

Die aufsteigende Zentralreihe in Einheitengruppen modularer Gruppenalgebren für Klassen metabelscher p -Gruppen

Dissertation
zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Christian-Albrechts-Universität zu Kiel

vorgelegt von
Mathias Theede

Kiel, 2016

Erster Gutachter:	Prof. Dr. Hartmut Laue
Zweiter Gutachter:	Prof. Dr. Jens Heber
Tag der mündlichen Prüfung:	01.06.2016
Zum Druck genehmigt:	01.06.2016

gez. Prof. Dr. Wolfgang J. Duschl, Dekan

Zusammenfassung

In der vorliegenden Arbeit beschäftigen wir uns im Fall eines Körpers K der Primzahlcharakteristik p und ausgewählter p -Gruppen G mit der Bestimmung der aufsteigenden Zentralreihe der Einheitengruppe $E(KG)$ von der modularen Gruppenalgebra KG .

Bezeichnen wir mit $\mathcal{J}(KG)$ das Radikal der Gruppenalgebra KG , so gilt $E(KG) \cong (1_G + \mathcal{J}(KG)) \times (K \setminus \{0_K\})$. Es ist $(1_G + \mathcal{J}(KG); \cdot)$ eine nilpotente Gruppe und es gilt $(1_G + \mathcal{J}(KG); \cdot) \cong (\mathcal{J}(KG); *)$ (wobei $a * b := a + b + ab$ für alle $a, b \in KG$).

Im Hinblick auf die aufsteigende Zentralreihe von $(\mathcal{J}(KG); *)$ untersuchen wir p -Gruppen G mit zyklischer Kommutatoruntergruppe $\gamma_2(G)$, wobei wir im Fall $p = 2$ zusätzlich $\gamma_3(G) \leq \gamma_2(G)^4$ voraussetzen. Darüber hinaus betrachten wir p -Gruppen, für die $\gamma_2(G) \cong C_p \times C_p$ gilt unter der Einschränkung, dass wir $p > 2$ und $C_G(\gamma_2(G))$ als abelsch im Fall $cl(G) = 3$ annehmen.

Nach einem Satz von Du [8] sind die in der aufsteigenden Zentralreihe von $(\mathcal{J}(KG); *)$ auftretenden Faktorgruppen K -Vektorräume. Für jeden dieser K -Vektorräume bestimmen wir dessen K -Dimension. Unser konstruktives Vorgehen liefert darüber hinaus Basen dieser Faktorräume. Es stellt sich heraus, dass sich bei den genannten Gruppentypen solche Basen durch eine Analyse der Restklassen bezüglich $\gamma_2(G)$ ermitteln lassen. Genauer zeigen wir, dass es für die Angabe von Basen (beziehungsweise der Dimensionen) ausreicht, in jeder Restklasse bezüglich $\gamma_2(G)$ ein Element einer Konjugiertenklasse minimaler Länge (beziehungsweise die Länge einer minimalen Konjugiertenklasse) sowie zusätzlich $\gamma_3(G)$ (beziehungsweise $|\gamma_3(G)|$) zu bestimmen.

Damit geben wir in dieser Arbeit im Fall $p > 2$ unter anderem ein Verfahren zur Bestimmung von Basen (und der Dimensionen) für die in der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ auftretenden Faktorräume für jede p -Gruppe G mit $|G| \leq p^4$ an.

Abstract

In this thesis we investigate the upper central series of unit groups $E(KG)$ of modular group algebras KG in the case of a field K of prime characteristic p and selected p -groups G .

Denoting $\mathcal{J}(KG)$ the radical of KG , we have $E(KG) \cong (1_G + \mathcal{J}(KG)) \times (K \setminus \{0_K\})$. $(1_G + \mathcal{J}(KG); \cdot)$ is a nilpotent group and $(1_G + \mathcal{J}(KG); \cdot) \cong (\mathcal{J}(KG); *)$ (where $a * b := a + b + ab$ for all $a, b \in KG$).

We investigate the upper central series of $(\mathcal{J}(KG); *)$ for p -groups G with a cyclic commutator subgroup $\gamma_2(G)$ under the condition that either p is odd or $p = 2$ and $\gamma_3(G) \leq \gamma_2(G)^4$. Moreover we consider p -groups for which the commutator subgroup is isomorphic to $C_p \times C_p$ under the restriction, that we assume $p > 2$ and $C_G(\gamma_2(G))$ to be abelian in the case of $cl(G) = 3$.

By applying a theorem of Du [8] every factor group in the upper central series of $(\mathcal{J}(KG); *)$ is a K -vector space. For each of these vector spaces we determine its K -dimension. In addition our constructive proceeding yields bases for these factor spaces. We show that we can determine bases (the dimensions respectively) for the factor spaces in the upper central series by analyzing the cosets with respect to $\gamma_2(G)$. We prove that for this determination it is sufficient to determine an element of a conjugacy class of minimal length for each coset in $G/\gamma_2(G)$ (the length of a minimal conjugacy class respectively) as well as $\gamma_3(G)$ (and $|\gamma_3(G)|$ respectively).

In particular for $p > 2$ this thesis provides a method to determine bases for the factor spaces in the upper central series of $\mathcal{J}(KG)$ for each p -group G with $|G| \leq p^4$.

Danksagung

Für die Betreuung dieser Arbeit, für die vielen Möglichkeiten meine Überlegungen vorzustellen und für die daraus resultierenden Anregungen möchte ich mich bei dem Betreuer meiner Promotion Herrn Prof. Dr. Hartmut Laue bedanken.

Weiter danke ich den Dozenten des Arbeitsbereichs Geometrie für die Bereitstellung einer Mitarbeiterstelle, die mir das Promotionsstudium sehr erleichtert hat.

Für die moralische Unterstützung beim Erstellen der Arbeit und die kritischen Anmerkungen bei deren Revision bedanke ich mich bei Jule, Dirk, Christina, Patrick, Nadja und Sven.

Mein besonderer Dank gilt meinen Eltern für ihre Unterstützung und das stete Vertrauen in mich.

Inhaltsverzeichnis

Einleitung	1
1 Grundlagen	5
1.1 Grundlegende Begriffe und Aussagen	5
1.2 Zahlentheoretische Hilfsmittel	14
1.3 Grundprinzip unserer Vorgehensweise	31
2 p-Gruppen mit zyklischer Kommutatoruntergruppe	33
2.1 Die Kommutatoruntergruppe und Konjugiertenklassen	33
2.2 Die aufsteigende Zentralreihe von $\mathcal{J}(KG)$	47
3 p-Gruppen mit p-elementar-abelscher Kommutatoruntergruppe	83
3.1 Nilpotenzklasse 2	83
3.2 Nilpotenzklasse 3	94
Symbolverzeichnis	111
Literaturverzeichnis	115

Einleitung

Das Radikal einer Gruppenalgebra KG über einem Körper K von Primzahlcharakteristik p und einer p -Gruppe G wurde bereits im Jahr 1941 von S. Jennings systematisch untersucht [13]. Hierbei wurde die Beschreibung des Radikals $\mathcal{J}(KG)$ als Augmentationsideal benutzt, um Basen für die Ideale $\mathcal{J}(KG)^n$ modulo $\mathcal{J}(KG)^{n+1}$ für alle $n \in \mathbb{N}$ zu bestimmen.

Die multiplikative Struktur des Radikals ist vor allem auch deshalb von Interesse, weil bekanntlich die Gruppe $(1_G + \mathcal{J}(KG)) \times (K \setminus \{0_K\})$ isomorph zur Einheitengruppe von KG ist. Deren Struktur zu studieren bedeutet daher im Wesentlichen, $(1_G + \mathcal{J}(KG); \cdot)$ beziehungsweise die dazu isomorphe Gruppe $(\mathcal{J}(KG); *)$ zu untersuchen, wobei $a * b := a + b + ab$ für alle $a, b \in KG$.

Eine erste Methode zur Bestimmung der Nilpotenzklasse der Einheitengruppe lieferten D. S. Coleman und D. S. Passman [6], die durch Immersion des Kranzproduktes $C_p \wr C_p$ in $(1_G + \mathcal{J}(KG); \cdot)$ zeigten, dass die Nilpotenzklasse von $(1_G + \mathcal{J}(KG); \cdot)$ im Fall einer nicht-abelschen p -Gruppe G mindestens p ist. Die Idee einer solchen Immersion griff A. Shalev 1990 in [20] und [21] auf. In diesen Artikeln weist er nach, dass die nächstgrößere auftretende Nilpotenzklasse $2p - 1$ ist und dass im Fall einer ungeraden Primzahl p und zyklischer Kommutatoruntergruppe G' von G die Nilpotenzklasse von $(1_G + \mathcal{J}(KG); \cdot)$ gleich $|G'|$ ist. Für eine allgemeine Theorie der Bestimmung der Nilpotenzklasse stellt sich die Vorgehensweise allerdings als unhandlich dar, sodass das Bedürfnis nach einem anderen Zugang entsteht.

Einen ersten Ansatz für eine alternative Vorgehensweise lieferte bereits S. Jennings in den 50er-Jahren des vergangenen Jahrhunderts. Er zeigte, dass in einem Radikal-Ring R folgender Zusammenhang zwischen dessen Lie- und dessen Gruppenstruktur besteht:

Satz (Jennings [12])

Sei R ein Radikal-Ring.

*$(R; *)$ ist genau dann als Gruppe nilpotent, falls R als Lie-Algebra nilpotent ist.*

Darüber hinaus vermutete er, dass im Falle der Nilpotenz die Nilpotenzklassen beider Strukturen übereinstimmen. Im Jahr 1992 gelang X. Du ein Beweis einer sogar wesentlich schärferen Aussage:

Satz (Du [8])

*Sei R ein Radikal-Ring und $(\mathcal{Z}_m(R))_{m \in \mathbb{N}_0}$ die aufsteigende Zentralreihe von $(R; *)$ und $(\mathcal{L}_m(R))_{m \in \mathbb{N}_0}$ die aufsteigende Zentralreihe von R als Lie-Algebra. Dann gilt*

$$\mathcal{L}_m(R) = \mathcal{Z}_m(R) \text{ für alle } m \in \mathbb{N}_0.$$

Insbesondere war damit auch die Vermutung von Jennings bewiesen.

Ferner gelang es Jennings in seiner Arbeit [13] aus dem Jahr 1941, die K -Dimensionen der Faktorräume $\mathcal{J}(KG)^n/\mathcal{J}(KG)^{n+1}$ mit Hilfe der Dimensionsuntergruppen zu beschreiben. A. K. Bhandari und I. B. S. Passi zeigten mit Hilfe der von Jennings entwickelten Theorie, dass über die oberen Lie-Dimensionsuntergruppen im Fall $p \geq 5$ ein unmittelbarer Zusammenhang mit der Nilpotenzklasse von $\mathcal{J}(KG)$ als Lie-Algebra gegeben ist.

Satz (Bhandari, Passi [2])

Sei $p \geq 5$, G eine p -Gruppe und K ein Körper mit $\text{char } K = p$. Sei $\mathcal{J}(KG)^{(1)} := \mathcal{J}(KG)$ und induktiv $\mathcal{J}(KG)^{(n)}$ das von $\{xy - yx \mid x \in \mathcal{J}(KG)^{(n-1)}, y \in \mathcal{J}(KG)\}$ erzeugte assoziative Ideal von KG für alle $n \in \mathbb{N}_{>1}$. Für alle $n \in \mathbb{N}$ sei $D_{(n)} := G \cap (1_G + \mathcal{J}(KG)^{(n)})$ und $d_{(n)} \in \mathbb{N}_0$ mit $p^{d_{(n)}} := |D_{(n)} : D_{(n+1)}|$. Dann gilt für $\mathcal{J}(KG)$ als Lie-Algebra:

$$cl(\mathcal{J}(KG)) = 1 + (p - 1) \sum_{n \in \mathbb{N}} n d_{(n+1)}.$$

Vermöge des Satzes von Du stellt diese Formel somit zugleich ein Mittel zur Berechnung der Nilpotenzklasse von Einheitengruppen modularer Gruppenalgebren dar. Der Satz führt damit die Bestimmung der Nilpotenzklasse auf die Problematik der Berechnung von $|D_{(n)} : D_{(n+1)}|$ für alle $n \in \mathbb{N}$ zurück. Dazu entwickelte Shalev in [19] Methoden, durch die er in Abhängigkeit vom Isomorphietyp von G' und der Klasse von G in einigen Fällen die Nilpotenzklasse des Radikals bestimmen konnte [22].

In dieser Arbeit ist es das Ziel, die aufsteigende Zentralreihe $(\mathcal{Z}_m)_{m \in \mathbb{N}_0}$ von $(\mathcal{J}(KG); *)$ für ausgewählte Klassen metabelscher p -Gruppen G mit Hilfe des Satzes von Du zu bestimmen. In erster Linie machen wir uns dabei die Vektorraum-Struktur der aufsteigenden (Lie-)Zentralreihe zu Nutze. Der Satz von Du ermöglicht es uns, das Problem der Bestimmung des $*$ -Inversen eines Elementes von $\mathcal{J}(KG)$ (1.1.3) und das Arbeiten mit aufwändigen $*$ -Kommutatoren zu umgehen.

Sei $d_m := \dim \mathcal{Z}_m/\mathcal{Z}_{m-1}$. Ist K endlich, $|K| = p^n$, so folgt aus einem Resultat von A. Bovdi und Z. Patay (1.12):

$$(\mathcal{Z}_m/\mathcal{Z}_{m-1}; *) \cong \underbrace{C_p \times \cdots \times C_p}_{nd_m}.$$

Wir bestimmen die Dimensionen d_m , indem sie zunächst nach unten abgeschätzt werden und sich anschließend ergibt, dass die Summe der Schranken gleich der Dimension von $\mathcal{J}(KG)$ ist. Folglich muss bei jeder getroffenen Abschätzung bereits Gleichheit gegolten haben. Eine hilfreiche und im sehr allgemeinen Rahmen gültige Reduktion bei der Bestimmung von \mathcal{Z}_m besteht in der Einsicht, dass es genügt, K -Linearkombinationen der Elemente fester Restklassen nach G' bezüglich ihrer Zugehörigkeit zu \mathcal{Z}_m zu untersuchen (1.14). Mit dieser Herangehensweise bestimmen wir für die von uns betrachteten Gruppenklassen die Dimensionen d_m , indem wir genauer Basen der Faktorräume $\mathcal{Z}_m/\mathcal{Z}_{m-1}$ ermitteln.

Zunächst betrachten wir p -Gruppen G mit zyklischer Kommutatoruntergruppe, wobei wir im Fall $p = 2$ zudem $[G', G]_{\mathfrak{S}} \leq G'^4$ fordern. Wir zeichnen gewisse Teilmengen $\tilde{\mathcal{D}}_H, \tilde{\mathcal{E}}_H$ von $\{1, 2, \dots, |G'|\}$ aus (1.32, 2.33), sodass für alle $m \in \mathbb{N}_{>1}$ gilt (Hauptsatz 2.37):

$$d_m = \left| \left\{ H \mid H \in G/G', m \in \tilde{\mathcal{E}}_H \right\} \right| + 2 \left| \left\{ H \mid H \in G/G', m \in \tilde{\mathcal{D}}_H \right\} \right|.$$

Gilt $m \leq |G'| - \frac{|G'|}{|[G', G]_{\mathfrak{S}}|}$ und $1 \not\equiv m \not\equiv 2$ modulo p , so liefert 2.37 genauer

$$d_m = |G/G'|.$$

Im Anschluss beschäftigen wir uns mit p -Gruppen mit p -elementar-abelscher Kommutatoruntergruppe und legen unser Hauptaugenmerk auf p -Gruppen mit $G' \cong C_p \times C_p$. Ist $cl(G) = 2$, $1 < m \leq 2p - 1$ und d die Anzahl der Konjugiertenklassen der Länge p , so weisen wir in Hauptsatz 3.11 nach:

$$d_m = \begin{cases} m \frac{|G| - |\mathcal{Z}(G)|}{|G'|} - \frac{d}{p} & \text{falls } m \leq p \\ (2p - m) \frac{|G| - |\mathcal{Z}(G)|}{|G'|} & \text{falls } m > p. \end{cases}$$

Die von Shalev auf ganz anderem Wege erhaltene Gleichung $cl(\mathcal{J}(KG)) = 2p - 1$ ist eine unmittelbare Folge [21]. Für $p > 3$ wurde in [22] gezeigt, dass diese nur unter den Voraussetzungen $G' \cong C_p \times C_p$ und $cl(G) = 2$ gilt.

Ist hingegen $cl(G) = 3$, so gelingt uns eine vollständige Klärung der aufsteigenden Zentralreihe nur in dem Fall, dass $p > 2$ und $C_G(G')$ abelsch ist. Die dabei auftretenden Dimensionen setzen sich hier bereits wesentlich unzugänglicher als im Fall $cl(G) = 2$ zusammen (Hauptsatz 3.22).

Zu den geklärten Fällen gehören insbesondere alle p -Gruppen G mit $|G| \leq p^4$. Die Diedergruppe, Semidiedergruppe und verallgemeinerte Quaternionengruppe der Ordnung 16 wurden bereits in [23] behandelt. Für $p > 2$ ergibt sich in der vorliegenden Arbeit unter anderem, dass für je zwei p -Gruppen der Ordnung p^4 , deren Kommutatoruntergruppen isomorph zu $C_p \times C_p$ sind, die Dimensionen der m -ten Zentralfaktoren für alle m übereinstimmen.

1 Grundlagen

In dieser Arbeit sei p stets eine Primzahl, $\mathbb{N} := \{1, 2, 3, \dots\}$ und für alle $M \subseteq \mathbb{N}$ sei $M_0 := M \cup \{0\}$. Ist $m \in \mathbb{N}$, so sei $\nu_p(m) := \max \{n \mid n \in \mathbb{N}_0, p^n \mid m\}$. Da wir in einem Kontext immer nur eine Primzahl betrachten, schreiben wir auch kurz ν anstatt ν_p . Außerdem verwenden wir folgende Notation:

Für alle $n \in \mathbb{N}_0$ sei $\underline{n} := \{m \mid m \in \mathbb{N}, 1 \leq m \leq n\}$. Insbesondere ist also $\underline{0} = \emptyset$ und $\underline{n} = \{0, 1, \dots, n\}$. Ist $n \in \mathbb{N}_0$ und K ein kommutativer unitärer Ring, so sei $n_K := \sum_{i=1}^n 1_K$. Besteht dabei in einem Kontext keinerlei Zweifel über K , so verzichten wir auf die Indizierung mit K .

1.1 Grundlegende Begriffe und Aussagen

In diesem einleitenden Abschnitt wollen wir eine kurze Einführung in die Thematik geben, dabei grundlegende Begriffe und Notationen klären und darüber hinaus wichtige Sätze vorstellen, die im Rahmen dieser Arbeit von Bedeutung sind. Des Weiteren stellen wir die Resultate aus [23] vor und geben in diesem Zusammenhang für das Auffinden der aufsteigenden Zentralreihe des Radikals einer Gruppenalgebra wichtige erste Einsichten an.

1.1 Definition. Sei K ein kommutativer unitärer Ring und A eine assoziative K -Algebra.

Wir definieren eine Verknüpfung $*$ auf A , indem wir für alle $a, b \in A$ setzen:

$$a * b := a + b + ab$$

1.1.1 Bemerkung. $(A; *)$ ist ein Monoid mit neutralem Element 0_A . □

Mit $Q(A)$ bezeichnen wir die Einheitengruppe von $(A; *)$. Ist A unitär, so bezeichnen wir mit $E(A)$ die Einheitengruppe von $(A; \cdot)$.

1.1.2 Bemerkung.

Ist A unitär, so ist $\beta: (A; *) \rightarrow (A; \cdot)$, $a \mapsto 1_A + a$ ein Monoid-Isomorphismus.

Insbesondere gilt $(Q(A); *) \cong (E(A); \cdot)$. □

Ist $a \in Q(A)$, so bezeichnen wir mit a^- das bezüglich $*$ inverse Element zu a .

Ist $n \in \mathbb{N}_0$, so sei $a^{(n)} := \underbrace{a * \dots * a}_n$ für alle $a \in A$.

1 Grundlagen

1.1.3 Bemerkung. Für alle $n \in \mathbb{N}_0$, $a \in A$ gilt:

$$(i) \quad a^{(n)} = \sum_{i=1}^n \binom{n}{i} a^i.$$

$$(ii) \quad \text{Gilt } \text{char } K = p, \text{ so gilt } a^{(p^n)} = a^{p^n}.$$

$$(iii) \quad \text{Ist } a^{n+1} = 0_A, \text{ so gilt } a \in Q(A) \text{ und } a^- = \sum_{i=1}^n (-a)^i.$$

Beweis. Ein Induktionsbeweis nach n liefert die ersten beiden Aussagen. Ist $a \in A$ mit $a^{n+1} = 0_A$, so folgt der dritte Teil aus

$$a * \sum_{i=1}^n (-a)^i = a + \sum_{i=1}^n (-a)^i - \sum_{i=1}^n (-a)^{i+1} = 0_A$$

sowie der (multiplikativen) Vertauschbarkeit von $\sum_{i=1}^n (-a)^i$ und a . □

1.1.4 Bemerkung. Sei $A \neq \{0_A\}$. Weiter existiere eine endliche K -Basis \mathfrak{B} von A . Dann ist die Abbildung

$$\alpha_{\mathfrak{B}}: A \rightarrow K, \quad \sum_{b \in \mathfrak{B}} c_b b \mapsto \sum_{b \in \mathfrak{B}} c_b \quad (\text{mit } c_b \in K \text{ für alle } b \in \mathfrak{B})$$

ein K -Raum-Epimorphismus.

Insbesondere gilt $A/\text{Kern } \alpha_{\mathfrak{B}} \cong K$ (K -Raum-Isomorphie).

Gilt zusätzlich $\mathfrak{B} \cdot \mathfrak{B} \subseteq \mathfrak{B}$, so ist $\alpha_{\mathfrak{B}}$ ein K -Algebren-Epimorphismus. □

Wir setzen $\text{Aug}_{\mathfrak{B}}(A) := \text{Kern } \alpha_{\mathfrak{B}}$ und spezialisieren Bemerkung 1.1.4 zu folgender Definition im Fall von Gruppenalgebren:

1.2 Definition. Sei K ein kommutativer unitärer Ring, G eine endliche Gruppe und $T \subseteq G$. Wir bezeichnen mit KG die Gruppenalgebra von G über K und setzen

$$\text{Aug}(KG) := \text{Aug}_G(KG) \quad \text{und} \quad \text{Aug}(KT) := \text{Aug}(KG) \cap \langle T \rangle_K.$$

Da in dieser Arbeit in einem Kontext stets nur ein einziger Körper K betrachtet wird, schreiben wir auch kurz $\text{Aug}(T)$ statt $\text{Aug}(KT)$.

1.2.1 Bemerkung. Sei $T \subseteq G$, $T \neq \emptyset$ und $t \in T$. Dann ist

$$\{g - t \mid g \in T \setminus \{t\}\}$$

eine K -Basis von $\text{Aug}(T)$.

Insbesondere ist $\{g - 1_G \mid g \in G \setminus \{1_G\}\}$ eine K -Basis von $\text{Aug}(KG)$. □

Ist K ein kommutativer unitärer Ring und A eine assoziative K -Algebra, so bezeichnen wir mit $\mathcal{J}(A)$ das Jacobson-Radikal von A . Folgender wichtiger Zusammenhang besteht zwischen der in Definition 1.1 eingeführten Verknüpfung auf A und dem Jacobson-Radikal $\mathcal{J}(A)$ [24, Kapitel 13, § 97.]:

$\mathcal{J}(A)$ ist das größte Ideal von A , das bezüglich $*$ eine Gruppe ist.

Im Fall von p -Gruppen und Körpern K mit $\text{char } K = p$ erhalten wir folgende, wohlbekannte Beschreibung des Jacobson-Radikals der zugehörigen Gruppenalgebra (siehe zum Beispiel [13], [25]):

1.3 Satz. *Sei G eine p -Gruppe und K ein Körper mit $\text{char } K = p$. Dann gilt*

$$\mathcal{J}(KG) = \text{Aug}(KG).$$

□

1.3.1 Bemerkung. *Es gilt*

$$(i) \quad (1_G + \mathcal{J}(KG); \cdot) \times (K \setminus \{0_K\}; \cdot) \cong (E(KG); \cdot) \quad \text{und}$$

$$(ii) \quad (\mathcal{J}(KG); *) \times (K \setminus \{-1_K\}; *) \cong (Q(KG); *).$$

Wir geben den kurzen auch in [23] dargelegten Beweis dieser bekannten Aussage an:

Beweis. Sei $x \in E(KG)$, $\lambda_g \in K$ für alle $g \in G$ mit $x = \sum_{g \in G} \lambda_g g$. Wir setzen $\sigma := \sum_{g \in G} \lambda_g$.

Dann gilt $\sigma \neq 0_K$, $\sigma^{-1}x - 1_G \in \mathcal{J}(KG)$ und es folgt

$$x = ((\sigma^{-1}x - 1_G) + 1_G)(\sigma \cdot 1_G) \in (\mathcal{J}(KG) + 1_G) \cdot ((K \setminus \{0_K\}) \cdot 1_G)$$

und damit $E(KG) \subseteq (1_G + \mathcal{J}(KG)) \cdot ((K \setminus \{0_K\}) \cdot 1_G)$. Da $(\mathcal{J}(KG); *)$ eine Gruppe ist, ist $1_G + \mathcal{J}(KG)$ nach Bemerkung 1.1.2 eine Untergruppe von $E(KG)$. Aus $(K \setminus \{0_K\}) \cdot 1_G \subseteq \mathcal{Z}(E(KG))$ folgt zum einen $(K \setminus \{0_K\}) \cdot 1_G \trianglelefteq E(KG)$ und damit die andere Inklusion, andererseits wegen $(1_G + \mathcal{J}(KG)) \cdot ((K \setminus \{0_K\}) \cdot 1_G) = E(KG)$ auch $(1_G + \mathcal{J}(KG)) \trianglelefteq E(KG)$. Außerdem gilt $(1_G + \mathcal{J}(KG)) \cap ((K \setminus \{0_K\}) \cdot 1_G) = \{1_G\}$, da jedes Element in $(1_G + \mathcal{J}(KG))$, als Linearkombination der Elemente aus G dargestellt, die Koeffizientensumme 1_K hat. Damit folgt der erste Teil der Behauptung.

Der zweite Teil folgt dann direkt aus Bemerkung 1.1.2. □

Für eine Analyse der Struktur von $(E(KG); \cdot)$ ist es daher von großem Interesse die Struktur der Gruppe $(1_G + \mathcal{J}(KG); \cdot)$ (beziehungsweise von $(\mathcal{J}(KG); *)$) zu verstehen. Ist G eine abelsche p -Gruppe und K ein endlicher Körper mit $\text{char } K = p$, so ist die Struktur von $(\mathcal{J}(KG); *)$ in [1], [18] und [25] untersucht und geklärt worden. Die Resultate der Untersuchungen in jenem Fall lassen bereits vermuten, dass für eine beliebige p -Gruppe G die Struktur von $(\mathcal{J}(KG); *)$ sehr komplex sein kann.

1 Grundlagen

Trivial ist hingegen die Feststellung, dass für jede assoziative K -Algebra A

$$(\mathcal{Z}(A); \cdot) = (\mathcal{Z}(A); *)$$

gilt, weshalb wir im Folgenden kurz $\mathcal{Z}(A)$ schreiben werden. Für das Zentrum einer Gruppenalgebra und deren Augmentationsideal sind K -Basen hinlänglich bekannt (siehe zum Beispiel [17, Chapter 4, Lemma 1.1.]). Um diese anzugeben, führen wir noch eine weitere Notation ein:

Ist G eine Gruppe, so bezeichnen wir mit $\mathcal{K}(G)$ die Menge der Konjugiertenklassen von G .

1.4 Satz. *Sei G eine endliche Gruppe und K ein kommutativer unitärer Ring.*

(i) $\left\{ \sum_{c \in C} c \mid C \in \mathcal{K}(G) \right\}$ ist eine K -Basis von $\mathcal{Z}(KG)$.

(ii) Es gilt $\mathcal{Z}(KG) + \text{Aug}(KG) = KG$ und $\mathcal{Z}(KG) \cap \text{Aug}(KG) = \mathcal{Z}(\text{Aug}(KG))$.

$$\mathfrak{B} := \{g - 1_G \mid g \in \mathcal{Z}(G) \setminus \{1_G\}\} \cup \left\{ \sum_{c \in C} c - |C| 1_G \mid C \in \mathcal{K}(G), |C| \neq 1 \right\}$$

ist eine K -Basis von $\mathcal{Z}(\text{Aug}(KG))$.

□

Da $p \mid |C|$ für alle $C \in \mathcal{K}(G)$ mit $|C| \neq 1$ in p -Gruppen G gilt, erhalten wir speziell:

1.5 Satz. *Sei G eine p -Gruppe und K ein Körper mit $\text{char } K = p$. Dann ist*

$$\mathfrak{B} := \{g - 1_G \mid g \in \mathcal{Z}(G) \setminus \{1_G\}\} \cup \left\{ \sum_{c \in C} c \mid C \in \mathcal{K}(G), |C| \neq 1 \right\}$$

eine K -Basis von $\mathcal{Z}(\mathcal{J}(KG))$ und $\dim \mathcal{Z}(\mathcal{J}(KG)) = \dim \mathcal{Z}(KG) - 1 = |\mathcal{K}(G)| - 1$.

□

Aufgrund ihrer besonderen Bedeutung in dieser Arbeit erinnern wir noch kurz an die Definition der Kommutatorbildung in Gruppen und assoziativen Algebren sowie an die Definition aufsteigender und absteigender Zentralreihen:

1.6 Definition. *Sei G eine Gruppe und R ein Ring. Für alle $g, h \in G$ und $a, b \in R$ setzen wir*

$$[g, h]_{\mathfrak{G}} := g^{-1} h^{-1} g h \quad \text{und} \quad [a, b]_{\mathfrak{L}} := ab - ba,$$

das heißt $[g, h]_{\mathfrak{G}}$ ist der (Gruppen-)Kommutator von g und h und $[a, b]_{\mathfrak{L}}$ der (Lie-)Kommutator von a und b . Für alle $n \in \mathbb{N}_{\geq 3}$, $a_1, \dots, a_n \in R$ und $g_1, \dots, g_n \in G$ setzen wir weiter induktiv:

$$[a_1, \dots, a_n]_{\mathfrak{L}} := [[a_1, \dots, a_{n-1}]_{\mathfrak{L}}, a_n]_{\mathfrak{L}} \quad \text{und} \quad [g_1, \dots, g_n]_{\mathfrak{G}} := [[g_1, \dots, g_{n-1}]_{\mathfrak{G}}, g_n]_{\mathfrak{G}}.$$

1.7 Definition. Sei G eine Gruppe und R ein Ring.

Wir setzen $\gamma_1(G) := G$, $\gamma_2(G) := G' = [G, G]_{\mathfrak{G}}$ und induktiv $\gamma_j(G) := [\gamma_{j-1}(G), G]_{\mathfrak{G}}$ für alle $j \in \mathbb{N}_{>2}$. Dann heißt $(\gamma_j(G))_{j \in \mathbb{N}}$ die absteigende Zentralreihe von G .

Wir setzen weiter $\mathcal{Z}_j(G) := \{1_G\}$ für alle $j \in \mathbb{Z}_{\leq 0}$ und induktiv $\mathcal{Z}_j(G)$ für jedes $j \in \mathbb{N}$ als den Normalteiler von G mit $\mathcal{Z}_j(G)/\mathcal{Z}_{j-1}(G) = \mathcal{Z}(G/\mathcal{Z}_{j-1}(G))$. Die Folge $(\mathcal{Z}_j(G))_{j \in \mathbb{N}_0}$ heißt die aufsteigende Zentralreihe von G .

Außerdem sei $\mathcal{L}_j(R) := \{0_R\}$ für alle $j \in \mathbb{Z}_{\leq 0}$ und induktiv sei

$$\mathcal{L}_j(R) := \{a \mid a \in R, \forall b \in R : [a, b]_{\mathfrak{L}} \in \mathcal{L}_{j-1}(R)\}$$

für jedes $j \in \mathbb{N}$. Die Folge $(\mathcal{L}_j(R))_{j \in \mathbb{N}_0}$ heißt die aufsteigende Zentralreihe von (der zu R gehörigen Lie-Algebra) $(R; +; [\cdot, \cdot]_{\mathfrak{L}})$.

Wir geben nun den Satz an, der die gesamte Arbeit motiviert [8].

1.8 Satz, Du (1992). ¹ Sei A eine Radikal-Algebra², $(\mathcal{Z}_j(A))_{j \in \mathbb{N}_0}$ die aufsteigende Zentralreihe von $(A; *)$ und $(\mathcal{L}_j(A))_{j \in \mathbb{N}_0}$ die aufsteigende Zentralreihe von $(A; +; [\cdot, \cdot]_{\mathfrak{L}})$. Dann gilt

$$\mathcal{L}_j(A) = \mathcal{Z}_j(A) \text{ für alle } j \in \mathbb{N}_0.$$

Insbesondere gilt:

$$(A; *) \text{ ist genau dann nilpotent, wenn } (A; +; [\cdot, \cdot]_{\mathfrak{L}}) \text{ nilpotent ist.}$$

Im Falle der Nilpotenz gilt dann $cl(A; *) = cl(A; +; [\cdot, \cdot]_{\mathfrak{L}})$. □

Für die absteigenden Zentralreihen von $(A; *)$ und $(A; +; [\cdot, \cdot]_{\mathfrak{L}})$ gilt ein entsprechendes Resultat nicht, wie wir sogleich aufzeigen werden. Im Fall von p -Gruppen G und Körpern K mit $\text{char } K = p$ ist nämlich das erste Glied der absteigenden Zentralreihe von $(\mathcal{J}(KG); +; [\cdot, \cdot]_{\mathfrak{L}})$ bekannt und lässt sich wie folgt beschreiben (siehe zum Beispiel [14, Chapter II, 2.2.]):

1.9 Satz. Sei G eine p -Gruppe und K ein Körper mit $\text{char } K = p$. Dann gilt

$$[\mathcal{J}(KG), \mathcal{J}(KG)]_{\mathfrak{L}} = \left\{ \sum_{g \in G} c_g g \mid \sum_{g \in C} c_g = 0_K \text{ für alle } C \in \mathcal{K}(G) \right\}.$$

□

Ist nun G eine nicht-abelsche p -Gruppe, so existiert $g \in \mathcal{Z}_2(G) \setminus \mathcal{Z}(G)$ und $h \in G$ mit $[g, h]_{\mathfrak{G}} \in \mathcal{Z}(G) \setminus \{1_G\}$ und es folgt

$$(g - 1_G)^- * (h - 1_G)^- * (g - 1_G) * (h - 1_G) \stackrel{1.1.2}{=} [g, h]_{\mathfrak{G}} - 1_G \notin [\mathcal{J}(KG), \mathcal{J}(KG)]_{\mathfrak{L}}.$$

¹H. Laue hat 2015 einen vereinfachten Beweis dieser Aussage erbracht [16].

²Eine assoziative Algebra A bezeichnet man als Radikal-Algebra, falls $\mathcal{Q}(A) = A$ gilt.

1 Grundlagen

Der folgende Satz von Bovdi [3] liefert das entscheidende Argument, warum im Fall eines endlichen Körpers K die Dimensionen der einzelnen Faktorräume in der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ die $*$ -Struktur der Faktorgruppen in der aufsteigenden Zentralreihe klärt. Für den mit Hilfe des Satzes von Du kurzen Beweis von Bovdi (siehe auch [25]) geben wir noch folgendes Lemma an:

1.10 Lemma. *Seien K ein kommutativer unitärer Ring, A eine assoziative K -Algebra, $n \in \mathbb{N}$ und $a, b \in A$. Dann gilt*

$$[a, \underbrace{b, \dots, b}_n]_{\mathfrak{L}} = \sum_{i=0}^n \binom{n}{i} (-1)^i b^i a b^{n-i}.$$

Ist $\text{char } K = p$, so gilt insbesondere $[a, \underbrace{b, \dots, b}_p]_{\mathfrak{L}} = [a, b^p]_{\mathfrak{L}}$.

Beweis. Ein Induktionsbeweis nach n liefert die Behauptung. □

1.11 Satz, Bovdi. *Sei K ein Körper mit $\text{char } K = p$, A eine K -Radikal-Algebra und $(\mathcal{Z}_j(A))_{j \in \mathbb{N}_0}$ die aufsteigende Zentralreihe von $(A; *)$, $m \in \mathbb{N}$ und $x \in \mathcal{Z}_m(A)$. Dann gilt*

$$x^{(p)} \in \mathcal{Z}_{\max\{1, m-p+1\}}(A).$$

Beweis. Es gilt $x^{(p)} = x^p$ nach Bemerkung 1.1.3 (ii). Sei $y \in A$. Aus Satz 1.8 folgt

$$[y, x^p]_{\mathfrak{L}} \stackrel{1.10}{=} [y, \underbrace{x, \dots, x}_p]_{\mathfrak{L}} \in \mathcal{Z}_{m-p}(A).$$

Wir erhalten also $x^{(p)} \in \mathcal{Z}_{m-p+1}(A)$ falls $m \geq p$, andernfalls gilt zumindest $x^{(p)} \in \mathcal{Z}(A)$. □

1.12 Korollar, Bovdi. *Sei K ein Körper mit $\text{char } K = p$, A eine nilpotente K -Radikal-Algebra, $(\mathcal{Z}_j(A))_{j \in \mathbb{N}_0}$ die aufsteigende Zentralreihe von $(A; *)$, $n := \text{cl}(A; *)$ und $m \in \underline{n} \setminus \{1\}$. Dann gilt*

$${}^3\text{exp}(\mathcal{Z}_m(A)/\mathcal{Z}_{m-1}(A)) = p.$$

Beweis. Dies folgt unmittelbar aus Satz 1.11. □

Die Frage nach dem Exponenten von $\mathcal{Z}(A)$ ist hingegen schwieriger zu beantworten. Eine detaillierte Analyse darüber im Falle $A = \mathcal{J}(KG)$ für eine p -Gruppe G und einen Körper K mit $\text{char } K = p$ findet sich in [25].

Das folgende Lemma und der anschließende Satz vermitteln einen ersten Eindruck einer Strategie zur Bestimmung der aufsteigenden Zentralreihe von $(\mathcal{J}(KG); +; [\cdot, \cdot]_{\mathfrak{L}})$.

³Ist G eine endliche Gruppe, so sei $\text{exp}(G) := \text{kgV}\{o(g) \mid g \in G\}$.

1.13 Lemma. Seien G eine endliche Gruppe, K ein kommutativer unitärer Ring, $m \in \mathbb{N}$ und $g, g_1, \dots, g_m \in G$. Dann gilt

$$[g, g_1, \dots, g_m]_{\mathfrak{L}} \in \text{Aug}(gg_1 \cdots g_m \gamma_2(G)).$$

Beweis. Ist $m = 1$, so folgt $[g, g_1]_{\mathfrak{L}} = g_1 g([g, g_1]_{\mathfrak{G}} - 1_G) \in \text{Aug}(gg_1 \gamma_2(G))$, da $G/\gamma_2(G)$ abelsch ist. Ist $m > 1$, so ist induktiv $x := [g, g_1, \dots, g_{m-1}]_{\mathfrak{L}} \in \text{Aug}(gg_1 \cdots g_{m-1} \gamma_2(G))$. Da x K -Linearkombination von Elementen aus $gg_1 \cdots g_{m-1} \gamma_2(G)$ ist, reicht es für alle $y \in gg_1 \cdots g_{m-1} \gamma_2(G)$ zu zeigen, dass $[y, g_m]_{\mathfrak{L}} \in \text{Aug}(gg_1 \cdots g_m \gamma_2(G))$ gilt. Dies folgt aber wie beim Induktionsanfang aus der Kommutativität von $G/\gamma_2(G)$. \square

1.14 Satz. Seien G eine endliche Gruppe, K ein kommutativer unitärer Ring, $n \in \mathbb{N}$, H_1, \dots, H_n paarweise verschiedene Restklassen bezüglich $\gamma_2(G)$ und $m \in \mathbb{N}$. Für alle $i \in \underline{n}$ sei $a_i \in \text{Aug}(H_i \cup \mathfrak{Z}(G))$.

(i) Gilt $a_i \in \text{Aug}(H_i)$ für alle $i \in \underline{n}$ und $\sum_{i=1}^n a_i = 0_{KG}$, so gilt bereits $a_i = 0_{KG}$ für alle $i \in \underline{n}$.

(ii) Gilt $\sum_{i=1}^n a_i \in \mathcal{L}_m(\text{Aug}(KG))$, so gilt schon $a_i \in \mathcal{L}_m(\text{Aug}(KG))$ für alle $i \in \underline{n}$.

Beweis. (i) folgt direkt aus

$$\text{Aug}(H_1) + \dots + \text{Aug}(H_n) = \text{Aug}(H_1) \oplus \dots \oplus \text{Aug}(H_n).$$

(ii): Die Aussage (i) stellt den Induktionsanfang der folgenden als Induktionsvoraussetzung über $m - 1$ formulierten Aussage (*) dar:

Sind $\tilde{H}_1, \dots, \tilde{H}_n$ paarweise verschiedene Restklassen bezüglich $\gamma_2(G)$, $b_i \in \text{Aug}(\tilde{H}_i)$

für alle $i \in \underline{n}$ und gilt $\sum_{i=1}^n b_i \in \mathcal{L}_{m-1}(\text{Aug}(KG))$, so gilt bereits $b_i \in \mathcal{L}_{m-1}(\text{Aug}(KG))$

für alle $i \in \underline{n}$.

Da für alle $g \in G$ nach Voraussetzung auch gH_1, \dots, gH_n paarweise verschieden sind und $\{g - 1_G \mid g \in G \setminus \{1_G\}\}$ eine K -Basis von $\text{Aug}(KG)$ ist, folgt:

$$\begin{aligned} \sum_{i=1}^n a_i \in \mathcal{L}_m(\text{Aug}(KG)) &\iff \forall g \in G : \left[\sum_{i=1}^n a_i, g - 1_G \right]_{\mathfrak{L}} \in \mathcal{L}_{m-1}(\text{Aug}(KG)). \\ &\iff \forall g \in G : \sum_{i=1}^n \underbrace{[a_i, g]_{\mathfrak{L}}}_{\in \text{Aug}(gH_i) \text{ nach 1.13}} \in \mathcal{L}_{m-1}(\text{Aug}(KG)). \\ &\stackrel{(*)}{\iff} \forall g \in G \forall i \in \underline{n} : [a_i, g]_{\mathfrak{L}} \in \mathcal{L}_{m-1}(\text{Aug}(KG)). \\ &\iff \forall g \in G \forall i \in \underline{n} : [a_i, g - 1_G]_{\mathfrak{L}} \in \mathcal{L}_{m-1}(\text{Aug}(KG)). \\ &\iff \forall i \in \underline{n} : a_i \in \mathcal{L}_m(\text{Aug}(KG)). \end{aligned}$$

\square

Eine unmittelbare Konsequenz ist die folgende, wichtige Bemerkung.

1.14.1 Bemerkung. Sei $A_i \subseteq \text{Aug}(H_i \cup \mathcal{Z}(G))$ und A_i modulo $\mathcal{L}_m(\text{Aug}(KG))$ K -linear unabhängig für alle $i \in \underline{n}$. Dann ist

$$\bigcup_{i \in \underline{n}} A_i \text{ modulo } \mathcal{L}_m(\text{Aug}(KG))$$

K -linear unabhängig.

Ist K ein Körper und gilt zusätzlich $A_i \subseteq \mathcal{L}_{m+1}(\text{Aug}(KG))$ für alle $i \in \underline{n}$, so folgt insbesondere

$$\dim(\mathcal{L}_{m+1}(\text{Aug}(KG))/\mathcal{L}_m(\text{Aug}(KG))) \geq \sum_{i=1}^n |A_i|.$$

□

Zum Auffinden der aufsteigenden Zentralreihe liegt es daher nahe, die Teilräume $\text{Aug}(H)$ für Restklassen H bezüglich $\gamma_2(G)$ zu untersuchen. Ein solches Vorgehen ist bereits in [23] verfolgt worden und führte zu folgenden beiden Hauptresultaten:

1.15 Satz. Sei G eine p -Gruppe mit $|\gamma_2(G)| = p$, $a \in G$ mit $\gamma_2(G) = \langle a \rangle$, K ein Körper mit $\text{char } K = p$ und Y ein Repräsentantensystem der nichtzentralen Konjugiertenklassen von G . Sei weiter $\bar{}$ jeweils der kanonische K -Vektorraum-Epimorphismus von $\mathcal{J}(KG)$ auf den jeweiligen Faktorraum der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ und $m \in \underline{p-1} \setminus \{1\}$. Dann gilt $\text{cl}(\mathcal{J}(KG)) = p$ und

$$\left\{ \overline{y \sum_{i=0}^{p-1} \binom{i}{m-1} a^i} \mid y \in Y \right\} \text{ ist } K\text{-Basis von } \mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG)),$$

$$\left\{ \overline{y - 1_G} \mid y \in Y \right\} \text{ ist } K\text{-Basis von } \mathcal{J}(KG)/\mathcal{Z}_{p-1}(\mathcal{J}(KG)).$$

□

1.16 Satz. Sei $n \in \mathbb{N}_{>3}$, K ein Körper mit $\text{char } K = 2$, $G \in \{D_{2^n}, SD_{2^n}, Q_{2^n}\}$, $a \in G$ mit $o(a) = 2^{n-1}$ und $b \in G \setminus \langle a \rangle$. Sei weiter $\bar{}$ der kanonische K -Vektorraum-Epimorphismus von $\mathcal{J}(KG)$ auf den jeweiligen Faktorraum der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$. Dann gilt $\text{cl}(\mathcal{J}(KG)) = 2^{n-2} = |\gamma_2(G)|$ und:

$$\text{Ist } m \in \{2, 4, \dots, 2^{n-2} - 2\}, \text{ so ist } \left\{ \overline{y \sum_{i=0}^{2^{n-2}-1} \binom{i}{m-1} a^{2i}} \mid y \in \{b, ba, a\} \right\}$$

$$K\text{-Basis von } \mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG)).$$

$$\text{Ist } m \in \{3, 5, \dots, 2^{n-2} - 1\}, \text{ so ist } \left\{ \overline{y \sum_{i=0}^{2^{n-2}-1} \binom{i}{m-1} a^{2i}} \mid y \in \{b, ba, 1_G\} \right\}$$

$$K\text{-Basis von } \mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG)).$$

Weiter ist $\{\overline{y - 1_G} \mid y \in \{a, b, ba\}\}$ K -Basis von $\mathcal{J}(KG)/\mathcal{Z}_{2^{n-2}-1}(\mathcal{J}(KG))$.

□

Ziel dieser Arbeit ist es unter anderem, den Satz 1.15 zu verallgemeinern. Wir werden ferner einsehen, dass die Gruppen in Satz 1.16 eine gesonderte Rolle spielen.

Generell von Bedeutung für die aufsteigende Zentralreihe von $\mathcal{J}(KG)$ sind, was bereits das Studium des Zentrums von $\mathcal{J}(KG)$ vermuten lässt, die Konjugiertenklassen der Gruppe G . Folgendes Lemma zeigt für den Spezialfall $k = 1$ einen einfachen Zusammenhang zu den Restklassen bezüglich $\gamma_2(G)$ auf:

1.17 Lemma. *Sei G eine Gruppe, $k \in \mathbb{N}$ und $x \in \gamma_k(G)$. Dann gilt*

$$x^G \subseteq x\gamma_{k+1}(G).$$

Insbesondere gilt $g^G \subseteq g\gamma_2(G)$ für alle $g \in G$.

Beweis. Ist $h \in G$, so folgt $x^h = x[x, h]_{\mathfrak{g}} \in x\gamma_{k+1}(G)$. □

Ist also G eine Gruppe und $\gamma_2(G)$ endlich, so ist die Länge jeder Konjugiertenklasse durch die Ordnung von $\gamma_2(G)$ nach oben beschränkt.

1.18 Definition. *Sei G eine Gruppe und $g \in G$. Wir nennen die Konjugiertenklasse g^G (und auch g selbst) zentral, falls $g \in \mathcal{Z}(G)$ gilt und g^G (und auch g) extremal, falls $g^G = g\gamma_2(G)$ gilt. Weiter setzen wir für alle $n \in \mathbb{N}$ und $T \subseteq G$:*

$$\mathcal{K}_{T,n}(G) := \{C \mid C \in \mathcal{K}(G), C \subseteq T, |C| = n\} \quad \text{und} \quad \mathcal{K}_T(G) := \bigcup_{m \in \mathbb{N}} \mathcal{K}_{T,m}(G).$$

1.19 Definition. *Sei G eine p -Gruppe.*

- (i) *Für alle $g \in G$ sei $\kappa(g) \in \mathbb{N}_0$ mit $p^{\kappa(g)} = |g^G|$.*
- (ii) *Für alle $T \subseteq G$, $T \neq \emptyset$, sei $\mu(T) = \min \{\kappa(g) \mid g \in T\}$.*

1.20 Satz. *Sei G eine p -Gruppe und K ein Körper mit $\text{char } K = p$. Ist $T \subseteq G$ mit $T \cap \mathcal{Z}(G) \neq \emptyset$, so sei $g_T \in T \cap \mathcal{Z}(G)$ und $\mathfrak{Z}_T := \{g - g_T \mid g \in (T \cap \mathcal{Z}(G)) \setminus \{g_T\}\}$, andernfalls sei $\mathfrak{Z}_T := \emptyset$. Für alle $T \subseteq G$ ist dann*

$$\mathfrak{B}_T := \mathfrak{Z}_T \cup \left\{ \sum_{c \in C} c \mid C \in \mathcal{K}_T(G), |C| \neq 1 \right\}$$

eine K -Basis von $\mathcal{Z}(\mathcal{J}(KG)) \cap \langle T \rangle_K$. Insbesondere gilt

- (i) $\dim(\mathcal{Z}(\mathcal{J}(KG)) \cap \langle T \rangle_K) = |\mathcal{K}_T(G)| - 1$ für alle $T \subseteq G$ mit $T \cap \mathcal{Z}(G) \neq \emptyset$,
- (ii) $\dim(\mathcal{Z}(\mathcal{J}(KG)) \cap \langle T \rangle_K) = |\mathcal{K}_T(G)|$ für alle $T \subseteq G$ mit $T \cap \mathcal{Z}(G) = \emptyset$,
- (iii) $\dim \mathcal{Z}(\mathcal{J}(KG)) = -1 + \sum_{H \in G/\gamma_2(G)} |\mathcal{K}_H(G)|$.

Beweis. Sei $T \subseteq G$. Dann ist \mathfrak{B}_T K -linear unabhängig aufgrund der Disjunktheit zweier Konjugiertenklassen und es gilt $\mathfrak{B}_T \subseteq \mathcal{Z}(\mathcal{J}(KG)) \cap \langle T \rangle_K$ nach Satz 1.5.

Sei $x \in \mathcal{Z}(\mathcal{J}(KG)) \cap \langle T \rangle_K$. Dann ist x insbesondere eine K -Linearkombination von Elementen der Basis \mathfrak{B} aus Satz 1.5. Wegen $x \in \langle T \rangle_K$ folgt aus der Disjunktheit verschiedener Konjugiertenklassen, dass x auch K -Linearkombination von Elementen aus \mathfrak{B}_T ist.

(i) und (ii) folgen unmittelbar aus der Basiseigenschaft von \mathfrak{B}_T .

Aus Lemma 1.17 und Satz 1.5 erhalten wir, dass

$$\bigcup_{H \in G/\gamma_2(G)} \mathfrak{B}_H \cup \{g_H - 1_G \mid H \in G/\gamma_2(G) \setminus \{\gamma_2(G)\}, \mu(H) = 0\}$$

eine K -Basis von $\mathcal{Z}(\mathcal{J}(KG))$ ist. Hieraus folgt (iii). □

1.2 Zahlentheoretische Hilfsmittel

In diesem Abschnitt beschäftigen wir uns mit zahlentheoretischen Überlegungen, die für die Rechnungen in den weiteren Kapiteln von Bedeutung sein werden. Dafür untersuchen wir zunächst Binomialkoeffizienten modulo der Primzahl p . Im Anschluss studieren wir Folgen von Binomialkoeffizienten und formulieren darüber hinaus erste, hieraus resultierende Aussagen im Gruppenring. Der zweite Teil nimmt die Untersuchung einer Funktion vorweg, die im Zusammenhang mit der Bestimmung der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ im Falle einer zyklischen Kommutatoruntergruppe von G auftreten wird (siehe Definition 2.33 und Bemerkung 2.33.1).

1.2.1 Binomialkoeffizienten

Für alle $n, k \in \mathbb{N}_0$ ist $\binom{n}{k}$ bekanntlich die Anzahl der k -elementigen Teilmengen einer n -elementigen Menge. Insbesondere gilt $\binom{n}{0} = 1$ und $\binom{n}{k} = 0$ für $k > n$. Für unsere Zwecke erweist sich darüber hinaus folgende Setzung als nützlich:

$$\text{Für alle } n \in \mathbb{N}_0, k \in \mathbb{Z}_{<0} \text{ sei } \binom{n}{k} := 0.$$

Eine einfache kombinatorische Überlegung liefert direkt:

1.21 Lemma (Vandermonde-Identität).

Für alle $m, n \in \mathbb{N}_0, k \in \mathbb{Z}$ gilt:

$$\binom{m+n}{k} = \sum_{i=0}^k \binom{m}{i} \binom{n}{k-i}.$$

□

Folgender Satz zeigt auf, wie man die Berechnung eines Binomialkoeffizienten modulo der Primzahl p allein auf die p -adischen Darstellungen der beteiligten natürlichen Zahlen zurückführen kann. Dieser Satz von Lucas aus dem Jahr 1878 (siehe zum Beispiel [9]) führt zu zahlreichen nützlichen Folgerungen.

1.22 Satz, Lucas. Seien $m, n, k \in \mathbb{N}_0$, $m_i, n_i \in \underline{p-1}_0$ für alle $i \in \underline{k}_0$ mit $m = \sum_{i=0}^k m_i p^i$ und $n = \sum_{i=0}^k n_i p^i$. Dann gilt

$$\binom{n}{m}_p \equiv \prod_{i=0}^k \binom{n_i}{m_i}.$$

Insbesondere gilt:

$$\binom{n}{m}_p \equiv 0 \iff \exists i \in \underline{k}_0 : n_i < m_i.$$

□

1.22.1 Bemerkung. Es gilt

$$\binom{n}{m}_p \equiv \binom{np^l}{mp^l}_p \text{ für alle } l \in \mathbb{N}_0.$$

Beweis. Es ist $np = \sum_{i=1}^{k+1} n_{i-1} p^i$ und $mp = \sum_{i=1}^{k+1} m_{i-1} p^i$. Wir erhalten

$$\binom{np}{mp}_p \equiv \binom{0}{0} \prod_{i=1}^{k+1} \binom{n_{i-1}}{m_{i-1}} = \prod_{i=0}^k \binom{n_i}{m_i}_p \equiv \binom{n}{m}_p.$$

Die Behauptung folgt nun mittels einer trivialen Induktion nach l . □

1.22.2 Bemerkung. Für alle $l \in \mathbb{N}_0$ mit $p^l > m$ gilt

$$\binom{n}{m}_p \equiv \binom{n+p^l}{m}_p.$$

Beweis. Ist $l \in \mathbb{N}_0$ mit $p^l > m$, so gilt $\binom{n}{m} = \binom{n}{m} \binom{p^l}{0} \stackrel{1.22}{\equiv}_p \binom{n+p^l}{m}$. □

1.22.3 Bemerkung. Sei $r \in \mathbb{N}$. Es gilt

$$(i) \quad \binom{n}{p^k - 1}_p \equiv 1 \iff n \equiv -1_{p^k} \quad \text{und}$$

$$(ii) \quad \binom{n}{rp^k - 1}_p \not\equiv 0 \implies n \equiv -1_{p^k}.$$

1 Grundlagen

Beweis. Ist $k = 0$, so sind (i) und (ii) trivial. Sei daher nun $k > 0$. Es gilt

$$(*) \quad n \equiv_{p^k} -1 \iff \forall i \in \underline{k-1}_0 : n_i = p-1$$

Außerdem gilt $rp^k - 1 = (r-1)p^k + (p-1) \sum_{i=0}^{k-1} p^i$ und folglich

$$\binom{n}{rp^k - 1} \equiv_p \prod_{i=0}^{k-1} \binom{n_i}{p-1} \binom{n_k p^k}{(r-1)p^k} \equiv_p \prod_{i=0}^{k-1} \binom{n_i}{p-1} \binom{n_k}{r-1}.$$

Es folgt

$$\binom{n}{rp^k - 1} \not\equiv_p 0 \implies \forall i \in \underline{k-1}_0 : n_i = p-1.$$

Im Spezialfall $r = 1$ gilt

$$\binom{n}{p^k - 1} \equiv_p 1 \iff \forall i \in \underline{k-1}_0 : n_i = p-1.$$

Aus (*) folgen nun die Behauptungen. □

1.22.4 Bemerkung. Ist $m \leq p^n - 1$, so gilt

$$\binom{p^n - 1}{m} \equiv_p (-1)^m.$$

Beweis. Ist $n = 0$, so ist $m = 0$ und die Behauptung trivial. Sei daher nun $n > 0$. Ist dann $m = 0$, so ist die Aussage wiederum offensichtlich. Andernfalls ist $m > 0$ und wir erhalten induktiv

$$0 = \binom{0}{m} \equiv_p \binom{p^n}{m} = \binom{p^n - 1 + 1}{m} \equiv_p \binom{p^n - 1}{m-1} + \binom{p^n - 1}{m} \equiv_p (-1)^{m-1} + \binom{p^n - 1}{m}.$$

Hieraus folgt die Behauptung. □

1.22.5 Bemerkung. Sei $r \in \mathbb{N}_0$, $l \in \mathbb{N}$ und $m \leq p^l - 2$. Dann gilt

$$\sum_{i=0}^{p^l-1} \binom{i+r}{m} \equiv_p 0.$$

Beweis. Es gilt $\sum_{i=0}^{p^l-1} \binom{i}{m} = \binom{p^l}{m+1}$. Falls $r = 0$ gilt, folgt die Behauptung nun wegen $m+1 < p^l$ aus Bemerkung 1.22.2. Den Fall $r > 0$ führen wir durch folgende Rechnung auf den gerade bewiesenen Spezialfall zurück:

$$\sum_{i=0}^{p^l-1} \binom{i+r}{m} \equiv_p \sum_{i=0}^{p^l-1} \sum_{j=0}^r \binom{r}{j} \binom{i}{m-j} = \sum_{j=0}^r \left(\binom{r}{j} \sum_{i=0}^{p^l-1} \binom{i}{m-j} \right) \equiv_p 0.$$

□

1.22.6 Bemerkung. Sei $i \in \mathbb{N}_0$, $n > 0$ und $r \in \underline{n}$. Dann gilt

$$(i) \quad \binom{i + p^n - 1}{m} \equiv_p \sum_{j=0}^{p-1} (-1)^j \binom{i + p^{n-1} - 1}{m - jp^{n-1}} \quad \text{und}$$

$$(ii) \quad \binom{i + p^n - 1}{m} \equiv_p \binom{i + p^{n-r} - 1}{m - p^n + p^{n-r}} + \sum_{s=1}^r \sum_{j=0}^{p-2} (-1)^j \binom{i + p^{n-s} - 1}{m - p^{n-s}(p^s - p + j)}.$$

Beweis. Es gilt

$$\begin{aligned} \binom{i + p^n - 1}{m} &\stackrel{1.21}{=} \sum_{j=0}^m \binom{i + p^{n-1} - 1}{m - j} \binom{(p-1)p^{n-1}}{j} \\ &= \sum_{j=0}^{(p-1)p^{n-1}} \binom{i + p^{n-1} - 1}{m - j} \binom{(p-1)p^{n-1}}{j} \\ &\stackrel{1.22}{=} \sum_{\substack{j \in \frac{(p-1)p^{n-1}}{p^{n-1}|j} \mathbb{N}_0}} \binom{i + p^{n-1} - 1}{m - j} \binom{(p-1)p^{n-1}}{j} \\ &\stackrel{1.22.1}{=} \sum_{j=0}^{p-1} \binom{i + p^{n-1} - 1}{m - jp^{n-1}} \binom{p-1}{j} \\ &\stackrel{1.22.4}{=} \sum_{j=0}^{p-1} (-1)^j \binom{i + p^{n-1} - 1}{m - jp^{n-1}}. \end{aligned}$$

(ii) Der Spezialfall $r = 1$ wurde bereits in (i) bewiesen und stellt somit den Induktionsanfang eines Induktionsbeweises nach r der zweiten Aussage dar. Wir nehmen daher im Folgenden $r > 0$ an. Es gilt

$$\begin{aligned} \binom{i + p^{n-(r-1)} - 1}{m - p^n + p^{n-(r-1)}} &\stackrel{(i)}{=} \sum_{j=0}^{p-1} (-1)^j \binom{i + p^{n-r} - 1}{m - p^n + p^{n-(r-1)} - jp^{n-r}} \\ &= \binom{i + p^{n-r} - 1}{m - p^n + p^{n-r}} + \sum_{j=0}^{p-2} (-1)^j \binom{i + p^{n-r} - 1}{m - p^{n-r}(p^r - p + j)} \end{aligned}$$

und folglich

$$\begin{aligned} \binom{i + p^n - 1}{m} &\stackrel{\text{Ind.vor.}}{=} \binom{i + p^{n-(r-1)} - 1}{m - p^n + p^{n-(r-1)}} + \sum_{s=1}^{r-1} \sum_{j=0}^{p-2} (-1)^j \binom{i + p^{n-s} - 1}{m - p^{n-s}(p^s - p + j)} \\ &= \binom{i + p^{n-r} - 1}{m - p^n + p^{n-r}} + \sum_{s=1}^r \sum_{j=0}^{p-2} (-1)^j \binom{i + p^{n-s} - 1}{m - p^{n-s}(p^s - p + j)}. \end{aligned}$$

□

1 Grundlagen

Nach dieser kurzen Einführung über Binomialkoeffizienten modulo der Primzahl p wollen wir uns mit Folgen von Binomialkoeffizienten beschäftigen.

1.23 Lemma. *Sei K ein kommutativer unitärer Ring, $T := \{r \in K \mid \exists k \in \mathbb{Z} : r = k1_K\}$ und X eine nichtleere Menge.*

(i) *T ist ein unitärer⁴ Teilring von K .*

(ii) *Vermöge der bildweisen Multiplikation*

$$\varphi \cdot \psi : X \rightarrow K, \quad x \mapsto x\varphi x\psi$$

für alle $\varphi, \psi \in K^X$ ist der K -Raum K^X eine K -Algebra.

(iii) *$T^{\mathbb{N}_0}$ ist eine T -Algebra und $\left\{ \left(\binom{i}{l} \right)_K \mid l \in \mathbb{N}_0 \right\}$ ist eine K -linear unabhängige Teilmenge von $K^{\mathbb{N}_0}$.*

(iv) *Sind $n \in \mathbb{N}_0$, $x_0, \dots, x_n \in X$ paarweise verschieden, so ist in dem über X freien K -Raum KX die Menge $\left\{ \sum_{i=0}^n \left(\binom{i}{l} \right)_K x_i \mid l \in \underline{n}_0 \right\}$ K -linear unabhängig.*

Beweis. Wir beschränken uns auf den Beweis von (iii) über die lineare Unabhängigkeit. Die Aussage (iv) folgt dann direkt aus (iii). Seien also $k \in \mathbb{N}_0$, $c_0, \dots, c_k \in K$ mit

$$\sum_{j=0}^k c_j \left(\binom{i}{j} \right)_K = 0_{T^{\mathbb{N}_0}}.$$

Dann gilt $\sum_{j=0}^k c_j \binom{0}{j}_K = c_0 1_K = 0_K$ und damit $c_0 = 0_K$. Ist weiter $0 < m \leq k$ und

gilt induktiv bereits $c_0 = \dots = c_{m-1} = 0_K$, so folgt aus $0_K = \sum_{j=m}^k c_j \binom{i}{j}_K = c_m 1_K$ die

Behauptung. □

Wir betrachten im Folgenden die \mathbb{Z} -Algebra $\mathbb{Z}^{\mathbb{N}_0}$ mit bildweiser Multiplikation wie in Lemma 1.23 (ii). Für unsere Zwecke sind dabei in erster Linie Folgen von Interesse, deren Bilder Binomialkoeffizienten sind.

Ist $m \in \mathbb{N}_0$, so schreiben wir für die Folge $\left(\binom{i}{m} \right)_{i \in \mathbb{N}_0}$ auch kurz $\binom{i}{m}_{i \in \mathbb{N}_0}$.

1.23.1 Bemerkung. *Für alle $m \in \mathbb{N}_0$ sei $k_m \in \mathbb{N}_0$. Für alle $n \in \mathbb{N}_0$ sei*

$$A_n := \left\{ \binom{i}{m}_{i \in \mathbb{N}_0} \mid m \in \underline{n}_0 \right\} \quad \text{und} \quad B_n := \left\{ \binom{i + k_m}{m}_{i \in \mathbb{N}_0} \mid m \in \underline{n}_0 \right\}.$$

Dann gilt

$$\langle A_n \rangle_{\mathbb{Z}} = \langle B_n \rangle_{\mathbb{Z}} \quad \text{für alle } n \in \mathbb{N}_0.$$

⁴Ein unitärer Teilring S eines unitären Ringes K heißt unital, falls $1_S = 1_K$ gilt.

Beweis. Wir zeigen die Behauptung durch Induktion nach n .

Es gilt $A_0 = \{1_{\mathbb{Z}^{\mathbb{N}_0}}\} = B_0$. Sei nun $n \in \mathbb{N}$. Dann folgt die Inklusion $\langle A_n \rangle_{\mathbb{Z}} \supseteq \langle B_n \rangle_{\mathbb{Z}}$ mittels Lemma 1.21 aus

$$\binom{i + k_m}{m} = \binom{i}{m} + \sum_{j=0}^{m-1} \binom{k_m}{m-j} \binom{i}{j} \quad \text{für alle } m \in \underline{n}_0 \text{ und } i \in \mathbb{N}_0.$$

Da wir induktiv aber auch $\langle A_{n-1} \rangle_{\mathbb{Z}} \subseteq \langle B_{n-1} \rangle_{\mathbb{Z}}$ voraussetzen dürfen, folgt aus dem Spezialfall $m = n$ auch die andere Inklusion. \square

1.23.2 Bemerkung.

Sei K ein Körper, V ein K -Vektorraum, $n \in \mathbb{N}$ und $T = \{x_0, \dots, x_{n-1}\}$ eine n -elementige, K -linear unabhängige Teilmenge von V . Sei weiter $k_m \in \mathbb{N}_0$ für alle $m \in \mathbb{N}_0$. Dann gilt

- (i) $\left\langle \sum_{i=0}^{n-1} \binom{i + k_m}{m} x_i \mid m \in \underline{s}_0 \right\rangle_K = \left\langle \sum_{i=0}^{n-1} \binom{i}{m} x_i \mid m \in \underline{s}_0 \right\rangle_K$ für alle $s \in \mathbb{N}_0$ und
- (ii) $\left\{ \sum_{i=0}^{n-1} \binom{i + k_m}{m} x_i \mid m \in \underline{n-1}_0 \right\}$ und $\left\{ \sum_{i=0}^{n-1} \binom{i}{m} x_i \mid m \in \underline{n-1}_0 \right\}$ sind K -linear unabhängig.

(iii) Sei $\text{char } K = p$ und es existiere $l \in \mathbb{N}$ mit $p^l = n$. Dann ist

$$\left\{ \sum_{i=0}^{n-1} \binom{i + k_m}{m} x_i \mid m \in \underline{n-2}_0 \right\} \text{ eine } K\text{-Basis von } \text{Aug}_T(\langle T \rangle_K).$$

Beweis. (i) folgt direkt aus Bemerkung 1.23.1 und (ii) aus (i) sowie Lemma 1.23 (iv).

(iii): Sei $\text{char } K = p$ und es existiere $l \in \mathbb{N}$ mit $p^l = n$. Es gilt $\dim \text{Aug}_T(\langle T \rangle_K) = n - 1$ und Bemerkung 1.22.5 liefert

$$\left\{ \sum_{i=0}^{n-1} \binom{i + k_m}{m} x_i \mid m \in \underline{n-2}_0 \right\} \subseteq \text{Aug}_T(\langle T \rangle_K).$$

Mittels (ii) folgt aus Dimensionsgründen die Behauptung. \square

1.24 Lemma. Seien $m, n \in \mathbb{N}_0$. Dann gilt

$$\binom{i}{n}_{i \in \mathbb{N}_0} \cdot \binom{i}{m}_{i \in \mathbb{N}_0} = \sum_{j=0}^n \binom{m}{n-j} \binom{j+m}{j} \left(\binom{i}{m+j} \right)_{i \in \mathbb{N}_0}.$$

Insbesondere gilt

$$\binom{i}{n}_{i \in \mathbb{N}_0} \cdot \binom{i}{m}_{i \in \mathbb{N}_0} \in \left\langle \binom{i}{m}_{i \in \mathbb{N}_0}, \binom{i}{m+1}_{i \in \mathbb{N}_0}, \dots, \binom{i}{m+n}_{i \in \mathbb{N}_0} \right\rangle_{\mathbb{N}_0}.$$

1 Grundlagen

Beweis. Ist $m = 0$ und $n = 0$, so ist die Behauptung trivial. Wir nehmen im Folgenden daher $m > 0$ oder $n > 0$ an. Einfaches Nachrechnen zeigt: Ist $j \in \mathbb{N}_0$, so gilt für alle $i \in \mathbb{N}_{\geq m}$:

$$(*) \quad \binom{i-m}{j} \binom{i}{m} = \binom{j+m}{j} \binom{i}{m+j}$$

Sei $c_j := \binom{m}{n-j}$ und $d_j := \binom{j+m}{j}$ für alle $j \in \underline{n}$. Nach Lemma 1.21 gilt für alle $i \in \mathbb{N}_{\geq m}$:

$$\binom{i}{n} = \binom{m + (i-m)}{n} = \sum_{j=0}^n c_j \binom{i-m}{j}$$

Es folgt

$$0 = \binom{i}{n} \binom{i}{m} = \sum_{j=0}^n c_j d_j \binom{i}{m+j} \text{ für alle } i \in \underline{m-1}_0 \text{ und}$$

$$\binom{i}{n} \binom{i}{m} = \left(\sum_{j=0}^n c_j \binom{i-m}{j} \right) \binom{i}{m} \stackrel{(*)}{=} \sum_{j=0}^n c_j d_j \binom{i}{m+j} \text{ für alle } i \in \mathbb{N}_{\geq m}.$$

□

1.24.1 Bemerkung. *Es gilt*

$$\left(\binom{ni}{m} \right)_{i \in \mathbb{N}_0} \in \left\langle \left(\binom{i}{j} \right)_{i \in \mathbb{N}_0} \mid j \in \underline{m}_0 \right\rangle_{\mathbb{N}_0}.$$

Beweis. Wir zeigen die Behauptung durch Induktion nach n . Ist $m = 0$, so gilt $1 = \binom{0i}{m} = \binom{i}{0}$ für alle $i \in \mathbb{N}_0$. Ist $m > 0$, so gilt $\binom{0i}{m} = 0$ für alle $i \in \mathbb{N}_0$. Sei nun $n > 0$. Dann gilt

$$\left(\binom{ni}{m} \right)_{i \in \mathbb{N}_0} \stackrel{1.21}{=} \sum_{j=0}^m \binom{(n-1)i}{j} \left(\binom{i}{m-j} \right)_{i \in \mathbb{N}_0}$$

und aus der Induktionsvoraussetzung folgt

$$\left(\binom{(n-1)i}{j} \right)_{i \in \mathbb{N}_0} \in \left\langle \left(\binom{i}{s} \right)_{i \in \mathbb{N}_0} \mid s \in \underline{j}_0 \right\rangle_{\mathbb{N}_0} \text{ für alle } j \in \underline{m}_0.$$

Aus Lemma 1.24 folgt die Behauptung. □

1.24.2 Bemerkung. Sei $l \in \mathbb{N}_0$ und $\bar{\cdot}$ der kanonische Epimorphismus von $\mathbb{Z}^{\mathbb{N}_0}$ auf $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}_0}$. Dann gilt

(i)

$$\overline{\binom{i + np^l}{m}}_{i \in \mathbb{N}_0} \in \overline{\binom{i}{m}}_{i \in \mathbb{N}_0} + \bar{n} \overline{\binom{i}{m - p^l}}_{i \in \mathbb{N}_0} + \left\langle \overline{\binom{i}{m - sp^l}}_{i \in \mathbb{N}_0} \mid s \in \mathbb{N}_{>1} \right\rangle_{\mathbb{N}_0},$$

(ii)

$$\overline{\binom{np^l i}{m}}_{i \in \mathbb{N}_0} = 0_{(\mathbb{Z}/p\mathbb{Z})^{\mathbb{N}_0}}, \quad \text{falls } p^l \nmid m \quad \text{und}$$

$$\overline{\binom{np^l i}{m}}_{i \in \mathbb{N}_0} \in \left\langle \overline{\binom{i}{j}}_{i \in \mathbb{N}_0} \mid j \in \underline{\tilde{m}_0} \right\rangle_{\mathbb{N}_0}, \quad \text{falls } p^l \mid m \quad \text{und } \tilde{m} = \frac{m}{p^l}.$$

Beweis. Es gilt

$$\binom{i + np^l}{m} \stackrel{1.21}{=} \sum_{j=0}^m \binom{i}{m-j} \binom{np^l}{j} \stackrel{1.22}{=} \sum_{\substack{j \in \underline{m_0}, \\ p^l \mid j}} \binom{i}{m-j} \binom{np^l}{j} \quad \text{für alle } i \in \mathbb{N}_0,$$

woraus zusammen mit Bemerkung 1.22.1 die erste Aussage folgt.

Der erste Teil von (ii) folgt direkt aus Satz 1.22, während der zweite Teil durch eine Anwendung der Bemerkungen 1.22.1 und 1.24.1 folgt. \square

1.25 Lemma. Sei G eine Gruppe, K ein Körper mit $\text{char } K = p$, $a \in G$ und es existiere $l \in \mathbb{N}_0$ mit $o(a) = p^l$. Seien $s, n \in \mathbb{N}_0$ und $m \in \underline{p^{s+l} - 1_0}$. Dann gilt

$$a^{-n} \sum_{i=0}^{p^l-1} \binom{p^s i + r}{m} a^i = \sum_{i=0}^{p^l-1} \binom{p^s(i+n) + r}{m} a^i \quad \text{für alle } r \in \mathbb{N}_0.$$

Beweis. Wir beweisen den Spezialfall $r = 0$. Ist $r > 0$, so folgt daraus die Behauptung durch eine Anwendung von Lemma 1.21. Zunächst beweisen wir nun den Spezialfall $s = 0$ und führen anschließend den Fall $s > 0$ auf diesen zurück.

1 Grundlagen

Es existieren eindeutig bestimmte $q \in \mathbb{N}_0$, $\tilde{n} \in \underline{p^l - 1}_0$ mit $n = qp^l + \tilde{n}$. Es gilt

$$\begin{aligned}
a^{-n} \sum_{i=0}^{p^l-1} \binom{i}{m} a^i &\stackrel{o(a)=p^l}{=} \sum_{i=0}^{p^l-1} \binom{i}{m} a^{i-\tilde{n}} \\
&= \sum_{i=0}^{\tilde{n}-1} \binom{i}{m} a^{i-\tilde{n}} + \sum_{i=\tilde{n}}^{p^l-1} \binom{i}{m} a^{i-\tilde{n}} \\
&= \sum_{i=p^l-\tilde{n}}^{p^l-1} \binom{i+\tilde{n}-p^l}{m} a^{i-p^l} + \sum_{i=\tilde{n}}^{p^l-1} \binom{i}{m} a^{i-\tilde{n}} \\
&\stackrel{1.22.2}{=} \sum_{m \leq p^l-1} \sum_{i=p^l-\tilde{n}}^{p^l-1} \binom{i+\tilde{n}}{m} a^i + \sum_{i=0}^{p^l-\tilde{n}-1} \binom{i+\tilde{n}}{m} a^i \\
&\stackrel{1.22.2}{=} \sum_{i=0}^{p^l-1} \binom{i+n}{m} a^i.
\end{aligned}$$

Sei nun $s \neq 0$. Gilt $p^s \nmid m$, so ist nach Bemerkung 1.24.2 nichts weiter zu zeigen. Andernfalls existiert $t \in \underline{p^l - 1}_0$ mit $p^s t = m$ und es folgt

$$\begin{aligned}
a^{-n} \sum_{i=0}^{p^l-1} \binom{p^s i}{m} a^i &= a^{-n} \sum_{i=0}^{p^l-1} \binom{p^s i}{p^s t} a^i \\
&\stackrel{1.22.1}{=} a^{-n} \sum_{i=0}^{p^l-1} \binom{i}{t} a^i \\
&= \sum_{i=0}^{p^l-1} \binom{i+n}{t} a^i \\
&\stackrel{1.22.1}{=} \sum_{i=0}^{p^l-1} \binom{p^s(i+n)}{m} a^i.
\end{aligned}$$

□

1.26 Korollar. Sei G eine Gruppe, K ein Körper mit $\text{char } K = p$ und U eine zyklische p -Untergruppe von G , $l \in \mathbb{N}_0$ mit $p^l = |U|$, $a \in G$ mit $\langle a \rangle = U$ und H eine Linksrestklasse bezüglich U . Sei weiter $k_m \in \mathbb{N}_0$ für alle $m \in \mathbb{N}_0$.

(i) Für alle $g, h \in H$ und $\tilde{m} \in \underline{p^l - 1}_0$ gilt

$$\left\langle g \sum_{i=0}^{p^l-1} \binom{i}{m} a^i \mid m \in \tilde{m}_0 \right\rangle_K = \left\langle h \sum_{i=0}^{p^l-1} \binom{i}{m} a^i \mid m \in \tilde{m}_0 \right\rangle_K.$$

(ii) Ist $U \neq \{1_G\}$, so ist für alle $g \in H$

$$\left\{ g \sum_{i=0}^{p^l-1} \binom{i+k_m}{m} a^i \mid m \in \underline{p^l-2}_0 \right\}$$

eine K -Basis von $\text{Aug}(H)$.

Beweis. Seien $g, h \in H$. Dann existiert $n \in \underline{p^l-1}_0$ mit $ga^{-n} = h$. Aus Lemma 1.25 und Bemerkung 1.23.2 (i) folgt dann direkt (i). (ii) folgt aus der dritten Aussage in Bemerkung 1.23.2. \square

In Lemma 1.25 haben wir für ein Element a von p -Potenzordnung p^l einer Gruppe G und einen Körper K mit $\text{char } K = p$ eine Rechenregel für die Multiplikation einer Linearkombination der Gestalt $\sum_{i=0}^{p^l-1} \binom{i}{m} a^i$ mit einem Element aus $\langle a \rangle$ formuliert. Im Folgenden werden wir nun für einen Gruppen-Automorphismus β von $\langle a \rangle$ eine Rechenvorschrift für $\sum_{i=0}^{p^l-1} \binom{i}{m} (a\beta)^i$ angeben. Für ein solches β existiert $n \in \mathbb{N}$, $p \nmid n$, mit $a\beta = a^n$ und β ist durch das Bild von a bereits eindeutig bestimmt.

1.27 Lemma. Sei G eine zyklische p -Gruppe, K ein Körper mit $\text{char } K = p$, $a \in G$ mit $\langle a \rangle = G$ und $l \in \mathbb{N}_0$ mit $|G| = p^l$. Sei $y \in \mathbb{Z}$ mit $p \nmid y$, $n \in \mathbb{N}$ mit $yn \equiv 1 \pmod{p^l}$ und $m \in \underline{p^l-1}_0$. Dann gilt

$$\sum_{i=0}^{p^l-1} \binom{i}{m} a^{yi} = \sum_{i=0}^{p^l-1} \binom{ni}{m} a^i.$$

Beweis. Ist $l = 0$, so ist die Behauptung trivial. Sei daher nun $l > 0$ angenommen. Sei $\bar{\cdot} : \mathbb{Z} \rightarrow \mathbb{Z}/p^l\mathbb{Z}$ der kanonische Ring-Epimorphismus. Für alle $i \in \underline{p^l-1}_0$ existiert ein eindeutig bestimmtes $n_i \in \underline{p^l-1}_0$ mit $\overline{ni} = \overline{n_i}$. Wegen $yn \equiv 1 \pmod{p^l}$ gilt $p \nmid n$ und folglich $\{\overline{ni} \mid i \in \underline{p^l-1}_0\} = \mathbb{Z}/p^l\mathbb{Z}$. Also ist die Abbildung

$$\underline{p^l-1}_0 \longrightarrow \underline{p^l-1}_0, \quad i \mapsto n_i$$

eine Bijektion. Es folgt

$$\sum_{i=0}^{p^l-1} \binom{i}{m} a^{yi} = \sum_{i=0}^{p^l-1} \binom{n_i}{m} a^{yn_i} \stackrel{1.22.2}{=} \sum_{o(a)=p^l} \sum_{i=0}^{p^l-1} \binom{ni}{m} a^{yni} = \sum_{i=0}^{p^l-1} \binom{ni}{m} a^i.$$

\square

1.28 Lemma. Sei G eine zyklische p -Gruppe, K ein Körper mit $\text{char } K = p$, $a \in G$ mit $\langle a \rangle = G$ und $l \in \mathbb{N}_0$ mit $|G| = p^l$.

(i) Sind $n \in \underline{l}_0$ und $r, \tilde{m} \in \mathbb{N}$, so folgt

$$\sum_{i=0}^{p^l-1} \binom{i+rp^n-1}{\tilde{m}p^n-1} a^i = \sum_{i=0}^{p^{l-n}-1} \binom{i+r-1}{\tilde{m}-1} a^{ip^n}.$$

(ii) Es gilt

$$\sum_{i=0}^{p^l-1} \binom{i+p^l-1}{p^l-1} a^i = 1_G.$$

Beweis. (i) Seien $n \in \underline{l}_0$ und $r, \tilde{m} \in \mathbb{N}$. Dann gilt

$$\begin{aligned} \sum_{i=0}^{p^l-1} \binom{i+rp^n-1}{\tilde{m}p^n-1} a^i &\stackrel{1.22.3(ii)}{=} \sum_{i=0}^{p^{l-n}-1} \binom{ip^n+rp^n-1}{\tilde{m}p^n-1} a^{ip^n} \\ &= \sum_{i=0}^{p^{l-n}-1} \binom{(i+r-1)p^n+p^n-1}{(\tilde{m}-1)p^n+p^n-1} a^{ip^n} \\ &\stackrel{1.22}{=} \sum_{i=0}^{p^{l-n}-1} \binom{(i+r-1)p^n}{(\tilde{m}-1)p^n} a^{ip^n} \\ &\stackrel{1.22.1}{=} \sum_{i=0}^{p^{l-n}-1} \binom{i+r-1}{\tilde{m}-1} a^{ip^n}. \end{aligned}$$

(ii) folgt direkt aus dem Spezialfall $n = l$ und $\tilde{m} = r = 1$ in (i). □

1.2.2 Eine Partition von $\{1, \dots, p^l\}$

Im Zuge der Untersuchung der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ im Fall eines Körpers K mit $\text{char } K = p$ und einer p -Gruppe G mit zyklischer Kommutatoruntergruppe wird sich herausstellen, dass eine rein zahlentheoretische Funktion eine tragende Rolle spielt (siehe Satz 2.32). Die Untersuchung dieser Funktion nehmen wir in diesem Abschnitt vor. Die Ergebnisse dieser Analyse werden die Problematik der Bestimmung der aufsteigenden Zentralreihe (vergleiche Erläuterungen vor Satz 2.32) entscheidend reduzieren.

1.29 Lemma. Für alle $m, r, t \in \mathbb{N}_0$, $s \in \mathbb{N}$ und $j \in \underline{s-1}_0$ gilt

- (i) $p^{t+s-1} \leq p^t (p^s - p^j) \leq p^t (p^s - 1) \leq p^t (p^s - p^{-r}) < p^{t+s}$ und
- (ii) $p^m \leq p^t (p^s - p^{-r}) \iff p^m \leq p^t (p^s - 1).$
- (iii) Ist $n \in \mathbb{N}$ mit $n \mid m$, so gilt: $m \leq n(p^s - p^{-r}) \iff m \leq n(p^s - 1).$

Beweis. Seien $m, r, t \in \mathbb{N}_0$, $s \in \mathbb{N}$ und $j \in \underline{s-1}_0$. (i) folgt aus

$$p^{s-1} \leq p^{s-1}(p-1) = p^s - p^{s-1} \leq p^s - p^j \leq p^s - 1 \leq p^s - p^{-r} < p^s.$$

(ii) folgt direkt aus (i).

(iii): Sei $n \in \mathbb{N}$ mit $n \mid m$. Dann existiert $k \in \mathbb{N}_0$ mit $nk = m$. Es folgt

$$\begin{aligned} nk \leq n(p^s - 1) &\iff k \leq p^s - 1 \\ &\iff k \leq p^s - p^{-r} \\ &\iff nk \leq n(p^s - p^{-r}). \end{aligned}$$

□

1.30 Definition. Für alle $r, l \in \mathbb{N}_0$ und $k, n \in \underline{l}_0$ sei

$$\psi_{(l,k,n,r)} : \underline{p^l} \longrightarrow \mathbb{Q}, \quad m \mapsto \max \{m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1, m - p^{l-n} + 1, 1\}.$$

Für $n \leq k$ sei

- $\mathcal{Z}_{(l,k,n)} := \{cp^j \mid j \in \underline{k-n}_0, c \in \underline{p^{l-k}}\}$ und
- $\mathcal{D}_{(l,k,n)} := \{p^{l-n} + sp^{k-n+1} \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1}}\}.$

Für $n > k$ sei

- $\mathcal{Z}_{(l,k,n)} := \underline{p^{l-n}}$ und
- $\mathcal{D}_{(l,k,n)} := \underline{p^l} \setminus \mathcal{Z}_{(l,k,n)}.$

1.31 Lemma. Sei $r \in \mathbb{N}_0$, $l \in \mathbb{N}$, $k \in \underline{l-1}_0$, $n \in \underline{l}_0$,

$$\psi := \psi_{(l,k,n,r)}, \quad \mathcal{Z} := \mathcal{Z}_{(l,k,n)} \quad \text{und} \quad \mathcal{D} := \mathcal{D}_{(l,k,n)}.$$

Dann gilt für alle $m \in \underline{p}^l$:

- (i) $\mathcal{Z} \cap \mathcal{D} = \emptyset$,
- (ii) $1\psi^- = \mathcal{Z}$,
- (iii) $(m\psi = m - p^{l-n} + 1 \wedge m\psi > 1) \iff m \in \mathcal{D}$.
- (iv) Ist $m \notin \mathcal{Z} \cup \mathcal{D}$, so gilt $m\psi = m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1$ und $m\psi > 1$.
- (v) Ist $p > 2$ oder $l = 1$ oder $l - k \geq 2$, so gilt

$$(m\psi = m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1 \wedge m\psi > 1) \iff m \notin \mathcal{Z} \cup \mathcal{D}.$$

Beweis. Sei $m \in \underline{p}^l$.

(i): Gilt $n > k$ oder $n = 0$, so folgt das Behauptete direkt aus den Definitionen von \mathcal{Z} und \mathcal{D} . Andernfalls folgt $\mathcal{Z} \cap \mathcal{D} = \emptyset$ aus

$$\max \mathcal{Z} = p^{l-n} < p^{l-n} + p^{k-n+1} = \min \mathcal{D}.$$

(ii): Sei zunächst $n \leq k$. Es gilt:

$$\begin{aligned} m \in \mathcal{Z} &\iff \exists j \in \underline{k-n}_0 \quad \exists c \in \underline{p}^{l-k} : m = cp^j \\ &\iff m \leq p^{l-n} \wedge (\exists c \in \underline{p}^{l-k-1} : p \nmid c \wedge m = cp^{\nu(m)}) \\ &\iff m \leq p^{l-n} \wedge m \leq p^{\nu(m)}(p^{l-k} - 1) \\ &\stackrel{1.29(iii)}{\iff} m - p^{l-n} + 1 \leq 1 \wedge m \leq p^{\nu(m)}(p^{l-k} - p^{-r}) \\ &\iff m - p^{l-n} + 1 \leq 1 \wedge m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1 \leq 1 \\ &\iff m\psi = 1. \end{aligned}$$

Ist hingegen $n > k$, so gilt:

$$\begin{aligned} m \in \mathcal{Z} &\iff m - p^{l-n} \leq 0 \\ &\stackrel{p^{l-n} < p^{l-k}}{\iff} m - p^{\nu(m)}(p^{l-k} - 1) \leq 0 \wedge m - p^{l-n} + 1 \leq 1 \\ &\stackrel{1.29(iii)}{\iff} m - p^{\nu(m)}(p^{l-k} - p^{-r}) \leq 0 \wedge m - p^{l-n} + 1 \leq 1 \\ &\iff m\psi = 1. \end{aligned}$$

(iii): Sei wiederum zunächst $n \leq k$. Es sind äquivalent:

$$\begin{aligned} m \in \mathcal{D} &\iff m > p^{l-n} \wedge \nu(m) \geq k - n + 1 \\ &\iff m > p^{l-n} \wedge p^{\nu(m)+l-k-1} \geq p^{l-n} \\ &\stackrel{1.29(i)}{\iff} m > p^{l-n} \wedge p^{\nu(m)}(p^{l-k} - p^{-r}) \geq p^{l-n} \\ &\iff m\psi = m - p^{l-n} + 1 > 1. \end{aligned}$$

Sei nun $n > k$. Dann gilt

$$p^{\nu(m)}(p^{l-k} - p^{-r}) \stackrel{1.29(i)}{\geq} p^{\nu(m)+l-k-1} \geq p^{l-n}.$$

Es folgt $m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1 \leq m - p^{l-n} + 1$, also

$$\begin{aligned} m \in \mathcal{D} &\iff m \geq p^{l-n} + 1 \\ &\iff m\psi = m - p^{l-n} + 1 > 1. \end{aligned}$$

Hieraus folgt (iii).

(iv) folgt direkt aus (ii) und (iii).

(v): Sei $p > 2$ oder $l = 1$ oder $l - k \geq 2$. Es bleibt die Implikation „ \Rightarrow “ zu zeigen. Es gelte $m\psi = m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1 > 1$. Wegen $m\psi > 1$ gilt $m \notin \mathcal{Z}$. Annahme: $m \in \mathcal{D}$. Dann gilt $\mathcal{D} \neq \emptyset$. Insbesondere gilt $n \neq 0$. Wegen $1 \in \mathcal{Z}$ folgt außerdem $m \neq 1$. Nach (iii) gilt $m\psi = m - p^{l-n} + 1$, also $p^{l-n} = p^{\nu(m)}(p^{l-k} - p^{-r})$. Damit ist $p^{\nu(m)}(p^{l-k} - p^{-r})$ eine p -Potenz. Nach Lemma 1.29 (i) gilt

$$p^{\nu(m)+l-k-1} \leq p^{\nu(m)}(p^{l-k} - 1) \leq p^{\nu(m)}(p^{l-k} - p^{-r}) < p^{\nu(m)+l-k}.$$

Hieraus folgt

$$(*) \quad p^{\nu(m)+l-k-1} = p^{\nu(m)}(p^{l-k} - 1) = p^{\nu(m)}(p^{l-k} - p^{-r}) = p^{l-n}.$$

Folglich gilt $p^{l-k} - 1 = 1$, also $p = 2$ und $l - k = 1$. Nach unserer Voraussetzung folgt damit $l = 1$. Wegen $n \neq 0$ und $n \in \mathbb{L}_0$ folgt $n = 1$ und aus $m \in \underline{p}^l$ erhalten wir $m = 2$. (*) liefert nun $2 = p^{\nu(m)} = p^{\nu(m)+l-k-1} = p^{l-n} = p^0 = 1$. Damit haben wir obige Annahme zum Widerspruch geführt. \square

Anmerkung

Unter den Voraussetzungen von (v) haben wir bewiesen:

Sei $m \in \underline{p}^l$ und $\tilde{r} \in \mathbb{N}_0$. Für alle $r \in \mathbb{N}_0$ gilt $m\psi_{(l,k,n,\tilde{r})} = m - p^{\nu(m)}(p^{l-k} - p^{-\tilde{r}}) + 1 > 1$ sowie $m\psi_{(l,k,n,r)} = m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1 > 1$ genau dann, wenn $m \notin \mathcal{Z} \cup \mathcal{D}$ gilt. Außerdem haben wir in (ii) und (iii) gezeigt, dass aus $m \in \mathcal{Z} \cup \mathcal{D}$ direkt $m\psi_{(l,k,n,r)} = m\psi_{(l,k,n,\tilde{r})}$ folgt. Unabhängig von r entscheidet also allein die Zugehörigkeit von m zu \mathcal{D} oder \mathcal{Z} , welche der drei möglichen Maxima m unter $\psi_{(l,k,n,r)}$ annimmt.

1 Grundlagen

Wir betrachten nun für jedes $m \in \underline{p}^l$ den Spezialfall $r = \nu(m)$ und definieren:

1.32 Definition. Sei $l \in \mathbb{N}$, $k \in \underline{l-1}_0$ und $n \in \underline{l}_0$. Wir definieren

$$\psi_{(l,k,n)} : \underline{p}^l \longrightarrow \underline{p}^l, \quad m \mapsto \max \{m - p^{\nu(m)+l-k} + 2, m - p^{l-n} + 1, 1\}$$

und setzen

- (i) $\tilde{\mathcal{K}}_{(l,k,n)} := \{m \mid m \in \underline{p}^l \setminus \{1\}, m\psi_{(l,k,n)}^- = \emptyset\},$
- (ii) $\tilde{\mathcal{E}}_{(l,k,n)} := \{m \mid m \in \underline{p}^l \setminus \{1\}, |m\psi_{(l,k,n)}^-| = 1\} \quad \text{und}$
- (iii) $\tilde{\mathcal{D}}_{(l,k,n)} := \{m \mid m \in \underline{p}^l \setminus \{1\}, |m\psi_{(l,k,n)}^-| = 2\}.$

1.33 Lemma. Sei $l \in \mathbb{N}$, $k \in \underline{l-1}_0$, $n \in \underline{l}_0$,

$$\psi := \psi_{(l,k,n)}, \quad \mathcal{Z} := \mathcal{Z}_{(l,k,n)}, \quad \mathcal{D} := \mathcal{D}_{(l,k,n)}, \quad \tilde{\mathcal{K}} := \tilde{\mathcal{K}}_{(l,k,n)}, \quad \tilde{\mathcal{D}} := \tilde{\mathcal{D}}_{(l,k,n)} \quad \text{und} \quad \tilde{\mathcal{E}} := \tilde{\mathcal{E}}_{(l,k,n)}.$$

Ist $p = 2$, so sei $l = 1$ oder $l - k \geq 2$. Dann gilt für alle $m \in \underline{p}^l$:

- (i) $1\psi^- = \mathcal{Z},$
- (ii) $(m\psi = m - p^{l-n} + 1 \wedge m\psi > 1) \iff m \in \mathcal{D} \quad \text{und}$
- (iii) $(m\psi = m - p^{\nu(m)+l-k} + 2 \wedge m\psi > 1) \iff m \notin \mathcal{Z} \cup \mathcal{D}.$

Ist $n \leq k$, so gilt

- (iv) $\{sp^{k-n+1} + 1 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1}}\} = \mathcal{D}\psi \subseteq (\underline{p}^l \setminus (\mathcal{Z} \cup \mathcal{D}))\psi,$
- (v) $\forall m \in \underline{p}^l \setminus \{1\} : |m\psi^-| \leq 2,$
- (vi) $\tilde{\mathcal{K}} = (-(\mathcal{Z} \setminus \{1\}) + p^l + 2) \cup \{sp^{k-n+1} + 2 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1}_0\},$
- (vii) $\tilde{\mathcal{E}} = \underline{p}^l \setminus (\tilde{\mathcal{K}} \cup \tilde{\mathcal{D}} \cup \{1\}),$
- (viii) $\tilde{\mathcal{D}} = \mathcal{D}\psi \quad \text{und}$
- (ix) $|\tilde{\mathcal{E}}| = p^l - 2|\tilde{\mathcal{D}}| - |\mathcal{Z}|.$

Gilt $n > k$, so gilt

- (x) $\psi|_{\mathcal{D}}$ ist injektiv,
- (xi) $\tilde{\mathcal{E}} = \underline{p^l - p^{l-n} + 1} \setminus \{1\} = \text{Bild } \psi|_{\mathcal{D}}$
- (xii) $\tilde{\mathcal{D}} = \emptyset \quad \text{und}$
- (xiii) $\tilde{\mathcal{K}} = \underline{p}^l \setminus \underline{p^l - p^{l-n} + 1}.$

Beweis. Die ersten drei Aussagen folgen direkt aus Lemma 1.31.

Es gelte zunächst $n \leq k$. Aus (ii) folgt dann direkt

$$\mathcal{D}\psi = \{sp^{k-n+1} + 1 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1}}\}.$$

Sei $b \in \mathcal{D}\psi$. Dann existiert $r \in \underline{p^{l+n-k-1} - p^{l-k-1}}$ mit $b = rp^{k-n+1} + 1$. Wir setzen $\hat{b} := b + p^{l-k} - 2$. Dann gilt

$$1 \leq \hat{b} \leq \max \mathcal{D}\psi + p^{l-k} - 2 = p^l - p^{l-n} + 1 + p^{l-k} - 2 \leq p^l$$

und $\hat{b} \equiv_p -1$, also $\nu(\hat{b}) = 0$ und $\hat{b} \notin \mathcal{D}$. Es folgt

$$\hat{b}\psi \stackrel{(i),(iii)}{=} \max\{\hat{b} - p^{l-k} + 2, 1\} = \max\{b, 1\} = b \geq \min \mathcal{D}\psi \stackrel{(ii)}{>} 1.$$

und damit die Aussage (iv).

Sei

$$\psi_1 : \mathbb{N} \longrightarrow \mathbb{Z}, \quad m \mapsto m - p^{\nu(m)+l-k} + 2 \quad \text{und} \quad \psi_2 : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad m \mapsto m - p^{l-n} + 1.$$

Dann ist ψ_1 injektiv und ψ_2 bijektiv, denn:

Seien $m, \hat{m} \in \mathbb{N}$ mit $m\psi_1 = m - p^{\nu(m)+l-k} + 2 = \hat{m} - p^{\nu(\hat{m})+l-k} + 2 = \hat{m}\psi_2$. Wäre $\nu(m) \neq \nu(\hat{m})$ und etwa $m > \hat{m}$, so folgte

$$\begin{aligned} \min\{\nu(m), \nu(\hat{m})\} &= \nu(m - \hat{m}) \\ &= \nu(p^{\nu(m)+l-k} - p^{\nu(\hat{m})+l-k}) \\ &= \min\{\nu(m) + l - k, \nu(\hat{m}) + l - k\}. \end{aligned}$$

Wegen $l > k$ erhielten wir also einen Widerspruch. Also ist $\nu(m) = \nu(\hat{m})$ und damit $m = \hat{m}$. Die Bijektivität von ψ_2 ist offensichtlich.

Für alle $m \in \underline{p^l} \setminus \{1\}$ folgt hieraus nach Definition von ψ einerseits $|m\psi^-| \leq 2$ und andererseits zusammen mit (iv) für alle $m \in \underline{p^l} \setminus \{1\}$

$$m \in \mathcal{D}\psi \iff m \in \tilde{\mathcal{D}},$$

also (v) und (viii).

Wir bestimmen nun $|\tilde{\mathcal{K}}|$: Ist $n = 0$, so gilt $\mathcal{D} = \emptyset$ und außerdem

$$\{sp^{k-n+1} + 2 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1_0}\} = \{2\} \subseteq (-(\mathcal{Z} \setminus \{1\}) + p^l + 2).$$

Ist $n \neq 0$, so gilt

$$\{sp^{k-n+1} + 2 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1_0}\} \cap (-(\mathcal{Z} \setminus \{1\}) + p^l + 2) = \emptyset,$$

denn es gilt dann

$$\begin{aligned} \max\{sp^{k-n+1} + 2 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1_0}\} &= p^l - p^{l-n} - p^{k-n+1} + 2 \\ &< p^l - p^{l-n} + 2 = \min(-(\mathcal{Z} \setminus \{1\}) + p^l + 2). \end{aligned}$$

1 Grundlagen

Ist $n \neq 0$, so folgt aus (iv) außerdem $|\mathcal{D}| = |\{sp^{k-n+1} + 2 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1_0}\}|$. Aus diesen Überlegungen erhalten wir die zweite Gleichheit in Gleichung (1.1).

Weiter gilt

$$\begin{aligned} |\text{Bild } \psi| &= |(\underline{p^l} \setminus (\mathcal{Z} \cup \mathcal{D}))\psi \cup \mathcal{D}\psi \cup \mathcal{Z}\psi| \\ &\stackrel{(iv)}{=} |(\underline{p^l} \setminus (\mathcal{Z} \cup \mathcal{D}))\psi \cup \mathcal{Z}\psi| \\ &\stackrel{(i),(iii)}{=} |(\underline{p^l} \setminus (\mathcal{Z} \cup \mathcal{D}))\psi| + |\mathcal{Z}\psi| \\ &\stackrel{(iii)}{\underset{\psi_1 \text{ inj.}}{=}} p^l - |\mathcal{D}| - |\mathcal{Z}| + 1. \end{aligned}$$

Es folgt

$$\begin{aligned} |\tilde{\mathcal{K}}| &= p^l - |\text{Bild } \psi| \\ &= |\mathcal{D}| + |\mathcal{Z}| - 1 \\ &= |(-(\mathcal{Z} \setminus \{1\}) + p^l + 2) \cup \{sp^{k-n+1} + 2 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1_0}\}|. \end{aligned} \tag{1.1}$$

Um (vi) und (vii) zu beweisen, reicht es daher (siehe auch Definition von $\tilde{\mathcal{E}}$) die Inklusion „ \supseteq “ in (vi) zu zeigen.

Sei also $m \in (-(\mathcal{Z} \setminus \{1\}) + p^l + 2) \cup \{sp^{k-n+1} + 2 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1_0}\}$. Wir überprüfen nun, ob m unter ψ ein Urbild hat.

1. Fall: Es gelte $m \in (-(\mathcal{Z} \setminus \{1\}) + p^l + 2)$.

Dann gilt $m \neq 1$ und es existiert $z \in \mathcal{Z} \setminus \{1\}$ mit $m = p^l - z + 2$. Es gilt wegen $\max \mathcal{Z} = p^{l-n}$

$$m\psi_2^{-1} = p^l - z + 2 + p^{l-n} - 1 = p^l + p^{l-n} - z + 1 > p^l.$$

Ist $z = p^l$ (im Fall $n = 0$), das heißt $m = 2$, und wäre $r \in \underline{p^l}$ mit $r\psi_1 = 2$, so wäre $r = p^{\nu(r)+l-k}$. Dies ist wegen $l > k$ nicht möglich. Andernfalls gilt $z < p^l$ und wegen $\nu(p^l - z + p^{\nu(z)+l-k}) \stackrel{l \geq k}{=} \nu(z)$ gilt dann

$$(p^l - z + p^{\nu(z)+l-k})\psi_1 = m.$$

Aus der Definition von \mathcal{Z} folgt $z < p^{\nu(z)+l-k}$ und damit $p^l - z + p^{\nu(z)+l-k} > p^l$. Wir erhalten aufgrund der Injektivität von ψ_1 beziehungsweise ψ_2 daher $m\psi^- = \emptyset$.

2. Fall: Es gelte $m \in \{sp^{k-n+1} + 2 \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1_0}\}$.

Dann gilt $m \neq 1$ und es existiert $r \in \underline{p^{l+n-k-1} - p^{l-k-1} - 1_0}$ mit $m = rp^{k-n+1} + 2$. Es gilt

$$m\psi_2^{-1} = rp^{k-n+1} + 2 + p^{l-n} - 1 = rp^{k-n+1} + p^{l-n} + 1 =: \check{m}.$$

Wegen $n \leq k < l$ gilt $\nu(\check{m}) = 0$. Es folgt

$$\check{m}\psi_2 = m = rp^{k-n+1} + 2 \stackrel{n \leq k}{<} rp^{k-n+1} + p^{l-n} + 1 - p^{l-k} + 2 = \check{m} - p^{l-k} + 2 = \check{m}\psi_1.$$

Setzen wir hingegen $\dot{m} := rp^{k-n+1} + p^{\nu(r)+l-n+1}$, so erhalten wir $\dot{m}\psi_1 = m$ wegen $\nu(\dot{m}) = \nu(r) + k - n + 1$, aber

$$\dot{m}\psi_1 = m = rp^{k-n+1} + 2 \stackrel{n < l}{<} rp^{k-n+1} + p^{\nu(r)+l-n+1} - p^{l-n} + 1 = \dot{m}\psi_2.$$

In beiden Fällen folgt aufgrund der Injektivität von ψ_2 beziehungsweise der Injektivität von ψ_1 aus der Definition von ψ : $m\psi^- = \emptyset$. Damit sind (vi) und (vii) bewiesen.

Es gilt $|\tilde{\mathcal{D}}| = |\mathcal{D}|$ aufgrund von (ii), (viii) und der Injektivität von ψ_2 . Folglich erhalten wir

$$|\tilde{\mathcal{E}}| \stackrel{(v)}{=} p^l - 1 - |\tilde{\mathcal{D}}| - |\tilde{\mathcal{K}}| \stackrel{(1.1)}{=} p^l - |\mathcal{Z}| - 2|\tilde{\mathcal{D}}|.$$

und damit Aussage (ix).

Ist nun $n > k$, so folgen die Aussagen (x) und (xi) unmittelbar aus den Definitionen von \mathcal{Z} und \mathcal{D} unter Verwendung der ersten beiden Aussagen dieses Lemmas.

Aussage (xii) folgt aus (xi) und $\mathcal{Z} \cup \mathcal{D} = \underline{p}$.

Der letzte Teil (xiii) folgt aus (x) und (xi). □

1.3 Grundprinzip unserer Vorgehensweise

Wir schildern im Folgenden die Idee, die uns für die Bestimmung der aufsteigenden Zentralreihe während der gesamten Arbeit begleiten wird.

Seien G eine Gruppe, $n \in \mathbb{N}$ mit $|\gamma_2(G)| = n$, $\gamma_2(G) = \{x_1, \dots, x_n\}$, $g \in G$, K ein Körper, $\lambda_1, \dots, \lambda_n \in K$ und $m \in \mathbb{N}$. Sei $w := \sum_{i=1}^n \lambda_i x_i$. Dann gilt $gw - \sum_{i=1}^n \lambda_i 1_G \in \text{Aug}(KG)$ und wir erhalten für alle $h \in G$:

$$\begin{aligned} \left[gw - \sum_{i=1}^n \lambda_i 1_G, h - 1_G \right]_{\mathfrak{L}} &= \left[g \sum_{i=1}^n \lambda_i x_i, h \right]_{\mathfrak{L}} \\ &= \sum_{i=1}^n \lambda_i [gx_i, h]_{\mathfrak{L}} \\ &= h \sum_{i=1}^n \lambda_i ((gx_i)^h - gx_i) \\ &= h \sum_{i=1}^n \lambda_i (g^h x_i^h - gx_i) \\ &= h \sum_{i=1}^n \lambda_i (g[g, h]_{\mathfrak{S}} x_i^h - gx_i) \\ &= hg \left([g, h]_{\mathfrak{S}} \sum_{i=1}^n \lambda_i x_i^h - \sum_{i=1}^n \lambda_i x_i \right) \\ &= hg \left([g, h]_{\mathfrak{S}} w^h - w \right). \end{aligned}$$

1 Grundlagen

Da $\{h - 1_G \mid h \in G \setminus \{1_G\}\}$ eine K -Basis von $\text{Aug}(KG)$ ist, folgt

$$gw - \sum_{i=1}^n \lambda_i 1_G \in \mathcal{L}_m(\text{Aug}(KG))$$

genau dann, wenn für alle $h \in G$ gilt:

$$hg[g, h]_{\mathfrak{G}} w^h \equiv_{\mathcal{L}_{m-1}(\text{Aug}(KG))} hgw$$

Umgekehrt reicht es für den Nachweis von $gw - \sum_{i=1}^n \lambda_i 1_G \notin \mathcal{L}_m(\text{Aug}(KG))$ natürlich, ein $h \in G$ zu finden, so dass gilt:

$$hg[g, h]_{\mathfrak{G}} w^h \not\equiv_{\mathcal{L}_{m-1}(\text{Aug}(KG))} hgw$$

Anmerkung

In unseren Anwendungen dieses Leitgedankens in den folgenden Kapiteln begegnen wir häufig dem Fall, dass $\sum_{i=1}^n \lambda_i = 0_K$ gilt.

2 p-Gruppen mit zyklischer Kommutatoruntergruppe

Ziel dieses Kapitels ist es, die Dimensionen der in der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ auftretenden Faktorräume für eine p -Gruppe G und einem Körper K mit $\text{char } K = p$ im Falle einer zyklischen Kommutatoruntergruppe $\gamma_2(G)$ zu bestimmen, wobei wir zusätzlich $\gamma_3(G) \leq \gamma_2(G)^4$ annehmen. Man beachte hierbei, dass die Bedingung an $\gamma_2(G)$ im Fall $p > 2$ stets erfüllt ist.

2.1 Die Kommutatoruntergruppe und Konjugiertenklassen

In diesem Abschnitt stellen wir Aussagen über p -Gruppen G mit zyklischer Kommutatoruntergruppe vor, die für die Bestimmung der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ von Bedeutung sind. Hierbei spielen in erster Linie Resultate über die Kommutatoruntergruppe selbst sowie über Konjugiertenklassen eine Rolle.

Folgendes Lemma findet sich beispielsweise in [10] und verifiziert man durch einen Induktionsbeweis nach n .

2.1 Lemma. *Sei G eine Gruppe und $\gamma_2(G)$ abelsch. Dann gilt*

$$[g, h^n]_{\mathfrak{G}} = \prod_{i=1}^n [g, \underbrace{h, \dots, h}_i]_{\mathfrak{G}}^{(n)_i}$$

für alle $g, h \in G$ und $n \in \mathbb{N}$. □

2.2 Lemma. *Sei G eine Gruppe. Dann gilt für alle $n \in \mathbb{N}$ und $g_1, \dots, g_n, h \in G$:*

$$[g_1 \cdots g_n, h]_{\mathfrak{G}} = [g_1, h]_{\mathfrak{G}}^{g_2 \cdots g_n} [g_2, h]_{\mathfrak{G}}^{g_3 \cdots g_n} \cdots [g_n, h]_{\mathfrak{G}}$$

und

$$[h, g_1 \cdots g_n]_{\mathfrak{G}} = [h, g_n]_{\mathfrak{G}} [h, g_{n-1}]_{\mathfrak{G}}^{g_n} \cdots [h, g_1]_{\mathfrak{G}}^{g_2 \cdots g_n}.$$

Beweis. Ein einfacher Induktionsbeweis nach n liefert die Behauptung. □

Eine unmittelbare Folgerung ist die folgende Bemerkung [11, Kapitel III, § 1., 1.3].

2.2.1 Bemerkung. Sind $g, h \in G$ mit $g \in C_G([g, h]_{\mathfrak{G}})$, so gilt

$$[g^n, h]_{\mathfrak{G}} = [g, h]_{\mathfrak{G}}^n \text{ und } [h, g^n]_{\mathfrak{G}} = [h, g]_{\mathfrak{G}}^n$$

für alle $n \in \mathbb{N}_0$. □

Für einen Beweis des folgenden Lemmas verweisen wir auf [10] oder [7].

2.3 Lemma. Seien G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $g, h \in G$ mit $h \notin C_G(g)$ und es gelte $[\gamma_2(G), \{g\}]_{\mathfrak{G}} \leq \gamma_2(G)^4$. Dann gilt

$$\frac{|\langle [g, h]_{\mathfrak{G}} \rangle|}{|\langle [g^p, h]_{\mathfrak{G}} \rangle|} = p.$$

□

2.3.1 Bemerkung. Sei $g \notin \mathcal{Z}(G)$ und $\gamma_3(G) \leq \gamma_2(G)^4$. Dann gilt

$$\frac{|[\{g\}, G]_{\mathfrak{G}}|}{|[\{g^p\}, G]_{\mathfrak{G}}|} = p.$$

Beweis. Da $g \notin \mathcal{Z}(G)$ und $\gamma_2(G)$ zyklisch ist, existiert $b \in G$, $b \notin C_G(g)$ mit $\langle [g, b]_{\mathfrak{G}} \rangle = [\{g\}, G]_{\mathfrak{G}}$. Nach Lemma 2.3 gilt außerdem $\frac{|\langle [g, b]_{\mathfrak{G}} \rangle|}{|\langle [g^p, b]_{\mathfrak{G}} \rangle|} = p$. Sei $c \in G$. Gilt $c \in C_G(g^p)$, so folgt $\langle [g^p, c]_{\mathfrak{G}} \rangle = \{1_G\} < [\{g\}, G]_{\mathfrak{G}}$. Gilt $c \notin C_G(g^p)$, so gilt auch $c \notin C_G(g)$ und aus 2.3 folgt $\langle [g^p, c]_{\mathfrak{G}} \rangle < \langle [g, c]_{\mathfrak{G}} \rangle \leq [\{g\}, G]_{\mathfrak{G}}$. In beiden Fällen ist $[g^p, c]_{\mathfrak{G}}$ also Element der maximalen Untergruppe $\langle [g^p, b]_{\mathfrak{G}} \rangle$ von $[\{g\}, G]_{\mathfrak{G}}$. Hieraus erhalten wir $\langle [g^p, b]_{\mathfrak{G}} \rangle = [\{g^p\}, G]_{\mathfrak{G}}$. □

2.4 Lemma. Sei G eine endliche Gruppe und $n \in \mathbb{N}$ mit $ggT(n, |G|) = 1$. Dann ist die Abbildung

$$\varphi : G \rightarrow G, \quad g \mapsto g^n$$

bijektiv.

Beweis. Sei $m \in \mathbb{N}$ mit $mn \equiv 1 \pmod{|G|}$ und $\psi : G \rightarrow G$, $g \mapsto g^m$. Dann gilt $\varphi\psi = id_G = \psi\varphi$. □

2.5 Lemma. Sei G eine Gruppe, $N \trianglelefteq G$, N zyklisch und endlich.

Dann gilt $H \trianglelefteq G$ für alle $H \leq N$.

Beweis. Da es zu jedem Teiler von $|N|$ genau eine Untergruppe von N gibt, folgt die Behauptung unmittelbar aus der Normalteilereigenschaft von N . □

2.6 Korollar. Seien G eine endliche Gruppe, $g, h \in G$ mit $G = \langle g, h \rangle$ und $\gamma_2(G)$ zyklisch. Dann ist

$$\gamma_2(G) = \langle [g, h]_{\mathfrak{G}} \rangle.$$

Beweis. Nach Lemma 2.5 gilt $\langle [g, h]_{\mathfrak{G}} \rangle \trianglelefteq G$ und es folgt aus Lemma 2.2:

$$[x_1 \cdots x_m, y_1 \cdots y_n]_{\mathfrak{G}} \in \langle [g, h]_{\mathfrak{G}} \rangle \text{ für alle } m, n \in \mathbb{N} \text{ und } x_1, \dots, x_m, y_1, \dots, y_n \in \{g, h\}.$$

□

Der folgende Satz aus [10] führt zu zahlreichen nützlichen Folgerungen. Er zeigt unter anderem, dass im Fall $\gamma_3(G) \leq \gamma_2(G)^4$ jedes Element der Kommutatoruntergruppe ein Kommutator von geeigneten Gruppenelementen ist.

2.7 Satz. *Seien G eine p -Gruppe und $g, h \in G$ mit $\langle [g, h]_{\mathfrak{G}} \rangle = \gamma_2(G)$. Es sind äquivalent:*

$$(i) \quad \gamma_2(G) = \{[g, h^k]_{\mathfrak{G}} \mid k \in \mathbb{N}_0\}$$

$$(ii) \quad [\gamma_2(G), \{h\}]_{\mathfrak{G}} \leq \gamma_2(G)^4$$

Beweis. Wir geben einen elementaren Beweis der für uns wichtigeren Implikation (ii) \Rightarrow (i) an: Sei $[\gamma_2(G), \{h\}]_{\mathfrak{G}} \leq \gamma_2(G)^4$, $l \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$ und $a := [g, h]_{\mathfrak{G}}$. Dann existiert $r \in \underline{p^l - 1}_0$, $p \mid r$ mit $a^h = a[a, h]_{\mathfrak{G}} = a^{1+r}$. Wir setzen $c := 1 + r$. Insbesondere gilt $c \in E(\mathbb{Z}/p^l\mathbb{Z})$. Für alle $n \in \mathbb{N}_0$ gilt

$$[g, h^n]_{\mathfrak{G}} \stackrel{2.2}{=} [g, h]_{\mathfrak{G}} [g, h]_{\mathfrak{G}}^h \cdots [g, h]_{\mathfrak{G}}^{h^{n-1}} = a^{1+c+\dots+c^{n-1}} = a^{\sum_{i=0}^{n-1} c^i}.$$

Zu zeigen ist also $\sum_{i=0}^{n-1} c^i \not\equiv \sum_{i=0}^{\tilde{n}-1} c^i \pmod{p^l}$ für alle $n, \tilde{n} \in \underline{p^l - 1}_0$ mit $n \neq \tilde{n}$. Für alle $n, \tilde{n} \in \mathbb{N}_0$, $n > \tilde{n}$ gilt:

$$\sum_{i=0}^{n-1} c^i \not\equiv \sum_{i=0}^{\tilde{n}-1} c^i \pmod{p^l} \iff \sum_{i=\tilde{n}}^{n-1} c^i \not\equiv 0 \pmod{p^l} \iff c^{\tilde{n}} \sum_{i=0}^{n-\tilde{n}-1} c^i \not\equiv 0 \pmod{p^l} \iff \sum_{i=0}^{n-\tilde{n}-1} c^i \not\equiv 0 \pmod{p^l}.$$

Es reicht also zu zeigen: Für alle $n \in \underline{p^l - 2}_0$ gilt: $\sum_{i=0}^n c^i \not\equiv 0 \pmod{p^l}$.

Sei $n \in \underline{p^l - 2}_0$. Dann gilt

$$\begin{aligned} \sum_{s=0}^n c^s &= \sum_{s=0}^n (1+r)^s = \sum_{s=0}^n \left(\sum_{i=0}^s \binom{s}{i} r^i \right) = \sum_{i=0}^n \left(\sum_{s=0}^n \binom{s}{i} \right) r^i \\ &= \sum_{i=0}^n \binom{n+1}{i+1} r^i = (n+1) + \sum_{i=1}^n \binom{n+1}{i+1} r^i. \end{aligned}$$

Es gilt $\nu(n+1) < l$. Ist $r = 0$, so folgt die Behauptung unmittelbar. Wir nehmen daher $r > 0$ an. Nach Wahl von r gilt dann insbesondere $\nu(r) > 0$. Außerdem erhalten wir:

$$(*) \quad \text{Es gilt } i\nu(r) > \nu(i+1) \text{ für alle } i \in \mathbb{N}.$$

Denn: Sei $i \in \mathbb{N}$. Ist $p > 2$ oder $i > 1$, so gilt offenbar $i > \nu(i+1)$. Ist aber $p = 2$ und $i = 1$, so gilt wegen $[\gamma_2(G), \{h\}]_{\mathfrak{S}} \leq \gamma_2(G)^4$ und $\nu(r) > 0$ dann $\nu(r) > 1 = \nu(2)$.

Ist nun $i \in \underline{n}$, so gilt

$$\begin{aligned} \nu \left(\binom{n+1}{i+1} r^i \right) &= \nu(n+1) - \nu(i+1) + \nu \left(\binom{n}{i} \right) + i\nu(r) \\ &\stackrel{(*)}{>} \nu(n+1) + \nu \left(\binom{n}{i} \right) \geq \nu(n+1). \end{aligned}$$

Hieraus folgt $\nu \left(\sum_{s=0}^n c^s \right) = \nu \left((n+1) + \sum_{i=1}^n \binom{n+1}{i+1} r^i \right) = \nu(n+1) < l$. \square

2.7.1 Bemerkung. Sei $n \in \mathbb{N}$, $p \nmid n$ und es gelte $\gamma_2(G) = \{[g, h^k]_{\mathfrak{S}} \mid k \in \mathbb{N}_0\}$. Dann gilt:

- (i) $x^G = \{h^{-k} x h^k \mid k \in \mathbb{N}_0\}$ für alle $x \in \{g, hg, gh, g^n\}$.
- (ii) g^G , $(hg)^G$, $(gh)^G$ und $(g^n)^G$ sind extremale Konjugiertenklassen.
- (iii) Ist $[\gamma_2(G), \{g\}]_{\mathfrak{S}} \leq \gamma_2(G)^4$, so sind zusätzlich h^G und $(h^n)^G$ extremale Konjugiertenklassen.

Beweis. Es gilt

$$\begin{aligned} g\gamma_2(G) &= g \{[g, h^k]_{\mathfrak{S}} \mid k \in \mathbb{N}_0\} = \{h^{-k} g h^k \mid k \in \mathbb{N}_0\} \subseteq g^G, \\ hg\gamma_2(G) &= hg \{[g, h^k]_{\mathfrak{S}} \mid k \in \mathbb{N}_0\} = \{h^{-(k-1)} g h h^{k-1} \mid k \in \mathbb{N}_0\} \subseteq (gh)^G = (hg)^G \end{aligned}$$

und damit mit Lemma 1.17 auch jeweils Gleichheit. Die Abbildung $\psi : g^G \rightarrow G$, $x \mapsto x^n$ ist nach Lemma 2.4 injektiv und da $(g^n)^G = (g^G)^n$ gilt und g^G eine extremale Konjugiertenklasse ist, folgen hieraus die ersten beiden Aussagen.

Ist nun die Voraussetzung von (iii) erfüllt, so folgt $\gamma_2(G) = \{[h, g^k]_{\mathfrak{S}} \mid k \in \mathbb{N}_0\}$ aus Satz 2.7 und damit das Behauptete aus (i) durch Vertauschen der Rollen von g und h . \square

2.7.2 Bemerkung. Gilt $\gamma_3(G) \leq \gamma_2(G)^4$, so ist die Menge der extremalen Elemente von G nicht leer.

Beweis. Die Aussage folgt direkt aus Satz 2.7 und Bemerkung 2.7.1 (ii). \square

2.8 Korollar.

Seien G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $g, h \in G$ und $[\gamma_2(G), \{h\}]_{\mathfrak{S}} \leq \gamma_2(G)^4$. Dann gilt

$$\gamma_2(\langle g, h \rangle) = \{[g, h^k]_{\mathfrak{S}} \mid k \in \mathbb{N}_0\}.$$

Beweis. Nach Korollar 2.6 gilt $\gamma_2(\langle g, h \rangle) = \langle [g, h]_{\mathfrak{G}} \rangle$. Sei $a \in G$ mit $\langle a \rangle = \gamma_2(G)$. Dann existiert $n \in \mathbb{N}_0$ mit $a^n = [g, h]_{\mathfrak{G}}$. Nach Voraussetzung gilt $[a, h]_{\mathfrak{G}} \in \langle a \rangle^4$. Für alle $m \in \mathbb{N}_0$ gilt

$$[a^m, h]_{\mathfrak{G}} \stackrel{2.2.1}{=} [a, h]_{\mathfrak{G}}^m \in \langle a \rangle^{4m} = \langle a^{4m} \rangle = \langle a^m \rangle^4.$$

Es folgt

$$[\gamma_2(\langle g, h \rangle), \{h\}]_{\mathfrak{G}} = [\langle a^n \rangle, \{h\}]_{\mathfrak{G}} \leq \langle a^n \rangle^4 = \gamma_2(\langle g, h \rangle)^4.$$

Die Behauptung folgt aus Satz 2.7. □

2.9 Satz. Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$ und $l \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$. Sei $g \in G$ und $a \in G$ mit $\langle a \rangle = \gamma_2(G)$. Dann gilt:

$$(i) \text{ Es existiert } h \in G \text{ mit } g^G = g \langle a^{p^{l-\kappa(g)}} \rangle = g \{ [g, h^k]_{\mathfrak{G}} \mid k \in \mathbb{N}_0 \}.$$

$$(ii) \text{ Es existiert } h \in G \text{ mit } [\{g\}, G]_{\mathfrak{G}} = \langle a^{p^{l-\kappa(g)}} \rangle = \{ [g, h^k]_{\mathfrak{G}} \mid k \in \mathbb{N}_0 \}.$$

Insbesondere gilt:

$$(iii) |g^G| = |[\{g\}, G]_{\mathfrak{G}}|,$$

$$(iv) a^G = a \langle a^{\frac{|\gamma_2(G)|}{|\gamma_3(G)|}} \rangle \quad \text{und} \quad p^{\kappa(a)} = |a^G| = |\gamma_3(G)|.$$

Beweis. Nach Definition von $\kappa(g)$ gilt $p^{\kappa(g)} = |g^G|$. Wir wählen $h \in G$ derart, dass $o([g, h]_{\mathfrak{G}})$ maximal ist. Wir zeigen nun $g^G = g\gamma_2(\langle g, h \rangle)$.

Aufgrund der Maximalität von $o([g, h]_{\mathfrak{G}})$ (und da $\gamma_2(G)$ zyklische p -Gruppe ist) gilt

$$g^{\tilde{g}} = g[g, \tilde{g}]_{\mathfrak{G}} \in g \langle [g, h]_{\mathfrak{G}} \rangle \stackrel{2.6}{=} g\gamma_2(\langle g, h \rangle) \text{ für alle } \tilde{g} \in G.$$

Außerdem sind die Voraussetzungen von Korollar 2.8 erfüllt. Wir erhalten

$$g\gamma_2(\langle g, h \rangle) \stackrel{2.8}{=} g \{ [g, h^k]_{\mathfrak{G}} \mid k \in \mathbb{N}_0 \} \subseteq g^G$$

und damit $g^G = g\gamma_2(\langle g, h \rangle)$. Hieraus folgt $p^{\kappa(g)} = |\gamma_2(\langle g, h \rangle)|$, also $\gamma_2(\langle g, h \rangle) = \langle a^{p^{l-\kappa(g)}} \rangle$ und damit die erste Gleichheit in (i). Die zweite Gleichheit folgt nun direkt aus Korollar 2.8.

Die Aussage (ii) folgt aus (i) und die Aussage (iii) direkt aus (i) und (ii).

Aussage (iv) folgt aus folgender Gleichung:

$$\gamma_3(G) = [\gamma_2(G), G]_{\mathfrak{G}} \stackrel{2.2.1}{=} [\{a\}, G]_{\mathfrak{G}} \stackrel{(ii)}{=} \langle a^{p^{l-\kappa(a)}} \rangle.$$

□

2.10 Korollar. Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$, $g \in G$ und $m \in \mathbb{N}_0$. Dann gilt:

- (i) Ist $m \leq \kappa(g)$, so gilt $|(g^{p^m})^G| = p^{\kappa(g)-m}$.
- (ii) Ist $m \geq \kappa(g)$, so gilt $g^{p^m} \in \mathcal{Z}(G)$.
- (iii) Es gilt $h^{|\gamma_2(G)|} \in \mathcal{Z}(G)$ für alle $h \in G$.

Beweis. Wir zeigen (i) durch einen Induktionsbeweis nach m . Es gelte $m \leq \kappa(g)$. Ist $m = 0$, so ist (i) trivial. Sei nun $0 < m \leq \kappa(g)$. Dann gilt $0 \leq m-1 < \kappa(g)$. Induktiv folgt

$$|[\{g^{p^{m-1}}\}, G]_{\mathfrak{S}}| \stackrel{2.9}{=} |(g^{p^{m-1}})^G| = p^{\kappa(g)-(m-1)} > 1,$$

insbesondere also $g^{p^{m-1}} \notin \mathcal{Z}(G)$. Wir erhalten

$$|(g^{p^m})^G| \stackrel{2.9}{=} |[\{g^{p^m}\}, G]_{\mathfrak{S}}| = |[\{g^{p^{m-1}}\}, G]_{\mathfrak{S}}| \frac{|[\{g^{p^m}\}, G]_{\mathfrak{S}}|}{|[\{g^{p^{m-1}}\}, G]_{\mathfrak{S}}|} \stackrel{2.3.1}{=} p^{\kappa(g)-(m-1)} p^{-1} = p^{\kappa(g)-m},$$

also die Aussage (i).

Insbesondere gilt $|(g^{p^{\kappa(g)}})^G| = 1$, also $g^{p^{\kappa(g)}} \in \mathcal{Z}(G)$. Ist $m \geq \kappa(g)$, so folgt hieraus $g^{p^m} \in \mathcal{Z}(G)$ und damit (ii).

Da $h^G \subseteq h\gamma_2(G)$, also $p^{\kappa(h)} \leq |\gamma_2(G)|$ für alle $h \in G$ gilt, folgt (iii) unmittelbar aus (ii). \square

2.10.1 Bemerkung.

Sei $m \in \mathbb{N}$ und es gelte $\nu(m) \leq \kappa(g)$. Dann gilt $|(g^m)^G| = p^{\kappa(g)-\nu(m)}$.

Beweis. Sei $s \in \mathbb{N}$ mit $sp^{\nu(m)} = m$. Dann gilt $p \nmid s$. Wir erhalten

$$p^{\kappa(g)-\nu(m)} \stackrel{2.10}{=} |(g^{p^{\nu(m)}})^G| \stackrel{2.4}{=} |(g^{sp^{\nu(m)}})^G| = |(g^m)^G|.$$

\square

Das folgende Lemma werden wir im Anschluss nutzen, um $\mathcal{K}_H(G)$ für alle $H \in G/\gamma_2(G)$ zu bestimmen.

2.11 Lemma. Seien G eine p -Gruppe, $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$, $a \in G$ mit $\gamma_2(G) = \langle a \rangle$, $l, k \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$ und $|\gamma_3(G)| = p^k$. Weiter sei $H \in G/\gamma_2(G)$, $h \in \bigcup \mathcal{K}_{H, p^{\mu(H)}}(G)$ und $m \in \underline{p^l - 1}$. Dann gilt:

- (i) Genau dann gilt $\nu(m) \leq k - \mu(H)$, wenn $(ha^m)^G = ha^m \langle a^{p^{l-(k-\nu(m))}} \rangle$ gilt.
Insbesondere gilt $\nu(m) \leq k - \mu(H)$ genau dann, wenn $|(ha^m)^G| = p^{k-\nu(m)}$ gilt.

- (ii) Genau dann gilt $\nu(m) \geq k - \mu(H)$, wenn $(ha^m)^G = ha^m \langle a^{p^{l-\mu(H)}} \rangle$ gilt.
 Insbesondere gilt $\nu(m) \geq k - \mu(H)$ genau dann, wenn $|(ha^m)^G| = p^{\mu(H)}$ gilt.

Beweis. Sei $g \in G$ und $x \in \mathbb{N}$ mit $p^{\nu(m)}x = m$. Nach Definition von $\nu(m)$ gilt $p \nmid x$. Nach Voraussetzung gilt außerdem $\mu(H) = \kappa(h)$ und Satz 2.9 (iv) liefert $k = \kappa(a)$. Nach Satz 2.9 (ii) existieren folglich $r, s \in \mathbb{N}_0$ mit $[h, g]_{\mathfrak{G}} = a^{rp^{l-\mu(H)}}$ und $[a, g]_{\mathfrak{G}} = a^{sp^{l-k}}$. Es folgt

$$[ha^m, g]_{\mathfrak{G}} \stackrel{2.2}{=} [h, g]_{\mathfrak{G}}[a^m, g]_{\mathfrak{G}} \stackrel{2.2.1}{=} [h, g]_{\mathfrak{G}}[a, g]_{\mathfrak{G}}^m = a^{rp^{l-\mu(H)}} a^{msp^{l-k}} = a^{rp^{l-\mu(H)} + msp^{l-k}}.$$

Sei zunächst $\nu(m) < k - \mu(H)$. Insbesondere gilt dann $\mu(H) < k$ und es folgt

$$rp^{l-\mu(H)} + msp^{l-k} = p^{l-k+\nu(m)}(rp^{k-\mu(H)-\nu(m)} + sx),$$

das heißt $[\{ha^m\}, G]_{\mathfrak{G}} \subseteq \langle a^{p^{l-(k-\nu(m))}} \rangle$. Nach Satz 2.9 existiert \tilde{g} mit $[a, \tilde{g}]_{\mathfrak{G}} = a^{p^{l-k}}$. Aus $p \nmid x$ und $p \mid p^{k-\mu(H)-\nu(m)}$ folgt, dass ein Erzeuger von $\langle a^{p^{l-(k-\nu(m))}} \rangle$ auch Element von $[\{ha^m\}, G]_{\mathfrak{G}}$ ist. Hieraus folgt die andere Inklusion und mit Satz 2.9 erhalten wir darüber hinaus $|(ha^m)^G| = p^{k-\nu(m)}$. Wir haben also die Implikation „ \Rightarrow “ in (i) für den Fall $\nu(m) < k - \mu(H)$ und damit wegen $\mu(H) \neq k - \nu(m)$ gleichzeitig die Implikation „ \Leftarrow “ in (ii) bewiesen.

Sei nun $\nu(m) \geq k - \mu(H)$. Dies ist insbesondere erfüllt, falls $\mu(H) \geq k$ gilt. Dann gilt

$$rp^{l-\mu(H)} + msp^{l-k} = p^{l-\mu(H)}(r + sxp^{\nu(m)-(k-\mu(H))}), \text{ also } [\{ha^m\}, G]_{\mathfrak{G}} \subseteq \langle a^{p^{l-\mu(H)}} \rangle.$$

Aus der Minimalität von $\mu(H)$ folgt mit Satz 2.9 aber auch $\langle a^{p^{l-\mu(H)}} \rangle \subseteq [\{ha^m\}, G]_{\mathfrak{G}}$ und somit die noch zu beweisenden Implikationen. Insbesondere folgt auch die Implikation „ \Rightarrow “ in (i) für den Fall $\nu(m) = k - \mu(H)$. \square

2.12 Satz. Seien G eine p -Gruppe, $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$, $l, k \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$, $|\gamma_3(G)| = p^k$ und $H \in G/\gamma_2(G)$. Es gelten die folgenden Aussagen:

- (i) Ist $\mu(H) \leq k$, so ist H die disjunkte Vereinigung von p^{l-k} Konjugiertenklassen der Länge $p^{\mu(H)}$ und $(p-1)p^{l-k-1}$ der Länge $p^{\mu(H)+j}$ für alle $j \in \underline{k - \mu(H)}$.
- (ii) Ist $\mu(H) \geq k$, so ist H die disjunkte Vereinigung von $p^{l-\mu(H)}$ Konjugiertenklassen der Länge $p^{\mu(H)}$.
- (iii) Insbesondere gilt $\mathcal{Z}(G) \cap \gamma_2(G) = \langle a^{p^k} \rangle$ für alle $a \in G$ mit $\langle a \rangle = \gamma_2(G)$.

2 p -Gruppen mit zyklischer Kommutatoruntergruppe

Beweis. (i): Sei $n := \mu(H)$ und $n < k$. Insbesondere gilt dann $0 < k < l$. Sei $j \in \underline{k-n}$, $h \in \bigcup \mathcal{K}_{H,p^n}(G)$ und $a \in G$ mit $\langle a \rangle = \gamma_2(G)$. Es gilt

$$\begin{aligned} \mathcal{K}_{H,p^{n+j}}(G) &= \left\{ (ha^m)^G \mid m \in \underline{p^l-1}, |(ha^m)^G| = p^{n+j} \right\} \\ &\stackrel{2.9}{=} \left\{ (ha^m)^G \mid m \in \underline{p^{l-n-j}-1}, |(ha^m)^G| = p^{n+j} = p^{k-(k-n-j)} \right\} \\ &\stackrel{2.11}{=} \left\{ (ha^m)^G \mid m \in \underline{p^{l-n-j}-1}, \nu(m) = k-n-j \right\}, \text{ denn:} \end{aligned}$$

Ist $m \in \underline{p^{l-(n+j)}-1}$ mit $|(ha^m)^G| = p^{n+j}$, so gilt wegen $j > 0$ also $|(ha^m)^G| \neq p^n$, nach Lemma 2.11 damit $|(ha^m)^G| = p^{k-\nu(m)}$. Dies liefert die Inklusion „ \subseteq “ der letzten Gleichheit. Die Inklusion „ \supseteq “ folgt wegen $k-n-j < k-n$ ebenfalls aus Lemma 2.11.

Sei $N := \{m \mid m \in \underline{p^{l-n-j}-1}, \nu(m) = k-n-j\}$. Aus Satz 2.9 folgt $(ha^m)^G \neq (ha^{\tilde{m}})^G$ für alle $m, \tilde{m} \in N$ mit $m \neq \tilde{m}$. Daher gilt

$$|\mathcal{K}_{H,p^{n+j}}(G)| = |\{(ha^m)^G \mid m \in N\}| = |N|.$$

Es ist $|N|$ die Anzahl der Erzeuger der zyklischen Gruppe $C_{p^{l-n-j}}/C_{p^{k-n-j}}$. Wegen $C_{p^{l-n-j}}/C_{p^{k-n-j}} \cong C_{p^{l-k}}$ folgt

$$(*) \quad |N| = {}^1\varphi(p^{l-k}) = (p-1)p^{l-k-1}.$$

Aus Lemma 2.11 erhalten wir, dass es in H nur Konjugiertenklassen der Längen $n, n+1, \dots, k$ geben kann. $(*)$ liefert folglich

$$\begin{aligned} \left| \left\{ \tilde{h} \in H \mid |\tilde{h}^G| = p^n \right\} \right| &= |H| - (p-1)p^{l-k-1} \sum_{i=1}^{k-n} p^{n+i} \\ &= p^l - (p-1)p^{l-k+n} \sum_{i=0}^{k-n-1} p^i \\ &= p^l - (p-1)p^{l-k+n}(p^{k-n} - 1)(p-1)^{-1} \\ &= p^l - p^{l-k+n}(p^{k-n} - 1) \\ &= p^{l-k+n}. \end{aligned}$$

Also gibt es genau p^{l-k} in H enthaltene Konjugiertenklassen der Länge p^n . Hieraus folgt (i) im Fall $\mu(H) < k$.

Die Aussage (i) im Fall $\mu(H) = k$ und die Aussage (ii) folgen direkt aus Lemma 2.11 (ii), da $\nu(m) \geq k - \mu(H)$ für alle $m \in \underline{p^l-1}$ im Fall $\mu(H) \geq k$ gilt.

(iii): Es gilt $\mathcal{Z}(G) = \{g \mid g \in G, |g^G| = 1\}$ und $\mu(\gamma_2(G)) = 0$. Wir betrachten den Spezialfall $H := \gamma_2(G)$. Die Behauptung folgt im Fall $k = 0$ aus (ii) und im Fall $k > 0$ aus (i). \square

¹ φ bezeichne hier die Eulersche φ -Funktion.

Satz 2.9 motiviert die folgende Definition:

2.13 Definition. Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$, $a \in G$ mit $\gamma_2(G) = \langle a \rangle$ und $l \in \mathbb{N}_0$ mit $p^l = |\gamma_2(G)|$. Für alle $g, h \in G$ sei $\omega_a(g, h) \in \underline{p^{\kappa(g)} - 1}_0$ das (nach Satz 2.9 eindeutig bestimmte) Element mit

$$a^{-\omega_a(g, h)p^{l-\kappa(g)}} = [g, h]_{\mathfrak{G}}.$$

Besteht über a kein Zweifel, so schreiben wir auch kurz $\omega(g, h)$ statt $\omega_a(g, h)$.

Für alle $g \in G$ sei

- (i) $\omega_{(a, g)} : G \rightarrow \mathbb{Z}/p^{\kappa(g)}\mathbb{Z}, \quad h \mapsto \omega_a(g, h) + p^{\kappa(g)}\mathbb{Z},$
- (ii) $\overline{\omega_{(a, g)}} := \overline{\omega_a(g, \cdot)} : G \rightarrow \mathbb{Z}/p\mathbb{Z}, \quad h \mapsto \omega_a(g, h) + p\mathbb{Z}$

und ω_g beziehungsweise $\overline{\omega_g}$ im Falle der zweifelsfreien Kenntnis über a die zugehörigen Kurzschreibweisen.

2.13.1 Bemerkung.

Sei $k \in \mathbb{N}_0$ mit $|\gamma_3(G)| = p^k$ und $g \in G$.

- (i) Sei $\kappa(g) \leq k$. Dann ist $\omega_g : G \rightarrow (\mathbb{Z}/p^{\kappa(g)}\mathbb{Z}; +)$ ein ²Kozyklus von G in $(\mathbb{Z}/p^{\kappa(g)}\mathbb{Z}; +)$, wobei die zugehörige Operation f durch

$$f : G \rightarrow \mathcal{S}_{\mathbb{Z}/p^{\kappa(g)}\mathbb{Z}}, \quad h \mapsto \left[\begin{array}{l} \mathbb{Z}/p^{\kappa(g)}\mathbb{Z} \rightarrow \mathbb{Z}/p^{\kappa(g)}\mathbb{Z} \\ r \mapsto r(1 - \omega_a(a, h)p^{l-k}) \end{array} \right]$$

gegeben ist.

Es gilt $\text{Kern } \omega_{(a, g)} = C_G(g)$.

Ist insbesondere $b \in G$ mit $\gamma_2(G) = \langle b \rangle$, so gilt $\text{Kern } \omega_{(a, g)} = \text{Kern } \omega_{(b, g)}$.

- (ii) Es ist $\overline{\omega_g} : G \rightarrow (\mathbb{Z}/p\mathbb{Z}; +)$ ein Gruppen-Homomorphismus. Gilt dabei $g \notin \mathcal{Z}(G)$, so ist $\overline{\omega_g}$ surjektiv.

- (iii) Ist $g \notin \mathcal{Z}(G)$, so gilt für alle $h \in G$:

$$[\{g\}, G]_{\mathfrak{G}} = \langle [g, h]_{\mathfrak{G}} \rangle \iff h \notin \text{Kern } \overline{\omega_g}.$$

²Seien G, H Gruppen und G operiere auf H vermöge f . Eine Abbildung $\omega : G \rightarrow H$ heißt Kozyklus von G in H , falls für alle $g, \tilde{g} \in G$ gilt: $(g\tilde{g})\omega = (g\omega)(\tilde{g}f)(\tilde{g}\omega)$

2 p -Gruppen mit zyklischer Kommutatoruntergruppe

Beweis. Seien $g, h, \tilde{h} \in G$. Es gilt

$$\begin{aligned}
 a^{-\omega(g, h\tilde{h})p^{l-\kappa(g)}} &= [g, h\tilde{h}]_{\mathfrak{G}} \\
 &\stackrel{2.2}{=} [g, \tilde{h}]_{\mathfrak{G}} [g, h]_{\mathfrak{G}}^{\tilde{h}} \\
 &= a^{-\omega(g, \tilde{h})p^{l-\kappa(g)}} (a^{-\omega(g, h)p^{l-\kappa(g)}})^{\tilde{h}} \\
 &= a^{-\omega(g, \tilde{h})p^{l-\kappa(g)}} (a[a, \tilde{h}]_{\mathfrak{G}})^{-\omega(g, h)p^{l-\kappa(g)}} \\
 &\stackrel{k=\kappa(a)}{=} a^{-\omega(g, \tilde{h})p^{l-\kappa(g)}} a^{(1-\omega(a, \tilde{h})p^{l-k})(-\omega(g, h)p^{l-\kappa(g)})} \\
 &= a^{(-\omega(g, \tilde{h})-\omega(g, h)(1-\omega(a, \tilde{h})p^{l-k}))p^{l-\kappa(g)}}.
 \end{aligned}$$

Da $a^{p^{l-\kappa(g)}}$ ein Element der Ordnung $p^{\kappa(g)}$ ist, folgt

$$\begin{aligned}
 (*) \quad -\omega(g, h\tilde{h}) &\equiv_{p^{\kappa(g)}} -\omega(g, \tilde{h}) - \omega(g, h)(1 - \omega(a, \tilde{h})p^{l-k}) \\
 &= -\omega(g, h) - \omega(g, \tilde{h}) + \omega(g, h)\omega(a, \tilde{h})p^{l-k}.
 \end{aligned}$$

Insbesondere gilt

$$\begin{aligned}
 1 - \omega(a, h\tilde{h})p^{l-k} &\equiv_{p^{\kappa(a)}} 1 - \omega(a, h)p^{l-k} - \omega(a, \tilde{h})p^{l-k} + \omega(a, h)\omega(a, \tilde{h})p^{2(l-k)} \\
 &= (1 - \omega(a, h)p^{l-k})(1 - \omega(a, \tilde{h})p^{l-k}).
 \end{aligned}$$

(i): Ist $\kappa(g) \leq k = \kappa(a)$, so folgt hieraus $(h\tilde{h})f = (hf)(\tilde{h}f)$ nach Definition von f . Also ist f in diesem Fall eine Operation von G auf $\mathbb{Z}/p^{\kappa(g)}\mathbb{Z}$ und es gilt

$$\begin{aligned}
 (h\tilde{h})\omega_g &= \omega(g, h\tilde{h}) + p^{\kappa(g)}\mathbb{Z} \\
 &\stackrel{(*)}{=} \omega(g, h) + \omega(g, \tilde{h}) - \omega(g, h)\omega(a, \tilde{h})p^{l-k} + p^{\kappa(g)}\mathbb{Z} \\
 &= h\omega_g(\tilde{h}f) + \tilde{h}\omega_g.
 \end{aligned}$$

Also ist ω_g ein Kozyklus von G in $(\mathbb{Z}/p^{\kappa(g)}\mathbb{Z}; +)$.

Weiter gilt

$$h \in \text{Kern } \omega_g \iff \omega(g, h) = 0 \iff h \in C_G(g),$$

woraus (i) folgt.

(ii): Ist $g \in \mathcal{Z}(G)$, so ist $\omega(g, h) = 0$ und damit $\overline{\omega_g} = 0_{(\mathbb{Z}/p\mathbb{Z})^G}$. Es gelte nun $g \notin \mathcal{Z}(G)$. Dann gilt $\kappa(g) > 0$ und G ist eine nicht-abelsche p -Gruppe. Folglich gilt $l - k \geq 1$ und (*) liefert

$$\omega(g, h\tilde{h}) \equiv_p \omega(g, h) + \omega(g, \tilde{h}).$$

Also ist $\overline{\omega_g}$ ein Gruppen-Homomorphismus. Die Surjektivität folgt aus Satz 2.9. Damit ist (ii) bewiesen.

(iii): Nach Satz 2.9 gilt $[\{g\}, G]_{\mathfrak{G}} = \langle a^{-p^{l-\kappa(g)}} \rangle$. Es folgt

$$[g, h]_{\mathfrak{G}} < [\{g\}, G]_{\mathfrak{G}} \iff p \mid \omega(g, h) \iff h \in \text{Kern } \overline{\omega_g}.$$

□

Folgender Satz zeigt auf, dass p -Gruppen mit zyklischer Kommutatoruntergruppe eine interessante Normalreihe liefern:

2.14 Satz. *Sei G eine p -Gruppe und $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$. Für alle $n \in \mathbb{N}_0$ setzen wir $\mathcal{K}_{\leq n}(G) := \{C \mid C \in \mathcal{K}(G), |C| \leq p^n\}$. Dann gilt*

$$\bigcup \mathcal{K}_{\leq n}(G) \trianglelefteq G$$

für alle $n \in \mathbb{N}_0$. Insbesondere gilt:

Ist $h \in G$ extremal und $g \in G$ nicht extremal, so sind gh und hg extremal.

Beweis. Sei $n \in \mathbb{N}_0$ und $l \in \mathbb{N}_0$ mit $p^l = |\gamma_2(G)|$. Gilt dann $n \geq l$, so gilt $\bigcup \mathcal{K}_{\leq n}(G) = G$ nach Lemma 1.17. Wir nehmen nun $n < l$ an. Dann gilt $1_G \in \mathcal{Z}(G) = \bigcup \mathcal{K}_{\leq 0}(G) \subseteq \bigcup \mathcal{K}_{\leq n}(G)$. Seien $g, \tilde{g} \in \bigcup \mathcal{K}_{\leq n}(G)$ und $a \in G$ mit $\langle a \rangle = \gamma_2(G)$. Dann folgt aus Satz 2.9 für alle $h \in G$:

$$(g\tilde{g})^h = g^h \tilde{g}^h \in g \langle a^{p^{l-n}} \rangle \tilde{g} \langle a^{p^{l-n}} \rangle \stackrel{2.5}{=} g\tilde{g} \langle a^{p^{l-n}} \rangle,$$

also $g\tilde{g} \in \bigcup \mathcal{K}_{\leq n}(G)$. Da die Abgeschlossenheit bezüglich Konjugation trivial ist, folgt die Behauptung aus der Endlichkeit von G .

Ist $h \in G$ extremal und $g \in G$ nicht extremal, so gilt $h \notin \bigcup \mathcal{K}_{\leq l-1}(G)$ und $g \in \bigcup \mathcal{K}_{\leq l-1}(G)$, also $hg, gh \notin \bigcup \mathcal{K}_{\leq l-1}(G)$. \square

2.15 Korollar. *Sei G eine p -Gruppe und $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$. Dann gibt es mindestens $(p-1)\frac{|G|}{p}$ extremale Elemente in G und mindestens $(p-1)\frac{|G|}{p|\gamma_2(G)|}$ extremale Konjugiertenklassen in G .*

Beweis. Nach Bemerkung 2.7.2 ist die Menge der extremalen Elemente in G nicht leer. Nach Satz 2.14 ist dann das Komplement dieser Menge in G eine echte Untergruppe (beziehungsweise die leere Menge, falls G abelsch ist) von G , enthält also höchstens $\frac{|G|}{p}$ Elemente. Hieraus folgt der erste Teil der Behauptung. Der zweite Teil folgt aus der Definition der Extremalität. \square

Die in Satz 2.14 angegebenen Normalteiler von G lassen sich häufig genauer beschreiben:

2.16 Satz. *Seien G eine p -Gruppe, $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$ und $k, m \in \mathbb{N}_0$ mit $|\gamma_2(G) \cap \mathcal{Z}_k(G)| = p^m$. Dann gilt (mit den Bezeichnungen aus Satz 2.14):*

$$\mathcal{Z}_{k+1}(G) = \bigcup \mathcal{K}_{\leq m}(G).$$

Inbesondere gilt: Ist $cl(G) \geq 2$, so gilt für alle $c \in \underline{cl(G) - 1}$:

$$\gamma_2(G) \cap \mathcal{Z}_{c-1}(G) < \gamma_2(G) \cap \mathcal{Z}_c(G).$$

Beweis. Sei $a \in G$ mit $\langle a \rangle = \gamma_2(G)$ und $l \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$. Nach Voraussetzung gilt $\gamma_2(G) \cap \mathcal{Z}_k(G) = \langle a^{p^{l-m}} \rangle$. Für alle $g \in G$ sind folgende Aussagen äquivalent:

$$\begin{aligned} |g^G| \leq p^m &\stackrel{2.9}{\iff} \forall h \in G : [g, h]_{\mathfrak{G}} \in \langle a^{p^{l-m}} \rangle \\ &\iff g \in \mathcal{Z}_{k+1}(G) \end{aligned}$$

Also ist $\mathcal{Z}_{k+1}(G) = \bigcup \mathcal{K}_{\leq m}(G)$.

Sei $n := cl(G) \geq 2$ und $c \in \underline{n-1}$. Dann gilt $\mathcal{Z}_{c-1}(G) \subset \mathcal{Z}_c(G) \subset \mathcal{Z}_{c+1}(G)$. Sind dann $m_1, m_2 \in \mathbb{N}_0$ mit $|\gamma_2(G) \cap \mathcal{Z}_{c-1}(G)| = p^{m_1}$ und $|\gamma_2(G) \cap \mathcal{Z}_c(G)| = p^{m_2}$, so folgt aus dem Bewiesenen $\bigcup \mathcal{K}_{\leq m_1}(G) = \mathcal{Z}_c(G) \subset \mathcal{Z}_{c+1}(G) = \bigcup \mathcal{K}_{\leq m_2}(G)$ und damit $m_1 < m_2$. \square

2.17 Lemma. *Sei G eine p -Gruppe und $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$. Für alle $g \in G$ existiert dann $h \in G$ mit h extremal und $\langle [g, h]_{\mathfrak{G}} \rangle = [\{g\}, G]_{\mathfrak{G}}$.*

Beweis. Sei $g \in G$, $l \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$ und $a \in G$ mit $\gamma_2(G) = \langle a \rangle$. Wir zeigen die Behauptung durch Induktion nach l . Im Fall $l = 0$ ist die Behauptung trivial. Sei also $l > 0$ und die Behauptung für alle p -Gruppen H mit $\gamma_2(H)$ zyklisch, $\gamma_3(H) \leq \gamma_2(H)^4$ und $|\gamma_2(H)| < p^l$ als wahr angenommen.

1. Fall: Ist $g \in \mathcal{Z}(G)$, so folgt das Behauptete direkt aus Bemerkung 2.7.2.

2. Fall: Ist $|g^G| = p$, so ist G nicht abelsch und es gilt $|C_G(g)| = \frac{|G|}{p}$. Da die Voraussetzung von Korollar 2.15 erfüllt ist, gibt es mindestens $(p-1)\frac{|G|}{p}$ extremale Elemente in G . Wegen $1_G \in C_G(g)$ gibt es damit insbesondere auch im Fall $p = 2$ in $G \setminus C_G(g)$ extremale Elemente. Jedes dieser Elemente erfüllt das Behauptete.

3. Fall: Es gelte $|g^G| \geq p^2$. Wir setzen $\tilde{g} := a^{p^{l-1}}$. Dann gilt $|\langle \tilde{g} \rangle| = p$ und nach Lemma 2.5 außerdem $\langle \tilde{g} \rangle \trianglelefteq G$. Es ist $\gamma_2(G/\langle \tilde{g} \rangle) = \gamma_2(G)/\langle \tilde{g} \rangle$ zyklisch, $|\gamma_2(G/\langle \tilde{g} \rangle)| = p^{l-1}$ und

$$\gamma_3(G/\langle \tilde{g} \rangle) = \gamma_3(G)\langle \tilde{g} \rangle / \langle \tilde{g} \rangle \leq \gamma_2(G)^4 \langle \tilde{g} \rangle / \langle \tilde{g} \rangle = (\gamma_2(G)/\langle \tilde{g} \rangle)^4 = \gamma_2(G/\langle \tilde{g} \rangle)^4.$$

Für $g\langle \tilde{g} \rangle \in G/\langle \tilde{g} \rangle$ existiert also induktiv $h \in G$ mit $|h\langle \tilde{g} \rangle^{G/\langle \tilde{g} \rangle}| = p^{l-1}$ und

$$\langle [g, h]_{\mathfrak{G}} \rangle \langle \tilde{g} \rangle / \langle \tilde{g} \rangle = \langle [g\langle \tilde{g} \rangle, h\langle \tilde{g} \rangle]_{\mathfrak{G}} \rangle \stackrel{\text{Ind. vor.}}{=} [\{g\langle \tilde{g} \rangle\}, G/\langle \tilde{g} \rangle]_{\mathfrak{G}} = [\{g\}, G]_{\mathfrak{G}} \langle \tilde{g} \rangle / \langle \tilde{g} \rangle.$$

Mit $\langle \tilde{g} \rangle \leq [\{g\}, G]_{\mathfrak{G}}$ folgt hieraus $\langle [g, h]_{\mathfrak{G}} \rangle \langle \tilde{g} \rangle = [\{g\}, G]_{\mathfrak{G}}$. Wegen $|\{g\}, G]_{\mathfrak{G}}| \stackrel{2.9}{=} |g^G| \geq p^2$ erhalten wir $\langle [g, h]_{\mathfrak{G}} \rangle = [\{g\}, G]_{\mathfrak{G}}$ und

$$p^{l-1} = |h\langle \tilde{g} \rangle^{G/\langle \tilde{g} \rangle}| \stackrel{2.9}{=} |[\{h\langle \tilde{g} \rangle\}, G/\langle \tilde{g} \rangle]_{\mathfrak{G}}| = |[\{h\}, G]_{\mathfrak{G}} / \langle \tilde{g} \rangle| = \frac{|[\{h\}, G]_{\mathfrak{G}}|}{|\langle \tilde{g} \rangle|} \stackrel{2.9}{=} \frac{|h^G|}{p},$$

also $|h^G| = p^l$. \square

2.18 Korollar. Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$ und $g \in G$. Für alle $\tilde{a} \in G$ mit $\langle \tilde{a} \rangle = [\{g\}, G]_{\mathfrak{S}}$ existiert $\tilde{h} \in G$ mit \tilde{h} extremal und $[g, \tilde{h}]_{\mathfrak{S}} = \tilde{a}$.

Beweis. Nach Lemma 2.17 existiert $h \in G$ mit h extremal und $\langle [g, h]_{\mathfrak{S}} \rangle = [\{g\}, G]_{\mathfrak{S}}$. Nach den Korollaren 2.6 und 2.8 gilt $\langle [g, h]_{\mathfrak{S}} \rangle = \gamma_2(\langle g, h \rangle) = \{[g, h^k]_{\mathfrak{S}} \mid k \in \mathbb{N}_0\}$. Sei $\tilde{a} \in \gamma_2(G)$ mit $\langle \tilde{a} \rangle = [\{g\}, G]_{\mathfrak{S}}$ und $n \in \mathbb{N}$ mit $[g, h^n]_{\mathfrak{S}} = \tilde{a}$. Ist $g \in \mathcal{Z}(G)$, so wählen wir $\tilde{h} := h$. Sei $g \notin \mathcal{Z}(G)$. Dann gilt $h \notin C_G(g)$ und wir setzen $\tilde{h} := h^n$. Aus den Lemmata 2.3 und 2.2 folgt $p \nmid n$. Gemäß Bemerkung 2.7.1 (iii) ist \tilde{h} damit extremal. \square

Die beiden folgenden Lemmata sowie der anschließende Satz sind teils implizit, teils explizit in [5, Lemma 1, Lemma 2, Theorem 1] enthalten. Sie liefern konkretere Einblicke in die Struktur von p -Gruppen mit zyklischer Kommutatoruntergruppe.

2.19 Lemma. Seien G eine p -Gruppe, $x, y \in G$ mit $G = \langle x, y \rangle$, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$ und $\varphi \in \text{Aut}(G)$. Dann ist φ genau dann ein innerer Automorphismus von G , wenn $g^{-1}g\varphi \in \gamma_2(G)$ für alle $g \in G$ gilt.

Beweis. Die Implikation „ \Rightarrow “ ist trivial. Es gelte daher nun $g^{-1}g\varphi \in \gamma_2(G)$ für alle $g \in G$. Es gilt $\langle [x, y]_{\mathfrak{S}} \rangle = \gamma_2(G)$ nach Korollar 2.6. Nach Satz 2.7 existiert $n \in \mathbb{N}$ mit $x^{-1}x\varphi = [x, y^n]_{\mathfrak{S}}$ und $m \in \mathbb{N}$ mit $y^{-1}y\varphi = [y, x^m]_{\mathfrak{S}}^{y^n}$. Es folgt

$$\begin{aligned} x^{-1}x\varphi &= [x, y^n]_{\mathfrak{S}} \stackrel{2.2}{=} [x, x^m y^n]_{\mathfrak{S}}, \\ y^{-1}y\varphi &= [y, x^m]_{\mathfrak{S}}^{y^n} \stackrel{2.2}{=} [y, x^m y^n]_{\mathfrak{S}}, \end{aligned}$$

also $x\varphi = x^{x^m y^n}$ und $y\varphi = y^{x^m y^n}$. Aus $G = \langle x, y \rangle$ folgt die Behauptung. \square

2.20 Lemma. Seien G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$, $x, y \in G$ mit $\langle [x, y]_{\mathfrak{S}} \rangle = \gamma_2(G)$. Dann gilt $\langle x, y \rangle \trianglelefteq G$, $C_G(x, y) \trianglelefteq G$ und $C_G(x, y) \langle x, y \rangle = G$.

Beweis. Sei $g \in G$. Wir setzen $N := \langle x, y \rangle$. Es gilt $\gamma_2(G) \leq N$, also gilt $N \trianglelefteq G$ und damit auch $C_G(N) \trianglelefteq G$. Daher ist $\varphi : N \rightarrow N$, $h \mapsto h^g$ ein Automorphismus von N . Wegen $\langle [x, y]_{\mathfrak{S}} \rangle = \gamma_2(G)$ ist φ nach Lemma 2.19 ein innerer Automorphismus von N . Daher existiert $\tilde{g} \in N$ mit $h^g = h^{\tilde{g}}$ für alle $h \in N$. Es folgt $g\tilde{g}^{-1} \in C_G(x, y)$, also $g = g\tilde{g}^{-1}\tilde{g} \in C_G(x, y) \langle x, y \rangle$. \square

2.21 Satz. Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch und $\gamma_3(G) \leq \gamma_2(G)^4$. Dann existieren $x, y \in G$ und $s \in \mathbb{N}$ mit

- (i) $\langle [x, y]_{\mathfrak{S}} \rangle = \gamma_2(G)$,
- (ii) $C_G(x, y) \langle x, y \rangle = G$ und
- (iii) $[x, y]_{\mathfrak{S}} \mathcal{Z}(G) = y^{p^s} \mathcal{Z}(G)$.

Inbesondere sind x und y extremal.

Beweis. Die Aussagen (i)-(iii) folgen direkt aus Lemma 2.20 und Lemma 3 in [5]. Der Zusatz folgt aus Satz 2.7 und Bemerkung 2.7.1 (ii) und (iii). \square

2.21.1 Bemerkung. Es gilt $y \in C_G(\gamma_2(G))$ und $|(y^{p^s})^G| = |\gamma_3(G)|$.

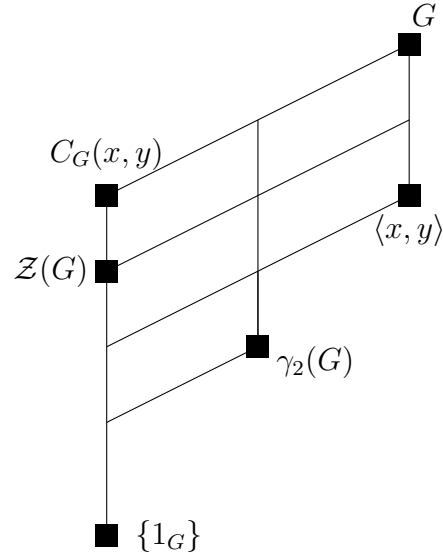
Beweis. Sei $a := [x, y]_{\mathfrak{G}}$. Dann gilt $\langle a \rangle = \gamma_2(G)$ nach (i) und aus (iii) folgt $y \in C_G(a) = C_G(\gamma_2(G))$. Aus (iii) erhalten wir weiter $|a^G| = |(y^{p^s})^G|$. Der zweite Teil der Bemerkung folgt nun aus Satz 2.9 (iv). \square

2.21.2 Bemerkung. Es gilt $(\gamma_2(G) \cap \mathcal{Z}(G)) \subseteq (\langle x, y \rangle \cap C_G(x, y)) \subseteq \mathcal{Z}(G)$.

Beweis. Sei $g \in \gamma_2(G) \cap \mathcal{Z}(G)$.

Dann folgt aus $g \in \gamma_2(G)$ nach Wahl von x und y direkt $g \in \langle x, y \rangle$ und wegen $g \in \mathcal{Z}(G)$ gilt offenbar $g \in C_G(x, y)$.

Ist $h \in \langle x, y \rangle \cap C_G(x, y)$, so folgt aus (ii) $h \in \mathcal{Z}(G)$.



2.21.3 Bemerkung. Gilt $cl(G) > 2$, so ist s eindeutig bestimmt und es gilt

$$o(y\mathcal{Z}(G)\gamma_2(G)) = p^s.$$

Beweis. Sei $cl(G) > 2$ und $l \in \mathbb{N}$ mit $p^l = |\gamma_2(G)|$. Dann gilt $[x, y]_{\mathfrak{G}} \notin \mathcal{Z}(G)$. Aus (iii) folgt $y^{p^s} \notin \mathcal{Z}(G)$ und $y^{p^s} \in \mathcal{Z}(G)\gamma_2(G)$. Sei nun $m \in \underline{s}$ mit $y^{p^m} \in \mathcal{Z}(G)\gamma_2(G)$. Dann gilt $y^{p^m} \notin \mathcal{Z}(G)$, folglich nach Korollar 2.10 (ii) $m < \kappa(y) \stackrel{2.21}{=} l$. Nach (i) und (iii) ist $y^{p^s}\mathcal{Z}(G)$ Erzeuger der zyklischen Gruppe $\mathcal{Z}(G)\gamma_2(G)/\mathcal{Z}(G)$. Insbesondere existiert $r \in \mathbb{N}$ und $z \in \mathcal{Z}(G)$ mit $y^{p^m} = y^{p^s r} z$. Nach Korollar 2.10 (iii) gilt $y^{p^l} \in \mathcal{Z}(G)$, wegen $y^{p^m} \notin \mathcal{Z}(G)$ folglich $\nu(p^s r) < l = \kappa(y)$. Wir erhalten

$$l - m \stackrel{2.10(i)}{=} \kappa(y^{p^m}) = \kappa(y^{p^s r} z) = \kappa(y^{p^s r}) \stackrel{2.10.1}{=} l - s - \nu(r)$$

und damit $m = s + \nu(r)$. Wegen $m \in \underline{s}$ folgern wir $\nu(r) = 0$ und $m = s$. Dies liefert $p^s = \min \{n \mid n \in \mathbb{N}, y^n \in \mathcal{Z}(G)\gamma_2(G)\}$. Insbesondere ist s in Satz 2.21 eindeutig bestimmt. \square

2.2 Die aufsteigende Zentralreihe von $\mathcal{J}(KG)$

In diesem Abschnitt sei K stets ein Körper mit $\text{char } K = p$.

Ist G eine Gruppe, $z \in \mathbb{Z}$ und $g \in G$, so schreiben wir wie gewohnt für das Element $(z1_K)g$ der Gruppenalgebra KG kurz zg .

Ziel dieses Abschnitts ist es, die aufsteigende Zentralreihe von $(\mathcal{J}(KG); *)$ für eine p -Gruppe G mit zyklischer Kommutatoruntergruppe zu bestimmen. Da $\mathcal{J}(KG)$ eine Radikal-Algebra ist, sind für alle $m \in \mathbb{N}_0$ die m -ten Glieder der aufsteigenden Zentralreihe der Gruppe $(\mathcal{J}(KG); *)$ und der Lie-Algebra $(\mathcal{J}(KG); +; [\cdot, \cdot]_{\mathcal{L}})$ nach Satz 1.8 gleich. Wir rechnen in der Lie-Algebra und verfolgen die in Abschnitt 1.3 erläuterte Idee.

In den ersten beiden Lemmata dieses Abschnitts geben wir zwei wichtige Rechenregeln für unser Vorgehen an.

2.22 Lemma. *Sei G eine zyklische p -Gruppe, $a \in G$ mit $\langle a \rangle = G$ und $l \in \mathbb{N}_0$ mit $|G| = p^l$. Sei $r \in \mathbb{N}_0$ und für alle $u \in \mathbb{Z}$ sei*

$$w_u := \sum_{i=0}^{p^l-1} \binom{i+r}{u-1} a^i.$$

Für alle $n \in \mathbb{N}_0$, $c \in \mathbb{N}_0$ und $m \in \mathbb{N}$ existieren dann $t \in \mathbb{N}$, $\vartheta_2, \dots, \vartheta_t \in K$ mit

$$a^{-cp^{l-n}} w_m = w_m + cw_{m-p^{l-n}} + \sum_{s=2}^t \vartheta_s w_{m-sp^{l-n}}.$$

Beweis. Seien $n \in \mathbb{N}_0$, $c \in \mathbb{N}_0$ und $m \in \mathbb{N}$. Nach Bemerkung 1.24.2 (i) existieren $t \in \mathbb{N}$ und $\vartheta_2, \dots, \vartheta_t \in K$ mit

$$(*) \quad \binom{i+cp^{l-n}+r}{m-1} \equiv_p \binom{i+r}{m-1} + c \binom{i+r}{m-1-p^{l-n}} + \sum_{s=2}^t \vartheta_s \binom{i+r}{m-1-sp^{l-n}}$$

für alle $i \in \mathbb{N}_0$. Es folgt

$$\begin{aligned} a^{-cp^{l-n}} w_m &= a^{-cp^{l-n}} \sum_{i=0}^{p^l-1} \binom{i+r}{m-1} a^i \\ &\stackrel{1.25}{=} \sum_{i=0}^{p^l-1} \binom{i+cp^{l-n}+r}{m-1} a^i \\ &\stackrel{(*)}{=} \sum_{i=0}^{p^l-1} \left(\binom{i+r}{m-1} + c \binom{i+r}{m-1-p^{l-n}} + \sum_{s=2}^t \vartheta_s \binom{i+r}{m-1-sp^{l-n}} \right) a^i \\ &= w_m + cw_{m-p^{l-n}} + \sum_{s=2}^t \vartheta_s w_{m-sp^{l-n}}. \end{aligned}$$

□

2.23 Lemma. Sei G eine zyklische p -Gruppe, $G \neq \{1_G\}$, $a \in G$ mit $\langle a \rangle = G$ und $l \in \mathbb{N}$ mit $|G| = p^l$. Seien $m \in \underline{p^l}$, $n \in \mathbb{N}_0$ mit $p^n \mid m$ und $\tilde{m} := \frac{m}{p^n}$, $k \in \underline{l-1}_0$ und $c \in \underline{p^k-1}_0$. Für alle $u \in \mathbb{Z}$ sei

$$w_u := \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{u-1} a^i.$$

Dann existieren $\delta_1, \dots, \delta_{\tilde{m}-2p^{l-k}+2} \in K$ mit

$$\begin{aligned} \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^{(-cp^{l-k}+1)i} &= w_m + c(\tilde{m}-1)w_{m-p^{n+l-k}} \\ &+ c\tilde{m}w_{m-p^n(p^{l-k}-1)} + \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s w_{sp^n}. \end{aligned}$$

Beweis. Wir setzen $b := a^{p^n}$. Aus Lemma 1.28 (i) erhalten wir

$$w_m = \sum_{i=0}^{p^{l-n}-1} \binom{i}{\tilde{m}-1} b^i.$$

Wir unterscheiden nun zwei Fälle:

(i) Es gelte $n \geq k$.

Dann gilt (unter Anwendung von Lemma 1.28 (i) auf den Erzeuger $a^{(-cp^{l-k}+1)}$ von G statt auf a) wegen $b^{-cp^{l-k}} = 1_G$:

$$\sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^{(-cp^{l-k}+1)i} = \sum_{i=0}^{p^{l-n}-1} \binom{i}{\tilde{m}-1} b^{(-cp^{l-k}+1)i} = \sum_{i=0}^{p^{l-n}-1} \binom{i}{\tilde{m}-1} b^i = w_m.$$

Außerdem gilt $w_{m-p^{n+l-k}} = 0_{KG}$ nach Voraussetzung über n . Ist $n < \nu(m)$, so gilt $\tilde{m} \equiv 0_p$. Ist $n = \nu(m)$, so gilt $m \leq p^n(p^{l-k}-1)$ wegen $m \leq p^l$. Es folgt jeweils $\tilde{m}w_{m-p^n(p^{l-k}-1)} = 0_{KG}$. Hieraus folgt die Behauptung.

(ii) Es gelte nun $n < k$.

Dann gilt $p^{l-n} > p^{l-k}$. Wir setzen $y := -cp^{l-k} + 1$. Es gilt $y \equiv_{p^{l-k}} 1$ und es existiert $z \in \underline{p^{l-n}-1}$ mit $yz \equiv_{p^{l-n}} 1$. Wegen $p^{l-n} > p^{l-k}$ gilt insbesondere $yz \equiv_{p^{l-k}} 1$ und damit $z \equiv_{p^{l-k}} 1$. Sei nun $d \in \underline{p^{k-n}-1}_0$ mit $z = dp^{l-k} + 1$. Dann gilt

$$1 \equiv_{p^{l-n}} zy = 1 + (d-c)p^{l-k} - dcp^{2(l-k)},$$

wegen $n < k < l$ also $d \equiv_p -(-c) = c$.

Wir erhalten unter Anwendung von Lemma 1.28 (i) auf den Erzeuger $a^{(-cp^{l-k}+1)}$ von G statt auf a und von Lemma 1.27 auf das Element b der Ordnung p^{l-n} :

$$\sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^{(-cp^{l-k}+1)i} \stackrel{1.28(i)}{=} \sum_{i=0}^{p^{l-n}-1} \binom{i}{\tilde{m}-1} b^{yi} \stackrel{1.27}{=} \sum_{i=0}^{p^{l-n}-1} \binom{zi}{\tilde{m}-1} b^i.$$

Für alle $i \in \mathbb{N}_0$ gilt:

$$\begin{aligned} \binom{zi}{\tilde{m}-1} &= \binom{dp^{l-k}i+i}{\tilde{m}-1} \\ &\stackrel{1.21}{=} \sum_{j=0}^{\tilde{m}-1} \binom{dp^{l-k}i}{j} \binom{i}{\tilde{m}-1-j} \\ &\stackrel{1.24.2(ii)}{=} \binom{i}{\tilde{m}-1} + \sum_{\substack{j \in \tilde{m}-1, \\ p^{l-k} \mid j}} \binom{dp^{l-k}i}{j} \binom{i}{\tilde{m}-1-j} \\ &\stackrel{1.22.1}{=} \binom{i}{\tilde{m}-1} + \binom{di}{1} \binom{i}{\tilde{m}-1-p^{l-k}} + \sum_{\substack{j \in \tilde{m}-1, \\ p^{l-k} \mid j, p^{l-k} \neq j}} \binom{dp^{l-k}i}{j} \binom{i}{\tilde{m}-1-j} \\ &\stackrel{1.22.1}{=} \binom{i}{\tilde{m}-1} + d \binom{i}{1} \binom{i}{\tilde{m}-1-p^{l-k}} + \sum_{\substack{j \in \mathbb{N}_{>1}, \\ jp^{l-k} \leq \tilde{m}-1}} \binom{di}{j} \binom{i}{\tilde{m}-1-jp^{l-k}} \\ &\stackrel{1.24.k < l}{=} \binom{i}{\tilde{m}-1} + d(\tilde{m}-1) \binom{i}{\tilde{m}-1-p^{l-k}} + d\tilde{m} \binom{i}{\tilde{m}-p^{l-k}} \\ &\quad + \sum_{\substack{j \in \mathbb{N}_{>1}, \\ jp^{l-k} \leq \tilde{m}-1}} \binom{di}{j} \binom{i}{\tilde{m}-1-jp^{l-k}} \end{aligned}$$

Es gilt $\max \{j + (\tilde{m}-1-jp^{l-k}) \mid j \in \mathbb{N}_{>1}\} = \tilde{m} - 2p^{l-k} + 1$. Aus Bemerkung 1.24.1 und Lemma 1.24 folgt daher: Es existieren $\delta_1, \dots, \delta_{\tilde{m}-2p^{l-k}+2} \in \mathbb{N}_0$, sodass für alle $i \in \mathbb{N}_0$ gilt:

$$\sum_{\substack{j \in \mathbb{N}_{>1}, \\ jp^{l-k} \leq \tilde{m}}} \binom{di}{j} \binom{i}{\tilde{m}-1-jp^{l-k}} = \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s \binom{i}{s-1}. \quad (2.1)$$

2 p -Gruppen mit zyklischer Kommutatoruntergruppe

Wir erhalten aus $d \equiv c$ unter Verwendung von Lemma 1.28 (i):

$$\begin{aligned}
\sum_{i=0}^{p^{l-n}-1} \binom{zi}{\tilde{m}-1} b^i &= \sum_{i=0}^{p^{l-n}-1} \binom{i}{\tilde{m}-1} b^i + c(\tilde{m}-1) \sum_{i=0}^{p^{l-n}-1} \binom{i}{\tilde{m}-1-p^{l-k}} b^i \\
&\quad + c\tilde{m} \sum_{i=0}^{p^{l-n}-1} \binom{i}{\tilde{m}-p^{l-k}} b^i + \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s \sum_{i=0}^{p^{l-n}-1} \binom{i}{s-1} b^i \\
&= w_m + c(\tilde{m}-1)w_{m-p^{n+l-k}} + c\tilde{m}w_{m-p^n(p^{l-k}-1)} + \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s w_{sp^n}.
\end{aligned}$$

□

2.23.1 Bemerkung. Gilt $p > 2$, $\tilde{m} \equiv -1$ und $2p^{l-k} - 1 \leq \tilde{m}$, so gilt $\delta_{\tilde{m}-2p^{l-k}+2} = 0_K$.

Beweis. Wir greifen Gleichung (2.1) auf und setzen $p > 2$, $\tilde{m} \equiv -1$ und $2p^{l-k} < \tilde{m}$ voraus. Nach Bemerkung 1.24.1 existieren dann $\lambda_0, \lambda_1, \lambda_2 \in \mathbb{N}_0$, sodass für alle $i \in \mathbb{N}_0$ gilt:

$$\begin{aligned}
\sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s \binom{i}{s-1} &= \sum_{\substack{j \in \mathbb{N}_{>2} \\ jp^{l-k} \leq \tilde{m}}} \binom{di}{j} \binom{i}{\tilde{m}-1-jp^{l-k}} + \binom{di}{2} \binom{i}{\tilde{m}-1-2p^{l-k}} \\
&= \sum_{\substack{j \in \mathbb{N}_{>2} \\ jp^{l-k} \leq \tilde{m}}} \binom{di}{j} \binom{i}{\tilde{m}-1-jp^{l-k}} \\
&\quad + \left(\lambda_0 \binom{i}{0} + \lambda_1 \binom{i}{1} + \lambda_2 \binom{i}{2} \right) \binom{i}{\tilde{m}-1-2p^{l-k}}.
\end{aligned}$$

Sei $F := \left\langle \binom{i}{r} \right\rangle_{i \in \mathbb{N}_0} \mid r \in \underline{\tilde{m}-2p^{l-k}}_{\mathbb{Z}}$. Es folgt in $\mathbb{Z}^{\mathbb{N}_0}$:

$$\begin{aligned}
\delta_{\tilde{m}-2p^{l-k}+2} \binom{i}{\tilde{m}-2p^{l-k}+1} &\equiv_F \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s \binom{i}{s-1} \\
&\stackrel{1.24, 1.24.1}{\equiv_F} \lambda_2 \binom{i}{2} \cdot \binom{i}{\tilde{m}-1-2p^{l-k}} \\
&\stackrel{1.24}{\equiv_F} \lambda_2 \binom{2+\tilde{m}-1-2p^{l-k}}{2} \binom{i}{\tilde{m}-2p^{l-k}+1}
\end{aligned}$$

Wegen $p > 2$ und $\tilde{m} \equiv -1$ gilt $p \mid \binom{2+\tilde{m}-1-2p^{l-k}}{2}$. Aus Lemma 1.23 (iii) folgt die Behauptung durch einen Koeffizientenvergleich. □

Die folgende Definition ist durch den anschließenden Satz motiviert, welcher von grundlegender Bedeutung zur Bestimmung der aufsteigenden Zentralreihe ist.

2.24 Definition. Für jede endliche Gruppe G sei

$$\alpha_G : G \times \mathbb{N}_0 \longrightarrow \mathbb{Q}, \quad (g, n) \mapsto \min \left\{ \frac{|\gamma_2(G)|}{|g^G|}, p^n \left(\frac{|\gamma_2(G)|}{|\gamma_3(G)|} - 1 \right) \right\}.$$

Da wir in einem Kontext nur eine Gruppe G betrachten werden, verzichten wir gewöhnlich auf die Indizierung von α mit G .

2.24.1 Bemerkung. Sei G eine p -Gruppe.

- (i) Für alle $g \in G$ und $n \in \mathbb{N}_0$ gilt $(g, n)\alpha \in \mathbb{N}_0$.
- (ii) Es gilt: G abelsch $\iff \exists g \in G \exists n \in \mathbb{N}_0 : (g, n)\alpha = 0$.
- (iii) Seien $g \in G$ und $n \in \mathbb{N}_0$. Ist $p > 2$ oder $|\gamma_2(G) : \gamma_3(G)| \geq 4$, so gilt

$$\frac{|\gamma_2(G)|}{|g^G|} \neq p^n \left(\frac{|\gamma_2(G)|}{|\gamma_3(G)|} - 1 \right).$$

- (iv) Ist $g \in G$ mit $|g^G| > |\gamma_3(G)|$, so gilt $(g, n)\alpha = \frac{|\gamma_2(G)|}{|g^G|}$.

Beweis. Die Aussagen (ii) und (iv) sind offensichtlich.

Da $\gamma_2(G)$, $\gamma_3(G)$ und g^G für alle $g \in G$ von p -Potenz-Mächtigkeit sind, folgt hieraus (i). Ist $p > 2$ oder $|\gamma_2(G) : \gamma_3(G)| \geq 4$, so ist $\frac{|\gamma_2(G)|}{|\gamma_3(G)|} - 1$ keine p -Potenz, woraus (iii) folgt. \square

2.25 Satz. Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch mit $\gamma_3(G) \leq \gamma_2(G)^4$, $a \in G$ mit $\langle a \rangle = \gamma_2(G)$ und $l \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$. Dann gilt

$$g \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^i \in \mathcal{Z}_{\max\{m-(g,n)\alpha+1, 1\}}(\mathcal{J}(KG)) \text{ und} \\ g - 1_G \in \mathcal{Z}_{|\gamma_2(G)| - \frac{|\gamma_2(G)|}{|g^G|} + 1}(\mathcal{J}(KG))$$

für alle $g \in G$, $m \in \underline{p^l - 1}$ und $n \in \mathbb{N}_0$ mit $p^n \mid m$.

Beweis. Sei $k \in \mathbb{N}_0$ mit $p^k = |\gamma_3(G)|$. Ist G abelsch, so ist die Behauptung trivial. Sei daher im Folgenden G als nicht abelsch angenommen.

Wir zeigen die Behauptung durch Induktion nach m . Es wird sich als günstig erweisen, im Beweis auch $m = p^l$ zuzulassen. Sei $g \in G$ und $m \in \underline{p^l}$. Da G nicht abelsch ist, gilt

$k < l$ und $(g, n)\alpha > 0$ für alle $n \in \mathbb{N}_0$ nach Bemerkung 2.24.1 (ii). Wir halten zunächst fest, dass

$$g \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^i \in \mathcal{J}(KG)$$

nach Bemerkung 1.22.5 im Fall $m \leq p^l - 1$ gilt. Ist $m = 1$, so folgt die Behauptung unmittelbar aus Lemma 1.17 und Satz 1.4 (i).

Sei also $m > 1$ und $n \in \mathbb{N}_0$ mit $p^n \mid m$.

Für alle $\tilde{g} \in G$ und $r, \tilde{r} \in \mathbb{N}_0$ gilt

$$\begin{aligned} \tilde{g} \sum_{i=0}^{p^l-1} \binom{i+\tilde{r}}{r-1} a^i &\stackrel{1.21}{=} \tilde{g} \sum_{i=0}^{p^l-1} \left(\sum_{j=0}^{r-1} \binom{\tilde{r}}{r-1-j} \binom{i}{j} \right) a^i \\ &= \sum_{j=1}^r \left(\binom{\tilde{r}}{r-j} \tilde{g} \sum_{i=0}^{p^l-1} \binom{i}{j-1} a^i \right) \end{aligned} \quad (2.2)$$

und wir dürfen induktiv für alle $j \in \underline{m-1}$

$$\tilde{g} \sum_{i=0}^{p^l-1} \binom{i}{j-1} a^i \in \mathcal{Z}_{\max\{j-(\tilde{g},0)\alpha+1,1\}}(\mathcal{J}(KG)) \stackrel{2.24.1(i),(ii)}{\subseteq} \mathcal{Z}_j(\mathcal{J}(KG))$$

voraussetzen, also nach Gleichung (2.2) auch

$$(*) \quad \tilde{g} \sum_{i=0}^{p^l-1} \binom{i+\tilde{r}}{r-1} a^i \in \mathcal{Z}_r(\mathcal{J}(KG))$$

für alle $\tilde{g} \in G, \tilde{r} \in \mathbb{N}_0$ und $r \in \underline{m-1}$.

Wir setzen der Übersicht halber

$$\tilde{m} := \frac{m}{p^n} \quad \text{und} \quad w_u := \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{u-1} a^i \quad \text{für alle } u \in \mathbb{Z}.$$

Wir folgen nun beim Beweis dem im Eingangskapitel erläuterten Grundprinzip. Sei $h \in G$ und $\tilde{c} := \omega(a, h)$. Dann gilt

$$a^h = a[a, h]_{\mathfrak{G}} = aa^{-\tilde{c}p^{l-\kappa(a)}} \stackrel{2.9(iv)}{=} a^{-\tilde{c}p^{l-k}+1}.$$

Nach Lemma 2.23 existieren $\delta_1, \dots, \delta_{\tilde{m}-2p^{l-k}+2} \in K$ mit

$$\begin{aligned} w_m^h &= \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^{(-\tilde{c}p^{l-k}+1)i} \\ &= w_m + \tilde{c}(\tilde{m}-1)w_{m-p^{n+l-k}} + \tilde{c}\tilde{m}w_{m-p^n(p^{l-k}-1)} + \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s w_{sp^n}. \end{aligned} \quad (2.3)$$

Für alle $s \in \underline{\tilde{m} - 2p^{l-k} + 2}$ gilt

$$sp^n \leq (\tilde{m} - 2p^{l-k} + 2)p^n = m - 2p^n(p^{l-k} - 1) \leq m - p^n(p^{l-k} - 1).$$

Nach (*) dürfen wir also

$$\tilde{g}w_{m-p^{n+l-k}}, \tilde{g}w_{m-p^n(p^{l-k}-1)}, \tilde{g}w_{sp^n} \in \mathcal{Z}_{m-p^n(p^{l-k}-1)}(\mathcal{J}(KG))$$

für alle $\tilde{g} \in G$ und alle $s \in \underline{\tilde{m} - 2p^{l-k} + 2}$ annehmen.

Wir erhalten demnach mit $\tilde{g} := hg[g, h]_{\mathfrak{S}}$ aus Gleichung (2.3):

$$hg[g, h]_{\mathfrak{S}} w_m^h \equiv_{\mathcal{Z}_{m-p^n(p^{l-k}-1)}(\mathcal{J}(KG))} hg[g, h]_{\mathfrak{S}} w_m. \quad (2.4)$$

Sei $c := \omega(g, h)$. Dann gilt $[g, h]_{\mathfrak{S}} = a^{-cp^{l-\kappa(g)}}$. Nach Lemma 2.22 existieren $t \in \mathbb{N}$ und $\vartheta_2, \dots, \vartheta_t \in K$ mit

$$[g, h]_{\mathfrak{S}} w_m = a^{-cp^{l-\kappa(g)}} w_m = w_m + cw_{m-p^{l-\kappa(g)}} + \sum_{s=2}^t \vartheta_s w_{m-sp^{l-\kappa(g)}}.$$

Mit $\tilde{g} := hg$ gilt nach (*) gilt für alle $s \in \underline{t}$:

$$hgw_{m-sp^{l-\kappa(g)}} \in \mathcal{Z}_{m-p^{l-\kappa(g)}}(\mathcal{J}(KG)).$$

Damit gilt also

$$hg[g, h]_{\mathfrak{S}} w_m \equiv_{\mathcal{Z}_{m-p^{l-\kappa(g)}}(\mathcal{J}(KG))} hg w_m. \quad (2.5)$$

Insgesamt folgern wir aus den Gleichungen (2.4), (2.5) und der Definition von $(g, n)\alpha$:

$$hg[g, h]_{\mathfrak{S}} w_m^h \equiv_{\mathcal{Z}_{m-(g, n)\alpha}(\mathcal{J}(KG))} hg w_m. \quad (2.6)$$

Ist $m < p^l$, so folgt aus dem Grundprinzip der erste Teil der Behauptung.

Um den zweiten Teil zu beweisen, betrachten wir den Spezialfall $m = p^l$ und $n = l$. Aus Lemma 1.28 (ii) folgt dann $w_{p^l} = 1_G$. Wegen $\frac{|\gamma_2(G)|}{|g^G|} \leq p^l$ folgt $(g, l)\alpha = \frac{|\gamma_2(G)|}{|g^G|}$.

Aus Gleichung (2.6) folgt die Behauptung dann mit dem Grundprinzip. \square

Aus diesem Satz werden wir nun eine Reihe von Folgerungen ziehen.

2.25.1 Bemerkung. Seien $g, h \in G$, $r \in \mathbb{N}_0$, $m \in \underline{p^l}$ und $n \in \mathbb{N}_0$ mit $p^n \mid m$. Dann gilt

(i)

$$gh \left(\sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^i \right)^h \equiv_{\mathcal{Z}_{m-p^n} \left(\frac{|\gamma_2(G)|}{|\gamma_3(G)|} - 1 \right) (\mathcal{J}(KG))} gh \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^i,$$

(ii)

$$gh \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^i \equiv_{\mathcal{Z}_{m-p^l-\kappa(g)} (\mathcal{J}(KG))} hg \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^i \quad \text{und}$$

(iii)

$$ga^{-r} \sum_{i=0}^{p^l-1} \binom{i}{m-1} a^i = g \sum_{i=0}^{p^l-1} \binom{i+r}{m-1} a^i \equiv_{\mathcal{Z}_{m-1} (\mathcal{J}(KG))} g \sum_{i=0}^{p^l-1} \binom{i}{m-1} a^i.$$

Beweis. (i) folgt aus Gleichung (2.4) und (ii) folgt aus Gleichung (2.5).

(iii): Es gilt $g \sum_{i=0}^{p^l-1} \binom{i}{j-1} a^i \in \mathcal{Z}_{m-1} (\mathcal{J}(KG))$ für alle $j \in \underline{m-1}$ nach Satz 2.25. Folglich erhalten wir aus Gleichung (2.2):

$$g \sum_{i=0}^{p^l-1} \binom{i+r}{m-1} a^i = \sum_{j=1}^m \left(\binom{r}{m-j} g \sum_{i=0}^{p^l-1} \binom{i}{j-1} a^i \right) \equiv_{\mathcal{Z}_{m-1} (\mathcal{J}(KG))}^{2.25} g \sum_{i=0}^{p^l-1} \binom{i}{m-1} a^i.$$

Die erste Gleichheit in (iii) folgt direkt aus Lemma 1.25. □

2.26 Korollar. Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$, $a \in G$ mit $\langle a \rangle = \gamma_2(G)$ und $l \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$. Sei $r \in \mathbb{N}_0$ und

$$w_m := \sum_{i=0}^{p^l-1} \binom{i+r}{m-1} a^i \quad \text{für alle } m \in \mathbb{Z}.$$

Dann ist für alle $m \in \underline{p^l-1}$ das von w_m erzeugte (assoziative) Ideal in $\mathcal{Z}_m (\mathcal{J}(KG))$ enthalten.

Beweis. Sei $m \in \underline{p^l-1}$ und $g \in G$. Es reicht $gw_m, w_mg \in \mathcal{Z}_m (\mathcal{J}(KG))$ zu zeigen. $gw_m \in \mathcal{Z}_m (\mathcal{J}(KG))$ folgt aber direkt aus Bemerkung 2.25.1 (iii) und Satz 2.25. Aus

$$w_mg = gw_m^g = g \sum_{i=0}^{p^l-1} \binom{i+r}{m-1} (a^g)^i$$

folgt mit dem bereits Bewiesenen die Behauptung, da $\langle a^g \rangle = \gamma_2(G)$ gilt. □

In einem nächsten Schritt werden wir sehen, dass die in Satz 2.25 getroffene Aussage in vielen Fällen „scharf“ ist.

2.27 Satz. *Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$, $a \in G$ mit $\langle a \rangle = \gamma_2(G)$ und $l \in \mathbb{N}_0$ mit $p^l = |\gamma_2(G)|$.*

(i) *Ist $m \in \underline{p^l - 1}$, $g \in G$, $n \in \mathbb{N}_0$ mit $p^n \mid m$ und gilt $(g, n)\alpha = \frac{|\gamma_2(G)|}{|g^G|}$, so ist*

$$g \sum_{i=0}^{p^l-1} \binom{i + p^n - 1}{m - 1} a^i \in \mathcal{Z}_{\max\{m-(g,n)\alpha+1, 1\}}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-(g,n)\alpha}(\mathcal{J}(KG)).$$

(ii) *Ist $m \in \underline{p^l - 1}$, $g \in G$, mit $(g, \nu(m))\alpha = p^{\nu(m)} \left(\frac{|\gamma_2(G)|}{|\gamma_3(G)|} - 1 \right)$, so gilt*

$$g \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m - 1} a^i \in \mathcal{Z}_{\max\{m-(g,\nu(m))\alpha+1, 1\}}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-(g,\nu(m))\alpha}(\mathcal{J}(KG)).$$

(iii) *Für alle $g \in G \setminus \{1_G\}$ gilt*

$$g - 1_G \in \mathcal{Z}_{|\gamma_2(G)| - \frac{|\gamma_2(G)|}{|g^G|} + 1}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{|\gamma_2(G)| - \frac{|\gamma_2(G)|}{|g^G|}}(\mathcal{J}(KG)).$$

Beweis. Ist G abelsch, so sind die Behauptungen trivial. Wir nehmen daher an, dass G nicht abelsch ist. Wie in Satz 2.25 zeigen wir durch einen Induktionsbeweis nach m die Aussage (i) und lassen erneut im Beweis zunächst auch $m = p^l$ zu.

Sei $m \in \underline{p^l}$, $n \in \mathbb{N}_0$ mit $p^n \mid m$ und $g \in G$. Wir setzen

$$w_u := \sum_{i=0}^{p^l-1} \binom{i + p^n - 1}{u - 1} a^i \text{ für alle } u \in \mathbb{Z}.$$

Da $gw_m \in \mathcal{J}(KG) \setminus \{0_{KG}\}$ im Fall $m \leq p^l - 1$ nach Bemerkung 1.22.5 gilt, folgen (i) und (ii) für $m \leq (g, n)\alpha$ direkt aus Satz 2.25.

Sei nun $p^l \geq m > (g, n)\alpha$.

Sei $\tilde{g} \in G$, \tilde{g} extremal. Dann gilt $(\tilde{g}, 0)\alpha = \frac{|\gamma_2(G)|}{|\tilde{g}^G|} = 1$. Ist $s < m$, so dürfen wir

$\tilde{g} \sum_{i=0}^{p^l-1} \binom{i}{s-1} a^i \notin \mathcal{Z}_{s-(\tilde{g},0)\alpha}(\mathcal{J}(KG)) = \mathcal{Z}_{s-1}(\mathcal{J}(KG))$ unter Anwendung der Induktionsvoraussetzung auf s annehmen, also nach Bemerkung 2.25.1 (iii) auch

$$(*) \quad \tilde{g}w_s \notin \mathcal{Z}_{s-1}(\mathcal{J}(KG)).$$

(i): Sei $(g, n)\alpha = \frac{|\gamma_2(G)|}{|g^G|} = p^{l-\kappa(g)}$.

Dann gilt $(g, n)\alpha \leq p^n \left(\frac{|\gamma_2(G)|}{|\gamma_3(G)|} - 1 \right)$. Wegen $p^l > (g, n)\alpha$ gilt außerdem $g \notin \mathcal{Z}(G)$. Nach Satz 2.9 gilt $[\{g\}, G]_{\mathfrak{S}} = \langle a^{p^{l-\kappa(g)}} \rangle$ und nach Korollar 2.18 existiert $h \in G$, h extremal, mit $[g, h]_{\mathfrak{S}} = a^{-p^{l-\kappa(g)}}$. Wegen $g \notin \mathcal{Z}(G)$ gilt insbesondere $\omega(g, h) = 1 \not\equiv 0$. Ist g extremal, so gilt $[g, h]_{\mathfrak{S}} = a^{-1}$. Dann ist hg wegen $\langle [g, h]_{\mathfrak{S}} \rangle = \gamma_2(G)$ nach Satz 2.7 und Bemerkung 2.7.1 (ii) extremal. Ist g nicht extremal, so ist hg nach Satz 2.14 extremal.

Ist $p = 2$ und $l = 1$, so gilt $a \in \mathcal{Z}(G)$ und damit $w_m^h = w_m$. Andernfalls gilt

$$p^{l-\kappa(g)} = \frac{|\gamma_2(G)|}{|g^G|} = (g, n)\alpha < p^n \left(\frac{|\gamma_2(G)|}{|\gamma_3(G)|} - 1 \right) = p^n (p^{l-k} - 1)$$

nach Bemerkung 2.24.1 (iii). In beiden Fällen können wir folgern

$$\begin{aligned} hg[g, h]_{\mathfrak{S}} w_m^h &\stackrel{2.25.1(i)}{\equiv}_{\mathcal{Z}_{m-(g,n)\alpha-1}(\mathcal{J}(KG))} hg[g, h]_{\mathfrak{S}} w_m = hga^{-p^{l-\kappa(g)}} w_m \\ &\stackrel{2.22, 2.26}{\equiv}_{\mathcal{Z}_{m-(g,n)\alpha-1}(\mathcal{J}(KG))} hgw_m + hgw_{p^{l-\kappa(g)}} \\ &\stackrel{(*)}{\not\equiv}_{\mathcal{Z}_{m-(g,n)\alpha-1}(\mathcal{J}(KG))} hgw_m. \end{aligned} \tag{2.7}$$

Aus Satz 2.25 und dem Grundprinzip folgt hieraus (i).

(ii): Sei $n = \nu(m)$ und $p^n \left(\frac{|\gamma_2(G)|}{|\gamma_3(G)|} - 1 \right) = (g, n)\alpha < \frac{|\gamma_2(G)|}{|g^G|} = p^{l-\kappa(g)}$.

Wegen $|\gamma_2(G)| = p^l \geq m > (g, n)\alpha$ folgt $1 < |\gamma_3(G)|$, das heißt es gilt $cl(G) > 2$. Da im Fall $p = 2$ nach Voraussetzung dann $|\gamma_2(G) : \gamma_3(G)| \geq 4$ gilt, folgt $(g, n)\alpha > 1$.

Sei $k \in \mathbb{N}$ mit $p^k = |\gamma_3(G)|$. Dann gilt $\langle a^{p^{l-k}} \rangle = [\{a\}, G]_{\mathfrak{S}}$ nach Satz 2.9 (iv). Nach Korollar 2.18 existiert $h \in G$, h extremal, mit $[a, h]_{\mathfrak{S}} = a^{-p^{l-k}}$. Aus $cl(G) > 2$ folgt insbesondere $c := \omega(a, h) = 1 \not\equiv 0$. Wir setzen $\tilde{m} := \frac{m}{p^n}$.

Folglich gilt $\tilde{m} \not\equiv 0$ nach Wahl von n . Nach Lemma 2.23 existieren $\delta_1, \dots, \delta_{\tilde{m}-2p^{l-k}+2} \in K$ mit

$$\begin{aligned} w_m^h &= \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^{(-cp^{l-k}+1)i} \\ &= w_m + (\tilde{m} - 1)w_{m-p^{n+l-k}} + \tilde{m}w_{m-p^n(p^{l-k}-1)} + \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s w_{sp^n}. \end{aligned}$$

Es folgt

$$\begin{aligned} hg[g, h]_{\mathfrak{S}} w_m^h &\stackrel{2.26}{=} \mathcal{Z}_{m-(g, n)\alpha-1}(\mathcal{J}(KG)) \quad hg[g, h]_{\mathfrak{S}}(w_m + \tilde{m}w_{m-p^n(p^l-k-1)}) \\ &\stackrel{2.25.1(ii)}{=} \mathcal{Z}_{m-(g, n)\alpha-1}(\mathcal{J}(KG)) \quad hgw_m + hg\tilde{m}w_{m-p^n(p^l-k-1)}. \end{aligned}$$

Wegen $(g, n)\alpha > 1$ gilt $|g^G| < |\gamma_2(G)|$. Also ist g nicht extremal und folglich hg nach Satz 2.14 extremal. Insbesondere erhalten wir aus (*):

$$hg\tilde{m}w_{m-p^n(p^l-k-1)} \notin \mathcal{Z}_{m-(g, n)\alpha-1}(\mathcal{J}(KG))$$

und damit

$$hg[g, h]_{\mathfrak{S}} w_m^h \not\equiv_{\mathcal{Z}_{m-(g, n)\alpha-1}(\mathcal{J}(KG))} hgw_m.$$

Hieraus folgt zusammen mit dem Grundprinzip die Aussage (ii).

(iii): Die Aussage (iii) ist trivial im Fall $g \in \mathcal{Z}(G) \setminus \{1_G\}$. Wir nehmen daher nun $g \notin \mathcal{Z}(G)$ an und betrachten den Spezialfall $m = p^l$ und $n = l$. Es gilt dann $(g, l)\alpha = \frac{|\gamma_2(G)|}{|g^G|} < p^l$ und $w_{p^l} = 1_G$ nach Lemma 1.28 (ii). (iii) folgt dann direkt aus Gleichung (2.7) in (i) und dem Grundprinzip. \square

Satz 2.12 zeigt, dass man (unter den Voraussetzungen von Satz 2.25) die Elemente aus $G/\gamma_2(G)$ in zwei Sorten unterteilen kann, nämlich in die Sorte solcher Restklassen, die eine Konjugiertenklasse der Länge $|\gamma_3(G)|$ enthalten, und in die Sorte solcher, die keine Konjugiertenklasse dieser Art enthalten. Für letztere können wir folgern:

2.28 Korollar. *Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$, $a \in G$ mit $\langle a \rangle = \gamma_2(G)$ und $l \in \mathbb{N}_0$ mit $p^l = |\gamma_2(G)|$. Sei $H \in G/\gamma_2(G)$ und es gelte $p^{\mu(H)} > |\gamma_3(G)|$. Dann gilt*

$$g \sum_{i=0}^{p^l-1} \binom{i+p^n-1}{m-1} a^i \in \mathcal{Z}_{\max\{m-\frac{|\gamma_2(G)|}{|g^G|}+1, 1\}}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-\frac{|\gamma_2(G)|}{|g^G|}}(\mathcal{J}(KG))$$

für alle $m \in \underline{p^l-1}$, $g \in H$ und $n \in \mathbb{N}_0$ mit $p^n \mid m$.

Insbesondere gilt: Ist $g \in G \setminus \{1_G\}$ extremal, so gilt

$$\begin{aligned} g \sum_{i=0}^{p^l-1} \binom{i}{m-1} a^i &\in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \text{ für alle } m \in \underline{p^l-1} \\ \text{und } g - 1_G &\in \mathcal{J}(KG) \setminus \mathcal{Z}_{p^l-1}(\mathcal{J}(KG)). \end{aligned}$$

Beweis. Sei $g \in H$. Dann gilt $|g^G| = p^{\mu(H)}$ nach Satz 2.12. Aus Bemerkung 2.24.1 (iv) folgt $(g, n)\alpha = \frac{|\gamma_2(G)|}{p^{\mu(H)}}$ nach Voraussetzung über H . Die Behauptungen folgen aus Satz 2.27 (i) und (iii). \square

Der erste Teil der nächsten Folgerung ist für $p > 2$, wie in der Einleitung bereits erwähnt, ein Resultat von A. Shalev [21], [22].

2.29 Korollar. *Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch und $\gamma_3(G) \leq \gamma_2(G)^4$.*

- (i) *Es gilt $cl(\mathcal{J}(KG); *) = |\gamma_2(G)|$.*
- (ii) *Ist G nicht abelsch, e die Anzahl der extremalen Konjugiertenklassen von G und $m \in \underline{|\gamma_2(G)|}$, so gilt*

$$\dim(\mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG))) \geq e.$$

Beweis. (i): Nach Bemerkung 2.7.2 gibt es in G extremale Elemente. Aus Korollar 2.28 folgt $cl(\mathcal{J}(KG); *) \geq |\gamma_2(G)|$. Da die K -Basis $\{g - 1_G \mid g \in G \setminus \{1_G\}\}$ von $\mathcal{J}(KG)$ gemäß Satz 2.27 (iii) in $\mathcal{Z}_{p^l}(\mathcal{J}(KG))$ enthalten ist, folgt aus Satz 1.8 die Aussage (i).

(ii): Seien G nicht abelsch, $e \in \mathbb{N}$ und H_1, \dots, H_e die paarweise verschiedenen extremalen Konjugiertenklassen von G . Da G nicht abelsch ist, ist 1_G nicht extremal und wir können den zweiten Teil von Korollar 2.28 anwenden. Sei $m \in \underline{|\gamma_2(G)|}$. Demnach existiert $a_i \in \text{Aug}(H_i \cup \mathcal{Z}(G))$ für alle $i \in \underline{e}$ mit $a_i \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG))$ und nach Bemerkung 1.14.1 ist $\{a_1, \dots, a_e\}$ modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ K -linear unabhängig im Fall $m > 1$. Ist $m = 1$, so folgt das Behauptete aus 1.4 (i). \square

Mit den bisher erzielten Resultaten können wir nun das vorletzte Glied der aufsteigenden Zentralreihe bestimmen:

2.30 Korollar. *Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$ und $l \in \mathbb{N}_0$ mit $p^l = |\gamma_2(G)|$. Für alle $H \in G/\gamma_2(G)$ sei $g_H \in H$. Dann gilt*

$$\mathcal{Z}_{p^l-1}(\mathcal{J}(KG)) = \langle g_H - 1_G \mid H \in G/\gamma_2(G) \setminus \{\gamma_2(G)\}, \mu(H) \neq l \rangle_K \oplus \bigoplus_{H \in G/\gamma_2(G)} \text{Aug}(H).$$

Beweis. Ist G abelsch, so ist die Behauptung trivial. Wir nehmen daher an, dass G nicht abelsch ist und setzen

$$A := \langle g_H - 1_G \mid H \in G/\gamma_2(G) \setminus \{\gamma_2(G)\}, \mu(H) \neq l \rangle_K \oplus \bigoplus_{H \in G/\gamma_2(G)} \text{Aug}(H).$$

Aus Korollar 1.26 (ii) (angewandt auf $U := \gamma_2(G)$) zusammen mit Satz 2.25 folgt die Inklusion $A \subseteq \mathcal{Z}_{p^l-1}(\mathcal{J}(KG))$. Sei $n \in \mathbb{N}$ mit $p^n = |G|$ und e die Anzahl der extremalen Konjugiertenklassen von G , das heißt

$$e = |\{H \mid H \in G/\gamma_2(G), \mu(H) = l\}|.$$

Es gilt

$$\begin{aligned} \dim A &\stackrel{1.26(ii)}{=} (p^l - 1)|G/\gamma_2(G)| + |\{H \mid H \in G/\gamma_2(G) \setminus \{\gamma_2(G)\}, \mu(H) \neq l\}| \\ &= (p^l - 1)p^{n-l} + p^{n-l} - 1 - e = p^n - 1 - e. \end{aligned}$$

Wegen

$$\begin{aligned} \dim A &\leq \dim \mathcal{Z}_{p^l-1}(\mathcal{J}(KG)) \\ &= \dim \mathcal{J}(KG) - \dim(\mathcal{J}(KG)/\mathcal{Z}_{p^l-1}(\mathcal{J}(KG))) \\ &\stackrel{2.29(ii)}{\leq} p^n - 1 - e \end{aligned}$$

folgt $\dim A = \dim \mathcal{Z}_{p^l-1}(\mathcal{J}(KG))$ und damit die behauptete Gleichheit. \square

Wir verfolgen bei der Bestimmung der Dimensionen der einzelnen Faktorräume in der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ für eine p -Gruppe G mit zyklischer Kommutatoruntergruppe $\gamma_2(G)$ nun folgende Strategie: Für alle $m \in \underline{|\gamma_2(G)|}$ bestimmen wir (möglichst große) $u_m \in \mathbb{N}$ mit

$$\dim(\mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG))) \geq u_m.$$

Wir haben bereits in Korollar 2.29 eingesehen, dass für jedes m die Anzahl der extremalen Konjugiertenklassen eine solche untere Schranke ist und in Korollar 2.30, dass es im Allgemeinen keine bessere gibt. Wenn wir anschließend

$$\sum_{j=1}^{|\gamma_2(G)|} u_j = \dim \mathcal{J}(KG)$$

nachweisen können, haben wir auf diesem Weg bei obiger Ungleichung die gewünschte Gleichheit eingesehen.

Unser bisheriges Vorgehen liefert dabei das Fundament für diese Vorgehensweise, zeigt aber auch gleichzeitig seine Schwäche auf:

Problem: Sei $l \in \mathbb{N}_0$ mit $p^l = |\gamma_2(G)|$ und $M := \underline{p^l}$. Wir definieren für alle $g \in G$ eine Relation \sim_g auf M durch

$$m \sim_g \tilde{m} \quad :\Longleftrightarrow \quad m - (g, \nu(m))\alpha + 1 = \tilde{m} - (g, \nu(\tilde{m}))\alpha + 1.$$

Als Bildgleichheitsrelation der Abbildung $m \mapsto m - (g, \nu(m))\alpha + 1$ ist \sim_g für alle $g \in G$ eine Äquivalenzrelation auf M . Sei $m \in \underline{p^l - 1}$, $g \in G$ und

$$B := \left\{ g \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(n)} - 1}{n-1} a^i \mid n \in [m]_{\sim_g} \right\}.$$

Nach Satz 2.27 gilt $B \subseteq \mathcal{Z}_{m-(g, \nu(m))\alpha+1}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-(g, \nu(m))\alpha}(\mathcal{J}(KG))$.

Ist dann B modulo $\mathcal{Z}_{m-(g, \nu(m))\alpha}(\mathcal{J}(KG))$ K -linear unabhängig?

Wir betrachten dazu ein Beispiel.

2.31 Beispiel. Sei $p = 5$, G eine 5-Gruppe, $\gamma_2(G)$ zyklisch mit $|\gamma_2(G)| = 125$ und $|\gamma_3(G)| = 25$, $g := 1_G$. (Eine solche Gruppe existiert, wie wir im dritten Beispiel von 2.38 sehen werden.) Es gilt

$$\nu(30) = 1, \quad \nu(14) = 0, \quad (g, \nu(30))\alpha = 20, \quad (g, \nu(14))\alpha = 4 \quad \text{und}$$

$$14 - (g, \nu(14))\alpha + 1 = 11 = 30 - (g, \nu(30))\alpha + 1.$$

Sei $a \in G$ mit $\langle a \rangle = \gamma_2(G)$. Dann gilt nach Satz 2.27 (ii)

$$B := \left\{ \sum_{i=0}^{124} \binom{i+4}{29} a^i, \sum_{i=0}^{124} \binom{i}{13} a^i \right\} \subseteq \mathcal{Z}_{11}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{10}(\mathcal{J}(KG)).$$

Ist dann B modulo $\mathcal{Z}_{10}(\mathcal{J}(KG))$ K -linear unabhängig?

Aus dem folgenden Satz werden wir ableiten, dass wir auf eine derartige K -lineare Unabhängigkeit einer Menge B wie oben nicht schließen können. Zugleich stellt er aber das entscheidene Hilfsmittel für eine Reduktion dieser Problematik dar.

2.32 Satz. Seien G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$, $a \in G$ mit $\langle a \rangle = \gamma_2(G)$ und $l, k \in \mathbb{N}_0$ mit $p^l = |\gamma_2(G)|$ und $p^k = |\gamma_3(G)|$. Für alle $r \in \mathbb{N}_0$ und $g \in G$ sei

$$\psi_{g,r} : \mathbb{N} \rightarrow \mathbb{Q}, \quad m \mapsto \max \{ m - p^{\nu(m)} (p^{l-k} - p^{-r}) + 1, m - p^{l-\kappa(g)} + 1, 1 \}.$$

Für alle $g \in G$, $m \in \underline{p^l - 1}$ und $r \in \underline{\nu(m)}_0$ existiert dann $x \in \text{Aug}(\gamma_2(G))$ mit

$$g \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^i + gx \in \mathcal{Z}_{m\psi_{g,r}}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m\psi_{g,r-1}}(\mathcal{J}(KG)).$$

Insbesondere gilt: Für alle $g \in G$ und $m \in \underline{p^l - 1}$ existiert $x \in \text{Aug}(\gamma_2(G))$ mit

$$g \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^i + gx \in \mathcal{Z}_{m\psi_{g,\nu(m)}}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m\psi_{g,\nu(m)-1}}(\mathcal{J}(KG)).$$

Beweis. Für alle $m \in \mathbb{N}$ sei

$$\tilde{m} := \frac{m}{p^{\nu(m)}}.$$

Sei $g \in G$, $m \in \underline{p^l - 1}$ und $r \in \underline{\nu(m)}_0$. Wir setzen

$$w_{(u,s)} := \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)-s} - 1}{u-1} a^i \quad \text{und} \quad w_u := w_{(u,0)}$$

für alle $u \in \mathbb{Z}$ und $s \in \underline{\nu(m)}_0$.

Ist $r = 0$, so gilt $m\psi_{g,r} = m - (g, \nu(m))\alpha + 1$ und die Behauptung folgt direkt aus Satz 2.27 mit der Setzung $x := 0_{KG}$.

Wir nehmen daher $\nu(m) \geq r > 0$ an. Wegen $m \in \underline{p^l - 1}$ gilt folglich $l \geq 2$. Insbesondere folgt $l > k$ und im Fall $p = 2$ darüber hinaus $l - k \geq 2$ nach Voraussetzung.

Ist $m\psi_{g,r} = 1$, so folgt $m \leq p^{l-\kappa(g)}$ und $m \leq p^{\nu(m)}(p^{l-k} - p^{-r})$. Aus Lemma 1.29 (iii) mit $n = p^{\nu(m)}$ folgt $m \leq p^{\nu(m)}(p^{l-k} - 1)$, also $m - (g, \nu(m))\alpha + 1 = 1$.

Ist $m\psi_{g,r} = m - p^{l-\kappa(g)} + 1$, so folgt $p^{l-\kappa(g)} \leq p^{\nu(m)}(p^{l-k} - p^{-r})$. Aus Lemma 1.29 (ii) folgt $p^{l-\kappa(g)} \leq p^{\nu(m)}(p^{l-k} - 1)$ und damit $(g, \nu(m))\alpha = p^{l-\kappa(g)}$.

In beiden Fällen folgt die Behauptung ebenfalls durch die Wahl von $x := 0_{KG}$ aus Satz 2.27.

Wir nehmen im Folgenden daher

$$m\psi_{g,r} > 1 \quad \text{und} \quad m\psi_{g,r} = m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1 > m - p^{l-\kappa(g)} + 1$$

an. Da wir damit auch $p^{l-\kappa(g)} > p^{\nu(m)}(p^{l-k} - p^{-r})$ voraussetzen, ist g nicht extremal (schärfer gilt sogar $\kappa(g) \leq k$). Wir setzen

$$\beta_j := (-1)^j \tilde{m} \sum_{s=1}^{j+1} (s1_K)^{-1} \quad \text{für alle } j \in \underline{p-2}_0.$$

Für alle $j \in \underline{p-2}_0$ gilt

$$\begin{aligned} \beta_{j-1} + \beta_j &= (-1)^{j-1} \tilde{m} \left(\sum_{s=1}^j (s1_K)^{-1} + (-1) \sum_{s=1}^{j+1} (s1_K)^{-1} \right) \\ &= (-1)^j \tilde{m} ((j+1)1_K)^{-1}. \end{aligned} \tag{2.8}$$

Sei $h \in G$ und $c := \omega_a(a, h) \in \underline{p^{\kappa(a)} - 1}_0$, das heißt $a^h = a[a, h]_{\mathfrak{G}} = a^{-cp^{l-\kappa(a)}+1}$.

Es gilt $k = \kappa(a)$ nach 2.9 (iv) und nach Lemma 2.23 existieren $\delta_1, \dots, \delta_{\tilde{m}-2p^{l-k}+2} \in K$ mit

$$\begin{aligned} w_m^h &= \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^{(-cp^{l-k}+1)i} \\ &= w_m + c(\tilde{m}-1)w_{m-p^{\nu(m)}+l-k} + c\tilde{m}w_{m-p^{\nu(m)}(p^{l-k}-1)} + \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s w_{sp^{\nu(m)}}. \end{aligned}$$

Wegen

$$\begin{aligned} (\tilde{m} - 2p^{l-k} + 2)p^{\nu(m)} &= m - p^{\nu(m)+l-k} (2 - 2p^{k-l}) \\ &\stackrel{l>k}{\leq} m - p^{\nu(m)+l-k} \leq m - p^{\nu(m)}(p^{l-k} - p^{-r}) - 1 \end{aligned}$$

folgt aus Korollar 2.26

$$ghc(\tilde{m} - 1)w_{m-p^{\nu(m)}+l-k}, gh \sum_{s=1}^{\tilde{m}-2p^{l-k}+2} \delta_s w_{sp^{\nu(m)}} \in \mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})-1}(\mathcal{J}(KG)),$$

also

$$ghw_m^h \equiv_{\mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})-1}(\mathcal{J}(KG))} ghw_m + ghc\tilde{m}w_{m-p^{\nu(m)}(p^{l-k}-1)}. \quad (2.9)$$

Im nächsten Schritt geben wir eine andere Darstellung von $ghc\tilde{m}w_{m-p^{\nu(m)}(p^{l-k}-1)}$, dem zweiten Summanden der letzten Kongruenz, an:

Wir setzen

$$A_{(s,j)} := (-1)^j w_{(m-p^{\nu(m)}-s)(p^{l-k}+s-p+j),s)}$$

für alle $j \in \underline{p-2}_0, s \in \underline{r}$.

Wir wenden nun Bemerkung 1.22.6 (ii) auf die Koeffizienten von $w_{m-p^{\nu(m)}(p^{l-k}-1)}$ an, das heißt, wir betrachten in 1.22.6 (ii) $m - p^{\nu(m)}(p^{l-k} - 1) - 1$ statt m und $\nu(m)$ statt n . Wir erhalten für alle $i \in \mathbb{N}_0$

$$\begin{aligned} \binom{i + p^{\nu(m)} - 1}{m - p^{\nu(m)}(p^{l-k} - 1) - 1} &\equiv_p \binom{i + p^{\nu(m)-r} - 1}{m - p^{\nu(m)}(p^{l-k} - p^{-r}) - 1} \\ &+ \sum_{s=1}^r \sum_{j=0}^{p-2} (-1)^j \binom{i + p^{\nu(m)-s} - 1}{m - p^{\nu(m)-s}(p^{l-k}+s-p+j) - 1}. \end{aligned}$$

Nach Definition von $A_{(s,j)}$ erhalten wir also folgende Darstellung von $w_{m-p^{\nu(m)}(p^{l-k}-1)}$:

$$\begin{aligned} w_{m-p^{\nu(m)}(p^{l-k}-1)} &= \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m - p^{\nu(m)}(p^{l-k} - 1) - 1} a^i \\ &= w_{(m-p^{\nu(m)}(p^{l-k}-p^{-r}),r)} + \sum_{s=1}^r \sum_{j=0}^{p-2} A_{(s,j)}. \end{aligned} \quad (2.10)$$

Die Gleichungen (2.9) und (2.10) liefern somit

$$ghw_m^h \equiv_{\mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})-1}(\mathcal{J}(KG))} ghw_m + ghc\tilde{m}w_{(m-p^{\nu(m)}(p^{l-k}-p^{-r}),r)} + ghc\tilde{m} \sum_{s=1}^r \sum_{j=0}^{p-2} A_{(s,j)}. \quad (2.11)$$

Für alle $s \in \underline{r}$ und $j \in \underline{p-2}_0$ sei

$$\begin{aligned} X_{(s,j)} &:= \beta_j w_{(m-p^{\nu(m)}-s)(p^{l-k+s}-p^{l-k}-p+1+j),s)}, \\ B_{(s,j)} &:= \beta_j (-2-j) w_{(m-p^{\nu(m)}-s)(p^{l-k+s}-p+1+j),s)}, \\ C_{(s,j)} &:= \beta_j (-1-j) w_{(m-p^{\nu(m)}-s)(p^{l-k+s}-p+j),s)} \quad \text{und} \\ x &:= \sum_{s=1}^r \sum_{j=0}^{p-2} X_{(s,j)}. \end{aligned}$$

Nach Bemerkung 1.22.5 gilt wegen $m \leq p^l - 1$ insbesondere $x \in \mathcal{J}(KG)$.

Dem Grundprinzip folgend untersuchen wir nun $hg[g, h]_{\mathfrak{S}} x^h$.

Diese Untersuchung führen wir in drei Schritten durch.

- (i) Zunächst betrachten wir $hg[g, h]_{\mathfrak{S}} X_{(s,j)}^h$ für alle $s \in \underline{r}$ und $j \in \underline{p-2}_0$.
- (ii) In einem zweiten Schritt untersuchen wir $hg[g, h]_{\mathfrak{S}} \sum_{j=0}^{p-2} X_{(s,j)}^h$ für alle $s \in \underline{r}$.
- (iii) Im letzten Schritt untersuchen wir schließlich $hg[g, h]_{\mathfrak{S}} x^h$.

(i): Sei $s \in \underline{r}$ und $j \in \underline{p-2}_0$. Wir setzen

$$m_0 := m - p^{\nu(m)-s}(p^{l-k+s} - p^{l-k} - p + 1 + j).$$

Aus $r \geq s > 0$ erhalten wir

$$m \geq m_0 > m - p^{\nu(m)-s}(p^{l-k+s} - 1) \geq m - p^{\nu(m)-r}(p^{l-k+r} - 1) = m - p^{\nu(m)}(p^{l-k} - p^{-r}).$$

Wegen

$$m\psi_{g,r} > 1 \quad \text{und} \quad m\psi_{g,r} = m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1 > m - p^{l-\kappa(g)} + 1$$

gilt folglich

$$\begin{aligned} m_0 &> m - p^{\nu(m)}(p^{l-k} - p^{-r}) > 0 \quad \text{und} \\ m - p^{\nu(m)}(p^{l-k} - p^{-r}) - 1 &\geq m - p^{l-\kappa(g)} \geq m_0 - p^{l-\kappa(g)}. \end{aligned}$$

Damit folgt aus Bemerkung 2.25.1 (ii)

$$\begin{aligned} hg[g, h]_{\mathfrak{S}} w_m &\equiv_{\mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})-1}(\mathcal{J}(KG))} hg w_m \quad \text{und} \\ hg[g, h]_{\mathfrak{S}} X_{(s,j)} &\equiv_{\mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})-1}(\mathcal{J}(KG))} hg X_{(s,j)}. \end{aligned} \tag{2.12}$$

2 p -Gruppen mit zyklischer Kommutatoruntergruppe

Aus $s > 0$ und $0 \leq j \leq p - 2$ erhalten wir außerdem

$$\nu(m_0) = \nu(m - p^{\nu(m)-s}(p^{l-k+s} - p^{l-k} - p + 1 + j)) = \nu(m) - s.$$

Es folgt

$$\begin{aligned} (*) \quad \tilde{m}_0 &= \frac{m_0}{p^{\nu(m)-s}} = \frac{m - p^{\nu(m)-s}(p^{l-k+s} - p^{l-k} - p + 1 + j)}{p^{\nu(m)-s}} \\ &\equiv_p p^{l-k} - p^{l-k+s} + p - 1 - j \equiv_p -1 - j. \end{aligned}$$

Außerdem gilt

$$\begin{aligned} (**) \quad m_0 - p^{\nu(m)-s+l-k} &= m - p^{\nu(m)-s}(p^{l-k+s} - p + 1 + j) \\ m_0 - p^{\nu(m)-s}(p^{l-k} - 1) &= m - p^{\nu(m)-s}(p^{l-k+s} - p + j). \end{aligned}$$

Wir wenden nun Lemma 2.23 auf m_0 für m und $\nu(m) - s$ für n an. Demnach existieren $\mu_1, \dots, \mu_{\tilde{m}_0-2p^{l-k}+2} \in K$ mit

$$\begin{aligned} X_{(s,j)}^h &= \beta_j w_{(m_0,s)}^h \\ &= \beta_j \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)-s} - 1}{m_0 - 1} a^{(-cp^{l-k}+1)i} \\ &\stackrel{2.23}{=} \beta_j w_{(m_0,s)} + c(\tilde{m}_0 - 1) \beta_j w_{(m-p^{\nu(m)-s}(p^{l-k+s}-p+1+j),s)} \\ &\quad + c\tilde{m}_0 \beta_j w_{(m-p^{\nu(m)-s}(p^{l-k+s}-p+j),s)} + \sum_{t=1}^{\tilde{m}_0-2p^{l-k}+2} \mu_t w_{(tp^{\nu(m)-s},s)} \\ &\stackrel{(*)}{=} X_{(s,j)} + cB_{(s,j)} + cC_{(s,j)} + \sum_{t=1}^{\tilde{m}_0-2p^{l-k}+2} \mu_t w_{(tp^{\nu(m)-s},s)}. \end{aligned} \tag{2.13}$$

Es gilt

$$\begin{aligned} &(\tilde{m}_0 - 2p^{l-k} + 2)p^{\nu(m)-s} \\ &\stackrel{(*)}{=} m - p^{\nu(m)-s}(p^{l-k+s} - p^{l-k} - p + 1 + j) - 2p^{l-k+\nu(m)-s} + 2p^{\nu(m)-s} \\ &= m - p^{\nu(m)-s}(p^{l-k+s} + p^{l-k} - p - 1 + j) \\ &= m - p^{\nu(m)+l-k} - p^{\nu(m)-s}(p^{l-k} - p - 1 + j). \end{aligned} \tag{2.14}$$

Wir zeigen nun

$$gh \sum_{t=1}^{\tilde{m}_0-2p^{l-k}+2} \mu_t w_{(tp^{\nu(m)-s},s)} \in \mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})-1}(\mathcal{J}(KG)). \tag{2.15}$$

Ist $l - k \geq 2$ (dies ist nach unserer Annahme insbesondere der Fall, falls $p = 2$ gilt) oder $j \neq 0$, so gilt $p^{l-k} - p - 1 + j \geq 0$ und damit nach (2.14):

$$(\tilde{m}_0 - 2p^{l-k} + 2)p^{\nu(m)-s} \leq m - p^{\nu(m)+l-k} \leq m - p^{\nu(m)}(p^{l-k} - p^{-r}) - 1.$$

Gemäß Korollar 2.26 folgt dann (2.15).

Ist hingegen $j = 0$ und $l - k = 1$, so gilt $p > 2$. Im Fall $\tilde{m}_0 < 2p^{l-k} - 1$ ist (2.15) dann trivial. Ist $\tilde{m}_0 \geq 2p^{l-k} - 1$, so gilt $\tilde{m}_0 \equiv -1 \pmod{p}$ nach (*) und Bemerkung 2.23.1 liefert $\mu_{\tilde{m}_0 - 2p^{l-k} + 2} = 0_K$. Da dann nach (2.14) wiederum

$$(\tilde{m}_0 - 2p^{l-k} + 1)p^{\nu(m)-s} \leq m - p^{\nu(m)+l-k} \leq m - p^{\nu(m)}(p^{l-k} - p^{-r}) - 1$$

gilt, erhalten wir (2.15) auch hier aus Korollar 2.26.

Insgesamt folgt mit Gleichung (2.13)

$$ghX_{(s,j)}^h \equiv_{Z_{m-p^{\nu(m)}(p^{l-k}-p^{-r})-1}(\mathcal{J}(KG))} ghX_{(s,j)} + ghcB_{(s,j)} + ghcC_{(s,j)}. \quad (2.16)$$

(ii): Sei $s \in \underline{r}$. Es gilt

$$\begin{aligned} & \sum_{j=0}^{p-2} \tilde{m}A_{(s,j)} + \sum_{j=0}^{p-2} B_{(s,j)} + \sum_{j=0}^{p-2} C_{(s,j)} \\ &= \sum_{j=0}^{p-2} \tilde{m}A_{(s,j)} + \sum_{j=1}^{p-1} \beta_{j-1}(-1-j)w_{(m-p^{\nu(m)}-s(p^{l-k}+s-p+j),s)} \\ & \quad + \sum_{j=0}^{p-2} \beta_j(-1-j)w_{(m-p^{\nu(m)}-s(p^{l-k}+s-p+j),s)} \\ &= \sum_{j=0}^{p-2} \tilde{m}A_{(s,j)} + \sum_{j=1}^{p-2} (\beta_{j-1} + \beta_j)(-1-j)w_{(m-p^{\nu(m)}-s(p^{l-k}+s-p+j),s)} \\ & \quad + \beta_0(-1)w_{(m-p^{\nu(m)}-s(p^{l-k}+s-p),s)} \\ & \quad + \beta_{p-2}(-p)w_{(m-p^{\nu(m)}-s(p^{l-k}+s-p+p-1),s)} \\ &\stackrel{(2.8)}{=} \sum_{j=0}^{p-2} \tilde{m}A_{(s,j)} + \sum_{j=1}^{p-2} \tilde{m}(-1)^{j+1}w_{(m-p^{\nu(m)}-s(p^{l-k}+s-p+j),s)} \\ & \quad + \tilde{m}(-1)w_{(m-p^{\nu(m)}-s(p^{l-k}+s-p),s)} \\ &= \sum_{j=0}^{p-2} \tilde{m}A_{(s,j)} - \sum_{j=0}^{p-2} \tilde{m}A_{(s,j)} \\ &= 0_{KG}. \end{aligned}$$

2 p -Gruppen mit zyklischer Kommutatoruntergruppe

Es folgt

$$\begin{aligned}
ghw_m^h + gh \sum_{j=0}^{p-2} X_{(s,j)}^h &\stackrel{(2.11),(2.16)}{=} ghw_m + gh \sum_{j=0}^{p-2} X_{(s,j)} \\
&\quad + ghc\tilde{m}w_{(m-p^{\nu(m)}(p^{l-k}-p^{-r}),r)} + ghc\tilde{m} \sum_{t=1}^r \sum_{j=0}^{p-2} A_{(t,j)} \\
&\quad + ghc \sum_{j=0}^{p-2} B_{(s,j)} + ghc \sum_{j=0}^{p-2} C_{(s,j)} \\
&= ghw_m + gh \sum_{j=0}^{p-2} X_{(s,j)} \\
&\quad + ghc\tilde{m}w_{(m-p^{\nu(m)}(p^{l-k}-p^{-r}),r)} + ghc\tilde{m} \sum_{\substack{t=1 \\ t \neq s}}^r \sum_{j=0}^{p-2} A_{(t,j)}.
\end{aligned}$$

(iii): Summation über s liefert insgesamt

$$\begin{aligned}
hg[g,h]_{\mathfrak{S}} w_m^h + hg[g,h]_{\mathfrak{S}} x^h &= ghw_m^h + gh \sum_{s=1}^r \sum_{j=0}^{p-2} X_{(s,j)}^h \\
&\stackrel{(2.12), 2.25.1(ii)}{=} ghw_m + ghx + ghc\tilde{m}w_{(m-p^{\nu(m)}(p^{l-k}-p^{-r}),r)} \\
&\stackrel{2.26}{=} hgw_m + hgx + hgc\tilde{m}w_{(m-p^{\nu(m)}(p^{l-k}-p^{-r}),r)} \\
&\stackrel{2.26}{=} hgw_m + hgx.
\end{aligned}$$

Aus dem Grundprinzip folgt

$$gw_m + gx \in \mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})+1}(\mathcal{J}(KG)) = \mathcal{Z}_{m\psi_{g,r}}(\mathcal{J}(KG)).$$

Nach Korollar 2.18 existiert nun insbesondere $h \in G$, h extremal, sodass $\omega(a, h) = c \not\equiv_p 0$ gilt. Da dann hg nach Satz 2.14 extremal ist und darüber hinaus $\tilde{m} \not\equiv_p 0$ gilt, folgt nach Korollar 2.28

$$hgc\tilde{m}w_{(m-p^{\nu(m)}(p^{l-k}-p^{-r}),r)} \notin \mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})-1}(\mathcal{J}(KG))$$

und aus der Grundidee damit

$$gw_m + gx \notin \mathcal{Z}_{m-p^{\nu(m)}(p^{l-k}-p^{-r})}(\mathcal{J}(KG)) = \mathcal{Z}_{m\psi_{g,r-1}}(\mathcal{J}(KG)).$$

□

Wir greifen noch einmal das Beispiel vor Satz 2.32 auf.

Fortsetzung von Beispiel 2.31

Sei $p = 5$, G eine 5-Gruppe, $\gamma_2(G)$ zyklisch mit $|\gamma_2(G)| = 125$ und $|\gamma_3(G)| = 25$.

Sei $g := 1_G$, $m := 30$ und $r := \nu(m) = 1$. Es gilt

$$30\psi_{1_G,1} = \max \{30 - 5(5 - 5^{-1}) + 1, 30 - 125 + 1, 1\} = \max \{30 - 24 + 1, 1\} = 7.$$

Sei $a \in G$ mit $\langle a \rangle = \gamma_2(G)$. Nach Satz 2.32 existiert $x \in \text{Aug}(\gamma_2(G))$ mit

$$(*) \quad \sum_{i=0}^{124} \binom{i+4}{29} a^i + x \in \mathcal{Z}_7(\mathcal{J}(KG)) \setminus \mathcal{Z}_6(\mathcal{J}(KG)).$$

Da der Beweis von Satz 2.32 konstruktiver Natur ist, können wir ein solches x konkret angeben. Seien β_j , $X_{(1,j)}$, $w_{(u,1)}$ für alle $j \in \mathbb{Z}_0$ und $u \in \mathbb{Z}$ wie im Beweis von Satz 2.32. Dann gilt $\beta_0 = \beta_1 = \beta_2 = 1_K$ und $\beta_3 = 0_K$ und $X_{(1,j)} = \beta_j w_{(14-j,1)}$ für alle $j \in \mathbb{Z}_0$ und

$$x = \sum_{j=0}^3 X_{(1,j)} = \sum_{i=0}^{124} \binom{i}{13} a^i + \sum_{i=0}^{124} \binom{i}{12} a^i + \sum_{i=0}^{124} \binom{i}{11} a^i$$

erfüllt das Geforderte.

Es gilt $13 - (1_G, \nu(13))\alpha + 1 = 13 - 4 + 1 = 10$ und $12 - (1_G, \nu(12))\alpha + 1 = 12 - 4 + 1 = 9$.

Aus Satz 2.25 folgt

$$\sum_{i=0}^{124} \binom{i}{12} a^i, \sum_{i=0}^{124} \binom{i}{11} a^i \in \mathcal{Z}_{10}(\mathcal{J}(KG)).$$

Aus (*) folgt, dass B in Beispiel 2.31 modulo $\mathcal{Z}_{10}(\mathcal{J}(KG))$ K -linear abhängig ist.

Die rein zahlentheoretische Untersuchung der in Satz 2.32 auftretenden Funktion wurde in Abschnitt 1.2.2 durchgeführt. Die Definitionen und Aussagen dieses Abschnitts ordnen wir nun durch folgende Anwendung in den Kontext von p -Gruppen ein:

2.33 Definition. Sei G eine nicht-abelsche p -Gruppe, $l \in \mathbb{N}$ mit $|\gamma_2(G)| = p^l$ und $k \in \mathbb{N}_0$ mit $|\gamma_3(G)| = p^k$. Für alle $H \in G/\gamma_2(G)$ setzen wir

(i) $\psi_H := \psi_{(l,k,\mu(H))}$,

(ii) $\mathcal{Z}_H := \mathcal{Z}_{(l,k,\mu(H))}$,

(iii) $\mathcal{D}_H := \mathcal{D}_{(l,k,\mu(H))}$,

(iv) $\tilde{\mathcal{K}}_H := \tilde{\mathcal{K}}_{(l,k,\mu(H))}$,

(v) $\tilde{\mathcal{E}}_H := \tilde{\mathcal{E}}_{(l,k,\mu(H))}$,

(vi) $\tilde{\mathcal{D}}_H := \tilde{\mathcal{D}}_{(l,k,\mu(H))}$.

Den letzten Teil von Satz 2.32 können wir nun wie folgt formulieren.

2.33.1 Bemerkung. Sei G eine nicht-abelsche p -Gruppe, $\gamma_2(G)$ zyklisch, $a \in G$ mit $\langle a \rangle = \gamma_2(G)$, $\gamma_3(G) \leq \gamma_2(G)^4$ und $l \in \mathbb{N}$ mit $p^l = |\gamma_2(G)|$. Sei $H \in G/\gamma_2(G)$ und $g \in H$ mit $\kappa(g) = \mu(H)$. Für alle $m \in \underline{p^l - 1}$ existiert dann $x \in \text{Aug}(\gamma_2(G))$ mit

$$g \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^i + gx \in \mathcal{Z}_{m\psi_H}(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m\psi_H-1}(\mathcal{J}(KG)).$$

2.33.2 Bemerkung. Es gilt $|\mathcal{Z}_H| = |\mathcal{K}_H(G)|$ für alle $H \in G/\gamma_2(G)$.

Beweis. Ist $\mu(H) > k$, so folgt die Behauptung direkt aus der Definition von \mathcal{Z}_H und Satz 2.12. Gilt andernfalls $\mu(H) \leq k$, so ist

$$\mathcal{Z}_H = \underline{p^{l-k}} \cup \bigcup_{j \in \underline{k-\mu(H)}} \{cp^j \mid c \in \{p^{l-k-1} + 1, \dots, p^{l-k}\}\}.$$

Wiederum folgt aus Satz 2.12 hieraus die Bemerkung. □

2.34 Korollar. Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$, $l \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$ und $a \in G$ mit $\langle a \rangle = \gamma_2(G)$. Sei $H \in G/\gamma_2(G)$ und $g \in H$ mit $\kappa(g) = \mu(H)$. Dann gilt:

(i) Ist $\mu(H) \neq 0$, so ist

$$\left\{ g \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^i \mid m \in \mathcal{Z}_H \right\} \text{ } K\text{-Basis von } \mathcal{Z}(\mathcal{J}(KG)) \cap \langle H \rangle_K.$$

(ii) Ist $\mu(H) = 0$, so ist

$$\left\{ g \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^i \mid m \in \mathcal{Z}_H \setminus \{p^l\} \right\} \text{ } K\text{-Basis von } \mathcal{Z}(\mathcal{J}(KG)) \cap \langle H \rangle_K.$$

Beweis. Ist G abelsch, so gilt $l = 0$, $\mu(H) = 0$, $\mathcal{Z}(\mathcal{J}(KG)) \cap \langle H \rangle_K = \text{Aug}(H) = \{0_{KG}\}$ und $\mathcal{Z}_H = \{1\}$. Hieraus folgt $\mathcal{Z}_H \setminus \{p^l\} = \emptyset$ und damit die Behauptung.

Sei nun G nicht abelsch und $k \in \mathbb{N}_0$ mit $p^k = |\gamma_3(G)|$. Ist $m \in \mathcal{Z}_H$, so gilt

$$1 \stackrel{1.31(ii)}{=} m\psi_{(l,k,\mu(H),0)} \stackrel{\text{Def. } \alpha}{=} m - (g, \nu(m))\alpha + 1.$$

Aus Satz 2.25 folgt

$$\left\{ g \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^i \mid m \in \mathcal{Z}_H \setminus \{p^l\} \right\} \subseteq \mathcal{Z}(\mathcal{J}(KG)) \cap \langle H \rangle_K.$$

Ist $\mu(H) \neq 0$, so gilt $p^l \notin \mathcal{Z}_H$ und aus Bemerkung 2.33.2 und Satz 1.20 folgt

$$\dim \mathcal{Z}(\mathcal{J}(KG)) \cap \langle H \rangle_K = |\mathcal{Z}_H|.$$

Ist $\mu(H) = 0$, so gilt $p^l \in \mathcal{Z}_H$ und ebenfalls aus Bemerkung 2.33.2 und Satz 1.20 folgt

$$\dim \mathcal{Z}(\mathcal{J}(KG)) \cap \langle H \rangle_K = |\mathcal{Z}_H| - 1.$$

In beiden Fällen erhalten wir aus Bemerkung 1.23.2 (ii) das Behauptete. \square

2.35 Satz. Sei G eine nicht-abelsche p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$, $l \in \mathbb{N}$ mit $|\gamma_2(G)| = p^l$ und $k \in \mathbb{N}_0$ mit $|\gamma_3(G)| = p^k$. Dann gilt für alle $H \in G/\gamma_2(G)$ und $m \in \underline{p}^l$:

$$(i) \quad 1\psi_H^- = \mathcal{Z}_H,$$

$$(ii) \quad (m\psi_H = m - p^{l-\mu(H)} + 1 \wedge m\psi_H > 1) \iff m \in \mathcal{D}_H \quad \text{und}$$

$$(iii) \quad (m\psi_H = m - p^{\nu(m)+l-k} + 2 \wedge m\psi_H > 1) \iff m \notin \mathcal{Z}_H \cup \mathcal{D}_H.$$

Weiter gilt für alle $H \in G/\gamma_2(G)$ mit $\mu(H) \leq k$:

$$(iv) \quad \{sp^{k-\mu(H)+1} + 1 \mid s \in \underline{p^{l+\mu(H)-k-1} - p^{l-k-1}}\} = \mathcal{D}_H\psi_H \subseteq (\underline{p}^l \setminus (\mathcal{Z}_H \cup \mathcal{D}_H))\psi_H,$$

$$(v) \quad \forall m \in \underline{p}^l \setminus \{1\} : |m\psi_H^-| \leq 2,$$

$$(vi) \quad \tilde{\mathcal{K}}_H = (-(\mathcal{Z}_H \setminus \{1\}) + p^l + 2) \cup \{sp^{k-\mu(H)+1} + 2 \mid s \in \underline{p^{l+\mu(H)-k-1} - p^{l-k-1} - 1_0}\},$$

$$(vii) \quad \tilde{\mathcal{E}}_H = \underline{p}^l \setminus (\tilde{\mathcal{K}}_H \cup \tilde{\mathcal{D}}_H \cup \{1\}),$$

$$(viii) \quad \tilde{\mathcal{D}}_H = \mathcal{D}_H\psi_H \quad \text{und}$$

$$(ix) \quad |\tilde{\mathcal{E}}_H| = p^l - 2|\tilde{\mathcal{D}}_H| - |\mathcal{Z}_H|.$$

Weiter gilt für alle $H \in G/\gamma_2(G)$ mit $\mu(H) > k$:

$$(x) \quad \psi|_{\mathcal{D}_H} \text{ ist injektiv,}$$

$$(xi) \quad \tilde{\mathcal{E}}_H = \underline{p^l - p^{l-\mu(H)} + 1} \setminus \{1\} = \text{Bild } \psi|_{\mathcal{D}_H},$$

$$(xii) \quad \tilde{\mathcal{D}}_H = \emptyset \quad \text{und}$$

$$(xiii) \quad \tilde{\mathcal{K}}_H = \underline{p^l} \setminus \underline{p^l - p^{l-\mu(H)} + 1}.$$

Beweis. Sämtliche Aussagen folgen direkt aus Lemma 1.33. \square

Vor Satz 2.32 haben wir erläutert, dass unser bisheriges Vorgehen zur Bestimmung der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ die Frage nach der K -linearen Unabhängigkeit gewisser Teilmengen von $\mathcal{J}(KG)$ modulo einem Glied der aufsteigenden Zentralreihe aufwirft. Wir schildern nun, wie aus Bemerkung 2.33.1 und Satz 2.35 eine solche Frage nach der linearen Unabhängigkeit hervorgeht und auf welche Problematik innerhalb der Gruppe G wir diese Frage zurückführen können. Das resultierende Problem ist die Motivation des im Anschluss vorgestellten Satzes.

Vorüberlegung

Sei G eine nicht-abelsche p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$, $a \in G$ mit $\langle a \rangle = \gamma_2(G)$, $l \in \mathbb{N}$ mit $|\gamma_2(G)| = p^l$ und $k \in \mathbb{N}_0$ mit $|\gamma_3(G)| = p^k$. Sei $H \in G/\gamma_2(G)$ und $g \in H$ mit $\kappa(g) = \mu(H)$. Wir setzen

$$w_m := \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^i$$

für alle $m \in \mathbb{N}$.

Nach Satz 2.35 (v) hat jedes $m \in \underline{p^l} \setminus \{1\}$ unter ψ_H höchstens zwei Urbilder. Wir betrachten nun Elemente aus $\underline{p^l} \setminus \{1\}$, die genau zwei Urbilder haben.

Ist $\mu(H) > k$, so gilt $\tilde{\mathcal{D}}_H = \emptyset$ nach 2.35 (xii). Gilt $\mu(H) = 0$, so gilt $\tilde{\mathcal{D}}_H = \emptyset$ nach 2.35 (iv) und (viii). Wir nehmen deshalb $0 < \mu(H) \leq k$ an.

Sei dann $m \in \tilde{\mathcal{D}}_H$. In 2.35 (viii) und (iv) haben wir die Elemente aus $\underline{p^l} \setminus \{1\}$ bestimmt, die unter ψ_H genau zwei Urbilder haben. Demnach existiert $s \in \underline{p^{l+\mu(H)-k-1} - p^{l-k-1}}$ mit $m = sp^{k-\mu(H)+1} + 1$. Sei $m_1 := p^{l-\mu(H)} + sp^{k-\mu(H)+1}$, $m_2 := p^{l-k} + sp^{k-\mu(H)+1} - 1$. Es gilt $\nu(m_1) \geq k - \mu(H) + 1$, $m_2 \equiv -1 \pmod{p}$ und damit $\nu(m_2) = 0$. Es folgt

$$\begin{aligned} p^{l-\mu(H)} &> p^{l-k} - 1 = p^{\nu(m_2)} (p^{l-k} - 1) = (g, \nu(m_2))\alpha \quad \text{und} \\ p^{\nu(m_1)} (p^{l-k} - 1) &\geq p^{k-\mu(H)+1} (p^{l-k} - 1) = p^{l-\mu(H)} (p - p^{k-l+1}) \geq p^{l-\mu(H)} = (g, \nu(m_1))\alpha. \end{aligned}$$

Wir erhalten unter Anwendung von Lemma 1.29 (ii)

$$m_1\psi_H = m = m_1 - (g, \nu(m_1))\alpha + 1 \quad \text{und} \quad m_2\psi_H = m = m_2 - (g, \nu(m_2))\alpha + 1. \quad (2.17)$$

Wegen $m \in \tilde{\mathcal{D}}_H$ folgt $m\psi_H^- = \{m_1, m_2\}$.

Wir unterscheiden nun zwei Fälle:

(i) Es gelte $m_1 = p^l$. Dann gilt $m_1\psi_H = m = p^l - p^{l-\mu(H)} + 1 = |\gamma_2(G)| - \frac{|\gamma_2(G)|}{|g^G|} + 1$. Nach Satz 2.27 gilt

$$g - 1_G \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG)).$$

Nach (2.17) und Satz 2.27 gilt

$$gw_{m_2} \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG)).$$

(ii) Es gelte $m_1 \neq p^l$. Nach (2.17) und Satz 2.27 gilt

$$gw_{m_1}, gw_{m_2} \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG)).$$

Ist dann

$$\{g - 1_G, gw_{m_2}\} \text{ beziehungsweise } \{gw_{m_1}, gw_{m_2}\}$$

modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ K -linear unabhängig?

Wegen $k > 0$ gilt $l > 1$ und aus Bemerkung 2.24.1 (iii) folgt

$$(*) \quad m_1 - p^{\nu(m_1)}(p^{l-k} - 1) < m_1 - (g, \nu(m_1))\alpha = m_1 - p^{l-\mu(H)} = sp^{k-\mu(H)+1} \quad \text{und}$$

$$(**) \quad m_2 - p^{l-\mu(H)} < m_2 - (g, \nu(m_2))\alpha = m_2 - (p^{l-k} - 1) = sp^{k-\mu(H)+1}.$$

Wir erhalten für alle $h \in G$:

$$\begin{aligned} hg[g, h]_{\mathfrak{S}} w_{m_1}^h &\stackrel{(*), 2.25.1(i)}{\equiv} hga^{-\omega(g, h)p^{l-\mu(H)}} w_{m_1} \\ &\stackrel{2.22, 2.26}{\equiv} hgw_{m_1} + hg(\omega(g, h)) \sum_{i=0}^{p^l-1} \binom{i + \nu(m_1) - 1}{sp^{k-\mu(H)+1} - 1} a^i \quad (2.18) \\ &\stackrel{2.25.1(iii)}{\equiv} hgw_{m_1} + hg(\omega(g, h)) \sum_{i=0}^{p^l-1} \binom{i}{sp^{k-\mu(H)+1} - 1} a^i \end{aligned}$$

und

$$\begin{aligned} hg[g, h]_{\mathfrak{S}} w_{m_2}^h &= hg[g, h]_{\mathfrak{S}} \sum_{i=0}^{p^l-1} \binom{i}{m_2 - 1} a^{(-\omega(a, h)p^{l-k} + 1)i} \\ &\stackrel{2.23, 2.26}{\equiv} hg[g, h]_{\mathfrak{S}} w_{m_2} + hg[g, h]_{\mathfrak{S}} (\omega(a, h))m_2 \sum_{i=0}^{p^l-1} \binom{i}{sp^{k-\mu(H)+1} - 1} a^i \\ &\stackrel{(**), 2.25.1(ii)}{\equiv} hgw_{m_2} + hg[g, h]_{\mathfrak{S}} (\omega(a, h))m_2 \sum_{i=0}^{p^l-1} \binom{i}{sp^{k-\mu(H)+1} - 1} a^i \\ &\stackrel{2.25.1(iii)}{\equiv} hgw_{m_2} - hg(\omega(a, h)) \sum_{i=0}^{p^l-1} \binom{i}{sp^{k-\mu(H)+1} - 1} a^i. \end{aligned} \quad (2.19)$$

Da $\mu(H) \leq k$ gilt, ist g nicht extremal. Nach Satz 2.14 ist damit hg extremal für alle extremalen $h \in G$. Insbesondere gilt für alle extremalen $h \in G$:

$$hg \sum_{i=0}^{p^l-1} \binom{i}{sp^{k-\mu(H)+1} - 1} a^i \notin \mathcal{Z}_{sp^{k-\mu(H)+1}-1}(\mathcal{J}(KG)).$$

Für alle $h \in G$, h extremal, erhalten wir aus dem Grundprinzip in Abschnitt 1.2.2 und den Gleichungen (2.18) und (2.19):

Sind $\lambda_1, \lambda_2 \in K$ mit $\lambda_1(g - 1_G) + \lambda_2 gw_2 \in \mathcal{Z}_{m-1}(\mathcal{J}(KG))$ beziehungsweise $\lambda_1 gw_1 + \lambda_2 gw_2 \in \mathcal{Z}_{m-1}(\mathcal{J}(KG))$, so folgt

$$\lambda_1 \omega(g, h) - \lambda_2 \omega(a, h) = 0_K.$$

Um die Frage nach der linearen Unabhängigkeit zu bejahen, reicht es daher nun die folgende Aussage zu beweisen, für welche wir ohne Beschränkung der Allgemeinheit $\mathbb{Z}/p\mathbb{Z} \subseteq K$ annehmen.

2.36 Satz. *Sei G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $\gamma_3(G) \leq \gamma_2(G)^4$ und $k \in \mathbb{N}_0$ mit $|\gamma_3(G)| = p^k$. Sei E die Menge der extremalen Elemente von G . Für alle $H \in G/\gamma_2(G)$ mit $0 < \mu(H) \leq k$, $g \in H$ mit $\kappa(g) = \mu(H)$ und $a \in G$ mit $\langle a \rangle = \gamma_2(G)$ ist dann $\{\overline{\omega_{(a,g)}}|_E, \overline{\omega_{(a,a)}}|_E\}$ K -linear unabhängig.*

Beweis. Sei $H \in G/\gamma_2(G)$ mit $0 < \mu(H) \leq k$ und $g \in H$ mit $\kappa(g) = \mu(H)$. Insbesondere gilt dann $cl(G) > 2$ und $g \notin \mathcal{Z}(G)$. Seien x, y, s wie in Satz 2.21 und $a := [x, y]_{\mathfrak{G}}$. Dann gilt $a \notin \mathcal{Z}(G)$. Um den Satz zu beweisen, zeigen wir schärfer:

$$\text{Kern } \overline{\omega_{(a,g)}}|_E \neq \text{Kern } \overline{\omega_{(a,a)}}|_E.$$

Dafür beweisen wir:

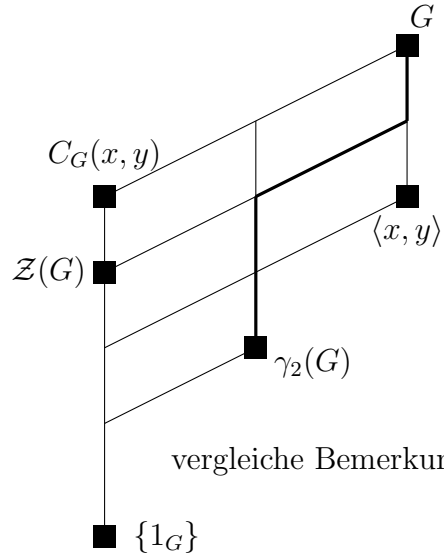
$$(*) \quad \text{Es existiert } \tilde{g} \in E \cap C_G(a) \text{ mit } \langle [g, \tilde{g}]_{\mathfrak{G}} \rangle = [\{g\}, G]_{\mathfrak{G}}.$$

Nach Bemerkung 2.13.1 (iii) gilt dann $\tilde{g} \notin \text{Kern } \overline{\omega_{(a,g)}}|_E$, aber $\tilde{g} \in \text{Kern } \overline{\omega_{(a,a)}}|_E$. Wegen $C_G(a) = C_G(\gamma_2(G)) = C_G(b)$ für alle $b \in \gamma_2(G)$ mit $\langle b \rangle = \gamma_2(G)$ reicht es daher auch den speziell gewählten Erzeuger a zu betrachten.

Für alle $u \in G$ sei

$$o_u := o(u\mathcal{Z}(G)\gamma_2(G)).$$

Sei \mathfrak{R}_1 ein in $\mathcal{Z}(G)$ enthaltenes Repräsentantensystem von $\mathcal{Z}(G)\gamma_2(G)/\gamma_2(G)$. Weiter existiert ein in $\{x^{n_1}y^{n_2} \mid n_1 \in \underline{o_x - 1_0}, n_2 \in \underline{o_y - 1_0}\}$ enthaltenes Repräsentantensystem \mathfrak{R}_2 von $\mathcal{Z}(G)\langle x, y \rangle/\mathcal{Z}(G)\gamma_2(G)$. Dann ist $\mathfrak{R}_1\mathfrak{R}_2$ ein Repräsentantensystem von $\mathcal{Z}(G)\langle x, y \rangle/\gamma_2(G)$. Nach (ii) in Satz 2.21 existiert nun ein in $C_G(x, y)$ enthaltenes Repräsentantensystem \mathfrak{R}_3 von $G/\mathcal{Z}(G)\langle x, y \rangle$. Sei $\mathfrak{R} := \mathfrak{R}_1\mathfrak{R}_2\mathfrak{R}_3$. Dann ist \mathfrak{R} ein Repräsentantensystem von $G/\gamma_2(G)$.



Sei $r \in \mathfrak{R} \cap H$. Für alle $i \in \mathfrak{J}$ existiert $r_i \in \mathfrak{R}_i$ mit $r = r_1 r_2 r_3$. Seien weiter $m_1 \in \underline{o_x - 1}_0$ und $m_2 \in \underline{o_y - 1}_0$ mit $r_2 = x^{m_1} y^{m_2}$.

Unser nächstes Ziel ist es, Elemente $h \in G$ mit $[\{r\}, G]_{\mathfrak{G}} = \langle [r, h]_{\mathfrak{G}} \rangle$ zu bestimmen. Sei dazu $h \in G$. Nach (ii) und (iii) in Satz 2.21 existieren $t, v \in \mathbb{N}_0$, $w \in C_G(x, y)$ mit $h = x^v y^t w$. Nach Satz 2.21 (i) und Bemerkung 2.21.1 gilt $y, r_3 \in C_G(\gamma_2(G))$. Hieraus folgt

$$\begin{aligned} [x^{m_1}, y^t]_{\mathfrak{G}} [y^{m_2}, x^v]_{\mathfrak{G}} [r_3, w]_{\mathfrak{G}} &\stackrel{2.2}{=} [x^{m_1}, h]_{\mathfrak{G}} [y^{m_2}, h]_{\mathfrak{G}} [r_3, h]_{\mathfrak{G}} \\ &\stackrel{2.2}{=} [x^{m_1} y^{m_2} r_3, h]_{\mathfrak{G}} \\ &\stackrel{r_1 \in \mathcal{Z}(G)}{=} [r_1 r_2 r_3, h]_{\mathfrak{G}} \\ &= [r, h]_{\mathfrak{G}} \in [\{r\}, G]_{\mathfrak{G}}. \end{aligned} \tag{2.20}$$

Da $[\{r\}, G]_{\mathfrak{G}}$ eine zyklische p -Gruppe ist, folgt

$$\begin{aligned} [\{r\}, G]_{\mathfrak{G}} &= [\{x^{m_1}\}, \langle y \rangle]_{\mathfrak{G}} \stackrel{2.2}{=} \langle [x^{m_1}, y]_{\mathfrak{G}} \rangle \text{ oder } [\{r\}, G]_{\mathfrak{G}} = [\{y^{m_2}\}, \langle x \rangle]_{\mathfrak{G}} \stackrel{2.2}{=} \langle [y^{m_2}, x]_{\mathfrak{G}} \rangle \text{ oder} \\ &[\{r\}, G]_{\mathfrak{G}} = [\{r_3\}, C_G(x, y)]_{\mathfrak{G}} = \langle [r_3, \tilde{w}]_{\mathfrak{G}} \rangle \text{ für ein geeignetes } \tilde{w} \in C_G(x, y). \end{aligned}$$

Wir unterscheiden nun die drei Möglichkeiten:

(i) Es gelte $[\{r\}, G]_{\mathfrak{G}} = \langle [x^{m_1}, y]_{\mathfrak{G}} \rangle \stackrel{(2.20)}{=} \langle [r, y]_{\mathfrak{G}} \rangle$. Wir setzen $\tilde{g} := y$. Dann ist \tilde{g} extremal nach Satz 2.21. Wegen $\mu(H) > 0$ gilt $r \notin \mathcal{Z}(G)$ und folglich $\omega_a(r, \tilde{g}) \not\equiv 0$ nach Bemerkung 2.13.1 (iii). Außerdem gilt $\tilde{g} \in C_G(a)$ nach Bemerkung 2.21.1.

(ii) Es existiere $\tilde{w} \in C_G(x, y)$ mit $[\{r\}, G]_{\mathfrak{G}} = \langle [r_3, \tilde{w}]_{\mathfrak{G}} \rangle \stackrel{(2.20)}{=} \langle [r, \tilde{w}]_{\mathfrak{G}} \rangle$. Gilt darüber hinaus $[\{r\}, G]_{\mathfrak{G}} = \langle [x^{m_1}, y]_{\mathfrak{G}} \rangle$, so wählen wir wie in (i) $\tilde{g} := y$. Wir nehmen daher

$$(**) \quad \langle [x^{m_1}, y]_{\mathfrak{G}} \rangle < [\{r\}, G]_{\mathfrak{G}}$$

an. Ist \tilde{w} extremal, so setzen wir $\tilde{g} := \tilde{w}$. Dann gilt $\tilde{g} \in C_G(a)$ nach Wahl von a . Andernfalls ist \tilde{w} nicht extremal. Wir betrachten dann das nach Satz 2.14 extremale Element $\tilde{g} := y\tilde{w} \in C_G(a)$. Es folgt

$$\langle [r, y\tilde{w}]_{\mathfrak{G}} \rangle \stackrel{(2.20)}{=} \langle [x^{m_1}, y]_{\mathfrak{G}} [r_3, \tilde{w}]_{\mathfrak{G}} \rangle \stackrel{(**)}{=} \langle [r_3, \tilde{w}]_{\mathfrak{G}} \rangle = [\{r\}, G]_{\mathfrak{G}}.$$

Wie in (i) folgt außerdem $\omega_a(r, \tilde{g}) \not\equiv 0$.

(iii) Es gelte $[\{r\}, G]_{\mathfrak{G}} = \langle [y^{m_2}, x]_{\mathfrak{G}} \rangle \stackrel{(2.20)}{=} \langle [r, x]_{\mathfrak{G}} \rangle$. Dann gilt $m_2 \neq 0$ gemäß unserer Voraussetzung über H . Nach 2.21 ist y extremal, das heißt es gilt $\kappa(y) = l$. Wir erhalten

$$\begin{aligned} |r^G| &\stackrel{2.9}{=} |[\{r\}, G]_{\mathfrak{G}}| = |\langle [y^{m_2}, x]_{\mathfrak{G}} \rangle| \stackrel{2.21(ii)}{=} |[\{y^{m_2}\}, G]_{\mathfrak{G}}| \stackrel{2.9}{=} |(y^{m_2})^G| \\ &\stackrel{2.10.1}{=} p^{l-\nu(m_2)} \stackrel{m_2 < o_y}{\stackrel{2.10(i)}{>}} |(y^{o_y})^G| \stackrel{2.21.3, 2.21.1}{=} |\gamma_3(G)|. \end{aligned}$$

Da wir aber $\mu(H) \leq k$ voraussetzen, erhalten wir auch

$$p^{\mu(H)} \leq |r^G| \stackrel{2.12}{\leq} p^k = |\gamma_3(G)|$$

und damit einen Widerspruch.

Insgesamt folgt also: Es existiert $\tilde{g} \in E \cap C_G(a)$ mit $\langle [r, \tilde{g}]_{\mathfrak{G}} \rangle = [\{r\}, G]_{\mathfrak{G}}$. Damit ist die Behauptung für das speziell gewählte Repräsentantensystem \mathfrak{R} bewiesen. Satz 2.36 folgt nun aus folgender Bemerkung. \square

2.36.1 Bemerkung. Sei \mathfrak{R} ein Repräsentantensystem von $G/\gamma_2(G)$, $\tilde{g} \in C_G(\gamma_2(G))$ und $r \in \mathfrak{R}$. Gilt dann $\langle [r, \tilde{g}]_{\mathfrak{G}} \rangle = [\{r\}, G]_{\mathfrak{G}}$, so gilt $\langle [g, \tilde{g}]_{\mathfrak{G}} \rangle = [\{g\}, G]_{\mathfrak{G}} = \langle [r, \tilde{g}]_{\mathfrak{G}} \rangle$ für alle $g \in r\gamma_2(G)$ mit $\kappa(g) \leq \kappa(r)$.

Beweis. Es gelte $\langle [r, \tilde{g}]_{\mathfrak{G}} \rangle = [\{r\}, G]_{\mathfrak{G}}$. Sei $g \in r\gamma_2(G)$. Dann existiert $b \in \gamma_2(G)$ mit $g = rb$. Es folgt

$$[g, \tilde{g}]_{\mathfrak{G}} = [rb, \tilde{g}]_{\mathfrak{G}} \stackrel{2.2}{=} [r, \tilde{g}]_{\mathfrak{G}}^b [b, \tilde{g}]_{\mathfrak{G}} \stackrel{\tilde{g} \in C_G(\gamma_2(G))}{=} [r, \tilde{g}]_{\mathfrak{G}}.$$

Die Behauptung folgt aus Satz 2.9. \square

Wir können nun den Hauptsatz dieses Kapitels formulieren und beweisen.

2.37 Hauptsatz.

Sei G eine nicht-abelsche p -Gruppe, $\gamma_2(G)$ zyklisch und $\gamma_3(G) \leq \gamma_2(G)^4$. Für alle $m \in \mathbb{N}$ sei

$$d_m := \dim(\mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG))).$$

Ist $m \in \mathbb{N}_{>1}$, so gilt

$$d_m = \left| \left\{ H \mid H \in G/\gamma_2(G), m \in \tilde{\mathcal{E}}_H \right\} \right| + 2 \left| \left\{ H \mid H \in G/\gamma_2(G), m \in \tilde{\mathcal{D}}_H \right\} \right|.$$

Sei $l \in \mathbb{N}$ mit $p^l = |\gamma_2(G)|$ und $k \in \mathbb{N}_0$ mit $p^k = |\gamma_3(G)|$. Genauer gilt:

(i) Ist $m \in \underline{p^l} \setminus \underline{p^l - p^{l-k} + 1}$, so gilt

$$d_m = \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) > k, m \leq p^l - p^{l-\mu(H)} + 1 \right\} \right|.$$

(ii) Ist $m \in \underline{p^l - p^{l-k} + 1} \setminus \{1\}$ und $1 \not\equiv_p m \not\equiv_p 2$, so gilt

$$d_m = |G/\gamma_2(G)|.$$

(iii) Ist $m \in \underline{p^l - p^{l-k} + 1} \setminus \{1\}$ und $m \equiv_p 2$, so gilt

$$d_m = \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) > k \right\} \right| + \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \notin \tilde{\mathcal{K}}_H \right\} \right|.$$

(iv) Ist $m \in \underline{p^l - p^{l-k} + 1} \setminus \{1\}$ und $m \equiv 1 \pmod{p}$, so gilt

$$\begin{aligned} d_m &= |\{H \mid H \in G/\gamma_2(G), \mu(H) > k\}| \\ &\quad + 2 \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \in \tilde{\mathcal{D}}_H \right\} \right| \\ &\quad + \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \notin \tilde{\mathcal{D}}_H \right\} \right|. \end{aligned}$$

Beweis. Sei $a \in G$ mit $\langle a \rangle = \gamma_2(G)$. Für alle $m \in \mathbb{N}$ sei

$$w_m := \sum_{i=0}^{p^l-1} \binom{i + p^{\nu(m)} - 1}{m-1} a^i.$$

Aus den bisherigen Überlegungen dieses Kapitels erhalten wir die folgende Aussagen (I), (II) und (III):

Sei $H \in G/\gamma_2(G)$ und $g \in H$ mit $\kappa(g) = \mu(H)$. Dann gilt:

- (I) Sei $\mu(H) > k$ und $m \in \tilde{\mathcal{E}}_H$. Dann ist $\hat{m} := m + p^{l-\mu(H)} - 1$ das Urbild von m unter ψ_H nach Satz 2.35 (ii) und (xi). Ist $\hat{m} < p^l$, so gilt $gw_{\hat{m}} \in \text{Aug}(g\gamma_2(G))$ nach Bemerkung 1.22.5 und

$$gw_{\hat{m}} \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG))$$

nach Satz 2.28.

Ist $\hat{m} = p^l$, so gilt $w_{\hat{m}} = 1_G$ nach Lemma 1.28 (ii) und $m = p^l - p^{l-\mu(H)} + 1$.

Es folgt $gw_{\hat{m}} - 1_G = g - 1_G \in \text{Aug}(g\gamma_2(G) \cup \mathcal{Z}(G))$ und Satz 2.27 (iii) liefert

$$g - 1_G \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG)).$$

- (II) Sei $\mu(H) \leq k$ und $m \in \tilde{\mathcal{E}}_H$. Nach Definition von \mathcal{D}_H gilt $p^l \in \mathcal{D}_H$. Also gilt $p^l \in \tilde{\mathcal{D}}_H \psi_H^-$ nach 2.35 (viii) und damit $p^l \notin \tilde{\mathcal{E}}_H \psi_H^-$. Sei daher $\hat{m} \in \underline{p^l - 1}$ das Urbild von m unter ψ_H . Nach Definition von $\tilde{\mathcal{E}}_H$ und Bemerkung 2.33.1 existiert (das im Beweis von Satz 2.32 konstruktiv konstruierte Element) $x \in \text{Aug}(\gamma_2(G))$ mit

$$gw_{\hat{m}} + gx \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG)).$$

Außerdem gilt $gw_{\hat{m}} + gx \in \text{Aug}(g\gamma_2(G))$.

- (III) Sei $\mu(H) \leq k$. Ist $\mu(H) = 0$, so gilt $\mathcal{D}_H \psi_H = \emptyset$ nach Satz 2.35 (iv) und damit $\tilde{\mathcal{D}}_H = \emptyset$. Sei daher $\mu(H) > 0$ und $m \in \tilde{\mathcal{D}}_H$. Seien m_1 und m_2 die Urbilder von m unter ψ_H . Ist $m_1 \neq p^l \neq m_2$, so gilt $gw_{m_1}, gw_{m_2} \in \text{Aug}(g\gamma_2(G))$ nach Bemerkung 1.22.5. Außerdem gilt nach der Vorüberlegung zu Satz 2.36 und Satz 2.36:

$$gw_{m_1}, gw_{m_2} \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG))$$

und $\{gw_{m_1}, gw_{m_2}\}$ ist modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ K -linear unabhängig.

Ist andernfalls ohne Beschränkung der Allgemeinheit $m_1 = p^l$ und $m_2 < p^l$, so gilt $g - 1_G \in \text{Aug}(g\gamma_2(G) \cup \mathcal{Z}(G))$, $gw_{m_2} \in \text{Aug}(g\gamma_2(G))$ und wir erhalten ebenfalls aus der Vorüberlegung zu Satz 2.36 und Satz 2.36:

$$g - 1_G, gw_{m_2} \in \mathcal{Z}_m(\mathcal{J}(KG)) \setminus \mathcal{Z}_{m-1}(\mathcal{J}(KG))$$

und $\{g - 1_G, gw_{m_2}\}$ ist modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ K -linear unabhängig.

Diese drei Aussagen liefern zusammen mit Bemerkung 1.14.1 folgende Abschätzung für alle $m \in \mathbb{N}_{>1}$:

$$\begin{aligned} d_m &\geq \left| \left\{ H \mid H \in G/\gamma_2(G), m \in \tilde{\mathcal{E}}_H \right\} \right| + 2 \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \in \tilde{\mathcal{D}}_H \right\} \right| \\ &\stackrel{2.35(\text{xii})}{=} \left| \left\{ H \mid H \in G/\gamma_2(G), m \in \tilde{\mathcal{E}}_H \right\} \right| + 2 \left| \left\{ H \mid H \in G/\gamma_2(G), m \in \tilde{\mathcal{D}}_H \right\} \right|. \end{aligned} \quad (2.21)$$

Es folgt

$$\begin{aligned} \dim \mathcal{J}(KG) &\stackrel{2.29(\text{i})}{=} \dim \mathcal{Z}(\mathcal{J}(KG)) + \sum_{m=2}^{p^l} d_m \\ &\stackrel{(2.21)}{\geq} \dim \mathcal{Z}(\mathcal{J}(KG)) + \sum_{m=2}^{p^l} \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) > k, m \in \tilde{\mathcal{E}}_H \right\} \right| \\ &\quad + \sum_{m=2}^{p^l} \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \in \tilde{\mathcal{E}}_H \right\} \right| \\ &\quad + \sum_{m=2}^{p^l} 2 \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \in \tilde{\mathcal{D}}_H \right\} \right| \\ &\stackrel{1.20(\text{iii}), 2.33.2}{=} \left(\sum_{H \in G/\gamma_2(G)} |\mathcal{Z}_H| \right) - 1 + \sum_{\substack{H \in G/\gamma_2(G) \\ \mu(H) > k}} |\tilde{\mathcal{E}}_H| + \sum_{\substack{H \in G/\gamma_2(G) \\ \mu(H) \leq k}} |\tilde{\mathcal{E}}_H| + \sum_{\substack{H \in G/\gamma_2(G) \\ \mu(H) \leq k}} 2|\tilde{\mathcal{D}}_H| \\ &\stackrel{2.35(\text{x}), (\text{xi})}{=} \left(\sum_{\substack{H \in G/\gamma_2(G) \\ \mu(H) > k}} |\mathcal{Z}_H| + |\mathcal{D}_H| \right) - 1 + \sum_{\substack{H \in G/\gamma_2(G) \\ \mu(H) \leq k}} \left(|\mathcal{Z}_H| + 2|\tilde{\mathcal{D}}_H| + |\tilde{\mathcal{E}}_H| \right) \\ &\stackrel{2.35(\text{ix})}{=} \left(\sum_{\substack{H \in G/\gamma_2(G) \\ \mu(H) > k}} p^l \right) - 1 + \sum_{\substack{H \in G/\gamma_2(G) \\ \mu(H) \leq k}} p^l \\ &= |G| - 1 \\ &= \dim \mathcal{J}(KG). \end{aligned}$$

Also gilt in obiger Ungleichung (2.21) die zu beweisende Gleichheit.

Mit Hilfe des Bewiesenen erläutern wir nun die Spezialisierungen. Für alle $H \in G/\gamma_2(G)$ gilt:

(i): Ist $\mu(H) \leq k$, so gilt $\underline{p^{l-k}} \subseteq \mathcal{Z}_H$ und damit $\tilde{\mathcal{E}}_H \subseteq \underline{p^l - p^{l-k} + 1} \setminus \{1\}$ nach Satz 2.35 (vi) und (vii). Außerdem gilt $\tilde{\mathcal{D}}_H \subseteq \underline{p^l - p^{l-k} + 1} \setminus \{1\}$ nach 2.35 (viii) und (iv). Ist $\mu(H) > k$, so gilt $\tilde{\mathcal{E}}_H = \underline{p^l - p^{l-\mu(H)} + 1} \setminus \{1\}$ nach 2.35 (xi).

(ii): Ist $\mu(H) > k$, so gilt $\underline{p^l - p^{l-k} + 1} \setminus \{1\} \subseteq \underline{p^l - p^{l-\mu(H)} + 1} \setminus \{1\} = \tilde{\mathcal{E}}_H$. Ist $\mu(H) \leq k$ und $m \in \underline{p^l - p^{l-k} + 1} \setminus \{1\}$, $2 \not\equiv m \not\equiv 1 \pmod{p}$, so gilt $m \notin \tilde{\mathcal{D}}_H$ nach Satz 2.35 (iv), (viii) und $m \notin \tilde{\mathcal{K}}_H$ nach Definition von \mathcal{Z}_H und 2.35 (vi). Nach 2.35 (vii) folgt dann $m \in \tilde{\mathcal{E}}_H$.

(iii): Ist $\mu(H) > k$, so gilt $\underline{p^l - p^{l-k} + 1} \setminus \{1\} \subseteq \underline{p^l - p^{l-\mu(H)} + 1} \setminus \{1\} = \tilde{\mathcal{E}}_H$. Ist $\mu(H) \leq k$ und $m \in \underline{p^l - p^{l-k} + 1} \setminus \{1\}$ mit $m \equiv 2 \pmod{p}$, so gilt $m \notin \tilde{\mathcal{D}}_H$ nach Satz 2.35 (iv) und (viii). Dann gilt nach 2.35 (vii) $m \notin \tilde{\mathcal{K}}_H$ genau dann, wenn $m \in \tilde{\mathcal{E}}_H$ gilt.

(iv): Ist $\mu(H) > k$, so gilt $\underline{p^l - p^{l-k} + 1} \setminus \{1\} \subseteq \underline{p^l - p^{l-\mu(H)} + 1} \setminus \{1\} = \tilde{\mathcal{E}}_H$. Ist $\mu(H) \leq k$ und $m \in \underline{p^l - p^{l-k} + 1} \setminus \{1\}$ mit $m \equiv 1 \pmod{p}$, so gilt $m \notin \tilde{\mathcal{K}}_H$ nach Definition von \mathcal{Z}_H und Satz 2.35 (vi). Dann gilt nach 2.35 (vii) $m \notin \tilde{\mathcal{D}}_H$ genau dann, wenn $m \in \tilde{\mathcal{E}}_H$ gilt.

Aus

$$d_m = \left| \left\{ H \mid H \in G/\gamma_2(G), m \in \tilde{\mathcal{E}}_H \right\} \right| + 2 \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \in \tilde{\mathcal{D}}_H \right\} \right|$$

folgt dann in jedem der vier Fälle die Behauptung. \square

2.37.1 Bemerkung. Sei $m \in \underline{p^l} \setminus \{1\}$. Die Aussagen (I) - (III) im Beweis des Hauptsatzes 2.37 liefern ein Verfahren zur Bestimmung einer Basis von $\mathcal{Z}_m(\mathcal{J}(KG))$ modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$. Ist $H \in G/\gamma_2(G)$ und $m \in \tilde{\mathcal{E}}_H$, so sei b_H das in der Aussage (I) beziehungsweise (II) angegebene Element aus $\text{Aug}(H \cup \mathcal{Z}(G))$. Ist $H \in G/\gamma_2(G)$ und $m \in \tilde{\mathcal{D}}_H$, so seien $b_{H,1}$ und $b_{H,2}$ die in Aussage (III) angegebenen Elemente aus $\text{Aug}(H \cup \mathcal{Z}(G))$. Sei

$$\mathfrak{B}_m := \left\{ b_H \mid H \in G/\gamma_2(G), m \in \tilde{\mathcal{E}}_H \right\} \cup \left\{ b_{H,i} \mid H \in G/\gamma_2(G), i \in \{1, 2\}, m \in \tilde{\mathcal{D}}_H \right\}.$$

Wir haben bewiesen, dass $d_m = |\mathfrak{B}_m|$ gilt, indem wir ausgenutzt haben, dass $\mathfrak{B}_m \subseteq \mathcal{Z}_m(\mathcal{J}(KG))$ modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ K -linear unabhängig ist. Damit haben wir also gezeigt:

\mathfrak{B}_m ist modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ eine K -Basis von $\mathcal{Z}_m(\mathcal{J}(KG))$.

2.38 Beispiele. Seien G eine p -Gruppe, $\gamma_2(G)$ zyklisch, $l, k \in \mathbb{N}_0$ mit $|\gamma_2(G)| = p^l$, $|\gamma_3(G)| = p^k$. Für alle $m \in \mathbb{N}$ sei

$$d_m := \dim(\mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG))).$$

1. Sei $cl(G) = 2$. Dann gilt $k = 0$ und $\gamma_3(G) \leq \gamma_2(G)^4$. Wir erhalten für alle $H \in G/\gamma_2(G)$ mit $\mu(H) = 0$ (das heißt in diesem Fall $H \subseteq \mathcal{Z}(G)$) nach Definition von \mathcal{Z}_H , \mathcal{D}_H und Satz 2.35:

$$\begin{aligned} \mathcal{Z}_H &= \underline{p}^l, \quad \mathcal{D}_H = \emptyset \quad \text{und} \quad \tilde{\mathcal{K}}_H = \underline{p}^l \setminus \{1\}, \text{ also} \\ \tilde{\mathcal{D}}_H &= \emptyset \quad \text{und} \quad \tilde{\mathcal{E}}_H = \emptyset. \end{aligned}$$

Außerdem gilt $\tilde{\mathcal{D}}_H = \emptyset$ für alle $H \in G/\gamma_2(G)$ mit $\mu(H) > 0$ nach 2.35 (xii). Wir erhalten damit für alle $m \in \mathbb{N}_{>1}$ aus Hauptsatz 2.37:

$$\begin{aligned} d_m &= \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) > 0, m \in \tilde{\mathcal{E}}_H \right\} \right| \\ &\stackrel{2.35(\text{xii})}{=} \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) > 0, m \leq p^l - p^{l-\mu(H)} + 1 \right\} \right| \end{aligned}$$

2. Sei $|\gamma_2(G)| = p$. Dann gilt $cl(G) = 2$, $l = 1$ und $k = 0$. Wie im ersten Beispiel gilt dann für alle $m \in \mathbb{N}_{>1}$:

$$\begin{aligned} d_m &= \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) > 0, m \leq p^l - p^{l-\mu(H)} + 1 \right\} \right| \\ &= \left| \left\{ H \mid H \in G/\gamma_2(G), \mu(H) = 1, m \leq p^l \right\} \right| \\ &= \left| \left\{ H \mid H \in \mathcal{K}(G), |H| \neq 1 \right\} \right| \end{aligned}$$

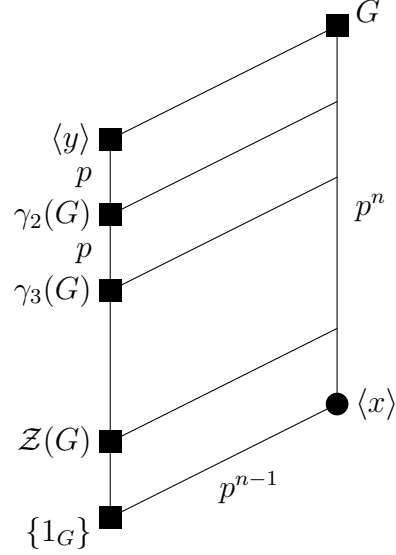
Dieser Spezialfall ist bereits aus der Diplomarbeit [23] bekannt und dort auf anderem Weg bewiesen worden.

3. Sei $p > 2$, $n \in \mathbb{N}_{>1}$, $N := C_{p^n}$. Dann gilt $\text{Aut}(N) \cong E(\mathbb{Z}/p^n\mathbb{Z}; \cdot)$ und $E(\mathbb{Z}/p^n\mathbb{Z}; \cdot)$ ist zyklisch mit $|E(\mathbb{Z}/p^n\mathbb{Z})| = (p-1)p^{n-1}$. (Satz von Gauß über die Existenz von Primitivwurzeln, siehe zum Beispiel [4, Kapitel 2, § 5.].) Sei P nun die (zyklische) p -Sylowgruppe von $\text{Aut}(N)$. Dann operiert P auf N vermöge $\beta : P \rightarrow \mathcal{S}_N, q \mapsto q$.

Sei $G := N \rtimes P$. Insbesondere gilt $|G| = p^{2n-1}$. Seien $x, y \in G$ mit $\langle y \rangle = N$, $\langle x \rangle = P$ und $y^x = y^{p+1}$. Es gilt $G = \langle x, y \rangle$ und

$$[\{y^{p^m}\}, G]_{\mathfrak{S}} \stackrel{2.2, 2.6}{=} \langle [y^{p^m}, x]_{\mathfrak{S}} \rangle = \langle y^{p^{m+1}} \rangle$$

für alle $m \in \mathbb{N}_0$. Insbesondere gilt $\gamma_2(G) \stackrel{2.6}{=} \langle [y, x]_{\mathfrak{S}} \rangle = \langle y^p \rangle$, $|\gamma_2(G)| = p^{n-1}$. Schärfer erhalten wir $\gamma_c(G) = \langle y^{p^{c-1}} \rangle$ für alle $c \in \mathbb{N}_{>1}$. Hieraus folgt $l = n-1$ und $k = n-2$. Insbesondere gilt $cl(G) = n$.



Es ist

$$\mathfrak{R} = \{y^{m_1}x^{m_2} \mid m_1 \in \underline{p-1}_0, m_2 \in \underline{p^{n-1}-1}_0\}$$

ein Repräsentantensystem von $G/\gamma_2(G)$. Die bisherigen Überlegungen zeigen, dass x und y die Bedingungen von erfüllen und \mathfrak{R} darüber hinaus ein solches wie im Beweis von Satz 2.36 konstruiertes Repräsentantensystem ist.

Nach Satz 2.21 sind insbesondere x und y extremale Elemente von G .

Sei $m_1 \in \underline{p-1}_0$ und $m_2 \in \underline{p^{n-1}-1}_0$. Es gilt

$$\begin{aligned} (*) \quad \langle [y^{m_1}x^{m_2}, x]_{\mathfrak{S}} \rangle &= \langle [y^{m_1}, x]_{\mathfrak{S}} \rangle \stackrel{2.2}{=} [\{y^{m_1}\}, G]_{\mathfrak{S}} \quad \text{und} \\ \langle [y^{m_1}x^{m_2}, y]_{\mathfrak{S}} \rangle &= \langle [x^{m_2}, y]_{\mathfrak{S}} \rangle \stackrel{2.2}{=} [\{x^{m_2}\}, G]_{\mathfrak{S}}. \end{aligned}$$

Es folgt

$$\begin{aligned} y^{m_1}x^{m_2} \text{ extremal} &\stackrel{(*), 2.9}{\iff} y^{m_1} \text{ extremal} \vee x^{m_2} \text{ extremal} \\ &\stackrel{2.10.1}{\iff} m_1 \neq 0 \vee p \nmid m_2 \end{aligned} \tag{2.22}$$

und damit

$$\begin{aligned}
 & |\{H \mid H \in G/\gamma_2(G), \mu(H) > k\}| \\
 & \stackrel{k=l-1}{=} |\{H \mid H \in G/\gamma_2(G), \mu(H) = l\}| \\
 & = |\{H \mid H \in \mathcal{K}(G), H \text{ extremal}\}| \\
 & \stackrel{(2.22)}{=} |\{(n_1, n_2) \mid n_1 \in \underline{p-1}_0, n_2 \in \underline{p^{n-1}-1}_0, n_1 \neq 0 \vee p \nmid n_2\}| \quad (2.23) \\
 & = (p-1)p^{n-1} + {}^3\varphi(p^{n-1}-1) \\
 & = (p-1)(p^{n-1} + p^{n-2}) \\
 & = p^n - p^{n-2}.
 \end{aligned}$$

Für alle $H \in G/\gamma_2(G)$ mit $\mu(H) \leq k$ gilt

$$\begin{aligned}
 \tilde{\mathcal{D}}_H & \stackrel{2.35(\text{viii}), (\text{iv})}{=} \{sp^{n-1-\mu(H)} + 1 \mid s \in \underline{p^{\mu(H)}-1}_1\}, \\
 \mathcal{Z}_H & \stackrel{\text{Def.}}{=} \{cp^j \mid j \in \underline{n-2-\mu(H)}_0, s \in \underline{p}\} \text{ und} \\
 \tilde{\mathcal{K}}_H & \stackrel{2.35(\text{vi})}{=} (-(\mathcal{Z}_H \setminus \{1\}) + p^l + 2) \cup \{sp^{n-\mu(H)-1} + 2 \mid s \in \underline{p^{\mu(H)}-2}_0\}.
 \end{aligned}$$

Sei $m \in \underline{p^{n-1}} \setminus \{1\}$. Es gilt $l - k = 1$. Dann folgt aus den Spezialisierungen von Hauptsatz 2.37:

(i) Ist $m \in \underline{p^{n-1}} \setminus \underline{p^{n-1}-p+1}_1$, so gilt

$$\begin{aligned}
 d_m & = |\{H \mid H \in G/\gamma_2(G), \mu(H) > k, m \leq p^l - p^{l-\mu(H)} + 1\}| \\
 & = |\{H \mid H \in G/\gamma_2(G), \mu(H) = l, m \leq p^{n-1}\}| \\
 & \stackrel{(2.23)}{=} p^n - p^{n-2}.
 \end{aligned}$$

(ii) Ist $m \in \underline{p^{n-1}-p+1}_1$ und $1 \not\equiv_p m \not\equiv_p 2$, so gilt

$$d_m = |G/\gamma_2(G)| = p^n.$$

(iii) Ist $m \in \underline{p^{n-1}-p+1}_1$ und $m \equiv_p 2$, so gilt

$$d_m \stackrel{(2.23)}{=} p^n - p^{n-2} + |\{H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \notin \tilde{\mathcal{K}}_H\}|.$$

(iv) Ist $m \in \underline{p^{n-1}-p+1}_1$ und $m \equiv_p 1$, so gilt

$$\begin{aligned}
 d_m & \stackrel{(2.23)}{=} p^n - p^{n-2} \\
 & + 2 \left| \{H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \in \tilde{\mathcal{D}}_H\} \right| \\
 & + \left| \{H \mid H \in G/\gamma_2(G), \mu(H) \leq k, m \notin \tilde{\mathcal{D}}_H\} \right|.
 \end{aligned}$$

³ φ sei hier die Eulersche φ -Funktion

Zum Schluss dieses Kapitels geben wir noch ein konkretes Zahlenbeispiel für das dritte Beispiel an: Sei $p = 5$, $n := 4$, $N = C_{625}$, P die 5-Sylowgruppe von $\text{Aut}(N) \cong C_{500}$ und $G := N \rtimes P$. Seien $x, y \in G$ mit $\langle y \rangle = N$ und $\langle x \rangle = P$. Es gilt $\langle y^5 \rangle = \gamma_2(G)$, $|\gamma_2(G)| = 125$ und

$$\mathfrak{R} := \{y^{m_1}x^{m_2} \mid m_1 \in \underline{4}_0, m_2 \in \underline{124}_0\}$$

ist ein Repräsentantensystem von $G/\gamma_2(G)$.

Nach Gleichung (2.23) gilt

$$|\{H \mid H \in G/\gamma_2(G), \mu(H) = 3\}| = |\{H \mid H \in \mathcal{K}(G), H \text{ extremal}\}| = 600.$$

Sei $m_1 \in \underline{4}_0$ und $m_2 \in \underline{124}_0$. Nach Gleichung (2.22) gilt

$$y^{m_1}x^{m_2} \text{ nicht extremal} \iff m_1 = 0 \wedge p \mid m_2.$$

Außerdem gilt

$$[\{x^u\}, G]_{\mathfrak{G}} \subseteq [\{x^u y^v\}, G]_{\mathfrak{G}}$$

für alle $u, v \in \mathbb{N}_0$.

Zusammen mit Satz 2.9 folgt $\kappa(g) = \mu(H)$ für alle $H \in G/\gamma_2(G)$ und $g \in \mathfrak{R} \cap H$. Wir erhalten für alle $s \in \{0, 1, 2\}$

$$\begin{aligned} |\{H \mid H \in G/\gamma_2(G), \mu(H) = s\}| &= \left| \left\{ (x^{\tilde{m}_2})^G \mid \tilde{m}_2 \in \underline{124}_0, |(x^{\tilde{m}_2})^G| = p^s \right\} \right| \\ &\stackrel{2.10.1}{=} |\{\tilde{m}_2 \mid \tilde{m}_2 \in \underline{125}, s = 3 - \nu(\tilde{m}_2)\}| \\ &= |\{\tilde{m}_2 \mid \tilde{m}_2 \in \underline{5}^3, \nu(\tilde{m}_2) = 3 - s\}| \\ &= \varphi(5^{3-(3-s)}) \\ &= \varphi(5^s). \end{aligned}$$

Es folgt

$$\begin{aligned} |\{H \mid H \in G/\gamma_2(G), \mu(H) = 2\}| &= 20, \\ |\{H \mid H \in G/\gamma_2(G), \mu(H) = 1\}| &= 4, \\ |\{H \mid H \in G/\gamma_2(G), \mu(H) = 0\}| &= 1. \end{aligned}$$

Mit Hilfe von Satz 2.12 und Satz 1.20 (iii) können wir $\dim \mathcal{Z}(\mathcal{J}(KG))$ ermitteln: Nach Satz 2.12 gilt

$$|\mathcal{K}_H(G)| = \begin{cases} 5 & \text{falls } \mu(H) = 2, \\ 9 & \text{falls } \mu(H) = 1, \\ 13 & \text{falls } \mu(H) = 0. \end{cases} \quad (2.24)$$

Aus Satz 1.20 (iii) folgt

$$\dim \mathcal{Z}(\mathcal{J}(KG)) = -1 + 600 + 5 \cdot 20 + 9 \cdot 4 + 13 \cdot 1 = 748.$$

2 p -Gruppen mit zyklischer Kommutatoruntergruppe

Es ergeben sich aus Beispiel 3 damit die in folgender Tabelle aufgelisteten K -Dimensionen für die Faktorräume der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$. In jeder „ungeraden“ Spalte repräsentiere die Ziffer i den Faktorraum $\mathcal{Z}_i(\mathcal{J}(KG))/\mathcal{Z}_{i-1}(\mathcal{J}(KG))$. Die Spalte rechts daneben gebe dann jeweils die K -Dimension dieses Raums an.

Dimensionen der Faktorräume in der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$:

1	748	26	649	51	649	76	649	101	649
2	600	27	600	52	600	77	600	102	600
3	625	28	625	53	625	78	625	103	625
4	625	29	625	54	625	79	625	104	625
5	625	30	625	55	625	80	625	105	625
6	645	31	645	56	645	81	645	106	645
7	605	32	605	57	605	82	605	107	600
8	625	33	625	58	625	83	625	108	625
9	625	34	625	59	625	84	625	109	625
10	625	35	625	60	625	85	625	110	625
11	645	36	645	61	645	86	645	111	645
12	605	37	605	62	605	87	605	112	600
13	625	38	625	63	625	88	625	113	625
14	625	39	625	64	625	89	625	114	625
15	625	40	625	65	625	90	625	115	625
16	645	41	645	66	645	91	645	116	645
17	605	42	605	67	605	92	605	117	600
18	625	43	625	68	625	93	625	118	625
19	625	44	625	69	625	94	625	119	625
20	625	45	625	70	625	95	625	120	625
21	645	46	645	71	645	96	645	121	645
22	605	47	605	72	605	97	605	122	600
23	625	48	625	73	625	98	625	123	600
24	625	49	625	74	625	99	625	124	600
25	625	50	625	75	625	100	625	125	600

3 p-Gruppen mit p-elementar-abelscher Kommutatoruntergruppe

In diesem Kapitel sei K stets ein Körper mit $\text{char } K = p$.

Wir untersuchen im Hinblick auf die aufsteigende Zentralreihe von $\mathcal{J}(KG)$ die Klasse von p -Gruppen G mit $\gamma_2(G) \cong C_p \times C_p$. Dabei können die Nilpotenzklassen 2 und 3 der Gruppe G auftreten. Gemäß dieser Unterscheidung ist dieses Kapitel in zwei Abschnitte unterteilt.

3.1 Nilpotenzklasse 2

Nach einer kurzen Einführung über p -Gruppen G mit Nilpotenzklasse 2 und p -elementar-abelscher Kommutatoruntergruppe beliebiger Mächtigkeit legen wir unser Hauptaugenmerk auf den Fall $\gamma_2(G) \cong C_p \times C_p$. Mit in Kapitel 2 bewährten Methoden werden wir die aufsteigende Zentralreihe von $\mathcal{J}(KG)$ in 3.11 bestimmen.

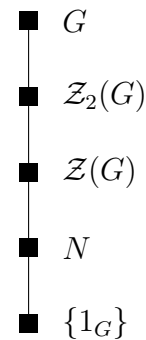
3.1 Lemma.

Sei G eine Gruppe. Für alle $h \in \mathcal{Z}_2(G)$ gilt

$$[\{h\}, G]_{\mathfrak{G}} = \{[h, g]_{\mathfrak{G}} \mid g \in G\} \trianglelefteq G.$$

Sei $N \leq \mathcal{Z}(G)$. Für alle $H \in \mathcal{Z}_2(G)/N$ und $h \in H$ gilt dann

$$[H, G]_{\mathfrak{G}} = \{[h, g]_{\mathfrak{G}} \mid g \in G\} \trianglelefteq G.$$



Insbesondere folgt: Ist $H \in \mathcal{Z}_2(G)/N$, so gilt $h^G = h[H, G]_{\mathfrak{G}}$ für alle $h \in H$.

Ist G endlich, so gilt $|\tilde{h}^G| = |h^G|$ für alle $H \in \mathcal{Z}_2(G)/N$ und $h, \tilde{h} \in H$.

Beweis. Sei $h \in \mathcal{Z}_2(G)$. Für alle $g_1, g_2 \in G$ gilt $[h, g_1]_{\mathfrak{G}}, [h, g_2]_{\mathfrak{G}} \in \mathcal{Z}(G)$ und damit

$$[h, g_1]_{\mathfrak{G}}[h, g_2]_{\mathfrak{G}} \stackrel{2.2}{=} [h, g_1 g_2]_{\mathfrak{G}}.$$

Also ist $[h, \cdot]_{\mathfrak{G}} : G \rightarrow \gamma_2(G)$ ein Homomorphismus mit $\text{Bild}[h, \cdot]_{\mathfrak{G}} = \{[h, g]_{\mathfrak{G}} \mid g \in G\}$. Aus $[\{h\}, G]_{\mathfrak{G}} \subseteq \mathcal{Z}(G)$ folgt die Normalteilereigenschaft.

3 p -Gruppen mit p -elementar-abelscher Kommutatoruntergruppe

Sei $N \leq \mathcal{Z}(G)$, $H \in \mathcal{Z}_2(G)/N$ und $h \in H$. Wegen $N \leq \text{Kern}[h, \cdot]_{\mathfrak{G}}$ induziert $[h, \cdot]_{\mathfrak{G}}$ einen Homomorphismus $[H, \cdot]_{\mathfrak{G}} : G \rightarrow \gamma_2(G)$ mit $\{[h, g]_{\mathfrak{G}} \mid g \in G\} = \text{Bild}[H, \cdot]_{\mathfrak{G}} \subseteq \mathcal{Z}(G)$.

Die zusätzlichen Aussagen folgen nun aus $h^G = h \{[h, g]_{\mathfrak{G}} \mid g \in G\}$. \square

Das folgende Lemma stammt aus [15, Kapitel 2, Satz 2].

3.2 Lemma.

Sei G eine nicht-abelsche p -Gruppe. Dann sind folgende Aussagen äquivalent:

- (i) Es gilt $|\gamma_2(G)| = p$.
- (ii) Jede nichtzentrale Konjugiertenklasse hat die Länge p .

\square

Die folgende Bemerkung ist eine unmittelbare Konsequenz.

3.2.1 Bemerkung. Ist G eine p -Gruppe mit $|\gamma_2(G)| = p^2$, so enthält G extremale Elemente. \square

3.3 Lemma. Sei G eine p -elementar-abelsche Gruppe, $G \neq \{1_G\}$, $l \in \mathbb{N}$ mit $|G| = p^l$ und $\{a_0, \dots, a_{l-1}\}$ eine $\mathbb{Z}/p\mathbb{Z}$ -Basis von G . Seien $m_0, \dots, m_{l-1}, c_0, \dots, c_{l-1} \in \underline{p-1}_0$. Für alle $k_0, \dots, k_{l-1} \in \mathbb{Z}$ setzen wir

$$w_{(k_0, \dots, k_{l-1})} := \sum_{0 \leq j_0, \dots, j_{l-1} < p} \left(\prod_{i=0}^{l-1} \binom{j_i}{k_i} a_i^{j_i} \right).$$

Dann existiert

$$x \in R := \left\langle w_{(k_0, \dots, k_{l-1})} \mid \forall i \in \underline{l-1}_0 : k_i \in \underline{m_i}_0, \sum_{i=0}^{l-1} k_i \leq -2 + \sum_{i=0}^{l-1} m_i \right\rangle_K$$

mit

$$\sum_{0 \leq j_0, \dots, j_{l-1} < p} \left(\prod_{i=0}^{l-1} \binom{j_i}{m_i} a_i^{j_i - c_i} \right) = w_{(m_0, \dots, m_{l-1})} + \sum_{i=0}^{l-1} c_i w_{(m_0, \dots, m_{i-1}, \dots, m_{l-1})} + x.$$

Beweis. Es gilt unter Ausnutzung der Distributivgesetze in KG

$$\sum_{0 \leq j_0, \dots, j_{l-1} < p} \left(\prod_{i=0}^{l-1} \binom{j_i}{m_i} a_i^{j_i - c_i} \right) = \prod_{i=0}^{l-1} \left(\sum_{j_i=0}^{p-1} \binom{j_i}{m_i} a_i^{j_i - c_i} \right) \stackrel{1.25}{=} \prod_{i=0}^{l-1} \left(\sum_{j_i=0}^{p-1} \binom{j_i + c_i}{m_i} a_i^{j_i} \right).$$

Für alle $i \in \underline{l-1}_0$ und $j_i \in \underline{p-1}_0$ gilt

$$\binom{j_i + c_i}{m_i} \stackrel{1.21}{=} \sum_{k_i=0}^{m_i} \binom{c_i}{k_i} \binom{j_i}{m_i - k_i} = \binom{j_i}{m_i} + c_i \binom{j_i}{m_i - 1} + \sum_{k_i=2}^{m_i} \binom{c_i}{k_i} \binom{j_i}{m_i - k_i}.$$

Es folgt

$$\begin{aligned} & \prod_{i=0}^{l-1} \left(\sum_{j_i=0}^{p-1} \binom{j_i + c_i}{m_i} a_i^{j_i} \right) \\ &= \prod_{i=0}^{l-1} \left(\sum_{j_i=0}^{p-1} \binom{j_i}{m_i} a_i^{j_i} + c_i \sum_{j_i=0}^{p-1} \binom{j_i}{m_i - 1} a_i^{j_i} + \sum_{k_i=2}^{m_i} \left(\binom{c_i}{k_i} \sum_{j_i=0}^{p-1} \binom{j_i}{m_i - k_i} a_i^{j_i} \right) \right). \end{aligned}$$

Durch Ausmultiplizieren erhalten wir nun: Es existiert $x \in R$ mit

$$\begin{aligned} & \prod_{i=0}^{l-1} \left(\sum_{j_i=0}^{p-1} \binom{j_i + c_i}{m_i} a_i^{j_i} \right) \\ &= \sum_{0 \leq j_0, \dots, j_{l-1} < p} \left(\prod_{i=0}^{l-1} \binom{j_i}{m_i} a_i^{j_i} \right) + \sum_{i=0}^{l-1} c_i \sum_{0 \leq j_0, \dots, j_{l-1} < p} \left(\binom{j_i}{m_i - 1} a_i^{j_i} \prod_{\substack{d \in \underline{l-1}_0, \\ i \neq d}} \binom{j_d}{m_d} a_d^{j_d} \right) + x \\ &= w_{(m_0, \dots, m_{l-1})} + \sum_{i=0}^{l-1} c_i w_{(m_0, \dots, m_{i-1}, \dots, m_{l-1})} + x. \end{aligned}$$

□

3.3.1 Bemerkung.

(i) Ist $\sum_{i=0}^{l-1} m_i \leq l(p-1) - 1$, so gilt $w_{(m_0, \dots, m_{l-1})} \in \mathcal{J}(KG)$.

(ii) Es gilt $w_{(p-1, \dots, p-1)} = \prod_{i=0}^{l-1} a_i^{p-1}$.

Beweis. (i) Sei $(j_0, \dots, j_{l-1})_p := \sum_{i=0}^{l-1} j_i p^i$ für alle $j_0, \dots, j_{l-1} \in \underline{p-1}_0$. Dann gilt

$$w_{(m_0, \dots, m_{l-1})} \stackrel{1.22}{=} \sum_{0 \leq j_0, \dots, j_{l-1} < p} \left(\binom{(j_0, \dots, j_{l-1})_p}{(m_0, \dots, m_{l-1})_p} \prod_{i=0}^{l-1} a_i^{j_i} \right) \stackrel{1.22.5}{\in} \mathcal{J}(KG).$$

(ii) folgt unmittelbar aus der Definition von $w_{(p-1, \dots, p-1)}$.

□

In [22, S.140] weist Shalev nach, dass $cl(\mathcal{J}(KG); *) = l(p-1) + 1$ im Fall $p \geq 5$ für eine p -Gruppe G mit $cl(G) = 2$ und elementar-abelscher Kommutatoruntergruppe der Ordnung p^l gilt. Der folgende Satz legt somit an dieser Stelle eine Vermutung nahe, wie man Basen für die einzelnen Glieder der aufsteigenden Zentralreihe finden kann.

3.4 Satz. Sei G eine p -Gruppe, $cl(G) = 2$ und es gelte $\gamma_2(G) \cong C_p^l$ für ein geeignetes $l \in \mathbb{N}$. Sei weiter $\{a_0, \dots, a_{l-1}\}$ eine $\mathbb{Z}/p\mathbb{Z}$ -Basis von $\gamma_2(G)$ und

$$w_{(k_0, \dots, k_{l-1})} := \sum_{0 \leq j_0, \dots, j_{l-1} < p} \left(\prod_{i=0}^{l-1} \binom{j_i}{k_i} a_i^{j_i} \right)$$

für alle $k_0, \dots, k_{l-1} \in \mathbb{Z}$. Seien $m_0, \dots, m_{l-1} \in \underline{p-1}_0$. Ist $\sum_{i=0}^{l-1} m_i \leq l(p-1) - 1$, so gilt

$$KGw_{(m_0, \dots, m_{l-1})} \subseteq \mathcal{Z}_{\left(\sum_{i=0}^{l-1} m_i\right)+1}(\mathcal{J}(KG)).$$

Außerdem gilt

$$\mathcal{J}(KG) = \mathcal{Z}_{l(p-1)+1}(\mathcal{J}(KG)).$$

Beweis. Für den ersten Teil des Satzes reicht es $gw_{(m_0, \dots, m_{l-1})} \in \mathcal{Z}_{\left(\sum_{i=0}^{l-1} m_i\right)+1}(\mathcal{J}(KG))$ für alle $g \in G$ zu zeigen.

Wir zeigen die Behauptung durch Induktion nach $\sum_{i=0}^{l-1} m_i$. Ist $\sum_{i=0}^{l-1} m_i = 0$, also $m_i = 0$ für alle $i \in \underline{l-1}_0$, so gilt nach 1.5 für alle $g \in G$

$$gw_{(0, \dots, 0)} = g \sum_{0 \leq j_0, \dots, j_{l-1} < p} \prod_{i=0}^{l-1} a_i^{j_i} = g \sum \gamma_2(G) \in \mathcal{Z}(\mathcal{J}(KG)).$$

Seien nun $\sum_{i=0}^{l-1} m_i > 0$ und $g, h \in G$. Induktiv dürfen wir

$$hgw_{(k_0, \dots, k_{l-1})} \in \mathcal{Z}_{\left(\sum_{i=0}^{l-1} k_i\right)+1}(\mathcal{J}(KG)) \subseteq \mathcal{Z}_{\left(\sum_{i=0}^{l-1} m_i\right)}(\mathcal{J}(KG))$$

für alle $k_i \in \underline{p-1}_0$, $i \in \underline{l-1}_0$, mit $\sum_{i=0}^{l-1} k_i < \sum_{i=0}^{l-1} m_i$ annehmen.

Es existieren $c_0, \dots, c_{l-1} \in \underline{p-1}_0$ mit $[g, h]_{\mathfrak{S}} = \prod_{i=0}^{l-1} a_i^{-c_i}$. Wir erhalten

$$\begin{aligned} hg[g, h]_{\mathfrak{S}} w_{(m_0, \dots, m_{l-1})}^h &\stackrel{cl(G)=2}{=} hg[g, h]_{\mathfrak{S}} w_{(m_0, \dots, m_{l-1})} \\ &= hg \sum_{0 \leq j_0, \dots, j_{l-1} < p} \left(\prod_{i=0}^{l-1} \binom{j_i}{m_i} a_i^{j_i - c_i} \right) \\ &\stackrel{3.3, \text{ Ind. vor. }}{=} \mathcal{Z}_{\left(\sum_{i=0}^{l-1} m_i\right)}(\mathcal{J}(KG)) hg w_{(m_0, \dots, m_{l-1})}. \end{aligned}$$

Ist nun $\sum_{i=0}^{l-1} m_i \leq l(p-1) - 1$, so folgt $gw_{(m_0, \dots, m_{l-1})} \in \mathcal{J}(KG)$ nach Bemerkung 3.3.1. Nach dem im Eingangskapitel erläuterten Grundprinzip folgt hieraus der erste Teil der Behauptung.

Ist $\sum_{i=0}^{l-1} m_i = l(p-1)$, das heißt $m_0 = \dots = m_{l-1} = p-1$, so gilt $w_{(p-1, \dots, p-1)} = \prod_{i=0}^{l-1} a_i^{p-1}$, also $w_{(p-1, \dots, p-1)} \notin \mathcal{J}(KG)$. Dann gilt aber $gw_{(p-1, \dots, p-1)} - 1_G \in \mathcal{Z}_{l(p-1)+1}(\mathcal{J}(KG))$ nach Abschnitt 1.3. Also enthält $\mathcal{Z}_{l(p-1)+1}(\mathcal{J}(KG))$ eine K -Basis von $\mathcal{J}(KG)$. Satz 1.8 liefert nun die Behauptung. \square

3.4.1 Bemerkung. Für alle $g \in G$, $a \in \gamma_2(G)$ gilt

$$ga w_{(m_0, \dots, m_{l-1})} \equiv_{\mathcal{Z}_{\left(\sum_{i=0}^{l-1} m_i\right)}(\mathcal{J}(KG))} gw_{(m_0, \dots, m_{l-1})}.$$

Beweis. Es existieren $c_0, \dots, c_{l-1} \in \underline{p-1}_0$ mit $a = \prod_{i=0}^{l-1} a_i^{-c_i}$. Aus Satz 3.4 und Lemma 3.3 folgt die Behauptung. \square

3.5 Lemma. Sei G eine p -Gruppe, $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 2$ und es existiere $g \in G$ mit $|g^G| = p$.

(i) Für alle $h \in G$, h extremal, mit $C_G(h) \setminus C_G(g) \neq \emptyset$ ist hg extremal.

Insbesondere gilt:

(ii) Ist $h \in G \setminus C_G(g)$, so gilt: h extremal $\iff hg$ extremal.

(iii) Ist $\tilde{g} \in G \setminus C_G(g)$ mit $|\tilde{g}^G| = p$, $h \in C_G(g)$ mit h extremal, so ist $h\tilde{g}$ extremal.

(iv) $G \setminus C_G(g)$ enthält ein extremes Element.

Beweis. (i) Sei $h \in G$, h extremal, mit $C_G(h) \setminus C_G(g) \neq \emptyset$, $x \in C_G(h) \setminus C_G(g)$. Nach Lemma 3.1 gilt $g^G = g[\{g\}, G]_{\mathfrak{S}}$ und folglich

$$\langle [hg, x]_{\mathfrak{S}} \rangle \stackrel{2.2}{=} \langle [g, x]_{\mathfrak{S}} \rangle \stackrel{|g^G|=p}{=} [\{g\}, G]_{\mathfrak{S}} \neq \{1_G\}.$$

Sei $a := [g, x]_{\mathfrak{S}}$. Da h extremal ist, existiert daher $y \in G$ mit

$$b := [hg, y]_{\mathfrak{S}} \stackrel{2.2}{=} [h, y]_{\mathfrak{S}} [g, y]_{\mathfrak{S}} \in \gamma_2(G) \setminus \langle a \rangle.$$

Folglich gilt $\langle a, b \rangle = \gamma_2(G)$. Aus Lemma 3.1 folgt $(hg)^G = hg\gamma_2(G)$, also die Extremalität von hg .

(ii) Sei $h \in G \setminus C_G(g)$. Dann gilt $h \in C_G(h) \setminus C_G(g)$ und aus (i) folgt die Implikation „ \Rightarrow “. Außerdem gilt $|(g^{-1})^G| = p$ und $hg \in C_G(hg) \setminus C_G(g^{-1})$. Durch erneutes Anwenden von (i) folgt hieraus die andere Implikation.

(iii) Es sei $\tilde{g} \in G \setminus C_G(g)$ mit $|\tilde{g}^G| = p$ und $h \in C_G(g)$ mit h extremal. Dann gilt $g \in C_G(h) \setminus C_G(\tilde{g})$, also $C_G(h) \setminus C_G(\tilde{g}) \neq \emptyset$. Die Behauptung folgt aus (i) mit \tilde{g} statt g .

(iv) Nach Bemerkung 3.2.1 existiert $h \in G$, h extremal. Ist $h \notin C_G(g)$, so ist nichts zu zeigen. Andernfalls gilt $h \in C_G(g)$. Sei $\tilde{g} \notin C_G(g)$. Ist \tilde{g} extremal, so ist nichts weiter zu beweisen. Im anderen Fall gilt $|\tilde{g}^G| = p$. Dann gilt $h\tilde{g} \notin C_G(g)$ und nach (iii) ist $h\tilde{g}$ extremal. \square

3.6 Lemma. *Sei G eine p -Gruppe, $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 2$ und $g \in G$ extremal. Dann existiert für alle $a \in \gamma_2(G)$ ein $h \in G$ mit hg extremal und $[g, h]_{\mathfrak{S}} = a$.*

Beweis. Sei $a \in \gamma_2(G)$. Ist $a = 1_G$, so wählen wir $h := 1_G$. Wir nehmen daher nun $a \neq 1_G$ an. Da g extremal ist, existiert $\tilde{h} \in G$ mit $[g, \tilde{h}]_{\mathfrak{S}} = a$. Da $g \notin C_G(\tilde{h}g)$, gilt folglich $|(\tilde{h}g)^G| \geq p$. Ist $\tilde{h}g$ extremal, so wählen wir $h := \tilde{h}$. Andernfalls gilt $|(\tilde{h}g)^G| = p$ und es gilt $g \in G \setminus C_G(\tilde{h}g)$. Nach (i) in Lemma 3.5 ist dann $g\tilde{h}g$ extremal, also auch $(g\tilde{h}g)^g = \tilde{h}g^2$. Setzen wir in diesem Fall daher $h := \tilde{h}g$, folgt hieraus die Behauptung. \square

3.7 Lemma. *Sei G eine p -Gruppe, $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 2$ und es existiere $g \in G$ mit $|g^G| = p$. Sei $b \in [\{g\}, G]_{\mathfrak{S}} \setminus \{1_G\}$ und $a \in \gamma_2(G) \setminus \langle b \rangle$. Dann ist*

$$\mathfrak{B} := \left\{ g \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{k} a^i b^j \mid k \in \underline{p-1}_0 \right\}$$

eine K -Basis von $\mathcal{Z}(\mathcal{J}(KG)) \cap \langle g\gamma_2(G) \rangle_K$.

Beweis. Es gilt $\gamma_2(G) = \langle a \rangle \langle b \rangle$ und nach Lemma 3.1 gilt $g^G = g \langle b \rangle$. Wegen

$$g \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{k} a^i b^j \stackrel{1.22}{=} g \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i+jp}{k} a^i b^j$$

für alle $k \in \underline{p-1}_0$ ist \mathfrak{B} nach 1.23.2 K -linear unabhängig. Außerdem erhalten wir aus Lemma 3.1: $(ga^i)^G = ga^i \langle b \rangle$ für alle $i \in \underline{p-1}_0$. Ist nun $k \in \underline{p-1}_0$, so folgt

$$g \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{k} a^i b^j = \sum_{i=0}^{p-1} \underbrace{g \left(\binom{i}{k} a^i \sum_{j=0}^{p-1} b^j \right)}_{\in \mathcal{Z}(\mathcal{J}(KG)) \cap \langle g\gamma_2(G) \rangle_K \text{ nach 1.5}} \in \mathcal{Z}(\mathcal{J}(KG)) \cap \langle g\gamma_2(G) \rangle_K.$$

Wegen $|\mathfrak{B}| = p = \frac{|\gamma_2(G)|}{|g^G|} \stackrel{3.1}{=} |\mathcal{K}_{g\gamma_2(G)}(G)| \stackrel{1.20(ii)}{=} \dim \mathcal{Z}(\mathcal{J}(KG)) \cap \langle g\gamma_2(G) \rangle_K$ folgt die Behauptung aus der K -linearen Unabhängigkeit von \mathfrak{B} . \square

3.8 Definition. Für alle $m \in \underline{2p-2}_0$ sei

$$\Sigma(m) := \{(r, s) \mid r, s \in \underline{p-1}_0, m = r + s\}.$$

Lemma 3.7 zeigt bereits, dass die im Satz 3.9 in (ii) auftretende Bedingung für die dortige Aussage notwendig ist. Tatsächlich ist sie aber auch hinreichend und ein Bestandteil des für den Hauptsatz dieses Abschnitts wichtigen Satzes:

3.9 Satz. Sei G eine p -Gruppe, $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 2$ und $g \in G \setminus \mathcal{Z}(G)$. Sei $b \in [\{g\}, G]_{\mathfrak{G}} \setminus \{1_G\}$ und $a \in \gamma_2(G) \setminus \langle b \rangle$. Für alle $r, s \in \mathbb{Z}$ setzen wir

$$w_{(r,s)} := \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} a^i b^j.$$

Sei $m \in \underline{2p-3}_0$. Dann gilt:

(i) Ist g extremal, so ist

$$\left\{ gw_{(r,s)} \mid (r, s) \in \Sigma(m) \right\}$$

modulo $\mathcal{Z}_m(\mathcal{J}(KG))$ K -linear unabhängig.

(ii) Ist $|g^G| = p$, so ist

$$\left\{ gw_{(r,s)} \mid (r, s) \in \Sigma(m), s \neq 0 \right\}$$

modulo $\mathcal{Z}_m(\mathcal{J}(KG))$ K -linear unabhängig.

(iii) Es gilt $g - 1_G \notin \mathcal{Z}_{2p-2}(\mathcal{J}(KG))$.

Beweis. Es gilt $\gamma_2(G) = \langle a \rangle \langle b \rangle$. Ist $m = 0$, so gilt $\Sigma(m) = \{(0, 0)\}$ und die Aussage (i) folgt in diesem Fall aus

$$g \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{0} \binom{j}{0} a^i b^j = g \sum \gamma_2(G) \stackrel{1.5}{\in} \mathcal{Z}(\mathcal{J}(KG)) \setminus \{0_{KG}\}. \quad (3.1)$$

Sei zunächst $0 < m < p$. Für alle $k \in \underline{m}_0$ sei $\lambda_k \in K$ und es gelte

$$\sum_{k=0}^m \lambda_k gw_{(k, m-k)} \in \mathcal{Z}_m(\mathcal{J}(KG)). \quad (3.2)$$

Um zu beweisen, dass

$$\{gw_{(k, m-k)} \mid k \in \underline{m}_0\} \text{ modulo } \mathcal{Z}_m(\mathcal{J}(KG))$$

K -linear unabhängig ist, ist also $\lambda_k = 0_K$ für alle $k \in \underline{m}_0$ zu zeigen.

3 p -Gruppen mit p -elementar-abelscher Kommutatoruntergruppe

Für alle $h \in G$ seien $h_0, h_1 \in \underline{p-1}_0$ mit $[g, h]_{\mathfrak{S}} = a^{-h_0} b^{-h_1}$. Dann gilt für alle $h \in G$:

$$\begin{aligned}
& hg[g, h]_{\mathfrak{S}} \sum_{k=0}^m \lambda_k w_{(k, m-k)}^h \stackrel{cl(G)=2}{=} hga^{-h_0} b^{-h_1} \sum_{k=0}^m \lambda_k w_{(k, m-k)} \\
& \stackrel{3.3, 3.4}{\equiv} \sum_{\mathcal{Z}_{m-1}(\mathcal{J}(KG))} hg \sum_{k=0}^m \lambda_k w_{(k, m-k)} + hg \sum_{k=0}^m \lambda_k h_0 w_{(k-1, m-k)} + hg \sum_{k=0}^m \lambda_k h_1 w_{(k, m-k-1)} \\
& = hg \sum_{k=0}^m \lambda_k w_{(k, m-k)} + hg \sum_{k=0}^{m-1} \lambda_{k+1} h_0 w_{(k, m-k-1)} + hg \sum_{k=0}^{m-1} \lambda_k h_1 w_{(k, m-k-1)} \\
& = hg \sum_{k=0}^m \lambda_k w_{(k, m-k)} + hg \sum_{k=0}^{m-1} (\lambda_{k+1} h_0 + \lambda_k h_1) w_{(k, m-k-1)}.
\end{aligned}$$

Aus obiger Annahme (3.2) und dem Grundprinzip erhalten wir

$$\sum_{k=0}^{m-1} (\lambda_{k+1} h_0 + \lambda_k h_1) hgw_{(k, m-k-1)} \in \mathcal{Z}_{m-1}(\mathcal{J}(KG)). \quad (3.3)$$

Sei nun $p \leq m \leq 2p-3$. Dann gilt $r \neq 0 \neq s$ für alle $(r, s) \in \Sigma(m)$. Sei dann $\lambda_k \in K$ für alle $k \in \{m-p+1, \dots, p-1\}$, $\lambda_p := 0$, $\lambda_{m-p} := 0$ und es gelte

$$\sum_{k=m-(p-1)}^{p-1} \lambda_k gw_{(k, m-k)} \in \mathcal{Z}_{m-1}(\mathcal{J}(KG)).$$

In diesem Fall erhalten wir analog zur obigen Rechnung

$$\sum_{k=m-p}^{p-1} (\lambda_{k+1} h_0 + \lambda_k h_1) hgw_{(k, m-k-1)} \in \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \quad (3.4)$$

für alle $h \in G$.

(i): Sei g extremal. Wir zeigen die Behauptung durch einen Induktionsbeweis nach m . Der Induktionsanfang $m=0$ folgt dabei aus Gleichung (3.1).

Sei nun $0 < m < p$.

Induktiv dürfen wir für alle $h \in G$ mit hg extremal annehmen:

$$\left\{ hgw_{(r,s)} \mid (r, s) \in \Sigma(m-1) \right\} \text{ ist modulo } \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \text{ } K\text{-linear unabhängig.}$$

Aus Gleichung (3.3) folgt dann $\lambda_{k+1} h_0 + \lambda_k h_1 = 0_K$ für alle $k \in \underline{m-1}_0$.

Nach Lemma 3.6 existieren $h, \tilde{h} \in G$, hg und $\tilde{h}g$ extremal, mit $(h_0, h_1) = (1, 0)$ und $(\tilde{h}_0, \tilde{h}_1) = (0, 1)$. Aus der Extremalität von hg folgt

$$\lambda_{k+1} = 0_K \text{ für alle } k \in \underline{m-1}_0,$$

also $\lambda_k = 0$ für alle $k \in \underline{m}$.

Aus der Extremalität von $\tilde{h}g$ folgt

$$\lambda_k = 0_K \text{ für alle } k \in \underline{m-1}_0,$$

also insgesamt $\lambda_k = 0_K$ für alle $k \in \underline{m}_0$.

Den Fall $p \leq m \leq 2p-3$ kann man auf ähnliche Weise mit Hilfe der Gleichung (3.4) verifizieren: Aus der Extremalität von hg können wir induktiv hier bereits auf

$$\lambda_{k+1} = 0_K \text{ für alle } k \in \{m-p, \dots, p-1\}$$

schließen, das heißt auf $\lambda_k = 0_K$ für alle $k \in \{m-(p-1), \dots, p\}$.

(ii): Sei $|g^G| = p$.

Nach 3.5 (iv) existiert $h \in G \setminus C_G(g)$ mit h extremal. Nach 3.5 (ii) ist dann auch hg extremal. Nach Lemma 3.1 gilt $|\{g\}, G]_{\mathfrak{G}}| = p$, also $\langle b \rangle = [\{g\}, G]_{\mathfrak{G}}$, insbesondere also $h_0 = 0$ und $h_1 \neq 0$.

Ist $0 < m < p$, so folgt aus Gleichung (3.3) und der bereits bewiesenen ersten Aussage nun $\lambda_k = 0_K$ für alle $k \in \underline{m-1}_0$. Man beachte, dass wir nicht auf $\lambda_m = 0_K$ schließen können.

Ist $p \leq m \leq 2p-3$, so folgt aus Gleichung (3.4) und Aussage (i) $\lambda_k = 0_K$ für alle $k \in \{m-(p-1), \dots, p-1\}$.

(iii) Es gilt $w_{(p-1,p-1)} = a^{p-1}b^{p-1}$. Wie in (i) und (ii) existiert nach 3.6 beziehungsweise 3.5 (iv) und (ii) $h \in G$ mit $h_0 = 0$, $h_1 \neq 0$ und hg extremal. Es folgt

$$\begin{aligned} hg[g, h]_{\mathfrak{G}} w_{(p-1,p-1)}^h &\stackrel{cl(G)=2}{=} hgb^{-h_1} w_{(p-1,p-1)} \\ &\stackrel{3.3, 3.4}{\equiv}_{\mathcal{Z}_{2p-3}(\mathcal{J}(KG))} hgw_{(p-1,p-1)} + hgh_1 w_{(p-1,p-2)} \\ &\stackrel{(i)}{\neq}_{\mathcal{Z}_{2p-3}(\mathcal{J}(KG))} hgw_{(p-1,p-1)} \end{aligned}$$

und damit nach dem Grundprinzip

$$g - 1_G \stackrel{3.4.1}{\equiv}_{\mathcal{Z}_{2p-2}(\mathcal{J}(KG))} (gw_{(p-1,p-1)} - 1_G) \notin \mathcal{Z}_{2p-2}(\mathcal{J}(KG)).$$

□

Als Korollar erhalten wir aus Satz 3.9 (iii) und Satz 3.4 ein Resultat aus [21]:

3.10 Korollar. *Sei G eine p -Gruppe, $\gamma_2(G) \cong C_p \times C_p$ und $cl(G) = 2$. Dann gilt*

$$cl(\mathcal{J}(KG); *) = 2p - 1.$$

□

3.11 Hauptsatz. Sei G eine p -Gruppe, $cl(G) = 2$, $\gamma_2(G) \cong C_p \times C_p$, $m \in \underline{2p-1} \setminus \{1\}$, d die Anzahl der Konjugiertenklassen der Länge p und

$$d_m := \dim(\mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG))).$$

Dann gilt

$$d_m = \begin{cases} m \frac{|G| - |\mathcal{Z}(G)|}{|\gamma_2(G)|} - \frac{d}{p} & \text{falls } m \leq p, \\ (2p - m) \frac{|G| - |\mathcal{Z}(G)|}{|\gamma_2(G)|} & \text{falls } m > p. \end{cases}$$

Beweis. Wegen $cl(G) = 2$ gilt $\gamma_2(G) \subseteq \mathcal{Z}(G)$. Sei \mathfrak{R} ein Repräsentantensystem von $(G/\gamma_2(G)) \setminus (\mathcal{Z}(G)/\gamma_2(G))$. Dann ist $e := |\{g \mid g \in \mathfrak{R}, g \text{ extremal}\}|$ die Anzahl der extremalen Konjugiertenklassen und $d = p |\{g \mid g \in \mathfrak{R}, |g^G| = p\}|$ nach Lemma 3.1.

Wir halten zunächst fünf einfache Beobachtungen fest.

$$(i) \text{ Für alle } n \in \underline{2p-1} \text{ gilt } |\Sigma(n-1)| = \begin{cases} n & \text{falls } n \leq p \\ 2p - n & \text{falls } n > p, \end{cases}$$

$$(ii) |\mathcal{K}(G)| = |\mathcal{Z}(G)| + d + e,$$

$$(iii) \gamma_2(G)\mathfrak{R} = \{g \mid g \in G, |g^G| \geq p\},$$

$$(iv) e + \frac{d}{p} = |\mathfrak{R}| = \frac{|G| - |\mathcal{Z}(G)|}{|\gamma_2(G)|} \quad \text{und}$$

$$(v) \sum_{n=1}^{2p-2} |\Sigma(n)| = p^2 - 1.$$

Für alle $g \in \mathfrak{R}$ sei $b_g \in [\{g\}, G]_{\mathfrak{G}} \setminus \{1_G\}$ und $a_g \in \gamma_2(G) \setminus \langle b_g \rangle$. Für alle $r, s \in \mathbb{Z}$ sei

$$w_{g,(r,s)} := \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} a_g^i b_g^j.$$

Ist dann $m \leq 2p - 2$, so folgt aus Satz 3.4

$$\mathfrak{B}_m := \{gw_{g,(r,s)} \mid (r,s) \in \Sigma(m-1), g \in \mathfrak{R}, s > 0 \text{ falls } |g^G| = p\} \subseteq \mathcal{Z}_m(\mathcal{J}(KG))$$

und \mathfrak{B}_m ist modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ K -linear unabhängig nach Satz 3.9 und Bemerkung 1.14.1. Nach Satz 3.4 gilt außerdem

$$\mathfrak{B}' := \{g - 1_G \mid g \in \mathfrak{R}\} \subseteq \mathcal{Z}_{2p-1}(\mathcal{J}(KG))$$

und \mathfrak{B}' ist modulo $\mathcal{Z}_{2p-2}(\mathcal{J}(KG))$ K -linear unabhängig nach Satz 3.9 und Bemerkung 1.14.1.

Folglich gilt

$$d_m \geq |\mathfrak{B}_m| = \left(e|\Sigma(m-1)| + \frac{d}{p} (|\Sigma(m-1)| - 1) \right),$$

falls $m \leq p$ und

$$d_m \geq |\mathfrak{B}_m| = \left(e + \frac{d}{p} \right) |\Sigma(m-1)|,$$

falls $m > p$ gilt.

Es folgt

$$\begin{aligned} \dim \mathcal{J}(KG) &\stackrel{3.10}{=} \dim \mathcal{Z}(\mathcal{J}(KG)) + \sum_{n=2}^{2p-1} \dim(\mathcal{Z}_n(\mathcal{J}(KG))/\mathcal{Z}_{n-1}(\mathcal{J}(KG))) \\ &\stackrel{1.5}{\geq} |\mathcal{K}(G)| - 1 + \sum_{n=2}^p \left(e|\Sigma(n-1)| + \frac{d}{p} (|\Sigma(n-1)| - 1) \right) \\ &\quad + \sum_{n=p+1}^{2p-1} \left(e + \frac{d}{p} \right) |\Sigma(n-1)| \\ &\stackrel{(iv)}{=} |\mathcal{K}(G)| - 1 + |\mathfrak{R}| \sum_{n=2}^{2p-1} |\Sigma(n-1)| - \frac{d}{p} (p-1) \\ &\stackrel{(ii),(v)}{=} |\mathcal{Z}(G)| + d + e - 1 + |\mathfrak{R}|(p^2 - 1) - d + \frac{d}{p} \\ &\stackrel{(iv)}{=} |\mathcal{Z}(G)| - 1 + |\gamma_2(G)| |\mathfrak{R}| \\ &\stackrel{(iii)}{=} |G| - 1 \\ &= \dim \mathcal{J}(KG). \end{aligned}$$

Damit liegt in obigen Ungleichungen Gleichheit vor und die Behauptung folgt aus (i) und (iv). \square

Im Beweis von Hauptsatz 3.11 haben wir die K -lineare Unabhängigkeit der Menge $\mathfrak{B}_m \subseteq \mathcal{Z}_m(\mathcal{J}(KG))$ modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ im Fall $m < 2p-1$ und der Menge \mathfrak{B}' modulo $\mathcal{Z}_{2p-2}(\mathcal{J}(KG))$ ausgenutzt. Da sich herausgestellt hat, dass die Dimension von $\mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ beziehungsweise von $\mathcal{J}(KG)/\mathcal{Z}_{2p-2}(\mathcal{J}(KG))$ gleich der Mächtigkeit dieser Menge ist, haben wir schärfer bewiesen:

3.11.1 Bemerkung.

- (i) Ist $m < 2p-1$, so ist \mathfrak{B}_m modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ eine K -Basis von $\mathcal{Z}_m(\mathcal{J}(KG))$.
- (ii) \mathfrak{B}' ist modulo $\mathcal{Z}_{2p-2}(\mathcal{J}(KG))$ eine K -Basis von $\mathcal{J}(KG)$.

\square

3.12 Beispiel. Sei $G := D_8 \times D_8$ (direktes Produkt von Diedergruppen der Ordnung 8) und K ein Körper mit $\text{char } K = 2$. Es gilt $\gamma_2(D_8) \cong C_2 \cong \mathcal{Z}(D_8)$ und damit $\gamma_2(G) \cong C_2 \times C_2 \cong \mathcal{Z}(G)$. Insbesondere gilt $cl(G) = 2$. Wegen $|\mathcal{Z}(D_8)| = 2$ enthält D_8 somit genau drei (extremale) Konjugiertenklassen der Länge zwei. Es folgt

$$\begin{aligned} |\{g^G \mid g \in G, \kappa(g) = 2\}| &= 3 \cdot 3 = 9, \\ |\{g^G \mid g \in G, \kappa(g) = 1\}| &= 3 \cdot 2 + 3 \cdot 2 = 12 \quad \text{und} \\ |\{g^G \mid g \in G, \kappa(g) = 0\}| &= 2 \cdot 2 = 4. \end{aligned}$$

Es gilt $\frac{|G| - |\mathcal{Z}(G)|}{|\gamma_2(G)|} = \frac{64 - 4}{4} = 15$. Aus Satz 1.5 und Hauptsatz 3.11 erhalten wir

$$\begin{aligned} \dim \mathcal{Z}(\mathcal{J}(KG)) &= |\mathcal{K}(G)| - 1 = 24, \\ \dim(\mathcal{Z}_2(\mathcal{J}(KG))/\mathcal{Z}_1(\mathcal{J}(KG))) &= 2 \cdot 15 - 6 = 24 \quad \text{und} \\ \dim(\mathcal{Z}_3(\mathcal{J}(KG))/\mathcal{Z}_2(\mathcal{J}(KG))) &= (2 \cdot 2 - 3)15 = 15. \end{aligned}$$

3.2 Nilpotenzklasse 3

In diesem Abschnitt untersuchen wir p -Gruppen G mit $\gamma_2(G) \cong C_p \times C_p$ und $cl(G) = 3$. Eine Bestimmung der Faktorräume in der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ gelingt uns in Hauptsatz 3.22 dabei in dem Fall, dass $p > 2$ gilt und $C_G(\gamma_2(G))$ abelsch ist. Obgleich dieser Einschränkungen setzen sich die Dimensionen der Faktorräume in der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$ bereits wesentlich unzugänglicher zusammen als im Fall der Nilpotenzklasse 2.

3.13 Lemma. *Sei G eine endliche nilpotente Gruppe und $g \in G$ mit $|g^G| = p$. Dann gilt*

$$\gamma_2(G) \leq C_G(g) \trianglelefteq G.$$

Beweis. Es gilt $p = |g^G| = \frac{|G|}{|C_G(g)|}$, also ist $C_G(g)$ eine maximale Untergruppe von G . Da G nilpotent ist, folgt nach einem Resultat von Wielandt [11, Kapitel III, § 3., 3.11]:

$$\gamma_2(G) \leq \Phi(G) \leq C_G(g).$$

□

Wir halten nun zunächst einige einfache Beobachtungen über den in diesem Abschnitt untersuchten Gruppentyp fest:

3.14 Lemma. *Sei G eine p -Gruppe mit $\gamma_2(G) \cong C_p \times C_p$ und $cl(G) = 3$.*

- (i) *Es gilt $\gamma_3(G) = \mathcal{Z}(G) \cap \gamma_2(G)$ und $|\gamma_3(G)| = p$.*
- (ii) *Für alle $z \in \gamma_3(G) \setminus \{1_G\}$ und $x \in \gamma_2(G) \setminus \mathcal{Z}(G)$ gilt $\gamma_2(G) = \langle x \rangle \langle z \rangle$.*
- (iii) *Für alle $x \in \gamma_2(G) \setminus \mathcal{Z}(G)$ gilt $C_G(\gamma_2(G)) = C_G(x)$ und $|G : C_G(\gamma_2(G))| = p$.*
- (iv) *Sind $g \in G$ und $z \in \gamma_3(G) \setminus \{1_G\}$ mit $gz \in g^G$, so gilt $g\gamma_3(G) \subseteq g^G$.*
- (v) *Ist $g \in \mathcal{Z}_2(G)$, so gilt für alle $h \in G \setminus C_G(g)$:*

$$g \{ [g, h^k]_{\mathfrak{S}} \mid k \in \underline{p-1}_0 \} = g \langle [g, h]_{\mathfrak{S}} \rangle = g^G.$$

- (vi) *Für alle $z \in \gamma_3(G)$ und $y \in G \setminus C_G(\gamma_2(G))$ existiert $x \in \gamma_2(G)$ mit $[x, y]_{\mathfrak{S}} = z$.*

Beweis. Wegen $cl(G) = 3$ gilt

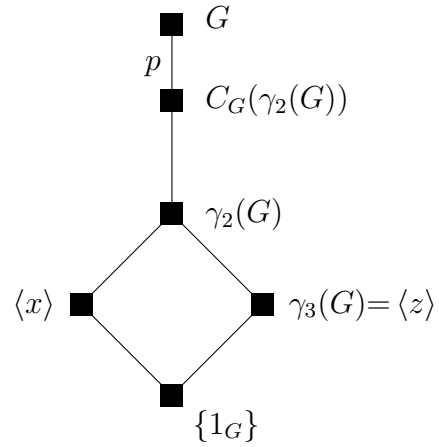
$$\{1_G\} \neq \gamma_3(G) \leq \mathcal{Z}(G) \cap \gamma_2(G) < \gamma_2(G).$$

Hieraus folgt direkt der erste Teil. Die Aussage (ii) folgt unmittelbar aus (i). Ist $x \in \gamma_2(G) \setminus \mathcal{Z}(G)$, so folgt $C_G(\gamma_2(G)) = C_G(x)$ aus (ii). Es gilt $x^G \stackrel{1.17}{=} x\gamma_3(G)$, also insbesondere $|x^G| = p$. Hieraus folgt (iii). Sind $g \in G$, $h \in G \setminus C_G(g)$ und $z \in \gamma_3(G) \setminus \{1_G\}$ mit $g^h = g[g, h]_{\mathfrak{S}} = gz$, so gilt $g[g, h^k]_{\mathfrak{S}} \stackrel{2.2}{=} gz^k$ für alle $k \in \mathbb{N}_0$. (iv) und (v) folgen somit aus $\gamma_3(G) = \langle z \rangle$.

Sei nun $z \in \gamma_3(G)$ und $y \in G \setminus C_G(\gamma_2(G))$. Sei $\tilde{x} \in \gamma_2(G) \setminus \mathcal{Z}(G)$ und $\tilde{z} := [\tilde{x}, y]_{\mathfrak{S}}$. Dann gilt $1_G \neq \tilde{z} \in \gamma_3(G)$ nach (iii) und folglich existiert $n \in \underline{p}$ mit $\tilde{z}^n = z$ nach (i). Wir setzen $x := \tilde{x}^n$ und erhalten aus

$$[x, y]_{\mathfrak{S}} = [\tilde{x}^n, y]_{\mathfrak{S}} \stackrel{2.2.1}{=} [\tilde{x}, y]_{\mathfrak{S}}^n = \tilde{z}^n = z$$

die Aussage (vi). □



Im Gegensatz zur Nilpotenzklasse 2 einer p -Gruppe G ist es dem Grundprinzip folgend für uns von Interesse, wie sich ausgewählte Elemente $w \in \langle \gamma_2(G) \rangle_K$ bei der Konjugation mit Elementen der Gruppe G verhalten. Ähnlich der Motivation von Lemma 2.23 resultiert hieraus das folgende, allgemeiner formulierte Lemma.

3.15 Lemma. Seien $G \cong C_p \times C_p$ und $x, z \in G$ mit $\langle x, z \rangle = G$. Für alle $r, s \in \mathbb{Z}$ sei

$$w_{(r,s)} := \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} x^i z^j.$$

Für alle $n, r, s \in \underline{p-1}_0$, $c \in \underline{s} \setminus \{1\}$ und $d \in \underline{c+r}_0$ existieren dann $\lambda_{(c,d)} \in K$ mit

$$\begin{aligned} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} x^i z^{-ni+j} &= w_{(r,s)} \\ &+ n(r+1)w_{(r+1,s-1)} + nrw_{(r,s-1)} \\ &+ \sum_{c=2}^s \sum_{d=0}^{c+r} \lambda_{(c,d)} w_{(d,s-c)}. \end{aligned}$$

Beweis. Seien $n, r, s \in \underline{p-1}_0$. Es gilt

$$\begin{aligned} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} x^i z^{-ni+j} &= \sum_{i=0}^{p-1} \left(\binom{i}{r} x^i \sum_{j=0}^{p-1} \binom{j}{s} z^{j-ni} \right) \\ &\stackrel{1.25}{=} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j+ni}{s} x^i z^j. \end{aligned}$$

Für alle $i, j \in \mathbb{N}_0$ erhalten wir

$$\begin{aligned} \binom{i}{r} \binom{j+ni}{s} &\stackrel{1.21}{=} \binom{i}{r} \sum_{c=0}^s \binom{j}{s-c} \binom{ni}{c} \\ &= \binom{i}{r} \binom{j}{s} + n \binom{i}{r} \binom{j}{s-1} \binom{i}{1} + \binom{i}{r} \sum_{c=2}^s \binom{j}{s-c} \binom{ni}{c}. \end{aligned}$$

Aus Lemma 1.24 folgt

$$\binom{i}{1} \binom{i}{r} = r \binom{i}{r} + (r+1) \binom{i}{r+1}$$

und damit

$$n \binom{i}{r} \binom{j}{s-1} \binom{i}{1} = nr \binom{i}{r} \binom{j}{s-1} + n(r+1) \binom{i}{r+1} \binom{j}{s-1}$$

für alle $i, j \in \mathbb{N}_0$.

Für alle $c \in \underline{s} \setminus \{1\}$ existieren nach 1.24.1 und Lemma 1.24 $\lambda_{(c,0)}, \dots, \lambda_{(c,c+r)} \in \mathbb{N}_0$, sodass für alle $i, j \in \mathbb{N}_0$ gilt:

$$\binom{j}{s-c} \binom{i}{r} \binom{ni}{c} = \binom{j}{s-c} \sum_{d=0}^{c+r} \lambda_{(c,d)} \binom{i}{d}.$$

Aus den dargelegten Rechnungen über Binomialkoeffizienten erhalten wir

$$\begin{aligned} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j+ni}{s} x^i z^j &= w_{(r,s)} \\ &+ n(r+1)w_{(r+1,s-1)} + nrw_{(r,s-1)} \\ &+ \sum_{c=2}^s \sum_{d=0}^{c+r} \lambda_{(c,d)} w_{(d,s-c)}. \end{aligned}$$

□

3.16 Satz.

Sei G eine p -Gruppe mit $\gamma_2(G) \cong C_p \times C_p$ und $cl(G) = 3$. Sei $x \in \gamma_2(G) \setminus \mathcal{Z}(G)$ und $z \in \gamma_3(G) \setminus \{1_G\}$ mit $\gamma_2(G) = \langle x \rangle \langle z \rangle$. Für alle $r, s \in \mathbb{Z}$ sei

$$w_{(r,s)} := \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} x^i z^j.$$

Für alle $r, s \in \underline{p-1}_0$ mit $(r, s) \neq (p-1, p-1)$ gilt dann

$$KGw_{(r,s)} \subseteq \mathcal{Z}_{2s+r+1}(\mathcal{J}(KG)).$$

Außerdem ist

$$\mathcal{J}(KG) = \mathcal{Z}_{3p-2}(\mathcal{J}(KG)).$$

Beweis. Seien $r, s \in \underline{p-1}_0$. Für den ersten Teil reicht es $gw_{(r,s)} \in \mathcal{Z}_{2s+r+1}(\mathcal{J}(KG))$ für alle $g \in G$ zu zeigen.

Sei $g \in G$. Wir zeigen die Behauptung durch Induktion nach $2s+r$. Gilt $2s+r=0$, also $r=0=s$, so folgt nach 1.5

$$gw_{(0,0)} = g \sum \gamma_2(G) \in \mathcal{Z}(\mathcal{J}(KG)).$$

Sei nun $2s+r > 0$ und $h \in G$. Nach Lemma 1.17 existieren $h_0, h_1, n \in \underline{p-1}_0$ mit $[g, h]_{\mathfrak{G}} = x^{-h_0} z^{-h_1}$ und $x^h = xz^{-n}$. Dann gilt

$$hg[g, h]_{\mathfrak{G}} w_{(r,s)}^h = hg[g, h]_{\mathfrak{G}} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} x^i z^{-ni+j}.$$

Für alle $c \in \underline{s}$ und $d \in \underline{c+r}_0$ gilt

$$2(s-c) + d \leq 2(s-c) + (c+r) = 2s+r-c < 2s+r.$$

Induktiv dürfen wir

$$\tilde{g}w_{(\tilde{r},\tilde{s})} \in \mathcal{Z}_{2\tilde{s}+\tilde{r}+1}(\mathcal{J}(KG)) \subseteq \mathcal{Z}_{2s+r}(\mathcal{J}(KG))$$

für alle $\tilde{g} \in G$ und $\tilde{r}, \tilde{s} \in \underline{p-1}_0$ mit $2\tilde{s} + \tilde{r} < 2s + r$ annehmen.

Aus Lemma 3.15 erhalten wir

$$hg[g,h]_{\mathfrak{S}}w_{(r,s)}^h \equiv_{\mathcal{Z}_{2s+r}(\mathcal{J}(KG))} hg[g,h]_{\mathfrak{S}}w_{(r,s)}$$

und weiter

$$hg[g,h]_{\mathfrak{S}}w_{(r,s)} = hg \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} x^{i-h_0} z^{j-h_1} \stackrel{3.3, \text{Ind.vor.}}{\equiv_{\mathcal{Z}_{2s+r}(\mathcal{J}(KG))}} hg w_{(r,s)}.$$

Ist nun $(r, s) \neq (p-1, p-1)$, so folgt $gw_{(r,s)} \in \mathcal{J}(KG)$ nach Bemerkung 3.3.1. Nach dem im Eingangskapitel erläuterten Grundprinzip folgt hieraus der erste Teil der Behauptung. Ist $(r, s) = (p-1, p-1)$, so gilt $w_{(r,s)} = x^{p-1}z^{p-1}$ nach 3.3.1, also $w_{(r,s)} \notin \mathcal{J}(KG)$. Dann gilt aber $gw_{(r,s)} - 1_G \in \mathcal{Z}_{3p-2}(\mathcal{J}(KG))$ nach Abschnitt 1.3. Also enthält $\mathcal{Z}_{3p-2}(\mathcal{J}(KG))$ eine K -Basis von $\mathcal{J}(KG)$. Satz 1.8 liefert nun die Behauptung. \square

Aus Lemma 3.3 und Satz 3.16 folgt direkt:

3.16.1 Bemerkung. Für alle $g \in G$, $a \in \gamma_2(G)$ und $r, s \in \underline{p-1}_0$ gilt

$$gaw_{(r,s)} \equiv_{\mathcal{Z}_{r+2s}(\mathcal{J}(KG))} gw_{(r,s)}.$$

\square

3.17 Lemma. Sei G eine p -Gruppe mit $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 3$ und $g \in G$. Dann gilt:

- (i) Ist $g \notin C_G(\gamma_2(G))$, so ist g extremal.
- (ii) Sei $C_G(\gamma_2(G))$ abelsch. Ist g extremal, so folgt $g \notin C_G(\gamma_2(G))$.

Insbesondere gilt dann $C_G(\gamma_2(G)) = \{h \mid h \in G, |h^G| \leq p\}$.

Beweis. Sei $x \in \gamma_2(G) \setminus \mathcal{Z}(G)$ und $z \in \gamma_3(G) \setminus \{1_G\}$ mit $\gamma_2(G) = \langle x \rangle \langle z \rangle$.

(i): Es gelte $g \notin C_G(\gamma_2(G))$. Aus $x \in \gamma_2(G) \setminus \mathcal{Z}(G)$ folgt $[g,x]_{\mathfrak{S}} \in \gamma_3(G) \setminus \{1_G\}$ nach Lemma 3.14 (iii), also $g[g,x]_{\mathfrak{S}} \in g^G$. Aus Lemma 3.14 (iv) erhalten wir $g\gamma_3(G) \subseteq g^G$ und damit $|g^G| \geq p$. Wegen

$$\mathcal{Z}_2(G) \stackrel{1.17, 3.14(i)}{\subseteq} \{h \mid h \in G, |h^G| \leq p\} \stackrel{3.13}{\subseteq} C_G(\gamma_2(G))$$

gilt außerdem $g \notin \mathcal{Z}_2(G)$. Also existiert $\tilde{g} \in G$ mit $g^{\tilde{g}} = g[g,\tilde{g}]_{\mathfrak{S}} \in g\gamma_2(G) \setminus g\gamma_3(G)$. Folglich erhalten wir $|g^G| > p$, also ist g extremal.

(ii): Sei $C_G(\gamma_2(G))$ abelsch und $y \in G \setminus C_G(\gamma_2(G))$. Nach Lemma 3.14 (iii) gilt

$$(*) \quad \bigcup_{k \in \underline{p-1}_0} C_G(\gamma_2(G))y^k = G.$$

Wir beweisen die Behauptung durch Kontraposition.

Es gelte also $g \in C_G(\gamma_2(G))$. Da $C_G(\gamma_2(G))$ abelsch ist, gilt $[g, h]_{\mathfrak{G}} = 1_G$ für alle $h \in C_G(\gamma_2(G))$. Für alle $\tilde{g} \in C_G(\gamma_2(G))$ und $k \in \mathbb{N}_0$ folgt aus der Kommutativität von $C_G(\gamma_2(G))$:

$$[g, \tilde{g}y^k]_{\mathfrak{G}} \stackrel{2.2}{=} [g, y^k]_{\mathfrak{G}}.$$

Da $y^p \in C_G(\gamma_2(G))$ nach Lemma 3.14 (iii) gilt, folgt $|g^G| \leq p$ aus (*) zusammen mit Lemma 1.17. Also ist g nicht extremal.

Der Zusatz zu (ii) folgt nun direkt aus (i) und (ii). \square

3.18 Lemma. Sei G eine p -Gruppe mit $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 3$ und $C_G(\gamma_2(G))$ abelsch. Dann gilt

$$\gamma_2(G)\mathcal{Z}(G) = \mathcal{Z}_2(G).$$

Beweis. Offenbar gilt $\gamma_2(G), \mathcal{Z}(G) \subseteq \mathcal{Z}_2(G)$, also $\gamma_2(G)\mathcal{Z}(G) \subseteq \mathcal{Z}_2(G)$.

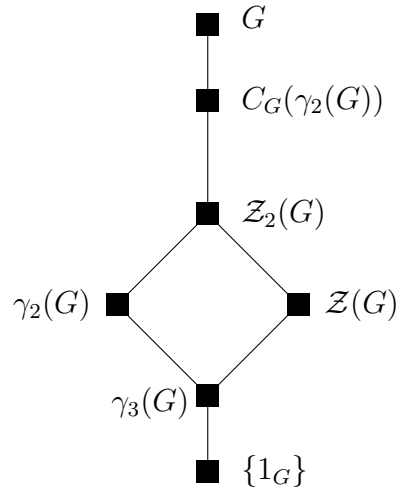
Sei nun $g \in \mathcal{Z}_2(G)$. Aus $g^G \subseteq g[\{g\}, G]_{\mathfrak{G}} \subseteq g\gamma_3(G)$ folgt $|g^G| \leq p$. Aus Lemma 3.17 erhalten wir $g \in C_G(\gamma_2(G))$. Sei $y \in G \setminus C_G(\gamma_2(G))$ und $z \in \gamma_3(G)$ mit $[g, y]_{\mathfrak{G}} = z$. Nach Lemma 3.14 (vi) existiert $x \in \gamma_2(G)$ mit $[x, y]_{\mathfrak{G}} = z$. Es folgt wegen $z \in \mathcal{Z}(G)$

$$1_G \stackrel{2.2}{=} [x, y]_{\mathfrak{G}}[x^{-1}, y]_{\mathfrak{G}},$$

also $[x^{-1}, y]_{\mathfrak{G}} = z^{-1}$. Sei $h \in G$. Nach Lemma 3.14 (iii) existieren $\tilde{h} \in C_G(\gamma_2(G))$, $k \in \underline{p-1}_0$ mit $h = y^k \tilde{h}$. Wir erhalten

$$\begin{aligned} [x^{-1}g, h]_{\mathfrak{G}} &= [x^{-1}g, y^k \tilde{h}]_{\mathfrak{G}} \stackrel{2.2}{=} [x^{-1}g, \tilde{h}]_{\mathfrak{G}}[x^{-1}g, y^k]_{\mathfrak{G}} \\ &\stackrel{C_G(\gamma_2(G))}{=} \stackrel{\text{abelsch}}{=} [x^{-1}g, y^k]_{\mathfrak{G}} \\ &\stackrel{2.2}{=} [x^{-1}, y^k]_{\mathfrak{G}}[g, y^k]_{\mathfrak{G}} \\ &\stackrel{2.2.1}{=} z^{-k} z^k = 1_G \end{aligned}$$

und damit $x^{-1}g \in \mathcal{Z}(G)$. \square



3.19 Lemma. *Sei G eine p -Gruppe mit $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 3$, $C_G(\gamma_2(G))$ abelsch und $g \in G \setminus \mathcal{Z}_2(G)$.*

- (i) *Ist g extremal, so existiert $h \in C_G(\gamma_2(G))$ mit $[g, h]_{\mathfrak{G}} \in \gamma_2(G) \setminus \gamma_3(G)$ und hg extremal.*
- (ii) *Ist g nicht extremal, so existiert $h \in G \setminus C_G(\gamma_2(G))$ mit $[g, h]_{\mathfrak{G}} \in \gamma_2(G) \setminus \gamma_3(G)$ und hg extremal.*

Beweis. Wegen $g \notin \mathcal{Z}_2(G)$ gilt insbesondere $g \notin \mathcal{Z}(G)$. Also ist g extremal oder $|g^G| = p$. Sei g zunächst extremal. Dann gilt $g \notin C_G(\gamma_2(G))$ nach Lemma 3.17 und $\langle g \rangle C_G(\gamma_2(G)) = G$ nach 3.14 (iii). Da $[g, g^k h]_{\mathfrak{G}} \stackrel{2.2}{=} [g, h]_{\mathfrak{G}}$ für alle $h \in C_G(\gamma_2(G))$ und $k \in \mathbb{N}$ gilt, existiert $h \in C_G(\gamma_2(G))$ mit $[g, h]_{\mathfrak{G}} \in \gamma_2(G) \setminus \gamma_3(G)$ aufgrund der Extremalität von g . Wegen $hg \notin C_G(\gamma_2(G))$ ist nach Lemma 3.17 auch hg extremal.

Sei nun $|g^G| = p$. Dann gilt $g \in C_G(\gamma_2(G))$ nach Lemma 3.17. Sei $h \in G$ extremal. Dann gilt $h \notin C_G(\gamma_2(G))$ und hg ist extremal. Da $g \notin \mathcal{Z}_2(G)$, existiert $y \in G$ mit $[g, y]_{\mathfrak{G}} \in \gamma_2(G) \setminus \gamma_3(G)$. Wegen der Kommutativität von $C_G(\gamma_2(G))$ gilt $[g, \tilde{g}h]_{\mathfrak{G}} \stackrel{2.2}{=} [g, h]_{\mathfrak{G}}$ für alle $\tilde{g} \in C_G(\gamma_2(G))$. Nach 3.14 (iii) gilt weiter $C_G(\gamma_2(G)) \langle h \rangle = G$. Dies impliziert, dass bereits $[g, h]_{\mathfrak{G}} \in \gamma_2(G) \setminus \gamma_3(G)$ gilt. \square

3.20 Definition. *Für alle $m \in \underline{3p-3}_0$ sei*

$$\Xi(m) := \{(r, s) \mid r, s \in \underline{p-1}_0, m = r + 2s\}.$$

3.21 Satz. *Sei $p > 2$, G eine p -Gruppe mit $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 3$ und $C_G(\gamma_2(G))$ abelsch. Sei $x \in \gamma_2(G) \setminus \mathcal{Z}(G)$, $z \in \gamma_3(G) \setminus \{1_G\}$ mit $\gamma_2(G) = \langle x \rangle \langle z \rangle$ und $g \in G$. Für alle $r, s \in \mathbb{Z}$ sei*

$$w_{(r,s)} := \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{r} \binom{j}{s} x^i z^j.$$

Für alle $m \in \underline{3p-4}_0$ gilt:

- (i) *Ist g extremal, so ist*

$$\left\{ gw_{(r,s)} \mid (r, s) \in \Xi(m) \right\}$$

modulo $\mathcal{Z}_m(\mathcal{J}(KG))$ K -linear unabhängig.

- (ii) *Ist $|g^G| = p$ und $g \notin \mathcal{Z}_2(G)$, so ist*

$$\left\{ gw_{(r,s)} \mid (r, s) \in \Xi(m), r \neq 0 \right\}$$

modulo $\mathcal{Z}_m(\mathcal{J}(KG))$ K -linear unabhängig.

(iii) Ist $g \in \mathcal{Z}(G)$, so ist

$$\left\{ gw_{(r,s)} \mid (r,s) \in \Xi(m), s \neq 0, r \neq p-1 \right\}$$

modulo $\mathcal{Z}_m(\mathcal{J}(KG))$ K -linear unabhängig.

(iv) Ist $g \notin \mathcal{Z}_2(G)$, so gilt $g - 1_G \notin \mathcal{Z}_{3p-3}(\mathcal{J}(KG))$.

Beweis. Sei $m \in \underline{3p-3}_0$. Es wird sich für den Beweis der Aussage (iv) als günstig erweisen, den Fall $m = 3p-3$ zunächst miteinzubeziehen.

Ist $m = 0$, so gilt $\Xi(m) = \{(0,0)\}$ und die Aussage (i) folgt in diesem Fall aus

$$g \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{0} \binom{j}{0} x^i z^j = g \sum \gamma_2(G) \stackrel{1.5}{\in} \mathcal{Z}(\mathcal{J}(KG)) \setminus \{0_{KG}\}. \quad (3.5)$$

Wir wollen nun die Aussage (i) durch Induktion nach m beweisen und diese dann nutzen, um die Aussagen (ii)-(iv) zu verifizieren.

Sei $m > 0$ und $\tilde{s} \in \underline{p-1}_0$ maximal mit $m - 2\tilde{s} \in \underline{p-1}_0$. Sei $\tilde{r} := m - 2\tilde{s}$. Dann gilt $\tilde{r} + 2\tilde{s} = m$ und

$$\Xi(m) = \{(\tilde{r} + 2k, \tilde{s} - k) \mid k \in \underline{p-1}_0, \tilde{r} + 2k \leq p-1, \tilde{s} - k \geq 0\}.$$

Sei $M := \{k \mid k \in \underline{p-1}_0, \tilde{r} + 2k \leq p-1, \tilde{s} - k \geq 0\}$.

Für alle $h \in G$ seien $h_0, h_1, h_2 \in \underline{p-1}_0$ mit

$$[g, h]_{\mathfrak{G}} = x^{-h_0} z^{-h_1} \quad \text{und} \quad x^h = x z^{-h_2}.$$

Für alle $k \in M$ sei $\lambda_k \in K$. Bevor wir mit dem Beweis von (i) beginnen, untersuchen wir der Idee des Grundprinzips folgend

$$hg[g, h]_{\mathfrak{G}} \sum_{k \in M} \lambda_k w_{(\tilde{r}+2k, \tilde{s}-k)}^h$$

für alle $h \in G$.

Es gilt für alle $h \in G$, $k \in M$, $c \in \underline{\tilde{s}-k} \setminus \{1\}$ und $d \in \underline{c + \tilde{r} + 2k}_0$:

$$\begin{aligned} 2(\tilde{s} - k - c) + d &\leq 2(\tilde{s} - k - c) + c + \tilde{r} + 2k = \tilde{r} + 2\tilde{s} - c < \tilde{r} + 2\tilde{s} - 1 = m - 1 \quad \text{und} \\ \tilde{r} + 2k + 2(\tilde{s} - k - 1) &< \tilde{r} + 2\tilde{s} - 1 = m - 1. \end{aligned} \quad (3.6)$$

Für alle $h \in G$ und $k \in M$ folgt hieraus

$$\begin{aligned} hg[g, h]_{\mathfrak{G}} w_{(\tilde{r}+2k, \tilde{s}-k)}^h &= hg[g, h]_{\mathfrak{G}} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{\tilde{r}+2k} \binom{j}{\tilde{s}-k} x^i z^{-h_2 i + j} \\ &\stackrel{3.15, 3.16}{=} hg[g, h]_{\mathfrak{G}} w_{(\tilde{r}+2k, \tilde{s}-k)} + hg[g, h]_{\mathfrak{G}} h_2(\tilde{r} + 2k + 1) w_{(\tilde{r}+2k+1, \tilde{s}-k-1)}. \end{aligned} \quad (3.7)$$

Außerdem gilt

$$hg[g, h]_{\mathfrak{G}} w_{(\tilde{r}+2k, \tilde{s}-k)} = hg[g, h]_{\mathfrak{G}} \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \binom{i}{\tilde{r}+2k} \binom{j}{\tilde{s}-k} x^{i-h_0} z^{j-h_1} \quad (3.8)$$

$$\stackrel{3.3, 3.16}{\equiv} \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \quad hgw_{(\tilde{r}+2k, \tilde{s}-k)} + hgh_0w_{(\tilde{r}+2k-1, \tilde{s}-k)}$$

für alle $h \in G$ und $k \in M$.

Wegen $m-1 = \tilde{r} + 2\tilde{s} - 1 = \tilde{r} + 2k + 1 + 2(\tilde{s} - k - 1)$ gilt darüber hinaus für alle $h \in G$ und $k \in M$:

$$hg[g, h]_{\mathfrak{G}} w_{(\tilde{r}+2k+1, \tilde{s}-k-1)} \stackrel{3.16.1}{\equiv} \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \quad hgw_{(\tilde{r}+2k+1, \tilde{s}-k-1)}. \quad (3.9)$$

Wir erhalten

$$\begin{aligned} hg[g, h]_{\mathfrak{G}} \sum_{k \in M} \lambda_k w_{(\tilde{r}+2k, \tilde{s}-k)} &\stackrel{(3.7)}{\equiv} \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \quad hg[g, h]_{\mathfrak{G}} \sum_{k \in M} \lambda_k w_{(\tilde{r}+2k, \tilde{s}-k)} \\ &+ hg[g, h]_{\mathfrak{G}} \sum_{k \in M} \lambda_k h_2(\tilde{r} + 2k + 1) w_{(\tilde{r}+2k+1, \tilde{s}-k-1)} \\ &\stackrel{(3.8), 3.16}{\equiv} \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \quad hg \sum_{k \in M} \lambda_k w_{(\tilde{r}+2k, \tilde{s}-k)} + hg \sum_{k \in M} \lambda_k h_0 w_{(\tilde{r}+2k-1, \tilde{s}-k)} \\ &+ hg[g, h]_{\mathfrak{G}} \sum_{k \in M} \lambda_k h_2(\tilde{r} + 2k + 1) w_{(\tilde{r}+2k+1, \tilde{s}-k-1)} \\ &\stackrel{(3.9)}{\equiv} \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \quad hg \sum_{k \in M} \lambda_k w_{(\tilde{r}+2k, \tilde{s}-k)} + hg \sum_{k \in M} \lambda_k h_0 w_{(\tilde{r}+2k-1, \tilde{s}-k)} \\ &+ hg \sum_{k \in M} \lambda_k h_2(\tilde{r} + 2k + 1) w_{(\tilde{r}+2k+1, \tilde{s}-k-1)} \end{aligned} \quad (3.10)$$

für alle $h \in G$.

Nach diesen Vorbetrachtungen sei nun $m \leq 3p - 4$ und es gelte

$$\sum_{k \in M} \lambda_k gw_{(\tilde{r}+2k, \tilde{s}-k)} \in \mathcal{Z}_m(\mathcal{J}(KG)). \quad (3.11)$$

Um zu beweisen, dass

$$\{gw_{(\tilde{r}+2k, \tilde{s}-k)} \mid k \in M\} \text{ modulo } \mathcal{Z}_m(\mathcal{J}(KG))$$

K -linear unabhängig ist, ist also $\lambda_k = 0_K$ für alle $k \in M$ zu zeigen.

Aus den Gleichungen (3.10), (3.11) und dem Grundprinzip folgt

$$\sum_{k \in M} \lambda_k h_0 hgw_{(\tilde{r}+2k-1, \tilde{s}-k)} + \sum_{k \in M} \lambda_k h_2(\tilde{r} + 2k + 1) hgw_{(\tilde{r}+2k+1, \tilde{s}-k-1)} \in \mathcal{Z}_{m-1}(\mathcal{J}(KG))$$

für alle $h \in G$ und es gilt mit $\lambda_k := 0_K$, falls $k \notin M$:

$$\begin{aligned} & \lambda_0 h_0 h g w_{(\tilde{r}-1, \tilde{s})} + \sum_{k \in M} (\lambda_{k+1} h_0 + \lambda_k h_2(\tilde{r} + 2k + 1)) h g w_{(\tilde{r}+2k+1, \tilde{s}-k-1)} \\ &= \sum_{k \in M} \lambda_k h_0 h g w_{(\tilde{r}+2k-1, \tilde{s}-k)} + \sum_{k \in M} \lambda_k h_2(\tilde{r} + 2k + 1) h g w_{(\tilde{r}+2k+1, \tilde{s}-k-1)} \in \mathcal{Z}_{m-1}(\mathcal{J}(KG)). \end{aligned} \quad (3.12)$$

(i) Sei g extremal. Wie eingangs erwähnt zeigen wir die Behauptung durch einen Induktionsbeweis nach m . Der Induktionsanfang $m = 0$ folgt dabei aus Gleichung (3.5).

Für alle $k \in M$ gilt

$$\tilde{r} + 2k + 1 + 2(\tilde{s} - k - 1) = \tilde{r} + 2\tilde{s} - 1 = m - 1 < \tilde{r} + 2\tilde{s}.$$

Induktiv dürfen wir für alle $h \in G$ mit hg extremal annehmen:

$$\left\{ h g w_{(r,s)} \mid (r,s) \in \Xi(m-1) \right\} \text{ ist modulo } \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \text{ } K\text{-linear unabhängig.}$$

Aus (3.12) folgt für alle $h \in G$ im Fall der Extremalität von hg daher:

(a) Ist $\tilde{r} \neq 0$, so gilt $\lambda_0 h_0 = 0_K$.

(b) Ist $k \in M$ mit $\tilde{r} + 2k + 1 \in \underline{p-1}_0$ und $\tilde{s} - k - 1 \in \underline{p-1}_0$, so ist

$$\lambda_{k+1} h_0 + \lambda_k h_2(\tilde{r} + 2k + 1) = 0_K.$$

Für alle $k \in M$ ist nach Gleichung (3.11) nun $\lambda_k = 0_K$ nachzuweisen.

Es gelte zunächst $\tilde{r} \neq 0$. Nach Lemma 3.19 existiert $h \in G$ mit $h_0 \neq 0$ und hg extremal. Aus (a) folgt dann $\lambda_0 = 0_K$. Induktiv (nach k) erhalten wir aus (b) damit $\lambda_{k+1} = 0_K$ für alle $k \in \underline{p-1}_0$ mit $\tilde{r} + 2k + 1 \leq p-1$ und $\tilde{s} - k - 1 \geq 0$. Insbesondere gilt dann $\lambda_k = 0_K$ für alle $k \in M$.

Es gelte $\tilde{r} = 0$ (und damit $\tilde{s} \neq 0$). Dann gilt $g_0 = 0$ und $g_2 \neq 0$, da nach Lemma 3.17 $g \notin C_G(\gamma_2(G))$ gilt. Da $p > 2$ gilt, ist g^2 nach Lemma 3.17 auch extremal. Sei nun $\tilde{k} \in M$ minimal mit $\tilde{r} + 2\tilde{k} + 1 > p-1$ oder $\tilde{s} - \tilde{k} - 1 < 0$. Dann gilt $\tilde{k} > 0$. Wir erhalten aus (b) damit $\lambda_k g_2(\tilde{r} + 2k + 1) = 0$ für alle $k \in M$ mit $k < \tilde{k}$, also $\lambda_k = 0_K$ für alle $k \in M$ mit $k < \tilde{k}$. Insbesondere gilt $\tilde{k} - 1 \in M$ und $\lambda_{\tilde{k}-1} = 0_K$. Nach Lemma 3.19 (i) existiert $h \in C_G(\gamma_2(G))$ mit $h_0 \neq 0$. Gemäß (b) folgt $\lambda_{\tilde{k}} = 0_K$ und damit $\lambda_k = 0_K$ für alle $k \in M$. Hieraus folgt (i).

(ii) Sei $|g^G| = p$, $g \notin \mathcal{Z}_2(G)$ und $\tilde{r} \neq 0$.

Nach 3.19 (ii) existiert $h \in G$ mit $h_0 \neq 0$ und hg extremal. Da $\tilde{r} \neq 0$ folgt aus (a) $\lambda_0 = 0_K$. Wie in (i) folgt dann $\lambda_k = 0_K$ für alle $k \in M$.

(iii) Sei $g \in \mathcal{Z}(G)$ und $k \in M$ mit $\tilde{r} + 2k < p - 1$ und $\tilde{s} - k > 0$. Dann gilt $\tilde{r} + 2k + 1 \leq p - 1$ und $\tilde{s} - k - 1 \geq 0$, sodass die Voraussetzungen von (b) erfüllt sind.

Sei $h \in G$ extremal. Dann gilt $h \notin C_G(\gamma_2(G))$, $h_0 = 0 = h_1$, $h_2 \neq 0$ und hg ist extremal. Aus (b) folgt dann $\lambda_k h_2(\tilde{r} + 2k + 1) = 0_K$. Wegen $h_2, \tilde{r} + 2k + 1 \not\equiv_p 0$ folgt hieraus $\lambda_k = 0_K$.

(iv) Sei $g \notin \mathcal{Z}_2(G)$. Es gilt $w_{(p-1, p-1)} = x^{p-1} z^{p-1}$ nach 3.3.1 (ii). Sei $m := 3p - 3$. Dann gilt $\tilde{s} = p - 1 = \tilde{r}$ und $M = \{0\}$. Wir setzen $\lambda_0 := 1_K$. Wegen $\tilde{r} + 1 = p$ folgt aus Gleichung (3.10) für alle $h \in G$:

$$hg[g, h]_{\mathfrak{G}w_{(p-1, p-1)}^h} \equiv_{\mathcal{Z}_{3p-4}(\mathcal{J}(KG))} hgw_{(p-1, p-1)} + hgh_0w_{(p-2, p-1)}. \quad (3.13)$$

Nach 3.19 existiert $h \in G$ mit $h_0 \neq 0$ und hg extremal. Aus Aussage (i) erhalten wir $hgh_0w_{(p-2, p-1)} \notin \mathcal{Z}_{3p-4}(\mathcal{J}(KG))$.

Hieraus folgt unter Anwendung des Grundprinzips

$$g - 1_G \equiv_{\mathcal{Z}_{3p-3}(\mathcal{J}(KG))}^{3.16.1} (gw_{(p-1, p-1)} - 1_G) \notin \mathcal{Z}_{3p-3}(\mathcal{J}(KG)).$$

□

3.22 Hauptsatz. Sei $p > 2$, G eine p -Gruppe mit $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 3$ und $C_G(\gamma_2(G))$ abelsch. Sei $m \in \underline{3p-2} \setminus \{1\}$ und

$$d_m := \dim(\mathcal{Z}_m(\mathcal{J}(KG)) / \mathcal{Z}_{m-1}(\mathcal{J}(KG))).$$

Dann gilt

$$d_m = \begin{cases} \frac{|G|}{|\gamma_2(G)|} |\Xi(m-1)| & \text{falls } m > p \text{ und } m \text{ gerade,} \\ \frac{|G|}{|\gamma_2(G)|} |\Xi(m-1)| - \frac{|C_G(\gamma_2(G))|}{|\gamma_2(G)|} & \text{falls } m < 2p \text{ und } m \text{ ungerade,} \\ \frac{|G|}{|\gamma_2(G)|} |\Xi(m-1)| - \frac{|\mathcal{Z}_2(G)|}{|\gamma_2(G)|} & \text{falls } m \leq p \text{ und } m \text{ gerade} \\ & \text{oder falls } m \geq 2p \text{ und } m \text{ ungerade.} \end{cases}$$

Beweis. Es gilt nach Lemma 3.18 und Lemma 3.17:

$$\begin{aligned} \{H \mid H \in G/\gamma_2(G), \mu(H) = 0\} &\stackrel{3.18}{=} \mathcal{Z}_2(G)/\gamma_2(G), \\ \{H \mid H \in G/\gamma_2(G), \mu(H) = 1\} &\stackrel{3.17, 3.18}{=} (C_G(\gamma_2(G))/\gamma_2(G)) \setminus (\mathcal{Z}_2(G)/\gamma_2(G)) \quad \text{und} \\ \{H \mid H \in G/\gamma_2(G), \mu(H) = 2\} &\stackrel{3.17}{=} (G/\gamma_2(G)) \setminus (C_G(\gamma_2(G))/\gamma_2(G)). \end{aligned}$$

Sei \mathfrak{R} eine Repräsentantensystem von $G/\gamma_2(G)$ mit $\kappa(g) = \mu(H)$ für alle $H \in G/\gamma_2(G)$ und $g \in \mathfrak{R} \cap H$. Wir setzen

$$\begin{aligned} c &:= |\{g \mid g \in \mathfrak{R}, \kappa(g) = 0\}|, \\ d &:= |\{g \mid g \in \mathfrak{R}, \kappa(g) = 1\}| \quad \text{und} \\ e &:= |\{g \mid g \in \mathfrak{R}, \kappa(g) = 2\}|. \end{aligned}$$

Dann gilt

- (i) $c = |\mathcal{Z}_2(G)/\gamma_2(G)|$,
- (ii) $c + d = |C_G(\gamma_2(G))/\gamma_2(G)|$,
- (iii) $c + d + e = \frac{|G|}{|\gamma_2(G)|} = |\mathfrak{R}|$,
- (iv) $|\mathcal{K}(G)| = c|\mathcal{K}_{\gamma_2(G)}(G)| + dp + e = c(p + (p - 1)) + dp + e = c(2p - 1) + dp + e$ und
- (v) $\sum_{n=2}^{3p-2} |\Xi(n - 1)| = p^2 - 1$.

Sei

$$\begin{aligned}
 \mathfrak{B}_c &:= \{gw_{(r,s)} \mid (r,s) \in \Xi(m-1), g \in \mathfrak{R}, \kappa(g) = 0, s \neq 0, r \neq p-1\}, \\
 \mathfrak{B}_d &:= \{gw_{(r,s)} \mid (r,s) \in \Xi(m-1), g \in \mathfrak{R}, \kappa(g) = 1, r \neq 0\}, \\
 \mathfrak{B}_e &:= \{gw_{(r,s)} \mid (r,s) \in \Xi(m-1), g \in \mathfrak{R}, \kappa(g) = 2\}, \\
 \mathfrak{B}_m &:= \mathfrak{B}_c \cup \mathfrak{B}_d \cup \mathfrak{B}_e \quad \text{und} \\
 \mathfrak{B}' &:= \{g - 1_G \mid g \in \mathfrak{R} \setminus \mathcal{Z}_2(G)\}.
 \end{aligned} \tag{3.14}$$

Ist $m < 3p - 2$, so folgt aus Satz 3.16

$$\mathfrak{B}_m \subseteq \mathcal{Z}_m(\mathcal{J}(KG)) \tag{3.15}$$

und aus Satz 3.21 und Bemerkung 1.14.1 folgt

$$\mathfrak{B}_m \text{ ist modulo } \mathcal{Z}_{m-1}(\mathcal{J}(KG)) \text{ } K\text{-linear unabhängig.} \tag{3.16}$$

Außerdem gilt nach Satz 3.16

$$\mathfrak{B}' \subseteq \mathcal{Z}_{3p-2}(\mathcal{J}(KG)) \tag{3.17}$$

und aus Satz 3.21 und Bemerkung 1.14.1 folgt

$$\mathfrak{B}' \text{ ist modulo } \mathcal{Z}_{3p-3}(\mathcal{J}(KG)) \text{ } K\text{-linear unabhängig.} \tag{3.18}$$

Wir erhalten nun folgende Abschätzungen für die Dimensionen der Faktorräume in der aufsteigenden Zentralreihe von $\mathcal{J}(KG)$:

1. Ist $m > p$ und m gerade, so gilt $m - 1 \geq p$ und $m - 1$ ist ungerade. Außerdem gilt $m < 3p - 2$. Sind $r, s \in \underline{p-1}_0$ mit $m - 1 = r + 2s$, so gilt $s \neq 0$ und r ist ungerade. Wegen $p > 2$ gilt $p - 1 \neq r \neq 0$. Es folgt aus (3.15) und (3.16):

$$d_m \geq (c + d + e)|\Xi(m - 1)| \stackrel{(iii)}{=} \frac{|G|}{|\gamma_2(G)|} |\Xi(m - 1)|.$$

3 p -Gruppen mit p -elementar-abelscher Kommutatoruntergruppe

2. Ist $m \in \underline{2p-1}_1$ und m ungerade, so gilt $m-1 \in \underline{2p-2}_0$ und $m-1$ ist gerade. Dann existiert $s \in \underline{p-1}_0$ mit $m-1 = 0 + 2s$. Also gilt $(0, s) \in \Xi(m-1)$.

Ist $m-1 \leq p-1$, so gilt $m-1 = m-1 + 2 \cdot 0$ und damit $(m-1, 0) \in \Xi(m-1)$.

Ist $m-1 > p-1$, so existiert $t \in \underline{p-1}_0$ mit $m-1 = p-1 + 2t$ und es gilt dann $(p-1, t) \in \Xi(m-1)$. Es folgt aus (3.15) und (3.16)

$$d_m \geq e|\Xi(m-1)| + (c+d)(|\Xi(m-1)| - 1) \stackrel{(iii)}{=} \frac{|G|}{|\gamma_2(G)|} |\Xi(m-1)| - (c+d).$$

3. Ist $m \in \underline{p}$ und m gerade, so ist $m-1 \leq p-1$ und $m-1$ ungerade. Dann gilt $m-1 = m-1 + 2 \cdot 0$, also $(m-1, 0) \in \Xi(m-1)$. Sind außerdem $r, s \in \underline{p-1}_0$ mit $m-1 = r + 2s$, so ist $0 \neq r \neq p-1$. Es folgt aus (3.15) und (3.16)

$$d_m \geq (e+d)|\Xi(m-1)| + c(|\Xi(m-1)| - 1) \stackrel{(iii)}{=} \frac{|G|}{|\gamma_2(G)|} |\Xi(m-1)| - c.$$

4. Ist $m \geq 2p$ und m ungerade, so gilt $m-1 \geq 2p-1$ und $m-1$ ist gerade. Sind dann $r, s \in \underline{p-1}_0$ mit $m-1 = r + 2s$, so gilt $r \neq 0 \neq s$. Wegen $p > 2$ existiert außerdem $t \in \underline{p-1}_0$ mit $m-1 = p-1 + 2t$, das heißt $(p-1, t) \in \Xi(m-1)$. Ist $m < 3p-2$, so folgt aus (3.15) und (3.16)

$$d_m \geq (e+d)|\Xi(m-1)| + c(|\Xi(m-1)| - 1) \stackrel{(iii)}{=} \frac{|G|}{|\gamma_2(G)|} |\Xi(m-1)| - c.$$

Ist $m = 3p-2$, so gilt $\Xi(m-1) = \{(p-1, p-1)\}$ und

$$d_m \geq (e+d)|\Xi(m-1)| + c(|\Xi(m-1)| - 1) \stackrel{(iii)}{=} \frac{|G|}{|\gamma_2(G)|} |\Xi(m-1)| - c$$

folgt aus (3.17) und (3.18).

Seien

$$\begin{aligned} A_2 &:= \{k \mid k \in \underline{2p-1}_1 \setminus \{1\}, k \text{ ungerade}\}, \\ A_3 &:= \{k \mid k \in \underline{p}, k \text{ gerade}\} \quad \text{und} \\ A_4 &:= \{k \mid k \in \underline{3p-2}, k \geq 2p, k \text{ ungerade}\}. \end{aligned} \tag{3.19}$$

Dann gilt $|A_2| = p-1$ und $|A_3| = \frac{p-1}{2} = |A_4|$.

Es folgt

$$\begin{aligned}
\dim \mathcal{J}(KG) &\stackrel{3.16}{=} \sum_{n=1}^{3p-2} d_n \\
&\geq \dim \mathcal{Z}(\mathcal{J}(KG)) + \left(\frac{|G|}{|\gamma_2(G)|} \sum_{n=2}^{3p-2} |\Xi(n-1)| \right) - (c+d)|A_2| - c(|A_3| + |A_4|) \\
&\stackrel{1.5.(v)}{=} |\mathcal{K}(G)| - 1 + \frac{|G|}{|\gamma_2(G)|} (p^2 - 1) - (c+d)(p-1) - c(p-1) \\
&\stackrel{(iv)}{=} c(2p-1) + dp + e - 1 + \frac{|G|}{|\gamma_2(G)|} (|\gamma_2(G)| - 1) - (2c+d)(p-1) \\
&= \frac{|G|}{|\gamma_2(G)|} (|\gamma_2(G)| - 1) + (e + c + d) - 1 \\
&\stackrel{(iii)}{=} |G| - 1 \\
&= \dim \mathcal{J}(KG).
\end{aligned}$$

Damit liegt bei den Ungleichungen in 1.-4. jeweils Gleichheit vor. Die Behauptung folgt nun aus 1.-4. sowie (i) und (ii). \square

Im Beweis von Hauptsatz 3.22 haben wir die K -lineare Unabhängigkeit der Menge $\mathfrak{B}_m \subseteq \mathcal{Z}_m(\mathcal{J}(KG))$ modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ im Fall $m < 3p-2$ und der Menge \mathfrak{B}' modulo $\mathcal{Z}_{3p-3}(\mathcal{J}(KG))$ ausgenutzt. Da sich herausgestellt hat, dass die Dimension von $\mathcal{Z}_m(\mathcal{J}(KG))/\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ beziehungsweise von $\mathcal{J}(KG)/\mathcal{Z}_{3p-3}(\mathcal{J}(KG))$ gleich der Mächtigkeit dieser Menge ist, haben wir schärfer bewiesen:

3.22.1 Bemerkung.

- (i) Ist $m < 3p-2$, so ist \mathfrak{B}_m modulo $\mathcal{Z}_{m-1}(\mathcal{J}(KG))$ eine K -Basis von $\mathcal{Z}_m(\mathcal{J}(KG))$.
- (ii) \mathfrak{B}' ist modulo $\mathcal{Z}_{3p-3}(\mathcal{J}(KG))$ eine K -Basis von $\mathcal{J}(KG)$.

\square

Die folgende Bemerkung zeigt, wie man die im Hauptsatz auftretende Mächtigkeit von $\Xi(m-1)$ berechnet.

3.22.2 Bemerkung. Es gilt

$$|\Xi(m-1)| = \begin{cases} \frac{p+1}{2}, & \text{falls } p \leq m \leq 2p, \text{ } m \text{ ungerade} \\ \frac{p-1}{2}, & \text{falls } p-1 \leq m \leq 2p, \text{ } m \text{ gerade} \\ \frac{m+1}{2}, & \text{falls } m < p-1, \text{ } m \text{ ungerade} \\ \frac{m}{2}, & \text{falls } m < p-1, \text{ } m \text{ gerade} \\ \frac{3p-m}{2}, & \text{falls } 2p < m, \text{ } m \text{ ungerade} \\ \frac{3p-1-m}{2}, & \text{falls } 2p < m, \text{ } m \text{ gerade} \end{cases}$$

3 p -Gruppen mit p -elementar-abelscher Kommutatoruntergruppe

Beweis. Sei m zunächst ungerade. Dann ist $m - 1$ gerade und es gilt nach Definition von $\Xi(m - 1)$:

$$\Xi(m - 1) = \left\{ \left(2k, \frac{m-1}{2} - k \right) \mid k \in \mathbb{N}_0, 0 \leq \frac{m-1}{2} - k \leq p-1 \wedge 0 \leq 2k \leq p-1 \right\}.$$

Ist $m \leq p$, so folgt

$$|\Xi(m - 1)| = \left| \left\{ k \mid k \in \mathbb{N}_0, k \leq \frac{m-1}{2} \right\} \right| = \frac{m+1}{2}.$$

Ist $p \leq m \leq 2p$, so folgt

$$|\Xi(m - 1)| = \left| \left\{ k \mid k \in \mathbb{N}_0, k \leq \frac{p-1}{2} \right\} \right| = \frac{p+1}{2}.$$

Ist $m > 2p$, so gilt

$$\Xi(m - 1) = \left\{ \left(2k, \frac{m-1}{2} - k \right) \mid k \in \underline{p-1}_0, \frac{m-1}{2} - k \leq p-1 \wedge k \leq \frac{p-1}{2} \right\}$$

und damit

$$\begin{aligned} |\Xi(m - 1)| &= \left| \left\{ k \mid k \in \underline{p-1}_0, \frac{m-1}{2} - (p-1) \leq k \leq \frac{p-1}{2} \right\} \right| \\ &= \frac{p-1}{2} - \left(\frac{m-1}{2} - (p-1) - 1 \right) \\ &= \frac{3p-m}{2}. \end{aligned}$$

Ist m gerade, so führt eine leichte Abwandlung obiger Überlegungen zu den Behauptungen. \square

3.23 Beispiel. Sei $p > 2$, G eine Gruppe der Ordnung p^4 mit $|\gamma_2(G)| = p^2$. Dann gilt $\gamma_2(G) \cong C_p \times C_p$, $cl(G) = 3$ und $C_G(\gamma_2(G))$ ist abelsch.

Beweis. Es gilt $\gamma_2(G) \leq \Phi(G)$ nach einem von Satz von Wielandt [11, Kapitel III, § 3., 3.11] und da G nicht zyklisch ist, gilt außerdem $|G/\Phi(G)| \geq p^2$, also $\gamma_2(G) = \Phi(G)$. Wegen $|\gamma_2(G)| = p^2$ ist $\gamma_2(G)$ abelsch.

Wir nehmen an, dass $\gamma_2(G)$ zyklisch ist. Sei $x \in G$ extremal. Nach den Sätzen 2.7 und 2.9 existiert $y \in G$ mit

$$\gamma_2(G) = \langle [x, y]_{\mathfrak{G}} \rangle = \{ [x, y^k]_{\mathfrak{G}} \mid k \in \underline{p^2-1}_0 \},$$

insbesondere gilt $[x, y^p]_{\mathfrak{G}} \neq 1_G$. Wegen $G/\Phi(G) \cong C_p \times C_p$ folgt $y^p \in \gamma_2(G)$ und damit $x \notin C_G(\gamma_2(G))$. Aus $\exp(\gamma_2(G)/\gamma_3(G)) \leq \exp(G/\gamma_2(G))$ (siehe zum Beispiel [11, Kapitel III, § 2., 2.13]) folgt außerdem $cl(G) = 3$. Damit gilt $\gamma_2(G) \cap \mathcal{Z}(G) = \gamma_3(G)$, $|\gamma_3(G)| = p$ und aus 2.9 (iv) erhalten wir $p^3 = |C_G([x, y]_{\mathfrak{G}})| = |C_G(\gamma_2(G))|$. Aus $cl(G) = 3$ folgt weiter

$\mathcal{Z}_2(G) = \gamma_2(G)$, da andernfalls aus $\gamma_2(G) \subset \mathcal{Z}_2(G)$ folgen würde, dass $\mathcal{Z}(G/\mathcal{Z}(G)) = \mathcal{Z}_2(G)/\mathcal{Z}(G)$ zyklisch und $G/\mathcal{Z}(G)$ somit abelsch wäre. Folglich gilt

$$\{g \mid g \in G, |g^G| \leq p\} \stackrel{2.16}{=} \mathcal{Z}_2(G) = \gamma_2(G) \subset C_G(\gamma_2(G)).$$

Somit enthält $C_G(\gamma_2(G))$ auch eine extremale Konjugiertenklasse, ein Widerspruch zu $x \notin C_G(\gamma_2(G))$.

Also gilt $\gamma_2(G) \cong C_p \times C_p$. Wegen $|G/\Phi(G)| = p^2$ existiert ein minimales Erzeugendensystem $\{g, h\}$ von G . Wäre $cl(G) = 2$, so wäre $\gamma_2(G) = \langle [g, h]_{\mathfrak{G}} \rangle$ nach Lemma 2.2 und Bemerkung 2.2.1, ein Widerspruch zu $\gamma_2(G) \cong C_p \times C_p$. Wegen $\gamma_2(G) \leq C_G(\gamma_2(G))$ und $|C_G(\gamma_2(G)) : \gamma_2(G)| = p$ ist $C_G(\gamma_2(G))$ außerdem abelsch. \square

3.24 Beispiel. Sei G eine Gruppe der Ordnung 625 mit $|\gamma_2(G)| = 25$. Dann gilt $\gamma_2(G) \cong C_5 \times C_5$, $cl(G) = 3$ und $C_G(\gamma_2(G))$ ist abelsch nach Beispiel 3.23. Außerdem gilt

$$|\mathcal{Z}_2(G)/\gamma_2(G)| = 1 \quad \text{und} \quad |C_G(\gamma_2(G))/\gamma_2(G)| = 5.$$

Ist dann K ein Körper mit $\text{char } K = 5$, so erhalten wir direkt aus 3.22 und 3.22.2:

$$\begin{aligned} \dim(\mathcal{Z}_2(\mathcal{J}(KG))/\mathcal{Z}_1(\mathcal{J}(KG))) &= 25 \cdot 1 - 1 = 24, \\ \dim(\mathcal{Z}_3(\mathcal{J}(KG))/\mathcal{Z}_2(\mathcal{J}(KG))) &= 25 \cdot 2 - 5 = 45, \\ \dim(\mathcal{Z}_4(\mathcal{J}(KG))/\mathcal{Z}_3(\mathcal{J}(KG))) &= 25 \cdot 2 - 1 = 49, \\ \dim(\mathcal{Z}_5(\mathcal{J}(KG))/\mathcal{Z}_4(\mathcal{J}(KG))) &= 25 \cdot 3 - 5 = 70, \\ \dim(\mathcal{Z}_6(\mathcal{J}(KG))/\mathcal{Z}_5(\mathcal{J}(KG))) &= 25 \cdot 2 = 50, \\ \dim(\mathcal{Z}_7(\mathcal{J}(KG))/\mathcal{Z}_6(\mathcal{J}(KG))) &= 25 \cdot 3 - 5 = 70, \\ \dim(\mathcal{Z}_8(\mathcal{J}(KG))/\mathcal{Z}_7(\mathcal{J}(KG))) &= 25 \cdot 2 = 50, \\ \dim(\mathcal{Z}_9(\mathcal{J}(KG))/\mathcal{Z}_8(\mathcal{J}(KG))) &= 25 \cdot 3 - 5 = 70, \\ \dim(\mathcal{Z}_{10}(\mathcal{J}(KG))/\mathcal{Z}_9(\mathcal{J}(KG))) &= 25 \cdot 2 = 50, \\ \dim(\mathcal{Z}_{11}(\mathcal{J}(KG))/\mathcal{Z}_{10}(\mathcal{J}(KG))) &= 25 \cdot 2 - 1 = 49, \\ \dim(\mathcal{Z}_{12}(\mathcal{J}(KG))/\mathcal{Z}_{11}(\mathcal{J}(KG))) &= 25 \cdot 1 = 25, \\ \dim(\mathcal{Z}_{13}(\mathcal{J}(KG))/\mathcal{Z}_{12}(\mathcal{J}(KG))) &= 25 \cdot 1 - 1 = 24. \end{aligned}$$

Symbolverzeichnis

Im Folgenden listen wir die wesentlichen Notationen dieser Arbeit auf. Dabei geben wir zu jeder dieser eine Kurzdefinition an und verweisen auf die Seite des erstmaligen Erscheinens des jeweiligen Symbols.

Kapitel 1

$\nu(m)$	$\max \{n \mid n \in \mathbb{N}_0, p^n \mid m\}$, Seite 5
\underline{n}	$\{1, \dots, n\}$, Seite 5
M_0	$M \cup \{0\}$, Seite 5
$a * b$	$:= a + b + ab$, Seite 5
$E(A)$	Einheitengruppe von $(A; \cdot)$, Seite 5
$Q(A)$	Einheitengruppe von $(A; *)$, Seite 5
$a^{(n)}$	$\underbrace{a * \dots * a}_n$, Seite 5
a^-	das inverse Element von a bezüglich $*$, Seite 5
$\text{char} K$	Charakteristik von K , Seite 6
$\langle T \rangle_K$	K -Raum Erzeugnis von T , Seite 6
$\text{Aug}_{\mathfrak{B}}(A)$	Augmentationsraum von A bezüglich der Basis \mathfrak{B} , Seite 6
KG	Gruppenalgebra von G über K , Seite 6
$\text{Aug}(KG)$	Augmentationsideal von KG , Seite 6
$\text{Aug}(T)$	$\text{Aug}(KG) \cap \langle T \rangle_K$ für $T \subseteq G$, Seite 6
$\mathcal{J}(A)$	Jacobson-Radikal von A , Seite 7
$N \trianglelefteq G$	N ist Normalteiler von G , Seite 7
$\mathcal{Z}(A)$	Zentrum von A , Seite 8
$\mathcal{K}(G)$	Menge der Konjugiertenklassen von G , Seite 8
$ T $	Mächtigkeit der Menge T , Seite 8
$[g, h]_{\mathfrak{G}}$	(Gruppen)-Kommutator $g^{-1}h^{-1}gh$ von g und h , Seite 8
$[a, b]_{\mathfrak{L}}$	(Lie)-Kommutator $ab - ba$ von a und b , Seite 8
$\gamma_2(G), G'$	Kommutatoruntergruppe von G , Seite 9
$(\gamma_j(G))_{j \in \mathbb{N}}$	Absteigende Zentralreihe der Gruppe G , Seite 9
$(\mathcal{Z}_j(G))_{j \in \mathbb{N}_0}$	Aufsteigende Zentralreihe der Gruppe G , Seite 9
$cl(G)$	Nilpotenzklasse von G , Seite 9
$(\mathcal{L}_j(R))_{j \in \mathbb{N}_0}$	Aufsteigende Zentralreihe der zu R gehörigen Lie-Algebra, Seite 9
$[U, V]_{\mathfrak{G}}$	$\langle [u, v]_{\mathfrak{G}} \mid u \in U, v \in V \rangle$, Seite 9
$[U, V]_{\mathfrak{L}}$	$\langle [u, v]_{\mathfrak{L}} \mid u \in U, v \in V \rangle_K$, Seite 9
$\exp(G)$	Exponent der Gruppe G , Seite 10
$U \oplus W$	Direkte Summe von U und W , Seite 11
$o(g)$	Ordnung von g , Seite 12

D_{2^n}	Diedergruppe der Ordnung 2^n , Seite 12
SD_{2^n}	Semidiedergruppe der Ordnung 2^n , Seite 12
Q_{2^n}	Verallgemeinerte Quaternionengruppe der Ordnung 2^n , Seite 12
g^G	Konjugiertenklasse von g , Seite 13
g^h	$h^{-1}gh$ für Elemente g und h einer Gruppe, Seite 13
$\mathcal{K}_T(G)$	in T enthaltene Konjugiertenklassen, Seite 13
$\mathcal{K}_{T,n}(G)$	in T enthaltene Konjugiertenklassen der Länge n , Seite 13
$\kappa(g)$	$p^{\kappa(g)} = g^G $ für ein Element g einer p -Gruppe G , Seite 13
$\mu(T)$	$\min \{ \kappa(g) \mid g \in T \}$, Seite 13
\equiv	Kongruenz modulo p , Seite 15
$\overset{p}{\equiv}$	
$(a_i)_{i \in \mathbb{N}_0}$	Folge mit $i \mapsto a_i$, Seite 18
$\langle B \rangle_{\mathbb{Z}}$	die von B erzeugte (additive) Gruppe, Seite 18
$\langle B \rangle_{\mathbb{N}_0}$	das von B erzeugte (additive) Monoid, Seite 19
$\langle a \rangle$	die von a erzeugte Untergruppe, Seite 23
$\mathcal{D}_{(l,k,n)}$	$\{ p^{l-n} + sp^{k-n+1} \mid s \in \underline{p^{l+n-k-1} - p^{l-k-1}} \}$, falls $n \leq k$, Seite 25
$\mathcal{D}_{(l,k,n)}$	$\underline{p^l} \setminus \mathcal{Z}_{(l,k,n)}$, falls $n > k$, Seite 25
$\mathcal{Z}_{(l,k,n)}$	$\{ cp^j \mid j \in k - n_0, c \in \underline{p^{l-k}} \}$, falls $n \leq k$, Seite 25
$\mathcal{Z}_{(l,k,n)}$	$\underline{p^{l-n}}$, falls $n > k$, Seite 25
$\psi_{(l,k,n,r)}$	$\underline{p^l} \longrightarrow \mathbb{Q}, m \mapsto \max \{ m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1, m - p^{l-n} + 1, 1 \}$, Seite 25
$m\psi^-$	das vollständige Urbild von m unter ψ , Seite 28
$\psi_{(l,k,n)}$	$\underline{p^l} \longrightarrow \underline{p^l}, m \mapsto \max \{ m - p^{\nu(m)+l-k} + 2, m - p^{l-n} + 1, 1 \}$, Seite 28
$\tilde{\mathcal{D}}_{(l,k,n)}$	$\{ m \mid m \in \underline{p^l} \setminus \{1\}, m\psi_{(l,k,n)}^- = 2 \}$, Seite 28
$\tilde{\mathcal{E}}_{(l,k,n)}$	$\{ m \mid m \in \underline{p^l} \setminus \{1\}, m\psi_{(l,k,n)}^- = 1 \}$, Seite 28
$\tilde{\mathcal{K}}_{(l,k,n)}$	$\{ m \mid m \in \underline{p^l} \setminus \{1\}, m\psi_{(l,k,n)}^- = \emptyset \}$, Seite 28
w^h	$h^{-1}wh$ für Elemente $w \in KG$ und $h \in G$ einer Gruppe G , Seite 31

Kapitel 2

$\gamma_3(G)$	$[\gamma_2(G), G]_{\mathfrak{S}} = [G', G]_{\mathfrak{S}}$, Seite 33
$C_G(g)$	Zentralisator von g in G , Seite 34
C_n	Zyklische Gruppe der Ordnung n , Seite 40
$\omega_a(g, h)$	$a^{-\omega_a(g, h)p^{l-\kappa(g)}} = [g, h]_{\mathfrak{S}}$, Seite 41
$\omega_{(a,g)}$	$\omega_{(a,g)} : G \mapsto \mathbb{Z}/p^{\kappa(g)}\mathbb{Z}, h \mapsto \omega_a(g, h) + p^{\kappa(g)}\mathbb{Z}$, Seite 41
$\overline{\omega_{(a,g)}}$	$\overline{\omega_a(g, \cdot)}$, Seite 41
\mathcal{S}_T	Symmetrische Gruppe auf der Menge T , Seite 41
$C_G(T)$	Zentralisator der Menge T in G , Seite 45
$(g, n)\alpha$	$\min \left\{ \frac{ \gamma_2(G) }{ g^G }, p^n \left(\frac{ \gamma_2(G) }{ \gamma_3(G) } - 1 \right) \right\}$, Seite 51
$\psi_{g,r}$	$\underline{p^l} \rightarrow \mathbb{Q}, m \mapsto \max \{ m - p^{\nu(m)}(p^{l-k} - p^{-r}) + 1, m - p^{l-\kappa(g)} + 1, 1 \}$, Seite 60
\mathcal{Z}_H	$\mathcal{Z}_{(l,k,\mu(H))}$, Seite 67
\mathcal{D}_H	$\mathcal{D}_{(l,k,\mu(H))}$, Seite 67

ψ_H	$\underline{p}^l \longrightarrow \underline{p}^l, m \mapsto \max \{m - p^{\nu(m)+l-k} + 2, m - p^{l-\mu(H)} + 1, 1\}$, Seite 67
$\tilde{\mathcal{D}}_H$	$\tilde{\mathcal{D}}_{(l,k,\mu(H))} = \{m \mid m \in \underline{p}^l \setminus \{1\}, m\psi_H^- = 2\}$, Seite 67
$\tilde{\mathcal{E}}_H$	$\tilde{\mathcal{E}}_{(l,k,\mu(H))} = \{m \mid m \in \underline{p}^l \setminus \{1\}, m\psi_H^- = 1\}$, Seite 67
$\tilde{\mathcal{K}}_H$	$\tilde{\mathcal{K}}_{(l,k,\mu(H))} = \{m \mid m \in \underline{p}^l \setminus \{1\}, m\psi_H^- = \emptyset\}$, Seite 67
$\text{Aut}(G)$	Automorphismengruppe von G , Seite 79
$N \rtimes P$	Inneres semidirektes Produkt von P und N , Seite 79

Kapitel 3

$\Sigma(m)$	$\{(r, s) \mid r, s \in \underline{p-1}_0, m = r + s\}$, Seite 89
$\Phi(G)$	Frattiniuntergruppe von G , Seite 94
$\Xi(m)$	$\{(r, s) \mid r, s \in \underline{p-1}_0, m = r + 2s\}$, Seite 100

Literaturverzeichnis

- [1] Albrecht, A. Die Struktur der Einheitengruppe endlicher kommutativer Gruppenringe, *Diplomarbeit*. Kiel. 1988.
- [2] Bhandari, A. K. und Passi, I. B. S. Lie nilpotency indices of group algebras. *Bull. London Math. Soc.* 24 (1992), 68–70.
- [3] Bovdi, A. und Patay, Z. On the central units of a modular group algebra. *Acta. Sci. Math.* 63 (1997), 71–83.
- [4] Bundschuh, P. *Einführung in die Zahlentheorie*. Springer, Berlin, 2002.
- [5] Cheng, Y. On finite p -groups with cyclic commutator subgroup. *Arch. Math.* 39 (1982), 295–298.
- [6] Coleman, D. B. und Passman, D. S. Units in modular group rings. *Proc. Amer. Math. Soc.* 25 (1970), 510–512.
- [7] Dark, R. S. und Newell, M. L. On conditions for commutators to form a subgroup. *J. London Math. Soc.* 17 (1978), 251–262.
- [8] Du, X. The centers of a radical ring. *Canad. Math. Bull.* 35 (1992), 174–179.
- [9] Fine, N. J. Binomial Coefficients Modulo a Prime. *The Amer. Math. Monthly* 54 (1947), 589–592.
- [10] Finogenov, A. A. Finite p -groups with a cyclic commutator subgroup. *Algebra and Logic* 34.No. 2 (1995), 125–129.
- [11] Huppert, B. *Endliche Gruppen I*. Springer, Berlin, 1967.
- [12] Jennings, S. A. Radical rings with nilpotent associated groups. *Trans. Roy. Soc. Can.* III 49 (1955), 31–38.
- [13] Jennings, S. A. The structure of the group ring of a p -group over a modular field. *Trans. Amer. Math. Soc.* 50.1 (1941), 175–185.
- [14] Karpilovsky, G. *The Jacobson Radical of Group Algebras*. North-Holland, 1987.
- [15] Knoche, H.-G. Über den Frobenius’schen Klassenbegriff in nilpotenten Gruppen. *Math. Z.* 55.1 (1951), 71–83.
- [16] Laue, H. Upper Central Chains in Rings. *Comm. Algebra* 43 (2015), 4705–4710.
- [17] Passman, Donald S. *The algebraic structure of group rings*. John Wiley und Sons, 1977.
- [18] Sandling, R. Units in the modular group algebra of a finite abelian p -group. *J. Pure Appl. Math.* 33 (1984), 337–346.

- [19] Shalev, A. Lie dimension subgroups, Lie nilpotency indices, and the exponent of the group of normalized units. *J. London Math. Soc.* 43 (1991), 23–36.
- [20] Shalev, A. The nilpotency class of the unit group of a modular group algebra I. *Israel J. Math.* 70 (1990), 257–266.
- [21] Shalev, A. The nilpotency class of the unit group of a modular group algebra II. *Israel J. Math.* 70 (1990), 267–277.
- [22] Shalev, A. The nilpotency class of the unit group of a modular group algebra III. *Arch. Math.* 60 (1993), 136–145.
- [23] Theede, M. Über die aufsteigende Zentralreihe von Einheitengruppen modularer Gruppenalgebren, *Diplomarbeit*. Kiel. 2012.
- [24] van der Waerden, B. L. *Algebra ; Band 2*. Springer, Berlin, 1967.
- [25] Wirsing, S. Über Einheitengruppen modularer Gruppenalgebren. *Diss.* Kiel. 2005.

Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit

*Die aufsteigende Zentralreihe in Einheitengruppen modularer Gruppenalgebren
für Klassen metabelscher p -Gruppen*

abgesehen von der Beratung durch den Betreuer meiner Promotion Herrn Prof. Dr. Hartmut Laue in Inhalt und Form selbstständig angefertigt habe und dabei die Regeln guter wissenschaftlicher Praxis der Deutschen Forschungsgemeinschaft eingehalten habe.

Diese Arbeit hat weder ganz noch in Teilen einer anderen Stelle im Rahmen eines Prüfungsverfahrens vorgelegen und wurde weder veröffentlicht noch zur Veröffentlichung eingereicht.

Kiel, den

Mathias Theede