Geometrie WS2018/19

Dozent: Prof. Dr. Arno Fehm

29. Oktober 2018

Inhaltsverzeichnis

Vorwort

Wir freuen uns, dass du unser Skript für die Vorlesung *Geometrie* bei Prof. Dr. Arno Fehm im WS2018/19 gefunden hast. Da du ja offensichtlich seit einem Jahr Mathematik studierst kannst du dich glücklich schätzen zu dem einen Drittel zu gehören, dass nicht bis zum zweiten Semester abgebrochen hat.

Wenn du schon das Vorwort zu *Lineare Algebra und analytische Geometrie 1+2* gelesen hast, weißt du sicherlich, dass Prof. Fehm ein Freud der Algebra ist.[1] Auf die Frage eines Kommilitonen, wo in seinem Inhaltsverzeichnis (Gruppen, Ringe, Körper) die Geometrie vorkomme, antwortete er:

> *Die Frage ist nicht, wieso wir in dieser Vorlesung Algebra statt Geometrie machen, sondern warum hier seit 20 Jahren Geometrie unterrichtet wird.*

Wie auch im letzten Vorwort können wir dir nur empfehlen die Vorlesung immer zu besuchen, denn dieses Skript ist kein Ersatz dafür. Es soll aber ein Ersatz für deine unleserlichen und (hoffentlich nicht) unvollständigen Mitschriften sein und damit die Prüfungsvorbereitung einfacher machen. Im Gegensatz zu letztem Semester veröffentlicht Prof. Fehm auf seiner Homepage (`http://www.math.tu-dresden.de/~afehm/lehre.html`) kein vollständiges Skript mehr, sondern nur noch eine Zusammenfassung.

Der Quelltext dieses Skriptes ist bei Github (`https://github.com/henrydatei/TUD_MATH_BA`) gehostet; du kannst ihn dir herunterladen, anschauen, verändern, neu kompilieren, ... Auch wenn wir das Skript immer wieder durchlesen und Fehler beheben, können wir leider keine Garantie auf Richtigkeit geben. Wenn du Fehler finden solltest, wären wir froh, wenn du ein neues Issue auf Github erstellst und dort beschreibst, was falsch ist. Damit wird vielen (und besonders nachfolgenden) Studenten geholfen.

Und jetzt viel Spaß bei *Geometrie*!

Henry, Pascal und Daniel

[1] In Zukunft wird sich Prof. Fehm richtig freuen dürfen, denn im Zuge einer neuen Studienordnung, die am 1.4.2019 in Kraft tritt, kommt so gut wie keine Geometrie im *Bachelor Mathematik* vor.

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).

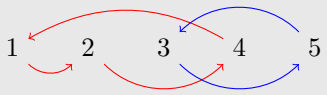
Lemma 1.13
Disjunkte Zykel kommutieren, das heißt sind $\tau_1, \tau_2 \in S_n$ disjunkte Zykel, so ist $\tau_1\tau_2 = \tau_2\tau_1$.

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 $N = |\{i \mid \sigma(i) \neq i\}|$.
$N = 0$: $\sigma = \text{id}$
$N > 0$: 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) $\text{ord}(g) = \#\langle g \rangle$, 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

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

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 $\text{ord}(g) = \infty$, so ist $\langle g \rangle = \{..., g^{-2}, g^{-1}, 1, g^1, g^2, ...\}$

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

(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 $0 \leq r < m$

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

■ **Beispiel 2.5**

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

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

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

mit $G = \biguplus_{i\in I} g_i H$. 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 $H \leq G$, 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: $\operatorname{ord}(g) = \#\langle g\rangle | \#G = n$. Nach Satz 2.4 ist $g^{\operatorname{ord}(g)} = 1$, somit auch

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

▶ **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 $\#H = d$.

3. Normalteiler und Quotientengruppen

Sei G eine Gruppe.

Definition 3.1 (normal, Normalteiler)
Eine Untergruppe $H \leq G$ ist normal (in Zeichen $H \trianglelefteq G$), wenn $g^{-1}hg \in H$ für alle $h \in H$ und $g \in G$. Ein Normalteiler von G ist eine normale Untergruppe von G.

Beispiel 3.2

(a) Ist G abelsch, so ist jede Untergruppe von G ein Normalteiler.

(b) Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so ist $\mathrm{Ker}(\varphi) \trianglelefteq G$, denn $\varphi(h) = 1 \Rightarrow \varphi(g^{-1}hg) = \varphi(g)^{-1}\varphi(h)\varphi(g) = 1 \ \forall g \in G$.

(c) Jede Gruppe G hat die trivialen Normalteiler $1 \trianglelefteq G$ und $G \trianglelefteq G$.

Lemma 3.3
Sei $H \leq G$ und $N \trianglelefteq G$.

(a) $H \trianglelefteq G \Leftrightarrow gH = Hg$ für alle $g \in G$

(b) $HN = NH$, $HN \leq G$, $N \trianglelefteq HN$, $H \cap N \leq N$, $H \cap N \trianglelefteq H$

(c) Sind $N, H \trianglelefteq G$, so ist $H \cap N \trianglelefteq G$, $HN \trianglelefteq G$

(d) Für $g, g' \in G$ ist $gN \cdot g'N = gg'N$

Beweis. (a) Hinrichtung: $\forall g \in G$, $\forall h \in H$: $g^{-1}hg \in H \Rightarrow gHg^{-1} \subseteq H \Rightarrow Hg = gH$ und $g^{-1}H \subseteq Hg^{-1} \Rightarrow gH = Hg$
Rückrichtung: $\forall g \in G$: $gH = Hg \Rightarrow \exists h' \in H$: $gh' = hg \Rightarrow g^{-1}hg = h \in H$

(b)
- $HN = \bigcup_{n\in\mathbb{N}} hN = \bigcup_{n\in\mathbb{N}} Nh = NH$
- $HN \cdot NH = H \cdot NH \cdot N = H \cdot HN \cdot N = HN$
  $(HN)^{-1} = N^{-1}H^{-1} = NH = HN$
- $N \trianglelefteq HN$: klar
- $H \cap N \leq N$: klar
- $H \cap N \trianglelefteq H$: $n \in H \cap N$, $h \in H \Rightarrow h^{-1}nh \in H \cap N$

(c)
- $H \cap N \trianglelefteq G$: $h \in H \cap N$, $g \in G \Rightarrow g^{-1}hg \in H \cap N$
- $HN \trianglelefteq G$: $g \in G \Rightarrow gHN \overset{a)}{=} Hg \cdot N = H \cdot gN \overset{a)}{=} H \cdot Ng = HNg$

(d) $gN \cdot g'N = g \cdot Ng' \cdot N \overset{a)}{=} g \cdot g'N = gg'N$ □

Satz 3.4
Sei $N \trianglelefteq G$. Dann ist G/N mit dem Komplexprodukt als Verknüpfung eine Gruppe, und $\pi_N : G \to G/N$, $g \mapsto gN$ ein Gruppenhomomorphismus mit Kern N.

Beweis.
- Komplexprodukt ist Verknüpfung auf G/N: Lemma 3.3
- Gruppenaxoime übertragen sich von G auf G/N: klar
- π_N ist ein Homomorphismus: Lemma 3.3
- $\mathrm{Ker}(\pi_N) = N$: Lemma 2.8 □

Folgerung 3.5
Die Normalteiler sind genau die Gruppenhomomorphismen.

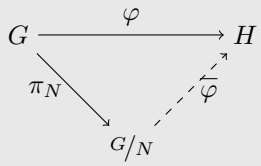
Definition 3.6 (Quotientengruppe)
Für $N \trianglelefteq G$ heißt ${}^{G}\!/_{N}$ zusammen mit dem Komplexprodukt als Verknüpfung die Quotientengruppe von G nach N (oder G modulo N).

Lemma 3.7
Sei $N \trianglelefteq G$. Für $H \leq G$ ist $\pi_N(H) = {}^{HN}\!/_{N} \leq {}^{G}\!/_{N}$, und $H \mapsto \pi(H)$ liefert eine Bijektion zwischen

- den $H \leq G$ mit $N \leq H$ und
- den $H \leq {}^{G}\!/_{N}$

Beweis.
- $\pi_N(H) = \{hN \mid h \in H\} = \{hnN \mid h \in H, n \in N\} = {}^{HN}\!/_{N}$
- Umkehrabbildung: $H \mapsto \pi_N^{-1}(H)$:
  $H \leq {}^{G}\!/_{N}$: $\pi_N(\pi_N^{-1}(H)) = H$, da π_N surjektiv
  $N \leq H \leq G$: $\pi_N^{-1}(\pi_N(H)) = \pi_N^{-1}({}^{HN}\!/_{N}) = HN \subseteq H \cdot H = H$ □

Satz 3.8 (Homomorphiesatz)
Sei $\varphi : G \to H$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ mit $N \leq \mathrm{Ker}(\varphi)$. Dann gibt es genau einen Gruppenhomomorphismus $\overline{\varphi} : {}^{G}\!/_{N} \to H$ mit $\overline{\varphi} \circ \pi_N = \varphi$.



Beweis. Existiert so ein $\overline{\varphi}$, so ist $\overline{\varphi}(gN) = (\overline{\varphi} \circ \pi_N)(g) = \varphi(g)$ eindeutig bestimmt. Definiere $\overline{\varphi}$ nun so.

- $\overline{\varphi}$ ist wohldefiniert: $gN = g'N \overset{2.8}{\Rightarrow} \exists g' = gn$ für ein $n \in N \Rightarrow \varphi(g') = \varphi(g) \cdot \underbrace{\varphi(n)}_{=1} = \varphi(g)$, da $n \in \mathrm{Ker}(\varphi)$
- $\overline{\varphi}$ ist Homomorphismus: $\overline{\varphi}(gN \cdot g'N) = \overline{\varphi}(gg'N) = \varphi(gg') = \varphi(g) \cdot \varphi(g') = \overline{\varphi}(gN) \cdot \overline{\varphi}(g'N)$ □

Folgerung 3.9
Ein Gruppenhomomorphismus $\varphi : G \to H$ liefert einen Isomorphismus

$$\bar{\varphi} : {}^{G}\!/_{\mathrm{Ker}(\varphi)} \xrightarrow{\cong} \mathrm{Im}(\varphi) \leq H$$

Folgerung 3.10 (1. Homomorphiesatz)
Seien $H \leq G$ und $N \trianglelefteq G$. Der Homomorphismus

$$\varphi : H \overset{i}{\hookrightarrow} HN \xrightarrow{\pi_N} {}^{HN}\!/_{N}$$

induziert einen Isomorphismus

$$\bar{\varphi} : {}^{H}\!/_{H \cap N} \xrightarrow{\cong} {}^{HN}\!/_{N}$$

Beweis.
- φ ist surjektiv: Für $h \in H$ und $n \in N$ ist

$$hnN = hN = \varphi(h) \in \varphi(H) = \mathrm{Im}(\varphi)$$

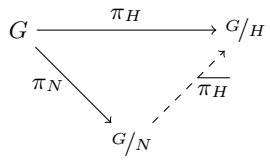
- $\mathrm{Ker}(\varphi) = H \cap \mathrm{Ker}(\pi_N) = H \cap N$

Mit Folgerung 3.9 folgt die Behauptung. □

Folgerung 3.11 (2. Homomorphiesatz)
Seien $N \trianglelefteq G$ und $N \leq H \trianglelefteq G$. Der Homomorphismus $\pi_H : G \to {}^{G}/_{H}$ induziert einen Isomorphismus

$${}^{(G/N)}/_{(H/N)} \xrightarrow{\cong} {}^{G}/_{H}$$

Beweis. Da $N \leq H$ liefert π_H einen Epimorphismus (mit Satz 3.8) $\overline{\pi_H} : {}^{G}/_{N} \to {}^{G}/_{H}$.



Dieser hat Kern $\mathrm{Ker}(\overline{\pi_H}) ?^{H}/_{N}$, induziert nach Folgerung 3.9 einen Isomorphismus

$${}^{(G/N)}/_{\mathrm{Ker}(\overline{\pi_H})} \xrightarrow{\cong} \mathrm{Im}(\overline{\pi_H}) = {}^{G}/_{H}$$

□

Definition 3.12 (Konjugation)
Seien $x, x', g \in G$ und $H, H' \leq G$.

(a) $x^g := g^{-1}xg$, Konjugation von x mit g

(b) x und x' sind konjugiert (in G) $\Leftrightarrow \exists g \in G$: $x' = x^g$

(c) H und H' heißen konjugiert (in G) $\Leftrightarrow \exists g \in G$: $H' = H^g = \{h^g \mid h \in H\}$

Lemma 3.13
Die Abbildung

$$\mathrm{int} : \begin{cases} G \to \mathrm{Aut}(G) \\ g \mapsto (x \mapsto x^g) \end{cases}$$

ist ein Gruppenhomomorphismus.

Beweis.
- $\mathrm{int}(g) \in \mathrm{Hom}(G, G)$: $(xy)^g = g^{-1}xyg = g^{-1}xgg^{-1}yg = x^g \cdot y^g$
- $(x^g)^h = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh) = x^{gh}$
- $\mathrm{int}(g) \in \mathrm{Aut}(G)$: Umkehrabbildung zu $\mathrm{int}(g)$ ist $\mathrm{int}(g^{-1})$
- $\mathrm{int}(g) \in \mathrm{Hom}(G, \mathrm{Aut}(G))$:

$$\mathrm{int}(gh) = \mathrm{int}(h) \circ \mathrm{int}(g) = \mathrm{int}(g) \cdot \mathrm{int}(h)$$

□

Definition 3.14 (innere Automorphismen, Zentrum, charakteristische Gruppe)

(a) $\mathrm{Inn}(G) = \mathrm{Im}(\mathrm{int}) \leq \mathrm{Aut}(G)$, die Gruppe der inneren Automorphismen von G

(b) $\mathrm{Z}(G) = \mathrm{Ker}(\mathrm{int}) = \{g \in G \mid xg = gx \quad \forall x \in G\}$, das Zentrum von G

(c) $H \leq G$ ist charakteristisch $\Leftrightarrow \forall \sigma \in \mathrm{Aut}(G)$: $H = H^\sigma$

▶ **Bemerkung 3.15**

(a) Konjugation ist eine Äquivalenzrelation

(b) $H \leq G$ ist normal $\Leftrightarrow H = H^\sigma \quad \forall \sigma \in \mathrm{Inn}(G)$

(c) Deshalb gilt für $H \leq G$: H ist charakteristisch $\Rightarrow H$ ist normal

■ **Beispiel 3.16**

$\mathrm{Z}(G)$ ist charakteristisch in G

4. Abelsche Gruppen

Sei G ein Gruppe.

Definition 4.1 (zyklische Gruppe)
Eine Gruppe G ist zyklisch $\Leftrightarrow G = \langle g \rangle$ für ein $g \in G$.

■ **Beispiel 4.2**

(a) $\mathbb{Z} = \langle 1 \rangle$

(b) $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$

(c) $C_n = \langle (1\,2\,...\,n) \rangle \leq S_n$

(d) Ist $\#G = p$ eine Primzahl, so ist G zyklisch (Übung 6)

Lemma 4.3
Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die $\langle k \rangle = \mathbb{Z}k$ mit $k \in \mathbb{N}_0$ und für $k_1, ..., k_r \in \mathbb{Z}$ ist $\langle k_1, ..., k_r \rangle = \langle k \rangle$ mit

$$k = \mathrm{ggT}(k_1, ..., k_r)$$

Beweis. Zwei Beweise sind möglich:

1. Jede Untergruppe von $\mathbb{Z}$ ist ein Ideal von $(\mathbb{Z}, +, \cdot)$ und $\mathbb{Z}$ ist ein Hauptidealring.
2. Sei $H \leq \mathbb{Z}$. Setze $k = \min\{H \cap N\}$, ohne Einschränkung $H \neq \{0\}$.
   - $H = \langle k \rangle$: $n \in H \Rightarrow n = qk + r$ mit $q, r \in \mathbb{Z}$, $0 \leq r < k \Rightarrow r = n - \underbrace{qk}_{k+...+k} \in H \xrightarrow{k \text{ minimal}} r = 0 \Rightarrow n \in \langle k \rangle$
   - $\langle k_1, ..., k_r \rangle = \langle k \rangle \Rightarrow k = \mathrm{ggT}(k_1, ..., k_r)$:
     $k_i \in \langle k \rangle \Rightarrow k | k_i \quad \forall i$
     $k \in \langle k_1, ..., k_r \rangle \Rightarrow k = n_1 k_1 + ... + n_r k_r$ mit $n_i \in \mathbb{Z}$ $\exists d | k_i \Rightarrow d | k \Rightarrow k = \mathrm{ggT}(k_1, ..., k_r)$ □

Satz 4.4 (Klassifikation von zyklischen Gruppen)
Sei $G = \langle g \rangle$ zyklisch. Dann ist G abelsch und

(a) $G \cong (\mathbb{Z}, +)$ oder

(b) $G \cong (\mathbb{Z}/n\mathbb{Z}, +)$ mit $n = \#G < \infty$

Beweis. Betrachte

$$\varphi : \begin{cases} \mathbb{Z} \to G \\ k \mapsto g^k \end{cases}$$

φ ist ein Homomorphismus und surjektiv, da $G = \langle g \rangle$. Nach Folgerung 3.9 ist $G = \mathrm{Im}(\varphi) \cong \mathbb{Z}/\mathrm{Ker}(\varphi)$. Nach Lemma 4.3 ist $\mathrm{Ker}(\varphi) = \langle n \rangle$ für ein $n \in \mathbb{N}_0$.

- $n = 0$, so ist $\mathrm{Ker}(\varphi) = \langle 0 \rangle$, also φ injektiv und $G \cong \mathbb{Z}$.
- $n > 0$, so ist $G \cong \mathbb{Z}/n\mathbb{Z}$ und $n = \#\mathbb{Z}/n\mathbb{Z} = \#G$. □

Satz 4.5
Sei $G = (G, +) = \langle g \rangle$ zyklisch der Ordnung $n \in \mathbb{N}$.

- Zu jedem $d \in \mathbb{N}$ mit $d \mid n$ hat G genau eine Untergruppe der Ordnung d, nämlich $U_d = \langle \frac{n}{d} g \rangle$
- Für $d \mid n$ und $d' \mid n$ ist $U_d \leq U_{d'} \Leftrightarrow d \mid d'$
- Für $h_1, \ldots, h_k \in \mathbb{Z}$ ist $\langle h_1 g, \ldots, h_r g \rangle = \langle eg \rangle = U_{\frac{n}{e}}$ mit $e = \mathrm{ggT}(h_1, \ldots, h_r, n)$
- Für $k \in \mathbb{Z}$ ist $\mathrm{ord}(kg) = \frac{n}{\mathrm{ggT}(k,n)}$

Beweis. Betrachte wieder $\varphi\colon \begin{cases} \bar{k} & \to G \\ k & \to kg \end{cases}$

1. Nach 3.7 und 4.3 liefert φ Bijektion $\{e \in \mathbb{N} \mid n\mathbb{Z} \leq e\mathbb{Z}\} \overset{1.1}{\to} \{H \leq G\}$ und $n\mathbb{Z} \leq e\mathbb{Z} \Leftrightarrow e \mid n$. Ist $H = \varphi(e\mathbb{Z}) = \langle e\mathbb{Z} \rangle$, so ist $H \cong {}^{e\mathbb{Z}}/_{n\mathbb{Z}}$, also $n = (\mathbb{Z}\colon n\mathbb{Z}) = (\mathbb{Z}\colon e\mathbb{Z}) \cdot (e\mathbb{Z}\colon n\mathbb{Z}) = e \cdot \#H$
2. $U_d \leq U_{d'} \Leftrightarrow \langle \frac{n}{d} g \rangle \leq \langle \frac{n}{d'} g \rangle = \frac{n}{d}\mathbb{Z} \leq \frac{n}{d'}\mathbb{Z} \Leftrightarrow \frac{n}{d'} \mid \frac{n}{d} \Leftrightarrow d \mid d'$
3. Mit $H = \langle h_1, \ldots, h_r, n \rangle \leq \mathbb{Z}$ ist $n\mathbb{Z} \leq H$, $\varphi(H) = \langle h_1 g, \ldots, h_r g$. Nach 4.3 ist $H = \langle e \rangle$ mit $e = \mathrm{ggT}(h_1, \ldots, h_r, n)$, somit $\langle h_1 g, \ldots, h_r g \rangle = \varphi(e\mathbb{Z}) = U_{\frac{n}{e}}$
4. $\mathrm{ord}(hg) = \#\langle hg \rangle \overset{c)}{=} \#U_{\frac{n}{e}}$ mit $e = \mathrm{ggT}(h, n)$ □

Lemma 4.6
Seien $a, b \in G$. Kommutieren a und b und sind $\mathrm{ord}(a)$ und $\mathrm{ord}(b)$ teilerfremd, so ist

$$\mathrm{ord}(a, b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$$

Beweis. Nach 2.12 ist $\langle a \rangle \cap \langle b \rangle = 1$. Ist $(ab)^k = 1 = a^k b^k$, so ist $a^k = b^{-k} \in \langle a \rangle \cap \langle b \rangle = 1$, also $a^k = b^k = 1$. Somit ist $(ab)^k = 1 \Leftrightarrow a^k = 1$ und $b^k = 1$ und damit $\mathrm{ord}(ab) = \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b)) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$ □

Folgerung 4.7
Ist G abelsch und sind $a, b \in G$ mit $\mathrm{ord}(a) = m < \infty$, $\mathrm{ord}(b) = n = \infty$, so existiert $c \in G$ mit

$$\mathrm{ord}(c) = \mathrm{kgV}(\mathrm{ord}(a), \mathrm{ord}(b))$$

Beweis. Schreibe $m = m_0 m'$ und $n = n_0 n'$ mit $m_0 n_0 = \mathrm{kgV}(m, n)$ und $\mathrm{ggT}(m_0, n_0) = 1 \Rightarrow \mathrm{ord}(a^{m'}) = m_0$, $\mathrm{ord}(b^{n'}) = n_0 \Rightarrow \mathrm{ord}(b^{n'} \cdot a^{m'}) \overset{4.6}{=} m_0 \cdot n_0 = \mathrm{kgV}(m, n)$. □

Theorem 4.8 (Struktursatz für endlich erzeugte abelsche Gruppen)
Jede endliche erzeugte abelsche Gruppe G ist eine direkte Summe zyklischer Gruppen

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{n} {}^{\mathbb{Z}}/_{d_i\mathbb{Z}}$$

mit eindeutig bestimmten $d_1, \ldots, d_k > 1$ die $d_1 \mid d_{i+1}$ für alle i erfüllen.

Beweis.
- Existenz: LAAG 2. VIII. 6.14

- Eindeutigkeit: Für $d \in \mathbb{N}$ ist

$$\#^G/_{dG} = \#\left(\mathbb{Z}/_{d\mathbb{Z}}\right)^r \oplus \bigoplus_{i=1}^{k} {}^{(\mathbb{Z}/_{d_i\mathbb{Z}})}/_{d \cdot (\mathbb{Z}/_{d_i\mathbb{Z}})}$$
$$\overset{4.5}{=} d^r \cdot \prod_{i=1}^{n} \frac{d_i}{\mathrm{ggT}(d, d_i)}$$

und daraus kann man $r, k, d_1, \ldots, d_k$ erhalten. □

Lemma 4.9
Sei $G = (G, +) = \langle g \rangle$ zyklisch der Ordnung $n \in \mathbb{N}_0$. Die Endomorphismen von G sind genau die

$$\varphi_{\overline{k}} : \begin{cases} G & \to G \\ x & \to kx \end{cases} \text{ für } \overline{k} = k + n\mathbb{Z} \in \mathbb{Z}/_{n\mathbb{Z}} \tag{1}$$

Dabei ist $\varphi_{\overline{l}} \circ \varphi_{\overline{k}} = \varphi_{\overline{kl}}$ für $\overline{k}, \overline{l} \in \mathbb{Z}/_{n\mathbb{Z}}$.

Beweis.
- $\varphi_{\overline{k}}$ wohldefiniert $\overline{k_1} = \overline{k_2} \Rightarrow k_2 = k_1 + an$ mit $a \in \mathbb{Z}$, $k_2 x = k_1 x + an \cdot x = k_1 x \forall x \in G$
- $\varphi_{\overline{k}} \in \mathrm{Hom}(G, G)$: Klar, da G abelsch
- $\overline{k} = \overline{l} \varphi_{\overline{k}} = \varphi_{\overline{l}}$
  $\varphi_{\overline{k}} = \varphi_{\overline{l}} \Rightarrow \varphi_{\overline{k}}(g) = \varphi_{\overline{k}}(g) \Rightarrow (k-l)g = 0 \overset{\mathrm{ord}(g)=n}{\Rightarrow} n \mid (k-l) \Rightarrow \overline{k} = \overline{l}$
- $\varphi \in \mathrm{Hom}(G, G) \Rightarrow \varphi = \varphi_{\overline{k}}$ für ein $k \in \mathbb{Z}$, $\varphi(g) = kg$ für ein $k \Rightarrow \varphi = \varphi_{\overline{k}}$
- $\varphi_{\overline{l}} \circ \varphi_{\overline{k}} = \varphi_{\overline{kl}}$: $l(kx) = (lk)x$ □

Satz 4.10
Ist G zyklisch von Ordnung $n \in \mathbb{N}$, so ist

$$\mathrm{Aut}(G) \cong \left(\mathbb{Z}/_{\mathbb{Z}}\right)^{\times}$$

Beweis. $\mathrm{Aut}(G) \subseteq \mathrm{Hom}(G, G) = \{\varphi_{\overline{k}} : k \in \mathbb{Z}/_{n\mathbb{Z}}\}$

$$\begin{aligned} &\varphi_{\overline{k}} \in \mathrm{Aut}(G) \Leftrightarrow \text{ existiert } \overline{l} \in \mathbb{Z}/_{n\mathbb{Z}} \text{ mit} \\ &\varphi_{\overline{l}} \circ \varphi_{\overline{k}} = \varphi_{\overline{1}} \Leftrightarrow \text{ existiert } \overline{l} \in \mathbb{Z}/_{n\mathbb{Z}} \end{aligned} \tag{2}$$

□

Kapitel II

Kommutative Ringe

Kapitel III

Körpererweiterungen

Anhang