

# **Geometrie WS2018/19**

Dozent: Prof. Dr. Arno Fehm

12. Oktober 2018

# *Inhaltsverzeichnis*

<b>I</b>	<b>Endliche Gruppen</b>	<b>2</b>
1	Erinnerung und Beispiele . . . . .	2
2	Ordnung und Index . . . . .	6
<b>II</b>	<b>Kommutative Ringe</b>	<b>9</b>
<b>III</b>	<b>Körpererweiterungen</b>	<b>10</b>
	<b>Anhang</b>	<b>12</b>
	<b>Index</b>	<b>12</b>

# *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  $\varphi$ . 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  $(i_1 \dots i_k)$  das  $\sigma \in S_n$  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  $\sigma$ ).



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  $\sigma$  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  $\tau_2, \dots, \tau_m$ .

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

■ **Beispiel**

$$(1\,2\,3\,4\,5)(2\,4) = (1\,4\,5)(2\,3) = (2\,3)(1\,4\,5) = (3\,2)(1\,4\,5) = (3\,2)(4\,5\,1) \neq (3\,2)(1\,5\,4)$$

## 2. Ordnung und Index

Sei  $G$  eine Gruppe,  $g \in G$ .

### Definition 2.1 (Ordnung)

- (a)  $\#G = |G| \in \mathbb{N} \cup \{\infty\}$ , die Ordnung von  $G$ .
- (b)  $\text{ord}(g) = \#\langle g \rangle$ , die Ordnung von  $g$ .

### ■ Beispiel 2.2

- (a)  $\#S_n = n!$
- (b)  $\#A_n = \frac{1}{2}n!$  für  $n \geq 2$
- (c)  $\#\mathbb{Z}/n\mathbb{Z} = n$

### Lemma 2.3

Für  $X \subseteq G$  ist

$$\langle X \rangle = \{g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r} \mid r \in \mathbb{N}_0, g_1, \dots, g_r \in X, \varepsilon_1, \dots, \varepsilon_r \in \{-1, 1\}\}$$

*Beweis.* klar, rechte Seite ist Untergruppe, die  $X$  enthält, und jede solche enthält alle Ausdrücke der Form  $g_1^{\varepsilon_1} \cdots g_r^{\varepsilon_r}$ .  $\square$

### Satz 2.4

- (a) Ist  $\text{ord}(g) = \infty$ , so ist  $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g^1, g^2, \dots\}$
- (b) Ist  $\text{ord}(g) = n$ , so ist  $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$
- (c) Es ist  $\text{ord}(g) = \inf\{k \in \mathbb{N} \mid g^k = 1\}$

*Beweis.* Nach Lemma 2.3 ist  $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ . Sei  $m = \inf\{k \in \mathbb{N} \mid g^k = 1\}$ .

- $|\{k \in \mathbb{N} \mid g^k = 1\}| = m$ : Sind  $g^a = g^b$  mit  $0 \leq a < b < m$ , so ist  $g^{b-a} = 1$ , aber  $0 < b-a < m$ , was ein Widerspruch zur Minimalität von  $m$  ist.
- $m = \infty \Rightarrow \text{ord}(g) = \infty$ : klar
- $m < \infty \Rightarrow \langle g \rangle = \{g^k \mid 0 \leq k < m\}$ : Für  $k \in \mathbb{Z}$  schreibe  $k = qm + r$  mit  $q, r \in \mathbb{Z}$  und  $0 \leq r < m$

$$g^k = g^{qm+r} = \underbrace{(g^m)^q}_{=1} \cdot g^r = g^r \in \{1, g, \dots, g^{m-1}\}$$

$\square$

### ■ Beispiel 2.5

- (a) Ist  $\sigma \in S_n$  ein  $k$ -Zykel, so ist  $\text{ord}(\sigma) = k$ .
- (b) Für  $\bar{1} \in \mathbb{Z}/n\mathbb{Z}$  ist  $\text{ord}(\bar{1}) = n$ .



**Definition 2.6 (Komplexprodukt, Nebenklasse)**

Seien  $A, B \subseteq G$ ,  $H \leq G$

- (a)  $AB := A \cdot B := \{ab \mid a \in A, b \in B\}$  das Komplexprodukt von  $A$  und  $B$ .
- (b)  $gH := \{g\} \cdot H = \{gh \mid h \in H\}$  die Linksnebenklasse von  $H$  bezüglich  $g$ .  
 $Hg := H \cdot \{g\} = \{hg \mid h \in H\}$  die Rechtsnebenklasse von  $H$  bezüglich  $g$ .
- (c)  $G/H := \{gH \mid g \in G\}$  die Menge der Linksnebenklassen.  
 $H \backslash G := \{Hg \mid g \in G\}$  die Menge der Rechtsnebenklassen.

**■ Beispiel 2.7**

Für  $h \in H$  ist  $hH = H = Hh$ .

**Lemma 2.8**

Seien  $H \leq G$ ,  $g, g' \in G$ .

- (a)  $gH = g'H \Leftrightarrow g' = gh$  für ein  $h \in H$   
 $Hg = Hg' \Leftrightarrow g' = gh$  für ein  $h \in H$
- (b) Es ist  $gH = g'H$  oder  $gH \cap g'H = \emptyset$  und  $Hg = Hg'$  oder  $Hg \cap Hg' = \emptyset$ .
- (c) Durch  $gH \mapsto Hg^{-1}$  wird eine wohldefinierte Bijektion  $G/H \rightarrow H \backslash G$  gegeben.

*Beweis.* (a) Hinrichtung:  $gH = g'H \Rightarrow g' = g' \cdot 1 \in g'H = gH \Rightarrow$  es existiert  $h \in H$  mit  $g' = gh$

Rückrichtung:  $g' = gh \Rightarrow g'H = ghH = gH$

(b) Ist  $gH \cap g'H \neq \emptyset$ , so existieren  $h, h' \in H$  mit  $gh = g'h' \Rightarrow gH = ghH = g'h'H = g'H$

(c) wohldefiniert:  $gH = g'H \xrightarrow{a)} g' = gh$  mit  $h \in H \Rightarrow H(g')^{-1} = Hh^{-1}g^{-1} = Hg^{-1}$

bijektiv: klar, Umkehrabbildung:  $Hg \mapsto g^{-1}H$

□

**Definition 2.9 (Index)**

Für  $H \subseteq G$  ist

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

der Index von  $H$  in  $G$ .

**■ Beispiel 2.10**

- (a)  $(S_n : A_n) = 2$  für  $n \geq 2$
- (b)  $(\mathbb{Z} : n\mathbb{Z}) = n$

**Satz 2.11**

Der Index ist multiplikativ: Sind  $K \leq H \leq G$ , so ist

$$(G : K) = (G : H) \cdot (H : K)$$

*Beweis.* Nach Lemma 2.8 bilden die Nebenklassen von  $H$  eine Partition von  $G$ , das heißt es gibt  $(g_i)_{i \in I}$  in  $G$

mit  $G = \bigsqcup_{i \in I} g_i H$ . Analog ist  $H = \bigsqcup_{j \in J} h_j K$  mit  $h_j \in H$ . Dann gilt:

$$\begin{aligned} H &= \bigsqcup_{j \in J} h_j K \stackrel{1.4}{\Rightarrow} gH = \bigsqcup_{j \in J} gh_j K \text{ f\"ur jedes } g \in G \\ G &= \bigsqcup_{i \in I} g_i H = \bigsqcup_{i \in I} \bigsqcup_{j \in J} g_i h_j K = \bigsqcup_{(i,j) \in I \times J} g_i h_j K \end{aligned}$$

Somit ist  $(G : K) = |I \times J| = |I| \cdot |J| = (G : H) \cdot (H : K)$ . □

**Folgerung 2.12 (Satz von Lagrange)**

Ist  $G$  endlich und  $H \leq G$ , so ist

$$\#G = \#H \cdot (G : H)$$

Insbesondere gilt  $\#H | \#G$  und  $(G : H) | \#G$ .

*Beweis.*  $\#G = (G : 1) \stackrel{2.11}{=} (G : H)(H : 1) = (G : H) \cdot \#H$ . □

**Folgerung 2.13 (kleiner Satz von Fermat)**

Ist  $G$  endlich und  $n = \#G$ , so ist  $g^n = 1$  f\"ur jedes  $g \in G$ .

*Beweis.* Nach Folgerung 2.12 gilt:  $\text{ord}(g) = \#\langle g \rangle | \#G = n$ . Nach Satz 2.4 ist  $g^{\text{ord}(g)} = 1$ , somit auch

$$g^n = \underbrace{(g^{\text{ord}(g)})}_{=1}^{\frac{n}{\text{ord}(g)}} = 1$$
□

► **Bemerkung 2.14**

Nach Folgerung 2.12 ist die Ordnung jeder Untergruppe von  $G$  ein Teiler der Gruppenordnung  $\#G$ . Umgekehrt gibt es im Allgemeinen aber nicht zu jedem Teiler  $d$  von  $\#G$  eine Untergruppe  $H$  von  $G$  mit  $\#H = d$ .

## Kapitel II

# *Kommutative Ringe*

## Kapitel III

# *Körpererweiterungen*

# Anhang

# Index

alternierende Gruppe, [3](#)

Automorphismen, [3](#)

Gruppe, [2](#)

    abelsch, [2](#)

    endlich erzeugt, [3](#)

Gruppenhomomorphismus, [2](#)

Index, [7](#)

Kern, [2](#)

Komplexprodukt, [7](#)

Linksnebenklasse, [7](#)

Ordnung, [6](#)

Rechtsnebenklasse, [7](#)

symmetrische Gruppe, [2](#)

Untergruppe, [2](#)

    erzeugte, [3](#)

Zykel, [4](#)

    disjunkt, [4](#)

Zykelzerlegung, [4](#)