

Geometrie WS2018/19

Dozent: Prof. Dr. Arno Fehm

10. Oktober 2018

Inhaltsverzeichnis

I	Endliche Gruppen	2
1	Erinnerung und Beispiele	2
II	Kommutative Ringe	5
III	Körpererweiterungen	6
	Anhang	8
	Index	8

Vorwort

Kapitel I

Endliche Gruppen

1. Erinnerung und Beispiele

► Erinnerung 1.1

Eine Gruppe ist ein Paar $(G, *)$ bestehend aus einer Menge G und einer Verknüpfung $* : G \times G \rightarrow G$, dass die Axiome Assoziativität, Existenz eines neutralen Elements und Existenz von Inversen erfüllt, und wir schreiben auch G für die Gruppe $(G, *)$. Die Gruppe G ist abelsch, wenn $g * h = h * g$ für alle $g, h \in G$. Eine allgemeine Gruppe schreiben wir multiplikativ mit neutralem Element 1, abelsche Gruppen auch additiv mit neutralem Element 0.

Eine Teilmenge $H \subseteq G$ ist eine Untergruppe von G , in Zeichen $H \leq G$, wenn $H \neq \emptyset$ und H abgeschlossen ist unter der Verknüpfung und den Bilden von Inversen. Wir schreiben 1 (bzw. 0) auch für die triviale Untergruppe $\{1\}$ (bzw. $\{0\}$) von G .

Eine Abbildung $\varphi : G \rightarrow G'$ zwischen Gruppen ist ein Gruppenhomomorphismus, wenn

$$\varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2) \quad \forall g_1, g_2 \in G$$

und in diesem Fall ist

$$\text{Ker}(\varphi) = \varphi^{-1}(\{1\})$$

der Kern von φ . Wir schreiben $\text{Hom}(G, G')$ für die Menge der Gruppenhomomorphismen $\varphi : G \rightarrow G'$.

■ Beispiel 1.2

Sei $n \in \mathbb{N}$, K ein Körper und X eine Menge.

- (a) $\text{Sym}(X)$, die symmetrische Gruppe aller Permutationen der Menge X mit $f \cdot g = g \circ f$, insbesondere $S_n = \text{Sym}(\{1, \dots, n\})$
- (b) \mathbb{Z} sowie $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ mit der Addition
- (c) $\text{GL}_n(K)$ mit der Matrizenmultiplikation, Spezialfall $\text{GL}_1(K) = K^\times = K \setminus \{0\}$
- (d) Für jeden Ring R bilden die Einheiten R^\times eine Gruppe unter der Multiplikation, zum Beispiel $\text{Mat}_n(K)^\times = \text{GL}_n(K)$, $\mathbb{Z}^\times = \mu_2 = \{1, -1\}$

■ Beispiel 1.3

Ist (G, \cdot) eine Gruppe, so ist auch (G^{op}, \cdot^{op}) mit $G = G^{op}$ und $g \cdot^{op} h = h \cdot g$ eine Gruppe.

► **Bemerkung 1.4**

Ist G eine Gruppe und $h \in G$, so ist die Abbildung

$$\tau_h = \begin{cases} G \rightarrow G \\ g \mapsto gh \end{cases}$$

eine Bijektion (also $\tau_h \in \text{Sym}(G)$) mit Umkehrabbildung $\tau_{h^{-1}}$.

Satz 1.5

Sei G eine Gruppe. Zu jeder Menge $X \subseteq G$ gibt es eine kleinste Untergruppe $\langle X \rangle$ von G , die X enthält, nämlich

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

► **Bemerkung 1.6**

Man nennt $\langle X \rangle$ die von X erzeugte von G . Die Gruppe G heißt endlich erzeugt, wenn $G = \langle X \rangle$ für eine endliche Menge $X \subseteq G$.

Satz 1.7

Ein Gruppenhomomorphismus $\varphi : G \rightarrow G'$ ist genau dann ein Isomorphismus, wenn es einen Gruppenhomomorphismus $\varphi' : G' \rightarrow G$ mit $\varphi' \circ \varphi = \text{id}_G$ und $\varphi \circ \varphi' = \text{id}_{G'}$ gibt.

■ **Beispiel 1.8**

Ist G eine Gruppe, so bilden die Automorphismen $\text{Aut}(G) \subseteq \text{Hom}(G, G)$ eine Gruppe unter $\varphi \circ \varphi' = \varphi' \circ \varphi$. Für $\varphi \in \text{Aut}(G)$ und $g \in G$ schreiben wir $g^\varphi = \varphi(g)$.

Satz 1.9

Einen Gruppenhomomorphismus $\varphi : G \rightarrow G'$ ist genau dann injektiv, wenn $\text{Ker}(\varphi) = 1$.

■ **Beispiel 1.10**

Sei $n \in \mathbb{N}$, K ein Körper.

- (a) $\text{sgn} : S_n \rightarrow \mu_2$ ist ein Gruppenhomomorphismus mit Kern die alternierende Gruppe A_n .
- (b) $\det : \text{GL}_n(K) \rightarrow K^\times$ ist ein Gruppenhomomorphismus mit Kern $\text{SL}_n(K)$.
- (c) $\pi_{n\mathbb{Z}} : \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z}$, $a \mapsto a + n\mathbb{Z}$ ist ein Gruppenhomomorphismus mit Kern $n\mathbb{Z}$.
- (d) Ist A eine abelsche Gruppe, so ist

$$[n] : \begin{cases} A \rightarrow A \\ x \mapsto nx \end{cases}$$

ein Gruppenhomomorphismus mit Kern $A[n]$, die n -Torsion von A und Bild nA .

(e) Ist G eine Gruppe, so ist

$$\begin{cases} G \rightarrow G^{op} \\ g \mapsto g^{-1} \end{cases}$$

ein Isomorphismus.

Definition 1.11 (Zykel, disjunkte Zykel)

Seien $n, k \in \mathbb{N}$. Für paarweise verschiedene Elemente $i_1, \dots, i_k \in \{1, \dots, n\}$ bezeichnen wir mit $(i_1 \dots i_k)$ des $\sigma \in S_n$ gegeben durch

$$\begin{aligned} \sigma(i_j) &= i_{j+1} \quad \text{für } j = 1, \dots, k-1 \\ \sigma(i_k) &= i_1 \\ \sigma(i) &= i \quad \text{für } i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\} \end{aligned}$$

Wir nennen $(i_1 \dots i_k)$ eine k -Zykel. Zwei Zykel $(i_1 \dots i_k)$ und $(j_1 \dots j_l) \in S_n$ heißen disjunkt, wenn $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$.

Satz 1.12

Jedes $\sigma \in S_n$ ist das Produkt von Transpositionen (das heißt 2-Zykeln).

Lemma 1.13

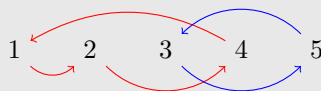
Disjunkte Zykel kommutieren, das heißt sind $\tau_1, \tau_2 \in S_n$ disjunkte Zykel, so ist $\tau_1 \tau_2 = \tau_2 \tau_1$.

Beweis. Sind $\tau_1 = (i_1 \dots i_k)$ und $\tau_2 = (j_1 \dots j_l)$ so ist

$$\tau_1 \tau_2(i) = \tau_2 \tau_1(i) = \begin{cases} \tau_1(i) & i \in \{i_1 \dots i_k\} \\ \tau_2(i) & i \in \{j_1 \dots j_l\} \\ i & \text{sonst} \end{cases} \quad \square$$

Satz 1.14

Jedes $\sigma \in S_n$ ist ein Produkt von paarweise disjunkten k -Zykeln mit $k \geq 2$ eindeutig bis auf Reihenfolge (sogenannte Zykelzerlegung von σ).



Also ein **3-Zykel** und ein **2-Zykel**.

Beweis. Induktion nach $N = |\{i \mid \sigma(i) \neq i\}|$.

$N = 0$: $\sigma = \text{id}$

$N > 0$: Wähle i_1 mit $\sigma(i_1) \neq i_1$, betrachte $i_1, \sigma(i_1), \sigma^2(i_1), \dots$. Da $\{1, \dots, n\}$ endlich und σ bijektiv ist, existiert ein minimales $k \geq 2$ mit $\sigma^k(i_1) = i_1$. Setze $\tau_1 = (i_1 \sigma(i_1) \dots \sigma^{k-1}(i_1))$. Dann ist $\sigma = \tau_1 \circ \tau_1^{-1} \sigma$, und nach Induktionshypothese ist $\tau_1^{-1} \sigma = \tau_2 \circ \dots \circ \tau_m$ mit disjunkten Zykeln τ_2, \dots, τ_m .

Eindeutigkeit ist klar, denn jedes i kann nur in einem Zykel $(i \sigma(i) \dots \sigma^{k-1}(i))$ vorkommen. \square

Kapitel II

Kommutative Ringe

Kapitel III

Körpererweiterungen

Anhang

Index

alternierende Gruppe, [3](#)

Automorphismen, [3](#)

Gruppe, [2](#)

 abelsch, [2](#)

 endlich erzeugt, [3](#)

Gruppenhomomorphismus, [2](#)

Kern, [2](#)

symmetrische Gruppe, [2](#)

Untergruppe, [2](#)

 erzeugte, [3](#)

Zykel, [4](#)

 disjunkt, [4](#)

Zykelzerlegung, [4](#)