Theorie der Invarianten endlicher Gruppen
Wintersemester 2009/10

H.-G. Gräbe, Institut für Informatik,
http://bis.informatik.uni-leipzig.de/HansGertGraebe

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

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

für diese Punkte zur selben Bedingung $f_1 = 0$.

```
f1a:=(x1+u)*(y2+v) - (x2+u)*(y1+v) + (x3+u)*(y1+v) - (y3+v)*(x1+u)
     + (x2+u)*(y3+v) - (x3+u)*(y2+v);

expand(f1a);
```

$$x_1y_2 - x_2y_1 + x_3y_1 - y_3x_1 + x_2y_3 - x_3y_2$$

Das Polynom f_1 ändert sich also nicht unter Verschiebungen

$$\tau_{(u,v)} : (x_i, y_i) \to (x_i + u, y_i + v) \text{ für } i = 1, 2, 3\,,$$

denn es gilt $f_1(x_1, y_1, x_2, y_2, x_3, y_3) = f_1(x_1^\tau, y_1^\tau, x_2^\tau, y_2^\tau, x_3^\tau, y_3^\tau)$. Die Menge V solcher Verschiebungen bildet eine Gruppe, unter deren Aktion das Polynom f_1 eine *Invariante* ist.

Das gilt im Prinzip nicht nur für Verschiebungen, sondern für beliebige affine Transformationen

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

Die durch g beschriebene allgemeine Substitution für (x, y) muss dabei auf die drei Paare (x_1, y_1), (x_2, y_2), (x_3, y_3) angewendet werden:

```
s:={x=a11*x+a12*y+a1,y=a21*x+a22*y+a2};
s1:=subs(s,x=x1,y=y1);
s2:=subs(s,x=x2,y=y2);
s3:=subs(s,x=x3,y=y3);

f1b:=subs(f1,s1,s2,s3);
```

$$\begin{aligned}&(a_1 + a_{11}x_1 + a_{12}y_1)(a_2 + a_{21}x_2 + a_{22}y_2) - (a_1 + a_{11}x_2 + a_{12}y_2)(a_2 + a_{21}x_1 + a_{22}y_1) \\ &\quad - (a_1 + a_{11}x_1 + a_{12}y_1)(a_2 + a_{21}x_3 + a_{22}y_3) + (a_2 + a_{21}x_1 + a_{22}y_1)(a_1 + a_{11}x_3 + a_{12}y_3) \\ &\quad + (a_1 + a_{11}x_2 + a_{12}y_2)(a_2 + a_{21}x_3 + a_{22}y_3) - (a_1 + a_{11}x_3 + a_{12}y_3)(a_2 + a_{21}x_2 + a_{22}y_2)\end{aligned}$$

`expand(f1b)` liefert hier nicht das ursprüngliche Polynom zurück.

Mit dem Kommando `factor(expand(f1b))` erkennt man, dass das Ergebnis ein Vielfaches von f_1 ist.

$$f_{1b} = (x_1y_2 - x_2y_1 - x_1y_3 + x_3y_1 + x_2y_3 - x_3y_2)(a_{11}a_{22} - a_{12}a_{21})$$

Es gilt also $f_{1b} = f_1^g = (a_{11}a_{22}-a_{12}a_{21})\cdot f_1$ und $f_1 = 0 \Leftrightarrow f_{1b} = 0$, denn der Kofaktor $a_{11}a_{22}-a_{12}a_{21}$ ist die Determinante der Transformationsmatrix und verschwindet deshalb nicht.

Ein solches Polynom, das nicht erhalten bleibt, sondern sich um einen nur von g abhängenden Faktor $f^g = c(g) \cdot f$ ändert, bezeichnet man als *Semiinvariante*. $c : G \to k$ ist hierbei ein Gruppenfunktional, denn es muss in diesem Fall $c(g_1 \cdot g_2) = c(g_1) \cdot c(g_2)$ für $g_1, g_2 \in G$ gelten.

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:

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

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

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

eine Koordinatendarstellung des Vektors $v \in W$. Die Funktionen $x_i : W \to k$ sind lineare Funktionale auf W und spannen den Raum $V = W^*$ der linearen Funktionale über W als k-Vektorraum auf. Sie heißen *Koordinatenfunktionen*. Im Raum aller Funktionen auf W erzeugen sie die k-Algebra $k[V] = k[x_1, \ldots, x_n]$ der polynomialen Funktionen auf W.

Als *(Links-)Aktion* ϕ der Gruppe G auf W bezeichnet man einen Gruppenhomomorphismus $\phi : G \to Gl(W)$, der also jedem $g \in G$ eine lineare Abbildung $\phi(g) \in GL(W)$ zuordnet, die auf W durch $v \to \phi(g)(v)$ wirkt. Operationstreue bedeutet, dass $\phi(g)(\phi(h)(v)) = \phi(g\,h)(v)$ für alle $g, h \in G, v \in W$ gilt. Wir wollen weiter voraussetzen, dass diese Aktion *treu* ist, d. h. dass $\ker(\phi) = 1$ gilt.

Im Weiteren werden wir nicht zwischen den Bezeichnungen g und $\phi(g)$ unterscheiden, sondern G mit der Untergruppe in $Gl(W)$ identifizieren. ϕ kann statt als $G \to (W \to W)$ auch als Abbildung $(G \times W) \to W$ angesehen werden, die einem Paar (g, v) das Element $g(v)$ zuordnet.

Eine solche Linksaktion von G auf W induziert eine Rechtsaktion von G auf dem Ring $k[V = W^*]$ der polynomialen Funktionen (und sogar auf dem Ring aller Funktionen auf W), die für $f \in k[V]$ durch $f^g(v) := f(g(v))$ definiert ist. g operiert dabei als Ringautomorphismus, so dass die Operation 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 W dual ist (es gilt $x_i(e_j) = \delta_{ij}$), wird (in der jeweiligen Basis) die lineare Variablensubstitution durch die transponierte Matrix M_g^T 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 vom Vektorraum V der homogenen Linearformen in $x_1, \ldots, x_n$ ausgehen, die polynomiale Funktionen auf V 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 $M_g \in GL(n, k) = Gl(V)$ 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 die Untersuchung der Struktur dieses Rings $k[V]^G$ für verschiedene Gruppenaktionen $G \subset GL(V)$ und Vektorräume V. 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 auf endlichen Vektorräumen V gehen.

1.3 Ein erstes Beispiel

Betrachten wir als Beispiel die Aktion der 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)$i=0..d);
      // generisches Polynom vom Grad d erzeugen
  s:=solve({coeff(f-g(f),[x,y])},[a[i]$i=0..d]);
      // 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	$f_{8a} = x^8+y^8,\ f_{8b} = xy(x^6-y^6),\ f_{8c} = x^2y^2(x^4+y^4),$ $f_{8d} = x^3y^3(x^2-y^2),\ f_{8e} = x^4y^4$

Aufgabe 1 Zeigen Sie, dass es unter der angegebenen Aktion keine Invarianten ungeraden Grades gibt.

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

Verfahren zur Berechnung einer k-Basis der Invarianten vom Grad d

Gegeben ist der Polynomring $R = k[x_1,\dots,x_n]$, ein Erzeugendensystem E der Gruppenaktion G sowie die Wirkung der Elemente $g \in E$ auf R.

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

(2) Berechne $f - f^g$ für alle $g \in E$.

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

(4) Aus einer Basis des Lösungsraums dieses Gleichungssystems ergibt sich unmittelbar eine Basis von $\bigl[k[V]^G\bigr]_d$.

Zur Komplexität dieses Verfahrens

Nehmen wir an, dass Rechnungen in k in konstanter Zeit möglich sind, dann kann das lineare Gleichungssystem in $O(D^3\,e)$ 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 und $e = |E|$ gilt.

In der Tat, ein $M \times N$-System vom Rang R lässt sich durch $O(M\,N\,R)$ Körperoperationen mit dem klassischen Gaussalgorithmus in Dreiecksform bringen. Hier ist $M = D$, $N = D\,e$ und $R \le D$, woraus sich die Abschätzung unmittelbar ergibt.

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

Der Gesamtaufwand wird unter den genannten Voraussetzungen (n und e vorgegeben, $d \to \infty$) also vom Lösen des Gleichungssystems dominiert und ist (klassisch) in der Größenordnung $O(D^3)$.

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

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

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. Wir setzen dazu die bisher gefundenen Invarianten als Substitutionslisten an, um gleichzeitig mit den Symbolen f_2 usw. und deren Werten rechnen zu können. Ein solcher Ansatz folgt den Empfehlungen aus dem Kurs „Einführung in das symbolische Rechnen“ zur Verwendung von Variablenbezeichnern, belässt die Bezeichner f_2 usw. global im Wertmodus und rechnet konsequent mit lokalen Wertzuweisungen durch den Substitutionsoperator sowie den Selektoren `rhs` und `lhs` für die jeweilige symbolische bzw. wertmäßige Auswertung der entsprechenden Ausdrücke.

```
B_2:=[f2=x^2+y^2];
B_4:=[f4a=x^4+y^4, f4b=x^3*y-x*y^3, f4c=x^2*y^2];
B_6:=[f6a=x^6+y^6, f6b=x^5*y-x*y^5, f6c=x^4*y^2+x^2*y^4];

p:=[u^4$u in B_2, u^2*v$u in B_2$v in B_4[2..3],
     B_4[2]^2, B_4[2]*B_4[3], B_4[3]^2];
r:=_plus(a[i]*p[i]$i=1..6);
sol:=solve({coeff(rhs(r),[x,y])},[a[i]$i=1..6]);
rel:=subs(lhs(r),sol[1],z=4);
```

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

Zwischen den sechs Invarianten vom Grad 8 besteht also die lineare Relation $f_{4b}^2 = f_2^2\,f_{4c} - 4\,f_{4c}^2$, so dass auch in diesem Grad keine „neuen“ Invarianten existieren. Wir vermuten deshalb, dass

$$R_1 = k[f_2, f_{4b}, f_{4c}]$$

bereits der vollständige Invariantenring ist. Allerdings sind die drei Erzeugenden nicht algebraisch unabhängig, sondern zwischen ihnen besteht eine polynomiale Relation, so dass R_1 isomorph zum Koordinatenring einer (quasihomogenen) Raumfläche

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

ist. Hierbei kann mit Mitteln der konstruktiven Algebra (Gröbnerbasen) leicht festgestellt werden, dass der Kern der Abbildung $\phi : k[A,B,C] \to k[f_2, f_{4b}, f_{4c}]$ in der Tat von $I = (B^2 + 4\,C^2 - A^2C)$ erzeugt ist, R' und R_1 also wirklich isomorph sind.

Die Invarianten f_2, f_{4b} und f_{4c} erzeugen R_1 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 $f \equiv P_1(A,C) + B \cdot P_2(A,C) \pmod I$ mit Polynomen $P_1, P_2 \in k[A,C]$, d. h. 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.*

Aus dieser Zerlegung folgt auch, dass $[R']_{2d}$ die Terme $A^{d-2i}C^i, d \geq 2i$, und $A^{d-2i-2}B\,C^i, d \geq 2i+2$, als Vektorraumbasis hat. Damit gilt $\dim_k([R']_{2d}) = 2 \cdot \left\lfloor \frac{d}{2} \right\rfloor + 1$; die Dimensionen stimmen mit den früher berechneten Dimensionen $\dim_k([R]_{2d})$ des Invariantenrings $R = k[V]^G$ überein.

Dies ergibt weitere Evidenz, wenn auch noch keinen Beweis dafür, dass R_1 bereits der volle Invariantenring ist. Die zum Nachweis erforderlichen Mittel entwickeln wir im nächsten Abschnitt.

1.4 Die Hilbertreihe einer homogenen k-Algebra

Ist R eine homogene k-Algebra, etwa der Ring der Invarianten, so ist die Dimension $\dim_k([R]_d)$ des Vektorraums der Elemente vom Grad d für verschiedene d eine wichtige Zahlenfolge. Sie ist in den meisten Fällen besonders einfach zu beschreiben, wenn diese Zahlen in einer *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 $S = k[x_1, \ldots, x_n]$

$$\dim_k([S]_d) = \binom{n+d-1}{n-1} \quad \text{und} \quad H(S,t) = \frac{1}{(1-t)^n}$$

und für $R = S/(f)$ mit einem homogenen Polynom f vom Grad $\deg(f) = d$

$$H(S/(f),t) = \frac{1-t^d}{(1-t)^n}$$

Im Falle quasihomogener Ringe gilt folgende Modifikation.

Satz 1 *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

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

und somit

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

woraus die Behauptung sofort folgt. □

Satz 2 *Ist $S = k[y_1, \ldots, y_n]$ ein gewichtet homogener Polynomring und f ein (quasi)-homogenes Polynom vom Grad d, so gilt*

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

Beweis: Der Beweis ergibt sich sofort aus folgendem Lemma

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

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

Zum Beweis des Lemmas wählen wir $e_1, \ldots, e_m$ 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 $\mathrm{im}(\phi)$.

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 $ker(\pi) = f \cdot S$

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

und schließlich die behauptete Beziehung. □

Liegt eine Hironakazerlegung vor, so können wir die Hilbertreihe ebenfalls leicht aus den Hilbertreihen der Bestandteile zusammensetzen.

Satz 3 *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*

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

Beispiel Für unser Beispiel $R_1 = k[A,B,C]/(B^2 + 4\,C^2 - A^2C)$ erhalten wir mit $\deg(A) = 2$, $\deg(B) = \deg(C) = 4$ aus den beiden Sätzen

$$\begin{aligned} H(R_1,t) &= \frac{1 - t^8}{(1-t^2)\,(1-t^4)^2} = \frac{1 + t^4}{(1-t^2)\,(1-t^4)} \\ &= 1 + t^2 + 3\,t^4 + 3\,t^6 + 5\,t^8 + 5\,t^{10} + 7\,t^{12} + 7\,t^{14} + 9\,t^{16} + 9\,t^{18} + \ldots \end{aligned}$$

Die letztere Zerlegung lässt sich mit MuPAD wie folgt berechnen:

```
f:=(1+t^4)/((1-t^2)*(1-t^4));
taylor(f,t=0,40);
```

Aufgabe 2 Zeigen Sie, dass

$$H = \frac{1 + z^2}{(1-z)\,(1-z^2)} = \sum_{d\geq 0} \left(2\left\lfloor \frac{d}{2} \right\rfloor + 1\right) z^d$$

die Taylorreihen-Entwicklung von H ist.
Hinweis: Zeigen Sie, dass

$$H = \sum_{k\geq 0} (2\,k+1)\,\left(z^{2k} + z^{2k+1}\right) = (1+z)\cdot \sum_{k\geq 0} (2\,k+1)\,z^{2k}$$

gilt und finden Sie eine geschlossene Formel für

$$F(z) = \sum_{k\geq 0} (2\,k+1)\,z^{2k} = \left(\sum_{k\geq 0} z^{2k+1}\right)' .$$

1.5 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, also die Molienreihe

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

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.

1.6 Einige grundlegende Prozeduren

Allgemein wird die Aktion eines Elements $g \in G$ der Gruppe auf dem Vektorraum $[S]_1$ durch eine Matrix $M_g \in Gl_n$ beschrieben, die zunächst in eine Liste von Substitutionsregeln $x_i \to x_i^g$ verwandelt werden muss, die sich aus der Beziehung

$$\begin{pmatrix} x_1^g \\ x_2^g \\ \dots \\ x_n^g \end{pmatrix} = M_g \cdot \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}$$

ergibt. Wir definieren hierzu folgende MuPAD-Funktion:

```
matrix2subrules:=proc(M:Dom::Matrix(),vars:DOM_LIST) 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;
```

Für die Verallgemeinerung der Funktion `computeBasis` benötigen wir zunächst eine Liste aller Terme vom Grad d in einer gegebenen Menge von Variablen. Diese kann mit der folgenden Funktion rekursiv erzeugt werden.

```
Terme:=proc(d,vars) local u;
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;
```

Nun können wir eine k-Basis der homogenen Invarianten vorgegebenen Grads bzgl. der Gruppenaktion G wie folgt bestimmen, wenn eine Liste `gList` der Erzeugenden von G in subRules-Notation gegeben ist:

```
computeBasis:=proc(d,gList,vars) local T,f,f1,i,s,g,newvars;
begin
  T:=Terme(d,vars);
  f:=_plus(a[i]*T[i]$i=1..nops(T));
      // generisches Polynom vom Grad d erzeugen
  s:=solve({coeff(f-subs(f,g),vars)$g in gList},[a[i]$i=1..nops(T)]);
      // lineares Gleichungssystem generieren und lösen
  f1:=subs(f,s[1]); // allgemeine Lösung zusammenbauen
      // ... und k-Basis extrahieren
  newvars:=[op(indets(f1) minus {op(vars)})];
  if iszero(f1) then [ ] else [coeff(f1,newvars)] end_if;
end_proc;
```

f_1 ist hierbei die allgemeine Form einer Invarianten der G-Aktion vom Grad d, die als homogene Linearkombination einer endlichen Anzahl von Invarianten dargestellt ist, welche eine k-Basis von $[R]_d$ bilden. Aus dieser allgemeinen Form werden mit `newvars` die von MuPAD während der Lösungsbestimmung neu generierten Variablen extrahiert, f_1 nach diesen Variablen gruppiert und schließlich die Liste der Koeffizienten in dieser Darstellung extrahiert.

Beispiel: C_n-Aktion auf $k[x,y]$, die der Drehgruppe eines regelmäßigen n-Ecks entspricht. Dem erzeugenden Element g dieser Gruppe entspricht die Matrix

$$M_g := \begin{pmatrix} \cos\left(\frac{2\,\pi}{n}\right) & \sin\left(\frac{2\,\pi}{n}\right) \\ -\sin\left(\frac{2\,\pi}{n}\right) & \cos\left(\frac{2\,\pi}{n}\right) \end{pmatrix}.$$

Mit folgenden Kommandos verschaffen wir uns im Fall $n = 3$ zunächst einen Überblick über die Invarianten, die $[R]_d$ für $d \leq 6$ als k-Vektorraum erzeugen:

```
vars:=[x,y];
M:=n->Dom::Matrix()([[cos(2*PI/n),sin(2*PI/n)],[-sin(2*PI/n),cos(2*PI/n)]]);
g:=matrix2subrules(M(3),vars);
gBasisList:=computeBasis(d,[g],vars)$d=1..6;
```

Als Dimensionen $\dim_k [R]_d$ ergeben sich $0, 1, 2, 1, 2, 3$. Als wichtige Invarianten finden wir

$$f_2 = x^2 + y^2,\ f_{3a} = x^3 - 3\,x\,y^2,\ f_{3b} = y^3 - 3\,x^2\,y\,,$$

aus denen sich die Erzeugendensysteme

$$[A = f_2], [B = f_{3a}, C = f_{3b}], [f_2^2], [f_2\,f_{3a}, f_2\,f_{3b}], [f_2^3, f_{3a}^2, f_{3a}\,f_{3b}, f_{3b}^2]$$

in den einzelnen Graden extrahieren lassen. Im Grad 6 haben wir 4 Erzeugende aufgelistet, wegen $\dim_k [R]_6 = 3$ muss es also zwischen ihnen eine lineare Abhängigkeitsrelation

$$A^3 = a_1\,B^2 + a_2\,B\,C + a_3\,C^2$$

geben. Um diese zu bestimmen, definieren wir in Verallgemeinerung unseres bisherigen Vorgehens die folgenden Funktion **findRelations**

```
findRelations:=proc(u,vars) local r,a,n,v,sol;
begin
  n:=nops(u); a:=genident();
  r:=_plus(a[i]*u[i]$i=1..n);
  sol:=solve({coeff(rhs(r),vars)},[a[i]$i=1..n]);
  map(sol,v->subs(lhs(r),v));
end_proc;
```

`u` ist dabei eine Liste der Länge n von Gleichungen $f_i = p_i(\mathbf{x})$, wobei p_i homogene Polynome gleichen Grads in den Variablen `vars` sind. Daraus wird eine generische Linearkombination $r = \sum_{i=1}^n a_i \cdot (f_i = p_i)$ mit frischen Bezeichnern a_i erzeugt. `rhs(r)` extrahiert daraus $\sum_{i=1}^n a_i\,p_i(\mathbf{x}) \in k[\mathbf{a}][\mathbf{x}]$, woraus durch Koeffizientenvergleich ein lineares Gleichungssystem für die a_i extrahiert, dieses gelöst und die Lösungsmenge in `lhs(r)` eingesetzt wird. Dies ist die generische Linearkombination $\sum_{i=1}^n a_i\,f_i$, für die $\sum_{i=1}^n a_i\,p_i(\mathbf{x}) = 0$ gilt.

Für den speziellen Fall unseres Beispiels können wir die erforderlichen Rechnungen nun wie folgt anschreiben:

```
B_2:=[f2=x^2+y^2];
B_3:=[f3a=x^3-3*x*y^2, f3b=y^3-3*x^2*y];

p:=[u^3$u in B_2, B_3[1]^2, B_3[1]*B_3[2]^2, B_3[2]^2];
r:=findRelations(p,[x,y]);
r1:=subs(r[1],z=1);
```

Wir erhalten die Abhängigheitsrelation $f_2^3 = f_{3a}^2 + f_{3b}^2$, was mit

```
expand(subs(r1,B_2,B_3));
```

auch noch einmal bestätigt werden kann. Dies ist – bis auf polynomiale Vielfache – zugleich die einzige polynomiale Relation zwischen f_2, f_{3a} und f_{3b}, so dass der Invariantenring R einen zum Ring $R' = k[A, B, C]/(A^3 - B^2 - C^2)$ isomorphen Unterring enthält und beide bis einschließlich Dimension 6 sogar zusammenfallen.

Die Produkte vom Grad 6 in f_2, f_{3a} und f_{3b} wurden dabei „per Hand“ erzeugt. Auch dies kann mit der folgenden Funktion **GewichteteProdukte** automatisiert werden.

```
GewichteteProdukte:=proc(d,pList,vars) local u,v,w;
// Liste aller Produkte von p in pList vom Grad d
begin
  if nops(pList)=0 then return([]) end_if;
```

```
  u:=pList[1]; w:=degree(rhs(u));
  if d<0 then []
  elif nops(pList)=1 then
    (if d mod w=0 then [u^(d/w)] else [] end_if)
  else v:=pList[2..nops(pList)];
    [op(map(GewichteteProdukte(d-i*w,v,vars),x->u^i*x))$i=0..d/w]
  end_if;
end_proc;
```

`pList` ist hierbei eine Liste von Ausdrücken $f_i = p_i(\mathbf{x})$, aus der alle Produkte $\prod f_i^{a_i}$ generiert werden, für die $\sum a_i \deg(p_i) = d$ gilt. Hier als Beispiel die obige Rechnung:

```
B:=[f2=x^2+y^2, f4b=x^3*y-x*y^3, f4c=x^2*y^2];
p:=GewichteteProdukte(8,B,[x,y]);
rel:=findRelations(p,[x,y]);
r:=subs(rel[1],z=1);
expand(subs(r,B));
```

Für die Hilbertreihe des Rings R' mit $\deg(A) = 2$, $\deg(B) = \deg(C) = 3$ ergibt sich

$$H(R',t) = \frac{1-t^6}{(1-t^2)\,(1-t^3)^2} = \frac{1+t^2+t^4}{(1-t^3)^2} = \frac{1+t^3}{(1-t^2)\,(1-t^3)}\,.$$

Den letzten beiden Darstellungen der Hilbertreihe entsprechen die beiden Hironakazerlegungen $R' = k[B,C] \oplus A \cdot k[B,C] \oplus A^2 \cdot k[B,C]$ sowie $R' = k[A,C] \oplus B \cdot k[A,C]$, je nachdem, ob die Relation $A^3 - B^2 - C^2$ verwendet wird, um A algebraisch durch B, C auszudrücken (erste Darstellung) oder B durch A, C (zweite Darstellung).

Aufgabe 3 Führen Sie dieselben Untersuchungen für die Aktion der Drehgruppe $G = C_5$ des regelmäßigen Fünfecks in $\mathbb{C}[x,y]$ aus.

2 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

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

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,

Als *Partition* der Zahl d bezeichnet man jede Folge $\lambda = (a_1, a_2, \ldots, a_k)$ mit $a_1 \geq a_2 \geq \cdots \geq a_k \geq 0$ und $a_1 + a_2 + \cdots + a_k = d$. Wir schreiben dafür $d \vdash \lambda$. Ist $k \leq n$, so heißt die Partition n-längenbegrenzt. Solche Partitionen können (und werden) wir durch Nullen auffüllen zu einer Partition $\lambda = (a_1, a_2, \ldots, a_n)$.

Zahlpartitionen und Ferrersdiagramme. Anzahl der Felder $d = |\lambda| = a_1 + a_2 + \cdots + a_n$.

Alternative Darstellung $\lambda = \left[1^{b_1}, 2^{b_2}, \ldots, n^{b_n}\right]$ für eine Partition, deren Ferrersdiagramm aus b_i Zeilen der Länge i besteht. Hier gilt $d = |\lambda| = b_1 + 2 \cdot b_2 + \cdots + n \cdot b_n$.

Monomiale Summe μ_λ für die n-längenbegrenzte Partition $d \vdash \lambda$.

Beispiel: $n = 3$, $\lambda = (2, 1, 1)$ ergibt $\mu_\lambda = x_1^2 x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2$.

Satz 4 (Dimensionssatz für symmetrische Polynome)
Für den Ring $R = S^{S_n}$ der symmetrischen Polynome gilt, dass $\dim_k([R]_d)$ gleich der Zahl n-längenbegrenzten Partitionen der Zahl d und damit auch gleich der Zahl der Ferrersdiagramme mit d Kästchen und $\leq n$ Spalten ist.

Beweis: Offensichtlich bilden die μ_λ, $d \vdash \lambda$ ein Erzeugendensystem: Ist $0 \neq f \in R$ ein symmetrisches Polynom und $c_\alpha x^\alpha = lm(f)$ dessen Leitmonom bzgl. der lexikographischen Ordnung, so gilt für den Exponentenvektor $\alpha = (\alpha_1, \ldots, \alpha_n)$ offensichtlich $\alpha_1 \geq \cdots \geq \alpha_n$, so dass α eine Partition ist und $f - c_\alpha \mu_\alpha$ wieder ein symmetrisches Polynom, dessen Leitterm aber kleiner als x^α ist.

Außerdem sind die Leitterme paarweise verschieden, also sind die Erzeugenden auch linear unabhängig. □

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

Ergebnis für $n = 6$ ist $[1, 1, 2, 3, 5, 7, 11]$. Beachte, dass für $n < 6$ nur n-längenbegrenzte Partitionen zu berücksichtigen sind.

Satz 5 (Molienreihe für symmetrische Polynome)

$$H(R = S^{S_n}, t) = \frac{1}{(1-t) \cdot (1-t^2) \cdot \ldots \cdot (1-t^n)}\,.$$

Beweis:

$$\begin{aligned} H(R,t) &= \sum_{d \geq 0} \#\left(\lambda : |\lambda| = d\right) t^d = \sum_{\lambda} t^{|\lambda|} = \sum_{(b_1,\ldots,b_n)} t^{b_1 + 2b_2 + \cdots + n\, b_n} \\ &= \sum_{b_1} t^{b_1} \cdot \sum_{b_2} \left(t^2\right)^{b_2} \cdot \ldots \cdot \sum_{b_n} \left(t^n\right)^{b_2} = \frac{1}{(1-t) \cdot (1-t^2) \cdot \ldots \cdot (1-t^n)}\,. \end{aligned}$$

□

```
f:=1/_mult(1-t^i$i=1..4);
taylor(f,t=0,13);
```

$$1 + t + 2\,t^2 + 3\,t^3 + 5\,t^4 + 6\,t^5 + 9\,t^6 + 11\,t^7 + 15\,t^8 + 18\,t^9 + 23\,t^{10} + 27\,t^{11} + 34\,t^{12} + \ldots$$

```
f:=1/_mult(1-t^i$i=1..12);
taylor(f,t=0,13);
```

$$1 + t + 2\,t^2 + 3\,t^3 + 5\,t^4 + 7\,t^5 + 11\,t^6 + 15\,t^7 + 22\,t^8 + 30\,t^9 + 42\,t^{10} + 56\,t^{11} + 77\,t^{12} + \ldots$$

Implementierung einiger Serien symmetrischer Funktionen in MuPAD[1]:

```
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) local f;
begin
  f:=map(combinat::permutations::list(vars),x->_mult(op(zip(x,l,'^'))));
  f:=_plus(op(f));
  f/lcoeff(f);
end_proc;
```

Wieviele Produkte aus den elementarsymmetrischen Polynomen gibt es von vorgegebenem Grad d? Es gibt eine offensichtliche 1-1-Korrespondenz zwischen diesen Produkten und den n-längenbegrenzten Partitionen $\lambda = [b_1, \ldots, b_n]$ (Ferrersdiagrammen).

$$e_1^{b_1} e_2^{b_2} \ldots e_n^{b_n} \longrightarrow \left(a_k := \sum_{i=k}^{n} b_i, k = 1, \ldots, n \right)$$

Offensichtlich ist weiter $lt\left(e_1^{b_1} e_2^{b_2} \ldots e_n^{b_n}\right) = x_1^{a_1} x_2^{a_2} \cdot \ldots \cdot x_n^{a_n}$ bzgl. der lexikographischen Termordnung.

Kann man also jedes symmetrische Polynom als Linearkombination von solchen Produkten schreiben, d. h. als polynomiale Kombination der elementarsymmetrischen Polynome? Falls das so ist,

[1] In Version 5 muss `combinat::permutations` durch die später eingeführte Funktion `allePermutationen` ersetzt werden.

gilt $R = S^{S_n} = k[e_1, \ldots, e_n]$ und der natürliche Morphismus

$$\phi : \; k[A_1, \ldots, A_n] \longrightarrow k[e_1, \ldots, e_n] \quad \text{via } A_i \to e_i$$

vom Polynomring $R_1 = k[A_1, \ldots, A_n]$ mit $\deg(A_i) = i$ nach R ist ein graderhaltender surjektiver Ringhomomorphismus mit $\dim_k [R_1]_d = \dim_k [R]_d$ (die Hilbertreihen stimmen überein), also ein Ringisomorphismus – die $e_1, \ldots, e_n$ sind algebraisch unabhängig.

Sind umgekehrt die $e_1, \ldots, e_n$ algebraisch unabhängig, so ist die Hilbertreihe von $R_2 = k[e_1, \ldots, e_n]$ dieselbe wie von R_1. Wegen $R_2 \subseteq R$ und $H(R_2, t) = H(R.t)$ ist dann aber kein Platz mehr für weitere Invarianten und somit $R_1 = R$.

Wie kann man für ein beliebiges Polynom eine solche Darstellung als polynomiale Kombination der elementarsymmetrischen Polynome finden?

Beispiele:

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

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

```
f1:=normal(f-e(3,vars)*e(2,vars)*e(1,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);
f1:=normal(f-e(3,vars)*e(2,vars)*e(1,vars)^2);
f2:=normal(f1+2*e(3,vars)*e(2,vars)^2);
f3:=normal(f2+e(3,vars)^2*e(1,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);
f1:=normal(f-e(3,vars)*e(2,vars)^2*e(1,vars)^2);
f2:=normal(f1+2*e(3,vars)^2*e(1,vars)^3);
f3:=normal(f2+2*e(3,vars)*e(2,vars)^3);
f4:=normal(f3-4*e(3,vars)^2*e(2,vars)*e(1,vars));
f5:=normal(f4+3*e(3,vars)^3); // =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 6 (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

$$k[y_1, \ldots, y_n] \longrightarrow S \quad \textit{via} \quad y_i \mapsto e_i$$

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].

Wendet man das Verfahren auf die h_d an, so ergeben sich folgende Darstellungen:

$$\begin{aligned}
h_1 &= e_1 \\
h_2 &= e_1^2 - e_2 \\
h_3 &= e_1^3 - 2\, e_1 e_2 + e_3 \\
h_4 &= e_1 - 3\, e_1^2 e_2 + e_2^2 + 2\, e_1 e_3 - e_4
\end{aligned}$$

In allen Fällen kann man h_i durch $e_j, j \leq i$ ausdrücken. Diese Beziehungen kann man allerdings umstellen und auch e_i durch $h_j, j \leq i$ ausdrücken. Die Beziehung zwischen den h_i und den e_i kann gut über die entsprechenden erzeugenden Funktionen ausgedrückt werden:

$$\begin{aligned}
H(T) &= \sum_d h_d\, T^d \\
&= \sum_{(a_1,\ldots,a_n)} (x_1 T)^{a_1} (x_2 T)^{a_2} \cdot \ldots \cdot (x_n T)^{a_n} \\
&= \frac{1}{(1 - x_1 T)(1 - x_2 T) \ldots (1 - x_n T)}
\end{aligned}$$

$$\begin{aligned}
E(T) &= \sum_d e_d\, T^d \\
&= (1 + x_1 T)(1 + x_2 T) \ldots (1 + x_n T)
\end{aligned}$$

Es gilt also

$$H(T) \cdot E(-T) = 1$$

oder expandiert und ausmultipliziert

$$\begin{aligned}
H(T) \cdot E(-T) &= \left(\sum_{d \geq 0} h_d\, T^d \right) \cdot \left(\sum_{d \geq 0} (-1)^d\, e_d\, T^d \right) \\
&= 1 + (h_1 - e_1)\, T + (h_2 - e_1 h_1 + e_2)\, T^2 + (h_3 - e_1 h_2 + e_2 h_1 - e_3)\, T^3 + \ldots
\end{aligned}$$

und die Beziehungen (Newtonsche Relationen) zwischen den h_i und e_i ergeben sich daraus durch Koeffizientenvergleich:

$$\sum_{i_0}^{d} (-1)^i h_{d-i} e_i = 0 \quad \text{für alle } d = 1, 2, \ldots.$$

Insbesondere kann h_d polynomial durch $h_i, e_i, i < d$ und e_d bzw. umgekehrt auch e_d polynomial durch $h_i, e_i, i < d$ und h_d dargestellt werden.

Jedes homogene symmetrische Polynom kann als Linearkombination von Termen in $e_1, \ldots, e_n$ desselben Grads dargestellt werden und diese lassen sich durch $h_1, \ldots, h_n$ ausdrücken. Also bilden die Terme in $h_1, \ldots, h_n$ vom Grad d ein k-lineares Erzeugendensystem von $[R]_d$. Da es genauso viele solche Terme vom Grad d in $e_1, \ldots, e_n$ und in $h_1, \ldots, h_n$ gibt, folgt daraus:

Satz 7 *Der Ring $R = S^{S_n}$ kann auch durch die ersten n vollen symmetrischen Summen $h_1, \ldots, h_n$ erzeugt werden: Es gilt $R = k[h_1, \ldots, h_n]$. $(h_1, \ldots, h_n)$ bilden also ebenfalls ein (algebraisch unabhängiges) System von Basisinvarianten.*

Dasselbe gilt für die Potenzsummen. Der Beweis ist allerdings etwas komplizierter.

Satz 8 *Der Ring $R = S^{S_n}$ kann ebenfalls durch die ersten n Potenzsummen $p_1, \ldots, p_n$ erzeugt werden: Es gilt $R = k[p_1, \ldots, p_n]$. $(p_1, \ldots, p_n)$ bilden also ebenfalls ein (algebraisch unabhängiges) System von Basisinvarianten.*

Beispiel: Versuche, möglichst hohe reine Grade zu erzeugen

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

Also gilt

$$\mu(5,3,1) = p_1p_3p_5 - p_4p_5 - p_3p_6 - p_1p_8 + 2p_9.$$

In dem Beispiel werden allerdings auch $p_k, k > n$, verwendet, so dass obiger Beweis für (h_i) und (e_i) nicht unmittelbar übertragen werden kann.

Beweis: Jedes homogene symmetrische Polynom kann als $f = \sum_\lambda c_\lambda \mu_\lambda$ 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 $p_i, i \leq \deg(f)$ wie im betrachteten Beispiel.

Die Aussage des Satzes ergibt sich nun daraus, dass jedes symmetrische Polynom durch die elemetarsymmetrischen Polynome dargestellt werden kann und diese, wie eben bewiesen, durch $p_i, i \leq n$.

Nun können wir wie bisher auch argumentieren. Details siehe [9]. □

Invarianten der alternierenden Gruppe $A_n \subset S_n$ Das Polynom

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

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 9 *Jedes Polynom $f \in S^{A_n}$ kann eindeutig als $f = f_1 + f_2\,D$ mit symmetrischen Polynomen f_1, f_2 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: Sei $g \in S_N$ eine ungerade Permutation. Dann gilt $f^g = f_1 - f_2\,D$ für eine Zerlegung $f = f_1 + f_2\,D$, so dass sich unmittelbar und eindeutig

$$f_1 = \frac{1}{2}\,(f + f^g) \text{ und } f_2\,D = \frac{1}{2}\,(f - f^g)$$

ergibt. Damit ist die Zerlegung eindeutig, falls sie existiert.
Ist $u \in S_n$ eine gerade Permutation, so gilt $f^u = f,\ (f^g)^u = f^{(g\,u\,g^{-1})g} = f^g$, da $g\,u\,g^{-1} \in A_n$. Ist u ungerade, so gilt $f^u = f^{u\,g^{-1}g} = f^g,\ (f^g)^u = f^{g\,u} = f$, da $g\,u \in A_n$.
Damit ist $f_1 = \frac{1}{2}\,(f + f^g)$ ein symmetrisches Polynom und $f' = \frac{1}{2}\,(f - f^g)$ eine Semiinvariante bzgl. des sgn-Charakters. Es bleibt zu zeigen, dass f' stets durch D teilbar ist.
Ist $u \in S_n$ die Transposition (i, j), so gilt offensichtlich $f'^u = -f'$, also

$$f'(\ldots, x_i, \ldots, x_j, \ldots) = -f'(\ldots, x_j, \ldots, x_i, \ldots)\,.$$

Damit ergibt sich $f'|_{x_i = x_j} = 0$, d. h. f' ist durch $x_i - x_j$ für jedes (i, j) mit $1 \le i < j \le n$ teilbar. Da diese Linearformen paarweise teilerfremd sind, ist damit f' auch durch D teilbar.
Details siehe [9]. □
Sei $\lambda = (a_1 \ge a_2 \ge \ldots \ge a_n \ge 0)$ 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 Darstellungstheorie der S_n. Da offensichtlich $lt(a_\lambda) = x_1^{a_1+n-1} x_2^{a_2+n-2} x_2^{a_n}$ und damit $lt(s_\lambda) = lt(\mu_\lambda)$ gilt, sind die s_λ eines fixierten Grads d alle linear unabhängig. Da ihre Anzahl gerade gleich der Vektorraumdimension von $[R]_d$ ist, ergibt sich als weitere Schlussfolgerung der folgende Satz.

Satz 10 *Die Schurpolynome $s_\lambda \in R = S^{S_n}, d \vdash \lambda$, bilden eine k-Vektorraumbasis von $[R]_d$.*

3 Grundlegende Eigenschaften des Invariantenrings

3.1 Transzendenzgrad und Primärinvarianten

Im Folgenden sei immer $G \subset GL(V)$ eine endliche Gruppe, die auf dem Vektorraum $V = [S]_1$ der Linearformen in $S = k[x_1, \ldots, x_n]$ operiert, $N = |G|$ die Gruppenordnung, k ein Körper der Charakteristik 0[2] und $R = S^G$ der Invariantenring dieser Aktion.

[2] Es reicht, dass $char(k)$ kein Teiler von N ist (nicht modularer Fall).

Der Körper $k(X)$ der rationalen Funktionen auf $X = (x_1, \ldots, x_n)$ ist der Quotientenkörper von S. Dessen Unterkörper

$$k(X)^G = \left\{ \frac{f}{h} \ : \ \forall\, g \in G \ \left(\frac{f}{h}\right)^g = \frac{f}{h} \right\}$$

bezeichnet man als den *Invariantenkörper* von G. Offensichtlich gilt die folgende Inklusion von Körpern: $k(X) \supset k(X)^G \supset k$ und damit für die Transzendenzgrade

$$tr.deg(k(X) : k(X)^G) + tr.deg(k(X)^G : k) = tr.deg(k(X) : k) = n\,.$$

Satz 11 *Für den Invariantenkörper $k(X)^G$ gilt:*

(1) $k(X)^G$ ist der Quotientenkörper von $k[X]^G$, d. h. jeder invariante Quotient ist ein Quotient von Invarianten.

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

(3) $k(X)/k(X)^G$ ist eine Galois-Erweiterung (d. h. normal und separabel) mit der Galois-Gruppe G.

Beweis:
(1) f/h ist in $k(X)^G$, 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

$$f_i(T) := \prod_{g\in G} (T - x_i^g) = T^N + \sum_{k=1}^{N} (-1)^k\, e_k(x_i^g | g \in G) \cdot T^k \in S[T]\,,$$

wobei $e_k(\ldots)$ die k-te elementarsymmetrische Summe in den angegebenen Termen ist. Diese Formel ergibt sich unmittelbar aus dem Satz von Vieta. Alle $e_k(x_i^g | g \in G)$ sind invariant unter der Aktion von $h \in G$, denn $(x_i^{gh} | g \in G)$ ist eine Permutation der $(x_i^g | g \in G)$, symmetrische Polynome aber invariant unter solchen Permutationen. Es gilt also sogar $f_i(T) \in R[T]$.
Alle x_i sind also algebraisch über $k(X)^G$ und damit ist auch $k(X)$ algebraisch über $k(X)^G$.
Die x_i sind sogar ganze algebraische Elemente über $k[V]^G$ und damit $k[V]^G$ in $k(X)^G$ ganzabgeschlossen.
(3) folgt aus der Definition, da $g \in G$ auf $k(X)$ als Körperautomorphismus operiert. □
Beispiel: Die bereits früher betrachtete C_4-Aktion auf $k[x, y]$.

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

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

Satz 12 (Charakterisierungssatz für Primärinvarianten)
Jedes System von Primärinvarianten von R hat genau n Elemente.
Die Menge homogener Polynome $F = \{f_1, \ldots, f_n\} \subset R$ (positiven Grads) ist genau dann 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* $\overline{k}$.

Beweis: (1) und (2) sind beide äquivalent zur Aussage $tr.deg(f_1, \ldots, f_n) = n$. Für (1) ist das offensichtlich, für (2) folgt es aus der Ungleichungskette

$$n = tr.deg(x_1, \ldots, x_n) \leq tr.deg(f_1, \ldots, f_n) \leq n\,.$$

(2) $\Rightarrow$ (3): Sei $\mathbf{a} = (a_1, \ldots, a_n)$ eine gemeinsame Nullstelle. Wir betrachten die nach (2) existierende algebraische Relation

$$x_i^M + \sum_{k<M} r_{ik}(f_1, \ldots, f_n)\, x_i^k = 0\,,$$

die wir o. B. d. A. als homogen voraussetzen können. Insbesondere sind die $r_{ik}(y_1, \ldots, y_n)$ (mit $\deg(y_i) = \deg(f_i)$) homogen vom Grad $M - k > 0$, so dass jeder Term wenigstens einen Faktor f_i enthält und folglich $r_{ik}(f_1, \ldots, f_n)(\mathbf{a}) = 0$ gilt. Es folgt $a_i^M = 0$ für alle i.

(3) $\Rightarrow$ (1): Dies folgt aus dem allgemeinen Zusammenhang zwischen der Ring-Dimension von S/I, wobei $I = (f_1, \ldots, f_n)$ das von den gegebenen Polynomen erzeugte Ideal ist, und dem Transzendenzgrad von $Q(S/I)$ über dem Grundkörper. $\square$

(3) ist von praktischem Interesse, weil damit die Entscheidung, ob ein System von Invarianten algebraisch unabhängig ist, auf die oft einfachere Frage der Lösung eines polynomialen Gleichungssystems zurückgeführt wird.

Beispiel: Die Invarianten $f_2 = x^2 + y^2,\ f_{4c} = x^2y^2$ der bereits mehrfach betrachteten C_4-Aktion auf $k[x, y]$ sind algebraisch unabhängig, da $f_{4c} = 0 \Leftrightarrow x = 0$ oder $y = 0$, und dies in $f_2 = 0$ eingesetzt in jedem Fall $x = y = 0$ als einzige gemeinsame Nullstelle ergibt.

Allgemeiner gilt

Satz 13 *Die Menge homogener Polynome* $F = \{f_1, \ldots, f_s\} \subset R$ *(positiven Grads) ist algebraisch unabhängig genau dann, wenn die Dimension des Nullstellengebildes* $V(f_1, \ldots, f_s) \subset \mathbb{A}^n$ *die Dimension* $n - s$ *hat.*

Diese Dimension kann mit dem Gröbner-Algorithmus (siehe Vorlesung „Gröbnerbasen und Anwendungen“) bestimmt werden. MuPAD stellt hierfür die Funktion `groebner::dimension` zur Verfügung.

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 14 (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 $char(k) = 0$ (oder allgemeiner k genügend groß), so finden sich immer solche l_i, da sie nur endlich viele echte Teilräume meiden müssen.

Beweis: Ist

$$l_i \notin \bigcup \left\{ k\langle l_1^{g_1}, \ldots, l_{i-1}^{g_{i-1}}\rangle,\ g_1, \ldots, g_{i-1} \in G \right\}\,,$$

so gilt auch

$$l_i^g \notin \bigcup \left\{ k\langle l_1^{g_1}, \ldots, l_{i-1}^{g_{i-1}}\rangle,\ g_1, \ldots, g_{i-1} \in G \right\}$$

für alle $g \in G$, so dass $k\langle l_1^{g_1}, \ldots, l_i^{g_i}\rangle$ in jedem Fall ein i-dimensionaler Unterraum von $[S]_1$ ist.

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 $l_i^{g_i}(a) = 0$. Wegen $\dim_k(k\langle l_1^{g_1}, \ldots, l_n^{g_n}\rangle) = n$ hat das lineare Gleichungssystem $\{l_i^{g_i} = 0,\ i = 1, \ldots, n\}$ aber nur die triviale Lösung. $\square$

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 $k\langle x\rangle \cup k\langle y\rangle$. 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.

Beispiel: C_3-Aktion auf $k[x, y]$, erzeugt von einer Drehung um den Winkel $\frac{2}{3}\pi$ mit Zentrum im Ursprung. In diesem Fall kann $l_1 = x$, $l_2 = y$ genommen werden. Wir rechnen

```
vars:=[x,y];
M:=n->Dom::Matrix()([[cos(2*PI/n),sin(2*PI/n)],[-sin(2*PI/n),cos(2*PI/n)]]);
C3:=[matrix2subrules(M(3)^i,vars)$i=0..2];
expand(_mult(op(map(C3,u->subs(x,u)))));
expand(_mult(op(map(C3,u->subs(y,u)))));
```

und erhalten damit die bereits früher bestimmten $B = f_{3a} = x^3 - 3\,x\,y^2$, $C = f_{3b} = y^3 - 3\,x^2\,y$ als System von Primärvarianten, aus der sich die Hironakazerlegung $R = k[B, C] \oplus A \cdot k[B, C] \oplus A^2 \cdot k[B, C]$ ergeben hatte.

3.2 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 15 (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;
```

3.3 Der Endlichkeitssatz – Hilberts Beweis

Satz 16 (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.

3.4 Emmy Noethers Gradschranke

Satz 17 (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

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

als Polynome in $(k[\mathbf{x}])[\mathbf{u}]$. Ausmultiplizieren liefert

$$\begin{aligned} S_e(\mathbf{u}, \mathbf{x}) &= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{a_1 + \cdots + a_n = e} \binom{e}{a_1 \cdots a_n} \left(u_1 x_1^g\right)^{a_1} \cdot \ldots \cdot \left(u_n x_n^g\right)^{a_n} \right) \\ &= \sum_{a_1 + \cdots + a_n = e} \binom{e}{a_1 \cdots a_n} \left(\frac{1}{|G|} \sum_{g \in G} \left(x_1^g\right)^{a_1} \cdot \ldots \cdot \left(x_n^g\right)^{a_n} \right) \cdot u_1^{a_1} \cdot \ldots \cdot u_n^{a_n} \\ &= \sum_{a_1 + \cdots + a_n = e} \binom{e}{a_1 \cdots a_n} \rho\left(x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}\right) \cdot u_1^{a_1} \cdot \ldots \cdot u_n^{a_n} \end{aligned}$$

wobei $\binom{e}{a_1 \ldots a_n} = \frac{e!}{a_1! \cdot \ldots \cdot a_n!} \in \mathbb{N}$ der multinomiale Koeffizient in der entsprechenden Expansion ist. Der Koeffizient vor $u_1^{a_1} \cdot \ldots \cdot u_n^{a_n}$ mit $a_1 + \ldots + a_n = e$ ist also (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 $P_i, i \le N$ 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 $\le N$. $\square$

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

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

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.

4 Permutationsdarstellungen

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

4.1 Elementares über Permutationen

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

Satz 18 *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:

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

Folgerung 1 *Die Invariantenringe der Permutationsdarstellungen zueinander konjugierter Permutationsgruppen sind isomorph.*

4.2 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 19 (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. Insbesondere sind die Stabilisatoren der Elemente $m \in T$ aus einem Orbit gleich mächtig.

3. $|m^G| \cdot |G_m| = |G|$.

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 eine 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.

```
Orbit:=proc(m,G) local g;
begin {subs(m,g)$g in G} end_proc:

OrbitSum:=proc(m,G) local g;
begin _plus(op(Orbit(m,G))) end_proc:
```

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

Solche Orbitsummen fallen zusammen oder sind disjunkt. Die Vektorraumdimension der homogenen Invarianten vom Grad k können wir also durch Abzählen der *verschiedenen* Orbitsummen im entsprechenden Grad bestimmen. Dazu bilden wir die *Menge* $\{\ldots\}$ der aus allen Termen vom Grad k erzeugten Orbitsummen (was automatisch doppelt auftretende Elemente entfernt) und bestimmen mit `nops` die Anzahl der Elemente dieser Menge. Eine entsprechende Funktionsdefinition in MuPAD lautet

```
H:=k->nops(map({op(Terme(k,vars))}, OrbitSum, G));
```

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

Wir wollen ein komplexeres Beispiel durchrechnen, um ein besseres Gefühl für die technischen Schwieirigkeiten der Berechnung des Rings der Invarianten zu bekommen.

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

Da Algorithmen für Permutationen in verschiedenen MuPAD-Versionen unterschiedlich anzusprechen sind, stellen wir den weiteren Betrachtungen eine eigene einheitliche Schnittstelle zur erforderlichen Funktionalität zusammen:

```
allePermutationen:=proc(l) local u;
// Alle Permutationen der Elemente der Liste l
begin
  u:=combinat::permutations(l); // Version 4
  if u=FAIL then // nicht Version 4
    combinat::permute(l) else u end_if;
end:

permutationMatrix:=proc(l) local i,n;
// Erzeugt aus Permutation von [1,..,n] eine Permutationsmatrix
begin
  n:=nops(l);
  return (Dom::Matrix()(n,n,[(i,l[i])=1 $ i=1..n]))
end:

setDiff:= // Mengendifferenz auch für Listen definieren
proc(a,b) begin _minus({op(a)},{op(b)}) end_proc:
```

Eine solche Permutationsmatrix ist eine Matrix, wo in jeder Zeile und Spalte genau eine 1 steht.

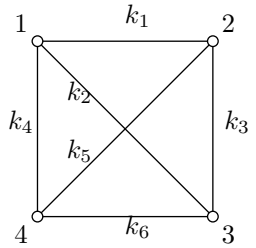
```
M:=permutationMatrix([3,1,2]);
```

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

Matrixdarstellungen können wir mit der früher eingeführten Funktion `matrix2subrules` in die subRules-Darstellungen umrechnen.

```
matrix2subrules(M,vars);
```

$$[x_1 = x_3,\ x_2 = x_1,\ x_3 = x_2]$$



Als nächstes ordnen wir den sechs Kanten des K_4 die Variablen $y_1, \ldots, y_6$ über eine Hashtabelle T zu. Für $T[\{i,j\}] = k$ ist k der Index, welcher der Kante $\{i,j\}$ zugeordnet wird.

```
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;

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;

T:=HashTabelle(4);
u:=allePermutationen([1,2,3,4]);  // 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,permutationMatrix);      // Matrixdarstellung
G:=map(w,matrix2subrules,vars);   // SubRules-Darstellung
```

Nun können wir über die Orbitsummen k-Basen der Invarianten in den verschiedenen Graden konstruieren.

Im Grad $d = 1$ gibt es eine einzige Orbitsumme

```
B_1:=[e_1 = OrbitSum(y1,G)];
```

$$e_1 = y_1 + y_2 + y_3 + y_4 + y_5 + y_6$$

Um die Invarianten im nächsten Grad $d = 2$ zu beschreiben, erzeugen wir die Menge U_d der Orbitsummen im Grad d, die eine k-Basis von $[R]_d$ bilden.

```
U_2:=map({op(Terme(2,vars))}, OrbitSum, G);
LU_2:=map(U_2,lterm,vars);
```

U_2 enthält 3 Elemente, deren (nach Konstruktion paarweise verschiedenen) Leitterme in der Menge LU_2 aufgesammelt sind. Im zweiten Schritt konstruieren wir die Liste V_2 alle Invarianten im Grad d, die sich als Produkte von Basisinvarianten kleineren Grades erzeugen lassen, sowie die Liste LV_2 der zugehörigen Leitterme.

```
V_2:=GewichteteProdukte(2,B_1,vars);
LV_2:=map(V_2,v->lterm(rhs(v)),vars);
```

Die folgende Funktion `setDiff` bestimmt die Differenzmenge zweier als Listen oder Mengen gegebener Termfamilien:

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

`setDiff(LU_2,LV_2)` bestimmt die beiden Terme im Grad 2, die noch nicht als Leitterme in V_2 vorkommen. Daraus erzeugen wir zwei neue Basisinvarianten

```
B_2:=[e_2a = OrbitSum(y1*y2,G), e_2b = OrbitSum(y1*y6,G)];
```

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

und haben auf diese Weise mit $V_2 \cup B_2$ eine k-Basis von $[R]_2$ bestimmt. Mit $e_2 = e_{2a} + e_{2b}$ lässt sich die elementarsymmetrische Summe e_2 – Invariante der symmetrischen Gruppe – als Summe zweier unter G invarianter Teilsummen $e_2 = e_{2a} + e_{2b}$ darstellen.

Analog erhalten wir eine k-Basis aus 6 Invarianten vom Grad $d = 3$.

```
U_3:=map({op(Terme(3,vars))}, OrbitSum, G);
LU_3:=map(U_3,lterm,vars);
```

Drei davon lassen sich als $e_1\,e_{2a}$, $e_1\,e_{2b}$ bzw. e_1^3 darstellen:

```
V_3:=GewichteteProdukte(3,B_1.B_2,vars);
LV_3:=map(V_3,v->lterm(rhs(v)),vars);
```

Weitere drei Invarianten sind in die Liste der Basisinvarianten aufzunehmen.

```
setDiff(LU_3,LV_3);
B_3:=[ e_3a = OrbitSum(y1*y2*y3,G),
       e_3b = OrbitSum(y1*y2*y4,G),
       e_3c = OrbitSum(y1*y2*y5,G)];
```

$$
\begin{aligned}
e_{3a} &= y_1\,y_2\,y_3 + y_1\,y_4\,y_5 + y_2\,y_4\,y_6 + y_3\,y_5\,y_6\\
e_{3b} &= y_1\,y_2\,y_4 + y_1\,y_3\,y_5 + y_2\,y_3\,y_6 + y_4\,y_5\,y_6\\
e_{3c} &= y_1\,y_2\,y_5 + y_1\,y_3\,y_4 + y_1\,y_2\,y_6 + y_2\,y_3\,y_4 + y_1\,y_3\,y_6 + y_2\,y_3\,y_5 + y_1\,y_4\,y_6 + y_2\,y_4\,y_5\\
&\quad + y_1\,y_5\,y_6 + y_3\,y_4\,y_5 + y_2\,y_5\,y_6 + y_3\,y_4\,y_6
\end{aligned}
$$

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 $d = 4$ ergeben die entsprechenden Rechnungen

```
U_4:=map({op(Terme(4,vars))}, OrbitSum, G);
LU_4:=map(U_4,lterm,vars);
V_4:=GewichteteProdukte(4,B_1.B_2.B_3,vars);
LV_4:=map(V_4,v->lterm(rhs(v)),vars);
[nops(U_4),nops(V_4),setDiff(LU_4,LV_4)];
```

folgendes Bild: U_4 als k-Basis besteht aus 11 Elementen, wovon mit V_4 9 Elemente mit paarweise verschiedenen Leittermen aus Invarianten kleineren Grads kombiniert werden können. Zwei weitere Invarianten

```
B_4:=[ e_4a = OrbitSum(y1*y2*y3*y4,G), e_4b = OrbitSum(y1*y2*y5*y6,G)];
```

$$
\begin{aligned}
e_{4a} &= y_1\,y_2\,y_3\,y_4 + y_1\,y_2\,y_3\,y_5 + y_1\,y_2\,y_3\,y_6 + y_1\,y_2\,y_4\,y_5 + y_1\,y_2\,y_4\,y_6 + y_1\,y_3\,y_4\,y_5\\
&\quad + y_1\,y_3\,y_5\,y_6 + y_2\,y_3\,y_4\,y_6 + y_1\,y_4\,y_5\,y_6 + y_2\,y_3\,y_5\,y_6 + y_2\,y_4\,y_5\,y_6 + y_3\,y_4\,y_5\,y_6\\
e_{4b} &= y_1\,y_2\,y_5\,y_6 + y_1\,y_3\,y_4\,y_6 + y_2\,y_3\,y_4\,y_5
\end{aligned}
$$

müssen zum System der Basisinvarianten hinzugenommen werden.

Im Grad $d = 5$ ergeben die entsprechenden Rechnungen

```
U_5:=map({op(Terme(5,vars))}, OrbitSum, G);
LU_5:=map(U_5,lterm,vars);
V_5:=GewichteteProdukte(5,B_1.B_2.B_3.B_4,vars);
LV_5:=map(V_5,v->lterm(rhs(v)),vars);
[nops(U_5),nops(V_5),setDiff(LU_5,LV_5)];
```

Die k-Basis U_5 besteht aus 18, das System V_5 aus 17 Elementen. Allerdings besteht die Differenzmenge der Leitterme aus *zwei* Elementen, woraus wir schlussfolgern, dass zwei Elemente aus V_5 denselben Leitterm haben.

Um dies genauer zu analysieren, nehmen wir zunächst die beiden Elemente

```
B_5:= [ u_5 = OrbitSum(y1^2*y2*y6^2,G), e_5 = OrbitSum(y1*y2*y3*y4*y5,G)];
```

hinzu und untersuchen die Menge $V_5 \cup B_5$ auf lineare Abhängigkeiten:

```
rel:=findRelations(V_5.B_5,vars);
r1:=subs(rel[1],z=1);
```

Die dabei hergeleitete Relation $e_5 + u_5 + e_1\, e_{4b} - e_{2b}\, e_{3c}$ zeigt, dass man eines der beiden Elemente weglassen kann. Wir entscheiden uns für das Weglassen von u_5.

```
B_5:= [ e_5 = OrbitSum(y1*y2*y3*y4*y5,G)];
```

Im Grad $d = 6$ werden die Zusammenhänge noch unübersichtlicher:

```
U_6:=map({op(Terme(6,vars))}, OrbitSum, G);
LU_6:=map(U_6,lterm,vars);
V_6:=GewichteteProdukte(6,B_1.B_2.B_3.B_4.B_5,vars);
LV_6:=map(V_6,v->lterm(rhs(v)),vars);
[nops(U_6),nops(V_6),setDiff(LU_6,LV_6)];
```

32 Invarianten in der Basis U_6 stehen 32 abgeleitete Invarianten V_6 gegenüber, aber zwei Leitterme kommen dabei nicht (und damit zwei andere doppelt) vor. Untersuchen wir wieder die entsprechenden linearen Abhängigkeiten in der Menge $V_6 \cup B_6$:

```
B_6:=[ u_6=OrbitSum(y1^2*y2*y3*y6^2,G), e_6=OrbitSum(y1*y2*y3*y4*y5*y6,G)];

rel:=findRelations(V_6.B_6,vars);
r1:=subs(rel[1],z1=48,z=0);
r2:=subs(rel[1],z1=0,z=3);
```

$$\begin{aligned} r_1 = {} & 48\, e_6 - 4\, e_{2a}\, e_{2b}^2 - 4\, e_1^2\, e_{4b} - 4\, e_{3c}^2 - 8\, e_1\, e_5 + 3\, e_{2a}\, e_{4a} + 16\ e_{2a}\, e_{4b} + 4\, e_{2b}\, e_{4a} \\ & - 3\, e_{3a}\, e_{3b} - 3\, e_{3a}\, e_{3c} - 3\, e_{3b}\, e_{3c} + 4\, e_1\, e_{2b}\, e_{3c} \qquad \text{(B.6.1)} \\ r_2 = {} & 3\, u_6 - e_{4b}\, e_1^2 + e_1\, e_{2b}\, e_{3c} + e_5\, e_1 - e_{2a}\, e_{2b}^2 - 2\, e_{4a}\, e_{2b} - e_{3c}^2 + 4\, e_{2a}\, e_{4b} \qquad \text{(B.6.2)} \end{aligned}$$

Im Grad $d = 6$ müssen wir also gar keine weiteren Invarianten zum Satz der Basisinvarianten hinzunehmen. Insbesondere ergibt sich auch e_6 als polynomiale Kombination von Basisinvarianten kleineren Grades.

Zur genaueren Analyse des Invariantenrings bestimmen wir nun zunächst weitere Summanden der Molienreihe mit der oben bereits eingeführten Funktion $H(k)$

```
H:=k->nops(map({op(Terme(k,vars))}, OrbitSum, G));

HK:=_plus(H(k)*t^k$k=0..15)+O(t^16)
```

$$\begin{aligned} & 1 + t + 3\, t^2 + 6\, t^3 + 11\, t^4 + 18\, t^5 + 32\, t^6 + 48\, t^7 + 75\, t^8 + 111\, t^9 + 160\, t^{10} + 224\, t^{11} \\ & \quad + 313\, t^{12} + 420\, t^{13} + 562\, t^{14} + 738\, t^{15} + O(t^{16}) \end{aligned}$$

Welche Teilmengen der Menge $B = B_1 \cup \cdots \cup B_5$ der Basisinvarianten können (statt $e_1, \ldots, e_6$) als Systeme von Primärinvarianten verwendet werden? Rechnung mit MuPAD zeigt

```
B:=B_1.B_2.B_3.B_4.B_5;
sys:=subs([e_1,e_2a,e_2b,e_3a,e_3b,e_3c],B);
solve(sys,vars,IgnoreSpecialCases);
```

dass dieses System nichttriviale Lösungen besitzt und folglich nicht als Primärinvarianten durchgeht. Analog kann man andere Kombinationen durchprobieren. Dies kann über die Analyse der Dimension entsprechender Teilsysteme mit `groebner::dimension` genauer untersucht werden. Zum Beispiel zeigt

```
sys:=subs([e_1,e_2a,e_2b],B);
groebner::dimension(sys);
```

dass dieses Teilsystem ein Nullstellengebilde der Dimension 3 hat und folglich algebraisch unabhängig ist. Untersuchen wir mögliche andere Ergänzungen

```
sys:=subs([e_1,e_2a,e_2b,e_3a,e_3b,e_4a],B); // (1)
sys:=subs([e_1,e_2a,e_2b,e_3a,e_3b,e_4b],B); // (2)
```

mit `groebner::dimension`, so erkennen wir, dass (1) nichttriviale Lösungen hat, (2) dagegen ein System von Primärinvarianten ist. $R_0 = k[e_1, e_{2a}, e_{2b}, e_{3a}, e_{3b}, e_{4b}]$ hat die Hilbertreihe

$$HK_0 = \frac{1}{(1-t)\,(1-t^2)^2\,(1-t^3)^2\,(1-t^4)}$$

und ein Vergleich der Taylorreihen

```
taylor(HK-HK0,t)
```

$$t^3 + 2\,t^4 + 5\,t^5 + +10\,t^6 + 18\,t^7 + 30\,t^8 + O(t^9)$$

zeigt, dass eine weitere Sekundärinvariante im Grad 3 zu suchen ist. Klar, dies ist e_{3c} und die nächste Näherung des Invariantenrings (die Existenz einer Hironakazerlegung vorausgesetzt) $R_1 = R_0 \oplus e_{3c}\,R_0$ hat die Hilbertreihe $HK_1 = (1+t^3)\,HK_0$. Der Vergleich dieser Hilbertreihen

```
taylor(HK-(1+t^3)*HK0,t)
```

ergibt eine weitere Sekundärinvariante im Grad 4 (e_{4a}) usw. Bis zur gegebenen Genauigkeit $O(t^{10})$ finden wir schließlich eine Zerlegung

$$R_0 \oplus e_{3c}\,R_0 \oplus e_{4a}\,R_0 \oplus e_5\,R_0 \oplus u_6\,R_0 \oplus u_9\,R_0$$

wovon wir einzig die Invarianten u_6 vom Grad 6 und u_9 vom Grad 9 noch nicht verstehen.

```
taylor(HK-(1+t^3+t^4+t^5+t^6+t^9)*HK0,t)
```

liefert auch bei höherer Anfangsgenauigkeit von HK nur Terme innerhalb der Toleranzgrenze, so dass wir vermuten können, ein vollständiges System von Sekundärinvarianten gefunden zu haben, wobei die genaue Bestimmung von u_6 und u_9 noch aussteht. Wir kommen auf dieses Beispiel weiter unten zurück.

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

Als weitere Beispiele wollen wir die oben entwickelte Vorgehensweise anwenden, um Invariantenringe von Untergruppen der S_4 zu klassifizieren. Solche Untergruppen 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 *fixpuntkfrei*, 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:

$$\mathbb{Q}[x_1, x_2, x_3, x_4]^G = \mathbb{Q}[x_1, x_2, x_3]^G \otimes_{\mathbb{Q}} \mathbb{Q}[x_4].$$

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 in Permutationsmatrizen, erzeugen daraus die jeweilige Menge der Gruppenelemente und wandeln diese Menge schließlich in die SubRules-Darstellung um.

Die zyklische Gruppe C_4 Markiert man die Ecken eines Quadrats mit $x_1, \ldots, x_4$, so wird diese Gruppe von der Eckenpermutation erzeugt, die von der Drehung s_1 des Quadrats um 90° induziert ist.

```
vars:=[x1,x2,x3,x4];
s1:=permutationMatrix([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 In derselben Interpretation wird diese Gruppe von den Eckenpermutationen erzeugt, die von den Geradenspiegelungen um die beiden Symmetrieachsen des Quadrats induziert werden, die durch gegenüberliegende Kantenmitten gehen. Das Produkt der beiden Geradenspiegelungen ist die Punktspiegelung des Quadrats, welche der Permutation s_1^2 entspricht. V_4 ist die kleinste nichtzyklische Gruppe.

```
s2a:=permutationMatrix([2,1,4,3]); // (12)(34)
s2b:=permutationMatrix([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 kleinste Gruppe, die C_4 und s_{2a} umfasst, wird von der Gruppe der acht Kongruenzbewegungen des Quadrats induziert. Das Produkt aus einer Drehung und einer Geradenspiegelung ist wieder eine Geradenspiegelung, wobei auch die Geradenspiegelungen an den Symmetrieachsen durch gegenüberliegende Eckpunkte vorkommen, welche nicht fixpunktfreie Eckenpermutationen induzieren. Dies ist zugleich die (bis auf Konjugation) einzige Untergruppe der Ordnung 8 der S_4.

```
M_D4:={(u,s2a*u)$u in M_C4};
s1*s2a = s2a*s1^3; // = (13)
D4:=map(M_D4,matrix2subrules,[x1,x2,x3,x4]);
```

Die Gruppe der geraden Permutationen A_4 Diese Gruppe aus 12 Elementen kann geometrisch als Drehgruppe des Tetraeders interpretiert werden. Sie ist die (wieder bis auf Konjugierte) einzige Untergruppe vom Index 2 der S_4 und kann als das halbdirekte Produkt der von (123) erzeugten zyklischen Gruppe C_3 und der V_4 angeschrieben werden. Den Ring der Invarianten der A_n hatten wir bereits für beliebige n beschrieben.

```
s3:=permutationMatrix([2,3,1,4]); // (123)
M_C3:={s3^i$i=0..2};
M_A4:={u*v$u in M_C3$v in M_V4};
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 und bestimmen nach dem oben beschriebenen Schema ein Anfangsstück der Molienreihe

```
H:=k->nops(map({op(Terme(k,vars))}, OrbitSum, C4));
HR:=_plus(H(k)*t^k$k=0..10)
```

$$1 + t + 3\,t^2 + 5\,t^3 + 10\,t^4 + 14\,t^5 + 22\,t^6 + 30\,t^7 + 43\,t^8 + 55\,t^9 + O(t^{10})$$

Wir führen die Rechnungen nach dem oben entwickelten Muster aus

```
B_1:=[e_1=OrbitSum(x1,C4)];
```

$$e_1 = x_1 + x_2 + x_3 + x_4$$

```
U_2:=map({op(Terme(2,vars))}, OrbitSum, C4); nops(%);
LU_2:=map(U_2,lterm,vars);
V_2:=GewichteteProdukte(2,B_1,vars);
LV_2:=map(V_2,v->lterm(rhs(v)),vars);
setDiff(LU_2,LV_2);
B_2:=[e_2a = OrbitSum(x1*x2,C4), e_2b = OrbitSum(x1*x3,C4)];
```

$$e_{2a} = x_1x_2 + x_1x_4 + x_2x_3 + x_3x_4, \quad e_{2b} = x_1x_3 + x_2x_4$$

Die drei Invarianten e_1, e_{2a}, e_{2b} sind auch algebraisch unabhängig:

```
groebner::dimension(subs([e_1,e_2a,e_2b],B_1.B_2));  // = 1
```

Im Grad 3 gehen wir ähnlich vor:

```
U_3:=map({op(Terme(3,vars))}, OrbitSum, C4); nops(%);
LU_3:=map(U_3,lterm,vars);
V_3:=GewichteteProdukte(3,B_1.B_2,vars);
LV_3:=map(V_3,v->lterm(rhs(v)),vars);
setDiff(LU_3,LV_3);
B_3:=[e_3a=OrbitSum(x1^2*x4,C4),e_3=OrbitSum(x1*x2*x3,C4)];
```

$$e_{3a} = x_1^2x_4 + x_1x_2^2 + x_2x_3^2 + x_3x_4^2, \quad e_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

Test mit `groebner::dimension` zeigt, dass keine dieser beiden Invarianten (e_1, e_{2a}, e_{2b}) zu einem algebraisch unabhängigen System ergänzt.

Im Grad 4 begegnen wir wieder dem Phänomen, dass V_4 zwar 8 Elemente enthält, aber nur 7 verschiedene Leitterme.

```
U_4:=map({op(Terme(4,vars))}, OrbitSum, C4); nops(%);
LU_4:=map(U_4,lterm,vars);
V_4:=GewichteteProdukte(4,B_1.B_2.B_3,vars);
LV_4:=map(V_4,v->lterm(rhs(v)),vars);
[nops(U_4),nops(V_4),setDiff(LU_4,LV_4)];
```

Invarianten mit den fehlenden Leittermen können wir als die zugehörigen Orbitsummen generieren.

```
B_4:=[ e_4a=OrbitSum(x1^2*x2*x4,C4),
       e_4b=OrbitSum(x1^2*x3*x4,C4),
       e_4=OrbitSum(x1*x2*x3*x4,C4)];
```

Zwischen diesen drei Invarianten besteht eine Relation

```
findRelations(V_4.B_4,vars);
```

$$4e_4 + e_{4a} - e_1e_3 + e_{2a}e_{2b}$$

Jede von diesen Invarianten ist algebraisch unabhängig von (e_1, e_{2a}, e_{2b}), so dass wir als System von Primärinvarianten etwa $(e_1, e_{2a}, e_{2b}, e_4)$ nehmen und e_{4a} im Weiteren wegfallen lassen können. Wir setzen $R_0 = k[e_1, e_{2a}, e_{2b}, e_4]$ mit der Hilbertreihe

$$H_0 = \frac{1}{(1-t)\,(1-t^2)^2\,(1-t^4)}\,.$$

Wir können unsere bisherigen Untersuchungen zusammenfassen zu der Aussage, dass – Hironakazerlegung vorausgesetzt – der Invariantenring einen Unterring der Struktur

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

hat. Ein Vergleich der Hilbertreihen

```
HR0:=1/((1-t)*(1-t^2)^2*(1-t^4));
taylor(HR-(1+2*t^3+t^4)*HR0,t);
```

liefert nur noch Terme der Größe $O(t^{10})$, was darauf hindeutet, dass wir schon den ganze Invariantenring gefunden haben.

Aufgabe 4 Bestimmen Sie die Darstellungen der Invarianten $e_3^2, e_3\,e_{3a}, \ldots$ als Elemente von R'.
Hinweis: Wenden Sie das Verfahren zur Bestimmung der Relationen an, welches unten am Beispiel der V_4 und D_4 demonstriert wird.

Die Invarianten der V_4

Bestimmen wir nach demselben Prinzip die Invarianten der V_4.

```
H:=k->nops(map({op(Terme(k,vars))}, Reynolds, V4));
HR:=_plus(H(k)*t^k$k=0..9)+O(t^10)
```

$$1 + t + 4\,t^2 + 5\,t^3 + 11\,t^4 + 14\,t^5 + 24\,t^6 + 30\,t^7 + 45\,t^8 + 55\,t^9 + O(t^{10})$$

```
B_1:=[ e_1=OrbitSum(x1,V4)];
B_2:=[ e_2a = OrbitSum(x1*x2,V4),
       e_2b = OrbitSum(x1*x3,V4),
       e_2c = OrbitSum(x1*x4,V4)];
```

$$e_1 = x_1 + x_2 + x_3 + x_4,\ e_{2a} = x_1x_2 + x_3x_4,\ e_{2b} = x_1x_3 + x_2x_4,\ e_{2c} = x_1x_4 + x_2x_3$$

Wir haben 4 Invarianten gefunden und stellen mit `groebner::dimension` fest, dass es sich bereits um ein System von Primärinvarianten handelt. Wir setzen $R_0 = k[e_1, e_{2a}, e_{2b}, e_{2c}]$ mit der Hilbertreihe

$$H_0 = \frac{1}{(1-t)\,(1-t^2)^3}.$$

Ein Vergleich der Hilbertreihen

```
HR0:=1/((1-t)*(1-t^2)^3);
taylor(HR-HR0,t);
```

zeigt, dass eine weitere Sekundärinvariante im Grad 3 zu suchen ist.

```
B_3:=[e_3=OrbitSum(x1*x2*x3,V4)];
```

$$e_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4$$

```
taylor(HR-(1+t^3)*HR0,t);
```

Damit scheinen wir alles gefunden zu haben, was die Vermutung $R = R_0 \oplus e_3 \cdot R_0$ nahe legt.
e_3^2 als Invariante vom Grad 6 muss eine Zerlegung als Element der Summe $[R_0]_6 \oplus e_3 \cdot [R_0]_3$ haben. Diese kann wieder über eine Analyse der Relationen der Invarianten vom Grad 6 gefunden werden.

```
B:=B_1.B_2.B_3;
V_6:=GewichteteProdukte(6,B,vars);
rel:=findRelations(V_6,vars);
r:=collect(subs(rel[1],z=1),e_3);
```

$$\begin{aligned}&4\,e_3^2 + \left(e_1^3 - 4\,e_1\,(e_{2a}+e_{2b}+e_{2c})\right)e_3\\ &\quad + \left(4\,e_{2a}^2e_{2b} - e_1^2(e_{2a}e_{2b}+e_{2a}e_{2c}+e_{2b}e_{2c}) + 4\,(e_{2a}+e_{2b})(e_{2a}+e_{2c})(e_{2b}+e_{2c})\right)\end{aligned}$$

Die Invarianten der D_4

Bestimmen wir nach demselben Prinzip die Invarianten der D_4.

```
H:=k->nops(map({op(Terme(k,vars))}, Reynolds, D4));
HR:=_plus(H(k)*t^k$k=0..9)+O(t^10)
```

$$1 + t + 3\,t^2 + 4\,t^3 + 8\,t^4 + 10\,t^5 + 16\,t^6 + 20\,t^7 + 29\,t^8 + 35\,t^9 + O(t^{10})$$

```
B_1:=[ e_1=OrbitSum(x1,D4)];
B_2:=[ e_2a = OrbitSum(x1*x2,D4), e_2b = OrbitSum(x1*x3,D4)];
```

$$e_1 = x_1 + x_2 + x_3 + x_4,\ e_{2a} = x_1x_2 + x_1x_4 + x_2x_3 + x_3x_4,\ e_{2b} = x_1x_3 + x_2x_4$$

Im Grad 3 findet sich als weitere Invariante

```
B_3:=[e_3=OrbitSum(x1*x2*x3,D4)];
```

die elementarsymmetrische Summe e_3, die aber von e_1, e_{2a}, e_{2b} algebraisch abhängt.
Im Grad 4 finden sich zwei weitere Elemente e_{4a}, e_4, die aber zusammen mit V_4 ein linear abhängiges System ergeben, aus dem e_{4a} weggelassen werden kann.

```
B_4:=[ e_4=OrbitSum(x1*x2*x3*x4,D4) ];
```

$(e_1, e_{2a}, e_{2b}, e_4)$ sind algebraisch unabhängig und somit ein System von Primärinvarianten. Mit $R_0 = k[e_1, e_{2a}, e_{2b}, e_4]$ ergibt sich die wieder die Vermutung $R = R_0 \oplus e_3 \cdot R_0$, die durch Vergleich der Molienreihen bestätigt wird.
Die Darstellung von e_3^2 als Invariante vom Grad 6

```
B:=B_1.B_2.B_3.B_4;
V_6:=GewichteteProdukte(6,B,vars);
rel:=findRelations(V_6,vars);
r:=collect(subs(rel[1],z=1),e_3);
```

ergibt in diesem Fall die Formel

$$e_3^2 - (e_1 e_{2b})\, e_3 + \left(e_4 e_1^2 + e_{2a} e_{2b}^2 - 4\, e_{2a} e_4\right)$$

Die Invarianten der A_4

Mit denselben Methoden ergeben sich als Basisinvarianten bis zum Grad 4 genau die elementarsymmetrischen Summen e_1, e_2, e_3, e_4. Diese bilden ein System von Primärinvarianten und ein Vergleich der Molienreihen weist auf eine weitere Basisinvariante vom Grad 6 hin. Hierfür kann

$$u_6 = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$$

genommen werden in Übereinstimmung mit der bereits früher gefundenen allgemeinen Charakterisierung des Invariantenrings der A_n.

5 Etwas mehr Theorie

Fassen wir unsere bisherigen Kenntnisse über die Nützlichkeit von Hilbertreihen in der Invariantentheorie zusammen:

Ist R_0 der freie Polynomring, der von Primärinvarianten erzeugt wird, und $R = h_1 \cdot R_0 \oplus \cdots \oplus h_k \cdot R_0$ eine Hironaka-Zerlegung des Invariantenrings mit den Sekundärinvarianten $h_1, \ldots, h_k$ (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 wie im Beispiel des Invariantenrings $R = S^{V_4}$ diesen als Faktorring $R = \mathbb{Q}[e_1, e_{2a}, e_{2b}, e_{2c}, e_3]/(f)$ darstellen und erhalten aus der entsprechenden Formel eine *exakte* Darstellung für die Hilbertreihe

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

Aus der Taylorreihenentwicklung dieser Funktion können wir 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);
```

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

5.1 Der Satz von Molien

In den bisherigen Beispielen hatten wir stets eine Unteralgebra $R' \subset R$ des zu berechnenden Invariantenrings gefunden und durch Vergleich der Hilbertreihen festgestellt, dass $[R']_d = [R]_d$ für alle $d \leq d_0$ gilt, wobei d_0 die Gradschranke war, bis zu der wir die Rechnungen vorangetrieben

hatten. Aus der bekannten Algebrastruktur von R' konnten wir dabei die Hilbertreihe $H(R',t)$ *exakt* berechnen. Verbleibende Unsicherheiten, ob bereits generell $R = R'$ gilt, rührten aus der ungenauen Kenntnis von $H(R,t)$ her.

Der folgende **Satz von Molien** erlaubt es, auch die Hilbertreihe $H(R,t)$ des Invariantenrings R allein aus der Kenntnis der Gruppenaktion, also der Wirkung von G auf $[S]_1$, zu bestimmen.

Satz 20 (Satz von Molien, 1897) *Gegeben ist die endliche Gruppe $G \subset Gl(n,k)$, die auf den Linearformen $[S]_1$ des Polynomring $S = k[x_1,\ldots,x_n]$ wirkt.*
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 $g = M_g = M_g^{(1)} \in Gl(n,k)$ die Matrixdarstellung der Aktion von $g \in G$ auf den Linearformen $[S]_1$ und E_n die Einheitsmatrix ist.

Die Hilbertreihe eines Invariantenrings wird zu Ehren des Entdeckers dieses Zusammenhangs 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 $R = S^{V_4}$

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

und aus der Taylorreihe die zu erwartenden Vektorraumdimensionen ebenfalls als

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

Beide Reihen sind als rationale Funktionen identisch, womit die Vektorraumdimensionen der homogenen Komponenten von $R' = R_0 \oplus e_3\cdot R_0$ und R in *allen* Graden übereinstimmen, so dass wir damit *bewiesen* 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.

5.2 Beweis des Satzes von Molien

Wir wollen im Weiteren G mit der Untergruppe $\{M_g : g \in G\} \subset Gl([S]_1)$ identifizieren.

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

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

Beispiel: Wir betrachten die Matrix $s_1 \in C_4$ aus obigem Beispiel

```
vars:=[x1,x2,x3,x4];
s1:=combinat::permutations::toMatrix([2,3,4,1]); // (1234)
```

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

und berechnen deren Eigenwerte und Eigenvektoren

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

$$\left[\left[1, 1, \left[\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right] \right], \left[-1, 1, \left[\begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \end{pmatrix} \right] \right], \left[-\mathrm{i}, 1, \left[\begin{pmatrix} -\mathrm{i} \\ -1 \\ \mathrm{i} \\ 1 \end{pmatrix} \right] \right], \left[\mathrm{i}, 1, \left[\begin{pmatrix} \mathrm{i} \\ -1 \\ -\mathrm{i} \\ 1 \end{pmatrix} \right] \right] \right]$$

Die Eigenräume sind eindimensional, so dass nach Basiswechsel mit der Matrix

```
TM:=linalg::concatMatrix(op(map(ev,u->u[3][1])));
```

$$\begin{pmatrix} 1 & -1 & -\mathrm{i} & \mathrm{i} \\ 1 & 1 & -1 & -1 \\ 1 & -1 & \mathrm{i} & -\mathrm{i} \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

Als neue Basis erhält man

```
neueBasis:=linalg::transpose(Dom::Matrix()([vars])*TM)
```

$$\begin{pmatrix} x_1+x_2+x_3+x_4 \\ x_2-x_1-x_3+x_4 \\ x_4-x_2+x_3\ \mathrm{i}-x_1\ \mathrm{i} \\ x_4-x_2-x_3\ \mathrm{i}+x_1\ \mathrm{i} \end{pmatrix}$$

Die Transformationsmatrix in der neuen Basis ist diagonal und hat folgendes Aussehen:

```
TM^(-1)*s1*TM
```

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -\mathrm{i} & 0 \\ 0 & 0 & 0 & \mathrm{i} \end{pmatrix}$$

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

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

und

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

5.3 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 $l_1+2\,l_2+\dots+n\,l_n=n$), so wird die Folge $(l_1,\dots,l_n)$ (auch als $1^{l_1}2^{l_2}\dots n^{l_n}$ geschrieben) als *Zyklentyp* von σ bezeichnet.

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

Lemma 1 *Hat die Permutation $g\in S_n$ den Zyklentyp $(l_1,\dots,l_n)$, 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 $D_{a_1},\dots,D_{a_k}$, 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:

$G = C_4$:

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

$G = V_4$:

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

$G = D_4$:

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

$G = A_4$:

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

$G = S_4$:

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

Diese Rechnungen zeigen, dass die im letzten Kapitel bestimmten Unterringe R' der jeweiligen Invariantenringe R, deren Übereinstimmung wir dort bis zu einer durch die Genauigkeit der Taylor-Expansion gegebenen Gradschranke bewiesen hatten, in der Tat in *allen* Graden übereinstimmen, da die zugehörigen Hilbertreihen von R' (im letzten Kapitel berechnet) und R (hier berechnet) als rationale Funktionen übereinstimmen.

5.4 Cohen-Macaulay-Ringe und die Hironaka-Zerlegung

$R = [R]_0 \oplus [R]_1 \oplus \ldots$ sei eine graduierte k-Algebra. Ein maximales System $(\theta_1, \ldots, \theta_n)$ 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 $U = R_0 = k[\theta_1, \ldots, \theta_n]$, lässt sich also als Summe $R = \sum_{m\in E} m \cdot R_0$ einer endlichen Anzahl homogener Elemente $m \in \Sigma$ schreiben. E ist dabei ein Erzeugendensystem von R als R_0-Modul.

5.5 Das graduierte Nakayama-Lemma

Ein minimales Erzeugendensystem E kann man durch „Ausfaktorisieren“ eines solchen Parametersystems $\Theta = (\theta_1, \ldots, \theta_n)$ gewinnen.

Lemma 2 (Graduiertes Nakayama-Lemma) *Ist $U = [U]_0 \oplus [U]_1 \oplus \ldots$ eine graduierte k-Algebra mit $[U]_0 = k$, $U_+ = \oplus_{d>0}[U]_d$ das von den homogenen Elementen positiven Grads erzeugte (einzige maximale homogene) Ideal in U, M ein graduierter U-Modul und $E \subset M$ eine endliche Menge homogener Elemente, so sind die folgenden beiden Bedingungen äquivalent:*

(1) E erzeugt M als U-Modul.

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

Ein *minimales* Erzeugendensystem von M als U-Modul korrespondiert also zu einer k-Vektorraumbasis von M/U_+M. Insbesondere sind Anzahl und Grade eines minimalen Erzeugendensystems von M als homogener U-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 $M_0 = \sum_{m\in E} m\,U$ liegt. Wegen (2) wissen wir, dass $\alpha_m \in k$ für $m \in E$ und homogene $a_i \in U_+, h_i \in M$ existieren, so dass

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

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 $h_i \in M_0$ nach Induktionsvoraussetzung und damit auch $g \in M_0$. $\square$

Setzen wir $M = R = S^G$ und $U = R_0 = k[\Theta]$, wobei $\Theta = (\theta_1, \ldots, \theta_n)$ 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 $(\theta_1, \ldots, \theta_n)$ erzeugte Ideal.

Beispiel: Kehren wir zur Berechnung des Invariantenrings der S_4-Aktion auf den sechs Kanten des K_4 zurück und sehen uns an, welche Relationen in verschiedenen Graden zwischen dem System $\Theta = (e_1, e_{2a}, e_{2b}, e_{3a}, e_{3b}, e_{4b})$ von Primärinvarianten und den Sekundärinvarianten e_{3c}, e_{4a}, e_5 bestehen:

```
pinv:=[e_1,e_2a,e_2b,e_3a,e_3b,e_4b];
sinv:=[e_3c,e_4a,e_5];
pzero:=map(pinv,u->u=0);
```

Die Substitution `pzero` entspricht dabei der Reduktion modulo Θ.

Weiter oben hatten wir bereits gesehen, dass die 32 Produkte in V_6 eine Basis von $[R]_6$ bilden. `map(`V_6`,lhs)` extrahiert die 32 Produkte, die $[R]_6$ als k-Vektorraum und damit erst recht als R_0-Modul erzeugen.

```
V_6:=GewichteteProdukte(6,B,vars);
subs(map(V_6,lhs),pzero);
```

Das zweite Kommando berechnet die Reste modulo Θ. 31 der Elemente reduzieren zu Null, sind also in

$$[R_0]_6 \oplus e_{3c}\,[R_0]_3 \oplus e_{4a}\,[R_0]_2 \oplus e_5\,[R_0]_1 \subset \Theta + e_{3c}\,\Theta + e_{4a}\,\Theta + e_5\,\Theta$$

enthalten. Neues erzeugendes Element im Grad 6 ist e_{3c}^2. Wir können also $u_6 = e_{3c}^2$ setzen.

Analog können wir die nächsten Grade inspizieren, um weitere Relationen zwischen den Basisinvarianten zu finden. Im Grad 7 ergibt sich

```
V_7:=GewichteteProdukte(7,B,vars);
rel:=findRelations(V_7,vars);
r3:=collect(coeff(rel[1],z),sinv);
```

$$\begin{aligned} 3\,e_{3c}\,e_{4a} = {} & e_1\,e_{3c}^2 - \left(e_1^2\,e_{2b}\right)\,e_{3c} + \left(2\,e_1\,e_{2b}\right)\,e_{4a} + \left(3\,e_{2a} - e_1^2\right)\,e_5 \\ & + \left(e_1^3\,e_{4b} - 3\,e_{2b}^2\,e_{3a} - 3\,e_{2b}^2\,e_{3b} + 9\,e_{3a}\,e_{4b} + 9\,e_{3b}\,e_{4b} - 4\,e_1\,e_{2a}\,e_{4b} + e_1\,e_{2a}\,e_{2b}^2\right) \end{aligned}$$

Diese Relation zeigt, dass $e_{3c}\,e_{4a} \in R'$ für $R' = R_0 \oplus e_{3c}\,R_0 \oplus e_{4a}\,R_0 \oplus e_5\,R_0 \oplus e_{3c}^2\,R_0$ gilt.

EIn Teil dieser Relationen ist aus kleineren Graden geerbt, liegt also in $\Theta\,R'$. Mit

```
subs(rel,pzero)
```

$$\{-3\, e_{3c}\, e_{4a}\, z\}$$

rechnen wir modulo dieser Relationen (Nakayama-Lemma) und erhalten ein übersichtlicheres Bild über neue Relationen. Aus dem Ergebnis können wir direkt auf $e_{3c}\, e_{4a} \in R'$ schließen.

Im Grad 8 erhalten wir auf diesem Weg als Raum von neuen Relationen

```
V_8:=GewichteteProdukte(8,B,vars);
rel:=findRelations(V_8,vars);
subs(rel,pzero);
```

$$\left\{e_{3c}\, e_5\, (4\, z + 4\, z_1) - e_{4a}^2\, (15\, z + 3\, z_1 + 3\, z_2)\right\}$$

mit den Lösungsparametern z, z_1, z_2 und schließen daraus $e_{3c}\, e_5, e_{4a}^2 \in R'$.

Im Grad 9 erhalten wir auf diesem Weg

```
V_9:=GewichteteProdukte(9,B,vars);
rel:=findRelations(V_9,vars);
subs(rel,pzero);
```

$$\left\{(3\, e_{4a}\, e_5 - e_{3c}^3)\, (4\, z + 16\, z_1 + 20\, z_2 + 4\, z_3)\right\}$$

und schließen daraus $3\, e_{4a}\, e_5 - e_{3c}^3 \in R'$.

Als noch fehlende Invariante können wir also $u_9 = e_{4a}\, e_5$ nehmen und wissen weiter, dass $e_{3c}^3 \in R' \oplus u_9\, R_0 = R''$ gilt.

Im Grad 10 stellt sich schließlich heraus, dass auch $e_{3c}^2\, e_{4a}, e_5^2 \in R''$ gilt, R'' also multiplikativ abgeschlossen ist.

Damit haben wir den gesamten Invariantenring als R_0-Modul und die grundlegende multiplikative Struktur der Sekundärinvarianten bestimmt.

5.6 Invariantenringe endlicher Gruppen und deren Hironaka-Zerlegung

Sei wieder $R = \oplus_{i\geq 0}[R]_i$ eine graduierte k-Algebra mit $[R]_0 = k$, also ein homogener lokaler Ring mit dem einzigen homogenen maximalen Ideal $R_+ = \oplus_{i>0}[R]_i$, $\Theta = (\theta_1, \ldots, \theta_n)$ ein homogenes Parametersystem, $R_0 = k[\theta_1, \ldots, \theta_n]$ und E ein Erzeugendensystem von R als R_0-Modul.

Besonders interessant ist der Fall, dass $R = \sum_{m\in E} m\, R_0$ eine *direkte* Summe, R als R_0-Modul also sogar frei ist. Es stellt sich heraus, dass diese Eigenschaft nicht vom konkreten Parametersystem abhängt. Für eine solche R sind die folgenden beiden Aussagen äquivalent:

(1) R ist frei über R_0 für *ein* homogenes Parametersystem $(\theta_1, \ldots, \theta_n)$

(2) R ist frei über R_0 für *jedes* homogene Parametersystem $(\phi_1, \ldots, \phi_n)$

Eine solche k-Algebra heißt *Cohen-Macaulay-Ring* (CM-Ring).

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

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

darstellen. Nach dem Nakayama-Lemma ist das genau für solche Systeme E homogener Elemente der Fall, für welche E eine Basis des Vektorraums $R/\Theta\, R$ ist.

Die von uns stets angenommene Struktur von R als *direkte* Summe der von den Sekundärinvarianten erzeugten R_0-Moduln ergibt sich also aus diesen allgemeinen Betrachtungen und dem folgenden Satz von Eagon und Hochster:

Satz 21 (Eagon, Hochster, 1971) *Der Invariantenring $R = S^G$ bzgl. einer regulären Aktion einer endlichen Gruppe G auf $[S]_1$ ist ein Cohen-Macaulay-Ring.*

Beweis: Wir zeigen hier nur, wie diese Eigenschaft aus der CM-Eigenschaft des Polynomrings $S = k[x_1, \ldots, x_n]$ folgt. Dazu fixieren wir ein System $\Theta = (\theta_1, \ldots, \theta_n)$ von Primärinvarianten und setzen $R_0 = k[\theta_1, \ldots, \theta_n]$.

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

Die Einbettung $\phi : R \to S$ induziert eine Abbildung $\phi : R \to S/\Theta\, S$ mit dem Kern $Ker(\phi) = R \cap \Theta\, S$. Dieser Kern fällt mit $\Theta\, R$ 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 $T' = R/\Theta\, R$ in T. Wählen wir eine Basis E' von T' und ergänzen sie zu einer Basis E von T, so ist nach dem Nakayama-Lemma

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

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

5.7 Hironaka-Zerlegung und Gradbeschränkungen

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

Satz 22 *Ist $\Theta = (\theta_1, \ldots, \theta_n)$ ein System von Primärinvarianten für $R = k[x_1, \ldots, x_n]^G$, $d_i = \deg(\theta_i)$, $R_0 = k[\theta_1, \ldots, \theta_n]$ und $R = \sum\limits_{m \in E} m\, R_0$ eine zugehörige Hironaka-Zerlegung, so gilt:*

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

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

(2) Die Zahl der zugehörigen Sekundärinvarianten ist gleich

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

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

Beweis: Die erste Aussage ergibt sich sofort aus den einschlägigen Formeln für die beteiligten Hilbertreihen.

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

$$\frac{1}{|G|} \prod_i \left(\frac{1 - t^{d_i}}{1 - t} \right) \Big|_{t \mapsto 1} = \frac{d_1 \cdot \ldots \cdot d_n}{|G|}$$

nach L'Hospital. Auf der rechten Seite können wir $t = 1$ direkt einsetzen und erhalten $|E|$. □

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:

$G = C_4$:

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

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 $R = k[P] \oplus e_3\cdot k[P]$

$G = D_4$:

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

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

$G = A_4$:

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

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 $\Theta = (\theta_1, \ldots, \theta_n)$ ein System E 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 $T' = R/\Theta\,R$ bilden. Wegen der Einbettung $T' \subset T$ (siehe den Beweis des Satzes von Eagon/Hochster) können wir diese Rechnungen über S ausführen:

Lemma 3 *In obiger Situation ist E genau dann ein vollständiges System von Sekundärinvarianten, wenn die $m \in E$ im k-Vektorraum $S/\Theta\,S$ linear unabhängig sind.*

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

6 Die Invariantenringe ausgewählter Klassen von Gruppenaktionen

6.1 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

$$\Theta = \left(y_1^{d_1}, \ldots, y_n^{d_n}\right)$$

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 $m_1 \in T(\Theta)$ und

$$m_0 \in E = \left\{ y_1^{a_1} \ldots y_n^{a_n} \in T(\mathbf{y}) \mid \sum a_i\alpha_i \equiv 0 \pmod{N} \text{ und } \forall\ 0 \le a_i < d_i \right\}$$

zerlegen. E 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 $m \cdot T(P)$, $m \in E$. Da jede Invariante eine Summe invarianter Terme ist, ergibt sich daraus für den Invariantenring $R = S^G$ mit $R_0 = K[\Theta]$ die Hironaka-Zerlegung

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

Für obiges Beispiel ergibt sich $\Theta = \left(y_1, y_2^2, y_3^4, y_4^4\right)$,

$$E = \left\{1, y_3\,y_4, y_2\,y_3^2, y_2\,y_4^2, y_3^2\,y_4^2, y_2\,y_3\,y_4^3, y_2\,y_3^3\,y_4, y_3^3\,y_4^3\right\}$$

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 23 (Struktursatz über Invarianten einer zyklischen Gruppenaktion)
Ist $y_1, \ldots, y_n$ eine Basis von $[S]_1$, in der die Aktion der zyklischen Gruppe $G = \langle\sigma\rangle$ diagonal mit $y_i^\sigma = \varepsilon^{\alpha_i}\, y_i$, $i = 1, \ldots, n$, ist, und $R = K[y_1, \ldots, y_n]^G$ der zugehörige Invariantenring, so bildet

$$\Theta = \left(y_1^{d_1}, \ldots, y_n^{d_n}\right)$$

mit $d_i = \frac{N}{\gcd(N,\alpha_i)}$ ein System von Primärinvarianten kleinstmöglichen Grads,

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

ein System von Sekundärinvarianten und der Invariantenring besitzt die Hironaka-Zerlegung

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

6.2 Invarianten abelscher Gruppen

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

Lemma 4 *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 $g \in G$ lässt sich V über einer solchen Erweiterung K/k 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 $R = S^G$ wie im Fall einer zyklischen Gruppenaktion von den monomialen Invarianten

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

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

Satz 24 (Struktursatz über die Invarianten einer abelschen Gruppe)
In der oben eingeführten Basis $y_1, \ldots, y_n$ von $[S]_1$ bildet $\Theta = \left(y_1^{d_1}, \ldots, y_n^{d_n}\right)$ mit

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

ein System von Primärinvarianten kleinstmöglichen Grads,

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

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

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

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 $\Theta = \left(y_1, y_2^2, y_3^2, y_4^2\right)$ mit den zugehörigen Sekundärinvarianten $E = \{1, y_2\, y_3\, y_4\}$.

6.3 Die Dreh- und Spiegelungsinvarianten regulärer n-Ecke

Die Drehgruppe $C_n \subset Gl(2,\mathbb{R})$ des regulären n-Ecks wird erzeugt von σ mit der Matrix

$$M_\sigma = \begin{pmatrix} \cos(\alpha_n) & \sin(\alpha_n) \\ -\sin(\alpha_n) & \cos(\alpha_n) \end{pmatrix}$$

wobei $\alpha_n = \frac{2\,\pi}{n}$ gilt. Wegen

$$det(E_2 - t\,M_\sigma^k) = (1 - t\,\cos(k\,\alpha_n))^2 + t^2\,\sin(k\,\alpha_n)^2 = 1 - 2\,t\,\cos(k\,\alpha_n) + t^2$$

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

$$T(n) := H(R_n,t) = \frac{1}{n}\sum_{k=0}^{n-1} \frac{1}{1 - 2\,t\,\cos(k\,\alpha_n) + t^2}\,. \tag{C.1}$$

Als erzeugende Funktion einer Abzählaufgabe gilt $H(R_n,t) \in \mathbb{Q}(t)$, d. h. diese Summe lässt sich zu einer rationalen Funktion mit ganzzahligen Koeffizienten vereinfachen.

Anmerkung: Die Darstellung (C.1) ist ein Spezialfall von Summationen der Art

$$S = \sum_{a\,:\,q(a)=0} f(a,t) \text{ mit } f(x,t) \in \mathbb{Q}(x,t)\,,$$

wobei über alle Nullstellen des quadratfreien Polynoms $q(x) \in \mathbb{Q}[x]$ summiert wird. Dazu gibt es eine umfangreiche Theorie.

In unserem Fall ergibt sich eine geschlossene Formel für (C.1) aus anderen Überlegungen. 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 ergeben die folgenden Kandidaten für Basiselemente

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

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 $\left\{e_1^3, e_2^2, e_2e_3\right\}$ ausgedrückt werden und führt auf die Relation $e_2^2 + e_3^2 = e_1^3$, so dass der Invariantenring isomorph zum Ring $R = k[E_1,E_2,E_3]/(E_2^2 + E_3^2 - E_1^3)$ ist.

```
vars:=[x1,x2];
s:=n->Dom::Matrix()([[cos(2*PI/n), sin(2*PI/n)], [-sin(2*PI/n), cos(2*PI/n)]]);
G:=map([s(3)^i$i=0..2],matrix2subrules,vars);

B:=[e_1=2*Reynolds(x1^2,G), e_2=4*Reynolds(x1^3,G), e_3=4*Reynolds(x2^3,G)];
B:=map(B,normal);

V_6:=GewichteteProdukte(6,B,vars);
rel:=findRelations(V_6,vars);
subs(rel,z=1);
```

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 $l = x_2$, die uns bereits im Satz von Dade begegnet sind.

Die Drehinvarianten regulärer n-Ecke

Der Ansatz funktioniert auch allgemein. Da C_n zyklisch ist, können wir zunächst das allgemeine Vorgehen für zyklische Gruppen anwenden.

$$y_1 = x_1 + \mathrm{i}\, x_2,\ y_2 = x_1 - \mathrm{i}\, x_2$$

ist eine Basis aus Eigenvektoren mit den Eigenwerten $\varepsilon = e^{2\pi\,\mathrm{i}/n}$ und ε^{-1}. Daraus ergibt sich unmittelbar $R = k\,[y_1^n, y_2^n, y_1\, y_2]$ als Darstellung des Invariantenrings mit den Primärinvarianten (y_1^n, y_2^n) und Sekundärinvarianten $E = \left\{(y_1\, y_2)^i, i = 0, \ldots, n-1\right\}$:

$$R = R_n = \bigoplus_{i=0}^{n-1} (y_1 y_2)^i\, R_0 \quad \text{mit } R_0 = k\,[y_1^n, y_2^n]$$

Für die zugehörige Hilbertreihe ergibt sich damit die Formel

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

was zugleich eine geschlossene Formel für die Summen $T(n)$ liefert.

Der letzte Teil der Formel legt nahe, dass es auch ein System von Primärinvarianten mit den Graden 2 und n geben könnte. Das ist in der Tat der Fall, denn $\Theta = (y_1\, y_2, y_1^n + y_2^n)$ hat offensichtlich $(0,0)$ als einzige Nullstelle. Wir erhalten in dem Fall die Hironaka-Zerlegung

$$R = R_n = R'_0 \oplus (y_1^n - y_2^n)\, R'_0 \quad \text{mit } R'_0 = k\,[y_1\, y_2, y_1^n + y_2^n]\ .$$

Beachten Sie, dass sich $e_1 = y_1\, y_2 = x_1^2 + x_2^2$, $e_2 = y_1^n + y_2^n$ und $e_3 = \mathrm{i}\,(y_1^n - y_2^n)$ als Polynome in $k[x_1, x_2]$ über dem Grundkörper k darstellen lassen.

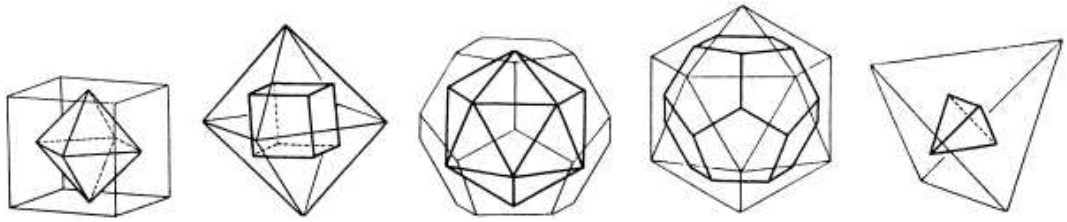
Die Spiegelungsinvarianten regulärer n-Ecke

Die volle Symmetriegruppe D_n des regulären n-Ecks wird erzeugt durch $C_n = \langle\sigma\rangle$ und eine weitere Spiegelung $\tau = (x \mapsto x, y \mapsto -y)$. $\sigma^k\tau$ 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 $R' = k[x_1, x_2]^{C_n}$)

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

Nach dieser Formel müsste es ein System von Primärinvarianten im Grad 2 und n geben, welche den Invariantenring bereits vollständig erzeugen. Dies sind offensichtlich die bereits weiter oben bestimmten e_1 und e_2. Der Invariantenring ist also in diesem Fall der Polynomring $S^{D_n} = k[e_1, e_2]$.

6.4 Die Invarianten der Drehgruppen der platonischen Körper



Die fünf Platonischen Körper und Dualitäten zwischen ihnen

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 $\pm 120°$.
- 3 Drehungen K mit Achse durch gegenüberliegende Kantenmitten um $\pm 180°$.
- Die identische Abbildung.

Die zugehörige Molienreihen

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

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

Die Hilbertreihe des Invariantenrings berechnet sich daraus nach der Molienformel zu

$$\begin{aligned} H(S^T, t) &= \frac{1}{12}\left(\frac{1}{(1-t)^3} + \frac{8}{(1-t)(1+t+t^2)} + \frac{3}{(1-t)(1+t)^2}\right) \\ &= \frac{1 - t^2 + t^4}{(1-t)^3(1+t)^2(1+t+t^2)} \\ &= \frac{1 + t^6}{(1-t^2)(1-t^3)(1-t^4)} \\ &= 1 + t^2 + t^3 + 2\,t^4 + t^5 + 4\,t^6 + \ldots \end{aligned}$$

Es sollte also ein System von Primärinvarianten vom Grad 2, 3 und 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.

Die Matrixdarstellung von T in Subrules-Darstellung ergibt sich wie folgt:

```
vars:=[x1,x2,x3];
s:=permutationMatrix([2,3,1]);
t:=Dom::Matrix()([[1,0,0],[0,-1,0],[0,0,-1]]);
MT:={ s^0,s^1,s^2, t,t*s,t*s^2, s^2*t*s,s^2*t*s^2,s^2*t, s*t*s^2,s*t,s*t*s};
T:=map(MT,matrix2subrules,vars);
```

Auch die Invarianten in den Graden 2, 3 und 4 sind schnell gefunden:

$$\begin{aligned} e_1 &= 3\,\texttt{Reynolds}(x_1^2, T) &&= x_1^2 + x_2^2 + x_3^2, \\ e_2 &= \texttt{Reynolds}(x_1x_2x_3, T) &&= x_1x_2x_3 \end{aligned}$$

(in jedem Element von T ändert sich das Vorzeichen bei jeweils genau zwei Elementen) sowie

$$\begin{aligned} e_3 &= 3\,\texttt{Reynolds}(x_1^2x_2^2, T) &&= x_1^2x_2^2 + x_1^2x_3^2 + x_2^2x_3^2 \\ \text{oder}\quad e_{3a} &= 3\,\texttt{Reynolds}(x_1^4, T) &&= x_1^4 + x_2^4 + x_3^4\,. \end{aligned}$$

Mit `groebner::dimension` prüft man wieder, dass es sich in der Tat um ein System von Primärinvarianten handelt. Ebenso lässt sich leicht die Beziehung $e_1^2 = 2\,e_3 + e_{3a}$ ableiten, so dass wir auf e_{3a} als Basisinvariante verzichten können.

Als neue Invariante vom Grad 4 kann auch das Orbitprodukt der Linearform $l = x_1 + x_2 + x_3$ genommen werden, die der Koordinatendarstellung eines der Eckpunkte entspricht.

$$\begin{aligned} e_{3b} &= (x_1 + x_2 + x_3)(x_1 - x_2 - x_2)(-x_1 + x_2 + x_3)(-x_1 - x_2 + x_3) \\ &= x_1^4 + x_2^4 + x_3^4 - 2\,x_1^2\,x_2^2 - 2\,x_1^2\,x_3^2 - 2\,x_2^2\,x_3^2 \\ &= e_1^2 - 4\,e_3 \end{aligned}$$

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. Als natürlicher Kandidat ergibt sich nach unseren bisherigen Rechnungen

$$e_{4a} = 3\,\texttt{Reynolds}(x_1^4\,x_3^2, T) = 3\,\texttt{Reynolds}(x_1^2\,x_2^4, T) = x_1^2\,x_2^4 + x_1^4\,x_3^2 + x_2^2\,x_3^4$$

Wir wollen jedoch auch das Polynom

$$e_{4b} = 3\,\texttt{Reynolds}(x_1^4\,x_2^2, T) = x_1^4\,x_2^2 + x_1^2\,x_3^4 + x_2^4\,x_3^2$$

in Betracht ziehen und wegen $e_{4a} + e_{4b} = \frac{1}{3}\,e_1\,e_3 - e_2^2 \in [R_0]_6$ schließlich $e_4 = e_{4a} - e_{4b}$ wählen. 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 $\pm 90°$.

- 3 Drehungen E_0 mit Achse durch gegenüberliegende Ecken um 180°.
- $4 \cdot 2 = 8$ Drehungen S mit Achse durch gegenüberliegende Seitenmitten um $\pm 120°$.
- 6 Drehungen K mit Achse durch gegenüberliegende Kantenmitten um 180°.
- 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 $24 \,|\, d_1\, d_2\, d_3$ gilt.

Es sollte also ein System von Primärinvarianten vom Grad 2, 4 und 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:=permutationMatrix([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);

B:=[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 (Grad 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 im Wesentlichen wieder die Determinante der Jacobimatrix von $[e_1, e_2, e_3]$.
Dahinter verbirgt sich ein allgemeiner Zusammenhang:

Satz 25 *Ist $(\theta_1, \ldots, \theta_n)$ ein System von Primärinvarianten und $J = Jacobi(\theta_1, \ldots, \theta_n) \in S$ die Determinante 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 $\pm 120°$.
- $6 \cdot 4 = 24$ Drehungen S_i mit Achse durch gegenüberliegende Seitenmitten um $i \cdot 72°, i = 1, 2, 3, 4$.
- 15 Drehungen K mit Achse durch gegenüberliegende Kantenmitten um $180°$.
- 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 $d_1 = 2$, $d_2 = 6$ und $d_3 = 10$,

```
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.

6.5 Invarianten der 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 der Spiegelungen, welche 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, e_2, 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.

8 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 $(x_1 + x_2, x_1 - x_2, x_2, \ldots, x_n)$ mit den Eigenwerten $(+1, -1, +1, \ldots, +1)$.

Satz 26 (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 5 *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. □

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

Lemma 6 *Sind $h_1, \ldots, h_m \in S$ homogene Polynome und $g_1, \ldots, g_m \in R$ Invarianten mit $h_1\, g_1 + \ldots + h_m\, g_m = 0$, so gilt entweder $h_1 \in I_G$ oder $g_1 \in (g_2, \ldots, g_m)$.*

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 $g_1 \in (g_2, \ldots, g_m)$.

Sei $\deg(h_1) > 0$ und $g_1 \notin (g_2, \ldots, g_m)$. 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 $g = \sigma_l \sigma_{l-1} \ldots \sigma_1$ ein beliebiges Element aus G, dargestellt als Produkt von Pseudoreflektionen. Dann gilt

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

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

(3) Sei weiter G von Pseudoreflektionen erzeugt. Wir zeigen nun, dass R als Algebra von n Invarianten erzeugt werden kann. Sei dazu $R = k[f_1, \ldots, f_m]$ 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 $g \in U = k[y_1, \ldots, y_m]$ ein Polynom mit $g(f_1, \ldots, f_m) = 0$. 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

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

Wegen $g_1 \notin (g_2, \ldots, g_m)$ 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:

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

Damit erhalten wir

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

Aus Gradgründen kann der erste Summand keinen Beitrag für eine Darstellung liefern, so dass schließlich $f_1 \in (f_2, \ldots, f_m)$ 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 of *Lecture Notes in Math.* 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.