I GRUPPEN

§1 GRUPPENAXIOME, UNTERGRUPPEN, BEISPIELE

1.1. Halbgruppen

Sei M eine Menge; eine (innere) Verknüpfung auf M ist eine Abbildung $*: M \times M \to M$, $(a,b) \mapsto a * b$

$*$ heißt assoziativ, falls

$$(a*b)*c = a*(b*c) \quad \forall a,b,c \in M,$$

und kommutativ, falls

$$a*b = b*a \quad \forall a,b \in M.$$

DEF: (i) Eine Menge H zusammen mit einer assoziativen Verknüpfung $*$ darauf heißt Halbgruppe; Schreibweise: $(H,*)$ ist Halbgruppe.

(ii) Sei $(H,*)$ eine Halbgruppe. Ein Element $e \in H$ heißt neutral (bzgl. $*$), falls

$$a = e*a = a*e \quad \forall a \in H.$$

BEM: e linksneutral, falls $a = e * a \quad \forall a \in H$;
(ähnlich rechtsneutral)

„Sätzchen": Ein neutrales Element ist eindeutig.

„Beweischen": seien e und e' neutral in $(H, *)$, dann folgt $e = e * e' = e'$ $\square$

BEISP: 1) $\mathbb{N} = \{0, 1, 2, \dots\}$

$(\mathbb{N}, +)$ kommutative Halbgruppe, 0 neutral

$(\mathbb{N}, \cdot)$ —— // ——, 1 neutral

2) $M \neq \emptyset$, $H := \{f : M \to M\}$ mit Verknüpfung von Abbildungen $(f \circ g)(x) = f(g(x))$, $f, g \in H$, $x \in M$

$f \circ (g \circ h) = (f \circ g) \circ h$ [1. Semester]

$id_M : M \to M$, $x \mapsto x$ ... identische Abb; ist neutral,

denn $(f \circ id_M)(x) = f(id_M(x)) = f(x)$ und

$(id_M \circ f)(x) = id_M(f(x)) = f(x) \quad \forall x \in M$

Bem: $|M| \geq 2 \Rightarrow (H, \circ)$ nicht kommutativ

3) $(M(n, \mathbb{R}), +)$ komm. Halbgr.; $(M(n, \mathbb{R}), \cdot)$ Halbgruppe nicht komm., falls $n \geq 2$

1.2. Gruppen

DEF: Eine Menge G mit Verknüpfung $*: G \times G \to G$ heißt Gruppe, wenn gilt:

(G1) $*$ ist assoziativ,

(G2) (a) $\exists$ (eindeutiges) neutrales Element $e \in G$, $\Big\}$ $(G,*)$ Halbgruppe mit neutr. El. e

(b) $\forall a \in G \; \exists! \, b \in G: b * a = a * b = e$.

b heißt Inverses zu a; wir schreiben $b = a^{-1}$.

$(G,*)$ heißt kommutative (oder abelsche) Gruppe, wenn $*$ kommutativ ist.

Schreibweisen: oft $a \cdot b$ oder ab statt $a*b$; bei abelschen Gruppen meistens $a+b$ statt $a*b$; neutr. El. bzgl $+$ mit 0, bzgl. $\cdot$ mit 1 bezeichnet; additiv Inverses zu a mit $-a$ notiert.

BEM: (i) durch Induktion: Assoziativität für endlich viele Faktoren, d.h. $a_1 * a_2 * \ldots * a_n$ sinnvoll definiert und unabhängig von Klammerung

(ii) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, denn $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a(b b^{-1}) a^{-1} = a a^{-1} = e$

und $(b^{-1} a^{-1})(a b) = b^{-1}(a^{-1} a) b = b^{-1} b = e$

LEMMA: Beim Nachweis der Gruppeneigenschaften genügt es, statt (G2) die folgende Version zu zeigen:

(G2') $\exists\, e \in G$ mit Eig:

(a) $e * a = a \quad \forall a \in G$ (e linksneutral),

(b) $\forall a \in G\ \exists b \in G : b * a = e$ (Linksinverses),

d.h. aus (G1) und (G2') folgt (G2).

Beweis: 1. Schritt: Jedes Linksinverse ist auch Rechtsinverses

sei b linksinvers zu a, d.h. $b \cdot a = e$, und sei c linksinvers zu b, d.h. $cb = e$; dann folgt

$$ab = (ea)b = ((cb)a)b = (c(ba))b = (ce)b = cb = e.$$

2. Schritt: e linksneutral $\Rightarrow$ e rechtsneutral;

insbesondere dann e wegen Sätzchen 1.1 eindeutig.

sei $a \in G$ mit Linksinversem $b \in G$, d.h. $ba = e$; wegen 1. Schritt auch $ab = e$; daher

$$ae = a(ba) = (ab)a = ea = a.$$

3. Schritt: Linksinverses ist eindeutig (somit ebenso Rechtsinv. eind.)

seien b, b' linksinvers zu a, dann gilt

$$b = eb = (b'a)b = b'(ab) = b'e = b' \qquad \square$$

BEISP: 1) $(\mathbb{Z},+)$ abelsche Gruppe

2) $(\mathbb{Z}_m,+)$ abelsche Gruppe mit m Elementen

3) $(S_3,\circ)$ nichtabelsche Gruppe mit $3!=6$ Elementen

(– siehe Einleitung zur VO)

SATZ: In einer Gruppe G sind für jedes $a\in G$ die Abbildungen $l_a: G\to G,\ x\mapsto a\cdot x$ (Linkstranslation) und $r_a: G\to G,\ x\mapsto x\cdot a$ (Rechtstranslation) bijektiv.

Insbesondere gelten die Kürzungsregeln:

$$ax=ay \Rightarrow x=y,$$
$$xa=ya \Rightarrow x=y.$$

Beweis: $l_a(x)=b \Leftrightarrow ax=b \Leftrightarrow x=a^{-1}b$, somit l_a injektiv und surj.;

ebenso $r_a(x)=b \Leftrightarrow x\cdot a=b \Leftrightarrow x=ba^{-1}$.

(x eindeutig)

(für jedes b lösbar)

$ax=ay$ bedeutet $l_a(x)=l_a(y)$, also $x=y$, weil l_a inj.

$xa=ya$ heißt $r_a(x)=r_a(y)$, also $x=y$

$\square$

1.3. Untergruppen

DEF: Sei G eine Gruppe und $H \subseteq G$. Dann heißt H Untergruppe von G, wir schreiben $H < G$, falls gilt

(U1) $a, b \in H \Rightarrow a \cdot b \in H$ (d.h. $(a,b) \mapsto a \cdot b$ ist Verknüpfung auf H; H ist „abgeschlossen" unter $\cdot$)

(U2) $(H, \cdot)$ ist eine Gruppe

LEMMA: $H \subseteq G$ ist Untergruppe genau dann, wenn $H \neq \emptyset$ und $\forall a, b \in H: a \cdot b^{-1} \in H$.

Beweis: 1) Wenn H Untergruppe $\Rightarrow \exists e \in H \Rightarrow H \neq \emptyset$; weiters $b^{-1} \in H$ und $a \cdot b^{-1} \in H$, weil $(H, \cdot)$ selbst Gruppe ist.

2) • Assoz.gesetz gilt in G, daher auch für alle Elemente von H;

• $H \neq \emptyset \Rightarrow \exists a \in H$; weiters $a \cdot a^{-1} = e \in H$;

• $b \in H \Rightarrow e b^{-1} = b^{-1} \in H$, also Inverse ex. in H;

• H abgeschlossen unter $\cdot$, denn mit $a, b \in H$ ist $a \cdot b = a \cdot (b^{-1})^{-1} \in H$ $\square$

BEM: (i) die Untergruppen $\{e\}$ und G gibt es immer; sogenannte triviale Untergruppen

(ii) $H_1 < G$ und $H_2 < G \Rightarrow H_1 \cap H_2 < G$

[Beweis in UE]

(gilt auch für beliebig viele Untergruppen)

SATZ: Sei G eine Gruppe und $M \subseteq G$ eine Teilmenge.

$$\mathrm{Erz}(M) := \{ a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \mid n \in \mathbb{N},\ a_i \in M,\ \varepsilon_i = \pm 1 \}$$

(Menge aller endlichen Produkte von Elementen aus M und ihren Inversen)

ist eine Untergruppe von G; die sogenannte von M erzeugte Untergruppe. $\mathrm{Erz}(\emptyset) := \{e\}$.
[bzw. $n=0$ oben]

Beweis: wegen $\{e\} \subseteq \mathrm{Erz}(M)$ ist $\mathrm{Erz}(M) \neq \emptyset$;

ist $a := a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$, $b := b_1^{\delta_1} \cdots b_m^{\delta_m} \in \mathrm{Erz}(M)$, denn

$$a \cdot b^{-1} = a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} \cdot b_m^{-\delta_m} \cdots b_1^{-\delta_1} = c_1^{\alpha_1} \cdots c_{n+m}^{\alpha_{n+m}}$$

mit $c_i = a_i$ $(1 \le i \le n)$, $c_j = b_{n+m+1-j}$ $(n+1 \le j \le n+m)$

$\alpha_i = \varepsilon_i$, $\alpha_j = -\delta_{n+m+1-j}$

also $a \cdot b^{-1} \in \mathrm{Erz}(M)$; Lemma $\Rightarrow$ $\mathrm{Erz}(M)$ Unt.gr. $\square$

BEM: (iii) G abelsch, dann können gleiche Faktoren in $Erz(M)$ immer zusammengeführt werden, z.B.: $a \cdot b^{-1} \cdot a \cdot c = a^2 \cdot b^{-1} \cdot c$; somit

$$Erz(M) = \{ a_1^{k_1} \cdots a_n^{k_n} \mid n \in \mathbb{N},\ k_i \in \mathbb{Z} \}$$

bzw. additiv geschrieben $\{ k_1 a_1 + \ldots + k_n a_n \mid k_i \in \mathbb{Z} \}$

(iv) Eine Gruppe G heißt endlich erzeugt, falls eine endliche Menge $M \subseteq G$ existiert mit $G = Erz(M)$. Falls $|M| = 1$, heißt G zyklisch; es ist dann $G = \{ a^k \mid k \in \mathbb{Z} \}$.

Beispiel: $\mathbb{Z} = Erz(\{1\})$
die zyklische Gruppe

1.4. Weitere Beispiele:

1) endliche Gruppen können (im Prinzip) durch Gruppentafeln beschrieben werden: z.B. für 3 El.

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

klar

klar

in jeder Zeile und Spalte muss jedes El. genau einmal vorkommen

~ „algebraisches Sudoku"

diese sind dann fixiert

$a^3 = e$

$G = Erz(\{a\})$

hier e würde unterhalb b erzwingen, dann doppelt in 3. Z.

2) V $\mathbb{K}$-Vektorraum

$GL(V) := \{ f: V \to V \mid \underbrace{f \text{ linear und bijektiv}}^{\text{VR-Isomorphismus}} \}$

mit Verknüpfung $\circ$ von Abb.;

Verknüpf. lin. Abb. ist linear; Assoz. gilt sowieso für alle Abb. bzgl. $\circ$

neutr. El. id_V; Inverse einer bij. lin. Abb. ist linear

„<u>general linear group</u>" (daher GL ... gen. lin.)

- für $V = \mathbb{R}^n$ ist $GL(V)$ beschreibbar als $GL(n, \mathbb{R})$ .... invertierbare $n \times n$-Matrizen über $\mathbb{R}$ mit Matrixmultiplikation; neutr. El. $I_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ nichtkommutativ für $n \geq 2$.
- analog $GL(n, \mathbb{C})$

3) $O(n) := \{ A \in GL(n, \mathbb{R}) \mid A \cdot A^t = I_n \} < GL(n, \mathbb{R})$

<u>orthogonale Gruppe</u> [Beweis in UE]

4) $(\mathbb{R}_+, \cdot)$ pos. reelle Zahlen mit Mult. sind Gruppe

5) $S^1 := \{ z \in \mathbb{C} \mid |z| = 1 \}$ ist Untergruppe von $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ bzgl. Multiplikation

§2 HOMOMORPHISMEN UND NORMALTEILER

2.1. Homomorphismen [homo-morph... griech.: „gleichgestaltig"]

DEF: Seien $(G,*)$ und $(G',*')$ Gruppen. $\varphi: G \to G'$ heißt Homomorphismus, wenn gilt

$$\varphi(a*b) = \varphi(a) *' \varphi(b) \quad \forall a,b \in G$$

(„φ respektiert die Gruppenverknüpfungen").

Ein bijektiver Homomorphismus heißt Isomorphismus; dann: G isomorph mit G', wir schreiben $G \cong G'$.
Homomorphismen $G \to G$ werden auch Endomorphismen genannt, Isomorphismen $G \to G$ auch Automorphismen.

Bild von φ.... $\mathrm{Im}(\varphi) := \varphi(G) \subseteq G'$

Kern von φ.... $\mathrm{Ker}(\varphi) := \{a \in G \mid \varphi(a) = e'\}$

neutr. El. in G'

Eigenschaften: (a) $\varphi(e) = e'$

(b) $\forall a \in G: \ \varphi(a)^{-1} = \varphi(a^{-1})$

(c) $H < G \Rightarrow \varphi(H) < G'$

(d) $H' < G' \Rightarrow \underbrace{\varphi^{-1}(H')}_{\text{Urbildmenge } \{a \in G \mid \varphi(a) \in H'\}} < G$

(e) φ injektiv $\Leftrightarrow \operatorname{Ker}(\varphi) = \{e\}$

(f) φ Isomorphismus $\Rightarrow \varphi^{-1}: G' \to G$ Isomorphismus

(g) $\psi: G' \to G''$ weiterer Homomorphismus

$\Rightarrow \psi \circ \varphi: G \to G''$ Homomorphismus

Beweis: (a) $\varphi(e) = \varphi(e \cdot e) = \varphi(e) \cdot \varphi(e) \overset{[\text{Kürz.reg.}]}{\Rightarrow} \varphi(e) = e'$

[wieder Schreibweise vereinfachen zu $\varphi(a) \cdot \varphi(b)$ statt $\varphi(a) *' \varphi(b)$ etc]

(b) $e' = \varphi(e) = \varphi(a a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) \Rightarrow \varphi(a)^{-1} = \varphi(a^{-1})$

(c) $a', b' \in \varphi(H) \Rightarrow \exists\, a, b \in H: a' = \varphi(a),\ b' = \varphi(b) \Rightarrow$

$a' \cdot (b')^{-1} = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(\underbrace{a b^{-1}}_{\in H}) \in \varphi(H)$

$[\varphi(e) \in \varphi(H) \Rightarrow \varphi(H) \neq \emptyset]$

(d) $a, b \in \varphi^{-1}(H') \Rightarrow \varphi(a), \varphi(b) \in H' \Rightarrow$

$\varphi(a b^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} \in H' \Rightarrow a \cdot b^{-1} \in \varphi^{-1}(H')$

(e) $\Rightarrow$: $e \in \operatorname{Ker}(\varphi)$, weil $\varphi(e) = e'$; $\varphi(a) = e' = \varphi(e)$

$\Rightarrow a = e$, weil φ inj.

$\Leftarrow$: $a, b \in G$ mit $\varphi(a) = \varphi(b) \Rightarrow \varphi(a b^{-1}) = \varphi(a) \cdot \varphi(b)^{-1} = e'$

$\Rightarrow a b^{-1} \in \operatorname{Ker}(\varphi) = \{e\} \Rightarrow a = b$; also φ injektiv

(f) • φ^{-1} Homomorphismus: $a', b' \in G' \Rightarrow \exists\, a, b \in G : a' = \varphi(a),$
$b' = \varphi(b),$

daher auch $a = \varphi^{-1}(a'), b = \varphi^{-1}(b')$; somit

$$\underline{\varphi^{-1}(a'b')} = \varphi^{-1}(\varphi(a)\cdot\varphi(b)) = \varphi^{-1}(\varphi(a\cdot b)) = a\cdot b = \underline{\varphi^{-1}(a')\cdot\varphi^{-1}(b')}$$

• φ^{-1} bijektiv, weil Inverse zu φ

(g) $a, b \in G$: $\underline{(\psi\circ\varphi)(a\cdot b)} = \psi(\varphi(ab)) = \psi(\varphi(a)\varphi(b)) =$

$= \psi(\varphi(a))\cdot\psi(\varphi(b)) = \underline{(\psi\circ\varphi)(a)\cdot(\psi\circ\varphi)(b)}$

$\square$

<u>KOR</u>: $\mathrm{Aut}(G) := \{\varphi : G \to G \mid \varphi \text{ Automorphismus}\}$ ist eine Gruppe bzgl. Verknüpfung von Abbildungen.

Beweis: • $\varphi\circ\psi$ wieder bijektiv, wenn φ und ψ bijektiv

• $\varphi, \psi : G \to G$ Homo. $\Rightarrow \varphi\circ\psi$ Homo. [(g) oben]

Also: $\varphi, \psi \in \mathrm{Aut}(G) \Rightarrow \varphi\circ\psi \in \mathrm{Aut}(G)$

• neutr. El. id_G ; • Assoziativität von $\circ$ gilt für alle Abbildungen

• Inverses zu φ ist φ^{-1} und $\varphi^{-1} \in \mathrm{Aut}(G)$ [(f) oben]

$\square$

<u>BEISP.</u>: 1) $m \in \mathbb{N}, m \geq 1$; $\varphi_m: \mathbb{Z} \to \mathbb{Z}, k \mapsto m \cdot k$ ist injektiver Homo.: $\varphi_m(k+l) = m \cdot (k+l) = mk + ml = \varphi_m(k) + \varphi_m(l)$;

$\varphi_m(k) = 0 \Leftrightarrow mk = 0 \Leftrightarrow k = 0$, also $\operatorname{Ker} \varphi_m = \{0\}$;

$\operatorname{Im} \varphi_m = \varphi_m(\mathbb{Z}) = m\mathbb{Z}$

2) $\varphi: \mathbb{Z} \to \mathbb{Z}_m, k \mapsto \bar{k} = k + m\mathbb{Z}$ ist surjektiver Homo. mit $\operatorname{Ker} \varphi = m\mathbb{Z}$: $\varphi(k+l) = \overline{k+l} = \bar{k} + \bar{l} = \varphi(k) + \varphi(l)$;

$\bar{l} \in \mathbb{Z}_m$, denn $\varphi(l) = \bar{l}$, also surjektiv;

$\varphi(m \cdot l) = \overline{m \cdot l} = \bar{0}$ und $\varphi(k) = \bar{0} \Rightarrow k \in m\mathbb{Z}$,

somit $\operatorname{Ker} \varphi = m\mathbb{Z}$

3) $\varphi: \mathbb{Z} \to S^1 = \{z \in \mathbb{C} \mid |z| = 1\}, k \mapsto \zeta_m^k = \left(e^{\frac{2\pi i}{m}}\right)^k = e^{\frac{2\pi i k}{m}}$

Homo.: $\varphi(k+l) = \zeta_m^{k+l} = \zeta_m^k \cdot \zeta_m^l = \varphi(k) \cdot \varphi(l)$

$\operatorname{Im} \varphi = C_m = \{\zeta_m^k \mid k \in \mathbb{Z}\}$ ... Gruppe der m-ten Einheitswurzeln [vgl. UE]

$\operatorname{Ker} \varphi$: $\varphi(m \cdot l) = \zeta_m^{ml} = e^{\frac{2\pi i l m}{m}} = e^{2\pi i l} = 1$;

$\varphi(k) = 1 \Rightarrow \zeta_m^k = 1 \Rightarrow e^{2\pi i \frac{k}{m}} = 1 \Rightarrow \frac{k}{m} \in \mathbb{Z} \Rightarrow k \in m\mathbb{Z}$,

also $\operatorname{Ker} \varphi = m\mathbb{Z}$

4) $\tilde{\varphi}: \mathbb{Z}_m \to C_m,\ \bar{k} \mapsto \zeta_m^k$ ist ein Isomorphismus von $(\mathbb{Z}_m, +)$ mit $(C_m, \cdot)$ [UE]

5) $\exp: \mathbb{R} \to \mathbb{R}^* := \mathbb{R} \setminus \{0\},\ x \mapsto e^x$ injektiver Homo. mit $\mathrm{Im}(\exp) = \mathbb{R}_+ :=]0, \infty[$ [UE]

6) $\exp: \mathbb{C} \to \mathbb{C}^*,\ z \mapsto e^z$ surj. Homo. mit $\mathrm{Ker}(\exp) = \{2\pi i n \mid n \in \mathbb{Z}\}$ [UE]

7) $\det: GL(n, \mathbb{R}) \to \mathbb{R}^*,\ A \mapsto \det A$ surj. Homo, weil $\det(A \cdot B) = \det A \cdot \det B$; $\det\begin{pmatrix} c & & 0 \\ & 1 & \\ 0 & & 1 \end{pmatrix} = c$, also surj.;

$\mathrm{Ker}(\det) = \{A \in GL(n, \mathbb{R}) \mid \det A = 1\} =: SL(n, \mathbb{R})$

8) Signum einer Permutation [$\rightsquigarrow$ Lin. Alg. / Determinanten]

$\mathrm{sign}: S_n \to \{-1, +1\},\ \sigma \mapsto \mathrm{sign}(\sigma)$ Homomorph.

mult. Gruppe

$(-1)^{\#\text{ der Fehlstände: } i<j, \text{ aber } \sigma(i) > \sigma(j)}$

bzw. $\mathrm{sign}(\sigma) = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i}$

$\mathrm{Ker}(\mathrm{sign}) = \{\sigma \in S_n \mid \mathrm{sign}\,\sigma = +1\} =: A_n$

<u>alternierende Gruppe</u>

9) G beliebige Gruppe, $a \in G$

<u>Konjugation</u> $\kappa_a : G \to G,\ x \mapsto a x a^{-1}$

ist ein Automorphismus; sogenannter <u>innerer Automorphismus</u>

(G abelsch $\Rightarrow \kappa_a(x) = x \quad \forall x \in G$, d.h. $\kappa_a = id_G$)

$$\underline{\kappa_a(x \cdot y)} = a x y a^{-1} = a x e y a^{-1} = a x a^{-1} a y a^{-1} = \underline{\kappa_a(x) \cdot \kappa_a(y)}$$

inj.: $\kappa_a(x) = e \Rightarrow a x a^{-1} = e \Rightarrow a x = a \Rightarrow x = e$

surj: $y \in G$; $x := a^{-1} y a \Rightarrow \kappa_a(x) = a(a^{-1} y a) a^{-1} = y$

<u>Bem</u>: $\kappa_a^{-1} = \kappa_{a^{-1}}$

2.2. Nebenklassen

(erinnere an Quotienten von Vektorräumen in der Lin. Alg.)

Sei H Untergruppe von G, $a, b \in G$:

<u>Idee</u>: nenne $a \underset{\ell}{\sim} b$, wenn $\exists x \in H$: $\underbrace{b = a x}_{\Updownarrow \; a^{-1} b = x \in H}$

(„$a \underset{\ell}{\equiv} b \pmod H$" ... „linkskongruent")

$\underset{\ell}{\sim}$ ist Äquivalenzrelation: • $a \underset{\ell}{\sim} a$ klar $[x = e]$

• $a \underset{\ell}{\sim} b \Rightarrow b = a x \Rightarrow a = b x^{-1} \Rightarrow b \underset{\ell}{\sim} a$

• $a \underset{\ell}{\sim} b,\ b \underset{\ell}{\sim} c \Rightarrow b = a x,\ c = b y$ mit $x, y \in H \Rightarrow c = a \overbrace{x y}^{\in H}$

Äquivalenzklasse von a ~~[illegible]~~ bzgl. $\underset{\ell}{\sim}$ ist

$$\{b \in G \mid \exists x \in H: b = a \cdot x\} =: a \cdot H$$

aH heißt <u>linke Nebenklasse</u> von a bzgl. H

analog: $a \underset{r}{\sim} b$, wenn $\exists x \in H: \underbrace{b = xa}$

$\Leftrightarrow ba^{-1} \in H$

$\Leftrightarrow ab^{-1} \in H$

$$Ha := \{b \in G \mid \exists x \in H: b = xa\}$$ <u>rechte Nebenklasse</u> von a bzgl. H

<u>LEMMA</u>: Folgende Aussagen sind äquivalent:

(i) $aH = bH$, (ii) $b \in aH$, (iii) $a^{-1}b \in H$

ebenso

(i') $Ha = Hb$, (ii') $b \in Ha$, (iii') $ab^{-1} \in H$.

Beweis: (i) $\Rightarrow$ (ii): $b = be \in bH = aH$

(ii) $\Rightarrow$ (iii): $\exists x \in H: b = ax \Rightarrow \exists x \in H: a^{-1}b = x$

$\Rightarrow a^{-1}b \in H$

(iii) $\Rightarrow$ (i): $aH \subseteq bH$: $y \in aH \Rightarrow \exists x \in H: y = ax \Rightarrow$

$$y = (bb^{-1}) \cdot ax = b\underbrace{(a^{-1}b)^{-1}}_{\in H}\underbrace{x}_{\in H} \in bH$$

- $bH \subseteq aH$: $y \in bH \Rightarrow \exists\, x \in H: y = bx \Rightarrow$

  $y = (a a^{-1}) b x = a \underbrace{(a^{-1}b)}_{\in H} \underbrace{x}_{\in H} \in aH$.

analog für $(i') \Rightarrow (ii') \Rightarrow (iii') \Rightarrow (i')$ $\square$

G kann also in entsprechende Äquivalenz=klassen zerlegt werden, mittels linker oder rechter Nebenklassen:

$$G/H := \{ aH \mid a \in G \}$$

$$H\backslash G := \{ Ha \mid a \in G \}$$

[es ist $aH = bH$ oder $aH \cap bH = \emptyset$, weil $\underset{\ell}{\sim}$ eine Äquiv.rel. ist

$G = \bigcup_{a \in G} aH$]

<u>BEM:</u> $\Phi : G/H \to H\backslash G$, $aH \mapsto Ha^{-1}$ ist bijektiv

$\left(aH = bH \Leftrightarrow a^{-1}b \in H \Leftrightarrow a^{-1}(b^{-1})^{-1} \in H \Leftrightarrow Ha^{-1} = Hb^{-1};\right.$
$\left. Hb = H(b^{-1})^{-1}, \text{ d.h. } Hb = \Phi(b^{-1}H) \right)$

$\boxed{!}$ Im Allgemeinen wird G/H nicht durch $(aH) * (bH) := abH$ zu einer Gruppe

$\rightsquigarrow$ das geht nur in ~~allen~~ abelschen Gruppen G oder für sogenannte Normalteiler H (siehe später)

2.3. Ordnung und Index

sei G eine Menge:

$$\mathrm{ord}(G) := \begin{cases} |\mathrm{ord}(G)|, & \text{falls } G \text{ endlich} \\ \infty, & \text{falls } G \text{ nicht endlich} \end{cases}$$ [Mächtigkeit; Anzahl der Elemente von G]

wegen der Bemerkung am Ende von 2.2. ist für eine Untergruppe H der Gruppe G stets

$$\mathrm{ord}(G/H) = \mathrm{ord}(H \backslash G)$$

DEF: Der Index von H in G ist

$$\mathrm{ind}(G:H) := \mathrm{ord}(G/H)$$

SATZ (von Lagrange): G endliche Gruppe, $H < G \Rightarrow$

$$\mathrm{ord}(G) = \mathrm{ord}(H) \cdot \mathrm{ind}(G/H)$$

Beweis: setze $m := \mathrm{ind}(G/H)$; es gibt $a_1, \dots, a_m \in G$, sodass $G = a_1 H \cup \dots \cup a_m H$ disjunkte Vereinigung (Zerlegung in Äquiv.klassen);

jedes $a_j H$ enthält genauso viele Elemente wie H, denn $x \mapsto a_j x$ ist bijektiv $H \to a_j H$

($a_j x = a_j y \Rightarrow x = y$, also inj.; ~~[illegible]~~ $a_j H = \{a_j x \mid x \in H\}$, also surj.)

Also hat G demnach $m \cdot \mathrm{ord}(H)$ viele Elemente $\square$

<u>KOR</u>: Ist ord(G) eine Primzahl, dann hat G nur die trivialen Untergruppen $\{e\}$ und G.

Bew: nach dem Satz v. Lagrange ist für $H < G$ stets ord(H) ein Teiler von ord(G) $\square$

<u>Ordnung eines Elements</u> $a \in G$ ist definiert als

$$\mathrm{ord}(a) := \mathrm{ord}(\mathrm{Erz}(\{a\}))$$

wegen $\mathrm{Erz}(\{a\}) = \{a^k \mid k \in \mathbb{Z}\}$ und $a^{k+l} = (a^l)^k$ gilt

$$\mathrm{ord}(a) = \min\{k \in \mathbb{N}\setminus\{0\} \mid a^k = e\}, \text{ falls } \mathrm{ord}(a) < \infty$$

<u>LEMMA</u>: Ist $\mathrm{ord}(a) < \infty$, so gilt für $k \in \mathbb{Z}$:

$$a^k = e \iff \mathrm{ord}(a) \mid k.$$

Speziell gilt immer $a^{\mathrm{ord}(G)} = e$ in endlichen Gruppen!

Beweis: $\Leftarrow$: klar ~~[illegible]~~

$\Rightarrow$: $\varphi: \mathbb{Z} \to G$, $k \mapsto a^k$ ist Homo. und $\mathrm{Ker}(\varphi) < \mathbb{Z}$;

Ü7 $\Rightarrow \exists m \in \mathbb{N}: \mathrm{Ker}(\varphi) = m \cdot \mathbb{Z}$;

somit $a^m = \varphi(m) = e$ und $a^j = \varphi(j) \neq e$ für $1 \leq j < m$;

also $m = \mathrm{ord}(a)$ und: $a^k = e \Rightarrow \varphi(k) = e \Rightarrow k \in \mathrm{Ker}(\varphi)$

$\Rightarrow k = m \cdot l \Rightarrow m \mid k$ $\square$

<u>Bem</u>: es muss nicht zu jedem Teiler n von ord(G) immer eine Untergr. H mit $n = \mathrm{ord}(H)$ geben.

BEISP: 1) $G=\mathbb{Z}$, $H=m\mathbb{Z}$, hier ist $\operatorname{ind}(\mathbb{Z}:m\mathbb{Z})=m$, weil

$$\mathbb{Z}/m\mathbb{Z}=\{k+m\mathbb{Z}\mid k\in\mathbb{Z}\}=\{\overline{0},\overline{1},\dots,\overline{m-1}\}=\mathbb{Z}_m$$

für $m=6$: $\operatorname{ord}(\overline{2})=3$, $\operatorname{ord}(\overline{3})=2$, $\operatorname{ord}(\overline{4})=3$,
$\operatorname{ord}(\overline{5})=6$

2) $G=GL(n,\mathbb{R})$, $H:=\{A\in GL(n,\mathbb{R})\mid \det A>0\}$
[Unt.gr, denn $\det A\cdot B^{-1}=\det A\cdot(\det B)^{-1}>0$]

sei $C\in GL(n,\mathbb{R})$ beliebig mit $\det C<0$;

$\forall A\in H$: $\det(A\cdot C)=\underbrace{\det A}_{>0}\cdot\underbrace{\det C}_{<0}<0$,

also $H\cdot C\subseteq\{B\mid\det B<0\}=:N$,
ist $B\in N$, denn $A:=B\cdot C^{-1}\in H$, weil $\det A=\underbrace{\det B}_{<0}\cdot\underbrace{(\det C)^{-1}}_{<0}>0$

somit $B=A\cdot C\in H\cdot C$, also $H\cdot C=N$;

weiters $C\cdot H=H\cdot C$, weil

$X=A\cdot C$ mit $A\in H$ $\Leftrightarrow$ $X=C\cdot\underbrace{C^{-1}AC}_{\det>0}=C\cdot A'$ mit $A'\in H$

Schließlich $G=\underbrace{\{A\mid\det A>0\}}_{H}\cup\underbrace{\{B\mid\det B<0\}}_{C\cdot H}$

$\operatorname{ind}(G:H)=2$; $\operatorname{ord}\begin{pmatrix}2&0\\0&1\end{pmatrix}=\infty$, $\operatorname{ord}\begin{pmatrix}0&1\\1&0\end{pmatrix}=2$

2.4. Normalteiler und Faktorgruppen

<u>DEF:</u> $H < G$ heißt <u>Normalteiler</u>, wir schreiben $H \triangleleft G$, wenn $\forall a \in G$: $aH = Ha$

– die linken und rechten Nebenklassen stimmen also überein

<u>Beisp:</u> $\varphi: G \to G'$ Homo. von Gruppen, $H := \operatorname{Ker}\varphi$, dann ist H Normalteiler, denn für $x \in H$ ist

$$ax = \underbrace{axa^{-1}}_{y} \cdot a \quad \text{und} \quad \varphi(\underbrace{axa^{-1}}_{y}) = \varphi(a)\underbrace{\varphi(x)}_{e}\varphi(a^{-1}) = \varphi(a)\cdot\varphi(a)^{-1} = e,$$

also $y \in H$ und somit $ax = ya \in Ha$;

ebenso $xa = a \cdot a^{-1}xa \in aH$; insgesamt $aH = Ha$.

<u>Varianten der Normalteilerbedingung:</u> für $H < G$ sind folgende Eigenschaften gleichwertig:

(i) $aH = Ha$, (ii) $aHa^{-1} \subseteq H$, (iii) $aHa^{-1} = H$ $\forall a \in G$

Beweis: (i) $\Rightarrow$ (ii): $x \in aHa^{-1} \Rightarrow \exists y \in H: x = aya^{-1} \Rightarrow$

$xa = ay \in aH = Ha \Rightarrow x \in H$

(ii) $\Rightarrow$ (iii): nach (ii) ist $\varkappa_a(H) \subseteq H$ $\forall a \in G$;

also auch $\varkappa_{a^{-1}}(H) \subseteq H$,

somit $\underset{\sim}{H} = (\varkappa_a \circ \varkappa_{a^{-1}})(H) = \varkappa_a(\varkappa_{a^{-1}}(H)) \subseteq \underset{\sim}{\varkappa_a(H) \subseteq H}$,

also $H = \varkappa_a(H) = aHa^{-1}$

(iii) $\Rightarrow$ (i): ~~[illegible]~~ $aH = \underbrace{aHa^{-1}}_{H} \cdot a = Ha$ $\square$

<u>Bem:</u> $\{e\}$ und G sind immer Normalteilen in G;
in abelschen Gruppen ist jede Untergruppe Normalteilen

<u>LEMMA:</u> $\varphi : G \to G'$ Homo. von Gruppen

(i) $N' \triangleleft G' \Rightarrow \varphi^{-1}(N') \triangleleft G$ (Spezialfall: $N' = \{e\}$, denn $\varphi^{-1}(N') = \operatorname{Ker}\varphi$)

(ii) φ surjektiv und $N \triangleleft G \Rightarrow \varphi(N) \triangleleft G'$

Beweis: (i): $\varphi^{-1}(N') < G'$ nach 2.1. Eig.

wir zeigen $a\varphi^{-1}(N')a^{-1} \subseteq \varphi^{-1}(N')$, denn fertig;

sei $x \in \varphi^{-1}(N')$, d.h. $x' := \varphi(x) \in N'$, denn

$\varphi(axa^{-1}) = \varphi(a)x'\varphi(a)^{-1} \in N'$, somit $axa^{-1} \in \varphi^{-1}(N')$

(ii): gemäß 2.1. Eig. ist $\varphi(N) < G'$;

wir zeigen $a'\varphi(N)a'^{-1} \subseteq \varphi(N)$, denn fertig;

$x' \in \varphi(N)$, d.h. $\exists x \in N : x' = \varphi(x)$; ~~[illegible]~~ sei $a' = \varphi(a)$ [Surj. von φ!]

$\Rightarrow a'x'a'^{-1} = \varphi(a)\varphi(x)\varphi(a^{-1}) = \varphi(\underbrace{axa^{-1}}_{\in N}) \in \varphi(N)$

$\square$

<u>SATZ</u>: G Gruppe und $N \trianglelefteq G$, dann definiert
$$(aN)*(bN) := (ab)\cdot N$$ eine Verknüpfung auf G/N, sodass $(G/N,*)$ eine Gruppe ist und die kanonische surjektive Abbildung $\rho: G \to G/N$, $a \mapsto aN \; (=Na)$ ein Homomorphismus ist.

Das neutrale Element in G/N ist N, das Inverse zu aN ist $a^{-1}\cdot N$, und $\operatorname{Ker}\rho = N$.

$(G/N,*)$ heißt <u>Faktorgruppe</u> von G nach N und $*$ ist die eindeutige Verknüpfung, die ρ zu einem Homo. macht. [schreiben später einfach $(aN)\cdot(bN)$ statt $(aN)*(bN)$]

Beweis:
wenn ρ Homo. sein soll, so muss
$$(aN)*(bN) = \rho(a)*\rho(b) = \rho(ab) = (ab)N$$ gelten,
daher $*$ eindeutig;

Wohldefiniertheit von $*$ (also Unabhängigkeit des „Wertes" $(aN)*(bN)$ von den Repräsentanten $a \in aN$, $b \in bN$):

seien $a' \in aN$ und $b' \in bN$, d.h. $aN = a'N$, $bN = b'N$;
$\forall x \in N$, $\exists y \in N$ mit $xb' = b'y$, weil $Nb' = b'N$ [Normalteiler!]

setze $x = a^{-1}a'$ [$\in N$, weil $aN = a'N$], dann folgt

$$(ab)^{-1}(a'b') = b^{-1}\underbrace{\underbrace{a^{-1}a'}_{x}\, b'}_{=b'y} = \underbrace{b^{-1}b'}_{\in N,\ \text{weil } bN = b'N} y \in N$$

$\Rightarrow (ab)N = (a'b')N$, somit $*$ wohldefiniert.

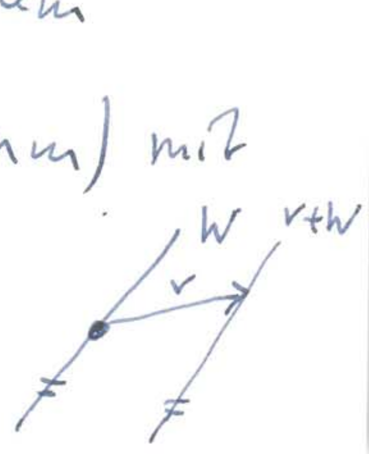
Assoziativität folgt leicht: $\big((aN)*(bN)\big)*(cN) =$
$= \big((ab)N\big)*(cN) = \big((ab)c\big)N = \big(a(bc)\big)N = (aN)*(bc)N =$
$= (aN)*\big((bN)*(cN)\big)$.

$N = eN$ ist neutr. El.: $(eN)*(aN) = (ea)N = (ae)N = (aN)*(eN)$

$(aN)^{-1} = a^{-1}N$, denn: $(a^{-1}N)*(aN) = (a^{-1}a)N = N = (aa^{-1}N) =$
$= (aN)*(a^{-1}N)$

$\square$

BEISP.: 1) V Vektorraum über $\mathbb{K}$, W Teilraum; dann ist W Normalteiler der additiven Gruppe $(V,+)$ und V/W entspricht dem Faktorraum (Quotientenvektorraum) mit $(v+W)+(v'+W) := (v+v')+W$



2) $G = \mathbb{Z}$, $N = m\mathbb{Z} \triangleleft \mathbb{Z}$ (weil abelsch)

Faktorgruppe ist $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ wie in 2.3. Beisp. 1)

$\mathbb{Z}$ zyklische Gruppe mit $\mathrm{ord}(\mathbb{Z}) = \infty$,

$\mathbb{Z}_m$ zyklische Gruppe mit $\mathrm{ord}(\mathbb{Z}_m) = m$

3) $G = GL(n, \mathbb{R})$ besitzt z.B. die Normalteiler

$GL_+(n,\mathbb{R}) := \{A \in GL(n,\mathbb{R}) \mid \det A > 0\}$ (vgl. 2.3. Beisp. 2))

und $SL(n,\mathbb{R}) := \{A \in GL(n,\mathbb{R}) \mid \det A = 1\}$ [Details in UE]

2.5. Isomorphiesätze

FAKTORISIERUNGSSATZ: Sei $\varphi: G \to G'$ Homo. von Gruppen, $N \triangleleft G$ mit $N \subseteq \mathrm{Ker}(\varphi)$ und $\rho: G \to G/N$ die kanonische Surjektion auf die Faktorgruppe. Dann $\exists!$ Gruppenhomo. $\overline{\varphi}: G/N \to G'$, sodass $\varphi = \overline{\varphi} \circ \rho$ gilt; d.h. das Diagramm

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\rho"'] & G' \\ G/N \arrow[ur, dashed, "\exists!\,\overline{\varphi}"'] & \end{tikzcd}$$

ist kommutativ (es kommt nicht darauf an, in welcher Reihenfolge wir den Pfeilen folgen)

Es ist dann weiters $\overline{\varphi}(G/N) = \varphi(G)$

und $\operatorname{Ker}\overline{\varphi} = \operatorname{Ker}\varphi/N$.

Beweis: Eindeutigkeit von $\overline{\varphi}$ aus der Bedingung $\varphi = \overline{\varphi}\circ\rho$, denn $\overline{\varphi}(\underbrace{aN}_{\rho(a)}) = (\overline{\varphi}\circ\rho)(a) = \varphi(a)$.

Also setzen wir mal $\overline{\varphi}: G/N \to G'$, $\overline{\varphi}(aN) := \varphi(a)$.

- $\overline{\varphi}$ wohldefiniert: $aN = bN \Rightarrow a^{-1}b \in N \overset{[N\subseteq \operatorname{Ker}\varphi]}{\Longrightarrow}$
  $e' = \varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) \Rightarrow \varphi(a) = \varphi(b)$
- $\overline{\varphi}$ Homo.: $\overline{\varphi}((aN)\cdot(bN)) = \overline{\varphi}((ab)N) = \varphi(ab) = \varphi(a)\varphi(b) =$
  $= \overline{\varphi}(aN)\cdot\overline{\varphi}(bN)$
- $\varphi = \overline{\varphi}\circ\rho$ lt. Konstr.
  - wegen $\overline{\varphi}(aN) = \varphi(a)$ ist $\overline{\varphi}(G/N) = \varphi(G)$
- $N \trianglelefteq G$ und $N \subseteq \operatorname{Ker}\varphi \Rightarrow N \trianglelefteq \operatorname{Ker}\varphi$
- $\operatorname{Ker}\overline{\varphi} \subseteq \operatorname{Ker}\varphi/N$: $aN \in \operatorname{Ker}\overline{\varphi} \Rightarrow \varphi(a) = \overline{\varphi}(aN) = e'$
  $\Rightarrow a \in \operatorname{Ker}\varphi \Rightarrow aN \in \operatorname{Ker}\varphi/N$
- $\operatorname{Ker}\overline{\varphi} \supseteq \operatorname{Ker}\varphi/N$: $aN \in \operatorname{Ker}\varphi/N \Rightarrow \exists b \in \operatorname{Ker}\varphi: aN = bN$
  $\Rightarrow a^{-1}b \in N \subseteq \operatorname{Ker}\varphi \Rightarrow a^{-1} = a^{-1}bb^{-1} \in \operatorname{Ker}\varphi \Rightarrow$
  $a \in \operatorname{Ker}\varphi \Rightarrow \overline{\varphi}(aN) = \varphi(a) = e' \Rightarrow aN \in \operatorname{Ker}\overline{\varphi}$.

Somit $\operatorname{Ker}\overline{\varphi} = \operatorname{Ker}\varphi/N$. $\square$

Anwendung auf die Bestimmung von Faktorgruppen (bis auf Isomorphie):

für $N = \operatorname{Ker}\varphi$ (ist immer Normalteiler!)

ergibt sich

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[d, "\rho"'] & G' \\ G/\operatorname{Ker}\varphi \arrow[ur, dashed, "\overline{\varphi}"'] & \end{tikzcd}$$

wobei $\overline{\varphi}$ nun injektiv ist, weil $\operatorname{Ker}\overline{\varphi} = \operatorname{Ker}\varphi / \operatorname{Ker}\varphi = \{N\}$

also ist $\overline{\varphi}$ bijektiv als Abbildung $G/_{\operatorname{Ker}\varphi} \to \varphi(G)$,

d.h. $\boxed{\varphi(G) \cong G/\operatorname{Ker}\varphi}$ (vermöge $\overline{\varphi}$)

sogenannter <u>erster Isomorphiesatz</u>

<u>Bem</u>: ist φ surjektiv, also $\varphi(G) = G'$, folgt

$$G' \cong G/\operatorname{Ker}\varphi \quad (\text{vermöge } \overline{\varphi}).$$

<u>BEISP.</u>: $\varphi_m : \mathbb{Z} \to S^1, k \mapsto \zeta_m^k$ aus 2.1. Beisp. 3);

$\varphi(\mathbb{Z}) = C_m$, $\operatorname{Ker}\varphi = m\mathbb{Z}$, somit $\mathbb{Z}_m = \underline{\mathbb{Z}/m\mathbb{Z} \cong C_m} = \varphi(\mathbb{Z})$

2.6. Klassifikation der zyklischen Gruppen

erinnere: G heißt zyklisch, wenn $\exists a \in G$ mit

$$G = \mathrm{Erz}(\{a\}) = \{a^k \mid k \in \mathbb{Z}\}$$

mit anderen „Worten": $\varphi: \mathbb{Z} \to G,\ k \mapsto a^k$ ist ein surjektiver Gruppenhomomorphismus

BEM: (i) Jede zyklische Gruppe ist kommutativ, denn

$$a^k \cdot a^l = a^{k+l} = a^l \cdot a^k$$

(ii) G endliche Gruppe mit $\mathrm{ord}(G)$ prim, $a \in G \setminus \{e\}$

$\Rightarrow$ G zyklisch und $G = \mathrm{Erz}(\{a\})$

Bew.: $p := \mathrm{ord}(G)$, $H := \mathrm{Erz}(\{a\})$

wegen $a \neq e$ ist $\mathrm{ord}(H) \geq 2$; nach Satz von Lagrange [2.3]

~~Nun~~ gilt auch $\mathrm{ord}(H) \mid p$;

somit muss $\mathrm{ord}(H) = p$ sein, also $H = G$ $\square$

SATZ: Sei G zyklische Gruppe mit erzeugendem Element $a \in G$. Dann ist entweder $G \cong \mathbb{Z}$ oder $\exists m \in \mathbb{N}, m \geq 1$, sodass $\varphi: \mathbb{Z}_m \to G,\ \bar{k} \mapsto a^k$ ein Isomorphismus ist, also $G \cong \mathbb{Z}_m$ ist.

Beweis: der Homomorphismus $\varphi: \mathbb{Z} \to G, k \mapsto a^k$ ist wegen $G = \{a^k \mid k \in \mathbb{Z}\}$ jedenfalls surjektiv;

- falls $\operatorname{Ker}\varphi = \{0\}$, also φ auch injektiv ist, dann gilt $G \cong \mathbb{Z}$ (vermöge φ); hier ist $\operatorname{ord}(G) = \infty$
- falls $\{0\} \subsetneq \operatorname{Ker}\varphi \subseteq \mathbb{Z}$ gibt es wegen $\operatorname{Ker}\varphi \underset{(< \text{genügt})}{\triangleleft} \mathbb{Z}$ gemäß Ü-Aufg. 7 ein $m \in \mathbb{N}, m \geq 1$ mit $\operatorname{Ker}\varphi = m \cdot \mathbb{Z}$; nach dem Isomorphiesatz 2.5 gilt also $\mathbb{Z}_m = \mathbb{Z}/\operatorname{Ker}\varphi \cong G$ mittels $\bar{\varphi}(\bar{k}) = \varphi(k) = a^k = \psi(\bar{k})$ $\square$

In diesem Sinne sind $(\mathbb{Z}_m, +)$ bzw. $(\mathbb{Z}, +)$ die „Grundmodelle" für alle zyklischen Gruppen.

<u>BEM:</u> (ohne Bew.)
- jede Untergruppe einer zyklischen Gruppe ist zyklisch
- G endliche zyklische Gruppe, $m = \operatorname{ord}(G)$, dann existiert zu jedem Teiler k von m genau eine Untergruppe $H < G$ mit $\operatorname{ord}(H) = k$