Die injektive Dimension endlicher Hecke-Algebren

Sebastian Melzer

Matr.-Nr. 3005111

15. Oktober 2018

Bachelorarbeit

Vorgelegt der
Fakultät für Mathematik
der Universität Duisburg-Essen

Betreut von Prof. Dr. Jan Kohlhaase

Inhaltsverzeichnis

Einleitung

In dieser Arbeit wird bewiesen, dass für ein endliches zerfallendes BN-Paar (G, B, N, S, U) die selbstinjektive Dimension der Hecke-Algebra $H_R(G, U)$ über einem kommutativen Ring R gleich der des Grundrings R ist. Dieser Satz geht im Wesentlichen auf Tinberg zurück (vgl. [11, Proposition 3.7]).

Dafür entwickeln wir in Kapitel 2 zuerst eine dimensionserhaltende Art von Ringerweiterung, die sogenannte α-Frobeniuserweiterung. Somit müssen wir nur zeigen, dass die Hecke-Algebra eine solche Erweiterung über ihrem Grundring ist. In den Kapiteln 3 und 4 werden die Gruppen, für die wir uns interessieren, näher betrachtet. Kapitel 3 behandelt dabei Coxetersysteme und ihre Eigenschaften. Für eine Diskussion zerfallender BN-Paare ist dies unerlässlich. Die Behandlung ist keineswegs vollständig und verzichtet auf übermäßig technische Beweise. In Kapitel 4 untersuchen wir dann die Struktur von (zerfallenden) BN-Paaren genauer. Alle Aussagen werden detailliert bewiesen. Die Ergebnisse dieses Kapitels liefern schließlich in Kapitel 5 das Hauptresultat der Arbeit.

Diese Bachelorarbeit entstand im Anschluss an das Seminar *Homologische Algebra* von Prof. Dr. Jan Kohlhaase aus dem Sommersemester 2018. Der homologische Anteil der Arbeit ist dennoch relativ klein – abgesehen vom Beweis von Satz 2.18, welcher grundlegende Eigenschaften der Ext-Funktoren verwendet, sollte es genügen, projektive und injektive Moduln zu kennen. Zur Gruppentheorie ist kein über die grundlegenden Begriffe hinausgehendes Vorwissen nötig. Kapitel 1 etabliert die nötigen Definitionen und Ergebnisse.

1 Grundlagen

1.1 Injektive Dimension und projektive Basen

In dieser Arbeit sind alle Ringe, Ringhomomorphismen und Moduln stets unitär. Ringe sind nicht notwendigerweise kommutativ und Moduln sind, sofern nicht anders angegeben, Linksmoduln. Ein (R, S)-Bimodul A wird gelegentlich mit ${}_RA$, A_S oder ${}_RA_S$ bezeichnet, wenn die jeweilige Struktur hervorgehoben werden soll. Die Skalarmultiplikation von r und m wird üblicherweise einfach rm geschrieben, wenn Missverständnisse ausgeschlossen sind; wäre dies missverständlich oder soll die Skalarmultiplikation hervorgehoben werden, schreiben wir $r.m$ für rm oder definieren explizit eine andere Notation.

Definition 1.1. *Sei S ein Ring und M ein S-Linksmodul. Die* injektive Dimension *von M ist die Länge einer kürzesten injektiven Auflösung von M. Eine* injektive Auflösung *ist dabei eine exakte Sequenz von S-Moduln der Form*

$$0 \to M \to I_0 \to I_1 \to \dots,$$

sodass alle I_n injektive Moduln sind.

Dabei hat eine Auflösung $M \to I_*$ Länge $n \in \mathbb{N}_0$, wenn sie von der Form

$$0 \to M \to I_0 \to \dots \to I_n \to 0$$

ist, und Länge ∞, falls alle $I_k \neq 0$ sind. Man schreibt $\mathrm{id}_S(M)$ für die injektive Dimension von M, oder einfach nur $\mathrm{id}(M)$, wenn S aus dem Kontext klar ist. Fasst man S als Linksmodul über sich selbst auf, heißt $\mathrm{id}_S(S)$ die (links)selbstinjektive Dimension *des Rings S. Analog definiert man die* (rechts)selbstinjektive Dimension.

Ein Modul ist genau dann injektiv, wenn seine injektive Dimension 0 beträgt. Für nichtkommutative Ringe stimmt die linksselbstinjektive Dimension im Allgemeinen nicht mit der rechtsselbstinjektiven Dimension überein (vgl. [7, Example 3.74B]). Die injektive Dimension ist durch folgende Eigenschaft mit den Ext-Funktoren verbunden. Der Beweis verläuft analog zum Fall der projektiven Dimension, den man in [3, Proposition 8.1.1] findet.

Proposition 1.2. *Sei S ein Ring, M ein S-Modul und $n \in \mathbb{N}$. Die folgenden Aussagen sind äquivalent:*

(i) $\mathrm{id}(M) \leq n$.

(ii) Für alle S-Linksmoduln N und $r > n$ gilt $\mathrm{Ext}^r_S(N, M) = 0$.

(iii) In jeder exakten Sequenz $0 \to M \to I_0 \to \dots \to I_{n-1} \to N \to 0$ mit $I_0, \dots, I_{n-1}$ injektiv ist auch N injektiv.

Kapitel 2 verwendet eine Charakterisierung projektiver Moduln, die auf dem folgenden Begriff einer *projektiven Basis* beruht.

Definition 1.3. *Eine* projektive Basis *eines R-Moduls M ist eine Familie $(m_i)_{i\in I}$ von Elementen von M und eine Familie $(f_i)_{i\in I}$ von Homomorphismen $f_i : M \to R$, sodass für jedes $m \in M$ fast alle $f_i(m) = 0$ sind und $\sum_{i\in I} f_i(m).m_i = m$ gilt.*

Ein R-Modul M ist genau dann projektiv, wenn er eine projektive Basis besitzt: Die R-lineare Abbildung $(e_i \mapsto m_i) : R^{(I)} \to M$ besitzt nämlich den Schnitt $(m \mapsto (f_i(m))_{i\in I})$, durch den M ein direkter Summand von $R^{(I)}$ ist. Ist umgekehrt M ein direkter Summand von $R^{(I)}$, so wähle man m_i als das Bild von e_i unter der Projektion $R^{(I)} \to M$ und f_i als Komposition von $M \hookrightarrow R^{(I)}$ mit der i-ten Koordinatenprojektion $R^{(I)} \to R$.

Ist M zusätzlich endlich erzeugt, lässt sich I auch endlich wählen. Die Homomorphismen f_i verallgemeinern die Koordinatenprojektionen eines freien Moduls. Für jeden Modul gibt es natürlich Erzeuger und Abbildungen, welche die Gleichung in 1.3 erfüllen – der Unterschied ist, dass die Abbildungen bei einer projektiven Basis sogar Homomorphismen sind.

1.2 Vorbereitungen aus der Gruppentheorie

Ist H eine Untergruppe von G, schreiben wir $H < G$. Ist H ein Normalteiler, notieren wir dies mit $H \lhd G$. Konjugation ist stets rechte Konjugation und wird $g^h = h^{-1}gh$ geschrieben. Ein Element $t \in G$ *normalisiert* eine Untergruppe $H < G$, wenn $H^t = H$ bzw. $Ht = tH$ gilt. Für endliche Gruppen ist das äquivalent zu $H^t \subset H$. Eine Teilmenge $T \subset G$ normalisiert H, wenn H von jedem $t \in T$ normalisiert wird. Eine Untergruppe ist z.B. genau dann ein Normalteiler von G, wenn sie von G normalisiert wird.

Eine *Wirkung* einer Gruppe G auf einer Menge X ist ein Gruppenhomomorphismus $\sigma : G \to \mathrm{Bij}(X)$. Wir schreiben $\sigma(g)(x)$ meist als $g.x$. Gelegentlich nennen wir X auch eine *G-Menge*. Die *G-äquivarianten Abbildungen* spielen die Rolle von G-Mengenhomomorphismen; sind X, Y zwei G-Mengen, so heißt $f : X \to Y$ G-äquivariant, wenn $f(g.x) = g.f(x)$ für alle $g \in G$ und $x \in X$ gilt.

Sind $H, K < G$ Untergruppen, so ist die *H-K-Doppelnebenklasse* von $g \in G$ die Menge $HgK = \{hgk \mid h \in H, k \in K\}$. Ähnlich wie für Nebenklassen zeigt man, dass die Doppelnebenklassen eine Partition von G bilden. Anders als Links- und Rechtsnebenklassen können Doppelnebenklassen jedoch unterschiedliche Kardinalitäten besitzen. Man sieht sofort, dass eine Doppelnebenklasse jeweils eine Vereinigung von Links- oder Rechtsnebenklassen ist, und sich Kardinalitätsunterschiede somit auf die Zahl der enthaltenen Links- bzw. Rechtsnebenklassen reduzieren lassen.

Sind $A, B, C < G$ Untergruppen und $g \in G$, so ist zwar $A(B \cup C) = AB \cup AC$ und $g(A \cap B) = gA \cap gB$, aber im Allgemeinen nur $A(B \cap C) \subset AB \cap AC$. Es gilt jedoch die folgende schwächere Eigenschaft:

Proposition 1.4. *Sind $A, B, C < G$ Untergruppen und ist $A < B$, gilt $A(B \cap C) = B \cap AC$.*

Diese Eigenschaft werden wir in Kapitel 4.3 häufig benutzen. Im Hinblick auf dieses Kapitel erwähnen wir auch Eigenschaften von p-Gruppen und semidirekten Produkten. Für eine Primzahl p heißt ein Element $g \in G$ *p-Element*, wenn seine Ordnung eine Potenz von p ist. Eine Gruppe, die aus p-Elementen besteht, heißt *p-Gruppe*. Eine maximale p-Untergruppe von G heißt *p-Sylowuntergruppe*. Wir erinnern an den folgenden Satz aus der Gruppentheorie.

Satz 1.5 (Zweiter sylowscher Satz)**.** *Ist p eine Primzahl, sind alle p-Sylowuntergruppen einer endlichen Gruppe G zueinander konjugiert.*

Ist eine p-Sylowuntergruppe U einer endlichen Gruppe G also ein Normalteiler, ist sie die einzige p-Sylowuntergruppe und enthält alle p-Gruppen. Da jedes p-Element in einer p-Sylowuntergruppe enthalten ist, besteht U genau aus den p-Elementen von G.

Definition 1.6. *Sei G eine Gruppe, $H < G$ eine Untergruppe, und $N \triangleleft G$ ein Normalteiler. Gelten $G = NH$ und $N \cap H = 1$, heißt G das* semidirekte Produkt *von N und H und wir schreiben $G = N \rtimes H$.*

Die folgende Aussage folgt direkt aus der Definition durch Betrachtung der Abbildung $((n,h) \mapsto nh) : N \times H \to G$.

Lemma 1.7. *Ist $G = N \rtimes H$ ein semidirektes Produkt, so besitzt jedes $g \in G$ eine eindeutige Darstellung $g = nh, n \in N, h \in H$.*

Lemma 1.8. *Sei G eine endliche Gruppe mit Untergruppen $H, K < G$, sodass $G = HK$. Dann gilt $|G| = \dfrac{|H|\,|K|}{|H \cap K|}$.*

Beweis. Ist Ω ein Repräsentantensystem von $H/(H \cap K)$, so besitzt G eine disjunkte Zerlegung $G = \bigsqcup_{h \in \Omega} hK$. □

Definition 1.9. *Sei S eine Menge. Die* freie Gruppe *auf S ist die bis auf Isomorphie eindeutig bestimmte Gruppe $\mathrm{F}(S)$, die S als Teilmenge enthält und die folgende universelle Eigenschaft erfüllt:*

> *Für jede Gruppe G ist jede Abbildung $f : S \to G$ zu einem eindeutig bestimmten Gruppenhomomorphismus $\mathrm{F}(S) \to G$ erweiterbar.*

Die freie Gruppe $\mathrm{F}(S)$ lässt sich als Gruppe aller reduzierten Zeichenketten (*Worte*) in $\{s, s^{-1} \mid s \in S\}$ realisieren. Ein Wort heißt *reduziert*, wenn es kein Teilwort der Form ss^{-1} oder $s^{-1}s$ enthält; jedes Wort lässt sich durch sukzessives Entfernen solcher Paare auf eine eindeutig bestimmte reduzierte Form bringen. Die Elemente von $\mathrm{F}(S)$ sind dann die reduzierten Worte, das Identitätselement ist das leere Wort, und die Multiplikation ist Aneinanderreihung gefolgt von Reduktion.

Durch Quotienten der freien Gruppe können wir zuletzt Präsentationen einer Gruppe definieren. Ist G eine Gruppe, $S \subset G$ eine Teilmenge und R eine Menge von Worten in S, so ist (S, R) eine *Präsentation* von G, wenn G isomorph zur Gruppe $\mathrm{F}(S)/N$ ist, wobei N der kleinste Normalteiler von $\mathrm{F}(S)$ ist, der R enthält.

Ein bekanntes Beispiel ist die folgende Präsentation der symmetrischen Gruppe $\mathfrak{S}_n$. Für alle $1 \leq i < n$ sei s_i die Permutation, die i und $i+1$ vertauscht. Dann wählen wir als Erzeuger $S = \{s_1, \ldots, s_{n-1}\}$ und als Relationen

$$R = \left\{ s_i^2 \,\middle|\, 1 \leq i \leq n-1 \right\} \cup \left\{ (s_i s_{i+1})^3 \,\middle|\, 1 \leq i \leq n-2 \right\} \cup \left\{ (s_i s_j)^2 \,\middle|\, |i-j| > 1 \right\}.$$

2 α-Frobeniuserweiterungen

In diesem Kapitel führen wir eine spezielle Art von Ringerweiterung ein und beweisen, dass die selbstinjektiven Dimensionen bei einer solchen Erweiterung erhalten bleiben. Auf diese Weise reduzieren wir das Hauptergebnis dieser Arbeit darauf, zu zeigen, dass die betrachtete Hecke-Algebra eine Erweiterung dieses Typs über ihrem Grundring ist. Die Behandlung von Frobeniuserweiterungen in diesem Kapitel orientiert sich hauptsächlich an [1].

2.1 Frobeniusalgebren

Der Begriff einer α-Frobeniuserweiterung ist isoliert betrachtet etwas undurchsichtig, daher gehen wir in diesem Abschnitt kurz auf seinen Ursprung in den *Frobeniusalgebren* ein.

In der Darstellungstheorie der Gruppen betrachtet man Wirkungen einer Gruppe G auf R-Moduln V, genannt *Darstellungen*, um den abstrakten Gruppenelementen eine konkret analysierbare Form als Automorphismen zu geben. Dabei ist R typischerweise kommutativ und meist sogar ein Körper, sodass Ergebnisse der linearen Algebra anwendbar sind. Ein Homomorphismus von Darstellungen über R ist eine G-äquivariante und R-lineare Abbildung zwischen den R-Moduln. Die Theorie der Darstellungen über kommutativen R läuft mithilfe der folgenden Konstruktion auf das Studium von Moduln über bestimmten Ringen hinaus.

Definition 2.1. *Sei R ein kommutativer Ring und G eine endliche Gruppe. Die* Gruppenalgebra *von G über R ist der freie R-Modul mit Basis G und wird mit $R[G]$ bezeichnet. Wir identifizieren jedes $g \in G$ mit seinem Basisvektor und wählen als Multiplikation das sogenannte* Faltungsprodukt

$$(\sum_{g\in G} x_g g) * (\sum_{h\in G} y_h h) = \sum_{g\in G}\sum_{h\in G} x_h y_{h^{-1}g} g.$$

Das Einselement ist der zu $1 \in G$ assoziierte Basisvektor.

Das Faltungsprodukt ist die einzige Multiplikation $*$ auf $R[G]$, die $g * h = gh \in R[G]$ erfüllt. Auf diese Weise lässt sich G als Untergruppe von $R[G]^\times$ auffassen, woran man sieht, dass der Gruppenring einer nichtabelschen Gruppe nicht kommutativ ist. Das Gegenteil ist schnell überprüft, sodass $R[G]$ genau dann kommutativ ist, wenn G abelsch ist.

Die $R[G]$-Moduln entsprechen den Darstellungen von G auf R-Moduln, indem man jeder Darstellung $\rho : G \to \mathrm{GL}(V)$ den $R[G]$-Modul V mit Skalarmultiplikation

$$(\sum_{g\in G} x_g g).v = \sum_{g\in G} x_g \rho(g)(v)$$

bzw. jedem $R[G]$-Modul M die Darstellung $\rho(g)(v) = g.v$ auf dem R-Modul M zuordnet. Homomorphismen zwischen zwei Strukturen des einen Typs sind automatisch Homomorphismen zwischen den entsprechenden Strukturen des anderen Typs.

Ist R nun ein kommutativer Ring und G eine endliche Gruppe, so gibt es zwei naheliegende Darstellungen über R. Die Erste entspricht $R[G]$ als Linksmodul über sich selbst und wird (erste) *reguläre Darstellung* genannt. Für die Zweite betrachten wir $R[G]$ als Rechtsmodul über sich selbst. Das Dual $(R[G]_{R[G]})^* = \mathrm{Hom}_R(R[G], R)$ ist dann ein $R[G]$-Linksmodul und seine zugehörige Darstellung heißt *zweite reguläre Darstellung*.

Frobenius untersuchte Bedingungen, unter denen diese zwei Darstellungen äquivalent (isomorph) sind, zu diesem Zeitpunkt noch mit der Beschränkung auf endlichdimensionale Vektorräume. Die Ausweitung dieser Methoden auf allgemeine Algebren statt Gruppenalgebren führte dann zum Begriff der Frobeniusalgebra.

Definition 2.2. *Eine* Frobeniusalgebra *ist eine endlichdimensionale Algebra A über einem Körper K mit einem Isomorphismus ${}_AA \cong (A_A)^*$ von A-Linksmoduln.*

Proposition 2.3. *Sei K ein Körper und G eine endliche Gruppe. Dann ist $K[G]$ eine Frobeniusalgebra, d.h. die $K[G]$-Linksmoduln $K[G]$ und $\mathrm{Hom}_K(K[G], K)$ sind isomorph.*

Beweis. Man betrachte die Dualbasis $(g^*)_{g\in G}$ zu $(g)_{g\in G}$ und die K-linearen Bijektionen

$$\psi : K[G] \to \mathrm{Hom}_K(K[G], K) \qquad\qquad \sigma : K[G] \to K[G]$$
$$\psi(g) = g^* \qquad\qquad \sigma(g) = g^{-1}.$$

Es genügt, zu zeigen, dass $\varphi := \psi \circ \sigma$ mit

$$\varphi(\sum_{g\in G} x_g g)(\sum_{g\in G} y_g g) = \psi(\sum_{g\in G} x_{g^{-1}} g)(\sum_{g\in G} y_g g) = \sum_{g\in G} x_{g^{-1}} y_g$$

sogar $K[G]$-linear ist. Für beliebige $x, y, z \in K[G]$ berechnet man direkt

$$\begin{aligned} \varphi(x \cdot y)(z) &= \varphi(\sum_{g,h\in G} x_h y_{h^{-1}g} g)(z) &&= \sum_{g,h\in G} x_h y_{(gh)^{-1}} z_g \\ \varphi(y)(z \cdot x) &= \varphi(y)(\sum_{g,h\in G} z_h x_{h^{-1}g} g) &&= \sum_{g,h\in G} y_{g^{-1}} z_h x_{h^{-1}g}. \end{aligned}$$

Die Permutation $(g, h) \mapsto (h, h^{-1}g)$ von $G \times G$ zeigt, dass beide Ausdrücke gleich sind. □

Dieser Begriff wurde in zwei Richtungen bedeutend verallgemeinert. Die erste Verallgemeinerung betrifft Eigenschaften des Rings A und seiner Moduln: Jede endlichdimensionale K-Algebra A ist auf beiden Seiten noethersch und ihr Dual $(A_A)^*$ ist immer ein injektiver A-Linksmodul.[i] Eine Frobeniusalgebra ist vermöge ihres Isomorphismus ${}_AA \cong (A_A)^*$ also auch ein linksselbstinjektiver Ring. Wir nennen linksnoethersche linksselbstinjektive Ringe *Quasifrobeniusringe*.

Diese überraschenderweise unter $(-)^{op}$ abgeschlossene Klasse von Ringen besteht genau aus den Ringen, für deren Moduln projektiv und injektiv äquivalent sind.[ii] Quasifrobeniusringe spielen in dieser Arbeit nur eine kleine Rolle, werden aber zum Ende von Kapitel 5 eine praktische Anwendung der bewiesenen Ergebnisse liefern.

Die zweite große Verallgemeinerung konzentriert sich stärker auf den Isomorphismus ${}_AA \cong (A_A)^*$ sowie andere Charakterisierungen über Beziehungen zwischen der Algebra A und dem Körper K. Diese Eigenschaften werden auf allgemeine Ringerweiterungen übertragen. An die Stelle von Körpern treten beliebige Ringe, und implizite Eigenschaften wie die Freiheit von A über K und die kompatible K-Vektorraumstruktur werden jeweils mit Projektivität und einer Bimodulstruktur ersetzt. Zuletzt werden noch Automorphismen α des Unterrings miteinbezogen. Auf diese Weise kommen wir zum Begriff der α-Frobeniuserweiterung.

[i] A_A ist projektiv und $\mathrm{Hom}_A(-, A_A)$ induziert eine Äquivalenz von Kategorien $\mathrm{Mod}_A \cong ({}_A\mathrm{Mod})^{op}$.
[ii] Diese Aussage wird in Sätzen 6.15.1 und 6.15.9 von [7] bewiesen.

2.2 Charakterisierungen

Definition 2.4. *Sei $\alpha : R \to R$ ein Ringautomorphismus. Eine Ringerweiterung $R \subset S$ heißt* α-Frobeniuserweiterung*, falls S als R-Linksmodul projektiv und endlich erzeugt ist und es einen (S, R)-Bimodulisomorphismus $\varphi : S \to \mathrm{Hom}_R(S, {}_\alpha R)$ gibt. Die (S, R)-Bimodulstruktur rechts ist dabei durch $(sfr)(x) = f(xs)r$ gegeben. Eine α-Frobeniuserweiterung $R \subset S$ heißt* frei*, wenn S als R-Linksmodul sogar frei ist.*

Beispiel 2.5. Jede Frobeniusalgebra A über einem Körper K ist eine freie id_K-Frobeniuserweiterung. Insbesondere ist mit 2.3 also die Gruppenalgebra $K[G]$ einer endlichen Gruppe eine id_K-Frobeniuserweiterung von K.

Frobeniusalgebren wurden durch die Existenz bestimmter Bilinearformen charakterisiert. Eine ähnliche Charakterisierung existiert für α-Frobeniuserweiterungen. Es ist meist einfacher, eine solche Form zu finden, als einen expliziten Isomorphismus zu konstruieren.

Definition 2.6. *Sei $\alpha : R \to R$ ein Ringautomorphismus. Eine* α-assoziative Form *von S nach R ist eine biadditive Abbildung $\langle -, - \rangle : S \times S \to R$, sodass für alle $r \in R$, $x, y, z \in S$ gilt:*

$$\langle rx, y \rangle = r \langle x, y \rangle \qquad \langle x, yr \rangle = \langle x, y \rangle \alpha(r) \qquad \langle xy, z \rangle = \langle x, yz \rangle$$

Eine solche Form heißt nicht entartet*, wenn $\langle x, S \rangle = 0 \implies x = 0$ und $\langle S, y \rangle = 0 \implies y = 0$ gelten. Umgekehrt heißt sie* entartet*, wenn eine dieser Bedingungen nicht erfüllt ist.*

Bemerkung 2.7. Obwohl sich Bilinearformen für viele Situationen eignen, ist es manchmal praktischer, stattdessen einen sogenannten *Frobeniushomomorphismus* anzugeben. Dies ist ein (R, R)-Bimodulhomomorphismus $\pi : S \to R_\alpha$, also eine additive Abbildung mit

$$\pi(rsr') = r\,\pi(s)\,\alpha(r')$$

für alle $r, r' \in R$ und $s \in S$. Wie man schnell nachprüft, gibt es eine 1:1-Korrespondenz zwischen solchen Homomorphismen von S nach R_α und den α-assoziativen Formen. Dabei definiert π die Form $\langle x, y \rangle = \pi(xy)$, und die Form $\langle -, - \rangle$ definiert π durch $\pi(s) = \langle s, 1 \rangle = \langle 1, s \rangle$. Eine α-assoziative Form ist genau dann entartet, wenn der Kern ihres Frobeniushomomorphismus ein von Null verschiedenes Links- oder Rechtsideal von S enthält.

Definition 2.8. *Sei $\alpha : R \to R$ ein Ringautomorphismus, $\langle -, - \rangle : S \times S \to R$ eine α^{-1}-assoziative Form und $x, y \in S^n$.*

(i) x, y bilden ein duales projektives Paar *bezüglich $\langle -, - \rangle$, wenn*

$$s = \sum_{i=1}^{n} \langle s, y_i \rangle\, x_i = \sum_{i=1}^{n} y_i \cdot \alpha(\langle x_i, s \rangle)$$

für jedes $s \in S$ gilt.

(ii) x, y bilden ein duales freies Paar *bezüglich $\langle -,- \rangle$, wenn*

$$S = \sum_{i=1}^{n} Rx_i = \sum_{i=1}^{n} y_i R$$

gilt und $\langle x_i, y_j \rangle = \delta_{i,j}$ für alle $1 \leq i, j \leq n$ ist.

Ist $x, y \in S^n$ ein duales projektives Paar wie in 2.8 (i), so ist x zusammen mit den Homomorphismen $f_i : {}_RS \to {}_RR$, $f_i(s) = \langle s, y_i \rangle$ eine projektive Basis von ${}_RS$. Zudem ist y zusammen mit den Homomorphismen $g_i : S_R \to R_R$, $g_i(s) = \alpha(\langle x_i, s \rangle)$ eine projektive Basis von S_R. Insbesondere ist S als R-Linksmodul und R-Rechtsmodul projektiv.

Obwohl ein duales freies Paar auf den ersten Blick wie ein anderer Begriff erscheint, ist es tatsächlich ein Spezialfall des dualen projektiven Paars.

Lemma 2.9. *Sei $\alpha : R \to R$ ein Ringautomorphismus, $\langle -,- \rangle : S \times S \to R$ eine α^{-1}-assoziative Form und $x, y \in S^n$. Die folgenden Aussagen sind äquivalent:*

(i) x, y ist ein duales freies Paar bezüglich $\langle -,- \rangle$.

(ii) x, y ist ein duales projektives Paar bezüglich $\langle -,- \rangle$, x ist eine Basis von ${}_RS$, und y ist eine Basis von S_R.

Beweis. (i) $\implies$ (ii): Für jedes $s \in S$ mit $s = \sum_{i=1}^n r_i x_i = \sum_{i=1}^n y_i r_i'$ gilt

$$\sum_{i=1}^{n} \langle s, y_i \rangle x_i = \sum_{i=1} r_i x_i = s, \qquad \sum_{i=1}^{n} y_i \alpha(\langle x_i, s \rangle) = \sum_{i=1} y_i \alpha(\alpha^{-1}(r_i')) = s.$$

Ist $\sum_{i=1}^n r_i x_i = 0 = \sum_{i=1}^n y_i r_i'$, so gilt für jedes $1 \leq j \leq n$

$$r_j = \sum_{i=1}^{n} r_i \langle x_i, y_j \rangle = \left\langle \sum_{i=1}^{n} r_i x_i,\ y_j \right\rangle = 0 = \left\langle x_j,\ \sum_{i=1}^{n} y_i r_i' \right\rangle = \sum_{i=1}^{n} \langle x_j, y_i \rangle \alpha^{-1}(r_i') = \alpha^{-1}(r_j').$$

Da α ein Automorphismus ist, folgt auch $r_j' = 0$.

(ii) $\implies$ (i): Offensichtlich sind x, y Erzeugendensysteme von ${}_RS$ bzw. S_R. Da sie Basen sind, sind die Koeffizienten aus 2.8 (i) eindeutig bestimmt. Setzt man nun x_i bzw. y_j für s ein, folgt $\langle x_i, y_j \rangle = \delta_{i,j}$. □

Lemma 2.10. *Seien $x, y \in S^n$ mit $S = \sum_{i=1}^n Rx_i = \sum_{i=1}^n y_i R$ und $\langle -,- \rangle : S \times S \to R$ eine α^{-1}-assoziative Form. Die folgenden Eigenschaften sind äquivalent.*

(i) x, y bilden ein duales projektives Paar bezüglich $\langle -,- \rangle$.

(ii) Die Matrix $A \in M_n(R)$ mit $A_{i,j} = \langle x_i, y_j \rangle$ ist idempotent und $\langle -,- \rangle$ ist nicht entartet.

Beweis. Ein direkte Rechnung zeigt

$$(A^2)_{i,j} = \sum_{k=1}^{n} \langle x_i, y_k \rangle \langle x_k, y_j \rangle = \left\langle x_i, \sum_{k=1}^{n} y_k \alpha(\langle x_k, y_j \rangle) \right\rangle = \left\langle \sum_{k=1}^{n} \langle x_i, y_k \rangle x_k, y_j \right\rangle.$$

Ist x, y also ein projektives Paar, so ist A idempotent. Gilt jeweils $\langle s, S\rangle = 0$ oder $\langle S, s'\rangle = 0$, so folgt $s = \sum_{i=1}^n \langle s, y_i\rangle x_i = 0$ bzw. $s' = \sum_{i=1}^n y_i\alpha(\langle x_i, s'\rangle) = 0$, weshalb $\langle -, -\rangle$ nicht entartet ist. Ist umgekehrt A idempotent, folgt aus der Rechnung zu Beginn

$$\left\langle x_i, y_j - \sum_{k=1}^n y_k\alpha(\langle x_k, y_j\rangle)\right\rangle = 0 = \left\langle x_i - \sum_{k=1}^n \langle x_i, y_k\rangle x_k, y_j\right\rangle$$

für alle $i, j = 1 \ldots n$. Ist $\langle -, -\rangle$ also nicht entartet, gilt die Gleichung in 2.8 (i) für alle x_i und y_j. Aus Linearität und $S = \sum_{i=1}^n Rx_i = \sum_{j=1}^n y_jR$ folgt dann, dass x, y ein duales projektives Paar bezüglich $\langle -, -\rangle$ bilden. □

Satz 2.11. *Sei $R \subset S$ eine Ringerweiterung und $\alpha : R \to R$ ein Ringautomorphismus. Die folgenden Aussagen sind äquivalent:*

(i) $R \subset S$ ist eine α-Frobeniuserweiterung.

(ii) Es existiert ein duales projektives Paar $x, y \in S^n$ bezüglich einer α^{-1}-assoziativen Form $\langle -, -\rangle : S \to R$.

(iii) Es existieren eine nichtentartete α^{-1}-assoziative Form $\langle -, -\rangle : S \times S \to R$, Elemente $x, y \in S^n$, und zwei Matrizen $P, Q \in M_n(R)$, die folgende Eigenschaften erfüllen:

(a) P ist linksinvertierbar und Q ist rechtsinvertierbar.

(b) PAQ mit $A_{i,j} = \langle x_i, y_j\rangle$ ist idempotent.

(c) $S = \sum_{i=1}^n Rx_i = \sum_{i=1}^n y_iR$.

Beweis. (i) $\implies$ (ii): Sei $\varphi : S \to \mathrm{Hom}_R(S, {}_\alpha R)$ der (S, R)-Bimodulisomorphismus der Erweiterung und $\langle x, y\rangle := \alpha^{-1}(\varphi(y)(x))$. Dies ist eine α^{-1}-assoziative Form, wie man mit der Bimodulstruktur von $\mathrm{Hom}_R(S, {}_\alpha R)$ direkt nachrechnet. Da ${}_RS$ endlich erzeugt und projektiv ist, gibt es eine projektive Basis $x \in S^n$, $f \in \mathrm{Hom}_R(S, R)^n$. Wegen $\alpha \circ f_i \in \mathrm{Hom}_R(S, {}_\alpha R)$ ist

$$y_i := \varphi^{-1}(\alpha \circ f_i) \in S$$

für alle $1 \le i \le n$ wohldefiniert und erfüllt $f_i = \langle -, y_i\rangle$. Für alle $s \in S$ gilt dann wie gefordert

$$s = \sum_{i=1}^n f_i(s)x_i = \sum_{i=1}^n \langle s, y_i\rangle x_i.$$

Wendet man nun $\varphi(s)$ auf die entsprechende Gleichung für ein beliebiges $z \in S$ an, so folgt

$$\varphi(s)(z) = \sum_{i=1}^n \varphi(s)(f_i(z) \cdot x_i) = \sum_{i=1}^n \alpha(f_i(z)) \cdot \varphi(s)(x_i) = \sum_{i=1}^n ((\alpha \circ f_i).\alpha(\langle x_i, s\rangle))(z),$$

also

$$\varphi(s) = \sum_{i=1}^n (\alpha \circ f_i).\alpha(\langle x_i, s\rangle) = \sum_{i=1}^n \varphi(y_i).\alpha(\langle x_i, s\rangle) = \sum_{i=1}^n \varphi(y_i \cdot \alpha(\langle x_i, s\rangle)).$$

Eine Anwendung von φ^{-1} liefert dann die zweite Gleichung in 2.8 (i).

(ii) $\implies$ (iii): Dies ist eine Folge von 2.10. Wir können $P = Q = 1$ setzen.

(iii) $\implies$ (i): Definiere $a, b \in S^n$ durch

$$(a_1, \dots, a_n)^T = P \cdot (x_1, \dots, x_n)^T, \qquad (b_1, \dots, b_n) = (y_1, \dots, y_n) \cdot \alpha(Q).$$

Dabei ist $\alpha(Q)_{i,j} = \alpha(Q_{i,j})$. Die Linksinvertierbarkeit von P zeigt $\sum_{i=1}^n Ra_i = \sum_{i=1}^n Rx_i = S$. Analog zeigt die Rechtsinvertierbarkeit von Q, dass $\alpha(Q)$ rechtsinvertierbar ist und somit auch $\sum_{i=1}^n b_i R = \sum_{i=1}^n y_i R = S$ gilt. Per Konstruktion gilt $\langle a_i, b_j \rangle = (PAQ)_{i,j}$; nach 2.10 ist a, b daher ein duales projektives Paar. Insbesondere ist S ein endlich erzeugter projektiver R-Modul.

Definiere $\varphi : S \to \mathrm{Hom}_R(S, {}_\alpha R)$ durch $\varphi(y)(x) = \alpha(\langle x, y \rangle)$. und $\psi : \mathrm{Hom}_R(S, {}_\alpha R) \to S$ durch $\psi(f) = \sum_{i=1}^n b_i f(a_i)$. Man rechnet direkt nach, dass φ ein Homomorphismus von (S, R)-Bimoduln ist. Für beliebige $s \in S$ und $f \in \mathrm{Hom}_R(S, {}_\alpha R)$ gilt:

$$\begin{aligned}
\psi(\varphi(s)) &= \sum_{i=1}^n b_i \alpha(\langle a_i, s \rangle) = s \\
\varphi(\psi(f))(s) &= \sum_{i=1}^n \alpha(\langle s, b_i f(a_i) \rangle) \\
&= \sum_{i=1}^n \alpha(\langle s, b_i \rangle) f(a_i) \\
&= f\left(\sum_{i=1}^n \langle s, b_i \rangle \, a_i \right) \\
&= f(s)
\end{aligned}$$

Somit ist φ ein Isomorphismus. □

Korollar 2.12. *Sei $R \subset S$ eine Ringerweiterung und $\alpha : R \to R$ ein Ringautomorphismus. Die folgenden Aussagen sind äquivalent:*

(i) $R \subset S$ ist eine freie α-Frobeniuserweiterung.

(ii) Es existiert ein duales freies Paar $x, y \in S^n$ bezüglich einer α^{-1}-assoziativen Form $\langle -, - \rangle : S \to R$.

(iii) Es gibt eine α^{-1}-assoziative Form $\langle -, - \rangle : S \times S \to R$ und $x, y \in S^n$ mit den folgenden Eigenschaften:

(a) Die Matrix $A \in M_n(R)$ mit $A_{i,j} = \langle x_i, y_j \rangle$ ist zweiseitig invertierbar.

(b) $S = \sum_{i=1}^n Rx_i = \sum_{i=1}^n y_i R.$

Beweis. (i) $\implies$ (ii): Seien $x \in S^n$ eine Basis von ${}_R S$, $\pi \in \mathrm{Hom}_R(S, R)^n$ die Projektionen bezüglich dieser Basis, und $\varphi : S \to \mathrm{Hom}_R(S, {}_\alpha R)$ der (S, R)-Bimodulisomorphismus der

Erweiterung. Wie in 2.11 definiere man $\langle x, y\rangle = \alpha^{-1}(\varphi(y)(x))$ und $y_j = \varphi^{-1}(\alpha \circ \pi_j)$ für alle $1 \leq j \leq n$; da x, π eine projektive Basis von ${}_RS$ ist, haben wir dort bereits bewiesen, dass die Form $\langle -, -\rangle$ α^{-1}-assoziativ ist und die y_j ein Erzeugendensystem von S_R bilden. Für alle $1 \leq i, j \leq n$ folgt dann aus direkter Berechnung $\langle x_i, y_j\rangle = \alpha^{-1}(\varphi(y_j)(x_i)) = \pi_j(x_i) = \delta_{i,j}$.

(ii) $\implies$ (iii) ist trivial, da A die Identitätsmatrix ist.

(iii) $\implies$ (i): Die Form kann nicht entartet sein, da A sonst im Widerspruch zur Invertierbarkeit eine Nullzeile oder -spalte enthielte. Dann zeigt 2.11 (iii) mit $P = A^{-1}$, $Q = 1$, dass $R \subset S$ eine α-Frobeniuserweiterung ist. Sei $a, b \in S^n$ das duale projektive Paar aus dem Beweis. Wir haben es so konstruiert, dass $\langle a_i, b_j\rangle = (PAQ)_{i,j}$ gilt; da jedoch $(PAQ)_{i,j} = \delta_{i,j}$ gilt, ist a, b sogar ein duales freies Paar, was nach 2.9 bedeutet, dass ${}_RS$ frei ist. □

2.3 Beispiele und Eigenschaften

Beispiel 2.13. Wir können 2.3 nun stark verallgemeinern. Sei R ein kommutativer Ring, G eine endliche Gruppe, und $H < G$ eine Untergruppe. Dann ist $R[H] \subset R[G]$ eine freie id_R-Frobeniuserweiterung; wir definieren eine id_R-assoziative Form durch den Frobeniushomomorphismus $\pi(\sum_{g\in G} r_g g) = \sum_{h\in H} r_h h$, also die Projektion auf den freien Untermodul $R[H] < R[G]$. Diese ist offensichtlich (R, R)-linear. Ist Ω dann ein Repräsentantensystem von G/H, so bilden $(x)_{x\in\Omega}$ und $(y^{-1})_{y\in\Omega}$ ein duales freies Paar bezüglich π.

Beispiel 2.14. Sei R ein Ring, $n \in \mathbb{N}$ und $S = M_n(R)$ der Matrixring über R. Die Spur $\mathrm{Tr} : S \to R$ ist ein (R, R)-Bimodulhomomorphismus, der eine id_R-assoziative Form definiert (siehe 2.7). Für $1 \leq i, j \leq n$ sei $E_{i,j}$ die Matrix, deren einziger Nichtnulleintrag eine Eins an der Stelle (i, j) ist. Das Produkt $E_{i,j}E_{x,y}$ besitzt höchstens einen Nichtnulleintrag; dieser ist in Zeile i, existiert nur, wenn $x = j$ ist, und liegt dann in Spalte y. Somit ist

$$\mathrm{Tr}(E_{i,j}E_{x,y}) = \begin{cases} 1 & \text{wenn } x = j \text{ und } y = i \\ 0 & \text{sonst.} \end{cases}$$

Die Mengen $(E_{i,j})_{i,j=1\ldots n}$ und $(E_{j,i})_{i,j=1\ldots n}$ bilden also ein duales freies Paar bezüglich Tr, und $M_n(R)$ ist eine freie id_R-Frobeniuserweiterung von R.

Beispiel 2.15 ([8, Example 1])**.** Seien K, L Körper, $S = K \times L \times L$ mit komponentenweiser Addition und Multiplikation, und R der Unterring $\{(k, l, l) \,|\, k \in K, l \in L\}$ von S. Dann ist $R \subset S$ eine id_R-Frobeniuserweiterung vermöge des Frobeniushomomorphismus $\pi((k, l, l')) = (k, l + l', l + l')$. Eine direkte Rechnung zeigt, dass π wirklich (R, R)-linear ist und $x_1 = y_1 = (1, 0, 0)$, $\quad x_2 = y_2 = (0, 1, 0)$, $\quad x_3 = y_3 = (0, 0, 1)$ ein duales projektives Paar bilden. Die Erweiterung ist jedoch nicht frei, da ${}_RS$ nicht frei ist.

Wäre ${}_RS$ frei von Rang n, so wäre für jedes Primideal $\mathfrak{p}$ von R auch die Lokalisierung, der $R_\mathfrak{p}$-Linksmodul $S_\mathfrak{p}$, frei von Rang n. Für $\mathfrak{p} = (0, 1, 1)R$ ist $L \cong R_\mathfrak{p} \hookrightarrow S_\mathfrak{p} \cong L \times L$ die Diagonalabbildung $l \mapsto (l, l)$, also müsste $n = 2$ sein. Doch für $\mathfrak{q} = (1, 0, 0)R$ ist $K \cong R_\mathfrak{q} \xrightarrow{\cong} S_\mathfrak{q}$ die Abbildung $k \mapsto (k, 0, 0)/1$, woraus $n = 1$ folgen würde. Somit kann ${}_RS$ nicht frei sein.

Lemma 2.16. *Für jede α-Frobeniuserweiterung $R \subset S$ ist $R^{op} \subset S^{op}$ eine α^{-1}-Frobeniuserweiterung. Die Erweiterung $R^{op} \subset S^{op}$ ist genau dann frei, wenn die Erweiterung $R \subset S$ frei ist. Insbesondere ist S sowohl als Links- wie auch Rechtsmodul frei, falls $R \subset S$ eine freie α-Frobeniuserweiterung ist.*

Beweis. Es bezeichne $\cdot$ die Multiplikation in S und $*$ die Multiplikation in S^{op}. Nach 2.11 (2.12) existiert eine α^{-1}-assoziative Form $\langle -,-\rangle : S \times S \to R$ mit zugehörigem projektivem (freiem) dualen Paar $x, y \in S^n$. Dann ist $[-,-] : S^{op} \times S^{op} \to R^{op}$ mit $[x,y] = \alpha(\langle y, x\rangle)$ eine α-assoziative Form, denn für alle $r \in R$, $x, y, s \in S$ gilt:

$$\begin{aligned}[r*x, y] &= \alpha(\langle y, x\cdot r\rangle) \\ &= \alpha(\langle y, x\rangle \cdot \alpha(r)^{-1}) \\ &= \alpha(\langle y, x\rangle)\cdot r \\ &= r * [x,y]\end{aligned} \qquad \begin{aligned}[x, y*r] &= \alpha(\langle r\cdot y, x\rangle) \\ &= \alpha(r\cdot \langle y, x\rangle) \\ &= \alpha(r)\cdot\alpha(\langle y, x\rangle) \\ &= [x,y]*\alpha(r)\end{aligned} \qquad \begin{aligned}[x*s, y] &= \alpha(\langle y, s\cdot x\rangle) \\ &= \alpha(\langle y\cdot s, x\rangle) \\ &= \alpha(\langle s*y, x\rangle) \\ &= [x, s*y]\end{aligned}$$

Das zu $[-,-]$ gehörige projektive (freie) duale Paar ist y, x, denn für alle $s \in S$ gilt im projektiven Fall

$$s = \sum_{i=1}^n y_i \alpha(\langle x_i, s\rangle) = \sum_{i=1}^n [s, x_i] * y_i, \qquad s = \sum_{i=1}^n \langle s, y_i\rangle\, x_i = \sum_{i=1}^n x_i * \alpha([y_i, s])$$

und im freien Fall $[y_i, x_j] = \alpha(\langle x_j, y_i\rangle) = \alpha(\delta_{ij}) = \delta_{ij}$ sowie

$$S = \sum_{i=1}^n Rx_i = \sum_{i=1}^n x_i * R^{op}, \qquad S = \sum_{i=1}^n y_i S = \sum_{i=1}^n S^{op} * y_i.$$

Also ist $R^{op} \subset S^{op}$ eine (freie) α^{-1}-Frobeniuserweiterung. Die zweite Bemerkung des Lemmas folgt aus erneutem Übergang zu Gegenringen; die Dritte folgt aus der Korrespondenz zwischen R^{op}-Linksmoduln und R-Rechtsmoduln oder 2.12. □

Lemma 2.16 übersetzt sich unmittelbar in das folgende Korollar.

Korollar 2.17. *Sei $\alpha : R \to R$ ein Ringautomorphismus und $R \subset S$ eine Ringerweiterung. Die folgenden Aussagen sind äquivalent:*

(i) $R \subset S$ ist eine α-Frobeniuserweiterung, d.h. S ist als R-Linksmodul endlich erzeugt und projektiv und es gibt einen (S,R)-Bimodulisomorphismus $S \cong \mathrm{Hom}_R(S, {}_\alpha R)$.

(ii) S ist als R-Rechtsmodul endlich erzeugt und projektiv und es gibt einen (R,S)-Bimodulisomorphismus $S \cong \mathrm{Hom}_R(S, R_{\alpha^{-1}})$.

Wir haben α-Frobeniuserweiterungen ursprünglich über Eigenschaften von Linksmoduln definiert. Korollar 2.17 zeigt, dass wir ohne Verluste auch Rechtsmoduln verwenden könnten, solange wir von α abhängige Konstruktionen durch Konstruktionen mit α^{-1} ersetzen. Dadurch sind einige von α unabhängige Ergebnisse automatisch symmetrisch – dies ist insbesondere bei folgendem Satz der Fall.

Satz 2.18. *Sei $R \subset S$ eine freie α-Frobeniuserweiterung. Dann ist $\mathrm{id}_R\,({}_R R) = \mathrm{id}_S\,({}_S S)$ und $\mathrm{id}_R\,(R_R) = \mathrm{id}_S\,(S_S)$.*

Beweis. [9, Lemma 5.3] Sei N ein R-Linksmodul mit einer projektiven Auflösung $N_* \to N$. Betrachte den Komplex $S \otimes_R N_*$; nach 2.17 ist S_R projektiv, also ist dieser Komplex exakt.

Er ist sogar eine Auflösung von $S \otimes_R N$ durch projektive S-Linksmoduln, da eine natürliche Äquivalenz $\mathrm{Hom}_S(S \otimes_R N_*, -) \cong \mathrm{Hom}_R(N_*, \mathrm{Hom}_S(S, -))$ existiert und ${}_R(N_*)$ sowie ${}_S S$ projektiv sind. Dann folgt

$$\begin{aligned}
\mathrm{Ext}_S^r(S \otimes_R N, S) &\cong H_r(\mathrm{Hom}_S(S \otimes_R N_*, S)) \\
&\cong H_r(\mathrm{Hom}_R(N_*, \mathrm{Hom}_S(S, S))) \\
&\cong \mathrm{Ext}_R^r(N, \mathrm{Hom}_S(S, S)) \\
&\cong \mathrm{Ext}_R^r(N, S) \\
&\cong \mathrm{Ext}_R^r(N, R)^n
\end{aligned}$$

aus der Tensor-Hom-Adjunktion und dem Isomorphismus $R^n \cong S \cong \mathrm{Hom}_S(S, S)$, der jedem $s \in S$ seine Rechtsmultiplikation zuordnet. Für $r > \mathrm{id}_S(S)$ verschwindet $\mathrm{Ext}_S^r(S \otimes_R N, S)$ (vgl. 1.2), also verschwindet auch $\mathrm{Ext}_R^r(N, R)$. Aus 1.2 folgt dann $\mathrm{id}_R(R) \leq \mathrm{id}_S(S)$.

Umgekehrt sei M ein S-Linksmodul mit projektiver Auflösung $M_* \to M$. S-lineare Abbildungen sind auch R-linear und S-projektive Moduln sind R-projektiv, da ${}_R S$ frei ist. Also ist $M_* \to M$ auch eine projektive Auflösung als R-Modul. Dann gilt

$$\begin{aligned}
\mathrm{Ext}_S^r(M, S) &\cong H_r(\mathrm{Hom}_S(M_*, S)) \\
&\cong H_r(\mathrm{Hom}_S(M_*, \mathrm{Hom}_R(S, {}_\alpha R))) \\
&\cong H_r(\mathrm{Hom}_R(S \otimes_S M_*, {}_\alpha R)) \\
&\cong H_r(\mathrm{Hom}_R(M_*, {}_\alpha R)) \\
&\cong \mathrm{Ext}_R^r(M, {}_\alpha R) \\
&\cong \mathrm{Ext}_R^r(M, R),
\end{aligned}$$

wobei man im letzten Schritt benutzt, dass $\alpha : R \to {}_\alpha R$ ein R-Modulisomorphismus ist. Verschwindet also $\mathrm{Ext}_R^r(M, R)$, verschwindet auch $\mathrm{Ext}_S^r(M, R)$, d.h. $\mathrm{id}_R(R) \geq \mathrm{id}_S(S)$ nach 1.2. Somit ist die linksselbstinjektive Dimension beider Ringe gleich. Die Aussage über die rechtsselbstinjektive Dimension folgt, indem man den Satz auf $R^{op} \subset S^{op}$ anwendet (vgl. 2.16). □

Insbesondere ist eine Frobeniuserweiterung über einem selbstinjektiven Ring auch selbstinjektiv. Zum Abschluss des Kapitels wenden wir diesen Satz auf Gruppenringe endlicher Gruppen über Quasifrobeniusringen an, um zu zeigen, dass diese selbst Quasifrobeniusringe sind. Dafür benötigen wir das folgende Lemma.

Lemma 2.19. *Sei R ein linksnoetherscher Ring und $\varphi : R \to S$ ein Ringhomomorphismus, sodass der R-Linksmodul $\varphi^* S$ endlich erzeugt ist. Dann ist auch S linksnoethersch.*

Beweis. Jedes Ideal I von S ist ein R-Untermodul von $\varphi^* S$, also endlich erzeugt über R und damit über S. □

Per Übergang zu den Gegenringen folgt die analoge Aussage für rechtsnoethersche Ringe.

Korollar 2.20. *Ist G eine endliche Gruppe und R ein kommutativer noetherscher Ring, dann ist $R[G]$ links- und rechtsnoethersch.*

Aus Beispiel 2.13, Satz 2.18 und Korollar 2.20 erhalten wir nun das folgende Resultat.

Korollar 2.21. *Ist G eine endliche Gruppe und R ein Quasifrobeniusring, so ist $R[G]$ auch ein Quasifrobeniusring.*

3 Coxetersysteme

Coxetersysteme beschreiben eine Gruppe W durch ein Erzeugendensystem selbstinverser Elemente S und verallgemeinern damit euklidische Spiegelungsgruppen. Tatsächlich sind die endlichen Spiegelungsgruppen genau die endlichen Gruppen, die ein Coxetersystem zulassen (siehe z.B. [6, Kapitel 6.4]). Wir interessieren uns in diesem Kapitel nur eingeschränkt für Eigenschaften eines Coxetersystems selbst und mehr für seine Verbindung zu einem bestimmten System von Vektoren, die wir später in Kapitel 4 benutzen werden. Unsere Behandlung, die sich im Wesentlichen an [6, Kapitel 5] orientiert, ist daher unvollständig und verweist für manche Beweise nur auf die Literatur.

3.1 Einfache Eigenschaften

Definition 3.1. *Sei W eine Gruppe und $S \subset W$ ein endliches System von Erzeugern der Ordnung 2. Für $s, s' \in S$ bezeichne $m(s, s') \in \mathbb{N} \cup \{\infty\}$ die Ordnung von ss'. Das Tupel (W, S) heißt* Coxetersystem*, wenn folgende Eigenschaften erfüllt sind:*

(i) Für $s, s' \in S$ mit $s \neq s'$ gilt $m(s, s') = m(s', s) \geq 2$.

(ii) Die Erzeuger S und Relationen $(ss')^{m(s,s')} = 1$ bilden eine Präsentation von W, d.h. jede Abbildung von Mengen $f : S \to G$ in eine Gruppe G mit $(f(s)f(s'))^{m(s,s')} = 1$ ist eindeutig zu einem Gruppenhomomorphismus $W \to G$ erweiterbar.

Die Kardinalität von S ist der Rang *des Coxetersystems.*

In diesem Kapitel ist (W, S) stets ein beliebiges Coxetersystem. Falls nicht anders definiert, sind $v, w \in W$ und $s, s' \in S$. Ist das Erzeugendensystem S aus dem Kontext klar, nennen wir W auch einfach *Coxetergruppe*. Dabei ist jedoch zu beachten, dass eine Coxetergruppe W mehrere Erzeugendensysteme S zulassen kann. Im Fall von Spiegelungsgruppen steht $m(s, s')$ in Beziehung zum Winkel zwischen den Spiegelungsachsen der Spiegelungen s, s'.

Bemerkung 3.2. Für selbstinverse s, s' und $m \in \mathbb{N}$ lässt sich $(ss')^m = 1$ auch als

$$ss's \ldots = s'ss' \ldots$$

ausdrücken, wobei auf jeder Seite ein Produkt von m Elementen steht. Diese Beziehung wird *Zopfrelation* genannt und ist für konkrete Berechnungen sehr nützlich. Intuitiv lässt sich ein Coxetersystem auch als Gruppe auffassen, in der jede Relation aus den Zopfrelationen hergeleitet werden kann.

Beispiel 3.3. Das einzige Coxetersystem von Rang 1 ist $\mathbb{Z}/2\mathbb{Z}$.

Beispiel 3.4. Die Präsentation der symmetrischen Gruppe $\mathfrak{S}_n$ am Ende von Kapitel 1.2 erfüllt offensichtlich die Axiome eines Coxetersystems.

Beispiel 3.5. Für $m \in \mathbb{N}$ sei D_{2m} die Untergruppe von $\mathrm{GL}_2(\mathbb{R})$, erzeugt von zwei Spiegelungen a, b, deren Spiegelungsgeraden im Winkel π/m zueinander stehen. Das Produkt ab ist eine Rotation um $2\pi/m$ und besitzt Ordnung m. D_{2m} heißt *Diedergruppe der Ordnung* $2m$.

Sei (W, S) ein Coxetersystem vom Rang 2 mit $S = \{s, s'\}$ und $m(s, s') = m$. Da die Spiegelungen a, b selbstinvers sind, existiert ein Gruppenhomomorphismus $f : W \to D_{2m}$ mit $f(s) = a$ und $f(s') = b$. Er ist surjektiv, weil das gesamte Erzeugendensystem von D_{2m} im Bild liegt, und injektiv, weil W höchstens $2m$ Elemente enthält; jedes $w \in W$ ist nämlich von der Form $(ss')^k$ oder $(ss')^k s$ für $0 \leq k < m$.

Somit ist jedes endliche Coxetersystem vom Rang 2 eine Diedergruppe.

Da Coxetersysteme durch Präsentationen charakterisiert werden, liegt es nahe, dass es eine engere Verbindung zwischen der Gruppenstruktur und den Darstellungen als Wort in S gibt. Dies äußert sich unter anderem im fundamentalem Begriff der Länge.

Definition 3.6. *Seien $w \in W$ und $s_1, \ldots, s_n \in S$. Ist $s_1 \ldots s_n = w$, so heißt das Wort $\vec{s} := (s_1, \ldots, s_n)$* Darstellung *von w. Besitzt $\vec{s}$ minimale Länge unter den Darstellungen von w, so ist $\vec{s}$ eine sogenannte* reduzierte Darstellung. *Die* Länge *von w ist die Länge seiner reduzierten Darstellungen und wird mit $\ell(w)$ bezeichnet, wobei nach Konvention $\ell(1) = 0$ ist.*

Die Abbildung von Mengen $S \to \{\pm 1\}$, die jedes $s \in S$ auf -1 abbildet, lässt sich eindeutig zu einem Homomorphismus $\varepsilon : W \to \{\pm 1\}$ fortsetzen, welcher in Spiegelungsgruppen mit der Determinante übereinstimmt und in Anlehnung an 3.4 *Signatur* genannt wird. Sein Kern ist die sogenannte *alternierende Untergruppe* von W. Ist $w = s_1 \ldots s_{\ell(w)}$ eine reduzierte Darstellung eines $w \in W$, so gilt $\varepsilon(w) = (-1)^{\ell(w)}$. Daraus folgt zum einen, dass alle Darstellungen von w die selbe Parität haben, und zum anderen, dass $\ell(sw) \neq \ell(w)$ und $\ell(ws) \neq \ell(w)$ gelten, da $\varepsilon(ws) = \varepsilon(sw) = -\varepsilon(w)$ ist.

Proposition 3.7. *Seien $v, w \in W$ und $s, s_1, \ldots, s_n \in S$. Für die Längenfunktion gilt:*

(i) $w = s_1 \ldots s_n \implies \ell(w) \leq n$

(ii) $\ell(w) = \ell(w^{-1})$

(iii) $\ell(wv) \leq \ell(w) + \ell(v)$

(iv) $\ell(wv) \geq |\ell(w) - \ell(v)|$

(v) $\ell(ws) = \ell(w) \pm 1$

Beweis. (i) ist trivial. Für (ii) sei $w = s_1 \ldots s_{\ell(w)}$ eine reduzierte Darstellung. Dann ist $w^{-1} = s_{\ell(w)} \ldots s_1$ eine Darstellung und damit $\ell(w^{-1}) \leq \ell(w)$ für alle w nach (i). Wendet man dies auf w^{-1} anstelle von w an, ergibt sich die andere Ungleichung.

Sind $w = s_1 \ldots s_q$ und $v = s'_1 \ldots s'_p$ reduzierte Darstellungen, so ist $wv = s_1 \ldots s_q s'_1 \ldots s'_p$ wieder eine Darstellung; somit folgt (iii) aus (i).

Setzt man in (iii) wv und v^{-1} für w und v ein, so folgt $\ell(w) \leq \ell(wv) + \ell(v^{-1}) \overset{(ii)}{=} \ell(wv) + \ell(v)$. Andersherum erhält man mit w^{-1} und wv die Ungleichung $\ell(v) \leq \ell(w) + \ell(wv)$, womit (iv) gezeigt ist. Zuletzt folgt (v) aus (iii) und (iv), indem man s für v einsetzt und $\ell(ws) = \ell(w)$ mithilfe der Signatur ausschließt. $\square$

Diese Eigenschaften machen Coxetergruppen zur natürlichen Umgebung für Induktionsargumente. Nichttriviale Elemente lassen sich immer durch ein $s \in S$ verkürzen, indem man für $w \in W$ mit $\ell(w) = n > 0$ eine Darstellung $w = s_1 \dots s_n$ wählt und $s = s_n$ setzt; aus 3.7 (i) und (v) folgt dann $\ell(ws_n) = n - 1$, was eine Induktion über $\ell(w)$ ermöglicht.

Die scheinbare Asymmetrie von 3.7 (v) bezüglich der Position von s auf der rechten Seite trügt. Da die Aussage für alle $w \in W$ gilt, gilt sie insbesondere auch für w^{-1}; mit 3.7 (ii) folgt dann

$$\ell(sw) = \ell(w^{-1}s) = \ell(w^{-1}) \pm 1 = \ell(w) \pm 1.$$

Viele Sätze über Coxetersysteme beschreiben, wie sich eine Konstruktion beim Übergang von w zu längerem ws verhält. Wir erhalten dann mit diesem Argument stets eine analoge Aussage für den Übergang von w zu längerem sw. Das folgende Lemma hilft bei induktiven Verallgemeinerungen solcher Aussagen.

Lemma 3.8. *Seien $v, w \in W$ mit $\ell(vw) = \ell(v) + \ell(w)$ und $\ell(w) > 0$. Dann gibt es ein $s \in S$ mit $\ell(ws) = \ell(w) - 1$ und $\ell(vws) = \ell(vw) - 1 = \ell(v) + \ell(ws)$.*

Beweis. Seien $v = s_1 \dots s_p$ und $w = s'_1 \dots s'_q$ reduzierte Darstellungen und $s = s'_q$. Dann ist $ws = s'_1 \dots s'_{q-1}$ reduziert, also $\ell(ws) = \ell(w) - 1$. Darüber hinaus ist $vws = s_1 \dots s_p s'_1 \dots s'_{q-1}$ reduziert, also gilt $\ell(vws) = \ell(vw) - 1 = \ell(v) + \ell(w) - 1 = \ell(v) + \ell(ws)$. □

3.2 Das Wurzelsystem

Wir entwickeln die meisten Eigenschaften von Coxetersystemen (W, S) anhand eines Systems von Vektoren, auf denen W wirkt. Sei V der $\mathbb{R}$-Vektorraum auf S mit Basisvektoren v_s und $[-,-]$ die eindeutig bestimmte symmetrische Bilinearform mit

$$[v_s, v_{s'}] = \begin{cases} -\cos(\frac{\pi}{m(s,s')}) & \text{falls } m(s,s') < \infty \\ -1 & \text{falls } m(s,s') = \infty. \end{cases}$$

Man vergleiche dies mit der Interpretation von $m(s, s')$ über Winkel im Fall von Spiegelungsgruppen. Wir nennen Vektoren mit $[v, w] = 0$ *orthogonal* und Abbildungen der Form

$$\sigma_v(x) = x - 2\frac{[x, v]}{[v, v]}v$$

Spiegelungen bezüglich v. Eine lineare Abbildung heißt *orthogonal*, wenn sie $[-,-]$ erhält; eine direkte Rechnung zeigt, dass Spiegelungen orthogonal sind. Wir rechtfertigen diese Terminologie damit, dass sie für endliche W ihre üblichen Bedeutungen besitzt (vgl. [6, Kapitel 6.4]) und wir in erster Linie am endlichen Fall interessiert sind.

Proposition 3.9. *Für jedes $s \in S$ sei $\sigma(s)$ die Spiegelung bezüglich des Einheitsvektors $v_s \in V$. Die Abbildung $s \mapsto \sigma(s)$ setzt sich zu einer Darstellung $\sigma : W \to \mathrm{GL}(V)$ fort.*

Beweis. Diese Aussage ist Gegenstand von [6, Kapitel 5.3] und wird im Wesentlichen durch Reduktion auf den zweidimensionalen Fall und Diedergruppen bewiesen. □

Da alle $\sigma(s)$ orthogonal sind, sind alle $\sigma(w)$ dies auch.

Definition 3.10. *Das* Wurzelsystem *von* (W, S) *ist die Menge* $\Phi = \{\sigma(w)(v_s) \mid w \in W, s \in S\}$ *aller Bilder der Basisvektoren unter* W. *Jede Wurzel* $r \in \Phi$ *ist eindeutig als Linearkombination der* v_s *darstellbar;* r *heißt* positiv *(bzw.* negativ*), wenn alle Koeffizienten nichtnegativ (bzw. nichtpositiv) sind.*

Per Definition ist $w.r := \sigma(w)(r)$ eine Wirkung von W auf Φ. Mit Φ^+, Φ^- bezeichnen wir jeweils die Mengen der positiven und negativen Wurzeln. Offensichtlich sind sie disjunkt und wir schreiben statt $r \in \Phi^+$ und $r \in \Phi^-$ auch jeweils suggestiv $r > 0$ oder $r < 0$. Für alle $s \in S$ gilt per Definition $v_s > 0$.

Satz 3.11. *Für alle* $w \in W$ *und* $s \in S$ *gilt:*

$$\begin{aligned} \ell(ws) > \ell(w) &\iff w.v_s > 0 \\ \ell(ws) < \ell(w) &\iff w.v_s < 0 \end{aligned}$$

Beweis. Diese (keineswegs triviale) Aussage wird in [6, Kapitel 5.4] bewiesen. □

Daraus folgt, dass die Abbildung $\sigma : W \to \mathrm{GL}(V)$ injektiv ist und wir W mit $\sigma(W)$ identifizieren können. Aus $\sigma(w) = 1$ folgt nämlich $w.v_s > 0$ und somit $\ell(ws) > \ell(w)$ für alle $s \in S$; für $w \neq 1$ mit reduzierter Darstellung $s_1 \dots s_n$ wäre aber $ws_n = s_1 \dots s_{n-1}$ und somit $\ell(ws_n) < \ell(w)$, weshalb $w = 1$ sein muss.

Satz 3.11 impliziert auch $\Phi = \Phi^+ \sqcup \Phi^-$, also dass jede Wurzel entweder positiv oder negativ ist. Ist $r > 0$, aber $w.r < 0$ (oder umgekehrt), sagen wir, dass *w das Vorzeichen von r ändert*. Durch die Verbindung zur Längenfunktion wird bereits deutlich, dass die von w verursachten Vorzeichenwechsel algebraische Informationen über w liefern. Um diese Vorzeichenwechsel zu untersuchen, betrachten wir Spiegelungen bezüglich Wurzeln.

Ist $\alpha = w.v_s \in \Phi$ eine Wurzel und σ_α die Spiegelung bezüglich α, so gilt

$$\begin{aligned} \sigma_\alpha(x) &= x - 2\,[x, w.v_s]\, w.v_s \\ &= w.(w^{-1}.x) - 2\left[w^{-1}.x, v_s\right] w.v_s \\ &= w.(s.(w^{-1}.x)). \end{aligned}$$

Schreiben wir $R := \{wsw^{-1} \mid w \in W, s \in S\}$, liegen also alle Spiegelungen bezüglich einer Wurzel in R, und ebenso ist jedes $t = wsw^{-1} \in R$ die Spiegelung bezüglich der Wurzel $w.v_s$. Sind $r, r' \in \Phi$ zwei Wurzeln mit gleichen Spiegelungen $\sigma_r = \sigma_{r'}$, so erhält man durch Einsetzen von r unter Verwendung von $[r, r] = 1$ die Gleichung $r = [r, r']\, r'$. Da alle Wurzeln Einheitsvektoren sind und damit $\mathbb{R}r \cap \Phi = \{r, \sigma_r(r)\} = \{\pm r\}$ gilt, ist dann jedes $t \in R$ die Spiegelung bezüglich genau einer positiven Wurzel, d.h. es gibt eine Bijektion $R \to \Phi^+$. Die zu t gehörige Wurzel nennen wir v_t; für $t \in R \cap S$ stimmt das mit unserer Notation für Basisvektoren überein.

Somit hätten wir das Wurzelsystem Φ auch abstrakt als Menge $\{\pm 1\} \times R$ mit einer passenden Wirkung von W definieren können. Dies wird zum Beispiel in [2] getan. Da alle w linear wirken, können wir die Vorzeichenwechsel nun an Φ^+, bzw. an den zu R assoziierten Vektoren, untersuchen.

Definition 3.12. *Für jedes* $w \in W$ *sei*

$$R_w^+ := \{t \in R \mid w.v_t > 0\}, \qquad R_w^- := \{t \in R \mid w.v_t < 0\}.$$

Lemma 3.13. *Für jedes $s \in S$ ist $R_s^- = \{s\}$.*

Beweis. Per Definition ist $s.v_s = -v_s$, also $s \in R_s^-$. Sei $t \in R \setminus \{s\}$ mit $v_t = \sum_{s \in S} \lambda_s v_s > 0$. Die einzige positive Vielfache von v_s in R ist v_s selbst, also muss es mindestens ein $s' \neq s$ mit $\lambda_{s'} > 0$ geben. Da die Wirkung von s aber per Definition nur die s-Komponente beeinflusst, muss $s.v_t$ weiterhin positiv sein. Es gilt also $t \in R_s^+$ und damit $t \notin R_s^-$. □

Als erste Anwendung dieser Maschinerie beweisen wir eine stärkere Version von 3.11.

Lemma 3.14. *Für alle $w \in W$ und $t \in R$ gilt:*

$$\ell(wt) > \ell(w) \iff t \in R_w^+$$
$$\ell(wt) < \ell(w) \iff t \in R_w^-$$

Beweis. Schreibe $t = vsv^{-1}$ mit $s \in S$ und $v \in W$. Dann gilt $\varepsilon(t) = \varepsilon(v)\varepsilon(s)\varepsilon(v^{-1}) = -1$ (vgl. Bemerkung nach 3.6), weshalb $\ell(wt) \neq \ell(w)$ ist. Wir müssen somit nur ($\Longrightarrow$) für beide Äquivalenzen zeigen.

Die erste Implikation beweisen wir per Induktion über $\ell(w)$, wobei der Fall $\ell(w) = 0$ trivial ist. Sei $\ell(w) > 0$ und $s \in S$ mit $\ell(sw) < \ell(w)$. Nach Annahme ist $\ell(wt) > \ell(w)$, womit

$$\ell(swt) \overset{3.7}{\geq} \ell(wt) - 1 > \ell(w) - 1 = \ell(sw)$$

gilt, also folgt induktiv $sw.v_t > 0$. Sollte dann dem Satz entgegen $w.v_t < 0$ sein, müsste wegen $s.v_{wtw^{-1}} = sw.v_t > 0$ also $wtw^{-1} \in R_s^- \overset{3.13}{=} \{s\}$ gelten. Doch $wt = sw$ widerspricht der Ungleichung $\ell(wt) > \ell(w) > \ell(sw)$, weshalb wie gefordert $w.v_t > 0$ (d.h. $t \in R_w^+$) ist.

Für die zweite Implikation wenden wir die erste auf $\ell(wt) < \ell(w) = \ell(wtt)$ an und erhalten $t \in R_{wt}^+$. Daraus folgt $w.v_t = wtt.v_t = wt.(-v_t) = -(wt.v_t) < 0$, also $t \in R_w^-$. □

Korollar 3.15. *Für $w \in W$ und $t \in R$ gilt:*

$$\ell(tw) > \ell(w) \iff t \in R_{w^{-1}}^+$$
$$\ell(tw) < \ell(w) \iff t \in R_{w^{-1}}^-$$

Beweis. Dies folgt durch Einsetzen von w^{-1} in 3.14, da $\ell(tw) = \ell(w^{-1}t)$ ist. □

Wir stellen nun konkrete Beziehungen zwischen verschiedenen $R_w^\pm$ her; diese werden in Kapitel 4 zu Zerlegungen von Gruppen verallgemeinert. Ebenfalls erhalten wir eine geometrische Interpretation der Länge $\ell(w)$ – diese beschreibt genau, wie viele Vorzeichen w umkehrt.

Lemma 3.16. *Sei $w \in W$ und $s \in S$. Ist $\ell(ws) > \ell(w)$, so gilt $R_{ws}^- = \{s\} \sqcup (R_w^-)^s$.*

Beweis. ($\subset$): Sei $t \in R_{ws}^-$. Im Fall $t = s$ ist nichts zu zeigen, also sei $t \neq s$. Dann ist

$$w.v_{sts} = ws.v_t < 0,$$

also gilt $t^s \in R_w^-$ und damit auch $t \in (R_w^-)^s$.

($\supset$): Da $\ell(wss) = \ell(w) < \ell(ws)$ ist, folgt $s \in R_{ws}^-$ aus 3.14. Sei $t \in R_w^-$, also $t^s \in (R_w^-)^s$, mit $t \neq s$. Dann ist auch $t^s \neq s$ und aus $ws.v_{sts} = w.v_t < 0$ folgt $t^s \in R_{ws}^-$.

Zuletzt folgt $s \in R_w^+$ aus 3.14, also ist $s = s^s \notin (R_w^-)^s$ und die Vereinigung ist disjunkt. □

Satz 3.17. *Für jedes $w \in W$ ist $|R_w^-| = \ell(w)$.*

Beweis. Wir führen eine Induktion über $\ell(w)$ durch, wobei der Fall $\ell(w) = 0$ trivial ist und der Fall $\ell(w) = 1$ aus 3.13 folgt. Ansonsten sei $w = vs$ mit $\ell(v) < \ell(w)$. Dann gilt

$$R_w^- = R_{vs}^- \overset{3.16}{=} \{s\} \sqcup (R_v^-)^s,$$

woraus induktiv schließlich $|R_w^-| = 1 + |(R_v^-)^s| = 1 + |R_v^-| = 1 + \ell(v) = \ell(w)$ folgt. □

Satz 3.18. *Seien $v, w \in W$, sodass $\ell(vw) = \ell(v) + \ell(w)$ ist. Dann gilt $R_{vw}^- = R_w^- \sqcup (R_v^-)^w$.*

Beweis. Es genügt wegen 3.17, nur $R_{vw}^- = R_w^- \cup (R_v^-)^w$ zu beweisen. Dies tun wir mit einer Induktion über $\ell(w)$, wobei der Fall $\ell(w) = 0$ trivial ist und der Fall $\ell(w) = 1$ in 3.16 behandelt wurde. Sei $s \in S$ wie in 3.8, sodass mit $w' := ws$ die Längengleichungen

$$\ell(vw) = \ell(vw's) = \ell(vw') + \ell(s), \qquad \ell(vw') = \ell(v) + \ell(w'), \qquad \ell(w) = \ell(w') + \ell(s)$$

gelten. Die Induktionsannahme ergibt dann die Mengengleichungen

$$R_{vw}^- = R_s^- \cup (R_{vw'}^-)^s, \qquad R_{vw'}^- = R_{w'}^- \cup (R_v^-)^{w'}, \qquad R_w^- = R_s^- \cup (R_{w'}^-)^s,$$

aus denen schließlich

$$\begin{aligned} R_{vw}^- &= R_s^- \cup (R_{vw'}^-)^s \\ &= R_s^- \cup (R_{w'}^- \cup (R_v^-)^{w'})^s \\ &= R_s^- \cup (R_{w'}^-)^s \cup (R_v^-)^{w's} \\ &= R_w^- \cup (R_v^-)^w \end{aligned}$$

folgt. □

Zuletzt etablieren wir eine zusätzlich Symmetrie im endlichen Fall, die es uns erlaubt, jedes R_w^- durch ein R_v^+ ausdrücken zu können. Auf diese Weise müssen wir in Kapitel 4 nur Analoga von R_w^+ definieren.

Satz 3.19. *Sei (W, S) ein Coxetersystem. Für $w_0 \in W$ sind folgende Eigenschaften äquivalent:*

(i) *Für alle $w \in W$ ist $\ell(w_0) \geq \ell(w)$.*

(ii) *$R_{w_0}^- = R$.*

(iii) *Für alle $w \in W$ ist $R_w^- = R_{w_0 w}^+$.*

(iv) *Für alle $w \in W$ gilt $\ell(w_0 w) = \ell(w_0) - \ell(w)$.*

Ein w_0 mit den obigen Eigenschaften ist eindeutig bestimmt, selbstinvers und heißt längstes Element *von (W, S). Es existiert genau dann, wenn W endlich ist.*

Beweis. (i) $\implies$ (ii): Sei $w_0 \in W$ ein Element maximaler Länge und $t \in R$ beliebig. Da $\ell(w_0 t) \leq \ell(w_0)$ gilt, folgt $t \in R^-_{w_0}$ aus 3.14.

(ii) $\implies$ (iii): Da w_0 nach Annahme die Vorzeichen aller Wurzeln umkehrt, ist dies trivial.

(iii) $\implies$ (iv): Wegen $R = R^+_1$ gilt

$$\ell(w_0 w) \overset{3.17}{=} \left|R^-_{w_0 w}\right| = \left|R^+_1\right| - \left|R^+_{w_0 w}\right| \overset{\text{(iii)}}{=} \left|R^-_{w_0}\right| - \left|R^-_w\right| \overset{3.17}{=} \ell(w_0) - \ell(w).$$

(iv) $\implies$ (i) ist ebenfalls trivial.

Eindeutigkeit folgt nun aus 3.17 wie folgt: Seien $v, w \in W$ Elemente, welche die vier Eigenschaften (i) - (iv) erfüllen. Eigenschaft (i) impliziert, dass $\ell(v) = \ell(w)$ ist. Dann gilt

$$\ell(vw^{-1}) \overset{\text{(iv)}}{=} \ell(v) - \ell(w^{-1}) = \ell(v) - \ell(w) = 0,$$

also ist $vw^{-1} = 1$, d.h. $v = w$.

Da $\ell(w_0) = \ell(w_0^{-1})$ ist, muss das längste Element w_0 selbstinvers sein. Jedes endliche Coxetersystem enthält offensichtlich ein längstes Element. Umgekehrt liefert ein solches Element eine obere Schranke für $|W|$, denn da S endlich ist, gibt es nur endlich viele Worte in S unter einer festen Länge. □

Korollar 3.20. *Für jedes $w \in W$ mit $n = \ell(w_0) - \ell(w) > 0$ existieren $s_1, \ldots, s_n \in S$, sodass für alle $1 \leq k \leq n$ die Gleichung $\ell(ws_1 \ldots s_k) = \ell(w) + k$ gilt.*

Beweis. Gibt es ein $s \in S$ mit $\ell(ws) > \ell(w)$, so gilt $\ell(ws) = \ell(w) + 1$ nach 3.7 (v) und wir können induktiv fortfahren. Also ist nur zu zeigen, dass w_0 das einzige $w \in W$ ist, das $\ell(ws) < \ell(w)$ für alle $s \in S$ erfüllt. Ist w ein solches Element, folgt $S \subset R^-_w$ aus 3.14. Ist also $r = \sum_{s \in S} \lambda_s v_s \in \Phi^+$ eine positive Wurzel, muss $w.r = \sum_{s \in S} \lambda_s w.v_s$ eine nichtnegative Linearkombination negativer Wurzeln und somit selbst eine negative Wurzel sein. Somit bildet w alle positiven Wurzeln auf negative ab; aus 3.19 (ii) folgt dann $w = w_0$. □

Korollar 3.21. *Für jedes $w \in W$ mit $n = \ell(w_0) - \ell(w) > 0$ existieren $s_1, \ldots, s_n \in S$, sodass für alle $1 \leq k \leq n$ die Gleichung $\ell(s_k \ldots s_1 w) = \ell(w) + k$ gilt.*

Beweis. Man wende das übliche Inversenargument auf 3.20 an und benutze $w_0 = w_0^{-1}$. □

Bemerkung 3.22. Wir erhalten mithilfe des längsten Elements w_0 noch eine andere Form von Symmetrie. Im Fall $\ell(wv) < \ell(w)$ gilt auch

$$\ell(w_0 wv) = \ell(w_0) - \ell(wv) > \ell(w_0) - \ell(w) = \ell(w_0 w).$$

Für Aussagen der Form $\ell(wv) > \ell(w) \implies P(w, v)$ erhalten wir also sofort Aussagen der Form $\ell(wv) < \ell(w) \implies P(w_0 w, v)$, ähnlich wie aus dem Inversenargument.

4 Endliche Gruppen mit zerfallendem BN-Paar

Nach den Vorbereitungen in Kapitel 3 widmen wir uns nun Gruppen mit BN-Paar. Diese Gruppen sind ausgesprochen verbreitet – ein Großteil der einfachen endlichen Gruppen fällt darunter – und in vielen Bereichen der Mathematik spielt die Unterklasse der Gruppen mit zerfallendem BN-Paar eine wichtige Rolle. Wir betrachten in diesem Kapitel diverse Zerlegungen solcher Gruppen in geeignete Untergruppen und Nebenklassen. Diese werden enge Verbindungen zu einem assoziierten Coxetersystem und dessen Wurzelsystem besitzen.

Wir behandeln zunächst BN-Paare im Allgemeinen und beweisen die sogenannte *Bruhat-Zerlegung*, die historisch die Entwicklung von BN-Paaren motivierte (vgl. [4, S.115f]). Inhaltlich folgen wir dabei grob [2] und [4], beschränken uns aber auf das Nötigste – wir gehen nicht auf die sogenannten Gebäude oder detailliert auf die Untergruppenstruktur ein. Danach definieren wir auf Basis von [10, §2-3] Untergruppen, die zu den Mengen $R_w^{\pm}$ aus Kapitel 3.2 analog sind. Die dort bewiesenen Beziehungen zwischen den $R_w^{\pm}$ liefern hier nützliche Zerlegungen in diese Untergruppen. Zuletzt gehen wir in Kapitel 4.3 zu zerfallenden BN-Paaren über und verschärfen die Ergebnisse der vorangehenden Kapitel mithilfe der zusätzlich verfügbaren Struktur. Neben einigen technischen Ergebnissen für Kapitel 5 erhalten wir dabei insbesondere eine starke Form der Bruhat-Zerlegung. Die Hauptreferenz dieses Abschnitts ist [11, §2].

4.1 Allgemeine BN-Paare und die Bruhat-Zerlegung

Definition 4.1. *Eine Gruppe G besitzt ein* BN-Paar*, wenn es zwei Untergruppen $B, N < G$ mit den folgenden Eigenschaften gibt:*

(i) $T := B \cap N$ ist ein Normalteiler von N und die Faktorgruppe $W := N/T$ besitzt ein Erzeugendensystem S, sodass (W, S) ein Coxetersystem ist.

(ii) B und N erzeugen G.

(iii) Für alle $s \in S$ und $w \in W$ gilt $sBw \subset BwB \cup BswB$.

(iv) Für alle $s \in S$ gilt $sBs \not\subset B$.

Wir bezeichnen das Tupel (G, B, N, S) selbst auch als BN-Paar*. Der* Rang *von (G, B, N, S) ist der Rang des Coxetersystems (W, S).*

Man bemerke, dass jedes $w \in W$ zunächst eine Menge der Form mT mit $m \in N$ ist und Axiome (iii) und (iv) somit Aussagen über Produkte von Teilmengen treffen. Da T aber eine Untergruppe von B ist, gilt $Bw = BTm = Bm$; ist $n \in N$ ein Repräsentant von $s \in S$, können wir die Axiome also alternativ auch als $nBm \subset BmB \cup BnmB$ und $nBn \not\subset B$ formulieren. Aus demselben Grund hängt die Konjugation $B^n = n^{-1}Bn$ nicht vom Repräsentanten n, sondern nur von der Klasse w ab. Wir schreiben daher $B^w := B^n$.

Setzt man w^{-1} in Axiom (iii) ein und bildet Inverse, ergibt sich die analoge Aussage $wBs \subset BwB \cup BwsB$. Die Definition eines BN-Paares ist also nicht gerichtet.

Beispiel 4.2. Sei K ein Körper und n eine natürliche Zahl mit $n > 1$. Dann besitzt die allgemeine lineare Gruppe $G = \mathrm{GL}_n(K)$ ein BN-Paar. Alle in diesem Beispiel betrachteten Matrizen seien implizit regulär.

Sei B die Untergruppe der oberen Dreiecksmatrizen und N die Untergruppe der sogenannten *Monomialmatrizen*, d.h. der Matrizen mit genau einem Nichtnulleintrag in jeder Zeile und Spalte. Dann ist $T = B \cap N$ die Untergruppe der Diagonalmatrizen.

Man betrachte den Homomorphismus $N \to \mathfrak{S}_n$, der jeder Monomialmatrix ihre durch Linksmultiplikation assoziierte Zeilenpermutation zuordnet. Dieser ist offensichtlich surjektiv und besitzt T als Kern. Also ist T ein Normalteiler von N und die Faktorgruppe $W = N/T$ ist isomorph zu $\mathfrak{S}_n$. Nach 3.4 ist W eine Coxetergruppe; ihr Erzeugendensystem S besteht aus den Klassen der $n-1$ Permutationsmatrizen, die jeweils zwei aufeinander folgende Zeilen vertauschen und alle anderen erhalten.

Für Axiom (ii) genügt es zu zeigen, dass jede Elementarmatrix von B und N erzeugt werden kann. Die Matrizen für Zeilenskalierung und Zeilenvertauschung sind offensichtlich Elemente von N. Die Matrizen für Zeilenaddition sind hingegen obere oder untere Dreiecksmatrizen; B enthält nur erstere. Ist jedoch $X \in N$ die Permutationsmatrix mit $Xe_i = e_{n-i+1}$ für alle i, prüft man schnell nach, dass Konjugation mit X obere Dreiecksmatrizen zu unteren Dreiecksmatrizen und umgekehrt transformiert. Somit ist auch jede untere Dreiecksmatrix als Produkt von Matrizen aus B und N darstellbar.

Axiom (iv) beweisen wir durch direkte Konstruktion einer Matrix, die in sBs, aber nicht in B liegt. Man repräsentiere s durch die Matrix P, welche die Zeilen i und $i+1$ vertauscht, und wähle eine obere Dreiecksmatrix $A \in B$ mit $A_{i,i+1} \neq 0$. Dann ist $PAP \in sBs$, aber wegen $(PAP)_{i+1,i} = (AP)_{i,i} = A_{i,i+1} \neq 0$ ist $PAP \notin B$.

Axiom (iii) ist involvierter. Zunächst formulieren wir mit $B' := wBw^{-1}$ und Rechtsmultiplikation mit w^{-1} die Bedingung $sBw \subset BwB \cup BswB$ zu

$$sB \subset BB' \cup BsB'$$

um.[iii] Es genügt also zu zeigen, dass jede Matrix $A \in sB$ aus einer Diagonalmatrix oder einer Matrix $M \in s$ entsteht, indem man links mit Matrizen aus B und rechts mit Matrizen aus B' multipliziert – oder äquivalent, dass sich A durch diese Operationen auf Diagonalform oder eine Matrix aus s bringen lässt.

$A \in sB$ ist von der unten gegebenen Form. Da A invertierbar ist, sind alle mit $*$ gekennzeichneten Diagonaleinträge ungleich 0. Durch Linksmultiplikation mit Elementarmatrizen in B kann man A daher auf die Form A' bringen.

$$A = \begin{pmatrix} * & \dots & & & \dots & * \\ & \ddots & & & & \vdots \\ & & 0 & c & \dots & * \\ & & a & b & \dots & * \\ & & & & \ddots & \vdots \\ & & & & & * \end{pmatrix} \qquad A' = \begin{pmatrix} * & & & & & 0 \\ & \ddots & & & & \\ & & 0 & c & & \\ & & a & b & & \\ & & & & \ddots & \\ 0 & & & & & * \end{pmatrix}$$

[iii] Vorsicht: Für das Produkt von Teilmengen gilt $ww^{-1} = T$, nicht $ww^{-1} = \{1\}$.

Im Fall $b = 0$ liegt A in s und wir sind fertig. Sei also ohne Beschränkung der Allgemeinheit $b \neq 0$. Da A' invertierbar ist, gilt $a \neq 0$. Durch Rechtsmultiplikation mit einer der unten gegebenen Matrizen X, X' lässt sich A' jeweils zu einer Matrix aus s oder auf obere Dreiecksform umformen; eine obere Dreiecksmatrix lässt sich dann mithilfe von B auf Diagonalform bringen.

$$X = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & -\frac{b}{a} & & \\ & & 0 & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix} \qquad X' = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & 0 & & \\ & & -\frac{a}{b} & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

Es bleibt also nur noch zu zeigen, dass mindestens eine dieser Matrizen in $B' = wBw^{-1}$ liegt. Sei P die eindeutig bestimmte Permutationsmatrix in w und $\pi \in \mathfrak{S}_n$ ihre assoziierte Zeilenpermutation. X liegt genau dann in B', wenn $P^{-1}XP$ eine obere Dreiecksmatrix ist, also genau dann, wenn $(P^{-1}XP)_{k,l} = X_{\pi(k),\pi(l)} = 0$ für alle $k > l$ gilt. Wie man schnell überprüft, ist dies aufgrund der Struktur von X äquivalent zu $\pi^{-1}(i) < \pi^{-1}(i+1)$. Ein völlig analoges Argument zeigt, dass $X' \in B'$ äquivalent zu $\pi^{-1}(i) > \pi^{-1}(i+1)$ ist. Da stets eine dieser beiden Bedingungen gilt, ist Axiom (iii) gezeigt.

Dieses Beispiel ist in gewisser Weise der Prototyp für BN-Paare. Die in diesem Kapitel bewiesenen Zerlegungen, insbesondere 4.4, besitzen für $\mathrm{GL}_n(K)$ eine sehr anschauliche und bekannte Interpretation; umgekehrt lassen sich diese Zerlegungen als Verallgemeinerungen von Methoden der linearen Algebra auffassen.

Wie man schnell nachprüft, sind Axiome (iii) und (iv) äquivalent zu Aussagen über die Multiplikation von B-Doppelnebenklassen:

$$BsB \cdot BwB \subset BwB \cup BswB \qquad\qquad BsB \cdot BsB \not\subset B1B = B$$

Da $BsBwB$ eine Vereinigung von B-Doppelnebenklassen ist und sw enthält, erhält man für Axiom (iii) sogar die Formulierung

$$BsB \cdot BwB \in \{BswB, BwB \cup BswB\}\,. \tag{*}$$

Wir untersuchen nun etwas genauer, wie die Doppelnebenklassen mit dem Coxetersystem W verbunden sind.

Proposition 4.3. *Seien $s_1, \ldots, s_n \in S$ und $w \in W$. Dann gilt*

$$Bs_1 \ldots s_n BwB \subset \bigcup_{z \in Z} BzwB,$$

wobei Z die Menge aller Teilworte von $s_1 \ldots s_n$ ist.

Beweis. Wir führen eine Induktion über n durch, wobei der Fall $n = 1$ nur eine Umformulierung von Axiom (iii) ist. Sei also $n > 1$, sodass die Proposition für $n-1$ gilt. Wir bezeichnen die Menge der Teilworte von $s_2 \dots s_n$ mit Z'. Dann gilt

$$Bs_1s_2 \dots s_nBwB \subset Bs_1Bs_2 \dots s_nBwB \overset{\text{IA}}{\subset} Bs_1 \cdot \bigcup_{z \in Z'} BzwB = \bigcup_{z \in Z'} Bs_1BzwB.$$

Nach Axiom (iii) ist $Bs_1BzwB \subset BzwB \cup Bs_1zwB$ für jedes $z \in Z'$. Da $z, s_1z \in Z$ sind, ist die Aussage gezeigt. □

Satz 4.4 (Bruhat-Zerlegung)**.** *Man hat die disjunkte Zerlegung*

$$G = \bigsqcup_{w \in W} BwB.$$

Beweis. Es gilt $\bigcup_{w \in W} w = N$, also sind $B, N \subset BWB$. Da BWB unter Inversion und nach 4.3 auch unter Multiplikation abgeschlossen ist, ist es eine Untergruppe von G, die B und N enthält, und somit nach Axiom (ii) bereits gleich G. Es muss dann nur noch gezeigt werden, dass BwB und BvB für verschiedene $w, v \in W$ ungleich und damit disjunkt sind.

Ohne Beschränkung der Allgemeinheit sei $\ell(v) \geq \ell(w)$, sodass wir die Aussage durch Induktion über $\ell(w)$ beweisen können. Im Fall $\ell(w) = 0$, d.h. $w = 1$, sei $n \in N$ mit $v = nT$. Aus $BvB = BwB = B$ folgt dann $n \in B \cap N = T$ und damit $v = 1 = w$.

Nun sei $\ell(v) \geq \ell(w) > 0$ und $v \neq w$. Wähle ein $s \in S$ mit $\ell(sw) = \ell(w) - 1$. Dann gilt

$$\ell(sv) \overset{3.7}{\geq} \ell(v) - 1 \geq \ell(w) - 1 = \ell(sw).$$

Aus $\ell(v) > \ell(sw)$ folgt insbesondere $v \neq sw$. Nach Annahme ist $v \neq w$ und damit auch $sv \neq sw$, was induktiv $BswB \notin \{BvB, BsvB\}$ ergibt. Äquivalenterweise ist

$$BswB \cap BvB = BswB \cap BsvB = \emptyset.$$

Wäre nun $BwB = BvB$, müsste

$$\begin{aligned} BswB &= BswB \cap BsBwB \\ &= BswB \cap BsBvB \\ &\subset BswB \cap (BvB \cup BsvB) \\ &= (BswB \cap BvB) \cup (BswB \cap BsvB) \\ &= \emptyset \end{aligned}$$

gelten, was offensichtlich absurd ist. Also ist $BwB \neq BvB$. □

In unserem prototypischen Beispiel $\mathrm{GL}_n(K)$ besagt dieser Satz, dass jede Matrix A von der Form $A = UPU'$ ist, wobei $U, U' \in B$ obere Dreiecksmatrizen sind und P die eindeutig bestimmte Permutationsmatrix in $w \in W$ mit $A \in BwB$ ist. Stellt man dies nun zu $P^{-1}U^{-1}A = U'$ um, wird deutlich, dass die Bruhat-Zerlegung eine Variante des bekannten Gauß-Eliminationsverfahrens zur Berechnung der Stufenform ist. Zeilen werden dabei nur auf höher liegende Zeilen addiert und erst zum Schluss permutiert. Die Bruhat-Zerlegung verallgemeinert dies auf viele weitere Gruppen.

Lemma 4.5. *Für alle $w \in W$ und $s \in S$ gilt:*

$$\begin{aligned} \ell(sw) > \ell(w) &\iff sBw \subset BswB \\ \ell(sw) < \ell(w) &\iff sBw \cap BwB \neq \emptyset \end{aligned}$$

Beweis. [5, 65.5, 65.6] Es genügt, ($\Longrightarrow$) für beide Äquivalenzen zu zeigen, da aus Axiom (iii) folgt, dass immer genau eine der rechten Aussagen wahr ist.

Für die erste Implikation führen wir eine Induktion über $\ell(w)$ durch, wobei der Fall $\ell(w) = 0$ trivial ist. Im Fall $\ell(w) > 0$ sei $w = vs'$ mit $v \in W$, $s' \in S$, $\ell(w) > \ell(v)$. Im Widerspruch zur Aussage sei $sBvs' = sBw \not\subset BswB$; nach Axiom (iii) muss dann $sBvs' \cap BwB \neq \emptyset$ gelten. Durch Rechtsmultiplikation mit s' erhalten wir

$$\begin{aligned} \emptyset &\neq (sBvs' \cap BwB)s' \\ &= sBv \cap BwBs' \\ &\subset sBv \cap (BwB \cup Bws'B) \\ &= sBv \cap (BwB \cup BvB). \end{aligned}$$

Es gilt $\ell(sv) > \ell(v)$, da sonst $\ell(sw) = \ell(svs') \leq \ell(sv) + 1 = \ell(v) < \ell(w)$ im Widerspruch zur Annahme $\ell(sw) > \ell(w)$ wäre. Induktiv folgt dann

$$\emptyset \neq BsBvB \cap (BwB \cup BvB) = BsvB \cap (BwB \cup BvB),$$

und die Bruhatzerlegung impliziert $sv \in \{w, v\}$. Da $sv = v$ unmöglich ist, muss $sv = w$ sein. Dann ist jedoch $\ell(sw) = \ell(v) < \ell(w)$, was der Annahme des Lemmas widerspricht.

Für die zweite Implikation bemerke man zuerst, dass aus Axiom (iii) $sBs \subset B \cup BsB$ und mit Axiom (iv) $sBs \cap BsB \neq \emptyset$ folgt. Eine Rechtsmultiplikation mit sw liefert dann

$$\emptyset \neq (sBs \cap BsB)sw = sBw \cap BsBsw.$$

Wenden wir nun die erste Implikation auf sw und s an, so erhalten wir $BsBsw \subset BwB$, und es folgt $sBw \cap BwB \neq \emptyset$. □

Mithilfe der Bemerkung vor 4.3 lässt sich Lemma 4.5 zu einer anschaulicheren Aussage über Doppelnebenklassen umformen. In Beweisen ist die ursprüngliche minimale Formulierung jedoch meist leichter anwendbar.

Proposition 4.6. *Für alle $w \in W$ und $s \in S$ gilt:*

$$\begin{aligned} \ell(sw) > \ell(w) &\iff BsBwB = BswB \\ \ell(sw) < \ell(w) &\iff BsBwB = BwB \cup BswB \end{aligned}$$

4.2 Transfer des Wurzelsystems auf B

Die Bruhatzerlegung sowie die Verbindung zwischen Axiom (iii) und der Längenfunktion verdeutlichen, wie stark BN-Paare von der Geometrie des assoziierten Coxetersystems beeinflusst werden. Wie wir in diesem Abschnitt zeigen werden, geht dieser Einfluss noch deutlich weiter. So können wir Analoga der Mengen $R_w^\pm$ aus Kapitel 3.2 innerhalb der Gruppe definieren, die sehr ähnliche Beziehungen untereinander besitzen. Zuletzt finden wir ein System von Untergruppen, auf dem W genau wie auf dem Wurzelsystem wirkt.

Wir nehmen ab hier an, dass W eine endliche Gruppe ist. Alle Ergebnisse treffen damit immer noch ohne Einschränkungen auf Beispiel 4.2 zu.

Definition 4.7. *Für beliebige $w \in W$ und $s \in S$ schreiben wir:*

$$B_w^+ = B \cap B^w \qquad\qquad B_s = B_s^-$$
$$B_w^- = B \cap B^{w_0 w} \qquad\qquad B^- = B_{w_0}^+$$

Wir erinnern daran, dass nach unserer Konvention $B^w = n^{-1}Bn$ für einen beliebigen Repräsentanten n von w gilt und dass w_0 das längste Element von W ist (vgl. 3.19). Wie die Notation suggeriert, nehmen B_w^+ und B_w^- die Rolle der Mengen R_w^+ und R_w^- ein. Die Definition von B_w^- basiert auf der Beziehung $R_w^- = R_{w_0 w}^+$ aus 3.19. B_s entspricht $R_s^- = \{s\}$ und B^- entspricht $R_{w_0}^+ = \emptyset$.

In Beispiel 4.2 mit $G = \mathrm{GL}_n(K)$ ist $B^- = B \cap B^{w_0} = T$. Insofern darf B^- nicht mit der oft verwendeten Notation $\overline{B}$ für die Gruppe der unteren Dreiecksmatrizen verwechselt werden.

Wir beginnen mit einigen technischen Lemmata. Diese schließen hauptsächlich Entartungen aus, entsprechen aber bereits einfachen Aussagen über $R_w^\pm$.

Lemma 4.8. *Seien $w \in W$ und $s \in S$ mit $\ell(sw) > \ell(w)$. Dann gilt $BB^{w^{-1}} \cap B^s \subset B$.*

Beweis. Sei der Aussage entgegen $x \in BB^{w^{-1}} \cap B^s$ aber $x \notin B$. Nach Axiom (iii) gilt $B^s \subset BsB \cup B$, also ist $x \in BB^{w^{-1}} \cap BsB \neq \emptyset$. Nach Rechtsmultiplikation mit w folgt dann

$$\emptyset \neq (BwBw^{-1} \cap BsB)w = BwB \cap BsBw \overset{4.5}{\subset} BwB \cap BswB,$$

was der Bruhat-Zerlegung (4.4) widerspricht. Es ist also tatsächlich $BB^{w^{-1}} \cap B^s \subset B$. □

Korollar 4.9. *Seien $w \in W$ und $s \in S$ mit $\ell(ws) > \ell(w)$. Dann gilt $BB^w \cap B^s \subset B$.*

Lemma 4.10. *Seien $w \in W$ und $s \in S$ mit $\ell(ws) > \ell(w)$. Dann gilt $B = B_s^+ B_w^+ = B_w^+ B_s^+$. Insbesondere folgt mit $w = w_0 s$ die Gleichung $B = B_s B_s^+ = B_s^+ B_s$.*

Beweis. Für den ersten Teil gilt $\supset$ per Definition; für $\subset$ betrachte man

$$B = s(sBw^{-1})w \overset{4.5}{\subset} s(Bsw^{-1}B)w = B^s B^w,$$

wobei 4.5 wegen $\ell(sw^{-1}) = \ell(ws) > \ell(w) = \ell(w^{-1})$ anwendbar ist. Für ein beliebiges $b \in B$ seien nun $b' \in B^s$ und $b'' \in B^w$ mit $b = b'b''$. Dann ist $b' = bb''^{-1} \in BB^w \cap B^s \subset B$ nach 4.9, also gilt $b' \in B_s^+$ und $b'' \in B_w^+$. Es folgt $b = b'b'' \in B_s^+ B_w^+$, was zu zeigen war. □

Lemma 4.11. *Seien $w \in W$ und $s \in S$ mit $\ell(sw) > \ell(w)$. Dann gilt $B_{sw}^+ \subset B_w^+$.*

Beweis. Per Definition ist $B_{sw}^+ \subset B$. Nun konjugiere man die Inklusion

$$(B \cap B^{sw})^{w^{-1}} = B^{w^{-1}} \cap B^s \subset BB^{w^{-1}} \cap B^s \overset{4.8}{\subset} B$$

mit w, um $B_{sw}^+ \subset B^w$ zu erhalten. □

Damit können wir nun beweisen, dass sich $B^- = B^+_{w_0}$ wie $R^+_{w_0} = \emptyset$ und $B_s = B^-_s$ wie die einelementige Menge $R^-_s \overset{3.13}{=} \{s\}$ verhält.

Lemma 4.12. *Ist $w_0 \in W$ das längste Element der Coxetergruppe W, so gilt*

$$\bigcap_{w \in W} B^w = B^-.$$

Insbesondere gelten $(B^-)^w = B^-$ und $B^- \subset B^+_w$ für alle $w \in W$.

Beweis. Für $w \in W$ seien $n = \ell(w_0) - \ell(w)$ und $s_1, \ldots, s_n \in S$ wie in 3.21. Für $k = 0, \ldots, n$ setze man $v_k := s_k \ldots s_1 w$, sodass $v_0 = w$ und $v_n = w_0$ gelten. Dann folgt aus 4.11 sofort $B^- = B^+_{v_n} \subset \ldots \subset B^+_{v_0} = B^+_w$ und es gilt

$$\bigcap_{w \in W} B^w \subset B \cap B^{w_0} = B^- \subset \bigcap_{w \in W} B^+_w = \bigcap_{w \in W} (B \cap B^w) \subset \bigcap_{w \in W} B^w.$$

Die Schlussbemerkungen folgen sofort aus der Hauptaussage. □

Lemma 4.13. *Für jedes $s \in S$ gilt $B_s \neq B^-$.*

Beweis. Wäre $B_s = B^-$, so gälte $B \overset{4.10}{=} B_s B^+_s = B^- B^+_s \overset{4.12}{=} B^+_s \subset B^s$, was nach Konjugation mit s im Widerspruch zu 4.1 (iv) steht. □

Satz 4.14 (vgl. 3.11)**.** *Für alle $w \in W$ und $s \in S$ gilt:*

$$\begin{aligned} \ell(ws) > \ell(w) \quad &\Longleftrightarrow \quad B_s \subset B^+_w \\ \ell(ws) < \ell(w) \quad &\Longleftrightarrow \quad B_s \not\subset B^+_w \text{ und } B_s \cap B^+_w = B^- \end{aligned}$$

Beweis. Da sich die rechten Aussagen gegenseitig ausschließen und immer genau eine linke Aussage wahr ist, genügt es, ($\Longrightarrow$) für beide Äquivalenzen zu zeigen. Für die Erste sei $w_0 s w^{-1} = s_q \ldots s_1$ eine reduzierte Darstellung und $v_j := s_j \ldots s_1 w$ für alle $0 \leq j \leq q$, d.h. $v_0 = w$ und $v_q = w_0 s$. Man bemerke, dass $w = w_0 s$ der Annahme $\ell(ws) > \ell(w)$ widerspricht und somit stets $q > 0$ ist. Dann gilt $\ell(v_j) = \ell(w) + j$ für alle j, da sonst absurderweise

$$\begin{aligned} \ell(w_0) - 1 &= \ell(w_0 s) \\ &= \ell(v_q) \\ &< q + \ell(w) \\ &= \ell(w_0 s w^{-1}) + \ell(w) \\ &= \ell(w_0) - \ell(s w^{-1}) + \ell(w) \\ &= \ell(w_0) + \ell(w) - \ell(ws) \\ &= \ell(w_0) - 1 \end{aligned}$$

wäre. Aus 4.11 folgt dann $B_s = B^+_{w_0 s} = B^+_{v_q} \subset \ldots \subset B^+_{v_0} = B^+_w$.

Für die zweite Implikation bemerke man zunächst, dass $\ell(wss) > \ell(ws)$ ist und deshalb

$$\begin{aligned} B^- &\overset{4.12}{\subset} B \cap B^w \cap B^{w_0 s} \\ &= ((B^s \cap B^{ws}) \cap B^{w_0})^s \\ &\overset{4.9}{\subset} (B \cap B^{w_0})^s \\ &\overset{4.12}{=} B^- \end{aligned}$$

gilt. Es ist also wie gefordert $B^- = B \cap B^w \cap B^{w_0 s} = B_s \cap B_w^+$. Wäre nun $B_s \subset B_w^+$, so würde $B_s = B_s \cap B_w^+ = B^-$ im Widerspruch zu 4.13 folgen. $\square$

Die naheliegende Aussage $\ell(ws) < \ell(w) \iff B_s \subset B_w^-$ ist auch wahr und folgt aus 3.22.

Lemma 4.15. *Seien $w \in W$ und $s \in S$ mit $\ell(ws) > \ell(w)$. Dann gilt $B_{ws}^- = B_s (B_w^-)^s$.*

Beweis. Die Bemerkung nach 4.14 zeigt $B_s \subset B_{ws}^-$, also gilt

$$\begin{aligned} B_{ws}^- &= B \cap B_{ws}^- \\ &\overset{4.10}{=} B_s B_s^+ \cap B_{ws}^- \\ &\overset{1.4}{=} B_s (B_s^+ \cap B_{ws}^-) \\ &= B_s (B \cap B^s \cap B^{w_0 ws}) \\ &= B_s (B^s \cap B \cap B^{w_0 w})^s. \end{aligned}$$

Es ist dann nur noch zu zeigen, dass $(B^s \cap B \cap B^{w_0 w}) = B_w^-$ ist. Es gilt $\ell(w_0 wss) > \ell(w_0 ws)$, also folgt $B^s \cap B^{w_0 ws} \subset B$ aus 4.9. Eine Konjugation mit s liefert dann $B \cap B^{w_0 w} \subset B^s$, woraus schließlich $(B^s \cap B \cap B^{w_0 w}) = B \cap B^{w_0 w} = B_w^-$ folgt. $\square$

Satz 4.16. *Für $w, v \in W$ mit $\ell(vw) = \ell(v) + \ell(w)$ gelten die Gleichungen:*

$$B_{vw}^- = B_w^- \cdot (B_v^-)^w \qquad\qquad B^- = B_w^- \cap (B_v^-)^w$$

Beweis. Für die erste Gleichung führen wir eine Induktion über $\ell(w)$ durch, wobei der Fall $\ell(w) = 0$ aus $B_1^- = B^- \overset{4.12}{\subset} B_{w_0 v}^+ = B_v^- = (B_v^-)^1$ folgt. Für $\ell(w) > 0$ seien $w' \in W$, $s \in S$ mit $w = w's$, $\ell(w) > \ell(w')$ und $\ell(vw) > \ell(vw')$ (vgl. 3.8). Dann gilt

$$\begin{aligned} B_{vw}^- &\overset{4.15}{=} B_s (B_{vw'}^-)^s \\ &\overset{\mathrm{IA}}{=} B_s (B_{w'}^- (B_v^-)^{w'})^s \\ &= B_s (B_{w'}^-)^s (B_v^-)^w \\ &\overset{4.15}{=} B_w^- (B_v^-)^w. \end{aligned}$$

Für die zweite Gleichung betrachte man

$$B^- \overset{4.12}{\subset} B_w^- \cap (B_v^-)^w = B \cap B^{w_0 w} \cap B^w \cap B^{w_0 vw} \subset (B^{w_0} \cap B)^w \overset{4.12}{=} B^-.$$

$\square$

Korollar 4.17. *Für alle $w \in W$ gelten die Gleichungen:*

$$B = B_w^- \cdot B_w^+ \qquad\qquad B^- = B_w^- \cap B_w^+$$

Beweis. Man wende 4.16 mit $v = w_0 w^{-1}$ an, was aufgrund von 3.19 möglich ist. Da w_0 selbstinvers ist, gilt sowohl $B_{w_0}^- = B$ als auch $(B_v^-)^w = (B_{w_0 w^{-1}}^-)^w = (B_{w^{-1}}^+)^w = B_w^+$. □

Zuletzt zeigen wir, dass sich das Wurzelsystem selbst auch in das BN-Paar übertragen lässt. Sei $\Sigma = \{wB_s w^{-1} \mid s \in S, w \in W\}$. Dann definiert $w.\sigma = w\sigma w^{-1}$ mit $w \in W$, $\sigma \in \Sigma$ eine Wirkung von W auf Σ.

Satz 4.18. *Die Abbildung $f : \Phi \to \Sigma$ mit $f(w.v_s) = wB_s w^{-1}$ ist eine wohldefinierte W-äquivariante Bijektion.*

Beweis. Wir zeigen zunächst, dass für $w, w' \in W$ und $s, s' \in S$ mit $w.v_s = w'.v_{s'}$ stets $f(w.v_s) = f(w'.v_{s'})$ gilt. Dabei können wir ohne Beschränkung der Allgemeinheit $w' = 1$ annehmen, sodass nur $B_s^{w^{-1}} = B_{s'}$ zu zeigen ist.

Es gelten $w.v_s = v_{s'} > 0$ und $s'w.v_s = s'.v_{s'} < 0$, also folgt $B_s \subset B_w^+ \cap B_{s'w}^-$ aus 3.14 und 4.14. Dabei benutzen wir, dass aus $\ell(s'ws) < \ell(s'w)$ die Ungleichung $\ell(w_0 s'ws) > \ell(w_0 s'w)$ folgt (vgl. 3.19 und 3.22). Dann gilt:

$$(B_s)^{w^{-1}} \subset (B_w^+)^{w^{-1}} \cap (B_{s'w}^-)^{w^{-1}} = B^{w^{-1}} \cap B \cap B^{w^{-1}} \cap B^{w_0 s'} \subset B_{s'}$$

Komplett analog folgt aus $w^{-1}.v_{s'} = v_s > 0$ und $sw^{-1}.v_{s'} = s.v_s < 0$, dass $(B_{s'})^w \subset B_s$ ist, was die andere Inklusion beweist. Somit ist f wohldefiniert.

Per Definition ist f W-äquivariant und surjektiv. Seien $r, r' \in \Phi$ mit $f(r) = f(r')$. Ohne Beschränkung der Allgemeinheit existieren $s, s' \in S$ und $w \in W$ mit $r = w.v_s$ und $r' = v_{s'}$. Aus $wB_s w^{-1} = B_{s'} = B \cap B^{w_0 s'}$ folgt dann $B_s = B^w \cap B^{w_0 s' w}$, und da $B_s \subset B$ ist, gelten $B_s \subset B_w^+$ und $B_s \subset B_{s'w}^-$. Mit 3.14 und 4.14 bedeutet das $w.v_s > 0$ sowie $s'w.v_s = s'.(w.v_s) < 0$, also $w.v_s = v_{s'}$ nach 3.13. □

4.3 Zerfallende BN-Paare

Definition 4.19. *Sei G eine endliche Gruppe, (G, B, N, S) ein BN-Paar und $p > 0$ eine Primzahl. (G, B, N, S, U) ist ein* zerfallendes BN-Paar von Charakteristik p*, wenn folgende Eigenschaften erfüllt sind:*

(v) $T = B \cap N$ ist abelsch.

(vi) U ist eine normale p-Sylowuntergruppe von B mit $B = U \rtimes T$.

Man bemerke, dass U als normale p-Sylowuntergruppe genau aus den p-Elementen von B besteht. Zerfallende BN-Paare werden häufig mit der zusätzlichen Bedingung $T = \bigcap_{n \in N} B^n$ definiert. Wir nennen solche BN-Paare wie in [11] *saturiert*. Saturierte Paare haben eine engere Verbindung zur Geometrie ihrer Gebäude und erlauben eine einfachere Berechnung bestimmter Nebenklassen.

Beispiel 4.20. Wir betrachten erneut die allgemeine lineare Gruppe $G = \mathrm{GL}_n(K)$, diesmal über einem endlichen Körper mit Charakteristik p und Kardinalität $q = p^k$. Sei (G, B, N, S) das BN-Paar in Beispiel 4.2 und $U < B$ die Untergruppe der Dreiecksmatrizen mit Einsen auf der Diagonale. Dann ist (G, B, N, S, U) ein zerfallendes BN-Paar von Charakteristik p.

Die Gruppe T ist selbst im allgemeinen Fall abelsch, also müssen wir nur (vi) zeigen. Offensichtlich ist $B = UT$ und $U \cap T = 1$. Ferner ist U als Kern des Gruppenhomomorphismus $B \to (K^\times)^n$ mit $A \mapsto (A_{1,1}, \ldots, A_{n,n})$ ein Normalteiler. Eine obere Dreiecksmatrix ist genau dann invertierbar, wenn die Diagonalelemente invertierbar sind, also ist $|B| = q^{n(n-1)/2}(q-1)^n$. Da jede unipotente obere Dreiecksmatrix invertierbar ist, gilt $|U| = q^{n(n-1)/2} = p^{kn(n-1)/2}$ und U ist eine maximale p-Gruppe.

Um die Ergebnisse aus Kapitel 4.2 auf U übertragen zu können, benötigen wir Analoga von $B_w^\pm$ in U. Für eine spätere Anwendung und einfachere Notation wählen wir an dieser Stelle ein beliebiges, aber festes Repräsentantensystem von $W = N/T$. Den Standardrepräsentanten von w bezeichnen wir dabei mit n_w. Ist H eine Untergruppe von G, so schreiben wir $H^w := n_w^{-1} H n_w$, was mit unserer Notation für B^w zu Beginn des Kapitels übereinstimmt.

Definition 4.21. *Für beliebige $w \in W$ und $s \in S$ und schreiben wir:*

$$\begin{aligned} U_w^+ &= U \cap U^w & \qquad U_s &= U_s^- \\ U_w^- &= U \cap U^{w_0 w} & \qquad U^- &= U_{w_0}^+ \end{aligned}$$

Im folgenden Lemma wird gezeigt, dass die hier benötigten Konjugationen wieder von der Wahl des Repräsentanten unabhängig sind.

Lemma 4.22. *Falls T eine Untergruppe $H < G$ normalisiert, so wird für alle $w \in W$ auch H^w von T normalisiert. Insbesondere normalisiert T alle Untergruppen aus 4.21.*

Beweis. H^w wird normalisiert, weil n_w und tn_w Repräsentanten der selben Klasse w sind und H^w nur von w abhängt. Die Aussage über 4.21 folgt daraus, dass U ein Normalteiler von B ist und Konjugationen mit Schnitten kommutieren. □

Die Beziehungen zwischen den $B_w^\pm$ aus dem letzten Kapitel liefern durch einen Schnitt mit U entsprechende Beziehungen zwischen den $U_w^\pm$. Da Schnitte Inklusionen erhalten und mit Konjugationen sowie anderen Schnitten kommutieren, genügt für die folgenden Sätze meist ein kurzes Argument, dass auch die betrachteten Schnitte und Produkte kommutieren.

Proposition 4.23. *Für alle $w \in W$ und $s \in S$ gelten die Gleichungen*

$$\begin{aligned} B_w^+ &= U_w^+ T, & \qquad B_w^+ \cap U &= U_w^+, \\ B_w^- &= U_w^- T, & \qquad B_w^- \cap U &= U_w^-, \\ B_s &= U_s T, & \qquad B_s \cap U &= U_s. \end{aligned}$$

Beweis. Es genügt, die oberen Gleichungen zu zeigen. Zunächst folgt $U_w^+ T \subset B_w^+$ aus

$$U_w^+ T = (U \cap U^w)T \subset UT \cap U^w T \overset{4.22}{=} UT \cap (UT)^w = B \cap B^w = B_w^+.$$

Sei andersherum $x \in B_w^+ = UT \cap U^w T$. Dann gibt es $u, u' \in U$ und $t, t' \in T$ mit

$$x = u't' = u^{n_w} t,$$

also ist $u^{n_w} = u't't^{-1} \in U^w \cap B$. Da u^{n_w} ein p-Element ist und U alle p-Elemente von B enthält, gilt $u^{n_w} \in U^w \cap U = U_w^+$, woraus $x = u^{n_w} t \in U_w^+ T$ folgt. Es ist also auch $B_w^+ \subset U_w^+ T$.

Für die zweite Gleichung betrachte man zuerst $U_w^+ = U_w^+ \cap U \subset U_w^+ T \cap U = B_w^+ \cap U$. Da $U_w^+ \subset U$ ist, impliziert die eindeutige Zerlegung in semidirekten Produkten (1.7) dann $U_w^+ T \cap U \subset U_w^+$, also ist insgesamt $B_w^+ \cap U = U_w^+$. □

Zusammen mit Lemma 4.12 erhalten wir daraus:

Korollar 4.24. *Es gilt*

$$\bigcap_{w \in W} U^w = U^-.$$

Insbesondere gelten $(U^-)^w = U^-$ und $U^- \subset U_w^+$ für alle $w \in W$.

Satz 4.25. *Für $w, v \in W$ mit $\ell(vw) = \ell(v) + \ell(w)$ gelten die Gleichungen:*

$$U_{vw}^- = U_w^- \cdot (U_v^-)^w \qquad U^- = U_w^- \cap (U_v^-)^w \qquad \left|U_{vw}^-\right| = \frac{|U_w^-| \cdot |U_v^-|}{|U^-|}$$

Beweis. Die erste Gleichung entsteht aus 4.16 durch einen Schnitt mit U:

$$\begin{aligned} U_{vw}^- &\overset{4.23}{=} B_{vw}^- \cap U \\ &\overset{4.16}{=} B_w^-(B_v^-)^w \cap U \\ &= U_w^- T (U_v^- T)^w \cap U \\ &\overset{4.22}{=} U_w^- (U_v^-)^w T \cap U. \end{aligned}$$

Nun besteht aber $U_w^-(U_v^-)^w \subset B_w^-(B_v^-)^w \overset{4.16}{=} B_{vw}^- \subset B$ aus p-Elementen, also folgt erneut $U_w^-(U_v^-)^w \subset U$ und dann $U_w^-(U_v^-)^w T \cap U = U_w^-(U_v^-)^w$ mit 1.7.

Für die zweite Gleichung folgt ($\subset$) sofort aus 4.24. Die andere Inklusion folgt aus

$$\begin{aligned} U_w^- \cap (U_v^-)^w &= U \cap U^{w_0 w} \cap (U \cap U^{w_0 v})^w \\ &= U \cap U^{w_0 w} \cap U^w \cap U^{w_0 v w} \\ &\subset U^{w_0 w} \cap U^w \\ &= (U^{w_0} \cap U)^w \\ &\overset{4.24}{=} U^-. \end{aligned}$$

Die dritte Gleichung ist eine triviale Anwendung von 1.8. □

Wie im Beweis von Korollar 4.17 erhält man daraus:

Korollar 4.26. *Für $w \in W$ gelten die Gleichungen:*

$$U = U_w^- \cdot U_w^+ \qquad U^- = U_w^- \cap U_w^+ \qquad |U| = \frac{|U_w^-| \cdot |U_w^+|}{|U^-|}$$

Wir können diese Ergebnisse nun nutzen, um die Bruhat-Zerlegung (4.4) deutlich zu verschärfen. Dabei spielen Repräsentantensysteme von $U/U^+_{w^{-1}}$ eine wichtige Rolle. Das folgende Lemma zeigt, dass man diese bereits aus Repräsentantensystemen von $U^-_{w^{-1}}/U^-$ erhält.

Wir gehen diesen Umweg hauptsächlich für den Beweis von 5.6; oft sind Repräsentantensysteme von $U^-_{w^{-1}}/U^-$ jedoch auch leichter zu finden. Für saturierte zerfallende BN-Paare wie 4.20 gilt nämlich $U^- = B^- \cap U = T \cap U = 1$, also genügt es, die Untergruppen $U^-_{w^{-1}}$ berechnen zu können. Für nichtsaturierte BN-Paare kann U^- nichttrivial sein, aber wie in [11, Theorem 4.5] gezeigt wird, ist U^- für ungerade p zumindest ein Normalteiler von G und damit von $U^-_{w^{-1}}$. Ebenso findet sich dort ein Gegenbeispiel in gerader Charakteristik.

Lemma 4.27. *Für alle $w \in W$ ist jedes Repräsentantensystem Ω_w von $U^-_{w^{-1}}/U^-$ auch ein Repräsentantensystem von $U/U^+_{w^{-1}}$. Es gilt $BwB = UwB = \Omega_w wB$.*

Beweis. Aus direkter Rechnung folgt

$$U \overset{4.26}{=} U^-_{w^{-1}}U^+_{w^{-1}} = \left(\bigcup_{x\in\Omega_w} xU^-\right)U^+_{w^{-1}} = \bigcup_{x\in\Omega_w} xU^-U^+_{w^{-1}} \overset{4.24}{=} \bigcup_{x\in\Omega_w} xU^+_{w^{-1}}.$$

Weil U endlich ist, ist diese Vereinigung genau dann disjunkt, wenn $|U| = |\Omega_w|\left|U^+_{w^{-1}}\right|$ gilt. Dies ist aber der Fall, da nach 4.26

$$|U| = \frac{\left|U^+_{w^{-1}}\right|\left|U^-_{w^{-1}}\right|}{|U^-|} = \frac{\left|U^+_{w^{-1}}\right||\Omega_w|\,|U^-|}{|U^-|} = \left|U^+_{w^{-1}}\right||\Omega_w|$$

gilt. Somit bildet Ω_w ein Repräsentantensystem von $U/U^+_{w^{-1}}$.

Es ist $BwB = UTwB = UwB$. Da Ω_w ein Repräsentantensystem von $U/U^+_{w^{-1}}$ ist, gilt $UwB = \Omega_w U^+_{w^{-1}} n_w B$. Nun berechnen wir

$$\begin{aligned}
\Omega_w U^+_{w^{-1}} n_w B &= \Omega_w (U \cap U^{w^{-1}}) n_w B \\
&= \Omega_w (U n_w \cap n^{-1}_{w^{-1}} U n_{w^{-1}} n_w) B \\
&= \Omega_w n_w (n_w^{-1} U n_w \cap n_w^{-1} n^{-1}_{w^{-1}} U n_{w^{-1}} n_w) B \\
&= \Omega_w n_w (U^w \cap U) B \\
&= \Omega_w n_w B \\
&= \Omega_w w B,
\end{aligned}$$

wobei wir in der vierten Gleichung verwenden, dass U von $n_{w^{-1}} n_w \in T$ normalisiert wird. □

Lemma 4.28. *Seien $w_1, w_2 \in W$, $u_1, u_2 \in U$ und $t_1, t_2 \in T$. Dann gilt*

$$u_1 t_1 n_{w_1} U = u_2 t_2 n_{w_2} U \iff w_1 = w_2,\ t_1 = t_2,\ u_2^{-1} u_1 \in U^+_{w_1^{-1}}.$$

Beweis. ($\Longleftarrow$): Sei $t := t_1 = t_2$ und $w := w_1 = w_2$. Dann gilt

$$n_w^{-1} t^{-1} u_2^{-1} u_1 t n_w \in (U^+_{w^{-1}})^{tn_w} = (U \cap U^{w^{-1}})^w = (U^w \cap U) \subset U,$$

und daher $u_1 t n_w U = u_2 t n_w U$.

($\Longrightarrow$): Wegen $u_i t_i n_{w_i} U \subset B w_i B$ folgt aus der Bruhat-Zerlegung sofort $w := w_1 = w_2$. Es gibt dann ein $u \in U$ mit $u_1 t_1 n_w = u_2 t_2 n_w u$. Seien ferner $t', t'' \in T$, sodass $t_2 n_w = n_w t'$ und $n_w^{-1} t_1^{-1} = t'' n_w^{-1}$ gelten. Das ist möglich, weil T ein Normalteiler von N ist. Dann gilt:

$$u_2^{-1} u_1 = (t_2 n_w) u (n_w^{-1} t_1^{-1}) = n_w (t' u t'') n_w^{-1} \in U \cap B^{w^{-1}}$$

Das zeigt $u_2^{-1} u_1 \in U^+_{w^{-1}}$, da

$$U \cap B^{w^{-1}} = U \cap B \cap B^{w^{-1}} = U \cap B^+_{w^{-1}} \overset{4.23}{=} U^+_{w^{-1}}$$

ist. Wir haben auch $u_2^{-1} u_1 = t_2 u^{n_w^{-1}} t_1^{-1} \in U^+_{w^{-1}}$ gezeigt, was $t_2 u^{n_w^{-1}} \in U^+_{w^{-1}} t_1 \overset{4.22}{=} t_1 U^+_{w^{-1}}$ zur Folge hat. Also ist $t_1^{-1} t_2 \in U^+_{w^{-1}} \cap T \subset U \cap T = \{1\}$, d.h. $t_1 = t_2$. □

Korollar 4.29. *Für jedes $w \in W$ sei Ω_w ein Repräsentantensystem von $U/U^+_{w^{-1}}$. Dann ist die Menge $\Gamma := \{u_w t n_w \,|\, w \in W, u_w \in \Omega_w, t \in T\}$ ein Repräsentantensystem von G/U.*

Beweis. Wegen $BwB \overset{4.27}{=} \Omega_w w B = \Omega_w T n_w U$ folgt das unmittelbar aus der Bruhat-Zerlegung und 4.28. □

Korollar 4.30. *Für jedes $w \in W$ sei Ω_w ein Repräsentantensystem von $U/U^+_{w^{-1}}$. Dann besitzt jedes $g \in G$ eine eindeutige Darstellung $g = u_w t n_w u$ mit $w \in W$, $t \in T$, $u_w \in \Omega_w$ und $u \in U$.*

Satz 4.31. *Es gibt eine Zerlegung*

$$G = \bigsqcup_{n \in N} UnU.$$

Beweis. Für jedes $w \in W$ sei Ω_w ein Repräsentantensystem von $U/U^+_{w^{-1}}$ und Γ wie in 4.29. Sei $g \in G$ mit einer Zerlegung $g = u t n_w u'$, $w \in W$, $u \in \Omega_w$, $t \in T$, $u' \in U$ wie in 4.30. Dann ist $g \in UgU = U u t n_w u' U = U t n_w U$, wobei $t n_w \in N$ ist.

Seien nun $n, m \in N$ mit $UnU = UmU$. Dann gibt es eine U-Linksnebenklasse, die sowohl in UnU als auch in UmU liegt, also gibt es $u_n, u_m \in U$ mit $u_n n U = u_m m U$. Sind $v, w \in W$ jeweils die Klassen von n und m, gibt es $t_n, t_m \in T$ mit $n = t_n n_v$ und $m = t_m n_w$. Mit 4.28 folgt dann aus

$$u_n t_n n_v U = u_n n U = u_m m U = u_m t_m n_w U,$$

dass $w = v$ und $t_n = t_m$, also $n = m$, ist. □

5 Die Hecke-Algebra $H_R(G,U)$

In Kapitel 2.1 haben wir die Gruppenalgebra definiert und skizziert, wie kompatible Gruppenwirkungen von G auf einem R-Modul M durch $R[G]$-Modulstrukturen auf M, also reine Modultheorie, untersucht werden können. Häufig ist man an den Invarianten einer Gruppenwirkung unter einer Untergruppe $H < G$ interessiert, also den Elementen, die von H fixiert werden. Ein Paradebeispiel dafür ist die Galoistheorie. Die Menge aller H-invarianten Elemente M^H ist ein R-Untermodul, denn für alle $h \in H$, $m, n \in M^H$ und $r \in R$ gilt:

$$h.0 = 0 \qquad h.(m+n) = h.m + h.n = m + n \qquad h.(r.m) = rh.m = r.m$$

Es gilt jedoch nicht unbedingt $hg.m = g.m$, was eine $R[G]$-Modulstruktur auf M^H im Allgemeinen verhindert. Für Normalteiler $H \triangleleft G$ ist dies kein Problem, da für $g \in G$ und $h \in H$ ein $h' \in H$ mit $hg = gh'$ existiert und somit $hg.m = gh'.m = g.m$ gilt, doch damit beschränken wir uns auf Normalteiler, was im Hinblick auf z.B. Galoistheorie bereits eine große Einschränkung ist.

Um dieses Problem zu lösen, stellen wir zunächst fest, dass die Wirkung von G auf M^H im Normalteilerfall tatsächlich eine Wirkung von G/H induziert, da für $g' = gh$ die Gleichung $g'.m = gh.m = g.m$ gilt. Auf M^H gibt es also eine natürliche $R[G/H]$-Modulstruktur.

Der Gruppenring $R[G/H]$ ist per Definition der freie Modul auf G/H mit dem Faltungsprodukt oder äquivalent der Modul aller Funktionen $G/H \to R$ mit punktweiser Addition, punktweiser Skalarmultiplikation und der Faltung von Funktionen als Produkt. Äquivalent dazu können wir auch Funktionen $f : G \to R$ mit der Invarianzbedingung $f(hgh') = f(g)$ für $g \in G$ und $h, h' \in H$ betrachten. Wir verwenden dabei zweiseitige anstelle der (für Normalteiler ausreichenden) einseitigen Invarianz, um uns von der Normalitätsbedingung zu lösen. Das Produkt ist dann jedoch nicht mehr das Produkt von Funktionen $G \to R$ wie in $R[G]$, sondern

$$(f * f')(g') = \sum_{g \in \Omega} f(g) f'(g^{-1}g'),$$

wobei Ω ein Repräsentantensystem von G/H ist. Dieses Produkt hängt nicht von Ω ab, da $f(gh) = f(g)$ und $f'(h^{-1}g^{-1}g') = f'(g^{-1}g')$ ist. Die resultierende Funktion ist offensichtlich rechtsinvariant. Für die Linksinvarianz gehen wir zum Repräsentantensystem durch die Konjugierten $\{hgh^{-1} \,|\, g \in \Omega\}$ über. Dann gilt

$$(f * f')(hg') = \sum_{g \in \Omega} f(hgh^{-1}) f'(hg^{-1}h^{-1}hg') = \sum_{g \in \Omega} f(g) f'(g^{-1}g') = (f * f')(g').$$

Diese neue Definition verwendet nirgendwo mehr, dass H ein Normalteiler ist.

Definition 5.1. *Sei R ein kommutativer Ring, G eine endliche Gruppe und $I < G$ eine Untergruppe. Die* Hecke-Algebra *von G und I über R ist der R-Modul*

$$H_R(G, I) = \{f : G \to R \,|\, \forall i, j \in I : \forall g \in G : f(igj) = f(g)\}$$

aller Abbildungen von G nach R, die unter Links- und Rechtsmultiplikation mit I invariant sind. Addition und Skalarmultiplikation sind jeweils punktweise definiert. Das Produkt von

$f, h \in H_R(G, I)$ ist die ebenfalls Faltungsprodukt genannte Abbildung $f * h : G \to R$ mit

$$(f * h)(g') = \sum_{g \in \Omega} f(g)h(g^{-1}g'),$$

wobei Ω ein beliebiges Repräsentantensystem von G/I ist. Das Nullelement ist wie bei Gruppenalgebren die Nullfunktion; das Einselement ist die Indikatorfunktion $\mathbf{1}_I$ von I.

Schreiben wir $e := \mathbf{1}_I$ und $i \in \Omega$ für den Repräsentanten von I, gilt tatsächlich

$$\begin{aligned}(e * f)(g') &= \sum_{g \in \Omega} e(g)f(g^{-1}g') = e(i)f(i^{-1}g') = f(g') \\ (f * e)(g') &= \sum_{g \in \Omega} f(g)e(g^{-1}g') = f(g'i^{-1})e(ig'^{-1}g') = f(g')e(i) = f(g'),\end{aligned}$$

denn $g^{-1}g' \in I \iff g \in g'I$. Man bemerke, dass die Hecke-Algebra $H_R(G, I)$ per Definition aus Funktionen $G \to R$ besteht und als R-Untermodul von $R[G]$ aufgefasst werden kann. Sie ist jedoch im Allgemeinen keine Unteralgebra: Die Einselemente stimmen nur überein, wenn $\mathbf{1}_I = \mathbf{1}_{\{1\}}$, d.h. $I = 1$, ist. Umgekehrt ist offensichtlich $H_R(G, 1) = R[G]$ als R-Algebra.

Der zu Beginn erwähnte Modul M^I der I-invarianten Elemente ist auf natürliche Weise ein $H_R(G, I)$-Modul, und durch den Übergang von M zu M^I ergibt sich ein Funktor $\mathrm{Mod}_{R[G]} \to \mathrm{Mod}_{H_R(G,I)}$. Im Allgemeinen liefert dieser keine einfache Korrespondenz zwischen $H_R(G, I)$-Moduln und den unter I invarianten Darstellungen von G. Da Hecke-Algebren jedoch explizit durch Erzeuger und Relationen beschrieben werden können (vgl. 5.8), sind die $H_R(G, I)$-Moduln relativ leicht zu klassifizieren. Dadurch erhofft man sich Rückschlüsse auf die Darstellungen von G. Ein großes Resultat in diese Richtung ist Theorem 3.24 in [11], das für einen algebraisch abgeschlossenen Körper K mit positiver Charakteristik und ein zerfallendes BN-Paar (G, B, N, S, U) derselben Charakteristik eine Korrespondenz zwischen Isomorphieklassen einfacher $K[G]$-Linksmoduln und einfacher $H_K(G, U)$-Rechtsmoduln etabliert.

Proposition 5.2. *Sei R ein kommutativer noetherscher Ring und G eine endliche Gruppe mit Untergruppe I. Dann ist die Hecke-Algebra $H = H_R(G, I)$ noethersch.*

Beweis. Die R-Modulstruktur von H entsteht aus Skalarrestriktion entlang dem Homomorphismus, der $1 \in R$ auf $\mathbf{1}_I \in H$ abbildet. Als R-Modul wird H von den Indikatorfunktionen $\mathbf{1}_{IgI}$ erzeugt; da G endlich ist, gibt es nur endlich viele davon. Die Aussage folgt dann aus 2.19. □

Wir betrachten die Hecke-Algebra für endliche zerfallende BN-Paare (G, B, N, S, U).

Proposition 5.3. *$H_R(G, U)$ ist ein freier R-Modul mit Basis $\{T_n := \mathbf{1}_{UnU} \mid n \in N\}$. Insbesondere ist jedes $f \in H_R(G, U)$ durch seine Werte auf N bestimmt.*

Beweis. Das folgt sofort aus 4.31, da jedes $f \in H_R(G, U)$ auf UnU konstant ist. □

Korollar 5.4. *Für $m, n, t \in N$ gibt es Konstanten $c_{mnt} \in R$ mit*

$$T_m * T_n = \sum_{t \in N} c_{mnt} T_t \qquad\qquad c_{mnt} = (T_m * T_n)(t).$$

Wir können nun die Struktur zerfallender BN-Paare benutzen, um die Multiplikation in $H_R(G,U)$ zu untersuchen. Da wir dafür die von Ω_w abhängigen Sätze aus Kapitel 4.3 benutzen, sei Ω_w ab hier für jedes $w \in W$ ein festes Repräsentantensystem von $U^-_{w^{-1}}/U^-$. Ebenso sei Γ bezüglich dieser Systemer wie in 4.29 gegeben.

Lemma 5.5. *Falls $UtU \not\subset UmUnU$ für $m,n,t \in N$ gilt, ist $c_{mnt} = 0$.*

Beweis. Es gilt

$$\begin{aligned}(T_m * T_n)(t) &= \sum_{\gamma\in\Gamma} \mathbf{1}_{UmU}(\gamma)\mathbf{1}_{UnU}(\gamma^{-1}t) \\ &= \sum_{\gamma\in\Gamma\cap UmU} \mathbf{1}_{UnU}(\gamma^{-1}t) \\ &= \left|\left\{\gamma \in \Gamma \cap UmU \,\middle|\, \gamma^{-1}t \in UnU\right\}\right| \\ &= |\{\gamma \in \Gamma \cap UmU \,|\, t \in \gamma UnU \subset UmUnU\}|\end{aligned}$$

wobei wir $\mathbb{N}_0$ durch wiederholtes Summieren von 1_R nach R abbilden. Aus $t \in UmUnU$ folgt $UtU \subset UmUnU$, also ist nach Annahme $c_{mnt} \overset{5.4}{=} (T_m * T_n)(t) = 0$. □

Proposition 5.6. *Seien $m,n \in N$ mit Klassen $w,v \in W$. Gilt $\ell(wv) = \ell(w) + \ell(v)$, so ist $T_m * T_n = T_{mn}$.*

Beweis. Nach Definition gilt

$$(T_m * T_n)(g) = \sum_{\gamma\in\Gamma} \mathbf{1}_{UmU}(\gamma)\mathbf{1}_{UnU}(\gamma^{-1}g) = \sum_{\gamma\in\Gamma\cap UmU} \mathbf{1}_{UnU}(\gamma^{-1}g)$$

Dieser Ausdruck benutzt ausschließlich die R-Modulstruktur und enthält keine Referenzen zum Faltungsprodukt mehr. Fassen wir also $H_R(G,U)$ als R-Untermodul von $R[G]$ auf, können wir das Produkt $T_m * T_n$ auch wie ein Element aus $R[G]$ untersuchen. Insbesondere können wir benutzen, dass in $R[G]$ wegen 4.28 und 4.30 die Gleichung

$$\mathbf{1}_{UnU} = \sum_{u\in\Omega_v} \mathbf{1}_{unU}$$

gilt und wegen $\gamma^{-1}g \in UnU \iff g \in \gamma UnU$ immer $\mathbf{1}_{unU}(\gamma^{-1}g) = \mathbf{1}_{\gamma unU}(g)$ ist.

Für $t = mn_w^{-1} \in T$ gilt $\Gamma \cap UmU = \Omega_w t n_w = \Omega_w m$ (vgl. 4.29), woraus

$$\begin{aligned}T_m * T_n &= \sum_{u\in\Omega_v}\sum_{\gamma\in\Gamma\cap UmU} \mathbf{1}_{\gamma unU} \\ &= \sum_{u\in\Omega_v}\sum_{u'\in\Omega_w} \mathbf{1}_{u'munU} \\ &= \sum_{u\in\Omega_v}\sum_{u'\in\Omega_w} \mathbf{1}_{(u'mum^{-1})mnU}\end{aligned}$$

folgt. Nach Definition von Ω_w und Ω_v ist $u \in U^-_{v^{-1}}$ und $u' \in U^-_{w^{-1}}$, was

$$u'mum^{-1} \in U^-_{w^{-1}} \cdot (U^-_{v^{-1}})^{m^{-1}} = U^-_{w^{-1}} \cdot (U^-_{v^{-1}})^{w^{-1}} \overset{4.25}{=} U^-_{(wv)^{-1}} \subset U$$

zur Folge hat. $T_m * T_n$ ist also eine Summe von $|\Omega_v| \cdot |\Omega_w|$ Indikatorfunktionen für in $UmnU$ enthaltene U-Linksnebenklassen. Da wir jedoch a priori wissen, dass $T_m * T_n \in H_R(G,U)$ ist, muss diese Summe ein Vielfaches von $\mathbf{1}_{UmnU} = T_{mn}$ sein, d.h. alle Linksnebenklassen treten gleich oft auf. Nach 4.29 gibt es genau $|\Omega_{wv}|$ Linksnebenklassen in $UmnU$, weshalb eine feste Linksnebenklasse genau

$$\frac{|\Omega_v|\,|\Omega_w|}{|\Omega_{wv}|} \overset{4.27}{=} \frac{\left|U^-_{w^{-1}}\right|\left|U^-_{v^{-1}}\right|}{|U^-|^2} \cdot \frac{|U^-|}{\left|U^-_{v^{-1}w^{-1}}\right|} \overset{4.25}{=} 1$$

Mal auftritt. Somit ist $T_m * T_n = T_{mn}$, was zu zeigen war. □

Korollar 5.7. *Sei $(n_s)_{s\in S}$ ein Repräsentantensystem von $S \subset W$ in N. Dann wird $H_R(G,U)$ als R-Algebra von $\{T_{n_s}, T_t \mid s \in S, t \in T\}$ erzeugt.*

Beweis. Sei $n \in N$, $v = nT \in W$, $v = s_1 \dots s_r$ eine reduzierte Darstellung von v und $t := n_{s_1}^{-1} \dots n_{s_r}^{-1} n \in T$. Wegen $\ell(v) = \sum_{i=1}^r \ell(s_i) + \ell(tT)$ folgt induktiv $T_{n_{s_1}} * \dots * T_{n_{s_r}} * T_t = T_n$ aus 5.6. Somit folgt die Behauptung, da eine R-Basis von $H_R(G,U)$ in der erzeugten R-Unteralgebra liegt. □

Bemerkung 5.8. Nach 5.6 gelten $T_{n_s} * T_t = T_{n_s t} = T_{n_s t n_s^{-1}} * T_{n_s}$ und $T_{n_s} * T_{n_{s'}} = T_{n_s n'_s}$ für die Erzeuger aus 5.7 und alle $t \in T$, $s, s' \in S$ mit $s \neq s'$. Darüber hinaus erfüllen die T_{n_s} gewisse quadratische Beziehungen (vgl. [11, Lemma 3.11]).

Satz 5.9. *$H_R(G,U)$ ist eine freie id_R-Frobeniuserweiterung von R.*

Beweis. Wir verwenden die Charakterisierung 2.12 (iii). Sei $n_0 \in N$ ein Urbild des längsten Elements $w_0 \in W$. Wir definieren die Bilinearform $f : H_R(G,U) \times H_R(G,U) \to R$ durch

$$f(x,y) := (x * y)(n_0).$$

Dank der R-Modul- und R-Algebraeigenschaften von $H_R(G,U)$ ist f id_R-assoziativ.

Für alle $m, n \in N$ mit $w := mT$, $v := nT$ seien $x_m = T_{n_0 m^{-1}}$ und $y_n = T_n$. Wir behaupten:

$$f(x_m, y_n) = \begin{cases} 0 & \text{falls } \ell(w) > \ell(v) \\ 0 & \text{falls } \ell(w) = \ell(v), \text{ aber } w \neq v \\ 0 & \text{falls } w = v, \text{ aber } m \neq n \\ 1 & \text{falls } m = n \\ * & \text{falls } \ell(w) < \ell(v) \end{cases}$$

Wir treffen keine Aussage über den Fall $\ell(w) < \ell(v)$ und nehmen daher im Folgenden stets $\ell(w) \geq \ell(v)$ an. Nach 5.5 ist $f(x_m, y_n) = 0$, falls $Un_0U \not\subset Un_0m^{-1}UnU$ gilt. In den ersten zwei Fällen ist das der Fall: Sei $w_0 w^{-1} = s_1 \dots s_p$ eine reduzierte Darstellung und Z die Menge der Teilworte von $s_1 \dots s_p$. Wäre nun $Un_0U \subset Un_0m^{-1}UnU$, so würde

$$Bw_0B = BUn_0UB \subset BUn_0m^{-1}UnUB \subset Bw_0w^{-1}BvB \overset{4.3}{\subset} \bigcup_{z\in Z} BzvB$$

gelten. Dann müsste es wegen 4.4 ein $z \in Z$ mit $zv = w_0$ geben, woraus

$$\ell(w_0) = \ell(zv) \leq \ell(z) + \ell(v) \leq \ell(w_0 w^{-1}) + \ell(v) = \ell(w_0) + \ell(v) - \ell(w) \leq \ell(w_0)$$

folgt. Dann ist $\ell(w_0) = \ell(zv)$ und $\ell(z) = \ell(w_0 w^{-1})$, also $w_0 = zv = w_0 w^{-1} v$ nach 3.19, und schließlich $v = w$, was den Annahmen des ersten bzw. zweiten Falls widerspricht.

Sei $w = v$. Dann ist $\ell(w_0) = \ell(w_0 w^{-1} v) = \ell(w_0 w^{-1}) + \ell(v)$ nach 3.19 (iv), also folgt

$$x_m * y_n = T_{n_0 m^{-1}} * T_n = T_{n_0 m^{-1} n}$$

aus 5.6. Nach 5.3 ist $T_{n_0 m^{-1} n}(n_0)$ entweder 1 (wenn $m = n$) oder 0 (wenn $m \neq n$).

Wir benötigen nun noch eine totale Ordnung auf N, sodass die Matrix A mit Einträgen $A_{i,j} = f(x_i, y_j)$, invertierbar ist. Das ist nach unserer Berechnung oben bereits der Fall, wenn für $m, n \in N$ mit $\ell(mT) < \ell(nT)$ stets $m < n$ gilt, da dann A eine obere Dreiecksmatrix mit Einsen auf der Diagonale ist. Da $m \leq n :\iff \ell(mT) \leq \ell(nT)$ eine Partialordnung auf der endlichen Menge N ist, existiert so eine Ordnung. □

In Kombination mit 2.18 ergibt sich schließlich das Hauptergebnis dieser Arbeit:

Korollar 5.10. *Sei R ein kommutativer Ring und $H = H_R(G, U)$ die Hecke-Algebra eines endlichen zerfallenden BN-Paares (G, B, N, S, U). Dann gilt für die injektiven Dimensionen*

$$\mathrm{id}\,(R) = \mathrm{id}\,({}_H H) = \mathrm{id}\,(H_H)\,.$$

Für den nulldimensionalen Fall erhalten wir, dass die Hecke-Algebra über kommutativen selbstinjektiven Ringen auch selbstinjektiv ist. Zieht man zusätzlich 5.2 in Betracht, sieht man, dass die Hecke-Algebra über kommutativen Quasifrobeniusringen (z.B. Körpern) ebenfalls ein Quasifrobeniusring ist – projektiv und injektiv sind für $H_R(G, U)$-Moduln also gleichbedeutend.

Literatur

[1] Bell, Allen D.; Farnsteiner, Rolf. *On the Theory of Frobenius Extensions and its Application to Lie Superalgebras*, Transactions of the American Mathematical Society, Volume 335, No. 1, 1993, S. 407-415.

[2] Bourbaki, Nicolas. *Lie Groups and Lie Algebras, Chapters 4-6*, Springer, 1968.

[3] Bourbaki, Nicolas. *Algèbre commutative, Chapitre 10*, Springer, 2007.

[4] Brown, Kenneth Stephen. *Buildings*. Springer, 1989.

[5] Curtis, Charles W.; Reiner, Irving. *Methods of Representation Theory with Applications to Finite Groups and Orders II*. Wiley Interscience, 1987.

[6] Humphreys, James Edward. *Reflection Groups and Coxeter Groups*. Cambridge University Press, 1990.

[7] Lam, Tsit Yuen. *Lectures on Modules and Rings*. Springer, 1990.

[8] Nakayama, Tadashi; Tsuzuku, Toshirou. *On Frobenius Extensions I*. Nagoya Math. J. Volume 17, 1960, S. 89-110.

[9] Ollivier, Rachel; Schneider, Peter. *Pro-p Iwahori-Hecke Algebras are Gorenstein*. Journal Inst. Math. Jussieu Volume 13, Issue 4, 2014, S. 753-809.

[10] Richen, Forrest. *Modular Representations of split (B, N)-pairs*. Trans. Amer. Math. Soc. 140, 1969, S. 435-460.

[11] Tinberg, N. B. *Modular representations of finite groups with unsaturated split (B, N)-pairs*. Can. J. Math., Volume 32, No. 3, 1980, S. 714-733.

Eidesstattliche Versicherung

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Bachelorarbeit unter Betreuung durch Prof. Dr. Jan Kohlhaase selbstständig verfasst und Zitate kenntlich gemacht habe. Andere als die angegebenen Quellen und Hilfsmittel wurden von mir nicht benutzt. Diese Arbeit hat in dieser oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegen.

Essen, den 15.10.2018

Sebastian Melzer