mathbb{Z}$.

Definition (Nebenklasse)

Sei G eine Gruppe und $H \leq G$ eine Untergruppe sowie $a \in G$. Dann nennen wir die Menge

$$aH := \{ah \mid h \in H\}$$

Linksnebenklasse von H und

$$Ha := \{ha \mid h \in H\}$$

Rechtsnebenklasse von H . Ein Element $a' \in aH$ (bzw. $a' \in Ha$) nennen wir *Repräsentant* der Nebenklasse aH (bzw. Ha).

Lemma 1.2.1

Sei $H \leq G$ eine Untergruppe einer Gruppe G und $a, b \in G$. Dann sind die folgenden Aussagen äquivalent:

$$i) \quad aH = bH$$

$$ii) \quad aH \cap bH \neq \emptyset$$

$$iii) \quad a \in bH$$

$$iv) \quad b^{-1}a \in H$$

Satz 1.2.2

Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann gibt es für alle $a, b \in G$ eine Bijektion $aH \rightarrow bH$ und G ist eine disjunkte Vereinigung von Linksnebenklassen von H .

Bemerkung: Satz 1.2.2 gilt ebenso für Rechtsnebenklassen.

Definition

Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Wir schreiben G/H (bzw. $H \backslash G$) für die Mengen der Links- (bzw. Rechts-)nebenklassen von H .

Bemerkung: Definieren wir

$$\begin{aligned} \varphi : G/H &\rightarrow H \backslash G \\ aH &\mapsto Ha \end{aligned}$$

so ist φ eine Bijektion zwischen G/H und $H \backslash G$.

Definition (Index)

Sei G eine Gruppe und $H \leq G$. Dann schreiben wir

$$(G : H) = |G/H| = |H \backslash G|$$

und nennen $(G : H)$ den Index von H in G .

Satz 1.2.3 (Satz von Lagrange)

Sei G eine endliche Gruppe und $H \leq G$. Dann gilt

$$|G| = |H| \cdot (G : H).$$

Korollar 1.2.4

Sei G eine endliche Gruppe und $H \leq G$. Dann gilt $|H| \mid |G|$.

Definition (Ordnung)

Sei G eine Gruppe und $a \in G$. Schreibe $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ für die von a erzeugte Untergruppe. Wir definieren $\text{ord}(a) := |\langle a \rangle|$ und nennen $\text{ord}(a)$ die *Ordnung von a* .

Korollar 1.2.5

Sei $a \in G$ und $|G| < \infty$ eine endliche Gruppe. Dann gilt

$$\text{ord}(a) \mid |G|.$$

Beispiel: Untergruppen der S_3 . Zykelschreibweise:

schreibe (12) für $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ und (123) für $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ und ebenso für Permutationen.

Dann ist

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

und Untergruppen H der S_3 haben Ordnung 1,2,3 oder 6.

Ordnung 6: $H = S_3$

Ordnung 1: $H = \{\text{id}\}$

Ordnung 2: $\langle (12) \rangle, \langle (13) \rangle, \langle (23) \rangle$

Ordnung 3: $H = \{\text{id}, (123), (132)\}$

Definitionen

Bild, [4](#)

Gruppe, [1](#)

 abelsche, [2](#)

Gruppenhomomorphismus, [3](#)

Index, [6](#)

Inverselemente, [1](#)

Kern, [4](#)

Monoid, [1](#)

Morphismen

 Automorphismus, [4](#)

 Endomorphismus, [4](#)

 Epimorphismus, [4](#)

 Isomorphismus, [4](#)

 Monomorphismus, [4](#)

Nebenklasse, [5](#)

Untergruppe, [2](#)

Untermonoid, [2](#)

Dateien

Datei 1, [1](#)

Datei 2, [3](#)

Datei 3, [5](#)