Algebra (Bachelor)

zur Vorlesung von Prof. Dr. Tobias Dyckerhoff

18. Oktober 2024

Inhaltsverzeichnis

1 Gruppen und Symmetrie **2**
- 1.1 Grundbegriffe . . . 2
- 1.2 Untergruppen . . . 3
- 1.3 Homomorphismen . . . 4

Konventionen

- TBD

Dies ist ein inoffizielles Skript zur Vorlesung Algebra bei Prof. Dr. Tobias Dyckerhoff im Wintersemester 24/25. Fehler und Verbesserungsvorschläge immer gerne an rasmus.raschke@uni-hamburg.de.

1 Gruppen und Symmetrie

Bemerkung. Wir möchten Gruppentheorie zunächst motivieren: Man betrachte einen Tetraeder. Um dessen Symmetrien zu erfassen, könnten wir z.B. schauen, welche Bewegungen diesen in sich selbst überführen. Es gibt vier Rotationsachsen, die eine Ecke und eine Fläche durchdringen und bei Rotation um 120° den Tetraeder in sich selbst überführen. Weiterhin gibt es drei 180°-Rotationsachsen mittig durch gegenüberliegende Kanten. Auch die Identität lässt den Tetraeder unverändert. Also gibt es $1 + 4 \cdot 2 + 3 = 12$ Symmetrien. Gruppen bieten eine Möglichkeit, solche Symmetrien und deren Verkettungen zu erfassen und zu untersuchen.

1.1 Grundbegriffe

Definition 1.1.1. Gruppe

Eine **Gruppe** ist ein Paar $(G, \circ)$, bestehend aus einer Menge[a] G und einer Abbildung

$$\circ : G \times G \to G \tag{1.1.1}$$
$$(g, h) \mapsto g \circ h \tag{1.1.2}$$

mit folgenden Eigenschaften:

(G1) Für alle $g_1, g_2, g_3 \in G$ gilt das Assoziativgesetz: $(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$.

(G2) Es gibt ein Element $e \in G$, sodass gilt:

(2a) Für jedes $g \in G$ gilt $e \circ g = g$.

(2b) Für jedes $g \in G$ existiert ein $g' \in G$ mit $g' \circ g = e$.

Die Abbildung $\circ$ heißt **Verknüpfung**, ein Element $e \in G$ mit den Eigenschaften aus 2. heißt **neutrales Element**, und ein Element $g' \in G$ zu gegebenem $g \in G$ mit Eigenschaft 2b heißt **Inverses** von g.

[a] im ZFC-Axiomensystem

Bemerkung. Übungsaufgabe:
Sei $(G, \circ)$ eine Gruppe. Dann gelte:

1. Das neutrale Element $e \in G$ ist eindeutig bestimmt, außerdem gelte $\forall g \in G : g \circ e = g$.
2. Zu gegebenem $g \in G$ ist das Inverse $g' \in G$ eindeutig bestimmt und erfüllt zudem $g \circ g' = e$.
3. Für $n \geq 3$ hängt das Produkt von Gruppenelementen $g_1, g_2, \ldots, g_n$ nicht von der Klammerung ab.

Beispiele. Wir geben einige Beispiele für Gruppen:

1. Die Gruppe $(\mathbb{Z}, +)$ der ganzen Zahlen $\mathbb{Z}$ mit der Addition $+$.
2. Für einen Körper $\mathbb{K}$ existiert die additive Gruppe $(\mathbb{K}, +)$ und die multiplikative Gruppe $(\mathbb{K}\backslash\{0\}, \cdot)$.
3. Für jede Menge M existiert die **symmetrische Gruppe** $(\mathfrak{S}_M, \circ)$, wobei $\mathfrak{S}_M$ die Menge der bijektiven Selbstabbildungen von M und $\circ$ die Komposition ist. Für $n \geq 1$ vereinbaren wir $\mathfrak{S}_n := \mathfrak{S}_{\{1,2,\ldots,n\}}$. Wir vereinbaren als Konvention die **Zykelschreibweise**. Z.B. in $\mathfrak{S}_3$ existieren Zykel
$$\sigma : \{1, 2, 3\} \to \{1, 2, 3\} \tag{1.1.3}$$
$$1 \mapsto 2 \tag{1.1.4}$$
$$2 \mapsto 1 \tag{1.1.5}$$
$$3 \mapsto 3, \tag{1.1.6}$$
auch darstellbar als
$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \tag{1.1.7}$$
oder (12).
4. Für $n \geq 1$ und einen Körper $\mathbb{K}$ ist die **allgemeine lineare Gruppe** $\mathrm{GL}(n, \mathbb{K}), \circ)$ definiert, wobei
$$\mathrm{GL}(n, \mathbb{K}) := \left\{ A \in \mathbb{K}^{n \times n} \mid \det A \neq 0 \right\} \tag{1.1.8}$$
Die Menge der invertierbaren $n \times n$-Matrizen mit Einträgen in $\mathbb{K}$ ist. Typische Beispiele für Körper sind $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_q$ mit $q = p^n$, p prim.
ÜA: $|\mathrm{GL}(n, \mathbb{F}_q)| = ?$.

Bemerkung. Um den alltäglichen Gebrauch von Gruppen zu vereinfachen, machen wir folgende Vereinbarungen:

1. Wir bezeichnen $(G, \circ)$ üblicherweise einfach mit G und lassen $\circ$ implizit.
2. Für $g, h \in G$ schreiben wir $gh = g \circ h$, für $e \in G$ schreiben wir 1 und für g' schlicht g^{-1}.
3. Gilt $g \circ h = h \circ g$ für alle $g, h \in G$, so heißt G **abelsch**. In diesem Fall wird die Verknüpfung oft mit $+$, das neutrale Element mit 0 und das inverse Element mit $-g$ bezeichnet.
4. Gemäß obiger ÜA zur Klammerung schreiben wir einfach $g_1 g_2 \cdots g_n \in G$ ohne Klammerung.

Definition 1.1.2. Ordnung

Für eine Gruppe G bezeichnen wir die Kardinalität

$$|G| \in \mathbb{N} \cup \{+\infty\} \tag{1.1.9}$$

als **Ordnung** von G.

1.2 Untergruppen

Definition 1.2.1. Untergruppe

Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $H \subseteq G$ heißt **Untergruppe**, falls gilt:
(U1) $H \neq \emptyset$
(U2) Abgeschlossenheit: Für alle $a, b \in H$ gilt $ab^{-1} \in H$.
Wir verwenden dann die Notation $H \leq G$, um Untergruppen zu kennzeichnen.

Bemerkung. Übungsaufgabe: Sei G eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt:

1. Aus Eigenschaft 1:Da $H \neq \emptyset$, existiert ein $a \in H$.
2. Aus Eigenschaft 2: $a \cdot a^{-1} = e \in H$.
3. Aus Eigenschaft 2: Für jedes $a \in H$ gilt $a^{-1} = e \cdot a^{-1} \in H$.
4. Aus Eigenschaft 2: Für jedes $a, b \in H$ gilt $ab = a \cdot (b^{-1})^{-1} \in H$.

Also: $H \subseteq G$ ist eine Untergruppe genau dann, wenn folgende alternativen Eigenschaften gelten:

1.* $e_G \in H$
2.* Für alle $a, b \in H$ muss $a \cdot b \in H$ gelten.
3.* Für alle $a \in H$ ist $a^{-1} \in H$.

Die andere Richtung der Äquivalenz ist trivial. Daraus folgt auch, dass $(H, \circ|_{H \times H})$ mit von G eingeschränkter Verknüpfung $\circ|_{H \times H}$ ist eine Gruppe.

Beispiele. Einige Beispiele für Untergruppen sind:

1. $(G, \circ) = (\mathbb{R}, +)$ hat $(\mathbb{Z}, +)$ als Untergruppe mit $\mathbb{Z} \subseteq \mathbb{R}$.
2. Sei $n \geq 1$ und $\mathbb{K}$ ein Körper. Die **spezielle lineare Gruppe**
$$\mathrm{SL}(n, \mathbb{K}) := \{A \in \mathrm{GL}(n, \mathbb{K}) \mid \det A = 1\} \leq \mathrm{GL}(n, \mathbb{K}) \tag{1.2.1}$$
ist eine Untergruppe von $\mathrm{GL}(n, \mathbb{K})$.
3. Für $n \geq$ und einen Körper $\mathbb{K}$ ist die **orthogonale Gruppe**
$$\mathrm{O}(n, \mathbb{K}) := \left\{A \in \mathrm{GL}(n, \mathbb{K}) \mid A^T A = I_n\right\} \leq \mathrm{GL}(n, \mathbb{K}) \tag{1.2.2}$$
definiert, die auch eine Untergruppe von $\mathrm{GL}(n, \mathbb{K})$ ist.
4. Seien $H_1, H_2 \leq G$ Untergruppen. Dann ist $H_1 \cap H_2 \leq G$ auch eine Untergruppe. So kann z.B. die **spezielle orthogonale Gruppe**
$$\mathrm{SO}(n, \mathbb{K}) := \mathrm{O}(n, \mathbb{K}) \cap \mathrm{SL}(n, \mathbb{K}) \tag{1.2.3}$$
als Untergruppe von $\mathrm{GL}(n, \mathbb{K})$ konstruiert werden.
5. Etwas allgemeiner: Für jede Familie $\{H_i\}_{i \in I}$ von Untergruppen $H_i \leq G$ gilt:
$$\bigcap_{i \in I} H_i \leq G \tag{1.2.4}$$
ist wieder eine Untergruppe.

Definition 1.2.2. Erzeugte Untergruppe

Sei G eine Gruppe und $M \subseteq G$ eine beliebige Teilmenge. Dann heißt die **Untergruppe**

$$\langle M \rangle := \bigcup_{M \subseteq H \leq G} H \leq G \tag{1.2.5}$$

die **von M erzeugte Untergruppe** von G.Falls $M = \{g\} \leq G$ eine einelementige Menge ist, schreiben wir

$$\langle g \rangle := \langle \{g\} \rangle \leq G. \tag{1.2.6}$$

Definition 1.2.3. Ordnung eines Elements

Sei G eine Gruppe und $g \in G$ ein Element. Dann heißt die Kardinalität

$$\mathrm{ord}(g) := |\langle g \rangle| \in \mathbb{N} \cup \{\infty\} \tag{1.2.7}$$

die **Ordnung von g**.

Satz 1.2.4. Charakterisierung von einelementigen Untergruppen

Sei G eine Gruppe und $g \in G$ ein Element.

1. Falls $\mathrm{ord}(g) < \infty$, dann gilt
$$\mathrm{ord}(g) = \min\{k \geq 1 | g^k = 1\} \tag{1.2.8}$$
und
$$\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}, \tag{1.2.9}$$
wobei $n := \mathrm{ord}(g)$.
2. Falls $\mathrm{ord}(g) = \infty$, dann gilt
$$\langle g \rangle = \{g^i | i \in \mathbb{Z}\} = \{\ldots, g^{-2}, g^{-1}, 1, g^1, g^2, \ldots\}, \tag{1.2.10}$$
wobei die Potenzen g^i, $i \in \mathbb{Z}$ paarweise verschiedene Elemente in G sind.

Beweis. Zunächst gilt für beliebiges $g \in G$ das Folgende:
$$\langle g \rangle = \{\ldots, g^{-2}, g^{-1}, 1, g, g^2, \ldots\} = \{g^i | i \in \mathbb{Z}\}, \tag{1.2.11}$$
wobei die Potenzen im Allgemeinen nicht notwendigerweise paarweise verschieden sind. Dies folgt, da, damit $\langle g \rangle$ eine Untergruppe sein kann, zunächst das neutrale Element $1 = g^0$ und g selbst enthalten sein muss. Dann muss aber auch die Selbstverknüpfung und das Inverse (sowie dessen Selbstverknüpfungen) enthalten sein.

1. Sei $\mathrm{ord}(g) < \infty$. Dann gibt es insbesondere $i, j \in \mathbb{Z}$ mit $i \neq j$ und $g^i = g^j$. O.B.d.A. sei $i > j$. Dann ist also $k = i - j \geq 1$ eine natürliche Zahl, für die gilt: $g^k = 1$. Nach dem Wohlordnungssatz existiert eine *kleinste* natürliche Zahl $n \geq 1$, für die gilt: $g^n = 1$. Sei nun $m \in \mathbb{Z}$. Dann gitb es eindeutig bestimmte Zahlen $a \in \mathbb{Z}$ und $0 \leq r < n$, sodass
$$m = an + r. \tag{1.2.12}$$
Damit folgt
$$g^m = g^{an+r} = (\underbrace{g^n}_{=1})^a \cdot g^r = g^r. \tag{1.2.13}$$
Dies impliziert $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$. Wir müssen noch zeigen, dass $1, g, \ldots, g^{n-1}$ paarweise verschieden sind. Dies folgt allerdings direkt aus der Tatsache, dass n minimal ist.
2. Das obige Argument zeigt per Kontraposition auch 2., denn wenn die Potenzen g^i, $i \in \mathbb{Z}$ nicht paarweise verschieden sind, dann zeigt obiges Argument, dass $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ für $n \in \mathbb{N}$, was ein Widerspruch zur Annahme $\mathrm{ord}(g) = \infty$ ist.

□

1.3 Homomorphismen

Definition 1.3.1. Homomorphismus

Seien G und G' Gruppen. Eine Abbildung
$$\phi : G \to G' \tag{1.3.1}$$
heißt **(Gruppen-)Homomorphismus**, falls gilt:

(H1) Für alle $g, h \in G$ gilt
$$\phi(gh) = \phi(g) \cdot \phi(h). \tag{1.3.2}$$
Die Menge der Homomorphismen von G nach G' wird mit $\mathrm{Hom}(G, G')$ bezeichnet.

Bemerkung. Jeder Homomorphismus erfüllt außerdem folgende Eigenschaften, die aus Definition 1.3.1 folgen:

(H2) $\phi(1_G) = 1_{G'}$

(H3) Für alle $g \in G$ gilt $\phi(g^{-1}) = \phi(g)^{-1}$.

Beispiele.

1. Die **Einbettung** $\phi : H \hookrightarrow G$ einer Untergruppe $H \leq G$ ist ein Homomorphismus.
2. Die **Determinantenabbildung**
$$\det : \mathrm{GL}(n, \mathbb{K}) \to (\mathbb{K}\backslash\{0\}, \cdot) \tag{1.3.3}$$
ist ein Homomorphismus.
3. Für $n \geq 1$ und einen Körper $\mathbb{K}$ ist die Permutationsabbildung
$$P : \mathfrak{S}_n \to \mathrm{GL}(n, \mathbb{K}) \tag{1.3.4}$$
$$\sigma \mapsto P_\sigma, \tag{1.3.5}$$
mit der **Permutation**
$$(P_\sigma)_{ij} := \begin{cases} 1 \,\text{falls}\, i = \sigma(j) \\ 0 \,\text{sonst} \end{cases} \tag{1.3.6}$$
ein Homomorphismus. *Der Beweis sei dem Leser überlassen.* Für $\sigma = (123) \in \mathfrak{S}_3$ gilt z.B.
$$P_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \tag{1.3.7}$$

4. Sei G eine Gruppe und $g \in G$. Dann ist
$$\gamma_g : G \to G \tag{1.3.8}$$
$$h \mapsto ghg^{-1} \tag{1.3.9}$$
ein Homomorphismus, genannt **Konjugation mit** g.
5. Sei G eine Gruppe und $g \in G$. Dann ist
$$\mathbb{Z} \to G \tag{1.3.10}$$
$$i \mapsto g^i \tag{1.3.11}$$
ein Homomorphismus von $(\mathbb{Z}, +)$ nach $(G, \circ)$.

Definition 1.3.2. Isomorphismus

Sei ϕ ein Gruppenhomomorphismus, der zusätzlich bijektiv ist. Dann heißt ϕ **Isomorphismus**. Zwei Gruppen G und G' heißen **isomorph**, in Zeichen $G \cong G'$, falls es einen Isomorphismus zwischen ihnen gibt.

Beispiel. Die Permutationsabbildung P induziert einen Isomorphismus
$$P : \mathfrak{S}_n \to P(n, \mathbb{K}) \tag{1.3.12}$$
$$\sigma \mapsto P_\sigma \tag{1.3.13}$$
zwischen der symmetrischen Gruppe und der Untergruppe der Permuationsmatrizen. Letztere sind Matrizen, die in jeder Zeile und Spalte *genau eine* 1 und sonst 0 haben. *Der Beweis sei dem Leser überlassen.*

Definition 1.3.3. Bild und Kern

Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann heißt die Teilmenge
$$\mathrm{im}(\phi) := \{g' \in G' | \exists g \in G : \phi(g) = g'\} \leq G', \tag{1.3.14}$$
das **Bild von** ϕ und die Teilmenge
$$\ker(\phi) := \{g \in G | \phi(g) = 1_{G'}\} \leq G, \tag{1.3.15}$$
der **Kern von** ϕ.

Satz 1.3.4. Bild und Kern sind Untergruppen

Sei $\phi : G \to G'$ ein Gruppenhomomorphismus. Dann sind $\mathrm{im}(\phi) \leq G'$ und $\ker(\phi) \leq G$ Untergruppen der jeweiligen Gruppen G und G'.

Beweis. Nachrechnen mittels (H1), (H2) und (H3), exemplarisch für den Kern gezeigt:
1. (U1) ist erfüllt, da $1_G \in \ker(\phi)$ wegen (H2) gilt.
2. (U2) kann nachgerechnet werden. Seien dafür $g, h \in \ker(\phi)$:
$$\phi(gh^{-1}) =^{(H1)} \phi(g) \cdot \phi(h^{-1}) =^{(H3)} \phi(g) \cdot \phi(h)^{-1} = 1_{G'}, \tag{1.3.16}$$
also $gh^{-1} \in \ker(\phi)$.

□

Satz 1.3.5

Für einen Homomorphismus $\phi : G \to G'$ sind folgende Aussagen äquivalent:
(i) ϕ ist injektiv.
(ii) $\ker(\phi) = \{1\}$

Beweis. (i) $\Rightarrow$ (ii) ist offensichtlich. Wir zeigen noch (ii) $\Rightarrow$ (i): Sei also $\ker(\phi) = \{1\}$ und $g, h \in G$ mit $\phi(g) = \phi(h)$. Dann gilt $\phi(gh^{-1}) = \phi(g)\phi(h)^{-1} = 1$, also ist $gh^{-1} \in \ker(\phi) = \{1\}$ und damit $g = h$. □