Geometrie WS 19/20

Dozent: Prof. Dr. Ulrich Krähmer

30. Oktober 2019

Inhaltsverzeichnis

Vorwort

Kapitel I

Gruppen

1. Wiederholung

Definition 1.1 (Halbgruppe, Monoid, Gruppe)
Eine Halbgruppe ist eine Menge G mit einem assoziativen Produkt

$$\cdot : G \times G \to G.$$

Ein Monoid ist eine Halbgruppe, in der ein Element $1 \in G$ existiert mit

$$1 \cdot x = x \cdot 1 = x \quad \forall x \in G.$$

Eine Gruppe ist ein Monoid, in dem für jedes $x \in G$ ein $y \in G$ existiert mit

$$xy = yx = 1.$$

▶ **Bemerkung 1.2**
1 ist eindeutig, wenn es existiert. y ist durch x eindeutig bestimmt: $x^{-1} = y$.

Definition 1.3 (Morphismus)
Ein Morphismus zwischen zwei Gruppen G und H ist eine Abbildung

$$f : G \to H \quad \text{mit} \quad f(xy) = f(x)f(y) \quad \forall x, y \in G.$$

Satz 1.4
Ist $f : G \to H$ ein Morphismus von Gruppen, so gilt

- $f(1) = 1$ und
- $f(x^{-1}) = f(x)^{-1}$ $\forall x \in G$.

Beweis. Für alle $x \in G$ gilt

$$f(x) = f(1 \cdot x) = f(1)f(x).$$

Gilt in einer beliebigen Gruppe jedoch $ab = b$ für zwei Elemente a, b, so folgt

$$(ab) \cdot b^{-1} = a\left(bb^{-1}\right) = a \cdot 1 = a \quad \text{mit} \quad bb^{-1} = 1.$$

Ferner gilt

$$f(x) \cdot f\left(x^{-1}\right) = f\left(x \cdot x^{-1}\right) = f(1) = 1$$

wie schon gezeigt (und analog $f(x^{-1})f(x) = 1$). Also ist $f(x^{-1}) = f(x)^{-1}$). □

■ **Beispiel 1.5**

1) Sei X eine beliebige Menge. $S_X = \{f\colon X \to X \mid f \text{ bijektiv}\}$ ist eine Gruppe bezüglich Komposition mit $1 = \mathrm{id}_X$. Insbesondere ist $S_n = S_{\{1,\dots,n\}}$ die symmetrische Gruppe und ein Element $f \in S_n$ ist eine Permutation.

2) $\mathrm{GL}(V) = \{f \in S_V \mid f \text{ linear}\}$, wobei V ein R-Modul ist mit kommutativen assoziativen Ring mit 1.

3) $\mathbb{Z}, \mathbb{Z}_n$ unter Addition

$$U_n = \mathbb{Z}_n^\times = \{m \in \{0,\dots,n-1\} \mid \mathrm{ggT}(m,n) = 1\}$$

Beide Gruppen sind abelsch, d.h.

$$\forall x, y \in G : xy = yx.$$

4) $G = U(1) = \{z \in C \mid |z| = 1\} = \left\{e^{it} \mid t \in [0, 2\pi]\right\}$

5) $G = U(1) \times \mathrm{SU}(2) \times \mathrm{SU}(3)$, die Eichgruppe im Standardmodell der Elementarteilchen

Definition 1.6 (Ordnung)
Ist G endlich, so nennt man $|G|$ die Ordnung von G.

■ **Beispiel 1.7**
$|S_n| = n!$

Definition 1.8 (p-Gruppe)
Ist $|G| = p^n$ für eine Primzahl p und ein $n \in \mathbb{N}$, so nennt man G eine p-Gruppe

Definition 1.9 (Untergruppe)
Sei G Gruppe. Eine Teilmenge $H \leq G$ ist eine Untergruppe $H < G$, wenn

(i) Für alle $x, y \in H$: $xy \in H$

(ii) $1 \in H$

(iii) Für alle $x \in H$: $x^{-1} \in H$

Satz 1.10
Ist $|G| < \infty$, so folgen Definitionen 1.9 (ii) und 1.9 (iii) bereits aus Definition 1.9 (i) und $H \neq \varnothing$.

Beweis. Sei $x \in H$ ein beliebiges Element. Aus 1.9 (i) folgt $x^n \in H$ für alle $n \in \mathbb{N}_+$. Da $|G| < \infty$ existiert $n \neq m$ mit $x^n = x^m$. O.E. sei $n > m$

$\Rightarrow\ x^{n-m}x^m = x^n$

$\Rightarrow\ x^{n-m} = 1$

$\Rightarrow$ 1.9 (ii)

Ferner impliziert die Existenz der inversen Elemente, dass die Linkstranslation

$$t_x\colon G \to G, y \mapsto xy \quad (x \in G \text{ fest})$$

injektiv ist, denn $(t_x)^{-1} = t_{x^{-1}}$. Ist $x \in H$, so heißt 1.9 (i) gerade $t_x(H) \subseteq H$, sprich t_x kann zu $t_x\big|_H\colon H \to H$

eingeschränkt werden. Die Einschränkung einer injektiven Abbildung ist injektiv. Da $|H| \leq |G| < \infty$, folgt $t_x\big|_H : H \to H$ ist surjektiv. Also existiert $y \in H$ mit $t_x(y) = 1$. Eindeutigkeit von x^{-1} heißt $y = x^{-1} \in H$. □

Definition 1.11 (Erzeugendensystem)
Ist $X \subseteq G$, so ist

$$\langle X \rangle = \bigcap_{\substack{H<G \\ X \subset H}} H$$

die von X erzeugte Untergruppe. Ist $\langle X \rangle = G$, nennen wir X ein Erzeugendensystem.

Definition 1.12 (Konjugation)
Ist $H < G$ und $x \in G$, so ist

$$x^{-1}Hx = \left\{x^{-1}Hx \mid y \in H\right\}$$

eine Untergruppe („$x^{-1}yx$“ y ist konjugiert mit x). Wir nennen diese zu H konjugiert.

Definition 1.13 (Konjugationsklasse)
Die Menge $\left\{x^{-1}yx \mid x \in G\right\}$ ist i.A. keine Untergruppe und diese nennt man Konjugationsklassen von y.

Definition 1.14 (Zentralisator, Zentrum)
Der Zentralisator von $y \in G$ ist

$$\{x \in G \mid xy = yx\} =: Z_G(y).$$

Das Zentrum von G ist

$$Z(G) = \bigcap_{y \in G} Z_G(y) = \{x \in G \mid \forall y \in G xy = yx\}.$$

■ **Beispiel 1.15**
Sei $G = S_n \ni f$ Permutation, z.B.

$$S_6 \in \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 1 & 2 & 3 \end{pmatrix} = (1524)(36)$$

letzteres nennt man Zykelnotation. 1-Zykeln, d.h. $i \in \{1, \ldots, n\}$ mit $f(i) = i$ werden meist nicht notiert, z.B.:

$$S_4 \in \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (12)$$

▶ **Bemerkung 1.16**
Ein k-Zykel ist ein Produkt von $k-1$ Transpositionen (2-Zykel), z.B.

$$(12345) = (15)(14)(13)(12)$$

ist das Produkt in S_5, d.h. Komposition! Also erzeugt $\{(i,j)\}$ die S_n. Jede Permutation kann also als Produkt von Transpositionen geschrieben werden. Diese Darstellung ist nicht eindeutig! (z.B. $(12)(23)(12) = (23)(12)(23)$) ("Braid relation") und $(12)(12) = ()$. Allerdings kommen in jeder solcher Darstellungen entweder eine gerade oder ungerade Anzahl von Transpositionen vor ($\to$ Fehlstände). Insbesondere bilden gerade Permutationen (gerade Anzahl an Fehlständen $\Leftrightarrow$ Produkte von zu Transpositionen) eine Untergruppe $A_n < S_n$, die sogenannte alternierende Gruppe.

■ **Beispiel 1.17**
Sei $G = \mathrm{GL}(n,R)$ die invertierbare Matrizen mit Einträgen in R (nur endliche, wenn $R^\times$*endlich*!). Untergruppen sind

- $\mathrm{SL}(n,R) = \{g \in \mathrm{GL}(n,R) \mid \det g = 1\}$
- $O(n,R) = \left\{g \in G \mid gg^T = g^T g = 1\right\}$ mit dem Skalarprodukt $\langle gv, gw\rangle = \langle v, w\rangle \quad \forall v, w \in R^n$
- $\mathrm{SO}(n,R) = \mathrm{SL}(n,R) \cap \mathrm{O}(n,R)$.

Ist R Ring mit Involuten (z.B. $R = \mathbb{C}, z = \bar{z}$)

- $U(n,R) = \{g \in \mathrm{GL}(n,R) \mid gg^* = g^* g = 1\}$
- $\mathrm{SU}(n,R) = \mathrm{SL}(n,R) \cap U(n,R)$

■ **Beispiel 1.18**
Sei D_n definiert durch

$$D_n = \left\{f\colon \mathbb{R}^2 \to \mathbb{R}^2 \text{ linear, bjektiv} \mid f(P_n) = P_n\right\},$$

wobei $P_n \subset \mathbb{R}^2$ das regulär n-gen ist, z.B. das Hexagon P_6. Alternativ ist $D_n \subseteq S_n$, wobei $\{1,\dots,n\}$ mit der Menge der Ecken von P_n identifiziert wird und man erhält alle Permutationen, die benachbarte Ecken auf benachbarte abbilden:

- r: Rotation um $2\pi/n$ im mathematische positiven Sinn
- s: eine beliebige Spiegelung in D_n

Also hat man

$$\langle\{s,r\}\rangle = D_n = \left\{s^i r^j \mid i = 0,1, j = 0,\dots,n-1\right\}$$

und der Mächtigkeit $|D_n| = 2n$.

Für die erzeugenden Elemente $D_n = \langle\{s,r\}\rangle$ gilt:

- $srs = r^{n-1}$,
- $r^{n-1} = r^{-1}$,
- $r^n = 1$,
- $s^2 = 1$.

Im unendlichen Fall $D_\infty \subset S_\mathbb{Z}$ gilt z.B. $r(z) = z+1$, $s(z) = -z$, wobei r, $s\colon \mathbb{Z} \to \mathbb{Z}$ sind und D_∞

erzeugen: $D_\infty = \langle\{r, s\}\rangle$.

2. Nebenklassen, Normalteiler, Isomorphiesätze

Definition 2.1
$A, B \subseteq G$ Teilmengen (nicht unbedingt Untergruppen!), dann:

- $AB = \{xy \in G \mid x \in A, y \in B\}$
- $A^{-1} = \left\{x^{-1} \in G \mid x \in A\right\}$

▶ **Bemerkung 2.2**
$\varnothing \neq H \subseteq G$ ist Untergruppe $\Leftrightarrow HH = H$, $H^{-1} = H$

Definition 2.3
Ist $x \in G$, so nennen wir

$$f_x \colon G \to G \text{ mit } y \mapsto x^{-1}yx$$

den durch x definierten inneren Automorphismus. Ist $H < G$, so nennen wir $f(H) = x^{-1}Hx$ eine zu H konjugierte Untergruppe.

Satz 2.4

- f_x ist ein Endomorphismus von G (d.h. ein Morphismus $G \to G$)
- Das Bild $\operatorname{Im} f$ eines beliebigen Gruppenmorphismus $f \colon K \to L$ ist eine Untergruppe: $\operatorname{Im} f < L$

Beweis.

- $f_x(yz) = x^{-1}yzx = x^{-1}y(xx^{-1})zx = (x^{-1}yx)(x^{-1}zx) = f_x(y)f_x(z)\ \forall y, z \in G$
- Wir untersuchen die drei Eigenschaften:
  - $\operatorname{Im} f$ ist abgeschlossen: seien $f(y), f(z) \in \operatorname{Im} f$. Dann gilt:
    $$f(y)f(z) = f(yz) \in \operatorname{Im} f$$
  - $f(1) = 1 \implies 1 \in \operatorname{Im} f$
  - $f(x)^{-1} = f(x^{-1}) \implies (\operatorname{Im} f)^{-1} = \operatorname{Im} f$ □

Definition 2.5
Ist $H < G, x \in G$, so nennt man

$$G \supseteq xH = \{x\}H = \{xy \in G \mid y \in H\} \quad \text{linke Nebenklasse}$$
$$G \supseteq Hx = \{yx \in G \mid y \in H\} \quad \text{rechte Nebenklasse}$$

■ **Beispiel 2.6**
Sei $G = V$ Vektorraum über Körper K mit $+$ als Gruppenstruktur, dann ist $H = W < V$ ein Untervektorraum und $xH = x + W \subseteq V$ affiner Unterraum, Element von V/W

Dies verallgemeinert sich zu

Definition 2.7
Sei $H < G$, $G/H = \{xH \mid x \in G\} \subseteq \mathcal{P}(G)$

▶ **Bemerkung 2.8**
$xH = yH \Leftrightarrow x \sim y$ definiert eine Äquivalenzrelation und das ist äquivalent zu

$$\exists h \in H : x = yh \Leftrightarrow y^{-1}y \in H.$$

Beachte dabei $G/H = G/N$ ist die Menge aller Äquivalenzklassen $xH = [x]$. Desweiteren gibt es die kanonische Projektion $\pi\colon G \to G/H, x \mapsto xH$.

Insbesondere ist G die disjunkte Vereinigung aller Äquivalenzklassen. Speziell ist für jedes $x \in G$ definiert:

$$t_x\colon G \to G, y \mapsto xy \text{ eine Bijektion}, \quad H = 1H = [x] \to xH = [x].$$

Alle xH haben also die gleiche Kardinalität und wir erhalten:

Satz 2.9 (Lagrange, Klausur!)
Sei $|G| < \infty$ und $H < G$. Dann gilt $|G| = |G/H| \cdot |H|$. Insbesondere ist $|G|$ durch $|H|$ teilbar.

Beweis. Beweisskizze: Äquivalenzrelation und Bijektion $xH \cong yH$.
Let $H < G$ a subgroup of G and $xH := \{xy \mid y \in H\} \leq G$ the coset of H in G. Then we have $G/H = \{xH \mid x \in G\} \subseteq \mathcal{P}(G)$. Then

$$xH = \tilde{x}H \Leftrightarrow \exists y \in H \quad x = \tilde{x}y \Leftrightarrow \tilde{x}^{-1}x \in H$$
$$G = \bigcup_{xH \in G/H} xH \implies |G| = |G/H| \cdot |H|$$
$$|xH| = |H| \quad \forall x \in G.$$

□

Folgerung 2.10
Sei $|G| < \infty$, dann gilt $|x| \mid |G|$ für alle $x \in G$. Dabei ist $|x| = |\langle\{x\}\rangle| = \min\{n \mid x^n = 1\}$. Also z.B. $\langle\{x\}\rangle \cong (\mathbb{Z}_{|x|}, +)$. Insbesondere gilt für alle $x \in G$: $x^{|G|} = 1$

Folgerung 2.11 (Eulers Theorem)
$|U_n| = \varphi(n) = |\{m \in \{1, \ldots, n\} \mid \text{ggT}(n, m) = 1\}| = |\{(\mathbb{Z}_n^\times, \cdot) \mid \text{ggT}(n, m) = 1\}|$ mit $n \in \mathbb{N}$. Also ist $m^{\varphi(n)} = 1 \mod n$.

Definition 2.12 (Index)
Sei $H < G$, dann ist $[G : H] := |G/H|$ der Index von H in G.

Folgerung 2.13
Sei $K < H < G$ und $|G| < \infty$, dann

$$[G : K] = |G/K| = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H][H : K].$$

3. Morphismen

Definition 3.1
Ein injektiver Morphismus $f\colon G \to H$ wird auch Einbettung genannt. Ein Isomorphismus ist ein bijektiver Morphismus.

▶ **Bemerkung**
Ein injektiver Morphismus wird auch Monomorphismus genannt und ein surjektiver Morphismus Epimorphismus.

■ **Beispiel 3.2**

1) Betrachte die Determinate $\det\colon \mathrm{GL}(n,R) \to R^\times$, diese ist ein surjektiver Morphismus von Gruppen mit

$$\det(gh) = \det(g)\det(h)$$

2) Die Wahl einer Basis B in einem endlich erzeugten freien Modul V ist ein Isomorphismus von Moduln $s_B\colon R^{|B|} \to V$. Dieser induziert einen Gruppenisomorphismus

$$\mathrm{GL}(n,R) \to \mathrm{GL}(V), g \mapsto s_B \circ M_g \circ s_B^{-1}$$

3) Die Linkstranslation $t\colon G \to S_G$ mit $x \mapsto t_x$ (mit $t_x(y) = xy$) ist ein injektiver Gruppenhomomorphismus

$$(t_x \circ t_z)(y) = t_x(t_z(y)) = t_x(zy) = xzy = t_{xz}(y)$$

also

$$t_x \circ t_y = t_{xy} \quad \forall x, y \in G$$

Ist $t_x = t_z$, so gilt $t_x(1) = t_z(1)$ und daraus $x1 = z1$, also $x = z$

Also kann jede endliche Gruppe als Untergruppe der S_n verstanden werden ($n = |G|$)!

■ **Beispiel 3.3**

1) $y \mapsto f_{x^{-1}}\colon G \to G$, $y \mapsto xyx^{-1}$ ist ein Morphismus $G \to \mathrm{Aut}\, G$ mit

$$f_x(y) = x^{-1}yx, \quad f_z(f_x(y)) = z^{-1}(x^{-1}yx)z = (xz)^{-1}y(xz) = f_{xz},$$

und ist i.A. nicht injektiv! Denke an G abelsch $\Leftrightarrow f_x = \mathrm{id}_G\ \forall x \in G$

2) $\mathrm{sgn}\colon S_n \to \mathbb{Z}_2 = \{-1, 1\}$

4. Normalteiler

Definition 4.1 (normale Untergruppe)
Eine Untergruppe $H < G$ ist normal $\Leftrightarrow \forall x \in G\colon xH = Hx$.

Satz 4.2

$$H < G \text{ ist normal } \Leftrightarrow \forall x \in G x^{-1}Hx = H \Leftrightarrow AH = HA \quad \forall A \subseteq G$$

Beweis. Sei H normal und $x \in G$. Dann gilt $xH = Hx \implies x^{-1}xH = x^{-1}Hx$. Hier verwende $A, B \subseteq G, AB = \{ab \mid a \in A, b \in B\}$ definiert ein assoziatives Produkt $u \in \mathcal{P}(G)$, angewendet auf $A(BH) = (AB)H, A = \left\{x^{-1}\right\}, B = \{x\}$. Umgekehrt genauso $xH = Hx \implies x^{-1}xH = x^{-1}Hx$. Weiter gilt:

$$AH = \bigcup_{x \in A} xH, \quad HA = \bigcup_{x \in A} Hx$$

Also $xH = Hx \quad \forall x \in G \implies AH = HA \forall A \subseteq G$. Umgekehrt: Nimm $A = \{x\}$. □

Warum relevant?
Weil G/H eine Gruppenstruktur von G erbt $\Leftrightarrow H \triangleleft G$

Satz 4.3
Sei $H \triangleleft G$. Dann definiert

$$xH \cdot yH = (xy)H$$

eine Gruppenstruktur auf G/H und $\pi : G \to G$ mit $x \mapsto xH$ ist eine surjektiver Morphismus von Gruppen.

Beweis. $xH \cdot yH$ kann ich in $\mathcal{P}(G)$ immer bilden. Ist $H \triangleleft G$, gilt $xH = Hx$, also $xH \cdot yH = HxyH = xyHH = xyH$. (oder $A = \{x\}, B = \{y\}, C, D = H$). Anders gedacht: $H \triangleleft G$ heißt: $H \in Z(\mathcal{P}(G))$. Sprich: $G/H \subseteq \mathcal{P}(G)$ ist eine Unterhalbgruppe, d.h. abgeschlossen unter $\cdot$. Ferner gilt: $H = 1H$ ist ein Einselement $(xH)H = x(HH) = xH, H(xH) = (Hx)H = xH = (Hx)H = (xH)H$. Ausserdem ist G/H Gruppe

$$xH \cdot x^{-1}H = Hx \cdot x^{-1}H = H1H = HH = H$$

und genauso $x^{-1}HxH = H$. Sei $\pi : G \to G/H$ mit $x \mapsto xH$ also $\pi(xy) = \pi(x)\pi(y)$ mit $xyH = xH \cdot yH$. □

Definition 4.4 (Kern einer Gruppe)
Ist $f : G \to K$ ein Morphismus von Gruppen, so definieren wir den Kern $\ker f = \{x \in G \mid f(x) = 1_K\}$

▶ **Bemerkung**
Ist K eine abelsche Gruppe, so schreibt man die Gruppenoperation oft als $+$ und 1 oft als 0.

Satz 4.5
Es gilt $\ker(f) \triangleleft G$.

Beweis.
1. Sind $x, y \in \ker f$, so gilt $f(x)f(y) = f(xy)$ (und $11 = 1$), also ist $kerf$ abgeschlossen unter $\cdot$.
2. Ferner $f(1) = 1$, da f Morphismus $\implies G \ni 1 \in \ker f$.

3. Zuletzt: $f(x)^{-1} = f(x^{-1})$, dann

$$x \in \ker f \implies f(x) = 1 \implies f(x^{-1}) = f(x)^{-1} \implies x^{-1} \in \ker f$$

4. Ferner gilt für $x \in G, y \in \ker f$:

$$f(x^{-1}yx) = f(x^{-1}f(y)f(x)) = f(x^{-1}) \cdot 1 f(x) = f(x^{-1}x) = f(1) = 1 \text{ also}$$
$$x^{-1} \in \ker f \subseteq \ker f \text{ also}$$
$$(x^{-1})^{-1} \ker f(x^{-1}) \subseteq \ker f \implies \ker f \subseteq x^{-1} \ker fx$$

5. $\ker f \triangleleft G$.

also 1. 2. 3. : $\ker f < G$. □

▶ **Bemerkung**
Ist $H \triangleleft G$, so gilt: $H = \ker \pi$ mit $\pi : G \to G/H$. (denn $\pi(x) = xH$, also $\ker \pi = \{x \mid xH = H\} = H$).
Normalerteiler sind also die Kerne von Morphismen.

Satz 4.6 (1. Isomorphiesatz, Klausur)
Ein Morphismus $f : G \to K$ von Gruppen induziert einen Isomorphismus:

$$\bar{f} : G/\ker f \to \operatorname{Im} f \text{ mit } [x] = x \ker f \mapsto f(x)$$

Beweis. Der einzig schwere Teil ist $\bar{f}$ ist wohldefiniert. $f(xH) := f(x) \in \operatorname{Im} f$, also landet $\bar{f}$ in $\operatorname{Im} f$. Ferner gilt: Ist $x \ker f = y \ker f$, so ist $y^{-1}x \in \ker f$ (allgemein: $xH = yH \Leftrightarrow y^{-1}xH$) $\Leftrightarrow f(y^{-1}x) = 1 \Leftrightarrow f(y^{-1})f(x) = 1 \Leftrightarrow f(y)^{-1}f(x) = 1 \Leftrightarrow f(x) = f(y)$. Also ist $\bar{f}$ wohldefiniert und injektiv. Surjektiv ist $\bar{f}$ per Definition.
Letzter Schritt: $\bar{f}(x \ker f \cdot y \ker f) = \bar{f}(xy \cdot \ker f)$ (**???**). $\bar{f}(x \ker f)\bar{f}(y \ker f) = f(x)f(y) = f(xy)$. Also ist $\bar{f}$ ein Morphismus von Gruppen. □

■ **Beispiel 4.7**
Sei $G = (\mathbb{R}, +)$, $K = (\mathbb{C} \setminus \{0\}, \cdot)$ und $f(t) = \exp(2\pi i t)$, dann $f(x + y) = \exp(x) + \exp(y)$ also ein Gruppenmorphismus $G \to K$. Dann $\operatorname{Im} f = U(1) = S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ und $\ker f = \mathbb{Z}$. Also ist $\mathbb{R}/\mathbb{Z} \cong S^1$ ($\mathbb{R}^2/\mathbb{Z}^2 \cong T$ ist dann der Torus T, $U(n) = \left\{A \in \operatorname{Mat}(n, \mathbb{C}) \mid AA^T = 1\right\}$ unitäre Gruppe)

Definition 4.8 (einfache Gruppe)
Eine Gruppe G ist einfach, wenn $H \triangleleft G \implies H = G$ und $H = \{1\}$.

▶ **Bemerkung**
D.h.: Ist $f : G \to K$ irgendein Morphismus, so ist $G \cong \operatorname{Im} f$ ($\ker f = \{1\}$) oder $\operatorname{Im} f = \{1\}$ ($\ker f = G$).

Die endlichen einfachen Gruppen sind klassifiziert!

■ **Beispiel 4.9**

1. Sei $G = \mathbb{Z}_p, p$ prim hat nach Lagrange (Satz 2.9) noch nicht mal irgendeine echte Untergruppe, ist also einfach.
2. $\operatorname{SL}(n, \mathbb{Z}_p)/Z(\operatorname{SL}(n, \mathbb{Z}_p)) = \operatorname{PSL}(n, \mathbb{Z}_p)$ (projective linear group)

Satz 4.10 (Korrespondenztheorem)
Ist $H \triangleleft G$, so induziert (definiert) $\pi : G \to G/H$ einen Isomorphismus von teilgeordneten Mengen (partial ordered sets)

$$\{L < G \mid H < L\} \to \{K < G/H\} \text{ mit } L \mapsto \pi(L)$$

Dieser erhält und reflektiert Normalität und auch Unterquotienten.

Satz 4.11 (2. Isomorphiesatz, Klausur)
Let $H < G$, $K \triangleleft G \implies H \cap K \triangleleft H, K \triangleleft H, K < G$ und

$$H/H \cap K \to HK/K \text{ with } x(H \cap K) \mapsto xK$$

ist ein Isomorphismus.

Beweis. 1. Durchschnitte von Untergruppen sind Untergruppen, also $H \cap K < H$. Ist ferner $x \in H$ und $y \in H \cap K$, so gilt $xyx^{-1} \in H$ (da H Untergruppe) und $xyx^{-1} \in K$, da $x \in G$ und $y \in K$ und auch $K \triangleleft G$. Also gilt $xyx^{-1} \in H \cap K$.

2. Auch klar, da $(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$ (wobei $K \triangleleft G$), Bemerkung: $H, K < G$ reicht nicht, HK ist i.A. keine Untergruppe von G. Klar das $1 = 1 \cdot 1 \in HK, 1 \in H, 1 \in K$ (da $H, K < G$).

   $$x \in H, y \in K \quad (xy)^{-1} = y^{-1}x^{-1} \implies (HK)^{-1} = K^{-1}H^{-1} = KH = KH, \text{ da } K \triangleleft G.$$

   Also gilt $HK < G$. $K \triangleleft HK$, wie im ersten Punkt des Beweises.

3. $$\varphi : H/H \cap K \to HK/K \text{ mit } (H \cap K) \mapsto xK$$

   wohldefiniert? Natürlich: Ist $x(H \cap K) = y(H \cap K)$ $x, y \in H$, so folgt $x = yz$ mit $z \in H \cap K$, also $yK = xK$, da 2. eben insbesondere in K ist. Gruppenhomomorphismus auch klar, da

   $$\varphi(x(H \cap K) \cdot y(H \cap K) = \varphi(xy(H \cap K)) = xyK$$
   $$\varphi(x(H \cap K))\varphi(y(H \cap K)) = xKyK$$ □

Lemma 4.12
$\varphi : G \to H$ ist injektiv genau, dann wenn $\ker \varphi = \{1\}$.

Beweis. Auf diesen Fall angewendet:

$$\ker \varphi = \{x(H \cap K) \subset H/H \cap K \mid xK = K\}$$

$xK = K$ heisst aber nichts anderes als $x \in K$, d.h.

$$\ker \varphi = \{x(H \cap K) \mid x \in H \cap K\} = H \cap K = 1$$

(in der Gruppe $H/H \cap K$) und surjektiv ist klar, da $xyK = xK$ für $x \in H, y \in K$. □

Satz 4.13 (3. Isomorphiesatz)
Sei $H \triangleleft G, K \triangleleft G, K < H$ impliziert $H/K \triangleleft G/H$ und es gilt

$$G/K \to H/H/H/K \text{ mit } xK \mapsto (xH) \cdot H/K$$

ist ein Isomorphismus.

5. Einfache Gruppen

Definition 5.1
G ist einfach, genau dann wenn $\{1\}, G$ sind die einzigen Normalteiler.

$$\varphi : G \to H \text{ mit } \operatorname{Im}\varphi = G/G/\ker\varphi$$
$$\operatorname{Im}\varphi \cong G \text{ oder } \operatorname{Im}\varphi = \{1\}$$

■ **Beispiel**
$G = \mathbb{Z}_p, p$ prim.

Satz 5.2
A_n ist einfach für $n > 4$.

▶ **Bemerkung**
$A_4 \triangleright \{(), (12)(34), (13)(24), (14)(23)\}$, d.h. A_4 ist nicht einfach.

Lemma 5.3
1. $S_n = \langle (ii+1) \rangle$ für $i = 1, \ldots, n-1$
2. $A_n = \langle (ijk) \rangle$

Beweis. 1. Betrachte $(23)(12)(23) = (13)$ und $(34)(13)(34) = (14)$, per Induktion folgt

$$(1i) \in \langle (ii+1) \rangle \text{ und } (1i)(1j)(1i) = (ij) \quad (i \neq j) \implies (ij) = \langle (rr+1) \rangle \quad r = 1, \ldots n-1$$

damit folgt 1.

2.

$$(ij)(jk) = (ijk) \text{ und } (ij)(kr) = (ijk)(jkr)$$

also folgt 2. □

Beweis (Satz 5.2). Sei $N \neq \{1\}$ Normalteiler von $A_n, n > 4$

1. Ist $(yk) \in N$, so gilt $(abc) \in N$ für alle a, b, c. Ist $\sigma \in S_n$, so gilt $\sigma(ijk)\sigma^{-1} = (\sigma(i)\sigma(j)\sigma(k))$ (siehe ÜA 5, 1. Blatt) Sei $\sigma \in S_n$so, dass $\sigma(i) = a$, $\sigma(j) = b$ und natürlich $\sigma(k) = c$. Ist $\sigma \in A_n$ so folgt (da $N \triangleleft A_n$, $(abc) \in N$). Wenn nicht wähle r, s ungleich und setze $\tilde{\sigma} := \sigma(rs) \in A_n$. Dann ist $\tilde{\sigma}(ijk)\tilde{\sigma}^{-1} =$

$\sigma(rs)(ijk)(rs)\sigma^{-1} = (abc)$.

2. Bleibt zu zeigen: $\exists(ijk) \in N$. Sei

$$1 \neq \sigma = \gamma_1\gamma_2 \dots \gamma_r \in N \text{ beliebig,}$$

wobei γ_i Zykel ist und die Länge der Zykel γ_i nicht wachse also $l(\gamma_i) \geq l(\gamma_{i+1})$. Fallunterscheidung: (Ziel ist in jedem Fall gibt es ein $(ijk) \in N$.)

(a) $l(\gamma_i) \geq 4$:
Sei $\gamma_1 = (i_1, \dots, i_k)$ und $\pi(i_1 i_2 i_3)$

$$\implies \pi_{\gamma_j} = \gamma_j\pi \quad \forall j > 1\sigma^{-1} \quad \underbrace{\pi^{-1}\sigma\pi}_{\in N,\text{ da } N\lhd A_n} = (i_1 i_2 i_4) \subset N$$

also einfach Nachrechnen.

(b) $l(\gamma_1) - l(\gamma_2) = 3$:
Sei $\gamma_1 = (ijk), \gamma_2 = (pqs)$. Nimm $\pi = (kpq)$ und daraus folgt $\sigma^{-1}\pi^{-1}\sigma\pi = (isk)$

(c) $l(\gamma_1) = 3, l(\gamma_2) = 2$:
$\gamma_1 = (ijk) \implies \sigma^2 = (ikj)$

(d) $l(\gamma_1) = l(\gamma_2) = 2, r = 2$:
Sei $\gamma_1 = (ij)$, $\gamma_2 = (kl)$ $n \geq 5 \implies \exists m \notin \{i, j, k, l\}$ und $\pi = (ijm)$
$\sigma\pi^{-1}\sigma\pi = (imj) \in N$

(e) $l(\gamma_i) = 2 \forall i, r > 2$:
$\sigma \in A_n$, $\gamma_1 = (ij)$, $\gamma_2 = (kl)$, sowie $\gamma_3 = (pq)$, $\gamma_4 = (st)$, setze $\pi = (ip)(jk)$ und $\sigma\pi\sigma\pi = (ipl)(jkq)$ und benutze Fall 2. □

Definition 5.4
Eine kurze Sequence von Gruppen ist ein Paar von Morphismen $f : H \to G$ mit $g : G \to K$ und dann

1. f ist injectiv
2. g ist surjektiv
3. $\operatorname{Im} f = \ker g$

Man schreibt auch:

$$\{1\} \longrightarrow H \xrightarrow{f} G \xrightarrow{g} K \longrightarrow \{1\}$$

Sprich: H ist (isomorph zu einer) normalen Untergruppe von G und K ist (isomorph zu) G/H
Allgemeiner: exakte Folgen:

$$\dots \xrightarrow{f_i} G_{i-1} \xrightarrow{f_{i-1}} G_{i-2} \longrightarrow \dots \qquad \operatorname{Im} f_i = \ker f_{i-1}$$

Einfachster Fall ($\implies$ langweiliger) Fall: Direkte Produkte

Definition 5.5 (äußeres direktes Produkt)
Seien H, K Gruppen. Auf der Menge $G := H \times K$ (Wenn sowas im Buch steht ist es direktes Produkt gemeint) erhalten von einer Gruppenstruktur durch

$$(a, b)(x, y) := (ax, by) \text{ mit } a, b \in H, x, y \in K$$

Definition 5.6 (inneres direktes Produkt)
Sei G Gruppe und $H, K \triangleleft G$ mit

1. $H \cap K = \{1\}$
2. $HK = G$

Dann nennen wir G das innere direkte Produkt von H und K.

Satz 5.7
Ist G das innere direkte Produkt von $H, K \triangleleft G$, so gilt

$$G \cong H \times K$$

als Gruppe.

Beweis. Wir zeigen, dass $\varphi : H \times K \to G$ mit $(a, b) \mapsto ab$ ein Isomorphismus von Gruppen ist. Es gilt für alle $a, x \in H, b, y \in K$.

$$\varphi((a,b)) \cdot \varphi((x,y)) = abxy = axx^{-1}bxb^{-1}by = axby = \varphi((ax, by))$$

denn der Kommutator $x^{-1}bxb^{-1}$ liegt in $H \cap K = \{1\}$. (denn $x^{-1}bx \in K$, da $K \triangleleft G$, also $x^{-1}bxb^{-1} \in K$, genauso $bxb^{-1} \in H$, da $H \triangleleft G$, also $x^{-1}bxb^{-1} \in H$) Nach Annahme 1. ist φ surjektiv. Die Abbildung ist injektiv, denn

$$ab = xy \implies x^{-1}a = yb^{-1} \in G \cap K = \{1\} \implies x = a, y = b \quad \forall y, x \in H, b, y \in K. \qquad \square$$

▶ **Bemerkung**
In diesem Fall ist $G/H \cong K, G/K \cong H$

$$1 \longrightarrow H \longrightarrow G \longrightarrow K \longrightarrow 1$$

$$1 \longrightarrow K \longrightarrow G \longrightarrow H \longrightarrow 1$$

■ **Beispiel**
Sei $G = D_6$, also die Sachen, die man mit einem Hexagon machen kann.

$$H = \left\{1, r^3\right\} \cong \mathbb{Z}_2 \text{ und } K = \left\{s^j r^{2i} \mid i = 0, 1, 2, j = 0, 1\right\} \cong D_3$$
$$D_6 \cong \mathbb{Z}_2 \times D_3$$

Kompositionsreihen und Jordan-Hölder.

Definition 5.8 (Kette,Subnormale Reihe,einfache Kompositionsreihe)
Eine Reihe in G ist eine Kette von Untergruppen

$$G = G_0 > G_1 > G_2 > \cdots > G_d = \{1\} \text{ mit } G_{i+1} \neq G,$$

Eine subnormale Reihe ist eine in der $G_{i+1} \triangleleft G_i$ gilt ($G_i \triangleleft G$ für alle $i \Leftrightarrow$ "normale Reihe"). Eine Kompositionsreihe ist eine solche mit G_i/G_{i+1} einfach.

▶ **Bemerkung**

Nach dem Korrespondenztheorem heisst G_i/G_{i+1} einfach genau, dass $G_{i+1} \triangleleft G_i$ eine maximale normale Untergruppe ist.

$$\{L < G_i \mid G_{i+1} < L\} \xrightarrow{\pi} \{P < G_i/G_{i+1}\}$$

■ **Beispiel 5.9**

Sei $G = G_0 = S_4, G_1 = A_4, S_4/A_4 \cong \mathbb{Z}_2$ (nach 1. Isomorphiesatz, $A_4 = \ker \operatorname{sgn}$ mit $\operatorname{sgn} : S_4 \to \mathbb{Z}_2$). Und die $G_2 = N = \{(12)(34), (13)(24), (14)(23), 1\}$ KLEINsche Vierergruppe. Dann

$$|A_4/N| = \frac{|A_4|}{|N|} = \frac{12}{4} = 3 \quad \text{Lagrange Theorem}$$
$$\implies A_4/N \cong \mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z} \text{ einfach.}$$

$$G_3 := \{1\}$$

$\{1\} \triangleleft H \triangleleft A_4 \triangleleft S_4$ ist Kompositionsreihe

$$\{1\} \longrightarrow N \longrightarrow A_4 \longrightarrow \mathbb{Z}_3 \longrightarrow \{1\}$$

$$\{1\} \longrightarrow A_4 \longrightarrow S_4 \longrightarrow \mathbb{Z}_2 \longrightarrow \{1\}$$

wobei $N, \mathbb{Z}_3, \mathbb{Z}_2$ einfach ist und A_4 gerade gebaut.

Satz 5.10

Ist G endliche Gruppe, so besitzt G eine Kompositionsreihe.

Beweis. Induktion nach $|G|$. Also $G = G_0$ gegeben

1. G einfach, dann $G_1 = \{1\}$ und $\checkmark G = G_0 \triangleright \{1\} = G_1$, also $G_0/G_1 = G$
2. G nicht einfach dann G_1 maximale normale Untergruppe, gibts da $|G| < \infty$. Dann $|G_1| < |G|$, also existiert nach Induktion Kompositionsreihe

   $$G_1 \triangleright G_2 \triangleright G_3 \triangleright \cdots \triangleright G_d \triangleright \{1\}$$

   Also $G_0 \triangleright G_1 \triangleright \ldots$ "tuts". □

■ **Beispiel**

$G = \mathbb{Z}$ hat keine Kompositionsreihe, denn

$$\mathbb{Z} = G_0 \triangleright G_1 \implies G_1 \cong \mathbb{Z}$$

Satz 5.11 (Jordan-Hölder)
Sei G endliche Gruppe und seien $\{H_i\}_{i=0,\dots,p}$ und $\{G_j\}_{j=0,\dots,n}$ zwei Kompositionsreihe der Länge p. Dann gilt $p = n$ und ex existiert $\sigma \in S_{0,\dots,n-1}$ mit

$$G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$$

Beweis.

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$$
$$G = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_p = \{1\}$$

Beweis erfolgt durch Induktion nach $m = \min(n, p)$
Beweise zuerst folgende Behauptung:
Ist $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_1 = 1$ Kompositionsreihe und $N \triangleleft G$, so ist $N = N \cap G_0 \triangleright N \cap N_1 \triangleright \ldots, \triangleright N \cap 1 = 1$ Kompositionsreihe (gegebenenfalls nach Auslassen von $N \cap G_1 = N$ß*cap*G_{i+1})

Beweis.

$$N \cap G_i/N \cap G_{i+1} = N \cap G_i/(N \cap G_i) \cap G_{i+1} \text{ mit } (G_{i+1} < G_1!)$$
$$\cong (N \cap G_1)G_{i+1}/G_{i+1} \triangleleft G_i/G_{i+1} \text{ einfach} \quad \cong \text{ da 2. Isomorphiesatz}$$

Also $N \cap G_i/N \cap G_{i+1} \cong G_i/G_{i+1}$ oder $N \cap G_i/N \cap G_{i+1} \Leftrightarrow N \cap G_i = N \cap G_{i+1}$. □

1. Fall 1: $G_1 = H_1$ folgt mit Induktion

$$G_i = H_1 \triangleright G_2 \triangleright \ldots \triangleright G_n = \{1\}$$
$$G_i = H_1 \triangleright G_2 \triangleright \ldots \triangleright H_p = \{1\}$$

2. Fall 2: $G_1 \neq H_1$. Dann ist $G \cap H_1 \triangleleft G_1$ (nicht gleich!). Beachte Nach Korrespondenztheorem ist $H_1 \leq ...$ □

Anhang

Index