Notizen zur Vorlesung
Theorie der Invarianten endlicher Gruppen
Wintersemester 2003/04

H.-G. Gräbe, Institut für Informatik,
`http://www.informatik.uni-leipzig.de/~graebe`

6. Februar 2004

1 Einführung

Viele Probleme der angewandten Mathematik haben Symmetrien oder sind invariant unter gewissen natürlichen Transformationen. So sind etwa alle *geometrischen* Größen und Eigenschaft invariant bzgl. der Auswahl eines Koordinatensystems, d.h. unter der Aktion der affinen Gruppe oder einer ihrer Untergruppen. Felix Klein benutzte in seinem *Erlanger Programm* sogar solche Invarianzeigenschaften unter Transformationsgruppen zur Klassifizierung verschiedener Arten von Geometrie und unterschied projektive, affine und Euklidsche Geometrie.

In der Physik spielen Invarianzbetrachtungen eine wesentliche Rolle für die spezielle und allgemeine Relativitätstheorie, wo relevante Eigenschaften unter entsprechenden Transformationen der Raum-Zeit-Koordinaten erhalten bleiben, also invariant unter der *Lorentzgruppe* sein sollen.

Sie sehen an diesen wenigen Beispielen zugleich, dass es sich bei solchen Invarianzuntersuchungen oftmals um Untersuchungen handelt, die einen mächtigen mathematischen Apparat erfordern. Wir wollen uns in dieser Vorlesung deshalb auf Invarianzuntersuchungen für *endliche Gruppen*, die linear auf Polynomringen operieren, beschränken.

Hierbei handelt es sich um ein klassisches Gebiet der konstruktiven Mathematik, das besonders von den Algebraikern zu Beginn des 20. Jahrhunderts im Rahmen ihrer Bemühungen um ein besseres Verständnis konstruktiver Aspekte in der Mathematik erschlossen wurde. Die Beweise der inzwischen klassischen Endlichkeitssätze ([3, 5]) über Systeme von Basisinvarianten endlicher Gruppen (in Charakteristik 0), aus denen man alle anderen gewinnen kann, geben zugleich ein Verfahren zu deren prinzipieller Berechenbarkeit, das aber nur für kleine Beispiele praktikabel ist.

Das Interesse an dieser Thematik erwachte erneut mit den wesentlich erweiterten Möglichkeiten zur symbolischen Formelmanipulation, die moderne Computeralgebrasysteme bieten. Neben die Frage der prinzipiellen Berechenbarkeit trat nun auch die nach der *effizienten* Berechnung von Basisinvarianten und der Relationen zwischen ihnen. Dabei stellte sich heraus, dass aus einem klugen Zusammenspiel verschiedener bekannter klassischer Konzepte und neuerer Verfahren, insbesondere der Gröbnerbasen, wesentliche Effizienzzuwächse möglich sind.

Die Vorlesung orientiert sich in ihrem theoretischen Teil am Buch [9]. Wir werden die wichtigsten algorithmischen Ideen jedoch auch in ihrer praktischen Wirksamkeit erproben, wozu einige Erfahrung mit einem Computeralgebrasystem von Vorteil ist. Die Beispiele werden weitgehend unter Verwendung des CAS MuPAD demonstriert.

1.1 Symmetrien und Invarianten – einführende Bemerkungen

Drei Punkte $A = (x_1, y_1), B = (x_2, y_2)$ und $C = (x_3, y_3)$ sind genau dann kollinear, wenn die Koordinaten der Bedingung

$$f_1 := det \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{pmatrix} = (x_1y_2 - x_2y_1 + x_3y_1 - y_3x_1 + x_2y_3 - x_3y_2) = 0$$

genügen. Diese Bedingung hängt nicht vom gewählten Koordinatensystem ab. Verschieben wir z.B. die Punkte um einen Vektor (u, v) zu $A' = (x_1+u, y_1+v), B' = (x_2+u, y_2+v), C' = (x_3+u, y_3+v)$, so vereinfacht die Linearitätsbedingung

$$\begin{gathered}(x_1 + u) \cdot (y_2 + v) - (x_2 + u) \cdot (y_1 + v) + (x_3 + u) \cdot (y_1 + v) - (y_3 + v) \cdot (x_1 + u) \\ + (x_2 + u) \cdot (y_3 + v) - (x_3 + u) \cdot (y_2 + v) = 0\end{gathered}$$

für diese Punkte zur selben Bedingung $f_1 = 0$. Das gilt nicht nur für Verschiebungen, sondern für beliebige affine Transformationen

$$g : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}.$$

Der Abstand zwischen A und B

$$f_2 := (x_1 - x_2)^2 + (y_1 - y_2)^2$$

ist dagegen nur unter gewissen Transformationen g invariant:

$$\begin{aligned} f_2 \circ g &= (a_{11}(x_1 - x_2) + a_{12}(y_1 - y_2))^2 + (a_{21}(x_1 - x_2) + a_{22}(y_1 - y_2))^2 \\ &= (a_{11}^2 + a_{21}^2)(x_1 - x_2)^2 + (a_{12}^2 + a_{22}^2)(y_1 - y_2))^2 + (a_{11}a_{12} + a_{21}a_{22})(x_1 - x_2)(y_1 - y_2) \\ &= f \end{aligned}$$

genau dann, wenn

$$a_{11}^2 + a_{21}^2 = a_{12}^2 + a_{22}^2 = 1 \text{ und } a_{11}a_{12} + a_{21}a_{22} = 0,$$

d.h. wenn g eine orthogonale Matrix ist.

Jedes Polynom, das eine geometrische Bedingung kodiert, muss unter solchen Transformationen invariant sein. Das Polynom

$$f_3 := x_1^2 + x_1y_1 + y_1^2 + x_2^2 + x_2y_2 + y_2^2$$

dagegen ist selbst unter Verschiebungen nicht invariant, hat also keine geometrische Bedeutung.

1.2 Die allgemeine Fragestellung

Wir werden im Folgenden keine affinen, sondern stets nur *lineare* Koordinatentransformationen betrachten. Genauer: V sei ein endlich dimensionaler Vektorraum der Dimension n über einem Körper k (der im Folgenden immer Charakteristik 0 haben soll), $e_1, \dots, e_n$ eine Basis von V und

$$v = x_1(v)\, e_1 + \ldots + x_n(v)\, e_n$$

eine Koordinatendarstellung des Vektors $v \in V$. Die Funktionen $x_i : V \to k$ sind lineare Funktionale auf V und heißen *Koordinatenfunktionen.* Im Raum aller Funktionen auf V erzeugen sie den Ring $k[V] = k[x_1, \dots, x_n]$ der polynomialen Funktionen auf V. Eine lineare Abbildung $g \in GL(V)$ induziert eine Abbildung auf den Funktionen $f \in k[V]$

$$f^g(v) := f(g^{-1}(v)),$$

die als Ringautomorphismus durch ihre Wirkung auf die Koordinatenfunktionen eindeutig bestimmt ist. Genauer: Ist $f = P(x_1, \ldots, x_n)$ die Darstellung der Funktion f als Polynom in den Koordinatenfunktionen, so gilt $f^g = P(x_1^g, \ldots, x_n^g)$. g wirkt auf den Polynomen also als lineare Variablensubstitution $x_i \mapsto x_i^g$. Da die Koordinatenfunktionen $\{x_i, i = 1, \ldots, n\}$ eine Vektorraumbasis von V^* bilden, die zur Basis $\{e_i, i = 1, \ldots, n\}$ von V dual ist (es gilt $x_i(e_j) = \delta_{ij}$), wird (in der jeweiligen Basis) die lineare Variablensubstitution durch die Matrix M_g^{-1} beschrieben, wenn die Operation von g auf V durch die Matrix M_g beschrieben wird.

Im Weiteren werden wir diese subtilen Unterscheidungen nicht weiter verfolgen, sondern polynomiale Funktionen mit den Polynomen in $x_1, \ldots, x_n$ identifizieren und die Operation von g als lineare Variablensubstitution $x_i \mapsto x_i^g$ bzw. durch die zugehörige Matrix $M_g \in GL(n, k)$ beschreiben.

Ein Polynom $f \in k[V]$ heißt *invariant* unter g, wenn $f = f^g$ gilt. Ist f unter g_1, g_2 invariant, so auch unter allen Elementen der von g_1, g_2 in $GL(V)$ erzeugten Gruppe. Wir untersuchen deshalb Invarianten ganzer Gruppen, wobei wir die Invarianz immer nur auf den Erzeugenden der Gruppe testen müssen.

Die Menge der invarianten Polynome

$$k[V]^G := \{f \in k[V] \ : \ f = f^g \text{ für alle } g \in G\}$$

bildet offensichtlich einen Ring (und genauer sogar eine homogene k-Algebra). Die homogenen Invarianten vom Grad d spannen (zusammen mit der 0) einen (endlich dimensionalen) Vektorraum $\left[k[V]^G\right]_d$ auf.

Gegenstand der Invariantentheorie ist es, die Struktur dieses Rings $k[V]^G$ für verschiedene Gruppenaktionen $G \subset GL(V)$ und Vektorräume V zu beschreiben. Konstruktive Zugänge sind bekannt für endliche Gruppen sowie Aktionen einer Reihe klassischer unendlicher Gruppen (insbesondere $GL(n, k), SL(n, k), SO(n, k), SU(n, k)$) auf Vektorräumen verschiedener Größe. In dieser Vorlesung wird es um die Beschreibung von $k[V]^G$ für Aktionen endlicher Gruppen $G \subset GL(V)$ gehen.

1.3 Ein erstes Beispiel

Betrachten wir als Beispiel die Gruppe $G \subset GL(2, \mathbb{C})$ der Drehungen der Ebene, welche das (zentrierte) Quadrat mit den Ecken $(0, 1), (1, 0), (0, -1), (-1, 0)$ in sich überführt. G ist eine zyklische Gruppe von vier Elementen, die von der Matrix (alle Rechnungen mit MuPAD)

```
M:=Dom::Matrix()([[0,1],[-1,0]]);
```

$$M_g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

erzeugt wird, welche der Transformation

$$g : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} y \\ -x \end{pmatrix}$$

entspricht.

Wir wollen alle unter g invarianten Polynome $f \in k[x, y]$ bestimmen und verwenden dazu einen Ansatz mit unbestimmten Koeffizienten für jeweils homogenes f, den wir gradweise abarbeiten, wobei wir die folgenden MuPAD-Funktionen verwenden:

```
g:=proc(u) begin subs(u, [x=y,y=-x]) end_proc;
  // g als Variablen-Substitution

computeBasis:=proc(d) local f,i,s;
begin
```

```
  f:=_plus(a[i]*x^i*y^(d-i)$i=0..d);
      // generisches Polynom vom Grad d erzeugen
  s:=solve({coeff(f-g(f),[x,y])});
      // lineares Gleichungssystem generieren und lösen
  subs(f,s[1]);
      // allgemeine Lösung zusammenbauen
end_proc;
```

d	Lösung
1	0
2	$a_2(x^2+y^2)$
3	0
4	$a_4(x^4+y^4)+a_3(x^3\,y-x\,y^3)+a_2\,x^2\,y^2$
5	0
6	$a_6(x^6+y^6)+a_5(x^5\,y-x\,y^5)+a_4(x^4\,y^2+x^2\,y^4)$
7	0
8	$a_8(x^8+y^8)+a_7(x^7\,y-x\,y^7)+a_6(x^6\,y^2+x^2\,y^6)+a_5(x^5\,y^3-x^3\,y^5)+a_4\,x^4\,y^4$

Als k-Vektorraumbasis der Invarianten erhalten wir daraus

d	Basis der Invarianten
2	$f_2=x^2+y^2$
4	$f_{4a}=x^4+y^4,\ f_{4b}=xy(x^2-y^2),\ f_{4c}=x^2y^2$
6	$f_{6a}=x^6+y^6,\ f_{6b}=xy(x^4-y^4),\ f_{6c}=x^2y^2(x^2+y^2)$
8	$f_{8a}=x^8+y^8,\ f_{8b}=xy(x^6-y^6),\ f_{8c}=x^2y^2(x^4+y^4),$ $f_{8d}=x^3y^3(x^2-y^2),\ f_{8e}=x^4y^4$

Halten wir zunächst fest, dass dieses Vorgehen allgemein angewandt werden kann.

Verfahren zur Berechnung einer Basis der Invarianten vom Grad d

(1) Erzeuge ein Polynom f vom Grad d in $x_1,\dots,x_n$ mit unbestimmten Koeffizienten.

(2) Berechne $f-f^{g_s}$, wobei $g_s, s=1,\dots,r$, ein Erzeugendensystem der Gruppe G durchläuft.

(3) Koeffizientenvergleich liefert daraus ein (homogens) lineares Gleichungssystem in den unbestimmten Koeffizienten.

(4) Eine Basis des Lösungsraums dieses Gleichungssystems bestimmt eine Basis von $\left[k[V]^G\right]_d$.

Zur Komplexität dieses Verfahrens

Nehmen wir an, dass Rechnungen in k in konstanter Zeit möglich sind, dann kann das lineare Gleichungssystem in $O(D^3)$ Zeiteinheiten (mit dem klassischen Gaußverfahren) gelöst werden, wobei $D=\binom{d+n-1}{n-1}=O(d^{n-1})$ die Anzahl der Monome vom Grad d in n Variablen (und damit die Zahl der unbestimmten Koeffizienten von f) angibt.

Im Schritt (2) ist f^g für eine vorgegebene Variablensubstitution $g: x_i \mapsto x_i^g, i=1,\dots,n$, zu berechnen. Dazu bietet sich ein rekursives Verfahren zur Berechnung von m^g für alle $O(d\cdot D)$ Terme M vom Grad $\leq d$ an, das Zwischenergebnisse speichert und jeweils Produkte $m^g\cdot x_i^g$ (Komplexität $O(D\cdot n)$) berechnet. Der Aufwand ist insgesamt $O(n\,d\,D)$, also gering. Überdies muss diese Berechnung nur einmal pro Grad ausgeführt werden.

Der Gesamtaufwand wird unter den genannten Voraussetzungen also vom Lösen des Gleichungssystems dominiert und ist (klassisch) in der Größenordnung $O(D^3)$.

Beachtenswert ist, dass für dieses Verfahren die Gruppenelemente von G nicht alle berechnet werden müssen.

Die Algebrastruktur des Beispiels

Die berechneten Invarianten bilden eine k-Vektorraumbasis von $R = k[V]^G$. Zwischen ihnen existieren also keine linearen Relationen mehr. Allerdings kann man durch Multiplikation aus homogenen Invarianten neue herleiten. So gilt in obigem Beispiel etwa $f_2^2 = f_{4a} + 2f_{4c} \in R_4$, so dass von den Invarianten vom Grad 4 nur zwei „wirklich" neu ist, f_{4a} dagegen durch f_2^2 ersetzt werden kann. Im Grad 6 gilt

$$f_2^3 = f_{6a} + 3f_{6c},\ f_2\, f_{4b} = f_{6b},\ f_2\, f_{4c} = f_{6c},$$

so dass alle berechneten Invarianten bereits aus Invarianten kleineren Grads zusammengesetzt werden können. Im Grad 8 schließlich gilt

$$\begin{array}{lll} f_2^4 = f_{8a} + 4f_{8c} + 6f_{8e}, & f_2^2\, f_{4b} = f_{8b} + f_{8d}, & f_2^2\, f_{4c} = f_{8c} + 2f_{8e}, \\ f_{4b}^2 = f_{8c} - 2f_{8e}, & f_{4b}\, f_{4c} = f_{8d}, & f_{4c}^2 = f_{8e}. \end{array}$$

Es gibt also 6 Produkte aus Basiselementen kleineren Grades, die Invarianten vom Grad 8 liefern, aber $dim_k([R]_8) = 5$. Folglich muss zwischen diesen 6 Produkten eine lineare Abhängigkeitsrelation bestehen, die wir wieder mit einem Ansatz mit unbestimmten Koeffizenten herausfinden können:

```
p:=[f2^4,f2^2*f4b, f2^2*f4c, f4b^2,f4c^2,f4b*f4c];
r:=_plus(a[i]*f[i]$i=1..6);
sol:=solve({coeff(subs(r,[f[i]=p[i]$i=1..6]),[x,y])});
subs(r,sol[1],a[5]=4);
                        f[4] - f[3] + 4 f[5]
```

Es gilt also

$$f_{4b}^2 = f_2^2\, f_{4c} - 4\, f_{4c}^2.$$

Auch im Grad 8 gibt es also keine „neuen" Invarianten, so dass wir vermuten, dass

$$R = k[f_2, f_{4b}, f_{4c}]$$

als k-Algebra gilt. Allerdings sind die drei Erzeugenden nicht algebraisch unabhängig, sondern zwischen ihnen besteht eine polynomiale Relation, so dass der Invariantenring isomorph zum Koordinatenring einer (quasihomogenen) Raumfläche

$$R = k[V]^G \simeq R' = k[A, B, C]/(B^2 + 4C^2 - A^2C) \text{ mit } A \mapsto f_2, B \mapsto f_{4b}, C \mapsto f_{4c}$$

ist. Dass dies bereits der volle Invariantenring ist, sieht man durch einen Vergleich der Dimensionen im Grad d, wobei $deg\, A = 2$ und $deg\, B = deg\, C = 4$ gesetzt wird: $[R']_{2d}$ hat die Terme $A^{d-2i}C^i, d \geq 2i$, und $A^{d-2i-1}B\, C^i, d > 2i$, als Vektorraumbasis.

> Aufgabe : Zeigen Sie, dass es unter der angegebenen Aktion keine Invarianten ungeraden Grades gibt.
>
> Finden Sie eine 1-1-Korrespondenz zwischen obiger Basis von $[R']_{2d}$ und einer Vektorraumbasis von $[R]_{2d}$.

Die Invarianten f_2, f_{4b} und f_{4c} erzeugen also $R = k[V]^G$ als k-Algebra, weshalb man sie auch als *Basisinvarianten* bezeichnet. Die algebraisch unabhängigen Invarianten $A = f_2, C = f_{4c}$ heißen dabei *Primär-*, die davon algebraisch abhängige Invariante $B = f_{4b}$ *Sekundärinvariante*.

Jede Invariante $f \in R$ lässt sich eindeutig darstellen als $f = P_1(A, C) + b \cdot P_2(A, C)$ mit Polynomen P_1, P_2, d.h. der Invariantenring R ist ein freier $k[A, C]$-Modul mit der Basis $\{1, B\}$:

$$R = k[A, C] \oplus B \cdot k[A, C].$$

Eine solche Darstellung von R als endlicher freier Modul über einem Polynomring bezeichnet man als *Hironaka-Zerlegung*.

1.4 Die Aufgabenstellung in der Invariantentheorie

Generell steht damit folgende Liste von Aufgaben, wenn der Invariantenring $R = k[V]^G$ beschrieben werden soll:

1. Bestimme wenigstens erst einmal die Dimension $dim_k([R]_d)$ des Vektorraums der Invarianten vom Grad d für verschiedene d.

   Das ist in den meisten Fällen relativ einfach, wenn die verschiedenen Dimensionen in der *erzeugenden Funktion*
   $$H(R, t) = \sum_{d=0}^{\infty} dim_k([R]_d) \cdot t^d$$
   zusammengefasst werden. Diese Reihe bezeichnet man allgemein für homogene k-Algebren R als *Hilbertreihe* und speziell für Invariantenringe auch als *Molienreihe*.

   Der Vorteil einer solchen Zusammenfassung liegt in der Einfachheit der Darstellung der Reihe als Taylorreihe einer analytischen Funktion. So gilt etwa für den ganzen Polynomring $S = k[x_1, \ldots, x_n]$
   $$dim_k([S]_d) = \binom{n+d-1}{n-1} \text{ und } H(S, t) = \frac{1}{(1-t)^n}.$$
   Das werden wir noch beweisen.

2. Wenn man die Dimensionen kennt, sind genügend viele (linear) unabhängige Invarianten vorgegebenen Grads zu konstruieren. Ein Verfahren haben wir bereits kennen gelernt.

   Auf diese Weise kann man alle Invarianten vorgegebenen Grads beschreiben. Allerdings besteht der Invariantenring aus unendlich vielen solchen Vektorräumen.

   Eine Beschreibung nur der Vektorraumbasen würde außerdem die Algebra-Struktur des Invariantenrings nicht widerspiegeln.

3. Unter den Invarianten sind Basisinvarianten zu finden, die den Invariantenring als k-Algebra erzeugen. Insbesondere steht die Frage, ob es immer endlich viele solche Invarianten gibt und wie man merkt, dass man alle gefunden hat.

4. Kennt man Basisinvarianten, so steht die Frage nach der genaueren Algebrastruktur, d.h. der Beschreibung von Relationen zwischen diesen Invarianten und der Aufteilung in einen algebraisch unabhängigen Teil, die Primärinvarianten, und einen „Rest“, die Sekundärinvarianten.

   Dabei ist insbesondere zu entscheiden, ob das System der Basisinvarianten minimal ist.

1.5 Symmetrische Polynome

Betrachten wir als erstes komplexes Beispiel die *symmetrischen Polynome*, deren Eigenschaften sich im *Fundamentalsatz über symmetrische Polynome* zusammenfassen lassen. Der Zweck dieser Untersuchungen ist dreifacher Art. Zum ersten ergeben sich für einige fundamentale Fragen der Invariantentheorie in diesem Fall besonders einfache Lösungen. Zum zweiten spielt der Fundamentalsatz eine zentrale Rolle in vielen Aussagen allgemeineren Charakters. Und zum dritten liefert der beweis des Fundamentalsatzes zugleich einen Algorithmus, der wichtige Techniken der Computeralgebra exemplarisch anwendet.

Im folgenden sei k ein Körper. Ein Polynom $f \in S = k[x_1, \ldots, x_n]$ heißt *symmetrisch*, wenn es invariant unter allen Variablenpermutationen ist. Z.B. ist $f_1 = x_1x_2 + x_1x_3$ nicht symmetrisch, weil $f_1(x_1, x_2, x_3) \neq f_1(x_2, x_1, x_3) = x_1x_2 + x_2x_3$ gilt. Dagegen ist $f_2 = x_1x_2 + x_1x_3 + x_2x_3$ symmetrisch.

Ist $\pi \in S_n$ eine solche Permutation der Indizes, so heißt $f \in S$ invariant unter π, wenn

$$f(x_1, x_2, \dots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(n)})$$

gilt. Die Permutation induziert eine lineare Abbildung π^* auf S_1, die man in Matrixnotation unter Verwendung der Permutationsmatrix $M_\pi := ||\delta_{\pi(i),j}||$ als

$$\pi^* \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = M_\pi \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

schreiben kann. π^* lässt sich eindeutig zu einem Ringautomorphismus $S \to S$ fortsetzen.

Ist ein Polynom bzgl. einer gewissen Menge von Permutationen invariant, so auch bzgl. all jener Permutationen, die sich durch Nacheinanderausführen der gegebenen Permutationen ergeben, d.h. der von diesen Permutationen erzeugten Untergruppe der S_n. Umgekehrt genügt es, die Invarianz eines Polynoms bzgl. der Erzeugenden einer Gruppe zu testen, also im Fall der symmetrischen Polynome etwa bzgl. aller *Transpositionen*, da sich jede Permutation als Nacheinanderausführung von Transpositionen darstellen lässt.

Die symmetrischen Polynome bilden wieder eine homogene k-Algebra $R := S^{S_n}$, welche als Vektorraum die direkte Summe der endlich dimensionalen Vektorräume $[R]_d$ der homogenen symmetrischen Polynome vom Grad $d \in \mathbb{N}$ ist.

Beispiele von symmetrischen Polynomen: Potenzsummen p_d, elementarsymmetrische Summe e_d, volle symmetrische Summe h_d, monomiale Summe μ_λ für $d \vdash \lambda$.

Zahlpartitionen und Ferrersdiagramme.

Satz 1 (Dimensionssatz für symmetrische Polynome)
Für den Ring $R = S^{S_n}$ der symmetrischen Polynome gilt, dass $\dim_k([R]_d)$ gleich der Zahl der Ferrersdiagramme mit d Kästchen und $\leq n$ Spalten ist.

Beweis : Offensichtlich bilden die $\mu_\lambda, d \vdash \lambda$ ein Erzeugendensystem. Außerdem sind die Leitterme paarweise verschieden. □

Bestimmung der Dimension bis zum Grad 6 durch Abzählen der Diagramme und Aufschreiben der jeweiligen monomialen Summen.

> Aufgabe : Zeigen Sie, dass für die erzeugende Funktion von $R = S^{S_n}$
>
> $$H(R, z) = \frac{1}{(1-z)(1-z^2) \cdot \ldots \cdot (1-z^n)}$$
>
> gilt.

Implementierung in MuPAD:

```
e:=proc(d,vars) local u;
begin
  if nops(vars)<d then 0
  elif d=0 then 1
  else u:=[op(vars,2..nops(vars))];
      expand(e(d,u)+op(vars,1)*e(d-1,u))
  end_if
end_proc;
```

```
h:=proc(d,vars) local u;
begin
  if d=0 then 1
  elif nops(vars)=1 then op(vars,1)^d
  else u:=[op(vars,2..nops(vars))];
      expand(h(d,u)+op(vars,1)*h(d-1,vars))
  end_if
end_proc;

p:=proc(d,vars) begin _plus(op(map(vars,x->x^d,x))) end_proc;

mu:=proc(l,vars)
begin
  _plus(op(map(combinat::permute(vars),x->_mult(op(zip(x,l,`^`))))));
end_proc;
```

Wieviele Produkte aus den elementarsymmetrischen Polynomen gibt es von vorgegebenem Grad? Es gibt eine 1-1-Korrespondenz

$$e_1^{a_1} e_2^{a_2} \dots e_n^{a_n} \longrightarrow (b_k := \sum_{i=k}^{n} a_i, k = 1, \dots, n)$$

zwischen diesen Produkten und den Zahlpartitionen (Ferrersdiagrammen).

Kann man also jedes symmetrische Polynom als Linearkombination von solchen Produkten schreiben, d.h. als polynomiale Kombination der elementarsymmetrischen Polynome? Wie kann man für ein beliebiges Polynom eine solche Darstellung finden ?

Beispiele:

```
vars:=[x1,x2,x3];
f:=mu([3,2,1],vars);
f:=poly(f,vars);
```

Der höchste Term $x_1^3 x_2^2 x_3$ stimmt mit dem von $e_1 e_2 e_3$ überein:

```
f1:=f-poly(e(3,vars)*e(2,vars)*e(1,vars),vars);
```

Es bleibt als Rest das Polynom

$$-3x_1^2 x_2^2 x_3^2$$

Also gilt

$$\mu(3,2,1) = e_1 e_2 e_3 - 3e_3^2.$$

```
f:=mu([4,2,1],vars);
f:=poly(f,vars);
f1:=f-poly(e(3,vars)*e(2,vars)*e(1,vars)^2,vars);
f2:=f1+poly(2*e(3,vars)*e(2,vars)^2,vars);
f3:=f2+poly(e(3,vars)^2*e(1,vars),vars); // =0
```

Also gilt

$$\mu(4,2,1) = e_1^2 e_2 e_3 - 2e_2^2 e_3 - e_1 e_3^2.$$

```
f:=mu([5,3,1],vars);
f:=poly(f,vars);
```

```
f1:=f-poly(e(3,vars)*e(2,vars)^2*e(1,vars)^2,vars);
f2:=f1+poly(2*e(3,vars)^2*e(1,vars)^3,vars);
f3:=f2+poly(2*e(3,vars)*e(2,vars)^3,vars);
f4:=f3-poly(4*e(3,vars)^2*e(2,vars)*e(1,vars),vars);
f5:=f4+poly(3*e(3,vars)^3,vars); // =0
```

Also gilt
$$\mu(5,3,1) = e_1^2 e_2^2 e_3 - 2e_1^3 e_3^2 + 4e_1 e_2 e_3^2 - 3e_3^3.$$

Satz 2 (Hauptsatz über symmetrische Polynome)
Jedes symmetrische Polynom $f(x_1, \ldots, x_n) \in R = S^{S_n}$ kann eindeutig als polynomiale Linearkombination
$$f(x_1, \ldots, x_n) = P(e_1, \ldots, e_n)$$
der elementarsymmetrischen Polynome dargestellt werden, d.h. die Abbildung
$$k[y_1, \ldots, y_n] \longrightarrow S \quad via \quad y_i \mapsto e_i$$
ist ein Ringisomorphismus.
Die elementarsymmetrischen Polynome $e_1, \ldots, e_n$ bilden also ein System von (algebraisch unabhängigen) Basisinvarianten für die angegebene Gruppenaktion.

Die Darstellbarkeit beweist man wie oben, denn es gilt allgemein bzgl. der lexikografischen Termordnung für eine Partition $(a_1 \geq \ldots \geq a_n \geq 0)$
$$lt(e_1^{a_1-a_2}\, e_2^{a_2-a_3} \ldots e_{n-1}^{a_{n-1}-a_n}\, e_n^{a_n}) = x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$$
Die Eindeutigkeit folgt aus dem Vergleich der Dimensionen von $[R]_d$ und $[k[y_1, \ldots, y_n]]_d$, wenn $deg(y_i) = i$ gesetzt wird.
Details zum Beweis siehe [9].

Satz 3 *Der Ring $R = S^{S_n}$ kann ebenfalls durch die ersten n Potenzsummen $p_1, \ldots, p_n$ erzeugt werden:*
$$R \simeq k[p_1, \ldots, p_n]$$
Diese bilden also ebenfalls ein (algebraisch unabhängiges) System von Basisinvarianten.

Beispiel:

```
f:=mu([5,3,1],vars);
f:=poly(f,vars);
f1:=f-poly(p(5,vars)*p(3,vars)*p(1,vars),vars);
f2:=f1+poly(p(5,vars)*p(4,vars),vars);
f3:=f2+poly(p(6,vars)*p(3,vars),vars);
f4:=f3+poly(p(8,vars)*p(1,vars),vars);
f5:=f4-poly(2*p(9,vars),vars);
```

Also gilt
$$\mu(5,3,1) = p_1 p_3 p_5 - p_4 p_5 - p_3 p_6 - p_1 p_8 + 2p_9.$$
In dem Beispiel werden allerdings auch $p_k, k > n$, verwendet.
Beweis : Jedes homogene symmetrische Polynom kann als $f = \sum_\lambda \mu_\lambda$ dargestellt werden. Die Darstellung ergibt sich aus den Termen $x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}, \lambda = (a_1 \geq \ldots \geq a_n \geq 0)$, in der expandierten Darstellung von f.

Führe Ordnung ein, so dass die lexikographisch kleinsten Partitionen die größten μ_λ ergeben. Dann ist für $i_1 \geq \ldots \geq i_n \geq 0$ und $p_0 := 1$

$$p_{i_1} \cdot \ldots p_{i_n} = \mu_{(i_1,\ldots,i_n)} + \text{ kleinere } \mu_\lambda$$

und ein Termersetzungsverfahren führt zu einer Darstellung von f durch $p_i, i \leq deg(f)$.

Die Aussage des Satzes ergibt sich nun daraus, dass jedes symmetrische Polynom durch die elementarsymmetrischen Polynome dargestellt werden kann und diese, wie eben bewiesen, durch $p_i, i \leq n$. Details siehe [9]. $\square$

Invarianten der alternierenden Gruppe $A_n \subset S_n$.

$$D(x_1,\ldots,x_n) = \prod_{1\leq i<j\leq n} (x_i - x_j).$$

Ist unter S_n keine Invariante, sondern eine *Semiinvariante* bzgl. des Charakters $\mathrm{sgn} : S_n \to k^*$. Für $g \in S_n$ gilt

$$D^g = \mathrm{sgn}(g) \cdot D.$$

Die Menge der Semiinvarianten zu einem Charakter $\chi : G \to k^*$

$$k[V]^G_\chi := \{f \in k[V] \,:\, f^g = \chi(g) \cdot f \text{ für alle } g \in G\}$$

bilden einen $K[V]^G$-Modul.

Die Semiinvarianten der S_n bzgl. $\chi = sgn$ heißen *alternierende Polynome*.

Satz 4 *Jedes Polynom $f \in S^{A_n}$ kann eindeutig als $f = g + h\,D$ mit symmetrischen Polynomen g, h geschrieben werden.*

$\{e_1,\ldots,e_n, D\}$ ist also ein System von Basisinvarianten von S^{A_n}, wobei D eine Sekundärinvariante ist, für die $D^2 \in k[e_1,\ldots,e_n]$ gilt.

Damit ist $S^{A_n} = k[e_1,\ldots,e_n] \oplus D \cdot k[e_1,\ldots,e_n] = S^{S_n} \oplus S^{S_n}_{\mathrm{sgn}}$ eine Hironaka-Zerlegung von S^{A_n}.

Beweis siehe [9].

Sei $\lambda = (a_1 \geq a_2 \geq \ldots \geq a_n \geq 0)$ eine Partition.

$$a_\lambda = det \begin{pmatrix} x_1^{a_1+n-1} & x_1^{a_2+n-2} & \ldots & x_1^{a_n} \\ x_2^{a_1+n-1} & x_2^{a_2+n-2} & \ldots & x_2^{a_n} \\ & \ldots & & \\ x_n^{a_1+n-1} & x_n^{a_2+n-2} & \ldots & x_n^{a_n} \end{pmatrix}$$

ist ein alternierendes Polynom vom Grad $deg(a_\lambda) = |\lambda| + \frac{n(n-1)}{2}$. Die a_λ sind (nach Definition der Determinante) genau die Bilder der x^λ unter Antisymmetrisierung, also ein Erzeugendensystem von $S^{S_n}_{\mathrm{sgn}}$. Außerdem sind sie als alternierende Polynome durch D teilbar und haben somit die Gestalt $a_\lambda = s_\lambda \cdot D$. Die Polynome $s_\lambda \in S^{S_n}$ heißen *Schurpolynome* und spielen eine wichtige Rolle in der Darstellungstehorie der S_n.

Satz 5 *Die Schurpolynome $s_\lambda \in R = S^{S_n}, d \vdash \lambda$, bilden eine k-Vektorraumbasis von $[R]_d$.*

2 Grundlegende Eigenschaften des Invariantenrings

2.1 Transzendenzgrad und Primärinvarianten

Im Folgenden sei immer G eine endliche Gruppe, die auf dem Vektorraum V der Dimension n linear operiert, k ein Körper, so dass $char(k)$ kein Teiler von $|G|$ ist (nicht modularer Fall), und

$S = k[V] = k[x_1, \ldots, x_n]$ Ring der polynomialen Funktionen auf V. Eine solche Gruppenaktion bezeichnen wir im Weiteren als *regulär*.

$g \in G$ kann auf V trivial operieren, d.h. $g(v) = v$ für alle $v \in V$ oder dual $l^g = l$ für alle $l \in [S]_1$ sein. Die Operation von G auf V heißt *treu*, wenn nur das Einselement $e \in G$ trivial operiert, d.h. $Ker(G \to Aut([S]_1)) = (e)$ gilt.

Satz 6 *Für den Invariantenkörper $k(V)^G$ gilt:*

(1) $k(V)^G$ ist der Quotientenkörper von $k[V]^G$.

(2) $k(V)^G$ hat Transzendenzgrad n über k.

(3) Operiert G treu, so ist $k(V)/k(V)^G$ eine Galois-Erweiterung (d.h. normal und separabel) mit Galois-Gruppe G.

Beweis :
(1) f/h ist in $k(V)^G$, wenn $f^g/h^g = f/h$ für alle $g \in G$ gilt. Durch Erweitern mit $\prod_{g\neq 1} h^g$ erhält man die Darstellung $f/h = F/H$ mit $H = \prod_{g\in G} h^g \in R$, $F = f \cdot \prod_{g\neq 1} h^g = f/h \cdot H \in R$. Also lässt sich jede rationale Invariante als Quotient invarianter Polynome darstellen.
(2) Betrachte

$$f_i(T) := \prod_{g\in G} (T - x_i^g) = \sum_k a_{ki}(x) \cdot T^k \in S[T]$$

Die Koeffienzienten sind invariant unter $h \in G$:

$$\sum_k a_{ki}^h(x) \cdot T^k = \prod_{g\in G} (T - x_i^{gh}) = \prod_{g\in G} (T - x_i^g) = \sum_k a_{ki}(x) \cdot T^k.$$

x_i ist Nullstelle von f_i, also ganze Relation und S modulendlich über R ($x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ mit $0 \leq a_i < |G|$ ist ein Erzeugendensystem von S über R).
(3) folgt aus der Definition, da $g \in G$ auf $k(V)$ als Körperautomorphismus operiert. □

Beispiel: C_4-Aktion auf $k[x, y]$.

$$f_x(T) = (T - x)(T - y)(T + x)(T + y) = T^4 - (x^2 + y^2)T^2 + x^2y^2$$

Bemerkung: Aus dem Beweis des Satzes folgt sogar ein (allerdings nicht konstruktiver) Beweis, dass es immer endlich viele Basisinvarianten gibt:

> Aus dem Beweis folgt, dass S sogar modulendlich über der Algebra $A = k[a_{11}, \ldots, a_{mn}]$ ist. A ist als endliche Erweiterung von k noethersch, also der A-Untermodul R des endlich erzeugten A-Moduls S ebenfalls endlich erzeugt als A-Modul. Diese Erzeugenden zusammen mit den a_{ij} bilden ein System von Basisinvarianten. Dieser Beweis ist auch im modularen Fall gültig.

Eine maximale algebraisch unabhängige Teilmenge $F \subset R$ aus homogenen Polynomen bezeichnet man als *System von Primärinvarianten.*

Korollar 1 (Charakterisierungssatz für Primärinvarianten)
Jedes System von Primärinvarianten von R hat genau n Elemente.
Die Menge homogener Polynome $F = \{f_1, \ldots, f_n\} \subset R$ ist ein System von Primärinvarianten, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:

(1) $\{f_1, \ldots, f_n\}$ sind algebraisch unabhängig.

(2) $\{x_1, \ldots, x_n\}$ sind algebraisch abhängig von $\{f_1, \ldots, f_n\}$.

(3) $\{f_1, \ldots, f_n\}$ *haben* $0 \in \mathbb{A}^n$ *als einzige gemeinsame Nullstelle über* $\overline{k}$.

(4) Der Faktorring $S/Id(f_1, \ldots, f_n)$ *hat die Krulldimension 0.*

Ein System von Primärinvarianten ist nicht eindeutig bestimmt, nicht einmal seine Grade: Mit $\{f_1, \ldots, f_n\}$ ist auch $\{f_1^{a_1}, \ldots, f_n^{a_n}\}$ ein System von Primärinvarianten.

Satz 7 (Algorithmus von Dade zur Berechnung von Primärinvarianten)
Seien $l_1, \ldots, l_n \in [S]_1$ *Linearformen mit der Eigenschaft, dass* l_i *in keiner der linearen Hüllen* $k\langle l_1^{g_1}, \ldots, l_{i-1}^{g_{i-1}}\rangle$, $g_1, \ldots, g_{i-1} \in G$, *liegt, so ist*

$$\left\{ f_i := \prod_{g \in G} l_i^g, i = 1, \ldots, n \right\}$$

ein System von Primärinvarianten.

Ist k genügend groß, so finden sich immer solche l_i, da sie nur endlich viele echte Teilräume meiden müssen.

Beweis : Sei $a \in \mathbb{A}^n$ eine gemeinsame Nullstelle der f_i. Dann gibt es $g_i \in G, i = 1, \ldots, n$, so dass $l_i^{g_i}(a) = 0$. Nach Konstruktion ist aber $dim_k(k\langle l_1^{g_1}, \ldots, l_n^{g_n}\rangle) = n$. Das lineare Gl.-S. $\{l_i^{g_i} i = 1, \ldots, n\}$ hat also nur die triviale Lösung. □

Beispiel: C_4-Aktion auf $k[x,y]$. Nimm $l_1 = x$. Dann ist $f_1 = x^2y^2$ und die zu meidenden Teilräume sind $k\langle x\rangle, k\langle y\rangle$. Also kann nicht $l_2 = y$ genommen werden. Aber $l_2 = x + y$ geht, was $f_2 = (x+y)^2(x-y)^2 = x^4 + y^4 - 2x^2y^2$ ergibt. Ist ein System von Primärinvarianten, aber nicht das vom Grad her kleinste.

2.2 Der Reynolds-Operator

$$\rho : S = k[V] \longrightarrow R = k[V]^G \text{ via } \rho(f) = \frac{1}{|G|} \sum_{g \in G} f^g$$

Satz 8 (Eigenschaften des Reynold-Operators)
Der Reynoldoperator ist ein R-linearer Projektionsoperator, d.h.

1. ρ *ist* k*-linear,*
2. $\rho^2 = \rho$, *d.h.* $\rho(I) = I$ *für* $I \in R$,
3. $\rho(f \cdot I) = I \cdot \rho(f)$ *für* $f \in S, I \in R$.

Insbesondere ist, wie bei jedem Projektionsoperator, ρ surjektiv und $[S]_d = \rho([S]_d) \oplus (1-\rho)([S]_d)$ eine Zerlegung des Vektorraums der Polynome vom Grad d in die direkte Summe aus dem invarianten Teil und einem dazu „orthogonalen“ Komplement. Aus 3. folgt, dass $(1-\rho)(S)$ sogar ein R-Modul ist.

Ein Erzeugendensystem von $[R]_d$ findet man also, indem der Reynoldsoperator auf die Elemente einer k-Basis von $[S]_d$ angewendet wird.

Ist G in SubRules-Darstellung gegeben, so kann der Reynolds-Operator wie folgt implementiert werden:

```
Reynolds:=proc(f,G) local x;
begin
  _plus(op(map([op(G)],x->subs(f,x))))/nops(G);
end_proc;
```

Beispiel: Noch einmal die C_4-Aktion auf $k[x,y]$.

```
M:=Dom::Matrix()([[0,1],[-1,0]]);
G:=map([M^0,M,M^2,M^3],matrix2subrules,[x,y])

Invarianten:=d->{Reynolds(x^i*y^(d-i),G)$i=0..d};

Invarianten(d)$d=1..8;
```

2.3 Der Endlichkeitssatz – Hilberts Beweis

Satz 9 (Hilberts Endlichkeitssatz)
Der Invariantenring $R = k[V]^G$ einer endlichen Matrixgruppe $G \subset GL(V)$ ist als k-Algebra endlich erzeugt, d.h. es existiert immer ein endliches System von Basisinvarianten.

Beweis : Sei $I \subset S = k[V]$ das Ideal, das von allen homogenen Invarianten mit positivem Grad erzeugt wird (etwa von den Invarianten $\rho(m)$, wobei m alle Terme $m \neq 1$ aus S durchläuft). Nach Hilberts Basissatz (VL Gröbnerbasen und Anwendungen) ist jedes solche Ideal endlich erzeugt und man kann sogar aus einem Erzeugendensystem des Ideals ein endliches Erzeugendensystem auswählen.

Seien also $f_1, \ldots, f_N \in R$ homogene Invarianten, die I als S-Ideal erzeugen. Wir zeigen, dass diese Invarianten bereits R als k-Algebra erzeugen.

Indirekter Beweis. Sei $R_0 = k[f_1, \ldots, f_N]$ und $f \in R \setminus R_0$ eine homogene Invariante kleinsten Grades. Wegen $f \in I$ existiert eine Darstellung $f = \sum_i r_i\, f_i$ mit $r_i \in S$. Wenden wir auf diese Darstellung den Reynolds-Operator an, so erhalten wir

$$\rho(f) = f = \sum_i \rho(r_i) f_i$$

mit Invarianten $\rho(r_i) \in R$ von kleinerem Grad als f. Folglich gilt $\rho(r_i) \in R_0$ und damit auch $f = \sum_i \rho(r_i) f_i \in R_0$. $\square$

Insbesondere erzeugen homogene invariante Elemente, die I als Ideal erzeugen, R als Algebra.

Der Beweis lässt sich auf unendliche Gruppen verallgemeinern, für welche ein Reynoldsoperator mit den oben zusammengestellten Eigenschaften definiert werden kann. Das ist z.B. für lineare reduktive Gruppen möglich, wo die Mittelung über alle Gruppenelemente durch ein Integral über das Haar-Maß der Gruppe erreicht werden kann.

2.4 Emmy Noethers Gradschranke

Satz 10 (Emmy Noethers Gradschranke)
Der Invariantenring $R = k[V]^G$ der endlichen Gruppe G hat ein System von homogenen Basisinvarianten vom Grad $\leq |G| = N$.

Beweis : Wir führen neue Variablen $u_1, \ldots, u_n$ ein und betrachten die Ausdrücke

$$\begin{aligned} S_e(\mathbf{u}, \mathbf{x}) &:= \rho\left((u_1 x_1 + \ldots + u_n x_n)^e\right) \\ &= \frac{1}{|G|} \sum_{g \in G} (u_1 x_1^g + \ldots + u_n x_n^g)^e \end{aligned}$$

als Polynome in $(k[\mathbf{x}])[\mathbf{u}]$. Der Koeffizient vor $u_1^{a_1} \ldots u_n^{a_n}$ mit $a_1 + \ldots + a_n = e$ ist (ein mglw. positives Vielfaches von) $\rho(x_1^{a_1} \ldots x_n^{a_n})$.

Andererseits bekommt man S_e aus der Potenzsumme $P_e = y_1^e + \ldots + y_N^e$ durch Substitution $y_i \mapsto u_1 x_1^{g_i} + \ldots + u_n x_n^{g_i}$, wobei $g_i \in G, i = 1, \ldots, N$, alle Gruppenelemente durchläuft. Nach dem Hauptsatz über symmetrische Funktionen kann jede Potenzsumme in $y_1, \ldots, y_N$ polynomial durch die Potenzsummen $P_i, i \leq N$ dargestellt werden: $P_e = P_e(P_1, \ldots, P_N)$.

Damit gilt aber $S_e = P_e(S_1, \ldots, S_N)$. Expandiert man die rechte Seite, sortiert nach **u**-Potenzen und führt einen Koeffizientenvergleich aus, so erhält man eine polynomiale Darstellung der Invarianten $\rho(x_1^{a_1} \ldots x_n^{a_n})$ durch die Koeffizienten von $S_1, \ldots, S_N$, also durch homogene Invarianten vom Grad $\leq N$. $\square$

Beispiel: $n = 1$. Gruppen auf $\mathbb{C}[x]$ können nur als $g : x \mapsto \zeta(g)\, x$ operieren, wobei $\zeta \in G^*$ ein Gruppencharakter ist. Ist die Gruppe endlich, so muss $\zeta(g)$ eine Einheitswurzel sein.

Treue Gruppenaktionen sind also genau die der zyklischen Gruppe $C_N = \langle\sigma\rangle$ mit $x^\sigma = \zeta_N\, x$ und einer primitiven N-ten Einheitswurzel ζ_N. Der Invariantenring ist $\mathbb{C}[x^N]$. Gradschranke wird hier erreicht.

Beispiel: Skalare Aktionen der zyklischen Gruppe $C_N = \langle\sigma\rangle$ auf $\mathbb{C}[x_1, \ldots, x_n]$ durch $x_i^\sigma = \zeta_N\, x_i$.

Reynoldsoperator liefert

$$\rho(x_1^{a_1} \ldots x_n^{a_n}) = \begin{cases} x_1^{a_1} \ldots x_n^{a_n} & \text{wenn } p \mid a_1 + \ldots + a_n \\ 0 & \text{sonst} \end{cases}$$

Auch in diesem Beispiel wird die Gradschranke erreicht und ein System von Basisinvarianten besteht aus *allen* Monomen vom Grad N.

Der Invariantenring der skalaren C_N-Aktion wird als k-Vektorraum also von den Termen erzeugt, deren Grad ein Vielfaches von N ist. Diesen Ring bezeichnet man auch als N-ten Veronesering.

3 Permutationsdarstellungen

Als *Permutationsdarstellung* bezeichnet man die Aktion einer Untergruppe $G \subset S_n$ auf dem Polynomring $k[V] = k[x_1, \ldots, x_n]$ durch Variablenpermutation. Damit ist $k[V]^G \supset k[V]^{S_n}$ und nach dem Hauptsatz über symmetrische Funktionen bilden die elementarsymmetrischen Funktionen ein System von Primärinvarianten für $k[V]^G$.

3.1 Ein Beispiel: Die Aktion der S_4 auf den Kanten des K_4

Um mit Permutationsdarstellungen rechnen zu können, müssen zunächst die Permutationen in Permutationsmatrizen bzw. in Substitutionsdarstellungen umgewandelt werden:

```
permu2matrix:=proc(u:DOM_LIST) local i,M,n;
// Permutation in Permutationsmatrix umwandeln
begin n:=nops(u);
  M:=Dom::Matrix()(n,n);
  for i from 1 to n do M[i,u[i]]:=1 end_for;
  return(M);
end_proc;
```

Beispiel:

```
vars:=[x1,x2,x3];
M:=permu2matrix([3,1,2]);
```

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

```
matrix2subrules:=proc(M:Dom::Matrix(),vars:DOM_LIST)
// Matrix in subRules-Darstellung umwandeln
local n,v,i;
begin n:=linalg::matdim(M)[1];
  v:=M*Dom::Matrix()(n,1,vars);
  [vars[i]=v[i]$i=1..n];
end_proc;
```

Beispiel:

```
matrix2subrules(M,vars);
                        [x1 = x3, x2 = x1, x3 = x2]
```

Als nächstes ordnen wir den sechs Kanten des K_4 die Variablen $y_1, \ldots, y_6$ über eine Hashtabelle T zu:

```
HashTabelle:=proc(n) local u,T;
begin
  u:=[{i,j}$i=1..(j-1)$j=2..n];
  (T[u[i]]:=i)$i=1..nops(u);
  T;
end_proc;
T:=HashTabelle(4);
```

Nun erzeugen wir die 24 Kantenpermutationen, indem wir jede der 24 Knotenpermutationen in die zugehörige Kantenpermutation umrechnen, und wandeln diese Kantenpermutationen in der SubRules-Darstellung um:

```
kantenpermutation:=proc(u:DOM_LIST,T) local i,j;
  begin [T[{u[i],u[j]}]$i=1..(j-1)$j=2..nops(u)] end_proc;

u:=combinat::permutations(4);   // Die Elemente der S_4
v:=map(u,kantenpermutation,T);
      // Die Darstellung der S_4 als Untergruppe der S_6
vars:=[y1,y2,y3,y4,y5,y6];
w:=map(v,permu2matrix);         // Matrixdarstellung
G:=map(w,matrix2subrules,vars); // SubRules-Darstellung
```

Nun können wir mit dem Reynolds-Operator Invarianten in den verschiedenen Graden konstruieren. In den folgenden Beispielen sind die Invarianten bereits so skaliert, dass sich nur Summen von Termen ergeben.

```
e_1 := 6*Reynolds(y1,G);
e_2a :=12*Reynolds(y1*y2,G);
e_2b:= 3*Reynolds(y1*y6,G);
```

$$e_1 = y_1 + y_2 + y_3 + y_4 + y_5 + y_6$$
$$e_{2a} = y_1\,y_2 + y_1\,y_3 + y_1\,y_4 + y_2\,y_3 + y_1\,y_5 + y_2\,y_4 + y_2\,y_6 + y_3\,y_5 + y_3\,y_6 + y_4\,y_5 + y_4\,y_6 + y_5\,y_6$$
$$e_{2b} = y_1\,y_6 + y_2\,y_5 + y_3\,y_4$$

Wir sehen, dass $dim_k([R]_1) = 1$ und $dim_k([R]_2) = 2$ gilt. Genauer: Die Invariante e_2 der symmetrischen Gruppe lässt sich als Summe zweier unter G invarianter Teilsummen $e_2 = e_{2a} + e_{2b}$ mit den Leittermen $lt(e_{2a}) = y_1\,y_2$ und $lt(e_{2b}) = y_1\,y_6$ darstellen.

Ein Erzeugendensystem für die Invarianten aus $[R]_d$ erhalten wir, wenn wir auf die Terme vom Grad d den Reynoldsoperator anwenden. Die folgende Funktion erzeugt alle Terme vom Grad d über einer vorgegebenen Liste von Variablen.

```
Terme:=proc(d,vars) local u;
// Alle Terme vom Grad d produzieren
begin
  if nops(vars)=1 then [vars[1]^d]
  else u:=[op(vars,2..nops(vars))];
    [op(map(Terme(d-i,u),x->vars[1]^i*x))$i=0..d]
  end_if;
end_proc;
```

Wenden wir den Reynolds-Operator auf alle Terme vom Grad 2 an, so erkennen wir, dass neben den bereits erzeugten Invarianten nur noch eine weitere Invariante entsteht

```
map({op(Terme(2,vars))}, Reynolds, G);
p_2:= 6*Reynolds(y1^2,G);
```

$$y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2 + y_5{}^2 + y_6{}^2$$

Diese hat den Leitterm y_1^2 und lässt sich aus e_1^2 und e_2 linear kombinieren, wird also für ein System von Basisinvarianten nicht benötigt.

Analog erhalten wir eine k-Basis aus 6 Invarianten vom Grad 3. Der Leitterm jeder dieser Invarianten fällt jeweils mit dem erzeugenden Term zusammen.

```
e_3a := 4*Reynolds(y1*y2*y3,G);
e_3b := 4*Reynolds(y1*y2*y4,G);
e_3c := 12*Reynolds(y1*y2*y5,G);

u_31 := 6*Reynolds(y1^3,G);
u_32 := 6*Reynolds(y1^2*y6,G);
u_33 := 24*Reynolds(y1^2*y2,G);
```

Aus Invarianten kleineren Grads lassen sich die Invarianten $e_1^3, e_1\, e_{2a}$ und $e_1\, e_{2b}$ mit den Leittermen $y_1^3, y_1^2 y_2$ und $y_1^2 y_6$ erzeugen. Diese hängen mit u_{31}, u_{32}, u_{33} wie folgt zusammen:

$$\begin{aligned} e_1^3 &= u_{31} + 3\, u_{32} + 3\, u_{33} + 6\, (e_{3a} + e_{3b} + e_{3c}) \\ e_1\, e_{2a} &= u_{33} + 3\, e_{3a} + 3\, e_{3b} + 2\, e_{3c} \\ e_1\, e_{2b} &= u_{32} + e_{3c} \end{aligned}$$

Die Invarianten u_{31}, u_{32}, u_{33} lassen sich also durch $e_1^3, e_1\, e_{2a}, e_1\, e_{2b}$ in einer k-Basis von $[R]_3$ ersetzen. Das System von Basisinvarianten besteht nach Analyse der Invarianten bis zum Grad 3 damit aus $(e_1, e_{2a}, e_{2b}, e_{3a}, e_{3b}, e_{3c})$. Diese stehen offensichtlich in eineindeutiger Beziehung zu den Isomorphieklassen von Teilgraphen des K_4 mit vorgegebener Kantenzahl.

Im Grad 4 liefert der Reynolds-Operator eine k-Basis aus den folgenden 11 Elementen:

```
e_4a := 12*Reynolds(y1*y2*y3*y4,G);
e_4b := 4*Reynolds(y1*y2*y5*y6,G);

u_41 := 6*Reynolds(y1^4,G);
u_42 := 12*Reynolds(y1^3*y2,G);
u_43 := 6*Reynolds(y1^3*y6,G);
u_44 := 12*Reynolds(y1^2*y2*y3,G);
u_45 := 12*Reynolds(y1^2*y2*y4,G);
u_46 := 12*Reynolds(y1^2*y2*y5,G);
```

```
u_47 := 12*Reynolds(y1^2*y2^2,G);
u_48 := 3*Reynolds(y1^2*y6^2,G);
u_49 := 24*Reynolds(y1^2*y2*y6,G);
```

Die beiden ersten Invarianten müssen zum System der Basisinvarianten hinzugenommen werden. Die anderen neun Invarianten entsprechen Invarianten, die sich aus den bereits bekannten Basisinvarianten vom Grad < 4 kombinieren lassen und diese neun Kombinationen haben paarweise verschiedene Leitterme, sind also ihrerseits linear unabhängig.

Das ändert sich erstmals im Grad 5. Neben der neuen Invarianten

```
e_5  := 6*Reynolds(y1*y2*y3*y4*y5,G);
```

gibt es 17 weitere Invarianten, denen 17 Invarianten vom Grad 5 gegenüberstehen, die sich aus den bisher berechneten Basisinvarianten vom Grad < 5 kombinieren lassen. Allerdings fallen die Leitterme der Invarianten $u_1 = e_{2b}\, e_{3c}$ und $u_2 = e_1\, e_{4b}$ zusammen, so dass wir nicht wie bisher allein aus der Inspektion der Leitterme auf die lineare Unabhängigkeit schließen können. Jedoch gilt

$$u_1 - u_2 - e_5 = y_1^2 y_2 y_6^2 + \text{ kleinere Terme}$$

und der Leitterm $y_1^2 y_2 y_6^2$ ist neu, so dass auch im Grad 5 die abgeleiteten Invarianten linear unabhängig sind.

Im Grad 6 wierden die Zusammenhänge noch unübersichtlicher, so dass die Untersuchungen hinaus schieben wollen, bis wir weitere Analysewerkzeuge in der Hand haben.

3.2 G-Orbits und der Orbitsatz

Permutationsdarstellungen haben gegenüber allgemeinen Darstellungen eine Besonderheit: G operiert nicht nur auf S, sondern bereits (Grad erhaltend) auf den Termen $T = T(x_1, \ldots, x_n)$ selbst.

Für $m \in T$ können wir das *Orbit* $m^G := \{m^g \in T \,:\, g \in G\}$ und den *Stabilisator* $G_m := \{g \in G \,:\, m^g = m\}$ definieren.

Für $g, h \in G$ bezeichnet man $g^h = h^{-1}\, g\, h \in G$ als zu g *konjugiertes Element* und $g^G = \{g^h \,:\, h \in G\}$ als *Konjugationsklasse* des Elements $g \in G$.

Satz 11 (Orbitsatz)

1. *$\{m^G \,:\, m \in T\}$ ist eine Klasseneinteilung von T, d.h. zwei Orbits m_1^G und m_2^G mit $m_1, m_2 \in T$ fallen entweder zusammen oder sind disjunkt.*

   Die zugehörige Äquivalenzrelation wird definiert durch

   $$m_1 \sim m_2 \Leftrightarrow \exists g \in G \,:\, m_1 = m_2^g\,.$$

2. *Der Stabilisator G_m ist eine Untergruppe von G.*

   Gilt $m_1 \sim m_2$, so sind die zugehörigen Stabilisatoren zueinander konjugierte Untergruppen. Insbeosndere sind die Stabilisatoren der Elemente $m \in T$ aus einem Orbit gleich mächtig.

3. *$|m^G| = |G| : |G_m|$.*

Dieser Satz gilt für beliebige Mengen T mit G-Aktion. Insbesondere ist er richtig für die Aktion von G auf sich selbst durch Konjugation. Orbits unter dieser G-Aktion sind die Konjugationsklassen. Konjugationsklassen fallen also ebenfalls entweder zusammen oder sind disjunkt.

Für eine Permutationsdarstellung besteht ine k-Basis von $[R]_d$ also aus den verschiedenen *Orbitsummen* $\mathrm{Orb}(m) = \sum_{t \in m^G} t$, denn $\mathrm{Orb}(m)$ stimmt mit $\mathrm{Reynolds}(m, G)$ bis auf einen Skalierungsfaktor überein und die Summandenmengen zweier verschiedener Orbitsummen sind disjunkt.

Beispiele für solche Orbitsummen sind etwa die monomialen symmetrischen Funktionen $\mu(\lambda)$ bzgl. der Aktion der vollen Permutationsgruppe S_n.

3.3 Darstellung von Permutationen

Darstellung als Liste, als Funktionswert-Tabelle, als Diagramm. Begriff des Zyklus und Zerlegung in elementfremde Zyklen.

Satz 12 *Jede Permutation $\sigma \in S_n$ besitzt eine Darstellung als Produkt elementfremder Zyklen. Die Faktoren einer solchen Darstellung kommutieren miteinander. Die Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.*

Die Längen der Zyklen in dieser Darstellung bezeichnet man auch als den Zyklentyp *von σ.*

Zwei Permutationen sind genau dann zueinander konjuguiert, wenn sie denselben Zyklentyp haben.

Sind $G, G' \subset S_n$ zwei zueinander konjugierte Permutationsgruppen, also $G' = \{\sigma^{-1}\, g\, \sigma \,:\, g \in G\}$ für ein $\sigma \in S_n$, so sind die Invariantenringe dieser Gruppen „im Wesentlichen“ gleich. Genauer: Die Variablenumbenennung $y_i = x_{\sigma(i)}, i = 1, \ldots, n$, induziert einen Ringisomorphismus

$$S = k[x_1, \ldots, x_n] \longrightarrow S' = k[y_1, \ldots, y_n],$$

der die G-Aktion auf S in die G'-Aktion auf S' überführt:

$$y_i = x_{\sigma(i)} \overset{g}{\mapsto} x_{g\sigma(i)} = y_{\sigma^{-1}g\sigma(i)}$$

3.4 Beispiel: Aktionen der Untergruppen der S_4 auf $\mathbb{Q}[x_1, x_2, x_3, x_4]$

Untergruppen der S_4 sind durch die Zyklentypen ihrer Elemente jeweils bis auf Konjugation eindeutig bestimmt. Wir können zur Bestimmung des zugehörigen Invariantenrings jeweils einen speziellen Vertreter wählen, da die Invariantenringe konjugierter Untergruppen zueinander isomorph sind.

Eine Permutationsgruppe $G \subset S_n$ heißt *fixpunktfrei*, wenn es kein $1 \le i \le n$ mit $g(i) = i$ ür alle $g \in G$ gibt. Hat $G \subset S_4$ etwa den Fixpunkt $i = 4$, so ist x_4 invariant und die Invariantenbestimmung für G lässt sich auf eine Invariantenbestimmungsaufgabe über $\mathbb{Q}[x_1, x_2, x_3]$ zurückführen. Wir wollen uns deshalb auf die Bestimmung der Invarianten der fixpunktfreien Permutationsgruppen C_4, V_4, D_4 und A_4 beschränken.

Mit MuPAD können wir diese Gruppen wie folgt generieren: Wir nehmen erzeugende Permutationen, transformieren diese mit Hilfe der Funktion `combinat::permutations::toMatrix` in Permutationsmatrizen, erzeugen daraus die jeweilige Menge der Gruppenelemente und wandeln diese Menge schließlich in die SubRules-Darstellung um.

Die zyklische Gruppe C_4 – Die Quadratdrehgruppe

```
vars:=[x1,x2,x3,x4];
s1:=combinat::permutations::toMatrix([2,3,4,1]); // (1234)
M_C4:={s1^i$i=0..3};
C4:=map(M_C4,matrix2subrules,[x1,x2,x3,x4]);
```

Die Kleinsche Vierergruppe V_4 – Eine spezielle Teilgruppe der Quadratsymmetrien

```
s2a:=combinat::permutations::toMatrix([2,1,4,3]); // (12)(34)
s2b:=combinat::permutations::toMatrix([3,4,1,2]); // (13)(24)
M_V4:={s2a^0,s2a,s2b,s2a*s2b};
V4:=map(M_V4,matrix2subrules,[x1,x2,x3,x4]);
```

Die Diedergruppe D_4 – Die Gruppe der Quadratsymmetrien

```
M_D4:={(s1^i,s2a*s1^i)$i=0..3};
s1*s2a = s2a*s1^3; // = (13)
D4:=map(M_D4,matrix2subrules,[x1,x2,x3,x4]);
```

Die Gruppe der geraden Permutationen A_4 – Die Drehgruppe des Tetraeders

```
s3:=combinat::permutations::toMatrix([2,3,1,4]); // (123)
M_A4:={(s3^i,s2a*s3^i,s2b*s3^i,s2a*s2b*s3^i)$i=0..2};
s2a*s3 = s3*s2b;      // = (243)
s2b*s3^2 = s3^2*s2a;  // = (234)
A4:=map(M_A4,matrix2subrules,[x1,x2,x3,x4]);
```

Die Invarianten der C_4

Sei wie immer $R = S^G$ der Invariantenring. Vektorraumbasen von $[R]_d$ können für die einzelnen Gruppenaktionen nach dem bisher entwickelten Schema bestimmt werden. Betrachten wir zunächst C_4. Der Reynoldsoperator bildet eine Basis der Terme von $[S]_d$ (bis auf Skalare) auf die entsprechenden Orbitsummen ab, die Summen aus paarweise disjunkten Summandenmengen und damit linear unabhängig sind. Die verschiedenen Orbitsummen im Grad d bilden also eine Vektorraumbasis von $[R]_d$.

```
e_1 :=4*Reynolds(x1,C4);

//== Grad 2: 3 Invarianten
map({op(Terme(2,vars))}, Reynolds, C4); nops(%);
```

Die drei Orbitsummen haben die Leitterme x_1^2, x_1x_2, x_1x_3. Aus der Invarianten e_1 vom Grad 1 lässt sich eine Invariante e_1^2 vom Grad 2 mit dem Leitterm x_1^2 erzeugen. Die beiden Invarianten

```
e_2a:=4*Reynolds(x1*x2,C4);
e_2b:=2*Reynolds(x1*x3,C4);
```

dagegen sind neu und für ein System von Basisinvarianten erforderlich. Die folgende Funktion bestimmt alle Leitterme.

```
getLeadTerms:=proc(u,vars) local x;
begin map([op(u)],x->expr(lterm(poly(x,vars)))) end_proc;
```

Da die Leitterme paarweise verschieden sind, haben wir also folgende Vektorraumbasis für $[R]_2$ gefunden:

```
B_2:=[e_1^2,e_2a,e_2b];
getLeadTerms(B_2,vars);
```

Im Grad 3 gehen wir ähnlich vor:

```
//== Grad 3: 5 Invarianten
U_3:=map({op(Terme(3,vars))}, Reynolds, C4); nops(%);
L_3:=sort(getLeadTerms(U_3,vars));
```

Neben den Invarianten, die man aus B_2 durch Multiplikation mit e_1 finden kann, sind das

```
e_3a:=4*Reynolds(x1^2*x4,C4);
e_3 :=4*Reynolds(x1*x2*x3,C4);
```

Eine Basis von $[R]_3$ (prüfe wieder auf paarweise verschiedene Leitterme) ist also

```
B_3:=[op(map(B_2,u->u*e_1)),e_3a,e_3]; nops(%);
getLeadTerms(B_3,vars);
```

Im Grad 4 beginnen wir mit Invarianten, die sich aus Invarianten kleineren Grades erzeugen lassen

```
//== Grad 4: 10 Invarianten
U_4:=map({op(Terme(4,vars))}, Reynolds, C4); nops(%);
L_4:=sort(getLeadTerms(U_4,vars));

B_4:=[op(map(B_3,u->u*e_1)),op(Terme(2,[e_2a,e_2b]))]; nops(%);
```

und bestimmen diejenigen Leitterme von Invarianten aus U_4, die damit noch nicht erfasst sind:

```
setDiff:=proc(a,b) begin _minus({op(a)},{op(b)}) end_proc;

getLeadTerms(B_4,vars);
setDiff(L_4,%);
```

Invarianten mit diesen Leittermen können wir als die zugehörigen Orbitsummen generieren.

```
e_4a:=4*Reynolds(x1^2*x2*x4,C4);
e_4b:=4*Reynolds(x1^2*x3*x4,C4);
e_4 :=Reynolds(x1*x2*x3*x4,C4);
```

Zwei der 8 Elemente von B_4 haben den gleichen Leitterm $x_1^2x_2x_3$, so dass die bisherige Argumentation für den Nachweis der linearen Unabhängigkeit der erzeugten Invarianten nicht mehr greift. In der Tat ist eine von ihnen überflüssig, denn wir wissen $dim_k([R]_4) = 10$, haben aber 11 Invarianten vom Grad 4 konstruiert. Gaussreduktion liefert die Beziehung

$$e_1e_3 = e_{2a}e_{2b} + 4\,e_4 + e_{4a},$$

so dass wir eine der vier beteiligten Invarianten für eine Vektorraumbasis B_4 von $[R]_4$ weglassen können. In der folgenden Aufstellung wurde die Basis so modifiziert, dass wieder paarweise verschiedene Leitterme vorliegen

```
B_4:=[op(map(B_3,u->u*e_1)),e_2a^2,e_2a*e_2b-e_1*e_3,e_2b^2,e_4b,e_4]; nops(%);
getLeadTerms(B_4,vars);
```

Allerdings wird es damit auch deutlich schwieriger, in den nächsten Graden ein linear unabhängiges System von solchen Invarianten anzugeben, die sich aus Invarianten kleineren Grades erzeugen lassen.

Wir wollen diese Untersuchungen deshalb hier abbrechen und noch nach einem System von Primärinvarianten fragen. Ein solches System besteht aus 4 algebraisch unabhängigen Invarianten und $(e_1, e_2 = e_{2a} + e_{2b}, e_3, e_4)$ ist ein solches System, weil es ein System von Primärinvarianten sogar für die S_4 ist. Gibt es Systeme von Primärinvarianten von kleinerem Grad?

Nach dem Charakterisierungssatz erkennen wir ein solches System daran, dass die vier Polynome nur den Nullpunkt als gemeinsame Nullstelle besitzen. Prüfen wir das für verschiedene Kombinationen:

```
solve([e_1,e_2a,e_2b,e_3], vars);  // geht nicht
solve([e_1,e_2a,e_2b,e_3a], vars); // geht nicht
solve([e_1,e_2a,e_2b,e_4], vars);
```

e_3 und e_{3a} sind also algebraisch abhängig von (e_1, e_{2a}, e_{2b}). Eine genauere Analyse mit CoCoA liefert $e_3^2, e_{3a}^2 \in Id(e_1, e_{2a}, e_{2b})$. So gilt etwa

$$e_3^2 = \begin{pmatrix} x_2\,x_3\,x_4^3 + x_2^3\,x_3\,x_4 + 2\,x_1\,x_2\,x_3\,x_4^2 + 2\,x_1\,x_2\,x_3^2\,x_4 + 2\,x_1\,x_2^2\,x_3\,x_4 + \\ 3\,x_2^2\,x_4^3 + 3\,x_2^3\,x_4^2 + x_1\,x_2^2\,x_3^2 + x_1\,x_2^2\,x_4^2 + x_1\,x_3^2\,x_4^2 + 3\,x_2^2\,x_3\,x_4^2 \\ -4\,x_2^2\,x_4^2 \\ -x_2^3\,x_3 - 3\,x_2\,x_4^3 - 3\,x_2^3\,x_4 - x_3\,x_4^3 - 3\,x_2\,x_3\,x_4^2 - 2\,x_2\,x_3^2\,x_4 - \\ 3\,x_2^2\,x_3\,x_4 - x_2^2\,x_3^2 - 6\,x_2^2\,x_4^2 - x_3^2\,x_4^2 \end{pmatrix}^T \cdot \begin{pmatrix} e_1 \\ e_{2a} \\ e_{2b} \end{pmatrix}$$

Da Terme in den Primärinvarianten linear unabhängig sind (jede lineare Abhängigkeitsrelation zwischen Termen in den Primärinvarianten wäre ja eine algebraische Abhängigkeitsrelation zwischen den Primärinvarianten selbst), bildet die Polynomalgebra $R_0 = \mathbb{Q}[e_1, e_{2a}, e_{2b}, e_4]$ eine Teilalgebra von R. Im Grad 2 stimmen beide sogar überein und B_2 ist eine Vektorraumbasis auch von $[R_0]_2$. B_3 zerlegt sich in $P_3 = e_1 \cdot B_2$ als Basis von $[R_0]_3$ und (e_3, e_{3a}), was einer Zerlegung

$$[R]_3 = [R_0]_3 \oplus e_3 \cdot [R_0]_0 \oplus e_{3a} \cdot [R_0]_0$$

entspricht. Diese setzt sich im Grad 4 fort zu einem System von 9 bereits bekannten Invarianten

$$[R_0]_4 \oplus e_3 \cdot [R_0]_1 \oplus e_{3a} \cdot [R_0]_1$$

```
P_4:=[op(map(B_2,u->u*e_1^2)),op(Terme(2,[e_2a,e_2b])),e_4];
B_4:=P_4 . [e_3*e_1, e_3a*e_1]; nops(%);
getLeadTerms(B_4,vars);
setDiff(L_4,%);
```

Es fehlen e_{4a} und e_{4b}, aber wir hatten oben festgestellt, dass e_{4a} eine Linearkombination bereits erzeugter Invarianten ist, so dass e_{4b} die bisher gefundenen Invarianten zu einer Vektorraumbasis von $[R]_4$ ergänzt:

$$[R]_4 = [R_0]_4 \oplus e_3 \cdot [R_0]_1 \oplus e_{3a} \cdot [R_0]_1 \oplus e_{4b} \cdot [R_0]_0$$

Setzen wir diese Rechnungen im Grad 5 fort. Die gefundene Zerlegung im Grad 4 setzt sich fort zu einer Zerlegung

$$[R_0]_5 \oplus e_3 \cdot [R_0]_2 \oplus e_{3a} \cdot [R_0]_2 \oplus e_{4b} \cdot [R_0]_1$$

```
//== Grad 5: 14 Invarianten
U_5:=map({op(Terme(5,vars))}, Reynolds, C4); nops(%);

P_5:=map(P_4,u->u*e_1); nops(%);
B_5:=P_5 . map(B_2,u->u*e_3) . map(B_2,u->u*e_3a) . [e_1*e_4b]; nops(%);
```

B_5 enthält 14 Invarianten, was mit der Vektorraumdimension von $[R]_5$ übereinstimmt. B_5 ist also eine Basis, wenn die 14 Invarianten linear unabhängig sind. Das können wir mit Methoden aus der linearen Algebra prüfen, indem wir aus der mit unbestimmten Koeffizenten a_i angesetzten Summe

$$\sum_{f_i \in B_5} a_i f_i = 0$$

durch Koeffizientenvergleich ein lineares Gleichungssystem für diese unbestimmten Koeffizienten extrahieren.

```
linTest:=proc(B,vars) local i,n,sys; save a;
begin
  n:=nops(B);
  sys:=[coeff(_plus(a[i]*B[i]$i=1..n),vars)];
  solve(sys,[a[i]$i=1..n]);
end_proc;
linTest(B_5,vars);
```

Der Test bestätigt, dass die Invarianten linear unabhängig sind, wir also eine Vektorraumbasis von $[R]_5$ gefunden haben. Auf ähnliche Weise lassen sich die Invarianten im Grad 6 bestimmen. Diese Rechnungen legen die Vermutung nahe, dass allgemein

$$R = R_0 \oplus e_3 \cdot R_0 \oplus e_{3a} \cdot R_0 \oplus e_{4b} \cdot R_0$$

gilt.

Die Invarianten der V_4

Bestimmen wir nach demselben Prinzip die Invarianten der V_4.

```
e_1 :=4*Reynolds(x1,V4);

//== Grad 2: 4 Invarianten
map({op(Terme(2,vars))}, Reynolds, V4); nops(%);

e_2a:=2*Reynolds(x1*x2,V4);
e_2b:=2*Reynolds(x1*x3,V4);
e_2c:=2*Reynolds(x1*x4,V4);

B_2:=[e_1^2,e_2a,e_2b,e_2c];
```

Wir haben 4 Invarianten gefunden und prüfen nun, ob es sich bereits um ein System von Primärinvarianten handelt:

```
solve([e_1,e_2a,e_2b,e_2c],vars);
```

Das System hat nur die triviale Lösung, also können wir $R_0 = \mathbb{Q}[e_1, e_{2a}, e_{2b}, e_{2c}]$ setzen. Im nächsten Grad ergibt sich

```
//== Grad 3: 5 Invarianten
U_3:=map({op(Terme(3,vars))}, Reynolds, V4); nops(%);
L_3:=sort(getLeadTerms(U_3,vars));

P_3:=[op(map(B_2,u->u*e_1))]; nops(%);
getLeadTerms(P_3,vars);
setDiff(L_3,%);
```

Es fehlt noch eine Invariante zur Vektorraumbasis

```
e_3 :=4*Reynolds(x1*x2*x3,V4);
B_3:=P_3 . [e_3];
```

Dieser Basis entspricht die Zerlegung

$$[R]_3 = [R_0]_3 \oplus e_3 \cdot [R_0]_0,$$

die sich im Grad 4 wie folgt fortsetzt:

```
//== Grad 4: 11 Invarianten
U_4:=map({op(Terme(4,vars))}, Reynolds, V4); nops(%);
L_4:=sort(getLeadTerms(U_4,vars));

P_4:=[op(map(P_3,u->u*e_1)),op(Terme(2,[e_2a,e_2b,e_2c]))]; nops(%);
B_4:=P_4 . [e_3*e_1];
getLeadTerms(B_4,vars);
setDiff(L_4,%);
```

Eigentlich enthält B_4 genug Terme, so dass wir vermuten können, dass der fehlende Leitterm, der zur Orbitsumme

```
e_4 :=Reynolds(x1*x2*x3*x4,V4);
```

gehört, auch durch Gaussreduktion gewonnen werden kann. Prüfen wir zunächst die lineare Unabhängigkeit von B_4

```
linTest(B_4,vars);
```

Also muss e_4 eine Linearkombination dieser Invarianten sein

```
linTest(B_4.[e_4],vars);
```

Die Lösung entspricht der Darstellung

$$4 \cdot e_4 = e_1 \cdot e_3 - (e_{2a} \cdot e_{2b} + e_{2a} \cdot e_{2c} + e_{2b} \cdot e_{2c})$$

Auch im Grad 5 und 6 wird die Vermutung $R = R_0 \oplus e_3 \cdot R_0$ bestätigt.

```
//== Grad 5: 14 Invarianten
U_5:=map({op(Terme(5,vars))}, Reynolds, V4); nops(%);

P_5:=map(P_4,u->u*e_1);
B_5:=P_5 . map(B_2,u->u*e_3); nops(%);
linTest(B_5,vars);

//== Grad 6: 24 Invarianten
U_6:=map({op(Terme(6,vars))}, Reynolds, V4); nops(%);
P_6:=[op(map(P_5,u->u*e_1)), op(Terme(3,[e_2a,e_2b,e_2c]))]; nops(%);
B_6:=P_6 . map(P_3,u->u*e_3); nops(%);
linTest(B_6,vars);
```

e_3^2 ist ebenfalls eine Invariante vom Grad 6, die folglich eine Zerlegung als Element der Summe $[R_0]_6 \oplus e_3 \cdot [R_0]_3$ haben muss. Lösen wir das entsprechende Gleichungssystem

```
linTest(B_6.[e_3^2],vars);
```

so ergibt sich mit $E = (e_{2a}, e_{2b}, e_{2c})$ die folgende algebraische Abhängigkeitsrelation

$$e_3^2 - e_1 \cdot e_3 \cdot e_1(E) + \frac{1}{4}\, e_1^3 \cdot e_3 - \frac{1}{4}\, e_1^2 \cdot e_2(E) + \mu_{(2,1)}(E) + 2 \cdot e_3(E) = 0\,.$$

4 Die Molienreihe

4.1 Erzeugende Funktionen von Polynomringen

Definition der erzeugenden Funktion einer homogenen k-Algebra R:

$$H(R,t) := \sum_{i=0}^{\infty} dim_k([R]_d)\, t^d.$$

Satz 13 *Ist $S = k[y_1, \ldots, y_n]$ ein gewichtet homogener Polynomring, wobei die Variablen die Grade $deg(y_i) = d_i$ haben, so gilt*

$$H(S,t) = \frac{1}{(1-t^{d_1})(1-t^{d_2}) \cdot \ldots \cdot (1-t^{d_n})}$$

Beweis : Der Beweis erfolgt durch Induktion nach n.

Für $n = 1$ erhalten wir

$$H(k[y_1], t) = 1 + t^{d_1} + t^{2\,d_1} + \ldots = \frac{1}{1 - t^{d_1}}\,.$$

Nehmen wir nun an, dass die Behauptung für $S' = k[y_1, \ldots, y_{n-1}]$ gilt. Eine Basis von $[S]_e$ besteht aus Termen vom Grad e in $y_1, \ldots, y_n$. Diese können wir unterteilen in solche, die y_n als Faktor enthalten und solche ohne einen Faktor y_n, also $[S]_e = y_n \cdot [S]_{e-d_n} \oplus [S']_e$. Auf der Ebene der Hilbertreihen ergibt dies

$$H(S,t) = \sum_{e \geq 0} dim([S]_e) t^e = \sum_{e \geq 0} dim([S]_{e-d_n}) t^e + \sum_{e \geq 0} dim([S']_e) t^e = t^{d_n}\, H(S,t) + H(S',t)$$

und somit

$$(1 - t^{d_n})\, H(S,t) = H(S',t)\,,$$

woraus die Behauptung sofort folgt. $\square$

Im letzten Abschnitt hatten wir festgestellt, dass der Invariantenring $R = S^{V_4}$ (wahrscheinlich) von den Basisinvarianten $(e_1, e_{2a}, e_{2b}, e_{2c}, e_3)$ erzeugt wird, von denen $(e_1, e_{2a}, e_{2b}, e_{2c})$ ein System von Primärinvarianten bildet, die Invariante e_3 aber einer algebraischen Relation $f = e_3^2 - \ldots$ vom Grad 6 genügt, mit welcher jeder polynomiale Ausdruck in den fünf Basisinvarianten als Summe

$$P_0(e_1, e_{2a}, e_{2b}, e_{2c}) + e_3 \cdot P_1(e_1, e_{2a}, e_{2b}, e_{2c}) \in R_0 \oplus e_3 \cdot R_0$$

geschrieben werden kann. Damit würde

$$R = R_0 \oplus e_3 \cdot R_0$$

gelten, woraus sich

$$H(R,t) = (1 + t^3)\, H(R_0,t) = \frac{1 + t^3}{(1-t)(1-t^2)^3}$$

herleitet. Allgemein gilt

Satz 14 *Ist $R = h_1 \cdot R_0 \oplus \cdots \oplus h_k \cdot R_0$ eine Zerlegung der homogenen k-Algebra R in die direkte Summe von homogenen R_0-Moduln (etwa mit $h_1 = 1$) und $deg(h_i) = d_i$, so gilt*

$$H(R,t) = (t^{d_1} + \cdots + t^{d_k})\, H(R_0,t).$$

Andererseits können wir in obigem Beispiel R als Faktorring $R = \mathbb{Q}[e_1, e_{2a}, e_{2b}, e_{2c}, e_3]/(f)$ darstellen.

Satz 15 *Ist $S = k[y_1, \ldots, y_n]$ ein gewichtet homogener Polynomring und f ein (quasi)-homogenes Polynom vom Grad d, so gilt*

$$H(S/(f),t) = (1 - t^d) H(S,t)$$

Der Beweis ergibt sich sofort aus folgendem Lemma

Lemma 1 *Ist $\phi : V \to W$ ein Homomorphismus endlich dimensionaler k-Vektorräume, so gilt*

$$dim_k(ker(\phi)) + dim_k(im(\phi)) = dim_k(V).$$

Beweis des Lemmas: Wir wählen $e_1, \ldots, e_m$ als Basis von $ker(\phi) \subset V$ und ergänzen diese durch $d_1, \ldots, d_k$ zu einer Basis von V. Dann ist $\phi(d_1), \ldots, \phi(d_k)$ eine Basis von $im(\phi)$. $\square$

Wenden wir das Lemma auf die Komponenten vom Grad e der kanonischen Abbildung $\pi : S \to S/(f)$ mit $\pi(h) = h \pmod f$ an, so erhalten wir wegen $ker(\pi) = f \cdot S$

$$t^d H(S,t) + H(S/(f),t) = H(S,t). \quad \square$$

4.2 Der Satz von Molien

Beispiel: Für $R = \mathbb{Q}[e_1, e_{2a}, e_{2b}, e_{2c}, e_3]/(f)$ ergibt sich wie oben

$$H(R,t) = \frac{1-t^6}{(1-t)(1-t^2)^3(1-t^3)} = \frac{1+t^3}{(1-t)(1-t^2)^3}.$$

Wir können aus der Taylorreihenentwicklung dieser Funktion die Vektorraumdimensionen der einzelnen Grade von $R = R_0 \oplus e_3 \cdot R_0$ und damit die Anzahl der aus den Basisinvarianten nach obigem Schma erzeugbaren Invarianten des jeweiligen Grads ablesen:

```
f:=(1+t^3)/((1-t)*(1-t^2)^3);
taylor(f,t=0,20);
```

$$1 + t + 4\,t^2 + 5\,t^3 + 11\,t^4 + 14\,t^5 + 24\,t^6 + 30\,t^7 + 45\,t^8 + 55\,t^9 + 76\,t^{10} + 91\,t^{11} + 119\,t^{12} + 140\,t^{13} + 176\,t^{14} + 204\,t^{15} + 249\,t^{16} + 285\,t^{17} + 340\,t^{18} + 385\,t^{19} + O\left(t^{20}\right)$$

Der folgende Satz erlaubt es, auch die Vektorraumdimensionen $dim_k([R]_e)$ für den Invariantenring selbst zu bestimmen, die wir in den bisherigen Beispielen jeweils aus der Anwendung des Reynoldoperators auf eine Basis von $[S]_e$ bestimmt hatten (wobei wir für die Feststellung der linearen Unabhängigkeit die spezielle Struktur der Invarianten einer Permutationsdarstellung als Orbitsummen ausgenutzt hatten). Ein Vergleich der beiden Dimensionen erlaubt Rückschlüsse, ob das System der Basisinvarianten bereits vollständig ist.

Satz 16 (Satz von Molien, 1897) *Die endliche Gruppe G operiere regulär auf dem Polynomring $S = k[x_1, \ldots, x_n]$. Dann gilt für die Hilbertreihe des Invariantenrings $R = S^G$*

$$H(R,t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{det(E_n - t \cdot M_g)},$$

wobei $M_g \in Gl(n,k)$ die Matrixdarstellung der Aktion von $g \in G$ und E_n die Einheitsmatrix ist. Die Hilbertreihe eines Invariantenrings wird deshalb auch als Molienreihe *bezeichnet.*

Beispiel: Für die Aktion der V_4 auf $S = \mathbb{Q}[x_1, x_2, x_3, x_4]$ ergibt sich wegen

$$M_{V_4} = \left\{ \begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix} \right\}$$

als Hilbertreihe des Invariantenrings

$$H(S^{V_4}, t) = \frac{1}{4}\left(\frac{1}{(1-t)^4} + \frac{3}{t^4 - 2t^2 + 1}\right) = \frac{t^2 - t + 1}{4\,t^3 - t^2 - 2\,t - t^4 - 2\,t^5 + t^6 + 1}$$

und aus der Taylorreihe die zu erwartenden Vektorraumdimensionen ebenfalls als

$$1 + t + 4\,t^2 + 5\,t^3 + 11\,t^4 + 14\,t^5 + 24\,t^6 + 30\,t^7 + 45\,t^8 + 55\,t^9 + 76\,t^{10} + 91\,t^{11} + 119\,t^{12} + 140\,t^{13} + 176\,t^{14} + 204\,t^{15} + 249\,t^{16} + 285\,t^{17} + 340\,t^{18} + 385\,t^{19} + O\left(t^{20}\right)$$

Beide Reihen sind auch als rationale Funktionen identisch, wie sich aus

```
normal(f);
```

sofort erkennen lässt. Damit stimmen die Vektorraumdimensionen der homogenen Komponenten von $R = R_0 \oplus e_3 \cdot R_0$ und S^{V_4} in *allen* Graden überein, so dass wir damit beweisen haben, dass R bereits der volle Invariantenring ist.

Die beiden Reihen – die aus dem Satz von Molien berechnete Hilbertreihe des Invariantenrings und die Hilbertreihe des aus den bisher konstruierten Primär- und Sekundärinvarianten erzeugten R_0-Moduls – erlauben es auch im allgemeinen Fall schnell die Grade zu finden, in welchen evtl. noch Invarianten fehlen bzw. die Vollständigkeit eines Systems von Basisinvarianten festzustellen.

4.3 Invarianten zyklischer Gruppenaktionen

Beispiel: Obige Aktion der C_4 auf $\mathbb{Q}[x_1, x_2, x_3, x_4]$.
$G = C_4$ wird erzeugt von $g = (1234)$, was der Matrix

$$M_g = s_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

entspricht. Diese Matrix hat (über $K = \mathbb{Q}[\mathrm{i}]$) eine Basis aus Eigenvektoren

```
linalg::eigenvectors(s1);
```

$$\begin{aligned} y_1 &= x_1 + x_2 + x_3 + x_4 && \text{mit } y_1^g = y_1 \\ y_2 &= x_1 - x_2 + x_3 - x_4 && \text{mit } y_2^g = -y_2 = \mathrm{i}^2\, y_2 \\ y_3 &= \mathrm{i}\,(x_1 - x_3) + (x_2 - x_4) && \text{mit } y_3^g = \mathrm{i}\, y_3 \\ y_4 &= \mathrm{i}\,(x_1 - x_3) - (x_2 - x_4) && \text{mit } y_4^g = -\mathrm{i}\, y_4 = \mathrm{i}^3\, y_4 \end{aligned}$$

Invarianten kann man in den (y_i) einfacher ausdrücken als in den (x_i), denn g überführt einen Term $m \in T(\mathbf{y})$ in ein skalares Vielfaches, so dass $R = S^G$ eine K-Basis aus invarianten Termen $m \in T(\mathbf{y})$ besitzt. Solche invarianten Terme sind etwa $y_1, y_2^2, y_3 y_4, y_3^4, y_4^4$. Solche Invarianten lassen sich mit B^{-1} zu Invarianten in den (x_i) transformieren, wobei B die Matrix des Basiswechsels $\mathbf{y}^T = B \cdot \mathbf{x}^T$ ist.

Dies gilt generell für zyklische Gruppenaktionen: Wenn $G = \langle\sigma\rangle$ eine (reguläre) zyklische Gruppenaktion auf $k[x_1, \ldots, x_n] = k[V]$ induziert, so hat M_σ über einer algebraischen Erweiterung K/k eine Basis aus Eigenvektoren $y_1, \ldots, y_n$, wobei $\mathbf{y}^T = B \cdot \mathbf{x}^T$ gilt für eine Basiswechsel-Matrix $B \in Gl(n, K)$. Die Eigenwerte dieser Eigenvektoren sind N-te Einheitswurzeln mit $N = \mathrm{ord}(\sigma) = |G|$. Bezeichnet $\varepsilon \in K$ eine primitive N-te Einheitswurzel, so gilt

$$y_i^\sigma = \varepsilon^{\alpha_i}\, y_i \qquad \text{für } i = 1, \ldots, n$$

und geeignete Exponenten $\alpha_i \in \mathbb{N}$. Damit wird unter σ (und folglich unter allen Elementen von G) ein Term $m = y_1^{a_1} \ldots y_n^{a_n} \in T(\mathbf{y})$ in ein skalares Vielfaches von m überführt und jede Invariante ist eine Summe von invarianten Termen. Eine solche Gruppenaktion bezeichnet man auch als *diagonale Gruppenaktion.*

m ist genau dann invariant unter σ, wenn

$$a_1\alpha_1 + \cdots + a_n\alpha_n \equiv 0 \pmod N$$

gilt.

Insbesondere ist $y_i^{d_i} \in T(\mathbf{y})$ mit $d_i = \frac{N}{\gcd(N,\alpha_i)}$ der invariante univariate y_i-Term kleinsten Grades und
$$P = \left\{y_1^{d_1}, \dots, y_n^{d_n}\right\}$$
damit ein System von Primärinvarianten. Jeden anderen invarianten Term $m \in T(\mathbf{y})$ kann man eindeutig in ein Produkt $m = m_0 \cdot m_1$ mit $m_1 \in T(P)$ und
$$m_0 \in \Sigma = \left\{y_1^{a_1} \dots y_n^{a_n} \in T(\mathbf{y}) \mid \sum a_i\alpha_i \equiv 0 \pmod N \text{ und } \forall\, 0 \le a_i < d_i\right\}$$
zerlegen. Σ ist eine endliche Menge (wegen $0 \le a_i < d_i$) und ein System von Sekundärinvarianten. Die Menge aller invarianten Terme aus $T(\mathbf{y})$ zerfällt in die disjunkte Vereinigung der Mengen
$$\dot{\bigcup_{m\in\Sigma}} m \cdot T(P).$$
Da jede Invariante eine Summe invarianter Terme ist, ergibt sich daraus für den Invariantenring $R = K[V]^G$ mit $R_0 = K[P]$ die Hironaka-Zerlegung
$$R = \bigoplus_{m\in\Sigma} m \cdot R_0.$$
Für obiges Beispiel ergibt sich $P = \{y_1, y_2^2, y_3^4, y_4^4\}$,
$$\Sigma = \left\{1, y_3\, y_4, y_2\, y_3^2, y_2\, y_4^2, y_3^2\, y_4^2, y_2\, y_3\, y_4^3, y_2\, y_3^3\, y_4, y_3^3\, y_4^3\right\}$$
und damit für die Hilbertreihe von R
$$H(R,t) = \frac{1 + t^2 + 2t^3 + t^4 + 2t^5 + t^6}{(1-t)(1-t^2)(1-t^4)^2}$$
Die Taylorreihenentwicklung zeigt, dass sich dieselben Dimensionen der homogenen Komponenten ergeben wie in unseren früheren Berechnungen.

```
taylor(f,t=0,10);
```

$$1 + t + 3\,t^2 + 5\,t^3 + 10\,t^4 + 14\,t^5 + 22\,t^6 + 30\,t^7 + 43\,t^8 + 55\,t^9 + O\left(t^{10}\right)$$
Allerdings haben die Primärinvarianten dabei höhere Grade und aus der Menge der konstruierten y-Basisinvarianten kann auch kein anderes Teilsystem als System von Primärinvarianten ausgewählt werden. Wir sehen an diesem Beispiel, dass die Grade der Primärinvarianten nicht nur nicht eindeutig bestimmt sind, sondern selbst die Minimalgrade der Primärinvarianten von der Koordinatenwahl abhängen kann.

Zusammenfassend gilt also der folgende

Satz 17 (Struktursatz über Invarianten einer diagonalen zyklischen Gruppenaktion)

Ist $y_1, \dots, y_n$ eine Basis von V, in der die Aktion der zyklischen Gruppe $G = \langle\sigma\rangle$ diagonal mit $y_i^\sigma = \varepsilon^{\alpha_i}\, y_i,\ i = 1, \dots, n$, ist, und $R = K[\boldsymbol{y}]^G$ der zugehörige Invariantenring, so bildet
$$P = \left\{y_1^{d_1}, \dots, y_n^{d_n}\right\}$$
mit $d_i = \frac{N}{\gcd(N,\alpha_i)}$ ein System von Primärinvarianten kleinstmöglichen Grads,
$$\Sigma = \left\{y_1^{a_1} \dots y_n^{a_n} \in T(\boldsymbol{y}) \mid \forall\, 0 \le a_i < d_i \text{ und } \sum a_i\alpha_i \equiv 0 \pmod N\right\}$$
ein System von Sekundärinvarianten und der Invariantenring besitzt die Hironaka-Zerlegung
$$R = \bigoplus_{m\in\Sigma} m \cdot R_0.$$

4.4 Beweis des Satzes von Molien

Wir wollen im Weiteren eine Gruppe G, die regulär auf einem endlichen Vektorraum V operiert, immer mit der Untergruppe $\{M_g : g \in G\} \subset Gl(V)$ identifizieren und eine solche Gruppe als *Matrixgruppe* bezeichnen.

1. Für eine Matrix A hängen deren Spur $Tr(A)$ und deren Determinante $det(A)$ nicht von der Basiswahl ab.

2. Ist $P : V \to V$ ein Projektionsoperator und M_P dessen Matrix, so gilt $dim_k(P(V)) = Tr(M_P)$: Wegen $V = P(V) \oplus (1 - P)(V)$ können wir eine Basis von V als Vereinigung von Basen aus beiden Komponenten wählen und $Tr(M_P)$ bzgl. dieser Basis berechnen.

3. Der Reynoldsoperator ρ ist ein Projektionsoperator auf allen $[S]_d$. Sind $M_\rho^{(d)}$ und $M_g^{(d)}$ die Matrizen der Aktionen von ρ und $g \in G$ jeweils auf $[S]_d$, so gilt also für die Hilbertreihe des Invariantenrings $R = S^G$

$$H(R,t) = \sum_{d\geq 0} Tr(M_\rho^{(d)})\, t^d = \sum_{d\geq 0} \frac{1}{|G|} \sum_{g\in G} Tr(M_g^{(d)})\, t^d = \frac{1}{|G|} \sum_{g\in G} \left(\sum_{d\geq 0} Tr(M_g^{(d)})\, t^d \right)$$

   und es bleibt nur noch zu zeigen, dass für jedes $g \in G$

$$\sum_{d\geq 0} Tr(M_g^{(d)})\, t^d = \frac{1}{det(E - t\, M_g)}$$

   gilt.

4. Für $g \in G$ existiert eine Basis aus Eigenvektoren $y_1, \ldots, y_n$ mit zugehörigen Eigenwerten $\lambda_1, \ldots, \lambda_n$. In dieser Basis ist M_g diagonal und es gilt

$$det(E - t\, M_g) = \prod_{i=1}^{n} (1 - t\, \lambda_i).$$

5. Die Terme vom Grad d in $T(\mathbf{y})$ bilden eine Basis aus Eigenvektoren von g von $[S]_d$, wobei $y_1^{a_1} \ldots y_n^{a_n}$ den Eigenwert $\lambda_1^{a_1} \ldots \lambda_n^{a_n}$ hat. Also gilt

$$Tr(M_g^{(d)}) = \sum_{a_1+\cdots+a_n=d} \lambda_1^{a_1} \cdot \ldots \cdot \lambda_n^{a_n}$$

   und

$$\sum_{d\geq 0} Tr(M_g^{(d)})\, t^d = \sum_{(a_1,\ldots,a_n)} \lambda_1^{a_1} \cdot \ldots \cdot \lambda_n^{a_n}\, t^{a_1+\cdots+a_n} = \prod_{i=1}^{n} \sum_{a=0}^{\infty} (\lambda_i\, t)^a = \prod_{i=1}^{n} \frac{1}{1 - \lambda_i\, t}\,.$$

4.5 Die Molienreihe von Permutationsdarstellungen

Eine Permutation $\sigma \in S_n$ lässt sich immer als Produkt elementfremder Zyklen darstellen, deren Längen eindeutig bestimmt sind. Ist l_i die Zahl der Zyklen der Länge i in dieser Darstellung (also insbesondere $l_1 + 2\, l_2 + \cdots + n\, l_n = n$), so wird die Folge $(l_1, \ldots, l_n)$ (auch als $1^{l_1} 2^{l_2} \ldots n^{l_n}$ geschrieben) als *Zyklentyp* von σ bezeichnet.

Für Permutationsdarstellungen lässt sich die Molienreihen-Formel auf besonders einfache Weise aufschreiben:

Lemma 2 *Hat die Permutation $g \in S_n$ den Zyklentyp $(l_1, \ldots, l_n)$, so gilt für die zugehörige Permutationsmatrix $M_g \in Gl(n, \mathbb{Z})$*

$$det(E_n - t\, M_g) = \prod_{i=1}^{n} (1 - t^i)^{l_i}\,.$$

Beweis : M_g hat Blockdiagonalstruktur mit Blöcken $D_{a_1}, \ldots, D_{a_k}$, so dass $det(E_n - t\, M_g) = \prod_i det(E_{a_i} - t\, D_{a_i})$ gilt. Für die Matrix D_a gilt $det(E_a - t\, D_a) = 1 - t^a$. □

Beispiele:

$G = C_4$:

$$H(R,t) = \frac{1}{4}\left(\frac{1}{(1-t)^4} + \frac{2}{(1-t^4)} + \frac{1}{(1-t^2)^2}\right) = \frac{t^3 + t^2 - t + 1}{(t^2+1)\cdot(t+1)^2\cdot(t-1)^4}$$

$G = V_4$:

$$H(R,t) = \frac{1}{4}\left(\frac{1}{(1-t)^4} + \frac{3}{(1-t^2)^2}\right) = \frac{t^2 - t + 1}{(t+1)^2\cdot(t-1)^4}$$

$G = D_4$:

$$\begin{aligned} H(R,t) &= \frac{1}{8}\left(\frac{1}{(1-t)^4} + \frac{2}{(1-t^4)} + \frac{3}{(1-t^2)^2} + \frac{2}{(1-t)^2(1-t^2)}\right) \\ &= \frac{t^2 - t + 1}{(t^2+1)\cdot(t+1)^2\cdot(t-1)^4} \end{aligned}$$

$G = A_4$:

$$\begin{aligned} H(R,t) &= \frac{1}{12}\left(\frac{1}{(1-t)^4} + \frac{8}{(1-t)(1-t^3)} + \frac{3}{(1-t^2)^2}\right) \\ &= \frac{t^4 - t^2 + 1}{(t+t^2+1)\cdot(t+1)^2\cdot(t-1)^4} \end{aligned}$$

$G = S_4$:

$$\begin{aligned} H(R,t) &= \frac{1}{24}\left(\frac{1}{(1-t)^4} + \frac{8}{(1-t)(1-t^3)} + \frac{3}{(1-t^2)^2} + \frac{6}{1-t^4} + \frac{6}{(1-t)^2(1-t^2)}\right) \\ &= \frac{1}{(t^2+1)\cdot(t+t^2+1)\cdot(t+1)^2\cdot(t-1)^4} \\ &= \frac{1}{(1-t)(1-t^2)(1-t^3)(1-t^4)} \end{aligned}$$

4.6 Invarianten abelscher Gruppen

Der Struktursatz über die Invarianten einer zyklischen Gruppe lässt sich relativ einfach auf Aktionen abelscher Gruppen erweitern.

Lemma 3 *Sei $G \subset Gl(V)$ eine endliche abelsche Gruppe, die auf einem endlich-dimensionalen k-Vektorrraum V regulär operiert. Dann hat V über einer algebraischen Erweiterung K/k eine Basis $v_1, \ldots, v_n$, die Eigenvektoren bzgl. aller $g \in G$ sind, d.h. die Gruppenaktion ist diagonalisierbar.*

Beweis : Für ein konkretes $g \in G$ hat V über einer solchen Erweiterung K/k eine Basis aus Eigenvektoren.

Genauer: V lässt sich in die direkte Summe $V = \oplus_\lambda V_\lambda$ der Eigenräume $V_\lambda = \{v \in V \ : \ v^g = \lambda\, v\}$ bzgl. der verschiedenen Eigenwerte λ von M_g zerlegen.

Ist $h \in G$ ein anderes Element mit $h \cdot g = g \cdot h$, so lässt h alle diese Eigenräume invariant: Für $v \in V_\lambda$ gilt

$$(v^h)^g = v^{gh} = (v^g)^h = (\lambda\, v)^h = \lambda\, v^h\,,$$

also auch $v^h \in V_\lambda$. Wir können also die Zerlegung $\oplus_\lambda V_\lambda$ zu einer Zerlegung in gemeinsame Eigenräume bzgl. g und h verfeinern und so fortfahren, bis wir alle Erzeugenden von G einbezogen haben. □

Wie im Fall einer zyklischen Gruppenaktion setzen wir $N = |G|$, nehmen eine primitive N-te Einheitswurzel $\varepsilon \in K$ und können dann die Gruppenaktion in der Basis $\mathbf{y}$ als

$$M_g = \begin{pmatrix} \varepsilon^{\alpha_1(g)} & & 0 \\ & \ddots & \\ 0 & & \varepsilon^{\alpha_n(g)} \end{pmatrix}$$

darstellen.

Damit wird der Invariantenring $R = K[V]^G$ wie im Fall einer zyklischen Gruppenaktion von den monomialen Invarianten

$$\{y_1^{a_1} \cdot \ldots \cdot y_n^{a_n} \ : \ a_1\, \alpha_1(g) + \ldots + a_n\, \alpha_n(g) \equiv 0 \pmod N \text{ für alle } g \in G\}$$

aus $T(\mathbf{y})$ als K-Vektorraum erzeugt und es gilt die folgende Verallgemeinerung des Struktursatzes für zyklische Gruppenaktionen.

Satz 18 (Struktursatz über die Invarianten einer abelschen Gruppe)
In der oben eingeführten Basis $y_1, \ldots, y_n$ von V bildet $P = \left\{y_1^{d_1}, \ldots, y_n^{d_n}\right\}$ mit

$$d_i = \frac{N}{\gcd_{\forall g \in G}(N, \alpha_i(g))}$$

ein System von Primärinvarianten kleinstmöglichen Grads,

$$\Sigma = \left\{y_1^{a_1} \ldots y_n^{a_n} \in T(\boldsymbol{y}) \,|\, \forall\ 0 \le a_i < d_i \text{ und } \forall\ g \in G :\ \sum a_i \alpha_i(g) \equiv 0 \pmod N\right\}$$

ein System von Sekundärinvarianten und der Invariantenring besitzt mit $R_0 = K[P]$ die Hironaka-Zerlegung

$$R = \bigoplus_{m \in \Sigma} m \cdot R_0.$$

Beispiel: Eine solche Aktion ist die Permutationsdarstellung der V_4. Die gemeinsamen Eigenvektoren (mit Eigenwerten jeweils ± 1) sind

$$\begin{aligned} y_1 &= x_1 + x_2 + x_3 + x_4 \\ y_2 &= x_1 + x_2 - x_3 - x_4 \\ y_3 &= x_1 - x_2 + x_3 - x_4 \\ y_4 &= x_1 - x_2 - x_3 + x_4\,. \end{aligned}$$

Ein System von Primärinvarianten ist $P = (y_1, y_2^2, y_3^2, y_4^2)$ mit den zugehörigen Sekundärinvarianten $\Sigma = (1, y_2\, y_3\, y_4)$.

5 Cohen-Macaulay-Ringe und die Hironaka-Zerlegung

$R = [R]_0 \oplus [R]_1 \oplus \dots$ sei eine graduierte k-Algebra. Ein maximales System $(\theta_1, \dots, \theta_n)$ von algebraisch unabhängigen homogenen Elementen positiven Grads aus R, das wir im Fall eines Invariantenrings als System von Primärinvarianten bezeichnet hatten, heißt im allgemeinen Fall *homogenes Parametersystem.*

R ist modulendlich über $R_0 = k[\theta_1, \dots, \theta_n]$, lässt sich also als Summe $R = \sum_{m\in\Sigma} m \cdot R_0$ mit homogenen Elementen m schreiben. Die Elemente einer solchen Menge Σ kann man ähnlich wie im Fall abelscher Gruppen durch „Ausfaktorisieren“ von $(\theta_1, \dots, \theta_n)$ gewinnen.

Lemma 4 (Graduiertes Nakayama-Lemma) *Ist $U = [U]_0 \oplus [U]_1 \oplus \dots$ sei eine graduierte k-Algebra mit $[U]_0 = k$, $U_+ = \oplus_{d>0}[U]_d$ das Ideal, welches von den homogenen Elementen positiven Grads erzeugt wird, M ein graduierter U-Modul und $\Sigma \subset M$ eine endliche Menge homogener Elemente, so sind die folgenden beiden Bedingungen äquivalent:*

(1) Σ erzeugt M als U-Modul.

(2) Σ erzeugt M/U_+M als k-Vektorraum.

Insbesondere sind Anzahl und Grade eines minimalen Erzeugendensystems von M als homogener R-Modul durch die Dimensionen der homogenen Komponenten des Vektorraums M/U_+M eindeutig bestimmt.

Beweis : (1) $\Rightarrow$ (2) ist klar.

Für die andere Richtung zeigen wir mit Induktion nach d, dass jedes homogene $g \in M$ vom Grad $deg(g) = d$ in $M_0 = \sum_{m\in\Sigma} m\, U$ liegt. Wegen (2) wissen wir, dass $\alpha_m \in K$ und homogene $a_i \in U_+, h_i \in M$ existieren, so dass

$$g = \sum_{m\in\Sigma} \alpha_m\, m + \sum_i a_i\, h_i$$

gilt, wobei alle Summanden vom Grad d seien (andere würden sich eh wegheben). Wegen $deg(a_i) > 0$ ist aber $deg(h_i) < d$, also $h_i \in M_0$ und damit auch $g \in M_0$. $\square$

Setzen wir $M = R = S^G$ und $U = R_0 = k[P]$, wobei $P = (\theta_1, \dots, \theta_n)$ ein System von Primärinvarianten ist, so sind wir gerade im Fall der Darstellung des Invariantenrings durch Primär- und Sekundärinvarianten. Anzahl und Grade eines minimalen Systems von Sekundärinvarianten sind also für ein vorgegebenes System von Primärinvarianten eindeutig bestimmt. In diesem Fall ist U_+ gerade das von $(\theta_1, \dots, \theta_n)$ erzegute Ideal.

Besonders interessant ist der Fall, dass die Summe $M = \sum m\, U$ eine *direkte* Summe, der U-Modul M also sogar frei ist. Es stellt sich heraus, dass diese Eigenschaft nicht vom konkreten Parametersystem abhängt. Für eine graduierte k-Algebra R sind die folgenden beiden Aussagen äquivalent:

(1) R ist frei über $R_0 = k[\theta_1, \dots, \theta_n]$ für *ein* homogenes Parametersystem $(\theta_1, \dots, \theta_n)$

(2) R ist frei über $R_0 = k[\phi_1, \dots, \phi_n]$ für *jedes* homogene Parametersystem $(\phi_1, \dots, \phi_n)$

Ein solcher Ring heißt *Cohen-Macaulay-Ring* (CM-Ring).

Für ein vorgegebenes Parametersystem $(\theta_1, \dots, \theta_n)$ lässt sich ein CM-Ring R also immer als direkte Summe

$$R = \bigoplus_{m\in\Sigma} m\, R_0$$

darstellen. Nach dem Nakayama-Lemma ist das genau für solche Systeme Σ homogener Elemente der Fall, für welche Σ eine Basis des Vektorraums $R/(\theta_1, \dots, \theta_n)R$ ist.

Satz 19 (Eagon, Hochster, 1971) *Der Invariantenring $R = k[V]^G$ bzgl. einer regulären Aktion einer endlichen Gruppe R auf V ist ein Cohen-Macaulay-Ring.*

Beweis : Wir zeigen hier nur, wie diese Eigenschaft aus der CM-Eigenschaft des Polynomrings $S = k[V]$ folgt. Dazu fixieren wir ein System $P = (\theta_1, \dots, \theta_n)$ von Primärinvarianten und setzen $R_0 = k[P]$.

P ist homogenes Parametersystem sowohl für R als auch für S, da beide Algebren denselben Transzendenzgrad n über k haben. Sei $T = S/(\theta_1, \dots, \theta_n)S$ der aus dem Nakayama-Lemma bekannte Vektorraum.

Die Einbettung $\phi : R \to S$ induziert eine Abbildung $\phi : R \to S/(\theta_1, \dots, \theta_n)S$ mit dem Kern $Ker(\phi) = R \cap (\theta_1, \dots, \theta_n)S$. Dieser Kern fällt mit $(\theta_1, \dots, \theta_n)R$ zusammen: Ist $f = \sum_i s_i\theta_i$ die Darstellung der Invarianten $f \in R$ als S-lineare Summe der θ_i, so liefert die Anwendung des Reynoldsoperators wegen $f^\rho = f, \theta_i^\rho = \theta_i$ die R-lineare Summe $f = \sum_i s_i^\rho \theta_i$.

Damit induziert ϕ eine Einbettung des Vektorraums $T' = R/(\theta_1, \dots, \theta_n)R$ in T. Wählen wir eine Basis Σ' von T' und ergänzen sie zu einer Basis Σ von T, so ist nach dem Nakayama-Lemma

$$R = \sum_{m\in\Sigma'} m\, R_0 \quad \text{und} \quad S = \sum_{m\in\Sigma} m\, R_0.$$

Aus der CM-Eigenschaft von S folgt, dass die Summendarstellung von S eine direkte Summe ist. Wegen $\Sigma' \subset \Sigma$ ist damit auch die Summendarstellung von R direkt und R ein Cohen-Macaulay-Ring. $\square$

Korollar 2 *Ist $R = k[V]^G$ ein Invariantenring bzgl. einer regulären Aktion einer endlichen Gruppe R auf V mit einem System P von Primärinvarianten und einem zugehörigen System Σ von Sekundärinvarianten, so besitzt R über $R_0 = k[P]$ die Hironaka-Zerlegung*

$$R = \bigoplus_{m\in\Sigma} m \cdot R_0$$

und für die Hilbertreihe gilt

$$H(R,t) = \left(\sum_{m\in\Sigma} t^{deg(m)}\right) H(R_0,t)\,.$$

Weder Primär- noch Sekundärinvarianten sind eindeutig bestimmt. Aus dem Satz von Molien ergeben sich aber einige Restriktionen auf mögliche Grade:

Satz 20 *Ist $P = (\theta_1, \dots, \theta_n)$ ein System von Primärinvarianten für $R = k[V]^G$ und $d_i = deg(\theta_i)$, so gilt:*

(1) Die Grade (mit Vielfachheiten) der zugehörigen Sekundärinvarianten $m \in \Sigma$ ergeben sich eindeutig aus der Formel

$$H(R,t) \cdot \prod_i (1 - t^{d_i}) = \sum_{m\in\Sigma} t^{deg(m)}.$$

(2) Die Zahl der zugehörigen Sekundärinvarianten ist gleich

$$|\Sigma| = \frac{d_1 \cdot \ldots \cdot d_n}{|G|}.$$

Insbesondere ist $|G|$ ein Teiler von $d_1 \cdot \ldots \cdot d_n$.

Beweis : Die erste Aussage ergibt sich sofort aus obigem Korollar.

Zum Beweis von (2) rechnen wir in (1) den Grenzwert $t \mapsto 1$ aus. Auf der linken Seite enthält $\prod_i (1-t^{d_i})$ den Faktor $(1-t)^n$, so dass in der Molienformel für $H(R,t)$ nur der Summand für $g = e$ einen nicht verschwindenden Beitrag zum Grenzwert liefert, und zwar

$$\frac{1}{|G|} \prod_i \left(\frac{1-t^{d_i}}{1-t} \right) \Big|_{t \mapsto 1} .$$

Auf der rechten Seite können wir $t = 1$ direkt einsetzen und erhalten $|\Sigma|$. □

Wir können diese Formeln verwenden, um aus der Hilbertreihe Informationen über mögliche Grade von Primär- und Sekundärinvarianten abzuleiten. Betrachten wir als Beispiel wieder die Permutationsdarstellungen der Untergruppen der S_4.

Beispiele:

$G = C_4$:

$$H(R,t) = \frac{t^3 + t^2 - t + 1}{(t^2+1) \cdot (t+1)^2 \cdot (t-1)^4} = \frac{1 + 2\,t^3 + t^4}{(1-t^4) \cdot (1-t^2)^2 \cdot (t-1)}$$

hat das einfachere System $P = (e_1, e_{2a}, e_{2b}, e_4)$ von Primärinvarianten und dann die Zerlegung

$$R = k[P] \oplus e_3 \cdot k[P] \oplus e_{3a} \cdot k[P] \oplus e_{4b} \cdot k[P]$$

$G = V_4$:

$$H(R,t) = \frac{t^2 - t + 1}{(t+1)^2 \cdot (t-1)^4} = \frac{1 + t^3}{(1-t^3) \cdot (1-t^2)^2 \cdot (1-t)}$$

hat mit $P = (e_1, e_{2a}, e_{2b}, e_{2c})$ die Zerlegung $R = k[P] \oplus e_3 \cdot k[P]$

$G = D_4$:

$$H(R,t) = \frac{t^2 - t + 1}{(t^2+1) \cdot (t+1)^2 \cdot (t-1)^4} = \frac{1 + t^3}{(1-t^4) \cdot (1-t^2)^2 \cdot (t-1)}$$

hat mit $P = (e_1, e_{2a}, e_{2b}, e_4)$ die Zerlegung $R = k[P] \oplus e_3 \cdot k[P]$

$G = A_4$:

$$H(R,t) = \frac{t^4 - t^2 + 1}{(t+t^2+1) \cdot (t+1)^2 \cdot (t-1)^4} = \frac{1 + t^6}{(1-t^3) \cdot (1-t^2)^2 \cdot (t-1)}$$

hat mit $P = (e_1, e_2, e_3, e_4)$ und $\Delta = \prod_{i<j} (x_i - x_j)$ die Zerlegung $R = k[P] \oplus \Delta \cdot k[P]$.

Haben wir zu einem System von Primärinvarianten $P = (\theta_1, \ldots, \theta_n)$ ein System Σ von Sekundärinvarianten der richtigen Anzahl und Grade gefunden, so müssen wir für den Nachweis der Vollständigkeit wegen des Nakayama-Lemmas nur prüfen, ob die Sekundärinvarianten eine k-Basis von $T' = R/Id(P)\,R$ bilden. Wegen der Einbettung $T' \subset T$ (siehe den Beweis des Satzes von Eagon/Hochster) können wir diese Rechnungen über S ausführen:

Lemma 5 *In obiger Situation ist Σ genau dann ein vollständiges System von Sekundärinvarianten, wenn die $m \in \Sigma$ im k-Vektorraum $S/Id(P)\,S$ linear unabhängig sind.*

Im Vektorraum $S/Id(P)\,S$ kann effektiv gerechnet werden, wenn man eine Gröbnerbasis $G = \texttt{gbasis}(P)$ kennt. Die $m \in \Sigma$ sind genau dann linear unabhängig in $S/Id(P)\,S$, wenn die Normalformen $\texttt{NF}(m, G)$ linear unabhängig über k sind. Darauf soll hier jedoch nicht weiter eingegangen werden.

6 Weitere Beispiele

6.1 Die Drehinvarianten ebener Vielecke

$C_n \subset Gl(2, \mathbb{R})$ wird erzeugt von σ mit der Matrix

$$M_\sigma = \begin{pmatrix} \cos(\frac{2\pi}{n}) & \sin(\frac{2\pi}{n}) \\ -\sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix}$$

Wegen

$$det(E_2 - t\,M_\sigma^k) = \left(1 - t\,\cos\left(\frac{2k\pi}{n}\right)\right)^2 + t^2\,\sin\left(\frac{2k\pi}{n}\right)^2 = 1 - 2t\cos\left(\frac{2k\pi}{n}\right) + t^2$$

ergibt sich für die Molienreihe des Invariantenrings $R_n = k[x_1, x_2]^{C_n}$ die Formel

$$H(R_n, t) = \frac{1}{n} \sum_{k=0}^{n-1} \frac{1}{1 - 2t\cos\left(\frac{2k\pi}{n}\right) + t^2}\,.$$

Schauen wir uns das zunächst für den Fall $n = 3$ an.

$$H(R_3, t) = \frac{1}{3}\left(\frac{1}{(1-t)^2} + \frac{2}{1+t+t^2}\right) = \frac{1 - t + t^2}{(1-t)(1-t^3)}\,.$$

Mit Blick auf den Satz über die Hilbertreihe einer Hironaka-Zerlegung suchen wir eine Darstellung mit Zählerpolynom in $\mathbb{N}[t]$.

$$H(R_3, t) = \frac{1 + t^3}{(1-t^2)(1-t^3)}\,.$$

Diese Darstellung suggeriert, dass es ein System von Primärinvarianten mit Grad 2 und 3 und dazu Sekundärinvarianten im Grad 0 und 3 gibt.

Rechnungen mit MuPAD: M eingeben, systematische Suche nach den Invarianten. Ad-hoc-Suche.

$$\begin{aligned} e_1 &= 2 * \texttt{Reynolds}(x_1^2, G) = x_1^2 + x_2^2 \\ e_2 &= 4 * \texttt{Reynolds}(x_1^3, G) = x_1(x_1^2 - 3\,x_2^2) \\ e_3 &= 4 * \texttt{Reynolds}(x_2^3, G) = x_2(x_2^2 - 3\,x_1^2) \end{aligned}$$

Entspricht mit $R_0 = k[e_1, e_2]$ der Hironaka-Zerlegung $R = R_0 \oplus e_3\,R_0$. $e_3^2 \in [R]_6$ kann durch die k-Basis $(e_1^3, e_2^2, e_2 e_3)$ ausgedrückt werden:

```
linTest([e_3^2,e_1^3,e_2^2,e_2*e_3],vars);
```

führt auf die Relation $e_2^2 + e_3^2 = e_1^3$, so dass der Invariantenring auch durch Erzeugende und Relationen als $R = k[E_1, E_2, E_3]/Id(E_2^2 + E_3^2 - E_1^3)$ dargestellt werden kann.

Wir können neben dem System (e_1, e_2) auch das System (e_2, e_3) als Primärinvarianten nehmen, denn die Hilbertreihe kann auch als

$$H(R_3, t) = \frac{1+t^3}{(1-t^2)(1-t^3)} = \frac{1-t^6}{(1-t^2)(1-t^3)^2} = \frac{1+t^2+t^4}{(1-t^3)^2}$$

geschrieben werden. Entspricht mit $R_0' = k[e_2, e_3]$ der Hironaka-Zerlegung $R = R_0' \oplus e_1\, R_0' \oplus e_1^2\, R_0'$.

Die Invarianten e_2 und e_3 lassen auch eine geometrische Interpretation zu. Es sind die Orbitprodukte von $l \cdot l^\sigma \cdot l^{\sigma^2}$ von $l = x_1$ und $l = x_2$.

Der Ansatz funktioniert auch allgemein: Invarianten $e_1 = x_1^2 + x_2^2$ sowie $e_2 = \prod x_1^{\sigma^k}, e_3 = \prod x_2^{\sigma^k}$. Bleibt zu prüfen, ob das alles ist.

Anwendung der Theorie

Eine Basis aus Eigenvektoren ist (auch für allgemeines n) $y_1 = x_1 + \mathrm{i}\, x_2, y_2 = x_1 - \mathrm{i}\, x_2$ mit Eigenwerten $\varepsilon = e^{2\pi\mathrm{i}/n}$ und ε^{-1}.

Darstellung des Invariantenrings als $R = k[y_1^n, y_2^n, y_1\, y_2]$ mit Primärinvarianten (y_1^n, y_2^n) und Sekundärinvarianten $\Sigma = \{(y_1 y_2)^i, i = 0, \ldots, n-1\}$. Molienreihe dazu ist

$$H(R_n, t) = \frac{1+t^2+\cdots+t^{2n-2}}{(1-t^n)^2} = \frac{1-t^{2n}}{(1-t^n)^2(1-t^2)}$$

Dieselben Invarianten in der Basis (x_1, x_2): $y_1 y_2 = x_1^2 + x_2^2$. y_1 und y_2 sind komplex konjugiert und damit $y_1^n = e_2 + \mathrm{i}\, e_3, y_2^n = e_2 - \mathrm{i}\, e_3$. Allerdings ist (e_1, e_2) auch ein System von Primärinvarianten. R hat bzgl. dieses Systems wieder eine einfachere Darstellung.

6.2 Die Dreh- und Spiegelungsinvarianten ebener Vielecke

Die Matrixgruppe wird durch $C_n = \langle\sigma\rangle$ und eine weitere Spiegelung $\tau = \{x \mapsto x, y \mapsto -y\}$ erzeugt. $\sigma^k\tau$ sind die anderen Spiegelungen. Jede Spiegelung hat die Eigenwerte $(+1, -1)$, also ist $det(E_2 - t\, M_\tau) = 1 - t^2$.

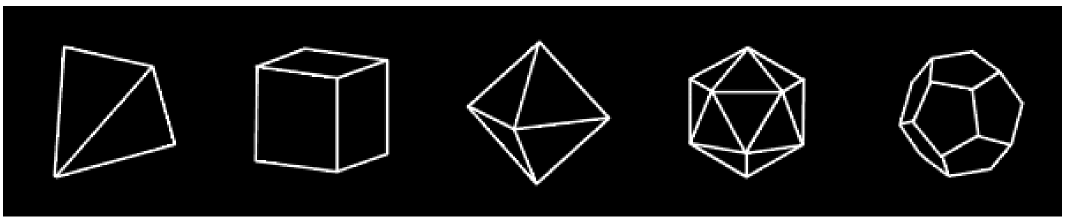
Wir bekommen für die Hilbertreihe (mit Invariantenring $R' = k[x_1, x_2]^{C_n}$)

$$H(R, t) = \frac{1}{2} H(R', t) + \frac{n}{2n}\frac{1}{1-t^2} = \frac{1}{2}\left(\frac{1-t^{2n}}{(1-t^n)^2(1-t^2)} + \frac{1}{1-t^2}\right) = \frac{1}{(1-t^n)(1-t^2)}$$

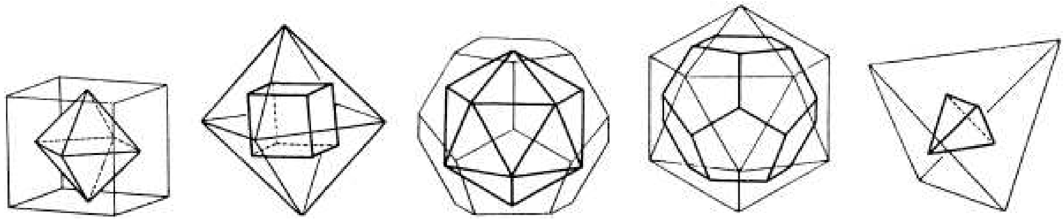
Nach dieser Formel müsste es ein System von Primärinvarianten im Grad 2 und n geben, welche den Invariantenring bereits vollständig erzeugen.

Aussehen von M_τ in den Basen (x_1, x_2) und (y_1, y_2). Also sind die gesuchten Primärinvarianten $e_1 = y_1 y_2 = x_1^2 + x_2^2$ und $e_2 = \frac{1}{2}(y_1^n + y_2^n)$.

6.3 Die Invarianten der Drehgruppen der platonischen Körper



Die fünf Platonischen Körper:
Tetraeder, Hexaeder (Würfel), Oktaeder, Dodekaeder und Ikosaeder



Dualität zwischen den fünf Platonischen Körpern

Damit sind Invarianten in $S = k[x_1, x_2, x_3]$ bzgl. der Drehgruppen T des Tetraeders, O des Oktaeders und D des Dodekaeders zu untersuchen. Eine solche Invariante ist stets $e_1 = x_1^2 + x_2^2 + x_3^2$.

Die Drehgruppe T des Tetraeders

Beschreibung der Drehgruppe

Die Drehgruppe des Tetraeders enthält $4 \cdot 3 = 12$ Elemente, und zwar

- $4 \cdot 2 = 8$ Drehungen E mit Achse durch Ecke und gegenüberliegende Seitenmitte um $\pm 120^o$.
- 3 Drehungen K mit Achse durch gegenüberliegende Kantenmitten um $\pm 180^o$.
- Die identische Abbildung.

Die zugehörige Molienreihen

Eine Drehung im Raum um den Winkel $\alpha = \frac{2\pi}{k}$ liefert

$$det(E_3 - t\,M_\alpha) = (1-t)\left(1 - 2t\cos\left(\frac{2k\pi}{k}\right) + t^2\right).$$

Die Hilbertreihe des Invariantenrings berechnet sich daraus nach der Molienformel zu

$$\begin{aligned} H(S^T, t) &= \frac{1}{12}\left(\frac{1}{(1-t)^3} + \frac{8}{(1-t)(1+t+t^2)} + \frac{3}{(1-t)(1+t)^2}\right) \\ &= \frac{1-t^2+t^4}{(1-t)^3(1+t)^2(1+t+t^2)} \\ &= \frac{1+t^6}{(1-t^2)(1-t^3)(1-t^4)} \end{aligned}$$

Es sollte also ein System von Primärinvarianten vom Grad 2,3,4 geben, dazu Sekundärinvarianten im Grad 0 und 6.

Bestimmung von Invarianten

Koordinatendarstellung der Drehgruppe in geeignetem Koordinatensystem: Achsen durch gegenüberliegende Kantenmitten stehen paarweise senkrecht aufeinander, also nehmen wir diese Achsen als Koordinatenachsen.

Eckpunkte haben dann die Koordinaten $(1,1,1), (1,-1,-1), (-1,1,-1), (-1,-1,1)$ und durch die 12 Drehungen werden die Koordinatenachsen mit ihren Orientierungen vertauscht.

Beschreibung der Matrixdarstellung von T in der Demo-Datei. Wir erhalten die 12 Elemente in Subrules-Darstellung als

$$\begin{array}{ccc} [x_1 = x_1, x_2 = x_2, x_3 = x_3] & [x_1 = x_2, x_2 = x_3, x_3 = x_1] & [x_1 = x_3, x_2 = x_1, x_3 = x_2] \\ [x_1 = x_1, x_2 = -x_2, x_3 = -x_3] & [x_1 = x_2, x_2 = -x_3, x_3 = -x_1] & [x_1 = x_3, x_2 = -x_1, x_3 = -x_2] \\ [x_1 = -x_1, x_2 = x_2, x_3 = -x_3] & [x_1 = -x_1, x_2 = -x_2, x_3 = x_3] & [x_1 = -x_2, x_2 = x_3, x_3 = -x_1] \\ [x_1 = -x_2, x_2 = -x_3, x_3 = x_1] & [x_1 = -x_3, x_2 = x_1, x_3 = -x_2] & [x_1 = -x_3, x_2 = -x_1, x_3 = x_2] \end{array}$$

Invarianten sind dann $e_1 = 3\,\texttt{Reynolds}(x_1^2, T), e_2 = x_1x_2x_3$ (in jedem Element von T ändert sich das Vorzeichen bei jeweils genau zwei Elementen) sowie $e_3 = 3\,\texttt{Reynolds}(x_1^2x_2^2, T)$ oder $e_{3a} = 3\,\texttt{Reynolds}(x_1^4, T)$. Mit

```
vars:=[x1,x2,x3];
solve({e_1,e_2,e_3},vars);
```

prüft man wieder, dass es sich in der Tat um ein System von Primärinvarianten handelt.

Die Invariante vom Grad 4 ergibt sich auch aus dem Orbitprodukt der Linearform $l = x_1+x_2+x_3$, die der Koordinatendarstellung eines der Eckpunkte entspricht.

$$\begin{aligned} e_3' &= (x_1 + x_2 + x_3)(x_1 - x_2 - x_2)(-x_1 + x_2 + x_3)(-x_1 - x_2 + x_3) \\ &= x_1^4 + x_2^4 + x_3^4 - 2\,x_1^2\,x_2^2 - 2\,x_1^2\,x_3^2 - 2\,x_2^2\,x_3^2 \\ &= e_1^2 - 4\,e_3 \end{aligned}$$

Die Invariante e_2 hat ebenfalls eine geometrische Bedeutung. Sie ist das „halbe" Orbitprodukt der Linearformen, welche den Koordinaten der Kantenmitten entsprechen. Das ganze Orbit besteht aus den Linearformen $(x_1, x_2, x_3, -x_1, -x_2, -x_3)$.

Bleibt noch die fehlende Sekundärinvariante vom Grad 6 zu finden, die nicht bereits in $R_0 = k[e_1, e_2, e_3]$ enthalten ist.

```
U_6:=map({op(Terme(6,vars))}, Reynolds, T);
B_6:=map([e_1^3,e_2^2,e_1*e_3],expand);
```

Es stehen zwei Kandidaten zur Auswahl,

$$\begin{aligned} e_{4a} &= 3\,\texttt{Reynolds}(x_1^2\,x_2^4, T) = x_1^2\,x_2^4 + x_1^4\,x_3^2 + x_2^2\,x_3^4 \text{ und} \\ e_{4b} &= 3\,\texttt{Reynolds}(x_1^2\,x_2^4, T) = x_1^4\,x_2^2 + x_1^2\,x_3^4 + x_2^4\,x_3^2\,. \end{aligned}$$

Da $e_{4a} + e_{4b} \in [R_0]_6$, wählen wir $e_4 = e_{4a} - e_{4b}$. Das sieht aus wie ein Determinantenausdruck und ist auch einer:

$$e_4 = -det \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2x_3 & x_1x_3 & x_1x_2 \\ x_1^3 & x_2^3 & x_3^3 \end{pmatrix}$$

Das ist im Wesentlichen die Jacobimatrix von $[e_1, e_2, e_{3a}]$.

Die Drehgruppe O des Oktaeders

Beschreibung der Drehgruppe

Die Drehgruppe des Oktaeders enthält $6 \cdot 4 = 24$ Elemente, und zwar

- $3 \cdot 2 = 6$ Drehungen E mit Achse durch gegenüberliegende Ecken um $\pm 90^o$.
- 3 Drehungen E_0 mit Achse durch gegenüberliegende Ecken um 180^o.
- $4 \cdot 2 = 8$ Drehungen S mit Achse durch gegenüberliegende Seitenmitten um $\pm 120^o$.
- 6 Drehungen K mit Achse durch gegenüberliegende Kantenmitten um 180^o.
- Die identische Abbildung.

Die zugehörige Molienreihen

$$\begin{aligned} H(S^O,t) &= \frac{1}{24}\left(\frac{1}{(1-t)^3}+\frac{8}{(1-t)(1+t+t^2)}+\frac{3+6}{(1-t)(1+t)^2}+\frac{6}{(1-t)(1+t^2)}\right) \\ &= \frac{1-t^3+t^6}{(1-t)^3(1+t)^2(1+t^2)(1+t+t^2)} \\ &= \frac{1+t^9}{(1-t^2)(1-t^4)(1-t^6)} \end{aligned}$$

Leitlinie bei der Umformung waren neben der Taylorreihe solche Grade d_1, d_2, d_3 der Primärinvarianten, so dass $24 \mid d_1\, d_2\, d_3$ gilt.

Es sollte also ein System von Primärinvarianten vom Grad 2,4,6 geben, dazu Sekundärinvarianten im Grad 0 und 9.

Bestimmung von Invarianten

Invarianten sind

$$e_1 = x_1^2+x_2^2+x_3^2,\ e_2 = x_1^2x_2^2+x_1^2x_3^2+x_2^2x_3^2,\ e_3 = x_1^2x_2^2x_3^2$$

oder

$$e_1 = x_1^2+x_2^2+x_3^2,\ e_2' = x_1^4+x_2^4+x_3^4,\ e_3' = x_1^6+x_2^6+x_3^6.$$

```
vars:=[x1,x2,x3];
f:=combinat::permutations::toMatrix([2,3,1]); /* Flächendrehung */
e:=Dom::Matrix()([[1,0,0],[0,0,1],[0,-1,0]]); /* Eckendrehung */
k:=Dom::Matrix()([[0,0,1],[0,-1,0],[1,0,0]]); /* Kantendrehung */

m1:={e^i*f^j$j=0..2$i=0..3}; nops(%);
m2:={e^l*k*e^i*f^j$l=0..3$j=0..2$i=1..2};
MO:=m1 union m2;
G:=map(MO,matrix2subrules,vars);
e_1:=3*Reynolds(x1^2,G);
e_2:=3*Reynolds(x1^4,G);
e_3:=3*Reynolds(x1^6,G);
```

Die Invarianten vom Grad 4 und 6 können auch wieder geometrisch interpretiert werden; sie haben enge Beziehung zum „halben“ Orbitprodukt der (Vektoren zu den) Mitten der Seitenflächen (Gard 4) bzw. zum Orbitprodukt der Eckpunkte (Grad 6).

Die Sekundärinvariante bekommt man als

```
e_4:=6*Reynolds(x1^5*x2^3*x3,G);
```

$$e_4 = x_1\,x_2^5\,x_3^3 - x_1\,x_2^3\,x_3^5 + x_1^3\,x_2\,x_3^5 - x_1^3\,x_2^5\,x_3 - x_1^5\,x_2\,x_3^3 + x_1^5\,x_2^3\,x_3$$

Sieht wieder aus wie eine Determinante und ist auch eine:

$$-e_4 = det\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1^3 & x_2^3 & x_3^3 \\ x_1^5 & x_2^5 & x_3^5 \end{pmatrix}$$

Ist wieder die Determinante der Jacobimatrix von $[e_1, e_2, e_3]$.

Dahinter verbirgt sich ein allgemeiner Zusammenhang:

Satz 21 *Ist* $(\theta_1, \ldots, \theta_n)$ *ein System von Primärinvarianten und* $J = Jacobi(\theta_1, \ldots, \theta_n) \in S$ *die Detrminante der zugehörigen Jacobimatrix, so gilt* $J^g = det(M_g)^{-1}\, J$ *für* $g \in G$*, d.h.* J *ist eine Semi-Invariante zum Charakter* $g \mapsto det(M_g)^{-1}$.

BEWEIS : Setzen wir $y_i = x_i^g$, dann ist

$$\left(\frac{\partial\theta_i}{\partial x_j}\right)^g \overset{(1)}{=} \frac{\partial\theta_i^g}{\partial y_j} \overset{(2)}{=} \frac{\partial\theta_i}{\partial y_j} = \sum_k \frac{\partial\theta_i}{\partial x_k}\,\frac{\partial x_k}{\partial y_j},$$

also

$$\left\|\left(\frac{\partial\theta_i}{\partial x_j}\right)^g\right\| = \left\|\frac{\partial\theta_i}{\partial x_k}\right\| \cdot \left\|\frac{\partial x_k}{\partial y_j}\right\| = \left\|\frac{\partial\theta_i}{\partial x_k}\right\| \cdot M_g^{-1}\,.$$

(1) ergibt sich aus der Definition der Ableitung und (2) gilt wegen $\theta_i^g = \theta_i$. □
In unserem Fall gilt $det(M_g) = 1$, d.h. diese Semiinvariante ist eine Invariante.

Die Drehgruppe D des Dodekaeders

Beschreibung der Drehgruppe

Die Drehgruppe des Dodekaeders enthält $12 \cdot 5 = 60$ Elemente, und zwar

- $10 \cdot 2 = 20$ Drehungen E mit Achse durch gegenüberliegende Ecken um $\pm 120^o$.
- $6 \cdot 4 = 24$ Drehungen S_i mit Achse durch gegenüberliegende Seitenmitten um $i \cdot 72^o, i = 1, 2, 3, 4$.
- 15 Drehungen K mit Achse durch gegenüberliegende Kantenmitten um 180^o.
- Die identische Abbildung.

Die zugehörige Molienreihen

$$H(S^D, t) = \frac{1}{60}\left(\frac{1}{(1-t)^3} + \frac{20}{(1-t)(1+t+t^2)} + \frac{15}{(1-t)(1+t)^2} + \frac{6\,f_s}{1-t}\right)$$

mit

$$f_s = \sum_{k=1}^{4} \frac{1}{1 - 2\cos(2\,k\pi/5)\,t + t^2} = \frac{4t^2 + 2t + 4}{t^4 + t^3 + t^2 + t + 1}\,,$$

woraus sich

$$H(R_D, t) = \frac{1 + t - t^3 - t^4 - t^5 + t^7 + t^8}{(1+t+t^2)\,(1+t+t^2+t^3+t^4)\,(1+t)^2\,(1-t)^3}$$

ergibt. Nun schauen wir uns die Taylorreihe an:

```
taylor(h,t=0,20);
```

$$1 + t^2 + t^4 + 2\,t^6 + 2\,t^8 + 3\,t^{10} + 4\,t^{12} + 4\,t^{14} + t^{15} + 5\,t^{16} + t^{17} + 6\,t^{18} + t^{19} + O\left(t^{20}\right)$$

Guter Tipp für die Grade von Primärinvarianten sind damit $d_1 = 2, d_2 = 6, d_3 = 10$, dann ist wieder $m = \frac{d_1 d_2 d_3}{|D|} = 2$.

```
normal(h*(1-t^2)*(1-t^6)*(1-t^10));
```

ergibt $1 + t^{15}$ und damit

$$H(R_D, t) = \frac{1 + t^{15}}{(1 - t^2)\,(1 - t^6)\,(1 - t^{10})}$$

Geometrische Suche nach Invarianten in den entsprechenden Graden. Gute Kandidaten sind $e_1 = x_1^2 + x_2^2 + x_3^2$, das „halbe“ Orbitprodukt zu den Eckpunkten des Dodekaeders (Grad 6) sowie das „halbe“ Orbitprodukt zu den Seitenmitten des Dodekaeders (Grad 10). Die Semiinvariante vom Grad 15 kann wieder als Jacobische bestimmt werden. Ein guter Kandidat ist ebenfalls das „halbe“ Orbitprodukt zu den Kantenmitten.

6.4 Invarianten der Dreh- und Spiegelungsgruppen der platonischen Körper

Bisher haben wir nur die Drehgruppen der platonischen Körper betrachtet. Wie im Fall der ebenen regelmäßigen Vielecke können wir jeweils auch die Gruppe der Drehungen und Spiegelungen betrachten, die wir mit $\widetilde{T}, \widetilde{O}$ und $\widetilde{D}$ bezeichnen wollen.

Die Gruppenordnung müsste jeweils ein Vielfaches der Gruppenordnung von T, O resp. D sein. Da eine Spiegelung durch die Angabe eines Punkt-Bildpunkt-Paares $P \neq P'$ eindeutig bestimmt ist (die Spiegelungsebene steht im Mittelpunkt von PP' senkrecht auf dieser Verbindungsstrecke), können wir die Anzahl Spiegelungen, die einen der platonischen Körper invariant lassen, leicht bestimmen. Diese Anzahlen sind

- 6 beim Tetraeder (eine Spiegelung pro Kante, welche die Endpunkte der Kante vertauscht),
- 9 beim Oktaeder (zu jedem der 6 Paare gegenüberliegender Kanten sowie zu jedem der 3 Paare gegenüberliegender Eckpunkte eine solche Spiegelung),
- 15 beim Dodekaeder (die Spiegelungsebenen enthalten jeweils ein Paar gegenüberliegender Kanten und gehen durch Seitenmitte und gegenüberliegenden Eckpunkt der angrenzenden Fünfecke),

also jeweils genau so viele wie der Grad der Sekundärinvariante e_4 im jeweiligen Beispiel angibt.

In keinem der Fälle kommen also genügend Spiegelungen zusammen, um wie im Fall $n = 2$ die gesamte Gruppe der Drehungen und Spiegelungen zu beschreiben.

Das ist im **Fall des Oktaeders** auch nicht verwunderlich, da die Punktspiegelung π mit der Matrix

$$M_\pi = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

in der von den Spiegelungen erzeugten Gruppe liegt, aber weder eine Drehung noch eine Spiegelung ist.

Die Nebenklasse $M_2 = \pi \cdot O$ enthält alle sechs Spiegelungen (sie werden hier als diejenigen Matrizen herausgefiltert, die nur zwei Eigenwerte enthalten)

```
p:=Dom::Matrix()([[-1,0,0],[0,-1,0],[0,0,-1]]); /* Punktspiegelung */
m2:=map(MO,x->p*x);
select(m2,x->nops(linalg::eigenvalues(x))=2);
```

so dass $\widetilde{O}$ die Gruppe ist, die von O und π erzeugt wird. π normalisiert O, d.h. es gilt $\pi^{-1}\, O\, \pi = O$, so dass wegen $\pi^2 = e$ die Menge $O \cup \pi\, O$ multiplikativ abgeschlossen ist und damit $\widetilde{O} = O \cup \pi\, O$ gilt.

```
m3:=map(MO,x->p*x*p);
_minus(m3,MO); _minus(MO,m3);
```

$S^{\widetilde{O}}$ besteht also aus allen Dreh-Invarianten $f \in S^O$, die auch unter π invariant bleiben. Offensichtlich gilt für homogene $f \in S$ die Beziehung $f^\pi = (-1)^{\deg(f)} f$.

Wir hatten für die Drehinvarianten des Oktaeders die Zerlegung $S^O = R_0 \oplus e_4 \cdot R_0$ mit $R_0 = \mathbb{Q}[e_1, e_2, e_3]$ gefunden, in der R_0 die homogenen Invarianten geraden Grads und $e_4 \cdot R_0$ diejenigen ungeraden Grads enthält. Es folgt $S^{\widetilde{O}} = R_0$ und dieser Invariantenring lässt sich als Algebra allein von den Primärinvarianten $e_1, 2_e, e_3$ erzeugen, ist also wie im Fall der Permutationsinvarianten der Gruppe $G = S_n$ isomorph zu einem freien Polynomring.

Ähnliches gilt im **Fall des Dodekaeders**, da π das Dodekaeder ebenfalls invariant lässt und S^T eine Struktur hat, die analog der von S^O ist. Auch hier ist der Invariantenring $S^{\widetilde{T}}$ isomorph zu einem freien Polynomring.

Etwas komplizierter ist der **Fall des Tetraeders**, da dieses nicht unter π invariant ist. Eine der 6 Spiegelungen τ ist durch die Matrix

$$M_\tau = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

gegeben. Die Nebenklasse $\tau \cdot T$ enthält auch die anderen 5 Spiegelungen

```
t:=Dom::Matrix()([[1,0,0],[0,0,1],[0,1,0]]); /* Spiegelung */
m4:=map(MT,x->t*x); /* Nebenklasse von MT */
select(m4,x->nops(linalg::eigenvalues(x))=2);
```

und ist zusammen mit T bereits die ganze Dreh- und Spiegelungsgruppe: $\widetilde{T} = T \cup \tau T$.

```
m5:=map(MT,x->u*x*u);
_minus(m5,MT); _minus(MT,m5);
```

Da die früher berechneten Drehinvarianten $e_1, e_2, e_3 \in S^T$ unter τ invariant sind, aber $e_4^\tau = -e_4$ gilt, haben wir auch in diesem Fall $S^{\widetilde{T}} = \mathbb{Q}[e_1, e_2, e_3]$, d.h. der Invariantenring ist ebenfalls isomorph zu einer freien Polynomalgebra.

7 Der Satz über die Invarianten von Reflektionsgruppen

Die Gruppen $\widetilde{T}, \widetilde{O}$ und $\widetilde{D}$ sind ebenso wie die Permutationsdarstellung der S_n Matrixgruppen, deren Elemente sich als Produkte von Spiegelungen darstellen lassen. Die zugehörigen Invariantenringe waren in allen Beispielen isomorph zu freien Polynomringen, ließen sich als Algebra also allein aus einem System von Primärinvarianten erzeugen.

In diesem Kapitel werden wir zeigen, dass dies generell für durch Spiegelungen erzeugbare Matrixgruppen gilt und diese Eigenschaft solche Gruppen sogar charakterisiert: Ein Invariantenring lässt sich als Algebra genau dann aus einem System von Primärinvarianten erzeugen, wenn die Matrix-Gruppe durch Pseudoreflektionen generiert werden kann.

$\sigma \in Gl(V)$ heißt *Pseudoreflektion*, wenn $Ker(\sigma - 1)$ eine $(n-1)$-dimensionale Hyperebene ist, d.h. $n-1$ Eigenwerte von M_σ gleich 1 sind. Eine Spiegelung zeichnet sich dadurch aus, dass der verbleibende Eigenwert -1 ist. Für Pseudoreflektionen in endlichen Gruppen kann dieser Eigenwert allgemeiner eine Einheitswurzel sein.

Zusammenhang zur Hilbertreihe: Pseudoreflektionen $\sigma \in G$ sind diejenigen Elemente, deren Beitrag in der Molienformel an der Stelle $t = 1$ einen Pol der Ordnung $n-1$ liefert. Einen

Pol der Ordnung n trägt nur das Einselement $e \in G$ bei. Für Pseudoreflektionen $\sigma \in G$ gilt $det(E_n - t\,M_\sigma) = (1-t)^{n-1}(1 - t\,det(M_\sigma))$.
Betrachten wir für $R = S^G$ die Darstellung von

$$F(t) = H(R,t)\,(1-t)^n = \frac{1}{|G|}\left(1 + a_{n-1}\,(1-t) + O\left((1-t)^2\right)\right),$$

so ergibt sich $a_{n-1} = \sum \frac{1}{1-det(M_\sigma)}$, wobei die Summe über alle Pseudoreflektionen aus G geht. Da mit σ auch σ^{-1} eine Pseudoreflektion ist, erhalten wir

$$2\,a_{n-1} = \sum \frac{1}{1-det(M_\sigma)} + \frac{1}{1-det(M_\sigma)^{-1}} = \sum 1,$$

so dass $2\,a_{n-1}$ mit der Anzahl der Pseudoreflektionen übereinstimmt. Wir haben damit für beliebige reguläre Gruppenaktionen folgenden Zusammenhang bewiesen:

$$F(t) = \frac{1}{|G|}\left(1 + \frac{r}{2}\,(1-t) + O\left((1-t)^2\right)\right),$$

wobei r die Zahl der Elemente in G angibt, die Pseudoreflektionen sind.
Hat insbesondere R ein System von Primärinvarianten der Grade $d_1, \ldots, d_n$, gilt also

$$H(R,t) = \frac{f(t)}{\prod_{i=1}^n (1-t^{d_i})}$$

mit $f(t) = \sum_{m\in\Sigma} t^{deg(m)} \in \mathbb{N}[t]$ und damit

$$F(t) = f(t)\prod_{i=1}^n \frac{1-t}{1-t^{d_i}},$$

so ergibt sich die Taylorreihe bei $t = 1$ als

$$F(t) = F(1) + F'(1)(t-1) + O((t-1)^2)$$

mit

$$F(1) = \frac{1}{|G|} = \frac{f(1)}{d_1 \cdot \ldots \cdot d_n}$$

(nach L'Hospital) und

$$\frac{F'(1)}{F(1)} = -\frac{r}{2} = \frac{f'(1)}{f(1)} - \sum_{i=1}^n \frac{\frac{1}{2}d_i(d_i-1)}{d_i}$$

als logarithmische Ableitung, also

$$r = (d_1 + \cdots + d_n - n) - 2\,\frac{f'(1)}{f(1)}\,. \tag{6}$$

Ist wie im Fall der Drehgruppen der platonischen Körper $r = 0$ und $\Sigma = \{1, m\}$ ein System von Sekundärinvarianten, so gilt

$$f(1) = |\Sigma| = 2, \quad f'(1) = \sum_{u\in\Sigma} deg(u) = deg(m)$$

und folglich

$$deg(m) = d_1 + \cdots + d_n - n$$

in Übereinstimmung mit unseren Beispiel-Rechnungen.

Als *Reflektionsgruppe* bezeichnet man eine solche Matrixgruppe $G \subset Gl(V)$, die von Pseudoreflektionen erzeugt werden kann.

Solche Reflektionsgruppen sind etwa die Spiegelungsgruppen in der Ebene oder im Raum, aber auch die Permutationsdarstellung der S_n. Letztere wird von Transpositionen erzeugt, die ebenfalls Spiegelungen sind, denn (1 2) etwa hat die Eigenbasis $(x_1 + x_2, x_1 - x_2, x_2, \dots, x_n)$ mit den Eigenwerten $(+1, -1, +1, \dots, +1)$.

Satz 22 (Shephard/Todd, Chevalley, 1954/55) *Der Invariantenring $R = k[V]^G$ einer endlichen (regulären) Matrixgruppe $G \subset Gl(V)$ kann genau dann von einem System von Primärinvarianten erzeugt werden, wenn G eine Reflektionsgruppe ist.*

Wir beweisen den Satz in mehreren Schritten.

(1) Zu einer Pseudoreflektion $\pi \in Gl(V)$ betrachten wir deren invariante Hyperebene $H_\pi = Ker(\pi - 1)$ und die Linearform $L_\pi \in [S]_1$, für welche $H_\pi = \{\mathbf{x} : L_\pi(\mathbf{x}) = 0\}$ gilt.

Lemma 6 *Für $f \in S$ gilt stets $L_\pi \mid f^\pi - f$.*

Beweis : Für einen Vektor $v \in H_\pi$ gilt $(f^\pi - f)(v) = f(v^\pi) - f(v) = 0$. Also verschwindet das Polynom $f^\pi - f$ auf ganz H_π und ist folglich ein Vielfaches des irreduziblen (weil Grad=1) Polynoms L_π. $\square$

(2) Sei nun G eine Reflektionsgruppe und $I_G = R_+ S$ wie im Hilbertschen Beweis des Endlichkeitssatzes das Ideal in S, welches von allen Invarianten positiven Grades erzeugt wird.

Lemma 7 *Sind $h_1, \dots, h_m \in S$ homogene Polynome und $g_1, \dots, g_m \in R$ Invarianten mit $h_1 g_1 + \dots + h_m g_m = 0$, so gilt entweder $h_1 \in I_G$ oder $g_1 \in Id(g_2, \dots, g_m)$.*

Beweis : Der Beweis erfolgt mit Induktion nach dem Grad von h_1. Für $deg(h_1) = 0$ ist $h_1 \in [R]_0 = k$ invertierbar und folglich $g_1 \in Id(g_2, \dots, g_m)$.

Sei $deg(h_1) > 0$ und $g_1 \notin Id(g_2, \dots, g_m)$. Ist $\sigma \in G$ eine Pseudoreflektion, so gilt nach (1) $h_i^\sigma - h_i = h_i' L_\sigma$ und damit

$$0 = \sum_i g_i h_i = \sum_i g_i h_i^\sigma = \sum_i g_i (h_i + h_i' L_\sigma = L_\sigma \sum_i g_i h_i',$$

also $\sum_i g_i h_i' = 0$ und wegen $deg(h_i') < deg(h_i)$ schließlich $h_i^\sigma - h_i = h_i' L_\sigma \in I_G$.

Sei nun $g = \sigma_l \sigma_{l-1} \dots \sigma_1$ ein beliebiges Element aus G, dargestellt als Produkt von Pseudoreflektionen. Dann gilt

$$h_1^g - h_1 = \sum_i h_1^{\sigma_{i+1} \dots \sigma_1} - h_1^{\sigma_i \dots \sigma_1} = \sum_i \left(h_1^{\sigma_{i+1}} - h_1\right)^{\sigma_i \dots \sigma_1} \in I_G\,,$$

da I_G natürlich G-invariant ist. Damit gilt aber auch $h_1^\rho - h_1 \in I_G$ und somit $h_1 \in I_G$. $\square$

(3) Sei weiter G von Pseudoreflektionen erzeugt. Wir zeigen nun, dass R als Algebra von n Invarianten erzeugt werden kann. Sei dazu $R = k[f_1, \dots, f_m]$ eine Darstellung mit zunächst $m \geq n$ homogenen Invarianten vom Grad $d_i = deg(f_i)$ und m minimal mit dieser Eigenschaft. Das ist zugleich ein minimales System von Erzeugenden für I_G.

Nehmen wir an, es ist $m > n$ und $g \in U = k[y_1, \dots, y_m]$ ein Polynom mit $g(f_1, \dots, f_m) = 0$. Wir können g als quasihomogen vom Grad d voraussetzen, wobei wir $deg(y_i) = d_i$ setzen, und annehmen, dass auch d minimal mit dieser Eigenschaft ist.

Wir betrachten nun die Invarianten

$$g_i = \frac{\partial g}{\partial y_i}(f_1, \ldots, f_m) \in R, \text{ mit } i = 1, \ldots, m.$$

Jedes der g_i ist entweder 0 oder eine homogene Invariante vom Grad $d - d_i < d$. Da g nicht konstant ist, gibt es ein i mit $\frac{\partial g}{\partial y_i}(y_1, \ldots, y_m) \neq 0$, so dass nach Wahl von d auch $g_i \neq 0$ gilt.

Sei I das von $(g_1, \ldots, g_m)$ erzeugte Ideal, wobei wir annehmen wollen, dass so nummeriert ist, dass I von $(g_1, \ldots, g_k)$ erzeugt wird, aber keine echte Teilmenge dafür ausreicht. Wir können dann die $g_i, i > k$, darstellen als $g_i = \sum_{j \leq k} h_{ij} g_j$ mit Polynomen h_{ij}, die entweder gleich 0 oder homogen vom Grad $deg(h_{ij}) = deg(g_i) - deg(g_j) = d_j - d_i$ sind.

Weiter gilt

$$\begin{aligned} 0 = \frac{\partial}{\partial x_s} (g(f_1 \ldots, f_s)) &= \sum_{i=1}^{m} g_i \frac{\partial f_i}{\partial x_s} \\ &= \sum_{i \leq k} g_i \frac{\partial f_i}{\partial x_s} + \sum_{i > k} \left(\sum_{j \leq k} h_{ij} g_j \right) \frac{\partial f_i}{\partial x_s} \\ &= \sum_{i \leq k} g_i \left(\frac{\partial f_i}{\partial x_s} + \sum_{j > k} h_{ji} \frac{\partial f_j}{\partial x_s} \right). \end{aligned}$$

Wegen $g_1 \notin Id(g_2, \ldots, g_m)$ folgt aus (2)

$$\frac{\partial f_1}{\partial x_s} + \sum_{j > k} h_{j1} \frac{\partial f_j}{\partial x_s} \in I_G \text{ für } s = 1, \ldots, n\,. \tag{4}$$

Für ein homogenes Polynom $f \in [S]_e$ gilt die Eulersche Formel

$$\sum_s x_s \frac{\partial f}{\partial x_s} = e \cdot f$$

(für Terme trivial, allgemein daraus über Linearität der Ableitungen). Wir multiplizieren deshalb (4) mit x_s und summieren über alle s:

$$\begin{aligned} &\sum_s x_s \frac{\partial f_1}{\partial x_s} + \sum_{j > k} h_{j1} \sum_s x_s \frac{\partial f_j}{\partial x_s} \\ =&d_1\, f_1 + \sum_{j > k} h_{j1} d_j\, f_j \in Id(x_1, \ldots, x_n)\, I_G\,. \end{aligned}$$

Damit erhalten wir

$$f_1 \in Id(x_1, \ldots, x_n) f_1 + Id(f_2, \ldots, f_m)$$

Aus Gradgründen kann der erste Summand keinen Beitrag für eine Darstellung liefern, so dass schließlich $f_1 \in Id(f_2, \ldots, f_m)$ folgt im Widerspruch zur Minimalität von m.

Damit ist der erste Teil des Beweises des Satzes von Shephard/Todd-Chevalley erbracht.

(5) Die andere Richtung ergibt sich aus der Analyse der Molienreihe, denn mit (6) und $f = 1$ haben wir für ein System von Algebraerzeugenden $R = k[f_1, \ldots, f_n]$ mit den Graden $deg(f_i) = d_i$ und

$$\begin{aligned} |G| &= d_1 \cdot \ldots \cdot d_n \\ r &= d_1 + \ldots + d_n - n \end{aligned}$$

Ist $H \subset G$ die Untergruppe in G, die von Pseudoreflektionen erzeugt wird, so gilt nach dem ersten Teil des Beweises $k[V]^H = k[g_1, \ldots, g_n]$ für ein System vom Primärinvarianten der Grade $deg(g_i) = e_i$, für die genauso gilt

$$\begin{aligned} |H| &= e_1 \cdot \ldots \cdot e_n \\ r &= e_1 + \ldots + e_n - n \end{aligned}$$

Wegen $R \subset k[V]^H$ gibt es polynomiale Darstellungen $f_i = P_i(g_1, \ldots, g_n)$. Die Jacobi-Determinante $det(\partial f_i / \partial g_j)$ verschwindet nicht, da auch $(f_1, \ldots, f_n)$ algebraisch unabhängig ist. Dann gibt es aber einen Eintrag

$$\frac{\partial f_{\pi(1)}}{\partial g_1} \cdots \frac{\partial f_{\pi(n)}}{\partial g_n} \neq 0$$

in der Jacobi-Matrix, womit $d_{\pi(i)} \geq e_i$ gilt. Wegen

$$d_1 + \ldots + d_n = r + n = e_1 + \ldots + e_n$$

müssen dann aber die Grade alle übereinstimmen, so dass auch $|G| = |H|$ und damit $G = H$ gilt.

Literatur

[1] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer, New York, 1992.

[2] H. Derksen and G. Kemper. *Computational invariant theory*, volume 130 of *Encyclopedia of Math. Sciences*. Springer, Berlin, 2002.

[3] E. Fischer. Zur Theorie der endlichen abelschen Gruppen. *Math. Ann.*, pages 81–88, 1916.

[4] I. G. MacDonald. *Symmetric functions and Hall polynomials*. Oxford Univ. Press, 1979.

[5] E. Noether. Der Endlichkeitssatz für Invarianten endlicher Gruppen. *Math. Ann.*, pages 89–92, 1916.

[6] T. A. Springer. *Invariant Theory*, volume 585. Springer, 1977.

[7] R. P. Stanley. Relative invariants of finite groups generated by pseudoreflections. *J. Alg.*, 49:134–148, 1977.

[8] R. P. Stanley. Invariants of finite groups and their applications to combinatorics. *Bull. AMS*, 1:475–511, 1979.

[9] B. Sturmfels. *Algorithms in invariant theory*. Springer, New York, 1993.