# Algebra

## Vorlesungsmitschrift

Prof. Dr. Damaris Schindler

LaTeX-Version von Ben Arnold und Niklas Sennewald

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

# Inhaltsverzeichnis

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. 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 $f : \mathbb{R} \to \mathbb{C}$ 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 $\circ : M \times M \to M$, 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:** ⓐ Die Gruppe aller Diagonalmatrizen in $GL_n(\mathbb{R})$

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

ist eine kommutative Gruppe unter Matrixmultiplikation.

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

**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 $\big((g_i)_{i\in I}, (h_i)_{i\in I}\big) \mapsto (\underbrace{g_i h_i}_{\in G_i})_{i\in I}$ für $g_i, h_i \in G_i, i \in I$.

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

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

für $m_1, \ldots, m_n \in N$ 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:** ⓐ Für eine beliebige Gruppe $G$ sind $\{e\}$ und $G$ stets Untergruppen von $G$.

ⓑ 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 $m \cdot \mathbb{Z}_{geq0}$ ein Untermonoid von $\mathbb{Z}$.

ⓒ $(\mathbb{Z}, +)$ ist eine Untergruppe $(\mathbb{C}, +)$, $(\mathbb{Z}_{geq0}, +)$ ist Untermonoid von $(\mathbb{C}, +)$.

ⓓ 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 $\varphi : G \to G'$ *Gruppenhomomorphismus*, wenn gilt

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

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

**Lemma 1**
*Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus und $e$ bzw. $e'$ die Einselemente von $G$ bzw. $G'$. Dann gilt*

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

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

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

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

einen Gruppenhomomorphismus. Wir setzen hier $g^0 := e$ und $g^{-m} := (g^{-1})^m$ für $m \in \mathbb{N}$. Jeder Gruppenhomomorphismus $\varphi : \mathbb{Z} \to G$ hat diese Form.
$\to$ im Allgemeinen ist $\varphi$ weder injektiv noch surjektiv!
$\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, n \mapsto n \mod m \quad \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}, n \mapsto (n, 0)$

ⓑ 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 $\varphi : S_m \to S_n$,

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

ein injektiver Gruppenhomomorphismus.

**Definition** (verschiedene Morphismen, Kern)
Ein Gruppenhomomorphismus $\varphi : G \to G'$ heißt *Isomorphismus/ Monomorphismus/ Epimorphismus*, falls $\varphi$ bijektiv/injektiv/surjektiv ist.
Ein Gruppenhomomorphismus $\varphi : G \to G$ nennen wir auch *Endomorphismus* und falls $\varphi$ bijektiv ist *Automorphismus*. Die Menge $\ker \varphi = \{g \in G \mid \varphi(g) = e'\} \subseteq G$ heißt *Kern von* $\varphi$ und $\operatorname{im} \varphi = \varphi(G) \subseteq G'$ *Bild von* $\varphi$.

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

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

ⓑ Seien $\varphi : G \to G'$ und $\psi : G' \to G''$ Gruppenhomomorphismen. Dann ist auch

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

ein Gruppenhomomorphismus

**Lemma 2**
*Sei $\varphi : G \to G'$ ein Gruppenhomomorphismus. Die Abbildung $\varphi$ ist genau dann ein Isomorphismus, wenn es einen Gruppenhomomorphismus $\psi : G' \to G$ gibt mit $\psi \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \psi = \mathrm{id}_{G'}$.*

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

$$\begin{aligned} G &\to \mathrm{Aut}(G) \\ a &\mapsto \varphi_a \end{aligned}$$

ein Gruppenhomomorphismus.

(ii) *Sein* $\in \mathbb{N}$ 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

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

ein Endomorphismus von $E_n$.

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

**Notation:** Für eine nichtleere Menge $X$ schreibe

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

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 3** (Satz von Cayley)
*Sei $G$ eine Gruppe mit $|G| = n < \infty$. Dann ist $G$ isomorph zu einer Untergruppe von $S_n$.*

# Definitionen