

UNIVERSITÄT KONSTANZ

Skriptum zur Vorlesung

---

# Einführung in die Algebra

---

Private Mitschrift

*gelesen von:*

Prof. Dr. Markus Schweighofer

Wintersemester 2014/15  
Stand vom 14. Dezember 2014



# Inhaltsverzeichnis

<b>1</b>	<b>Gruppen</b>	<b>5</b>
1.1	Gruppen und Untergruppen . . . . .	5



# § 1 Gruppen

---

## § 1.1 Gruppen und Untergruppen

---

**1.1.1 Definition** Eine Gruppe ist ein geordnetes Paar  $(G, \cdot)$ , wobei  $G$  eine Menge ist und  $\cdot : G \times G \rightarrow G$  eine meist infix (und manchmal gar nicht) notierte Abbildung mit folgenden Eigenschaften ist:

$$(A) \quad \forall a, b, c \in G : a(bc) = (ab)c \quad \text{„assoziativ“}$$

$$(N) \quad \exists e \in G \quad \forall a \in G : ae = a = ea \quad \text{„neutrales Element“}$$

$$(I) \quad \forall a \in G \quad \exists g \in G : ag = 1 = ga \quad \text{„inverse Elemente“}$$

„ $\cdot$ “ heißt Gruppenmultiplikation oder Gruppenverknüpfung. Gilt zusätzlich

$$(K) \quad \forall a, b \in G : ab = ba$$

so heißt  $(G, \cdot)$  abelsch oder kommutativ.

**Anmerkung** Sind  $e, e' \in G$  neutral, so  $e = ee' = e'$ . Daher gibt es genau ein neutrales Element, für welches man oft „1“ schreibt.

### 1.1.2 Bemerkung

(a) Sei  $(G, \cdot)$  eine Gruppe und  $a \in G$ . Seien  $b, b'$  invers zu  $a$ . Dann

$$b \stackrel{(N)}{=} b \cdot 1 \stackrel{(I)}{=} b(ab') \stackrel{(A)}{=} (ba)b' \stackrel{(I)}{=} 1 \cdot b \stackrel{(N)}{=} b'.$$

Daher gibt es zu jedem  $a \in G$  genau ein inverses Element in  $G$ , welches wir mit  $a^{-1}$  bezeichnen.

(b) (N) und (I) kann man wie folgt schreiben:

$$(N) \quad \forall a \in G : a1 = a = 1a$$

$$(I) \quad \forall a \in G : aa^{-1} = 1 = a^{-1}a$$

## 1 Gruppen

- (c) Oft: „Sei  $G$  eine Gruppe“, statt: „Sei  $(G, \cdot)$  eine Gruppe.“
- (d) Sei  $G$  eine Gruppe,  $n \in \mathbb{N}_0$  und  $a_1, \dots, a_n \in G$ . Dann definiert man  $\prod_{i=1}^n a_i := a_1 \cdot \dots \cdot a_n$  als 1 für  $n = 0$  und indem man  $a_1 \cdot \dots \cdot a_n$  sinnvoll mit Klammern versieht, sonst. Dies hängt nicht von der Wahl der Klammerung da, wie (A) für  $n = 3$  besagt. Für  $n > 3$  siehe [→ LA 2.1.6] oder mache es als Übung per Induktion. Falls  $G$  additiv geschrieben ist, schreibt man  $\sum_{i=1}^n a_i$ , statt  $\prod_{i=1}^n a_i$ .
- (e) Sei  $G$  eine Gruppe,  $n \in \mathbb{Z}$  und  $a \in G$ . Dann definiert man

$$a^n := \begin{cases} \prod_{i=1}^n a, & \text{für } n \geq 0, \\ \prod_{i=1}^n (a^{-1}), & \text{für } n \leq 0. \end{cases}$$

Fall  $G$  additiv geschrieben ist, schreibt man  $na$ , statt  $a^n$ .

**1.1.3 Definition** Ist  $(G, \cdot)$  eine Gruppe, so nennt man  $\#G \in \mathbb{N}_0 \cup \{\infty\}$  die Ordnung von  $(G, \cdot)$ .

### 1.1.4 Beispiel

- (a) Für jede Menge  $M$  bildet die Menge  $S_M := \{f \mid f : M \rightarrow M \text{ bijektiv}\}$  mit der durch  $fg := f \circ g$  ( $f, g \in S_M$ ) gegebenen Multiplikation eine Gruppe. Man nennt sie die symmetrische Gruppe auf  $M$ . Das neutrale Element von  $S_M$  ist die Identität auf  $M$  und das zu einem  $f \in S_M$  inverse Element ist die Umkehrfunktion von  $f$ , wodurch die Notation  $f^{-1}$  nicht zweideutig ist.
- Für  $n \in \mathbb{N}_0$  ist  $S_n := S_{\{1, \dots, n\}}$  eine Gruppe der Ordnung  $n! := \prod_{i=1}^n i$  „ $n$  Fakultät“. Für  $n \geq 3$  ist die nicht abelsch, dann die Transpositionen  $\tau_{1,2}$  und  $\tau_{2,3}$  konvertieren nicht, d.h.  $\tau_{1,2}\tau_{2,3} \neq \tau_{2,3}\tau_{1,2}$ . In der Tat:  $(\tau_{1,2}\tau_{2,3})(1) = \tau_{1,2}(1) = 2$  und  $(\tau_{2,3}\tau_{1,2})(1) = \tau_{2,3}(2) = 3$ .
- (b) Für jeden Vektorraum  $V$  ist die Menge  $\text{Aut}(V) := \{f \mid f : V \rightarrow V \text{ linear und bijektiv}\}$  mit der Hintereinanderschaltung als Multiplikation eine Gruppe.
- (c) Ist  $R$  ein kommutativer Ring (z. B.  $R = \mathbb{Z}$ ), so ist  $\text{GL}_n(R) := \{A \in R^{n \times n} \mid A \text{ invertierbar}\} = \{A \in R^{n \times n} \mid \det A \in R^\times\}$  eine Gruppe.

**1.1.5 Proposition** Sei  $G$  eine Gruppe und  $a, b \in G$ .

- (a)  $ab = 1 \iff a = b^{-1} \iff b = a^{-1}$
- (b)  $(a^{-1})^{-1} = a$
- (c)  $(ab)^{-1} = b^{-1}a^{-1}$

**Beweis:**

## 1.1 Gruppen und Untergruppen

- (a) Gilt  $ab = 1$ , so  $a \stackrel{(N)}{=} a1 \stackrel{(I)}{=} a(bb^{-1}) \stackrel{(A)}{=} (ab)b^{-1} = 1b \stackrel{(N)}{=} b^{-1}$ . Gilt  $a = b^{-1}$ , so  $b \stackrel{(N)}{=} 1b \stackrel{(I)}{=} (a^{-1}a)b \stackrel{(A)}{=} a^{-1}(ab) = a^{-1}(b^{-1}b) \stackrel{(I)}{=} a^{-1}1 \stackrel{(N)}{=} a^{-1}$ . Gilt  $b = a^{-1}$ , so  $ab = 1$ .
- (b) Aus  $aa^{-1} \stackrel{(I)}{=} 1$  folgt mit (a)  $(a^{-1})^{-1} = a$ .
- (c) Aus  $(ab)(b^{-1}a^{-1}) \stackrel{(A)}{=} a(b(b^{-1}a^{-1})) \stackrel{(A)}{=} a((bb^{-1})a^{-1}) \stackrel{(I)}{=} a(1a^{-1}) \stackrel{(N)}{=} aa^{-1} \stackrel{(I)}{=} 1$  folgt mit (a)  $(ab)^{-1} = b^{-1}a^{-1}$ .  $\square$

**1.1.6 Definition** Seien  $(G, \cdot_G)$  und  $(H, \cdot_H)$  Gruppen. Dann heißt  $(H, \cdot_H)$  eine Untergruppe von  $(G, \cdot_G)$ , wenn  $H \subseteq G$  und  $\forall a, b \in H : a \cdot_H b = a \cdot_G b$ .

**1.1.7 Proposition** Sei  $(G, \cdot_G)$  eine Gruppe und  $H$  eine Menge. Dann ist  $H$  genau dann Trägermenge einer Untergruppe von  $(G, \cdot_G)$ , wenn  $H \subseteq G$ ,  $1_G \in H$ ,  $\forall a, b \in H : a \cdot_G b \in H$  und  $\forall a \in H : a^{-1} \in H$ .

In diesem Fall gibt es genau eine Abbildung  $\cdot_H : H \times H \rightarrow H$  derart, dass  $(H, \cdot_H)$  eine Untergruppe von  $(G, \cdot_G)$  ist. Es gilt dann  $1_H = 1_G$ ,  $\forall a, b \in H : a \cdot_H b = a \cdot_G b$  und  $a^{-1} = a^{-1}$  (je in  $G$  und  $H$  gebildet).

**Beweis:** Klar oder vgl. LA § 2.  $\square$

### 1.1.8 Bemerkung

- (a) Ist  $(H, \cdot_H)$  Untergruppe von  $(G, \cdot_G)$ , so schreibt man meist  $\cdot$  statt  $\cdot_H$ . Oft erwähnt man  $\cdot_H$  gar nicht mehr und schreibt einfach „ $H$  ist Untergruppe von  $G$ “ oder  $H \leq G$ .
- (b) Untergruppen abelscher Gruppen sind abelsch.

### 1.1.9 Beispiel

- (a) Für  $n \in \mathbb{N}_0$  ist  $A_n := \{\sigma \in S_n \mid \text{sgn } \sigma = 1\}$  eine Untergruppe von  $S_n$ , die man alternierende Gruppe nennt. [→ LA § 9.1]