Geometrie WS2018/19

Dozent: Prof. Dr. Arno Fehm

12. Oktober 2018

Inhaltsverzeichnis

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 $* : G \times G \to G$, 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 $\varphi : G \to G'$ 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

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

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

■ **Beispiel 1.2**

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

(a) $\mathrm{Sym}(X)$, die symmetrische Gruppe aller Permutationen der Menge X mit $f \cdot g = g \circ f$, insbesondere $S_n = \mathrm{Sym}(\{1, ..., n\})$

(b) $\mathbb{Z}$ sowie $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ mit der Addition

(c) $\mathrm{GL}_n(K)$ mit der Matrizenmultiplikation, Spezialfall $\mathrm{GL}_1(K) = K^\times = K \backslash \{0\}$

(d) Für jeden Ring R bilden die Einheiten $R^\times$ eine Gruppe unter der Multiplikation, zum Beispiel $\mathrm{Mat}_n(K)^\times = \mathrm{GL}_n(K)$, $\mathbb{Z}^\times = \mu_2 = \{1, -1\}$

■ **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

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

eine Bijektion (also $\tau_h \in \mathrm{Sym}(G)$) 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 $\varphi : G \to G'$ ist genau dann ein Isomorphismus, wenn es einen Gruppenhomomorphismus $\varphi' : G' \to G$ mit $\varphi' \circ \varphi = \mathrm{id}_G$ und $\varphi \circ \varphi' = \mathrm{id}_{G'}$ gibt.

■ **Beispiel 1.8**
Ist G eine Gruppe, so bilden die Automorphismen $\mathrm{Aut}(G) \subseteq \mathrm{Hom}(G, G)$ eine Gruppe unter $\varphi \circ \varphi' = \varphi' \circ \varphi$. Für $\varphi \in \mathrm{Aut}(G)$ und $g \in G$ schreiben wir $g^\varphi = \varphi(g)$.

Satz 1.9
Einen Gruppenhomomorphismus $\varphi : G \to G'$ ist genau dann injektiv, wenn $\mathrm{Ker}(\varphi) = 1$.

■ **Beispiel 1.10**
Sei $n \in \mathbb{N}$, K ein Körper.

(a) $\mathrm{sgn} : S_n \to \mu_2$ ist ein Gruppenhomomorphismus mit Kern die alternierende Gruppe A_n.

(b) $\det : \mathrm{GL}_n(K) \to K^\times$ ist ein Gruppenhomomorphismus mit Kern $\mathrm{SL}_n(K)$.

(c) $\pi_{n\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto a + n\mathbb{Z}$ ist ein Gruppenhomomorphismus mit Kern $n\mathbb{Z}$

(d) Ist A eine abelsche Gruppe, so ist

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

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

(e) Ist G eine Gruppe, so ist

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

ein Isomorphismus.

Definition 1.11 (Zykel, disjunkte Zykel)
Seien $n, k \in \mathbb{N}$. Für paarweise verschiedene Elemente $i_1, ..., i_k \in \{1, ..., n\}$ bezeichnen wir mit $(i_1 ... i_k)$ das $\sigma \in S_n$ gegeben durch

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

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

Satz 1.12
Jedes $\sigma \in S_n$ ist das Produkt von Transpositionen (das heißt 2-Zykeln).

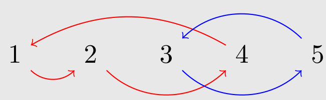
Lemma 1.13
Disjunkte Zykel kommutieren, das heißt sind $\tau_1, \tau_2 \in S_n$ disjunkte Zykel, so ist $\tau_1 \tau_2 = \tau_2 \tau_1$.

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

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

□

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 $N = |\{i \mid \sigma(i) \neq i\}|$.
$N = 0$: $\sigma = \mathrm{id}$
$N > 0$: Wähle i_1 mit $\sigma(i_1) \neq i_1$, betrachte $i_1, \sigma(i_1), \sigma^2(i_1), ...$ Da $\{1, ..., n\}$ endlich und σ bijektiv ist, existiert ein minimales $k \geq 2$ mit $\sigma^k(i_1) = i_1$. Setze $\tau_1 = (i_1 \, \sigma(i_1) ... \sigma^{k-1}(i_1))$. Dann ist $\sigma = \tau_1 \circ \tau_1^{-1} \sigma$, und nach Induktionshypothese ist $\tau_1^{-1} \sigma = \tau_2 \circ ... \circ \tau_m$ mit disjunkten Zyklen $\tau_2, ..., \tau_m$.
Eindeutigkeit ist klar, denn jedes i kann nur in einem Zykel $(i \, \sigma(i) ... \sigma^{k-1}(i))$ vorkommen. □

■ **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) $\operatorname{ord}(g) = \#\langle g \rangle$, 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

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

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

Satz 2.4

(a) Ist $\operatorname{ord}(g) = \infty$, so ist $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g^1, g^2, \dots\}$

(b) Ist $\operatorname{ord}(g) = n$, so ist $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$

(c) Es ist $\operatorname{ord}(g) = \inf\{k \in \mathbb{N} \mid g^k = 1\}$

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.
- $m = \infty \Rightarrow \operatorname{ord}(g) = \infty$: 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 $0 \leq r < m$

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

Beispiel 2.5

(a) Ist $\sigma \in S_n$ ein k-Zykel, so ist $\operatorname{ord}(\sigma) = k$.

(b) Für $\overline{1} \in \mathbb{Z}/n\mathbb{Z}$ ist $\operatorname{ord}(\overline{1}) = n$.

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 ${}^{G}\!/_{H} \to {}_{H}\backslash^{G}$ 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: $gH = g'H \overset{a)}{\Rightarrow} g' = gh$ 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 beweis 6 bilden die Nebenklassen von H eine Partition von G, das heißt es gibt $(g_i)_{i \in I}$ in G mit

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

$$H = \biguplus_{j\in J} h_j K \overset{1.4}{\Rightarrow} gH = \biguplus_{j\in J} gh_j K \text{ für jedes } g \in G$$
$$G = \biguplus_{i\in I} g_i H = \biguplus_{i\in I} \biguplus_{j\in J} g_i h_j K = \biguplus_{(i,j)\in I\times J} g_i h_j K$$

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 $H \le G$, so ist

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

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

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

Folgerung 2.13 (kleiner Satz von Fermat)
Ist G endlich und $n = \#G$, so ist $g^n = 1$ für jedes $g \in G$.

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

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

▶ 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