Über Gruppen quasiregulärer Elemente in assoziativen Algebren

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

vorgelegt von
Juliane Hansmann

Kiel, 2015

Erster Gutachter:	Prof. Dr. Hartmut Laue
Zweiter Gutachter:	Prof. Dr. Richard Weidmann
Tag der mündlichen Prüfung:	11. Dezember 2015
Zum Druck genehmigt:	11. Dezember 2015
gez.	Prof. Dr. Wolfgang Duschl, Dekan

Zusammenfassung

In der vorliegenden Arbeit untersuchen wir die Struktur der Gruppe quasiregulärer Elemente in frei nilpotenten Algebren. Ein Element einer assoziativen Algebra A heißt quasiregulär, wenn es bezüglich der auf A definierten Verknüpfung $a * b := a + b + ab$ invertierbar ist. Wir bezeichnen mit X eine (zumeist endliche) nichtleere Menge und mit $N = N_{K,X,k}$ die frei nilpotente K-Algebra der Klasse k über X. Dabei ist K ein kommutativer unitärer Ring, oftmals wählen wir $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ für ein $c \in \mathbb{N}_{>1}$.

Als Spezialfall bestimmen wir für $|X| = 1$, also in dem Fall, dass $(N, *)$ abelsch ist, den Isomorphietyp dieser Gruppe. Dabei stellt sich heraus, dass ein Großteil der Strukturinformationen an geeignet gewählten Intervallzerlegungen von $\{1, \ldots, k\}$ abgelesen werden kann. Dieses Hilfsmittel verwenden wir erneut, um auch ausgehend von größeren Mengen Strukturinformationen für die von X erzeugte Untergruppe $\langle X \rangle_*$ im Fall eines endlichen Grundrings K zu erhalten: Nach dem Satz von Magnus [Mag35] wissen wir, dass die von X erzeugte Gruppe in der Potenzreihenalgebra frei über der Menge X ist. Für den Fall $K = \mathbb{Z}$ zeigen wir in dieser Arbeit, dass $\langle X \rangle_*$ frei nilpotent von der Klasse k über X ist. Ist nun K ein Faktorring von $\mathbb{Z}$, so ist die von X erzeugte Untergruppe erneut in einer geeignet gewählten Gruppenklasse frei über X. Dazu betrachten wir die Klasse der nilpotenten Gruppen von der Klasse höchstens k, bei denen wir, in Abhängigkeit von K, Bedingungen an die Exponenten der absteigenden Zentralreihe stellen. Ein weiteres wichtiges Hilfsmittel bei der Betrachtung der von X erzeugten Gruppe in N sind die Elementarkommutatoren, wie sie beispielsweise von M. Hall in [Hal76, Chapter 11] definiert werden.

Die Untersuchung des von der Kommutatoruntergruppe N' erzeugten assoziativen Ideals ermöglicht es uns, die Gruppe $(N, *)$ semidirekt zu zerlegen. Zudem beschreiben wir die Gruppe $(N, *)$ für die Nilpotenzklassen $k = 2$ und $k = 3$, indem wir die Gruppe so zerlegen, dass wir jeden Faktor entweder als bereits bekannt identifizieren oder ihn durch Erzeuger und Relationen beschreiben. Hierbei wird deutlich, wie schnell die Komplexität mit wachsender Nilpotenzklasse zunimmt.

Abstract

In this thesis, we study the group of quasi-regular elements in free nilpotent algebras. An element of an associative algebra A is called quasi-regular if it is invertible with respect to the operation $a * b := a + b + ab$ on A. We denote by X an (in most cases finite) non-empty set and by $N = N_{K,X,k}$ the free nilpotent algebra of class k, freely generated by X, where K denotes a commutative unitary ring. We often choose K as $K = \mathbb{Z}$ or $K = \mathbb{Z}/c\mathbb{Z}$ for some $c \in \mathbb{N}_{>1}$.

We consider the special case $|X| = 1$, i.e., $(N, *)$ is abelian, and we determine the isomorphism type of $(N, *)$. In doing so, we find that most of the structural information is encoded in a special partition of the interval $\{1, \ldots, k\}$. This suitably chosen partition also turns out to be useful to determine the structure of the subgroup $\langle X \rangle_*$ of $(N, *)$: The Magnus theorem [Mag35] states that the subgroup generated by X in the algebra of formal power series is a free group, freely generated by X. In this thesis, we show that for $K = \mathbb{Z}$ the group $\langle X \rangle_*$ generated by X in N is free nilpotent of class k and X is a nilpotently free generating set for $\langle X \rangle_*$. Passing on to the case where K is a quotient ring of $\mathbb{Z}$, we find that the group $\langle X \rangle_*$ is also freely generated by X in a suitable class of groups. For that purpose, we consider the class of nilpotent groups of class at most k where we have additional conditions on the exponent of the groups in the lower central series, depending on K. An additional tool for the examination of the subgroup of N which is generated by X are the basic commutators as they are, for instance, defined by M. Hall in [Hal76, Chapter 11].

The study of the associative ideal generated by the derived subgroup N' enables us to split the group $(N, *)$ into a semidirect product. For $k = 2$ and $k = 3$, we determine the isomorphism type of $(N, *)$ by splitting the group into subgroups whose isomorphism type we already know or which we can describe in terms of generators and relations. During these calculations we clearly see how the level of complexity rises with increasing nilpotency class.

Inhaltsverzeichnis

Einleitung

Die quasiregulären Elemente in Algebren werden das erste Mal 1942 von Sam Perlis in [Per42] definiert. In diesem Artikel betrachtet er zunächst unitäre assoziative Algebren A und beweist die Gleichheit

$$N(A) = \{h \in A \mid \forall g \in E(A) : g + h \in E(A)\},$$

wobei $N(A)$ das Nil-Radikal und $E(A)$ die Einheitengruppe von A bezeichnet. Sein Ziel ist es, dieses Resultat auf Algebren zu erweitern, die nicht notwendigerweise ein Einselement besitzen. Zu diesem Zweck definiert er ein Element $x \in A$ als *quasiregulär*, falls es ein $y \in A$ gibt mit

$$x + xy + y = 0$$

und nennt y in diesem Fall *quasi-invers* zu x. Mit Hilfe der so definierten Quasiregularität beschreibt er das Nil-Radikal einer assoziativen Algebra A über einem Körper F als

$$N(A) = \{r \in A \mid \forall x \in Q(A)\, \forall \alpha \in F : x + \alpha r \in Q(A)\},$$

wobei $Q(A)$ die Menge der quasiregulären Elemente von A bezeichnet.

Diese Beschreibung des Nil-Radikals greift Reinhold Baer 1943 in [Bae43, Abschnitt 10] für Ringe auf. Er definiert dort ein Rechtsideal eines Ringes als *quasiregulär*, falls jedes Element in diesem quasiregulär ist. Er zeigt, dass die Summe aller quasiregulären Rechtsideale wieder ein quasiregulläres Rechtsideal ist und es modulo diesem keine nichttrivialen quasiregulären Rechtsideale gibt. In diesem Artikel wird auch die Formel zur Berechnung des Quasi-Inversen für nilpotente Elemente (vergleiche Lemma 1.2 (c)) angegeben.

Erst Nathan Jacobson hebt 1945 in [Jac45] in klarer Weise hervor, dass außer der von Perlis und Baer betrachteten (nur rechtsseitigen) Quasiregularität auch die linksseitige Quasiregularität eines Elementes $x \in A$, das heißt

$$x + yx + y = 0 \quad \text{für ein } y \in A,$$

notwendig ist. Er untersucht das von Baer als Summe aller quasiregulären Rechtsideale definierte Rechtsideal J in einem Ring, indem er analog das Linksideal der Summe aller linksquasiregulären Linksideale bildet und anschließend deren Gleichheit beweist. Damit ist das von ihm definierte Radikal J ein beidseitiges Ideal, das heute als *Jacobson-Radikal* bekannt ist. Des Weiteren nennt er beidseitig quasiregulläre Elemente *quasiregulär* und stellt fest, dass für quasiregulläre Elemente die rechten und linken Quasi-Inversen übereinstimmen. Damit sind alle Elemente von J schon quasiregulär.

Ist nun K ein kommutativer unitärer Ring und A eine assoziative K-Algebra, so definiert

$$* : A \times A \to A,\ a * b := a + b + ab$$

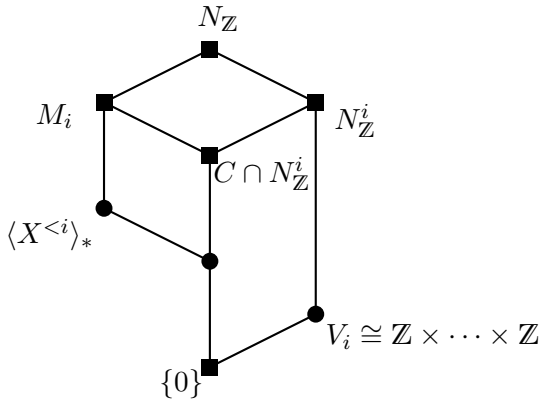
eine assoziative Verknüpfung auf A mit neutralem Element 0, und die bezüglich $*$ invertierbaren Elemente sind genau die quasiregulären Elemente, wie sie von Jacobson definiert wurden. Insbesondere ist also das Jacobson-Radikal mit dieser Verknüpfung eine Gruppe. Das Ideal $J \subseteq A$ ist sogar maximal mit dieser Eigenschaft.

Der Satz von Magnus [Mag35] besagt, dass die von der Menge X bezüglich $*$ erzeugte Untergruppe der Potenzreihenalgebra P im Fall des Koeffizientenrings $K = \mathbb{Z}$ frei über X ist. In Satz 2.14 gelingt es uns, diese Aussage unabhängig von K zu beweisen:

In P ist die von X bezüglich $*$ erzeugte Untergruppe frei über X.

In dieser Arbeit sei X eine endliche nichtleere Menge und $k \in \mathbb{N}$. Wir betrachten die $*$-Gruppe der frei nilpotenten Algebra N_K über X der Klasse k über einem kommutativen unitären Ring K (vergleiche Bemerkung 1.20). Dabei betrachten wir insbesondere den Fall, dass K ein Faktorring von $\mathbb{Z}$ ist. Wir werden einige Zerlegungen der Gruppe $(N_K, *)$ angeben und in diesem Zusammenhang auch das von der Kommutatoruntergruppe N_K' erzeugte Ideal C beschreiben. Anschließend betrachten wir die von X erzeugte Untergruppe $\langle X \rangle_*$.

Wir betrachten zunächst den Spezialfall $K = \mathbb{Z}$. Sei X endlich und $i \geq \left\lceil \frac{k+1}{2} \right\rceil$ und $\langle X^{<i} \rangle_*$ die von den Worten bis zur Länge i erzeugte Untergruppe von $(N_\mathbb{Z}, *)$. Wir zeigen (Satz 3.3, Bemerkung 3.18):



Sei $M_i := (C \cap N_\mathbb{Z}^i) * \langle X^{<i} \rangle$. Dann ist M_i ein Normalteiler von $(N_\mathbb{Z}, *)$, der ein frei abelsches Komplement V_i in $N_\mathbb{Z}$ besitzt. Dabei ist die Operation von V_i auf M_i durch

$$m^{(v)} = m + [m, v]$$

für alle $m \in M_i$ und $v \in V_i$ gegeben.

Wir geben also eine semidirekte Zerlegung der Gruppe an, bei der wir sowohl die Operation als auch den Faktor V_i gut beschreiben können. Der Normalteiler M_i hingegen ist komplizierter in seiner Struktur.

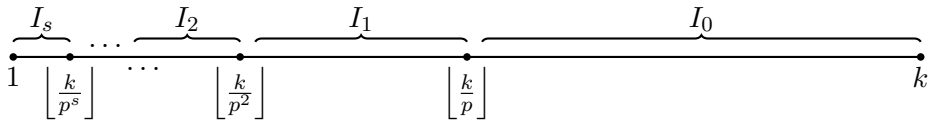
Das von $N_\mathbb{Z}'$ erzeugte assoziative Ideal C können wir explizit als Schnitt über die Kerne geeigneter K-linearer Augmentationsabbildungen angeben (vergleiche Definition 3.5), während es uns in der Untergruppe $\langle X^{<i} \rangle_*$ nur gelingt, die von X erzeugte Untergruppe zu beschreiben (Satz 3.48 (b)):

Die von X erzeugte Gruppe in N ist frei nilpotent über X von der Klasse k.

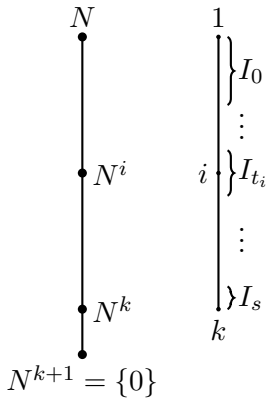
Dieses Resultat klärt zumindest einen Teil der Struktur von $\langle X^{<i} \rangle_*$ und ist zudem eine Fortsetzung des Freiheitsbeweises von Magnus.

Verlassen wir den Fall $K = \mathbb{Z}$ und gehen zu echten Faktorringen K über, so ist die betrachtete Algebra N_K endlich. In Satz 1.38 reduzieren wir die Fragen auf Betrachtungen des Falls eines Faktorringes K von Primzahlpotenzmächtigkeit.

Sei nun also $K = \mathbb{Z}/p^l\mathbb{Z}$ für eine Primzahl p und ein $l \in \mathbb{N}$. Wir definieren auf $\underline{k}$ $(= \{1, \ldots, k\})$ eine Intervallzerlegung wie folgt (vergleiche Definition 1.16):



Diese wirkt sich wie folgt auf die Elementordnungen in $(N_{\mathbb{Z}/p^l\mathbb{Z}}, *)$ aus (vergleiche Lemma 1.35):



Es sei $i \in \underline{k}$, $i \in I_{t_i}$. Dann gilt für alle $a \in N_{\mathbb{Z}/p^l\mathbb{Z}}$:

$$a \in N^i_{\mathbb{Z}/p^l\mathbb{Z}} \Rightarrow o(a) \mid p^{l+t_i}$$

Betrachten wir nun den Spezialfall, dass die Menge X einelementig – und damit $(N_{\mathbb{Z}/p^l\mathbb{Z}}, *)$ abelsch – ist, so sehen wir unmittelbar, wie sich die Intervallzerlegung nicht nur auf die Elementordnungen in $(N_{\mathbb{Z}/p^l\mathbb{Z}}, *)$ sondern damit auch auf die Gruppenstruktur auswirkt.

Sei $|X| = 1$. Dann gilt

$$(N_{\mathbb{Z}/p^l\mathbb{Z}}, *) \cong \mathcal{C}_{p^{l-1}}^{\left\lfloor \frac{k}{p} \right\rfloor} \times \bigtimes_{t=0}^{s} \mathcal{C}_{p^{l+t}}^{(|I_t| - |I_{t+1}|)}.$$

Dieses Resultat zeigen wir für eine größere Klasse von Grundringen K – unter anderem auch für endliche Körper – in Satz 3.33.

Auch in $N_{\mathbb{Z}/p^l\mathbb{Z}}$ lässt sich das von $N'_{\mathbb{Z}/p^l\mathbb{Z}}$ erzeugte assoziative Ideal C als Schnitt über die Kerne geeigneter K-linearer Augmentationsabbildungen angeben (vergleiche Definition 3.5) und es gelingt uns, die Untergruppe $\langle X \rangle_*$ zu beschreiben. Dazu definieren wir zunächst für alle Tupel $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_k) \in \mathbb{N}^k$:

Sei $\mathfrak{N}_{n,k,\varepsilon}$ die Klasse der nilpotenten Gruppen $\mathcal{G}$ mit höchstens n Erzeugern, von der Nilpotenzklasse höchstens k und bei denen für alle $i \in \underline{k}$ gilt:

Der Exponent von $\gamma_i(\mathcal{G})$ teilt ε_i.

Es ist nicht schwer einzusehen, dass es in dieser Klasse ein freies Objekt gibt (Satz 3.39), welches wir mit $\mathcal{N}_{n,k,\varepsilon}$ bezeichnen. Wir zeigen in Satz 3.48 (c):

Für alle $i \in \underline{k}$ sei $t_i \in \underline{s}_0$ mit $i \in I_{t_i}$. Dann gilt in $N_{\mathbb{Z}/p^l\mathbb{Z}}$

$$\langle X\rangle_* \cong \mathcal{N}_{n,k,(p^{l+t_1},\ldots,p^{l+t_k})}.$$

Neben dieser abstrakten Beschreibung der Gruppe $\langle X\rangle_*$ erhalten wir – wie im Fall der frei nilpotenten Gruppe – eine eindeutige Darstellung der Elemente durch Elementarkommutatoren, indem wir die zugelassenen Exponentenbereiche gemäß ihrer Elementordnungen einschränken. Insbesondere können wir damit die Mächtigkeit von $\langle X\rangle_*$ berechnen (μ bezeichnet hier die Möbiusfunktion):

$$|\langle X\rangle_*| = \prod_{i=1}^{k}(p^{l+t_i})^{n_i} \quad \textit{mit} \quad n_i = \frac{1}{i}\sum_{d|i}\mu(d)n^{\frac{i}{d}}.$$

Die Ordnung der von X erzeugten Gruppe hängt also neben $|K| = p^l$ und der Nilpotenzklasse k auch von den Zahlen n_i für alle $i \in \underline{k}$ ab, die in den Witt'schen Dimensionsformeln in der Theorie der freien Lie-Algebren bereits auftreten.

Zusammenfassend erhalten wir für die von X erzeugte Untergruppe in P, $N_{\mathbb{Z}}$ und $N_{\mathbb{Z}/p^l\mathbb{Z}}$:

In P: $\langle X\rangle_*$ ist frei über X.

In $N_{\mathbb{Z}}$: $\langle X\rangle_*$ ist frei nilpotent über X.

In $N_{\mathbb{Z}/p^l\mathbb{Z}}$: $\langle X\rangle_*$ ist frei in $\mathfrak{N}_{n,k,\varepsilon}$.

Diese und einige weitere Resultate in dieser Arbeit kommen ohne die Endlichkeit der Menge X aus.

Versuchen wir nun, die obige Zerlegungsaussage auf den Fall $K = \mathbb{Z}/p^l\mathbb{Z}$ zu übertragen, so sehen wir, dass dies nur unter der Zusatzvoraussetzung $p > k$ gelingt:

Sei $p > k$ und $M_i := (C \cap N^i) * \langle X^{<i}\rangle$. Dann ist M_i ein Normalteiler von $(N, *)$, der ein Komplement

$$V_i \cong (K,+) \times \cdots \times (K,+)$$

in N besitzt. Dabei ist die Operation von V_i auf M_i durch

$$m^{(v)} = m + [m, v]$$

für alle $m \in M_i$ und $v \in V_i$ gegeben.

Auch hier fällt die Analyse des Normalteilers M_i schwer.

Im letzten Teil dieser Arbeit beschreiben wir die Gruppe $(N_K, *)$ für die Nilpotenzklassen $k = 2$ (Satz 4.4) und $k = 3$ (Satz 4.14) in dem Fall, dass K ein Faktorring von $\mathbb{Z}$ ist. Wir zerlegen die Gruppe so in Untergruppen, dass wir jede entweder als bereits bekannt erkennen oder sie zumindest durch Erzeuger und Relationen beschreiben können. Hierbei wird deutlich, wie schnell die Komplexität mit wachsender Nilpotenzklasse zunimmt.

Bedanken möchte ich mich ganz herzlich bei Herrn Laue für die Betreuung dieser Arbeit und die vielen Gelegenheiten meine Überlegungen vorstellen zu können. Ebenfalls bedanken möchte ich mich bei allen Mitgliedern des Oberseminars Algebrentheorie für die vielen anregenden Diskussionen. Mein Dank gilt auch meinen kritischen Lesern Mathias, Christian, Markus, Simon und Patrick.

Ebenfalls bedanken möchte ich mich an dieser Stelle bei allen Mitarbeitern des Mathematischen Seminars der Uni in Kiel für die großartige Arbeitsatmosphäre und ganz besonders bei Herrn Heber, Herrn Müller und Herrn Weiß, die mir in den vergangenen Jahren Stellen zur Verfügung gestellt haben.

Danke, Gunnar.

1 Grundlagen

In diesem Kapitel wollen wir die Grundlagen für die wesentlichen Erkenntnisse dieser Arbeit schaffen. Dazu führen wir zunächst die $*$-Verknüpfung auf Algebren ein und untersuchen sie auf Zusammenhänge zur Algebrenstruktur. Anschließend betrachten wir diese Verknüpfung im Spezialfall der Potenzreihenalgebra P und der frei nilpotenten Algebra N, die einem Großteil der Überlegungen im zweiten Kapitel zu Grunde liegt. Dabei werden wir sehen, dass wir im Fall einer Charakteristik $\neq 0$ des Grundringes K mit Hilfe einiger zahlentheoretischer Aussagen schon viel über $*$-Elementordnungen in N aussagen können. Zudem führen wir in diesem Kapitel das Konzept der Elementarkommutatoren in Gruppen und elementaren Lie-Klammern in assoziativen Algebren ein und untersuchen sie im Spezialfall der Algebren P und N auf Zusammenhänge. Im letzten Teil dieses Kapitels befassen wir uns mit Zerlegungen in Gruppen und deren Anwendungen im Fall der auf- und absteigenden Zentralreihe.

In diesem Kapitel sei stets K ein kommutativer unitärer Ring; insbesondere gelte $0_K \neq 1_K$.

1.1 Quasiregularität

Wir wollen nun auf einer gegebenen assoziativen K-Algebra eine weitere Verknüpfung definieren und diese auf erste Eigenschaften untersuchen. Viele der Aussagen dieses Abschnitts finden sich bereits in meiner Diplomarbeit [Han12].

Es sei in diesem Abschnitt stets A eine assoziative K-Algebra.

Definition und Bemerkung 1.1 Wir definieren die Verknüpfung $*$ auf A durch

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

für alle $a, b \in A$. Es ist $(A, *)$ ein Monoid mit neutralem Element 0_A. Sind $n \in \mathbb{N}$ und $a, a_1, \ldots, a_n \in A$, so setzen wir

$$a^{(n)} := \underbrace{a * \ldots * a}_{n} \quad \text{und} \quad \overset{n}{\underset{i=1}{\bigstar}} a_i := a_1 * \ldots * a_n.$$

Ist $a \in A$ bezüglich $*$ in A invertierbar, so nennen wir a quasiregulär. Das $*$-Inverse bezeichnen wir mit a^-. Wir setzen

$$Q(A) := \{a \in A \mid a \text{ ist quasiregulär}\}.$$

Ist $a \in Q(A)$ und $n \in \mathbb{N}$ so setzen wir $a^{(-n)} := (a^-)^{(n)}$.

Lemma 1.2 (a) Sei $B \subseteq A$. Dann stimmt der Zentralisator von B in A mit dem Monoid-Zentralisator von B in $(A, *)$ überein, es gilt also

$$\{a \in A \mid \forall b \in B : ab = ba\} = \{a \in A \mid \forall b \in B : a * b = b * a\}.$$

Insbesondere stimmen die Zentren der Algebra A und des Monoids $(A, *)$ überein und $(A, *)$ ist genau dann kommutativ, wenn A kommutativ ist.

(b) Sei $a \in Q(A)$. Dann gilt $aa^- = a^-a$ und für alle $l \in \mathbb{N}$

$$a^- = \sum_{i=1}^{l}(-a)^i + (-a)^l a^- = \sum_{i=1}^{l}(-a)^i + a^-(-a)^l.$$

(c) Sei $a \in A$ nilpotent, etwa $a^{k+1} = 0_A$ für ein $k \in \mathbb{N}_0$. Dann ist $a \in Q(A)$ und es gilt

$$a^- = \sum_{i=1}^{k}(-a)^i.$$

Ist insbesondere A nil, so ist $(A, *)$ eine Gruppe.

(d) Sind $n \in \mathbb{N}_0$ und $a_1, \ldots, a_n \in A$, so ist

$$\overset{n}{\underset{i=1}{\bigstar}} a_i = \sum_{j=1}^{n} \sum_{1 \le i_1 < \cdots < i_j \le n} a_{i_1} \ldots a_{i_j}.$$

(e) Sei $a \in A$ und $n \in \mathbb{N}_0$. Dann ist

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

(f) Sei $a \in A$ nilpotent, etwa $a^{k+1} = 0_A$ für ein $k \in \mathbb{N}_0$. Dann gilt für alle $n \in \mathbb{N}$

$$a^{(-n)} = \sum_{i=1}^{k}(-1)^i \binom{n+i-1}{i} a^i.$$

Beweis. (a) Sei $a \in A$ und $b \in B$. Dann gilt $a * b - b * a = ab - ba$. Daraus folgt (a).
(b) Sei $a \in Q(A)$. Mit $a * a^- = 0_A = a^- * a$ folgt $aa^- = a^-a$ aus (a). Damit genügt es, die erste Gleichheit zu beweisen. Es gilt mit $0_A = a * a^- = a + a^- + aa^-$ die Behauptung für $l = 1$ und induktiv für $l > 1$

$$a^- = -a - aa^- \overset{\text{I.V.}}{=} -a - a\left(\sum_{i=1}^{l-1}(-a)^i + (-a)^{l-1}a^-\right) = \sum_{i=1}^{l}(-a)^i + (-a)^l a^-.$$

(c) Dies folgt unmittelbar aus (b).
(d) Wir zeigen die Behauptung mit Induktion nach n. Dabei ist für $n = 0$ und $n = 1$ die

Aussage klar. Seien $n > 1$ und $a_1, \ldots, a_n \in A$. Dann gilt

$$\begin{aligned}
\overset{n}{\underset{i=1}{\bigstar}} a_i &\overset{\text{I.V.}}{=} \left(\sum_{j=1}^{n-1} \sum_{1 \le i_1 < \cdots < i_j \le n-1} a_{i_1} \ldots a_{i_j} \right) * a_n \\
&= \sum_{j=1}^{n-1} \sum_{1 \le i_1 < \cdots < i_j \le n-1} a_{i_1} \ldots a_{i_j} + a_n + \left(\sum_{j=1}^{n-1} \sum_{1 \le i_1 < \cdots < i_j \le n-1} a_{i_1} \ldots a_{i_j} \right) a_n \\
&= \sum_{j=1}^{n} \sum_{1 \le i_1 < \cdots < i_j \le n} a_{i_1} \ldots a_{i_j}.
\end{aligned}$$

(e) Dies folgt aus (d) mit $a = a_1 = \cdots = a_n$.
(f) Wir zeigen diese Aussage induktiv nach n. Die Aussage für $n = 1$ finden wir in (c). Für $n > 1$ gilt mit (c)

$$\begin{aligned}
a^{(-n)} = a^{(-n+1)} * a^{-} &\overset{\text{I.V.}}{=} \left(\sum_{i=1}^{k} (-1)^i \binom{n+i-2}{i} a^i \right) * \left(\sum_{i=1}^{k} (-1)^i a^i \right) \\
&= \sum_{i=1}^{k} (-1)^i \left(\binom{n+i-2}{i} + 1 \right) a^i + \left(\sum_{i=1}^{k} (-1)^i \binom{n+i-2}{i} a^i \right) \left(\sum_{i=1}^{k} (-1)^i a^i \right) \\
&= \sum_{i=1}^{k} (-1)^i \left(\binom{n+i-2}{i} + 1 \right) a^i + \sum_{j=1}^{k} \sum_{i=1}^{k} (-1)^{j+i} \binom{n+j-2}{j} a^{j+i} \\
&\overset{a^{k+1}=0}{=} \sum_{i=1}^{k} (-1)^i \left(\binom{n+i-2}{i} + 1 \right) a^i + \sum_{i=1}^{k} (-1)^i \left(\sum_{j=1}^{i-1} \binom{n+j-2}{j} \right) a^i \\
&= \sum_{i=1}^{k} (-1)^i \left(\sum_{j=0}^{i} \binom{n+j-2}{j} \right) a^i \\
&= \sum_{i=1}^{k} (-1)^i \binom{n+i-1}{i} a^i.
\end{aligned}$$

□

Wir wollen uns nun mit dem Zusammenhang zwischen der K-Algebren-Struktur und der $*$-Struktur beschäftigen.

Bemerkung 1.3 Sei $A = Q(A)$ und T ein Teilring von A.

(a) $(T, *)$ ist ein Monoid.

(b) Ist T nil, so ist T eine Untergruppe von $(A, *)$.

(c) Ist T ein Rechts- oder Linksideal, so ist T eine Untergruppe von $(A, *)$.

(d) Ist T ein Ideal, so ist T eine Normalteiler von $(A, *)$. Insbesondere ist A^i für alle $i \in \mathbb{N}$ ein Normalteiler von $(A, *)$.

(e) Für alle $i \in \mathbb{N}$ ist $A^i/A^{i+1} \subseteq Z(A/A^{i+1})$.

(f) Ist A eine nilpotente Algebra mit $A^{k+1} = \{0_A\}$ für ein $k \in \mathbb{N}$, so ist $(A, *)$ eine nilpotente Gruppe der Klasse höchstens k.

Beweis. (a) Dies gilt nach Bemerkung 1.1.
(b) Sei T nil. Nach (a) ist $(T, *)$ ein Monoid. Sei $a \in T$ und $k \in \mathbb{N}$ mit $a^{k+1} = 0_A$. Dann gilt $a^- \overset{1.2(c)}{=} \sum_{i=1}^{k} (-a)^i \in T$.
(c) Sei o.B.d.A. T ein Rechtsideal. Dann ist nach (a) $(T, *)$ ein Monoid und es gilt $a^- \overset{1.2(b)}{=} -a - aa^- \in T$ für alle $a \in T$.
(d) Sei T ein Ideal von A. Nach (c) ist T eine $*$-Untergruppe von A. Zudem gilt für alle $t \in T$ und $a \in A$

$$a^- * t * a = t + a^- t + ta + a^- ta \in T.$$

(e) Für alle $a \in A^i$ und $b \in A$ ist $ab + A^{i+1} = A^{i+1} = ba + A^{i+1}$. Die Behauptung folgt mit 1.2 (a).
(f) Sei A nilpotent und $k \in \mathbb{N}$ mit $A^{k+1} = \{0_A\}$. Dann ist $A, A^2, \ldots, A^{k+1}(= \{0_A\})$ nach (e) eine absteigende Zentralkette in A und damit ist $(A, *)$ eine nilpotente Gruppe der Klasse höchstens k. □

Bemerkung 1.4 (a) Sei I ein Rechts- beziehungsweise Linksideal von A und $a \in Q(A)$. Dann ist

$$I * a = I + a \text{ beziehungsweise } a * I = a + I.$$

(b) Sei $A = Q(A)$, I ein Ideal von A und U eine $*$-Untergruppe von A. Dann ist auch $I + U$ eine $*$-Untergruppe von A.

Beweis. (a) Sei o.B.d.A I ein Linksideal. Es genügt $I = \{i + ai \mid i \in I\}$ zu zeigen. Dabei gilt $i + ai \in I$ für alle $i \in I$. Sei nun $j \in I$. Wir setzen $i := a^- * (j + a)$. Dann gilt

$$\begin{aligned} i = a^- + j + a + a^- j + a^- a = j + a^- j \in I \text{ und} \\ i + ai = a * i - a = a * a^- * (j + a) - a = j. \end{aligned}$$

Es folgt $I = \{i + ai \mid i \in I\}$ und damit die Behauptung.
(b) Nach Bemerkung 1.3 (d) ist I ein $*$-Normalteiler von A. Es folgt $I + U = I * U$ mit (a), also ist $I + U$ eine $*$-Untergruppe von A. □

Lemma 1.5 Sei U ein Teilmonoid von $(A, *)$, I ein Rechts- oder Linksideal von A und $i \in \mathbb{N}$ mit $A^i \cap I \subseteq U$. Ist $a \in U + (A^i \cap I)$, so ist $a \in U + (A^j \cap I)$ für alle $j \geq i$.
Ist insbesondere A nilpotent, so folgt $a \in U$ und damit $U + (A^i \cap I) = U$.

Beweis. Sei o.B.d.A. I ein Linksideal. Wir zeigen die Behauptung induktiv nach j.
Für $j = i$ gilt die Aussage nach Voraussetzung. Sei $j > i$ und es gelte $a \in U + (A^{j-1} \cap I)$.

Sei $c \in A^{j-1} \cap I$ mit $a - c \in U$. Dann ist $ac - c^2 \in A^j \cap I$ und nach Voraussetzung ist $c \in A^i \cap I \subseteq U$. Damit folgt

$$a = a - c + c + ac - c^2 - ac + c^2 = \underbrace{(a-c) * c}_{\in U} - \underbrace{(ac - c^2)}_{\in A^j \cap I} \in U + \left(A^j \cap I\right).$$

□

Wir haben auf der Menge A mehrere Verknüpfungen, bezüglich derer wir Erzeugnisse betrachten wollen. Dabei verwenden wir die folgenden Notationen:

Bezeichnungen 1.6 Sei $B \subseteq A$. Es bezeichne

$\langle B \rangle_K$ den von B erzeugten K-Teilraum von A,
$\langle B \rangle_{\mathbb{Z}}$ die von B erzeugte additive Gruppe in A und
$\langle B \rangle_{\mathfrak{A}^K}$ die von B erzeugte K-Teilalgebra von A.

Ist $B \subseteq Q(A)$, so sei

$\langle B \rangle_*$ die von B erzeugte Untergruppe von $(A, *)$.

Definition und Bemerkung 1.7 Sei $B \subseteq Q(A)$ mit $B^2 = \{0_A\}$. Dann gilt

$$+_{|B \times B} = *_{|B \times B}$$

für die eingeschränkten Verknüpfungen auf B und es folgt $\langle B \rangle_{\mathbb{Z}} = \langle B \rangle_*$. In diesem Fall setzen wir

$$\langle B \rangle := \langle B \rangle_{\mathbb{Z}}.$$

Lemma 1.8 Sei U eine $*$-Untergruppe von A. Dann gilt:

(a) (M. Sowa, T. Sohr) Ist $2U \subseteq U$, so ist $U = -U$.

(b) Ist U additiv abgeschlossen, so ist U ein Teilring von A.

(c) Ist U multiplikativ abgeschlossen, so gilt

$$U + U \subseteq U + \langle U^n \rangle_{\mathbb{Z}}$$

für alle $n \in \mathbb{N}$. Ist insbesondere U als Teilmenge der Algebra A nilpotent, so ist U ein Teilring von A.

Beweis. (a) Es gelte $2U \subseteq U$. Sei $u \in U$. Dann gilt

$$-u = u^- + uu^- = u + 2u^- + 2uu^- = u * 2u^- \in U$$

und damit $-U = U$.
(b) Sei U additiv abgeschlossen. Dann ist $(U, +)$ eine Gruppe nach (a). Weiter gilt $uv = u * v - u - v \in U$ für alle $u, v \in U$. Damit ist U ein Teilring von A.
(c) Sei U multiplikativ abgeschlossen. Wir zeigen

$$\forall u, v \in U \, \forall n \in \mathbb{N} \, \exists w_n \in \langle U^n \rangle_{\mathbb{Z}} : \, u + v + w_n \in U.$$

Seien $u, v \in U$. Für $n = 1$ ist dies klar mit $w_1 := uv \in U$. Sei nun $n \in \mathbb{N}_{>1}$ und induktiv gebe es $w_{n-1} \in \langle U^{n-1} \rangle_{\mathbb{Z}}$ mit $u + v + w_{n-1} \in U$. Es seien $m \in \mathbb{N}$ und $u_1, \ldots, u_m \in U^{n-1}$ sowie $\sigma : \underline{m} \to \{-1, 1\}$ mit $w_{n-1} = \sum_{i=1}^{m} (i\sigma) u_i$. Wir setzen $r := \left(\bigstar_{i=1}^{m} u_i^{(-i\sigma)} \right) + w_{n-1}$. Es gilt

$$\begin{aligned} r &\overset{1.2(d)}{=} \sum_{j=1}^{m} \sum_{1 \le i_1 < \cdots < i_j \le m} u_{i_1}^{(-i_1\sigma)} \ldots u_{i_j}^{(-i_j\sigma)} + w_{n-1} \\ &= \sum_{j=2}^{m} \sum_{1 \le i_1 < \cdots < i_j \le m} u_{i_1}^{(-i_1\sigma)} \ldots u_{i_j}^{(-i_j\sigma)} + \sum_{i=1}^{m} \left(u_i^{(-i\sigma)} + (i\sigma) u_i \right) \\ &\overset{1.2(c)}{=} \sum_{j=2}^{m} \sum_{1 \le i_1 < \cdots < i_j \le m} \underbrace{u_{i_1}^{(-i_1\sigma)} \ldots u_{i_j}^{(-i_j\sigma)}}_{\in U^n} + \sum_{\substack{i=1 \\ i\sigma=1}}^{m} \sum_{j=2}^{k} (-1)^j \underbrace{u_i^j}_{\in U^n} \in \langle U^n \rangle_{\mathbb{Z}}. \end{aligned}$$

Weiter sei

$$w_n := r - u w_{n-1} - v w_{n-1} - w_{n-1}^2 + ur + vr + w_{n-1} r \in \langle U^n \rangle_{\mathbb{Z}}.$$

Dann gilt

$$\begin{aligned} u + v + w_n &= (u + v + w_{n-1}) * (-w_{n-1} + r) \\ &= (u + v + w_{n-1}) * \left(\bigstar_{i=1}^{m} u_i^{(-i\sigma)} \right) \in U. \end{aligned}$$

Ist nun U nilpotent, so ist $\langle U^k \rangle_{\mathbb{Z}} = \{0_A\}$ für ein $k \in \mathbb{N}$ und damit ist U additiv abgeschlossen. Mit (b) ist U somit ein Teilring von A. □

Neben den auf der Algebra A gegebenen Verknüpfungen haben wir noch die Lie-Klammer als weiteres Produkt. Zudem haben wir die $*$-Verknüpfung eingeführt und erhalten damit für quasireguläre Elemente zudem die Konjugation und die $*$-Kommutatorbildung als weitere Verknüpfungen. Wir verwenden dafür in dieser Arbeit die folgenden Bezeichnungen:

Bezeichnungen 1.9 Seien $a, b \in A$. Wir bezeichnen mit

$$[a, b] := ab - ba$$

die Lie-Klammer von a und b. Ist $a \in Q(A)$, so setzen wir

$$b^{(a)} := a^- * b * a$$

als das $*$-Konjugierte von b unter a. Sind $a, b \in Q(A)$, so sei

$$[a, b]_* := a^- * b^- * a * b$$

der $*$-Kommutator von a und b.

Lemma 1.10 (a) Jeder Ring-Homomorphismus von A ist ein Monoid-Homomorphismus von $(A, *)$.

(b) Sei $a \in Q(A)$. Wir definieren $\kappa_a : A \to A$ durch $b \mapsto b^{(a)}$ für alle $b \in A$. Dann ist κ_a ein K-Algebren-Homomorphismus.

(c) Sei A' eine unitäre assoziative K-Algebra und $\varphi : A \to A'$ ein K-Algebren-Homomorphismus. Dann ist

$$\mu : A \to A', \quad a \mapsto 1_{A'} + a\varphi$$

ein Monoid-Homomorphismus von $(A, *)$ in $(A, \cdot)$. Es ist μ genau dann injektiv, wenn φ injektiv ist und genau dann surjektiv, wenn φ surjektiv ist.

Beweis. (a) Dies ist nach Definition der $*$-Verknüpfung klar.
(b) Offenbar ist κ_a ein $*$-Homomorphismus. Seien $b, c \in A$ und $k \in K$. Dann gilt

$$\begin{aligned}
(b+c)\kappa_a &= a^- * (b+c) * a \\
&= a^- + b + c + a + a^-(b+c) + a^-a + (b+c)a + a^-(b+c)a \\
&= b + a^-b + ba + a^-ba + c + a^-c + ca + a^-ca \\
&= b\kappa_a + c\kappa_a \quad \text{und} \\
(bc)\kappa_a &= (b * c - b - c)\kappa_a \\
&= (b\kappa_a * c\kappa_a) - b\kappa_a - c\kappa_a \\
&= b\kappa_a c\kappa_a \quad \text{sowie} \\
(kb)\kappa_a &= a^- * (kb) * a \\
&= a^- + kb + a + a^-(kb) + a^-a + (kb)a + a^-(kb)a \\
&= k(b + a^-b + ba + a^-ba) \\
&= k(b\kappa_a).
\end{aligned}$$

(c) Seien $a, b \in A$. Dann gilt

$$\begin{aligned}
0_A\mu &= 1_{A'} + 0_A\varphi = 1_{A'} \quad \text{und} \\
(a * b)\mu &= 1_{A'} + (a + b + ab)\varphi \\
&= 1_{A'} + a\varphi + b\varphi + (a\varphi)(b\varphi) \\
&= (1_{A'} + a\varphi)(1 + b\varphi) \\
&= a\mu b\mu.
\end{aligned}$$

Injektivität und Surjektivität übertragen sich offensichtlich. □

Lemma 1.11 (a) Sind $a, b \in Q(A)$, so gilt in $K \oplus A$

$$[a, b]_* = (1 + a)^{-1}(1 + b)^{-1}[a, b].$$

(b) Seien $a, b \in A$ nilpotent und $k \in \mathbb{N}$ mit $a^{k+1} = 0_A = b^{k+1}$. Dann ist

$$[a, b]_* = [a, b] + \left(\sum_{i=1}^{k} (-1)^i \sum_{j=0}^{i} a^j b^{i-j} \right) [a, b].$$

(c) Seien $a, b \in A$ nilpotent und $k \in \mathbb{N}$ mit $a^{k+1} = 0_A = b^{k+1}$. Dann ist

$$[a,b]_* * A^{l+1} = [a,b]_* + A^{l+1} = [a,b] + A^{l+1} = [a,b] * A^{l+1}.$$

Beweis. Sei $\mu : A \to K \oplus A$, $a \mapsto 1_K + a$. Nach Lemma 1.10 (c) ist μ ein Isomorphismus von $(A, *)$ auf $(K \oplus A, \cdot)$.
(a) Seien $a, b \in Q(A)$. Dann gilt

$$\begin{aligned} a\mu b\mu &= 1 + a + b + ab = 1 + b + a + ba + [a,b] = b\mu a\mu + [a,b] \quad \text{und damit} \\ [a,b]_* &= ([a,b]_*)\mu\mu^{-1} \\ &= ((a\mu)^{-1}(b\mu)^{-1}a\mu b\mu)\mu^{-1} \\ &= ((a\mu)^{-1}(b\mu)^{-1}(b\mu a\mu + [a,b]))\mu^{-1} \\ &= (1 + (a\mu)^{-1}(b\mu)^{-1}[a,b]) - 1 \\ &= (1+a)^{-1}(1+b)^{-1}[a,b]. \end{aligned}$$

(b) Es gilt in $K \oplus A$

$$\begin{aligned} [a,b]_* &\overset{(a)}{=} (1+a)^{-1}(1+b)^{-1}[a,b] \\ &= (a^-\mu)(b^-\mu)[a,b] \\ &\overset{1.2(c)}{=} \left(1 + \sum_{i=1}^{k}(-a)^i\right)\left(1 + \sum_{i=1}^{k}(-b)^i\right)[a,b] \\ &= [a,b] + \left(\sum_{i=1}^{k}(-1)^i \sum_{j=0}^{i} a^j b^{i-j}\right)[a,b]. \end{aligned}$$

(c) Seien $a, b \in Q(A)$ und $l \in \mathbb{N}$ mit $[a,b] \in A^l$. Dann ist $c[a,b] \in A^{l+1}$ für alle $c \in A$ und damit

$$[a,b]_* + A^{l+1} \overset{(b)}{=} [a,b] + \left(\sum_{i=1}^{k}(-1)^i \sum_{j=0}^{i} a^j b^{i-j}\right)[a,b] + A^{l+1} = [a,b] + A^{l+1}.$$

Die erste und letzte Gleichheit der Behauptung gilt nach Bemerkung 1.4. □

1.2 Zahlentheoretische Hilfsmittel

Um im Fall char $K \neq 0$ die $*$-Potenzen eines Elementes zu beschreiben, benötigen wir zunächst einige Aussagen über Binomialkoeffizienten modulo p^l für eine Primzahl p und ein $l \in \mathbb{N}$.

In diesem Abschnitt sei stets $p \in \mathbb{P}$.

Bezeichnungen 1.12 Es seien $\pi_p, \pi_{p'} : \mathbb{N} \to \mathbb{N}$ mit

$$\left(\prod_{q\in\mathbb{P}} q^{n_q}\right)\pi_p = p^{n_p} \quad \text{und} \quad \left(\prod_{q\in\mathbb{P}} q^{n_q}\right)\pi_{p'} = \prod_{q\in\mathbb{P}\setminus\{p\}} q^{n_q}.$$

Die folgende Bemerkung folgt direkt aus der Definition:

Bemerkung 1.13 Seien $m, n \in \mathbb{N}$. Dann gilt:

(a) $(mn)\pi_p = (m\pi_p)(n\pi_p)$ und $(mn)\pi_{p'} = (m\pi_{p'})(n\pi_{p'})$,

(b) $(m+n)\pi_p \geq \min\{m\pi_p, n\pi_p\}$, $m\pi_p \neq n\pi_p \Rightarrow (m+n)\pi_p = \min\{m\pi_p, n\pi_p\}$,

(c) ist $m > n$, so ist $(m-n)\pi_p \geq \min\{m\pi_p, n\pi_p\}$ und $m\pi_p \neq n\pi_p$ impliziert Gleichheit,

(d) $(n\pi_p)(n\pi_{p'}) = n$,

(e) $m\pi_{p'} + p^l\mathbb{Z} \in (\mathbb{Z}/p^l\mathbb{Z})^*$ für alle $l \in \mathbb{N}$,

(f) $\left(m \mid n \Rightarrow (\frac{n}{m})\pi_p = \frac{n\pi_p}{m\pi_p}\right) \wedge \left((\frac{n}{m})\pi_{p'} = \frac{n\pi_{p'}}{m\pi_{p'}}\right)$ und

(g) $(m \mid n \wedge m\pi_p = n\pi_p) \Rightarrow \frac{n}{m} = \frac{n\pi_{p'}}{m\pi_{p'}}$.

Bemerkung 1.14 Seien $j, l, s, t \in \mathbb{N}$ mit $j \leq l$ und $sp^j \leq tp^l$. Dann gilt

$$\left(sp^j - 1\right)!\pi_{p'} = \left(\prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1} i\right)\left(sp^{j-1} - 1\right)!\pi_{p'} \quad \text{und}$$

$$\prod_{i=1}^{sp^j-1}\left(tp^l - i\right)\pi_{p'} = \left(\prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1}\left(tp^l - i\right)\right)\prod_{i=1}^{sp^{j-1}-1}\left(tp^{l-1} - i\right)\pi_{p'}.$$

Insbesondere folgt

$$\frac{\left(sp^j - 1\right)!\pi_{p'}}{\left(sp^{j-1} - 1\right)!\pi_{p'}} = \prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1} i \quad \text{und} \quad \frac{\prod_{i=1}^{sp^j-1}\left(tp^l - i\right)\pi_{p'}}{\prod_{i=1}^{sp^{j-1}-1}\left(tp^{l-1} - i\right)\pi_{p'}} = \prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1}\left(tp^l - i\right).$$

Beweis. Es gilt

$$\begin{aligned}
\big(sp^j-1\big)!\pi_{p'} &\overset{1.13\,(a)}{=} \left(\prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1} i\pi_{p'}\right)\left(\prod_{i=1}^{sp^{j-1}-1}(pi)\pi_{p'}\right) = \left(\prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1} i\right)\left(\prod_{i=1}^{sp^{j-1}-1} i\right)\pi_{p'} \\
&= \left(\prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1} i\right)\big(sp^{j-1}-1\big)!\pi_{p'} \quad \text{und} \\
\prod_{i=1}^{sp^j-1}\Big(tp^l-i\Big)\pi_{p'} &\overset{1.13\,(a)}{=} \left(\prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1}(tp^l-i)\pi_{p'}\right)\left(\prod_{i=1}^{sp^{j-1}-1}((tp^{l-1}-i)p)\pi_{p'}\right) \\
&= \left(\prod_{\substack{i=1\\ p\nmid i}}^{sp^j-1}(tp^l-i)\right)\prod_{i=1}^{sp^{j-1}-1}\Big(tp^{l-1}-i\Big)\pi_{p'}.
\end{aligned}$$

□

Lemma 1.15 Seien $i,l,s,t\in\mathbb{N}$, $j\in\mathbb{N}_0$ mit $j\le i$, $p\nmid s$, $t<p$ und $sp^j\le tp^i$. Dann gilt

$$\binom{tp^i}{sp^j}\pi_p = p^{i-j} \quad \text{und} \quad \binom{tp^l}{sp^{j+1}} \underset{p^l}{\equiv} \binom{tp^{l-1}}{sp^j}.^{1}$$

Beweis. Sei $a := \prod_{r=1}^{sp^j-1}(tp^i-r)$ und $b := (sp^j-1)!$. Dann gilt:

$$\begin{aligned}
a\pi_p &= \prod_{r=1}^{sp^j-1}\big(tp^i-r\big)\,\pi_p \overset{(\star)}{=} \prod_{r=1}^{sp^j-1} r\pi_p = b\pi_p \\
\Rightarrow\quad \binom{tp^i}{sp^j}\pi_p &= \frac{\big(tp^i\big)!}{(tp^i-sp^j)!\,(sp^j)!}\pi_p = \frac{t\cdot p^i\cdot a}{s\cdot p^j\cdot b}\pi_p = \frac{p^i\cdot(a\pi_p)}{p^j\cdot(b\pi_p)} = p^{i-j}.
\end{aligned}$$

$(\star)$: Für jedes $r\in\underline{sp^j-1}$ gilt nach Voraussetzung $r<sp^j\le tp^i<p^{i+1}$ und damit ist $r\pi_p\le p^i$. Ist also $r\pi_p<p^i$, so folgt $(tp^i-r)\pi_p=r\pi_p$ aus Bemerkung 1.13 (c) und ist $r\pi_p=p^i$, so folgt (da $p^{i+1}>tp^i>tp^i-r$): $p^i\ge(tp^i-r)\pi_p\ge\min\{(tp^i)\pi_p,r\pi_p\}=p^i$ ebenfalls mit Bemerkung 1.13 (c), also gilt auch hier $(tp^i-r)\pi_p=r\pi_p$.
Damit ist der erste Teil der Behauptung gezeigt.
Sei nun $N:=\{n\mid n\in\underline{sp^{j+1}-1}, p\nmid n\}$. Dann gilt

$$(*)\quad |N| \underset{2}{\equiv} \begin{cases} 1 & p=2, j=0 \\ 0 & \text{sonst} \end{cases},$$

[1] Die erste Aussage lässt sich auch als Korollar des Satzes von Kummer [AA09, Seite 204, Theorem 10.2.2] beweisen.

denn: Ist $p \neq 2$, so ist $|N|$ als Vielfaches von $(p-1)$ gerade. Ist $p = 2$, so gilt:

$$|N| \underset{2}{\equiv} \begin{cases} 1, & s2^{j+1} - 1 \underset{4}{\equiv} 1 \\ 0, & s2^{j+1} - 1 \underset{4}{\equiv} 3 \end{cases} = \begin{cases} 1, & 2^{j+1} \underset{4}{\equiv} 2, \\ 0, & 2^{j+1} \underset{4}{\equiv} 0 \end{cases} = \begin{cases} 1, & j = 0 \\ 0, & j > 0 \end{cases}.$$

Wir setzen nun

$$\begin{aligned} a_1 &:= \left(tp^l - 1\right)\left(tp^l - 2\right)\cdots\left(tp^l - sp^{j+1} + 1\right), \\ a_2 &:= \left(tp^{l-1} - 1\right)\left(tp^{l-1} - 2\right)\cdots\left(tp^{l-1} - sp^{j} + 1\right), \\ b_1 &:= \left(sp^{j+1} - 1\right)! \quad \text{und} \\ b_2 &:= \left(sp^{j} - 1\right)!. \end{aligned}$$

Dann gilt

$$\frac{a_1}{b_1} = \frac{\left(tp^l - 1\right)!}{\left(\left(tp^l - 1\right) - \left(sp^{j+1} - 1\right)\right)!\,\left(sp^{j+1} - 1\right)!} = \binom{tp^l - 1}{sp^{j+1} - 1},$$

also $b_1 \mid a_1$. Zudem gilt mit dem ersten Teil

$$p^{l-j-1} = \binom{tp^l}{sp^{j+1}}\pi_p = \frac{t \cdot p^l \cdot a_1}{s \cdot p^{j+1} \cdot b_1}\pi_p = p^{l-j-1}\frac{a_1\pi_p}{b_1\pi_p}.$$

Damit ist $a_1\pi_p = b_1\pi_p$ und wir erhalten

$$\begin{aligned} \binom{tp^l}{sp^{j+1}} &= \frac{t \cdot p^l \cdot a_1}{s \cdot p^{j+1} \cdot b_1} \overset{1.13\,(g)}{=} p^{l-j-1}\frac{t \cdot a_1\pi_{p'}}{s \cdot b_1\pi_{p'}} \quad \text{und ebenso} \\ \binom{tp^{l-1}}{sp^{j}} &= p^{l-j-1}\frac{t \cdot a_2\pi_{p'}}{s \cdot b_2\pi_{p'}}. \end{aligned}$$

Weiter gilt nach Bemerkung 1.14

$$\frac{a_1\pi_{p'}}{a_2\pi_{p'}} = \prod_{\substack{i=1 \\ p \nmid i}}^{sp^{j+1}-1}\left(tp^l - i\right) \underset{p^l}{\equiv} (-1)^{|N|}\prod_{\substack{i=1 \\ p \nmid i}}^{sp^{j+1}-1} i = (-1)^{|N|}\frac{b_1\pi_{p'}}{b_2\pi_{p'}}$$

und damit

$$\begin{aligned} \binom{tp^l}{sp^{j+1}} &= p^{l-j-1}\frac{t \cdot a_1\pi_{p'}}{s \cdot b_1\pi_{p'}} \\ &\underset{p^l}{\equiv} p^{l-j-1}\frac{t \cdot (-1)^{|N|}\frac{b_1\pi_{p'}}{b_2\pi_{p'}} \cdot a_2\pi_{p'}}{s \cdot b_1\pi_{p'}} \\ &= (-1)^{|N|}p^{l-j-1}\frac{t \cdot a_2\pi_{p'}}{s \cdot b_2\pi_{p'}} \\ &= (-1)^{|N|}\binom{tp^{l-1}}{sp^{j}}. \end{aligned}$$

Ist nun $(p, j) \neq (2, 0)$, so ist die Behauptung mit $(*)$ gezeigt. Im Fall $(p, j) = (2, 0)$ folgt mit dem ersten Teil der Behauptung $2^{l-1} \mid \binom{t2^{l-1}}{s2^0}$ und damit $\binom{t2^{l-1}}{s2^0} \underset{2^l}{\equiv} -\binom{t2^{l-1}}{s2^0}$. □

Wie wir in den folgenden Abschnitten sehen werden, hängt die Struktur der $*$-Gruppe im Fall eines Ringes der Charakteristik p^l davon ab, wie sich p und die Nilpotenzklasse k zueinander verhalten; genauer: Welches ist die höchste p-Potenz, die kleiner gleich k ist? Dazu machen wir hier schon einige Vorbetrachtungen:

Definition 1.16 Sei $k \in \mathbb{N}$. Für alle $t \in \mathbb{N}_0$ setzen wir

$$c_{k,p,t} := \left\lfloor \frac{k}{p^t} \right\rfloor, \; I_{k,p,t} := (c_{k,p,t+1}, c_{k,p,t}] \cap \mathbb{N} \quad \text{und}$$
$$s_{k,p} := \max\{t \in \mathbb{N}_0 \mid c_{k,p,t} \neq 0\} \; (= \max\{t \in \mathbb{N}_0 \mid p^t \leq k\}).$$

Damit ist $s_{k,p}$ die höchste p-Potenz, die in der p-adischen Zerlegung von k auftritt. Ist k oder p im jeweiligen Kontext eindeutig bestimmt, so verzichten wir auf die Indizierung.

Beispiel 1.17 Wir betrachten den Fall $k = 10$ und $p = 3$. Dann gilt

$$c_0 = \left\lfloor \frac{10}{3^0} \right\rfloor = 10,\; c_1 = \left\lfloor \frac{10}{3} \right\rfloor = 3,\; c_2 = \left\lfloor \frac{10}{3^2} \right\rfloor = 1 \text{ und } c_j = \left\lfloor \frac{10}{3^j} \right\rfloor = 0 \text{ für alle } j \geq 3.$$

Damit folgt $s = 2$ und

$$\begin{aligned} I_0 &= (3, 10] \cap \mathbb{N} = \{4, 5, 6, 7, 8, 9, 10\}, \\ I_1 &= (1, 3] \cap \mathbb{N} = \{2, 3\}, \\ I_2 &= (0, 1] \cap \mathbb{N} = \{1\} \quad \text{und} \\ I_j &= \emptyset \text{ für alle } j \geq 3. \end{aligned}$$

Bemerkung 1.18 Sei $k \in \mathbb{N}$ und $p \in \mathbb{P}$. Dann gilt:

(a) $k = c_0 > c_1 > \cdots > c_s > c_{s+1} = 0 = c_{s+2} = c_{s+3} = \ldots$

(b) $\forall t \in \mathbb{N}_{>s} : I_t = \emptyset$

(c) $\dot{\bigcup}_{t \in \underline{s}_0} I_t = \underline{k}$

(d) Seien $k_0, \ldots, k_s \in \underline{p-1}_0$ mit $k = \sum_{i=0}^{s} k_i p^i$ (p-adische Zerlegung von k). Dann gilt $c_t = \sum_{i=0}^{s-t} k_{t+i} p^i$ für alle $t \in \mathbb{N}_0$.

(e) $\forall r, t \in \mathbb{N}_0 : \left\lfloor \frac{c_t}{p^r} \right\rfloor = c_{t+r}$

(f) $\forall r, t \in \mathbb{N}_0 : |\underline{c_t} \cap p^r \mathbb{N}| = c_{t+r}$

(g) $\forall t \in \mathbb{N}_0 : |I_t \cap p\mathbb{N}| = |I_{t+1}|$

(h) $\forall t \in \mathbb{N}_0 : |I_t \setminus p\mathbb{N}| = |I_t| - |I_{t+1}|$

Beweis. Die Aussagen (a), (b) und (c) folgen sofort aus der Definition.
Sei $t \in \mathbb{N}_0$. Nach Definition ist c_t die eindeutig bestimmte Zahl mit $c_t p^t \leq k$ und $(c_t+1)p^t > k$. Seien $k_0, \ldots, k_s \in \underline{p-1}_0$ wie in (d). Dann gilt

$$\left(\sum_{i=0}^{s-t} k_{t+i}p^i\right) p^t = \sum_{i=t}^{s} k_i p^i \leq \sum_{i=0}^{s} k_i p^i = k \quad \text{und}$$
$$\left(\sum_{i=0}^{s-t} k_{t+i}p^i + 1\right) p^t = \sum_{i=0}^{s} k_i p^i + \underbrace{p^t - \sum_{i=0}^{t-1} k_i p^i}_{>0} > k.$$

Damit folgt $c_t = \sum_{i=0}^{s-t} k_{t+i}p^i$. Weiter ist für alle $r \in \mathbb{N}_0$

$$\left\lfloor \frac{c_t}{p^r} \right\rfloor p^{t+r} \leq \frac{c_t}{p^r} p^{t+r} = c_t p^t \leq k \quad \text{und}$$
$$\left(\left\lfloor \frac{c_t}{p^r} \right\rfloor + 1\right) p^{t+r} \geq \left(\frac{c_t - (p^r-1)}{p^r} + 1\right) p^{t+r} = (c_t+1)p^t > k.$$

Damit ist $\left\lfloor \frac{c_t}{p^r} \right\rfloor = c_{t+r}$ und (d) und (e) sind gezeigt. (f) ist eine direkte Konsequenz von (e) und es folgt daraus $|I_t \cap p\mathbb{N}| = |\underline{c_t}| \cap p\mathbb{N}| - |\underline{c_{t+1}}| \cap p\mathbb{N}| = c_{t+1} - c_{t+2} = |I_{t+1}|$ und $|I_t \setminus p\mathbb{N}| = |I_t| - |I_t \cap p\mathbb{N}| = |I_t| - |I_{t+1}|$. Damit gilt die Behauptung. □

1.3 Frei nilpotente Algebren und Potenzreihenalgebren

Im zweiten, dritten und vierten Kapitel dieser Arbeit wollen wir insbesondere die Gruppe der quasiregulären Elemente in der frei nilpotenten Algebra und in der Potenzreihenalgebra betrachten. In diesem Abschnitt führen wir diese Strukturen mit geeigneten Darstellungen ein und treffen erste Aussagen über ihre $*$-Strukturen. Zudem betrachten wir im späteren Teil dieses Abschnitts, wie sich eine Charakteristik $\neq 0$ des Rings K auf die $*$-Gruppe auswirkt.

Einige Teile der Aussagen dieses Abschnitts finden sich bereits in meiner Diplomarbeit [Han12].

In diesem Abschnitt seien stets $k, n \in \mathbb{N}$ und X eine nichtleere Menge.

Bezeichnungen 1.19 Wir bezeichnen mit

X^+	die Menge der nichtleeren Worte in X,
$l(f)$	die Länge eines Wortes $f \in X^+$,
$X^{=k}$	die Menge der Worte der Länge k in X^+ und
$X^{\leq k}$	die Menge der Worte bis zur Länge k in X^+.

Es sei

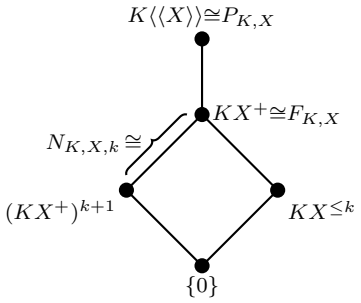
$F_{K,X}$	die freie K-Algebra über X,
$N_{K,X,k}$	die frei nilpotente K-Algebra über X von der Klasse k und
$P_{K,X}$	die K-Potenzreihenalgebra über X.[2]

Ist dabei $|X| = n$, so schreiben wir auch $F_{K,n}$, $N_{K,n,k}$ und $P_{K,n}$. Sind K, X, n oder k im Kontext eindeutig gegeben, so verzichten wir ganz oder teilweise auf die Indizierung.

Bemerkung 1.20 (a) Der K-Raum

$$K\langle\langle X\rangle\rangle = \left\{ \sum_{f\in X^+} \alpha_f f \mid \alpha_f \in K \text{ für alle } f \in X^+ \right\}$$

ist mit der Multiplikation, die als distributive Fortsetzung der Konkatenation auf X^+ entsteht, eine K-Algebra und als solche isomorph zu $P_{K,X}$.



(b) Die K-Teilalgebra KX^+ der endlichen K-Linearkombinationen über X^+ in $K\langle\langle X\rangle\rangle$ ist isomorph zu $F_{K,X}$ als K-Algebra.

(c) Es ist $N_{K,X,k} \cong F_{K,X}/(F_{K,X})^{k+1}$.

Korollar 1.20.1 Wir definieren auf dem K-Raum $KX^{\leq k}$ mit Basis $X^{\leq k}$ eine Multiplikation als distributive Fortsetzung von

$$\forall f, g \in X^{\leq k} : f \cdot g := \begin{cases} fg & l(f) + l(g) \leq k \\ 0_{KX^{\leq k}} & \text{sonst} \end{cases}.$$

Mit dieser Multiplikation ist $KX^{\leq k}$ eine K-Algebra und als solche isomorph zu $N_{K,X,k}$.

Korollar 1.20.2 Ist X n-elementig, so ist $\mathrm{rk}_K(N_{K,X,k}) = \sum_{i=1}^{k} n^i = \frac{n^{k+1}-n}{n-1}$.

Anmerkung 1.21 Im Folgenden verwenden wir die Begriffe der freien Algebra, der frei nilpotenten Algebra und der Potenzreihenalgebra synonym zu ihren hier vorgestellten Darstellungen. Dabei ist zu beachten, dass $N = KX^{\leq k}$ ein K-Teilraum von $P = K\langle\langle X\rangle\rangle$ ist, jedoch keine Teilalgebra, da auf N eine andere Multiplikation definiert wird. Dadurch ergeben sich auch verschiedene $*$-Verknüpfungen auf P und N.

Bemerkung 1.22 $(P, *)$ und $(N, *)$ sind Gruppen. Es gilt in $(P, *)$ für alle $a, b \in P$ und

[2] Wir betrachten in dieser Arbeit die freie Algebra und die Potenzreihenalgebra als nicht-unitäre und (für $|X| > 1$) nicht-kommutative Algebren.

$m \in \mathbb{N}$

$$a^{(-m)} = \sum_{i \in \mathbb{N}} (-1_K)^i \binom{m+i-1}{i} a^i \text{ und}$$

$$[a,b]_* = [a,b] + \left(\sum_{i \in \mathbb{N}} (-1)^i \sum_{j=0}^{i} a^j b^{i-j} \right) [a,b].$$

Beweis. Nach Bemerkung 1.1 sind $(P, *)$ und $(N, *)$ Monoide. Nach Lemma 1.2 (c) ist $Q(N) = N$, also ist $(N, *)$ eine Gruppe. Weiter gilt für alle $a \in P$

$$a * \left(\sum_{i=1}^{\infty} (-1_K)^i a^i \right) = a + \sum_{i=1}^{\infty} (-1_K)^i a^i + \sum_{i=1}^{\infty} (-1_K)^i a^{i+1} = 0$$

und damit ist jedes Element von P quasiregulär. Also ist auch $(P, *)$ eine Gruppe. Der letzte Teil der Behauptung folgt induktiv nach m wie in Lemma 1.2 (f) und analog zu dem Beweis von Lemma 1.11 (b). □

Im allgemeinen Fall ist wenig über die Gruppen $(P, *)$ und $(N, *)$ bekannt, die wir im zweiten Teil dieser Arbeit untersuchen wollen. Wichtig ist aber in diesem Zusammenhang der nun folgende Satz von Magnus aus [Mag35].

Satz 1.23 (Magnus, 1935) In $P_{\mathbb{Z},X}$ ist $\langle X \rangle_*$ frei von X erzeugt.

Definition und Lemma 1.24 Sei $i \in \mathbb{N}$ und $g \in X^+$. Wir setzen

$$\pi_i : P \to \langle X^{=i} \rangle_K, \sum_{f \in X^+} \alpha_f f \mapsto \sum_{f \in X^{=i}} \alpha_f f,$$

$$\pi_{\leq i} : P \to \langle X^{\leq i} \rangle_K, \sum_{f \in X^+} \alpha_f f \mapsto \sum_{f \in X^{\leq i}} \alpha_f f,$$

$$\pi_{>i} := \mathrm{id} \; - \pi_{\leq i} \quad \text{und}$$

$$\pi_g : P \to \langle g \rangle_K, \sum_{f \in X^+} \alpha_f f \mapsto \alpha_g g.$$

Wir nennen π_i die Projektion auf die i-te homogene Komponente und π_g die Projektion auf den g-Anteil. Ein Element $a \in P$ nennen wir homogen, falls es ein $j \in \mathbb{N}$ gibt, sodass $a\pi_l = 0$ für alle $l \in \mathbb{N} \setminus \{j\}$ gilt. In diesem Fall nennen wir a auch homogen vom Grad j. π_i, $\pi_{\leq i}$ und π_g sind K-Raum-Endomorphismen von P. Dabei sind F und N π_i-, $\pi_{\leq i}$- und π_g-invariant. Zudem gilt $N = F\pi_{\leq k}$.

Korollar 1.24.1 Bezeichnet $\underset{P}{\cdot}$ die Multiplikation auf P und $\underset{N}{\cdot}$ die auf N, so gilt für alle $a, b \in N$

$$a \underset{N}{\cdot} b = \left(a \underset{P}{\cdot} b \right) \pi_{\leq k}.$$

Bemerkung 1.25 (a) Sind $\alpha_f, \beta_f \in K$ für alle $f \in X^+$ mit

$$\sum_{f \in X^+} \alpha_f f = \sum_{f \in X^+} \beta_f f,$$

so folgt $\alpha_f = \beta_f$ für alle $f \in X^+$. Insbesondere ist P als K-Raum sowohl die unbeschränkte direkte Summe über $\{P\pi_i \mid i \in \mathbb{N}\}$ als auch über $\{P\pi_g \mid g \in X^+\}$.

(b) X^+ ist eine K-Basis von F und es gilt $F = \bigoplus_{i \in \mathbb{N}} P\pi_i = \bigoplus_{g \in X^+} P\pi_g$ als K-Raum.

(c) $X^{\leq k}$ ist eine K-Basis von N und $N = \bigoplus_{i=1}^{k} P\pi_i = \bigoplus_{g \in X^{\leq k}} P\pi_g$ als K-Raum. Gilt insbesondere $|X| = n$, so ist

$$\mathrm{rk}_K N = \sum_{i=1}^{k} n^i = \frac{n^{k+1} - n}{n - 1}.$$

Oftmals ist es für uns nicht von Interesse, wie genau die homogenen Komponenten eines Elementes $a \in P$ aussehen, sondern lediglich welche Komponenten $\neq 0$ sind und welche die kleinste Komponente $\neq 0$ ist. Dafür verwenden wir den Begriff der Länge.

Definition 1.26 Wir definieren die (X-)Länge eine Elementes $a \in P$ als

$$L(a) := \begin{cases} \infty & a = 0 \\ \min\{i \in \mathbb{N} \mid a\pi_i \neq 0\} & \text{sonst} \end{cases}.$$

Außerdem sei

$$\pi_{\min} : P \setminus \{0\} \to P \setminus \{0\}, a \mapsto a\pi_{L(a)}.$$

Bemerkung 1.27 Seien $a, b \in P$ und $\alpha \in K$. Dann gilt bezüglich der Verknüpfungen auf P und N:

(a) $L(a+b) \geq \min\{L(a), L(b)\}$, $L(\alpha a) \geq L(a)$ und $L(ab) \geq L(a) + L(b)$ sowie

(b) $L(-a) = L(a)$ und $L(a^-) = L(a)$.

(c) Sei $m \in \mathbb{Z}$ mit $L(ma) = L(a)$. Dann ist $L(a^{(m)}) = L(a)$. Insbesondere ist $a^{(m)} \neq 0$ für $a \neq 0$.

(d) Ist K ein Integritätsbereich und $\alpha \neq 0_K$, so ist $L(\alpha a) = L(a)$ und bezüglich der Multiplikation auf P gilt $L(ab) = L(a) + L(b)$. In N gilt mit der dortigen Multiplikation $L(ab) = L(a) + L(b)$ falls $L(a) + L(b) \leq k$ und $L(ab) = \infty$ sonst.

(e) Es ist $P^i = \{a \in P \mid L(a) \geq i\}$ und $N^i = \{a \in N \mid L(a) \geq i\}$ für alle $i \in \mathbb{N}$.

Beweis. (a) und (d) folgen direkt aus der Definition der Länge. Für $a = 0$ sind (b), (c) klar. Es gilt für $a \neq 0$

$$-a = \sum_{i=L(a)}^{\infty} -a\pi_i \Rightarrow L(-a) = L(a).$$

Es folgt in P

$$a^- \overset{1.22}{=} \sum_{i=1}^{\infty}(-1_K)^i a^i \overset{(a)}{\Rightarrow} L(a^-) = L(-a) = L(a)$$

und in N

$$a^- \overset{1.2(c)}{=} \sum_{i=1}^{k}(-1_K)^i a^i \overset{(a)}{\Rightarrow} L(a^-) = L(-a) = L(a).$$

Ist $m \in \mathbb{Z}$ mit $L(ma) = L(a)$, so folgt aus Lemma 1.2 (e), (f)

$$L(a^{(m)}) = L(|m|a) \overset{(b)}{=} L(ma) = L(a).$$

Damit gelten (b) und (c).
(e) Nach Korollar 1.24.1 genügt es, die Aussage für P zu beweisen. Sei $i \in \mathbb{N}$. Sind $a_1, \ldots, a_i \in P$, so gilt nach (a) $L(a_1 \ldots a_i) \geq \sum_{j=1}^{i} L(a_j) \geq i$ und ebenfalls nach (a) und (b) ist $\{a \in P \mid L(a) \geq i\}$ ein K-Raum. Also ist $P^i \subseteq \{a \in P \mid L(a) \geq i\}$. Zudem ist offenbar $X^+ \setminus X^{\leq i-1} \subseteq P^i$ und damit folgt aus der Definition der Länge $P^i \supseteq \{a \in P \mid L(a) \geq i\}$. □

Korollar 1.27.1 Sei $m \in \mathbb{N} \cup \{\infty\}$ das Minimum der additiven Elementordnungen in $K \setminus \{0\}$. Dann gilt $a^{(i)} \neq 0$ für alle $i \in \mathbb{N}_{<m}$ und $a \in P \setminus \{0\}$ bezüglich der $*$-Verknüpfung auf P und auf N.

Beweis. Sei $a \in P \setminus \{0\}$ und $i \in \mathbb{N}_{<m}$. Dann gilt $L(ia) = L(a)$ und die Behauptung folgt aus Bemerkung 1.27 (c). □

Korollar 1.27.2 Es ist $\{P\pi_i \mid i \in \mathbb{N}\}$ eine Graduierung von F und $\{P\pi_i \mid i \in \underline{k}\}$ eine Graduierung von N.

Beweis. Seien $i, j \in \mathbb{N}$. Es ist $P\pi_i = \langle X^{=i} \rangle_K$, $P\pi_j = \langle X^{=j} \rangle_K$ und $X^{=i} \cdot X^{=j} = X^{=i+j}$. Damit folgt $P\pi_i \cdot P\pi_j = P\pi_{i+j}$ und die Behauptung für N mit Korollar 1.24.1. □

Bemerkung 1.28 Sei L ein weiterer kommutativer unitärer Ring. Dann sind

$$P_{K\times L} \cong P_K \times P_L,\ F_{K\times L} \cong F_K \times F_L \quad \text{und} \quad N_{K\times L} \cong N_K \times N_L$$

als $(K \times L)$-Algebren.

Beweis. Sei

$$\varphi : P_{K\times L} \to P_K \times P_L,\ \sum_{f\in X^+}(\alpha_f, \beta_f)f \mapsto \left(\sum_{f\in X^+}\alpha_f f,\ \sum_{f\in X^+}\beta_f f\right).$$

Dann sind φ, $\varphi_{|F_{K\times L}}$ und $\varphi_{|N_{K\times L}}$ $(K \times L)$-Algebren-Isomorphismen zwischen den jeweiligen Strukturen. □

Nun wollen wir untersuchen, unter welchen Bedingungen die Gruppen $(N, *)$ und $(P, *)$ abelsch sind und ihre Zentren beschreiben.

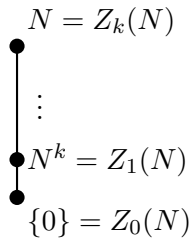
Bemerkung 1.29 (a) P und F sind genau dann kommutativ, wenn $|X| = 1$ gilt.

(b) N ist genau dann kommutativ, wenn $|X| = 1$ oder $k = 1$ gilt.

Lemma 1.30 (a) Gilt $|X| = 1$, so sind $(P, *)$ und $(N, *)$ abelsch.

(b) Ist $|X| > 1$, so ist $Z(P) = \{0\}$.

(c) Ist $|X| > 1$, so ist $Z(N) = N^k = F\pi_k$. Insbesondere ist in diesem Fall $(N, *)$ nilpotent von der Klasse k und $(\{0\} = N^{k+1}, N^k, N^{k-1}, \ldots, N^2, N)$ ist die aufsteigende Zentralreihe von N.



Beweis. (a) und (b) sind klar.
(c) $N^k \subseteq Z(N)$ folgt aus Bemerkung 1.3 (e).
Sei nun $a \in Z(N)$. Dann existieren $\alpha_f \in K$ für alle $f \in X^{\leq k}$ mit $a = \sum_{f \in X^{\leq k}} \alpha_f f$ und es gilt für alle $x \in X$

$$ax = xa \Rightarrow 0 = \sum_{f \in X^{\leq k}} \alpha_f (fx - xf).$$

Da $X^{\leq k}$ K-linear unabhängig ist, gilt: Gibt es $g, h \in X^{\leq k}$ mit $xg = hx$, so endet g mit dem Buchstaben x. Damit folgt $k_f = 0$ für alle $f \in X^{\leq k-1}$, die nicht auf x enden. Da $|X| > 1$ ist, folgt damit $k_f = 0$ für alle $f \in X^{\leq k-1}$.
Wie zeigen den zweiten Teil der Aussage induktiv nach k. Dabei ist für $k = 1$ bereits alles gezeigt. Sei nun $k > 1$. Dann gilt mit Bemerkung 1.20 (c)

$$N_k/Z(N_k) = N_k/N_k^k \cong (F/F^{k+1})/(F^k/F^{k+1}) \cong F/F^k \cong N_{k-1}.$$

Nach Induktionsvoraussetzung ist $(N_{k-1}^k, N_{k-1}^{k-1}, \ldots, N_{k-1}^2, N_{k-1})$ die aufsteigende Zentralreihe von N_{k-1} und N_{k-1} ist nilpotent von der Klasse $k-1$. Damit ist N_k nilpotent von der Klasse k und $(\{0\} = N_k^{k+1}, N_k^k, \ldots, N_k)$ ist die aufsteigende Zentralreihe von N_k. □

Nun wollen wir Basen der Ideale N^t von N aus Basen der homogenen Komponenten $N\pi_i$ konstruieren. Mit Hilfe dieser werden wir anschließend $*$-Erzeugendensysteme der Ideale angeben.

Lemma 1.31 Für alle $i \in \underline{k}$ sei $B_i \subseteq N^i$, so dass $B_i\pi_i$ eine K-Basis von $N\pi_i$ ist. Für alle $t \in \underline{k}$ setzen wir $B_{\geq t} := \cup_{i=t}^k B_i$. Dann ist $B_{\geq t}$ eine K-Basis von N^t für alle $t \in \underline{k}$.

Beweis. Wir zeigen induktiv nach r, dass $B_{\geq k-r}$ eine K-Basis von N^{k-r} ist.
Für $r = 0$ ist $B_k = B_k\pi_k$ nach Voraussetzung eine K-Basis von $N\pi_k = N^k$.

Sei nun $r > 0$ und $a \in N^{k-r}$. Dann existieren nach Voraussetzung $C \subseteq B_{k-r}$ endlich, $\alpha_c \in K$ für alle $c \in C$ mit

$$a\pi_{k-r} = (\underbrace{\sum_{c\in C} \alpha_c c}_{=:d\in\langle B_{k-r}\rangle_K})\pi_{k-r}. \quad \text{Dann folgt}$$

$$a = a\pi_{k-r} + a\pi_{>k-r} = d\pi_{k-r} + a\pi_{>k-r} = d + a\pi_{>k-r} - d\pi_{>k-r}.$$

Nach Induktionsvoraussetzung ist $a\pi_{>k-r} - d\pi_{>k-r} \in \langle B_{\geq k-r+1}\rangle_K$ und daraus folgt $a \in \langle B_{\geq k-r}\rangle_K$. Damit ist $B_{\geq k-r}$ ein K-Erzeugendensystem von N^{k-r}.
Sei $C \subseteq B_{\geq k-r}$ endlich und für alle $c \in C$ sei $\alpha_c \in K$ mit

$$0_N = \sum_{c\in C} \alpha_c c.$$

Es folgt

$$0_N = \left(\sum_{c\in C} \alpha_c c\right)\pi_{k-r} = \sum_{c\in C\cap B_{k-r}} \alpha_c c\pi_{k-r}$$

und damit nach Voraussetzung $\alpha_c = 0_K$ für alle $c \in C \cap B_{k-r}$. Damit ist

$$\sum_{c\in C\cap B_{\geq k-r+1}} \alpha_c c = 0_K$$

und mit der Induktionsvoraussetzung folgt $\alpha_c = 0$ für alle $c \in C$. Damit ist $B_{\geq k-r}$ eine K-Basis von N^{k-r}. □

Wir können mit Hilfe von speziellen K-Erzeugendensystemen von N und additiven Erzeugendensystemen von K nun $*$-Erzeugendensysteme von Idealen von N angeben.

Lemma 1.32 Es sei κ ein additives Erzeugendensystem von K, I ein Rechts- oder Linksideal von N und B ein K-Erzeugendensystem von I, so dass $(B \setminus \{0\})\pi_{\min}$ für alle $i \in \underline{k}$ ein K-Erzeugendensystem von $N\pi_i \cap I$ enthält. Dann ist $\kappa B = \{\alpha b \mid \alpha \in \kappa, b \in B\}$ ein $*$- Erzeugendensystem von I.

Beweis. Sei $U := \langle \kappa B\rangle_*$. Wir zeigen induktiv nach j

$$N^{k-j} \cap I \subseteq U$$

für alle $j \in \underline{k-1}_0$. Dann folgt $I = N \cap I \subseteq U$ und damit $U = I$, da $\kappa B \subseteq I$ gilt und I nach Bemerkung 1.3 $*$-Gruppe ist.
Für $j = 0$ gilt: Nach Voraussetzung und der Definition von $\pi_{\min}$ enthält B ein K-Erzeugendensystem von $N^k \cap I$, etwa B_0. Da $a*b = a+b$ und $a^- = -a$ für alle $a, b \in N^k$ gilt, folgt

$$I \cap N^k = \langle B_0\rangle_K = \langle \kappa B_0\rangle_{\mathbb{Z}} = \langle \kappa B_0\rangle_* \subseteq U.$$

Sei nun $j > 0$ und es gelte $N^{k-j+1} \cap I \subseteq U$. Wir setzen $B_j := \{b \in B \mid L(b) \geq k - j\}$. Sei $a \in N^{k-j} \cap I$. Dann gibt es nach Voraussetzung $z_{\alpha,b} \in \mathbb{Z}$ für alle $\alpha \in \kappa$ und $b \in B_j$ mit

$$a = \sum_{b \in B_j} \sum_{\alpha \in \kappa} z_{\alpha,b} \alpha b.$$

Dann gibt es für jede Reihenfolge der $*$-Produkte ein $a' \in N^{k-j+1} \cap I$ mit Lemma 1.2 (d), (e), (f) mit

$$a + a' = \bigstar_{b \in B_j} \bigstar_{\alpha \in \kappa} (\alpha b)^{(z_{\alpha,b})} \in U,$$

da bei jeder Reihenfolge der $*$-Produkte a als Summand vorkommt. Mit Lemma 1.5 folgt $a \in U$. □

Korollar 1.32.1 Es gilt $\langle \kappa X^{\leq k} \rangle_* = N$. Ist insbesondere K ein Faktorring von $\mathbb{Z}$, so ist $X^{\leq k}$ ein $*$-Erzeugendensystem von N.

Beweis. Wir wählen $I = N$ und $B = X^{\leq k}$ in Lemma 1.32. Dann ist $X^{\leq k}$ eine K-Basis von N und für alle $i \in \underline{k}$ ist $X^{=i}\pi_{\min} = X^{=i}$ eine K-Basis von $N\pi_i$. □

Korollar 1.32.2 Ist X endlich und $(K, +)$ endlich erzeugt, so ist $(N, *)$ endlich erzeugt.

Nun wollen wir uns mit $(N_{K,X,k}, *)$ im Fall eines Grundrings der Charakteristik $\neq 0$ befassen. Dazu betrachten wir zunächst, wie die $*$-Ordnung eines Elementes mit seiner additiven Ordnung zusammenhängt.

Bezeichnungen 1.33 Wir haben auf der Menge N zwei Verknüpfungen, bezüglich derer N eine Gruppe ist: die Addition und die $*$-Verknüpfung. Verwenden wir die Ordnung bezüglich beider Verknüpfungen, so schreiben wir für alle $a \in N$

$$o_+(a) \quad \text{beziehungsweise} \quad o_*(a)$$

für die additive beziehungsweise $*$-Ordnung von a. Schreiben wir nur $o(a)$, so beziehen wir uns stets auf die $*$-Verknüpfung.

Bemerkung 1.34 Sei $a \in N$ und $p \in \mathbb{P}$ sowie $l \in \mathbb{N}$ mit $o_+(a) \mid p^l$. Dann gilt

$$a^{(p^l)} = (a^p)^{(p^{l-1})}.$$

Beweis. Nach Lemma 1.15 existieren für alle $i, j \in \underline{p^l}$ mit $p \nmid i$ natürliche Zahlen $m, m' \in \mathbb{N}$ mit $\binom{p^l}{i} = mp^l$ und $\binom{p^l}{jp} = m'p^l + \binom{p^{l-1}}{j}$. Es folgt

$$(\star) \quad \binom{p^l}{i} a^i = m \left(p^l a\right) a^{i-1} = 0 \quad \text{und}$$

$$(\star\star) \quad \binom{p^l}{jp} a^{jp} = m' \left(p^l a\right) a^{jp-1} + \binom{p^{l-1}}{j} a^{jp} = \binom{p^{l-1}}{j} a^{jp}$$

und damit erhalten wir

$$a^{(p^l)} \overset{1.2\,(e)}{=} \sum_{i=1}^{p^l} \binom{p^l}{i} a^i \overset{(\star)}{=} \sum_{i=1}^{p^{l-1}} \binom{p^l}{ip} a^{ip} \overset{(\star\star)}{=} \sum_{i=1}^{p^{l-1}} \binom{p^{l-1}}{i} (a^p)^i \overset{1.2\,(e)}{=} (a^p)^{(p^{l-1})}.$$

□

Korollar 1.34.1 Es gilt

$$\left(a^{(p)} * (a^p)^-\right)^{(p^{l-1})} = 0 \quad \text{und}$$
$$\left(a^{(p)} * (a^p)^-\right)^{(p^{l-2})} \pi_{L(a)} = p^{l-1} a \pi_{L(a)} \quad \text{für } l \geq 2 \text{ und } a \neq 0.$$

Ist insbesondere char $K = p^l$, so gilt für alle $b \in N$

$$o_*\left(b^{(p)} * (b^p)^-\right) \mid p^{l-1} \quad \text{und} \quad o_*\left(x^{(p)} * (x^p)^-\right) = p^{l-1}$$

für alle $x \in X$.

Beweis. Sei $a \in N$ mit $o_+(a) \mid p^l$. Der erste Teil der Behauptung ist direkte Folgerung aus Bemerkung 1.34. Weiter folgt für $l \geq 2$ und $a \neq 0$

$$\left(a^{(p)} * (a^p)^-\right)^{(p^{l-2})} \pi_{L(a)} \overset{L(a^p) \geq L(a)}{=} \left(a^{(p)}\right)^{(p^{l-2})} \pi_{L(a)} = a^{(p^{l-1})} \pi_{L(a)} \overset{1.2\,(e)}{=} p^{l-1} a \pi_{L(a)}.$$

Es sei nun char $K = p^l$, $b \in N$ und $x \in X$. Dann gilt $o_+(b) \mid p^l$ und $o_+(x) = p^l$ und mit dem ersten Teil folgt $o_*(b^{(p)} * (b^p)^-), o_*(x^{(p)} * (x^p)^-) \mid p^{l-1}$ und mit dem zweiten Teil $o_*(x^{(p)} * (x^p)^-) \nmid p^{l-2}$. Also ist $o_*(x^{(p)} * (x^p)^-) = p^{l-1}$. □

Lemma 1.35 Sei $a \in N$ und $p \in \mathbb{P}$ sowie $l \in \mathbb{N}$ mit $o_+(a) \mid p^l$. Sei $t \in \underline{s}_0$ mit $L(a) \in I_t$ (vergleiche Definition 1.16). Dann gilt

$$o_*(a) \mid p^{l+t}.$$

Beweis. Es gilt für alle $i \in \mathbb{N}$

$$(\star) \quad L\left(a^{ip^{t+1}}\right) \geq L\left(a^{p^{t+1}}\right) \geq p^{t+1} L(a) \overset{L(a) \in I_t}{\geq} p^{t+1}(c_{t+1} + 1) > k \Rightarrow a^{ip^{t+1}} = 0.$$

Außerdem existiert nach Lemma 1.15 für alle $i \in \mathbb{N}$ mit $p^{t+1} \nmid i$ eine natürliche Zahl $m \in \mathbb{N}$ mit $mp^l = \binom{p^{l+t}}{i}$, es gilt also

$$(\star\star) \quad \binom{p^{l+t}}{i} a^i = m \left(p^l a\right) a^{i-1} = 0.$$

Damit folgt

$$a^{(p^{l+t})} \overset{1.2\,(e)}{=} \sum_{i=1}^{p^{l+t}} \binom{p^{l+t}}{i} a^i \overset{(\star\star)}{=} \sum_{i=1}^{p^{l-1}} \binom{p^{l+t}}{p^{t+1} i} a^{ip^{t+1}} \overset{(\star)}{=} 0.$$

□

Korollar 1.35.1 Ist $K = \mathbb{Z}/p^l\mathbb{Z}$ und $a \neq 0$ mit $o_+(a\pi_{\min}) = p^l$, so gilt

$$o_*(a) = o_+(a)p^t = p^{l+t}.$$

Beweis. Sei $K = \mathbb{Z}/p^l\mathbb{Z}$ und $a \in N\setminus\{0\}$ mit $o_+(a\pi_{\min}) = p^l$ (dann ist auch $o_+(a) = p^l$). Nach Lemma 1.35 genügt es $a^{(p^{l+t-1})} \neq 0$ zu zeigen. Wie im Beweis zu Lemma 1.35 ist $\binom{p^{l+t-1}}{i}a^i = 0$ für alle $i \in \mathbb{N}$ mit $p^t \nmid i$ und es folgt

$$a^{(p^{l+t-1})} \overset{1.2\,(e)}{=} \sum_{i=1}^{p^{l+t-1}} \binom{p^{l+t-1}}{i} a^i = \sum_{i=1}^{p^{l-1}} \binom{p^{l+t-1}}{ip^t} a^{ip^t}.$$

Seien nun $\alpha_f \in K$ für alle $f \in X^{\leq k} \setminus X^{\leq L(a)-1}$ so, dass $a = \sum_{f\in X^{\leq k}\setminus X^{\leq L(a)-1}} \alpha_f f$ ist. Da $o_+(a\pi_{\min}) = p^l$ ist und $K = \mathbb{Z}/p^l\mathbb{Z}$ gilt, existiert ein $f \in X^{=L(a)}$ mit $o_+(\alpha_f) = p^l$, also ist α_f eine Einheit in K. Nach Lemma 1.15 existiert ein $m \in \mathbb{N}$ mit $p \nmid m$ und $\binom{p^{l+t-1}}{p^t} = p^{l-1}m$. Damit ist $m\alpha_f^{p^t}$ eine Einheit in K und es folgt

$$\begin{aligned} a^{(p^{l+t-1})}\pi_{f^{p^t}} &= \sum_{i=1}^{p^{l-1}} \binom{p^{l+t-1}}{ip^t} a^{ip^t}\pi_{f^{p^t}} = \binom{p^{l+t-1}}{p^t} a^{p^t}\pi_{f^{p^t}} = p^{l-1}m(a\pi_f)^{p^t} \\ &= \underbrace{p^{l-1}m\alpha_f^{p^t}}_{\neq 0_K} f^{p^t} \neq 0. \end{aligned}$$

□

Korollar 1.35.2 Sei $K = \mathbb{Z}/c\mathbb{Z}$ für ein $c \in \mathbb{N}_{>1}$ mit $\mathrm{ggT}(c, k!) = 1$. Dann gilt

$$o_*(a) \mid c \qquad \text{für alle } a \in N.$$

Beweis. Für $a = 0$ ist die Behauptung klar. Sei $a \in N \setminus \{0\}$. Seien $q, r_1, \ldots, r_q \in \mathbb{N}$ und $p_1, \ldots, p_q \in \mathbb{P}$ paarweise verschieden mit $c = p_1^{r_1} \ldots p_q^{r_q}$. Dann gilt nach Voraussetzung $c_{k,p_i,1} = 0$ für alle $i \in \underline{q}$. Damit ist $L(a) \in I_{k,p_i,0}$ für alle $i \in \underline{q}$. Für alle $i \in \underline{q}$ bezeichnen wir mit $\varphi_i : N_{\mathbb{Z}/c\mathbb{Z}} \to N_{\mathbb{Z}/p_i^{r_i}\mathbb{Z}}$ die Fortsetzung des kanonischen Ring-Epimorphismus $\mathbb{Z}/c\mathbb{Z} \to \mathbb{Z}/p_i^{r_i}\mathbb{Z}$. Dann gilt mit Lemma 1.35

$$o_*(a\varphi_i) \mid p_i^{r_i}p^0 = p_i^{r_i} \quad \text{für alle } i \in \underline{q}.$$

Damit ist

$$a^{(c)} \in \bigcap_{i=1}^{q} \mathrm{Kern}\ \varphi_i = \bigcap_{i=1}^{q} N_{p_i^{r_i}\mathbb{Z}/c\mathbb{Z}} = \{0\}.$$

Damit folgt $o_*(a) \mid c$. □

Beispiel 1.36 Sei $K = \mathbb{Z}/3^3\mathbb{Z}$, $k = 10$ und $x \in X$. Es sei

$$a := x^2 \quad \text{und} \quad b := 9x + x^{10}.$$

Dann ist

$$o_+(a) = 3^3 = o_+(a\pi_{\min}) \quad \text{und} \quad o_+(b) = 3^3 \neq 3 = o_+(b\pi_{\min}).$$

Nach Beispiel 1.17 ist $L(a) = 2 \in I_1$ und $L(b) = 1 \in I_2$. Wir erhalten

$$\begin{aligned} \text{Korollar 1.35.1:} \quad & o_*(a) = 3^3 \cdot 3^1 = 3^4 \quad \text{und} \\ \text{Lemma 1.35:} \quad & o_*(b) \mid 3^3 \cdot 3^2 = 3^5. \end{aligned}$$

Tatsächlich gilt jedoch

$$\begin{aligned} b^{(3)} &= 3b + 3b^2 + b^3 = 3b = 3x^{10} \quad \text{und damit} \\ b^{(3^2)} &= 9x^{10} \neq 0 \text{ sowie} \\ b^{(3^3)} &= 27x^{10} = 0. \end{aligned}$$

Somit ist $o_*(b) = 3^3$.

Wir haben nun gesehen, dass es im Fall einer Primzahlpotenzcharakteristik möglich ist, Aussagen über Elementordnungen zu machen. Wir wollen nun zeigen, dass es in vielen Fällen genügt, sich mit diesen Grundringen zu beschäftigen.

Bemerkung 1.37 Sei X endlich und seien $c, m \in \mathbb{N}$ mit $(K, +) \cong ((\mathbb{Z}/c\mathbb{Z})^m, +)$ (mit K unitär ist $c \neq 1$). Seien $q, r_1, \ldots, r_q \in \mathbb{N}$ und $p_1, \ldots, p_q \in \mathbb{P}$ paarweise verschieden mit $c = p_1^{r_1} \ldots p_q^{r_q}$. Für alle $i \in \underline{q}$ sei $d_i := \frac{c}{p_i^{r_i}}$. Dann ist für alle $i \in \underline{q}$

$$d_i N = \left\{ \sum_{f \in X^{\leq k}} (d_i \alpha_f) f \mid \forall f \in X^{\leq k} : \alpha_f \in K \right\}$$

ein Ideal von N und es gilt $Syl_{p_i}(N) = \{d_i N\}$. Insbesondere ist $\{d_i N \mid i \in \underline{q}\}$ eine Idealzerlegung von N.

Beweis. Sei $b := |X^{\leq k}|$ und $i \in \underline{q}$. Da $d_i K$ ein Ideal von K ist, ist auch $d_i N$ ein Ideal von N. Zudem gilt

$$|d_i N| = |d_i K|^b = |d_i \mathbb{Z}/c\mathbb{Z}|^{mb} = \left(\frac{c}{d_i}\right)^{mb} = p_i^{r_i mb}.$$

Als Ideal ist $d_i N$ ein Normalteiler von $(N, +)$ und nach Bemerkung 1.3 (d) auch ein $*$-Normalteiler. Außerdem ist

$$|N| = |K|^b = c^{mb} = p_1^{r_1 mb} \ldots p_q^{r_q mb}.$$

Damit ist $p_i^{r_i mb} = |d_i N|$ die maximale p_i-Potenz, die $|N|$ teilt, also ist $d_i N$ sowohl additiv als auch bezüglich $*$ die einzige p_i-Sylowgruppe und diese bilden eine direkte Zerlegung von N bezüglich $+$ und $*$. Damit ist $\{d_i N \mid i \in \underline{q}\}$ eine Idealzerlegung von N. □

Satz 1.38 Sei X endlich und seien $c, q, r_1, \ldots, r_q \in \mathbb{N}$ und $p_1, \ldots, p_q \in \mathbb{P}$ paarweise verschieden mit $c = p_1^{r_1} \ldots p_q^{r_q}$. Für alle $i \in \underline{q}$ sei $d_i := \frac{c}{p_i^{r_i}}$. Dann ist für alle $i \in \underline{q}$

$$d_i N_{\mathbb{Z}/c\mathbb{Z}} \cong N_{\mathbb{Z}/p_i^{r_i}\mathbb{Z}} \text{ als } (\mathbb{Z}/p_i^{r_i}\mathbb{Z})\text{-Algebren.}$$

Insbesondere ist

$$N_{\mathbb{Z}/c\mathbb{Z}} \cong \bigoplus_{i=1}^{q} N_{\mathbb{Z}/p_i^{r_i}\mathbb{Z}} \quad \text{und damit}$$
$$(N_{\mathbb{Z}/c\mathbb{Z}}, *) \cong \bigtimes_{i=1}^{q} (N_{\mathbb{Z}/p_i^{r_i}\mathbb{Z}}, *).^3$$

Beweis. Sei $i \in \underline{q}$. Offenbar ist $d_i N_{\mathbb{Z}/c\mathbb{Z}}$ eine $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$-Algebra. Es sei

$$\varphi : N_{\mathbb{Z}/p_i^{r_i}\mathbb{Z}} \to d_i N_{\mathbb{Z}/c\mathbb{Z}} \quad \text{die Fortsetzung von} \quad x \mapsto d_i x \quad \text{für alle } x \in X.$$

Nach Definition ist dies ein $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$-Algebren-Homomorphismus. Es sind Definitions- und Bildbereich endlich und gleichmächtig, somit genügt es die Surjektivität von φ nachzuweisen. Es ist $d_i X^{\leq k}$ eine $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$-Basis von $d_i N_{\mathbb{Z}/c\mathbb{Z}}$ und damit genügt es, $d_i X^{\leq k} \subseteq$ Bild φ nachzuweisen. Sei dazu $g \in X^{\leq k}$, $l := L(g)$ und seien $x_1, \ldots, x_l \in X$ mit $g = x_1 \ldots x_l$. Wir setzen $\alpha := d_i^{l-1} + p_i^{r_i}\mathbb{Z}$. Dann ist α eine Einheit in $\mathbb{Z}/p_i^{r_i}\mathbb{Z}$ und es folgt

$$(\alpha^{-1} x_1 \ldots x_l)\varphi = \alpha^{-1} d_i^l x_1 \ldots x_l = \alpha^{-1}\alpha d_i g = d_i g.$$

Somit ist φ ein $(\mathbb{Z}/p_i^{r_i}\mathbb{Z})$-Algebren-Isomorphismus. Die Zerlegungsaussagen folgen nun aus Bemerkung 1.37. □

1.4 Elementarkommutatoren und elementare Lie-Klammern

In diesem Abschnitt sei X eine nichtleere Menge. Es sei $X^{(+)}$ das freie Magma über der Menge X und $l : X^{(+)} \to \mathbb{N}$ die Längenabbildung. Die Definition der Elementarelemente mit ihren Anwendungen in Lie-Algebren und Gruppen findet sich bereits in meiner Diplomarbeit [Han12, Kapitel 2.2]. Wir orientieren unsere Definitionen an dem Vorgehen von M. Hall in [Hal76, Chapter 11.1].

Die Elementarelemente in $X^{(+)}$ definieren wir rekursiv nach ihrer Länge:

[3] Einen weiteren Beweis dieser Aussagen erhält man mit $\mathbb{Z}/c\mathbb{Z} \cong \bigtimes_{i=1}^{q} \mathbb{Z}/p_i^{r_i}\mathbb{Z}$ nach dem chinesischen Restsatz und der Anwendung von Bemerkung 1.28.

Definition 1.39 Die Elementarelemente der Länge 1 sind die Elemente in X.
Es seien die Elementarelemente bis zur Länge $m-1$ für ein $m \in \mathbb{N}_{>1}$ bereits konstruiert und so angeordnet, dass für zwei Elementarelemente u, v stets gilt: $l(u) < l(v) \Rightarrow u \prec v$, wobei „$\prec$“ die gewählte Ordnung auf den bereits konstruierten Elementarelementen bezeichne.
Das Element (uv) heißt Elementarelement der Länge m falls gilt

- u, v sind Elementarelemente mit $l(u) + l(v) = m$,
- $u \succ v$ und
- ist $u = (ab)$ für Elementarelemente a, b, so ist $b \preceq v$.

Beispiel 1.40 Es sei $|X| = 2$, $X = \{x, y\}$. Es gelte $x \prec y$ und die weitere Ordnung der Elementarelemente sei durch ihre Reihenfolge in der Auflistung gegeben. Dann sind die folgenden Elemente in $X^{(+)}$ Elementarelemente:

Länge	Elementarelemente
1	x, y
2	(yx)
3	$((yx)x), ((yx)y)$
4	$(((yx)x)x), (((yx)x)y), (((yx)y)y)$
5	$(((yx)x)(yx)), (((yx)y)(yx)), ((((yx)x)x)x), ((((yx)x)x)y),$ $((((yx)x)y)y), ((((yx)y)y)y)$
$\vdots$	$\vdots$

Definition und Bemerkung 1.41 Ist X endlich, etwa $|X| = n$, so gibt es zu jeder Länge $i \in \mathbb{N}$ nur endlich viele Elementarelemente in $X^{(+)}$. Seien n_i die Anzahl der Elementarelemente von der Länge i und $e_{i,1}, \ldots, e_{i,n_i}$ die Elementarelemente von der Länge i, wobei für alle $j, k \in \underline{n_i}$ gelte: $j < k \Leftrightarrow e_{i,j} \prec e_{i,k}$. Wir setzen

$$\mathfrak{E}_i^{(+)} := (e_{i,1}, \ldots, e_{i,n_i})$$

als das Tupel der Elementarelemente von der Länge i. Insbesondere ist $n_1 = n$ und

$$\mathfrak{E}_1^{(+)} = (x_1, \ldots, x_n)$$

wobei $X = \{x_1, \ldots, x_n\}$.

Diese Definition wollen wir nun auf Lie-Algebren in assoziativen Algebren und auf Gruppen übertragen. Dazu sei $n \in \mathbb{N}$, X n-elementig, etwa $X = \{x_1, \ldots, x_n\}$.

Definition 1.42 Es sei A eine assoziative K-Algebra mit n-elementigem K-Algebren-Erzeugendensystem Y, $Y = \{y_1, \ldots, y_n\}$. Es sei α der durch $x \mapsto x$ für alle $x \in X$ definierte Homomorphismus des freien Magmas $X^{(+)}$ in $(F_{K,X}, [\cdot, \cdot])$. Weiter sei β der K-Algebren-Epimorphismus $F_{K,X} \to A$, der als Fortsetzung der Abbildung $x_i \mapsto y_i$ für alle $i \in \underline{n}$ entsteht. Dann heißen die Bilder der Elementarelemente unter der Abbildung

$\alpha\beta : X^{(+)} \to F_{K,X} \to A$ die elementaren Lie-Worte in A. Seien $i \in \mathbb{N}$ und $n_i, e_{i,1}, \ldots, e_{i,n_i}$ wie in Definition 1.41. Dann setzen wir

$$\mathfrak{E}_i^{\mathfrak{L},\beta} := (e_{i,1}\alpha\beta, \ldots, e_{i,n_i}\alpha\beta) \quad \text{und} \quad \mathfrak{E}_i^{\mathfrak{L}} := \mathfrak{E}_i^{\mathfrak{L},id}.$$

Wir ordnen jedem elementaren Lie-Wort e

$$\min\left\{l(u) \mid u \text{ ist Elementarelement in } X^{(+)}, u\alpha\beta = e\right\}$$

als Gewicht zu.

Beispiel 1.43 Wir betrachten die K-Algebra Δ der oberen 2×2-Matrizen über K. Es ist

$$E := \left\{E_1 := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, E_2 := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, E_3 := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right\}$$

ein K-Algebren-Erzeugendensystem von Δ (E ist sogar eine K-Raum-Basis). Nun sollen die elementaren Lie-Worte bezüglich dieses Erzeugendensystems bestimmt werden. Dabei sei $n = 3$, $X = \{x_1, x_2, x_3\}$ und es gelte $x_i\beta = E_i$ für alle $i \in \underline{3}$. Die elementaren Lie-Worte vom Gewicht 1 sind E_1, E_2, E_3. Es gilt $[E_3, E_1] = 0_\Delta$, $[E_3, E_2] = E_2$ und $[E_2, E_1] = E_2$, es entstehen also außer der Nullmatrix keine weiteren elementaren Lie-Worte. Damit ist die Menge der elementaren Lie-Worte $\{E_1, E_2, E_3, 0_\Delta, -E_2\}$ und es gilt (bei geeignet gewählter Reihenfolge der Elementarelemente in $\{x_1, x_2, x_3\}^{(+)}$ und linksnormierter Schreibweise):

$$\begin{aligned}
\mathfrak{E}_1^{\mathfrak{L},\beta} &= (E_1, E_2, E_3),\\
\mathfrak{E}_2^{\mathfrak{L},\beta} &= ([E_3, E_1], [E_3, E_2], [E_2, E_1]) = (0_\Delta, E_2, E_2),\\
\mathfrak{E}_3^{\mathfrak{L},\beta} &= ([E_3, E_1, E_1], [E_3, E_1, E_2], [E_3, E_1, E_3], [E_3, E_2, E_2], [E_3, E_2, E_3],\\
&\qquad [E_2, E_1, E_1], [E_2, E_1, E_2], [E_2, E_1, E_3])\\
&= (0_\Delta, 0_\Delta, 0_\Delta, 0_\Delta, -E_2, E_2, 0_\Delta, -E_2)
\end{aligned}$$

und in allen Tupeln $\mathfrak{E}_i^{\mathfrak{L},\beta}$ mit $i \geq 4$ kommen nur noch die Einträge $0_\Delta, E_2$ und $-E_2$ vor. Für alle $i \in \mathbb{N}$ ist

$$(\cdots((x_2 \underbrace{x_1)x_1)\cdots x_1)}_{i-1} \quad \text{ein Elementarelement von der Länge } i \text{ und somit}$$

$$[E_2, \underbrace{E_1, E_1, \ldots, E_1}_{i-1}] = E_2 \quad \text{ein Eintrag} \neq 0_\Delta \text{ in } \mathfrak{E}_i^{\mathfrak{L},\beta}.$$

Somit ist $\mathfrak{E}_i^{\mathfrak{L},\beta}$ für alle $i \in \mathbb{N}$ nicht das Nulltupel.

Wir notieren einige bekannte Aussagen über elementare Lie-Klammern:

Satz 1.44 Sei α der durch $x \mapsto x$ für alle $x \in X$ definierte Homomorphismus des freien Magmas $X^{(+)}$ in $(F_{K,X}, [\cdot,\cdot])$. Dann ist α eingeschränkt auf die Menge der Elementarelemente injektiv und

$$\left\{ e\alpha \mid e \text{ ist Elementarelement in } X^{(+)} \right\}$$

ist eine K-Basis der über X freien Lie-Algebra.
Ist zudem X endlich, etwa $|X| = n$, so gibt es genau

$$n_i = \frac{1}{i} \sum_{d|i} \mu(d) n^{\frac{i}{d}}$$

Elementarelemente von der Länge i in $X^{(+)}$ (beziehungsweise elementare Lie-Worte vom Gewicht i in $F_{K,X}$) für alle $i \in \mathbb{N}$, wobei μ die Möbius-Funktion bezeichne (Witt'sche Dimensionsformel).

Beweis. Nach [Bah87, Seite 51, Theorem 1] ist die Menge der elementaren Lie-Klammern eine K-Basis für die freie Lie-Algebra in $F_{K,X}$. Nach Definition der Elementarelemente erhalten wir damit, dass α eingeschränkt auf die Menge der Elementarelemente injektiv ist. Die Witt'sche Dimensionsformel findet sich beispielsweise in [Bah87, Seite 74, Theorem 1]. □

Die elementaren Lie-Worte bilden also eine K-Basis der in $F_{K,X}$ enthaltenen freien Lie-Algebra. Der folgende Satz zeigt, wie man aus den elementaren Lie-Worten eine K-Basis für $F_{K,X}$ selbst gewinnen kann. Es sei weiterhin X eine n-elementige Menge.

Satz 1.45 (Poincaré, Birkhoff, Witt 1937, Formulierung in der freien Algebra) Für alle $i \in \mathbb{N}$ seien $e_{i,1}, \ldots, e_{i,n_i} \in F_{K,X}$ mit $\mathfrak{E}_i^{\mathfrak{L}} = (e_{i,1}, \ldots, e_{i,n_i})$. Dann ist

$$\left\{ e_{i_1,j_1} \ldots e_{i_m,j_m} \mid m \in \mathbb{N}, (i_1,j_1) \underset{lex}{\leq} \ldots \underset{lex}{\leq} (i_m,j_m) \right\}$$

eine K-Basis von $F_{K,X}$. Insbesondere ist für alle $i \in \mathbb{N}$

$$\left\{ e_{i_1,j_1} \ldots e_{i_m,j_m} \mid m \in \mathbb{N}, (i_1,j_1) \underset{lex}{\leq} \ldots \underset{lex}{\leq} (i_m,j_m), \sum_{r=1}^{m} i_r = i \right\}$$

eine K-Basis von $F_{K,X}\pi_i$.

Beweis. Nach 1.44 ist die Menge der elementaren Lie-Klammern eine K-Basis für die freie Lie-Algebra $L_{K,X}$ in $F_{K,X}$. Da $F_{K,X}$ die universelle Einhüllende von $L_{K,X}$ ist [Reu93, Seite 6, Theorem 0.5], folgt die Behauptung aus dem Satz von Poincaré, Birkhoff und Witt [Bah87, Seite 58]. □

Nun wollen wir die Elementarelemente in Gruppen betrachten:

Definition 1.46 Es sei $\mathcal{G}$ eine Gruppe mit n-elementigem Erzeugendensystem Y, etwa $Y = \{y_1, \ldots, y_n\}$. Es bezeichne $\mathcal{F}_X$ die freie Gruppe über X. Es sei α der durch $x \mapsto x$ für alle $x \in X$ definierte Homomorphismus des freien Magmas $X^{(+)}$ in $(\mathcal{F}_X, (\cdot,\cdot))$ (hierbei bezeichne $(\cdot,\cdot)$ die Kommutatorbildung in $\mathcal{F}_X$). Weiter sei β der Gruppen-Epimorphismus $\mathcal{F}_X \to \mathcal{G}$ der als Fortsetzung der Abbildung $x_i \mapsto y_i$ für alle $i \in \underline{n}$ entsteht. Dann heißen die Bilder der Elementarelemente unter der Abbildung $\alpha\beta : X^{(+)} \to \mathcal{F}_X \to \mathcal{G}$ die Elementarkommutatoren in $\mathcal{G}$. Seien $i \in \mathbb{N}$ und $n_i, e_{i,1}, \ldots, e_{i,n_i}$ wie in Definition 1.41. Dann setzen wir

$$\mathfrak{E}_i^{\mathfrak{G},\beta} := (e_{i,1}\alpha\beta, \ldots, e_{i,n_i}\alpha\beta) \quad \text{und} \quad \mathfrak{E}_i^{\mathfrak{G}} := \mathfrak{E}_i^{\mathfrak{G},id}.$$

Wir ordnen jedem Elementarkommutator e

$$\min\left\{l(u) \mid u \text{ ist Elementarelement in } X^{(+)}, u\alpha\beta = e\right\}$$

als Gewicht zu.

Beispiel 1.47

1. Ist $\mathcal{G}$ abelsch, $Y = \{y_1, \ldots, y_n\}$ ein Erzeugendensystem von $\mathcal{G}$, so ist (bei geeigneter Wahl der Reihenfolge) $\mathfrak{E}_1^{\mathfrak{G},\beta} = (y_1, \ldots, y_n)$ und $\mathfrak{E}_i^{\mathfrak{G},\beta}$ das Nulltupel für alle $i > 1$, da jeder Kommutator in $\mathcal{G}$ trivial ist.

2. Wir betrachten die Quaternionengruppe $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ und wählen $n = 2$, $X = \{x, y\}$ und $\{i, j\}$ als Erzeugendensystem sowie $\beta : F(\{x, y\}) \to Q_8$ als die epimorphe Fortsetzung von $x \mapsto i$, $y \mapsto j$ wobei $x \prec y$ in $\{x, y\}^{(+)}$ gelte. Q_8 ist eine nilpotente Gruppe von der Klasse 2, also sind die Elementarkommutatoren vom Gewicht ≥ 3 trivial. Weiter gilt

$$(yx)(\alpha\beta) = (y, x)\beta = (y\beta, x\beta) = (j, i) = (-j)(-i)ji = (ji)^2 = (-k)^2 = -1.$$

Damit ergibt sich

$$\mathfrak{E}_1^{\mathfrak{G},\beta} = (i, j)$$
$$\mathfrak{E}_2^{\mathfrak{G},\beta} = (-1)$$

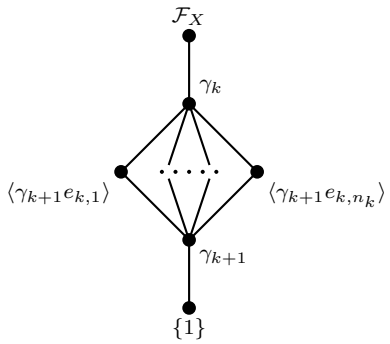
und $\mathfrak{E}_i^{\mathfrak{G},\beta}$ ist das Einstupel für alle $i > 2$.

Ein Beweis der folgenden Aussage findet sich beispielsweise in [Hal76, Seite 175, Theorem 11.2.4]. Weiterhin sei X eine n-elementige Menge.

Satz 1.48 Sei $\mathcal{F}_X$ die freie Gruppe über X. Für alle $i \in \mathbb{N}$ seien $e_{i,1}, \ldots, e_{i,n_i} \in \mathcal{F}_X$ mit $\mathfrak{E}_i^{\mathfrak{G}} = (e_{i,1}, \ldots, e_{i,n_i})$. Sei $f \in \mathcal{F}_X$, $k \in \mathbb{N}$ und $\gamma_{k+1}(\mathcal{F}_X)$ das $(k+1)$-te Glied der absteigenden Zentralreihe. Dann gibt es eindeutig bestimmte $\alpha_{i,j} \in \mathbb{Z}$ für alle $i \in \underline{k}$ und $j \in \underline{n_i}$ mit

$$\gamma_{k+1}(\mathcal{F}_X)f = \gamma_{k+1}(\mathcal{F}_X)\prod_{i=1}^{k}\prod_{j=1}^{n_i} e_{i,j}^{\alpha_{i,j}}.$$

Insbesondere gilt: Ist $\beta : \mathcal{F}_X \to \mathcal{F}_X/\gamma_{k+1}(\mathcal{F}_X)$ die kanonische Projektion, so ist $\mathfrak{E}_k^{\mathfrak{G},\beta}$ ein $\mathbb{Z}$-Basistupel für $\gamma_k(\mathcal{F})/\gamma_{k+1}(\mathcal{F})$ für alle $k \in \mathbb{N}$.



Korollar 1.48.1 Sei $\mathcal{G}$ eine nilpotente Gruppe der Klasse höchstens k, $Y = \{y_1, \ldots, y_n\}$ ein Erzeugendensystem von $\mathcal{G}$ und $\beta : \mathcal{F}_X \to \mathcal{G}$ die homomorphe Fortsetzung der Abbildung $x_i \mapsto y_i$ für alle $i \in \underline{n}$. Weiter seien $e_{i,1}, \ldots, e_{i,n_i} \in \mathcal{G}$ mit $\mathfrak{E}_i^{\mathfrak{G},\beta} = (e_{i,1}, \ldots, e_{i,n_i})$ für alle $i \in \mathbb{N}$. Dann gilt

$$\mathcal{G} = \left\{ \prod_{i=1}^{k} \prod_{j=1}^{n_i} e_{i,j}^{\alpha_{i,j}} \mid \forall i \in \underline{k}, j \in \underline{n_i} : \alpha_{i,j} \in \mathbb{Z} \right\}.$$

Ist insbesondere $\mathcal{G}$ endlich, so folgt

$$|\mathcal{G}| \leq \prod_{i=1}^{k} \prod_{j=1}^{n_i} o(e_{i,j}).$$

Beispiel 1.49

1. Wir betrachten das Beispiel 1.47, Teil 2. Dann gilt mit $o(-1) = 2$ und $o(i) = 4 = o(j)$

$$Q_8 = \left\{ i^\alpha j^\beta (-1)^\gamma \mid \alpha, \beta \in \{0,1,2,3\}, \gamma \in \{0,1\} \right\}.$$

   Außerdem ist $|Q_8| = 8 \leq 32 = 4 \cdot 4 \cdot 2$. Diese Darstellung der Q_8 liefert damit keine eindeutige Elementdarstellung.

2. Wir betrachten die Diedergruppe D_8 der Ordnung 8 in der symmetrischen Gruppe S_4 mit der Erzeugermenge $\{(13), (12)(34)\}$. Sei $\beta : F(\{x,y\}) \to D_8$ die epimorphe Fortsetzung von $x \mapsto (13)$, $y \mapsto (12)(34)$ wobei $x \prec y$ in $\{x,y\}^{(+)}$ gelte. Dann ist

$$\mathfrak{E}_1^{\mathfrak{G},\beta} = ((13), (12)(34)),\ \mathfrak{E}_2^{\mathfrak{G},\beta} = ((13)(34))$$

   und $\mathfrak{E}_i^{\mathfrak{G},\beta}$ ist das Nulltupel für alle $i \geq 3$. Es folgt

$$D_8 = \left\{ (13)^\alpha ((12)(34))^\beta ((13)(24))^\gamma \mid \alpha, \beta, \gamma \in \{0,1\} \right\}$$

   mit $2 = o((13)) = o((12)(34)) = o((13)(24))$. Es ist $|D_8| = 8 = 2^3$ und damit ist hier die Elementdarstellung eindeutig.

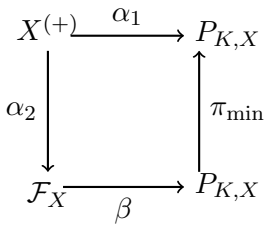
Wir wollen nun den Zusammenhang der elementaren Lie-Worte und Elementarkommutatoren (bezüglich $*$) in N betrachten.

Lemma 1.50 Sei $\beta : \mathcal{F}_X \to (P_{K,X}, *)$ die homomorphe Fortsetzung der Abbildung $x \mapsto x$ für alle $x \in X$. Dann gilt für alle $i \in \mathbb{N}$

$$\mathfrak{E}_i^{\mathfrak{L}} = \mathfrak{E}_i^{\mathfrak{G},\beta} \pi_{\min}.^4$$

[4] Wir verstehen die Anwendung von $\pi_{\min}$ auf das Tupel $\mathfrak{E}_i^{\mathfrak{G},\beta}$ komponentenweise.

Beweis. Für alle $i \in \mathbb{N}$ seien $e_{i,1}, \dots e_{i,n_i} \in X^{(+)}$ mit $\mathfrak{E}_i^{(+)} = (e_{i,1}, \dots, e_{i,n_i})$. Seien $\alpha_1 : X^{(+)} \to (F_{K,X}, [\cdot,\cdot])$ und $\alpha_2 : X^{(+)} \to (\mathcal{F}_X, (\cdot,\cdot))$ jeweils die homomorphe Fortsetzung von $x \mapsto x$ für alle $x \in X$. Dann gilt für alle $i \in \mathbb{N}$



$$\mathfrak{E}_i^{\mathfrak{L}} = (e_{i,1}\alpha_1, \dots, e_{i,n_i}\alpha_1) \quad \text{und}$$
$$\mathfrak{E}_i^{\mathfrak{G},\beta}\pi_{\min} = (e_{i,1}\alpha_2\beta\pi_{\min}, \dots, e_{i,n_i}\alpha_2\beta\pi_{\min}).$$

Wir zeigen nun induktiv nach i:

$$\forall j \in \underline{n_i} : e_{i,j}\alpha_1 = e_{i,j}\alpha_2\beta\pi_{\min}$$

Sei $i = 1$ und $j \in \underline{n_1}$. Dann existiert $x \in X$ mit $e_{1,j} = x$ und es folgt

$$e_{1,j}\alpha_1 = x\alpha_1 = x = x\pi_{\min} = x\beta\pi_{\min} = x\alpha_2\beta\pi_{\min}.$$

Sei nun $i > 1$ und $j \in \underline{n_i}$. Dann existieren Elementarelemente $f, g \in X^{(+)}$, $l(f), l(g) < i$, mit $e_{i,j} = (fg)$. Es sind $f\alpha_2\beta$, $g\alpha_2\beta$ und $[f\alpha_2\beta, g\alpha_2\beta]_*$ Elementarkommutatoren und nach Induktionsvoraussetzung sind $f\alpha_2\beta\pi_{\min}$ und $g\alpha_2\beta\pi_{\min}$ elementare Lie-Klammern. Damit ist auch $[f\alpha_2\beta\pi_{\min}, g\alpha_2\beta\pi_{\min}]$ eine elementare Lie-Klammer und als solche nach Satz 1.44 in einer Basis enthalten. Damit ist insbesondere $[f\alpha_2\beta\pi_{\min}, g\alpha_2\beta\pi_{\min}] \neq 0$ und es folgt

$$(\star) \qquad [f\alpha_2\beta\pi_{\min}, g\alpha_2\beta\pi_{\min}] \;=\; [f\alpha_2\beta, g\alpha_2\beta]\pi_{\min} \overset{1.22}{=} [f\alpha_2\beta, g\alpha_2\beta]_*\pi_{\min}.$$

Wir erhalten

$$\begin{aligned} e_{i,j}\alpha_1 &= (fg)\alpha_1 \\ &= [f\alpha_1, g\alpha_1] \\ &\overset{\text{I.V.}}{=} [f\alpha_2\beta\pi_{\min}, g\alpha_2\beta\pi_{\min}] \\ &\overset{(\star)}{=} [f\alpha_2\beta, g\alpha_2\beta]_*\pi_{\min} \\ &= (f\alpha_2, g\alpha_2)\beta\pi_{\min} \\ &= (fg)\alpha_2\beta\pi_{\min} \\ &= e_{i,j}\alpha_2\beta\pi_{\min}. \end{aligned}$$

□

Korollar 1.50.1 Ist $k \in \mathbb{N}$ und $\beta : \mathcal{F}_X \to (N_{K,X,k}, *)$ die homomorphe Fortsetzung der Abbildung $x \mapsto x$ für alle $x \in X$, so gilt

$$\mathfrak{E}_i^{\mathfrak{L}} = \mathfrak{E}_i^{\mathfrak{G},\beta}\pi_{\min} \quad \text{für alle } i \in \underline{k}.$$

Beispiel 1.51 Sei $|X| = 2$, $X = \{x, y\}$, und die Reihenfolge der Elementarelemente in $X^{(+)}$ wie in Beispiel 1.40. Sei β wie in Korollar 1.50.1. Dann gilt

$$n_3 \overset{1.44}{=} \frac{1}{3}\left(\mu(1)2^3 + \mu(3)2^1\right) = \frac{8-2}{3} = 2,$$
$$\mathfrak{E}_3^{\mathfrak{L}} = ([[y,x],x],[[y,x],y]) \quad \text{und}$$
$$\mathfrak{E}_3^{\mathfrak{G},\beta}\pi_{\min} = ([[y,x]_*,x]_*\pi_{\min}, [[y,x]_*,y]_*\pi_{\min}) \overset{1.11(c)}{=} ([[y,x],x],[[y,x],y]).$$

Wir wollen nun eine alternative Basis zu $X^{\leq k}$ für N angeben.

Lemma 1.52 Sei $k \in \mathbb{N}$, X n-elementig und $\beta : \mathcal{F}_X \to (N_{K,X,k}, *)$ die homomorphe Fortsetzung von $x \mapsto x$ für alle $x \in X$. Für alle $i \in \underline{k}$ sei $\mathfrak{E}_i^{\mathfrak{G},\beta} = (e_{i,1}, \ldots, e_{i,n_i})$. Wir setzen für alle $i \in \underline{k}$

$$B_i := \left\{ e_{i_1,j_1} \ldots e_{i_m,j_m} \middle| m \in \mathbb{N}, i_1, \ldots, i_m \in \underline{k}, \forall t \in \underline{m} : j_t \in \underline{n_{i_t}}, \right.$$
$$\left. (i_1, j_1) \underset{lex}{\leq} \ldots \underset{lex}{\leq} (i_m, j_m), \sum_{r=1}^{m} i_r = i \right\}$$

und $B := \cup_{i \in \underline{k}} B_i$. Dann ist B eine K-Basis von $N_{K,X,k}$.

Beweis. Für alle $i \in \underline{n}$ ist $B_i \subseteq N^i$ und mit Korollar 1.50.1 ist nach Satz 1.45 $B_i\pi_i$ eine K-Basis für $N_{K,X,k}\pi_i = F_{K,X}\pi_i$. Nach Lemma 1.31 ist dann B eine K-Basis von $N_{K,X,k}$. □

Bemerkung 1.53 Sei $p \in \mathbb{P}$, $l \in \mathbb{N}$ und $K = \mathbb{Z}/p^l\mathbb{Z}$. Sei $k \in \mathbb{N}$, X n-elementig und $e \in N_{K,X,k}$ ein Elementarkommutator vom Gewicht $i \in \underline{k}$, sowie $t \in \underline{s_{k,p}}$ mit $i \in I_{k,p,t}$. Dann ist $o(e) = p^{l+t}$.
Insbesondere haben Elementarkommutatoren vom gleichen Gewicht die gleiche Ordnung.

Beweis. Nach Korollar 1.50.1 ist $e\pi_{\min}$ eine elementare Lie-Klammer und damit nach Satz 1.44 Element einer K-Basis. Damit ist $o_+(e\pi_{\min}) = p^l$ und nach Korollar 1.35.1 ist $o(e) = p^{l+t}$. □

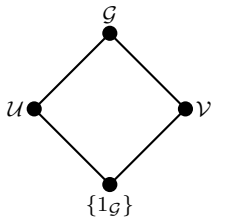
1.5 Eindeutige Darstellungen in Gruppen

Es bezeichne $\mathfrak{G}$ die Klasse der Gruppen. Es sei stets $\mathcal{G} \in \mathfrak{G}$.

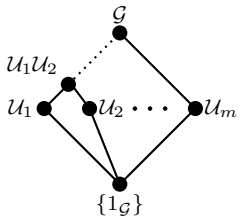
Bezeichnungen 1.54 Für alle $i \in \mathbb{N}_0$ sei $Z_i(\mathcal{G})$ das i-te Glied der aufsteigenden Zentralreihe (es ist $Z_0(\mathcal{G}) = \{1_\mathcal{G}\}$) und für alle $i \in \mathbb{N}$ sei $\gamma_i(\mathcal{G})$ das i-te Glied der absteigenden Zentralreihe (es ist $\gamma_1(\mathcal{G}) = \mathcal{G}$). Ist in dem gegebenen Kontext $\mathcal{G}$ eindeutig bestimmt, so schreiben wir auch Z_i und γ_i.

Definition 1.55

(a) Seien $\mathcal{U}, \mathcal{V} \leq \mathcal{G}$. Wir nennen $(\mathcal{U}, \mathcal{V})$ eine Zerlegung von $\mathcal{G}$, falls $\mathcal{U}\mathcal{V} = \mathcal{G}$ und $\mathcal{U} \cap \mathcal{V} = \{1_\mathcal{G}\}$ ist.



(b) Seien $m \in \mathbb{N}$ und $\mathcal{U}_1, \ldots, \mathcal{U}_m \leq \mathcal{G}$. Wir nennen $(\mathcal{U}_1, \ldots, \mathcal{U}_m)$ eine Zerlegung von $\mathcal{G}$, falls $\prod_{i=1}^m \mathcal{U}_i = \mathcal{G}$ gilt, $\prod_{i=1}^j \mathcal{U}_i$ für alle $j \in \underline{m}$ eine Untergruppe von $\mathcal{G}$ ist und $(\prod_{i=1}^j \mathcal{U}_i, \mathcal{U}_{j+1})$ für alle $j \in \underline{m-1}$ eine Zerlegung von $\prod_{i=1}^{j+1} \mathcal{U}_i$ ist.



Bemerkung 1.56 Seien $m \in \mathbb{N}$ und $\mathcal{U}_1, \ldots, \mathcal{U}_m \leq \mathcal{G}$. Dann sind äquivalent:

(i) $\prod_{i=1}^m \mathcal{U}_i = \mathcal{G}$ und $(\mathcal{U}_j, \prod_{i=j+1}^m \mathcal{U}_i)$ ist für alle $j \in \underline{m}$ eine Zerlegung von $\prod_{i=j}^m \mathcal{U}_i$.

(ii) $(\mathcal{U}_m, \ldots, \mathcal{U}_1)$ ist eine Zerlegung in $\mathcal{G}$.

Es übertragen sich die folgenden Aussagen entsprechend.

Das folgende Lemma zeigt die Äquivalenz von einer Zerlegung einer Gruppe mit der eindeutigen Darstellung ihrer Elemente.

Lemma 1.57 Seien $m \in \mathbb{N}$ und $\mathcal{U}_1, \ldots, \mathcal{U}_m \leq \mathcal{G}$. Für alle $j \in \underline{m}$ sei $\mathcal{H}_j := \prod_{i=1}^j \mathcal{U}_i$ eine Untergruppe von $\mathcal{G}$. Dann sind äquivalent:

(i) $(\mathcal{U}_1, \ldots, \mathcal{U}_m)$ ist eine Zerlegung von $\mathcal{H}_m$.

(ii) Sind $u_i, v_i \in \mathcal{U}_i$ für alle $i \in \underline{m}$ mit $\prod_{i=1}^m u_i = \prod_{i=1}^m v_i$, so folgt $u_i = v_i$ für alle $i \in \underline{m}$.

(iii) Ist $u_i \in \mathcal{U}_i$ für alle $i \in \underline{m}$ mit $\prod_{i=1}^m u_i = 1_\mathcal{G}$, so folgt $u_i = 1_\mathcal{G}$ für alle $i \in \underline{m}$.

Beweis. (i) $\Rightarrow$ (ii): Sei $(\mathcal{U}_1, \ldots, \mathcal{U}_m)$ eine Zerlegung von $\mathcal{H}_m$. Wir setzen $\mathcal{H}_0 := \{1_\mathcal{G}\}$. Seien $u_i, v_i \in \mathcal{U}_i$ für alle $i \in \underline{m}$ mit $\prod_{i=1}^m u_i = \prod_{i=1}^m v_i$. Gäbe es $t \in \underline{m}$ maximal mit $u_t \neq v_t$, so folgte

$$\prod_{i=1}^t u_i = \prod_{i=1}^t v_i \;\Rightarrow\; u_t v_t^{-1} = \left(\prod_{i=1}^{t-1} u_i\right)^{-1} \prod_{i=1}^{t-1} v_i \in \mathcal{U}_t \cap \mathcal{H}_{t-1},$$

da nach Voraussetzung $\mathcal{H}_{t-1}$ eine Untergruppe von G ist. Nach (i) ist $\mathcal{U}_t \cap \mathcal{H}_{t-1} = \{1_\mathcal{G}\}$ und somit folgte $u_t = v_t$, ein Widerspruch.
(ii) $\Rightarrow$ (iii): Dies ist trivial.
(iii) $\Rightarrow$ (i): Es gelte (iii). Sei $t \in \underline{m-1}$. Sei $u_{t+1} \in \mathcal{H}_t \cap \mathcal{U}_{t+1}$. Dann existieren $u_i \in \mathcal{U}_i$ für alle $i \in \underline{t}$ mit $u_{t+1} = \prod_{i=1}^t u_i$. Es folgt $1_\mathcal{G} = (\prod_{i=1}^t u_i) u_{t+1}^{-1}$. Mit (iii) folgt insbesondere $u_{t+1} = 1_\mathcal{G}$, also $\mathcal{H}_t \cap \mathcal{U}_{t+1} = \{1_\mathcal{G}\}$. Damit ist $(\mathcal{U}_1, \ldots, \mathcal{U}_m)$ eine Zerlegung von $\mathcal{H}_m$. $\square$

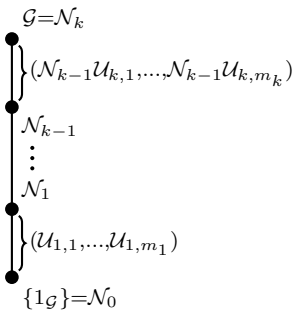
Wir werden nun sehen, unter welchen Voraussetzungen aus Zerlegungen von Faktorstücken einer Gruppe eine Zerlegung der ganzen Gruppe konstruiert werden kann.

Satz 1.58 Sei $k \in \mathbb{N}$ und $\{1_\mathcal{G}\} = \mathcal{N}_0 \trianglelefteq \cdots \trianglelefteq \mathcal{N}_k = \mathcal{G}$ eine Subnormalreihe in $\mathcal{G}$. Für alle $i \in \underline{k}$ sei $m_i \in \mathbb{N}$ und $\mathcal{U}_{i,1}, \ldots \mathcal{U}_{i,m_i} \leq \mathcal{G}$, sodass

$$(\mathcal{N}_{i-1}\mathcal{U}_{i,1}/\mathcal{N}_{i-1}, \ldots, \mathcal{N}_{i-1}\mathcal{U}_{i,m_i}/\mathcal{N}_{i-1})$$

eine Zerlegung von $\mathcal{N}_i/\mathcal{N}_{i-1}$ ist. Für alle $i \in \underline{k}$ und $j \in \underline{m_i}$ sei

$$\mathcal{H}_{i,j} := \left(\prod_{r=1}^{i-1}\prod_{s=1}^{m_r}\mathcal{U}_{r,s}\right)\prod_{s=1}^{j}\mathcal{U}_{i,s}.$$



Dann gilt:

(a) Für alle $i \in \underline{k}$ und $j \in \underline{m_i}$ ist $\mathcal{H}_{i,m_i} = \mathcal{N}_i$ und $\mathcal{H}_{i,j} = \mathcal{N}_{i-1}\prod_{s=1}^{j}\mathcal{U}_{i,s}$.

(b) Für alle $i \in \underline{k}$ und $j \in \underline{m_i}$ ist $\mathcal{H}_{i,j}$ eine Untergruppe von $\mathcal{G}$.

(c) Gilt $\mathcal{U}_{i,j} \cap \mathcal{N}_{i-1} = \{1_\mathcal{G}\}$ für alle $i \in \underline{k}$ und $j \in \underline{m_i}$, so ist

$$(\mathcal{U}_{1,1}, \mathcal{U}_{1,2}, \ldots, \mathcal{U}_{1,m_1}, \mathcal{U}_{2,1}, \ldots, \mathcal{U}_{k,m_k})$$

eine Zerlegung von $\mathcal{G}$.

Beweis. (a) Wir zeigen zunächst $\mathcal{H}_{i,m_i} = \mathcal{N}_i$ induktiv nach i. Dabei ist für $i = 1$ nach Voraussetzung $(\mathcal{U}_{1,1}, \ldots, \mathcal{U}_{1,m_1})$ eine Zerlegung von $\mathcal{N}_1$ und damit

$$\mathcal{H}_{1,m_1} = \prod_{s=1}^{m_1}\mathcal{U}_{1,s} = \mathcal{N}_1.$$

Sei nun $i > 1$. Dann gilt

$$\mathcal{N}_i/\mathcal{N}_{i-1} \overset{\text{Vor.}}{=} \prod_{s=1}^{m_i}(\mathcal{N}_{i-1}\mathcal{U}_{i,s}/\mathcal{N}_{i-1}) = \left(\prod_{s=1}^{m_i}\mathcal{N}_{i-1}\mathcal{U}_{i,s}\right)/\mathcal{N}_{i-1} = \mathcal{N}_{i-1}\left(\prod_{s=1}^{m_i}\mathcal{U}_{i,s}\right)/\mathcal{N}_{i-1}$$

mit $\mathcal{N}_{i-1} \trianglelefteq \mathcal{N}_i$ und $\mathcal{U}_{i,s} \leq \mathcal{N}_i$. Also ist

$$\mathcal{N}_i = \mathcal{N}_{i-1}\prod_{s=1}^{m_i}\mathcal{U}_{i,s} \overset{\text{I.V.}}{=} \mathcal{H}_{i-1,m_{i-1}}\prod_{s=1}^{m_i}\mathcal{U}_{i,s} = \mathcal{H}_{i,m_i}.$$

Sei nun $i \in \underline{k}$ und $j \in \underline{m_i}$. Dann gilt mit obigen Betrachtungen und $\mathcal{H}_{0,m_0} := \{1_\mathcal{G}\}$

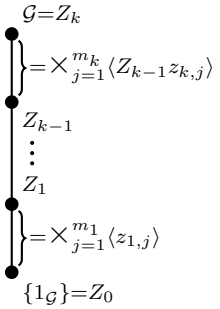
$$\mathcal{H}_{i,j} \overset{\text{Def.}}{=} \mathcal{H}_{i-1,m_{i-1}}\prod_{s=1}^{j}\mathcal{U}_{i,s} = \mathcal{N}_{i-1}\prod_{s=1}^{j}\mathcal{U}_{i,s}.$$

(b) Sei $i \in \underline{k}$ und $j \in \underline{m_i}$. Es ist nach Voraussetzung $\mathcal{H}_{i,j}/\mathcal{N}_{i-1} \overset{(a)}{=} (\mathcal{N}_{i-1}\prod_{s=1}^{j}\mathcal{U}_{i,s})/\mathcal{N}_{i-1}$ eine Untergruppe von $\mathcal{N}_i/\mathcal{N}_{i-1}$ und damit ist $\mathcal{H}_{i,j}$ Untergruppe von $\mathcal{G}$.
(c) Es gelte $\mathcal{U}_{i,j} \cap \mathcal{N}_{i-1} = \{1_G\}$ für alle $i \in \underline{k}$ und $j \in \underline{m_i}$. Es sei $\mathcal{H}_{0,m_0} := \{1_\mathcal{G}\}$.
Sei $i \in \underline{k}$ und $j \in \underline{m_i}$. Ist $j = 1$, so ist $\mathcal{H}_{i-1,m_{i-1}} \cap \mathcal{U}_{i,1} = \{1_\mathcal{G}\}$ zu zeigen. Dies gilt nach Voraussetzung und (a). Sei nun $j > 1$. Dann ist $\mathcal{H}_{i,j-1} \cap \mathcal{U}_{i,j} = \{1_G\}$ zu zeigen. Sei $u \in \mathcal{H}_{i,j-1} \cap \mathcal{U}_{i,j}$. Dann existieren $u_s \in \mathcal{U}_{i,s}$ für alle $s \in \underline{j-1}$ mit $\mathcal{N}_{i-1}u = \prod_{s=1}^{j-1}\mathcal{N}_{i-1}u_s$. Mit Lemma 1.57 folgt $\mathcal{N}_{i-1}u = \mathcal{N}_{i-1}$, also $u \in \mathcal{U}_{i,j} \cap \mathcal{N}_{i-1} \overset{\text{Vor.}}{=} \{1_\mathcal{G}\}$. □

Diesen Satz wenden wir nun auf die auf- oder absteigende Zentralreihe in einer endlich erzeugten nilpotenten Gruppe an:

Korollar 1.58.1 Sei $k \in \mathbb{N}$, $\mathcal{G}$ nilpotent von der Klasse k und endlich erzeugt. Für alle $i \in \underline{k}$ seien $m_i \in \mathbb{N}$ und $z_{i,1}, \ldots, z_{i,m_i} \in Z_i$ mit

$$Z_i/Z_{i-1} = \bigtimes_{j=1}^{m_i} \langle Z_{i-1} z_{i,j} \rangle.$$



Für alle $i \in \underline{k}$ und alle $j \in \underline{m_i}$ setzen wir

$$\mathcal{H}_{i,j} := \left(\prod_{r=1}^{i-1} \prod_{s=1}^{m_r} \langle z_{r,s} \rangle \right) \prod_{s=1}^{j} \langle z_{i,s} \rangle$$

und

$$O_{i,j} := \begin{cases} \underline{o(z_{i,j}) - 1} & o(z_{i,j}) \text{ ist endlich} \\ \mathbb{Z} & \text{sonst} \end{cases}.$$

Dann gilt:

(a) Für alle $i \in \underline{k}$ und $j \in \underline{m_i}$ ist $\mathcal{H}_{i,m_i} = Z_i$ und $\mathcal{H}_{i,j} = Z_{i-1} \prod_{s=1}^{j} \langle z_{i,s} \rangle$.

(b) Für alle $i \in \underline{k}$ und $j \in \underline{m_i}$ ist $\mathcal{H}_{i,j} \trianglelefteq \mathcal{G}$.

(c) Ist $Z_{i-1} \cap \langle z_{i,j} \rangle = \{1_\mathcal{G}\}$ für alle $i \in \underline{k}$ und $j \in \underline{m_i}$ so gilt

$$\mathcal{G} = \left\{ \prod_{i=1}^{k} \prod_{j=1}^{m_i} z_{i,j}^{\alpha_{i,j}} \mid \forall i \in \underline{k}, j \in \underline{m_i} \colon \alpha_{i,j} \in O_{i,j} \right\}$$

und die Darstellung der Elemente von $\mathcal{G}$ in dieser Form ist eindeutig.

Beweis. $\{1_\mathcal{G}\} = Z_0, \ldots, Z_k = \mathcal{G}$ ist eine Normalreihe in $\mathcal{G}$. Wir setzen $\mathcal{U}_{i,j} := \langle z_{i,j} \rangle$ für alle $i \in \underline{k}$ und $j \in \underline{m_i}$. Dann ist für alle $i \in \underline{k}$

$$(Z_{i-1}\mathcal{U}_{i,1}/Z_{i-1}, \ldots, Z_{i-1}\mathcal{U}_{i,m_i}/Z_{i-1})$$

eine Zerlegung von Z_i/Z_{i-1}. Damit folgt (a) aus Satz 1.58 (a), für alle $i \in \underline{k}$ und alle $j \in \underline{m_i}$ ist $\mathcal{H}_{i,j}$ eine Untergruppe von $\mathcal{G}$ und mit $\mathcal{H}_{i,j}/Z_{i-1} \leq Z_i/Z_{i-1} = Z(\mathcal{G}/Z_{i-1})$ folgt $\mathcal{H}_{i,j}/Z_{i-1} \trianglelefteq \mathcal{G}/Z_{i-1}$, also $\mathcal{H}_{i,j} \trianglelefteq \mathcal{G}$.
Gilt nun $Z_{i-1} \cap \mathcal{U}_{i,j} = \{1_\mathcal{G}\}$ für alle $i \in \underline{k}$ und $j \in \underline{m_i}$, so ist nach Satz 1.58 (c)

$$(\mathcal{U}_{1,1}, \mathcal{U}_{1,2}, \ldots, \mathcal{U}_{k,m_k})$$

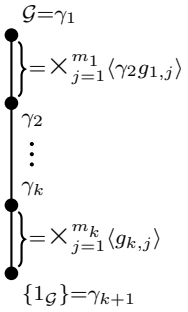
eine Zerlegung von G. Damit folgt

$$\mathcal{G} = \left\{ \prod_{i=1}^{k} \prod_{j=1}^{m_i} z_{i,j}^{\alpha_{i,j}} \mid \forall i \in \underline{k}, j \in \underline{m_i} \colon \alpha_{i,j} \in O_{i,j} \right\}$$

und die Eindeutigkeit der Darstellung aus Lemma 1.57. □

Korollar 1.58.2 Sei $k \in \mathbb{N}$, $\mathcal{G}$ nilpotent von der Klasse k und endlich erzeugt.
Für alle $i \in \underline{k}$ seien $m_i \in \mathbb{N}$ und $g_{i,1}, \ldots, g_{i,m_i} \in \gamma_i$ mit

$$\gamma_i/\gamma_{i+1} = \bigtimes_{j=1}^{m_i} \langle \gamma_{i+1} g_{i,j} \rangle.$$



Für alle $i \in \underline{k}$ und alle $j \in \underline{m_{k+1-i}}$ setzen wir

$$\mathcal{H}_{i,j} := \left(\prod_{r=1}^{i-1} \prod_{s=1}^{m_{k+1-r}} \langle g_{k+1-r,m_{k+1-r}+1-s} \rangle \right) \prod_{s=1}^{j} \langle g_{k+1-i,m_{k+1-i}+1-s} \rangle$$

und

$$O_{i,j} := \begin{cases} \underline{o(g_{i,j}) - 1} & o(g_{i,j}) \text{ ist endlich} \\ \mathbb{Z} & \text{sonst} \end{cases}.$$

Dann gilt:

(a) Für alle $i \in \underline{k}$ und $j \in \underline{m_{k+1-i}}$ ist

$$\mathcal{H}_{i,m_{k+1-i}} = \gamma_{k+1-i} \text{ und } \mathcal{H}_{i,j} = \gamma_{k+2-i} \prod_{s=1}^{j} \langle g_{k+1-i,m_{k+1-i}+1-s} \rangle.$$

(b) Für alle $i \in \underline{k}$ und $j \in \underline{m_{k+1-i}}$ ist $\mathcal{H}_{i,j} \trianglelefteq \mathcal{G}$.

(c) Ist $\gamma_{i+1} \cap \langle g_{i,j} \rangle = \{1_\mathcal{G}\}$ für alle $i \in \underline{k}$ und $j \in \underline{m_i}$ so gilt

$$\mathcal{G} = \left\{ \prod_{i=1}^{k} \prod_{j=1}^{m_i} g_{i,j}^{\alpha_{i,j}} \mid \forall i \in \underline{k}, j \in \underline{m_i} : \alpha_{i,j} \in O_{i,j} \right\}$$

und die Darstellung der Elemente von $\mathcal{G}$ in dieser Form ist eindeutig.

(d) Es gilt $m_i \leq \frac{1}{i} \sum_{d|i} \mu(d) m_1^{\frac{i}{d}}$ für alle $i \in \underline{k}$.

Beweis. $\{1_\mathcal{G}\} = \gamma_{k+1}, \ldots, \gamma_1 = \mathcal{G}$ ist eine Normalreihe in $\mathcal{G}$. Wir setzen $\mathcal{U}_{i,j} := \langle g_{i,j} \rangle$ für alle $i \in \underline{k}$ und $j \in \underline{m_i}$. Dann ist für alle $i \in \underline{k}$

$$(\gamma_{k+2-i}\mathcal{U}_{i,m_i}/\gamma_{k+2-i}, \ldots, \gamma_{k+2-i}\mathcal{U}_{i,1}/\gamma_{k+2-i})$$

eine Zerlegung von $\gamma_{k+1-i}/\gamma_{k+2-i}$. Damit folgt (a) aus Satz 1.58 (a), für alle $i \in \underline{k}$ und alle $j \in \underline{m_{k+1-i}}$ ist $\mathcal{H}_{i,j}$ eine Untergruppe von $\mathcal{G}$ und mit

$$\mathcal{H}_{i,j}/\gamma_{k+2-i} \leq \gamma_{k+1-i}/\gamma_{k+2-i} \leq Z(\mathcal{G}/\gamma_{k+2-i})$$

folgt $\mathcal{H}_{i,j}/\gamma_{k+2-i} \trianglelefteq \mathcal{G}/\gamma_{k+2-i}$, also $\mathcal{H}_{i,j} \trianglelefteq \mathcal{G}$.
Gilt nun $\gamma_{i+1} \cap \mathcal{U}_{i,j} = \{1_\mathcal{G}\}$ für alle $i \in \underline{k}$ und $j \in \underline{m_i}$, so ist nach Satz 1.58 (c)

$$(\mathcal{U}_{k,m_k}, \mathcal{U}_{k,m_k-1}, \ldots, \mathcal{U}_{k,1}, \mathcal{U}_{k-1,m_{k-1}}, \ldots, \mathcal{U}_{1,1})$$

eine Zerlegung von G. Da $\mathcal{G} = \{g^{-1} \mid g \in \mathcal{G}\}$ ist, folgt damit

$$\mathcal{G} = \left\{ \prod_{i=1}^{k} \prod_{j=1}^{m_i} g_{i,j}^{\alpha_{i,j}} \mid \forall i \in \underline{k}, j \in \underline{m_{ij}} \colon \alpha_{i,j} \in O_{i,j} \right\}$$

und die Eindeutigkeit der Darstellung aus Lemma 1.57.
(d) Sei $n := m_1$, X eine n-elementige Menge, $X = \{x_1, \ldots, x_n\}$, $\mathcal{F}_X$ die freie Gruppe über X und $\varphi : \mathcal{F}_X \to \mathcal{G}$ die homomorphe Fortsetzung der Abbildung $x_j \mapsto g_{1,j}$ für alle $j \in \underline{n}$. Für alle $i \in \underline{k}$ und $j \in \underline{n_{ij}}$ sei $e_{i,j} \in \mathcal{G}$ mit

$$\mathfrak{E}_i^{\mathfrak{G},\varphi} = (e_{i,1}, \ldots, e_{i,n_i}).$$

Nach Satz 1.48 ist dann $\{\gamma_{i+1} e_{i,j} \mid j \in \underline{n_{ij}}\}$ für alle $i \in \underline{k}$ ein Erzeugendensystem von γ_i/γ_{i+1} und damit folgt $m_i \leq n_i = \frac{1}{i} \sum_{d|i} \mu(d) m_1^{\frac{i}{d}}$ nach Satz 1.44. □

Beispiel 1.59 Wir greifen das Beispiel 1.49 wieder auf.

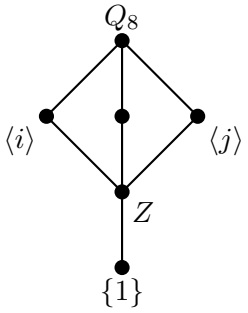
1. Wir betrachten $Q_8 = \langle i, j \rangle$. Dann ist

   $$Z := Z_1 = \gamma_2 = \langle -1 \rangle$$

   und $\{Zi, Zj\}$ ist ein Erzeugendensystem von Q_8/Z. Damit ist

   $$Q_8 = \left\{ i^\alpha j^\beta (-1)^\gamma \mid \alpha, \beta \in \{0,1,2,3\}, \gamma \in \{0,1\} \right\}.$$

   Es gilt jedoch $Z \cap \langle i \rangle = Z = Z \cap \langle j \rangle$. Damit ist die Voraussetzung von Korollar 1.58.2 (c) nicht erfüllt. Hier liegt auch keine Eindeutigkeit der Darstellung vor, wie wir bereits in Beispiel 1.49 gesehen haben.



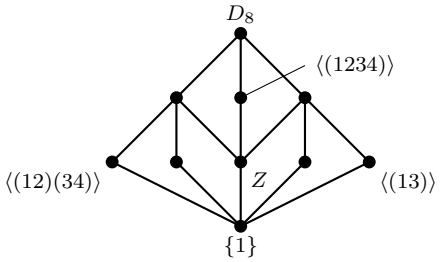
2. Wir betrachten nun die Gruppe

   $$D_8 = \langle (13), (12)(34) \rangle.$$

   Dann ist $Z := Z_1 = \gamma_2 = \langle (13)(24) \rangle$ und $\{Z(13), Z(12)(34)\}$ ist ein Erzeugendensystem von D_8/Z. Damit ist

   $$D_8 = \{(13)^\alpha ((12)(34))^\beta ((13)(24))^\gamma \mid \alpha, \beta, \gamma \in \{0,1\}\}.$$

   Mit $|D_8| = 8 = 2^3$ folgt sofort die Eindeutigkeit der Darstellung im Sinne von Korollar 1.58.1 (c) und 1.58.2 (c). Dieses haben wir auch in Beispiel 1.49 bereits gesehen.



Wählen wir statt (12)(34) das Element (1234) als zweiten Erzeuger, so erhalten wir

$$D_8 = \left\{ (13)^\alpha (1234)^\beta ((13)(24))^\gamma \mid \alpha, \gamma \in \{0,1\}, \beta \in \{0,1,2,3\} \right\}.$$

In diesem Fall liegt wegen $|D_8| = 8 < 16 = 2^2 \cdot 4$ keine Eindeutigkeit der Darstellung vor, wie sich auch mit $(1234)^2 = (13)(24)$ sofort einsehen lässt.

2 Die Gruppe quasiregulärer Elemente in der äußeren Algebra und in der Potenzreihenalgebra

In diesem Kapitel betrachten wir die $*$-Gruppe in konkret gegebenen K-Algebren. Dabei betrachten wir die äußeren Algebra und die Potenzreihenalgebra.

Es sei K stets ein kommutativer unitärer Ring.

2.1 Die äußere Algebra

Wir wollen nun die $*$-Gruppe des Jacobson-Radikals der äußeren Algebra betrachten. Diese ist – im Verhältnis zu $(N_{K,X,k}, *)$ – leicht zu beschreiben. Da das Jacobson-Radikal der äußeren Algebra nilpotent ist, ist es epimorphes Bild von $N_{K,X,k}$ für geeignetes $k \in \mathbb{N}$ und somit können wir aus den Aussagen über diese Gruppe Rückschlüsse auf $(N_{K,X,k}, *)$ ziehen.

Es sei in diesem Abschnitt $n \in \mathbb{N}$ und X eine n-elementige Menge, $X = \{x_1, \ldots, x_n\}$. Es bezeichne $\Lambda_K(X)$ die (bis auf Isomorphie eindeutig bestimmte) äußere Algebra über dem K-Raum der K-Linearkombinationen über X. Zur Definition der äußeren Algebra siehe [Bou74, Seite 507, Definition 1]. Wir bezeichnen mit $\wedge$ die Multiplikation auf $\Lambda_K(X)$.

Beweise der folgenden Aussagen findet sich in [Bou74, Chapter III, §7].

Definition und Lemma 2.1 Es gilt für alle $i, j \in \underline{n}$

$$x_i \wedge x_i = 0, \quad x_j \wedge x_i = -x_i \wedge x_j$$

und $\Lambda_K(X)$ ist ein freier K-Raum mit Basis

$$B := \{x_{i_1} \wedge \cdots \wedge x_{i_m} \mid m \in \underline{n}_0,\, i_1, \ldots, i_m \in \underline{n}, i_1 < \cdots < i_m\}.$$

Bezeichnungen 2.2 Für alle $b \in B$ sei $\pi_b : \Lambda_K(X) \to \langle b \rangle_K$ die Projektion bezüglich $\Lambda_K(X) = \bigoplus_{c \in B} \langle c \rangle_K$. Für alle $j \in \underline{n}_0$ sei

$$B_j := \{x_{i_1} \wedge \cdots \wedge x_{i_j} \mid i_1, \ldots, i_j \in \underline{n}, i_1 < \cdots < i_j\} \quad \text{und} \quad \Lambda_K^j(X) := \langle B_j \rangle_K.$$

Dann ist $(\Lambda_K^j(X))_{j\in\underline{n}_0}$ eine Graduierung von $\Lambda_K(X)$ und wir bezeichnen für alle $j \in \underline{n}_0$ die Projektion bezüglich dieser Zerlegung mit $\pi_j : \Lambda_K(X) \to \Lambda_K^j(X)$. Wir setzen

$$G_1 := \bigoplus_{j\in\underline{n}_0, j \text{ gerade}} \Lambda_K^j(X), \quad G := \bigoplus_{j\in\underline{n}, j \text{ gerade}} \Lambda_K^j(X) \text{ und}$$
$$U := \bigoplus_{j\in\underline{n}, j \text{ ungerade}} \Lambda_K^j(X).$$

Dann ist $\Lambda_K(X) = G_1 \oplus U$. Wir bezeichnen mit π_{G_1} und π_U die jeweiligen Projektionen. Es ist

$$J := G \oplus U = \bigoplus_{j\in\underline{n}} \Lambda_K^j(X)$$

das Jacobson-Radikal von $\Lambda_K(X)$. Insbesondere ist also $(J, *)$ eine Gruppe. Wir bezeichnen mit π_G die Projektion auf G bezüglich $J = G \oplus U$.
Es ist

$$B_{G_1} := \bigcup_{j\in\underline{n}_0,\, 2|j} B_j \text{ beziehungsweise } B_G := \bigcup_{j\in\underline{n},\, 2|j} B_j$$

eine K-Basis von G_1 beziehungsweise G und

$$B_U := \bigcup_{j\in\underline{n},\, 2\nmid j} B_j$$

eine K-Basis von U.

Beispiel 2.3 Sei $n = 3$ und $X = \{x_1, x_2, x_3\}$. Dann ist

$$B_0 = \{1_{\Lambda_K(X)}\},\ B_1 = \{x_1, x_2, x_3\},\ B_2 = \{x_1 \wedge x_2, x_1 \wedge x_3, x_2 \wedge x_3\} \text{ und}$$
$$B_3 = \{x_1 \wedge x_2 \wedge x_3\},$$

das heißt $\Lambda_K(X)$ ist vom Rang 8 und

$$J = G \oplus U = \langle B_2\rangle_K \oplus \langle B_1 \cup B_3\rangle_K$$

ist vom Rang 7. Es gilt

$$x_3 \wedge x_1 \wedge x_2 = -x_1 \wedge x_3 \wedge x_2 = x_1 \wedge x_2 \wedge x_3.$$

Bemerkung 2.4 Seien $a, c \in \Lambda_K(X)$, $b \in B$, $g, h \in G_1$, $\tilde{g} \in G$, $u, v \in U$ und $m \in \mathbb{N}$. Dann gilt

(a) $b \wedge b = 0$,

(b) $g \wedge h = h \wedge g \in G_1$ und $g \wedge \tilde{g} \in G$,

(c) $g \wedge u = u \wedge g \in U$,

(d) $u \wedge v = -v \wedge u \in G$, insbesondere ist $u \wedge u = 0$,

(e) $a \wedge c = c \wedge a + 2a\pi_U \wedge c\pi_U$,

(f) $[a, c] = 2a\pi_U \wedge c\pi_U$,

(g) $a^m = \sum_{i=0}^{m} \binom{m}{i} (a\pi_{G_1})^i \wedge (a\pi_U)^{m-i} = (a\pi_{G_1})^m + m(a\pi_{G_1})^{m-1} \wedge a\pi_U$,

(h) $a * c = c * a + 2a\pi_U \wedge c\pi_U$,

(i) falls $a \in J$ ist, gilt $a^- = \sum_{i=1}^{n} (-1)^i ((a\pi_G)^i + i(a\pi_G)^{i-1} \wedge a\pi_U)$ und

(j) $[u, v]_* = [u, v]$.

Beweis. (a), (b), (c) und (d) folgen direkt aus der Definition von B, G_1, G und U.
(e) Es gilt

$$\begin{aligned} a \wedge c &= (a\pi_{G_1} + a\pi_U) \wedge (c\pi_{G_1} + c\pi_U) \\ &= a\pi_{G_1} \wedge c\pi_{G_1} + a\pi_{G_1} \wedge c\pi_U + a\pi_U \wedge c\pi_{G_1} + a\pi_U \wedge c\pi_U \\ &\overset{\text{(b),(c),(d)}}{=} c\pi_{G_1} \wedge a\pi_{G_1} + c\pi_{G_1} \wedge a\pi_U + c\pi_U \wedge a\pi_{G_1} - c\pi_U \wedge a\pi_U \\ &\overset{(d)}{=} c \wedge a + 2a\pi_U \wedge c\pi_U. \end{aligned}$$

(f) ist direkte Folgerung von (e).
(g) Da nach (c) $a\pi_{G_1}$ und $a\pi_U$ miteinander kommutieren, folgt

$$\begin{aligned} a^m &= (a\pi_{G_1} + a\pi_U)^m \\ &= \sum_{i=0}^{m} \binom{m}{i} (a\pi_{G_1})^i \wedge (a\pi_U)^{m-i} \\ &\overset{\text{(d)}}{=} (a\pi_{G_1})^m + m(a\pi_{G_1})^{m-1} \wedge a\pi_U. \end{aligned}$$

(h) Es ist

$$a * c = a + c + a \wedge c \overset{\text{(e)}}{=} c + a + c \wedge a + 2a\pi_U \wedge c\pi_U = c * a + 2a\pi_U \wedge c\pi_U.$$

(i) Sei $a \in J$. Dann ist $a^{n+1} = 0$ und es folgt mit Lemma 1.2 (c)

$$a^- = \sum_{i=1}^{n} (-a)^i \overset{\text{(g)}}{=} \sum_{i=1}^{n} (-1)^i ((a\pi_G)^i + i(a\pi_G)^{i-1} \wedge a\pi_U).$$

(j) Nach Lemma 1.11 (b) gilt

$$\begin{aligned} [u, v]_* &= [u, v] + \sum_{i=1}^{n} (-1)^i \sum_{j=0}^{i} u^j \wedge v^{i-j} \wedge [u, v] \\ &\overset{\text{(d)}}{=} [u, v] + u \wedge [u, v] + v \wedge [u, v] + u \wedge v \wedge [u, v] \\ &\overset{\text{(f)}}{=} [u, v] + 2(\underbrace{u \wedge u}_{=0} \wedge v - \underbrace{v \wedge v}_{=0} \wedge u - u \wedge \underbrace{v \wedge v}_{=0} \wedge u) \\ &= [u, v]. \end{aligned}$$

□

Mit Hilfe dieser Rechenregeln wollen wir nun das Zentrum von $\Lambda_K(X)$ und J untersuchen.

Lemma 2.5 (a) Es gilt $G_1 + \Lambda_K^n(X) \subseteq Z(\Lambda_K(X))$ und $G + \Lambda_K^n(X) \subseteq Z(J)$.

(b) Sowohl $Z(\Lambda_K(X)) = G_1 + \Lambda_K^n(X)$ als auch $Z(J) = G + \Lambda_K^n(X)$ gelten genau dann, wenn $n = 1$ oder 2 kein Nullteiler in K ist.

(c) $(G, *)$ ist ein Normalteiler von $(J, *)$.

Beweis. (a) Nach Bemerkung 2.4 (b) und (c) ist G_1 in $Z(\Lambda_K(X))$ enthalten. Außerdem gilt für alle $a \in \Lambda_K^n(X)$ und $b \in \Lambda_K(X)$

$$a \wedge b = a \wedge b\pi_0 = b\pi_0 \wedge a = b \wedge a,$$

also ist auch $\Lambda_K^n(X) \subseteq Z(\Lambda_K(X))$. Es folgt

$$G_1 + \Lambda_K^n(X) \subseteq Z(\Lambda_K(X)) \text{ und } G + \Lambda_K^n(X) \subseteq Z(\Lambda_K(X)) \cap J = Z(J).$$

(b) Für $n = 1$ gilt $Z(\Lambda_K(X)) = \Lambda_K(X) = G_1 + \Lambda_K^1(X)$ und $Z(J) = J = G + \Lambda_K^1(X)$.
Sei 2 kein Nullteiler in K und $n > 1$. Es gilt für alle $x \in X$ und $a \in \Lambda_K(X)$ mit Bemerkung 2.4 (f)

$$[a, x] = 2a\pi_U \wedge x.$$

Sei nun $a \in \Lambda_K(X) \setminus (G_1 + \Lambda_K^n(X))$. Dann existiert ein $j \in \underline{n-1}$ ungerade mit $a\pi_j \neq 0$. Sei $b \in B_j$ mit $a\pi_b \neq 0$. Da $j < n$ ist, existiert $x \in X$ derart, dass x nicht in der Produktdarstellung von b vorkommt. Sei $x \in X$ mit dieser Eigenschaft gewählt und sei $c \in B_{j+1} \cap \{b \wedge x, -b \wedge x\}$. Dann ist

$$(2a\pi_U \wedge x)\pi_c = 2\underbrace{(a\pi_b) \wedge x}_{\neq 0} \neq 0,$$

da 2 kein Nullteiler in K ist. Damit ist $a \notin Z(\Lambda_K(X))$. Es folgt $Z(\Lambda_K(X)) = G_1 + \Lambda_K^n(X)$ und $Z(J) = Z(\Lambda_K(X)) \cap J = G + \Lambda_K^n(X)$.
Sei nun 2 ein Nullteiler in K und $n > 1$. Sei $\alpha \in K \setminus \{0\}$ mit $2\alpha = 0$. Dann gilt für alle $i, j \in \underline{n}$

$$[\alpha x_i, x_j] \overset{2.4(f)}{=} 2\alpha x_i \wedge x_j = 0,$$

also ist $\alpha x_i \in Z(\Lambda_K(X)) \setminus G_1 + \Lambda_K^n(X)$ für alle $i \in \underline{n}$.
(c) Nach Bemerkung 2.4 (b) und (i) ist $(G, *)$ eine Gruppe, die nach (a) im Zentrum liegt. Also ist $(G, *)$ Normalteiler. □

In Bemerkung 1.3 (d) haben wir gesehen, dass jedes Ideal ein $*$-Normalteiler ist. Hier sehen wir nun, dass die Umkehrung im Allgemeinen falsch ist: Ist $n \geq 3$, so ist G kein Ideal von J, da $x_1 \wedge x_2 \in G$ aber $x_1 \wedge x_2 \wedge x_3 \notin G$ gilt. Nach Lemma 2.5 (c) ist G jedoch ein $*$-Normalteiler.
Die folgenden Beobachtungen benötigen wir zur Bestimmung der Kommutatoruntergruppe.

Bemerkung 2.6 Für alle $a \in \Lambda_K(X)$ gilt $a^2 \in 2\Lambda_K(X)$.

Beweis. Sei $a \in \Lambda_K(X)$. Es gilt

$$a^2 = (a\pi_{G_1} + a\pi_U)^2 \overset{2.4(g)}{=} (a\pi_{G_1})^2 + \underbrace{2a\pi_{G_1} \wedge a\pi_U}_{\in 2\Lambda_K(X)}.$$

Sei $\alpha_b \in K$ für alle $b \in B_{G_1}$ mit $a\pi_{G_1} = \sum_{b \in B_{G_1}} \alpha_b b$. Weiter sei $<$ eine totale Ordnung auf B_{G_1}. Dann gilt mit $b \wedge b = 0$ für alle $b \in B_{G_1}$:

$$(a\pi_{G_1})^2 = \sum_{b,c \in B_{G_1}} \alpha_b \alpha_c b \wedge c = \sum_{b<c} \alpha_b \alpha_c (b \wedge c + \underbrace{c \wedge b}_{=b \wedge c}) = 2 \sum_{b<c} \alpha_b \alpha_c b \wedge c \in 2\Lambda_K(X).$$

□

Lemma 2.7 Für alle $a, b \in J$ ist $[a, b]_* \in G$.

Beweis. Wegen $a\pi_G, b\pi_G \in Z(J)$ ist $[a, b] = [a\pi_U, b\pi_U] \in G$. Zudem gilt für alle $i \in \mathbb{N}$

$$a^i \wedge [a, b] \overset{2.4(g)}{=} \underbrace{(a\pi_G)^i \wedge [a\pi_U, b\pi_U]}_{\in G} + i(a\pi_G)^{i-1} \wedge \underbrace{a\pi_U \wedge [a\pi_U, b\pi_U]}_{=0, \text{ da } a\pi_U \wedge a\pi_U = 0}.$$

Ebenso gilt auch $b^i \wedge [a, b] \in G$ für alle $i \in \mathbb{N}$. Es folgt für alle $i, j \in \mathbb{N}$

$$\begin{aligned} a^i \wedge b^j \wedge [a, b] &= a^i \wedge (b\pi_G)^j \wedge [a\pi_U, b\pi_U] = (b\pi_G)^j \wedge a^i \wedge [a\pi_U, b\pi_U] \\ &= (b\pi_G)^j \wedge (a\pi_G)^i \wedge [a\pi_U, b\pi_U] \in G \end{aligned}$$

und damit

$$[a, b]_* \overset{1.11(b)}{=} \underbrace{[a, b]}_{\in G} + \sum_{i=1}^{k} (-1)^i \sum_{j=0}^{i} \underbrace{a^j \wedge b^{i-j} \wedge [a, b]}_{\in G} \in G.$$

□

Korollar 2.7.1 Für die Kommutatoruntergruppe J' von $(J, *)$ gilt $J' \subseteq 2G$.

Beweis. Offenbar ist $(2G, *)$ eine Untergruppe von J und für alle $a, b \in J$ gilt mit Lemma 2.7 und Bemerkung 2.4 (f)

$$[a, b]_* \overset{1.11(b)}{=} [a, b] + \sum_{i=1}^{k} (-1)^i \sum_{j=0}^{i} a^j \wedge b^{i-j} \wedge [a, b] \in 2J \cap G = 2G.$$

□

Nun können wir die Kommutatoruntergruppe in $(J, *)$ bestimmen.

Satz 2.8 Es gilt $J' = 2G$.

Beweis. Nach Korollar 2.7.1 ist $J' \subseteq 2G$.
Ist $n = 1$, so ist $(J, *)$ abelsch und $J' = \{0\} = G = 2G$.
Sei $n > 1$ und κ ein additives Erzeugendensystem von K. Sei Y eine $\binom{n}{2}$-elementige Menge (insbesondere ist Y nichtleer) und $I := 2N_{K,Y,n}$. Dann ist I ein Ideal von $N_{K,Y,n}$ und $B = 2Y^{\leq n}$ ist ein K-Erzeugendensystem von I und enthält mit $2Y^{=i}$ ein K-Erzeugendensystem von $N_{K,Y,n}\pi_i \cap I$ für alle $i \in \mathbb{N}$. Nach Lemma 1.32 ist $2\kappa Y^{\leq n}$ ein $*$-Erzeugendensystem von I.
Sei $\bar{\varphi} : Y \to B_2$ eine Bijektion und $\varphi : N_{K,Y,n} \to G$ die Fortsetzung von $\bar{\varphi}$ zu einem K-Algebren-Homomorphismus. Da $\langle B_2 \rangle_{\mathfrak{A}^K} = G$ ist, ist φ surjektiv. Es folgt

$$2G = 2(N_{K,Y,n}\varphi) = (2N_{K,Y,n})\varphi = I\varphi = \langle 2\kappa Y^{\leq n} \rangle_* \varphi = \langle 2\kappa (Y^{\leq n}\varphi) \rangle_* = \langle 2\kappa B_G \rangle_*.$$

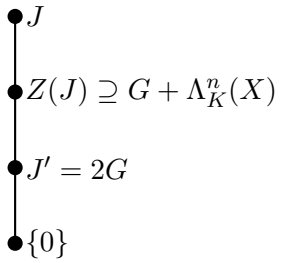
Damit ist $2\kappa B_G$ ein $*$-Erzeugendensystem von $2G$. Sei $b \in B_G$, $c \in \kappa$. Dann gibt es $y \in B_U$, $z \in X$ mit $b = y \wedge z$. Es folgt mit Bemerkung 2.4 (j)

$$2cb = 2cy \wedge z = [cy, z] = [cy, z]_* \in J'.$$

Damit gilt die Behauptung. □

Korollar 2.8.1 (a) Ist $n = 1$ oder char $K = 2$, so ist $(J, *)$ abelsch.

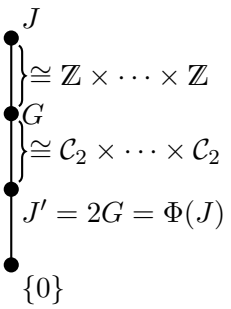
(b) Ist $n > 1$ und char $K \neq 2$, so ist $(J, *)$ nilpotent von der Klasse 2 und es gilt $J' = Z(J)$ genau dann, wenn n gerade und 2 eine Einheit in K ist.



Beweis. (a) Ist $n = 1$ oder char $K = 2$, so ist $J' = 2G = \{0\}$ nach Satz 2.8. Damit ist $(J, *)$ abelsch.
(b) Sei $n > 1$ und char $K \neq 2$. Dann ist $J' = 2G \neq \{0\}$ nach Satz 2.8, also ist $(J, *)$ nicht abelsch. Zudem ist $J' = 2G \subseteq G + \Lambda_K^n(X) = Z(J)$, also ist $(J, *)$ von Klasse 2. Ist n ungerade, so ist $\Lambda_K^n(X) \subseteq Z(J) \setminus J'$ nach Lemma 2.5 (a), also $Z(J) \neq J'$. Ist n gerade und 2 keine Einheit in K, so ist $x_1 \wedge x_2 \in Z(J) \setminus J'$ nach Lemma 2.5 (a), also $Z(J) \neq J'$. Ist n gerade und 2 eine Einheit in K, so ist 2 insbesondere kein Nullteiler in K und es folgt $J' = 2G = G = G + \Lambda_K^n(X) = Z(J)$ mit Lemma 2.5 (b). □

Korollar 2.8.2 Es gelte $(K, +) \cong (\mathbb{Z}^m, +)$ für ein $m \in \mathbb{N}$. Dann ist J/G frei abelsch und $\Phi(J) = J'$. Genauer gilt

$$J/G \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \quad \text{und} \quad G/J' \cong \mathcal{C}_2 \times \cdots \times \mathcal{C}_2.$$



Beweis. Da $(K,+)$ endlich erzeugt ist, ist nach Korollar 1.32.2 auch $(N_{K,X,n},*)$ endlich erzeugt. Da J epimorphes Bild von $N_{K,X,n}$ ist, ist damit auch $(J,*)$ endlich erzeugt. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen genügt es also für alle Elemente $a*J' \in J/J'$ zu zeigen, dass sie von Ordnung 1, 2 oder von unendlicher Ordnung sind. Sei also $a \in J \setminus J'$.
Gibt es $s \in \mathbb{N}$ mit $a^{(s)} \in G$, so folgt

$$a^{(s)} = \sum_{i=1}^{s} \binom{s}{i} a^i \overset{2.4(g)}{=} \sum_{i=1}^{s} \binom{s}{i} \left(\underbrace{(a\pi_G)^i}_{\in G} + \underbrace{i(a\pi_G)^{i-1} \wedge a\pi_U}_{\in U} \right) \in G$$

$$\Rightarrow \underbrace{\sum_{i=1}^{s} \binom{s}{i} i(a\pi_G)^{i-1} \wedge a\pi_U}_{=:b} \in G \cap U = \{0\}.$$

Es folgt

$$0 = b\pi_1 = sa\pi_1 \text{ und damit } a\pi_1 = 0.$$

Sei $j \in \underline{n}$ ungerade und induktiv gelte $a\pi_i = 0$ für alle $i \in \underline{j}$, i ungerade. Dann folgt

$$0 = b\pi_{j+2} \overset{\text{I.V.}}{=} \binom{s}{1} a\pi_{j+2} \text{ und damit } a\pi_{j+2} = 0.$$

Also ist in diesem Fall $a \in G$.
Damit folgt $a \in G$ oder $a*G \in J/G$ ist von unendlicher Ordnung. Insbesondere ist J/G frei abelsch. Ist $a \in G$, so folgt mit Bemerkung 2.6

$$a^{(2)} = 2a + a^2 \in G \cap 2J = 2G = J',$$

das heißt, $a*J'$ von Ordnung 2. Es folgt

$$J/J' \cong \mathcal{C}_2 \times \cdots \times \mathcal{C}_2 \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

und da die Frattini-Untergruppe von $\mathcal{C}_2 \times \cdots \times \mathcal{C}_2 \times \mathbb{Z} \times \cdots \times \mathbb{Z}$ trivial ist, folgt die Behauptung. □

Wir wollen nun die Beschreibung der Kommutatoruntergruppe in J auf $N_{K,X,k}$ anwenden.

Bemerkung 2.9 Sind $n,k \geq 3$ und char $K \neq 2$, so ist die Kommutatoruntergruppe in $N_{K,n,k}$ kein Ideal von $N_{K,n,k}$.

Beweis. Sei char $K \neq 2$. Sei X dreielementig, $X = \{x,y,z\}$. Dann ist $2x \wedge y \in 2G = J'$, aber $(2x \wedge y) \wedge z = 2x \wedge y \wedge z \notin J'$. Damit ist J' kein Ideal von J.
Seien nun $n,k \geq 3$. Dann ist J epimorphes Bild von $N_{K,n,k}$. Wäre die Kommutatoruntergruppe in $N_{K,n,k}$ ein Ideal, so wäre auch J' ein Ideal von J, ein Widerspruch. □

2.2 Die Potenzreihenalgebra

Wir wollen uns nun mit der $*$-Gruppe der Potenzreihenalgebra $P_{K,X}$ beschäftigen. Dabei werden wir die Aussage des Satzes von Magnus (Satz 1.23) verallgemeinern, uns mit der Berechnung der Koeffizienten von $*$-Inversen in P in der Basisdarstellung bezüglich X^+ beschäftigen und die so gewonnenen Aussagen zahlentheoretisch deuten.

In diesem Abschnitt sei stets X eine nichtleere Menge und p eine Primzahl.

Die folgenden Aussagen finden sich bereits in Abschnitt 1.3.

Wiederholung 2.10 $(P, *)$ ist eine Gruppe und für alle $a \in P$ und $m \in \mathbb{N}$ ist

$$a^{(m)} = \sum_{i=1}^{m} \binom{m}{i} a^i \text{ und } a^{(-m)} = \sum_{i \in \mathbb{N}} (-1)^i \binom{m+i-1}{i} a^i.$$

Ist $|X| > 1$, so ist $Z(P) = \{0\}$. Außerdem ist $\{P\pi_i \mid i \in \mathbb{N}\}$ eine Graduierung von P. Für alle $i \in \mathbb{N}$ nennen wir die Elemente von $P\pi_i$ homogen vom Grad i.
Die von X bezüglich $*$ in $P_{\mathbb{Z},X}$ erzeugte Gruppe ist frei über X.

Lemma 2.11 Für alle $i \in \mathbb{N}$ ist $\gamma_i(P) \subseteq P^i$. Insbesondere ist $(P, *)$ residuell nilpotent.

Beweis. Nach Lemma 1.11 (a) gilt für alle $a, b \in P$

$$\begin{aligned}[a,b]_* &= (1+a)^{-1}(1+b)^{-1}[a,b] \\ &= (1+a^-)(1+b^-)[a,b] \\ &= [a,b] + a^-[a,b] + b^-[a,b] + a^-b^-[a,b]\end{aligned}$$

und daraus folgt mit Bemerkung 1.27

$$L([a,b]_*) \geq L([a,b]) \geq L(a) + L(b).$$

Es folgt $\gamma_2(P) \subseteq P^2$ und induktiv $\gamma_i(P) \subseteq P^i$ für alle $i \in \mathbb{N}$. Damit ist

$$\bigcap_{i \in \mathbb{N}} \gamma_i(P) \subseteq \bigcap_{i \in \mathbb{N}} P^i = \{0\}.$$

□

Wir werden in der Folge sehen, dass die von X bezüglich $*$ in $P_{K,X}$ erzeugte Gruppe, unabhängig vom gewählten Grundring, frei über X ist. Dafür betrachten wir zunächst die Elementordnungen in $(P, *)$. Wir werden sehen, dass es unabhängig von der Wahl des Grundringes Elemente unendlicher Ordnung in $(P, *)$ gibt. Ist die Charakteristik $\neq 0$, so treten auch Elemente endlicher Ordnung in $(P, *)$ auf.

Bemerkung 2.12 (a) Für alle $f \in X^+$ ist f von unendlicher Ordnung in $(P_{K,X}, *)$.

(b) Ist $0 \neq \operatorname{char} K =: c$ und $l \in \mathbb{N}$ mit $p^l \mid c$, so gilt $o\left(\frac{c}{p^{l-1}}a\right) \mid p^l$ für alle $a \in P_{K,X}$.

Beweis. (a) Sei $f \in X^+$ und $m \in \mathbb{N}$. Dann gilt

$$f^{(m)}\pi_{mL(f)} = \left(\sum_{i=1}^{m} \binom{m}{i} f^i\right) \pi_{mL(f)} = f^m \neq 0.$$

Damit ist $f^{(m)} \neq 0$.
(b) Sei nun $0 \neq \operatorname{char} K =: c$, $l \in \mathbb{N}$ mit $p^l \mid c$ und $a \in P$. Dann gilt

$$\left(\frac{c}{p^{l-1}}a\right)^{(p^l)} = \sum_{i=1}^{p^l} \binom{p^l}{i} \left(\frac{c}{p^{l-1}}\right)^i a^i.$$

Wir zeigen nun

$$\forall i \in \underline{p^l\rfloor} : \; c \,\Big|\, \binom{p^l}{i} \left(\frac{c}{p^{l-1}}\right)^i.$$

Daraus folgt direkt die Behauptung.
Sei $i \in \underline{p^l\rfloor}$. Sei $s \in \mathbb{N}_0$ und $r \in \mathbb{N}$ mit $p \nmid r$ und $i = p^s r$. Dann gilt mit Lemma 1.15

$$p^l \mid p^{l+(p^s r - s)} = p^{l-s} p^{p^s r} = p^{l-s} p^i \,\Big|\, \binom{p^l}{p^s r} p^i = \binom{p^l}{i} p^i \quad \text{und damit}$$
$$c = p^l \frac{c}{p^l} \,\Big|\, \binom{p^l}{i} p^i \left(\frac{c}{p^l}\right)^i = \binom{p^l}{i} \left(\frac{c}{p^{l-1}}\right)^i.$$

□

Bemerkung 2.13 Sei $\tilde{K} = \langle 1_K \rangle_{\mathbb{Z}}$ der Primring von K. Dann ist $\langle X \rangle_*$ als Untergruppe von P_K in $P_{\tilde{K}}$ enthalten.

Beweis. Aus den Darstellungen von $x^{(m)}$ und $x^{(-m)}$ wie sie in Wiederholung 2.10 stehen folgt $x^{(m)}, x^{(-m)} \in P_{\tilde{K}}$ für alle $x \in X$ und $m \in \mathbb{N}$ und damit die Behauptung. □

Wir zeigen nun die Verallgemeinerung des Satzes von Magnus.

Satz 2.14 Die Untergruppe $\langle X \rangle_*$ von $(P_{K,X}, *)$ ist frei über X.

Beweis. Nach Bemerkung 2.13 können wir o.B.d.A. annehmen, dass K ein Faktorring von $\mathbb{Z}$ ist.
Wie betrachten zunächst den Fall, dass K nullteilerfrei ist, also $K = \mathbb{Z}$ oder $K = \mathbb{Z}/q\mathbb{Z}$ für eine Primzahl q. Seien $l \in \mathbb{N}$, $y_1, \ldots, y_l \in X$ mit $y_i \neq y_{i+1}$ für alle $i \in \underline{l-1\rfloor}$ und $z_1, \ldots, z_l \in \mathbb{Z} \setminus \{0\}$. Sei

$$a := \bigstar_{i=1}^{l} y_i^{(z_i)}.$$

Wir zeigen $a \neq 0$. Die Freiheit über X folgt dann mit [LS77, Seite 4, Proposition 1.9]. Für alle $i \in \underline{l}$ sei $m_i := L(y_i^{(z_i)})$ (es ist $m_i \in \mathbb{N}$ nach Bemerkung 2.12 (a)). Es gibt für alle $i \in \underline{l}$ ein $\alpha_i \in K \setminus \{0_K\}$ mit $y_i^{(z_i)}\pi_{m_i} = \alpha_i y_i^{m_i}$. Wir setzen $f := \prod_{i=1}^{l} y_i^{m_i} \in X^+$. Dann gilt

$$\begin{aligned} a\pi_f &= \left(\bigstar_{i=1}^{l} y_i^{(z_i)}\right)\pi_f \overset{1.2\,(\mathrm{d})}{=} \left(\prod_{i=1}^{l} y_i^{(z_i)}\right)\pi_f \\ &= \prod_{i=1}^{l}(y_i^{(z_i)}\pi_{m_i}) = \prod_{i=1}^{l}(\alpha_i y_i^{m_i}) = \left(\prod_{i=1}^{l}\alpha_i\right) f \neq 0. \end{aligned}$$

Es folgt $a \neq 0$.
Sei nun $c \in \mathbb{N}_{>1}$ und $K = \mathbb{Z}/c\mathbb{Z}$. Sei $q \in \mathbb{P}$ mit $q \mid c$. Seien

$$\varphi_c : P_{\mathbb{Z},X} \to P_{\mathbb{Z}/c\mathbb{Z},X} \quad \text{und} \quad \varphi_q : P_{\mathbb{Z}/c\mathbb{Z},X} \to P_{\mathbb{Z}/q\mathbb{Z},X}$$

die durch die kanonischen Ring-Epimorphismen $\mathbb{Z} \to \mathbb{Z}/c\mathbb{Z}$ und $\mathbb{Z}/c\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ induzierten Epimorphismen. Dann ist $x\varphi_c = x$ und $x\varphi_q = x$ für alle $x \in X$. Es folgt $\langle X\rangle_*\varphi_c = \langle X\rangle_*$ und $\langle X\rangle_*\varphi_q = \langle X\rangle_*$. Wir erhalten also:

$$\varphi_c\varphi_q : \underbrace{\langle X\rangle_*}_{\leq P_{\mathbb{Z},X}} \overset{\varphi_c}{\to} \underbrace{\langle X\rangle_*}_{\leq P_{\mathbb{Z}/c\mathbb{Z},X}} \overset{\varphi_q}{\to} \underbrace{\langle X\rangle_*}_{\leq P_{\mathbb{Z}/q\mathbb{Z},X}}$$

ist nach (a) ein Epimorphismus einer über X freien Gruppe auf eine über X freie Gruppe. Ist nun X endlich, so ist $\langle X\rangle_*$ in $P_{\mathbb{Z},X}$ als endlich erzeugte freie Gruppe hopfsch[5] [LS77, Seite 14, Proposition 3.5], also folgt, dass $\varphi_c\varphi_q$ und damit auch φ_c, φ_q Isomorphismen sind. Damit ist auch $\langle X\rangle_*$ in $P_{\mathbb{Z}/c\mathbb{Z},X}$ frei über X.
Ist nun X unendlich und $f \in \text{Kern } \varphi_{c|\langle X\rangle_*}$, so existiert $Y \subset X$, Y endlich, mit $f \in \langle Y\rangle_*$. Dann ist nach vorherigen Betrachtungen $\varphi_{c|\langle Y\rangle_*}$ injektiv und es folgt

$$f \in \text{Kern } \varphi_{c|\langle X\rangle_*} \cap \langle Y\rangle_* = \text{Kern } \varphi_{c|\langle Y\rangle_*} = \{0\}.$$

Damit ist $f = 0$ und $\varphi_{c|\langle X\rangle_*}$ ein Isomorphismus. Also ist auch in diesem Fall $\langle X\rangle_*$ in $P_{\mathbb{Z}/c\mathbb{Z},X}$ frei über X. □

Korollar 2.14.1 Es gilt

$$\langle X\rangle_* \cap pP_{\mathbb{Z}} = \{0\}.$$

Beweis. Sei $\varphi : P_{\mathbb{Z}} \to P_{\mathbb{Z}/p\mathbb{Z}}$ die lineare Fortsetzung von $f \mapsto f$ für alle $f \in X^+$. Dann ist φ ein Ring-Homomorphismus. Nach Definition ist $\varphi_{|\langle X\rangle_*}$ surjektiv auf $\langle X\rangle_*$. Ist X endlich, so bildet $\varphi_{|\langle X\rangle_*}$ nach Satz 2.14 eine freie Gruppe vom Rang $|X|$ auf eine freie Gruppe vom Rang $|X|$ ab. Da endlich erzeugte freie Gruppen hopfsch sind, ist somit $\varphi_{|\langle X\rangle_*}$ ein Isomorphismus. Ist nun X unendlich, so folgt aus dem vorherigen Fall wie im Beweis zu Satz 2.14, dass $\varphi_{|\langle X\rangle_*}$ ein Isomorphismus ist. Damit folgt

$$\{0\} = \text{Kern } \varphi_{|\langle X\rangle_*} = \langle X\rangle_* \cap \text{Kern } \varphi = pP_{\mathbb{Z}} \cap \langle X\rangle_*.$$

□

[5] Eine Gruppe $\mathcal{G}$ heißt hopfsch, wenn $\mathcal{G} \ncong \mathcal{G}/\mathcal{N}$ für alle $\mathcal{N} \trianglelefteq \mathcal{G}$, $\mathcal{N} \neq \{1\}$ gilt.

Wir sehen also in Satz 2.14, dass die Gruppen $\langle X\rangle_*$ innerhalb der Potenzreihenalgebren $P_{\mathbb{Z}}$ und $P_{\mathbb{Z}/c\mathbb{Z}}$ isomorph sind. Dies können wir im Falle der frei nilpotenten Algebra schon deshalb nicht erwarten, da zumindest für endliche Mengen X die Gruppe $\langle X\rangle_* \leq N_{\mathbb{Z}}$ unendlich ist, $N_{\mathbb{Z}/c\mathbb{Z}}$ jedoch nicht.

Wir wollen nun die Frage untersuchen, wie man zu bezüglich der Basis X^+ gegebenem $a \in P$ das Inverse a^- in der Basisdarstellung durch X^+ berechnet. Dazu betrachten wir zunächst, wie sich der Grundring K auf das Rechnen in P auswirkt.

Bemerkung 2.15 Sei K nullteilerfrei. Sind $a, b \in P \setminus \{0\}$ homogen, so ist $ab \in P \setminus \{0\}$ homogen.

Beweis. Seien $a, b \in P \setminus \{0\}$, $i, j \in \mathbb{N}$, und a homogen vom Grad i, b homogen vom Grad j. Dann ist ab homogen vom Grad $i + j$, also Linearkombination von Elementen aus $X^{=i+j}$, welche eindeutig als Produkt von Elementen aus $X^{=i}$ und $X^{=j}$ geschrieben werden können. Die Behauptung folgt aus der Nullteilerfreiheit. □

Korollar 2.15.1 Ist $(K, +)$ torsionsfrei oder K ein Körper der Charakteristik p, so ist $(P, *)$ torsionsfrei.

Beweis. Sei $a \in P \setminus \{0\}$ und $m \in \mathbb{N}$.
Ist $(K, +)$ torsionsfrei, so folgt

$$a^{(m)}\pi_{L(a)} \overset{1.2\,(e)}{=} (ma)\pi_{L(a)} = m(a\pi_{L(a)}) \neq 0,$$

also ist $a^{(m)} \neq 0$.
Sei nun K ein Körper der Charakteristik p. Dann ist insbesondere K nullteilerfrei und es gilt $b^{(p)} = b^p$ mit Lemma 1.2 (e) und Lemma 1.15 für alle $b \in P$. Seien nun $i, j \in \mathbb{N}_0$, $j < p$ mit $m = ip + j$.
Ist $j \neq 0$, so folgt

$$a^{(m)}\pi_{L(a)} = \left(\left(a^{(i)}\right)^p * a^{(j)}\right)\pi_{L(a)} = a^{(j)}\pi_{L(a)} = (ja)\pi_{L(a)} \neq 0.$$

Sei $j = 0$. Dann gibt es $l \in \mathbb{N}$ maximal mit $p^l \mid m$, etwa $m = p^l \cdot s$ mit $p \nmid s$. Dann gilt wieder mit Lemma 1.2 (e) und Lemma 1.15

$$a^{(m)}\pi_{p^l \cdot L(a)} = \left(\left(a^{(s)}\right)^{p^l}\right)\pi_{p^l \cdot L(a)} = \left((sa)\,\pi_{L(a)}\right)^{p^l} \overset{2.15}{\neq} 0.$$

□

Korollar 2.15.2 Ist K nullteilerfrei, so ist $Q(F) = \{0\}$. In F ist also kein Element $\neq 0$ quasiregulär.

Beweis. Seien $a, b \in F \setminus \{0\}$ und $i, j \in \mathbb{N}$ maximal mit $a\pi_i \neq 0$ und $b\pi_j \neq 0$. Dann gilt $(a * b)\pi_{i+j} = \tilde{a} \cdot \tilde{b} \overset{2.15}{\neq} 0$. □

Wir sehen also, dass im Falle eines nullteilerfreien Ringes zu jedem $a \in F \setminus \{0\}$ das Inverse a^- nicht in F liegt. Wir werden später sehen, dass es Elemente in $P \setminus F$ gibt, deren Inverses wieder in $P \setminus F$ liegt. Ist K jedoch nicht nullteilerfrei, so ist die Aussage von Korollar 2.15.2 im Allgemeinen falsch; beispielsweise gilt in $P_{\mathbb{Z}/4\mathbb{Z}}$ für alle $x \in X$

$$(2x)^{(2)} = 2x + 2x + (2x)^2 = 4x + 4x^2 = 0.$$

Von nun an sei X endlich.

Definition 2.16 Ist $s \in \mathbb{N}$ und sind $g_1, \ldots, g_s, f \in X^+$ mit $g_1 \ldots g_s = f$, so heißt das Tupel $(g_1, \ldots, g_s)$ eine Zerlegung von f und wir schreiben $(g_1, \ldots, g_s) \vDash f$.

Es sei eine Ordnung $\leq$ auf X gegeben, welche wir folgendermaßen zu einer totalen Ordnung $\leq$ auf X^+ fortsetzen:

$$\forall f, g \in X^+ : f \leq g :\Leftrightarrow l(f) < l(g) \vee l(f) = l(g), f \underset{lex}{\leq} g$$

Dabei bezeichne $\underset{lex}{\leq}$ die von der Ordnung auf X induzierte lexikographische Ordnung von X^+. Es sei $x \in X$ das bezüglich dieser Ordnung kleinste Element von X^+.

Definition 2.17 Wir definieren rekursiv (bezüglich obiger Ordnung) für alle $g \in X^+$ Polynome $f_g \in K[t_x, \ldots, t_g]$ durch

$$f_x = -t_x \quad \text{und} \quad f_g = -\sum_{(g_1,g_2)\vDash g} t_{g_1} f_{g_2} - t_g.$$

Im Fall $|X| = 1$, etwa $X = \{x\}$, setzen wir $f_i := f_{x^i}$ für alle $i \in \mathbb{N}$.

Lemma 2.18 Sei $a \in P$, etwa $a = \sum_{g \in X^+} \alpha_g g$. Dann gilt

$$a^- = \sum_{g \in X^+} f_g(\alpha_x, \ldots, \alpha_g) g.$$

Beweis. Seien $\alpha_g^- \in K$ für alle $g \in X^+$ mit $a^- = \sum_{g \in X^+} \alpha_g^- g$. Dann gilt für alle $g \in X^+$:

$$\begin{aligned} 0 = (a * a^-)\pi_g &= \left(\alpha_g + \alpha_g^- + \sum_{(g_1,g_2)\vDash g} \alpha_{g_1} \alpha_{g_2}^- \right) g \\ \Rightarrow 0 &= \alpha_g + \alpha_g^- + \sum_{(g_1,g_2)\vDash g} \alpha_{g_1} \alpha_{g_2}^- \\ (\star) \qquad \Rightarrow \alpha_g^- &= -\sum_{(g_1,g_2)\vDash g} \alpha_{g_1} \alpha_{g_2}^- - \alpha_g \end{aligned}$$

Es folgt $\alpha_x^- = -\alpha_x = f_x(\alpha_x)$ und

$$\alpha_g^- = -\sum_{(g_1,g_2)\vDash g} \alpha_{g_1} \alpha_{g_2}^- - \alpha_g \overset{\text{I.V.}}{=} \left(-\sum_{(g_1,g_2)\vDash g} t_{g_1} f_{g_2} - t_g \right)(\alpha_x, \ldots, \alpha_g) = f_g(\alpha_x, \ldots, \alpha_g)$$

induktiv aus $(\star)$ □

Korollar 2.18.1 Es gilt

$$f_i(\underbrace{(1,1,\ldots,1)}_{i}) = \begin{cases} -1 & i=1 \\ 0 & \text{sonst} \end{cases} \quad \text{und} \quad f_i(\underbrace{(-1,1,-1,\ldots,(-1)^i)}_{i}) = \begin{cases} 1 & i=1 \\ 0 & \text{sonst} \end{cases}.$$

Beweis. Wir betrachten $(-x)^- = \sum_{i\in\mathbb{N}} x^i$ beziehungsweise $x^- = \sum_{i\in\mathbb{N}}(-x)^i$. □

Lemma 2.19 Für alle $g \in X^+$ gilt

$$f_g = \sum_{s=1}^{l(g)} (-1)^s \sum_{(g_1,\ldots,g_s)\vDash g} t_{g_1}\ldots t_{g_s}.$$

Beweis. Wir beweisen dies mittels Induktion nach g.
Ist $g = x$, so gilt

$$\sum_{s=1}^{l(x)} (-1)^s t_x = -t_x = f_x.$$

Sei nun $g > x$. Dann gilt

$$\begin{aligned}
&\sum_{s=1}^{l(g)} (-1)^s \sum_{(g_1,\ldots,g_s)\vDash g} t_{g_1}\ldots t_{g_s} \\
&\quad = \sum_{s=2}^{l(g)} (-1)^s \sum_{g_1\in X^+} t_{g_1} \left(\sum_{\substack{(g_2,\ldots,g_s)\in (X^+)^{s-1} \\ (g_1,\ldots,g_s)\vDash g}} t_{g_2}\ldots t_{g_s} \right) - t_g \\
&\quad = -\sum_{g_1\in X^+} t_{g_1} \left(\sum_{s=1}^{l(g)-l(g_1)} (-1)^s \sum_{\substack{(h_1,\ldots,h_s)\vDash h \\ g_1 h = g}} t_{h_1}\ldots t_{h_s} \right) - t_g \\
&\quad \overset{\text{I.V.}}{=} -\sum_{(g_1,h)\vDash g} t_{g_1} f_h - t_g \\
&\quad = f_g.
\end{aligned}$$

□

Wir haben im Fall eines nullteilerfreien Ringes in Korollar 2.15.2 bereits gesehen, dass Inverse zu Elementen aus $F \setminus \{0\}$ nicht wieder in F liegen können. Nun können wir genauer bestimmen, in welchen „Abständen“ Koeffizienten $\neq 0$ in der Basisdarstellung des Inversen bezüglich X^+ auftreten müssen.

Bemerkung 2.20 Sei K nullteilerfrei. Sei $a \in F \setminus \{0\}$, $a = \sum_{f=x}^{h} \alpha_f f$ wobei $h \in X^+$ maximal mit $\alpha_h \neq 0$ gewählt sei. Weiter sei $a^- = \sum_{f \in X^+} \alpha_f^- f$. Dann gilt

$$\forall g \in X^+ \, \exists \tilde{g} \in X^+ : \quad |l(g) - l(\tilde{g})| < l(h) \quad \wedge \quad \alpha_{\tilde{g}}^- \neq 0.$$

Das heißt, das Doppelte der Länge des größten Summanden h ist eine obere Schranke für die Abstände der Länge, in welchen bei dem Inversen von a ein Koeffizient $\neq 0$ auftreten muss.

Beweis. Sei $g \in X^+$.
Falls $g \leq h$ ist, wählen wir $\tilde{g} := \min\{f \in X^+ \mid \alpha_f \neq 0\}$. Dann sind $g, \tilde{g} \leq h$ und damit $|l(g) - l(\tilde{g})| < l(h)$ und es gilt $\alpha_{\tilde{g}}^- = -\alpha_{\tilde{g}} \neq 0$.
Sei nun $g > h$. Annahme: Es ist $\alpha_{\tilde{g}}^- = 0$ für alle $\tilde{g} \in X^+$ mit $|l(g) - l(\tilde{g})| < l(h)$.
Sei $b \in X^+$ mit $l(b) = l(g) + l(h)$ und seien $b_1, b_2 \in X^+$ mit $b_1 \leq h$ und $b = b_1 b_2$. Dann gilt

$$l(b_2) = l(b) - l(b_1) \geq l(b) - l(h) = l(g)$$

und damit $0 \leq l(b_2) - l(g) < l(b) - l(g) = l(h)$, also ist nach Annahme $\alpha_{b_2}^- = 0$. Wir erhalten

$$\alpha_b^- \overset{2.18}{=} f_b(\alpha_x, \ldots, \alpha_b) = - \sum_{(a_1,a_2) \vDash b} \underbrace{\alpha_{a_1}}_{[=0 \text{ für alle } a_1 > h]} \underbrace{\alpha_{a_2}^-}_{[=0 \text{ für alle } a_1 \leq h]} - \underbrace{\alpha_a}_{=0} = 0.$$

Somit ist induktiv $\alpha_b^- = 0$ für alle $b > g$, ein Widerspruch zu Korollar 2.15.2. □

Korollar 2.20.1 Sei K nullteilerfrei. Ist $a \in P$, $a = \sum_{f \in X^+} \alpha_f f$, mit

$$\forall n \in \mathbb{N} \, \exists l \in \mathbb{N} \, \forall f \in X^+ : \, l \leq l(f) \leq l + n \Rightarrow \alpha_f = 0,$$

so gilt $a^- \notin F$.

Damit erhalten wir, dass jedes Element in P_K mit nullteilerfreiem K, bei dem die Anzahl der aufeinanderfolgenden homogenen Komponenten, die Null sind, nicht beschränkt ist, kein Inverses in F_K hat. Somit gibt es Elemente $a \in P_K \setminus F_K$ mit $a^- \in P_K \setminus F_K$, beispielsweise

$$a = \sum_{i \in \mathbb{N}} x^{2^i} \in P_{\mathbb{Z},\{x\}}.$$

2.2.1 Zahlentheoretische Anwendungen

Die in Lemma 2.19 bewiesene Gleichheit ermöglicht es uns, die Polynome f_i in einem zahlentheoretischen Kontext zu betrachten. Dabei interessieren wir uns für die Frage

nach Zerlegungen einer gegebenen Zahl n in Summanden aus einer vorgegebenen Teilmenge von $\mathbb{N}$, wie sie unter Anderem auch in der analytischen Zahlentheorie betrachtet werden (vergleiche [New98]).

Wir betrachten den Fall $K = \mathbb{Z}$ und $X = \{x\}$. Für alle $i \in \mathbb{N}$ sei $t_i = t_{x^i}$ und wie zuvor sei $f_i := f_{x^i} \in \mathbb{Z}[t_1, \ldots, t_i]$ für alle $i \in \mathbb{N}$. Es gilt

$$\begin{aligned} &f_1 = -t_1 \quad \text{und} \\ &f_i = -\sum_{j=1}^{i-1} t_j f_{i-j} - t_i = \sum_{s=1}^{i} (-1)^s \sum_{(j_1,\ldots,j_s)\vDash i} t_{j_1} \ldots t_{j_s} \quad \text{für alle } i \in \mathbb{N}_{>1}. \end{aligned}$$

Definition 2.21 Sei $n \in \mathbb{N}$ und $B \subseteq \mathbb{N}$. Sind $s \in \mathbb{N}$ und $i_1, \ldots, i_s \in B$ mit $\sum_{j=1}^{s} i_j = n$, so nennen wir $(i_1, \ldots, i_s)$ eine $\underline{B\text{-Zerlegung}}$ von n und schreiben $(i_1, \ldots, i_s) \vDash_B n$. Wir bezeichnen mit $g_B(n)$ die Anzahl aller B-Zerlegungen von n.

Lemma 2.22 Sei $B \subseteq \mathbb{N}$. Wir definieren für alle $i \in \mathbb{N}$

$$\beta_i := \begin{cases} -1 & i \in B \\ 0 & i \notin B \end{cases}.$$

Dann gilt $f_n(\beta_1, \ldots, \beta_n) = g_B(n)$ für alle $n \in \mathbb{N}$.

Beweis. Es gilt für alle $n \in \mathbb{N}$

$$\begin{aligned} f_n(\beta_1, \ldots, \beta_n) &= \sum_{s=1}^{n} (-1)^s \sum_{(j_1,\ldots,j_s)\vDash n} \beta_{j_1} \ldots \beta_{j_s} = \sum_{s=1}^{n} (-1)^s \sum_{\substack{(j_1,\ldots,j_s)\vDash n \\ \forall i \in \underline{s}: j_i \in B}} \beta_{j_1} \ldots \beta_{j_s} \\ &= \sum_{s=1}^{n} (-1)^s \sum_{(j_1,\ldots,j_s)\vDash_B n} (-1)^s = \sum_{s=1}^{n} \sum_{(j_1,\ldots,j_s)\vDash_B n} 1 = g_B(n). \end{aligned}$$

□

Wir betrachten nun den folgenden Spezialfall:
Sei $z \in \mathbb{N}$ und $k \in \underline{z}_0$, $B := [k]_{\equiv z}$. Weiter sei β_i für alle $i \in \mathbb{N}$ gemäß Lemma 2.22 gesetzt, das heißt

$$\beta_i = \begin{cases} -1 & i \equiv k \mod z \\ 0 & \text{sonst} \end{cases}.$$

Sei nun $n \in \mathbb{N}$, $n > z$, und $s \in \mathbb{N}$, $t \in \underline{z-1}_0$ mit $n = sz + t$. Wir setzen

$$m := \begin{cases} s-1 & k \geq t \\ s & k < t \end{cases}.$$

Dann ist für alle $j \in \underline{m}_0$

$$n - jz - k \geq n - mz - k = (s-m)z + t - k \geq 1$$

und es gilt

$$\begin{aligned}\sum_{j=1}^{m} f_{n-jz-k}(\beta_1,\dots,\beta_{n-jz-k}) &= \sum_{j=0}^{m-1} f_{n-z-jz-k}(\beta_1,\dots,\beta_{n-z-jz-k})\\ &= -\sum_{j=0}^{m-1} \underbrace{\beta_{jz+k}}_{-1} f_{n-z-jz-k}(\beta_1,\dots,\beta_{n-z-jz-k})\\ &= -\sum_{\substack{j=1\\ j\underset{z}{\equiv}k}}^{n-z-1} \beta_j f_{n-z-j}(\beta_1,\dots,\beta_{n-z-j})\\ &= -\sum_{j=1}^{n-z-1} \beta_j f_{n-z-j}(\beta_1,\dots,\beta_{n-z-j}).\end{aligned}$$

Damit erhalten wir

$$\begin{aligned}f_n(\beta_1,\dots,\beta_n) &= -\sum_{j=1}^{n-1} \beta_j f_{n-j}(\beta_1,\dots,\beta_{n-j}) - \beta_n\\ &= \sum_{\substack{j=1\\ j\underset{z}{\equiv}k}}^{n-1} f_{n-j}(\beta_1,\dots,\beta_{n-j}) - \beta_n\\ &= \sum_{j=0}^{m} f_{n-jz-k}(\beta_1,\dots,\beta_{n-jz-k}) - \beta_{n-z}\\ &= f_{n-k}(\beta_1,\dots,\beta_{n-k}) + \sum_{j=1}^{m} f_{n-jz-k}(\beta_1,\dots,\beta_{n-jz-k}) - \beta_{n-z}\\ &= f_{n-k}(\beta_1,\dots,\beta_{n-k}) - \sum_{j=1}^{n-z-1} \beta_j f_{n-z-j}(\beta_1,\dots,\beta_{n-z-j}) - \beta_{n-z}\\ &= f_{n-k}(\beta_1,\dots,\beta_{n-k}) + f_{n-z}(\beta_1,\dots,\beta_{n-z}).\end{aligned}$$

Dies motiviert die folgende Definition:

Definition 2.23 Sei $z \in \mathbb{N}$ und $k \in \underline{z}$. Zu dem Paar (z,k) definieren wir rekursiv die verallgemeinerte Fibonacci-Folge $\left(b_n^{(z,k)}\right)_{n\in\mathbb{N}}$ durch

$$\begin{aligned}\forall n \le z:\ b_n^{(z,k)} &:= \begin{cases} 1 & k \mid n \\ 0 & \text{sonst} \end{cases} \quad \text{und}\\ \forall n > z:\ b_n^{(z,k)} &:= b_{n-z}^{(z,k)} + b_{n-k}^{(z,k)}.\end{aligned}$$

Bemerkung 2.24 Für $(z,k) = (2,1)$ erhalten wir die bekannte Fibonacci-Folge.

Damit folgt:

Satz 2.25 Sei $z \in \mathbb{N}$ und $k \in \underline{z}$. Dann gilt

$$g_{[k]_{\equiv z}}(n) = b_n^{(z,k)}$$

für alle $n \in \mathbb{N}$. Insbesondere gibt es $b_n^{(2,1)}$ Zerlegungen von n in ungerade Zahlen.

3 Die Gruppe quasiregulärer Elemente in der frei nilpotenten Algebra

In diesem Kapitel wollen wir die $*$-Gruppe der frei nilpotenten Algebra $N_{K,X,k}$ betrachten. Dazu zerlegen wir diese Gruppe zunächst in Untergruppen, bevor wir uns ihrer Kommutator- und Frattini-Untergruppe näheren. Dabei werden wir in Satz 3.23 sehen, dass die bisher verwandten Werkzeuge der Algebrentheorie hier nicht mehr helfen: Zwar ist nach Bemerkung 1.3 jede Teilalgebra eine $*$- Untergruppe und jedes Ideal ein $*$-Normalteiler, aber die Umkehrung gilt im Allgemeinen nicht. Wir zeigen, dass im Allgemeinen die Kommutatoruntergruppe N' keine Teilalgebra von N ist. Ferner bestimmen wir ein kleinstmögliches Ideal von N, welches N' enthält. Im Allgemeinen gelingt es uns jedoch nicht, N' zu beschreiben.

Anschließend betrachten wir den Fall, dass die Menge X einelementig ist. In diesem Fall ist $(N, *)$ abelsch und bei geeigneter Wahl von K endlich erzeugt. In Satz 3.33 gelingt es uns, den Isomorphietyp dieser Gruppe zu bestimmen.

Danach beschäftigen wir und mit der von X erzeugten Untergruppe von N. Wie schon im Fall der Potenzreihenalgebra können wir über diese Untergruppe mehr aussagen als über die ganze Gruppe. In P war diese Gruppe nach Satz 2.14 frei und wir werden sehen, dass auch in N die von X erzeugte Gruppe frei in einer geeigneten Klasse ist.

In dem ganzen Kapitel seien X eine nichtleere Menge, K ein kommutativer unitärer Ring und $k, n \in \mathbb{N}$.

3.1 Zerlegungen der Gruppe $(N, *)$

In diesem Abschnitt werden wir die Gruppe $(N, *)$ zunächst auf zwei verschiedene Arten semidirekt zerlegen.
Erst werden wir eine durch Teilmengen von X induzierte Zerlegung betrachten. Diese ist auch algebrentheoretisch eine Zerlegung der Algebra N in ein Ideal und eine Teilalgebra und kann unabhängig von der Wahl des Grundringes K durchgeführt werden.
Die zweite hier vorgestellte Zerlegung basiert auf der Beobachtung

$$(N^i, *) = (N^i, +) \cong (K, +) \times \cdots \times (K, +) \quad \text{für alle} \quad i \geq \left\lceil \frac{k+1}{2} \right\rceil.$$

Wir versuchen also eine möglichst große Untergruppe in N^i mit $i \geq \lceil \frac{k+1}{2} \rceil$ zu finden, die wir semidirekt abspalten können. Diese Zerlegung erfordert allerdings $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ mit $c \in \mathbb{N}_{>1}$ und $\mathrm{ggT}(c, k!) = 1$ und nur eine der auftretenden Untergruppen ist eine Teilalgebra von N.

Im letzten Teil diese Abschnitts zerlegen wir die Gruppe $(N, *)$ für geeignete Grundringe in ein iteriertes semidirektes Produkt von zyklischen Untergruppen.

Satz 3.1 Sei $Y \subseteq X$, $Y \neq \emptyset$, und $M := \langle X^{\leq k} \setminus Y^{\leq k} \rangle_K$. Dann ist M ein Ideal von N_X, N_Y eine Teilalgebra von N_X und es gilt

$$N_X = N_Y \ltimes M \qquad \text{als } *\text{-Gruppen.}$$

Beweis. Es ist $N_Y \subseteq N_X$ eine Algebra, also ist N_Y eine Teilalgebra von N_X. Nach Definition ist M ein K-Raum, der wegen $X^{\leq k}\left(X^{\leq k} \setminus Y^{\leq k}\right) \subseteq \left(X^{\leq k} \setminus Y^{\leq k}\right) \cup \{0\}$ und $\left(X^{\leq k} \setminus Y^{\leq k}\right) X^{\leq k} \subseteq \left(X^{\leq k} \setminus Y^{\leq k}\right) \cup \{0\}$ ein Ideal von N_X ist. Nach Bemerkung 1.3 (b) und (d) ist somit N_Y eine $*$-Untergruppe und M ein $*$-Normalteiler von N_X. Es ist $Y^{\leq k}$ eine K-Basis von N_Y und $X^{\leq k} \setminus Y^{\leq k}$ eine K-Basis von M. Damit folgt $N_Y \cap M = \{0\}$ und mit Bemerkung 1.4 folgt $N_X = N_Y + M = N_Y * M$. □

Bemerkung 3.2 Wie in Satz 3.1 erhalten wir auch eine Zerlegung von P_X: Sei $Y \subseteq X$, $Y \neq \emptyset$, und $M := \langle X^+ \setminus Y^+ \rangle_K$. Dann ist $P_X = P_Y \ltimes M$.

Wir wollen nun den Satz über die zweite Zerlegung angeben. Im Fall $K = \mathbb{Z}$ findet sich dieses Resultat bereits in meiner Diplomarbeit [Han12, Satz 2.26].

Satz 3.3 Sei $i \geq \left\lceil \frac{k+1}{2} \right\rceil$ und X n-elementig. Ist $K = \mathbb{Z}$ oder gilt $K = \mathbb{Z}/c\mathbb{Z}$ mit $\mathrm{ggT}(c, k!) = 1$, so gibt es einen Normalteiler M_i von $(N, *)$ mit

$$N \cong (K, +)^{r_i} \ltimes M_i \quad \text{mit} \quad r_i = \binom{n+k}{n} - \binom{n+i-1}{n}.$$

Dabei kann die Gruppe M_i als Produkt zweier Untergruppen beschrieben werden und enthält die Untergruppe $\langle X \rangle_*$, die wir in Abschnitt 3.4 genauer betrachten werden.

Zur Konstruktion der Untergruppe M_i benötigen wir zunächst das Ideal C von N, welches wir als Augmentationsideal über gewissen Teilmengen der kanonischen Basis $X^{\leq k}$ von N erhalten. Dafür sei X n-elementig, $X = \{x_1, \ldots, x_n\}$.

Definition und Bemerkung 3.4 Seien $f, g \in X^+$. Wir nennen f und g assoziiert, falls sie durch Vertauschung von Buchstaben auseinander hervorgehen. Das heißt: Sind $l \in \mathbb{N}$ und $y_1, \ldots, y_l \in X$ mit $f = y_1 \ldots y_l$, so existiert ein $\sigma \in \mathcal{S}_l$ mit

$$\sigma f := y_{1\sigma} \ldots y_{l\sigma} = g.$$

Sind f, g assoziiert, so schreiben wir kurz $f \sim g$.
Es definiert $\sim$ auf X^+ und eingeschränkt auf $X^{\leq k}$ eine Äquivalenzrelation. Die Äquivalenzklassen bezüglich $\sim$ heißen Assoziiertenklassen. Die Menge der Assoziiertenklassen bezeichnen wir mit $X^+_\sim$ beziehungsweise $X^{\leq k}_\sim$.
Sind f und g assoziiert, so gilt insbesondere $l(f) = l(g)$. Also können wir auch von der Länge einer Assoziiertenklasse sprechen.

Definition und Lemma 3.5 Sei $W \in X_{\sim}^{\leq k}$. Wir setzen

$$\eta_W : N \to K, \sum_{f \in X^{\leq k}} \alpha_f f \mapsto \sum_{f \in W} \alpha_f.$$

Offenbar ist η_W K-linear. Weiter sei

$$C := \bigcap_{V \in X_{\sim}^{\leq k}} \text{Kern } \eta_V.$$

Dann ist C ein Ideal von N und wir nennen C das Augmentationsideal bezüglich der Assoziiertenklassen. Außerdem gilt

$$C = \bigoplus_{i=1}^{k} C\pi_i.$$

Beweis. Da η_V für alle $V \in X_{\sim}^{\leq k}$ K-linear ist, ist C ein K-Raum. Für alle $W \in X_{\sim}^{\leq k}$ sei $f_W \in W$. Dann ist

$$B := \bigcup_{W \in X_{\sim}^{\leq k}} \{f_W - f \mid f \in W \setminus \{f_W\}\}$$

eine K-Basis von C und wegen der K-Linearität der η_V genügt es

$$(g(f - f_W))\eta_V = 0 = ((f - f_W)g)\eta_V$$

für alle $V, W \in X_{\sim}^{\leq k}$, $f \in W$ und $g \in X^{\leq k}$ zu zeigen.
Seien $V, W \in X_{\sim}^{\leq k}$, $f \in W$ und $g \in X^{\leq k}$. Sei o.B.d.A. $l(f) + l(g) \leq k$. Dann sind $gf, fg, gf_W, f_W g$ assoziiert und es gilt

$$\begin{aligned}(g(f - f_W))\eta_V &= (gf)\eta_V - (gf_W)\eta_V = (gf)\eta_V - (gf)\eta_V = 0 \quad \text{und} \\ ((f - f_W)g)\eta_V &= (fg)\eta_V - (f_W g)\eta_V = (fg)\eta_V - (fg)\eta_V = 0.\end{aligned}$$

Damit ist C ein Ideal von N.
Da B nur homogene Elemente enthält, folgt $C = \bigoplus_{i=1}^{k} C\pi_i$. □

Lemma 3.6 Seien $W \in X_{\sim}^{\leq k}$ und $a, b \in N$. Dann gelten die folgenden Eigenschaften:

(a) Es sind $[a, b], [a, b]_* \in C$.

(b) Es gilt $N' \subseteq C$.

(c) Seien $t \in \mathbb{N}$, $a_1, \ldots, a_t \in N$ und $\sigma \in \mathcal{S}_t$. Dann ist $(a_1 \cdots a_t)\eta_W = (a_{1\sigma} \cdots a_{t\sigma})\eta_W$. Insbesondere ist η_W auf den Assoziiertenklassen von $X^{\leq k}$ konstant.

(d) Seien $g, h \in X^{\leq k}$ mit $g \sim h$. Dann gilt

$$(a * g * b)\eta_W = (a * h * b)\eta_W.$$

Beweis. (a) Nach Definition von C ist $[f,g] \in C$ für alle $f,g \in X^{\leq k}$. Mit der Bilinearität von $[.,.]$ folgt $[a,b] \in C$. Daraus folgt $[a,b]_* \in C$ mit Lemma 1.11, da C ein Ideal von N ist.
(b) Es ist C ein Ideal von N, also nach Bemerkung 1.3 auch eine $*$-Gruppe. Es folgt $N' \subseteq C$ mit (a).
(c) Da η_W K-linear ist, genügt es die Behauptung für $a_1,\ldots,a_t \in X$ zu zeigen. Sind $a_1,\ldots,a_t \in X$, so gilt $a_1\cdots a_t \sim a_{1\sigma}\cdots a_{t\sigma}$. Damit folgt (c).
(d) Mit (c) gilt

$$\forall f,\tilde{f} \in X^{\leq k} : \; fg\tilde{f} \in W \Leftrightarrow fh\tilde{f} \in W,$$

und damit gilt wegen der K-Linearität von η_W schon

$$(ag)\eta_W = (ah)\eta_W,\ (gb)\eta_W = (hb)\eta_W \quad \text{und} \quad (agb)\eta_W = (ahb)\eta_W.$$

Damit ergibt sich

$$\begin{aligned}(a*g*b)\eta_W &= (a+g+b+ag+ab+gb+agb)\eta_W\\ &= a\eta_W + g\eta_W + b\eta_W + (ag)\eta_W + (ab)\eta_W + (gb)\eta_W + (agb)\eta_W\\ &= a\eta_W + h\eta_W + b\eta_W + (ah)\eta_W + (ab)\eta_W + (hb)\eta_W + (ahb)\eta_W\\ &= (a+h+b+ah+ab+hb+ahb)\eta_W = (a*h*b)\eta_W.\end{aligned}$$

□

Wie wir in Lemma 3.6 (a) gesehen haben, enthält C die Kommutatoruntergruppe N' von $(N,*)$. Wir werden uns nun überlegen, dass C das kleinste Ideal von N mit dieser Eigenschaft ist, das heißt, C ist eine bestmögliche Abschätzung für N' nach oben gegen ein Ideal.

Lemma 3.7 *C ist das von $[N,N] = \langle [a,b] \mid a,b \in N\rangle_K$ erzeugte assoziative Ideal.*

Beweis. Sei I das von $[N,N]$ erzeugte assoziative Ideal in N. Mit $[N,N] \subseteq C$ nach Lemma 3.6 (a) ist $I \subseteq C$. Für alle $W \in X^{\leq k}_{\sim}$ sei $f_W \in W$. Dann ist

$$\bigcup_{W \in X^{\leq k}_{\sim}} \{f_W - f \mid f \in W \setminus \{f_W\}\}$$

eine K-Basis von C. Es genügt also $f_W - f \in I$ für alle $W \in X^{\leq k}_{\sim}$ und $f \in W$ zu zeigen. Sei $W \in X^{\leq k}_{\sim}$, $w \in \underline{k}$ die Länge von W und $f \in W$. Für $w = 1$ ist nichts zu zeigen. Sei $w > 1$ und seien $\alpha,\beta \in \mathcal{S}_w$, $\alpha := ((w-1)w)$ und $\beta := (1\ldots w)$. Dann gilt[6] $\langle \alpha,\beta\rangle = \mathcal{S}_w$. Also gibt es ein $j \in \mathbb{N}$ sowie $\tau_1,\ldots,\tau_j \in \{\alpha,\beta\}$ mit $f = \tau_j\cdots\tau_1 f_W$.
Für alle $g \in X^{=w}$ und $\tau \in \{\alpha,\beta\}$ gilt $g - \tau g \in I$, denn mit $g = y_1\cdots y_w$, $y_1,\ldots,y_w \in X$, gilt

$$\begin{aligned}&\text{1. Fall: } \tau = \alpha \Rightarrow g - \tau g = y_1\cdots y_w - y_1\cdots y_{w-2}y_w y_{w-1}\\ &\qquad\qquad = y_1\cdots y_{w-2}[y_{w-1},y_w] \in I \quad \text{und}\\ &\text{2. Fall: } \tau = \beta \Rightarrow g - \tau g = y_1\cdots y_w - y_2\cdots y_w y_1 = [y_1,y_2\ldots y_w] \in I.\end{aligned}$$

[6] Mit α und β ist auch $\beta^{-s}\alpha\beta^s = ((w-s-1)(w-s)) \in \langle\alpha,\beta\rangle$ für alle $s \in \underline{w-1}$ und mit [Hup67, Seite 138, Beispiel 19.7 b] folgt $\langle\alpha,\beta\rangle = \mathcal{S}_w$.

Damit folgt

$$f_W - f = f_W - \tau_j \dots \tau_1 f_W = \sum_{i=1}^{j} \tau_{i-1} \cdots \tau_1 f_W - \tau_i(\tau_{i-1} \cdots \tau_1 f_W) \in I.$$

□

Korollar 3.7.1 C ist das kleinste Ideal von N, das N' enthält.

Beweis. Nach Lemma 3.6 (a) ist $N' \subseteq C$. Sei I ein Ideal von N mit $N' \subseteq I$. Dann ist I nach Bemerkung 1.3 auch $*$-Normalteiler und damit ist N/I als $*$- Gruppe abelsch. Es gilt also nach Bemerkung 1.4 für alle $a, b \in N$:

$$\begin{aligned} & a + b + ab + I = a * b + I = a * b * I = b * a * I = b * a + I = b + a + ba + I \\ \Rightarrow \quad & ab + I = ba + I \\ \Rightarrow \quad & [a, b] \in I \end{aligned}$$

Damit gilt $[N, N] \subseteq I$. Da C das von $[N, N]$ erzeugte Ideal ist, folgt $C \subseteq I$. □

Korollar 3.7.2 Ist $k \in \{1, 2\}$, so ist $N' = C$.

Beweis. Für $k = 1$ ist jede Assoziiertenklasse einelementig und $(N, *)$ ist abelsch. Also ist $C = \{0\} = N'$.
Für $k = 2$ ist $[a, b]_* = [a, b]$ für alle $a, b \in N$ nach Lemma 1.11 (b). Damit ist $N' \subseteq N^2$, also $NN' = \{0\} = N'N$. Damit ist N' als $*$-Gruppe additiv abgeschlossen, wegen der K-Bilinearität von $[.,.]$ ein K-Raum und damit ein Ideal von N. Mir Korollar 3.7.1 folgt $N' = C$. □

Nun wenden wir uns der Konstruktion der zu $(K, +)^{r_i}$ isomorphen Untergruppe in Satz 3.3 zu.

Bezeichnungen 3.8 Es sei R_i für alle $i \in \underline{k}$ ein Repräsentantensystem der Assoziiertenklassen der Länge $\geq i$ und $r_i = |R_i|$.

Bemerkung 3.9 Es gilt $r_i = \binom{n+k}{n} - \binom{n+i-1}{n}$ für alle $i \in \underline{k}$.

Beweis. Sei $i \in \underline{k}$. Ein Repräsentantensystem für die Assoziiertenklassen der Länge $\geq i$ ist

$$B_i := \left\{ x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mid i_1, \dots, i_n \in \mathbb{N}_0, i_1 + \cdots + i_n \in \{i, \dots, k\} \right\},$$

also ist $r_i = |B_i|$ und damit ist r_i gleich der Anzahl der Tupel $(i_1, \ldots, i_n) \in \mathbb{N}_0^n$ für die $\sum_{j=1}^n i_j \in \{i, \ldots, k\}$ gilt. Sei $m \in \underline{k}$.
Es sei $B_{=m} := \left\{(i_1, \ldots, i_n) \in \mathbb{N}_0^n \mid \sum_{j=1}^n i_j = m\right\}$ und

$$\alpha : B_{=m} \to \left\{ y \in \{0,1\}^{m+n-1} \mid \sum_{j=1}^{m+n-1} y_j = m \right\} =: N_m,$$
$$(i_1, \ldots, i_n) \mapsto (\underbrace{1, \ldots, 1}_{i_1}, 0, \underbrace{1, \ldots, 1}_{i_2}, 0, \ldots, 0, \underbrace{1, \ldots, 1}_{i_n}).$$

Es ist α offenbar eine Bijektion und es ist $|N_m| = \binom{m+n-1}{n-1}$. Damit folgt

$$\begin{aligned} r_i = |B_i| &= \sum_{m=i}^{k} |B_{=m}| = \sum_{m=i}^{k} |N_m| \\ &= \sum_{m=i}^{k} \binom{m+n-1}{n-1} = \sum_{m=0}^{k} \binom{m+n-1}{n-1} - \sum_{m=0}^{i-1} \binom{m+n-1}{n-1} \\ &= \binom{n+k}{n} - \binom{n+i-1}{n}. \end{aligned}$$

□

Bezeichnungen 3.10 Es sei nun $i \geq \left\lceil \frac{k+1}{2} \right\rceil$. Wir setzen

$$V_{i,R_i} := \langle R_i \rangle.$$

Nach Wahl von i entspricht die $*$-Verknüpfung auf V_{i,R_i} der Addition, da alle Produkte in V_{i,R_i} Null sind. Es folgt somit aus der K-linearen Unabhängigkeit der Elemente von R_i

$$V_{i,R_i} \cong (K, +)^{r_i}.$$

Da bei dem weiteren Vorgehen in diesem Kapitel die Wahl des Repräsentantensystems R_i keinen Einfluss hat, schreiben wir auch V_i statt V_{i,R_i}. Es enthält R_i (und damit auch V_i) genau ein Element jeder Assoziiertenklasse der Länge $\geq i$. Es folgt:

Bemerkung 3.11 Es gilt $V_i \cap C = \{0\}$ und V_i ist eine K-Teilalgebra von N.

Bezeichnungen 3.12 Es sei für alle $i \in \underline{k}$

$$C_i := C \cap N^i.$$

Als Schnitt zweier $*$-Normalteiler ist C_i ein $*$-Normalteiler von N. Weiter sei

$$M_i := \left\langle X^{<i} \right\rangle_* * C_i.$$

Es ist M_i eine Untergruppe von N, da $C_i \trianglelefteq N$ ist.

Für den Rest dieses Abschnittes sei nun $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ mit $c \in \mathbb{N}_{>1}$.

Lemma 3.13 Für alle $i \geq \left\lceil \frac{k+1}{2} \right\rceil$ gilt $V_i * M_i = N$.

Beweis. Sei $i \geq \left\lceil \frac{k+1}{2} \right\rceil$. Wir zeigen zunächst, dass $V_i * M_i$ Untergruppe von $(N, *)$ ist. Sei $m \in M_i$ und $v \in V_i$. Dann gilt

$$\begin{aligned} m^{(v)} &= v^- * m * v = m + \underbrace{v^- m}_{=-vm} + mv + \underbrace{v^- mv}_{=0} \\ &= m + [m, v] \in M_i + C_i. \end{aligned}$$

Wir verwenden Lemma 1.5 mit $I = C$ und $U = M_i$. Es ist $N^i \cap C = C_i \subseteq M_i$ und $m^{(v)} \in M_i + C_i$, also ist $m^{(v)} \in M_i$ mit Lemma 1.5. Damit ist V_i im Normalisator von M_i enthalten und somit ist $V_i * M_i$ Untergruppe von $(N, *)$.
Es ist $X^{<i} \subseteq M_i$. Sei $f \in X^{\geq i}$. Ist $f \in R_i$, so ist nach Definition $f \in V_i$. Ist $f \notin R_i$, so gibt es ein $g \in R_i$ mit $f \sim g$ und es folgt

$$f = g + (f - g) = \underbrace{g}_{\in V_i} * \underbrace{(f - g)}_{\in C_i \subseteq M_i}.$$

Also ist $X^{\leq k} \subseteq V_i * M_i$ und es folgt $V_i * M_i = N$ mit Korollar 1.32.1. □

Wir sehen also, dass das Produkt von M_i und V_i die ganze Gruppe N ergibt. Nun müssen wir den Schnitt $M_i \cap V_i$ betrachten. Dafür untersuchen wir zunächst, wie sich das $*$-Produkt von Elementen aus $X^{\leq k}$ unter den Abbildungen η_W mit $W \in X^{\leq k}_{\sim}$ verhält.

Lemma 3.14 Seien $m \in \mathbb{N}$ und $f_1, \ldots, f_m \in X^{\leq k}$. Weiter seien $\alpha_1, \ldots, \alpha_m \in \mathbb{Z} \setminus \{0\}$ falls $K = \mathbb{Z}$, beziehungsweise $\alpha_1, \ldots, \alpha_m \in \underline{c-1}$ falls $K = \mathbb{Z}/c\mathbb{Z}$, und $a := \bigstar_{r=1}^{m} f_r^{(\alpha_r)}$. Es sei $W \in X^{\leq k}_{\sim}$ mit minimaler Länge gewählt, sodass $W \cap \{f_1, \ldots, f_m\} \neq \emptyset$ gilt. Dann folgt in K

$$a\eta_W = \sum_{f_i \in W \cap \{f_1, \ldots, f_m\}} \alpha_i.$$

Beweis. Wir fixieren wie folgt eine totale Ordnung $\propto$ auf den Elementen von $X^{\leq k}$:

- Sind $f, g \in X^{\leq k}$ so gelte: $l(f) < l(g) \Rightarrow f \propto g$
- Innerhalb einer Länge seien die Elemente von $X^{\leq k}$ so geordnet, dass Elemente der gleichen Assoziiertenklassen direkt hintereinander stehen.
- Unter den Assoziiertenklassen der gleichen Länge wie W seien die Elemente von W zuerst aufgeführt.

Für die Betrachtung von $a\eta_W$ kann wegen $N' \subseteq C$ nach Lemma 3.6 (b) o.B.d.A. angenommen werden, dass $f_1, \ldots, f_m$ gemäß $\propto$ geordnet sind. Dann gibt es auf Grund der

gewählten Ordnung ein $s \in \underline{m}$ maximal mit $f_1, \ldots, f_s \in W$. Sei $r := \bigstar_{r=s+1}^{m} f_r^{(\alpha_r)}$. Dann folgt

$$\begin{aligned}
a\eta_W &= \left(\bigstar_{r=1}^{m} f_r^{(\alpha_r)} \right) \eta_W \\
&= \left(\bigstar_{r=1}^{s} f_r^{(\alpha_r)} \right) \eta_W + \underbrace{r\eta_W}_{=0 \text{ nach Wahl von } \propto} + \underbrace{\left(\left(\bigstar_{r=1}^{s} f_r^{(\alpha_r)} \right) \cdot r \right) \eta_W}_{=0 \text{ nach Wahl von } \propto} \\
&= \left(\sum_{r=1}^{s} f_r^{(\alpha_r)} \right) \eta_W \qquad \text{(nach Lemma 1.2 (d), da Produkte der } f_i \text{ keine Summanden in } W \text{ haben)} \\
&= \left(\sum_{r=1}^{s} \alpha_r f_r \right) \eta_W \qquad \text{(Lemma 1.2 (e), nur der kürzeste Summand liegt in } W) \\
&= \sum_{r=1}^{s} \alpha_r.
\end{aligned}$$

□

Korollar 3.14.1 Es gelte $K = \mathbb{Z}$ oder $\mathrm{ggT}(c, k!) = 1$. Seien in Lemma 3.14 $f_1, \ldots, f_m$ gemäß $\propto$ geordnet. Es gebe also $t, s_1, \ldots, s_t \in \underline{m}$, $s_t = m$ und $W_1, \ldots, W_t \in X_{\sim}^{\leq k}$ paarweise verschieden mit

$$\underbrace{f_1, \ldots, f_{s_1}}_{\in W_1}, \underbrace{f_{s_1+1}, \ldots, f_{s_2}}_{\in W_2}, \underbrace{f_{s_2+1}, \ldots}_{\in W_3} \ldots \ldots, \underbrace{f_{s_t}}_{\in W_t}.$$

Weiter gelte $a\eta_{W_i} = 0_K$ für alle $i \in \underline{t}$. Dann folgt $a\eta_W = 0_K$ für alle $W \in X_{\sim}^{\leq k}$.

Beweis. Sei $s_0 := 0$. Für alle $i \in \underline{t}$ sei $\beta_i := \sum_{j=s_{i-1}+1}^{s_i} \alpha_j$. Da nach Voraussetzung $a\eta_{W_i} = 0_K$ gilt, folgt mit Lemma 3.14 $\beta_1 = 0$, falls $K = \mathbb{Z}$, und $c \mid \beta_1$, falls $K = \mathbb{Z}/c\mathbb{Z}$. Ist $K = \mathbb{Z}$, so ist $b^{(\beta_1)} = b^{(0)} = 0$ für alle $b \in N$ und ist $K = \mathbb{Z}/c\mathbb{Z}$ so ist nach Korollar 1.35.2 $b^{(\beta_1)} = 0$ für alle $b \in N$, da nach Voraussetzung $\mathrm{ggT}(c, k!) = 1$ gilt.
Sei $W \in X^{\leq k}$. Dann gilt

$$\begin{aligned}
a\eta_W &= \left(\bigstar_{r=1}^{m} f_r^{(\alpha_r)} \right) \eta_W \\
&\overset{3.6\,(\mathrm{d})}{=} \left(\bigstar_{i=1}^{t} f_{s_i}^{(\sum_{j=s_{i-1}+1}^{s_i} \alpha_j)} \right) \eta_W \\
&= \left(\bigstar_{i=1}^{t} f_{s_i}^{(\beta_i)} \right) \eta_W \\
&\overset{f_{s_1}^{(\beta_1)}=0}{=} \left(\bigstar_{i=2}^{t} f_{s_i}^{(\beta_i)} \right) \eta_W.
\end{aligned}$$

Die Behauptung folgt mit Induktion nach t. □

Lemma 3.15 Sei $i \in \underline{k}$. Dann gilt

$$M_i \cap N^i = C_i.$$

Beweis. „$\supseteq$“ Folgt direkt aus der Definition von M_i und C_i.
„$\subseteq$“ Sei $a \in M_i \cap N^i$ und $\propto$ wie in dem Beweis zu Lemma 3.14. Dann gibt es ein $m \in \mathbb{N}_0$ und $f_1, \ldots, f_m \in X^{<i}$ und $\alpha_1, \ldots, \alpha_m \in \mathbb{Z} \setminus \{0\}$, falls $K = \mathbb{Z}$, beziehungsweise $\alpha_1, \ldots, \alpha_m \in \underline{c-1}$, falls $K = \mathbb{Z}/c\mathbb{Z}$, sowie $b \in C \cap N^i$ mit

$$a = \underbrace{\left(\mathop{\bigstar}_{r=1}^{m} f_r^{(\alpha_r)} \right)}_{=:r} * b.$$

Da wir uns nur für $a\eta_W$ für alle $W \in X_{\sim}^{\leq k}$ interessieren, können wir wegen $N' \subseteq C$ o.B.d.A. annehmen, dass $f_1, \ldots, f_m$ gemäß $\propto$ geordnet sind. Zum Beweis der Behauptung genügt es, $a\eta_W = 0$ für alle $W \in X_{\sim}^{\leq k}$ zu zeigen. Sei $W \in X_{\sim}^{\leq k}$. Dann gilt mit Bemerkung 3.5

$$\begin{aligned} a\eta_W &= (r * b)\eta_W \\ &= r\eta_W + \underbrace{b\eta_W}_{=0, \text{ da } b \in C} + \underbrace{(rb)\eta_W}_{=0, \text{ da } b \in C \text{ und } C \text{ Ideal}} \\ &= r\eta_W. \end{aligned}$$

Also bleibt $r\eta_W = 0$ zu zeigen.
Es liegen $f_1, \ldots, f_m$ in Assoziiertenklassen der Länge $< i$. Ist daher $f_j \in V$ für ein $j \in \underline{m}$, $V \in X_{\sim}^{\leq i}$, so folgt $r\eta_V \overset{\text{s.o.}}{=} a\eta_V = 0$, da $a \in N^i$ gilt. Somit ist die Voraussetzung von Korollar 3.14.1 erfüllt und es folgt $a\eta_W = r\eta_W = 0$ für alle Assoziiertenklassen W. Also ist $a \in C \cap N^i = C_i$. □

Korollar 3.15.1 Für alle $i \geq \left\lceil \frac{k+1}{2} \right\rceil$ folgt $M_i \cap V_i = \{0\}$.

Beweis. Sei $i \geq \left\lceil \frac{k+1}{2} \right\rceil$. Es ist $V_i \subseteq N^i$. Damit folgt

$$M_i \cap V_i = M_i \cap (N^i \cap V_i) = (M_i \cap N^i) \cap V_i \overset{3.15}{=} C_i \cap V_i \overset{3.11}{=} \{0\}.$$

□

Es gilt also $M_i * V_i = N$ und $M_i \cap V_i = \{0\}$ für alle $i \geq \left\lceil \frac{k+1}{2} \right\rceil$. Damit bleibt für Satz 3.3 nur noch die Normalteilereigenschaft von M_i zu zeigen.

Bemerkung 3.16 Es ist M_i für alle $i \geq \left\lceil \frac{k+1}{2} \right\rceil$ ein $*$-Normalteiler von N.

Beweis. Es genügt zu zeigen, dass M_i/C_i ein Normalteiler von N/C_i ist. Nach Lemma 3.6 (a) und Lemma 1.11 gilt $[N^{i-1}, N]_* \subseteq C \cap N^i = C_i$. Also dürfen modulo C_i die Elemente der Länge $\geq i - 1$ mit allen Elementen vertauscht werden. Sei nun $a \in M_i$

und $b \in N$. Nach Lemma 3.13 gibt es $b_M \in M_i$ und $b_V \in V_i$ mit $b = b_M * b_V$. Dann ist $d := a^{(b_M)} \in M_i$ und $b_V \in N^{i-1}$. Es folgt mit Lemma 1.11 (b) und Lemma 3.6 (a)

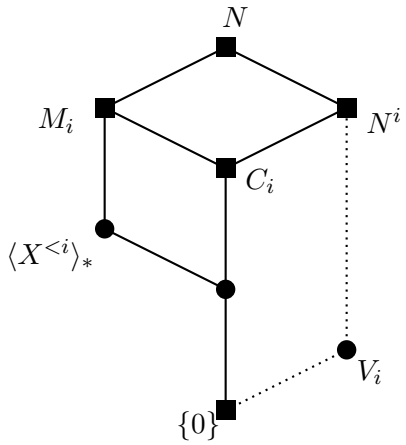
$$[b_V, d]_* \in N^i \cap C = C_i.$$

Damit erhalten wir

$$(a * C_i)^{(b*C_i)} = a^{(b)} * C_i = (a^{(b_M)})^{(b_V)} * C_i = d^{(b_V)} * C_i = d * C_i \in M_i/C_i.$$

Also ist M_i Normalteiler von N. □

Nun können wir Satz 3.3 unter Angabe der Untergruppen formulieren und beweisen:



Satz 3.3 (ausführliche Formulierung)
Sei $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ für ein $c \in \mathbb{N}_{>1}$ mit $\mathrm{ggT}(c, k!) = 1$. Sei $i \geq \left\lceil \frac{k+1}{2} \right\rceil$, R_i ein Repräsentantensystem der Assoziiertenklassen der Länge $\geq i$,

$$M_i := \langle X^{<i}\rangle_* * C_i \quad \text{und}$$
$$V_i := \langle R_i \rangle.$$

Dann ist

$$N = V_i \ltimes M_i$$

und $V_i \cong (K,+)^{\binom{n+k}{n}-\binom{n+i-1}{n}}$.

Beweis. Es sind M_i, V_i Untergruppen von N mit $M_i \cap V_i = \{0\}$ nach Korollar 3.15.1. Weiter ist $M_i * V_i = N$ nach Lemma 3.13. Nach Bemerkung 3.16 ist M_i ein Normalteiler von N. Insgesamt folgt also

$$N = V_i \dot{\ltimes} M_i \overset{3.10}{\cong} (K,+)^{r_i} \ltimes M_i$$

mit $r_i = \binom{n+k}{n} - \binom{n+i-1}{n}$ nach Bemerkung 3.9. □

Bemerkung 3.17 Der Fall $i = k$ liefert eine Zerlegung, bei der V_k eine Untergruppe des Zentrums ist. In diesem Fall gilt also sogar $N = V_k \times M_k$ im direkten Produkt. Außerdem ist

$$V_k \cong (K,+)^{\binom{n+k}{n}-\binom{n+k-1}{n}} = (K,+)^{\binom{n+k-1}{n-1}}.$$

Bemerkung 3.18 Sei $i \geq \left\lceil \frac{k+1}{2} \right\rceil$. Die Operation von V_i auf M_i ist gegeben durch

$$m^{(v)} = m + [m, v] \qquad \text{für alle } v \in V_i \text{ und } m \in M_i.$$

Beweis. Es gilt für alle $a \in N^i$ und $b \in N$

$$\begin{aligned} b^{(a)} &= a^- + b + a + a^-b + a^-a + ba + a^-ba \\ &= \underbrace{a^- + a + a^-a}_{=0} + b + \underbrace{a^-}_{=-a \text{ nach Wahl von } i} + b + ba + \underbrace{a^-ba}_{=0 \text{ nach Wahl von } i} \\ &= b + [b, a]. \end{aligned}$$

Mit $V_i \subseteq N^i$ folgt die Behauptung. □

Wir wollen nun bemerken, dass die Annahme $\mathrm{ggT}(c, k!) = 1$ im Fall $K = \mathbb{Z}/c\mathbb{Z}$ für die Aussage des Satzes 3.3 nötig ist:
Ist beispielsweise $c = 2 = k$ und $x \in X$, so ist $x^2 = 2x + x^2 = x^{(2)} \in \langle X \rangle_* \leq M_2$. Andererseits ist x^2 aber auch in jedem Repräsentantensystem der Assoziiertenklassen der Länge 2 enthalten. Also gilt auch $x^2 \in V_2$ und somit ist $M_2 \cap V_2 \neq \{0\}$.

Das Verhältnis von c und k wird auch in dem folgenden Satz und in den weiteren Abschnitten immer wieder eine Rolle spielen. Das Ideal C wird uns insbesondere im nächsten Abschnitt über die Kommutator- und Frattini-Untergruppe weiter begleiten.

Nun werden wir die Gruppe $(N, *)$ als Produkt von zyklischen Gruppen schreiben und unter geeigneten Bedingungen an den Grundring einsehen, dass dieses Produkt eine semidirekte Zerlegung ist. Auch hierfür sei X n-elementig.

Satz 3.19 Für alle $i \in \underline{k}$ sei $B_i \subseteq N^i$ eine n^i-elementige Menge, $B_i = \{b_{i,1}, \ldots, b_{i,n^i}\}$, sodass $\{b_{i,1}\pi_i, \ldots, b_{i,n^i}\pi_i\}$ eine K-Basis von $N\pi_i$ ist. Sei $s \in \mathbb{N}$ und $\kappa = \{c_1, \ldots, c_s\} \subseteq K$ ein additives Erzeugendensystem von K. Wir setzen

$$\mathcal{U}_{i,j,r} := \langle c_r b_{i,j} \rangle_*$$

für alle $i \in \underline{k}$, $j \in \underline{n^i}$ und $r \in \underline{s}$.

(a) Es gilt

$$N = \bigstar_{i=1}^{k} \bigstar_{j=1}^{n_i} \bigstar_{r=1}^{s} \mathcal{U}_{i,j,r}.$$

(b) Sei $p \in \mathbb{P}_{>k}$, $l \in \mathbb{N}$ und $(K, +) \in \{(\mathbb{Z}^s, +), ((\mathbb{Z}/p^l\mathbb{Z})^s, +)\}$.[7] Sei κ eine $\mathbb{Z}$- beziehungsweise $\mathbb{Z}/p^l\mathbb{Z}$-Basis von K und

$$O := \begin{cases} \underline{p^l - 1_0} & \text{char } K = p^l \\ \mathbb{Z} & \text{sonst} \end{cases}.$$

Dann ist

$$\left(\mathcal{U}_{k,n^k,s}, \mathcal{U}_{k,n^k,s-1}, \ldots, \mathcal{U}_{k,1,1}, \mathcal{U}_{k-1,n^{k-1},s}, \ldots, \mathcal{U}_{1,1,1}\right)$$

[7] Diese Voraussetzung enthält neben $\mathbb{Z}$ und den Faktorringen von $\mathbb{Z}$ auch den Fall endlicher Körper der Charakteristik $> k$ und beispielsweise auch $\mathbb{Z}[i]$.

eine Zerlegung von N. Insbesondere gilt

$$N = \left\{ \mathop{\bigstar}_{i=1}^{k} \mathop{\bigstar}_{j=1}^{n^i} \mathop{\bigstar}_{r=1}^{s} (c_r b_{i,j})^{(\alpha_{r,i,j})} \mid \forall i \in \underline{k}, j \in \underline{n^i}, r \in \underline{s} : \alpha_{r,i,j} \in O \right\}$$

und die Darstellung der Elemente von N in dieser Form ist eindeutig.

Beweis. (a) Für alle $i \in \underline{k}$ und $j \in \underline{n^i}$ sei $\mathcal{U}_{i,j} := \bigstar_{r=1}^{s} \mathcal{U}_{i,j,r}$. Dann ist nach Lemma 1.32 für alle $i \in \underline{k}$

$$N^i/N^{i+1} = \mathop{\bigtimes}_{j=1}^{n^i} (\mathcal{U}_{i,j} * N^{i+1})/N^{i+1}.$$

Mit Satz 1.58 (a) folgt

$$N = N^- = \left(N^1\right)^- = \left(\mathop{\bigstar}_{i=0}^{k-1} \mathop{\bigstar}_{j=0}^{n^{k-i}-1} \mathcal{U}_{k-i,n^{k-i}-j} \right)^- = \mathop{\bigstar}_{i=1}^{k} \mathop{\bigstar}_{j=1}^{n^i} \mathcal{U}_{i,j} = \mathop{\bigstar}_{i=1}^{k} \mathop{\bigstar}_{j=1}^{n^i} \mathop{\bigstar}_{r=1}^{s} \mathcal{U}_{i,j,r}.$$

(b) Sei $i \in \underline{k}$, $j \in \underline{n^i}$ und $r \in \underline{s}$. Ist char $K = p^l$, so ist $o(c_r b_{i,j}) = p^l$ nach Korollar 1.35.1. Ist char $K = 0$, so ist nach Korollar 1.27.1 $c_r b_{i,j}$ von unendlicher Ordnung.
Wir zeigen nun die Voraussetzungen von Korollar 1.58.1. Es ist $(N^{k+1}, N^k, \ldots, N^2, N)$ nach Lemma 1.30 (c) die aufsteigende Zentralreihe von N. Es ist für alle $i \in \underline{k}$

$$N^i/N^{i+1} = \mathop{\bigtimes}_{j=1}^{n^i} \mathop{\bigtimes}_{r=1}^{s} \mathcal{U}_{i,j,r} * N^{i+1}/N^{i+1}.$$

Außerdem ist für alle $i \in \underline{k}$, $j \in \underline{n^i}$, $r \in \underline{s}$ und $m \in O \setminus \{0\}$

$$(c_r b_{i,j})^{(m)} \pi_i = (m c_r) b_{i,j} \pi_i \neq 0.$$

Damit ist $\langle c_r b_{i,j} \rangle_* \cap N^{i+1} = \{0\}$. Nach Satz 1.58 ist damit

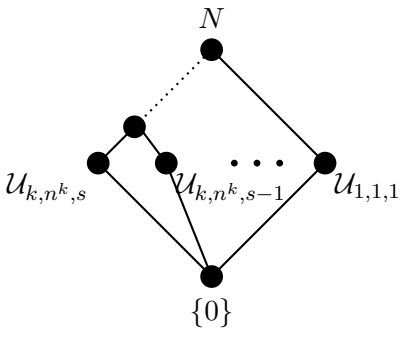
$$(\mathcal{U}_{k,n^k,s}, \mathcal{U}_{k,n^k,s-1}, \ldots, \mathcal{U}_{k,1,1}, \mathcal{U}_{k-1,n^{k-1},s}, \ldots, \mathcal{U}_{1,1,1})$$

eine Zerlegung von N und mit Korollar 1.58.1 (c) folgt die Eindeutigkeit der Darstellung. □

Korollar 3.19.1 Es ist $\mathcal{U}_{i,j,r} * N^{i+1}/N^{i+1} \leq N^i/N^{i+1} = Z(N/N^{i+1})$ für alle $i \in \underline{k}$, $j \in \underline{n^i}$ und $r \in \underline{s}$. Damit folgt

$$N = (\cdots(\mathcal{U}_{k,n^k,s} \rtimes \mathcal{U}_{k,n^k,s-1}) \rtimes \ldots) \rtimes \mathcal{U}_{k,1,1}) \rtimes \mathcal{U}_{k-1,n^{k-1},s}) \rtimes \ldots) \rtimes \mathcal{U}_{1,1,1}).$$

Außerdem ist $\mathcal{U}_{i,j,r} \cong \mathbb{Z}$, falls char $K = 0$, und $\mathcal{U}_{i,j,r} \cong \mathcal{C}_{p^l}$, falls char $K = p^l$, für alle $i \in \underline{k}$, $j \in \underline{n^i}$ und $r \in \underline{s}$. Damit ist die in Satz 3.19 (b) angegebene Zerlegung eine iterierte semidirekte Zerlegung von N in zyklische Gruppen.



Bemerkung 3.20 $B_i := X^{=i}$ für alle $i \in \underline{k}$ erfüllt die Voraussetzung von Satz 3.19.

3.2 Zur Kommutator- und Frattini-Untergruppe

Wir wollen nun die Kommutatoruntergruppe N' und die Frattini-Untergruppe $\Phi(N)$ von $(N, *)$ betrachten. Wir haben in Korollar 3.7.1 bereits gesehen, dass das Ideal C immer N' enthält und sogar das kleinste Ideal mit dieser Eigenschaft ist. Außerdem wissen wir, dass $(N, *)$ nilpotent ist, und damit $N' \leq \Phi(N)$ nach [Hal76, Seite 157, Theorem 10.4.3] gilt.

Das Problem bei der Bestimmung der Kommutatoruntergruppe ist, dass sie im Allgemeinen kein Teilring von N ist. Daher ist N' nach Lemma 1.8 weder additiv noch multiplikativ abgeschlossen. Wir können mit Hilfe von Lemma 1.11 zwar die Kommutatoren berechnen, aber deren $*$-Abschluss zu beschreiben wird uns im Allgemeinen nicht gelingen.

Wir wollen nun ein Beispiel für eine nilpotente Algebra konstruieren, in welcher die $*$-Kommutatoruntergruppe kein Teilring ist.

In diesem Abschnitt sei X n-elementig, $X = \{x_1, \ldots, x_n\}$.

Bezeichnungen 3.21 In $N := N_{K,\{x,y\},4}$ sei I das von x^2 und y^2 erzeugte Ideal. Wir setzen $H := N/I$. Nach Bemerkung 1.4 gilt $a * I = a + I$ für alle $a \in N$.

Wir wollen nun die Kommutatoruntergruppe H' von $(H, *)$ bestimmen.

Lemma 3.22 (a) Die Menge

$$B := \{x + I, y + I, xy + I, yx + I, xyx + I, yxy + I, xyxy + I, yxyx + I\}$$

ist eine K-Basis von H.

Sei $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ für ein $c \in \mathbb{N}_{>1}$.

(b) Für die Kommutatoruntergruppe von H gilt

$$H' = \langle [x, y] + xyxy + I, xyx + I, yxy + I, [x, yxy] + I \rangle_*.$$

(c) Gilt $K = \mathbb{Z}$ oder $2 \nmid c$, so ist H' nicht multiplikativ abgeschlossen. Insbesondere ist dann H' keine Teilalgebra von H.

Beweis. (a) Es ist $X^{\leq 4}$ eine K-Basis von N und nach Definition von I ist die Menge

$$B_I := \left\{ f \in X^{\leq 4} \mid \ x^2 \text{ ist Teilwort von } f \text{ oder } y^2 \text{ ist Teilwort von } f \right\} \subseteq X^{\leq 4}$$

eine K-Basis von I. Damit ist

$$B = \{f + I \mid f \in X^{\leq 4} \setminus B_I\}$$

eine K-Basis für H.
(b) Sei

$$U := \langle [x,y] + xyxy + I, xyx + I, yxy + I, [x,yxy] + I \rangle_*.$$

Es gilt mit Lemma 1.11

$$\begin{aligned}
[x,yxy] + I &= [x,yxy]_* + I \in H', \\
xyx + I &= xyx - yx^2 - x^2yx + xyx^2 + I \\
&= [x,yx] - x[x,yx] + I \\
&= [x,yx]_* + I \in H', \\
yxy + I &= yxy - xy^2 - y^2xy + yxy^2 + I \\
&= [y,xy] - y[y,xy] + I \\
&= [y,xy]_* + I \in H' \quad \text{und} \\
[x,y] + xyxy + I &= [x,y] - x^2y + xyx - xyx - yxy + yxy + y^2x + xyxy - xy^2x + I \\
&= \underbrace{[x,y] - x[x,y] - y[x,y] + xy[x,y]}_{=[x,y]_*} - xyx + yxy + I \\
&= [x,y]_* - [x,yx] + [y,xy] - \underbrace{yx^2 + xy^2}_{\in I} + I \\
&= [x,y]_* \underbrace{- [x,yx] + \underbrace{x[x,yx]}_{\in I}}_{=[x,yx]_*^-} + \underbrace{[y,xy] - \underbrace{y[y,xy]}_{\in I}}_{=[y,xy]_*} + I \\
&= ([x,y]_* + I) * ([x,yx]_* + I)^- * ([y,xy]_* + I) \in H'.
\end{aligned}$$

Damit folgt $U \leq H'$.
Nach Lemma 1.32 ist B_I ein $*$-Erzeugendensystem von I und nach Korollar 1.32.1 ist $X^{\leq 4}$ ein $*$-Erzeugendensystem von N. Damit ist B ein $*$-Erzeugendensystem von H. Es gilt für alle $a, b, c \in H$

$$[a, b * c]_* = [a,c]_* * [a,b]_*^{(c)}.$$

Damit genügt es für $H' \leq U$ zu zeigen, dass U ein Normalteiler von H ist, der alle Kommutatoren in $B \cup B^-$ enthält.
Wir zeigen zunächst die Normalteilereigenschaft von U. Sei dazu

$$D := \{[x,y] + xyxy + I, xyx + I, yxy + I, [x,yxy] + I\}.$$

Dann ist D ein $*$-Erzeugendensystem von U. Wir zeigen $d^{(b)} \in U$ für alle $d \in D$ und $b \in B$. Sei $d \in D$ und $b \in B$. Wir nutzen in den folgenden Rechnungen aus, dass nach Bemerkung 1.3 (e) $H, H^2, H^3, H^4, H^5 = \{0\}$ eine absteigende Zentralkette von $(H, *)$ ist.

- Ist $d = [x,yxy] + I$, so ist $d \in Z(H)$ und damit $d^{(b)} = d \in U$.

- Sei $d \in \{xyx + I, yxy + I\}$. Dann ist

$$\begin{aligned} d^{(b)} &\in \Big\{xyx + I, yxy + I, \underbrace{(xyx)^{(x)} + I}_{=xyx+I}, (yxy)^{(x)} + I, (xyx)^{(y)} + I, \underbrace{(yxy)^{(y)} + I}_{=yxy+I}\Big\} \\ &= \{xyx + I, yxy + I, yxy - [x, yxy] + I, xyx + [x, yxy] + I\} \\ &= \{xyx + I, yxy + I, (yxy + I) * ([x, yxy] + I)^-, (xyx + I) * ([x, yxy] + I)\} \\ &\subseteq U. \end{aligned}$$

- Sei $d = [x, y]+xyxy+I$. Wegen $xyxy+I \in Z(H)$ ist $d^{(b)} = ([x, y]+I)^{(b)}+xyxy+I$ nach Lemma 1.10 (b). Es folgt

$$\begin{aligned} d^{(b)} &\in \{d, [x, y]^{(x)} + xyxy + I, [x, y]^{(y)} + xyxy + I, \\ &\qquad \underbrace{[x, y]^{(xy)} + xyxy + I}_{=[x,y]+[[x,y],xy]+xyxy+I=d}, \quad \underbrace{[x, y]^{(yx)} + xyxy + I}_{=[x,y]+[[x,y],yx]+xyxy+I=d} \} \\ &= \{d, [x, y] - x[x, y] + [x, y]x - x[x, y]x + xyxy + I, \\ &\qquad [x, y] - y[x, y] + [x, y]y - y[x, y]y + xyxy + I\} \\ &= \{d, [x, y] + 2xyx + xyxy + I, [x, y] - 2yxy + xyxy + I\} \\ &= \Big\{d, d * (xyx + I)^{(2)}, d * (yxy + I)^{(-2)}\Big\} \subseteq U. \end{aligned}$$

Damit ist U ein Normalteiler von H.
Nun zeigen wir, dass U alle Kommutatoren von Elementen aus $B \cup B^-$ enthält. Seien $a, b \in B \cup B^-$. In den folgenden Berechnungen nutzen wir erneut aus, dass nach Bemerkung 1.3 (e) $H, H^2, H^3, H^4, H^5 = \{0\}$ eine absteigende Zentralkette von $(H, *)$ ist. Außerdem verwenden wir die Formel aus Lemma 1.11 (b) für die Berechnung der $*$-Kommutatoren.

- Ist $a \in \{xyxy + I, yxyx + I, (xyxy + I)^-, (yxyx + I)^-\}$, so ist $a \in Z(H)$ und $[a, b]_* = 0 \in U$.

- Sei $a \in \{xyx + I, yxy + I, (xyx + I)^-, (yxy + I)^-\}$. Dann ist $[a, b]_* = [a, b]$ und $a^- = -a$. Es folgt

$$\begin{aligned} [a, b]_* &\in \{0, \pm[xyx, x] + I, \pm[yxy, x] + I, \pm[xyx, y] + I, \pm[yxy, y] + I\} \\ &= \{0, [x, yxy] + I, ([x, yxy] + I)^-\} \subseteq U. \end{aligned}$$

- Sei $a \in \{xy + I, yx + I, (xy + I)^-, (yx + I)^-\}$. Es ist

$$\begin{aligned} [a, b]_* &= [a, b] - b[a, b] = [a, b] * (b[a, b])^- \quad \text{und} \\ [a, b] &\in \{0, \pm[xy, x] + I, \pm[xy, y] + I, \pm[xy, yx] + I, \pm[yx, x] + I, \pm[yx, y] + I\} \\ &= \{0, \pm xyx + I, \pm yxy + I\} \\ &= \{0, xyx + I, yxy + I, (xyx + I)^-, (yxy + I)^-\} \subseteq U \quad \text{sowie} \\ b[a, b] &\in \{0, \pm x[xy, x] + I, \pm y[xy, y] + I, \pm x[yx, x] + I, \pm y[yx, y] + I\} = \{0\} \subseteq U. \end{aligned}$$

Also ist $[a, b]_* \in U$.

- Sei $a \in \{x+I, y+I, (x+I)^-, (y+I)^-\}$. Ist $b \notin \{x+I, y+I, (x+I)^-, (y+I)^-\}$, so folgt $[a,b]_* \in U$ mit $[a,b]_* = [b,a]_*^-$ aus den bereits betrachteten Fällen. Sei also $b \in \{x+I, y+I, (x+I)^-, (y+I)^-\}$. Dann ist $a^2 = 0 = b^2$ und damit $a^- = -a$ sowie $b^- = -b$. Es folgt

$$\begin{aligned}[a,b]_* &= [a,b] - a[a,b] - b[a,b] + ab[a,b] \\ &= [a,b] - a^2b + aba - bab + b^2a + abab - ab^2a \\ &= [a,b] * aba * (bab)^- * abab \\ &= [a,b] * abab * aba * (bab)^-.\end{aligned}$$

  Sei o.B.d.A. $a \in \{x+I, (x+I)^-\}$ und $b \in \{y + I(y+I)^-\}$. Dann ist

$$\begin{aligned}aba &\in \{xyx+I, -xyx+I\} = \{xyx+I, (xyx+I)^-\} \subseteq U, \\ bab &\in \{yxy+I, -yxy+I\} = \{yxy+I, (yxy+I)^-\} \subseteq U \quad \text{und} \\ [a,b] * abab &\in \{[x,y] + xyxy + I, -[x,y] + xyxy + I\} \\ &= \{[x,y] + xyxy + I, -[x,y] + [x,y]^2 - yxyx + I\} \\ &= \{[x,y] + xyxy + I, -[x,y] - xyxy + [x,y]^2 + [x,yxy] + I\} \\ &= \{[x,y] + xyxy + I, ([x,y] + xyxy + I)^- * ([x,yxy] + I)\} \subseteq U.\end{aligned}$$

  Somit ist $[a,b]_* \in U$.

Damit enthält U alle Kommutatoren in $B \cup B^-$ und es folgt $U = H'$.
(c) Es ist H' abelsch, da die in (b) angegebenen Erzeuger paarweise miteinander kommutieren und $([x,y] + xyxy + I)^2$ ist das einzige Produkt in den Erzeugern, dass nicht Null ist. Damit ist nach Lemma 1.2 (d) und (e)

$$H' = \left\{ ([x,y] + xyxy)^{(\alpha)} + \beta xyx + \gamma yxy + \delta[x,yxy] + I \mid \alpha, \beta, \gamma, \delta \in \mathbb{Z} \right\}.$$

Weiter ist

$$([x,y] + xyxy + I)^2 = (xy - yx)^2 + I = xyxy + yxyx + I.$$

Angenommen, es ist $([x,y] + xyxy + I)^2 \in H'$. Dann gibt es $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ mit

$$(xyxy + I) + (yxyx + I) = ([x,y] + xyxy)^{(\alpha)} + \beta xyx + \gamma yxy + \delta(xyxy - yxyx) + I.$$

Ist $\alpha \geq 0$, so ist nach Lemma 1.2 (c)

$$\begin{aligned}(xyxy + I) + (yxyx + I) &= \alpha(xy + I) - \alpha(yx + I) + \beta(xyx + I) + \gamma(yxy + I) \\ &\quad + \left(\alpha + \binom{\alpha}{2} + \delta\right)(xyxy + I) + \left(\binom{\alpha}{2} - \delta\right)(yxyx + I)\end{aligned}$$

und ist $\alpha < 0$, so ist nach Lemma 1.2 (f)

$$\begin{aligned}(xyxy + I) + (yxyx + I) &= \alpha(xy + I) - \alpha(yx + I) + \beta(xyx + I) + \gamma(yxy + I) \\ &\quad + \left(\alpha + \binom{|\alpha| + 1}{2} + \delta\right)(xyxy + I) + \left(\binom{|\alpha| + 1}{2} - \delta\right)(yxyx + I)\end{aligned}$$

Ist $K = \mathbb{Z}$, so folgt in beiden Fällen mit Koeffizientenvergleich $\alpha = \beta = \gamma = 0$ und damit $1 = \delta = -1$, ein Widerspruch.

Sei $K = \mathbb{Z}/c\mathbb{Z}$ mit $2 \nmid c$. Dann können wir o.B.d.A $\alpha, \beta, \gamma, \delta \geq 0$ annehmen, da H endlich ist. Es folgt mit Koeffizientenvergleich $c \mid \alpha, \beta, \gamma$ und

$$\binom{\alpha}{2} + \delta \underset{c}{\equiv} \alpha + \binom{\alpha}{2} + \delta \underset{c}{\equiv} \binom{\alpha}{2} - \delta, \quad \text{also} \quad 2\delta \underset{c}{\equiv} 0.$$

Mit $2 \nmid c$ folgt daraus $c \mid \delta$. Außerdem gilt $c \mid \binom{\alpha}{2}$ mit $2 \nmid c$ und $c \mid \alpha$ nach Lemma 1.15 und wir erhalten

$$(xyxy + I) + (yxyx + I) = 0,$$

ein Widerspruch. □

Nun können wir für $K = \mathbb{Z}$ und $K = \mathbb{Z}/c\mathbb{Z}$ mit $2 \nmid c$ bestimmen, für welche Anzahl n von Erzeugern und für welche Nilpotenzklasse k die Kommutatoruntergruppe N' Ideal, Teilalgebra oder keine Teilalgebra von N ist.

Satz 3.23 Sei $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ mit $c \in \mathbb{N}_{>1}$, $2 \nmid c$. Dann gilt:

(a) $N'_{n,k}$ ist ein Ideal von $N_{n,k}$ genau dann, wenn $n = 1$ oder $k \leq 2$ oder $(n, k) = (2, 3)$ gilt. In diesem Fall ist $N'_{n,k} = C$.

(b) $N'_{n,k}$ ist eine Teilalgebra, aber kein Ideal von $N_{n,k}$, genau dann, wenn $k = 3$ und $n \geq 3$ gilt.

(c) $N'_{n,k}$ ist kein Teilring von $N_{n,k}$ genau dann, wenn $n \geq 2$ und $k \geq 4$ gilt.

Beweis. Für $n = 1$ oder $k = 1$ ist $(N, *)$ abelsch, also ist $N' = \{0\}$ und damit insbesondere ein Ideal von N.
Ist $k \in \{2, 3\}$, so ist wegen $N' \subseteq N^2$, also $(N')^2 = \{0\}$, N' additiv abgeschlossen und damit nach Lemma 1.8 ein Teilring von N. Mit der Wahl von K ist damit N' eine Teilalgebra von N.
Ist $k = 2$, so gilt für alle $a \in N'$ und alle $b \in N$ schon $ab = 0 = ba$ und damit ist insbesondere N' ein Ideal von N.
Wir betrachten nun den Fall $(n, k) = (2, 3)$. Sei $X = \{x, y\}$. Seien $a, b, c \in N$ und $\alpha_x, \alpha_y, \beta_x, \beta_y, \gamma_x, \gamma_y \in \mathbb{Z}$ mit

$$a\pi_1 = \alpha_x x + \alpha_y y,\ b\pi_1 = \beta_x x + \beta_y y \quad \text{und} \quad c\pi_1 = \gamma_x x + \gamma_y y.$$

Dann gilt mit Lemma 1.11 (b)

$$\begin{aligned}
[a, b]_* c &= [a, b]c \\
&= [a\pi_1, b\pi_1](c\pi_1) \\
&= [\alpha_x x + \alpha_y y, \beta_x x + \beta_y y](\gamma_x x + \gamma_y y) \\
&= \alpha_x\beta_y\gamma_x[x, y]x + \alpha_x\beta_y\gamma_y[x, y]y + \alpha_y\beta_x\gamma_x[y, x]x + \alpha_y\beta_x\gamma_y[y, x]y \\
&= \underbrace{(\alpha_x\beta_y\gamma_x - \alpha_y\beta_x\gamma_x)}_{=:R}[x, yx] + \underbrace{(\alpha_x\beta_y\gamma_y - \alpha_y\beta_x\gamma_y)}_{=:S}[xy, y] \\
&= R[x, yx]_* + S[xy, y]_* \\
&= [x, yx]_*^{(R)} * [xy, y]_*^{(S)} \in N'.
\end{aligned}$$

Ebenso folgt $c[a,b]_* \in N'$. Damit ist N' ein Ideal von N.
Ist $k = 3$ und $n \geq 3$, so ist nach Bemerkung 2.9 N' kein Ideal von N.
Seien $n \geq 2$, $k \geq 4$ und $x, y \in X$, $x \neq y$. Wir betrachten die Fortsetzung von

$$X \mapsto \{x, y\},\ z \mapsto \begin{cases} z & z \in \{x, y\} \\ 0 & \text{sonst} \end{cases}$$

zu einem Epimorphismus $N_{n,k} \to H$. Nach Lemma 3.22 (c) ist H' kein Teilring von H. Damit ist auch N' keine Teilring von N. □

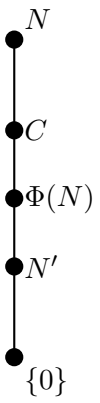
Anmerkung 3.24 Die Voraussetzung $2 \nmid c$ geht nur an der Stelle ein, wo wir zeigen, dass N' für $n \geq 2$ und $k \geq 4$ kein Teilring ist.

Korollar 3.24.1 In den Fällen (b) und (c) ist $N' \neq C$.

Wir wollen nun Beispiele für K angeben, in denen $\Phi(N_K) \subseteq C$ gilt.

Lemma 3.25 Sei $K = \mathbb{Z}$ beziehungsweise $K = \mathbb{Z}/p\mathbb{Z}$ mit $p \in \mathbb{P}$ und $p > k$. Dann ist $(N/C, *)$ frei abelsch beziehungsweise p-elementar-abelsch. Insbesondere ist $\Phi(N) \subseteq C$.

Beweis. Nach Lemma 3.6 (a) ist $N' \subseteq C$ und damit ist N/C abelsch. Nach Korollar 1.32.1 ist $(N, *)$ endlich erzeugt und somit auch $(N/C, *)$. Damit genügt es, den Exponenten von $(N/C, *)$ zu betrachten.



Sei $K = \mathbb{Z}$. Wir zeigen $a^{(m)} \notin C$ für alle $a \in N \setminus C$ und $m \in \mathbb{N}$.
Sei $a \in N \setminus C$ und $m \in \mathbb{N}$. Nach Bemerkung 3.5 existiert $l \in \underline{k}$ minimal mit $a\pi_l \notin C$. Dann gilt $a^i\pi_l \in C$ für alle $i > 1$ nach Wahl von l und damit

$$a^{(m)}\pi_l = \left(\sum_{i=1}^{m} \binom{m}{i} a^i\right)\pi_l = \underbrace{ma\pi_l}_{\notin C} + \sum_{i=2}^{l} \binom{m}{i} \underbrace{a^i\pi_l}_{\in C} \notin C.$$

Mit Bemerkung 3.5 folgt $a^{(m)} \notin C$.
Ist $K = \mathbb{Z}/p\mathbb{Z}$ mit $p \in \mathbb{P}$ und $p > k$, so gilt mit Lemma 1.2 (e)

$$a^{(p)} = \sum_{i=1}^{p} \binom{p}{i} a^i = a^p = 0$$

für alle $a \in N$. Damit ist $(N, *)$ vom Exponenten p und somit auch $(N/C, *)$.
In beiden Fällen ist $\Phi(N/C) = \{0\}$ und damit $\Phi(N) \subseteq C$. □

Korollar 3.25.1 Gilt zudem $n = 1$ oder $k \leq 2$ oder $(n, k) = (2, 3)$, so ist

$$N' = \Phi(N) = C.$$

Beweis. Nach Satz 3.23 (a) ist in diesen Fällen N' ein Ideal von N.[8] Mit Korollar 3.7.1 folgt daraus $N' = C$ und wegen $N' \subseteq \Phi(N) \subseteq C$ folgt damit $N' = \Phi(N) = C$. □

Für $K = \mathbb{Z}$ wissen wir nun, dass $N' \subseteq \Phi(N) \subseteq C$ gilt. Wir wollen nun den Index von N' in $\Phi(N)$ und den von $\Phi(N)$ in C genauer untersuchen. Dazu werden wir diese sowohl in dem Jacobson-Radikal J der äußeren Algebra (vergleiche Kapitel 2.1) als auch in $N_{\mathbb{Z}/p\mathbb{Z}}$ für Primzahlen $p > k$ betrachten.

Zunächst betrachten wir den Fall der äußeren Algebra. Zusätzlich zu den dort verwandten Bezeichnungen führen wir die folgenden Notationen ein:

Bezeichnungen 3.26 Falls $k \geq n$ sei $\tilde{\varphi} : X \to X$, $x \mapsto x$, und $\varphi : N \to J$ die homomorphe Fortsetzung von $\tilde{\varphi}$.
Falls $k < n$ sei $\tilde{\varphi} : X \to \{x_1, \ldots, x_k\}$, $x_i \mapsto x_i$ für alle $i \leq k$ und $x_i \mapsto 0$ für alle $i > k$ und $\varphi : N \to J(\Lambda_K(\{x_1, \ldots, x_k\}))$ die homomorphe Fortsetzung von $\tilde{\varphi}$.

Bemerkung 3.27 Es gilt

$$C\varphi = 2\left(\bigoplus_{j=2}^{n} \Lambda_K^j(X)\right).$$

Beweis. Es ist

$$C = \langle f - g \mid f, g \in X^{\leq k}, f \sim g \rangle_K.$$

Somit genügt es, $(f-g)\varphi$ für assoziierte f, g zu bestimmen.
Seien $f, g \in X^{\leq k}$ assoziiert, etwa $f = \sigma g$ für ein geeignetes $\sigma \in \mathcal{S}_{l(f)}$. Ist $\operatorname{sgn}(\sigma) = 1$, so ist $f\varphi = g\varphi$, also $(f-g)\varphi = 0$. Ist $\operatorname{sgn}(\sigma) = -1$, so ist $l(f) > 1$ und $f\varphi = -(g\varphi)$, also ist $(f-g)\varphi = 2f\varphi$. Damit gilt $C\varphi \subseteq 2\left(\bigoplus_{j=2}^{n} \Lambda_K^j(X)\right)$.
Sei $h \in X^{\leq k}$ mit $l(h) > 1$, etwa $h = y_1 \wedge \cdots \wedge y_{l(h)}$ mit $y_1, \ldots, y_{l(h)} \in X$. Dann ist

$$\begin{aligned} 2h &= y_1 \wedge \cdots \wedge y_{l(h)} + y_1 \wedge \cdots \wedge y_{l(h)} \\ &= y_1 \wedge \cdots \wedge y_{l(h)} - y_2 \wedge y_1 \wedge y_3 \wedge \cdots \wedge y_{l(h)} \\ &= (y_1 \cdots y_{l(h)} - y_2 y_1 y_3 \cdots y_{l(h)})\varphi \in C\varphi. \end{aligned}$$

Damit folgt auch $C\varphi \supseteq 2\left(\bigoplus_{j=2}^{n} \Lambda_K^j(X)\right)$. □

Lemma 3.28 Sei $n \geq 3$ und $K = \mathbb{Z}$. Dann ist der Index von $\Phi(J)$ in $C\varphi$ unendlich.

Beweis. Es gilt nach Satz 2.8

$$2 \bigoplus_{j \in \underline{n},\, 2|j} \Lambda_{\mathbb{Z}}^j(X) = J' \overset{2.8.2}{=} \Phi(J).$$

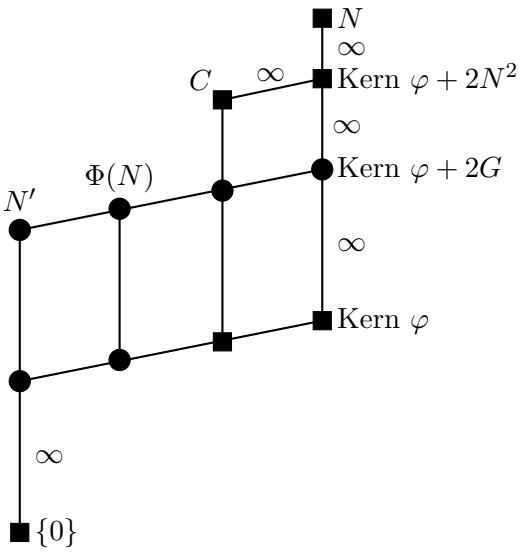
[8] Der Fall $p = 2$ und $k = 1$ fällt nicht unter die Voraussetzungen von Satz 3.23. In diesem Fall ist $(N, *)$ abelsch und damit $N' = \{0\}$ ein Ideal von N.

Damit ist $2x_1 \wedge x_2 \wedge x_3 \in C\varphi \setminus \Phi(J)$ und es gilt für alle $m \in \mathbb{N}$ mit Bemerkung 2.4 (d)

$$(2x_1 \wedge x_2 \wedge x_3)^{(m)} = \binom{m}{1} 2x_1 \wedge x_2 \wedge x_3 = 2mx_1 \wedge x_2 \wedge x_3 \notin \Phi(J).$$

□

Korollar 3.28.1 Sind $k, n \geq 3$, so gilt $\Phi(N) \subsetneq C$ und der Index von $\Phi(N)$ in C ist unendlich.



Im Bild seien $K = \mathbb{Z}$ und $k \geq n \geq 3$ gewählt. Zudem sei

$$G := \bigoplus_{i=1,\, 2|i}^{n} N\pi_i.$$

Die Kästchen kennzeichnen Ideale von N.

Es ist Kern $\varphi + 2N^2$ nach Bemerkung 3.27 das volle Urbild von $C\varphi$ und wegen $J' = \Phi(J)$ ist Kern $\varphi + 2G$ nach Lemma 3.28 das volle Urbild von J' und $\Phi(J)$.

Seien $x, y, z \in X$ paarweise verschieden. Dann sind die folgende Elemente von unendlicher Ordnung:

- $[x^{k-1}, y] = [x^{k-1}, y]_* \in \text{Kern } \varphi \cap N'$,
- $2xy + \text{Kern } \varphi \in (\text{Kern } \varphi + 2G)/\text{Kern } \varphi$,
- $2xyz + (\text{Kern } \varphi + 2G) \in (\text{Kern } \varphi + 2N^2)/(\text{Kern } \varphi + 2G)$,
- $x + (\text{Kern } \varphi + 2N^2) \in N/(\text{Kern } \varphi + 2N^2)$ und
- $2xy + C \in (\text{Kern } \varphi + 2N^2)/C$.

Nun wollen wir Kern φ bestimmen.

Bemerkung 3.29 Für alle $W \in X^{\leq k}_{\sim}$ sei $f_W \in W$ und zu $f \in W$ sei $\sigma_f \in \mathcal{S}_{l(f)}$ mit $\sigma_f f = f_W$. Dann ist

$$\text{Kern } \varphi = \left\{ \sum_{f \in X^{\leq k}} \alpha_f f \mid \forall W \in X^{\leq k}_{\sim} : f_W \varphi \neq 0 \Rightarrow \sum_{f \in W} \text{sgn } (\sigma_f)\alpha_f = 0 \right\}.$$

Beweis. Es ist $f\varphi = \text{sgn }(\sigma_f) f_W \varphi$ für alle $W \in X_{\sim}^{\leq k}$ und $f \in W$. Damit folgt

$$\begin{aligned}\left(\sum_{f\in X^{\leq k}} \alpha_f f\right)\varphi &= \left(\sum_{W\in X_{\sim}^{\leq k}} \sum_{f\in W} \alpha_f f\right)\varphi \\ &= \sum_{W\in X_{\sim}^{\leq k}} \sum_{f\in W} \alpha_f (f\varphi) \\ &= \sum_{W\in X_{\sim}^{\leq k}} \left(\sum_{f\in W} \text{sgn }(\sigma_f)\alpha_f\right)(f_W\varphi) \\ &= \sum_{W\in X_{\sim}^{\leq k}, f_W\varphi\neq 0} \left(\sum_{f\in W} \text{sgn }(\sigma_f)\alpha_f\right)(f_W\varphi)\end{aligned}$$

Da die $f_W\varphi$, die nicht im Kern von φ liegen, in J K-linear-unabhängig sind, ist somit $\sum_{f\in X^{\leq k}} \alpha_f f$ genau dann im Kern von φ enthalten, wenn für alle $W \in X_{\sim}^{\leq k}$ mit $f_W\varphi \neq 0$ die Bedingung

$$\sum_{f\in W} \text{sgn }(\sigma_f)\alpha_f = 0$$

erfüllt ist. □

Wir betrachten $N'_{\mathbb{Z}/p\mathbb{Z}}$ und $\Phi(N_{\mathbb{Z}/p\mathbb{Z}})$ für eine Primzahl p.

Lemma 3.30 Sei $p \in \mathbb{P}$ und $K = \mathbb{Z}/p\mathbb{Z}$.

(a) Ist $p \leq k$, so ist $N' \subsetneq \Phi(N)$.

(b) Ist $p > k$, so ist $N' = \Phi(N)$.

Beweis. Es ist $\Phi(N) = N^{(p)} * N'$ nach dem Burnside'schen Basissatz [Hup67, Seite 272, 3.14 a] und $N^{(p)} = N^p$, da char $K = p$ gilt.
Ist $k < p$, so folgt $N^p = \{0\}$ und damit $\Phi(N) = N'$.
Sei $k \geq p$ und $x \in X$. Dann ist $x^{(p)} = x^p \in \Phi(N)$, aber $x^p \notin C \supseteq N'$. Also folgt $x^p \in \Phi(N) \setminus N'$. □

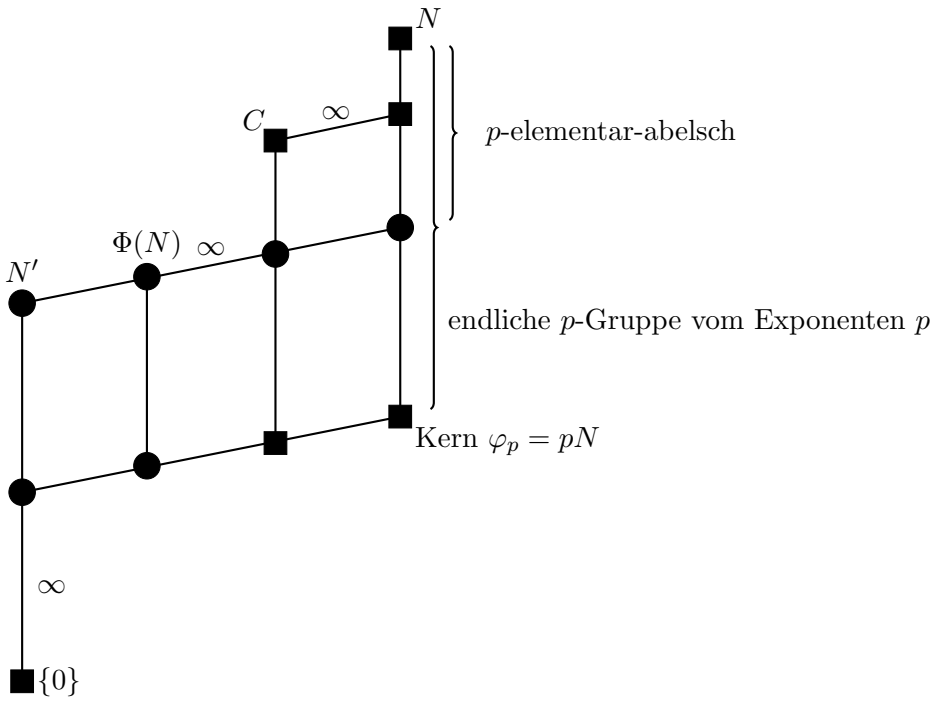
In dem folgenden Bild sei $K = \mathbb{Z}$ und $n, k \geq 3$ gewählt. Sei p eine Primzahl mit $p > k$ und $\varphi_p : N_{\mathbb{Z}} \to N_{\mathbb{Z}/p\mathbb{Z}}$ die Fortsetzung des kanonischen Ringepimorphismus $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Die Kästchen kennzeichnen Ideale von $N := N_{\mathbb{Z}}$.

Mit $N'_{\mathbb{Z}/p\mathbb{Z}} = \Phi(N_{\mathbb{Z}/p\mathbb{Z}})$ ist $N' + pN = \Phi(N) + pN$.
Wie bereits gezeigt, ist $C/\Phi(N)$ unendlich, aber $C/((N' + pN) \cap C)$ ist isomorph zu einer Faktorgruppe von N/pN und damit endlich. Also muss $((N' + pN) \cap C)/\Phi(N)$ unendlich sein.
Für $x, y \in X$ mit $x \neq y$ sind

- $px + C \in (pN + C)/C$ und

- $p[x^{k-1}, y] = [px^{k-1}, y]_* \in N' \cap pN$

von unendlicher Ordnung.



3.3 Der abelsche Fall

In diesem Abschnitt wollen wir den Fall untersuchen, dass die Gruppe $(N, *)$ abelsch ist. Dies ist nach Bemerkung 1.29 genau dann gegeben, wenn die Nilpotenzklasse k der Algebra 1 ist oder wenn N als Algebra von nur einem Element erzeugt ist, also $|X| = 1$ gilt.
Im ersten Fall erhalten wir

$$(N, *) \cong (K, +)^{|X|},$$

hier ist also nichts weiter zu zeigen.
Ist im zweiten Fall

$$(K, +) \cong (\mathbb{Z}, +)^m$$

für ein $m \in \mathbb{N}$, so ist $(N, *)$ nach Korollar 1.32.2 endlich erzeugt und jedes Element $\neq 0_N$ ist nach Korollar 1.27.1 von unendlicher Ordnung. Damit ist in diesem Fall $(N, *)$ frei abelsch. Genauer gilt:

Bemerkung 3.31 Es ist

$$(N_{\mathbb{Z},1,k}, *) \cong (\mathbb{Z}, +)^k.$$

Beweis. Sei $X = \{x\}$. Nach Korollar 1.32.1 ist $\{x^i \mid i \in \underline{k}\}$ ein $*$-Erzeugendensystem von N. Seien $\alpha_1, \ldots, \alpha_k \in \mathbb{Z}$ mit

$$0 = \overset{k}{\underset{i=1}{\bigstar}} (x^i)^{(\alpha_i)}.$$

Dann folgt

$$0 = \left(\overset{k}{\underset{i=1}{\bigstar}} (x^i)^{(\alpha_i)} \right) \pi_1 = \alpha_1 x,$$

also $\alpha_1 = 0$, und damit induktiv für alle $l \leq k$

$$0 = \left(\overset{k}{\underset{i=1}{\bigstar}} (x^i)^{(\alpha_i)} \right) \pi_l \overset{\text{I.V.}}{=} \left(\overset{k}{\underset{i=l}{\bigstar}} (x^i)^{(\alpha_i)} \right) \pi_l = \alpha_l x^l,$$

also $\alpha_l = 0$ für alle $l \in \underline{k}$. Damit ist $\{x^i \mid i \in \underline{k}\}$ eine $\mathbb{Z}$- Basis von $(N, *)$. □

Sei in diesem Abschnitt $|X| = 1$, etwa $X = \{x\}$, $p \in \mathbb{P}$, $l, m \in \mathbb{N}$ und K ein kommutativer unitärer Ring mit

$$(K, +) \cong (\mathbb{Z}/p^l\mathbb{Z}, +)^m$$

so, dass es eine $\mathbb{Z}/p^l\mathbb{Z}$-Basis κ von $(K, +)$ gibt mit $\kappa = \kappa^p = \{c^p \mid c \in \kappa\}$.

Bemerkung 3.32 Ist $K = \mathbb{Z}/p^l\mathbb{Z}$, so ist $\kappa = \{1\}$ eine $\mathbb{Z}/p^l\mathbb{Z}$-Basis mit $\kappa^p = \kappa$.
Ist K ein endlicher Körper, so gibt es nach [LN83, Seite 60, Theorem 2.35] eine Normalbasis[9] κ von K über seinem Primkörper. Ist also K ein endlicher Körper mit char $K = p$, so existiert eine $\mathbb{Z}/p\mathbb{Z}$-Basis κ von K mit $\kappa^p = \kappa$.

Satz 3.33 Es gilt

$$(N_{K,1,k}, *) \cong \left(\mathcal{C}_{p^{l-1}}^{c_{k,p,1}} \times \bigtimes_{t=0}^{s_{k,p}} \mathcal{C}_{p^{l+t}}^{(|I_{k,p,t}| - |I_{k,p,t+1}|)} \right)^m.$$

Beweis. Sei $\kappa = \{k_1, \ldots, k_m\}$. Für alle $i \in \underline{m}$ und $r \in \underline{c_1}$ sei $y_{i,r} := (k_i x^r)^{(p)} * ((k_i x^r)^p)^-$. Sei

$$B := \{k_i x^j \mid i \in \underline{m}, j \in \underline{k}, p \nmid j\} \cup \{y_{i,r} \mid i \in \underline{m}, r \in \underline{c_1}\}.$$

[9] Ist K/K_0 eine endliche galoissche Körpererweiterung, so heißt eine Basis der Form $\{c\alpha \mid \alpha \in \mathrm{Aut}_{K_0} K\}$ für ein $c \in K$ eine Normalbasis der Körpererweiterung. Ist dabei K endlich mit char $K = p$, so ist $\mathrm{Aut}_{K_0} K$ von einer Potenz des Frobeniusautomorphismus erzeugt und wir erhalten eine Basis der Form $\left\{ c, c^{|K_0|}, c^{|K_0|^2}, \ldots, c^{\frac{|K|}{|K_0|}} \right\}$.

Wir zeigen zunächst $\langle B\rangle_* = N$. Nach Korollar 1.32.1 ist $\{k_i x^j \mid i \in \underline{m_\mathbb{J}},\, j \in \underline{k_\mathbb{J}}\}$ ein $*$-Erzeugendensystem von N. Wir zeigen induktiv nach j für alle $i \in \underline{m_\mathbb{J}}$: $k_i x^j \in \langle B\rangle_*$.
Sei also $i \in \underline{m_\mathbb{J}}$. Für $j = 1$ gilt $k_i x^j \in B$ nach Definition von B. Sei nun $j > 1$. Gilt $p \nmid j$, so gilt wieder $k_i x^j \in B$ nach Definition. Andernfalls sei $l \in \underline{m_\mathbb{J}}$ mit $k_l^p = k_i$ (ein solches l existiert nach Wahl von κ) und $r \in \underline{c_{1\mathbb{J}}}$ mit $j = pr$. Dann ist nach Induktionsvoraussetzung $k_l x^r \in \langle B\rangle_*$ und wir erhalten

$$k_i x^j = (k_l x^r)^p = \left((k_l x^r)^{(p)} * ((k_l x^r)^p)^-\right)^- * (k_l x^r)^{(p)} = (y_{l,r})^- * (k_l x^r)^{(p)} \in \langle B\rangle_*.$$

Damit ist $\langle B\rangle_* = N$.
Weiter gilt $o(y_{i,r}) \mid p^{l-1}$ nach Korollar 1.34.1 für alle $i \in \underline{m_\mathbb{J}}$ und alle $r \in \underline{c_{1\mathbb{J}}}$. Damit folgt

$$\prod_{r\in\underline{c_{1\mathbb{J}}}}\prod_{i\in\underline{m_\mathbb{J}}} o(y_{i,r}) \le p^{(l-1)mc_1} \quad \text{und}$$

$$\prod_{\substack{j\in\underline{k_\mathbb{J}}\\ p\nmid j}}\prod_{i\in\underline{m_\mathbb{J}}} o\left(k_i x^j\right) \overset{1.18}{=} \prod_{t=0}^{s}\prod_{j\in I_t\setminus p\mathbb{N}}\prod_{i\in\underline{m_\mathbb{J}}} o\left(k_i x^j\right)$$

$$\overset{1.35}{\le} \prod_{t=0}^{s} p^{(l+t)m|I_t\setminus p\mathbb{N}|}$$

$$\overset{1.18}{=} p^{m\sum_{t=0}^{s}(l+t)(|I_t|-|I_{t+1}|)}.$$

Außerdem gilt

$$\begin{aligned}(l-1)c_1+\sum_{t=0}^{s}(l+t)(|I_t|-|I_{t+1}|) &= (l-1)c_1 + l|I_0| + \sum_{t=1}^{s}|I_t| - (l+s)\underbrace{|I_{s+1}|}_{=0}\\ &= (l-1)c_1 + l(c_0-c_1) + \sum_{t=1}^{s}(c_t - c_{t+1})\\ &= -c_1 + lc_0 + c_1 - \underbrace{c_{s+1}}_{=0}\\ &= lc_0\\ &= lk.\end{aligned}$$

Damit erhalten wir insgesamt

$$\begin{aligned}p^{lmk} &= |K|^k\\ &= |N|\\ &= |\langle B\rangle_*| \le \prod_{b\in B} o(b)\\ &= \left(\prod_{r\in\underline{c_{1\mathbb{J}}}}\prod_{i\in\underline{m_\mathbb{J}}} o(y_{i,r})\right)\left(\prod_{\substack{j\in\underline{k_\mathbb{J}}\\ p\nmid j}}\prod_{i\in\underline{m_\mathbb{J}}} o\left(k_i x^j\right)\right)\\ &= p^{m((l-1)c_1+\sum_{t=0}^{s}(l+t)(|I_t|-|I_{t+1}|))}\\ &= p^{mkl}.\end{aligned}$$

Damit folgt $o(y_{i,r}) = p^{l-1}$ für alle $r \in \underline{c_1}$, $i \in \underline{m}$ und $o\left(k_i x^j\right) = p^{l+t}$ für alle $t \in \underline{s}$, $j \in I_t \setminus p\mathbb{N}$ und $i \in \underline{m}$. Wir erhalten

$$N = \bigtimes_{b \in B} \langle b \rangle_* \cong \left(\mathcal{C}_{p^{l-1}}^{c_1} \times \bigtimes_{t=0}^{s} \mathcal{C}_{p^{l+t}}^{(|I_t|-|I_{t+1}|)} \right)^m .$$

□

Zusatz Genauer zeigen wir in dem Beweis von Satz 3.33, dass B ein minimales Erzeugendensystem mit $\times_{b \in B} \langle b \rangle_* = N$ ist.

Korollar 3.33.1 (a) Sei $c \in \mathbb{N}_{>1}$ und $K = \mathbb{Z}/c\mathbb{Z}$. Seien $q, r_1, \ldots r_q \in \mathbb{N}$ sowie $p_1, \ldots, p_q \in \mathbb{P}$ paarweise verschieden mit $c = p_1^{r_1} \ldots p_q^{r_q}$. Dann gilt

$$(N, *) \cong \bigtimes_{i=1}^{q} \left(\mathcal{C}_{p_i^{r_i-1}}^{c_{p_i,1}} \times \bigtimes_{t=0}^{s_{p_i}} \mathcal{C}_{p_i^{r_i+t}}^{(|I_{p_i,t}|-|I_{p_i,t+1}|)} \right).$$

(b) Sei K ein endlicher Körper der Charakteristik p, $|K| = p^m$. Dann ist

$$(N, *) \cong \bigtimes_{t=0}^{s} \mathcal{C}_{p^{1+t}}^{m(|I_t|-|I_{t+1}|)} = \bigtimes_{t=1}^{s+1} \mathcal{C}_{p^t}^{m(|I_{t-1}|-|I_t|)}.$$

Beweis. (a) Im Fall $c = p_1^{r_1}$ gilt die Behauptung mit Satz 3.33 mit $\kappa = \{1\}$ und der allgemeine Fall folgt daraus mit Satz 1.38.
(b) Dies folgt direkt aus Satz 3.33 mit Bemerkung 3.32. □

Beispiel 3.34 Sei $p = 3 = l$ und $k = 10$. Nach Beispiel 1.17 ist

$$c_1 = 3, \quad |I_0| - |I_1| = 7 - 2 = 5, \quad |I_1| - |I_2| = 2 - 1 = 1 \quad \text{und} \quad |I_2| - |I_3| = |I_2| = 1.$$

Mit Satz 3.33 folgt

$$(N, *) \cong \mathcal{C}_9^3 \times \mathcal{C}_{27}^5 \times \mathcal{C}_{81} \times \mathcal{C}_{243}.$$

Wir wollen nun im Fall char $K = p$ die Frattini-Untergruppe $\Phi(N)$ bestimmen.

Bemerkung 3.35 Es sei char $K = p$ und $l = 1$. Dann gilt

$$N_{K,X,k}^{(p^t)} = \bigoplus_{\substack{j=1 \\ p^t | j}}^{k} Kx^j \quad \text{für alle } t \in \mathbb{N}_0.$$

Insbesondere ist $|N^{(p^t)}| = |K|^{c_t}$ für alle $t \in \mathbb{N}_0$ und

$$\Phi(N_{K,X,k}) = \bigoplus_{\substack{j=1 \\ p | j}}^{k} Kx^j.$$

Beweis. Sei $t \in \mathbb{N}_0$. Sei $a \in N$, etwa $a = \sum_{i=1}^{k} \alpha_i x^i$ mit $\alpha_1, \ldots, \alpha_k \in K$. Dann gilt mit char $K = p$

$$a^{(p^t)} = a^{p^t} = \sum_{i=1}^{k} \alpha_i^{p^t} x^{ip^t} \in \bigoplus_{\substack{j=1 \\ p^t|j}}^{k} Kx^j. \quad \text{Also ist} \quad N^{(p^t)} \subseteq \bigoplus_{\substack{j=1 \\ p^t|j}}^{k} Kx^j.$$

Außerdem ist $|\underline{k} \cap p^t\mathbb{N}| = c_t$ nach Bemerkung 1.18 Teil 6. und wir erhalten

$$|\bigoplus_{\substack{j=1 \\ p^t|j}}^{k} Kx^j| = |K|^{c_t}.$$

Nach Satz 3.33 ist

$$N \cong \left(\bigtimes_{r=0}^{s} \mathcal{C}_{p^{1+r}}^{(|I_r|-|I_{r+1}|)} \right)^m$$

und damit

$$\begin{aligned} N^{(p^t)} &\cong \left(\bigtimes_{r=t}^{s} \mathcal{C}_{p^{1+r-t}}^{(|I_r|-|I_{r+1}|)} \right)^m, \quad \text{also} \\ |N^{(p^t)}| &= \prod_{r=t}^{s} p^{m(1+r-t)(|I_r|-|I_{r+1}|)} \\ &= p^{m\sum_{r=t}^{s}(1+r-t)(|I_r|-|I_{r+1}|)} \\ &= |K|^{\sum_{r=t}^{s}(1+r-t)(|I_r|-|I_{r+1}|)}. \end{aligned}$$

Mit

$$\begin{aligned} \sum_{r=t}^{s}(1+r-t)(|I_r|-|I_{r+1}|) &= \sum_{r=t}^{s}|I_r| - (1+s-t)\underbrace{|I_{s+1}|}_{=0} \\ &= \sum_{r=t}^{s}(c_r - c_{r+1}) \\ &= c_t - \underbrace{c_{s+1}}_{=0} \\ &= c_t \end{aligned}$$

folgt die angegebene Mächtigkeit von $N_{(p^t)}$ und damit die behauptete Gleichheit. Die Behauptung für $\Phi(N)$ folgt aus $\Phi(N) = N^{(p)} * N' = N^{(p)}$, da N eine abelsche p-Gruppe ist. □

Wir wollen nun eine Anwendung des Satzes 3.33 betrachten.

Lemma 3.36 Sei K ein beliebiger kommutativer unitärer Ring und $\mathcal{G}$ eine Gruppe. Sei $g \in \mathcal{G}$ und A die von $1-g$ erzeugte K-Teilalgebra von $K\mathcal{G}$. Dann gilt $1-g^n \in A$ für alle $n \in \mathbb{N}_0$.

Beweis. Wir zeigen die Behauptung mittels Induktion nach n. Dabei ist für $n = 0$ und $n = 1$ nichts zu zeigen. Sei also $n > 1$. Dann folgt:

$$\begin{aligned}
\underbrace{(1-g)^n}_{\in A} + \underbrace{\sum_{i=1}^{n-1} \binom{n}{i}(-1)^i(1-g^i)}_{\in A \text{ nach I.V.}} &= \sum_{i=0}^{n} \binom{n}{i}(-1)^i g^i + \sum_{i=1}^{n-1} \binom{n}{i}(-1)^i(1-g^i) \\
&= 1 + (-1)^n g^n + \sum_{i=1}^{n-1} \binom{n}{i}(-1)^i \\
&= (-1)^n g^n + \underbrace{\sum_{i=0}^{n} \binom{n}{i}(-1)^i}_{=0} - (-1)^n \\
&= (-1)^{n+1}(1-g^n).
\end{aligned}$$

Damit folgt $1 - g^n \in A$. □

Korollar 3.36.1 Ist $\mathcal{G}$ zyklisch von g erzeugt, so ist $A = \text{Aug}\,(K\mathcal{G})$.

Satz 3.37 Sei K ein endlicher Körper mit Charakteristik p und $\mathcal{G} \cong \mathcal{C}_{p^l}$, $k := p^l - 1$. Dann gilt

$$N_{K,1,k} \cong \text{Aug}\,(K\mathcal{G}) \quad \text{als } K\text{-Algebren.}$$

Beweis. Sei g ein Erzeuger von $\mathcal{G}$. Dann ist $A = \text{Aug}\,(K\mathcal{G})$ von $1 - g$ als K-Algebra erzeugt und es ist $\text{Aug}\,(K\mathcal{G})^{p^l} = \{0\}$. Damit lässt sich die Abbildung $x \mapsto 1-g$ zu einem K-Algebren-Epimorphismus $N_{K,\{x\},k} \to \text{Aug}\,(K\mathcal{G})$ fortsetzen, der wegen

$$|N| = |K|^k = |K|^{p^l-1} = |K|^{|\mathcal{G}|-1} = |\text{Aug}\,(K\mathcal{G})|$$

ein Isomorphismus ist. □

Damit erhalten wir den Spezialfall der zyklischen Gruppe eines Resultats für abelsche p-Gruppen, das sich bei S. Wirsing [Wir05, Seite 80, 4.2.1.4] findet:

Korollar 3.37.1 Sei zusätzlich $|K| = p^m$. Dann ist

$$(\text{Aug}\,(K\mathcal{G}), *) \cong \bigtimes_{t=1}^{l} \mathcal{C}_{p^t}^{m\left(|\mathcal{G}^{p^{t-1}}| - 2|\mathcal{G}^{p^t}| + |\mathcal{G}^{p^{t+1}}|\right)}.$$

Beweis. Es gilt

$$c_t = \begin{cases} \left\lfloor \frac{p^l-1}{p^t} \right\rfloor = p^{l-t} - 1 & \text{für alle } t \in \underline{l-1}_0 \\ c_t = 0 & \text{für alle } t \geq l \end{cases}.$$

Damit ist $s = l - 1$. Weiter gilt für alle $t \in \underline{s}$

$$\begin{aligned}|I_{t-1}| - |I_t| &= c_{t-1} - 2c_t + c_{t+1} \\ &= p^{l-(t-1)} - 1 - 2(p^{l-t} - 1) + p^{l-(t+1)} - 1 \\ &= p^{l-(t-1)} - 2p^{l-t} + p^{l-(t+1)} \\ &= \left|\mathcal{G}^{p^{t-1}}\right| - 2\left|\mathcal{G}^{p^t}\right| + \left|\mathcal{G}^{p^{t+1}}\right|,\end{aligned}$$

da $\mathcal{G}$ eine zyklische Gruppe der Ordnung p^l ist. Es folgt

$$\begin{aligned}(\text{Aug }(K\mathcal{G}), *) &\cong (N_{K,1,k}, *) \\ &\overset{3.33.1(b)}{\cong} \bigtimes_{t=0}^{l-1} \mathcal{C}_{p^{t+1}}^{m(|I_t|-|I_{t+1}|)} \\ &= \bigtimes_{t=1}^{l} \mathcal{C}_{p^t}^{m(|I_{t-1}|-|I_t|)} \\ &= \bigtimes_{t=1}^{l} \mathcal{C}_{p^t}^{m\left(\left|\mathcal{G}^{p^{t-1}}\right| - 2\left|\mathcal{G}^{p^t}\right| + \left|\mathcal{G}^{p^{t+1}}\right|\right)}.\end{aligned}$$

□

3.4 Die von X erzeugte Untergruppe

Nun betrachten wir die von X bezüglich $*$ erzeugte Untergruppe von $N_{K,X,k}$. Der Satz von Magnus sagt uns, dass $\langle X\rangle_*$ in der Potenzreihenalgebra $P_{\mathbb{Z},X}$ frei über X ist und Satz 2.14 gibt uns dieses Resultat in der Potenzreihenalgebra $P_{K,X}$ über einem beliebigen kommutativen unitären Grundring K an.
In der Diplomarbeit [Han12, Satz 2.16] haben wir bereits gezeigt, dass $\langle X\rangle_*$ in $N_{\mathbb{Z},X,k}$ frei nilpotent von der Klasse k über der Menge X ist. Im Fall eines Ringes K mit Charakteristik $\neq 0$ ist diese Gruppe jedoch endlich und kann somit nicht mehr frei nilpotent sein. Wir werden in diesem Abschnitt jedoch sehen, dass die $\langle X\rangle_*$ eine $\mathfrak{N}_{n,k,\varepsilon}$-freie Gruppe über X ist, also wieder freies Objekt in einer geeigneten Klasse.
Wir werden zunächst die Klassen $\mathfrak{N}_{n,k,\varepsilon}$ definieren und auf Eigenschaften untersuchen und anschließend zeigen, dass $\langle X\rangle_*$ in $N_{K,X,n}$ frei in einer in Abhängigkeit von K gewählten Klasse von Gruppen $\mathfrak{N}_{n,k,\varepsilon}$ ist.

In diesem Abschnitt seien $n, k \in \mathbb{N}$ und $\varepsilon := (\varepsilon_1, \ldots, \varepsilon_k) \in \mathbb{N}^k$.

Definition 3.38 Es bezeichne $\mathfrak{N}_k$ die Klasse der nilpotenten Gruppen von der Klasse höchstens k. Weiter bezeichne $\mathfrak{N}_{k,\varepsilon}$ die Klasse der Gruppen $\mathcal{N} \in \mathfrak{N}_k$ bei denen ε_i für alle $i \in \underline{k}$ von dem Exponenten von $\gamma_i(\mathcal{N})$ geteilt wird. Insbesondere teilt der Exponent

dieser Gruppen ε_1.
Es bezeichne zudem $\mathfrak{N}_{n,k}$ die Klasse der nilpotenten Gruppen von der Klasse höchstens k mit n Erzeugern und $\mathcal{N}_{n,k}$ das freie Objekt in dieser Klasse. Ist $\mathcal{F}_n$ die freie Gruppe mit n Erzeugern, so ist $\mathcal{N}_{n,k} \cong \mathcal{F}_n/\gamma_{k+1}(\mathcal{F}_n)$.
Außerdem sei $\mathfrak{N}_{n,k,\varepsilon}$ die Klasse der Gruppen $\mathcal{N} \in \mathfrak{N}_{k,\varepsilon}$, die von n Elementen erzeugt werden.

Wir erhalten nun freie Gruppen in diesen Klassen wie folgt:

Satz und Definition 3.39 Es gibt eine $\mathfrak{N}_{k,\varepsilon}$-freie Gruppe über X. Ist $\mathcal{F}_X$ die freie Gruppe über X, so ist die $\mathfrak{N}_{k,\varepsilon}$-freie Gruppe über X isomorph zu

$$\mathcal{F}_X \Big/ \left(\left(\prod_{i=1}^{k} \gamma_i(\mathcal{F}_X)^{\varepsilon_i} \right) \gamma_{k+1}(\mathcal{F}_X) \right).$$

Ist $|X| = n$, so ist diese frei in $\mathfrak{N}_{n,k,\varepsilon}$ und wir bezeichnen sie mit $\mathcal{N}_{n,k,\varepsilon}$.

Beweis. Wir setzen

$$\mathcal{N} := \left(\prod_{i=1}^{k} \gamma_i(\mathcal{F}_X)^{\varepsilon_i} \right) \gamma_{k+1}(\mathcal{F}_X).$$

Dann ist $\mathcal{N} \trianglelefteq \mathcal{F}_X$. Sei $\mathcal{G} \in \mathfrak{N}_{k,\varepsilon}$ und $\varphi : \mathcal{F}_X \to \mathcal{G}$ ein Gruppen-Homomorphismus. Da $\mathcal{G}$ nilpotent von Klasse k ist, ist $\gamma_{k+1}(\mathcal{F}_X) \subseteq \operatorname{Kern} \varphi$. Sei $i \in \underline{k}$ und $g \in \gamma_i(\mathcal{F}_X)$. Dann gilt $g\varphi \in \gamma_i(\mathcal{G})$ und damit

$$(g^{\varepsilon_i})\varphi = (g\varphi)^{\varepsilon_i} = 1_{\mathcal{G}}.$$

Also ist $g^{\varepsilon_i} \in \operatorname{Kern} \varphi$ und damit $\gamma_i(\mathcal{F}_X)^{\varepsilon_i} \leq \operatorname{Kern} \varphi$ für alle $i \in \underline{k}$. Es folgt $\mathcal{N} \leq \operatorname{Kern} \varphi$.
Mit $\mathcal{F}_X/\mathcal{N} \in \mathfrak{N}_{k,\varepsilon}$ ist $\mathcal{F}_X/\mathcal{N}$ $\mathfrak{N}_{k,\varepsilon}$-frei über X. □

Bemerkung 3.40 Sei $\mathcal{N} \in \mathfrak{N}_k$ und X ein Erzeugendensystem von $\mathcal{N}$.

(a) Ist für alle $Y \subseteq X$, Y endlich, Y ein $\mathfrak{N}_k$-freies Erzeugendensystem von $\langle Y \rangle$, so ist X ein $\mathfrak{N}_k$-freies Erzeugendensystem von $\mathcal{N}$.

(b) Sei $\mathcal{N} \in \mathfrak{N}_{k,\varepsilon}$. Ist für alle $Y \subseteq X$, Y endlich, Y ein $\mathfrak{N}_{k,\varepsilon}$-freies Erzeugendensystem von $\langle Y \rangle$, so ist X ein $\mathfrak{N}_{k,\varepsilon}$-freies Erzeugendensystem von $\mathcal{N}$.

Beweis. (a) Sei $\mathcal{G} \in \mathfrak{N}_k$ und $\bar{\varphi} : X \to \mathcal{G}$ eine Abbildung. Seien $g \in \mathcal{N}$, $m, l \in \mathbb{N}$, $x_1, \ldots, x_m, y_1, \ldots, y_l \in X$ und $\alpha_1, \ldots \alpha_m, \beta_1, \ldots, \beta_l \in \{1, -1\}$ mit

$$x_1^{\alpha_1} \ldots x_m^{\alpha_m} = g = y_1^{\beta_1} \ldots y_l^{\beta_l}.$$

Sei $Y := \{x_1, \ldots, x_m, y_1, \ldots, y_l\}$. Dann ist Y endlich und nach Voraussetzung lässt sich $\bar{\varphi}_{|Y}$ zu einem Homomorphismus nach $\mathcal{G}$ fortsetzen, das heißt, es gilt

$$(x_1\bar{\varphi})^{\alpha_1} \ldots (x_m\bar{\varphi})^{\alpha_m} = (y_1\bar{\varphi})^{\beta_1} \ldots (y_l\bar{\varphi})^{\beta_l}.$$

Also werden je zwei verschiedenen Darstellungen eines Elementes das gleiche Element im Bildbereich zugeordnet und damit lässt sich $\bar{\varphi}$ zu einem Gruppen-Homomorphismus fortsetzen.
(b) Diese Aussage folgt analog. □

Nachdem wir nun die Klassen $\mathfrak{N}_{k,\varepsilon}$ und $\mathfrak{N}_{n,k,\varepsilon}$ definiert haben und eingesehen haben, dass es in diesen Klassen freie Objekte gibt, wollen wir nun den Spezialfall $k = 1$ betrachten. Anschließend überlegen wir uns, dass nicht jede Wahl von ε zu verschiedenen Klassen führt. Je kleiner die Einträge in ε sind, desto besser lässt es sich in der Gruppe rechnen. Also wollen wir ε mit möglichst kleinen Einträgen wählen können ohne die Klasse zu verändern.

Definition und Bemerkung 3.41 Es ist $\mathcal{N}_{1,1,(\varepsilon_1)}$ eine zyklische Gruppe der Ordnung ε_1. Diese bezeichnen wir mit $\mathcal{C}_{\varepsilon_1}$. Weiter ist $\mathcal{N}_{n,1,(\varepsilon_1)} \cong \underbrace{\mathcal{C}_{\varepsilon_1} \times \cdots \times \mathcal{C}_{\varepsilon_1}}_{n}$.

Lemma 3.42 Sei $i \in \underline{k-1}$. Für alle $j \in \underline{k}$ setzen wir

$$\tilde{\varepsilon}_j := \begin{cases} \mathrm{ggT}(\varepsilon_i, \varepsilon_{i+1}) & j = i+1 \\ \varepsilon_j & j \neq i+1 \end{cases} \quad \text{und} \quad \tilde{\varepsilon} := (\tilde{\varepsilon}_1, \ldots, \tilde{\varepsilon}_k).$$

Dann gilt $\mathfrak{N}_{k,\varepsilon} = \mathfrak{N}_{k,\tilde{\varepsilon}}$ und $\mathfrak{N}_{n,k,\varepsilon} = \mathfrak{N}_{n,k,\tilde{\varepsilon}}$.

Beweis. $\mathfrak{N}_{k,\tilde{\varepsilon}} \subseteq \mathfrak{N}_{k,\varepsilon}$ gilt trivialerweise.
Sei $\mathcal{G} \in \mathfrak{N}_{k,\varepsilon}$. Sei $j \in \underline{k}$ und $g \in \gamma_j(\mathcal{G})$. Ist $j \neq i+1$, so ist $g^{\tilde{\varepsilon}_j} = g^{\varepsilon_j} = 1_{\mathcal{G}}$. Ist $j = i+1$, so gilt

$$g^{\varepsilon_i} \overset{g \in \gamma_i(\mathcal{G})}{=} 1_{\mathcal{G}} \overset{g \in \gamma_{i+1}(\mathcal{G})}{=} g^{\varepsilon_{i+1}} \quad \text{und damit} \quad g^{\tilde{\varepsilon}_{i+1}} = g^{\mathrm{ggT}(\varepsilon_i, \varepsilon_{i+1})} = 1_{\mathcal{G}}.$$

Damit folgt $\mathcal{G} \in \mathfrak{N}_{k,\tilde{\varepsilon}}$.
$\mathfrak{N}_{n,k,\varepsilon} = \mathfrak{N}_{n,k,\tilde{\varepsilon}}$ folgt entsprechend. □

Nun können wir eine obere Schranke für die in $\mathfrak{N}_{n,k,\varepsilon}$ auftretenden Gruppenordnungen angeben. Je kleiner wir die Einträge von ε mit vorherigem Lemma wählen können, desto besser wird unsere Schranke.

In Korollar 1.48.1 haben wir gezeigt, dass wir in $\mathcal{N}_{n,k,\varepsilon}$ die Elemente durch Elementarkommutatoren darstellen können. Dies wollen wir uns in der Folge zunutze machen. Wir verwenden hier die gleichen Notationen wie in Abschnitt 1.4.

Lemma 3.43 (a) Sei $\mathcal{G} \in \mathfrak{N}_{n,k,\varepsilon}$. Dann gilt

$$|\mathcal{G}| \leq \prod_{i=1}^{k} \varepsilon_i^{n_i}. \tag{3.1}$$

Insbesondere ist $\mathcal{N}_{n,k,\varepsilon}$ endlich.

(b) Sei $X = \{x_1, \ldots, x_n\}$, $Y = \{y_1, \ldots, y_n\}$ ein Erzeugendensystem von $\mathcal{N}_{n,k,\varepsilon}$ und $\beta : \mathcal{F}_X \to \mathcal{N}_{n,k,\varepsilon}$ die homomorphe Fortsetzung von $x_j \mapsto y_j$ für alle $j \in \underline{n}$. Für alle $i \in \underline{k}$ sei $\mathfrak{E}_i^{\mathfrak{G},\beta} = (e_{i,1}, \ldots, e_{i,n_i})$ das Tupel der Elementarkommutatoren vom Gewicht i. Dann gilt

$$\mathcal{N}_{n,k,\varepsilon} = \left\{ \prod_{i=1}^{k} \prod_{j=1}^{n_i} e_{i,j}^{\alpha_{i,j}} \,\middle|\, \forall i \in \underline{k},\, j \in \underline{n_i} :\, \alpha_{i,j} \in \underline{\varepsilon_i} \right\}$$

und die Darstellung der Elemente in dieser Form ist genau dann eindeutig, wenn in (3.1) die Gleichheit gilt.

Beweis. Dies folgt aus Korollar 1.48.1. □

Korollar 3.43.1 Sei $\mathcal{G}$ eine nilpotente Gruppe der Klasse höchstens k mit n Erzeugern und vom Exponenten ε_1. Dann gilt

$$|\mathcal{G}| \leq \varepsilon_1^{\sum_{i=1}^{k} n_i}.$$

Wir erhalten also nur in Abhängigkeit von der Nilpotenzklasse k, der Erzeugerzahl n und dem Exponenten ε_1 eine obere Schranke für die Gruppenordnung. In [Qui89, Theorem 1] wird eine weitere Schranke angegeben:

Satz 3.44 Sei $\mathcal{G}$ eine nilpotente Gruppe der Klasse höchstens k mit $n > 1$ Erzeugern und vom Exponenten ε_1. Dann gilt

$$|\mathcal{G}| \leq n^{\frac{1}{2}\varepsilon_1 k(k+1)}.$$

Beispiel 3.45 Sei $\mathcal{G}$ eine nilpotente Gruppe der Klasse $k = 10$ mit $n = 2$ Erzeugern.

- Sei $\mathcal{G}$ vom Exponenten $\varepsilon_1 = 3$. Dann gilt:

  (3.43.1) $\quad |\mathcal{G}| \leq 3^{2+1+2+3+6+9+18+30+56+99} = 3^{226}$ und

  (3.44) $\quad |\mathcal{G}| \leq 2^{\frac{1}{2}\cdot 3\cdot 10\cdot 11} = 2^{165}$.

  Hier ist die Abschätzung aus Satz 3.44 besser.

- Sei $\mathcal{G}$ vom Exponenten $\varepsilon_1 = 3^3$. Dann gilt:

  (3.43.1) $\quad |\mathcal{G}| \leq 3^{3(2+1+2+3+6+9+18+30+56+99)} = 3^{678} \approx 3,1 \cdot 10^{323}$ und

  (3.44) $\quad |\mathcal{G}| \leq 2^{\frac{1}{2}\cdot 3^3\cdot 10\cdot 11} = 2^{1485} \approx 1,1 \cdot 10^{447}$.

  Hier ist also unsere Abschätzung aus Korollar 3.43.1 besser.

Beim Vergleich der beiden Abschätzungen fällt auf, dass unsere Abschätzung bei festem n und k für große Exponenten eine bessere Abschätzung liefert, da das Wachstum nicht mehr exponentiell, sondern polynomiell ist.

Da wir nun wissen, dass unsere Gruppen endlich und nilpotent sind, können wir sie mit Hilfe ihrer Sylowgruppen zerlegen und erhalten damit eine Reduktion auf den Fall, dass ε nur p-Potenz-Einträge zu einer festen Primzahl p hat.

Lemma 3.46 Seien $q \in \mathbb{N}$ und $p_1, \ldots, p_q \in \mathbb{P}$ paarweise verschieden. Für alle $i \in \underline{k}$ und $j \in \underline{q}$ sei $r_{i,j} \in \mathbb{N}_0$. Dann gilt

$$\mathcal{N}_{n,k,\left(\prod_{j=1}^{q} p_j^{r_{1,j}},\ldots,\prod_{j=1}^{q} p_j^{r_{k,j}}\right)} \cong \bigtimes_{j=1}^{q} \mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}.$$

Beweis. Für alle $j \in \underline{q}$ sei S_j die p_j-Sylowgruppe von $\mathcal{N}_{n,k,\left(\prod_{j=1}^{q} p_j^{r_{1,j}},\ldots,\prod_{j=1}^{q} p_j^{r_{k,j}}\right)}$. Da $\mathcal{N}_{n,k,\left(\prod_{j=1}^{q} p_j^{r_{1,j}},\ldots,\prod_{j=1}^{q} p_j^{r_{k,j}}\right)}$ endlich und nilpotent ist, gilt

$$\mathcal{N}_{n,k,\left(\prod_{j=1}^{q} p_j^{r_{1,j}},\ldots,\prod_{j=1}^{q} p_j^{r_{k,j}}\right)} = \bigtimes_{j=1}^{q} S_j.$$

Sei $l \in \underline{q}$, $i \in \underline{k}$ und $g \in \gamma_i(S_l)$. Dann ist $g \in \gamma_i\left(\mathcal{N}_{n,k,\left(\prod_{j=1}^{q} p_j^{r_{1,j}},\ldots,\prod_{j=1}^{q} p_j^{r_{k,j}}\right)}\right)$ und damit gilt $o(g) \mid \prod_{t=1}^{q} p_t^{r_{i,t}}$. Da $g \in S_l$ ist, ist $o(g)$ eine p_l-Potenz und es folgt $o(g) \mid p_l^{r_{i,l}}$. Somit ist $S_l \in \mathfrak{N}_{n,k,\left(p_l^{r_{1,l}},\ldots,p_l^{r_{k,l}}\right)}$ für alle $j \in \underline{q}$.
Außerdem ist

$$\bigtimes_{j=1}^{q} \mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)} \in \mathfrak{N}_{n,k,\left(\prod_{j=1}^{q} p_j^{r_{1,j}},\ldots,\prod_{j=1}^{q} p_j^{r_{k,j}}\right)}, \quad \text{denn:}$$

Sei $i \in \underline{k}$ und $g \in \gamma_i\left(\times_{j=1}^{q} \mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}\right) = \times_{j=1}^{q} \gamma_i\left(\mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}\right)$. Dann existieren $g_j \in \gamma_i\left(\mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}\right)$ für alle $j \in \underline{q}$ mit $g = g_1 \ldots g_q$ und $g_1, \ldots, g_q$ kommutieren paarweise miteinander. Außerdem gilt $o(g_j) \mid p_j^{r_{i,j}}$ für alle $i \in \underline{q}$. Damit folgt

$$g^{\prod_{j=1}^{q} p_j^{r_{i,j}}} = g_1^{\prod_{j=1}^{q} p_j^{r_{i,j}}} \cdots g_q^{\prod_{j=1}^{q} p_j^{r_{i,j}}} = 1 \cdots 1 = 1, \quad \text{also ist}$$
$$\bigtimes_{j=1}^{q} \mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)} \in \mathfrak{N}_{n,k,\left(\prod_{j=1}^{q} p_j^{r_{1,j}},\ldots,\prod_{j=1}^{q} p_j^{r_{k,j}}\right)}.$$

Wir erhalten

$$\begin{aligned}
\prod_{j=1}^{q} |S_j| &\leq \prod_{j=1}^{q} \left|\mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}\right| \\
&= \left|\bigtimes_{j=1}^{q} \mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}\right| \\
&\leq \left|\mathcal{N}_{n,k,\left(\prod_{j=1}^{q} p_j^{r_{1,j}},\ldots,\prod_{j=1}^{q} p_j^{r_{k,j}}\right)}\right| \\
&= \left|\bigtimes_{j=1}^{q} S_j\right| \\
&= \prod_{j=1}^{q} |S_j|.
\end{aligned}$$

Damit folgt $|S_j| = \left|\mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}\right|$ und damit $S_j \cong \mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}$ für alle $j \in \underline{q}$. Wir erhalten

$$\mathcal{N}_{n,k,\left(\prod_{j=1}^q p_j^{r_{1,j}},\ldots,\prod_{j=1}^q p_j^{r_{k,j}}\right)} = \bigtimes_{j=1}^q S_j \cong \bigtimes_{j=1}^q \mathcal{N}_{n,k,\left(p_j^{r_{1,j}},\ldots,p_j^{r_{k,j}}\right)}.$$

□

Aus Lemma 3.42 und dem vorherigen Lemma folgt, dass es genügt die Gruppenklassen $\mathfrak{N}_{n,k,\varepsilon}$ zu studieren, bei denen $\varepsilon = (p^{r_1},\ldots,p^{r_k})$ für eine Primzahl p und $r_1,\ldots,r_k \in \mathbb{N}$ mit $r_1 \geq \cdots \geq r_k$ gilt.
In dem folgenden Lemma sehen wir, wie wir $\mathcal{N}_{n,k,\zeta}$ aus $\mathcal{N}_{n,k,\varepsilon}$ durch Faktorisierung nach geeigneten Normalteilern für geeignete $\zeta \in \mathbb{N}^k$ konstruieren können.

Lemma 3.47 Sei $\zeta = (\zeta_1,\ldots,\zeta_k) \in \mathbb{N}^k$, so dass $\zeta_i \mid \varepsilon_i$ für alle $i \in \underline{k}$ gilt. Dann gilt

$$\mathcal{N}_{n,k,\varepsilon} / \prod_{i=1}^k \gamma_i(\mathcal{N}_{n,k,\varepsilon})^{\zeta_i} \cong \mathcal{N}_{n,k,\zeta}.$$

Beweis. Es ist $\mathcal{N}_{n,k,\varepsilon} / \prod_{i=1}^k \gamma_i(\mathcal{N}_{n,k,\varepsilon})^{\zeta_i} \in \mathfrak{N}_{n,k,\zeta}$.
Sei $\mathcal{G} \in \mathfrak{N}_{n,k,\zeta}$. Dann ist nach Voraussetzung $\mathcal{G} \in \mathfrak{N}_{n,k,\varepsilon}$ und damit gibt es einen Epimorphismus $\varphi : \mathcal{N}_{n,k,\varepsilon} \to \mathcal{G}$ und offenbar ist $\gamma_i(\mathcal{N}_{n,k,\varepsilon})^{\zeta_i} \leq \text{Kern } \varphi$ für alle $i \in \underline{k}$, also ist $\prod_{i=1}^k \gamma_i(\mathcal{N}_{n,k,\varepsilon})^{\zeta_i} \leq \text{Kern } \varphi$. □

Nun wollen wir einsehen, dass die von X in $N_{K,X,k}$ $*$-erzeugte Gruppe frei in einer geeigneten Klasse ist und in dieser Gruppe in (3.1) die Gleichheit gilt. Wir gewinnen also eine eindeutige Darstellung von Elementen. Die Aussage (b) findet sich bereits in [Han12, Satz 2.16].

Satz 3.48 Sei $n > 1$ und X n-elementig, $X = \{x_1,\ldots,x_n\}$. Sei $\beta : \mathcal{F}_X \to (N_{K,X,k}, *)$ die homomorphe Fortsetzung von $x \mapsto x$ für alle $x \in X$. Weiter sei $\mathfrak{E}_i^{\mathfrak{G},\beta} = (e_{i,1},\ldots,e_{i,n_i})$ für alle $i \in \underline{k}$ das Tupel der Elementarkommutatoren in $N_{K,X,k}$ vom Gewicht i. Für alle $i \in \underline{k}$ und $j \in \underline{n_i}$ sei

$$O_{i,j} := \begin{cases} \dfrac{o(e_{i,j}) - 1_0}{\mathbb{Z}} & o(e_{i,j}) \text{ ist endlich} \\ & \text{sonst} \end{cases}.$$

Dann gilt:

(a) Es ist Bild $\beta = \langle X\rangle_*$ und

$$\langle X\rangle_* = \left\{ \bigstar_{i=1}^k \bigstar_{j=1}^{n_i} e_{i,j}^{(\alpha_{i,j})} \mid \forall i \in \underline{k}, j \in \underline{n_i} :\ \alpha_{i,j} \in O_{i,j} \right\}.$$

Dabei ist die Darstellung der Elemente von $\langle X\rangle_*$ in dieser Form eindeutig.

(b) Ist char $K = 0$, so ist $O_{i,j} = \mathbb{Z}$ für alle $i \in \underline{k}$ und $j \in \underline{n_i}$ und es gilt

$$\langle X \rangle_* \cong \mathcal{N}_{n,k}.$$

(c) Sei char $K \neq 0$ und $c := \operatorname{char} K$. Seien $q \in \mathbb{N}$, $p_1, \ldots, p_q \in \mathbb{P}$ paarweise verschieden und $r_1, \ldots, r_q \in \mathbb{N}$ mit $c = p_1^{r_1} \ldots p_q^{r_q}$. Für alle $i \in \underline{k}$ sei $t_{l,i} \in \underline{s_{p_l}}_0$ mit $i \in I_{p_l,t_{l,i}}$ für alle $l \in \underline{q}$. Dann ist $o(e_{i,j}) = p_1^{r_1+t_{1,i}} \ldots p_q^{r_q+t_{q,i}}$ für alle $j \in \underline{n_i}$.
Sei $\varepsilon := (o(e_{1,1}), \ldots, o(e_{k,1}))$. Dann ist

$$\langle X \rangle_* \cong \mathcal{N}_{n,k,\varepsilon} \quad \text{und} \quad |\langle X \rangle_*| = \prod_{i=1}^{k} o(e_{i,1})^{n_i}.$$

Ist insbesondere $K = \mathbb{Z}/p^l\mathbb{Z}$ für ein $p \in \mathbb{P}$ und ein $l \in \mathbb{N}$ und ist $t_i \in \underline{s}_0$ mit $i \in I_{t_i}$ für alle $i \in \underline{k}$, so ist

$$\langle X \rangle_* \cong \mathcal{N}_{n,k,(p^{l+t_1},\ldots,p^{l+t_k})}.$$

Beweis. (a) Bild $\beta = \langle X \rangle_*$ folgt aus der Definition von β.
Wir wollen nun die Voraussetzungen von Korollar 1.58.2 (c) nachweisen. Für alle $i \in \underline{k}$ sind $e_{i,1}, \ldots, e_{i,n_i} \in \gamma_i(\langle X \rangle_*)$ und es gilt nach Satz 1.48

$$\gamma_i(\langle X \rangle_*)/\gamma_{i+1}(\langle X \rangle_*) = \langle e_{i,j}\gamma_{i+1}(\langle X \rangle_*) \mid j \in \underline{n_i} \rangle_*.$$

Wir setzen für alle $i \in \underline{k}$ und $j \in \underline{n_i}$

$$\begin{aligned}
M_{i,1} = \Big\{ & e_{r_1,t_1} \ldots e_{r_m,t_m} \mid m \in \mathbb{N}, r_1, \ldots, r_m \in \{i+1, \ldots, k\}, \\
& \forall u \in \underline{m} : t_u \in \underline{n_{r_u}}, (r_1, t_1) \underset{lex}{\leq} \ldots \underset{lex}{\leq} (r_m, t_m) \Big\}, \\
M_{i,2} = \big\{ & e_{i,t_1} \ldots e_{i,t_m} \mid m \in \mathbb{N}, t_1, \ldots, t_m \in \underline{n_i}, t_1 \leq \cdots \leq t_m \big\}, \\
M_{(i,j)} = \big\{ & e_{i,j}^m \mid m \in \underline{k} \big\} \quad \text{und} \\
M_{(i,>j)} = \{ & e_{i,t_1} \ldots e_{i,t_m} \mid m \in \mathbb{N}, t_1, \ldots, t_m \in \{j+1, \ldots, n_i\}, t_1 \leq \cdots \leq t_m \}.
\end{aligned}$$

Sei

$$\begin{aligned}
B = \Big\{ & e_{i_1,j_1} \ldots e_{i_m,j_m} \mid m \in \mathbb{N}, i_1, \ldots, i_m \in \underline{k}, \forall t \in \underline{m} : j_t \in \underline{n_{i_t}}, \\
& (i_1, j_1) \underset{lex}{\leq} \ldots \underset{lex}{\leq} (i_m, j_m) \Big\}
\end{aligned}$$

die in Lemma 1.52 konstruierte Basis von N. Dann sind

$$M_{i,1} \setminus \{0\}, M_{i,2} \setminus \{0\}, M_{(i,j)} \setminus \{0\}, M_{(i,>j)} \setminus \{0\} \subseteq B$$

für alle $i \in \underline{k}$ und $j \in \underline{n_i}$ und es gilt bei festem $i \in \underline{k}$ und $j \in \underline{n_i}$

$$M_{i,1} \cap M_{i,2}, M_{i,1} \cap M_{(i,j)}, M_{(i,j)} \cap M_{(i,>j)} \subseteq \{0\}$$

und damit

$$\langle M_{i,1} \rangle_K \cap \langle M_{i,2} \rangle_K = \{0\} = \langle M_{i,1} \rangle_K \cap \langle M_{(i,j)} \rangle_K = \langle M_{(i,j)} \rangle_K \cap \langle M_{(i,>j)} \rangle_K.$$

Sei $i \in \underline{k}$ und $j \in \underline{n_{i,}}$. Dann gilt mit Lemma 1.2 (e), (f)

$$\langle e_{i,j}\rangle_* \subseteq \langle M_{(i,j)}\rangle_K \quad \text{und} \quad \gamma_{i+1}(\langle X\rangle_*) \subseteq \langle M_{i,1}\rangle_K$$

mit Satz 1.48. Es folgt $\langle e_{i,j}\rangle_* \cap \gamma_{i+1}(\langle X\rangle_*) = \{0\}$.
Sei nun $i \in \underline{k}$ und $\alpha_j \in \mathbb{Z}$ für alle $j \in \underline{n_{i,}}$ mit $\bigstar_{j=1}^{n_i} e_{i,j}^{(\alpha_j)} \in \gamma_{i+1}(\langle X\rangle_*)$. Dann gilt mit Lemma 1.2 (d)

$$\begin{aligned}
&\bigstar_{j=1}^{n_i} e_{i,j}^{(\alpha_j)} \in \langle M_{i,2}\rangle_K \text{ und}\\
&\bigstar_{j=1}^{n_i} e_{i,j}^{(\alpha_j)} \in \gamma_{i+1}(\langle X\rangle_*) \subseteq \langle M_{i,1}\rangle_K, \text{ also}\\
&\bigstar_{j=1}^{n_i} e_{i,j}^{(\alpha_j)} \in \langle M_{i,1}\rangle_K \cap \langle M_{i,2}\rangle_K = \{0\}.
\end{aligned}$$

Damit ist $\bigstar_{j=1}^{n_i} e_{i,j}^{(\alpha_j)} = 0$. Es folgt $e_{i,1}^{(-\alpha_1)} = \bigstar_{j=2}^{n_i} e_{i,j}^{(\alpha_j)}$ und

$$e_{i,1}^{(-\alpha_1)} \in \langle M_{(i,1)}\rangle_K \quad \text{und} \quad \bigstar_{j=2}^{n_i} e_{i,j}^{(\alpha_j)} \in \langle M_{(i,>1)}\rangle_K.$$

Es folgt $e_{i,1}^{(\alpha_1)} = 0 = \bigstar_{j=2}^{n_i} e_{i,j}^{(\alpha_j)}$ und induktiv $e_{i,j}^{(\alpha_j)} = 0$ für alle $j \in \underline{n_{i,}}$. Damit ist

$$\gamma_i(\langle X\rangle_*)/\gamma_{i+1}(\langle X\rangle_*) = \bigtimes_{j=1}^{n_i} \langle e_{i,j}\gamma_{i+1}(\langle X\rangle_*)\rangle_*.$$

Somit gelten nun die Voraussetzungen von Korollar 1.58.2 (c) und es folgt damit

$$\langle X\rangle_* = \left\{ \bigstar_{i=1}^{k} \bigstar_{j=1}^{n_i} e_{i,j}^{(\alpha_{i,j})} \mid \forall i \in \underline{k}, j \in \underline{n_{i,}} \colon \alpha_{i,j} \in O_{i,j} \right\}$$

und die Darstellung der Elemente von $\langle X\rangle_*$ in dieser Form ist eindeutig.
(b) Sei $\operatorname{char} K = 0$. Dann ist nach Korollar 1.27.1 die Ordnung von $e_{i,j}$ unendlich und damit $O_{i,j} = \mathbb{Z}$ für alle $i \in \underline{k}$ und $j \in \underline{n_{i,}}$. Sei $Y = \{y_1, \dots y_n\}$ ein $\mathfrak{N}_{n,k}$-freies Erzeugendensystem von $\mathcal{N}_{n,k}$ und $\varphi : \mathcal{N}_{n,k} \to \langle X\rangle_*$ die homomorphe Fortsetzung von $y_i \mapsto x_i$ für alle $i \in \underline{n}$. Dann ist φ surjektiv und aus der Eindeutigkeit der Darstellung in (a) folgt $\operatorname{Kern}\varphi = \{1\}$. Damit ist φ ein Isomorphismus und damit $\mathcal{N}_{n,k} \cong \langle X\rangle_*$.
(c) Sei $\operatorname{char} K \neq 0$ und $c := \operatorname{char} K$. Sei $\tilde{K} = \langle 1_K\rangle_{\mathbb{Z}}$ der Primring von K. Dann ist $\langle X\rangle_* \subseteq N_{\tilde{K},X,k}$ und $\tilde{K} \cong \mathbb{Z}/c\mathbb{Z}$. Wir nehmen o.B.d.A. an, dass $c = p^l$ für eine Primzahl p und $l \in \mathbb{N}$ gilt. Der allgemeine Fall folgt aus diesem mit Satz 1.38. Sei $i \in \underline{k}$, $j \in \underline{n_{i,}}$ und $t \in \underline{s_{p,}}$ mit $i \in I_{p,t}$. Dann ist $o(e_{i,j}) = p^{l+t}$ nach Bemerkung 1.53.
Sei $\varepsilon := (o(e_{1,1}), \dots, o(e_{k,1}))$. Nach Lemma 1.35 ist $\langle X\rangle_* \in \mathfrak{N}_{n,k,\varepsilon}$ und es gilt

$$|\langle X\rangle_*| \overset{\text{(a)}}{=} \prod_{i=1}^{k}\prod_{j=1}^{n_i} o(e_{i,j}) \overset{1.53}{=} \prod_{i=1}^{k} o(e_{i,1})^{n_i} \overset{3.43}{\geq} |\mathcal{N}_{n,k,\varepsilon}|.$$

Es folgt $\mathcal{N}_{n,k,\varepsilon} \cong \langle X\rangle_*$. □

Korollar 3.48.1 In $P_{\mathbb{Z},X}$ gilt

$$\langle X\rangle_* \cap P_{\mathbb{Z},X}^{k+1} = \gamma_{k+1}(\langle X\rangle_*).$$

Beweis. Es ist $\pi_{\leq k}$ ein Algebren-Epimorphismus von $P_{\mathbb{Z},X}$ auf $N_{\mathbb{Z},X,k}$ und es gilt

$$\text{Kern } \pi_{\leq k|\langle X\rangle_*} = \langle X\rangle_* \cap P_{\mathbb{Z},X}^{k+1}.$$

Mit dem Homomorphiesatz ist

$$\underbrace{\langle X\rangle_*/\text{Kern } \pi_{\leq k|\langle X\rangle_*}}_{\text{in } P} \cong \underbrace{\langle X\rangle_*}_{\text{in } N} \overset{3.48(b)}{\cong} \mathcal{N}_{n,k}.$$

Nach Satz 2.14 ist $\langle X\rangle_*$ frei über X und damit gilt in P

$$\langle X\rangle_*/\text{Kern } \pi_{\leq k|\langle X\rangle_*} \cong \langle X\rangle_*/\gamma_{k+1}(\langle X\rangle_*).$$

Da $\gamma_{k+1}(\langle X\rangle_*) \leq P_{\mathbb{Z},X}^{k+1} \cap \langle X\rangle_* = \text{Kern } \pi_{\leq k|\langle X\rangle_*}$ gilt und nach [MKS76, Seite 296, Theorem 5.5] endlich erzeugte nilpotente Gruppen hopfsch sind, folgt

$$\gamma_{k+1}(\langle X\rangle_*) = \text{Kern } \pi_{\leq k|\langle X\rangle_*} = \langle X\rangle_* \cap P_{\mathbb{Z},X}^{k+1}.$$

□

Korollar 3.48.2 (a) In $(N_{\mathbb{Z},X,k}, *)$ ist die von X erzeugte Gruppe $\mathfrak{N}_k$-frei über X.

(b) Mit $\varepsilon = (o(e_{1,1}), \ldots, o(e_{k,1}))$ wie zuvor ist in $(N_{\mathbb{Z}/c\mathbb{Z},X,k}, *)$ ist die von X erzeugte Gruppe $\mathfrak{N}_{k,\varepsilon}$-frei über X.

Beweis. Für endliche X wissen wir dies bereits und die allgemeine Behauptung folgt mit Bemerkung 3.40. □

Beispiel 3.49 Sei $k = 2 = p$, $l = 1$ und $n = 2$, etwa $X = \{x, y\}$. Dann ist (x, y) das Tupel der Elementarkommutatoren vom Gewicht 1 und $([y, x]_*)$ das Tupel der Elementarkommutatoren vom Gewicht 2. Es folgt mit Bemerkung 1.53 und Satz 3.48 (c)

$$|\langle X\rangle_*| = o(x) \cdot o(y) \cdot o([x, y]_*) = 4 \cdot 4 \cdot 2 = 32.$$

Zudem lässt sich die Abbildung

$$X \to \langle a, b \mid \{a^4, b^4, (a, b)^2, (a, b, b), (a, b, b)\}\rangle, \quad x \mapsto a,\ y \mapsto b,$$

zu einem Homomorphismus fortsetzen. Die durch Erzeuger und Relationen angegebene Gruppe ist eine Gruppe der Ordnung 32, das heißt die Abbildung ist ein Isomorphismus. Die Gruppe ist somit isomorph zu der Gruppe mit der Hall-Senior-Nummer 18 unter den Gruppen der Ordnung 32, welche der SmallGroup(32,2) in der GAP-Nummerierung entspricht.

Beispiel 3.50 Nach Satz 3.48 ist in $N_{\mathbb{Z}/3^3\mathbb{Z},2,10}$ mit Hilfe von Beispiel 1.17

$$\langle X\rangle_* \cong \mathcal{N}_{2,10,(3^5,3^4,3^4,3^3,\ldots,3^3)}.$$

Außerdem ist nach Berechnung von $n_1,\ldots,n_{10}$ für $n=2$

$$\begin{aligned}|\langle X\rangle_*| &= \left(3^5\right)^2\cdot\left(3^4\right)^1\cdot\left(3^4\right)^2\cdot\left(3^3\right)^3\cdot\left(3^3\right)^6\cdot\left(3^3\right)^9\cdot\left(3^3\right)^{18}\cdot\left(3^3\right)^{30}\cdot\left(3^3\right)^{56}\cdot\left(3^3\right)^{99}\\ &= 3^{685}.\end{aligned}$$

Wir sehen in Satz 3.48 (c), dass in der Ungleichung (3.1) der Fall der Gleichheit vorkommt. Es stellt sich also die Frage, für welche Wahlen der Parameter n,k,ε die Gleichheit angenommen wird. Nach Lemma 3.43 (b) ist dies äquivalent zur eindeutigen Darstellbarkeit der Elemente durch Elementarkommutatoren.

Bemerkung 3.51 (a) Sei $\mathcal{N}_{n,k,\varepsilon}$ abelsch. Dann gilt die Gleichheit in (3.1) genau dann, wenn $\varepsilon_i = 1$ für alle $i \in \underline{k}\setminus\{1\}$ gilt. Insbesondere gilt dies für $k=1$.

(b) Sei $p\in\mathbb{P}$ und $l\in\mathbb{N}$. Dann wird für $n>1$ in $\mathcal{N}_{n,p-1,(p^l,\ldots,p^l)}$ die Gleichheit in (3.1) angenommen.

Beweis. (a) Sei X ein $\mathcal{N}_{n,k,\varepsilon}$-freies Erzeugendensystem von $\mathcal{N}_{n,k,\varepsilon}$. Da $\mathcal{N}_{n,k,\varepsilon}$ abelsch ist, folgt

$$\mathcal{N}_{n,k,\varepsilon} = \langle X\rangle = \prod_{x\in X}\langle x\rangle \quad \text{ und damit } \quad |\mathcal{N}_{n,k,\varepsilon}| \le \varepsilon_1^n.$$

Außerdem ist

$$\underbrace{\mathcal{C}_{\varepsilon_1}\times\cdots\times\mathcal{C}_{\varepsilon_1}}_{n}$$

epimorphes Bild von $\mathcal{N}_{n,k,\varepsilon}$ und damit folgt $|\mathcal{N}_{n,k,\varepsilon}| = \varepsilon_1^n$.
(b) Sei X n-elementig. Es ist $I_0 = \underline{k}$ und damit $o(e_{i,1}) = p^l$ in $N_{\mathbb{Z}/p^l\mathbb{Z},X,p-1}$ nach Bemerkung 1.53. Nach Satz 3.48 (c) ist somit $\mathcal{N}_{n,p-1,(p^l,\ldots,p^l)} \cong \langle X\rangle_* \le N_{\mathbb{Z}/p^l\mathbb{Z},X,p-1}$ und es gilt die Gleichheit in (3.1). □

Wir sehen, dass die Gleichheit in (3.1) nicht immer angenommen wird: Ist $\varepsilon_1 = 2$, so ist $\mathcal{N}_{n,k,\varepsilon}$ abelsch, also gilt nach (a) beispielsweise in $\mathcal{N}_{2,2,(2,2)}$ nicht die Gleichheit. Allerdings ist in allen bisher beschriebenen Fällen, bei denen in (3.1) nicht die Gleichheit gilt, die Gruppe $\mathcal{N}_{n,k,\varepsilon}$ abelsch. Wir betrachten nun ein weiteres Beispiel, in dem die Ungleichung (3.1) nicht mit Gleichheit erfüllt ist. Auch hier stellt sich raus, dass die Nilpotenzklasse kleiner ist als die ursprünglich angegebene.

Beispiel 3.52 $\mathcal{N}_{2,3,(3,3,3)}$ ist von Klasse 2 und es ist $|\mathcal{N}_{2,3,(3,3,3)}| = 3^3$. Insbesondere gilt in (3.1) nicht die Gleichheit.

Beweis. Sei $k = 3$ und $n = 2$. Es ist $n_1 = 2$, $n_2 = 1$ und $n_3 = 2$ und damit

$$|\mathcal{N}_{2,3,(3,3,3)}| \leq 3^2 \cdot 3 \cdot 3^2 = 3^5.$$

Es ist nach Lemma 3.47 und Satz 3.48 (c)

$$\mathcal{N}_{2,3,(3,3,3)} \cong \mathcal{N}_{2,3,(9,3,3)} / \prod_{i=1}^{3} \gamma_i(\mathcal{N}_{2,3,(9,3,3)})^3 \cong \langle X \rangle_* / \langle X \rangle_*^{(3)},$$

wobei wir $\langle X \rangle_*$ in $N := N_{\mathbb{Z}/3\mathbb{Z},X,3}$ mit $X = \{x, y\}$ betrachten. Wir wollen nun $\langle X \rangle_*^{(3)}$ untersuchen. Da char $K = 3$ ist, ist $\langle X \rangle_*^{(3)} = \langle X \rangle_*^3 \subseteq N^3$. Daher ist $(\langle X \rangle_*^3, *) = (\langle X \rangle_*^3, +)$. Außerdem ist $\gamma_3(\langle X \rangle_*)$ von den Elementarkommutatoren vom Gewicht 3, also beispielsweise von

$$[[y, x]_*, x]_* = [[y, x], x] \quad \text{und} \quad [[y, x]_*, y]_* = [[y, x], y]$$

erzeugt. Es gilt mit char $K = 3$

$$\begin{aligned}
[[y, x], y] &= 2xy^2 + 2yxy + 2y^2x \\
&= x^3 + y^3 + xyx + x^2y + yx^2 + xy^2 + y^2x + yxy \\
&\quad - x^3 - y^3 - xyx - x^2y - yx^2 + xy^2 + y^2x + yxy \\
&= (x + y)^3 + (x^3 - y^3 - xyx - x^2y - yx^2 + xy^2 + y^2x + yxy) + x^3 \\
&= (x + y)^3 + (x - y)^3 + x^3 \\
&= (x * y)^3 + (x * y^-)^3 + x^3 \\
&= (x * y)^3 * ((x * y^-)^3) * x^3 \in \langle X \rangle_*^3 \quad \text{und} \\
[[y, x], x] &= xyx + x^2y + yx^2 \\
&= x^3 + y^3 + xyx + x^2y + yx^2 + xy^2 + y^2x + yxy \\
&\quad + 2xy^2 + 2yxy + 2y^2x - x^3 - y^3 \\
&= (x + y)^3 + [[y, x], y] - x^3 - y^3 \\
&= (x * y)^3 * \underbrace{[[y, x], y]}_{\in \langle X \rangle_*^3, \text{ s. oben}} * (x^3)^- * (y^3)^- \in \langle X \rangle_*^3.
\end{aligned}$$

Damit ist $\gamma_3(\langle X \rangle_*) \leq \langle X \rangle_*^3$. Also ist die Nilpotenzklasse von $\mathcal{N}_{2,3,(3,3,3)}$ höchstens 2. Wegen $L([x, y]_*) = 2$, also $[x, y]_* \notin \langle X \rangle_*^3$, folgt, dass die Nilpotenzklasse 2 ist. Damit folgt

$$|\mathcal{N}_{2,3,(3,3,3)}| \leq 3^2 \cdot 3 = 3^3.$$

Da jede Gruppe der Ordnung 3 und 3^2 abelsch ist, folgt $|\mathcal{N}_{2,3,(3,3,3)}| = 3^3$. □

Nun werden wir mit Hilfe der Isomorphie $\langle X \rangle_* \cong \mathcal{N}_{n,k,\varepsilon}$ eine Darstellung der Gruppe durch Erzeuger und Relationen angeben.

Definition und Lemma 3.53 Sei Y eine n-elementige Menge, $Y = \{y_1, \ldots, y_n\}$. Für alle $i \in \mathbb{N}$ sei $\mathfrak{E}_i^{\mathfrak{G}} = (e_{i,1}, \ldots, e_{i,n_i})$ das Tupel der Elementarkommutatoren vom Gewicht i in $\mathcal{F}_Y$. Wir setzen

$$\mathcal{M}_{n,k,\varepsilon} := \langle y_1, \ldots, y_n \mid \{e_{i,j}^{\varepsilon_i} \mid i \in \underline{k}, j \in \underline{n_i}\} \cup \{(y_{i_1}, \ldots, y_{i_{k+1}}) \mid i_1, \ldots, i_{k+1} \in \underline{n}\}\rangle.$$

Dann gilt:

(a) Es gibt einen Epimorphismus $\varphi : \mathcal{M}_{n,k,\varepsilon} \to \mathcal{N}_{n,k,\varepsilon}$.

(b) Es ist $|\mathcal{M}_{n,k,\varepsilon}| \leq \prod_{i=1}^{k} \varepsilon_i^{n_i}$.

(c) Gilt in (3.1) die Gleichheit, so ist $\mathcal{N}_{n,k,\varepsilon} \cong \mathcal{M}_{n,k,\varepsilon}$. Ist insbesondere $c := \text{char } K \neq 0$ und ε wie in Satz 3.48 (c), so gilt $\langle X\rangle_* \cong \mathcal{M}_{n,k,\varepsilon}$ in $N_{K,n,k}$.

Beweis. (a) Dies folgt direkt aus der Definition von $\mathcal{M}_{n,k,\varepsilon}$.
(b) Da $\mathcal{M}_{n,k,\varepsilon}$ nach [Hup67, Seite 258, 1.11 a] nilpotent von Klasse k ist, folgt dies mit Korollar 1.48.1.
(c) Es ist nach Voraussetzung mit Satz 3.48 (c)

$$|\mathcal{N}_{n,k,\varepsilon}| = \prod_{i=1}^{k} \varepsilon_i^{n_i} \geq |\mathcal{M}_{n,k,\varepsilon}|.$$

Mit (a), (b) und Satz 3.48 (c) folgt die Behauptung. □

Bemerkung 3.54 $\mathcal{M}_{n,k,\varepsilon} \in \mathfrak{N}_{n,k,\varepsilon}$ gilt im Allgemeinen nicht. Insbesondere ist

$$\mathcal{M}_{2,2,(2,2)} \cong D_8$$

und damit nicht vom Exponenten 2.

Beweis. Die Abbildung $y_1 \mapsto (13)$ und $y_2 \mapsto (12)(34)$ lässt sich wegen

$$o((13)) = 2 = o((12)(34)),\ o(((13),(12)(34))) = o((13)(24)) = 2$$

und da D_8 von der Klasse 2 ist zu einem Epimorphismus $\mathcal{M}_{n,k,\varepsilon} \to D_8$ fortsetzen. Mit Lemma 3.53 (b) ist $|\mathcal{M}_{2,2,(2,2)}| \leq 2^2 \cdot 2^1 = 8$ und damit folgt die Isomorphie. □

Wir können also die Gruppe $\mathcal{N}_{n,k,\varepsilon}$ – und damit auch $\langle X\rangle_*$ – im Fall der Gleichheit in (3.1) als Erzeuger und Relationen angeben.

Wir wollen nun zeigen, dass wir im Fall $n = 2 = k$ die Gruppe $\mathcal{N}_{n,k,(p^l,p^l)}$ mit $p \neq 2$ als Heisenberggruppe wiederfinden.

Definition 3.55 Wir definieren

$$\mathcal{H}_K := \left\{ \begin{pmatrix} 0 & a & c \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix} \mid a, b, c \in K \right\}.$$

Da $\mathcal{H}_K$ im Radikal von $K^{3\times 3}$ liegt, ist $(\mathcal{H}_K, *)$ eine Gruppe, die nach Lemma 1.10(c) isomorph zur Heisenberggruppe

$$\left(\left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in K \right\}, \cdot \right)$$

ist.

Nun wollen wir diese Gruppe untersuchen.

Lemma 3.56 Seien

$$X_1 := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, X_2 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, Y := \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathcal{H}_K.$$

Dann gilt

(a) $AB = \begin{cases} Y & A = X_1, B = X_2 \\ 0 & \text{sonst} \end{cases}$ für alle $A, B \in \{X_1, X_2, Y\}$,

(b) $A^- = -A$ für alle $A \in \{X_1, X_2, Y\}$ und

(c) $[X_1, X_2]_* = Y$.

(d) Ist $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ mit $c \in \mathbb{N}_{>1}$, so ist $\mathcal{H}_K = \langle X_1, X_2 \rangle_*$.

Beweis. (a) Seien $A, B \in \{X_1, X_2, Y\}$. Ist $A \neq X_1$, so ist $AB = 0$, da B in der letzten Zeile nur den Eintrag Null hat. Ist $A = X_1$ und $B \neq X_2$, so ist $AB = 0$, da B in der zweiten Zeile nur den Eintrag Null hat. Weiter ist

$$X_1 X_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = Y.$$

(b) Sei $A \in \{X_1, X_2, Y\}$. Nach (a) ist $A^2 = 0$ und damit $A^- = -A$.
(c) Mit (a) und (b) folgt

$$\begin{aligned} [X_1, X_2]_* &= (-X_1) * (-X_2) * X_1 * X_2 \\ &= (-X_1 - X_2 + Y) * (X_1 + X_2 + Y) \\ &= 2Y - Y \\ &= Y. \end{aligned}$$

(d) Sei $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ mit $c \in \mathbb{N}_{>1}$. Mit $X_1, X_2 \in \mathcal{H}_K$ folgt $\langle X_1, X_2 \rangle_* \subseteq \mathcal{H}_K$. Außerdem ist $Y \in \langle X_1, X_2 \rangle_*$ nach (c). Seien $\alpha, \beta, \gamma \in \mathbb{Z}$. Dann gilt nach (a) und (b) $X_1^{(\alpha)} = \alpha X_1$, $X_2^{(\beta)} = \beta X_2$ und $Y^{(\gamma)} = \gamma Y$ und es folgt

$$X_2^{(\beta)} * X_1^{(\alpha)} * Y^{(\gamma)} = \beta X_2 + \alpha X_1 + \gamma Y = \begin{pmatrix} 0 & \alpha & \gamma \\ 0 & 0 & \beta \\ 0 & 0 & 0 \end{pmatrix}.$$

Da K ein Faktorring von $\mathbb{Z}$ ist, ist damit auch $\mathcal{H}_K \subseteq \langle X_1, X_2 \rangle_*$. □

Satz 3.57 Sei $K = \mathbb{Z}$ oder $K = \mathbb{Z}/c\mathbb{Z}$ mit $c \in \mathbb{N}_{>1}$ und $2 \nmid c$. Dann gilt

$$\mathcal{H}_K \cong \begin{cases} \mathcal{N}_{2,2} & \text{falls } K = \mathbb{Z} \\ \mathcal{N}_{2,2,(c,c)} & \text{falls } K = \mathbb{Z}/c\mathbb{Z} \end{cases}.$$

Beweis. Nach Lemma 3.56 (d) ist $\mathcal{H}_K$ von zwei Elementen erzeugt und da $\mathcal{H}_K^3 = \{0\}$ ist, ist $(\mathcal{H}_K, *)$ nach Bemerkung 1.3 (f) nilpotent von der Klasse höchstens 2. Also ist $\mathcal{H}_K \in \mathfrak{N}_{2,2}$.
Sei $K = \mathbb{Z}/c\mathbb{Z}$ mit $c \in \mathbb{N}_{>1}$ und $2 \nmid c$. Dann gilt

$$\binom{c}{2} = c\underbrace{\frac{c-1}{2}}_{\in\mathbb{N}} \quad \text{und damit} \quad A^{(c)} = cA + \binom{c}{2}A^2 = 0$$

für alle $A \in \mathcal{H}_K$. Damit ist $\mathcal{H}_K \in \mathfrak{N}_{2,2,(c,c)}$ und es folgt mit Lemma 3.43 (a)

$$|\mathcal{H}_K| = |K|^3 = c^3 = c^2 \cdot c \geq |\mathcal{N}_{2,2,(c,c)}|.$$

Da $\mathcal{N}_{2,2,(c,c)}$ frei in $\mathfrak{N}_{2,2,(c,c)}$ ist, folgt $\mathcal{H}_K \cong \mathcal{N}_{2,2,(c,c)}$.
Sei $K = \mathbb{Z}$. Seien X_1, X_2, Y wie in Lemma 3.56 und $\{a_1, a_2\}$ ein $\mathfrak{N}_{2,2}$-freies Erzeugendensystem von $\mathcal{N}_{2,2}$. Sei $\varphi : \mathcal{N}_{2,2} \to \mathcal{H}_\mathbb{Z}$ die homomorphe Fortsetzung der Abbildung $a_1 \mapsto X_1$ und $a_2 \mapsto X_2$. Nach Lemma 3.56 ist φ ein Epimorphismus. Nach Korollar 1.48.1 ist

$$\mathcal{N}_{2,2} = \left\{ a_2^\alpha a_1^\beta (a_1, a_2)^\gamma \mid \alpha, \beta, \gamma \in \mathbb{Z} \right\}.$$

Seien $\alpha, \beta, \gamma \in \mathbb{Z}$ mit $a_2^\alpha a_1^\beta (a_1, a_2)^\gamma \in \text{Kern } \varphi$. Dann ist wie im Beweis von 3.56 (d)

$$0 = X_2^{(\alpha)} * X_1^{(\beta)} * [X_1, X_2]_*^{(\gamma)} = \alpha X_2 + \beta X_1 + \gamma Y = \begin{pmatrix} 0 & \beta & \gamma \\ 0 & 0 & \alpha \\ 0 & 0 & 0 \end{pmatrix},$$

also $\alpha = \beta = \gamma = 0$. Damit ist Kern $\varphi = \{0\}$ und somit φ ein Isomorphismus. □

Wir haben in Satz 3.48 gezeigt, dass die Elemente in $\langle X \rangle_*$ eine eindeutige Darstellung als geordnetes Produkt von Elementarkommutatoren haben. Leider hilft das beim konkreten Rechnen innerhalb der Gruppe nicht weiter, wie das folgende Beispiel zeigt:

Beispiel 3.58 Wir rechnen in $N_{\mathbb{Z},X,4}$. Sei $X = \{x_1, \ldots x_n\}$ und $\mathfrak{E} = (e_1, \ldots, e_m)$ das Tupel der gemäß ihres Gewichtes geordneten Elementarkommutatoren in X bis zum Gewicht 4, so dass die Elementarkommutatoren vom Gewicht 1, 2, 3 und 4 jeweils in der Reihenfolge nach der lexikographischen Ordnung der auftretenden Indizes geordnet seien. [10]

Seien $i, j \in \underline{m}$ mit $i > j$. Es gilt

$$e_i * e_j = e_j * e_i * [e_i, e_j]_*.$$

Wir wollen nun $[e_i, e_j]_*$ wieder als geordnetes Produkt von Elementarkommutatoren schreiben. Wir betrachten dazu die folgende Fallunterscheidung, deren Resultate wir durch einfache Rechnungen erhalten:

[10] Beispiel: $[x_3, x_1, x_1, x_2]_* < [[x_3, x_1]_*, [x_2, x_1]_*]_*$, da $(3,1,1,2) \underset{lex}{<} (3,1,2,1)$.

1. Sei $L(e_j) > 2$. Dann ist $[e_i, e_j]_* = 0$.
2. Sei $L(e_j) = 2$.
   a) Sei $L(e_i) > 2$. Dann ist $[e_i, e_j]_* = 0$.
   b) Sei $L(e_i) = 2$. Dann ist $[e_i, e_j]_*$ wegen $i > j$ und $L(e_i) = L(e_j)$ ein Elementarkommutator.
3. Sei $L(e_j) = 1$. Dann ist $e_j = x_j$.
   a) Sei $L(e_i) > 3$. Dann ist $[e_i, e_j]_* = 0$.
   b) Sei $L(e_i) = 3$. Dann existieren $i_1, i_2, i_3 \in \underline{n}$, mit $i_1 > i_2$ und $i_2 \leq i_3$, so dass $e_i = [x_{i_1}, x_{i_2}, x_{i_3}]_*$ ist.
      i. Sei $i_3 \leq j$. Dann ist $[e_i, e_j]_* = [x_{i_1}, x_{i_2}, x_{i_3}, x_j]_*$ ein Elementarkommutator.
      ii. Sei $j \leq i_2 \leq i_3 \leq i_1$. Dann gilt

$$\begin{aligned}[e_i, e_j]_* =& [x_{i_1}, x_{i_2}, x_{i_3}, x_j]_* = [x_{i_2}, x_j, x_{i_3}, x_{i_1}]_*^- * \\ & [x_{i_1}, x_j, x_{i_2}, x_{i_3}]_* * [[x_{i_1}, x_{i_2}]_*, [x_{i_3}, x_j]_*]_* * [[x_{i_1}, x_{i_3}]_*, [x_{i_2}, x_j]_*]_*.\end{aligned}$$

      iii. Sei $j \leq i_2 \leq i_1 \leq i_3$. Dann gilt

$$\begin{aligned}[e_i, e_j]_* &= [x_{i_1}, x_{i_2}, x_{i_3}, x_j]_* \\ &= [x_{i_2}, x_j, x_{i_1}, x_{i_3}]_*^- * [x_{i_1}, x_j, x_{i_2}, x_{i_3}]_* * [[x_{i_3}, x_j]_*, [x_{i_1}, x_{i_2}]_*]_*^-.\end{aligned}$$

      iv. Sei $i_2 \leq j \leq i_3 \leq i_1$. Dann gilt

$$[e_i, e_j]_* = [x_{i_1}, x_{i_2}, x_{i_3}, x_j]_* = [x_{i_1}, x_{i_2}, x_j, x_{i_3}]_* * [[x_{i_1}, x_{i_2}]_*, [x_{i_3}, x_j]_*]_*.$$

      v. Sei $i_2 \leq j \leq i_1 \leq i_3$. Dann gilt

$$[e_i, e_j]_* = [x_{i_1}, x_{i_2}, x_{i_3}, x_j]_* = [x_{i_1}, x_{i_2}, x_j, x_{i_3}]_* * [[x_{i_3}, x_j]_*, [x_{i_1}, x_{i_2}]_*]_*^-.$$

      vi. Sei $i_2 \leq i_1 \leq j \leq i_3$. Dann gilt

$$[e_i, e_j]_* = [x_{i_1}, x_{i_2}, x_{i_3}, x_j]_* = [x_{i_1}, x_{i_2}, x_j, x_{i_3}]_* * [[x_{i_3}, x_j]_*, [x_{i_1}, x_{i_2}]_*]_*^-.$$

   c) Sei $L(e_i) = 2$. Dann gibt es $i_1, i_2 \in \underline{n}$ mit $i_1 > i_2$ und $e_i = [x_{i_1}, x_{i_2}]_*$.
      i. Sei $i_2 \leq j$. Dann ist $[e_i, e_j]_* = [x_{i_1}, x_{i_2}, x_j]_*$ ein Elementarkommutator.
      ii. Sei $i_2 > j$. Dann gilt

$$\begin{aligned}[e_i, e_j]_* =& [x_{i_1}, x_{i_2}, x_j]_* = [x_{i_2}, x_j, x_{i_1}]_*^- * [x_{i_1}, x_j, x_{i_2}]_* * \\ & [[x_{i_1}, x_j]_*, [x_{i_2}, x_j]_*]_* * [[x_{i_1}, x_{i_2}]_*, [x_{i_2}, x_j]_*]_* * [[x_{i_1}, x_{i_2}]_*, [x_{i_1}, x_j]_*]_*.\end{aligned}$$

   d) Sei $L(e_i) = 1$. Dann ist $[e_i, e_j]_*$ ein Elementarkommutator.

4 Die Gruppe quasiregulärer Elemente in der frei nilpotenten Algebra der Nilpotenzklasse $k \leq 3$

In diesem letzten Kapitel befassen wir uns mit der Gruppe $(N_{K,n,k}, *)$ für Faktorringe K von $\mathbb{Z}$, $n \in \mathbb{N}_{>1}$ und $k \in \{1, 2, 3\}$ und werden dabei sehen, dass selbst in diesen kleinen Fällen es im Allgemeinen nicht einfach ist, diese Gruppe zu beschreiben.

In diesem Abschnitt sei stets $K = \mathbb{Z}$ oder $K = \mathbb{Z}/p^l\mathbb{Z}$ mit $p \in \mathbb{P}$ und $l \in \mathbb{N}$. Weiter seien $k, n \in \mathbb{N}_{>1}$ und X eine n-elementige Menge, $X = \{x_1, \ldots, x_n\}$. Mit Hilfe von Bemerkung 1.28 und Satz 1.38 lassen sich dann die Resultate für Ringe der Form $(\mathbb{Z}/c\mathbb{Z})^m$ für beliebige $c, m \in \mathbb{N}$, $c \neq 1$, übertragen.

Im Fall $k = 1$ gilt $(N_{K,n,k}, *) \cong (K, +)^n$, hier ist also nichts weiter zu zeigen.

Wir wollen nun den Fall der Nilpotenzklasse $k = 2$ untersuchen. Dazu machen wir erst einige einfache Beobachtungen.

Lemma 4.1 Sei $\mathcal{G}$ eine von n Elementen erzeugte nilpotente Gruppe von der Klasse 2 und $Y = \{y_1, \ldots, y_n\}$ ein Erzeugendensystem von $\mathcal{G}$. Dann gilt

$$\mathcal{G} = \left\{ \prod_{i=1}^{n} y_i^{\alpha_i} \prod_{i=2}^{n} \prod_{j=1}^{i-1} (y_i, y_j)^{\beta_{ij}} \mid \forall i \in \underline{n}, j \in \underline{i-1} : \alpha_i, \beta_{ij} \in \mathbb{Z} \right\}.$$

Beweis. Auf Y ist eine Ordnung durch die Indizierung der Elemente gegeben. Sei $\beta : \mathcal{F}_Y \to \mathcal{G}$ die homomorphe Fortsetzung von $y \mapsto y$ für alle $y \in Y$. Dann ist $\mathfrak{E}_1^{\mathfrak{G},\beta} = (y_1, \ldots, y_n)$ das Tupel der Elementarkommutatoren in Y vom Gewicht 1 und (bei geeigneter Anordnung) $\mathfrak{E}_2^{\mathfrak{G},\beta} = ((y_2, y_1), (y_3, y_1), (y_3, y_2), (y_4, y_1), \ldots, (y_n, y_{n-1}))$ das Tupel der Elementarkommutatoren in Y vom Gewicht 2. Die Behauptung folgt aus Korollar 1.48.1. □

Bemerkung 4.2 Es gilt für alle $a, b \in N$ und alle $m \in \mathbb{N}_0$

$$a^{(m)} = ma + \binom{m}{2} a^2 \quad \text{und} \quad [a, b]_* = [a, b].$$

Außerdem ist $Z(N) = N^2$ und $\mathrm{rk}_K N = 2n + 2\binom{n}{2}$.

Beweis. Dies folgt aus Lemma 1.2 (e), Lemma 1.11 (b) und Lemma 1.30 (c). Außerdem ist $\mathrm{rk}_K N = n + n^2$ nach Korollar 1.20.2 und es gilt

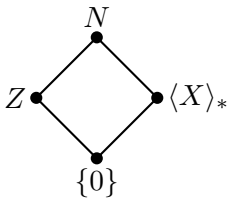
$$2n + 2\binom{n}{2} = 2n + n(n-1) = n^2 + n.$$

□

Nun wollen die Gruppe direkt zerlegen. Im Fall $K = \mathbb{Z}$ oder $p \neq 2$ können wir dies mit Hilfe von Satz 3.3 erreichen, der Fall $p = 2$ muss hingegen gesondert betrachtet werden und führt zu einer anderen Zerlegung von N.

Lemma 4.3 (a) Sei $p \neq 2$. Wir setzen

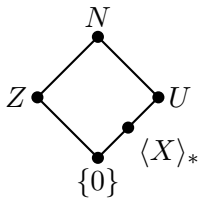
$$Z := \langle x_i x_j \mid i, j \in \underline{n}, i \leq j \rangle.$$



Dann ist $Z \leq Z(N)$, $Z \cong (K,+)^{n+\binom{n}{2}}$ und $N = Z \times \langle X \rangle_*$.

(b) Sei $K = \mathbb{Z}/2^l\mathbb{Z}$,

$$Z := \langle x_i x_j \mid i, j \in \underline{n}, i < j \rangle \quad \text{und} \quad U := \langle x_i, x_i^2 \mid i \in \underline{n} \rangle_*.$$



Dann ist $Z \leq Z(N)$, $Z \cong (K,+)^{\binom{n}{2}}$ und $N = Z \times U$.

Beweis. (a) Mit der ausführlichen Formulierung von Satz 3.3 auf Seite 72 (mit $i = 2$, $V_2 = Z$ und $M_2 = \langle X \rangle_*$) folgt $Z \cong (K,+)^{n+\binom{n}{2}}$ und $N = Z \times \langle X \rangle_*$. $Z \leq Z(N)$ folgt aus Bemerkung 4.2.
(b) $Z \leq Z(N)$ folgt aus Bemerkung 4.2. Es ist $Z^2 = \{0\}$ und damit $Z \cong (K,+)^{\binom{n}{2}}$, da die angegeben Erzeuger K-linear unabhängig sind.
Wir zeigen nun $Z * U = N$. Sei $f \in X^{\leq 2}$. Ist $f \in X$, so ist $f \in U$. Sei $f \notin X$. Dann gibt es $i, j \in \underline{n}$ mit $f = x_i x_j$.

- Ist $i < j$, so ist $f \in Z$.
- Ist $i = j$, so ist $f \in U$.
- Ist $i > j$, so ist $f = x_j x_i + [x_i, x_j] = (x_j x_i) * [x_i, x_j]_* \in Z * U$.

Also ist $X^{\leq 2} \subseteq Z * U$ und damit ist $Z * U = N$ nach Korollar 1.32.1.
Weiter gilt für alle $i, j \in \underline{n}$ mit Korollar 1.35.1, Korollar 1.34.1 und Bemerkung 1.53

$$(x_i)^{(2^{l+1})} = 0,\ (x_i^2)^{(2^l)} = 0 \quad \text{und} \quad [x_i, x_j]_*^{(2^l)} = 0. \tag{4.1}$$

Damit erhalten wir (da $(x_i)^{(2^l)} = \binom{2^l}{2} x_i^2 \in \langle x_i^2 \rangle$ und $x_i^2 \in Z(N)$) aus Lemma 4.1

$$U = \left\{ \bigstar_{i=1}^{n} (x_i)^{(\alpha_i)} \bigstar_{i=1}^{n} (x_i^2)^{(\beta_i)} \bigstar_{i=1}^{n-1} \bigstar_{j=i+1}^{n} [x_i, x_j]_*^{(\gamma_{ij})} \middle| \forall i, j \in \underline{n} :\ \alpha_i, \beta_i, \gamma_{ij} \in \underline{2^l} \right\}$$

und damit $|U| \leq \left(2^l\right)^{2n+\binom{n}{2}}$. Es folgt mit Bemerkung 4.2

$$\left(2^l\right)^{2n+2\binom{n}{2}} = |N| = |Z * U| \leq |Z| \cdot |U| \leq \left(2^l\right)^{\binom{n}{2}} \cdot \left(2^l\right)^{2n+\binom{n}{2}} = \left(2^l\right)^{2n+2\binom{n}{2}}.$$

Damit gilt überall die Gleichheit und es folgt $Z \cap U = \{0\}$, also $N = Z \times U$. □

Wir fassen die Ergebnisse für $k = 2$ zusammen:

Satz 4.4 Es gilt:

(a) Ist $K = \mathbb{Z}$ so folgt

$$(N, *) \cong (K, +)^{n+\binom{n}{2}} \times \mathcal{N}_{n,2}.$$

(b) Ist $p \neq 2$ und $K = \mathbb{Z}/p^l\mathbb{Z}$ so folgt

$$(N, *) \cong (K, +)^{n+\binom{n}{2}} \times \mathcal{N}_{n,2,(p^l,p^l)}.$$

(c) Ist $K = \mathbb{Z}/2^l\mathbb{Z}$ so folgt

$$(N, *) \cong (K, +)^{\binom{n}{2}} \times \langle a_1, \ldots, a_n, b_1, \ldots, b_n \mid \{a_i^{2^{l+1}}, b_i^{2^l}, a_i^{2^l} b_i^{2^{l-1}}, (a_i, a_j)^{2^l}, (a_i, b_j), (b_i, b_j), (a_i, a_j, a_t) \mid i, j, t \in \underline{n}\}\rangle.$$

Beweis. Im Fall (b) ist $s_{2,p} = 0$. In den Fällen (a) und (b) folgt damit aus Lemma 4.3 (a)

$$(N, *) \cong (K, +)^{n+\binom{n}{2}} \times \langle X \rangle_*$$

und damit die Behauptungen aus Satz 3.48.
(c) Sei $K = \mathbb{Z}/2^l\mathbb{Z}$ und U wie in Lemma 4.3 (b). Dann ist $N \cong (K, +)^{\binom{n}{2}} \times U$. Wir wollen also die Struktur von U untersuchen. Wir setzen

$$R := \Big\langle a_1, \ldots, a_n, b_1, \ldots, b_n \mid \{a_i^{2^{l+1}}, b_i^{2^l}, a_i^{2^l} b_i^{2^{l-1}}, (a_i, a_j)^{2^l}, (a_i, b_j), (b_i, b_j), (a_i, a_j, a_t) \mid i, j, t \in \underline{n}\}\Big\rangle.$$

Mit $N^2 = \{0\}$, (4.1) und Korollar 1.34.1 lässt sich die Abbildung $a_i \mapsto x_i$ und $b_i \mapsto x_i^2$ für alle $i \in \underline{n}$ zu einem Epimorphismus $\varphi : R \to U$ fortsetzen. Mit $a_i^{2^l} = b_i^{-2^{l-1}} \in Z(R)$ erhalten wir aus Lemma 4.1

$$R = \left\{ \prod_{i=1}^{n} a_i^{\alpha_i} \prod_{i=1}^{n} b_i^{\beta_i} \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} (a_i, a_j)^{\gamma_{ij}} \Big| \forall i, j \in \underline{n} : \alpha_i, \beta_i, \gamma_{ij} \in \underline{2^l} \right\}$$

und damit $|R| \leq \left(2^l\right)^{2n+\binom{n}{2}}$. Im Beweis zu Lemma 4.3 haben wir $|U| = |K|^{2n+\binom{n}{2}}$ gezeigt. Damit ist φ ein Isomorphismus und es folgt die Behauptung (c). □

Nachdem wir nun $(N, *)$ in dem Fall $k = 2$ für die Faktorringe von $\mathbb{Z}$ beschrieben haben, betrachten wir nun den Fall $k = 3$. Hier ist $\mathrm{ggT}(p^l, k!) = 1$ für $p \in \{2, 3\}$ nicht erfüllt, also können wir dort Satz 3.3 nicht anwenden. Wir müssen somit $p = 2$ und $p = 3$ gesondert betrachten. Bei der Zerlegung von N erhalten wir für $k = 3$ in Abhängigkeit von K drei verschiedene Zerlegungen: Eine für $K = \mathbb{Z}$ oder $K = \mathbb{Z}/p^l\mathbb{Z}$ mit $p \notin \{2, 3\}$ mit Hilfe von Satz 3.3, eine für $K = \mathbb{Z}/3^l\mathbb{Z}$ und eine für $K = \mathbb{Z}/2^l\mathbb{Z}$.

Auch im Fall der Nilpotenzklasse 3 benötigen wir die Darstellung von Gruppenelementen in nilpotenten Gruppen der Klasse 3 mittels Elementarkommutatoren.

Lemma 4.5 Es sei $\mathcal{G}$ eine endlich erzeugte nilpotente Gruppe von der Klasse 3 und $Y = \{y_1, \ldots, y_n\}$ ein (gemäß der Indizes geordnetes) Erzeugendensystem von $\mathcal{G}$. Dann gilt

$$\mathcal{G} = \left\{ \prod_{i=1}^{n} y_i^{\alpha_i} \prod_{i>j} (y_i, y_j)^{\beta_{ij}} \prod_{i>j\leq l} (y_i, y_j, y_l)^{\gamma_{ijl}} \mid \forall i,j,l \in \underline{n} : \alpha_i, \beta_{ij}, \gamma_{ijl} \in \mathbb{Z} \right\}.^{11}$$

Insbesondere gibt es $n_1 = n$ Elementarkommutatoren vom Gewicht 1, $n_2 = \binom{n}{2}$ Elementarkommutatoren vom Gewicht 2 und $n_3 = 2\binom{n}{2} + 2\binom{n}{3}$ Elementarkommutatoren vom Gewicht 3.

Beweis. Die Darstellung folgt aus Korollar 1.48.1 und nach Satz 1.44 gilt

$$\begin{aligned} n_1 &= n, \\ n_2 &= \frac{1}{2}\left(n^2 - n\right) = \frac{n(n-1)}{2} = \binom{n}{2} \quad \text{und} \\ n_3 &= \frac{1}{3}\left(n^3 - n\right) = \frac{2}{6}n^3 + \left(-\frac{6}{6} + \frac{2}{2}\right)n^2 + \left(\frac{4}{6} - \frac{2}{2}\right)n \\ &= 2\frac{n(n-1)(n-2)}{6} + 2\frac{n(n-1)}{2} = 2\binom{n}{3} + 2\binom{n}{2}. \end{aligned}$$

□

Bemerkung 4.6 Es gilt für alle $a, b, c \in N$ und alle $m \in \mathbb{N}_0$

$$\begin{aligned} a^{(m)} &= ma + \binom{m}{2}a^2 + \binom{m}{3}a^3, \\ [a,b]_* &= [a,b] + [ab,a] + [b,ba] \quad \text{und} \\ [a,b,c]_* &= [a,b,c]. \end{aligned}$$

Außerdem ist $Z(N) = N^3$ und $\mathrm{rk}_K N = 3n + 8\binom{n}{2} + 6\binom{n}{3}$.

Beweis. Dies folgt wie in Bemerkung 4.2 mit

$$\begin{aligned} 3n + 8\binom{n}{2} + 6\binom{n}{3} &= 3n + 8\frac{n(n-1)}{2} + 6\frac{n(n-1)(n-2)}{6} \\ &= 3n + 4n^2 - 4n + n^3 - 3n^2 + 2n \\ &= n^3 + n^2 + n. \end{aligned}$$

□

Zunächst betrachten wir den Fall $K = \mathbb{Z}$ oder $K = \mathbb{Z}/p^l\mathbb{Z}$ mit $p \notin \{2, 3\}$.

[11] In einer nilpotenten Gruppe der Klasse 3 ist die Kommutatorgruppe abelsch. Daher ist es nicht notwendig, bei den beiden hinteren Produkten eine Reihenfolge anzugeben.

Lemma 4.7 Sei $K = \mathbb{Z}$ oder $K = \mathbb{Z}/p^l\mathbb{Z}$ mit $p \in \mathbb{P} \setminus \{2, 3\}$. Sei R ein Repräsentantensystem der Assoziiertenklassen der Länge mindestens zwei in $X^{\leq 3}$,

$$V := \langle R \rangle \quad \text{und} \quad U := \langle X \rangle_* * C.$$

Dann ist $V \cong (K, +)^{2n+3\binom{n}{2}+\binom{n}{3}}$ und $N = V \ltimes U$.

Beweis. Dies folgt aus dem Beweis zu Satz 3.3 mit

$$\begin{aligned}\binom{n+3}{n} - \binom{n+1}{n} &= \binom{n+3}{3} - (n+1) \\ &= \sum_{i=0}^{3} \binom{n}{i}\binom{3}{3-i} - (n+1) \\ &= \binom{n}{3} + 3\binom{n}{2} + 3n + 1 - (n+1) \\ &= \binom{n}{3} + 3\binom{n}{2} + 2n.\end{aligned}$$

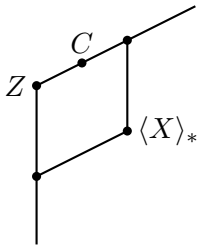
□

Unser Ziel ist es, U als direktes Produkt zweier Untergruppen zu beschreiben. Das folgende Lemma gilt für jeden echten Faktorring von $\mathbb{Z}$:

Lemma 4.8 Sei $K = \mathbb{Z}/c\mathbb{Z}$ für ein $c \in \mathbb{N}_{>1}$ und

$$\begin{aligned}Z := \langle &[x_ix_j, x_i], [x_ix_j, x_j] \mid i, j \in \underline{n}, i < j\rangle\oplus \\ &\langle x_ix_jx_l - x_ix_lx_j, [x_ix_j, x_l], [x_ix_l, x_j] \mid i, j, l \in \underline{n}, i < j < l\rangle.\end{aligned}$$

Dann gilt $Z \cong (K, +)^{2\binom{n}{2}+3\binom{n}{3}}$, $Z \subseteq C$ und $C \subseteq \langle X \rangle_* * Z$.



Beweis. Da $Z \leq N^3 = Z(N)$, ist $Z^2 = \{0\}$ und damit $Z \cong (K, +)^{2\binom{n}{2}+3\binom{n}{3}}$, da die angegebenen Erzeuger linear unabhängig sind. Außerdem liegen alle diese Erzeuger in C, also ist $Z \subseteq C$ und es ist $\langle X \rangle_* * Z$ eine Untergruppe von N. Weiter ist

$$\begin{aligned}B := &\{x_ix_jx_l - g \mid i, j, l \in \underline{n}, i < j < l, g \sim x_ix_jx_l\} \\ &\cup \{x_i^2x_j - g \mid i, j, l \in \underline{n}, i < j, g \sim x_i^2x_j\} \\ &\cup \{x_ix_j^2 - g \mid i, j, l \in \underline{n}, i < j, g \sim x_ix_j^2\} \\ &\cup \{[x_i, x_j] \mid i, j \in \underline{n}, i < j\}\end{aligned}$$

nach Wahl von K ein additives Erzeugendensystem von C. Damit genügt es nach Lemma 1.32 also $B \subseteq \langle X \rangle_* * Z$ nachzuweisen.
Seien $i, j \in \underline{n}$ mit $i < j$, o.B.d.A. $i = 1$ und $j = 2$. Sei $f := x_1^2x_2$ und $g \sim f$. Dann gilt:

- Falls $g = f$:

$$f - g = 0 \in \langle X \rangle_* * Z.$$

- Falls $g = x_1x_2x_1$:

$$f - g = [x_1, x_1x_2] = [x_1x_2, x_1]^- \in Z \subseteq \langle X \rangle_* * Z.$$

- Falls $g = x_2x_1^2$:

$$f - g = [x_1, x_2, x_1] - 2[x_1x_2, x_1] = [x_1, x_2, x_1]_* * [x_1x_2, x_1]^{(-2)} \in \langle X \rangle_* * Z.$$

Seien $i, j \in \underline{n}$ mit $i < j$, o.B.d.A. $i = 1$ und $j = 2$. Sei $f := x_1x_2^2$ und $g \sim f$. Dann gilt:

- Falls $g = f$:

$$f - g = 0 \in \langle X \rangle_* * Z.$$

- Falls $g = x_2x_1x_2$:

$$f - g = [x_1x_2, x_2] \in Z \subseteq \langle X \rangle_* * Z.$$

- Falls $g = x_2^2x_1$:

$$f - g = -[x_1, x_2, x_2] + 2[x_1x_2, x_2] = [x_1, x_2, x_2]_*^- * [x_1x_2, x_2]^{(2)} \in \langle X \rangle_* * Z.$$

Seien $i, j, l \in \underline{n}$ mit $i < j < l$, o.B.d.A. $i = 1$, $j = 2$ und $l = 3$. Sei $f := x_1x_2x_3$ und $g \sim f$. Dann gilt:

- Falls $g = f$:

$$f - g = 0 \in \langle X \rangle_* * Z.$$

- Falls $g = x_1x_3x_2$:

$$f - g = x_1x_2x_3 - x_1x_3x_2 \in Z \subseteq \langle X \rangle_* * Z.$$

- Falls $g = x_2x_1x_3$:

$$f - g = (x_1x_2x_3 - x_1x_3x_2) + [x_1x_3, x_2] \in Z \subseteq \langle X \rangle_* * Z.$$

- Falls $g = x_2x_3x_1$:

$$\begin{aligned} f - g &= -[x_1, x_3, x_2] + [x_1x_2, x_3] + [x_1x_3, x_2] \\ &= [x_1, x_3, x_2]_*^- * ([x_1x_2, x_3] + [x_1x_3, x_2]) \in \langle X \rangle_* * Z. \end{aligned}$$

- Falls $g = x_3x_1x_2$:

$$f - g = [x_1x_2, x_3] \in Z \subseteq \langle X \rangle_* * Z.$$

- Falls $g = x_3x_2x_1$:

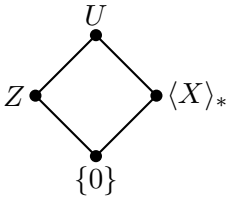
$$\begin{aligned} f - g &= -[x_1, x_2, x_3] + (x_1x_2x_3 - x_1x_3x_2) + [x_1x_2, x_3] + [x_1x_3, x_2] \\ &= [x_1, x_2, x_3]_*^- * ((x_1x_2x_3 - x_1x_3x_2) + [x_1x_2, x_3] + [x_1x_3, x_2]) \in \langle X \rangle_* * Z. \end{aligned}$$

Damit haben wir bereits $C \cap N^3 \subseteq \langle X\rangle_* * Z$ gezeigt. Seien nun $i,j \in \underline{n}$. Dann gilt

$$\begin{aligned}[x_i,x_j] &= [x_i,x_j]_* + [x_i, x_ix_j] + [x_jx_i, x_j]\\ &= [x_i,x_j]_* * \underbrace{([x_i,x_ix_j] + [x_jx_i,x_j])}_{\in C\cap N^3} \in \langle X\rangle_* * Z.\end{aligned}$$

Somit folgt $C \subseteq \langle X\rangle_* * Z$. □

Lemma 4.9 Sei $K = \mathbb{Z}$ oder $K = \mathbb{Z}/p^l\mathbb{Z}$ mit $p \in \mathbb{P}\setminus\{2,3\}$. Sei



$$\begin{aligned}U &= \langle X\rangle_* * C \quad \text{wie in Lemma 4.7 und}\\ Z &= \langle [x_ix_j,x_i],[x_ix_j,x_j] \mid i,j\in\underline{n}, i<j\rangle \oplus\\ &\quad \langle x_ix_jx_l - x_ix_lx_j, [x_ix_j,x_l],[x_ix_l,x_j] \mid i,j,l\in\underline{n}, i<j<l\rangle\end{aligned}$$

wie in Lemma 4.8. Dann gilt $U = \langle X\rangle_* \times Z$.

Beweis. Wir müssen zeigen, dass $\langle X\rangle_* * Z = U$ und $\langle X\rangle_* \cap Z = \{0\}$ gilt.
Für $\langle X\rangle_* * Z = U$ genügt es (wegen $Z \subseteq C$ und nach Definition von U) $C \subseteq \langle X\rangle_* * Z$ nachzuweisen und dies ist nach Lemma 4.8 erfüllt.
Um $\langle X\rangle_* \cap Z = \{0\}$ zu zeigen, berechnen wir obere Schranken für $\mathrm{rk}_K(\langle X\rangle_* \cap N^3)$, $\mathrm{rk}_K Z$ und $\mathrm{rk}_K C \cap N^3$. Außerdem zeigen wir $C \cap N^3 = (\langle X\rangle_* \cap N^3) * Z$ und folgern daraus $|\langle X\rangle_* \cap Z| = 1$, also $\langle X\rangle_* \cap Z = \{0\}$.
Nach Satz 3.48 gilt $\langle X\rangle_* \cong \mathcal{N}_{n,3}$ oder $\langle X\rangle_* \cong \mathcal{N}_{n,3,(p^l,p^l,p^l)}$. Sei $O := \mathbb{Z}$ falls $K = \mathbb{Z}$ und $O := \underline{p^l - 1}_0$ falls $K = \mathbb{Z}/p^l\mathbb{Z}$. Dann gilt nach Satz 3.48

$$\langle X\rangle_* = \left\{ \bigstar_{i=1}^{n} x_i^{(\alpha_i)} \bigstar_{i>j} [x_i,x_j]_*^{(\beta_{ij})} \bigstar_{i>j\le l} [x_i,x_j,x_l]_*^{(\gamma_{ijl})} \,\middle|\, \forall i,j,l\in\underline{n}\colon\ \alpha_i,\beta_{ij},\gamma_{ijl}\in O \right\}.$$

Sei nun $a \in \langle X\rangle_* \cap N^2$, $\alpha_i,\beta_{ij},\gamma_{ijl} \in O$ für alle $i,j,l \in \underline{n}$ mit

$$a = \bigstar_{i=1}^{n} x_i^{(\alpha_i)} \bigstar_{i>j} [x_i,x_j]_*^{(\beta_{ij})} \bigstar_{i>j\le l} (x_i,x_j,x_l)^{(\gamma_{ijl})}.$$

Dann folgt

$$0 = a\pi_1 = \left(\bigstar_{i=1}^{n} x_i^{(\alpha_i)}\right)\pi_1 = \sum_{i=1}^{n} \alpha_i x_i,$$

also $\alpha_1 = \cdots = \alpha_n = 0$, und falls $a \in N^3$

$$0 = a\pi_2 = \left(\bigstar_{i>j} [x_i,x_j]_*^{(\beta_{ij})}\right)\pi_2 = \sum_{i>j} \beta_{ij}[x_i,x_j],$$

also $\beta_{ij} = 0$ für alle $i,j \in \underline{n}$ mit $i > j$. Damit folgt

$$\begin{aligned}\langle X\rangle_* \cap N^2 &= \left\{ \bigstar_{i>j} [x_i,x_j]_*^{(\beta_{ij})} \bigstar_{i>j\le l} [x_i,x_j,x_l]_*^{(\gamma_{ijl})} \mid \forall i,j,l\in\underline{n}\colon\ \beta_{ij},\gamma_{ijl}\in O \right\}\\ \langle X\rangle_* \cap N^3 &= \left\{ \bigstar_{i>j\le l} [x_i,x_j,x_l]_*^{(\gamma_{ijl})} \mid \forall i,j,l\in\underline{n}\colon\ \gamma_{ijl}\in O \right\}\\ &= \langle [x_i,x_j,x_l] \mid i,j,l\in\underline{n}, i>j\le l\rangle_K\end{aligned}$$

und somit

$$\langle X\rangle_* \cap N^3 \subseteq \langle X\rangle_* \cap N^2 \subseteq N' \overset{3.6(b)}{\subseteq} C$$

sowie $\mathrm{rk}_K(\langle X\rangle_* \cap N^3) \leq n_3$.
Ist nun $u \in U \cap N^3$, etwa $u = a * c$ mit $a \in \langle X\rangle_*$ und $c \in C$, so ist $a^- * u = c \in C \subseteq N^2$, also $a \in \langle X\rangle_* \cap N^2$ und damit $a \in C$, also $u \in C \cap N^3$. Damit ist $C \cap N^3 = U \cap N^3$ und es folgt

$$C \cap N^3 = U \cap N^3 = (\langle X\rangle_* * Z) \cap N^3 \overset{\text{Dedekind-Id.}}{=} (\langle X\rangle_* \cap N^3) * Z. \tag{4.2}$$

Es sind $C \cap N^3$, $\langle X\rangle_* \cap N^3$ und Z freie K-Moduln mit

$$\begin{aligned}
\mathrm{rk}_K(C \cap N^3) &= \sum_{M \in X^{\overline{=}3}_{\sim}} (|M| - 1) \\
&= \sum_{i,j \in \underline{n}, i<j} \big((|[x_i^2 x_j]_\sim| - 1) + (|[x_i x_j^2]_\sim| - 1)\big) + \sum_{i,j,l \in \underline{n}, i<j<l} (|[x_i x_j x_l]_\sim| - 1) \\
&= 4\binom{n}{2} + 5\binom{n}{3}, \\
\mathrm{rk}_K Z &= 2\binom{n}{2} + 3\binom{n}{3} \text{ nach Lemma 4.8 und} \\
\mathrm{rk}_K(\langle X\rangle_* \cap N^3) &\leq n_3 \overset{4.5}{=} 2\binom{n}{2} + 2\binom{n}{3}.
\end{aligned}$$

Es folgt mit (4.2)[12]

$$\begin{aligned}
4\binom{n}{2} + 5\binom{n}{3} &= \mathrm{rk}_K(C \cap N^3) \leq \mathrm{rk}_K Z + \mathrm{rk}_K(\langle X\rangle_* \cap N^3) \\
&\leq 2\binom{n}{2} + 3\binom{n}{3} + 2\binom{n}{2} + 2\binom{n}{3} = 4\binom{n}{2} + 5\binom{n}{3}.
\end{aligned}$$

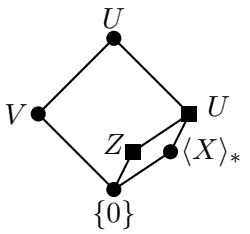
Damit muss überall die Gleichheit gelten und somit folgt

$$\langle X\rangle_* \cap Z = \langle X\rangle_* \cap N^3 \cap Z = \{0\},$$

also gilt die Behauptung. □

Nun haben wir im Fall $K = \mathbb{Z}$ oder $K = \mathbb{Z}/p^l\mathbb{Z}$ mit $p > 3$ die Gruppe $(N, *)$ zerlegt in

$$N = V \ltimes U = V \ltimes (Z \times \langle X\rangle_*).$$

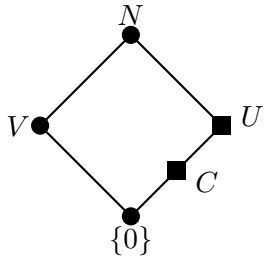


Wir wollen nun die Fälle $p = 2$ und $p = 3$ betrachten. Der große Unterschied zu den Vorherigen ist, dass $x^{|K|} \neq 0$ gilt, also $\langle X\rangle_*$ eine größere Untergruppe wird.

[12] Ist $K = \mathbb{Z}$, so ist $\mathrm{rk}(S+T) = \mathrm{rk}S + \mathrm{rk}T - \mathrm{rk}(S \cap T)$ in frei abelschen Gruppen. Ist K endlich, so folgt dies aus $|S+T| = \frac{|S|\cdot|T|}{|S\cap T|}$.

Lemma 4.10 Sei $p \in \{2,3\}$ und $K = \mathbb{Z}/p^l\mathbb{Z}$. Sei R ein Repräsentantensystem der Assoziiertenklassen von $X^{\leq 3}$ und $\tilde{R} := R \setminus \{x, x^p \mid x \in X\}$. Für alle $j \in \underline{n}$ setzen wir $y_j := x_j^{(p)} * (x_j^p)^-$. Es sei

$$V := \langle \tilde{R} \rangle \quad \text{und}$$
$$U := \langle x_i, y_i \mid i \in \underline{n} \rangle_* * C.$$



Dann ist $V \cong (K,+)^{n+3\binom{n}{2}+\binom{n}{3}}$ und $N = V \ltimes U$.

Beweis. Es ist $\tilde{R} \subseteq N^2$ und damit $\tilde{R}^2 = \{0\}$. Die Elemente von $\tilde{R}$ sind linear unabhängig. Damit folgt $V \cong (K,+)^{|\tilde{R}|}$. Es ist

$$\begin{aligned}
|\tilde{R}| &= \left|\{x_i^2 \mid i \in \underline{n}\}\right| + |\{x_i x_j \mid i,j \in \underline{n}, i<j\}| + \left|\{x_i^3 \mid i \in \underline{n}\}\right| \\
&\quad + \left|\{x_i^2 x_j \mid i,j \in \underline{n}, i<j\}\right| + \left|\{x_i x_j^2 \mid i,j \in \underline{n}, i<j\}\right| \\
&\quad + |\{x_i x_j x_l \mid i,j,l \in \underline{n}, i<j<l\}| - |\{x_i^p \mid i \in \underline{n}\}| \\
&= n + \binom{n}{2} + n + \binom{n}{2} + \binom{n}{2} + \binom{n}{3} - n \\
&= n + 3\binom{n}{2} + \binom{n}{3}.
\end{aligned}$$

Damit ist $V \cong (K,+)^{n+3\binom{n}{2}+\binom{n}{3}}$.
Für $N = V * U$ genügt es $X^{\leq 3} \subseteq V * U$ nach Korollar 1.32.1 nachzuweisen. Sei also $f \in X^{\leq 3}$.

- Sei $f \in X^{=3}$. Ist $f = x_i^3$ für ein $i \in \underline{n}$, so ist $f \in \tilde{R} \subseteq V$ für $p = 2$ und
$$f = x_i^3 = (x_i^{(3)} * (x_i^3)^-)^- * x_i^{(3)} = y_i^- * x_i^{(3)} \in U$$
für $p = 3$. Ist $f \neq x_i^3$ für alle $i \in \underline{n}$, so existiert $g \in \tilde{R}$ mit $f \sim g$. Dann ist $f - g \in C \subseteq U$ und damit $f = g + f - g = g * (f - g) \in V * U$.
- Sei $f \in X^{=2}$. Ist $f = x_i^2$ für ein $i \in \underline{n}$, so ist $f \in \tilde{R} \subseteq V$ für $p = 3$ und
$$f = x_i^2 = (x_i^{(2)} * (x_i^2)^-)^- * x_i^{(2)} = y_i^- * x_i^{(2)} \in U$$
für $p = 2$. Ist $f \neq x_i^2$ für alle $i \in \underline{n}$, so existiert $g \in \tilde{R}$ mit $f \sim g$. Dann ist $f - g \in C \subseteq U$ und damit $f = g + f - g = g * (f - g) \in V * U$.
- Ist $f \in X$, so ist $f \in U$.

Damit ist $X^{\leq 3} \subseteq V * U$, also $N = V * U$.
Nach Lemma 3.6 ist $N' \subseteq C \subseteq U$ und damit $U \trianglelefteq N$.
Wir wollen nun $|U|$ und $|V|$ abschätzen, um $V \cap U = \{0\}$ zu beweisen. Dabei haben wir $|V| = p^{l\left(n+3\binom{n}{2}+\binom{n}{3}\right)}$ bereits gezeigt.
Wir setzen $U_1 := \langle X \rangle_* * C$. Nach Korollar 1.35.1 ist $o(x) = p^{l+1}$ für alle $x \in X$, da $1 \in I_{3,p,1}$ ist. Da $N' \subseteq C$ gilt mit Lemma 4.5

$$U_1 = \underbrace{\left\{ \bigstar_{i=1}^{n} x_i^{(\alpha_i)} \,\middle|\, \alpha_1, \ldots, \alpha_n \in \underline{p^{l+1}} \right\}}_{=:M} * C$$

und damit $|U_1| \leq |M| \cdot |C|$. Es ist

$$\begin{aligned} B := &\left\{x_i x_j - x_j x_i \mid i,j \in \underline{n}, i<j\right\} \cup \left\{x_i^2 x_j - x_i x_j x_i, x_i^2 x_j - x_j x_i^2 \mid i,j \in \underline{n}, i \neq j\right\} \\ &\cup \left\{x_i x_j x_l - x_i x_l x_j, x_i x_j x_l - x_j x_l x_i, x_i x_j x_l - x_j x_i x_l, x_i x_j x_l - x_l x_i x_j,\right. \\ &\qquad \left. x_i x_j x_l - x_l x_j x_i \mid i,j,l \in \underline{n}, i<j<l\right\} \end{aligned}$$

eine K-Basis von C und damit

$$|C| = |K|^{\mathrm{rk}_K C} = \left(p^l\right)^{|B|} = \left(p^l\right)^{\binom{n}{2}+4\binom{n}{2}+5\binom{n}{3}} = \left(p^l\right)^{5\binom{n}{2}+5\binom{n}{3}}.$$

Damit ist

$$|U_1| \leq |M| \cdot |C| \leq \left(p^{l+1}\right)^n \left(p^l\right)^{5\binom{n}{2}+5\binom{n}{3}}.$$

Weiter gilt für alle $i \in \underline{n}$ und alle $u \in U_1$

$$\begin{aligned} (y_i)^- * u * y_i &= x_i^p * \underbrace{x_i^{(-p)} * u * x_i^{(p)}}_{=:\tilde{u} \in U_1, \text{ da } x_i \in U_1} *(x_i^p)^- \\ &= \tilde{u} + x_i^p \tilde{u} + \tilde{u}(x_i^p)^- \\ &= \tilde{u} + x_i^p \tilde{u} - \tilde{u} x_i^p \\ &= \tilde{u} * \underbrace{[x_i^p, \tilde{u}]_*}_{\in N' \subseteq C} \in U_1, \end{aligned}$$

also ist y_i ein Element des Normalisators von U_1. Damit ist $\langle y_i \mid i \in \underline{n}\rangle_* * U_1$ eine Untergruppe von N und damit gilt $\langle y_i \mid i \in \underline{n}\rangle_* * U_1 = U$. Nach Korollar 1.34.1 ist $o(y_i) = p^{l-1}$ für alle $i \in \underline{n}$. Da $N' \subseteq C$ ist, gilt erneut mit Lemma 4.5

$$U = \underbrace{\left\{ \bigstar_{i=1}^{n} y_i^{(\alpha_i)} \middle| \alpha_1, \ldots, \alpha_n \in \underline{p^{l-1}} \right\}}_{=:L} * U_1.$$

Wir erhalten mit Bemerkung 4.6

$$\begin{aligned} |N| &= |V * U| \\ &\leq |V| \cdot |U| \\ &\leq |V| \cdot |L| \cdot |U_1| \\ &\leq \left(p^l\right)^{(n+3\binom{n}{2}+\binom{n}{3})} \left(p^{l-1}\right)^n \left(p^{l+1}\right)^n \left(p^l\right)^{5\binom{n}{2}+5\binom{n}{3}} \\ &= \left(p^l\right)^{3n+8\binom{n}{2}+6\binom{n}{3}} \\ &= |N|. \end{aligned}$$

Damit gilt überall Gleichheit und somit $U \cap V = \{0\}$. □

Korollar 4.10.1 Aus dem Beweis von Lemma 4.10 folgt $|U| = \left(p^l\right)^{2n+5\binom{n}{2}+5\binom{n}{3}}$.

Bemerkung 4.11 In den Lemmata 4.9 und 4.10 ist die Operation von V auf U gegeben durch

$$u^{(v)} = u + [u, v] \quad \text{für alle } u \in U \text{ und alle } v \in V.$$

Beweis. Sei $u \in U$ und $v \in V$. Dann ist $v \in N^2$ und damit gilt

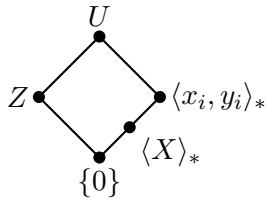
$$\begin{aligned} u^{(v)} &= v^- * u * v \\ &= v^- + u + v + v^-u + v^-v + uv + v^-uv \\ &= u + v^-u + uv \\ &= u + uv - vu = u + [u, v]. \end{aligned}$$

□

Wir wollen nun auch im Fall der Primzahlen $p = 2$ und $p = 3$ untersuchen, ob der semidirekte Faktor U aus Lemma 4.10 zerfällt. Dazu betrachten wir zunächst den Fall $p = 3$.

Bemerkung 4.12 Sei $K = \mathbb{Z}/3^l\mathbb{Z}$, $y_i := x_i^{(3)} * (x_i^3)^-$ für alle $i \in \underline{n}$,

$$\begin{aligned} U &= \langle x_i, y_i \mid i \in \underline{n} \rangle_* * C \quad \text{wie in Lemma 4.10 und} \\ Z &= \langle [x_ix_j, x_i], [x_ix_j, x_j] \mid i, j \in \underline{n}, i < j \rangle \oplus \\ &\quad \langle x_ix_jx_l - x_ix_lx_j, [x_ix_j, x_l], [x_ix_l, x_j] \mid i, j, l \in \underline{n}, i < j < l \rangle \end{aligned}$$



wie in Lemma 4.8. Dann ist $Z \cong (K, +)^{2\binom{n}{2}+3\binom{n}{3}}$ und $U = \langle x_i, y_i \mid i \in \underline{n} \rangle_* \times Z$.

Beweis. Der erste Teil der Behauptung folgt direkt aus Lemma 4.8. Außerdem ist $Z \subseteq C$ und damit

$$\begin{aligned} U = \langle x_i, y_i \mid i \in \underline{n} \rangle_* * C &\overset{4.8}{\subseteq} \langle x_i, y_i \mid i \in \underline{n} \rangle_* * \langle X \rangle_* * Z \\ = \langle x_i, y_i \mid i \in \underline{n} \rangle_* * Z &\subseteq \langle x_i, y_i \mid i \in \underline{n} \rangle_* * C = U. \end{aligned}$$

Damit ist $U = \langle x_i, y_i \mid i \in \underline{n} \rangle_* * Z$. Mit der Definition der y_i folgt

$$\langle x_i, y_i \mid i \in \underline{n} \rangle_* = \langle x_i, x_i^3 \mid i \in \underline{n} \rangle_*.$$

Wir setzen $W := \langle x_i^3 \mid i \in \underline{n} \rangle \leq Z(N)$. Dann ist $\langle x_i, y_i \mid i \in \underline{n} \rangle_* = \langle X \rangle_* * W$. Für alle $i \in \underline{n}$ ist $3^{l-1}x_i^3 = \binom{3^l}{3}x_i^3 = x_i^{(3^l)} \in \langle X \rangle_*$ mit Lemma 1.15 und damit

$$|\langle x_i, y_i \mid i \in \underline{n} \rangle_* / \langle X \rangle_*| = |\langle X \rangle_* * W / \langle X \rangle_*| \leq \left(3^{l-1}\right)^n.$$

Außerdem ist mit Satz 3.48, Bemerkung 1.53 und Lemma 4.5

$$|\langle X \rangle_*| = \left(3^{l+1}\right)^{n_1} \left(3^l\right)^{n_2+n_3} = \left(3^{l+1}\right)^n \left(3^l\right)^{3\binom{n}{2}+2\binom{n}{3}}.$$

Es folgt insgesamt mit Korollar 4.10.1

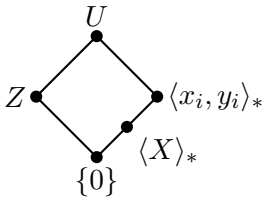
$$\begin{aligned}\left(3^l\right)^{2n+5\binom{n}{2}+5\binom{n}{3}} &= |U| = |\langle x_i, y_i \mid i \in \underline{n}\rangle_* * Z| \\ &\leq |\langle x_i, y_i \mid i \in \underline{n}\rangle_*| \cdot |Z| \\ &= |\langle x_i, y_i \mid i \in \underline{n}\rangle_*/\langle X\rangle_*| \cdot |\langle X\rangle_*| \cdot |Z| \\ &\leq \left(3^{l-1}\right)^n \left(3^{l+1}\right)^n \left(3^l\right)^{3\binom{n}{2}+2\binom{n}{3}} \left(3^l\right)^{2\binom{n}{2}+3\binom{n}{3}} \\ &= \left(3^l\right)^{2n+5\binom{n}{2}+5\binom{n}{3}}.\end{aligned}$$

Damit folgt $\langle x_i, y_i \mid i \in \underline{n}\rangle_* \cap Z = \{0\}$ und mit $Z \subseteq N^3 = Z(N)$ folgt die Behauptung. □

Abschließend betrachten wir den Fall $p = 2$.

Bemerkung 4.13 Sei $K = \mathbb{Z}/2^l\mathbb{Z}$, $y_i := x_i^{(2)} * (x_i^2)^-$ für alle $i \in \underline{n}$,

$$\begin{aligned}U &= \langle x_i, y_i \mid i \in \underline{n}\rangle_* * C \quad \text{wie in Lemma 4.10 und} \\ Z &:= \langle x_i x_j x_l - x_i x_l x_j, [x_i x_j, x_l], [x_i x_l, x_j] \\ &\qquad \mid i, j, l \in \underline{n}, i < j < l\rangle.\end{aligned}$$



Dann ist $Z \cong (K, +)^{3\binom{n}{3}}$ und

$$U = \langle x_i, y_i, [x_i, x_i x_j] \mid i, j \in \underline{n}\rangle_* \times Z.$$

Beweis. Der erste Teil der Behauptung folgt aus $Z \subseteq N^3$, da die angegebenen Erzeuger K-linear unabhängig sind.
Wir setzen $S := \langle x_i, y_i, [x_i, x_i x_j] \mid i, j \in \underline{n}\rangle_*$. Dann ist $S = \langle x_i, x_i^2, [x_i, x_i x_j] \mid i, j \in \underline{n}\rangle_*$ nach der Definition der y_i. Wir zeigen zunächst $S * Z = U$. Mit $S, Z \subseteq U$ und $x_i, y_i \in S$ für alle $i \in \underline{n}$ genügt es, $C \subseteq S * Z$ nachzuweisen. Wir orientieren uns an dem Vorgehen in Lemma 4.8. Es ist

$$\begin{aligned}B := \left\{x_i x_j x_l - g \mid i, j, l \in \underline{n}, i < j < l, g \sim x_i x_j x_l\right\} \\ \cup \left\{x_i^2 x_j - g \mid i, j \in \underline{n}, i < j, g \sim x_i^2 x_j\right\} \\ \cup \left\{x_i x_j^2 - g \mid i, j \in \underline{n}, i < j, g \sim x_i x_j^2\right\} \\ \cup \left\{[x_i, x_j] \mid i, j \in \underline{n}, i < j\right\}\end{aligned}$$

ein additives Erzeugendensystem von C. Damit genügt es $B \subseteq S * Z$ nach Lemma 1.32 nachzuweisen.
Seien $i, j \in \underline{n}$ mit $i < j$, o.B.d.A. $i = 1$ und $j = 2$. Sei $f := x_1^2 x_2$ und $g \sim f$. Dann gilt:

- Falls $g = f$:

$$f - g = 0 \in S * Z.$$

- Falls $g = x_1 x_2 x_1$:

$$f - g = [x_1, x_1 x_2] \in S \subseteq S * Z.$$

- Falls $g = x_2x_1^2$:

$$f - g = [x_1^2, x_2] = [y_1^- * x_1^{(2)}, x_2]_* \in S \subseteq S * Z.$$

Seien $i, j \in \underline{n}$ mit $i < j$, o.B.d.A. $i = 1$ und $j = 2$. Sei $f := x_1x_2^2$ und $g \sim f$. Dann gilt:

- Falls $g = f$:

$$f - g = 0 \in S * Z.$$

- Falls $g = x_2x_1x_2$:

$$f - g = [x_1x_2, x_2] = -[x_2^2, x_1] + [x_2, x_2x_1] = [y_2^- * x_2^{(2)}, x_1]_*^- * [x_2, x_2x_1] \in S \subseteq S * Z.$$

- Falls $g = x_2^2x_1$:

$$f - g = [x_1, x_2^2] = [x_1, y_2^- * x_2^{(2)}]_* \in S \subseteq S * Z.$$

Seien $i, j, l \in \underline{n}$ mit $i < j < l$, o.B.d.A. $i = 1$, $j = 2$ und $l = 3$. Sei $f := x_1x_2x_3$ und $g \sim f$. Dann gilt:

- Falls $g = f$:

$$f - g = 0 \in S * Z.$$

- Falls $g = x_1x_3x_2$:

$$f - g = x_1x_2x_3 - x_1x_3x_2 \in Z \subseteq S * Z.$$

- Falls $g = x_2x_1x_3$:

$$f - g = (x_1x_2x_3 - x_1x_3x_2) + [x_1x_3, x_2] \in Z \subseteq S * Z.$$

- Falls $g = x_2x_3x_1$:

$$\begin{aligned} f - g &= -[x_1, x_3, x_2] + [x_1x_2, x_3] + [x_1x_3, x_2] \\ &= [x_1, x_3, x_2]_*^- * ([x_1x_2, x_3] + [x_1x_3, x_2]) \in S * Z. \end{aligned}$$

- Falls $g = x_3x_1x_2$:

$$f - g = [x_1x_2, x_3] \in Z \subseteq S * Z.$$

- Falls $g = x_3x_2x_1$:

$$\begin{aligned} f - g &= -[x_1, x_2, x_3] + (x_1x_2x_3 - x_1x_3x_2) + [x_1x_2, x_3] + [x_1x_3, x_2] \\ &= [x_1, x_2, x_3]_*^- * ((x_1x_2x_3 - x_1x_3x_2) + [x_1x_2, x_3] + [x_1x_3, x_2]) \in S * Z. \end{aligned}$$

Damit haben wir bereits $C \cap N^3 \subseteq S * Z$ gezeigt. Seien nun $i, j \in \underline{n}$. Dann gilt

$$[x_i, x_j] \overset{4.6}{=} [x_i, x_j]_* + \underbrace{[x_i x_j, x_i] + [x_j, x_j x_i]}_{\in C \cap N^3} \in S * Z.$$

Also ist $C \subseteq S * Z$ und damit $S * Z = U$.
Sei $S_1 := \langle x_i, [x_i, x_i x_j], [x_i^2, x_j] \mid i, j \in \underline{n} \rangle_*$. Es sind $[x_i, x_i x_j], [x_i^2, x_j] \in Z(N)$ für alle $i, j \in \underline{n}$ und es gilt

$$\begin{aligned} x_i^{(y_j)} &= (x_j^{(2)} * (x_j^2)^-)^- * x_i * (x_j^{(2)} * (x_j^2)^-) \\ &= (x_j^2) * \underbrace{x_j^{(-2)} * x_i * x_j^{(2)}}_{=:s \in S_1} * (x_j^2)^- \\ &= s + [x_j^2, s] \\ &= s * [x_j^2, s\pi_1] \\ &= s * [x_j^2, x_i] \in S_1. \end{aligned}$$

Damit ist y_j für alle $j \in \underline{n}$ im Normalisator von S_1 enthalten. Also ist $S_1 * \langle y_i \mid i \in \underline{n} \rangle_*$ eine Untergruppe es folgt $S = S_1 * \langle y_i \mid i \in \underline{n} \rangle_*$.
Sei $S_2 := \langle [x_i, x_i x_j], [x_i^2, x_j] \mid i, j \in \underline{n} \rangle$. Dann ist $S_2 \subseteq Z(N)$ und damit $S_1 = \langle X \rangle_* * S_2$. Außerdem ist für alle $i, j \in \underline{n}$

$$\begin{aligned} [x_i, x_j, x_i]_* &= [x_i, x_j, x_i] \\ &= 2x_i x_j x_i - x_j x_i^2 - x_i^2 x_j \\ &= x_i^2 x_j - x_j x_i^2 - 2x_i^2 x_j + 2x_i x_j x_i \\ &= [x_i^2, x_j] - 2[x_i, x_i x_j] \in \langle X \rangle_* \cap S_2. \end{aligned}$$

Wie im Beweis zu Bemerkung 4.12 ist $|\langle X \rangle_*| = \left(2^{l+1}\right)^n \left(2^l\right)^{3\binom{n}{2}+2\binom{n}{3}}$ und $o(y_i) = 2^{l-1}$ für alle $i \in \underline{n}$. Außerdem ist nach Korollar 1.35.1

$$o([x_i, x_i x_j]) = 2^l = o([x_i^2, x_j]) = o([x_i, x_j, x_i])$$

für alle $i, j \in \underline{n}$ mit $i \neq j$.
Insgesamt erhalten wir

$$\begin{aligned} |S| &= |S_1 * \langle y_i \mid i \in \underline{n} \rangle_*| \\ &\leq |S_1| \cdot |\langle y_i \mid i \in \underline{n} \rangle_*| \\ &= |\langle X \rangle_* * S_2| \cdot |\langle y_i \mid i \in \underline{n} \rangle_*| \\ &\leq \frac{|\langle X \rangle_*| \cdot |S_2|}{|\langle [x_i, x_j, x_i] \mid i, j \in \underline{n} \rangle|} \cdot |\langle y_i \mid i \in \underline{n} \rangle_*| \\ &= \frac{\left(\left(2^{l+1}\right)^n \left(2^l\right)^{3\binom{n}{2}+2\binom{n}{3}}\right) \left(2^l\right)^{4\binom{n}{2}}}{\left(2^l\right)^{2\binom{n}{2}}} \left(2^{l-1}\right)^n \\ &= \left(2^l\right)^{2n+5\binom{n}{2}+2\binom{n}{3}} \quad \text{und damit nach Korollar 4.10.1} \end{aligned}$$

$$\begin{aligned}\left(2^l\right)^{2n+5\binom{n}{2}+5\binom{n}{3}} &= |U| = |S * Z| \\ &\leq |S| \cdot |Z| \\ &\leq \left(2^l\right)^{2n+5\binom{n}{2}+2\binom{n}{3}} \left(2^l\right)^{3\binom{n}{3}} \\ &= \left(2^l\right)^{2n+5\binom{n}{2}+5\binom{n}{3}}.\end{aligned}$$

Damit ist $S \cap Z = \{0\}$ und mit $Z \subseteq N^3 = Z(N)$ folgt die Behauptung. □

Nachdem wir nun $K = \mathbb{Z}$ und $K = \mathbb{Z}/p^l\mathbb{Z}$ in verschiedenen Fällen diskutiert haben, führen wir nun all diese Resultate zu einem Hauptsatz zusammen:

Satz 4.14 Es gilt:

(a) Ist $K = \mathbb{Z}$ so folgt

$$(N, *) \cong K^{2n+3\binom{n}{2}+\binom{n}{3}} \ltimes \left(K^{2\binom{n}{2}+3\binom{n}{3}} \times \mathcal{N}_{n,3}\right).$$

(b) Ist $p \neq 2, 3$ und $K = \mathbb{Z}/p^l\mathbb{Z}$ so folgt

$$(N, *) \cong K^{2n+3\binom{n}{2}+\binom{n}{3}} \ltimes \left(K^{2\binom{n}{2}+3\binom{n}{3}} \times \mathcal{N}_{n,3,(p^l,p^l,p^l)}\right).$$

(c) Ist $K = \mathbb{Z}/3^l\mathbb{Z}$ so folgt

$$(N, *) \cong K^{n+3\binom{n}{2}+\binom{n}{3}} \ltimes (K^{2\binom{n}{2}+3\binom{n}{3}} \times \langle a_1, b_1, \ldots, a_n, b_n \mid T_3\rangle)$$

mit

$$\begin{aligned}T_3 := \Big\{ & a_i^{3^{l+1}}, b_i^{3^l}, a_i^{3^l} b_i^{-3^{l-1}}, (a_i, a_j)^{3^l}, (a_i, b_j), (b_i, b_j), (a_i, a_j, a_s)^{3^l}, (a_i, a_j, a_s, a_t) \Big| \\ & i, j, s, t \in \underline{n} \Big\}.\end{aligned}$$

(d) Ist $K = \mathbb{Z}/2^l\mathbb{Z}$ so folgt

$$(N, *) \cong K^{n+3\binom{n}{2}+\binom{n}{3}} \ltimes (K^{3\binom{n}{3}} \times \langle a_1, b_1, \ldots, a_n, b_n, c_{1,2}, c_{2,1}, c_{1,3}, \ldots, c_{n,n-1} \mid T_2\rangle)$$

mit

$$\begin{aligned}T_2 := \Big\{ & a_i^{2^{l+1}}, b_i^{2^l}, c_{i,j}^{2^l}, a_i^{2^l} b_i^{2^{l-1}}, (a_i, a_j)^{2^l}, (a_i, b_i), (a_i, b_j) c_{j,i}^2 (a_j, a_i, a_j), (a_i, c_{s,t}), \\ & (b_i, b_j), (b_i, c_{s,t}), (c_{i,j}, c_{s,t}), (a_i, a_j, a_s)^{2^l}, (a_i, b_j, a_s), (a_i, a_j, a_s, a_t) \Big| \\ & i, j, s, t \in \underline{n}, i \neq j, s \neq t \Big\}.\end{aligned}$$

In allen Fällen ist die Operation des semidirekten Produktes gemäß Bemerkung 4.11 gegeben.

Beweis. Wir betrachten zunächst die Fälle (a) und (b). Sei R ein Repräsentantensystem der Assoziiertenklassen der Länge ≥ 2 und

$$V := \langle R \rangle \text{ und}$$
$$U := \langle X \rangle_* * C.$$

Dann gilt $N = V \ltimes U$ und $V \cong K^{2n+3\binom{n}{2}+\binom{n}{3}}$ nach Lemma 4.7 und $U \cong K^{2\binom{n}{2}+3\binom{n}{3}} \times \langle X \rangle_*$ nach Lemma 4.9. Nach Satz 3.48 ist $\langle X \rangle_* \cong \mathcal{N}_{n,3}$ im Fall (a) und $\langle X \rangle_* \cong \mathcal{N}_{n,3,(p^l,p^l,p^l)}$ im Fall (b).
(c) Sei $K = \mathbb{Z}/3^l\mathbb{Z}$. Seien U, V, Z und y_i wie in Lemma 4.10 beziehungsweise Bemerkung 4.12. Dann gilt $N = V \ltimes (Z \times \langle x_i, y_i \mid i \in \underline{n} \rangle_*)$. Damit ist nur noch $\langle x_i, y_i \mid i \in \underline{n} \rangle_* \cong R$ mit

$$R := \langle a_1, b_1, \ldots, a_n, b_n \mid T_3 \rangle$$

zu beweisen.
Es ist $\langle x_i, y_i \mid i \in \underline{n} \rangle_* = \langle x_i, x_i^3 \mid i \in \underline{n} \rangle_*$ nach Definition der y_i und es gilt nach Korollar 1.35.1, Korollar 1.34.1 und da $x_i^3 \in Z(N)$ für alle $i \in \underline{n}$

$$\begin{aligned} 1 = x_i^{(3^{l+1})} = \left(x_i^3\right)^{(3^l)} = x_i^{(3^l)} \left(x_i^3\right)^{(-3^{l-1})} = [x_i, x_j]_*^{(3^l)} \\ = [x_i, x_j^3]_* = [x_i^3, x_j^3]_* = [x_i, x_j, x_t]_*^{(3^l)} = [x_i, x_j, x_s, x_t]_* \end{aligned}$$

für alle $i, j, s, t, \in \underline{n}$. Damit lässt sich die Abbildung $a_i \mapsto x_i$ und $b_i \mapsto x_i^3$ zu einem Epimorphismus $\varphi : R \to \langle x_i, y_i \mid i \in \underline{n} \rangle_*$ fortsetzen. Da R eine nilpotente Gruppe von der Klasse 3 ist, $a_i^{3^l} \in \langle b_i \rangle$ für alle $i \in \underline{n}$ gilt und b_i für alle $i \in \underline{n}$ im Zentrum liegt, erhalten wir mit der Darstellung durch Elementarkommutatoren nach Lemma 4.5

$$R = \left\{ \prod_{i=1}^{n} a_i^{\alpha_i} \prod_{i=1}^{n} b_i^{\beta_i} \prod_{i>j} (a_i, a_j)^{\gamma_{ij}} \prod_{i>j\leq t} (a_i, a_j, a_t)^{\delta_{ijt}} \mid \alpha_i, \beta_i, \gamma_{ij}, \delta_{ijt} \in \underline{p^l} \right\}.$$

Damit ist $|R| \leq \left(3^l\right)^{n+n+n_2+n_3} = \left(3^l\right)^{2n+3\binom{n}{2}+2\binom{n}{3}}$ mit Lemma 4.5. Da nach dem Beweis zu Bemerkung 4.12 gilt mit den dortigen Bezeichnungen

$$|\langle x_i, y_i \mid i \in \underline{n} \rangle_*| = \frac{|U|}{|Z|} = \left(3^l\right)^{2n+3\binom{n}{2}+2\binom{n}{3}}$$

gilt, ist der Epimorphismus φ ein Isomorphismus. Es folgt Teil (c).
(d) Wir gehen wie in Teil (c) vor. Sei $K = \mathbb{Z}/2^l\mathbb{Z}$. Seien $U, V, Z, S, y_1, \ldots, y_n$ wie in Lemma 4.10 beziehungsweise Bemerkung 4.13. Dann ist

$$N = V \ltimes U = V \ltimes (Z \times S) \cong K^{n+3\binom{n}{2}+\binom{n}{3}} \ltimes (K^{3\binom{n}{3}} \times S).$$

Sei

$$R := \langle a_1, b_1, \ldots, a_n, b_n, c_{1,2}, c_{2,1}, c_{1,3}, \ldots, c_{n,n-1} \mid T_2 \rangle.$$

Wir wollen $R \cong S$ beweisen. Dazu zeigen wir, dass sich die Abbildung

$$a_i \mapsto x_i,\ b_i \mapsto x_i^2 \quad \text{und} \quad c_{i,j} \mapsto [x_i, x_i x_j]$$

zu einem Isomorphismus $\varphi : R \to S$ fortsetzen lässt, also dass in S alle der in T_2 angegebenen Relationen erfüllt sind.
Nach Korollar 1.35.1 ist $o(x_i) = 2^{l+1}$ und $o(x_i^2) = 2^l = o([x_i, x_i x_j])$ für alle $i, j \in \underline{n}$. Außerdem ist $o(y_i) = 2^{l-1}$ nach Korollar 1.34.1 für alle $i \in \underline{n}$. Weiter ist $[x_i, x_i x_j] \in Z(N)$ und $[x_i^2, x_j^2] = 0$. Zudem kommutieren x_i und x_i^2 für alle $i \in \underline{n}$ miteinander und jeder Kommutator der Länge 4 in S ist trivial. Es $S' \subseteq N^2$ und damit ist $s^{(2^l)} = 0$ mit Lemma 1.35 für jeden Kommutator $s \in S$. Zuletzt gilt für alle $i, j, s \in \underline{n}$

$$L([x_i, x_j^2, x_s]_*) = 4 \quad \text{und damit} \quad [x_i, x_j^2, x_s]_* = 0.$$

Zudem ist für alle $i \in \underline{n}$ nach Lemma 1.15

$$x_i^{(2^l)} * (x_i^2)^{(2^{l-1})} = (2^{l-1} x_i^2) * (2^{l-1} x_i^2) = 0$$

und für alle $i, j \in \underline{n}$

$$\begin{aligned}[x_i, x_j^2]_* * [x_j, x_j x_i]^{(2)} * [x_j, x_i, x_j]_* &= [x_i, x_j^2] + 2[x_j, x_j x_i] + [x_j, x_i, x_j] \\ &= x_i x_j^2 - x_j^2 x_i + 2x_j^2 x_i - 2x_j x_i x_j + 2x_j x_i x_j - x_i x_j^2 - x_j^2 x_i \\ &= 0.\end{aligned}$$

Damit lässt sich die oben angegebene Abbildung zu einem Homomorphismus $\varphi : R \to S$ fortsetzen, der nach Definition von S ein Epimorphismus ist. Weiter gilt nach Lemma 4.5 mit $a_i^{2^l} \in \langle b_i \rangle$ für alle $i \in \underline{n}$ und $(a_i, b_j) \in \langle c_{j,i}, (a_j, a_i, a_j) \rangle \subseteq Z(R)$ für alle $i, j \in \underline{n}$

$$R = \Big\{ \prod_{i=1}^{n} a_i^{\alpha_i} \prod_{i=1}^{n} b_i^{\beta_i} \prod_{i \neq j}^{n} c_{i,j}^{\gamma_{ij}} \prod_{i>j} (a_i, a_j)^{\delta_{ij}} \prod_{i>j\leq t} (a_i, a_j, a_t)^{\epsilon_{ijt}} \Big| \\ \forall i, j, t \in \underline{n} : \ \alpha_i, \beta_j, \gamma_{ij}, \delta_{ij}, \epsilon_{ijt} \in \underline{2^l} \Big\}$$

und damit folgt wie in (c)

$$|R| \leq \left(2^l\right)^{n+n+2\binom{n}{2}+\binom{n}{2}+(2\binom{n}{2}+2\binom{n}{3})} = \left(2^l\right)^{2n+5\binom{n}{2}+2\binom{n}{3}} \overset{\text{Bew. von } 4.13}{=} |S|.$$

Damit ist φ ein Isomorphismus und die Behauptung ist gezeigt. □

Also ist es uns auch im Fall $k = 3$ gelungen, die Gruppe $(N, *)$ zu beschreiben. Hier ist gut zu erkennen, dass die Beschreibung für $p = 2$ und $p = 3$ deutlich komplizierter wird.

Bei größerer Nilpotenzklasse k wird die Voraussetzung $\mathrm{ggT}(p^l, k!) = 1$, also $p > k$, des Satzes 3.3 für immer weniger Primzahlen p erfüllt, wobei gleichzeitig der Faktor $U = \left\langle X^{<\lceil \frac{k+1}{2} \rceil} \right\rangle_* * C$ im Satz 3.3 immer mehr von der bereits analysierten Untergruppe $\langle X \rangle_*$ abweicht. Es ist also nicht zu erwarten, dass mit den in dieser Arbeit angewandten Methoden eine Beschreibung der Gruppe $(N_{K,X,k}, *)$ für größere k gelingen wird.

Bezeichnungen

Es seien stets

n, k	natürliche Zahlen,
K	ein kommutativer unitärer Ring (insbesondere sei $1_K \neq 0_K$),
X	eine nichtleere Menge.

Es bezeichnet in dieser Arbeit

$\mathbb{N}$	die Menge der natürlichen Zahlen ($0 \notin \mathbb{N}$),
$\mathbb{P}$	die Menge der Primzahlen,
$\underline{n}$	$= \{1, 2, \ldots, n\}$,
$\underline{n}_0$	$= \{0, 1, 2, \ldots, n\}$,
$\left\lceil \frac{n}{k} \right\rceil$	$= \min\{m \in \mathbb{N} \mid m \geq \frac{n}{k}\}$,
$\left\lfloor \frac{n}{k} \right\rfloor$	$= \max\{m \in \mathbb{N} \mid m \leq \frac{n}{k}\}$,
$\mathcal{C}_n$	die zyklische Gruppe der Ordnung n.

Wir verwenden in der gesamten Arbeit linksnormierte Schreibweise für Lie-Klammern und Gruppen-Kommutatoren. Die folgenden Bezeichnungen werden in der Reihenfolge, in der sie zum ersten Mal in dieser Arbeit vorkommen, aufgelistet.

1.1: Seien A eine assoziative K-Algebra, $a, b, a_1, \ldots, a_n \in A$ und $B \subseteq A$. Es sei

$a * b$	$:= a + b + ab$ (1.1),
$a^{(n)}$	die n-te $*$-Potenz von a (1.1),
$\bigstar_{i=1}^{n} a_i$	$:= a_1 * \ldots * a_n$ (1.1),
a^-	das $*$-Inverse von a (1.1),
$Q(A)$	die Menge der $*$-invertierbaren Elemente in A (1.1),
$a^{(-n)}$	das $*$-Inverse von $a^{(n)}$ (1.1),
A^n	$\langle a_1 \cdots a_n \mid a_1, \ldots, a_n \in A \rangle_K$ (1.3),
$\langle B \rangle_K$	der von B erzeugten K-Teilraum von A (1.6),
$\langle B \rangle_{\mathbb{Z}}$	die von B erzeugte additive Gruppe in A (1.6),
$\langle B \rangle_{\mathfrak{A}^K}$	die von B erzeugte K-Teilalgebra von A (1.6),
$\langle B \rangle_*$	für $B \subseteq Q(A)$ die von B erzeugte Untergruppe von $(A, *)$ (1.6),
$\langle B \rangle$	für $B \subseteq Q(A)$ die von B erzeugte additive Gruppe in A, wenn $\langle B \rangle_{\mathbb{Z}} = \langle B \rangle_*$ gilt (1.7),
$[a, b]$	$:= ab - ba$ die Lie-Klammer von a und b (1.9),
$b^{(a)}$	$:= a^- * b * a$ für $a \in Q(A)$ das $*$-Konjugierte von b unter a (1.9),
$[a, b]_*$	$:= a^- * b^- * a * b$ für $a, b \in Q(A)$ der $*$-Kommutator von a und b (1.9).

1.2: Sei $p \in \mathbb{P}$. Es sei

π_p	die Abbildung, die jede Zahl n auf ihren größten p-Anteil abbildet (1.12, diese Bezeichnung wird nur in Abschnitt 1.2 verwandt),
$\pi_{p'}$	die Abbildung, die n auf ihren größten p'-Anteil abbildet (1.12),
$c_{k,p,t}$	$= \left\lfloor \frac{k}{p^t} \right\rfloor$ für alle $t \in \mathbb{N}_0$ (1.16),
$I_{k,p,t}$	$= (c_{k,p,t+1}, c_{k,p,t}] \cap \mathbb{N}$ für alle $t \in \mathbb{N}_0$ (1.16),
$s_{k,p}$	die größte Zahl $t \in \mathbb{N}_0$ mit $p^t \leq k$ (1.16),
c_t, I_t, s	$c_{k,p,t}$, $I_{k,p,t}$ bzw. $s_{k,p}$, wenn k und p im Kontext eindeutig gegeben sind (1.16).

1.3: Es sei

X^+	die Menge der nichtleeren Worte in X (1.19),
$l(f)$	die Länge eines Wortes $f \in X^+$ (1.19),
$X^{=k}$	die Menge der Worte der Länge k in X^+ (1.19),
$X^{\leq k}$	die Menge der Worte bis zur Länge k in X^+ (1.19),
$F_{K,X}/F_{K,n}$	die freie K-Algebra über X / über einer n-elementigen Menge (1.19),
$N_{K,X,k}/N_{K,n,k}$	die frei nilpotente K-Algebra über X / über einer n-elementigen Menge von der Klasse k (1.19),
$P_{K,X}/P_{K,n}$	die nichtunitäre, nichtkommutative K-Potenzreihenalgebra über X / über einer n-elementigen Menge (1.19),
F, N, P	$F_{K,X}$, $P_{K,X}$, $P_{K,X}$, wenn K, n, k im Kontext eindeutig gegeben sind,
π_n	die Projektion auf die n-te homogene Komponente (1.24),
$\pi_{\leq n}$	die Projektion auf die $KX^{\leq n}$ (1.24),
$\pi_{>n}$	$:= \mathrm{id} - \pi_{\leq n}$ (1.24),
π_g	für $g \in X^+$ die Projektion auf die $\langle g \rangle_K$ (1.24),
$L(a)$	die Länge eines Elementes $a \in P$ (1.26),
$\pi_{\min}$	die Projektion auf die kleinste homogene Komponente $\neq 0$ (1.26),
$o_+(a)$	die additive Ordnung eines Elements $a \in P$ (1.33),
$o_*(a)/o(a)$	die $*$-Ordnung eines Elements $a \in P$ (1.33),
$Syl_p(N)$	die Menge der p-Sylowgruppen in $(N, *)$ für $p \in \mathbb{P}$ (1.37).

1.4: Es sei $i \in \mathbb{N}$. Es bezeichne

$X^{(+)}$	das freie Magma über X,
$l(f)$	die Länge eines Elementes $f \in X^{(+)}$,
μ	$\mathbb{N} \to \{-1, 0, 1\}$ die Möbius-Funktion,
n_i	$= \frac{1}{i} \sum_{d \mid i} \mu(d) n^{\frac{i}{d}}$ die Anzahl der Elementarelemente von der Länge i über einer n-elementigen Menge (1.41),
$\mathfrak{E}_i^{(+)}$	das Tupel der Elementarelemente von der Länge i (1.41),
$\mathfrak{E}_i^{\mathfrak{L},\beta}$	das Tupel der elementaren Lie-Klammern vom Gewicht i unter der Abbildung β (1.42),

$\mathfrak{E}_i^{\mathfrak{L}}$	$:= \mathfrak{E}_i^{\mathfrak{L},\mathrm{id}}$ (1.42),
$\mathcal{F}_X/\mathcal{F}_n$	die freie Gruppe über X / über einer n-elementigen Menge (1.46),
$\langle x_1,\ldots,x_n \mid R\rangle$	für $R \subseteq \mathcal{F}_{\{x_1,\ldots,x_n\}}$ die von den Erzeugern $x_1,\ldots,x_n$ und Relationen in R definierte Gruppe,
$(\cdot,\cdot)$	die Kommutatorbildung in $\mathcal{F}_X$ (1.46),
$\mathfrak{E}_i^{\mathfrak{G},\beta}$	das Tupel der Elementarkommutatoren vom Gewicht i unter der Abbildung β (1.46),
$\mathfrak{E}_i^{\mathfrak{G}}$	$:= \mathfrak{E}_i^{\mathfrak{G},\mathrm{id}}$ (1.46),
$\gamma_n(\mathcal{G})$	das n-te Glied der absteigenden Zentralreihe einer Gruppe $\mathcal{G}$ (es ist $\gamma_1(\mathcal{G}) = \mathcal{G}$) (1.48).

1.5: Es sei

$\mathfrak{G}$	die Klasse der Gruppen,
$\mathcal{G}^n$	$\langle g^n \mid g \in \mathcal{G}\rangle$ für $\mathcal{G} \in \mathfrak{G}$,
$Z_n(\mathcal{G})$	das n-te Glied der aufsteigenden Zentralreihe von $\mathcal{G} \in \mathfrak{G}$ (es ist $Z_0(\mathcal{G}) = \{1_{\mathcal{G}}\}$) (1.54),
Z_n, γ_n	$Z_n(\mathcal{G})$, $\gamma_n(\mathcal{G})$ wenn $\mathcal{G}$ im Kontext eindeutig bestimmt ist (1.54).

2.1: Es sei

$\Lambda_K(X)$	die äußere Algebra über den K-Linearkombinationen über X,
J	das Jacobson-Radikal von $\Lambda_K(X)$ (2.1),
$\Phi(J)$	die Frattini-Untergruppe von $(J,*)$.

2.2: Es sei $\leq$ eine Ordnung auf X und $x \in X$ minimal bezüglich dieser Ordnung. Es sei $(g_1,\ldots,g_k) \in (X^+)^k$, $(m_1,\ldots,m_k) \in \mathbb{N}^k$ und $B \subseteq \mathbb{N}$. Dann bezeichne

f_x	$= -t_x \in K[t_x]$ (2.17),
$(g_1,\ldots,g_k) \vDash g$	eine Zerlegung von $g \in X^+$,
f_g	$= -\sum_{(g_1,g_2)\vDash g} t_{g_1} f_{g_2} - t_g \in K[t_x, \ldots t_g]$ für $g \in X^+ \setminus \{x\}$ (2.17),
$(m_1,\ldots,m_k) \vDash_B n$	eine Zerlegung von n, bei der jeder Summand in B liegt (2.21),
f_n	$= f_{x^n}$ falls $X = \{x\}$ (2.17).

3.1: Es bezeichne

$\mathcal{S}_n$	die symmetrische Gruppe auf $\underline{n}$ (3.4),
C	das Augmentationsideal in N über die Assoziiertenklassen (3.5),
N'	die Kommutatoruntergruppe in $(N,*)$ (3.6).

3.2: Es sei

$\Phi(N)$	die Frattini-Untergruppe von $(N, *)$.

3.4: Es sei $\varepsilon = (\varepsilon_1, \ldots, \varepsilon_k) \in \mathbb{N}^k$. Es bezeichne

$\mathfrak{N}_k$	die Klasse der nilpotenten Gruppen der Klasse höchstens k (3.38),
$\mathfrak{N}_{k,\varepsilon}$	die Klasse der Gruppen in $\mathfrak{N}_k$, bei denen ε_i von dem Exponenten von γ_i für alle $i \in \underline{k}$ geteilt wird (3.38),
$\mathfrak{N}_{n,k}$	die Klasse der Gruppen in $\mathfrak{N}_k$ mit n Erzeugern (3.38),
$\mathcal{N}_{n,k}$	die frei nilpotente Gruppe der Klasse k mit n Erzeugern (3.38),
$\mathfrak{N}_{n,k,\varepsilon}$	die Klasse der Gruppen in $\mathfrak{N}_{k,\varepsilon}$ mit n Erzeugern (3.38),
$\mathcal{N}_{n,k,\varepsilon}$	die $\mathfrak{N}_{n,k,\varepsilon}$-freie Gruppe (3.39),
$\mathcal{M}_{n,k,\varepsilon}$	$:= \langle y_1, \ldots, y_n \mid \{e_{i,j}^{\varepsilon_i}\} \cup \{(y_{i_1}, \ldots, y_{i_{k+1}})\}\rangle$ (3.53),
$\mathcal{H}_K$	die Heisenberggruppe über K (3.55).

Literaturverzeichnis

[AA09] Andreescu, Titu ; Andrica, Dorin: *Number theory*. Birkhäuser Boston, Inc., Boston, MA, 2009. – Structures, examples, and problems

[Bae43] Baer, Reinhold: Radical ideals. In: *Amer. J. Math.* 65 (1943), S. 537–568

[Bah87] Bahturin, Yu. A.: *Identical relations in Lie algebras*. VNU Science Press, b.v., Utrecht, 1987

[Bou74] Bourbaki, Nicolas: *Elements of mathematics. Algebra, Part I: Chapters 1-3*. Hermann, Paris; Addison-Wesley Publishing Co., Reading Mass., 1974. – Translated from the French

[Hal76] Hall, Marshall Jr.: *The theory of groups*. Chelsea Publishing Co., New York, 1976

[Han12] Hansmann, Juliane: *Über die Gruppe quasiregulärer Elemente in frei nilpotenten Ringen*, Mathematisches Seminar der Christian-Albrechts-Universität zu Kiel, Diplomarbeit, 2012

[Hup67] Huppert, B.: *Endliche Gruppen. I*. Springer-Verlag, Berlin-New York, 1967 (Die Grundlehren der Mathematischen Wissenschaften, Band 134)

[Jac45] Jacobson, N.: The radical and semi-simplicity for arbitrary rings. In: *Amer. J. Math.* 67 (1945), S. 300–320

[LN83] Lidl, Rudolf ; Niederreiter, Harald: *Encyclopedia of Mathematics and its Applications*. Bd. 20: *Finite fields*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1983. – With a foreword by P. M. Cohn

[LS77] Lyndon, Roger C. ; Schupp, Paul E.: *Combinatorial group theory*. Springer-Verlag, Berlin-New York, 1977

[Mag35] Magnus, Wilhelm: Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring. In: *Math. Ann.* 111 (1935), Nr. 1, S. 259–280

[MKS76] Magnus, Wilhelm ; Karrass, Abraham ; Solitar, Donald: *Combinatorial group theory*. Dover Publications, Inc., New York, 1976

[New98] Newman, Donald J.: *Graduate Texts in Mathematics*. Bd. 177: *Analytic number theory*. Springer-Verlag, New York, 1998

[Per42] Perlis, Sam: A characterization of the radical of an algebra. In: *Bull. Amer. Math. Soc.* 48 (1942), S. 128–132

[Qui89] Quintana, Ricardo Jr.: A bound on the order of finitely generated nilpotent groups with an exponent. In: *J. Algebra* 127 (1989), Nr. 1, S. 55–56

[Reu93] Reutenauer, Christophe: *London Mathematical Society Monographs. New Series*. Bd. 7: *Free Lie algebras*. The Clarendon Press, Oxford University Press, New York, 1993. – Oxford Science Publications

[Wir05] Wirsing, Sven: *Über Einheitengruppen modularer Gruppenalgebren*, Mathematisches Seminar der Christian-Albrechts-Universität zu Kiel, Diss., 2005

Erklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit – abgesehen von der Beratung durch den Betreuer meiner Promotion – 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

Juliane Hansmann