
Algebra (Bachelor)

zur Vorlesung von Prof. Dr. Tobias Dyckerhoff

23. Oktober 2024

Inhaltsverzeichnis

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

Konventionen

- Wir schreiben für einen Körper \mathbb{K} kurz $\mathbb{K}^* := \mathbb{K} \setminus \{0\}$.
- Real- und Imaginärteil werden mit $\operatorname{Re}(\cdot)$ respektive $\operatorname{Im}(\cdot)$ bezeichnet, das Bild einer Abbildung f hingegen mit $\operatorname{im}(f)$.

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

$$\circ : G \times G \rightarrow G \quad (1.1.1)$$

$$(g, h) \mapsto g \circ h \quad (1.1.2)$$

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 (2G) heißt **neutrales Element**, und ein Element $g' \in G$ zu gegebenem $g \in G$ mit Eigenschaft (2b) heißt **Inverses** von g .

^aim 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, \dots, 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 $(\mathbb{K} \setminus \{0\}, \cdot)$.
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 $\mathfrak{S}_n := \mathfrak{S}_{\{1, 2, \dots, n\}}$. Wir vereinbaren als Konvention die **Zykelschreibweise**. In \mathfrak{S}_3 beispielsweise ist ein Zykel

$$\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\} \quad (1.1.3)$$

$$1 \mapsto 2 \quad (1.1.4)$$

$$2 \mapsto 1 \quad (1.1.5)$$

$$3 \mapsto 3, \quad (1.1.6)$$

auch darstellbar als

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad (1.1.7)$$

oder einfacher als (12).

4. Für $n \geq 1$ und einen Körper \mathbb{K} ist die **allgemeine lineare Gruppe** $(\text{GL}(n, \mathbb{K}), \circ)$ definiert, wobei

$$\text{GL}(n, \mathbb{K}) := \{A \in \mathbb{K}^{n \times n} \mid \det A \neq 0\} \quad (1.1.8)$$

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: $|\text{GL}(n, \mathbb{F}_q)| = ?$.

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

$$|G| \in \mathbb{N} \cup \{+\infty\} \quad (1.1.9)$$

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 der auf H eingeschränkten Verknüpfung $\circ|_{H \times H}$ eine Gruppe ist.

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**

$$\mathrm{SL}(n, \mathbb{K}) := \{A \in \mathrm{GL}(n, \mathbb{K}) \mid \det A = 1\} \leq \mathrm{GL}(n, \mathbb{K}) \quad (1.2.1)$$

ist eine Untergruppe von $\mathrm{GL}(n, \mathbb{K})$.

3. Für $n \geq 1$ und einen Körper \mathbb{K} ist die **orthogonale Gruppe**

$$\mathrm{O}(n, \mathbb{K}) := \{A \in \mathrm{GL}(n, \mathbb{K}) \mid A^T A = I_n\} \leq \mathrm{GL}(n, \mathbb{K}) \quad (1.2.2)$$

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**

$$\mathrm{SO}(n, \mathbb{K}) := \mathrm{O}(n, \mathbb{K}) \cap \mathrm{SL}(n, \mathbb{K}) \quad (1.2.3)$$

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, dass

$$\bigcap_{i \in I} H_i \leq G \quad (1.2.4)$$

wieder eine Untergruppe ist.

Definition 1.2.2. Erzeugte Untergruppe

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

$$\langle M \rangle := \bigcup_{M \subseteq H \leq G} H \leq G \quad (1.2.5)$$

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

$$\langle g \rangle := \langle \{g\} \rangle \leq G. \quad (1.2.6)$$

Definition 1.2.3. Ordnung eines Elements

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

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

die **Ordnung von g** und $\langle g \rangle$ **zyklisch** der Ordnung $\mathrm{ord}(g)$.

Satz 1.2.4. Charakterisierung von einelementigen Untergruppen

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

1. Falls $\text{ord}(g) < \infty$, dann gilt

$$\text{ord}(g) = \min\{k \geq 1 \mid g^k = 1\} \quad (1.2.8)$$

und

$$\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}, \quad (1.2.9)$$

wobei $n := \text{ord}(g)$.

2. Falls $\text{ord}(g) = \infty$, dann gilt

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\} = \{\dots, g^{-2}, g^{-1}, 1, g^1, g^2, \dots\}, \quad (1.2.10)$$

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:

$$\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\} = \{g^i \mid i \in \mathbb{Z}\}, \quad (1.2.11)$$

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 $\text{ord}(g) < \infty$. 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 gibt es eindeutig bestimmte Zahlen $a \in \mathbb{Z}$ und $0 \leq r < n$, sodass

$$m = an + r. \quad (1.2.12)$$

Damit folgt

$$g^m = g^{an+r} = \underbrace{(g^n)^a}_{=1} \cdot g^r = g^r. \quad (1.2.13)$$

Dies impliziert $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$. Wir müssen noch zeigen, dass $1, g, \dots, g^{n-1}$ 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 $\langle g \rangle = \{1, g, \dots, g^{n-1}\}$ für $n \in \mathbb{N}$, was ein Widerspruch zur Annahme $\text{ord}(g) = \infty$ ist.

□

1.3 Homomorphismen

Definition 1.3.1. Homomorphismus

Seien G und G' Gruppen. Eine Abbildung

$$\phi : G \rightarrow G' \quad (1.3.1)$$

heißt **(Gruppen-)Homomorphismus**, falls gilt:

(H1) Für alle $g, h \in G$ gilt

$$\phi(gh) = \phi(g) \cdot \phi(h). \quad (1.3.2)$$

Die Menge der Homomorphismen von G nach G' wird mit $\text{Hom}(G, G')$ 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**

$$\det : \text{GL}(n, \mathbb{K}) \rightarrow (\mathbb{K} \setminus \{0\}, \cdot) \quad (1.3.3)$$

ist ein Homomorphismus.

3. Für $n \geq 1$ und einen Körper \mathbb{K} ist die Permutationsabbildung

$$P : \mathfrak{S}_n \rightarrow \text{GL}(n, \mathbb{K}) \quad (1.3.4)$$

$$\sigma \mapsto P_\sigma, \quad (1.3.5)$$

mit der **Permutation**

$$(P_\sigma)_{ij} := \begin{cases} 1 & \text{falls } i = \sigma(j) \\ 0 & \text{sonst} \end{cases} \quad (1.3.6)$$

ein Homomorphismus. *Der Beweis sei dem Leser überlassen.* Für $\sigma = (123) \in \mathfrak{S}_3$ gilt z.B.

$$P_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \quad (1.3.7)$$

4. Sei G eine Gruppe und $g \in G$. Dann ist

$$\gamma_g : G \rightarrow G \quad (1.3.8)$$

$$h \mapsto ghg^{-1} \quad (1.3.9)$$

ein Homomorphismus, genannt **Konjugation mit g** .

5. Sei G eine Gruppe und $g \in G$. Dann ist

$$\mathbb{Z} \rightarrow G \quad (1.3.10)$$

$$i \mapsto g^i \quad (1.3.11)$$

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.

Bemerkung. Anschaulich bedeutet das, dass zwei isomorphe Gruppen identisch bis auf Umbenennung ihrer Elemente sind.

Beispiele. 1. Die Permutationsabbildung P induziert einen Isomorphismus

$$P : \mathfrak{S}_n \rightarrow P(n, \mathbb{K}) \quad (1.3.12)$$

$$\sigma \mapsto P_\sigma \quad (1.3.13)$$

zwischen der symmetrischen Gruppe und der Untergruppe der Permutationsmatrizen. Letztere sind Matrizen, die in jeder Zeile und Spalte *genau eine* 1 und sonst 0 haben. *Der Beweis sei dem Leser überlassen.*

2. Die **Exponentialfunktion**

$$\exp : (\mathbb{R}, +) \rightarrow (\mathbb{R}_{>0}, \cdot) \quad (1.3.14)$$

und ihre Umkehrfunktion, gegeben durch den **Logarithmus**

$$\ln : (\mathbb{R}_{>0}, \cdot) \rightarrow (\mathbb{R}, +), \quad (1.3.15)$$

bilden einen Isomorphismus, also gilt $(\mathbb{R}, +) \cong (\mathbb{R}_{>0}, \cdot)$.

Definition 1.3.3. Bild und Kern

Sei $\phi : G \rightarrow G'$ ein Gruppenhomomorphismus. Dann heißt die Teilmenge

$$\text{im}(\phi) := \{g' \in G' \mid \exists g \in G : \phi(g) = g'\} \leq G', \quad (1.3.16)$$

das **Bild von ϕ** und die Teilmenge

$$\ker(\phi) := \{g \in G \mid \phi(g) = 1_{G'}\} \leq G, \quad (1.3.17)$$

der **Kern von ϕ** .

Satz 1.3.4. Bild und Kern sind Untergruppen

Sei $\phi : G \rightarrow G'$ ein Gruppenhomomorphismus. Dann sind $\text{im}(\phi) \leq G'$ 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 $g, h \in \ker(\phi)$:

$$\phi(gh^{-1}) \stackrel{(H1)}{=} \phi(g) \cdot \phi(h^{-1}) \stackrel{(H3)}{=} \phi(g) \cdot \phi(h)^{-1} = 1_{G'}, \quad (1.3.18)$$

also $gh^{-1} \in \ker(\phi)$.

□

Satz 1.3.5

Für einen Homomorphismus $\phi : G \rightarrow G'$ 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 $g = h$. □

Definition 1.3.6. Links- und Rechtsnebenklassen

Sei G eine Gruppe und $H \leq G$ eine Untergruppen. Dann ist die **Linksnebenklasse von H bezüglich g** als

$$gH := \{gh \mid h \in H\} \quad (1.3.19)$$

und die **Rechtsnebenklasse von H bezüglich g** als

$$Hg := \{hg \mid h \in H\} \quad (1.3.20)$$

definiert.

Satz 1.3.7. Nebenklassen sind Äquivalenzklassen

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

1. Die Linksnebenklassen sind die Äquivalenzklassen bezüglich der Äquivalenzrelation

$$a \sim_L b :\Leftrightarrow b^{-1}a \in H \quad (1.3.21)$$

auf G .

2. Die Rechtsnebenklassen sind die Äquivalenzklassen bezüglich der analogen Äquivalenzrelation

$$a \sim_R b :\Leftrightarrow ab^{-1} \in H. \quad (1.3.22)$$

Beweis. Dem Leser als Übung überlassen. Es ist insbesondere auch zu zeigen, dass \sim tatsächlich eine Äquivalenzrelation definiert. \square

Damit bezeichnen wir die Menge der Linksnebenklassen von H mit $G/H = G/\sim_L$ und die der Rechtsnebenklassen mit $G/H = G/\sim_R$. **Hier Quotient umdrehen!**

Definition 1.3.8. Index

Die Kardinalität

$$(G : H) := |G/H| \in \mathbb{N} \cup \{\infty\} \quad (1.3.23)$$

heißt **Index von H in G** .

Man beachte, dass $|H/G| = |H/G|$ [**Hier auch Quotient umdrehen!**] gilt, da die Abbildung

Theorem 1.3.9. Satz von Lagrange

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

$$|G| = (G : H) \cdot |H|. \quad (1.3.24)$$

Ist $|G| < \infty$, so gilt insbesondere

$$(G : H) = \frac{|G|}{|H|} = |G/H|. \quad (1.3.25)$$

Beweis. Dies ist ein direktes Korollar von Satz 1.3.7: Als Äquivalenzklassen bzgl. einer Äquivalenzrelation bilden die Linksklassen eine Partition von G , also

$$G = \bigsqcup_{gH \in G/H} gH. \quad (1.3.26)$$

Es gilt zudem für alle $g \in G$, dass $|gH| = |H|$, da Linksmultiplikation mit g , definiert durch

$$G \rightarrow G \quad (1.3.27)$$

$$x \mapsto gx, \quad (1.3.28)$$

bijektiv ist, also eine Bijektion $H \rightarrow gH$ induziert. Insbesondere gilt für jedes $g \in G$, dass $\text{ord}(g) \mid |G|$. \square

Definition 1.3.10. Normalteiler

Eine Untergruppe $N \leq G$ heißt **normal** oder **Normalteiler**, falls für alle $g \in G$

$$gN = Ng \quad (1.3.29)$$

gilt. Wir schreiben dafür $N \trianglelefteq G$.

Bemerkung. Eine Untergruppe $N \leq G$ ist normal genau dann, wenn für alle $g \in G$ und $n \in N$ gilt:

$$gng^{-1} \in N, \quad (1.3.30)$$

also N abgeschlossen unter Konjugation mit beliebigen Elementen aus G ist.

Satz 1.3.11. S

Sei $\phi : G \rightarrow G'$ ein Gruppenhomomorphismus. Dann gilt $\ker(\phi) \trianglelefteq G$.

Beweis. Sei $g \in G$ und $x \in \ker(\phi)$, also $\phi(x) = 1$. Dann gilt auch

$$\phi(gxg^{-1}) = \phi(g)\underbrace{\phi(x)}_{=1}\phi(g^{-1}) = \phi(g)\phi(g)^{-1} = 1. \quad (1.3.31)$$

\square

Beispiele. Wir betrachten einige Beispiele für Normalteiler:

1. Sei $n \geq 1$ und \mathbb{K} ein Körper. Für

$$\det : \mathrm{GL}(n, \mathbb{K}) = \mathbb{K}^* \quad (1.3.32)$$

gilt

$$\ker(\det) = \mathrm{SL}(n, \mathbb{K}) \trianglelefteq \mathrm{GL}(n, \mathbb{K}). \quad (1.3.33)$$

2. Betrachte für $n \geq 1$ die Komposition

$$\mathfrak{S}_n \xrightarrow{P} P(n, \mathbb{Q}) \xrightarrow{\det} \{+1, -1\}.$$

Also ist

$$A_n := \ker(\mathrm{sgn}) \trianglelefteq \mathfrak{S}_n \quad (1.3.34)$$

normal. A_n heißt **alternierende Gruppe**.

Satz 1.3.12. Gruppenstruktur auf Nebenklassen

Sei G eine Gruppe und $N \trianglelefteq G$. Dann gilt:

1. Auf der Menge G/N von Nebenklassen von N existiert eine Gruppenstruktur mit Verknüpfung

$$G/N \times G/N \rightarrow G/N \quad (1.3.35)$$

$$(aN, bN) \mapsto abN. \quad (1.3.36)$$

2. Die Quotientenabbildung

$$\pi : G \rightarrow G/N \quad (1.3.37)$$

$$a \mapsto aN \quad (1.3.38)$$

ist ein Gruppenhomomorphismus mit $\ker(\pi) = N$.

Beweis.

1. Zunächst muss die Wohldefiniertheit der Verknüpfung bewiesen werden. Seien $\tilde{a} \in aN$ und $\tilde{b} \in bN$ Vertreter der Nebenklassen aN und bN ($\Leftrightarrow \tilde{a}N = aN$). Dann existieren $m, n \in N$ mit $\tilde{a} = am$ und $\tilde{b} = bn$. Nun gilt

$$\tilde{a} \cdot \tilde{b} = am \cdot bn = ab \cdot \underbrace{m^{-1}mb}_{N \trianglelefteq G \Rightarrow \in N} n \in N, \quad (1.3.39)$$

also ist der Ausdruck wohldefiniert.

(G1) Seien $aN, bN, cN \in G/N$. Dann gilt

$$(aN \cdot bN) \cdot cN \stackrel{(G1)}{=} (ab)cN = a(bc)N = aN(bN \cdot cN). \quad (1.3.40)$$

(G2) Neutrales Element: $1 \cdot N = N$

(G3) Inverses Element: $(aN)^{-1} = a^{-1}N$

2. Es gilt

$$\pi(ab) = (ab)N = (aN)(bN) = \pi(a)\pi(b) \quad (1.3.41)$$

nach Definition von π , also ist π ein Homomorphismus. Darüber hinaus gilt

$$a \in \ker(\pi) \Leftrightarrow \pi(a) = 1_{G/H} = N \Leftrightarrow aN = N \Leftrightarrow a \in N, \quad (1.3.42)$$

also gilt $\ker(\pi) = N$.

□

Satz 1.3.13. Homomorphiesatz (erster Isomorphiesatz)

Sei $\phi : G \rightarrow G'$ ein Gruppenhomomorphismus. Dann induziert ϕ einen Isomorphismus

$$\bar{\phi} : G/\ker(\phi) \rightarrow \mathrm{im}(\phi) \quad (1.3.43)$$

$$g \ker(\phi) \mapsto \phi(g). \quad (1.3.44)$$

Beweis. Zunächst ist Wohldefiniertheit zu zeigen. Für $\tilde{g} \in gN$, also $\tilde{g} = gn$ für $n \in \ker(\phi)$, gilt:

$$\phi(\tilde{g}) = \phi(gn) = \phi(g) \underbrace{\phi(n)}_{=1} = \phi(g), \quad (1.3.45)$$

also ist die Abbildung wohldefiniert.

Die Surjektivität von $\bar{\phi}$ ist trivial. Wir wissen, dass $\bar{\phi}$ genau dann injektiv ist, wenn $\ker(\bar{\phi}) = \{1_{G/\ker(\phi)}\} = \ker(\phi)$.

Wir rechnen nach:

$$g \ker(\phi) \in \ker(\bar{\phi}) \Leftrightarrow \phi(g) = 1_{G'} \Leftrightarrow g \in \ker(\phi) \Leftrightarrow g \ker(\phi) = \ker(\phi) \quad (1.3.46)$$

□