Über die Isomorphie der Kohomologiegruppen einer zyklischen Gruppe von Primzahlordnung

Diplomarbeit

vorgelegt von

Andreas Röscheisen

aus

Heidenheim

angefertigt am

Mathematischen Institut der Georg-August-Universität zu Göttingen

2003

Über die Isomorphie der Kohomologiegruppen einer zyklischen Gruppe von Primzahlordnung

Diplomarbeit

vorgelegt von

Andreas Röscheisen

aus

Heidenheim

angefertigt am

Mathematischen Institut der
Georg-August-Universität zu Göttingen

2003

Danksagung

An dieser Stelle möchte ich allen danken, die zum Gelingen dieser Diplomarbeit beigetragen haben. Insbesondere möchte ich Herrn Professor Smith danken für das Seminar über die Kohomologie von Gruppen, das mein Interesse für dieses Gebiet geweckt hat, und vor allem für das interessante Thema und die gute Betreuung bei der Bearbeitung.
Das weiteren gilt mein Dank Kristin Stroth und Karsten Roeseler, die sich die Zeit genommen und die Mühe gemacht haben, die Arbeit Korrektur zu lesen. Danken möchte ich auch Barbara Zwicknagl, die mich in Motivationskrisen immer wieder angespornt hat.

Inhaltsverzeichnis

Einleitung

In der Invariantentheorie betrachtet man die Invarianten einer Algebra A bezüglich einer Gruppe G, die auf A mittels Algebra-Endomorphismen operiert. Die Invarianten bilden einen Ring, den sogenannten Invariantenring A^G. Das Hauptaugenmerk der Invariantentheorie liegt hierbei auf der Algebra $\mathbb{F}[V]$, der Algebra der polynomialen Formen auf einem endlich-dimensionalen $\mathbb{F}$-Vektorraum V. $\mathbb{F}$ ist hierbei ein Körper, und die Operation einer Gruppe G auf $\mathbb{F}[V]$ wird induziert durch eine Darstellung $\rho : G \to GL(V)$.
Der Invariantenring einer G-Algebra A ist zugleich die nullte Kohomologiegruppe von G mit Koeffizienten in A und operiert durch das Cup-Produkt auf den höheren Kohomologiegruppen $H^m(G, A)$. Andrerseits bergen die höheren Kohomologiegruppen auch wieder Informationen über den Invariantenring.

Das Ziel dieser Arbeit ist es zu zeigen, dass die Kohomologiegruppen der zyklischen Gruppe $\mathbb{Z}/p$ ($p \geq 3$ Primzahl) mit Koeffizienten in der $\mathbb{Z}/p$-Algebra $\mathbb{F}_q[V]$ im Allgemeinen zwar nicht als Moduln über $\mathbb{F}_q[V]^{\mathbb{Z}/p}$, aber doch als Moduln über der Dicksonalgebra, dem Invariantenring $\mathbb{F}_q[V]^{GL(V)}$, isomorph sind.[1]

Die Arbeit gliedert sich im Wesentlichen in drei Teile.
Am Anfang, in den Kapiteln 1–3, werden die Definitionen und Konstruktionen eingeführt, die für die Gruppenkohomologie notwendig sind. Hier wurde zu großen Teilen nach [Weiss] verfahren. Es wird in dieser Arbeit nicht auf die Beschreibung der Kohomologiegruppen als Ext-Funktor und den daraus folgenden Ergebnissen eingegangen. Die Arbeit beschränkt sich vielmehr auf die explizite Vorgehensweise zur Berechnung sowohl der Kohomologiegruppen selbst als auch des Cup-Produkts.
Zum Schluss des dritten Kapitels wird dann der Nachweis erbracht, dass für eine G-Algebra A die nullte Kohomologie $H^0(G, A)$ mit Hilfe des Cup-Produkts einen Ring bildet (den Invariantenring) und die höheren Kohomologiegruppen Moduln über $H^0(G, A)$ werden.

Im Kapitel 4 wird dann für die Gruppe $\mathbb{Z}/p$ explizit eine Auflösung von $\mathbb{Z}$ angegeben, aus der die Kohomologie direkt berechnet und damit die schon länger bekannte Tatsache bewiesen werden kann, dass für jeden $\mathbb{Z}/p$-Modul A die Kohomologiegruppen $H^n(\mathbb{Z}/p, A)$ und $H^{n+2}(\mathbb{Z}/p, A)$ für alle $n \geq 1$ isomorph sind (siehe z. B. [Evens]), und zwar nicht nur isomorph als Gruppen, sondern sogar bezüglich jeder durch das Cup-Produkt induzierten Modulstruktur.
Weiter erhält man für einen $\mathbb{F}_q$-Vektorraum W, dass die (höheren) Kohomologiegruppen von $\mathbb{Z}/p$ mit Koeffizienten in W alle isomorph als $\mathbb{F}_q$-Vektorräume sind.

[1] $\mathbb{F}_q$ sei ein endlicher Körper der Charakteristik p mit $|\mathbb{F}_q| = q$

Der dritte Teil, ab Kapitel 5, untersucht nun speziell die Gruppen $H^n(\mathbb{Z}/p, \mathbb{F}_q[V])$. Durch explizite Berechnung der Kohomologiegruppen wird in Kapitel 5 gezeigt, dass für einen 2-dimensionalen Vektorraum V, auf dem $\mathbb{Z}/p$ durch eine unzerlegbare Darstellung operiert, die ungeraden Kohomologiegruppen zu den geraden Kohomologiegruppen als Moduln über $\mathbb{F}_q[V]^{\mathbb{Z}/p}$ nicht isomorph sind. In diesem Fall sind sie aber isomorph als Moduln über der Dicksonalgebra $\mathbb{F}_q[V]^{GL(V)}$.
In Kapitel 6 wird nachgewiesen, dass diese Isomorphie bei jeder unzerlegbaren Darstellung $\rho : \mathbb{Z}/p \to GL(V)$ gilt. Dieses Ergebnis wird dann in Kapitel 7 auf beliebige Darstellungen von $\mathbb{Z}/p$ verallgemeinert, dass also für jeden endlichdimensionalen $\mathbb{F}_q$-Vektorraum V und jede Darstellung $\rho : \mathbb{Z}/p \to GL(V)$ die Kohomologiegruppen $H^n(\mathbb{Z}/p, \mathbb{F}_q[V]), n \geq 1$, als $\mathbb{F}_q[V]^{GL(V)}$-Moduln zueinander isomorph sind.

1 Grundlagen

G sei stets eine endliche Gruppe.
R sei ein Ring mit Einselement.

1.1 Freie und projektive Moduln

Definition 1.1 *Ein R-Modul F heißt* **frei***, wenn es eine Indexmenge I und zu R isomorphe R-Moduln R_i $(i \in I)$ so gibt, dass*

$$F \cong \bigoplus_{i \in I} R_i \,.$$

Definition 1.2 *Ein R-Modul P heißt* **projektiv***, wenn er folgende Eigenschaft erfüllt: Zu jedem R-Homomorphismus $f : P \to B$ und jedem surjektiven R-Homomorphismus $g : A \to B$ von R-Moduln A und B existiert ein R-Homomorphismus $h : P \to A$ so, dass $f = g \circ h$ gilt.*

$$\begin{tikzcd} & P \arrow[dl, dashed, "h"'] \arrow[d, "f"] & \\ A \arrow[r, "g"] & B \arrow[r] & 0 \end{tikzcd}$$

Anders ausgedrückt: Für jeden surjektiven Homomorphismus $g : A \to B$ von R-Moduln A und B ist auch die Abbildung $g_* : \mathrm{Hom}_R(P, A) \to \mathrm{Hom}_R(P, B)$, $h \mapsto g \circ h$, surjektiv.

Bemerkung In den meisten Büchern, z. B. in [Lang] wird ein projektiver Modul als ein Modul definiert, der eine von mehreren äquivalenten Eigenschaften (darunter die obige), erfüllt. Da die anderen Eigenschaften nicht benötigt werden, wird hier als Definition nur diese eine Eigenschaft gefordert.

1.2 G-Moduln und G-Algebren

Sei G eine multiplikative Gruppe und $\Gamma = \mathbb{Z}[G]$ der ganzzahlige Gruppenring von G. Die Elemente des Rings Γ sind formale Summen $\sum_{\sigma \in G} n_\sigma \sigma$, $n_\sigma \in \mathbb{Z}$ [2]; Addition in Γ erfolgt komponentenweise, während die Multiplikation in natürlicher Weise durch die Multiplikation in G festgelegt ist – im Detail:

$$\sum_{\sigma \in G} m_\sigma \sigma + \sum_{\sigma \in G} n_\sigma \sigma = \sum_{\sigma \in G} (m_\sigma + n_\sigma)\sigma,$$

$$\left(\sum_{\sigma \in G} m_\sigma \sigma\right) \left(\sum_{\sigma \in G} n_\sigma \sigma\right) = \sum_{\sigma \in G} \left(\sum_{\tau\rho = \sigma} m_\tau n_\rho\right) \sigma.$$

[2] Da G endlich ist, sind alle auftretenden Summen endlich. Für unendliche Gruppen müsste noch zusätzlich vorausgesetzt werden, dass $n_\sigma = 0$ für alle bis auf endlich viele σ gilt.

G ist in Γ eingebettet unter der Identifikation von $\sigma \in G$ mit $1 \cdot \sigma \in \Gamma$. Speziell bezeichne 1 das Einselement sowohl von G als auch von Γ.
Eine abelsche Gruppe A wird als **G-Modul** bezeichnet, wenn A ein Links-Γ-Modul ist. Wenn A ein G-Modul ist, gelten offensichtlich:

$$\begin{aligned} \sigma(a+b) &= \sigma(a)+\sigma(b), \\ \sigma(\tau a) &= (\sigma\tau)(a), \\ 1(a) &= a. \end{aligned} \tag{1}$$

Umgekehrt, wenn G so auf der additiven Gruppe A operiert, dass obige Gleichungen gelten, wird A ein G-Modul, wenn die Operation von Γ auf A durch $\left(\sum_{\sigma\in G} n_\sigma \sigma\right)(a) = \sum_{\sigma \in G} n_\sigma(\sigma a)$ definiert wird. Die Gültigkeit der obigen Gleichungen ist äquivalent dazu, dass es einen Gruppenhomomorphismus $\rho : G \to \mathrm{Aut}_{\mathbb{Z}}(A)$ gibt ($\mathrm{Aut}_{\mathbb{Z}}(A)$ bezeichne die Gruppe der Automorphismen von A als $\mathbb{Z}$-Moduln). Dann wird $\sigma(a)$ definiert als $\sigma(a) := \rho(\sigma)(a)$.
Für jedes G definieren wir eine triviale Operation von G auf $\mathbb{Z}$, d. h. $\sigma n = n$ $\forall\, n \in \mathbb{Z}, \sigma \in G$, sodass $\mathbb{Z}$ ein G-Modul wird. Jeder Körper wird ebenfalls als trivialer G-Modul betrachtet.

Ein Ring A wird als **G-Algebra** bezeichnet, wenn die abelsche Gruppe A ein G-Modul ist und für alle $a, b \in A$, $\sigma \in G$

$$\sigma(ab) = \sigma(a)\sigma(b)$$

gilt. Die letzte Gleichung kann auch so beschrieben werden:[3] Die Multiplikation $\mu : A \otimes A \to A$ ist ein G-Homomorphismus, wobei $A \otimes A$ auf natürliche Weise mittels $\sigma(a \otimes b) := \sigma(a) \otimes \sigma(b)$ ein G-Modul ist. Äquivalent zu der angegeben Definition ist, dass es einen Gruppenhomomorphismus $\rho : G \to \mathrm{Aut}(A)$ gibt, wobei $\mathrm{Aut}(A)$ die Gruppe der Algebra-Automorphismen von A bezeichnet. Wie bei der Definition eines G-Moduls operiert G dann mittels $\sigma(a) := \rho(\sigma)(a)$ $\forall\, \sigma \in G, a \in A$.
Der triviale G-Modul $\mathbb{Z}$ – und jeder andere Ring R mit trivialer G-Operation – ist eine G-Algebra.

Sei R ein Ring und A ein R-Modul. Ist weiterhin eine Operation von G auf A gegeben, die mit der R-Operation kommutiert, d. h. es gilt $\sigma(ra) = r\sigma(a)$ $\forall\, \sigma \in G, r \in R, a \in A$, so wird A ein Modul über dem Gruppenring $R[G]$, welcher analog zum ganzzahligen Gruppenring definiert ist. Das heißt die Elemente von $R[G]$ sind die formalen Summen $\sum_{\sigma \in G} r_\sigma \sigma$, $r_\sigma \in R$; Addition und Multiplikation sind wie beim ganzzahligen Gruppenring definiert.
Dass die Operationen von G und R kommutieren, ist wiederum äquivalent dazu, dass es einen Gruppenhomomorphismus $\rho : G \to \mathrm{Aut}_R(A)$ gibt. $\mathrm{Aut}_R(A)$ ist hierbei die Gruppe der R-Modul-Automorphismen von A.

[3] Tensorprodukte sind stets Tensorprodukte als $\mathbb{Z}$-Moduln.

1.3 Kettenkomplexe

Definition 1.3 *Ein* **Kettenkomplex** (X, d) *über* R *ist eine Familie von* R*-Moduln* $(X_n)_{n\in\mathbb{Z}}$ *zusammen mit* R*-Homomorphismen* $d_n : X_n \to X_{n-1}$ *so, dass* $d_{n-1} \circ d_n = 0$ *für alle* $n \in \mathbb{Z}$.
Ein Kettenkomplex heißt **positiv**, *wenn* $X_n = 0$ *für alle* $n < 0$.
Ein Kettenkomplex heißt **exakt**, *wenn* $\mathrm{Im}(d_{n+1}) = \mathrm{Ker}(d_n)\ \forall\, n \in \mathbb{Z}$.

Definition 1.4 *Seien* (X, d) *und* (X', d') *Kettenkomplexe. Eine* **Kettenabbildung** *von* X *nach* X' *ist eine Familie* $(f_n)_{n\in\mathbb{Z}}$ *von* R*-Homomorphismen* $f_n : X_n \to X'_n$ *so, dass für alle* $n \in \mathbb{Z}$ *das Diagramm*

$$\begin{tikzcd} X_n \arrow[r, "d_n"] \arrow[d, "f_n"] & X_{n-1} \arrow[d, "f_{n-1}"] \\ X'_n \arrow[r, "d'_n"] & X'_{n-1} \end{tikzcd}$$

kommutiert.

Definition 1.5 *Seien* (X, d) *und* (X', d') *Kettenkomplexe. Zwei Kettenabbildungen* f *und* g *von* X *nach* X' *heißen* **kettenhomotop**, *wenn es eine Familie* $(D_n)_{n\in\mathbb{Z}}$ *von Homomorphismen* $D_n : X_n \to X'_{n+1}$ *so gibt, dass gilt:*

$$f_n - g_n = d'_{n+1} \circ D_n + D_{n-1} \circ d_n \quad \forall n \in \mathbb{Z}$$

Definition 1.6 *Sei* A *ein* G*-Modul. Eine* G**-Auflösung** *von* A *ist ein positiver Kettenkomplex* (X, d) *über* $\mathbb{Z}[G]$ *mit einem* G*-Homomorphismus* $\varepsilon : X_0 \to A$ *so, dass die Folge*

$$\cdots \to X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{\varepsilon} A \to 0$$

exakt ist.
Eine G*-Auflösung heißt* **projektiv**, *falls alle* X_n *projektiv sind, und* **frei**, *falls alle* X_n *frei sind.*

Proposition 1.7 *Sei* (X, d) *eine projektive* G*-Auflösung eines* G*-Moduls* A *und* (X', d') *eine weitere (nicht notwendig projektive)* G*-Auflösung von* A. *Sei* $h : A \to A$ *ein* G*-Homomorphismus und* $f, \tilde{f} : X \to X'$ *Kettenabbildungen derart, dass*

$$\begin{tikzcd} X_0 \arrow[r, "\varepsilon"] \arrow[d, "f_0"] & A \arrow[d, "h"] \\ X'_0 \arrow[r, "\varepsilon'"] & A \end{tikzcd} \qquad \textit{und} \qquad \begin{tikzcd} X_0 \arrow[r, "\varepsilon"] \arrow[d, "\tilde{f}_0"] & A \arrow[d, "h"] \\ X'_0 \arrow[r, "\varepsilon'"] & A \end{tikzcd}$$

kommutieren. Dann sind f *und* $\tilde{f}$ *kettenhomotop.*

2 Gruppenkohomologie

2.1 Kohomologiegruppen

Sei (X, d) eine projektive G-Auflösung von $\mathbb{Z}$.[4] Wir betrachten die additiven Gruppen $\mathrm{Hom}_G(X_n, A)$. Für $n \geq 0$ induziert die Abbildung d_n einen Homomorphismus $\delta_n : \mathrm{Hom}_G(X_{n-1}, A) \to \mathrm{Hom}_G(X_n, A)$ durch $f \mapsto f \circ d_n$. Wir nennen

$\mathcal{C}^n = \mathcal{C}^n(G, A) = \mathrm{Hom}_G(X_n, A)$	die **n-Koketten** von G in A,
$\mathcal{Z}^n = \mathcal{Z}^n(G, A) = \mathrm{Ker}(\delta_{n+1})$	die **n-Kozykeln** von G in A und
$\mathcal{B}^n = \mathcal{B}^n(G, A) = \mathrm{Im}(\delta_n)$	die **n-Koränder** von G in A.

Wegen $\delta_{n+1} \circ \delta_n = 0$ ist $\mathcal{B}^n$ Untergruppe von $\mathcal{Z}^n$ und wir definieren die **n-te Kohomologiegruppe** von G in A als

$$H^n(G, A) := \mathcal{Z}^n / \mathcal{B}^n.$$

Genau genommen müsste man noch die Auflösung X mit angeben, von der $H^n(G, A)$ a priori abhängt. Es wird aber gezeigt werden, dass $H^n(G, A)$ bis auf eindeutige Isomorphismen unabhängig von der Wahl von (X, d) ist.

2.2 Abbildungen von Kohomologiegruppen

Betrachten wir nun, wie sich die Kohomologie bei Änderung der Gruppe und des G-Moduls verhält. Zwar wird unser Hauptaugenmerk auf der zyklischen Gruppe $\mathbb{Z}/p$ liegen und wir werden auch den Modul nicht wechseln, aber die folgenden Betrachtungen dienen dazu, das Cup-Produkt leichter zu definieren und besser zu verstehen.

Proposition 2.1 *Seien G und G' endliche Gruppen und A und B seien G-Moduln. Sei weiter $\lambda : G' \to G$ ein Gruppenhomomorphismus. Dann*

(i) *wird A durch $\sigma'(a) := \lambda(\sigma')(a)\ \forall\, \sigma' \in G', a \in A$ ein G'-Modul und*

(ii) *jeder G-Homomorphismus von A nach B ist auch ein G'-Homomorphismus, d. h. $\mathrm{Hom}_G(A, B) \subset \mathrm{Hom}_{G'}(A, B)$.*

Beweis Direkte Rechnung. □

Bezeichnung Im Folgenden schreiben wir (G, A) und nennen es ein **Paar**, um auszudrücken, dass A ein G-Modul ist.
Sei (G', A') ein weiteres Paar. Ist $\lambda : G' \to G$ ein Gruppenhomomorphismus

[4] Wir verzichten hier auf den Beweis, dass so eine Auflösung existiert.

(unter anderem wird A dadurch ein G'-Modul) und $f : A \to A'$ ein G'-Modul-Homomorphismus, so bezeichnen wir dies als **Homomorphismus von Paaren** und schreiben $(\lambda, f) : (G, A) \to (G', A')$.

Bemerkung Kompositionen von Paarhomomorphismen sind wieder Paarhomomorphismen.

Es wird nun gezeigt, dass ein Paarhomomorphismus $(\lambda, f) : (G, A) \to (G', A')$ einen Gruppenhomomorphismus $(\lambda, f)_* : H^n(G, A) \to H^n(G', A')$ induziert.

Lemma 2.2 *Seien $\lambda : G' \to G$ ein Gruppenhomomorphismus, (X, d) eine projektive G-Auflösung von $\mathbb{Z}$ und (X', d') eine projektive G'-Auflösung von $\mathbb{Z}$. Dann gibt es G'-Homomorphismen $\Lambda_n : X'_n \to X_n\ \forall n \geq 0$ so, dass*

$$\begin{aligned} \varepsilon \circ \Lambda_0 &= \varepsilon' \qquad \textit{und} \\ d_{n+1} \circ \Lambda_{n+1} &= \Lambda_n \circ d'_{n+1}\ \forall n \geq 0 \end{aligned}$$

Bemerkung Anders gesagt ist $(\Lambda_n)_{n\in\mathbb{Z}}$, wobei $\Lambda_n := 0$ für $n < 0$, eine Kettenabbildung von X nach X' mit der zusätzlichen Eigenschaft $\varepsilon \circ \Lambda_0 = \varepsilon'$.

Beweis durch vollständige Induktion
Induktionsanfang: $n = 0$: Die Definition eines projektiven Moduls besagt, dass es einen G'-Homomorphismus $\Lambda_0 : X'_0 \to X_0$ so gibt, dass

$$\begin{tikzcd} & X'_0 \arrow[dl, dashed, "\Lambda_0"'] \arrow[d, "\varepsilon'"] & \\ X_0 \arrow[r, "\varepsilon"] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

kommutiert. Das heißt aber gerade, dass $\varepsilon \circ \Lambda_0 = \varepsilon'$.

Induktionsvoraussetzung: Seien $\Lambda_k : X'_k \to X_k$ für alle $k \leq n$ so gegeben, dass $d_k \circ \Lambda_k = \Lambda_{k-1} \circ d'_k$ für alle $1 \leq k \leq n$.
Induktionsschluss: Nach Induktionsvoraussetzung kommutiert das Diagramm

$$\begin{tikzcd} X'_{n+1} \arrow[r, "d'_{n+1}"] & X'_n \arrow[r, "d'_n"] \arrow[d, "\Lambda_n"'] & X'_{n-1} \arrow[d, "\Lambda_{n-1}"'] \\ X_{n+1} \arrow[r, "d_{n+1}"] & X_n \arrow[r, "d_n"] & X_{n-1} \end{tikzcd}$$

(Für $n = 0$ ersetzen wir für den Beweis X'_{-1} und X_{-1} durch $\mathbb{Z}$, d'_0 und d_0 durch ε' bzw. ε und Λ_{-1} durch die Identität auf $\mathbb{Z}$.)
Wegen $d_n \circ \Lambda_n \circ d'_{n+1} = \Lambda_{n-1} \circ d'_n \circ d'_{n+1} = 0$ gilt:

$$\mathrm{Im}(\Lambda_n \circ d'_{n+1}) \subset \mathrm{Ker}(d_n) = \mathrm{Im}(d_{n+1}).$$

Also haben wir folgendes Diagramm mit exakter Zeile:

$$\begin{tikzcd} & X'_{n+1} \arrow[d, "\Lambda_n \circ d'_{n+1}"] & \\ X_{n+1} \arrow[r, "d_{n+1}"] & \mathrm{Im}(d_{n+1}) \arrow[r] & 0 \end{tikzcd}$$

Da X'_{n+1} projektiv ist, gibt es einen Homomorphismus $\Lambda_{n+1} : X'_{n+1} \to X_{n+1}$ so, dass $d_{n+1} \circ \Lambda_{n+1} = \Lambda_n \circ d'_{n+1}$ gilt. $\square$

Satz 2.3 *Sei $(\lambda, f) : (G, A) \to (G', A')$ ein Paarhomomorphismus. Seien (X, d) eine projektive G-Auflösung von $\mathbb{Z}$ und (X', d') eine projektive G'-Auflösung von $\mathbb{Z}$. Dann ist dadurch für jedes $n \geq 0$ ein Homomorphismus*

$$(\lambda, f)_{X,X'} : H^n(G, A; X) \to H^n(G', A'; X')$$

so bestimmt, dass folgende Eigenschaften gelten:

(i) $(1, 1)_{X,X} : H^n(G, A; X) \to H^n(G, A; X)$ *ist die Identität.*

(ii) *Falls $(\lambda', f') : (G', A') \to (G'', A'')$ ein weiterer Paarhomomorphismus und (X'', d'') eine projektive G''-Auflösung ist, so gilt:*
$(\lambda \circ \lambda', f' \circ f)_{X,X''} = (\lambda', f')_{X',X''} \circ (\lambda, f)_{X,X'}$

(iii) *Ist $g : A \to A'$ ein weiterer G'-Homomorphismus, so gilt:*
$(\lambda, f + g)_{X,X'} = (\lambda, f)_{X,X'} + (\lambda, g)_{X,X'}$

Beweis Seien $\Lambda_n : X'_n \to X_n$ die G'-Homomorphismen, wie sie in Lemma 2.2 konstruiert wurden. Dies liefert dann Homomorphismen

$$(\Lambda_n, f)_* : \mathrm{Hom}_G(X_n, A) \to \mathrm{Hom}_{G'}(X'_n, A'),\ g \mapsto f \circ g \circ \Lambda_n.$$

Weiter gilt für $g \in \mathrm{Hom}_G(X_n, A)$:

$$\begin{aligned} \left(\delta'_{n+1} \circ (\Lambda_n, f)_*\right)(g) &= \delta'_{n+1}(f \circ g \circ \Lambda_n) \\ &= f \circ g \circ \Lambda_n \circ d'_{n+1} \\ &= f \circ g \circ d_{n+1} \circ \Lambda_{n+1} \\ &= (\Lambda_{n+1}, f)_*(g \circ d_{n+1}) \\ &= ((\Lambda_{n+1}, f)_* \circ \delta_{n+1})(g)\,. \end{aligned}$$

Ist also $g \in \mathcal{Z}^n(G, A)$, so ist $(\Lambda_n, f)_*(g) \in \mathcal{Z}^n(G', A')$, denn

$$\delta'_{n+1}\left((\Lambda_n, f)_*(g)\right) = (\Lambda_{n+1}, f)_*(\delta_{n+1}(g)) = 0\,.$$

Ist $g \in \mathcal{B}^n(G,A)$, d. h. $\exists\, h \in \mathcal{C}^{n-1}(G,A)$ mit $\delta_n(h) = g$, so ist $(\Lambda_n, f)_*(g) \in \mathcal{B}^n(G', A')$, denn

$$(\Lambda_n, f)_*(g) = (\Lambda_n, f)_*(\delta_n(h)) = \delta'_n\left((\Lambda_{n-1}, f)_*(h)\right) .$$

Somit induziert $(\Lambda, f)_*$ eine Abbildung in Kohomologie. Die folgende Rechnung zeigt, dass diese Abbildung nicht von der Wahl von Λ abhängt:
Zwei mögliche Abbildungen Λ und $\tilde{\Lambda}$ sind nach Proposition 1.7 kettenhomotop, d. h. es gibt eine Familie $(D_n)_{n\in\mathbb{Z}}$ von Homomorphismen ($D_n : X'_n \to X_{n+1}$) so, dass

$$\Lambda_n - \tilde{\Lambda}_n = d_{n+1} \circ D_n + D_{n-1} \circ d'_n.$$

Für alle Kozykeln $g \in \mathrm{Hom}_G(X_n, A)$ ist:

$$\begin{aligned}
(\Lambda_n, f)_*(g) &= f \circ g \circ \Lambda_n \\
&= f \circ g \circ (\tilde{\Lambda}_n + d_{n+1} \circ D_n + D_{n-1} \circ d'_n) \\
&= f \circ g \circ \tilde{\Lambda}_n + f \circ g \circ d_{n+1} \circ D_n + f \circ g \circ D_{n-1} \circ d'_n \\
&= (\tilde{\Lambda}_n, f)_*(g) + f \circ \underbrace{\delta_{n+1}(g)}_{=0} \circ D_n + \delta'_n(f \circ g \circ D_{n-1})
\end{aligned}$$

Die Bilder unterscheiden sich also nur um einen Korand, weshalb in Kohomologie die gleiche Abbildung induziert wird.

Die Eigenschaften **(i)** bis **(iii)** sind leicht nachzurechnen. □

Bemerkung Sind X und $\widetilde{X}$ zwei verschiedene G-Auflösungen, so folgt aus den Eigenschaften **(i)** und **(ii)** von Satz 2.3, dass die induzierten Abbildungen $(1,1)_{X,\widetilde{X}}$ und $(1,1)_{\widetilde{X},X}$ zueinander invers sind. Somit sind die Kohomologiegruppen bis auf eindeutige Isomorphismen unabhängig von der Auflösung X, was die Schreibweise $H^n(G,A)$ rechtfertigt.

Abschließende Bemerkung Für jede Gruppe G und jeden G-Modul A gilt:

$$H^0(G,A) \cong A^G = \{a \in A \mid \sigma(a) = a \;\forall \sigma \in G\}$$

Diese Tatsache wird hier allgemein nicht bewiesen, ist aber zum Beispiel in [Evens] nachzulesen. Bei der Berechnung der Kohomologiegruppen von $\mathbb{Z}/p$ wird aber auch dieses Ergebnis zutage treten.

3 Cup-Produkt

Ist A ein G-Modul und B ein G'-Modul, so ist $A \otimes B$ ein $(G \times G')$-Modul mittels $(\sigma, \sigma')(a \otimes b) = \sigma(a) \otimes \sigma'(b)$ für alle $\sigma \in G, \sigma' \in G', a \in A$ und $b \in B$. Weiter ist $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ ein $(G \times G')$-Modul mittels $(\sigma, \sigma')(f) = \sigma' \circ f \circ \sigma^{-1}$ für alle $\sigma \in G, \sigma' \in G'$ und $f \in \mathrm{Hom}_{\mathbb{Z}}(A, B)$.
Speziell für $G = G'$ werden $A \otimes B$ und $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ durch die Diagonalabbildung $\Delta : G \to G \times G, \sigma \mapsto (\sigma, \sigma)$, zu G-Moduln.

Das Cup-Produkt, das wir im Folgenden konstruieren wollen, ist eine Operation, die für alle G-Moduln A und B bilineare Abbildungen

$$\cup : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B) \ \forall\, p, q \geq 0$$

darstellt.

3.1 Tensorprodukt von Kettenkomplexen

Definition 3.1 *Seien (X, d) ein Kettenkomplex von G-Moduln und (X', d') ein Kettenkomplex von G'-Moduln, dann definieren wir den Kettenkomplex $(X \otimes X', \overline{d})$ durch*

$$(X \otimes X')_n := \bigoplus_{p+q=n} X_p \otimes X'_q$$

und

$$\overline{d}_n := (d \otimes 1 \pm 1 \otimes d')_n \,,$$

genauer: $\forall\, x_p \in X_p, x'_q \in X'_q$

$$\begin{aligned} \overline{d}_{p+q}(x_p \otimes x'_q) &:= (d_p \otimes 1)(x_p \otimes x'_q) + (-1)^p (1 \otimes d'_q)(x_p \otimes x'_q) \\ &= d_p(x_p) \otimes x'_q + (-1)^p x_p \otimes d'_q(x'_q) \end{aligned}$$

Bemerkung $(X \otimes X', \overline{d})$ ist tatsächlich ein Kettenkomplex, denn für alle $x_p \in X_p, x'_q \in X'_q$ gilt:

$$\begin{aligned} (\overline{d}_{p+q-1} \circ \overline{d}_{p+q})(x_p \otimes x'_q) &= \overline{d}_{p+q-1}(d_p(x_p) \otimes x'_q + (-1)^p x_p \otimes d'_q(x'_q)) \\ &= d_{p-1}(d_p(x_p)) \otimes x'_q + (-1)^{p-1} d_p(x_p) \otimes d'_q(x'_q) \\ &\quad + (-1)^p d_p(x_p) \otimes d'_q(x'_q) + x_p \otimes d'_{q-1}(d'_q(x'_q)) \\ &= 0 \end{aligned}$$

Also ist $\overline{d}_{p+q-1} \circ \overline{d}_{p+q} = 0$.

Lemma 3.2 *Sind X_p ein projektiver G-Modul und X'_q ein projektiver G'-Modul, so ist $X_p \otimes X'_q$ ein projektiver $(G \times G')$-Modul.*

Beweis Zu zeigen ist, dass für jeden Epimorphismus von $(G \times G')$-Moduln $h : A \to B$ die Abbildung $h_* : \mathrm{Hom}_{G\times G'}(X_p \otimes X'_q, A) \to \mathrm{Hom}_{G\times G'}(X_p \otimes X'_q, B)$ wieder surjektiv ist. Für einen beliebigen $(G \times G')$-Modul A ist die Zuordnung

$$\varphi_A : \mathrm{Hom}_{G\times G'}(X_p \otimes X'_q, A) \to \mathrm{Hom}_G\big(X_p, \mathrm{Hom}_{G'}(X'_q, A)\big)$$

mit

$$\varphi_A(f)(x_p)(x'_q) = f(x_p \otimes x'_q) \quad \forall\ x_p \in X_p, x'_q \in X'_q$$

ein Isomorphismus von $\mathbb{Z}$-Moduln.[5]
Außerdem kommutiert für einen Homomorphismus $h : A \to B$ das Diagramm

$$\begin{tikzcd}
\mathrm{Hom}_{G\times G'}(X_p \otimes X'_q, A) \arrow[r, "\varphi_A", "\cong"'] \arrow[d, "h_*"] & \mathrm{Hom}_G\big(X_p, \mathrm{Hom}_{G'}(X'_q, A)\big) \arrow[d, "h_*"] \\
\mathrm{Hom}_{G\times G'}(X_p \otimes X'_q, B) \arrow[r, "\varphi_B", "\cong"'] & \mathrm{Hom}_G\big(X_p, \mathrm{Hom}_{G'}(X'_q, B)\big)
\end{tikzcd}$$

Sei h surjektiv. Dann ist $h_* : \mathrm{Hom}_{G'}(X'_q, A) \to \mathrm{Hom}_{G'}(X'_q, B)$ surjektiv, da X'_q ein projektiver G'-Modul ist. Da weiter X_p ein projektiver G-Modul ist, ist damit auch $h_* : \mathrm{Hom}_G\big(X_p, \mathrm{Hom}_{G'}(X'_q, A)\big) \to \mathrm{Hom}_G\big(X_p, \mathrm{Hom}_{G'}(X'_q, B)\big)$ surjektiv. Wegen der Kommutativität des obigen Diagramms ist auch die Abbildung $h_* : \mathrm{Hom}_{G\times G'}(X_p \otimes X'_q, A) \to \mathrm{Hom}_{G\times G'}(X_p \otimes X'_q, B)$ surjektiv. Also ist $X_p \otimes X'_q$ ein projektiver $(G \times G')$-Modul. $\square$

Lemma 3.3 *Sei $A \xrightarrow{f} B \xrightarrow{g} C$ eine exakte Folge von G-Moduln und sei X ein freier $\mathbb{Z}$-Modul. Dann sind die Folgen $A \otimes X \xrightarrow{f\otimes 1} B \otimes X \xrightarrow{g\otimes 1} C \otimes X$ und $X \otimes A \xrightarrow{1\otimes f} X \otimes B \xrightarrow{1\otimes g} X \otimes C$ wieder exakt.*

Beweis Dies ist eine allgemein gültige Eigenschaft freier Moduln. $\square$

Satz 3.4 *Seien (X, d) eine projektive G-Auflösung von $\mathbb{Z}$ und (X', d') eine projektive G'-Auflösung von $\mathbb{Z}$. Dann ist $(X \otimes X', \overline{d})$ eine projektive $(G \times G')$-Auflösung von $\mathbb{Z} = \mathbb{Z} \otimes \mathbb{Z}$.*

Beweis Da nach Lemma 3.2 $X_p \otimes X'_q$ ein projektiver $(G \times G')$-Modul ist und damit auch $(X \otimes X')_n = \bigoplus_{p+q=n} X_p \otimes X'_q$, ist nur noch zu zeigen, dass

$$\ldots \xrightarrow{\overline{d}_2} (X_0 \otimes X'_1) \oplus (X_1 \otimes X'_0) \xrightarrow{\overline{d}_1} X_0 \otimes X'_0 \xrightarrow{\varepsilon\otimes\varepsilon'} \mathbb{Z} \to 0 \qquad (*)$$

exakt ist.

[5] vgl. [Lane], Kap. 5, §3

Nach Lemma 3.3 besitzt das Diagramm

$$
\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
\cdots \arrow[r] & X_2 \otimes X_1' \arrow[r, "1\otimes d_1'"] \arrow[d, "d_2\otimes 1"'] & X_2 \otimes X_0' \arrow[r, "1\otimes\varepsilon'"] \arrow[d, "d_2\otimes 1"'] & X_2 \otimes \mathbb{Z} \arrow[r] \arrow[d, "d_2\otimes 1"'] & 0 \\
\cdots \arrow[r] & X_1 \otimes X_1' \arrow[r, "1\otimes d_1'"] \arrow[d, "d_1\otimes 1"'] & X_1 \otimes X_0' \arrow[r, "1\otimes\varepsilon'"] \arrow[d, "d_1\otimes 1"'] & X_1 \otimes \mathbb{Z} \arrow[r] \arrow[d, "d_1\otimes 1"'] & 0 \\
\cdots \arrow[r] & X_0 \otimes X_1' \arrow[r, "1\otimes d_1'"] \arrow[d, "\varepsilon\otimes 1"'] & X_0 \otimes X_0' \arrow[r, "1\otimes\varepsilon'"] \arrow[d, "\varepsilon\otimes 1"'] & X_0 \otimes \mathbb{Z} \arrow[r] \arrow[d, "\varepsilon\otimes 1"'] & 0 \\
\cdots \arrow[r] & \mathbb{Z} \otimes X_1' \arrow[r, "1\otimes d_1'"] \arrow[d] & \mathbb{Z} \otimes X_0' \arrow[r, "1\otimes\varepsilon'"] \arrow[d] & \mathbb{Z} \otimes \mathbb{Z} = \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}
$$

exakte Zeilen und Spalten. (Projektive G-Moduln sind als $\mathbb{Z}$-Moduln frei.) Außerdem kommutiert jedes Quadrat.

- Da $\varepsilon \otimes 1$ und $1 \otimes \varepsilon'$ surjektiv sind, ist auch ihre Komposition $\varepsilon \otimes \varepsilon'$ surjektiv.

- Exaktheit von $(*)$ bei $X_0 \otimes X_0'$:
  Für alle $x_1 \otimes x_0' \in X_1 \otimes X_0'$ gilt:

$$
\begin{aligned}
((\varepsilon \otimes \varepsilon') \circ \overline{d}_1)(x_1 \otimes x_0') =& (\varepsilon \otimes \varepsilon')\big(d_1(x_1) \otimes x_0' - x_1 \otimes d_0'(x_0')\big) \\
=& \varepsilon(d_1(x_1)) \otimes \varepsilon'(x_0') = 0
\end{aligned}
$$

  und analog für alle $x_0 \otimes x_1' \in X_0 \otimes X_1'$:

$$
\begin{aligned}
((\varepsilon \otimes \varepsilon') \circ \overline{d}_1)(x_0 \otimes x_1') =& (\varepsilon \otimes \varepsilon')\big(d_0(x_0) \otimes x_1' + x_0 \otimes d_1'(x_1')\big) \\
=& \varepsilon(x_0) \otimes \varepsilon'(d_1'(x_1')) = 0
\end{aligned}
$$

  Also gilt: $(\varepsilon \otimes \varepsilon') \circ \overline{d}_1 = 0$.
  Der zweite Teil wird eine kleine Diagrammjagd:
  Sei $y \in \mathrm{Ker}(\varepsilon \otimes \varepsilon') \subset X_0 \otimes X_0'$. Dann ist $(\varepsilon \otimes 1)(y) \in \mathrm{Ker}(1 \otimes \varepsilon')$. Da die unterste Zeile in obigem Diagramm exakt ist, gibt es ein $z \in \mathbb{Z} \otimes X_1'$ mit $(1 \otimes d_1')(z) = (\varepsilon \otimes 1)(y)$. Des Weiteren gibt es ein $w_1 \in X_0 \otimes X_1'$ mit $(\varepsilon \otimes 1)(w_1) = z$. Damit gilt:

$$
\begin{aligned}
(\varepsilon \otimes 1)\big(y - (1 \otimes d_1')(w_1)\big) =& (\varepsilon \otimes 1)(y) - (\varepsilon \otimes d_1')(w_1) \\
=& (\varepsilon \otimes 1)(y) - (1 \otimes d_1')(z) = 0
\end{aligned}
$$

d. h. $y - (1 \otimes d_1')(w_1) \in \mathrm{Ker}(\varepsilon \otimes 1) = \mathrm{Im}(d_1 \otimes 1)$.
Somit gibt es ein $w_2 \in X_1 \otimes X_0'$ mit $(d_1 \otimes 1)(w_2) = y - (1 \otimes d_1')(w_1)$.
Nun ist $(w_1, w_2) \in (X_0 \otimes X_1') \oplus (X_1 \otimes X_0')$ ein gesuchtes Urbild von y bzgl. $\overline{d}_1$, denn es gilt:

$$\begin{aligned} \overline{d}_1(w_1, w_2) &= (d_0 \otimes 1 + 1 \otimes d_1')(w_1) + (d_1 \otimes 1 - 1 \otimes d_0')(w_2) \\ &= (1 \otimes d_1')(w_1) + (d_1 \otimes 1)(w_2) = y \end{aligned}$$

- Exaktheit von $(*)$ bei $\bigoplus_{p+q=n} X_p \otimes X_q'$ für $n > 0$:
  Da $(X \otimes X', \overline{d})$ Kettenkomplex ist, gilt $\overline{d}_n \circ \overline{d}_{n+1} = 0$. Noch zu zeigen ist, dass $\mathrm{Ker}(\overline{d}_n) \subset \mathrm{Im}(\overline{d}_{n+1})$.
  Angenommen $\mathrm{Ker}(\overline{d}_n) \not\subset \mathrm{Im}(\overline{d}_{n+1})$.
  Sei nun $(z_0, \ldots, z_k, z_{k+1}, \ldots, z_n) \in \mathrm{Ker}(\overline{d}_n) \setminus \mathrm{Im}(\overline{d}_{n+1})$, $z_i \in X_i \otimes X_{n-i}'$ mit $z_{k+1} = 0, \ldots, z_n = 0$ für geeignetes $k \leq n$. $(z_0, \ldots, z_k, z_{k+1}, \ldots, z_n)$ sei so gewählt, dass k möglichst klein ist, d. h. es gibt kein
  $(y_0, y_1, \ldots, y_n) \in \mathrm{Ker}(\overline{d}_n) \setminus \mathrm{Im}(\overline{d}_{n+1})$ mit $y_k = 0, y_{k+1} = 0, \ldots, y_n = 0$.

  Fall 1: $k < n$:
  Der Anteil von $\overline{d}_n(z_0, \ldots, z_k, 0, \ldots, 0)$ in $X_k \otimes X_{n-k-1}'$ ist $(-1)^k(1 \otimes d_{n-k})(z_k)$, da $z_{k+1} = 0$. Wegen $\overline{d}_n(z_0, \ldots, z_k, 0, \ldots, 0) = 0$ ist $z_k \in \mathrm{Ker}(1 \otimes d_{n-k}) = \mathrm{Im}(1 \otimes d_{n-k+1})$. Somit gibt es ein $w_k \in X_k \otimes X_{n-k+1}'$ mit $(1 \otimes d_{n-k+1})(w_k) = z_k$. Betrachte nun:

  $$\begin{aligned} v &:= (z_0, \ldots, z_{k-1}, z_k, 0, \ldots, 0) - (-1)^k \overline{d}_{n+1}(w_k) \\ &= (z_0, \ldots, z_{k-1}, z_k, 0, \ldots, 0) - (-1)^k (d_k \otimes 1 + (-1)^k (1 \otimes d_{n-k+1}'))(w_k) \\ &= (z_0, \ldots, z_{k-1}, z_k, 0, \ldots, 0) - (0, \ldots, (-1)^k (d_k \otimes 1)(w_k), z_k, 0 \ldots 0) \\ &= (z_0, \ldots, z_{k-1} - (-1)^k (d_k \otimes 1)(w_k), 0, \ldots, 0) \end{aligned}$$

  Da $(-1)^k \overline{d}_{n+1}(w_k) \in \mathrm{Im}(\overline{d}_{n+1}) \subset \mathrm{Ker}(\overline{d}_n)$ ist, ist zum einen $v \in \mathrm{Ker}(\overline{d}_n)$ und zum anderen $v \notin \mathrm{Im}(\overline{d}_{n+1})$, da $(z_0, \ldots, z_{k-1}, z_k, 0, \ldots, 0) \notin \mathrm{Im}(\overline{d}_{n+1})$. Dies widerspricht aber der Minimalität von k.

Fall 2: $k = n$:
Für die Diagrammjagd betrachten wir folgenden Teil des Diagramms:

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
\cdots \arrow[r] & X_{n+1} \otimes X'_1 \arrow[r, "1\otimes d'_1"] \arrow[d, "d_{n+1}\otimes 1"'] & X_{n+1} \otimes X'_0 \arrow[r, "1\otimes\varepsilon'"] \arrow[d, "d_{n+1}\otimes 1"'] & X_{n+1} \otimes \mathbb{Z} \arrow[r] \arrow[d, "d_{n+1}\otimes 1"'] & 0 \\
\cdots \arrow[r] & X_n \otimes X'_1 \arrow[r, "1\otimes d'_1"] \arrow[d, "d_n\otimes 1"'] & X_n \otimes X'_0 \arrow[r, "1\otimes\varepsilon'"] \arrow[d, "d_n\otimes 1"'] & X_n \otimes \mathbb{Z} \arrow[r] \arrow[d, "d_n\otimes 1"'] & 0 \\
\cdots \arrow[r] & X_{n-1} \otimes X'_1 \arrow[r, "1\otimes d'_1"] \arrow[d] & X_{n-1} \otimes X'_0 \arrow[r, "1\otimes\varepsilon'"] \arrow[d] & X_{n-1} \otimes \mathbb{Z} \arrow[r] \arrow[d] & 0 \\
 & \vdots & \vdots & \vdots &
\end{tikzcd}$$

Der Anteil von $\overline{d}_n(z_0, \dots, z_n)$ in $X_{n-1} \otimes X'_0$ ist
$(-1)^{n-1}(1 \otimes d'_1)(z_{n-1}) + (d_n \otimes 1)(z_n)$. Wegen $\overline{d}_n(z_0, \dots, z_n) = 0$ ist also $(-1)^{n-1}(1 \otimes d'_1)(z_{n-1}) + (d_n \otimes 1)(z_n) = 0$ und daher

$$0 = (1 \otimes \varepsilon')\big((-1)^{n-1}(1 \otimes d'_1)(z_{n-1}) + (d_n \otimes 1)(z_n)\big) = (d_n \otimes \varepsilon')(z_n)$$

Also ist $(1 \otimes \varepsilon')(z_n) \in \operatorname{Ker}(d_n \otimes 1) = \operatorname{Im}(d_{n+1} \otimes 1)$. Somit gibt es ein $y_{n+1} \in X_{n+1} \otimes \mathbb{Z}$ mit $(d_{n+1} \otimes 1)(y_{n+1}) = (1 \otimes \varepsilon')(z_n)$ und weiter ein $w_{n+1} \in X_{n+1} \otimes X'_0$ mit $(1 \otimes \varepsilon')(w_{n+1}) = y_{n+1}$.
Daher gilt:

$$\begin{aligned}
(1 \otimes \varepsilon')\big(z_n - (d_{n+1} \otimes 1)(w_{n+1})\big) &= (1 \otimes \varepsilon')(z_n) - (d_{n+1} \otimes \varepsilon')(w_{n+1}) \\
&= (1 \otimes \varepsilon')(z_n) - (d_{n+1} \otimes 1)(y_{n+1}) = 0
\end{aligned}$$

d. h. $\big(z_n - (d_{n+1} \otimes 1)(w_{n+1})\big) \in \operatorname{Ker}(1 \otimes \varepsilon') = \operatorname{Im}(1 \otimes d'_1)$.
Also gibt es ein $w_n \in X_n \otimes X'_1$ mit $(1 \otimes d'_1)(w_n) = z_n - (d_{n+1} \otimes 1)(w_{n+1})$, d. h. $z_n = (1 \otimes d'_1)(w_n) + (d_{n+1} \otimes 1)(w_{n+1})$.
Betrachte nun

$$\begin{aligned}
v &:= (z_0, \dots, z_n) - (-1)^n \overline{d}_{n+1}(w_n) - \overline{d}_{n+1}(w_{n+1}) \\
&= (z_0, \dots, z_n) - (-1)^n (d_n \otimes 1 + (-1)^n (1 \otimes d'_1))(w_n) \\
&\qquad - (d_{n+1} \otimes 1 + (-1)^{n+1}(1 \otimes d'_0))(w_{n+1}) \\
&= (z_0, \dots, z_n) - (0, \dots, (-1)^n (d_n \otimes 1)(w_n), z_n) \\
&= (z_0, \dots, z_{n-1} - (-1)^n (d_n \otimes 1)(w_n), 0)
\end{aligned}$$

Da $(-1)^n \overline{d}_{n+1}(w_n) + \overline{d}_{n+1}(w_{n+1}) \in \operatorname{Im}(\overline{d}_{n+1}) \subset \operatorname{Ker}(\overline{d}_n)$ ist, ist zum einen $v \in \operatorname{Ker}(\overline{d}_n)$ und zum anderen $v \notin \operatorname{Im}(\overline{d}_{n+1})$, da $(z_0, \dots, z_n) \notin \operatorname{Im}(\overline{d}_{n+1})$. Dies widerspricht aber der Minimalität von k. $\square$

3.2 Definition des Cup-Produkts

Definition 3.5 *Seien (X,d) eine projektive G-Auflösung und (X',d') eine projektive G'-Auflösung von $\mathbb{Z}$, B sei ein G-Modul und B' sei ein G'-Modul. Weiter seien $f \in \operatorname{Hom}_G(X_p, B)$ und $g \in \operatorname{Hom}_{G'}(X'_q, B')$ Koketten. Dann definieren wir die Kokette $f \otimes g \in \operatorname{Hom}_{G\times G'}((X \otimes X')_{p+q}, B \otimes B')$ durch ($x \in X_r, x' \in X'_s$):*

$$(f \otimes g)(x \otimes x') := \begin{cases} f(x) \otimes g(x') & \textit{falls } r = p, s = q \\ 0 & \textit{sonst} \end{cases}$$

Proposition 3.6 *Seien (X,d) eine projektive G-Auflösung und (X',d') eine projektive G'-Auflösung von $\mathbb{Z}$, B sei ein G-Modul und B' sei ein G'-Modul. Weiter seien $f \in \operatorname{Hom}_G(X_p, B)$ und $g \in \operatorname{Hom}_{G'}(X'_q, B')$ Koketten. Dann gilt:*

(i)	*f und g Kozykel*	$\Rightarrow$	*$f \otimes g$ Kozykel*
(ii)	*f Korand, g Kozykel*	$\Rightarrow$	*$f \otimes g$ Korand*
(iii)	*f Kozykel, g Korand*	$\Rightarrow$	*$f \otimes g$ Korand*

Beweis Wir behaupten $\overline{\delta}_{p+q+1}(f \otimes g) = (\delta_{p+1}(f) \otimes g) + (-1)^p(f \otimes \delta'_{q+1}(g))$. Um dies nachzuweisen, betrachten wir Folgendes:
Für alle $x_r \in X_r, x'_s \in X'_s$ mit $r + s = p + q + 1$ gilt einerseits

$$\begin{aligned} \overline{\delta}_{p+q+1}(f \otimes g)(x_r \otimes x'_s) &= (f \otimes g)\big(\overline{d}_{p+q+1}(x_r \otimes x'_s)\big) \\ &= (f \otimes g)\big(d_r(x_r) \otimes x'_s + (-1)^r x_r \otimes d'_s(x'_s)\big) \\ &= \begin{cases} f(d_r(x_r)) \otimes g(x'_s) & r = p+1, s = q \\ (-1)^r f(x_r) \otimes g(d'_s(x'_s)) & r = p, s = q+1 \\ 0 & \text{sonst} \end{cases} \end{aligned}$$

und andrerseits:

$$\begin{aligned} (\delta_{p+1}(f) \otimes g) &+ (-1)^p(f \otimes \delta'_{q+1}(g))(x_r \otimes x'_s) \\ &= (\delta_{p+1}(f) \otimes g)(x_r \otimes x'_s) + (-1)^p(f \otimes \delta'_{q+1}(g))(x_r \otimes x'_s) \\ &= \begin{cases} f(d_r(x_r)) \otimes g(x'_s) & r = p+1, s = q \\ (-1)^r f(x_r) \otimes g(d'_s(x'_s)) & r = p, s = q+1 \\ 0 & \text{sonst} \end{cases} \end{aligned}$$

(i), **(ii)** und **(iii)** folgen jetzt recht schnell:
Zu **(i)**: Ist $\delta_{p+1}(f) = 0$ und $\delta'_{q+1}(g) = 0$, so gilt:
$\overline{\delta}_{p+q+1}(f \otimes g) = (\delta_{p+1}(f) \otimes g) + (-1)^p(f \otimes \delta'_{q+1}(g)) = 0$.
Also ist $(f \otimes g)$ Kozykel.

Zu **(ii)**: Ist $f = \delta_p(h)$ und $\delta'_{q+1}(g) = 0$, so gilt:
$f \otimes g = \delta_p(h) \otimes g = \overline{\delta}_{p+q}(h \otimes g) - (-1)^{p-1} h \otimes \delta'_{q+1}(g) = \overline{\delta}_{p+q}(h \otimes g)$.
Also ist $(f \otimes g)$ Korand.

Die Rechnung zu **(iii)** läuft analog zu der zu **(ii)**. □

Korollar 3.7 *Die Abbildungen*

$$\mathrm{Hom}_G(X_p, B) \times \mathrm{Hom}_{G'}(X'_q, B') \to \mathrm{Hom}_{G\times G'}((X \otimes X')_{p+q}, B \otimes B')\,,$$

wie in Definition 3.5 eingeführt, induzieren bilineare Abbildungen in Kohomologie:

$$\times_H : H^p(G, B) \times H^q(G', B') \to H^{p+q}(G \times G', B \otimes B')$$

Definition 3.8 *Für G-Moduln A und B definieren wir das* **Cup-Produkt**

$$\cup : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

durch $\cup = (\Delta, 1)_* \circ \times_H$.

Bezeichnung Für das Cup-Produkt zweier Elemente $f \in H^q(G, A)$ und $g \in H^r(G, B)$ schreiben wir $f \cup g$ anstelle von $\cup(f, g)$.

Bemerkung Das Cup-Produkt ist assoziativ, d. h. für $f \in H^p(G, A)$, $g \in H^q(G, B)$ und $h \in H^r(G, C)$ gilt:

$$(f \cup g) \cup h = f \cup (g \cup h) \in H^{p+q+r}(G, A \otimes B \otimes C)$$

Definition 3.9 *Ist weiter ein G-Homomorphismus* $f : A \otimes B \to C$ *gegeben, so definieren wir das* **Cup-Produkt relativ zu f** *durch:*

$$\cup_f := (\Delta, f)_* \circ \times_H = (1, f)_* \circ \cup\,.$$

Beispiele:

1. A sei eine G-Algebra, d. h. ein G-Modul A mit einer Multiplikation auf A, die ein G-Homomorphismus $\mu : A \otimes A \to A$ ist. Dann ist für $f \in H^p(G, A), g \in H^q(G, A)$:

   $$f \cup_\mu g \in H^{p+q}(G, A)$$

   und wegen der Assoziativität von μ gilt $(f \cup_\mu g) \cup_\mu h = f \cup_\mu (g \cup_\mu h)$ für alle $f \in H^p(G, A), g \in H^q(G, A)$ und $h \in H^r(G, A)$.
   Speziell für $p = q = r = 0$ erhalten wir eine assoziative Multiplikation auf $H^0(G, A)$, d. h. $H^0(G, A)$ ist ein Ring. Nach der letzten Bemerkung in Kapitel 2 ist $H^0(G, A) \cong A^G$ als abelsche Gruppe. Man kann sogar zeigen, dass sie auch als Ringe isomorph sind.

2. R sei eine G-Algebra und A ein R-Modul, auf dem G operiert. Die Operation von G sei mit der Modulstruktur verträglich, d. h. $\forall \sigma \in G,\ r \in R,\ a \in A$ gilt $\sigma(ra) = \sigma(r) \cdot \sigma(a)$. Oder äquivalent dazu sei die Operation von G definiert durch einen Gruppenhomomorphismus $G \to \mathrm{Aut}_R(A)$. Diese Verträglichkeit besagt aber gerade, dass die Operation von R auf A, $R \otimes A \to A$, ein G-Homomorphismus ist.
   Durch das relative Cup-Produkt erhält man also eine Operation des Ringes $H^0(G,R)$ auf jede der Gruppen $H^n(G,A)$, d. h. $H^n(G,A)$ wird ein $H^0(G,R)$-Modul.

   Im Speziellen ist $H^n(G,R)$ auch ein $H^0(G,R)$-Modul.

3. (Spezialfall von 2.) G operiere auf R trivial.
   Dann ist $H^0(G,R) = R^G = R$ und für einen R-Modul A ist auch die Kohomologiegruppe $H^n(G,A)$ ein R-Modul.

4 Kohomologie von $\mathbb{Z}/p$

4.1 Bezeichnungen

In diesem Kapitel wird $\mathbb{Z}/p$, die zyklische Gruppe der Ordnung p, betrachtet.[6] Wir betrachten $\mathbb{Z}/p$ als multiplikative Gruppe mit Erzeuger γ. Der Gruppenring $\Gamma = \mathbb{Z}[\mathbb{Z}/p]$ ist dann der Ring der Polynome in γ mit ganzzahligen Koeffizienten modulo der Relation $\gamma^p = 1$. Zwei spezielle Elemente in Γ sind:

$$Tr = 1 + \gamma + \cdots + \gamma^{p-1} \quad \text{und} \quad \partial = \gamma - 1$$

4.2 Berechnung der Kohomologiegruppen

Lemma 4.1 *Eine projektive $\mathbb{Z}/p$-Auflösung von $\mathbb{Z}$ ist gegeben durch (X, d) mit*

$$X_n = \begin{cases} \mathbb{Z}[\mathbb{Z}/p] & n \geq 0 \\ 0 & n < 0 \end{cases}$$

und

$$d_n(x_n) = \begin{cases} Tr \cdot x_n & n > 0 \text{ gerade} \\ \partial \cdot x_n & n > 0 \text{ ungerade} \\ 0 & n \leq 0 \end{cases}$$

sowie

$$\varepsilon : X_0 \to \mathbb{Z}, \quad \varepsilon\left(\sum_{i=0}^{p-1} a_i \gamma^i\right) = \sum_{i=0}^{p-1} a_i.$$

Beweis

- $\mathbb{Z}[\mathbb{Z}/p]$ ist freier, also auch projektiver $\mathbb{Z}[\mathbb{Z}/p]$-Modul.

- Es ist $Tr \cdot \partial = \partial \cdot Tr = (\gamma - 1)\sum_{i=0}^{p-1} \gamma^i = \gamma^p - 1 = 0$, weshalb $d_{n-1} \circ d_n = 0$ $\forall n \in \mathbb{Z}$.
  Außerdem ist

$$\begin{aligned} \varepsilon \circ d_1 \left(\sum_{i=0}^{p-1} a_i \gamma^i\right) &= \varepsilon\left((\gamma - 1)\sum_{i=0}^{p-1} a_i \gamma^i\right) = \varepsilon\left(\sum_{i=0}^{p-1} a_i \gamma^{i+1} - \sum_{i=0}^{p-1} a_i \gamma^i\right) \\ &= \sum_{i=0}^{p-1} a_i - \sum_{i=0}^{p-1} a_i = 0. \end{aligned}$$

[6] Zu Beginn ist $p \in \mathbb{N}$ noch beliebig, doch wird später p stets eine ungerade Primzahl sein.

- zur Exaktheit: Da offensichtlich ε surjektiv ist, ist noch zu zeigen, dass $\mathrm{Ker}(d_{n-1}) \subset \mathrm{Im}(d_n)$ und $\mathrm{Ker}(\varepsilon) \subset \mathrm{Im}(d_1)$.

  Sei $u = \sum_{i=0}^{p-1} a_i\gamma^i$.
  Es ist $Tr \cdot u = \sum_{j=0}^{p-1} \gamma^j \cdot \sum_{i=0}^{p-1} a_i\gamma^i = \sum_{i=0}^{p-1} \left(\sum_{j=0}^{p-1} a_j\right)\gamma^i$.
  Ist also $Tr \cdot u = 0$, so folgt $\sum_{j=0}^{p-1} a_j = 0$. Für diese u gilt nun aber:

$$\begin{aligned} u &= \sum_{i=0}^{p-1} a_i\gamma^i = \sum_{i=0}^{p-1} a_i\gamma^i - \sum_{i=0}^{p-1} a_i \\ &= \sum_{i=0}^{p-1} a_i(\gamma^i - 1) = (\gamma - 1)\sum_{i=0}^{p-1} a_i(1 + \gamma + \cdots + \gamma^{i-1}) \\ &= \partial \cdot \sum_{i=0}^{p-1} a_i(1 + \gamma + \cdots + \gamma^{i-1}) \end{aligned}$$

  Daher ist $\mathrm{Ker}(d_{n-1}) \subset \mathrm{Im}(d_n)$ für ungerade n und $\mathrm{Ker}(\varepsilon) \subset \mathrm{Im}(d_1)$.

  Es ist

$$\begin{aligned} \partial \cdot u = (\gamma - 1) \cdot \sum_{i=0}^{p-1} a_i\gamma^i &= \sum_{i=0}^{p-1} a_i(\gamma^{i+1} - \gamma^i) \\ &= (a_{p-1} - a_0) + \sum_{i=1}^{p-1}(a_{i-1} - a_i)\gamma^i. \end{aligned}$$

  Ist also $\partial \cdot u = 0$, so folgt $a_0 = a_1 = \cdots = a_{p-1}$ und daher

$$u = \sum_{i=0}^{p-1} a_i\gamma^i = \sum_{i=0}^{p-1} a_0\gamma^i = Tr \cdot a_0.$$

  Daher ist $\mathrm{Ker}(d_{n-1}) \subset \mathrm{Im}(d_n)$ für gerade n.

$\square$

Bemerkung Für einen $\mathbb{Z}/p$-Modul A definieren wir die Abbildungen:

$$Tr_A : A \to A, a \mapsto Tr(a) \quad \text{und} \quad \partial_A : A \to A, a \mapsto \partial a.$$

Wenn der Modul aus dem Kontext ersichtlich ist, werden wir später den Index auch wieder weglassen, sodass Tr und ∂ nicht nur Elemente in Γ, sondern auch Abbildungen bezeichnen.

Satz 4.2 *Für die zyklische Gruppe $\mathbb{Z}/p$ der Ordnung p mit Erzeuger γ und einen $\mathbb{Z}/p$-Modul A gilt:*

$$\begin{aligned} H^0(\mathbb{Z}/p, A) &= \operatorname{Ker}(\partial_A) = A^{\mathbb{Z}/p} \\ H^n(\mathbb{Z}/p, A) &= \operatorname{Ker}(Tr_A)/\operatorname{Im}(\partial_A) \quad \forall\, n > 0 \text{ ungerade} \\ H^n(\mathbb{Z}/p, A) &= \operatorname{Ker}(\partial_A)/\operatorname{Im}(Tr_A) \quad \forall\, n > 0 \text{ gerade} \end{aligned}$$

Beweis Die Koketten von $\mathbb{Z}/p$ mit Koeffizienten in A sind $\mathcal{C}^n(\mathbb{Z}/p, A) = \operatorname{Hom}_\Gamma(X_n, A) = \operatorname{Hom}_\Gamma(\Gamma, A) \cong A$. Die letzte Isomorphie ist hierbei gegeben durch die Zuordnung $\operatorname{Hom}_\Gamma(\Gamma, A) \ni \alpha \,\widehat{=}\, \alpha(1) \in A$. Die Korandabbildungen δ_n sind nun genau die Abbildungen Tr_A bzw. ∂_A, woraus obige Isomorphien folgen. □

Korollar 4.3 *Für den trivialen $\mathbb{Z}/p$-Modul $\mathbb{Z}$ ergibt sich:*

$$\begin{aligned} H^0(\mathbb{Z}/p, \mathbb{Z}) &= \mathbb{Z} \\ H^n(\mathbb{Z}/p, \mathbb{Z}) &= 0 \quad \forall\, n > 0 \text{ ungerade} \\ H^n(\mathbb{Z}/p, \mathbb{Z}) &= \mathbb{Z}/p\mathbb{Z} \quad \forall\, n > 0 \text{ gerade} \end{aligned}$$

4.3 Berechnung des Cup-Produkts

Um das Cup-Produkt dieser Kohomologiegruppen zu berechnen, benötigt man nach Kapitel 3 eine Kettenabbildung $\Lambda : X \to X \otimes X$ so, dass $(\varepsilon \otimes \varepsilon) \circ \Lambda_0 = \varepsilon$. Wir verwenden die Auflösung aus Lemma 4.1, d. h. $X_n = \mathbb{Z}[\mathbb{Z}/p]\ \forall n \geq 0$.

Lemma 4.4 *Definiere für alle $r, q \geq 0$ die $\mathbb{Z}/p$-Homomorphismen $\Lambda_{r,q} : X_{r+q} \to X_r \otimes X_q$ durch*

$$\Lambda_{r,q}(1) := \begin{cases} 1 \otimes 1 & r \text{ gerade} \\ 1 \otimes \gamma & r \text{ ungerade}, q \text{ gerade} \\ \sum_{0 \leq k < l \leq p-1} \gamma^k \otimes \gamma^l & r \text{ ungerade}, q \text{ ungerade} \end{cases}$$

und setze für $n \geq 0$

$$\Lambda_n := \sum_{r=0}^{n} \Lambda_{r,n-r} : X_n \to (X \otimes X)_n = \bigoplus_{r=0}^{n} X_r \otimes X_{n-r}.$$

Mit $\Lambda_n := 0$ für $n < 0$ ist dann $(\Lambda_n) : X \to X \otimes X$ eine Kettenabbildung und es gilt $(\varepsilon \otimes \varepsilon) \circ \Lambda_0 = \varepsilon$.

Beweis Es gilt:

$$\begin{aligned}
(\gamma\otimes\gamma-1\otimes 1)\cdot\sum_{0\le k<l\le p-1}\gamma^k\otimes\gamma^l &= \sum_{k=0}^{p-2}\sum_{l=k+1}^{p-1}\gamma^{k+1}\otimes\gamma^{l+1}-\gamma^k\otimes\gamma^l\\
&= \sum_{k=1}^{p-1}\sum_{l=k+1}^{p}\gamma^k\otimes\gamma^l-\sum_{k=0}^{p-2}\sum_{l=k+1}^{p-1}\gamma^k\otimes\gamma^l\\
&= \sum_{k=1}^{p-1}\gamma^k\otimes\gamma^p+\sum_{l=p}^{p-1}\gamma^{p-1}\otimes\gamma^l-\sum_{l=1}^{p-1}\gamma^0\otimes\gamma^l\\
&= \sum_{k=0}^{p-1}\gamma^k\otimes 1-\sum_{l=0}^{p-1}1\otimes\gamma^l\\
&= Tr\otimes 1-1\otimes Tr
\end{aligned}$$

Wir zeigen nun, dass $\overline{d}_n\circ\Lambda_n(1)=\Lambda_{n-1}\circ d_n(1)\ \forall\, n>0$ gilt (für $n\le 0$ sind beide Seiten offensichtlich null). Da sowohl $\overline{d}_n\circ\Lambda_n$ als auch $\Lambda_{n-1}\circ d_n$ Homomorphismen von $\mathbb{Z}/p$-Moduln sind und $X_n=\mathbb{Z}[\mathbb{Z}/p]$ gilt, sind dann auch die Abbildungen gleich.
Linke Seite:

$$\begin{aligned}
\left(\overline{d}_n\circ\Lambda_n\right)(1) &= \overline{d}_n\left(\sum_{r=0}^{n}\Lambda_{r,n-r}(1)\right)\\
&= \sum_{r=0}^{n}\big((d_r\otimes 1)(\Lambda_{r,n-r}(1))+(-1)^r(1\otimes d_{n-r})(\Lambda_{r,n-r}(1))\big)
\end{aligned}$$

Der Anteil in $X_s\otimes X_{n-s-1}$ $(s=0,\dots,n-1)$ ist damit:

$$a_s:=(d_{s+1}\otimes 1)(\Lambda_{s+1,n-s-1}(1))+(-1)^s(1\otimes d_{n-s})(\Lambda_{s,n-s}(1))$$

Rechte Seite:

$$\left(\Lambda_{n-1}\circ d_n\right)(1)=\sum_{r=0}^{n-1}\Lambda_{r,n-r-1}(d_n(1))$$

Der Anteil in $X_s\otimes X_{n-s-1}$ $(s=0,\dots,n-1)$ ist damit:

$$b_s:=\Lambda_{s,n-s-1}(d_n(1))$$

Fallunterscheidungen:
Für n, s gerade gilt:

$$\begin{aligned}
a_s &= (d_{s+1} \otimes 1) \left(\sum_{0 \leq k < l \leq p-1} \gamma^k \otimes \gamma^l \right) + (1 \otimes d_{n-s})(1 \otimes 1) \\
&= \sum_{0 \leq k < l \leq p-1} (\gamma - 1)\gamma^k \otimes \gamma^l + 1 \otimes Tr \\
&= \sum_{l=0}^{p-1} \gamma^l \otimes \gamma^l - \sum_{l=0}^{p-1} 1 \otimes \gamma^l + 1 \otimes Tr \\
&= \sum_{l=0}^{p-1} \gamma^l \otimes \gamma^l = \Lambda_{s,n-s-1}(Tr) = b_s
\end{aligned}$$

Für n gerade, s ungerade gilt:

$$\begin{aligned}
a_s &= (d_{s+1} \otimes 1)(1 \otimes 1) - (1 \otimes d_{n-s}) \left(\sum_{0 \leq k < l \leq p-1} \gamma^k \otimes \gamma^l \right) \\
&= Tr \otimes 1 - \sum_{0 \leq k < l \leq p-1} \gamma^k \otimes (\gamma - 1)\gamma^l \\
&= Tr \otimes 1 - \sum_{k=0}^{p-1} \gamma^k \otimes \gamma^p + \sum_{k=0}^{p-1} \gamma^k \otimes \gamma^{k+1} \\
&= \Lambda_{s,n-s-1} \left(\sum_{k=0}^{p-1} \gamma^k \right) = b_s
\end{aligned}$$

Für n ungerade, s gerade gilt:

$$\begin{aligned}
a_s &= (d_{s+1} \otimes 1)(1 \otimes \gamma) - (1 \otimes d_{n-s})(1 \otimes 1) \\
&= (\gamma - 1) \otimes \gamma + 1 \otimes (\gamma - 1) = \gamma \otimes \gamma - 1 \otimes 1 \\
&= \Lambda_{s,n-s-1}(\gamma - 1) = b_s
\end{aligned}$$

Für n, s ungerade gilt:

$$\begin{aligned}
a_s &= (d_{s+1} \otimes 1)(1 \otimes 1) - (1 \otimes d_{n-s})(1 \otimes \gamma) \\
&= Tr \otimes 1 - 1 \otimes (Tr \cdot \gamma) \\
&= (\gamma \otimes \gamma - 1 \otimes 1) \sum_{0 \leq k < l \leq p-1} \gamma^k \otimes \gamma^l \,, \quad \text{da } Tr \cdot \gamma = Tr \,, \\
&= \sum_{0 \leq k < l \leq p-1} \gamma^{k+1} \otimes \gamma^{l+1} - \sum_{0 \leq k < l \leq p-1} \gamma^k \otimes \gamma^l \\
&= \Lambda_{s,n-s-1}(\gamma) - \Lambda_{s,n-s-1}(1) = b_s
\end{aligned}$$

Die letzte Bedingung, dass $(\varepsilon \otimes \varepsilon) \circ \Lambda_0 = \varepsilon$ gilt, ist offensichtlich. □

Seien nun $a \in A$ und $a' \in A'$ Vertreter von Elementen aus $H^r(\mathbb{Z}/p, A)$ bzw. $H^q(\mathbb{Z}/p, A')$ und $\alpha \in \mathrm{Hom}_\Gamma(X_p, A)$ mit $\alpha(1) = a$, $\alpha' \in \mathrm{Hom}_\Gamma(X'_q, A')$ mit $\alpha'(1) = a'$.
Für r gerade gilt:

$$a \cup a' = (\alpha \cup \alpha')(1) = (\alpha \otimes \alpha') \circ \Lambda_{r,q}(1) = (\alpha \otimes \alpha')(1 \otimes 1) = \alpha(1) \otimes \alpha'(1) = a \otimes a'$$

Für r ungerade und q gerade gilt:

$$\begin{aligned} a \cup a' &= (\alpha \otimes \alpha') \circ \Lambda_{r,q}(1) = (\alpha \otimes \alpha')(1 \otimes \gamma) = \alpha(1) \otimes \alpha'(\gamma) \\ &= \alpha(1) \otimes \gamma\alpha'(1) = \alpha(1) \otimes \alpha'(1) = a \otimes a' \end{aligned}$$

Hierbei wurde ausgenutzt, dass $a'(1) \in \mathrm{Ker}(\partial_A)$, d. h. $\gamma a'(1) = a'(1)$.
Das Cup-Produkt in zwei ungeraden Graden ist nicht durch eine einfache Formel zu beschreiben. Da es sowieso nicht gebraucht wird, lassen wir diese Rechnung weg.

4.4 Isomorphie der geraden bzw. der ungeraden Kohomologiegruppen

Für jeden $\mathbb{Z}/p$-Modul A ist die Abbildung $A \otimes \mathbb{Z} \to A, a \otimes 1 \mapsto a$, ein $\mathbb{Z}/p$-Homomorphismus ($\mathbb{Z}/p$ operiert trivial auf $\mathbb{Z}$).
Der Isomorphismus $H^n(\mathbb{Z}/p, A) \to H^{n+2}(\mathbb{Z}/p, A), \forall n \geq 1$, der der Identität $\mathrm{Ker}(Tr_A)/\mathrm{Im}(\partial_A) \to \mathrm{Ker}(Tr_A)/\mathrm{Im}(\partial_A)$ für ungerades n, bzw. $\mathrm{Ker}(\partial_A)/\mathrm{Im}(Tr_A) \to \mathrm{Ker}(\partial_A)/\mathrm{Im}(Tr_A)$ für gerade n entspricht, kann nun mit Hilfe des Cup-Produkts konstruiert werden. Für die Restklasse der $1 \in \mathbb{Z}$, $1_2 \in H^2(\mathbb{Z}/p, \mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$ ist nämlich

$$* \cup 1_2 : H^n(\mathbb{Z}/p, A) \to H^{n+2}(\mathbb{Z}/p, A),\ \alpha \mapsto \alpha \cup 1_2$$

nach vorherigen Berechnungen genau dieser Isomorphismus.

Seien R eine $\mathbb{Z}/p$-Algebra und A ein $R[\mathbb{Z}/p]$-Modul. Nach Beispiel 2 am Ende von Kapitel 3 ist $H^n(\mathbb{Z}/p, A)$ ein $H^0(\mathbb{Z}/p, R) = R^{\mathbb{Z}/p}$-Modul.

Satz 4.5 *Die Abbildung* $* \cup 1_2 : H^n(\mathbb{Z}/p, A) \to H^{n+2}(\mathbb{Z}/p, A), \alpha \mapsto \alpha \cup 1_2$ *ist ein Isomorphismus von* $R^{\mathbb{Z}/p}$*-Moduln.*

Beweis Das Diagramm

$$\begin{tikzcd} R \otimes A \otimes \mathbb{Z} \arrow[r] \arrow[d, "\mu \otimes 1"'] & R \otimes A \arrow[d, "\mu"] \\ A \otimes \mathbb{Z} \arrow[r] & A \end{tikzcd}$$

kommutiert, weshalb für alle $r \in R^{\mathbb{Z}/p}, \alpha \in H^n(\mathbb{Z}/p, A)$ gilt: $r \cup_\mu (\alpha \cup 1_2) = (r \cup_\mu \alpha) \cup 1_2$. □

Bezeichnung Da $H^n(\mathbb{Z}/p, A)$ und $H^{n+2}(\mathbb{Z}/p, A)$ isomorph sind, schreiben wir statt $H^n(\mathbb{Z}/p, A)$ auch oft $H^{ev}(\mathbb{Z}/p, A)$, falls $n > 0$ gerade ist, und $H^{od}(\mathbb{Z}/p, A)$, falls $n > 0$ ungerade ist.

Sei A eine $\mathbb{Z}/p$-Algebra. Durch das Cup-Produkt erhalten wir nun Abbildungen $H^2(\mathbb{Z}/p, A) \times H^{od}(\mathbb{Z}/p, A) \to H^{od}(\mathbb{Z}/p, A)$ und $H^2(\mathbb{Z}/p, A) \times H^{ev}(\mathbb{Z}/p, A) \to H^{ev}(\mathbb{Z}/p, A)$. Diese Abbildungen, wie in 4.3 berechnet, erfolgen durch Multiplikation der Restklassenvertreter in A. Wegen der Wohldefiniertheit gelten folgende Regeln (die auch durch direkte Rechnung verifiziert werden können):
Seien $x, z \in A$.

$$\begin{aligned}
x \in \mathrm{Ker}(\partial), z \in \mathrm{Ker}(Tr) &\;\Rightarrow\; x \cdot z \in \mathrm{Ker}(Tr) \\
x \in \mathrm{Ker}(\partial), z \in \mathrm{Im}(\partial) &\;\Rightarrow\; x \cdot z \in \mathrm{Im}(\partial) \\
x \in \mathrm{Ker}(\partial), z \in \mathrm{Ker}(\partial) &\;\Rightarrow\; x \cdot z \in \mathrm{Ker}(\partial) \\
x \in \mathrm{Ker}(\partial), z \in \mathrm{Im}(Tr) &\;\Rightarrow\; x \cdot z \in \mathrm{Im}(Tr)
\end{aligned}$$

und

$$\begin{aligned}
x \in \mathrm{Im}(Tr), z \in \mathrm{Ker}(Tr) &\;\Rightarrow\; x \cdot z \in \mathrm{Im}(\partial) \\
x \in \mathrm{Im}(Tr), z \in \mathrm{Ker}(\partial) &\;\Rightarrow\; x \cdot z \in \mathrm{Im}(Tr)
\end{aligned}$$

Anders gesagt erhalten wir folgende

Proposition 4.6 $\mathrm{Ker}(\partial)$ *ist ein Unterring*[7] *von* A *und* $\mathrm{Ker}(Tr)$, $\mathrm{Im}(\partial)$ *und* $\mathrm{Im}(Tr)$ *sind* $\mathrm{Ker}(\partial)$*-Moduln. Die Operation von* $\mathrm{Im}(Tr) \subset \mathrm{Ker}(\partial) = A^{\mathbb{Z}/p}$ *sowohl auf* $H^{ev}(\mathbb{Z}/p, A)$ *als auch auf* $H^{od}(\mathbb{Z}/p, A)$ *ist trivial, d. h. jedes Element aus* $\mathrm{Im}(Tr)$ *annulliert* $H^{ev}(\mathbb{Z}/p, A)$ *und* $H^{od}(\mathbb{Z}/p, A)$.

4.5 Koeffizienten in einem $\mathbb{F}_q$-Vektorraum

Sei nun p ungerade Primzahl und sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik p mit $|\mathbb{F}_q| = q = p^\nu$. $\mathbb{Z}/p$ operiere auf $\mathbb{F}_q$ trivial. Weiter sei W ein $\mathbb{F}_q$-Vektorraum, auf dem $\mathbb{Z}/p$ mittels einer Darstellung $\varrho : \mathbb{Z}/p \to \mathrm{Aut}_{\mathbb{F}_q}(W) = GL(W)$ operiere. In den Beispielen am Ende von Kapitel 3 haben wir gesehen, dass $H^n(\mathbb{Z}/p, W)$ wieder ein $\mathbb{F}_q$-Vektorraum ist.

Satz 4.7 $\mathbb{Z}/p$ *operiere auf dem* $\mathbb{F}_q$*-Vektorraum* W *mittels einer Darstellung* $\varrho : \mathbb{Z}/p \to \mathrm{Aut}_{\mathbb{F}_q}(W)$. *Dann sind* $H^{od}(\mathbb{Z}/p, W)$ *und* $H^{ev}(\mathbb{Z}/p, W)$ *isomorph als* $\mathbb{F}_q$*-Vektorräume.*

[7] Diese Tatsache ergibt sich auch aus $\mathrm{Ker}(\partial) = A^{\mathbb{Z}/p}$.

Beweis Wir betrachten die exakte Folge von Vektorräumen

$$0 \to \operatorname{Ker}(\partial) \to W \stackrel{\partial}{\to} W \to \operatorname{Coker}(\partial) \to 0.$$

Diese Folge liefert einen Vektorraum-Isomorphismus

$$\operatorname{Ker}(\partial) \oplus W \cong W \oplus \operatorname{Coker}(\partial)$$

und daher

$$\operatorname{Ker}(\partial) \cong \operatorname{Coker}(\partial)$$

Des weiteren induziert $Tr : W \to W$ eine Abbildung $Tr : \operatorname{Coker}(\partial) \to \operatorname{Ker}(\partial)$. Der Kern dieser Abbildung ist aber gerade $\operatorname{Ker}(Tr)/\operatorname{Im}(\partial) = H^{od}(\mathbb{Z}/p, W)$ und der Kokern ist $\operatorname{Ker}(\partial)/\operatorname{Im}(Tr) = H^{ev}(\mathbb{Z}/p, W)$. Also erhalten wir die exakte Folge

$$0 \to H^{od}(\mathbb{Z}/p, W) \to \operatorname{Coker}(\partial) \stackrel{Tr}{\to} \operatorname{Ker}(\partial) \to H^{ev}(\mathbb{Z}/p, W) \to 0$$

und dadurch einen Isomorphismus

$$H^{od}(\mathbb{Z}/p, W) \oplus \operatorname{Ker}(\partial) \cong H^{ev}(\mathbb{Z}/p, W) \oplus \operatorname{Coker}(\partial).$$

Zusammen mit $\operatorname{Ker}(\partial) \cong \operatorname{Coker}(\partial)$ folgt somit $H^{od}(\mathbb{Z}/p, W) \cong H^{ev}(\mathbb{Z}/p, W)$. $\square$

5 Die Kohomologiegruppen $H^m(\mathbb{Z}/p, \mathbb{F}_q[V])$

Sei im Folgenden stets p eine ungerade Primzahl und $\mathbb{F}_q$ ein endlicher Körper der Charakteristik p mit $|\mathbb{F}_q| = q = p^\nu$.
Im letzten Kapitel wurde gezeigt, dass für einen $\mathbb{F}_q$-Vektorraum W alle Kohomologiegruppen $H^m(\mathbb{Z}/p, W), m > 0$, als Vektorräume über $\mathbb{F}_q$ isomorph sind. Es stellt sich nun die Frage, ob $H^{ev}(\mathbb{Z}/p, W)$ und $H^{od}(\mathbb{Z}/p, W)$ nicht nur als $\mathbb{F}_q$-Vektorräume isomorph sind, sondern auch unter stärkeren Aspekten, z. B. als Moduln über $W^{\mathbb{Z}/p}$ oder einem Unterring, wenn W eine $\mathbb{Z}/p$-Algebra ist.

Für die Invariantentheorie interessant sind hier die Kohomologiegruppen von $\mathbb{Z}/p$ mit Koeffizienten in der Algebra $\mathbb{F}_q[V]$, der Algebra[8] der polynomialen Formen auf dem Vektorraum V. Dieses und die nächsten Kapitel werden zeigen, dass im Allgemeinen $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V]) \ncong H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ als $\mathbb{F}_q[V]^{\mathbb{Z}/p}$-Moduln gilt, aber stets $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V]) \cong H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ als Moduln über der Dicksonalgebra $D(n) = \mathbb{F}_q[V]^{GL(V)}$ (n bezeichne hierbei die Dimension von V).

5.1 Operation von $\mathbb{Z}/p$ auf $\mathbb{F}_q[V]$

Rechenregeln in $\mathbb{F}_q$:

(i) $Tr = 1 + \gamma + \cdots + \gamma^{p-1} = (\gamma - 1)^{p-1} = \partial^{p-1} \in \mathbb{F}_q[\mathbb{Z}/p]$.

(ii) $\forall \lambda \in \mathbb{F}_q$ ist $\lambda^q = \lambda$.

(iii) $\forall x, y \in \mathbb{F}_q[V]$ gilt: $(x + y)^q = x^q + y^q$

(iv) $\forall x, y \in \mathbb{F}_q[V]$ gilt: $\prod_{\lambda \in \mathbb{F}_q} (x - \lambda y) = x^q - xy^{q-1}$

(v) $\forall x, y \in \mathbb{F}_q[V]$ gilt: $\prod_{i=0}^{p-1} (x - iy) = x^p - xy^{p-1}$

Wir betrachten zunächst eine unzerlegbare Darstellung $\varrho : \mathbb{Z}/p \to GL(V)$, d. h. einen Gruppenhomomorphismus ϱ so, dass es keine echte Zerlegung von V als Summe $\mathbb{Z}/p$-invarianter Unterräume gibt.

Lemma 5.1 *Es gibt eine Basis $\{x_1, \ldots, x_n\}$ von V so, dass die Matrix von $\varrho(\gamma)$ bzgl. dieser Basis ein Jordanblock* $J = \begin{pmatrix} 1 & & \ldots & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 1 \end{pmatrix}$ *ist.*

[8] Vergleiche hierzu [NeSmi] Kap. 1.

Beweis Wegen $\gamma^p = 1$ gilt $\varrho(\gamma)^p - 1 = 0 \in End_{\mathbb{F}_q}(V)$. Aber $\varrho(\gamma)^p - 1 = (\varrho(\gamma) - 1)^p$ nach den Rechenregeln in $\mathbb{F}_q$. Das Minimalpolynom [9] von $\varrho(\gamma)$ zerfällt also in Linearfaktoren und hat 1 als einzige Nullstelle. Somit lässt sich $\varrho(\gamma)$ auf Jordanform bringen und 1 ist einziger Eigenwert von $\varrho(\gamma)$. Da die Darstellung unzerlegbar sein soll, existiert nur ein Jordanblock. Also ist die Matrix von $\varrho(\gamma)$ bezüglich der Jordanbasis $\{x_1, \ldots, x_n\}$ gerade die obige. □

Bemerkung Für die Matrix J gilt $J^p = 1$ genau dann, wenn ihr Rang$(J) \leq p$ ist, also $n \leq p$. Ist $n > p$, so gibt es also gar keine unzerlegbare Darstellung von $\mathbb{Z}/p$.

Sei nun $\{x_1, \ldots, x_n\}$ die Jordanbasis zu $\varrho(\gamma)$ und $\{z_1, \ldots, z_n\}$ die zugehörige duale Basis von V^*. Dann ist $\mathbb{F}_q[V] = \mathbb{F}_q[z_1, \ldots, z_n]$. Auf V^* operiert nun $\mathbb{Z}/p$ durch

$$\gamma(z) := z \circ \varrho(\gamma) \ \forall z \in V^*.$$

Speziell gilt:

$$\begin{aligned} \gamma(z_1) &= z_1, \\ \gamma(z_j) &= z_j + z_{j-1}, \quad 2 \leq j \leq n \end{aligned}$$

Auf $\mathbb{F}_q[V]$ operiert $\mathbb{Z}/p$, indem es auf $V^* \subset \mathbb{F}_q[V]$ wie eben definiert und auf Summen bzw. Produkten summandenweise bzw. faktorweise operiert. $\mathbb{F}_q[V]$ wird dadurch eine $\mathbb{Z}/p$-Algebra.

Als Polynomalgebra ist $\mathbb{F}_q[V]$ sogar eine graduierte Algebra. Da $\mathbb{Z}/p$ graderhaltend operiert, ist $\mathbb{F}_q[V]$ damit eine graduierte $\mathbb{Z}/p$-Algebra. Jedes Polynom lässt sich als Summe homogener Polynome schreiben, weshalb wir im Folgenden auch nur homogene Polynome betrachten. Alle Beweise, die später erbracht werden, lassen sich direkt von homogenen Polynomen auf beliebige Polynome übertragen. Den sogenannten homogenen Anteil von $\mathbb{F}_q[V]$ im Grad m bezeichnen wir mit $\mathbb{F}_q[V]_m$.

5.2 Berechnung für $\dim(V) = 2$

In diesem Unterkapitel betrachten wir den Fall $\dim(V) = 2$.
Um Verwirrung durch Indizes zu vermeiden, bezeichnen wir die Basis von V^* jetzt nicht mit $\{z_1, z_2\}$, sondern mit $\{z, y\}$. Es gilt dann

$$\gamma(z) = z \quad \text{und} \quad \gamma(y) = y + z.$$

[9] Das Minimalpolynom $m(t)$ ist ein Teiler von $(t-1)^p$, da es jedes Polynom teilt, das $\varrho(\gamma)$ annulliert.

Weiter gilt also $\gamma^k(y) = y + kz\ \forall\, k \in \mathbb{Z}$.
Wir werden später auch die Gleichung

$$\prod_{i=0}^{p-1} \gamma^{-i}(y) = \prod_{i=0}^{p-1}(y - iz) = y^p - yz^{p-1}$$

benutzen.

Für die Berechnung der Kohomologiegruppen müssen wir zunächst $\mathrm{Ker}(\partial)$, $\mathrm{Im}(\partial)$, $\mathrm{Ker}(Tr) = \mathrm{Ker}(\partial^{p-1})$ und $\mathrm{Im}(Tr) = \mathrm{Im}(\partial^{p-1})$ berechnen. Da die Gruppenoperation graderhaltend ist, können wir die Operation von ∂ gradweise betrachten. Die Polynome $\{z^{m-n} \cdot \prod_{i=0}^{n-1} \gamma^{-i}(y) | n = 0, \ldots m\}$ bilden eine Basis von $\mathbb{F}_q[z, y]_m$ als $\mathbb{F}_q$-Vektorraum (das leere Produkt ist gleich 1).
Nun ist

$$\partial(z^m) = \gamma(z)^m - z^m = 0$$

und für $n > 0$ gilt:

$$\begin{aligned}
\partial\left(z^{m-n} \cdot \prod_{i=0}^{n-1} \gamma^{-i}(y)\right) &= \gamma(z)^{m-n} \cdot \prod_{i=0}^{n-1} \left(\gamma^{1-i}(y)\right) - z^{m-n} \cdot \prod_{i=0}^{n-1} \gamma^{-i}(y) \\
&= z^{m-n} \cdot \prod_{i=0}^{n-2} \gamma^{-i}(y) \cdot \left(\gamma(y) - \gamma^{1-n}(y)\right) \\
&= n \cdot z^{m-(n-1)} \cdot \prod_{i=0}^{n-2} \gamma^{-i}(y)
\end{aligned}$$

Die zu ∂ gehörige Abbildungsmatrix bezüglich dieser Basis ist also:

$$\begin{pmatrix}
0 & 1 & 0 & \ldots & \ldots & 0 \\
\vdots & 0 & 2 & 0 & & \vdots \\
 & & \ddots & \ddots & \ddots & \vdots \\
 & & & \ddots & \ddots & 0 \\
\vdots & & & & 0 & m \\
0 & \ldots & & & \ldots & 0
\end{pmatrix}$$

Unter Beachtung von $p = 0$ in $\mathbb{F}_q$ erhält man also im Grad m:

$$\begin{aligned}
\mathrm{Ker}(\partial)_m &= \mathrm{Span}_{\mathbb{F}_q}\{z^{m-pn} \cdot \textstyle\prod_{i=0}^{pn-1} \gamma^{-i}(y) \mid 0 \le pn \le m\} \\
\mathrm{Im}(\partial)_m &= \mathrm{Span}_{\mathbb{F}_q}\{z^{m-n} \cdot \textstyle\prod_{i=0}^{n-1} \gamma^{-i}(y) \mid n = 0, \ldots, m-1; p \text{ teilt nicht } n+1\} \\
\mathrm{Ker}(\partial^{p-1})_m &= \mathrm{Span}_{\mathbb{F}_q}\{z^{m-n} \cdot \textstyle\prod_{i=0}^{n-1} \gamma^{-i}(y) \mid n = 0, \ldots, m; p \text{ teilt nicht } n+1\} \\
\mathrm{Im}(\partial^{p-1})_m &= \mathrm{Span}_{\mathbb{F}_q}\{z^{m-pn} \cdot \textstyle\prod_{i=0}^{pn-1} \gamma^{-i}(y) \mid 0 \le pn \le m-p+1\}
\end{aligned}$$

Für die graduierten Moduln erhalten wir also:

$$\begin{aligned}
\operatorname{Ker}(\partial) &= \operatorname{Span}_{\mathbb{F}_q}\{z^k \cdot (y^p - z^{p-1}y)^n \mid k,n \geq 0\} \\
\operatorname{Im}(\partial) &= \operatorname{Span}_{\mathbb{F}_q}\{z^{k+1}(y^p - z^{p-1}y)^n \cdot \textstyle\prod_{i=0}^{l-1}\gamma^{-i}(y) \mid k,n \geq 0; l = 0,\ldots,p-2\} \\
\operatorname{Ker}(\partial^{p-1}) &= \operatorname{Span}_{\mathbb{F}_q}\{z^k \cdot (y^p - z^{p-1}y)^n \cdot \textstyle\prod_{i=0}^{l-1}\gamma^{-i}(y) \mid k,n \geq 0; l = 0,\ldots,p-2\} \\
\operatorname{Im}(\partial^{p-1}) &= \operatorname{Span}_{\mathbb{F}_q}\{z^{k+p-1} \cdot (y^p - z^{p-1}y)^n \mid k,n \geq 0\}
\end{aligned}$$

oder kurz:

$$\begin{aligned}
\operatorname{Ker}(\partial) &= \mathbb{F}_q\left[z, y^p - z^{p-1}y\right] \\
\operatorname{Im}(\partial) &= \langle z \cdot \textstyle\prod_{i=0}^{l-1}\gamma^{-i}(y) \mid l = 0,\ldots,p-2\rangle \cdot \mathbb{F}_q\left[z, y^p - z^{p-1}y\right] \\
\operatorname{Ker}(\partial^{p-1}) &= \langle \textstyle\prod_{i=0}^{l-1}\gamma^{-i}(y) \mid l = 0,\ldots,p-2\rangle \cdot \mathbb{F}_q\left[z, y^p - z^{p-1}y\right] \\
\operatorname{Im}(\partial^{p-1}) &= \langle z^{p-1}\rangle \cdot \mathbb{F}_q\left[z, y^p - z^{p-1}y\right]
\end{aligned}$$

Und daher:

$$\begin{aligned}
H^{od}(\mathbb{Z}/p, \mathbb{F}_q[z,y]) &= \frac{\operatorname{Ker}(\partial^{p-1})}{\operatorname{Im}(\partial)} = \frac{\operatorname{Ker}(\partial^{p-1})}{z \cdot \operatorname{Ker}(\partial^{p-1})} \\
H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[z,y]) &= \frac{\operatorname{Ker}(\partial)}{\operatorname{Im}(\partial^{p-1})} = \frac{\operatorname{Ker}(\partial)}{z^{p-1} \cdot \operatorname{Ker}(\partial)}
\end{aligned}$$

Satz 5.2 *$H^{od}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ und $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ sind nicht isomorph als Moduln über $\mathbb{F}_q[z,y]^{\mathbb{Z}/p}$.*

Beweis Aufgrund der Gleichung $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[z,y]) = \frac{\operatorname{Ker}(\partial^{p-1})}{\operatorname{Im}(\partial)} = \frac{\operatorname{Ker}(\partial^{p-1})}{z\cdot\operatorname{Ker}(\partial^{p-1})}$ wird ganz $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ von $z \in \mathbb{F}_q[z,y]^{\mathbb{Z}/p}$ annulliert. Andrerseits ist z. B. $z \cdot 1 = z \notin \operatorname{Im}(\partial^{p-1}) = z^{p-1} \cdot \operatorname{Ker}(\partial)$, d. h. die von 1 vertretene Restklasse in $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ wird von z nicht annulliert. Damit können $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ und $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ als Moduln über dem Invariantenring $\mathbb{F}_q[z,y]^{\mathbb{Z}/p}$ nicht isomorph sein. □

Die Kohomologiegruppen sind also nicht isomorph als Moduln über dem Invariantenring $\mathbb{F}_q[z,y]^{\mathbb{Z}/p}$. Betrachten wir nun die Kohomologiegruppen als Moduln über der Dicksonalgebra $D(2) = \mathbb{F}_q[z,y]^{GL(V)}$. Wie in [Wilk] nachzulesen ist (vgl. auch nächstes Kapitel), ist die Dicksonalgebra eine Polynomalgebra $D(2) = \mathbb{F}_q[d_{2,0}, d_{2,1}]$ mit

$$d_{2,0} = z^{q-1}\left(y^q - yz^{q-1}\right)^{q-1} \text{ und } d_{2,1} = z^{(q-1)q} + \left(y^q - yz^{q-1}\right)^{q-1}.$$

Wegen $d_{2,1} \in \mathbb{F}_q[z,y]^{\mathbb{Z}/p}$ und $z^{(q-1)q} \in \mathbb{F}_q[z,y]^{\mathbb{Z}/p}$ ist auch $(y^q - yz^{q-1})^{q-1} \in \mathbb{F}_q[z,y]^{\mathbb{Z}/p}$. Somit ist $d_{2,0} \in z^{p-1} \cdot \mathrm{Ker}(\partial) = \mathrm{Im}(\partial^{p-1})$ und operiert damit trivial auf $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ und $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ (vgl. Prop 4.6). Dagegen operiert $d_{2,1}$ auf beiden Kohomologiegruppen wie $f := (y^q - yz^{q-1})^{q-1}$. Da f als Summand das Monom $y^{(q-1)q}$ enthält, gilt für alle $g \in \mathrm{Ker}(\partial)$:

$$f \cdot g \in \mathrm{Im}(\partial^{p-1}) \Leftrightarrow g \in \mathrm{Im}(\partial^{p-1})$$

und für alle $g \in \mathrm{Ker}(\partial^{p-1})$:

$$f \cdot g \in \mathrm{Im}(\partial) \Leftrightarrow g \in \mathrm{Im}(\partial)$$

(Vergleiche hierzu auch den Beweis für allgemeines n in Lemma 6.11.)
Somit operiert f (und damit auch $d_{2,1}$) frei sowohl auf $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$ als auch auf $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[z,y])$. Da die Kohomologiegruppen aber als graduierte Vektorräume über $\mathbb{F}_q$ isomorph sind, sind sie somit isomorphe freie $\mathbb{F}_q[d_{2,1}]$-Moduln, also isomorphe $D(2)$-Moduln.

Für den Fall $\dim(V) = 2$ sind also alle Kohomologiegruppen isomorph als Moduln über der Dicksonalgebra $D(2) = \mathbb{F}_q[V]^{GL(V)}$. Im folgenden Kapitel werden wir zeigen, dass auch im Allgemeinen die Kohomologiegruppen isomorph als Moduln über der Dicksonalgebra $D(n) = \mathbb{F}_q[V]^{GL(V)}$, $n = \dim(V)$, sind, zunächst für eine unzerlegbare Darstellung von $\mathbb{Z}/p$ und anschließend auch für eine beliebige Darstellung von $\mathbb{Z}/p$.

6 Isomorphie der Kohomologiegruppen als Moduln über der Dicksonalgebra

6.1 Die Dicksonalgebra

Wir übernehmen die Bezeichnungen aus dem vorigen Kapitel. Insbesondere operiere $\mathbb{Z}/p$ mittels einer unzerlegbaren Darstellung $\varrho : \mathbb{Z}/p \to GL(V)$ auf $\mathbb{F}_q[V]$. Die Dicksonalgebra ist definiert als $D(n) = \mathbb{F}_q[V]^{GL(V)}$, wobei $n = \dim(V)$. In verschiedenen Büchern, z. B. in [Wilk], ist nachzulesen, dass $D(n)$ eine Polynomalgebra in n Variablen ist, d. h. $D(n) = \mathbb{F}_q[d_{n,0}, \dots, d_{n,n-1}]$. Hierbei sind die $d_{n,i}$ definiert als die Koeffizienten des folgenden Polynoms:

$$\prod_{z \in V^*} (X - z) = X^{q^n} - d_{n,n-1} \cdot X^{q^{n-1}} + \cdots \pm d_{n,1} \cdot X^q \mp d_{n,0} \cdot X$$

Wie in [Wilk] auch zu lesen ist, lassen sich die Dicksonpolynome rekursiv berechnen mit der Formel:[10]

$$d_{n,i} = d_{n-1,i-1}^q + d_{n-1,i} \left(\prod_{v \in \mathrm{Span}\{z_1,\dots,z_{n-1}\}} (z_n - v) \right)^{q-1}$$

Diese Formel ist für unsere Zwecke äußerst praktisch, weil, wie wir im Folgenden zeigen werden, auch die „niedrigeren“ Dicksonpolynome $d_{k,i}$ mit $k < n$ und auch die Produkte $\prod_{v \in \mathrm{Span}\{z_1,\dots,z_{k-1}\}} (z_k - v)$ in $\mathbb{F}_q[z_1, \dots, z_n]^{\mathbb{Z}/p}$ liegen.

6.2 Vorbereitende Definitionen und Lemmata

Definition 6.1 *Für $0 \le k \le n$ sei V_k^* der von $\{z_1, z_2, \dots, z_k\}$ aufgespannte Untervektorraum von V^* (speziell $V_0^* = \{0\}$ und $V_n^* = V^*$).*

Bemerkung V_k^* ist invariant unter der Operation von $\gamma \in \mathbb{Z}/p$.

Definition 6.2 *Für $0 \le k \le n$ werden Funktionen $f_k : V^* \to \mathbb{F}_q[V]$ definiert durch*

$$f_k(x) := \prod_{v \in V_k^*} (x - v), \qquad x \in V^*$$

Bemerkung Es gilt $f_k(x) = 0 \Leftrightarrow x \in V_k^*$ und für $x \in V^* \setminus V_k^*$ hat $f_k(x)$ Grad q^k in $\mathbb{F}_q[V]$.

[10] Für $i = 0$ bzw. $i = n-1$ müssen $d_{n-1,i-1}$ bzw. $d_{n-1,i}$ als 0 bzw. 1 gesetzt werden. Vergleiche hierzu auch Proposition 6.3.

Proposition 6.3 *Für $0 \leq k \leq n$ und $j \leq k$ lassen sich die Dicksonpolynome in k Variablen berechnen durch:*

$$d_{k,j} = \begin{cases} 0 & j < 0 \\ 1 & k = j \geq 0 \\ d_{k-1,j-1}^{\,q} + d_{k-1,j} \cdot f_{k-1}(z_k)^{q-1} & 0 \leq j \leq k-1 \end{cases}$$

Beweis Siehe [Wilk]. □

Lemma 6.4 *Die Abbildungen f_k sind linear für alle $0 \leq k \leq n$ und für $1 \leq k \leq n$ gilt die Rekursionsformel*

$$f_k(x) = f_{k-1}(x)^q - f_{k-1}(x) f_{k-1}(z_k)^{q-1} .$$

Beweis durch Induktion
Induktionsanfang: $k = 0$:

$$f_0(x) = \prod_{v \in V_0^*} (x - v) = x - 0 = x$$

ist offensichtlich linear.
Induktionsschluss:

$$\begin{aligned} f_k(x) &= \prod_{v \in V_k^*} (x - v) = \prod_{\lambda \in \mathbb{F}_q} \prod_{v \in V_{k-1}^*} \big(x - (\lambda \cdot z_k + v)\big) \\ &= \prod_{\lambda \in \mathbb{F}_q} f_{k-1}(x - \lambda \cdot z_k) \\ &= \prod_{\lambda \in \mathbb{F}_q} \big(f_{k-1}(x) - \lambda \cdot f_{k-1}(z_k)\big) \quad \text{nach } \textit{Ind.-Vor.} \\ &= f_{k-1}(x)^q - f_{k-1}(x) f_{k-1}(z_k)^{q-1} \end{aligned}$$

Somit gilt die Rekursionsformel für k.
Linearität von f_k:

$$\begin{aligned} & f_k(\lambda x + \mu y) \\ &\quad = f_{k-1}(\lambda x + \mu y)^q - f_{k-1}(\lambda x + \mu y) f_{k-1}(z_k)^{q-1} \\ &\quad = \big(\lambda f_{k-1}(x) + \mu f_{k-1}(y)\big)^q - \big(\lambda f_{k-1}(x) + \mu f_{k-1}(y)\big) f_{k-1}(z_k)^{q-1} \\ &\quad = \lambda^q f_{k-1}(x)^q + \mu^q f_{k-1}(y)^q - \big(\lambda f_{k-1}(x) + \mu f_{k-1}(y)\big) f_{k-1}(z_k)^{q-1} \\ &\quad = \lambda \left(f_{k-1}(x)^q - f_{k-1}(x) f_{k-1}(z_k)^{q-1}\right) \\ &\quad\quad + \mu \left(f_{k-1}(y)^q - f_{k-1}(y) f_{k-1}(z_k)^{q-1}\right) \\ &\quad = \lambda f_k(x) + \mu f_k(y) \end{aligned}$$

□

Lemma 6.5 *f_k vertauscht mit γ.*

Beweis

$$\begin{aligned} f_k\big(\gamma(x)\big) &= \prod_{v\in V_k^*}\big(\gamma(x)-v\big) \\ &= \prod_{v\in V_k^*}\big(\gamma(x)-\gamma(v)\big), \quad \text{da } V_k^* \ \gamma\text{-invariant}, \\ &= \gamma\left(\prod_{v\in V_k^*}(x-v)\right) \\ &= \gamma\big(f_k(x)\big) \end{aligned}$$

□

Korollar 6.6 *f_k vertauscht mit ∂.*

Beweis Wegen der Linearität von f_k und nach vorigem Lemma gilt:

$$f_k\big(\partial(x)\big) = f_k\big(\gamma(x)-x\big) = f_k\big(\gamma(x)\big) - f_k(x) = \gamma\big(f_k(x)\big) - f_k(x) = \partial\big(f_k(x)\big)$$

□

Lemma 6.7 *$f_k(z_{k+1}) \in \mathrm{Ker}(\partial)$ für $0 \leq k \leq n-1$ und $f_k(z_{k+1}) \in \mathrm{Im}(\partial)$ für $0 \leq k \leq n-2$.*

Beweis Es ist:

$$\partial z_{k+1} = \begin{cases} z_k \in V_k^* & 1 \leq k \leq n-1 \\ 0 \in V_0^* & k = 0 \end{cases}$$

Somit:

$$\partial\big(f_k(z_{k+1})\big) = f_k\big(\partial(z_{k+1})\big) = 0$$

nach Korollar 6.6 und der Bemerkung zu Beginn des Kapitels.
Also gilt: $f_k(z_{k+1}) \in \mathrm{Ker}(\partial)$ für $0 \leq k \leq n-1$.
Weiter gilt: $z_{k+1} = \partial z_{k+2}$ für $0 \leq k \leq n-2$ und daher:

$$f_k(z_{k+1}) = f_k(\partial z_{k+2}) = \partial f_k(z_{k+2}) \in \mathrm{Im}(\partial).$$

□

Lemma 6.8 *Sei $h \in \mathbb{F}_q[V]$. Dann gilt für $h \in \mathrm{Ker}(\partial) \cap \mathrm{Im}(\partial)$:*

$$h^j \in \mathrm{Im}(\partial^j) \quad \forall\ 1 \leq j \leq p-1$$

und

$$h^l \in \mathrm{Im}(\partial^j) \quad \forall\ 1 \leq j \leq p-1, l \geq j.$$

Beweis Sei $h = \partial x$ und $1 \leq j \leq p-1$. Dann setze für $0 \leq i \leq j$:

$$y_i := \frac{1}{(j-i)!} h^i \prod_{\nu=0}^{j-i-1} \gamma^{-\nu}(x)$$

(speziell gilt dann $y_j = h^j$)
Behauptung: Es gilt $\partial y_i = y_{i+1}$
Beweis der Behauptung (*Rechnung*):

$$\begin{aligned}
\partial y_i &= \partial\left(\frac{1}{(j-i)!} h^i \prod_{\nu=0}^{j-i-1} \gamma^{-\nu}(x)\right) \\
&= \frac{1}{(j-i)!}\gamma(h)^i \prod_{\nu=0}^{j-i-1} \gamma^{-\nu+1}(x) - \frac{1}{(j-i)!} h^i \prod_{\nu=0}^{j-i-1} \gamma^{-\nu}(x) \\
&= \frac{1}{(j-i)!} h^i \left(\prod_{\nu=0}^{j-i-1} \gamma^{-\nu+1}(x) - \prod_{\nu=0}^{j-i-1} \gamma^{-\nu}(x)\right), \quad \text{da } \gamma(h) = h \\
&= \frac{1}{(j-i)!} h^i \left(\gamma(x) - \gamma^{-j+i+1}(x)\right) \prod_{\nu=0}^{j-i-2} \gamma^{-\nu}(x) \\
&= \frac{1}{(j-i)!} h^i \underbrace{\left(1 + \gamma^{-1} + \cdots + \gamma^{-j+i+1}\right) \underbrace{(\gamma - 1)(x)}_{=h,\ \text{da } \gamma - 1 = \partial}}_{=(j-i)\cdot h} \prod_{\nu=0}^{j-i-2} \gamma^{-\nu}(x) \\
&= \frac{1}{(j-(i+1))!} h^{i+1} \prod_{\nu=0}^{j-(i+1)-1} \gamma^{-\nu}(x) \\
&= y_{i+1}
\end{aligned}$$

Somit gilt: $\partial^j y_0 = \partial^0 y_j = y_j = h^j$
$\Rightarrow h^j \in \mathrm{Im}(\partial^j)$

Da $\mathrm{Im}(\partial^j)$ ein $\mathrm{Ker}(\partial)$-Modul ist, gilt für $h \in \mathrm{Ker}(\partial) \cap \mathrm{Im}(\partial)$ auch:
$h^l \in \mathrm{Im}(\partial^j) \quad \forall\ 1 \leq j \leq p-1,\ l \geq j.$ □

Lemma 6.9 *Für* $0 \leq k \leq n-2$ *gilt* $f_k(z_{k+1})^{q-1} \in \mathrm{Im}(\partial^{p-1}) = \mathrm{Im}(Tr)$.

Beweis Dies folgt direkt aus den vorangegangenen zwei Lemmata. □

6.3 Isomorphie als Moduln über der Dicksonalgebra

Satz 6.10

$$d_{n,0},\ldots,d_{n,n-2}\in \mathrm{Im}(\partial^{p-1})=\mathrm{Im}(Tr)$$

und

$$d_{n,n-1}-f_{n-1}(z_n)^{q-1}\in \mathrm{Im}(\partial^{p-1})=\mathrm{Im}(Tr)$$

Beweis

- Zeige durch Induktion nach k ($k\le n$), dass $d_{k,j}\in \mathrm{Ker}(\partial)\ \forall\, j<k$:
  Induktionsanfang: $k=0$:

  $$d_{0,j}=0\in \mathrm{Ker}(\partial)\ \forall\, j<0.$$

  Induktionsschluss:

  $$d_{k,j}=\underbrace{d^{\,q}_{k-1,j-1}}_{\in \mathrm{Ker}(\partial)\text{ nach } \textit{Ind.-Vor.}}+\underbrace{d_{k-1,j}}_{\in \mathrm{Ker}(\partial)\text{ s. unten}}\cdot\underbrace{f_{k-1}(z_k)^{q-1}}_{\in \mathrm{Ker}(\partial)\text{ nach Lemma 6.7}}\in \mathrm{Ker}(\partial)$$

  Für $j<k-1$ ist $d_{k-1,j}\in \mathrm{Ker}(\partial)$ nach *Induktionsvoraussetzung* und für $j=k-1$ ist $d_{k-1,j}=1\in \mathrm{Ker}(\partial)$.

- Zeige durch Induktion nach k, dass $d_{k,j}\in \mathrm{Im}(\partial^{p-1})\ \forall\ 0\le k\le n-1, j<k$:
  Induktionsanfang: $k=0$:

  $$d_{0,j}=0\in \mathrm{Im}(\partial^{p-1})\ \forall\ j<0.$$

  Induktionsschluss:

  $$d_{k,j}=\underbrace{d^{\,q}_{k-1,j-1}}_{\in \mathrm{Im}(\partial^{p-1})\text{ nach } \textit{Ind.-Vor.}}+\underbrace{d_{k-1,j}}_{\in \mathrm{Ker}(\partial)}\cdot\underbrace{f_{k-1}(z_k)^{q-1}}_{\in \mathrm{Im}(\partial^{p-1})\text{ nach Lemma 6.9}}\in \mathrm{Im}(\partial^{p-1})$$

- Somit ist für $0\le j\le n-2$:

  $$d_{n,j}=\underbrace{d^{\,q}_{n-1,j-1}}_{\in \mathrm{Im}(\partial^{p-1})}+\underbrace{d_{n-1,j}}_{\in \mathrm{Im}(\partial^{p-1})}\cdot\underbrace{f_{n-1}(z_n)^{q-1}}_{\in \mathrm{Ker}(\partial)\text{ nach Lemma 6.7}}\in \mathrm{Im}(\partial^{p-1})$$

- Als Letztes folgt:

  $$\begin{aligned} d_{n,n-1} &= d^{\,q}_{n-1,n-2}+d_{n-1,n-1}\cdot f_{n-1}(z_n)^{q-1}\\ &= d^{\,q}_{n-1,n-2}+f_{n-1}(z_n)^{q-1}\\ \Rightarrow d_{n,n-1}-f_{n-1}(z_n)^{q-1} &= d^{\,q}_{n-1,n-2}\in \mathrm{Im}(\partial^{p-1})\end{aligned}$$

$\square$

Lemma 6.11 *Das Polynom $f := f_{n-1}(z_n)^{q-1} \in \mathbb{F}_q[V]^{\mathbb{Z}/p}$ operiert frei auf den Gruppen $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$.*

Beweis Zu zeigen:
a) $h \in \mathrm{Ker}(\partial^{p-1})$ mit $f \cdot h \in \mathrm{Im}(\partial) \Rightarrow h \in \mathrm{Im}(\partial)$.
b) $h \in \mathrm{Ker}(\partial)$ mit $f \cdot h \in \mathrm{Im}(\partial^{p-1}) \Rightarrow h \in \mathrm{Im}(\partial^{p-1})$.

zu a): Sei $f \cdot h \in \mathrm{Im}(\partial) \Rightarrow \exists g$ mit $\partial g = f \cdot h$.
Betrachte alle Polynome als Polynome in z_n mit Koeffizienten in $\mathbb{F}_q[z_1, \ldots, z_{n-1}]$. Da f ein normiertes Polynom ist, ist eine Polynomdivision durch f durchführbar. Also ist $g = f \cdot k + r$ mit $\deg_{z_n}(r) < \deg_{z_n}(f)$. Damit gilt:

$$\begin{aligned} f \cdot h &= \partial g = \partial(f \cdot k + r) \\ &= \gamma(f) \cdot \gamma(k) - f \cdot k + \partial r \\ &= f \cdot \partial k + \partial r, \quad \text{da } f \in \mathrm{Ker}(\partial) \\ \Rightarrow \partial r &= f \cdot (h - \partial k) \end{aligned}$$

Nun ist allerdings $\deg_{z_n}(\partial r) \leq \deg_{z_n}(r) < \deg_{z_n}(f)$, weshalb $\partial r = 0$, d. h. $h = \partial k$.
Teil b) folgt induktiv aus Teil a). □

Satz 6.12 *$H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ sind isomorph als $\mathbb{F}_q[f]$-Moduln.*

Beweis Wie in 4.7 gesehen sind $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ isomorph als $\mathbb{F}_q$-Vektorräume und da γ graderhaltend operiert, sogar isomorph in jedem Polynomgrad.
Ein Vektorraum-Isomorphismus $\varphi : H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V]) \to H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ ist also genau dann ein $\mathbb{F}_q[f]$-Modul-Homomorphismus, wenn $f \cdot \varphi(g) = \varphi(f \cdot g)$ $\forall g \in H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$.
Wähle eine Basis von $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ sukzessiv in den Graden $0, 1, 2, \ldots$ so, dass für jedes Basiselement g im Grad $\deg(g)$ auch $f \cdot g$ Basiselement im Grad $\deg(f) + \deg(g)$ ist. Dies ist machbar, da f frei operiert und daher für eine linear unabhängige Teilmenge $\{g_1, \ldots, g_k\}$ auch $\{f \cdot g_1, \ldots, f \cdot g_k\}$ linear unabhängig ist.
Wähle nun auf die gleiche Weise eine Basis von $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$.
Dann ist der Vektorraum-Isomorphismus, den man durch Zuordnen dieser Basen erhält, ein $\mathbb{F}_q[f]$-Modul-Isomorphismus. □

Satz 6.13 *$H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ sind isomorph als Moduln über der Dicksonalgebra $D(n)$.*

Beweis Nach Satz 6.10 sind $d_{n,0}, \ldots, d_{n,n-2} \in \mathrm{Im}(\partial^{p-1}) = \mathrm{Im}(Tr)$ und operieren daher trivial auf $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$. Außerdem ist $d_{n,n-1} - f_{n-1}(z_n)^{q-1} \in \mathrm{Im}(Tr)$, weshalb $d_{n,n-1}$ wie $f = f_{n-1}(z_n)^{q-1}$ operiert. Somit operiert die Dicksonalgebra $D(n)$ auf $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ wie die Algebra $\mathbb{F}_q[f]$. Die Kohomologiegruppen sind also isomorph als Moduln über der Dicksonalgebra. □

7 Isomorphie für beliebige Darstellungen von $\mathbb{Z}/p$

Sei $\varrho : \mathbb{Z}/p \to GL(V)$ eine beliebige Darstellung von $\mathbb{Z}/p$. Es sei V wie bisher ein $\mathbb{F}_q$-Vektorraum der Dimension $n < \infty$. Für eine unzerlegbare Darstellung ρ wurde die Isomorphie von $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ als Moduln über der Dicksonalgebra $D(n) = \mathbb{F}_q[V]^{GL(V)}$ schon bewiesen. Der Beweis beinhaltet, dass die Dicksonpolynome $d_{n,0}, \ldots, d_{n,n-2}$ auf $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ trivial operieren und dass $d_{n,n-1}$ wie das Polynom $f := f_{n-1}(z_n)^{q-1}$ operiert.

Sei nun $V = V_1 \oplus V_2 \oplus \cdots \oplus V_s$ die bis auf Permutation eindeutige Zerlegung von V in unzerlegbare Unterräume bezüglich ϱ. Dann lässt sich die Algebra $\mathbb{F}_q[V]$ als $\mathbb{Z}/p$-Algebra zerlegen in $\mathbb{F}_q[V] = \mathbb{F}_q[V_1] \otimes \mathbb{F}_q[V_2] \otimes \cdots \otimes \mathbb{F}_q[V_s]$. Die Darstellung ϱ lässt sich faktorisieren in

$$\mathbb{Z}/p \to \underbrace{\mathbb{Z}/p \times \cdots \times \mathbb{Z}/p}_{s-\text{mal}} \to GL(V_1) \times \cdots \times GL(V_s) \to GL(V).$$

Es ist also $D(n) \subset \mathbb{F}_q[V]^{GL(V_1)\times\cdots\times GL(V_s)} = D(n_1) \otimes \cdots \otimes D(n_s)$ und daher impliziert eine Isomorphie als Moduln über $D(n_1) \otimes \cdots \otimes D(n_s)$ eine Isomorphie als $D(n)$-Moduln (n_i bezeichne die Dimension des Vektorraumes V_i). Wir benutzen wieder die gleichen Bezeichnungen wie im vorigen Kapitel, wobei Zugehörigkeiten zu den Untervektorräumen V_1 bis V_s durch obere Indizes angezeigt werden. So sei zum Beispiel die Jordanbasis des Dualraums V_1^* bezüglich γ mit $\{z_1^{(1)}, \ldots, z_{n_1}^{(1)}\}$ bezeichnet. Für $i = 1, \ldots, s$ bezeichnet des weiteren $f^{(i)}$ das Polynom $f_{n_i-1}^{(i)}(z_{n_i}^{(i)})^{q-1} \in \mathbb{F}_q[V_i]$. Nach den Berechnungen im vorigen Kapitel sind die Dicksonpolynome $d_{n_i,0}^{(i)}, \ldots, d_{n_i,n_i-2}^{(i)}$ $(i = 1, \ldots, s)$ aus $\mathrm{Im}(\partial^{p-1})$ und operieren daher trivial auf $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$. Weiter operieren $d_{n_i,n_i-1}^{(i)}$ wie $f^{(i)}$, $i = 1, \ldots, s$. Somit operiert $\mathbb{F}_q[V]^{GL(V_1)\times\cdots\times GL(V_s)} = D(n_1) \otimes \cdots \otimes D(n_s)$ auf $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ wie die Polynomalgebra $\mathbb{F}_q[f^{(1)}, \ldots, f^{(s)}]$.

Definition 7.1 (Kanonische Zerlegung) *Für ein Polynom $g \in \mathbb{F}_q[V]$ konstruieren wir die kanonische Zerlegung folgendermaßen:*
Wir betrachten $f^{(1)}$ als Polynom in $z_{n_1}^{(1)}$ mit Koeffizienten in $\mathbb{F}_q[z_1^{(1)}, \ldots, z_{n_1-1}^{(1)}]$. Dann ist $f^{(1)}$ ein normiertes Polynom, weshalb eine Polynomdivision durchführbar ist. Die Polynomdivision von g durch $f^{(1)}$ liefert:

$$g = f^{(1)} g_1 + r_1, \qquad \deg_{z_{n_1}^{(1)}}(r_1) < \deg_{z_{n_1}^{(1)}}(f^{(1)})$$

Weiter ist $f^{(2)}$ als Polynom in $z_{n_2}^{(2)}$ mit Koeffizienten in $\mathbb{F}_q[z_1^{(2)}, \ldots, z_{n_2-1}^{(2)}]$ ein normiertes Polynom. Die Polynomdivision von r_1 durch $f^{(2)}$ liefert:

$$r_1 = f^{(2)} g_2 + r_2$$

Entsprechend führen wir nacheinander für jedes $i \leq s-1$ eine Polynomdivision des letzten Restes r_i durch das Polynom $f^{(i+1)}$ bezüglich $z_{n_{i+1}}^{(i+1)}$ durch. Rückeinsetzen liefert nun die **kanonische Zerlegung***:*

$$g = f^{(1)}g_1 + f^{(2)}g_2 + \cdots + f^{(s)}g_s + r \qquad (r := r_s)$$

Für die Polynome $g_2, \ldots, g_s$ und r gelten nach Konstruktion:

$$\deg_{z_{n_i}^{(i)}}(g_j) < \deg_{z_{n_i}^{(i)}}(f^{(i)}) \qquad \forall\, 1 \leq i < j \leq s \qquad (*)$$

$$\deg_{z_{n_i}^{(i)}}(r) < \deg_{z_{n_i}^{(i)}}(f^{(i)}) \qquad \forall\, 1 \leq i \leq s \qquad (**)$$

Lemma 7.2 *Die kanonische Zerlegung ist durch die Bedingungen $(*)$ und $(**)$ eindeutig bestimmt.*

Beweis Sei $g = f^{(1)}g_1 + \cdots + f^{(s)}g_s + r$ die kanonische Zerlegung und $g = f^{(1)}h_1 + \cdots + f^{(s)}h_s + t$ eine weitere Zerlegung, die die Bedingungen $(*)$ und $(**)$ erfüllt. Dann gilt $f^{(1)}g_1 + \cdots + f^{(s)}g_s + r = f^{(1)}h_1 + \cdots + f^{(s)}h_s + t$ und daher

$$f^{(1)}(g_1 - h_1) = f^{(2)}(h_2 - g_2) + \cdots + f^{(s)}(h_s - g_s) + t - r\,.$$

Auf der rechten Seite steht nun ein Polynom, dessen Grad bezüglich $z_{n_1}^{(1)}$ wegen der Bedingungen $(*)$ und $(**)$ kleiner ist als $\deg_{z_{n_1}^{(1)}}(f^{(1)})$. Wenn nun $g_1 - h_1 \neq 0$ wäre, stünde auf der linken Seite ein Polynom, dessen Grad bezüglich $z_{n_1}^{(1)}$ größer als oder gleich $\deg_{z_{n_1}^{(1)}}(f^{(1)})$ wäre. Also gilt: $g_1 - h_1 = 0$, d. h. $g_1 = h_1$.
Nun gilt

$$f^{(2)}(g_2 - h_2) = f^{(3)}(h_3 - g_3) + \cdots + f^{(s)}(h_s - g_s) + t - r$$

und auf die gleiche Weise wie eben erhält man $g_2 = h_2$.
Schritt für Schritt erhält man also: $g_1 = h_1, g_2 = h_2, g_3 = h_3, \ldots, g_s = h_s$ und schließlich $r = t$. $\square$

Bemerkung Die kanonische Zerlegung ist additiv, d. h. wenn $g = f^{(1)}g_1 + \cdots + f^{(s)}g_s + r$ und $h = f^{(1)}h_1 + \cdots + f^{(s)}h_s + t$ die kanonischen Zerlegungen von g und h sind, ist die kanonische Zerlegung von $g+h$ gerade $g + h = f^{(1)}(g_1 + h_1) + \cdots + f^{(s)}(g_s + h_s) + (r + t)$.

Lemma 7.3 *Sei $g \in \mathbb{F}_q[V]$ und $g = f^{(1)}g_1 + \cdots + f^{(s)}g_s + r$ die kanonische Zerlegung. Dann gelten:*

$$\begin{array}{lll}
\textbf{(i)} & g \in \operatorname{Ker}(\partial) & \Leftrightarrow \quad g_1, \ldots, g_s, r \in \operatorname{Ker}(\partial) \\
\textbf{(ii)} & g \in \operatorname{Im}(\partial) & \Leftrightarrow \quad g_1, \ldots, g_s, r \in \operatorname{Im}(\partial) \\
\textbf{(iii)} & g \in \operatorname{Im}(\partial^{p-1}) & \Leftrightarrow \quad g_1, \ldots, g_s, r \in \operatorname{Im}(\partial^{p-1}) \\
\textbf{(iv)} & g \in \operatorname{Ker}(\partial^{p-1}) & \Leftrightarrow \quad g_1, \ldots, g_s, r \in \operatorname{Ker}(\partial^{p-1})
\end{array}$$

Beweis Es sind $f^{(1)}, \dots, f^{(s)} \in \operatorname{Ker}(\partial)$. Da $\operatorname{Ker}(\partial), \operatorname{Im}(\partial), \operatorname{Im}(\partial^{p-1})$ und $\operatorname{Ker}(\partial^{p-1})$ Moduln über $\operatorname{Ker}(\partial)$ sind, sind die Rückrichtungen jeweils offensichtlich.

(i) Sei $g \in \operatorname{Ker}(\partial)$, d. h. $0 = \partial g = \partial(f^{(1)}g_1 + \dots + f^{(s)}g_s + r) = f^{(1)}\partial g_1 + \dots + f^{(s)}\partial g_s + \partial r$. Nun gilt für alle $1 \leq i < j \leq s$:

$$\deg_{z^{(i)}_{n_i}}(\partial g_j) \leq \deg_{z^{(i)}_{n_i}}(g_j) < \deg_{z^{(i)}_{n_i}}(f^{(i)})$$

und für alle $1 \leq i \leq s$:

$$\deg_{z^{(i)}_{n_i}}(\partial r) \leq \deg_{z^{(i)}_{n_i}}(r) < \deg_{z^{(i)}_{n_i}}(f^{(i)})$$

und daher folgt nach Lemma 7.2: $\partial g_1 = \dots = \partial g_s = \partial r = 0$, d. h. $g_1, \dots, g_s, r \in \operatorname{Ker}(\partial)$.

(ii) Sei $g = \partial h$ und $h = f^{(1)}h_1 + \dots + f^{(s)}h_s + t$ die kanonische Zerlegung von h. Es ist: $\partial h = f^{(1)}\partial h_1 + \dots + f^{(s)}\partial h_s + \partial t$, d. h. $f^{(1)}g_1 + \dots + f^{(s)}g_s + r = g = \partial h = f^{(1)}\partial h_1 + \dots + f^{(s)}\partial h_s + \partial t$. Wiederum ist für alle $1 \leq i < j \leq s$:

$$\deg_{z^{(i)}_{n_i}}(\partial h_j) \leq \deg_{z^{(i)}_{n_i}}(h_j) < \deg_{z^{(i)}_{n_i}}(f^{(i)})$$

und für alle $1 \leq i \leq s$:

$$\deg_{z^{(i)}_{n_i}}(\partial t) \leq \deg_{z^{(i)}_{n_i}}(t) < \deg_{z^{(i)}_{n_i}}(f^{(i)}).$$

Wegen Lemma 7.2 ist also: $g_1 = \partial h_1, \dots, g_s = \partial h_s, r = \partial t$, d. h. $g_1, \dots, g_s, r \in \operatorname{Im}(\partial)$.

(iii) Analog zu **(ii)**.

(iv) Analog zu **(i)**.

□

Bezeichnung $A := \mathbb{F}_q[f^{(1)}, \dots, f^{(s)}] \subset \mathbb{F}_q[V]^{\mathbb{Z}/p}$.
Bemerkung Ist $k \in A$ (homogen) und $k = f^{(1)}k_1 + \dots + f^{(s)}k_s + k_{s+1}$ die kanonische Zerlegung von k, dann ist: $k_j \in \mathbb{F}_q[f^{(j)}, \dots, f^{(s)}] \quad \forall\, 1 \leq j \leq s$. Weiter ist $k_{s+1} \in \mathbb{F}_q$, d. h. falls $k \notin \mathbb{F}_q$ ist, ist $k_{s+1} = 0$.

Satz 7.4 *Sei l eine natürliche Zahl und seien $g_1, \dots g_l \in \mathbb{F}_q[V]$ Polynome so, dass die Restklassen $\overline{g_1}, \dots, \overline{g_l} \in H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ einen freien A-Untermodul von $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ erzeugen. Zusätzlich seien $g_1, \dots, g_l$ so gewählt, dass alle $v \in \mathbb{F}_q[V]$, deren Polynomgrad kleiner* $\max\{\deg(g_1), \dots, \deg(g_l)\}$ *ist, in $Ag_1 + \dots + Ag_l + \operatorname{Im}(\partial)$ enthalten sind. D. h. $\overline{g_1}, \dots, \overline{g_l}$ erzeugen schon den Anteil* *von $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ in den Graden kleiner $\max\{\deg(g_1), \ldots, \deg(g_l)\}$. Sei nun $g_{l+1} \in \mathbb{F}_q[V]$, $g_{l+1} \notin Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$ von minimalem Polynomgrad. Dann gilt:*

$$k \cdot g_{l+1} \notin Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial) \quad \forall\, k \in A \setminus \{0\}.$$

Oder anders ausgedrückt: Dann ist $A\overline{g_1} + \cdots + A\overline{g_{l+1}}$ freier A-Untermodul von $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$.

Zum Beweis benötigen wir zuerst ein kleines Lemma:

Lemma 7.5 *Seien $g_1, \ldots, g_l$ wie im voranstehenden Satz gewählt. Ist $v \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial) \subset \mathbb{F}_q[V]$ und $v = f^{(1)}v_1 + \cdots + f^{(s)}v_s + v_{s+1}$ die kanonische Zerlegung von v, so gilt: $v_1, \ldots, v_s, v_{s+1} \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$*

Beweis Da die kanonische Zerlegung additiv ist, genügt es, die Behauptung zu zeigen für:

(i) $k \cdot g_i \; \forall\, k \in A, 1 \leq i \leq l$
(ii) $v \in \mathrm{Im}(\partial)$

(ii) wurde schon in Lemma 7.3 gezeigt.
Zu **(i)**: Sei $g_i = f^{(1)}g_{i,1} + \cdots + f^{(s)}g_{i,s} + r_i$ die kanonische Zerlegung. Wegen $\deg(g_{i,j}) < \deg(g_i)$ gilt nach Voraussetzung

$$g_{i,j} \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial) \text{ für alle } 1 \leq j \leq s$$

und damit ist auch (∗)

$$r_i = g_i - \left(f^{(1)}g_{i,1} + \cdots + f^{(s)}g_{i,s}\right) \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$$

Sei nun $k = f^{(1)}k_1 + \cdots + f^{(s)}k_s + k_{s+1}$ die kanonische Zerlegung von k, dann ist:

$$\begin{aligned} k \cdot g_i &= f^{(1)}k_1 g_i + f^{(2)}k_2 g_i + \cdots + f^{(s)}k_s g_i + k_{s+1} g_i \\ &= f^{(1)}k_1 g_i + f^{(1)}\left(f^{(2)}k_2 g_{i,1}\right) + f^{(2)}k_2\left(f^{(2)}g_{i,2} + \cdots + f^{(s)}g_{i,s} + r_i\right) \\ &\quad + f^{(1)}\left(f^{(3)}k_3 g_{i,1}\right) + f^{(2)}\left(f^{(3)}k_3 g_{i,2}\right) + f^{(3)}k_3\left(f^{(3)}g_{i,3} + \cdots + r_i\right) \\ &\quad + \cdots + f^{(1)}k_{s+1}g_{i,1} + f^{(2)}k_{s+1}g_{i,2} + \cdots + f^{(s)}k_{s+1}g_{i,s} + k_{s+1}r_i \end{aligned}$$

Durch Zusammenfassen der entsprechenden Terme erhält man jetzt die kanonische Zerlegung von kg_i. Wegen (∗) sind nun alle Komponenten dieser Zerlegung aus $Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$. □

Beweis des Satzes
Angenommen, es gebe ein $k \in A \setminus \{0\}$ mit $k \cdot g_{l+1} \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$. Betrachten wir ein solches k von minimalem Polynomgrad.
Die kanonischen Zerlegungen von g_{l+1} und k seien $g_{l+1} = f^{(1)}g_{l+1,1} + \cdots + f^{(s)}g_{l+1,s} + r_{l+1}$ und $k = f^{(1)}k_1 + \cdots + f^{(s)}k_s + k_{s+1}$.
Die gleiche Rechnung wie im Lemma liefert:

$$\begin{aligned} k \cdot g_{l+1} = f^{(1)}k_1 g_{l+1} &+ f^{(1)}\left(f^{(2)}k_2 g_{l+1,1}\right) + f^{(2)}k_2\left(f^{(2)}g_{l+1,2} + \cdots + f^{(s)}g_{l+1,s} + r_{l+1}\right) \\ &+ f^{(1)}\left(f^{(3)}k_3 g_{l+1,1}\right) + f^{(2)}\left(f^{(3)}k_3 g_{l+1,2}\right) + f^{(3)}k_3\left(f^{(3)}g_{l+1,3} + \cdots + r_{l+1}\right) \\ &+ \cdots + f^{(1)}k_{s+1}g_{l+1,1} + f^{(2)}k_{s+1}g_{l+1,2} + \cdots + f^{(s)}k_{s+1}g_{l+1,s} + k_{s+1}r_{l+1} \end{aligned}$$

Nach dem Lemma sind alle Komponenten aus $Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$ und wegen $\deg(g_{l+1,j}) < \deg(g_{l+1})$ gilt nach Voraussetzung an g_{l+1}, dass $g_{l+1,j} \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$ für alle $1 \le j \le s$. Die einzelnen Komponenten liefern somit $k_1 r_{l+1}, \ldots, k_s r_{l+1}, k_{s+1}r_{l+1} \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$.
Wegen $k \neq 0$ ist $k_j \neq 0$ für ein j.

Fall 1: $k_{s+1} \neq 0$. Da $k_{s+1} \in \mathbb{F}_q$, folgt somit $r_{l+1} \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$ und daher $g_{l+1} \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$. Widerspruch!

Fall 2: $k_j \neq 0$ für ein j mit $1 \le j \le s$. Dann ist $k_j g_{l+1} = f^{(1)}k_j g_{l+1,1} + \cdots + f^{(s)}k_j g_{l+1,s} + k_j r_{l+1} \in Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)$. Wegen $\deg(k_j) < \deg(k)$ steht dies aber im Widerspruch zur Minimalität von k.

Somit gilt

$$k \cdot g_{l+1} \notin Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial)\ \forall\, k \in A \setminus \{0\}.$$

□

Satz 7.6 *Sei l eine natürliche Zahl und seien $g_1, \ldots, g_l \in \mathbb{F}_q[V]$ Polynome so, dass die Restklassen $\overline{g_1}, \ldots, \overline{g_l} \in H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ einen freien A-Untermodul von $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ erzeugen. Zusätzlich seien $g_1, \ldots, g_l$ so gewählt, dass alle $v \in \mathbb{F}_q[V]$, deren Polynomgrad kleiner $\max\{\deg(g_1), \ldots, \deg(g_l)\}$ ist, in $Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial^{p-1})$ enthalten sind. D. h. $\overline{g_1}, \ldots, \overline{g_l}$ erzeugen schon den Anteil von $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ in den Graden kleiner $\max\{\deg(g_1), \ldots, \deg(g_l)\}$. Sei nun $g_{l+1} \in \mathbb{F}_q[V]$, $g_{l+1} \notin Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial^{p-1})$ von minimalem Polynomgrad. Dann gilt:*

$$k \cdot g_{l+1} \notin Ag_1 + \cdots + Ag_l + \mathrm{Im}(\partial^{p-1}) \quad \forall\, k \in A \setminus \{0\}.$$

Oder anders ausgedrückt: Dann ist $A\overline{g_1} + \cdots + A\overline{g_{l+1}}$ freier A-Untermodul von $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$.

Beweis Analog zum Beweis des vorigen Satzes. □

Satz 7.7 *$H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ sind isomorph als Moduln über der Algebra $A = \mathbb{F}_q[f^{(1)}, \ldots, f^{(s)}]$.*

Beweis Konstruiere eine Folge $(g_m)_{m\in\mathbb{N}}$ von Elementen in $\mathrm{Ker}(\partial)$ so, dass $g_l \notin Ag_1 + \cdots + Ag_{l-1} + \mathrm{Im}(\partial^{p-1})$ von minimalem Polynomgrad für alle $l \in \mathbb{N}$ ist. Somit bilden die Restklassen $(\overline{g_m})_{m\in\mathbb{N}}$ ein Erzeugendensystem für $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ als A-Modul. Nach Satz 7.6 sind aber $\overline{g_1}, \ldots, \overline{g_l}$ für jedes l linear unabhängig, d. h. $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ ist ein freier A-Modul mit Basis $(\overline{g_m})_{m\in\mathbb{N}}$.

Konstruiere weiter eine Folge $(h_m)_{m\in\mathbb{N}}$ von Elementen in $\mathrm{Ker}(\partial^{p-1})$ so, dass $g_l \notin Ah_1 + \cdots + Ah_{l-1} + \mathrm{Im}(\partial)$ von minimalem Polynomgrad für alle $l \in \mathbb{N}$ ist. Somit bilden die Restklassen $(\overline{h_m})_{m\in\mathbb{N}}$ ein Erzeugendensystem für $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ als A-Modul. Nach Satz 7.4 sind aber $\overline{h_1}, \ldots, \overline{h_l}$ für jedes l linear unabhängig, d. h. $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ ist ein freier A-Modul mit Basis $(\overline{h_m})_{m\in\mathbb{N}}$.

Wie in Satz 4.7 gesehen, haben $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ in jedem Grad dieselbe Vektorraum-Dimension. Für die Basen $(\overline{g_m})_{m\in\mathbb{N}}$ und $(\overline{h_m})_{m\in\mathbb{N}}$ gilt also $\deg(g_m) = \deg(h_m)\ \forall\, m \in \mathbb{N}$.
Eine Zuordnung der Basen liefert also einen Isomorphismus von $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ nach $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ als graduierte A-Moduln. □

Alles in allem haben wir somit den folgenden Satz bewiesen.

Satz 7.8 *$H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ sind isomorph als Moduln über der Dicksonalgebra $D(n)$.*

8 Schlussbetrachtungen

Die vorangegangenen Kapitel haben gezeigt, dass $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ stets als $D(n)$-Moduln isomorph sind. Wir werden jetzt den Beweis der Isomorphie genauer analysieren, um noch größere Ringe zu finden, über denen $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ isomorph sind.
Betrachten wir zunächst wieder den Fall einer unzerlegbaren Darstellung $\rho : \mathbb{Z}/p \to GL(V)$. Die Isomorphie als $D(n)$-Moduln wurde hergeleitet über die Polynome $f_k(z_{k+1})$, $k = 0, \ldots, n-1$. Wie unter anderem in [Smith] (Kap. 8.3) nachzulesen ist, sind diese Polynome gerade die Erzeuger des Invariantenrings $\mathbb{F}_q[V]^{Syl_p}$, wobei Syl_p die p-Sylowgruppe von $GL(V)$ bezeichne, die aus den unteren Dreiecksmatrizen mit Einsen auf der Diagonalen besteht. Die Polynome $f_k(z_{k+1})$ sind sogar algebraisch unabhängig, d. h. dass der Invariantenring $\mathbb{F}_q[V]^{Syl_p} = \mathbb{F}_q[f_0(z_1), \ldots, f_{n-1}(z_n)]$ eine Polynomalgebra ist.

Versuchen wir also, die Frage zu klären, für welche Potenzen r die Kohomologiegruppen isomorph als Moduln über der Algebra $\mathbb{F}_q[f_0(z_1)^r, \ldots, f_{n-1}(z_n)^r]$ sind.

Für $r = 1$ können wir die Frage im Allgemeinen direkt verneinen. Es ist nämlich $f_0(z_1) = z_1$ und in Unterkapitel 5.2 haben wir gesehen, dass z_1 jedes Element in $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ annulliert, aber zum Beispiel nicht die von 1 vertretene Restklasse in $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$. Dasselbe gilt für jede Potenz z_1^r mit $r \leq p-2$. Für $r \geq p-1$ dagegen erhalten wir eine positive Antwort: Nach Lemma 6.7 und Lemma 6.9 ist nämlich $f_k(z_{k+1})^r \in \mathrm{Im}(Tr)$ für $0 \leq k \leq n-2$, weshalb sie auf $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ trivial operieren. Die Algebra $\mathbb{F}_q[f_0(z_1)^r, \ldots, f_{n-1}(z_n)^r]$ operiert also auf $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ wie $\mathbb{F}_q[f_{n-1}(z_n)^r]$. Da $f_{n-1}(z_n)^r$, als Polynom in z_n mit Koeffizienten in $\mathbb{F}_q[z_1, \ldots, z_{n-1}]$ betrachtet, normiert ist, erhalten wir auf die gleiche Weise wie in Lemma 6.11, dass $f_{n-1}(z_n)^r$ sowohl auf $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ als auch auf $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ frei operiert. Also sind $H^{od}(\mathbb{Z}/p, \mathbb{F}_q[V])$ und $H^{ev}(\mathbb{Z}/p, \mathbb{F}_q[V])$ isomorph als Moduln über der Algebra $\mathbb{F}_q[f_0(z_1)^r, \ldots, f_{n-1}(z_n)^r]$ für $r \geq p-1$.

Literatur

[Evens] Leonard Evens, *The Cohomology of Groups*; Oxford Mathematical Monographs (1991)

[Lane] Saunders Mac Lane, *Homology*; Mathematische Wissenschaften, Band 114, Springer (1963)

[Lang] Serge Lang, *Algebra*; Addison-Wesley Publishing Company Inc.; 3. Edition (1993), Reprint with corrections, January 1997

[NeSmi] Mara D. Neusel, Larry Smith, *Invariant Theory of Finite Groups*; Am. Math. Soc., Math. Surveys and Monographs, Vol. 94 (2002)

[Smith] Larry Smith, *Polynomial Invariants of Finite Groups*; Research Notes in Mathematics, Vol. 6 (1995)

[Weiss] Edwin Weiss, *Cohomology of Groups*; Academic Press New York and London (1969)

[Wilk] Clarence Wilkerson, *A Primer on the Dickson Invariants*; Contemporary Mathematics 19 (1983), corrected version