

Erinnerung:

Eine Menge G , zusammen mit einer
Abbildung $G \times G \xrightarrow{(\cdot)} G, (g, h) \mapsto g \cdot h$,
heißt **Gruppe**, falls

- $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ für $g, h, k \in G$
- $\exists 1 = 1_G \in G$ mit $1 \cdot g = g$
und $g \cdot 1 = g$ für $g \in G$

Es liegt 1_G eindeutig fest.

- $\forall g \in G \exists g^{-1} = g^{-1} \in G$ mit
 $g \cdot g^{-1} = 1_G$
 $g^{-1} \cdot g = 1_G$

Für $g \in G$ liegt g^{-1} eindeutig fest.

Beispiele : • Symmetrische Gruppe S_n auch: $\{1, \dots, n\}$
auf einer Menge Ω
- z.B. $S_{\{1, \dots, n\}} =: S_n$ für $n \geq 0$

- $GL_n(K)$ für Körper K und $n \geq 0$
- Untergruppen davon

G : Gruppe

Π : Menge

symmetrischer Gruppe auf Π

• $\alpha: G \rightarrow S_\Pi$ Gruppenhomomorphismus

$\leadsto \Pi = (\Pi, \alpha)$ ist G -Menge

$$g \cdot u := (\alpha(g))(u)$$

• Zugang via Multiplikationsabbildung:

Sei $G \times \Pi \rightarrow \Pi$
 $(g, u) \mapsto g \cdot u$

mit
$$\begin{cases} 1 \cdot u = u & \text{für } u \in \Pi \\ (g \cdot h) \cdot u = g \cdot (h \cdot u) & \text{für } g, h \in G, u \in \Pi \end{cases}$$

$$\Rightarrow (\alpha(g))(u) := g \cdot u$$

$\Rightarrow \Pi = (\Pi, \alpha)$ ist G -Menge

Operator α injektiv

Bsp

• $U \leq S_n \Rightarrow [1, n]$ ist treue

symmetrischer Gruppe, $n \geq 0$

U -Menge

mit $u \cdot k = u(k)$

• $U \leq G$

$$\Rightarrow G/U = \{hU : h \in G\}$$

ist G -Menge mit $g \cdot (hU) := (gh)U$
 für $g \in G$ und $h \in G$

G : Gruppe

Π, N : G -Mengen

• $\Pi \xrightarrow{f} N$ heißt **G -Abbildung**,
falls $f(g \cdot u) = g \cdot f(u)$ für $g \in G, u \in \Pi$

• Ist die G -Abbildung f bijektiv, so heißt
sie **G -Bijektion** oder **Isomorphismus von G -Mengen**.

• $u \in \Pi \Rightarrow G \cdot u = \{g \cdot u : g \in G\} \subseteq \Pi$
heißt **Bahn** von u

• Disjunkte Zerlegung: $\Pi = \bigcup_{i \in [1, k]} G u_i$,
wobei $\{u_1, \dots, u_k\}$ gewählte
Repräsentantenmenge der Bahnen.

$k \geq 0$

• $\Pi^{\times k} = \{(u_i)_{i \in [1, k]} : u_i \in \Pi \text{ für } i \in [1, k]\}$
ist G -Menge vda $g \cdot (u_i)_i := (g \cdot u_i)_i$

• $\Pi^{\times k, \neq} = \{(u_i)_i \in \Pi^{\times k} : u_i \neq u_j \text{ falls } i \neq j\}$
ist G -Teilmenge in $\Pi^{\times k}$

G : Gruppe

Ω : G -Menge

Ω heißt **transitiv**, wenn Ω aus genau einer Bahn besteht. D.h. wenn $\Omega = G\omega$ für $\omega \in \Omega$.

$k \geq 0$

Ω heißt **k -fache transitiv**, wenn $\Omega^{\times k} \neq \emptyset$

transitiv ist.

Bsp: Die S_n -Menge $[1, n]$ ist n -fache transitiv.

Bahnenlemma: $\omega \in \Omega$

$$G_\omega = \{g \in G : g \cdot \omega = \omega\}$$

Stabilisator

G -Bijektion:

$$\begin{array}{ccc} G/G_\omega & \xrightarrow{\sim} & G \cdot \omega \\ gG_\omega & \mapsto & g \cdot \omega \end{array}$$

Lemma 2.2 Ω : transitive G -Menge, T : G -Menge
 $\Omega \xrightarrow{f} T$ surj. G -Abbildung
 $\omega \in \Omega$

(1) $G_\omega \leq G_{f(\omega)} \leq G$

(2) $G_\omega = G_{f(\omega)} \iff f$ bij.

(3) $G_{f(\omega)} = G \iff T$ trivial

note!
??

G : Gruppe

Π : transitiver G -Menge

• Sei Π nichttrivial.

Es heißt Π **primär**, falls

$\Pi \xrightarrow[\substack{\text{surj.} \\ G\text{-Abb.}}]{f} T \implies f \text{ bijektiv oder } T \text{ trivial}$

• $B \subseteq \Pi$ heißt **Block**, falls $gB = B$ oder $gB \cap B = \emptyset$ für $g \in G$.

Lemma 2.8

Π transitiv und nichttrivial.

Äquivalent sind:

(1) Π ist primär

(2) Es gibt auf Π keine G -Äquivalenzrelation, die weder diskret noch vollständig ist

(3) Es gibt in Π keinen Block B mit

$|B| > 1$ und $B \subseteq \Pi$

(4) $\exists m \in \Pi$ mit: $C_G(m) \stackrel{\max}{<} G$

(5) $\forall m \in \Pi$ ist: $C_G(m) \stackrel{\max}{<} G$

Bew.

(4) $\iff$ (5) $\iff$ (1) $\iff$ (2) $\iff$ (3)

G : endliche unendl. Gruppe

$S \subseteq G$: endl. Teilmenge mit $G = \langle S \rangle$

$$S^{\pm} := S \cup \{s^{-1} : s \in S, | \langle S \rangle | = \infty\}$$

$\uparrow$ Falls G endlich, dann $S^{\pm} = S$

Jedes Element von $G = \langle S \rangle$ kann also
als Produkt von Elementen aus $S^{\pm}$ geschrieben
werden.

Π : G -Menge

$u \in \Pi$: Element mit $G \cdot u = \{g \cdot u : g \in G\}$
endlich. $\leftarrow$ z.B.: Π endlich,
 $u \in \Pi$ beliebig

Wollen: $G \cdot u = \{g \cdot u : g \in G\}$

und

$$C_G(u) = \{g \in G : g \cdot u = u\}$$

sparsam berechnen

(Erzeuger für $C_G(u)$)

Bsp:

$$G = \langle \overset{=:a}{(1,2,3)}, \overset{=:b}{(3,4,5)} \rangle$$

$$\leq S_6$$

$$\Pi = \{1, 2, 3, 4, 5, 6\}$$

$$u = 3$$

7

① Nicht in Kästen:

$$G \cdot 3 = \{1, 2, 3, 4, 5\}$$

② In Kästen:

$$\text{II: } \tau(b a a)^{-1} \circ (b a a)$$

$$= a^{-1} \circ b \circ a = (2, 4, 5)$$

$$\text{IV: } \tau(a b b)^{-1} \circ (a b b)$$

$$= b^{-1} \circ a \circ b = (1, 2, 5)$$

$$\text{III: } \tau(a^3)^{-1} \circ a^3$$

$$= \text{id}^{-1} \circ a^3 = \text{id}$$

$$\text{II: } \tau(b a a)^{-1} \circ b a a^2$$

$$= (a^2)^{-1} \circ b \circ a^2 = (1, 4, 5)$$

$$\text{V: } \tau(a a b^2)^{-1} \circ a a b^2$$

$$= (b^2)^{-1} \circ a \circ b^2 = (1, 2, 4)$$

$$\text{III: } \tau(b^3)^{-1} \circ b^3$$

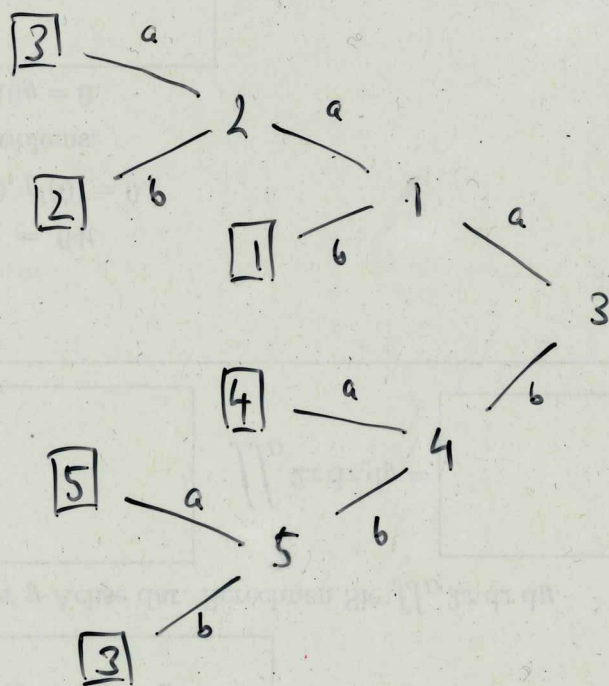
$$= \text{id}^{-1} \circ b^3 = \text{id}$$

$$\Rightarrow C_a(3) = \langle (2, 4, 5), (1, 2, 5), (1, 4, 5), (1, 2, 4) \rangle$$

$$\begin{aligned} & \textcircled{*} \langle (2, 4, 5), (1, 2, 5) \rangle \Rightarrow |G| = |C_a(3)| \cdot |G \cdot 3| = 60 \\ & \text{extra Rechnung} \rightarrow 12 \quad 5 \leftarrow \text{S.o.} \end{aligned}$$

Baum von rechts nach links

Kasten, falls schon vorher aufgeschrieben



$$\begin{aligned} & \textcircled{*} (1, 3, 5) \\ & (2, 4, 5) = (5, 4, 1) = (1, 4, 5) \\ & (1, 5, 2) (2, 4, 5) = (1, 4, 2) = (1, 2, 4) \\ & \leadsto (1, 4, 5), (1, 2, 4) \\ & \text{nicht benötigt} \end{aligned}$$

G : endl. Grp

p : Primzahl

$$a \in \mathbb{Z}_{\neq 0}, \quad a = p^k \cdot \frac{a'}{p^0} \quad \frac{a'}{p^0} \neq 0$$

$$\Rightarrow a [p] := p^k$$

$$\text{Syl}_p(G) = \{ P \leq G : |P| = |G| [p] \}$$

Menge der p -Sylow untergruppen in G

Satz 38 (Sylow)

(1) $\text{Syl}_p(G) \neq \emptyset$

(2) $\text{Syl}_p(G)$ ist transitive G -Menge unter Konjugation

(3) $|\text{Syl}_p(G)| \equiv_p 1$

• Für $P \in \text{Syl}_p(G)$:

$$|\text{Syl}_p(G)| = \frac{|G|}{|N_G(P)|}, \quad \text{was } \frac{|G|}{|G| [p]} \text{ teilt}$$

(4) $U \leq G$ p -Untergruppe

$$\Rightarrow \exists P \in \text{Syl}_p(G) \text{ mit } U \leq P$$

Bsp Sei $|G| = 30$.

$$|\text{Syl}_5(G)| \equiv_5 1 \quad \text{und} \quad |\text{Syl}_5(G)| \text{ teilt } \frac{30}{30/5} = 6$$

$$\Rightarrow |\text{Syl}_5(G)| \in \{1, 6\}.$$

G : Gruppe

Lemma 4.3 (Iwasawa - Kriterium)

$\pi = (\pi, \alpha)$: primitive G -Rang

$m \in \pi$

$$\begin{array}{c} \uparrow \\ G \xrightarrow{\alpha} S_m \end{array}$$

$m \in \pi$

$K := \text{Kern}(\alpha)$

$C := C_G(m)$

$A \trianglelefteq C$ und A abelsch
und $G \triangleleft A \trianglelefteq G$.

Normalteilererzeugnis

$$G \triangleleft A \trianglelefteq G = \langle \bigcup_{g \in G} gAg^{-1} \rangle \trianglelefteq G$$

$[a, b] = a^{-1}b^{-1}ab$

$G^{(1)} = [G, G] \trianglelefteq G$

Kommutatoruntergruppe

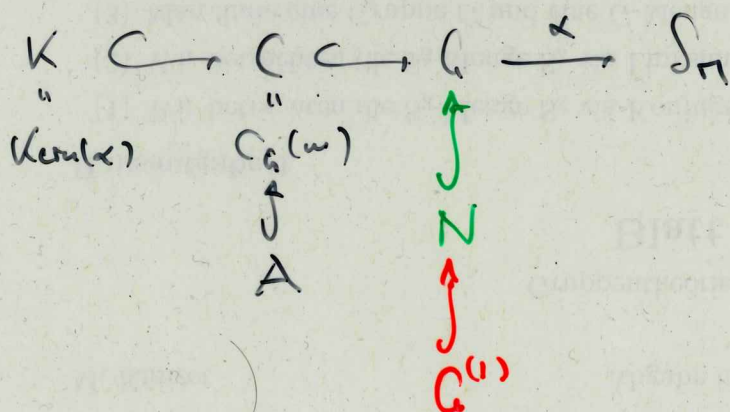
(1) $N \trianglelefteq G$ und $N \not\subseteq K$. Dann $G^{(1)} \leq N$

(2) G perfekt $\Rightarrow G/K$ einfach
 $G^{(1)} = G$

hat nur
Normalteiler

1 und G/K

Situation:



Nichtabelsche einfache Gruppen:

z.B.:

• $A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = +1\}$
ist eine einfache Gruppe für $n \geq 5$

• $PSL_n(F) = SL_n(F) / Z(SL_n(F))$
für einen Körper F , für $n \geq 2$,
vorausgesetzt $(n, |F|) \notin \{(2, 2), (2, 3)\}$,
ist eine einfache Gruppe

Betrachtung von Ordnungen:

• $|A_5| = \frac{1}{2} \cdot 5! = 60$

$|A_6| = \frac{1}{2} \cdot 6! = 360$

• $|PSL_2(\mathbb{F}_7)| = \frac{|SL_2(\mathbb{F}_7)|}{|Z(SL_2(\mathbb{F}_7))|} = \frac{8 \cdot 42}{2} = 168$

$|SL_2(\mathbb{F}_7)| = \frac{|GL_2(\mathbb{F}_7)|}{|\mathbb{F}_7^\times|} = \frac{(49-1)(49-7)}{6} = 8 \cdot 42$

$Z(SL_2(\mathbb{F}_7)) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix} \right\}$ hat Ordnung 2

$\Rightarrow PSL_2(\mathbb{F}_7) \not\cong A_n$ für $n \geq 5$

Normalalgorithmus für Relationen

$G = \langle g_1, \dots, g_n \rangle$: endliche Gruppe

$\{\hat{g}_1, \dots, \hat{g}_n\}$: Menge mit n Elementen

$F = F(\{\hat{g}_1, \dots, \hat{g}_n\})$: freie Gruppe

$F \xrightarrow{\varphi} G : \hat{g}_i \mapsto g_i \text{ für } i \in \{1, \dots, n\}$

ist ein surjektiver Gruppenmorphimus.

$\text{Kern}(\varphi) = \underbrace{C_F(1_G)}_{\text{mit Normalalgorithmus berechenbar}} = \langle k_1, \dots, k_m \rangle$

$\Rightarrow \text{Kern}(\varphi) = F \triangleleft \underbrace{k_1, \dots, k_m}_{\text{häufig noch reduzierbar}} \triangleright$

$\Rightarrow F / \text{Kern}(\varphi)$

$= \underbrace{\langle \hat{g}_1, \dots, \hat{g}_n : \underbrace{r_1, \dots, r_m}_{\text{Relationen}} \rangle}_{\substack{\text{Erzeuger} \\ \text{endliche präsentische Gruppe}}} \xrightarrow{\sim} G$

G : Gruppe

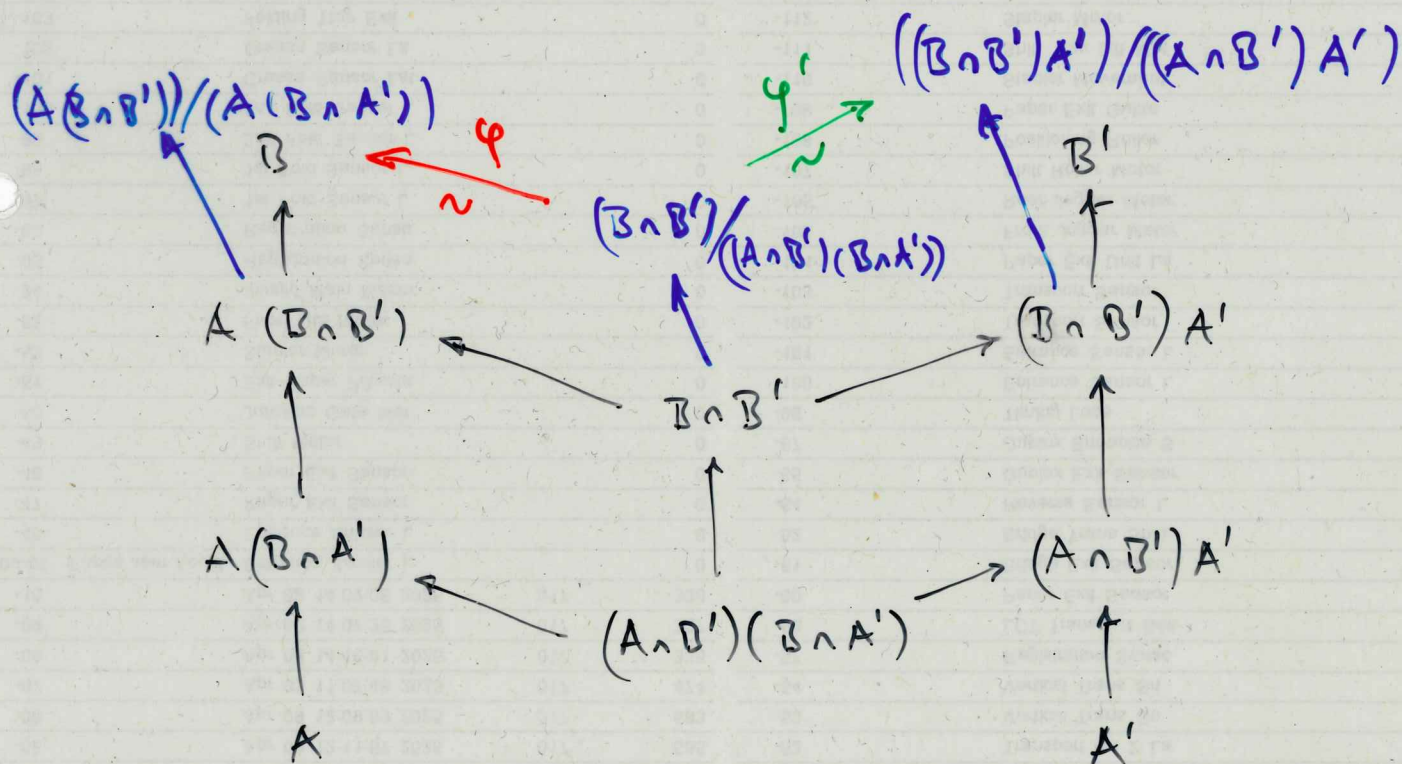
Lemma 63 (Schmetterlingslemma)

Sei $A \leq B \leq G$. Sei $A' \leq B' \leq G$.

$$\begin{aligned} \text{Dann: } (A \cap B')(B \cap A') &\trianglelefteq B \cap B' \\ A(B \cap A') &\trianglelefteq A(B \cap B') \\ (A \cap B')A' &\trianglelefteq (B \cap B')A' \end{aligned}$$

$$\begin{aligned} \text{Und: } (B \cap B') / ((A \cap B')(B \cap A')) &\xrightarrow[\sim]{\varphi} (A(B \cap B')) / (A(B \cap A')) \\ \times ((A \cap B')(B \cap A')) &\xrightarrow{\quad} \times (A(B \cap A')) \end{aligned}$$

$$\begin{aligned} \text{Und: } (B \cap B') / ((A \cap B')(B \cap A')) &\xrightarrow[\sim]{\varphi'} ((B \cap B')A') / ((A \cap B')A') \\ \times ((A \cap B')(B \cap A')) &\xrightarrow{\quad} \times ((A \cap B')A') \end{aligned}$$



$$\text{Insbesondere: } (A(B \cap B')) / (A(B \cap A')) \xrightarrow[\sim]{\varphi' \circ \varphi} ((B \cap B')A') / ((A \cap B')A')$$

G : Gruppe

Subnormalreihe:

$$G = U_0 \supseteq U_1 \supseteq \dots \supseteq U_s = 1$$

- Falls $U_i \supset U_{i+1}$ stets, dann **stabil**
- Falls U_i/U_{i+1} einfach stets, dann **Kompositionsreihe**.

$(U_i)_{i \in [0, s]}$, $(V_j)_{j \in [0, t]}$ Subnormalreihen

- $(U_i)_{i \in [0, s]}$ und $(V_j)_{j \in [0, t]}$ **äquivalent**,
falls $\sigma: [0, s-1] \rightarrow [0, t-1]$ bij. existiert mit
 $U_i/U_{i+1} \cong V_{\sigma(i)}/V_{\sigma(i)+1}$ stets

- $(V_j)_{j \in [0, t]}$ **Verfeinerung** von $(U_i)_{i \in [0, s]}$,

falls es eine injektive monotone Abb.

$$\rho: [0, s] \rightarrow [0, t] \text{ mit } \rho(0) = 0, \rho(s) = t \text{ gibt}$$

$$\text{mit } U_i = V_{\rho(i)} \text{ für } i \in [0, s].$$

Beu 6.7. Auf der Menge der stabilen Subnormalreihen von G ist $(\leq)$ eine Totalordnung.

- wird zu zeigen** { • Ein Element darin ist genau dann maximal, wenn es eine Kompositionsreihe ist.

Fortsetzung des Beweises von Lemma 71.1)

15

Situation:

G : Gruppe, $G \neq 1$

$(u_i)_{i \in [0, s]}$, $(V_j)_{j \in [0, t]}$: Folgenendketten von G

$$\varphi: [0, st-1] \xrightarrow{\sim} [0, s-1] \times [0, t-1]$$

$$k \mapsto \varphi(k) = (q_1(k), q_2(k)), \quad k = t \cdot q_1(k) + \underbrace{q_2(k)}_{\text{Rest}}$$

$$\gamma: [0, st-1] \xrightarrow{\sim} [0, t-1] \times [0, s-1]$$

$$l \mapsto \gamma(l) = (z_1(l), z_2(l)), \quad l = s \cdot z_1(l) + \underbrace{z_2(l)}_{\text{Rest}}$$

$$\tau: [0, s-1] \times [0, t-1] \xrightarrow{\sim} [0, t-1] \times [0, s-1]$$

$$(i, j) \mapsto (j, i)$$

$$\sigma: [0, st-1] \xrightarrow{\sim} [0, st-1]$$

$$k \mapsto \sigma(k) = \varphi^{-1}(\tau(\varphi(k)))$$

$$u'_k := u_{q_1(k)+1} (u_{q_1(k)} \cap V_{q_2(k)}) \quad \text{für } k \in [0, st-1],$$

$$u'_{st} := 1$$

$$v'_l := (V_{z_1(l)} \cap u_{z_2(l)}) v_{z_1(l)+1} \quad \text{für } l \in [0, st-1],$$

$$v'_{st} := 1$$

Haben:

$$(u_i)_{i \in [0, s]} \quad (V_j)_{j \in [0, t]}$$

$$\Downarrow \quad \Downarrow$$

$$(u'_k)_{k \in [0, st]} \quad (v'_l)_{l \in [0, st]}$$

Zu zeigen:

die $u'_k / u'_{k+1} \stackrel{!}{=} v'_{\sigma(k)} / v'_{\sigma(k)+1}$ für $k \in [0, st-1]$
 sind äquivalent zu σ

Verwendbare Formeln:

- $(q_1(\sigma(k)), q_2(\sigma(k))) = (q_2(k), q_1(k))$ für $k \in [0, st-1]$
- $u'_{k+1} = u_{q_1(k)+1} (u_{q_1(k)} \cap V_{q_2(k)+1})$ für $k \in [0, st-1]$
- $v'_{l+1} = (V_{z_1(l)} \cap u_{z_2(l)+1}) \cdot v_{z_1(l)+1}$ für $l \in [0, st-1]$

G: endl. Gruppe

- G heißt **auflösbar**, falls es in G eine Subnormalreihe
 $(U_i)_{i \in \{0, \dots, s\}}$ gibt mit U_i/U_{i+1} abelsch für $i \in \{0, \dots, s-1\}$
 — eine **auflösende Reihe**.

- G heißt **überauflösbar**, falls es in G eine Subnormalreihe
 $(U_i)_{i \in \{0, \dots, s\}}$ gibt mit $U_i \leq G$ für $i \in \{0, \dots, s\}$
 und U_i/U_{i+1} zyklisch für $i \in \{0, \dots, s-1\}$
 — eine **überauflösende Reihe**.

- G heißt **nilpotent**, falls es in G eine Subnormalreihe
 $(U_i)_{i \in \{0, \dots, s\}}$ gibt mit $U_i \leq G$ für $i \in \{0, \dots, s\}$
 und $U_i/U_{i+1} \leq Z(G/U_{i+1})$ für $i \in \{0, \dots, s-1\}$
 — eine **nilpotent auflösende Reihe**.

-
- abelsch $\Rightarrow$ nilpotent $\Rightarrow$ überauflösbar $\Rightarrow$ auflösbar
 - S_3 ist überauflösbar, aber nicht nilpotent
 - A_4 ist auflösbar, aber nicht überauflösbar
 - p -Gruppen sind nilpotent
 - auflösbar $\Leftrightarrow$ alle Kompositionsfaktoren sind isomorph zu einer zyklischen Gruppe von Primzahlordnung

G : endl. Grp.

Def. $G^{(i)}$: $G^{(0)} := G$
 "normal:" $G^{(i+1)} := [G^{(i)}, G^{(i)}]$ für $i \geq 0$

Def. $G^{[i]}$: $G^{[0]} := G$
 "abg." : $G^{[i+1]} := [G^{[i]}, G]$ für $i \geq 0$

Def. $G^{\gamma i}$: $G^{\gamma 0} = 1$
 "invers abg." : $G^{\gamma i+1}$ ist festgelegt durch:
 $G^{\gamma i} \leq G^{\gamma i+1} \leq G$
 und $G^{\gamma i+1} / G^{\gamma i} = Z(G / G^{\gamma i})$
 für $i \geq 0$

Bem. 82

(1) $G^{(1)} = G^{[1]} = [G, G]$
 $G^{\gamma 1} = Z(G)$
 (2) $G^{(i)} \trianglelefteq G$, $G^{[i]} \trianglelefteq G$, $G^{\gamma i} \trianglelefteq G$
 (3) $G^{(i)} \leq G^{[i]}$ stets
 (4) Sei $i \geq 0$. Sei $x \in G$. Dann:
 $x \in G^{\gamma i+1} \iff [x, G] \leq G^{\gamma i}$

charakteristisches
 Untergruppe,
 d.h. steht
 unter
 Automorphismen
 von G

G : endliche Gruppe

$$G \text{ auflösbar} \iff \exists i \geq 0 : G^{(i)} = 1$$

$$G \text{ nilpotent} \iff \exists i \geq 0 : G^{L,i} = 1$$

$$\iff \exists j \geq 0 : G^{J,j} = G$$

Bsp 83

K : endl. K_v .

$$G = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in K \right\} \leq GL_3(K)$$

$$\underbrace{\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}}_{= G^{L,0} = G^{J,2}} \geq \underbrace{\begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{= G^{L,1} = G^{J,1}} \geq \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{= G^{L,2} = G^{J,0}}$$

Bsp 84

$$B = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in GL_2(\mathbb{F}_3) : a, c \in \mathbb{F}_3^\times, b \in \mathbb{F}_3 \right\}$$

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{= B^{J,0}} \leq \underbrace{\left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle}_{= B^{J,1}} = \underbrace{\left\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle}_{= B^{J,2}} = \dots$$

Gruppen erreichen B nicht

H, N : Gruppen

$H \xrightarrow{\alpha} \text{Aut}(N)$: Gruppenmorphisms

• $(\alpha(h))(n) =: {}^h n$ für $h \in H, n \in N$
 $\in \text{Aut}(N)$

• $h h' n = h(h' n), \quad {}^h(n u') = {}^h n \cdot {}^{h'} u'$
 für $h, h' \in H, n, u' \in N$

Wir bilden das **(äußere) semidirekte Produkt**
 von N mit H mittels α :

$N \rtimes_\alpha H = \left\{ (n, h) : n \in N, h \in H \right\}$
 (als Menge $N \times H$)

mit der Multiplikation

$(n, h) \cdot (n', h') := (n \cdot {}^h n', h \cdot h')$
 "vorheften" "Preis für Vorheften"

für $(n, h), (n', h') \in N \rtimes_\alpha H$

ist eine Gruppe.

Off: $N \rtimes H \stackrel{\text{kurz}}{=} N \rtimes_\alpha H$

G : Gruppe

$$H \leq G, \quad N \trianglelefteq G$$

$$\Rightarrow \alpha: H \rightarrow \text{Aut}(N) : h \mapsto (\alpha(h))(n) := h n h^{-1} = {}^h n$$

und Gruppenmorphisms

$$N \rtimes_{\alpha} H \xrightarrow{\varphi} G$$

$$(n, h) \mapsto nh$$

Falls $N \cap H = 1$ und $NH = G$,

dann: φ ist Isomorphismus

H ist Komplement zu N in G

G ist inneres semidirektes Produkt von N mit G

Bsp 96: $(1) \langle (1, 2, 3) \rangle \rtimes_{\alpha} \langle (1, 2) \rangle \xrightarrow{\varphi} S_3$

(2) $\underbrace{\langle (1, 2, 3, 4) \rangle}_a, \underbrace{\langle (1, 3)(2, 4) \rangle}_b \rtimes_{\alpha} \underbrace{\langle (1, 2, 3) \rangle}_c \xrightarrow{\varphi} A_4$

Or. α hat:
$$\begin{cases} c_a = \overbrace{(1, 2, 3)}^{(1, 2, 3)} (1, 4)(3, 4) = (2, 3)(1, 4) = a \circ b \\ \text{Konj. in } A_4 \\ c_b = \overbrace{(1, 2, 3)}^{(1, 2, 3)} (1, 3)(2, 4) = (2, 1)(3, 4) = a \end{cases}$$

hat wegen
Fließband von
Bezeichnungen
mit zwei
Bedeutungen:
• Konjugation
• Operation
von α
Diese stimmen
überein.

Gegeben:

Kurz exakte Sequenz von Gruppen und Gruppenmorphismen

$$N \xrightarrow{i} G \xrightarrow{r} H$$

$\overset{s}{\curvearrowright}$

+ Gruppenmorphisms s
 mit $r \circ s = \text{id}_H$

Dann:

- Operationen α von H auf N , für die gilt:

$$i(h \cdot n) = s(h) \cdot i(n) \quad \text{für } n \in N, h \in H$$

- Gruppenisomorphismus

$$N \times H \xrightarrow[\sim]{f} G$$

$$(n, h) \mapsto i(n) \cdot s(h)$$

Bsp:

$$A_5 \hookrightarrow S_5 \xrightarrow{\text{sgn}} \{\pm 1\}$$

kurz exakte Seq.

$\Rightarrow$

$$A_5 \times \{\pm 1\} \xrightarrow[\sim]{+} S_5$$

$$(a, \varepsilon) \mapsto a \cdot s(\varepsilon)$$

Kurz: $S_5 \cong A_5 \rtimes C_2$

H : Gruppe

A : abelsche Gruppe, $\alpha: H \rightarrow \text{Aut}(A)$ Gruppenchar.
 $h \mapsto (a \mapsto {}^h a)$

$$Z^1(H, A) := \left\{ H \xrightarrow{d} A : {}^h d(h') \cdot d(h h')^{-1} \cdot d(h) = 1 \text{ für } h, h' \in H \right\}$$

Derivationen oder 1-Cozyklen

$$B^1(H, A) := \left\{ H \xrightarrow{d_b} A, h \mapsto d_b(h) := {}^h b \cdot b^{-1} : b \in A \right\}$$

innere Derivationen oder 1-Grenzer

$$H^1(H, A) := Z^1(H, A) / B^1(H, A) : \text{erste Cohomologiegruppe}$$

$$Z^2(H, A) := \left\{ H \times H \xrightarrow{z} A : {}^h z(h', h'') \cdot z(h h', h'')^{-1} \cdot z(h, h' h'') \cdot z(h, h') = 1 \text{ für } h, h', h'' \in H \right\}$$

2-Cozyklen

$$B^2(H, A) := \left\{ H \times H \xrightarrow{z_c} A : (h, h') \mapsto z_c(h, h') = {}^h c(h') \cdot c(h h')^{-1} \cdot c(h) : H \xrightarrow{c} A \text{ Abbildung} \right\}$$

2-Grenzer

$$H^2(H, A) := Z^2(H, A) / B^2(H, A) : \text{zweite Cohomologiegruppe}$$

Bsp 106

p prim, $H = C_p = \langle h : h^p = 1 \rangle$, $A = C_p = \langle a : a^p = 1 \rangle$,
 $\alpha = ! : H \rightarrow \text{Aut}(A)$, d.h. ${}^h a = a$

$$(1) H^1(H, A) \cong C_p$$

Lemma 107

H : Gruppe, A : abelsche Gruppe, $\kappa: H \rightarrow \text{Aut}(A)$
 $h \mapsto (a \mapsto {}^h a)$

$K \leq H$ Untergruppe mit $[H:K]$ endlich

$$H = \bigsqcup_{t \in T} Kt, \quad t \in T, \quad h = \underbrace{\kappa(h)}_{\in K} \cdot \underbrace{\tau(h)}_{\in T}$$

(1) Wir haben Gruppenmorphisamen

$$\begin{array}{ccc} Z'(K, A) & \longleftrightarrow & Z'(H, A) \\ d \downarrow & \longmapsto & \left(d \uparrow_K^H : H \rightarrow A \right) \\ & & h \mapsto \prod_{t \in T} {}^t d(\kappa(th)) \end{array}$$

$$\tilde{d}|_K \longleftarrow \tilde{d}$$

(2) Wir haben Gruppenmorphisamen

$$\begin{array}{ccc} H'(K, A) & \longleftrightarrow & H'(H, A) \\ \text{Cores} \uparrow_K^H & & \\ d \cdot B'(K, A) & \longmapsto & \left(d \uparrow_K^H \cdot B'(H, A) \right) \\ \text{Res} \downarrow_K^H & & \\ \tilde{d}|_K \cdot B'(K, A) & \longleftrightarrow & \tilde{d} \cdot B'(H, A) \end{array}$$

Sei $\xi := \tilde{d} \cdot B'(H, A) \in H'(H, A)$ gegeben.

Es ist

$$\left(\text{Cores} \uparrow_K^H \circ \text{Res} \downarrow_K^H \right) (\xi) = \sum_{[H:K]}$$

Beweis zu (2) !

Allgemein: Für $h \in H$ ist $\bigsqcup_{t \in T} Kth^{-1} = H$.

Also: Wenn $t \in T$ durchläuft, dann durchläuft auch $\tau(th^{-1})$ die Menge T .

Lemma III

$A \xrightarrow{i} G \xrightarrow{r} H$: k.e.S. von Gruppen, A : abelsch

$\leadsto \alpha : H \rightarrow \text{Aut}(A) : h \mapsto (a \mapsto {}^h a)$

mit $i({}^h a) = g i(a)$,

wobei $g \in G$ mit $r(g) = h$

$H'(H, A)$: gebildet bzgl. α

$G \begin{array}{c} \xleftarrow{s} \\ \xrightarrow{r} \end{array} H$: s Gruppenmgl. mit $r \circ s = \text{id}_H$

Äquivalent sind (1, 2) :

(1) $H'(H, A) = 1$

(2) Für jeden Gruppenvergleich

$\tilde{s} : H \rightarrow G$ mit $r \circ \tilde{s} = \text{id}_H$
gibt es ein $b \in A$ mit $i(b) \cdot s(h) = \tilde{s}(h)$ für $h \in H$,

Bew.

(1) $\Rightarrow$ (2)

Gegeben : $G \begin{array}{c} \xleftarrow{s} \\ \xrightarrow{r} \end{array} H$ mit $r \circ s = \text{id}_H$

Gesucht : $b \in A$ mit $i(b) \cdot s(h) = \tilde{s}(h)$ für $h \in H$

Verwendbar : $Z'(H, A) = B'(H, A)$,

haben : $d : H \rightarrow A$ mit $i(d(h)) = s(h) \cdot \tilde{s}(h)^{-1}$ für $h \in H$.

Wissen : $d \in Z'(H, A)$. $\leftarrow$ "Quotient von s und $\tilde{s}$ ist ein 1-Cocycle"

H : Gruppe

A : abelsche Gruppe

$\alpha : H \rightarrow \text{Aut}(A) : h \mapsto (a \mapsto {}^h a)$ Gruppenhomomorphismus

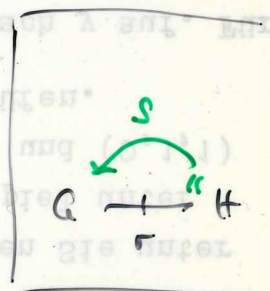
$H^2(H, A)$: bezüglich α gebildet

Äquivalent sind (1, 2) :

(1) $H^2(H, A) = 1$

(2) Für jede kurze exakte Sequenz $A \xrightarrow{i} G \xrightarrow{r} H$,
wobei i. S. v. 1.109 das α gilt,
existiert ein Gruppenhomomorphismus

$s : H \rightarrow A$ mit $r \circ s = \text{id}_H$



Bew. zu (1) $\Rightarrow$ (2) : Verwendbar : $Z^2(H, A) = B^2(H, A)$.

Sei $A \xrightarrow{i} G \xrightarrow{r} H$ eine k.e.S. wie beschrieben.

Sei $s : H \rightarrow A$ eine Abbildung mit $r \circ s = \text{id}_H$.

Sei $i(z(h, h')) = s(h) \cdot s(h') \cdot s(hh')^{-1}$,

wobei $z(h, h') \in A$ für $h, h' \in H$.

Dann : $z \in Z^2(H, A)$

"Nützlicher
Gruppenhomomorphismus
gilt 2-Gezähl"