Tzu-Chun Lin

Über Poincarédualitätsalgebra in der Invariantentheorie

Cuvillier Verlag Göttingen

Über Poincarédualitätsalgebra in der Invariantentheorie

Dissertation
zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultäten
der Georg-August-Universität zu Göttingen

vorgelegt von
Tzu-Chun Lin
aus Tainan/Taiwan

Göttingen 2003

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.
1. Aufl. - Göttingen : Cuvillier, 2003
Zugl.: Göttingen, Univ., Diss., 2003
ISBN 3-89873-759-4

D7

Referent:	Prof. Dr. L. Smith
Korreferentin:	Prof. Dr. I. Kersten
Tag der mündlichen Prüfung:	29. Jan. 03

© CUVILLIER VERLAG, Göttingen 2003
Nonnenstieg 8, 37075 Göttingen
Telefon: 0551-54724-0
Telefax: 0551-54724-21
www.cuvillier.de

Alle Rechte vorbehalten. Ohne ausdrückliche Genehmigung des Verlages ist es nicht gestattet, das Buch oder Teile daraus auf fotomechanischem Weg (Fotokopie, Mikrokopie) zu vervielfältigen.
1. Auflage, 2003
Gedruckt auf säurefreiem Papier

ISBN 3-89873-759-4

Inhaltsverzeichnis

Vorwort **2**

1 Grundlagen **9**

2 Irreduzible Ideale **15**

3 Zerlegung in direkter Summe **22**

4 Hochhebung einer Gruppendarstellung **27**

5 Die reguläre Darstellung **39**

Literaturverzeichnis **43**

Danksagung **45**

Vorwort

Ausgangspunkt ist eine treue Darstellung $G \hookrightarrow GL(V)$ einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Der Invariantenring $\mathbb{F}[V]^G$ ist eine endlich erzeugte Unteralgebra der Algebra $\mathbb{F}[V]$ von Polynomfunktionen auf dem $\mathbb{F}$-Vektorraum V. Einer der Schwerpunkte in der Invariantentheorie besteht darin, sämtliche Erzeuger eines Invariantenrings zu finden. Ein Standardbeispiel dafür ist eine Darstellung $\Sigma_n \hookrightarrow GL(V)$ einer symmetrischen Gruppe Σ_n mit der Ordung $n!$ auf $V \cong \mathbb{F}^n$. Der Invariantenring $\mathbb{F}[V]^{\Sigma_n}$ ist der Polynomring $\mathbb{F}[e_1, \cdots, e_n]$ mit den elementarsymmetrischen Polynomen $e_1, \cdots, e_n$ als Variablen. Aber das ist leider nur einer der wenigen gefundenen speziellen Fällen. Meistens ist noch nicht bekannt, wieviele Erzeuger $\mathbb{F}[V]^G$ hat.
Für den Fall, daß $\operatorname{Char} \mathbb{F} = 0$, haben R. Steinberg ([28]) und R. Kane ([14]) ein interessantes Kriterium für polynomiale Invariantenringe herausgefunden. Im Folgenden wird ihre Beweismethode grob erläutert :

Es sei V ein endlichdimensionaler Vektorraum über einem Körper $\mathbb{F}$ der Charakteristik 0. Angenommen $\alpha_1, \cdots, \alpha_n$ sei eine $\mathbb{F}$-Basis von V und $x_1, \cdots, x_n$ eine $\mathbb{F}$-Basis von $V^* = Hom_{\mathbb{F}}(V, \mathbb{F})$, die dual zur Basis $\alpha_1, \cdots, \alpha_n$ ist. Die graduierten polynomialen Algebren $\mathbb{F}[\mathfrak{A}] := \mathbb{F}[\alpha_1, \cdots, \alpha_n]$ und $\mathbb{F}[\mathfrak{X}] := \mathbb{F}[x_1, \cdots, x_n]$ sind zueinander duale, primitiv endlich erzeugte Hopf-Algebren [1] ($\deg x_i = \deg \alpha_i = 1,\ i = 1, \cdots, n$). Die Arbeit von R. Steinberg basiert auf der Differentialoperation auf einer Polynomalgebra. Wir betrachten die Polynomalgebra $\mathbb{F}[\mathfrak{A}]$ als die graduierte Hopf-Algebra von Differentialoperatoren auf $\mathbb{F}[\mathfrak{X}]$. Für jedes $\alpha \in V$ ist ein Differentialoperator D_α auf V^* definiert durch

$$\begin{aligned} D_\alpha(x) &= \langle \alpha \ , \ x \rangle \\ D_\alpha(xy) &= D_\alpha(x)y + xD_\alpha(y) \ \text{ für } \alpha \in V,\ x, y \in V^*, \end{aligned}$$

wobei $\langle \ , \ \rangle : V \otimes V^* \longrightarrow \mathbb{F}$ das innere Produkt ist. Der Operator $D : \mathbb{F}[\mathfrak{A}] \times \mathbb{F}[\mathfrak{X}] \longrightarrow \mathbb{F}[\mathfrak{X}]$ ist dann bestimmt durch die Regel $D_{st} = D_s \circ D_t$ für $s, t \in \mathbb{F}[\mathfrak{A}]$. Das innere Produkt wird durch

$$\langle \ s \ , \ f \ \rangle = (D_s(f))(0) \ , \ s \in \mathbb{F}[\mathfrak{A}],\ f \in \mathbb{F}[\mathfrak{X}] \tag{1}$$

auf die Polynomalgebren erweitert. Die Hopf-Algebra $\mathbb{F}[\mathfrak{A}]$ bzw. $\mathbb{F}[\mathfrak{X}]$ beinhaltet die koalgebraische Struktur Δ bzw. Δ^*.

[1] siehe z.B. M.E. Sweedler, Hopf Algebras, (1969)

Durch die Definiton der dualen algebraischen Struktur erhalten wir $\langle s \ , \ f \cdot h \rangle = \langle \Delta(s) \ , \ f \otimes h \rangle$, $\langle s \cdot t \ , \ f \rangle = \langle s \otimes t \ , \ \Delta^*(f) \rangle$, für $s, t \in \mathbb{F}[\mathfrak{A}]$, $f, h \in \mathbb{F}[\mathfrak{X}]$. Die Operation von G auf V induziert eine Operation auf V^* durch

$$\langle \ g \cdot x \ , \ \alpha \ \rangle = \langle \ x \ , \ g^{-1} \cdot \alpha \ \rangle,$$

für alle $x \in V^*, \alpha \in V, g \in G$. Die Operation von G auf V bzw. V^* erweitert sich auf $\mathbb{F}[\mathfrak{A}]$ bzw. $\mathbb{F}[\mathfrak{X}]$; wir erhalten dann $g(D_s f) = D_{gs}(gf)$, $s \in \mathbb{F}[\mathfrak{A}]$, $f \in \mathbb{F}[\mathfrak{X}]$, $g \in G$. Ein Element $f \in \mathbb{F}[\mathfrak{X}]$ heißt G-**harmonisch**, wenn $D_s(f) = 0$ für alle $s \in \mathbb{F}[\mathfrak{A}]^G$ ist.

Sei $H := \{f \in \mathbb{F}[\mathfrak{X}] \mid D_s(f) = 0, \ \forall \ s \in \mathbb{F}[\mathfrak{A}]^G\}$ die Menge von harmonischen Elementen. Es ist leicht nachzuweisen, daß es eine bijektive Korrespondenz zwischen dem Untermodul H von $\mathbb{F}[\mathfrak{X}]$ und dem Quotienten $\mathbb{F}[\mathfrak{A}]/(\overline{\mathbb{F}[\mathfrak{A}]^G})$ gibt. [2] Wir setzen $\mathbb{F}[\mathfrak{A}]_G := \mathbb{F}[\mathfrak{A}]/(\overline{\mathbb{F}[\mathfrak{A}]^G})$.

Satz 0.1 *(R. Steinberg, R. Kane) Sei $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$ der Charakteristik 0 und $x_1, \cdots, x_n$ eine $\mathbb{F}$-Basis von V^*.*
Dann sind die folgenden Aussagen äquivalent :

1. *Der Invariantenring $\mathbb{F}[\mathfrak{X}]^G$ ist eine Polynomalgebra.*
2. *Der Untermodul H ist ein zyklischer Modul.*
3. *$\mathbb{F}[\mathfrak{X}]_G$ ist eine Poincarédualitätsalgebra.* [3]

R. Steinberg verwendete den folgenden Satz, um den Erzeuger für H durch Pseudospiegelungen in G zu konstruieren.

Satz 0.2 *(G.C. Shephard-J.A. Todd, C. Chevalley [6][22][25]) Seien $\varrho : G \hookrightarrow GL(V)$ eine Darstellung einer endlichen Gruppe G und V ein n-dimensionaler Vektorraum über einem Körper $\mathbb{F}$. Für $|G| \in \mathbb{F}^\times$ sind die folgenden Aussagen äquivalent :*

1. *G ist eine Pseudospiegelungsgruppe.*
2. *$\mathbb{F}[\mathfrak{X}]^G$ ist eine Polynomalgebra.*
3. *$\mathbb{F}[\mathfrak{X}]^G$ wird durch n algebraisch unabhängige Polynome erzeugt.*
4. *$\mathbb{F}[\mathfrak{X}]$ ist ein freie $\mathbb{F}[\mathfrak{X}]^G$-Modul.*

[2] siehe Definition im Abschnitt 1
[3] siehe Definition im Abschnitt 2

Eine **Pseudospiegelung** ist ein Automorphismus $\sigma : V \longrightarrow V$ mit den Eigenschaften :

1. $\sigma \neq id$;
2. σ hat endliche Ordnung;
3. der Unterraum $V^\sigma := \{v \in V \mid \sigma v = v\}$ hat die Kodimension 1. Der Raum V^σ heißt **Hyperebene** von σ.

Eine **Pseudospiegelungsgruppe** ist eine Gruppe, die durch ihre Pseudospiegelungen erzeugt wird. Eine Pseudospiegelung σ ist genau dann diagonalisierbar, wenn $\operatorname{Char}\mathbb{F} = 0$ oder $|G| \in \mathbb{F}^\times$ ist. Für jede Pseudospiegelung $\sigma \in Aut(V)$ gibt es einen Vektor $0 \neq a \in \operatorname{Im}(1-\sigma)$, so daß $\sigma(v) = v + l_\sigma(v) \cdot a$, für alle $v \in V$ und $l_\sigma : V \to \mathbb{F}$ eine lineare Funktion mit $\ker l_\sigma = V^\sigma$ ist.
R. Steinberg konstruierte nun ein homogenes Element Ω in $\mathbb{F}[\mathfrak{X}]$ aus allen linearen Funktionen l_σ, $\sigma \in s(G)$, nämlich

$$\Omega := \prod_{\sigma \in s(G)} l_\sigma,$$

wobei $s(G)$ die Menge aller Pseudospiegelungen in G ist. In der Tat können aber verschiedene Pseudospiegelungen dieselbe Hyperebene besitzen. Für eine feste Hyperebene $V^{\bar\sigma}$ ist die Menge $C_H := \{ \sigma \in s(G) \mid V^\sigma = V^{\bar\sigma} \} \cup \{id\} \cong \langle \sigma_{V^{\bar\sigma}} \rangle$ eine zyklische Gruppe mit dem Erzeuger $\sigma_{V^{\bar\sigma}}$, also

$$\Omega \cong \prod_{V^{\bar\sigma}} l_{\sigma_{V^{\bar\sigma}}}^{|\sigma_{V^{\bar\sigma}}|-1}.$$

Ω ist ein homogenes Element in dem Ring $\mathbb{F}[\mathfrak{X}]^G_{\det^{-1}}$, das heißt,

$$g \cdot \Omega = \det{}^{-1}(g) \cdot \Omega \ , \ \forall\, g \in G,$$

und zwar gilt (Satz von R.P. Stanley [26])

$$\mathbb{F}[\mathfrak{X}]^G_{\det^{-1}} = \Omega \cdot \mathbb{F}[\mathfrak{X}]^G. \tag{2}$$

Sei nun $D\Omega := \{ D_s(\Omega) \mid s \in \mathbb{F}[\alpha_1, \cdots, \alpha_n] \}$ ein Unterraum von $\mathbb{F}[\mathfrak{X}]$. Mit Hilfe von (2) läßt sich zeigen :

Lemma 0.3 *Ist der Invariantenring $\mathbb{F}[\mathfrak{X}]^G$ polynomial, dann gilt $H \cong D\Omega$, also H ist zyklisch.*

Im nächsten Schritt ist zu zeigen, daß $\dim_{\mathbb{F}}(\mathbb{F}[\mathfrak{X}]_G) = |G|$ ist. Nun betrachten wir die Algebra $\hat{S}^*$, die durch die Menge $\{ e^x := \sum_{m\geq 0} \frac{x^m}{m!} \mid \forall\ x \in V^* \}$ und $\mathbb{F}[\mathfrak{X}]$ erzeugt wird. Die Differentialoperation von $\mathbb{F}[\mathfrak{A}]$ auf $\hat{S}^*$ wird zusätzlich durch $D_s(e^x) = s(x)e^x$, für alle $s \in \mathbb{F}[\mathfrak{A}]$, definiert. Für $x \in V^*$ definieren wir einen endlichdimensionalen Vektorraum $H_x := \{ h \in \hat{S}^* \mid D_s(h) = s(x)h,$ für alle $s \in \mathbb{F}[\mathfrak{A}]^G \}$.
Angenommen $s_1, \cdots, s_k$ seien homogene Elementen in $\mathbb{F}[\mathfrak{A}]$, die auf eine Basis für $\mathbb{F}[\mathfrak{A}]_G$ projiziert werden. Jedes homogene Element $F \in H_x$ läßt sich in der Form

$$F = D_s(\Omega e^x), \quad s = \sum_{i=1}^{k} c_i s_i,\ c_i \in \mathbb{F}$$

schreiben. Nach der Berechnung gilt, daß $F \neq 0$ ist, wenn $s \neq 0$. Das bedeutet, daß die Abbildung

$$\{s | s = \sum_{i=1}^{k} c_i s_i,\ c_i \in \mathbb{F},\ s_i \text{ ein Basiselement in } \mathbb{F}[\mathfrak{A}]_G \} \longrightarrow H_x$$

injektiv ist. Damit folgt $\dim_{\mathbb{F}}(\mathbb{F}[\mathfrak{X}]_G) \leq \dim_{\mathbb{F}} H_x$ für jedes $x \in V^*$, daher ist die Zahl $\dim_{\mathbb{F}}(H_x)$ unabhängig von der Wahl von x. Nun betrachten wir statt der Gruppe G die Isotropiegruppe $G_x := \{ g \in G \mid g \cdot x = x \}$ von $x \in V^*$. Jedes homogene Element $F \in H_x$ läßt sich dann in der Form

$$F = \sum_{g \in G} g(Pe^x) \text{ mit } \deg(gP) \geq (|G_x| - 1)^n, \text{ für alle } g \in G, \tag{3}$$

schreiben, wobei $P \in H$ mit $D_s(P) = 0$, für alle $s \in \mathbb{F}[\mathfrak{A}]^{G_x}$. Da die Zahl $\dim_{\mathbb{F}} H_x$ unabhängig von der Wahl von x ist, wählen wir ein $x \in V^*$, so daß $G_x = \{id\}$. Aus der Formel (3) mit $G_x = \{id\}$ folgt somit, daß F eine lineare Kombination von $\{e^{g(x)}\}_{g \in G}$ über $\mathbb{F}$ ist. Außerdem gilt im Allgemeinen $\dim_{\mathbb{F}}(\mathbb{F}[\mathfrak{X}]_G) \geq |G|$ im Sinne der Graduierung. Daraus ist zu schließen :

Lemma 0.4 *Sei $H \cong D\Omega$, dann gilt* $\dim_{\mathbb{F}}(\mathbb{F}[\mathfrak{X}]_G) = |G|$.

Mit dem Isomorphismus $\mathbb{F}[\mathfrak{X}]_G \cong \mathbb{F} \otimes_{\mathbb{F}[\mathfrak{X}]^G} \mathbb{F}[\mathfrak{X}]$ läßt sich feststellen, daß $\mathbb{F}[\mathfrak{X}]$ als $\mathbb{F}[\mathfrak{X}]^G$-Modul durch die $k = |G|$ homogenen Elemente $s_1, \cdots, s_k$ endlich erzeugt wird. Um die lineare Unabhängigkeit von $s_1, \cdots, s_k$ über $\mathbb{F}[\mathfrak{X}]$ zu zeigen, wurde zuerst eine sogenannte Twisted-Derivation $\triangle_\sigma$ bezüglich einer Pseudospieglung $\sigma \in G$ definiert :

$$\triangle_\sigma(f) := \frac{f - \sigma f}{l_\sigma}\ ,\ \forall\ f \in \mathbb{F}[x_1, \cdots, x_n].$$

Der Grad von $\triangle_\sigma(f)$ unterscheidet sich von dem Grad von f um 1. Dies ist zweckmäßig für die Anwendung von Induktion. Genauere Details für den Beweis befinden sich zum Beispiel in ([25] ab S. 77). Unter der Bedingung, daß $\dim_{\mathbb{F}}(\mathbb{F}[\mathfrak{X}]_G) = |G|$ ist, ist nun $\mathbb{F}[\mathfrak{X}]$ frei über $\mathbb{F}[\mathfrak{X}]^G$. Also haben wir (1) $\Leftrightarrow$ (2) im Satz (0.1) gezeigt. Letzlich erbrachte R. Kane den Beweis (2) $\Leftrightarrow$ (3). Er erklärte :
Die zuvor definierte Differentialoperation D induziert eine Differentialoperation, bezeichnet wieder mit D, von $\mathbb{F}[\mathfrak{A}]_G$ auf H, nämlich auf $\mathbb{F}[\mathfrak{X}]_G$. Das homogene Element Ω ist dann die Fundamentalklasse in $\mathbb{F}[\mathfrak{X}]_G$. Die Abbildung

$$\begin{array}{rcl} (\mathbb{F}[\mathfrak{A}]_G)_i \times (\mathbb{F}[\mathfrak{A}]_G)_{m-i} & \to & (\mathbb{F}[\mathfrak{X}]_G)_m \cong \mathbb{F} \\ (\alpha, \beta) & \mapsto & \langle\ \alpha\beta\ ,\ \Omega\ \rangle, \end{array}$$

für alle $i \geq 0, m = \deg(\Omega)$, ist eine nichtausgeartete Bilinearform. Aus der Dualität zwischen $(\mathbb{F}[\mathfrak{A}]_G)_j$ und $(\mathbb{F}[\mathfrak{X}]_G)_j$, für alle $j \geq 0$, ergibt sich die Eigenschaft der Poincarédualität. Außerdem ist die Bedingung $H \cong D\Omega$ äquivalent zur Bedingung $\langle \alpha\ , D_\beta(\Omega)\rangle \in \mathbb{F} - \{0\}$ für $\alpha \neq 0, D_\beta(\Omega) \neq 0$. Und durch die Gleichung

$$\langle \alpha\beta\ , \Omega\rangle = \langle \alpha\ , D_\beta(\Omega)\rangle$$

ist dann (2) $\Leftrightarrow$ (3) von Satz (0.1) gezeigt.

R. Steinberg und R. Kane haben sich nur mit der Bedingung $\operatorname{Char}\mathbb{F} = 0$ beschäftigt. Ihre Beweisführung funktioniert leider in der Charakteristik $p \neq 0$ nicht, da z.B. die dual Hopf-Algebra zu $\mathbb{F}[x_1, \cdots, x_n]$ keine Polynomalgebra ist, sondern eine Algebra von dividierten Potenzen, die kein noetherscher Ring ist. Darüber hinaus gilt das Argument, welches die Unabhängigkeit von $\dim_{\mathbb{F}}(H_x)$ zeigt, auch nicht ohne weiteres in der Charakteristik $p \neq 0$.
Der Anlaß zu dieser Arbeit ist der o.g. Artikel von R. Steinberg. Im ersten Abschnitt werden die Grundlagen, die in den weiteren Abschnitten benötigt werden, eingeführt. In den Abschnitten zwei betrachten wir $\mathbb{F}$-Vektorräume V mit $\dim_{\mathbb{F}}(V) = 2$. Wir zeigen für den modularen Fall (d.h. beliebige Charakteristik):

$$\begin{array}{ll} \mathbb{F}[V]_G & \text{ist genau dann eine Poincarédualitätsalgebra,} \\ \text{wenn} & \mathbb{F}[V]^G \text{ eine Polynomalgebra ist.} \end{array} \qquad (*)$$

Im Abschnitt drei betrachten wir den Fall $\dim_{\mathbb{F}}(V) = 3$, in dem die endlichen p-Gruppen P ($p = \operatorname{Char}(\mathbb{F})$) eine entscheidende Rolle spielen.

Im Abschnitt vier zeigen wir, daß diese Ergebnisse (*) auch unter den Voraussetzungen $|G| \in \mathbb{F}^\times$ und $\dim_{\mathbb{F}}(V) < \infty$ noch gültig sind.

Zum Schluß gehen wir auf den Satz von C. Chevalley ([7][22]) ein :

$$\text{Seien } |G| \in \mathbb{F}^\times \text{ und } \mathbb{F}[V]^G \text{ eine Polynomalgebra,}$$
$$\text{dann ist } \mathbb{F}[V]_G \text{ eine reguläre Darstellung von } G.$$

Für eine beliebige Charakteristik ist der Satz nicht richtig, allerdings ist er auf die sogenannte Grothendieck-Gruppe übertragbar.

Notation :

$Ann_A(M) := \{a \in A \mid am = 0,\ \forall\, m \in M\}$ der Annullator von M

$Ass_A(M) := \{\mathfrak{p} \mid \mathfrak{p}$ Primideal in $A, \exists\, m \in M$ mit $\mathfrak{p} = Ann_A(m)\}$

$\dim(A) :=$ Krulldimension einer Algebra A

$\dim_{\mathbb{F}}(V) :=$ Dimension eines Vektorraums V über einem Körper $\mathbb{F}$

$\mathbb{F}^\times := \mathbb{F} - \{0\}$, $\mathbb{F}$ ist ein Körper.

$\mathbb{F}_q :=$ endlicher Körper mit q Elementen

$FF(A) :=$ Quotientenkörper von A

$\mathbb{F}(G) :=$ Gruppenalgebra von G über $\mathbb{F}$

$\mathbb{F}[V] :=$ Algebra von Polynomfunktionen auf den $\mathbb{F}$-Vektorraum V

$\mathbb{F}(V) :=$ Quotientenkörper $FF(\mathbb{F}[V])$ von $\mathbb{F}[V]$

$\mathbb{F}[V]^G :=$ Algebra von G-invarianten Polynomfunktionen auf V

$\mathbb{F}[V]_G := \mathbb{F}[V]/h(G)$ Koinvariantenalgebra einer Gruppe G, die auf V operiert

$\overline{\mathbb{F}[V]^G} :=$ Menge aller Elemente in $\mathbb{F}[V]^G$ vom streng positiven Grad

$h(G) :=$ Hilbert-Ideal in $\mathbb{F}[V]$

$|G| :=$ Ordnung einer endlichen Gruppe G

$|G| \in \mathbb{F}^\times :=$ $|G|$ ist prim zur $\operatorname{Char}\mathbb{F} \neq 0$ oder $\operatorname{Char}\mathbb{F} = 0$

$GL(n, \mathbb{F}) :=$ Menge der invertierbaren $n \times n$ Matrizen über $\mathbb{F}$

$GL(V) :=$ Automorphismen eines Vektorraums V

Wenn nicht anders gesagt, identifizieren wir $GL(n, \mathbb{F})$ immer mit $GL(V)$.

$Im(\varphi) :=$ Bild einer Abbildung φ

$\ker(\varphi) :=$ Kern einer Abbildung φ

$\mathbb{Z} :=$ Menge der ganzen Zahlen

1 Grundlagen

Gegeben sei eine treue Darstellung $\varrho : G \hookrightarrow GL(n, \mathbb{F})(= GL(V))$ einer endlichen Gruppe G über einem Körper $\mathbb{F}$. In diesem Fall sagen wir auch, daß V ein (n-dimensionaler) $\mathbb{F}(G)$-Modul ist. Für einen n-dimensionalen Vektorraum V über $\mathbb{F}$ betrachten wir $\mathbb{F}[V]$ als die Algebra von Polynomfunktionen auf V über $\mathbb{F}$. Die Operation von G auf V induziert eine Operation auf $\mathbb{F}[V]$ durch

$$(\sigma f)(v) = f(\varrho(\sigma)^{-1}v), \quad \text{für alle} \quad \sigma \in G, v \in V, f \in \mathbb{F}[V].$$

Damit es nicht zu Mißverständnissen kommt, schreiben wir kurz G statt $\varrho(G)$ und σ statt $\varrho(\sigma)$.

Definition 1.1 *Sei $\varrho : G \hookrightarrow GL(V)$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$.*

1. *Die G-Fixpunktmenge*

$$\mathbb{F}[V]^G := \{f \in \mathbb{F}[V] \mid \sigma f = f \ , \forall\, \sigma \in G\}$$

   heißt **Invariantenring** *und seine Elemente* **invariante Polynome** *(oder* **invariante Elemente** *).*

2. $\overline{\mathbb{F}[V]^G} := \{f \in \mathbb{F}[V]^G \mid \deg(f) \neq 0\}$ *ist die Menge aller invarianten Polynome vom streng positiven Grad.*

3. *Das durch die Menge $\overline{\mathbb{F}[V]^G}$ erzeugte Ideal in $\mathbb{F}[V]$, nämlich*

$$h(G) := (\ \overline{\mathbb{F}[V]^G}\ )$$

   heißt **Hilbert-Ideal** *in $\mathbb{F}[V]$.*

4. *Der Quotient von $\mathbb{F}[V]$ durch $h(G)$ heißt* **Koinvariantenring** *und wird mit $\mathbb{F}[V]_G$ bezeichnet.*

Bemerkung 1.2 *Der Isomorphismus*

$$\mathbb{F}[V]_G \cong \mathbb{F} \otimes_{\mathbb{F}[V]^G} \mathbb{F}[V] \tag{4}$$

ist definiert durch die Multiplikation von $\mathbb{F}[V]^G$ auf $\mathbb{F}[V]$ und die Augmentation $\epsilon : \oplus \mathbb{F}[V]_j^G \longrightarrow \mathbb{F}$ mit $\epsilon(f) = \begin{cases} f & , \ \deg(f) = 0, \\ 0 & , \ \textit{sonst.} \end{cases}$

Die Grundlage der Invariantentheorie ist ausführlich beschrieben in [22].
Ein **graduierter Vektorraum** (**graduierter Modul**) M über einem Körper (einem Ring) $\mathbb{F}$ ist die Familie von Vektorräumen (Moduln) $M := \{M_i \mid i \in \mathbb{Z}\}$ (gewöhnlich schreiben wir auch $M = \oplus_{i\in\mathbb{Z}} M_i$). Ein graduierter $\mathbb{F}$-Vektorraum ($\mathbb{F}$-Modul) M heißt **positiv**, wenn $M_k = 0$, für alle $k < 0$ ist. Für zwei graduierte Vektorräume (graduierte Moduln) M und N über $\mathbb{F}$ ist ein Homomorphismus $f : M \longrightarrow N$ vom Grad d eine Folge von linearen Transformationen $\{f_i : M_i \longrightarrow N_{i+d} \mid i \in \mathbb{Z}\}$. Eine **graduierte Algebra** über $\mathbb{F}$ ist ein graduierter Vektorraum (graduierter Modul) A zusammen mit den Homomorphismen $\eta : \mathbb{F} \to A$ und $\mu : A \otimes A \to A$, so daß die Assoziativ- und Distributivgesetze erfüllt werden und $\eta(1) \in A$ eine zweiseitige Einheit ist. Die Komponente A_i von A heißt **homogene Komponente** vom Grad i. Eine positiv graduierte $\mathbb{F}$-Algebra A heißt **zusammenhängend**, wenn $A_0 \cong \mathbb{F}$ ist.

Im folgenden werden die Polynomalgebren $\mathbb{F}[V]$ immer als zusammenhängende graduierte kommutative Algebren über $\mathbb{F}$ betrachtet.

Bemerkung 1.3 *Die Operation von G auf $\mathbb{F}[V]$ bildet homogene Polynome auf homogene Polynome ab. So erbt $\mathbb{F}[V]^G$ (bzw. $h(G)$ bzw. $\mathbb{F}[V]_G$) die Graduierung von $\mathbb{F}[V]$.*

In dieser Arbeit läßt sich $\mathbb{F}[V]^G$ (bzw. $h(G)$ bzw. $\mathbb{F}[V]_G$) automatisch als graduiert betrachten.

Lemma 1.4 *Sei H eine normale Untergruppe von G. Dann gilt*

$$\mathbb{F}[V]^G \cong (\mathbb{F}[V]^H)^{G/H}.$$

Satz 1.5 *([22] S. 9, [27] S. 73) Sei $\varrho : G \hookrightarrow GL(V)$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$ und $\mathbb{F}(V)^G := \{ f/g \in \mathbb{F}(V) \mid \sigma(f/g) = f/g, \text{ für alle } \sigma \in g \}$. Dann gilt:*

1. *$\mathbb{F}(V)$ ist eine galoissche Erweiterung von $\mathbb{F}(V)^G$ mit der Galoisgruppe G.*
2. *$\mathbb{F}(V)^G$ ist identisch mit dem Quotientenkörper $FF(\mathbb{F}[V]^G)$ von $\mathbb{F}[V]^G$.*
3. *$\mathbb{F}[V]^G$ ist ganz abgeschlossen in $\mathbb{F}(V)^G$.*
4. *$\mathbb{F}[V]^G$ besitzt genau $\dim_{\mathbb{F}}(V)$ algebraisch unabhängige Elemente.*

Satz (1.5)(4) bedeutet, daß es mindestens $\dim_{\mathbb{F}}(V)$ Erzeuger für $\mathbb{F}[V]^G$ gibt. Aber sie sind im Allgemeinen nicht ausreichend, um den ganzen Invariantenring $\mathbb{F}[V]^G$ zu erzeugen.

Beispiel 1.6 *Definieren wir die Darstellung $\mathbb{Z}/4 \hookrightarrow GL(2,\mathbb{F})$ durch die Matrix $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Sei $\{x, y\}$ eine Basis für V^* über $\mathbb{F}$ und die Charakteristik von $\mathbb{F} \neq 2$. Dann sind*

$$\begin{aligned} f_1 &= x^2 + y^2, \\ f_2 &= x^2 y^2 \end{aligned}$$

zwei Erzeuger für $\mathbb{F}[x,y]^{\mathbb{Z}/4}$. Es ist leicht zu sehen, daß das Element $x^3y - xy^3$ auch ein invariantes Polynom ist, welches aber nicht von f_1 und f_2 erzeugt werden kann.

Satz 1.7 *(E. Noether [18][19][22]) Sei $\varrho : G \hookrightarrow GL(n,\mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Dann gilt :*

1. *$\mathbb{F}[V]$ ist ein endlich erzeugter $\mathbb{F}[V]^G$-Modul.*
2. *$\mathbb{F}[V]^G$ ist eine endlich erzeugte $\mathbb{F}$-Algebra.*

Korollar 1.8 *Sei $\varrho : G \hookrightarrow GL(n,\mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Dann ist $\mathbb{F}[V]_G$ ein endlichdimensionaler $\mathbb{F}$-Vektorraum. Insbesondere gilt $\dim_{\mathbb{F}}(\mathbb{F}[V]_G) = \dim_{\mathbb{F}}(\oplus_{i\geq 0}(\mathbb{F}[V]_G)_i) \geq |G|$.*

Der folgende Satz bietet eine Möglichkeit, sich alle invarianten Polynome in einer Kombination von algebraisch unabhängigen invarianten Polynomen darstellen zu lassen.

Proposition 1.9 *([22] S. 125) Sei $\varrho : G \hookrightarrow GL(n,\mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Seien $f_1, \cdots, f_n \in \mathbb{F}[V]^G$, $d_i := \deg(f_i)$ für $i = 1, \cdots, n$, so daß gilt :*

1. *$\prod_{i=1}^n d_i = |G|$,*
2. *$f_1, \cdots, f_n$ ist ein Parametersystem für $\mathbb{F}[V]^G$.*

Dann ist $\mathbb{F}[V]^G = \mathbb{F}[f_1, \cdots, f_n]$ eine Polynomalgebra.

Beispiel 1.10 *Sei $D_8 \hookrightarrow GL(2,\mathbb{R})$ eine Darstellung der Diedergruppe D_8 von der Ordnung 8, die durch*

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \textit{und} \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

erzeugt wird. Sei x, y eine $\mathbb{R}$-Basis für V^*. Dann ist $x^2 + y^2$ und $x^2 \cdot y^2$ eine $\mathbb{R}[x,y]^{D_8}$-reguläre Folge, also ein Parametersystem, und $\deg(x^2+y^2) \cdot \deg(x^2y^2) = 2 \cdot 4 = 8 = |D_8|$. Es gilt $\mathbb{R}[x,y]^{D_8} = \mathbb{R}[x^2+y^2, x^2y^2]$.

Poincaré-Reihe

Definition 1.11 *Sei $M = \{M_j\}_{j \geq 0}$ ein graduierter Vektorraum über einem Körper $\mathbb{F}$ mit $\dim_{\mathbb{F}}(M_j) < \infty$, für alle j. Die* **Poincaré-Reihe** *von M ist die formale Potenzreihe*

$$P(M,t) = \sum_{j=0}^{\infty} \dim_{\mathbb{F}}(M_j) t^j.$$

M ist **total endlich**, *wenn der Wert von $P(M,t)$ in $t = 1$ endlich ist, d.h. wenn $M_j \neq \{0\}$ nur für endlich viele j gilt. $P(M,t)|_{t=1}$ entspricht im total endlichen Fall $\dim_{\mathbb{F}}(M)$.*

Eigenschaften 1.12 *Seien M, M', M'' positiv graduierte Vektorräume.*

1. *Sei $0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$ eine kurze exakte Folge . Dann gilt*

$$P(M,t) = P(M',t) + P(M'',t).$$

2. *Für das Tensorprodukt $M' \otimes M''$ gilt*

$$P(M' \otimes M'', t) = P(M',t) \cdot P(M'',t).$$

3. *(D. Hilbert, J.-P. Serre) Sei A eine graduierte zusammenhängende kommutative $\mathbb{F}$-Algebra, die durch homogene Elemente $x_1, \cdots, x_n$ erzeugt wird und sei M ein endlich erzeugter graduierter A-Modul. Dann gilt*

$$P(M,t) = \frac{f(t)}{\prod_{j=1}^{s}(1-t^{k_j})} \in \mathbb{Q}[t],$$

wobei $k_j = \deg(x_j)$, $j = 1, \cdots, s$, und $f(t) \in \mathbb{Z}[t]$ ist.

Beispiel 1.13 *Für die Polynomalgebra* $A = \mathbb{F}[x_1, \cdots, x_s] \cong \mathbb{F}[x_1] \otimes \cdots \otimes \mathbb{F}[x_s]$ *mit* $d_i = \deg(x_i) \geq 1$, $i = 1, \cdots, s$, *ist die Poincaré-Reihe*

$$P(A,t) = \prod_{i=1}^{s} P(\mathbb{F}[x_i], t) = \prod \sum_{j \geq 0} t^{jd_i} = \prod_{i=1}^{s} \frac{1}{1 - t^{d_i}}.$$

Satz 1.14 *(T. Molien [22] S. 86) Sei* $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ *eine Darstellung einer endlichen Gruppe* G *über einem Körper* $\mathbb{F}$ *der Charakteristik* 0. *Dann ist die Poincaré-Reihe von* $\mathbb{F}[V]^G$ *gegeben durch*

$$\begin{aligned} P(\mathbb{F}[V]^G, t) &= \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - g^{-1}t)} = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(1 - gt)} && (5) \\ &= \frac{1/|G|}{(1-t)^n} + \frac{\ldots}{(1-t)^{n-1}} + \cdots. && (6) \end{aligned}$$

So ist $(1-t)^n P(\mathbb{F}[V]^G, t)|_{t=1} = \frac{1}{|G|}$. Diese rationale Zahl $(1-t)^n P(\mathbb{F}[V]^G, t)|_{t=1}$ wird **Grad** von $\mathbb{F}[V]^G$ genannt, geschrieben $\deg(\mathbb{F}[V]^G)$. Im Folgenden werden wir sehen, daß das Resultat $\deg(\mathbb{F}[V]^G) = \frac{1}{|G|}$ allgemein gültig ist.

Unter einem **graduierten Körper** verstehen wir einen graduierten Ring $K = \{K_i : i \in \mathbb{Z}\}$, so daß es für jedes $x \in K_i$ und jedes $i \in \mathbb{Z}$ ein $y \in K_{-i}$ mit $xy = 1$ gibt. Sei nun A eine zusammenhängende graduierte kommutative Algebra über einem Körper $\mathbb{F}$ und ein Integritätsring. Der graduierte Quotientenkörper $\mathbb{K}$ von A ist definiert durch $\mathbb{K} := \{\mathbb{K}_j \mid -\infty < j < \infty\}$ mit $\mathbb{K}_j := \{\frac{x}{y} \mid x \in A_{m+j},\ y \in A_m - \{0\}$ mit $m \geq \max\{0, -j\}\}$.

Proposition 1.15 *[22] Sei* $B \supseteq A$ *eine endliche Erweiterung von endlich erzeugten graduierten zusammenhängenden kommutativen Integritätsringen über einem Körper* $\mathbb{F}$ *und* $L \supseteq K$ *die Erweiterung der graduierten Quotientenkörper von* $B \supseteq A$. *Dann gilt*

$$\deg(B) = |L : K| \deg(A),$$

wobei $|L : K|$ *die Anzahl der Erzeuger des* K*-Moduls* L *ist.*

Setzen wir nun $A = \mathbb{F}[V]^G$ und $B = \mathbb{F}[V]$. Dann folgt sofort

Satz 1.16 *([22] S. 124) Sei* $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ *eine Darstellung einer endlichen Gruppe* G *über einem Körper* $\mathbb{F}$. *Dann gelten*

$$\begin{aligned} \deg(\mathbb{F}[V]^G) &= \frac{1}{|G|}, \text{ und} \\ P(\mathbb{F}[V]^G, t) &= \frac{\frac{1}{|G|}}{(1-t)^n} + \cdots. \end{aligned}$$

Beweis: $\mathbb{F}(V)$ ist eine galoissche Körpererweiterung von $\mathbb{F}(V)^G$ mit der Galoisgruppe G. Und $P(\mathbb{F}[V], t) = \frac{1}{(1-t)^n}$, also $\deg(\mathbb{F}[V]) = 1$. ■

Korollar 1.17 *Sei $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Ist $\mathbb{F}[V]^G = \mathbb{F}[f_1, \cdots, f_n]$ ein Polynomring mit $d_i := \deg(f_i), i = 1, \cdots, n$. Dann gilt $|G| = \prod_{i=1}^n d_i$.*

2 Irreduzible Ideale

In dem Rest dieser Arbeit diskutieren wir die Beziehung zwischen dem Invariantenring $\mathbb{F}[V]^G$ und dem Koinvariantenring $\mathbb{F}[V]_G$ einer endlichen Gruppe G. L. Smith hat bewiesen, daß $\mathbb{F}[V]_G$ eine Poincarédualitätsalgebra ist, wenn $\mathbb{F}[V]^G$ eine Polynomalgebra ist. Ist die Umkehrung auch gültig ? Im folgenden versuchen wir diese Frage zu beantworten.
Für $\dim_{\mathbb{F}}(V) \leq 3$ besitzt ein Invariantenring $\mathbb{F}[V]^G$ die sonderbare sogenannte Cohen-Macaulay-Eigenschaft. In diesem Abschnitt betrachten wir den Fall $\dim_{\mathbb{F}}(V) = 2$ und im nächsten Abschnitt den Fall $\dim_{\mathbb{F}}(V) = 3$.
Im Folgenden sei A eine graduierte zusammenhängende kommutative noethersche Algebra über einem Körper $\mathbb{F}$ und M ein endlich erzeugter graduierter A-Modul.

Definition 2.1 *Unter der* **Krulldimension** *von A, bezeichnet mit* $\dim(A)$, *wird die Zahl $max\{d \mid$ Primidealkette $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d$ in $A\}$ verstanden.*
Für einen endlich erzeugten A-Modul M wird seine Krulldimension durch $\dim(M) := \dim(A/Ann_A(M))$ *definiert.*

Für eine ganze Ringerweiterung sind ihre Krulldimension gleichwertig. Ferner gilt $\dim(\mathbb{F}[V]^G) = \dim(\mathbb{F}[V]) = \dim_{\mathbb{F}}(V)$ für eine Darstellung $G \hookrightarrow GL(V)$ einer endlichen Gruppe G über einem Körper $\mathbb{F}$.

Definition 2.2 *Ein* **homogenes Parametersystem** *für M mit* $\dim(M) = s$ *ist ein endliches System $a_1, \cdots, a_s$ von homogenen Elementen aus $\overline{A}$, so daß* $\frac{M}{(a_1,\cdots,a_s)M}$ *total endlich ist.*

Definition 2.3

1. *Ein Element x in M heißt* **regulär**, *wenn x kein Nullteiler in M ist, das heißt $x \cdot y \neq 0$, für alle $0 \neq y \in M$.*

2. *Eine endliche Folge $a_1, \cdots, a_s$ von homogenen Elementen aus $\overline{A}$ heißt eine M-***reguläre Folge**, *wenn*

   (a) $(a_1, \cdots, a_s)M \neq M$,

   (b) a_1 *ist kein Nullteiler in M, und*

   (c) a_{i+1} *ist kein Nullteiler in* $M/(a_1, \cdots, a_i)$ *für alle* $1 \leq i \leq s$.

Ein homogenes Parametersystem für M ist algebraisch unabhängig in A. Jede M-reguläre Folge kommt in einem homogenen Parametersystem für M vor, ist also auch algebraisch unabhängig. Die Länge einer M-regulären Folge ist nicht größer als die Krulldimension von M.

Definition 2.4 *Ein endlich erzeugter graduierter A-Modul M heißt* **Cohen-Macaulay**, *wenn $depth(M) = \dim(M)$ ist. Ein Ring A heißt* **Cohen-Macaulay-Ring**, *wenn A als A-Modul Cohen-Macaulay ist.*
Dabei ist $depth(M)$:= die Länge einer maximalen M-regulären Folge in $\overline{A}$.

Beispielsweise sind die Körper und die Polynomringe Cohen-Macaulay.

Satz 2.5 *(F.S. Macaulay [6] S. 57) Sei M ein Cohen-Macaulay A-Modul. Dann ist jedes homogene Parametersystem für M eine maximale M-reguläre Folge.*

Satz 2.6 *([3] S. 51) Sei M ein A-Modul. Die folgenden Aussagen sind äquivalent:*

1. *M ist ein Cohen-Macaulay A-Modul mit der Krulldimension d.*
2. *Es gibt ein homogenes Parametersystem $a_1, \cdots, a_d \in \overline{A}$ für M, so daß M ein endlich erzeugter freier $\mathbb{F}[a_1, \cdots, a_d]$-Modul ist.*

Korollar 2.7 *Es seien $f_1, \cdots, f_n \in \mathbb{F}[x_1, \cdots, x_n]$ ein homogenes Parametersystem für $\mathbb{F}[x_1, \cdots, x_n]$. Dann ist $\mathbb{F}[x_1, \cdots, x_n]$ ein endlich erzeugter freier $\mathbb{F}[f_1, \cdots, f_n]$-Modul.*

Satz 2.8 *([22] S. 258, [23]) Sei $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Für $n \leq 3$ ist der Ring $\mathbb{F}[V]^G$ Cohen-Macaulay.*

Definition 2.9 *Sei $H = \oplus_{i \geq 0} H_i$ eine graduierte zusammenhängende kommutative Algebra über $\mathbb{F}$. H heißt* **Poincarédualitätsalgebra** *der formalen Dimension d, wenn H die folgenden Bedingungen erfüllt :* [4]

1. *$H_i = 0$, $\forall\, i \geq d+1$.*
2. *$\dim_{\mathbb{F}}(H_d) = 1$ und $H_d = Span_{\mathbb{F}}\{[H]\}$, wobei $[H]$ die Fundamentalklasse von H ist.*
3. *Die Bilinearform $H_i \otimes_{\mathbb{F}} H_{d-i} \longrightarrow H_d$, $a \otimes b \mapsto a \cdot b$, ist nichtausgeartet, das heißt, eine Klasse $a \in H_i$ ist genau dann 0, wenn $a \cdot b = 0$ für alle $b \in H_{d-i}$ ist.*

[4] Die formale Dimension einer graduierten Algebra $H = \oplus_{i \geq 0} H_i$ ist $\max\{d \,|\, H_d \neq 0\}$.

Bemerkung 2.10 *Für eine graduierte zusammenhängende Algebra* $A = \oplus_{i\geq 0} A_i$ *definieren wir das Ideal* $\bar{A} := \oplus_{i\geq 1} A_i$. *Das Ideal* $\bar{A}$ *ist das einzige maximale homogene Ideal in* A. A *ist somit in diesem Sinn ein lokaler Ring.*

Definition 2.11 *Es sei* A *ein graduierter zusammenhängender kommutativer noetherscher Ring und* M *ein endlich erzeugter graduierter* A*-Modul. Die Menge*

$$Soc(M) := \{x \in M \mid \bar{A} \cdot x = 0\}$$

heißt der **Sockel** *von* M.

Definition 2.12 *Ein Ideal in* A *(bzw. ein* A*-Modul)* I *heißt* **irreduzibel**, *wenn* I *der Durchschnitt zweier größeren Idealen (bzw.* A*-Moduln)* U_1, U_2 *ist, dann ist* $I = U_1$ *oder* $I = U_2$.

Satz 2.13 *Die folgenden Aussagen sind äquivalent für einen graduierten zusammenhängenden kommutativen noetherschen Ring* A *und ein* $\bar{A}$*-primäres Ideal* $\mathfrak{q}$ *in* A *:*

1. *Das primäres Ideal* $\mathfrak{q}$ *ist irreduzibel.*
2. $Soc(A/\mathfrak{q})$ *ist ein freier* $A/\bar{A}$*-Modul vom Rang* 1 *(und ist die Komponent von* $A/\mathfrak{q}$ *vom Grad* d *).*
3. *Der Quotient* $A/\mathfrak{q}$ *ist eine Poincarédualitätsalgebra (der formalen Dimension* d*).*

Beweis:
(1) $\Leftrightarrow$ (2) : Der folgende Beweis basiert auf der folgenden Äquivalenz :
" $\mathfrak{q}$ ist irreduzibel $\Longleftrightarrow$ Der Nullmodul (0) in $A/\mathfrak{q}$ ist irreduzibel."
$\Rightarrow$: Angenommen $Soc(A/\mathfrak{q})$ sei ein freier Modul vom Rang 2. Wir finden zwei Untermoduln $U_1, U_2 \subset Soc(A/\mathfrak{q})$ mit $U_i \neq (0), i = 1, 2$, und $U_1 \cap U_2 = (0)$. Dies steht im Widerspruch zur Irreduzibilität von $\mathfrak{q}$.
$\Leftarrow$: Wäre das Ideal $\mathfrak{q}$ reduzibel, so existierten Untermoduln $U_1, U_2 \subset A/\mathfrak{q}$ und $U_i \neq (0),\ i = 1, 2$, mit $U_1 \cap U_2 = (0)$. Aber $U_i \cap Soc(A/\mathfrak{q}) \neq (0),\ i = 1, 2$, denn es gilt $Ass(U_i) = \{\bar{A}\}$ und deshalb existiert ein $x \in U_i \setminus \{0\}$, so daß $\bar{A} \cdot x = 0$. Der $A/\bar{A}$-Modul $Soc(A/\mathfrak{q})$ muß dann ein freier Modul vom Rang ≥ 2 sein.

(2) $\Rightarrow$ (3): Wir setzen $A/\mathfrak{q} := \oplus_{i\geq 0} H_i$ als einen positiv graduierten Modul. Da $Soc(A/\mathfrak{q})$ ein homogener Untermodul vom $A/\mathfrak{q}$ ist, existiert ein $d \in \mathbb{N}$, so daß $H_d \cong Soc(A/\mathfrak{q})$. Es ist klar, daß $H_i = 0$, für alle $i \geq d+1$ ist. Es bleibt noch zu zeigen, daß die Bilinearform $H_i \otimes H_{d-i} \longrightarrow H_d$ nichtausgeartet ist : Es gibt ein homogenes Element $a \in A/\mathfrak{q}, a \neq 0$, so daß $H_d \cong Soc(A/\mathfrak{q}) \subseteq (a) \subset A/\mathfrak{q}$ gilt. So existiert für jedes homogene Element $x \neq 0$ in $Soc(A/\mathfrak{q})$ ein homogenes Element $b \in A/\mathfrak{q}$, so daß $x = ab \neq 0$ gilt.
(3) $\Rightarrow$ (2): Es ist offensichtlich, weil $Soc(A/\mathfrak{q}) \cong H_d$ ist. ■

Lemma 2.14 *Sei $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G. Dann ist das homogene Hilbert-Ideal $h(G)$ ein $\overline{\mathbb{F}[V]}$-primäres Ideal in $\mathbb{F}[V]$.*

Beweis: Die Behauptung folgt unmittelbar aus der Tatsache, daß der $\mathbb{F}[V]^G$-Modul $\mathbb{F}[V]_G$ total endlich ist. ■

Satz 2.15 *(L. Smith [22] S. 156) Es seien $f_1, \cdots, f_n \in \mathbb{F}[x_1, \cdots, x_n]$ eine maximale reguläre Folge und $\mathbb{F}$ ein Körper. Wir setzen $H := \frac{\mathbb{F}[x_1,\cdots,x_n]}{(f_1,\cdots,f_n)}$ und $f_i = \sum_j a_{ij}x_j$ mit $a_{ij} \in \mathbb{F}[x_1, \cdots, x_n]$. Dann ist H eine Poincarédualitätsalgebra mit der Fundamentalklasse $[H] = \det(a_{ij})$.*

Satz 2.16 *Sei $G \hookrightarrow GL(2, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Ist $\mathbb{F}[V]_G$ eine Poincarédualitätsalgebra, dann ist $\mathbb{F}[V]^G$ eine Polynomalgebra.*

Der Beweis des Satzes (2.16) basiert auf folgenden Theorien :

Satz 2.17 *(Vasconcelos [29]) Es sei $(A, \mathfrak{m})$ ein 2-dimensionaler lokaler Cohen-Macaulay-Ring und I ein irreduzibles $\mathfrak{m}$-primäres Ideal. Falls I eine endliche projektive Dimension besitzt, dann ist I durch eine A-reguläre Folge erzeugt.*

Aus Satz (2.17) geht hervor, daß das Hilbert-Ideal $h(G)$ durch eine $\mathbb{F}[V]$-reguläre Folge erzeugt wird. Es bleibt nur noch zu zeigen, daß diese $\mathbb{F}[V]$-reguläre Folge durch eine $\mathbb{F}[V]^G$-reguläre Folge ersetzt werden kann. Dies erfolgt mittels Transfer bzw. Reynolds-Operator von $\mathbb{F}[V]$ auf $\mathbb{F}[V]^G$, die in nächster Seite eingeführt werden.

Bemerkung 2.18 *Wir werden ein Körper $\mathbb{F}$ der Charakteristik $p \neq 0$ als einen endlichen Körper $\mathbb{F}_q$ mit q Elementen betrachten, wobei q eine Potenz von p ist, wenn es für den Beweis nötig ist.*

Lemma 2.19 *Sei $\varrho : P \hookrightarrow GL(V)$ eine Darstellung einer endlichen p-Gruppe P mit einem Körper $\mathbb{F}$ der Charakteristik $p \neq 0$.*
Dann ist $\mathbb{F}[V]_1^P \neq \{0\}$.

Beweis: Es gilt $|V| \equiv 0 \mod p$. Der $\mathbb{F}$-Vektorraum V wird in einer disjunkten Vereinigung zerlegt

$$V = V^P \sqcup B_1 \sqcup \cdots \sqcup B_m,$$

wobei $B_i := \{\sigma x_i \mid \sigma \in P\}$ eine nichttriviale P-Bahn eines Elementes $x_i \in V$, $i = 1, \cdots, m$, ist. Da $|P| \equiv 0 \mod p$ ist, ist dann $|B_i| \equiv 0 \mod p$, für alle $i = 1, \cdots, m$. Daher folgt $|V^P| \equiv 0 \mod p$. Da der Nullvektor 0 ein Fixpunkt von P ist, ist $V^P \neq \emptyset$, also gilt $\dim_{\mathbb{F}}(V^P) \geq 1$. ■

Proposition 2.20 *([22] S. 251) Sei $P \hookrightarrow GL(2, \mathbb{F})$ eine Darstellung einer endlichen p-Gruppe P über einem Körper $\mathbb{F}$ der Charakteristik $p \neq 0$. Dann ist $\mathbb{F}[V]^P$ ein Polynomring.*

Beweis: Setzen wir $\mathbb{F} = \mathbb{F}_q$ als einen endlichen Körper mit $q = p^m$ $(m \geq 1)$ Elementen. Es gibt dann einen $\mathbb{F}_p$-Unterraum U von $\mathbb{F}_q$, so daß $P \cong \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in U \right\}$ [5]. Somit ist $\mid P \mid = \mid U \mid$. Sei x, y eine $\mathbb{F}$-Basis von V^*. Es ist leicht zu sehen, daß y und $f := \prod_{a \in U}(x + ay) \in \mathbb{F}[x, y]^P$ und $\deg(y) \cdot \deg(f) = \mid P \mid$ sind. $\{y, f\}$ ist ein Parametersystem. Daher ist $\deg(\mathbb{F}[x, y]^P) = \deg(\mathbb{F}[y, f])$ und nach Proposition (1.15) $FF(\mathbb{F}[x, y]^P) = FF(\mathbb{F}[y, f])$. Es ist ersichtlich, daß $\mathbb{F}[y, f]$ ganz abgeschlossen in $FF(\mathbb{F}[x, y]^P)$ ist. Es folgt dann $\mathbb{F}[x, y]^P = \mathbb{F}[y, f]$. ■

[5] Eine p-Sylow-Untergruppe $Syl_p(GL(n, \mathbb{F}))$ von $GL(n, \mathbb{F})$ besteht aus unipotenten Matrizen $\left\{ \begin{pmatrix} 1 & * & * * * & \\ 0 & 1 & * * * & \\ \cdots & \cdots & \ddots & * \\ 0 & \cdots & 0 & 1 \end{pmatrix} \mid * \in \mathbb{F} \right\}$.

Sei H eine Untergruppe einer endlichen Gruppe G und V ein endlichdimensionaler $\mathbb{F}(G)$-Modul. Der **Transfer** ist definiert durch ([22] S. 28)

$$\begin{aligned} Tr_H^G : \mathbb{F}[V]^H &\longrightarrow \mathbb{F}[V]^G, \\ f &\longmapsto \sum_{g \in G/H} g \cdot f. \end{aligned}$$

Der Transfer Tr_H^G ist ein $\mathbb{F}[V]^G$-Modulhomomorphismus. Setzen wir $Tr^G = Tr_{\{1\}}^G$. Es ist klar, daß $Tr^G = Tr_H^G \circ Tr^H$ ist. Wenn $\mid G : H \mid \in \mathbb{F}^\times$ ist, ist der Transfer Tr_H^G surjektiv und der **Reynolds-Operator** $\pi_H^G := \frac{1}{|G:H|} Tr_H^G : \mathbb{F}[V]^H \longrightarrow \mathbb{F}[V]^G$ eine Projektion mit $\pi_H^G \circ \pi_H^G = \pi_H^G$ und $\mathrm{Im}(\pi_H^G) = \mathbb{F}[V]^G$.

Sei nun $G \hookrightarrow GL(2, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G und $\mathbb{F}$ ein Körper der Charakteristik $p \neq 0$. Aus Proposition (2.20) wissen wir, daß der Invariantenring $\mathbb{F}[V]^{Syl_p(G)}$ polynomial ist, wobei $Syl_p(G)$ eine p-Sylow-Untergruppe von G ist. $\mathbb{F}[V]$ ist also ein freier $\mathbb{F}[V]^{Syl_p(G)}$-Modul. Es existert dann ein Epimorphismus $\mathbb{F}[V] \longrightarrow \mathbb{F}[V]^{Syl_p(G)}$ von $\mathbb{F}[V]^{Syl_p(G)}$-Moduln mit der Inklusion $\mathbb{F}[V]^{Syl_p(G)} \hookrightarrow \mathbb{F}[V]$ als spaltendem Homomorphismus. So ist die Komposition

$$\theta : \mathbb{F}[V] \longrightarrow \mathbb{F}[V]^{Syl_p} \xrightarrow{\pi_{Syl_p(G)}^G} \mathbb{F}[V]^G$$

surjektiv mit der Inklusion $i : \mathbb{F}[V]^G \longrightarrow \mathbb{F}[V]$ als spaltendem Homomorphismus. In dem Fall $\dim_{\mathbb{F}}(V) = 2$ läßt sich $\mathbb{F}[V]$ dann in die direkte Summe

$$\mathbb{F}[V] = \mathbb{F}[V]^G \oplus \ker(\theta)$$

zerlegen.

Ein Ideal I in einem Ring A heißt ein M-**reguläres Ideal** in A, wenn I durch eine M-reguläre Folge erzeugt wird.

Lemma 2.21 *Sei $G \hookrightarrow GL(2, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper der Charakteristik $p \neq 0$. Ist das Hilbert-Ideal $h(G)$ isomorph zu einem $\mathbb{F}[V]$-regulären Ideal, dann ist $h(G)$ isomorph zu einem $\mathbb{F}[V]^G$-regulären Ideal.*

Beweis: Wie schon gezeigt, ist die Abbildung $\theta : \mathbb{F}[V] \longrightarrow \mathbb{F}[V]^G$ ein Epimorphismus. Sei $h(G) \cong (f_1, f_2)$ mit einer $\mathbb{F}[V]$-regulären Folge f_1, f_2. Somit ist die induzierte Abbildung

$$\bar{\pi}^G : \frac{\mathbb{F}[V]}{(f_1, f_2)} \longrightarrow \frac{\mathbb{F}[V]^G}{(\theta(f_1), \theta(f_2)) \cdot \mathbb{F}[V]^G}$$

auch surjektiv. Da $\mathbb{F}[V]/(f_1, f_2) \cong \mathbb{F}[V]/h(G)$ total endlich ist, ist

$\mathbb{F}[V]^G/(\theta(f_1),\theta(f_2))\mathbb{F}[V]^G$ auch total endlich. Also ist $\theta(f_1),\theta(f_2)$ ein homogenes Parametersystem in $\mathbb{F}[V]^G$ und daher eine $\mathbb{F}[V]^G$-reguläre Folge. Es ist klar, daß $(\theta(f_1),\theta(f_2)) \subseteq (f_1,f_2)$ ist. Aufgrund des Vergleiches der Grade gilt sofort

$$(\theta(f_1),\theta(f_2)) \cong (f_1,f_2).$$

■

Wegen der Existenz eines Epimorphismus $\mathbb{F}[V] \longrightarrow \mathbb{F}[V]^G$ mit der Inklusion $\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]$ als spaltendem Homorphismus gibt es eine kleinste $d \in \mathbb{N}$, so daß $\mathbb{F}[F_1,F_2]_d \cong \mathbb{F}[V]^G_d$ ist, wobei $F_i := \theta(f_i),\ i = 1,2$, sind. Angenommen sei $k \geq d$ mit $\mathbb{F}[F_1,F_2]_k \cong \mathbb{F}[V]^G_k$. Sei nun $h \in \mathbb{F}[V]^G$ vom Grad $> k$, dann ist h von der Form $h = \alpha F_1 + \beta F_2$ mit passenden $\alpha,\beta \in \mathbb{F}[V]$. Daher gilt $h = \theta(\alpha)F_1 + \theta(\beta)F_2$ und $\deg(\theta(\alpha)),\deg(\theta(\beta)) \leq k$. Aus der Annahme folgt $\theta(\alpha),\theta(\beta) \in \mathbb{F}[F_1,F_2]$. Ferner gilt $h \in \mathbb{F}[F_1,F_2]$, also $\mathbb{F}[V]^G_l \cong \mathbb{F}[F_1,F_2]_l$, für alle $l \in \mathbb{N}$. Damit ist Satz (2.16) bewiesen.

3 Zerlegung in direkter Summe

Definition 3.1 *Sei $(A, \mathfrak{m}, k)$ ein Cohen-Macaulay lokaler Ring. Ein A-Modul $\omega(A)$ heißt ein* **kanonischer Modul** *von A, falls gilt :*

1. *$\omega(A)$ ist ein maximaler Cohen-Macaulay A-Modul, das heißt, die Krulldimension $\dim(\omega(A)) = \dim A$.*
2. *$\omega(A)$ ist von Typ 1, das heißt, die Zahl $r(\omega(A)) := \dim_k(Ext^i_A(k, \omega(A))) = 1$, für $i = depth(\omega(A))$.*
3. *$\omega(A)$ besitzt endliche injektive Dimension, die $injdim(A) < \infty$ geschrieben wird.*

Ein A-Modul M ist genau dann ein kanonischer Modul von A, wenn ([6] S. 107)

$$\dim_k(Ext^i_A(k, M)) = \begin{cases} 1 & , \quad i = \dim(A), \\ 0 & , \quad \text{sonst.} \end{cases} \tag{7}$$

Wenn ein kanonischer Modul existiert, ist er bis auf Isomorphismus eindeutig bestimmt.

Satz und Definition 3.2 *[6] Sei $(A, \mathfrak{m}, k)$ ein lokaler Cohen-Macaulay Ring. A heißt* **Gorenstein**, *wenn A eine der folgenden äquivalenten Bedingungen erfülllt :*

1. *A besitzt endliche injektive Dimension (in der Tat ist $injdim(A) = depth(A)$).*
2. *$\omega(A) \cong A$.*
3. *Jedes Ideal in A, das durch ein Parametersystem erzeugt wird, ist irreduzibel.*

Seien A ein lokaler Gorensteinring mit $d = \dim(A)$ und B eine A-Algebra mit $n = \dim(B)$. Wenn B ein Faktorring von A ist, dann existiert der kanonische Modul $\omega(B)$ von B und ist isomorph zu $Ext^{d-n}_A(B, A)$.

Lemma 3.3 *[2] Sei $(A, \mathfrak{m}, k)$ ein d-dimensionaler lokaler Cohen-Macaulay Ring und I ein $\mathfrak{m}$-primäres Ideal in A. Dann sind die folgenden Aussagen äquivalent :*

1. *Der Quotient A/I ist Gorenstein.*
2. $Ext^i_A(A/I, A) \cong \begin{cases} A/I & , \quad i = d, \\ 0 & , \quad sonst. \end{cases}$

Ausführlichere Informationen über Gorensteinringe und kanonische Moduln sind in [1] [2][6] gegeben.

Bemerkung 3.4 *Es seien G eine endliche Gruppe und V ein endlichdimensionaler $\mathbb{F}(G)$-Modul. Wenn $\mathbb{F}[V]_G$ eine Poincaŕedualitätsalgebra ist, ist sie ein 0-dimensionaler Gorensteinring.*

Satz 3.5 *([6] S. 116) Es sei $(A, \mathfrak{m}, k)$ ein lokaler Cohen-Macaulay Ring mit einem kanonischen Modul $\omega(A)$. Ist A ein faktorieller Ring und ein Quotient eines lokalen Gorensteinringes, dann ist A Gorenstein.*

Beweis: Angenommen A sei ein Quotient eines n-dimensionalen lokalen Gorensteinringes R und $d := \dim(A)$. Setzen wir $\omega(A) := Ext^{n-d}_R(A, R)$.
Behauptung : Ist x ein reguläres Element in A, dann ist x auch ein reguläres Element in $\omega(A)$. Denn $x \notin Ann_A(a), \forall\, a \in A$. Das bedeutet, daß x in keinem Primideal in $Ass_A(A)$ liegt. Aber jedes Primideal in $Ass_A(M)$ ist ein minimales Primideal. So liegt x auch in keinem Primideal in $Ass_A(M)$.
Diese Behauptung bedeutet, daß der A-Modul $\omega(A)$ torsionsfrei ist. Folglich ist seine Lokalisierung $\omega(A)_\mathfrak{p}$, $\forall\ \mathfrak{p} \in Spec(A)$ mit $ht(\mathfrak{p}) = 1$ [6], torsionsfrei. Daher sind $\omega(A)_\mathfrak{p}$, $\forall\ \mathfrak{p} \in Spec(A)$ mit $ht(\mathfrak{p}) = 1$, frei also projektiv und daher reflexiv [7] über $A_\mathfrak{p}$. Ferner gilt der Isomorphismus

$$\omega(A)^{\vee\vee} = \bigcap_{ht(\mathfrak{p})=1} \omega(A)^{\vee\vee}_\mathfrak{p} \cong \bigcap_{ht(\mathfrak{p})=1} \omega(A)_\mathfrak{p}.$$

[6] $ht(\mathfrak{p})$ ist die Höhe eines Primideals $\mathfrak{p}$.

[7] Für einen A-Modul M definieren wir den dualen Modul $M^\vee := Hom_A(M, A)$ und den kanonischen Homomorphismus von M in das Bidual $M^{\vee\vee}$ als $\varphi : M \longrightarrow M^{\vee\vee}, \varphi(m)(\alpha) := \alpha(m)$, $m \in M$, $\alpha \in M^\vee$. Ein A-Modul M heißt **reflexiv**, wenn $M \cong M^{\vee\vee}$ ist.

Daraus folgt, daß der A-Modul $\omega(A)$ reflexiv ist. Denn der endlich erzeugte torsionsfreie A-Modul $\omega(A)$ ist zu einem Untermodul eines freien A-Moduls isomorph, also zu einem Ideal in A. Wir bezeichnen dieses Ideal wieder mit $\omega(A)$. Ein reflexives Ideal ist ein divisorielles Ideal [8] . In einem faktoriellen Ring sind alle divisoriellen Ideale Hauptideale ([5] S. 160); so ist $\omega(A)$ ein freier Modul vom Rang 1. Anders ausgedrückt, gibt es einen Isomorphismus von A-Moduln

$$\omega(A) \cong A$$

A ist somit Gorenstein. ■

Korollar 3.6 *Sei $P \hookrightarrow GL(3, \mathbb{F})$ eine Darstellung einer endlichen p-Gruppe P über einem Körper $\mathbb{F}$ der Charakteristik $p \neq 0$. Dann ist $\mathbb{F}[V]^P$ ein Gorensteinring.*

Beweis: $\mathbb{F}[V]^P$ ist ein faktorieller Ring ([22](1.5.8)) und ein Cohen-Macaulay-Ring (Satz 2.8).

■

Lemma 3.7 *Sei $(A, \mathfrak{m}, k)$ ein d-dimensionaler lokaler Gorensteinring und M ein endlich erzeugter A-Modul mit endlicher projektiver Dimension. Dann gilt der Isomorphismus*

$$Tor_i^A(k, M) \cong Ext_A^{d-i}(k, M)\ ,\ 0 \leq i \leq d. \tag{8}$$

Beweis: Sei $0 \to F_d \to F_{d-1} \to \cdots \to F_1 \to F_0 \to 0$ eine minimale freie Auflösung von k. Wir setzen $F_i^* = Hom_A(F_i, A)$ für $i = 1, \cdots, d$. Dann ist

$$0 \to F_0^* \to F_1^* \to \cdots \to F_{d-1}^* \to F_d^* \to 0$$

eine minimale freie Auflösung des kanonischen Moduls $\omega(k)$ von k. Wegen des Isomorphismus $F_i^* \otimes_A M \cong Hom_A(F_i, M)$ ergibt sich

$$Tor_i^A(\omega(k), M) \cong Ext_A^{d-i}(k, M).$$

Denn Körper sind Gorenstein, daher ist die Behauptung bewiesen. ■

[8] Ein divisorielles Ideal $\mathfrak{a}$ ist ein nichttriviales gebrochenes Ideal von A mit $\mathfrak{a} = (\mathfrak{a}^{-1})^{-1}$, wobei $(\mathfrak{a})^{-1} := (A : \mathfrak{a}) \cong Hom_A(\mathfrak{a}, A)$.

Korollar 3.8 *Seien $G \hookrightarrow GL(3, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$ der Charakteristik $p \neq 0$ und $\mathbb{F}[V]^G$ ein Gorensteinring. Dann gelten*

$$\mathbb{F} \otimes_{\mathbb{F}[V]^G} \mathbb{F}[V] \cong Ext^3_{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]) , \tag{9}$$

$$\mathbb{F} \otimes_{\mathbb{F}[V]^{Syl_p(G)}} \mathbb{F}[V] \cong Ext^3_{\mathbb{F}[V]^{Syl_p(G)}}(\mathbb{F}, \mathbb{F}[V]) , \tag{10}$$

wobei $Syl_p(G)$ die p-Sylow-Untergruppe von G ist.

Nun sei H eine Untergruppe einer endlichen Gruppe G und V ein endlichdimensionaler $\mathbb{F}(G)$-Modul. Sei $P_\bullet : \cdots\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0$ eine $\mathbb{F}(G)$- bzw. $\mathbb{F}(H)$-projektive Auflösung von $\mathbb{F}$. Betrachten wir nun den Transfer $Tr^G_H : \mathbb{F}[V]^H \longrightarrow \mathbb{F}[V]^G$, $f \mapsto \sum_{g \in G/H} g(f)$. Für jedes $\alpha \in Hom_{\mathbb{F}(H)}(P_i, \mathbb{F}[V])$ gilt $Tr^G_H(\alpha) \in Hom_{\mathbb{F}(G)}(P_i, \mathbb{F}[V])$. So erhalten wir $Tr^G_H \circ d_{i+1} = Tr^G_H(\alpha \circ d_{i+1})$ und $d_i \circ Tr^G_H(\alpha) = Tr^G_H(d_i \circ \alpha)$. Hieraus induziert der Transfer einen Homomorphismus, bezeichnet wieder mit Tr^G_H,

$$Tr^G_H : Ext^i_{\mathbb{F}[V]^H}(\mathbb{F}, \mathbb{F}[V]) \longrightarrow Ext^i_{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]). \tag{11}$$

Und der Einschränkungshomomorphismus

$$Res^H_G : Ext^i_{\mathbb{F}[V]^G}(\mathbb{F}, \mathbb{F}[V]) \longrightarrow Ext^i_{\mathbb{F}[V]^H}(\mathbb{F}, \mathbb{F}[V]) \tag{12}$$

ist definiert durch die Inklusion $\mathbb{F}[V]^G \hookrightarrow \mathbb{F}[V]^H$.

Proposition 3.9 *([9] S. 39) Sei $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$ und H eine Untergruppe von G. Dann ist die Komposition*

$$Tr^G_H \circ Res^H_G = |G : H| \cdot id_{\mathbb{F}[V]^G}. \tag{13}$$

Korollar 3.10 *Sei $G \hookrightarrow GL(3, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$ der Charakteristik $p \neq 0$. Wenn $\mathbb{F}[V]_G$ eine Poincarédualitätsalgebra ist, dann läßt $\mathbb{F}[V]_G$ sich in die direkte Summe*

$$\mathbb{F}[V]_G \cong \mathbb{F}[V]_{Syl_p(G)} \oplus \frac{h(Syl_p(G))}{h(G)} \tag{14}$$

zerlegen.

Beweis: $Res^{Syl_p(G)}_G : \mathbb{F}[V]_G \longrightarrow \mathbb{F}[V]_{Syl_p(G)}$ ist ein spaltender Homomorphismus für den Reynolds-Operator $\pi^G_{Syl_p(G)} := \frac{1}{|G:Syl_p(G)|} Tr^G_{Syl_p(G)}$. ■

Satz 3.11 *Sei $G \hookrightarrow GL(3, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$ der Charakteristik $p \neq 0$. Ist $\mathbb{F}[V]_G$ eine Poincarédualitätsalgebra, dann ist $\mathbb{F}[V]_{Syl_p(G)}$ auch eine Poincarédualitätsalgebra, und daher ist $\mathbb{F}[V]^{Syl_p(G)}$ eine Polynomalgebra.*

Beweis: Nach Lemma (3.3) und Korollar (3.10) folgt sofort :

$$\begin{aligned} \mathbb{F}[V]_G &\cong Ext^3_{\mathbb{F}[V]}(\mathbb{F}[V]_G, \mathbb{F}[V]) \\ &\cong Ext^3_{\mathbb{F}[V]}(\mathbb{F}[V]_{Syl_p(G)}, \mathbb{F}[V]) \oplus Ext^3_{\mathbb{F}[V]}(\frac{h(Syl_p(G))}{h(G)}, \mathbb{F}[V]), \end{aligned}$$

also ist $\mathbb{F}[V]_{Syl_p(G)} \cong Ext^3_{\mathbb{F}[V]}(\mathbb{F}[V]_{Syl_p(G)}, \mathbb{F}[V])$ ein 0-dimensionaler Gorensteinring. Für zweite Behauptung siehe Satz (3.12). ■

Satz 3.12 *Sei $P \hookrightarrow GL(3, \mathbb{F})$ eine Darstellung einer endlichen p-Gruppe P über einem Körper $\mathbb{F}$ der Charakteristik $p \neq 0$. Wenn $\mathbb{F}[V]_P$ eine Poincarédualitätsalgebra ist, dann ist $\mathbb{F}[V]^P$ eine Polynomalgebra.*

Beweis: $\mathbb{F}[V]^P$ besitzt mindestens eine Linearform, bezeichnet mit l, als einen Erzeuger. $\mathbb{F}[V]/(l)$ ist dann ein 2-dimensionaler Cohen-Macaulay-Ring. Wenden wir nun den Satz (2.16) an : $h(P)/(l)$ wird durch eine $\mathbb{F}[V]^P$-reguläre Folge, nämlich (f, h), erzeugt. Also ist $h(P) \cong (l, f, h)$, das heißt $\mathbb{F}[V]^P \cong \mathbb{F}[l, f, h]$ ist eine Polynomalgebra. ■

4 Hochhebung einer Gruppendarstellung

Satz 4.1 *(R. Steinberg, R. Kane) Sei* $\mathbb{F}$ *ein Körper der Charakteristik* 0 *und* $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ *eine Darstellung einer endlichen Gruppe* G *über* $\mathbb{F}$. *Dann sind die folgenden Aussagen äquivalent :*

1. $\mathbb{F}[V]^G$ *ist eine Polynomalgebra.*
2. $\mathbb{F}[V]_G$ *ist eine Poincarédualitätsalgebra.*

Unser Ziel hier ist es zu zeigen, daß $\mathbb{F}[V]^G$ eine Polynomalgebra ist, wenn $\mathbb{F}[V]_G$ eine Poincarédualitätsalgebra und $\mid G \mid \in \mathbb{F}^\times$ ist. Das Resultat erhalten wir durch die folgenden Schritte : Zuerst konstruieren wir den neuen Körper $\mathbb{K}$ der Charakteristik 0 durch den sogenannten Witt-Ring des gegebenen vollkommenen Körpers $\mathbb{F}$; zweitens zeigen wir, daß eine Darstellung $\hat{\rho} : G \hookrightarrow GL(n, \mathbb{K})$ auf $\mathbb{K}$ existiert, die die Darstellung $G \hookrightarrow GL(n, \mathbb{F})$ induziert.

Witt-Ring

([10] ab S. 144, [12] ab S. 501) Sei p eine feste Primzahl. Wir betrachten Vektoren $Z = (Z_0, Z_1, \cdots, Z_m)$, $m = 1, 2, \cdots, \infty$, mit den Komponenten Z_i, die wir als Unbestimmte oder auch als Polynome in Unbestimmten mit Koeffizienten in $\mathbb{Z}[\frac{1}{p}]$ voraussetzen. Für $n = 0, 1, \cdots, m$ setzen wir

$$Z^{(n)} = Z_0^{p^n} + pZ_1^{p^{n-1}} + \cdots + p^n Z_n,$$

und nennen sie die **Nebenkomponenten** von Z.
Setzen wir $Z^p := (Z_0^p, Z_1^p, \cdots, Z_n^p)$, so können wir die Nebenkomponenten durch die Rekursionsformeln

$$\begin{aligned} Z^{(0)} &= Z_0 \\ Z^{(n)} &= (Z^p)^{(n-1)} + p^n Z_n \ , \text{ für alle } n \geq 1, \end{aligned}$$

ausdrücken. Ein Vektor Z ist dann durch seine Nebenkomponenten $Z^{(n)}$ bestimmt. Wir erhalten

$$\begin{aligned} Z_0 &= Z^{(0)}, \\ Z_n &= \frac{1}{p^n}(Z^{(n)} - (Z^p)^{(n-1)}) \\ &= \frac{1}{p^n}(Z^{(n)} - Z_0^{p^n} - pZ_1^{p^{n-1}} - \cdots - p^{n-1}Z_{n-1}), \text{ für alle } n \geq 1. \end{aligned}$$

Für die Vektoren $X = (X_0, X_1, \cdots, X_m)$ und $Y = (Y_0, Y_1, \cdots, Y_m)$ definieren wir $X \star Y = (X_0 \star Y_0, \cdots, X_m \star Y_m)$ durch Vorgabe der Nebenkomponenten $(X \star Y)^{(n)} = X^{(n)} \star Y^{(n)}$. Dabei bezeichne $\star$ eine der Rechenoperationen $+, -, \cdot$. Es ist klar, daß $(X \star Y)_n$ ein Polynom mit den Ausgangskomponenten X_i, Y_i $(i \leq n)$, mit einer Potenz von p in den Koeffizientennennern ist. In der Tat ist es erstaunlicherweise aber so, daß alle p-Potenzen in den Nennern verschwinden. Beispielsweise sind

$$\begin{aligned}
(X+Y)_0 &= X_0 + Y_0, \qquad (XY)_0 = X_0 Y_0, \\
(X+Y)_1 &= \frac{1}{p}(X+Y)^{(1)} - \frac{1}{p}(X+Y)_0^p \\
&= \frac{1}{p}(X^{(1)} + Y^{(1)}) - \frac{1}{p}(X_0 + Y_0)^p \\
&= X_1 + Y_1 + \frac{1}{p}[X_0^p + Y_0^p - \sum_{i=0}^{p} X_0^{p-i} Y_0^i]. \\
(X \cdot Y)_1 &= \frac{1}{p}[(X \cdot Y)^{(1)} - (X^p \cdot Y^p)^{(0)}] \\
&= \frac{1}{p}[(X_0^p + pX_1)(Y_0^p + pY_1) - X_0^p \cdot Y_0^p] \\
&= X_0^p \cdot Y_1 + X_1 \cdot Y_0^p + pX_1 \cdot Y_1.
\end{aligned}$$

Lemma 4.2 *([10] [12] S. 504) Für $n = 0, 1, 2, \cdots, m$ sind $(X \star Y)_n$ Polynome in den Variablen $X_0, Y_0, X_1, Y_1, \cdots, X_n, Y_n$ mit Koeffizienten in $\mathbb{Z}$.*

Wir bezeichnen die Polynome $(X \star Y)_n$ mit $S_n^\star(X, Y) = S_n^\star(X_0, Y_0, \cdots, X_n, Y_n)$. Sei nun A ein beliebiger kommutativer Ring mit Eins und $W_m(A)$ die Menge aller Vektoren $a = (a_0, a_1, \cdots, a_{m-1})$ mit den Komponenten $a_i \in A$ und den Nebenkomponenten $a^{(i)} = a_0^{p^i} + pa_1^{p^{i-1}} + \cdots + p^i a_i$, $0 \leq i \leq m-1$. Wir definieren die Addition und Multiplikation in $W_m(A)$ durch

$$(a \star b)_n := \bar{S}_n^\star(a_0, b_0, \cdots, a_n, b_n) \ , \ 0 \leq i \leq m-1,$$

für $a = (a_0, a_1, \cdots, a_{m-1})$ und $b = (b_0, b_1, \cdots, b_{m-1})$ in $W_m(A)$, mit dem Homomorphismus

$$\mathbb{Z}[X_0, Y_0, \cdots, X_n, Y_n] \longrightarrow A,$$

der durch $X_i \mapsto a_i$ und $Y_i \mapsto b_i$ definiert ist. Das Polynom $\bar{S}_n^\star(a_0, b_0, \cdots, a_n, b_n)$ ist dann das Bild von $S_n^\star(X_0, Y_0, \cdots, X_n, Y_n)$ in A.

Lemma 4.3 *([12] S. 505) Für jedes $m \geq 1$ ist $(W_m(A), +, \cdot)$ ein kommutativer Ring mit dem neutralen Element $1 = (1, 0, \cdots, 0)$ bezüglich der Multiplikation und dem neutralen Element $0 = (0, 0, \cdots, 0)$ bezüglich der Addition.*

Der Ring $W_m(A)$ wird als **Ring der Witt-Vektoren** der Länge m über A genannt. $W_1(A)$ wird mit dem Ring A identifiziert, da die Abbildung $A \longrightarrow W_1(A)$, $a \mapsto (a)$, ein Isomorphismus ist. Schließlich führen wir eine wichtige Regel ein, durch die die Vektoren $p^\alpha a$ in einfacher Weise beschrieben werden.

Lemma 4.4 *([10] S. 152) Für alle $\alpha \in W_m(A)$ gilt die Kongruenz $p^\alpha a \equiv V^\alpha a^{p^\alpha} \mod p$, für alle $\alpha \in \mathbb{N}$, dabei ist V die Verschiebungsoperation, die durch $Va = V(a_0, a_1, ..., a_{m-1}) = (0, a_1, a_2, ..., a_{m-2})$, für alle $a \in W_m(A)$ definiert wird.*

Beweis: Diese Kongruenz folgt aus der Gleichung

$$(p^\alpha a)^{(n)} = p^\alpha a^{(n)} = p^\alpha a_0^{p^n} + ... + p^{n+\alpha} a_n = (V^\alpha a)^{(n+\alpha)}.$$

■

Im Folgenden werden die wichtigsten Eigenschaften für die spätere Anwendung erläutert: Es sei nun $\mathbb{F}$ ein vollkommener Körper der Charakteristik p, d.h. $\mathbb{F}^p = \mathbb{F}$; beispielsweise ist jeder endliche Körper ein vollkommener Körper.

1. Die Ringe $W_m(\mathbb{F}), m \geq 1$, mit den Einschränkungshomomorphismen

   $$\lambda_{m-1} : W_m(\mathbb{F}) \longrightarrow W_{m-1}(\mathbb{F}),$$

   die durch $(a_0, \cdots, a_{m-1}) \mapsto (a_0, \cdots, a_{m-2})$ definiert sind, bilden ein projektives System. Der dadurch definierte projektive Limes $\varprojlim W_m(\mathbb{F})$ ist isomorph zu dem Ring $W_\infty(\mathbb{F})$ der Witt-Vektoren der Länge ∞. Wir identifizieren $W_\infty(\mathbb{F})$ mit $\varprojlim W_m(\mathbb{F})$, bezeichnen ihn mit $W(\mathbb{F})$ und nennen ihn **Witt-Ring** von $\mathbb{F}$.

2. Aus Lemma (4.4) erhalten wir die Gleichung

   $$p^\alpha a = V^\alpha a^p = (0, \cdots, 0, a_0^{p^\alpha}, a_1^{p^\alpha}, \cdots) \ , \ \forall\, a \in W(\mathbb{F}),\ \alpha \geq 1,$$

   daher besteht das Ideal $p^\alpha W(\mathbb{F})$ von $W(\mathbb{F})$ aus Vektoren von $W(\mathbb{F})$, deren erste α Komponenten 0 sind. Das Ideal $pW(\mathbb{F})$ ist dann das maximale Ideal in $W(\mathbb{F})$.

3. Wir definieren eine Abbildung $\nu : W(\mathbb{F}) \longrightarrow \mathbb{Z} \cup \{\infty\}$ durch $\nu(a) := min\{\ i \mid a_i \neq 0\}$. Setzen wir $\nu(0) = \infty$. Der Wert $\nu(a)$ ist wegen der Eigenschaft (2) auch der Exponent der höchsten Potenz von p, durch die a in $W(\mathbb{F})$ teilbar ist. Ferner gibt es für jeden Vektor $a \neq 0$ aus $W(\mathbb{F})$ die eindeutige Darstellung

   $$a = p^r \cdot u \quad \text{mit} \quad u \neq 0 \text{ und } u \not\equiv 0 \mod p,$$

   dabei ist $r = \nu(a)$.

4. Wegen $a \star b = (a_0, a_1, \cdots) \star (b_0, b_1, \cdots) = (a_0 \star b_0, \cdots)$, da $a_0 = a^{(0)}$ ist, entstehen folgende Regeln : $\nu(a \cdot b) = \nu(a) + \nu(b)$ und $\nu(a + b) \geq min\{\nu(a), \nu(b)\}$ für $a, b \in W(\mathbb{F})$. Daher ist der Ring $W(\mathbb{F})$ ein Integritätsring und hat die Charakterisik 0. Denn $n \cdot 1 = n \cdot (1, 0, \cdots) = (n, 0, \cdots, 0) \neq 0$ für $n \not\equiv 0 \ mod \ p$ und $p \cdot 1 = V(1^p, 0, \cdots) = (0, 1, 0, \cdots) \neq 0$.

5. Die Abbildung ν von $W(\mathbb{F})$ wird in der üblichen Weise auf den Quotientenkörper $\mathbb{K} = FF(W(\mathbb{F}))$ von $W(\mathbb{F})$ fortgesetzt und wieder mit ν bezeichnet. Ein Element in $\mathbb{K}$ hat die Gestalt $p^\alpha \frac{a}{b}$, $a, b \in W(\mathbb{F})$ und $\nu(a) = \nu(b) = 0$. Diese Abbildung ν wird **diskrete Bewertung** von $\mathbb{K}$ genannt und $W(\mathbb{F})$ ihr **diskreter Bewertungsring**.

6. Wegen der Vollkommenheit von $\mathbb{F}$ ist es möglich, ein Element $a = (a_0, a_1, \cdots)$ von $W(\mathbb{F})$ in der Form $a = (a_0, a_1^p, a_2^{p^2}, \cdots)$ umzuschreiben. Es gilt dann $a = (a_0, a_1^p, a_2^{p^2}, \cdots) = (a_0, 0, \cdots) + (0, a_1^p, 0, \cdots) + \cdots + (0, \cdots, 0, a_{n-1}^{p^{n-1}}, 0, \cdots) + (0, \cdots, 0, a_n^{p^n}, a_{n+1}^{p^{n+1}}, \cdots) = \alpha_0 + p\alpha_1 + p^2\alpha_2 + \cdots + p^{n-1}\alpha_{n-1} + p^n\alpha$ mit $\alpha_i = (a_i, 0, 0, \cdots)$ und einem Rest α in $W(\mathbb{F})$, also

$$a \equiv \alpha_0 + p\alpha_1 + p^2\alpha_2 + \cdots + p^{n-1}\alpha_{n-1} \ \ mod \ p^n.$$

Die Elemente von $W(\mathbb{F})$ lassen sich deshalb in einer formalen unendlichen Reihe

$$a = \sum_{i=0}^{\infty} \alpha_i p^i$$

schreiben.

7. Der Witt-Ring $W(\mathbb{F}_p)$ eines endlichen Körpers $\mathbb{F}_p$ mit p Elementen stimmt mit dem Ring $\hat{\mathbb{Z}}_p$ der ganzen p-adischen Zahlen überein, denn es existiert ein kanonischer Isomorphismus $W_m(\mathbb{F}_p) \to \mathbb{Z}/p^m\mathbb{Z}$, $(a_0, \cdots, a_{m-1}) \mapsto \tilde{a}_0 + \tilde{a}_1 p + \cdots + \tilde{a}_{m-1}p^{m-1} \ \ mod \ p^n$, $\forall \ m \geq 1$ mit $\tilde{a} \in \{0, 1, \cdots, p-1\}$.

8. Sei q eine Potenz von p. Dann hat jedes Element a von $W(\mathbb{F}_q)$ die Form

$$a = \sum a_i p^i, \quad \forall \ a_i \in \{0, 1, \xi, \xi^2, \cdots, \xi^{q-1}\}, \tag{15}$$

wobei ξ eine primitive $(q-1)$-te Einheitswurzel ist.

Gerade haben wir einen diskreten Bewertungsring $W(\mathbb{F})$ konstruiert, dessen Restklassenkörper $W(\mathbb{F})/pW(\mathbb{F})$ gleich dem gegebenen vollkommenen Körper $\mathbb{F}$ ist. Der Quotientenkörper $\mathbb{K}$ von $W(\mathbb{F})$ hat die Charakteristik 0. Also haben wir einen Brauer-Kontext in der Sinne von J.-P. Serre geschaffen.

Satz 4.5 *Sei G eine endliche Gruppe mit $\mid G \mid \in \mathbb{F}^{\times}$. Für jede Darstellung $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ existiert bis auf Konjugation genau eine Hochhebung $\tilde{\varrho} : G \hookrightarrow GL(n, W(\mathbb{F}))$ von ϱ.*

Der Beweis von Satz (4.5) erfördert einige Vorkehrungen.

Wegen $W(\mathbb{F}) = \varprojlim_r W_r(\mathbb{F})$ bzw. $GL(n, W(\mathbb{F})) = GL(n, \varprojlim_r W_r(\mathbb{F})) = \varprojlim_r GL(n, W_r(\mathbb{F}))$ reicht es zu zeigen:

Proposition 4.6 *Sei G eine endliche Gruppe mit $\mid G \mid \in F^{\times}$. Für eine Darstellung $\varrho_r : G \hookrightarrow GL(n, W_r(\mathbb{F}))$ auf $W_r(\mathbb{F})$ gibt es bis auf Konjugation genau eine Darstellung $\varrho_{r+1} : G \hookrightarrow GL(n, W_{r+1}(\mathbb{F}))$ auf $W_{r+1}(\mathbb{F})$,*
für alle $r \geq 1$.

Dies folgt aus der Tatsache, daß die zweite Kohomologiegruppe der Gruppe $\varrho_r(G)$ verschwunden ist. Im Folgenden werden die Kohomologiegruppe $H^*(\varrho_r(G), \ker(\pi_r))$ der Gruppe $\varrho_r(G)$ mit Koeffizienten in $\ker(\pi_r)$ durch die Standardauflösung definiert.

Bemerkung 4.7 *Die Inklusion $W_r(\mathbb{F}) \hookrightarrow W_{r+1}(\mathbb{F})$, für alle $r \geq 1$, definiert eine surjektive Abbildung $\pi_r : GL(n, W_{r+1}(\mathbb{F})) \longrightarrow GL(n, W_r(\mathbb{F}))$, dessen Kern eine endliche abelsche p-Gruppe ist, nämlich $\ker(\pi_r) \cong \mathbb{F}^n$.*

Angenommen F_m $(m \geq 1)$ sei ein freier $\mathbb{Z}(G)$-Modul mit den geordneten m-Tupeln $\{ (x_1, \cdots, x_m) \mid x_i \in G \}$ als Basis und F_0 sei ein freier $\mathbb{Z}(G)$-Modul mit einem einzigen Basiselement, bezeichnet mit $[\,]$ (manchmal identifizieren wir F_0 mit $\mathbb{Z}(G)$, dann ist $[\,] \cong 1$). In diesem Abschnitt definieren wir die Kohomologiegruppe $H^*(G, M)$ durch die Standardauflösung ([4][11]) :

$$\mathbf{F}_* : \cdots \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} \mathbb{Z} \to 0 \ ,$$

mit den Homomorphismen

$$\begin{aligned} d_0([\,]) &:= 1 \\ d_n(x_1, \cdots, x_n) &:= x_1(x_2, \cdots, x_n) \\ &+ \sum_{i=1}^{n-1} (-1)^i (x_1, \cdots, x_{i-1}, x_i x_{i+1}, x_{i+2}, \cdots, x_n) \\ &+ (-1)^n (x_1, \cdots, x_{n-1}). \end{aligned}$$

Dadurch erhalten wir den folgenden Komplex für einen G-Modul M

$$0 \to Hom_{\mathbf{Z}(G)}(F_0, M) \stackrel{d_1^*}{\to} Hom_{\mathbf{Z}(G)}(F_1, M) \stackrel{d_2*}{\to} \cdots$$

mit

$$\begin{aligned}(d_n^* f)(x_1, \cdots, x_n) &= x_1 f(x_2, \cdots, x_n) \\ &+ \sum_{i=1}^{n-1} (-1)^i f(x_1, \cdots, x_{i-1}, x_i x_{i+1}, \cdots, x_n) \\ &+ (-1)^n f(x_1, \cdots, x_{n-1}).\end{aligned}$$

Nun definieren wir die i-te Kohomologiegruppe der Gruppe G mit Koeffizienten in einem $\mathbb{Z}(G)$-Modul M durch

$$H^i(G, M)(\cong Ext^i_{\mathbf{Z}(G)}(\mathbb{Z}, M)) = \frac{ker(d_{i+1}^*)}{Im(d_i^*)}.$$

Insbesondere wird ein Element aus $\ker(d_2^*)$ bzw. aus $\mathrm{Im}(d_1^*)$ eine **Derivation** (crossed homomorphism) bzw. **Hauptderivation** (principal crossed homomorphism) von G zu M genannt und ein Element in $\ker(d_3^*)$ bzw. in $\mathrm{Im}(d_2^*)$ **Faktorsystem** bzw. **Hauptfaktorsystem** von G zu M.

Hilfslemma 4.8 *([4][11] S. 226) Es sei H eine Untergruppe einer endlichen Gruppe G mit dem Index $\mid G : H \mid = m$ und M ein $\mathbb{Z}(G)$-Modul. Setzen wir $G = \cup_{i=1}^m H x_i$, dann ist die Komposition*

$$Tr \circ Res : H^k(G, M) \longrightarrow H^k(G, M), \text{ für alle } k \geq 0,$$

die Multiplikation mit m, wobei die Einschränkungsabbildung $Res := Res_G^H : H^k(G, M) \longrightarrow H^k(H, M), k \geq 0$, ein Homomorphismus ist, der durch die Einbettung $i : H \hookrightarrow G$ definiert wird. Ebenso ist der Transfer $Tr := Tr_H^G : H^k(H, M) \longrightarrow H^k(G, M)$ ein Homomorphismus, der durch die Komposition $H^k(H, M) \simeq H^k(G, Hom_H(\mathbb{Z}(G), M)) \longrightarrow H^k(G, M)$ mit dem G-Modul-Epimorphismus $\theta : Hom_H(\mathbb{Z}(G), M) \longrightarrow M, \varphi \mapsto \theta(\varphi) := \sum_{i=1}^n x_i^{-1} \varphi x_i$ definiert wird.

Beweis: Durch Induktion über k :
Für $k = 0$ gilt $H^0(G, M) = M^G$, also $Tr \circ Res : M^G \longrightarrow M^G, a \mapsto \sum_{x \in G/H} xa = ma$, für alle $a \in M^G$.

Für $k \geq 1$: Wählen wir eine exakte Folge $0 \longrightarrow M \longrightarrow I \longrightarrow M' \longrightarrow 0$ von G-Moduln mit einem injektiven Modul I. Dann kommutiert das folgende Diagramm, in dem die beiden horizontalen Folgen exakt sind :

$$\begin{array}{ccccccccc}
\cdots \longrightarrow 0 & \longrightarrow & H^{k-1}(G,M') & \longrightarrow & H^k(G,M) & \longrightarrow & H^k(G,I) & \longrightarrow \cdots \\
 & & \downarrow {\scriptstyle TroRes} & & \downarrow {\scriptstyle TroRes} & & \downarrow {\scriptstyle TroRes} & \\
\cdots \longrightarrow 0 & \longrightarrow & H^{k-1}(G,M') & \longrightarrow & H^k(G,M) & \longrightarrow & H^k(G,I) & \longrightarrow \cdots
\end{array}$$

Daraus folgt die Behauptung. ■

Korollar 4.9 *Ist G eine endliche Gruppe der Ordnung m, dann gilt*

$$mH^k(G,M) = 0, \text{ für alle } k \geq 1.$$

Beweis: Die Behauptung folgt unmittelbar aus Hilfslemma (4.8) mit $H = \{1\}$. ■

Hilfslemma 4.10 *Seien $\mathfrak{R}$ ein Körper der Charakteristik p und G eine endliche Gruppe, deren Ordnung prim zu p ist. Dann gilt $H^k(G,M) = 0$, $\forall\, k \geq 1$, für alle $\mathfrak{R}(G)$-Moduln M.*

Beweis: Angenommen m sei die Ordnung von G. Wir definieren einen G-Modulhomomorphismus $m : M \longrightarrow M$ durch $\alpha \mapsto m\alpha, \forall\, \alpha \in M$. Wegen $\mid G \mid \in \mathfrak{R}^\times$ ist $m : M \longrightarrow M$ ein Isomorphismus. Daher ist $m^* : H^k(G,M) \longrightarrow H^k(G,M)$ mit $m^*(f) = m \cdot f$, $\forall\ f \in H^k(G,M)$, ein Isomorphismus. Da $m \cdot H^k(G,M) = 0$, $\forall\, k \geq 1$, folgt sofort $H^k(G,M) = 0, \forall\, k \geq 1$. ■

Beweis: von Proposition (4.6) :
(Existenz) : Betrachten wir die exakte Folge von Gruppen

$$0 \longrightarrow \ker(\breve{\pi}_r) \hookrightarrow \breve{G} \xrightarrow{\breve{\pi}_r} \varrho_r(G) \longrightarrow 1, \quad (r \geq 1),$$

wobei $\ker(\breve{\pi}_r)$ eine abelsche p-Gruppe und eine normale Untergruppe von $\breve{G}$ ist und $\breve{G} \leq GL(n, W_{r+1}(\mathbb{F}_q))$. Sei $\lambda : \varrho_r(G) \longrightarrow \breve{G}$ eine Abbildung mit $\breve{\pi}_r \circ \lambda = id_{\varrho_r(G)}$ und $\lambda(1) = 1$.
Behauptung : Diese Abbildung $\lambda : \varrho_r(G) \longrightarrow \breve{G}$ ist ein Homomorphismus.
Da $\ker(\breve{\pi}_r) \trianglelefteq \breve{G}$ ist, gilt $\lambda(x)b\lambda^{-1}(x) \in \ker(\breve{\pi}_r)$, für alle $x \in \varrho_r(G)$, $b \in \ker \breve{\pi}_r$. Das Element $\lambda(x)b\lambda^{-1}(x)$ ist unabhängig von der Wahl von λ. Sei λ' eine andere Abbildung mit $\breve{\pi}_r\lambda' = id_{\varrho_r(G)}$, so gilt die Gleichung $\breve{\pi}_r(\lambda' \cdot \lambda^{-1})(x) = (\breve{\pi}_r\lambda')(\breve{\pi}_r\lambda)^{-1}(x) = 1$. Setzen wir $\lambda' = c \cdot \lambda$ für ein $c \in \ker(\breve{\pi}_r)$, dann

ist $\lambda'(x)b\lambda'(x)^{-1} = c\lambda(x)b\lambda^{-1}c^{-1} = \lambda(x)b\lambda^{-1}(x)$. Deshalb können wir $xb := \lambda(x)b\lambda^{-1}(x)$, für $x \in \varrho_r(G), b \in \ker(\breve{\pi}_r)$ definieren.
Angenommen λ sei kein Homomorphismus. Die Elemente $\lambda(xy)$ und $\lambda(x)\lambda(y)$ unterscheiden sich daher mit einem Element aus $\ker(\breve{\pi}_r)$. So definieren wir eine Funktion $f : \varrho_r(G) \times \varrho_r(G) \longrightarrow \ker(\breve{\pi}_r)$ durch die Gleichung $\lambda(x)\lambda(y) = f(x,y)\lambda(xy)$, für alle $x, y \in \varrho_r(G)$. Nun wenden wir das Assoziativitätsgesetz in $\breve{G}$ an :

$$\begin{aligned}
[\lambda(x)\lambda(y)]\lambda(z) &= f(x,y)\lambda(xy)\lambda(z) &= f(x,y)f(xy,z)\lambda(xyz), \\
\lambda(x)[\lambda(y)\lambda(z)] &= \lambda(x)[f(y,z)\lambda(yz)] &= \lambda(x)f(y,z)\lambda^{-1}(x)\lambda(x)\lambda(yz) \\
&= xf(y,z)\lambda(x)\lambda(yz) &= xf(y,z)f(x,yz)\lambda(xyz).
\end{aligned}$$

Somit ist $f(x,y)f(xy,z) = xf(y,z)f(x,yz)$. f korrespondiert also mit einem Element aus $H^2(\varrho_r(G), \ker(\breve{\pi}_r))$. Aber $H^2(\varrho_r(G), \ker(\breve{\pi}_r)) = 0$; λ ist somit ein Homomorphismus. Daraus ergibt sich, daß $\breve{G}$ das semidirekte Produkt von $\ker(\breve{\pi}_r)$ und $\varrho_r(G)$ ist. Nun kann eine Abbildung ϱ_{r+1} durch $\varrho_{r+1} \equiv \varrho_r \; mod \; p$ definiert werden.
(Eindeutigkeit) : Die Hochhebung ϱ_{r+1} von ϱ_r ist bis auf Konjugation eindeutig bestimmt. Mit anderen Worten, es ein Element $a \in \ker(\breve{\pi}_r)$ gibt mit

$$\lambda_1(g) = i(a)\lambda_2(g)i(a)^{-1} \quad \forall\, g \in \varrho_r(G),$$

wenn λ_1 und λ_2 zwei Spaltabbildungen von $\varrho_r(G)$ auf $\breve{G}$ sind. Da $\breve{G}$ das semidirekte Produkt von $ker(\breve{\pi}_r)$ und $\varrho_r(G)$ ist, lassen sich die Abbildungen $\lambda_i, i = 1{,}2$, in der Form

$$\lambda_i(g) = (d_i(g), g)\ ,\ \forall\, g \in \varrho_r(G)$$

darstellen, wobei $d_i, i = 1{,}2$, Derivationen von $\varrho_r(G)$ auf $ker(\breve{\pi}_r)$ sind. Ferner gilt

$$\begin{aligned}
\lambda_1(g) &= (d_1(g), g) \\
&= (a,1)(d_2(g), g)(a,1)^{-1} \\
&= (a + d_2(g) - ga, g) \\
&= i(a)\lambda_2(g)i(a)^{-1},
\end{aligned}$$

also $d_2(g) - d_1(g) = ga - a$. Damit ist $d_2 - d_1$ eine Hauptderivation. Die Menge $\ker(\breve{\pi}_r)$-konjugierter Klassen von Spaltabbildungen $\lambda : \varrho_r(G) \longrightarrow \breve{G}$ steht dann in bijektiver Korrespondenz zu der 1-ten Kohomologiegruppe $H^1(\varrho_r(G), \ker(\breve{\pi}_r))$. Die ist aber verschwunden, daher gibt es nur eine konjugierte Klasse. ■

Beweis: von Satz (4.5) :
Setzen wir $\varrho := \varrho_1 : G \hookrightarrow GL(n, \mathbb{F})$, $\tilde{\varrho} := \varprojlim \varrho_r : G \hookrightarrow GL(n, W(\mathbb{F}_q))$ und $\pi := \breve{\pi}_1 \circ \breve{\pi}_2 \circ \cdots \circ \breve{\pi}_r$. Da $H^2(\varrho(G), ker\pi) = H^2(\varrho_1(G), \ker(\breve{\pi}_1)) \cdot \prod_{i=2}^{r} H^2(\varrho_i(G), \ker(\breve{\pi}_i)) = 0$ und $H^2(\varrho(G), \varprojlim \pi) = \varprojlim H^2(\varrho(G), \ker(\pi)) = 0$, gilt $\tilde{\varrho}(G) \equiv \varrho(G)$ *mod* p. ■

Für eine Darstellung $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ einer endlichen Gruppe G über einem vollkommenen Körper $\mathbb{F}$ mit $\mid G \mid \in \mathbb{F}^\times$ erhalten wir nun eine Darstellung $\tilde{\varrho} : G \hookrightarrow GL(n, W(\mathbb{F}))$ auf den Ring $W(\mathbb{F})$ der Charakteristik 0. Und wir gewinnen eine Darstellung, bezeichnet mit $\hat{\varrho}$, auf $FF(W(\mathbb{F}))$ durch die Inklusion $W(\mathbb{F}) \hookrightarrow FF(W(\mathbb{F}))$.

Notation :

$\mathbb{F}$:= Vollkommener Körper der Charakteristik p
$\boldsymbol{A} := W(\mathbb{F})$
$\mathbb{K} := FF(W(\mathbb{F})$
$M \cong \boldsymbol{A}^n$
$V = \mathbb{F} \otimes_{\boldsymbol{A}} M \cong \mathbb{F}^n$.
$W = \mathbb{K} \otimes_{\boldsymbol{A}} M \cong \mathbb{K}^n$.
$G := \varrho(G)$.
$\tilde{G} := \tilde{\varrho}(G)$.
$\hat{G} := \hat{\varrho}(G)$.
n.b. $G \cong \tilde{G} \cong \hat{G}$.
Aus den obigen Bezeichungen besteht ein Brauer-Kontext in der Sinne von J.-P. Serre.

Im Folgenden wird vorausgesetzt, daß $\mid G \mid$ prim zu p ist.

Proposition 4.11 *Es sei $\tilde{\varrho} : G \hookrightarrow GL(M)$ eine Hochhebung einer Darstellung $\varrho : G \hookrightarrow GL(V)$ einer endlichen Gruppe G über einem Körper $\mathbb{F}$ und $\hat{\varrho} : G \hookrightarrow GL(W)$ eine Erweiterung von $\tilde{\varrho}$ auf den Körper $\mathbb{K}$ der Charakteristik 0. Dann gibt es Isomorphismen*

$$\mathbb{F} \otimes_{\boldsymbol{A}} \boldsymbol{A}[M]^{\tilde{G}} \longrightarrow \mathbb{F}[V]^G \quad \textit{und} \qquad \mathbb{K} \otimes_{\boldsymbol{A}} \boldsymbol{A}[M]^{\tilde{G}} \longrightarrow \mathbb{K}[W]^{\hat{G}}.$$

Beweis:

1. Sei $\psi : \mathbb{F} \otimes \boldsymbol{A}[M]^{\tilde{G}} \longrightarrow \mathbb{F}[V]^G$ eine Abbildung, die durch $a \otimes \tilde{f} \mapsto a\tilde{f}$, für alle $\tilde{f} \in \boldsymbol{A}[M]^{\tilde{G}}$, $a \in \mathbb{F}$, definiert sei.
   ψ ist ein Homomorphismus : Das ist klar.

ψ ist surjektiv : Für ein Polynom $f \in \mathbb{F}[V]^G$ gibt es ein Polynom $\tilde{f} \in \boldsymbol{A}[M]$. Wegen $\mid G \mid \in \mathbb{F}^\times$ ist das Bild des Reynolds-Operators $\pi^{\tilde{G}}\ \boldsymbol{A}[M]^{\tilde{G}}$.
ψ ist injektiv : Sei $\tilde{f} \in \boldsymbol{A}[M]^{\tilde{G}}$ mit $\psi(1 \otimes \tilde{f}) = 0$, das heißt $0 = \psi(1 \otimes \tilde{f}) = 1 \otimes \tilde{f}$ *mod* p, so ist $\tilde{f} \equiv 0$ *mod* p. Es existiert dann ein $\tilde{h} \in \boldsymbol{A}[M]^{\tilde{G}}$, so daß $\tilde{f} = p \cdot \tilde{h}$ ist. Nach der Tensorproduktregel folgt $1 \otimes \tilde{f} = p \otimes \tilde{h} \equiv 0 \otimes \tilde{h} = 0$.

2. $\psi : \mathbb{K} \otimes \boldsymbol{A}[M]^{\tilde{G}} \longrightarrow \mathbb{K}[W]^{\hat{G}}$ wird definiert durch $a \otimes \tilde{f} \mapsto a \cdot \tilde{f}$.

■

Korollar 4.12 *Seien ϱ, $\tilde{\varrho}$ und $\hat{\varrho}$ wie in Proposition (4.11). Dann existieren Isomorphismen*

$$\mathbb{F} \otimes_{\boldsymbol{A}} h_{\boldsymbol{A}}(\tilde{G}) \longrightarrow h_{\mathbb{F}}(G) \qquad \textit{und} \qquad \mathbb{K} \otimes_{\boldsymbol{A}} h_{\boldsymbol{A}}(\tilde{G}) \longrightarrow h_{\mathbb{K}}(\hat{G}).$$

Korollar 4.13 *Seien ϱ, $\tilde{\varrho}$ und $\hat{\varrho}$ wie in Proposition (4.11). Dann existieren Isomorphismen*

$$\begin{array}{rcl} \mathbb{F} \otimes_{\boldsymbol{A}} (\boldsymbol{A}[M]/h_{\boldsymbol{A}}(\tilde{G})) & \longrightarrow & \mathbb{F}[V]/h_{\mathbb{F}}(G) \quad \textit{und} \\ \mathbb{K} \otimes_{\boldsymbol{A}} (\boldsymbol{A}[M]/h_{\boldsymbol{A}}(\tilde{G})) & \longrightarrow & \mathbb{K}[W]/h_{\mathbb{K}}(\hat{G}). \end{array}$$

Lemma 4.14 *Es sei $\tilde{\varrho} : G \hookrightarrow GL(M)$ eine Hochhebung einer Darstellung $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ über $\mathbb{F}$. Sei $\mathbb{F}[V]_G := \oplus_{i=0}^{d} H_i$ eine Poincarédualitätsalgebra der formalen Dimension d. Dann ist auch $\boldsymbol{A}[M]_{\tilde{G}} := \oplus_{i \geq 0} \tilde{H}_i$ eine Poincarédualitätsalgebra, wobei H_i bzw. $\tilde{H}_i$ die homogene Komponente vom Grad i ist.*

Beweis: Wegen des Isomorphismus von $\mathbb{F} \otimes_{\boldsymbol{A}} \tilde{H}_d \longrightarrow H_d$ gilt $1 = \dim_{\mathbb{F}}(H_d) = \dim_{\mathbb{F}}(\mathbb{F} \otimes_{\boldsymbol{A}} \tilde{H}_d) = \dim_{\boldsymbol{A}}(\tilde{H}_d)$. Aus Satz (2.13) folgt dann sofort, daß $\boldsymbol{A}[M]_{\tilde{G}} := \oplus_{i \geq 0} \tilde{H}_i$ eine Poincarédualitätsalgebra ist. ■

Lemma 4.15 *Es seien $\tilde{\varrho} : G \hookrightarrow GL(M)$ eine Hochhebung einer Darstellung $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ über $\mathbb{F}$ und $\hat{\varrho} : G \hookrightarrow GL(W)$ eine Erweiterung von ϱ auf den Körper $\mathbb{K}$ der Charakteristik 0. Sei $\boldsymbol{A}[M]_{\tilde{G}}$ eine Poincarédualitätsalgebra, dann ist auch $\mathbb{K}[W]_{\hat{G}}$ eine Poincarédualitätsalgebra.*

Zur Erinnerung : Sei $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Für $\operatorname{Char} \mathbb{F} = 0$ gilt
$\mathbb{F}[V]_G$ ist genau dann eine Poincarédualitätsalgebra, wenn $\mathbb{F}[V]^G$ eine Polynomalgebra ist.

Satz 4.16 *Es seien $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$ mit $n = \dim_{\mathbb{F}}(V)$ und $\hat{\varrho} : G \hookrightarrow GL(W)$ eine Erweiterung von ϱ auf den Körper $\mathbb{K}$ der Charakteristik 0.*
Sei $\mathbb{K}[W]^{\hat{G}} = \mathbb{K}[f_1, \cdots, f_n]$ eine Polynomalgebra, die durch die algebraisch unabhängigen invarianten Polynome $f_1, f_2, \cdots, f_n$ erzeugt wird, dann ist $\mathbb{F}[V]^G$ auch eine Polynomalgebra.

Beweis:

1. Behauptung : $\boldsymbol{A}[M]^{\tilde{G}}$ ist eine Polynomalgebra .
   Es wurde schon gezeigt, daß der Isomorphismus $\mathbb{K} \otimes \boldsymbol{A}[M]^{\tilde{G}} \longrightarrow \mathbb{K}[W]^{\hat{G}}$ gilt. Für jeden Erzeuger $f_i \in \mathbb{K}[W]^{\hat{G}}, i = 1, 2, \cdots, n$, gibt es ein Polynom $\tilde{f}_i$ aus $\boldsymbol{A}[M]^{\tilde{G}}$, so daß $f_i = a_i \tilde{f}_i$ für ein passendes $a_i \in \mathbb{K}$ gilt. Daraus folgt : $\mathbb{K} \otimes \boldsymbol{A}[\tilde{f}_1, \cdots, \tilde{f}_n] \cong \mathbb{K}[W]^{\hat{G}} \cong \mathbb{K} \otimes \boldsymbol{A}[M]^{\tilde{G}}$ und $\boldsymbol{A}[\tilde{f}_1, \cdots, \tilde{f}_n] \hookrightarrow \boldsymbol{A}[M]^{\tilde{G}}$ ist ein Monomorphismus. Setzen wir nun $d_i = \deg(f_i)$, für alle i. Aus den Gleichungen der Poincaré-Reihen

$$\begin{aligned}
P(\mathbb{K}[W]^{\hat{G}}, t) &= P(\boldsymbol{A}[M]^{\tilde{G}}, t) = P(\boldsymbol{A}[\tilde{f}_1, \cdots, \tilde{f}_n], t) \text{ , und} \\
\deg(\mathbb{K}[W]^{\hat{G}}) &= \frac{1}{\mid \hat{G} \mid} = \frac{1}{d_1 \cdot \ldots \cdot d_n} \\
&= (1-t)^n P(\boldsymbol{A}[\tilde{f}_1, \cdots, \tilde{f}_n], t)|_{t=1} \\
&= (1-t)^n P(\boldsymbol{A}[M]^{\tilde{G}}, t)|_{t=1} \\
&= \deg(\boldsymbol{A}[M]^{\tilde{G}}) = \frac{1}{\mid \tilde{G} \mid}
\end{aligned}$$

   erhalten wir $\mid \hat{G} \mid = d_1 \cdot \ldots \cdot d_n = \mid \tilde{G} \mid$. Da $f_1, \cdots, f_n$ algebraisch unabhängig über $\mathbb{K}$ sind, sind $\tilde{f}_1, \cdots, \tilde{f}_n$ algebraisch unabhängig über $\boldsymbol{A}$. Daher folgt aus Proposition (1.9) $\boldsymbol{A}[M]^{\tilde{G}} \cong \boldsymbol{A}[\tilde{f}_1, \cdots, \tilde{f}_n]$.

2. Behauptung : $\mathbb{F}[V]^G$ ist eine Polynomalgebra.
   Wir wenden den Isomorphismus an :

$$\mathbb{F} \otimes \boldsymbol{A}[\tilde{f}_1, \cdots, \tilde{f}n] \cong \mathbb{F} \otimes \boldsymbol{A}[M]^{\tilde{G}} \cong \mathbb{F}[V]^G.$$

■

In diesem Abschnitt haben wir uns bis jetzt nur mit vollkommenen Körpern von positiver Charakteristik beschäftigt. In der Tat ist das obige Resultat aber auch gültig für einen beliebigen Körper der positiven Charakteristik. Denn : Für einen Körper $\mathbb{F}$ der Charakteristik $\neq 0$, der nicht notwendig ein vollkommener Körper ist, finden wir einen lokalen Ring der Charakteristik 0, der ein Unterring des Witt-Rings $W(\mathbb{F})$ von $\mathbb{F}$ ist, so daß sein Restklassenkörper gerade der gegebene Körper $\mathbb{F}$ ist. Eine ausführliche Beschreibung dafür ist in [20]

gegeben. So existiert für eine Darstellung $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ einer endlichen Gruppe G über einem Körper $\mathbb{F}$ mit $\mid G \mid \in \mathbb{F}^{\times}$ (bis auf Konjugation) genau eine Hochhebung auf diesen lokalen Ring. Damit haben wir den folgenden Satz bewiesen.

Satz 4.17 *Sei $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$ und $\mid G \mid \in \mathbb{F}^{\times}$. Dann sind die folgenden Aussagen äquivalent :*

1. *$\mathbb{F}[V]^G$ ist eine Polynomalgebra.*
2. *$\mathbb{F}[V]_G$ ist eine Poincarédualitätsalgebra.*

5 Die reguläre Darstellung

Es sei $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G über einem Körper $\mathbb{F}$. Unter der **regulären Darstellung** von G wird ein $\mathbb{F}(G)$-Modul M mit einer $\mathbb{F}$-Basis $\{ \ g \cdot m \ \mid \ g \in G \ \}$ für ein Element $m \in M$ verstanden. Wir bezeichnen die reguläre Darstellung von G mit $\mathrm{Reg}_{\mathbb{F}}(G)$. In diesem Abschnitt diskutieren wir die Beziehung zwischen dem Koinvariantenring $\mathbb{F}[V]_G$ und der regulären Darstellung $\mathrm{Reg}_{\mathbb{F}}(G)$.

Satz 5.1 *(C. Chevalley [7][22] S. 220) Es seien $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ eine Darstellung einer endlichen Gruppe G und $\mathbb{F}[V]^G$ eine Polynomalgebra. Sei $\mid G \mid \in \mathbb{F}^{\times}$, dann ist $\mathbb{F}[V]_G = Reg_{\mathbb{F}}(G)$.*

Im modularen Fall (das heißt $(\mathrm{Char}\,\mathbb{F}, \mid G \mid) \neq 1$) ist Satz (5.1) falsch. Denn sonst wäre die triviale 1-dimensionale Darstellung $\mathbb{F} \subseteq \mathbb{F}[V]_G$ ein projektiver $\mathbb{F}(G)$-Modul. Wird die Gruppenalgebra $\mathbb{F}(G)$ also in ihre irreduziblen Komponenten zerlegt, so steht das im Widerspruch zum Satz von Maschke ([12]). Aber wir können den Satz(5.1) auf die sogenannte Grothendieck-Gruppe übertragen.

Definition 5.2 *Die* **Grothendieck-Gruppe** *von endlich erzeugten $\mathbb{F}(G)$-Moduln, bezeichnet mit $R_{\mathbb{F}}(G)$, ist die abelsche Gruppe mit Isomorphieklassen von endlich erzeugten $\mathbb{F}(G)$-Moduln als Gruppenelementen, bezeichnet mit $[-]$. Wir setzen $S_{\mathbb{F}}(G)$ als die Teilmenge von $R_{\mathbb{F}}(G)$, die aus Isomorphieklassen aller irreduziblen $\mathbb{F}(G)$-Moduln besteht.*

Ein Element $g \in G$ heißt p-**regulär**, wenn die Ordnung von g prim zu p ist. Die Menge aller p-regulären Elemente von G wird mit G_{reg} bezeichnet. Dabei soll die Primzahl p die Körpercharakteristik sein. Die Elemente aus G_{reg} sind deshalb diagonalisierbar. G_{reg} ist im Allgemein keine Untergruppe von G.
Es seien nun $\lambda_1(g), \cdots, \lambda_m(g)$ die Eigenwerte von $g \in G_{reg}$.

Definition 5.3 *Sei $\mathbb{K}$ ein Zerfällungskörper für G (das heißt, jeder irreduzible $\mathbb{K}(G)$-Modul ist absolut irreduzibel). Für einen $\mathbb{F}(G)$-Modul M mit $\dim_{\mathbb{F}}(M) = m$ definieren wir seinen* **modularen Charakter** *χ_M durch die Funktion*

$$\begin{aligned} \chi_M : G_{reg} &\longrightarrow \mathbb{K}\,, \\ g &\mapsto \chi_M(g) := \sum_{i=1}^{m} \lambda_i(g) = Spur(g). \end{aligned}$$

Eigenschaften 5.4 *([21] S. 147) Der modulare Charakter* $\chi_M : G_{reg} \longrightarrow \mathbb{K}$ *hat unmittelbar folgende Eigenschaften :*

1. $\chi_M(1) = \dim_{\mathbb{F}}(M)$.
2. χ_M *ist eine Klassenfunktion auf* G_{reg}*, das heißt,* $\chi_M(\sigma g \sigma^{-1}) = \chi_M(g)$ *für* $g \in G_{reg}$ *und* $\sigma \in G$.
3. *Für endlich erzeugte* $\mathbb{F}(G)$*-Moduln* M, N *und ihre modularen Charaktere* χ_M, χ_N *setzen wir* $\langle \chi_M, \chi_N \rangle := \frac{1}{|G|} \sum_{g \in G_{reg}} \chi_N(g^{-1}) \chi_M(g)$ *und* $\langle M, N \rangle := \dim_{\mathbb{F}}(Hom_{\mathbb{F}(G)}(M, N))$*. Es seien* F *ein endlich erzeugter* $\mathbb{F}(G)$*-Modul und* P *ein endlich erzeugter projektiver* $\mathbb{F}(G)$*-Modul. Dann gilt*
$$\langle F, P \rangle = \langle \chi_F, \chi_P \rangle.$$
4. *Es seien* $E_1 \neq E_2$ *zwei irreduzible* $\mathbb{F}(G)$*-Moduln mit projektiven Hüllen* P_{E_1}, P_{E_2}*. Dann gilt die Orthogonalitätsrelation*
$$\langle P_{E_i}, E_j \rangle = \delta_{ij} \quad , \quad i, j = 1, 2.$$
Daraus erhalten wir $\langle M, E_i \rangle = \langle P_{E_i}, M \rangle$ *für einen beliebigen endlich erzeugten* $\mathbb{F}(G)$*-Modul* M.

Bemerkung 5.5 *Jede irreduzible Isomorphieklasse* $[E]$ *in* $S_{\mathbb{F}}(G)$ *korrespondiert mit einem modularen Charakter* χ_E*, der* **irreduzibler modularer Charakter** *von* G *heißt.*

Satz 5.6 *(Brauer)([21] S. 149) Es sei* $\mathbb{K}$ *ein Zerfällungskörper von* G*. Die irreduziblen modularen Charaktere* χ_E *,* $[E] \in S_{\mathbb{F}}(G)$*, bilden eine Basis des* $\mathbb{K}$*-Vektorraums aller Klassenfunktionen von* G_{reg} *auf* $\mathbb{K}$.

Nun betrachten wir im Rest dieses Abschnitts einen Körper $\mathbb{F}$ von positiver Charakteristik p, welcher einer Zerfällungskörper für G ist. Der Grund dafür ist folgender : Wenn ein Erweiterungskörper $\mathbb{K}$ von $\mathbb{F}$ ein Zerfällungskörper für G ist und M ein endlich erzeugter (projektiver) $\mathbb{F}(G)$-Modul ist, dann ist die Erweiterung $M \otimes_{\mathbb{F}} \mathbb{K}$ ein endlich erzeugter (projektiver) $\mathbb{K}(G)$-Modul und $\dim_{\mathbb{F}}(M) = \dim_{\mathbb{K}}(M \otimes_{\mathbb{F}} \mathbb{K})$.

Satz 5.7 *([16]) Es sei* $\varrho : G \hookrightarrow GL(n, \mathbb{F})$ *eine Darstellung einer endlichen Gruppe* G *und* $\operatorname{Char} \mathbb{F} = p \neq 0$*. Sei* $\mathbb{F}[V]^G = \mathbb{F}[f_1, \cdots, f_n]$ *eine Polynomalgebra mit Erzeugern* $f_1, \cdots, f_n$ *der Grade* $d_1, \cdots, d_n$*. Dann gilt*
$$[\mathbb{F}[V]_G] = [Reg_{\mathbb{F}}(G)] \quad \text{in } R_{\mathbb{F}}(G).$$

Beweis: Der Satz von Brauer besagt, daß alle modularen Charaktere χ_M , $[M] \in R_{\mathbb{F}}(G)$, in direkte Summe von irreduziblen modularen Charakteren χ_{E_i} , $[E_i] \in S_{\mathbb{F}}(G)$ zerlegt werden können, nämlich

$$\chi_M = \bigoplus_{[E_i]\in S_{\mathbb{F}}(G)} n_i \cdot \chi_{E_i}(1) \cdot \chi_{E_i} \tag{16}$$

$$= \bigoplus_{[E_i]\in S_{\mathbb{F}}(G)} n_i \cdot \dim_{\mathbb{F}}(E_i) \cdot \chi_{E_i}, \tag{17}$$

wobei $n_i \cdot \chi_{E_i}(1)$ die Multiplizität von E_i ist. Ferner gilt für $[M] \in R_{\mathbb{F}}(G)$

$$[M] = \bigoplus_{[E_i]\in S_{\mathbb{F}}(G)} n_i \chi_{E_i}(1) \cdot [E_i].$$

Aus der Definition von regulären Darstellungen geht leicht hervor, daß

$$[\mathrm{Reg}_{\mathbb{F}}(G)] = \bigoplus_{[E_i]\in S_{\mathbb{F}}(G)} \chi_{E_i}(1) \cdot [E_i]. \tag{18}$$

Es bleibt noch zu zeigen, daß $[\mathbb{F}[V]_G]$ auch eine solche Zerlegung besitzt.

Es seien $[M] = \bigoplus_{i\geq o} [M_i]$ ein graduierter endlich erzeugter $\mathbb{F}(G)$-Modul in $R_{\mathbb{F}}(G)$ und $[E] \in S_{\mathbb{F}}(G)$. Die **$E$-isotypische Komponente** von $[M]$, bezeichnet mit $[M]|_E$, ist eine direkte Summe der zu E isomorphen irreduziblen Komponenten von $[M]$. Es folgt dann unmittelbar

$$[M] = \bigoplus_{[E]\in S_{\mathbb{F}}(G)} [M]|_E. \tag{19}$$

Definition 5.8 *Es seien $S_{\mathbb{F}}(G) = \{ [E_1], \cdots, [E_k] \}$, P_{E_i} die projektive Hülle von E_i , $1 \leq i \leq k$, und $[M] = \bigoplus_{i\geq 0} [M_i]$ ein graduierter endlich erzeugter $\mathbb{F}(G)$-Modul in $R_{\mathbb{F}}(G)$, so daß $[M_i] = \langle \chi_{P_{E_1}}, \chi_{M_i} \rangle [E_1] \oplus \cdots \oplus \langle \chi_{P_{E_k}}, \chi_{M_i} \rangle [E_k]$, für alle i, ist. Die* **modulare Poincaré-Reihe** *von $[M]$ bzw. $[M]|_E$, $[E] \in S_{\mathbb{F}}(G)$, wird wie folgt definiert :*

$$P([M], t) := \sum_{i=0}^{\infty} \sum_j \langle \chi_{P_{E_j}}, \chi_{M_i} \rangle \cdot \dim_{\mathbb{F}}(E_j) \cdot t^i \tag{20}$$

$$= \sum_{i=0}^{\infty} \sum_j \langle \chi_{P_{E_j}}, \chi_{M_i} \rangle \cdot \chi_{E_j}(1) \cdot t^i. \tag{21}$$

$$P([M]|_E, t) := \sum_{i=0}^{\infty} \sum_j \langle \chi_{P_{E_j}}, \chi_{M_i} \rangle \cdot \langle \chi_{E_j}, \chi_E \rangle \cdot t^i \tag{22}$$

$$= \sum_{i=0}^{\infty} \sum_j \langle \chi_{P_{E_j}}, \chi_{M_i} \rangle \cdot t^i. \tag{23}$$

Mit der Eigenschaft (5.4)(3) erhalten wir für einen irreduzible $\mathbb{F}(G)$-Modul in $S_{\mathbb{F}}(G)$

$$\begin{aligned} P([M]|_E, t) &= \frac{1}{\mid G \mid} \sum_{g \in G_{reg}} \chi_{P_E}(g^{-1}) \cdot \sum_{i=o}^{\infty} \chi_{M_i}(g) \cdot t^i && (24) \\ &= \frac{1}{\mid G \mid} \sum_{g \in G_{reg}} \chi_{P_E}(g^{-1}) \cdot \frac{1}{\det(1 - g^{-1}t)}. && (25) \end{aligned}$$

Nun setzen wir $M = \mathbb{F}[V]_G$. Für den polynomialen Invariantenring $\mathbb{F}[V]^G \cong \mathbb{F}[f_1, \cdots, f_n]$ mit $d_i = \deg(f_i) \neq 0$ gilt dann für jeden irreduzible $\mathbb{F}(G)$-Modul E in $S_{\mathbb{F}}(G)$

$$\begin{aligned} P([\mathbb{F}[V]_G]|_E, t) &= \frac{P([\mathbb{F}[V]]|_E, t)}{P(\mathbb{F}[V]^G, t)} && (26) \\ &= \frac{1}{\mid G \mid} \prod_{i=1}^{n} (1 - t^{d_i}) \sum_{g \in G_{reg}} \chi_{P_E}(g^{-1}) \frac{1}{\det(1 - g^{-1}t)}, && (27) \end{aligned}$$

also

$$\begin{aligned} P([\mathbb{F}[V]_G]|_E, t)\big|_{t=1} &= \frac{1}{\mid G \mid} \chi_{P_E}(1) \prod_{i=1}^{n} d_i \\ &= 1 \cdot \chi_{P_E}(1). \end{aligned}$$

Weiter gilt

$$\begin{aligned} [\mathbb{F}[V]_G] &= \bigoplus_{[E] \in S_{\mathbb{F}}(G)} [\mathbb{F}[V]_G]|_E \\ &= \bigoplus_{[E] \in S_{\mathbb{F}}(G)} \chi_{P_E}(1) \cdot [E]. \end{aligned}$$

Somit ist Satz (5.7) bewiesen. ■

Literatur

[1] S. Balcerzyk, T. Józefiak, *Commutative Rings : dimension, multiplicity and homological methods*, Polish Scientific Publishers, Warsaw, 1989.

[2] H. Bass, *On the ubiquity of Gorensteinrings*, Math. Zeitschr. 82(1963), 8-28.

[3] D.J. Benson, *Polynomial Invariants of Finite Groups*, Cambridge Univ. Press, London, 1993.

[4] K.S. Brown, *Cohomology of Groups*, GTM 87, Springer-Verlag, New York, 1982.

[5] R. Brüske, F. Ischebeck, F. Vogel, *Kommutative Algebra*, BI-Wissenschaftsverlag, Mannheim, Wien, Zürich, 1989.

[6] W. Bruns, J. Herzog, *Cohen-Macaulay rings*, Cambridge University Press, 1996.

[7] C. Chevalley, *Invariantens of Finite Groups Generated by Reflections*, Amer. J. Math. 77(1955), 778-782.

[8] A. Clark, J. Ewing, *The Realization of Polynomial Algebras as Cohomology Rings*, Pac. J. Math. 50(1974), 425-434.

[9] L. Evens, *The Cohomology of Groups*, Clarendon Press, Oxford, New York, Tokyo, 1991.

[10] H. Hasse, *Zahlentheorie*, Akademie-Verlag, Berlin, 1963.

[11] P.J. Hilton, U. Stammbach, *A Course in Homological Algebra*, GTM 4, Springer-Verlag, New York, 1997.

[12] N. Jacobson, *Basic Algebra II*, W.H. Freeman and Compang, New York, 1989.

[13] E. Kunz, *Einführung in die kommutative Algebra und algebraische Geometrie*, Vieweg-Verlag, Braunschweig, Wiesbaden, 1980.

[14] R. Kane, *Poincaré Duality and the Ring of Coinvariants*, Canad. Math. Bull. 37(1)(1994), 82-88.

[15] H. Matsumura, *Commutative ring theory*, Cambridge studies in advanced mathematics 8, Cambridge, 1994.

[16] S.A. Mitchell, *Finite Complexes with $A(n)$-Free Cohomology*, Topology 24(2)(1985), 227-248.

[17] F. Neumann, M.D. Neusel, L. Smith, *Rings of Generalized and Stable Invariants for Pseudoreflections and Pseudoreflection Groups*, J. of Algebra 182(1996), 85-122.

[18] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. 77(1916), 89-92.

[19] E. Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. v. d. Ges. d. Wiss. zu Göttingen (1926), 28-35.

[20] C. Schoeller, *Groupes Affines, Commutatifs, Unipotents sur un Corps Non Parfait*, Bull. Soc. math. France 100(1972), 241-300.

[21] J.-P. Serre, *Linear Representations of Finite Groups*, GTM 42, Springer-Verlag, New York, 1977.

[22] L. Smith, *Polynomial Invariants of Finite Groups*, A.K. Peter-Verlag, Wellesley, Massachusetts, 1995.

[23] L. Smith, *Some Rings of Invariants that are Cohen-Macaulay*, Canad. Math. Bull. 39(2)(1996), 238-240.

[24] L. Smith, *On a Theorem of R. Steinberg*, AG-Invariantentheorie, Preprint 2000, erscheint in PAMS, April 2003.

[25] T.A. Springer, *Invariant Theory*, LNM 585, Springer-Verlag, Heidelberg, Berlin, 1977.

[26] R.P. Stanley, *Relative Invariants of Finite Groups*, J. of Alg. 49(1977), 134-148.

[27] R.P. Stanley, *Invariants of Finite Groups and their Applications to Combinatorics*, Bull. Amer. Math. Soc. 1(3)(1979), 475-511.

[28] R. Steinberg, *Differental Equations Invariant under Finite Reflection Groups*, Trans. Amer. Math. Soc. 112(1964), 392-400.

[29] W.V. Vasconcelos, *Ideals Generated by R-Sequences*, J. Algebra 6(1967), 309-316.

[30] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grade p^n*, J. reine angw. Math. 176(1936), 126-140.

Danksagung

Zuerst und ganz besonders danke ich meinem Doktorvater Prof. Dr. L. Smith für sein Interesse und die Umsicht, mit denen er meine Arbeit von den ersten unsicheren Anfängen bis zur Fertigstellung unterstützt hat.
Für die spontane Bereitschaft, die Aufgabe der Korreferentin zu übernehmen, und ihre hilfreichen Anmerkungen möchte ich Prof. Dr. I. Kersten herzlich Dank sagen.
Für die unschätzbare Hilfe in den Bereichen Computer allgemein und $\mathcal{L}$aTeX insbesondere danke ich Herrn Lidong Xia und Herrn Yue-Lin Huang.
Den aufopferungsvollen Korrekturlesern Frau Bianca Gramann, Frau Kathrin Kuhnigk und Herrn Cyril Franke bin ich zutiefst zu Dank verpflichtet.
Für die unermüdlichen Beweise ihrer Freundschaft danke ich besonders Frau Bianca Gramann.
Allen übrigen Mitmenschen - namentlich Gerda, Matthias, Jane - möchte ich für ihre Toleranz in der Endphase danken.

Lebenslauf

30. Juni 63	in Tainan/Taiwan geboren, Staatsangehörigkeit Taiwan (Republic of China)
Juli 82	Abschluß an der Mädchenschule Chang Jung in Tainan/Taiwan
Juni 88	Bachelor an die National Cheng Kung Universität in Tainan/Taiwan für die Fächer angewandte Mathematik
Nov. 97	Diplomprüfung Mathematik an der Universität Göttingen
1998 - 99	wissenschaftliche Assistentin am mathematischen Institut der Akademie Sinica in Taipei/Taiwan
Seit 1998	Promotion