# Vortrag 4 Filtrierungen und die Golod-Schafarewitsch'sche Ungleichung

Patrick Engels, Sebastian Throm

06.05.2010

## Teil 1

### Filtrierungen

Vorbemerkung: Die eingeklammerten Nummern beziehen sich auf die Nummerierung im Buch von Koch, ebenso wie die Nummern zitierter Sätze, die kursiv abgedruckt sind.

Sei $I^n(G)$ das von den $n$-ten Potenz des Ideals $I(G)$ erzeugte Ideal in $\mathbb{F}_p\,[[G]]$.

**Lemma 1.1 (7.9)**: Sei $G$ eine endliche $p$-Gruppe. Dann ist $I^n(G) = \{0\}$ für genügend großes $n$.

Beweis: Sei $n \in \mathbb{N}_0$ beliebig und

$$I^n(G) = A_0 \supseteq A_1 \supseteq \cdots \supseteq A_s = \{0\}$$

eine Kompositionsreihe von $I^n(G)$ als $G$-Modul.
Dann gilt $A_\nu/A_{\nu+1} \cong \mathbb{F}_p$, denn nach Lemma (4.13) enthält $A_\nu/A_{\nu+1}$ einen zu $\mathbb{F}_p$ isomorphen Untermodul und da $A_\nu/A_{\nu+1}$ einfach ist folgt $A_\nu/A_{\nu+1} \cong \mathbb{F}_p$.
Daher: $\forall g \in G$, $\forall a \in I^n(G)$

$$ga \equiv a \mod A_1$$

$\Longrightarrow (g-1)I^n(G) \subseteq A_1 \Longrightarrow I^{n+1}(G) \subseteq A_1 \Longrightarrow$ Beh.

*Lemma 4.13 Sei $A \neq 1$ eine endliche $p$-Gruppe, $G$ eine Untergruppe der Automorphismengruppe von $A$ der Ordnung $p$. Dann gilt $A^G \neq 1$.*

*Lemma 4.14 Sei $G$ eine pro-$p$-Gruppe und $H \neq \{1\}$ ein Normalteiler von $G$. Dann gibt es einen Normalteiler $H'$ von $G$ mit $H' \subset H$, $[H : H'] = p$.*

**Lemma 1.2 (7.10)** Sei $G$ eine endlich erzeugte pro-$p$-Gruppe. Dann gilt: $(\mathbb{F}_p\,[[G]] : I^n\,(G)) < \infty$, $\forall n \geq 1$.

Beweis: Seien $s_1, \cdots, s_m$ die Erzeugenden von $G$. Setze

$$x_i := s_i - 1,\ i = 1, \ldots, m,\ I = I\,(G)\,.$$

Beh: $I^n/I^{n+1} < \infty$
Bew:(durch Induktion)
I. $n = 1$. Setze

$$A_1 = \mathbb{F}_p x_1 + \ldots \mathbb{F}_p x_m.$$

$A_1 + I^2$ ist abgeschlossene Untergruppe von $I$. Da

$$gg' - 1 = (g-1)(g'-1) + g - 1 + g' - 1 \quad (*)$$

gilt $gg' - 1 \in A_1 + I^2$ falls $g - 1, g' - 1 \in A_1 + I^2$. Daher folgt $A_1 + I^2 = I$.
II. Sei $I^{n-1}/I^n < \infty$ für ein $n$ und $I^{n-1} = A_{n-1} + I^n$ eine Zerlegung abelscher Gruppen mit endlichem $A_{n-1}$. Dann ist $A_1 A_{n-1} + I^{n+1}$ abgeschlossene Untergruppe von $I^n$ und mit $*$ folgt:

$$I^n = \left\langle \left( (g-1) I^{n-1} \right) \right\rangle_{\mathbb{F}_p} = \left\langle (g-1) A_{n-1} + I^{n+1} \right\rangle_{\mathbb{F}_p} = A_1 A_{n-1} + I^{n+1}$$

($\langle x_i \rangle_{\mathbb{F}_p}$ ist der kleinste abgeschlossene Unterraum topologischer $\mathbb{F}_p$-Vektorräume der die $x_i$ enthält). Da $A_1 A_{n-1}$ endlich ist folgt $I^n/I^{n+1}$ ist endlich.

**Satz 1.3 (7.8)** Sei $G$ eine endlich erzeugte pro-$p$-Gruppe. Dann bildet $\{I^n(G) | n \in \mathbb{N}_0\}$ eine Umgebungsbasis der 0 in $\mathbb{F}_p[[G]]$.

Beweis: Nach Lemma 1.2 (7.10) sind die $I^n(G)$ offen. Weiter bildet $\{\ker \phi_U | U \in \mathfrak{U}_G\}$ für

$$\phi_U : \mathbb{F}_p[[G]] \longrightarrow \mathbb{F}_p[G/U], \ U \in \mathfrak{U}_G$$

ein volles Umgebungssystem von $0 \in \mathbb{F}_p[[G]]$. Es genügt daher zu zeigen, dass für jedes $U \in \mathfrak{U}_G$ ein $n$ existiert mit $I^n(G) \subseteq \ker \phi_U$.
Nach Lemma 1.1 (7.9) gibt es ein $n$ mit $I^n(G/U) = \{0\} \Longrightarrow I^n(G) \subseteq \ker \phi_U$.

*Satz 7.2 iii Sei $\varphi : G \longrightarrow G'$ ein Morphismus proendlicher Gruppen mit Kern $N$. Der Kern des induzierten Morphismus $\Lambda[[G]] \longrightarrow \Lambda[[G']]$ ist der Abschluss des Ideal $I(N) = \langle h - 1 | h \in N \rangle$*

Die Filtrierung $\{I^n(G) | n \in \mathbb{N}\}$ induziert eine Filtrierung $\{G_n | n \in \mathbb{N}\}$ von $G$, die sog. Zassenhaus-Filtrierung:

$$G_n = \{g | g - 1 \in I^n(G)\} \triangleleft G$$

**Satz 1.4 (7.11)** Sei $G$ eine endlich erzeugte pro-$p$-Gruppe. Dann ist $\{G_n | n \in \mathbb{N}\}$ ein volles Umgebungssystem von $1 \in G$ und $G_n/G_{n+1}$ liegt im Zentrum von $G/G_{n+1}$.

Beweis: Nach $*$ induziert die Zuordnung

$$g \longmapsto g - 1, \ g \in G$$

eine Injektion

$$G_n/G_{n+1} \longrightarrow I^n(G)/I^{n+1}(G).$$

$\Longrightarrow G_n$ ist offener Normalteiler von $G$ ($G_n \triangleleft G$ offen)
Ist $U \triangleleft G$ offen beliebig, dann gibt es ein $n$ mit $I^n(G) \subseteq \ker \phi_U \Longrightarrow G_n \subseteq U$. Zur zweiten Behauptung reicht es für $g \in G_n$ und $h \in G$ zu zeigen, dass $[g, h] = g^{-1}h^{-1}gh \in G_{n+1}$ gilt. $\Longleftrightarrow g^{-1}h^{-1}gh - 1 \in I^{n+1}(G)$ also $hg \equiv gh \mod I^{n+1}(G)$, was nach $*$ gilt.

**Satz 1.5 (7.12)** Sei $G$ eine pro-$p$-Gruppe und $g \in G_n$. Dann gilt $g^p \in G_{np}$ und $[g,h] \in G_{n+1}$ $\forall h \in G_n$.

Beweis: Die zweite Behauptung wurde gerade bewiesen. Die erste Behauptung folgt aus

$$g^p - 1 = (g-1)^p \in I^{np}(G).$$

Definition weiterer Filtrierungen:

Sei $G$ eine pro-$p$-Gruppe, $n \in \mathbb{N}$ und $q = p^n$ oder $q = 0$. Für $n = 1$ setze

$$G^{(1,q)} = G$$

und definiere induktiv für $n \geq 1$

$$G^{(n+1,q)} := \left(G^{(n,q)}\right)^q \left[G^{(n,q)}, G\right].$$

Per Definition ist $G^{(n,q)}$ ein Normalteiler von $G$ und $G^{(n,q)}/G^{(n+1,q)}$ liegt im Zentrum von $G/G^{(n+1,q)}$. Schreibe ferner $G^{(n)}$ statt $G^{(n,0)}$.

**Satz 1.6 (7.13)** Sei $G$ eine endlich erzeugte pro-$p$-Gruppe. Dann ist $\left\{G^{(n,q)} | n \in \mathbb{N}\right\}$ ein volles Umgebungssystem bei $1 \in G$.

Beweis: Beh: $\left(G : G^{(n,q)}\right) < \infty$
Bew (durch Induktion). $n = 1$ ist trivial
Sei $G/G^{(n,q)}$ endlich für ein $n$. Dann ist nach Beispiel 6.3 $G' = G^{(n,q)}$ endlich erzeugte pro-$p$-Gruppe. Ferner $G'^q [G', G'] \subseteq G^{(n+1,q)}$. Mit $G'/G'^q [G', G']$ ist auch $G^{(n,q)}/G^{(n+1,q)}$ endlich.
Wegen $G^{(n,q)} \subseteq G_n$ nach 7.12 und da $\{G_n | n \in \mathbb{N}\}$ volles Umgebungssystem bei $1 \in G$ ist folgt die Behauptung.

*Beipsiel 6.3: Sei $F$ eine endlich erzeugte freie Gruppe. Dann gilt $\chi(F) = 1 - d(F)$ und für eine Untergruppe $U$ von endlichem Index von $F$ gilt: $d(U) = (F : U)\{d(F) - 1\} + 1$.*
*Wobei $d(F) = \dim H^1(G)$ (als $\mathbb{F}_p$-Vektorraum) und $\chi(F) = \sum_{n=0}^{\infty} (-1)^n \dim H^n(G)$ gilt.*

Rechenregeln für Kommutatoren und Potenzen (im Gruppenring $\mathbb{Z}_p[[F]]$ für eine endlich erzeugte freie pro-$p$-Gruppe $F$)

Sei $C_q$ das von $q$ und $\{g - 1 | g \in G\}$ erzeugte Ideal in $\mathbb{Z}_p[[G]]$ und $C_q^n$ das von den $n$-ten Potenz von $C_q$ erzeugte Ideal.

Sei $g \in G^{(n,q)}$. Durch Induktion folgt $g - 1 \in C_q^n$ und die Abbildung

$$g \longrightarrow (g-1) + C_q^{n+1}, \; g \in G^{(n,q)}$$

ist ein Homomorphismus. Die induzierte Abbildung

$$\phi_q^n : G^{(n,q)}/G^{(n+1,q)} \longrightarrow C_q^n / C_q^{n+1}$$

ist ein $\mathbb{Z}_p$-Modulhomomorphismus.

**Satz 1.7 (7.14)** Sei $F$ eine endlich erzeugte freie pro-$p$-Gruppe, dann ist $\phi_q^n$ injektiv. Ferner gilt für $g \in F$: $g \in F^{(n,q)} \Longleftrightarrow g - 1 \in C_q^n$.

Beweis: Sei $q = 0$: Dann ist $\phi_q^n$ nach M. Hall Lemma 11.2.3 injektiv. Sei $h - 1 \in C_q^n$ $h \in G^{(s)} - G^{(s+1)}$. Angenommen $s < n \Longrightarrow \phi_q^s(hG^{(s+1)}) = 0$ Widerspruch zu $\phi_q^s$ injektiv.
Sei $q \neq 0$ und $h - 1 \in C_q^n$. Dann gibt es ein $i$ mit $1 \leq i < n$ so dass

$$h - 1 = q^{n-i}c_i + q^{n-i-1}c_{i+1} + \cdots + c_n,\ c_\nu \in C_0^\nu \text{ für } \nu = i, \ldots, n.$$

Daher gilt $h \in F^i$ und da $\phi_0^i$ ein Morphismus von $\mathbb{Z}_p$-Moduln ist, gibt es ein $h_i \in F^{(i)}$ sodass

$$h \equiv h_i^{q^{n-i}} \mod F^{(i+1)}$$

Dann kann $hh_1^{-q^{n-1}} - 1$ in der Form

$$hh_1^{-q^{n-1}} - 1 = q^{n-i-1}c'_{i+1} + \cdots + c'_n,\ c'_\nu \in C_0^\nu \text{ für } \nu = 1, \ldots, n,$$

geschrieben werden und damit folgt, dass $\phi_q^n$ injektiv ist.

**Satz 1.8 (7.15)** Sei $G$ eine pro-$p$-Gruppe. Für $a \in G^{(n,q)}$, $b \in G^{(m,q)}$ und $c \in G$ gilt:

- $[a, b] \in G^{(n+m,q)}$
- $[a, b^q] \equiv [a, b]^q \left[[a, b], b\right]^{\binom{q}{2}} \mod G^{(n+m+2,q)}$
- $[a, bc] \equiv [a, b]\,[a, c] \mod G^{(n+m+1,q)}$
- $(ac)^q \equiv a^q c^q \,[a, c]^{\binom{q}{2}} \mod G^{(n+2,q)}$

Beweis: Es genügt 1.7 für eine endlich erzeugte freie Gruppe $F$ zu zeigen. Daher kann Satz 1.6 (7.14) angewendet werden. Aus $x = a - 1 \in C_q^n$, $y = b - 1 \in C_q^m$ folgt

$$\begin{aligned}
[a, b] - 1 &= a^{-1}b^{-1}ab - 1 \\
&= (1 - x + x^2 \pm \cdots)(1 - y + y^2 \pm \cdots)(1 + x)(1 + y) - 1 \\
&\equiv 0 \mod C_q^{n+m}
\end{aligned}$$

und daher $[a, b] \in F^{(n+m+1,q)}$
Die restlichen Behauptungen folgen in ähnlicher Weise oder direkt aus

$$[a, bc] = [a, c]\,[a, b]\,\left[[a, b], c\right]$$

und der ersten Behauptung.

## Der Gruppenring einer freien pro-$p$-Gruppe

Betrachte für $I = \{1, \ldots, m\}$ die Algebra $\Lambda(I) = \mathbb{F}_p(m)$. Sei ferner $\{D^n | n \in \mathbb{N}\}$ das definierende Umgebungssystem von $0 \in \mathbb{F}_p(m)$ wobei $D^n$ das Ideal aller Potenzreihen aus $\mathbb{F}_p(m)$ ist, deren homogene Bestandteile mindestens Grad $n$ haben.

**Satz 1.9 (7.16)** Sei $F$ eine freie pro-$p$-Gruppe mit dem Erzeugendensystem $s_1, \ldots, s_m$. Die Zuordnung

$$x_i \longrightarrow s_i,\ i = 1, \ldots, m,$$

lässt sich zu einem Isomorphismus $\mathbb{F}_p(m) \cong \mathbb{F}_p[[F]]$ fortsetzten.

Beweis: Sei $P(x_1, \ldots, x_m)$ eine Potenzreihe aus $\mathbb{F}_p(m)$. Nach Satz 1.3 (7.8) ist $P(s_1 - 1, \ldots, s_m - 1)$ ein wohlbestimmtes Element in $\mathbb{F}_p[[F]]$. Die Zuordnung

$$\phi : P(x_1, \ldots, x_m) \longrightarrow P(s_1 - 1, \ldots, s_m - 1)$$

ist ein Morphismus von $\mathbb{F}_p(m)$ in $\mathbb{F}_p[[F]]$.
Andererseits kann die Zuordnung

$$s_i \longrightarrow 1 + x_i,\ s_i^{-1} \longmapsto \sum_{\nu=0}^{\infty} (-x_i)^{\nu}$$

zu einem Homomorphismus $\psi$ der freien Gruppe $F(m)$, die von $s_1, \ldots, s_m$ erzeugt wird, in die Einheitengruppe von $\mathbb{F}_p(m)$ fortgesetzt werden. Durch Induktion zeigt man, dass $F(m) \cap F_n$ auf $1 + D^n$ abgebildet wird. Nach Satz 1.3 (7.8) ist dann $\psi$ stetig. Daher gibt es eine stetige Forsetzung von $\psi$ auf $F$ und nach Satz (7.2 ii) auf $\mathbb{F}_p[[F]]$. Die so definierte Abbildung $\mathbb{F}_p[[F]] \longrightarrow \mathbb{F}_p(m)$ ist offenbar invers zu $\phi$ also ist $\phi$ ein Isomorphismus.

*Satz 7.2 ii Sei $A$ eine kompakte $\Lambda$-Algebra (wobei $\Lambda$ kompakter Ring ist). Jeder Morphismus $\varphi : G \longrightarrow A^{\times}$ von $G$ in die Einheitengruppe $A^{\times}$ von $A$ kann eindeutig zu einem Morphismus $\Lambda[[G]] \longrightarrow A$ fortgesetzt werden.*

Im Folgenden wird $\mathbb{F}_p(m)$ mit $\mathbb{F}_p[[F]]$ identifiziert.

**Satz 1.10 (7.17)** Sei $G$ eine endlich erzeugte pro-$p$-Gruppe mit der Darstellung

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

Sei $\{r_i | i \in I\}$ ein Relationensystem bezüglich dieser Darstellung. Dann wird der Kern der induzierten Abbildung $\mathbb{F}_p[[F]] \longrightarrow \mathbb{F}_p[[G]]$ als Ideal von $\mathbb{F}_p[[F]]$ erzeugt von $\{r_i - 1 | i \in I\}$

Beweis: Nach Satz (7.2 iii) ist der Kern von $\mathbb{F}_p[[F]] \longrightarrow \mathbb{F}_p[[G]]$ gleich $I(R)$ und $I(R)$ wird als Ideal von den Elementen $r_i - 1\ i \in I$ erzeugt.

*Satz 7.2 iii Sei $\varphi : G \longrightarrow G'$ ein Morphismus proendlicher Gruppen mit Kern $N$. Der Kern des induzierten Morphismus $\Lambda[[G]] \longrightarrow \Lambda[[G']]$ ist das abgeschlossene Ideal $I(N) = \langle h - 1 | h \in N \rangle$*

# Teil 2

## Der Satz von Golod-Shafarevich

**Definition 2.1 (7.18)** Sei $G$ eine pro-$p$-Gruppe mit endlich vielen Erzeugern und sei

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

eine Darstellung von $G$, wobei $F$ eine endlich erzeugte freie pro-$p$-Gruppe ist. Unter der Stufe von $r \in R$ versteht man die natürliche Zahl $m$ sodass $r \in F_m \backslash F_{m+1}$, wobei $\{F_n | n \in \mathbb{N}\}$ die Zassenhaus-Filtrierung ist.

**Lemma 2.2 (7.19)** Es gelten die Voraussetzungen von 2.1. Sei ferner $S$ ein Relationensystem von $G$ bezüglich obiger Darstllung. Sei $S$ die disjunkte Vereinigung endlicher Teilmengen $S_n$ die aus Relationen einer Stufe $\geq n$ bestehen. (Aufgrund der Voraussetzungen kann $S_n$ immer endlich gewählt werden.)

$$r_n = \#S_n,\ b_n = \dim I^n(G)/I^{n+1}(G),\ c_n = \sum_{\nu=0}^{n} b_\nu,\ r_0 = b_0 = c_0 = 1.$$

Dann gilt:

$$1 \leq -c_{n-1}d + \sum_{\nu=0}^{n} c_\nu r_{n-\nu}$$

für alle $n \geq 1$. $d$ sei der Erzeugendenrang von $F$, d.h. $d = \dim \mathrm{H}^1(F)$ als $\mathbb{F}_p$-Vektorraum.

Beweis: Sei $M = I(R)$, und $L$ der abgeschlossene $\mathbb{F}_p$-Vektorraum in $\mathbb{F}_p\left[[F]\right]$, der von den Elementen $r-1$ $r \in S$ erzeugt wird. Setze

$$M_n = I^n(F) \cap M,\ L_n = I^n(F) \cap L.$$

Im Folgenden werden Terme mittels der bekannten Isomorphiesätze sowie der Dimensionsformel umgeformt ohne dies jedes Mal zu erwähnen!
Dann gilt

$$\mathbb{F}_p\left[[G]\right] \cong \mathbb{F}_p\left[[F]\right]/M$$

und

$$\dim L/L_{n+1} \leq \sum_{\nu=1}^{n} r_\nu \tag{1}$$

Ferner sei $B_\nu$ der Modul der homogenen Polynome in $x_i = s_i - 1$, $i = 1, \ldots, d$ vom Grad $n$. Nach Satz 1.9 (7.16) gilt

$$I^n(F) = B_n \oplus I^{n+1}(F)$$

und

$$\dim B_n = d^n.$$

Für $n \in \mathbb{N}$ wähle Unterräume $C_n \subseteq B_n$ mit

$$I^n(F) \equiv M_n \oplus C_n \mod I^{n+1}(F)$$

und setze $C_0 = \mathbb{F}_p$. Da

$$\begin{aligned}
(\mathbb{F}_p[[F]]/I^n(F))/(MI^n(F)/I^n(F)) &\cong (\mathbb{F}_p[[F]]/M)/(MI^n(F)/M) \\
&\cong \mathbb{F}_p[[G]]/I^n(G)
\end{aligned}$$

und

$$MI^n(F)/I^n(F) \cong M/M_n$$

folgt

$$\dim \mathbb{F}_p[[F]]/I^n(F) = \dim M/M_n + \dim \mathbb{F}_p[[G]]/I^n(G). \tag{2}$$

Andererseits gilt

$$\dim I^n(F)/I^{n+1}(F) = \dim M_n/M_{n+1} + \dim C_n,$$

folglich

$$\dim \mathbb{F}_p[[F]]/I^{n+1}(F) = \dim M/M_{n+1} + \sum_{\nu=0}^{n} \dim C_\nu. \tag{3}$$

Aus (2)und (3) folgt

$$c_n = \sum_{\nu=0}^{n} \dim C_\nu,\ \ b_n = \dim C_n.$$

Sei $C$ der abgeschlossene $\mathbb{F}_p$-Vektorraum der von den $C_n$ $n \in \mathbb{N}$ erzeugt wird und $A = \mathbb{F}_p[[F]]$. Dann gilt

$$A \equiv M \oplus C \mod I^n(F),$$

folglich

$$A = M \oplus C.$$

Ferner gilt

$$\begin{aligned}
AL &= ML + CL \subseteq MAB_1 + CL = MB_1 + CL, \\
M &= ALA = ALAB_1 + AL = MB_1 + AL,
\end{aligned}$$

folglich

$$M \equiv MB_1 + CL \mod I^{n+1}(F).$$

Hieraus folgt

$$\begin{aligned}
\dim M/M_{n+1} \leq{} & \dim MB_1/MB_1 \cap I^{n+1}(F) \\
& + \dim CL/CL \cap I^{n+1}(F).
\end{aligned} \tag{4}$$

Die rechte Seite lässt sich umformen: Durch den durch

$$\bar{m} \otimes b \longmapsto \bar{mb},\ \ m \in M, b \in B_1$$

definierten Epimorphismus erhält man

$$\dim MB_1/MB_1 \cap I^{n+1}(F) \leq d \cdot \dim M/M_n, \tag{5}$$

und der Epimorphismus

$$\bigoplus_{\nu=1}^{n}(C_{n-\nu} \otimes_{\mathbb{F}_p} L/L_{\nu+1}) \longrightarrow CL/CL \cap I^{n+1}(F)$$

der durch

$$c \otimes \bar{l} \longmapsto \bar{cl},\ c \in C_{n-\nu}, l \in L$$

definiert ist impliziert

$$\dim CL/CL \cap I^{n+1}(F) \leq \sum_{\nu=1}^{n} b_{n-\nu} \dim L/L_{\nu+1} \tag{6}$$

Aus (1)-(6) folgt

$$\sum_{\nu=0}^{n} d^{\nu} - c_n \leq d \left( \sum_{\nu=0}^{n-1} d^{\nu} - c_{n-1} \right) + \sum_{\nu=1}^{n} b_{n-\nu} \left( \sum_{\mu=1}^{\nu} r_{\mu} \right)$$

Hieraus folgt zunächst:

$$\begin{aligned} 1 &\leq -dc_{n-1} + c_n + \sum_{\nu=1}^{n} b_{n-\nu} \left( \sum_{\mu=1}^{\nu} r_{\mu} \right) = -dc_{n-1} + c_n + \sum_{\nu=1}^{n} \sum_{\mu=1}^{n-\nu} b_{\mu} r_{\nu} \\ &= -dc_{n-1} + c_n + \sum_{\nu=1}^{n} c_{n-\nu} r_{\nu} = -dc_{n-1} + \sum_{\nu=0}^{n} c_{n-\nu} r_{\nu} \\ &= -dc_{n-1} + \sum_{\nu=0}^{n} c_{\nu} r_{n-\nu} \end{aligned}$$

also

$$1 \leq -dc_{n-1} + \sum_{\nu=0}^{n} c_{\nu} r_{n-\nu}$$

**Satz 2.3 (7.20)** Sei $G$ eine endliche $p$-Gruppe und seien $d, r_1, r_2, \ldots$ wie in Lemma 2.2 (7.19) definiert und angenommen die Reihe

$$\phi(t) = 1 + (r_1 - d)t + r_2 t^2 + \ldots$$

konvergiert für $0 < t < 1$. Dann gilt $\phi(t) > 0$ für $0 < t < 1$.

Bemerkung: Da der Relationenang $r(G) = \dim \mathrm{H}^2(G)$ endlich ist, kann man das Relationensystem so wählen, dass fast alle $r_n$ verschwinden.

Beweis: Nach Lemma 1.1 (7.9) gilt $b_n = 0$ für fast alle $n$. Daher ist die Reihe $\sum_{n=0}^{\infty} b_n t^n$ ein Polynom und die Reihe $\sum_{n=0}^{\infty} c_n t^n$ konvergiert für $0 < t < 1$. Daher kann man das Produkt umschreiben:

$$\left( \sum_{n=0}^{\infty} c_n t^n \right) \left( \sum_{n=0}^{\infty} r_n t^n \right) = \sum_{n=0}^{\infty} \left( \sum_{\nu=0}^{n} c_{\nu} r_{n-\nu} \right) t^n.$$

Nach Lemma 2.2 (7.19) gilt:

$$\sum_{\nu=0}^{n} c_\nu r_{n-\nu} \geq 1 + dc_{n-1} \text{ für alle } n \geq 1$$

Daher

$$\begin{aligned}
\left(\sum_{n=0}^{\infty} c_n t^n\right)\left(\sum_{n=0}^{\infty} r_n t^n\right) &= \sum_{n=0}^{\infty}\left(\sum_{\nu=0}^{n} c_\nu r_{n-\nu}\right) t^n \geq 1 + \sum_{n=1}^{\infty}(1+dc_{n-1})t^n \\
&= \sum_{n=0}^{\infty} t^n + \sum_{n=1}^{\infty} dc_{n-1}t^n = \frac{1}{1-t} + dt\sum_{n=0}^{\infty} c_n t^n
\end{aligned}$$

Damit folgt

$$\frac{1}{1-t} \leq \left(\sum_{n=0}^{\infty} c_n t^n\right)\left(\sum_{n=0}^{\infty} r_n t^n - dt\right)$$

für $0 < t < 1$ und nach Division durch $\sum_{n=0}^{\infty} c_n t^n$

$$0 < \sum_{n=0}^{\infty} r_n t^n - dt.$$

**Satz 2.4 (7.21)** Sei $G$ eine endliche $p$-Gruppe und

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1$$

eine minimale Darstellung von $G$ mit $R \subseteq F_m$ für ein $m$, wobei $\{F_n | n \in \mathbb{N}\}$ die Zassenhaus-Filtrierung von $F$ ist.
Dann stehen der Erzeugendenrang $d$ und der Relationenrang $r$ von $G$ über die Ungleichung

$$r > \frac{d^m}{m^m}(m-1)^{m-1}$$

in Beziehung.

Beweis: Im vorliegenden Fall hat $\phi(t)$ die Form

$$\phi(t) = 1 - dt + rt^m.$$

Angenommen $r \leq \frac{d^m}{m^m}(m-1)^{m-1}$. Dann gilt zunächst:

$$\begin{aligned}
r &\leq \frac{d^m}{m^m}(m-1)^{m-1} \\
\frac{1}{r} &\geq \frac{m^m}{d^m}\frac{1}{(m-1)^{m-1}} \\
-\left(\frac{1}{r}\right)^{m-1} &\leq -\frac{m}{d(m-1)}\left(\frac{m}{d}\right)^{1/(m-1)} \quad (**)
\end{aligned}$$

Setzt man nun $t = t_0 = (d/mr)^{1/(m-1)}$ in $\phi(t)$ ein folgt:

$$
\begin{aligned}
\phi(t_0) &= 1 - dt + rt^m = 1 - d\left(\frac{d}{mr}\right)^{1/(m-1)} + r\frac{d}{mr}\left(\frac{d}{mr}\right)^{1/(m-1)} \\
&= 1 - \left(\frac{1}{r}\right)^{1/(m-1)} d\left(\frac{d}{m}\right)^{1/(m-1)}\left(1-\frac{1}{m}\right) \\
&\underbrace{\leq}_{(**)} 1 - d\left(\frac{d}{m}\right)^{1/(m-1)}\left(1-\frac{1}{m}\right)\frac{m}{d(m-1)}\left(\frac{m}{d}\right)^{1/(m-1)} \\
&= 1 - \left(1-\frac{1}{m}\right)\frac{m}{m-1} = 1 - \frac{m}{m-1} + \frac{1}{m-1} = 0
\end{aligned}
$$

Also

$\phi(t_0) \leq 0$ im Widerspruch zu Satz 2.3 (7.20).

Quellen:

*H. Koch: Galois'sche Theorie der p-Erweiterungen, VEB Deutscher Verlag der Wissenschaften 1970*

*H. Koch: Galois Theory of p-extensions, Springer 2002*