§2 Nilpotente Gruppen

1. Kommutatoren

Konvention: $[a,b] = ab(ba)^{-1}$
$= aba^{-1}b^{-1}$

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

sowie $[a,bc] = [a,b]\, b\, [a,c]\, b^{-1}$ (nachrechnen)

Für Untergruppen $A, B \leq G$ setze $[A,B] = \langle [a,b] \mid a \in A, b \in B \rangle$
(Achtung! Erzeugnis)

Es gilt $A \leq N_G(B) \Leftrightarrow [A,B] \subseteq B$, denn:

$a \in N_G(B) \Rightarrow [a,b] = aba^{-1}b^{-1} \in B \Rightarrow [A,B] \leq B$

$aba^{-1}b^{-1} \in B \Rightarrow aba^{-1} \in B \Rightarrow aBa^{-1} \subseteq B$

Weiter gilt stets $[A,B] = [B,A] \trianglelefteq \langle A \cup B \rangle$ (ÜA)

Die Kommutatorgruppe einer Gruppe G ist $DG = [G,G]$.

Def Eine Untergruppe $H \leq G$ heißt charakteristisch in G, wenn für jeden Automorphismus $\alpha \in \mathrm{Aut}(G)$ gilt $\alpha(H) = H$.

Klar: charakteristische Untergruppen sind stets Normalteiler (denn $c_g : x \mapsto gxg^{-1}$ ist für jedes $g \in G$ ein Automorphismus von G).

2. Erinnerung: Man setzt $D^0 G = G$ sowie $D^{n+1} G = D(D^n G)$. Diese Gruppen sind offensichtlich charakteristisch in G, also insbesondere normal.
Eine Gruppe G heißt auflösbar, wenn $D^n G = \{1\}$ für ein $n \gg 0$.

Lemma: Untergruppen und Bilder von auflösbaren Gruppen sind auflösbar.

Beweis: Sei G auflösbar. Für $H \leq G$ Untergruppe gilt $D^n H \leq D^n G$ (Induktion nach n), also $D^n G = \{1\} \Rightarrow D^n H = \{1\}$.
Ist $\varphi : G \to K$ Homomorphismus, so folgt
$$D^n \varphi(G) = \varphi(D^n G) \Rightarrow \varphi(G) \text{ auflösbar.} \quad \square$$

Lemma: Ist $N \trianglelefteq G$ auflösbar und ist G/N auflösbar, so ist G auflösbar.

Beweis: Angenommen, $D^k N = \{1\}$ und $D^l(G/N) = \{N\}$.
Es folgt $D^l G \leq N \Rightarrow D^{k+l} G = \{1\}$ $\square$

Bsp: Jede abelsche Gruppe ist auflösbar.

3. __Def__ Sei G eine Gruppe. Wir setzen $L_0 G = G$ $\quad L_{n+1} G = [G, L_n G]$. Klar: $L_n G$ ist charakteristisch in G (also normal), damit $L_{n+1} G \subseteq L_n G$. Weiter $L_1 G = D^1 G$. Mit Induktion folgt $D^n G \subseteq L_n G$, denn

$$D^{n+1} G = [D^n G, D^n G] \subseteq [L_n G, G] = L_{n+1} G$$

Wir nennen G __nilpotent__, wenn es ein $n \geq 0$ gibt mit $L_n G = \{1\}$. Die __Nilpotenzklasse__ einer nilpotenten Gruppe ist das kleinste $n \geq 0$ mit $L_n G = \{1\}$.

Klasse 0 $\Leftrightarrow$ $G = \{1\}$

Klasse 1 $\Leftrightarrow$ $G \neq \{1\}$ abelsch

Klar nach obiger Bemerkung:

Abelsch $\Rightarrow$ nilpotent $\Rightarrow$ auflösbar.

__Bsp__ $\mathrm{Sym}(3)$ ist auflösbar, $D\,\mathrm{Sym}(3) = \mathrm{Alt}(3) \cong \mathbb{Z}/3$, aber __nicht__ nilpotent. Denn

$L_1 \mathrm{Sym}(3) = \mathrm{Alt}(3)$

$L_2 \mathrm{Sym}(3) = [\mathrm{Alt}(3), \mathrm{Sym}(3)] = \mathrm{Alt}(3)$

$(1,2)(1,2,3)(1,2)(3,2,1) = (1,2,3)$ erzeugt $\mathrm{Alt}(3)$

Lemma Untergruppen und Bilder nilpotenter Gruppen sind wieder nilpotent.

Beweis Sei G nilpotent, $H \leq G$ Untergruppe.

$$L_{n+1} H = [L_n H, H] \underset{\substack{\uparrow \\ \text{Induktion}}}{\leq} [L_n G, G] = L_{n+1} G$$

$\varphi : G \to K$ Homomorphismus $\Rightarrow$ $\varphi(L_n G) = L_n(\varphi(G))$. $\square$

Vorsicht: Das 2. Lemma in § 2.2 hat kein Analogon für nilpotente Gruppen. Bsp. K Körper, $\operatorname{char} K \neq 2$

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \;\middle|\; a, b \in K, a \neq 0 \right\}$$

$$U = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in K \right\} \cong (K, +)$$

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (a^2-1)b \\ 0 & 1 \end{pmatrix}$$

Klar: $DG \leq U$ und damit G auflösbar

$\rightsquigarrow$ DG enthält alle Quadrate in K

$\rightsquigarrow$ DG enthält alle $x \in K$ (weil $\operatorname{char} K \neq 2$ gilt für alle $x \in K$ $x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$)

Also $DG = U$ (für $\operatorname{char} K \neq 2$) und

$[DG, U] = U$ $\rightsquigarrow$ G nicht nilpotent, $L_1 G = L_2 G$

Aber $U \trianglelefteq G$, U abelsch (also nilpotent)

$G/U \cong K^*$ abelsch (also nilpotent)

Fazit: Ist $N \trianglelefteq G$ und sind N, G/N nilpotent, so folgt nicht immer, dass G nilpotent ist.

Es gilt aber noch folgendes.

Lemma: Ist $G/\mathrm{Cen}(G)$ nilpotent, so ist G nilpotent.

Beweis: $L_n(G/\mathrm{Cen}(G)) = \{\mathrm{Cen}(G)\} \Rightarrow L_n G \subseteq \mathrm{Cen}(G)$

$\Rightarrow L_{n+1} G = [G, L_n G] = \{1\}$ □

Erinnerung: Ist p eine Primzahl und G endlich mit Ordnung $\# G = p^l$ für ein $l \geq 0$, so heißt G p-Gruppe.

4\. Lemma: p-Gruppen sind nilpotent.

Beweis: Sei $\# G = p^l$. Für $l = 1$ ist $G \cong \mathbb{Z}/p$ abelsch $\to$ fertig. Jetzt Induktion nach l.

Klassengleichung: $\# G = \# \mathrm{Cen}(G) + \sum_{i=1}^{r} \# K_i$

K_i Konjugationsklassen der nicht-zentralen Elemente in G

$K_i = \{gag^{-1} \mid g \in G\}$ $\quad \# K_i = \dfrac{\# G}{\# \mathrm{Cen}_G(a)} \geq 1$

$\Rightarrow p \mid \# K_i$ für alle i $\Rightarrow p \mid \# \mathrm{Cen}(G) \Rightarrow \mathrm{Cen}(G) \neq 1$

Nach Induktionsannahme ist $G/\mathrm{Cen}(G)$ nilpotent. □

#

5. Definition $Z_0 G = \{1\}$ $Z_1 G = \mathrm{Cen}(G)$

allgemein $Z_{i+1} G = \pi^{-1}(\mathrm{Cen}(G/Z_i G))$, wobei

$\pi : G \to G/Z_i G$ die kanonische Projektion ist.

Man nennt $Z_n G$ das <u>n-te Zentrum</u> von G.

Klar: $Z_n G$ ist charakteristisch in G und

$Z_n G \subseteq Z_{n+1} G$ und $\mathrm{Cen}(G/Z_i G) = Z_{i+1}G / Z_i G$

<u>Satz</u> G ist genau dann nilpotent, wenn $Z_n G = G$

für ein $n \gg 0$. Wenn G nilpotent ist, so gilt

$$Z_j G = G \iff L_j G = \{1\}$$

<u>Bew.</u> Angenommen, $L_m G = \{1\}$. Wir zeigen, dass

$L_{m-j} G \subseteq Z_j G$. Für $j=0$ stimmt das.

Jetzt Induktion.

$$[L_{m-j-1} G, G] = L_{m-j} G \overset{\text{I.A.}}{\subseteq} Z_j G \text{, also}$$

$$L_{m-j-1} G \cdot Z_j G / Z_j G \subseteq \mathrm{Cen}(G/Z_j G) = Z_{j+1} G / Z_j G$$

$\Rightarrow L_{m-j-1} G \subseteq Z_{j+1} G$. $\to$ Induktion klappt.

Also $L_0 G = G \subseteq Z_m G$.

Angenommen, $Z_m G = G$ für ein $m \gg 0$. Beh.: Dann gilt $L_j G \leq Z_{m-j} G$. Wieder mit Induktion, für $j=0$ stimmt das.

Wenn $L_j G \leq Z_{m-j} G$, dann

$$L_{j+1} G = [G, L_j G] \leq [G, Z_{m-j} G] \leq Z_{m-j-1} G$$

nach Definition der $Z_j G$. Induktion klappt.

Also $L_m G \leq Z_0 G = \{1\}$ $\square$

<u>Korollar</u> Die Nilpotenzklasse einer nilpotenten Gruppe G ist $\min\{j \mid Z_j G = G\}$

$$= \min\{j \mid L_j G = \{1\}\}.$$

Wenn $G/_{\mathrm{Cen}(G)}$ Nilpotenzklasse m hat und $G \neq \{1\}$, dann hat G Nilpotenzklasse $m+1$ $\square$

<u>Bem</u> Man nennt die Folge von charakteristischen Untergruppen $L_j G \trianglelefteq G$ die <u>untere Zentralreihe</u> und $Z_j G$ die <u>obere Zentralreihe</u> einer Gruppe G.

Der vorige Satz besagt, dass in einer nilpotenten Gruppe beide Reihen die gleiche Länge haben, nämlich die Nilpotenzklasse von G.

6. In jeder Gruppe gilt die <u>Hall-Witt-Identität</u>

$$a\left[c\left[a^{-1},b\right]a^{-1}\cdot b\left[a\left[b^{-1},c\right]b^{-1}\cdot c\left[b\left[c^{-1},a\right]c^{-1}=1\right.\right.\right.$$

<u>Korollar</u> (Hall) Sind $A, B, C \subseteq G$ Untergruppen mit

$[A,[B,C]] = [C,[A,B]] = 1$, so gilt auch

$[B,[C,A]] = 1$

<u>Beweis</u> Mit der Identität oben folgt $[b[c^{-1},a]] = 1$

für alle $b \in B$, $c \in C$, $a \in A$, d.h. B zentralisiert die Erzeuger von $[C,A]$, also B zentralisiert $[C,A]$ $\square$

<u>Satz</u> In jeder Gruppe gilt

$$[L_i G, L_j G] \subseteq L_{i+j+1} G$$

<u>Beweis</u> Induktion nach j. (i beliebig.) Für $j=0$ haben wir

$[L_i G, L_0 G] = [L_i G, G] = L_{i+1} G$ (✓)

Jetzt Induktionsschritt

$[L_i G, L_{j+1} G] = [L_i G, [G, L_j G]]$

Nun gilt $[G,[L_j G, L_i G]] \subseteq [G, L_{i+j+1} G] = L_{i+j+2} G$

$[L_j G, [L_i G, G]] = [L_j G, L_{i+1} G] \subseteq L_{i+j+2} G$

Nach obigem Korollar also auch

$[L_i G, [G, L_j G]] \subseteq L_{i+j+2} G$ $\square$

7. **Def** Ein iterierter $(l+1)$-facher Kommutator ist eine Abbildung $G^{l+1} \to G$, die durch Verknüpfen der Kommutatorabbildung $[\,,\,] : G \times G \to G$ entsteht, etwa

$$(a,b,c,d) \longmapsto [[a,c],[b,d]]$$
$$(a,b,c,d) \longmapsto [a,[c,[d,b]]]$$

Satz Ist $c : G^{l+1} \to G$ solch ein $(l+1)$-facher Kommutator, so gilt $c(\underbrace{G \times \dots \times G}_{l+1}) \subseteq L_l(G)$.

Beweis Induktion nach l. $l = 1$

$(a,b) \longmapsto [a,b]$ oder $(a,b) \longmapsto [b,a]$,

Bild liegt in $L_1 G = DG$ ($\checkmark$)

Allgemein $c : G^{l+1} \to G$, $\pi \in \mathrm{Sym}(l+1)$

$$c(g_0, \dots, g_l) = \underbrace{[\underbrace{c_1(g_{\pi_0}, \dots, g_{\pi_k})}_{\in L_k G}, \underbrace{c_2(g_{\pi_{k+1}}, \dots, g_{\pi_l})}_{\in L_{l-k-1} G}]}_{\in L_l G}$$

$\square$

Korollar Ist G nilpotent der Klasse l, so verschwinden alle j-fachen Kommutatoren für $j > l$. $\square$

8. Endlich erzeugte abelsche Gruppen

Erinnerung: Ist $(A,+)$ frei abelsch, $A \cong \mathbb{Z}^n$, so heißt $B \subseteq A$ Basis, wenn B ein EZS für A ist, so dass jedes $a \in A$ eine eindeutige Darstellung

$$a = \sum_{b \in B} b a_b \qquad a_b \in \mathbb{Z} \qquad \text{hat}$$

(Äquivalent: die Elemente von B sind in $\mathbb{Q}^n$ $\mathbb{Q}$-linear unabhängig und ein EZS von $\mathbb{Z}^n$) Alle Basen für $\mathbb{Z}^n$ haben Länge n.

Theorem (Elementarteilersatz)

Sei $H \leq A \cong \mathbb{Z}^n$ eine beliebige Untergruppe, $H \neq \{0\}$.

Dann existiert eine Basis $B = \{b_1, \dots, b_n\}$ von A sowie Zahlen $m_1, \dots, m_d \geq 1$ mit $m_j \mid m_{j+1}$, so dass $H = \left\{ \sum_{i=1}^{d} b_i m_i k_i \;\middle|\; k_i \in \mathbb{Z} \right\} \cong \mathbb{Z}^d$.

Diese Elementarteiler m_i sind durch H eindeutig bestimmt.

Beweis: Sei $\mathcal{B}$ die Menge aller Basen von A.

Für $h \in H - \{0\}$ und $B \in \mathcal{B}$ setze

$$h = \sum_{b \in B} b h_b \qquad \text{sowie} \quad n(h,B) = \min\{|h_b| \mid h_b \neq 0\}$$

Wähle nun $h \in H - \{0\}$ und $B \in \mathcal{B}$ so, dass

$m = n(h,B)$ minimal ist.

Wegen $n(h,B) = n(-h,B)$ können wir

schreiben $h = bm + \sum_{c \in G} c\,h_c$ $\qquad G = B - \{b\}$

<u>Beh: Für alle $c \in G$ gilt $m \mid h_c$.</u>

Denn: schreibe $h_c = m \cdot q_c + r_c$ $\qquad 0 \leq r_c < m$

$b' = b + \sum_{c \in G} c \cdot q_c$. Dann ist $B' = \{b'\} \cup G$

wieder eine Basis. Wäre ein $r_c \neq 0$, so

wäre $n(h, B') < m$ $\lightning$ $(h = b' \cdot m + \sum_{c \in G} c\,r_c)$.

Also gilt $m \mid h_c$ für alle c und $h = b'm$ $\#$

Sei $\pi : A \to \mathbb{Z}$ die Abbildung, die jedem $a \in A$ den Koeffizienten von b' bzgl der Basis B' zuordnet. Es folgt $\pi(H) = m\mathbb{Z}$. Für jedes $x \in H$ gilt $x - \underbrace{b'\pi(x)}_{\in H} \in H \cap A' = H'$

wobei $A' = \langle G \rangle \cong \mathbb{Z}^{n-1}$. Also

$$A = b'\mathbb{Z} \oplus A'$$

$$H = b'm\mathbb{Z} \oplus H'$$

Ist nun E eine beliebige Basis von A', so ist $\{b'\} \cup E$ eine Basis für A und das Argument oben zeigt, dass m alle Koeffizienten der $h \in H$ bzgl. $E \cup \{b'\}$ teilt.

Die Beh. folgt nun mit Induktion. Aus der Konstruktion $m = m_1 = \min\{n(h,B) \mid h \in H - \{0\}, B \in \mathcal{B}\}$ folgt die Eindeutigkeit von m_1 und damit induktiv die Eindeutigkeit der m_i. $\square$

Korollar Ist $(A,+)$ eine endlich erzeugte abelsche Gruppe, so existieren Zahlen $m_1 | m_2 | \ldots | m_d$ mit

$$A \cong \mathbb{Z}/m_1 \oplus \mathbb{Z}/m_2 \oplus \ldots \oplus \mathbb{Z}/m_d \oplus \mathbb{Z}^k$$

Beweis Da A endlich erzeugt ist, existiert ein Epimorphismus $\mathbb{Z}^n \to A$ mit Kern $H \subseteq \mathbb{Z}^n$. Wende nun den Elementarteilersatz an. $\square$

Korollar Untergruppen von endlich erzeugten abelschen Gruppen sind wieder endlich erzeugt. $\square$

Sei $(A,+)$ eine beliebige abelsche Gruppe. Die Torsionsgruppe von A ist $tA = \{a \in A \mid$ es gibt $m \geq 1$ mit $m \cdot a = 0\}$. Wenn gilt $tA = \{0\}$, so heißt A torsionsfrei. Der Quotient A/tA ist stets torsionsfrei. Ist A endlich erzeugt, so gilt $A \cong \mathbb{Z}^k \oplus tA$. Man nennt den $\mathrm{rk}_{\mathbb{Q}}(A) = k$ den $\mathbb{Q}$-Rang von A.

Ist also $(A,+)$ endlich erzgt abelsch Gruppe mit $rk_{\mathbb{Q}} A = n$, so folgt

$$\beta_{A,S} \sim t^n$$

<u>Bem</u> Es gibt torsionsfreie abelsch Gruppen, die <u>nicht</u> frei sind, z.B. $(\mathbb{Q},+)$ oder $\mathbb{Z}^{\mathbb{N}}$.

9. <u>Lemma</u> (Baer) Ist G endlich erzeugt und nilpotent, so ist DG endlich erzgt.

<u>Beweis</u> In jeder Gruppe gilt

$$[a,b][a,c] = [a,bc]\,[b,[c,a]] \qquad \text{(nachrechnen)}$$

$$\Rightarrow \quad [a,bc] = [a,b][a,c][[c,a],b]$$

Sei $S \subseteq G$ ein endliches Erzeugendensystem.

Da DG von den Kommutatoren erzeugt wird, wird mit der Identität oben DG von allen Elementen $c(t_1,\dots,t_e)$ $t_j \in S \cup S^{-1}$ erzeugt, wobei c alle iterierte Kommutatoren der Länge l durchläuft, für alle $l \geq 2$.

Da G nilpotent ist, müssen wir nur Kommutatoren der Länge $l \leq n$ betrachten, wobei n die

Nilpotenzklasse ist. Davon gibt es nur endlich viele. $\square$

<u>Theorem</u> (<u>Baer</u>) Ist G nilpotent und endlich erzeugt, so ist <u>jede</u> Untergruppe $H \leq G$ endlich erzeugt.

<u>Beweis</u> Setze $H_i = H \cap D^i G$. Da G auflösbar ist, ist $H_n = \{1\}$ für $n \gg 0$. Wir zeigen: ist H_{i+1} endlich erzeugt, so ist auch H_i endlich erzeugt. Da H_n endlich erzeugt ist, folgt, dass $H = H_0$ endlich erzeugt ist.

$$\underset{\uparrow \text{ Isomorphiesatz}}{H_i/H_{i+1} \cong H_i D^{i+1}G / D^{i+1}G} \leq D^i G / D^{i+1} G$$

Nun ist $D^1 G$ endlich erzeugt nilpotent, also auch $D^2 G$, $D^3 G$ usw $\Rightarrow$ $D^i G / D^{i+1} G$ ist endlich erzeugte abelsche Gruppe. Folglich ist nach §2.8 auch H_i / H_{i+1} endlich erzeugt. Da H_{i+1} endlich erzeugt ist, ist dann auch H_i endlich erzeugt. $\square$

10. Das Wachstum nilpotenter Gruppen

Sei G eine endlich erzeugte nilpotente Gruppe von Nilpotenzklasse r. Wir überlegen, dass $\beta_{G,S}$ polynomial beschränkt ist.

$\underline{r=1}$ $L_1 G = \{1\} \Rightarrow G$ abelsch, und §2.8 gilt $G \cong \mathbb{Z}^k \times \underbrace{tG}_{\text{endlich}}$, also ist G virtuell isomorph zu $(\mathbb{Z}^k,+)$ und $\beta_{G,S}(l) \sim l^k$, vgl. §1.15.

$\underline{r=2}$ $L_1 G \neq \{1\} = L_2 G$ d.h. $L_1 G = DG \subseteq Cen(G)$ (wegen $[G, L_1 G] = \{1\}$).

Nach Baers Satz §2.9 ist $L_1 G$ endlich erzeugt. Wir wählen ein endliches EZS $S = \{s_1, \ldots, s_m\} \subseteq G$ so, dass $L_1 G = \langle S \cap L_1 G \rangle$. Sei $l \geq 1$.

Wie viele Elemente g hat G mit $l_S(g) \leq l$?

$l_S(g) = l \Rightarrow g = t_1 \cdots t_l \qquad t_i \in S \cup S^{-1}$

Mit $ab = [a,b]ba$ können wir die t_i umsortieren.

Die dabei entstehenden Kommutatoren $[t_i, t_j]$ vertauschen mit allen Gruppenelementen. Also

$g = \tilde{g}\, s_1^{l_1} \cdots s_m^{l_m}$ und $\tilde{g}$ ist ein

$|l_1| + \cdots + |l_m| \leq l$

Produkt von l' Kommutatoren von Elementen aus $S \cup S^{-1}$, mit $l' \leq l^2$ (öfter müssen wir nicht vertauschen).

Die abelsche Gruppe $L_1 G \cong \mathbb{Z}^k \oplus E$ hat
$\uparrow$ endlich

Wachstum $\sim t^k$. Es gibt nur endlich viele Kommutatoren mit Einträgen aus $S \cup S^{-1}$, insbesondere gibt es eine obere Schranke C' für die Wortlänge dieser Kommutatoren bzgl. $S \cap L_1 G$. Die Anzahl der Möglichkeiten für $\tilde{g}$ ist damit beschränkt durch

$$\sim (C' \cdot l')^k \sim (l')^k \leq (l^2)^k = l^{2k},$$

Die Anzahl der Möglichkeiten für $s_1^{l_1} \ldots s_m^{l_m}$ ist beschränkt durch l^m, wegen $|l_i| \leq l$.

Also $\beta_{G,S}(t) \leq t^m \cdot t^{2k} = t^{m+2k}$ polynomial.

#

Jetzt allgemein $r \geq 2$, Induktion nach r ($r = 1$ ok)

Wir wählen S so, dass $\langle S \cap L_1 G \rangle = L_1 G$.

Nach Induktionsannahme hat $L_1 G$ polynomiales Wachstum. bzgl.

Sei $g \in G$, $l_S(g) = l$, $g = t_1 \cdots t_l$ $t_i \in S \cup S^{-1}$.

Wir sortieren wieder die Erzeuger alphabetisch von nach rechts und erhalten

$$g = \tilde{g} \cdot s_1^{l_1} \cdots s_m^{l_m} \qquad |l_i| \leq l.$$

Dann ist $\tilde{g}$ Produkt von iterierten Kommutatoren der Länge $\leq r$, mit Einträgen aus $S \cup S^{-1}$.

Wieviele solche Kommutatoren der Länge t entstehen

$$\left.\begin{array}{ll} t = 2 & \text{höchstens } l^2 \\ t = 3 & \text{höchstens } l^3 \\ \vdots & \\ t = r & \text{höchstens } l^r \end{array}\right\} \text{höchstens } r l^r \text{ Kommutatoren.}$$

Die Wortlänge der Kommutatoren mit Einträgen aus $S \cup S^{-1}$ ist beschränkt $\Rightarrow$ Für $\tilde{g}$ höchstens

$p(C \cdot l^{r+1})$ Möglichkeiten, p Polynom

da die Kommutatoren in $L_1 G$ liegen.

Damit Anzahl der Möglichkeiten für g höchstens

$$l^m \cdot p(C' l^r) \quad \text{polynomial.}$$

Theorem Endlich erzeugte nilpotente Gruppen haben polynomiales Wachstum.
Etwas allgemeiner: endlich erzeugte virtuell nilpotente Gruppen haben polynomiales Wachstum.

11. Torsion in nilpotenten Gruppen

Erinnerung: G heißt torsionsfrei, wenn gilt $\{g \in G \mid o(g) < \infty\} = \{1\}$.

Sei G nilpotent und sei $tG = \{g \in G \mid o(g) < \infty\}$.

Unser Ziel ist zu zeigen, dass tG eine charakteristische Untergruppe ist.

Lemma Sei G nilpotent mit Nilpotenzklasse r. Sei $g \in G$ beliebig. Dann gilt

$$N = \langle g \rangle L_1 G \trianglelefteq G \quad \text{und} \quad L_{r-1} N = \{1\}$$

Beweis Da $L_1 G \trianglelefteq G$ ein Normalteiler ist, ist $\langle g \rangle L_1 G \leq G$ eine Untergruppe. Sei $a \in G$, $k \in \mathbb{Z}$, $h \in L_1 G$. Dann gilt

$$a(g^k h)a^{-1} = a g^k a^{-1} \underbrace{a h a^{-1}}_{= h' \in L_1 G} = \underbrace{\underbrace{a g^k a^{-1} g^{-k}}_{\in L_1 G} \underbrace{g^k h'}_{\in N}}_{\in N}$$

also $N \trianglelefteq G$.

Sei jetzt $a, b \in L_1 G$ beliebig, $k, l \in \mathbb{Z}$

$$[g^k a, g^l b] = [g^k a, g^l] \underbrace{[g^k a, b]}_{\in L_2 G} \underbrace{[[b, g^k a], g^l]}_{\in L_3 G}$$

$$\equiv [g^k a, g^l] \mod L_2 G$$

$$\equiv [g^k, g^l] \mod L_2 G$$

$$\equiv 1 \mod L_2 G$$

d.h. $L_1 N \leq L_2 G \Rightarrow L_{r-1} N \leq L_r G = \{1\}$ $\square$

<u>Theorem</u> Wenn G nilpotent ist, dann ist $tG = \{g \in G \mid o(g) < \infty\}$ eine charakteristische Untergruppe in G und $G/_{tG}$ ist torsionsfrei.

<u>Beweis</u> Induktion nach der Nilpotenzklasse $r_n G$.
$r = 0, 1$ klar, vgl §2.8.
Sei nun $a, b \in tG$ mit $a^m = 1$. Setze $N = \langle b \rangle L_1 G$. Nach Induktionsannahme ist tN eine charakteristische Untergruppe. Da $N \trianglelefteq G$ ist $tN \trianglelefteq G$. Es gilt

$(ab)^m = ab a^{-1} a^2 b a^{-2} \cdots a^m b \underbrace{a^{-m}}_{=1} \in B$ (weil $B \trianglelefteq G$). Für alle k gilt nun $a^k b a^{-k} \in tB$

$\Rightarrow (ab)^m \in tB \Rightarrow o(ab^m) < \infty \Rightarrow o(ab) < \infty$

d.h. $ab \in tG$.

Ist $gtG \in t(G/tG)$ so folgt $g^k \in tG$ für ein $k > 0$ $\Rightarrow o(g^k) < \infty \Rightarrow o(g) < \infty$

$\Rightarrow g \in tG$. Also ist G/tG torsionsfrei.

Korollar Ist G endlich erzeugt und nilpotent mit $tG = G$, so ist G endlich.

Beweis Induktion nach Nilpotenzklasse r.

$r = 0, 1 \Rightarrow$ ok nach §2.8. Jetzt $r \geq 2$.

$L_1 G$ endlich nach Ind. ann. und G/L_1G endlich

$\Rightarrow G$ endlich. $\square$

Korollar Ist G endlich erzeugt und nilpotent, so ist tG endlich.

Beispiel $G = \{ x \mapsto ax+b \mid a = \pm 1,\ b \in \mathbb{Z} \}$

G wird erzeugt von $x \mapsto -x$ und $x \mapsto 1-x$

$DG = \{ x \mapsto x+b \} \cong \mathbb{Z}$, $[G : DG] = 2$, also

ist G virtuell abelsch (und virtuell nilpotent), sowie auflösbar.

Es gilt aber

$$\{ g \in G \mid o(g) < \infty \} = \{ x \mapsto b-x \} = \{ g \in G \mid o(g) = 2 \}$$

keine Untergruppe, nicht endlich (G nicht nilpotent!)

12. Erinnerung Eine Normalreihe in einer Gruppe G

ist eine Folge von Untergruppen

$$\{1\} = G_m \subseteq G_{m-1} \subseteq \dots \subseteq G_0 = G$$

mit $G_{i+1} \trianglelefteq G_i$. Die Quotienten G_i / G_{i+1} nennt

man Faktoren der Normalreihe.

Bsp G auflösbar $\Leftrightarrow$ G besitzt eine Normalreihe mit abelschen Faktoren

(Ü 4)

Def Eine Gruppe G heißt polyzyklisch, wenn

G eine Normalreihe mit zyklischen Faktoren

hat. Polyzyklische Gruppen sind also auflösbar.

Eine Gruppe heißt überauflösbar (super-solvable), wenn es eine Folge von

Normalketten $1 = N_m \leq \ldots \leq N_0 = G$
gibt, $N_i \trianglelefteq G$, so dass N_i/N_{i+1} zyklisch ist.

Also

über auflösbar $\Rightarrow$ polyzyklisch $\Rightarrow$ auflösbar.

Beispiel $\mathrm{Alt}(4)$ ist auflösbar und polyzyklisch, aber nicht nilpotent und nicht über auflösbar. (ÜA)

13 Satz Jede endlich erzeugte nilpotente Gruppe ist über auflösbar, also polyzyklisch.

Beweis Sei $a \in L_n G$. Dann gilt
$\langle a \rangle L_{n+1} G \trianglelefteq G$, denn: für jedes $g \in G$ gilt

$[g,a] \equiv 1 \mod L_{n+1} G$

$\Leftrightarrow$ $gag^{-1} \equiv a \mod L_{n+1} G$

$\Leftrightarrow$ $g\, a L_{n+1}G\, g^{-1} = a L_{n+1} G$

Ist nun G endlich erzeugt, so gibt es
$a_1, \ldots, a_s \in L_n G$ mit

$$L_nG/L_{n+1}G \cong \mathbb{Z}/m_1 \oplus \ldots \oplus \mathbb{Z}/m_s \qquad m_s \neq 1$$

$a_i L_{n+1}$ Erzeuger des Faktors $\mathbb{Z}/m_i$

Äquivalent:

$$L_nG/_{L_{n+1}G} = \langle a_1 L_{n+1}G\rangle \oplus \dots \oplus \langle a_s L_{n+1}G\rangle$$

Jede Untergruppe $A_j = \langle a_j\rangle L_{n+1}G$

ist normal in G, also auch $N_j = A_1 \cdots A_j \trianglelefteq G$

$N_{j+1}/N_j \cong \mathbb{Z}/m_{j+1}$. Damit verfeinern wir

die Normalreihe

$$L_0G \supseteq L_1G \supseteq \quad \supseteq L_rG = \{1\}$$

zu einer Normalreihe mit zyklischen Faktoren so, dass die Gruppen der Normalreihe alle normal in G sind. $\square$

14. <u>Erinnerung</u>: Eine Gruppe G heißt <u>residuell endlich</u>, wenn es zu jedem $g \in G - \{1\}$ einen Normalteiler $N \trianglelefteq G$ gibt mit $g \notin N$ und $[G:N] < \infty$. Äquivalent dazu: es gibt eine (möglicherweise unendliche) Familie $(E_i)_{i\in I}$ von endlichen Gruppen und einen Monomorphismus

$$G \to \prod_{i\in I} E_i$$

Untergruppen von residuell endlichen Gruppen sind residuell endlich.

Lemma Ist G Gruppe, $H \subseteq G$ Untergruppe mit $[G:H] < \infty$ und ist H residuell endlich, so ist G residuell endlich.

Beweis Sei $g \in G - \{1\}$. Dann gibt es eine Untergruppe $H' \subseteq H$ mit endlichem Index in H, die g nicht enthält. Weiter ist $[G:H'] = [G:H][H:H'] < \infty$. Unter dem Homomorphismus

$$\begin{aligned} G &\longrightarrow \mathrm{Sym}(G/H') \\ g &\longmapsto [aH' \mapsto gaH'] \end{aligned}$$

hat g nichttriviales Bild. $\square$

Lemma Ist G endlich erzeugte Gruppe, so gibt es für jedes $n \geq 1$ nur endlich viele Untergruppen vom Index n in G.

Beweis Da G endlich erzeugt ist, ist $\mathrm{Hom}(G, \mathrm{Sym}(n))$ endlich. Für jede Untergruppe $H \subseteq G$ vom Index n wähle eine Bijektion $\alpha_H : G/H \longrightarrow \{1, \dots, n\}$ mit $\alpha_H(H) = 1$, so erhalte Homomorphismus $\tau_H : G \to \mathrm{Sym}(n)$, Stabilisator von $1 \in \{1, \dots, n\}$ ist genau H.

Da es nur endlich viele G-Wirkungen auf $\{1, \dots, n\}$ gibt, gibt es nur endlich viele Untergruppen vom Index n. $\square$

Wenn gilt $[G:K], [G:L] < \infty$, so folgt $[G:K\cap L] < \infty$.

Denn: betrachte die Wirkung

$$G \times G/K \to G/K, \text{ damit } L \times G/K \to G/K$$

Der Stabilisator von K in L ist $K \cap L$.

Wir erhalten eine <u>injektive</u> Abbildung

$$L/K\cap L \longrightarrow G/K$$
$$g(K\cap L) \longrightarrow gK$$

Da G/K endlich ist, ist $L/K\cap L$ endlich, also

$$[G:K\cap L] = [G:L][L:K\cap L] < \infty$$

$\square$

Kor Ist G endlich erzeugt und $H \leq G$ mit endlichem Index, so gibt es eine charakteristische Untergruppe $M \leq G$ mit $[G:M] < \infty$ und $M \leq H$.

Beweis Sei $n = [G:H]$, setze $M = \bigcap \{H' \leq G \mid [G:H'] = n\}$. $\square$

15 Satz (Malcev) Sei G eine Gruppe, $N \trianglelefteq G$ Normalteiler, $E \leq G$ Untergruppe mit $G = EN$ und $E \cap N = \{1\}$ (d.h. G ist semidirektes Produkt aus E und N). Wenn E residuell endlich ist und N endlich erzeugt und residuell endlich ist, so ist G residuell endlich.

Beweis Ist $g \in G - N$, so betrachte $G/N \cong E$. Da E residuell endlich ist, existiert eine endliche Gruppe F, ein Homomorphismus $\varphi: E \to F$ sodass, dass

$$G \to G/N \cong E \to F$$

g nicht trivial abbildet.

Ist $g \in N$, so wähle $M \leq N$ charakteristisch mit $[N:M] < \infty$ und $g \notin M$. Da N normal in G ist, folgt $M \trianglelefteq G$. Weiter gilt $g \notin EM$, denn $g = ab$ $\begin{matrix} a \in E \\ b \in M \end{matrix}$

$\Rightarrow a = gb^{-1} \in N \Rightarrow a = 1 \Rightarrow g = b \in M$ ↯

Nun gilt $G = EN$, $N = Mx_1 \cup \ldots \cup Mx_s$
$[N:M] = s \Rightarrow G = EMx_1 \cup \ldots \cup EMx_s$, $[G:EM] = s$
und $g \notin EM$. Wir erhalten einen Homomorphismus
$G \xrightarrow{\Psi} \mathrm{Sym}(G/EM)$ mit $\Psi(g) \neq id$. $\square$

16. <u>Korollar</u> Polyzyklische Gruppen sind residuell endlich.

<u>Beweis</u> Sei $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_m = \{1\}$ mit
$G_{i+1} \trianglelefteq G_i$, G_i/G_{i+1} zyklisch. Induktion nach m.

<u>$m=1$</u> G zyklisch, also residuell endlich, fertig.

<u>$m \geq 2$</u> 1. Fall G_0/G_1 endlich
Dann ist G_1 residuell endlich, also nach §2.14 auch G.
2. Fall $G_0/G_1 \cong \mathbb{Z}$. Wähle $u \in G$ so, dass uG_1 Erzeuger von G_0/G_1 ist.
Setze $E = \langle u \rangle$, es folgt $E \cap G_1 = \{1\}$ und $G = E \cdot G_1$. Da G_1 endlich erzeugt und residuell endlich ist (Induktion für erstere) ist nach Malcevs Satz auch G residuell endlich.

17. **Lemma** Ist G residuell endlich und ist $E \leq G$ endliche Untergruppe, so existiert ein Normalteiler $N \trianglelefteq G$ mit $N \cap E = \{1\}$ und $[G:N] < \infty$.

Beweis Sei $E - \{1\} = \{a_1, \ldots, a_m\}$. Wähle $N_j \trianglelefteq G$ mit $a_j \notin N_j$ und $[G:N_j] < \infty$.
Setze $N = N_1 \cap \ldots \cap N_m$. $\square$

18. **Theorem** Ist G eine endlich erzeugte nilpotente Gruppe, so ist G residuell endlich. Es gibt einen torsionsfreien Normalteiler $N \trianglelefteq G$ mit $[G:N] < \infty$.

Beweis Nach § 2.12 ist G polyzyklisch, also residuell endlich nach § 2.16. Nach § 2.11 ist tG endlich. Nach § 2.17 existiert $N \trianglelefteq G$ mit $(tG) \cap N = \{1\}$ und $[G:N] < \infty$. $\square$

Zum Abschluss betrachten wir noch die Struktur der endlichen nilpotenten Gruppen.

19. Lemma Sei G eine endliche Gruppe, X endliche Menge, $G \times X \to X$ eine Wirkung und sei $p \in \mathbb{P}$ Primzahl. Wenn es zu jedem $x \in X$ eine p-Gruppe $P(x) \leq G$ gibt mit $\{x\} = \mathrm{Fix}(P(x), X)$, so ist die Wirkung transitiv und $\# X \equiv 1 \pmod p$

Beweis Angenommen, $X = Y \dot\cup Z$, G wirkt auf beiden Mengen, $Y \neq \emptyset \neq Z$. Sei $y \in Y$. Es folgt $\mathrm{Fix}(P(y), Z) = \emptyset$ sowie $\# Y \equiv 1 \pmod p$ (alle $P(y)$-Bahnen in Y haben als Länge eine p-Potenz) und $\# Z \equiv 0 \pmod p$. Vertauschen von Y und Z ergibt Widerspruch. Also wirkt G transitiv und $\# X \equiv 1 \pmod p$ $\square$

20. Satz (Cauchy) Ist G endlich, p Primzahl, die $\# G$ teilt, so existiert $g \in G$ mit $o(g) = p$.

Beweis Sei $X = \{(x_1, \dots, x_p) \in G \times \dots \times G \mid x_1 \cdots x_p = 1\}$

$\Rightarrow \# X = (\# G)^{p-1} \Rightarrow p \mid \# X$. Die Gruppe $\mathbb{Z}/p$ wirkt auf X durch zyklische Permutation der p-Tupel. Jede Bahn dieser Wirkung hat Länge 1 oder p. Es gibt einen Fixpunkt $(1, \dots, 1)$, also mindestens einen weiteren Fixpunkt $(g, \dots, g) \in X \Rightarrow g^p = 1$ $\square$

21. <u>Theorem</u> (Sylows Theorem) Sei G endliche Gruppe, $p \in \mathbb{P}$ ein Teiler von $\#G$. Sei p^m die größte p-Potenz, die $\#G$ teilt. Sei $\mathrm{Syl}_p(G) = \{ P \leq G \mid \#P = p^m \}$. Dann gilt:

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

(2) G wirkt durch Konjugation transitiv auf $\mathrm{Syl}_p(G)$

(3) $\# \mathrm{Syl}_p(G) \equiv 1 \pmod p$

(4) jede p-Gruppe $H \leq G$ ist in einer <u>Sylow-p-Gruppe</u> $P \in \mathrm{Syl}_p(G)$ enthalten.

<u>Beweis</u> Sei $\Gamma = \{ H \leq G \mid H \text{ } p\text{-Gruppe} \}$ und $\Omega = \{ H \leq G \mid H \text{ maximale } p\text{-Gruppe} \}$. Nach Cauchys Theorem ist $\Omega \neq \emptyset \neq \Gamma$. Die Gruppe G operiert durch Konjugation auf Ω und Γ.

<u>Beh</u> Für jedes $H \in \Omega$ ist H der einzige Fixpunkt der H-Wirkung auf Ω.

<u>Beweis</u> Annahme, H fixiert $K \in \Omega$, d.h. $H \leq No_G(K)$. Es folgt: HK ist Untergruppe, $HK/K \cong H/H \cap K$ (Isom. Satz) $\Rightarrow HK \in \Gamma \Rightarrow HK = H$, weil H maximal $\Rightarrow HK = K$ weil K maximal. $\square$

Nach Lemma §2.19 wirkt G transitiv auf Ω und $\#\Omega \equiv 1 \pmod p$.

Es bleibt zu zeigen, dass $\mathrm{Syl}_p(G) = \Omega$, und "$\subseteq$" ist klar.

Angenommen, $H \in \Omega$, $\# H = p^n < p^m$. Der Stabilisator der G-Wirkung auf Ω von H ist $M = Nor_G(H)$. Es gilt $\# G/M = \# \Omega \equiv 1 \pmod p$, also $p^m \mid \# M \Rightarrow p \mid \# M/N$. Nach Cauchys Satz § 2.10 gibt es $g \in G$ mit $o(gH) = p$. Damit ist $L = \langle g \rangle H$ eine p-Gruppe mit $L \supsetneq H$ ↯ □

52½

22. <u>Lemma</u> Ist G nilpotent und $H \leq G$ eine Untergruppe mit $H \neq G$, so ist $Nor_G(H) \neq H$.

<u>Beweis</u> Induktion nach der Nilpotenzklasse r.

$r = 0, 1 \leadsto G$ abelsch, $Nor_G(H) = G$ (✓)

Sei jetzt $r \geq 2$, $H = Nor_G(H)$. Es folgt $Cen(G) \subseteq H$. Setze $H' = H/Cen(G) \leq G/Cen(G) = G'$

<u>Beh</u>: $Nor_{G'}(H') = Nor_G(H)/Cen(G) = H'$,

denn für $g \in G$, $h \in H$ gilt

$$g\, h\, Cen(G)\, g^{-1} \subseteq H\, Cen(G) = H$$

$$\Leftrightarrow g h g^{-1}\, Cen(G) \subseteq H\, Cen(G) = H$$

$$\Leftrightarrow g h g^{-1} \in H \leadsto \text{Beh}$$

Da G' kleinere Nilpotenzklasse hat, folgt $H' = G'$ und damit $H = G$ ↯ □

Addendum zu Sylows Theorem

(1) Mit den Bezeichnungen von §2.21 gilt

$$\# G = p^m \cdot s\,(kp+1)$$

$$kp+1 = \#\, Syl_p(G)$$

$$p^m \cdot s = \#\, Nor_G(P) \qquad P \in Syl_p(G) \text{ beliebig.}$$

Denn: $P \leq Nor_G(P) \Rightarrow \#\, Nor_G(P) = p^m \cdot s$

G transitiv auf $Syl_p(G)$, Stabilisator von P ist genau $Nor_G(P) \Rightarrow \# G = \underbrace{\# Nor_G(P)}_{p^m \cdot s} \cdot \underbrace{\# Syl_p(G)}_{kp+1}$

(2) Ist $P \in Syl_p(G)$ und $0 \leq l \leq m$, so gibt es $H \leq P$ mit $\# H = p^l$ (ÜA)

Korollar Jede endliche nilpotente Gruppe G ist direktes Produkt ihrer Sylow-Gruppen (für alle

Beweis Sei p ein Teiler von $\# G$, sei $P \in Syl_p(G)$. Sei $M = Nor_G(P)$ folgt $P \trianglelefteq Nor_G(P) = M$.

Wäre $M \neq G$, so $\tilde{M} = Nor_G(M) \neq M$. Da P charakteristisch in M ist ($Syl_p(M) = \{P\}$), gilt $P \trianglelefteq \tilde{M} \Rightarrow \tilde{M} \subseteq M$ ↯. Also $M = G$, d.h. $P \trianglelefteq G$.

Ist q Primzahl, $p \neq q$, q Teiler von G, so folgt genauso $Syl_q(G) = \{Q\}$. Damit $[P,Q] \subseteq P \cap G = \{1\}$. Sei $p_1 < p_2 < \dots < p_s$ die Primteiler von $\# G$, mit zugehörigen Sylow-p_i-Gruppen $P_i \trianglelefteq G$. Wir erhalten einen Homomorphismus

$$\varphi : P_1 \times \dots \times P_s \longrightarrow G$$
$$(g_1, \dots, g_s) \longmapsto g_1 \cdots g_s$$

Ist $g_i \neq 1$, so folgt $(g_1 \cdots g_s)^k = g_i^k \neq 1$ für $k = \frac{\# G}{\# P_i}$, also $\ker(\varphi) = \{1\}$. Da beide Gruppen gleich lang sind, ist φ Isomorphismus. $\square$

<u>Korollar</u> Jede endlich abelsche Gruppe A ist Produkt von endlichen abelschen p-Gruppen, für verschiedene Primzahlen p_i. Genauer: es gibt

$$p_1 < \ldots < p_s \ , \quad A = A_1 \oplus \ldots \oplus A_s$$

$$A_i \cong \mathbb{Z}/p_i^{l_1} \oplus \ldots \oplus \mathbb{Z}/p_i^{l_{s_i}} \qquad 1 \leq l_1 \leq l_2 \leq \ldots \leq l_{s_i}$$

Das ist eine andere Normalform als in §2.8.

<u>Bem</u> $Sym(3)$ ist überauflösbar:

$$Sym(3) \supsetneq Alt(3) \cong \mathbb{Z}/3 \supsetneq \{1\}$$

aber <u>nicht</u> nilpotent.

<u>Für endliche Gruppen:</u>

nilpotent $\Rightarrow$ überauflösbar $\Rightarrow$ auflösbar = polyzyklisch

$$\Uparrow \qquad\qquad\qquad \Uparrow$$

$$\not\Leftarrow Sym(3) \qquad\qquad \not\Leftarrow Alt(4)$$