Technische Universität München
Zentrum Mathematik

Über die Tiefe von Invariantenringen unendlicher Gruppen

Martin Wilhelm Kohls

Vollständiger Abdruck der von der Fakultät für Mathematik der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktors der Naturwissenschaften (Dr. rer. nat.)

genehmigten Dissertation.

Vorsitzender:		Univ.-Prof. Dr. Peter Rentrop
Prüfer der Dissertation:	1.	Univ.-Prof. Dr. Gregor Kemper
	2.	Prof. Dr. Harm Derksen University of Michigan, USA (schriftliche Beurteilung)
	3.	Univ.-Prof. Dr. Werner Heise (mündliche Prüfung)

Die Dissertation wurde am 15.05.2007 bei der Technischen Universität eingereicht und durch die Fakultät für Mathematik am 17.10.2007 angenommen.

Inhaltsverzeichnis

Abstract

The topic of this thesis is the depth of invariant rings of infinite groups. The main result is a lower bound for the Cohen-Macaulay defect

$$\operatorname{cmdef} K[V]^G := \dim K[V]^G - \operatorname{depth} K[V]^G$$

of the invariant ring $K[V]^G$ of a rational representation V (also called a G-module) of a reductive group G. With K we denote an algebraically closed field. So far, such bounds have only been known for finite groups. In particular, we will show the following result:

For each reductive group G that is not linearly reductive, there exists a faithful rational representation V of G such that

$$\operatorname{cmdef} K\left[\bigoplus_{k=1}^{n} V\right]^G \geq n-2 \quad \text{for all } n \in \mathbb{N},$$

in particular we have

$$\lim_{n\to\infty} \operatorname{cmdef} K\left[\bigoplus_{k=1}^{n} V\right]^G = \infty.$$

In the proof, such a G-module V will be given explicitely. We show a similar result for additive and unipotent groups of positive characteristic (these groups are not reductive).

In another chapter, we concentrate on the group SL_2, and refining our methods that lead to the above result, we receive the following:

Let $\langle X, Y\rangle$ denote the natural representation of the group SL_2, $\operatorname{char} K = p > 0$. Let further denote $\langle X^p, Y^p\rangle$ the submodule of the pth symmetric power $S^p(\langle X, Y\rangle)$ spanned by the pth power of the variables. Then we have

$$\operatorname{cmdef} K\left[\langle X^p, Y^p\rangle \oplus \bigoplus_{i=1}^{k} \langle X, Y\rangle\right]^{\mathrm{SL}_2} \geq k-3.$$

It is worth noting that the underlying module is self-dual and completely reducible (as a direct sum of self-dual, irreducible modules).

In the final chapter, we develop an algorithm to compute these special invariant rings. With an implementation in Magma, this allowed us to compute the Cohen-Macaulay defect explicitely for the cases $(p,k) = (2,4), (2,5), (3,4)$ to $1, 2, 1$, so the lower bound is sharp in these cases.

This thesis also contains a chapter on the cohomolgy of groups, chapter 2, which is almost independent of the others. In this chapter we investigate annihilators of n-cocycles of infinite groups. In particular, we show the following: Let G be any (possibly infinite) group, $d_0 : KG \to K$ the augmentation map (which sends each $\sigma \in G$ to $1 \in K$). Then for each KG-module V (not necessary finite-dimensional) and each $g \in H^n(G, V)$ we have $d_0 \cdot g = 0 \in H^n(G, \operatorname{Hom}_K(KG, V))$.

Einleitung

Die Tiefe von Invarianten *endlicher* Gruppen ist ein in den letzten 25 Jahren viel beachtetes und gut untersuchtes Gebiet. Als eine (sicher unvollständige) Liste von Arbeiten zu diesem Thema seien hier [5, 9, 15, 17, 18, 19, 21, 25, 30, 32, 34, 35, 42, 43, 49, 57, 58] genannt. Als bahnbrechend muss hier sicher die Arbeit von Ellingsrud und Skjelbred [15] hervorgehoben werden.

Dagegen ist die vorliegende Dissertation die erste Arbeit, die sich mit der Tiefe von Invariantenringen *unendlicher* (genauer: zusammenhängender) Gruppen befasst. Genauer betrachten wir folgende Situation: K ist ein algebraisch abgeschlossener Körper und G eine über K definierte lineare algebraische Gruppe, die linear und rational auf einem endlich-dimensionalen Vektorraum V operiert. Dadurch wird auch eine Operation auf dem Ring der Polynomfunktionen $K[V]$ auf V induziert, und die Menge aller invarianten Polynomfunktionen bezeichnen wir mit $K[V]^G$. Wir interessieren uns dabei nur für den Fall, dass $K[V]^G$ endlich erzeugt ist (z.B. wenn G eine reduktive Gruppe ist), es sich also um eine graduierte affine Algebra handelt. Wichtige Kenngrößen einer solchen Algebra R sind die *Tiefe* $\operatorname{depth} R$, die *Dimension* $\dim R$ und der Cohen-Macaulay-Defekt $\operatorname{cmdef} R := \dim R - \operatorname{depth} R$, welcher stets größer gleich 0 ist. Je größer der Cohen-Macaulay-Defekt, desto „komplizierter“ ist die Struktur von R. Ringe mit $\operatorname{cmdef} R = 0$ (die „schönsten“ also) heißen *Cohen-Macaulay*. Der Satz von Hochster und Roberts besagt, dass für *linear reduktive* Gruppen G und jeden G-Modul V der Invariantenring $K[V]^G$ stets Cohen-Macaulay ist, also stets $\operatorname{cmdef} K[V]^G = 0$ gilt. Ziel dieser Arbeit ist es, *untere* Schranken für $\operatorname{cmdef} K[V]^G$ zu finden (da $\dim K[V]^G$ meist bekannt, ist dies äquivalent zum finden oberer Schranken für die Tiefe $\operatorname{depth} K[V]^G$), wenn G nicht linear reduktiv ist. Das Ergebnis ist unser (technischer) Hauptsatz 3.6. Ein Großteil der restlichen Arbeit beschäftigt sich dann mit der expliziten Konstruktion von G-Moduln V, auf die der Hauptsatz anwendbar ist. Als „griffiges“ Ergebnis erhalten wir (siehe Korollar 3.9, Bemerkung 3.10 und Abschnitt 4.2):

Für jede reduktive, nicht linear reduktive Gruppe G existiert ein treuer G-Modul V (den wir *explizit* angeben können) mit

$$\operatorname{cmdef} K\left[\bigoplus_{k=1}^{n} V\right]^G \geq n-2 \quad \text{für alle } n \in \mathbb{N},$$

insbesondere also

$$\lim_{n\to\infty} \operatorname{cmdef} K\left[\bigoplus_{k=1}^{n} V\right]^G = \infty.$$

Dies ist eine Verschärfung des Resultats von Kemper [33], welches besagt, dass für jede reduktive, nicht linear reduktive Gruppe G ein G-Modul V mit $\operatorname{cmdef} K[V]^G > 0$ existiert.

Die nach diesem allgemeinen Resultat konstruierten G-Moduln V haben eine relativ große Dimension und komplizierte Struktur. In Satz 4.28, dem zweiten Hauptresultat dieser Arbeit, wird eine sehr einfach gebaute Folge von SL_2- bzw. $\mathbb{G}_a$-Moduln angegeben,

deren Cohen-Macaulay-Defekt der zugehörigen Invariantenringe gegen unendlich geht. Unter anderem zeigen wir dort (Satz 4.28):

Ist $\langle X, Y\rangle$ die natürliche Darstellung der SL_2, $\operatorname{char} K = p > 0$, so gilt

$$\operatorname{cmdef} K\left[\langle X^p, Y^p\rangle \oplus \bigoplus_{i=1}^{k}\langle X, Y\rangle\right]^{\mathrm{SL}_2} \geq k - 3.$$

Alle hier dargestellten Ergebnisse spielen sich in positiver Charakteristik ab, denn in Charakteristik 0 ist jede reduktive Gruppe auch linear reduktiv, und damit Invariantenringe reduktiver Gruppen stets Cohen-Macaulay. Bevor ich mich dem Thema der vorliegenden Arbeit gewidmet habe, habe ich ein halbes Jahr lang ohne nennenswertes Ergebnis versucht, einen nicht Cohen-Macaulay Invariantenring in Charakteristik 0 zu konstruieren. Dabei war mein Ansatz hauptsächlich experimenteller Natur, d.h. ich habe für verschiedene Darstellungen V nicht reduktiver Gruppen G den Invariantenring heuristisch auf die Cohen-Macaulay-Eigenschaft getestet (mit Hilfe von Magma). Zwar kann man auch für nicht reduktive Gruppen mit Lemma 3.2 leicht drei Elemente $a_1, a_2, a_3 \in K[V]^G$ konstruieren, die als Annullatoren eines Kozyklus $g \in H^1(G, K[V])$ keine reguläre Sequenz in $K[V]^G$ sind und ein phsop in $K[V]$ bilden. (Dies ging sogar leichter als für reduktive Gruppen, da die Kozyklen einfacher waren). Doch leider ist für reduktive Gruppen Lemma 1.55 falsch (dies ist das Haupthindernis), also hat man kein a priori Kriterium für das Vorliegen eines phsops im Invariantenring. Um zu testen, ob nun doch ein phsop vorliegt, bleibt also nichts übrig, als (heuristisch) Generatoren für den Invariantenring $K[V]^G$ und deren Relationenideal zu berechnen, und so den Test im Restklassenring eines Polynomrings mit Magma durchzuführen.

Da kein Algorithmus bekannt ist, um für nicht reduktive Gruppen den Invariantenring zu berechnen, habe ich einfach jeweils genügend viele Invarianten berechnet, so dass ich von der davon erzeugten Unteralgebra A vermutete, dass sie gleich $K[V]^G$ ist. Dabei ist im Allgemeinen nicht einmal garantiert, dass $K[V]^G$ überhaupt endlich erzeugt ist. In den Fällen, in denen ich das Relationenideal von A berechnen konnte, hat sich A immer als Cohen-Macaulay herausgestellt. Insbesondere haben die drei Annullatoren eines Kozyklus kein phsop in A gebildet.

Für einige Darstellungen, die mir als „heisse“ Kandidaten vorkamen, lies sich das Relationenideal von A nicht in akzeptabler Zeit berechnen, so dass ich hier keine Aussage machen konnte.

Aufbau der Arbeit

Abschnitt 1 gibt die benötigten Grundlagen wieder. Obwohl sich hier keine wesentlich neuen Resultate finden, ist der Abschnitt sehr ausführlich gehalten. Zum einen sollte die Darstellung natürlich so selbsttragend wie möglich sein, zum anderen werden etwa die Resultate, die wir für noethersche *graduierte* Ringe benötigen, in der Literatur (etwa Eisenbud [14] oder Bruns und Herzog [6]) fast ausschliesslich für noethersche *lokale* Ringe formuliert. Die dortigen Beweise gehen zwar meist mit kleinen Modifikationen auch für den graduierten Fall durch, aber um nicht durch „sinngemäßes Zitieren“ eine Lücke entstehen zu lassen habe ich wo nötig einen vollständigen Beweis für den graduierten Fall gegeben.

Hierzu noch eine Bemerkung, die auch für die anderen Abschnitte gilt: Natürlich kann auch diese Arbeit nicht bei Null beginnen. Vorausgesetzt werden die Grundlagen der kommutativen Algebra und der algebraischen Geometrie, wie sie sich etwa in (der ersten Hälfte von) Standardlehrbüchern wie Eisenbud [14] oder Kunz [40] finden. Der Leser sollte also mit Begriffen wie noethersche Ringe und Moduln, Ringerweiterungen und Ganzheit, Lying-over, Going-up und Going-down, Dimension und Höhe, assoziierte Primideale, Gröbner Basen, affine Varietäten und Morphismen etwas anfangen können. Die meisten der hier erwähnten Begriffe werden wir aber zumindest erklären und Referenzen geben. Wenn möglich verweisen wir für die Grundlagen der Theorie der linearen algebraischen Gruppen immer auf die erste Auflage des vergleichsweise elementar gehaltenen Lehrbuchs Springer [59]. Teilweise müssen wir auf dessen tiefer gehende zweite Auflage [60] bzw. auf Humphreys [29] verweisen. Die Grundlagen der „modernen“ (im Gegensatz zur „klassischen“) Invariantentheorie finden sich etwa in Derksen und Kemper [12]. Unter diesen Voraussetzungen sind die Beweise dieser Arbeit vollständig. Ein Leser ohne die genannten Kenntnisse wird zwar nicht jedes Detail auf Korrektheit verifizieren, aber wie ich hoffe doch mit Hilfe der angegebenen Referenzen nachvollziehen können.

Im Unterabschnitt über lineare algebraische Gruppen geben wir ein Kriterium für die lineare Reduktivität von Gruppen, Satz 1.39, welches sich innerhalb eines Beweises von Nagata [45] findet und wenig bekannt zu sein scheint. Wir werden von diesem Kriterium intensiv Gebrauch machen, und geben daher einen (bei den genannten Vorkenntnissen) vollständigen, geglätteten Beweis.

Es folgt eine Einführung in die erste Kohomologie algebraischer Gruppen, welche unser wichtigstes technisches Hilfsmittel darstellt. Wir schliessen mit der Bereitstellung der von uns benötigten Resultate der Invariantentheorie.

Abschnitt 2 hat als wesentliches Ziel, ein Resultat von Kemper über die Annullation von 1-Kozyklen auf n-Kozyklen zu erweitern, siehe Satz 2.28. Insbesondere erhalten wir hieraus, dass die Augmentationsabbildung $KG \to K$ (G eine beliebige, nicht notwendig endliche Gruppe) jeden n-Kozyklus annulliert, Korollar 2.29, was das entsprechende Resultat für endliche Gruppen verallgemeinert.

Dieses Ergebnis steht in dieser Arbeit für sich allein und wird hier nicht mehr verwendet. Daher ist es möglich, dieses Kapitel beim ersten Lesen zu überspringen und nur bei Interesse an dem dargestellten Resultat darauf zurückzukommen. Das Verständnis der restlichen Kapitel wird dabei nicht gestört.

Abschnitt 3 enthält den technischen Hauptsatz, die bereits angesprochene untere Schranke für den Cohen-Macaulay Defekt. Wir vergleichen unser Resultat mit den entsprechenden Ergebnissen für endliche Gruppen.

Im anknüpfenden **Abschnitt 4** fließen die Ergebnisse der vorherigen Abschnitte zusammen, und wir erhalten so explizit Darstellungen, deren Cohen-Macaulay-Defekt der Vektorinvarianten gegen unendlich geht. Wir untersuchen die explizite Konstruktion für einige Fälle konkret und kommen so für diese Fälle noch zu Vereinfachungen. Der Abschnitt schließt mit der bereits erwähnten einfach gebauten Serie von SL_2-Invariantenringen für beliebige Charakteristik $p > 0$, deren Cohen-Macaulay-Defekt gegen unendlich geht.

Im letzten **Abschnitt 5** untersuchen wir die Ringe dieser Serie mit algorithmischen Me-

thoden (mit Hilfe von Magma) genauer. Insbesondere entwickeln wir einen Algorithmus, der in kurzer Rechenzeit und mit wenig Speicherbedarf (hieran scheitert der Standardalgorithmus) Generatoren dieser speziellen Invariantenringe liefert. Für drei Fälle können wir so den Cohen-Macaulay-Defekt exakt bestimmen (wir erhalten als Defekte zweimal 1 und einmal 2).

Dank

An dieser Stelle möchte ich mich ganz herzlich bei meinem Betreuer, Prof. Dr. Gregor Kemper bedanken. Zum einen weil er es immer geschafft hat, mich wenn nötig für eine bestimmte Richtung zu motivieren, zum anderen aber auch, weil er mir immer genügend Freiraum gelassen hat, um eigenverantwortlich zu forschen.

Bei Dr. Frank Himstedt bedanke ich mich für die immer kompetente Hilfe bei meinen Fragen zur Darstellungstheorie von Gruppen.

Weiter bedanke ich mich beim Graduiertenkolleg „Angewandte Algorithmische Mathematik“, von dem ich im ersten Jahr dieser Arbeit finanziell unterstützt wurde.

Zuguterletzt gilt mein Dank den restlichen Mitgliedern der Lehr- und Forschungseinheit M11 - für die vielen Kaffee-Pausen.

1 Grundlagen der kommutativen Algebra und der Invariantentheorie

Wir geben zunächst die benötigten Grundlagen und Begriffe der kommutativen Algebra und Invariantentheorie wieder. Dabei soll auch jeweils der algorithmische Aspekt berücksichtigt werden.

Standardvoraussetzung. In dieser Arbeit bezeichnen wir mit K stets einen algebraisch abgeschlossenen Körper der Charakteristik $p \geq 0$.

1.1 Graduierte affine Algebren

Eine *K-Algebra* ist (in dieser Arbeit, es gibt inkompatible Definitionen) ein K-Vektorraum R, der zusätzlich ein kommutativer Ring mit $1 \neq 0$ ist, so dass stets $\lambda(ab) = (\lambda a)b = a(\lambda b)$ für $\lambda \in K, a, b \in R$ gelten (insbesondere ist $K \cong K \cdot 1 \subseteq R$). R heißt *graduiert*, falls es eine direkte Zerlegung in Vektorräume $R = \bigoplus_{i=0}^{\infty} R_i$ gibt, wobei zusätzlich $R_i R_j \subseteq R_{i+j}$ für alle $i, j \in \mathbb{N}_0$ gelten soll. Dabei soll in dieser Arbeit dann auch immer $R_0 = K = K \cdot 1$ gelten, d.h. R soll dann zusätzlich *zusammenhängend* sein. Dann ist das Ideal $R_+ := \bigoplus_{i=1}^{\infty} R_i$ wegen $R/R_+ \cong R_0 = K$ maximal, es heißt das *maximale homogene Ideal von R*.

Die Elemente aus $R_i \backslash \{0\}$ heißen *homogen vom Grad i*. In der üblichen Weise ist dann auch eine Gradfunktion deg auf $R \setminus \{0\}$ definiert (oft setzen wir auch $\deg 0 := -\infty$). Ein Ideal $I \trianglelefteq R$ heißt *homogen*, wenn es von homogenen Elementen erzeugt wird, was gleichbedeutend damit ist, dass es mit jedem $f \in I$ auch alle homogenen Komponenten von f enthält. Im wesentlichen interessieren uns in dieser Arbeit nur *affine* (d.h. endlich erzeugte) graduierte Algebren. Dann gibt es homogene Elemente $a_1, \ldots, a_n \in R$ mit $R = K[a_1, \ldots, a_n]$. (Eine zusammenhängende graduierte Algebra ist genau dann affin, wenn sie noethersch ist. In unserem Standardfall für Algebren sind also affin und noethersch synonym.) Man hat dann einen Epimorphismus ϕ vom Polynomring $P = K[X_1, \ldots, X_n]$ auf R, gegeben durch $X_i \mapsto a_i$, welcher bei Verwendung der Graduierung $\deg X_i := \deg a_i$ auf P homogen wird, d.h. homogene Elemente auf homogene Element gleichen Grades (oder die 0) abbildet. Insbesondere ist dann $I := \ker \phi$ ein *homogenes* Ideal in P, das *Relationenideal*, und es gilt $R \cong P/I$. Eine nullteilerfreie, endlich erzeugte K-Algebra heißt ein *K-Bereich*.

Standardvoraussetzung. Wenn nicht anders vermerkt, bezeichnen wir mit R von nun an stets einen zusammenhängenden, graduierten, endlich erzeugten K-Bereich.

Um mit affinen graduierten Algebren rechnen zu können, benötigt man praktisch immer eine solche Darstellung als Restklassenring eines Polynomrings modulo des Relationenideals (außer falls zusätzliche Eigenschaften bekannt sind). Ist R endlich erzeugte Unteralgebra eines Polynomrings, so kann man das Relationenideal I mit Standard-Methoden (Eliminationstheorie) berechnen, siehe etwa Eisenbud [14, Proposition 15.30]. In Magma [4] ist ein solcher Algorithmus bereits implementiert und kann mit dem Befehl `RelationIdeal` aufgerufen werden. Oft scheitert hier bereits das weitere Vorgehen aufgrund der zu langen Rechenzeit.

1.1.1 Dimension, Höhe und Noether-Normalisierung

Sei R eine affine Algebra, $\wp$ ein Primideal von R. Dann ist die *Höhe* von $\wp$, bezeichnet mit $\text{height}(\wp)$, die maximale Länge n einer echt aufsteigenden Kette von Primidealen $\wp_0 \subset \wp_1 \subset \ldots \subset \wp_n$ mit $\wp_n = \wp$. Ist $I \neq R$ ein beliebiges Ideal von R, so ist $\text{height}(I)$ das Minimum der Höhen der I umfassenden Primideale. (Dabei haben echte Ideale in noetherschen Ringen nach dem Krullschen Hauptidealsatz stets endliche Höhe.) Die *Krulldimension* von R ist das Maximum der Höhen aller Primideale von R, d.h. die maximale Länge n einer echt aufsteigenden Kette von Primidealen $\wp_0 \subset \wp_1 \subset \ldots \subset \wp_n$ von R, und wird mit $\dim R$ bezeichnet. Ist R ein K-Bereich, so gilt $\dim R = \text{trdeg}\,\text{Quot}(R)/K$ ([14, Theorem 13.A]). Man setzt $\dim I := \dim R/I$. Zwischen Höhe und Dimension eines Ideals besteht folgende fundamentale Relation:

Proposition 1.1 *Ist R eine affine Algebra und $I \neq R$ ein Ideal, so gilt*

$$\dim R \geq \dim I + \text{height}\, I.$$

Ist R ein affiner Bereich, so gilt sogar Gleichheit.

Beweis. Sei $\wp_0 \supset \wp_1 \supset \ldots \supset \wp_m \supseteq I$ eine Kette von Primidealen von R mit $m = \dim R/I$. Offenbar gilt dann $\dim R \geq m + \text{height}\, \wp_m \geq \dim R/I + \text{height}\, I$. Für das Gleichheitszeichen im Fall eines affinen Bereichs siehe [14, Corollary 13.4]. □

Ist R ein Polynomring, so lässt sich $\dim I$ mit Gröbner-Basis Methoden berechnen [12, Algorithm 1.2.4]. Insbesondere lässt sich die Dimension eines affinen Rings berechnen, wenn das Relationenideal bekannt ist. Zentral ist der folgende

Satz 1.2 (Noether-Normalisierung) *Sei R eine graduierte affine K-Algebra. Dann gibt es homogene, über K algebraisch unabhängige Elemente $a_1, \ldots, a_n \in R_+$, so dass R ganz über $A := K[a_1, \ldots, a_n]$ ist (oder äquivalent: R ist endlich erzeugt als Modul über A). Dabei ist $n = \dim R$ eindeutig bestimmt.*

Ein Beweis folgt nach Korollar 1.7.

Definition 1.3 *Eine Menge $\{a_1, \ldots, a_n\}$ mit den im Noetherschen Normalisierungssatz genannten Eigenschaften heißt ein* homogenes Parametersystem (hsop). *Eine Menge heißt* partielles homogenes Parametersystem (phsop)*, wenn sie Teilmenge eines hsops ist.*

Für eine alternative Charakterisierung von Parametersystemen (in affinen *Bereichen*) benötigen wir zunächst ein allgemeines Lemma.

Lemma 1.4 *Sei S/R eine ganze Erweiterung noetherscher Integritätsringe und zusätzlich R* normal. *Ist $I \neq R$ ein Ideal von R, so ist* $\text{height}(I) = \text{height}(SI)$.

Beweis. Unter den gemachten Voraussetzungen gilt „going-down“ [14, Theorem 13.9]. Insbesondere gilt für jedes Primideal $\mathcal{P} \lhd S$, dass

$$\text{height}(\mathcal{P}) = \text{height}(\mathcal{P} \cap R)$$

(siehe Kunz [40, Korollar VI.2.9]). Sei nun $\wp \lhd R$ ein I umfassendes Primideal mit $\operatorname{height}(\wp) = \operatorname{height}(I)$. Nach „lying-over“ ([40, Satz VI.2.3]) existiert ein Primideal $\mathcal{P} \lhd S$ mit $\wp = \mathcal{P} \cap R$. Da $I \subseteq \wp \subseteq \mathcal{P}$, gilt auch $SI \subseteq \mathcal{P}$, und damit

$$\operatorname{height}(SI) \leq \operatorname{height}(\mathcal{P}) = \operatorname{height}(\mathcal{P} \cap R) = \operatorname{height}(\wp) = \operatorname{height}(I).$$

Sei umgekehrt $\mathcal{P} \lhd S$ ein SI umfassendes Primideal mit $\operatorname{height}(\mathcal{P}) = \operatorname{height}(SI)$. Dann ist $I \subseteq \mathcal{P} \cap R$, und damit

$$\operatorname{height}(I) \leq \operatorname{height}(\mathcal{P} \cap R) = \operatorname{height}(\mathcal{P}) = \operatorname{height}(SI).$$

Insgesamt gilt also $\operatorname{height}(I) = \operatorname{height}(SI)$. □

(Der in [32, Lemma 1.5.e] gegebene Beweis für diesen Satz ohne die gemachten Voraussetzungen an R und S (R normal und S nullteilerfrei fehlen) enthält eine Lücke.) Wie üblich bezeichnen wir für einen R-Modul M mit $\operatorname{Ass}_R M$ die Menge der assoziierten Primideale von M in R (siehe Eisenbud [14, Chapter 3.1]).

Lemma 1.5 *Sei R eine graduierte affine K-Algebra. Es gilt stets* $\operatorname{height} R_+ = \dim R$. *Seien weiter $a_1, \ldots, a_k \in R$ ($k = 0$ möglich) homogene Elemente positiven Grades, sowie $I \neq R$ ein homogenes Ideal von R.*

(a) Gilt $\operatorname{height}(a_1, \ldots, a_k) = k$, *so ist $a_1, \ldots, a_k$ ein phsop von R. Ist hierbei $k = \dim R$, so handelt es sich sogar um ein hsop. Ist R nullteilerfrei und $a_1, \ldots, a_k$ ein phsop von R, so gilt umgekehrt* $\operatorname{height}(a_1, \ldots, a_k) = k$.

(b) Ist $a_1, \ldots, a_k \in I$ mit $\operatorname{height}(a_1, \ldots, a_k) = k$ *und* $r = \operatorname{height} I$, *so gibt es homogene Elemente positiven Grades $a_{k+1}, \ldots, a_r \in I$ mit* $\operatorname{height}(a_1, \ldots, a_r) = r$. *Ist R nullteilerfrei, so kann man also ein in I liegendes phsop zu einem in I liegenden phsop mit* $\operatorname{height}(I)$ *Elementen ergänzen.*

Für einen affinen Bereich ist also $a_1, \ldots, a_k$ genau dann ein phsop, wenn $\operatorname{height}(a_1, \ldots, a_k) = k$ *gilt.*

Beweis. (b) Sei $\operatorname{height}(a_1, \ldots, a_k) = k$. Ist $k = \operatorname{height}(I)$, so sind wir fertig, sei also $k < \operatorname{height}(I)$. Es genügt offenbar für den Beweis, ein weiteres homogenes Element $a_{k+1} \in I$ zu finden, so dass $\operatorname{height}(a_1, \ldots, a_{k+1}) = k + 1$ ist (da $I \neq R$ hat a_{k+1} dann automatisch positiven Grad). Sei $\{\wp_1, \ldots, \wp_s\}$ die Menge der minimalen, $(a_1, \ldots, a_k)$ umfassenden Primideale. Diese Menge ist endlich und alle Primideale sind homogen, da sie Teilmenge der endlichen Menge homogener Primideale $\operatorname{Ass}_R(R/(a_1, \ldots, a_k))$ ist ([14, Theorem 3.1.a], [40, Satz C.23]), und es gilt $\operatorname{height}(\wp_i) \leq k$ für alle i nach dem Krullschen Hauptidealsatz ([14, Theorem 10.2]). Es gilt sogar Gleichheit, da $\operatorname{height}(\wp_i) \geq \operatorname{height}(a_1, \ldots, a_k) = k$. Wäre $I \subseteq \bigcup_{i=1}^{s} \wp_i$, so gäbe es ein i mit $I \subseteq \wp_i$ (Lemma über das Vermeiden von Primidealen, [14, Lemma 3.3] oder [40, Lemma III.3.6]). Dann wäre $\operatorname{height}(I) \leq \operatorname{height}(\wp_i) = k$, im Widerspruch zur Voraussetzung. Also gibt es ein nach dem zitierten Lemma sogar homogenes $a_{k+1} \in I \setminus \bigcup_{i=1}^{s} \wp_i$. Ein minimales Primideal $\wp$ mit $(a_1, \ldots, a_{k+1}) \subseteq \wp$ umfasst dann eins der minimalen Primideale $\wp_i$ ([40, Satz III.1.10.b]), und da $a_{k+1} \notin \wp_i$, ist die Inklusion echt. Es folgt $\operatorname{height}(\wp) \geq \operatorname{height}(\wp_i) + 1 = k + 1$. Nach Krulls Hauptidealsatz gilt auch $\operatorname{height}(\wp) \leq k + 1$, also Gleichheit. Da dies für jedes solche minimale Primideal $\wp$ gilt, folgt also $\operatorname{height}(a_1, \ldots, a_{k+1}) = k + 1$, was zu zeigen war.

(Ist R nullteilerfrei, so bilden $a_1, \ldots, a_k \in I$ nach (a) genau dann ein phsop, wenn $\text{height}(a_1, \ldots, a_k) = k$. Daher kann man ein in I liegendes phsop zu einem in I liegenden phsop mit $\text{height}(I)$ Elementen ergänzen. Dies beweist dann den Zusatz in (b), den wir natürlich nicht für den folgenden Beweis von (a) brauchen.)

(a) (i) Sei $\text{height}(a_1, \ldots, a_k) = k$. Nach (b) mit $I = R_+$ und $n := \text{height}\, R_+$ lassen sich die k Elemente aus R_+ zu einer in R_+ liegenden Menge homogener Elemente $\{a_1, \ldots, a_n\}$ mit $\text{height}(a_1, \ldots, a_n) = n = \text{height}\, R_+$ ergänzen. Wir zeigen, dass eine solche Menge ein hsop ist, und das $\text{height}\, R_+ = \dim R$ gilt, was die ersten beiden Teile der Behauptung (a) sowie die Behauptung im Vorspann zeigt. Ein über $(a_1, \ldots, a_n)$ liegendes minimales Primideal $\wp$ ist homogen (s.o.), liegt also im maximalen homogenen Ideal R_+, und aus $n = \text{height}(a_1, \ldots, a_n) \leq \text{height}(\wp) \leq \text{height}(R_+) = n$ folgt $\wp = R_+$. Also ist $\wp$ maximal, und damit ist $\dim R/(a_1, \ldots, a_n) = 0$. Ist $A := K[a_1, \ldots, a_n]$, so bedeutet dies $\dim R/A_+R = 0$, d.h. $\dim_K R/A_+R < \infty$. Nach dem graduierten Nakayama Lemma [12, Lemma 3.5.1] ist dann R endlich erzeugt als A-Modul, also ist R ganz über A. Damit ist $\dim A = \dim R$. Ist $J \lhd K[X_1, \ldots, X_n] =: K[X]$ das Relationenideal von $a_1, \ldots, a_n$, so ist $A \cong K[X]/J$. Wären $a_1, \ldots, a_n$ nicht algebraisch unabhängig, also $J \neq (0)$, so wäre $\dim R = \dim A = \dim K[X_1, \ldots, X_n]/J < n = \text{height}(R_+)$. Da aber offenbar $\text{height}\, R_+ \leq \dim R$ gilt, ist dies ein Widerspruch und $J = (0)$. Also ist $a_1, \ldots, a_n$ ein hsop, und wir haben $\dim R = \dim A = n = \text{height}\, R_+$ gezeigt.

(ii) Sei nun R zusätzlich nullteilerfrei. Man ergänze das phsop $a_1, \ldots, a_k$ zu einem hsop $a_1, \ldots, a_n$ von R. Dann ist R ganz über dem (normalen, da faktoriellen) Polynomring $A = K[a_1, \ldots, a_n]$. Mit Lemma 1.4, das wir wegen der Nullteilerfreiheit von R und der Normalität von A auf die Erweiterung R/A anwenden können, folgt daher sofort $\text{height}(a_1, \ldots, a_k)_R = \text{height}(a_1, \ldots, a_k)_A = k$.

Der Zusatz ist lediglich ein Spezialfall von (a). □

Bemerkung 1.6 Da die Höhe eines Ideals nicht von der Graduierung abhängt, folgt im nullteilerfreien Fall aus Teil (*a*), dass Elemente die bezüglich zweier verschiedener Graduierungen von R homogen und positiven Grades sind und ein phsop bezüglich einer dieser Graduierungen bilden, auch bezüglich der anderen ein phsop bilden.

Korollar 1.7 *Sei S/R eine ganze Erweiterung noetherscher graduierter affiner Bereiche und zusätzlich R* normal. *Homogene Elemente $a_1, \ldots, a_k \in R_+$ bilden genau dann ein phsop in R, wenn sie eines in S bilden.*

Beweis. Dies folgt sofort mit Lemma 1.5 (a) und

$$\text{height}(a_1, \ldots, a_k)_R = \text{height}(a_1, \ldots, a_k)_S$$

nach Lemma 1.4. □

Beweis des Noetherschen Normalisierungssatzes 1.2. Man ergänze die leere Menge gemäß Lemma 1.5 (b) mit $I = R_+$ zu einer Menge homogener Elemente positiven Grades $a_1, \ldots, a_n$ mit $\text{height}(a_1, \ldots, a_n) = n = \text{height}\, R_+ = \dim R$. Nach Teil (a) des Lemmas ist diese Menge ein hsop von R. Ist umgekehrt R ganz über einem Polynomring A, so ist $n = \dim A = \dim R$ eindeutig bestimmt. □

Bemerkung 1.8 Ist $a_1, \ldots, a_n$ ein hsop von R, (also $n = \dim R$), so gilt umgekehrt stets $\text{height}(a_1, \ldots, a_n) = n$ (auch wenn es Nullteiler gibt). Sei nämlich $A := K[a_1, \ldots, a_n]$ und $\wp \supseteq (a_1, \ldots, a_n)$ ein minimales Primideal. Dann ist $\wp$ homogen, also $\wp \subseteq R_+$. Damit gilt $A_+ \subseteq \wp \cap A \subseteq R_+ \cap A = A_+$ (Definition der Graduierung von A), also Gleichheit. Über dem Primideal A_+ von A (wg. $A/A_+ = K$) liegen also die Primideale $\wp \subseteq R_+$ von R, und da R/A ganz, darf es keine echte Inklusion geben [40, Satz VI.2.3], d.h. $\wp = R_+$. Also ist $\text{height}(a_1, \ldots, a_n) = \text{height}\, \wp = \text{height}\, R_+ = \dim R = n$.

Damit wir die dargestellten Resultate stets voll verwenden können, haben wir „R nullteilerfrei“ in unsere Standardvoraussetzung mit aufgenommen.

Aus der Definition der Höhe folgt sofort, dass ein Ideal I gleiche Höhe wie sein Radikalideal $\sqrt{I}$ hat, also

$$\text{height}(I) = \text{height}(\sqrt{I}). \tag{1}$$

Dies ergibt

Lemma 1.9 *Seien $f_1, \ldots, f_k \in R_+$ homogen und $i_1, \ldots, i_k \geq 1$. Dann ist $f_1, \ldots, f_k$ genau dann ein phsop in R, wenn $f_1^{i_1}, \ldots, f_k^{i_k}$ eines ist.*

Beweis. Dies folgt sofort aus Lemma 1.5 (a) und

$$\text{height}(f_1, \ldots, f_k) \overset{(1)}{=} \text{height}\, \sqrt{(f_1, \ldots, f_k)} = \text{height}\, \sqrt{(f_1^{i_1}, \ldots, f_k^{i_k})} \overset{(1)}{=} \text{height}(f_1^{i_1}, \ldots, f_k^{i_k}).$$

□

Bemerkung 1.10 Wir haben den Begriff „phsop“ nur für graduierte affine Algebren definiert. Ist R allgemeiner ein Noetherscher Ring, so heißt etwa in Kemper [32, vor Lemma 1.5] $a_1, \ldots, a_k \in R$ ein *partielles Parametersystem (psop)*, wenn $(a_1, \ldots, a_k) \neq R$ und $\text{height}(a_1, \ldots, a_i) = i$ für *alle* $i = 1, \ldots, k$ gilt. Für graduierte affine Bereiche stimmt diese Definition im Fall homogener a_i mit unserer überein, denn wenn die letzte Gleichung für $i = k$ gilt, also nach Lemma 1.5 ein phsop vorliegt, so ist aufgrund unserer Definition erst Recht $a_1, \ldots, a_i$ ein phsop für jedes $i \leq k$, und wieder nach Lemma 1.5 gilt dann auch $\text{height}(a_1, \ldots, a_i) = i$.

Ist $R = P/I$ als Faktorring eines Polynomrings gegeben und nullteilerfrei, so kann man mit Lemma 1.5 leicht entscheiden, ob gegebene homogene Elemente $(a_1, \ldots, a_k)$ ein phsop bilden. Dann ist nämlich $\text{height}(a_1, \ldots, a_k)_R = \dim R - \dim R/(a_1, \ldots, a_k)_R = \dim P/I - \dim P/(I + (a_1, \ldots, a_k)_P)$, und in Polynomringen lässt sich die Dimension von Idealen wie bereits bemerkt berechnen.

Um eine Algebra R genauer zu untersuchen, ist die Konstruktion eines (p)hsops oft unerlässlich. Der Algorithmus von Kemper [31] berechnet ein „optimales“ hsop, wobei (u.a.) das obige Kriterium verwendet wird. Hier muss also das Relationenideal bekannt sein.

Exkurs: Berechnung eine hsops

In diesem Exkurs verlassen wir kurz den systematischen Aufbau der Grundlagen. Die Resultate dieses Abschnitts werden nicht weiter verwendet, so dass dieser Abschnitt bedenkenlos

übersprungen werden kann.

Die meisten Beweise des Noetherschen Normalisierungssatzes sind in irgendeiner Form ebenfalls konstruktiv, siehe z.B. Eisenbud [14, Theorem 13.3] oder Fogarty [20, Theorem 5.44]. Wir wollen hier kurz ein Verfahren zur Bestimmung eines hsops angeben, das im Prinzip im explizit machen der Beweise aus Eisenbud/Fogarty besteht, und ohne die Berechnung des vollständigen Relationenideals auskommt. Leider lässt sich der angegebene Algorithmus zwar theoretisch leicht umsetzen, scheitert in der Praxis aber daran, dass die in jedem Schritt auftretenden Relationenhauptideale von Polynomen von immer größer werdendem Grad erzeugt wurden, bis diese nicht mehr (in akzeptabler Zeit) gefunden werden konnten. Hier also zunächst die Rohfassung des Verfahrens:

Algorithmus 1.11 Bestimmung eines hsops einer Unteralgebra R eines Polynomrings $K[X]$
Eingabe: Erzeuger $f_1, \ldots, f_n \in K[X]$ von R, also $R = K[f_1, \ldots, f_n] \subseteq K[X]$.
Ausgabe: Ein hsop für R.
BEGIN

1. $hsop_0 := \emptyset$
2. For $i := 1$ to n do
   a) Falls $hsop_{i-1} \cup \{f_i\}$ algebraisch unabhängig ist, so setze $hsop_i := hsop_{i-1} \cup \{f_i\}$.
   b) Sonst bestimme ein $hsop$ für $K[hsop_{i-1} \cup \{f_i\}]$ und setze $hsop_i := hsop$.
3. Return($hsop_n$)

END

Bevor wir erklären, wie die Schritte (a) und (b) umzusetzen sind, machen wir zunächst folgende *Beobachtung*: Es ist stets $hsop_i$ ein hsop von $K[f_1, \ldots, f_i]$ (insbesondere also $hsop_n$ ein hsop von R).
Beweis. Offenbar ist in jedem Schritt $hsop_i$ algebraisch unabhängig. Wir machen Induktion nach i, um die Ganzheitsrelation zu zeigen.
$i = 0$: Die leere Menge $hsop_0$ ist ein hsop für K.
$(i-1) \to i$: Nach Voraussetzung sind $f_1, \ldots, f_{i-1}$ ganz über $K[hsop_{i-1}]$. Da diese Elemente dann auch ganz über $K[hsop_{i-1}, f_i]$ sind, und f_i dies natürlich ebenfalls ist, ist also $K[f_1, \ldots, f_i]$ ganz über $K[hsop_{i-1}, f_i]$. Damit folgt die Aussage im Fall, dass $hsop_i$ nach (a) berechnet wird. Im Fall (b) ist nun $K[hsop_{i-1}, f_i]$ nach Konstruktion ganz über $K[hsop_i]$, und aufgrund der Transitivität der Relation „ganz“ ist also $K[f_1, \ldots, f_i]$ ganz über $K[hsop_i]$. □

Umsetzung der Schritte (a) und (b):
Zu (a). Es sei zunächst bemerkt, dass der Algorithmus nicht falsch wird, wenn man in jedem Schritt nach (b) vorgeht, z.B. weil aufgrund des folgenden Korollars keine Aussage gemacht werden kann.

Satz 1.12 (Jacobi-Kriterium) *Seien $g_1, \ldots, g_n \in K[X_1, \ldots, X_n]$ Elemente eines Polynomrings, und $J := \left(\frac{\partial g_i}{\partial X_j}\right)_{i,j=1,\ldots,n}$ die zugehörige* Jacobi-Matrix. *Dann gilt:*
$K(X_1, \ldots, X_n)/K(g_1, \ldots, g_n)$ ist genau dann eine endliche und separable Körpererweiterung, falls $\det J \neq 0$ ist.

Beweis. Siehe [1], Proposition 5.4.2. □

Korollar 1.13 *Seien $g_1, \ldots, g_k \in K[X_1, \ldots, X_n]$ Elemente eines Polynomrings, und $J := \left(\frac{\partial g_i}{\partial X_j}\right)_{i=1,\ldots,k, j=1,\ldots,n}$ die zugehörige* Jacobi-Matrix. *Dann gilt: Gibt es eine $k \times k$ Teilmatrix von J mit Determinante ungleich 0, so sind $g_1, \ldots, g_k$ algebraisch unabhängig. In Charakteristik 0 gilt sogar die Umkehrung dieser Aussage.*

Beweis. Falls es eine solche Teilmatrix mit Determinante ungleich 0 gibt und $j_1, \ldots, j_k$ die zugehörigen Spalten sind, so hat die zu $\{g_1, \ldots, g_k\} \cup \{X_i : i \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_k\}\}$ gehörige Jacobi-Determinante Wert ungleich 0. Nach dem Jacobi-Kriterium ist die betrachtete Menge also eine Transzendenzbasis, und die Teilmenge $\{g_1, \ldots, g_k\}$ damit algebraisch unabhängig.

Sind umgekehrt $\{g_1, \ldots, g_k\}$ algebraisch unabhängig, so kann man diese Menge mit $n - k$ Elementen aus der Transzendenzbasis $\{X_1, \ldots, X_n\}$ zu einer Transzendenzbasis ergänzen (Austauschsatz für Transzendenzbasen). Sei also $\{g_1, \ldots, g_k, X_{j_1}, \ldots, X_{j_{n-k}}\}$ eine Transzendenzbasis, mit zugehöriger Jacobi-Determinante J. Dann ist die Körpererweiterung $K(X_1, \ldots, X_n)/K(g_1, \ldots, g_k, X_{j_1}, \ldots, X_{j_{n-k}})$ endlich und in Charakteristik 0 automatisch separabel, also $\det J \neq 0$. Dies bedeutet, dass die zu den Zeilen/Spalten $\{1, \ldots, n\} \setminus \{j_1, \ldots, j_{n-k}\}$ gehörige Teilmatrix von J Determinante ungleich 0 hat. □

Der Beweis zeigt auch, wie man ggf. die gegebenen Polynome mit den Variablen zu einer Transzendenzbasis ergänzen kann. Im Falle positiver Charakteristik p wird die Umkehrung des Kriteriums falsch; etwa ist X^p eine Transzendenzbasis von $K(X)$, aber $J = (pX^{p-1}) = (0)$ - die Erweiterung $K(X)/K(X^p)$ ist zwar endlich, aber nicht separabel.

In positiver Charakteristik wird man bei der Durchführung des Algorithmus also so vorgehen: Man testet im Schritt (a) zunächst auf die Existenz einer nicht-singulären $i \times i$ Teilmatrix. Hat man eine solche, so ist die betrachtete Menge algebraisch unabhängig und man kann wie beschrieben vorgehen. Ansonsten kann man keine Aussage machen, und man muss Schritt (b) durchführen.

Die Voraussetzung des Korollars bedeutet natürlich nichts anderes, als das $\operatorname{rang} J = k$ über dem rationalen Funktionenkörper $K(X_1, \ldots, X_n)$, und man kann dies mit dem Gauss-Algorithmus entscheiden, und erhält so ggf. auch die Spalten einer nicht-singulären Teilmatrix. Die folgende Variante um zu testen, ob J eine solche Teilmatrix besitzt, lies sich mit den in Magma vorhandenen Funktionen jedoch etwas schneller implementieren, und lieferte in den betrachteten Fällen das Ergebnis praktisch in Nullzeit.

Test ob eine nichtsinguläre $k \times k$ Teilmatrix von J existiert, wobei gleich die zugehörigen Spalten $j_1, \ldots, j_n$ dieser Matrix, falls sie existiert, mitbestimmt werden: Wähle zunächst j_1 als den kleinsten Index j mit $\frac{\partial g_1}{\partial X_j} \neq 0$. Falls es keinen solchen Eintrag gibt, so gibt es auch keine nichtsinguläre $k \times k$ Teilmatrix. Seien nun $j_1, \ldots, j_i$ bereits konstruiert, so dass die zu diesen Spaltenindizes und zu den ersten i Zeilen gehörige Teilmatrix Determinante ungleich 0 hat. Für j_{i+1} wähle man nun den kleinsten Index $1, \ldots, n$, so dass die zugehörige $(i+1) \times (i+1)$ Determinante einen Wert ungleich 0 hat. Gibt es keinen solchen Index, so gibt es auch keine nichtsinguläre $k \times k$ Teilmatrix.

Zu (b) in Algorithmus 1.11, Schritt 2. Als erstes müssen wir das Relationenideal von $hsop_{i-1} \cup \{f_i\}$ bestimmen. Wir gehen hier davon aus, dass man im Schritt (b) ankommt,

weil bekannt ist, dass die in (a) betrachtete Menge $hsop_{i-1} \cup \{f_i\}$ algebraisch abhängig ist. Ist dies nicht der Fall, etwa in positiver Charakteristik, so muss man eines der Standard-(Gröbner-Basis)-Verfahren verwenden, um das Relationenideal von $hsop_{i-1} \cup \{f_i\}$ zu bestimmen. Ist es das Nullideal, so zeigt das nachträglich die algebraische Unabhängigkeit dieser Menge. Das folgende Lemma zeigt, dass das Relationenideal jedenfalls stets ein Hauptideal ist (nach Konstruktion ist $hsop_{i-1}$ stets algebraisch unabhängig, und daher ist das folgende Lemma anwendbar).

Lemma 1.14 *Sei $\{f_1, \ldots, f_{k+1}\} \subseteq K[Y]$ eine algebraisch abhängige Menge von Polynomen, so dass $\{f_1, \ldots, f_k\}$ algebraisch unabhängig sind. Sei $\tilde{p}(X_{k+1}) \in K[f_1, \ldots, f_k][X_{k+1}]$ dasjenige Polynom, das aus dem Minimalpolynom p von f_{k+1} über dem Quotientenkörper $K(f_1, \ldots, f_k)$ durch Multiplikation mit dem Hauptnenner der Koeffizienten hervorgeht.*

Dann ist das Relationenideal von $\{f_1, \ldots, f_{k+1}\}$ in $K[X_1, \ldots, X_{k+1}]$ ein Hauptideal, erzeugt von dem Polynom, das aus $\tilde{p}$ durch Ersetzen von (den algebraisch unabhängigen Elementen) $f_1, \ldots, f_k$ durch $X_1, \ldots, X_k$ hervorgeht.

Beweis. Nach Voraussetzung ist $R := K[f_1, \ldots, f_k] \cong K[X_1, \ldots, X_k]$, insbesondere ist R faktoriell. Sei $F := \mathrm{Quot}(R) = K(f_1, \ldots, f_k)$ und $p(X_{k+1})$ das Minimalpolynom von f_{k+1} über F. Mit c bezeichnen wir den *Inhalt* eines Polynoms aus $F[X_{k+1}]$, der mit Hilfe eines fest gewählten Repräsentantensystems der Primelemente von R berechnet wird. (Erinnerung: Der Inhalt $c(f)$ eines Polynoms $f \in R[X]$ ist der ggT seiner Koeffizienten, berechnet mit dem Repräsentantensystem ($c(0) := 0$). Ist $f \in \mathrm{Quot}(R)[X]$ und $a \in R \setminus \{0\}$ mit $af \in R[X]$, so ist $c(f) := c(af)/c(a)$. Für $f, g \in \mathrm{Quot}(R)[X]$ gilt $c(fg) = c(f)c(g)$, und aus $c(f) = 1$ folgt $f \in R[X]$. Insbesondere ist für $f \neq 0$ stets $f/c(f) \in R[X]$.) Dann ist $\tilde{p} = p/c(p)$.

Sei nun $0 \neq g \in K[X_1, \ldots, X_{k+1}] \cong R[X_{k+1}]$ eine Relation, d.h. $g(f_1, \ldots, f_{k+1}) = 0$. Fassen wir g als Element von $R[X_{k+1}]$ auf, so bedeutet dies $g(f_{k+1}) = 0$. Es ist zu zeigen, dass g polynomiales Vielfaches von $p/c(p) \in R[X_{k+1}]$ ist. Da p das Minimalpolynom von f_{k+1} über F ist, gibt es ein $h \in F[X_{k+1}]$ mit $ph = g$, also $c(p)c(h) = c(g)$. Damit ist $g = \frac{p}{c(p)} \cdot \frac{h}{c(h)} \cdot c(g)$, und da jeder der drei Faktoren in $R[X_{k+1}]$ liegt, folgt die Behauptung. □

Da in unserem Fall alle Polynome homogen sind, ist die das Relationenideal erzeugende Relation ebenfalls homogen bei Gewichtung $\deg X_i := \deg f_i$. Falls man weis, dass die in (a) betrachtete Menge algebraisch abhängig ist, es also Relationen positiven Grades gibt, kann man nacheinander alle Grade $d = 1, 2, 3, \ldots$ durchlaufen, in jedem Grad d die Menge der Monome vom Grad d in $hsop_{i-1} \cup \{f_i\}$ bilden und hiervon dann eine nichttriviale Linearkombination der 0 suchen - in jedem Schritt wird also ein homogenes lineares Gleichungssystem gelöst. Sobald man eine Lösung hat, ist diese dann somit die minimale, erzeugende Relation, und das Verfahren terminiert. Wie bereits erwähnt wurden die minimalen Grade d in der Praxis meist bald so groß, dass die erzeugende Relation nicht mehr gefunden werden konnte.

Hat man die Relation erstmal gefunden, ist die Berechnung des hsops vergleichsweise leicht. Sind nämlich $f = f_1, f_2, \ldots, f_n \in K[X_1, \ldots, X_n] =: K[X]$ und interpretiert man f als Relation, so sind $f_2, \ldots, f_n$ genau dann ein hsop für $K[X]/(f)$, falls $f, f_2, \ldots, f_n$ ein hsop für $K[X]$ ist. Nach Eisenbud [14, Lemma 13.2.c] kann man dazu für $i \geq 2$ z.B. $f_i = X_i - a_i X_1$ (ggf. vorher homogenisiert) wählen mit $a_i \in K$ geeignet. In der Praxis reicht es meist, zwei der a_i ungleich 0 zu wählen. Häufig ist z.B. (nach umnumerieren)

$f \in X_1^i X_2^j + (X_3, \ldots, X_n)$, und für f_2 bietet sich dann eine Homogenisierung von $X_1 + X_2$ an, und für die restlichen Elemente $f_i = X_i$, $i > 2$. Dies ist dann tatsächlich ein hsop, da die gemeinsame Nullstellenmenge der n Polynome offenbar nur aus $0 \in K^n$ besteht (aus $X_n = \ldots = X_3 = 0$ folgt mit $f = 0$ dann $X_1 X_2 = 0$; zusammen mit $X_1 + X_2 = 0$ dann auch $X_1 = X_2 = 0$). Hilberts Nullstellensatz liefert die Ganzheit von $K[X]/K[f_1, \ldots, f_n]$. Man sieht bereits, dass das Relationenideal des nächsten hsops entsprechend komplizierter wird.

1.1.2 Tiefe und reguläre Sequenzen

Definition 1.15 *Sei R kommutativer Ring mit 1, und M ein R-Modul. Eine Folge von Elementen $a_1, \ldots, a_n \in R$ heißt eine M-*reguläre Sequenz (der Länge n)*, falls gelten:*

(a) $(a_1, \ldots, a_n)M \neq M$.

(b) a_i ist kein Nullteiler von $M/(a_1, \ldots, a_{i-1})M$ für alle $i = 1, \ldots, n$. (D.h.: Ist $a_1 m_1 + \ldots + a_i m_i = 0$ mit $m_1, \ldots, m_i \in M$, so ist $m_i \in (a_1, \ldots, a_{i-1})M$.)

Ist I ein Ideal von R mit $IM \neq M$, so wird mit $\operatorname{depth}(I, M)$ *die* Tiefe *von I auf M bezeichnet, die grösste auftretende Länge einer in I liegenden, M-regulären Sequenz (diese Zahl ist endlich für R noethersch und M endlich erzeugter R-Modul ([14, Proposition 18.2])). Man schreibt auch* $\operatorname{depth}(I) := \operatorname{depth}(I, R)$. *Eine solche reguläre Sequenz größtmöglicher Länge heißt dann eine* die (I-)Tiefe messende *reguläre Sequenz.*

Eine in I liegende reguläre Sequenz $(a_1, \ldots, a_n)$ heißt maximal*, wenn sie nicht zu einer längeren regulären Sequenz in I ergänzt werden kann, d.h. I besteht nur aus Nullteilern von $M/(a_1, \ldots, a_n)M$.*

Ist R sogar eine eine graduierte Algebra, und M ein graduierter R-Modul (d.h. $M = \bigoplus_{i=b}^{\infty} M_i$ als K-Vektorräume, $b \in \mathbb{Z}$, und $R_i M_j \subseteq M_{i+j}$ für alle i, j), und sind alle Elemente einer regulären Sequenz zusätzlich homogen, so spricht man von einer homogenen regulären Sequenz*. Ist R_+ das maximale homogene Ideal von R, so heißt* $\operatorname{depth}(M) := \operatorname{depth}(R_+, M)$ *die* Tiefe von $M (\neq 0)$*, insbesondere ist* $\operatorname{depth}(R) = \operatorname{depth}(R_+, R)$ *die* Tiefe von R*.*

Ein Ideal I von R ist auch ein R-Modul. Mit $\operatorname{depth}(I)$ meint man dann aber immer $\operatorname{depth}(I, R)$ und nie $\operatorname{depth}(R_+, I)$.

Ist $R = P/I$ als Quotient eines Polynomrings P nach einem Ideal I gegeben, so lässt sich algorithmisch entscheiden, ob eine Folge $a_1, \ldots, a_n \in R$ R-regulär ist. Offenbar ist nämlich a_1 genau dann kein Nullteiler von R, wenn für das Quotientenideal $I : (a_1) = I$ gilt. Weiter ist genau dann a_2 kein Nullteiler auf $R/(a_1) \cong P/(I + (a_1))$, wenn $(I + (a_1)) : (a_2) = I + (a_1)$ gilt u.s.w. Quotientenideale lassen sich aber mit Gröbner-Basen berechnen, siehe z.B. [12, section 1.2.4]. Ein entsprechender Algorithmus ist in Magma mit dem Befehl `IsZeroDivisor` implementiert.

Satz 1.16 (Rees) *Sei R ein noetherscher Ring, M ein endlich erzeugter R-Modul und I ein Ideal von R mit $IM \neq M$. Dann haben je zwei maximale M-reguläre Sequenzen in I die gleiche Länge, nämlich* $\operatorname{depth}(I, M)$*. Eine M-reguläre Sequenz in I ist also genau dann maximal, wenn sie die Tiefe misst. Insbesondere kann jede in I liegende M-reguläre Sequenz zu einer die Tiefe von I messenden M-regulären Sequenz ergänzt werden. Ist daher*

$(a_1, \ldots, a_r)$ eine M-reguläre Sequenz in I, so ist

$$\operatorname{depth}(I, M/(a_1, \ldots, a_r)M) = \operatorname{depth}(I, M) - r. \tag{2}$$

Beweis. Siehe Bruns und Herzog [6, Theorem 1.2.5] oder [40, Satz E.7]. □

Der folgende Satz besagt, dass wir uns zur Bestimmung der Tiefe in den uns interessierenden Fällen auf homogene reguläre Sequenzen beschränken können.

Satz 1.17 *Ist R eine graduierte* affine *Algebra, M ein* endlich erzeugter*, graduierter R-Modul, und I ein* homogenes *Ideal von R mit $IM \neq M$, so existiert eine* homogene *M-reguläre Sequenz der Länge* $\operatorname{depth}(I, M)$ *in I. Genauer lässt sich jede in I liegende homogene M-reguläre Sequenz zu einer die Tiefe* $\operatorname{depth}(I, M)$ *messenden, in I liegenden homogenen M-regulären Sequenz ergänzen.*

Beweis. (Vgl. Bruns und Herzog [6, Propositon 1.5.11].) Sei $a_1, \ldots, a_k \in I$ eine homogene M-reguläre Sequenz ($k = 0$ erlaubt). Ist $k = \operatorname{depth}(I, M)$, so sind wir fertig. Sei also $k < \operatorname{depth}(I, M)$. Nach Satz 1.16 ist die M-Sequenz $a_1, \ldots, a_k$ dann nicht maximal, d.h. I besteht nicht nur aus Nullteilern von $N := M/(a_1, \ldots, a_k)M \neq 0$. Da die Menge der Nullteiler von N in R (und der 0) durch $\bigcup \operatorname{Ass}_R N$ gegeben ist (Eisenbud [14, Theorem 3.1.b]), gilt also $I \not\subseteq \bigcup \operatorname{Ass}_R N$. Da die a_i homogen sind, ist N ein graduierter R-Modul, und damit sind die (endlich vielen) Elemente von $\operatorname{Ass}_R N$ homogene Primideale (Eisenbud [14, Theorem 3.1.a, 3.12]). Nach dem (graduierten) Lemma über das Vermeiden von Primidealen ([40, Lemma III.3.6] oder [6, Lemma 1.5.10]) existiert dann ein homogenes $a_{k+1} \in I$ mit $a_{k+1} \notin \bigcup \operatorname{Ass}_R N$. Dann ist a_{k+1} kein Nullteiler von $N = M/(a_1, \ldots, a_k)$ und damit $a_1, \ldots, a_{k+1}$ eine homogene M-reguläre Sequenz in I. Durch Induktion folgt die Behauptung. □

Trägt R also zwei verschiedene Graduierungen, die beide das gleiche maximale homogene Ideal R_+ haben, so gibt es für jede der Graduierungen jeweils eine homogene reguläre Sequenz der gleichen Länge $\operatorname{depth} R$.

Die Gültigkeit dieser Sätze zu gewährleisten ist einer der Gründe für die Forderung $IM \neq M$ in der Definition der Tiefe eines Ideals. In der graduierten Situation bedeutet die Standardbedingung $IM \neq M$ übrigens lediglich $M \neq 0$ und $I \subseteq R_+$.

Homogene reguläre Sequenzen haben - im Gegensatz zu den nicht homogenen - sehr angenehme Eigenschaften. Zum Beispiel gilt

Satz 1.18 *Sei R eine graduierte Algebra, $M \neq 0$ ein graduierter R-Modul. Ist dann $(a_1, \ldots, a_n)$ eine* homogene *M-reguläre Sequenz, so ist für jede Permutation $\pi \in S_n$ auch $(a_{\pi(1)}, \ldots, a_{\pi(n)})$ eine homogene M-reguläre Sequenz.*

Beweis. Da S_n von den Transpositionen $(k, k+1)$ mit $1 \leq k \leq n-1$ ezeugt wird, genügt es den Satz für eine solche Permutation zu beweisen. Hierfür ist lediglich noch zu zeigen, dass a_{k+1} kein Nullteiler von $N := M/(a_1, \ldots, a_{k-1})$ und a_k kein Nullteiler von $N/(a_{k+1})N$ ist, wobei a_k, a_{k+1} eine N-reguläre Sequenz ist. Es genügt also den Satz für $n = 2$ und $\pi = (1, 2)$ zu beweisen.

Wir zeigen zuerst, dass a_2 kein Nullteiler auf M ist. Sei nämlich $m \in M$ mit $a_2 m = 0$. Da dies dann auch für jede homogene Komponente von m gilt (weil a_2 homogen ist), können

wir m als homogen annehmen. Es gilt dann erst recht $a_2 m = 0 \in M/(a_1)M$, und wegen der M-Regularität von a_1, a_2 folgt $m \in (a_1)M$. Es gibt also $m' \in M$ mit $m = a_1 m'$. Da m und a_1 homogen sind, können wir dann auch m' homogen wählen, und es ist wegen $\deg a_1 > 0$ dann $m = 0$ (dann sind wir fertig) oder $\deg m' < \deg m$. Aus $0 = a_2 m = a_1 a_2 m'$ und weil a_1 kein Nullteiler ist, folgt $a_2 m' = 0$. Da die Graduierung von M nach Definition nach unten beschränkt ist, folgt durch Induktion nach $\deg m$ (genauer: „Jagd nach dem kleinsten Verbrecher“) dann $m' = 0$ und damit dann doch $m = a_1 m' = 0$.

Sei nun $m_1 \in M$ mit $a_1 m_1 = 0 \in M/(a_2)M$, d.h. es gibt $m_2 \in M$ mit $a_1 m_1 + a_2 m_2 = 0$. Wir müssen $m_1 \in (a_2)M$ zeigen. Da a_1, a_2 M-regulär ist, gilt $m_2 \in (a_1)M$, d.h. es gilt $m_2 = a_1 m'$ mit $m' \in M$. Also ist $0 = a_1 m_1 + a_2 m_2 = a_1 m_1 + a_1 a_2 m' = a_1(m_1 + a_2 m')$. Da a_1 kein Nullteiler auf M ist, folgt also $m_1 = -a_2 m' \in (a_2)M$, was zu zeigen war. (Vgl. auch [40, Korollar E.16 und Satz E.17] für eine Verallgemeinerung (mit anderem Beweis).) □

Satz 1.19 *Sei R eine graduierte affine K-Algebra, M ein endlich erzeugter graduierter R-Modul, I ein homogenes Ideal von R und a ein homogenes Element von R. Ist dann $(I + (a))M \neq M$, so gilt*

$$\operatorname{depth}(I + (a), M) \leq \operatorname{depth}(I, M) + 1.$$

Wir geben zunächst einen allgemeinen Beweis, und dann einen elementaren Beweis unter einer Zusatzannahme, die in dieser Arbeit stets eintreffen wird, da bei uns immer $M = S$ eine nullteilerfreie Oberalgebra von R sein wird. Der 1. Beweis kann daher ggf. übersprungen werden.

1. Beweis (mit Homologie). Wir übersetzen den in Eisenbud [14, Lemma 18.3] gegebenen Beweis (für einen lokalen Ring R) in unsere graduierte Situation. Sei $x_1, \ldots, x_n$ ein homogenes Erzeugendensystem von I, und sei

$$k + 1 := \operatorname{depth}(I + (a), M).$$

Sei dann $K(x_1, \ldots, x_n, a)$ der zu diesem Erzeugendensystem von $I + (a)$ gehörende *Koszul-Komplex*, siehe [14, Section 17.2]. Nach der Charakterisierung der Tiefe durch das Verschwinden der Homologie des Koszul-Komplexes [14, Theorem 17.4] ist dann $H^i(M \otimes K(x_1, \ldots, x_n, a)) = 0$ für $i \leq k$. Nun hat man nach [14, Corollary 17.11] eine exakte Sequenz

$$H^i(M \otimes K(x_1, \ldots, x_n)) \xrightarrow{a} H^i(M \otimes K(x_1, \ldots, x_n)) \to H^{i+1}(M \otimes K(x_1, \ldots, x_n, a)),$$

wobei die erste Abbildung durch Multiplikation mit a gegeben ist. Für $i \leq k - 1$ sind die rechten Homologiemoduln gleich 0, d.h. die Linksmultiplikation mit a ist surjektiv. Also gilt

$$H^i(M \otimes K(x_1, \ldots, x_n)) = (a)_R \cdot H^i(M \otimes K(x_1, \ldots, x_n)).$$

Nun sind die Homologien des Koszul-Komplexes graduierte R-Moduln, und $(a)_R$ ist ein homogenes Ideal in R. Aufgrund obiger Gleichung folgt dann aus dem graduierten Nakayama-Lemma [14, Exercise 4.6] oder [40, Lemma A.9], dass $H^i(M \otimes K(x_1, \ldots, x_n)) = 0$ für $i \leq k - 1$. Wieder aufgrund der Charakterisierung der Tiefe mittels Homologie folgt $\operatorname{depth}(I, M) \geq k$, und mit der Definition von k die Behauptung. □

Die Idee für den folgenden Beweis hat mir Gregor Kemper beim Kaffee-trinken mitgeteilt.

2. Beweis (elementar) unter der Zusatzvoraussetzung, dass a kein Nullteiler auf M ist, (a) also selber eine reguläre Sequenz der Länge 1 in $I + (a)$ ist. Nach Satz 1.17 kann man a zu einer maximalen homogenen regulären Sequenz $a, b_1 + r_1 a, b_2 + r_2 a, \ldots, b_k + r_k a$, mit $b_i \in I, r_i \in R$ homogen, in $I + (a)$ ergänzen. Insbesondere gilt dann

$$\operatorname{depth}(I + (a), M) = k + 1. \tag{3}$$

Nun gilt aber für alle $i = 1, \ldots, k$, dass

$$(a, b_1 + r_1 a, b_2 + r_2 a, \ldots, b_{i-1} + r_{i-1} a)M = (a, b_1, b_2, \ldots, b_{i-1})M,$$

und für $m \in M$ ist dann

$$(b_i + r_i a)m \in (a, b_1 + r_1 a, b_2 + r_2 a, \ldots, b_{i-1} + r_{i-1} a)M \Leftrightarrow b_i m \in (a, b_1, b_2, \ldots, b_{i-1})M, \tag{4}$$

und ebenso

$$m \in (a, b_1 + r_1 a, b_2 + r_2 a, \ldots, b_{i-1} + r_{i-1} a)M \Leftrightarrow m \in (a, b_1, b_2, \ldots, b_{i-1})M. \tag{5}$$

Da $a, b_1 + r_1 a, b_2 + r_2 a, \ldots, b_k + r_k a$ regulär ist, ist dann also auch $(a, b_1, b_2, \ldots, b_k)$ M-regulär - man lese dazu (4) von rechts nach links, verwende die Regularität und lese dann (5) von links nach rechts. Zusätzlich ist die Sequenz homogen, und damit ist nach Satz 1.18 auch die Permutation $(b_1, b_2, \ldots, b_k, a)$ M-regulär. Insbesondere ist dann $(b_1, b_2, \ldots, b_k)$ eine reguläre, in I liegende Sequenz. Es folgt $k \leq \operatorname{depth}(I)$, mit (3) also $\operatorname{depth}(I + (a), M) \leq \operatorname{depth}(I, M) + 1$. □

Korollar 1.20 *Sind in obiger Situation $a_1, \ldots, a_n \in R$ homogen mit $(I + (a_1, \ldots, a_n))M \neq M$, so gilt*

$$\operatorname{depth}(I + (a_1, \ldots, a_n), M) \leq \operatorname{depth}(I, M) + n$$

Beweis. Induktiv folgt $\operatorname{depth}(I + (a_1, \ldots, a_n), M) \leq \operatorname{depth}(I + (a_1, \ldots, a_{n-1}), M) + 1 \leq \operatorname{depth}(I + (a_1, \ldots, a_{n-2}), M) + 2 \leq \ldots \leq \operatorname{depth}(I, M) + n$ □

Mit Hilfe des folgenden Satzes lässt sich die Tiefe eines Ideals oft bestimmen. Er ist inspiriert von Shank und Wehlau [57, Theorem 2.1], welche sich nach eigenen Angaben von Eisenbud [14, Corollary 17.12] inspirieren ließen.

Satz 1.21 *Sei R eine graduierte affine K-Algebra, $M \neq 0$ ein endlich erzeugter graduierter R-Modul. Seien $a_1, \ldots, a_n \in R_+$ homogen und $a_1, \ldots, a_k$ eine M-reguläre Sequenz ($k \leq n$). Gibt es dann ein $m \in M$ mit $m \notin (a_1, \ldots, a_k)M$, aber $a_i m \in (a_1, \ldots, a_k)M$ für alle $i = 1, \ldots, n$, so gilt*

$$\operatorname{depth}((a_1, \ldots, a_n)_R, M) = k.$$

Äquivalente Formulierung: Ist $I \neq R$ ein homogenes Ideal, $a_1, \ldots, a_k \in I$ eine homogene M-reguläre Sequenz, und gibt es ein $m \in M$ mit $m \notin (a_1, \ldots, a_k)M$, aber $rm \in (a_1, \ldots, a_k)M$ für alle $r \in I$, so gilt

$$\operatorname{depth}(I, M) = k.$$

Beweis. Nach Satz 1.16 genügt es zu zeigen, dass $a_1, \ldots, a_k$ eine maximale reguläre Sequenz in $I := (a_1, \ldots, a_n)_R$ ist, denn dann misst sie die Tiefe. Wäre dem nicht so, so gäbe es ein $a = r_1a_1 + \ldots + r_na_n \in I$ (mit $r_i \in R$ für alle i), so dass $a_1, \ldots, a_k, a$ ebenfalls M-regulär ist. Nach Voraussetzung ist aber $am = r_1a_1m + \ldots + r_na_nm \in (a_1, \ldots, a_k)M$, jedoch $m \notin (a_1, \ldots, a_k)M$, was im Widerspruch zur Regularität von $a_1, \ldots, a_k, a$ steht.

Für die äquivalente Formulierung wähle man einfach homogene $a_{k+1}, \ldots, a_n \in I$ mit $I = (a_1, \ldots, a_n)$. Genau dann ist $rm \in (a_1, \ldots, a_k)M$ für alle $r \in I$, wenn $a_im \in (a_1, \ldots, a_k)M$ für $i = 1, \ldots, n$.

Man kann auch so schließen: Nach Voraussetzung besteht I nur aus Nullteilern von $M/(a_1, \ldots, a_k)M$. Daher ist $a_1, \ldots, a_k$ eine maximale M-reguläre Sequenz in I und misst damit die Tiefe. □

Es gilt auch die **Umkehrung:** *Ist $a_1, \ldots, a_k$ eine maximale homogene M-reguläre Sequenz in I, so gibt es ein $m \in M$ mit $m \notin (a_1, \ldots, a_k)M$ aber $Im \subseteq (a_1, \ldots, a_k)M$.*

Beweis. Nach Voraussetzung besteht I nur aus Nullteilern von $N := M/(a_1, \ldots, a_k)M$. Nach [14, Theorem 3.1.b] ist also $I \subseteq \bigcup_{\wp \in \mathrm{Ass}_R(N)} \wp$, und nach [14, Lemma 3.3] gibt es dann $\wp \in \mathrm{Ass}_R N$ mit $I \subseteq \wp$. Zu $\wp$ gibt es dann ein $n \in N \setminus \{0\}$ mit $\wp = \mathrm{Ann}_R n$, und für $m \in M$ mit $n = m + (a_1, \ldots, a_k)M$ gilt dann $m \notin (a_1, \ldots, a_k)M$ aber $Im \subseteq (a_1, \ldots, a_k)M$. □

1.1.3 Die Cohen-Macaulay Eigenschaft

In diesem Abschnitt führen wir die Cohen-Macaulay Eigenschaft ein und bringen den Zusammenhang zwischen phsops und regulären Sequenzen.

Ab jetzt sei immer R eine graduierte affine K-Algebra und M ein endlich erzeugter graduierter R-Modul.

Für jedes Ideal $I \neq R$ gilt

$$\mathrm{depth}(I) \leq \mathrm{height}(I), \tag{6}$$

siehe [14, Proposition 18.2]. Daher ist die im Folgenden definierte Zahl stets größer gleich 0.

Definition 1.22 *Der* Cohen-Macaulay-Defekt *eines echten Ideals I von R ist die Differenz von Höhe und Tiefe,*

$$\mathrm{cmdef}(I) := \mathrm{height}(I) - \mathrm{depth}(I).$$

Der Cohen-Macaulay-Defekt *von R ist die Differenz von Krulldimension und Tiefe, also*

$$\mathrm{cmdef}(R) := \dim(R) - \mathrm{depth}(R) = \mathrm{cmdef}(R_+).$$

R heißt Cohen-Macaulay, *falls* $\mathrm{cmdef}(R) = 0$, *also wenn es eine homogene reguläre Sequenz der Länge* $\dim(R)$ *gibt.*

Beispielsweise sind Polynomringe $R = K[X_1, \ldots, X_n]$ Cohen-Macaulay, da offenbar die Folge der Variablen $X_1, \ldots, X_n$ eine reguläre Sequenz der Länge $n = \dim R$ bildet.

Satz 1.23 *(a) Jede homogene R-reguläre Sequenz $a_1, \ldots, a_k \in R_+$ erzeugt ein Ideal der Höhe k,* $\mathrm{height}(a_1, \ldots, a_k) = k$, *ist also insbesondere ein phsop.*

(b) Ist R Cohen-Macaulay, so ist auch umgekehrt jedes phsop (der Länge k) eine R-reguläre Sequenz (und erzeugt damit nach (a) ein Ideal der Höhe k).

(c) R ist genau dann Cohen-Macaulay, wenn für ein hsop $a_1, \ldots, a_n$ von R und $A := K[a_1, \ldots, a_n]$ der dann über A endlich erzeugte A-Modul R sogar frei ist. Wenn diese Eigenschaft für ein hsop gilt (also R Cohen-Macaulay ist), dann gilt sie sogar für jedes hsop.

Beweis. (a) Sei $a_1, \ldots, a_k$ eine homogene reguläre Sequenz. Diese ist dann natürlich maximal regulär in dem Ideal $(a_1, \ldots, a_k)_R$, und daher ist

$$k = \operatorname{depth}(a_1, \ldots, a_k)_R \overset{(6)}{\leq} \operatorname{height}(a_1, \ldots, a_k)_R \leq k,$$

wobei im letzten Schritt Krulls Hauptidealsatz verwendet wurde. Also gilt Gleichheit, und mit Lemma 1.5 ist $a_1, \ldots, a_k$ ein phsop.

(b) und (c). (i) Sei zunächst $a_1, \ldots, a_n$ ein hsop von R, $n = \dim R$, so dass R frei über $A := K[a_1, \ldots, a_n]$ ist. Dann gibt es $g_1, \ldots, g_m \in R$ mit

$$R = \bigoplus_{j=1}^{m} Ag_j \quad \text{und} \quad A \to Ag_j,\ a \mapsto ag_j \text{ injektiv für } j = 1, \ldots, m.$$

(Die zweite Bedingung, die für ein nichtnullteilerfreies R nötig ist um „R frei über A“ zu formulieren, wird in der Literatur oft vergessen.) Wir zeigen, dass dann $a_1, \ldots, a_n$ eine reguläre Sequenz ist - dann ist insbesondere R Cohen-Macaulay. Sei also $k \leq n$ und $r_1, \ldots, r_k \in R$ mit

$$r_1 a_1 + \ldots + r_k a_k = 0.$$

Zu $r_i \in \bigoplus_{j=1}^{m} Ag_j$, $i = 1, \ldots, k$ gibt es dann $p_{ij} \in A$, $j = 1, \ldots, m$ mit $r_i = \sum_{j=1}^{m} p_{ij} g_j$. Es folgt

$$\sum_{i=1}^{k} \sum_{j=1}^{m} p_{ij} g_j a_i = 0.$$

Aufgrund der Direktheit der Summe $R = \bigoplus_{j=1}^{m} Ag_j$ und der Injektivität von $A \to Ag_j$ folgt $\sum_{i=1}^{k} p_{ij} a_i = 0$ für $j = 1, \ldots, m$. Aus

$$p_{kj} a_k = -\sum_{i=1}^{k-1} p_{ij} a_i, \qquad j = 1, \ldots, m,$$

und weil A ein Polynomring ist, folgt, dass die rechte Seite (nach Zusammenfassen) nur aus Monomen besteht, von denen jedes durch a_k und wenigstens durch ein a_i, $i = 1, \ldots, k-1$ teilbar ist. Es folgt

$$p_{kj} \in Aa_1 + \ldots + Aa_{k-1} \quad j = 1, \ldots, m,$$

und daher

$$r_k = \sum_{j=1}^{m} p_{kj} g_j \in Ra_1 + \ldots + Ra_{k-1}.$$

Dies zeigt die Regularität der Folge $a_1, \ldots, a_n$, und da $n = \dim R$ ist R Cohen-Macaulay.

(ii) Sei nun umgekehrt R Cohen-Macaulay, also $\operatorname{depth} R = \dim R =: n$, und $a_1, \ldots, a_n$ ein hsop sowie $A = K[a_1, \ldots, a_n]$. Aufgrund des nachfolgenden Lemmas 1.24 ist dann ebenfalls

$\operatorname{depth}(A_+, R) = n$. Da R endlich erzeugter A-Modul ist, besitzt R nach dem Hilbertschen Syzygien Satz ([14, Cororllary 19.8]) eine endliche freie Auflösung über dem Polynomring A. Insbesondere ist damit die *projektive Dimension* von R als A-Modul endlich, $\operatorname{pd}_A R < \infty$. Damit sind die Voraussetzungen zur Anwendung der graduierten Auslander-Buchsbaum Formel (Eisenbud [14, Exercise 19.8]) erfüllt, und nach dieser gilt dann

$$\operatorname{pd}_A R = \operatorname{depth}(A_+, A) - \operatorname{depth}(A_+, R) = n - n = 0.$$

Daher gibt es eine projektive Auflösung von R der Länge 0, d.h. R ist selbst projektiv als A-Modul. Endlich erzeugte projektive graduierte Moduln über graduierten noetherschen Ringen sind aber frei ([14, Theorem 19.2]). Also ist R frei als A-Modul.

Zusammenfassend haben wir also gesehen: (i) Wenn es ein hsop gibt, so dass R frei über $A = K[hsop]$ ist, so ist dieses hsop eine reguläre Sequenz. Insbesondere ist R Cohen-Macaulay. (ii) Wenn R Cohen-Macaulay ist, so ist R frei über A. Insbesondere ist also nach (i) das zu A gehörige hsop eine reguläre Sequenz. Dies zeigt (b) und (c). □

So wie $\operatorname{cmdef} R = 0$ bedeutet, dass R frei über $A = K[hsop]$ ist, so bedeutet $\operatorname{cmdef} R = 1$, dass der erste Syzygien-Modul (der Generatoren von R als A-Modul) frei über A ist. Allgemein folgt aus der Auslander-Buchsbaum-Formel

$$\operatorname{pd}_A R = \operatorname{depth}(A_+, A) - \operatorname{depth}(A_+, R) = \dim R - \operatorname{depth} R = \operatorname{cmdef} R,$$

dass $\operatorname{cmdef} R = k$ äquivalent ist zur Existenz einer minimalen freien Auflösung

$$0 \to A^{n_k} \to \ldots \to A^{n_1} \to A^{n_0} \to R \to 0.$$

Also bedeutet $\operatorname{cmdef} R = k$, dass der k-te Syzygien-Modul $\operatorname{im}(A^{n_k} \to A^{n_{k-1}}) = \ker(A^{n_{k-1}} \to A^{n_{k-2}})$ (dabei „$A^{n_{-1}} := R,\ A^{n_{-2}} := 0$“) frei über A ist.

Ist M ein R-Modul und A ein Unterring von R (mit $1_R \in A$), so ist M auch ein A-Modul. Sind $a_1, \ldots, a_n \in A$, so gilt

$$(a_1, \ldots, a_n)M := (a_1, \ldots, a_n)_R M = (a_1, \ldots, a_n)_A M.$$

Beweis. Die Inklusion „$\supseteq$“ ist wegen $R \supseteq A$ offensichtlich. Ist $b = (\sum_{i=1}^n a_i r_i)\, m \in (a_1, \ldots, a_n)_R M$ mit $r_1, \ldots, r_n \in R$, $m \in M$, so ist wegen $r_i m \in M$ auch $b = \sum_{i=1}^n a_i (r_i m) \in (a_1, \ldots, a_n)_A M$. Da die betrachteten Elemente b den linken Modul erzeugen, zeigt dies die Inklusion „$\subseteq$“. □

Aufgrund dieser Eigenschaft kann man also den Index R bzw. A bei der betrachteten Menge weglassen.

Lemma 1.24 *Sei A eine graduierte affine Unteralgebra von R, so dass R ganz über A ist (z.B. A die von einem homogenen Parametersystem erzeugte Unteralgebra), und $M \neq 0$ ein endlich erzeugter graduierter R-Modul (z.B. $M = R$). Dann gilt*

$$\operatorname{depth}(R_+, M) = \operatorname{depth}(A_+, M),$$

d.h. die Tiefe von M als R-Modul ist gleich der Tiefe von M als A-Modul.

Beweis. (vgl. [12, Lemma 3.7.2].) Da R endlich erzeugt als A-Modul, ist auch M endlich erzeugt als A-Modul. Sei $a_1, \ldots, a_k \in A_+$ eine maximale M-reguläre Sequenz in A_+. Es genügt zu zeigen, dass diese auch in R_+ maximal ist (wegen Satz 1.16), also dass R_+ nur aus Nullteilern von $N := M/(a_1, \ldots, a_k)M$ besteht (wir nehmen hier die 0 auch als Nullteiler). Nach Voraussetzung besteht jedenfalls A_+ nur aus Nullteilern von N. Dann liegt A_+ erst recht in der Menge aller Nullteiler von N in R, welche nach [14, Theorem 3.1] gleich der Vereinigung der assoziierten Primideale von N in R, also gleich $\bigcup \operatorname{Ass}_R N$ ist. Dann gilt also $A_+ \subseteq \bigcup_{\mathcal{P} \in \operatorname{Ass}_R N} \mathcal{P} \cap A$, und rechts steht eine endliche ([14, Theorem 3.1]) Vereinigung von Primidealen von A. Nach dem Lemma über das Vermeiden von Primidealen [14, Lemma 3.3] liegt A_+ also in einem dieser Primideale, d.h. es gibt $\mathcal{P} \in \operatorname{Ass}_R N$ mit $A_+ \subseteq A \cap \mathcal{P} \subset A$ (da $1 \notin \mathcal{P}$). Da A_+ maximales Ideal ist (wg. $A/A_+ = K$), folgt also $A_+ = A \cap \mathcal{P}$. Nach Definition der Graduierung auf A gilt auch $A_+ = A \cap R_+$. Nach [14, Proposition 3.12] ist $\mathcal{P}$ ein homogenes Primideal, also $\mathcal{P} \subseteq R_+$. Da R/A ganz ist, gibt es zwischen den über A_+ liegendenen Primidealen $\mathcal{P}$ und R_+ aber keine echte Inklusion [14, Corollary 4.18]. Also gilt $\mathcal{P} = R_+$, d.h. als assoziiertes Primideal besteht R_+ nur aus Nullteilern von N. Dies war zu zeigen. □

Korollar 1.25 *Ist $a_1, \ldots, a_n$ ein hsop von R, so ist*

$$\operatorname{depth} R = \operatorname{depth}(a_1, \ldots, a_n)_R.$$

Beweis. Nach dem vorigen Lemma gilt mit $A := K[a_1, \ldots, a_n]$

$$\begin{aligned} \operatorname{depth}(R) &= \operatorname{depth}(R_+, R) = \operatorname{depth}(A_+, R) \\ &\leq \operatorname{depth}(A_+R, R) = \operatorname{depth}((a_1, \ldots, a_n)_R, R) \\ &\leq \operatorname{depth}(R_+, R) = \operatorname{depth}(R). \end{aligned}$$

Also gilt überall Gleichheit. □

Satz 1.26 *Sei R eine graduierte affine K-Algebra, und $I \neq R$ ein homogenes Ideal. Dann gilt*

$$\operatorname{cmdef} R \geq \operatorname{cmdef} I = \operatorname{height} I - \operatorname{depth} I.$$

Ist insbesondere R Cohen-Macaulay, so gilt für jedes homogene Ideal $I \neq R$

$$\operatorname{depth} I = \operatorname{height} I.$$

Beweis. Sei $a_1, \ldots, a_r$ eine maximale homogene reguläre Sequenz in I, also $\operatorname{depth} I = r$ (vgl. Sätze 1.16, 1.17). Dann gilt $\operatorname{height}(a_1, \ldots, a_r) = r$ (Satz 1.23 (a)). Nach Lemma 1.5 (b) gibt es homogene $a_{r+1}, \ldots, a_{r+k} \in I$ mit $\operatorname{height}(a_1, \ldots, a_{r+k}) = r+k = \operatorname{height}(I)$. Dann ist

$$k = \operatorname{height}(I) - \operatorname{depth}(I).$$

Nochmals nach Lemma 1.5 (b) (mit $I = R_+$) ergänze man $a_1, \ldots, a_{r+k}$ zu einer Menge homogener Elemente $a_1, \ldots, a_n \in R_+$ mit $n = \operatorname{height}(a_1, \ldots, a_n) = \operatorname{height} R_+ = \dim R$. Nach Lemma 1.5 (a) ist diese Menge insbesondere ein hsop von R. Es folgt

$$\begin{aligned} \operatorname{depth}(R) &= \operatorname{depth}((a_1, \ldots, a_n)_R, R) \quad \text{(Korollar 1.25)} \\ &\leq \operatorname{depth}((a_1, \ldots, a_{r+k})_R, R) + (n - r - k) \quad \text{(Korollar 1.20)}. \end{aligned}$$

Nun ist $(a_1, \ldots, a_{r+k})_R \subseteq I$, und $a_1, \ldots, a_r$ ist maximale reguläre Sequenz in I. Also ist es erst recht eine maximale reguläre Sequenz in $(a_1, \ldots, a_{r+k})_R$, d.h.

$$\operatorname{depth}((a_1, \ldots, a_{r+k})_R, R) = r$$

(Satz 1.16). Damit folgt aus obiger Ungleichung also $\operatorname{depth} R \leq r + (n - r - k) = n - k$, oder $k = \operatorname{height} I - \operatorname{depth} I \leq n - \operatorname{depth} R = \dim R - \operatorname{depth} R = \operatorname{cmdef} R$.

Ist nun R Cohen-Macaulay, also $\operatorname{cmdef} R = 0$, so gilt nach der gerade bewiesenen Ungleichung $0 \geq \operatorname{height}(I) - \operatorname{depth}(I)$, und wegen $\operatorname{depth}(I) \leq \operatorname{height}(I)$ (siehe (6)) gilt sogar Gleichheit. □

An der Stelle in obigem Beweis, bei der Korollar 1.25 verwendet wird, könnte man stattdessen auch nochmal Lemma 1.24 verwenden und dann mehrmals zwischen der Betrachtung von R als R- oder A-Modul hin und her wechseln. Die Betrachtung als A-Modul kann auch deshalb nützlich sein, weil Ideale in (dem Polynomring!) A oft besser überblickbar sind als in R.

Wir wollen für diesen Satz, der unser wichtigstes Hilfsmittel sein wird, noch den „Lehrbuch“-Beweis angeben (in den Lehrbüchern findet sich - wie fast immer - nur der Fall noetherscher lokaler Ringe aufgeschrieben). Die folgende Proposition ist dabei auch von unabhängigem Interesse.

Proposition 1.27 *Sei R eine graduierte affine Algebra und $M \neq 0$ ein endlich erzeugter graduierter R-Modul. Dann gilt für jedes assoziierte Primideal $\wp \in \operatorname{Ass}_R M$*

$$\operatorname{depth}(R_+, M) \leq \dim(R/\wp).$$

Bemerkung. Hieraus folgt mit $\dim M := \dim R/\operatorname{Ann}_R M = \max\{\dim R/\wp \mid \wp \in \operatorname{Ass}_R M\}$ auch $\operatorname{depth} M \leq \dim M$.

Beweis. (Bruns und Hezog [6, Proposition 1.2.13] oder [40, Satz VII.2.3] für den lokalen Fall). Wir machen Induktion nach der Tiefe $\operatorname{depth}(R_+, M)$. Ist diese gleich 0, so ist die Aussage klar. Sei also $\operatorname{depth}(R_+, M) > 0$. Dann gibt es eine homogene M-reguläre Sequenz $a \in R_+$ der Länge 1, und es gilt $\operatorname{depth}(R_+, M/(a)M) = \operatorname{depth}(R_+, M) - 1$ (Satz 1.16). Nach Induktion gilt also

$$\operatorname{depth}(R_+, M/(a)M) \leq \dim(R/\mathcal{P}) \quad \text{für alle } \mathcal{P} \in \operatorname{Ass}_R M/(a)M. \tag{7}$$

Da $\wp \in \operatorname{Ass}_R M$ und M noethersch ist, gibt es ein nach [14, Proposition 3.12] *homogenes* $0 \neq m \in M$, so dass Rm maximaler von einem homogenen Element erzeugter Modul mit der Eigenschaft $\wp \cdot Rm = 0$ ist. Dann ist die Restklasse $\bar{m}$ von m in $M/(a)M$ ungleich Null:

Sei nämlich stattdessen $m \in (a)M$, also $m = am'$ mit $m' \in M$. Da m und a homogen, und a kein Nullteiler ist, ist dann auch m' homogen. Wegen $0 = \wp \cdot m = a \cdot \wp m'$ und der M-Regularität von a wäre dann auch $\wp \cdot m' = 0$, also $\wp \cdot Rm' = 0$ und $Rm \subseteq Rm'$. Da $\deg a > 0, m \neq 0$ und $m = am'$ ist jedoch $\deg m' < \deg m$, also $Rm \subset Rm'$ im Widerspruch zur Maximalität von Rm.

Da also $\bar{m} \neq 0$ und $\wp \cdot \bar{m} = 0$, besteht $\wp$ nur aus Nullteilern von $M/(a)M$ und liegt daher in einem assoziierten Primideal $\mathcal{P} \in \operatorname{Ass}_R M/(a)M$, $\wp \subseteq \mathcal{P}$. Weiter ist $a \notin \wp$ (da a M-regulär und $\wp \in \operatorname{Ass}_R M$) aber $a \in \mathcal{P}$ (da $a \in \operatorname{Ann}_R M/(a)M \subseteq \mathcal{P}$), also $\wp \subset \mathcal{P}$. Mit Gleichung (7) folgt also

$$\operatorname{depth}(R_+, M) - 1 = \operatorname{depth}(R_+, M/(a)M) \leq \dim R/\mathcal{P} \leq \dim R/\wp - 1$$

und damit die Behauptung. □

Korollar 1.28 *Sei R eine graduierte affine Algebra und $I \neq R$ ein homogenes Ideal. Dann gilt*

$$\operatorname{depth} R \leq \operatorname{depth} I + \dim I.$$

Insbesondere gilt $\operatorname{cmdef} R \geq \operatorname{cmdef} I$.

Beweis. (Bruns und Herzog [6, Exercise 1.2.23]). Sei $a_1, \ldots, a_k \in I$ eine maximale homogene reguläre Sequenz in I, also $k = \operatorname{depth}(I, R)$. Wir wählen $M := R/(a_1, \ldots, a_k)$ in der Proposition. Da I nur aus Nullteilern von M besteht, also $I \subseteq \bigcup_{\wp \in \operatorname{Ass}_R M} \wp$, gibt es ein $\wp \in \operatorname{Ass}_R M$ mit $I \subseteq \wp$. Mit der Proposition und Satz 1.16 gilt dann

$$\operatorname{depth}(R_+, M) = \operatorname{depth} R - k \leq \dim R/\wp \leq \dim R/I,$$

also $\operatorname{depth} R \leq \operatorname{depth} I + \dim I$. Da in jeder affinen Algebra $\dim I + \operatorname{height} I \leq \dim R$ gilt (Proposition 1.1), folgt hieraus auch $\operatorname{depth} R \leq \operatorname{depth} I + \dim R - \operatorname{height} I$. □

1.2 Lineare algebraische Gruppen und G-Moduln

In diesem Abschnitt beziehen sich topologische Begriffe immer auf die Zariski-Topologie. Dabei ist eine Teilmenge von K^n genau dann abgeschlossen, wenn sie eine affine Varietät ist, d.h. Nullstellenmenge eines Systems von Polynomen in $K[X_1, \ldots, X_n]$. Morphismen sind Abbildungen zwischen affinen Varietäten, die durch Polynome gegeben sind.

Definition 1.29 *Eine* lineare algebraische Gruppe *ist eine affine Varietät $G \subseteq K^r$ zusammen mit Morphismen $\cdot : G \times G \to G$ und $^{-1} : G \to G$, so dass $(G, \cdot)$ zusammen mit der durch $^{-1}$ gegebenen Inversenbildung eine Gruppe wird.*

Wenn nicht anders vermerkt, bezeichnen wir das Einselement einer Gruppe immer mit ι.

Standardvoraussetzung. Ab jetzt bezeichnen wir mit G stets eine lineare algebraische Gruppe, und mit V einen G-Modul (siehe die folgende Definition).

Definition 1.30 *Ein* G-Modul *oder eine* rationale Darstellung von G *ist ein endlichdimensionaler K-Vektorraum V zusammen mit einer linearen Operation von G auf V, die durch einen Morphismus $G \to \mathrm{GL}(V)$ gegeben ist.*

In der üblichen Weise wird V dann Linksmodul über dem (im Allgemeinen nichtkommutativen) *Gruppenring* KG. Dabei handelt es sich um den K-Vektorraum mit Basis G, der durch distributive Fortsetzung der Multiplikation von G zu einem Ring wird.

Bemerkung 1.31 Ist $V = K^n$, so ist $\mathrm{GL}(V) = \mathrm{GL}_n$ als affine Varietät realisiert durch die Menge

$$X := \left\{(A, e) \in K^{n \times n} \times K : e \cdot \det A - 1 = 0\right\}.$$

Sind $f_{ij} \in K[G]$, $i, j = 1, \ldots, n$ so, dass durch $f : G \to \mathrm{GL}_n$, $\sigma \mapsto (f_{ij}(\sigma))_{i,j}$ ein Gruppenhomomorphismus gegeben ist, so ist durch $F : G \to X$, $\sigma \mapsto \big(f(\sigma), \det(f(\sigma^{-1}))\big)$ ein Morphismus (und damit eine rationale Darstellung von G) gegeben; Denn $\sigma \mapsto \sigma^{-1}$ ist ein Morphismus (also durch Polynome gegeben), und damit auch $\sigma \mapsto \det(f(\sigma^{-1}))$, und es ist $\det f(\sigma^{-1}) \det f(\sigma) = \det f(\sigma^{-1}\sigma) = 1$.

Die *d-te symmetrische Potenz* $S^d(V)$ eines G-Moduls V besteht aus den „homogenen Polynomen vom Grad d in den Basiselementen von V und der Null“ - genauer handelt es sich um den Faktormodul des d-fachen Tensorproduktes von V mit sich selbst modulo allen Relationen, die Polynome erfüllen (Kommutativität). Insbesondere setzt man $S^0(V) := K$. $S^d(V)$ ist in kanonischer Weise ebenfalls ein G-Modul.

Ein Homomorphismus linearer algebraischer Gruppen G, H ist ein Morphismus $f : G \to H$, der zugleich ein Gruppenhomomorphismus ist. (Insbesondere ist ein G-Modul V also nichts anderes als ein algebraischer Homomorphismus $G \to \mathrm{GL}(V)$). Dann ist $f(G) \subseteq H$ automatisch eine *abgeschlossene* Untergruppe von H ([59, Proposition 2.2.5 (ii)]). Zwei lineare algebraische Gruppen G, H heißen (algebraisch) isomorph, wenn es einen Isomorphismus von Gruppen $f : G \to H$ gibt, so dass f und f^{-1} Morphismen von Varietäten sind.

Bemerkung 1.32 (Normalteiler und Faktorgruppen) Ist N ein abgeschlossener Normalteiler von G, so kann man G/N die Struktur einer linearen algebraischen Gruppe geben, derart dass die kanonische Abbildung $G \to G/N$ ein Homomorphismus linearer algebraischer Gruppen wird ([59, Proposition 5.2.5] oder [29, Theorem 11.5] zusammen mit [59, Proposition 2.2.5 (ii)]).

Ist X eine affine Varietät und $f : G \to X$ ein Morphismus von affinen Varietäten mit $f(gn) = f(g)$ für alle $g \in G, n \in N$, so induziert f einen *Morphismus* von affinen Varietäten $G/N \to X,\ gN \mapsto f(g)$ ([59, Exercise 5.2.6 (2)] oder [29, Section 12.3]).

Ist V ein G-Modul, so ist V^N ein G/N-Modul. Ist nämlich $v \in V^N$ und $g \in G$, so gibt es zu $n \in N$ ein $n' \in N$ mit $ng = gn'$, also ist $n \cdot gv = g \cdot n'v \overset{v \in V^N}{=} gv$, also $gv \in V^N$, und damit ist V^N ein G-Untermodul. Weiter ist für $g \in G$, $n \in N$ stets $gn \cdot v \overset{v \in V^N}{=} g \cdot v$. Damit ist der Morphismus $G \to \mathrm{GL}(V^N)$ konstant auf den Nebenklassen von N und induziert damit nach oben einen Morphismus $G/N \to \mathrm{GL}(V^N)$, so dass V^N also ein G/N-Modul ist.

Satz 1.33 *Jede lineare algebraische Gruppe ist (algebraisch) isomorph zu einer abgeschlossenen Untergruppe einer geeigneten* $\mathrm{GL}_n(K)$*. Dann ist* $V = K^n$ *ein* G*-Modul mit einer treuen Darstellung* $G \to \mathrm{GL}(V)$*.*

Beweis. Siehe [59, Theorem 2.3.6] □

Eigenschaften, die Matrixgruppen bzw. ihren Elementen zukommen, können so auch linearen algebraischen Gruppen zugeordnet werden, indem man sie mittels dieses Satzes als Untergruppe einer $\mathrm{GL}_n(K)$ auffasst. So heißt ein $\sigma \in G \subseteq \mathrm{GL}_n(K)$ *unipotent*, wenn es ein $k \in \mathbb{N}$ gibt mit $(\sigma - \iota)^k = 0 \in K^{n \times n}$ (hier ist $\iota = I_{n \times n} \in K^{n \times n}$ die Einheitsmatrix). G heißt *unipotent*, wenn jedes ihrer Elemente unipotent ist. Ein Element $\sigma \in G \subseteq \mathrm{GL}_n(K)$ heißt *halbeinfach*, wenn σ ähnlich zu einer Diagonalmatrix ist. (Achtung: Eine Gruppe heißt *nicht* halbeinfach, wenn jedes ihrer Elemente halbeinfach ist!)

Die Eigenschaften „unipotent“ und „halbeinfach“ sind dabei wohldefiniert, denn wenn sie für das Bild eines $\sigma \in G$ unter *einer* treuen rationalen Darstellung $G \to \mathrm{GL}_n(K)$ gelten, so auch für das Bild unter *jeder* solchen Darstellung (siehe [59, Theorem 2.4.8]).

Satz und Definition 1.34 *Mit* G^0 *bezeichnen wir die Zusammenhangskomponente von* G*, die das neutrale Element* ι *enthält. Sie ist die eindeutig bestimmte irreduzible Komponente von* G*, die* ι *enthält, und ein abgeschlossener Normalteiler von* G *von endlichem Index.* G *heißt* zusammenhängend*, wenn* $G = G^0$*. (Siehe [59, Proposition 2.2.1]).*

Definition 1.35 *G heißt* reduktiv*, wenn jeder abgeschlossene, zusammenhängende und unipotente Normalteiler von G trivial ist, d.h. nur aus dem Einselement ι besteht.*

Alle klassischen Gruppen $\mathrm{SL}_n, \mathrm{GL}_n, \mathrm{Sp}_n, \mathrm{SO}_n, \mathrm{O}_n$ sind in allen Charakteristiken reduktiv (siehe etwa [54, Chapter 5.9]). Auch alle endlichen Gruppen sind reduktiv, da die einzige zusammenhängende Untergruppe die Einsgruppe $\{\iota\}$ ist. Dagegen sind die additiven Gruppen $\mathbb{G}_a = (K, +)$ nicht reduktiv, da sie selbst zusammenhängend und unipotent sind.

Definition 1.36 *G heißt* linear reduktiv*, wenn jeder G-Modul vollständig reduzibel ist. D.h. für jeden G-Modul V und jeden G-Untermodul $U \leq V$ existiert ein Komplement, d.h. ein G-Untermodul $W \leq V$ mit $V = U \oplus W$.*

Wir werden noch sehen, dass jede linear reduktive Gruppe auch reduktiv ist. Die klassischen Gruppen sind nur in Charakteristik 0 linear reduktiv. In positiver Charakteristik gibt es nur sehr wenige linear reduktive Gruppen. Es gilt nämlich

Satz 1.37 (Nagata [45]) *Sei* $\operatorname{char} K = p > 0$*. G ist genau dann linear reduktiv, wenn G^0 ein Torus ist und $(G : G^0)$ nicht durch p teilbar ist.*

Diesen Satz können wir erst auf Seite 36 beweisen. Deshalb werden wir Teile von ihm in den folgenden Sätzen nochmals formulieren und ihn dann aus diesen folgern.

Dabei ist ein Torus eine zu einer $\mathbb{G}_m^k$ isomorphe Gruppe ($k \geq 0$), wobei $\mathbb{G}_m = \mathrm{GL}_1 = \{(a, b) \in K^2 : ab - 1 = 0\} \cong (K \setminus \{0\}, \cdot)$ die multiplikative Gruppe des Körpers ist. Tori sind in allen Charakteristiken linear reduktiv [59, Theorem 2.5.2], in positiver Charakteristik sind sie nach obigem Satz sogar die einzigen zusamenhängenden und linear reduktiven Gruppen.

Interessanterweise genügt für die lineare Reduktivität sogar die Forderung, dass ein *spezieller* G-Modul vollständig reduzibel ist. Zunächst noch eine

Bemerkung und Definition 1.38 *Sei G eine lineare algebraische Gruppe,* $\operatorname{char} K = p > 0$*, und V ein G-Modul mit Basis $\{X_1, \ldots, X_n\}$. Dann ist der Untervektorraum $\langle X_1^p, \ldots, X_n^p \rangle_K$ von $S^p(V)$ wegen des Frobenius-Homomorphismus sogar ein G-Untermodul und unabhängig von der speziellen Wahl der Basis von V. Daher kann er basisunabhängig bezeichnet werden als die p-te* Frobenius-Potenz von V*,*

$$F^p(V) := \langle X_1^p, \ldots, X_n^p \rangle_K \subseteq S^p(V).$$

Offenbar besteht $F^p(V)$ genau aus den p-ten Potenzen aller Elemente aus V, also

$$F^p(V) = \{ f \in S^p(V) : \text{ es gibt } v \in V \text{ mit } f = v^p \}.$$

Satz 1.39 (Nagata [45]) *Sei G eine lineare algebraische Gruppe, V ein* treuer G*-Modul (existiert stets nach Satz 1.33) und* $p = \operatorname{char} K$*.*

(a) Ist $p = 0$, so ist G genau dann linear reduktiv, wenn V vollständig reduzibel ist.

(b) Ist $p > 0$ und G zusätzlich zusammenhängend*, so ist G genau dann linear reduktiv, wenn der Untermodul $F^p(V)$ von $S^p(V)$ ein Komplement in $S^p(V)$ hat. Dies ist weiter genau dann der Fall, wenn G ein Torus ist.*

Beweis. (a) Siehe [45, Theorem 3].

(b) ist im Beweis von [45, Theorem 1] versteckt. Da Nagatas Beweis etwas kryptisch ist und wir das Resultat an entscheidender Stelle verwenden werden, bringen wir der Vollständigkeit halber einen geglätteten Beweis im folgenden Unterabschnitt. Diesen Teil werden wir auch zum Beweis von Satz 1.37 verwenden. □

Korollar 1.40 *Sei* $\operatorname{char} K = p > 0$*, G eine lineare algebraische Gruppe, so dass die Zusammenhangskomponente G^0 kein Torus ist, und V ein* treuer G*-Modul. Dann hat der Untermodul $F^p(V)$ von $S^p(V)$ kein Komplement in $S^p(V)$. Insbesondere ist G nicht linear reduktiv.*

Beweis. Da G^0 kein Torus ist, hat nach Satz 1.39 (b) dann $F^p(V)$ (welches sowohl G^0-, G- als auch $\mathrm{GL}(V)$-Untermodul ist) kein G^0-invariantes Komplement in $S^p(V)$. Dann gibt es erst recht kein G-invariantes Komplement, und damit ist G nicht linear reduktiv. □

Unter einer speziellen Zusatzvoraussetzung, die für viele Darstellungen klassischer Gruppen erfüllt ist, wollen wir kurz noch einen sehr *anschaulichen Beweis* dafür geben, dass $F^p(V)$ kein Komplement in $S^p(V)$ hat. Wir nehmen an, dass $G \subseteq \mathrm{GL}(V)$ eine nichttriviale abgeschlossene unipotente Untergruppe U enthält, so dass $S(V)^U = K[f]$ mit einem $f \in V$ gilt. (Da U nichttrivial folgt $\dim V \geq 2$. Weiter ist $U^0 \subseteq G^0$ eine abgeschlossene, zusammenhängende nichttriviale unipotente Untergruppe, so dass G^0 kein Torus ist - es handelt sich also tatsächlich um eine Zusatzvoraussetzung). Insbesondere ist dann $\dim S^p(V)^U = \dim K[f]_p = 1$. Wäre nun $S^p(V) = F^p(V) \oplus W$ mit einem G- (also erst recht U-) invarianten Komplement W, so enthielten (etwa nach Springer [59, Theorem 2.4.11]) sowohl $F^p(V)$ als auch $W \neq 0$ (wegen $\dim V \geq 2$) eine von 0 verschiedene U-Invariante, also $\dim S^p(V)^U \geq 2$, Widerspruch.

Hier nun eine Situation, unter der die gemachte Voraussetzung gilt. Wir betrachten $V = \langle X_1, \ldots, X_n \rangle$ als Dual von $V^* := K^n = \langle e_1, \ldots, e_n \rangle$ (mit Standardbasis), also $X_i(e_j) = \delta_{ij}$ für alle i, j. Sei weiter $U \subseteq \mathrm{GL}(V)$ eine abgeschlossene Gruppe oberer Dreiecksmatrizen mit $\overline{U \cdot e_1} = \{e_1 + \sum_{i=2}^n \lambda_i e_i : \lambda_i \in K\}$ (Zariski-Abschluss) $(*)$. Dann gilt $S(V)^U = K[V^*]^U = K[X_1]$. Offenbar ist nämlich $X_1 \in K[V^*]^U$. Sei umgekehrt $f = f(X_1, \ldots, X_n) \in K[V^*]^U$. Für ein festes $x_1 \in K \setminus \{0\}$ gilt dann wegen $f \in K[V^*]^U$ stets $f((x_1, 0, \ldots, 0)) = f(\sigma(x_1, 0, \ldots, 0))$ für alle $\sigma \in U$. Wegen $(*)$ und weil Multiplikation mit $x_1 \neq 0$ ein Homöomorphismus ist, gilt dann $f((x_1, 0, \ldots, 0)) = f((x_1, x_2, \ldots, x_n))$ für alle $x_i \in K$ mit $x_1 \neq 0$. Weil die Menge der $x_1 \neq 0$ Zariski-dicht in K liegt, gilt dies dann auch für $x_1 \in K$ beliebig. Insbesondere erhalten wir damit

$$f((x_1, x_2, \ldots, x_n)) = f((x_1, 0, \ldots, 0)) = f(X_1, 0, \ldots, 0)(x_1, x_2, \ldots, x_n)$$

für alle $x_i \in K$, und weil $|K| = \infty$ dann $f = f(X_1, 0, \ldots, 0) \in K[X_1]$. □

Dagegen ist etwa für $\operatorname{char} K = 2$, $G = Z_2 = \{\iota, \sigma\}$ (also $G^0 = \{\iota\}$ ein Torus) und $V = \langle X, Y \rangle$ die reguläre Darstellung (mit $\sigma X = Y$, $\sigma Y = X$) durch $K \cdot XY$ ein Komplement zu $F^2(V)$ in $S^2(V)$ gegeben. Dennoch gilt die Aussage des Satzes in vielen weiteren Fällen, etwa wenn $p \geq 3$ und $G \subseteq \mathrm{GL}(V)$ eine *Transvektion* enthält, siehe Satz 4.6 und die anschliessenden Bemerkungen nach dessen Beweis.

Wir führen nun für den Rest der Arbeit noch etwas **Notation** ein: Ist V ein G-Modul, so meinen wir mit $V = \langle X_1, \ldots, X_n \rangle$, dass $\{X_1, \ldots, X_n\}$ eine Basis von V als K-Vektorraum ist, und eine eventuelle Darstellung $G \to \mathrm{GL}_n(K)$, $\sigma \mapsto A_\sigma$ bezüglich dieser Basis berechnet wird. Ist $G \subseteq \mathrm{GL}_n(K)$, so bezeichnen wir mit $\langle X_1, \ldots, X_n \rangle$ auch die *natürliche Darstellung* von G, also für $\sigma = (a_{ij}) \in \mathrm{GL}_n(K)$ soll $\sigma X_j = \sum_{i=1}^n a_{ij} X_i$ gelten. Im Fall $n = 2$ schreiben wir meist X und Y statt X_1 und X_2. Symmetrische Potenzen schreiben wir entsprechend als homogene Polynome in den Basisvektoren, etwa $S^2(\langle X, Y \rangle) = \langle X^2, Y^2, XY \rangle$.

Wir werden auch häufig den bekannten **Kalkül** zum Rechnen mit Darstellungen verwenden: Hat $V = \langle X_1, \ldots, X_n \rangle$ die Darstellung $\sigma \mapsto A_\sigma = (a_{ij}^\sigma)$, so hat der *Dual* $V^* = \mathrm{Hom}_K(V, K) = \langle X_1^*, \ldots, X_n^* \rangle$ mit Operation $\sigma \cdot \varphi := \varphi \circ \sigma^{-1}$ (mit $\varphi \in V^*, \sigma \in G$) bezüglich der angegebenen *Dualbasis* (also $X_i^*(X_j) = \delta_{ij}$) die Darstellung $\sigma \mapsto A_{\sigma^{-1}}^T$.

Ist $W = \langle Y_1, \ldots, Y_m \rangle$ ein weiterer G-Modul mit Darstellung $\sigma \mapsto B_\sigma$, so hat $V \otimes W = \langle X_1 \otimes Y_1, \ldots, X_1 \otimes Y_m, \ldots, X_n \otimes Y_1, \ldots, X_n \otimes Y_m \rangle$ die Darstellung $\sigma \mapsto A_\sigma \otimes B_\sigma := (a_{ij}^\sigma B_\sigma)_{i,j=1,\ldots,n}$ (Block-Matrix, Kronecker-Produkt von Matrizen). Ist $T = (t_{ij})$ Koordinatenmatrix eines Elements $t = \sum_{i,j} t_{ij} X_i \otimes Y_j \in V \otimes W$, so hat $\sigma \cdot t$ die Koordinatenmatrix $A_\sigma T B_\sigma^T$.

1.2.1 Beweis von Satz 1.39 (b)

Wir benötigen zunächst noch zwei Lemmata über zusammenhängende lineare algebraische Gruppen.

Lemma 1.41 *Falls jedes Element einer* zusammenhängenden *linearen algebraischen Gruppe G halbeinfach ist, dann ist G ein Torus.*

Beweis. Da das einzige halbeinfache und unipotente Element einer Gruppe das Einselement ι ist, also insbesondere $\{\iota\}$ die einzige unipotente Untergruppe von G ist, ist G nach Definition reduktiv. Als zusammenhängende reduktive Gruppe wird G nach Humphreys [29, Theorem 26.3(d)] von einem maximalen Torus und den „Wurzeluntergruppen“ erzeugt. Da die Wurzeluntergruppen nur aus unipotenten Elementen bestehen (ebenfalls [29, Abschnitt 26.3]), sind sie also trivial, und damit ist G ein Torus. □

Ich danke Frank Himstedt für die Hilfe bei diesem Beweis; In Nagatas Arbeit [45, Lemma 3] steht hierzu einfach: „the following was proved by Borel“.

Lemma 1.42 *Ist G zusammenhängend und $u \in G$ unipotent, so existiert eine abgeschlossene, zusammenhängende, unipotente Untergruppe U von G mit $u \in U$.*

Beweis. Nach [59, Theorem 7.3.3 (i)] liegt u in einer zusammenhängenden, abgeschlossenen auflösbaren Untergruppe B von G, einer sog. „Boreluntergruppe“ (vgl. [59, vor Theorem 7.2.6]). Für die auflösbare, zusammenhängende Gruppe B bildet die Menge all ihrer unipotenten Elemente U nach [59, Corollary 6.9 (ii)] ebenfalls eine abgeschlossene, zusammenhängende, unipotente Untergruppe, und offenbar ist $u \in U$. □

Schliesslich noch ein einfaches Lemma über das Transformationsverhalten gewisser Koordinatenringe.

Lemma 1.43 *Sei $V \subseteq K^{m\times n}$ eine affine Varietät, $\sigma \in \mathrm{GL}_m, \tau \in \mathrm{GL}_n$ und $W := \sigma V \tau \subseteq K^{m\times n}$. Dann ist $\varphi : V \to W,\ v \mapsto \sigma v \tau$ ein Isomorphismus von Varietäten. Seien $K[V] = K[X_{ij} : i = 1,\dots,m,\ j = 1,\dots,n]$ und $K[W] := K[Y_{ij} : i = 1,\dots,m,\ j = 1,\dots,n]$ jeweils die Koordinatenringe mit $X_{ij}(v) = v_{ij}$, $v = (v_{ij}) \in V$ bzw. $Y_{ij}(w) = w_{ij}$, $w = (w_{ij}) \in W$. Sei $\varphi^* : K[W] \to K[V], f \mapsto f \circ \varphi$ der zu φ gehörige Isomorphismus der Koordinatenringe. Dann gilt*

$$(\varphi^*(Y_{ij}))_{\substack{i=1,\dots,m\\ j=1,\dots,n}} = \sigma \cdot (X_{ij})_{\substack{i=1,\dots,m\\ j=1,\dots,n}} \cdot \tau.$$

Außerdem ist

$$\begin{aligned}\varphi^*(K[Y_{ij}^p : 1 \le i \le m,\ 1 \le j \le n]) &= K[\varphi^*(Y_{ij})^p : 1 \le i \le m,\ 1 \le j \le n]\\ &= K[X_{ij}^p : 1 \le i \le m,\ 1 \le j \le n]).\end{aligned}$$

Beweis. Da φ Einschränkung eines linearen Isomorphismus von $K^{m\times n}$ ist, ist klar dass auch W eine Varietät, φ ein Isomorphismus von Varietäten sowie φ^* ein Isomorphismus der Koordinatenringe ist. Sei nun $v = (v_{ij}) \in V, \sigma = (\sigma_{ij}) \in \mathrm{GL}_m, \tau = (\tau_{ij}) \in \mathrm{GL}_n$. Dann ist

$$\begin{aligned}\varphi^*(Y_{ij})(v) &= Y_{ij}(\varphi(v)) = Y_{ij}(\sigma v \tau)\\ &= \sum_{k=1,\dots,m,l=1,\dots,n} \sigma_{ik} v_{kl} \tau_{lj}\\ &= \sum_{k=1,\dots,m,l=1,\dots,n} \sigma_{ik} X_{kl} \tau_{lj}(v) \qquad \text{für alle } v \in V,\end{aligned}$$

also gilt die angegebene Transformationsformel. Die letzte Aussage des Satzes folgt mit dem Frobenius-Homomorphismus. □

Damit kommen wir zum

Beweis von Satz 1.39 (b). Es sei G eine zusammenhängende lineare algebraische Gruppe, $\operatorname{char} K = p > 0$, $V = K^n = \langle X_1, \dots, X_n\rangle$ ein G-Modul mit der treuen rationalen Darstellung $\rho : G \to \mathrm{GL}(V) = \mathrm{GL}_n$ und

$$W := F^p(V) = \langle X_1^p, \dots, X_n^p\rangle \subseteq S^p(V).$$

Wenn G ein Torus ist, so ist G nach Springer [59, Theorem 2.5.2 (c)] linear reduktiv (der Beweis ist elementar führbar). Wenn G linear reduktiv ist, so ist klar, dass W ein Komplement in $S^p(V)$ hat.

Sei nun umgekehrt $U \subseteq S^p(V)$ ein G-Untermodul mit

$$S^p(V) = U \oplus W.$$

Wir zeigen, dass dann G ein Torus ist. Angenommen, G sei *kein* Torus. Nach Lemma 1.41 ist dann nicht jedes Element von G halbeinfach. Da es für jedes $x \in G$ nach [59, Theorem 2.4.8] eine eindeutige Zerlegung $x = x_h x_u$ mit $x_h \in G$ halbeinfach und $x_u \in G$ unipotent gibt, enthält also G ein vom neutralen Element verschiedenes unipotentes Element. Dieses liegt dann nach Lemma 1.42 in einer nichttrivialen, zusammenhängenden, abgeschlossenen unipotenten Untergruppe H von G. Dann ist auch $\rho(H) \subseteq \mathrm{GL}_n$ eine nichttriviale, zusammenhängende, abgeschlossene unipotente Untergruppe von GL_n (Springer [59, Proposition

2.2.5, Theorem 2.4.8]). Da $S^p(V), U, W$ erst recht H- bzw. $\rho(H)$-Moduln sind, können wir ab jetzt $G = \rho(H)$ annehmen, um die Existenz der Zerlegung $S^p(V) = U \oplus W$ für eine abgeschlossene, zusammenhängende, unipotente, nichttriviale Gruppe $G \subseteq \mathrm{GL}_n$ zum Widerspruch zu führen. Nach [59, 2.4.11] gibt es ein $\sigma \in \mathrm{GL}_n$, so dass alle Elemente aus $\sigma G \sigma^{-1}$ obere Dreiecksmatrizen sind. Dann sind $\sigma S^p(V) = S^p(V)$, σU und $\sigma W = W$ (Frobenius-Homomorphismus!) jeweils $\sigma G \sigma^{-1}$-Moduln, und damit $S^p(V) = \sigma U \oplus W$, d.h. W hat auch als $\sigma G \sigma^{-1}$-Modul ein Komplement. Wir nehmen also weiter an, dass alle Elemente aus G bereits obere Dreiecksmatrizen sind. Für $\sigma = (\sigma_{ij})_{i,j=1,\dots,n} \in G$ gilt also $\sigma_{ii} = 1$ für $i = 1, \dots, n$ und $\sigma_{ij} = 0$ für $i > j$. Wir können also G als abgeschlossene Teilmenge von $K^{\frac{1}{2}n(n-1)}$ auffassen, d.h. wir identifizieren $\sigma \in G$ mit $(\sigma_{ij})_{1 \le i < j \le n} \in K^{\frac{1}{2}n(n-1)}$. Der entsprechende Koordinatenring von G ist dann

$$K[G] = K\left[S_{ij} : 1 \le i < j \le n\right] \quad \text{mit } S_{ij}(\sigma) = \sigma_{ij} \text{ für } \sigma = (\sigma_{ij}) \in G.$$

(Denn es ist $S_{ii} = 1$ und $S_{ij} = 0$ für $i > j$.) Wir setzen

$$A := K\left[S_{ij}^p : 1 \le i < j \le n\right] = \{f^p : f \in K[G]\},$$

die Unteralgebra von $K[G]$, die aus allen p-ten Potenzen besteht.
Behauptung: Es existiert $1 \le k < l \le n$ mit $S_{kl} \notin A$.

Denn nach Humphreys [29, Corollary 17.5] ist G als unipotente Gruppe nilpotent, also auflösbar. Da G auch zusammenhängend und kein Torus ist, gibt es nach Springer [59, Lemma 6.10] eine abgeschlossene Untergruppe $H \le G$ mit $H \cong \mathbb{G}_a$. Daher gibt es Morphismen $f : \mathbb{G}_a \to H$ und $g : H \to \mathbb{G}_a$ mit $g(f(t)) = t$ für alle $t \in \mathbb{G}_a$. Zu f gibt es dann Polynome in einer Variable $f_{ij} \in K[T]$ mit $f(t) = (f_{ij}(t))_{i,j=1,\dots,n} \in H \le G$. Da $g((f_{ij}(t))_{i,j=1,\dots,n}) = t$ und g ebenfalls durch Polynome gegeben ist, gibt es wenigstens ein Indexpaar (k,l), so dass T als Monom in f_{kl} vorkommt. Dann gilt $k < l$, denn $f_{ii} = 1$ für alle i und $f_{ij} = 0$ für alle $i > j$. Es folgt $f_{kl}(T) \notin K[f_{ij}^p(T) : 1 \le i < j \le n]$, denn in keinem Element der rechten Seite kommt T als Monom vor. Damit ist erst recht $S_{kl} \notin A$, sonst gäbe es nämlich $F \in K[G]$ mit $S_{kl} = F^p$, und auswerten an der Stelle $f(t) \in G$ liefert $f_{kl}(t) = F^p((f_{ij}(t))_{i,j=1,\dots,n})$ für alle $t \in \mathbb{G}_a$, also doch $f_{kl}(T) = F^p((f_{ij}(T))_{i,j=1,\dots,n}) \in K[f_{ij}^p(T) : 1 \le i < j \le n]$ - Widerspruch. Dies zeigt die Behauptung.

Aufgrund der Behauptung existiert nun genau ein Indexpaar (k,l), so dass gilt

- $S_{kl} \notin A, \quad S_{ij} \in A$ für $i \le j < l, \quad S_{il} \in A$ für $i < k \qquad$ (dabei ist $k < l$). $\qquad (*)$

Man erhält es, indem man erst ein maximales l wählt so dass $S_{ij} \in A$ für alle $i \le j < l$ gilt und dann das kleinste k mit $S_{kl} \notin A$. Auf der Menge $\{(i,j) : 1 \le i < j \le n\}$ führen wir nun folgende Ordnung ein:

$$(i_1, j_1) < (i_2, j_2) :\Leftrightarrow j_1 < j_2 \text{ oder } j_1 = j_2,\ i_1 < i_2.$$

Für jede unipotente, obere Dreiecksmatrix $\tau \in \mathrm{GL}_n$ ist $\tau G \tau^{-1}$ ebenfalls eine zusammenhängende, unipotente Gruppe oberer Dreiecksmatrizen, und daher existiert zu jeder solchen Gruppe genau ein Indexpaar (k,l) mit der Eigenschaft $(*)$. Da die Menge der Indexpaare endlich ist, können wir ein τ mit *maximalem* zugehörigen Indexpaar gemäß obiger Ordnung wählen, und wir ersetzen G durch $\tau G \tau^{-1}$ (dann ist entsprechend τU das neue Komplement zu W). Wir zeigen nun, dass die Maximalität von (k,l) folgende Konsequenz hat:

$$\lambda_i \in K \text{ für } i = 1, \ldots, n,\ \lambda_k \neq 0 \Rightarrow \sum_{i=1}^{n} \lambda_i S_{il} \notin A. \tag{8}$$

Sei nämlich stattdessen $\sum_{i=1}^{n} \lambda_i S_{il} \in A$. Da $\lambda_k \neq 0$, können wir O.E. $\lambda_k = 1$ annehmen. Da $S_{il} \in A$ für $i < k$ nach $(*)$, $S_{ll} = 1 \in A$ und $S_{il} = 0 \in A$ für $i > l$, gilt dann auch

$$\textbf{Annahme:} \qquad \sum_{i=k}^{l-1} \lambda_i S_{il} \in A, \quad \text{mit } \lambda_k = 1 \quad (\text{und } \lambda_i \in K \text{ für } i = k, \ldots, l-1). \tag{9}$$

Sei $I_m \in K^{m \times m}$ die $m \times m$ Einheitsmatrix. Wir betrachten nun die unipotente obere Dreiecksmatrix

$$\tau := \begin{pmatrix} I_{k-1} & & & & & & & \\ & 1 & \lambda_{k+1} & \ldots & \ldots & \lambda_{l-1} & & \\ & & 1 & 0 & \ldots & 0 & & \\ & & & \ddots & \ddots & \vdots & & \\ & & & & 1 & 0 & & \\ & & & & & 1 & & \\ & & & & & & I_{n-l+1} & \end{pmatrix} \in \mathrm{GL}_n\,.$$

Beim Inversen τ^{-1} erhalten dann lediglich die λ_i in obiger Matrix ein Minuszeichen. Sei dann $K[Y_{ij} : 1 \leq i < j \leq n] = K[\tau G \tau^{-1}]$ der zur Varietät $\tau G \tau^{-1}$ gehörige Koordinatenring (wobei wieder $Y_{ii} = 1$ und $Y_{ij} = 0$ für $i > j$). Nach Lemma 1.43 gibt es dann einen Isomorphismus $\varphi^* : K[Y_{ij} : 1 \leq i < j \leq n] \to K[G]$ mit

$$(\varphi^*(Y_{ij}))_{i,j=1,\ldots,n} = \tau \cdot (S_{rs})_{r,s=1,\ldots,n} \cdot \tau^{-1}.$$

Ist $e_i \in K^n$ der i-te Einheitsvektor, δ_{jk} das Kronecker-Symbol und setzen wir $\lambda_i = 0$ für $i < k$ oder $i \geq l$, so ist also für alle $1 \leq i, j \leq n$

$$\varphi^*(Y_{ij}) = e_i^T \tau \cdot (S_{rs})_{r,s=1,\ldots,n} \cdot (e_j - \lambda_j e_k + \delta_{jk} e_k).$$

Für $j < l$ bestehen wegen $k < l$ bereits die Komponenten von

$$(S_{rs})_{r,s=1,\ldots,n} \cdot (e_j - \lambda_j e_k + \delta_{jk} e_k)$$

nur aus Linearkombinationen von S_{rs} mit $s < l$, liegen also nach $(*)$ in A. Damit gilt auch

$$\varphi^*(Y_{ij}) \in A \quad \text{für } j < l.$$

Für $j = l$ und $i < k$ ist

$$\varphi^*(Y_{il}) = e_i^T \cdot (S_{rs})_{r,s=1,\ldots,n} \cdot e_l = S_{il} \in A$$

wegen $(*)$.

Schliesslich ist für $j = l$ und $i = k$

$$\varphi^*(Y_{kl}) = e_k^T \tau \cdot (S_{rs})_{r,s=1,\ldots,n} \cdot e_l = \sum_{r=k}^{l-1} \lambda_r S_{rl} \in A$$

nach (9). Nach der letzten Aussage von Lemma 1.43 gilt $A = \varphi^*(K[Y_{ij}^p : 1 \leq i < j \leq n])$. Da φ^* ein Isomorphismus ist, folgt nun aus obigen drei Enthaltenseinsrelationen, dass das zu $\tau G \tau^{-1}$ gehörige, $(*)$ erfüllende eindeutige Indexpaar (k', l') größer ist als (k, l), was im Widerspruch zur Maximalität von (k, l) steht. Damit ist die Annahme (9) falsch, d.h. (8) ist richtig.

Sei nun $\sigma = (\sigma_{ij})_{i,j=1,\ldots,n} \in G$ (fest). Wir betrachten

$$\phi : K[G] \to K[G],\ f \mapsto \phi(f)$$

mit

$$\phi(f) : G \to K,\ x \mapsto f(\sigma x).$$

Es folgt

$$\phi(S_{ij})(x) = S_{ij}(\sigma x) = \sum_{r=1}^{n} (\sigma_{ir} x_{rj}) = \sum_{r=1}^{n} \sigma_{ir} S_{rj}(x) \quad \text{für alle } x \in G,$$

also

$$\phi(S_{ij}) = \sum_{r=1}^{n} \sigma_{ir} S_{rj}.$$

Der Frobenius-Homomorphismus liefert sofort $\phi(A) \subseteq A$. Da $S_{il} \in A$ für $i < k$ nach $(*)$, ist dann also auch $\phi(S_{il}) \in A$, d.h.

$$\phi(S_{il}) = \sum_{r=1}^{n} \sigma_{ir} S_{rl} \in A,$$

also $\sigma_{ik} = 0$ nach (8). Dies gilt für alle $i < k$, und da σ eine unipotente obere Dreiecksmatrix ist, ist die k-te Spalte von σ damit gleich dem k-ten Einheitsvektor e_k. Dies gilt für alle $\sigma \in G$, d.h. X_k ist unter G invariant:

$$\sigma \cdot X_k = X_k \quad \text{für alle } \sigma \in G. \tag{10}$$

Wir kehren nun zurück zur Zerlegung $S^p(V) = U \oplus W$. Für $i \neq k$ betrachten wir die eindeutige Zerlegung

$$X_i X_k^{p-1} = u_i + w_i \quad \text{mit } u_i \in U, w_i \in W. \tag{11}$$

Für $\sigma = (\sigma_{ij})_{i,j=1,\ldots,n} \in G$ ist

$$\sigma \cdot X_l X_k^{p-1} \overset{(10)}{=} \sum_{i=1}^{l} \sigma_{il} X_i X_k^{p-1} \tag{12}$$

und damit

$$\begin{aligned} \sigma \cdot u_l &= \sigma(X_l X_k^{p-1} - w_l) = \sum_{i=1}^{l} \sigma_{il} X_i X_k^{p-1} - \sigma w_l = \sum_{i=1, i\neq k}^{l} \sigma_{il} X_i X_k^{p-1} + \sigma_{kl} X_k^p - \sigma w_l \\ &\overset{(11)}{=} \sum_{i=1, i\neq k}^{l} \sigma_{il} u_i + \sum_{i=1, i\neq k}^{l} \sigma_{il} w_i + \sigma_{kl} X_k^p - \sigma w_l. \end{aligned}$$

Die letzten drei Terme liegen dabei alle in $W = \langle X_1^p, \ldots, X_n^p \rangle$, und der erste Term in U. Da U ein G-Modul ist, also $\sigma u_l \in U$, folgt damit aus $U \cap W = \{0\}$:

$$\sigma \cdot u_l = \sum_{i=1, i \neq k}^{l} \sigma_{il} u_i. \tag{13}$$

Sei $(X_k^p)^* \in S^p(V)^*$ das Funktional, dass von einem Polynom in $S^p(V)$ gerade den Koeffizienten von X_k^p liefert. Dann ist

$$f : G \to K,\ \sigma \mapsto (X_k^p)^*(\sigma \cdot u_l)$$

durch Polynome gegeben, also $f \in K[G]$. Wegen (13) ist

$$f(\sigma) = \sum_{i=1, i \neq k}^{l} \sigma_{il} (X_k^p)^*(u_i) = \sum_{i=1, i \neq k}^{l} (X_k^p)^*(u_i) S_{il}(\sigma) \quad \text{für alle } \sigma \in G,$$

also mit $\lambda_i := (X_k^p)^*(u_i)$

$$f = \sum_{i=1, i \neq k}^{l} \lambda_i S_{il}. \tag{14}$$

Es ist aber

$$\begin{aligned} (f - S_{kl})(\sigma) &= (X_k^p)^*(\sigma \cdot u_l) - \sigma_{kl} \overset{(11)}{=} (X_k^p)^*(\sigma \cdot (X_l X_k^{p-1} - w_l)) - \sigma_{kl} \\ &\overset{(12)}{=} (X_k^p)^* \left(\sum_{i=1}^{l} \sigma_{il} X_i X_k^{p-1} - \sigma w_l \right) - \sigma_{kl} = \sigma_{kl} - (X_k^p)^*(\sigma w_l) - \sigma_{kl} \\ &= -(X_k^p)^*(\sigma w_l). \end{aligned}$$

Da aber $w_l \in W = \langle X_1^p, \ldots, X_n^p \rangle$, sind die Koeffizienten der Monome von $\sigma \cdot w_l$ Polynome in den p-ten Potenzen σ_{ij}^p der Koeffizienten von σ, und damit

$$f - S_{kl} \in A.$$

Wegen (14) ist dann aber

$$\sum_{i=1, i \neq k}^{l} \lambda_i S_{il} - S_{kl} \in A,$$

im Widerspruch zu (8). Damit war die Annahme, dass G kein Torus ist falsch, und der Satz ist bewiesen. □

1.3 Erste Kohomologie algebraischer Gruppen

Sei V ein G-Modul. Ein *(1)-Kozyklus* ist ein Morphismus

$$g : G \to V \quad \text{mit} \quad g_{\sigma\tau} = \sigma g_\tau + g_\sigma \text{ für alle } \sigma, \tau \in G.$$

Insbesondere gilt für das neutrale Element $\iota \in G : g_\iota = g_{\iota\iota} = \iota g_\iota + g_\iota$, also $g_\iota = 0$. Ist $v \in V$, so ist durch $\sigma \mapsto (\sigma - 1)v := \sigma v - v$ ebenfalls ein Kozyklus gegeben, und ein Kozyklus der

sich so schreiben lässt, heißt ein *Korand* oder ein *trivialer Kozyklus*. Die additive Gruppe aller Kozyklen wird mit $Z^1(G,V)$ bezeichnet, die Untergruppe aller Koränder mit $B^1(G,V)$, und die Faktorgruppe (1. Kohomologiegruppe) mit $H^1(G,V) = Z^1(G,V)/B^1(G,V)$. Für ein $g \in Z^1(G,V)$ definiert man den *erweiterten* G-Modul $\tilde{V} := V \oplus K$ mit der Operation $\sigma(v,\lambda) := (\sigma v + \lambda g_\sigma, \lambda)$ für $v \in V, \lambda \in K$. Man rechnet sofort nach, dass dadurch tatsächlich eine Operation auf $\tilde{V}$ definiert ist. In $\tilde{V}$ wird g zu einem Korand, $g \in B^1(G,\tilde{V})$, denn $g_\sigma = (g_\sigma, 0) = (\sigma - 1)(0,1)$ für alle $\sigma \in G$.

Ist $V = K^n$ mit Darstellung $\sigma \mapsto A_\sigma \in K^{n\times n}$ und $\sigma \mapsto g_\sigma \in K^n$ ein Kozyklus, so hat $\tilde{V}$ die Darstellung

$$\sigma \mapsto \begin{pmatrix} A_\sigma & g_\sigma \\ & 1 \end{pmatrix}. \tag{15}$$

(Lücken in Blockmatrizen wie hier werden wie üblich mit Nullen aufgefüllt).

Seien V, W jeweils G-Moduln. Dann ist auch $\mathrm{Hom}_K(V,W)$ ein G-Modul mit Operation gegeben durch $\sigma \cdot f := \sigma \circ f \circ \sigma^{-1}$ für $f \in \mathrm{Hom}_K(V,W)$, $\sigma \in G$. Für den Fixmodul schreiben wir $\mathrm{Hom}_K(V,W)^G =: \mathrm{Hom}_G(V,W) = \mathrm{Hom}_{KG}(V,W)$.

Satz und Definition 1.44 *Sei V ein G-Modul und W ein Untermodul. Dann ist*

$$\mathrm{Hom}_K(V,W)_0 := \{f \in \mathrm{Hom}_K(V,W) : f|_W = 0\} \cong W \otimes (V/W)^*$$

ein Untermodul von $\mathrm{Hom}_K(V,W)$*. Damit gilt*

$$\dim_K \mathrm{Hom}_K(V,W)_0 = \dim_K(W \otimes (V/W)^*) = \dim_K W \cdot (\dim_K V - \dim_K W).$$

Beweis. Nur die angegebene Isomorphie ist beweisbedürftig. Sei $\rho : V \to V/W$ der kanonische Epimorphismus. Dann ist $\mathrm{Hom}_K(V/W,W) \to \mathrm{Hom}_K(V,W)_0$, $f \mapsto f \circ \rho$ ein Isomorphismus von G-Moduln, und daher

$$\mathrm{Hom}_K(V,W)_0 \cong \mathrm{Hom}_K(V/W,W) \cong W \otimes (V/W)^*.$$

□

Zur Anwendung der nächsten Proposition ist die folgende einfache Aussage oft hilfreich:

Bemerkung 1.45 *Sei $U \le V \le W$ eine Kette von G-Moduln. Wenn U kein Komplement in V hat, so auch nicht in W.*

Beweis. Angenommen, $W = U \oplus U'$. Dann gilt auch $V = U \oplus (U' \cap V)$, im Widerspruch zur Voraussetzung: Für $v \in V \le W$ gibt es nämlich $u \in U, u' \in U'$ mit $v = u + u'$, also $u' = v - u \in U' \cap V$. Außerdem ist $U \cap (U' \cap V) \subseteq U \cap U' = \{0\}$. □

Proposition 1.46 *Sei W Untermodul eines G-Moduls V, sowie $\iota \in \mathrm{Hom}_K(V,W)$ mit $\iota|_W = \mathrm{id}_W$. Dann ist durch $\sigma \mapsto g_\sigma := (\sigma - 1)\iota$ ein Kozyklus in $Z^1(G, \mathrm{Hom}_K(V,W)_0)$ gegeben, welcher genau dann ein Korand ist, wenn W ein (G-invariantes) Komplement in V hat.*

Beweis. Zunächst ist $g_\sigma \in \mathrm{Hom}_K(V,W)_0$ für $\sigma \in G$ zu zeigen: Für $w \in W$ ist

$$g_\sigma(w) = ((\sigma - 1)\iota)(w) = \sigma\left(\iota(\sigma^{-1}w)\right) - w \overset{\iota|_W = \mathrm{id}_W}{=} \sigma\sigma^{-1}w - w = 0, \tag{16}$$

also $g_\sigma|_W = 0$ und damit $g_\sigma \in \mathrm{Hom}_K(V,W)_0$. Es ist klar, dass g ein Kozyklus ist.

Sei nun g ein Korand, d.h. es gibt $f \in \mathrm{Hom}_K(V,W)_0$ mit $g_\sigma = (\sigma-1)\iota = (\sigma-1)f$ für alle $\sigma \in G$. Für $h := \iota - f$ folgt dann $\sigma h = h$, also $h \in \mathrm{Hom}_G(V,W)$, und $\ker h$ ist damit ein Untermodul (G-invarianter Untervektorraum) von V. Für $w \in W$ gilt ferner $h(w) = \iota(w) - f(w) = w - 0 = w$, also $h|_W = \mathrm{id}_W$. Da dann $h(V) = W$, folgt also $h(h(v)) = h(v)$ für alle $v \in V$. Also ist h Projektion auf W, und in üblicher Weise folgt nun $V = W \oplus \ker h$:

$$\text{für alle } v \in V: \quad v = \underbrace{(v - h(v))}_{\in \ker h} + \underbrace{h(v)}_{\in W},$$

denn $h(v - h(v)) = h(v) - h(h(v)) = h(v) - h(v) = 0$. Ferner gilt für $v \in W \cap \ker h$, dass $v \overset{h|_W = \mathrm{id}_W}{=} h(v) = 0$, also ist die Summe direkt.

Gilt umgekehrt $V = W \oplus U$ mit einem G-invarianten Teilraum U, so wähle

$$f \in \mathrm{Hom}_K(V,W)_0 \text{ mit } f|_W = 0,\ f|_U = \iota|_U.$$

Wir zeigen $g_\sigma = (\sigma-1)f$: Für $w \in W, u \in U$ ist

$$\begin{aligned} g_\sigma(w+u) &\overset{(16)}{=} g_\sigma(u) = ((\sigma-1)\iota)(u) = \sigma(\iota(\sigma^{-1}u)) - \iota(u) \overset{f|_U = \iota|_U}{=} \\ \sigma(f(\sigma^{-1}u)) - f(u) &= ((\sigma-1)f)(u) \overset{f|_W = 0}{=} ((\sigma-1)f)(w+u), \end{aligned}$$

also Gleichheit auf $V = W \oplus U$, und g ist ein Korand. □

Diese Proposition zeigt, dass wenn es einen G-Modul gibt, der einen Untermodul ohne Komplement besitzt (also wenn G nicht linear reduktiv ist), dann gibt es einen nichttrivialen Kozyklus (der Gruppe G). Ist umgekehrt V ein G-Modul und $g \in Z^1(G,V)$ ein nichttrivialer Kozyklus, so hat V kein G-invariantes Komplement in $\tilde{V} = V \oplus K$ - insbesondere ist G nicht linear reduktiv. Wäre nämlich $K(v,\lambda)$ ein solches ($v \in V, \lambda \in K \setminus \{0\}$), so wäre $\sigma(v,\lambda) - (v,\lambda) = (\sigma(v) - v + \lambda g_\sigma, 0) \in K(v,\lambda) \cap V = \{0\}$ für alle $\sigma \in G$, also $\sigma \mapsto g_\sigma = (\sigma-1)(-\frac{1}{\lambda}v)$ doch ein trivialer Kozyklus. Damit ist folgender Satz gezeigt (Kemper [33, Proposition 1], in weniger moderner Formulierung im wesentlichen auch bei Nagata [45, Theorem 4]):

Proposition 1.47 *Eine lineare algebraische Gruppe G ist genau dann linear reduktiv, wenn jeder Kozyklus ein Korand ist, d.h. $H^1(G,V) = 0$ für jeden G-Modul V gilt.*

Korollar 1.48 *Sei G eine lineare algebraische Gruppe und $N \lhd G$ ein* abgeschlossener *Normalteiler. Ist G linear reduktiv, so auch G/N. Sind umgekehrt N und G/N linear reduktiv, so auch G.*

Man beachte hierbei, dass man G/N die Struktur einer linearen algebraischen Gruppe geben kann, siehe Bemerkung 1.32.

Beweis. Ist G linear reduktiv, so ist jeder G/N-Modul via des Homomorphismus $G \to G/N$ auch G-Modul mit den gleichen Untermoduln und damit vollständig reduzibel, so dass auch G/N linear reduktiv ist. Seien umgekehrt N und G/N linear reduktiv und V ein G-Modul. Nach der Proposition müssen wir $H^1(G,V) = 0$ zeigen. Sei also $g \in Z^1(G,V)$. Dann ist erst recht $g|_N \in Z^1(N,V) = B^1(N,V)$, denn N ist linear reduktiv, also $H^1(N,V) = 0$

nach der Proposition. Damit gibt es ein $v \in V$ mit $g_\tau = (\tau - 1)v$ für alle $\tau \in N$. Für $h_\sigma := g_\sigma - (\sigma - 1)v$ für alle $\sigma \in G$ gilt dann

$$h_\tau = 0 \quad \text{für alle } \tau \in N \tag{17}$$

sowie $h \in Z^1(G, V)$ mit $h + B^1(G, V) = g + B^1(G, V)$. Es genügt also $h \in B^1(G, V)$ zu zeigen. Für $\sigma \in G$, $\tau \in N$ gilt $h_{\sigma\tau} = \sigma h_\tau + h_\sigma \overset{(17)}{=} h_\sigma$. Weiter ist $\tau\sigma = \sigma\tau'$ mit einem $\tau' \in N$, und damit ist dann auch $h_{\tau\sigma} = h_{\sigma\tau'} = h_\sigma$ nach eben, insgesamt also

$$h_{\sigma\tau} = h_{\tau\sigma} = h_\sigma \quad \text{für alle } \sigma \in G,\ \tau \in N. \tag{18}$$

Mit der Kozyklus Eigenschaft gilt dann

$$\tau h_\sigma = h_{\tau\sigma} - h_\tau \overset{(18),\ (17)}{=} h_\sigma \quad \text{für alle } \sigma \in G, \tau \in N,$$

also $h_\sigma \in V^N$ für alle $\sigma \in G$. Wegen (18) und Bemerkung 1.32 ist also mit $H : G/N \to V^N$, $\sigma N \mapsto h_\sigma$ dann $H \in Z^1(G/N, V^N) = B^1(G/N, V^N)$, denn G/N ist linear reduktiv. Also gibt es $w \in V^N$ mit $H(\sigma N) = (\sigma N - 1)w$ d.h. $h_\sigma = (\sigma - 1)w$ für alle $\sigma \in G$, und damit $h \in B^1(G, V)$. Also ist G linear reduktiv. □

Korollar 1.49 (Maschke) *Eine endliche Gruppe, aufgefasst als lineare algebraische Gruppe über einem Körper der Charakteristik $p \geq 0$, ist genau dann linear reduktiv, wenn p kein Teiler der Gruppenordnung ist.*

Beweis. „⇒." Sei $p = \operatorname{char} K$ kein Teiler der Gruppenordnung $|G|$, und $g \in Z^1(G, V)$ ein Kozyklus eines G-Moduls V. Da $|G|$ in K invertierbar ist, ist

$$v := \frac{-1}{|G|} \sum_{\tau \in G} g_\tau \in V$$

wohldefiniert. Aus der Kozyklus Eigenschaft $\sigma g_\tau = g_{\sigma\tau} - g_\sigma$ folgt

$$\begin{aligned} \sigma v - v &= \frac{-1}{|G|} \sum_{\tau \in G} (g_{\sigma\tau} - g_\sigma) - v \\ &= v + |G| \cdot \frac{1}{|G|} g_\sigma - v = g_\sigma \quad \text{für alle } \sigma \in G. \end{aligned}$$

Daher ist jeder Kozyklus g ein Korand, also nach Proposition 1.47 G linear reduktiv.

„⇐ ." Sei p ein Teiler von $|G|$. Betrachte den *regulären* G-Modul V mit Basis $\{e_\sigma\}_{\sigma \in G}$ und der Operation gegeben durch $\tau e_\sigma = e_{\tau\sigma}$. Offenbar ist dann

$$e := \sum_{\sigma \in G} e_\sigma \in V^G.$$

Wäre G linear reduktiv, so hätte Ke ein Komplement U in V, also $V = Ke \oplus U$ (mit U Untermodul). Sei $u = \sum_{\sigma \in G} \lambda_\sigma e_\sigma \in U$ mit $\lambda_\sigma \in K$ für alle $\sigma \in G$. Es folgt

$$\sum_{\tau \in G} \tau u = \sum_{\sigma \in G} \lambda_\sigma \underbrace{\sum_{\tau \in G} e_{\tau\sigma}}_{e} = \sum_{\sigma \in G} \lambda_\sigma e \in U \quad (\text{da } U \text{ Untermodul}).$$

Da $e \notin U$, folgt

$$\sum_{\sigma\in G} \lambda_\sigma = 0 \quad \text{für alle } u = \sum_{\sigma\in G} \lambda_\sigma e_\sigma \in U. \tag{19}$$

Sei

$$W := \left\{ \sum_{\sigma\in G} \lambda_\sigma e_\sigma \in V : \sum_{\sigma\in G} \lambda_\sigma = 0 \right\}.$$

Dann ist $\dim W = \dim V - 1$ und $U \subseteq W$ nach (19). Da auch $\dim U = \dim V - 1$, folgt also $U = W$. Da aber $|G| \cdot 1 = 0$, ist auch $e = \sum_{\sigma\in G} 1 \cdot e_\sigma \in W = U$. Dies ist ein Widerspruch zu $Ke \cap U = \{0\}$. □

Aus dem Beweis notieren wir

Korollar 1.50 *Sei G eine endliche Gruppe, $p = \operatorname{char} K$ ein Teiler der Gruppenordnung $|G|$, V die reguläre Darstellung von G mit Basis $\{e_\sigma\}_{\sigma\in G}$ und $e := \sum_{\sigma\in G} e_\sigma \in V^G$. Dann hat der Untermodul Ke kein Komplement in V.*

Nun können wir den Satz von Nagata beweisen:

Beweis von Satz 1.37. Sei G linear reduktiv. Nach Korollar 1.40 ist dann G^0 ein Torus. Nach Korollar 1.48 ist auch die (endliche, Satz 1.34) Faktorgruppe G/G^0 linear reduktiv, und nach dem Satz von Maschke gilt damit $p \nmid (G : G^0)$. Ist umgekehrt G^0 ein Torus und $p \nmid (G : G^0)$, so sind der Normalteiler G^0 bzw. die Faktorgruppe G/G^0 nach dem bereits zitierten Springer [59, Theorem 2.5.2(c)] bzw. dem Satz von Maschke linear reduktiv. Nach Korollar 1.48 ist dann auch G linear reduktiv. □

Die folgende Proposition (allgemeiner in Kemper [33, Proposition 2], allerdings ohne die Formel (20)) besagt, dass man jeden nichttrivialen Kozyklus annullieren kann. Sie wird eines der wichtigsten Hilfsmittel für den Beweis unseres Hauptresultats sein. Wir verwenden folgende Notation: Für G-Moduln V, W und $\pi \in W^G$, $g \in Z^1(G, V)$ bezeichnen wir mit $\pi \otimes g \in H^1(G, W \otimes V)$ die Restklasse des durch $\sigma \mapsto \pi \otimes g_\sigma$ gegebenen Kozyklus aus $Z^1(G, W \otimes V)$.

Proposition 1.51 *Sei V ein G-Modul, $g \in Z^1(G, V)$ und $\tilde{V}$ der entsprechende erweiterte G-Modul. Sei $\{v_1, \ldots, v_{n+1}\}$ eine Basis von $\tilde{V}$, derart dass $\{v_1, \ldots, v_n\}$ Basis von V ist und $\sigma v_{n+1} = v_{n+1} + g_\sigma$ für alle $\sigma \in G$ gilt (vgl. die Darstellung (15), S. 33). Ist dann $\{v_1^*, \ldots, v_{n+1}^*\}$ die zugehörige Dualbasis von $\tilde{V}^*$ (also $v_i^*(v_j) = \delta_{ij}$), so ist $\pi := v_{n+1}^*$ invariant, und der Kozyklus $\sigma \mapsto \pi \otimes g_\sigma$ aus $Z^1(G, \tilde{V}^* \otimes V)$ ist trivial (d.h. $\pi \otimes g = 0 \in H^1(G, \tilde{V}^* \otimes V)$). Genauer gilt*

$$\pi \otimes g_\sigma = -(\sigma - 1)(v_1^* \otimes v_1 + \ldots + v_n^* \otimes v_n) \quad \text{für alle } \sigma \in G. \tag{20}$$

Beweis. Bekanntlich ist durch lineare Fortsetzung von $\varphi \otimes v \mapsto v\varphi(\cdot)$ ein G-Modul-Isomorphismus $\tilde{V}^* \otimes V \to \operatorname{Hom}_K(\tilde{V}, V)$ gegeben, und wir identifizieren deshalb beide Moduln miteinander. Es genügt dann zu zeigen, dass beide Seiten von (20) auf der Basis $\{v_1, \ldots, v_{n+1}\}$ von $\tilde{V}$ übereinstimmen. Da $\{v_1, \ldots, v_n\}$ Basis von V ist, ist $(v_1^* \otimes v_1 + \ldots + v_n^* \otimes v_n)|_V = \mathrm{id}_V$. Da V ein Untermodul von $\tilde{V}$ ist, folgt $\sigma \cdot \mathrm{id}_V = \mathrm{id}_V$, so dass die rechte Seite von (20) eingeschränkt auf V gleich 0 ist, und damit gleich der linken Seite eingeschränkt auf V (da

$\pi|_V = 0$). Es bleibt Übereinstimmung auf v_{n+1} zu zeigen. Die linke Seite liefert g_σ, und die rechte wegen $(v_1^* \otimes v_1 + \ldots + v_n^* \otimes v_n)(v_{n+1}) = 0$ ebenfalls

$$-\left(\sum_{i=1}^{n} \sigma v_i v_i^* \left(\sigma^{-1} v_{n+1}\right)\right) = -\sigma\left(\sum_{i=1}^{n} v_i v_i^* \left(v_{n+1} + g_{\sigma^{-1}}\right)\right) = -\sigma g_{\sigma^{-1}} = g_\sigma,$$

wobei im letzten Schritt die Kozyklus Eigenschaft $0 = g_{\sigma\sigma^{-1}} = \sigma g_{\sigma^{-1}} + g_\sigma$ von g ausgenutzt wurde. □

Mit einem $\pi \in \tilde{V}^{*G}$ wie in Proposition 1.51 erhalten wir eine kurze exakte Sequenz von G-Moduln

$$0 \to V \hookrightarrow \tilde{V} \xrightarrow{\pi} K \to 0, \tag{21}$$

wir können also jedem Kozyklus eine solche kurze exakte Sequenz zuordnen. Umgekehrt „induziert“ eine kurze exakte Sequenz der Form (21) eindeutig ein Element aus $H^1(G, V)$. Sei nämlich $v \in \tilde{V}$ mit $\pi(v) = 1$. Es ist $\sigma v - v \in \ker \pi = V$ ($\sigma \in G$), und damit ist mit $h_\sigma := \sigma v - v$ dann $h \in Z^1(G, V)$. (Für die Situation aus der Proposition und $v = v_{n+1}$ erhalten wir gerade $h = g$ zurück.) Ist auch $v' \in \tilde{V}$ mit $\pi(v') = 1$, so ist wegen $\pi(v - v') = 0$ dann $u := v - v' \in V$, und für $h'_\sigma := \sigma v' - v'$ gilt $h_\sigma - h'_\sigma = (\sigma - 1)u$, also $h - h' \in B^1(G, V)$. Der exakten Sequenz kann also wohldefiniert das Element $h + B^1(G, V) \in H^1(G, V)$ zugeordnet werden.

Wir verfolgen diesen Zusammenhang allgemeiner in Abschnitt 2. Dort werden wir als Verallgemeinerung von Proposition 1.51 Annullatoren von Kozyklen in höherer Kohomologie behandeln.

Hat $\tilde{V}$ eine Darstellung wie in Gleichung (15), so hat $\tilde{V}^*$ die Darstellung

$$\sigma \mapsto \begin{pmatrix} A^T_{\sigma^{-1}} & \\ g^T_{\sigma^{-1}} & 1 \end{pmatrix},$$

woran man nochmal unmittelbar sieht, dass der letzte Basisvektor π invariant ist.

Wir untersuchen kurz das Zusammenspiel der Propositionen 1.46 und 1.51: Sei V ein G-Modul, $0 \neq v \in V^G$ so, dass Kv kein G-invariantes Komplement in V hat. Sei weiter $V = Kv \oplus U$ mit einem Untervektorraum U, und $\iota \in \mathrm{Hom}_K(V, Kv)$ mit $\iota|_U = 0$ und $\iota(v) = v$. Dann ist durch $g_\sigma = (\sigma - 1)\iota$ ein nichttrivialer Kozyklus mit Werten in $M := \mathrm{Hom}_K(V, Kv)_0 \cong Kv \otimes (V/Kv)^* \cong (V/Kv)^*$ gegeben. Der zugehörige erweiterte Modul ist dann $\tilde{M} = \mathrm{Hom}_K(V, Kv)_0 + K\iota = \mathrm{Hom}_K(V, Kv) \cong V^*$. Es folgt $\tilde{M}^* \cong V$, und wegen $\sigma\iota = \iota + g_\sigma$ und $v(\iota) := \iota(v) = 1 \cdot v$, kann man ι und v zu einem Paar dualer Basen in $\tilde{M}$ bzw. $V \cong \tilde{M}^*$ wie in Proposition 1.51 ergänzen, so dass $v = \iota^*$. Nach dieser Proposition wird dann $g \in H^1(G, M)$ von $v \in V \cong \tilde{M}^*$ annulliert.

Quintessenz: Jede Invariante ohne Komplement tritt als Annullator eines nichttrivialen Kozyklus auf.

1.4 Invariantentheorie

Sei V ein endlich-dimensionaler K-Vektorraum. Nach Wahl einer Basis kann man V als K^n auffassen. Dann bezeichnet $K[V]$ die zum Polynomring $K[X_1, \ldots, X_n]$ isomorphe Algebra der Polynomfunktionen auf V. Die Graduierung ist hier durch den Totalgrad gegeben, und

$K[V]_d$ bezeichnet dann die Menge der homogenen Polynome vom Grad d und die 0. Ist V sogar ein G-Modul, so operiert G auf $K[V]$ mittels $\sigma \cdot f := f \circ \sigma^{-1}$ für $f \in K[V], \sigma \in G$. Damit ist $K[V]$ isomorph zur *symmetrischen Algebra* $S(V^*)$ des Duals, $K[V] \cong S(V^*) := \sum_{d=0}^{\infty} S^d(V^*)$.

1.4.1 Invariantentheorie reduktiver Gruppen

Wir kommen zur invariantentheoretischen Charakterisierung der Reduktivität.

Satz 1.52 *Sei G eine lineare algebraische Gruppe.*

(a) G ist genau dann reduktiv, wenn G geometrisch reduktiv *ist, d.h. wenn für jeden G-Modul V und $0 \neq v \in V^G$ ein homogenes $f \in K[V]_+^G$ existiert mit $f(v) \neq 0$.*

(b) G ist genau dann linear reduktiv, wenn für jeden G-Modul V und $0 \neq v \in V^G$ ein $f \in K[V]_1^G = V^{*G}$ existiert mit $f(v) \neq 0$.

Insbesondere ist jede linear reduktive Gruppe auch reduktiv.

Da wir nun alle Arten von Reduktivität beisammen haben, noch eine Bemerkung zum Begriffsbabylon in der Literatur: In älteren Arbeiten wie denen von Nagata wird mit dem Wort „semi-reduktiv“ unser *geometrisch reduktiv* bezeichnet (was also nach Satz 1.52 mit unserem reduktiv zusammenfällt), und mit dem Wort „reduktiv“ unser *linear reduktiv*. (Nagata definiert „semi-reduktiv“ über den Dual und mit speziellen Korändern, man sieht aber leicht, dass seine Definition zu unserer von „geometrisch reduktiv“ äquivalent ist). Unser „reduktiv“ wird daher zur besseren Unterscheidung oft als *gruppentheoretisch reduktiv* bezeichnet. Insbesondere bei der Verwendung von „reduktiv“ ist also Vorsicht geboten.

Beweis. (a) Nach Nagata und Miyata [48, Theorem 2] ist jede geometrisch reduktive (also „semi-reduktive“ bei Nagata) Gruppe reduktiv. Mumford et al. [44] folgend kann man diese Beweisrichtung auch so führen: Wenn G geometrisch reduktiv ist, so ist nach Nagata [46] $K[X]^G$ endlich erzeugt für jede G-Varietät X. Nach Popov [51] folgt hieraus jedoch, dass G reduktiv ist.

Für die Umkehrung siehe Haboush [23].

(b) Ist G linear reduktiv und $0 \neq v \in V^G$, so existiert ein Untermodul U von V mit $V = Kv \oplus U$. Dann existiert ein lineares Funktional $f \in V^*$ mit $f(v) = 1, f|_U = 0$, und ein solches ist G-invariant.

Sei umgekehrt die zweite Bedingung erfüllt. Wir zeigen, dass jeder Kozyklus $g \in Z^1(G, V)$ eines G-Moduls V trivial ist, wobei wir die Bezeichnungen aus Proposition 1.51 verwenden. Mit Proposition 1.47 folgt dann die lineare Reduktivität von G. Offenbar ist $v_{n+1}^* \in \tilde{V}^{*G}$. Daher existiert nach Voraussetzung ein $v \in \tilde{V}^{**G} = \tilde{V}^G$ mit $v(v_{n+1}^*) = v_{n+1}^*(v) \neq 0$, wobei wir den üblichen Isomorphismus $V \to V^{**}$ verwendet haben. Wir können O.E. $v_{n+1}^*(v) = 1$ annehmen, und dann ist $v = v_{n+1} - u$ mit einem $u \in V$. Da $v \in \tilde{V}^G$, gilt $\sigma v = v$ für alle $\sigma \in G$, also $v_{n+1} + g_\sigma - \sigma u = v_{n+1} - u$, oder $g_\sigma = (\sigma - 1)u$ für alle $\sigma \in G$. Da $u \in V$ ist also $g \in B^1(G, V)$ ein Korand. □

In Charakteristik 0 fallen die Begriffe reduktiv und linear reduktiv zusammen:

Satz 1.53 (Nagata und Miyata [48]) *In Charakteristik 0 ist eine lineare algebraische Gruppe genau dann reduktiv, wenn sie linear reduktiv ist.*

Der folgende Beweis ist im wesentlichen der Originalbeweis, wobei wir jedoch Nagatas Begrifflichkeiten in unsere äquivalente übersetzt haben. (Insbesondere Nagatas „semireduktiv“ in unser geometrisch reduktiv.)

Beweis. Wir wissen bereits, dass jede linear reduktive Gruppe auch reduktiv ist.

Sei umgekehrt also G reduktiv in Charakteristik 0. Wir zeigen wieder, dass jeder Kozyklus $g \in Z^1(G,V)$ eines beliebigen G-Moduls V ein Korand ist, was nach Proposition 1.47 die lineare Reduktivität von G zeigt. Wir verwenden wieder die Notation von Proposition 1.51. Außerdem identifizieren wir $\tilde{V} = K[\tilde{V}^*]_1$. Da $v_{n+1}^* \in \tilde{V}^{*G}$, existiert wegen der Reduktivität von G ein homogenes $f \in K[\tilde{V}^*]^G = S(\tilde{V})^G$ vom Grad $d \geq 1$ mit $f(v_{n+1}^*) = 1$ (O.E.). Damit hat f die folgende Form:

$$f = v_{n+1}^d + a_{d-1}v_{n+1}^{d-1} + \ldots + a_0 \text{ mit } a_k \in S^{d-k}(V).$$

Also ist

$$\begin{aligned} \sigma f &= (v_{n+1} + g_\sigma)^d + \sigma a_{d-1}(v_{n+1} + g_\sigma)^{d-1} + \ldots \\ &= v_{n+1}^d + (dg_\sigma + \sigma a_{d-1})v_{n+1}^{d-1} + \ldots \end{aligned}$$

Da $S(V)$ G-invariant ist und $\sigma f = f$, erhält man durch Koeffizientenvergleich bei v_{n+1}^{d-1} also $dg_\sigma + \sigma a_{d-1} = a_{d-1}$ mit $a_{d-1} \in S^1(V) = V$. Da $\operatorname{char} K = 0$, ist d invertierbar, also $g_\sigma = (\sigma - 1)(-\frac{1}{d}a_{d-1})$ für alle $\sigma \in G$ mit $-\frac{1}{d}a_{d-1} \in V$. Damit ist $g \in B^1(G,V)$ ein Korand. □

Wie wir bereits im Beweis von Satz 1.52 bemerkt haben, ist nach Nagata [46] für reduktive Gruppen G und einen G-Modul V der Invariantenring $K[V]^G$ endlich erzeugt (das gilt sogar wenn V blos eine *G-Varietät* ist), und damit also ein graduierter, affiner Bereich (und nach Popov [51] folgt umgekehrt aus der endlichen Erzeugbarkeit von $K[X]^G$ für jede *G-Varietät* X die Reduktivität von G). Damit können also Invariantenringe reduktiver Gruppen mit den in Abschnitt 1.1 entwickelten Methoden und Begriffen untersucht und beschrieben werden. Dies ist einer der Gründe, warum man heute ausreichend Theorie nur für Invariantenringe reduktiver Gruppen zur Verfügung hat. Das folgende Lemma, das im wesentlichen von Nagata stammt, ist eines der Hauptwerkzeuge bei der Arbeit mit Invariantenringen reduktiver Gruppen:

Lemma 1.54 (Nagata) *Sei G eine reduktive Gruppe, V ein G-Modul und $I \subseteq K[V]^G$ ein Ideal. Dann gilt*

$$\sqrt{IK[V]} \cap K[V]^G = \sqrt{I}.$$

Beweis. (vgl. [33, Lemma 3]). Nach Nagata [46, Lemma 5.2.B] (oder Newstead [50, Lemma 3.4.2]) gilt

$$IK[V] \cap K[V]^G \subseteq \sqrt{I}$$

für jedes endlich erzeugte Ideal I von $K[V]^G$. Da Nagata in derselben Arbeit zeigt, dass $K[V]^G$ eine endlich erzeugte K-Algebra, also noethersch ist, gilt diese Gleichung also für jedes Ideal von $K[V]^G$. Gilt nun $f \in \sqrt{IK[V]} \cap K[V]^G$, so existiert ein n mit $f^n \in IK[V] \cap K[V]^G$, also $f \in \sqrt{I}$ nach obiger Gleichung. Gilt umgekehrt $f \in \sqrt{I}$, so gibt es ein n mit $f^n \in I \subseteq IK[V] \cap K[V]^G$, und dann gilt auch $f \in \sqrt{IK[V]} \cap K[V]^G$. □

Damit können wir die für uns wichtigste Eigenschaft reduktiver Gruppen beweisen (Kemper [33, Lemma 4]):

Lemma 1.55 *Ist G reduktiv und bilden $a_1, \ldots, a_k \in K[V]^G_+$ ein phsop im Polynomring $K[V]$, so bilden sie auch ein phsop im Invariantenring $K[V]^G$.*

Beweis. Sei $I := (a_1, \ldots, a_k)_{K[V]^G}$. Nach Lemma 1.5 ist $\text{height}(I) = k$ zu zeigen. Sei $\wp \supseteq I$ ein minimales Primideal. Nach dem Krullschen Hauptidealsatz ([14, Theorem 13.2]) gilt $\text{height}(\wp) \leq k$, d.h. wir müssen noch $\text{height}(\wp) \geq k$ zeigen. Nach Lemma 1.54 gilt

$$\wp \supseteq \sqrt{I} = \sqrt{IK[V]} \cap K[V]^G = \bigcap_{\substack{\mathcal{P} \supseteq IK[V] \\ \text{min. Primideal}}} \mathcal{P} \cap K[V]^G.$$

Da $\wp$ prim und rechts ein Schnitt über endlich viele Ideale steht ([40, Satz III.1.10.c]), umfasst $\wp$ eines dieser Ideale. Daher existiert ein minimales Primideal $\mathcal{P} \supseteq IK[V]$ mit $\wp \supseteq \mathcal{P} \cap K[V]^G \supseteq I$. Da aber $\wp$ ein minimaler Primteiler von I ist, folgt $\wp = \mathcal{P} \cap K[V]^G$. Da $\mathcal{P}$ ein minimaler Primteiler von $IK[V] = (a_1, \ldots, a_k)_{K[V]}$ ist, gilt nach Krulls Hauptidealsatz $\text{height}(\mathcal{P}) \leq k$. Da $a_1, \ldots, a_k$ ein phsop in $K[V]$ ist, gilt aber auch $k = \text{height}(a_1, \ldots, a_k)_{K[V]} \leq \text{height}(\mathcal{P})$ nach Lemma 1.5 und nach Definition der Höhe, insgesamt also $\text{height}(\mathcal{P}) = k$. Wir ergänzen nun das phsop zu einem hsop $a_1, \ldots, a_n$ von $K[V]$ (wobei i.a. $a_{k+i} \notin K[V]^G$), und setzen $A := K[a_1, \ldots, a_n]$. Offenbar gilt $\mathcal{P} \cap A \supseteq (a_1, \ldots, a_k)_A$, und da $K[V]/A$ eine ganze Erweiterung von Integritätsringen mit A normal ist, gilt „going-down“ und damit ([40, Korollar VI.2.9]) $k = \text{height}(\mathcal{P}) = \text{height}(\mathcal{P} \cap A) \geq \text{height}(a_1, \ldots, a_k)_A = k$, also $\mathcal{P} \cap A = (a_1, \ldots, a_k)_A$, denn auf beiden Seiten stehen Primideale von A. Nun gibt es nach „going-down“ ([14, Theorem 13.9]) eine Kette von Primidealen $\mathcal{P} = \mathcal{P}_k \supset \mathcal{P}_{k-1} \supset \ldots \supset \mathcal{P}_0$ von $K[V]$ mit $\mathcal{P}_i \cap A = (a_1, \ldots, a_i)_A$ für $i = 0, \ldots, k$. Dann ist $\wp = \mathcal{P}_k \cap K[V]^G \supseteq \mathcal{P}_{k-1} \cap K[V]^G \supseteq \ldots \supseteq \mathcal{P}_0 \cap K[V]^G$ eine Kette von Primidealen in $K[V]^G$ mit echten Inklusionen; Es gilt nämlich $a_i \in (a_1, \ldots, a_i)_A \subseteq \mathcal{P}_i$ für $1 \leq i \leq k$, also $a_i \in \mathcal{P}_i \cap K[V]^G$, und wäre $a_i \in \mathcal{P}_{i-1} \cap K[V]^G$, so hätte man auch $a_i \in \mathcal{P}_{i-1} \cap A = (a_1, \ldots, a_{i-1})_A$, ein Widerspruch (da A Polynomring). Dies zeigt $\text{height}(\wp) \geq k$. □

Die Invariantentheorie linear reduktiver Gruppen wird entscheidend geprägt von

Satz 1.56 (Hochster und Roberts [28]) *Ist G* linear reduktiv*, so ist $K[V]^G$ Cohen-Macaulay für jeden G-Modul V.*

Zusammen mit dem Satz von Nagata und Miyata 1.53 sind also in Charakteristik 0 Invariantenringe reduktiver Gruppen stets Cohen-Macaulay. Bis heute kennt man in Charakteristik 0 kein Beispiel eines nicht Cohen-Macaulay Invariantenringes.

1.4.2 Roberts' Isomorphismus

Wir werden später massiv von einem Isomorphismus von SL_2-Invariantenringen nach $\mathbb{G}_a$-Invariantenringen gebrauch machen, der (in Charakteristik 0) auf Roberts [52] aus dem Jahr 1861 zurückgeht. Wir geben hier einen Beweis, der im wesentlichen eine Spezialisierung des in [7, Theorem 3.2] gegebenen Beweises für einen allgemeineren Satz ist. Weitere Referenzen sind Tyc [61], Seshadri [55] und Weitzenböck [62].

Ist V ein SL_2-Modul, so ist V auch ein $\mathbb{G}_a$-Modul via

$$t \cdot v := \sigma_t \cdot v \quad \text{mit} \quad \sigma_t := \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2 \quad \text{für } v \in V,\, t \in \mathbb{G}_a. \tag{22}$$

Satz 1.57 (Roberts' Isomorphismus) *Sei V ein beliebiger SL_2-Modul und $U = K^2$ der SL_2-Modul mit der natürlichen Darstellung*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix} \quad \textit{für } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K),\, \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \in U.$$

Wir schreiben $f \in K[U \oplus V]^{\mathrm{SL}_2}$ mit drei Koordinaten, d.h. für die Auswertung von f an einem $((x_1, x_2), v) \in U \oplus V$ schreiben wir $f(x_1, x_2, v)$. Dann ist durch

$$\phi : K[U \oplus V]^{\mathrm{SL}_2} \to K[V]^{\mathbb{G}_a}, \quad f \mapsto \phi(f) := f(1, 0, \cdot)$$

(d.h. für $v \in V$ ist $\phi(f)(v) := f(1, 0, v)$) ein Algebren-Isomorphismus gegeben.

Beweis. Wir prüfen zunächst die Wohldefiniertheit von ϕ. Sei also $f \in K[U \oplus V]^{\mathrm{SL}_2}$. Zu zeigen ist, dass $\phi(f) \in K[V]$ dann $\mathbb{G}_a$-invariant ist. Für $t \in \mathbb{G}_a$, σ_t wie oben und $(1, 0) \in U$ ist $\sigma_t(1, 0) = (1, 0)$. Daher ist für $t \in \mathbb{G}_a, v \in V$

$$\begin{array}{rcl} (t \cdot \phi(f))(v)) & = & \phi(f)(\sigma_{-t}v) = f(1, 0, \sigma_{-t}v) = (f \circ \sigma_{-t})(1, 0, v) \\ & \underset{f \in K[U \oplus V]^{\mathrm{SL}_2}}{=} & f(1, 0, v) = \phi(f)(v). \end{array}$$

Da dies für alle $v \in V$ gilt, ist also $t \cdot \phi(f) = \phi(f)$ für $t \in \mathbb{G}_a$, oder $\phi(f) \in K[V]^{\mathbb{G}_a}$.

Offenbar ist ϕ linear und erfüllt auch $\phi(fg) = \phi(f)\phi(g)$ für $f, g \in K[U \oplus V]^{\mathrm{SL}_2}$, d.h. ϕ ist ein Algebren-Homomorphismus.

Nun zur Injektivität von ϕ. Sei $f \in K[U \oplus V]^{\mathrm{SL}_2}$ und $\phi(f) = 0$. Dann ist

$$f(1, 0, v) = 0 \quad \text{für alle } v \in V.$$

Da für alle $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2$ gilt dass $f = f \circ \sigma^{-1}$, ist dann auch

$$f(1, 0, v) = \left(f \circ \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \right)(1, 0, v) = f(d, -c, \sigma^{-1}v) = 0 \quad \text{für alle } v \in V.$$

Ist $w \in V$ beliebig und setzt man $v := \sigma w$, so gilt also $f(d, -c, w) = 0$ für alle $w \in V$ und alle c, d, die an entsprechender Stelle in Elementen aus SL_2 vorkommen können, also $(c, d) \neq (0, 0)$. Da die beschriebene Menge aller $(d, -c, w)$ in $K^2 \oplus V$ Zariski-dicht liegt, ist also $f = 0 \in K[U \oplus V]$. Also ist ϕ injektiv.

Nun zum schwierigsten Teil des Beweises, der Surjektivität von ϕ. Wir konstruieren ein Urbild zu einem $g \in K[V]^{\mathbb{G}_a}$. Dazu betrachten wir

$$G : \mathrm{SL}_2 \times V \to K, \quad (\sigma, v) \mapsto G(\sigma, v) := g(\sigma^{-1}v).$$

Für σ_t wie in (22) gilt $g \circ \sigma_{-t} = g$ wegen $g \in K[V]^{\mathbb{G}_a}$. Also gilt

$$G(\sigma\sigma_t, v) = g(\sigma_{-t}\sigma^{-1}v) = g(\sigma^{-1}v) = G(\sigma, v) \quad \text{für alle } \sigma \in \mathrm{SL}_2, t \in \mathbb{G}_a, v \in V. \tag{23}$$

Wir interpretieren diese Gleichung nun für $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2$ (also $ad - bc = 1$) und unterscheiden die Fälle $a \neq 0$ und $c \neq 0$.

1.Fall: $a \neq 0$. Dann setzen wir $t := -\frac{b}{a}$ und erhalten aus (23)

$$\begin{aligned} G(\sigma, v) &= G(\sigma\sigma_t, v) = G\left(\begin{pmatrix} a & 0 \\ c & \frac{1}{a} \end{pmatrix}, v\right) \\ &= \frac{1}{a^k} p_1(a, c, v) \quad \text{mit } k \in \mathbb{N}_0 \text{ und } p_1 \in K[U \oplus V]. \end{aligned}$$

Im letzten Schritt wurde verwendet, dass $G(\sigma, v) = g(\sigma^{-1}v)$ ein Polynom in den Koordinaten von σ und v ist, da g ein Polynom ist und die Operation von SL_2 auf V durch Polynome in den Koordinaten a, b, c, d eines $\sigma \in \mathrm{SL}_2$ gegeben ist. Da man für eine Variable $\frac{1}{a}$ einsetzt, kann man einen Hauptnenner der Form a^k ausklammern, und erhält dann das Polynom p_1. Mit diesem (festen) Polynom gilt obige Gleichung dann für alle σ, v mit $a \neq 0$.

2.Fall: $c \neq 0$. Dann setzen wir $t := -\frac{d}{c}$ und erhalten aus (23) analog wie oben

$$\begin{aligned} G(\sigma, v) &= G(\sigma\sigma_t, v) = G\left(\begin{pmatrix} a & -\frac{1}{c} \\ c & 0 \end{pmatrix}, v\right) \\ &= \frac{1}{c^l} p_2(a, c, v) \quad \text{mit } l \in \mathbb{N}_0 \text{ und } p_2 \in K[U \oplus V]. \end{aligned}$$

Sind nun $a \neq 0$ und $c \neq 0$, so sind beide Ausdrücke für $G(\sigma, v)$ gleich, und man erhält

$$c^l p_1(a, c, v) = a^k p_2(a, c, v) \quad \text{für alle } a \neq 0, c \neq 0, v \in V.$$

Da die rechts beschriebene Menge jedoch Zariski-dicht liegt und es sich um eine Polynomgleichung handelt, gilt die Identität allgemein, also gilt auch mit unabhängigen Variablen A, C und $X = (X_1, \ldots, X_n), n = \dim V$ eines Polynomrings $K[A, C, X]$, dass

$$C^l p_1(A, C, X) = A^k p_2(A, C, X).$$

Da A, C teilerfremd sind, folgt $C^l | p_2(A, C, X)$ und $A^k | p_1(A, C, X)$. Daher gilt mit dem Polynom $f := p_1(A, C, X)/A^k = p_2(A, C, X)/C^l \in K[U \oplus V]$, dass

$$G(\sigma, v) = g(\sigma^{-1}v) = g\left(\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} v\right) = f(a, c, v) \quad \text{für alle } \sigma \in \mathrm{SL}_2, v \in V. \tag{24}$$

Wir behaupten, dass f das gesuchte Urbild zu g ist, also $f \in K[U \oplus V]^{\mathrm{SL}_2}$ und $g = \phi(f)$. Wir zeigen zuerst, dass f invariant ist. Sei also $(x, y) \in U \setminus (0, 0), v \in V, \sigma \in \mathrm{SL}_2$. Dann ist

$$(\sigma^{-1}f)(x, y, v) = f(\sigma(x, y), \sigma v) = f(ax + by, cx + dy, \sigma v),$$

und wir müssen zeigen, dass dies gleich $f(x, y, v)$ ist. Aufgrund der Zariski-Dichtheit der beschriebenen Koordinatenmenge in $U \oplus V$ folgt dann allgemein die Invarianz von f. Wir unterscheiden wieder $x \neq 0$ und $y \neq 0$.

1. Fall: $x \neq 0$. Dann ist $\begin{pmatrix} \frac{1}{x} & 0 \\ -y & x \end{pmatrix} \in \mathrm{SL}_2$, und es folgt

$$\begin{aligned} f(x, y, v) &\overset{(24)}{=} g\left(\begin{pmatrix} \frac{1}{x} & 0 \\ -y & x \end{pmatrix} v\right) = g\left(\begin{pmatrix} \frac{1}{x} & 0 \\ -y & x \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \sigma v\right) \\ &= g\left(\begin{pmatrix} * & * \\ -(cx + dy) & ax + by \end{pmatrix} \sigma v\right) \\ &\overset{(24)}{=} f(ax + by, cx + dy, \sigma v). \end{aligned}$$

2. Fall: $y \neq 0$. Wir erhalten analog

$$\begin{aligned} f(x,y,v) &\overset{(24)}{=} g\left(\begin{pmatrix} 0 & \frac{1}{y} \\ -y & x \end{pmatrix} v\right) = g\left(\begin{pmatrix} 0 & \frac{1}{y} \\ -y & x \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\sigma v\right) \\ &= g\left(\begin{pmatrix} * & * \\ -(cx+dy) & ax+by \end{pmatrix}\sigma v\right) \\ &\overset{(24)}{=} f(ax+by, cx+dy, \sigma v). \end{aligned}$$

Damit ist $f \in K[U \oplus V]^{\mathrm{SL}_2}$ gezeigt. Schliesslich gilt mit der Definition von ϕ

$$\phi(f)(v) = f(1,0,v) \overset{(24)}{=} g\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} v\right) = g(v)$$

für alle $v \in V$, also $\phi(f) = g$, so dass f das gesuchte Urbild ist. □

Wir haben Roberts' Isomorphismus hier auf der Ebene von Koordinatenringen $K[V] = S(V^*)$ angegeben. Für uns fast wichtiger ist er auf der Ebene der symmetrischen Algebra $S(V)$. Wir verwenden die Notation im Satz und wie auf S. 27 beschrieben. Es hat $U = \langle X, Y\rangle$ die Darstellung $\sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Daher hat $U^* = \langle X^*, Y^*\rangle$ die Darstellung $\sigma \mapsto \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$, also ist $U^* \cong \langle Y, -X\rangle$ - man hat also die Entsprechung $X^* \mapsto Y$ und $Y^* \mapsto -X$ und wir wollen hier kurz sogar identifizieren. Roberts' Isomorphismus

$$S(\langle X^*, Y^*\rangle \oplus V^*)^{\mathrm{SL}_2} = S(\langle Y, -X\rangle \oplus V^*)^{\mathrm{SL}_2} \to S(V^*)^{\mathbb{G}_a}$$

lässt sich dann beschreiben durch

$$f(X^*, Y^*, T) = f(Y, -X, T) \mapsto f(1, 0, T),$$

wobei $T = (T_1, \ldots, T_n)$ eine Basis von V^* ist. Ersetzen wir V^* durch V, so erhalten wir also als Umformulierung:

Korollar 1.58 (Roberts' Isomorphismus für die symmetrische Algebra) *Sei V ein SL_2-Modul mit Basis $T = (T_1, \ldots, T_n)$, $\langle X, Y\rangle$ der SL_2-Modul mit der natürlichen Darstellung. Dann ist durch*

$$\phi : S(\langle X, Y\rangle \oplus V)^{\mathrm{SL}_2} \to S(V)^{\mathbb{G}_a}, \quad f(X, Y, T) \mapsto f(0, 1, T)$$

ein Isomorphismus gegeben.

Wir wollen uns noch die Umkehrabbildung ansehen. Sei wieder T eine Basis von V. Ist dann $g \in K[V^*]^{\mathbb{G}_a}$, so hat man für ein Urbild $f \in K[U \oplus V^*]^{\mathrm{SL}_2}$ und $(x, y) \in U, x \neq 0, v \in V^*$ gemäß (24):

$$f(x,y,v) = g\left(\begin{pmatrix} 1/x & 0 \\ -y & x \end{pmatrix} v\right) = \left(\begin{pmatrix} x & 0 \\ y & 1/x \end{pmatrix} \cdot g\right)(v).$$

Die Operation von SL_2 ist durch Polynome gegeben. In diese lassen sich aber nicht nur Körperelemente, sondern auch neue Variablen einsetzen. Da wir die Entsprechungen $x \leftrightarrow X^* \leftrightarrow Y$ und $y \leftrightarrow Y^* \leftrightarrow -X$ und $T \leftrightarrow v$ haben, erhalten wir so aus der letzten Gleichung

$$f(Y, -X, T) = \left(\begin{pmatrix} Y & 0 \\ -X & 1/Y \end{pmatrix} \cdot g\right)(T).$$

Wir dürfen hier den Übergang zu Variablen machen, da links eine Polynomfunktion in den Koordinaten x, y, v steht und rechts eine rationale Funktion in x, y, v mit höchstens einer Potenz von x im Nenner. Multipliziert man mit diesem Nenner, hat man ein Gleichung von Polynomfunktionen, die für alle $x \neq 0$ gilt, also auf einer Zariski-dichten Menge. Dann müssen aber auch die entsprechenden Polynome gleich sein, und insbesondere kann der Nenner gekürzt werden, so dass auf beiden Seiten Polynome stehen. Da $f(Y, -X, T)$ das gesuchte Urbild von g ist, erhalten wir also

Korollar 1.59 (Umkehrung von Roberts' Isomorphismus) *Es sei V ein SL_2-Modul und $\langle X, Y\rangle$ der SL_2-Modul mit der natürlichen Darstellung. Dann ist durch*

$$\phi^{-1} : S(V)^{\mathbb{G}_a} \to S(\langle X, Y\rangle \oplus V)^{\mathrm{SL}_2}, \quad g \mapsto \begin{pmatrix} Y & 0 \\ -X & 1/Y \end{pmatrix} \cdot g$$

die Umkehrung von Roberts' Isomorphismus gegeben. Das angegebene Urbildelement $\phi^{-1}(g)$ erhält man dabei dadurch, indem man in die durch Polynome gegebene Operation von SL_2 auf $g \in S(V)$ statt Körperelemente neue unabhängige Variablen X, Y wie angegeben in die entsprechenden Polynome einsetzt (Details im Beweis).

Beispiel. Sei $V = \langle X_1, Y_1\rangle \oplus \langle X_2, Y_2\rangle$ die zweifache Summe der natürlichen Darstellung von SL_2. Wir berechnen die Urbilder der $\mathbb{G}_a$-Invarianten X_1 und $X_1Y_2 - X_2Y_1$:

$$\phi^{-1}(X_1) = YX_1 - XY_1, \text{ und}$$

$$\phi^{-1}(X_1Y_2 - X_2Y_1) = (YX_1 - XY_1) \cdot Y_2/Y - (YX_2 - XY_2) \cdot Y_1/Y = X_1Y_2 - X_2Y_1.$$

Man verifiziert sofort, dass tatsächlich

$$\phi(YX_1 - XY_1) = X_1, \quad \phi(X_1Y_2 - X_2Y_1) = X_1Y_2 - X_2Y_1$$

gilt.

An diesem Beispiel sehen wir auch, dass Roberts' Isomorphismus nicht homogen ist, zumindest dann, wenn wir beidemale die Standardgraduierung verwenden. So ist $\deg YX_1 - XY_1 = 2$, aber $\deg X_1 = 1$. Zumindest bildet ϕ aber die maximalen homogenen Ideale aufeinander ab, d.h. es gilt

$$\phi(S(\langle X, Y\rangle \oplus V)_+^{\mathrm{SL}_2}) = S(V)_+^{\mathbb{G}_a}. \tag{25}$$

Beweis. Sei $f \in S(\langle X, Y\rangle \oplus V)_+^{\mathrm{SL}_2}$. Dann gibt es eine eindeutige Zerlegung $f = g + h$ mit $g \in S(\langle X, Y\rangle) \cdot S(V)_+$ (die Menge der endliche Summen aller Produkte aus beiden Mengen) und $h \in S(\langle X, Y\rangle)$. Da die letzten beiden Mengen SL_2-invariant sind, sind mit f auch g und h invariant, also $h \in S(\langle X, Y\rangle)^{\mathrm{SL}_2} = K$. Da $f \in S(\langle X, Y\rangle \oplus V)_+$ und g keinen konstanten Anteil hat, ist also $h = 0$ und $f = g \in S(\langle X, Y\rangle)S(V)_+$. Da die Anwendung von ϕ einfach ersetzen von $X = 0$, $Y = 1$ bedeutet, ist also $\phi(f) \in S(V)_+$. Dies zeigt die Inklusion „$\subseteq$“ in (25). Da weiter $\phi(K) = K$, also $\phi(S(\langle X, Y\rangle \oplus V)_0^{\mathrm{SL}_2}) = S(V)_0^{\mathbb{G}_a}$ und ϕ bijektiv ist, gilt sogar Gleichheit. □

Wir können ϕ nun dadurch homogen machen, dass wir auf $S(V)^{\mathbb{G}_a}$ einfach die Graduierung von $S(\langle X, Y\rangle \oplus V)^{\mathrm{SL}_2}$ via ϕ vererben. Nach (25) ändert sich bei diesem Wechsel

der Graduierung das maximale homogene Ideal von $S(V)^{\mathbb{G}_a}$ nicht, und damit auch nicht $\operatorname{depth} S(V)^{\mathbb{G}_a} = \operatorname{depth}(S(V)^{\mathbb{G}_a}_+, S(V)^{\mathbb{G}_a})$ (vgl. Definition 1.15). Insbesondere haben wir für jeden SL_2-Modul V, dass

$$\operatorname{cmdef} S(V)^{\mathbb{G}_a} = \operatorname{cmdef} S(\langle X, Y\rangle \oplus V)^{\mathrm{SL}_2}. \tag{26}$$

Man beachte, dass Roberts' Isomorphismus nicht besagt, dass jeder $\mathbb{G}_a$-Invariantenring $S(V)^{\mathbb{G}_a}$ zu einem SL_2-Invariantenring isomorph ist. Als Voraussetzung hierfür muss sich die $\mathbb{G}_a$-Darstellung auf V zu einer SL_2-Darstellung erweitern lassen, so dass man die $\mathbb{G}_a$-Darstellung gemäß (22), S. 41 zurückerhält. Eine solche fortsetzbare Darstellung von $\mathbb{G}_a$ heißt dann *fundamental*. Ein Beispiel für eine nicht fundamentale Darstellung in positiver Charakteristik p ist

$$\mathbb{G}_a \to \mathrm{GL}_3, \quad t \mapsto \begin{pmatrix} 1 & t & t^p \\ & 1 & \\ & & 1 \end{pmatrix},$$

siehe Fauntleroy [16, vor Lemma 2]. In Charakteristik 0 dagegen ist jede $\mathbb{G}_a$-Darstellung fundamental. Wir geben hier nur einen elementaren Beweis für $K = \mathbb{C}$, für den allgemeinen Beweis (für den man die Theorie der Lie-Algebren benötigt) siehe [22, Lemma 10.2] oder [39, III.3.9]. Dann ist also in Charakteristik 0 jeder $\mathbb{G}_a$-Invariantenring isomorph zu einem SL_2-Invariantenring (insbesondere also endlich erzeugt - das ist der Satz von Weitzenböck [62]), und damit nach Hochster und Roberts (Satz 1.56) Cohen-Macaulay. In Charakteristik 0 kann man also nicht nur für reduktive Gruppen, sondern auch für die einfachste nichtreduktive Gruppe $\mathbb{G}_a$ kein Beispiel eines nicht Cohen-Macaulay Invariantenringes finden.

Satz 1.60 *Sei $K = \mathbb{C}$, und $\langle X, Y\rangle$ die Einschränkung der natürlichen Darstellung von* SL_2 *auf $\mathbb{G}_a$, d.h. die Darstellung $\mathbb{G}_a \to \mathrm{GL}_2$, $t \mapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$. Dann ist jede Darstellung von $\mathbb{G}_a$ isomorph zu einer direkten Summe von symmetrischen Potenzen $S^m(\langle X, Y\rangle)$ (für $m = 0$ ist dies gleich K, die triviale Darstellung) und damit insbesondere fundamental.*

Beweis. Wir berechnen zunächst die Darstellung von $S^m(\langle X, Y\rangle) = \langle X^m, X^{m-1}Y, \ldots, Y^m\rangle$. Es ist

$$\begin{aligned} t \cdot X^{m-j}Y^j &= X^{m-j}(tX + Y)^j = \sum_{k=0}^{j} X^{m-j}\binom{j}{k}(tX)^{j-k}Y^k \\ &= \sum_{k=0}^{j}\binom{j}{k}t^{j-k}X^{m-k}Y^k. \end{aligned} \tag{27}$$

Sei nun $\rho : \mathbb{C} \to \mathrm{GL}_n$, $t \mapsto \rho(t)$ eine beliebige Darstellung von $\mathbb{G}_a$, d.h. $\rho(z + w) = \rho(z)\rho(w) = \rho(w + z) = \rho(w)\rho(z)$ für alle $z, w \in \mathbb{C}$ und $\rho(0) = I_n$, wobei I_n die $n \times n$ Einheitsmatrix ist. Da die Einträge von $\rho(z)$ Polynome in z sind, ist die Einschränkung $\rho|_{\mathbb{R}}$ differenzierbar. Mit Hilfe der Funktionalgleichung für ρ erhalten wir dann

$$\begin{aligned} \frac{d\rho}{dt}(t) &= \lim_{h\to 0}\frac{\rho(t+h) - \rho(t)}{h} = \lim_{h\to 0}\frac{\rho(h)\rho(t) - \rho(t)}{h} \\ &= \underbrace{\lim_{h\to 0}\frac{\rho(h) - I_n}{h}}_{=:A}\rho(t) = A\rho(t) \quad \text{für alle } t \in \mathbb{R}. \end{aligned}$$

Die Lösung der *reellen* Differenzialgleichung $\dot{\rho} = A\rho$, $A \in \mathbb{C}^{n\times n}$ mit Anfangswert $\rho(0) = I_n$ ist bekanntlich eindeutig bestimmt und gegeben durch $\rho(t) = \exp(A \cdot t)$, $t \in \mathbb{R}$. Da aber jede Komponente von $z \mapsto \rho(z)$ und $z \mapsto \exp(Az)$ eine holomorphe Funktion ist, und beide Funktionen auf $\mathbb{R}$ übereinstimmen, stimmen sie auf ganz $\mathbb{C}$ überein, also gilt $\rho(z) = \exp(Az)$ für alle $z \in \mathbb{C}$.

Wir zeigen als nächstes, dass alle Eigenwerte von $\rho(z)$ gleich 1 sind für jedes $z \in \mathbb{C}$. Sei also $\lambda \in \mathbb{C}$ ein Eigenwert von $\rho(z)$ und $v \in \mathbb{C}^n \setminus \{0\}$ ein zugehöriger Eigenvektor, also $\rho(z)v = \lambda v$. Sukzessives multiplizieren mit $\rho(z)$ ergibt $\rho(nz)v = \lambda^n v$ für alle $n \in \mathbb{N}$. Da die Einträge von $\rho(nz)$ Polynome in nz sind und v eine Komponente v_i ungleich 0 hat, ergibt sich durch Betrachten dieser Komponente von $\rho(nz)v = \lambda^n v$ und Division durch v_i die Existenz eines Polynoms $P(n)$ mit $P(n) = \lambda^n$ für alle $n \in \mathbb{N}$. Es folgt

$$P(n+1) = \lambda^{n+1} = \lambda P(n) \quad \text{für alle } n \in \mathbb{N}.$$

Da also die beiden Polynomfunktionen $x \mapsto P(x+1)$ und $x \mapsto \lambda P(x)$ auf $\mathbb{N}$ übereinstimmen, sind sie auch als Polynome gleich, also $P(X+1) = \lambda P(X)$. Da aber $P(X+1)$ denselben Grad und Leitkoeffizient wie $P(X)$ hat, folgt $\lambda = 1$.

Da also alle Eigenwerte von $\rho(z)$ gleich 1 sind, gilt $(\rho(z) - I_n)^n = 0$ für alle $z \in \mathbb{C}$, also auch $\left(\frac{\rho(h)-I_n}{h}\right)^n = 0$ für alle $h \in \mathbb{R} \setminus \{0\}$. Der Grenzübergang $h \to 0$ liefert $A^n = 0$, d.h. A ist nilpotent. Die Jordanblöcke von A sind damit von der Form

$$J_m = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix} \in \mathbb{C}^{m+1\times m+1}.$$

Ist $J = SAS^{-1}$ die Jordan-Normalform von A, so ist $\exp(Jz) = S\exp(Az)S^{-1} = S\rho(z)S^{-1}$, liefert also eine eine zu ρ isomorphe Darstellung. Die verschiedenen Jordanblöcke von J entsprechen dabei direkten Summanden der Darstellung. Wir beenden den Beweis, indem wir zeigen dass $z \mapsto \exp(J_m z)$ (bei geeigneter Basiswahl) eine Darstellung von $S^m(\langle X, Y\rangle)$ ist. Bekanntlich ist

$$\exp(J_m t) = \sum_{k=0}^{\infty} \frac{(J_m t)^k}{k!} = \begin{pmatrix} 1 & t & \frac{t^2}{2!} & \frac{t^3}{3!} & \cdots & \frac{t^m}{m!} \\ & 1 & t & \frac{t^2}{2!} & \ddots & \vdots \\ & & 1 & t & \ddots & \frac{t^3}{3!} \\ & & & \ddots & \ddots & \frac{t^2}{2!} \\ & & & & 1 & t \\ & & & & & 1 \end{pmatrix}. \tag{28}$$

Aus (27),

$$t \cdot \frac{1}{j!} X^{m-j} Y^j = \sum_{k=0}^{j} \frac{t^{j-k}}{(j-k)!} \cdot \frac{1}{k!} X^{m-k} Y^k,$$

ersehen wir, dass die Darstellung von $S^m(\langle X, Y\rangle)$ bezüglich der Basis $\{\frac{1}{j!} X^{m-j} Y^j : j = 0, \ldots, m\}$ genau durch (28) gegeben ist. □

1.4.3 Die Dimension von Invariantenringen

Wir geben hier einige Zusammenhänge von $\dim K[V]^G$, $\dim_K V$ und $\dim G$. Sei ferner $K(V) := \mathrm{Quot}(K[V])$ der *Körper der rationalen Funktionen auf* V. Für einen G-Modul V operiert G in kanonischer Weise auch auf $K(V)$. Dann ist

$$K(V)^G := \{f \in K(V) : \sigma \cdot f = f \text{ für alle } \sigma \in G\}$$

der *Invariantenkörper*. Da er Zwischenkörper der endlich erzeugten Körpererweiterung $K \leq K(V)$ ist, ist er nach [47, Theorem 4.1.5] stets endlich erzeugt über K.

Offenbar gilt $K(V)^G \supseteq \mathrm{Quot}(K[V]^G)$. Das folgende Lemma (siehe [13, Exercise 6.10]) gibt ein Kriterium, wann Gleichheit gilt.

Lemma 1.61 *Sei G eine lineare algebraische Gruppe, so dass jeder algebraische Gruppenhomomorphismus $G \to \mathbb{G}_m \cong (K \setminus \{0\}, \cdot)$ trivial ist. Dann gilt*

$$K(V)^G = \mathrm{Quot}\, K[V]^G$$

für jeden G-Modul V.

Man beachte dabei, dass ein algebraischer Homomorphismus $\chi : G \to \mathbb{G}_m = \{(a,b) \in K^2 : ab - 1 = 0\} \cong (K \setminus \{0\}, \cdot)$ ein Gruppenhomomorphismus ist, der durch einen Morphismus von Varietäten gegeben ist. Schreibt man $\chi = (\chi', \chi'')$, so ist also $\chi' \in K[G]$ und χ' induziert einen Gruppenhomomorphismus $G \to (K \setminus \{0\}, \cdot)$.

Ist umgekehrt durch $\chi' \in K[G]$ ein Gruppenhomomorphismus $G \to (K \setminus \{0\}, \cdot)$ gegeben, so ist durch $\chi : G \to \mathbb{G}_m$, $\sigma \mapsto (\chi'(\sigma), \chi'(\sigma^{-1}))$ ein algebraischer Gruppenhomomorphismus gegeben, denn $\chi'(\sigma)\chi'(\sigma^{-1}) = \chi'(\sigma\sigma^{-1}) = 1$ (also $\chi(\sigma) \in \mathbb{G}_m$), und da $G \to G, \sigma \mapsto \sigma^{-1}$ ein Morphismus ist (und damit $(\sigma \mapsto \chi'(\sigma^{-1})) \in K[G]$), ist auch χ ein Morphismus.

Die algebraischen Gruppenhomomorphismen $G \to \mathbb{G}_m$ entsprechen also eindeutig den $\chi' \in K[G]$, die einen Homomorphismus $G \to (K \setminus \{0\}, \cdot)$ induzieren. (Vgl. Bemerkung 1.31; es ist $\mathbb{G}_m = \mathrm{GL}_1$.)

Beweis des Lemmas. Sei $0 \neq f \in K(V)^G$ und $g, h \in K[V]$ teilerfremd mit $f = \frac{g}{h}$ sowie $\sigma \in G$. Aus $f = \sigma \cdot f$ folgt $g(\sigma \cdot h) = h(\sigma \cdot g)$, also $h | g(\sigma \cdot h)$. Da h, g teilerfremd, folgt also $h | \sigma \cdot h$, und da $\deg h = \deg \sigma \cdot h$ gibt es ein $\chi(\sigma) \in K \setminus \{0\}$ mit $\sigma \cdot h = \chi(\sigma)h$. Da die Operation von σ auf h durch Polynome in den Koordinaten von σ gegeben ist, gilt $\chi \in K[G]$. Ferner sieht man aus $\chi(\sigma\tau)h = (\sigma\tau) \cdot h = \sigma(\tau h) = \sigma \cdot (\chi(\tau)h) = \chi(\sigma)\chi(\tau)h$, dass $\chi(\sigma\tau) = \chi(\sigma)\chi(\tau)$ für alle $\sigma, \tau \in G$, also dass χ ein algebraischer Homomorphismus $G \to \mathbb{G}_m$ ist. Nach Voraussetzung ist also $\chi = 1$ und damit $h \in K[V]^G$. Dann ist auch $g = fh \in K[V]^G$. Dies zeigt $f \in \mathrm{Quot}(K[V]^G)$ und damit die fehlende Inklusion. □

Dass die Aussage des Lemmas für endliche Gruppen G gilt (wo es durchaus nichttriviale Homomorphismen $G \to \mathbb{G}_m$ geben kann, z.B. $G \subseteq \mathbb{G}_m$ endliche Untergruppe), sieht man an der Gleichung (Bezeichnungen wie im Beweis)

$$f = \frac{g}{h} = \frac{g \cdot \prod_{\sigma \in G \setminus \{\iota\}} \sigma h}{\prod_{\sigma \in G} \sigma h}.$$

Dann ist $\prod_{\sigma \in G} \sigma h \in K[V]^G$ und mit f ist auch $f \cdot \prod_{\sigma \in G} \sigma h = g \cdot \prod_{\sigma \in G \setminus \{\iota\}} \sigma h$ invariant, also in $K[V]^G$. Damit ist $f \in \mathrm{Quot}\, K[V]^G$.

Satz 1.62 *Sei G eine lineare algebraische Gruppe und V ein G-Modul. Dann gilt*

$$\operatorname{trdeg} K(V)^G/K \geq \dim V - \dim G.$$

Ist jeder algebraische Homomorphismus $G \to \mathbb{G}_m \cong (K \setminus \{0\}, \cdot)$ trivial, und ist $K[V]^G$ endlich erzeugt, so gilt insbesondere

$$\dim K[V]^G \geq \dim V - \dim G. \tag{29}$$

Hierbei ist $\dim G = \dim K[G]$ die Krulldimension der affinen Varietät G und $\dim V$ die Dimension von V als K-Vektorraum (was gleich der Dimension von V als affine Varietät ist).

Beweis. Die erste Aussage des Satzes folgt aus Dolgachev [13, Corollary 6.2] oder Popov/Vinberg *Invariant Theory* in [56, Corollary zu Lemma 2.4, p. 156 und Formel in Section 1.4, p. 151]. Unter der Zusatzvoraussetzung gilt dann nach Lemma 1.61, dass $K(V)^G = \operatorname{Quot} K[V]^G$, und aus $\dim K[V]^G = \operatorname{trdeg} \operatorname{Quot}(K[V]^G)/K$ für endlich erzeugtes $K[V]^G$ folgt dann die Behauptung. □

Satz 1.63 *Es gibt keinen nichttrivialen algebraischen Homomorphismus $\mathbb{G}_a \to \mathbb{G}_m$. Insbesondere gilt für jeden $\mathbb{G}_a$-Modul V stets $K(V)^{\mathbb{G}_a} = \operatorname{Quot} K[V]^{\mathbb{G}_a}$. Ist $K[V]^{\mathbb{G}_a}$ endlich erzeugt, so gilt außerdem $\dim K[V]^{\mathbb{G}_a} \geq \dim V - 1$.*

Beweis. Sei

$$\lambda : \mathbb{G}_a \to \mathbb{G}_m, \quad a \mapsto \sum_{k=0}^{n} \lambda_k a^k \quad \text{mit } \lambda_k \in K \text{ und } \lambda_n \neq 0$$

ein algebraischer Homomorphismus. Es folgt

$$1 = \lambda(0) = \lambda(a)\lambda(-a) = \left(\sum_{k=0}^{n} \lambda_k a^k\right)\left(\sum_{k=0}^{n} \lambda_k (-a)^k\right) \quad \text{für alle } a \in K.$$

Koeffizientenvergleich liefert sofort $n = 0$, also $\lambda(a) = \lambda_0 = \lambda(0) = 1$ für alle $a \in \mathbb{G}_a$.

Die restlichen beiden Aussagen folgen sofort aus Lemma 1.61 und Satz 1.62 mit $\dim \mathbb{G}_a = \dim K^1 = 1$. □

Dagegen ist $\exp : (\mathbb{C}, +) \to (\mathbb{C} \setminus \{0\}, \cdot)$ zwar ein Gruppenhomomorphismus, aber eben nicht algebraisch.

Satz 1.64 *Es gibt keinen nichttrivialen Gruppenhomomorphismus $\mathrm{SL}_n \to \mathbb{G}_m$. Insbesondere gilt für jeden SL_n-Modul V stets $K(V)^{\mathrm{SL}_n} = \operatorname{Quot} K[V]^{\mathrm{SL}_n}$ und*

$$\dim K[V]^{\mathrm{SL}_n} \geq \dim V - n^2 + 1.$$

Beweis. Sei $\phi : \mathrm{SL}_n \to \mathbb{G}_m$ ein Gruppenhomomorphismus. Dann ist $\phi(\mathrm{SL}_n) \subseteq \mathbb{G}_m$ insbesondere abelsch, und damit liegt die *Kommutatorgruppe* SL_n' im Kern von ϕ, also $\mathrm{SL}_n' \subseteq \ker \phi$. Nach Hein [24, Satz I.6.9] gilt aber $\mathrm{SL}_n' = \mathrm{SL}_n$ (d.h. SL_n ist *perfekt*), also ist $\ker \phi = \mathrm{SL}_n$ und damit ϕ trivial.

Die restlichen beiden Aussagen folgen nun wieder aus Satz 1.62 mit $\dim \mathrm{SL}_n = n^2 - 1$. Da SL_n reduktiv ist, ist $K[V]^{\mathrm{SL}_n}$ stets endlich erzeugt. □

Dass es keinen *algebraischen* Homomorphismus $\mathrm{SL}_n \to \mathbb{G}_m$ gibt, kann man auch leicht beweisen, ohne dass man die Perfektheit von SL_n benutzen muss: Sei also $\phi : \mathrm{SL}_n \to \mathbb{G}_m$ ein algebraischer Homomorphismus. Sei $I_n \in K^{n\times n}$ die $n \times n$ Einheitsmatrix und $E_{ij} = (\delta_{ki}\delta_{lj})_{kl} \in K^{n\times n}$ die Matrix, die genau in der i-ten Zeile und j-ten Spalte eine 1 und sonst nur Nullen hat. Für $i \neq j$ sei $N_{ij}(a) := I_n + aE_{ij}$. Bekanntlich wird SL_n erzeugt von der Menge $\{N_{ij}(a) : i \neq j, 1 \leq i, j \leq n, a \in K\}$ (Gauss-Algorithmus, siehe auch Hein [24, Satz I.2.8]). Da $N_{ij}(a)N_{ij}(b) = N_{ij}(a + b)$ für $a, b \in K$, ist die Abbildung

$$\phi \circ N_{ij} : \mathbb{G}_a \to \mathbb{G}_m, \quad a \mapsto \phi\left(N_{ij}\left(a\right)\right)$$

ein algebraischer Homomorphismus, also nach Satz 1.63 trivial. Damit gilt $\phi\left(N_{ij}\left(a\right)\right) = 1$ für alle $i \neq j$ und $a \in K$. Da also ϕ auf einem Erzeugendensystem von SL_n konstant gleich 1 ist, ist ϕ trivial.

Dagegen ist etwa $\det : \mathrm{GL}_n \to \mathbb{G}_m$ ein nichttrivialer algebraischer Homomorphismus. Seien $\langle X_i, Y_i\rangle$ jeweils die natürliche Darstellung der GL_2 und $V^* := \bigoplus_{i=1}^n \langle X_i, Y_i\rangle$. Dann ist bekanntlich $K[V]^{\mathrm{GL}_2} = K$ (siehe etwa [11]). Dagegen ist $\frac{X_1Y_2 - X_2Y_1}{X_1Y_3 - X_3Y_1} \in K(V)^{\mathrm{GL}_2}$. Es ist also $K(V)^{\mathrm{GL}_2} \neq \operatorname{Quot} K[V]^{\mathrm{GL}_2}$. Außerdem ist $\dim K[V]^{\mathrm{GL}_2} = 0 \not\geq \dim V - \dim \mathrm{GL}_2 = 2n - 4$ für $n > 2$. Gleichung (29) gilt also nicht allgemein.

Satz 1.65 *Sei G eine lineare algebraische Gruppe und V ein G-Modul, so dass die Darstellung $G \to \mathrm{GL}(V)$ unendliches Bild hat. Ist dann $K[V]^G$ endlich erzeugt, so gilt*

$$\dim K[V]^G < \dim V.$$

Beweis. Sei $n = \dim V$ und $\sigma \mapsto A_\sigma \in K^{n\times n}$ die Darstellung von G auf V bzgl. einer Basis. Nach Voraussetzung ist die Menge $\{A_\sigma : \sigma \in G\}$ unendlich. Dann gibt es auch eine Zeile i, so dass $\{e_i^T A_\sigma : \sigma \in G\}$ (mit $e_i \in K^n$ i-ter Spalteneinheitsvektor) unendlich ist. Ist $V^* = \langle X_1, \ldots, X_n\rangle$ mit Darstellung $\sigma \mapsto A_{\sigma^{-1}}^T$, so ist $A_{\sigma^{-1}}^T e_i$ der Koordinatenvektor von $\sigma \cdot X_i$. Also ist $\{\sigma \cdot X_i : \sigma \in G\}$ unendlich. Es ist $K[V] = S(V^*) = K[X_1, \ldots, X_n]$. Jedenfalls ist $\dim K[V]^G = \operatorname{trdeg} \operatorname{Quot}(K[V]^G)/K \leq \operatorname{trdeg} K(V)/K = n$. Angenommen, es wäre $\dim K[V]^G = n$. Dann wäre $\operatorname{trdeg} \operatorname{Quot}(K[V]^G)/K = n = \operatorname{trdeg} K(V)/K$, also wegen der Additivität des Transzendenzgrades $\operatorname{trdeg} K(V)/\operatorname{Quot}(K[V]^G) = 0$. Insbesondere wäre $X_i \in K(V)$ algebraisch über $\operatorname{Quot}(K[V]^G)$. Daher gäbe es ein $0 \neq f \in \operatorname{Quot}(K[V]^G)[T]$ mit $f(X_i) = 0$. Da die Koeffizienten von f invariant unter G sind, folgt dann

$$0 = \sigma \cdot 0 = \sigma \cdot f(X_i) = f(\sigma \cdot X_i) \quad \text{für alle } \sigma \in G.$$

Also hätte f die unendlich vielen Nullstellen $\sigma \cdot X_i, \sigma \in G$, ein Widerspruch. □

Damit erhalten wir die folgende Charakterisierung endlicher Gruppen:

Korollar 1.66 *Sei G eine reduktive Gruppe. G ist genau dann endlich, wenn für jeden G-Modul V $\dim K[V]^G = \dim V$ gilt.*

Beweis. Ist G endlich, so ist $K[V]/K[V]^G$ sogar ganz, insbesondere also $\dim K[V]^G = \dim K[V] = \dim V$. Ist G unendlich, so ist für eine nach Satz 1.33 existierende treue Darstellung V das Bild von $G \to \mathrm{GL}(V)$ mit G unendlich, und nach obigem Satz gilt dann $\dim K[V]^G < \dim V$. □

Bemerkung 1.67 *Jede echte abgeschlossene Teilmenge (insbesondere jede echte abgeschlossene Untergruppe) von $\mathbb{G}_a = K^1$ ist endlich. Insbesondere hat eine nichttriviale rationale Darstellung $\rho : \mathbb{G}_a \to \mathrm{GL}(V)$ stets endlichen Kern und unendliches Bild $\rho(\mathbb{G}_a)$.*

Beweis. Da $K[\mathbb{G}_a] \cong K[X]$ ein Hauptidealring ist, ist jede echte abgeschlossene Teilmenge von $\mathbb{G}_a$ Nullstellenmenge eines nichtkonstanten Polynoms und somit endlich. Ist ρ eine nichttriviale rationale Darstellung von $\mathbb{G}_a$, so ist $\ker \rho = \rho^{-1}(\mathrm{id}_V)$ also als echte abgeschlossene Untergruppe von $\mathbb{G}_a$ endlich. Dann ist $\rho(\mathbb{G}_a) \cong \mathbb{G}_a/\ker \rho$ natürlich unendlich. □

Ein Beispiel für eine nichttriviale und nichttreue Darstellung der $\mathbb{G}_a$ ist zum Beispiel für $\mathrm{char}\, K = p,\ q = p^n > 1$ gegeben durch $\rho : \mathbb{G}_a \to \mathrm{GL}_2,\ a \mapsto \begin{pmatrix} 1 & a^q - a \\ & 1 \end{pmatrix}$ mit $\ker \rho = \mathbb{F}_q$.

Korollar 1.68 *Sei V ein nichttrivialer $\mathbb{G}_a$-Modul und $K[V]^{\mathbb{G}_a}$ endlich erzeugt ist. Dann gilt*

$$\dim K[V]^{\mathbb{G}_a} = \dim V - 1$$

Beweis. Dies folgt mit der Bemerkung sofort aus den Sätzen 1.63 und 1.65. □

Korollar 1.69 *Sei V' ein nichttrivialer SL_2-Modul, $\langle X, Y\rangle$ die natürliche Darstellung der SL_2 und $V := V' \oplus \langle X, Y\rangle$. Dann gilt*

$$\dim K[V]^{\mathrm{SL}_2} = \dim V - 3.$$

Beweis. Nach Roberts' Isomorphismus 1.57 ist $K[V]^{\mathrm{SL}_2} \cong K[V']^{\mathbb{G}_a}$. Wir zeigen, dass V' auch nichttrivialer $\mathbb{G}_a$-Modul ist, wobei hier $\mathbb{G}_a = \left\{ \begin{pmatrix} 1 & a \\ & 1 \end{pmatrix} : a \in K \right\} \subseteq \mathrm{SL}_2$. Sei $\rho : \mathrm{SL}_2 \to \mathrm{GL}(V')$ die Darstellung von V'. Nach Voraussetzung ist $\ker \rho \lhd \mathrm{SL}_2$ ein echter Normalteiler. Nach Hein [24, Satz 1.2.12, 1.2.10] folgt hieraus $\ker \rho \subseteq \{I_2, -I_2\}$. Insbesondere ist $\mathbb{G}_a \cap \ker \rho = \{I_2\}$ und damit V' sogar ein treuer $\mathbb{G}_a$-Modul. Also gilt nach dem letzten Korollar

$$\dim K[V]^{\mathrm{SL}_2} = \dim K[V']^{\mathbb{G}_a} = \dim V' - 1 = \dim V - 3.$$

□

An dem Beweis sehen wir auch, dass jede nichttriviale, fundamentale (also auf SL_2 fortsetzbare) Darstellung der $\mathbb{G}_a$ treu ist; Insbesondere ist die oben angegebene nicht treue Darstellung der $\mathbb{G}_a$ nicht fundamental.

Bemerkung 1.70 Das Korollar gilt auch, wenn $V = \langle X^p, Y^p\rangle \oplus V'$ ist. Wir werden nämlich in Satz 5.1 sehen, dass

$$S(\langle X^p, Y^p\rangle \oplus V')^{\mathrm{SL}_2} \cong S(\langle X, Y\rangle \oplus V')^{\mathrm{SL}_2} \cap K[X^p, Y^p] \otimes S(V')$$

gilt. Außerdem ist $R_1 := S(\langle X, Y\rangle \oplus V')^{\mathrm{SL}_2}$ ganz über $R_2 := S(\langle X, Y\rangle \oplus V')^{\mathrm{SL}_2} \cap K[X^p, Y^p] \otimes S(V')$, denn für $f \in R_1$ ist $f^p \in R_2$. Dann ist also $\dim R_2 = \dim R_1 = \dim V' - 1$, und damit auch $\dim S(V)^{\mathrm{SL}_2} = \dim R_2 = \dim V - 3$.

2 Kohomologie von Gruppen

Dieser Abschnitt ist im wesentlichen als Exkurs zu verstehen, da die Resultate im weiteren nicht verwendet werden. Ziel ist es, eine Verallgemeinerung von Proposition 1.51 für höhere Kohomologie zu geben. Das Ergebnis könnte zwar im Zusammenhang etwa mit [32, Theorem 1.4 oder Corollary 1.6] von Bedeutung sein, aber da sich die gemeinsamen Voraussetzungen schwer unter einen Hut bringen lassen, ist das Ergebnis mehr von „akademischem Interesse“. Wer an dieser Verallgemeinerung nicht interessiert ist, kann diesen Abschnitt daher (evtl. nach Einführung der Grundbegriffe in Abschnitt 2.1) überspringen. Im Gegensatz zu der in der Literatur üblichen abstrakten Einführung der n-ten Kohomologiegruppen als $\mathrm{Ext}^n_{KG}(K,V)$ verwenden wir den expliziten und elementaren Zugang über n-Kozyklen.

Eine weitere Besonderheit dieses Abschnitts ist eine andere Bedeutung bereits verwendeter Begriffe. Zunächst ist G hier eine *beliebige* (also nicht notwendig lineare algebraische) Gruppe. Trägt G zusätzlich eine algebraische Struktur, wird diese ignoriert. Einen *G-Modul* (oder auch KG-Modul) nennen wir in diesem Abschnitt einen (nicht notwendig endlich-dimensionalen) K-Vektorraum V, auf dem G linear operiert (auch für eine lineare algebraische Gruppe muss die Operation nicht durch einen Morphismus gegeben sein).

2.1 Koketten, Kozyklen und Koränder

Sei G eine Gruppe und V ein G-Modul. Es sei

$$C^n(G,V) := \{g : G^n \to V\}, \quad n \geq 1$$

die Menge aller Abbildungen von G^n nach V und

$$C^0(G,V) := V.$$

Ist $v \in C^0(G,V)$ und $f : V \to W$ eine Abbildung in einen G-Modul W, so schreiben wir auch $f \circ v$ für $f(v)$. Dann ist $f \circ v \in C^0(G,W)$. Ein Element $g \in C^n(G,V)$ mit $n \geq 0$ heißt *n-Kokette (mit Koeffizienten in V)*. Offenbar ist $C^n(G,V)$ in kanonischer Weise KG-Modul (für $g \in C^n(G,V)$, $\sigma \in G$ ist σg definiert durch $(\sigma g)(x) := \sigma(g(x))$ für alle $x \in G^n$), inbesondere also auch K-Vektorraum und additive Gruppe. Wir betrachten für $n \geq 0$ die K-lineare Abbildung

$$\partial^V_n : C^n(G,V) \to C^{n+1}(G,V), \quad g \mapsto \partial^V_n g$$

mit

$$\begin{aligned} \partial^V_n g(\sigma_1,\ldots,\sigma_{n+1}) \;:=\; & \sigma_1 g(\sigma_2,\ldots,\sigma_{n+1}) + \sum_{i=1}^{n} (-1)^i g(\sigma_1,\ldots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\ldots,\sigma_{n+1}) \\ & +(-1)^{n+1} g(\sigma_1,\ldots,\sigma_n) \quad \text{für } (\sigma_1,\ldots,\sigma_{n+1}) \in G^{n+1}. \end{aligned} \tag{30}$$

Falls keine Verwechslungsgefahr besteht, schreiben wir auch ∂_n statt ∂^V_n. Wir schreiben die Formel für $n = 0, 1, 2$ und jeweils $g \in C^n(G,V)$ explizit auf:

$$\begin{aligned} \partial_0 g(\sigma) &= \sigma g - g \quad \text{für alle } \sigma \in G \quad (\text{hier ist } g \in C^0(G,V) = V) \\ \partial_1 g(\sigma,\tau) &= \sigma g(\tau) - g(\sigma\tau) + g(\sigma) \quad \text{für alle } \sigma,\tau \in G \\ \partial_2 g(\sigma_1,\sigma_2,\sigma_3) &= \sigma_1 g(\sigma_2,\sigma_3) - g(\sigma_1\sigma_2,\sigma_3) + g(\sigma_1,\sigma_2\sigma_3) - g(\sigma_1,\sigma_2) \quad \forall \sigma_1,\sigma_2,\sigma_3 \in G. \end{aligned}$$

Wir definieren

$$Z^n(G,V) := \ker \partial_n^V \subseteq C^n(G,V), \quad n \geq 0,$$

die additive Gruppe der *n-Kozyklen (mit Koeffizienten in V)*. Im nächsten Unterabschnitt zeigen wir $\partial_{n+1}^V \circ \partial_n^V = 0$ für alle $n \geq 0$, daher ist die Gruppe der *n-Koränder (mit Koeffizienten in V)*,

$$B^n(G,V) := \operatorname{im} \partial_{n-1}^V \subseteq Z^n(G,V), \quad n \geq 1,$$

eine Untergruppe von $Z^n(G,V)$. Die Faktorgruppe

$$H^n(G,V) := Z^n(G,V)/B^n(G,V), \quad n \geq 1$$

heißt *n-te Kohomologiegruppe von G (mit Koeffizienten in V)*. Wir setzen auch $H^0(G,V) := Z^0(G,V) = V^G$ und $B^0(G,V) := 0$. Ein n-Kozyklus $g \in Z^n(G,V)$ heißt *trivial*, falls $g \in B^n(G,V)$, sonst *nichttrivial*.

Ein 0-Kozyklus ist also eine Invariante $g \in V^G$. Ein 1-Korand ist eine Abbildung $g : G \to V$, für die es ein $v \in V = C^0(G,V)$ gibt mir $g(\sigma) = \sigma v - v$ für alle $\sigma \in G$. Ein 1-Kozyklus ist eine Abbildung $g : G \to V$, die die Funktionalgleichung $g(\sigma\tau) = \sigma g(\tau) + g(\sigma)$ für alle $\sigma, \tau \in G$ erfüllt. In Abschnitt 1.3, wo wir die erste Kohomologie *algebraischer* Gruppen definiert haben, haben wir zusätzlich gefordert, dass g ein Morphismus ist. Um die n-te Kohomologie *algebraischer* Gruppen zu definieren, würde man für eine lineare algebraische Gruppe G und eine rationale Darstellung V überall $C^n(G,V)$ durch

$$C^n_{mor}(G,V) := \{f : G^n \to V, \quad f \text{ Morphismus}\}$$

ersetzen (für endliche Gruppen ist dies gleich $C^n(G,V)$). In diesem Exkurs werden wir dies jedoch nicht weiter verfolgen.

2.2 Der Kokomplex

Wir müssen noch zeigen, dass

$$\ldots \overset{\partial_{n-1}^V}{\to} C^n(G,V) \overset{\partial_n^V}{\to} C^{n+1}(G,V) \overset{\partial_{n+1}^V}{\to} C^{n+2}(G,V) \overset{\partial_{n+2}^V}{\to} \ldots$$

ein *Kokomplex* ist, d.h. dass

$$\partial_{n+1}^V \circ \partial_n^V = 0 \in \operatorname{Hom}_K(C^n(G,V), C^{n+2}(G,V))$$

ist. (Bei einem Kokomplex ist die Indizierung nach rechts aufsteigend, bei einem Komplex absteigend). Dies lässt sich direkt durch Anwenden der Definitionsgleichung zeigen, doch ist die entstehende Rechung etwas unübersichtlich. Stattdessen gehen wir ähnlich wie in Benson [2, section 3.4] in mehreren Schritten vor.

Beweis. (i) Wir betrachten für $n \geq 1$ folgenden Untervektorraum von $C^n(G,V)$,

$$L^n(G,V) := \{h \in C^n(G,V) : h(\sigma\sigma_1, \ldots, \sigma\sigma_n) = \sigma h(\sigma_1, \ldots, \sigma_n) \quad \text{für } \sigma, \sigma_1, \ldots, \sigma_n \in G\}.$$

Dann ist durch

$$\Psi_n : C^n(G,V) \to L^{n+1}(G,V), \quad g \mapsto \Psi_n g \quad (n \geq 0)$$

mit

$$\Psi_n g(\sigma_0, \ldots, \sigma_n) := \sigma_0 g(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \ldots, \sigma_{n-1}^{-1}\sigma_n) \quad \text{für alle } \sigma_0, \ldots, \sigma_n \in G$$

eine K-lineare Abbildung gegeben; Für die Wohldefiniertheit überprüfen wir

$$\begin{aligned} \Psi_n g(\sigma\sigma_0, \ldots, \sigma\sigma_n) &= \sigma\sigma_0 g(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \ldots, \sigma_{n-1}^{-1}\sigma_n) \\ &= \sigma\Psi_n g(\sigma_0, \ldots, \sigma_n) \quad \text{für alle } \sigma, \sigma_0, \ldots, \sigma_n \in G, \end{aligned}$$

also tatsächlich $\Psi_n g \in L^{n+1}(G, V)$. Weiter betrachten wir die lineare Abbildung

$$\Phi_n : L^{n+1}(G, V) \to C^n(G, V), \quad h \mapsto \Phi_n h \quad (n \geq 0)$$

mit

$$\Phi_n h(\sigma_1, \ldots, \sigma_n) := h(1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1\sigma_2 \cdot \ldots \cdot \sigma_n) \quad \text{für alle } \sigma_1, \ldots, \sigma_n \in G.$$

Wir bezeichnen hier mit $1 \in G$ das neutrale Element von G.

(ii) Wir zeigen

$$\Psi_n \circ \Phi_n = \mathrm{id}_{L^{n+1}(G,V)} \quad \text{und} \quad \Phi_n \circ \Psi_n = \mathrm{id}_{C^n(G,V)} \quad (n \geq 0). \tag{31}$$

(Die zweite Gleichung benötigen wir nicht und dient nur der Vollständigkeit.)
Für $\sigma_0, \ldots, \sigma_n \in G$ und $h \in L^{n+1}(G, V), g \in C^n(G, V)$ gilt nämlich

$$\begin{aligned} \Psi_n \Phi_n h(\sigma_0, \ldots, \sigma_n) &= \sigma_0 \Phi_n h(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \ldots, \sigma_{n-1}^{-1}\sigma_n) \\ &= \sigma_0 h(1, \sigma_0^{-1}\sigma_1, \sigma_0^{-1}\sigma_2, \ldots, \sigma_0^{-1}\sigma_n) \\ &= h(\sigma_0, \ldots, \sigma_n) \end{aligned}$$

(im letzten Schritt haben wir $h \in L^{n+1}(G, V)$ verwendet), also $\Psi_n \Phi_n h = h$, und analog

$$\begin{aligned} \Phi_n \Psi_n g(\sigma_1, \ldots, \sigma_n) &= \Psi_n g(1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1 \cdot \ldots \cdot \sigma_n) \\ &= g(\sigma_1, \ldots, \sigma_n), \end{aligned}$$

also $\Phi_n \Psi_n g = g$.

(iii) Wir betrachten nun die lineare Abbildung

$$\delta_n : L^n(G, V) \to L^{n+1}(G, V), \quad h \mapsto \delta_n h \quad (n \geq 1)$$

mit

$$\delta_n h(\sigma_0, \ldots, \sigma_n) := \sum_{i=0}^{n} (-1)^i h(\sigma_0 \ldots, \hat{\sigma_i}, \ldots, \sigma_n) \quad \text{für alle } \sigma_0, \ldots, \sigma_n \in G,$$

wobei das Dach $\hat{}$ bedeutet, dass der Eintrag gestrichen wird. Man prüft leicht nach, dass $\delta_n h \in L^{n+1}(G, V)$ gilt. Als nächstes zeigen wir

$$\delta_{n+1} \circ \delta_n = 0 \in \mathrm{Hom}_K(L^n(G, V), L^{n+2}(G, V)) \quad (n \geq 1), \tag{32}$$

dass also ein Kokomplex vorliegt: Für $\sigma_0, \ldots, \sigma_{n+1} \in G$ gilt

$$\begin{aligned}\delta_{n+1}\delta_n h(\sigma_0, \ldots, \sigma_{n+1}) &= \sum_{i=0}^{n+1}(-1)^i \delta_n h(\sigma_0 \ldots, \hat{\sigma_i}, \ldots, \sigma_{n+1}) \\ &= \sum_{i=0}^{n+1}(-1)^i \Big(\sum_{j=0}^{i-1}(-1)^j h(\sigma_0, \ldots, \hat{\sigma_j} \ldots, \hat{\sigma_i}, \ldots, \sigma_{n+1}) \\ &\quad + \sum_{j=i+1}^{n+1}(-1)^{j+1} h(\sigma_0, \ldots, \hat{\sigma_i} \ldots, \hat{\sigma_j}, \ldots, \sigma_{n+1}) \Big) = 0.\end{aligned}$$

(iv) Wir zeigen nun

$$\partial_n^V = \Phi_{n+1} \circ \delta_{n+1} \circ \Psi_n \quad (n \geq 0). \tag{33}$$

Für $g \in C^n(G, V)$ und $\sigma_1, \ldots, \sigma_{n+1} \in G$ gilt

$$\begin{aligned}\Phi_{n+1}\delta_{n+1}\Psi_n g(\sigma_1, \ldots, \sigma_{n+1}) &= \delta_{n+1}\Psi_n g(1, \sigma_1, \ldots, \sigma_1\sigma_2 \cdot \ldots \cdot \sigma_{n+1}) \\ &= \Psi_n g(\sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1\sigma_2 \cdot \ldots \cdot \sigma_{n+1}) \\ &\quad + \sum_{i=1}^{n+1}(-1)^i \Psi_n g(1, \sigma_1, \ldots, \sigma_1 \widehat{\cdot \ldots \cdot} \sigma_i, \ldots, \sigma_1\sigma_2 \cdot \ldots \cdot \sigma_{n+1}) \\ &= \sigma_1 g(\sigma_2, \ldots, \sigma_{n+1}) + \sum_{i=1}^{n}(-1)^i g(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{n+1}) \\ &\quad + (-1)^{n+1} g(\sigma_1, \sigma_2, \ldots, \sigma_n) \\ &= \partial_n^V g(\sigma_1, \sigma_2, \ldots, \sigma_{n+1}).\end{aligned}$$

(v) Damit folgt dann für $n \geq 0$

$$\begin{aligned}\partial_{n+1}^V \circ \partial_n^V &\overset{(33)}{=} \Phi_{n+2} \circ \delta_{n+2} \circ \underbrace{\Psi_{n+1} \circ \Phi_{n+1}}_{=\mathrm{id}_{L^{n+2}(G,V)} \ (31)} \circ \delta_{n+1} \circ \Psi_n \\ &= \Phi_{n+2} \circ \underbrace{\delta_{n+2} \circ \delta_{n+1}}_{=0 \ (32)} \circ \Psi_n \\ &= 0 \ \in \mathrm{Hom}_K(C^n(G, V), C^{n+2}(G, V)).\end{aligned}$$

Dies wollten wir zeigen. □

2.3 Die bar resolution

In diesem Abschnitt geben wir eine freie Auflösung von K als KG-Modul an, die sogenannte *bar resolution*. Wie üblich operiert hier G trivial auf K. Sei

$$P_n := \{f : G^n \to KG : f(x) \neq 0 \text{ nur für endlich viele } x \in G^n\} \quad (n \geq 1)$$

der freie KG-Modul mit Basis $\{[\sigma_1, \ldots, \sigma_n] : \sigma_1, \ldots, \sigma_n \in G\}$, wobei

$$[\sigma_1, \ldots, \sigma_n] : G^n \to KG, \quad (\tau_1, \ldots, \tau_n) \mapsto \delta_{\sigma_1,\tau_1} \cdot \ldots \cdot \delta_{\sigma_n,\tau_n}.$$

(Hier ist δ das Kronecker-Symbol.) Weiter sei

$$P_0 := KG \text{ mit einzigem Basiselement } [] = 1 \in KG.$$

Wir betrachten die Folge von Abbildungen $d_n \in \mathrm{Hom}_{KG}(P_n, P_{n-1})$ $(n \geq 1)$ gegeben durch KG-lineare Fortsetzung von

$$\begin{aligned} d_n([\sigma_1, \ldots, \sigma_n]) &:= \sigma_1[\sigma_2, \ldots, \sigma_n] + \sum_{i=1}^{n-1} (-1)^i [\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n] \\ &\quad + (-1)^n [\sigma_1, \ldots, \sigma_{n-1}], \end{aligned} \tag{34}$$

sowie $d_0 \in \mathrm{Hom}_{KG}(P_0, K)$ gegeben durch KG-lineare Fortsetzung von

$$d_0([]) := 1. \tag{35}$$

Ziel dieses Abschnitts ist es zu zeigen, dass

$$\ldots \overset{d_{n+1}}{\to} P_n \overset{d_n}{\to} P_{n-1} \overset{d_{n-1}}{\to} P_{n-2} \overset{d_{n-2}}{\to} \ldots \overset{d_2}{\to} P_1 \overset{d_1}{\to} P_0 \overset{d_0}{\to} K \to 0 \tag{36}$$

eine exakte Sequenz ist (d.h. es gilt $\ker d_n = \mathrm{im}\, d_{n+1}$ für alle $n \geq 0$), also eine freie Auflösung des KG-Moduls K. Diese Auflösung heißt *bar resolution*.

Beweis. Für jeden KG-Modul V und $n \geq 0$ definieren wir eine lineare Abbildung

$$\omega_n^V : C^n(G, V) \to \mathrm{Hom}_{KG}(P_n, V), \quad g \mapsto \omega_n^V(g) \tag{37}$$

mit

$$\omega_n^V(g) : P_n \to V, \quad [\sigma_1, \ldots, \sigma_n] \mapsto g(\sigma_1, \ldots, \sigma_n) \quad (KG - \text{linear fortgesetzt}).$$

Dann ist ω_n^V bijektiv, denn für

$$e_n \in C^n(G, P_n) \text{ mit } e_n(\sigma_1, \ldots, \sigma_n) := [\sigma_1, \ldots, \sigma_n] \tag{38}$$

gilt

$$\omega_n^V(g) \circ e_n = g \quad \text{ für alle } g \in C^n(G, V) \tag{39}$$

und

$$\omega_n^V(\varphi \circ e_n) = \varphi \quad \text{ für alle } \varphi \in \mathrm{Hom}_{KG}(P_n, V). \tag{40}$$

Insbesondere für $\varphi = \mathrm{id}_{P_n}$ folgt

$$\omega_n^{P_n}(e_n) = \mathrm{id}_{P_n}. \tag{41}$$

Anhand der Definitionen (30) und (34) prüft man leicht, dass für $g \in C^n(G, V)$ $(n \geq 0)$ die Gleichung

$$\omega_{n+1}^V(\partial_n^V g) = \omega_n^V(g) \circ d_{n+1} \tag{42}$$

gilt. Insbesondere haben wir für $e_n \in C^n(G, P_n)$

$$\begin{aligned} \omega_{n+2}^{P_n}(\underbrace{\partial_{n+1}^{P_n} \partial_n^{P_n} e_n}_{=0}) &\overset{(42)}{=} \omega_{n+1}^{P_n}(\partial_n^{P_n} e_n) \circ d_{n+2} \\ &\overset{(42)}{=} \omega_n^{P_n}(e_n) \circ d_{n+1} \circ d_{n+2} \\ &\overset{(41)}{=} \mathrm{id}_{P_n} \circ d_{n+1} \circ d_{n+2} = d_{n+1} \circ d_{n+2}, \end{aligned}$$

und damit $d_{n+1} \circ d_{n+2} = 0$ ($n \geq 0$). Da auch $d_0 \circ d_1 = 0$ (es ist $d_0(d_1([\sigma])) = d_0(\sigma[] - []) = 1 - 1 = 0$ für alle $\sigma \in G$), ist also (36) ein Komplex, also $\operatorname{im} d_{n+1} \subseteq \ker d_n$ für alle $n \geq 0$.

Um die umgekehrte Inklusion zu zeigen, betrachten wir die K-linearen Abbildungen

$$t_n : P_n \to P_{n+1}, \quad \sigma_0[\sigma_1, \ldots, \sigma_n] \mapsto [\sigma_0, \sigma_1, \ldots, \sigma_n] \quad (K\text{-linear fortgesetzt}).$$

Da $\{\sigma_0[\sigma_1, \ldots, \sigma_n] : \sigma_0, \ldots, \sigma_n \in G\}$ eine Basis von P_n als K-Vektorraum ist, ist t_n wohldefiniert. Dann gilt

$$\mathrm{id}_{P_n} = d_{n+1} \circ t_n + t_{n-1} \circ d_n \quad (n \geq 1),$$

denn unter der rechten Abbildung erhalten wir

$$\begin{aligned}
\sigma_0[\sigma_1, \ldots, \sigma_n] \;\mapsto\; & d_{n+1}([\sigma_0, \sigma_1, \ldots, \sigma_n]) + t_{n-1}\Big(\sigma_0\big(\sigma_1[\sigma_2, \ldots, \sigma_n] \\
& + \sum_{i=1}^{n-1}(-1)^i[\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n] + (-1)^n[\sigma_1, \ldots, \sigma_{n-1}]\big)\Big) \\
= \;& \sigma_0[\sigma_1, \ldots, \sigma_n] + \sum_{i=0}^{n-1}(-1)^{i+1}[\sigma_0, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n] \\
& + (-1)^{n+1}[\sigma_0, \ldots, \sigma_{n-1}] + [\sigma_0\sigma_1, \sigma_2, \ldots, \sigma_n] \\
& + \sum_{i=1}^{n-1}(-1)^i[\sigma_0, \sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_n] + (-1)^n[\sigma_0, \ldots, \sigma_{n-1}] \\
= \;& \sigma_0[\sigma_1, \ldots, \sigma_n],
\end{aligned}$$

d.h. die rechte Abbildung ist gleich der Identität. Damit können wir nun $\ker d_n \subseteq \operatorname{im} d_{n+1}$ für $n \geq 1$ zeigen: Für $x \in \ker d_n$ ist

$$x = \mathrm{id}_{P_n}(x) = d_{n+1} \circ t_n(x) + \underbrace{t_{n-1} \circ d_n(x)}_{=0} = d_{n+1} \circ t_n(x) \in \operatorname{im} d_{n+1}.$$

Bleibt noch der Fall $n = 0$. Für $x = \sum_{i=1}^k \lambda_i \sigma_i[] \in \ker d_0$ mit $\lambda_i \in K, \sigma_i \in G$ folgt $d_0(x) = \sum_{i=1}^k \lambda_i = 0$. Mit $y := \sum_{i=1}^k \lambda_i[\sigma_i]$ folgt

$$d_1(y) = \sum_{i=1}^k \lambda_i(\sigma_i[] - []) = \sum_{i=1}^k \lambda_i \sigma_i[] = x,$$

also auch $\ker d_0 \subseteq \operatorname{im} d_1$. Damit ist nun bewiesen, dass (36) eine exakte Sequenz ist. □

2.4 Beschreibung der Kohomologie durch Ext

Ist V ein G-Modul, so erhält man aus dem Komplex (36) den Kokomplex

$$0 \overset{d_0^*}{\to} \mathrm{Hom}_{KG}(P_0, V) \overset{d_1^*}{\to} \ldots \overset{d_{n-1}^*}{\to} \mathrm{Hom}_{KG}(P_{n-1}, V) \overset{d_n^*}{\to} \mathrm{Hom}_{KG}(P_n, V) \overset{d_{n+1}^*}{\to} \ldots \tag{43}$$

mit Differentialen

$$d_n^* : \mathrm{Hom}_{KG}(P_{n-1}, V) \to \mathrm{Hom}_{KG}(P_n, V), \quad f \mapsto d_n^*(f) = f \circ d_n \quad (n \geq 1),$$

und $d_0^* := 0$. Man bezeichnet mit

$$\mathrm{Ext}_{KG}^n(K,V) := \ker d_{n+1}^* / \operatorname{im} d_n^* \quad (n \geq 0)$$

die n-te Kohomologiegruppe dieses Kokomplexes. Wir zeigen die Isomorphie der additiven Gruppen

$$H^n(G,V) \cong \mathrm{Ext}_{KG}^n(K,V),$$

womit (im wesentlichen) der Bogen zu der in der Literatur üblichen Beschreibung gespannt ist.

Aus Gleichung (42) folgt sofort

$$\omega_{n+1}^V \circ \partial_n^V = d_{n+1}^* \circ \omega_n^V, \quad (n \geq 0)$$

und aus der Bijektivität von ω_n^V für alle $n \geq 0$ folgt hieraus

$$\omega_n^V(\ker \partial_n^V) = \ker d_{n+1}^* \quad \text{und} \quad \omega_{n+1}^V(\operatorname{im} \partial_n^V) = \operatorname{im} d_{n+1}^* \quad \text{für alle } n \geq 0.$$

Daher induziert ω_n^V einen Gruppenisomorphismus von $\ker \partial_n^V / \operatorname{im} \partial_{n-1}^V = H^n(G,V)$ auf $\ker d_{n+1}^* / \operatorname{im} d_n^* = \mathrm{Ext}_{KG}^n(K,V)$ $(n \geq 1)$, und ω_0^V einen Gruppenisomorphismus von $\ker \partial_0^V = H^0(G,V)$ auf $\ker d_1^* = \mathrm{Ext}_{KG}^0(K,V)$.

2.5 Von kurzen zu langen exakten Sequenzen

Wir wollen der Vollständigkeit halber noch eine häufig benutzte Eigenschaft der Kohomologiegruppen beschreiben (wir verwenden diese nicht weiter, so dass dieser Abschnitt übersprungen werden kann):

Satz 2.1 *Eine kurze exakte Sequenz von G-Moduln*

$$0 \to U \overset{\varepsilon}{\hookrightarrow} V \overset{\pi}{\to} W \to 0$$

induziert eine lange exakte Sequenz von Kohomologiegruppen

$$0 \to U^G \overset{\varepsilon_0}{\to} V^G \overset{\pi_0}{\to} W^G \overset{\gamma_0}{\to} H^1(G,U) \overset{\varepsilon_1}{\to} H^1(G,V) \overset{\pi_1}{\to} H^1(G,W) \overset{\gamma_1}{\to} H^2(G,U) \overset{\varepsilon_2}{\to} \dots$$
$$\dots \overset{\pi_{n-1}}{\to} H^{n-1}(G,W) \overset{\gamma_{n-1}}{\to} H^n(G,U) \overset{\varepsilon_n}{\to} H^n(G,V) \overset{\pi_n}{\to} H^n(G,W) \overset{\gamma_n}{\to} H^{n+1}(G,U) \overset{\varepsilon_{n+1}}{\to} \dots$$

mit folgenden Übergangshomomorphismen ($n \geq 0$):

$$\begin{aligned}
\varepsilon_n: &\quad H^n(G,U) \to H^n(G,V), && g + B^n(G,U) \mapsto \varepsilon \circ g + B^n(G,V) \quad (g \in Z^n(G,U)) \\
\pi_n: &\quad H^n(G,V) \to H^n(G,W), && g + B^n(G,V) \mapsto \pi \circ g + B^n(G,W) \quad (g \in Z^n(G,V)) \\
\gamma_n: &\quad H^n(G,W) \to H^{n+1}(G,U), && g + B^n(G,W) \mapsto \partial_n^V h + B^{n+1}(G,U) \quad (g \in Z^n(G,W)), \\
& && \text{wenn } h \in C^n(G,V) \text{ mit } g = \pi \circ h.
\end{aligned}$$

Beweis. (i) Wir zeigen zunächst die Wohldefiniertheit von π_n. Ist $g \in Z^n(G,V)$, also $\partial_n^V g = 0$, so ist $\partial_n^W(\pi \circ g) = \pi \circ \partial_n^V g = 0$, also $\pi \circ g \in Z^n(G,W)$. Ist $g \in B^n(G,V)$, also $g = \partial_{n-1}^V h$ mit $h \in C^{n-1}(G,V)$, so ist $\pi \circ g = \pi \circ \partial_{n-1}^V h = \partial_{n-1}^W(\pi \circ h)$ mit $\pi \circ h \in C^{n-1}(G,W)$. Dies zeigt $\pi \circ g \in B^n(G,W)$. Es folgt die Wohldefiniertheit von π_n. Die Wohldefiniertheit von ε_n zeigt man genauso. Es ist klar, dass π_n und ε_n Gruppenhomomorphismen sind.

(ii) Wir zeigen die Exaktheit an der Stelle $H^n(G,V)$. Aus $\pi\circ\varepsilon = 0$ folgt sofort $\pi_n\circ\varepsilon_n = 0$, also $\operatorname{im}\varepsilon_n \subseteq \ker\pi_n$. Für die umgekehrte Inklusion sei $g \in Z^n(G,V)$ mit $\pi_n(g+B^n(G,V)) = 0$, d.h. $\pi\circ g \in B^n(G,W)$. Dann existiert ein $h' \in C^{n-1}(G,W)$ mit $\pi\circ g = \partial^W_{n-1}h'$. Da π surjektiv, existiert zu h' ein $h \in C^{n-1}(G,V)$ mit $h' = \pi\circ h$. Es folgt $\pi\circ g = \partial^W_{n-1}(\pi\circ h) = \pi\circ\partial^V_{n-1}h$, also $\pi\circ(g-\partial^V_{n-1}h) = 0$. Aus $\ker\pi = U$ folgt also $f := g - \partial^V_{n-1}h \in C^n(G,U)$. Wegen $U \subseteq V$ ist dann

$$\partial^U_n f = \partial^V_n g - \partial^V_n\partial^V_{n-1}h = 0$$

wegen $g \in Z^n(G,V) = \ker\partial^V_n$ und $\partial_n\circ\partial_{n-1} = 0$. Also ist $f \in Z^n(G,U)$ und

$$\varepsilon_n(f+B^n(G,U)) = f+B^n(G,V) = g-\partial^V_{n-1}h+B^n(G,V) = g+B^n(G,V).$$

Es folgt $\ker\pi_n \subseteq \operatorname{im}\varepsilon_n$.

(iii) Wir zeigen die Wohldefiniertheit von γ_n. Ist $g \in Z^n(G,W)$, so existiert wegen der Surjektivität von π jedenfalls ein $h \in C^n(G,V)$ mit $g = \pi\circ h$. Es folgt $0 = \partial^W_n g = \pi\circ\partial^V_n h$, also $\partial^V_n h \in C^{n+1}(G,U)$. Es folgt $\partial^U_{n+1}(\partial^V_n h) = \partial^V_{n+1}\partial^V_n h = 0$, also $\partial^V_n h \in Z^{n+1}(G,U)$. Ist auch $h' \in C^n(G,V)$ mit $g = \pi\circ h'$, so ist $0 = \pi\circ(h-h')$, also $h-h' \in C^n(G,U)$. Dann ist $\partial^V_n h - \partial^V_n h' = \partial^U_n(h-h') \in B^{n+1}(G,U)$ und damit $\partial^V_n h + B^{n+1}(G,U) = \partial^V_n h' + B^{n+1}(G,U)$. Daher ist die Abbildung

$$\begin{aligned}\Gamma_n : Z^n(G,W) \to H^{n+1}(G,U), \qquad & g \mapsto \partial^V_n h + B^{n+1}(G,U) \quad (g \in Z^n(G,W)) \\ & \text{wenn } h \in C^n(G,V) \text{ mit } g = \pi\circ h\end{aligned}$$

wohldefiniert. Man sieht auch leicht, dass Γ_n ein Gruppenhomomorphismus ist. Wir zeigen, dass $B^n(G,W)$ im Kern von Γ_n liegt, was dann zeigt, dass γ_n wohldefiniert und ein Gruppenhomomorphismus ist. Ist $g \in B^n(G,W)$, so gibt es $f \in C^{n-1}(G,W)$ mit $g = \partial^W_{n-1}f$. Zu f gibt es dann $t \in C^{n-1}(G,V)$ mit $f = \pi\circ t$. Dann ist $g = \partial^W_{n-1}(\pi\circ t) = \pi\circ\partial^V_{n-1}t$, und für $h := \partial^V_{n-1}t \in C^n(G,V)$ gilt dann $g = \pi\circ h$ und $\partial^V_n h = \partial^V_n\partial^V_{n-1}t = 0$, also $\Gamma_n(g) = 0$. Dies zeigt $B^n(G,W) \subseteq \ker\Gamma_n$.

(iv) Exaktheit an der Stelle $H^n(G,W)$. Sei $g \in Z^n(G,V)$. Dann ist $\pi\circ g \in Z^n(G,W)$. Es folgt

$$\gamma_n(\pi\circ g + B^n(G,W)) = \partial^V_n g + B^{n+1}(G,U) = 0 + B^{n+1}(G,U),$$

da $\partial^V_n g = 0$. Also ist $\gamma_n\circ\pi_n = 0$ und $\operatorname{im}\pi_n \subseteq \ker\gamma_n$. Für die umgekehrte Inklusion sei $g \in Z^n(G,W)$ mit $\gamma_n(g+B^n(G,W)) = 0$, d.h. für $h \in C^n(G,V)$ mit $g = \pi\circ h$ gilt $\partial^V_n h \in B^{n+1}(G,U)$. Dann gibt es $f \in C^n(G,U)$ mit $\partial^V_n h = \partial^U_n f$, also $\partial^V_n(h-f) = 0$ oder $h-f \in Z^n(G,V)$. Da $\pi\circ f = 0$ (wegen $f \in C^n(G,U)$), folgt also $g = \pi\circ h = \pi\circ(h-f)$ und damit $g + B^n(G,W) = \pi_n(h-f+B^n(G,V))$. Dies zeigt $\ker\gamma_n \subseteq \operatorname{im}\pi_n$.

(v) Exaktheit an der Stelle $H^n(G,U)$. Sei $f \in Z^{n-1}(G,W)$ und $h \in C^{n-1}(G,V)$ mit $f = \pi\circ h$. Dann ist $\gamma_{n-1}(f+B^{n-1}(G,W)) = \partial^V_{n-1}h + B^n(G,U)$ und damit $\varepsilon_n(\gamma_{n-1}(f+B^{n-1}(G,W))) = \partial^V_{n-1}h + B^n(G,V) = 0 + B^n(G,V)$, da $h \in C^{n-1}(G,V)$. Also ist $\varepsilon_n\circ\gamma_{n-1} = 0$ und $\operatorname{im}\gamma_{n-1} \subseteq \ker\varepsilon_n$. Sei umgekehrt $g \in Z^n(G,U)$ mit $g + B^n(G,U) \in \ker\varepsilon_n$, also $g \in B^n(G,V)$. Dann gibt es $f \in C^{n-1}(G,V)$ mit $g = \partial_{n-1}f$. Für $\pi\circ f \in C^{n-1}(G,W)$ gilt dann $\partial^W_{n-1}(\pi\circ f) = \pi\circ\partial^V_{n-1}f = \pi\circ g = 0$, da $g \in Z^n(G,U)$. Also ist $\pi\circ f \in Z^{n-1}(G,W)$ und $\gamma_{n-1}(\pi\circ f + B^{n-1}(G,W)) = \partial^V_{n-1}f + B^n(G,U) = g + B^n(G,U)$. Dies zeigt $\ker\varepsilon_n \subseteq \operatorname{im}\gamma_{n-1}$.

Insgesamt haben wir die Exaktheit der langen Sequenz gezeigt. □

2.6 Von exakten Sequenzen zu Kozyklen

In diesem Abschnitt wollen wir eine Konstruktion angeben, bei der gewissen exakten Sequenzen ein bis auf einen Korand eindeutiger Kozyklus zugewiesen wird.

Satz und Definition 2.2 *Sei $n \geq 1$,*

$$0 \to U_n \overset{\pi_n}{\to} U_{n-1} \overset{\pi_{n-1}}{\to} U_{n-2} \overset{\pi_{n-2}}{\to} \dots \overset{\pi_1}{\to} U_0 \overset{\pi_0}{\to} U_{-1} \tag{44}$$

eine exakte Sequenz von G-Moduln und $w \in U_{-1}^G \cap \operatorname{im}\pi_0$. Für $k = 0, \dots, n$ sei $g_k \in C^k(G, U_k)$ mit

$$\pi_0(g_0) = w \quad \text{und} \quad \pi_k \circ g_k = \partial_{k-1}^{U_{k-1}} g_{k-1} \quad \text{für } k = 1, \dots, n. \quad (*)$$

Dann ist $g_n \in Z^n(G, U_n)$. Eine Folge (g_k) mit den Eigenschaften $(*)$ existiert immer, und die Restklasse $g_n + B^n(G, U_n)$ ist unabhängig von der speziellen Wahl einer Folge (g_k) mit den Eigenschaften $(*)$. Ist $g_n' \in g_n + B^n(G, U_n)$ ein weiterer Repräsentant der Restklasse, so existieren dazu $g_k' \in C^k(G, U_k)$, $k = 0, \dots, n-1$ mit der $(*)$ entsprechenden Eigenschaft, d.h. jeder Kozyklus der induzierten Restklasse kann durch die Konstruktion auch „realisiert" werden.

Existiert ein $v \in U_0^G$ mit $\pi_0(v) = w$, oder für ein $0 \leq k_0 \leq n$ ein G-Homomorphismus $\mu_{k_0} : U_{k_0-1} \to U_{k_0}$ mit $\pi_{k_0} \circ \mu_{k_0} = \mathrm{id}_{U_{k_0-1}}$ (d.h. ein rechts-Splitting *an der Stelle k_0) oder $\mu_{k_0} \circ \pi_{k_0} = \mathrm{id}_{U_{k_0}}$ (d.h. ein* links-Splitting *an der Stelle k_0), so ist $g_n \in B^n(G, U_n)$.*

Im Falle einer exakten Sequenz der Länge n in Standardform*,*

$$0 \to U_n \overset{\pi_n}{\to} U_{n-1} \overset{\pi_{n-1}}{\to} U_{n-2} \overset{\pi_{n-2}}{\to} \dots \overset{\pi_1}{\to} U_0 \overset{\pi_0}{\to} K \to 0 \tag{45}$$

und $w = 1 \in K$ nennen wir g_n einen von der exakten Sequenz (45) induzierten Kozyklus*.*

In Beispiel 2.4 werden wir sehen, dass die angegebenen Kriterien für das Vorliegen eines Korands nur hinreichend, aber nicht notwendig sind. Falls man ein links/rechts Splitting hat, dass nicht am linken/rechten Rand liegt, so ist das Kriterium relativ trivial, da dann die links/rechts benachbarte Abbildung die Nullabbildung ist.

Interpretiert man π_n als Inklusion $U_n \hookrightarrow U_{n-1}$, so folgt aus $(*)$, das $g_n = \partial_{n-1}^{U_{n-1}} g_{n-1}$, also $g_n \in B^n(G, U_{n-1})$. In U_{n-1} wird g_n also zu einem Korand.

Beweis. (i) Wir zeigen zunächst die Existenz einer Folge (g_k) mit der Eigenschaft $(*)$. Da $w \in \operatorname{im}\pi_0$ (dies gilt insbesondere für den Fall der Sequenz (45) und $w = 1 \in K = K^G$), existiert ein $g_0 \in C^0(G, U_0) = U_0$ mit $\pi_0(g_0) = w$. Dann gilt für $\sigma \in G$, dass $\partial_0^{U_0} g_0(\sigma) = \sigma g_0 - g_0$, also $\pi_0(\partial_0^{U_0} g_0(\sigma)) = \sigma w - w = 0$ ($w \in U_{-1}^G$). Da $\ker\pi_0 = \operatorname{im}\pi_1$, existiert also $g_1 \in C^1(G, U_1)$ mit $\partial_0^{U_0} g_0 = \pi_1 \circ g_1$. Wir haben also $(*)$ für $k = 1$.

Es sei nun $g_0, \dots, g_k$ mit $(*)$ bereits konstruiert. Es folgt

$$\pi_k \circ \partial_k^{U_k} g_k = \partial_k^{U_{k-1}}(\pi_k \circ g_k) \overset{(*)}{=} \partial_k^{U_{k-1}} \partial_{k-1}^{U_{k-1}} g_{k-1} = 0, \tag{46}$$

(da $\partial_k \circ \partial_{k-1} = 0$) und wegen $\ker\pi_k = \operatorname{im}\pi_{k+1}$ gibt es also $g_{k+1} \in C^{k+1}(G, U_{k+1})$ mit $\pi_{k+1} \circ g_{k+1} = \partial_k^{U_k} g_k$. Dies ist $(*)$ für $k+1$.

(ii) Ist nun (g_k) ein Folge mit $(*)$, so gilt insbesondere für $k = n$, dass

$$\pi_n \circ \partial_n^{U_n} g_n = \partial_n^{U_{n-1}}(\pi_n \circ g_n) \overset{(*)}{=} \partial_n^{U_{n-1}} \partial_{n-1}^{U_{n-1}} g_{n-1} = 0.$$

(Der Leser mag einwenden, dass diese Gleichung nur ein Spezialfall von (46) für $k = n$ ist. Auf (46) werden wir aber durch *Konstruktion* einer *speziellen* Folge geführt, die $(*)$ erfüllen *soll*, während wir vorige Gleichung für *jede* Folge zeigen, die $(*)$ erfüllt. Die Rechnung ist natürlich die gleiche.) Da π_n injektiv, folgt dann aber $\partial_n^{U_n} g_n = 0$, also $g_n \in Z^n(G, U_n)$.

(iii) Sei nun $h_k \in C^k(G, U_k)$ für $k = 0, \ldots, n$ eine weitere Folge mit der Eigenschaft $(*)$, also

$$\pi_0(h_0) = w \quad \text{und} \quad \pi_k \circ h_k = \partial_{k-1}^{U_{k-1}} h_{k-1} \quad \text{für } k = 1, \ldots, n.$$

Wir müssen $g_n + B^n(G, U_n) = h_n + B^n(G, U_n)$ zeigen.

Wir zeigen zunächst: Für $k = 1, \ldots, n$ existiert ein $f_k \in C^{k-1}(G, U_k)$ mit

$$\pi_k \circ (g_k - h_k) = \pi_k \circ \partial_{k-1}^{U_k} f_k. \quad (**)$$

Da $\pi_0(g_0 - h_0) = w - w = 0$ und $\ker \pi_0 = \operatorname{im} \pi_1$, gibt es $f_1 \in C^0(G, U_1)$ mit $\pi_1 \circ f_1 = g_0 - h_0$. Dann ist

$$\pi_1 \circ (g_1 - h_1) \overset{(*)}{=} \partial_0^{U_0}(g_0 - h_0) = \partial_0^{U_0}(\pi_1 \circ f_1) = \pi_1 \circ \partial_0^{U_1} f_1.$$

Dies ist $(**)$ für $k = 1$. Sei nun $f_1, \ldots, f_k$ mit $(**)$ bereits konstruiert. Dann ist

$$\pi_k \circ (g_k - h_k - \partial_{k-1}^{U_k} f_k) = 0,$$

und wegen $\ker \pi_k = \operatorname{im} \pi_{k+1}$ existiert ein $f_{k+1} \in C^k(G, U_{k+1})$ mit

$$g_k - h_k - \partial_{k-1}^{U_k} f_k = \pi_{k+1} \circ f_{k+1}.$$

Anwenden von $\partial_k^{U_k}$ liefert

$$\partial_k^{U_k} g_k - \partial_k^{U_k} h_k - \partial_k^{U_k} \partial_{k-1}^{U_k} f_k = \partial_k^{U_k}(\pi_{k+1} \circ f_{k+1}) = \pi_{k+1} \circ \partial_k^{U_{k+1}} f_{k+1},$$

und wegen $\partial_k^{U_k} \circ \partial_{k-1}^{U_k} = 0$ und $(*)$ folgt

$$\pi_{k+1} \circ (g_{k+1} - h_{k+1}) = \pi_{k+1} \circ \partial_k^{U_{k+1}} f_{k+1}.$$

Dies ist $(**)$ für $k + 1$. Insbesondere für $k = n$ folgt aus $(**)$ und der Injektivität von π_n, dass

$$g_n - h_n = \partial_{n-1}^{U_n} f_n \in B^n(G, U_n).$$

Damit ist also die Restklasse $g_n + B^n(G, U_n) = h_n + B^n(G, U_n)$ von der speziellen Wahl der Folge (g_k) mit $(*)$ unabhängig.

(iv) Sei nun $g'_n \in g_n + B^n(G, U_n)$ ein weiterer Repräsentant der Restklasse, d.h. $g'_n = g_n + \partial_{n-1}^{U_n} f$ mit $f \in C^{n-1}(G, U_n)$. Wir setzen $g'_{n-1} := g_{n-1} + \pi_n \circ f \in C^{n-1}(G, U_{n-1})$ und $g'_k := g_k$ für $k = 0, \ldots, n-2$. Dann hat die Folge der g'_k mit $k = 0, \ldots, n$ die $(*)$ entsprechende Eigenschaft und induziert damit g'_n. Nach Konstruktion müssen wir dabei $(*)$ nur noch für $k = n$ und $k = n - 1$ testen. Da

$$\begin{aligned} \pi_n \circ g'_n &= \pi_n \circ (g_n + \partial_{n-1}^{U_n} f) \overset{(*)}{=} \partial_{n-1}^{U_{n-1}} g_{n-1} + \partial_{n-1}^{U_{n-1}}(\pi_n \circ f) \\ &= \partial_{n-1}^{U_{n-1}}(g_{n-1} + \pi_n \circ f) = \partial_{n-1}^{U_{n-1}} g'_{n-1}, \end{aligned}$$

also $(*)$ für die Folge (g'_k) und $k = n$ gilt, sowie

$$\begin{aligned}\pi_{n-1} \circ g'_{n-1} &= \pi_{n-1} \circ (g_{n-1} + \pi_n \circ f) \overset{\pi_{n-1}\circ\pi_n=0}{=} \pi_{n-1} \circ g_{n-1} \\ &\overset{(*)}{=} \partial_{n-2}^{U_{n-2}} g_{n-2} = \partial_{n-2}^{U_{n-2}} g'_{n-2}\end{aligned}$$

gilt, also $(*)$ für die Folge (g'_k) und $k = n-1$ gilt, erfüllt also auch die Folge (g'_k) für $k = 0, \ldots, n$ die Bedingung $(*)$ und induziert den Repräsentant der Restklasse g'_n. (Im Fall $n = 1$ und $k = n-1 = 0$ erhält man analog $\pi_0(g'_0) = \pi_0(g_0 + \pi_1 \circ f) = w$).

(v) Wir nehmen nun die Existenz eines $v \in U_0^G$ mit $\pi_0(v) = w$ an. Wir definieren $g'_k \in C^k(G, U_k)$ für $k = 0, \ldots, n$ durch $g'_0 := v$ und $g'_k := 0$ für $k = 1, \ldots, n$. Dann gilt $\pi_0(g'_0) = w$. Weiter gilt

$$\partial_0^{U_0} g'_0(\sigma) = \sigma v - v \overset{v\in U_0^G}{=} 0 = \pi_1 \circ g'_1(\sigma),$$

und offenbar auch $\pi_k \circ g'_k = 0 = \partial_{k-1}^{U_{k-1}} g'_{k-1}$ für $k = 2, \ldots, n$. Dies ist $(*)$ für die Folge (g'_k), und nach der bereits bewiesenen Unabhängigkeit der induzierten Restklasse folgt $g_n + B^n(G, U_n) = g'_n + B^n(G, U_n) = 0 + B^n(G, U_n)$, d.h. g_n ist ein n-Korand.

(vi) Sei nun für ein $0 \leq k_0 \leq n$ ein G-Homomorphismus $\mu_{k_0} : U_{k_0-1} \to U_{k_0}$ mit $\pi_{k_0} \circ \mu_{k_0} = \mathrm{id}_{U_{k_0-1}}$ gegeben, also ein rechts-Splitting. Im Fall $k_0 = 0$ setzen wir $v := \mu_0(w) \in U_0^G$ (dann gilt $\pi_0(v) = w$) und kommen zum vorherigen Fall (v). Sei daher nun $1 \leq k_0 \leq n$. Sei weiter $(g_k)_{k=0,\ldots,n}$ eine Folge mit $(*)$. Aus $\ker \pi_{k_0-1} = \mathrm{im}\, \pi_{k_0} = U_{k_0-1}$ (da $\pi_{k_0} \circ \mu_{k_0} = \mathrm{id}_{U_{k_0-1}}$) folgt $\pi_{k_0-1} = 0$ und daraus sofort, dass man $g_k = 0 \in B^k(G, U_k)$ für $k \geq k_0 - 1$ wählen kann.

Wir geben noch ein alternatives Argument. (Der eilige Leser kann zu (vii) springen). Dieses funktioniert auch dann, wenn μ_{k_0} nur auf einem „hinreichend großen“ Untermodul $U' \subseteq U_{k_0-1}$ definiert ist und $\pi_{k_0} \circ \mu_{k_0} = \mathrm{id}_{U'}$ erfüllt; Hinreichend groß heißt hier, dass $\mu_{k_0} \circ \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1}$ definiert ist, die Bedingung hängt also von der Wahl der Folge (g_k) ab. Wir setzen $g'_{k_0} := \mu_{k_0} \circ \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1} \in C^{k_0}(G, U_{k_0})$ und $g'_k := 0 \in C^k(G, U_k)$ für $k = k_0 + 1, \ldots, n$, und behaupten, dass die Folge $g_0, \ldots, g_{k_0-1}, g'_{k_0}, g'_{k_0+1}, \ldots, g'_n$ die $(*)$ entsprechende Eigenschaft mit $g'_n \in B^n(G, U_n)$ erfüllt. Dann gilt $g_n - g'_n \in B^n(G, U_n)$ nach dem bereits bewiesenen, und damit auch $g_n \in B^n(G, U_n)$. Offenbar ist $(*)$ nur noch für $k = k_0$ und $k = k_0 + 1$ (wenn $k_0 < n$) zu prüfen. Für $k = k_0$ erhalten wir

$$\pi_{k_0} \circ g'_{k_0} = \pi_{k_0} \circ \mu_{k_0} \circ \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1} = \mathrm{id}_{U_{k_0-1}} \circ \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1} = \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1},$$

also $(*)$ für $k = k_0$, und für $k = k_0 + 1$ erhalten wir

$$\partial_{k_0}^{U_{k_0}} g'_{k_0} = \partial_{k_0}^{U_{k_0}} \left(\mu_{k_0} \circ \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1} \right) = \mu_{k_0} \circ \partial_{k_0}^{U_{k_0-1}} \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1} = 0 = \pi_{k_0+1} \circ g'_{k_0+1},$$

da $\partial_{k_0}^{U_{k_0-1}} \circ \partial_{k_0-1}^{U_{k_0-1}} = 0$ und $g'_{k_0+1} = 0$, also $(*)$ für $k = k_0 + 1$. Ist $k_0 < n$, so ist $g'_n = 0 \in B^n(G, U_n)$. Für $k_0 = n$ erhalten wir nach Definition ebenfalls $g'_n = g'_{k_0} = \mu_{k_0} \circ \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1} = \partial_{k_0-1}^{U_{k_0}} (\mu_{k_0} \circ g_{k_0-1}) \in B^n(G, U_n)$.

(vii) Wir kommen zum Fall, dass für ein $0 \leq k_0 \leq n$ ein G-Homomorphismus $\mu_{k_0} : U_{k_0-1} \to U_{k_0}$ mit $\mu_{k_0} \circ \pi_{k_0} = \mathrm{id}_{U_{k_0}}$ gegeben ist, also ein links-Splitting. (Auch hier genügt es, dass μ_{k_0} auf einem „hinreichend großen“ Untermodul definiert ist, vgl. die Bemerkung

oben). Sei wieder $(g_k)_{k=0,\dots,n}$ eine Folge mit $(*)$. Im Fall $k_0 = 0$ folgt aus $\pi_0(g_0) = w$ nach Anwendung von μ_0, dass $g_0 = \mu_0(w) \in U_0^G$ (da $w \in U_{-1}^G$); Nach dem bereits betrachteten Kriterium mit $v := g_0$ folgt $g_n \in B^n(G, U_n)$. Sei also $k_0 \geq 1$. Wir setzen $g'_k := 0 \in C^k(G, U_k)$ für $k = k_0 + 1, \dots, n$ und zeigen, dass die Folge $g_0, \dots, g_{k_0}, g'_{k_0+1}, \dots, g'_n$ die $(*)$ entsprechende Eigenschaft erfüllt. Dabei ist $(*)$ diesmal offenbar nur für $k = k_0 + 1$ (falls $k_0 < n$) zu prüfen. Aus $\pi_{k_0} \circ g_{k_0} \overset{(*)}{=} \partial_{k_0-1}^{U_{k_0-1}} g_{k_0-1}$ folgt nach Anwenden von μ_{k_0} unter Beachtung von $\mu_{k_0} \circ \pi_{k_0} = \mathrm{id}_{U_{k_0}}$ dann $g_{k_0} = \partial_{k_0-1}^{U_{k_0}}(\mu_{k_0} \circ g_{k_0-1})$. Also gilt $g_{k_0} \in B^{k_0}(G, U_{k_0})$. Ist $k_0 = n$, so haben wir damit bereits die Behauptung. Wenn $k_0 < n$, so gilt $\pi_{k_0+1} \circ g'_{k_0+1} = 0 = \partial_{k_0}^{U_{k_0}} g_{k_0}$ (da $g'_{k_0+1} = 0$ und $g_{k_0} \in B^{k_0}(G, U_{k_0})$), also $(*)$. Wir erhalten $g_n = g_n - g'_n \in B^n(G, U_n)$, also die Behauptung. □

Bemerkung 2.3 Wählt man jeweils die konstruierte Folge (mit der Mischung aus g'_k und g_k) in einem der Kriterien für das Vorliegen eines Korands als alternative Folge (h_k) zur Konstruktion der Folge (f_k) gemäß $(**)$, so erhält man wegen π_n injektiv im Fall $h_n = 0$ aus $(**)$ also insbesondere $g_n = \partial_{n-1} f_n$ (wenn $h_n \neq 0$, so konnten wir g_n im Beweis sowieso schon so schreiben). Da die Konstruktion der Folge (f_k) explizit ist (sofern man Urbilder unter den π_k explizit angeben kann), zeigt der Beweis also auch, wie man dann g_n explizit als $n-$Korand schreiben kann.

Beispiel 2.4 Wir betrachten die exakte Sequenz von $\mathbb{G}_a$-Moduln

$$0 \to K \overset{\pi_2}{\to} K^2 \overset{\pi_1}{\to} K^2 \overset{\pi_0}{\to} K \to 0$$

mit $\pi_2(x) := (x, 0)$, $\pi_1(x, y) = (y, 0)$ und $\pi_0(x, y) = y$ für $x, y \in K$. Die Operation auf K ist dabei trivial, und die Operation auf K^2 gegeben durch $a \cdot (x, y) := (x + ay, y)$ für alle $a \in \mathbb{G}_a, (x, y) \in K^2$. Offenbar ist $\pi_0(0, 1) = 1$, also wählen wir $g_0 = (0, 1) \in C^0(\mathbb{G}_a, K^2)$. Sei ab jetzt $x, y \in K,\ a, b \in \mathbb{G}_a$. Es ist $\partial_0 g_0(a) = (a, 1) - (0, 1) = (a, 0) = \pi_1(0, a)$, und wir wählen daher $g_1 \in C^1(\mathbb{G}_a, K^2)$ mit $g_1(a) := (0, a)$. Es ist

$$\partial_1 g_1(a, b) = a \cdot g_1(b) - g_1(a + b) + g_1(a) = (ab, b) - (0, a + b) + (0, a) = (ab, 0) = \pi_2(ab).$$

Daher wählen wir $g_2 \in C^2(\mathbb{G}_a, K)$ mit $g_2(a, b) = ab$. Dann ist $g_2 \in Z^2(\mathbb{G}_a, K)$.

Ist $\mathrm{char}\, K \neq 2$, so ist mit $h \in C^1(\mathbb{G}_a, K)$ gegeben durch $h(a) := -\frac{1}{2}a^2$

$$g_2(a, b) = ab = -\frac{1}{2}b^2 + \frac{1}{2}(a + b)^2 - \frac{1}{2}a^2 = a \cdot h(b) - h(a + b) + h(a) = \partial_1 h(a, b),$$

also $g_2 \in B^2(\mathbb{G}_a, K)$. Dennoch gibt es kein $(x, y) \in (K^2)^{\mathbb{G}_a}$ mit $\pi_0(x, y) = 1$. Dann gibt es erst recht kein $\mu_0 : K \to K^2$ mit $\pi_0 \circ \mu_0 = \mathrm{id}$. Aus $\mu_0 \circ \pi_0 = \mathrm{id}$ folgte der Widerspruch $\pi_1 = 0$. Gäbe es $\mu_1 : K^2 \to K^2$ mit $\pi_1 \circ \mu_1 = \mathrm{id}$ bzw. $\mu_1 \circ \pi_1 = \mathrm{id}$, so wäre $\pi_0 = 0$ bzw. $\pi_2 = 0$. Gäbe es $\mu_2 : K^2 \to K$ mit $\pi_2 \circ \mu_2 = \mathrm{id}$, so wäre $\pi_1 = 0$. Es bleibt der Fall $\mu_2 \circ \pi_2 = \mathrm{id}$. Dann wäre aber $\ker \mu_2$ ein $\mathbb{G}_a$-stabiles Komplement zu $\mathrm{im}\, \pi_2 = K \cdot (1, 0)$ in K^2 - ein Widerspruch. Unsere Kriterien für das Vorliegen eines Korands sind also nur hinreichend, aber nicht notwendig.

Sei nun $\mathrm{char}\, K = 2$. Angenommen, es gäbe $h \in C^1(\mathbb{G}_a, K)$ mit $g_2 = \partial_1 h$. Dann ist

$$g_2(a, b) = ab = a \cdot h(b) - h(a + b) + h(a) = h(a) + h(b) + h(a + b) \quad \text{für alle } a, b \in K.$$

Für $a = b$ folgt hieraus $a^2 = h(0)$ für alle $a \in K$, ein Widerspruch. Dies zeigt $g_2 \notin B^2(\mathbb{G}_a, K)$ für $\mathrm{char}\, K = 2$.

2.7 Pushout und Pullback

Für die Konstruktion von exakten Sequenzen aus Kozyklen benötigen wir die Konstruktionen „Pushout“ und „Pullback“. Diese sind Spezialfälle von direktem und inversem Limes. Für diese allgemeineren Konstrukte siehe etwa [53, S. 39ff]. Wir beschränken uns hier auf KG-Moduln. Die Formulierung für R-Moduln mit einem beliebigen Ring R ist wörtlich dieselbe.

2.7.1 Pushout

Satz und Definition 2.5 *Seien X, Y_1, Y_2 jeweils G-Moduln und $\varphi_1 : X \to Y_1$, $\varphi_2 : X \to Y_2$ jeweils G-Homomorphismen. Der* Pushout *von φ_1 und φ_2 ist der G-Modul*

$$Z := (Y_1 \oplus Y_2)/W \quad \textit{mit} \quad W := \{(\varphi_1(x), -\varphi_2(x)) \in Y_1 \oplus Y_2 : x \in X\}$$

zusammen mit den Homomorphismen

$$\pi_1 : Y_1 \to Z, \quad y_1 \mapsto (y_1, 0) + W$$

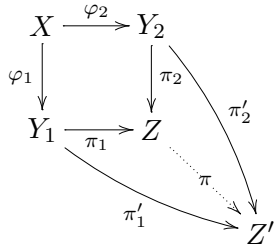
und

$$\pi_2 : Y_2 \to Z, \quad y_2 \mapsto (0, y_2) + W.$$

Dann gilt $\pi_1 \circ \varphi_1 = \pi_2 \circ \varphi_2$,

$$\begin{array}{ccc} X & \xrightarrow{\varphi_2} & Y_2 \\ {\scriptstyle\varphi_1}\downarrow & & \downarrow{\scriptstyle\pi_2} \\ Y_1 & \xrightarrow[\pi_1]{} & Z, \end{array}$$

und es gilt folgende universelle Eigenschaft: Für jeden weiteren G-Modul Z' und Homomorphismen $\pi_1' : Y_1 \to Z'$ und $\pi_2' : Y_2 \to Z'$ mit $\pi_1' \circ \varphi_1 = \pi_2' \circ \varphi_2$ existiert genau ein Homomorphismus $\pi : Z \to Z'$, der das folgende Pushout-Diagramm *kommutativ macht:*



Weiter gilt: Ist φ_1 injektiv/surjektiv, so ist auch π_2 injektiv/surjektiv.

Beweis. Offenbar ist W ein G-Untermodul von $Y_1 \oplus Y_2$ und daher Z ein G-Modul. Für $x \in X$ ist

$$\begin{aligned} \pi_1 \circ \varphi_1(x) &= (\varphi_1(x), 0) + W = (\varphi_1(x), 0) - (\varphi_1(x), -\varphi_2(x)) + W \\ &= (0, \varphi_2(x)) + W = \pi_2 \circ \varphi_2(x), \end{aligned}$$

also $\pi_1 \circ \varphi_1 = \pi_2 \circ \varphi_2$. Sind weiter Z', π_1', π_2' wie beschrieben, so gilt für

$$\pi' : Y_1 \oplus Y_2 \to Z', \quad (y_1, y_2) \mapsto \pi_1'(y_1) + \pi_2'(y_2)$$

wegen $\pi_1' \circ \varphi_1 = \pi_2' \circ \varphi_2$ offenbar $W \subseteq \ker \pi'$. Daher induziert π' eine Abbildung

$$\pi : Z = (Y_1 \oplus Y_2)/W \to Z', \quad \text{mit} \quad (y_1, y_2) + W \mapsto \pi_1'(y_1) + \pi_2'(y_2),$$

die offenbar $\pi \circ \pi_1 = \pi_1'$ und $\pi \circ \pi_2 = \pi_2'$ erfüllt. Ist $\bar{\pi}$ eine weitere solche Abbildung, so gilt offenbar

$$\bar{\pi}((y_1, y_2) + W) = \bar{\pi}(\pi_1(y_1) + \pi_2(y_2)) = \pi_1'(y_1) + \pi_2'(y_2) = \pi((y_1, y_2) + W),$$

also $\pi = \bar{\pi}$.

Sei nun φ_1 injektiv, und $y_2 \in Y_2$ mit $\pi_2(y_2) = 0$, d.h. $(0, y_2) \in W$. Dann gibt es $x \in X$ mit $\varphi_1(x) = 0$ und $\varphi_2(x) = y_2$. Aus der Injektivität von φ_1 folgt $x = 0$ und damit dann auch $y_2 = \varphi_2(x) = 0$, d.h. π_2 ist injektiv.

Sei nun φ_1 surjektiv. Zu $(y_1, y_2) + W \in Z$ (mit $y_i \in Y_i$, $i = 1, 2$) existiert dann ein $x \in X$ mit $y_1 = \varphi_1(x)$. Dann gilt

$$\begin{aligned} \pi_2(y_2 + \varphi_2(x)) &= (0, y_2 + \varphi_2(x)) + W = (0, y_2 + \varphi_2(x)) + (\varphi_1(x), -\varphi_2(x)) + W \\ &= (\varphi_1(x), y_2) + W = (y_1, y_2) + W, \end{aligned}$$

also ist auch π_2 surjektiv. □

Der Rest dieses Unterabschnitts wird nur für eine alternative Konstruktion gebraucht und kann übersprungen werden.

Korollar 2.6 *Im folgenden Diagramm von G-Moduln*

$$\begin{array}{ccccc} Y_1 & \xrightarrow{\varepsilon_1} & Y_2 & \xrightarrow{\varepsilon_2} & Y_3 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} \\ X_1 & \xrightarrow[\pi_1]{} & X_2 & \xrightarrow[\pi_2]{} & X_3 \end{array}$$

sei die obere Zeile exakt und φ_1 surjektiv. Weiter sei X_2 der Pushout von φ_1 und ε_1 mit Homomorphismen π_1 und φ_2, sowie X_3 der Pushout von φ_2 und ε_2 mit Homomorphismen π_2 und φ_3. Dann sind auch φ_2, φ_3 surjektiv, und auch die untere Zeile ist exakt.

Beweis. Die Surjektivität von φ_2 und φ_3 folgt direkt aus dem Satz. Aufgrund der Konstruktion ist das angegebene Diagramm jedenfalls kommutativ. Daher gilt

$$\pi_2 \circ \pi_1 \circ \varphi_1 = \varphi_3 \circ \underbrace{\varepsilon_2 \circ \varepsilon_1}_{=0} = 0,$$

und wegen der Surjektivität von φ_1 folgt auch $\pi_2 \circ \pi_1 = 0$, also $\operatorname{im} \pi_1 \subseteq \ker \pi_2$.

Sei umgekehrt $x_2 \in X_2$ mit $\pi_2(x_2) = 0$. Nach Definition des Pushouts ist $X_3 = (X_2 \oplus Y_3)/W$ mit $W = \{(\varphi_2(y_2), -\varepsilon_2(y_2)) \in X_2 \oplus Y_3 : y_2 \in Y_2\}$, und $\pi_2(x_2) = (x_2, 0) + W \in X_3$. Aus $\pi_2(x_2) = 0$ folgt daher $(x_2, 0) \in W$, d.h. es gibt $y_2 \in Y_2$ mit $x_2 = \varphi_2(y_2)$, $\varepsilon_2(y_2) = 0$. Mit der Exaktheit der oberen Sequenz gibt es also wegen $y_2 \in \ker \varepsilon_2 = \operatorname{im} \varepsilon_1$ ein $y_1 \in Y_1$ mit $y_2 = \varepsilon_1(y_1)$. Damit ist $x_2 = \varphi_2(y_2) = \varphi_2(\varepsilon_1(y_1)) = \pi_1(\varphi_1(y_1)) \in \operatorname{im} \pi_1$, also $\ker \pi_2 \subseteq \operatorname{im} \pi_1$. □

Beispiel 2.7 In diesem (Gegen-)Beispiel wollen wir zeigen, dass die Surjektivität von φ_1 in Korollar 2.6 notwendig ist, damit die induzierte Sequenz überhaupt ein Komplex ist. Sei K^n jeweils ein trivialer KG-Modul. Wir betrachten mit den Bezeichnungen des Korollars das folgende kommutative Diagramm

$$\begin{array}{ccccc} K & \xrightarrow{\varepsilon_1} & K^2 & \xrightarrow{\varepsilon_2} & K \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} \\ K^2 & \xrightarrow[\pi_1]{} & K^3 & \xrightarrow[\pi_2]{} & K^2 \end{array}$$

mit

$$\varepsilon_1(x_1) = (x_1, 0), \quad \varepsilon_2(x_1, x_2) = x_2$$
$$\varphi_1(x_1) = (x_1, 0), \quad \varphi_2(x_1, x_2) = (x_1, x_2, 0), \quad \varphi_3(x_2) = (x_2, 0)$$
$$\pi_1(x_1, x_3) = (x_1, 0, x_3), \quad \pi_2(x_1, x_2, x_3) = (x_2, x_3)$$

jeweils für $x_1, x_2, x_3 \in K$. Man beachte, dass hier φ_1 nicht surjektiv ist. Dabei sind in der unteren Zeile die rechten beiden Moduln Pushouts wie im Korollar beschrieben. Jedoch ist $\pi_2 \circ \pi_1(x_1, x_3) = (0, x_3)$, d.h. die untere Zeile ist nicht einmal ein Komplex.

2.7.2 Pullback

Wir kommen zu der zum Pushout „dualen“ Konstruktion.

Satz und Definition 2.8 *Seien X_1, X_2, Y jeweils G-Moduln und $\varphi_1 : X_1 \to Y$ sowie $\varphi_2 : X_2 \to Y$ jeweils G-Homomorphismen. Der* Pullback *von φ_1 und φ_2 ist der G-Modul*

$$Z := \{(x_1, x_2) \in X_1 \oplus X_2 : \quad \varphi_1(x_1) = \varphi_2(x_2)\}$$

zusammen mit den Homomorphismen

$$\pi_1 : Z \to X_1, \quad (x_1, x_2) \mapsto x_1$$

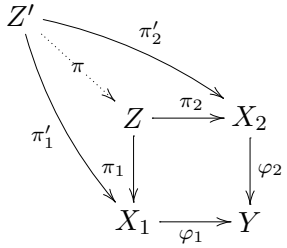
und

$$\pi_2 : Z \to X_2, \quad (x_1, x_2) \mapsto x_2.$$

Dann gilt $\varphi_1 \circ \pi_1 = \varphi_2 \circ \pi_2$,

$$\begin{array}{ccc} Z & \xrightarrow{\pi_2} & X_2 \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \varphi_2} \\ X_1 & \xrightarrow[\varphi_1]{} & Y, \end{array}$$

und es gilt folgende universelle Eigenschaft: Für jeden weiteren G-Modul Z' und Homomorphismen $\pi_1' : Z' \to X_1$ und $\pi_2' : Z' \to X_2$ mit $\varphi_1 \circ \pi_1' = \varphi_2 \circ \pi_2'$ existiert genau ein Homomorphismus $\pi : Z' \to Z$, der das folgende Pullback-Diagramm *kommutativ macht:*



Weiter gilt: Ist φ_2 injektiv/surjektiv, so ist auch π_1 injektiv/surjektiv.

Beweis. Offenbar ist Z ein G-Untermodul von $X_1 \oplus X_2$. Aufgrund der Definition von Z gilt $\varphi_1 \circ \pi_1 = \varphi_2 \circ \pi_2$. Sind weiter Z', π_1', π_2' wie beschrieben, so ist

$$\pi : Z' \to Z, \quad z' \mapsto (\pi_1'(z'), \pi_2'(z'))$$

wohldefiniert, denn $\varphi_1(\pi_1'(z')) = \varphi_2(\pi_2'(z'))$, also $(\pi_1'(z'), \pi_2'(z')) \in Z$. Ferner gilt für $z' \in Z'$ offenbar $\pi_1(\pi(z')) = \pi_1((\pi_1'(z'), \pi_2'(z'))) = \pi_1'(z')$, also $\pi_1 \circ \pi = \pi_1'$ und analog $\pi_2 \circ \pi = \pi_2'$. Ist nun $\bar{\pi} : Z' \to Z$ eine weitere Abbildung mit diesen Eigenschaften, so gilt für $z' \in Z'$ und $\bar{\pi}(z') = (x_1, x_2)$ mit $x_i \in X_i$, $i = 1, 2$ dann $x_1 = \pi_1((x_1, x_2)) = \pi_1(\bar{\pi}(z')) = \pi_1'(z')$ und analog $x_2 = \pi_2'(z')$. Also ist $\bar{\pi}(z') = (\pi_1'(z'), \pi_2'(z')) = \pi(z')$, also $\bar{\pi} = \pi$.

Sei nun φ_2 injektiv. Für $z = (x_1, x_2) \in \ker \pi_1$ folgt dann $0 = \pi_1(z) = x_1$. Da $z \in Z$ gilt $\varphi_2(x_2) = \varphi_1(x_1) = 0$. Aus der Injektivität von φ_2 folgt dann $x_2 = 0$, und damit $z = (x_1, x_2) = (0, 0) = 0 \in Z$. Also ist $\ker \pi_1 = 0$ und π_1 injektiv.

Sei nun φ_2 surjektiv. Zu $x_1 \in X_1$ gibt es dann $x_2 \in X_2$ mit $\varphi_1(x_1) = \varphi_2(x_2)$. Also ist $(x_1, x_2) \in Z$ und $\pi_1((x_1, x_2)) = x_1$, d.h. π_1 ist surjektiv. □

Der Rest dieses Unterabschnitts wird nur für eine alternative Konstruktion gebraucht und kann übersprungen werden.

Korollar 2.9 *In dem folgenden kommutativen Diagramm von G-Moduln*

$$\begin{array}{ccccc} X_1 & \overset{\pi_1}{\dashrightarrow} & X_2 & \overset{\pi_2}{\dashrightarrow} & X_3 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} \\ Y_1 & \xrightarrow[\varepsilon_1]{} & Y_2 & \xrightarrow[\varepsilon_2]{} & Y_3 \end{array}$$

sei die untere Zeile exakt und φ_3 injektiv. Weiter sei X_2 der Pullback von ε_2 und φ_3 mit Homomorphismen φ_2 und π_2, sowie X_1 der Pullback von ε_1 und φ_2 mit Homomorphismen φ_1 und π_1. Dann sind auch φ_1 und φ_2 injektiv und die obere Zeile ist ebenfalls exakt.

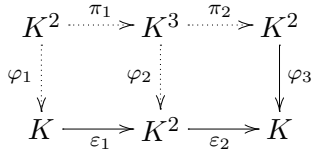
Beweis. Die Injektivität von φ_2 und φ_1 folgt direkt aus dem Satz. Aufgrund der Konstruktion ist das Diagramm kommutativ. Damit ist

$$\varphi_3 \circ \pi_2 \circ \pi_1 = \underbrace{\varepsilon_2 \circ \varepsilon_1}_{=0} \circ \varphi_1 = 0,$$

und wegen der Injektivität von φ_3 folgt auch $\pi_2 \circ \pi_1 = 0$, also $\operatorname{im} \pi_1 \subseteq \ker \pi_2$.

Sei nun umgekehrt $x_2 \in \ker \pi_2$. Da $x_2 \in X_2 = \{(y_2, x_3) \in Y_2 \oplus X_3 : \quad \varepsilon_2(y_2) = \varphi_3(x_3)\}$, gibt es also $y_2 \in Y_2$, $x_3 \in X_3$ mit $x_2 = (y_2, x_3)$ und $\varepsilon_2(y_2) = \varphi_3(x_3)$. Aus $0 = \pi_2(x_2) = \pi_2((y_2, x_3)) = x_3$ (Definition von π_2) folgt $0 = \varphi_3(x_3) = \varepsilon_2(y_2)$, also $y_2 \in \ker \varepsilon_2 = \operatorname{im} \varepsilon_1$ (Exaktheit der unteren Sequenz). Daher gibt es $y_1 \in Y_1$ mit $y_2 = \varepsilon_1(y_1)$. Wir setzen $x_1 := (y_1, x_2) \in Y_1 \oplus X_2$. Da $\varepsilon_1(y_1) = y_2 = \varphi_2((y_2, x_3)) = \varphi_2(x_2)$, gilt sogar $x_1 \in X_1$. Dann ist $\pi_1(x_1) = \pi_1((y_1, x_2)) = x_2$, also $x_2 \in \operatorname{im} \pi_1$ und damit $\ker \pi_2 \subseteq \operatorname{im} \pi_1$. □

Beispiel 2.10 Auch für den Pullback wollen wir anhand eines Gegenbeispiels zeigen, dass die Injektivität von φ_3 in obigem Korollar eine notwendige Voraussetzung ist. Es seien jeweils wieder K^n triviale KG-Moduln. Wir betrachten



mit

$$\varepsilon_1(x_1) = (x_1, 0), \quad \varepsilon_2(x_1, x_2) = x_2$$

$$\varphi_1(x_1, x_3) = x_1, \quad \varphi_2(x_1, x_2, x_3) = (x_1, x_2), \quad \varphi_3(x_2, x_3) = x_2$$

$$\pi_1(x_1, x_3) = (x_1, 0, x_3), \quad \pi_2(x_1, x_2, x_3) = (x_2, x_3)$$

jeweils für $x_1, x_2, x_3 \in K$. Man beachte, dass hier φ_3 nicht injektiv ist. Dabei sind in der oberen Zeile die linken beiden Moduln Pullbacks wie im Korollar beschrieben. Jedoch ist $\pi_2 \circ \pi_1(x_1, x_3) = (0, x_3)$, d.h. die obere Zeile ist nicht einmal ein Komplex.

2.8 Homomorphe Bilder von Kozyklen

Seien U, V jeweils G-Moduln, $\varepsilon : U \to V$ ein Homomorphismus von G-Moduln und $g \in Z^n(G, U)$ ein Kozyklus, d.h. $\partial_n^U g = 0$. Dann ist offenbar auch $\varepsilon \circ g \in Z^n(G, V)$ ein Kozyklus, denn es gilt auch $\partial_n^V(\varepsilon \circ g) = \varepsilon \circ \partial_n^U g = 0$. Ein häufiger Fall ist hierbei, dass $U \subseteq V$ ein Untermodul und $\varepsilon : U \hookrightarrow V$ die Inklusion ist.

Wir wollen in diesem Abschnitt zeigen, wie man aus einer exakten Sequenz, die $g \in Z^n(G, U)$ induziert, eine exakte Sequenz machen kann, die $\varepsilon \circ g \in Z^n(G, V)$ induziert.

Satz 2.11 *Sei $n \geq 1$,*

$$0 \to U_n \overset{\pi_n}{\to} U_{n-1} \overset{\pi_{n-1}}{\to} U_{n-2} \overset{\pi_{n-2}}{\to} \ldots \overset{\pi_1}{\to} U_0 \overset{\pi_0}{\to} U_{-1}$$

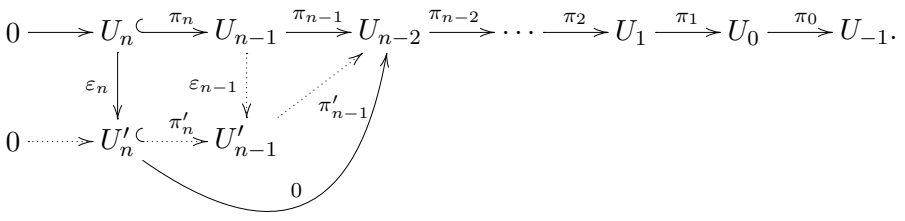
eine exakte Sequenz von G-Moduln und $w \in U_{-1}^G \cap \operatorname{im} \pi_0$. Für $k = 0, \ldots, n$ sei $g_k \in C^k(G, U_k)$ mit

$$\pi_0(g_0) = w \quad \text{und} \quad \pi_k \circ g_k = \partial_{k-1}^{U_{k-1}} g_{k-1} \quad \text{für } k = 1, \ldots, n \qquad (*)$$

eine Folge, die $g_n \in Z^n(G, U_n)$ gemäß Definition 2.2 induziert.

Sei U_n' ein weiterer G-Modul und $\varepsilon_n : U_n \to U_n'$ ein Homomorphismus von G-Moduln.

Sei weiter U_{n-1}' der Pushout von ε_n und π_n mit Homomorphismen π_n' und ε_{n-1}. Gemäß der universellen Eigenschaft des Pushouts bilde man weiter die Abbildung $\pi_{n-1}' : U_{n-1}' \to U_{n-2}$, die folgendes Diagramm kommutativ macht (Details im Beweis):



Dann ist die nach unten abknickende, zu U_n' führende Sequenz exakt und induziert (mit gleichem $w \in U_{-1}^G \cap \operatorname{im} \pi_0$) gemäß Definition 2.2 den Kozyklus $\varepsilon_n \circ g_n \in Z^n(G, U_n')$.

Beweis. Da π_n injektiv ist, ist nach Satz 2.5 auch π'_n injektiv und damit die untere Sequenz an der Stelle U'_n exakt. Ferner gilt mit der Nullabbildung $0 : U'_n \to \mathrm{im}(\pi_{n-1})$, dass $0 \circ \varepsilon_n = \pi_{n-1} \circ \pi_n$, denn die obere Sequenz ist exakt. Nach der universellen Eigenschaft des Pushouts, angewendet auf die Abbildungen $0 : U'_n \to \mathrm{im}(\pi_{n-1})$ und $\pi_{n-1} : U_{n-1} \to \mathrm{im}(\pi_{n-1})$ (beachte die Einschränkung des Bildbereichs!) existiert also wie behauptet eine Abbildung $\pi'_{n-1} : U'_{n-1} \to \mathrm{im}(\pi_{n-1}) \subseteq U_{n-2}$, die das Diagramm kommutativ macht. Nach Definition gilt dann $\mathrm{im}(\pi'_{n-1}) \subseteq \mathrm{im}(\pi_{n-1})$. Aufgrund der Kommutativität des Diagramms gilt $\pi'_{n-1} \circ \varepsilon_{n-1} = \pi_{n-1}$, und damit umgekehrt auch $\mathrm{im}(\pi_{n-1}) \subseteq \mathrm{im}(\pi'_{n-1})$, folglich $\mathrm{im}(\pi'_{n-1}) = \mathrm{im}(\pi_{n-1}) = \ker(\pi_{n-2})$. Damit ist die nach unten abgebogene Sequenz an der Stelle U_{n-2} exakt.

Weiter folgt aus der Kommutativität des Diagramms $0 = \pi'_{n-1} \circ \pi'_n$, also $\mathrm{im}\,\pi'_n \subseteq \ker \pi'_{n-1}$. Nach Konstruktion des Pushouts als Faktormodul $U'_{n-1} = (U'_n \oplus U_{n-1})/W$, wobei dann π'_n und ε_{n-1} die entsprechenden Projektionen sind (siehe Definition 2.5), gilt $U'_{n-1} = \pi'_n(U'_n) + \varepsilon_{n-1}(U_{n-1})$. Insbesondere gibt es zu $x \in \ker \pi'_{n-1} \subseteq U'_{n-1}$ dann $x_1 \in U'_n$ und $x_2 \in U_{n-1}$ mit $x = \pi'_n(x_1) + \varepsilon_{n-1}(x_2)$. Anwenden von π'_{n-1} auf diese Gleichung unter Beachtung der Kommutativität des Diagramms liefert $0 = 0 + \pi_{n-1}(x_2)$, also $x_2 \in \ker \pi_{n-1} = \mathrm{im}\,\pi_n$. Also gibt es $x_3 \in U_n$ mit $x_2 = \pi_n(x_3)$, und wir erhalten $x = \pi'_n(x_1) + \varepsilon_{n-1}(x_2) = \pi'_n(x_1) + \varepsilon_{n-1}(\pi_n(x_3)) = \pi'_n(x_1) + \pi'_n(\varepsilon_n(x_3)) \in \mathrm{im}\,\pi'_n$. Es gilt also auch $\ker \pi'_{n-1} \subseteq \mathrm{im}\,\pi'_n$ und damit insgesamt $\ker \pi'_{n-1} = \mathrm{im}\,\pi'_n$. Also ist die nach unten abgebogene Sequenz auch an der Stelle U'_{n-1} exakt. Damit ist sie dann überall exakt.

Wir setzen nun $g'_n := \varepsilon_n \circ g_n \in C^n(G, U'_n)$, $g'_{n-1} := \varepsilon_{n-1} \circ g_{n-1} \in C^{n-1}(G, U'_{n-1})$ und $g'_k := g_k \in C^k(G, U_k)$ für $k = 0, \ldots, n-2$, und zeigen, dass die Folge (g'_k) die entsprechende Eigenschaft $(*)$ aus Satz 2.2 besitzt. Gemäß Definition induziert die Sequenz dann den Kozyklus $g'_n = \varepsilon_n \circ g_n \in Z^n(G, U'_n)$ wie behauptet. Dabei ist $(*)$ offenbar nur noch für $k = n$ und $k = n-1$ zu prüfen. Wir verfizieren

$$\begin{aligned} \pi'_n \circ g'_n &= \pi'_n \circ \varepsilon_n \circ g_n = \varepsilon_{n-1} \circ \pi_n \circ g_n \overset{(*)}{=} \varepsilon_{n-1} \circ \partial_{n-1}^{U_{n-1}} g_{n-1} \\ &= \partial_{n-1}^{U'_{n-1}}(\varepsilon_{n-1} \circ g_{n-1}) = \partial_{n-1}^{U'_{n-1}} g'_{n-1}, \end{aligned}$$

also die $(*)$ entsprechende Eigenschaft für die Folge (g'_k) und $k = n$, und ebenso

$$\pi'_{n-1} \circ g'_{n-1} = \pi'_{n-1} \circ \varepsilon_{n-1} \circ g_{n-1} = \pi_{n-1} \circ g_{n-1} \overset{(*)}{=} \partial_{n-2}^{U_{n-2}} g_{n-2} = \partial_{n-2}^{U_{n-2}} g'_{n-2},$$

also die $(*)$ entsprechende Eigenschaft für $k = n-1$. Für $n = 1$ und $k = 0$ erhält man entsprechend $\pi'_0(g'_0) = \pi_0(g_0) = w$. □

2.9 Der generische n-Kozyklus

Wir betrachten nochmals die bar resolution

$$\ldots \overset{d_{n+1}}{\to} P_n \overset{d_n}{\to} P_{n-1} \overset{d_{n-1}}{\to} P_{n-2} \overset{d_{n-2}}{\to} \ldots \overset{d_2}{\to} P_1 \overset{d_1}{\to} P_0 \overset{d_0}{\to} K \to 0$$

und verwenden die Bezeichnungen aus Abschnitt 2.3. Aus den Definitionen von d_n (S. 55, (34)), $\partial_n^{P_n}$ (S. 51, (30)) und e_n (S. 55, (38)) erhalten wir sofort

$$d_0(e_0) = 1 \quad \text{und} \quad d_n \circ e_n = \partial_{n-1}^{P_{n-1}} e_{n-1} \quad \text{für alle } n \geq 1. \tag{47}$$

Wir betrachten nun

$$\overline{P_n} := P_n / \mathrm{im}\, d_{n+1} \tag{48}$$

mit der kanonischen Projektion

$$p_n : P_n \to \overline{P_n} \tag{49}$$

sowie

$$\overline{e_n} := p_n \circ e_n \in C^n(G, \overline{P_n}). \tag{50}$$

Dann gilt

$$\partial_n^{\overline{P_n}} \overline{e_n} = \partial_n^{\overline{P_n}}(p_n \circ e_n) = p_n \circ \partial_n^{P_n} e_n \overset{(47)}{=} p_n \circ d_{n+1} \circ e_n = 0,$$

(da $p_n \circ d_{n+1} = 0$), also $\overline{e_n} \in Z^n(G, \overline{P_n})$. Wir nennen diesen „allgemeinsten“ Kozyklus den *generischen n-Kozyklus*.

Da $\operatorname{im} d_{n+1} = \ker d_n$ existiert eine *injektive* Abbildung

$$\overline{d_n} : \overline{P_n} \to P_{n-1} \quad \text{mit} \quad \overline{d_n} \circ p_n = d_n, \tag{51}$$

und wir erhalten so die *generische exakte Sequenz des generischen n-Kozyklus*

$$0 \to \overline{P_n} \overset{\overline{d_n}}{\to} P_{n-1} \overset{d_{n-1}}{\to} P_{n-2} \overset{d_{n-2}}{\to} \dots \overset{d_2}{\to} P_1 \overset{d_1}{\to} P_0 \overset{d_0}{\to} K \to 0. \tag{52}$$

Wegen (47) und

$$\overline{d_n} \circ \overline{e_n} \overset{(50)}{=} \overline{d_n} \circ p_n \circ e_n \overset{(51)}{=} d_n \circ e_n \overset{(47)}{=} \partial_{n-1}^{P_{n-1}} e_{n-1} \tag{53}$$

erfüllt die Folge $e_0, \dots, e_{n-1}, \overline{e_n}$ die Voraussetzung $(*)$ von Definition 2.2, so dass $\overline{e_n}$ von der generischen Sequenz induziert wird.

Satz 2.12 *Der generische n-Kozyklus $\overline{e_n} \in Z^n(G, \overline{P_n})$ besitzt folgende universelle Eigenschaft: Zu jedem G-Modul V und jedem n-Kozyklus $g \in Z^n(G, V)$ existiert genau eine KG-lineare Abbildung $\phi_g^n : \overline{P_n} \to V$ mit $g = \phi_g^n \circ \overline{e_n}$.*

Beweis. Wir betrachten gemäß der Konstruktion (37), S. 55 die KG-lineare Abbildung

$$\omega_n^V(g) : P_n \to V, \quad \text{mit} \quad [\sigma_1, \dots, \sigma_n] \mapsto g(\sigma_1, \dots, \sigma_n).$$

Nach Gleichung (42) gilt

$$\omega_n^V(g) \circ d_{n+1} = \omega_{n+1}^V(\partial_n^V g) = \omega_{n+1}^V(0) = 0,$$

da $g \in Z^n(G, V)$. Also ist $\omega_n^V(g)|_{\operatorname{im} d_{n+1}} = 0$, und damit existiert eine Faktorisierung

$$\phi_g^n : \overline{P_n} = P_n / \operatorname{im} d_{n+1} \to V \quad \text{mit} \quad \omega_n^V(g) = \phi_g^n \circ p_n \tag{54}$$

(siehe (49)). Wir erhalten

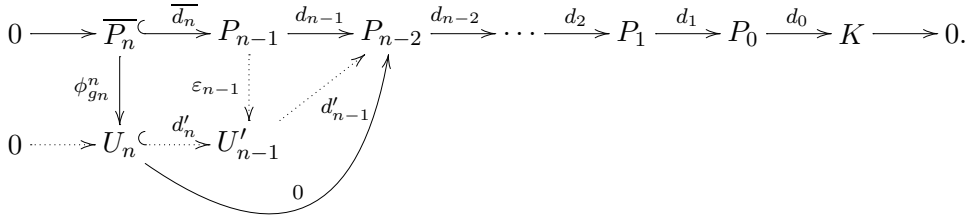
$$\phi_g^n \circ \overline{e_n} \overset{(50)}{=} \phi_g^n \circ p_n \circ e_n \overset{(54)}{=} \omega_n^V(g) \circ e_n \overset{(39)}{=} g$$

wie gewünscht. Die Eindeutigkeit folgt, weil $\overline{P_n}$ als KG-Modul von $\overline{e_n}(G^n)$ erzeugt wird.□

2.10 Von Kozyklen zu exakten Sequenzen

In Satz 2.2 haben wir gesehen, dass jeder exakten Sequenz der Form (45) ein bis auf einen Korand eindeutiger Kozyklus zugeordnet werden kann. Wir wollen nun zeigen, dass jedem Kozyklus auch eine ihn induzierende Sequenz der Form (45) zugeordnet werden kann.

Satz 2.13 *Sei $n \geq 1$, U_n ein G-Modul und $g_n \in Z^n(G, U_n)$ ein n-Kozyklus. Dann existiert eine exakte Sequenz der Form* (45)*, die g_n induziert. Genauer kann man hierfür die nach unten abknickende Sequenz des folgenden Diagramms wählen,*



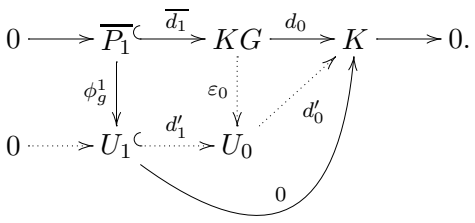
Hierbei ist die obere Zeile die generische exakte Sequenz des generischen n-Kozyklus (52)*, $\phi^n_{g_n} : \overline{P_n} \to U_n$ die KG-lineare Abbildung aus Satz 2.12, und die untere Zeile wird mit Hilfe des Pushouts wie in Satz 2.11 gebildet.*

Beweis. Die obere Zeile induziert nach Abschnitt 2.9 den generischen n-Kozyklus $\overline{e_n} \in Z^n(G, \overline{P_n})$. Nach Satz 2.12 gilt für den KG-Homomorphismus $\phi^n_{g_n} : \overline{P_n} \to U_n$ dann $g_n = \phi^n_{g_n} \circ \overline{e_n}$. Nach Satz 2.11 induziert dann die nach unten abknickende Sequenz den Kozyklus g_n. □

Dieser Satz liefert eine eher unhandliche exakte Sequenz zurück. Insbesondere sind für unendliches G die P_k unendlichdimensional, während man den Kozyklus dennoch oft durch eine Sequenz aus endlichdimensionalen Moduln induzieren kann.

Beispiel 2.14 Um eine induzierende Sequenz für einen Korand $g_n \in B^n(G, U_n)$ anzugeben, können wir nach Satz 2.2 ohne Einschränkung $g_n = 0 \in B^n(G, U_n)$ annehmen (denn eine Sequenz induziert jeden Repräsentanten der Restklasse). Dann ist $\phi^n_{g_n} = 0$, und nach Konstruktion des Pushouts gilt dann $U'_{n-1} = (U_n \oplus P_{n-1})/\{(0, -\overline{d_n}(x)) : x \in \overline{P_n}\} \cong U_n \oplus (P_{n-1}/\operatorname{im} d_n) \overset{(48)}{=} U_n \oplus \overline{P_{n-1}}$. Es ist dann d'_n durch die Einbettung $U_n \hookrightarrow U_n \oplus \overline{P_{n-1}}$ gegeben, und es existiert ein „links-Splitting“ $\mu_n : U'_{n-1} \to U_n$ mit $\mu_n \circ d'_n = \mathrm{id}_{U_n}$, wie in einem der Kriterien von Satz 2.2 für das Vorliegen eines Korands gefordert. Auch wenn dieses Kriterium nicht notwendig für das Vorliegen eines Korands ist (wie wir in Beispiel 2.4 gesehen haben), gibt es also wenigstens eine induzierende Sequenz zu einem gegebenen Korand, die dieses Kriterium erfüllt.

Beispiel 2.15 Wir untersuchen die Konstruktion im Fall $n = 1$ noch etwas expliziter. Sei also $g = g_1 \in Z^1(G, U_1)$. Wir haben also das Diagramm



Dann ist $U_0 := (U_1 \oplus KG)/W$ mit

$$W = \langle \{(g(\sigma), -(\sigma - \iota)) \in U_1 \oplus KG : \quad \sigma \in G\} \rangle_{KG}.$$

($\iota \in G$ das neutrale Element.) Da

$$(\tau g(\sigma), -\tau(\sigma - \iota)) = (g(\tau\sigma), -(\tau\sigma - \iota)) - (g(\tau), -(\tau - \iota))$$

(aufgrund der Kozyklus-Eigenschaft), gilt sogar

$$W = \langle \{(g(\sigma), -(\sigma - \iota)) \in U_1 \oplus KG : \quad \sigma \in G\} \rangle_{K}. \tag{55}$$

Wir definieren $\tilde{U_1} := U_1 \oplus K$ mit G-Operation

$$\sigma \cdot (u, \lambda) := (\sigma u + \lambda g(\sigma), \lambda) \quad \text{für } u \in U_1,\ \lambda \in K,\ \sigma \in G$$

(wie in Abschnitt 1.3) und behaupten, dass durch

$$F : \tilde{U_1} \to U_0, \quad (u, \lambda) \mapsto (u, \lambda \cdot \iota) + W$$

ein Isomorphismus von KG-Moduln gegeben ist. Die K-Linearität ist klar. Ferner ist

$$\begin{aligned} F(\sigma \cdot (u, \lambda)) &= F((\sigma u + \lambda g(\sigma), \lambda)) = (\sigma u + \lambda g(\sigma), \lambda \cdot \iota) + W \\ &= (\sigma u + \lambda g(\sigma), \lambda \cdot \iota) - \lambda(g(\sigma), -(\sigma - \iota)) + W = \\ &= (\sigma u, \lambda\sigma) + W = \sigma F(u, \lambda) \quad \text{für alle } u \in U_1, \lambda \in K, \end{aligned}$$

d.h. F ist KG-linear. F ist injektiv, denn für $u \in U_1, \lambda \in K$ mit $F((u, \lambda)) = 0$ folgt $(u, \lambda \cdot \iota) \in W$. Nach (55) gibt es dann $\sigma_i \in G, \lambda_i \in K$, $i = 1, \ldots, n$ mit

$$(u, \lambda \cdot \iota) = \sum_{i=1}^{n} (\lambda_i g(\sigma_i), -\lambda_i(\sigma_i - \iota)). \tag{56}$$

Dabei können wir O.E. $\sigma_i \neq \sigma_j$ für $i \neq j$ annehmen. Da $g(\iota) = g(\iota\iota) = \iota g(\iota) + g(\iota)$, also $g(\iota) = 0$, können wir außerdem $\sigma_i \neq \iota$ für alle i annehmen. Da in der zweiten Komponente der linken Seite von (56) kein Term mit $\sigma_i \neq \iota$ vorkommt, rechts aber $\lambda_i\sigma_i$, folgt $\lambda_i = 0$ für alle i. Mit (56) folgt $(u, \lambda) = 0$, also ist F injektiv.

Zum Beweis der Surjektivität genügt es wegen der KG-Linearität von F ein Urbild für $(u, \lambda\sigma) + W$ ($u \in U_1, \lambda \in K, \sigma \in G$) anzugeben. Da

$$\begin{aligned} F((u + \lambda g(\sigma), \lambda)) &= (u + \lambda g(\sigma), \lambda\iota) + W \\ &= (u + \lambda g(\sigma), \lambda\iota) - \lambda(g(\sigma), -(\sigma - \iota)) + W \\ &= (u, \lambda\sigma) + W, \end{aligned}$$

ist F also auch surjektiv.

Der Abbildung $d_1' : U_1 \to U_0$, $u \mapsto (u, 0) + W$ entspricht via F dann die Abbildung $\pi_1 : U_1 \to \tilde{U_1}$, $u \mapsto (u, 0)$.

Nach dem Beweis zur universellen Eigenschaft des Pushouts (Satz 2.5) gilt für d_0' ferner

$$d_0'((u, \lambda \cdot \iota) + W) = 0(u) + d_0(\lambda \cdot \iota) = \lambda \quad \text{für alle } u \in U_1, \lambda \in K.$$

Also entspricht d_0' via F der Abbildung $\pi_0 : \tilde{U_1} \to K$, $(u, \lambda) \mapsto \lambda$, und wir erhalten die exakte Sequenz

$$0 \to U_1 \overset{\pi_1}{\to} \tilde{U_1} \overset{\pi_0}{\to} K \to 0.$$

Damit entspricht unsere Konstruktion einer exakten Sequenz aus einem 1-Kozyklus genau der im Text nach Proposition 1.51 angegebenen.

Konstruktion durch sukzessive Pushout-Bildung

In diesem ergänzenden Abschnitt wollen wir eine weitere Konstruktion einer exakten Sequenz angeben, die einen vorgegebenen Kozyklus induziert. Diese funktioniert zwar nur unter Zusatzvoraussetzungen, führt aber im Allgemeinen zu „kleineren" Moduln in der Sequenz. Dieser Abschnitt kann übersprungen werden.

Ist $U_n' \subseteq U_n$ ein Untermodul und $g_n \in Z^n(G, U_n)$, so dass $g_n(G^n) \subseteq U_n'$, so ist offenbar auch $g_n \in Z^n(G, U_n')$. Mit Hilfe von Satz 2.13 kann man dann also auch eine exakte Sequenz konstruieren, die $g_n \in Z^n(G, U_n')$ induziert. Ist $g_n \in Z^n(G, U_n)$ nichttrivial, so gilt dies erst recht für $g_n \in Z^n(G, U_n')$. Der kleinste Untermodul $U_n' \subseteq U_n$ mit $g_n(G^n) \subseteq U_n'$ ist offenbar gegeben durch $\langle g_n(G^n)\rangle_{KG}$, und wegen $\partial_n g_n = 0$ und der Definition von ∂_n ist

$$\langle g_n(G^n)\rangle_K = \langle g_n(G^n)\rangle_{KG},$$

also der von den $g_n(\sigma_1, \ldots, \sigma_n)$, $\sigma_1, \ldots, \sigma_n \in G$ erzeugte K-Unterraum sogar ein KG-Untermodul. Ist also $g_n \in Z^n(G, U_n)$ nichttrivial, so erst recht $g_n \in Z^n(G, \langle g_n(G^n)\rangle_K)$. Es ist daher keine große Einschränkung, wenn wir $g_n \in Z^n(G, U_n)$ *nichttrivial* und

$$U_n = \langle g_n(G^n)\rangle_K \tag{57}$$

fordern. (Gegebenenfalls kann man mit Satz 2.11 dann nachträglich U_n in einen größeren Modul einbetten und erhält so auch für den größeren Modul eine exakte Sequenz). Unter diesen Voraussetzungen wollen wir in diesem Abschnitt eine alternative Konstruktion einer exakten Sequenz (45) (S. 59) angeben, die g_n induziert.

Wir verwenden wieder die Notation von Abschnitt 2.3, S. 54, insbesondere benötigen wir die numerierten Gleichungen.

Offenbar ist (57) genau dann erfüllt, wenn

$$\varphi_n := \omega_n^{U_n}(g_n) \in \mathrm{Hom}_{KG}(P_n, U_n)$$

(siehe (37), S. 55) surjektiv ist. Durch sukzessive Pushout-Bildung erhalten wir aus der bar resolution (36) (S. 55) und φ_n das folgende kommutative Diagramm:

$$\begin{array}{ccccccccccccccc}
P_{n+1} & \xrightarrow{d_{n+1}} & P_n & \xrightarrow{d_n} & P_{n-1} & \xrightarrow{d_{n-1}} & P_{n-2} & \xrightarrow{d_{n-2}} & \cdots & \xrightarrow{d_3} & P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & P_0 & \xrightarrow{d_0} & K & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n-1}} & & \downarrow{\scriptstyle \varphi_{n-2}} & & & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi_{-1}} & & \downarrow{\scriptstyle \varphi_{-2}} \\
0 & \longrightarrow & U_n & \xrightarrow[\pi_n]{} & U_{n-1} & \xrightarrow[\pi_{n-1}]{} & U_{n-2} & \xrightarrow[\pi_{n-2}]{} & \cdots & \xrightarrow[\pi_3]{} & U_2 & \xrightarrow[\pi_2]{} & U_1 & \xrightarrow[\pi_1]{} & U_0 & \xrightarrow[\pi_0]{} & U_{-1} & \xrightarrow[\pi_{-1}]{} & U_{-2}
\end{array}$$

Hierbei ist für $k = n-1, \ldots, -2$ jeweils U_k der Pushout von φ_{k+1} und d_{k+1} mit Homomorphismen π_{k+1} und φ_k.

Satz 2.16 *Sei $n \geq 1$ und $g_n \in Z^n(G, U_n)$ ein* nichttrivialer *n-Kozyklus, so dass*

$$U_n = \langle \{ g_n(\sigma_1, \ldots, \sigma_n) : \quad \sigma_1, \ldots, \sigma_n \in G \} \rangle_K .$$

Dann ist die untere Zeile des obigen kommutativen Diagramms eine exakte Sequenz der Form

$$0 \longrightarrow U_n \xrightarrow{\pi_n} U_{n-1} \xrightarrow{\pi_{n-1}} U_{n-2} \xrightarrow{\pi_{n-2}} \cdots \xrightarrow{\pi_3} U_2 \xrightarrow{\pi_2} U_1 \xrightarrow{\pi_1} U_0 \xrightarrow{\pi_0} K \longrightarrow 0$$

und induziert (gemäß Satz/Definition 2.2) den Kozyklus g_n.

Da die φ_k zwar surjektiv sind, in der Regel aber nicht injektiv sein werden, sind die U_k also als Faktormoduln der P_k „kleiner“ als die Moduln der nach Satz 2.13 konstruierten Sequenz.

Beweis. Da die obere Sequenz exakt und φ_n nach Voraussetzung surjektiv ist, ist nach Korollar 2.6 auch die untere Sequenz (bis evtl. an der Stelle U_n) exakt und alle φ_k ebenfalls surjektiv. Für die Exaktheit an der Stelle U_n zeigen wir, dass π_n injektiv ist. Sei also $u \in U_n$ mit $\pi_n(u) = 0 \in U_{n-1}$. Nach Konstruktion ist $U_{n-1} = (U_n \oplus P_{n-1})/W$ mit $W = \{(\varphi_n(x), -d_n(x)) \in U_n \oplus P_{n-1} : \quad x \in P_n\}$, und es ist $\pi_n(u) = (u, 0) + W$. Aus $\pi_n(u) = 0$ folgt also $(u, 0) \in W$, d.h. es gibt ein $x \in P_n$ mit $u = \varphi_n(x)$ und $0 = d_n(x)$. Wegen der Exaktheit der oberen Sequenz und $x \in \ker d_n = \operatorname{im} d_{n+1}$ gibt es $y \in P_{n+1}$ mit $x = d_{n+1}(y)$. Dann ist also

$$u = \varphi_n(x) = \varphi_n \circ d_{n+1}(y) = \omega_n^{U_n}(g_n) \circ d_{n+1}(y) \overset{(42)}{=} \omega_{n+1}^{U_n}(\partial_n^{U_n} g_n)(y) = 0,$$

da $\partial_n^{U_n} g_n = 0$ wegen $g_n \in Z^n(G, U_n)$. Also ist $\ker \pi_n = 0$ und die untere Sequenz exakt.

Aus der Surjektivität von φ_{-2} folgt außerdem $U_{-2} = 0$.

Mit e_k wie in (38) gilt

$$\varphi_n \circ e_n = \omega_n^{U_n}(g_n) \circ e_n \overset{(39)}{=} g_n,$$

und wir setzen daher auch für $k = n - 1, \ldots, 0$

$$g_k := \varphi_k \circ e_k \in C^k(G, U_k). \tag{58}$$

Dann gilt

$$\omega_k^{U_k}(g_k) = \omega_k^{U_k}(\varphi_k \circ e_k) \overset{(40)}{=} \varphi_k \quad \text{für alle } k = 0, \ldots, n. \tag{59}$$

Mit der Kommutativität des Diagramms erhalten wir

$$\begin{aligned} \pi_k \circ g_k &\overset{(58)}{=} \pi_k \circ \varphi_k \circ e_k = \varphi_{k-1} \circ d_k \circ e_k \overset{(59)}{=} \omega_{k-1}^{U_{k-1}}(g_{k-1}) \circ d_k \circ e_k \\ &\overset{(42)}{=} \omega_k^{U_{k-1}}(\partial_{k-1}^{U_{k-1}} g_{k-1}) \circ e_k \overset{(39)}{=} \partial_{k-1}^{U_{k-1}} g_{k-1} \quad \text{für alle } k = 1, \ldots, n, \end{aligned}$$

also

$$\pi_k \circ g_k = \partial_{k-1}^{U_{k-1}} g_{k-1} \quad \text{für alle } k = 1, \ldots, n, \tag{60}$$

d.h. die g_k erfüllen den zweiten Teil der Bedingung $(*)$ von Satz 2.2 (S. 59). Wenn wir nun noch $U_{-1} \cong K$ und $\pi_0(g_0) = 1$ zeigen, so ist die untere Sequenz von der behaupteten Form und induziert nach Satz 2.2 den Kozyklus g_n. Wir zeigen $\pi_0(g_0) \neq 0$. Dann ist insbesondere $U_{-1} \neq 0$ (da $\pi_0(g_0) \in U_{-1}$), und aus der Surjektivität der KG-linearen Abbildung $\varphi_{-1} : K \to U_{-1}$ folgt dann $U_{-1} \cong K$. Da man den Isomorphismus so wählen kann, dass $\pi_0(g_0) \neq 0$ gerade $1 \in K$ entspricht, sind wir dann fertig.

Wir nehmen also stattdessen $\pi_0(g_0) = 0$ an, und zeigen für $k = 1, \ldots, n$ die Existenz eines

$$h_k \in C^{k-1}(G, U_k) \quad \text{mit} \quad \pi_k \circ g_k = \pi_k \circ \partial_{k-1}^{U_k} h_k. \tag{61}$$

Da $g_0 \in \ker \pi_0 = \operatorname{im} \pi_1$, gibt es ein $h_1 \in U_1 = C^0(G, U_1)$ mit $g_0 = \pi_1 \circ h_1$. Es folgt

$$\pi_1 \circ g_1 \overset{(60)}{=} \partial_0^{U_0} g_0 = \partial_0^{U_0}(\pi_1 \circ h_1) = \pi_1 \circ \partial_0^{U_1} h_1,$$

also (61) für $k = 1$.

Sei nun $h_1, \dots, h_k$ bereits konstruiert. Aus (61) folgt

$$\pi_k \circ (g_k - \partial_{k-1}^{U_k} h_k) = 0.$$

Da $\ker \pi_k = \operatorname{im} \pi_{k+1}$, gibt es also $h_{k+1} \in C^k(G, U_{k+1})$ mit

$$g_k - \partial_{k-1}^{U_k} h_k = \pi_{k+1} \circ h_{k+1}. \tag{62}$$

Mit Hilfe von $\partial_k^{U_k} \circ \partial_{k-1}^{U_k} = 0$ erhalten wir hieraus

$$\pi_{k+1} \circ g_{k+1} \overset{(60)}{=} \partial_k^{U_k} g_k \overset{(62)}{=} \partial_k^{U_k}(\pi_{k+1} \circ h_{k+1}) = \pi_{k+1} \circ \partial_k^{U_{k+1}} h_{k+1},$$

also (61) für $k + 1$.

Mit der Injektivität von π_n erhalten wir aus (61) insbesondere für $k = n$, dass

$$g_n = \partial_{n-1}^{U_n} h_n \in B^n(G, U_n),$$

im Widerspruch zur vorausgesetzten Nichttrivialität von g_n. Also ist $\pi_0(g_0) \neq 0$. □

Beispiel 2.17 Wir wollen noch kurz zeigen, dass auch diese Konstruktion im Fall $n = 1$ zum selben Ergebnis führt wie in Abschnitt 1.3. Dabei sehen wir auch gut, wo die Surjektivität von φ_n ins Spiel kommt. Wir haben dann also das Diagramm

$$\begin{array}{ccccccccc}
P_2 & \xrightarrow{d_2} & P_1 & \xrightarrow{d_1} & KG & \xrightarrow{d_0} & K & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi_{-1}} & & \\
0 & \longrightarrow & U_1 & \xrightarrow[\pi_1]{} & U_0 & \xrightarrow[\pi_0]{} & U_{-1} & \longrightarrow & 0
\end{array}$$

Wir können hier an Beispiel 2.15 anknüpfen (und verwenden die dortigen Bezeichnungen): Die Konstruktion von $U_0 = (U_1 \oplus KG)/W$ ist identisch, und es ist $d_1' = \pi_1$. Es bleibt also noch die Konstruktion von U_{-1} und π_0. Um π_0 explizit anzugeben, schreiben wir $(u, x)_W := (u, x) + W$ für $u \in U_1$, $x \in KG$, und es ist $U_{-1} = (U_0 \oplus K)/W_0$. In U_{-1} gilt

$$((0, \sigma)_W, 0) \equiv ((0, 0)_W, 1) \quad \text{für } \sigma \in G. \tag{63}$$

Es ist $\pi_0 : U_0 \to U_{-1}$, $(u, x)_W \mapsto ((u, x)_W, 0) + W_0$. Nach Voraussetzung ist $U_1 = \langle g(\sigma) : \sigma \in G \rangle_K$. Für ein $u \in U_1$ gibt es also eine Darstellung $u = \sum_{i=1}^n \lambda_i g(\sigma_i)$ mit $\lambda_i \in K, \sigma_i \in G$ für alle i (hier geht also die Surjektivität von φ_1 ein!). Da $(g_\sigma, 0)_W = (0, \sigma - \iota)_W$ für alle $\sigma \in G$, ist also für $\lambda \in K$

$$(u, \lambda\iota)_W = \left(\sum_{i=1}^n \lambda_i g(\sigma_i), \lambda\iota \right)_W = \left(0, \lambda\iota + \sum_{i=1}^n \lambda_i (\sigma_i - \iota) \right)_W.$$

Daher ist

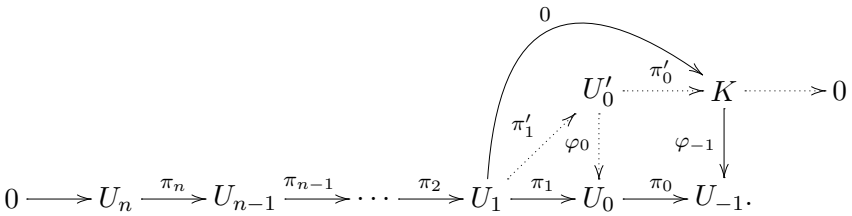
$$\begin{aligned}
\pi_0((u, \lambda\iota)_W) &= \left(\left(0, \lambda\iota + \sum_{i=1}^n \lambda_i (\sigma_i - \iota) \right)_W, 0 \right) + W_0 \\
&\overset{(63)}{=} ((0, 0)_W, \lambda \cdot 1 + \sum_{i=1}^n \lambda_i \cdot (1 - 1))) + W_0 \\
&= ((0, 0)_W, \lambda) + W_0.
\end{aligned}$$

Also entspricht π_0 via F der Abbildung $\tilde{U_1} \to K$, $(u, \lambda) \mapsto \lambda$ wie erwartet.

2.11 Induktion von Kozyklen durch Standardsequenzen

Gemäß Satz 2.13 können wir jeden Kozyklus durch eine „Standardsequenz“, also eine exakte Sequenz der Form (45) (S. 59) induzieren. Dabei sind die P_k jedoch oft „unnötig groß“. Ist der Kozyklus bereits durch eine exakte Sequenz der Form (44) (S. 59) gegeben, so kann man mit Hilfe des Pullbacks diese Sequenz auf eine Standardform bringen, die denselben Kozyklus induziert. Wir verwenden dazu jeweils ein zu den Konstruktionen aus Abschnitt 2.10 „duales“ Verfahren. Beim ersten Verfahren bilden wir einmal einen Pullback und hängen diesen mittels dessen universeller Eigenschaft an die alte Sequenz an. Bei der zweiten Methode (die wieder nur unter einer Zusatzvoraussetzung funktioniert) bilden wir sukzessive Pullbacks. Der Vorteil dieser Verfahren gegenüber einer Anwendung von Satz 2.13 besteht darin, dass die Moduln in der gegebenen Sequenz vermutlich einfachere Struktur haben als in der bar resolution, und bei den in diesem Abschnitt vorgestellten Verfahren bleibt diese Struktur eher erhalten. Besteht insbesondere eine gegebene Sequenz (44) nur aus endlich-dimensionalen Moduln, so gilt dies auch für die daraus in diesem Abschnitt konstruierten Sequenzen.

Satz 2.18 *Ein n-Kozyklus ($n \geq 1$) werde durch eine exakte Sequenz der Form (44) (S. 59) gegeben (mit vorgegebenem $w \in \operatorname{im}\pi_0 \cap U_{-1}^G$). Sei U_0' der Pullback von π_0 und $\varphi_{-1} : K \to U_{-1},\ \lambda \mapsto \lambda \cdot w$ mit Homomorphismen φ_0 und π_0', und π_1' die nach der universellen Eigenschaft des Pullbacks existierende Abbildung, die folgendes Diagramm kommutativ macht (Details im Beweis):*



Dann ist die nach oben abknickende „Standardsequenz“ exakt und induziert denselben Kozyklus wie die untere exakte Sequenz.

Beweis. Mit der Nullabbildung $0 : U_1 \to K$ gilt $\varphi_{-1} \circ 0 = \pi_0 \circ \pi_1$, und gemäß der universellen Eigenschaft des Pullback gibt es eine Abbildung $\pi_1' : U_1 \to U_0'$, die das Diagramm kommutativ macht. Wir zeigen zunächst, dass die nach oben abknickende Sequenz exakt ist. Nach Definition des Pullbacks ist

$$U_0' = \{(u_0, \lambda) \in U_0 \oplus K : \quad \pi_0(u_0) = \varphi_{-1}(\lambda) = \lambda \cdot w\},$$

und φ_0 bzw. π_0' sind dann die Projektionen auf die erste bzw. zweite Koordinate. Nach Voraussetzung gibt es ein $u_0 \in U_0$ mit $\pi_0(u_0) = w$. Dann ist $u_0' := (u_0, 1) \in U_0'$ und $\pi_0'(u_0') = 1$, also π_0' surjektiv und die abknickende Sequenz an der Stelle K exakt. Aus der Kommutativität des Diagramms folgt $0 = \pi_0' \circ \pi_1'$, also $\operatorname{im}\pi_1' \subseteq \ker\pi_0'$. Ist umgekehrt $(u, \lambda) \in \ker\pi_0' \subseteq U_0'$, also $\lambda = 0$, so folgt aus $\pi_0(u) = \lambda \cdot w = 0$ also $u \in \ker\pi_0 = \operatorname{im}\pi_1$. Also gibt es $u_1 \in U_1$ mit $\pi_1(u_1) = u$. Nach Konstruktion der Abbildung π_1' (siehe der Beweis zu Satz 2.8) gilt dann $\pi_1'(u_1) = (\pi_1(u_1), 0(u_1)) = (u, 0) = (u, \lambda)$, also auch $\ker\pi_0' \subseteq \operatorname{im}\pi_1'$, und wir haben Exaktheit an der Stelle U_0'. Weiter gilt für $u_2 \in U_2$ stets

$\pi_1' \circ \pi_2(u_2) = (\pi_1(\pi_2(u_2)), 0(\pi_2(u_2))) = (0,0)$ (da $\pi_1 \circ \pi_2 = 0$) und damit $\operatorname{im}\pi_2 \subseteq \ker \pi_1'$. Ist umgekehrt $u_1 \in \ker \pi_1'$, also $(\pi_1(u_1), 0) = (0,0)$, so folgt $u_1 \in \ker \pi_1 = \operatorname{im}\pi_2$ und somit auch $\ker \pi_1' \subseteq \operatorname{im}\pi_2$. Dies zeigt Exaktheit an der Stelle U_1, und damit ist die Sequenz insgesamt exakt.

Wir müssen noch zeigen, dass beide Sequenzen den gleichen Kozyklus induzieren. Sei dazu $g_0' \in U_0'$ mit $\pi_0'(g_0') = 1$, $g_1 \in C^1(G, U_1)$ mit $\pi_1' \circ g_1 = \partial_0^{U_0'} g_0'$ und für $k = 2, \ldots, n$ jeweils $g_k \in C^k(G, U_k)$ mit $\pi_k \circ g_k = \partial_{k-1}^{U_{k-1}} g_{k-1}$, d.h. die angegebene Folge erfüllt die Eigenschaft $(*)$ aus Satz 2.2. Dann induziert die nach oben abknickende Sequenz also gemäß Satz 2.2 den Kozyklus $g_n \in Z^n(G, U_n)$. Wir setzen nun $g_0 := \varphi_0(g_0') \in U_0$ und zeigen, dass die Folge der $g_0, \ldots, g_n$ ebenfalls die Eigenschaft $(*)$ aus Satz 2.2 erfüllt. Es gilt $\pi_0(g_0) = \pi_0(\varphi_0(g_0')) = \varphi_{-1}(\pi_0'(g_0')) = \varphi_{-1}(1) = w$ und $\pi_1 \circ g_1 = \varphi_0 \circ \pi_1' \circ g_1 = \varphi_0 \circ \partial_0^{U_0'} g_0' = \partial_0^{U_0}(\varphi_0(g_0')) = \partial_0^{U_0} g_0$. Für die anderen Werte von k gilt $(*)$ sowieso. Also induziert auch die ursprüngliche Sequenz den Kozyklus $g_n \in Z^n(G, U_n)$, und damit beide Sequenzen den gleichen Kozyklus. □

Konstruktion durch sukzessive Pullback-Bildung

Diese alternative Konstruktion kann wieder übersprungen werden.

Wir wollen hier die exakte Standardsequenz mit Hilfe von Korollar 2.9 konstruieren. In der Situation von Satz 2.2 ist dabei $\varphi_{-1} : K \to U_{-1}, \quad \lambda \mapsto \lambda \cdot w$ für $w \neq 0$ ein injektiver KG-Homomorphismus, und dann können wir das Korollar anwenden. Durch sukzessive Pullbackbildung erhält man so das kommutative Diagramm

$$\begin{array}{ccccccccccccc}
0 & \overset{\varepsilon_{n+1}}{\dashrightarrow} & V_n & \overset{\varepsilon_n}{\dashrightarrow} & V_{n-1} & \overset{\varepsilon_{n-1}}{\dashrightarrow} & \cdots & \overset{\varepsilon_2}{\dashrightarrow} & V_1 & \overset{\varepsilon_1}{\dashrightarrow} & V_0 & \overset{\varepsilon_0}{\dashrightarrow} & K & \dashrightarrow & 0 \\
\downarrow{\scriptstyle \varphi_{n+1}} & & \downarrow{\scriptstyle \varphi_n} & & \downarrow{\scriptstyle \varphi_{n-1}} & & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi_{-1}} & & \\
0 & \xrightarrow[\pi_{n+1}]{} & U_n & \xrightarrow[\pi_n]{} & U_{n-1} & \xrightarrow[\pi_{n-1}]{} & \cdots & \xrightarrow[\pi_2]{} & U_1 & \xrightarrow[\pi_1]{} & U_0 & \xrightarrow[\pi_0]{} & U_{-1}. & &
\end{array}$$

Dabei ist V_i für $i = 0, \ldots, n+1$ jeweils Pullback von π_i und φ_{i-1} mit Homomorphismen φ_i und ε_i. Nach dem Korollar sind dann mit φ_{-1} auch die φ_i mit $i = 0, \ldots, n+1$ injektiv und die obere Sequenz exakt (Surjektivität von ε_0 zeigen wir gleich). Aus der Injektivität von $\varphi_{n+1} : V_{n+1} \to 0$ folgt $V_{n+1} = 0$. Sei $g_k \in C^k(G, U_k)$ mit $(*)$ wie in Satz 2.2, also

$$\pi_0(g_0) = w \quad \text{und} \quad \pi_k \circ g_k = \partial_{k-1}^{U_{k-1}} g_{k-1} \quad \text{für } k = 1, \ldots, n. \quad (*)$$

Wir konstruieren $h_k \in C^k(G, V_k),\ k = 0, \ldots, n$ mit der $(*)$ entsprechenden Eigenschaft

$$\varepsilon_0(h_0) = 1 \quad \text{und} \quad \varepsilon_k \circ h_k = \partial_{k-1}^{V_{k-1}} h_{k-1} \quad \text{für } k = 1, \ldots, n, \quad (**)$$

sowie

$$\varphi_k \circ h_k = g_k. \quad (***)$$

Wir setzen zunächst $h_0 := (g_0, 1) \in U_0 \oplus K$. Dann ist $\pi_0(g_0) = w = \varphi_{-1}(1)$, nach Definition des Pullbacks also sogar $h_0 \in V_0 = C^0(G, V_0)$ sowie $\varepsilon_0(h_0) = 1$ und $\varphi_0 \circ h_0 = g_0$. Wegen $\varepsilon_0(h_0) = 1$ ist dann insbesondere auch ε_0 surjektiv, d.h. die obere exakte Sequenz ist tatsächlich von der angegebenen Form. Sei nun $h_0, \ldots, h_{k-1}$ mit $(**)$ und $(***)$ bereits konstruiert. Wir setzen dann

$$h_k := (g_k, \partial_{k-1}^{V_{k-1}} h_{k-1}) \in C^k(G, U_k \oplus V_{k-1}).$$

Da

$$\varphi_{k-1} \circ \partial_{k-1}^{V_{k-1}} h_{k-1} = \partial_{k-1}^{U_{k-1}} (\varphi_{k-1} \circ h_{k-1}) \overset{(***)}{=} \partial_{k-1}^{U_{k-1}} g_{k-1} \overset{(*)}{=} \pi_k \circ g_k,$$

ist sogar $h_k \in C^k(G, V_k)$. Weiter gilt $\varepsilon_k \circ h_k = \partial_{k-1}^{V_{k-1}} h_{k-1}$ und $\varphi_k \circ h_k = g_k$ nach Definition der Homomorphismen des Pullbacks. Dies sind $(**)$ und $(***)$ für k.

Insbesondere gilt dann nach Satz 2.2 $h_n \in Z^n(G, V_n)$, und es ist $g_n = \varphi_n \circ h_n$ mit einer injektiven Abbildung φ_n. Falls $\langle g_n(G^n) \rangle_{KG} = U_n$, so ist φ_n sogar surjektiv, also $U_n \cong V_n$.

In diesem Fall induziert die obere Sequenz also (bis auf Isomorphie) den Kozyklus g_n.

Ist φ_n nicht surjektiv, so kann man noch Satz 2.11 anwenden, um eine Sequenz zu erhalten, die mit U_n endet und $g_n = \varphi_n \circ h_n \in Z^n(G, U_n)$ induziert.

2.12 Äquivalenz von Sequenzen

Dieser Abschnitt dient nur der Vollständigkeit und kann übersprungen werden.

Ein Element $g_n \in H^n(G, U_n)$ kann offenbar durch viele verschiedene, auf U_n endende exakte Sequenzen der Länge n in Standardform (45) induziert werden.

Definition 2.19 *Wir nennen zwei exakte Sequenzen der Länge $n \geq 1$ in Standardform*

$$E_1 : \quad 0 \to U_n \overset{\pi_n}{\to} U_{n-1} \overset{\pi_{n-1}}{\to} U_{n-2} \overset{\pi_{n-2}}{\to} \dots \overset{\pi_1}{\to} U_0 \overset{\pi_0}{\to} K \to 0 \tag{64}$$

und

$$E_2 : \quad 0 \to U_n \overset{\pi'_n}{\to} U'_{n-1} \overset{\pi'_{n-1}}{\to} U'_{n-2} \overset{\pi'_{n-2}}{\to} \dots \overset{\pi'_1}{\to} U'_0 \overset{\pi'_0}{\to} K \to 0 \tag{65}$$

mit gleichem Ende U_n äquivalent*, in Zeichen $E_1 \sim E_2$, wenn sie die gleiche Restklasse $g_n + B^n(G, U_n) \in H^n(G, U_n)$ induzieren.*

Die so definierte Äquivalenz ist offenbar symmetrisch, reflexiv und transitiv. Obwohl die Gesamtheit der zugrundeliegenden Objekte keine Menge sondern eine „Klasse“ bildet, wollen wir bei einer Relation mit diesen drei Eigenschaften von einer *Äquivalenzrelation* sprechen.

Ziel dieses Abschnitts ist es, die Äquivalenz von Sequenzen in Standardform mit gleichem Ende U_n auf eine weitere Art zu charakterisieren.

Definition 2.20 *Zwei exakte Sequenzen* (64), (65) *der Länge $n \geq 1$ in Standardform mit gleichem Ende U_n heißen* Yoneda-prääquivalent*, in Zeichen $E_1 \sim_{pY} E_2$, , wenn es für $k = 0, \dots, n-1$ KG-Homomorphismen $\varphi_k : U_k \to U'_k$ gibt, so dass folgendes Diagramm kommutativ wird:*

$$\begin{array}{lccccccccccccc}
E_1 : & 0 & \longrightarrow & U_n & \xrightarrow{\pi_n} & U_{n-1} & \xrightarrow{\pi_{n-1}} & \cdots & \xrightarrow{\pi_2} & U_1 & \xrightarrow{\pi_1} & U_0 & \xrightarrow{\pi_0} & K & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle \mathrm{id}_{U_n}} & & \downarrow{\scriptstyle \varphi_{n-1}} & & & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \mathrm{id}_K} & & \\
E_2 : & 0 & \longrightarrow & U_n & \xrightarrow[\pi'_n]{} & U'_{n-1} & \xrightarrow[\pi'_{n-1}]{} & \cdots & \xrightarrow[\pi'_2]{} & U'_1 & \xrightarrow[\pi'_1]{} & U'_0 & \xrightarrow[\pi'_0]{} & K & \longrightarrow & 0.
\end{array}$$

Die Yoneda-Prääquivalenz ist offenbar reflexiv und transitiv, im Allgemeinen aber nicht symmetrisch.

Lemma 2.21 *Sind zwei exakte Sequenzen* (64), (65) *der Länge $n \geq 1$ in Standardform mit gleichem Ende U_n Yoneda-prääquivalent, also $E_1 \sim_{pY} E_2$, so sind sie auch äquivalent, also $E_1 \sim E_2$.*

Beweis. Wir verwenden die Bezeichnungen von Definition 2.20. Sei $g_k \in C^k(G, U_k)$ für $k = 0, \ldots, n$ eine Folge mit $(*)$ aus Definition 2.2, also

$$\pi_0(g_0) = 1 \quad \text{und} \quad \pi_k \circ g_k = \partial_{k-1}^{U_{k-1}} g_{k-1} \quad \text{für } k = 1, \ldots, n, \quad (*)$$

d.h. E_1 induziert $g_n \in Z^n(G, U_n)$. Wir setzen zusätzlich $\varphi_n := \mathrm{id}_{U_n}$ und $g'_k := \varphi_k \circ g_k \in C^k(G, U'_k)$ für $k = 0, \ldots, n$ und zeigen, dass die Folge der (g'_k) die $(*)$ entsprechende Eigenschaft erfüllt. Dann induziert E_2 ebenfalls den Kozyklus $g'_n = g_n \in Z^n(G, U_n)$, und damit gilt dann $E_1 \sim E_2$. Aus der Kommutativität des Diagramms folgt

$$\pi'_0(g'_0) = \pi'_0(\varphi_0(g_0)) = \mathrm{id}_K(\pi_0(g_0)) \overset{(*)}{=} 1$$

sowie

$$\begin{aligned} \pi'_k \circ g'_k &= \pi'_k \circ \varphi_k \circ g_k = \varphi_{k-1} \circ \pi_k \circ g_k \overset{(*)}{=} \varphi_{k-1} \circ \partial_{k-1}^{U_{k-1}} g_{k-1} \\ &= \partial_{k-1}^{U'_{k-1}}(\varphi_{k-1} \circ g_{k-1}) = \partial_{k-1}^{U'_{k-1}} g'_{k-1} \quad \text{für alle } k = 1, \ldots, n, \end{aligned}$$

und dies ist $(*)$ für die Folge (g'_k). □

Definition 2.22 *Zwei exakte Sequenzen E, E' in Standardform mit gleichem Ende U_n ($n \geq 1$) heißen* Yoneda-äquivalent, *in Zeichen $E \sim_Y E'$, wenn es eine Zahl $m \geq 0$ und exakte Sequenzen $E_1, \ldots, E_m$ der Länge n in Standardform mit gleichem Ende U_n gibt, so dass für die Folge $E_0 := E, E_1, E_2, \ldots, E_m, E_{m+1} := E'$ gilt: Für jedes $k = 0, \ldots, m$ gilt $E_k \sim_{pY} E_{k+1}$ oder $E_{k+1} \sim_{pY} E_k$, d.h. je zwei benachbarte Glieder sind evtl. nach Vertauschen Yoneda-präääquivalent.*

Satz 2.23 *Zwei exakte Sequenzen E, E' in Standardform mit gleichem Ende U_n ($n \geq 1$) sind genau dann äquivalent, wenn sie Yoneda-äquivalent sind, also*

$$E \sim E' \quad \Leftrightarrow \quad E \sim_Y E'.$$

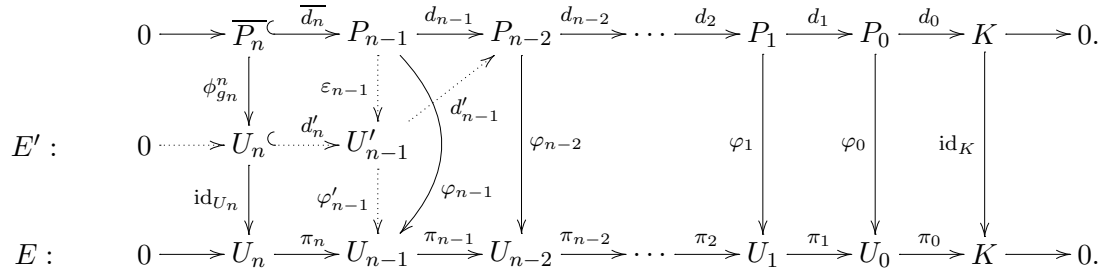
Insbesondere ist die Yoneda-Äquivalenz eine Äquivalenzrelation.

Beweis. Sei zunächst $E \sim_Y E'$, d.h. es gibt exakte Sequenzen $E_1, \ldots, E_m$ wie in Definition 2.22. Wir setzen wieder $E_0 := E$, $E_{m+1} := E'$. Nach Lemma 2.21 und weil $\sim$ symmetrisch ist, gilt dann $E_k \sim E_{k+1}$ für $k = 0, \ldots, m$, und da $\sim$ eine Äquivalenzrelation ist gilt dann auch $E \sim E'$.

Sei umgekehrt $E \sim E'$, d.h. E und E' induzieren dieselbe Restklasse $g_n + B^n(G, U_n) \in H^n(G, U_n)$. Nach Satz 2.2 induzieren beide Sequenzen dann auch jeden Repräsentanten dieser Restklasse, d.h. beide Sequenzen induzieren insbesondere auch $g_n \in Z^n(G, U_n)$. Im nächsten Lemma zeigen wir, dass es eine nur von U_n und $g_n \in Z^n(G, U_n)$ abhängige Sequenz E_1 gibt mit $E_1 \sim_{pY} E$ und $E_1 \sim_{pY} E'$. Nach Definition 2.22 (mit $m = 1$) gilt dann $E \sim_Y E'$. □

Lemma 2.24 *Sei $n \geq 1$ und E eine exakte Sequenz der Länge n in Standardform mit Ende U_n, die den Kozyklus $g_n \in Z^n(G, U_n)$ induziert. Sei weiter E' die in Satz 2.13 aus g_n und U_n konstruierte nach unten abknickende exakte Sequenz, die ebenfalls g_n induziert. Dann gilt $E' \sim_{pY} E$.*

Beweis. Sei E gegeben wie in Gleichung (64). Wir betrachten das folgende Diagramm, dessen oberen beiden Zeilen sich gemäß der Konstruktion aus Satz 2.13 aus g_n und U_n ergeben. Die dritte Zeile ist die gegebene Sequenz E.



Sei weiter $g_k \in C^k(G, U_k)$ für $k = 0, \ldots, n$ mit der $(*)$ entsprechenden Eigenschaft aus Satz 2.2, also

$$\pi_0(g_0) = 1 \quad \text{und} \quad \pi_k \circ g_k = \partial_{k-1}^{U_{k-1}} g_{k-1} \ \text{ für } k = 1, \ldots, n. \quad (*)$$

Wir verwenden wieder die Notation aus Abschnitt 2.3, und gemäß Gleichung (37) (S. 55) definieren wir

$$\varphi_k := \omega_k^{U_k}(g_k) \quad \text{für } k = 0, \ldots, n.$$

Mit $e_k \in C^k(G, P_k)$ wie in (38) gilt dann

$$\begin{aligned} \pi_0(\varphi_0(e_0)) &= \pi_0(\omega_0^{U_0}(g_0) \circ e_0) \overset{(39)}{=} \pi_0(g_0) \overset{(*)}{=} 1 \\ &\overset{(35),S.55}{=} \mathrm{id}_K(d_0(e_0)) \end{aligned}$$

und

$$\begin{aligned} \pi_k \circ \varphi_k \circ e_k &= \pi_k \circ \omega_k^{U_k}(g_k) \circ e_k \overset{(39)}{=} \pi_k \circ g_k \overset{(*)}{=} \partial_{k-1}^{U_{k-1}} g_{k-1} && (66) \\ &\overset{(39)}{=} \partial_{k-1}^{U_{k-1}}(\omega_{k-1}^{U_{k-1}}(g_{k-1}) \circ e_{k-1}) = \partial_{k-1}^{U_{k-1}}(\varphi_{k-1} \circ e_{k-1}) && (67) \\ &= \varphi_{k-1} \circ \partial_{k-1}^{P_{k-1}} e_{k-1} \overset{(47),S.68}{=} \varphi_{k-1} \circ d_k \circ e_k \quad \text{für } k = 1, \ldots, n. && (68) \end{aligned}$$

Da die Bilder $e_k(G^k)$ jeweils P_k als KG-Modul erzeugen und alle betrachteten Abbildungen KG-linear sind, gilt also

$$\pi_0 \circ \varphi_0 = \mathrm{id}_K \circ d_0 \quad \text{und} \quad \pi_k \circ \varphi_k = \varphi_{k-1} \circ d_k \ \text{ für } k = 1, \ldots, n, \quad (69)$$

insbesondere kommutiert das Diagramm „rechtsseitig“ der Abbildung φ_{n-1}. Weiter gilt mit $\overline{e_n}$ wie in (50), S. 69

$$\begin{aligned} \pi_n \circ \phi^n_{g_n} \circ \overline{e_n} &\overset{\text{Satz 2.12}}{=} \pi_n \circ g_n \overset{(66),\,(68)}{=} \varphi_{n-1} \circ d_n \circ e_n \\ &\overset{(53),S.69}{=} \varphi_{n-1} \circ \overline{d_n} \circ \overline{e_n}, \end{aligned}$$

und da $\overline{e_n}(G^n)$ den KG-Modul $\overline{P_n}$ erzeugt, also

$$\pi_n \circ \phi^n_{g_n} = \varphi_{n-1} \circ \overline{d_n}.$$

Da U'_{n-1} als Pushout von $\phi^n_{g_n}$ und $\overline{d_n}$ definiert ist, liefert dessen universelle Eigenschaft also eine Abbildung $\varphi'_{n-1} : U'_{n-1} \to U_{n-1}$ mit

$$\varphi'_{n-1} \circ d'_n = \pi_n = \pi_n \circ \mathrm{id}_{U_n}, \tag{70}$$

also Kommutativität des Diagramms „links unten“, und

$$\varphi'_{n-1} \circ \varepsilon_{n-1} = \varphi_{n-1}. \tag{71}$$

Da wir in Satz 2.13 d'_{n-1} ebenfalls aus der universellen Eigenschaft des Pushouts erhalten haben, gilt ausserdem

$$d'_{n-1} \circ \varepsilon_{n-1} = d_{n-1}. \tag{72}$$

Wir müssen als letztes noch die Kommutatvität des „Trapezes“ zeigen, nämlich $\pi_{n-1} \circ \varphi'_{n-1} = \varphi_{n-2} \circ d'_{n-1}$. Sei dazu $y \in U'_{n-1}$ beliebig. Nach Konstruktion des Pushouts (siehe Definition 2.5) gilt $U'_{n-1} = d'_n(U_n) + \varepsilon_{n-1}(P_{n-1})$, d.h. zu y gibt es $u \in U_n$, $x \in P_{n-1}$ mit

$$y = d'_n(u) + \varepsilon_{n-1}(x). \tag{73}$$

Dann gilt

$$\begin{aligned}
\pi_{n-1} \circ \varphi'_{n-1}(y) &\overset{(73)}{=} \pi_{n-1} \circ \varphi'_{n-1}(d'_n(u) + \varepsilon_{n-1}(x)) \\
&\overset{(70),\ (71)}{=} \pi_{n-1} \circ \pi_n(u) + \pi_{n-1} \circ \varphi_{n-1}(x) \\
&\overset{\pi_{n-1}\circ\pi_n=0,\ (69)}{=} \varphi_{n-2} \circ d_{n-1}(x) \\
&\overset{(72)}{=} \varphi_{n-2} \circ d'_{n-1} \circ \varepsilon_{n-1}(x) \\
&\overset{d'_{n-1}\circ d'_n=0}{=} \varphi_{n-2} \circ d'_{n-1}(d'_n(u) + \varepsilon_{n-1}(x)) \\
&\overset{(73)}{=} \varphi_{n-2} \circ d'_{n-1}(y)
\end{aligned}$$

für alle $y \in U'_{n-1}$, d.h. $\pi_{n-1} \circ \varphi'_{n-1} = \varphi_{n-2} \circ d'_{n-1}$. Also kommutiert das gesamte Diagramm, und damit gilt $E' \sim_{pY} E$ nach Definition 2.20. □

Beispiel 2.25 Wir wollen die (Yoneda-)Äquivalenz für den Fall $n = 1$ untersuchen und zeigen, dass sie hier mit der Yoneda-Prääquivalenz übereinstimmt, dass hier also insbesondere bereits die Yoneda-Prääquivalenz eine Äquivalenzrelation ist. Wir betrachten dazu zwei Yoneda-prääquivalente exakte Sequenzen $E \sim_{pY} E'$, haben also ein kommutatives Diagramm

$$\begin{array}{lccccccccc}
E: & 0 & \longrightarrow & U_1 & \xrightarrow{\pi_1} & U_0 & \xrightarrow{\pi_0} & K & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle \mathrm{id}_{U_1}} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \mathrm{id}_K} & & \\
E': & 0 & \longrightarrow & U_1 & \xrightarrow[\pi'_1]{} & U'_0 & \xrightarrow[\pi'_0]{} & K & \longrightarrow & 0.
\end{array}$$

Wir zeigen, dass dann φ_0 ein Isomorphismus ist, woraus dann auch $E' \sim_{pY} E$ folgt. Sei $u_0 \in \ker \varphi_0$. Dann ist $0 = \pi'_0(\varphi_0(u_0)) = \mathrm{id}_K(\pi_0(u_0))$, also $u_0 \in \ker \pi_0 = \operatorname{im} \pi_1$. Dann gibt es $u_1 \in U_1$ mit $u_0 = \pi_1(u_1)$. Es folgt $0 = \varphi_0(u_0) = \varphi_0(\pi_1(u_1)) = \pi'_1(\mathrm{id}_{U_1}(u_1))$. Da

π_1' injektiv ist, folgt $u_1 = 0$ und damit $u_0 = \pi_1(u_1) = 0$, also $\ker \varphi_0 = 0$ und φ_0 ist injektiv. Zum Beweis der Surjektivität von φ_0 sei $u_0' \in U_0'$. Da π_0 surjektiv ist, gibt es dann $u_0 \in U_0$ mit $\pi_0(u_0) = \pi_0'(u_0')$. Dann ist $\pi_0'(u_0' - \varphi_0(u_0)) = \pi_0'(u_0') - \pi_0(u_0) = 0$, also $u_0' - \varphi_0(u_0) \in \ker \pi_0' = \operatorname{im} \pi_1'$. Es gibt also $u_1' \in U_1$ mit $\pi_1'(u_1') = u_0' - \varphi_0(u_0)$. Es folgt $\varphi_0(u_0 + \pi_1(u_1')) = \varphi_0(u_0) + \pi_1'(u_1') = u_0'$, also die Surjektivität von φ_0.

Im Fall $n = 1$ gibt es also zu jedem Kozyklus im Wesentlichen nur eine exakte Sequenz, die diesen induziert.

Bemerkung 2.26 Aus Satz 2.2, Beispiel 2.14 und Satz 2.23 folgt: Ein von einer exakten Sequenz mit Ende U_n induzierter Kozyklus ist genau dann trivial, wenn die exakte Sequenz (Yoneda-)äquivalent ist zu einer exakten Sequenz $0 \to U_n \xrightarrow{\pi_n} U_{n-1} \to \ldots$, für die ein links-Splitting $\mu_n : U_{n-1} \to U_n$ mit $\mu_n \circ \pi_n = \mathrm{id}_{U_n}$ existiert. Im Fall $n = 1$ folgt aus Beispiel 2.25, dass dies genau dann der Fall ist, wenn für eine beliebige (und dann jede) den Kozyklus induzierende Sequenz ein solches Splitting existiert.

2.13 Annullation von n-Kozyklen

Sind V, W jeweils KG-Moduln und $g \in C^n(G, V)$ sowie $\varphi \in (W^*)^G$, so schreiben wir $\varphi \cdot g \in C^n(G, \mathrm{Hom}_K(W, V))$ für die Abbildung $G^n \to \mathrm{Hom}_K(W, V)$, $x \mapsto \varphi \cdot g(x)$ mit $\varphi \cdot g(x) : W \to V$, $w \mapsto \varphi(w)g(x)$. Ist $g \in Z^n(G, V)$, also $\partial_n^V g = 0$, so folgt wegen $\varphi \in (W^*)^G$ dann auch $\partial_n^{\mathrm{Hom}_K(W,V)}(\varphi \cdot g) = 0$, also $\varphi \cdot g \in Z^n(G, \mathrm{Hom}_K(W, V))$. Ist $g \in B^n(G, V)$, also $g = \partial_{n-1}^V f$ mit $f \in C^{n-1}(G, V)$, so gilt entsprechend auch $\varphi \cdot g = \varphi \cdot \partial_{n-1}^V f = \partial_{n-1}^{\mathrm{Hom}_K(W,V)}(\varphi \cdot f) \in B^n(G, \mathrm{Hom}_K(W, V))$. Die Multiplikation mit φ induziert also eine Abbildung $H^n(G, V) \to H^n(G, \mathrm{Hom}_K(W, V))$. Unter anderem werden wir in diesem Abschnitt zeigen, dass die *Augmentationsabbildung* $d_0 \in (KG)^*$, $\sum_{\sigma \in G} \lambda_\sigma \cdot \sigma \mapsto \sum_{\sigma \in G} \lambda_\sigma$ (wobei nur endlich viele $\lambda_\sigma \in K$ ungleich 0 sind) stets die Nullabbildung induziert.

Ist W *endlich-dimensional*, so gilt bekanntlich die Isomorphie $W^* \otimes_K V \cong \mathrm{Hom}_K(W, V)$, gegeben durch lineare Fortsetzung von $\varphi \otimes v \to \varphi \cdot v$. Entsprechend ist dann $\varphi \otimes g \in Z^n(G, W^* \otimes_K V)$ definiert.

Sind U, V, W jeweils KG-Moduln und $\psi \in \mathrm{Hom}_G(U, V)$ (also $\psi \circ \sigma = \sigma \circ \psi$ für alle $\sigma \in G$), so ist die Abbildung $\psi_* : \mathrm{Hom}_K(W, U) \to \mathrm{Hom}_K(W, V)$, $f \mapsto \psi \circ f$ ein Element aus $\mathrm{Hom}_G(\mathrm{Hom}_K(W, U), \mathrm{Hom}_K(W, V))$. Denn für $\sigma \in G$, $f \in \mathrm{Hom}_K(W, U)$ gilt $\psi_*(\sigma \cdot f) = \psi \circ \sigma \circ f \circ \sigma^{-1} = \sigma \circ \psi \circ f \circ \sigma^{-1} = \sigma \cdot \psi_*(f)$. Das folgende Lemma ist dann wohlbekannt.

Lemma 2.27 *Sind A, B, C, W jeweils KG-Moduln und ist*

$$A \xrightarrow{\varepsilon} B \xrightarrow{\pi} C$$

eine exakte Sequenz von KG-Moduln, so ist auch

$$\mathrm{Hom}_K(W, A) \xrightarrow{\varepsilon_*} \mathrm{Hom}_K(W, B) \xrightarrow{\pi_*} \mathrm{Hom}_K(W, C)$$

eine exakte Sequenz von KG-Moduln.

Beweis. (Der Vollständigkeit halber.) Für $f \in \mathrm{Hom}_K(W, A)$ gilt $\pi_* \circ \varepsilon_*(f) = \pi \circ \varepsilon \circ f = 0$, da $\pi \circ \varepsilon = 0$, also $\operatorname{im} \varepsilon_* \subseteq \ker \pi_*$. Sei umgekehrt $g \in \ker \pi_*$, also $\pi \circ g = 0$. Dann ist $\operatorname{im} g \subseteq \ker \pi = \operatorname{im} \varepsilon$. Da wir von Vektorräumen sprechen, gibt es dann ein $f \in \mathrm{Hom}_K(W, A)$

mit $g = \varepsilon \circ f = \varepsilon_*(f) \in \operatorname{im} \varepsilon_*$, also auch $\ker \pi_* \subseteq \operatorname{im} \varepsilon_*$. □

Wir kommen zu der angekündigten Verallgemeinerung von Proposition 1.51, dem eigentlichen Ziel und Hauptresultat dieses Abschnitts über Kohomologie von Gruppen.

Satz 2.28 *Sei $n \geq 1$ und*

$$0 \longrightarrow U_n \xrightarrow{\pi_n} U_{n-1} \xrightarrow{\pi_{n-1}} U_{n-2} \xrightarrow{\pi_{n-2}} \cdots \xrightarrow{\pi_3} U_2 \xrightarrow{\pi_2} U_1 \xrightarrow{\pi_1} U_0 \xrightarrow{\pi_0} K \longrightarrow 0$$

eine exakte Sequenz von G-Moduln, die einen Kozyklus $g \in Z^n(G, U_n)$ induziert. Dann ist $\pi_0 \in (U_0^*)^G$, und es gilt $\pi_0 \cdot g \in B^n(G, \operatorname{Hom}_K(U_0, U_n))$. Anders fomuliert: $\pi_0 \cdot g = 0 \in H^n(G, \operatorname{Hom}_K(U_0, U_n))$, d.h. die Restklasse von g in $H^n(G, U_n)$ wird von π_0 annulliert.

Falls $\dim_K U_0 < \infty$, so gilt entsprechend $\pi_0 \otimes g \in B^n(G, U_0^* \otimes_K U_n)$,

Beweis. Da π_0 ein G-Homomorphimsmus ist, ist $\pi_0 \in (U_0^*)^G$. Sei $g_n := g$ und $g_k \in C^k(G, U_k)$ für $k = 0, \ldots, n$ die zugehörige g induzierende Folge mit $(*)$ wie in Satz/Definition 2.2, d.h.

$$\pi_0(g_0) = 1 \quad \text{und} \quad \pi_k \circ g_k = \partial_{k-1}^{U_{k-1}} g_{k-1} \quad \text{für } k = 1, \ldots, n. \quad (*)$$

Wir wenden nun auf die exakte Sequenz den „Funktor“ $\operatorname{Hom}_K(U_0, \cdot)$ an und erhalten so die nach dem Lemma ebenfalls exakte Sequenz

$$0 \longrightarrow \operatorname{Hom}_K(U_0, U_n) \xrightarrow{\pi_{n*}} \operatorname{Hom}_K(U_0, U_{n-1}) \xrightarrow{\pi_{n-1*}} \operatorname{Hom}_K(U_0, U_{n-2}) \xrightarrow{\pi_{n-2*}} \cdots\cdots\cdots$$

$$\cdots \xrightarrow{\pi_{3*}} \operatorname{Hom}_K(U_0, U_2) \xrightarrow{\pi_{2*}} \operatorname{Hom}_K(U_0, U_1) \xrightarrow{\pi_{1*}} \operatorname{Hom}_K(U_0, U_0) \xrightarrow{\pi_{0*}} \operatorname{Hom}_K(U_0, K) \quad (**)$$

mit π_{k*} definiert wie oben durch Verkettung mit π_k. Für die Folge der

$$\pi_0 \cdot g_k \in C^k(G, \operatorname{Hom}_K(U_0, U_k)) \quad \text{mit} \quad k = 0, \ldots, n$$

gilt dann offenbar

$$\pi_{0*}(\pi_0 \cdot g_0) = \pi_0 \cdot \pi_0(g_0) \overset{(*)}{=} \pi_0 \cdot 1 = \pi_0$$

und

$$\begin{aligned} \pi_{k*} \circ (\pi_0 \cdot g_k) &= \pi_0 \cdot (\pi_k \circ g_k) \overset{(*)}{=} \pi_0 \cdot \partial_{k-1}^{U_{k-1}} g_{k-1} \\ &= \partial_{k-1}^{\operatorname{Hom}_K(U_0, U_{k-1})}(\pi_0 \cdot g_{k-1}) \quad \text{für alle } k = 1, \ldots, n. \end{aligned}$$

Dies ist die Eigenschaft $(*)$ von Satz/Definition 2.2 für die exakte Sequenz $(**)$ (mit $w := \pi_0 \cdot 1 \in \operatorname{Hom}_K(U_0, K)^G$), und damit induziert die exakte Sequenz $(**)$ den n-Kozyklus $\pi_0 \cdot g_n \in Z^n(G, \operatorname{Hom}_K(U_0, U_n))$.

Wir betrachten nun $\mathrm{id}_{U_0} \in \operatorname{Hom}_K(U_0, U_0)^G$. Es gilt $\pi_{0*}(\mathrm{id}_{U_0}) = \pi_0 \circ \mathrm{id}_{U_0} = \pi_0 = \pi_0 \cdot 1$. Nach Satz/Definition 2.2 (mit $v = \mathrm{id}_{U_0}$) ist also $\pi_0 \cdot g_n \in B^n(G, \operatorname{Hom}_K(U_0, U_n))$.

Der Zusatz für $\dim_K U_0 < \infty$ folgt nun aus der Isomorphie $\operatorname{Hom}_K(U_0, U_n) \cong U_0^* \otimes_K U_n$. □

Im Falle $n = 1$ und eines Kozyklus $g \in Z^1(G, U)$ mit $\dim_K U < \infty$, der von einer kurzen exakten Sequenz

$$0 \to U \hookrightarrow \tilde{U} \xrightarrow{\pi} K \to 0$$

induziert wird (siehe Beispiel 2.15), liefert der Satz $\pi \otimes g \in B^1(G, \tilde{U}^* \otimes_K U)$. Mit der in Bemerkung 2.3 beschriebenen Konstruktion ergibt sich auch die Formel (20) (S. 36). Wir erhalten also Proposition 1.51 zurück.

Korollar 2.29 *Sei G eine beliebige Gruppe und*

$$d_0 : KG \to K, \quad \sum_{\sigma \in G} \lambda_\sigma \cdot \sigma \mapsto \sum_{\sigma \in G} \lambda_\sigma$$

(mit nur endlich vielen $\lambda_\sigma \in K$ ungleich 0) die Augmentationsabbildung. *Dann annulliert d_0 jeden Kozyklus eines jeden G-Moduls U, d.h. für alle $g \in Z^n(G,U)$ ($n \geq 1$) gilt $d_0 \cdot g \in B^n(G, \mathrm{Hom}_K(KG,U))$.*

Beweis. Sei zunächst $n \geq 2$ und $U_n := U$. Nach Satz 2.13 wird $g \in Z^n(G,U_n)$ von einer exakten Sequenz der Form

$$0 \longrightarrow U_n \xrightarrow{d'_n} U_{n-1} \xrightarrow{d'_{n-1}} P_{n-2} \xrightarrow{d_{n-2}} \cdots \xrightarrow{d_1} KG \xrightarrow{d_0} K \longrightarrow 0$$

induziert, die also „auf die bar resolution endet“ (da $n \geq 2$, kommt $P_0 = KG$ tatsächlich vor). Nach Satz 2.28 gilt also $d_0 \cdot g \in B^n(G, \mathrm{Hom}_K(KG,U))$.

Es bleibt der Fall $n = 1$. Wir erledigen ihn durch explizite Rechnung. Sei also $g \in Z^1(G,U)$. Wir definieren dazu $f \in \mathrm{Hom}_K(KG,U)$ durch K-lineare Fortsetzung von

$$G \to U, \quad \tau \mapsto -g_\tau$$

(G ist K-Basis von KG). Wir berechnen nun

$$\partial_0^{\mathrm{Hom}_K(KG,U)} f(\sigma) = (\sigma - 1)f = \sigma \circ f \circ \sigma^{-1} - f \in \mathrm{Hom}_K(KG,U),$$

indem wir die Bilder dieser Abbildung auf der Basis G von KG angeben. Für $\tau \in G$ gilt

$$\begin{aligned} ((\partial_0 f)(\sigma))(\tau) &= (\sigma \circ f \circ \sigma^{-1})(\tau) - f(\tau) = \sigma(-g_{\sigma^{-1}\tau}) + g_\tau \\ &= -(\sigma g_{(\sigma^{-1}\tau)} + g_\sigma - g_\sigma) + g_\tau \\ &= -g_{\sigma(\sigma^{-1}\tau)} + g_\sigma + g_\tau = g_\sigma = (d_0 \cdot g_\sigma)(\tau), \end{aligned}$$

wobei wir die Kozyklus Eigenschaft von g verwendet haben. Also gilt $\partial_0 f(\sigma) = d_0 \cdot g_\sigma$ oder $d_0 \cdot g = \partial_0 f \in B^1(G, \mathrm{Hom}_K(KG,U))$. □

Wir geben noch einen

2. Beweis. Wir betrachten den generischen n-Kozyklus $\overline{e_n} \in Z^n(G, \overline{P_n})$ (50), S. 69. Er wird induziert von der exakten Sequenz (52), und nach Satz 2.28 gilt also $d_0 \cdot \overline{e_n} \in B^n(G, \mathrm{Hom}_K(KG, \overline{P_n}))$, d.h. es gibt $f_{n-1} \in C^{n-1}(G, \mathrm{Hom}_K(KG, \overline{P_n}))$ mit

$$d_0 \cdot \overline{e_n} = \partial_{n-1}^{\mathrm{Hom}_K(KG, \overline{P_n})} f_{n-1}. \tag{74}$$

Sei nun $g_n \in Z^n(G,U_n)$ mit einem G-Modul U_n. Wir betrachten die Abbildung $\phi^n_{g_n} \in \mathrm{Hom}_{KG}(\overline{P_n}, U_n)$ aus Satz 2.12 mit

$$g_n = \phi^n_{g_n} \circ \overline{e_n}. \tag{75}$$

Wie wir in der Diskussion am Anfang dieses Abschnitts gesehen haben, ist dann die Abbildung

$$(\phi^n_{g_n})_* : \mathrm{Hom}_K(KG, \overline{P_n}) \to \mathrm{Hom}_K(KG, U_n), \quad \psi \mapsto (\phi^n_{g_n})_*(\psi) = \phi^n_{g_n} \circ \psi$$

ebenfalls ein KG-Homomorphismus, also

$$(\phi^n_{g_n})_* \in \mathrm{Hom}_{KG}(\mathrm{Hom}_K(KG, \overline{P_n}), \mathrm{Hom}_K(KG, U_n)). \tag{76}$$

Damit erhalten wir

$$\begin{aligned} d_0 \cdot g_n &\overset{(75)}{=} d_0 \cdot (\phi^n_{g_n} \circ \overline{e_n}) = (\phi^n_{g_n})_* \circ (d_0 \cdot \overline{e_n}) \\ &\overset{(74)}{=} (\phi^n_{g_n})_* \circ \partial_{n-1}^{\mathrm{Hom}_K(KG, \overline{P_n})} f_{n-1} \\ &\overset{(76)}{=} \partial_{n-1}^{\mathrm{Hom}_K(KG, U_n)}((\phi^n_{g_n})_* \circ f_{n-1}) \end{aligned}$$

mit $(\phi^n_{g_n})_* \circ f_{n-1} \in C^{n-1}(G, \mathrm{Hom}_K(KG, U_n))$, also $d_0 \cdot g_n \in B^n(G, \mathrm{Hom}_K(KG, U_n))$. □

Bemerkung 2.30 Ist $|G| < \infty$, so ist KG selbstdual als G-Modul. Ist nämlich $\delta_\tau \in \mathrm{Hom}_K(KG, K)$ für $\tau \in G$ gegeben durch K-lineare Fortsetzung von

$$\delta_\tau(\sigma) = \begin{cases} 1 & \text{für } \sigma = \tau \\ 0 & \text{sonst,} \end{cases}$$

so bilden die δ_τ eine Basis von $(KG)^* = \mathrm{Hom}_K(KG, K)$. Ferner ist durch K-lineare Fortsetzung von $\tau \mapsto \delta_\tau$ ein G-Isomorphismus $KG \to (KG)^*$ gegeben, denn für $\sigma \in G$ gilt $\sigma \cdot \delta_\tau = \delta_\tau \circ \sigma^{-1} = \delta_{\sigma\tau}$. Die Augmentationsabbildung $d_0 = \sum_{\sigma \in G} \delta_\sigma \in \mathrm{Hom}_K(KG, K)$ entspricht also der „Spur“ $\pi := \sum_{\sigma \in G} \sigma \in KG$. Da $\dim_K KG < \infty$, also $\mathrm{Hom}_K(KG, U) \cong (KG)^* \otimes_K U \cong KG \otimes_K U$ für jeden G-Modul U gilt, haben wir also mit dem Korollar für jedes $g \in Z^n(G, U)$, dass $\pi \otimes g \in B^n(G, KG \otimes_K U)$. Dieses Resultat über die Annullation von Kozyklen endlicher Gruppen ist bekannt, siehe etwa Kemper [32, Lemma 1.7] oder [34, Proposition 2.3].

Wir geben noch ein letztes Beispiel.

Beispiel 2.31 Wir greifen Beispiel 2.4 wieder auf, also den von der exakten Sequenz

$$0 \to K \xrightarrow{\pi_2} K^2 \xrightarrow{\pi_1} K^2 \xrightarrow{\pi_0} K \to 0$$

induzierten 2-Kozyklus $g \in Z^2(\mathbb{G}_a, K)$ mit $g(a, b) = ab$ für alle $a, b \in \mathbb{G}_a$. Für $\mathrm{char}\, K = 2$ ist g nichttrivial, aber nach dem Satz gilt $\pi_0 \otimes g \in B^2(\mathbb{G}_a, (K^2)^* \otimes_K K)$. Tatsächlich kann $\pi_0 \otimes g$ mit $h \in Z^2(\mathbb{G}_a, K^2)$ mit $h(a, b) = (ab, 0)$ für alle $a, b \in \mathbb{G}_a$ identifiziert werden, und dann ist $h = \partial_1 f$, mit $f \in C^1(\mathbb{G}_a, K^2)$ gegeben durch $f(a) = (0, a)$ für alle $a \in \mathbb{G}_a$ - also wie vom Satz behauptet $h \in B^2(\mathbb{G}_a, K^2)$.

3 Folgen von Invariantenringen mit unbeschränkt wachsendem Cohen-Macaulay-Defekt

In diesem Abschnitt behandeln wir eines der Hauptresultate dieser Arbeit - insbesondere werden wir für jede reduktive, nicht linear reduktive Gruppe G einen G-Modul V konstruieren mit $\lim_{k\to\infty} \operatorname{cmdef} K[\bigoplus_{i=1}^{k} V]^G = \infty$.

Im folgenden Lemma ist G eine beliebige (nicht notwendig reduktive) lineare algebraische Gruppe.

Lemma 3.1 *Homogene Elemente $a_1, a_2 \in K[V]_+$ bilden genau dann ein phsop in $K[V]$, wenn sie teilerfremd sind, was genau dann der Fall ist, wenn sie eine reguläre Sequenz in $K[V]$ bilden.*

Gilt dann zusätzlich $a_1, a_2 \in K[V]^G$, so bilden sie auch eine reguläre Sequenz in $K[V]^G$ (und dann dort auch ein phsop, falls $K[V]^G$ endlich erzeugt, z.B. G reduktiv).

Beweis. Ist a_1, a_2 ein phsop in $K[V]$, so ist es dort auch eine reguläre Sequenz, denn der Polynomring $K[V]$ ist Cohen-Macaulay. Ist nun $d \in K[V]$ ein gemeinsamer Teiler von a_1, a_2, also $a_1 = dt_1, a_2 = dt_2$ mit $t_1, t_2 \in K[V]$, so folgt $t_1 a_2 = dt_1 t_2 = t_2 a_1 \in (a_1)$. Aufgrund der Regularität hat man also $t_1 \in (a_1)$, oder $t_1 = a_1 t'$ mit $t' \in K[V]$. Es folgt $t_1 = dt_1 t'$ oder $1 = dt'$. Also ist der gemeinsame Teiler d eine Einheit und damit a_1, a_2 teilerfremd.

Seien nun a_1, a_2 teilerfremd. Wir zeigen, dass dann a_1, a_2 eine reguläre Sequenz in $K[V]$ bzw. unter der Zusatzvoraussetzung auch in $K[V]^G$ ist. Dann bilden die beiden Elemente dort auch jeweils ein phsop (Satz 1.23 (a)).

Sei je nachdem $R = K[V]$ oder $R = K[V]^G$, und $h_2 \in R$ mit $h_2 a_2 \in (a_1)_R$. Dann existiert $h_1 \in R$ mit $h_2 a_2 = h_1 a_1$. Da a_1, a_2 in $K[V]$ teilerfremd sind, folgt also aus $a_1 | h_2 a_2$, dass $a_1 | h_2$ in $K[V]$; D.h. es gibt ein $t \in K[V]$ mit $h_2 \overset{(*)}{=} a_1 t$, d.h. $h_2 \in (a_1)_{K[V]}$. Dies zeigt die $K[V]$-Regularität. Im Fall $R = K[V]^G$ sind $h_2 \in R$ und a_1 invariant, und Anwendung eines $\sigma \in G$ auf Gleichung $(*)$ liefert $h_2 = a_1(\sigma t)$. Da $K[V]$ nullteilerfrei ist, ist auch $t = h_2/a_1 = \sigma t$ invariant, also $t \in K[V]^G$. Damit ist $h_2 = a_1 t \in (a_1)_{K[V]^G}$, also a_1, a_2 auch $K[V]^G$-regulär. □

3.1 Die Charakterisierung linear reduktiver Gruppen nach Kemper

Das Haupthilfsmittel für die Konstruktion von Invariantenringen mit beliebig großem Cohen-Macaulay-Defekt ist das folgende Lemma, das im Beweis von Kemper [33, Proposition 6] steckt, und zur Konstruktion von nicht-Cohen-Macaulay-Invariantenringen (also Invariantenringen mit positivem Cohen-Macaulay-Defekt) führt. Aus diesem folgt dann auch die Charakterisierung linear reduktiver Gruppen nach Kemper als diejenigen reduktiven Gruppen, deren Invariantenringe stets Cohen-Macaulay sind.

Lemma 3.2 *Sei G eine lineare algebraische Gruppe, V ein G-Modul, und es existiere ein $0 \neq g \in H^1(G, K[V])$. Seien weiter $a_1, a_2 \in K[V]_+^G$ homogen und teilerfremd in $K[V]$ (d.h. ein phsop in $K[V]$), die beide g annullieren, also $a_i g = 0 \in H^1(G, K[V])$ für $i = 1, 2$.*

Dann gibt es ein $m \in K[V]^G$ mit $m \notin (a_1, a_2)_{K[V]^G}$, so dass für jedes weitere $a_3 \in K[V]^G$ mit $a_3 g = 0 \in H^1(G, K[V])$ gilt, dass $m a_3 \in (a_1, a_2)_{K[V]^G}$.

Ist G reduktiv und bilden a_1, a_2, a_3 mit obigen Eigenschaften ein phsop in $K[V]$, so bilden sie aufgrund der Reduktivität von G auch eines in $K[V]^G$, aber dort keine reguläre Sequenz, insbesondere ist also $K[V]^G$ nicht Cohen-Macaulay.

Beweis. Wir klären zunächst die einfache Folgerung. Ist G reduktiv und bilden a_1, a_2, a_3 ein phsop in $K[V]$, so wegen Lemma 1.55 auch eines in $K[V]^G$. Da aber nach dem ersten Teil des Satzes $ma_3 \in (a_1, a_2)_{K[V]^G}$, aber $m \notin (a_1, a_2)_{K[V]^G}$, bildet das phsop dort keine reguläre Sequenz. Also ist $K[V]^G$ nach Satz 1.23 (b) nicht Cohen-Macaulay.

Nun zum eigentlichen Beweis des Lemmas. Sei $(\sigma \mapsto g_\sigma) \in Z^1(G, K[V])$ der zu g gehörige Kozyklus. Nach Voraussetzung sind die Kozyklen $(\sigma \mapsto a_i g_\sigma) \in Z^1(G, K[V]), i = 1, 2, 3$ trivial, also gibt es $b_i \in K[V]$ mit

$$a_i g_\sigma = (\sigma - 1)b_i \quad \text{für alle } \sigma \in G, \quad i = 1, 2, 3.$$

Sei

$$u_{ij} = a_i b_j - a_j b_i \text{ für } 1 \leq i < j \leq 3.$$

Offenbar ist $u_{ij} \in K[V]^G$ $(\sigma u_{ij} = a_i(b_j + a_j g_\sigma) - a_j(b_i + a_i g_\sigma) = u_{ij})$, und es gilt

$$u_{23}a_1 - u_{13}a_2 + u_{12}a_3 = \begin{vmatrix} a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} = 0.$$

Wir setzen nun $m := u_{12} = a_1 b_2 - a_2 b_1$. Dabei hängt m nur von a_1 und a_2 ab, und nach obiger Gleichung gilt $ma_3 \in (a_1, a_2)_{K[V]^G}$. Wir müssen zeigen, dass $m \notin (a_1, a_2)_{K[V]^G}$, und nehmen dazu das Gegenteil an, also $m = u_{12} \in (a_1, a_2)_{K[V]^G}$. Dann gibt es $f_1, f_2 \in K[V]^G$ mit

$$u_{12} = a_1 b_2 - a_2 b_1 = f_1 a_1 + f_2 a_2.$$

Aus $a_1(b_2 - f_1) = a_2(f_2 + b_1)$ und der Teilerfremdheit von a_1, a_2 folgt dann, dass a_1 Teiler von $f_2 + b_1$ ist, also $f_2 + b_1 = a_1 \cdot h$ mit $h \in K[V]$. Nun ist

$$a_1 \cdot (\sigma - 1)h = (\sigma - 1)(a_1 h) = (\sigma - 1)(f_2 + b_1) = (\sigma - 1)b_1 = a_1 g_\sigma \qquad \text{für alle } \sigma \in G,$$

also $g_\sigma = (\sigma - 1)h$. Damit ist die zugehörige Restklasse $g \in H^1(G, K[V])$ gleich 0, was im Widerspruch zur Voraussetzung steht. Also war die Annahme falsch, und es gilt $m \notin (a_1, a_2)_{K[V]^G}$. □

Aus $a_1 g_\sigma = (\sigma - 1)b_1$ für alle $\sigma \in G$ mit $b_1 \in K[V]$ folgt übrigens, dass $(g_\sigma)_{\sigma \in G}$ „gradbeschränkt“ ist, also dass es Zahlen $0 \leq m \leq n < \infty$ gibt mit $(g_\sigma)_{\sigma \in G} \in Z^1(G, \oplus_{k=m}^n S^k(V))$. Außerdem folgt aus $g_\sigma = \frac{1}{a_1}(\sigma - 1)b_1$, dass g in jedem Fall durch einen Morphismus gegeben ist (Polynomdivison, etwa bzgl. graduierter lexikographischer Ordnung, gibt die Koeffizienten von g_σ als Linearkombination der Koeffizienten von $(\sigma - 1)b_1$), auch falls man diese Forderung an die Elemente aus $Z^1(G, K[V])$ (wie in Abschnitt 2) zunächst nicht stellen will.

Korollar 3.3 *Sei G eine reduktive Gruppe, $g \in Z^1(G, U)$ ein nichttrivialer Kozyklus, und $\tilde{U}$ der zugehörige erweiterte G-Modul (siehe Abschnitt 1.3). Ist dann*

$$V^* := U \oplus \tilde{U}^* \oplus \tilde{U}^* \oplus \tilde{U}^* \quad \text{d.h. } V := U^* \oplus \tilde{U} \oplus \tilde{U} \oplus \tilde{U},$$

so ist $K[V]^G$ nicht Cohen-Macaulay.

Beweis. Es ist $K[V] = S(V^*) = S(U \oplus \tilde{U}^* \oplus \tilde{U}^* \oplus \tilde{U}^*)$. Dann ist auch $g \in Z^1(G, S(V^*))$ ein nichttrivialer Kozyklus, denn U ist direkter Summand von $S(V^*)$. Nach Proposition 1.51 gibt es $\pi \in \tilde{U}^{*G} \setminus \{0\}$, so dass $\pi \otimes g = 0 \in H^1(G, \tilde{U}^* \otimes U)$. Sind a_1, a_2, a_3 die drei Kopien von π in den entsprechenden direkten Summanden von $S(V^*)$, so bilden diese also ein annullierendes phsop des Kozyklus g in $K[V]$, und nach vorhergehendem Lemma ist $K[V]^G$ nicht Cohen-Macaulay. □

Man beachte, dass bei dieser Konstruktion V bzw. V^* niemals vollständig reduzibel sein kann: Die Nichttrivialität des Kozyklus g ist nämlich äquivalent dazu, dass $U \subseteq \tilde{U}$ bzw. $K\pi \subseteq \tilde{U}^*$ kein Komplement hat. Mit Hilfe verfeinerter Methoden werden wir später dennoch Beispiele mit V vollständig reduzibel und nicht Cohen-Macaulay Invariantenring angeben.

Es folgt die Charakterisierung linear reduktiver Gruppen nach Kemper:

Satz 3.4 (Kemper [33]) *Eine reduktive Gruppe G ist genau dann linear reduktiv, wenn $K[V]^G$ für jeden G-Modul V Cohen-Macaulay ist.*

Beweis. Ist G linear reduktiv, so ist $K[V]^G$ nach Hochster und Roberts stets Cohen-Macaulay. Ist G reduktiv, aber nicht linear reduktiv, so gibt es nach Proposition 1.47 einen G-Modul U mit $H^1(G, U) \neq 0$, d.h. es existiert ein nichttrivialer Kozyklus $g \in Z^1(G, U)$. Nach dem Korollar existiert dann aber ein G-Modul V mit nicht Cohen-Macaulay Invariantenring $K[V]^G$. □

Wir wollen abschliessend noch eine Begründung angeben, warum man mit Lemma 3.2 die meisten bekannten Beispiele von nicht Cohen-Macaulay Invariantenringen verstehen kann. Die nicht Cohen-Macaulay Eigenschaft ergibt sich nämlich in vielen Fällen aus einem phsop der Länge 3, welches keine reguläre Sequenz ist. (Das folgende Lemma (allgemeiner in [32, Theorem 1.4]) wird nicht weiter verwendet und kann ggf. übersprungen werden.)

Lemma 3.5 *Sei $K[V]^G$ endlich erzeugt und $a_1, a_2, a_3 \in K[V]^G$ ein phsop in $K[V]$. Ist a_1, a_2, a_3 keine reguläre Sequenz in $K[V]^G$, so gibt es ein $0 \neq g \in H^1(G, K[V])$ mit $a_i g = 0 \in H^1(G, K[V])$, $i = 1, 2, 3$.*

Beweis. Nach Lemma 3.1 sind a_1, a_2 teilerfremd in $K[V]$ und bilden eine reguläre Sequenz in $K[V]^G$. Da aber a_1, a_2, a_3 nicht $K[V]^G$-regulär sind, gibt es dann also $r_1, r_2, r_3 \in K[V]^G$ mit $r_1a_1 + r_2a_2 + r_3a_3 = 0$ und $r_3 \notin (a_1, a_2)_{K[V]^G}$. Da $K[V]$ Cohen-Macaulay und a_1, a_2, a_3 dort ein phsop ist, gibt es aber nach Satz 1.23 $s_1, s_2 \in K[V]$ mit

$$r_3 = s_1a_1 + s_2a_2.$$

Wir wenden hierauf $(\sigma - 1)$ mit $\sigma \in G$ an. Wegen $r_3, a_1, a_2 \in K[V]^G$ erhalten wir

$$0 = a_1(\sigma - 1)s_1 + a_2(\sigma - 1)s_2.$$

Da a_1, a_2 in $K[V]$ teilerfremd sind, folgt $a_2 | (\sigma - 1)s_1$. Daher ist

$$g_\sigma := \frac{(\sigma - 1)s_1}{a_2} = -\frac{(\sigma - 1)s_2}{a_1} \in K[V] \quad \text{für alle } \sigma \in G.$$

Offenbar ist $g \in Z^1(G, K[V])$ und $a_1 g, a_2 g \in B^1(G, K[V])$. Weiter ist

$$\begin{aligned} 0 &= r_1 a_1 + r_2 a_2 + r_3 a_3 = r_1 a_1 + r_2 a_2 + (s_1 a_1 + s_2 a_2) a_3 \\ &= (r_1 + s_1 a_3) a_1 + (r_2 + s_2 a_3) a_2. \end{aligned}$$

Da a_1, a_2 teilerfremd sind, folgt $a_2 | (r_1 + s_1 a_3)$, also gibt es $h \in K[V]$ mit

$$r_1 + s_1 a_3 = a_2 h.$$

Es folgt

$$a_3 g_\sigma = \frac{(\sigma - 1)(a_3 s_1)}{a_2} = \frac{(\sigma - 1)(r_1 + a_3 s_1)}{a_2} = \frac{(\sigma - 1)(a_2 h)}{a_2} = (\sigma - 1)h \text{ für alle } \sigma \in G,$$

also auch $a_3 g \in B^1(G, K[V])$. Wäre auch $g \in B^1(G, K[V])$, so gäbe es $v \in K[V]$ mit $g_\sigma = (\sigma - 1)v$ für alle $\sigma \in G$. Es folgt $(\sigma - 1)s_1 = (\sigma - 1)(a_2 v)$ und $(\sigma - 1)s_2 = (\sigma - 1)(-a_1 v)$ für alle $\sigma \in G$, also $s_1 - a_2 v, s_2 + a_1 v \in K[V]^G$. Damit wäre dann doch

$$r_3 = s_1 a_1 + s_2 a_2 = (s_1 - a_2 v) a_1 + (s_2 + a_1 v) a_2 \in (a_1, a_2)_{K[V]^G},$$

Widerspruch! □

3.2 Der Hauptsatz - eine untere Schranke für den Cohen-Macaulay-Defekt

Wir leiten in diesem Abschnitt eine untere Schranke für den Cohen-Macaulay-Defekt her, die es uns erlauben wird, für jede reduktive, nicht linear reduktive Gruppe einen Invariantenring mit beliebig großem Cohen-Macaulay-Defekt zu konstruieren, und dies lässt sich dann sogar mit Vektorinvarianten erreichen. Der folgende (technische) Satz, zusammen mit seinen unmittelbaren, weniger technischen Folgerungen und den Anwendungen im nächsten Abschnitt mit konkreten Beispielen stellt das Hauptresultat dieser Arbeit dar.

Hauptsatz 3.6 *Sei G eine reduktive Gruppe, V ein G-Modul, und es existiere ein $0 \neq g \in H^1(G, K[V])$. Seien weiter $a_1, \ldots, a_k \in K[V]^G$ mit $k \geq 2$ ein phsop in $K[V]$ mit $a_i g = 0 \in H^1(G, K[V])$ für $i = 1, \ldots, k$. Dann gilt*

$$\operatorname{depth}(a_1, \ldots, a_k)_{K[V]^G} = 2, \quad \textit{also } \operatorname{cmdef}(a_1, \ldots, a_k)_{K[V]^G} = k - 2,$$

und damit

$$\operatorname{cmdef} K[V]^G \geq k - 2.$$

Wir werden auch die folgende **allgemeinere Formulierung** brauchen: *Sei G eine beliebige lineare algebraische Gruppe, V ein G-Modul so, dass $K[V]^G$ endlich erzeugt ist, und $0 \neq g \in H^1(G, K[V])$. Seien weiter $a_1, \ldots, a_k \in K[V]^G_+$ homogen mit $a_i g = 0 \in H^1(G, K[V])$. Ist a_1, a_2 teilerfremd in $K[V]$, so gilt* $\operatorname{depth}(a_1, \ldots, a_k)_{K[V]^G} = 2$. *Ist zusätzlich $a_1, \ldots, a_k$ ein phsop in $K[V]^G$, so gilt* $\operatorname{cmdef}(a_1, \ldots, a_k)_{K[V]^G} = k - 2$ *und damit* $\operatorname{cmdef} K[V]^G \geq k - 2$

Beweis. Nach Lemma 3.1 bildet a_1, a_2 eine reguläre Sequenz in $K[V]^G$. Nach Lemma 3.2 existiert ein $m \in K[V]^G$ mit $m \notin (a_1, a_2)_{K[V]^G}$, aber $m a_i \in (a_1, a_2)_{K[V]^G}$ für alle $i = 1, \ldots, k$.

Satz 1.21 mit $M = R = K[V]^G$ liefert dann $\operatorname{depth}(a_1, \ldots, a_k)_{K[V]^G} = 2$. Da $a_1, \ldots, a_k$ ein phsop in $K[V]$ ist, ist es wegen Lemma 1.55 also auch eines in $K[V]^G$ (in der allgemeineren Formulierung ist dies eine Voraussetzung), und es folgt $\operatorname{height}(a_1, \ldots, a_k)_{K[V]^G} = k$ (Lemma 1.5). Damit gilt nach Definition 1.22 $\operatorname{cmdef}(a_1, \ldots, a_k)_{K[V]^G} = k-2$, und mit Satz 1.26 also $\operatorname{cmdef} K[V]^G \geq k-2$. □

Der Beweis ist aufgrund der in Abschnitt 1 gemachten Vorbereitungen ziemlich kurz. Ich möchte noch einen Beweis angeben, der zwar etwas länger ist, weil er im Prinzip den Beweis von Satz 1.26 in einer etwas übersichtlicheren Situation mit eingebaut hat, mir aber ebenfalls lehrreich erscheint und näher an meinem ursprünglichen Beweis für diesen Satz liegt.

2. Beweis. Genau wie beim ersten Beweis folgert man zunächst $\operatorname{depth}(a_1, \ldots, a_k)_{K[V]^G} = 2$.

Sei nun $n = \dim K[V]^G$, und man ergänze $a_1, \ldots, a_k$ zu einem hsop $a_1, \ldots, a_k, a_{k+1}, \ldots, a_n$ von $K[V]^G$. Es gilt dann

$$\begin{aligned} \operatorname{depth} K[V]^G &= \operatorname{depth}(a_1, \ldots, a_k, a_{k+1}, \ldots, a_n)_{K[V]^G} \quad \text{(Korollar 1.25)} \\ &\leq \operatorname{depth}(a_1, \ldots, a_k)_{K[V]^G} + (n-k) \quad \text{(Korollar 1.20)} \\ &= 2 + (n-k), \end{aligned}$$

also

$$k - 2 \leq n - \operatorname{depth} K[V]^G = \dim K[V]^G - \operatorname{depth} K[V]^G = \operatorname{cmdef} K[V]^G.$$

□

Wir ziehen die Korollar 3.3 entsprechende Folgerung; Für $k = 3$ erhalten wir sogar genau das Korollar 3.3 zurück.

Korollar 3.7 *Sei G eine reduktive Gruppe, $g \in Z^1(G, U)$ ein nichttrivialer Kozyklus, und $\tilde{U}$ der zugehörige erweiterte G-Modul (siehe Abschnitt 1.3). Ist dann*

$$V^* := U \oplus \bigoplus_{i=1}^{k} \tilde{U}^* \qquad \text{d.h. } V := U^* \oplus \bigoplus_{i=1}^{k} \tilde{U}$$

so gilt

$$\operatorname{cmdef} K[V]^G \geq k - 2.$$

Beweis. Analog wie der Beweis von Korollar 3.3. Die k Kopien $a_1, \ldots, a_k \in K[V]^G$ des nach Proposition 1.51 existierenden Annullators $\pi \in \tilde{U}^{*G} \setminus \{0\}$ des (eingebetteten) Kozyklus $0 \neq g \in H^1(G, K[V])$ erfüllen die Voraussetzungen des Hauptsatzes. □

Damit erhalten wir auch eine neue Charakterisierung linear reduktiver Gruppen. Zum Vergleich beachte man, dass man Satz 3.4 auch so formulieren kann:

Eine reduktive Gruppe G ist genau dann linear reduktiv, wenn $\operatorname{cmdef} K[V]^G = 0$ *für jeden G-Modul V ist.*

Korollar 3.8 *Eine reduktive Gruppe G ist genau dann linear reduktiv, wenn es eine „globale Cohen-Macaulay-Defekt Schranke“ gibt, d.h. eine Zahl $B \in \mathbb{N}$ mit* $\operatorname{cmdef} K[V]^G \leq B$ *für jeden G-Modul V.*

Beweis. Ist G linear reduktiv, so ist der Cohen-Macaulay-Defekt stets 0. Ist G reduktiv, aber nicht linear reduktiv, so gibt es einen G-Modul U mit $H^1(G,U) \neq 0$ (Proposition 1.47), so dass die Voraussetzungen von Korollar 3.7 erfüllt sind. Setzt man dort $k > B+2$, so erhält man mit dem dortigen Modul V also $\operatorname{cmdef} K[V]^G > B$, also existiert keine globale Cohen-Macaulay-Defekt Schranke B. □

Man kann den Cohen-Macaulay-Defekt sogar mit Vektorinvarianten gegen unendlich treiben:

Korollar 3.9 *Ist G reduktiv, aber nicht linear reduktiv, so existiert ein G-Modul V mit*

$$\operatorname{cmdef} K\left[\oplus_{i=1}^k V\right]^G \geq k-2 \quad \text{für alle } k \in \mathbb{N},$$

insbesondere also

$$\lim_{k\to\infty} \operatorname{cmdef} K\left[\oplus_{i=1}^k V\right]^G = \infty.$$

Beweis. Da G nicht linear reduktiv ist, gibt es nach Proposition 1.47 einen G-Modul U mit nichttrivialem Kozyklus wie in Korollar 3.7 gefordert. Der dortige Beweis bleibt richtig, wenn man anstatt $U^* \oplus \bigoplus_{i=1}^k \tilde{U}$ den Modul $W := \bigoplus_{i=1}^k \left(U^* \oplus \tilde{U}\right)$ betrachtet - weitere nichttriviale Kozyklen in $K[W]$ stören ja nicht. Man wählt einen einzigen der k nichttrivialen Kozyklen aus, und dieser wird dann von den k Kopien der Invarianten $\pi \in \tilde{U}^{*G} \subseteq S(W^*)^G$ annulliert. Mit $V := U^* \oplus \tilde{U}$ gilt dann also die Behauptung. □

Bemerkung 3.10 Die Frage, ob in den Korollaren 3.7 oder 3.9 jeweils auch ein *treuer* G-Modul V mit den genannten Eigenschaften existiert, lässt sich sehr leicht mit „Ja“ beantworten: Man nehme einfach einen beliebigen, treuen G-Modul M (der ja stets existiert, Satz 1.33) als Summand hinzu, setze also etwa $V' := V \oplus M$. Nichttriviale Kozyklen bleiben auch in $K[V']$ nichttrivial, und entsprechendes gilt für annullierende phsops im Polynomring; und mit M ist natürlich auch V' treu. Damit gelten die Aussagen der beiden Korollare dann auch für V' statt V.

Zum Vergleich geben wir noch das entsprechende Resultat für endliche Gruppen an:

Satz 3.11 (Gordeev, Kemper) *Sei* $\operatorname{char} K = p > 0$, *$G$ eine endliche Gruppe, V ein G-Modul, N der Kern der Darstellung $G \to \mathrm{GL}(V)$ und p ein Teiler des Index $(G:N)$. Dann gilt*

$$\lim_{k\to\infty} \operatorname{cmdef} K\left[\oplus_{i=1}^k V\right]^G = \infty.$$

Genauer: Ist $r_0 > 0$ mit $H^{r_0}(G/N, K) \neq 0$ (ein solches r_0 gibt es stets) oder $H^{r_0}(G/N, V^*) \neq 0$ oder $H^{r_0}(G/N, K[V]) \neq 0$, so gilt

$$\operatorname{cmdef} K\left[\oplus_{i=1}^k V\right]^G \geq k - r_0 - 1 \quad \text{für alle } k \in \mathbb{N}.$$

Es gilt sogar folgende **Verallgemeinerung:** *Es erfülle $V_1 := V$ obige Voraussetzungen, wobei zusätzlich V* treu *sei. Ist $(V_i)_{i\geq 2}$ eine beliebige Folge* treuer *G-Moduln, so gilt*

$$\operatorname{cmdef} K\left[\oplus_{i=1}^k V_i\right]^G \geq k - r_0 - 1 \quad \text{für alle } k \in \mathbb{N}.$$

Man beachte, dass G/N treu auf V operiert und $K[V]^{G/N} = K[V]^G$ gilt. Der Satz gibt damit das bestmögliche Resultat, denn wenn p kein Teiler von $(G : N)$ ist, so kommt die G-Operation letztlich von der linear reduktiven Gruppe G/N, und dann gilt natürlich nach Hochster und Roberts cmdef $K\left[\oplus_{i=1}^k V\right]^G = 0$ für alle k.

In Gordeev, Kemper [21, Corollary 5.15] wird der Satz aus einem allgemeineren Resultat gefolgert; Wir geben einen etwas elementareren Beweis, der auf den Resultaten der Arbeit [32] basiert.

Beweis. Nach dem Vorspann können wir annehmen, dass G treu auf V operiert und p ein Teiler der Gruppenordnung $|G|$ ist. Es genügt dann offenbar, die Verallgemeinerung zu beweisen (man kann ja $V_i := V$ für alle i wählen). Setze $R := K\left[\oplus_{i=1}^k V_i\right]$. Nach [3, Theorem 4.1.3] existiert wegen $p \mid |G|$ ein $r_0 > 0$, so dass die r_0-te Kohomologiegruppe $H^{r_0}(G, K) \neq 0$ ist. Ist diese oder eine der anderen beiden Bedingungen erfüllt, so ist auch $H^{r_0}(G, R) \neq 0$ (denn es sind K bzw. V^* bzw. $K[V]$ jeweils direkte, G-stabile Summanden von R mit G-stabilem Komplement). Insbesondere gibt es dann ein minimales $1 \leq r \leq r_0$ mit der Eigenschaft $H^r(G, R) \neq 0$. Man kann dann $0 \neq g \in H^r(G, R)$ wählen, so dass der zugehörige nichttriviale r-Kozyklus nur Werte in einer homogenen Komponente annimmt (indem man etwa eine geeignete homogene Komponente eines gegebenen nichttrivialen Kozyklus g wählt - da G endlich, sind nur endlich viele Projektionen von g auf eine homogene Komponente ungleich Null, und wären alle solchen Projektionen trivial, so auch g). Insbesondere ist dann das „Annullationsideal“

$$I_g := \left\{a \in R^G : ag = 0 \in H^r(G, R)\right\} \lhd R^G$$

homogen. Nach [32, Corollary 1.6] gilt dann

$$\operatorname{depth} I_g \leq r + 1 \leq r_0 + 1. \tag{77}$$

Für $\sigma \in G$ sei $A_{i,\sigma}$ die zugehörige lineare Abbildung auf V_i, und B_σ die zugehörige lineare Abbildung auf $\oplus_{i=1}^k V_i$. Da G treu auf V_i operiert, gilt für jedes $\sigma \neq \iota$ ($\iota \in G$ neutrales Element), dass $\operatorname{rang}\left(A_{i,\sigma} - \mathrm{id}_{V_i}\right) \geq 1$, und damit $\operatorname{rang}\left(B_\sigma - \mathrm{id}_{\oplus_{i=1}^k V_i}\right) \geq k$. Nach [32, Lemma 2.1, Lemma 1.7] gibt es dann $a_1, \ldots, a_k \in I_g$ mit $\operatorname{height}(a_1, \ldots, a_k)_{R^G} = k$, und es folgt $\operatorname{height}(I_g) \geq k$. Mit Gleichung (77) folgt also

$$\operatorname{cmdef} I_g = \operatorname{height}(I_g) - \operatorname{depth}(I_g) \geq k - r_0 - 1,$$

und aus Satz 1.26 dann $\operatorname{cmdef} R^G \geq k - r_0 - 1$. Hieraus folgen die Behauptungen. □

Wir geben eine hübsche Anwendung.

Korollar 3.12 (Campbell, Geramita, Hughes, Kemper, Shank, Wehlau)
Sei K ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$ und G eine endliche Gruppe, die einen Normalteiler vom Index p enthält (z.B. G eine p-Gruppe, oder G nilpotent und $p||G|$). Dann gilt für jeden treuen G-Modul V

$$\operatorname{cmdef} K\left[\oplus_{i=1}^k V\right]^G \geq k - 2,$$

insbesondere ist der Invariantenring für $k \geq 3$ nicht Cohen-Macaulay.

Ist G eine p-Gruppe, so existiert eine Unterguppe $N \subseteq G$ mit $(G : N) = p$, und eine solche ist automatisch auch Normalteiler vom Index p. Ist G nilpotent, also direktes Produkt ihrer Sylow-Untergruppen, so ist das direkte Produkt eines Normalteilers der p-Sylowgruppe vom Index p (existiert nach eben) und der anderen Sylowgruppen ein Normalteiler von G vom Index p.

Beweis. (vgl. [9, Corollary 21] sowie [8, Theorem 1.2] und [32, Theorem 2.3]). Sei $\mathbb{F}_p \subseteq K$ der Primkörper von K. Sei $N \lhd G$ ein Normalteiler mit $(G : N) = p$. Dann ist $G/N \cong Z_p \cong (\mathbb{F}_p, +) \subseteq (K, +)$. ($Z_p$ ist die zyklische Gruppe der Ordnung p). Wir schreiben G multiplikativ und bezeichnen für $a \in G$ mit $\bar{a} \in K$ das $aN \in G/N$ entsprechende Element gemäß obiger Einbettung. Dann ist $\overline{ab} = \bar{a} + \bar{b}$ $(a, b \in G)$.

Offenbar ist durch $g : G \to K, a \mapsto g_a = \bar{a}$ ein nichttrivialer Kozyklus gegeben (K trägt triviale G-Operation, hier bezeichnet mit $\circ$): Zum einen ist

$$g_{ab} = \overline{ab} = \bar{a} + a \circ \bar{b} = a \circ g_b + g_a \quad \text{für alle } a, b \in G,$$

also g ein Kozyklus, und für alle $v \in K$ und $a \in G$ ist $(a - 1) \circ v = v - v = 0$, also g nichttrivial. Dies zeigt $H^1(G, K) \neq 0$, und mit $r_0 = 1$ in Satz 3.11 folgt die Behauptung. □

Im Gegensatz zu Satz 3.11 besagt Korollar 3.9 nur, dass überhaupt eine Darstellung existiert, deren Cohen-Macaulay-Defekt der Vektorinvarianten gegen unendlich geht. Man könnte vermuten, dass dennoch die entsprechende Aussage für treue rationale Darstellungen reduktiver, nicht linear reduktiver Gruppen gilt, aber dem ist nicht so. Es gilt nämlich:

Satz 3.13 *Sei* $\operatorname{char} K$ *beliebig und* $V = K^n$*. Ist dann* G *eine der Gruppen* $\mathrm{SL}_n(K), \mathrm{GL}_n(K)$ *oder* $\mathrm{SO}_n(K)$ *(dann* $\operatorname{char} K \neq 2$*), so ist* $K\left[\oplus_{i=1}^k V\right]^G$ *Cohen-Macaulay für alle* $k \in \mathbb{N}$*.*

Beweis. Für die Gruppe SO_n siehe die erst in Kürze erscheinende Arbeit [41]. Für $G = \mathrm{SL}_n$ wird $K\left[\oplus_{i=1}^k V\right]^G$ nach de Concini und Procesi [11] auch in positiver Charakteristik von den sogenannten „Plücker-Invarianten“ erzeugt, und bildet daher den Koordinatenring einer Grassman-Varietät. Ein solcher ist nach Hochster [26, Corollary 3.2] Cohen-Macaulay. (Vgl. auch Hochster und Eagon [27, p.1029, mitte]). Für $G = \mathrm{GL}_n$ gilt dagegen nach [11] stets $K\left[\oplus_{i=1}^k V\right]^G = K$, so dass diese Invariantenringe trivialerweise ebenfalls stets Cohen-Macaulay sind. □

Die Gruppen $\mathrm{SL}_n, \mathrm{GL}_n$ mit $n \geq 2$ und SO_n mit $n \geq 3$ und $p \neq 2$ sind in positiver Charakteristik zwar reduktiv, aber nicht linear reduktiv (siehe Bemerkung 4.5), und operieren treu auf $V = K^n$. Dennoch sind die zugehörigen Vektorinvarianten nach diesem Satz stets Cohen-Macaulay. Daher lässt sich Satz 3.11 nicht auf unendliche Gruppen verallgemeinern.

Wir haben im Beweis von Satz 3.11 ein Resultat über die Tiefe des sogenannten Annullationsideals eines r-Kozyklus (für endliche Gruppen) verwendet. Mit unseren Methoden können wir dieses Resultat für $r = 1$ auch auf unendliche Gruppen verallgemeinern. Nochmal die Definition für den Fall $r = 1$: Ist $g \in H^1(G, K[V])$, so wird das *Annullationsideal* definiert als

$$I_g := \left\{a \in K[V]^G : ag = 0 \in H^1(G, K[V])\right\},$$

und man sieht sofort, dass dies tatsächlich ein Ideal in $K[V]^G$ ist. Wir nennen einen Kozyklus $g \in Z^1(G, K[V])$ (bzw. seine Restklasse in $H^1(G, K[V])$ *homogen*, wenn es ein

$d \in \mathbb{N}_0$ gibt mit $g_\sigma \in K[V]_d$ für alle $\sigma \in G$. Für einen homogenen Kozyklus ist offenbar I_g ein homogenes Ideal. Der folgende Satz ist eine Version des Hauptsatzes (mit praktisch demselben Beweis) mit schwächeren Forderungen, die entsprechend auch eine schwächere Aussage liefert.

Satz 3.14 *Sei G eine (nicht notwendig reduktive!) lineare algebraische Gruppe und V ein G-Modul, so dass $K[V]^G$ endlich erzeugt ist. Sei ferner $0 \neq g \in H^1(G, K[V])$ homogen. Falls I_g zwei homogene, in $K[V]$ teilerfremde Elemente positiven Grades enthält, so gilt*

$$\operatorname{depth}(I_g) = 2.$$

Beweis. Aufgrund der Voraussetzungen ist $I_g \neq K[V]^G$ ein homogenes Ideal, denn $g \neq 0$ (also $1 \notin I_g$) und g ist homogen. Seien $a_1, a_2 \in I_g$ homogen, positiven Grades und teilerfremd. Nach Lemma 3.1 bilden a_1, a_2 eine reguläre Sequenz in I_g, und nach Lemma 3.2 gibt es ein $m \in K[V]^G$ mit $m \notin (a_1, a_2)_{K[V]^G}$ aber $am \in (a_1, a_2)_{K[V]^G}$ für alle $a \in I_g$. Nach Satz 1.21 (der „äquivalenten Formulierung“) folgt $\operatorname{depth} I_g = 2$. □

Kennt man zusätzlich eine untere Schranke für $\operatorname{height} I_g$, $\operatorname{height} I_g \geq k$, etwa weil man ein in I_g liegendes phsop von $K[V]^G$ der Länge k kennt, so erhält man mit Satz 1.26 die Abschätzung

$$\operatorname{cmdef} R \geq \operatorname{height}(I_g) - \operatorname{depth}(I_g) \geq k - 2.$$

Insbesondere erhält man so auch nochmal die Aussage des Hauptsatzes, wenn G reduktiv ist und man ein annullierendes phsop in $K[V]$ hat.

Man vergleiche diesen Satz mit dem entsprechenden Resultat für endliche Gruppen (nur den Spezialfall für die erste Kohomologie), Kemper [32, Corollary 1.6], welches wir (für allgemeines r) im Beweis von Satz 3.11 verwendet haben:

Korollar 3.15 *Ist G eine endliche Gruppe, $0 \neq g \in H^1(G, K[V])$ homogen, so ist*

$$\operatorname{depth}(I_g) = \min\{2, \operatorname{height}(I_g)\}.$$

Beweis. Im Fall $\operatorname{height}(I_g) = 0$ ist $I_g = \{0\}$, also auch $\operatorname{depth}(I_g) = 0 = \min\{2, 0\}$. Im Fall $\operatorname{height}(I_g) = 1$ ist $I_g \neq \{0\}$. Da $K[V]^G$ nullteilerfrei, ist dann auch $1 \leq \operatorname{depth}(I_g) \leq \operatorname{height}(I_g) = 1$, also $\operatorname{depth}(I_g) = 1 = \min\{2, 1\}$. Ist nun $\operatorname{height}(I_g) \geq 2$, so enthält I_g ein phsop a_1, a_2 von $K[V]^G$ der Länge 2 (Lemma 1.5 (b)). Da $K[V]$ eine ganze Erweiterung des normalen Rings $K[V]^G$ ([12, Proposition 2.3.11]) ist, ist a_1, a_2 nach Korollar 1.7 auch ein phsop in $K[V]$, also dort teilerfremd (Lemma 3.1). Mit Satz 3.14 folgt also $\operatorname{depth}(I_g) = 2 = \min\{2, \operatorname{height}(I_g)\}$. □

Die Verallgemeinerung des Korollars auf unendliche Gruppen scheitert (zumindest bei diesem Beweis) offenbar daran, dass es dann phsops in $K[V]^G$ gibt, die kein phsop in $K[V]$ bilden. Siehe etwa [33, Remark 5] für ein Beispiel.

4 Anwendungen des Hauptsatzes

Im Folgenden wollen wir konkret Darstellungen V für eine reduktive, nicht linear reduktive Gruppe G angeben, die die Voraussetzungen des Hauptsatzes 3.6 mit beliebig vorgegebenem k erfüllen, für die also $\operatorname{cmdef} K[V]^G \geq k-2$ gilt. Mit den Ergebnissen aus Abschnitt 1.4.3 lässt sich oft auch $\dim K[V]^G$ exakt angeben, so dass wir eine Abschätzung $\operatorname{depth} K[V]^G \leq \dim K[V]^G - k + 2$ erhalten. Für die allgemeine Konstruktion müssen wir dabei nur die Ergebnisse der letzten Abschnitte zusammensetzen, was allerdings zu einer großen Vektorraumdimension des Darstellungsmoduls V führt. Wir führen daher auch verfeinerte Betrachtungen durch, die zu teils erheblich niedrigeren Dimensionen führen. Dabei verwenden wir Roberts' Isomorphismus, der außerdem auch Beispiele für eine Klasse von nicht reduktiven Gruppen liefert.

4.1 Motivation: Additive Gruppen endlicher Körper

Sei K ein algebraisch abgeschlossener Körper der Charakteristik p. Für jede Potenz q von p ist

$$G := \{a \in K : a^q - a = 0\} \subseteq K^1$$

zusammen mit der Addition „+“ von K eine lineare algebraische Gruppe, die isomorph ist zur additiven Gruppe $(\mathbb{F}_q, +)$ des endlichen Körpers mit q Elementen. Sei $\langle X, Y\rangle$ der G-Modul mit der natürlichen Darstellung

$$a \mapsto \begin{pmatrix} 1 & a \\ & 1 \end{pmatrix}.$$

Dabei ist $\langle X, Y\rangle$ selbstdual, genauer ist $\langle X, Y\rangle^* = \langle X^*, Y^*\rangle \cong \langle Y, -X\rangle$. Wir betrachten nun die n-fache direkte Summe der natürlichen Darstellung,

$$V^* := \bigoplus_{i=1}^{n} \langle X_i, Y_i\rangle.$$

Als nächstes benötigen wir einen nichttrivialen Kozyklus in $K[V] \cong S(V^*)$. Ein solcher wird gegeben durch

$$g : G \to K[V] = S(V^*), \quad a \mapsto a \cdot 1_{K[V]} \in K[V]_0.$$

Dabei ist g ein Kozyklus in $Z^1(G, K[V])$, denn es gilt $g_{a\circ b} = g_{a+b} = (a+b)\cdot 1_{K[V]} = g_b + g_a = a \cdot g_b + g_a$ (die Operation von G auf $K[V]_0 = K$ ist trivial). Außerdem ist g auch nichttrivial, denn wenn es ein $v \in K[V]$ gäbe mit $g_a = (a-1)v$ für alle $a \in G$, dann könnte man v auch homogen vom Grad 0 wählen, also $v \in K = K[V]_0$. Dann ist aber $a \cdot v - v = v - v = 0$, im Widerspruch etwa zu $g_1 = 1$.

Weiter sind die $X_i, i = 1, \ldots, n$ Annullatoren des Kozyklus g, denn es gilt

$$X_i g_a = a X_i = (a-1) \cdot Y_i \quad \text{für alle } a \in G,$$

also $X_i g \in B^1(G, K[V])$. Da $X_1, \ldots, X_n$ als Variablen außerdem ein phsop bilden, liefert der Hauptsatz 3.6 also sofort

$$\operatorname{cmdef} K[V]^G = \operatorname{cmdef} K\left[\bigoplus_{i=1}^{n} \langle X_i, Y_i\rangle\right]^{(\mathbb{F}_q,+)} \geq n-2. \tag{78}$$

(Wir hätten dies natürlich auch aus Korollar 3.12 folgern können). Da G eine endliche Gruppe ist, gilt $\dim K[V]^G = \dim_K V = 2n$, und damit

$$\operatorname{depth} K[V]^G = \dim K[V]^G - \operatorname{cmdef} K[V]^G \leq 2n - (n-2) = n+2.$$

Die rechte Seite ist offenbar gleich $\dim_K V^G + 2$. Nach dem folgenden Resultat, das auch noch etwas allgemeiner gilt, gilt hier sogar Gleichheit (dabei ist $V^\sigma = \{v \in V : \sigma v = v\}$):

Satz 4.1 (Campbell, Ellingsrud, Hughes, Kemper, Shank, Skjelbred, Wehlau) *Sei* $\operatorname{char} K = p > 0$*,* G *eine* p-Gruppe *und* V *ein* G*-Modul. Falls* G nicht *von den Elementen* $\sigma \in G$ *mit* $\dim V^\sigma > \dim V^G$ *erzeugt wird (z.B. wenn* G *eine zyklische* p*-Gruppe ist), dann gilt*

$$\operatorname{depth} K[V]^G = \min\{\dim_K V^G + 2, \dim_K V\}.$$

Beweis. Siehe Campbell, Hughes, Kemper, Shank, Wehlau [9], Theorem 1, Theorem 2 und Remark 4 (a). Im zyklischen Fall folgt aus $\dim V^\sigma > \dim V^G$ jedenfalls, dass σ nicht G erzeugt, und daher in der eindeutig bestimmten Untergruppe vom Index p liegt, d.h. alle solchen σ können höchstens diese Untergruppe erzeugen. Der zyklische Fall wurde bereits in der bahnbrechenden Arbeit von Ellingsrud und Skjelbred [15] behandelt. □

In unserem Fall $V \cong V^* = \bigoplus_{i=1}^n \langle X_i, Y_i\rangle$ ist offenbar $\dim V^G = n$, und das einzige $\sigma \in G$ mit $\dim V^\sigma > \dim V^G$ ist das neutrale Element $\sigma = \iota$, von welchem G nicht erzeugt wird. Damit ist der Satz anwendbar und liefert $\operatorname{depth} K[V]^G = \min\{n+2, 2n\}$. Insbesondere gilt dann in (78) Gleichheit, wenn $n \geq 2$ ist.

Was passiert, wenn man q „gegen unendlich“ gehen lässt, also zu der gesamten additiven Gruppe $\mathbb{G}_a = (K, +)$ des Körpers übergeht? $\mathbb{G}_a$ ist nicht reduktiv, und der Hauptsatz nicht anwendbar. Obwohl die Gleichung (78) unabhängig von q ist, gilt sie nun nicht mehr. Stattdessen gilt stets (in beliebiger Charakteristik)

$$\operatorname{cmdef} K\left[\bigoplus_{i=1}^n \langle X_i, Y_i\rangle\right]^{\mathbb{G}_a} = 0,$$

denn nach Roberts' Isomorphismus 1.57 gilt ja die Isomorphie

$$K\left[\bigoplus_{i=1}^n \langle X_i, Y_i\rangle\right]^{\mathbb{G}_a} \cong K\left[\bigoplus_{i=1}^{n+1} \langle X_i, Y_i\rangle\right]^{\mathrm{SL}_2}$$

(wobei auf der rechten Seite $\langle X_i, Y_i\rangle$ die natürliche Darstellung der SL_2 ist), und der rechte Invariantenring ist nach Satz 3.13 Cohen-Macaulay[1]. Das Argument des Hauptsatzes geht dabei deshalb schief, weil dann $X_1, \ldots, X_i$ für $i \geq 3$ kein phsop mehr im Invariantenring bildet.

Wir werden in Satz 4.28 sehen, wie man durch Hinzunahme des Summanden $\langle X_0^p, Y_0^p\rangle$ zu V die Ungleichung (78) auch für die volle additive Gruppe $\mathbb{G}_a$ (in positiver Charakteristik p) retten kann.

[1] Der Invariantenring ist also nicht nach Hochster und Roberts Cohen-Macaulay, sondern nach Hochster und Roberts' Isomorphismus!

4.2 Konstruktion von Darstellungen mit großem Cohen-Macaulay-Defekt des Invariantenrings

Wir geben nun für jede reduktive Gruppe, für die das überhaupt möglich ist, *explizit* eine Folge von Darstellungen an, für die der Cohen-Macaulay-Defekt des zugehörigen Invariantenrings beliebig groß wird.

Satz 4.2 *Sei G eine reduktive, aber nicht linear reduktive Gruppe in positiver Charakteristik $p = \operatorname{char} K$. Wir unterscheiden zwei Fälle:*

1. *Falls die Zusammenhangskomponente G^0 kein Torus ist, so sei V ein treuer G-Modul (existiert nach Satz 1.33),*

   $$U := \operatorname{Hom}_K(S^p(V), F^p(V))_0$$

   (siehe Definition 1.44) und $\iota \in \operatorname{Hom}_K(S^p(V), F^p(V))$ mit $\iota|_{F^p(V)} = \mathrm{id}_{F^p(V)}$.

2. *Falls die Zusammenhangskomponente G^0 ein Torus ist, so teilt p die Ordnung der endlichen Gruppe $H := G/G^0$. (Dies ist insbesondere dann der Fall, wenn G endlich ist. Dann ist $|G^0| = 1$ und H=G). Jeder H-Modul ist auch G-Modul mittels des kanonischen Homomorphismus $G \to H = G/G^0$. Sei dann $V := \oplus_{\sigma\in H} Ke_\sigma$ die reguläre Darstellung von H, also $\sigma e_\tau = e_{\sigma\tau}$ für alle $\sigma, \tau \in H$. Mit $e := \sum_{\sigma\in H} e_\sigma$ betrachte dann*

   $$U := \operatorname{Hom}_K(V, Ke)_0$$

   und $\iota \in \operatorname{Hom}_K(V, Ke)$ mit $\iota|_{Ke} = \mathrm{id}_{Ke}$.

Es sei dann jeweils $g : G \to U$, $\sigma \mapsto (\sigma - 1)\iota$ der zugehörige Kozyklus $g \in Z^1(G, U)$. Weiter sei dann $\tilde{U}$ der zu g und U gehörige erweiterte G-Modul (siehe Abschnitt 1.3), d.h. es ist

$$\tilde{U} = U \oplus K \cdot \iota.$$

Dann gilt

$$\operatorname{cmdef} K \left[U^* \oplus \bigoplus_{i=1}^{k} \tilde{U} \right]^G \geq k - 2.$$

Insbesondere ist der Invariantenring für $k \geq 3$ nicht Cohen-Macaulay.

Beweis. Da G nicht linear reduktiv ist, ist nach Satz 1.37 entweder G^0 kein Torus oder falls doch, p ein Teiler von $|G/G^0|$. Daher tritt einer der beiden Fälle auf. Wenn gezeigt ist, dass der Kozyklus g nichttrivial ist, folgt die Behauptung des Satzes dann sofort aus Korollar 3.7.

Im 1. Fall hat $F^p(V)$ kein Komplement in $S^p(V)$ nach Korollar 1.40.

Im 2. Fall hat Ke kein Komplement in V nach Korollar 1.50.

Daher ist in beiden Fällen nach Proposition 1.46 der Kozyklus g nichttrivial. Dies war zu zeigen. □

Im 2. Fall kann man alternativ auch Satz 3.11 zur Konstruktion verwenden. Es ist z.B. $U \cong (V/Ke)^*$ (siehe Satz 1.44) für $|H| \neq 2$ ein treuer H-Modul mit $H^1(H, U) \neq 0$, und mit $r_0 = 1$ in Satz 3.11 folgt $\operatorname{cmdef} K \left[\bigoplus_{i=1}^{k} U^*\right]^H \geq k - 2$.

Wir berechnen noch die Dimension der Darstellung $M = U^* \oplus \bigoplus_{i=1}^{k} \tilde{U}$.

1. Fall: Es ist $\dim_K S^p(V) = \binom{n+p-1}{p}$, wobei $n = \dim_K V = \dim_K F^p(V)$, also

$$\dim_K U = \dim_K F^p(V)(\dim_K S^p(V) - \dim_K F^p(V)) = n\left(\binom{n+p-1}{p} - n\right).$$

Da $\dim_K \tilde{U} = \dim_K(U) + 1$, ist $\dim_K M = (k+1)\dim_K U + k$, also

$$\dim_K M = n(k+1)\left(\binom{n+p-1}{p} - n\right) + k. \tag{79}$$

Insbesondere für $n = 2$ ist dies

$$\dim_K M = 2(k+1)(p-1) + k.$$

2. Fall: Sei $m := |G/G^0|$. Es ist $\dim_K V = m$, $\dim_K Ke = 1$ und damit $\dim_K U = 1 \cdot (m-1)$, also

$$\dim_K M = (k+1)(m-1) + k. \tag{80}$$

Bemerkung 4.3 Man kann die Dimension von M etwas drücken, denn es ist U von der Form $\mathrm{Hom}_K(V,W)_0 = W \otimes (V/W)^*$ (siehe Satz 1.44). Daher kann man den Summand U^* von M durch $W^* \oplus (V/W)$ ersetzen. Denn dann ist $K[M] = S(M^*) = S(W \oplus (V/W)^* \oplus \ldots)$, und wegen

$$U \cong W \otimes (V/W)^* \leq S^2(W \oplus (V/W)^*) \cong S^2(W) \oplus S^2((V/W)^*) \oplus W \otimes (V/W)^*$$

hat auch hier $S(M^*)$ einen nichttrivialen Kozyklus, der nun Werte in der zweiten symmetrischen Potenz annimmt. Der Beweis von Korollar 3.7 gilt dann weiterhin mit dieser Ersetzung. Im ersten Fall von Satz 4.2 ist außerdem $W^* = F^p(V)^*$ mit V ein treuer G-Modul, der damit als direkter Summand in M auftaucht, so dass dann M auch treu ist; Der Modul U ist dagegen nicht immer treu. Im 2. Fall allein deshalb nicht, weil es sich im Allgemeinen um die Darstellung einer Faktorgruppe handelt. Ein Beispiel für den 1. Fall mit U nicht treu ist gegeben durch $G = \mathrm{SL}_2$ mit natürlicher Darstellung $V = \langle X, Y\rangle$ in Charakteristik 3. Wir werden in Abschnitt 4.5.2 sehen, dass dann $U \cong \langle X, Y\rangle \otimes \langle X^3, Y^3\rangle$ ist, d.h. die Darstellung von U ist gegeben durch

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a^3 & b^3 \\ c^3 & d^d \end{pmatrix} \in K^{4\times 4}$$

(Kronecker Produkt von Matrizen), insbesondere wird das negative der Einheitsmatrix $\sigma = -I_2 \in \mathrm{SL}_2$ auf die Identität $I_4 \in K^{4\times 4}$ abgebildet, d.h. U ist nicht treu. Auch $\tilde{U}$ ist hier nicht treu, wie die Darstellung (89) (S. 111) (wieder für $\sigma = -I_2 \in \mathrm{SL}_2$) zeigt; Siehe auch Bemerkung 3.10 für eine andere Lösung dieses Problems.

Wir formulieren noch kurz das entsprechende explizite Resultat für Vektorinvarianten. Dieses ergibt sich sofort aus Korollar 3.9 (bzw. dem Beweis) und Satz 4.2 zusammen mit der Bemerkung. Wir beschränken uns auf den 1. Fall, der 2. Fall wird genauso behandelt.

Korollar 4.4 *Seien die Voraussetzungen des 1. Falls von Satz 4.2 erfüllt. Dann ist*

$$W := F^p(V)^* \oplus (S^p(V)/F^p(V)) \oplus \tilde{U}$$

ein treuer *G-Modul mit*

$$\operatorname{cmdef} K \left[\bigoplus_{i=1}^{k} W \right]^G \geq k - 2.$$

Der zweite Fall von Satz 4.2 handelt im wesentlichen von endlichen Gruppen. Für diese gibt es in der Literatur bessere Ergebnisse als unser Satz liefert, siehe etwa Satz 4.1 für p-Gruppen. Interessant sind daher für uns die Gruppen, für die der erste Fall zutrifft, für die also die Zusammenhangskomponente kein Torus ist. Insbesondere trifft dies für praktisch alle Klassischen Gruppen zu. Hier die vollständige Übersicht der für die Klassischen Gruppen auftretenden Fälle:

Bemerkung 4.5 *Sei* $\operatorname{char} K = p$, $n \geq 2$.

1. *Die Gruppen* SL_n, GL_n, Sp_n *sind zusammenhängend (n gerade für* Sp_n*) und kein Torus.*
2. *Für* $p \neq 2, n \geq 3$ *ist* SO_n *zusammenhängend, kein Torus und die Zusammenhangskomponente von* O_n*.*
3. *Für* $p \neq 2$, $n = 2$ *ist* SO_2 *ein Torus, die Zusammenhangskomponente von* O_2 *und es ist* $\mathrm{O}_2 / \mathrm{SO}_2 = Z_2$*; insbesondere sind beide Gruppen linear reduktiv.*
4. *Für* $p = 2$ *sind die orthogonalen Gruppen speziell definiert (siehe der folgende Beweis), und es gilt* $\mathrm{SO}_n = \mathrm{O}_n$*. Es ist dann für* $n \geq 3$ *die Zusammenhangskomponente von* SO_n *kein Torus. Ferner ist* SO_2 *semidirektes Produkt eines Torus mit der* Z_2*, und damit nicht linear reduktiv.*

Insbesondere also liefert Satz 4.2 für jede der in $1, 2, 4$ *genannten Gruppen* G *im Fall* $p > 0$ *zu gegebenem* k explizit *eine Darstellung* V *mit* $\operatorname{cmdef} K[V]^G \geq k - 2$.

Für die in 3. *genannten Gruppen dagegen ist jeder Invariantenring Cohen-Macaulay.*

Beweis. Um zu zeigen dass die Zusammenhangskomponente G^0 einer linearen algebraischen Gruppe G kein Torus ist, genügt es, eine nichttriviale, abgeschlossene, zusammenhängende, unipotente Untergruppe $U \subseteq G$ anzugeben. Dann ist nämlich $U \subseteq G^0$, und damit ist G^0 kein Torus. Denn Elemente eines Torus sind halbeinfach, und nur das neutrale Element ist zugleich halbeinfach und unipotent, d.h. man hätte sonst $U = \{\iota\}$. Hierfür genügt es wiederum, einen nichttrivialen algebraischen Homomorphismus $\rho : \mathbb{G}_a \to G$ anzugeben. Denn dann ist $\rho(\mathbb{G}_a) \subseteq G$ eine nichttriviale, zusammenhängende abgeschlossene unipotente Untergruppe ([59, 2.2.5, 2.4.8]).

1. Es sind $\mathrm{SL}_n \subseteq K^{n^2}$ bzw. $\mathrm{GL}_n \subseteq K^{n^2+1}$ Nullstellenmengen der irreduziblen Polynome $\det - 1$ bzw. $E \cdot \det - 1$ (die zu E gehörige Koordinate liefert hier das Inverse der Determinante der zugehörigen Matrix) und damit als Varietäten irreduzibel, also zusammenhängend. Für den Zusammenhang von Sp_n siehe [60, Exercise 2.2.9]. Mit $n = 2m$, $J_2 := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ und $J_{2m} := \operatorname{diag}(J_2, \ldots, J_2) \in K^{2m \times 2m}$ (Blockdiagonalmatrix) ist

$$\mathrm{Sp}_n = \left\{ A \in K^{n \times n} : A^T J_n A = J_n \right\}.$$

Man verifiziert sofort, dass $\mathrm{Sp}_2 = \mathrm{SL}_2$, und mit $A \mapsto \mathrm{diag}(A, I_2, \ldots, I_2) \in K^{n\times n}$ hat man eine Einbettung $\mathrm{SL}_2 \subseteq \mathrm{Sp}_n$ ($I_2 \in K^{2\times 2}$ Einheitsmatrix). Analog hat man Einbettungen $\mathrm{SL}_2 \subseteq \mathrm{SL}_n, \mathrm{GL}_n$. Da

$$\mathbb{G}_a \to \mathrm{SL}_2, \quad a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \tag{81}$$

ein injektiver algebraischer Homomorphismus ist, ist keine der drei zusammenhängenden Gruppen ein Torus.

2. Für den Zusammenhang von SO_n siehe [60, Exercise 2.2.2]. Da $\mathrm{O}_n / \mathrm{SO}_n \cong Z_2$, ist $\mathrm{SO}_n = \mathrm{O}_n^0$. Offenbar hat man eine Einbettung $\mathrm{SO}_3 \subseteq \mathrm{SO}_n$. Mit i einer festen Lösung von $X^2 + 1 = 0$ und $\sqrt{2}$ einer festen Lösung von $X^2 - 2 = 0$ in K prüft man leicht (aber etwas mühsam) nach, dass durch

$$\rho : \mathbb{G}_a \to \mathrm{SO}_3, \quad a \mapsto \begin{pmatrix} 1 & i\sqrt{2}a & \sqrt{2}a \\ -i\sqrt{2}a & 1+a^2 & -ia^2 \\ -\sqrt{2}a & -ia^2 & 1-a^2 \end{pmatrix} \tag{82}$$

ein Homomorphismus gegeben ist, so dass SO_n kein Torus ist.

3. Wir müssen nur noch zeigen, dass SO_2 ein Torus ist. Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SO}_2$. Aus $a^2+b^2 = 1 = a^2+c^2$ folgt $c = \pm b$ und analog $d = \pm a$. Eine kurze Fallunterscheidung zeigt, dass

$$\mathrm{SO}_2 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in K,\, a^2 + b^2 = 1 \right\}.$$

Ist $i = \sqrt{-1}$ ein feste Wurzel von $X^2 + 1 = 0$ in K, so zeigt

$$\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} = \frac{i}{2} \begin{pmatrix} -i & -1 \\ -i & 1 \end{pmatrix} \begin{pmatrix} a+ib & a-ib \\ ia-b & -ia-b \end{pmatrix} =$$

$$= \frac{i}{2} \begin{pmatrix} -ia+b-ia+b & -ia-b+ia+b \\ -ia+b+ia-b & -ia-b-ia-b \end{pmatrix} = \begin{pmatrix} a+ib & 0 \\ 0 & a-ib \end{pmatrix},$$

dass die SO_2 diagonalisierbar ist. Da die $a+ib$ mit $a^2+b^2 = 1$ auch ganz $K\setminus\{0\}$ ausschöpfen (für $t \in K \setminus \{0\}$ setze $a := \frac{1+t^2}{2t}$. Mit $b = \sqrt{1-a^2}$ und geeignetem Vorzeichen ist dann $a + ib = t$), ist $\mathrm{SO}_2 \cong \mathbb{G}_m$ ein Torus. Da $\mathrm{O}_2 / \mathrm{SO}_2 = Z_2$ sind also SO_2 und O_2 für $p \neq 2$ nach Satz 1.37 linear reduktiv.

4. Wir erinnern zunächst an die Definition der orthogonalen Gruppen in Charakteristik 2 (vgl. Carter [10, 1.6]). Für $n = 2m$ betrachte

$$f = X_1X_2 + X_3X_4 + \ldots + X_{n-1}X_n.$$

Für $n = 2m + 1$ betrachte

$$f = X_1X_2 + X_3X_4 + \ldots + X_{n-2}X_{n-1} + X_n^2.$$

Dann ist

$$\mathrm{O}_n = \mathrm{SO}_n = \{\sigma \in \mathrm{GL}_n : f \circ \sigma = f\}.$$

Offenbar hat man Einbettungen $\mathrm{O}_3 \subseteq \mathrm{O}_{2m+1}$ bzw. $\mathrm{O}_4 \subseteq \mathrm{O}_{2m}$ für $m \geq 1$ bzw. $m \geq 2$.

Für O_3 betrachte

$$\rho : \mathbb{G}_a \to \mathrm{GL}_3, \quad a \mapsto \begin{pmatrix} 1 & & \\ a^2 & 1 & \\ a & & 1 \end{pmatrix}. \tag{83}$$

Offenbar ist ρ ein Homomorphismus, und wegen

$$f(\rho(a)(x_1, x_2, x_3)) = f(x_1, a^2x_1 + x_2, ax_1 + x_3) = x_1x_2 + a^2x_1^2 + a^2x_1^2 + x_3^2 = x_1x_2 + x_3^2$$

ist $\rho(a) \in \mathrm{O}_3$. Damit enthält O_{2m+1}^0 eine zusammenhängende unipotente Untergruppe, ist also kein Torus.

Für O_4 betrachte den Homomorphismus

$$\rho : \mathbb{G}_a \to \mathrm{GL}_4, \quad a \mapsto \begin{pmatrix} 1 & & & \\ & 1 & a & \\ & & 1 & \\ a & & & 1 \end{pmatrix}. \tag{84}$$

Es folgt

$$\begin{aligned} f(\rho(a)(x_1, x_2, x_3, x_4)) &= f(x_1, x_2 + ax_3, x_3, ax_1 + x_4) \\ &= x_1x_2 + ax_1x_3 + ax_1x_3 + x_3x_4 = x_1x_2 + x_3x_4, \end{aligned}$$

also auch hier $\rho(a) \in \mathrm{O}_4$, und O_{2m}^0 ist kein Torus für $m \geq 2$.

O_2 schliesslich besteht aus allen Elementen der Form $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ und $\begin{pmatrix} 0 & b \\ -b^{-1} & 0 \end{pmatrix}$, und ist damit isomorph zu $\mathbb{G}_m \rtimes Z_2$.

Jede der in $1, 2, 4$ genannten Gruppen G ist also im Fall $p > 0$ nicht linear reduktiv (Satz 1.37). Außer im Fall SO_2 für $p = 2$ ist nämlich G^0 kein Torus, und da dann jeweils K^n ein treuer G-Modul ist, liefert Satz 4.2 nach Fall 1. zu gegebenem k explizit einen G-Modul V mit $\operatorname{cmdef} K[V]^G \geq k - 2$. Die Gruppe $G = \mathrm{SO}_2$, $p = 2$, für die G^0 ein Torus ist, aber $p = 2$ Teiler von $|G/G^0|$ ist, wird entsprechend von Fall 2. in Satz 4.2 abgedeckt.

Da die Gruppen in 3. linear reduktiv sind, folgt die letzte Aussage aus dem Satz von Hochster und Roberts 1.56. □

4.3 Nichttriviale Kozyklen auf elementarem Weg und Beispiele für endliche Gruppen

Die für unser Konstruktionsverfahren benötigten nichttrivialen Kozyklen hängen im wesentlichen an dem relativ komplizierten Satz von Nagata, Korollar 1.40. Hat man aber eine Gruppe konkret vorgegeben, z.B. SL_n, und dazu einen G-Modul V sowie einen Kozyklus $g \in Z^1(G, V)$, so kann man relativ leicht feststellen, ob ein Kozyklus nichttrivial ist. Man macht dazu für einige $\sigma_i \in G$, $i = 1, \ldots, m$ den Ansatz

$$(\sigma_i - 1)v = g_\sigma, \quad i = 1, \ldots, m,$$

und erhält so ein inhomogenes lineares Gleichungssystem für v. Bei geschickter (meist naheliegender) Wahl der σ_i erhält man dann entweder einen Widerspruch, was dann zeigt, dass g nichttrivial ist, oder eine Lösung v_0 für v (evtl. gibt es mehrere Lösungen). Dann

muss man noch verifizieren, ob allgemein $g_\sigma = (\sigma - 1)v_0$ für alle $\sigma \in G$ gilt, was dann zeigt dass g trivial ist. Ist dies nicht der Fall, so kann man eine andere Lösung probieren oder mittels Erhöhung von m die Lösungen weiter einschränken und von vorne beginnen. Für die Wahl der σ_i ist (falls existent) etwa ein Homomorphismus $\rho : \mathbb{G}_a \to G$ nützlich, und man wählt dann einige Bilder von ρ als die σ_i. Falls N der grösste Grad eines der Polynome in der Koordinatendarstellung von ρ ist, wird man dann $m = N + 2$ wählen (denn ein Polynom vom Grad N ist durch $N + 2$ Werte „überbestimmt“).

In der Praxis führt die skizzierte Heuristik in der Regel schnell zum Ziel.

Im folgenden Satz demonstrieren wir dieses Verfahren für die Kozyklen für die Gruppen $\mathrm{SL}_n, \mathrm{GL}_n$ und Sp_n, die wir gemäß Proposition 1.46 und Korollar 1.40 bereits als nichttrivial erkannt haben. Dazu verwenden wir den Homomorphismus (81). Zusätzlich erhalten wir dabei das Ergebnis, dass der Kozyklus auch bei Einschränkung auf viele endliche Untergruppen $G \subseteq \mathrm{GL}_n$ nichttrivial bleibt. Dies liefert dann in der Regel kleinere Beispiele von G-Moduln V mit $\operatorname{cmdef} K[V]^G \geq k - 2$ als die Konstruktion gemäß Fall 2. in Satz 4.2, wo über die reguläre Darstellung von G gegangen wird.

Um die entsprechenden Resultate für die in 2. und 4. genannten Gruppen von Bemerkung 4.5 zu erhalten (insbesondere also für deren endlichen Untergruppen), kann man die Homomorphismen (82), (83) und (84) verwenden.

Satz 4.6 (Kohls [38]) *Sei* $\operatorname{char} K = p > 0$, $n \geq 2$ *und* G *eine abgeschlossene Untergruppe von* GL_n *mit*

(a) Falls $p = 2$*:* $\begin{pmatrix} 1 & a & \\ & 1 & \\ & & I_{n-2} \end{pmatrix} \in G$ *für wenigstens drei verschiedene Werte von* $a \in K$ *(*$a = 0$ *ist stets ein solcher).*

(b) Falls $p \geq 3$*:* $\begin{pmatrix} 1 & 1 & \\ 0 & 1 & \\ & & I_{n-2} \end{pmatrix} \in G$.

Sei weiter $V = S^p(\langle X_1, \ldots, X_n \rangle)$ *die* p*-te symmetrische Potenz der natürlichen Darstellung von* G*,* $W := F^p(\langle X_1, \ldots, X_n \rangle) \subseteq V$ *die* p*-te Frobenius-Potenz der natürlichen Darstellung und* $U := \operatorname{Hom}_K(V, W)_0$*.*

Sei ferner $\iota \in \operatorname{Hom}_K(V, W)$ *gegeben durch* $\iota|_W = \mathrm{id}_W$ *und* ι *gleich* 0 *auf allen Monomen, die nicht in* W *liegen. Dann ist durch* $g : G \to U$, $\sigma \mapsto g_\sigma := (\sigma - 1)\iota$ *ein nichttrivialer Kozyklus* $g \in Z^1(G, U)$ *gegeben.*

Beweis. Nach Proposition 1.46 ist jedenfalls $g \in Z^1(G, U)$. Wir zeigen $g \notin B^1(G, U)$. Wir wählen dazu für V eine monomiale Basis $\mathcal{B}$, wobei wir die Reihenfolge der ersten $n+1$ bzw. $n + 2$ Monome in den Fällen (a) bzw. (b) vorgeben, und zwar
im Fall (a):

$$\mathcal{B} = \{X_1^2, \ldots, X_n^2, X_1X_2, \ldots\}$$

im Fall (b):

$$\mathcal{B} = \{X_1^p, \ldots, X_n^p, X_1^{p-1}X_2, X_1^{p-2}X_2^2, \ldots\}$$

Als Basis $\mathcal{C}$ von W dienen die ersten n Einträge von $\mathcal{B}$. Sei $N := |\mathcal{B}| = \binom{n+p-1}{p}$. Wir verwenden die folgende **Notation**: Für $A \in K^{n\times N}$ sei $A_{\mathcal{C},\mathcal{B}}$ das Element von $\mathrm{Hom}_K(V,W)$, dass A als Darstellungsmatrix bezüglich der Basen $\mathcal{B}$ von V und $\mathcal{C}$ von W hat. Analog sei für $x \in K^N$ durch $x_{\mathcal{B}}$ das Element von V gegeben, das x als Koordinatenvektor bezüglich der Basis $\mathcal{B}$ von V hat.

Wir bezeichnen mit $f_p : \mathrm{GL}_n(K) \to \mathrm{GL}_n(K)$ den koeffizientenweisen Frobenius-Homomorphismus, also $f_p(a_{ij}) = (a_{ij}^p)$. Ist $A_\sigma \in K^{N\times N}$ die Darstellungsmatrix von $\sigma \in G$ bzgl. der Basis $\mathcal{B}$, so hat diese die Form

$$A_\sigma = \begin{pmatrix} f_p(\sigma) & * \\ 0_{(N-n)\times n} & * \end{pmatrix} \in \mathrm{GL}_N(K).$$

(Dabei schreiben wir $0_{k\times l} \in K^{k\times l}$ für die Nullmatrix, analoges gilt später für $0_k \in K^k$.) Weiter haben wir bzgl. der Basen $\mathcal{C},\mathcal{B}$

$$U = \left\{ \begin{pmatrix} 0_{n\times n} & B \end{pmatrix}_{\mathcal{C},\mathcal{B}} \in K^{n\times N} : B \in K^{n\times(N-n)} \right\},$$

und für $f = \begin{pmatrix} 0_{n\times n} & B \end{pmatrix}_{\mathcal{C},\mathcal{B}}$ haben wir die Operation gegeben durch

$$\sigma \cdot f = \sigma \circ f \circ \sigma^{-1} = \left(f_p(\sigma) \cdot \begin{pmatrix} 0_{n\times n} & B \end{pmatrix} \cdot A_{\sigma^{-1}} \right)_{\mathcal{C},\mathcal{B}}.$$

Die Darstellungsmatrix von ι bzgl. $\mathcal{C},\mathcal{B}$ ist gegeben durch

$$J := \begin{pmatrix} I_n & 0_{n\times(N-n)} \end{pmatrix} \in K^{n\times N}, \text{ also } \iota = J_{\mathcal{C},\mathcal{B}}.$$

Um $g \notin B^1(G,U)$ zu zeigen, gehen wir vor wie im Vorspann beschrieben, d.h. wir nehmen die Existenz eines

$$u = Z_{\mathcal{C},\mathcal{B}} \in U \quad \text{mit } Z = \begin{pmatrix} 0_{n\times n} & \hat{Z} \end{pmatrix} \in K^{n\times N},\ \hat{Z} = (z_{ij}) \in K^{n\times(N-n)}$$

an mit $g_\sigma = (\sigma - 1)\iota = (\sigma - 1)u$ für alle $\sigma \in G$, d.h.

$$f_p(\sigma) J A_{\sigma^{-1}} - J = f_p(\sigma) Z A_{\sigma^{-1}} - Z \quad \text{für alle } \sigma \in G. \tag{85}$$

Wir werden diese Gleichung nun in beiden Fällen zum Widerspruch führen.

(a) Mit

$$\sigma := \begin{pmatrix} 1 & a & & \\ 0 & 1 & & \\ & & I_{n-2} & \end{pmatrix} = \sigma^{-1}, \quad a \in K \text{ so dass } \sigma \in G,$$

berechnen wir die $(n+1)$te Spalte von $A_{\sigma^{-1}}$:

$$\begin{aligned} \sigma^{-1} \cdot X_1 X_2 &= X_1(aX_1 + X_2) \\ &= aX_1^2 + X_1X_2 \\ &= (a, 0_{n-1}, 1, 0_{N-n-1})_{\mathcal{B}}^T. \end{aligned}$$

Nun vergleichen wir auf beiden Seiten von (85) die Einträge in der ersten Zeile und der $(n+1)$ten Spalte:
Linke Seite:

$$(1, a^2, 0_{n-2}) \begin{pmatrix} I_n & 0_{n\times(N-n)} \end{pmatrix} \begin{pmatrix} a \\ 0_{n-1} \\ 1 \\ 0_{N-n-1} \end{pmatrix} = a$$

Rechte Seite:

$$(1, a^2, 0_{n-2}) \begin{pmatrix} 0_{n\times n} & \hat{Z} \end{pmatrix} \begin{pmatrix} a \\ 0_{n-1} \\ 1 \\ 0_{N-n-1} \end{pmatrix} - z_{11} = z_{11} + a^2 z_{21} - z_{11}$$
$$= a^2 z_{21}$$

Mit $c := z_{21}$ und gleichsetzen beider Seiten erhalten wir, dass

$$ca^2 + a = 0$$

für wenigstens drei Werte $a \in K$ gelten muss. Dies ist nicht möglich.

(b) Wir betrachten

$$\sigma = \begin{pmatrix} 1 & 1 & & \\ 0 & 1 & & \\ & & I_{n-2} & \end{pmatrix}, \sigma^{-1} = \begin{pmatrix} 1 & -1 & & \\ 0 & 1 & & \\ & & I_{n-2} & \end{pmatrix} \in G$$

und berechnen die $(n+1)$te und $(n+2)$te Spalte von $A_{\sigma^{-1}}$:
$(n+1)$te Spalte:

$$\begin{aligned} \sigma^{-1} \cdot X_1^{p-1} X_2 &= X_1^{p-1}(-X_1 + X_2) \\ &= -X_1^p + X_1^{p-1} X_2 \\ &= (-1, 0_{n-1}, 1, 0_{N-n-1})_{\mathcal{B}}^T \end{aligned}$$

$(n+2)$te Spalte:

$$\begin{aligned} \sigma^{-1} \cdot X_1^{p-2} X_2^2 &= X_1^{p-2}(X_1^2 - 2X_1X_2 + X_2^2) \\ &= X_1^p - 2X_1^{p-1}X_2 + X_1^{p-2}X_2^2 \\ &= (1, 0_{n-1}, -2, 1, 0_{N-n-2})_{\mathcal{B}}^T \end{aligned}$$

Wir vergleichen wieder beide Seiten von (85):
(i) Erste Zeile, $(n+1)$te Spalte
Linke Seite:

$$\begin{pmatrix} 1 & 1 & 0_{n-2} \end{pmatrix} \begin{pmatrix} I_n & 0_{n\times(N-n)} \end{pmatrix} \begin{pmatrix} -1 \\ 0_{n-1} \\ 1 \\ 0_{N-n-1} \end{pmatrix} = -1$$

Rechte Seite:

$$\begin{pmatrix} 1 & 1 & 0_{n-2} \end{pmatrix} \begin{pmatrix} 0_{n\times n} & \hat{Z} \end{pmatrix} \begin{pmatrix} -1 \\ 0_{n-1} \\ 1 \\ 0_{N-n-1} \end{pmatrix} - z_{11} = z_{11} + z_{21} - z_{11} = z_{21}.$$

Gleichsetzen beider Seiten liefert

$$z_{21} = -1. \tag{86}$$

(ii) Zweite Zeile, $(n+2)$te Spalte
Linke Seite:

$$\begin{pmatrix} 0 & 1 & 0_{n-2} \end{pmatrix} \begin{pmatrix} I_n & 0_{n\times(N-n)} \end{pmatrix} \begin{pmatrix} 1 \\ 0_{n-1} \\ -2 \\ 1 \\ 0_{N-n-2} \end{pmatrix} = 0$$

Rechte Seite:

$$\begin{pmatrix} 0 & 1 & 0_{n-2} \end{pmatrix} \begin{pmatrix} 0_{n\times n} & \hat{Z} \end{pmatrix} \begin{pmatrix} 1 \\ 0_{n-1} \\ -2 \\ 1 \\ 0_{N-n-2} \end{pmatrix} - z_{22} = -2z_{21} + z_{22} - z_{22} = -2z_{21}$$

Da $p \geq 3$ ist $2 \neq 0$, und gleichsetzen beider Seiten liefert

$$z_{21} = 0,$$

im Widerspruch zu (86). □

Eine Matrix (bzw. die zugehörige lineare Abbildung) heißt *Transvektion*, wenn sie die Matrix aus Fall (b) als Jordan-Normalform hat. Offenbar ist $A \in K^{n\times n}$ genau dann eine Transvektion, wenn $\operatorname{rang}(A - I_n) = 1$ und $(A - I_n)^2 = 0$ ist (I_n die Einheitsmatrix). Dies zeigt, dass A genau dann eine Transvektion ist, wenn es Spaltenvektoren $0 \neq u, v \in K^n$ gibt mit $A = I_n + uv^T$ und $v^T u = 0$.

Da die Voraussetzungen in Satz 4.6 natürlich nur bis auf Konjugation in GL_n zu verstehen sind, liefert dieser also (für $p \geq 3$) für jede abgeschlossene Untergruppe $G \subseteq \mathrm{GL}_n$, die eine Transvektion enthält, einen nichttrivialen Kozyklus. Die Nichttrivialität des Kozyklus ist nach Proposition 1.46 äquivalent dazu, dass $W = F^p(X)$ (mit $X = \langle X_1, \ldots, X_n \rangle$) kein Komplement in $V = S^p(X)$ hat. Da Konjugation von G in GL_n lediglich einem Basiswechsel von X entspricht, $F^p(X)$ aber Basisunabhängig ist (vgl. Definition 1.38), sehen wir, dass $F^p(X)$ kein Komplement in $S^p(X)$ hat, wenn G eine Transvektion enthält ($p \geq 3$). Dies erweitert Korollar 1.40.

Definition 4.7 *Ist $G \subseteq \mathrm{GL}_n$ eine abgeschlossene Untergruppe,* $\operatorname{char} K = p > 0$ *und $q = p^m > 1$, so schreiben wir*

$$G(\mathbb{F}_q) := G \cap \mathrm{GL}_n(\mathbb{F}_q) := \{(a_{ij}) \in G : a_{ij}^q - a_{ij} = 0 \quad \textit{für alle } i, j = 1, \ldots, n\},$$

und dies ist dann ebenfalls eine abgeschlossene Untergruppe. Insbesondere sind so $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{Sp}_n(\mathbb{F}_q)$, $\mathrm{SO}_n(\mathbb{F}_q)$, $\mathrm{O}_n(\mathbb{F}_q)$ *über dem Körper K definierte lineare algebraische Gruppen.*

Die Voraussetzungen von Satz 4.6 sind offenbar für die endlichen Gruppen $\mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{Sp}_n(\mathbb{F}_q)$ erfüllt, falls $q \geq 3$ ist, und dieser liefert so einen nichttrivialen Kozyklus. Entsprechendes gilt auch für die Gruppe $(\mathbb{F}_q, +)$ via der Einbettung (81). Korollar 3.7 ist also anwendbar und liefert

Korollar 4.8 *Sei $G \subseteq \mathrm{GL}_n$ eine reduktive Untergruppe, die die Voraussetzungen von Satz 4.6 (bis auf Konjugation in GL_n) erfüllt, z.B. $G = \mathrm{SL}_n(\mathbb{F}_q)$, $\mathrm{GL}_n(\mathbb{F}_q)$, $\mathrm{Sp}_n(\mathbb{F}_q)$,$(\mathbb{F}_q, +)$ für $n \geq 2, q = p^m \geq 3$, oder G enthalte eine Transvektion und $p \geq 3$, oder auch G eine der Gruppen SL_n, GL_n oder Sp_n, oder G eine reduktive Gruppe, die eine dieser Gruppen enthält. Ist dann U der Modul aus Satz 4.6 und $\tilde{U}$ der zu dem nichttrivialen Kozyklus g gehörige erweiterte G-Modul, so ist*

$$\operatorname{cmdef} K \left[U^* \oplus \bigoplus_{i=1}^{k} \tilde{U} \right]^G \geq k - 2.$$

Da hier jeweils $U \subseteq S^2(W \oplus (V/W)^*)$ ist, ist also $W \oplus (V/W)^*$ jeweils ein treuer G-Modul mit $H^1(G, K[W^* \oplus (V/W)]) \neq 0$. Für endliches G ist also auch Satz 3.11 mit $W^* \oplus (V/W)$ (statt V) und $r_0 = 1$ anwendbar.

Wie bereits bemerkt, kann man das Korollar unter geeigneten Voraussetzungen noch auf die Gruppen $\mathrm{SO}_n(\mathbb{F}_q)$ und $\mathrm{O}_n(\mathbb{F}_q)$ (sowie deren reduktiven (z.B. endlichen) Obergruppen) ausdehnen, indem man einen zu Satz 4.6 analogen Satz mit Hilfe des Homomorphismus (82) beweist. Da der Beweis letztlich genauso läuft wie im Fall (a) von Satz 4.6, wollen wir hier darauf verzichten.

Jedenfalls lässt sich Satz 4.6 so wie er dasteht nicht auf orthogonale Gruppen anwenden. Man kann nämlich zeigen, dass orthogonale Gruppen in ungerader Charakteristik überhaupt keine Transvektionen enthalten, und orthogonale Gruppen in gerader Charakteristik keine zwei Transvektionen mit demselben Fixraum enthalten. Dafür geben wir im nächsten Abschnitt eine alternative, elementare Konstruktion von nichttrivialen Kozyklen für gewisse orthogonale Gruppen an, die einfacher, aber weniger allgemein ist.

4.4 Weitere Beispiele für einige orthogonale Gruppen

Der wesentliche Schritt einen nichttrivialen Kozyklus zu konstruieren ist nach Proposition 1.46, einen Untermodul ohne Komplement zu finden. Ist $G = \mathrm{SO}_n$ oder O_n und $V = K^n = \langle X_1, \ldots, X_n \rangle$ die natürliche Darstellung, so bietet sich (abgesehen von $F^p(V) \subseteq S^p(V)$) der von der kanonischen Invariante $X_1^2 + \ldots + X_n^2$ erzeugte Untermodul in $S^2(V)$ an.

Satz 4.9 *Sei* $\operatorname{char} K = p \neq 2$, $G = \mathrm{SO}_n$ *oder* O_n *und $\langle X_1, \ldots, X_n \rangle$ die natürliche Darstellung. Genau dann hat $K \cdot (X_1^2 + \ldots + X_n^2)$ ein Komplement in $S^2(\langle X_1, \ldots, X_n \rangle)$, wenn $p \nmid n$ gilt.*

Beweis. Wir setzen $V := S^2(\langle X_1, \ldots, X_n \rangle)$ und $e := X_1^2 + \ldots + X_n^2 \in V^G$.
„$\Leftarrow$“ Sei $p \nmid n$. Wir behaupten, dass dann

$$U := \langle X_i X_j : i \neq j \rangle_K \oplus \left\{ a_1 X_1^2 + \ldots + a_n X_n^2 : \ a_i \in K, \ a_1 + \ldots + a_n = 0 \right\}$$

ein G-invariantes Komplement zu Ke ist. Offenbar ist $\dim U = \dim V - 1$. Ferner ist $e \notin U$, sonst wäre $1 + \ldots + 1 = n = 0$, aber $p \nmid n$. Also ist $V = Ke \oplus U$. Es ist also nur noch $GU \subseteq U$ zu zeigen. Sei $\sigma = (s_{ij}) \in G$. Dann ist

$$\sigma \cdot X_i X_j = (\text{Terme in } X_k X_l \text{ mit } k \neq l) + \sum_{k=1}^{n} s_{ki} s_{kj} X_k^2.$$

Für $i \neq j$ ist $\sum_{k=1}^n s_{ki}s_{kj} = (\sigma^T\sigma)_{ij} = \delta_{ij} = 0$, und damit $\sigma \cdot X_iX_j \in U$. Ist weiter $a_1 + \ldots + a_n = 0$ mit $a_i \in K$, so gilt

$$\sigma \cdot (a_1X_1^2 + \ldots + a_nX_n^2) = (\text{Terme in } X_kX_l \text{ mit } k \neq l) + \sum_{i=1}^n \sum_{j=1}^n a_j s_{ij}^2 X_i^2 \in U,$$

denn $\sum_{j=1}^n a_j \underbrace{\sum_{i=1}^n s_{ij}^2}_{1} = \sum_{j=1}^n a_j = 0$. Also ist $\sigma U \subseteq U$.

„⇒“ Sei $p|n$. Angenommen, es gäbe einen Untermodul U mit $V = Ke \oplus U$. Wir führen die Annahme durch Induktion zum Widerspruch.

1. $p = n$*:* Sei σ die lineare Fortsetzung der Permutation

$$X_1 \mapsto X_2 \mapsto X_3 \mapsto \ldots \mapsto X_p \mapsto X_1.$$

Dann ist $\sigma \in \mathrm{O}_p$, und wegen $\det\sigma = \mathrm{sgn}(12\ldots p) = (-1)^{p+1} = 1$ ist sogar $\sigma \in \mathrm{SO}_p$ (weil die entsprechende Eigenschaft für gerades n nicht gilt, benötigen wir den Schritt *2.*). Wir betrachten die von σ erzeugte zyklische Untergruppe der Ordnung p, $Z_p := \langle\sigma\rangle \subseteq G$. Dann ist $V = Ke \oplus U$ erst recht eine Zerlegung von Z_p-Moduln $(*)$. Auch $W := \langle X_1^2, \ldots, X_p^2\rangle$ ist ein Z_p-Modul (aber kein G-Modul), der isomorph ist zur regulären Darstellung von Z_p (X_i^2 entspricht e_{σ^i}). Nach Korollar 1.50 hat dann Ke kein Z_p-Komplement in W, also nach Bemerkung 1.45 erst recht nicht in V, im Widerspruch zu $(*)$.

2. $p < n$*:* Sei $n = k + m$ mit $p|k, m$ und $k, m > 0$. Sei $e_1 := X_1^2 + \ldots + X_k^2$ und $e_2 = X_{k+1}^2 + \ldots + X_n^2$. Falls $e_1 \notin U$, so ist wegen $\dim U = \dim V - 1$ dann $V = Ke_1 \oplus U$. Mittels $A \mapsto \mathrm{diag}(A, I_m)$ (I_m die Einheitsmatrix) kann man die Gruppe SO_k in G einbetten, und dann ist $V = Ke_1 \oplus U$ eine Zerlegung in SO_k-Moduln $(*)$. Aber auch $W := S^2(\langle X_1, \ldots, X_k\rangle) \subseteq V$ ist ein SO_k-Untermodul, und wegen $(*)$ und Bemerkung 1.45 hätte Ke_1 dann auch ein SO_k-Komplement in W, im Widerspruch zur Induktionsvoraussetzung. Also ist $e_1 \in U$. Analog folgt $e_2 \in U$ und damit $e = e_1 + e_2 \in U$, im Widerspruch zu $Ke \cap U = \{0\}$. □

Fast genauso beweist man

Satz 4.10 *Sei* $\mathrm{char}\, K = 2$*,* $2|n$*,* $\langle X_1, \ldots, X_{2n}\rangle$ *die natürliche Darstellung der* SO_{2n}*. Dann hat* $K \cdot (X_1X_2 + \ldots + X_{2n-1}X_{2n})$ *kein Komplement in* $S^2(\langle X_1, \ldots, X_{2n}\rangle)$*.*

Beweis. Sei $V := S^2(\langle X_1, \ldots, X_{2n}\rangle)$, $e := X_1X_2 + \ldots + X_{2n-1}X_{2n} \in V$ die SO_{2n} definierende quadratische Form, und $U := \langle X_1X_2, X_3X_4, \ldots, X_{2n-1}X_{2n}\rangle \subseteq V$. Wir betrachten die lineare Fortsetzung σ von $X_i \mapsto X_{i+2}$ (zyklisch). Dann gilt $\sigma \cdot X_{2k-1}X_{2k} = X_{2k+1}X_{2k+2}$, insbesondere $\sigma \cdot e = e$, also $\sigma \in \mathrm{SO}_{2n}$ und U ist die reguläre Darstellung von $Z_n := \langle\sigma\rangle$. Nach Korollar 1.50 hat dann also Ke kein Z_n-Komplement in U, nach Bemerkung 1.45 also auch nicht in V. Dann gibt es aber erst recht kein SO_{2n}-Komplement in V. □

Diese beiden Sätze liefern (mit Proposition 1.46 bzw. der „Quintessenz“, S. 37) also auf elementarem Weg nichttriviale Kozyklen für einige orthogonale Gruppen. Außerdem sind die zugehörigen Moduln von niedrigerer Dimension als diejenigen aus dem Satz von Nagata. Für die Gruppe SO_n mit $p \neq 2$, $p|n$ und dem aus dem vorletzten Satz konstruierten Modul mit Kozyklus U gilt dann etwa für die zugehörige Erweiterung $\tilde{U}$, dass

$\tilde{U}^* = S^2(\langle X_1, \ldots, X_n\rangle)$, also $\dim \tilde{U} = \binom{n+1}{2}$. Bei der Konstruktion nach Nagata dagegen hätte man $\dim \tilde{U} = n\left(\binom{n+p-1}{p} - n\right) + 1$, siehe S. 97, was im Allgemeinen deutlich größer ist. Insbesondere haben dann natürlich auch die nach Korollar 3.7 konstruierten SO_n-Moduln V mit $\operatorname{cmdef} K[V]^{\mathrm{SO}_n} \geq k-2$ eine entsprechend geringere Dimension.

4.5 Die Beispiele für die SL_2 in Charakteristik 2 und 3

Wir wollen hier die nach Satz 4.2 konstruierten SL_2-Moduln V mit $\operatorname{cmdef} K[V]^{\mathrm{SL}_2} \geq k-2$ mit $p = \operatorname{char} K \in \{2,3\}$ genauer untersuchen. Zum einen werden wir V zunächst wie vom Satz geliefert, aber etwas expliziter angeben. Schliesslich ändern wir das Konstruktionsverfahren für V etwas ab, um eine geringere Dimension zu erhalten. Anstatt nämlich wie in Korollar 3.7 einfach $V^* = U \oplus \bigoplus_{i=1}^{k} \tilde{U}^*$ zu setzen, wobei dann jeder Summand $\tilde{U}^*$ einen Annullator a_i enthält, ersetzen wir hier grob gesprochen $\tilde{U}^*$ durch Moduln kleinerer Dimension W, so dass $\tilde{U}^* \subseteq S^2(W)$ gilt. Die Annullatoren a_i des nichttrivialen Kozyklus (mit Werten in U) liegen also hier in der zweiten symmetrischen Potenz. Manchmal enthält $S^2(W)$ sogar gleich mehrere Kopien von $\tilde{U}^*$ und damit auch mehrere Annullatoren. Diese kann man aber nicht immer alle verwenden, denn um den Hauptsatz 3.6 anzuwenden, müssen sie zusätzlich noch ein phsop im Polynomring bilden, d.h. man muss eine geschickte Auswahl treffen. Wie wir außerdem bereits gesehen haben (siehe Bemerkung 4.3), kann man auch den Kozyklus in die zweite symmetrische Potenz bringen, um die Dimension von V zu verringern.

Für die hier dargestellten Ergebnisse benötigen wir Resultate, die sich in meiner Diplomarbeit [37] und in dem daraus entstandenen Artikel [38] finden. In diesen Arbeiten ging es darum, nicht Cohen-Macaulay Invariantenringe zu konstruieren; Mit dem Hauptsatz können wir nun auch noch den Cohen-Macaulay-Defekt gegen unendlich treiben. Die in diesem Abschnitt dargestellten Ergebnisse verschärfen also die Resultate aus [37] und [38]. Sämtliche hier weggelassenen Zwischenrechungen (die zwar alle einfach, aber teilweise doch umfangreich sind), finden sich in [37, Abschnitt 6].

Wir beschränken uns hier der Einfachheit halber auf die Gruppe SL_2. Sämtliche Ergebnisse gehen natürlich auch für reduktive Untergruppen der SL_2 durch, die die entsprechende Voraussetzung aus Satz 4.6 erfüllen, z.B. endliche $\mathrm{SL}_2(\mathbb{F}_q)$ wobei q entsprechend eine 2- oder 3-Potenz ist. In den Arbeiten [37] bzw. [38] habe ich außerdem gezeigt, wie man durch „Tensorieren mit dem Inversen der Determinante“ die betrachteten SL_2-Moduln zu GL_2-Moduln machen kann, so dass auch hier die Ergebnisse mit etwas Modifikation durchgehen.

Wir erinnern nochmal an die auf S. 27 eingeführte **Notation.** Mit $\langle X, Y\rangle$ bezeichnen wir die natürliche Darstellung der SL_2. Mit $\sigma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2$ gilt dann also

$$\sigma \cdot X = aX + cY, \quad \sigma \cdot Y = bX + dY.$$

Wenn wir diese Operation entsprechend auf homogene Polynome in X und Y fortsetzen, erhalten wir die Operation auf den symmetrischen Potenzen

$$S^k(\langle X, Y\rangle) =: \langle X^k, X^{k-1}Y, \ldots, XY^{k-1}, Y^k\rangle.$$

Um Matrizen bezüglich gegebener Basen lineare Abbildungen zuzuordnen, verwenden wir die Notation, die wir im Beweis von Satz 4.6 eingeführt haben.

Die natürliche Darstellung der SL_2 ist selbstdual (für beliebige Charakteristik), genauer haben $\langle X, Y\rangle^* = \langle X^*, Y^*\rangle$ (mit Dualbasis) und $\langle Y, -X\rangle$ die gleiche Darstellung.

4.5.1 Charakteristik 2

Wir gehen die Konstruktion nach Satz 4.2 Schritt für Schritt durch. Da SL_2^0 kein Torus ist, benötigen wir zunächst einen treuen SL_2-Modul und wählen $V = \langle X, Y\rangle$. Dann ist

$$\begin{aligned} S^2(V) &= \langle X^2, Y^2, XY\rangle, \\ F^2(V) &= \langle X^2, Y^2\rangle. \end{aligned}$$

Wir schreiben $\mathcal{B}$ und $\mathcal{C}$ für die beiden gegebenen Basen. Die Darstellungen der beiden Moduln bezüglich dieser Basen sind dann gegeben durch

$$\sigma \mapsto \begin{pmatrix} a^2 & b^2 & ab \\ c^2 & d^2 & cd \\ 0 & 0 & 1 \end{pmatrix} \text{ und } \sigma \mapsto \begin{pmatrix} a^2 & b^2 \\ c^2 & d^2 \end{pmatrix}.$$

Gemäß Satz 4.2 betrachten wir den Modul $U := \mathrm{Hom}_K(S^2(V), F^2(V))_0$. Dessen Elemente (gewisse lineare Abbildungen) werden bezüglich der Basen $\mathcal{B}$ und $\mathcal{C}$ durch 2×3 Matrizen beschrieben, die nur in der letzten Spalte von Null verschiedene Einträge haben. Mit dieser Beschreibung erhält man dann (bei naheliegender Basiswahl), dass eine Darstellung von U durch $\sigma \mapsto \begin{pmatrix} a^2 & b^2 \\ c^2 & d^2 \end{pmatrix}$ gegeben ist. Damit ist $U \cong \langle X^2, Y^2\rangle$, und wir identifizieren im Folgenden $\langle X^2, Y^2\rangle$ mit U. Als nächstes brauchen wir ein wie in Satz 4.2 gefordertes ι, und wir wählen natürlich $\iota = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}_{\mathcal{C},\mathcal{B}}$. Für die Operation von SL_2, angewendet auf ι erhalten wir dann mit obiger Identifikation $\sigma\iota = abX^2 + cdY^2 + \iota$. Damit ist die Operation auf $\tilde{U} = U \oplus K\iota = \langle X^2, Y^2, \iota\rangle$ gegeben durch $\sigma \mapsto \begin{pmatrix} a^2 & b^2 & ab \\ c^2 & d^2 & cd \\ 0 & 0 & 1 \end{pmatrix}$, also $\tilde{U} = \langle X^2, Y^2, XY\rangle$, wobei wir XY mit ι identifiziert haben. Der nichttriviale Kozyklus in $Z^1(\mathrm{SL}_2, U)$ ist dann gegeben durch $g_\sigma = (\sigma - 1)\iota = (\sigma - 1)XY$. Da $U = \langle X^2, Y^2\rangle$ mit $\langle X, Y\rangle$ selbstdual ist, liefert Satz 4.2 sofort:

Beispiel 4.11 *Sei* $\mathrm{char}\, K = 2$ *und* $\langle X, Y\rangle$ *die natürliche Darstellung der* SL_2. *Dann gilt*

$$\mathrm{cmdef}\, K \left[\langle X^2, Y^2\rangle \oplus \bigoplus_{i=1}^{k} \langle X^2, Y^2, XY\rangle\right]^{\mathrm{SL}_2} \geq k - 2.$$

Die Dimension des Invariantenringes ist nach Bemerkung 1.70 gegeben durch $3k - 1$. (Der zugrundeliegende Modul ist weder selbstdual noch vollständig reduzibel, da er $\tilde{U}$ als Summanden enthält).

Wir versuchen nun, $\tilde{U}^*$ in einer zweiten symmetrischen Potenz wiederzufinden. Wir verwenden folgende Notation für die zugehörige Dualbasis:

$$\mu := (X^2)^*, \nu := (Y^2)^*, \pi := (XY)^*, \text{ also } \tilde{U}^* = \langle \mu, \nu, \pi\rangle.$$

Dann ist π die den Kozyklus g annullierende Invariante gemäß Proposition 1.51. Die Darstellung von $\tilde{U}^*$ bezüglich dieser Basis ist gegeben durch

$$\sigma \mapsto \begin{pmatrix} a^2 & b^2 & ab \\ c^2 & d^2 & cd \\ 0 & 0 & 1 \end{pmatrix}^{-T} = \begin{pmatrix} d^2 & c^2 & 0 \\ b^2 & a^2 & 0 \\ bd & ac & 1 \end{pmatrix}. \tag{87}$$

Wir betrachten nun das Tensorprodukt der natürlichen Darstellung mit sich selbst, $\langle X, Y\rangle \otimes \langle X, Y\rangle$, und berechnen seine Darstellung bezüglich der Basis $\{Y \otimes Y, X \otimes X, X \otimes Y - Y \otimes X, Y \otimes X\}$ zu

$$\sigma \mapsto \begin{pmatrix} d^2 & c^2 & 0 & cd \\ b^2 & a^2 & 0 & ab \\ bd & ac & 1 & bc \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Da die linke obere 3×3 Block-Matrix aber die Darstellung von $\langle \mu, \nu, \pi\rangle$ ist, siehe (87), haben wir also (bis auf Isomorphie)

$$\langle \mu, \nu, \pi\rangle \subseteq \langle X, Y\rangle \otimes \langle X, Y\rangle \subseteq S^2\left(\langle X_1, Y_1\rangle \oplus \langle X_2, Y_2\rangle\right).$$

Dabei entspricht dann $X_1Y_2 - X_2Y_1$ der annullierenden Invariante π des Kozyklus g. Hat man nun die k-fache direkte Summe der natürlichen Darstellung, so liegen in ihrer zweiten Potenz offenbar $\binom{k}{2}$ solche Annullatoren. Wir werden in Lemma 4.13 zeigen, dass $k-1$ von ihnen ein phsop im Polynomring bilden. Damit haben wir nach dem Hauptsatz 3.6 (mit $k-1$ statt k)

Beispiel 4.12 *Ist* $\operatorname{char} K = 2$ *und* $\langle X, Y\rangle$ *die natürliche Darstellung der* SL_2*, so gilt*

$$\operatorname{cmdef} K\left[\langle X^2, Y^2\rangle \oplus \bigoplus_{i=1}^{k} \langle X, Y\rangle\right]^{\mathrm{SL}_2} \geq k - 3.$$

Die Dimension des Invariantenringes ist $2k-1$ nach Korollar 1.69.

Bemerkenswert ist, dass der hier auftretende, treue SL_2-Modul selbstdual ist (als direkte Summe selbstdualer Moduln), und außerdem noch vollständig reduzibel (als Summe irreduzibler Moduln). K.N. Raghavan stellte in einer E-Mail an Gregor Kemper die Frage, ob ein vollständig reduzibler G-Modul V mit nicht Cohen-Macaulay Invariantenring $K[V]^G$ existiert. Mit diesem Beispiel lautet die Antwort also „Ja“.

Mit ziemlichem Aufwand werden wir dieses Beispiel im nächsten Abschnitt (mit fast völlig anderer Methode) auf Charakteristik p verallgemeinern.

Es fehlt noch das versprochene phsop im Polynomring:

Lemma 4.13 *Es sei* $\operatorname{char} K$ *beliebig und* $R = K[X_1, Y_1, \ldots, X_n, Y_n]$ *der Polynomring in* $2n$ *Variablen. Mit*

$$g_{ij} := X_iY_j - X_jY_i$$

ist $G := \{g_{12}, g_{23}, g_{34}, \ldots, g_{n-1,n}\}$ *ein phsop in* R *der Länge* $n-1$ *.*

Beweis. Wir zeigen zunächst, dass G eine Gröbner-Basis des Ideals $I := (G)$ ist, und zwar bezüglich graduierter lexikographischer Ordnung mit

$$X_1 > Y_1 > X_2 > Y_2 > \ldots > X_n > Y_n.$$

Für $f \in R$ bezeichnen wir mit $\mathrm{LM}(f)$ das *Leitmonom* (normiert) von f bezüglich dieser Ordnung. Offenbar ist

$$\mathrm{LM}(g_{i,i+1}) = X_i Y_{i+1}.$$

Gemäß dem Buchberger-Kriterium (Eisenbud [14, Theorem 15.8]) müssen wir zeigen, dass der Divisionsalgorithmus [14, Division Algorithm 15.7] bzgl. G, angewendet auf die *s-Polynome*

$$\mathrm{spol}(g_{i,i+1}, g_{j,j+1}) = \mathrm{LM}(g_{j,j+1}) g_{i,i+1} - \mathrm{LM}(g_{i,i+1}) g_{j,j+1}$$

für $1 \leq i, j \leq n-1$ jeweils ohne Rest aufgeht. Aufgrund der Struktur unserer Monomordnung können wir O.E. $i = 1$, $j > 1$ annehmen. Es ist dann also

$$\begin{aligned} r_0 := \mathrm{spol}(g_{12}, g_{j,j+1}) &= X_j Y_{j+1}(X_1 Y_2 - X_2 Y_1) - X_1 Y_2 (X_j Y_{j+1} - X_{j+1} Y_j) \\ &= X_1 Y_2 X_{j+1} Y_j - X_2 Y_1 X_j Y_{j+1}. \end{aligned}$$

Es wird $\mathrm{LM}(r_0) = X_1 Y_2 X_{j+1} Y_j$ von $\mathrm{LM}(g_{12})$ geteilt, also

$$r_1 := r_0 - X_{j+1} Y_j (X_1 Y_2 - X_2 Y_1) = X_2 Y_1 X_{j+1} Y_j - X_2 Y_1 X_j Y_{j+1}.$$

Schliesslich wird $\mathrm{LM}(r_1) = X_2 Y_1 X_j Y_{j+1}$ von $\mathrm{LM}(g_{j,j+1})$ geteilt, und es ist

$$r_2 := r_1 + X_2 Y_1 (X_j Y_{j+1} - X_{j+1} Y_j) = 0,$$

also ist G eine Gröbner-Basis.

Für eine Menge $M \subseteq \{X_1, Y_1, \ldots, X_n, Y_n\}$ minimaler Mächtigkeit mit der Eigenschaft, dass für alle $g_{i,i+1} \in G$ das Leitmonom $\mathrm{LM}(g_{i,i+1}) = X_i Y_{i+1}$ wenigstens eine Variable aus M enthält, gilt offenbar $|M| = n-1$ (z.B. $M = \{X_1, \ldots, X_{n-1}\}$), denn keine Variable kommt in zwei Leitmonomen $\mathrm{LM}(g_{i,i+1})$, $\mathrm{LM}(g_{j,j+1})$ mit $i \neq j$ gleichzeitig vor. Nach [12, Algorithm 1.2.4] gilt dann $\dim I = 2n - |M|$ und damit $\mathrm{height}\, I = |M| = n-1$. Also ist G ein phsop nach Lemma 1.5. □

4.5.2 Charakteristik 3

Wir gehen wieder Schritt für Schritt Satz 4.2 durch, wobei wir wieder die natürliche Darstellung $V = \langle X, Y \rangle$ als treue Darstellung verwenden. Dann ist

$$\begin{aligned} S^3(V) &= S^3(\langle X, Y \rangle) = \langle X^3, Y^3, X^2 Y, X Y^2 \rangle && \text{mit Basis } \mathcal{B} \\ \text{und } F^3(V) &= \langle X^3, Y^3 \rangle && \text{mit Basis } \mathcal{C}. \end{aligned}$$

Mit $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K)$, erhalten wir die Darstellung von $S^3(V)$ bezüglich der Basis $\mathcal{B}$ zu

$$\sigma \mapsto A_\sigma = \begin{pmatrix} a^3 & b^3 & a^2 b & a b^2 \\ c^3 & d^3 & c^2 d & c d^2 \\ 0 & 0 & a & -b \\ 0 & 0 & -c & d \end{pmatrix}.$$

Die linke obere Block-Matrix gibt dabei die Darstellung von $F^3(V)$ und die rechte untere Block-Matrix diejenige von $S^3(V)/F^3(V)$. Transponieren und auswerten bei σ^{-1} liefert die

Darstellung von $(S^3(V)/F^3(V))^*$, wir erhalten $\sigma \mapsto \begin{pmatrix} d & c \\ b & a \end{pmatrix}$, und das ist die Darstellung von $\langle Y, X\rangle$. Es gilt also $(S^3(V)/F^3(V))^* \cong \langle X, Y\rangle$, und für den Modul U mit nichttrivialem Kozyklus aus Satz 4.2 erhalten wir

$$U := \mathrm{Hom}_K(S^3(V), F^3(V))_0 \cong F^3(V) \otimes (S^3(V)/F^3(V))^* = \langle X^3, Y^3\rangle \otimes \langle X, Y\rangle.$$

Gemäß Bemerkung 4.3 werden wir später U durch $\langle X^3, Y^3\rangle \oplus \langle X, Y\rangle$ ersetzen, so dass unser nichttrivialer Kozyklus dann in Grad 2 liegt. Wir berechnen nun die Darstellungen von U und $\tilde{U}$. Die Elemente von $U = \{f \in \mathrm{Hom}_K(S^3(V), F^3(V)) : f|_{F^3(V)} = 0\}$ werden bezüglich der Basen $\mathcal{B}$ und $\mathcal{C}$ durch Darstellungsmatrizen der Form $\begin{pmatrix} 0 & 0 & x_1 & x_2 \\ 0 & 0 & x_3 & x_4 \end{pmatrix}$ beschrieben. Die zugehörige Operation von G erhalten wir dann durch

$$\sigma \cdot \begin{pmatrix} 0 & 0 & x_1 & x_2 \\ 0 & 0 & x_3 & x_4 \end{pmatrix} = \begin{pmatrix} a^3 & b^3 \\ c^3 & d^3 \end{pmatrix} \begin{pmatrix} 0 & 0 & x_1 & x_2 \\ 0 & 0 & x_3 & x_4 \end{pmatrix} A_{\sigma^{-1}}.$$

Bei dieser Operation spielt nur der rechte untere Block von $A_{\sigma^{-1}}$ eine Rolle, d.h. wir können die Operation auch durch

$$\sigma \cdot \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} a^3 & b^3 \\ c^3 & d^3 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \begin{pmatrix} d & c \\ b & a \end{pmatrix}^T$$

beschreiben. Aber dies ist eine Darstellung von $\langle X^3, Y^3\rangle \otimes \langle Y, X\rangle$, wobei die Koordinaten $(x_1, x_2, x_3, x_4)^T$ ihre Entsprechung in $x_1X^3 \otimes Y + x_2X^3 \otimes X + x_3Y^3 \otimes Y + x_4Y^3 \otimes X$ haben. Bezüglich dieser Koordinaten ist die Darstellung von U gegeben durch

$$\sigma \mapsto \begin{pmatrix} a^3 & b^3 \\ c^3 & d^3 \end{pmatrix} \otimes \begin{pmatrix} d & c \\ b & a \end{pmatrix} = \begin{pmatrix} a^3d & a^3c & b^3d & b^3c \\ a^3b & a^4 & b^4 & ab^3 \\ c^3d & c^4 & d^4 & cd^3 \\ bc^3 & ac^3 & bd^3 & ad^3 \end{pmatrix}. \tag{88}$$

Dies ist zugleich die Darstellung des Untermoduls $\langle X^3Y, X^4, Y^4, XY^3\rangle$ von $S^4(\langle X, Y\rangle)$, wie man leicht anhand des durch $X^3 \otimes Y \mapsto X^3Y,\ X^3 \otimes X \mapsto X^4,\ Y^3 \otimes Y \mapsto Y^4,\ Y^3 \otimes X \mapsto XY^3$ gegebenen Isomorphismus sieht.
Nun benötigen wir noch die Darstellung des Kozyklus, den wir gemäß Satz 4.2 aus

$$\sigma \cdot \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & -ab(ad+bc) & a^2b^2 \\ 0 & 1 & c^2d^2 & -cd(ad+bc) \end{pmatrix}$$

erhalten. Der rechte 2×2 Block enthält die Koordinaten von g_σ, also

$$g_\sigma = (-ab(ad+bc), a^2b^2, c^2d^2, -cd(ad+bc))^T.$$

Zusammen mit der Darstellung (88) von U erhalten wir so als Darstellung von $\tilde{U}$:

$$\sigma \mapsto \begin{pmatrix} a^3d & a^3c & b^3d & b^3c & -ab(ad+bc) \\ a^3b & a^4 & b^4 & ab^3 & a^2b^2 \\ c^3d & c^4 & d^4 & cd^3 & c^2d^2 \\ bc^3 & ac^3 & bd^3 & ad^3 & -cd(ad+bc) \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{89}$$

Man kann g als Kozyklus mit Werten in $\langle X^3Y, X^4, Y^4, XY^3\rangle$ interpretieren. Dazu berechnen wir in $S^4(\langle X, Y\rangle)$

$$\sigma \cdot X^2Y^2 \quad = \quad -ab(ad+bc)X^3Y + a^2b^2X^4 + c^2d^2Y^4 - cd(ad+bc)XY^3 + X^2Y^2,$$

d.h. g entspricht dem Kozyklus $\sigma \mapsto (\sigma - 1)X^2Y^2$. Wir fassen zusammen:

Lemma 4.14 *Zu dem Untermodul* $U := \langle X^4, X^3Y, XY^3, Y^4\rangle$ *von*

$$\tilde{U} = \langle X^4, X^3Y, X^2Y^2, XY^3, Y^4\rangle = S^4\left(\langle X, Y\rangle\right)$$

existiert ein nichttrivialer Kozyklus $g \in Z^1(\mathrm{SL}_2, U)$*, der durch* $g_\sigma := (\sigma - 1)X^2Y^2$ *gegeben ist. Es gilt*

$$U \cong \langle X^3, Y^3\rangle \otimes \langle X, Y\rangle \subseteq S^2\left(\langle X^3, Y^3\rangle \oplus \langle X, Y\rangle\right).$$

U ist mit seinen Faktoren $\langle X^3, Y^3\rangle$ und $\langle X, Y\rangle$ selbstdual. Eine Darstellung von $\tilde{U}$ ist durch (89) gegeben.

Korollar 3.7 liefert nun sofort

Beispiel 4.15 *Ist* $\operatorname{char} K = 3$ *und* $\langle X, Y\rangle$ *die natürliche Darstellung der* SL_2*, so gilt*

$$\operatorname{cmdef} K \left[\langle X^3, Y^3\rangle \oplus \langle X, Y\rangle \oplus \bigoplus_{i=1}^{k} S^4\left(\langle X, Y\rangle\right)\right]^{\mathrm{SL}_2} \geq k - 2.$$

Die Dimension des Invariantenringes ist $5k + 1$ nach Korollar 1.69. (Der zugrundeliegende Modul ist weder selbstdual noch vollständig reduzibel, da er $\tilde{U}$ als Summanden enthält).

Wir wollen dieses Beispiel noch etwas vereinfachen (insbesondere die Dimension reduzieren), indem wir $\tilde{U}^*$ als Untermodul einer zweiten symmetrischen Potenz zu finden versuchen. Dazu berechnen wir zunächst die Darstellung von $\tilde{U}^*$, in dem wir (89) invertieren (d.h bei σ^{-1} auswerten) und transponieren. Wir erhalten

$$\sigma \mapsto \begin{pmatrix} ad^3 & -bd^3 & -ac^3 & bc^3 & 0 \\ -cd^3 & d^4 & c^4 & -c^3d & 0 \\ -ab^3 & b^4 & a^4 & -a^3b & 0 \\ b^3c & -b^3d & -a^3c & a^3d & 0 \\ bd(ad+bc) & b^2d^2 & a^2c^2 & ac(ad+bc) & 1 \end{pmatrix}. \tag{90}$$

Diese Darstellung ist bezüglich einer Basis gegeben, die als letztes Element die annullierende Invariante π gemäß Proposition 1.51 enthält.
Wir betrachten nun den Modul $M := \langle X^2, Y^2, XY\rangle$. Eine kurze Berechnung der Darstellung zeigt, dass M selbstdual ist. Da M keinen eindimensionalen Untermodul enthält, ist M dann auch irreduzibel. Nun berechnen wir die Darstellung von

$$S^2(M) = \langle (XY)Y^2, -(Y^2)^2, -(X^2)^2, (XY)X^2, X^2Y^2 - (XY)^2, (XY)^2\rangle$$

bezüglich der angegebenen Basis (man beachte, dass man hier zwischen $(XY)^2$ und X^2Y^2 unterscheiden muss!). Eine etwas längliche, aber einfache Rechnung zeigt, dass die Darstellung von $S^2(M)$ durch

$$\sigma \mapsto \begin{pmatrix} ad^3 & -bd^3 & -ac^3 & bc^3 & 0 & -cd(ad+bc) \\ -cd^3 & d^4 & c^4 & -c^3d & 0 & -c^2d^2 \\ -ab^3 & b^4 & a^4 & -a^3b & 0 & -a^2b^2 \\ b^3c & -b^3d & -a^3c & a^3d & 0 & -ab(ad+bc) \\ bd(ad+bc) & b^2d^2 & a^2c^2 & ac(ad+bc) & 1 & -abcd \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{91}$$

gegeben ist. Vergleichen wir diese mit der Darstellung (90), so erkennen wir $\tilde{U}^*$ als Untermodul von $S^2(\langle X^2, Y^2, XY\rangle)$, wobei die annullierende Invariante π ihre Entsprechung in $X^2Y^2 - (XY)^2$ hat. Die folgende Bemerkung zeigt, dass k Kopien von ihnen ein phsop im Polynomring liefern:

Bemerkung 4.16 *Seien $V_1, \ldots, V_k$ G-Moduln, $V = V_1 \oplus \ldots \oplus V_k$ und $0 \neq f_i \in S^{d_i}(V_i) \subseteq S(V)$, $i = 1, \ldots, k$ (mit $d_i \geq 1$). Dann bilden $f_1, \ldots, f_k$ ein phsop in $S(V)$.*

Beweis. Da $S(V_i)$ ein Polynomring und $f_i \neq 0$ ist, ist $\mathrm{height}(f_i)_{S(V_i)} = 1$. Also ist f_i ein phsop in $S(V_i)$, und man kann dies zu einem hsop $f_{i1} := f_i, f_{i2}, \ldots, f_{in_1}$ (mit $n_i = \dim V_i$) von $S(V_i)$ ergänzen. Dann ist $f_{11}, \ldots, f_{kn_k}$ ein hsop von $S(V)$. Denn es hat die Mächtigkeit $n_1 + \ldots + n_k = \dim S(V)$, und $S(V)$ ist ganz über $K[f_{11}, \ldots, f_{kn_k}]$, da dies offenbar für die ($S(V)$ erzeugenden) Elemente von Basen von $S^1(V_i)$ gilt. □

Der Hauptsatz 3.6 liefert nun sofort

Beispiel 4.17 *Ist* $\mathrm{char}\, K = 3$ *und* $\langle X, Y\rangle$ *die natürliche Darstellung der* SL_2*, so ist*

$$\mathrm{cmdef}\, K \left[\langle X, Y\rangle \oplus \langle X^3, Y^3\rangle \oplus \bigoplus_{i=1}^{k} \langle X^2, Y^2, XY\rangle\right]^{\mathrm{SL}_2} \geq k - 2.$$

Der hier auftretende Modul ist selbstdual und vollständig reduzibel als direkte Summe selbstdualer, irreduzibler Moduln.

Die Dimension des Invariantenrings ist $3k + 1$ nach Korollar 1.69.

4.6 Beispiele für SL_2 und $\mathbb{G}_a$ in beliebiger positiver Charakteristik

In diesem Abschnitt sei stets $p = \mathrm{char}\, K > 0$.

Die von Satz 4.2 gelieferten SL_2-Moduln V mit $\mathrm{cmdef}\, K[V]^{\mathrm{SL}_2} \geq k-2$ haben eine mit der Charakteristik p schnell wachsende Dimension, siehe Gleichung (79) (S. 97). Auch im vorigen Abschnitt hatten die Moduln für Charakteristik 3 größere Dimension als für Charakteristik 2. In diesem Abschnitt werden wir Beispiel 4.12 auf beliebige Charakteristik $p > 0$ verallgemeinern, und so Darstellungen erhalten, deren Dimension nicht von p abhängt. Unser Vorgehen wird folgendes sein: Wir geben einen nichttrivialen Kozyklus und Annullatoren für die additive Gruppe an. Die Urbilder der Annullatoren unter Roberts' Isomorphismus bilden ein phsop im Polynomring, also auch im entsprechenden SL_2-Invariantenring. Nochmals Roberts' Isomorphismus angewandt zeigt, dass die Annullatoren auch ein phsop im $\mathbb{G}_a$-Invariantenring bilden. Der Hauptsatz in der allgemeineren Fassung liefert die Aussage über den Cohen-Macaulay-Defekt für den $\mathbb{G}_a$-Invariantenring. Ein letztes Mal Roberts' Isomorphismus angewendet liefert die Aussage für den SL_2-Invariantenring.

Um diese auf den ersten Blick vielleicht unnötig kompliziert erscheinende Methode zu rechtfertigen, zeigen wir kurz die Probleme auf, die beim Versuch der Verallgemeinerung etwa gemäß dem letzten Abschnitt entstehen.

4.6.1 Wo's hakt

In Charakteristik 2 hatten wir durch $g_\sigma = (\sigma - 1)XY$ einen nichttrivialen Kozyklus in $Z^1(\mathrm{SL}_2, \langle X^2, Y^2\rangle)$. In beliebiger Charakteristik liegt jedoch $(\sigma - 1)XY = abX^2 + cdY^2 + (ad + bc)XY$ im Allgemeinen nicht mehr in $\langle X^2, Y^2\rangle$. Eine Verallgemeinerung auf einen Kozyklus in $Z^1(\mathrm{SL}_2, \langle X^p, Y^p\rangle)$ liegt nicht auf der Hand.

Ein weiterer naheliegender Ansatz wäre, von der Invariante $X \otimes Y - Y \otimes X \in \langle X, Y\rangle \otimes \langle X, Y\rangle$ auszugehen. Diese hat jedoch für $p \neq 2$ ein Komplement (d.h. der durch Übergang zum Dual erhaltene Kozyklus ist trivial), wie folgende Überlegung zeigt: $\langle X, Y\rangle$ ist selbstdual, und der Dual hat die Darstellung $\sigma \mapsto \sigma^{-T}$. Bezüglich einer Koordinatenmatrix $C \in K^{2\times 2}$, die ein Element aus $\langle X, Y\rangle \otimes \langle Y, -X\rangle$ darstellt, ist die Operation dann gegeben durch $\sigma \cdot C = \sigma C(\sigma^{-T})^T = \sigma C \sigma^{-1}$, also durch Konjugation. Die Einheitsmatrix I_2 ist invariant und entspricht genau dem Element $X \otimes Y - Y \otimes X$. In Charakteristik 2 gilt $\operatorname{Spur} I_2 = 0$. In Charakteristik $p \neq 2$ dagegen ist $\operatorname{Spur} I_2 \neq 0$, und die Matrizen mit Spur 0 bilden ein SL_2-invariantes Komplement zu KI_2.

4.6.2 Charakteristik-p-Relationen von Binomialkoeffizienten

Wir beginnen mit einigen Charakteristik-p-Relationen von Binomialkoeffizienten.

Lemma 4.18 *Sei* $\operatorname{char} K = p > 0$. *Dann gilt für* $0 \leq i < p$ *bzw.* $0 \leq i \leq j < p$ *in* K

(a) $i! = (-1)^i \frac{(p-1)!}{(p-1-i)!}$.

(b) $\binom{j}{i} = (-1)^{i+j}\binom{p-1-i}{p-1-j}$.

(c) $\binom{p-1}{i} = (-1)^i$.

Beweis. (a) Es gilt

$$\begin{aligned} i! &= i(i-1)(i-2)\cdot\ldots\cdot 3\cdot 2\cdot 1 \\ &= (-1)^i(p-i)(p-i+1)(p-i+2)\cdot\ldots\cdot(p-3)(p-2)(p-1) \\ &= (-1)^i\frac{(p-1)!}{(p-1-i)!}. \end{aligned}$$

(b) Mit (a) gilt

$$\begin{aligned} \binom{j}{i} &= \frac{j!}{i!(j-i)!} = \frac{(-1)^j\frac{(p-1)!}{(p-1-j)!}}{(-1)^i\frac{(p-1)!}{(p-1-i)!}\cdot(j-i)!} \\ &= (-1)^{i+j}\frac{(p-1-i)!}{(p-1-j)!(j-i)!} = (-1)^{i+j}\binom{p-1-i}{p-1-j}. \end{aligned}$$

(c) Wir verwenden (b) mit $j = p-1$:

$$\binom{p-1}{i} = (-1)^{i+p-1}\binom{p-1-i}{p-1-(p-1)} = (-1)^i\binom{p-1-i}{0} = (-1)^i.$$

□

Mit den folgenden Regeln lassen sich auch Binomialkoeffizienten behandeln, deren Einträge größer als p sind.

Lemma 4.19 *Sei* $\operatorname{char} K = p > 0$ *und* $n \geq 0$. *Dann gilt*

(a) Ist $0 \leq k < p$, *so gilt* $\binom{n+p}{k} = \binom{n}{k}$.

(b) Sei $0 \leq k \leq n + p < 2p$ *(also* $n < p$*). Dann gilt*

$$\binom{n+p}{k} = \begin{cases} \binom{n}{k} & \text{für } k \leq n \\ 0 & \text{für } n < k < p \\ \binom{n}{k-p} & \text{für } p \leq k \leq n+p. \end{cases}$$

Beweis. (a) Es ist

$$\binom{n+p}{k} = \frac{(n+p)(n+p-1)\cdot\ldots\cdot(n+p-k+1)}{k!} = \frac{n(n-1)\cdot\ldots\cdot(n-k+1)}{k!} = \binom{n}{k}.$$

(b) In den ersten beiden Fällen ist die linke Seite nach (a) (wegen $n < p$ ist $k < p$) gleich $\binom{n}{k}$, und im zweiten Fall ist dies gleich 0.

Im dritten Fall $p \leq k \leq n + p$ betrachten wir zunächst $\binom{n+p}{k} = \binom{n+p}{n+p-k}$. Da $n + p - k \leq n < p$, reduziert sich dies nach dem 1. Fall zu $\binom{n}{n+p-k} = \binom{n}{k-p}$. □

4.6.3 Ein nichttrivialer Kozyklus

Ab jetzt betrachten wir die natürliche Darstellung $\langle X, Y\rangle$ der SL_2 wieder als $\mathbb{G}_a$-Modul via des Homomorphismus (22) (S.41), also

$$\begin{aligned} t \cdot X &= X \\ t \cdot Y &= tX + Y \qquad \text{für } t \in \mathbb{G}_a = (K, +). \end{aligned}$$

Wir berechnen als erstes die Darstellungen $t \mapsto A_t = (a_{ij}^t)_{i,j=0,\ldots,k} \in K^{(k+1)\times(k+1)}$ der symmetrischen Potenzen $S^k(X, Y) = \langle X^k, X^{k-1}Y, \ldots, XY^{k-1}, Y^k\rangle$ bezüglich der gegebenen Basis. Aus

$$t \cdot X^{k-j}Y^j = X^{k-j}(tX + Y)^j = X^{k-j}\sum_{i=0}^{j}\binom{j}{i}(tX)^{j-i}Y^i = \sum_{i=0}^{j} t^{j-i}\binom{j}{i}X^{k-i}Y^i$$

folgt

$$a_{ij}^t = \begin{cases} t^{j-i}\binom{j}{i} & \text{für } 0 \leq i \leq j \leq k \\ 0 & \text{für } i > j. \end{cases} \tag{92}$$

Insbesondere ist A_t eine unipotente obere Dreiecksmatrix. Für $k < l$ hat man ein Einbettung

$$S^k(\langle X, Y\rangle) \to S^l(\langle X, Y\rangle), \quad f \mapsto X^{l-k} \cdot f,$$

wobei man beide Moduln als Teilmengen von $S(\langle X, Y\rangle)$ auffasst und daher mit $X^{l-k} \in S(\langle X, Y\rangle)$ multiplizieren darf, mit Bild

$$\langle X^l, X^{l-1}Y, \ldots X^{l-k}Y^k\rangle \cong S^k(\langle X, Y\rangle).$$

Entsprechend ist dann auf diesem Bild auch die Multiplikation mit $\frac{1}{X^{l-k}}$ als die Umkehrung der Multiplikation mit X^{l-k} definiert.

Lemma 4.20 *Sei $U := S^{p-2}(\langle X, Y\rangle)$. Dann ist durch*

$$t \mapsto g_t := \frac{1}{X}\left((t-1)\cdot Y^{p-1}\right), \quad t \in \mathbb{G}_a$$

ein nichttrivialer Kozyklus $g \in Z^1(\mathbb{G}_a, U)$ gegeben und es ist $\tilde{U} = S^{p-1}(\langle X, Y\rangle)$ der zugehörige erweiterte $\mathbb{G}_a$-Modul. Weiter ist $\tilde{U}$ selbstdual, und die g annullierende Invariante in $\tilde{U}$ gemäß Proposition 1.51 ist gegeben durch X^{p-1}.

Beweis. Da

$$g_t = \frac{1}{X}\left((tX+Y)^{p-1} - Y^{p-1}\right) = \sum_{i=0}^{p-2} \binom{p-1}{i} t^{p-1-i} X^{(p-2-i)} Y^i,$$

gilt tatsächlich $g_t \in S^{p-2}(\langle X, Y\rangle)$ für alle $t \in \mathbb{G}_a$. Die Kozyklus-Eigenschaft ist dann auch klar, da X invariant ist. Der Koeffizient von Y^{p-2} in g_t ist

$$\binom{p-1}{p-2} t^{(p-1)-(p-2)} = -t \tag{93}$$

(Lemma 4.18 (c)). Dagegen ist der Koeffizient von Y^{p-2} in

$$(t-1)\cdot X^{p-2-j}Y^j = X^{p-2-j}\left((tX+Y)^j - Y^j\right) \quad (j = 0, \ldots, p-2) \tag{94}$$

gleich 0 für alle $j = 0, \ldots, p-2$, und damit ist der Koeffizient von Y^{p-2} in $(t-1)\cdot v$ gleich 0 für jedes $v \in U$ (denn v ist Linearkombination der $X^{p-2-j}Y^j$, $j = 0, \ldots, p-2$). Also ist g nichttrivial.

Als nächstes zeigen wir, dass $\tilde{U}$ selbstdual ist, genauer $\tilde{U}^* \cong \langle Y^{p-1}, XY^{p-2}, \ldots, X^{p-1}\rangle$. Da der Kozyklus in $U \cong \langle X^{p-1}, X^{p-2}Y, \ldots, XY^{p-2}\rangle \subseteq \tilde{U}$ durch $(t-1)Y^{p-1}$ gegeben ist, insbesondere also $\tilde{U} \cong \langle X^{p-1}, X^{p-2}Y, \ldots, Y^{p-1}\rangle = S^{p-1}(\langle X, Y\rangle)$ gilt, zeigt dies dann gemäß Proposition 1.51 auch die Aussage über den Annullator. Ist $t \mapsto A_t$ die Darstellung von $\tilde{U}$ gemäß (92), so hat $\tilde{U}^*$ bezüglich der entsprechenden Dualbasis die Darstellung $t \mapsto B_t = (b_{ij}^t) = A_{-t}^T$, also $b_{ij}^t = a_{ji}^{-t}$. Drehen wir nun die Reihenfolge der Vektoren in der Dualbasis um, und bezeichnen die zugehörige Darstellung mit $t \mapsto C_t = (c_{ij}^t)$, so gilt also

$$\begin{aligned}
c_{ij}^t &= b_{p-1-i,p-1-j}^t = a_{p-1-j,p-1-i}^{-t} \\
&\overset{(92)}{=} \begin{cases} (-t)^{(p-1-i)-(p-1-j)}\binom{p-1-i}{p-1-j} & \text{für } 0 \le p-1-j \le p-1-i \le p-1 \\ 0 & \text{sonst} \end{cases} \\
&\overset{\text{Lemma 4.18}(b)}{=} \begin{cases} t^{j-i}\binom{j}{i} & \text{für } 0 \le i \le j \le p-1 \\ 0 & \text{sonst} \end{cases} \\
&\overset{(92)}{=} a_{ij}^t.
\end{aligned}$$

Aus $A_t = C_t$ für alle $t \in \mathbb{G}_a$ folgt die behauptete Isomorphie. □

4.6.4 Der endgültige Kozyklus

Das Lemma über den Kozyklus aus dem letzten Abschnitt haben wir nur benötigt, um einfach an einen Annullator für den folgenden Kozyklus zu kommen. Er entsteht aus dem vorigen Kozyklus durch multiplizieren mit einer Invariante und wird unser nichttrivialer Kozyklus zur Anwendung des Hauptsatzes werden.

Lemma 4.21 *Für* $U := \langle X^p, Y^p\rangle \otimes S^{p-2}(\langle X, Y\rangle)$ *ist mit*

$$\mathbb{G}_a \to U,\ t \mapsto g_t := X^p \otimes \frac{1}{X}\left((t-1)\cdot Y^{p-1}\right)$$

ein nichttrivialer Kozyklus $g \in Z^1(\mathbb{G}_a, U)$ *gegeben.*

Beweis. Wir bezeichnen mit h den nichttrivialen Kozyklus aus Lemma 4.20, also $h_t = \frac{1}{X}\left((t-1)\cdot Y^{p-1}\right) \in S^{p-2}(\langle X, Y\rangle)$. Da $X^p \in \langle X^p, Y^p\rangle$ invariant unter $\mathbb{G}_a$ ist, ist also auch $t \mapsto g_t = X^p \otimes h_t$ ein Kozyklus. Wir müssen zeigen, dass g nichttrivial ist, und rechnen hierzu mit der Basis $\mathcal{B} := \{X^p \otimes X^{p-2}, \ldots, X^p \otimes Y^{p-2}, Y^p \otimes X^{p-2}, \ldots, Y^p \otimes Y^{p-2}\}$.

Der Koeffizient von $X^p \otimes Y^{p-2}$ für $j = 0, \ldots, p-2$ in

$$(t-1)\left(X^p \otimes X^{p-2-j}Y^j\right) = X^p \otimes \left((t-1)X^{p-2-j}Y^j\right)$$

ist gleich 0 gemäß Gleichung (94).

Der Koeffizient von $X^p \otimes Y^{p-2}$ für $j = 0, \ldots, p-2$ in

$$\begin{aligned} & (t-1)\left(Y^p \otimes X^{p-2-j}Y^j\right) \\ = \ & (t^pX^p + Y^p) \otimes \left(X^{p-2-j}(tX+Y)^j\right) - Y^p \otimes X^{p-2-j}Y^j \end{aligned}$$

ist jedenfalls gleich 0 für $j = 0, \ldots, p-3$ (wegen des Faktors X^{p-2-j} auf der rechten Seite aller auftretenden tensoriellen Produkte); Für $j = p-2$ ist der Koeffizient von $X^p \otimes Y^{p-2}$ in

$$(t^pX^p + Y^p) \otimes (tX+Y)^{p-2} - Y^p \otimes Y^{p-2}$$

dagegen gleich t^p.

Für ein beliebiges $v \in U$ (welches Linearkombination der Basiselemente $\mathcal{B}$ ist), ist der Koeffizient von $X^p \otimes Y^{p-2}$ in $(t-1)v$ also gleich

$$\lambda \cdot t^p,$$

wobei $\lambda \in K$ der Koeffizient von $Y^p \otimes Y^{p-2}$ in v ist.

Der Koeffizient von $X^p \otimes Y^{p-2}$ in der Darstellung von $g_t = X^p \otimes h_t$ bezüglich $\mathcal{B}$ ist nach Gleichung (93) dagegen gleich

$$-t.$$

Hätten wir also $g_t = (t-1)v$ für alle $t \in \mathbb{G}_a$, so wäre

$$\lambda \cdot t^p = -t \quad \text{für alle } t \in K.$$

Da $|K| = \infty$, ist dies ein Widerspruch. Also ist g ein nichttrivialer Kozyklus. □

4.6.5 Annullatoren des Kozyklus

Als nächstes geben wir vier verschiedene Typen von Annullatoren des Kozyklus aus dem letzten Lemma an. Dabei betten wir den Kozyklus gleich in den Polynomring ein, auf den wir dann den Hauptsatz anwenden wollen. Seien dazu ab jetzt $\langle X_i, Y_i\rangle \cong \langle X, Y\rangle$ für $i \geq 1$ Kopien der natürlichen Darstellung und $\langle X_0, Y_0\rangle :\cong \langle X^p, Y^p\rangle$, also

$$\begin{aligned} t \cdot X_0 &= X_0 \\ t \cdot Y_0 &= t^p X_0 + Y_0 \qquad \text{für } t \in \mathbb{G}_a = (K, +). \end{aligned}$$

(Entsprechend auch, falls wir $\langle X_0, Y_0\rangle$ als SL_2-Modul auffassen.)

Wir erinnern an folgende Gleichung: Ist $V = \bigoplus_{i=1}^n V_i$ (mit V_i jeweils G-Modul), so ist

$$S(V) = \bigoplus_{i_1,\ldots,i_n \geq 0} S^{i_1}(V_1) \otimes \ldots \otimes S^{i_n}(V_n) \tag{95}$$

Dabei ist $S^0(V_i) \cong K$, so dass man in den Summanden Faktoren mit $i_k = 0$ weglassen kann.

Für den Rest dieses Abschnitts behalten wir die Bezeichnungen des folgenden Korollars bei.

Korollar 4.22 *Sei $V := \langle X_0, Y_0\rangle \oplus \bigoplus_{i=1}^k \langle X_i, Y_i\rangle$. Dann ist durch*

$$t \mapsto g_t := X_0 \cdot \frac{1}{X_1}\left((t-1) \cdot Y_1^{p-1}\right)$$

ein nichttrivialer Kozyklus $g \in Z^1(\mathbb{G}_a, S(V))$ gegeben.

Beweis. Aufgefasst als Kozyklus in $Z^1(\mathbb{G}_a, U)$ mit $U := \langle X_0, Y_0\rangle \otimes S^{p-2}(\langle X_1, Y_1\rangle)$ ist g nichttrivial gemäß Lemma 4.21. Da aber U nach (95) ein *direkter* Summand von $S(V)$ ist, ist g auch aufgefasst als Kozyklus in $Z^1(\mathbb{G}_a, S(V))$ nichttrivial. □

Wir können nun die ersten beiden Typen von Annullatoren angeben:

Lemma 4.23 *Der Kozyklus g wird annulliert von den Invarianten $X_1, X_i^{p-1} \in S(V)^{\mathbb{G}_a}$ mit $i \geq 2$, d.h. $X_1 g = X_i^{p-1} g = 0 \in H^1(\mathbb{G}_a, S(V))$.*

Beweis. Nach Definition von g ist

$$X_1 g_t = X_0 \cdot \left((t-1) \cdot Y_1^{p-1}\right) = (t-1) \cdot X_0 Y_1^{p-1},$$

also $X_1 g \in B^1(\mathbb{G}_a, S(V))$.

Wir betrachten nun den Kozyklus $t \mapsto h_t := \frac{1}{X_1}\left((t-1) \cdot Y_1^{p-1}\right) \in S^{p-2}(\langle X_1, Y_1\rangle) =: U$. Nach Lemma 4.20 gilt $\tilde{U}^* \cong S^{p-1}(\langle X_i, Y_i\rangle)$ und X_i^{p-1} ist der zugehörige Annullator, also $X_i^{p-1} \otimes h = 0 \in H^1(\mathbb{G}_a, U \otimes \tilde{U}^*)$. Mit den offensichtlichen Einbettungen von U und $\tilde{U}^*$ in $S(V)$ ist dann auch $X_i^{p-1} h = 0 \in H^1(\mathbb{G}_a, S(V))$, d.h. es gibt ein $v \in S(V)$ mit $X_i^{p-1} h_t = (t-1)v$ für alle $t \in \mathbb{G}_a$. Dann ist aber auch

$$X_i^{p-1} g_t = X_i^{p-1} X_0 h_t = (t-1)(X_0 v) \quad \text{für alle } t \in \mathbb{G}_a,$$

also $X_i^{p-1} g \in B^1(\mathbb{G}_a, S(V))$. □

Leider bilden $X_1, X_2^{p-1}, \ldots, X_i^{p-1}$ für $i \geq 3$ kein phsop in $S(V)^{\mathbb{G}_a}$. Daher benötigen wir weitere Typen von Annullatoren.

Lemma 4.24 *Der Kozyklus g wird annulliert von den Invarianten $X_1Y_i - X_iY_1 \in S(V)^{\mathbb{G}_a}$ mit $i \geq 2$. Genauer gilt*

$$(X_1Y_i - X_iY_1)\, g_t = (t-1) \cdot \left(Y_1^{p-1} Y_i X_0 - X_1^{p-1} X_i Y_0\right) \quad \textit{für alle } t \in \mathbb{G}_a.$$

Beweis. O.E. sei $i = 2$. Die rechte Seite der behaupteten Gleichung ist

$$\begin{aligned} & (tX_1 + Y_1)^{p-1} (tX_2 + Y_2) X_0 - X_1^{p-1} X_2 (t^p X_0 + Y_0) - \left(Y_1^{p-1} Y_2 X_0 - X_1^{p-1} X_2 Y_0\right) \\ = & \sum_{j=0}^{p-1} \binom{p-1}{j} t^j X_1^j Y_1^{p-1-j} (tX_2 + Y_2) X_0 - t^p X_1^{p-1} X_2 X_0 - Y_1^{p-1} Y_2 X_0, \end{aligned}$$

wobei sich der Term $X_1^{p-2} X_2 Y_0$ weggehoben hat. Der zweite Term $-t^p X_1^{p-1} X_2 X_0$ hebt sich mit dem Term aus der Summe für $j = p-1$ und dem Faktor tX_2 (aus $(tX_2 + Y_2)$) weg. Der dritte Term $-Y_1^{p-1} Y_2 X_0$ hebt sich mit dem Term aus der Summe für $j = 0$ und dem Faktor Y_2 weg. Zusammen mit Lemma 4.18 (c) bleibt daher

$$\begin{aligned} & X_0 X_2 Y_1 \sum_{j=0}^{p-2} (-1)^j t^{j+1} X_1^j Y_1^{p-2-j} + X_0 X_1 Y_2 \sum_{j=0}^{p-2} (-1)^{j+1} t^{j+1} X_1^j Y_1^{p-2-j} \\ = & (X_1Y_2 - X_2Y_1) X_0 \sum_{j=0}^{p-2} (-1)^{j+1} t^{j+1} X_1^j Y_1^{p-2-j} \\ = & (X_1Y_2 - X_2Y_1) X_0 \frac{1}{X_1} \left((tX_1 + Y_1)^{p-1} - Y_1^{p-1}\right) \\ = & (X_1Y_2 - X_2Y_1) g_t, \end{aligned}$$

also die linke Seite und damit die Behauptung. □

Da die Annullatoren dieses Lemmas alle im Summanden $\langle X_1, Y_1 \rangle$ „verankert“ sind, können wir wieder nur maximal zwei für ein phsop verwenden, und etwa in der Kombination $X_1, X_2^{p-1}, X_1Y_3 - X_3Y_1$ sogar nur einen. Man könnte vermuten, dass auch die $X_iY_j - X_jY_i$ Annullatoren sind, doch leider ist dem nicht so. Nach Erheben in die $p-1$-te Potenz sind sie es aber, und dies liefert uns den letzten „Typ“ von Annullatoren.

Lemma 4.25 *Der Kozyklus g wird annulliert von den Invarianten $(X_iY_j - X_jY_i)^{p-1} \in S(V)^{\mathbb{G}_a}$ mit $i, j \geq 1$.*

Beweis. Sei O.E. $i = 2, j = 3$, und $t \in \mathbb{G}_a$. Wir nummerieren in diesem Beweis alle Zeilen und Spalten von Matrizen von 0 beginnend, es ist also z.B. $e_0 = (1, 0, \ldots)$, $e_1 = (0, 1, \ldots)$ usw. jeweils ein 0ter bzw. 1ter Basisvektor. Wir setzen

$$M_2 := \langle X_2^{p-1}, X_2^{p-2} Y_2, \ldots, Y_2^{p-1} \rangle$$

und

$$M_3 := \langle Y_3^{p-1}, X_3 Y_3^{p-2}, \ldots, X_3^{p-1} \rangle.$$

Die Darstellung von M_2 ist nach (92) gegeben durch $t \mapsto A_t = (a_{ij}^t)$ mit

$$a_{ij}^t = \begin{cases} t^{j-i}\binom{j}{i} & \text{für } 0 \leq i \leq j \leq p-1 \\ 0 & \text{für } i > j. \end{cases} \tag{96}$$

Nach dem Beweis von Lemma 4.20 gilt $M_3 \cong M_2^*$, und zwar so, dass die Basis von M_3 der dualen Basis zu M_2^* entspricht. Also hat M_3 die Darstellung $t \mapsto A_{-t}^T$. Wir betrachten das Tensorprodukt $M_2 \otimes M_3$. Wir identifizieren $M_2 \otimes M_3$ mit dem entsprechenden Untermodul von $S(V)$. Weiter identifizieren wir die Elemente von $M_2 \otimes M_3$ mit ihren zugehörigen Koordinatenmatrizen $X \in K^{p \times p}$. Die Operation von $\mathbb{G}_a$ ist dann gegeben durch

$$t \cdot X = A_t X A_{-t}^{TT} = A_t X A_{-t}.$$

Sei $\pi = I_{p \times p} \in K^{p \times p}$ die $p \times p$ Einheitsmatrix. Wir sehen sofort, dass π unter der Operation von $\mathbb{G}_a$ invariant ist. Es gilt

$$\begin{aligned} \pi &= \sum_{i=0}^{p-1} X_2^{p-1-i} Y_2^i \otimes X_3^i Y_3^{p-1-i} \\ &\overset{\text{Lemma 4.18}(c)}{=} \sum_{i=0}^{p-1} \binom{p-1}{i} (-1)^i X_2^{p-1-i} Y_2^i X_3^i Y_3^{p-1-i} \\ &= (X_2 Y_3 - X_3 Y_2)^{p-1}. \end{aligned}$$

Wir sehen, dass π der Invariante entspricht, von der wir behaupten, dass sie g annulliert. Sei nun U wie in Lemma 4.21. Wenn wir nun einen π enthaltenden Untermodul M von $M_2 \otimes M_3$ angeben, der zu $\tilde{U}^*$ isomorph ist, so dass π dessen annullierender Invariante gemäß Proposition 1.51 entspricht, so sind wir fertig. Wir setzen

$$M := \langle v_0, v_1, \ldots, v_{p-2}, w_0, \ldots, w_{p-2}, \pi \rangle \subseteq K^{p \times p}$$

mit folgenden Basisvektoren: $v_i \in K^{p \times p}, i = 0, \ldots, p-2$ seien die Matrizen, die genau in der $i+1$-ten oberen Nebendiagonale Einsen haben, also

$$v_0 := \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & 0 \\ & & & \ddots & 1 \\ & & & & 0 \end{pmatrix}, \ldots, v_{p-2} := \begin{pmatrix} 0 & \ldots & \ldots & 0 & 1 \\ & \ddots & \ddots & \ddots & 0 \\ & & \ddots & \ddots & \vdots \\ & & & \ddots & 0 \\ & & & & 0 \end{pmatrix} \in K^{p \times p}.$$

Entsprechend seien $w_i \in K^{p \times p}, i = 0, \ldots, p-2$ die Matrizen, die genau in der $i+1$-ten unteren Nebendiagonale Einsen haben, also $w_i = v_i^T$. Dann besteht M genau aus den Matrizen mit „konstanten Diagonalen“. Wir zeigen, dass M ein $\mathbb{G}_a$-Modul ist (d.h. $\mathbb{G}_a \cdot M \subseteq M$) mit $M \cong \tilde{U}^*$ so, dass π der annullierenden Invariante von $\tilde{U}^*$ entspricht.

Als erstes bestimmen wir die $\mathbb{G}_a$-Operation auf den v_k, und berechnen dazu die i-te Zeile und j-te Spalte von $t \cdot v_k$, mit $i, j = 0, \ldots, p-1$. Seien dazu $e_0 = (1, 0, \ldots, 0)^T$, $e_1 = (0, 1, 0, \ldots, 0)^T, \ldots, e_{p-1} = (0, \ldots, 0, 1)^T \in K^p$ die Spalteneinheitsvektoren. Dann ist

$$\begin{aligned}
(t \cdot v_k)_{i,j} &= (A_t v_k A_{-t})_{i,j} = e_i^T A_t v_k A_{-t} e_j \\
&= (a_{i0}^t, \ldots, a_{i,p-1}^t) v_k \begin{pmatrix} a_{0j}^{-t} \\ a_{1j}^{-t} \\ \vdots \\ a_{p-1,j}^{-t} \end{pmatrix} \\
&= (0, \ldots, 0, a_{i0}^t, \ldots, a_{i,p-2-k}^t) \begin{pmatrix} a_{0j}^{-t} \\ a_{1j}^{-t} \\ \vdots \\ a_{p-1,j}^{-t} \end{pmatrix},
\end{aligned}$$

wobei man bei dem Zeilenvektor $k+1$ führende Nullen hat. Mit Gleichung (96) erhalten wir also

$$\begin{aligned}
(t \cdot v_k)_{i,j} &= \sum_{l=0}^{p-2-k} a_{i,l}^t a_{k+1+l,j}^{-t} = \sum_{l=i}^{j-k-1} a_{i,l}^t a_{k+1+l,j}^{-t} \\
&= \sum_{l=i}^{j-k-1} t^{l-i} \binom{l}{i} (-t)^{j-k-1-l} \binom{j}{k+1+l} \\
&= \sum_{l=i}^{j-k-1} t^{j-k-i-1} (-1)^{j-k-l-1} \binom{l}{i} \binom{j}{k+l+1}.
\end{aligned}$$

Bei dem zweiten Gleichheitszeichen haben wir dabei für die Summationsindizes verwendet, dass A_t eine obere Dreiecksmatrix ist. Die leere Summe (falls $i > j-k-1$) ist hier wie üblich als 0 zu lesen. Ab jetzt sei daher

$$0 \leq j - k - i - 1. \tag{97}$$

Wir verschieben nun l um $-i$ und erhalten

$$\begin{aligned}
(t \cdot v_k)_{i,j} &= \sum_{l=0}^{j-k-i-1} t^{j-k-i-1} (-1)^{j-k-l-i-1} \binom{l+i}{i} \binom{j}{k+l+i+1} \\
&\overset{\text{Lemma 4.18}(b)}{=} \sum_{l=0}^{j-k-i-1} t^{j-k-i-1} (-1)^{j-k-i-1} \binom{p-1-i}{p-1-i-l} \binom{j}{k+l+i+1}.
\end{aligned}$$

Dabei dürfen wir Lemma 4.18 (b) anwenden, denn $0 \leq i \leq l+i \leq j-k-1 \leq p-2 < p$

Nun wenden wir auf beide Binomialkoeffizienten die Regel $\binom{n}{k} = \binom{n}{n-k}$ an und erhalten

$$(t \cdot v_k)_{i,j} = \sum_{l=0}^{j-k-i-1} (-t)^{j-k-i-1} \binom{p-1-i}{l} \binom{j}{(j-k-i-1)-l}.$$

Mit der Formel $\binom{m+n}{k} = \sum_{j=0}^{k} \binom{m}{j}\binom{n}{k-j}$ ergibt sich schliesslich

$$(t \cdot v_k)_{i,j} \quad = \quad (-t)^{j-k-i-1}\binom{p+j-i-1}{j-i-1-k}.$$

Da $0 \overset{(97)}{\leq} j-i-1-k \leq j-i-1 \leq p-1$, folgt mit Lemma 4.19 (a) weiter

$$\begin{aligned}(t \cdot v_k)_{i,j} &= (-t)^{j-k-i-1}\binom{j-i-1}{j-i-1-k} \\ &= (-t)^{(j-i-1)-k}\binom{j-i-1}{k}.\end{aligned}$$

Zusammen mit $(t \cdot v_k)_{i,j} = 0$ für $k > j-i-1$ erhalten wir damit durch Vergleich mit (96)

$$(t \cdot v_k)_{i,j} = \begin{cases} a_{k,j-i-1}^{-t} & \text{für } j-i-1 \geq 0 \\ 0 & \text{sonst.} \end{cases}$$

Dies bedeutet, dass die Matrix $t \cdot v_k \in K^{p\times p}$ eine nilpotente obere Dreiecksmatrix ist und in der oberen Nebendiagonalen Nr. $j-i$ konstant der Eintrag $a_{k,j-i-1}^{-t}$ steht. Also gilt

$$t \cdot v_k = \sum_{l=0}^{p-2} a_{k,l}^{-t} v_l, \quad k = 0, \ldots, p-2,$$

oder **Zusammengefasst**: Sei $B_t \in K^{(p-1)\times(p-1)}$ die linke obere $(p-1)\times(p-1)$ Teilmatrix von A_t. Dann ist $\langle v_0, \ldots, v_{p-2}\rangle$ ein Untermodul mit Darstellung $t \mapsto B_{-t}^T$.

Im nächsten Schritt bestimmen wir die Operation auf den w_k, $k = 0, \ldots, p-2$. Es ist

$$\begin{aligned}(t \cdot w_k)_{i,j} &= (A_t w_k A_{-t})_{i,j} = e_i^T A_t w_k A_{-t} e_j \\ &= (a_{i0}^t, \ldots, a_{i,p-1}^t) w_k \begin{pmatrix} a_{0j}^{-t} \\ a_{1j}^{-t} \\ \vdots \\ a_{p-1,j}^{-t} \end{pmatrix} \\ &= (a_{i,k+1}^t, \ldots, a_{i,p-1}^t, 0, \ldots, 0) \begin{pmatrix} a_{0j}^{-t} \\ a_{1j}^{-t} \\ \vdots \\ a_{p-1,j}^{-t} \end{pmatrix} \\ &= \sum_{l=0}^{p-k-2} a_{i,k+1+l}^t a_{l,j}^{-t}.\end{aligned}$$

Mit Gleichung (96) erhalten wir also

$$(t \cdot w_k)_{i,j} \quad = \quad \sum_{l=\max(0,i-k-1)}^{\min(p-k-2,j)} t^{k+1+j-i}(-1)^{j-l}\binom{k+1+l}{i}\binom{j}{l}.$$

Da $i < p$, ist diese Summe genau dann leer, wenn $i - k - 1 > j$. Sei daher ab jetzt

$$0 \leq j - i + k + 1. \tag{98}$$

Da $i \leq k + 1 + l \leq k + 1 + p - k - 2 = p - 1$ erhalten wir mit Lemma 4.18 (b)

$$\begin{aligned}(t \cdot w_k)_{i,j} &= \sum_{l=\max(0,i-k-1)}^{\min(p-k-2,j)} t^{k+1+j-i}(-1)^{k+1+j-i}\binom{p-1-i}{p-2-k-l}\binom{j}{l} \\ &= (-t)^{k+1+j-i}\binom{p-1-i+j}{p-2-k},\end{aligned}$$

wobei wir nochmals dir Formel $\binom{m+n}{k} = \sum_{j=0}^{k}\binom{m}{j}\binom{n}{k-j} = \sum_{j=\max(0,k-n)}^{\min(k,m)}\binom{m}{j}\binom{n}{k-j}$ verwendet haben. Wir machen nun eine Fallunterscheidung:

1. Fall: $0 \leq i - j - 1$. Dann ist natürlich $i - j - 1 \leq p - 2$, und wir erhalten

$$\begin{aligned}(t \cdot w_k)_{i,j} &= (-t)^{(p-2-(i-j-1))-(p-2-k)}\binom{p-2-(i-j-1)}{p-2-k} \\ &= a^{-t}_{p-2-k,p-2-(i-j-1)}.\end{aligned}$$

Wir sehen, dass dies auch im Fall der leeren Summe, also wenn $i - j - 1 > k$, richtig ist.

2. Fall: $0 = i - j$. Dann ist

$$\begin{aligned}(t \cdot w_k)_{i,j} &= (-t)^{k+1}\binom{p-1}{p-2-k} \\ &= a^{-t}_{p-2-k,p-1}.\end{aligned}$$

3. Fall: $0 \leq j - i - 1$. Jedenfalls ist

$$(t \cdot w_k)_{i,j} = (-t)^{k+1+j-i}\binom{p+(j-i-1)}{p-2-k}.$$

3.1. Fall: $0 \leq j - i - 1 < p - 2 - k$. Nach Lemma 4.19 (b, 2. Fall) ist dann

$$(t \cdot w_k)_{i,j} = 0.$$

3.2. Fall: $p - 2 - k \leq j - i - 1$. Dann ist nach Lemma 4.19 (b, 1. Fall)

$$\begin{aligned}(t \cdot w_k)_{i,j} &= (-t)^p(-t)^{j-i-1-(p-2-k)}\binom{j-i-1}{p-2-k} \\ &= (-t)^p a^{-t}_{p-2-k,j-i-1}.\end{aligned}$$

Da A_{-t} eine obere Dreiecksmatrix ist, ist dieses Ergebnis auch im Fall 3.1 richtig.

Wir fassen zusammen:

$$(t \cdot w_k)_{i,j} = \begin{cases} a^{-t}_{p-2-k,p-2-(i-j-1)} & \text{für } 0 \leq i - j - 1 \\ a^{-t}_{p-2-k,p-1} & \text{für } i = j \\ (-t)^p a^{-t}_{p-2-k,j-i-1} & \text{für } 0 \leq j - i - 1 \end{cases}$$

Wir sehen zunächst, dass das Ergebnis nur von der Differenz $i-j$ abhängt, also dass in jeder Nebendiagonalen gleiche Einträge stehen. Insgesamt erhalten wir

$$t \cdot w_k = \sum_{j=0}^{p-2} a^{-t}_{p-2-k,p-2-j} w_j + \sum_{j=0}^{p-2} (-t)^p a^{-t}_{p-2-k,j} v_j + a^{-t}_{p-2-k,p-1}\pi.$$

Wir setzen nun $\tilde{w}_k := w_{p-2-k}$ für $0 \le k \le p-2$ und $\tilde{w}_{p-1} := \pi$. Dann ist für $0 \le k \le p-2$

$$\begin{aligned} t \cdot \tilde{w}_k &= t \cdot w_{p-2-k} = \sum_{j=0}^{p-2} a^{-t}_{k,p-2-j} w_j + \sum_{j=0}^{p-2} (-t)^p a^{-t}_{k,j} v_j + a^{-t}_{k,p-1}\pi \\ &= \sum_{j=0}^{p-1} a^{-t}_{k,j} \tilde{w}_j + \sum_{j=0}^{p-2} (-t)^p a^{-t}_{k,j} v_j \end{aligned}$$

Weiter ist auch

$$\begin{aligned} t \cdot \tilde{w}_{p-1} &= t \cdot \pi = \pi \\ &= \sum_{j=0}^{p-1} a^{-t}_{p-1,j} \tilde{w}_j, \end{aligned}$$

denn A_{-t} ist eine unipotente obere Dreiecksmatrix. Wir schreiben nun

$$A_t = \begin{pmatrix} B_t & h_t \\ 0_{1\times(p-1)} & 1 \end{pmatrix},$$

d.h. $h_t \in K^{p-1}$ sind die ersten $p-1$ Zeilen der letzten Spalte von A. Mit der Zusammenfassung von S. 122 erhalten wir nun:

Die Darstellung von $M = \langle v_0, \ldots, v_{p-2}, \tilde{w}_0, \ldots, \tilde{w}_{p-1} \rangle$ ist gegeben durch

$$\begin{aligned} t \mapsto C_t &:= \left(\begin{array}{c|c|c} B^T_{-t} & (-t)^p B^T_{-t} & 0_{(p-1)\times 1} \\ \hline 0_{p\times(p-1)} & \multicolumn{2}{c}{A^T_{-t}} \end{array}\right) \in K^{(2p-1)\times(2p-1)} \\ &= \begin{pmatrix} B^T_{-t} & (-t)^p B^T_{-t} & \\ & B^T_{-t} & \\ & h^T_{-t} & 1 \end{pmatrix}. \end{aligned}$$

Wir interpretieren nun M als ein $\tilde{W}^*$ und gehen Proposition 1.51 „rückwärts“, um zu einem Modul W mit einem Kozyklus zu gelangen, der von $\pi = \tilde{w}_{p-1}$ annulliert wird. Dann hat $\tilde{W} = M^*$ die Darstellung

$$t \mapsto C^T_{-t} = \begin{pmatrix} B_t & & \\ t^p B_t & B_t & h_t \\ & & 1 \end{pmatrix}.$$

Streichen wir hiervon die letzte Zeile und Spalte, so erhalten wir die Matrix $\begin{pmatrix} 1 & \\ t^p & 1 \end{pmatrix} \otimes B_t$, was gerade der Darstellung von $U = \langle Y^p, X^p \rangle \otimes S^{p-2}(\langle X, Y \rangle)$ entspricht. In der rechten unteren 2×2 Blockmatrix von C^T_{-t} steht die Darstellung von $S^{p-1}(\langle X, Y \rangle)$. Damit entspricht der letzten Spalte von C^T_{-t} gerade die Erweiterung von U zu $\tilde{U}$ durch den Kozyklus

$t \mapsto X^p \otimes \frac{1}{X}(t-1)Y^{p-1}$ (vgl. Gleichung (15), S. 33). Es gilt also $\tilde{W} \cong \tilde{U}$ oder $M \cong \tilde{U}^*$, und $\pi = \tilde{w}_{p-1} \in M$ entspricht genau der annullierenden Invariante in $\tilde{U}^*$. Dies wollten wir zeigen. □

Bemerkung 4.26 Mit der Formel (20), S.36 folgt

$$\begin{aligned} -(X_2Y_3 - X_3Y_2)^{p-1} g_t &= (t-1) \cdot \Bigg(Y_0 \sum_{i=0}^{p-2} \sum_{j=0}^{p-2-i} (X_1^{p-2-i}Y_1^i)(X_2^{p-1-j}Y_2^j)(X_3^{i+j+1}Y_3^{p-2-i-j}) \\ &\quad + X_0 \sum_{i=0}^{p-2} \sum_{j=0}^{p-2-i} (X_1^i Y_1^{p-2-i})(X_2^j Y_2^{p-1-j})(X_3^{p-2-i-j}Y_3^{i+j+1}) \Bigg). \end{aligned}$$

Ausgehend von dieser Formel, die ich durch Experimente mit MAGMA geraten habe, ist das Lemma und der Beweis entstanden.

4.6.6 Ein phsop

Wir wählen nun aus den annullierenden Invarianten ein phsop aus:

Lemma 4.27 *Die annullierenden Invarianten*

$$X_1, X_2^{p-1}, X_1Y_3 - X_3Y_1, (X_iY_{i+1} - X_{i+1}Y_i)^{p-1} \in S(V)^{\mathbb{G}_a}$$

mit $i = 3, \ldots, k-1$ bilden ein phsop der Länge k in $S(V)^{\mathbb{G}_a}$.

Beweis. Wir betrachten

$$V := \langle X_0, Y_0 \rangle \oplus \bigoplus_{i=1}^{k} \langle X_i, Y_i \rangle$$

und $V \oplus \langle X_{k+1}, Y_{k+1} \rangle$ sowohl als $\mathbb{G}_a$ als auch als SL_2-Moduln. Nach Roberts' Isomorphismus, Korollar 1.58, gilt $S(V \oplus \langle X_{k+1}, Y_{k+1} \rangle)^{\mathrm{SL}_2} \cong S(V)^{\mathbb{G}_a}$, wobei der Isomorphismus durch Einsetzen von $X_{k+1} = 0$ und $Y_{k+1} = 1$ gegeben ist. Insbesondere werden die Invarianten

$$X_1Y_{k+1} - X_{k+1}Y_1, (X_2Y_{k+1} - X_{k+1}Y_2)^{p-1}, X_1Y_3 - X_3Y_1, (X_iY_{i+1} - X_{i+1}Y_i)^{p-1} \tag{99}$$

aus $S(V \oplus \langle X_{k+1}, Y_{k+1} \rangle)^{\mathrm{SL}_2}$ mit $i = 3, \ldots, k-1$ in dieser Reihenfolge abgebildet auf die Invarianten

$$X_1, X_2^{p-1}, X_1Y_3 - X_3Y_1, (X_iY_{i+1} - X_{i+1}Y_i)^{p-1}$$

aus $S(V)^{\mathbb{G}_a}$ mit $i = 3, \ldots, k-1$. Schreiben wir nun die bei den SL_2-Invarianten (99) vorkommenden Indizes in der Reihenfolge

$$2, k+1, 1, 3, 4, 5, \ldots, k$$

auf, so sehen wir, dass für genau zwei benachbarte i, j jeweils eine Potenz von $X_iY_j - X_jY_i$ in (99) vorkommt. Nach den Lemmata 4.13 (umnummerieren!) und 1.9 ist also (99) ein phsop im Polynomring $S(V \oplus \langle X_{k+1}, Y_{k+1} \rangle)$. Da SL_2 aber reduktiv ist, bildet nun (99) nach Lemma 1.55 auch ein phsop im Invariantenring $S(V \oplus \langle X_{k+1}, Y_{k+1} \rangle)^{\mathrm{SL}_2}$. Die Bilder von (99) unter Roberts' Isomorphismus bilden dann natürlich ein phsop in $S(V)^{\mathbb{G}_a}$ - zunächst nur bezüglich der via Roberts' Isomorphismus vererbten Graduierung, aber da die Bilder hier auch bezüglich der Standardgraduierung homogen sind, dann auch bezüglich dieser (vgl. Bemerkung 1.6). □

4.6.7 Ernte

Nun haben wir alles zusammen, um die Beispiele für SL_2 und $\mathbb{G}_a$ zu formulieren. Sie stellen ein weiteres Hauptresultat dieser Arbeit dar.

Satz 4.28 *Sei $\langle X, Y\rangle$ die natürliche Darstellung der SL_2, $\operatorname{char} K = p > 0$. Wir fassen jeden SL_2-Modul via $t \mapsto \begin{pmatrix} 1 & t \\ & 1 \end{pmatrix}$ auch als $\mathbb{G}_a$-Modul auf. Sei*

$$V := \langle X^p, Y^p\rangle \oplus \bigoplus_{i=1}^{k} \langle X, Y\rangle.$$

Dann gilt

$$\operatorname{cmdef} K[V]^{\mathbb{G}_a} \geq k-2 \quad \textit{und} \quad \operatorname{cmdef} K[V]^{\mathrm{SL}_2} \geq k-3.$$

Als direkte Summe selbstdualer $\mathbb{G}_a$- bzw. SL_2- Moduln ist V selbstdual. Aufgefasst als SL_2-Modul ist V außerdem vollständig reduzibel als direkte Summe irreduzibler SL_2-Moduln. Ferner gilt

$$\dim K[V]^{\mathbb{G}_a} = 2k+1 \quad \textit{und} \quad \dim K[V]^{\mathrm{SL}_2} = 2k-1.$$

Damit erhalten wir die Abschätzungen

$$\operatorname{depth} K[V]^{\mathbb{G}_a} \leq k+3 \quad \textit{und} \quad \operatorname{depth} K[V]^{\mathrm{SL}_2} \leq k+2.$$

Beweis. Die Aussagen über die Dimension folgen sofort aus den Korollaren 1.68 und 1.69, und mit der Abschätzung für den Cohen-Macaulay-Defekt folgt dann die Abschätzung über die Tiefe.

Nach Roberts' Isomorphismus, Satz 1.57, gilt $K[V]^{\mathbb{G}_a} \cong K[V \oplus \langle X, Y\rangle]^{\mathrm{SL}_2}$ (insbesondere ist damit auch der erste Invariantenring endlich erzeugt), so dass es genügt, die Aussage für die $\mathbb{G}_a$ zu beweisen (vgl. auch (26), S. 45). Da V selbstdual ist, ist $K[V] = S(V^*) \cong S(V)$ (als $\mathbb{G}_a$-Algebren) und $K[V]^{\mathbb{G}_a} = S(V^*)^{\mathbb{G}_a} \cong S(V)^{\mathbb{G}_a}$. Nach Korollar 4.22 existiert ein nichttrivialer Kozyklus $g \in Z^1(\mathbb{G}_a, S(V))$. Nach Lemma 4.27 hat man ein phsop der Länge k in $S(V)^{\mathbb{G}_a}$, welches nach den Lemmata 4.23, 4.24 und 4.25 aus Annullatoren von g besteht. Ferner sind die ersten beiden phsop Elemente X_1, X_2^{p-1} aus Lemma 4.27 offenbar teilerfremd in $S(V)$. Der Hauptsatz 3.6 in seiner allgemeineren Formulierung (da $\mathbb{G}_a$ nicht reduktiv ist), liefert nun sofort die Behauptung. □

Wir erinnern nochmals daran, dass wenn man in V den Summanden $\langle X^p, Y^p\rangle$ durch $\langle X, Y\rangle$ ersetzt, die zugehörigen Invariantenringe dann Cohen-Macaulay sind - siehe die Diskussion auf S. 95.

4.7 Additive und unipotente Gruppen

Ist V ein SL_2-Modul, der sich schreiben lässt als direkte Summe $V = U \oplus \langle X, Y\rangle$, so ist nach Roberts' Isomorphismus $K[V]^{\mathrm{SL}_2} \cong K[U]^{\mathbb{G}_a}$. Insbesondere folgt aus $\operatorname{cmdef} K[V]^{\mathrm{SL}_2} \geq k-2$ sofort $\operatorname{cmdef} K[U]^{\mathbb{G}_a} \geq k-2$. Lässt sich V nicht auf diese Weise schreiben, wurde aber $\operatorname{cmdef} K[V]^{\mathrm{SL}_2} \geq k-2$ mit Hilfe des Hauptsatzes gefolgert, so gilt auch $\operatorname{cmdef} K[V \oplus \langle X, Y\rangle]^{\mathrm{SL}_2} \geq k-2$; Denn ein phsop in $K[V]$ bleibt auch eines nach Einbetten in $K[V \oplus \langle X, Y\rangle]$, und genauso bleiben Kozyklen nichttrivial - der Hauptsatz kann also weiterhin

(mit „selbem“ phsop und Kozyklus) angewendet werden. Nach Roberts' Isomorphismus gilt dann also auch $\operatorname{cmdef} K[V]^{\mathbb{G}_a} = \operatorname{cmdef} K[V \oplus \langle X, Y\rangle]^{\mathrm{SL}_2} \geq k-2$. Somit lassen sich aus SL_2-Beispielen immer $\mathbb{G}_a$-Beispiele mit großem Cohen-Macaulay-Defekt konstruieren. Auf diese Weise erhalten wir etwa aus Beispiel 4.11

Beispiel 4.29 *Sei* $\operatorname{char} K = 2$ *und* $\langle X, Y\rangle$ *die natürliche Darstellung der additiven Gruppe* $\mathbb{G}_a$*. Dann gilt*

$$\operatorname{cmdef} K\left[\langle X^2, Y^2\rangle \oplus \bigoplus_{i=1}^{k} \langle X^2, Y^2, XY\rangle\right]^{\mathbb{G}_a} \geq k-2.$$

Die Dimension des Invariantenringes ist $3k+1$ *nach Korollar 1.68.*

Analog erhalten wir aus Beispiel 4.17 durch weglassen des Summanden $\langle X, Y\rangle$

Beispiel 4.30 *Ist* $\operatorname{char} K = 3$ *und* $\langle X, Y\rangle$ *die natürliche Darstellung der additiven Gruppe* $\mathbb{G}_a$*, so gilt*

$$\operatorname{cmdef} K\left[\langle X^3, Y^3\rangle \oplus \bigoplus_{i=1}^{k} \langle X^2, Y^2, XY\rangle\right]^{\mathbb{G}_a} \geq k-2.$$

Die Dimension des Invariantenringes ist $3k+1$ *nach Korollar 1.68.*

Sind G und H lineare algebraische Gruppen und ist $f : G \to H$ ein surjektiver (algebraischer) Homomorphismus, so ist jeder H-Modul V via f auch ein G-Modul. Aufgrund der Surjektivität von f gilt dann auch $K[V]^G = K[V]^H$. Aus Beispielen für H-Invariantenringe mit großem Cohen-Macaulay-Defekt erhält man so Beispiele für G. Das folgende Lemma, das sich etwa in [7, kurz vor Abschnitt 3] findet, stellt einen solchen Homomorphismus für nichttriviale zusammenhängende unipotente Gruppen zur Verfügung.

Lemma 4.31 *Sei* G *eine nichttriviale, zusammenhängende unipotente lineare algebraische Gruppe. Dann gibt es einen surjektiven algebraischen Homomorphismus* $G \to \mathbb{G}_a$*.*

Beweis. Als unipotente Gruppe ist G nilpotent ([29, Corollary 17.5]), also auflösbar. Nach [29, Theorem 19.3] enthält G einen abgeschlossenen Normalteiler N mit $\dim G - \dim N = 1$. Nach [29, Theorem 11.5] gibt es eine rationale Darstellung $\varphi : G \to \mathrm{GL}(V)$ mit $\ker\varphi = N$. Nach [59, Proposition 2.2.5 (ii)] ist $\varphi(G) \subseteq \mathrm{GL}(V)$ abgeschlossen, außerdem mit G zusammenhängend und unipotent ([59, Theorem 2.4.8]). Weiter gilt nach [59, Corollary 4.3.4] $\dim\varphi(G) = \dim G - \dim\ker\varphi = 1$. Also ist $\varphi(G)$ eine zusammenhängende, unipotente, eindimensionale lineare algebraische Gruppe, und damit isomorph zu $\mathbb{G}_a$ ([59, Proposition 2.6.6]). □

Satz 4.32 *Sei* G *eine nichttriviale, zusammenhängende unipotente lineare algebraische Gruppe in positiver Charakteristik. Dann gibt es für jedes* $k \in \mathbb{N}$ *einen* $2k+2$*-dimensionalen* G*-Modul* V *mit*

$$\operatorname{cmdef} K[V]^G \geq k-2.$$

Beweis. Wir machen den von Satz 4.28 gelieferten $2k+2$-dimensionalen $\mathbb{G}_a$-Modul V mit cmdef $K[V]^{\mathbb{G}_a} \geq k-2$ mittels des surjektiven Homomorphismus $G \to \mathbb{G}_a$ aus Lemma 4.31 zu einem G-Modul. Aus $K[V]^G = K[V]^{\mathbb{G}_a}$ folgt sofort die Behauptung. □

Man kann ein entsprechendes Resultat auch für nichtzusammenhängende unipotente Gruppen angeben. Dann hat nämlich jedes Element von G/G^0 p-Potenzordnung (ist $G \subseteq \mathrm{GL}_n$ unipotent, so gibt es zu $A \in G$ ein $N \in \mathbb{N}$ mit $(A - I_n)^N = 0$. Für k mit $p^k \geq N$ ist dann $0 = (A - I_n)^{p^k} = A^{p^k} - I_n$, vgl. [59, 2.4]), so dass $H := G/G^0$ eine (endliche) p-Gruppe ist. Man muss hier also auf entsprechende Resultate im modularen Fall, etwa Satz 3.11 zurückgreifen.

Man beachte, dass unendliche unipotente Gruppen G nicht reduktiv sind, denn dann ist $G^0 \neq \{\iota\}$ ein zusammenhängender, abgeschlossener, nichttrivialer unipotenter Normalteiler von G (vgl. Satz bzw. Definition 1.34 und 1.35).

5 Algorithmische Untersuchungen

In diesem Abschnitt wollen wir im Wesentlichen die in Satz 4.28 beschriebenen Invariantenringe mit „a posteriori“ Methoden untersuchen, d.h. wir berechnen zunächst Erzeuger für $K[V]^G$ (als K-Algebra). Hierfür entwickeln wir ein speziell angepasstes Verfahren, da der allgemeine Algorithmus [36] auch in kleinen Fällen nicht durchkommt (ich habe die Rechnung bei knapp 70 *Giga*byte Speicherbedarf abgebrochen). Danach berechnen wir das Relationenideal und rechnen so im Restklassenring eines Polynomrings weiter, und berechnen so explizit den Cohen-Macaulay-Defekt für die Fälle $(p,k) \in \{(2,3),(2,4),(3,3)\}$ zu $1,2,1$ (für die $\mathbb{G}_a$-Invarianten). Genau genommen berechnen wir jeweils eine obere Schranke für den Cohen-Macaulay-Defekt, die zusammen mit der unteren Schranke aus Satz 4.28 das angegebene Ergebnis liefert.

5.1 Berechnung von Frobenius-Invarianten

Sei G eine lineare algebraische Gruppe in Charakteristik $p > 0$, und U, V zwei G-Moduln, so dass $S(U \oplus V)^G$ endlich erzeugt ist. Mit F^p bezeichnen wir die p-te Frobenius-Potenz, vgl. Definition 1.38. Wir untersuchen folgendes Problem:

Wie kann man Generatoren für $S(F^p(U) \oplus V)^G$ effizient berechnen, wenn Generatoren für $S(U \oplus V)^G$ bekannt sind?

Ohne formale Definition nennen wir dieses Problem im Folgenden die „Berechnung von Frobenius-Invarianten“.

5.1.1 Der Isomorphismus

Seien

$$U = \langle X_1, \ldots, X_n \rangle, \quad V = \langle Y_1, \ldots, Y_m \rangle, \quad \text{und} \quad F^p(U) = \langle X_1^p, \ldots, X_n^p \rangle =: \langle Z_1, \ldots, Z_n \rangle$$

G-Moduln. Dann ist

$$P := S(U \oplus V) = K[X_1, \ldots, X_n, Y_1, \ldots, Y_m],$$

$$Q := S(F^p(U) \oplus V) = K[Z_1, \ldots, Z_n, Y_1, \ldots, Y_m].$$

Wir betrachten den Algebrenhomomorphismus

$$\phi : Q \to P \quad \text{mit } Z_i \mapsto X_i^p,\ Y_i \mapsto Y_i,$$

welcher als Abbildung des Polynomrings Q eindeutig und wohldefiniert ist durch Angabe der Bilder der unabhängigen Variablen.

Satz 5.1 *Durch die Einschränkung $\varphi := \phi|_{Q^G}$ ist ein Isomorphismus*

$$\varphi : Q^G \to P^G \cap K[X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m]$$

gegeben.

Beweis. Wir bezeichnen mit $G \to \mathrm{GL}_n, \sigma \mapsto A_\sigma = (a_{ij,\sigma})$ die Darstellung von U und analog mit $G \to \mathrm{GL}_m, \sigma \mapsto B_\sigma = (b_{ij,\sigma})$ die Darstellung von V. Die Darstellung von $F^p(U)$ ist damit gegeben durch $\sigma \mapsto (a^p_{ij,\sigma})$. Es gilt also

$$\sigma \cdot X_j = \sum_{i=1}^{n} a_{ij,\sigma} X_i, \quad \sigma \cdot Z_j = \sum_{i=1}^{n} a^p_{ij,\sigma} Z_i, \quad \sigma \cdot Y_j = \sum_{i=1}^{m} b_{ij,\sigma} Y_i.$$

Es ist klar, dass $\varphi : Q^G \to P$ mit ϕ ein Algebren-Homomorphismus ist. Da $X_1^p, \ldots, X_n^p$, $Y_1, \ldots, Y_m$ offenbar algebraisch unabhängig sind, ist ϕ und damit auch die Einschränkung φ injektiv. Wir müssen nun nur noch $\varphi(Q^G) = P^G \cap K[X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m]$ zeigen.

„$\subseteq$“. Die Inklusion $\varphi(Q^G) \subseteq K[X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m]$ ist klar. Sei nun

$$f = f(Z_1, \ldots, Z_n, Y_1, \ldots, Y_m) \in Q^G,$$

d.h.

$$\sigma \cdot f \overset{(*)}{=} f\left(\sum_{i=1}^{n} a^p_{i1,\sigma} Z_i, \ldots, \sum_{i=1}^{n} a^p_{in,\sigma} Z_i, \sum_{i=1}^{m} b_{i1,\sigma} Y_i, \ldots, \sum_{i=1}^{m} b_{im,\sigma} Y_i\right) = f. \tag{100}$$

Dann ist

$$\varphi(f) = f\left(X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m\right),$$

und damit für $\sigma \in G$

$$\begin{aligned}
\sigma \cdot \varphi(f) &= f\left(\left(\sum_{i=1}^{n} a_{i1,\sigma} X_i\right)^p, \ldots, \left(\sum_{i=1}^{n} a_{in,\sigma} X_i\right)^p, \sum_{i=1}^{m} b_{i1,\sigma} Y_i, \ldots, \sum_{i=1}^{m} b_{im,\sigma} Y_i\right) \\
&= f\left(\sum_{i=1}^{n} a^p_{i1,\sigma} X_i^p, \ldots, \sum_{i=1}^{n} a^p_{in,\sigma} X_i^p, \sum_{i=1}^{m} b_{i1,\sigma} Y_i, \ldots, \sum_{i=1}^{m} b_{im,\sigma} Y_i\right) \\
&\overset{(*)}{=} \varphi(\sigma \cdot f) \\
&\overset{(100)}{=} \varphi(f),
\end{aligned}$$

also $\varphi(f) \in P^G$. (Man kann auch argumentieren, dass φ G-äquivariant ist).

„$\supseteq$“. Sei nun umgekehrt

$$F = F(X_1, \ldots, X_n, Y_1, \ldots, Y_m) \in P^G \cap K[X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m].$$

Dann gibt es jedenfalls ein $f = f(Z_1, \ldots, Z_n, Y_1, \ldots, Y_m) \in Q$ mit

$$F = f(X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m) = \phi(f).$$

Wir müssen daher nur noch $f \in Q^G$ zeigen. Für $\sigma \in G$ ist

$$\begin{aligned}
\sigma \cdot F &= \sigma \cdot f(X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m) \\
&= f\left(\sum_{i=1}^{n} a^p_{i1,\sigma} X_i^p, \ldots, \sum_{i=1}^{n} a^p_{in,\sigma} X_i^p, \sum_{i=1}^{m} b_{i1,\sigma} Y_i, \ldots, \sum_{i=1}^{m} b_{im,\sigma} Y_i\right) \\
&\overset{(*)}{=} f(X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m) = F,
\end{aligned}$$

da $F \in P^G$. Die Gleichung $(*)$ beschreibt eine Gleichung in $K[X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m]$. Da dieser Ring isomorph zu einem Polynomring ist, darf man in $(*)$ die „unabhängige Variable“ X_i^p durch Z_i ersetzen. Dies liefert

$$\begin{aligned} \sigma \cdot f &= \sigma \cdot f(Z_1, \ldots, Z_n, Y_1, \ldots, Y_m) \\ &= f\left(\sum_{i=1}^{n} a_{i1,\sigma}^p Z_i, \ldots, \sum_{i=1}^{n} a_{in,\sigma}^p Z_i, \sum_{i=1}^{m} b_{i1,\sigma} Y_i, \ldots, \sum_{i=1}^{m} b_{im,\sigma} Y_i\right) \\ &\overset{(*)}{=} f(Z_1, \ldots, Z_n, Y_1, \ldots, Y_m) = f, \end{aligned}$$

also $f \in Q^G$. □

5.1.2 Zwischenspiel: Der Kern einer linearen Abbildung von Moduln

Sei $K[X] = K[X_1, \ldots, X_n]$ ein Polynomring und $A = K[f_1, \ldots, f_k]$ mit $f_i \in K[X]$ für alle $i = 1, \ldots, k$ eine endlich erzeugte Unteralgebra. Sei ferner $B = \sum_{i=1}^{r} At_i$ mit $t_i \in K[X]$ für alle $i = 1, \ldots, r$ ein endlich erzeugter A-Modul sowie $D : B \to K[X]^m$ eine A-lineare Abbildung. Der folgende Algorithmus (der eine Verallgemeinerung von Kemper [36, Algorithm 4.2] ist), liefert ein endliches Erzeugendensystem von $\ker D$ als A-Modul.

Algorithmus 5.2 Berechnung des Kerns einer linearen Abbildung von Moduln.
Eingabe:

- Ein Polynomring $K[X] = K[X_1, \ldots, X_n]$.
- Generatoren $f_1, \ldots, f_k \in K[X]$ von $A := K[f_1, \ldots, f_k]$.
- Modulerzeuger $t_1, \ldots, t_r \in K[X]$ von $B := \sum_{i=1}^{r} At_i$.
- Die Bilder $D(t_1), \ldots, D(t_r) \in K[X]^m$ einer A-linearen Abbildung $D : B \to K[X]^m$. (Der Anwender hat sicherzustellen, dass die Bilder tatsächlich von einer A-linearen Abbildung D abstammen!)

Ausgabe: A-Modul Erzeuger von $\ker D$.
BEGIN

1. Berechne Generatoren des Syzygien-Moduls

   $$M := \{(a_1, \ldots, a_r) \in K[X]^r : a_1 D(t_1) + \ldots + a_r D(t_r) = 0\}$$

   (als $K[X]$-Modul) mit einem der üblichen Standard-Verfahren, siehe etwa Eisenbud [14, Chapter 15.5].

2. Berechne Generatoren $b_1, \ldots, b_s$ von $M \cap A^r$ als A-Modul mittels Kemper [36, Algorithm 4.5] (siehe auch Kemper [30, Algorithm 7]). Dieser Algorithmus verlangt als Eingabe die Generatoren von A und die in Schritt 1. berechneten Generatoren von M als $K[X]$-Modul.

3. Setze

   $$c_i := \sum_{\mu=1}^{r} (b_i)_\mu t_\mu \quad \text{für } i = 1, \ldots, s$$

   mit $b_i = ((b_i)_1, \ldots, (b_i)_r) \in A^r$.

4. **RETURN** $c_1, \ldots, c_s$.

END

Satz 5.3 *Algorithmus 5.2 ist korrekt, d.h.*

$$\ker D = \sum_{i=1}^{s} Ac_i.$$

Beweis. Für $f \in K[X]$ gilt $f \in \ker D$ genau dann, wenn es $a_1, \ldots, a_r \in A$ gibt mit

$$f = \sum_{\mu=1}^{r} a_\mu t_\mu \quad \text{und} \quad D(f) = \sum_{\mu=1}^{r} a_\mu D(t_\mu) = 0, \tag{101}$$

denn die t_μ erzeugen B als A-Modul, und D ist A-linear. Wir zeigen nun beide Inklusionen der Behauptung.

„$\supseteq$“. Da $b_i = ((b_i)_1, \ldots, (b_i)_r) \in M \cap A^r$ (Schritt 2.), gilt nach Definition von M (Schritt 1.) jedenfalls $\sum_{\mu=1}^{r} (b_i)_\mu D(t_\mu) = 0$, und damit (Schritt 3.) $c_i = \sum_{\mu=1}^{r} (b_i)_\mu t_\mu \in \ker D$ nach (101).

„$\subseteq$“. Sei $f \in \ker D$, d.h. f habe eine Darstellung wie in (101). Dann gilt $a = (a_1, \ldots, a_r) \in M \cap A^r$ nach Definition von M. Nach Schritt 2. gibt es dann $p_1, \ldots, p_s \in A$ mit

$$a = \sum_{i=1}^{s} p_i b_i, \quad \text{also } a_\mu = \sum_{i=1}^{s} p_i (b_i)_\mu.$$

Es folgt

$$f = \sum_{\mu=1}^{r} a_\mu t_\mu = \sum_{\mu=1}^{r} \sum_{i=1}^{s} p_i (b_i)_\mu t_\mu = \sum_{i=1}^{s} p_i \underbrace{\sum_{\mu=1}^{r} (b_i)_\mu t_\mu}_{c_i},$$

und damit gilt $f \in \sum_{i=1}^{s} Ac_i$. □

5.1.3 Schnitt einer Algebra mit $K[X^p, Y]$

Wir verwenden wieder die Bezeichnungen aus Abschnitt 5.1.1. Außerdem kürzen wir mit X^p die Variablen $X_1^p, \ldots, X_n^p$ ab. Von dem Isomorphismus φ kann man auch leicht die Umkehrung durchführen, indem man in einem Polynom f aus dem Bild einfach in jedem Monom X_i^p durch Z_i ersetzt. Da ein Algebrenisomorphismus Generatoren auf Generatoren abbildet, können wir zur Berechnung von Q^G (was unser Ziel ist) zunächst Generatoren für das Bild von φ berechnen, um durch Anwendung von φ^{-1} Generatoren von Q^G zu erhalten. Wir versuchen dazu, $\varphi(Q^G) = P^G \cap K[X^p, Y]$ als Kern einer geeigneten A-linearen Abbildung zu erhalten, den wir mit Algorithmus 5.2 berechnen können.

Sei also allgemeiner $B \subseteq K[X, Y]$ eine endlich erzeugte Algebra (z.B. $B = P^G$),

$$B := K[f_1, \ldots, f_k, g_1, \ldots, g_l] \quad \text{mit } f_i \in K[X, Y],\ g_i \in K[Y] \ \text{ für alle } i.$$

Gesucht ist der Schnitt $B \cap K[X^p, Y]$. Wir setzen dazu

$$A := K[f_1^p, \ldots, f_k^p, g_1, \ldots, g_l] \subseteq B \cap K[X^p, Y]$$

und bilden

$$\{t_1, \ldots, t_r\} := \left\{ f_1^{e_1} \cdot \ldots \cdot f_k^{e_k} : 0 \leq e_i < p \right\}.$$

Dann ist offenbar $B = \sum_{i=1}^{r} A t_i$. Für $j = 1, \ldots, n$ ist die Abbildung

$$\frac{\partial}{\partial X_j} : B \to K[X, Y]$$

A-linear, denn für $a \in A, b \in B$ gilt wegen $A \subseteq K[X^p, Y]$

$$\frac{\partial(ab)}{\partial X_j} = a\frac{\partial b}{\partial X_j} + b \underbrace{\frac{\partial a}{\partial X_j}}_{=0}.$$

Weiter liegt ein $f \in B$ genau dann in $K[X^p, Y]$, wenn $\frac{\partial f}{\partial X_j} = 0$ für $j = 1, \ldots, n$ gilt, also wenn f im Kern der linearen Abbildung

$$D : B \to K[X, Y]^n, f \mapsto D(f) := \left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n} \right) \tag{102}$$

liegt. Damit erhalten wir folgenden Algorithmus, um Algebra-Erzeuger für $B \cap K[X^p, Y] = \ker D$ zu erhalten:

Algorithmus 5.4 Schnitt einer Algebra B mit $K[X^p, Y]$, wobei $p = \operatorname{char} K > 0$.
Eingabe:

- Ein Polynomring $K[X_1, \ldots, X_n, Y_1, \ldots, Y_m] =: K[X, Y]$.
- $B := K[f_1, \ldots, f_k, g_1, \ldots, g_l]$ mit $f_i \in K[X, Y]$, $g_i \in K[Y]$ für alle i.

Ausgabe: Generatoren von $B \cap K[X_1^p, \ldots, X_n^p, Y_1, \ldots, Y_m] =: B \cap K[X^p, Y]$.
BEGIN

1. Setze $A := K[f_1^p, \ldots, f_k^p, g_1, \ldots, g_l]$ und bilde
$$T := \{t_1, \ldots, t_r\} := \left\{ f_1^{e_1} \cdot \ldots \cdot f_k^{e_k} : 0 \leq e_i < p \right\}.$$
2. Übergib die Daten A, T und $D(t_1), \ldots, D(t_r)$ mit D wie in (102) an Algorithmus 5.2. Erhalte Generatoren $c_1, \ldots, c_s$ von $\ker D = B \cap K[X^p, Y]$ als A-Modul.
3. **RETURN** $f_1^p, \ldots, f_k^p, g_1, \ldots, g_l, c_1, \ldots, c_s$.

END

Satz 5.5 *Der Algorithmus ist korrekt, d.h.*

$$B \cap K[X^p, Y] = K[f_1^p, \ldots, f_k^p, g_1, \ldots, g_l, c_1, \ldots, c_s].$$

Beweis. Da $B \cap K[X^p, Y] = \ker D = \sum_{i=1}^{s} A c_i$ nach Satz 5.3, gilt erst recht $B \cap K[X^p, Y] = A[c_1, \ldots, c_s] = K[f_1^p, \ldots, f_k^p, g_1, \ldots, g_l, c_1, \ldots, c_s]$. □

5.1.4 Der Algorithmus

Wir erhalten nun den folgenden Algorithmus zur Berechnung von $S(F^p(U) \oplus V)^G$:

Algorithmus 5.6 Berechnen von $S(F^p(U) \oplus V)^G$, falls $S(U \oplus V)^G$ bekannt ist.
Eingabe: Generatoren von $S(U \oplus V)^G$.
Ausgabe: Generatoren von $S(F^p(U) \oplus V)^G$.
BEGIN

1. Schreibe $S(U \oplus V) = K[X, Y]$, $S(F^p(U) \oplus V) = K[Z, Y]$.
2. Sei $S(U \oplus V)^G = K[f_1, \ldots, f_k, g_1, \ldots, g_l]$ mit $f_i \in K[X, Y]$, $g_i \in K[Y]$.
3. Berechne Generatoren $H_1, \ldots, H_s$ von $S(U \oplus V)^G \cap K[X^p, Y]$ mit Hilfe von Algorithmus 5.4.
4. Ersetze für $i = 1, \ldots, s$ in H_i jedes X_j^p durch Z_j und schreibe für das Ergebnis h_i.
5. **RETURN** $h_1, \ldots, h_s$.

END

Die Korrektheit von Algorithmus 5.6, also $S(U \oplus V)^G = K[h_1, \ldots, h_s]$, folgt sofort aus Satz 5.1.

5.1.5 Beispiele

Algorithmus 5.6 lässt sich einfach in Magma implementieren. Wir wenden ihn an für $G = \mathrm{SL}_2$ und $U = \langle X_0, Y_0 \rangle$ (natürliche Darstellung) und $V = \bigoplus_{i=1}^k \langle X_i, Y_i \rangle$ (k-fache direkte Summe der natürlichen Darstellung). Nach de Concini und Procesi [11] wird $S(U \oplus V)^{\mathrm{SL}_2}$ auch in positiver Charakteristik erzeugt von

$$\{X_i Y_j - X_j Y_i : 0 \leq i < j \leq k\}.$$

Damit erhält man mittels des Frobenius-Homomorphismus auch leicht Erzeuger für $S(U \oplus V)^{\mathbb{G}_a}$, indem man in obiger Menge zunächst $k+1$ statt k wählt und dann die Ersetzung $X_{k+1} = 0, Y_{k+1} = 1$ vornimmt. Damit wird $S(U \oplus V)^{\mathbb{G}_a}$ erzeugt von

$$\{X_i Y_j - X_j Y_i : 0 \leq i < j \leq k\} \cup \{X_i : 0 \leq i \leq k\}.$$

Auch wenn man an $S(F^p(U) \oplus V)^{\mathrm{SL}_2}$ interessiert ist, empfiehlt sich dringend, stattdessen $S(F^p(U) \oplus V)^{\mathbb{G}_a}$ (mit $k-1$ statt k) zu berechnen und dann darauf die Umkehrung von Roberts' Isomorphismus (Korollar 1.59) anzuwenden. So dauert etwa die Rechnung für das Tupel ($G = \mathrm{SL}_2, p = 3, k = 4$) etwa $250s$, dagegen die äquivalente Rechnung für ($G = \mathbb{G}_a, p = 3, k = 3$) nur $73s$.

Wir haben den Schnitt

$$S(U \oplus V)^{\mathbb{G}_a} \cap K[X_0^p, Y_0^p, X_1, Y_1, \ldots, X_k, Y_k]$$

für einige weitere Werte von p und k mit Hilfe einer Implementierung von Algorithmus 5.6 in Magma berechnet. Die folgenden Tabelle gibt die Entwicklung der Rechenzeit (t) sowie der Anzahl (#) der Generatoren von $S(F^p(U) \oplus V)^{\mathbb{G}_a}$ für diese Werte wieder. Die Lücken in der Tabelle resultieren daher, dass ich die Rechnung für die entsprechenden Werte nach etwa einem Monat ohne Ergebnis abgebrochen habe.

p\k	2	3	4	5
2	t=0.1s, #6	t=1.750s, #11	t=53.56s, #20	t=6.25h, #37
3	t=1.1s, #6	t=73.16s, #14	t=20.4h, #46	
5	t=50.41s, #6	t=32.15h, #30		

Rechenzeiten (t) von Algorithmus 5.6 und Anzahl (#) der berechneten Generatoren.

Der Speicherbedarf in den aufwändigeren Fällen betrug bis zu 23GB. Zur Abrundung wollen wir für den kleinsten interessanten Fall $p = 2, k = 3$ die berechneten Generatoren des Schnitts explizit angeben:

Satz 5.7 (MAGMA und Algorithmus 5.6) *Sei* $p = \operatorname{char} K = 2$ *sowie* $\langle X_i, Y_i\rangle$ *für* $i = 0, \ldots, 3$ *jeweils die natürliche Darstellung der additiven Gruppe* $\mathbb{G}_a$. *Es wird*

$$\begin{aligned} & S\left(\langle X_0, Y_0\rangle \oplus \bigoplus_{i=1}^{3}\langle X_i, Y_i\rangle\right)^{\mathbb{G}_a} \cap K[X_0^2, Y_0^2, X_1, Y_1, X_2, Y_2, X_3, Y_3] \\ \cong\ & S\left(\langle X_0^2, Y_0^2\rangle \oplus \bigoplus_{i=1}^{3}\langle X_i, Y_i\rangle\right)^{\mathbb{G}_a} \end{aligned}$$

erzeugt von den 11 *Generatoren*

$$\begin{gathered} X_0^2, \quad X_1, \quad X_2, \quad X_3, \\ X_1Y_2 + Y_1X_2, \quad X_1Y_3 + Y_1X_3, \quad X_2Y_3 + Y_2X_3, \\ X_1^2Y_0^2 + Y_1^2X_0^2, \quad X_2^2Y_0^2 + Y_2^2X_0^2, \quad X_3^2Y_0^2 + Y_3^2X_0^2, \\ X_1X_2X_3Y_0^2 + X_1Y_2Y_3X_0^2 + Y_1X_2Y_3X_0^2 + Y_1Y_2X_3X_0^2. \end{gathered}$$

5.2 Untere Schranken für die Tiefe

Während der Hauptsatz 3.6 „a priori“ eine obere Schranke für die Tiefe gibt, geben wir hier eine einfache Heuristik zur „a posteriori“ Bestimmung unterer Schranken für die Tiefe. Wir gehen dabei von der Situation aus, dass der Ring R (bis auf Isomorphie) gegeben ist als Restklassenring eines Polynomrings $P = K[X_1, \ldots, X_n]$ modulo eines Ideals $I \trianglelefteq P$, welches durch ein endliches Erzeugendensystem gegeben ist, also $R \cong P/I$. Im Fall $R = K[V]^G$ müssen dazu zunächst Generatoren $f_1, \ldots, f_n \in K[V]$ von $K[V]^G$ berechnet werden, und dann I als Kern des Einsetzungshomomorphismus $P \to K[V]^G, X_i \mapsto f_i$ (siehe etwa [14, Proposition 15.30]). Beide Schritte sind rechenintensiv und können dem Vorhaben bereits ein Ende setzen.

Um nun zu prüfen, ob die Restklassen gegebener $g_1, \ldots, g_m \in P$ eine reguläre Sequenz in R bilden, muss man testen, ob jeweils g_i ein Nichtnullteiler in $R/(g_1, \ldots, g_{i-1})_R \cong P/I + (g_1, \ldots, g_{i-1})_P$ ist (Details hierzu auf S. 14). (Falls die Restklassen der g_i in R nicht homogen und positiven Grades sind bzw. R nicht graduiert ist, muss man noch $(g_1, \ldots, g_m) \neq R$ testen, damit man wirklich eine reguläre Sequenz hat.)

Unsere Heuristik besteht nun einfach daraus, dass der Anwender eine Folge von Elementen $g_1, \ldots, g_m \in P$ vorgibt. Falls im i-ten Schritt dann g_i ein Nichtnullteiler modulo I ist, so merken wir uns i und setzen $I := I + (g_i)$. Die gemerkten g_i geben dann einer reguläre Sequenz und ihre Anzahl eine untere Schranke für die Tiefe. Formal aufgeschrieben:

Algorithmus 5.8 (Heuristik zum finden regulärer Sequenzen)
Eingabe:

- Polynomring $P = K[X_1, \ldots, X_n]$.
- Ein Ideal $I \trianglelefteq P$, gegeben durch endlich viele Generatoren.
- Eine Testsequenz $g_1, \ldots, g_m \in P$.

Ausgabe: Eine in $R := P/I$ reguläre Teilfolge der Testsequenz $g_{i_1}, \ldots, g_{i_k}$, im Fall eines graduierten Rings R und alle $g_i + I \in R_+$ insbesondere also eine untere Schranke für die Tiefe,

$$k \leq \operatorname{depth}(R).$$

BEGIN

1. Setze $k := 0, J := I$.
2. Für $i = 1, \ldots, m$
   - FALLS g_i ein Nichtnullteiler modulo J ist, so setze
   $$k := k + 1, \quad i_k := i, \quad J := J + (g_i)_P.$$
3. Falls die Restklassen der $g_1, \ldots, g_m$ modulo I nicht im maximalen homogenen Ideal R_+ eines graduierten Rings $R = P/I$ lagen, so erniedrige evtl. k, damit $(g_{i_1}, \ldots, g_{i_k}) + I \neq P$.
4. **RETURN** Reguläre Sequenz $g_{i_1}, \ldots, g_{i_k}$, untere Schranke für die Tiefe k.

END

5.3 Ein hsop für $S\left(\bigoplus_{i=1}^{n}\langle X, Y\rangle\right)^{\mathrm{SL}_2}$

Für die Anwendung von Algorithmus 5.8 ist die Angabe einer geeigneten Testsequenz essentiell. Zum einen sollte man von ihr erwarten können, dass sie eine möglichst lange reguläre Sequenz enthält, zum anderen müssen ihre Elemente einfach genug sein, dass der Test auf Nullteiler in Schritt 2. noch schnell genug durchgeführt werden kann. Hieran scheiterten (bei meinen Versuchen) alle Testsequenzen, die durch Ergänzen des phsop aus Lemma 4.27 entstanden sind. Zum Erfolg führte dagegen eine Testsequenz, die aus den f_k (mit geeigneten Exponenten e_{ij}) des folgenden Satzes bestand.

Satz 5.9 *Sei $n \geq 2$ und $R := S\left(\bigoplus_{i=1}^{n}\langle X_i, Y_i\rangle\right)^{\mathrm{SL}_2}$. Dann gilt $\dim R = 2n - 3$. Sei $g_{ij} := X_iY_j - X_jY_i \in R$, und für $k = 3, \ldots, 2n-1$ sei*

$$f_k := \sum_{\substack{i+j=k \\ i<j}} g_{ij}^{e_{ij}} \quad \textit{mit } e_{ij} \geq 1.$$

Dann ist $\dim(f_3, \ldots, f_{2n-1})_R = 0$. Insbesondere bilden die $2n-3$ Elemente $f_3, \ldots, f_{2n-1}$ bei geeigneter Wahl der e_{ij} und einer Graduierung von R (z.B. Standardgraduierung und alle $e_{ij} = 1$) ein hsop von R.

Im Beweis verwenden wir

Lemma 5.10 *Sind $x_1, \ldots, x_n \in K$ mit*

$$x_1^{e_1} + \ldots + x_n^{e_n} = 0 \text{ mit } e_i \geq 1 \text{ für alle } i \quad \text{und} \quad x_i x_j = 0 \text{ für alle } 1 \leq i < j \leq n,$$

so gilt

$$x_1 = \ldots = x_n = 0.$$

Beweis. Für $n = 1$ folgt die Behauptung aus $x_1^{e_1} = 0$. Wegen $x_i x_n = 0$ für alle $i < n$ können wir O.E. $x_n = 0$ voraussetzen. Die restlichen Gleichungen stellen genau die Voraussetzung an $x_1, \ldots, x_{n-1}$ im Fall $n - 1$ dar und liefern durch Induktion $x_1 = \ldots = x_{n-1} = 0$. □

Beweis von Satz 5.9. 1. Schritt. Wir zeigen zunächst $\dim(f_3, \ldots, f_{2n-1})_R = 0$.

Sei $P := K[G_{ij} : 1 \leq i < j \leq n]$ der Polynomring mit $\binom{n}{2}$ unabhängigen Variablen G_{ij}. Wir schreiben zusätzlich $G_{ji} := -G_{ij}$ für $i < j$ Nach de Concini und Procesi [11] ist auch in positiver Charakteristik der Einsetzungshomomorphismus

$$\phi : P \to R, \quad G_{ij} \mapsto g_{ij}$$

surjektiv, und $\ker \phi =: J$ wird erzeugt von den Plücker-Relationen

$$G_{ij}G_{kl} - G_{ik}G_{jl} + G_{il}G_{jk} \quad \text{mit } i, j, k, l \text{ paarweise verschieden.}$$

Wir schreiben $F_k := \sum_{i+j=k, i<j} G_{ij}^{e_{ij}}$ für $k = 3, \ldots, 2n-3$, so dass $\phi(F_k) = f_k$, und setzen

$$I := J + (F_3, \ldots, F_{2n-1})_P.$$

Dann ist $P/I \cong R/(f_3, \ldots, f_{2n-1})_R$. Wir zeigen, dass die Nullstellenmenge $\mathcal{V}(I)$ in $K^{\binom{n}{2}}$ nur aus der 0 besteht. Dann ist $0 = \dim P/I = \dim R/(f_3, \ldots, f_{2n-1})_R$.

Offenbar ist $0 \in \mathcal{V}(I)$. Sei nun umgekehrt $x = (x_{12}, x_{13}, \ldots, x_{n-1,n}) \in \mathcal{V}(I)$. Da $F_3 = G_{12}^{e_{12}}, F_4 = G_{13}^{e_{13}} \in I$, folgt sofort $x_{12} = x_{13} = 0$. Dies ist der Induktionsanfang ($k = 5$) der folgenden

Behauptung: Es gilt

$$x_{ij} = 0 \quad \text{für } 1 \leq i < j \leq n,\ i + j \leq k - 1. \tag{103}$$

Wir zeigen, dass diese Aussage dann auch für $k + 1$ statt k gilt. Dazu genügt es, $x_{1,k-1} = x_{2,k-2} = \ldots = 0$ zu zeigen, und hierfür genügt es zu zeigen, dass die involvierten Variablen die Voraussetzung von Lemma 5.10 erfüllen. Die erste benötigte Gleichung folgt sofort aus $F_k(x) = 0$. Seien $i_1 + j_1 = k = i_2 + j_2$ mit $i_1 < j_1$, $i_2 < j_2$ und $i_1 < i_2$. Wir müssen $x_{i_1,j_1} x_{i_2,j_2} = 0$ zeigen. Die Plücker-Relation liefert

$$x_{i_1,j_1}x_{i_2,j_2} - x_{i_1,i_2}x_{j_1,j_2} + x_{i_1,j_2}x_{j_1,i_2} = 0, \tag{104}$$

wobei wir auch hier $x_{ji} := -x_{ij}$ für $i < j$ setzen. Aus $i_1 < i_2$ folgt $j_1 > j_2$, und damit $i_1 + j_2 < i_1 + j_1 = k$. Damit ist nach (103) $x_{i_1,j_2} = 0$, und damit ist auch der dritte Summand in (104) gleich 0.

Falls $i_1 + i_2 < k$ oder $j_1 + j_2 < k$, so ist wieder nach (103) der zweite Summand in (104) ebenfalls gleich 0, und damit auch der erste, was zu zeigen ist.

Sei daher jetzt $i_1 + i_2 \geq k$ und $j_1 + j_2 \geq k$. Da aber $i_1 + j_1 + i_2 + j_2 = 2k$, gilt beidemale Gleichheit. Dann ist also $i_1 + i_2 = k = i_1 + j_1$, also $i_2 = j_1$ und genauso $i_1 = j_2$. Dann folgt aber $i_1 = j_2 > i_2 = j_1$, im Widerspruch zu $i_1 < j_1$.

Der letzte Fall tritt also nicht auf, und wir haben $x_{i_1,j_1} x_{i_2,j_2} = 0$ gezeigt. Aus Lemma 5.10 folgt dann die Behauptung (103) für $k+1$ statt k, und damit insgesamt $\mathcal{V}(I) = 0$. Dies zeigt dann

$$\dim(f_3, \ldots, f_{2n-1})_R = 0.$$

2. Schritt. Da R ein Integritätsring ist, folgt aus der Nulldimensionalität des Ideals

$$\dim R = \operatorname{height}(f_3, \ldots, f_{2n-1})_R.$$

Nach Korollar 1.69 gilt $\dim R = 2n - 3$. Für $e_{ij} = 1$ (bzw. geeignete Graduierung von R) bilden daher die $2n-3$ Elemente $f_3, \ldots, f_{2n-1}$ nach Lemma 1.5 ein hsop in R. □

5.4 Anwendung auf $S(\langle X^p, Y^p \rangle \oplus \bigoplus_{i=1}^k \langle X, Y \rangle)^{\mathrm{SL}_2}$

Wir setzen nun

$$\langle \tilde{X}, \tilde{Y} \rangle := \langle X^p, Y^p \rangle$$

und

$$V := \langle \tilde{X}, \tilde{Y} \rangle \oplus \bigoplus_{i=1}^{k} \langle X_i, Y_i \rangle \cong \langle X^p, Y^p \rangle \oplus \bigoplus_{i=1}^{k} \langle X, Y \rangle.$$

Im Polynomring $S(V) = K[\tilde{X}, \tilde{Y}, X_1, Y_1, \ldots, X_n, Y_n]$ sollen alle unabhängigen Variablen den Grad 1 haben. Weiter betrachten wir

$$U := \langle X_0, Y_0 \rangle \oplus \bigoplus_{i=1}^{k} \langle X_i, Y_i \rangle,$$

wobei alle $\langle X_i, Y_i \rangle$ für $i = 0, \ldots, k$ Kopien der natürlichen Darstellung sind. In $S(U) = K[X_0, Y_0, X_1, Y_1, \ldots, X_n, Y_n]$ wählen wir die Graduierung

$$\deg X_0 := \deg Y_0 := \frac{1}{p} \quad \text{und} \quad \deg X_i := \deg Y_i = 1 \ \text{ für } i \geq 1.$$

Wer sich bei den gebrochen rationalen Graden unwohl fühlt, kann immer alle Grade mit p durchmultiplizieren.

Nach Satz 5.1 haben wir die Isomorphie

$$S(V)^{\mathrm{SL}_2} \cong S(U)^{\mathrm{SL}_2} \cap K[X_0^p, Y_0^p, X_1, Y_1, \ldots, X_n, Y_n] =: R,$$

gegeben durch Ersetzen von $\tilde{X} \mapsto X_0^p, \tilde{Y} \mapsto Y_0^p$ und Beibehalten der restlichen Variablen X_i, Y_i. Mit der gewählten Graduierung ist dieser Isomorphismus sogar graderhaltend. Wir wählen nun für $S(U)^{\mathrm{SL}_2}$ das hsop aus Satz 5.9, wobei $n = k+1$ und wir X_0, Y_0 für X_{k+1}, Y_{k+1}

einsetzen. Mit unserer Graduierung ist dann

$$\begin{aligned}
f_3 &= X_1Y_2 - X_2Y_1\\
f_4 &= X_1Y_3 - X_3Y_1\\
f_5 &= (X_1Y_4 - X_4Y_1) + (X_2Y_3 - X_3Y_2)\\
&\vdots\\
f_{k+1} &= (X_1Y_k - X_kY_1) + (X_2Y_{k-1} - X_{k-1}Y_2) + (X_3Y_{k-2} - X_{k-2}Y_3) + \dots\\
f_{k+2} &= (X_0^pY_1^p - X_1^pY_0^p)^2 + (X_1Y_{k+1} - X_{k+1}Y_1)^{p+1} + (X_2Y_{k-1} - X_{k-1}Y_2)^{p+1} + \dots\\
f_{k+3} &= (X_0^pY_2^p - X_2^pY_0^p)^2 + (X_2Y_{k+1} - X_{k+1}Y_2)^{p+1} + (X_3Y_{k-1} - X_{k-1}Y_3)^{p+1} + \dots\\
&\vdots\\
f_{2k+1} &= (X_0^pY_k^p - X_k^pY_0^p)
\end{aligned}$$

ein hsop für $S(U)^{\mathrm{SL}_2}$ mit $\deg f_i = 2$ für $i = 3, \dots, k+1$, $\deg f_i = 2(p+1)$ für $i = k+2, \dots, 2k-1$ und $\deg f_{2k} = \deg f_{2k+1} = p+1$. Dann ist $S(U)^{\mathrm{SL}_2}$ also ein endlich erzeugter $A := K[f_3, \dots, f_{2k+1}]$-Modul. Da $A \subseteq R \subseteq S(U)^{\mathrm{SL}_2}$ und A ein noetherscher Ring ist, ist also auch der A-Untermodul R von $S(U)^{\mathrm{SL}_2}$ endlich erzeugt. Insbesondere ist also $f_3, \dots, f_{2k+1}$ ein hsop von R. Ersetzt man nun jeweils X_0^p durch $\tilde{X}$ und Y_0^p durch $\tilde{Y}$, so erhält man ein hsop für $S(V)^{\mathrm{SL}_2}$. Um den Test auf Regularität schneller zu machen, war es in der Praxis nützlich, die Elemente $f_{k+2}, \dots, f_{2k-1}$ nicht wie angegeben zum Grad $2(p+1)$ zu homogenisieren (also in den geklammerten Termen die Exponenten $2, p+1, \dots, p+1$ wegzulassen) - man kann die Tiefe ja auch mit nicht homogenen regulären Sequenzen messen, solange die Testsequenz nur im maximalen homogenen Ideal R_+ liegt.

Wir führen nun also folgende Schritte durch:

Algorithmus 5.11 Untere Schranke für die Tiefe von $K[\langle X^p, Y^p\rangle \oplus \bigoplus_{i=1}^k \langle X, Y\rangle]^{\mathrm{SL}_2}$.

1. Berechne Generatoren von

   $$K[\{X_iY_j - X_jY_i : 0 \le i < j \le n\}] \cap K[X_0^p, Y_0^p, X_1, \dots, Y_k]$$

   mit Algorithmus 5.4. Ersetze X_0^p und Y_0^p durch X_0 und Y_0, um den nächsten Schritt zu beschleunigen.

2. Berechne des Relationenideal $I \trianglelefteq P$ der Generatoren aus Schritt 1, wobei der Polynomring P soviele Variablen hat, wie es Generatoren gibt.

3. Bilde in P eine Testsequenz, die obigen $f_3, \dots, f_{2k+1}$ entspricht (evtl. ab f_{k+2} nicht mehr homogenisiert).

4. Untersuche diese Testsequenz mit Algorithmus 5.8, und erhalte eine reguläre Sequenz und eine untere Schranke für die Tiefe.

Wir haben hier das Verfahren für die SL_2 angegeben. In der Praxis wird man vorher noch Roberts' Isomorphismus anwenden, um sich im ersten Schritt zwei Variablen zu sparen.

5.5 Ergebnisse der Untersuchung

Wir geben hier die Ergebnisse wieder, die wir durch Anwenden der Methode aus dem letzten Abschnitt mit Hilfe von MAGMA erhalten haben. In den drei Fällen, in denen $K[V]^{\mathrm{SL}_2}$ dann nicht Cohen-Macaulay war, war jeweils $f_3, f_4, f_{k+2}, \ldots, f_{2k+1}$ eine reguläre Sequenz der Länge $k+2$, was dann eine untere Schranke für die Tiefe ist. Insbesondere war damit die obere Schranke für die Tiefe aus Satz 4.28 scharf, und damit auch die Schranke für den Cohen-Macaulay-Defekt. Dies lässt vermuten, dass sie es im Fall $k \geq 3$ immer ist.

Man beachte, dass genügende große Potenzen der $f_3, \ldots, f_{k+1}$ unter Roberts' Isomorphismus aus Summen von Annullatoren eines Kozyklus bestehen (siehe Abschnitt 4.6.5, insbesondere Lemma 4.25), also selbst Annullatoren sind; Nach dem Hauptsatz 3.6 lässt sich also f_3, f_4 durch kein Element aus $f_5, \ldots, f_{k+1}$ zu einer regulären Sequenz ergänzen (eine Folge von homogenen Elementen ist genau dann regulär, wenn ihre beliebig potenzierten Folgeglieder regulär sind, siehe etwa [37, Lemma 2.30]). Damit ist klar, dass die in den untersuchten Fällen ausgewählte reguläre Sequenz $f_3, f_4, f_{k+2}, \ldots, f_{2k+1}$ die „maximal mögliche“ ist.

In MAGMA haben wir immer mit $\mathbb{G}_a$ gerechnet. Die so erhaltenen exakten Werte für den Cohen-Macaulay-Defekt finden sich in der folgenden Tabelle:

p\k	2	3	4
2	0	1	2
3	0	1	-
5	0	-	-

Werte von cmdef $K[\langle X^p, Y^p\rangle \oplus \bigoplus_{i=1}^{k}\langle X, Y\rangle]^{\mathbb{G}_a}$.

Hier die benötigten Gesamtrechenzeiten für Algorithmus 5.11, wobei die $f_{k+2}, \ldots, f_{2k-1}$ nicht homogenisiert waren; Mit Homogenisierung hatte die Rechenzeit etwa im Fall $(p, k) = (2, 4)$ 11 Tage (!) betragen, also deutlich länger als ohne die Homogenisierung.

p\k	2	3	4
2	0.11s	2.29s	4.23h
3	1.13s	3.73h	-
5	50.4s	-	-

Gesamtlaufzeiten von Algorithmus 5.11 (für $\mathbb{G}_a$).

Der Großteil der Rechenzeit wurde dabei für die Berechnung des Relationenideals benötigt. Der Gesamtspeicherbedarf betrug etwa 30MB. Für andere Parameter habe ich die Rechnung nach zu großer Rechenzeit (> 1 Monat) abgebrochen.

Die folgende Tabelle gibt die mit Roberts' Isomorphismus übersetzten Werte an:

p\k	3	4	5
2	0	1	2
3	0	1	-
5	0	-	-

Werte von cmdef $K[\langle X^p, Y^p\rangle \oplus \bigoplus_{i=1}^{k}\langle X, Y\rangle]^{\mathrm{SL}_2}$.

5.6 Bemerkung zur Buchsbaum-Eigenschaft

Ein graduierter Ring R heißt *Buchsbaum*, wenn jedes phsop eine *schwach reguläre Sequenz* ist. Dabei heißt eine Folge $a_1, \ldots, a_k \in R$ schwach regulär, wenn für alle $i \leq k$ und $m \in R$ mit $ma_i \in (a_1, \ldots, a_{i-1})$ auch $mR_+ \in (a_1, \ldots, a_{i-1})$ gilt. (Regularität würde dagegen wegen $m \in (a_1, \ldots, a_{i-1})$ sogar $mR \in (a_1, \ldots, a_{i-1})$ implizieren). In Buchsbaum-Ringen gilt die Eigenschaft, dass jedes hsop die Tiefe misst, d.h. wenn $a_1, \ldots, a_n \in R$ ein hsop ist und $k = \operatorname{depth} R$, so ist $a_1, \ldots, a_k$ eine reguläre Sequenz (siehe etwa [9, section 5]). Wenn $R = K[V]^G$ die Voraussetzungen des Hauptsatzes 3.6 mit $k \geq 3$ erfüllt und wenn zusätzlich $\operatorname{depth} R > 2$ gilt, so kann damit R nicht Buchsbaum sein, denn dann ist das phsop a_1, a_2, a_3 keine reguläre Sequenz - kein hsop, dass mit a_1, a_2, a_3 beginnt, kann also die Tiefe messen. Mit dem Hauptsatz dürfte es also extrem schwer fallen, einen nicht-Cohen-Macaulay Invariantenring zu konstruieren, der Buchsbaum ist. Für Invariantenringe endlicher Gruppen gilt sogar, dass beide Eigenschaften äquivalent sind (vermutet in [9, Conjecture 27], bewiesen in Kemper [35, Theorem 3.4]).

Da die im letzten Abschnitt untersuchten nicht Cohen-Macaulay Ringe alle eine Tiefe größer als 2 hatten, ist jedenfalls keiner von ihnen Buchsbaum.

Literatur

[1] D. J. Benson. *Polynomial invariants of finite groups*, volume 190 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1993.

[2] D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1998. Basic representation theory of finite groups and associative algebras.

[3] D. J. Benson. *Representations and cohomology. II*, volume 31 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1998. Cohomology of groups and modules.

[4] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[5] Dorra Bourguiba and Said Zarati. Depth and the Steenrod algebra. *Invent. Math.*, 128(3):589–602, 1997. With an appendix by J. Lannes.

[6] Winfried Bruns and Jürgen Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[7] Roger M. Bryant and Gregor Kemper. Global degree bounds and the transfer principle for invariants. *J. Algebra*, 284(1):80–90, 2005.

[8] H. E. A. Campbell, A. V. Geramita, I. P. Hughes, R. J. Shank, and D. L. Wehlau. Non-Cohen-Macaulay vector invariants and a Noether bound for a Gorenstein ring of invariants. *Canad. Math. Bull.*, 42(2):155–161, 1999.

[9] H. E. A. Campbell, I. P. Hughes, G. Kemper, R. J. Shank, and D. L. Wehlau. Depth of modular invariant rings. *Transform. Groups*, 5(1):21–34, 2000.

[10] Roger W. Carter. *Simple groups of Lie type*. John Wiley & Sons, London-New York-Sydney, 1972. Pure and Applied Mathematics, Vol. 28.

[11] C. de Concini and C. Procesi. A characteristic free approach to invariant theory. *Advances in Math.*, 21(3):330–354, 1976.

[12] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[13] Igor Dolgachev. *Lectures on invariant theory*, volume 296 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2003.

[14] David Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[15] Geir Ellingsrud and Tor Skjelbred. Profondeur d'anneaux d'invariants en caractéristique p. *Compositio Math.*, 41(2):233–244, 1980.

[16] A. Fauntleroy. On Weitzenböck's theorem in positive characteristic. *Proc. Amer. Math. Soc.*, 64(2):209–213, 1977.

[17] Peter Fleischmann, Gregor Kemper, and R. James Shank. On the depth of cohomology modules. *Q. J. Math.*, 55(2):167–184, 2004.

[18] Peter Fleischmann, Gregor Kemper, and R. James Shank. Depth and cohomological connectivity in modular invariant theory. *Trans. Amer. Math. Soc.*, 357(9):3605–3621 (electronic), 2005.

[19] Peter Fleischmann and R. James Shank. The relative trace ideal and the depth of modular rings of invariants. *Arch. Math.*, 80(4):347–353, 2003.

[20] John Fogarty. *Invariant theory*. W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[21] Nikolai Gordeev and Gregor Kemper. On the branch locus of quotients by finite groups and the depth of the algebra of invariants. *J. Algebra*, 268(1):22–38, 2003.

[22] Frank D. Grosshans. *Algebraic homogeneous spaces and invariant theory*, volume 1673 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.

[23] W. J. Haboush. Reductive groups are geometrically reductive. *Ann. of Math. (2)*, 102(1):67–83, 1975.

[24] Wolfgang Hein. *Einführung in die Struktur- und Darstellungstheorie der klassischen Gruppen*. Hochschultext. Springer-Verlag, Berlin, 1990.

[25] Hans-Werner Henn. A variant of the proof of the Landweber Stong conjecture. In *Group representations: cohomology, group actions and topology (Seattle, WA, 1996)*, volume 63 of *Proc. Sympos. Pure Math.*, pages 271–275. Amer. Math. Soc., Providence, RI, 1998.

[26] M. Hochster. Grassmannians and their Schubert subvarieties are arithmetically Cohen-Macaulay. *J. Algebra*, 25:40–57, 1973.

[27] M. Hochster and John A. Eagon. Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci. *Amer. J. Math.*, 93:1020–1058, 1971.

[28] Melvin Hochster and Joel L. Roberts. Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. *Advances in Math.*, 13:115–175, 1974.

[29] James E. Humphreys. *Linear algebraic groups*. Springer-Verlag, New York, 1975. Graduate Texts in Mathematics, No. 21.

[30] Gregor Kemper. Calculating invariant rings of finite groups over arbitrary fields. *J. Symbolic Comput.*, 21(3):351–366, 1996.

[31] Gregor Kemper. An algorithm to calculate optimal homogeneous systems of parameters. *J. Symbolic Comput.*, 27(2):171–184, 1999.

[32] Gregor Kemper. On the Cohen-Macaulay property of modular invariant rings. *J. Algebra*, 215(1):330–351, 1999.

[33] Gregor Kemper. A characterization of linearly reductive groups by their invariants. *Transform. Groups*, 5(1):85–92, 2000.

[34] Gregor Kemper. The depth of invariant rings and cohomology. *J. Algebra*, 245(2):463–531, 2001. With an appendix by Kay Magaard.

[35] Gregor Kemper. Loci in quotients by finite groups, pointwise stabilizers and the Buchsbaum property. *J. Reine Angew. Math.*, 547:69–96, 2002.

[36] Gregor Kemper. Computing invariants of reductive groups in positive characteristic. *Transform. Groups*, 8(2):159–176, 2003.

[37] M. Kohls. Invarianten zusammenhängender Gruppen und die Cohen-Macaulay Eigenschaft. *Diplomarbeit, Technische Universität München*, pages 1–100, 2005.

[38] M. Kohls. Non Cohen-Macaulay invariant rings of infinite groups. *J. Algebra*, 306:591–609, 2006.

[39] Hanspeter Kraft. *Geometrische Methoden in der Invariantentheorie*. Aspects of Mathematics, D1. Friedr. Vieweg & Sohn, Braunschweig, 1984.

[40] Ernst Kunz. *Einführung in die algebraische Geometrie*. Vieweg Verlag, 1997.

[41] V. Lakshmibai, K.N. Raghavan, P. Sankaran, and P. Shukla. Standard monomial bases, moduli spaces of vector bundles & invariant theory. *Journal of Transformation Groups, erscheint demnächst, Preprint: arXiv:math.AG/0604321*, 2006.

[42] Peter S. Landweber and Robert E. Stong. The depth of rings of invariants over finite fields. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 259–274. Springer, Berlin, 1987.

[43] M. Lorenz and J. Pathak. On Cohen-Macaulay rings of invariants. *J. Algebra*, 245(1):247–264, 2001.

[44] D. Mumford, J. Fogarty, and F. Kirwan. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (2)*. Springer-Verlag, Berlin, third edition, 1994.

[45] Masayoshi Nagata. Complete reducibility of rational representations of a matric group. *J. Math. Kyoto Univ.*, 1:87–99, 1961/1962.

[46] Masayoshi Nagata. Invariants of a group in an affine ring. *J. Math. Kyoto Univ.*, 3:369–377, 1963/1964.

[47] Masayoshi Nagata. *Field theory*. Marcel Dekker Inc., New York, 1977. Pure and Applied Mathematics, No. 40.

[48] Masayoshi Nagata and Takehiko Miyata. Note on semi-reductive groups. *J. Math. Kyoto Univ.*, 3:379–382, 1963/1964.

[49] M. D. Neusel. Comparing the depths of rings of invariants. In *Invariant theory in all characteristics*, volume 35 of *CRM Proc. Lecture Notes*, pages 189–192. Amer. Math. Soc., Providence, RI, 2004.

[50] P. E. Newstead. *Introduction to moduli problems and orbit spaces*, volume 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Tata Institute of Fundamental Research, Bombay, 1978.

[51] V. L. Popov. On Hilbert's theorem on invariants. *Dokl. Akad. Nauk SSSR*, 249(3):551–555, 1979.

[52] Michael Roberts. On the Covariants of a Binary Quantic of the n^{th} Degree. *The Quarterly Journal of Pure and Applied Mathematics*, 4:168–178, 1861.

[53] Joseph J. Rotman. *An introduction to homological algebra*, volume 85 of *Pure and Applied Mathematics*. Academic Press Inc., New York, 1979.

[54] Walter Ferrer Santos and Alvaro Rittatore. *Actions and Invariants of Algebraic Groups*. Pure and Applied Mathematics 269. Boca Raton, FL: Chapman & Hall/CRC. xvi, 454 p., 2005.

[55] C. S. Seshadri. On a theorem of Weitzenböck in invariant theory. *J. Math. Kyoto Univ.*, 1:403–409, 1961/1962.

[56] I. R. Shafarevich, editor. *Algebraic geometry. IV*, volume 55 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1994. Linear algebraic groups. Invariant theory, A translation of *Algebraic geometry. 4* (Russian), Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989, Translation edited by A. N. Parshin and I. R. Shafarevich.

[57] R. James Shank and David L. Wehlau. On the depth of the invariants of the symmetric power representations of $\mathrm{SL}_2(\mathbf{F}_p)$. *J. Algebra*, 218(2):642–653, 1999.

[58] Larry Smith. Homological codimension of modular rings of invariants and the Koszul complex. *J. Math. Kyoto Univ.*, 38(4):727–747, 1998.

[59] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston, Mass., 1981.

[60] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, second edition, 1998.

[61] Andrzej Tyc. An elementary proof of the Weitzenböck theorem. *Colloq. Math.*, 78(1):123–132, 1998.

[62] R. Weitzenböck. Über die Invarianten von linearen Gruppen. *Acta. Math.*, 58:231–293, 1932.

Notation

Die Einträge sind thematisch geordnet.

cmdef	Cohen-Macaulay-Defekt
depth	Tiefe
dim	(Krull-)Dimension
height	Höhe
K	algebraisch abgeschlossener Körper
p	Charakteristik von K, $p = \operatorname{char} K$
$R \subseteq S$	affine (graduierte) Algebren
$\wp \lhd R, \mathcal{P} \lhd S$	Primideale
R_+	maximales homogenes Ideal
M	R-Modul
$\operatorname{Ass}_R M$	Menge der assoziierten Primideale von M in R
G	(lineare algebraische) Gruppe
KG	Gruppenring
G^0	Zusammenhangskomponente des Einselements von G
$\mathbb{G}_a$	additive Gruppe $(K, +)$
$\mathbb{G}_m$	multiplikative Gruppe $(K \setminus \{0\}, \cdot)$
$\sigma \in G$	Gruppenelement
$\iota \in G$	neutrales Element von G
V, W	G-Modul
$\operatorname{Hom}_K(V, W)_0$	S. 33
$\operatorname{Hom}_G(V, W)$	S. 33
$V = \langle X_1, \ldots, X_n \rangle$	G-Modul mit geordneter Basis $\{X_1, \ldots, X_n\}$
$\langle X, Y \rangle$	natürliche Darstellung der $\mathrm{SL}_2, \mathrm{GL}_2$ oder $\mathbb{G}_a$
A_σ	Darstellungsmatrix eines G-Moduls bzgl. der angegebenen Basis
X	G-Varietät
$K[V]$	Polynomring, Ring der Polynomfunktionen auf dem G-Modul V
$K[X]$	Koordinatenring, Ring der Polynomfunktionen auf der (G)-Varietät X oder: $K[X] := K[X_1, \ldots, X_n]$ Polynomring mit n unabhängigen Variablen
$K[V]^G, K[X]^G$	Invariantenring
$K(V)$	Körper der rationalen Funktionen auf V
$K(V)^G$	Invariantenkörper
$F^p(V)$	p-te Frobenius Potenz von V, S. 25
$S^p(V)$	p-te symmetrische Potenz von V
$C^n(G, V)$	Gruppe der n-Koketten mit Werten in V
$B^n(G, V)$	Gruppe der n-Koränder mit Werten in V
$Z^n(G, V)$	Gruppe der n-Kozyklen mit Werten in V
$H^n(G, V)$	n-te Kohomologiegruppe mit Werten in V
P_n	Freie Moduln der bar resolution
$d_n : P_n \to P_{n-1}$	Differentiale der bar resolution
$g \in Z^n(G, V)$	n-Kozyklus
∂_n^V	S. 51
$\tilde{V}$	Erweiterung des G-Moduls V durch einen 1-Kozyklus $g \in Z^1(G, V)$, S. 32

Index