1 Gruppen

1.1 Grundlagen

1.2 Homomorphie- und Isomorphiesätze

Sind G und G' Gruppen und $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann gilt:

$$G/\mathrm{Kern}(\varphi) \cong \mathrm{Bild}(\varphi)$$

Beispiele 1.1 (a) $G/Z(G) \cong \mathrm{Aut}_i(G)$

Satz 1

Sei G eine Gruppe, $N \subseteq G$ ein Normalteiler und $H \subseteq G$ eine Untergruppe.

(a) Es gilt:

$$H/(H \cap N) \cong HN/N$$

Dabei sei $HN := \{h \cdot n : h \in H, n \in N\}$

(b) Ist $N \subseteq H$ und H ein Normalteiler in G, so gilt:

$$(G/N)/(H/N) \cong G/H$$

1.2.1 Exakte Sequenzen

Definition + Bemerkung 1.2 1. Eine Sequenz

$$1 \longrightarrow G_0 \longrightarrow \cdots \longrightarrow G_{i-1} \xrightarrow{\varphi_i} G_i \xrightarrow{\varphi_{i+1}} G_{i+1} \longrightarrow \cdots \longrightarrow G_n \longrightarrow 1$$

von Gruppenhomomorphismen heißt *exakt an der Stelle G_i*, wenn

$$\mathrm{Bild}(\varphi_i) = \mathrm{Kern}(\varphi_{i+1})$$

gilt. Die Sequenz heißt *exakt*, wenn sie an jeder Stelle exakt ist.

2. Eine Sequenz

$$1 \longrightarrow G' \xrightarrow{\alpha} G \xrightarrow{\beta} G'' \longrightarrow 1$$

von Gruppenhomomorphismen heißt *kurze Sequenz*.

3. Eine kurze Sequenz ist genau dann exakt, wenn die folgenden Bedingungen erfüllt sind:

a) α ist injektiv (sprich: man kann G' als Untergruppe von G auffassen)

b) β ist surjektiv

c) $\mathrm{Bild}(\alpha) = \mathrm{Kern}(\beta)$

Beispiele 1.3

Ist G eine Gruppe und $N \trianglelefteq G$, so ist die folgende kurze Sequenz exakt:

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1$$

Eine kurze exakte Sequenz *spaltet*, wenn es einen Gruppenhomomorphismus $\gamma : G'' \longrightarrow G$ gibt mit $\beta \circ \gamma = \mathrm{id}_{G''}$.

$$1 \longrightarrow G' \xrightarrow{\alpha} G \underset{\xleftarrow{\gamma}}{\xrightarrow{\beta}} G'' \longrightarrow 1$$

In diesem Fall ist γ injektiv, man kann also auch G'' als Untergruppe von G auffassen.

1.3 Kommutatoren

Bemerkung 1.4

Grundlegende Eigenschaften von Kommutatoren.

1. Genau dann ist eine Gruppe G abelsch, wenn $K(G) = \{e\}$.

Bemerkung 1.5

Kommutatoren und Homomorphismen.

Seien G und G' eine Gruppen und $\varphi : G \to G'$ ein Gruppenhomomorphismus.

(a) $\varphi([a, b]) = [\varphi(a), \varphi(b)]$.

(b) $\varphi(K(G)) \subseteq K(G')$

(c) Ist φ zudem noch surjektiv, so gilt: $\varphi(K(G)) = K(G') = K(\varphi(G))$.

Beweis:

(a) $\varphi([a, b]) = \varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} = [\varphi(a), \varphi(b)]$

(b) Sei $[a, b] \in K(G)$. Dann ist $\varphi([a, b]) = [\varphi(a), \varphi(b)] \in K(G')$

(c) Sei $[a', b'] \in K(G')$. Da φ surjektiv ist, gibt es $a, b \in G$ mit $\varphi(a) = a'$ und $\varphi(b) = b'$. Dann gilt $[a', b'] = [\varphi(a), \varphi(b)] = \varphi([a, b]) \in \varphi(K(G))$. ■

Bemerkung 1.6

Kommutatoren und Normalteiler.

Es sei G eine Gruppe.

(a) Es sei $N \trianglelefteq G$.
Genau dann ist G/N abelsch, wenn $K(G) \subseteq N$.

(b) $G^{ab} := G/K(G)$ ist eine abelsche Gruppe.

Beweis:

(a) $\Rightarrow$ Es sei G abelsch. Also: $K(G) = \{e\} \subseteq N$.

$\Leftarrow$ Es sei $K(G) \subseteq N$ und $\pi : G \to G/N$ die kanonische Projektion. Da π surjektiv ist, gilt: $\pi(K(G)) = K(\pi(G)) = K(G/N)$. Da $K(G) \subseteq N$, ist $K(G/N) = \{N\}$. Also ist G/N abelsch.

(b) Blatt 3, Aufgabe 1, a).

(c) Blatt 3, Aufgabe 1, b). ■

Beispiele 1.7 1. Symmetrische Gruppe:

a) $K(S_1) =$

b) $K(S_n) = A_n$ (für $n \geq 2$)

2. Alternierende Gruppe:

a) $K(A_2) = K(A_3) = \{\mathrm{id}\}$

b) $K(A_4) = V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (kleinsche Vierergruppe)

c) $K(A_n) = A_n$ (für $n \geq 5$)

3. Diedergruppe.

1.4 Konstruktion von Gruppen

1.4.1 Direktes Produkt

1.4.2 Semidirektes Produkt

Seien H, N Gruppen und $\phi : H \to \mathrm{Aut}(N)$ ein Gruppenhomomorphismus. Auf der Menge $G := N \times H$ definiert man eine Verknüpfung $\star$ wie folgt:

$$(n_1, h_1) \star (n_2, h_2) := (n_1\phi(h_1)(n_2), h_1h_2),$$

wobei jeweils die Verknüpfungen in N bzw. H verwendet werden.
$(G, \star)$ heißt *semidirektes Produkt* von H mit N.
G ist eine Gruppe, die $N \times \{e_H\}$ als Normalteiler und $\{e_N\} \times H$ als Untergruppe enthählt.

Bemerkung 1.8
(Splitting Lemma)
Sei

$$1 \longrightarrow G' \xrightarrow{\alpha} G \xrightarrow{\beta} G'' \longrightarrow 1$$

eine kurze exakte Sequenz, die spaltet. Das bedeutet, dass es einen Gruppenhomomorphismus $\gamma : G'' \to G$ gibt mit $\beta \circ \gamma = \mathrm{id}_{G''}$

G ist dann bezüglich einer geeigneten Abbildung $\varphi : G'' \longrightarrow \mathrm{Aut}(G')$ ein semidirektes Produkt von G' und G''.

Setze

$$\varphi(h)(n) := \alpha^{-1}(\gamma(h)\alpha(n)\gamma(h^{-1}))$$

Da α und γ injektiv sind, kann man sich G' ung G'' als Untergruppe von G vorstellen. In diesem Fall ergibt sich

$$\varphi(h)(n) := hnh^{-1}$$

1.5 Eigenschaften von Gruppen

1.5.1 Zyklische Gruppen

Definition + Bemerkung 1.9 (a) G heißt zyklisch, wenn es ein $g \in G$ gibt mit $G = \langle g \rangle$.

1.5.2 Abelsche Gruppen

Definition + Bemerkung 1.10 (a) A heißt **freie abelsche Gruppe** mit Basis X, wenn jedes $a \in A$ eine eindeutige Darstellung $a = \sum\limits_{x \in X} n_x x$ hat mit $n_x \in \mathbb{Z}$, $n_x \neq 0$ nur für endlich viele $x \in X$. Ist in dieser Situation $|X| = n$, so heißt n der **Rang** von A. A ist isomorph zu $\mathbb{Z}^X := \bigoplus\limits_{x \in X} \mathbb{Z}$

(b) (UAE der freien abelschen Gruppe)
Zu jeder abelschen Gruppe A und jeder Abbildung $f : X \to A$ gibt es genau einen Homomorphismus $\varphi : \mathbb{Z}^X \to A$ mit $\forall x \in X : \varphi(x) = f(x)$

Beispiele 1.11

X endlich, $X = \{x_1, \dots, x_n\}$. Dann ist $\mathbb{Z}^X \cong \mathbb{Z}^n$

$\mathbb{Z}^n$ ist "so etwas ähnliches" wie ein Vektorraum *("freier Modul")*. Insbesondere lassen sich die Gruppenhomomorphismen $\mathbb{Z}^n \to \mathbb{Z}^m$ durch eine $m \times n$-Matrix mit Einträgen in $\mathbb{Z}$ beschreiben.

Satz 2 (Elementarteilersatz)

Sei H eine Untergruppe von $\mathbb{Z}^n$ ($n \in \mathbb{N} \setminus \{0\}$). Dann gibt es eine Basis $\{x_1, \dots, x_n\}$ von $\mathbb{Z}^n$, ein $r \in \mathbb{N}$ mit $0 \leq r \leq n$ und $a_1, \dots, a_r \in \mathbb{N} \setminus \{0\}$ mit a_i teilt a_{i+1} fr̈ $i = 1, \dots, r-1$, so daß $a_1 x_1, \dots, a_r x_r$ eine Basis von H ist. Insbesondere ist H ebenfalls eine freie abelsche Gruppe.

Klassifizierung:

Satz 3 (Struktursatz für endlich erzeugte abelsche Gruppen)
Sei A endlich erzeugte abelsche Gruppe.

$$\Rightarrow A \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$$

mit $a_1, \dots, a_m \in \mathbb{N}$, $\forall i : a_i \geq 2$, a_i teilt a_{i+1} für $i = 1, \dots, m-1$. Dabei sind r, m und die a_i eindeutig bestimmt.

Abgeschlossenheit:

1. Untergruppen abelscher Gruppen sind abelsch.
2. Faktorgruppen abelscher Gruppen sind abelsch.
3. Produkte abelscher Gruppen sind abelsch.
4. Direkte Summen abelscher Gruppen sind abelsch.
5. Seien G, G' Gruppen, $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus.
   Ist G abelsch, so ist $\varphi(G)$ auch abelsch.

Beispiele für abelsche Gruppen:

- zyklische Gruppen
- Gruppen der Ordnung p oder p^2
- $\mathrm{Aut}(G)$ ist zyklisch
- $G = H/[H, H]$
- Für alle $x \in G$ gilt $x^2 = e$.

Beispiele für *nicht* abelsche Gruppen:

- D_n
- S_n (für $n \geq 3$)
- A_n (für $n \geq 4$)

1.5.3 Einfache Gruppen

Beispiele 1.12 (a) Es gibt keine einfachen Gruppen der Ordnung 21.

Beweis: Die Sätze von Sylow liefern, dass es nur eine 7-Sylowgruppe gibt. Diese muss also auch Normalteiler sein. ■

(b) Es gibt keine einfachen Gruppen der Ordnung 30.

Beweis: Es sei G eine Gruppe der Ordnung 30. Die Sätze von Sylow liefern $s_3 \in \{1, 10\}$ und $s_5 \in \{1, 6\}$. Falls $s_3 = 1$ oder $s_5 = 1$ gilt, so gibt es nach dem vorigen Argument einen Normalteiler in G. Es gelte also im folgenden $s_3 = 10$ und $s_5 = 6$. Die 5-Sylowgruppen sind zyklisch und bis auf das Neutralelement disjunkt. In den 5-Sylowgruppen liegen also $6 \cdot 4 = 25$ Elemente ($\neq e_G$). Die 3-Sylowgruppen sind zyklisch und bis auf das Neutralelement diskunkt. In den 3-Sylowgruppen liegen also $10 \cdot 2 = 20$ Elemente ($\neq e_G$). Je eine 3-Sylowgruppe und eine 5-Sylowgruppe schneiden sich trivial. Es gibt also mindestens $25 + 20 + 1 = 46$ Elemente in G. Widerspruch. ■

(c) Es gibt keine einfachen Gruppen der Ordnung 36.

Beweis: Es sei G eine Gruppe der Ordnung 36. Die Sätze von Sylow liefern $s_2 \in \{1, 3, 9\}$ und $s_3 \in \{1, 4\}$. Ohne Einschränkung gelte $s_3 = 4$. Je 2 3-Sylowgruppen sind konjugiert, deshalb operiert G auf der Menge M der 3-Sylowgruppen durch Konjugation (nichttrivial). Nenne diese 3-Sylowgruppen $M = \{1, 2, 3, 4\}$. Man erhählt durch diese Operation einen Gruppenhomomorphismus $\varphi : G \to \mathrm{Perm}(M) = S_4$. φ ist nicht injektiv, da $|G| = 36$, $|S_4| = 24$. φ ist nicht der triviale Homomorphismus, da G nichttrivial auf M operiert. $\mathrm{Kern}(\varphi)$ ist also ein echter, nichttrivialer Normalteiler in G. ■

(d) Es gibt keine einfachen Gruppen der Ordnung 300.

Beweis: Es sei G eine Gruppe der Ordnung 300. Die Sätze von Sylow liefern $s_2 \in \{1, 3, 5, 15, 25, 75\}$, $s_3 \in \{1, 4, 10, 25, 100\}$ und $s_5 \in \{1, 6\}$. Ohne Einschränkung gelte $s_5 = 6$. Je 2 5-Sylowgruppen sind konjugiert, deshalb operiert G auf der Menge M der 5-Sylowgruppen durch Konjugation (nichttrivial). Nenne diese 5-Sylowgruppen $M = \{1, 2, 3, 4, 5, 6\}$. Man erhählt durch diese Operation einen Gruppenhomomorphismus $\varphi : G \to \mathrm{Perm}(M) = S_6$. $|G| = 300$ ist kein Teiler von $|S_6| = 720$, also ist φ nicht injektiv. φ ist nicht der triviale Homomorphismus, da G nichttrivial auf M operiert. $\mathrm{Kern}(\varphi)$ ist also ein echter, nichttrivialer Normalteiler in G. ■

(e) Gruppen der Ordnung $2m$ (m ungerade) enthalten einen Normalteiler der Ordnung m. Hinweis: Satz von Cayley. Zeige, dass eine Untergruppe der S_n, die eine ungerade Permutation enthält, einen Normalteiler von Index 2 besitzt (Isomorphiesätze).

Beweis: Es sei U eine Untergruppe der S_n, $\sigma \in U \setminus A_n$ (d.h. σ ungerade). A_n ist ein Normalteiler in S_n, U ist eine Untergruppe in S_n, also ist nach den Isomorphiesätzen UA_n eine Untergruppe von S_n und $U \cap A_n$ ein Normalteiler in U. Weiter gilt: $U/(U \cap A_n) \cong UA_n/A_n$. Andererseits ist $UA_n \lneq A_n \leq S_n$. Da $(S_n : A_n) = 2$ muss also $UA_n = S_n$ gelten. Einsetzen: $U/(U \cap A_n) \cong S_n/A_n$. Insbesondere: $(U : (U \cap A_n)) = (S_n : A_n) = 2$

Zu der eigentlichen Aussage: Sei G eine Gruppe der Ordnung $2m$, m ungerade. Nach dem Satz von Cayley ist $\tau : G \to \mathrm{Perm}(G),\ g \mapsto \tau_g$ ein injektiver Homomorphismus (τ_g: Konjugation mit g). Nummeriert man die Elemente von G durch, so kann man den Homomorphismus auch als $\tau : G \to S_{2m}$ auffassen. Da τ injektiv ist, ist $U := \tau(G)$ eine Untergruppe von S_n und $U \cong G$. In G gibt es ein Element der Ordnung 2 (Sylow), in U also auch. Es sei also $\sigma \in U$ mit $\mathrm{ord}(\sigma) = 2$.
to be continued ■

1.5.4 Auflösbare Gruppen

Definition + Bemerkung 1.13 (a) Eine Gruppe heißt *auflösbar*, wenn sie eine Normalreihe mit abelschen Faktorgruppen besitzt.

(b) Eine endliche Gruppe ist genau dann auflösbar, wenn die Faktoren in ihrer Kompositionsreihe zyklisch von Primzahlordnung sind.

(c) Sei
$$1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1$$
eine kurze exakte Sequenz von Gruppen. Dann gilt:
G ist auflösbar $\Leftrightarrow$ G' und G'' sind auflösbar.
Ist N ein Normalteiler in G, so gilt also:
G ist auflösbar $\Leftrightarrow$ N und G/N sind auflösbar.

1.5.5 Freie Gruppen

1.6 Monographien von Gruppen

1.6.1 Symmetrische Gruppe

Eigenschaften:

- Anzahl der Elemente: $|S_n| = n!$
- Im allgemeinen *nicht* abelsch.

1.6.2 Alternierende Gruppe

Eigenschaften:

- Anzahl der Elemente: $|A_n| = n!/2$
- Im allgemeinen *nicht* abelsch.

1.6.3 Diedergruppe

- Definition: $D_n :=< D, S >$, $\mathrm{ord}(D) = n$, $\mathrm{ord}(S) = n$
- Anzahl der Elemente: $|D_n| = 2n$
- Im allgemeinen *nicht* abelsch.

Charakterisierende Eigenschaft:

- Es gibt ein Element S der Ordnung 2.
- Es gibt ein Element D der Ordnung n.
- $SD = D^{-1}S$

Rechenregeln in der Diedergruppe

1. $D^n = e$
2. $S^2 = e$
3. $(D^iS)^2 = e$
4. $SD = D^{-1}S$
5. $SD^i = D^{n-i}S$

Weitere Eigenschaften:

1. Zentralisator: $< D >$

Beispiele 1.14

- D_6, $N :=< D^3 > \trianglelefteq D_6$
- D_{12}, $N :=< D^3 > \trianglelefteq D_{12}$
  D_{12}/N ist nicht abelsch.

1.7 Bestimmung aller Isomorphieklassen

Einige Kandidaten für Untergruppen:

- Zyklische Gruppen
- Abelsche Gruppen
- Diedergruppe D_n
- Alternierende Gruppe A_n
- Kleinsche Vierergruppe V_4
- Quaternionengruppe

Bestimmen Sie alle Isomorphieklassen von Gruppen der Ordnung n.

- Satz von Lagrange
- Sätze von Sylow
- abelsch oder nicht abelsch? (Klassifizierung endlicher abelscher Gruppen)

Spezialfälle

- $n = p$ Primzahl (nur die zyklische Gruppe)
- $n = p^2$, p Primzahl ($\mathbb{Z}_{p^2}$ oder $\mathbb{Z}_p \times \mathbb{Z}_p$)
- $n = 2p$, $p \geq 3$ Primzahl (nur Diedergruppe und zyklische Gruppe)
- $n = pq$, p, q Primzahlen, $p > q$, q teilt nicht $p - 1$: $\mathbb{Z}_{pq}$

Seien $U_1, \ldots, U_k$ k paarweise (bis auf das Neutralelement) disjunkte Untergruppen von G. Dann gilt: $xy = yx$, für $\in G_i, y \in G_j$

Wenn alle Sylowgruppen normal in einer Gruppe G sind, so ist G isomorph zum direkten Produkt dieser Sylowgruppen.