Das Noethersche Problem und generische Polynome

Gregor Kemper *

IWR
Im Neuenheimer Feld 368
69 120 Heidelberg
Germany

email kemper@kalliope.iwr.uni-heidelberg.de

24. August 1994

Abstract

It is well known that an affirmative answer to Noether's Problem for a permutation group G leads to a parametric representation for all polynomials which have G as Galois group. In the first section of the present paper it is shown that in the case of a *linear* group G acting on an m-dimensional vector space over a field K, an affirmative answer affords a *generic polynomial* $g(t_1, \ldots, t_m, X)$ for G. This means that $g(X)$, considered as a polynomial over $K(t_1, \ldots, t_m)$, has Galois group G and, moreover, every Galois extension N/L with $L \geq K$ an infinite field and $\mathrm{Gal}(N/L) = G$ can be obtained by specializing the parameters t_i in $g(X)$ to values of L and taking the splitting field of the resulting polynomial over L.

The aim of the second section is to develop an algorithm which calculates the ring of invariants of a finite linear group. In Section 3, we present a strategy to find affirmative answers to Noether's problem for a given group. While many of the known results can be obtained in this way, our approach proves to be particularly successful in the modular case. Among the applications are affirmative answers to Noether's Problem for the simple subgroups $\Omega_n(q)$ of the orthogonal groups $\mathrm{O}_n(q)$ for n and q uneven and for the groups $\mathrm{CSp}_{2n}(q)$ and $\mathrm{SU}_n(q)$ (with q a square), all with their natural representation over $\mathbb{F}_q$. In many cases, the corresponding generic polynomials are calculated explicitly.

*Der Autor wird unterstützt vom Graduiertenkolleg „Modellierung und wissenschaftliches Rechnen in Mathematik und Naturwissenschaften“, welches von der DFG und vom Land Baden-Württemberg getragen wird.

Inhaltsverzeichnis

Einleitung

Problemstellung.

Das klassische *Noethersche Problem* stellt die Frage, ob der Invariantenkörper einer Permutationsgruppe G, die auf einem rationalen Funktionenkörper durch Vertauschungen der Unbestimmten operiert, wieder rein transzendent über dem Grundkörper ist. Ist dies der Fall, so bekommt man nach NOETHER [41] eine *Parameterdarstellung* für sämtliche Polynome mit Galoisgruppe G. Das Noethersche Problem stellt sich jedoch auch, wenn G als endliche lineare Gruppe auf einem m-dimensionalen K-Vektorraum operiert. Eine zentrale Idee der vorliegenden Arbeit ist, daß man dann aus einer positiven Antwort immerhin ein *generisches Polynom* $g(t_1, \ldots, t_m, X)$ in m Parametern für G erhält. Dies bedeutet, daß $g(X)$ als Polynom über $K(t_1, \ldots, t_m)$ die Galoisgruppe G hat und daß man alle galoisschen Körpererweiterungen N/L mit der Gruppe G und unendlichem Körper $L \geq K$ bekommen kann, indem man in $g(X)$ die Parameter t_i zu Werten aus L spezialisiert und dann den Zerfällungskörper über L nimmt. Da generische Polynome somit einen Überblick über sämtliche Galoiserweiterungen mit einer vorgegebenen Gruppe gewähren, sind sie natürlich sehr begehrt, allerdings auch sehr rar. Der oben genannte Zusammenhang zum Noetherschen Problem für lineare Gruppen erweist sich nun als eine Quelle besonders einfacher generischer Polynome, wie in dieser Arbeit demonstriert werden soll.

Der wesentliche Schritt besteht darin, für vorgegebene lineare Gruppen G eine positive Antwort auf das Noethersche Problem nachzuweisen. Ein weiteres Hauptanliegen dieser Arbeit ist daher, Methoden und Algorithmen zu entwickeln, mit deren Hilfe diese Frage angegangen werden kann. Eine wichtige Zwischenstation ist hierbei die Berechnung des *Invariantenrings*, die weitgehend algorithmisierbar ist. Dies funktioniert allerdings nicht im *modularen* Fall, d.h. wenn die Gruppenordnung $|G|$ ein Vielfaches der Charakteristik des Grundkörpers K ist. Gerade dieser Fall ist aber besonders interessant, da es zu gegebener Gruppe oft modulare Darstellungen besonders niedrigen Grades gibt, die in allgemeiner Charakteristik nicht vorhanden sind. Man hat dann gute Chancen, für diese Darstellungen positive Antworten auf das Noethersche Problem zu finden.

Der Wissensstand.

Zunächst ist klar, daß die Antwort auf das Noethersche Problem positiv ist, falls schon der Invariantenring isomorph zu einem Polynomring ist. Dies ist nach einem Satz von CHEVALLEY und SHEPHARD-TODD im nicht modularen Fall genau für die Spiegelungsgruppen (siehe Abschnitt 2.1) der Fall. Für die Mehrzahl der mathematisch relevanten Gruppen ist die Antwort bisher jedoch nicht bekannt. Von einem einigermaßen umfassenden Überblick ist man noch weit entfernt.

Schon als E. NOETHER die Frage 1918 formulierte [41], war bekannt, daß sie für eine abelsche Gruppe vom Exponenten m eine positive Antwort hat, sofern der Grundkörper K eine primitive m-te Einheitswurzel enthält (FISCHER [18]). NOETHER [41] wies mit Hilfe zweier Reduktionsschritte und mit Sätzen von LÜROTH und CASTELNUOVO eine positive Antwort für alle Permutationsgruppen vom Grad ≤ 4 nach. S. BREUER hat in [7, 8, 9] positive Antworten auf das Noethersche Problem für einige zyklische und metazyklische Gruppen über dem Grundkörper $K = \mathbb{Q}$ gegeben. Die Frage, ob dies für sämtliche zyklische Gruppen möglich ist, führte über Arbeiten von MASUDA [35] und CHARNOW [13] zum ersten

Gegenbeispiel, das 1969 von SWAN [50] gegeben wurde: Für $G = Z_{47}$ ist die Antwort über dem Grundkörper $K = \mathbb{Q}$ negativ! 1974 führte LENSTRA [33] das Noethersche Problem für abelsche Gruppen auf ein rein zahlentheoretisches Kriterium zurück. Abgesehen von den Spiegelungsgruppen bilden die abelschen Gruppen damit die einzige Klasse von Gruppen, für die man einen Überblick über das Verhalten beim Noetherschen Problem hat. Während das Hindernis bei den abelschen Gruppen nur im Fehlen genügend vieler Einheitswurzeln im Grundkörper liegt, hat SALTMAN [43] im Jahre 1984 auch Gegenbeispiele über einem algebraisch abgeschlossenen Grundkörper gefunden.

Im übrigen gibt es einige sporadische Beispiele von Gruppen, für die eine positive Antwort auf das Noethersche Problem bekannt ist, so die Quaternionengruppe Q_8 (GRÖBNER [22]) und die alternierende Gruppe A_5 (MAEDA [34]). Zu den Ergebnissen im modularen Fall siehe Abschnitt 3.3.

Der Begriff der *generischen Erweiterung*, der unserem Begriff des generischen Polynoms zugrunde liegt, wurde von SALTMAN eingeführt. Die wesentlichen bisherigen Ergebnisse zu diesem Thema finden sich in seiner Arbeit [42]. Dort werden (neben einigen anderen Beispielen) generische Erweiterungen für abelsche Gruppen vom Exponenten m mit $8 \nmid m$ über dem Grundkörper $K = \mathbb{Q}$ konstruiert. Außerdem gibt SALTMAN einige Reduktionssätze an: So gewinnt man aus generischen Erweiterungen für die Gruppen G und H auch eine solche für das Kranzprodukt $H \wr G$. Entsprechendes gilt für direkte Produkte und unter gewissen Zusatzvoraussetzungen auch für semidirekte Produkte und für Faktorgruppen. Weiter finden wir in SALTMANs Arbeit einige Ergebnisse im modularen Fall, und es wird vermerkt, daß es für alle Gruppen, bei denen das *klassische* Noethersche Problem eine positive Antwort hat, eine generische Erweiterung gibt.

Aufbau der Arbeit.

Im ersten Abschnitt dieser Arbeit wird zunächst in die Thematik des Noetherschen Problems und der generischen Polynome eingeführt. Dann wird der Hauptsatz über den Zusammenhang zwischen dem Noetherschen Problem für lineare Gruppen und generischen Polynomen in mehreren Schritten bewiesen. Ohne weitere Hilfsmittel lassen sich damit schon die „klassischen“ Beispiele für generische Polynome (Polynome mit der vollen symmetrischen Gruppe, reine Polynome und Artin-Schreier Polynome) gewinnen.

Der Invariantenkörper einer endlichen Gruppe ist der Quotientenkörper des Invariantenrings. Daher liegt es nahe, zunächst den Invariantenring zu studieren. Damit beschäftigt sich Abschnitt 2 der vorliegenden Arbeit. Hier wird die Theorie der Invariantenringe endlicher Gruppen dargestellt und daraus ein Algorithmus zur Berechnung einer Präsentation des Invariantenrings entwickelt. Daneben wird in die Theorie der Spiegelungsgruppen eingeführt, die für das Noethersche Problem natürlich von großer Wichtigkeit sind.

Erst im dritten und letzten Abschnitt wenden wir uns wieder dem Invariantenkörper zu. Es geht hierbei um die Entwicklung einer Strategie zum Auffinden von Minimalbasen. Diese Strategie wird allerdings nicht algorithmisierbar sein, und es gibt keine Garantie, daß sie tatsächlich eine Minimalbasis liefert, falls das Noethersche Problem eine positive Antwort hat. Es werden dann einige Anwendungen im nicht modularen und im modularen Fall zusammengestellt. Zum Schluß stellen wir einen Reduktionssatz vor, der sich nun wieder auf das klassische Noethersche Problem anwenden läßt.

Ergebnisse.

Mit dem Hauptsatz (Satz 1.11) erhalten wir aus bisher schon bekannten Lösungen des Noetherschen Problems eine Reihe einfacher, bisher unbekannter generischer Polynome für verschiedene Gruppen. Dazu gehören die V_4, die D_4, die Z_4, die $\mathrm{SL}_2(3)$ und die A_5. Auch für die verallgemeinerten Quaternionengruppen Q_{4n} führt der Nachweis einer positiven Antwort auf das Noethersche Problem zu generischen Polynomen.

Die Existenz von generischen Polynomen über $K = \mathbb{F}_q$ kann so auch für alle p-Gruppen (wobei $q = p$), für die Gruppen $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{Sp}_{2n}(q)$, $\mathrm{O}_n(q)$ (mit ungeradem q) und $U_n(q)$ (mit q quadratisch) nachgewiesen werden. Mit den Methoden aus Abschnitt 3.1 werden Minimalbasen für die konformen symplektischen Gruppen $\mathrm{CSp}_{2n}(q)$, für die einfachen Gruppen $\Omega_n(q)$ (mit q und n ungerade), für einige Untergruppen der $\mathrm{O}_n(q)$ (mit n gerade) und für die speziellen unitären Gruppen $\mathrm{SU}_n(q)$ gefunden. Als „Nebenprodukt“ ergibt sich dabei, daß der Invariantenring der orthogonalen Gruppen $\mathrm{O}_3(q)$ mit der natürlichen Darstellung ein Polynomring ist. Damit sind die klassischen Gruppen weitgehend abgedeckt.

Die Betrachtungen in Abschnitt 3.4 ermöglichen eine positive Antwort auf das Noethersche Problem für $\mathrm{PSL}_2(7)$ mit einer beliebigen Permutationsdarstellung, wobei der Grundkörper $K = \mathbb{Q}(\sqrt{-7})$ ist.

Schließlich sei noch erwähnt, daß im Rahmen dieses Dissertationsprojekts zwei Programmpakete entstanden sind (zur Berechnung von Invariantenringen und von Körpergraden; siehe KEMPER [27] und KEMPER [28]), die in die *Maple Share Library* aufgenommen wurden.

Dank.

An erster Stelle möchte ich mich bei Herrn Prof. Dr. B. H. Matzat bedanken, der mich zu dieser Arbeit anregte und sie in allen Phasen tatkräftig unterstützte. Ihm verdanke ich unter anderem die Idee, mich überhaupt mit dem modularen Fall zu beschäftigen. Mein Dank gilt auch Frank Lübeck, Gunter Malle und Gerhard Hiß für viele wertvolle Gespräche. Viel Mühe haben sich Ralf Dentzer und meine Eltern mit dem Durchlesen der Arbeitsversion gemacht. Für ihre Korrekturen und Anregungen bin ich besonders dankbar. Schließlich bedanke ich mich beim Graduiertenkolleg „Modellierung und wissenschaftliches Rechnen in Mathematik und Naturwissenschaften“, das mich während meiner Arbeit finanziell unterstützt hat.

1 Von Minimalbasen zu generischen Polynomen

In diesem einführenden Abschnitt geht es darum, den Zusammenhang zwischen generischen Polynomen und dem Noetherschen Problem für lineare Gruppen herzustellen. Für einige Beispiele, in denen das Noethersche Problem ohne weitere Hilfsmittel lösbar ist, geben wir dann die entsprechenden generischen Polynome an.

1.1 Das Noethersche Problem

In diesem Abschnitt soll das Noethersche Problem vorgestellt werden. Außerdem legen wir einige grundlegende Bezeichnungen fest.

Invariantenringe und Invariantenkörper.

Ist K ein beliebiger Körper und V ein n-dimensionaler K-Vektorraum, so bezeichnen wir mit $V^* = \mathrm{Hom}_K(V, K)$ seinen Dualraum. Für die symmetrische Algebra $S(V^*)$ (siehe etwa LANG [32]) schreiben wir dann $K[V]$. Diese ist isomorph zur Polynomalgebra in n Unbestimmten über K, und ist zudem K ein unendlicher Körper, so identifiziert sich $K[V]$ mit einer Algebra von K-wertigen Funktionen auf V. Weiter sei

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

der rationale Funktionenkörper.

Sei nun $G \leq \mathrm{GL}(V)$ eine endliche Untergruppe der linearen Gruppe von V. Dann operiert G auf V^* vermöge

$$\sigma(f) = f \circ \sigma^{-1} \text{ für } \sigma \in G,\ f \in V^*.$$

Durch homomorphe Fortsetzung wird G zu einer Gruppe von K-Automorphismen von $K[V]$ bzw. $K(V)$. Dann heißt

$$K[V]^G = \{f \in K[V] \mid \sigma(f) = f\ \forall \sigma \in G\}$$

bzw.

$$K(V)^G = \{f \in K(V) \mid \sigma(f) = f\ \forall \sigma \in G\}$$

der **Invariantenring** bzw. der **Invariantenkörper** von G.

Ein Polynom $f \in K[V]$ heißt **Pseudo-Invariante (zum Gewicht χ)**, falls

$$\sigma(f) = \chi(\sigma) \cdot f\ \forall \sigma \in G$$

mit $\chi(\sigma) \in K$. Es folgt dann, daß χ ein Homomorphismus von G in $K^\times$ ist.

Über das Verhältnis zwischen dem Invariantenring und dem Invariantenkörper läßt sich folgendes sagen:

Proposition 1.1. *Mit den obigen Bezeichnungen gelten:*

(a) $K(V)^G = \mathrm{Quot}\left(K[V]^G\right)$.

(b) Für teilerfremde $f, g \in K[V]$ liegt f/g genau dann in $K(V)^G$, wenn f und g Pseudo-Invarianten zum gleichen Gewicht χ sind.

Beweis.

(a) Für $f/g \in K(V)^G$ mit $f, g \in K[V]$ erhält man durch Erweiterung des Bruchs mit dem Produkt aller $\sigma(g)$, $\iota \neq \sigma \in G$, eine Darstellung mit Zähler und Nenner in $K[V]^G$.

(b) Die Implikation „$\Leftarrow$“ ist klar.

Es sei also $f/g \in K(V)^G$. Für $\sigma \in G$ folgt dann

$$f \cdot \sigma(g) = \sigma(f) \cdot g,$$

also wegen der Teilerfremdheit $f = \chi(\sigma) \cdot \sigma(f)$ und $g = \chi(\sigma) \cdot \sigma(g)$ mit $\chi(\sigma) \in K[V]$. Da f und $\sigma(f)$ aber denselben Grad haben, muß $\chi(\sigma)$ eine Konstante sein. □

Noethersches Problem.

Als das **Noethersche Problem** (für G) bezeichnen wir die Frage, ob $K(V)^G$ eine rein transzendente Körpererweiterung von K ist. Hierfür ist es zwar hinreichend, aber keineswegs notwendig, daß $K[V]^G$ isomorph zu einer Polynomalgebra ist (siehe z.B. Abschnitt 2.4.1). Hat das Noethersche Problem für G eine positive Antwort, so heißt ein algebraisch unabhängiges Erzeugendensystem von $K(V)^G$ über K eine **Minimalbasis**.

Proposition 1.2. *In der obigen Situation gelten:*

(a) $K(V)$ ist endlich über $K(V)^G$, und es gilt

$$\left[K(V) : K(V)^G\right] = |G|.$$

(b) Ein Erzeugendensystem von $K(V)^G$ über K hat mindestens $n = \dim_K(V)$ Elemente.

(c) Hat K die Charakteristik 0, so gibt es ein Erzeugendensystem von $K(V)^G$, welches aus $n+1$ Elementen besteht.

(d) Ein Erzeugendensystem von $K(V)^G$ ist genau dann eine Minimalbasis, wenn es n Elemente hat.

(e) Sind $\varphi_1, \ldots, \varphi_n \in K(V)^G$ Invarianten, so bilden sie genau dann eine Minimalbasis, wenn $[K(V) : K(\varphi_1, \ldots, \varphi_n)] < 2|G|$ gilt.

Beweis. Teil (a) folgt sofort nach Galoistheorie, da G eine endliche Gruppe von K-Automorphismen von $K(V)$ ist. Insbesondere haben $K(V)$ und $K(V)^G$ denselben Transzendenzgrad über K, nämlich n, woraus (b) und (d) folgen. Teil (e) ergibt sich nun aus (a) und (d).

Für (c) sei $t_1, \ldots, t_n$ eine Transzendenzbasis von $K(V)^G$ und $L = K(t_1, \ldots, t_n)$. Dann ist $K(V)$ endlich erzeugt und algebraisch über L, also endlich. Dies gilt dann auch für $K(V)^G$, und nach dem Satz vom primitiven Element folgt $K(V)^G = K(t_1, \ldots, t_n, \vartheta)$. □

Der klassische Fall.

Den von NOETHER [41] betrachteten Spezialfall, daß G als *Permutationsgruppe* auf einer Basis $e_1, \ldots, e_n$ von V operiert, wollen wir als das **klassische Noethersche Problem** bezeichnen. Ist dann $x_1, \ldots, x_n \in V^*$ die Dualbasis, also $x_i(\xi_1 e_1 + \cdots + \xi_n e_n) = \xi_i$ für $\xi_i \in K$, so gilt

$$\sigma(x_i)\colon \sum_{j=1}^{n} \xi_j e_j \mapsto x_i \left(\sum_{j=1}^{n} \xi_j e_{\sigma^{-1}(j)} \right) = \xi_{\sigma(i)},$$

also $\sigma(x_i) = x_{\sigma(i)}$.

Die Koeffizienten des Polynoms

$$f(X) = \prod_{i=1}^{n} (X - x_i) \in K[V][X]$$

sind dann Invarianten, und falls es eine Minimalbasis $\varphi_1, \ldots, \varphi_n$ gibt, so folgt $f(X) = g(\varphi_1, \ldots, \varphi_n, X)$ mit $g(t_1, \ldots, t_n, X) \in K(t_1, \ldots, t_n)[X]$.

NOETHER hat nun gezeigt, daß $g(X)$ eine *Parameterdarstellung* für die G-Polynome ist. Dies bedeutet, daß $g(X)$ als Polynom über $K(t_1, \ldots, t_n)$ selbst die Galoisgruppe G hat, und daß sämtliche Polynome mit der Galoisgruppe G durch Spezialisierung aus $g(X)$ hervorgehen, genauer: Es gibt ein Polynom $0 \neq p \in K[x_1, \ldots, x_n]$, so daß für alle Körper $L \geq K$ und alle Polynome $h(X) \in L[X]$ mit $\mathrm{Gal}\,(h(X)) \cong G$ (als Permutationsgruppe) gilt: Ist $p(\vartheta_1, \ldots, \vartheta_n) \neq 0$ für die Nullstellen $\vartheta_1, \ldots, \vartheta_n$ von $h(X)$, so gibt es Elemente $\lambda_1, \ldots, \lambda_n \in L$, so daß $h(X) = g(\lambda_1, \ldots, \lambda_n, X)$ ist. KUYK [31] hat gezeigt, daß man trotz der Einschränkung $p(\vartheta_1, \ldots, \vartheta_n) \neq 0$ jedenfalls für alle Galoiserweiterungen N/L mit der Gruppe G durch geeignetes Spezialisieren von $g(X)$ ein erzeugendes Polynom $h(X)$ erhält. Dies wird ein Spezialfall unseres Satzes 1.11 (auf S. 16) sein und führt uns nun zunächst auf den Begriff des generischen Polynoms, der eine Abschwächung der obigen Eigenschaft von $g(X)$ darstellt.

1.2 Generische Polynome

Um einen direkten Bezug zum Begriff der generischen Erweiterung von SALTMAN zu erhalten, wollen wir diesen bei unserer Definition eines generischen Polynoms zugrunde legen. Man könnte den Begriff des generischen Polynoms auch durch die Haupteigenschaft (Proposition 1.5) definieren, die wesentlich intuitiver ist.

Die Definition.

SALTMANS Theorie der generischen Erweiterungen spielt sich im Bereich der *Ringe* ab. Bevor wir seine Definition bringen, führen wir den Begriff einer galoisschen Ringerweiterung ein.

Definition 1.3 (DEMEYER und INGRAHAM [16, S. 81]). *Sei S ein kommutativer Ring, $R \leq S$ ein Unterring und G eine endliche Gruppe von Automorphismen von S. Dann heißt S/R eine* **galoissche Ringerweiterung** *mit der Gruppe G, falls gelten:*

(a) $S^G = R$.

(b) Ist $M \lhd S$ *ein maximales Ideal und* $\mathrm{id} \neq \sigma \in G$*, so existiert ein* $x \in S$ *mit* $(\sigma(x) - x) \notin M$*.*

Definition 1.4. *Es sei* K *ein Körper und* G *eine endliche Gruppe.*

(a) Eine Erweiterung S/R *von kommutativen* K*-Algebren heißt* **generische Erweiterung** *für* G *über* K*, falls folgende Bedingungen gelten:*

(i) $R = K[t_1, \ldots, t_m, 1/s]$ *mit Unbestimmten* $t_1, \ldots, t_m$ *und* $0 \neq s \in K[t_1, \ldots, t_m]$*.*

(ii) S/R *ist galoissch mit der Gruppe* G*.*

(iii) Sei L *ein unendlicher Körper, der* K *enthält, und* N/L *eine galoissche Ringerweiterung mit der Gruppe* G*. Dann gibt es einen* K*-Algebren-Homomorphismus* $\varphi\colon R \to L$*, so daß*

$$N \cong L \otimes_R S,$$

wobei der Isomorphismus die Operation von G *respektiert. Dabei werden* L *und* N *als* R*-Algebren via* φ *betrachtet.*

(b) Seien $t_1, \ldots, t_m$ *Unbestimmte, und sei* $g(X) \in K(t_1, \ldots, t_m)[X]$ *ein separables Polynom mit höchstem Koeffizienten 1 und Nullstellen* $\vartheta_1, \ldots, \vartheta_n$ *in einem Zerfällungskörper* N *über* $K(t_1, \ldots, t_m)$*. Dann heißt* $g(X)$ *ein* **generisches Polynom** *(in* m *Parametern) für* G *über* K*, falls es ein* $0 \neq s \in K[t_1, \ldots, t_m]$ *gibt, so daß durch* $R = K[t_1, \ldots, t_m, 1/s] \subset K(t_1, \ldots, t_m)$ *und* $S = R[\vartheta_1, \ldots, \vartheta_n] \subset N$ *eine generische Erweiterung* S/R *für* G *über* K *gegeben wird.*

Anmerkung. In der Definition von SALTMAN [42] wird bei (iii) nicht vorausgesetzt, daß L ein *unendlicher* Körper ist. Für $|K| < \infty$ weicht unsere Definition also von der von SALTMAN ab. Dadurch lassen sich einige unserer Resultate leichter formulieren, in denen der Grundkörper K ein endlicher Körper $\mathbb{F}_q$ ist (siehe Abschnitt 1.4.3 und 3.3). Mit der ursprünglichen Definition von SALTMAN würden sich nämlich an den entsprechenden Stellen Polynome ergeben, die über jedem unendlichen Körper K mit $\mathbb{F}_q \subset K$ generisch sind, während wir nun einfach von generischen Polynomen über $\mathbb{F}_q$ reden können. Auf der anderen Seite ist diese Änderung der Definition nicht einschneidend, da der Fall endlicher Körper L als hinreichend geklärt gelten darf.

Vermutlich kann man (auch unter Vergrößerung von s) nicht jede generische Erweiterung aus einem generischen Polynom nach der in Definition 1.4(b) angegebenen Art gewinnen. Es ist mir jedoch kein Gegenbeispiel bekannt, welches dies belegt. ◁

Eigenschaften.

Es folgt nun die Haupteigenschaft von generischen Polynomen.

Proposition 1.5. *Sei* K *ein Körper,* G *eine endliche Gruppe und* $g(t_1, \ldots, t_m, X) \in K(t_1, \ldots, t_m)[X]$ *ein generisches Polynom für* G *über* K*. Dann gelten:*

(a) $\mathrm{Gal}\left(g(X)\right) \cong G$*.*

(b) *Sei L ein unendlicher Körper mit $K \leq L$ und N/L eine galoissche Körpererweiterung mit der Gruppe G. Dann gibt es $\lambda_1, \ldots, \lambda_m \in L$, so daß N ein Zerfällungskörper von $\bar{g}(X) = g(\lambda_1, \ldots, \lambda_m, X)$ ist.*

Beweis. Es seien $\vartheta_1, \ldots, \vartheta_n$, s, R und S wie in Definition 1.4(b).

(a) $K(t_1, \ldots, t_m)$ ist eine kommutative R-Algebra, nach DeMeyer und Ingraham [16, S. 85] ist also $K(t_1, \ldots, t_m) \otimes_R S$ galoissch über $K(t_1, \ldots, t_m)$ mit der Gruppe G. Aber $K(t_1, \ldots, t_m) \otimes_R S \cong K(t_1, \ldots, t_m, \vartheta_1, \ldots, \vartheta_n)$, also folgt $\mathrm{Gal}\left(g(X)\right) \cong G$.

(b) Wir haben $\varphi\colon R \to L$, so daß

$$N \cong L \otimes_R S.$$

Seien $\lambda_i = \varphi(t_i) \in L$ und $\alpha_i = 1 \otimes \vartheta_i \in N$. Dann gilt $N = L(\alpha_1, \ldots, \alpha_n)$.

Ist $g(X) = \sum_{i=1}^{n} a_i X^i$, so liegen die a_i im Quotientenkörper $\mathrm{Quot}(R)$. Nach DeMeyer und Ingraham [16, S. 81] ist S ein endlich erzeugter R-Modul, also sind die ϑ_i und damit die a_i ganz über R. R ist aber als Ring mit eindeutiger Primzerlegung ganz abgeschlossen (Lang [32, Ch. II, Ex. 5 und Ch. IX, § 1, Prop. 6]), also $a_i \in R$. Es folgt

$$\begin{aligned}\prod_{i=1}^{n}(X - \alpha_i) &= 1 \otimes g(X) = \sum_{i=1}^{n}(1_L \otimes a_i \cdot 1_S)X^i = \\ &= \sum_{i=1}^{n}(a_i \cdot 1_L \otimes 1_S)X^i = \sum_{i=1}^{n}\left(\varphi(a_i) \otimes 1_S\right)X^i = \bar{g}(X),\end{aligned}$$

N ist also in der Tat ein Zerfällungskörper von $\bar{g}(X)$. □

Wir zeigen noch einige weitere Eigenschaften von generischen Polynomen.

Proposition 1.6. *Es sei $g(t_1, \ldots, t_m, X) \in K(t_1, \ldots, t_m)[X]$ ein generisches Polynom für G über K. Dann gelten:*

(a) $g(X)$ ist generisch für G über jeder Körpererweiterung L von K (über der die t_i weiterhin algebraisch unabhängig sind).

(b) $g(X)$ definiert eine geometrische Erweiterung von $K(t_1, \ldots, t_m)$, d.h. K ist algebraisch abgeschlossen im Zerfällungskörper von $g(X)$ über $K(t_1, \ldots, t_m)$.

(c) Ist $L \geq K$ ein Hilbertkörper, so bleibt die Galoisgruppe von $\bar{g}(X) = g(\lambda_1, \ldots, \lambda_m, X)$ über L für unendlich viele m-Tupel $(\lambda_1, \ldots, \lambda_m) \in L^m$ isomorph zu G.

Beweis.

(a) Seien $\vartheta_1, \ldots, \vartheta_n$, s, R und S wie in Definition 1.4(b). Nach Saltman [42] ist S'/R' mit $S' = L \otimes_K S$ und $R' = L \otimes_K R$ generisch für G über L. Es gilt $R' = L[t_1, \ldots, t_m, 1/s]$, wir müssen also nur noch $S' \cong R'[\vartheta_1, \ldots, \vartheta_n]$ zeigen. Dies ist dann richtig, wenn $g(X)$ über $L(t_1, \ldots, t_m)$ die volle Galoisgruppe G hat, $\mathrm{Gal}\left(g(X)/L(t_1, \ldots, t_m)\right) \cong G$. Dann hat $R'[\vartheta_1, \ldots, \vartheta_n]$ nämlich den Rang $|G|$ über R', und S' zerfällt nicht in Komponenten.

Für den Nachweis nehmen wir eine treue Permutationsdarstellung $G \hookrightarrow S_r$. Dann operiert G auf dem rationalen Funktionenkörper $L(x_1, \ldots, x_r)$, und mit $M = L(x_1, \ldots, x_r)^G$ gilt $\mathrm{Gal}\,(L(x_1, \ldots, x_r)/M) \cong G$. Nach Proposition 1.5(b) existieren also $\lambda_1, \ldots, \lambda_m \in M$, so daß $L(x_1, \ldots, x_r)$ der Zerfällungskörper von $\bar{g}(X) = g(\lambda_1, \ldots, \lambda_m, X)$ ist, insbesondere also $\mathrm{Gal}\,(\bar{g}(X)/M) \cong G$. Die Galoisgruppe von $g(X)$ wird durch Spezialisieren allenfalls verkleinert (siehe VAN DER WAERDEN [54, §66] oder MATZAT [36, S. 127]), also

$$G \leq \mathrm{Gal}\left(g(X)/M(t_1, \ldots, t_m)\right). \tag{1.1}$$

Die Restriktionen von $M(t_1, \ldots, t_m, \vartheta_1, \ldots, \vartheta_n)$ auf $L(t_1, \ldots, t_m, \vartheta_1, \ldots, \vartheta_n)$ und von $L(t_1, \ldots, t_m, \vartheta_1, \ldots, \vartheta_n)$ auf $K(t_1, \ldots, t_m, \vartheta_1, \ldots, \vartheta_n)$ liefern Monomorphismen

$$\begin{aligned} \mathrm{Gal}\left(g(X)/M(t_1, \ldots, t_m)\right) &\hookrightarrow \mathrm{Gal}\left(g(X)/L(t_1, \ldots, t_m)\right) \hookrightarrow \\ &\hookrightarrow \mathrm{Gal}\left(g(X)/K(t_1, \ldots, t_m)\right), \end{aligned}$$

wobei die letzte Gruppe nach Proposition 1.5(a) isomorph zu G ist. Mit der Ungleichung (1.1) ergibt sich hieraus

$$G \leq \mathrm{Gal}\left(g(X)/M(t_1, \ldots, t_m)\right) \leq \mathrm{Gal}\left(g(X)/L(t_1, \ldots, t_m)\right) \leq G,$$

also $\mathrm{Gal}\left(g(X)/L(t_1, \ldots, t_m)\right) \cong G$.

(b) Sei N der Zerfällungskörper von $g(X)$ über $K(t_1, \ldots, t_m)$ und L ein Körper zwischen K und N, der über K algebraisch ist. Nach Teil (a) ist dann $g(X)$ generisch für G über L, wir erhalten nach Proposition 1.5(a) also $\mathrm{Gal}\left(N/L(t_1, \ldots, t_m)\right) \cong G$. Nach Galoistheorie folgt $L(t_1, \ldots, t_m) = K(t_1, \ldots, t_m)$, also $L = K$.

(c) Nach Teil (a) und Proposition 1.5(a) gilt $\mathrm{Gal}\left(g(X)/L(t_1, \ldots, t_m)\right) \cong G$. Die Behauptung ist somit die Definition eines Hilbertkörpers. □

1.3 Der Hauptsatz

Das Ziel dieses Abschnitts ist der Beweis des Satzes 1.11 (auf S. 16). Hierzu betrachten wir zunächst die speziellere Situation, daß G auf einem Vektorraum operiert, der in einem Permutationsmodul liegt, und führen den Beweis hierfür durch. Dann zeigen wir, daß man die Voraussetzungen abschwächen kann (Zusatz 1.10), und schließlich, daß eine Einbettung in einen Permutationsmodul immer möglich ist.

1.3.1 Beweis in einer speziellen Situation

Wir betrachten die folgende Situation:

Es sei K ein Körper und $G \leq S_n$ eine Permutationsgruppe. G operiere auf $V = K^n$ durch Vertauschung der Standardbasisvektoren e_i, und $x_1, \ldots, x_n \in K[V]$ sei die Dualbasis zu $e_1, \ldots, e_n$. Weiter sei $W \leq V$ ein m-dimensionaler, G-invarianter Unterraum mit treuer Operation von G.

Die Einschränkungen $x_i|_W$ der x_i auf W müssen nicht paarweise verschieden sein, aber G operiert treu auf der Menge $\mathcal{M} = \{x_i|_W \mid i = 1, \ldots, n\}$, da die Operation auf W^* treu ist. Setze

$$f(X) = \prod_{y \in \mathcal{M}} (X - y) \in K[W]^G[X].$$

Wir nehmen nun an, daß das Noethersche Problem für die Darstellung $G \hookrightarrow \mathrm{GL}(W)$ eine positive Antwort habe, es gebe also eine Minimalbasis $\varphi_1, \ldots, \varphi_m \in K(W)^G$. Dann kann man $f(X)$ schreiben als

$$f(X) = g(\varphi_1, \ldots, \varphi_m, X)$$

mit $g(t_1, \ldots, t_m, X) \in K(t_1, \ldots, t_m)\,[X]$.

Satz 1.7. *Mit den oben eingeführten Bezeichnungen gebe es zusätzlich einen KG-Epimorphismus $\pi\colon V \to W$, wobei KG den Gruppenring bezeichne. Dann ist $g(X)$ ein generisches Polynom für G über K.*

Beweis. Da die φ_i algebraisch unabhängig über K sind, können wir sie anstelle der t_i in Definition 1.4(b) nehmen und müssen nun zeigen, daß $f(X)$ ein generisches Polynom für G über K ist. Wir nehmen also $R = K[\varphi_1, \ldots, \varphi_m, 1/s]$ mit einem noch zu spezifizierenden $0 \neq s \in K[\varphi_1, \ldots, \varphi_m]$. Ist $\mathcal{M} = \{y_1, \ldots, y_r\}$ mit paarweise verschiedenen y_i, so setzen wir $S = R[y_1, \ldots, y_r]$ und müssen nun (ii) und (iii) aus Definition 1.4(a) für S/R nachweisen.

Wegen der Injektivität von $G \to \mathrm{GL}(W)$ gilt $\mathrm{Gal}\left(K(W)/K(W)^G\right) = G$, und da die y_i ganz $K(W)$ erzeugen, wird G durch die Restriktion von $K(W)$ auf S isomorph zu einer Gruppe von Automorphismen von S/R. Wir nehmen für s einen gemeinsamen Nenner der Koeffizienten von $f(X)$, wodurch S/R ganz wird. S^G liegt nun im Quotientenkörper von R und ist als Teilring von S ganz über R. R ist aber als Ring mit eindeutiger Primzerlegung ganz abgeschlossen (Lang [32, Ch. II, Ex. 5 und Ch. IX, § 1, Prop. 6]), also folgt der Teil (a) von Definition 1.3.

Nach dem Satz vom primitiven Element gibt es $\vartheta \in K(W)$, für welches sämtliche $\sigma(\vartheta)$, $\sigma \in G$, verschieden sind, und wir können durch Hinzumultiplizieren eines Elements von $K[\varphi_1, \ldots, \varphi_m]$ erreichen, daß ϑ in S liegt und ganz über $K[\varphi_1, \ldots, \varphi_m]$ ist. Wir nehmen nun noch die Diskriminante von ϑ als weiteren Faktor zu s hinzu. Für $\mathrm{id} \neq \sigma \in G$ gibt es dann ein zu ϑ konjugiertes Element $\vartheta' \in S$, so daß $\sigma(\vartheta') \neq \vartheta'$, und es folgt $(\sigma(\vartheta') - \vartheta') \,\big|\, s \in R^\times$, also liegt die Differenz in $S^\times$. Damit ist (b) aus Definition 1.3 erfüllt.

Es steht noch der Nachweis der Haupteigenschaft (iii) aus Definition 1.4(a) aus.

Es sei $q_1 \in K[W]$ ein gemeinsamer Nenner der φ_i. Weiter sei d der Maximalgrad (d.h. der größte Totalgrad der Monome in den Unbestimmten $\varphi_1, \ldots, \varphi_m$) von s. Dann liegt

$$q_2 = \mathrm{discr}_X(f) \cdot q_1^d s(\varphi_1, \ldots, \varphi_m) \neq 0$$

in $K[W]$. Da $\pi\colon V \to W$ als surjektiv vorausgesetzt war, ist der funktorielle Homomorphismus $\pi^*\colon K[W] \to K[V]$ injektiv, also gilt

$$h = \pi^*(q_1 \cdot q_2) \neq 0.$$

Sei jetzt $L \geq K$ ein unendlicher Körper und N/L eine galoissche Ringerweiterung mit der Gruppe G, und zwar operiere G durch $\Phi\colon G \xrightarrow{\sim} \mathrm{Gal}\,(N/L)$. Gemäß dem nachfolgenden

Lemma 1.8 existieren $\alpha_1, \ldots, \alpha_n \in N$ mit $\Phi(\sigma)(\alpha_i) = \alpha_{\sigma(i)}$ und $h(\alpha_1, \ldots, \alpha_n) \in N^\times$. Die Idee ist nun, aus den α_i Linearkombinationen ϑ_i zu bilden, die genau die Nullstellen einer Spezialisierung von $f(X)$ sind.

Wir bezeichnen den tensorierten Homomorphismus

$$N \otimes_K \pi\colon N^n = N \otimes_K V \to N \otimes_K W \subset N^n$$

auch mit π und setzen

$$\mathrm{v} = \pi \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \text{ und } \vartheta_i = y_i(\mathrm{v}) \in N \quad (i = 1, \ldots, r). \tag{1.2}$$

Für $\sigma \in G$ sei die Anwendung von $\Phi(\sigma)$ auf N^n komponentenweise definiert. Dann gilt

$$\Phi(\sigma)(\mathrm{v}) = \pi \begin{pmatrix} \Phi(\sigma)(\alpha_1) \\ \vdots \\ \Phi(\sigma)(\alpha_n) \end{pmatrix} = \pi \begin{pmatrix} \alpha_{\sigma(1)} \\ \vdots \\ \alpha_{\sigma(n)} \end{pmatrix} = \pi \left(\sigma^{-1} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \right) = \sigma^{-1}(\mathrm{v}), \tag{1.3}$$

da π G-invariant ist.

Wegen $h(\alpha_1, \ldots, \alpha_n) \in N^\times$ ist $q_1(\mathrm{v}) \in N^\times$, also sind die $\lambda_i = \varphi_i(\mathrm{v})$ definiert, und wegen $q_2(\mathrm{v}) \in N^\times$ liegt auch $s(\mathrm{v})$ in $N^\times$. Man kann also alle Elemente von $S \subset K(W)$ bei v auswerten und erhält so einen Homomorphismus

$$\varphi\colon S \to N.$$

Nach Gleichung (1.3) gilt

$$\Phi(\sigma)(\lambda_i) = \varphi_i\left(\Phi(\sigma)(\mathrm{v})\right) = \varphi_i\left(\sigma^{-1}(\mathrm{v})\right) = \sigma(\varphi_i)(\mathrm{v}) = \lambda_i,$$

da $\varphi_i \in K(W)^G$. Damit liegen die λ_i in $N^G = L$. Weiter haben wir

$$\Phi(\sigma)\left(x_i(\mathrm{v})\right) = x_i\left(\Phi(\sigma)(\mathrm{v})\right) = x_i\left(\sigma^{-1}(\mathrm{v})\right) = \sigma(x_i)(\mathrm{v}),$$

also ist φ ein KG-Homomorphismus.

Wegen $q_2(\mathrm{v}) \neq 0$ wird durch φ eine mit der Operation von G verträgliche Bijektion zwischen $\mathcal{M}$ und der Menge $\{\vartheta_1, \ldots, \vartheta_r\}$ (mit $\vartheta_i = \varphi(y_i)$ aus (1.2)) gegeben. Damit operiert G treu auf dieser Menge, für $\sigma \neq \mathrm{id}$ gibt es also ein ϑ_i mit $\sigma(\vartheta_i) = \vartheta_j$, $j \neq i$. Es folgt $(\sigma(\vartheta_i) - \vartheta_i) \,|\, q_2(\mathrm{v}) \in N^\times$, also $\sigma(\vartheta_i) - \vartheta_i \in N^\times$. Damit ist $N' := L[\vartheta_1, \ldots, \vartheta_r]$ eine galoissche Erweiterung über L mit der Gruppe G, es folgt also $\dim_L(N') = |G| = \dim_L(N)$ nach DeMeyer und Ingraham [16, S. 85]. Dies zeigt $N = L[\vartheta_1, \ldots, \vartheta_r]$.

Es seien $T_1, \ldots, T_r$ Unbestimmte und $I \trianglelefteq R[T_1, \ldots, T_r]$ der Kern von

$$R[T_1, \ldots, T_r] \to S,\ T_i \mapsto y_i.$$

Die koeffizientenweise Anwendung von φ auf $R[T_1, \ldots, T_r]$ ergibt einen Homomorphismus $\psi\colon R[T_1, \ldots, T_r] \to L[T_1, \ldots, T_r]$. Weiter sei $J \trianglelefteq L[T_1, \ldots, T_r]$ das Erzeugnis von $\psi(I)$. Mit der Abbildung $L[T_1, \ldots, T_r] \to N$, $T_i \mapsto \vartheta_i$ erhalten wir dann folgendes kommutatives Diagramm:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I & \longrightarrow & R[T_1,\ldots,T_r] & \longrightarrow & S & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \psi|_I} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \varphi} & & \\ 1 & \longrightarrow & J & \longrightarrow & L[T_1,\ldots,T_r] & \longrightarrow & N & \longrightarrow & 1 \end{array}$$

Die obere Zeile ist exakt, und ebenso die untere an den Stellen J und N. Wir weisen nun die Exaktheit bei $L[T_1,\ldots,T_r]$ nach. Aus der Kommutativität des Diagramms folgt, daß J im Kern von $L[T_1,\ldots,T_r] \to N$ liegt. Nun enthält I Polynome $g_i \in R[T_1,\ldots,T_i]$ $(i = 1,\ldots,r)$ mit $\prod_{i=1}^{r} \deg_{T_i}(g_i) = |G|$, wo $\deg_{T_i}(g_i)$ den Grad in T_i bezeichnet. Dabei kommt g_i nämlich vom Minimalpolynom von y_i über $R[y_1,\ldots,y_{i-1}]$. Durch Anwendung von ψ folgt

$$\dim_L \Big(L[T_1,\ldots,T_r] \Big/ J \Big) \le |G|.$$

(Sollte es dabei Probleme geben, weil Koeffizienten der g_i unter φ zu 0 spezialisieren, so nehme man diese zu s hinzu.) Da andererseits $\dim_L(N) = |G|$ gilt, muß J der volle Kern sein, womit die Exaktheit der unteren Zeile des Diagramms bewiesen ist. Die Isomorphie

$$N \cong L \otimes_R S$$

folgt nun nach Lemma 1.9. Daß der im Beweis zu Lemma 1.9 konstruierte Isomorphismus die Operation von G respektiert, liegt daran, daß das dortige φ_2 unserem $\varphi\colon S \to N$ entspricht, welches ein G-Homomorphismus ist. □

Zwei Lemmata.

In dem Beweis wurde auf zwei Lemmata vorverwiesen, die jetzt bewiesen werden sollen. Das erste findet sich im wesentlichen (und für den Spezialfall transitiver Gruppen G) schon bei KUYK [31]; siehe auch SALTMAN [42].

Lemma 1.8. *Sei L ein unendlicher Körper, $G \le S_n$ eine Permutationsgruppe, N/L eine galoissche Ringerweiterung mit der Gruppe G und $0 \ne f \in L[x_1,\ldots,x_n]$ ein Polynom. Dann existieren $\alpha_1,\ldots,\alpha_n \in N$ mit*

(a) $\sigma(\alpha_i) = \alpha_{\sigma(i)}$ *für alle* $\sigma \in G$,

(b) $f(\alpha_1,\ldots,\alpha_n) \in N^\times$.

Beweis. Nach SALTMAN [42] gibt es eine Normalbasis $\{\vartheta_\sigma \mid \sigma \in G\} \subset N$ von N/L. Wir konstruieren paarweise verschiedene $\beta_1,\ldots,\beta_n \in N$ mit $\sigma(\beta_i) = \beta_{\sigma(i)}$ auf folgende Weise.

Seien $B_1,\ldots,B_r \subset \{1,\ldots,n\}$ die Bahnen von G, $m_i \in B_i$ jeweils irgendein Element und $H_i = \{\sigma \in G \mid \sigma(m_i) = m_i\} \le G$ die Fixgruppe. Wir setzen

$$\beta_{\sigma(m_i)} = \sum_{\rho \in H_i} \vartheta_{\sigma\rho}.$$

Wegen

$$\sum_{\rho\in H_i} \vartheta_{\sigma\rho} = \sum_{\rho\in H_i} \vartheta_{\tau\rho} \iff \sigma^{-1}\tau \in H_i \iff \sigma(m_i) = \tau(m_i)$$

sind die $\beta_{\sigma(m_i)}$ dadurch wohldefiniert und verschieden. Wir haben außerdem $\sigma(\beta_j) = \beta_{\sigma(j)}$.

Die Gleichungen

$$\beta_{j'} = \beta_j + \gamma_i \text{ mit } j \in B_i,\ j' \in B_{i'},\ i' < i$$

für ein $\gamma_i \in L$ bilden nur endlich viele Bedingungen, und jede wird höchstens von einem γ_i erfüllt. Da L unendlich ist, kann man γ_i so wählen, daß keine der Gleichungen gilt. Geht man die B_i nacheinender durch, so kann man also die β_j durch Hinzuaddieren von Konstanten aus L paarweise verschieden wählen.

Es sei $\widetilde{L} = L(x_1, \ldots, x_n)$, $\widetilde{N} = N(x_1, \ldots, x_n)$ und $\widetilde{\beta}_i = \sum_{j=1}^n x_j \cdot \beta_i^{j-1} \in \widetilde{N}$. Dann gilt $\sigma(\widetilde{\beta}_i) = \widetilde{\beta}_{\sigma(i)}$, wobei G auf den x_i trivial operiere. Die Übergangsdeterminante von den x_i zu den $\widetilde{\beta}_i$ ist $D = \prod_{i<j}(\beta_i - \beta_j) \in N$. D teilt $\prod_{i\neq j}(\beta_i - \beta_j) \in L^\times$, liegt also selbst in $N^\times$. Damit sind die $\widetilde{\beta}_i$ algebraisch unabhängig über L. Mit

$$f^*(x_1, \ldots, x_n) = \prod_{\sigma\in G} f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) \neq 0$$

folgt dann $f^*(\widetilde{\beta}_1, \ldots, \widetilde{\beta}_n) \neq 0$. Aber $f^*(\widetilde{\beta}_1, \ldots, \widetilde{\beta}_n)$ ist ein Polynom in den x_i über N, und nach Konstruktion von f^* invariant unter allen $\sigma \in G$, also $f^*(\widetilde{\beta}_1, \ldots, \widetilde{\beta}_n) = g(x_1, \ldots, x_n) \in L[x_1, \ldots, x_n]$. Da L unendlich ist, existieren $\xi_1, \ldots, \xi_n \in L$ mit $g(\xi_1, \ldots, \xi_n) \in L^\times$. Die $\alpha_i = \sum_{j=1}^n \xi_j \cdot \beta_i^{j-1}$ erfüllen dann die Behauptung (a) und $f^*(\alpha_1, \ldots, \alpha_n) \in L^\times$, woraus (b) folgt. □

Lemma 1.9. *Es seien R und L kommutative Ringe, und L werde durch einen Homomorphismus $\varphi\colon R \to L$ zur R-Algebra. Weiter seien $T_1, \ldots, T_r$ Unbestimmte, $I \trianglelefteq R[T_1, \ldots, T_r]$ ein Ideal und $S = R[T_1, \ldots, T_r]\big/ I$. Sei $J \trianglelefteq L[T_1, \ldots, T_r]$ das Erzeugnis von $\varphi(I)$. Dann gilt*

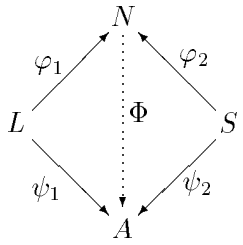
$$L \otimes_R S \cong L[T_1, \ldots, T_r]\big/ J.$$

Beweis. Sei $N = L[T_1, \ldots, T_r]\big/ J$. Nach Lang [32, Ch. XVI, § 4] müssen wir zeigen, daß N die universelle Abbildungseigenschaft von Koprodukten von kommutativen R-Algebren erfüllt. Wir haben R-Homomorphismen

$$\begin{aligned} \varphi_1\colon &\quad L \to N, &\quad l &\mapsto l + J, \\ \varphi_2\colon &\quad S \to N, &\quad f + I &\mapsto \varphi(f) + J. \end{aligned}$$

Dabei ist φ_2 wohldefiniert.

Sei nun A irgendeine kommutative R-Algebra mit R-Homomorphismen $\psi_1\colon L \to A$ und $\psi_2\colon S \to A$. Zu zeigen ist, daß es genau einen R-Homomorphismus Φ gibt, so daß folgendes Diagramm kommutiert:



Die Eindeutigkeit ist klar: Es muß $\Phi(l+J) = \psi_1(l)$ für $l \in L$ und $\Phi(T_i + J) = \psi_2(T_i + I)$ sein, also

$$\Phi\left(f(T_1,\ldots,T_r)+J\right) = \psi_1(f)\left(\psi_2(T_1+I),\ldots,\psi_2(T_r+I)\right)$$

für $f \in L[T_1,\ldots,T_r]$.

Wenn gezeigt ist, daß das Φ dadurch eindeutig definiert ist, so folgen die gewünschten Eigenschaften sofort. Es sei also $f \in J$. Dann existieren $g_i \in I$ und $h_i \in L[T_1,\ldots,T_r]$ $(i = 1,\ldots,s)$, so daß

$$f = \sum_{i=1}^{s} h_i \cdot \varphi(g_i) = \sum_{i=1}^{s} g_i \cdot h_i,$$

da $g_i \in R[T_1,\ldots,T_r]$. Es folgt $\psi_1(f) = \sum_{i=1}^{s} g_i \cdot \psi_1(h_i)$, aber

$$g_i\left(\psi_2(T_1+I),\ldots,\psi_2(T_r+I)\right) = \psi_2\left(g_i(T_1,\ldots,T_r)+I\right) = 0,$$

also $\Phi(f) = 0$. □

1.3.2 Beweis des allgemeinen Falles

Abschwächung der Voraussetzungen.

Die in Satz 1.7 vorausgesetzte Existenz eines KG-Epimorphismus $\pi\colon V \to W$ ist nach dem Satz von Maschke immer gewährleistet, falls die Charakteristik von K kein Teiler der Gruppenordnung $|G|$ ist. Sie ist trivialerweise gewährleistet, falls $V = W$, womit der klassische Fall des Noetherschen Problems also schon erledigt wäre. Ist allerdings die Charakteristik des Grundkörpers ein Teiler der Gruppenordnung, so existiert π im allgemeinen nicht. Es lohnt sich also, die Voraussetzung in Satz 1.7 loszuwerden.

Zusatz 1.10. *Satz 1.7 gilt auch ohne die Existenz von π.*

Beweis. Die Idee ist, V in einen größeren Permutationsmodul einzubetten.

Wir haben $G \leq S_n$, und $m_1,\ldots,m_s \in \{1,\ldots,n\}$ seien Vertreter der G-Bahnen. Die Fixgruppe von m_i bezeichnen wir mit $H_i \leq G$. Weiter sei $v_1,\ldots,v_r$ ein Erzeugendensystem von W als KG-Modul. Wir machen nun Gebrauch von der natürlichen Operation von G auf seine $r \cdot s$-fache disjunkte Vereinigung

$$\mathcal{M} = \bigcup_{i=1}^{s} \bigcup_{j=1}^{r} \left(\{i\} \times \{j\} \times G\right).$$

Dazu gehört der Permutationsmodul

$$\widetilde{V} = \bigoplus_{(i,j,\tau)\in\mathcal{M}} K\widetilde{e}_{i,j,\tau} \text{ mit } \sigma(\widetilde{e}_{i,j,\tau}) = \widetilde{e}_{i,j,\sigma\tau}.$$

Die Vorschrift

$$\Phi\colon V \to \widetilde{V},\ e_{\sigma(m_i)} \mapsto \sum_{j=1}^{r} \sum_{\tau\in H_i} \widetilde{e}_{i,j,\sigma\tau}$$

liefert nun einen (wohldefinierten) KG-Monomorphismus. Es sei $\widetilde{W} = \Phi(W)$, und $\Psi\colon K(W) \xrightarrow{\sim} K(\widetilde{W})$ sei die Inverse von $(\Phi|_W)^*$. Dann ist $\Psi(\varphi_1), \ldots, \Psi(\varphi_m)$ eine Minimalbasis von $K(\widetilde{W})^G$, und wir erhalten

$$\widetilde{f}(X) := \prod_{y\in\{\widetilde{x}_{i,j,\sigma}|_{\widetilde{W}} \mid (i,j,\sigma)\in\mathcal{M}\}} \Big(X - y\Big) = \widetilde{g}\Big(\Psi(\varphi_1), \ldots, \Psi(\varphi_m),\, X\Big)$$

mit $\widetilde{g}(t_1, \ldots, t_m,\, X) \in K(t_1, \ldots, t_m)[X]$, wobei $\{\widetilde{x}_{i,j,\sigma} \mid (i,j,\sigma) \in \mathcal{M}\} \subset K[\widetilde{V}]$ die Dualbasis zu $\{\widetilde{e}_{i,j,\sigma} \mid (i,j,\sigma) \in \mathcal{M}\}$ sei.

Als zweiten wichtigen Bestandteil des Beweises liefert

$$\pi\colon \widetilde{V} \to \widetilde{W},\ \widetilde{e}_{i,j,\sigma} \mapsto \Phi\Big(\sigma(v_j)\Big)$$

einen KG-Epimorphismus. Die Voraussetzung in Satz 1.7 ist also für die Permutationsdarstellung von G auf $\mathcal{M}$ erfüllt, also ist $\widetilde{g}(X)$ generisch für G. Wir zeigen jetzt $\widetilde{g} = g$.

Dazu berechnen wir

$$\begin{aligned}
\widetilde{x}_{i,j,\sigma}\Big(\Phi(e_{\tau(m_k)})\Big) &= \sum_{l=1}^{r}\sum_{\rho\in H_i} \widetilde{x}_{i,j,\sigma}(\widetilde{e}_{k,l,\tau\rho}) = \left\{ \begin{array}{ll} 0, & i \neq k \\ \displaystyle\sum_{\rho\in H_i} \widetilde{x}_{i,j,\sigma}(\widetilde{e}_{i,j,\tau\rho}), & i = k \end{array} \right\} \\
&= \left\{ \begin{array}{ll} 1, & i = k \text{ und } \sigma \in \tau H_i \\ 0, & \text{sonst} \end{array} \right\} = \left\{ \begin{array}{ll} 1, & \sigma(m_i) = \tau(m_k) \\ 0, & \text{sonst} \end{array} \right. ,
\end{aligned}$$

also $\widetilde{x}_{i,j,\sigma} \circ \Phi = x_{\sigma(m_i)}$ und daraus $\widetilde{x}_{i,j,\sigma}|_{\widetilde{W}} = \Psi(x_{\sigma(m_i)}|_W)$. Die meisten der $\widetilde{x}_{i,j,\sigma}|_{\widetilde{W}}$ sind also gleich!

Wir erhalten aus der Definition von $f(X)$ und $\widetilde{f}(X)$ nun

$$\Psi\Big(f(X)\Big) = \widetilde{f}(X),$$

also in der Tat $\widetilde{g} = g$. □

Einbettung in eine Permutationsdarstellung.

Nun sind wir in der Lage, den Hauptsatz zu beweisen.

Satz 1.11. *Eine positive Antwort auf das Noethersche Problem für eine treue lineare Darstellung einer endlichen Gruppe G führt zu einem generischen Polynom für G.*

Genauer: Es sei K ein Körper, V ein m-dimensionaler K-Vektorraum und $G \leq \mathrm{GL}(V)$ eine endliche Gruppe von regulären linearen Abbildungen von V. Weiter gebe

es $\varphi_1, \ldots, \varphi_m \in K(V)^G$, so daß $K(V)^G = K(\varphi_1, \ldots, \varphi_m)$ gilt. Ist dann $\mathcal{M} \subset V^*$ eine endliche, G-stabile Teilmenge des Dualraums $V^* \subset K[V]$, die ganz V^* als K-Vektorraum erzeugt, so sei

$$f(X) = \prod_{y \in \mathcal{M}} (X - y) \in K[V]^G[X],$$

also $f(X) = g(\varphi_1, \ldots, \varphi_m, X)$ mit $g(t_1, \ldots, t_m, X) \in K(t_1, \ldots, t_m)[X]$. Dann ist $g(X)$ ein generisches Polynom für G über K.

Beweis. G operiert als Permutationsgruppe auf $\mathcal{M}$. Um zu der Situation von Abschnitt 1.3.1 zu gelangen, bilden wir $\widetilde{V} = \bigoplus_{y \in \mathcal{M}} K e_y$ mit formalen Basisvektoren e_y und definieren

$$\Phi\colon V \to \widetilde{V},\ v \mapsto \sum_{y \in \mathcal{M}} y(v) \cdot e_y.$$

Man überzeugt sich leicht, daß dies ein KG-Monomorphismus ist.

Es seien $\widetilde{W} = \Phi(V)$ und $\Psi\colon K[V] \xrightarrow{\sim} K[\widetilde{W}]$ die Inverse von Φ^*. Ist $\{x_y | y \in \mathcal{M}\} \subset \widetilde{V}^*$ die Dualbasis zu $\{e_y | y \in \mathcal{M}\}$, so gilt für $v \in V$ und $y \in \mathcal{M}$

$$x_y\Big(\Phi(v)\Big) = y(v),$$

also $x_y|_{\widetilde{W}} = \Psi(y)$.

Aus Zusatz 1.10 erhalten wir ein generisches Polynom $\tilde{g}(X)$, und es folgt nun wie im obigen Beweis, daß $g = \tilde{g}$ gilt. □

Anmerkung.

(a) Die Frage, ob mit Satz 1.11 sämtliche generische Erweiterungen gewonnen werden können, muß zumindest für den Grundkörper $K = \mathbb{Q}$ negativ beantwortet werden, denn für die zyklische Gruppe Z_{47} der Ordnung 47 gibt es nach SALTMAN [42] eine generische Erweiterung, nach SWAN [50] und LENSTRA [33] hat jedoch das Noethersche Problem für jede treue lineare Darstellung von Z_{47} eine negative Antwort. Dies ist auch kaum zu erwarten, da im Beweis zu Satz 1.7 die ϑ_i durch eine *lineare* Transformation aus den α_i gewonnen werden. Im allgemeinen ist für einen solchen Normalisierungsprozeß jedoch irgendeine rationale Transformation möglich.

(b) Hat man für eine treue, endlich dimensionale lineare Darstellung $G \hookrightarrow \mathrm{GL}(V)$ einer endlichen Gruppe G eine Minimalbasis des Invariantenkörpers gefunden, so stellt sich die Aufgabe, Vektoren $0 \neq v \in V^*$ mit möglichst kurzen Bahnen oder, äquivalent, mit möglichst großen Fixgruppen $H \leq G$ zu finden. Dann bekommt man nämlich eine erträglich kleine Menge $\mathcal{M} \subset V^*$ und damit ein generisches Polynom von geringem Grad. Im Falle $\mathrm{char}(K) \nmid |G|$ läßt eine Untergruppe $H \leq G$ genau dann einen nichttrivialen Vektor fest, wenn für den zu der Darstellung $G \to \mathrm{GL}(V)$ gehörenden Charakter χ gilt:

$$\sum_{\sigma \in H} \chi(\sigma) > 0. \tag{1.4}$$

Die Suche nach Vektoren mit kurzer Bahn reduziert sich also auf die Suche nach möglichst großen Untergruppen H mit der Eigenschaft (1.4). ◁

Ein Zusatz.

Wir nennen eine rationale Funktion f **homogen**, falls sie Quotient von homogenen Polynomen ist. Ihr Grad $\deg(f)$ ist dann die Differenz aus Zählergrad und Nennergrad. In Abschnitt 3.1.1 werden wir zeigen, daß für endliche $G \leq \mathrm{GL}(V)$ folgendes gilt: Falls es ein homogenes Erzeugendensystem $\varphi_1, \ldots, \varphi_r$ von $K(V)^G$ gibt, so kann man dieses auch so wählen, daß $\deg(\varphi_1) = e$ und $\deg(\varphi_2) = \ldots = \deg(\varphi_r) = 0$ gilt, wo e die Anzahl der skalaren $\sigma \in G$ ist, also der Elemente von G, die auf V als Multiplikation mit einem Körperelement aus K wirken. In diesem Lichte erscheinen die Voraussetzungen des folgenden Zusatzes durchaus nicht exotisch.

Zusatz 1.12. *Es seien die Voraussetzungen von Satz 1.11 gegeben, und zudem seien $\varphi_1, \ldots, \varphi_m$ homogen mit*

$$\deg(\varphi_1) = 1 \text{ und } \deg(\varphi_2) = \ldots = \deg(\varphi_m) = 0.$$

Dann ist

$$g(1, t_2, \ldots, t_m, X)$$

(d.h. in g wird $t_1 = 1$ gesetzt) ein generisches Polynom in $m-1$ Parametern für G über K.

Beweis. Sei $h(X) = t_1^{-n} \cdot g(t_1 \cdot X)$, wobei n der Grad von $g(X)$, also $n = |\mathcal{M}|$ sei. Wir haben also

$$h(\varphi_1, \ldots, \varphi_m, X) = \prod_{y \in \mathcal{M}} \left(X - \frac{y}{\varphi_1} \right) \in K(V)_0^G[X],$$

wobei $K(V)_0^G$ den Körper aller Invarianten vom Grad 0 bezeichne. Wenn wir zeigen können, daß $K(V)_0^G = K(\varphi_2, \ldots, \varphi_m)$ gilt, so folgt, daß t_1 in $h(X)$ nicht vorkommt, insbesondere also $h(X) = g(1, t_2, \ldots, t_m, X)$.

Wir schreiben $N_1 = K(\varphi_2, \ldots, \varphi_m)$ und $N_2 = K(V)_0^G$. Dann gilt $N_1 \leq N_2$. Das Element φ_1 ist jedoch transzendent über N_2, und andererseits hat $K(V)^G/N_1$ den Transzendenzgrad 1, also ist N_2/N_1 algebraisch. N_2 liegt aber in $K(V)^G$, welches eine rein transzendente Erweiterung von N_1 ist, also $N_2 = N_1$.

Nach Satz 1.11 gibt es ein $0 \neq s \in K[t_1, \ldots, t_m]$, so daß $R = K[t_1, \ldots, t_m, 1/s]$ und $S = R[\vartheta_1, \ldots, \vartheta_n]$ eine generische Erweiterung für G liefert, wobei $\vartheta_1, \ldots, \vartheta_n$ die Nullstellen von $g(X)$ sind. Ein Blick in den Beweis zu Satz 1.7 zeigt, daß sich s aus dem Nenner von $g(X)$ und der Diskriminante eines Elements $\vartheta \in K(V)$ ($\cong \mathrm{Quot}(S)$) zusammensetzt. Wegen der speziellen Gestalt von $g(X)$ liegt sein Nenner in $K[t_2, \ldots, t_m]$, und außerdem kann man ϑ aus $K(V)_0$ wählen, da G treu auf diesem Körper operiert. Für unsere Zwecke ist es noch besser, t_1 zu ϑ hinzuzumultiplizieren. Es gilt dann $s = t_1^{|G|(|G|-1)} s'$ mit $s' \in K[t_2, \ldots, t_m]$.

Insbesondere folgt $1/t_1 \in R$, also $S = R[\vartheta_1', \ldots, \vartheta_n']$ mit $\vartheta_i' = \vartheta_i/t_1$, die Nullstellen von $h(X)$. Man prüft nun leicht nach, daß auch $R' = K[t_2, \ldots, t_m, 1/s']$ und $S' = R'[\vartheta_1', \ldots, \vartheta_n']$ die Eigenschaften einer generischen Erweiterung für G über K erfüllen. □

1.4 Erste Anwendungen

In diesem Abschnitt sollen einige Anwendungsbeispiele zusammengestellt werden, bei denen das Aufstellen einer Minimalbasis leicht ohne zusätzliche Hilfsmittel möglich ist. Die

Abschnitte 1.4.2 und 1.4.3 liefern dabei die seit langem bekannten klassischen Beispiele für generische Polynome. Wir übernehmen die Notation von Satz 1.11. Die Vektoren der Dualbasis zur Standardbasis des K^n werden mit $x_1, \ldots, x_n$ bezeichnet.

1.4.1 Symmetrische Gruppen

Die symmetrische Gruppe $G = S_n$ (wobei $n \geq 3$) operiere durch Vertauschungen der Standardbasisvektoren auf $V = K^n$, und wir setzen $\mathrm{char}(K) \nmid n$ voraus. Es seien $s_1, \ldots, s_n \in K[V]$ die elementarsymmetrischen Polynome und

$$W = \{v \in V \mid s_1(v) = 0\} \leq V.$$

Dann liefert $\pi\colon V \to W$, $v \mapsto v - \frac{1}{n}s_1(v)$ eine KG-Projektion, und G operiert treu auf W. Für $f \in K[W]$ ist $\pi^*(f) \in K[V]$ und $\pi^*(f)|_W = f$. Ist $f \in K[W]^G$, so folgt $\pi^*(f) \in K[V]^G = K[s_1, \ldots, s_n]$, also

$$f \in K[s_1|_W, \ldots, s_n|_W] = K[f_2, \ldots, f_n]$$

mit $f_i = s_i|_W$, da $s_1|_W = 0$. Die f_i erzeugen also $K[W]^G$. Um Zusatz 1.12 anwenden zu können, nehmen wir

$$\varphi_0 = \frac{f_3}{f_2} \text{ und } \varphi_{i-2} = (-1)^i \frac{f_i}{\varphi_0^i} \ (i = 3, \ldots, n)$$

als Minimalbasis von $K(W)^G$. Mit $\mathcal{M} = \{x_1|_W, \ldots, x_n|_W\}$ ergibt sich

$$g(X) = X^n - t_1 \cdot X^{n-2} + t_1 \cdot X^{n-3} + t_2 \cdot X^{n-4} + \cdots + t_{n-2}$$

als generisches Polynom für G in $n-2$ Parametern.

1.4.2 Kummer-Theorie

Es sei G eine endliche abelsche Gruppe vom Exponenten m, und der Grundkörper K enthalte m verschiedene m-te Einheitswurzeln, also $G \cong \mathrm{Hom}(G, K^\times)$. Ist

$$\mathrm{Hom}(G, K^\times) \cong \langle \psi_1 \rangle \times \cdots \times \langle \psi_r \rangle$$

eine Darstellung der dualen Gruppe als direktes Produkt von zyklischen Untergruppen, so wird durch

$$G \to \mathrm{GL}_r(K), \ \sigma \mapsto \begin{pmatrix} \psi_1(\sigma) & & \\ & \ddots & \\ & & \psi_r(\sigma) \end{pmatrix}$$

eine treue Darstellung gegeben. Die Invarianten $\varphi_i = x_i^{m_i}$ mit $m_i = \mathrm{ord}(\psi_i)$ bilden nach Proposition 1.2(e) eine Minimalbasis von $K(x_1, \ldots, x_r)^G$. Die Menge $\mathcal{M} = \{\psi_i(\sigma) \cdot x_i \mid i = 1, \ldots, r, \ \sigma \in G\}$ erfüllt die Voraussetzungen von Satz 1.11, und es gilt

$$f(X) := \prod_{y \in \mathcal{M}} (X - y) = \prod_{i=1}^{r} (X^{m_i} - \varphi_i).$$

Wir erhalten also

$$g(X) = \prod_{i=1}^{r} (X^{m_i} - t_i)$$

als generisches Polynom für G. Somit ergibt sich die Theorie der Kummer-Erweiterungen als einfache Anwendung von Satz 1.11.

1.4.3 Verallgemeinerte Artin-Schreier Polynome

Wir konstruieren generische Polynome für metazyklische Erweiterungen der zyklischen Gruppe Z_p über Körpern der Charakteristik p. Dies Resultat findet sich schon (in weniger expliziter Form) bei SALTMAN [42].

Es sei also p eine Primzahl, $K = \mathbb{F}_p$, m ein Teiler von $p-1$ und

$$G = \langle \sigma, \tau \mid \sigma^p = \tau^m = \iota,\ \tau^{-1}\sigma\tau = \sigma^w \rangle$$

mit einem Element w von $K^\times$ der Ordnung m. Durch

$$\sigma \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & w \end{pmatrix}$$

wird eine Darstellung auf $V = K^2$ definiert. Sie ist treu, denn $\tau^k\sigma^i(e_2) = i \cdot e_1 + w^k \cdot e_2$. Wir haben Invarianten

$$\varphi_1 = x_2^m \text{ und } \varphi_2 = \prod_{i \in \mathbb{F}_p} (x_1 - i \cdot x_2) = x_1^p - x_1 x_2^{p-1},$$

und es gilt

$$\begin{aligned} \Big[K(V) : K(\varphi_1, \varphi_2)\Big] &= \Big[K(V) : K(\varphi_2, x_2)\Big] \cdot \Big[K(\varphi_2, x_2) : K(\varphi_1, \varphi_2)\Big] \leq \\ &\leq \deg_{x_1}(\varphi_2) \cdot \deg_{x_2}(\varphi_1) = p \cdot m = |G|, \end{aligned}$$

also $K(V)^G = K(\varphi_1, \varphi_2)$ nach Proposition 1.2(e).[1]
Für $\mathcal{M}$ nehmen wir $\{x_1 - ix_2 | i \in K\}$ und erhalten

$$f(X) = \prod_{y \in \mathcal{M}} (X - y) = X^p - x_1^p - (X - x_1)x_2^{p-1} = X^p - \varphi_1^k \cdot X - \varphi_2$$

mit $k = \frac{p-1}{m}$. Damit ist schon ein generisches Polynom in zwei Parametern gefunden. Um den Zusatz 1.12 anwenden zu können, benutzen wir die neue Minimalbasis

$$\psi_1 = \frac{\varphi_2}{\varphi_1^k} \text{ und } \psi_2 = \frac{\varphi_1^p}{\varphi_2^m},$$

also

$$\varphi_1 = \psi_1^m \psi_2 \text{ und } \varphi_2 = \psi_1^p \psi_2^k.$$

Es gilt $\deg(\psi_1) = 1$ und $\deg(\psi_2) = 0$, also erhalten wir nach Zusatz 1.12

$$g(X) = X^p - t^k X - t^k \quad (k = \tfrac{p-1}{m})$$

als generisches Polynom für G.

Im Falle $m = 1$ sei ϑ eine Nullstelle von $g(X)$. Dann hat ϑ/t das Minimalpolynom $X^p - X - t^{-1}$, wir kommen also bei den Artin-Schreier Polynomen an.

[1] Es folgt nun sogar $K[V]^G = R$ mit $R = K[\varphi_1, \varphi_2]$: Jede Invariante aus $K[V]$ liegt im Quotientenkörper von R, ist aber als Element von $K[V]$ auch ganz über R. R ist jedoch als Polynomring ganz abgeschlossen.

2 Invariantenringe

In diesem Abschnitt soll der Invariantenring untersucht werden, bevor wir uns dann im nächsten wieder seinem Quotientenkörper zuwenden.

Die Invariantentheorie endlicher Gruppen erweist sich als sehr viel einfacher als die Invariantentheorie allgemeiner reduktiver Gruppen, wie schon der elementare Beweis der endlichen Erzeugung von NOETHER [40] zeigt. Einführende Darstellungen findet man in BENSON [3], STANLEY [47], STURMFELS [49] oder MCSHANE und GROVE [37]. Ziel des Abschnitts ist die Entwicklung eines Algorithmus, mit dem man für den Invariantenring einer endlichen Gruppe eine Präsentation als K-Algebra berechnen kann. Dazu tragen wir in Abschnitt 2.2 die Grundlagen der Theorie zusammen. Daraus wird dann der Algorithmus formuliert. Zunächst behandeln wir jedoch die Frage, wann schon der Invariantenring isomorph zu einer Polynomalgebra ist.

2.1 Spiegelungsgruppen

Die Frage, unter welchen Bedingungen der Invariantenring polynomial ist, führt in die Theorie der Spiegelungsgruppen, auf die in diesem Abschnitt kurz eingegangen werden soll. Hieraus ergeben sich dann einige direkte Anwendungen.

Definition und Haupteigenschaft.

Wir führen zunächst den Begriff einer Spiegelungsgruppe ein.

Definition 2.1 (BOURBAKI [6]). *Sei V ein endlich dimensionaler Vektorraum über einem Körper K. Ein Endomorphismus φ von V heißt* **Spiegelung** *(in der älteren Literatur „Pseudo-Spiegelung"), falls $\mathbf{1} - \varphi$ den Rang 1 hat.*

Eine endliche Untergruppe $G \leq \mathrm{GL}(V)$ heißt **Spiegelungsgruppe**, *falls sie von Spiegelungen erzeugt wird.*

Der Zusammenhang zur Invariantentheorie wird gegeben durch

Satz 2.2 (CHEVALLEY-SHEPHARD-TODD-BOURBAKI). *Sei K ein Körper, V ein endlich dimensionaler K-Vektorraum und $G \leq \mathrm{GL}(V)$ eine endliche lineare Gruppe. Dann gelten:*

(a) Ist $K[V]^G$ isomorph zu einer Polynomalgebra über K, so ist G eine Spiegelungsgruppe.

(b) Ist G eine Spiegelungsgruppe und $\mathrm{char}(K) \nmid |G|$, so ist $K[V]^G$ isomorph zu einer Polynomalgebra. Dabei können für die algebraisch unabhängigen Erzeuger homogene Polynome gewählt werden.

(c) Falls $K[V]^G = K[f_1, \ldots, f_n]$ isomorph ist zu einer Polynomalgebra in homogenen, algebraisch unabhängige Erzeugern f_i vom Grade d_i, so folgt

$$\prod_{i=1}^{n} d_i = |G|.$$

Die d_i aus (c) heißen die **Grade** *von G.*

Beweis. Teil (a) findet sich in BENSON [3, *Theorem* 7.2.1][2]. Teil (b) ist BOURBAKI [6, Chap. V, §5, Théorème 4], und (c) wird in [loc. cit., Chap. V, ex. 5 zu §5] gezeigt. □

Im Abschnitt 1.4.3 haben wir ein Beispiel kennengelernt, in dem der Invariantenring eine Polynomalgebra war, obwohl die Voraussetzung $\mathrm{char}(K) \nmid |G|$ in Satz 2.2(b) fehlte. Daß diese Voraussetzung dennoch nicht überflüssig ist, zeigt die Arbeit von TODA [53], in der bewiesen wird, daß der Invariantenring der Weylgruppe $W(F_4)$ zur exzeptionellen Liegruppe F_4 über $K = \mathbb{F}_3$ keine Polynomalgebra ist. Weitere Gegenbeispiele liefern die orthogonalen Gruppen $\mathrm{O}_n(q)$ für $n \geq 4$, deren Invariantenringe (bezüglich der natürlichen Darstellung über $\mathbb{F}_q$) nach NAKAJIMA [39] nicht polynomial sind.

Klassifikation.

Die Klassifikation von SHEPHARD und TODD [45] gibt einen vollständigen Überblick über die irreduziblen Spiegelungsgruppen über $K = \mathbb{C}$. Demnach gliedern sich diese Gruppen in drei unendliche Serien (die zyklischen, eindimensionalen Gruppen, die vollen symmetrischen Gruppen und eine weitere Serie, welche die Diedergruppen einschließt) und zusätzlich 34 „sporadische“ Spiegelungsgruppen. Aus der Arbeit von BENARD [2] gewinnt man zusätzliche Informationen über die Isomorphieklassen einiger Spiegelungsgruppen. Zu den Spiegelungsgruppen über $K = \mathbb{Q}_p$ und $K = \mathbb{F}_p$ siehe außerdem KANE [25].

In unserem Zusammenhang sind in erster Linie Spiegelungsgruppen über wesentlich kleineren Körpern als $\mathbb{C}$ (sogar über Körpern mit endlicher Charakteristik) interessant. Die folgende Proposition, die ich in der Literatur nirgends gefunden habe, stellt den Zusammenhang mit den komplexen Spiegelungsgruppen her.

Proposition 2.3. *Es sei G eine komplexe Spiegelungsgruppe, χ der zugehörige Charakter und I die Maximalordnung in dem von allen $\chi(\sigma)$, $\sigma \in G$, erzeugten Zahlkörper. Ist K dann ein Körper mit $\mathrm{char}(K) \nmid |G|$, so daß es einen Homomorphismus $\varphi\colon I \to K$ gibt, so existiert eine über K definierte Spiegelungsgruppe $\bar{G}$, welche (als abstrakte Gruppe) isomorph zu G ist. Außerdem haben die G und $\bar{G}$ zugrunde liegenden Vektorräume über K bzw. $\mathbb{C}$ dieselbe Dimension, und die Grade von G und $\bar{G}$ sind gleich.*

Beweis. Nach BENSON [3, Prop. 7.1.1] kann man ohne Einschränkung annehmen, daß die Matrixeinträge der Matrizendarstellung von G in $L = \mathbb{Q}(\chi(\sigma) \mid \sigma \in G)$ liegen. Nach HUPPERT [23, Kap. V, 12.5] liegen sie nach Wahl einer passenden Basis sogar in I. Wir gewinnen die Gruppe $\bar{G}$ nun, indem wir φ auf alle Matrixeinträge anwenden. Wir müssen zeigen, daß dabei ein Spiegelung von G auf eine solche von $\bar{G}$ übergeht, und daß nur das Einselement von G auf die identische Matrix in $\bar{G}$ geht.

Es sei $|G| = m$ und ζ_m eine primitive m-te Einheitswurzel über L. Dann liegt das Minimalpolynom $g(X)$ von ζ_m über L in $I[X]$, wir können also $\varphi(g) \in K[X]$ bilden und davon eine Nullstelle $\bar{\zeta}_m$ über K nehmen. Dann liefert

$$I[\zeta_m] \to K(\bar{\zeta}_m),\ f(\zeta_m) \mapsto \varphi(f)(\bar{\zeta}_m)$$

[2] Der dortige Beweis geht in allgemeiner Charakteristik.

eine Fortsetzung von φ, die wir auch mit φ bezeichnen. Ist $\mathfrak{p}$ der Kern von φ und $p = \mathrm{char}(K)$, so folgt $(p) = \mathfrak{p} \cap \mathbb{Z}$. Es gilt

$$\prod_{k=1}^{m-1} (1 - \zeta_m^k) = m,$$

wegen $p \nmid m$ liegt das Produkt also nicht in $\mathfrak{p}$ und damit auch keiner der Faktoren. Wir haben also $\varphi(\zeta_m^k) = 1$ nur für $\zeta_m^k = 1$. Ist nun $f(X) = \prod_{i=1}^n (X - \zeta_m^{k_i})$ das charakteristische Polynom zu einem $\sigma \in G$, so hat das entsprechende Element $\bar{\sigma} \in \bar{G}$ das charakteristische Polynom $\varphi(f) = \prod_{i=1}^n (X - \bar{\zeta}_m^{k_i})$. Nun folgt, daß $\bar{\sigma}$ genau dann eine Spiegelung bzw. die identische Matrix ist, wenn dies für σ der Fall ist.

Das Übereinstimmen der Grade von G und $\bar{G}$ beweisen wir durch einen Vorgriff auf Abschnitt 2.2.2. Die Molien-Reihen von G und $\bar{G}$ stimmen nämlich nach Satz 2.12 und nach Konstruktion überein. Nach Proposition 2.11 gilt jedoch

$$P_G(\lambda) = \frac{1}{(1 - \lambda^{d_1}) \cdots (1 - \lambda^{d_n})},$$

wobei $d_1, \ldots, d_n$ die Grade von G sind, und entsprechend für $\bar{G}$. □

Permutationsgruppen als Spiegelungsgruppen.

Die folgende Proposition zeigt, daß der Invariantenring einer Permutationsgruppe nur in trivialen Fällen eine Polynomalgebra ist.

Proposition 2.4. *Es sei K ein Körper, und die transitive Permutationsgruppe $G \leq S_n$ operiere auf $V = K^n$ durch Vertauschung der Standardbasisvektoren. Dann ist G genau dann eine Spiegelungsgruppe, falls $G = S_n$.*

Beweis. Aus der Zerlegung in elementfremde Zyklen folgt sofort, daß eine Permutation genau dann eine Spiegelung ist, wenn sie eine Transposition ist. Die volle S_n ist damit eine Spiegelungsgruppe. Ist umgekehrt G eine Spiegelungsgruppe, so wird G durch seine Transpositionen erzeugt.

Seien $k, l \in \{1, \ldots, n\}$ verschieden. Wegen der Transitivität von G gibt es Transpositionen $\tau_1, \ldots, \tau_m \in G$ mit $\sigma = \tau_1 \circ \ldots \circ \tau_m \colon k \mapsto l$. Wir sind fertig, wenn wir zeigen können, daß man im Falle $m > 1$ auch mit höchstens $m-1$ Transpositionen aus G auskommt. Dann folgt nämlich per Induktion $(k, l) \in G$.

Ist $\tau_m = (i, j)$ mit $i, j \neq k$, so folgt $\tau_1 \circ \ldots \circ \tau_{m-1} \colon k \mapsto l$. Es sei also $\tau_m = (i, k)$ mit $i \neq k$. Im Falle $i = l$ ist $\tau_m \colon k \mapsto l$. Ist jedoch $i \neq l$, so folgt $\tau_m \circ \sigma \colon k \mapsto l$, aber $\tau_m \circ \sigma = \tau_1^{\tau_m} \circ \ldots \circ \tau_{m-1}^{\tau_m}$ und $\tau_i^{\tau_m} \in G$. □

Es wird sich in Abschnitt 3.4 zeigen, daß man aus der Theorie der Spiegelungsgruppen dennoch auch für das klassische Noethersche Problem Nutzen ziehen kann.

Anwendungen.

Wir wollen nun als Anwendung aus den in SHEPHARD und TODD [45] erhaltenen Spiegelungsgruppen zwei Beispiele herausgreifen und für diese das generische Polynom nach Satz 1.11 berechnen.

Beispiel 2.5 (Diedergruppen). Es sei $G = \langle \sigma, \tau | \sigma^n = \tau^2 = (\sigma\tau)^2 = \iota \rangle$ für $n \geq 2$ die Diedergruppe D_n der Ordnung $2n$. Für K setzen wir

$$\mathrm{char}(K) \nmid 2n \text{ und } \zeta_n + \zeta_n^{-1} \in K$$

voraus, wo ζ_n eine primitive n-te Einheitswurzel sei. Dann wird durch

$$\sigma \mapsto \begin{cases} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, & n = 2 \\ \begin{pmatrix} 0 & 1 \\ -1 & \zeta_n + \zeta_n^{-1} \end{pmatrix}, & \text{sonst} \end{cases}, \quad \tau \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

eine treue Darstellung von G auf $V = K^2$ gegeben, so daß G als Spiegelungsgruppe operiert. Nach Satz 2.2(b) wird daher schon $K[V]^G$ durch zwei homogene Invarianten erzeugt, nach Satz 1.11 existiert also ein generisches Polynom vom Grad n (bzw. $2n$ für $n = 2$) in zwei Parametern für G über K, da die Bahn von x_1 die Länge n (bzw. $2n$) hat. Explizit erhalten wir eine Invariante

$$s_2 = x_1^2 - (\zeta_n + \zeta_n^{-1}) x_1 x_2 + x_2^2$$

vom Grad 2. Die andere erzeugende Invariante s_n muß also vom Grad n sein. Hierfür können wir im Fall $n \neq 2$ das Produkt über die Bahn von x_1 nehmen. Da nämlich die Existenz eines $s_n' \in K[V]^G$ vom Grad n mit $K[V]^G = K[s_2, s_n']$ durch Satz 2.2 gesichert ist, muß unser s_n eine Linearkombination von s_n' und einer Potenz von s_2 sein, also in der Tat $K[V]^G = K[s_2, s_n]$, falls nicht s_n eine Potenz von s_2 ist, was offenkundig nicht der Fall ist. Speziell ergibt sich:

(a) Für $n = 2$ kann man $s_1 = -x_1^2 - x_2^2$ und $s_2 = x_1 x_2$ als Erzeuger von $K[V]^G$ nehmen und erhält

$$g(X) = X^4 + t_1 \cdot X^2 + t_2^2$$

als generisches Polynom für $D_2 = V_4$. Dieses Polynom ist im Gegensatz zu dem generischen Polynom $(X^2 - t_1)(X^2 - t_2)$ für V_4 aus Abschnitt 1.4.2 irreduzibel. Es gehört zu einer anderen Permutationsdarstellung der V_4.

(b) Für $n = 4$ sind die oben angegebenen Invarianten $s_2 = x_1^2 + x_2^2$ und $s_4 = x_1^2 x_2^2$, und man erhält

$$g(X) = X^4 + t_1 \cdot X^2 + t_2$$

als generisches Polynom für D_4.

Man kann nun für beliebiges n das generische Polynom ausrechnen; es sieht jedoch nicht so aus, als ob sich sämtliche generische Polynome in einer Formel geschlossen darstellen ließen.

Zum Noetherschen Problem für D_n siehe auch KEMPER [26]. ◁

Beispiel 2.6 (Die $\mathrm{SL}_2(3)$). Nach BENARD [2] hat $G = \mathrm{SL}_2(3)$ eine zweidimensionale Spiegelungsdarstellung. Der zugehörige Charakter χ ist genau einmal im Permutationscharakter vom Grad 8 (siehe BUTLER und MCKAY [10]) enthalten. Da bei den Werten von χ dritte Einheitswurzeln vorkommen, setzen wir für den Grundkörper K folgendes voraus:

$$\mathrm{char}(K) \neq 2, 3 \text{ und } \zeta_3 \in K$$

mit einer primitiven dritten Einheitswurzel ζ_3. Nach Proposition 2.3 und Satz 2.2(b) wird der Invariantenring als Polynomalgebra über K von zwei Invarianten von den Graden 4 und 6 erzeugt, da dies die Grade von G sind. Explizit erhält man die Spiegelungsdarstellung auf folgende Weise: Ist $\psi\colon G \to \mathrm{GL}_8(K)$ die Permutationsdarstellung vom Grad 8, so liefert nach HUPPERT [23, Kap. V, 5.15]

$$\pi = \frac{\chi(\iota)}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1}) \cdot \psi$$

eine G-Projektion auf einen zweidimensionalen Unterraum $V \leq K^8$, der χ realisiert. Wir berechnen die erzeugenden Invarianten und nehmen für die Menge $\mathcal{M}$ aus Satz 1.11 die Einschränkungen der $x_1, \ldots, x_8$ auf V. Es ergibt sich

$$g(X) = X^8 + 6t_1 \cdot X^4 + t_2 \cdot X^2 - 3t_1^2$$

als generisches Polynom für $\mathrm{SL}_2(3)$. Die Rechnungen hierzu wurden mit MAPLE unter Verwendung des *Invar*-Pakets (siehe Abschnitt 2.3) durchgeführt.

Schreibt man $g(X)$ als $h(X^2)$, so ergibt sich die Diskriminante von h zu $-27(64t_1^3 + t_2^2)^2$. Man erhält also durch keine Spezialisierung von $g(X)$ ein $\mathrm{SL}_2(3)$-Polynom über $\mathbb{Q}$; dann müßte das entsprechende h nämlich die Galoisgruppe A_4 haben. Die Körper $K = \mathbb{F}_q(t)$ mit $q \equiv 1 \bmod 3$ erfüllen jedoch die Voraussetzungen, und sie sind nach FRIED und JARDEN [19, *Theorem* 12.10] auch Hilbertkörper. Über diesen Körpern erhält man also nach Proposition 1.6(c) Polynome mit der Galoisgruppe $\mathrm{SL}_2(3)$. ◁

Anmerkung. Zum Charakter $\chi + \overline{\chi}$ aus dem letzten Beispiel gehört eine treue lineare Darstellung vom Grad 4 über $\mathbb{Q}$, für die eine Antwort auf das Noethersche Problem noch aussteht. ◁

2.2 Die Struktur der Invariantenringe

Grundlegend für das Studium des Invariantenrings ist seine graduierte Struktur, von der wir auch in Abschnitt 2.3 starken Gebrauch machen werden.

2.2.1 Graduierte Algebren und Moduln

Definition 2.7. *Es sei K ein Körper. Eine* **graduierte Algebra** *über K ist eine kommutative K-Algebra mit Eins, zusammen mit einer direkten Zerlegung $A = \bigoplus_{i \in \mathbb{N}_0} A_i$ in K-Vektorräume $A_0, A_1, \ldots$, so daß gelten:*

(a) $A_0 = K$,

(b) $A_i \cdot A_j \subset A_{i+j}$ *für* $i, j \in \mathbb{N}_0$.

Sei A eine graduierte K-Algebra. Dann ist ein **graduierter Modul** *über A ein A-Modul mit einer Zerlegung $M = \bigoplus_{i \in \mathbb{N}_0} M_i$ in K-Vektorräume M_i, so daß*

$$A_i \cdot M_j \subset M_{i+j}$$

für $i, j \in \mathbb{N}_0$.

Ein Element $0 \neq f \in M_i$ *bzw.* A_i *heißt* **homogen** *vom Grad* i. *Wir schreiben* $\deg(f) = i$.

Ist V ein K-Vektorraum, so trägt $K[V]$ als symmetrische Algebra von V^* eine natürliche Struktur als graduierte Algebra. Es ergibt sich unmittelbar, daß der Invariantenring $K[V]^G$ zu einer Gruppe $G \leq \mathrm{GL}(V)$ auch eine graduierte Algebra mit $K[V]^G_i = K[V]^G \cap K[V]_i$ ist.

Homogene Erzeugung.

In der Literatur ist ständig von *homogenen* Erzeugern des Invariantenrings die Rede. Es findet sich jedoch nirgends der Beweis, daß dies keine Einschränkung ist, wenn es um die Anzahl der Erzeuger geht.

Proposition 2.8. *Sei* M *ein durch* n *Elemente erzeugter graduierter Modul über einer graduierten* K*-Algebra* A. *Dann läßt sich* M *auch durch höchstens* n homogene *Elemente erzeugen.*

Beweis. Während dieses Beweises bezeichne $\langle X \rangle$ das Erzeugnis von $X \subset M$ als A-Modul. Ist $f \in M$ bzw. A, so sei $f^{(i)} \in M_i$ bzw. A_i die homogene Komponente vom Grad i.

Sind $f_1, \ldots, f_n$ die Erzeuger von M, so setze $X_{-1} = \{f_1, \ldots, f_n\}$. Für $d = 0, 1, 2, \ldots$ konstruieren wir Teilmengen X_d und Y_d von M, die folgende Bedingungen erfüllen:

(a) $Y_d \subset X_{d-1}$,

(b) $|X_d| \leq |X_{d-1}| - |Y_d|$,

(c) $f^{(i)} = 0$ für $f \in X_d$ und $i \leq d$,

(d) Mit $Z_d = \{f^{(d)} \mid f \in Y_d\}$ gilt: Z_d ist modulo $\langle Z_0 \cup \ldots \cup Z_{d-1} \rangle \cap M_d$ linear unabhängig über K,

(e) $M_d \subset \langle Z_0 \cup \ldots \cup Z_d \rangle$,

(f) $\langle Y_0 \cup \ldots \cup Y_d \cup X_d \rangle = M$.

Dann folgt die Behauptung. Es gilt nämlich $M = \langle f_i^{(j)} \mid i = 1, \ldots, n,\ j \in \mathbb{N}_0 \rangle$, für $d_0 = \max\{d \in \mathbb{N}_0 \mid f_i^{(d)} \neq 0 \text{ für ein } i\}$ impliziert (e) also $M = \langle Z_0 \cup \ldots \cup Z_{d_0} \rangle$, aber $|Z_0 \cup \ldots \cup Z_{d_0}| \leq |X_{-1}| - |X_{d_0}| \leq n$ nach (b).

Die X_i und Y_i seien für $i < d$ konstruiert. Für Y_d nehmen wir nun eine minimale Teilmenge von X_{d-1}, so daß das in (d) definierte Z_d zusammen mit $\langle Z_0 \cup \ldots \cup Z_{d-1} \rangle \cap M_d$ den von $\{f^{(d)} \mid f \in X_{d-1}\}$ und $\langle Z_0 \cup \ldots \cup Z_{d-1} \rangle \cap M_d$ erzeugten K-Vektorraum aufspannt. Dann folgen (a) und (d). Nach Konstruktion und nach (c) läßt sich jedes $f \in X_{d-1} \setminus Y_d$ durch Subtraktion eines Elements von $\langle Y_0 \cup \ldots \cup Y_d \rangle$ zu einem $\tilde{f}$ mit $\tilde{f}^{(i)} = 0$ für $i \leq d$ machen. Mit $X_d = \{\tilde{f} \mid f \in X_{d-1} \setminus X_d\}$ folgen (b) und (c) und wegen $M = \langle Y_0 \cup \ldots \cup Y_d \cup (X_{d-1} \setminus Y_d) \rangle$ auch (f).

Wir müssen nur noch die Eigenschaft (e) zeigen. Es sei also $f \in M_d$. Wegen (f) gilt

$$f = \sum_{g \in Y_0} a_g \cdot g + \cdots + \sum_{g \in Y_{d-1}} a_g \cdot g + \sum_{g \in X_{d-1}} a_g \cdot g, \tag{2.1}$$

jeweils mit $a_g \in A$. Für $g \in X_{d-1}$ ist dabei wegen (c) und nach Konstruktion

$$(a_g \cdot g)^{(d)} = a_g^{(0)} \cdot g^{(d)} \in \langle Z_0 \cup \ldots \cup Z_d \rangle.$$

Weiter zeigen wir per Induktion nach i, daß $a_g^{(0)} = 0$ für $g \in Y_i$, $i < d$ gilt. Dies sei für $j < i$ richtig. Dann lautet die homogene Komponente von Grad i der Formel (2.1)

$$0 = \sum_{g \in Y_0} \sum_{j=1}^{i} a_g^{(j)} g^{(i-j)} + \sum_{g \in Y_1} \sum_{j=1}^{i-1} a_g^{(j)} g^{(i-j)} + \cdots + \sum_{g \in Y_{i-1}} a_g^{(1)} g^{(i-1)} + \sum_{g \in Y_i} a_g^{(0)} g^{(i)},$$

da $g^{(j)} = 0$ für $g \in Y_k$ mit $k > j$. In der Formel liegen wegen (e) alle $a^{(j)} g^{(i-j)}$ mit Ausnahme derjenigen in der letzten Summe in $\langle Z_0 \cup \ldots \cup Z_{i-1} \rangle \cap M_i$, wegen (d) folgt also, wie behauptet, $a_g^{(0)} = 0$ für $g \in Y_i$.

Für $g \in Y_i$ mit $i < d$ folgt also mit (e)

$$(a_g \cdot g)^{(d)} = \sum_{j=1}^{d} a_g^{(j)} g^{(d-j)} \in \langle Z_0 \cup \ldots \cup Z_{d-1} \rangle,$$

insgesamt liefert Formel (2.1) also $f \in \langle Z_0 \cup \ldots \cup Z_d \rangle$. □

Korollar 2.9. *Es sei A eine durch n Elemente erzeugte graduierte K-Algebra. Dann läßt sich A auch durch höchstens n* homogene *Elemente erzeugen.*

Beweis. Es sei $A = K[f_1, \ldots, f_n]$. Durch Subtraktion der $f_i^{(0)} \in K$ kann man erreichen, daß die f_i in $A^+ = \bigoplus_{i=1}^{\infty} A_i$ liegen. A^+ ist dann ein graduierter A-Modul, der von $f_1, \ldots, f_n$ erzeugt wird. Nach Proposition 2.8 wird A^+ also von homogenen Elementen $g_1, \ldots, g_m$ ($m \leq n$) als A-Modul erzeugt.

Wir zeigen durch Induktion nach i, daß A_i in $K[g_1, \ldots, g_m]$ liegt. Für $i = 0$ ist dies richtig. Sei $f \in A_i$ für $i > 0$. Dann existieren $a_j \in A$ mit

$$f = \sum_{j=1}^{m} a_j \cdot g_j = \sum_{j=1}^{m} a_j^{(i-d_j)} \cdot g_j$$

mit $d_j = \deg(g_j) > 0$ und $a_j^{(k)} = 0$ für $k < 0$. Nach der Induktionsannahme ist aber $a_j^{(i-d_j)} \in K[g_1, \ldots, g_m]$, also in der Tat $A_i \in K[g_1, \ldots, g_m]$. □

2.2.2 Poincaré-Reihen

Definition 2.10. *Sei M ein graduierter Modul über einer graduierten K-Algebra A mit endlich dimensionalen homogenen Teilräumen M_i. Dann heißt die formale Potenzreihe*

$$P_M(\lambda) = \sum_{i=0}^{\infty} \dim_K(M_i) \cdot \lambda^i$$

die **Poincaré-Reihe** *(auch Hilbert-Reihe) von M. Die Poincaré-Reihe von A erhält man, indem man A als graduierten Modul über sich selbst auffaßt.*

Sind M und N graduierte Moduln über einer graduierten K-Algebra A, so werden auch $M \oplus N$ und $M \otimes_K N$ auf natürliche Weise zu graduierten A-Moduln. Wir haben folgende Rechenregeln.

Proposition 2.11. *Seien M und N graduierte A-Moduln mit endlich dimensionalen homogenen Teilräumen. Dann gelten:*

(a) $P_{M\oplus N}(\lambda) = P_M(\lambda) + P_N(\lambda)$.

(b) $P_{M\otimes_K N}(\lambda) = P_M(\lambda) \cdot P_N(\lambda)$.

(c) Ist $A = K[f]$ mit f transzendent über K und homogen vom Grad d, so gilt

$$P_A(\lambda) = \frac{1}{1-\lambda^d}.$$

Beweis. Wir führen nur den Beweis zu Teil (b).

Der i-te homogene Teilraum von $M \otimes_K N$ wird erzeugt von allen $v \otimes w$ mit $v \in M$, $w \in N$ homogen vom Grad j bzw. k mit $j + k = i$, also

$$(M \otimes_K N)_i = \bigoplus_{j+k=i} M_j \otimes_K N_k.$$

Hieraus ergibt sich die Behauptung. □

Zerlegung von $K[V]$.

Sei V ein endlich dimensionaler Vektorraum über einem Körper K, $R = K[V]$ und $G \leq \mathrm{GL}(V)$ endlich. Wir setzen voraus, daß die Charakteristik von K kein Teiler der Gruppenordnung $|G|$ ist. Dann haben wir die gewöhnliche Darstellungstheorie über einem algebraischen Abschluß $\bar{K}$ von K (siehe z.B. HUPPERT [23, Kap. V]). Es sei also $X(G)$ die Menge der irreduziblen Charaktere von G (mit Werten in $\bar{K}$). Konjugiertheit über K ist eine Äquivalenzrelation auf $X(G)$. Mit $X_K(G)$ bezeichnen wir die Menge der Summen über jeweils eine solche Äquivalenzklasse. Zu $\psi \in X_K(G)$ ist dann

$$\pi_\psi = \frac{\chi(\iota)}{|G|} \sum_{\sigma \in G} \psi(\sigma^{-1}) \cdot \sigma$$

ein Element aus dem Gruppenring KG, wobei $\chi \in X(G)$ einer der Summanden von ψ ist. Nach HUPPERT [23, Kap. V, 5.15] sind die π_ψ orthogonale Idempotente, deren Summe 1 ergibt. Mit $R_\psi = \pi_\psi(R)$ erhalten wir also eine direkte Zerlegung von R. Der Einscharakter $\mathbf{1}$ liegt in $X_K(G)$, und es gilt $R_{\mathbf{1}} = R^G$. Man nennt $\pi_{\mathbf{1}}$ auch den **Reynolds-Operator**. Offensichtlich sind alle R_ψ graduierte Moduln über R^G. Es stellt sich heraus, daß die homogenen Komponenten von R_ψ direkte Summen von KG-Moduln mit dem Charakter ψ sind. Ist speziell ψ ein linearer Charakter, so ist R_ψ demnach der Modul der Pseudo-Invarianten zum Gewicht ψ.

Die Poincaré-Reihe $P_{R_\psi}(\lambda)$ (jetzt wieder für beliebiges $\psi \in X_K(G)$) wird auch **Molien-Reihe** genannt und mit $P_{G,\psi}(\lambda)$ bezeichnet, für $\psi = \mathbf{1}$ auch $P_G(\lambda)$. Ihr i-ter Koeffizient, dividiert durch $\deg(\psi)$, gibt an, wie oft die Darstellung mit dem Charakter ψ als direkter Summand im i-ten homogenen Teilraum R_i von R steckt, wobei $\deg(\psi)$ der Grad dieser Darstellung ist.

Die Moliensche Formel.

Der folgende, bemerkenswerte Satz erlaubt die einfache Berechnung der Molien-Reihe.

Satz 2.12 (MOLIEN). *Mit den obigen Bezeichnungen gilt im Falle* $\mathrm{char}(K) = 0$

$$P_{G,\psi} = \frac{\chi(\iota)}{|G|} \cdot \sum_{\sigma \in G} \frac{\psi(\sigma^{-1})}{\det(\mathrm{id}_V - \lambda \cdot \sigma)},$$

wo $\chi \in X(G)$ *einer der Summanden von* ψ *ist.*

Ist $\mathrm{char}(K) = p \neq 0$ *(mit* $p \nmid m := |G|$*), so wähle man je eine feste primitive* m*-te Einheitswurzel* ζ_m *bzw.* $\bar{\zeta}_m$ *über* $\mathbb{Q}$ *bzw.* K *und einen* KG*-Modul* W *mit Charakter* ψ*. Weiter sei* $g(X) = \prod_{i=1}^{r}(X - \bar{\zeta}_m^{k_i})$ *das charakteristische Polynom eines* $\sigma \in G$*, aufgefaßt als Element von* $\mathrm{GL}(W)$*. Dann definiert*

$$\psi_{Br}(\sigma) = \sum_{i=1}^{r} \zeta_m^{k_i}$$

den **Brauer-Charakter** *zu* ψ *(näheres hierzu siehe in* CURTIS *und* REINER *[15, §17]). Ebenso setzen wir*

$$\Phi_\sigma(\lambda) = \prod_{i=1}^{n}(1 - \lambda \cdot \zeta_m^{l_i}),$$

falls $f(X) = \prod_{i=1}^{n}(X - \bar{\zeta}_m^{l_i})$ *das charakteristische Polynom von* σ *als Element von* $\mathrm{GL}(V)$ *ist. Dann gilt*

$$P_{G,\psi} = \frac{d}{|G|} \cdot \sum_{\sigma \in G} \frac{\psi_{Br}(\sigma^{-1})}{\Phi_\sigma(\lambda)},$$

wobei d *der Grad eines irreduziblen Summanden* $\chi \in X(G)$ *von* ψ *ist.*

Der Beweis ist erstaunlich einfach und findet sich beispielsweise in STANLEY [47] oder BENSON [3].

Im nächsten Abschnitt werden wir sehen, wie man aus der Molien-Reihe „fast alles“ über die Struktur der Moduln R_ψ, insbesondere also des Invariantenrings, ablesen kann. Es ist also ein großer Vorteil, daß diese sich mit Satz 2.12 leicht ausrechnen läßt.

2.2.3 Die Cohen-Macaulay Eigenschaft

Parametersysteme.

Sei A eine endlich erzeugte graduierte Algebra über einem Körper K. Dann gibt es nach dem *Noetherschen Normalisierungssatz* (siehe z.B. BENSON [3, *Theorem* 2.2.7]) algebraisch unabhängige, homogene Elemente $f_1, \ldots, f_n$, so daß A ganz ist über $K[f_1, \ldots, f_n]$.

Definition 2.13. *Sei* A *eine endlich erzeugte graduierte* K*-Algebra und* M *ein graduierter* A*-Modul.

(a) *Sind* $f_1, \ldots, f_n \in A$ *homogen und algebraisch unabhängig über* K*, so daß* A *ganz ist über* $K[f_1, \ldots, f_n]$*, so heißt* $f_1, \ldots, f_n$ *ein* **homogenes Parametersystem** *von* A*.*

(b) *M heißt ein* **Cohen-Macaulay-Modul**, *falls für ein homogenes Parametersystem $f_1, \ldots, f_n$ von A gilt: M ein freier Modul über $K[f_1, \ldots, f_n]$ mit einer endlichen, aus homogenen Elementen bestehenden Basis. (Es stellt sich heraus, daß dies dann für jedes homogene Parametersystem gilt.)*

A heißt **Cohen-Macaulay-Algebra**, *falls A als Modul über sich selbst ein Cohen-Macaulay-Modul ist.*

Der Hauptsatz.

Wir wollen diese Begriffe nun auf die Invariantenringe anwenden. Es sei also V ein n-dimensionaler Vektorraum über einem Körper K und $G \leq \mathrm{GL}(V)$ endlich. Dann bilden homogene Invarianten $f_1, \ldots, f_n \in K[V]^G$ genau dann ein Parametersystem von $K[V]^G$, wenn das durch $f_1, \ldots, f_n$ gegebene Nullstellengebilde über dem algebraischen Abschluß $\bar{K}$ von K genau der Nullpunkt ist (siehe z.B. McShane und Grove [37]). Die Elemente $f_1, \ldots, f_n$ eines homogenen Parametersystems heißen auch **primäre Invarianten**.

Im Falle $\mathrm{char}(K) \nmid |G|$ gilt nun

Satz 2.14 (Hochster-Eagon). *Mit den Bezeichnungen von Seite 28 ist R_ψ für $\psi \in X_K(G)$ ein Cohen-Macaulay-Modul über R^G. Insbesondere ist der Invariantenring selbst eine Cohen-Macaulay-Algebra.*

Der Hauptteil des Beweises besteht in dem Nachweis, daß es gleichbedeutend ist, in Definition 2.13(b) „für *ein* homogenes Parametersystem“ oder „für *jedes* homogene Parametersystem“ zu schreiben. R ist nämlich ein freier Modul (mit 1 als einzigem Erzeuger!) über $K[x_1, \ldots, x_n]$, wo $x_1, \ldots, x_n$ eine Basis von V^* ist, und wir erhalten dann, daß R auch ein freier Modul mit endlicher, homogener Basis über $K[f_1, \ldots, f_n]$ für ein homogenes Parametersystem $f_1, \ldots, f_n$ von R^G ist. Mit Hilfe der Projektionen π_ψ von Seite 28 kann man nun Basen für die R_ψ „isolieren“.

Ohne die Voraussetzung $\mathrm{char}(K) \nmid |G|$ ist R^G im allgemeinen keine Cohen-Macaulay-Algebra. Ein Gegenbeispiel wird schon durch $R = \mathbb{F}_2[x_1, x_2, x_3, x_4]$ und $G = Z_4$ (mit zyklischer Vertauschung der x_i) geliefert (siehe Bertin [4]). Nach Benson [3, *Theorem* 1.3.1] ist R^G jedoch für endliche G immer eine endlich erzeugte K-Algebra.

Nach Satz 2.14 gibt es zu einem homogenen Parametersystem $f_1, \ldots, f_n$ von R^G homogene $g_1, \ldots, g_m \in R_\psi$, so daß gilt

$$R_\psi = \bigoplus_{i=1}^{m} A \cdot g_i \tag{2.2}$$

mit $A = K[f_1, \ldots, f_n]$. Die g_i heißen **sekundäre Invarianten**. Es seien $d_i = \deg(f_i)$ und $e_i = \deg(g_i)$. Da die f_i algebraisch unabhängig über K sind, haben wir $A \cong K[f_1] \otimes_K \cdots \otimes_K K[f_n]$, nach Proposition 2.11(b) und (c) also $P_A(\lambda) = \frac{1}{(1-\lambda^{d_1})\cdots(1-\lambda^{d_n})}$. Aus Gleichung (2.2) folgt nun mit Proposition 2.11(a) für die Molien-Reihe

$$P_{G,\psi}(\lambda) = \frac{\lambda^{e_1} + \cdots + \lambda^{e_m}}{(1-\lambda^{d_1}) \cdots (1-\lambda^{d_n})}. \tag{2.3}$$

Die aus Satz 2.12 gewonnene Molien-Reihe läßt sich also auf wundersame Weise stets in die Form (2.3) mit $d_i \in \mathbb{N}$ und $e_i \in \mathbb{N}_0$ bringen!

Uneindeutigkeit der Molien-Reihe.

Eine solche Darstellung ist natürlich auf verschiedene Weisen möglich (man erweitere nur mit einem $(1+\lambda^{d_i})$), und es stellt sich die Frage, ob es zu *gegebener* Darstellung der Molien-Reihe in der Form (2.3) tatsächlich primäre Invarianten $f_1, \ldots, f_n$ mit $\deg(f_i) = d_i$ gibt. Dann kann man an der Molien-Reihe auch die Grade der sekundären Invarianten ablesen. Dabei ist es natürlich wünschenswert, dies für Darstellungen mit möglichst kleinen d_i zu bekommen, weil dann auch die Anzahl und die Grade der sekundären Invarianten klein werden. Es ist gar nicht leicht, ein Beispiel anzugeben, bei dem es zu einer Darstellung der Form (2.3) keine entsprechenden primären Invarianten gibt, aber solche Beispiele existieren. In dieser Unsicherheit liegt gewissermaßen die Crux beim Berechnen von Invariantenringen.

Beispiel 2.15 (STANLEY, zu finden in SLOANE [46]). Es sei $\mathrm{char}(K) \neq 2$, $i = \sqrt{-1} \in K$, und $G \leq \mathrm{GL}_3(K)$ werde von

$$\sigma = \begin{pmatrix} -1 & & \\ & -1 & \\ & & -1 \end{pmatrix} \text{ und } \tau = \begin{pmatrix} 1 & & \\ & 1 & \\ & & i \end{pmatrix}$$

erzeugt, also $G \cong Z_2 \times Z_4$. Die Molien-Reihe ist

$$P_G(\lambda) = \frac{1}{(1-\lambda^2)^3},$$

aber der K-Vektorraum der Invarianten vom Grad 2 wird erzeugt von x_1^2, x_2^2 und x_1x_2. Es gibt also kein homogenes Parametersystem aus drei Invarianten vom Grad 2. Die Darstellung

$$P_G(\lambda) = \frac{1+\lambda^2}{(1-\lambda^2)^2(1-\lambda^4)}$$

spiegelt jedoch einen tatsächlich existierenden Satz von primären und sekundären Invarianten wider.

Daß die erste Darstellung der Molien-Reihe nicht die richtige war, kann man auch schon erkennen, indem man die Molien-Reihe zu dem durch $\sigma \mapsto -1$, $\tau \mapsto 1$ gegebenen Charakter χ berechnet:

$$P_{G,\chi}(\lambda) = \frac{2\lambda}{(1-\lambda^2)^2(1-\lambda^4)}.$$

Hierfür gibt es keine Darstellung der Form (2.3) mit dem Nenner $(1-\lambda^2)^3$.

Es stellt sich hier also die Aufgabe, eine endliche Gruppe $G \leq \mathrm{GL}_n(K)$ und Exponenten $d_1, \ldots, d_n$ anzugeben, so daß die Molienreihe $P_{G,\chi}(\lambda)$ für alle irreduziblen Charaktere χ von G eine Darstellung in der Form (2.3) mit dem Nenner $(1-\lambda^{d_1}) \cdots (1-\lambda^{d_n})$ hat, daß es aber kein Parametersystem aus Invarianten der Grade $d_1, \ldots, d_n$ gibt. ◁

Zusammenfassung.

Wir fassen die Ergebnisse über die Invariantenringe endlicher Gruppen zusammen.

Satz 2.16 (Struktur der Invariantenringe endlicher Gruppen). *Es sei K ein Körper, V ein n-dimensionaler K-Vektorraum und $G \leq \mathrm{GL}(V)$ eine endliche lineare Gruppe, deren Ordnung kein Vielfaches der Charakteristik von K sei. Es sei $R = K[V]$, und $X_K(G)$ und R_ψ für $\psi \in X_K(G)$ seien wie auf Seite 28, insbesondere also $R^G = R_{\mathbf{1}}$. Dann gelten:*

(a) Es gibt homogene Invarianten $f_1, \ldots, f_n \in R^G$, so daß für $\xi_1, \ldots, \xi_n \in \bar{K}$, dem algebraischen Abschluß von K, gilt:

$$f_i(\xi_1, \ldots, \xi_n) = 0 \ \forall i \iff \xi_1 = \ldots = \xi_n = 0.$$

Diese Bedingung ist gleichbedeutend damit, daß $f_1, \ldots, f_n$ ein homogenes Parametersystem von R^G ist.

(b) Homogene Invarianten $f_1, \ldots, f_n$ sind genau dann ein Parametersystem von R^G, wenn für ein und damit für alle $\psi \in X_K(G)$ gilt, daß R_ψ ein freier Modul mit einer endlichen, homogenen Basis über $K[f_1, \ldots, f_n]$ ist.

(c) Es seien $f_1, \ldots, f_n$ ein homogenes Parametersystem für R^G, $A = K[f_1, \ldots, f_n]$ und $R_\psi = \oplus_{i=1}^m A \cdot g_i$ mit homogenen $g_i \in R_\psi$. Mit $d_i = \deg(f_i)$ und $e_i = \deg(g_i)$ gilt dann die Formel (2.3) für die Molien-Reihe $P_{G,\psi}(\lambda)$ von R_ψ.

Die f_i aus (c) heißen **primäre Invarianten**, *und die g_i* **sekundäre Invarianten**—*letzteres nur im Falle $\psi = \mathbf{1}$. Zusammen bilden sie eine* **Cohen-Macaulay-Basis** *(auch Hironaka-Zerlegung) von R_ψ.*

Auch für unendliche, reduktive Gruppen G ist der Invariantenring eine Cohen-Macaulay-Algebra. Der Beweis ist hier jedoch wesentlich schwieriger und wurde 1974 von HOCHSTER und ROBERTS erbracht. Für endliche G beruht der einfachere Beweis auf der Tatsache, daß ein homogenes Parametersystem für $K[V]^G$ auch ein solches für $K[V]$ ist. Im allgemeinen Fall ist jedoch das Kriterium für ein homogenes Parametersystem, daß das von ihm erzeugte Nullstellengebilde gerade der sogenannte *null cone* von G ist, welcher eben im allgemeinen nicht nur aus dem Nullpunkt besteht. Näheres hierzu und zum Beweis von HOCHSTER und ROBERTS findet man bei KEMPF [29]. Selbstverständlich hat man für unendliche Gruppen auch keine Moliensche Formel und keine einfache obere Schranke für die Grade der erzeugenden Invarianten.

2.3 Der Algorithmus

Aus den Ergebnissen über die Struktur der Moduln R_ψ (insbesondere also des Invariantenrings) kann man nun leicht einen Algorithmus ableiten, der eine Cohen-Macaulay-Basis von R_ψ liefert. Werden außerdem im Falle $\psi = \mathbf{1}$ noch die Relationen zwischen den sekundären Invarianten berechnet, so erhält man eine Präsentation des Invariantenrings als kommutative K-Algebra.

Im folgenden sollen die einzelnen Schritte des Algorithmus dargestellt werden. Teilalgorithmen werden dabei entweder in Worten oder durch eine Pseudo-Programmiersprache beschrieben. Die Generalvoraussetzungen seien wie in Satz 2.16, es sei also V ein n-dimensionaler Vektorraum über einem Körper K und $G \leq \mathrm{GL}(V)$ eine endliche lineare

Gruppe, so daß $\mathrm{char}(K) \nmid |G|$. Wir schreiben $R = K[V]$ und übernehmen die Bezeichnungen R_ψ von Seite 28.

Während der Arbeiten zur vorliegenden Dissertation wurde der Algorithmus in der Programmiersprache MAPLE implementiert. Das dabei entstandene Programmpaket „*Invar*“ wurde in der *Maple Share Library* veröffentlicht und damit allgemein zugänglich gemacht. *Invar* funktioniert für $\psi = \mathbf{1}$ (also Berechnung des Invariantenrings) und $K = \mathbb{Q}$ oder ein algebraischer Zahlkörper. Bezüglich detaillierter Informationen zu dem Programmpaket sei auf die Beschreibung in KEMPER [27] verwiesen.

2.3.1 Abspalten des Fixraums

Dieser erste, vorbereitende Schritt dient lediglich der Vereinfachung der weiteren Rechnungen.

Ist $W \leq V$ der Unterraum derjenigen Vektoren, die unter der Operation von G festbleiben, so gibt es nach dem Satz von Maschke ein G-Komplement V' von W. Mit $R' = K[V']$ gilt dann

$$R \cong K[W] \otimes_K R'.$$

Für $f \otimes g \in K[W] \otimes R'$ und $\psi \in X_K(G)$ ist $\pi_\psi(f \otimes g) = \pi_\psi(f) \otimes \pi_\psi(g) = f \otimes \pi_\psi(g)$, also

$$R_\psi \cong K[W] \otimes_K R'_\psi.$$

Hat man eine Cohen-Macaulay-Basis von R'_ψ, so ergibt sich durch Hinzunahme einer Basis von W^* zu den primären Invarianten eine Cohen-Macaulay-Basis von R_ψ. Das Rechnen in R' ist jedoch wesentlich weniger aufwendig: Zum einen verringert sich die Anzahl der Variablen, zum anderen treten die Invarianten vom Grad 1 nicht mehr in Relationen auf. Beide Aspekte können zu immensen Einsparungen an Rechenzeit führen. Der Übergang von R zu R' ist eine Verallgemeinerung der „ersten Reduktion“ bei NOETHER [41], wo G als Permutationsgruppe auf einer Basis $e_1, \ldots, e_n$ von V operiert, so daß durch $\sum_{i=1}^n e_i$ auf jeden Fall ein nicht triviales Element von W gegeben ist.

Der erste Schritt des Algorithmus besteht also darin, den Fixraum W und ein G-Komplement V' auszurechnen und für die weitere Rechnung V durch V' zu ersetzen. In den folgenden Abschnitten werden wir weiterhin V statt V' schreiben und annehmen, daß die Abspaltung des Fixraums bereits erfolgt ist.

2.3.2 Berechnen von primären Invarianten

Aus der Molien-Reihe $P_G(\lambda)$ erhält man nach Satz 2.16(c) zwar *mögliche* Gradverteilungen $d_1, \ldots, d_n$ eines homogenen Parametersystems, man weiß jedoch nicht, ob ein solches zu gegebenen d_i tatsächlich existiert, geschweige denn, wie die primären Invarianten dann zu konstruieren sind. Hier ist das Verfahren auf Strategien des Ausprobierens angewiesen, die allerdings in der praktischen Erfahrung sehr gute Ergebnisse liefern.

Als erstes stellt sich die Aufgabe, die homogenen Invarianten von einem vorgegebenen Grad d zu berechnen. Hierfür bieten sich zwei einfache Methoden an.

Algorithmus 2.17 (Homogene Teilräume von R_ψ, ψ linear).

EINGABE: Ein endliches Erzeugendensystem $\sigma_1, \ldots, \sigma_r$ von $G \leq GL(V)$ und die Werte $\psi(\sigma_i)$ eines linearen Charakters $\psi \in X_K(G)$.

AUSGABE: Eine K-Basis des homogenen Teilraums $(R_\psi)_d$ vom Grad d von R_ψ.

ABLAUF: Setze ein allgemeines Polynom f in R vom Grad d mit unbestimmten Koeffizienten $\alpha_1, \ldots, \alpha_m$ (mit $m = \binom{n+d-1}{d}$) an. Die Bedingungen $\sigma_i(f) = \psi(\sigma_i) \cdot f$ führen dann auf ein lineares Gleichungssystem in den α_i über K. Aus der Lösung erhält man eine K-Basis von $(R_\psi)_d$.

Algorithmus 2.18 (Homogene Teilräume von R_ψ).

EINGABE: Alle Elemente von $G \leq \mathrm{GL}(V)$ und $\psi \in X_K(G)$.

AUSGABE: Eine K-Basis des homogenen Teilraums $(R_\psi)_d$ vom Grad d von R_ψ.

ABLAUF: Wende den Reynolds-Operator π_ψ auf sämtliche Monome in $R \cong K[x_1, \ldots, x_n]$ vom Grad d an und suche unter den erhaltenen Elementen von $(R_\psi)_d$ eine K-Basis aus.

Der Algorithmus 2.17 erweist sich in den meisten Situationen als schneller, während Algorithmus 2.18 allgemeiner ist.

Als nächste Teilaufgabe brauchen wir einen Test, der entscheidet, ob ein System von Polynomen aus R ein homogenes Parametersystem von R und damit auch von R^G ist oder nicht.

Algorithmus 2.19 (Test auf Parametersystem).

INPUT: Homogene Polynome $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$.

OUTPUT: TRUE, falls die f_i ein homogenes Parametersystem von $K[x_1, \ldots, x_n]$ bilden, sonst FALSE.

```
BEGIN
    FOR i = 1,...,n DO {
        Berechne eine Gröbnerbasis B von {f_j|_{x_i=1} | j = 1,...,n} bezüglich irgendeiner
        Termordnung ;
        IF B ≠ {1} THEN RETURN FALSE
            (Es gibt eine Nullstelle mit x_i ≠ 0.)
        ELSE { FOR j = 1,...,n DO f_j := f_j|_{x_i=0} }
            (Alle Nullstellen haben x_i = 0.)
    }
    RETURN TRUE
END.
```

Die Gültigkeit des Algorithmus geht aus den eingeklammerten Kommentaren hervor. Er bietet den Vorteil, daß die zu berechnenden Gröbnerbasen nur $n-1, n-2$ usw. Unbestimmte haben.

Wir kommen nun zum Hauptalgorithmus für die Berechnung eines Parametersystems, den wir wegen der oben angeführten Schwierigkeiten zunächst nicht vollständig spezifizieren.

Algorithmus 2.20 (Primäre Invarianten).
INPUT: Eine endliche Gruppe $G \leq \mathrm{GL}(V)$.
OUTPUT: Ein homogenes Parametersystem $f_1, \ldots, f_n$ von R^G.
BEGIN
Berechne die Molien-Reihe $P_G(\lambda)$ nach Satz 2.12;
FOR $(d_1, \ldots, d_n) \in \mathbb{N}^n$ DO {
(*Die Vektoren aus* $\mathbb{N}^n$ *werden der Reihe nach durchgegangen, beginnend mit niedrigen* d_i*.*)
IF NOT $\prod_{i=1}^{n}(1-\lambda^{d_i}) \cdot P_G(\lambda) = \sum_{i=1}^{m} \lambda^{e_i}$ mit $m \in \mathbb{N}$, $e_i \in \mathbb{N}_0$,
THEN NEXT $(d_1, \ldots, d_n)$;
Berechne mit Algorithmus 2.17 oder 2.18 K-Basen für die homogenen Teilräume $(R^G)_{d_i}$;
FOR $(f_1, \ldots, f_n)$ mit $f_i \in (R^G)_{d_i}$ DO {
(*In einer noch zu spezifizierenden Reihenfolge werden Invarianten* f_i *als Linearkombinationen der Basiselemente gebildet.*)
IF $\Big($ $(f_1, \ldots, f_n)$ bildet ein Parametersystem (Algorithmus 2.19) $\Big)$
THEN RETURN $(f_1, \ldots, f_n)$
ELSE IF (Abbruchbedingung) THEN NEXT $(d_1, \ldots, d_n)$
(*Es ist noch zu spezifizieren, wann ein Exponentenvektor* $(d_1, \ldots, d_n)$ *„aufgegeben" werden soll.*)
}
}
END.

Für die noch offenen Stellen in diesem Algorithmus konnten keine vollständig befriedigenden Lösungen gefunden werden. In der Implementierung werden zwei Varianten angeboten:

(a) Die automatische Variante:
Die f_i aus Algorithmus 2.20 sind von der Form

$$f_i = \sum_{j=1}^{m_{d_i}} \alpha_{i,j} \cdot b_j^{(d_i)},$$

wobei $\{b_1^{(d_i)}, \ldots, b_{m_{d_i}}^{(d_i)}\}$ die berechnete K-Basis von $(R^G)_{d_i}$ ist. Nun werden die Vektoren $(\alpha_{i,j}) \in \mathbb{Z}^m$ $(m = \sum_{i=1}^{n} m_{d_i})$ der Reihe nach durchgegangen, beginnend mit kleinen $|\alpha_{i,j}|$. Dabei werden solche $(\alpha_{i,j})$ übergangen, bei denen die zugehörigen f_i Linearkombinationen aus bereits getesteten f_i sind.

Die Abbruchbedingung ergibt sich in dieser Variante dadurch, daß die Suche nach zehn Versuchen (zugunsten des nächsten Exponentenvektors $(d_1, \ldots, d_n)$) aufgegeben wird.

(b) Die interaktive Variante:
Nach jedem erfolglosen Versuch fragt das System den Benutzer, welche Linearkombinationen der $b_j^{(d_i)}$ als nächstes getestet werden sollen, oder ob die Suche aufgegeben werden soll.

Es ist mir kein Beispiel bekannt, in dem nicht eine der beiden Varianten (in der Regel schon (a)) zum Ziel führte.

2.3.3 Berechnen der sekundären Invarianten

Nachdem primäre Invarianten $f_1, \ldots, f_n$ gefunden sind, geht es nun um die Berechnung einer Basis des Moduls R_ψ über $A = K[f_1, \ldots, f_n]$. Das folgende Lemma erlaubt es, einen Algorithmus hierfür anzugeben.

Lemma 2.21. *Sei M ein endlich erzeugter graduierter Modul über einer graduierten K-Algebra A, $M = \sum_{i=1}^m Af_i$ mit homogenen f_i, so daß $\deg(f_i) \leq \deg(f_j)$ für $i \leq j$ gilt. Sind dann $g_1, \ldots, g_m \in M$ homogen mit $\deg(g_i) = \deg(f_i)$ und $g_i \notin \sum_{j=1}^{i-1} Ag_j$, so folgt $M = \sum_{i=1}^m Ag_i$.*

Beweis. Wir führen den Beweis durch Induktion nach $d = \deg(f_m)$.

Die f_i mit $\deg(f_i) = d$ seien genau $f_k, \ldots, f_m$. Die Induktionsannahme liefert

$$\sum_{i=1}^{k-1} Af_i = \sum_{i=1}^{k-1} Ag_i.$$

Seien $V = (\sum_{i=1}^m Ag_i)_d$ und $W = (\sum_{i=1}^{k-1} Af_i)_d \leq V$ die homogenen Teilräume vom Grad d. Aus $g_i \notin \sum_{j=1}^{i-1} Ag_j$ folgt dann $\dim_K(V/W) \geq m - k + 1$. Wegen $M_d = W + \sum_{i=k}^m Kf_i$ ist andererseits $\dim_K(M_d/W) \leq m - k + 1$, also $M_d = V$. Dies war zu zeigen. □

Der folgende Algorithmus berechnet im Falle $\psi = \mathbf{1}$ außer den sekundären Invarianten noch ein minimales Erzeugendensystem von R^G als A-Algebra.

Algorithmus 2.22 (Sekundäre Invarianten).

INPUT: Eine endliche Gruppe $G \leq \mathrm{GL}(V)$, $\psi \in X_K(G)$ und primäre Invarianten $f_1, \ldots, f_n \in R^G$.

OUTPUT: Eine Modulbasis $g_1, \ldots, g_m$ von R_ψ als Modul über $A = K[f_1, \ldots, f_n]$.
Falls $\psi = \mathbf{1}$, zusätzlich ein minimales Erzeugendensystem $h_1, \ldots, h_r$ von $R_\psi = R^G$ als A-Algebra. Dabei sind alle g_i Potenzprodukte von h_j's.

BEGIN
Berechne die Molien-Reihe $P_{G,\psi}(\lambda)$ mit Satz 2.12;
Erhalte Grade $e_1 \leq \ldots \leq e_m$ aus $P_{G,\psi}(\lambda) \cdot \prod_{i=1}^n \left(1 - \lambda^{\deg(f_i)}\right) = \sum_{i=1}^m \lambda^{e_i}$;
r:=0;
FOR $i = 1, \ldots, m$ DO {
IF $\psi = \mathbf{1}$ THEN {
FOR $P \in$ {Potenzprodukte von $h_1, \ldots, h_r$ vom Grad e_i} DO {
IF $P \notin \sum_{j=1}^{i-1} Ag_j$ THEN {
(*Der obige Test auf Mitgliedschaft läuft auf das Lösen eines linearen Gleichungssystems über K hinaus.*)
$g_i := P$;
NEXT i
}
}
}
Berechne mit Algorithmus 2.17 oder 2.18 eine K-Basis B von $(R_\psi)_d$;

```
        For b ∈ B Do {
            If  b ∉ ∑_{j=1}^{i=1} A g_j Then {
                r := r + 1;
                h_r := b;
                g_i := b;
                Next i
            }
        }
    }
End.
```

Der Algorithmus liefert deshalb (im Falle $\psi = \mathbf{1}$) ein *minimales* Erzeugendensystem $h_1, \ldots, h_r$ von R^G als A-Algebra, weil es bei der Frage nach einem Erzeugendensystem nur darauf ankommt, für jeden Grad d den K-Vektorraum $\left(A[\sum_{i<d}(R^G)_i]\right)_d$ (d.h. den Grad-d-Anteil der von den Invarianten vom Grad $< d$ erzeugten A-Algebra) zu $(R^G)_d$ zu ergänzen.

2.3.4 Berechnen der Relationen

Im Falle $\psi = \mathbf{1}$ liefert Algorithmus 2.22 ein Erzeugendensystem $f_1, \ldots, f_n, h_1, \ldots, h_r$ von R^G als K-Algebra. Im letzten Schritt sollen in diesem Fall noch die Relationen zwischen den h_i („Syzygien erster Art“) berechnet werden, so daß man eine Präsentation des Invariantenrings als kommutative K-Algebra erhält. Dazu muß für alle Produkte $h_i \cdot g_j$ die Darstellung mit Hilfe der Cohen-Macaulay-Basis $f_1, \ldots, f_n, g_1, \ldots, g_m$ bekannt sein. Um nun ein *minimales* System von Relationen zu bekommen, stellen wir folgende Betrachtung an.

Es seien $X_1, \ldots, X_n, T_1, \ldots, T_r$ Unbestimmte, denen wir Grade $\deg(X_i) = \deg(f_i)$, $\deg(T_i) = \deg(h_i)$ zuweisen. Dann ist $S = K[X_1, \ldots, X_n, T_1, \ldots, T_r]$ eine graduierte K-Algebra, und der Kern I des Homomorphismus

$$S \to R^G,\ X_i \mapsto f_i,\ T_i \mapsto h_i$$

ist ein endlich erzeugter graduierter S-Modul. Nach Proposition 2.8 gibt es ein minimales Erzeugendensystem aus homogenen Elementen, und man bekommt ein solches, indem man für $d = 1, \ldots, \deg(h_r \cdot g_m)$ den K-Vektorraum $(\sum_{i<d} S \cdot I_i)_d$ zu I_d ergänzt. Es ergibt sich der folgende Algorithmus.

Algorithmus 2.23 (Relationen).

Input: Primäre Invarianten $f_1, \ldots, f_n$, homogene Erzeuger $h_1, \ldots, h_r$ von R^G als $K[f_1, \ldots, f_n]$-Algebra und Potenzprodukte $G_1, \ldots, G_m \in K[T_1, \ldots, T_r]$, so daß $g_i = G_i(h_1, \ldots, h_r)$ sekundäre Invarianten sind.

Output: Ein minimales Erzeugendensystem $r_1, \ldots, r_s$ des Kerns von $S \to R^G,\ X_i \mapsto f_i,\ T_i \mapsto h_i$ (siehe obige Notation).

```
Begin
    s := 0;
    For d = 1, ..., deg(h_r · g_m) Do {
```

FOR $f \in \{T_i \cdot G_j(T_1, \ldots, T_r) \mid 1 \leq i \leq r,\ 1 \leq j \leq m,\ \deg(h_i \cdot g_j) = d\}$ DO {
$M = \{r \in (r_1, \ldots, r_s) \trianglelefteq S \mid \deg(r) = d, r$ enthält den Term f, und alle andere Monome von r sind von der Form $m(X_1, \ldots, X_n) \cdot G_i$, m ein Monom$\}$;
(*Die Berechnung von M führt auf ein lineares Gleichungssystem über K. Ist $M \neq \emptyset$, so enthält $(r_1, \ldots, r_s)$ schon eine Relation, welche die Darstellung von $f(h_1, \ldots, h_r)$ mit Hilfe der Cohen-Macaulay-Basis liefert.*)
IF $M = \emptyset$ THEN {
Stelle $f(h_1, \ldots, h_r)$ als Element $r'(f_1, \ldots, f_n, h_1, \ldots, h_r)$ von $\sum_{i=1}^{m} K[f_1, \ldots, f_n] \cdot g_i$ dar;
(*Dies läuft wie in Algorithmus 2.22 auf die Lösung eines linearen Gleichungssystems hinaus.*)
$s := s + 1$;
$r_s := f - r'(X_1, \ldots, X_n, T_1, \ldots, T_r)$
}
}
}
END.

2.4 Anwendungen

Es gibt nur wenige Beispiele, in denen man aus der Präsentation des Invariantenrings schon „mit bloßem Auge“ eine Minimalbasis für den Invariantenkörper ablesen kann.

2.4.1 Die Z_3

Es sei $\mathrm{char}(K) \neq 2, 3$, und $G \cong Z_3$ operiere durch Permutation der Unbestimmten auf $K[x_1, x_2, x_3]$. Mit der Technik des Abspaltens des Fixraums erhalten wir ein homogenes Parametersystem

$$f_1 = s_1(x_1, x_2, x_3),\ f_2 = s_2(y_1, y_2, y_3),\ f_3 = s_3(y_1, y_2, y_3),$$

wobei s_i die elementarsymmetrischen Polynome sind und $y_i = x_i - f_1/3$. Sekundäre Invarianten sind 1 und $g = \prod_{i<j}(x_i - x_j)$, und es gilt die Diskriminantenrelation

$$g^2 + 4f_2^3 + 27f_3^2 = 0.$$

Mit $\varphi_1 = f_3/f_2$ und $\varphi_2 = g/f_2$ folgt

$$\varphi_2^2 + 4f_2 + 27\varphi_1^2 = 0,$$

also liegen f_2 und damit auch f_3 und g in $K(\varphi_1, \varphi_2)$. Es gilt

$$\prod_{i=1}^{3}(X - y_i) = X^3 + f_2 \cdot X - f_3,$$

wir erhalten also das generische Polynom

$$g(X) = X^3 - \frac{1}{4}\left(27t_1^2 + t_2^2\right) \cdot X + \frac{t_1}{4}\left(27t_1^2 + t_2^2\right).$$

Mit $p = \frac{3}{2}t_1$ und $q = \frac{1}{6}t_2$ ergibt sich das Polynom von SEIDELMANN [44]:

$$g(X) = X^3 - 3\left(p^2 + 3q^2\right) \cdot X + 2p\left(p^2 + 3q^2\right).$$

Dabei kann man nach Zusatz 1.12 noch p oder q gleich 1 setzen und erhält dann immer noch ein generisches Polynom.

In diesem Beispiel ist der Invariantenring *nicht* polynomial; erst sein Quotientenkörper wird rein transzendent über K.

2.4.2 Die D_4

Die Diedergruppe $G = D_4$ der Ordnung 8 operiere durch Vertauschungen der x_i auf $K[x_1, \ldots, x_4]$, $\mathrm{char}(K) \neq 2$. Die Rechnung mit Hilfe des *Invar*-Programmpakets liefert primäre Invarianten $f_1, \ldots, f_4$ der Grade 1,2,2,4 und eine weitere erzeugende Invariante g vom Grad 3. Die einzige Relation ist

$$g^2 + 4f_3f_4 - f_3(f_2 + f_3)^2 = 0,$$

aus der man sofort

$$K(x_1, \ldots, x_4)^G = K(f_1, f_2, f_3, g)$$

sieht. Als generisches Polynom erhält man

$$g(X) = X^4 + 2t_1 \cdot X^2 - 4t_2t_3 \cdot X + \left((t_1 + t_2)^2 - 2t_2t_3^2\right),$$

woraus sich mit $e = \frac{1}{2t_3}$, $f = 2t_2t_3^2$ und $g = -t_1 - \frac{t_2}{2}$ die SEIDELMANNsche Form ergibt.

3 Invariantenkörper

Nun kommen wir zum eigentlichen Objekt unseres Interesses, dem Invariantenkörper. In diesem Abschnitt wird eine Strategie entwickelt, mit deren Hilfe man in vielen Fällen Minimalbasen finden kann. Es gibt jedoch keinerlei Garantie, daß diese Strategie tatsächlich eine Minimalbasis liefert, falls eine solche existiert. Daher muß sich die Strategie in den Anwendungen bewähren, um die es in den Abschnitten 3.2 und 3.3 geht. Zum Schluß beschäftigen wir uns mit einem Reduktionssatz, der Anwendungen im Bereich des klassischen Noetherschen Problems erlaubt.

3.1 Konstruktion von Minimalbasen

Der erste Schritt der hier zu entwickelnden Strategie beruht auf der Reduktion des Rationalitätsproblems auf rationale Invarianten vom Grad 0. Dieser Schritt allein liefert schon einige interessante Anwendungen (siehe Beispiel 3.5). In Abschnitt 3.1.3 wird dann die Strategie zur Konstruktion einer Minimalbasis des Körpers dieser Invarianten formuliert. Außerdem benötigen wir ein Verfahren zur Verifikation von Kandidaten für eine Minimalbasis. Dies bringen wir aus beweistechnischen Gründen schon vor der Strategie.

3.1.1 Reduktion auf Invarianten vom Grad 0

Es sei K ein Körper, $A \neq K$ eine nullteilerfreie graduierte K-Algebra und $L = \mathrm{Quot}(A)$ ihr Quotientenkörper. Ein Element $f \in L$ heißt **homogen vom Grad** d, falls es sich als $f = p/q$ mit $p, q \in A$ homogen mit $\deg(p) - \deg(q) = d$ schreiben läßt. Wir schreiben

$$L_0 = \{f \in L \mid f \text{ ist homogen vom Grad } 0\} \cup \{0\},$$

also $K \leq L_0 \leq L$.

Proposition 3.1. *In der obigen Situation gelten:*

(a) Ist $g \in L$ homogen von minimalem positiven Grad e, so folgt $L = L_0(g)$, und g ist transzendent über L_0. Insbesondere ist L eine rein transzendente Erweiterung von L_0 vom Transzendenzgrad 1.

(b) Gilt $L = K(f_1, \ldots, f_r)$ mit homogenen $f_i \in L$, so gibt es $g_1, \ldots, g_{r-1} \in L_0$, so daß

$$L_0 = K(g_1, \ldots, g_{r-1}).$$

Außerdem gilt $\mathrm{ggT}\,(\deg(f_1), \ldots, \deg(f_r)) = e$.

Beweis.

(a) Die Transzendenz von g über L_0 folgt aus $\deg(g) > 0$.

Es genügt nun zu zeigen, daß jedes homogene Element f von A in $L_0(g)$ liegt. Dazu sei

$$\deg(f) = k \cdot e + r$$

mit $k, r \in \mathbb{Z}$ und $0 \leq r < e$. Dann hat $f \cdot g^{-k}$ den Grad r, wegen der Minimalität von e also $r = 0$, d.h. $f \cdot g^{-k} \in L_0$.

(b) Es sei $d_i = \deg(f_i)$ und $d = \mathrm{ggT}(d_1, \ldots, d_r)$. Es gibt ganze Zahlen $k_1, \ldots, k_r$ mit $\sum_{i=1}^r k_i \cdot d_i = d$. Wir haben $\mathrm{ggT}(k_1, \ldots, k_r) = 1$, denn jeder gemeinsame Teiler x der k_i erfüllt $d \cdot x \mid k_i \cdot d_i$, also $d \cdot x \mid d$.

Das folgende Lemma liefert eine ganzzahlige Matrix $A = (c_{i,j})_{1 \le i,j \le r}$ mit $c_{1,i} = k_i$ und $\det(A) = \pm 1$, so daß also auch $A^{-1} =: (a_{i,j})$ ganzzahlig ist. Wir bilden

$$\varphi_i = \prod_{j=1}^{r} f_j^{c_{i,j}}.$$

Dann folgt $f_i = \prod_{j=1}^r \varphi_j^{a_{i,j}}$, also $K(\varphi_1, \ldots, \varphi_r) = L$. Nun sei

$$g_{i-1} = \varphi_i \cdot \varphi_1^{-\deg(\varphi_i)/d} \in L_0 \ (i = 2, \ldots, r).$$

Es folgt

$$L = K(g_1, \ldots, g_{r-1}, \varphi_1),$$

also $L_0 = K(g_1, \ldots, g_{r-1})$, da φ_1 transzendent über L_0 ist.

Nun folgt auch $L = L_0(\varphi_1)$, insbesondere ist das g aus Teil (a) eine rationale Funktion in φ_1. Es folgt $d \mid e$, wegen der Minimalität von e also $d = e$. □

Es fehlt noch das im Beweis benutzte

Lemma 3.2. *Zu vorgegebenen $c_{1,1}, \ldots, c_{1,r} \in \mathbb{Z}$ existiert eine ganzzahlige Matrix $A = (c_{i,j})_{1 \le i,j \le r}$ mit $\det(A) = \pm \mathrm{ggT}(c_{1,1}, \ldots, c_{1,r})$.*

Beweis. Für $r = 1$ ist nichts zu zeigen, und wir können außerdem annehmen, daß alle $c_{1,i} \neq 0$ seien.

Das Lemma sei schon für $r - 1$ bewiesen, es existiert also $A' = (c_{i,j})_{1 \le i,j < r}$ mit $c_{i,j} \in \mathbb{Z}$ und $\det(A') = \mathrm{ggT}(c_{1,1}, \ldots, c_{1,r-1}) =: e'$. Es gilt $e := \mathrm{ggT}(c_{1,1}, \ldots, c_{1,r}) = x \cdot c_{1,r} + y \cdot e'$ mit $x, y \in \mathbb{Z}$. Setze

$$c_{r,r} = \frac{e}{e'} - \frac{x}{e'} \cdot c_{1,r}, \text{ und } c_{r,j} = -\frac{x}{e'} \cdot c_{1,j} \ (j < r)$$

Dann ist $c_{r,r} = y \in \mathbb{Z}$, und die anderen $c_{r,j}$ sind wegen $e' \mid c_{1,j}$ ganz. Die $c_{i,r}$ $(1 < i < r)$ kann man beliebig wählen.

Um die Determinante von $A = (c_{i,j})_{1 \le i,j \le r}$ zu berechnen, addieren wir das $\frac{x}{e'}$-fache der ersten Zeile zur r-ten Zeile und erhalten

$$\det(A) = \begin{vmatrix} c_{1,1} & \cdots & c_{1,r-1} & c_{1,r} \\ c_{2,1} & \cdots & c_{2,r-1} & c_{2,r} \\ \vdots & & \vdots & \vdots \\ c_{r-1,1} & \cdots & c_{r-1,r-1} & c_{r-1,r-1} \\ 0 & \cdots & 0 & e/e' \end{vmatrix} = \pm \frac{e}{e'} \cdot \det(A') = \pm e.$$

□

Anmerkung. Proposition 3.1(a) verallgemeinert die „zweite Reduktion“ bei NOETHER [41]. ◁

Wir betrachten nun die speziellere Situation, daß A ein Invariantenring ist.

Proposition 3.3. *Sei V ein endlich dimensionaler K-Vektorraum, $G \leq \mathrm{GL}(V)$ eine endliche lineare Gruppe und $S = \{\lambda \cdot \mathrm{id}_V \in G \mid \lambda \in K\}$ die Untergruppe der skalaren Matrizen in G. Dann gelten:*

(a) Der Kern der Operation von G auf $K(V)_0$ ist genau S.

(b) Es gilt $|S| = e$ mit dem e aus Proposition 3.1(a).

Beweis.

(a) Alle $\sigma \in S$ liegen im Kern der Operation von G auf $K(V)_0$. Umgekehrt operiere $\sigma \in G$ trivial auf $K(V)_0$. Für linear unabhängige Linearformen $\lambda_1, \lambda_2 \in V^* \subset K[V]$ gilt $\frac{\lambda_1}{\lambda_2} \in K(V)^{\langle\sigma\rangle}$, nach Proposition 1.1(b) folgt also $\sigma(\lambda_i) = \chi \cdot \lambda_i$ mit $\chi \in K^\times$ (i=1,2). Damit operiert σ als Skalar auf V^* und damit auf V.

(b) Mit einem $0 \neq x \in V^*$ und g wie in Proposition 3.1(a) haben wir

$$\begin{aligned} |G| &= \left[K(V) : K(V)^G\right] = \left[K(V) : \left(K(V)_0\right)(x^e)\right] \cdot \left[\left(K(V)_0\right)(x^e) : K(V)^G\right] \\ &= e \cdot \left[\left(K(V)_0\right)(g) : \left(K(V)_0^G\right)(g)\right] = e \cdot \left[K(V)_0 : K(V)_0^G\right] = e \cdot \frac{|G|}{|S|}, \end{aligned}$$

wobei die letzte Gleichheit aus Teil (a) folgt. Es ergibt sich $|S| = e$. □

Korollar 3.4. *Es seien G und S wie in Proposition 3.3. Außerdem sei $H \leq G$ eine Untergruppe mit $S \cdot H = G$. Ist dann $K(V)^G$ rein transzendent über K mit einer homogenen Minimalbasis, so auch $K(V)^H$.*

Beweis. Nach Voraussetzung gilt $H/(S \cap H) \cong G/S$, nach Proposition 3.3(a) also $K(V)_0^G = K(V)_0^H$. Nach Proposition 3.1(b) ist aber $K(V)_0^G$ rein transzendent über K. Nun ist aber $K(V)^H$ nach Proposition 3.1(a) wiederum rein transzendent über $K(V)_0^H$. Damit ergibt sich die Behauptung. □

Als einfache Anwendung erhalten wir

Beispiel 3.5. Einige der Spiegelungsgruppen (siehe Abschnitt 2.1) entstehen als direktes Produkt einer Gruppe G' mit einer Gruppe von skalaren Matrizen. Nach Korollar 3.4 ist damit auch $K(V)^{G'}$ rein transzendent über K. Unter den Beispielen finden sich einige einfache Gruppen G'. Wir haben (in der Nomenklatur von SHEPHARD und TODD [45]):

(a) $G_{23} \cong \{\pm 1\} \times A_5$ mit $\dim(V) = 3$ und Definitionskörper $\mathbb{Q}(\sqrt{5})$.

Hier genügt es nach Proposition 2.3, $\mathrm{char}(K) \neq 2, 3, 5$ und $5 \in (K^\times)^2$ vorauszusetzen. Nach Korollar 3.4 ist dann $K(V)^{A_5}$ rein transzendent über K.

Wir möchten für dieses Beispiel explizit eine Minimalbasis ausrechnen. Aus den Graden von G_{23} sieht man, daß es homogene Invarianten s_2, s_6 und s_{10} vom Grad 2,6 und

10 gibt, die $K[V]^{G_{23}}$ erzeugen. Wir brauchen noch eine Invariante ungeraden Grades und nehmen hierfür beispielsweise die Jacobi-Determinante s_{15} von (s_2, s_6, s_{10}). Dann liefert

$$\varphi_0 = \frac{s_{15}}{s_2^8},\ \varphi_1 = \frac{s_6}{s_2^3},\ \varphi_2 = \frac{s_{10}}{s_2^5}$$

eine Minimalbasis für $K(V)^{A_5}$. Um aus dieser ein generisches Polynom zu gewinnen, suchen wir nach der in der Anmerkung nach Satz 1.11 angegebenen Methode eine möglichst kleine G-stabile Menge $\mathcal{M} \leq V^*$. Es stellt sich heraus, daß die größte Untergruppe H, die die dortige Bedingung (1.4) erfüllt, eine Z_5 ist. So erhält man nach Zusatz 1.12 ein generisches Polynom vom Grad 12 in zwei Parametern. Die Rechnungen wurden mit MAPLE unter Einsatz des *Invar*-Pakets (siehe KEMPER [27]) für $K = \mathbb{Q}(\sqrt{5})$ durchgeführt. Das generische Polynom lautet

$$\begin{aligned} g(X) \;=\; & X^{12} + 2\sqrt{5}\,u \cdot X^{10} + 7u^2 \cdot X^8 + 2\sqrt{5}\,(1+t_1)\,u^3 \cdot X^6 + \\ & + (6t_1+1)\,u^4 \cdot X^4 + \left(\sqrt{5}\,t_1 + (682+305\sqrt{5})t_2\right) u^5 \cdot X^2 + t_1^2 u^6 \end{aligned}$$

mit

$$\begin{aligned} u \;=\; & (682+305\sqrt{5})\left(25\sqrt{5}(682+305\sqrt{5})t_2^3 + (325\,t_1 - 4)\,t_2^2\right) - \\ & -(682-305\sqrt{5})\left(1728\,t_1^5 - 688\,t_1^4 + 91\,t_1^3 - 4\,t_1^2\right) - \\ & -\sqrt{5}\,t_1 t_2\left(720\,t_1^2 - 159\,t_1 + 8\right). \end{aligned}$$

(b) $G_{24} \cong \{\pm 1\} \times \mathrm{PSL}_2(7)$ mit $\dim(V) = 3$ und Definitionskörper $\mathbb{Q}(\sqrt{-7})$.

Es sei $\mathrm{char}(K) \neq 2, 3, 7$ und $-7 \in (K^\times)^2$. Auch hier liefert Korollar 3.4, daß $K(V)^{\mathrm{PSL}_2(7)}$ rein transzendent über K ist. Will man mit demselben Verfahren wie oben ein zugehöriges generisches Polynom von minimalem Grad konstruieren, so erhält man als größte Untergruppe H mit der Eigenschaft (1.4) diesmal eine Z_4. Das generische Polynom ist also vom Grad 42 und ließe sich wohl kaum auf einer Druckseite wiedergeben!

Zum Noetherschen Problem für die $\mathrm{PSL}_2(7)$ siehe auch KEMPER [26] wo eine Minimalbasis von $K(V)^{\mathrm{PSL}_2(7)}$ für $K = \mathbb{Q}(\sqrt{-7})$ explizit berechnet wird.

(c) $G_{33} \cong \{\pm 1\} \times \mathrm{PSp}_4(3)$ mit $\dim(V) = 5$ und Definitionskörper $\mathbb{Q}(\sqrt{-3})$.

Hier muß man $\mathrm{char}(K) \neq 2, 3, 5$ und $-3 \in (K^\times)^2$ voraussetzen.

Ist man etwas bescheidener und betrachtet auch solche Untergruppen G' einer Spiegelungsgruppe, die noch skalare Matrizen enthalten, so erhält man für eine Reihe weiterer „spiegelungsnaher" Gruppen eine positive Antwort auf das Noethersche Problem. Beispielsweise ist $G_{20} \cong \langle \zeta_3 \rangle \times \mathrm{SL}_2(5)$ und $G_{27} \cong \{\pm 1\} \times \widetilde{A_6}$, wobei $\widetilde{A_6}$ eine nicht zerfallende Erweiterung der A_6 mit dem Kern Z_3 ist. Die Angaben über die Isomorphietypen der Spiegelungsgruppen sind hierbei BENARD [2] entnommen. ◁

3.1.2 Verifikation von Minimalbasen

Unsere Strategie (Abschnitt 3.1.3) wird unter Umständen nur *Kandidaten* für eine Minimalbasis liefern. Zur Verifikation solcher Kandidaten dient ein Algorithmus, der im wesentlichen auf M. SWEEDLER zurückgeht. Dieses Verfahren besprechen wir schon hier, da das

Korollar 3.8 in den Beweis zu Lemma 3.10 im nächsten Abschnitt eingeht. Wir verwenden die Abkürzungen $\underline{X}$ für $X_1, \ldots, X_m$, $\underline{T}$ für $T_1, \ldots, T_n$ u.s.w.

Ist V ein endlich dimensionaler K-Vektorraum und $G \leq \mathrm{GL}(V)$ endlich, so liefert der Algorithmus aus Abschnitt 2.3 eine Präsentation des Invariantenrings:

$$K[V]^G = K[\vartheta_1, \ldots, \vartheta_m] \cong K[X_1, \ldots, X_m] \Big/ (r_1, \ldots, r_s)$$

mit erzeugenden Invarianten ϑ_i. Seien nun $\varphi_1, \ldots, \varphi_n \in K(V)^G$ gegeben, also $\varphi_i = f_i(\underline{\vartheta})$ mit $f_i \in K(\underline{X})$. Mit $N = K(V)^G$ und $L = K(\underline{\vartheta})$ soll nun der Grad $[N : L]$ bestimmt werden. Die Grundidee ist, die Gleichungen

$$r_i = 0 \ (i = 1, \ldots, s) \text{ und } f_i = T_i \ (i = 1, \ldots, n)$$

mit zusätzlichen Unbestimmten T_i nach den X_i aufzulösen.

Der Algorithmus funktioniert in folgender, allgemeinerer Situation.

Der Algorithmus.

Es seien $K \leq L \leq N$ Körper, so daß N über K endlich erzeugt ist, $N = K(\vartheta_1, \ldots, \vartheta_m)$. Dann ist auch L/K endlich erzeugt (siehe z.B. KEMPER [28]), etwa $L = K(\varphi_1, \ldots, \varphi_n)$. Wir haben

$$\varphi_i = \frac{g_i(\underline{\vartheta})}{h_i(\underline{\vartheta})} \text{ mit } g_i, h_i \in K[X_1, \ldots, X_m],$$

wobei die X_i Unbestimmte seien. Nach dem Hilbertschen Basissatz ist der Kern von

$$K[\underline{X}] \to N, \ X_i \mapsto \vartheta_i$$

endlich erzeugt. Eine Idealbasis sei durch $r_1, \ldots, r_s \in K[\underline{X}]$ gegeben.

Man führe nun folgenden Algorithmus aus:

Algorithmus 3.6 (Berechnen von Körpergraden).
EINGABE: Polynome g_i, h_i und r_i wie oben.

AUSGABE: Der Transzendenzgrad von N/L und der Grad $[N : L]$, falls endlich.

ABLAUF:

1) Wähle Polynome $p_1, \ldots, p_k \in K[\underline{X}]$, so daß für das Produkt $d = p_1 \cdots p_k$ ein $e \in \mathbb{N}$ existiert mit $h_i \mid d^e \ \forall i$. (Man kann für die p_i beispielsweise die Primteiler von $h_1 \cdots h_n$ nehmen, oder auch $k = 1$ und $p_1 = h_1 \cdots h_n$.)

2) Bilde

$$I = (p_1 U_1 - 1, \ldots, p_k U_k - 1, r_1, \ldots, r_s, g_1 - T_1 h_1, \ldots, g_n - T_n h_n) \trianglelefteq K[\underline{T}, \underline{X}, \underline{U}]$$

mit weiteren Unbestimmten $U_1, \ldots, U_k$ und $T_1, \ldots, T_n$.

3) Wähle eine Termordnung $\prec$ auf $K[\underline{T}, \underline{X}, \underline{U}]$, so daß

$$\begin{aligned} U_i &\succ \text{(jedes Monom in } \underline{T} \text{ und } \underline{X}) \text{ und} \\ X_i &\succ \text{(jedes Monom in } \underline{T} \text{ und } X_1, \ldots, X_{i-1}). \end{aligned}$$

4) Berechne eine minimale Gröbnerbasis G von I bezüglich $\prec$.

5) Auswertung: Setze

$$\begin{aligned} G_T &= G \cap K[\underline{T}], \\ G_i &= G \cap K[\underline{T}, X_1, \ldots, X_i] \setminus K[\underline{T}, X_1, \ldots, X_{i-1}] \ (i = 1, \ldots, m). \end{aligned}$$

Die Anzahl der leeren G_i sei t, und für $G_i \neq \emptyset$ sei f_i ein minimales Element von G_i (bezüglich $\prec$), $d_i = \deg_{X_i}(f_i)$ sein X_i-Grad.
Die Ausgabewerte siehe Satz 3.7.

Satz 3.7. *Mit den Bezeichnungen von Algorithmus 3.6 gelten:*

(a) G_T erzeugt den Kern von $K[\underline{T}] \to L,\ T_i \mapsto \varphi_i$.

(b) Der Transzendenzgrad von N/L ist gleich t.

(c) Es seien alle $G_i \neq \emptyset$. Dann enthält das Leitmonom von f_i keines der X_j, $j < i$, und ersetzt man $T_j = \varphi_j$ $(j = 1, \ldots, n)$ und $X_j = \vartheta_j$ $(j = 1, \ldots, i-1)$ in f_i, so erhält man ein (im allgemeinen nicht normiertes) Minimalpolynom von ϑ_i über $L(\vartheta_1, \ldots, \vartheta_{i-1})$. Insbesondere folgt

$$[N : L] = \prod_{i=1}^{m} d_i.$$

Beweis. Die Beweise der Aussagen (a) und (b) und der Gradformel in (c) finden sich bei SWEEDLER [51]. Die entscheidende Beobachtung ist, daß I der Kern von

$$K[\underline{T}, \underline{X}, \underline{U}] \to N,\ T_i \mapsto \varphi_i,\ X_i \mapsto \vartheta_i,\ U_i \mapsto \frac{1}{p_i(\underline{\vartheta})}$$

ist [loc. cit., Lemma 3.1]. Unter der Voraussetzung von Teil (c) ist N/L algebraisch, also $L(\vartheta_1, \ldots, \vartheta_i) = L[\vartheta_1, \ldots, \vartheta_i]$ für alle i. Wir fixieren ein i. Es folgt, daß das Minimalpolynom $g(X_i)$ von ϑ_i über $L(\vartheta_1, \ldots, \vartheta_{i-1})$ in $L[\vartheta_1, \ldots, \vartheta_{i-1}][X_i]$ liegt. Nach Multiplikation mit einem Element von $K[\underline{\varphi}]$ können wir ohne Beschränkung der Allgemeinheit $g(X_i) \in K[\underline{\varphi}, \vartheta_1, \ldots, \vartheta_{i-1}][X_i]$ annehmen, wobei $g(X_i)$ nicht mehr normiert ist. Wir nehmen ein $f \in K[\underline{T}, X_1, \ldots, X_i]$, das unter $T_j \mapsto \varphi_j$ und $X_j \mapsto \vartheta_j$ $(j < i)$ auf $g(X_i)$ abgebildet wird und schon modulo G_T reduziert ist. Dann liegt f in I, hat also den G-Rest 0. Aus der speziellen Wahl der Termordnung $\prec$ ergibt sich nun, daß das Leitmonom $\mathrm{LM}(f)$ von f durch das Leitmonom eines $h \in G$ teilbar sein muß, und nach Konstruktion enthält $\mathrm{LM}(f)$ keines der X_j $(j < i)$. Also liegt h in G_i und führt umgekehrt wieder zu einem Polynom für ϑ_i über $L(\vartheta_1, \ldots, \vartheta_{i-1})$. Nun folgt $h = f_i$ (mit f_i aus Schritt 5 des Algorithmus), und auch Teil (c) ist vollständig bewiesen. □

Ein Beweis zu Satz 3.7 befindet sich auch in KEMPER [28]. Dieser Artikel ist gleichzeitig eine Programmbeschreibung zu einer Implementierung von Algorithmus 3.6 in der MAPLE-Programmiersprache. Es handelt sich dabei um das Programmpaket „*Fields*“, welches in der *Maple Share Library* verfügbar gemacht wurde. Dabei kann als Grundkörper $K = \mathbb{Q}$ oder ein algebraische Zahlkörper gewählt werden. Der rechnerisch aufwendige Teil des Algorithmus ist das Berechnen der Gröbnerbasis in Schritt 4. Hier erhält man gute

probabilistische Ergebnisse, indem man die T_i zu zufälligen Werten spezialisiert und modulo einer (großen) Primzahl p rechnet. Dadurch verringert sich die Rechenzeit natürlich erheblich. Um diese Option möglich zu machen, wurde ein partielles Interface zu dem speziellen Computeralgebrasystem MACAULAY (siehe [48]) eingebaut.

Eine Folgerung.

Korollar 3.8. *Mit den Bezeichnungen aus Satz 3.7 sei zusätzlich der Transzendenzgrad von N/K gerade gleich n, und wir fassen I als Ideal in $K(\underline{T})[\underline{X}, \underline{U}]$ auf. Dann gelten:*

(a) Es ist $I = (1)$ genau dann, wenn die φ_i algebraisch abhängig sind über K.

(b) Sind die φ_i algebraisch unabhängig über K, so folgt

$$\dim_{K(\underline{T})} \left(K(\underline{T})[\underline{X}, \underline{U}] \Big/ I \right) = [N : L].$$

Beweis.

(a) Die φ_i sind nach Satz 3.7(a) genau dann algebraisch abhängig, wenn $G_T \neq \emptyset$, und dies ist gleichbedeutend mit $I = (1)$, da die T_i nun im Konstantenkörper $K(\underline{T})$ liegen.

(b) Wegen der Voraussetzung an den Transzendenzgrad von N/L sind alle $G_i \neq \emptyset$. Es gilt $1/p_i(\underline{\vartheta}) \in L[\underline{\vartheta}]$, also enthält die Gröbnerbasis G Polynome der Form

$$\left(U_i \text{ minus ein Polynom in den } X_i \text{ über } K(\underline{T}) \right).$$

Diese bilden zusammen mit den f_i $(i = 1, \ldots, m)$ aus Satz 3.7(c) eine Gröbnerbasis von I als Ideal in $K(\underline{T})[\underline{X}, \underline{U}]$. (Dies folgt aus der besonderen Gestalt der f_i.) Wir erhalten

$$\dim_{K(\underline{T})} \left(K(\underline{T})[\underline{X}, \underline{U}] \Big/ I \right) = \prod_{i=1}^{m} d_i = [N : L].$$

□

3.1.3 Die Strategie

Das Lemma 3.10 beruht in erster Linie auf dem Satz von Bézout, den wir in der folgenden Form benötigen.

Satz 3.9 (Satz von Bézout). *Es seien K ein algebraisch abgeschlossener Körper, $f_1, \ldots, f_n \in K[x_0, \ldots, x_n]$ homogene Polynome mit $\deg(f_i) = d_i$, $\mathcal{V}_i = \mathcal{V}(f_i) \in \mathbb{P}^n(K)$ die projektiven Nullstellengebilde der f_i und $\mathcal{M} \subset \mathcal{V}_1 \cap \ldots \cap \mathcal{V}_n$ eine Menge isolierter Schnittpunkte. Weiter sei*

$$i_P = \dim_K \left(\mathcal{O}_P(\mathbb{P}^n(K)) \Big/ (f_1, \ldots, f_n) \right)$$

die Schnittvielfachheit von $\mathcal{V}_1, \ldots, \mathcal{V}_n$ bei P, wobei $\mathcal{O}_P(\mathbb{P}^n(K))$ den Ring der regulären Funktionskeime bei P bezeichnet. Dann gelten:

(a) $\displaystyle\sum_{P \in \mathcal{M}} i_P \leq \prod_{i=1}^{n} d_i.$

(b) Gilt $\mathcal{M} = \mathcal{V}_1 \cap \ldots \cap \mathcal{V}_n$, so gilt in obiger Formel „=“.

Insbesondere ist $|\mathcal{M}| \leq \prod_{i=1}^{n} d_i$.

Beweis. Alle $\mathcal{V}_i$ sind nach FULTON [21, S. 145] Cohen-Macaulay, nach [loc. cit., S. 226] also

$$\sum_{P \in \mathcal{M}} l\left(\mathcal{O}_P(\textstyle\bigcap_{i=1}^{n} \mathcal{V}_i)\right) \cdot \deg(P) \leq \sum_{i=1}^{n} d_i$$

mit den dortigen Bezeichnungen. In [loc. cit., S. 145] finden wir nun wiederum

$$l\left(\mathcal{O}_P(\textstyle\bigcap_{i=1}^{n} \mathcal{V}_i)\right) \cdot \deg(P) = i_P.$$

Dies liefert Teil (a), und (b) folgt direkt nach Formel (3) in [loc. cit., S. 145]. □

Nun können wir das für unsere Strategie entscheidende Lemma beweisen, welches schon (in speziellerer Form) von KERVAIRE und VUST [30] implizit verwendet wird.

Lemma 3.10 („Strategielemma“). *Sei K ein Körper, $x_0, \ldots, x_n$ Unbestimmte, $\varphi_i = \frac{f_i}{g_i} \in K(x_0, \ldots, x_n)$ für $i = 1, \ldots, n$ mit homogenen f_i, $g_i \in K[x_0, \ldots, x_n]$, $\deg(f_i) = \deg(g_i) =: d_i$. Außerdem seien $T_1, \ldots, T_n$ weitere Unbestimmte und $\widetilde{K}$ der algebraische Abschluß von $K(T_1, \ldots, T_n)$. Für $P \in \mathbb{P}^n(\widetilde{K})$ bezeichne i_P die Schnittvielfachheit der durch $f_i - T_i \cdot g_i$ gegebenen projektiven Kurven $\mathcal{V}_i$ in P.*

Weiter sei $h = \prod_{i=1}^{n} g_i$, $\mathcal{M} \subset \mathbb{P}^n(\widetilde{K})$ eine Menge isolierter Schnittpunkte P der $\mathcal{V}_i$ mit $h(P) = 0$ ($\mathcal{M} = \emptyset$ zugelassen) und

$$d = \prod_{i=1}^{n} d_i - \sum_{P \in \mathcal{M}} i_P.$$

Dann gelten:

(a) Ist $\mathcal{V}_1 \cap \ldots \cap \mathcal{V}_n$ endlich und enthält $\mathcal{M}$ alle *Schnittpunkte P mit $h(P) = 0$, so folgt:*

(i) Die φ_i sind genau dann algebraisch unabhängig über K, wenn $d > 0$ gilt.

(ii) Sind die φ_i algebraisch unabhängig über K, so ist

$$\left[K(x_0, \ldots, x_n)_0 : K(\varphi_1, \ldots, \varphi_n)\right] = d.$$

(b) Es sei bekannt, daß die φ_i algebraisch unabhängig über K sind. Dann folgt

$$\left[K(x_0, \ldots, x_n)_0 : K(\varphi_1, \ldots, \varphi_n)\right] \leq d.$$

Beweis. Sind die φ_i algebraisch unabhängig über K, so erfüllen alle x_i/x_j eine Gleichung $f_{i,j}$ über $L := K(\varphi_1, \ldots, \varphi_n)$:

$$f_{i,j}(x_i/x_j,\, \varphi_1, \ldots, \varphi_n) = 0.$$

Mit $\mathcal{M}' := \{P \in \mathcal{V}_1 \cap \ldots \cap \mathcal{V}_n \mid h(P) \neq 0\}$ gilt für jedes $P = [\xi_0, \ldots, \xi_n] \in \mathcal{M}'$

$$\varphi_i(\xi_0, \ldots, \xi_n) = T_i,$$

also $f_{i,j}(\xi_i/\xi_j, T_1, \ldots, T_n) = 0$. Damit ist $\mathcal{M}'$ eine endliche Menge, falls die φ_i algebraisch unabhängig sind. Im Falle (a) gilt dies sowieso nach Voraussetzung. Satz 3.9 liefert nun

$$\sum_{P \in \mathcal{M}'} i_P \leq d,$$

wobei im Falle (a) Gleichheit gilt.

Da $\mathcal{M} \cup \mathcal{M}'$ endlich ist, können wir durch eine lineare Transformation der x_i erreichen, daß alle $P \in \mathcal{M} \cup \mathcal{M}'$ von der Form $P = [1, \xi_1, \ldots, \xi_n]$ sind. Mit $y_i = x_i/x_0$ gilt dann

$$i_P = \dim_{\widetilde{K}} \left(\mathcal{O}_{(\xi_1,\ldots,\xi_n)}(\mathbb{A}^n(\widetilde{K})) \Big/ \left(\psi_1, \ldots, \psi_n\right)\right)$$

mit $\psi_i = f_i(1, y_1, \ldots, y_n) - T_i \cdot g_i(1, y_1, \ldots, y_n)$. Dabei bezeichnet $\mathbb{A}^n(\widetilde{K})$ den n-dimensionalen affinen Raum.

Wir führen eine zusätzliche Unbestimmte u ein und setzen

$$I = \left(\psi_1, \ldots, \psi_n,\, u \cdot h(1, y_1, \ldots, y_n) - 1\right) \trianglelefteq K(T_1, \ldots, T_n)\left[y_1, \ldots, y_n, u\right].$$

Zu $P = [1, \xi_1, \ldots, \xi_n] \in \mathcal{M}'$ existiert genau ein $\xi \in \widetilde{K}$ mit $\xi \cdot h(1, \xi_1, \ldots, \xi_n) - 1 = 0$, und es gilt

$$i_P = \dim_{\widetilde{K}} \left(\mathcal{O}_{(\xi_1,\ldots,\xi_n,\xi)}(\mathbb{A}^{n+1}(\widetilde{K})) \Big/ I \right).$$

Nach FULTON [20, Ch. II.9, Proposition 6] ist aber

$$\sum_{(\xi_1,\ldots,\xi_n,\xi) \in \mathcal{V}(I)} \dim_{\widetilde{K}} \left(\mathcal{O}_{(\xi_1,\ldots\xi_n,\xi)}(\mathbb{A}^{n+1}(\widetilde{K})) \Big/ I \right) = \dim_{\widetilde{K}} \left(\widetilde{K}[y_1, \ldots, y_n, u] \Big/ I \right).$$

Wir setzen alles zusammen und erhalten

$$\begin{aligned} d &\geq \dim_{\widetilde{K}} \left(\widetilde{K}[y_1, \ldots, y_n, u] \Big/ I \right) = \\ &= \dim_{K(T_1,\ldots,T_n)} \left(K(T_1, \ldots, T_n)\,[y_1, \ldots, y_n, u] / I \right) \end{aligned}$$

mit „=“ im Falle (a).

Nun folgen beide Behauptungen mit Korollar 3.8. □

Korollar 3.11. *Es sei K ein Körper, $x_1, \ldots, x_n$ Unbestimmte und $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$ algebraisch unabhängige, homogene Polynome. Dann gilt*

$$\left[K(x_1, \ldots, x_n) : K(f_1, \ldots, f_n)\right] \leq \prod_{i=1}^{n} \deg(f_i).$$

Beweis. Sei x_0 eine weitere Unbestimmte und $d_i = \deg(f_i)$. Dann sind

$$\varphi_i = \frac{f_i}{x_0^{d_i}}$$

algebraisch unabhängig, nach Lemma 3.10(b) folgt also

$$\left[K(x_0, \ldots, x_n)_0 : K(\varphi_1, \ldots, \varphi_n)\right] \leq \prod_{i=1}^{n} d_i.$$

Aber $x_i \mapsto x_i/x_0$ liefert einen Isomorphismus $K(x_1, \ldots, x_n) \to K(x_0, \ldots, x_n)_0$ mit $f_i \mapsto \varphi_i$. □

Formulierung der Strategie.

Unsere Strategie zum Auffinden einer Minimalbasis ergibt sich nun direkt aus Lemma 3.10. Es sei also V ein n-dimensionaler K-Vektorraum, $G \leq \mathrm{GL}(V)$ endlich und S die Untergruppe der skalaren Matrizen in G (siehe Proposition 3.3). Dann schlagen wir folgende Vorgehensweise vor:

(1) Als optionale Vorbereitung berechne im Falle $\mathrm{char}(K) \nmid |G|$ mit dem Algorithmus aus Abschnitt 2.3 eine Präsentation des Invariantenrings $K[V]^G$.

Dieser Schritt wird nicht immer notwendig sein.

(2) Suche homogene $g_1, \ldots, g_{n-1}$ und $h_1, \ldots, h_{n-1} \in K[V]$ von möglichst kleinen Graden $d_i := \deg(g_i) = \deg(h_i)$, so daß jeweils g_i und h_i Invarianten bzw. Pseudo-Invarianten zum selben Gewicht sind, und vermeide dabei, daß die $\varphi_i := g_i/h_i$ algebraisch abhängig über K werden. Im Falle $\mathrm{char}(K) \nmid |G|$ kann man sich mit Hilfe der Molien-Reihe $P_{G,\chi}(\lambda)$ (die sich nach Satz 2.12 berechnen läßt) einen Überblick über die Invarianten bzw. Pseudo-Invarianten verschaffen. Gibt es beispielsweise zwei linear unabhängige Pseudo-Invarianten g_χ und h_χ zum Gewicht χ und von einem gewissen Grad, so kann man diese nur für *ein* φ_i benutzen, da $\frac{g_\chi}{h_\chi}$ und $\frac{\alpha g_\chi + \beta h_\chi}{\gamma g_\chi + \delta h_\chi}$ $(\alpha, \beta, \gamma, \delta \in K$ schon algebraisch abhängig sind.

(3) Falls nicht schon

$$\prod_{i=1}^{n-1} d_i < 2 \cdot \frac{|G|}{|S|},$$

so versuche, die g_i und h_i so zu wählen, daß das d aus Lemma 3.10 kleiner als $2 \cdot |G|/|S|$ wird. Es ist also das Ziel, für möglichst viele gemeinsame Nullstellen der g_i und h_i zu sorgen.

(4) Oft wird man die Voraussetzungen in Lemma 3.10 nicht nachweisen oder die Schnittvielfachheiten nicht genau berechnen können. Dann bietet sich Algorithmus 3.6 zur Verifikation einer Minimalbasis an. Wir haben zwei Varianten:

   (a) Falls eine Präsentation des Invariantenrings berechnet wurde, so stelle die φ_i als rationale Funktionen in den erzeugenden Invarianten dar und verfahre nach der zu Beginn von Abschnitt 3.1.2 angegebenen Methode.

   (b) Setze $N = K(V)_0$ ($n-1$ Erzeuger ohne Relationen) und prüfe mit Algorithmus 3.6, ob $[N : K(\varphi_1, \ldots, \varphi_{n-1})] = \frac{|G|}{|S|}$.

In einigen Fällen kann es natürlich auch möglich sein, algebraisch unabhängige Invarianten $f_1, \ldots, f_n \in K[V]^G$ mit $\prod_{i=1}^n \deg(f_i) < 2 \cdot |G|$ zu finden, die dann nach Korollar 3.11 eine Minimalbasis liefern.

Insbesondere im Schritt (3) können erhebliche Schwierigkeiten auftreten, die in der Regel mit wachsendem n steigen werden. Es sei an dieser Stelle noch einmal betont, daß die oben beschriebene Strategie noch weit davon entfernt ist, automatisierbar zu sein. Noch weniger kann garantiert werden, daß tatsächlich eine Minimalbasis gefunden wird, falls das Noethersche Problem eine positive Antwort hat. Auf der anderen Seite haben die mit obiger Strategie gewonnenen Minimalbasen gegenüber denjenigen aus anderen Quellen

(z.B. der Theorie des Noetherschen Problems abelscher Gruppen, siehe LENSTRA [33]) den Vorteil, daß sie aus Invarianten kleiner Grade bestehen und somit besser handhabbar sind und zu wesentlich einfacheren generischen Polynomen führen. Der Wert der Strategie muß sich jedoch an seiner Anwendbarkeit messen, die im folgenden Abschnitt anhand einiger Beispiele belegt werden soll. Weitere Anwendungen aus dem Bereich der modularen Darstellungen werden dann in Abschnitt 3.3 folgen.

3.2 Anwendungen in nicht singulärer Charakteristik

Bevor wir zu einigen neuen Beispielen kommen, sei erwähnt, daß sämtliche bisher in dieser Arbeit vorgeführte Lösungen des Noetherschen Problems auch mit unserer Strategie zu gewinnen gewesen wären.

3.2.1 Die Z_4

Für die Z_4 haben wir schon in Abschnitt 1.4.2 unter der Voraussetzung $\zeta_4 \in K$ eine positive Antwort auf das Noethersche Problem gefunden. Nun setzen wir nur $\mathrm{char}(K) \neq 2$ voraus und betrachten

$$G = \left\langle\ \sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\ \right\rangle \cong Z_4.$$

Die Molien-Reihe ergibt sich nach Satz 2.12 zu

$$P_G(\lambda) = \frac{1+\lambda^4}{(1-\lambda^2)(1-\lambda^4)} = 1 + \lambda^2 + 3\lambda^4 + 3\lambda^6 + \cdots,$$

und mit dem linearen Charakter $\chi\colon \sigma \mapsto -1$

$$P_{G,\chi}(\lambda) = \frac{2\lambda^2}{(1-\lambda^2)(1-\lambda^4)} = 2\lambda^2 + 2\lambda^4 + 4\lambda^6 + \cdots,$$

man kann also für φ_1 den Quotienten zweier linear unabhängiger Pseudo-Invarianten vom Grad 2 zum Gewicht χ nehmen. Dann ist $\varphi_1 \notin K$, also algebraisch unabhängig, und nach Lemma 3.10(b) und Proposition 3.3(a) folgt

$$[K(V)_0 : K(\varphi_1)] \leq 2 = \frac{|G|}{|\{\pm\mathbf{1}\}|} = \left[K(V)_0 : K(V)_0^G\right],$$

womit nach Proposition 3.1(a) eine positive Antwort auf das Noethersche Problem gefunden wäre.

Explizit erhält man

$$\varphi_0 = x_1^2 + x_2^2 \text{ und } \varphi_1 = \frac{x_1^2 - x_2^2}{x_1 x_2}$$

als Minimalbasis, und mit $\mathcal{M} = \{\pm x_1, \pm x_2\}$ (in der Notation von Satz 1.11) wird

$$g(X) = X^4 - t_1 \cdot X^2 + \frac{t_1^2}{t_2^2 + 4}$$

ein generisches Polynom für Z_4.

Etwas komplizierter wird es, wenn man die vierdimensionale Permutationsdarstellung der Z_4 zugrunde legt. Dann nimmt man zunächst $x_1 + + \cdots + x_4$ als primäre Invariante und spaltet den Fixraum ab (siehe Abschnitt 2.3.1). Nun kann man für φ_1 den Quotienten zweier linear unabhängiger Invarianten vom Grad 2 und für φ_2 den Quotienten zweier Pseudo-Invarianten zum Gewicht χ, auch vom Grad 2, nehmen. Diesmal ist die Untergruppe S der skalaren Matrizen trivial, und man verifiziert mit Algorithmus 3.6, daß man auf diese Weise in der Tat eine Minimalbasis bekommt. Das entsprechende generische Polynom füllt allerdings eine komplette Druckseite!

3.2.2 Die D_5

Die D_5 ist unter der Voraussetzung $\sqrt{5} \in K$ schon durch Beispiel 2.5 abgedeckt. Hier soll nun eine Minimalbasis für die Permutationsdarstellung vom Grad 5 mit $K = \mathbb{Q}$ gefunden werden.

Nach Abspalten des Fixraums brauchen wir noch drei algebraisch unabhängige Erzeuger von $K(V)_0^G$. Es stellt sich heraus, daß es jeweils zwei linear unabhängige Invarianten von den Graden 2 und 3 und zwei linear unabhängige Pseudo-Invarianten vom Grad 3 zum nicht trivialen linearen Charakter $\chi\colon G \to \{\pm 1\}$ gibt. Die Abschätzung

$$2 \cdot 3 \cdot 3 < 2 \cdot |G|$$

gibt Anlaß zu der Erwartung, daß die drei Quotienten φ_1, φ_2 und φ_3 eine Minimalbasis von $K(V)_0^G$ liefern. Die φ_i sind jedoch so unübersichtlich, daß man kaum die Voraussetzungen zu Lemma 3.10(a) oder (b) nachweisen kann. Eine Verifikation mit Verfahren (b) aus dem Verifikationsschritt (4) unserer Strategie scheitert an der Schwierigkeit der Gröbnerbasisberechnung. Aber man kann mit dem Algorithmus aus Abschnitt 2.3 eine Präsentation des Invariantenrings berechnen und erhält dann nach dem Verfahren (a) den Nachweis, daß die φ_i ganz $K(V)_0^G$ erzeugen.

3.2.3 Die A_4

Bei den bisherigen Beispielen war es nicht nötig, gemäß Schritt (3) in der Strategie bei den g_i und h_i für gemeinsame Nullstellen zu sorgen. In diesem Beispiel werden wir es nicht ganz so leicht haben.

Wir betrachten $G = A_4$ mit der dreidimensionalen Darstellung, die sich aus der natürlichen Permutationsdarstellung durch Abspalten des Fixraums ergibt, und es sei $\mathrm{char}(K) \neq 2,3$. Der Invariantenring ist

$$K[V]^G = K[s_2, s_3, s_4, d]$$

mit der Relation

$$d^2 = \mathrm{discr}_X(X^4 + s_2X^2 - s_3X + s_4).$$

Dabei kommen die s_i von den elementarsymmetrischen Polynomen und d vom Produkt der $x_i - x_j$ $(i < j)$, insbesondere also $\deg(s_i) = i$ und $\deg(d) = 6$.

Die Lösung von KERVAIRE und VUST.

Wir folgen zunächst KERVAIRE und VUST [30] und versuchen, eine Minimalbasis von $K(V)_0^G$ von der Form

$$\varphi_1 = \frac{s_4}{s_2^2} \text{ und } \varphi_2 = \frac{d + \alpha s_3^2}{s_2^3}$$

mit einem noch zu spezifizierenden $\alpha \in K$ zu finden. Die Gradabschätzung liefert hier $4 \cdot 6 = 2 \cdot |G|$, was nicht ganz ausreicht. Wir brauchen also gemeinsame Nullstellen von s_2, s_4 und $d + \alpha s_3^2$. Man sieht leicht, daß die gemeinsamen projektiven Nullstellen von s_2 und s_4 genau durch die G-Bahn von $[1, \zeta_3, 0]$ mit einer primitiven dritten Einheitswurzel ζ_3 gegeben werden. Wir haben

$$\begin{aligned} d(1, \zeta_3, 0) &= 3\sqrt{-3}, \\ s_3(1, \zeta_3, 0) &= 1, \end{aligned}$$

also führt $\alpha = -3\sqrt{-3}$ zu einer gemeinsamen Nullstelle, wobei man zusätzlich $\sqrt{-3} \in K$ voraussetzen muß.

Nun kann man $K(V)_0^G = K(\varphi_1, \varphi_2)$ entweder direkt mit Algorithmus 3.6 verifizieren oder nachrechnen, daß die Jacobi-Determinante von s_2, s_4 und $d - 3\sqrt{-3}s_3^2$ ungleich 0 ist. Dann folgt nach BENSON [3, Prop. 5.4.2] die algebraische Unabhängigkeit dieser drei Polynome, also auch der φ_i, und wir können Lemma 3.10(b) anwenden.

Dasselbe Ziel läßt sich einfacher erreichen, indem man Pseudo-Invarianten zum (bis auf Konjugation eindeutig bestimmten) nicht trivialen linearen Charakter χ der A_4 betrachtet. Vom Grad 4 gibt es davon nämlich gerade zwei linear unabhängige, was sofort zur günstigeren Gradabschätzung $4 \cdot 4 < 2 \cdot |G|$ führt. Nun wird auch klarer, weshalb die Bedingung $\sqrt{-3} \in K$ ins Spiel kam: Sie sorgt dafür, daß χ Werte in K hat.

Minimalbasis über $K = \mathbb{Q}$.

Nun wissen wir aber aus NOETHER [41], daß es auch über $K = \mathbb{Q}$ eine Minimalbasis gibt. Wir möchten eine solche mit unserer Strategie finden und kommen (nach einigem Probieren) zu dem Ansatz

$$\varphi_1 = \frac{s_2 s_4 + \alpha s_2^3}{d}, \ \varphi_2 = \frac{s_3^2 + \beta s_2^3}{d}$$

mit $\alpha, \beta \in K$. Statt nun zu versuchen, α und β so zu legen, daß viele gemeinsame Nullstellen möglichst hoher Vielfachheit entstehen, gehen wir direkt in das Verifikationsverfahren (Schritt 4(a) der Strategie). Wir haben

$$K(V)_0^G = K\left(\frac{s_2^3}{s_3^2}, \frac{s_4 s_2^4}{s_3^4}, \frac{s_2^6 d}{s_3^6}\right) \cong K(X, Y, Z)$$

mit

$$Z^2 = 16YX^4 - 4X^5 - 128Y^2X^2 + 144YX^3 - 27X^4 + 256Y^3. \tag{3.1}$$

Außerdem haben wir aus dem Ansatz die Gleichungen

$$Z \cdot T_1 = X(Y + \alpha X^2) \text{ und } Z \cdot T_2 = X^2(1 + \beta X) \tag{3.2}$$

mit zusätzlichen Unbestimmten T_1 und T_2 (siehe Abschnitt 3.1.2), die man sofort nach Z und Y auflösen kann. Einsetzen der erhaltenen Werte für Z und Y in (3.1) ergibt eine Gleichung f für X, die nun eindeutig lösbar sein muß. Diese Gleichung ist länglich und soll hier nicht wiedergegeben werden; man sieht ihr jedoch nicht unmittelbar an, wie die Parameter α und β zu legen sind, damit sie nur eine Lösung X hat. Bringt man jedoch die Nebenbedingung $X, Z \neq 0$ ins Spiel, so kann man zunächst X^3 von f abdividieren und erhält nun ein Polynom vom Grad 3 in X. Wegen

$$Z = \frac{X^2(1+\beta X)}{T_2}$$

muß man nun erreichen, daß

$$(1+\beta X)^2 \Big| f/X^3.$$

Dies führt auf ein algebraischen Gleichungssystem in α und β, das durch

$$\alpha = \frac{1}{12} \text{ und } \beta = \frac{8}{27}$$

gelöst wird. Bis hierhin haben wir mehr oder minder „auf Verdacht“ gerechnet. Verifikation unseres Ergebnisses mit Algorithmus 3.6 liefert nun

$$X = \frac{6912\,T_1^3}{729\,T_2^3 - 3888\,T_2^2T_1 + 5184\,T_2T_1^2 - 2048\,T_1^3 + 27\,T_2},$$

woraus mit (3.2) die Darstellungen von Y und Z als rationale Funktionen in T_1 und T_2 folgen.

Es bleibt die Frage, welche Bedeutung die Konstanten $1/12$ und $8/27$ haben.

3.2.4 Verallgemeinerte Quaternionengruppen

Es sei $n > 1$ und

$$G = \langle \sigma, \tau \mid \sigma^n = \tau^2, \tau^4 = \iota, \tau^{-1}\sigma\tau = \sigma^{-1} \rangle \cong Q_{4n}$$

die verallgemeinerte Quaternionengruppe der Ordnung $4n$.

Die zweidimensionale Darstellung.

Es sei K ein Körper mit $\mathrm{char}(K) \nmid 2n$ und $\zeta_{2n}, i \in K$, wobei ζ_{2n} eine primitive $2n$-te Einheitswurzel ist und $i^2 = -1$. Eine durch

$$\sigma \mapsto \begin{pmatrix} \zeta_{2n} & 0 \\ 0 & \zeta_{2n}^{-1} \end{pmatrix}, \ \tau \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

gegebene zweidimensionale Darstellung von G über K finden wir in Benson [3, App. A]. Dort sind auch Invarianten s_1, s_2 und s_3 von den Graden 4, $2n$ und $2n+2$ angegeben, die den Invariantenring erzeugen.

Mit $\varphi_1 = \frac{s_2}{s_1^{n/2}}$ für n gerade bzw. $\varphi_1 = \frac{s_3}{s_1^{(n+1)/2}}$ für n ungerade gilt $K(x_1,x_2)_0^G = K(\varphi_1)$, da

$$\deg(s_2), \deg(s_3) \leq 2n+2 < 2 \cdot \frac{|G|}{|\{\pm \mathbf{1}\}|}.$$

Damit ist das Noethersche Problem für diese Darstellung positiv beantwortet.

Indem wir φ_1 durch eine rationale Invariante vom Grad 2 zu einer Minimalbasis ergänzen und die in [3] angegebene Relation zwischen den s_i benutzen, erhalten wir

$$g(X) = \begin{cases} X^{4n} - t_1^n t_2 (t_2^2-4)^{\frac{n}{2}} \cdot X^{2n} + t_1^{2n}(t_2^2-4)^n, \ n \text{ gerade} \\ \\ X^{4n} - t_1^n (t_2^2-4)^{\frac{n+1}{2}} \cdot X^{2n} - t_1^{2n}(t_2^2-4)^n, \ n \text{ ungerade} \end{cases}$$

als generisches Polynom für G über K.

Hierfür mußten wir ζ_{2n} und $i \in K$ voraussetzen. Da der Charakter ψ zu der zweidimensionalen Darstellung die Schur-Invariante -1 hat, ist es auch nicht möglich, eine Darstellung zu ψ über einem reellen Körper zu finden. Hierzu müssen wir zum Charakter $2 \cdot \psi$ vom Grad 4 übergehen.

Die vierdimensionale Darstellung.

Der Charakter ψ ist zweimal in der regulären Darstellung von G enthalten, also gibt es eine Darstellung mit dem Charakter $2 \cdot \psi$, die über einem Körper K mit $\psi(\sigma) \in K \ \forall \sigma \in G$ definiert ist. Unter den schwächeren Voraussetzungen

$$\text{char}(K) \nmid 2n, \ \zeta_{2n} + \zeta_{2n}^{-1} \in K \text{ und } i^n \in K$$

möchten wir jetzt für diese vierdimensionale Darstellung eine Minimalbasis finden. Durch

$$\begin{aligned} \chi_1 &: \ \tau \mapsto -1, \ \sigma \mapsto 1 \text{ und} \\ \chi_2 &: \ \tau \mapsto i^n, \ \sigma \mapsto -1 \end{aligned}$$

werden zwei lineare Charaktere von G definiert. Wir werden sehen, daß es drei linear unabhängige Pseudo-Invarianten s_1, s_2 und s_3 vom Grad 2 zum Gewicht χ_1 und (mindestens) zwei linear unabhängige Pseudo-Invarianten t_1 und t_2 vom Grad n zu χ_2 gibt. Mit

$$\varphi_1 = \frac{s_1}{s_3}, \ \varphi_2 = \frac{s_2}{s_3} \text{ und } \varphi_3 = \frac{t_1}{t_2}$$

erhalten wir dann die Gradabschätzung

$$2 \cdot 2 \cdot n = 2 \cdot \frac{|G|}{|\{\pm \mathbf{1}\}|},$$

was nicht ganz ausreicht. Die Polynome

$$f_i := s_i - T_i \cdot s_3 \ (i = 1,2) \text{ und } f_3 := t_1 - T_3 \cdot t_2$$

(siehe Lemma 3.10) haben jedoch gemeinsame projektive Nullstellen P mit $s_3(P) = 0$, ohne daß wir uns um die Wahl der s_i weiter kümmern müßten! In der vierdimensionalen Darstellung hat σ nämlich jeweils $\zeta_{2n}^{\pm 1}$ als doppelten Eigenwert. Ist W der Eigenraum zu ζ_{2n}, so folgt für $w \in W$

$$\zeta_{2n}^2 \cdot s_i(w) = s_i(\zeta_{2n} w) = s_i(\sigma(w)) = \chi_1(\sigma^{-1}) \cdot s_i(w) = s_i(w),$$

also $s_i|_W = 0$. Nun ist $f_3|_W$ ein homogenes Polynom in zwei Unbestimmten, hat also projektive Nullstellen.

Nach Lemma 3.10 folgt $K(V)_0^G = K(\varphi_1, \varphi_2, \varphi_3)$, wenn die Existenz der s_i und t_i und die algebraische Unabhängigkeit der φ_i gezeigt ist. Die Existenz könnte man schon anhand der Molien-Reihen (und sogar ohne genaue Angabe der Darstellung) nachweisen. Für die algebraische Unabhängigkeit müssen wir jedoch expliziter rechnen.

Die Darstellung wir durch

$$\sigma \mapsto \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & \alpha & 0 & 0 \\ 0 & 0 & \alpha & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \ \tau \mapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

mit $\alpha = \zeta_{2n} + \zeta_{2n}^{-1}$ gegeben. Für die s_i können wir

$$\begin{aligned} s_1 &= x_1x_4 + x_2x_3 + \alpha x_2x_4, \\ s_2 &= x_1^2 + x_2^2 + \alpha x_1x_2 - \left(x_3^2 + x_4^2 + \alpha x_3x_4\right), \\ s_3 &= x_1x_3 - x_2x_4 \end{aligned}$$

nehmen. Die t_i konstruieren wir auf folgende Weise:

Zu $a, b \in K$ sei $p_{a,b} = \prod_{i=0}^{n-1} \sigma^i(ax_1 + bx_2)$. Über $K(\zeta_{2n})$ ist σ diagonalisierbar, mit geeigneten Koordinaten x_1' und x_2' gilt also $ax_1 + bx_2 = a'x_1' + b'x_2'$ mit $a', b' \in K(\zeta_{2n})$ und $\sigma^i(ax_1 + bx_2) = \zeta_{2n}^i(a'x_1' + \zeta_{2n}^{-2i} \cdot b'x_2')$. Bis auf Konstante ist $p_{a,b}$ damit gleich $a'^n x_1'^n - b'^n x_2'^n$, also $\sigma(p_{a,b}) = -p_{a,b}$, und $p_{a,b}$ hat keine mehrfachen Faktoren. Durch $t_{a,b} = p_{a,b} + i^{-n} \cdot \tau(p_{a,b})$ erhalten wir nun Pseudo-Invarianten vom Grad n zum Gewicht χ_2. Wir wählen $p_1 = p_{1,0}$ und $t_1 = t_{1,0}$.

Es gibt $a, b \in K$, so daß $p_{a,b}$ teilerfremd zu p_1 ist. Sonst würde nämlich $|\mathbb{P}^1(K)| = n$ folgen, also $|K| = n - 1$. Dann wäre $\zeta_{2n} \notin K$, also $[K(\zeta_{2n}) : K] = 2$, und $\mathrm{Gal}\,(K(\zeta_{2n})/K)$ würde durch $\zeta_{2n} \mapsto \zeta_{2n}^{n-1}$ erzeugt. Es folgte $\zeta_{2n}^{n-1} = \zeta_{2n}^{-1}$, also $2n \mid n$, ein Widerspruch. Durch geeignete Wahl von a und b erhalten wir also ein $p_2 = p_{a,b}$ und $t_2 = t_{a,b}$, so daß p_1 und p_2 teilerfremd sind.

Betrachtet man die φ_i nun als Funktionen in x_1/x_4, x_2/x_4 und x_3/x_4, so ist zu zeigen, daß die Jacobi-Determinante $\mathcal{J}$ der φ_i nicht verschwindet. Dann folgt die algebraische Unabhängigkeit nach Benson [3, Prop. 5.4.2], da man im Falle endlicher Charakteristik annehmen kann, daß K ein endlicher Körper und damit vollkommen ist.

Mit $\nabla = \begin{pmatrix} \partial_{x_1} \\ \partial_{x_2} \\ \partial_{x_3} \end{pmatrix}$ ist

$$\begin{aligned} \mathcal{J} &= \left(\frac{1}{s_3^{12}t_2^6} \cdot \left|s_3\nabla s_1 - s_1\nabla s_3, s_3\nabla s_2 - s_2\nabla s_3, t_2\nabla t_1 - t_1\nabla t_2\right|\right)\Big|_{x_4=1} = \\ &= \left(\frac{1}{s_3^9t_2^6} \cdot \underbrace{\left|s_3\nabla s_1 - s_1\nabla s_3, \nabla s_2, t_2\nabla t_1 - t_1\nabla t_2\right|}_{:= \mathcal{J}_0}\right)\Big|_{x_4=1}. \end{aligned}$$

Wir spezialisieren $x_1 = x_3 = 0$ und erhalten $t_1 = 0$, $t_2 \neq 0$, $\partial_{x_1} t_1 = c \cdot x_2^{n-1}$ mit $c \in K^\times$,

$\partial_{x_2} t_1 = 0$ und $\partial_{x_3} t_1 = i^{-n} \cdot c$, also

$$\begin{aligned} \mathcal{J}_0\Big|_{x_1=x_3=0,\ x_4=1} &= t_2\Big|_{x_1=x_3=0,\ x_4=1} \cdot \begin{vmatrix} -x_2 & \alpha x_2 & c x_2^{n-1} \\ 0 & 2x_2 & 0 \\ -x_2^2 & -\alpha & i^{-n} c \end{vmatrix} = \\ &= t_2\Big|_{x_1=x_3=0,\ x_4=1} \cdot 2cx_2^2(x_2^n - i^{-n}) \neq 0. \end{aligned}$$

Damit ist gezeigt, daß das Noethersche Problem auch für die vierdimensionale Darstellung eine positive Antwort hat.

W. GRÖBNER hat in [22] für $n = 2$ auf anderem Wege eine Minimalbasis gefunden und das zugehörige generische Polynom berechnet. Es erübrigt sich daher, dies hier anzugeben. Die erzeugenden Invarianten $j_1, \ldots, j_4$ aus [22] lassen sich leicht als rationale Funktionen in unseren φ_i (mit einer Invariante vom Grad 2 als φ_4) darstellen und umgekehrt.

Grenzen der Strategie.

Es dürfte anhand der Beispiele klar geworden sein, wie schwierig die Anwendung unserer Strategie im Einzelfall ist. Es überrascht daher nicht, daß das Verfahren schon bei relativ kleinen Graden an seine Grenzen stößt. Ein Beispiel hierfür ist die einfache Gruppe A_5 mit ihrer natürlichen Permutationsdarstellung, für die das Noethersche Problem nach MAEDA [34] eine positive Antwort über $K = \mathbb{Q}$ hat. Es ist jedoch trotz langen Versuchens nicht gelungen, mit Hilfe unserer Strategie eine Minimalbasis zu finden. Selbst die Verifikation der in [34] angegebenen Minimalbasis mit Algorithmus 3.6 scheitert an der Schwierigkeit der Gröbnerbasisberechnung.

Auf der anderen Seite werden wir im folgenden Abschnitt sehen, daß sich für modulare Darstellungen mit der Strategie sehr viel erreichen läßt.

3.3 Modulare Anwendungen

Während wir im letzten Abschnitt stets $\mathrm{char}(K) \nmid |G|$ vorausgesetzt haben, betrachten wir nun Fälle von „schlechter“ Charakteristik (*modulare Darstellungen*). Obwohl hier die Invariantentheorie generell schwieriger wird, treten einige Darstellungen niedrigen Grades auf, die es in allgemeiner Charakteristik gar nicht gibt. Daher hat man für diese gute Chancen, positive Antworten auf das Noethersche Problem zu finden. Durch den direkten Übersetzungsmechanismus aus Satz 1.11 lassen sich in vielen Fällen dann sofort generische Polynome angeben.

In Abschnitt 1.4.3 haben wir schon die metazyklischen Gruppen mit Normalteiler Z_p als Beispiel kennengelernt. Hier werden nun zunächst einige Beispiele aus der Literatur zusammengestellt, und die Frage nach den zugehörigen generischen Polynomen wird untersucht. Danach werden für die konformen symplektischen Gruppen $\mathrm{CSp}_{2n}(q)$, für die einfachen Gruppen $\Omega_n(q)$ (n ungerade), für weitere Untergruppen der orthogonalen Gruppen und für die speziellen unitären Gruppen $\mathrm{SU}_n(q^2)$ Minimalbasen konstruiert. Damit ist das Feld der klassischen Gruppen weitgehend abgedeckt.

3.3.1 Lineare Gruppen und p-Gruppen

p-Gruppen.

Es sei K ein Körper der Charakteristik p, V ein n-dimensionaler K-Vektorraum und $G \leq \mathrm{GL}(V)$ eine p-Gruppe. Nach MIYATA [38] ist dann $K(V)^G$ rein transzendent über K. Satz 1.11 liefert also, daß jede p-Gruppe ein generisches Polynom über $\mathbb{F}_p$ besitzt.

Im Beweis zeigt MIYATA zunächst, daß man eine K-Basis finden kann, so daß jedes $\sigma \in G$ als obere Dreiecksmatrix mit Einsen in der Diagonale operiert. Ist G speziell die Gruppe *aller* solcher Matrizen und $K = \mathbb{F}_q$, so liefern die Produkte über die Bahnen

$$s_i := \prod_{f \in \{\sigma(x_i) \mid \sigma \in G\}} f = \prod_{a_{i+1},\ldots,a_n \in K} (x_i + a_{i+1}x_{i+1} + \cdots + a_n x_n)$$

eine Minimalbasis (siehe WILKERSON [55]), und es gilt sogar für den Invariantenring

$$K[V]^G = K[s_1, \ldots, s_n].$$

Für das $\mathcal{M} \subset V^*$ aus Satz 1.11 kann man die Bahn von x_1 nehmen und erhält so ein generisches Polynom vom Grad q^{n-1} in n oder nach Zusatz 1.12 sogar in $n-1$ Parametern. Für $n = 2$, also

$$G = \{\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in K\} \cong \mathbb{F}_q^+,$$

haben wir

$$\prod_{a \in \mathbb{F}_q} (X - x_1 - ax_2) = (X - x_1)^q - (X - x_1)x_2^{q-1} = X^q - s_2^{q-1} \cdot X - s_1,$$

was nach Zusatz 1.12 zu dem generischen Polynom

$$g(X) = X^q - X - t$$

führt, eine weitere Verallgemeinerung der Artin-Schreier Polynome (siehe auch Abschnitt 1.4.3).

Für $n = 3$, also

$$G = \{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in K\},$$

ergibt sich aus einer etwas längeren Rechnung

$$g(X) = X^{q^2} - (1 + t_1^{q-1}) \cdot X^q + t_1^{q-1} \cdot X + t_2$$

als generisches Polynom für G über $K = \mathbb{F}_q$.

$\mathrm{GL}_n(q)$ und $\mathrm{SL}_n(q)$.

Es ist schon seit DICKSONS Arbeit [17] aus dem Jahre 1911 bekannt, daß für $V = \mathbb{F}_q^n$ die Invariantenringe $\mathbb{F}_q[V]^{\mathrm{GL}_n(q)}$ und $\mathbb{F}_q[V]^{\mathrm{SL}_n(q)}$ Polynomringe sind. Daraus erhalten wir

Satz 3.12. *Sei $n \geq 2$ eine natürliche Zahl, q eine Primzahlpotenz und $K = \mathbb{F}_q$. Dann gelten:*

(a) Das Polynom

$$g(X) = X^{q^n-1} + t_1 \cdot X^{q^{n-1}-1} + \cdots + t_{n-1} \cdot X^{q-1} + t_n$$

ist ein generisches Polynom für die Gruppe $\mathrm{GL}_n(q)$ über K.

(b) Das Polynom

$$g(X) = X^{q^n-1} + t_1 \cdot X^{q^{n-1}-1} + \cdots + t_{n-1} \cdot X^{q-1} + t_n^{q-1}$$

ist ein generisches Polynom für die Gruppe $\mathrm{SL}_n(q)$ über K.

Insbesondere haben die Gruppen $\mathrm{GL}_n(q)$, $\mathrm{SL}_n(q)$, $\mathrm{PGL}_n(q)$ und $\mathrm{PSL}_n(q)$ Galoisrealisierungen über dem Körper $\mathbb{F}_q(t)$.

Beweis. Wir lassen $G = \mathrm{GL}_n(q)$ in natürlicher Weise auf $V = K^n$ operieren. Nach WILKERSON [55] gilt dann

$$\prod_{y \in V^*} (X - y) = X^{q^n} + c_{n-1} \cdot X^{q^{n-1}} + \cdots + c_1 \cdot X^q + c_0 \cdot X,$$

und die c_i erzeugen $K[V]^G$. Mit $\mathcal{M} = V^* \setminus \{\mathbf{0}\}$ folgt dann aus Satz 1.11 sofort Teil (a). Die c_i sind die sogenannten **Dickson-Invarianten**.

Weiter gibt es nach WILKERSON [55] für $G' = \mathrm{SL}_n(q)$ ein $u \in K[V]^{G'}$ mit $u^{q-1} = c_0$, so daß $c_1, \ldots, c_{n-1}$ und u ganz $K[V]^{G'}$ erzeugen. Hieraus folgt Teil (b).

Die Galoisrealisierungen der projektiven Gruppen erhält man, indem man den Fixkörper des Zentrums von G bzw. von G' nimmt. Da $\mathbb{F}_q(t)$ nach FRIED und JARDEN [19, *Theorem* 12.10] ein Hilbertkörper ist, erhalten wir auch Erweiterungen über $\mathbb{F}_q(t)$ mit den angegebenen Galoisgruppen. □

Mit $n = 3$ und $q = 2$ ergibt sich beispielsweise

$$g(X) = X^7 + t_1 X^3 + t_2 X + t_2$$

als generisches Polynom für $\mathrm{GL}_3(2) \cong \mathrm{PSL}_2(7)$ über $\mathbb{F}_2$, wobei wir wegen $\deg\left(\frac{c_0}{c_1}\right) = 1$ Zusatz 1.12 benutzen konnten.

ABHYANKAR untersucht in [1] die in Satz 3.12 angegebenen Polynome. Demnach läßt sich das t_n aus Teil (b) zu einem Element aus $\mathbb{F}_q$ spezialisieren, und man erhält immer noch ein $\mathrm{SL}_n(q)$-Polynom. Es werden auch die entsprechenden $\mathrm{PGL}_n(q)$- und $\mathrm{PSL}_n(q)$-Polynome angegeben (welche selbstverständlich nicht generisch sind).

3.3.2 Symplektische Gruppen und konforme symplektische Gruppen

D. CARLISLE und P. H. KROPHOLLER haben für einige klassische Gruppen (mit ihrer natürlichen Darstellung) Invariantenringe beziehungsweise -körper untersucht. Wir beginnen mit ihrem Ergebnis über die symplektischen Invarianten und geben dann mit Hilfe unserer Methoden Minimalbasen für die konformen symplektischen Gruppen an.

Die $\mathrm{Sp}_{2n}(q)$.

Sei V ein $2n$-dimensionaler, nicht ausgearteter symplektischer Vektorraum über $K = \mathbb{F}_q$ mit einer Primzahlpotenz q und $G = \mathrm{Sp}(V)$ die symplektische Gruppe von V. CARLISLE und KROPHOLLER haben den Invariantenring $K[V]^G$ untersucht (siehe BENSON [3]) und dabei unter anderem gezeigt, daß $K(V)^G$ rein transzendent über K ist (siehe den Beweis zu *Theorem* 8.3.4 in [loc. cit.]). Im Beweis werden Invarianten $s_1, \ldots, s_{2n} \in K[V]^G$ vom Grad $\deg(s_i) = q^i + 1$ angegeben, die direkt von der symplektischen Form her kommen. Diese sind gegeben durch

$$s_i(v) = \langle v, F^i(v) \rangle$$

für $v \in \bar{K} \otimes_K V$, wobei $\langle \cdot, \cdot \rangle$ die symplektische Form, F der Frobenius-Automorphismus und $\bar{K}$ ein algebraischer Abschluß von K sind. Wegen des Nichtverschwindens der Jacobi-Determinante der s_i sind diese nach BENSON [3, Prop. 5.4.2] algebraisch unabhängig. Nun werden explizite Formeln hergeleitet, nach denen sich die Dickson-Invarianten c_i (siehe der Beweis zu Satz 3.12) als rationale Funktionen in den s_i darstellen lassen. Hierin steckt die Hauptarbeit des Beweises. Es folgt

$$K(V) \geq K(s_1, \ldots, s_{2n}) \geq K(V)^{\mathrm{GL}_{2n}(q)},$$

und ein einfaches galoistheoretisches Argument liefert nun

$$K(V)^G = K(s_1, \ldots, s_{2n}). \tag{3.3}$$

Bei der Frage nach den entsprechenden generischen Polynomen geht es nun darum, eine möglichst kurze G-Bahn $\mathcal{M}$ in $V^* \setminus \{\mathbf{0}\}$ zu finden. Da die symplektische Form einen mit G verträglichen Isomorphismus zwischen V und V^* liefert, können wir diese Bahn in V suchen. G operiert jedoch nach HUPPERT [23, Kap. II, Satz 9.15] transitiv auf $V \setminus \{\mathbf{0}\}$, also ist das $f(X)$ aus Satz 1.11

$$f(X) = \prod_{y \in V^* \setminus \{\mathbf{0}\}} (X - y) = X^{q^{2n}-1} + c_{2n-1} \cdot X^{q^{2n-1}-1} + \cdots + c_1 \cdot X^{q-1} + c_0.$$

Um das generische Polynom $g(X)$ für G zu erhalten, muß man also nur die c_i als rationale Funktionen in den s_i darstellen, was durch die Formeln von CARLISLE und KROPHOLLER bewerkstelligt wird. Diese Formeln lassen sich zwar für einzelne n leicht auswerten, ihre allgemeine Darstellung ist jedoch recht kompliziert. Deshalb soll hier auf die Wiedergabe verzichtet werden.

Anmerkung. Der Nachweis von Gleichung (3.3) ließe sich für $q \geq 3$ auch durch einfache Gradabschätzung nach Korollar 3.11 durchführen. Es gilt nämlich

$$\frac{\prod_{i=1}^{2n} \deg(s_i)}{|G|} = \frac{\prod_{i=1}^{2n}(q^i + 1)}{q^{n^2} \prod_{i=1}^{n}(q^{2i} - 1)} = \frac{\prod_{i=n+1}^{2n}(q^i + 1)}{q^{n^2} \prod_{i=1}^{n}(q^i - 1)} < 2,$$

wobei die letzte Abschätzung aus Lemma 3.13 folgt. Die Formal für $|G|$ ist dabei JACOBSON [24, 6.10] entnommen. ◁

Die $\mathrm{CSp}_{2n}(q)$**.**

Es sei nun $G = \mathrm{CSp}(V)$ die konforme symplektische Gruppe, d.h.

$$G = \left\{ \sigma \in \mathrm{GL}(V) \,\middle|\, \exists \chi(\sigma) \in K\colon \langle \sigma(v), \sigma(w) \rangle = \chi(\sigma) \cdot \langle v, w \rangle \ \ \forall v, w \in V \right\}.$$

Dann ist $\chi\colon G \to K^\times$ ein Homomorphismus, der sich als surjektiv herausstellt. Die exakten Sequenzen

$$1 \ \to \ \mathrm{Sp}(V) \ \to \ G \ \to \ \ K^\times \ \ \to \ 1 \quad \text{und}$$

$$1 \ \to \ \ K^\times \ \ \to \ G \ \to \ \mathrm{PCSp}(V) \ \to \ 1$$

liefern $|\mathrm{PCSp}(V)| = |\mathrm{Sp}(V)|$, wobei $\mathrm{PCSp}(V)$ die Faktorgruppe nach den in G enthaltenen skalaren Matrizen bezeichnet. Für die s_i von Carlisle und Kropholler gilt $\sigma(s_i) = \chi(\sigma^{-1}) \cdot s_i$ $(\sigma \in G)$. Die folgenden rationalen Funktionen sind also G-Invarianten vom Grad 0:

$$\varphi_1 = \frac{s_1^{q^2+1}}{s_2^{q+1}}, \ \varphi_{2i} = \frac{s_{2i+1}}{s_1^{q^{2i}-q^{2i-1}+-\cdots-q+1}}, \ \varphi_{2i+1} = \frac{s_{2i+2}}{s_1^{q^{2i+1}-q^{2i}+-\cdots+q^3-q^2} \cdot s_2} \ (i = 1, \ldots, n-1).$$

Es gilt $K(s_1, \varphi_1, \varphi_2^{q+1}, \ldots, \varphi_{2n-1}^{q+1}) = K(s_1, s_2^{q+1}, \ldots, s_{2n}^{q+1})$, wobei der zweite Körper über K den Transzendenzgrad $2n$ hat, also sind die φ_i algebraisch unabhängig. Wir haben die Gradabschätzung

$$\frac{\deg\left(s_1^{q^2+1}\right) \cdot \prod_{i=1}^{n-1} \left(\deg(s_{2i+1}) \cdot \deg(s_{2i+2})\right)}{|\mathrm{PCSp}(V)|} = \frac{\prod_{i=1}^{2n}(q^i+1)}{q^{n^2} \cdot \prod_{i=1}^{n}(q^{2i}-1)}.$$

Für $q \geq 3$ ist dies nach dem nachfolgenden Lemma 3.13 echt kleiner als 2. Dann folgt nach Lemma 3.10, daß

$$K(V)_0^{\mathrm{PCSp}(V)} = K(\varphi_1, \ldots, \varphi_{2n-1}),$$

nach Proposition 3.3(a) und 3.1(a) ist also auch $K(V)^G$ rein transzendent über K. Für $q = 2$ gilt dies sowieso, da dann $G = \mathrm{Sp}(V)$ ist.

Es fehlt noch das folgende

Lemma 3.13. *Es seien q, n und $m \in \mathbb{N}_0$ nicht negative ganze Zahlen, so daß $q \geq 4$ oder $q = 3$ und $m \geq 2$, oder $q = 3$, $m = 1$ und $n \leq 2$. Dann ist*

$$\rho := \frac{\prod_{i=m+1}^{n+m}(q^i+1)}{q^{nm} \cdot \prod_{i=1}^{n}(q^i-1)} < 2.$$

Beweis. Wir betrachten zunächst den Fall $n = 1$. Dann ist

$$\rho = 1 + \frac{q^m+1}{q^{m+1}-q^m} < 2 \ \Leftrightarrow \ q^m(q-2) > 1.$$

Dies ist für $q \geq 4$ oder $q = 3$ und $m \geq 1$ erfüllt.

Nun sei $n > 1$. Dann gilt

$$\rho \leq \frac{(q^{m+1}+1)(q^{m+2}+1)\prod_{i=m+3}^{n+m}(q^i+q^m)}{q^{nm}(q-1)(q^2-1)\prod_{i=3}^{n}(q^i-1)} = \underbrace{\frac{(q^{m+1}+1)(q^{m+2}+1)}{q^{2m}(q-1)(q^2-1)}}_{:=\rho_1} \cdot \underbrace{\prod_{i=3}^{n}\left(\frac{q^i+1}{q^i-1}\right)}_{:=\rho_2}.$$

Dabei ist wegen $\ln(1+x) \leq x$ für $x > 0$

$$\ln(\rho_2) \leq \sum_{i=3}^{\infty} \frac{2}{q^i-1} \leq \sum_{i=3}^{\infty} \frac{2}{q^i - q^i/q^3} = \frac{2q}{(q^3-1)(q-1)}$$

und

$$\rho_1 \leq \frac{(q+1)(q^2+1)}{(q-1)(q^2-1)} = \frac{q^2+1}{(q-1)^2}.$$

Für $q \geq 4$ ergibt sich die Abschätzung

$$\rho \leq \frac{17}{9} \cdot e^{8/189} \approx 1.970558113 < 2.$$

Für $q = 3$ und $m \geq 2$ erhalten wir für ρ_1 die bessere Abschätzung

$$\rho_1 \leq \frac{(q^3+1)(q^4+1)}{q^4(q-1)(q^2-1)} = \frac{287}{162}$$

und damit

$$\rho \leq \frac{287}{162} \cdot e^{3/26} \approx 1.988281098 < 2.$$

Schließlich verifizieren wir die Ungleichung für $q = 3$, $m = 1$ und $n = 2$ durch direktes Nachrechnen. □

3.3.3 Orthogonale Gruppen

Carlisle und Kropholler geben in [11] Minimalbasen für alle orthogonalen Gruppen $\mathrm{O}_n(q)$ (wobei q eine ungerade Primzahlpotenz ist) mit ihrer natürlichen Darstellung über $\mathbb{F}_q$ an. Von großem Interesse sind auch die Kommutatorgruppen $\Omega_n(q)$ der orthogonalen Gruppen, deren Faktorgruppen $\mathrm{P}\Omega_n(q)$ nach den Untergruppen der skalaren Matrizen bis auf einige Ausnahmen (siehe z.B. im Atlas [14]) einfach sind. Für ungerades n ist $\mathrm{P}\Omega_n(q) = \Omega_n(q)$, und dies ist einfach, wenn nicht $n = q = 3$. Außerdem sind die Zwischengruppen interessant, von denen es wegen

$$\mathrm{O}_n(q) \Big/ \Omega_n(q) \cong Z_2 \times Z_2 \text{ (für } n \geq 3)$$

drei echte gibt. Die $\mathrm{SO}_n(q)$ ist eine davon.

Satz 3.14. *Es seien q eine ungerade Primzahlpotenz, $K = \mathbb{F}_q$ und V ein n-dimensionaler, nicht ausgearteter orthogonaler Raum über K, $n \geq 3$. Mit $\mathrm{O}(V)$, $\Omega(V)$ bzw. $\mathrm{SO}(V)$ bezeichnen wir die orthogonale Gruppe von V, deren Kommutatorgruppe bzw. die spezielle orthogonale Gruppe. Dann gelten:*

(a) *Sei n ungerade. Dann ist $K(V)^G$ für alle fünf Zwischengruppen $\Omega(V) \leq G \leq \mathrm{O}(V)$ rein transzendent über K.*

(b) *Sei n gerade. Dann ist $K(V)^G$ für alle Zwischengruppen $\Omega(V) \leq G \leq \mathrm{O}(V)$ außer $G = \Omega(V)$ und $G = \mathrm{SO}(V)$ rein transzendent über K.*

(c) *Sei $n = 3$. Ist dann $\sigma \in \mathrm{O}(V)$ eine Spiegelung entlang einem Vektor $v \in V$ mit Skalarprodukt $\langle v, v\rangle = -1$ (Ein solcher existiert immer!) und $G = \langle \Omega(V), \sigma\rangle$, so sind $K[V]^G$ und $K[V]^{\mathrm{O}(V)}$ Polynomringe über K. Für $q \equiv 1 \bmod 4$ ist $G = \Omega(V) \times \{\pm \mathbf{1}\}$.*

Anmerkung. Nach NAKAJIMA [39] ist $K[V]^G$ für *keine* Zwischengruppe $\Omega(V) \leq G \leq \mathrm{O}(V)$ (mit den Bezeichnungen von Satz 3.14) ein Polynomring über K, falls $n \geq 4$. Die Aussage in Satz 3.14(c) gilt also für kein anderes n außer $n = 3$. Es ist mir nicht bekannt, ob diese Aussage in der Literatur schon zu finden ist. ◁

Beweis zu Satz 3.14. Es seien $e_1, \ldots, e_n \in V$ eine Orthogonalbasis, $x_1, \ldots, x_n \in V^*$ die Dualbasis und $\lambda_i = \langle e_i, e_i\rangle$ die Skalarprodukte. Dann bilden

$$s_i = \sum_{j=1}^{n} \lambda_j \cdot x_j^{q^i+1} \quad (i = 0, \ldots, n-1)$$

die von CARLISLE und KROPHOLLER angegebene Minimalbasis. (Es ist unmittelbar einzusehen, daß die s_i Invarianten unter der $\mathrm{O}(V)$ sind, da $s_i(v) = \langle v, F^i(v)\rangle$ für $v \in \bar{K} \otimes_K V$, wobei F der Frobenius und $\bar{K}$ ein algebraischer Abschluß von K sind.) Die Idee ist nun, s_{n-1} durch eine Invariante t von kleinerem Grad zu ersetzen.

Es sei $b \in K^\times$ und $V_b := \{v \in V \mid \langle v, v\rangle = b\}$. (Nach JACOBSON [24, 6.10] gilt immer $V_b \neq \emptyset$, und V_b ist nach dem Wittschen Fortsetzungssatz genau eine Bahn unter $\mathrm{O}(V)$.) Mit einem v liegt auch $-v$ in V_b, wir können also ein Vertretersystem V_b' von $V_b/\{\pm 1\}$ wählen. Für $v \in V_b'$ ist dann $v^* := \langle v, \cdot\rangle \in V^*$ eine Linearform, und wir bilden

$$t_b = \prod_{v \in V_b'} v^* \in K[V],$$

welches bis auf Vorzeichen eindeutig durch b bestimmt ist. Für $\sigma \in \mathrm{O}(V)$ ist $\sigma(t_b) = \pm 1 \cdot t_b$, also definiert $\sigma \mapsto \sigma(t_b)/t_b$ einen linearen Charakter von $\mathrm{O}(V)$, der auf $\Omega(V) = \mathrm{O}(V)'$ trivial sein muß, d.h. $t_b \in K[V]^{\Omega(V)}$.

Wir zeigen nun, daß die Jacobi-Determinante $\mathcal{J}$ von $(s_0, \ldots, s_{n-2}, t_b)$ nicht verschwindet, so daß nach BENSON [3, Prop. 5.4.2] die algebraische Unabhängigkeit dieser Invarianten folgt. Wir haben

$$\frac{\partial s_0}{\partial x_j} = 2\lambda_j x_j, \quad \frac{\partial s_i}{\partial x_j} = \lambda_j x_j^{q^i} \quad (i \geq 1)$$

und $t_b = v^* \cdot g$ mit irgendeinem $v \in V_b$ und $g \in K[V]$. Dabei gilt $v^* \nmid g$, weil $-v$ das einzige skalare Vielfache von v in V_b ist. Wir können $\mathcal{J}$ auch bezüglich einer Orthogonalbasis berechnen, die v enthält, und somit ohne Beschränkung der Allgemeinheit annehmen, daß $v = e_1$ und $v^* = x_1$ ist. Wir spezialisieren $x_1 = 0$ und erhalten

$$\mathcal{J}\,|_{x_1=0} = 2 \cdot \begin{vmatrix} 0 & \lambda_2 x_2 & \cdots & \lambda_n x_n \\ \vdots & \vdots & & \vdots \\ 0 & \lambda_2 x_2^{q^{n-2}} & \cdots & \lambda_n x_n^{q^{n-2}} \\ g\,|_{x_1=0} & 0 & \cdots & 0 \end{vmatrix} \neq 0,$$

da $x_1 \nmid g$. Damit sind die $s_0, \ldots, s_{n-2}, t_b$ tatsächlich algebraisch unabhängig über K, und die Voraussetzungen für die Anwendung von Korollar 3.11 sind gegeben. Nun geht es darum, in den einzelnen Fällen durch entsprechende Wahl des $b \in K^\times$ eine günstige Gradabschätzung zu erreichen.

(a) Es gilt $n = 2m + 1$, und nach JACOBSON [24, 6.10] ist

$$|V_b| = q^{2m} \pm q^m, \tag{3.4}$$

wobei das „$\pm$" hier davon abhängt, ob b in $(K^\times)^2$ liegt oder nicht. Wir können also b so wählen, daß der Grad von $t := t_b$ gerade wird. Dann gilt $t \in K[V]^{\Omega(V)\times\{\pm\mathbf{1}\}}$. Die Ordnung der $\Omega(V)$ entnehmen wir [loc. cit.] und erhalten

$$\begin{aligned} \frac{\prod_{i=0}^{n-2} \deg(s_i) \cdot \deg(t)}{|\Omega(V) \times \{\pm\mathbf{1}\}|} &= \frac{\prod_{i=0}^{n-2}(q^i+1) \cdot q^m \cdot (q^m \pm 1)/2}{q^{m^2} \cdot \prod_{i=1}^{m}(q^{2i}-1)} \leq \\ &\leq \frac{(q^m+1) \cdot \prod_{i=m+1}^{2m-1}(q^i+1)}{q^{m(m-1)} \cdot \prod_{i=1}^{m}(q^i-1)}. \end{aligned} \tag{3.5}$$

Der letzte Ausdruck ist aber nach dem folgenden Lemma 3.13 echt kleiner als 2, ausgenommen der Fall $m = 1$ und $q = 3$. In allen anderen Fällen folgt mit Korollar 3.11

$$K(V)^{\Omega(V)\times\{\pm\mathbf{1}\}} = K(s_0, \ldots, s_{n-2}, t) \tag{3.6}$$

und mit derselben Gradabschätzung

$$K(V)^{\mathrm{O}(V)} K(s_0, \ldots, s_{n-2}, t^2), \tag{3.7}$$

da t^2 eine $\mathrm{O}(V)$-Invariante ist. Für $m = 1$ und $q = 3$ ist der Quotient in (3.5) genau 2, es genügt also nach Lemma 3.10, gemeinsame projektive Nullstellen von s_0, s_1 und t nachzuweisen. Nach JACOBSON [24, 6.10] kann man $\lambda_1 = 1$ und $\lambda_2 = \lambda_3 = -1$ annehmen und dann $b = -1$ wählen. Dann liegt $(0,0,1) \in V_b$, also $t(\xi_1, \xi_2, 0) = 0$ mit irgendwelchen ξ_i. Also liefert beispielsweise $s_i(1,1,0) = 0$ eine gemeinsame projektive Nullstelle, und damit gelten (3.6) und (3.7) auch für $m = 1$ und $q = 3$.

Korollar 3.4 liefert jetzt sofort, daß auch $K(V)^{\Omega(V)}$ rein transzendent über K ist. Für die verbleibenden zwei Zwischengruppen G gilt

$$\{\pm\mathbf{1}\} \cdot G = \mathrm{O}(V)$$

wegen $\mathrm{O}(V)/\Omega(V) \cong Z_2 \times Z_2$, also folgt auch hier, daß $K(V)^G$ rein transzendent über K ist.

(b) Es sei nun $n = 2m$. Nach JACOBSON [24, 6.10] gilt immer

$$|V_b| = q^{2m-1} - \epsilon \cdot q^{m-1}, \tag{3.8}$$

wobei $\epsilon = 1$ bzw. -1 ist, falls wir es bei $\mathrm{O}(V)$ mit dem Typ $\mathrm{O}^+_{2m}(q)$ bzw. $O^-_{2m}(q)$ zu tun haben. Der Grad von t_b ist also unabhängig von der Wahl von b. Wir wollen untersuchen, ob man durch diese Wahl immerhin die genaue Zwischengruppe $\Omega(V) \leq G \leq \mathrm{O}(V)$, die t_b festläßt, steuern kann.

Es sei $\sigma \in \mathrm{O}(V)$ die Spiegelung entlang einem Vektor $v_1 \in V$. Wir ergänzen v_1 zu einer Orthogonalbasis $v_1, \ldots, v_n$ von V. Bezüglich dieser Basis bedeutet die Anwendung von σ also das Umdrehen der ersten Koordinate. Wählt man nun ein Vertretersystem B von $K^\times/\{\pm 1\}$ und dann das Vertretersystem V_b' von $V_b/\{\pm 1\}$ so, daß die v_1-Koordinate jedes Vektors $v \in V_b'$ Null ist oder in B liegt, so ist die Anzahl der Elemente aus V_b', die bei Anwendung von σ auf ein $-v$ mit $v \in V_b'$ gehen, gerade

$$l = \big|\{v \in V_b' \mid \text{die } v_1\text{-Koordinate von } v \text{ ist} \neq 0\}\big| = |V_b'| - |W_b|/2,$$

wobei $W = v_1^\perp$ der von $v_2, \ldots, v_n$ aufgespannte orthogonale Raum ist und W_b die Menge der darin enthaltenen Vektoren der Norm b. Aber die Restklasse von $|W_b|/2$ modulo 2 läßt sich nach Formel (3.4) durch die Wahl von b steuern, und damit auch $\sigma(t_b)/t_b = (-1)^l$. Man kann also für jede Spiegelung σ das b so wählen, daß $t := t_b \in K[V]^G$ mit $G = \langle \Omega(V), \sigma \rangle$. Auf diese Weise erreicht man beide in der Behauptung (b) nicht ausgeschlossenen echten Zwischengruppen G.

Wir haben die Gradabschätzung

$$\frac{\prod_{i=1}^{n-2} \deg(s_i) \cdot \deg(t)}{|G|} = \frac{q^{m-1}(q^m - \epsilon) \cdot \prod_{i=1}^{2m-2}(q^i + 1)}{q^{m(m-1)}(q^m - \epsilon) \cdot \prod_{i=1}^{m-1}(q^{2i} - 1)} < 2$$

nach Lemma 3.13, Korollar 3.11 liefert also

$$K(V)^G = K(s_0, \ldots, s_{n-2}, t),$$

und mit derselben Abschätzung

$$K(V)^{\mathrm{O}(V)} = K(s_0, \ldots, s_{n-2}, t^2).$$

(c) Nach Jacobson [24, 6.10] können wir wieder $\lambda_1 = 1$ und $\lambda_2 = \lambda_3 = -1$ annehmen. Wir wählen b so, daß $-b \notin (K^\times)^2$. Es sei $v \in V$ mit $\langle v, v \rangle = -1$ und σ die Spiegelung entlang v. Dann hat der orthogonale Raum $W = v^\perp$ die Diskriminante -1, W_b hat also nach Formel (3.8) genau $q - 1$ Elemente. Wie im Beweis zu Teil (b) haben wir jetzt $\sigma(t_b)/t_b = (-1)^l$ mit

$$l = (|V_p| - |W_p|)/2 \equiv (q^2 - 2q + 1)/2 \equiv 0 \bmod 2,$$

also ist $t := t_b$ tatsächlich invariant unter σ. Die Gradabschätzung liefert hier sogar

$$\deg(s_0) \cdot \deg(s_1) \cdot \deg(t) = |G|,$$

nach Korollar 3.11 ist also $K(V)^G = K(s_0, s_1, t)$ und $K(V)^{\mathrm{O}(V)} = K(s_0, s_1, t^2)$.

Wir zeigen nun, daß s_0, s_1 und t nur den Nullvektor $\mathbf{0}$ als gemeinsame Nullstelle in $\bar{K}^n$ haben. Dann bilden diese Invarianten ein homogenes Parametersystem (siehe Abschnitt 2.2.3), $K[V]^G$ ist also ganz über $R := K[s_0, s_1, t]$. Damit liegt jede Invariante $f \in K[V]^G$ in $\mathrm{Quot}(R)$ und ist ganz über R, also $f \in R$, da R als Polynomring ganz abgeschlossen ist. Dieselbe Argumentation gilt dann für $K[V]^{\mathrm{O}(V)}$.

Nach einem Basiswechsel können wir annehmen, daß das Skalarprodukt die Gestalt

$$\langle (\xi_1, \xi_2, \xi_3), (\eta_1, \eta_2, \eta_3) \rangle = \xi_1\eta_2 + \xi_2\eta_1 - \xi_3\eta_3$$

hat. Dann liegt $v = (b, 1/2, 0)$ in V_b. Es sei nun $(\underline{\xi}) = (\xi_1, \xi_2, \xi_3) \in \bar{K}^3$ eine gemeinsame Nullstelle von s_0, s_1 und t. Dann existiert ein $w \in V_b$ mit $\langle w, (\underline{\xi})\rangle = 0$. Nach dem Wittschen Fortsetzungssatz gibt es $\sigma \in \mathrm{O}(V)$ mit $\sigma(w) = v$, also $\langle v, \sigma(\underline{\xi})\rangle = 0$. Da auch $\sigma(\underline{\xi})$ eine gemeinsame Nullstelle ist, können wir

$$\xi_1/2 + b \cdot \xi_2 = \langle v, (\underline{\xi})\rangle = 0$$

annehmen. Nun folgt

$$\xi_3^2 + 4b\xi_2^2 = -s_0(\underline{\xi}) = 0,$$

$(\underline{\xi}) \neq \mathbf{0}$ impliziert also ohne Einschränkung $\xi_2 = 1$ und dann $\xi_1 = -2b$ und $\xi_3^2 = -4b$. Aus

$$0 = -s_1(\underline{\xi}) = 2b + 2b + (-4b)^{\frac{q+1}{2}}$$

folgt nun $(-4b)^{\frac{q-1}{2}} = 1$, im Widerspruch zu $-b \notin (K^\times)^2$. □

Anmerkung. Die hier verwendete Methode führt auch zu einer einfachen Verifikation der von CARLISLE und KROPHOLLER [11] angegebenen Minimalbasen für $\mathrm{O}_n(q)$. Das Nichtverschwinden der Jacobi-Determinante ist hier sofort klar, und die Gradabschätzung lautet im Falle $n = 2m + 1$

$$\frac{\prod_{i=0}^{n-1} \deg(s_i)}{|\,\mathrm{O}_n(q)|} = \frac{\prod_{i=m+1}^{2m}(q^i + 1)}{q^{m^2} \cdot \prod_{i=1}^{m}(q^i - 1)} < 2$$

und im Falle $n = 2m$

$$\frac{\prod_{i=0}^{n-1} \deg(s_i)}{|\,\mathrm{O}_n(q)|} \leq \frac{\prod_{i=1}^{2m-1}(q^i + 1)}{q^{m(m-1)} \cdot (q^m - 1) \cdot \prod_{i=1}^{m-1}(q^{2i} - 1)} < 2,$$

jeweils nach Lemma 3.13. ◁

Die generischen Polynome.

Aus Satz 3.14 erhalten wir nun natürlich auch die entsprechenden generischen Polynome.

Korollar 3.15. *Für die in Satz 3.14(a) und (b) genannten Zwischengruppen $\Omega(V) \leq G \leq \mathrm{O}(V)$ existieren generische Polynome $g(X)$ in n Parametern (bzw. $n - 1$, falls $-\mathbf{1} \notin G$) für G über $\mathbb{F}_q$. Für $n = 3$ und $G = \Omega(V) \cong \mathrm{PSL}_2(q)$ kann man $g(X)$ so wählen, daß $\deg(g) = (q^2 - 1)/2$. Für die ersten drei q erhalten wir*

$q = 3$, also $G \cong A_4$:

$$g(X) = X^4 - u \cdot X^2 + u^2 \cdot X - (t_1 + 1)u^2$$

mit

$$u = t_2^2 + (t_1 + 1)\,(t_1 - 1)^2,$$

$q = 5$, also $G \cong A_5$:

$$g(X) = X^{12} - 2\,u^2 \cdot X^8 + 2\,(t_1 + 1)u^4 \cdot X^4 + 2\,t_2\,u^5 \cdot X^2 + (t_1 - 2)^2 u^6$$

mit

$$u = t_2^2 + (t_1 - 2)^2\,(t_1 + 2)^3,$$

$q = 7$, also $G \cong \mathrm{PSL}_2(7)$:

$$\begin{aligned} g(X) \;=\; & X^{24} - 3\,u^3 \cdot X^{18} + (t_1 + 1)u^6 \cdot X^{12} - \\ & -3\,(t_1^2 + t_1 - 1)u^9 \cdot X^6 + u^{11} \cdot X^3 - (t_1 - 2)^3 u^{12} \end{aligned}$$

mit

$$u = t_2^2 + (t_1 - 2)^3\,(t_1 + 2)^4.$$

Beweis. Die Behauptung folgt direkt mit Satz 1.11 bzw. Zusatz 1.12 aus Satz 3.14. Nur im Fall $n = 3$ und $G = \Omega(V)$ müssen wir zeigen, daß es eine G-stabile Teilmenge $\mathcal{M} \subset V^*$ mit $(q^2 - 1)/2$ Elementen gibt, die ganz V^* aufspannt. Da $V^* \cong V$ (G-isomorph), können wir $\mathcal{M}$ in V suchen. Um einen genauen Überblick über $\Omega(V)$ zu bekommen, benutzen wir den Isomorphismus $\Omega(V) \cong \mathrm{PSL}_2(q)$. Durch

$$\Phi\colon \mathrm{PSL}_2(q) \to \mathrm{GL}_3(q),\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad + bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}$$

wird ein Monomorphismus gegeben, und man sieht durch Nachrechnen, daß die Bilder unter Φ die quadratische Form $x_2^2 - x_1 x_3$ festlassen und die Determinante 1 haben, also ist $\mathrm{Bild}(\Phi)$ eine Untergruppe der $\mathrm{SO}_3(q)$ vom Index 2 und muß damit $= \Omega_3(q)$ sein. Nun sieht man aber sofort, daß der erste Standardbasisvektor e_1 eine Fixgruppe der Ordnung q hat, und daß seine Bahn ganz K^3 aufspannt. Die Bahnlänge ist also genau $(q^2 - 1)/2$. □

3.3.4 Unitäre Gruppen

In der oben genannten Arbeit [11] geben CARLISLE und KROPHOLLER auch Minimalbasen für die unitären Gruppen $\mathrm{U}_n(q^2)$ mit ihrer natürlichen linearen Darstellung an. Mit denselben Ideen wie im letzten Abschnitt erhalten wir nun auch Minimalbasen für die Gruppen $\mathrm{SU}_n(q^2)$.

Satz 3.16. *Es sei q eine Primzahlpotenz, $K = \mathbb{F}_{q^2}$ und V ein n-dimensionaler, nicht ausgearteter unitärer Raum über K, $n \geq 2$, wobei wir die Fälle $(n,q) = (2,2)$, $(2,3)$ oder $(3,2)$ ausschließen. Dann ist $K(V)^{\mathrm{SU}(V)}$ rein transzendent über K.*
Für $n = 2$ sind sogar $K[V]^{\mathrm{U}(V)}$ und $K[V]^{\mathrm{SU}(V)}$ Polynomringe.

Anmerkung. Die letzte Aussage ist für $\mathrm{char}(K) \neq 2,3$ ein Spezialfall von NAKAJIMA [39, *Theorem* 5.1]. Aus [loc. cit., *Theorem* 5.2] geht hervor, daß $n = 2$ das einzige n ist, für das diese Aussage gilt. ◁

Beweis zu Satz 3.16. Es seien $e_1, \ldots, e_n$ eine Basis von V und $x_1, \ldots, x_n$ die Dualbasis. Wir können annehmen, daß die hermitesche Form auf V die Gestalt

$$\Big\langle \sum_{i=1}^n \xi_i e_i, \sum_{j=1}^n \eta_i e_i \Big\rangle = \sum_{i=1}^n \xi_i \cdot \eta_i^q$$

hat. CARLISLE und KROPHOLLER geben die Invarianten

$$s_i = \sum_{j=1}^{n} x_j^{q^{2i-1}+1} \quad (i = 1, \ldots, n)$$

an[3] und zeigen, daß diese eine Minimalbasis von $K(V)^{\mathrm{U}(V)}$ bilden. Wir ersetzen s_n wieder durch eine $\mathrm{SU}(V)$-Invariante kleineren Grades, die wir durch Produktbildung über die Bahn einer Linearform modulo Konstanten konstruieren.

Es sei $V_1 = \{\sigma(e_1) \mid \sigma \in \mathrm{U}(V)\}$ die Bahn von e_1. Dann gilt

$$|\mathrm{U}(V)| = |V_1| \cdot |\mathrm{Stab}(e_1)|\,,$$

wobei $\mathrm{Stab}(e_1)$ den Stabilisator bezeichnet. Aber $\mathrm{Stab}(e_1) = \mathrm{U}(e_1^{\perp}) \cong U_{n-1}(q^2)$, wegen

$$\left|\mathrm{U}_n(q^2)\right| = q^{\frac{n(n-1)}{2}} \cdot \prod_{i=1}^{n} (q^i - (-1)^i)$$

(siehe z.B. ATLAS [14]) folgt also $|V_1| = q^{n-1} \cdot (q^n - (-1)^n)$. Mit $Z = \{z \in K \mid z^{q+1} = 1\}$ ist $S = \{z \cdot \mathrm{id}_V \mid z \in Z\}$ die Untergruppe der skalaren Matrizen in $\mathrm{U}(V)$, und für $v \in V_1$ ist $\{z \cdot v \mid z \in Z\}$ genau die Menge der skalaren Vielfachen von v, die auch in V_1 liegen. Wir wählen also ein Vertretersystem V_1' von V_1/Z und setzen

$$t = \prod_{v \in V_1'} v^* \in K[V],$$

wobei zu $v \in V$ die Linearform $v^* \in V^*$ durch $w \mapsto \langle w, v\rangle$ gegeben sei. Für $\sigma \in \mathrm{U}(V)$ folgt $\sigma(t)/t \in K^{\times}$, und wegen $\mathrm{U}(V)' = \mathrm{SU}(V)$ (*Theorem* 10.9, 4.4 und die Beweise zu *Theorem* 10.15 und 10.20 in TAYLOR [52]) ist t invariant unter $\mathrm{SU}(V)$.

Wegen $|Z| = q + 1$ gilt $\deg(t) = \frac{q^{n-1}(q^n-(-1)^n)}{q+1}$, und wir erhalten die Gradabschätzung

$$\frac{\prod_{i=1}^{n-1} \deg(s_i) \cdot \deg(t)}{|\mathrm{SU}(V)|} = \frac{\prod_{i=1}^{n-1}(q^{2i-1}+1)}{q^{\frac{(n-1)(n-2)}{2}} \cdot \prod_{i=1}^{n-1}(q^i - (-1)^i)}.$$

Für $n = 2m$ ist dies

$$\frac{\prod_{i=m+1}^{2m-1}(q^{2i-1}+1)}{q^{(n-1)(m-1)} \cdot \prod_{i=1}^{m-1}(q^{2i}-1)} \le \frac{\prod_{i=m}^{2m-2}(q^{2i}+1)}{q^{2(m-1)^2} \cdot \prod_{i=1}^{m-1}(q^{2i}-1)} < 2,$$

und für $n = 2m+1$

$$\frac{\prod_{i=m+1}^{2m}(q^{2i-1}+1)}{q^{m(n-2)} \cdot \prod_{i=1}^{m}(q^{2i}-1)} \le \frac{\prod_{i=m}^{2m-1}(q^{2i}+1)}{q^{2m(m-1)} \cdot \prod_{i=1}^{m}(q^{2i}-1)} < 2,$$

jeweils nach Lemma 3.13.

Es fehlt jetzt nur noch der Nachweis, daß die Jacobi-Determinante $\mathcal{J}$ von $(s_1, \ldots, s_{n-1}, t)$ nicht verschwindet. Dieser verläuft ganz analog zum entsprechenden Nachweis bei

[3] Hier liegt in [11] ein Druckfehler vor.

Satz 3.14. Wir haben hier $t = x_1 \cdot g$ mit $x_1 \nmid g$, die spezialisierte Jacobi-Determinante ergibt sich also zu

$$\mathcal{J}\,|_{x_1=0} = \begin{vmatrix} 0 & x_2^q & \cdots & x_n^q \\ 0 & x_2^{q^3} & \cdots & x_n^{q^3} \\ \vdots & \vdots & & \vdots \\ 0 & x_2^{q^{2n-3}} & \cdots & x_n^{q^{2n-3}} \\ g\,|_{x_1=0} & 0 & \cdots & 0 \end{vmatrix} \neq 0.$$

Es gilt also tatsächlich $K(V)^{\mathrm{SU}(V)} = K(s_1, \ldots, s_{n-1}, t)$, und mit derselben Gradabschätzung wie oben folgt auch $K(V)^{\mathrm{U}(V)} = K(s_1, \ldots, s_{n-1}, t^{q+1})$.

Für $n = 2$ haben s_1 und t nur den Nullvektor als gemeinsame Nullstelle in $\bar{K}^2$: Jede gemeinsame Nullstelle (ξ_1, ξ_2) läßt sich nämlich mit einem $\sigma \in \mathrm{U}(V)$ so transformieren, daß $\xi_1 = 0$ gilt, also auch $\xi_2^{q+1} = s_1(\xi_1, \xi_2) = 0$. Nun folgt wie im Beweis zu Satz 3.14(c), daß $K[V]^{\mathrm{SU}(V)} = K[s_1, t]$ und $K[V]^{\mathrm{U}(V)} = K[s_1, t^{q+1}]$. □

3.4 Treue Faktormoduln

In diesem Abschnitt, der im Grunde einen Anhang zu den vorherigen darstellt, geht es um den Zusammenhang zwischen dem Noetherschen Problem für $K(V)^G$ und $K(W)^G$, wobei W ein epimorphes Bild des KG-Moduls V ist, auf dem G treu operiert. Im Falle $\mathrm{char}(K) \nmid |G|$ ist ein solches W nach dem Satz von Maschke isomorph zu einem direkten Summanden von V. Der oben genannte Zusammenhang wird als Anwendung dann positive Antworten auf das *klassische* Noethersche Problem für die Gruppen A_5 und $\mathrm{PSL}_2(7)$ liefern, allerdings nicht über $K = \mathbb{Q}$. Siehe dazu auch Kemper [26].

Proposition 3.17. *Sei L ein Körper, $G \leq \mathrm{Aut}(L)$ endlich und $K \leq L^G$ ein G-invarianter Unterkörper. Ist dann V ein endlich dimensionaler K-Vektorraum mit einer linearen G-Operation, $V_L = L \otimes_K V$, so sind die Körper $L(V_L)^G$ und $L(V_L)_0^G$ (mit der Bezeichnung aus Abschnitt 3.1.1) rein transzendent über L^G.*

Beweis. Nach Lenstra [33, Prop. 1.3] enthält $L(V_L)^G$ eine L-Basis $x_1, \ldots, x_n$ von V_L^*, also $L(V_L) = L(x_1, \ldots, x_n)$ und $L(V_L)^G = L^G(x_1, \ldots, x_n)$, $L(V_L)_0^G = L^G(x_2/x_1, \ldots, x_n/x_1)$. □

Ist beispielsweise W ein treuer KG-Modul und V wie in Proposition 3.17, so folgt, daß $K(V \oplus W)^G$ rein transzendent über $K(W)^G$ ist. Die folgende Proposition ist also im Falle $\mathrm{char}(K) \nmid |G|$ eine Folge von Proposition 3.17.

Proposition 3.18 (Miyata [38]). *Sei V ein endlich dimensionaler K-Vektorraum, $G \leq \mathrm{GL}(V)$ endlich und $\pi\colon V \twoheadrightarrow W$ ein Epimorphismus von KG-Moduln, wobei G treu auf W operiere. Dann ist $K(V)^G$ eine rein transzendente Erweiterung von $K(W)^G$, wobei die Inklusion durch $\pi^*\colon K(W) \hookrightarrow K(V)$ gegeben ist.*

Der Unterschied zu Miyata [38, Remark 3] rührt daher, daß bei Miyata $K(V) = \mathrm{Quot}(S(V))$, während in dieser Arbeit $K(V) = \mathrm{Quot}(S(V^*))$ (siehe Abschnitt 1.1). Epimorphismen von V auf W entsprechen aber genau Monomorphismen $W^* \hookrightarrow V^*$.

Beispiel 3.19 (Diedergruppen). Es sei $G = D_n$ die Diedergruppe der Ordnung $2n$, und wir setzen $\mathrm{char}(K) \nmid 2n$ und $\zeta_n + \zeta_n^{-1} \in K$ mit einer primitiven n-ten Einheitswurzel ζ_n voraus. Mit den Erzeugern σ und τ aus Beispiel 2.5 erhalten wir eine treue Permutationsdarstellung vom Grad n auf den Nebenklassen nach $H = \langle\tau\rangle$. Ist χ_2 der Charakter der zweidimensionalen linearen Darstellung $G \to \mathrm{GL}(W)$ von G aus Beispiel 2.5, so folgt $\sum_{\rho\in H} \chi(\rho) = 2$, also ist χ_2 nach Frobeniusreziprozität in der Permutationsdarstellung enthalten.

Nach Beispiel 2.5 ist jedoch $K(W)^G$ rein transzendent über K, also liefert Proposition 3.18 auch eine positive Antwort auf das Noethersche Problem für die Permutationsdarstellung. ◁

Maedas Idee.

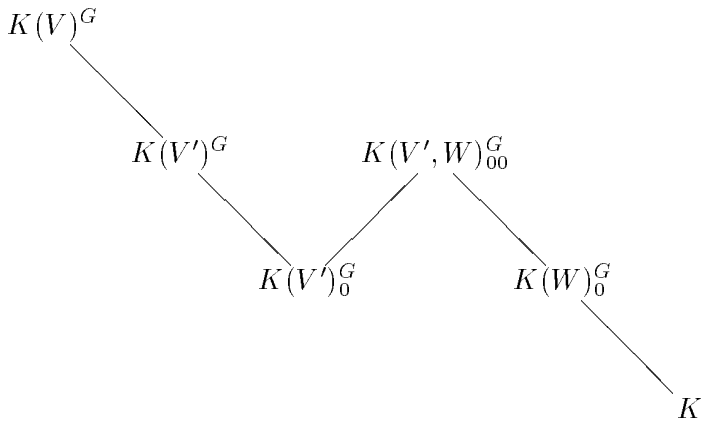
Nach einer Idee von Maeda lassen sich nun die Propositionen 3.17 und 3.18 mit Hilfe einer „Ziehharmonikatechnik“ auch dann anwenden, wenn kein direkter Zusammenhang zwischen V und W besteht ([34]). Dies ist der Inhalt des folgenden Satzes.

Satz 3.20. *Es sei K ein Körper, G eine endliche Gruppe, V ein endlich erzeugter KG-Modul und $V \twoheadrightarrow V'$ ein Epimorphismus von KG-Moduln, so daß die Operation von G auf V' treu sei. W sei ein weiterer treuer KG-Modul mit*

$$\dim_K(W) \le \dim_K(V) - \dim_K(V') + 2. \tag{3.9}$$

Ist dann $K(W)_0^G$ rein transzendent über K, so auch $K(V)^G$.

Beweis. Der Körper $L(V'_L)_0$ mit $L = K(W)_0$ werde mit $K(V', W)_{00}$ bezeichnet. Es ist klar, daß diese Bildung symmetrisch in V' und W ist. Nach den Propositionen 3.1(a), 3.17 und 3.18 und wegen der Voraussetzung sind sämtliche Erweiterungen in folgendem Diagramm rein transzendent.

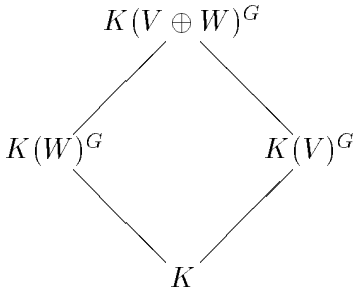


Für die Transzendenzgrade gilt

$$\begin{aligned} \deg_{tr}\left(K(V)^G / K(V')_0^G\right) &= \dim_K(V) - (\dim_K(V') - 1) \ge \\ &\ge \dim_K(W) - 1 = \deg_{tr}\left(K(V', W)_{00}^G / K(V')_0^G\right). \end{aligned}$$

Man kann daher die algebraisch unabhängigen Erzeuger von $K(V',W)_{00}^G$ über $K(V')_0^G$ auf solche von $K(V)$ über $K(V')_0^G$ abbilden und erhält so einen K-Isomorphismus zwischen $K(V',W)_{00}^G$ und einem Körper, über dem $K(V)^G$ rein transzendent ist. Nun folgt die Behauptung. □

Anmerkung. Eine Körpererweiterung L/K heißt **stabil rational**, falls es eine rein transzendente Erweiterung N von L gibt, so daß N/K rein transzendent ist. Rein transzendente Erweiterungen sind demnach stabil rational. Lange Zeit war es unklar, ob auch die umgekehrte Inklusion gilt. Wäre dies der Fall, so könnte man in Satz 3.20 die Bedingung (3.9) weglassen, und es würde aus dem Diagramm



folgen, daß eine positive Antwort auf das Noethersche Problem für *eine* treue lineare Darstellung eine solche für *sämtliche* treue lineare Darstellungen impliziert. Einer Bemerkung in BOGOMOLOV und KATSYLO [5] ist jedoch zu entnehmen, daß für diese umgekehrte Implikation inzwischen Gegenbeispiele gefunden wurden. ◁

Beispiel 3.21 (A_5 und $\mathrm{PSL}_2(7)$). Es sei G eine der Gruppen A_5 oder $\mathrm{PSL}_2(7)$ und K ein Körper mit

$$\begin{aligned} \mathrm{char}(K) \neq 2,3,5 \text{ und } 5 \in (K^\times)^2 \quad &\text{im Falle} \quad G = A_5, \\ \mathrm{char}(K) \neq 2,3,7 \text{ und } -7 \in (K^\times)^2 \quad &\text{im Falle} \quad G = \mathrm{PSL}_2(7). \end{aligned}$$

Dann hat das Noethersche Problem für jede treue Permutationsdarstellung von G eine positive Antwort. Es sei nämlich V der K-Vektorraum, auf dem G durch Vertauschungen der Basisvektoren $e_1,\ldots,e_n$ operiert. Dann hat der durch $e_1+\cdots+e_n$ aufgespannte Unterraum ein G-Komplement V', welches als direkter Summand ein epimorphes Bild von V ist. Außerdem ist $\dim_K(V) - \dim_K(V') = 1$, und G operiert treu auf V'. Für die dreidimensionale Darstellungen $G \to \mathrm{GL}(W)$ aus Beispiel 3.5 ist also die Dimensionsbedingung (3.9) erfüllt. Nach Beispiel 3.5 ist $K(W)_0^G$ rein transzendent über K, und Satz 3.20 liefert nun die Behauptung. ◁

A Zusammenfassung der Ergebnisse

Um dem Leser einen einfachen Überblick über die in dieser Arbeit verstreuten Anwendungen zu ermöglichen, geben wir eine tabellarische Übersicht über die Gruppen, für die hier Minimalbasen und/oder generische Polynome gefunden wurden.

Gruppe G	Grundkörper K	Darstellung	generisches Polynom berechnet?	Referenz
S_n, $n \geq 3$	$\mathrm{char}(K) \nmid n$	linear vom Grad $n-1$†	ja, $n-2$ Parameter	Abschnitt 1.4.1
G abelsch vom Exponenten m	$\mathrm{char}(K) \nmid m$, $\zeta_m \in K$	linear†	ja	Abschnitt 1.4.2
Z_3	$\mathrm{char}(K) \neq 2,3$	Permutationsdarstellung	ja, 1 Parameter, Grad 3	Seidelmann [44], Abschnitt 2.4.1
V_4, D_4	$\mathrm{char}(K) \neq 2$	linear vom Grad 2†	ja, 2 Parameter, Grad 4	Beispiel 2.5
Z_4	$\mathrm{char}(K) \neq 2$	linear vom Grad 2	ja, 2 Parameter, Grad 4	Abschnitt 3.2.1
A_4	$\mathrm{char}(K) \neq 2,3$	Permutationsdarstellung	nein	Noether [41], Abschnitt 3.2.3
D_5	$K = \mathbb{Q}$	"	nein	Breuer [8, 9], Abschnitt 3.2.2
Q_{4n}	$\mathrm{char}(K) \nmid 2n$, $\zeta_{2n} + \zeta_{2n}^{-1}$, $i^n \in K$	linear vom Grad 4	für eine zweidimensionale Darstellung	Abschnitt 3.2.4, Gröbner [22]
$\mathrm{SL}_2(3)$	$\mathrm{char}(K) \neq 2,3$, $\sqrt{-3} \in K$	linear vom Grad 2†	ja, 2 Parameter, Grad 8	Beispiel 2.6
A_5*	beliebig	Permutationsdarstellung	nein	Maeda [34]
"	$\mathrm{char}(K) \neq 2,3,5$, $\sqrt{5} \in K$	linear vom Grad 3	ja, 2 Parameter, Grad 12	Beispiel 3.5
$\mathrm{PSL}_2(7)$*	$\mathrm{char}(K) \neq 2,3,7$, $\sqrt{-7} \in K$	"	nein, 2 Parameter, Grad 42	"
"	"	Permutationsdarstellung	nein	Beispiel 3.21

Tabelle 1. *Anwendungen in nicht singulärer Charakteristik*

*Die Gruppe ist einfach
†Spiegelungsdarstellung

Gruppe G	Grundkörper K	Darstellung	generisches Polynom berechnet?	Referenz
p-Gruppe	$\mathbb{F}_p$	beliebig	nein	Miyata [38]
$G = Z_p \rtimes Z_m$ metazyklisch	$\mathbb{F}_p$	linear vom Grad 2†	ja, 2 Parameter, Grad p	Saltman [42], Abschnitt 1.4.3
$\mathrm{GL}_n(q)$ und $\mathrm{SL}_n(q)$	$\mathbb{F}_q$	natürliche Darstellung†	ja, n Parameter, Grad $q^n - 1$	Wilkerson [55], Abschnitt 3.3.1
$\mathrm{Sp}_{2n}(q)$	"	natürliche Darstellung	nein, $2n$ Parameter, Grad $q^{2n} - 1$	Carlisle und Kropholler, siehe [3]
$\mathrm{CSp}_{2n}(q)$	"	"	nein	Abschnitt 3.3.2
$\mathrm{O}_n(q)$, q ungerade	"	"	"	Carlisle und Kropholler [11]
$\Omega_n(q)$*, q und n ungerade	"	"	nur für $n = 3$, $q \leq 7$	Satz 3.14
$\mathrm{O}_3(q)$ und eine Untergruppe	"	natürliche Darstellung†	nein	"
Einige weitere Untergruppen der $\mathrm{O}_n(q)$	"	natürliche Darstellung	"	"
$\mathrm{U}_n(q^2)$	$\mathbb{F}_{q^2}$	"	"	Carlisle und Kropholler [11]
$\mathrm{SU}_n(q^2)$, $(n,q) \neq (2,2), (2,3), (3,2)$	"	"	"	Satz 3.16
A_5*	$\mathbb{F}_5$	$A_5 \cong \Omega_3(5)$	ja, 2 Parameter, Grad 12	Korollar 3.15
$\mathrm{PSL}_2(7)$*	$\mathbb{F}_2$	$\mathrm{PSL}_2(7) \cong \mathrm{GL}_3(2)$	ja, 2 Parameter, Grad 7	Abschnitt 3.3.1
"	$\mathbb{F}_7$	$\mathrm{PSL}_2(7) \cong \Omega_3(7)$	ja, 2 Parameter, Grad 24	Korollar 3.15

Tabelle 2. *Modulare Anwendungen*

*Die Gruppe ist einfach

†Der Invariantenring ist ein Polynomring

Literatur

[1] S. S. Abhyankar, *Mathieu Group Coverings and Linear Group Coverings*, erscheint in: Proc. of the AMS Conference on Recent Developments in the Inverse Galois Problem, Seattle, Juli 1993

[2] M. Benard, *Schur Indices and Splitting Fields of the Unitary Reflection Groups*, J. of Algebra **38** (1976), 318–342

[3] D. J. Benson, *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lecture Note Ser. **190**, Cambridge Univ. Press 1993

[4] M.-J. Bertin, *Anneaux d'invariants d'anneaux de polynômes, en caractéristique p*, C. R. Acad. Sci. Paris **264** (Série A) (1967), 653–656

[5] F. A. Bogomolov, P. I. Katsylo, *Rationality of Some Quotient Varieties*, Math. USSR, Sb. **54** (1986), 571–576

[6] N. Bourbaki, *Groupes et algèbres de Lie, Chap. IV, V, VI*, Hermann, Paris 1968

[7] S. Breuer, *Zyklische Gleichungen 6. Grades und Minimalbasis*, Math. Ann. **86** (1922), 108–113

[8] S. Breuer, *Zur Bestimmung der metazyklischen Minimalbasis von Primzahlgrad*, Math. Ann. **92** (1924), 126–144

[9] S. Breuer, *Metazyklische Minimalbasis und komplexe Primzahlen*, J. Reine Angew. Math. **156** (1927), 13–42

[10] G. Butler, K. McKay, *The Transitive Groups of Degree up to Eleven*, Comm. in Algebra **11(8)** (1983), 863–911

[11] D. Carlisle, P. H. Kropholler, *Rational Invariants of Certain Orthogonal and Unitary Groups*, Bull. London Math. Soc. **24** (1992), 57–60

[12] B. Char, K. Geddes, G. Gonnet, M. Monagan and S. Watt, *Maple Reference Manual (5th Edn.)*, Waterloo Maple Publishing, Waterloo, Ontario 1990

[13] A. Charnow, *On the Fixed Field of a Linear Abelian Group*, J. London Math. Soc. (2) **1** (1969), 348–350

[14] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of Finite Groups*, Clarendon Press, Oxford 1985

[15] C. W. Curtis, I. Reiner, *Methods of Representation Theory*, Vol. I, Wiley & Sons, New York 1981

[16] F. DeMeyer, E. Ingraham, *Separable Algebras Over Commutative Rings*, Springer-Verlag, Berlin, Heidelberg, New York 1971

[17] L. E. Dickson, *A Fundamental System of Invariants of the General Modular Linear Group with a Solution of the Form Problem*, Trans. Amer. Math. Soc. **12** (1911), 75–98

[18] E. Fischer, *Die Isomorphie der Invariantenkörper der endlichen Abelschen Gruppen linearer Transformationen*, Nachr. Königl. Ges. Wiss. Göttigen (1915), 77–80

[19] M. D. Fried, M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, Heidelberg 1986

[20] W. Fulton, *Algebraic Curves*, Benjamin, New York 1969

[21] W. Fulton, *Intersection Theory*, Springer-Verlag, Berlin, Heidelberg 1984

[22] W. Gröbner, *Minimalbasis der Quaternionengruppe*, Monatshefte f. Math. und Physik **41** (1934), 78–84

[23] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, Berlin, Heidelberg, New York 1967

[24] N. Jacobson, *Basic Algebra I*, Freeman, New York 1985

[25] R. M. Kane, *The Homology of Hopf Spaces*, Elsevier Science Publishers B.V., Amsterdam 1988

[26] G. Kemper, *Das Noethersche Problem für* $L_2(7)$, IWR Preprint **93-26**, Heidelberg 1993

[27] G. Kemper, *The* Invar *Package for Calculating Rings of Invariants*, IWR Preprint **93-34**, Heidelberg 1993

[28] G. Kemper, *An Algorithm to Determine Properties of Field Extensions Lying over a Ground Field*, IWR Preprint **93-58**, Heidelberg 1993

[29] G. R. Kempf, *Computing Invariants*, in: S. S. Koh (Ed.), *Invariant Theory*, Springer-Verlag, Berlin, Heidelberg 1987

[30] M. Kervaire, T. Vust, *Fractions rationelles invariantes par un groupe fini: quelques exemples*, in: H. Kraft et al. (Eds.), *Algebraische Transformationsgruppen und Invariantentheorie*, DMV Seminar **13**, Birkhäuser, Basel 1989

[31] W. Kuyk, *On a Theorem of E. Noether*, Nederl. Akad. Wetensch. Proc. Ser. A **67** (1964), 32–39

[32] S. Lang, *Algebra*, Addison-Wesley, Reading, Massachusetts 1965

[33] H. W. Lenstra, *Rational Functions Invariant under a Finite Abelian Group*, Invent. Math. **25** (1974), 299–325

[34] T. Maeda, *Noether's Problem for* A_5, J. of Algebra **125** (1989), 418-430

[35] K. Masuda, *On a Problem of Chevalley*, Nagoya Math. J. **8** (1955), 59–63

[36] B. H. Matzat, *Konstruktive Galoistheorie*, Springer-Verlag, Berlin, Heidelberg 1987

[37] J. M. McShane, L. C. Grove, *Polynomial Invariants of Finite Groups*, in: Algebras, Groups and Geometries, Vol. **10**, No. **1** (1993), 1–12

[38] T. Miyata, *Invariants of Certain Groups I*, Nagoya Math. J. **41** (1971), 69–73

[39] H. Nakajima, *Invariants of Finite Groups Generated by Pseudo-Reflections in Positive Characteristic*, Tsukuba J. Math. **3** (1979), 109–122

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

[41] E. Noether, *Gleichungen mit vorgeschriebener Gruppe*, Math. Ann. **78** (1918), 221–229

[42] D. J. Saltman, *Generic Galois Extensions and Problems in Field Theory*, Adv. in Math. **43** (1982), 250–283

[43] D. J. Saltman, *Noether's Problem over an Algebraically Closed Field*, Invent. Math. **77** (1984), 71–84

[44] F. Seidelmann, *Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich*, Math. Ann. **78** (1918), 230–233

[45] G. C. Shephard, J. A. Todd, *Finite Unitary Reflection Groups*, Canad. J. Math. **6** (1954), 274–304

[46] N. J. A. Sloane, *Error-Correcting Codes and Invariant Theory: New Applications of a Nineteenth-Century Technique*, Amer. Math. Monthly **84** (1977), 82–107

[47] R. P. Stanley, *Invariants of Finite Groups and their Applications to Combinatorics*, Bull. Amer. Math. Soc. **1**, no. 3 (1979), 475–511

[48] Maureen Stillman, Michael Stillman, Dave Bayer, *Macaulay User Manual*, 1989

[49] B. Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Wien, New York 1993

[50] R. Swan, *Invariant Rational Functions and a Problem of Steenrod*, Invent. Math. **7** (1969), 148–158

[51] M. Sweedler, *Using Gröbner Bases to Determine the Algebraic and Transcendental Nature of Field Extensions: Return of the Killer Tag Variables*, in: Gérard Cohen, Teo Mora, Oscar Moreno (Eds.), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer-Verlag LNCS **673** (1993), 66–75

[52] D. E. Taylor, *The Geometry of the Classical Groups*, Heldermann, Berlin 1992

[53] H. Toda, *Cohomology mod 3 of the Classifying Space BF_4 of the Exceptional Group F_4*, J. Math. Kyoto Univ. **13** (1972), 97–115

[54] B. L. van der Waerden, *Algebra I*, siebente Auflage, Springer-Verlag, Berlin, Heidelberg, New York 1966

[55] C. Wilkerson, *A Primer on the Dickson Invariants*, Amer. Math. Soc. Contemp. Math. Series **19** (1983), 421–434