-Diplomarbeit-
Buchbergeralgorithmus und Hilbertreihen

Hendrik Spiewok
Universität Kassel FB 17 - Mathematik
Betreuer: Prof. Dr. W. Koepf

An erster Stelle gilt mein Dank Herrn Prof. Dr. Koepf für die Vergabe des Themas und seine Unterstützung bei der Fertigstellung der Arbeit. Ferner möchte ich mich bei Harald Weber und Jörg Handrack bedanken, die die Korrektur lasen.

Inhaltsverzeichnis

Einleitung

In dieser Diplomarbeit wird eine Methode vorgestellt, die Performanz des Buchbergeralgorithmus mit Hilfe des Einsatzes von Hilbertreihen zu steigern.

Der Begriff der Gröbnerbasen wurde um 1965 von B. Buchberger entwickelt. Ein Ausgangspunkt seiner Überlegungen war hierbei das so genannte *"Ideal Membership Problem*". Dieses kann wie folgt formuliert werden:

Sei $g \in k[X]$ ein Polynom und I ein Ideal in $k[X]$. Ist g ein Element des Ideals I? Der Polynomring $k[X]$ ist ein Polynomring in mehreren Unbekannten (multivariat). Im univariaten Fall, mit nur einer Unbekannten x, kann das Problem einfach durch den Euklidischen Algorithmus gelöst werden. Denn in diesem Fall ist der Polynomring $k[x]$ ein Hauptidealring. Das bedeutet, dass man zu einem Ideal $I \subset k[x]$ immer ein einzelnes Polynom finden kann, welches das Ideal erzeugt. Hat man eine Menge von Erzeugern eines Ideals gegeben, dann findet man mit dem größten gemeinsamen Teiler der Erzeuger ein solches Polynom. Dividiert man jetzt ein $g \in k[x]$ durch den größten gemeinsamen Teiler der Erzeuger, so gehört g genau dann zum Ideal I, wenn der Rest Null ist.

Im multivariaten Fall haben wir mit $k[X]$ keinen Hauptidealring vor uns. Im Allgemeinen wird hier ein Ideal immer von mehreren Polynomen erzeugt. Um das Ideal Membership Problem in diesem Fall zu lösen, versuchen wir, eine spezielle Basis eines Ideals zu finden. Diese Basis sollte obige Eigenschaft des größten gemeinsamen Teilers besitzen: Das getestete Polynom g gehört genau dann zum entsprechenden Ideal, wenn der Divisionsrest nach Division von g durch die Basiselemente gleich Null ist. Insbesondere soll der Rest der Division unabhängig von der Reihenfolge der Basispolynome bei der Division sein. Das ist im Allgemeinen nicht so.

Dies leisten die Gröbnerbasen und lösen so das Ideal Membership Problem. Das bedeutet ebenfalls, dass die Gröbnerbasis eine Art von Normalformdarstellung von Polynomen ermöglicht.

Gröbnerbasen haben viele weitere Anwendungsmöglichkeiten. Das liegt zum Teil daran, dass sie ein handliches Werkzeug in Computeralgebra-Systemen darstellen. Man kann mit ihnen an viele Probleme herangehen, die sich mit Polynomsystemen formulieren lassen. Die Berechnung von Gröbnerbasen stellt z.B. eine Art verallgemeinertes Gaußsches Eliminationsverfahren dar. So ist es möglich, automatische Beweise für geometrische Probleme zu erstellen [3, S. 255 ff.], bzw. neue Sätze aufstellen [8].

Besitzt man nun eine Menge von Polynomen G, die ein Ideal $I \subset k[X]$ erzeugen, notiert mit $I = \langle G \rangle$, dann dient der *Buchbergeralgorithmus* zum Bestimmen einer Gröbnerbasis G' dieses

Ideals aus der gegebenen Erzeugendenmenge. Das Kernstück des Buchbergeralgorithmus ist nun wieder der Divisionsalgorithmus in multivariaten Polynomringen.

Damit wir den Divisionsalgorithmus in $k[X]$ überhaupt anwenden können, ist es nötig, dass wir auf $k[X]$ eine Monomordnung $>$ definieren. Nur so ist definiert, welcher Term eines Polynoms der Größte ist. Dieser Term wird als Leitterm $\mathrm{LT}(f) = \mathrm{LT}_{>}(f)$ des Polynoms f bezeichnet. Dieser Leitterm ist nun der Term, der bei der Polynomdivision als erster reduziert wird, danach der Leitterm des Restes usw. Prinzipiell gibt es von einem Ideal zu jeder Monomordnung eine entsprechende Gröbnerbasis. Dazu sei mit $G \subset k[X]$ noch folgende Notation gegeben:

$$\mathrm{LT}(G) := \{\mathrm{LT}(g) \mid g \in G\} \text{ (abhängig von } >).$$

Wie sich herausstellt, bezieht sich die Charakterisierung der Gröbnerbasen genau auf diese Leitterme. Eine Erzeugendenmenge $G = \{g_1, ..., g_s\}$ eines Ideals $I \subset k[X]$ ist eine Gröbnerbasis des Ideals genau dann, wenn das Ideal der Leitterme von I (das Leitideal von I) von den Leittermen der Elemente von G aufgespannt wird .

$$\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s) \rangle$$

Ebenso bestehen die Gröbnerbasen aus endlich vielen Polynomen (siehe Hilbertscher Basissatz).

Sehen wir uns den Buchbergeralgorithmus näher an. Wir gehen aus von einer Erzeugendenmenge G mit $I = \langle G \rangle$ und erweitern G schrittweise zu einer Gröbnerbasis. Die dabei entstehenden Zwischenergebnisse bezeichnen wir mit G'. Mit dem Divisionsalgorithmus werden die Erzeuger aus G' paarweise reduziert und gegebenenfalls neue Polynome in die so entstehende Gröbnerbasis G' aufgenommen. Dazu wird eine besondere Linearkombination, genannt *S-Polynom*, von je zwei Erzeugern aus G', genannt *kritisches Paar*, gebildet. Dieses S-Polynom wird durch alle Elemente der bisher berechneten Erzeugendenmenge dividiert. Entweder der Rest ist Null, oder er wird in die Erzeugendenmenge G' mit aufgenommen.

Dieser notwendige Divisionsschritt ist auch der, der die meiste Rechenzeit im Algorithmus in Anspruch nimmt. Durch die Division entstehen auch schnell sehr große natürliche Zahlen als Koeffizienten der Polynome, welche die Berechnung zusätzlich verlangsamen. Kommt ein neues Polynom zur Erzeugendenmenge hinzu, dann müssen zudem eine ganze Menge neuer kritischer Paare gebildet werde. Das heißt, man bildet jeweils ein Paar aus dem neuen Element mit jedem schon existierenden Erzeugerpolynom. Das ist eine sehr schnell wachsende Menge.

Das Thema dieser Arbeit zielt folgerichtig genau auf dieses Problem. Wie kann man diese Berechnungsschritte vermeiden, d. h. konkret, wie kann man kritische Paare von der Berechnung ausschließen?

Es werden im implementierten Buchbergeralgorithmus zuerst die klassischen, von Buchberger selbst gegebenen, Kriterien eingebaut. Diese beziehen sich z.B. auf die spezielle Struktur der S-Polynome, welche mit einem Modul korrespondiert.

Weitergehend ziehen wir folgende Überlegung in Betracht: Die Erfahrung hat gezeigt, dass es ”teure” Monomordnungen gibt, bzgl. derer eine Gröbnerbasis berechnet wird, und solche, die

nicht so viel Rechenzeit verbrauchen. Diesen Umstand nutzen wir nun für folgenden weiterführenden Ansatz über die Hilbertreihen.

Die Hilbertreihe eines Ideals gibt zusätzliche Strukturinformationen, die man auf die entstehende Gröbnerbasis des Ideals beziehen kann. Die Hilbertreihe eines Ideals ist vereinfacht gesagt die Potenzreihe, deren Koeffizienten die Dimensionen der entsprechenden linearen Unterräume in $k[X]$ ist.

Man fasst $k[X]$ als linearen Raum, bzw. Modul, auf. Diesen Raum kann man in lineare Unterräume $H_i(k[X])$ zerlegen. Im i-ten Unterraum $H_i(k[X])$ liegen alle Elemente von $k[X]$ mit dem Grad gleich i. Das heißt, der Polynomring und damit seine Ideale bekommen die Struktur einer Graduierung. Somit wird ein Ideal $I \subset k[X]$, bzw. sein Komplement, wie folgt zerlegt:

$$k[X]/I = \oplus_{i=0}^{\infty} H_i(k[X]/I).$$

Diese Zerlegung reflektiert sich in der entsprechenden Hilbertreihe. Wir bezeichnen sie hier vereinfachend mit $\mathrm{HS}(I) \in k[[t]]$:

$$\mathrm{HS}(I) = \sum_{i=0}^{\infty} \dim(H_i(k[X]/I)) \cdot t^i.$$

BEISPIEL. Sei $I = \langle xy^3 + z^4, x^3y^2 + xz\rangle \subset k[x, y, z]$ (siehe auch Beispiel auf Seite 62). Es ergibt sich bzgl. der lexikographischen Monomordnung: $LT(I) = \langle xy^3, x^3y^2\rangle$ und

$$\mathrm{HS}(I) = 1 \cdot t^0 + 3 \cdot t^1 + 6 \cdot t^2 + 10 \cdot t^3 + 14 \cdot t^4 + 17 \cdot t^5 \cdots .$$

Im Komplement von I befinden sich folgende Monome bzgl. ihres Grades i, welche jeweils den Unterraum $H_i(k[X]/I)$ aufspannen:

Grad i	:	Monome
0	:	$\{1\}$
1	:	$\{x, y, z\}$
2	:	$\{x^2, y^2, z^2, xy, xz, yz\}$
3	:	$\{x^2y, x^2z, xy^2, xz^2, y^2z, yz^2, x^3, y^3, z^3, xyz\}$
4	:	$\{x^3y, x^3z, y^3z, yz^3, x^4, y^4, z^4, x^2y^2, x^2yz, x^2z^2, y^2z^2, xy^2z, xyz^2, xz^3\}$
	⋮	

Was nützt uns diese Struktur nun bei der Berechnung der Gröbnerbasis?

Unter bestimmten Voraussetzungen (siehe Affiner Dimensionssatz), z.B. bei graduierter Monomordnung oder homogenem Erzeugendensystem B, ist die Hilbertreihe des erzeugten Ideals $I = \langle B\rangle$ gleich der Hilbertreihe seines Leitideals $\langle \mathrm{LT}(I)\rangle$. Es gilt dann

$$\mathrm{HS}(I) = \mathrm{HS}(\langle \mathrm{LT}(I)\rangle).$$

Diese Voraussetzungen sehen wir im Folgenden als gegeben an, da wir im Algorithmus nur homogene Erzeugendensysteme zulassen, wenn wir den Hilbertreihenteil mit benutzen. Im anderen

Fall müssen die Elemente von B homogenisiert werden. Wenn $B = \{g_1, ..., g_s\}$ eine Gröbnerbasis von I ist, dann gilt sogar

$$\mathrm{HS}(I) = \mathrm{HS}(\langle \mathrm{LT}(g_1, ..., g_s)\rangle).$$

Dies bedeutet erstens, dass wir uns bei der Berechnung der Hilbertreihe selbst auf eine einfache Variante der Berechnung der Hilbertreihe beschränken können. Denn das Leitideal ist ein monomiales Ideal und so müssen wir zum Bestimmen seiner Hilbertreihe auch nur mit Monomen und nicht Polynomen umgehen.

Das bedeutet aber zweitens, dass wir über das Leitideal einen direkten Bezug zwischen der Hilbertreihe eines Ideals und der der Gröbnerbasen des Ideals besitzen. Die Gröbnerbasen eines Ideals besitzen *alle* die gleiche Hilbertreihe wie das Ideal selbst.

Setzen wir jetzt voraus: Sei G eine homogene Erzeugendenmenge eines Ideals $I \subset k[X]$.

Sei es nun nötig, eine Gröbnerbasis G' aus G zu einer "teuren" Monomordnung zu bestimmen. Besitzen wir ferner schon eine Gröbnerbasis G_r zu einer anderen Monomordnung oder können eine solche zu einer weniger rechenintensiven Monomordnung berechnen, so können wir sie als Referenz nutzen. Denn wir besitzen den Zusammenhang $\mathrm{HS}(I) = \mathrm{HS}(\langle \mathrm{LT}(G_r)\rangle)$.

Wir werden also die Referenz-Hilbertreihe $\mathrm{HS}(I)$ des Ideals aus den Leittermen der vorhandenen Gröbnerbasis G_r bestimmen. Im Buchbergeralgorithmus wird aus dem Ausgangssystem G mit jedem Schritt eine Erzeugendenmenge G' als Zwischenergebnis berechnet. Bilden wir nun die temporäre Hilbertreihe $\mathrm{HS}(\langle \mathrm{LT}(G')\rangle)$ und dazu die Differenz dieser und der Referenz-Hilbertreihe.

$$\mathrm{HS}(\langle LT(G')\rangle) - \mathrm{HS}(I) = \sum_{i=0}^{\infty} \{\dim(H_i(k[X]/\langle G'\rangle)) - \dim(H_i(k[X]/I))\} \cdot t^i$$

Jetzt sehen wir, bei welchem kleinsten Grad i beide Reihen eine erste Differenz aufweisen und wie groß diese ist.

Damit haben wir den linearen Unterraum $H_i(k[X]/I)$ gefunden, mit kleinstem Grad i, von welchem G' noch Polynome zur Gröbnerbasis hin fehlen. Die Differenz

$$\Delta_i := \dim(H_i(k[X]/\langle \mathrm{LT}(G')\rangle)) - \dim(H_i(k[X]/\langle \mathrm{LT}(G_r)\rangle))$$

sagt ja gerade, dass der lineare Unterraum $H_i(k[X]/\langle \mathrm{LT}(G')\rangle)$ der Dimension nach größer ist als $H_i(k[X]/\langle \mathrm{LT}(G_r)\rangle)$. Somit fehlen Leitterme mit dem Grad i in der Menge G', bis sie eine Gröbnerbasis ist.

Die Größe der Differenz ist gleich der Anzahl der fehlenden Leitterme. Wir berechnen aber eine spezielle Form der Gröbnerbasis - die *minimale Gröbnerbasis*. Bei der minimalen Gröbnerbasis sind alle Koeffizienten der Leitterme der Basiselemente auf Eins normiert und es besitzen keine zwei Elemente den gleichen Leitterm. Wenn also Δ_i Leitterme fehlen, dann auch genau soviele Basiselemente.

BEISPIEL. Sei $G = G' = \{1 - x - xy^2 - xz^2, 1 - y - yz^2 - yx^2, 1 - z - zy^2 - zx^2\}$, dann ergibt sich $\mathrm{LT}(G') = \{xy^2, x^2y, x^2z\}$ und damit die Hilbertreihe

$$\mathrm{HS}(\langle \mathrm{LT}(G')\rangle = \frac{1 - \lambda^3 - 2(1 - \lambda)\lambda^3}{(1 - \lambda)^3}.$$

Besitzen wir die Referenz-Gröbnerbasis G_r bzgl. $>_{grevlex}$ (siehe Monomordnung), dann erhalten wir $\mathrm{LT}(G_r) = \{x^2z, xy^2, x^2y, y^2z^2, y^3z, y^4, x^4, z^5, yz^4, xz^4, xyz^3\}$ und

$$\mathrm{HS}(\langle \mathrm{LT}(G_r)\rangle) = \frac{1-(1-\lambda)\lambda^3-\lambda^4-(1-\lambda)\lambda^4-2(1-\lambda)^2\lambda^4-4(1-\lambda)^2\lambda^5-\lambda^3(1-\lambda^2)-(1-\lambda)\lambda^3(1-\lambda^2)}{(1-\lambda)^3}.$$

Der Differenzvektor bzgl. der Grade ist $(\Delta_0, \Delta_1, \Delta_2, ...) = (0, 0, 0, 0, 4, 9, 10, 11, 12, ...)$. So ergibt sich, dass der kleinste Grad i, bei dem eine Differenz $\Delta_i \neq 0$ auftritt, $i = 4$ ist und $\Delta_4 = 4$ Leitterme fehlen. Das sind in unserem Fall die Leitterme $\mathrm{LT}(G_r) - \mathrm{LT}(G')$ mit Grad 4: $\{y^2z^2, y^3z, y^4, x^4\}$.

Sehen wir uns nun die kritischen Paare an. Man kann noch *vor* der Konstruktion und Reduktion der entsprechenden S-Polynome sagen, welchen Grad ein eventueller Rest maximal haben wird, den wir zur entstehenden Gröbnerbasis hinzufügen würden. Ist dieser nun kleiner als unser gefundener Grad i, dann können wir solche Paare von der Berechnung ausschließen. Der Grad i ist ja gerade der kleinste Grad mit der Eigenschaft, dass Δ_i Polynome als Erzeugende fehlen.

Ferner gilt, wenn wir keine Differenz $\Delta_i \neq 0$ der Hilbertreihen haben, dann ist unsere Zwischenlösung G' schon eine Gröbnerbasis von I und wir können die Berechung abbrechen.

Dies ist der Kern des Ansatzes mit den Hilbertreihen. Bei jedem neu hinzukommenden Rest nach Division muss allerdings die temporäre Hilbertreihe neu berechnet werden. Auch sonst ist eine Menge Rechenaufwand in diesem Zusammenhang vonnöten.

Die Arbeit besteht aus drei Teilen. Im ersten Teil werden die algebraischen Grundlagen wie Monomordnung bis hin zur Gröbnerbasis dargestellt. Daran anschließend wird der Buchbergeralgorithmus in seiner Grundform vorgestellt. Ausführlich werden die schon von Buchberger selbst gefundenen Kriterien behandelt, die die Berechnungen des Algorithmus beschleunigen. Ebenso wird kurz auf die in [4] vorgestellte Sugar-Strategie eingegangen. Vorbereitend schließt sich ein Stück der Theorie von graduierten Ringen und Modulen an.

Der zweite Teil widmet sich dem Komplex der Hilbertreihen. Hier findet sich eine elementare Herleitung und Einführung über Hilbertfunktion und Hilbertpolynom. Danach wird dieses Konzept auf Hilbertreihen von graduierten Modulen verallgemeinert.

Der letzte Abschnitt beschäftigt sich schließlich mit dem theoretischen Fundament, um die Hilbertreihen praktisch berechnen zu können. Danach kommen wir zur Algorithmik selbst.

Die Umsetzung erfolgt im Computeralgebra-System Mathematica© 5.0.0. Die Implementierung befindet sich auf der CD neben einer Dokumentation der Pakete und Funktionen und einigen Beispieldateien.

Bezeichnungen

$\subset_M$	:	Untermodulrelation
$\|G\|$	:	Mächtigkeit der Menge G
$\#G$	:	Mächtigkeit der Menge G
$\bigsqcup_i G_i$	:	disjunkte Vereinigung der Mengen G_i
$\langle g_1, ..., g_s \rangle$	:	das von den Polynomen $g_1, ..., g_s$ erzeugte Ideal
$\langle G \rangle$	:	das von der Menge (von Polynomen) G erzeugte Ideal
$C(I)$	:	Komplement des Ideal I
$\deg(f)$	:	totaler Grad des Polynoms f
$\dim(V)$	:	Dimension des linearen Raumes V
$\overline{f}^G$	:	Rest der Division des Polynoms f durch die Polynome der Menge G
$f \longrightarrow^G 0$	:	das Polynom f reduziert bezüglich der Polynome der Menge G zu Null
I^h	:	Homogenisierung des Ideals I
f^h	:	Homogenisierung des Polynoms f
R_{hom}	:	Menge aller homogenen Komponenten des graduierten Ringes R
M_{hom}	:	Menge aller homogenen Komponenten des graduierten Moduls M
$H_i(I)$	:	i-te Komponente der Graduierung des Ideals I
$\mathrm{img}(f)$	:	Bild der Abbildung f
k	:	ein Körper
$k[X]$	:	Polynomring in den Unbekannten $x_1, ..., x_n$
$k[X]_{\leq d}$	:	Menge der Polynome aus $k[X]$ mit dem Grad kleiner oder gleich d
$k[X]_d$	:	Menge der Polynome am Grad gleich d und Null
$\mathrm{kern}(f)$	:	Kern der Abbildung f
$\mathrm{LT}(f)$	:	Leitterm des Polynoms f
$\mathrm{LT}(G)$	:	Menge der Leitterme der Polynome aus der Menge G
$\mathrm{LM}(f)$	:	Leitmonom des Polynoms f

$\mathrm{LC}(f)$	:	Leitkoeffizient des Polynoms f
$\mathrm{LCM}_{f,g}$	:	kleinstes gemeinsames Vielfaches der Leitterme von f und g
$\mathrm{multideg}(f)$	:	Multigrad vom Polynom f
$\mathrm{rank}(M)$	:	Rang der Matrix M
$S(F)$	:	die Menge der Syzygys des geordneten Tupels F von Polynomen
$S(g_i, g_j)$	:	S-Polynom der Polynome $g_i$und g_j
S_i	:	i-te Komponente des Ausdruckes S
S_{ij}	:	die dem S-Polynom $S(g_i, g_j)$ korrespondierende Syzygy
$\mathrm{span}(v_1, ..., v_s)$	:	der von den Elementen v_i erzeugte lineare Raum
$\mathrm{supp}(f)$	:	Träger der Funktion f
X	:	abkürzende Schreibweise der Unbekannten $x_1, ..., x_n$
X'	:	abkürzende Schreibweise der Unbekannten $x_1, ..., x_{n+1}$
$\mathbb{Z}$	:	Menge der ganzen Zahlen

KAPITEL 1

Buchbergeralgorithmus

1.1. Grundlagen

Sei in Folge $k[X]$ der multivariate Polynomring über einem Körper k in den Unbekannten $x_1, ..., x_n$. Ein Monom ist ein Ausdruck der Form $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ mit $\alpha \in \mathbb{Z}_{\geq 0}^n$ und $|\alpha| = \sum_{i=1}^n \alpha_i \in \mathbb{R}_0^+$. Die Betragsstriche $|\cdot|$ (oder auch #) auf eine Menge angewandt meint hingegen die Anzahl ihrer Elemente. Ein Polynom p ist eine Linearkombination von Monomen $p(x) = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^n} a_\alpha x^\alpha$ mit $a_\alpha \neq 0 \in k$ für endlich viele α.

Sei weiter $f_i(x) = 0$ mit $f_i \in k[X]$ für $i = 1, ..., m$ ein polynomiales Gleichungssystem. Sehen wir uns das entsprechende von den f_i erzeugte Ideal $I = \langle f_1, ..., f_m \rangle \subset k[X]$ an. (Diese eckigen Klammern symbolisieren immer die Erzeugung eines Ideals). Dann stellt sich die Frage, ob ein Erzeugendensystem existiert, welches eine besonders aussagekräftige Struktur besitzt und wie man zu einer konstruktiven Existenzaussage kommen kann.

Der Algorithmus, mit welchem aus einem gegebenen Erzeugendensystem eines Ideals eine Gröbnerbasis berechnet wird, ist der Buchbergeralgorithmus. Dieser wiederum benötigt im Kern den Divisionsalgorithmus für Polynome in $k[X]$. Zuerst wären die grundlegenden algebraischen Strukturen darzustellen, dann der Divisionsalgorithmus zu definieren und anschließend den Buchbergeralgorithmus.

Bezüglich des Divisionsalgorithmus auf $k[X]$ benötigen wir eine Ordnung $>$ der Monome in den entsprechenden Polynomen. Dies ist notwendig, um zu bestimmen, welcher Term als der Größte zuerst reduziert (dividiert) werden soll. Hierzu konstatieren wir zuerst eine Bijektion zwischen dem Exponentenvektor eines Monoms und 'seinem' Monom $\alpha \mapsto x^\alpha$. Diese induziert für jede Ordnung auf $\mathbb{Z}_{\geq 0}^n$ eine solche auf den korrespondierenden Monomen vermöge $\alpha > \beta \Rightarrow x^\alpha > x^\beta$, bzw. umgekehrt. Doch was ist nun eine monomiale Ordnung?

DEFINITION 1.1.1. [3, S. 54] **Monomiale Ordnung oder Monomordnung**

Eine Relation $>$ auf $k[X]$ heißt **Monomordnung** auf $k[X]$, wenn für alle $x^\alpha, x^\beta, x^\gamma \in k[X]$ gilt:

(1) $>$ ist eine Totalordnung (jedes Monompaar mit eindeutiger Relation $>$,$<$,$=$)
(2) $x^\alpha > x^\beta \Longrightarrow x^\alpha x^\gamma > x^\beta x^\gamma$ (Verträglichkeit mit der Multiplikation in $k[X]$)
(3) $>$ ist eine Wohlordnung (jede nicht leere Monommenge besitzt ein kleinstes Element bzgl. $>$)

Man kann zeigen (Dicksons Lemma, [3, S. 68]), dass die letzte Bedingung (3) in diesem Zusammenhang äquivalent ist mit der Aussage $\forall \alpha \in \mathbb{Z}_{\geq 0}^n$: $\alpha \geq 0$ oder anders ausgedrückt $x^\alpha \geq x^0$

für alle $\alpha \in \mathbb{Z}^n_{\geq 0}$.

Wenn klar hervorgeht, auf was sich die Monomordnung bezieht, wird dies nicht weiter benannt. Nun ein paar Beispiele für einfache, aber oft verwendete Ordnungen.

BEISPIEL 1.1.2. **Monomordnungen**

(1) Lexikographische Ordnung oder **lex** order $>_{lex}$ ist eine der einfachsten Ordnungen.
$x^\alpha >_{lex} x^\beta \Leftrightarrow \exists i$ mit $\alpha_j = \beta_j$ für $n \geq i > j$ und $\alpha_i > \beta_i$
Lexikographisch heißt diese Ordnung deshalb, weil es eine ihr analoge Ordnung bzgl. Zeichenketten gibt: "also">$_{lex}$"a" und "aba">$_{lex}$"aaa".
Es gibt auch eine Menge von **graduierten** Ordnungen, welche erfahrungsgemäß bessere Eigenschaften bezüglich der Berechenbarkeit als lex haben, was unseren Fall der Gröbnerbasen angeht.
(2) **graded lex** order $>_{grlex}$
$x^\alpha > x^\beta \Leftrightarrow (|\alpha| > |\beta|)$ oder $(\alpha >_{lex} \beta \wedge |\alpha| = |\beta|)$

(3) **graded reverse lex** order $>_{grevlex}$
$x^\alpha >_{grevlex} x^\beta \Leftrightarrow (|\alpha| > |\beta|)$ oder $(\exists i$ mit $(\alpha_j = \beta_j) \wedge (\alpha_i < \beta_i)$ für $n > j > i > 0 \wedge |\alpha| = |\beta|)$

Diese aufgeführten Ordnungen sind implizit von der Ordnung der Variablen, bzw. Unbekannten, x_i abhängig. So existieren beispielsweise $n!$ lex Ordnungen über $x_1, ..., x_n$ je nach der Ordnung der Unbekannten. Allgemein wird in Folge vorausgesetzt, dass gilt:

$$x_i > x_{i+1} \text{ für } 0 < i < n - 1.$$

Bei graduierten Ordnungen wird zuerst nach dem Betrag des Exponentenvektors entschieden, welches Monom größer ist. Sie haben den Vorzug, dass nicht die Variablen x_i unabhängig von ihrem Exponenten die Ordnung dominieren. So gilt z.B unter Voraussetzung der Variablenordnung $x > y$, dass $x >_{lex} y^{1000}$ ist, aber $y^2 >_{grlex} x$.

Mit einer solchen Monomordnung (inklusive der Variablenordnung) kann man jetzt die Terme eines Polynoms ordnen.

BEISPIEL. Hier ein paar einfache Beispiele für Vergleiche von Monomen.

$$x^{511} >_{lex} x^{124} \qquad x^{511} >_{lex} x^{125}$$
$$x^{511} >_{grlex} x^{124} \qquad x^{125} >_{grlex} x^{511}$$
$$x^{124} >_{grevlex} x^{511} \qquad x^{125} >_{grevlex} x^{511}$$

Auf Grundlage der Monomordnung führen wir weitere Begriffe für Polynome ein.

DEFINITION 1.1.3. Sei $f \in k[X]$ gegeben als $f = \sum_\alpha a_\alpha x^\alpha$ mit $>$ einer Monomordnung, dann ist

(1) der **Multigrad** oder multidegree von f: $\text{multideg}(f) = \max_>\{\alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0\}$
(2) der **totale Grad** oder einfach Grad von f: $\deg(f) = |\text{multideg}(f)|$

(3) der **Leitkoeffizient** oder leading coefficient von f: $\mathrm{LC}(f) = a_{\mathrm{multideg}(f)}$
(4) das **Leitmonom** oder leading monomial von f: $\mathrm{LM}(f) = x^{\mathrm{multideg}(f)}$
(5) der **Leitterm** oder leading term von f: $\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f)$.

BEMERKUNG 1.1.4. Ist es notwendig die Monomordnung anzugeben, so wird sie z.B. beim Leitterm wie folgt notiert: $\mathrm{LT}(f) = \mathrm{LT}_{>}(f)$.

Dem Nullpolynom $0 = 0_{k[X]}$, das ist das Polynom mit $\forall \alpha \in \mathbb{Z}^n_{\geq 0} : a_\alpha = 0$, wird kein Grad zugeordnet. Ist k ein unendlicher Körper, dann entspricht das Nullpolynom auch der Nullpolynomfunktion.

BEISPIEL 1.1.5. Sei gegeben der endliche Körper $\mathbb{Z}_2 = (\{0, 1\}, +, \cdot)$

$$f(x) = x^2 + x$$

Dann ergibt sich bei Auswertung des Polynoms $f(x)$:

$$\begin{aligned} f(0) &= 0^2 + 0 = 0 \\ f(1) &= 1^2 + 1 = 0 \end{aligned}$$

Damit bildet $f(x)$ alle Elemente des Körpers nach Null ab und ist somit die Nullfunktion $f(x) \equiv 0$. Aber es ist nicht das Nullpolynom $f(x) = 0$.

Eine alternative Darstellung für Monomordnungen kann man über Matrizen finden.

DEFINITION 1.1.6. Sei $>_\sigma$ eine Monomordnung und $M \in \mathbb{Z}^{r,k}$ eine Matrix mit folgenden Eigenschaften

(1) $\forall j \; \exists i_j$ für welches gilt $\forall i < i_j \; m_{i,j} = 0$ und $m_{i_j,j} > 0$, sowie
(2) $\mathrm{rank}(M) = k$.

Für $\alpha, \beta \in \mathbb{Z}^k_{\geq 0}$ ist vermöge $x^\alpha >_M x^\beta \Leftrightarrow \alpha >_M \beta \Leftrightarrow (M \cdot \alpha) >_{lex} (M \cdot \beta)$, bzw. bei Gleichheit gilt $\alpha >_\sigma \beta$, eine Monomordnung induziert. D. h., es existiert ein i' mit $\forall i < i' \; (M\alpha)_i = (M\beta)_i$ und $(M\alpha)_{i'} > (M\beta)_{i'}$.

Die erste Bedingung sorgt dafür, dass Konstante immer die kleinsten Monome sind. Also $\forall \alpha \in (\mathbb{Z}^k_{\geq 0} \setminus \{0\})$ gilt $\alpha >_M 0 \in \mathbb{Z}^k$. Der erste von Null verschiedene Eintrag $(M\alpha)_i$ kann nur positiv sein. Sucht man sich das kleinste i mit $m_{i,j} \neq 0$ für ein j mit $\alpha_j \neq 0$, so sind diese $m_{i,j} > 0$. Wenn dies für ein j nicht gilt, dann gäbe es ein $m_{i',j} > 0$ mit $i' < i$ als erstem Eintrag dieser j-ten Spalte in der i'-ten Zeile. Dies steht im Widerspruch dazu, dass i die kleinste Zeile mit der Eigenschaft ist, von Null verschiedene Einträge an diesen Stellen j zu haben. Somit ist also der erste von Null verschiedene Eintrag von $(M\alpha)$ positiv, womit $\alpha >_M 0$ ist.

Ein voller Rang $k = r$ [4, S.5] sorgt hingegen dafür, dass $>_M$ selbst eine Totalordnung ist, also für $\alpha \neq \beta$ gilt entweder $\alpha >_M \beta$ oder umgekehrt. Das bedeutet, dass wir keinen Rückgriff auf $>_\sigma$ benötigen.

BEMERKUNG 1.1.7. In [3, S. 74] wird aufgezeigt, wie man sich eine entsprechende $\mathbb{R}^{r,k}$- Matrix schrittweise konstruieren kann. Dabei wird von einem Vektor $u_1 \in \mathbb{R}^k$ ausgegangen und jeweils zwei verschiedenen Exponentenvektoren α und β. Es wird definiert, dass $\alpha > \beta$, wenn $\alpha \cdot u_1 > \beta \cdot u_1$. Gibt es nun noch Werte mit $\alpha \cdot u_1 = \beta \cdot u_1$, dann nimmt man einen zweiten Vektor $u_2 \in \mathbb{R}^k$. Man definiert weiter $\alpha > \beta$, wenn $\alpha \cdot u_1 > \beta \cdot u_1$ oder $\alpha \cdot u_1 = \beta \cdot u_1$ und $\alpha \cdot u_2 > \beta \cdot u_2$ usw.. Das ist der zweite Teil des folgenden Beispiels. So erreicht man sukzessiv eine Totalordnung.

BEISPIEL. Die lexikographische Ordnung auf $k[X]$ lässt sich durch die der Identität entsprechende Matrix $I^{n,n}$ darstellen. Für die graduierte lexikographische Ordnung muss man noch eine Zeile für den Gradvergleich "aufsetzen". Die entsprechende Matrix besitzt die Form $M = \begin{pmatrix} 1 & \cdots & 1 \\ & I^{n,n} & \end{pmatrix} \in \mathbb{Z}_{\geq 0}^{n+1,n}$. Die erste Zeile stellt nach der Vektormultiplikation den Grad des Monoms dar $(M\alpha)_1 = \sum_{i=1}^{n} 1 \cdot \alpha_i = \deg(x^\alpha)$.

Kommen wir nun zu der grundlegenden algebraischen Struktur, die uns begleiten wird, dem Ideal.

DEFINITION 1.1.8. Sei $(R, +, \cdot)$ ein Ring, dann heißt I **Ideal** in R, wenn gilt $\forall f, g \in I$ und $h \in R$

(1) $f + g \in I$
(2) $h \cdot f \in I$
(3) $0 = 0_R \in I$

Betrachten wir nun zuerst spezielle Ideale, welche allein von Monomen eines Polynomrings erzeugt sind. An ihnen kann man viele Eigenschaften einfacher untersuchen.

DEFINITION 1.1.9. **Monomiales Ideal, Leitideal**

Sei $I \subset k[X]$ ein Ideal, dann heißt I ein **monomiales Ideal**, wenn eine Menge $A \subset \mathbb{Z}_{\geq 0}^n$ existiert, mit $\forall f \in I : f = \sum_{\alpha \in A} h_\alpha x^\alpha$ und $h_\alpha \in k[X]$. Somit ist $\{x^\alpha \mid \alpha \in A\}$ ein Erzeugendensystem von I. Dies wird notiert mit:

$$I = \langle x^\alpha \mid \alpha \in A \rangle.$$

Sei $\{0\} \neq G \subset k[X]$, dann ist die **Menge der Leitterme** von G definiert durch

$$\mathrm{LT}(G) := \{\mathrm{LT}(f) \mid f \in G\}.$$

Das von dieser Menge erzeugte Ideal $\langle \mathrm{LT}(G) \rangle$ heißt **Leitideal** oder das Ideal der Leitterme von G.

Es ist zu sehen, dass ein Monom genau dann zu einem monomialen Ideal gehört, falls es ein Erzeugermonom gibt, welches dieses teilt.

Um uns nun der Gröbnerbasis eines Ideals zu nähern, betrachten wir den Divisionsalgorithmus. Im Gegensatz zum Divisionsalgorithmus in $k[x]$ ergeben sich für den multivariaten Fall notwendig weitere Überlegungen. Es ist $k[X]$ im Allgemeinen kein Hauptidealring ($k[x]$ ist einer). So wird ein Ideal in $k[X]$ im Allgemeinen von mehreren Polynomen erzeugt.

1.1.1. Gröbnerbasen

Der Divisionsalgorithmus in $k[X]$ sei kurz dargestellt.

ALGORITHMUS 1.1.10. *Sei $F = (f_1, ..., f_m) \in k[X]^m$ ein geordnetes m-Tupel und $f \in k[x]$. Dann ist die Division von f durch Fwie folgt im Pseudocode definiert.*

$r := 0; a_1 := 0; ...; a_m := 0; div :=$ FALSE; $p := f$;
while($p \neq 0$){
$i := 1$; $div :=$ FALSE;
  while($div =$ FALSE and $i \leq m$){
    if(LT(f_i)/LT(f)){
      $a_i := a_i +$ LT(p)/LT(f_i); $p := p -$ LT(p)/LT(f_i) $* f_i$; $div :=$ TRUE; // Reduktionsschritt
      }else{
      i++; // versuche es mit dem nächsten f_i
      }
  }// alle $f_i$wurden an LT (p) probiert
  if($div =$ FALSE){
  $r := r +$ LT(p); $p := p -$ LT(p); // der Leitterm von p konnte nicht reduziert werden und
                    //wandert in den Rest
  }
}

Das soeben definierte Verfahren hat nun die folgenden Eigenschaften.

SATZ 1.1.11. **Divisionsalgorithmus auf k[X]**

Seien $>$ eine monomiale Ordnung und $F = (f_1, ..., f_m) \in k[X]^m$ ein geordnetes m-Tupel, dann kann jedes $f \in k[X]$ dargestellt werden als

$$f = \sum_{i=1}^{m} a_i f_i + r$$

*mit $\forall i = 1, ..., m : a_i \in k[X]$. Wenn $a_i f_i \neq 0$ ist, dann gilt multideg$(f) \geq$ multideg$(a_i f_i)$. Es ist $r \in k[X]$. Entweder ist $r = 0$, oder kein Monom von r ist teilbar durch ein LT(f_i) für alle i. Das Polynom r heißt auch **Rest** der Division von f durch F. Dies wird notiert mir $\overline{f}^F$.* [3, S.60]

Ein Mangel ist, dass der Rest r anders als bei der Division in $k[x]$ im Allgemeinen nicht eindeutig ist. Er hängt neben der Monomordnung von der Reihenfolge der Division durch Polynome aus F ab.

BEISPIEL. Sei $f = x^2y + xz^2 + y - 2$ und $F = \{xz + y, x + 1\}$ mit $>_{lex}$ als Monomordnung.

So ist $\overline{f}^{(xz+y,x+1)} = 2y - yz - 2$, dagegen ergibt sich $\overline{f}^{(x+1,xz+y)} = 2y - z^2 - 2$.

Dieses Problem löst sich, wenn F eine Gröbnerbasis ist. Doch zuerst noch die Frage nach der Endlichkeit der Basis eines Ideals in $k[X]$.

SATZ 1.1.12. ***Dicksons Lemma*** [3, S. 70]

Sei $I = \langle x^\alpha \mid \alpha \in A \subset \mathbb{Z}^n_{\geq 0} \rangle \subset k[X]$ ein monomiales Ideal, dann existiert eine endliche Menge $B \subset A$ mit $I = \langle x^\beta \mid \beta \in B \rangle$, I ist endlich erzeugt.

Aus diesem Lemma lässt sich nun das wichtige Hilbert-Basis-Theorem folgern.

SATZ 1.1.13. **Hilbert-Basis-Theorem**

Sei $I \subset k[X]$ ein Ideal, dann existiert eine endliche Menge $\{f_1, ..., f_s\} \subset I$ mit $I = \langle f_1, ..., f_s \rangle$, d. h. I ist endlich erzeugt.

BEWEIS. Ist $I = \{0\}$, so ist I endlich erzeugt. Sei also nun $I \neq \{0\}$ ein Ideal in $k[X]$. Nach Dicksons Lemma existieren $F = \{f_1, ..., f_s\} \subset I$ mit $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(f_1), ..., \mathrm{LT}(f_s) \rangle$, da $\langle \mathrm{LT}(I) \rangle$ ein monomiales Ideal und somit endlich erzeugt ist. Klar ist, dass $\langle F \rangle \subset I$. Sei $f \in I$, dann gibt uns der Divisionsalgorithmus $f = \sum_{i=1}^{s} h_i f_i + r$. Nun ist aber auch $r = \sum_{i=1}^{s} h_i f_i - f \in I$. Wenn $r \neq 0$ gilt $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle$ und r wird somit von einem $\mathrm{LT}(f_i)$ geteilt. Dies ist ein Widerspruch und so folgt: $r = 0 \Rightarrow f \in \langle F \rangle$. ■

Direkt aus dem Theorem folgt eine oft verwendete Bedingung.

KOROLLAR 1.1.14. ***ACC für Ideale*** *(Ascend Chain Condition)*

Sei $I_1 \subset I_2 \subset ...$ eine aufsteigende Kette von Idealen in $k[X]$. Dann existiert ein $j \geq 1$ mit $\forall m \in \mathbb{N} : I_j = I_{j+m}$, d. h., die Kette wird stationär.

BEWEIS. Da für $f, g \in I = \bigcup_{i=1}^{\infty} I_i$ wegen der sukzessiven Inklusion ein $i \geq 1$ existiert mit $f, g \in I_i$ und gleichfalls 0, $(f + g)$ und $(h \cdot f) \in I_i \subset I$ mit $h \in k[X]$, ist I ein Ideal . Da nun nach dem Hilbert-Basis-Theorem I eine endliche Basis besitzt, existiert ein $j \geq 1$, so dass I_j alle Erzeuger von I enthält und somit gilt $I_j = I$, womit ab diesem j die Kette stationär ist. ■

Definieren wir nun die Gröbnerbasis eines Ideals und gehen auf die wichtigsten Eigenschaften ein.

DEFINITION 1.1.15. **Gröbnerbasis**

Sei $>$ eine Monomordnung und $I \subset k[X]$ ein Ideal und $G = \{g_1, ..., g_s\} \subset I$, mit

$$\langle \mathrm{LT}(g_1), ..., \mathrm{LT}(g_s) \rangle = \langle \mathrm{LT}(I) \rangle,$$

dann heißt G eine **Gröbnerbasis** oder Standardbasis von I, notiert mit $G \in \mathrm{GB}(I)$.

Bleibt also festzuhalten, dass die Gröbnerbasis von der gewählten Monomordnung abhängig ist und eine Gröbnerbasis auch eine Basis des Ideals ist. Aus dem Beweis des Hilbert-Basis-Theorems lässt sich ebenfalls eine Aussage über die Existenz einer Gröbnerbasis gewinnen.

BEISPIEL. Sei $G = \{x^2, x \cdot y^3 + z^{10}\}$, so ist bezüglich der Ordnung *lex* die Basis G' des Ideals $\langle G \rangle$ gegeben mit $G' = \{z^{20}, x \cdot z^{10}\} \cup G$. Es kommen also zwei Erzeugerpolynome hinzu. Verwendet man hingegen die Ordnung *grlex*, so ist G schon die gesuchte Gröbnerbasis. Aber G ist keine Gröbnerbasis bezüglich *lex*.

LEMMA 1.1.16. ***Existenzsatz***

Sei $\{0\} \neq I \subset k[X]$*, dann existiert eine Gröbnerbasis, welche eine Basis von I ist.*

An dieser Stelle könnte man einen formalen Beweis antreten. Das wird aber besser konstruktiv durch den Buchbergeralgorithmus geleistet, welcher aus einem Erzeugendensystem eine Gröbnerbasis erzeugt.

Nun stellt sich gleich die Frage nach der Eindeutigkeit der Gröbnerbasis eines Ideals. Sehen wir uns dazu eine Verfeinerungen der Definition der Gröbnerbasis an.

DEFINITION 1.1.17. **Minimale Gröbnerbasis**

Sei G eine Gröbnerbasis. Wenn für alle $p \in G$ gilt

(1) $\mathrm{LT}(p) \notin \langle \mathrm{LT}(G - \{p\}) \rangle$ und
(2) $\mathrm{LC}(p) = 1$ (Normierung), dann heißt G **minimale Gröbnerbasis**.

Es gibt zu einem Ideal und einer Monomordnung viele verschiedene minimale Gröbnerbasen.

DEFINITION 1.1.18. **Reduzierte Gröbnerbasis**

Sei G eine Gröbnerbasis. Wenn für alle $p \in G$ gilt

(1) kein Monom von p liegt in $\langle \mathrm{LT}(G - \{p\}) \rangle$ und
(2) $\mathrm{LC}(p) = 1$, dann heißt G **reduzierte Gröbnerbasis**.

Im Gegensatz zu minimalen Basen existiert zu einem Ideal $I \neq \{0\}$ und einer Monomordnung *genau eine* reduzierte Gröbnerbasis. Es ist auch so, dass eine berechnete Gröbnerbasis gegenüber ihrer reduzierten Form signifikant mehr Elemente besitzen kann. Damit ist die Reduktion der Basis zu einer reduzierten Gröbnerbasis immer empfehlenswert.

BEISPIEL. Sei ein Erzeugendensystem G mit neun Elementen gegeben.

$$\begin{aligned} G \;=\; & \{x^{25}w + y^2z, -xzw + y^{23}z, x^3w^3 + yz^3 * w^3, \\ & x^2w + xzw, -xyz^2w^3 - xz^3w^4, xy^2z + y^2z^2, \\ & -y^4z - y^2z^2w, -y^6z^2 + y^3z^4w^2, -yz^8w^4 - yz^7w^3\} \end{aligned}$$

Die vom in Mathematica implementierten Buchbergeralgorithmus intern berechnete Gröbnerbasis G_{temp} hat vor der Reduktion 30 Elemente.

$$\begin{aligned} G_{temp} = \{&wx^{25} + y^2z, -wxz + y^{23}z, w^3x^3 + w^3yz^3, wx^2 + wxz, -w^3xyz^2 - w^4xz^3,\\ &xy^2z + y^2z^2, -y^4z - wy^2z^2, -y^6z^2 + w^2y^3z^4, -w^3yz^7 - w^4yz^8, -w^3xz^4 + w^2y^2z^4,\\ &-wxz + w^3xz^3, wxz^2 - w^2y^2z^4, -wxz + wxyz, w^2xz + w^3xz^2, wxz + wy^2z^2,\\ &-wxz - w^2xz^2, y^2z + wxz^{24}, -wxz + y^2z, -y^2z + y^3z, -w^2y^2z - y^2z^{22},\\ &-w^3y^2z + y^2z^{21}, -w^4y^2z - y^2z^{20}, -w^5y^2z + y^2z^{19}, w^6y^2z + y^2z^{18}, w^7y^2z - y^2z^{17},\\ &w^8y^2z + y^2z^{16}, -w^9y^2z + y^2z^{15}, -w^{10}y^2z - y^2z^{14}, -w^11y^2z + y^2z^{13}, w^12y^2z + y^2z^{12}\} \end{aligned}$$

Die reduzierte Gröbnerbasis G_{red} hingegen besitzt nur 8 Elemente.

$$\begin{aligned} G_{red} = \{&wx^2 + y^2z, -y^2z + y^3z, -wy^2z + w^3yz^3,\\ &wxz - y^2z, xy^2z + y^2z^2, y^2z + wy^2z^2,\\ &-w^{11}y^2z + y^2z^{13}, w^12y^2z + y^2z^{12}\} \end{aligned}$$

SATZ 1.1.19. ***Eindeutigkeit der reduzierten Gröbnerbasis***

Zu jedem Ideal $\{0\} \neq I \subset k[X]$ *und* $>$ *eine Monomordnung existiert eine eindeutige reduzierte Gröbnerbasis.*

BEWEIS. Sei $\{0\} \neq I \subset k[X]$ ein Ideal und $G = \{g_1, ..., g_s\}$ sowie $G' = \{f_1, ..., f_t\}$ seien reduzierte Gröbnerbasen von I bezüglich der gleichen Monomordnung $>$. Für beide gilt

$$\langle \mathrm{LT}(G)\rangle = \langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(G')\rangle.$$

Sei $f \in G'$ aber $f \notin G$. Also gilt $f = \sum_{i=1}^{s} h_i g_i$ mit $h_i \in k[X]$ für alle i und insbesondere $\mathrm{LT}(f) \in \langle \mathrm{LT}(G)\rangle$. Wegen der Minimalität von G existiert genau ein $g \in G$ mit $\mathrm{LT}(g)|\mathrm{LT}(f)$. Umgekehrt gilt mit der gleichen Argumentation, dass $\mathrm{LT}(f)|\mathrm{LT}(g)$. Damit gilt $\mathrm{LT}(f) = \mathrm{LT}(g)$(*), welches auf alle $f \in G'$ angewendet heißt $\mathrm{LT}(G) = \mathrm{LT}(G')$(**).

Bleibt zu zeigen, dass nicht nur (*) gilt, sondern stärker $f = g$. Sei hierzu $h = f - g$. Für h gilt, dass $h \in I$ und somit gilt $\overline{h}^G = 0$. Da aber (*) gilt, heben sich die Leitterme von f und g, die Koeffizienten sind ja auf Eins normiert, gegenseitig in h auf. Die verbleibenden Terme von h hingegen sind aber wegen der Reduziertheit von G von keinem anderen Polynom aus G teilbar. Desgleichen sind sie wegen (**) auch nicht von Polynomen aus G' teilbar. Der Rest ist $\overline{h}^G = 0$. Das bedeutet aber, dass diese Terme nur Null sein können und somit $h = 0$ gilt. ■

Kommen wir noch einmal auf den Rest bei der Division in $k[X]$ zurück. Eine Gröbnerbasis G hat gerade die gute Eigenschaft, dass der Rest $\overline{f}^G$ bei der Division eines Polynoms $f \in k[X]$ eindeutig ist und nicht von der Reihenfolge der Division durch Polynome aus G abhängt.

SATZ 1.1.20. ***Eindeutigkeit des Rests bei Division***

Sei $G = \{f_1, ..., f_s\}$ eine Gröbnerbasis zu $I \subset k[X]$ und $f \in k[X]$, dann ist $r = \overline{f}^G$ eindeutig und unabhängig von der Reihenfolge in G bei der Division.

BEWEIS. Seien $r_1, r_2 \in k[X]$ mit $r_1 \neq r_2$ zwei verschiedene Reste von f nach Division durch G. f besitzt folgende Darstellungen $f = \sum_{i=1}^{s} h_i f_i + r_1 = \sum_{j=1}^{s} t_j f_j + r_2$ mit $h_i, t_j \in k[X]$ und $f_i, f_j \in G$ für alle i,j. Es gilt $r := r_1 - r_2 \in I$ mit $\mathrm{LT}(r) \in \langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(G) \rangle$. Das bedeutet, dass ein $g \in G$ existiert mit $\mathrm{LT}(g) | \mathrm{LT}(r)$, was ein Widerspruch zum Divisionsalgorithmus 1.1.11 ist. Also haben wir mit $r = 0$ die Eindeutigkeit, und damit die Unabhängigkeit von der Reihenfolge der Division. ■

Hiermit lässt sich nun auch das "Ideal Membership Problem" lösen, d. h. die Frage, ob ein Polynom f zu einem Ideal I gehört. Das war auch der Ausgangspunkt, welcher zur Theorie der Gröbnerbasen geführt hat.

KOROLLAR 1.1.21. ***Ideal Membership***

Sei G eine Gröbnerbasis zu einem Ideal $I \subset k[X]$ und $f \in k[X]$, dann gilt

$$f \in I \iff \overline{f}^G = 0 \in k[X].$$

Gegeben sei eine Gröbnerbasis $G = \{g_1, ..., g_s\}$ eines Ideals $I \subset k[X]$ bzgl. einer Monomordnung $>$. Die resultierende Darstellung eines Polynoms $f \in k[X]$ bei der Division durch G ist

$$f = \sum_{i=1}^{s} h_i g_i + r$$

mit $h_i \in k[X]$ für alle i. Sie wird auch **Normalform** von f genannt mit der Notation $\mathrm{normalf}_{>}(f, G)$.

Sehen wir uns noch kurz die geometrische Seite unserer bisher betrachteten Strukturen an.

DEFINITION 1.1.22. **Affine Varietät**

Sei $I \subset k[X]$ ein Ideal, dann heißt die Menge

$$\mathbb{V}(I) = \{a \in k^n \mid \forall f \in I \,:\, f(a) = 0 \in k\} \subset k^n$$

affine Varietät von I.

Also ist $\mathbb{V}(I)$ die gemeinsame Nullstellenmenge der Polynome in I und stellt die Menge der Lösungen des linearen Gleichungssystems

$$f_i(a) = 0,\ i = 1, ..., m$$

dar, mit $I = \langle f_1, ..., f_m \rangle$ (endlich erzeugt). Fasst man $\mathbb{V}(I)$ als Untermenge von k^n auf, so ergibt sich hier ein Zusammenhang zwischen der Geometrie von $\mathbb{V}(I)$ und den algebraischen Eigenschaften von I. Dies nutzen wir später, wenn wir z.B. die Hilbertreihen in Bezug auf die Dimension von Varietäten entwickeln.

BEMERKUNG. Z.B. in [3] werden hierzu korrespondierende Eigenschaften von Idealen und zugehörigen Varietäten dargestellt. So korrespondiert eine irreduzible Varietät (sie lässt sich nicht als Vereinigung zweier nicht leerer Varietäten darstellen) mit der Eigenschaft des zugehörigen Ideals, ein Primideal zu sein. Diese Parallelität von geometrischen und algebraischen Eigenschaften macht man sich oft zunutze, wenn ein Problem in einem Gebiet einfacher zu lösen ist als im anderen und man das Ergebnis wieder reformulieren kann.

1.1.2. Homogenität

Weil wir später zumeist homogene Ideale betrachten, bietet es sich an, an dieser Stelle die Begrifflichkeit einzuführen. Außerdem kann man zeigen, dass sich die Eigenschaft der Homogenität im Buchbergeralgorithmus erhält und man mit ihr vereinfachend vorgehen kann.

DEFINITION 1.1.23. **Homogenität**

Ein Polynom $f = \sum_{\alpha \in A} a_\alpha x^\alpha \in k[X]$ heißt **homogen** vom Grad d oder d**-homogen**, wenn gilt: $\forall \alpha \in A : \deg(x^\alpha) = |\alpha| = d$, also insbesondere gilt $d = \deg(f)$.

Hierbei kann man nun jedes Polynom in seine homogenen Bestandteile in der Form $f = \sum_i f_i$ zerlegen, wobei die f_i die **homogenen Komponenten** von f genannt werden und homogene Polynome vom Grad i sind.

BEISPIEL. Für ein Polynom $f \in k[x, y, z]$ ergibt sich z.B. folgende Zerlegung in homogene Komponenten:

$$f = \underbrace{x^2yz^4 + 3y^6z}_{f_7} + \underbrace{5xy + 15z^2}_{f_2} + \underbrace{1}_{f_0} \tag{1.1.1}$$

(bzgl. der "natürlichen Graduierung").

Was bedeutet das für ein Ideal? Die Summe zweier homogener Polynome eines Ideals ist nicht unbedingt wieder ein homogenes Polynom. Wird aber das Ideal von homogenen Polynomen erzeugt, dann liegen die Summen dieser Erzeuger wieder im Ideal. Genau auf diese Weise wird ein homogenes Ideal charakterisiert.

DEFINITION 1.1.24. **Homogenes Ideal**

Ein Ideal $I \subset k[X]$ heißt **homogen**, wenn für jedes $f \in I$ auch alle seine homogenen Komponenten enthalten sind.

Jedes Ideal, welches von einer Menge homogener Polynome erzeugt wird, ist auch ein homogenes Ideal, da somit sofort alle auftretenden homogenen Komponenten der erzeugten Polynome im Ideal liegen. Insbesondere ist jedes monomiale Ideal ein homogenes Ideal, da seine Erzeuger, die Monome, trivialerweise homogen sind.

Nun kann man jedem Polynom ein homogenes Polynom zuordnen, indem man vom Polynomring $k[X]$ zu $k[X']$ übergeht mit $X' = \{x_0, ..., x_n\}$. Es wird eine neue Unbekannte x_0 einführt und mit diesem Freiheitsgrad ein homogenes Polynom erzwungen. Dies nennt man Homogenisierung.

Sei die Notation für Monome wie folgt: $x^{\alpha'} = x_0^{\alpha_0} \cdots x_n^{\alpha_n} = x_0^{\alpha_0} \cdot x^{\alpha} \in k[X']$.

DEFINITION 1.1.25. **Homogenisierung**

Sei $f \in I \subset k[X]$ mit $\deg(f) = d$ in seinen homogenen Komponenten f_i vermöge $f = \sum_{i=0}^{d} f_i$ gegeben. Dann heißt das Polynom $f^h(x_o, x_1, ..., x_n) = \sum_{i=0}^{d} f_i \cdot x_0^{d-i} \in k[X']$ die **Homogenisierung** von f. Hingegen heißt das Polynom $f^h(1, x_1, ..., x_n)$ **Dehomogenisierung** von f^h.

Klar ist, dass f^h ein homogenes Polynom vom Grad $d = \deg(f)$ ist, da alle Terme nach Konstruktion diesen Grad besitzen.

BEISPIEL. Zum Polynom des vorherigen Beispiels (1.1.1) ergibt sich die folgende Homogenisierung: $f^h = x^2yz^4 + 3y^6z + 5u^5xy + 15u^5z^2 + u^7 \in k[u, x, y, z]$ mit $x_0 = u$. Das entstehende Polynom f^h ist homogen zum Grad 7.

Natürlich kann man auch umgekehrt jedes Polynom bzgl. einer Unbekannten dehomogenisieren. Folgende Aussage gibt uns dann den Zusammenhang zwischen Homogenisierung und Dehomogenisierung. Dabei stellt sich die Umkehrbarkeit bis auf einen "größten gemeinsamen Faktor" heraus.

SATZ 1.1.26. *Sei $F \in k[X']$ ein homogenes Polynom und x_0^e, $e \in \mathbb{Z}_{\geq 0}$ das höchste Vorkommen von x_0 mit $x_0^e | F$ und $f := F(1, x_1, ..., x_n)$ seine Dehomogenisierung. Dann gilt*

$$F = x_0^e \cdot f^h.$$

BEWEIS. Da gilt $x_0^e | F$, ist F darstellbar als $F = x_0^e \cdot f$ mit $d = \deg(F) = \deg(f) + e$. Sei $m := \deg(f)$. Dehomogenisiert ist $F(1, x_1, ..., x_n) = 1^e \cdot f(1, x_1, ..., x_n)$ und $\deg(F(1, x_1, ..., x_n)) = \deg(f(1, x_1, ..., x_n)) = m$.

$$\begin{aligned} F &= x^e \sum_{i=0}^{n} a_i x^{\alpha_i'} = x^e \sum_{i=0}^{n} a_i x_0^{m-|\alpha_i|} \cdot x^{\alpha_i} \\ f &= \sum_{i=0}^{n} a_i x^{\alpha_i} \\ f^h &= \sum_{i=0}^{n} a_i x_0^{m-|\alpha_i|} \cdot x^{\alpha_i} = \sum_{i=0}^{n} a_i x^{\beta_i} \end{aligned}$$

Wieder homogenisiert ist $F^h(1, x_1, ..., x_n) = f^h$ ein m-homogenes Polynom in $k[X']$. Weil sich im Exponentenvektor nur die erste Komponente bei (De)-Homogenisierung verändert, reicht es, sie alleine zu betrachten.

Da f^h m-homogen ist, hat jedes Monom von f^h die Form $x^{\alpha'}$ mit der ersten Komponente des Exponentenvektors $(\alpha')_0 = m - |\alpha|$. Dehomogenisiert wird $x^{\alpha'}$ zu x^{α}. Wird nun wieder homogenisiert, ist die erste Komponente des Exponentenvektors des entsprechenden Monoms x^{β} in f^h von der Form $(\alpha^{\beta})_0 = m - |\alpha| = (\alpha')_0$. Somit ist $F = x_0^e \cdot f = x_0^e \cdot f^h(1, x_1, ..., x_n)$. ■

Analog können wir von einer Homogenisierung eines Ideals sprechen, wobei diese Homogenisierung dann selbst ein homogenes Ideal ist.

DEFINITION 1.1.27. **Homogenisierung eines Ideals**

Sei $I \subset k[X]$ ein Ideal, dann heißt $I^h = \langle f^h \mid f \in I \rangle \subset k[X']$ die **Homogenisierung** von I.

Zu guter Letzt sei noch der Zusammenhang zwischen Gröbnerbasis und homogenem Ideal dargestellt.

SATZ 1.1.28. *Sei $I \subset k[X']$ ein Ideal, dann gilt die Äquivalenz*

(1) I ist homogenes Ideal
(2) Es existiert eine Menge $\{f_1, ..., f_s \mid f_i$ homogen für alle $i\} \subset k[X']$ mit $I = \langle f_1, ..., f_s \rangle$.
(3) Eine reduzierte Gröbnerbasis von I enthält nur homogene Polynome. (bel. Monomordnung)

BEWEIS. (2)⇒(1) Ist klar. Wenn die Erzeuger homogen sind, dann enthält I alle homogenen Komponenten daraus erzeugter Elemente.
(3)⇒(2) Zu I existiert lt. Vor. eine reduzierte Gröbnerbasis homogener Polynome und damit eine Menge derart.
(1)⇒(3) Da I ein Ideal ist, existiert genau eine reduzierte Gröbnerbasis G. Sei $G := \{g, f_1, ..., f_s\}$ und habe g die verschiedenen homogenen Komponenten $a, b \neq 0 \in k[X']$ mit $g = a + b$.
Da I ein homogenes Ideal ist, gilt $a, b \in I$ und damit $\mathrm{LT}(a), \mathrm{LT}(b) \in \langle \mathrm{LT}(I) \rangle$. Sei o. B. d. A $\mathrm{LT}(b) \neq \mathrm{LT}(g)$.
Also $\exists i \in \{1, ..., s\} : \mathrm{LT}(f_i) | \mathrm{LT}(b)$, womit ein Term von g existiert mit $\mathrm{LT}(b) \in \langle \mathrm{LT}(G - \{g\}) \rangle$, da $G - \{g\} = \{f_1, ..., f_s\}$. Dies ist ein Widerspruch zur Eigenschaft der reduzierten Gröbnerbasis. ■

Schauen wir uns an, welche Monomordnung auf dem durch Homogenisierung erweiterten Ring ihre Gültigkeit hat. Dabei wird diese so definiert, dass die Ordnung $>$ bzgl. des ursprünglichen Polynomrings $k[X]$ auf $k[X']$ eine Monomordnung wie folgt induziert:

SATZ 1.1.29. ***Induzierte Monomordnung***

Sei $>$ eine Monomordnung auf $k[X]$, dann induziert sie mit $>_h$ eine Monomordnung auf $k[X']$, gegeben durch:

$$x_0^{\alpha_0} x^\alpha >_h x_0^{\beta_0} x^\beta \iff (x^\alpha > x^\beta) \vee (x^\alpha = x^\beta \wedge \alpha_0 > \beta_0)$$

BEWEIS. Überprüfen wir nun, ob $>_h$ eine Monomordnung ist. Dabei nutzen wir, dass $>$ dominiert.
zu (1): Für $x^\alpha, x^\beta \in k[X]$ gilt mit $>$ als Totalordnung o. B. d. A $x^\alpha > x^\beta$ oder beide gleich.
Mit $x^\alpha > x^\beta \Rightarrow^{lt.Def.} x^{\alpha'} >_h x^{\beta'}$ und für $x^\alpha = x^\beta$ mit o. B. d. A $\alpha_0 > \beta_0 \Rightarrow x^{\alpha'} >_h x^{\beta'}$, also ist $>_h$ eine Totalordnung.
zu (2): Mit $x^{\alpha'}, x^{\beta'}, x^{\gamma'} \in k[X']$, so gilt o. B. d. A $x^\alpha > x^\beta \Rightarrow (x^\alpha x^\gamma > x^\beta x^\gamma) \Rightarrow x^{(a,\alpha+\gamma)} >_h x^{(b,\beta+\gamma)}$ also $x^{\alpha'} x^{\gamma'} >_h x^{\beta'} x^{\gamma'}$ mit $a = \alpha_0 + \gamma_0$ und $b = \beta_0 + \gamma_0$.

zu (3): Es gilt $\forall \alpha \in \mathbb{Z}^n_{\geq 0} : \alpha \geq 0$, also ist $x^\alpha \geq 1 = x^0$
und mit $\mathbb{Z}_{\geq 0} \ni \alpha_0$ gilt $x^\alpha \geq 1 \Rightarrow x^{\alpha'} \geq_h (x_0^0 \cdot x^0) = 1$, also $\alpha' \geq 0$. ■

BEMERKUNG. Diese Definition einer induzierten Monomordnung ließe sich verallgemeinern als eine Produktordnung.

BEISPIEL. Da $x^0 = 1$ gilt $\forall |\alpha| \neq 0 : x^\alpha > 1$. Insbesondere gilt mit der Dominanz von $>$ und $|\alpha| = 1$ $\forall i = 1, ..., n : x_i >_h 1 \cdot x_0$.
Also gilt für die Exponentenvektoren laut Definition

$(0, ..., 0, 1, 0, ..., 0) > (0, ..., 0) \Rightarrow (0, ..., 0, 1, 0..., 0) >_h (n, 0, ..., 0)$ für alle $n \in \mathbb{Z}_{\geq 0}$ wegen der Dominanz von $>$ gegenüber $>_h$.

An dieser Stelle machen wir noch eine kurze Überlegung. Wenn $x^{(a,\alpha)} >_h x^{(b,\beta)}$, anders ausgedrückt $x_0^b x^{(a-b,\alpha)} >_h x_0^b x^{(0,\beta)}$, mit $a, b \in \mathbb{Z}_{\geq 0}$, so folgt $x^{(a-b,\alpha)} >_h x^{(0,\beta)}$(**). Dies gilt, da entweder sowie schon $x^\alpha > x^\beta$. Ist andererseits $x^\alpha = x^\beta$, so muss notwendig $a > b$ sein, was äquivalent zu $(a - b) > 0$ ist.

Es stellt sich die Frage, wie sich eine Gröbnerbasis bei Homogenisierung verhält.

SATZ 1.1.30. ***Homogenisierung einer Gröbnerbasis***

Sei $I \subset k[X]$ ein Ideal und $G = \{g_1, ..., g_s\}$ eine Gröbnerbasis von I bezüglich einer graduierten Monomordnung $>$, dann ist $G^h = \{g_1^h, ..., g_s^h\}$ eine Gröbnerbasis von $I^h \subset k[X']$ für eine entsprechende induzierte Ordnung $>_h$ auf $k[X']$.

BEWEIS. Zuerst folgende Überlegung zu $f \in k[X]$. Da $>$ eine graduierte Ordnung ist, besitzt der Leitterm von f maximalen Grad bzgl. $>$. Damit hat bei der Homogenisierung von f^h das entsprechende Monom den Grad 0 bzgl. der neuen Unbekannten x_0 und ist also *nicht* verändert. Somit gilt:

$$\mathrm{LT}_>(f) = \mathrm{LT}_{>_h}(f^h)\,(*).$$

Bleibt also zu zeigen, dass $\langle \mathrm{LT}_{>_h}(I^h)\rangle = \langle \mathrm{LT}_{>_h}(G^h)\rangle$.
Da $G^h \subset I^h \Rightarrow \langle G^h\rangle \subset I^h$. Sei nun $F \in I^h$ und f seine Dehomogenisierung. Mit dem Satz 1.1.26 auf Seite 23 gilt: $\exists e \in \mathbb{Z}_{\geq 0} : F = x_0^e \cdot f^h$. Also ist $\mathrm{LM}_{>_h}(F) = \mathrm{LM}_{>_h}(x_0^e \cdot f^h) =^{(**)} x_0^e \cdot \mathrm{LM}_{>_h}(f^h)$.
Zusammen mit (*) gilt: $x_0^e \cdot \mathrm{LM}_{>_h}(f^h) = x_0^e \cdot \mathrm{LM}_>(f)$. G ist Gröbnerbasis von I, also $\exists i \in \{1, ..., s\}$: $\mathrm{LT}_>(g_i)|\mathrm{LM}_>(f)$. Mit (*) ist $\mathrm{LM}_>(g_i) = \mathrm{LM}_{>_h}(g_i^h)$. Damit $\mathrm{LT}_{>_h}(g_i^h)|\mathrm{LM}_>(f)$ und gleichfalls mit (*) $\mathrm{LT}_{>_h}(g_i^h)|\mathrm{LM}_{>_h}(f^h)$.
Daraus folgt die Behauptung, da $\mathrm{LT}_{>_h}(g_i^h)|x_0^e \cdot \mathrm{LM}_{>_h}(f^h)$. Damit wird auch $\mathrm{LM}_{>_h}(F)$ geteilt, woraus folgt, dass $\mathrm{LM}_{>_h}(F) \in \langle \mathrm{LT}_{>_h}(G)\rangle$ ist. ■

BEMERKUNG 1.1.31. Bei der Variante des Buchbergeralgorithmus mit Hilbertreihen sind wir darauf angewiesen, Erzeugendenmengen aus homogenen Polynomen zu verwenden. Sei $I \subset k[X]$ das Ausgangsideal. Dann ist es notwendig, die nicht homogenen Erzeuger zu homogenisieren. Dann wird eine reduzierte Gröbnerbasis G des homogenisierten Ideals $I^h \subset k[X']$ bzgl. einer

Monomordnung > auf $k[X']$ berechnet. Dieses Ergebnis wird dann bzgl. der neuen Unbekannten x_0 wieder dehomogenisiert.

Sei f ein Polynom aus I^h. Die Normalform von f ist $f = \sum_{i=1}^{s} h_i g_i$ mit $G = \{g_1, ..., g_s\}$ und $h_i \in k[X']$ für alle i. Wird f jetzt bzgl. x_0 dehomogenisiert, dann insbesondere seine Erzeuger g_i. Dies bedeutet aber, dass die Dehomogenisierung von G eine Basis zu I ist.

Ist nun die verwendete Monomordnung > graduiert, dann wird das Leitideal von I weder durch die Homogenisierung noch die darauf folgende Dehomogenisierung bzgl. der gleichen neuen Unbekannten verändert. Das bedeutet aber, dass die berechnete Gröbnerbasis nur dehomogenisiert werden muss, um eine Gröbnerbasis für das ursprüngliche Ideal zu erhalten.

Verwenden wir *lex* und die Variablenordnung $\forall i \neq 0 : x_i > x_0$ bzgl. der neuen Unbekannten x_0, dann verändert sich das Leitideal ebenfalls nicht, da z.B. $x^2 >_{lex} y^{10}$ und nach der Homogenisierung gilt ebenfalls $x^2 x_0^8 >_{lex} y^{10}$. Zwar wird hier anders als bei einer graduierten Ordnung der Leitterm verändert, aber er bleibt auf Grund der Variablenordnung der Leitterm. Mit $x_0 > x > y$ wäre hingegen $x^3 >_{lex} y$ und nach der Homogenisierung der neue Leitterm $x_0^2 y >_{lex} x^2$.

1.2. Buchbergeralgorithmus

Kommen wir nun zu einem Algorithmus, um eine Gröbnerbasis zu berechnen. Der Weg hierzu hat seinen Ausgangspunkt in einer gegebenen Menge von Erzeugenden $G = \{f_1, ..., f_s\} \subset I \subset k[X]$ mit $I = \langle G \rangle$. Wann ist G eine Gröbnerbasis von I? Gesucht ist eine Charakterisierung und ferner dann eine Methode, um G gegebenenfalls zu einer Gröbnerbasis zu ergänzen. Vorbereitend betrachten wir die Syzygien, bzw. die S-Polynome.

DEFINITION 1.2.1. **Syzygie**

Sei $F = (f_1, ..., f_s) \in k[X]^s$, ein s-Tupel $S = (h_1, ..., h_s) \in k[X]^s$ heißt **Syzygie** bezüglich der Leitterme $\mathrm{LT}(f_i)$ für alle i, wenn

$$S \cdot F = \sum_{i=1}^{s} h_i \cdot \mathrm{LT}(f_i) = 0 \in k[X].$$

Dabei ist $S(F)$ die Menge aller Syzygien bezüglich dieser Leitterme.

Es ist zu sehen, dass $S(F) \subset_M k[X]^s$ ein $k[X]$-Untermodul (notiert mit $\subset_M$) von $k[X]^s$ ist (bei komponentenweiser Addition und entsprechender skalarer Multiplikation). Seien die Basisvektoren von $S(F)$ mit $e_i := (0, ..., 1, ...0)$, einer 1 im i-ten Eintrag, gegeben. Hiermit kann ein Syzygie $S \in S(F)$ in der Form geschrieben werden: $S = \sum_{i=1}^{s} h_i e_i$ mit $h_i \in k[X]$ für alle i. Sehen wir uns die besonderen Syzygien der Form

$$S_{i,j} := (0, .., h_i, 0, ..., 0, h_j, ..., 0)$$

an.

DEFINITION 1.2.2. **S-Polynom** und **LCM**

(1) Seien $f, g \in k[X]\backslash\{0\}$, dann heißt das Monom
$$\mathrm{LCM}_{f,g} = \mathrm{LCM}(\mathrm{LM}(f), \mathrm{LM}(g)) = x^{\gamma}$$
das kleinste gemeinsame Vielfache oder **least common multiple** von $\mathrm{LM}(f)$ und $\mathrm{LM}(g)$ vermöge $\gamma = (\gamma_1, ..., \gamma_n)$ und $\gamma_i = \max(\alpha_i, \beta_i)$ mit $\alpha = \mathrm{multideg}(f)$, $\beta = \mathrm{multideg}(g)$ für alle i.

(2) Das Polynom
$$S(f, g) := \frac{\mathrm{LCM}_{f,g}}{\mathrm{LT}(f)} \cdot f - \frac{\mathrm{LCM}_{f,g}}{\mathrm{LT}(g)} \cdot g$$
heißt **S-Polynom** von f und g.

Nun gibt es eine Korrespondenz zwischen bestimmten Syzygien der Form S_{ij} und den zugehörigen S-Polynomen $S(f_i, f_j)$ mittels:
$$S_{ij} = \frac{\mathrm{LCM}_{f_i,f_j}}{\mathrm{LT}(f_i)} \cdot e_i - \frac{\mathrm{LCM}_{f_i,f_j}}{\mathrm{LT}(f_j)} \cdot e_j \in S(F).$$

Das heißt, dass sich ein S-Polynom als ein bestimmte Linearkombination in $S(F)$ darstellen lässt.

BEISPIEL. Sei $F = (f_1, ..., f_4) = (xy^2 + R_1, x^2y + R_2, z + R_3, x^3z + R_4) \in k[x, y, z]^4$, so erhalten wir das S-Polynom $S(f_1, f_2) = x \cdot f_1 - y \cdot f_2 = x \cdot R_1 + y \cdot R_2 \in \langle F \rangle$ mit der korrespondierenden Syzygie $S_{12} = \begin{pmatrix} x \\ -y \\ 0 \\ 0 \end{pmatrix} \in S(F)$.

Wozu braucht man nun diese Objekte? Genauer gefragt, welche Polynome aus $I = \langle G \rangle$ mit einem Erzeugendensystem G kann es geben, deren Leitterm nicht in $\langle \mathrm{LT}(G) \rangle$ ist, bzw. welche eben in der Differenz $\langle \mathrm{LT}(I) \rangle - \langle \mathrm{LT}(G) \rangle$ liegen. Um diese "fehlenden" Polynome müsste man ja G ergänzen, um es zu einer Gröbnerbasis von I zu machen.

Sehen wir uns die S-Polynome an, so sind sie genau so definiert, dass sich die Leitterme von f,$g \in G$ möglichst aufheben und $\mathrm{multideg}(S(f, g)) \leq \mathrm{multideg}(f)$ bzw. $\mathrm{multideg}(g)$ ist. Der folgende Satz benutzt, dass sich nun jeder Fall, in welchem sich Leitterme aufheben, von der Art der S-Polynome ist. Es liegt die folgende Idee nahe. Im Falle, dass alle möglichen S-Polynome einer Basis G unter Division durch G den Rest Null ergeben, ist diese Basis eine Gröbnerbasis.

LEMMA 1.2.3. ***Auslöschungen*** [3, p.83]

Sei $G = \{g_1, ..., g_s\} \subset k[X]$ *und* $f = \sum_{i=1}^{s} c_i x^{\alpha_i} g_i$, $c_i \in k$ *und* $\alpha_i + multideg(g_i) = \delta \in \mathbb{Z}^s_{\geq 0}$, *wenn* $c_i \neq 0$.

Wenn $multideg(f) < \delta$, *dann existieren* $c_{jk} \in k$ *derart, dass*
$$f = \sum_{j,k} c_{j,k} x^{\delta - \gamma_{j,k}} S(g_j, g_k) \text{ mit } x^{\gamma_{j,k}} = LCM(g_j, g_k)$$

und

$$multideg(x^{\delta-\gamma_{j,k}}S(g_j, g_k)) < \delta \text{ für } j, k = 1, ..., s$$

gilt.

Es ist also ein Ausdruck f gegeben als Linearkombination aus G. Jeder Term von f hat für sich den multideg$(f) = \delta$. Aber f besitzt insgesamt einen niedrigeren Grad. Das bedeutet, dass Auslöschungen auftreten. Die Aussage des Lemmas ist nun so zu deuten, dass sich bei derartiger Konstellation f in S-Polynomen ausdrücken lässt und die Auslöschungen dann in ihnen auftreten müssen.

SATZ 1.2.4. ***S-Polynom-Charakterisierung***

Sei $I \subset k[X]$ ein Ideal und $G = \{f_1, ..., f_s\}$ mit $\langle G\rangle = I$.

G ist eine Gröbnerbasis $\iff \forall i, j \in \{1, ..., s\}$ mit $i \neq j : \overline{S(f_i, f_j)}^G = 0 \in k[X]$.

BEWEIS. $\Rightarrow$: Da die S-Polynome im Ideal liegen, welches von G erzeugt wird, ist der Rest der Division bzgl. G gleich Null.
$\Leftarrow$: Zu zeigen ist, wenn $0 \neq f \in I$ und die Reste der S-Polynome Null sind, ist LT$(f) \in \langle$LT$(G)\rangle$ und somit G eine Gröbnerbasis.
Da G eine Basis von I ist, lässt sich f darstellen in der Form:

$$f = \sum_{i=1}^{s} h_i g_i \text{ mit } \forall i \ : \ h_i \in k[X].$$

Sei nun $m(i) :=$ multideg$(h_i g_i)$ und $\delta = \max_i(m(i))$, dann gilt multideg$(f) \leq \delta$ für alle möglichen Darstellungen von f derart.

Sei δ nun *minimal*. (Die Monomordnungen sind wohlgeordnet.) Wenn nun keine Gleichheit im letzten Ausdruck gilt, multideg$(f) < \delta$, dann gibt es in den Termen $h_i g_i$ Auslöschungen. Haben wir hingegen Gleichheit, dann existiert ein i mit LT(g_i)|LT(f), womit nun LT$(f) \in \langle$LT$(G)\rangle$ ist. Es gilt also, den ersten Fall auszuschließen.
Angenommen multideg$(f) < \delta$, womit Auslöschungen vorliegen. Schreiben wir nun f in einer Form, welche explizit auf die Leitterme Bezug nimmt und zerlegen die Terme $h_i g_i$ mit den höchstgradigen Leittermen.

$$f = \{ \sum_{m(i)=\delta} \text{LT}(h_i) g_i + \sum_{m(i)=\delta} [h_i - \text{LT}(h_i)] g_i \ \} + \sum_{m(i)<\delta} h_i g_i. \tag{1.2.1}$$

Die letzte Summe beherbergt nur niedergradige Terme. In der zweiten Summe sind die Leitterme von h_i ausgelöscht, wodurch der Grad der Terme auch kleiner als δ ist. Nach unserer Annahme ist nur noch für die erste Summe zu prüfen, ob die Terme den Multigrad kleiner als δ haben wie in den anderen beiden Summen, welches der gesuchte Widerspruch zur Minimalität von δ wäre.

Sei LT$(g_i) = c_i x^{\alpha_i} g_i$ und somit die erste Summe in der Form $S = \sum_{m(i)=\delta} c_i x^{\alpha_i} g_i$ ($c_i \in k$ für alle i). Nun ist mit Lemma 1.2.3 auf der vorherigen Seite gezeigt worden, dass hier Auslöschungen

erfolgen. Denn es ist multideg(S) $< \delta$, aber für alle Terme gilt multideg(LT(h_i)g_i) $= \delta$. Diese haben nach dem vorhergehenden Lemma die Form

$$S = \sum_{j,k} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k) \text{ mit } c_{jk} \in k \wedge x^{\gamma_{jk}} = \text{LCM}_{g_j,g_k} \quad \text{und}$$

$$\text{multideg}(x^{\delta-\gamma_{jk}} S(g_j, g_k)) < \delta$$

Dies heißt nichts weiter, als dass man jede Form der Auslöschung durch S-Polynome ausdrücken kann. Da laut Voraussetzung $\overline{S(g_j, g_k)}^G = 0$ ist, gilt weiterhin nach dem Divisionsalgorithmus $S(g_j, g_k) = \sum_{l=1}^{s} a_{jkl} \cdot g_l$ mit $a_{jkl} \in k[X]$ und ebenfalls

$$\text{multideg}(a_{jkl} g_l) \leq \text{multideg}(S(g_j, g_k)) \text{ für alle } j, k, l. \tag{1.2.2}$$

Hieraus folg:

$$\begin{aligned} S &= \sum_{j,k} (c_{jk} x^{\delta-\gamma_{jk}} \sum_{l=1}^{s} a_{jkl} g_l) \\ &= \sum_{l=1}^{s} A_l g_l \text{ mit } A_l = \sum_{j.k} c_{jk} a_{jkl} x^{\delta-\gamma_{jk}}. \end{aligned}$$

Da aber multideg($A_l g_l$) $\leq$ multideg($x^{\delta-\gamma_{jk}} S(g_j, g_k)$) $< \delta$ ist, haben wird eine Darstellung von S und damit f gefunden, bei welcher jeder Summand einen Grad kleiner als δ hat. Das widerspricht der Minimalität von δ. ■

Nach diesen Vorbetrachtungen ist hier nun der Buchbergeralgorithmus in seiner Grundform gegeben.

ALGORITHMUS 1.2.5. ***Buchbergeralgorithmus***

Input: Erzeugendenmenge $G = \{f_1, ..., f_s\}$ eines Ideals $I \subset k[X]$, $>$ eine Monomordnung auf $k[X]$

Output: eine Gröbnerbasis von I bzgl. $>$

$G := \{f_1, ..., f_s\}$;
$P := \{(i, j) \mid i < j \wedge i, j = 1, ..., s\}$;
$p :=$ next(P); //p ist ein Paar (i, j);

while($P = \emptyset$){
$p :=$ next(P);
if ($r := \overline{S(f_i, f_j)}^G \neq 0$)

{

$G := G \cup \{r\}$; $P :=$ addpairs(r); //neue Paare zu P hinzufügen

```
        };
    };
```

BEWEIS. Da die auftretenden S-Polynome in I liegen und ebenso die Reste r, welche gegebenenfalls zu G hinzukommen, bleibt G ein Erzeugendensystem für I. Nach der S-Polynom-Charakterisierung ist das resultierende G nach Konstruktion eine Gröbnerbasis von I.
Weiterhin gilt für den i-ten Schritt und der dabei berechneten Menge G_i : $\mathrm{LT}(G_i) \supsetneq \mathrm{LT}(G_{i-1})$, wenn $G_i \neq G_{i-1}$. Somit bilden die Ideale $\langle \mathrm{LT}(G_i) \rangle$ eine aufsteigende Kette, welche nach ACC stationär wird. Also gilt, ab einem $j \in \mathbb{N}$ ist $G_j = G_{j+1}$. Damit terminiert die angegebene Vorschrift mit $P = \emptyset$ und ist somit ein Algorithmus. ■

Dass hier nur die Paare $i < j$ betrachtet werden, erschließt sich nach der Betrachtung zum 2. Buchbergerkriterium. Die Paare (i, j), welche zur Reduktion als S-Polynom anstehen, werden auch als **kritische Paare** bezeichnet, weil sie im Zweifelsfall erhebliche Rechenzeit bei der Berechnung der Reste bzgl. G benötigen.

1.2.1. Buchbergerkriterien

Man sieht, dass der Rechenaufwand bei großem G beträchtlich steigen kann, wenn man die ganzen resultierenden Paare bzgl. der Reduktion zu Null überprüfen möchte. Deshalb ist man daran interessiert, die Kriterien und damit ihre Berechnung zu vereinfachen, also so viele kritische Paare wie möglich von vornherein auszuschließen. In diesem Abschnitt geht es um die "klassischen" Kriterien, welche schon Buchberger selbst formuliert hat. Die speziell auf den Hilbertreihen beruhenden Verbesserungen werden nach der Einführung in die entsprechende Theorie später gegeben.

Zuerst wird die S-Polynom-Charakterisierung abgeschwächt. Wir erhalten dadurch in Folge leichter zu handhabende Charakterisierungen einer Gröbnerbasis, insbesondere neue Kriterien, nach welchen man die Berechnung von S-Polynomen vermeiden kann. Es ist nicht mehr ausschlaggebend, dass alle S-Polynome bzgl. der Menge G den Rest Null haben, um G als Gröbnerbasis zu bestimmen, sondern sie müssen "nur" zu Null reduzieren.

DEFINITION 1.2.6. **Reduziert zu Null**

Sei $G = \{g_1, ..., g_s\} \subset k[X]$, $f \in k[X]$ und eine Monomordnung $>$ auf $k[X]$, wenn f die Darstellung hat:

$$f = \sum_{i=1}^{s} a_i g_i$$

mit $a_i \in k[X]$ für alle i und für $a_i g_i \neq 0 \in k[X]$ gilt:

$$\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i g_i).$$

Dann heißt f **reduziert zu Null bezüglich** G und wird notiert mit

$$f \to^G 0.$$

Es bedeutet also, dass zumindest der Grad der addierten Terme nicht kleiner wird, also keine Auslöschungen passieren. Folgendes Lemma verschafft uns den Zusammenhang zwischen diesem Kriterium und der S-Polynom-Charakterisierung.

LEMMA 1.2.7. ***Zusammenhang der Kriterien***

Sei $G = \{g_1, ..., g_s\} \subset k[X]$ *eine geordnete Menge,* $f \in k[X]$ *und eine Monomordnung* $>$ *auf* $k[X]$*, dann gilt*

$$\overline{f}^G = 0 \Rightarrow f \to^G 0$$

Die Umkehrung gilt im allgemeinen nicht.

BEWEIS. Wenn $\overline{f}^G = 0$ ist, dann gibt uns der Divisionsalgorithmus $f = \sum_{i=1}^{s} a_i g_i$ und für $a_i g_i \neq 0 \in k[X]$: multideg$(f) \geq$ multideg$(a_i g_i)$. ■

BEISPIEL 1.2.8. Haben wir eine Menge G, die keine Gröbnerbasis ist. Bilden wir nun ein S-Polynom $f = S(g_i, g_j)$ zweier Polynome aus G. Reduziert dieses nicht zu Null, dann existiert somit ein Polynom f, mit multigrad$(f) <$ multideg$(a_\nu g_\nu)$ für $\nu = i, j$. Sei $G = \{x^2, xy^3 + z^{10}\}$ und wir betrachten das S-Polynom bezüglich der Ordnung *lex*: $S = \frac{x^2y^3}{x^2} \cdot x^2 - \frac{x^2y^3}{xy^3} \cdot (xy^3 + z^{10}) = xz^{10}$. Dieses S-Polynom reduziert nicht zu Null bezüglich G, da multigrad$(x^2) = (2, 0, 0) >_{lex}$ $(0, 0, 10) =$ multigrad(S).

Aber die Umkehrung obigen Lemmas gilt genau dann, wenn G eine Gröbnerbasis ist. Das sagt folgender Satz:

SATZ 1.2.9. ***Verallgemeinerung der S-Polynom-Charakterisierung***

Sei $G = \{g_1, ..., g_s\} \subset k[X]$ *eine Basis zu einem Ideal I, dann ist G eine Gröbnerbasis genau dann, wenn* $\forall i \neq j : S(g_i, g_j) \to^G 0$.

BEWEIS. Wenn man sich (1.2.2) im Beweis für die S-Polynom-Charakterisierung auf Seite 29 ansieht, erkennt man, dass nur die Eigenschaft das $S(g_i, g_j)$ zu Null reduziert, verwendet wird. Das bedeutet, dass der Beweis demnach analog geführt werden kann. ■

Konkret ergibt sich nun daraus das 1. Buchbergerkriterium.

KRITERIUM 1.2.10. ***1. Buchbergerkriterium***

Sei $G = \{g_1, ..., g_s\} \subset k[X]$ *und* $i, j \in \{1, ..., s\}$ *:* $LCM(LM(g_i), LM(g_j)) = LM(g_i) \cdot LM(g_j)$ *, dann gilt* $S(g_i, g_j) \to^G 0$.

Dies ist leicht auszurechnen und gibt uns ein algorithmisch gut zu handhabendes Kriterium. Wir müssen nur diese Teilerfremdheit überprüfen. Für diese Paare (i, j) können wir uns also die Berechnung und Reduktion des S-Polynoms zum Feststellen des Restes $\overline{S(g_i, g_j)}^G$ sparen.

Für das zweite Buchbergerkriterium müssen wir etwas mehr Aufwand betreiben. Sehen wir uns den Modul der Syzygien $S(F)$ näher an. Hierfür benutzen wir die Korrespondenz zwischen S-Polynomen und den Syzygien. Wenn nun $S(F)$ ein Modul ist, stellt sich die Frage nach dessen Basis und ob uns diese Strukturkenntnis hilft, Berechnungen von S-Polynomen zu umgehen. Dabei interessiert uns insbesondere, ob eine homogene Basis existiert.

DEFINITION 1.2.11. **Homogene Syzygie**

Sei S ein Syzygie $S \in S(F) \subset k[X]^s$ mit $F = (f_1, ..., f_s)$. S heißt **homogen vom Grad** $\alpha \in \mathbb{Z}^n_{\geq 0}$, so es die Form besitzt:

$$S = (c_1 x^{\alpha_1}, ..., c_s x^{\alpha_s})^T,\ c_i \in k \text{ und für } i \text{ mit } c_i \neq 0 \text{ gilt: } \alpha_i + \text{multideg}(f_i) = \alpha.$$

Nun kann man leicht sehen, dass sich jede Syzygie eindeutig als eine Summe α-homogener Syzygien S_α mit

$$S = \sum_\alpha S_\alpha$$

schreiben lässt. Wir zerlegen S einfach in seine α-homogenen Komponenten in jeder Koordinate. Da in jeder homogenen Komponente S_α in der i-ten Koordinate entweder Null oder ein Eintrag mit Grad $\alpha - \text{multideg}(f_i)$ steht, ist diese Zerlegung eindeutig. Wenn man sich die den S-Polynomen $S(f_i, f_j)$ korrespondierenden Syzygien S_{ij} ansieht, so sind sie auf gewisse Weise "elementar". Sie enthalten die Mindestanzahl zwei der zur Reduktion notwendigen Einträge und sind auch homogen zum Grad γ mit $x^\gamma = \text{LCM}_{f_i, f_j}$.

BEISPIEL 1.2.12. Das S-Polynom aus Beispiel 1.2.8 $S(x^2, xy^3 + z^{10}) = xz^{10}$ korrespondiert mit der Syzygie $S = (y^3, -x)^T$. Sehen wir uns die ganze Gröbnerbasis bzgl. *lex* mit $(x^2, xy^3 + z^{10}, xz^{10}, z^{20})$ als geordnetes Tupel an, so ergibt sich z.B. die Syzygie S.

$$\begin{aligned} S &= \begin{pmatrix} xy^3 + y^3z^2 \\ -x^2 - xz^2 \\ 23 \cdot y^5 z^{10} \\ -23 \cdot y^5 x \end{pmatrix} \\ &= (x + z^2) S_{1,2} + (23 \cdot y^5) S_{3,4} \\ &= (x + z^2) \begin{pmatrix} y^3 \\ -x \\ 0 \\ 0 \end{pmatrix} + (23 \cdot y^5) \begin{pmatrix} 0 \\ 0 \\ z^{10} \\ -x \end{pmatrix} \end{aligned}$$

Dabei ist $S_{1,2}$ homogen zum Multigrad $(2, 3, 0)$ und $S_{3,4}$ die homogene Komponente von S zum Multigrad $(1, 0, 20)$.

In der Tat kann man jedes Element aus $S(F)$ schreiben in der Form

$$S = \sum_{i<j} u_{ij} S_{ij} \text{ mit } u_{ij} \in k[X].$$

Hierbei sind S_{ij} die zu S-Polynomen korrespondierenden Syzygien. Wir können nach der ersten Überlegung annehmen, dass S α-homogen ist und mindestens zwei Einträge ungleich Null besitzt. Letzteres gilt, da sonst für diesen Grad keine Auslöschung im Ausdruck $S \cdot F$ für ein f_i passieren könnte. Seien diese Einträge bei $i < j$ nach Definition mit $S_i = c_i x^{\alpha_i}$, $S_j = c_j x^{\alpha_j}$ und $\alpha_i + \text{multideg}(f_i) = \alpha_j + \text{multideg}(f_j) = \alpha$ gegeben. Also gilt mit $x^\gamma := \text{LCM}_{f_i,f_j}$, dass $x^\gamma | x^\alpha$.

Schauen wir uns die folgende Syzygie an: $A = S - c_i \text{LC}(f_i) x^{\alpha-\gamma} S_{ij} \in S(F)$, die so konstruiert ist, die i-te Komponente von S verschwinden zu lassen.

Für die i-te Komponente von A gilt:

$$\begin{aligned} A_i = & \quad S_i - c_i \text{LC}(f_i)\{x^{\alpha-\gamma}\,(S_{ij})_i\} \\ = & \quad c_i x^{\alpha_i} - c_i \text{LC}(f_i)\{x^{\alpha-\gamma} \cdot \tfrac{x^{\gamma-\text{multideg}(f_i)}}{\text{LC}(f_i)}\} \\ = & \quad c_i x^{\alpha_i} - c_i x^{\alpha-\text{multideg}(f_i)} \qquad = 0 \end{aligned}$$

A ist also eine α-homogene Syzygie, welche in i einen Eintrag von Null mehr besitzt als S. Entweder A ist selbst Null oder wir können dieses Verfahren solange fortsetzen, bis dies der Fall ist. Damit ergibt sich aber die gesuchte Darstellung einer Syzygie als Linearkombination von S_{ij}.

So gerüstet können wir nun unser zweites Kriterium vorbereiten.

SATZ 1.2.13. *$G = \{g_1, ..., g_s\}$ ist eine Gröbnerbasis zu einem Ideal $I \subset k[X] \iff \forall S$ einer homogenen Basis von $S(G)$: $S \cdot G \to^G 0$.*

BEWEIS. $\Rightarrow$: Folgt sofort, da alle S-Polynome zu G verschwinden bei Division durch G und sie somit ebenfalls alle zu Null reduzieren.

$\Leftarrow$: Sei $f = \sum_{i=1}^s h_i g_i \in I$ mit $h \in k[X]$ mit $m_i := \text{multideg}(h_i g_i)$ für alle i. Stellen wir uns nun alle möglichen derartigen Darstellungen von f vor und bestimmen δ als das kleinste $\delta = \max_i(m_i)$ bezüglich dieser Darstellungen.
Angenommen multideg$(f) < \delta$, was heißt, dass Auslöschungen von Leittermen passieren müssen. Von hier ausgehend wird ein Widerspruch erzeugt. Man zeigt, dass wegen der Auslöschungen schließlich für $\forall i$: multideg$(h_i g_i) < \delta$. Das steht im Widerspruch dazu, dass alle $S \cdot G \to^G 0$.
Zuerst gilt nach der Annahme multideg$(\sum_{i=1}^s h_i g_i) < \delta$. Wir können wieder f zerlegen in der Form (1.2.1) wie im Beweis auf Seite 28. Betrachtet man nur die Leitterme höchsten Grades δ (die erste Summe der drei), für die anderen ist die Annahme ja schon erfüllt, so folgt

$$\sum_{m(i)=\delta} \text{LT}(h_i)\text{LT}(g_i) = 0. \tag{1.2.3}$$

D. h., somit ist eine Syzygie gegeben $S = \sum_{m(i)=\delta} \text{LT}(h_i) e_i$, welche offensichtlich homogen vom Grad δ ist. Nach Voraussetzung besitzen wir eine homogene Basis $\{S_1, ..., S_m\}$ von $S(F)$. Damit lässt sich dieses S darstellen als $S = \sum_{j=1}^m u_j S_j$.

Wir wissen, dass S sich eindeutig als Linearkombination von homogenen Syzygien vom Grad δ schreiben lässt. So erhält man eine Darstellung, dass entweder $u_j = 0 \in k[X]$ oder $u_j S_j$ homogen

vom Grad δ ist. Im weiteren werden nur j mit $u_j \neq 0$ betrachtet. Da nun der Grad γ_j von einem S_j selbst kleiner sein kann als δ, ergibt sich zwingend die Form $u_j = c_j x^{\delta-\gamma_j}$ und somit

$$S = \sum_{j=1}^{m} c_j x^{\delta-\gamma_j} S_j.$$

Es gilt $S \cdot G = \sum_{j=1}^{m} c_j x^{\delta-\gamma_j} S_j \cdot G$ und für einen einzelnes $j : S_j \cdot G = \sum_{i=1}^{s} a_{ij} g_i$ mit $a_{ij} \in k[X]$ und

$$\text{multideg}(a_{ij} g_i) \leq \text{multideg}(S_j \cdot G), \tag{1.2.4}$$

letzteres da nach Voraussetzung $S_j \cdot G \to^G 0$.
Aus (1.2.3) folgt nun aber, dass für ein einzelnes Element gilt $S_j \cdot \text{LT}_G = 0$ mit $\text{LT}_G := \sum_{i=1}^{s} \text{LT}(g_i) e_i$.
Für den Grad des Ausdrucks folgt somit $\text{multideg}(S_j \cdot G) < \gamma_j$ und $\text{multideg}(x^{\delta-\gamma_j} S_j \cdot G) < \delta$ für alle entsprechenden j. Insgesamt gilt also

$$\begin{aligned} S \cdot G &= \sum_{j=1}^{m} c_j x^{\delta-\gamma_j} \Big(\sum_{i=1}^{s} a_{ij} g_i\Big) \\ &= \sum_{i,j} c_j x^{\delta-\gamma_j} a_{ij} g_i \,(\text{entsprechende Indexmenge}) \\ &= \sum_{i} A_i g_i \,\text{mit}\, A_i = \sum_{j=1}^{m} c_j x^{\delta-\gamma_j} a_{ij}. \end{aligned}$$

Dabei ist $\text{multideg}(A_i g_i) < \delta$ wegen (1.2.4). Damit haben wir eine Darstellung von f gefunden, bei welcher jeder Term einen Multigrad kleiner δ hat, was der Annahme von δ widerspricht. ■

Somit kann man sich also bei der Berechnung auf die S-Polynome, welche zu dieser Basis korrespondieren, beschränken. Wie kann man diese selbst aber noch weiter einschränken?

KRITERIUM 1.2.14. ***2. Buchbergerkriterium***

Sei $F = \{f_1, ..., f_s\} \subset k[X]$ und $S \subset \{S_{ij} \mid 0 \leq i < j \leq s\} \subset S(F)$ eine Basis zu $S(F)$. Wenn $f_i, f_j, f_k \in F$ alle verschieden mit

$$LT(f_k) | LCM_{f_i, f_j} \text{ und } S_{ik}, S_{jk} \in S,$$

dann gilt $S - \{S_{ij}\}$ ist auch eine Basis für $S(F)$.

(Für $i > j$ setzen wir $S_{ij} = S_{ji}$.)

BEWEIS. Sei $i < j < k$ und $x^{\gamma_{ij}} := \text{LCM}_{f_i, f_j}$. Nach Voraussetzung gilt nun $x^{\gamma_{ik}} | x^{\gamma_{ij}}$, da $\text{LT}(f_k) | x^{\gamma_{ij}}$ gilt. Ebonso gilt $\text{LT}(f_i) | x^{\gamma_{ij}}$ und damit wird auch ihr kleinstes gemeinsames Vielfaches

geteilt. Analog gilt $x^{\gamma_{jk}} | x^{\gamma_{ij}}$.

$$\begin{aligned} S_{ij} &= \frac{x^{\gamma_{ij}}}{\mathrm{LT}(f_i)} e_i - \frac{x^{\gamma_{ij}}}{\mathrm{LT}(f_j)} e_j \in S(F) \\ &= \frac{x^{\gamma_{ij}}}{\mathrm{LT}(f_i)} e_i - \frac{x^{\gamma_{ij}}}{\mathrm{LT}(f_j)} e_j + (\frac{x^{\gamma_{ij}}}{\mathrm{LT}(f_k)} e_k - \frac{x^{\gamma_{ij}}}{\mathrm{LT}(f_k)} e_k) \\ &= \frac{x^{\gamma_{ij}}}{x^{\gamma_{ik}}} (\frac{x^{\gamma_{ik}}}{\mathrm{LT}(f_i)} e_i - \frac{x^{\gamma_{ik}}}{\mathrm{LT}(f_k)} e_k) + \frac{x^{\gamma_{ij}}}{x^{\gamma_{jk}}} (\frac{x^{\gamma_{jk}}}{\mathrm{LT}(f_j)} e_j - \frac{x^{\gamma_{jk}}}{\mathrm{LT}(f_k)} e_k) \\ S_{ij} &= aS_{ik} + bS_{jk}\, a, b \in k[X] \end{aligned}$$

Damit ist also S_{ij} redundant. ■

Hier sehen wir also die Begründung für die schon vorweggenommene Annahme unseres Buchbergeralgorithmus, dass es ausreichend ist, die S-Polynome mit $i < j$ zu betrachten.

Es taucht bei der Umsetzung dieses Kriteriums allerdings ein Problem auf [4, S. 12]. Wenn $\mathrm{LCM}_{f_i,f_k} = \mathrm{LCM}_{f_i,f_j}$, dann besteht die Gefahr, beide Paare (i, j) und (j, k) zu entfernen, wobei nur eines entfernt werden darf. Dieses Problem wird im Algorithmus damit umgangen, dass man zwischen "alten" und "neuen" Paaren unterscheidet, wobei dieses Kriterium nur auf die neu hinzukommenden Paare angewandt wird.

1.2.2. Sugar-Strategie

Wir haben uns nun die klassischen Kriterien angesehen, und wie man mit ihrer Hilfe die Reduzierung der S-Polynome umgehen kann. Beim praktischen Umsetzen des Algorithmus tauchen aber wieder andere Probleme auf. Zum Beispiel, nach welcher Methode bzw. in welcher Reihenfolge greift man zur Bearbeitung auf die Paare (i, j) zu? Dasselbe gilt für die Reihenfolge der Elemente der werdenden Gröbnerbasis bei der Reduktion der S-Polynome im Divisionsalgorithmus. Da im Augenblick keine mathematisch beste Sortierung bekannt ist, stützt man sich auf eine gute Heuristik.

Die erste Methode ist die normale Buchberger-Art, die kritischen Paare nach ihrem LCM bezüglich der gewählten Monomordnung zu ordnen. Eine weitere verbreitete Methode ist die so genannte *Sugar-Strategie.* Hierbei wird jedem (S-)Polynom ein bestimmter "Phantomgrad" zugeordnet, nach welchem geordnet wird. Dieser Grad entspricht dem totalen Grad, falls man das Polynom homogenisieren würde. Die Punkte 2 und 3 der Definition beschreiben, wie man den Sugar bestimmen kann, ohne das Polynom selbst zu homogenisieren, insbesondere, wenn man aus zwei Polynomen das entsprechende S-Polynom bestimmt.

DEFINITION. [5] **Sugar**

Sei $f, g, h \in k[X]$, dann ist

(1) sugar(f):= $\deg(f^h)$,
(2) $x^\alpha \in k[X]$, so $\mathrm{sugar}(x^\alpha \cdot f) = \deg(x^\alpha) + \mathrm{sugar}(f)$,

(3) wenn $f = g + h$, dann sugar(f) = max{sugar(g), sugar(h)}.

BEMERKUNG 1.2.15. Bemerkt sei, dass der Sugar eines Polynoms nicht unbedingt mit seinem totalen Grad bezüglich einer beliebigen Monomordnung übereinstimmt. Bei der späteren Verwendung des Hilbertreihen-Kriteriums werden die Ausgangspolynome in unserer Implementation bzgl. eines Systems von Gewichten als homogen vorausgesetzt. Dann ist ihr Sugar aber gleich ihrem totalen Grad.

1.2.3. Umsetzung der Kriterien

Bei der Umsetzung der Kriterien habe ich mich am Algorithmus von Frau Gatermann [5] orientiert. Dabei wird, wie schon angesprochen, zwischen alten und neuen Paaren unterschieden, um die Schwierigkeiten mit dem 2. Kriterium zu umgehen. Dieses wird in mehrere Fälle aufgeteilt und diese nacheinander angewandt. Sei f_k ein neues Polynom, welches zu unserer werdenden Gröbnerbasis G hinzuzufügen ist. Dann sind die neuen kritischen Paare $(\cdot, k)$ in die bestehende Paarliste einzufügen, d. h., diese sind zu ordnen und einzumischen.

Das 2. Buchbergerkriterium besagt, dass im Falle S_{ik}, S_{jk} zu Null reduzieren (oder von einem anderen Kriterium entfernt wurden) und $\mathrm{LT}(f_k)|\mathrm{LCM}_{f_i,f_j}$, dann ist es überflüssig S_{ij} zu betrachten. Wir formulieren das Kriterium um:

$$\mathrm{LT}(f_k)|\mathrm{LCM}_{f_i,f_j} \Leftrightarrow \mathrm{LCM}_{f_k,f_i}|\mathrm{LCM}_{f_i,f_j} \Leftrightarrow \mathrm{LCM}_{f_k,f_j}|\mathrm{LCM}_{f_i,f_j}.$$

Das Problem ist nun, wenn $\mathrm{LCM}_{f_i,f_k} = \mathrm{LCM}_{f_i,f_j}$, dass dann sowohl (i, k) als auch (i, j) nicht beachtet werden. Es wird im Zweifelsfall das Kriterium zweimal angewandt, obwohl nur einmal richtig sein könnte.

(1) *BuchbergerCriteria2* Diese Unterfunktion operiert nur auf den alten Paaren und benutzt die strikte Form des Kriteriums 2. Wenn $\mathrm{LCM}_{f_k,f_i}|\mathrm{LCM}_{f_i,f_j} \wedge \mathrm{LCM}_{f_k,f_j}|\mathrm{LCM}_{f_i,f_j}$ (beides striktes Teilen), dann sind die Paare (i, j) überflüssig.
(2) *BuchbergerCriteria1and2a* Hier wird das 1. und ein Teil des 2. Kriteriums abgebildet. Die Funktion operiert nur auf den neuen Paaren. Wenn $\mathrm{LT}(f_i)$ und $\mathrm{LT}(f_j)$ koprim sind wird geschaut, ob $\mathrm{LCM}_{f_k,f_i} = \mathrm{LCM}_{f_k,f_j}$ mit $i < j$. Also gilt (j, k) in den neuen Paaren ist überflüssig. Wenn zusätzlich $i = j$ gilt, ist dies das erste Buchberger Kriterium.
(3) *BuchbergerCriteria2b* Es wird ebenfalls nur auf den neuen Paaren operiert. Wenn $\mathrm{LCM}_{f_k,f_i}|\mathrm{LCM}_{f_k,f_j}$ strikt mit $i < j$, so sind die folgenden Paare (j, k) überflüssig.

Ein weiteres wird im Anschluss als Kriterium benutzt. Sofern $\mathrm{LT}(f_i)|\mathrm{LT}(f_j)$ und das Paar (i, j) ist abgearbeitet, dann können die Paare (j, k) von der Liste gelöscht werden. Sie werden im Algorithmus als 'Superfluous', überflüssig, gekennzeichnet. Denn f_j kann ja nun durch f_i und S_{ij} ausgedrückt werden. Dieses Kriterium bringt zum Teil große Ersparnisse.

1.3. Graduierung und Gewichte

In diesem Abschnitt führen wir neue algebraische Strukturen ein, die im Wesentlichen auf eine Zerlegung des Polynomrings in lineare Räume abzielt. Informationen dieser Struktur, der Graduierung, wiederum liefert uns dann später die entsprechende Hilbertreihe. Durch die Zerlegung kann man sich auf die für die Berechnung der Gröbnerbasis notwendigen "Teilstücke" des Polynomrings konzentrieren.

1.3.1. Graduierung und Gewichte

Was man unter dem Grad eines Polynoms versteht, ist schon bekannt. Nun kann man aber eine Gewichtung bezüglich jeder Unbekannten in X einführen wie folgt:

DEFINITION 1.3.1. **Gewichtete Ordnung**

Sei $w \in \mathbb{Z}^n_{\geq 0}$ und $>_\sigma$ eine Monomordnung und es gilt:

$$x^\alpha >_{w,\sigma} x^\beta \iff (w\alpha > w\beta) \vee (x^{w\alpha} = x^{w\beta} \wedge x^\alpha >_\sigma x^\beta) \text{ (dabei ist } > \text{ die Ordnung auf } \mathbb{Z}).$$

Man schreibt auch $>_{W,\sigma}$ mit $W : \{x_1, ..., x_n\} \to \mathbb{Z}$ vermöge $W(x_i) = w_i$ für alle i.

Dann heißt $>_{w,\sigma}$ **gewichtete Ordnung bezüglich** W. Hierbei heißt w auch **Gewichtsvektor**.

So wird auch der **gewichtete** (totale) **Grad** eines Monoms $x^\alpha \in k[X]$ mit $\deg_W(x^\alpha) = w \cdot \alpha$ bestimmt.

Analog ist $\text{multideg}_W(f) = \max_{>_w}\{\alpha \mid a_\alpha \neq 0\}$ für $f = \sum_\alpha a_\alpha x^\alpha \in k[X] - \{0\}$.

Es bedeutet hierbei $w\alpha = w \cdot \alpha = \sum_{i=1}^n w_i\alpha_i$ das Produkt der Vektoren.

Die **natürliche Gewichtung** N ist gegeben durch den Gewichtsvektor $w = (1, ..., 1) \in \mathbb{Z}^n_{\geq 0}$.

Ein homogenes Polynom bezüglich einer gewichteten Ordnung mit dem Gewichtsvektor w bezeichnet man auch als **homogen bzgl. W,** W-homogen oder, wenn der Zusammenhang klar ist, kurz homogen**.** Man sieht hier auch schon den Zusammenhang von gewichteter Ordnung mit der schon vorher eingeführten Matrix-Ordnung. Die eine lässt sich durch die andere ausdrücken.

BEISPIEL. Das Polynom $f = f(x, y, z) = x^2y^{40} + y^{14}z^{10} \in k[x, y, z]$ ist zwar homogen bzgl. $W = (2, 1, 3)$ zum Grad 44, da $\deg_W(f) = 44$ ist. Aber f ist nicht homogen bzgl. N, da $\deg_N(x^2y^{40}) = 42 \neq 24 = \deg_N(y^{14}z^{10})$.

Sei nun $A \subset k[X]$, dann bezeichnet $H_i^W(A) = span(\{f \in A \mid \deg_W(f) = i\})$ den linearen Teilraum gebildet von den i-homogen Polynomen bzgl. W.

Wenn $W = N$, dann wird das N auch weggelassen $H_i^N(A) =: H_i(A)$. Hierbei wird auch die Notation $k[X]_i^W := H_i^W(k[X])$ verwendet. Man sieht schon, dass sich hier die Möglichkeit einer nutzbaren Zerlegung bietet. Dies wird nun in folgender Weise verallgemeinert.

DEFINITION 1.3.2. **Graduierter Ring**

Sei R ein kommutativer Ring und habe als additive Gruppe die Zerlegung

$$R = \bigoplus_{i=-\infty}^{\infty} R_i \text{ mit } \forall i, j \in \mathbb{Z}: R_i \cdot R_j \subset R_{i+j},$$

dann heißt R **graduierter Ring** die Zerlegung selbst heißt **Graduierung**.
Ist die Graduierung bezüglich einer Gewichtung W gebildet, dann heißt R ein **graduierter Ring bezüglich** W. Die auftretenden Mengen R_i werden auch als **homogene Komponenten** von R bezeichnet.
$R_{hom}^W = R_{hom} = \cup_{i=-\infty}^{\infty} R_i$ bezeichne die Menge aller homogenen Elemente von R [4, S. 3] .

Man kann wie folgt diese Definition noch bezüglich der Indexmenge verallgemeinern.

DEFINITION. Sei $(G, +, 0)$ eine abelsche Halbgruppe mit 0-Element und es sei R ein Ring mit einer direkten Summenzerlegung als additiver Gruppe $R = \oplus_{i\in G} R_i$, dann heißt R **G-graduierter Ring.** Die Familie $\{R_g\}_{g\in G}$ heißt **G-Graduierung** [7, S. 92ff]**.**

D. h., dass wir einen Ring bezüglich einer Graduierung zerlegen, welche z.B. beim Polynomring in Form des totalen Grades gegeben ist. Die $\mathbb{Z}$-Graduierung bzgl. N, der natürlichen Gewichte, heißt auch **Standardgraduierung**. Hierfür könnte man die Indexmenge auf $\mathbb{Z}_{\geq 0}$ beschränken. Da wir aber Gewichtsvektoren einbeziehen, bleiben wir in der Folge bei $i \in (-\infty, \infty)$.
Ein Polynom $f \in k[X]$ ist also i-homogen bzgl. der Graduierung, wenn es ein i gibt, dass $f \in k[X]_i$. Wie schon gesehen, lässt sich ein Polynom immer als eindeutige Summe seiner homogenen Komponenten schreiben, also quasi seiner "Projektion" in den entsprechenden Unterraum $k[X]_i$. Für $R = k[X]$ ist also ein Element der Standardgraduierung gegeben durch $R_i = k[X]_i^N$.
Wie eben angedeutet lässt sich der Begriff der Homogenität selbst nun auf graduierte Ringe erweitern und wir lösen uns dabei von der konkreten Struktur des Polynomrings zugunsten der des graduierten Ringes.

DEFINITION. **Homogenes Element**

Ein Element $r \in R$ eines G-graduierten Rings heißt **homogen**, wenn es in einer Komponente der Graduierung liegt. Also es existiert ein $i \in G$ mit $r \in R_i$. Für solche r ist der (totale) **Grad** mit i bestimmt.

BEISPIEL.

(1) Sei R ein Ring, so ist die **triviale Graduierung** in Form von $R_0 = R$ und $R_i = \langle 0 \rangle$ für $i \neq 0$ gegeben.
(2) Ein einfaches Beispiel eines graduierten Ringes ist der Polynomring $k[X] = \oplus_{i=-\infty}^{\infty} H_i^W(k[X])$. Ein Polynom f ist mit $k[X] \ni f(X) = \sum_{i=-\infty}^{\infty} f_i(X)$ in seine homogenen Komponenten f_i gegeben. Dabei ist die Basis eines Unterraums $k[X]_i^W$ die Menge der Monome, welche den Grad i bzgl. W aufweisen.

BEMERKUNG.

(1) Man sieht, wenn $R = \oplus_{i=-\infty}^{\infty} R_i$ ein graduierter Ring über dem Körper k ist, dann ist R_0 ein Unterring von R. Man hat z.B. $k = R_0$ eingebettet. Dies gilt, da R_0 nach Zerlegung eine additive Gruppe ist und mit $R_0 \cdot R_0 \subset R_0$ wegen der Graduierung von R als Ring abgeschlossen unter $'\cdot'$ ist.
(2) Ebenso ist jeder Teilraum R_i ein R_0-Modul.
Sieht man sich die Zerlegung der Eins mit $1 = 1_R \in R$ an: $1 = \sum_{i=-\infty}^{\infty} e_i$. So gilt $\forall r \in R_{hom} : r = r \cdot 1 = \sum_{i=-\infty}^{\infty} r \cdot e_i$. Sei $r \in R_{i_r}$, so gilt ja einzig $R_0 \cdot R_{i_r} \subset R_{i_r}$. Da durch Koeffizientenvergleich gilt $r \cdot e_0 = r$ und $\deg(r \cdot e_0) = \deg(r) + \deg(e_0)$ nur für e_0 mit $\deg(e_0) = 0$ gilt. Also ist die gesuchte Eins für den Modul R_i $1 = e_0 \in R_0$, da sich jedes Element r aus R als Summe seiner homogenen Komponenten aus R_{hom} darstellen lässt und $r \cdot 1 = r \cdot e_0 = \sum_i r_i \cdot e_0 = \sum_i r_i = r$.
Mit $R_0 \cdot R_i \subset R_i$ als skalarer Multiplikation und wie eben gezeigt $1 \in R_0$ ist jedes R_i ein R_0-Modul. Additive Gruppe ist R_i ja nach Definition.

Auf dieser Struktur des graduierten Ringes definieren wir nun den entsprechend verträglichen Modul.

DEFINITION 1.3.3. **Graduierter Modul**

Sei M ein R-Modul und R ein graduierter Ring und M habe die Darstellung $M = \oplus_{i=-\infty}^{\infty} M_i$ mit $\forall i, j \in \mathbb{Z} : R_j \cdot M_i \subset M_{i+j}$, dann heißt M **graduierter Modul**. $M_{hom} := \cup_{i=-\infty}^{\infty} M_i$ ist die Menge der homogenen Elemente in M.

Das heißt also, der Modul besitzt selbst eine Zerlegung und selbige ist zu der im Ring verträglich. Ist der Modul endlich erzeugt, so besitzt er auch ein endliches homogenes Erzeugendensystem in Form der homogenen Komponenten seiner Erzeuger. Die Definition für eine G-Graduierung eines Moduls ist analog wie beim Ring mit der Indexmenge G.
Um nun graduierte Quotientenmodule bilden zu können, die wir noch benötigen werden, definieren wir den entsprechenden Untermodul. Wir übertragen dabei die Struktur vom $G-$graduierten Modul M. Jedes Element $m \in M$ lässt sich eindeutig darstellen als $m = \sum_{g \in G} r_g m_g$ mit $R \ni r_g \neq 0$ für *endlich* viele $g \in G$ und $m_g \in M_g$ für alle $g \in G$.

DEFINITION 1.3.4. **Graduierter Untermodul**

Sei $N \subset_M M$ (ein Untermodul), $M = \oplus_{i=-\infty}^{\infty} M_i$ ein graduierter Modul und N habe die Zerlegung $N = \oplus_{i=-\infty}^{\infty} N_i$ mit $N_i = N \cap M_i$, dann heißt N **graduierter** oder auch **homogener Untermodul** von M.

Es ist klar, wenn N von homogenen Elementen aus M erzeugt wird, ist N homogen und umgekehrt.

BEISPIEL.

(1) Wenn $I \subset k[X]$ ein *homogenes* Ideal ist bzgl. W, d. h., es ist von homogenen Polynomen bzgl. W erzeugt, dann ist I ein graduierter Untermodul bzgl. W von $k[X]$ der Form

$$I = \bigoplus_{i=-\infty}^{\infty} H_i^W(I).$$

Da das homogene Ideal alle homogenen Komponenten seiner Elemente enthält, gilt $H_i^W(I) \subset I$. Zerlegt man jedes Polynom in I in seine homogenen Komponenten bzgl. W, so ist diese Zerlegung eindeutig (entsprechend der direkten Summe). Angenommen, zwei Polynome $f \in H_r^W(k[X])$, $g \in H_s^W(I)$ haben jeweils den Grad r und s und $(f \cdot g) \in I$ entsprechend den Grad $r + s$ bzgl. W. Da beide homogen sind, so ist bei jedem Term $(f_t \cdot g_{t'})$ der Grad $r+s$. Also folgt $(f \cdot g) \in H_{r+s}^W(I)$ und somit $H_r^W(k[X]) \cdot H_s^W(I) \subset H_{r+s}^W(I)$. Andererseits, wenn I ein graduiertes Ideal bzgl. W ist, dann lassen sich homogene Erzeuger finden, welche die Komponenten $H_i^W(I)$ des Ideals aufspannen.

(2) Ebenso kann man den Quotientenring $k[X]/I$ als graduierten Modul bzgl W über $k[X]$ auffassen, wenn I ein *homogenes* Ideal bzgl. W ist. Es gilt, wie gleich gezeigt wird

$$k[X]/I = \bigoplus_{i=-\infty}^{\infty} H_i^W(k[X]/I) = \bigoplus_{i=-\infty}^{\infty} (H_i^W(k[X])/H_i^W(I)).$$

Die Restklassen $[\, f \,] = [\, f \,]_I := \{f + h \mid h \in I\} \in k[X]/I$ lassen sich wieder *eindeutig* in ihre homogenen Komponenten bzgl. W zerlegen.
Sei eine solche Zerlegung gegeben mit $f = \sum_{i=0}^{m_f} f_i \in k[X]$ und sei $m_f := \deg^W(f)$

$$\begin{aligned} [\, f \,] &= \{f + h \mid h \in I\} \\ &= \sum_{i=0}^{m_f} (f_i + \bigoplus_{j=-\infty}^{\infty} H_j^W(I)) \\ &= \bigoplus_{i=-\infty}^{\infty} f_i + H_i^W(I) \text{ mit } f_i := 0 \text{ für } i \notin [0, m_f] \subset \mathbb{Z} \end{aligned}$$

Für die i-te Komponente bekommen wir die Darstellung

$$\{f_i + H_i^W(I) \mid f_i \in H_i^W(k[X])\} = H_i^W(k[X])/H_i^W(I).$$

Somit haben wir die gesuchte, bzgl. der Teilräume eindeutige, Zerlegung für jedes Element $[\, f \,]_I$ gefunden. Für jedes f gibt es nur jeweils endlich viele homogene Komponenten und damit endlich viele Anteile in der direkten Summe.

Diesen Sachverhalt fassen wir nun allgemeiner.

LEMMA. *Sei $M = \oplus_{i \in G} M_i$ ein G-graduierter Modul (über ein G-graduiertem Ring R) und $N \subset_M M$ ein Untermodul, dann gilt, N ist ein homogener Untermodul genau dann, wenn die Familie*

$$\{(M_i + N)/N\}_{i \in G} \tag{1.3.1}$$

eine Graduierung von M/N ist. D. h., es gilt

$$M/N = \bigoplus_{i\in G}(M_i + N)/N.$$

BEWEIS. $\Rightarrow$: Sei $f_i \in M_i$ und $[\, f_i \,]_N$ die entsprechende Restklasse in M/N.
Dass $M/N = \sum_{i\in G}(M_i + N)/N$ gilt, ist klar. Bleibt zu zeigen, dass die Summe direkt ist. Angenommen $\sum_{i\in G}[\, f_i \,]_N = 0 \in M/N$, dann ist $\sum_{i\in G} f_i \in N$. Da N ein homogener Untermodul ist, folgt für die einzelnen $f_i \in N$ und somit $[\, f_i \,]_N = 0 \in M/N$. Somit ist die Summe eine direkte.
$\Leftarrow$: Sei $N \ni f = \sum_{i\in G} f_i$ mit $f_i \in M_i$ für alle i. So gilt $\sum_{i\in G}[\, f_i \,]_N = 0 \in M/N$. Da wir aber eine Graduierung haben gilt $[\, f_i \,] = 0$ und somit $f_i \in N$ für alle i. Damit enthält N alle homogenen Komponenten seiner Elemente und ist somit homogener Untermodul von R. ■

BEMERKUNG. Wenn nicht anders benannt, so wird die Graduierung (1.3.1) für den Quotientenmodul angenommen. Es wird in der Literatur auch oft die Graduierung $\{M_i/N_i\}_{i\in G}$ mit $M/N = \oplus_{i\in G} M_i/N_i$ [7, S. 93] gegeben. Der Zusammenhang zwischen beiden Graduierungen ist im Zusammenhang von $(M_i + N)/N$ und $(M_i + N_i)/N$ zu finden.

Im ersten Fall sind in $M_i + N$ außer den linearen Kombinationen mit den Elementen von N keine weiteren Elemente aus M mit Grad ungleich i zu finden. Diese werden aber gerade "ausfaktorisiert", wonach in beiden Darstellungen der Graduierung von M/N, also die Äquivalenzklassen, übereinstimmen.

Allgemeiner gilt. Ist $I \subset R$ ein homogenes Ideal eines G-graduierten Ringes, so ist R/I nicht nur ein G-graduierter Modul, sondern sogar ein G-graduierter Ring. Die Ringeigenschaft ist klar und die Graduierung ist gegeben über

$$(R/I)_i := (R_i + I)/I \qquad (\text{für } i \in G)$$

1.3.2. Multigraduierung

Was passiert nun aber, wenn wir eine Graduierung bezüglich mehrerer Gewichte haben? Dann lässt sich die Zerlegung allgemein wie folgt sukzessive gewinnen:

$$\begin{aligned} H_{i,j}^{W_1,W_2}(A) :=&\quad H_i^{W_1}(A) \cap H_j^{W_2}(A) \text{ mit } A \subset k[X] \\ k[X] =&\quad \oplus_{i=-\infty}^{\infty} \oplus_{j=-\infty}^{\infty} H_{i,j}^{W_1,W_2}(k[X]) \end{aligned}$$

Dabei hat ein Polynom $f \in A$ den Grad

$$\deg_W(f) = \deg_{W_1,W_2}(f) := (\deg_{W_1}(f), \deg_{W_2}(f)) \in \mathbb{Z}^2$$

und man schreibt $W = (W_1, W_2)$. Diese so genannte **Bigraduierung** ist ein Spezialfall der **Multigraduierung**. Im Prinzip wird jeder i-te Teilraum bzgl. W_1 seinerseits in eine direkte Summe von Teilräumen bzgl. W_2 zerlegt. So kann man den Begriff der Homogenität auch auf ein (endliches) System von Graduierungen (respektive Gewichten) analog erweitern.

BEISPIEL. Das Polynom $f = f(x, y, z) = x^2y^{40} + y^{14}z^{10} \in k[x, y, z]$ aus dem vorherigen Beispiel ist nicht nur bzgl.

$W_1 = (2, 1, 3)$ homogen zum Grad 44, sondern auch homogen bzgl. $W_2 = (7, 1, 4)$ zum Grad 54. Also ist f homogen bzgl. W zum Grad $(44, 45)$ mit $W = (W_1, W_2)$.

1.3.3. Beschränkte Gröbnerbasis

Im Kontext der vorherigen Definitionen erweitern wir nun den Begriff der Gröbnerbasis.

DEFINITION 1.3.5. **Beschränkte Gröbnerbasis** [4, S. 15]

Sei $W = \{W_1, ..., W_r\}$ eine Menge von Graduierungen auf $k[X]$ mit $W_i \in \mathbb{N}^n$ für alle i, $d \in \mathbb{N}^n$ ein fester Multigrad, $>$ eine Monomordnung und $I \subset k[X]$ ein homogenes Ideal bzgl. W. Sei G eine endliche Menge homogener Polynome bzgl. W. $G \subset I$ heißt **d-beschränkte Gröbnerbasis bzgl. W** (und $>$), wenn gilt

$$\begin{aligned} \langle \{LT(g) \mid g \in G \wedge \deg_{W_i}(g) \leq d_i\} \rangle &= \bigoplus_{\alpha \leq d} H^W_\alpha(\langle LT(I) \rangle),\ \alpha \in \mathbb{N}^n, \\ \text{wobei } \bigoplus_{\alpha \leq d} H^W_\alpha(\langle LT(I) \rangle) &= \bigcap_{i=1}^{r} \bigoplus_{j=0}^{d_i} H_j^{W_i}(\langle LT(I) \rangle). \end{aligned}$$

Wir sehen, im Kern ist die Gröbnerbasis das Erzeugendensystem geblieben, von welchem die Leitterme das Leitideal des ganzen Ideals aufspannen. Aber man beschränkt sich auf die Unterräume bis zu einem bestimmten Grad d. Wir haben uns auch auf *positive* Gewichte beschränkt, so dass $k[X]_0^W$ die kleinste Komponente ist. Die entsprechende Monomordnung wird, wenn wir sie nicht explizit benötigen, nicht benannt.

Die Zielrichtung des weiteren Vorgehens sei nun in folgenden zwei Aspekten beschrieben. Seien $f, g \in k[X]$ zu einer Menge W von Gewichten homogen. So ist das entsprechende S-Polynom, wenn es ungleich Null ist, ebenfalls homogen bzgl. W, da sein Grad der von $\mathrm{LCM}_{f,g}$ ist, welches man an

$$S(f, g) = \frac{\mathrm{LCM}_{f,g}}{\mathrm{LT}(f)} \cdot f - \frac{\mathrm{LCM}_{f,g}}{\mathrm{LT}(g)} \cdot g$$

sieht. Jeder Term wird durch die Multiplikation auf denselben Grad $\deg_W(f) + (\deg_W(\mathrm{LCM}_{f,g}) - \deg_W(f))$ gebracht, für g analog.

Wie schon angedeutet, erhält der Buchbergeralgorithmus die Homogenität der auftretenden Polynome. Man operiert also innerhalb $(k[X])_{hom}$ der Menge aller homogenen Polynome in $k[X]$. Um noch ein allgemeineres Resultat hierzu zu bringen:

LEMMA 1.3.6. *Sei R ein G-graduierter Ring und $(G, <) = \{g_1, g_2, ...\}$ eine geordnete abelsche Gruppe, dann gilt, ist R ein Integritätsring, so sind die Teiler homogener Elemente homogen.*

BEWEIS. Sei $f = r \cdot s \in R$ homogen und insbesondere nicht 0_R. Da G geordnet ist, lässt sich $r = \sum_{i=g_{1_r}}^{g_{t_r}} r_i$ schreiben mit $g_{1_r} < ... < g_{t_r}$ und s analog. So ist $r \cdot s = r_{g_{1_r}} \cdot s_{g_{1_s}} = ... = r_{g_{t_r}} \cdot s_{g_{t_s}}$, da alle den gleichen Grad haben und damit in der gleichen homogenen Komponente R_i liegen. Damit gilt ebenfalls $t_r = t_s = 1$ und so $r, s \in R_{hom}$. ■

Es gilt insbesondere im Polynomring $k[X]$ über dem Körper k, dass die Teiler homogener Polynome homogen sind. Ebenso sind die irreduziblen Faktoren homogener Polynome homogen.

PROBLEM 1.3.7. Des weiteren wissen wir, dass der Grad des S-Polynoms vor seiner eigentlichen Berechnung über den Grad der korrespondierenden Syzygie bekannt ist. Weiß man jetzt z.B., wie viele S-Polynome noch zur Berechnung der beschränkten Gröbnerbasis fehlen, so kann man schon "ausgefüllte" Komponenten $H_i^W(I)$ außer Acht lassen. Damit werden weitere S-Polynome mit Grad i nicht erst berechnet. Um an diese Information zu gelangen, benötigt man aber eine Aussage, ob die Komponente $H_i^W(I)$ schon vollständig bestimmt ist. D. h., die entsprechende Basis enthält schon alle Elemente oder, wenn nicht, weiß man, wie viele Elemente noch fehlen. Man benötigt also die Bestimmung der Dimension dieses linearen Teilraumes. Das ist genau die Idee, Hilbertreihen zu benutzen.

KAPITEL 2

Hilbertreihen

Wir haben uns schon angesehen, wie man einen Polynomring mittels Graduierung in lineare Teilräume zerlegen kann. Nun wenden wir uns der Kernstruktur des Ansatzes zur Beschleunigung des Buchbergeralgorithmus zu, den Hilbertreihen. Dabei wird die Hilbertreihe zuerst bezüglich des Polynomrings $k[X]$ elementar entwickelt. Daran anschließend wird sie bezüglich einer Graduierung betrachtet.

2.1. Algebraisch geometrische Zusammenhänge

Zuerst ist es nötig, die grundlegendsten Zusammenhänge zwischen Idealen und Varietäten zu entwickeln, da wir in Folge ständig zwischen diesen beiden Welten in der Betrachtung wechseln werden. Schlussendlich wird auch die Hilbertreihe über die Dimension von Varietäten bestimmt werden. Den Begriff der Varietät als gemeinsamer Nullstellenmenge der Polynome eines Ideals hatten wir schon eingeführt.

2.1.1. Die korrespondierenden Abbildungen

Nun definieren wir uns die entsprechenden vermittelnden Abbildungen zwischen den Varietäten einerseits und den Idealen andererseits, um danach deren wichtigste Eigenschaften anzusehen.

DEFINITION 2.1.1. **Vermittlungsabbildungen oder Korrespondenzen I und V**

Sei $V \in k^n$ eine affine Varietät, so ist

$$\mathbb{I}(V) = \{f \in k[X] \mid \forall a \in V \,:\, f(a) = 0 \in \mathbb{R}\} \subset k[X]$$

wieder mit $X = x_1, ..., x_n$ das **korrespondierende Ideal**. Umgekehrt, wenn $I \in k[X]$ ein Ideal, so ist

$$\mathbb{V}(I) = \{a \in k^n \mid \forall f \in i \,:\, f(a) = 0 \in \mathbb{R}\} \subset k^n$$

die **korrespondierende** affine **Varietät**.

Man schreibt auch kurz $\mathbb{V}(f_1, ..., f_s) = \mathbb{V}(\langle f_1, ..., f_s \rangle)$. Wir wissen nach dem Hilbert-Basis-Theorem, dass wir immer ein Ideal mit endlicher Basis für eine gegebene Varietät finden können. Welche Eigenschaften lassen sich nun an den Korrespondenzen erkennen?

Wenn $I = \mathbb{I}(M)$ mit $M \subset k^n$, dann ist I ebenfalls ein Ideal. So folgt mit $0 \in I$ und $f, g \in I$, $h \in k[X]$, dass $(f + g)(x) = f(x) + g(x) = 0 + 0 = 0$ auf M verschwindet. Auch gilt $(hf)(x) = h(x)f(x) = h(x) \cdot 0 = 0$, was zeigt, das I ein Ideal ist. Wir werden noch sehen, wenn M eine Varietät ist, dass I das größte Ideal ist, dessen Elemente auf M verschwinden. I ist "radikal".

PROBLEM 2.1.2.

(1) Die Abbildung $\mathbb{V}$ ist nicht injektiv, da $\mathbb{V}(x) = \mathbb{V}(x^3) = \{(0, a) \mid a \in k\} \in k^2$ bezüglich $k[x, y]$ ist.
(2) Weiterhin tauchen Probleme auf, wenn k nicht algebraisch abgeschlossen ist. Dann ist z.B. $k = \mathbb{R} : \mathbb{V}(\langle 1 + x^2 \rangle) = \mathbb{V}(\langle 1 \rangle) = \emptyset$, wobei im ersten Fall keine reellen Wurzeln auftreten und die letzte Gleichheit immer gilt. Der folgende Satz nun garantiert, dass algebraische Abgeschlossenheit hinreichend dafür ist, zumindest unser zweites Problem zu lösen.

SATZ 2.1.3. ***Schwacher Nullstellensatz*** [3, S.169]

Sei k ein algebraisch abgeschlosser Körper, und $I \subset k[X]$ ein Ideal mit $\mathbb{V}(I) = \emptyset$, dann ist $I = \langle 1 \rangle$ $(= \overline{k[X]})$.

Im Fall $k = \mathbb{C}$ ist dieser Satz dem Hauptsatz der Algebra äquivalent. Jedes Polynomsystem ungleich dem ganzen Polynomring $\mathbb{C}[X]$ hat mindestens eine gemeinsame Lösung. Berechnen wir also als reduzierte Gröbnerbasis eines solchen Ideals die Eins, so existiert keine gemeinsame Wurzel.

PROBLEM 2.1.4. Die Frage, die sich nun anschließt ist, wann sind die Korrespondenzen $\mathbb{V}$ und $\mathbb{I}$ bijektiv?

Arbeiten wir mit algebraisch abgeschlossenen Körpern, dann ist zumindest die Eindeutigkeit bzgl. der leeren Menge gesichert. Aber die fehlende Eindeutigkeit von 2.1.2(1) ist damit nicht gelöst. Am Beispiel $\mathbb{V}(x) = \mathbb{V}(x^3)$ ersieht man, dass das Vorkommen von Vielfachen von Polynomen ein Grund dafür ist. Einen ersten Hinweis zur Lösung liefert uns der folgende Satz.

SATZ 2.1.5. ***Hilbertscher Nullstellensatz*** [3]

Sei k ein algebraisch abgeschlossener Körper und $f, f_1, ..., f_s \in k[X]$. Wenn $f \in \mathbb{I}(\mathbb{V}(f_1, ..., f_s))$, dann existiert ein $m \geq 1 \in \mathbb{Z}$ mit $f^m \in \langle f_1, ..., f_s \rangle$ und umgekehrt.

Der Satz zeigt den einzigen Grund, weshalb ein Ideal nicht alle auf der Varietät verschwindenden Polynome enthält. Dies ist nur der Fall, wie das Beispiel nahe legt, wenn zwar ein Vielfaches eines Polynoms aber nicht es selbst Element des Ideals ist.

Es ist nun ein so umfassendes Ideal I zu finden, dass keine Polynome hinzuzufügen sind, um die gleiche Varietät $\mathbb{V}(I)$ zu erhalten. Dies heißt also, es müssen alle Polynome, die auf V verschwinden, erfasst sein.
Wenn $f^m \in \mathbb{I}(V)$, dann ist auch $f \in \mathbb{I}(V)$, da

$$f(a) = 0 \Leftrightarrow f^m(a) = 0.$$

Also müssen alle Polynome, deren Vielfache im Ideal liegen, enthalten sein. Dies ist genau dann der Fall, wenn wir das Radikal eines Ideals betrachten.

DEFINITION 2.1.6. **Radikal** (eines Ideals) **und radikales Ideal**

Sei $I \subset k[X]$ ein Ideal, so heißt $\sqrt{I} = \{f \in k[X] \mid \exists m \geq 1 \text{ mit } f^m \in I\}$ das **Radikal** von I, bzw. ein Ideal mit dieser Eigenschaft (es ist sein eigenes Radikal) heißt **radikales Ideal**.

Offensichtlich ist $\mathbb{I}(V)$ ein radikales Ideal und es gilt $I \subset \sqrt{I}$. Wie man leicht nachprüfen kann, ist $\sqrt{I}$ selbst ein Ideal und radikal. Den Zusammenhang dieser Begriffsbildung und den Korrespondenzabbildungen reflektiert folgender Satz.

SATZ 2.1.7. ***Starker Nullstellensatz***

Sei $I \subset k[X]$ ein Ideal und k ist algebraisch abgeschlossen, so ist $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.

BEWEIS. Seien die Voraussetzungen erfüllt. Da mit $f \in \sqrt{I} \Rightarrow f^m \in I$ für ein $m \geq 1$ gilt, verschwindet auch f auf $\mathbb{V}(I)$ und liegt somit in $\mathbb{I}(\mathbb{V}(I))$. Also gilt $\sqrt{I} \subset I(V(I))$. Umgekehrt, ist $f \in \mathbb{I}(\mathbb{V}(I))$, dann verschwindet f auf $\mathbb{V}$. Nun gilt nach dem Hilbertschen Nullstellensatz, es existiert ein $m \geq 1$ mit $f^m \in I$. Aber dann ist $f \in I$ und die Gleichheit in der Behauptung gezeigt. ■

Der Nullstellensatz gibt uns nun folgende Eigenschaften für die Korrespondenzen $\mathbb{V}$ und $\mathbb{I}$.

SATZ 2.1.8. ***Die Ideal-Varietät-Korrespondenz***

Seien die Abbildungen $\mathbb{V}$ und $\mathbb{I}$ die entsprechende Korrespondenz, so folgt

(1) $\mathbb{V}$ und $\mathbb{I}$ sind inklusionsumkehrend,
(2) für alle Ideale $I \in k[X]$ gilt $\mathbb{V}(\mathbb{I}(V)) = V$, d. h. die Abbildung $\mathbb{I}$ ist immer bijektiv,
(3) wenn k algebraisch abgeschlossen ist, dann sind $\mathbb{V}$ und $\mathbb{I}$ beschränkt auf die radikalen Ideale bijektiv und die Umkehrabbildung der jeweils anderen.

BEWEIS. zu (1) Seien $I_1 \subset I_2$ Ideale in $k[X]$, dann verschwinden alle $f \in I_2 - I_1$ nicht unbedingt auf der gesamten gemeinsamen Nullstellenmenge $\mathbb{V}(I_1)$ und somit gilt $\mathbb{V}(I_1) \supset \mathbb{V}(I_2)$. So bleibt von $\mathbb{V}(\langle x \rangle) = 0 \times k \subset k^2$ nur noch $\mathbb{V}(\langle x, y \rangle) = \{(0, 0)\} \subset k^2$.
Umgekehrt, wenn $V_1 \subset V_2$ Varietäten sind, dann gilt $f \in \mathbb{I}(V_2)$ und f verschwindet insbesondere auch auf V_1. Damit gilt $f \in \mathbb{I}(V_1)$ und $\mathbb{I}(V_1) \supset \mathbb{I}(V_2)$.

zu (2) Wenn $f \in \mathbb{I}(V)$ gilt, dann folgt sofort nach Definition $V \subset \mathbb{V}(\mathbb{I}(V))$. Umgekehrt existieren $f_1, ..., f_s$ mit $V = V(f_1, ..., f_s)$. So gilt nach Definition von $\mathbb{I}$, dass $\langle f_1, ..., f_s \rangle \subset \mathbb{I}(V)$. Da $\mathbb{V}$ inklusionsumkehrend ist, gilt $\mathbb{V}(\mathbb{I}(V)) \subset \mathbb{V}(\langle f_1, ..., f_s \rangle) = V$. Somit ist die Gleichheit und die Bijektivität von $\mathbb{I}$ gezeigt.

zu (3) Zu zeigen ist, dass $I = \mathbb{I}(\mathbb{V}(I))$ ist, sofern I radikal ist. Der Nullstellensatz aber sagt, dass $\mathbb{I}(\mathbb{V}(I))$ radikal ist. Bei radikalen Idealen gilt, dass $\sqrt{I} = I$.
Da jede Korrespondenz die Umkehrabbildung der anderen Korrespondenz ist und beide bijektiv sind, folgt die Aussage des Satzes. ■

Dieser Satz gibt uns die Möglichkeit, Probleme von einer in die andere Welt zu übertragen.

Wenn man Zerlegungen von Varietäten betrachtet, kommt man z.B. zu der Frage, ob sich eine Varietät zerlegen lässt, bzw. wie sich dies in den korrespondierenden Idealen widerspiegelt. Die entsprechenden Zerlegungskomponenten müssten dann "atomar" sein, nicht mehr zerlegbar. So erscheint eine Gerade oder Ebene von dieser Art zu sein.

DEFINITION 2.1.9. **Irreduzible Varietät**

Sei $V \in k^n$ eine Varietät und $V = V_1 \cup V_2 \Rightarrow V_1 = V$ oder $V_2 = V$, so heißt V **irreduzibel**.

Wie zu erwarten korrespondiert ein ebenso wenig zerlegbares Ideal zu solch einer Varietät.

DEFINITION 2.1.10. **Primideal**

Sei $I \in k[X]$ ein Ideal und es gilt $f \cdot g \in I \Rightarrow f \in I \vee g \in I$, dann heißt I Primideal.

LEMMA 2.1.11. ***Zusammenhang***

Sei $V \in k^n$ eine Varietät, dann ist V irreduzibel $\Longleftrightarrow \mathbb{I}(V)$ ein Primideal.

BEWEIS. $\Rightarrow$: Sei $V \in k^n$ eine irreduzible Varietät und $fg \in \mathbb{I}(V)$. Stellen wir also $\mathbb{I}(V)$ dar als $\mathbb{I}(V) = I \cdot J$ mit $f \in I$ und $g \in J$. (Das Idealprodukt wird im nächsten Abschnitt eingeführt. Es ist zwar immer $IJ \subset I \cap J$, aber es kann z.B. sein, dass $J = k[X] \supset I$.) Für die Korrespondenz galt $V = \mathbb{V}(\mathbb{I}(V)) = \mathbb{V}(I \cdot J)$. Wie wir noch sehen werden, ist $\mathbb{V}(I \cdot J) = \mathbb{V}(I) \cup \mathbb{V}(J)$. Da V irreduzibel ist, sei o. B. d. A $V = \mathbb{V}(I)$ und mit $\mathbb{I}(V) = \mathbb{I}(\mathbb{V}(I)) \supset I$ also $f \in \mathbb{I}(V)$.

$\Leftarrow$: Sei also nun $\mathbb{I}(V) \subset k[X]$ ein Primideal. Stellen wir die Varietät $V \subset k^n$ dar als $V = V_1 \cup V_2$, dann folgt $V_2 \subset V$ und $\mathbb{I}(V_2) \supset \mathbb{I}(V)$. Dasselbe gilt analog für V_1. Sei nun $f \in \mathbb{I}(V_1) - \mathbb{I}(V)$ und $g \in \mathbb{I}(V_2)$ aus dem Ideal der anderen Komponente von V beliebig. Somit ist $fg \in \mathbb{I}(V)$, da $fg \in \mathbb{I}(V_i)$ für alle i. Da $\mathbb{I}(V)$ prim ist, ist $g \in \mathbb{I}(V)$, da f ja davon ausgenommen war. D. h. aber, dass $\mathbb{I}(V_2) \subset \mathbb{I}(V)$, woraus folgt $\mathbb{I}(V) = \mathbb{I}(V_2)$. ■

Wenn nun ein Ideal I prim ist, heißt das aber auch, dass mit $I \ni f^m = f^{m-1} \cdot f$ entweder $f \in I$ oder $f^{m-1} \in I$. Nach $(m-1)$-maliger Anwendung dieses Arguments folgt, dass I radikal ist.

$$I \text{ ist Primideal} \Rightarrow I \text{ radikal}$$

Somit gibt es eine Bijektion zwischen Primidealen und irreduziblen Varietäten nach der Einschränkung der Korrespondenzabbildungen $\mathbb{I}$ und $\mathbb{V}$ auf diese entsprechenden Mengen und über algebraisch abgeschlossenen Körpern.

2.2. Operationen auf Idealen

Nachdem wir uns die grundsätzlichen Zusammenhänge zwischen korrespondierenden Idealen und Varietäten angesehen haben, benötigen wir weitergehende Aussagen. Was ist beispielsweise die Varietät einer Summe von Idealen? Allgemeiner gesagt, wie ist der Zusammenhang zwischen Operationen auf Idealen und den zugehörigen Varietäten?

DEFINITION 2.2.1. **Summe von Idealen**

Seien I und J Ideale in $k[X]$, dann heißt die Menge $I + J := \{f + g \mid f \in I, g \in J\}$ die Summe der Ideale I und J.

Die wichtigsten Eigenschaften beschreibt folgendes Lemma.

LEMMA 2.2.2. *Seien $I, J \subset k[X]$ Ideale, dann ist*

(1) $I + J$ ein Ideal,
(2) $I + J$ das kleinste Ideal, welches diese beiden Ideale enthält und
(3) die Vereinigung der Erzeugenden von I und J sind Erzeugende von $I + J$.

BEWEIS. zu (1) Dass $0 \in I + J$ ist, ist klar. Ebenso, dass $h \cdot (f + g) \in I + J$ mit $h \in k[X]$, $f \in I$ und $g \in J$. Da für $h \cdot (f + g) = h \cdot f + h \cdot g$ ist, gilt $h \cdot f \in I$ und $h \cdot g \in J$. Sei $h, l \in I + J$, dann haben sie die Darstellungen $h = f_1 + g_1$ und $l = f_2 + g_2$ mit $f_1, f_2 \in I$ und $g_1, g_2 \in J$. Dann gilt $h + l = (f_1 + f_2) + (g_1 + g_2) \in I + J$. Also ist $I + J$ ein Ideal.

zu (2) Sei H ein Ideal, welches I und J enthält. Da H als Ideal auch alle Summen von Elementen aus I und J enthalten muss, gilt $I + J \subset H$.

zu (3) Seien $I = \langle f_1, ..., f_s \rangle$ und $J = \langle g_1, ..., g_m \rangle$, so gilt $I + J \subset \langle f_1, ..., f_s, g_1, ..., g_m \rangle$. Da umgekehrt $0 \in I, J$ ist und somit $f_i + 0, 0 + g_j \in I + J$ für alle i und j gilt, folgt $I + J = \langle f_1, ..., f_s, g_1, ..., g_m \rangle$. ■

BEISPIEL. Seien $I = \langle x^2 \rangle$ und $J = \langle y - z^3 \rangle$ Ideale in $\mathbb{R}^3$. Da $I + J = \langle x^2, y - z^3 \rangle$ ist, muss $\mathbb{V}(I + J)$ alle die Punkte enthalten, bei welchen alle Polynome aus I und J verschwinden. Dies ist aber nun gerade $\mathbb{V}(I) \cap \mathbb{V}(J) = \{(0, y, z) \mid y, z \in \mathbb{R} \text{ mit } y = z^3\}$.

So motiviert fassen wir diesen Zusammenhang in folgendes Lemma.

LEMMA 2.2.3. ***Zusammenhang***

Seien $I, J \subset k[X]$ Ideale, dann ist

$$\mathbb{V}(I + J) = \mathbb{V}(I) \cap \mathbb{V}(J).$$

BEWEIS. Da $I, J \subset I + J$ ist, gilt $\mathbb{V}(I + J) \subset \mathbb{V}(I)$ und $\mathbb{V}(J)$ analog. Also ist $\mathbb{V}(I + J) \subset \mathbb{V}(I) \cap \mathbb{V}(J)$.
Andererseits sei $h = f + g \in I + J$ mit $f \in I$, $g \in J$ und $x \in \mathbb{V}(I) \cap \mathbb{V}(J)$. Damit gilt $h(x) = f(x) + g(x) = 0 \in k$, da $g(x) = f(x) = 0 \in k$ ist. Hieraus folgt, da h beliebig war, $x \in \mathbb{V}(I + J)$. ■

Wenn wir ein Ideal in seinen Erzeugern gegeben haben: $I = \langle f_1, ..., f_s \rangle \subset k[X]$, dann kann man I als Summe darstellen:

$$I = \sum_{i=1}^{s} \langle f_i \rangle$$

und die zugehörige Varietät in der Form:

$$\mathbb{V}(I) = \bigcap_{i=1}^{s} \mathbb{V}\langle f_i \rangle.$$

DEFINITION 2.2.4. **Produkt von Idealen**

Seien $I, J \subset k[X]$ Ideale, dann heißt $I \cdot J = IJ := \langle f \cdot g \,|\, f \in I \wedge g \in J \rangle$ das Produkt der Ideale I und J.

Dieses Produkt ist per Definition ein Ideal. Alleine die Menge der Produkte ist kein Ideal, weil sie nicht unter Addition abgeschlossen ist. Mit fg und $f'g'$ liegt noch lange nicht $fg + f'g'$ im Ideal IJ.

BEISPIEL. Wenn $I = \langle x \rangle$ und $J = \langle y \rangle$ ist, dann ist $IJ = \langle xy \rangle$ und somit gilt $IJ \subset I, J$, da z.B $x \notin IJ$. Aber mit $J = k[X]$ ist $V(IJ) = V(I) \cup \emptyset = V(I)$.

Die Inklusion gilt allgemein, da IJ aus Summen der Form $f = \sum_{i=1}^{s} h_i f_i g_i$ besteht mit $h_i \in k[X]$, $f_i \in I$ und $g_i \in J$ für alle i. Dabei ist f offensichtlich in I und J, also $IJ \subset I, J$. Für die korrespondierende Varietät gilt folgendes:

LEMMA 2.2.5. ***Zusammenhang***

Seien $I, J \subset k[X]$ Ideale, dann gilt

$$\mathbb{V}(IJ) = \mathbb{V}(I) \cup \mathbb{V}(J).$$

BEWEIS. Sei $x \in \mathbb{V}(I) \cup \mathbb{V}(J)$ also o. B. d. A. $x \in \mathbb{V}(I)$ und damit $\forall f \in I$ ist $f(x) = 0 \in k$. Sei $g \in J$, somit ist $f(x) \cdot g(x) = 0$ und dies letztlich für alle Elemente in IJ. Das heißt nichts anderes als $x \in \mathbb{V}(IJ)$.
Andererseits, wenn $x \in \mathbb{V}(IJ)$ ist, d. h. $\forall h \in IJ$, folgt $h(x) = 0$. Dann gilt das insbesondere für $f(x) \cdot g(x) = 0$ mit $f \in I$ und $g \in J$ beliebig. Also müssen in einesm solchen Produkt die Elemente mindestens eines Ideals für x verschwinden, womit $x \in \mathbb{V}(I) \subset \mathbb{V}(I) \cup \mathbb{V}(J)$ gilt. ■

Kommen wir nun zum Schnitt von Idealen.

DEFINITION 2.2.6. **Schnitt von Idealen**

Seien $I, J \subset k[X]$ Ideale, dann heißt $I \cap J = \{f \in k[X] \mid f \in I \wedge f \in J\}$ der Schnitt der Ideale I und J.

Es ist leicht zu sehen, dass $I \cap J$ wiederum ein Ideal ist. Nach der Bemerkung zum Produkt von Idealen ist zu sehen, dass gilt

$$IJ \subset I \cap J.$$

BEISPIEL. Mit $I = \langle x \rangle$ und $J = \langle y \rangle$ gilt $I \cap J = \langle xy \rangle = IJ$. Aber es gilt in manchen Fällen die strenge Inklusion wenn z.B. $I = \langle x^\alpha \rangle = J$. Dann haben wir $IJ = \langle x^{2\alpha} \rangle \subsetneq \langle x^\alpha \rangle = I \cap J$, da $x^\alpha \notin IJ$.

LEMMA 2.2.7. ***Zusammenhang***

Seien $I, J \subset k[X]$ Ideale, dann gilt

$$\mathbb{V}(I \cap J) = \mathbb{V}(I) \cup \mathbb{V}(J).$$

BEWEIS. Es gilt $IJ \subset I \cap J$. Mit der inklusionsumkehrenden Korrespondenz und nach dem vorhergehenden Lemma folgt $\mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(IJ) \supset \mathbb{V}(I \cap J)$.
Seien andererseits $x \in \mathbb{V}(I) \cup \mathbb{V}(J)$ und o. B. d. A. $x \in \mathbb{V}(I)$. So gilt $\forall f \in I$: $f(x) = 0 \in k$. Also gilt dies insbesondere für $f \in I \cap J$. Das heißt aber $\mathbb{V}(I) \cup \mathbb{V}(J) \subset \mathbb{V}(I \cap J)$. ■

Da wir den Idealquotienten bei der praktischen Berechnung der Hilbertreihe benötigen, sehen wir ihn uns als letzte Operation in diesem Abschnitt an.

DEFINITION 2.2.8. **Idealquotient**

Seien $I, J \subset k[X]$ Ideale, dann heißt $I : J = \{f \in k[X] \mid fg \in I,$ für alle $g \in J\}$ der Idealquotient von I und J.

BEISPIEL. Seien $I = \langle xz, yz \rangle$ und $J = \langle z \rangle$ Ideale in $k[x, y, z]$. Dann ist $I : J = \langle x, y \rangle$, da für $f = ax + by$ mit $a, b \in k$ gilt, dass $f \cdot z = axz + byz \in I$. Damit haben wir $(I : J) \cdot J = \langle x, y \rangle \cdot \langle z \rangle = I$, was die Bezeichnung als Quotient motiviert.

Dass der Idealquotient selbst ein Ideal ist, lässt sich nun leicht nachrechnen. Es ist ebenfalls klar, dass $I \subset I : J$ ist, da $f \cdot g \in I$ für alle $g \in k[X]$ ist, also insbesondere für $g \in J$.

Die Entsprechung bzgl. der Varietäten ist hier nicht so einfach gestaltet, wie bei den vorherigen Operationen. Mit den Idealen aus dem obigem Beispiel ist $V = \mathbb{V}(I)$ die xy-Ebene vereinigt mit der z-Achse. $W = \mathbb{V}(J)$ stellt hingegen die z-Achse dar. Betrachtet man nun $M = V - W$ als die Differenzmenge, so ist M die xy-Ebene ohne $0 \in k^3$. M ist keine Varietät. Aber $\mathbb{V}(x, y)$ (die ganze xy-Ebene) ist die kleinste Varität, welche M enthält. Das motiviert zu folgender Definition.

DEFINITION. **Zariski-Abschluss**

Sei $M \subset k^n$ und V die kleinste Varietät, die M enthält, so heißt V Zariski-Abschluss von M und wird geschrieben $\overline{M}$.

Nun kann man zeigen [3, S.193]:

LEMMA. ***Zusammenhang***

Seien $I, J \subset k[X]$ Ideale, I radikal und k algebraisch abgeschlossen, dann gilt

$$\mathbb{V}(I : J) = \overline{V(I) - V(J)}$$

2.3. Dimension einer Varietät

An dieser Stelle werden wir von der Seite der Geometrie, die algebraische Struktur der Hilbertreihe elementar bestimmen. Eine der wichtigsten Eigenschaften im Zusammenhang mit linearen Räumen ist, welche Dimension sie haben. Die Varietät des letzten Beispiels bestand aus zwei irreduziblen Varietäten, einer Ebene und einer Achse. Wie kann man nun die Dimension der gesamten Varietät bestimmen? Intuitiv würde man sagen, dass die Dimension einer Varietät die Dimension ihrer größten Teilvarietät ist. Später werden wir sehen, dass dies mit der Definition bezüglich der entsprechenden Hilbertreihe verträglich ist.

DEFINITION. **Dimension einer Varietät**

Sei V eine affine Varietät und habe die Darstellung $V = \bigcup_{i=1}^{s} V_i$ mit V_i affine Varietät für alle i. Dann ist die **Dimension** von V definiert als $\dim(V) := \max_{i\in\{1,\dots,s\}}\{\dim(V_i)\}$.

Jetzt betrachten wir die Varietäten von Koordinatenunterräumen, also der einfachsten Form bzgl. monomialer Ideale. Dann gehen wir zu monomialen Idealen über, um schließlich Ideale allgemein zu behandeln.

2.3.1. Monomiale Ideale

DEFINITION 2.3.1. **Koordinatenunterraum**

Sei $M = \{x_i \in X \mid i \in \{1, \dots, n\}\}$, dann heißt $\mathbb{V}(M) \subset k^n$ **Koordinatenunterraum** von k^n. Man notiert $H_{xy} := \mathbb{V}(x, y)$ als Hyperebene in k^n.

BEISPIEL. Für $I = \langle xy, yz\rangle \subset k[x, y, z]$ gilt $\mathbb{V}(I) = \mathbb{V}(xy) \cap \mathbb{V}(yz) = (H_x \cup H_y) \cap (H_y \cup H_z) = H_y$, also die xy-Ebene. Wir können sagen, die Varietät ist zweidimensional.
Ein zweites Beispiel wäre die z-Achse $H_x \cap H_y = \mathbb{V}(x, y)$ als Schnitt zweier Koordinatenunterräume.

Der Koordinatenunterraum $k^3 \supset H_{xyz} = \mathbb{V}(x, y, z) = H_x \cap H_y \cap H_z = \{0\}$ umfasst dagegen nur den Nullpunkt.

Nun kann man jede Varietät $\mathbb{V}(I)$ eines monomialen Ideals I als endliche Vereinigung von solchen Koordinatenunterräumen darstellen. Ein monomiales Ideal $I \subset k[X]$ habe das endliche Erzeugendensystem $\{x^\alpha \mid \alpha \in A \subset \mathbb{Z}^n_{\geq 0},\ |A| < \infty\}$. Dass ein solches existiert, sagt Dicksons Lemma 1.1.12. Nun wissen wir, dass $I = \sum_{\alpha\in A}\langle x^\alpha\rangle$ als Idealsumme den geometrischen Zusammenhang $\mathbb{V}(I) = \bigcap_{\alpha\in A} \mathbb{V}(x^\alpha)$ impliziert. Des weiteren sei das **reduzierte Monom** gegeben mit

$$x^\alpha_{red} := \prod_{i:\alpha_i\neq 0} x_i.$$

Dies ergibt $\forall \alpha \in A : \mathbb{V}(\langle x^\alpha \rangle) = \mathbb{V}(\langle x_{red}^\alpha \rangle) = \bigcup_{i:\alpha_i \neq 0} H_{x_i}$. Da wir also einen endlichen Schnitt über endliche Vereinigungen von Hyperebenen haben, folgt mit der Distributivität der behauptete Zusammenhang:

$$V = \bigcup_{i=1}^{s} V_i \text{ für alle } i \text{ sind die } V_i \text{ Koordinatenunterräume.} \tag{2.3.1}$$

Der Schnitt zweier Koordinatenunterräume ist natürlich wieder einer, denn es ist geometrisch gesehen ja der Schnitt von Hyperebenen in k^n.

Desweiteren kann man so eine Varietät V in eindeutiger Weise zerlegen mit $V = \bigcup_{i=1}^{s} V_i$ mit der Minimalitätseigenschaft $V_i \not\supseteq V_j$ für alle $i \neq j$. Im Beispiel ist eine Varietät die Vereinigung von einer Ebene und einer Koordinatenachse. Im vorherigen Abschnitt wurden irreduzible Varietäten behandelt. Dazu folgende Überlegungen:

SATZ 2.3.2. ***DCC für Varietäten (Descending Chain Condition)***

Sei $\{V_i\}_{i\in\mathbb{N}}$ eine absteigende Folge (oder Kette) von Varietäten in k^n mit $V_{i+1} \subset V_i$ für alle i. Dann existiert ein $N \in \mathbb{N}$ mit $\forall i \geq N : V_i = V_N$.

BEWEIS. Die absteigende Kette von Varietäten V_i entspricht einer aufsteigenden Kette der korrespondierenden Ideale $I_i = \mathbb{I}(V_i)$. Nach ACC für Ideale wird diese Idealfolge stationär, sagen wir bei $N \in \mathbb{N}$ $\forall i \geq N : I_i = I_N$ und analog $\mathbb{V}(I_i) = \mathbb{V}(I_N)$. Schließlich folgt mit der Eindeutigkeit von $\mathbb{I}$: $V_i = \mathbb{V}(I_i) = \mathbb{V}(I_N) = V_N$. ■

Mit diesem Theorem lässt sich die Zerlegung von Varietäten in irreduzible Teilvarietäten zeigen.

SATZ 2.3.3. ***Zerlegung von Varietäten***

Sei $V \subset k^n$ eine Varietät, dann lässt sie sich in folgender Weise eindeutig bis auf die Reihenfolge zerlegen:

$$V = \bigcup_{i=1}^{s} V_i$$

mit $V_i \not\supseteq V_j$ für alle $i \neq j$ und V_i irreduzibel für alle i.

BEWEIS. Sei $V \subset k^n$ eine Varietät. Wenn V irreduzibel ist, sind wir fertig.
Wenn nicht, so kann V mindestens in zwei Varietäten zerlegt werden. Nun wenden wir das gleiche Argument wieder an. Diese Zerlegungskomponenten von V bilden absteigende Ketten und jede dieser wird nach endlich vielen Schritten stationär.
Bleibt die Eindeutigkeit nachzuweisen. Sobald $V_i \subset V_j$ gilt, kann man V_i streichen. Auf diese Weise kommen wir zu einer der Anzahl nach minimalen Darstellung von V. Sei nun $V = \bigcup_{i=1}^{s'} V_i'$ eine weitere Zerlegung derart und $S(V_i) = \{V_j' \mid V_j' \cap V_i \neq \emptyset\}$ für ein beliebiges aber festes $i \in \{1, ..., s\}$. Offensichtlich ist $V_i \subset S(V_i)$, da $V_i \subset V = \bigcup_{i=1}^{s'} V_i'$ ist. Da V_i irreduzibel ist, gilt $|S(V_i)| = 1$, weil sonst V_i in Varietäten zerlegt werden könnte (der Schnitt von Varietäten ist wieder eine). Die Minimalität der Zerlegung $\{V_j'\}_{j\in\{1,...s'\}}$ stellt sicher, dass es kein ν gibt mit $V_j' \subsetneq V_\nu' \in S(V_i)$ und damit

$|S(V_i)| > 1$. Also existiert ein $j \in \{1, ..., s'\}$ mit $V'_j \supset V_i$. Wenden wir das gleiche Argument auf dieses V'_j an, gilt mit $V_i \in S'(V'_j)$, S' analog zu S, $|S'(V'_j)| = 1$ und $V'_j \subset V_i$. Da i beliebig war, ist der einzige mögliche Unterschied beider Zerlegungen von V die Reihenfolge der Teilvarietäten. ■

DEFINITION. **Minimalzerlegung einer Varietät**

Eine solche Zerlegung wie im obigen Satz heißt auch Minimalzerlegung von V.

BEMERKUNG. Implizit benutzt man hier die Endlichkeit der Zerlegung in Koordinatenunterräume, da man ja sonst z.B. eine Ebene in eine Vereinigung unendlich vieler Linien zerlegen könnte. Diese Zerlegung in z.B. eine Ebene wäre somit nicht minimal.

Mit Hilfe der Minimalzerlegung einer Varietät lässt sich natürlich die korrespondierende *Zerlegung in Primideale* unter den entsprechenden Voraussetzungen schlussfolgern (unter Voraussetzung algebraisch abgeschlossener Körper und radikaler Ideale).

Sei nun eine Varietät $V \subset k^n$ zerlegt wie nach (2.3.1) in Koordinatenunterräume V_i mit der Minimalitätseigenschaft, dann ist sie von der Form

$$V_i = \mathbb{V}(\langle x^{\alpha}_{red} \rangle)$$

mit $\alpha \in \mathbb{Z}^n_{\geq 0}$. Aber $\langle x^{\alpha}_{red} \rangle$ ist offensichtlich ein Primideal und damit die V_i irreduzibel. Mit der Minimalität der Darstellung ist die gegebene Zerlegung die Minimalzerlegung von V. Klar ist auch, dass $I = \langle x^{\alpha}_{red} \rangle$ radikal ist, da mit $(x^{\alpha}_{red})^{\beta}$ und $\beta \in \mathbb{Z}^n_{\geq 0}$ alle Vielfachen von x^{α}_{red} in I enthalten sind.

DEFINITION. **Echtes Ideal**

Ein Ideal $I \in k[X]$ heißt **echt**, wenn $I \neq k[X]$.

Wir haben gesehen, dass sich eine Varietät eines monomialen Ideals immer in endlich viele Koordinatenunterräume zerlegen lässt. Die Dimension dieser Varietät war bestimmt als die größte Dimension einer dieser Teilvarietäten. Wie drückt sich dies nun in der Sprache der Ideale aus?

Je umfassender das Erzeugendensystem des Ideals ist, um so kleiner ist die korrespondierende Varietät, also deren Dimension. Ist das Ideal der ganze Polynomring, dann bleibt nur die leere Menge. Deshalb beschränken wir uns auch auf echte Ideale.
Eine Schlüsselerkenntniss bezüglich dieses Bereiches stellt die Einsicht HILBERTs dar, dass die Monome, welche *nicht* im Ideal liegen, die Dimension der korrespondierenden Varietät bestimmen. Also versuchen wir, eine Funktion zu finden, welche die Anzahl dieser Monome darstellt, um mit ihrer Hilfe die Dimension selbst zu berechnen. Dazu bilden wir die Begrifflichkeit des Komplements eines Ideals.

DEFINITION 2.3.4. **Komplement eines (monomialen) Ideals**

Sei $I \subset k[X]$ ein monomiales Ideal, dann heißt

$$C(I) := \{\alpha \in \mathbb{Z}^n_{\geq 0} | x^{\alpha} \notin I\}$$

das **Komplement** von I. Ferner seien die Basisvektoren kanonisch definiert als

$$e_i := (0, ..., 1, ..., 0) \in \mathbb{Z}^n_{\geq 0}$$

mit dem i-ten Eintrag als Eins und $i \in \{1, ..., n\}$.
Ein **Koordinatenunterraum** von $\mathbb{Z}^n_{\geq 0}$ wird notiert als

$$[e_{i_1}, ..., e_{i_s}] := \text{span}(e_{i_1}, ..., e_{i_s}) \subset \mathbb{Z}^n_{\geq 0}$$

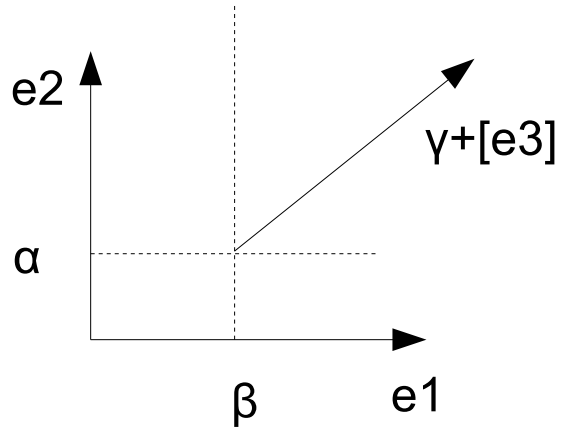
mit $i_1 < ... < i_s$ als s-dimensionaler linearer Unterraum. Eine **Verschiebung** eines solchen Unterraums wird mit

$$\alpha + [e_{i_1}, ..., e_{i_s}] := \{\alpha + \beta \,|\, \beta \in [e_{i_1}, ..., e_{i_s}]\}$$

erklärt mit $\alpha \in \mathbb{Z}^n_{\geq 0}$ und $\alpha_i \neq 0$ nicht für $i \in \{i_1, ..., i_s\}$ (also ist α "orthogonal" zu diesem Unterraum).

Sehen wir uns noch einmal den Schnitt zweier solcher Verschiebungen an:

BEISPIEL. Gegeben seinen $\alpha = 1 \cdot e_2$ und $\beta = 2 \cdot e_1$, dann ist $\alpha + [e_1] \cap \beta + [e_2] = (2 \cdot e_1 + e_2) + 0 = \gamma + 0 = \gamma$. Dieser Schnitt ergibt also den Punkt $\gamma = (2, 1)$.
Der Schnitt $\alpha + [e_1 + e_3] \cap \beta + [e_2 + e_3] = (2 \cdot e_1 + e_2) + [e_3] = \gamma + [e_3]$ ist wieder eine Verschiebung des Koordinatenunterraumes $[e_3]$.



Seien $A = \alpha + [e_{i_1}, ..., e_{i_s}] \neq B = \beta + [e_{j_1}, ..., e_{j_r}]$ zwei Verschiebungen. Zuerst widmen wir uns der Dimension des Schnittes $A \cap B$. Die Dimension von A und B sei jeweils s und t. Die Annahme ist, dass gilt

$$\dim(A \cap B) < \max(\dim(A), \dim(B)), \tag{2.3.2}$$

wenn $A \cap B \neq \emptyset$ ist.
Wenn $[e_{i_1}, ..., e_{i_s}] = [e_{j_1}, ..., e_{j_r}]$ ist, so muss $\alpha \neq \beta$ sein. Dann aber ist der Schnitt leer, wie die Ungleichung $x^\alpha \cdot x_{i_1}^{a_1} \cdots x_{i_s}^{a_s} \neq x^\beta \cdot x_{i_1}^{a_1} \cdots x_{i_s}^{a_s}$ für alle i $a_i \in \mathbb{Z}_{\geq 0}$ zeigt. Damit gilt die Ungleichung.
Sei nun $[e_{i_1}, ..., e_{i_s}] \neq [e_{j_1}, ..., e_{j_r}]$. Das heißt aber, dass sich A und B mindestens in einem e_i unterscheiden müssen. Sei $E = \{e_{k_1}, ..., e_{k_t}\} := \{e_{i_1}, ..., e_{i_s}\} \cap \{e_{j_1}, ..., e_{j_r}\}$. Dann folgt $\dim(A \cap B) = |E| = t < \max(r, s)$.

LEMMA. *Bleibt zu zeigen, dass der nichtleere Schnitt zweier Verschiebungen selbst wieder eine Verschiebung oder ein Punkt ist.*

BEWEIS. Der Schnitt besteht aber wie gesehen aus Monomen der Form $x^\alpha \cdot x_{i_1}^{a_{i_1}} \cdots x_{i_s}^{a_{i_s}} = x^\beta \cdot x_{j_1}^{a_{j_1}} \cdots x_{j_r}^{a_{j_r}}$ für alle $k, l : a_{i_k}, a_{j_l} \in \mathbb{Z}_{\geq 0}$. Die Menge E bestimmt die Menge der Linien im Schnitt. Ist $E = \emptyset$, so kann der Schnitt maximal Punkte enthalten, bzw. nur einen Punkt. Dies wird im obigen Beispiel sichtbar mit $E = \emptyset$ bzw. $E = [e_3]$.
Was sind die entsprechenden Koordinaten von γ? Seien $M_\alpha = \{i_1, ..., i_s\}$, $M_\beta = \{j_1, ..., j_k\}$, für beide gilt $M_\alpha, M_\beta \subset N = \{1, ..., n\}$ und für ihre Komplemente $U = N \backslash M_\alpha$ und $V = N \backslash M_\beta$. Die Punkte besitzen die Darstellungen $\alpha = \sum_{u \in U'} a_u e_u$ und $\beta = \sum_{v \in V'} b_v e_v$, wobei die Koeffizienten größer gleich Null und nicht Null für $U \subset U'$ und $V \subset V'$ sein sollen. Schließlich sind somit die Verschiebungen selbst als

$$A := \alpha + [\{e_\nu \mid \nu \in M_\alpha\}]$$

und $B := \beta + [\{e_\mu \mid \mu \in M_\beta\}]$ gegeben. Stellt der Schnitt $S := A \cap B \neq \emptyset$ eine Verschiebung dar? Wenn α und β gemeinsame Koordinaten haben, dann bezeichnen wir dies mit $E_{\alpha\beta} := \{u \in U \cap V \mid a_u e_u = b_u e_u\}$. Liegen von den beiden Punkten Koordinaten im jeweils anderen Koordinatenunterraum, so wird diese mit $E_\alpha := M_\beta \cap U$ und $E_\beta := M_\alpha \cap V$ bezeichnet. Schneiden sich die beiden Koordinatenunterräume selbst, so notieren wir

$$E := \{e_l \mid l \in M_\alpha \cap M_\beta\}.$$

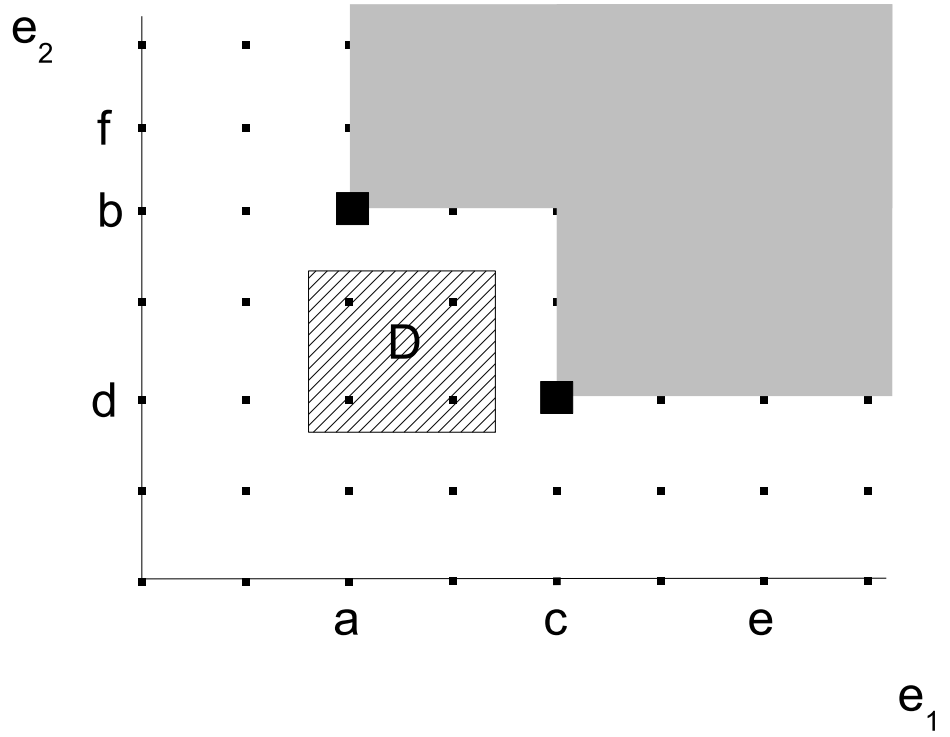
Der Ausgangspunkt γ der neuen möglichen Verschiebung S besitzt damit die Form

$$\gamma = \sum_{u \in E_{\alpha\beta}} a_u e_u + \sum_{\mu \in E_\alpha} a_\mu e_\mu + \sum_{\nu \in E_\beta} b_\nu e_\nu.$$

Nun sind die möglichen Komponenten des Schnittes beisammen.

Wenn $\gamma = 0$ und $E = \emptyset$ ist, so ist S leer, was nicht der Voraussetzung entspricht.
1. Sei hingegen $\gamma = 0$ aber $E \neq \emptyset$, so ist $S = [E]$, also ein Koordinatenunterraum und insbesondere eine Verschiebung.
2. Im Falle, dass $\gamma \neq 0$ und $E = \emptyset$ ist, gilt $S = \{\gamma\}$. Das heißt, der Schnitt besteht nur aus einem Punkt.
3. Seien beide Komponenten des Schnittes nicht Null bzw. nicht leer, dann hat S die Form $S = \gamma + [E]$ und ist eine Verschiebung. ■

BEISPIEL 2.3.5. Sehen wir uns nun folgende Darstellung des Ideals $I = \langle x^{(a,b)}, x^{(c,d)}, x^{(e,f)} \rangle \subset k[x, y]$ mit $d < b < f$ und $a < c < e$ an. Der Einfachheit halber ist es ein zweidimensionales Beispiel. Dieses zeigt alle wichtigen Elemente, die es bei der Berechnung von $C(I)$ zu beachten gilt.



Mit $a = \min(\{a, c, e\})$ und $d = \min(\{b, d, f\})$ ist ein Bereich $D \subset C(I)$ bestimmt, der endlich viele Punkte enthält. Unendlich viele Punkte aus $C(I)$ befinden sich hingegen auf den Geraden $L_y(t) = \{(x, t) \mid x \in \mathbb{Z}^2_{\geq 0}\}$ mit jeweils $t < d$ und $L_x(t') = \{(t', y) \mid \mathbb{Z}^2_{\geq 0}\}$ und $t' < a$. Dabei kann man L_y darstellen als Verschiebung eines Koordinatenunterraumes mit $L_y(t) = t \cdot e_2 + [e_1]$ und L_x analog. Es entspricht $L_y(t)$ somit die Monommenge $\{x^k y^t \mid k \in \mathbb{Z}_{\geq 0}\}$.

Für das gesamte Komplement des Ideals gilt:

$$C(I) = \bigcup_{t \leq d} (t \cdot e_2 + [e_1]) \cup \left(\bigcup_{t' \leq a} (t' \cdot e_1 + [e_2]) \right) \cup D.$$

Weiter gilt es zu beachten, dass auf diese Art die Punkte in der Schnittmengen der Geraden L_y und L_x doppelt vorkommen bzw. im n-dimensionalen Fall bis zu n-fach, z.B. $(0, ..., 0) \in \mathbb{Z}^n$.

Kommen wir nun dazu, den angesprochenen Zusammenhang zwischen dem Komplement eines Ideals und der korrespondierenden Varietät zu konkretisieren. Gerade die Koordinaten x_i, welche im Komplement $C(I)$ des Ideals liegen verschwinden nicht. Also bestimmen sie die Dimension der Varietät.

SATZ 2.3.6. *Sei $I \subsetneq k[X]$ ein echtes Ideal, dann gilt*

(1) $\mathbb{V}(\{x_i \mid i \notin A\}) \subset \mathbb{V}(I)$ mit $A = \{i_1, ..., i_r\} \Longleftrightarrow [e_i \mid i \in A] \subset C(I)$.
(2) Die Dimension von $\mathbb{V}(I)$ ist die des größten Koordinatenunterraumes in $C(I)$.

BEWEIS. zu (1) $\Leftarrow$: Sei $\emptyset \neq [e_i \mid i \in A] \subset C(I)$ für $I \subsetneq k[X]$ ein echtes Ideal. In $\langle \{x_i \mid i \notin A\} \rangle$ sind insbesondere alle Erzeuger von I enthalten, d. h. $M = \{x^\alpha \mid \alpha \in \mathbb{Z}^n_{\geq 0} \setminus C(I)\}$ mit $\mathbb{V}(\{x_i \mid i \notin A\}) \subset \mathbb{V}(M) \subset \mathbb{V}(I)$.

$\Rightarrow$: Sei nun andererseits der Punkt $a \in \mathbb{V}(\{x_i \mid i \notin A\}) \subset \mathbb{V}(I)$. Angenommen a hat die Form $a_i = 0$ für $i \notin A$ und $a_i = 0$ sonst. Dann ist $f(a) = 0$ für $f \in I$. Für das Mengenkomplement $\{x_i \mid i \in A\}$ gilt $x^\alpha \in \langle \{x_i \mid i \in A\} \rangle$ und es kann geschrieben werden als $f(x) = x^\alpha = \prod_{i \in A} x_i^{\alpha_i}$. Dann existiert mindestens ein solches i. Aber ausgewertet in a gilt $f(a) = 1$ und damit $f \notin I$. Also ist $x_i \notin I$ für solche $i \in A$ und die entsprechenden $e_i \in C(I)$.

zu (2): Laut Definition ist die Dimension einer Varietät die Dimension ihrer größten Untervarietät. Nach (1) gilt, besitzt $[e_i \mid i \in A] \subset C(I)$ die Dimension r, so korrespondiert dieser Koordinatenunterraum zu einer Untervarietät $U \subset \mathbb{V}(I)$ mit $U = \mathbb{V}(\{x_i \mid i \notin A\})$ und somit hat U die gleiche Dimension r. Letzteres gilt, da für alle $a \in U$ alle Koordinaten a_i mit $i \notin A$ verschwinden. Also bestimmt der größte Koordinatenunterraum in $C(I)$ die größte Untervarietät in $\mathbb{V}(I)$. ■

Sehen wir uns das Komplement eines monomialen Ideals genauer an. Da man ein monomiales Ideal durch endlich viele Erzeuger charakterisieren kann, legt das vorherige Beispiel nahe, dass man $C(I)$ durch endlich viele Geraden L_x, L_y und einen endlichen Bereich D von Punkten in $\mathbb{Z}^n_{\geq 0}$ beschreiben kann. Letztendlich wäre also $C(I)$ als *endliche* (nicht notwendig disjunkte) Vereinigung von Verschiebungen von Koordinatenunterräumen darstellbar [3, Theorem 3, S.439].

Jetzt kann man die Brücke von der Dimension von Varietäten monomialer Ideale zur ihrer Darstellung in Form von Polynomen auf elementare Weise schlagen. Dazu sehen wir uns die Bestimmung der Anzahl der Monome an, welche nicht in einem Ideal liegen.

LEMMA 2.3.7. ***Anzahl der Monome***

(1) Die Anzahl $A(s; n)$ der Monome in $k[X]$ vom Grad $\leq s \in \mathbb{N}$ ist

$$\begin{pmatrix} n+s \\ s \end{pmatrix}.$$

(2) Sei $A = \alpha + [e_{i_1}, ..., e_{i_m}]$ eine Verschiebung eines m-dimensionalen Koordinatenunterraumes von $\mathbb{Z}^n_{\geq 0}$ und $s > |\alpha|$, dann ist die Anzahl der Monome vom Grad kleiner gleich s

$$\begin{pmatrix} m+s-|\alpha| \\ s-|\alpha| \end{pmatrix}.$$

(3) Ist $s > |\alpha|$, dann ist die Anzahl der Monome in A durch ein Polynom in s vom Grad m mit positivem Koeffizienten $\frac{1}{m!}$ des Leitterms gegeben.

BEWEIS. zu (1): Induktion nach der Anzahl n der Unbekannten x_i. Für $n = 1$ haben wir $A(s;1) = |\{1, x_1^1, x_1^2, ..., x_1^s\}| = s+1 = \begin{pmatrix} 1+s \\ 1 \end{pmatrix} = \frac{(s+1)!}{s!\cdot 1!} = s+1$. Angenommen die Aussage ist für $n = k$ wahr. Für $n = k+1$ führen wir die möglichen Monome nach Potenzen in x_{k+1} vom Grad kleiner gleich s mit der entsprechenden Anzahl nach Induktionsvoraussetzung auf:

$$\begin{aligned}
x_{k+1}^s &: \begin{pmatrix} k+0 \\ 0 \end{pmatrix}; \text{ es ist nur das Monom } x_{k+1}^s \text{ selbst} \\
x_{k+1}^{s-1} &: \begin{pmatrix} k+1 \\ 1 \end{pmatrix}; \text{ das sind die } k+1 \text{ Monome } (x_{k+1}^{s-1}\cdot x_1^1), ..., (x_{k+1}^{s-1}\cdot x_k^1), x_{k+1}^{s-1} \\
&\vdots \quad \vdots \\
x_{k+1}^{s-s} = 1 &: \begin{pmatrix} k+s \\ s \end{pmatrix}; \text{ hier kommen alle Monome der Induktionsvoraussetzung vor}
\end{aligned}$$

So ergibt sich wie behauptet nach dem Additionstheorem für Binomialkoeffizienten [2]:

$$A(s;k+1) = \sum_{i=0}^{s} \begin{pmatrix} k+i \\ i \end{pmatrix} = \begin{pmatrix} k+s+1 \\ s \end{pmatrix}.$$

zu (2): Sei nun die Verschiebung eines Koordinatenunterraumes $A = \alpha + [e_{i_1}, ..., e_{i_m}]$ mit $\alpha \in \mathbb{Z}_{\geq 0}^n$ gegeben. Jedes entsprechende Monom aus A hat die Form x^βmit $\beta = \alpha + \beta'$ und $|\beta| = |\alpha| + |\beta'|$. Die Anzahl der Monome in A vom Grad $|\beta| \leq s$ ist gleich der Anzahl der Monome in $[e_{i_1}, ..., e_{i_m}]$ vom Grad $\leq |\beta'| = |\beta| - |\alpha| \leq s - |\alpha|$ bezüglich m Unbekannter, also gleich $A(s-|\alpha|;m)$.

zu (3): Es ist $A(s;n) = \begin{pmatrix} n+s \\ n \end{pmatrix} = \frac{1}{n!}\underbrace{(n+s)\cdots(s+1)}_{\text{n Faktoren in s}}$ ein Polynom in s mit positivem Koeffizient $\frac{1}{n!}$ in s^n. (Dies ist auch schon im Wesentlichen die Form des zu definierenden *Hilbertpolynoms*.)

Da $\begin{pmatrix} m+s-|\alpha| \\ s-|\alpha| \end{pmatrix} = \begin{pmatrix} m+s-|\alpha| \\ m \end{pmatrix} = \frac{1}{m!}(m+s-|\alpha|)\cdots(s-|\alpha|+1)$ [2, S. 105] wieder ein Polynom in s mit Grad m und positivem Koeffizienten $\frac{1}{m!}$ ist, folgt der letzte Teil der Behauptung. ■

BEMERKUNG. Der Schlüssel ist, dass der Grad der betrachteten Polynome in s gleich $\deg(A(s;m)) = m$ ist, gleich der Dimension des entsprechenden Koordinatenunterraumes. Hier wird auch ersichtlich, warum s erst ab einer bestimmten Größe (bezüglich α) die Aussage zulässt.

Betrachtet man diesen Umstand nun geometrisch an $C(I)$ aus dem Beispiel 2.3.5 auf Seite 56. Bei entsprechend kleinem Grad s werden alle Punkte in der mit D gekennzeichneten Region und die entsprechenden Punkte auf den Geraden gezählt. Bei weiterer Vergrößerung von s bringen nur noch die Geraden L_x und L_y einen Beitrag. Beim Zählen der Monome dürfen aber die jeweiligen Schnitte von z.B. L_x und L_y nur einmal berücksichtigt werden. Es geht also darum, die gemeinsamen Elemente entsprechend auszuschließen nach folgendem Prinzip:

LEMMA. *Inklusions-Exklusions-Prinzip*

Seien $A_1, ..., A_n$ endliche Mengen, dann ist

$$|\bigcup_{i=1}^{n} A_i| = \sum_{j=1}^{n}((-1)^{j-1} \sum_{0<i_1<...<i_j\leq n} |A_{i_1} \cap ... \cap A_{i_j}|) =: \Phi_n.$$

BEWEIS. Wir führen die Induktion nach der Anzahl der Mengen durch.
$n = 2 : |A \cup B| = |A| + |B| - |A \cap B|$ ist offensichtlich, da die in A und B vorkommenden Elemente genau einmal wieder abgezogen werden.
Angenommen, die Aussage ist wahr für $n = k$.
Für $n = k + 1$ gilt mit

$$A = \bigcup_{i=1}^{k} A_i \text{ und } B = A_{k+1}$$

nach Induktionsvoraussetzung für $|A \cup B|$:

$$|\bigcup_{i=1}^{k} A_i \cup A_{k+1}| = \Phi_k + |A_{k+1}| - |\bigcup_{i=1}^{k} A_i \cap A_{k+1}|.$$

Nun muss sichergestellt werden, dass die Schnitte des letzten Terms eine Ergänzung von Φ_k zu Φ_{k+1} sind. Schauen wir uns den letzten Term genauer an und wenden die Induktionsvoraussetzung an, dann folgt:

$$-|\bigcup_{i=1}^{k} A_i \cap A_{k+1}| \quad = (-1) \cdot \textstyle\sum_{j=1}^{k}((-1)^{j-1} \sum_{\sigma\in I_{j,k}} |\bigcap_{i\in\sigma} A_i \cap A_{k+1}|)$$

$$\text{mit der Indexmenge } I_{j,k} := \{i_\nu \,|\, 0 < i_1 < ... < i_j \leq k, \nu = 1, ..., j\}.$$

Die entstehenden Terme zu den verschiedenen j-Werten ergeben bei Umformulierung von $I_{j,k}$ auf $I_{j,k+1}$:

$$\begin{aligned}
j = 1 \text{ in } I_{j,k} : \ (-1)(-1)^{1-1} \sum_{i=1}^{k} |A_i \cap A_{k+1}| &= (-1) \sum_{i_1,i_2\in I_{2,k+1}} |A_{i_1} \cap A_{i_2}| \\
&\vdots \quad \vdots \\
j = r : \ (-1)(-1)^{k-r} \sum_{\sigma\in I_{r,k}} |\bigcap_{i\in\sigma} A_i \cap A_{k+1}| &= (-1)^{(r+1)-1} \sum_{\sigma\in I_{r+1,k+1}} |\bigcap_{i\in\sigma} A_i| \\
&\vdots \quad \vdots \\
j = k : \ (-1)(-1)^{k-1} \sum_{\sigma\in I_{k,k}} |\bigcap_{i\in\sigma} A_i \cap A_{k+1}| &= (-1)^{(k+1)-1} \sum_{\sigma\in I_{k+1,k+1}} |\bigcap_{i\in\sigma} A_i|.
\end{aligned}$$

Diese Terme für $I_{j,k}$ auf der linken Seite sind also genau die Terme für $I_{j,k+1}$ in Φ_{k+1} auf der rechten Seite, welche die Differenz $\Phi_{k+1} - \Phi_k$ bilden, d. h., in denen A_{k+1} vorkommt. Wir erhalten also alle Terme, in denen A_{k+1} vorkommt für jeden Schnitt von $j = 2, ..., k+1$ Mengen. Der Term für $j = 1$ in Φ_{k+1} ist $|A_{k+1}|$ selbst.
Das Vorzeichen wechselt bei einem Term bei der Umformulierung wie behauptet, da das j zu $j' = j + 1$ wird und somit der Vorzeichenwechsel stattfinden muss. Besitzt ein Term z.B. ein negatives Vorzeichen bei $j = r$, so wird der Term positiv, da mit A_{k+1} eine weitere Menge hinzukommt. Also gilt

$$|\bigcup_{i=1}^{k} A_i \cup A_{k+1}| = \Phi_{k+1}.$$

■

Da wir in der Folge immer mit *gradbeschränkten* Monomen bzw. Polynomen arbeiten werden, führen wir folgende Notation ein.

DEFINITION. Sei $I \subset k[X]$ ein Ideal, dann ist

$$\begin{aligned} k[X]_{\leq s} &:= \{f \in k[X] \mid grad(f) \leq s\} \\ k[X]_s &:= \{f \in k[X] \mid grad(f) = s\} \cup \{0\} \\ I_{\leq s} &:= I \cap k[X]_{\leq s} \\ I_s &:= I \cap k[X]_s. \end{aligned}$$

Das Nullpolynom in $k[X]_s$ ist notwendig, damit dieser ein Modul bildet mit der Abgeschlossenheit unter $'+'$.
Kommen wir jetzt zur Zusammenfassung der Resultate und stellen den Zusammenhang zwischen der Dimension einer Varietät und einem entsprechenden Polynom dar. Hierbei wird die Betrachtung der Varietät V mit der Dimension d auf den, es ist mindestens einer, Koordinatenunterraum $T_i \subset C(I)$ reduziert, der gerade diese Dimension d besitzt. Dafür steht uns die Polynomdarstellung der Anzahl seiner Monome mit Lemma 2.3.7 auf Seite 58 schon zur Verfügung.

SATZ 2.3.8. ***Zusammenhang Dimension und Polynomdarstellung***

Sei $I \subset k[X]$ ein monomiales Ideal und $dim(\mathbb{V}(I)) = d$, dann ist für genügend großes s die Anzahl der Monome im Komplement von I mit Grad $\leq s$ gegeben durch ein Polynom in s mit dem Grad d und positivem Koeffizienten von s^d.

BEWEIS. Gegeben ist $\{0\} \neq I \subset k[X]$ ein Ideal und $\dim(\mathbb{V}(I)) = d$. Für den trivialen Fall ist die Aussage klar. Wie schon festgestellt, lässt sich $C(I)$ als endliche Vereinigung von Verschiebungen von Koordinatenunterräumen T_i darstellen. Sei also

$$C(I) = \bigcup_{i=1}^{r} T_i$$

mit $T_i \neq T_j$ für $i \neq j$. Da die Dimension der Varietät d ist, gilt $\forall i : m_i := dim(T_i) \leq d$ und bei mindestens einem i gilt die Gleichheit.

Nun ist die Anzahl der Monome in $C(I)$ mit einem Grad kleiner gleich einem s zu berechnen. Wie man im Beispiel der Geraden $L_x$und L_y sehen konnte, sind die T_i nicht notwendig disjunkt, womit Punkte vielfach gezählt werden würden. Deshalb verwenden wir das Inklusions-Exklusions-Zählprinzip, um Mehrfachzählung zu vermeiden. Da wir uns beim Zählen auf Monome vom Grad $\leq s$ beschränken, wird dies durch ^{s} gekennzeichnet. Erst dadurch ist für alle $i : |T_i^s| < \infty$.

$$|C(I)^s| = \sum_{j=1}^{r} ((-1)^{j-1} \sum_{0<i_1<\ldots<i_j\leq n} |T_{i_1}^s \cap \ldots \cap T_{i_j}^s|) \tag{2.3.3}$$

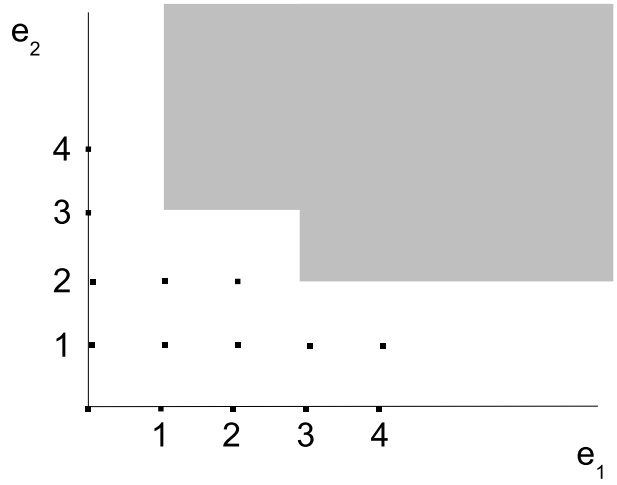
(Hierbei ist j die Anzahl der am Schnitt beteiligten Verschiebungen T_i^s.) Für geeignetes s ist die Anzahl der Punkte in T_i^s durch ein Polynom in s vom Grad $m_i \leq d$ bestimmt mit dem Koeffizienten in d von $\frac{1}{m_i!} > 0$.
Wenn nun gezeigt wird, dass der Grad aller Polynome, welche die Anzahl der Punkte in $T_{i_1}^s \cap \ldots \cap T_{i_j}^s$ bestimmen, für $\underline{j > 1}$ echt kleiner als d ist, dann wird die Anzahl der Punkte in $C(I)^s$ durch ein Polynom in s bestimmt vom Grad d mit positivem Koeffizienten von s^d.
Nun ist aber die Dimension eines nicht leeren Schnittes zweier (und damit endlich vieler) nicht identischer Verschiebungen nach (2.3.2) kleiner als das Maximum beider Dimensionen und somit insbesondere kleiner als d und dieser Schnitt ist wieder eine Verschiebung. Damit wird die Anzahl der Punkte durch ein Polynom mit dem Grad echt kleiner d dargestellt, für hinreichend großes s selbstverständlich. Das wollten wir zeigen.
In der Summe für $|C(I)^s|$ bei $j = 1$ besitzen alle Koeffizienten von s^d der Polynome bezüglich der T_i nicht negative Koeffizienten. Damit finden keine Aufhebungen statt und der Grad des Polynoms bzgl. $|C(I)^s|$ ist gleich d. ■

BEMERKUNG. Man sieht also einerseits, der Dimension der Varietät d eines monomialen Ideals I entspricht der Grad d eines speziellen Polynoms in s. Dieses ergibt ausgewertet für genügend großes s die Anzahl der Monome $|C(I)^s|$. Auf der anderen Seite haben wir gesehen, dass $\dim(\mathbb{V}(I))$ gleich ist der Dimension des größten Koordinatenunterraumes T_i^s in $C(I)$. Dieser bestimmt nun aber nach (2.3.3) gerade besagtes Polynom bezüglich seines Grades. Dies ist schön zu sehen, wenn man (2.3.3) umformuliert:

$$|C(I)^s| = \underbrace{(-1)^0 \cdot \sum_{i=1}^{s} |T_i^s|}_{\text{Polynom vom Grad} = d} + \underbrace{\sum_{j=2}^{r} ((-1)^{j-1} \sum_{\sigma\in I_{j,r}} |\bigcap_{i\in\sigma} T_i^s|)}_{\text{Polynom Grad} < d} .$$

So kann man die Aussage entsprechend des Satzes 2.3.6 konkretisieren.

KOROLLAR 2.3.9. *Wenn $I \subset k[X]$ ein monomiales Ideal ist, dann ist $dim(\mathbb{V}(I))$ gleich der Dimension des größten Koordinatenunterraumes T_i^s von $C(I)$ für genügend großes s.*



BEISPIEL 2.3.10.

Sei das monomiale Ideal $I = \langle xy^3, x^3y^2 \rangle \subset k[x, y]$ und damit Komplement mit $D = \{(1, 2), (2, 2)\}$ gegeben:

$$C(I) = L_y(0) \cup L_x(0) \cup L_x(1) \cup \{(1, 2), (2, 2)\}.$$

Seien $s = 4$ und $T_1 = L_y(0), ..., T_4 = D$. Es gilt z.B. $|T_1^4| = \begin{pmatrix} s+1 \\ 1 \end{pmatrix}$, da $T_1 = [e_2]$ eindimensional ist. So folgen nun die Darstellungen:

$$\begin{aligned}
|C(I)^4| &= |L_y(0)^4| + |L_x(0)^4| + |L_x(1)^4| + |D| \\
&- (|L_y(0)^4 \cap L_x(0)^4| + |L_y(0)^4 \cap L_x(0)^4| + |L_x(0)^4 \cap L_x(1)^4|) + |L_x(0)^4 \cap D| + |L_x(1)^4 \cap D|) \\
&+ (|L_y(0)^4 \cap L_x(0)^4 \cap L_x(1)^4| + |L_x(0)^4 \cap L_x(1)^4 \cap D|) \\
&- (|L_y(0)^4 \cap L_x(0)^4 \cap L_x(1)^4 \cap D|) \\
&= 17 - 2 + 0 - 0 = 15
\end{aligned}$$

Die ersten drei Summanden sind gleich $\begin{pmatrix} s+1 \\ 1 \end{pmatrix} = s + 1 = 5$. Dazu kommen die 2 Punkte aus D. Das sind also im ersten Teil 17 Punkte. Die einzigen beiden nicht leeren Schnitte sind $L_y(0)^4 \cap L_x(0)^4$ und $L_y(0)^4 \cap L_x(1)^4$ mit jeweils einem Punkt. Damit ergibt sich die Polynomdarstellung:

$$|C(I)^4| = p(s) = \frac{3}{1!}(s + 1) - 2 + 0 + 2.$$

Die korrespondierende Varietät ist $\mathbb{V}(I) = \mathbb{V}(xy^3, x^3y^2) = \mathbb{V}(xy) = H_x \cup H_y \subset k^2$. Die Dimension der Varietät ist Eins und somit gleich dem Grad $\deg(p) = 1$.

Würden wir hingegen das Ideal I innerhalb von $k[x, y, z]$ betrachten, dann wäre z.B. $T_1 = [e_2, e_3]$ zweidimensional und $|T_1^s| = \begin{pmatrix} s+2 \\ 2 \end{pmatrix}$. Der Punkt $(1, 2)$ aus D ist nun die eindimensionale $(m = 1)$

Verschiebungen $T = 1e_1 + 2e_2 + [e_3] = \alpha + [e_3]$ und es gilt $|T^s| = \begin{pmatrix} s+m-|\alpha| \\ m \end{pmatrix} = \begin{pmatrix} s+1-3 \\ 1 \end{pmatrix}$. T^4 besteht dabei aus den Monomen $\{xy^2z^0, xy^2z^1\}$. T_1 bestimmt auch in diesem Fall den Grad des Polynoms und die korrespondierende Varietät $\mathbb{V}(xy) = H_x \cup H_y \subset k^3$ hat nun die Dimension 2.

2.3.2. Ideale allgemein

Jetzt können wir unsere Ergebnisse auf beliebige Ideale übertragen. Haben wir ein Ideal $I \subset k[X]$ vor uns und betrachten die Menge $C(I)$. Dann kann es im Gegensatz zum monomialen Fall Elemente $f(X) = \sum_\alpha a_\alpha x^\alpha \in I$ geben, bei welchen die Monome x^αselbst nicht in I liegen, z.B. $I = \langle x^\alpha - x^\beta \rangle$. Wir müssen also $C(I)$ modifizieren, damit auch die Monome in linearer Abhängigkeit zu I Beachtung finden. Dies ist aber gerade der Quotientenraum $k[X]/I$. Die entsprechenden Äquivalenzklassen seien $[\cdot]_I$. Man sieht leicht, dass $I_{\leq s} \subset_V k[X]_{\leq s}$ ein linearer Unterraum ist und so der Quotient wohl definiert ist. Dies erinnert auch schon an die eingeführte Graduierung auf Moduln. Nun definieren wir die Hilbertfunktion (verschiedentlich auch SAMUELFUNKTION genannt).

DEFINITION 2.3.11. **Affine Hilbertfunktion**

Sei $I \subset k[X]$ ein Ideal, dann heißt

$$^aHF_I(s) := \dim(k[X]_{\leq s}/I_{\leq s}) = \dim(k[X]_{\leq s}) - \dim(I_{\leq s})$$

die **affine Hilbertfunktion** von I mit $s \in \mathbb{Z}_{>0}$ und ist somit eine nicht negative Funktion

$$^aHF_I : \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{Z}_{\geq 0}.$$

Nun benötigen wir den Zusammenhang der Hilbertfunktion zu einer möglichen Darstellung als Polynom und $C(I)$ aus dem letzten Abschnitt. Sei zuerst $I \subsetneq k[X]$ ein monomiales Ideal und $s \in \mathbb{Z}_{>0}$. Es hat $k[X]_{\leq s}$ als linearer Raum offensichtlich die Basis $\{x^\alpha \,|\, |\alpha| \leq s\}$. Es gilt also $k[X]_{\leq s} = \text{span}(\{x^\alpha \,|\, |\alpha| \leq s\})$. Analog besitzt $I_{\leq s}$die Basis $\{x^\alpha \,|\, |\alpha| \leq s \wedge \alpha \notin C(I)^s\}$. Somit gilt:

$$k[X]_{\leq s}/I_{\leq s} = \text{span}(\{[x^\alpha]_{I_{\leq s}} \,|\, \alpha \in C(I)^s\}).$$

Also ist

$$\begin{aligned} ^aHF_I(s) &= |\{[x^\alpha]_{I_{\leq s}} \,|\, \alpha \in C(I)^s\}| \\ &= |\{x^\alpha \,|\, \alpha \in C(I)^s\}| \\ &\quad \text{(als Repräsentantensystem)} \\ &= |C(I)^s|. \end{aligned}$$

Für genügend großes s folgt, dass $^aHF_I(s)$ wieder als Polynom darstellbar ist. Fassen wir das in einem Satz zusammen:

SATZ 2.3.12. *Sei $I \subset k[X]$ ein <u>echtes</u> Ideal, dann gilt:*

(1) *$^aHF_I(s)$ ist die Anzahl der Monome mit Grad kleiner gleich $s \in \mathbb{Z}_{\geq 0}$ in $C(I)$.*
(2) *Für genügend großes s kann $^aHF_I(s)$ als Polynom dargestellt werden.*
(3) *Der Grad dieses Polynoms ist die Dimension des größten Koordinatenunterraumes in $C(I)^s$ und damit die Dimension der korrespondierenden Varietät $\mathbb{V}(I)$.*

Definieren wir dieses Polynom nun:

DEFINITION 2.3.13. **Affines Hilbertpolynom**

Sei $I \subset k[X]$ ein Ideal. Das Polynom aus $k[s]$ welches für ein genügend großes s gleich der affinen Hilbertfunktion ${}^aHF_I(s)$ ist, heißt **affines Hilbertpolynom** und wird mit ${}^aHP_I(s)$ notiert. Das kleinste $s \in \mathbb{Z}_{\geq 0}$, für das diese Gleichheit gilt, heißt **Regularitätsindex** von I.

Stellt sich nun die Frage, ob eine solche Darstellung als Polynom nicht nur im monomialen Fall zu finden ist. Dazu wird im folgenden Theorem der Zusammenhang der Hilbertfunktion eines Ideals zu der seines Leitideals hergestellt, wobei letzteres ja ein monomiales Ideal ist und die gefundenen Aussagen gelten.

SATZ 2.3.14. *Sei $I \subset k[X]$ ein Ideal und $>$ ein graduierte Ordnung, dann gilt*

$$ {}^aHF_I(s) = {}^a HF_{\langle LT_>(I)\rangle}(s). \tag{2.3.4}$$

BEWEIS. Sei $G = \{f_1, ..., f_m\} \subset I_{\leq s}$ derart, dass für

$$\mathrm{LM}(I) := \{\mathrm{LM}(f) \mid f \in I_{\leq s}\} = \{\mathrm{LM}(f_1), ..., \mathrm{LM}(f_m)\}(*)$$

alle Monome verschieden sind und $\mathrm{LM}(f_1) > ... > \mathrm{LM}(f_m)$ gilt. Sei $\sum_{i=1}^m a_i f_i$ eine Linearkombination und nicht alle a_i Null, dann gibt es keine Auslöschungen der Leitterme und somit ist G linear unabhängig und $W := [f_1, ..., f_m] \subset_V I_{\leq s}$. Sei $f \in I_{\leq s} - W$ mit dem kleinsten $\mathrm{LM}(f)$, dann ist $\mathrm{LM}(f) = \lambda \mathrm{LM}(f_i)$ für ein i. Aber es ist $f - \lambda f_i \in W$, da $\deg(f - \lambda f_i) < \deg(f)$ gilt und f das Polynom mit dem kleinsten Leitmonom in der Differenz ist. Dies ist ein Widerspruch, da $f \in W$ folgt. Also gilt $[G] = I_{\leq s}$.
Bleibt zu zeigen, dass $[\mathrm{LM}(G)] = \langle \mathrm{LT}(I)\rangle_{\leq s}$ als linearer Raum ist. Weil $>$ graduiert ist, gilt

$$\deg(f) = \deg(\mathrm{LM}(f)).$$

Dann folgt aber $\{f \mid \deg(f) \leq s\} = \{f \mid \deg(\mathrm{LT}(f)) \leq s\}$. Damit und (*) werden schon alle Leitmonome durch $\mathrm{LM}(G)$ aufgespannt. Dies bedeutet, dass $\dim(\langle \mathrm{LT}(I)\rangle_{\leq s}) = \dim(I_{\leq s})$ ist, womit die Behauptung folgt. ■

Die Graduierung der Monomordnung sichert hier, dass $\deg(f) = \deg(\mathrm{LM}(f))$. Also reicht es aus, dies vorauszusetzen.

Nun sehen wir uns den Zusammenhang der Hilbertfunktionen von einem Ideal und seinem Radikal an. Dazu bestimmen wir erst einmal eine weitere wichtige Eigenschaft der Dimension von Varietäten bezüglich ihrer Ideale.

LEMMA 2.3.15. *Seien $I_1, I_2 \subset k[X]$ zwei Ideale, dann gilt für ein genügend großes s*

$$ I_1 \subset I_2 \Rightarrow deg({}^aHP_{I_{2_{\leq s}}}(s)) \leq deg({}^aHP_{I_{1_{\leq s}}}(s)). \tag{2.3.5}$$

BEWEIS. Aus der Voraussetzung folgt $\mathrm{LT}(I_2) \supset \mathrm{LT}(I_1)$, damit $\langle \mathrm{LT}(I_2)\rangle \supset \langle \mathrm{LT}(I_1)\rangle$ und direkt $C(\langle \mathrm{LT}(I_2)\rangle) \subset C(\langle \mathrm{LT}(I_1)\rangle)$ bezüglich $\mathbb{Z}^n_{\geq 0}$. Sei nun $s \geq 0$ fest.

$$\begin{aligned} I_1 &\subset I_2 \\ \Rightarrow \dim({I_2}_{\leq s}) &\geq \dim({I_1}_{\leq s}) \\ \Rightarrow \dim(k[X]_{\leq s}) - \dim({I_2}_{\leq s}) &\leq \dim(k[X]_{\leq s}) - \dim({I_1}_{\leq s}) \\ \Rightarrow {}^aHF_{{I_2}_{\leq s}}(s) &\leq {}^aHF_{{I_1}_{\leq s}}(s) \end{aligned}$$

Angenommen, es würde gelten $d := \deg({}^aHP_{{I_2}_{\leq s}}(s)) > \deg({}^aHP_{{I_1}_{\leq s}}(s))$. Sei s genügend groß. Bilden wir die Differenz P beider Hilbertpolynome, so ist $P = a_0 s^d + \sum_{i=1}^{d-1} a_i s^i$ mit $a_0 > 0$. Für genügend großes s wird der Term $a_0 s^d$ größer als die Betragssumme der restlichen Terme, weil gilt:

$$A := \frac{a_0 s^d}{\sum_{i=1}^{d-1} |a_i s^i|} = \frac{a_0}{\sum_{i=1}^{d-1} |a_i s^{i-d}|} \longrightarrow \infty \text{ für } s \to \infty.$$

Dann ist ab einem bestimmten s der Ausdruck $A > 1$. Wenn für zwei Polynome p, q gilt $p(s) > q(s)$ ab einem bestimmten s, dann gilt $\text{grad}(p) \geq \text{grad}(q)$. Ab einem bestimmten s würde gelten ${}^aHP_{{I_2}_{\leq s}}(s) \geq {}^aHP_{{I_1}_{\leq s}}(s)$ und damit wäre ${}^aHF_{{I_2}_{\leq s}}(s) \geq {}^aHF_{{I_1}_{\leq s}}(s)$. Dies ist ein Widerspruch und ergibt, dass $\deg({}^aHP_{{I_2}_{\leq s}}(s)) \leq \deg(HP_{{I_1}_{\leq s}}(s))$ und die Aussage des Lemmas gilt. ■

Einen weiteren Zusammenhang zwischen Ideal und Hilbertpolynom gibt der nächste Satz.

SATZ 2.3.16. *Sei $I \subset k[X]$ ein Ideal, dann gilt*

$$deg({}^aHP_I(s)) = deg({}^aHP_{\sqrt{I}}(s)).$$

BEWEIS. Sei $>$ eine graduierte Monomordnung. Zu zeigen ist, dass gilt:

$$\langle \text{LT}(I) \rangle \subset \langle \text{LT}(\sqrt{I}) \rangle \subset \sqrt{\langle \text{LT}(I) \rangle}.$$

Da $I \subset \sqrt{I}$ ist, folgt die erste Inklusion sofort.
Wenn $x^\alpha \in \sqrt{\langle \text{LT}(I) \rangle}$ ist, so existiert ein $f \in I$ mit $\text{LT}_>(f) = x^\alpha$. Auch existiert ein $g = f^m \in I$ für ein $m \geq 0$ mit $\text{LT}(g) = x^{\alpha \cdot m} \in \langle \text{LT}(I) \rangle$. Aber damit ist nach Definition $x^\alpha \in \sqrt{\langle \text{LT}(I) \rangle}$. Mit Lemma 2.3.15 folgt:

$$\deg({}^aHP_{\langle \text{LT}(I) \rangle}(s)) \geq \deg({}^aHP_{\langle \text{LT}(\sqrt{I}) \rangle}(s)) \geq \deg({}^aHP_{\sqrt{\langle \text{LT}(I) \rangle}}(s)).$$

Weil $>$ eine graduierte Ordnung ist, folgt zusammen mit Satz 2.3.14: $\deg({}^aHP_I(s)) = \deg({}^aHP_{\langle \text{LT}(I) \rangle}(s))$. Für ein monomiales Ideal J ist $\mathbb{V}(J) = \mathbb{V}(\sqrt{J})$ und $\deg({}^aHP_J(s))$ ist mit Satz 2.3.6 die Dimension des größten Koordinatenunterraumes von $\mathbb{V}(J)$. Deswegen ist $\deg({}^aHP_{\langle \text{LT}(I) \rangle}(s)) = \deg({}^aHP_{\sqrt{\langle \text{LT}(I) \rangle}}(s))$. ■

Jetzt haben wir einen algebraischen Zusammenhang zur Dimension einer Varietät, gehen den umgekehrten Weg und definieren die Dimension einer Varietät mit Hilfe des Hilbertpolynoms.

DEFINITION 2.3.17. **Dimension einer affinen Varietät**

Sei $V \subset k^n$ eine Varietät, dann ist $\dim(V) := \deg({}^aHP_{\mathbb{I}(V)}(s))$.

BEMERKUNG. Wenn $V = \emptyset$ gilt $\mathbb{I}(V) = \langle 1 \rangle = k[X]$ und für jedes s ist $k[X]_{\leq s} = I_{\leq s}$, also $k[X]_{\leq s}/I_{\leq s} = [0]_{I_{\leq s}}$. Da das Nullpolynom keinen Grad hat (manchmal wird ∞ angegeben), hat V in diesem Falle keine Dimension.
Also ist die Dimension einer Varietät über das Hilbertpolynom des korrespondierenden Ideals bestimmt. Das Berechnen von $\mathbb{I}(V)$ kann in vielen Fällen sehr viel Zeit in Anspruch nehmen.

Es wäre schön, wenn wir ein beliebiges Ideal mit $\mathbb{V}(I) = V$ benutzen könnten, um $\dim(V)$ zu berechnen. Das dies im Allgemeinen nicht funktioniert, zeigt folgendes Beispiel:

BEISPIEL 2.3.18. Sei $I = \langle x^2 + y^2 \rangle \subset \mathbb{R}[x, y]$, dann ist $V = \mathbb{V}(I) = \{0\} \subset \mathbb{R}^2$ und infolge dessen $\dim(V) = 0$. Benutzen wir die Monomordnung *grlex*, dann ist $\langle \mathrm{LT}(I) \rangle = \langle x^2 \rangle$ und es gilt weiterhin ${}^aHF_I(s) = {}^aHF_{\mathrm{LT}(I)}(s)$. Aber es ist ${}^aHP_I(s) = 2(s+1)$ und somit $\deg({}^aHP_J(s)) = 1 \neq 0$.

In diesem Fall finden wir $\mathbb{I}(V) = \langle x, y \rangle$ schnell. Das zugehörige Hilbertpolynom ist ${}^aHP_{\mathbb{I}(V)}(s) = 1$, da nur noch der Nullpunkt von $\mathbb{Z}^2_{\geq 0}$ in $C(\mathbb{I}(V))$ liegt. Damit ist denn auch $\deg({}^aHP_{\mathbb{I}(V)}(s)) = 0 = \dim(V)$.

Auch dieses Ergebnis liegt wieder daran, dass $\mathbb{R}$ nicht algebraisch abgeschlossen ist. Also kann man wieder den starken Nullstellensatz zu Rate ziehen und andererseits den Zusammenhang zum Radikal des Ideals mit dem Starken Nullstellensatz im Auge behalten.

SATZ 2.3.19. ***(Affiner Dimensionssatz)***
Sei k ein algebraisch abgeschlossener Körper und $V \subset k^n$ eine affine Varietät und $V = \mathbb{V}(I)$, dann gilt:

$$dim(V) = deg({}^aHP_I(s)).$$

Sei ferner $>$ eine graduierte Ordnung, dann gilt:

$$dim(V) = deg({}^aHP_{\langle LT_>(I)\rangle}(s)).$$

BEWEIS. Da k algebraisch abgeschlossen ist, gilt mit dem Satz 2.1.7: $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$ und somit

$$\dim(V) = \deg({}^aHP_{\mathbb{I}(V)}(s)) = \deg({}^aHP_{\sqrt{I}}(s)) = \deg({}^aHP_I(s)) = \deg({}^aHP_{\langle \mathrm{LT}(I)\rangle}(s)).$$

■

2.3.3. Dimension einer projektiven Varietät

Auf den $(n-1)$-dimensionalen Projektiven Raum $\mathbb{P}^n(k)$ wollen wir nicht weiter eingehen. Ein Punkt $P = (P_1, ..., P_{n+1}) \in \mathbb{P}^n(k)$ ist gegeben durch eine Äquivalenzklasse

$$P = [p]_\sim \in (k^{n+1} - \{0\}/\sim)$$

mit $p \sim p' :\Leftrightarrow p = \lambda p'$ für $p, p' \in k^{n+1} - \{0\} \wedge \lambda \in k$. Also ist die Menge dieser Punkte geometrisch gesehen die Menge der Geraden durch den Koordinatenursprung. Zeichnet man jetzt eine Komponente, z. B. P_{n+1} aus, dann ist die Abbildung

$$\Phi : \mathbb{P}^n(k) \backslash H_\infty \mapsto k^n$$

vermöge $(P_1, ..., P_{n+1}) \mapsto (P_1/P_{n+1}, ..., P_n/P_{n+1})$ die kanonische Einbettung in k^n. Die Gerade im Unendlichen bzw. der Punkt ∞ ist mit $H_\infty := \{P \in \mathbb{P}^n(k) \,|\, P_{n+1} = 0\}$ gegeben.

DEFINITION. Eine **projektive Varietät** $V \subset \mathbb{P}^n(k)$ ist gegeben als

$$V = \mathbb{V}(f_1, .., f_s) = \{P \in \mathbb{P}^n(k) \,|\, \forall i = 1, ..., s \,:\, f_i(P) = 0\},$$

wobei für alle i gilt $f_i \in k[X']_{hom}$.

Die homogenen Polynome in $k[X']$ operieren verträglich auf der Struktur dieses Raumes, da $0 = f(p) = f(\lambda p) = \lambda^d f(p) = 0$ mit $f(X) = \sum_\alpha x^\alpha \in k[X']$ gilt für alle α: $|\alpha| = \deg(f) = d$. Denn es ist $f(\lambda p) = \sum_\alpha \lambda^{\alpha_0} \cdots \lambda^{\alpha_n} \cdot p_0^{\alpha_0} \cdots p_n^{\alpha_n} = \lambda^d \cdot \sum_\alpha p^\alpha$.

Gesucht ist nun die Anzahl der Monome mit genau dem Grad s. Das stellt sich mit unserer Notation und dem Additionstheorem dar als:

$$\begin{aligned}
\dim(k[X']_s) &= A(n+1; s) - A(n+1; s-1) \\
&= \left(\begin{array}{c} (n+1)+s \\ s \end{array} \right) - \left(\begin{array}{c} (n+1)+(s-1) \\ (s-1) \end{array} \right) \\
&= \left(\begin{array}{c} (n+1)+s \\ n+1 \end{array} \right) - \left(\begin{array}{c} (n+1)+(s-1) \\ (n+1) \end{array} \right) \\
&= \left(\begin{array}{c} n+s \\ n \end{array} \right) = \left(\begin{array}{c} n+s \\ s \end{array} \right),
\end{aligned}$$

bzw. $\dim(k[X]) = \left(\begin{array}{c} n-1+s \\ s \end{array} \right) = \left(\begin{array}{c} n-1+s \\ n-1 \end{array} \right)$.

Die projektive Hilbertfunktion wird dann wie folgt definiert:

DEFINITION 2.3.20. **Projektive Hilbertfunktion**

Sei $I \subset k[X']$ ein homogenes Ideal, dann heißt

$$HF_I(s) := \dim(k[X']_s/I_s)$$

die **projektive Hilbertfunktion** von I.

Betrachten wir die entsprechenden Basen, so gilt analog zum affinen Fall:

$$\begin{aligned}
k[X']_s &= \text{span}(\{x^\alpha | \alpha \in \mathbb{Z}_{\geq 0}^{n+1} \wedge |\alpha| = s\}) \\
k[X']_s/I_s &= \text{span}(\{[x^\alpha]_I | \alpha \in C(I_s) \cap k[X']_s \wedge |\alpha| = s\}) \\
&= \text{span}(\{x^\alpha | \alpha \in C(I_s) \cap k[X']_s \wedge |\alpha| = s\}).
\end{aligned}$$

Dann ist $HF_I(s) = |\{x^\alpha | \alpha \in C(I_s) \cap k[X']_s \wedge |\alpha| = s\}|$. Die Hilbertfunktion kumuliert also die Werte bezüglich der Grade nicht wie im affinen Fall, sondern betrachtet nur eine Komponente jeweils bezüglich der "natürlichen Graduierung".

Analog zum affinen Fall wird das projektive Hilbertpolynom $HP_I(s)$ bestimmt und damit die Dimension einer projektiven Varietät. Im Satz 2.3.14 auf Seite 65 benötigt man keine graduierte Monomordnung, da im homogenen Fall immer $\deg(f) = \deg(\mathrm{LT}(f))$ gilt. Nach leichter Modifikation des Beweises gilt dessen Aussage auch im projektiven Fall

$$HF_I(s) = HF_{\langle \mathrm{LT}(I)\rangle}(s)$$

für ein homogenes Ideal $I \in k[X']$.

DEFINITION. **Dimension einer projektiven Varietät**

Sei $V \subset \mathbb{P}^n(k)$ eine projektive Varietät, dann ist

$$\dim(V) = \deg(HP_I(s))$$

mit $I = \mathbb{I}(V) \subset k[X']$ dem korrespondierenden homogenen Ideal.

SATZ 2.3.21. ***Zusammenhang der affinen und projektiven Hilbertfunktion***
Sei $I \subset k[X']$ ein homogenes Ideal und $s \geq 1$, dann gilt

$$HF_I(s) = {}^aHF_I(s) - {}^aHF_I(s-1).$$

Umgekehrt, sei $I \subset k[X]$ ein Ideal und $s \geq 0$, dann gilt

$${}^aHF_I(s) = HF_{I^h}(s).$$

Zum Beweis siehe [3, S.454]. Im eigentlichen Algorithmus werden später nur homogene Polynome verwandt.

2.4. Hilbertreihe graduierter Module und Gewichte

Bisher wurden Hilbertreihen auf elementarer Ebene über die Hilbertfunktion betrachtet, um die tieferen Zusammenhänge zu entschlüsseln. Nun ist es an der Zeit, einen abstrakteren Zugang zu wählen (siehe [5],[6, S.213ff],[7, S.93ff]), um noch mehr aus der gewonnenen Struktur herausholen zu können. Dazu stecken wir den Rahmen ab, in welchem wir die Endlichkeit der homogenen Komponenten des graduierten Moduls sicherstellen.

DEFINITION. **Noethersch**

Noethersch heißt ein Ring, wenn jedes seiner Ideale endlich erzeugt ist, was bei $k[X]$ nach dem Hilbertschen Basissatz der Fall ist. Analog heißt ein Modul **noethersch**, wenn jeder seiner Untermodule endlich erzeugt ist.

Allgemeiner kann man formulieren, dass ein Ring noethersch ist, wenn die Menge seiner Ideale ACC erfüllen, d. h., jede aufsteigende Kette von Idealen bzgl. der Mengeninklusion wird stationär. Diese Bedingung war gerade an Hand $k[X]$ formuliert worden.

DEFINITION. **Artinsch**

Ein Ring heißt **artinsch**, wenn die Menge seiner Ideale DCC erfüllen, d. h., jede absteigende Kette dieser Ideale wird stationär. Analog ist ein Modul **artinsch**, wenn die Menge der Untermodule DCC erfüllt.

Sei $I_1 \supset ... \supset I_i \supset I_{i+1} \supset ...$ eine absteigende Kette von Idealen in $k[X]$. Nach dem Hilbertschen Basissatz ist I_1 endlich erzeugt und somit wird diese Kette stationär, was bedeutet, dass $k[X]$ artinsch ist.

DEFINITION 2.4.1. **Endlich erzeugter R-Modul**

Einen graduierten R-Modul $M = \oplus_{g\in G} M_g$ nennen wir **endlich erzeugt**, wenn er von endlich vielen homogenen Elementen erzeugt wird.

So ist auch jeder Untermodul von M also auch die homogenen Komponenten $M_g \subset_M M$ als R_0-Module für alle $g \in G$ endlich erzeugt. Das bedeutet insbesondere, dass M noethersch ist.

BEISPIEL. So ist $I \subset k[X]$ ein homogenes Ideal nach dem Hilbertschen Basissatz mit $I = \langle f_1, ..., f_s\rangle$ als Ideal endlich erzeugt und somit ein endlich erzeugter R-Modul mit $R_0 = k$ und $R = k[X]$. $k[X]$ ist ja selbst als Ring mit den Gewichten W über k mit den Monomen $\{x_i^{w_i}\}_{i=1,...,n}$ endlich erzeugt. Als Modul über sich selbst hingegen ist $k[X]$ mit $\{1\}$ endlich erzeugt.

Allgemeiner könnte man R_0 als einen artinschen Ring annehmen (vgl. Kunz [6, S.212]).

DEFINITION 2.4.2. **Allgemeine Hilbertreihe**

Sei $R = \oplus_{i\in\mathbb{Z}} R_i$ ein noetherscher, graduierter Ring mit $R_0 = k$ ein Körper. Ferner sei $M = \oplus_{i\in\mathbb{Z}} M_i$ ein endlich erzeugter graduierter R-Modul. Dann ist die Potenzreihe in $\mathbb{Z}$ in der Unbekannten t

$$HS(t) = HS_M(t) := \sum_{i\in\mathbb{Z}} \dim(M_i)t^i \in \mathbb{Z}[[t]]$$

die **Hilbertreihe**, auch Hilbert-Poincaré-Reihe oder formale Laurentreihe, von M.
Wenn $W = \{W_1, ..., W_r\}$ eine Multigraduierung ist, dann ist die Hilbertreihe vom M bzgl. W definiert als

$$HS^W(t) = HS^W_M(t) := \sum_{\alpha\in\mathbb{Z}^r} \dim(H^W_\alpha(M))t^\alpha$$

mit der Unbestimmten $t = (t_1, ..., t_r)$ und $t^\alpha := \prod_{i=1}^r t_i^{\alpha_i}$.

DEFINITION 2.4.3. **Gewichtssystem**

Sei $W = (W_1, ..., W_r) \in (\mathbb{Z}^n_{\geq 0})^r$ ein Tupel von Gewichten auf $k[X]$ mit

(1) $W_j(x_i) \geq 0$ für alle i, j
(2) für alle i existiert ein j mit $W_j(x_i) > 0$

(3) $\{W_1, ..., W_r\}$ ist linear unabhängig,
dann heißt W ein **Gewichtssystem**.

Die einzelnen Gewichte werden notiert mit $w_{ij} = W_j(x_i) := (W_i)_j$ für $i \in \{1, ..., r\}$ und $j \in \{1, ..., n\}$. Die i-te Komponente der Gewichtsvektoren (bzgl. x_i) schreibt man $w_i := (w_{i1}, ..., w_{ir})$ mit $i = 1, ..., n$.

Diese Definition stellt sicher, dass $R_0 = H_0^W(k[X]) = k$ ist. Wir müssen sichern, dass die einzelnen Komponenten auch nach der Gewichtung endlich bleiben.

Nach Definition ist $H_0^W(k[X]) = \bigcap_{i=1}^r H_0^{W_i}(k[X])$, da alle Gewichte positiv sind. Nach Bedingung (2) gibt es für jede Koordinate x_i immer ein j mit $W_j(x_i) > 0$. So gilt für das lineare Monom $x_i \notin H_0^{W_j}(k[X])$ und es liegt auch nicht im Schnitt $H_0^W(k[X])$. Im Schnitt liegen also nur Polynome f bestehend aus Monomen der Grade α mit $\alpha_i = 0$ für alle i. Das heißt, dass $f \in k$ ist. Der Punkt (3) sichert eine gewisse Minimalität des Systems. Ist die Graduierung also ein Gewichtssystem, dann ist es z.B. möglich, die eben definierten Hilbertreihen $HS^W(t)$ bezüglich $k[X]$ zu formulieren.

BEISPIEL. Die so genannte Γ-Graduierung ist *kein* Gewichtssystem. Sie ist definiert auf $k[X, Z]$ durch $\Gamma(x_i) = 0$ für alle i, $Z = (z_1, ..., z_l)$: $\Gamma(z_j) = 1$ und $Z = \{z_j\}$ für $j = 1, ..., l$. Hier ist $H_0^\Gamma(k[X, Z]) = k[X] \neq k$. Damit verfügt sie aber nicht über die Eigenschaften, um bezüglich ihrer eine Hilbertreihe bilden zu können, da $\dim(k[X]) = \infty$ ist.

Sei andererseits $W = \{(2, 3, 1)^T, (7, 7, 0)^T\}$ auf $k[x, y, z]$, so sind die Bedingungen erfüllt und man kann die Hilbertreihe bilden.

$$\begin{aligned} HS^W_{k[x,y,z]}(t) &= \sum_{i=(0,0)}^{\infty} \dim(H_i^W(k[x, y, z]))t^i \\ &= \sum_{r,s=(0,0)}^{\infty} \dim(H_r^{W_1}(k[x, y, z]) \cap H_s^{W_2}(k[x, y, z]))t^{(r,s)} \end{aligned}$$

Wenn nun $W = \{W_1, ..., W_r\}$ ein Gewichtssystem ist, so ist $HS^W_{k[X]}(t) = \sum_{\alpha \in \mathbb{N}^r} \dim(H_\alpha^W(k[X]))t^\alpha$ wohl definiert.

Im Fall $W = N$ ergibt sich nach den vorherigen Abschnitten:

$$\begin{aligned} HS_{k[X]}(t) &= \sum_{i=0}^{\infty} \dim(k[X]_i) \cdot t^i \\ &= \sum_{i=0}^{\infty} \begin{pmatrix} i+n-1 \\ n-1 \end{pmatrix} \cdot t^i \\ &= \frac{1}{\Pi_{i=1}^n (1-t)}. \end{aligned} \tag{2.4.1}$$

BEISPIEL 2.4.4. Sehen wir uns ein sehr einfaches Ideal $I = \langle x^3 \rangle \subset k[x, y, z]$ an. Die Hilbertreihe ist dann:

$$HS_{k[x,y,z]/I}(t) = \frac{1 - t^3}{(1-t)^3} = 1 \cdot t^0 + 3 \cdot t^1 + 6 \cdot t^2 + 9 \cdot t^3 + 12 \cdot t^4 + \cdots$$

In der Reihenentwicklung um $t = 0$ sieht man die Dimensionen der Unterräume von $C(I)$ als Koeffizienten. Führen wir kurz die ersten dieser Unterräume mit ihrer Dimension und ihrer jeweiligen Basis auf:

Grad	:	Monome
0	:	$\{1\}$
1	:	$\{x, y, z\}$
2	:	$\{x^2, y^2, z^2, xy, xz, yz\}$
3	:	$\{x^2y, xy^2, x^2z, xz^2, y^2z, yz^2, y^3, z^3, xyz\}$
4	:	$\{x^3y, x^2y, x^3z, x^2z^2, y^2z^2, y^3z, yz^3, y^4, z^4, x^2yz, xy^2z, xyz^2$
	⋮	

Für das Ideal $I = \langle xy^3, x^3y^2 \rangle \subset k[x, y, z]$ aus dem Beispiel auf Seite 62 ergibt sich:

$$HS_{k[x,y,z]/I}(t) = \frac{1 - t^5 - t^4(1-t^2)}{(1-t)^3} = 1 \cdot t^0 + 3 \cdot t^1 + 6 \cdot t^2 + 10 \cdot t^3 + 14 \cdot t^4 + \cdots$$

Der Zusammenhang mit dem vorher elementar Entwickelten stellt sich wie folgt dar. Sei $I \subset k[X]$ ein Ideal. Die affine Hilbertfunktion liefert uns zu jedem s die Dimension, d. h. die Anzahl der entsprechenden Monome von $k[X]_{\leq s}/I_{\leq s}$. Das ist aber nichts anderes als die Aufsummierung der Anzahl der Monome pro Grad bis zum Grad s, also

$$\begin{aligned} {}^aHF_I(s) &= \sum_{i=0}^{s} HF_I(i), \text{ bzw. in der (projektiven) Hilbertfunktion ausgedrückt} \\ HS_{k[X]/I}(t) &= \sum_{i=0}^{\infty} HF_I(i) \cdot t^i. \end{aligned}$$

Die Koeffizientendarstellung der eben definierten Hilbertreihe erhält die Form:

$${}^aHF_I(s) = HS_{k[X]/I;s}(1),$$

wenn man die Reihe $HS_{k[X]/I}$ bis zum s-ten Glied betrachtet und an der Stelle $t = 1$ auswertet. Wohl bemerkt, zielte die Entwicklung von ${}^aHF_I(s)$ nur auf den Grad des entsprechenden Hilbertpolynoms ab, um die Dimension der korrespondierenden Varietät zu bestimmen und nichts weiter.

Jetzt interessieren wir uns für die dahinter liegende Struktur selbst, also gerade die Dimensionen der einzelnen Teilräume der Graduierung, die in der obigen Potenzreihe auftauchen. In diesem

Zusammenhang wird die Hilbertfunktion auch in folgender alternativer Weise definiert mit der Graduierung $G = \mathbb{Z}$

$$HS_M(t) = \sum_{k\in\mathbb{Z}} \chi_M(k) \cdot t^k$$

mit der allgemeiner gefassten charakteristischen Funktion

$$\chi_M(g) := \dim(M_g)$$

auf einem graduierten Modul $M = \oplus_{g\in G} M_G$.

Nun suchen wir eine Darstellung dieser Potenzreihe, die gut in einen Algorithmus umzusetzen wäre. Wie sich die affine Hilbertfunktion für ein geeignetes s als Polynom darstellen lässt, wissen wir. Kann man für die Hilbertreihe eine analoge Darstellung finden.

Dazu sind einige Vorbetrachtungen zu machen.

LEMMA. *Sei M ein G-graduierter R-Modul und $\overline{M} := M/rM$. Dann ist $\overline{M}$ ein graduierter Modul.*

BEWEIS. $\overline{M}$ ist ein Modul, da $rM \subset_M M$ für $r \in R$ und $\deg(r) = d$ ein Untermodul ist.

Eine homogene Komponente von $\overline{M}$ ist für $g \in G$ gegeben mit:

$$(M/rM)_g := M_g/rM_{g-d} \cong (M_g + rM)/rM.$$

Dies gilt, da $(M/rM)_g \ni [m] = \{m' \in M \mid m - m' = r \cdot m'' \wedge m', m'' \in M\}$ gilt. Es ist $\deg(m) = \deg(m') = g$ und $\deg(m'') = g - d$. Für die skalare Multiplikation mit $[m] \in (M/rM)_g$ gilt $r \cdot [m] = [r \cdot m]$ mit $\deg(r \cdot m) = d + g$ also $[r \cdot m] \in (M/rM)_{g+d}$.
Ebenso folgt mit $[m'] \in \overline{M}_{g'} : [m'] + [m] = [m + m'] \in (M/rM)_{g+g'}$. Jedes Element $[m] \in \overline{M}$ ist gegeben in der Darstellung $[m] = \sum_{g\in G}[m_g]$ mit $[m_g] \in (M/rM)_g$. Also ist $\overline{M}$ ein G-graduierter R-Modul. ■

Der nächste Schritt wird sein, dass wir uns ansehen, wie die Hilbertreihe bezüglich eines Quotientenmoduls aussieht.

DEFINITION. **Exakte Folge**

Sei $(\phi_i)_{i\in\mathbb{N}}$ eine Folge von Homomorphismen, bei welchem das Bild von ϕ_i der Kern von ϕ_{i+1}ist

$$\mathrm{img}(\phi_i) = \phi_i(M_i) = \mathrm{kern}(\phi_{i+1}),$$

heißt **exakte Folge**. Dabei gilt $\phi_i : M_i \to M_{i+1}$. Die exakte Folge wird notiert mit:

$$... \to M_i \to M_{i+1} \to ...$$

Mit dieser Notation lassen sich die Homomorphiesätze elegant ausdrücken, z.B folgt aus obigem Fragment $M_{i+2} \cong M_{i+1}/M_i$.

Die Voraussetzungen des nächsten Satzes bzgl. des Ringes R stellen sicher, dass die Moduln M_g als R_0-Moduln für alle $g \in G$ der Graduierung endlich erzeugt sind, somit also $\chi_{M_g}(g) < \infty$ gilt. R ist hier nicht als noethersch vorausgesetzt. Zunächst betrachten wir den Fall von einfacher Graduierung W, also einem Gewichtsvektor w.

LEMMA 2.4.5. [6, S.212] *Sei $M = \oplus_{g\in G} M_g$ ein endlich erzeugter, graduierter R-Modul und $r \in R^W_{hom}$ homogen zum Grad d, welches kein Nullteiler von M ist (M-reguläres Element) und der graduierte Ring $R = R_0[X]$ und W gegeben als $grad(x_i) = w_i > 0$ für alle i. Dann gilt*

$$\chi_{M/rM}(g) = \chi_M(g) - \chi_M(g-d) \tag{2.4.2}$$

und für $G = \mathbb{Z}$ gilt die spezielle Form

$$HS_{M/rM}(t) = (1-t^d)\cdot HS_M(t). \tag{2.4.3}$$

BEWEIS. Sei $r \in R$, homogen zum Grad d und kein Nullteiler in M. Dann induziert r eine exakte Folge endlich dimensionaler Vektorräume

$$0 \to^{\iota} M_{g-d} \to^{s_r} M_g \to^{\pi} (M/rM)_g \to^{\nu} 0.$$

Die Abbildung $s = s_r$ ist gegeben mit $m \mapsto r\cdot m$. Also ist $s(M_{g-d}) = rM_{g-d}$. Da r kein Nullteiler von M ist, ist s injektiv. Und es gilt $\ker(s) = 0 = \mathrm{img}(\iota) = \iota(0)$.

Die Abbildung π ist hingegen die kanonische Projektion von M in die Äquivalenzklassen M/rM. So ist $\ker(\pi) = rM$ und bezüglich der g-ten homogenen Komponente des Bildes

$$\ker(\pi\,|_{M_g}) = rM_{g-d} = \mathrm{img}(s) = s(M_{g-d}).$$

Die letzte Abbildung ν der exakten Folge ist die Nullabbildung $\nu \equiv 0$, womit $\ker(\nu) = (M/rM)_g = \mathrm{img}(\pi)$ gilt. Also gilt nach der exakten Folge $M_g/M_{g-d} \cong (M/rM)_g$ und somit gilt die erste Gleichung $\dim((M/rM)_g) = \dim(M_g) - \dim(M_{g-d})$.

Mit $G = \mathbb{Z}$ und $\deg(r) = k$ können wir den Ausdruck verfeinern:

$$\begin{aligned} HS_{M/rM}(t) &= \sum_{k\in\mathbb{Z}} (\chi_M(k) - \chi_M(k-d))t^k \\ &= \sum_{k\in\mathbb{Z}} \chi_M(k)t^k - \chi_M(k-d)t^k \\ &= \sum_{k\in\mathbb{Z}} \chi_M(k)t^k - \sum_{k\in\mathbb{Z}} \chi_M(k-d)t^{k-d} \\ &= (1-t^k)HS_M(t). \end{aligned}$$

Damit folgt auch die zweite behauptete Gleichung. ■

2.4.1. Multigraduierung und die Darstellung

Betrachten wir nun den Fall der Multigraduierung W, wobei $W = \{W_1, ..., W_s\}$ ein Gewichtssystem ist. Die Hilbertreihe kann man analog zum einfachen Fall entwickeln. Für die Hilbertfunktion ergibt sich mit dem Multigrad $\alpha \in \mathbb{Z}^s_{\geq 0}$: $\chi_M(\alpha) = \dim(H^W_\alpha(M))$.

Das homogene M-reguläre Element $r \in R^W_{hom}$ habe den multigrad$(r) = \alpha_r$. Die Abbildung $s_r : m \longmapsto r \cdot m$ hat die Eigenschaft, dass $s(M_{\alpha_k - \alpha_r}) = M_{\alpha_k}$ ist und s wieder injektiv ist mit kern$(s) = 0$. Nun bildet man wieder die Äquivalenzklassen M/rM und $M_{\alpha_k}/M_{\alpha_k - \alpha_r} \simeq (M/rM)_{\alpha_k}$. Damit gilt wieder die Gleichung (2.4.2) und mit $G = \mathbb{Z}^s_{\geq 0}$ und auch die zweite Aussage des Satzes. Mit Hilfe dieses Zusammenhanges lässt sich nun sehr einfach eine Darstellung der Hilbertreihe z.B. für den ganzen Polynomring $k[X]$ oder seine Quotientenmoduln finden.

(1) Sei $R = k[X]$ mit dem Gewichtssystem $W = \{W_1, ..., W_r)\}$, dann ist $R/\langle x_n \rangle = k[x_1, ..., x_{n-1}]$. Für die entsprechende Hilbertreihe erhalten wir (wieder mit $t^{w_i} := \Pi_{j=1}^s t_j^{w_{ij}}$)

$$1 = HS_k(t) = HS_{R/\langle x_1,...,x_n\rangle}(t) = \prod_{i=1}^{n}(1 - t^{w_i}) \cdot HS_{k[X]}(t).$$

So lässt sich für die Hilbertreihe des ganzen Polynomrings analog (2.4.1) eine Darstellung als rationale Funktion in $k(t)$ finden:

$$HS_{k[X]}(t) = 1/\prod_{i=1}^{n}(1 - t^{w_i}) = 1/\prod_{i=1}^{n}(1 - t^{w_{i1}} \cdots t^{w_{ir}}). \tag{2.4.4}$$

(Die Implementation des Nenners der Hilbertreihen bezüglich Gewichten ist aufgeführt auf Seite 92.) Mit der natürlichen einfachen Gewichtung N und dem schon bekannten Zusammenhang bzgl. der Anzahl der Monome zum Grad i hatten wir elementar hergeleitet:

$$HS_{k[X]}(t) = 1/(1 - t)^n = \sum_{i=0}^{\infty} \chi_{k[x]}(i) \cdot t^i = \sum_{i=0}^{\infty} \begin{pmatrix} i + n - 1 \\ n - 1 \end{pmatrix} t^i.$$

(2) Seien nun $f_1, ..., f_s \in k[X]_{hom}$ mit dem Gewichtssystem $W = (W_1, ..., W_r)$ mit $w_{ij} > 0$ und $d_{ij} := \deg_{W_j}(f_i) > 0$ für alle i und j. Ferner dürfen die Polynome f_i keine "Nullteiler" sein. Dies ist in der Weise gemeint, dass das Bild von f_i in $k[X]/\langle f_1, ..., f_{i-1}\rangle$ für $i = 1, ..., s$ kein Nullteiler ist. Wendet man nun das vorherige Lemma an, dann ergibt sich sukzessiv

$$\begin{aligned} HS_{k[X]/\langle f_1,...,f_s\rangle}(t) &= \prod_{i=1}^{s}(1 - t^{d_i}) \cdot HS_{k[X]}(t) \\ &= \prod_{i=1}^{s}(1 - t^{d_i})/\prod_{i=1}^{n}(1 - t^{w_i}) \\ &= g^{\langle f_1,...,f_s\rangle}(t)/\prod_{i=1}^{n}(1 - t^{w_i}). \end{aligned}$$

(3) Für die Multigraduierung aus dem vorherigen Beispiel mit dem Gewichtssystem $W = \{(2, 3, 1)^T, (7, 7, 0)^T\}$ auf $k[x, y, z]$ können wir nun die entsprechende Hilbertreihe

mit $t = t_1 \cdot t_2$ explizit und analog zu (2) aufschreiben:

$$\begin{aligned} HS^W_{k[x,y,z]}(t) &= \sum_{i=(0,0)}^{\infty} \dim(H^W_i(k[x, y, z]))t^i \\ &= \frac{1}{(1 - t_1^2 \cdot t_2^7)(1 - t_1^3 \cdot t_2^7)(1 - t_1)} \\ &= \frac{1}{(1 - t^{(2,7)})(1 - t^{(3,7)})(1 - t^{(1,0)})}. \end{aligned}$$

DEFINITION 2.4.6. **Numerator der Hilbertreihendarstellung**

Sei die Hilbertreihe eines Ideals $I = \langle f_1, ..., f_s\rangle \subset k[X]$ in der Form

$$HS_{k[X]/\langle f_1,...,f_s\rangle}(t) = g^{\langle f_1,...,f_s\rangle}(t) / \prod_{i=1}^{n}(1 - t^{w_i})$$

gegeben. Das Polynom $g^{\langle f_1,...,f_s\rangle}(t) \in k[t]$ im Zähler der Hilbertreihe $HS_{k[X]/\langle f_1,...,f_s\rangle}(t)$ bezeichnen wir als den **Numerator** und notieren ihn mit

$$\text{num}(\langle f_1, ..., f_s\rangle) := g^{\langle f_1,...,f_s\rangle}(t).$$

Dies ist auch der später eigentlich zu berechnende Term der Hilbertreihe im Algorithmus, da der Nenner immer den gleichen Ausdruck (2.4.4) bezüglich des jeweiligen Raumes $k[X]$ und der Gewichte W darstellt.

KAPITEL 3

Hilbertreihen und Buchbergeralgorithmus

3.1. Berechnung von Hilbertreihen

Nun besitzen wir einen abstrakteren Zugang zu den Hilbertreihen. Nachdem eine Darstellung als rationale Funktion gefunden ist, betrachten wir ein paar der vorherigen Überlegungen unter dem Gesichtspunkt der Multigraduierung. Danach wenden wir uns einer Anzahl von Sätzen zu, welche die Berechnung einer Hilbertreihe eines Ideals erlauben. Die Darstellung folgt hierin im Wesentlichen [4].

LEMMA 3.1.1. *Sei $d \in \mathbb{N}^r$ ein fester Grad und G eine d-beschränkte Gröbnerbasis eines homogenen Ideals $I \subset k[X]$ bzgl. $W = \{W_1, ..., W_r\}$ einer Graduierungen auf $k[X]$, $f \in k[X]$ mit $deg_{W_j}(f) \leq d_j$ für alle $j = 1, .., r$, dann gilt*

$$f \in I \Longleftrightarrow \overline{f}^G = 0.$$

BEWEIS. Beim Beweis des analogen Satzes für einfache Gröbnerbasen $B = \{g_1, ..., g_s\}$ und $f \in I$ war grundlegend, dass der Rest r bei Division durch die Elemente der Gröbnerbasis selbst ein Element des Ideals war: $r := \overline{f}^B \in I$. Dies rührte daher, dass nach dem Divisionsalgorithmus kein Monom in r durch einen Leitterm von Elementen aus G teilbar war. Somit wäre $f = (\sum_{i=1}^{s} h_i g_i) + r \notin I$ ein Widerspruch.

Wie sieht das nun im multigraduierten Fall unserer beschränkten Gröbnerbasis G aus?
Da multigrad$(r) \leq$ multigrad$(f) \leq d$ ist, folgt dass $r \in I_{\leq d}$. Dies ergibt, dass die Monome von r durch die Leitterme der Elemente aus G geteilt werden müssen, denn den Divisionsalgorithmus selbst berührt die Graduierung nicht. Das bedeutet aber, dass $r = 0$ gilt.

Wenn andererseits der Divisionsrest $r = 0$ ist, so kann man f in der Form $f = \sum_{i=1}^{s} h_i g_i$ darstellen. Damit ist $f \in I$. ■

Auf die gleiche Weise müssen wir den Zusammenhang zwischen den Hilbertreihen eines Ideals und seinem Leitideal bzgl. einer Graduierung darstellen.

SATZ 3.1.2. ***Hilbertreihe und Gewichte*** [4, S.19]

Sei $I \subset k[X]$ ein homogenes Ideal bzgl. W einem Gewichtssystem mit $W = \{W_1, ..., W_r\}$, dann gilt

$$HS_I^W(t) = HS_{\langle LT(I)\rangle}^W(t).$$

Auf Grund dieses Satzes ist es nur nötig, die Hilbertreihe bezüglich monomialer Ideale zu berechnen. Den Kern der sukzessiven Berechnungen dieser Hilbertreihen stellt der Berechnungssatz dar. Für seinen Beweis aber stellen wir folgende Überlegungen voran, die sich auf Idealquotienten beziehen.

Analog zum Idealquotient $I : J$ definieren wir folgenden Quotienten:

$$I : x^\alpha := \{f \in k[X] \,|\, f \cdot x^\alpha \in I\} \supset I.$$

Wenn $f_1, f_2 \in I : x^\alpha$ ist, dann gilt $(f_i \cdot x^\alpha) \in I$ für $i = 1, 2$. Da I ein Ideal ist, folgt für die Addition $I \ni (f_1 \cdot x^\alpha) + (f_2 \cdot x^\alpha) = (f_1 + f_2) \cdot x^\alpha$, womit $(f_1 + f_2) \in I : x^\alpha$ ist. Dergleichen gilt für die Multiplikation mit $h \in k[X]$ $h \cdot (f_1 \cdot x^\alpha) \in I$, da I ein Ideal ist. Ferner ist $h \cdot (f_1 \cdot x^\alpha) = (h \cdot f_1) \cdot x^\alpha$ und damit ist $(h \cdot f_1) \in I : x^\alpha$. Das bedeutet aber, dass $I : x^\alpha$ ein Ideal ist.

BEISPIEL 3.1.3. Sei $I = \langle x^{(2,6)}, x^{(3,2)}\rangle \subset k[x, y]$ und $x^\alpha = x^{(1,3)} \notin I$, so ist $I \cap \langle x^\alpha\rangle = \langle x^{(2,6)}, x^{(3,3)}\rangle$. Für $x^\gamma \in I : x^\alpha$ gilt $x^\gamma \cdot x^\alpha = x^{\gamma+\alpha} \in I$.

Der Quotient hat die Form $I : x^{(1,3)} = \langle x^{(1,3)}, x^{(2,0)}\rangle$. Es gilt allgemein für ein monomiales Ideal $k[X] \ni I = \langle x^{\beta_i}\rangle_{i=1,\dots,s}$: $(I : x^\alpha) = \langle x^{\gamma_1}, \dots, x^{\gamma_s}\rangle$ mit $(\gamma_i)_j := (\beta_i)_j - (\alpha_i)_j$ falls die Differenz nicht negativ ist, sonst Null für alle $i = 1, \dots, s$ und $j = 1, \dots, n$ oder besser
$(\gamma_i)_j := \max((\beta_i)_j, (\alpha_i)_j) - (\alpha_i)_j$.

DEFINITION. Sei $f = \sum_{\alpha\in A} a_\alpha x^\alpha \in k[X]$, dann heißt $\mathrm{supp}(f) = \{\alpha \in \mathbb{Z}^n_{\geq 0} \,|\, a_\alpha \neq 0\}$ das **Newtonpolytop** von f oder einfach Polytop.

Mit Hilfe des Polytops lassen sich Polynome in einem n-dimensionalen Koordinatensystem, gleich den Koordinatenunterräumen des vorherigen Abschnitts, gut geometrisch darstellen.

LEMMA. *Sei $I \subset k[X]$ ein monomiales Ideal und $x^\alpha \in k[X]$, dann gilt*

$$I \cap \langle x^\alpha\rangle = x^\alpha \cdot (I : x^\alpha).$$

BEWEIS. Sei $f \in I \cap \langle x^\alpha\rangle$, dann hat f die Form $f = \sum_{i=1}^s h_i (x^\alpha)^i = x^\alpha \cdot h$ mit $h_i,\ h \in k[X]$ für alle i. Somit ist $h \in (I : x^\alpha)$ und $f \in x^\alpha \cdot (I : x^\alpha)$.

Ist andererseits $f \in x^\alpha \cdot (I : x^\alpha)$, so besitzt f die Form $f = x^\alpha \cdot h$ mit $x^\alpha \cdot h \in I$, da $h \in (I : x^\alpha)$. Daraus folgt $f \in I$ und $f \in \langle x^\alpha\rangle$. ■

Jetzt ist zu untersuchen, ob folgender Zusammenhang gilt:

LEMMA. *Sei $\langle x^{\beta_1}, \dots, x^{\beta_s}\rangle = I \subset k[X]$ ein monomiales Ideal und $x^\alpha \in k[X]\backslash I$, dann gilt*

$$\langle x^\alpha\rangle/(I \cap \langle x^\alpha\rangle) \simeq k[X]/(I : x^\alpha). \tag{3.1.1}$$

BEWEIS. Zuerst folgt aus dem vorherigen Lemma, dass

$$\langle x^\alpha\rangle/(I \cap \langle x^\alpha\rangle) \simeq \langle x^\alpha\rangle/x^\alpha \cdot (I : x^\alpha).$$

Sei $I^{-\alpha} := \langle x^{\widehat{\beta_i}}\rangle_{i=1,\dots,s}$ mit der koordinatenweisen Zuordnung $\widehat{(\beta)}_j = (\beta)_j - (\alpha)_j$, wenn $(\beta)_j - (\alpha)_j \geq 0$, sonst $\widehat{(\beta)}_j := 0$, für alle $j = 1, \dots, n$. (Dies ist geometrisch eine Verschiebung der Menge der Koordinatenunterräume in $\mathbb{Z}^n$ von I um den Vektor α zum Koordinatenursprung.) So gesehen ist

ja $I^{-\alpha} = I : x^\alpha$. Für den rechten Term in (3.1.1) gilt $k[X]/I^{-\alpha} = \{h + I^{-\alpha} \,|\, h \in k[X]\}$. Der linke lässt sich schreiben als

$$\begin{aligned}\langle x^\alpha\rangle/(x^\alpha \cdot I^{-\alpha}) &= \{x^\alpha \cdot h + (x^\alpha \cdot I^{-\alpha}) \,|\, h \in k[X]\} \\ &= \{x^\alpha \cdot (h + I^{-\alpha}) \,|\, h \in k[X]\} \\ &= \{x^\alpha \cdot g \,|\, g \in k[X]/I^{-\alpha}\}.\end{aligned}$$

Der Homomorphismus $\phi : g \to x^\alpha \cdot g$ kann geometrisch als Verschiebung des Polytops eines jeden $g \in k[X]/I^{-\alpha}$ um α gedeutet werden. Die linke Seite der Behauptung ist somit als "Verschiebung" der rechten Seite um α darstellbar. Da der kern$(\phi) = \{0\}$ ist, gilt die Behauptung. ■

Kommen wir nun zur letzten Beziehung zwischen Quotientenmoduln, die uns in diesem Zusammenhang interessiert.

LEMMA. *Sei $I \subset k[X]$ ein monomiales Ideal und $x^\alpha \in k[X]\backslash I$, dann gilt*

$$k[X]/(I \cap \langle x^\alpha\rangle) \simeq k[X]/\langle x^\alpha\rangle \oplus \langle x^\alpha\rangle/(I \cap \langle x^\alpha\rangle).$$

BEWEIS. Zuerst muss untersucht werden, ob die direkte Summe der rechten Seite gewährleistet ist - also die Eindeutigkeit der Darstellung. $k[X]/\langle x^\alpha\rangle$ kann ausgedrückt werden durch seine Äquivalenzklassen $k[X]/\langle x^\alpha\rangle = \{h + \langle x^\alpha\rangle \,|\, h \in k[X]\} =: \{[h]_1\}_{h\in k[X]}$ und stellt die Menge der Polynome im Komplement von $\langle x^\alpha\rangle$ dar, mit Ausnahme der Null.
Hingegen repräsentiert $\langle x^\alpha\rangle/(I \cap \langle x^\alpha\rangle) = \{g + (I \cap \langle x^\alpha\rangle) \,|\, g \in \langle x^\alpha\rangle\} =: \{[g]_2\}_{g\in\langle x^\alpha\rangle}$ eine bestimmte Menge in $\langle x^\alpha\rangle$ selbst. Das sind gerade die Polynome, die in $\langle x^\alpha\rangle$ aber nicht auch in I liegen. Sei nun

$$[h]_1 + [g]_2 = [h']_1 + [g']_2, \tag{3.1.2}$$

wobei $'+'$ kanonisch elementweise im Modul $k[X]$ definiert ist. Also folgt $[h]_1 - [h']_1 = [g']_2 - [g]_2$ mit $g, g' \in \langle x^\alpha\rangle$ und $h, h' \in k[X]\backslash(\langle x^\alpha\rangle\backslash\{0\})$ und für die Repräsentanten $[h-h']_1 = [g'-g]_2 = [g'']_2$ mit $g'' \in \langle x^\alpha\rangle$. Womit nur übrig bleibt, dass $h - h' = 0 \in k[X]$ und deswegen $g'' = 0 \in k[X]$. Das bedeutet, dass aus (3.1.2) $h = h'$ folgt und mit $g = g'$ die Eindeutigkeit der Darstellung. Deswegen kann man schreiben: $[h]_1 + [g]_2 =: [h + g]_3$.
Betrachten wir nun folgende Abbildung π:

$$\pi : k[X]/(I \cap \langle x^\alpha\rangle) \to k[X]/\langle x^\alpha\rangle \oplus \langle x^\alpha\rangle/(I \cap \langle x^\alpha\rangle)$$

mit $\pi([h]_{(I\cap\langle x^\alpha\rangle)}) = [h]_1 + [h]_2 = [h]_3$.
Für den Fall $h \in \langle x^\alpha\rangle - (\langle x^\alpha\rangle \cap I)$ ist $[h]_1 = [0]_1$ und $[h]_2 \neq [0]_2$ und somit $[h]$.
Sei $h \in (\langle x^\alpha\rangle \cap I)$, dann ist $[h]_1 = [0]_1$ und $[h]_2 = [0]_2$.
Für $h \in k[X] \setminus \langle x^\alpha\rangle$ folgt endlich $[h]_1 \neq [0]$ und $[h]_2 = [0]_2$.

Dies bedeutet aber, dass $[h]_1 + [h]_2 = [0]_1 + [0]_2$ genau dann, wenn $h \in (\langle x^\alpha\rangle \cap I)$ ist. Somit ist kern$(\pi) = (\langle x^\alpha\rangle \cap I)$ und wir erhalten vermöge π die Abbildung $[h] \mapsto [h]_3$ und somit die Behauptung. ■

Seien $A, B \subset_M M$ Untermoduln eines graduierten Moduls M bzgl. W mit einer direkten Summe $A \oplus B$. Für die jeweiligen linearen Unterräume gilt $H_i^W(A \oplus B) = H_i^W(A) \oplus H_i^W(B)$ und

$$\dim(H_i^W(A \oplus B)) = \dim(H_i^W(A)) + \dim(H_i^W(B)).$$

SATZ 3.1.4. ***Berechnungssatz*** [4, Lemma 1.2.3]

Sei $J \subset k[X]$ ein monomiales Ideal und $B = \{x^{\beta_i}\}_{i=1,...,l}$ ein minimales Erzeugendensystem für J. Ferner sei $x^\alpha \notin J$ so, dass $\{x^\alpha\} \cup B$ ein minimales Erzeugendensystem für $\langle x^\alpha, B\rangle =: I$ ist und $W = \{W_1, ..., W_r\}$ ein Gewichtssystem mit der Notation $W_i(\alpha) := deg_{W_i}(x^\alpha)$ für $i = 1, ..., r$ und $W(\alpha) := (W_1(\alpha), ..., W_r(\alpha))$.

Dann gilt:

(1) $\text{num}(\langle x^\alpha\rangle) = 1 - t^{W(\alpha)}$
(2) $\text{num}(\langle x^\alpha\rangle \cap J) = \text{num}(\langle x^\alpha\rangle) + \text{num}(J : x^\alpha) \cdot t^{W(\alpha)}$
(3) $\text{num}(I) = \text{num}(J) - \text{num}(J : x^\alpha) \cdot t^{W(\alpha)}$

BEWEIS. zu (1): Das Ideal hat die Form $\langle x^\alpha\rangle = \{x^\beta \in k[X] \,|\, \alpha + \gamma = \beta \,\text{mit}\, \gamma \in \mathbb{Z}^n_{\geq 0}\} = \{x^\gamma \cdot x^\alpha \,|\, \gamma \in \mathbb{Z}^n_{\geq 0}\}$. D. h., dieses monomiale Hauptideal ist als Menge von Koordinatenräumen darstellbar als der um $W(\alpha)$ verschobene gesamte Raum $k[X]$. Damit ergibt sich für die Dimensionen der Teilräume zum Grad $i \in \mathbb{Z}^r_{\geq 0}$

$$\begin{aligned} |\{x^\gamma \cdot x^\alpha \,|\, \gamma \in \mathbb{Z}^n_{\geq 0}\}| &= |\langle x^\alpha\rangle| \\ \dim(H^W_{i-W(\alpha)}(k[X])) &= \dim(H_i^W(\langle x^\alpha\rangle)) \end{aligned}$$

Sei hierzu vereinbart, dass $\dim(H_i^W(\cdot)) = 0$ ist, sobald ein Index j existiert mit $i_j < 0$. Die ist nötig, da ja auch Polynome gewichteter positiver Grade betrachtet werden.

Also kann man die Hilbertreihe auf die folgende Weise darstellen, da auch $W_j(\alpha) \geq \alpha_j$ für alle j:

$$\begin{aligned} HS^W_{\langle x^\alpha\rangle}(t) &= \sum_{i \in \mathbb{Z}^r_{\geq 0}} \dim(H_i^W(\langle x^\alpha\rangle)) \cdot t^i \\ &= \sum_{i \in \mathbb{Z}^r_{\geq 0}} \dim(H^W_{i-W(\alpha)}(k[X])) \cdot t^i \\ &= \sum_{i \in \mathbb{Z}^r_{\geq 0}} \dim(H_i^W(k[X])) \cdot t^{i+W(\alpha)} \\ &= t^{W(\alpha)} \cdot \sum_{i \in \mathbb{Z}^r_{\geq 0}} \dim(H_i^W(k[X])) \cdot t^i \\ &= t^{W(\alpha)} \cdot HS^W_{k[X]}(t). \end{aligned}$$

Für die Hilbertreihe des Quotientenmoduls gilt dementsprechend:

$$\begin{aligned} HS^W_{k[X]/\langle x^\alpha\rangle}(t) &= \sum_{i\in\mathbb{Z}^r_{\geq 0}} \dim(H^W_i(k[X]/\langle x^\alpha\rangle)) \cdot t^i \\ &= \sum_{i\in\mathbb{Z}^r_{\geq 0}} [\dim(H^W_i(k[X])) - \dim(H^W_{i-W(\alpha)}(k[X]))] \cdot t^i \\ &= \sum_{i\in\mathbb{Z}^r_{\geq 0}} \dim(H^W_i(k[X])) \cdot t^i - \sum_{i\in\mathbb{Z}^r_{\geq 0}} \dim(H^W_i(k[X])) \cdot t^{i+W(\alpha)} \\ &= (1-t^{W(\alpha)}) \cdot HS^W_{k[X]}(t) \\ \mathrm{num}(\langle x^\alpha\rangle) &= (1-t^{W(\alpha)}). \end{aligned}$$

zu (2): Aus den vorherigen Lemmata und der Unterraumbeziehung folgt:

$$\begin{aligned} HS^W_{k[X]/(J\cap\langle x^\alpha\rangle)}(t) &= HS^W_{k[X]/\langle x^\alpha\rangle}(t) + HS^W_{\langle x^\alpha\rangle/(J\cap\langle x^\alpha\rangle)}(t) \\ &= \mathrm{num}(\langle x^\alpha\rangle) \cdot HS^W_{k[X]}(t) + t^{W(\alpha)} \cdot HS^W_{k[X]/(J:x^\alpha)}(t) \\ &= \mathrm{num}(\langle x^\alpha\rangle) \cdot HS^W_{k[X]}(t) + \mathrm{num}(J:x^\alpha) t^{W(\alpha)} \cdot HS^W_{k[X]}(t) \\ \mathrm{num}(J\cap\langle x^\alpha\rangle) &= \mathrm{num}(\langle x^\alpha\rangle) + \mathrm{num}(J:x^\alpha) t^{W(\alpha)}. \end{aligned}$$

Nun wissen wir, dass in Lemma 3.1 eine Verschiebung bezüglich der Indizes beschrieben wird (bzw. der Grade der linearen Unterräume). Dort betrug diese Verschiebung α, da wir die natürliche Gewichtung N betrachteten. Währenddessen handelt es sich hier um eine Verschiebung bzgl. W, welche $W(\alpha)$ beträgt. Das bedeutet, dass $H^W_{i+W(\alpha)}(k[X]/(J:x^\alpha)) = H^W_i(\langle x^\alpha\rangle/(J\cap\langle x^\alpha\rangle))$ und daraus entsteht der zusätzliche Faktor $t^{W(\alpha)}$ in der Reihendarstellung.
zu 3) Folgende Aussage ermöglicht uns das sukzessive Berechnen der Hilbertreihe. Die Monome, welche nicht in $I = \langle J \cup \{x^\alpha\}\rangle$ liegen, liegen außerhalb von $\langle x^\alpha\rangle$ und J. Für die Berechnung ihrer Anzahl, muss man die Monome im Schnitt dieser beiden Ideale abziehen. Das bildet sich ab in den entsprechenden Hilbertreihen und es folgt die Beziehung ihrer Numeratoren:

$$\begin{aligned} \mathrm{num}(I) &= \mathrm{num}(\langle x^\alpha\rangle) + \mathrm{num}(J) - \mathrm{num}((J\cap\langle x^\alpha\rangle) \\ &= \mathrm{num}(J) + \mathrm{num}(\langle x^\alpha\rangle) - [\mathrm{num}(\langle x^\alpha\rangle) + \mathrm{num}(J:x^\alpha)\cdot t^{W(\alpha)}] \\ &= \mathrm{num}(J) - \mathrm{num}(J:x^\alpha)\cdot t^{W(\alpha)}. \end{aligned}$$

■

Auf Grund dieses Satzes lässt sich nun eine einfache Vorschrift finden, den Numerator einer Hilbertreihe zu berechnen.

KOROLLAR 3.1.5. *Sei* $I = \langle x^{\beta_i} \rangle_{i=1,...,s} \subset k[X]$, *dann gilt:*

$$num(I) = num(x^{\beta_1}) - \sum_{j=2}^{s} num(\langle x^{\beta_1}, ..., x^{\beta_{j-1}} \rangle : x^{\beta_j}) \cdot t^{W(\beta_j)}.$$

Zum konkreten Berechnen der Quotienten $J = \langle x^{\beta_1}, ..., x^{\beta_{j-1}} \rangle : x^{\beta_j}$ können wir nach Beispiel 3.1.3 vorgehen. Dabei sind die Generatoren von J gegeben durch $g_i := \frac{\text{LCM}(x^{\beta_j}, x^{\beta_i})}{x^{\beta_j}}$. Dabei ist der k-te Eintrag des Exponentenvektors des LCM gleich dem $\max(\beta_{ik}, \beta_{ik})$. Nun folgt ein Lemma, welches die Berechnung weiter vereinfacht.

LEMMA 3.1.6. ***Berechnung bei disjunkter Zerlegung*** [1, S. 43]

Sei $I \subset k[X]$ *ein monomiales Ideal. Angenommen die Variablen* x_i *lassen sich in disjunkte Mengen* X_j *so teilen,* $\bigsqcup_{j=0}^{l} X_j$, *dass jeder Generator von* I *in genau einem* $k[X_j]$ *liegt. Sei* $I_j := I \cap k[X_j]$. *Dann gilt:*

$$num(I) = \prod_{j=0}^{l} num(I_j).$$

BEWEIS. Die Tensorproduktzerlegung ist

$$k[X]/I = k[X_1]/I_1 \otimes \cdots \otimes k[X_l]/I_l.$$

Die Hilbertreihen sind mit diesem Tensorprodukt verträglich. ■

3.2. Berechnung von Gröbnerbasen mittels Hilbertreihen

Wie schon angedeutet, wollen wir über die Hilbertreihe strukturelle Informationen nutzten, umso als überflüssig erkannte Berechnungen zu vermeiden. Dazu brauchen wir aber noch den Zusammenhang zwischen den S-Polynomen bzw. den noch fehlenden Elementen der Gröbnerbasis eines bestimmten Grades und der Hilbertreihe.

3.2.1. Hilbertreihen bzgl. einem einzelnen Gewichtsvektor

LEMMA 3.2.1. ***Satz über Anzahl fehlender S-Polynome*** [4, S. 23]

Sei W *ein Gewichtsvektor, welcher ein Gewichtssystem bildet,* $F = \{f_1, ..., f_s\} \subset k[X]$ *homogen bzgl.* W *und* $I = \langle F \rangle$. *Ferner sei* $J = \langle LT(f_1), ..., LT(f_s) \rangle \subset \langle LT(I) \rangle$ *zu einer gegebenen Monomordnung* $>$. *Die jeweiligen Hilbertreihe sei gegeben durch*

$$\begin{aligned} HS^W_{k[X]/\langle LT(I) \rangle}(t) &= \sum_{i=0}^{\infty} a_i t^i \\ HS^W_{k[X]/J}(t) &= \sum_{i=0}^{\infty} b_i t^i. \end{aligned}$$

(1) Wenn nun für $i = 0, ..., d$ gilt $a_i = b_i$, dann ist F eine d-beschränkte Gröbnerbasis bzgl. W.
(2) So für $a_{d+1} < b_{d+1}$ gilt, dann gibt es keinen größeren Grad als d bzgl. W, für welches F eine solche Basis ist.
(3) Einer minimalen Gröbnerbasis von I fehlen zum Grad $d+1$ bzgl. W noch genau $b_{d+1} - a_{d+1}$ Elemente. Diese bilden das direkte Komplement zu $\sum_{i=1}^{s} H^W_{d-\deg_W(f_i)+1}(k[X]) \cdot f_i \subset H^W_{d+1}(I)$. (Das sind genau die schon durch F erzeugten Polynome aus I zum Grad d bzgl W.)

BEWEIS. zu (1): Da die LT(F) graduiert sind, ist Modul $S(F) \subset_M k[X]^s$ der Syzygien damit gleichfalls graduiert. Wir können ja eine Syzygie in ihre α-homogenen Komponenten eindeutig zerlegen. Dies gilt auch für die Multigraduierung, bei der man eine Syzygie S eindeutig schreiben kann als $S = \sum_{W(\alpha)} S_{W(\alpha)}$. Wenn $S \in S(F)$ und $\deg(S) \leq d$ ist, so heißt das $\deg(S \cdot F) \leq d$. Weil $a_i = b_i$ für $i \leq d$ ist, gilt für die lineare Teilräume $H^W_i(\langle \mathrm{LT}(I)\rangle) = H^W_i(J)$. Damit reduzieren sich alle diese Syzygien $\overline{S \cdot F}^F = 0$ und F ist zum Grad d eine beschränkte Gröbnerbasis.
zu (2): Sei nun der zu betrachtende Grad $d+1$ mit $b_{d+1} - a_{d+1} =: \delta > 0$. Es existieren also δ verschiedene Leitterme, die nicht in J liegen, aber in $\langle LT(I)\rangle$. Da diese fehlenden Elemente auch Elemente in allen höheren Unterräumen $H^W_i(\langle \mathrm{LT}(I)\rangle)$ mit $i > d$ erzeugen, z.B. bei Multiplikation mit Elementen aus $H^W_i(k[X])$ für beliebiges i. Damit gilt die Behauptung.
zu (3): Haben wir nun diese fehlenden δ Polynome mit den entsprechenden Leittermen gefunden, dann ist für den Grad $d+1$ wieder der Fall (1) eingetreten. ■

Was wir hier explizit ausnutzen ist, dass eine Gröbnerbasis gleichzeitig eine Basis des entsprechenden linearen Raumes darstellt. Suchen wir den kleinsten Grad, bei dem Differenzen der beiden Hilbertreihen auftreten, und berechnen weitere Elemente der Gröbnerbasis. Die Idee ist, den Grad zu erhöhen, wenn die beiden Hilbertreihen zu einem bestimmten Grad keine Differenz aufweisen. Dies tun wir solange, bis wir zum Fall (2) des vorherigen Lemmas gelangen, um dann zu diesem Grad die fehlenden Polynome zu suchen. Alle S-Polynome niederer Grade kann man von der Berechnung auf Grund obigen Lemmas ausschließen. Dieses Vorgehen kann man nun in folgendem Algorithmus sehen.

ALGORITHMUS 3.2.2. ***Modifizierter Buchbergeralgorithmus***

Input: W-homogene Erzeugenden-Menge $G = \{f_1, ..., f_s\}$ eines Ideals $I \subset k[X]$, $>$ eine Monomordnung auf $k[X]$, GB eine Gröbnerbasis zu I, die berechnete
Referenz-Hilbertreihe $HS^W_{k[X]/GB}(t) := \sum_{i=0}^{\infty} a_i t^i$, W ein Gewichtssystem
HT := HT(G);

$HS^W_{k[X]/G}(t) := \sum_{i=0}^{\infty} b_i t^i$;// Berechnen der temporären Hilbertreihe

if($HS^W_{k[X]/G}(t) = HS^W_{k[X]/GB}(t)$){break();} //wir haben schon unsere Gröbnerbasis

d := minimalDegree($HS^W_{k[X]/G}(t)$, $HS^W_{k[X]/GB}(t)$); // Bestimmen des kleinsten Grades, bei welchem Polynome zur Gröbnerbasis fehlen

$c := b_d - a_d$; // die Anzahl der fehlenden Polynome zum kleinsten Grad d

$P := \{(i, j) \mid i < j \wedge i, j = 1, ..., s \wedge \mathrm{LCM}_{f_i, f_j} > d\}$; // Löschen der entsprechenden kritischen Paare

P :=order(P); // Ordnen von P

p ist das erste Paar (i,j) aus P mit $p = (p_1, p_2)$;
while($P = \emptyset$)

{

$p := next(P)$;

if $(r = \overline{S(f_{p_1}, f_{p_2})}^{G} \neq 0)$

{

$G := G \cup \{r\}$;

$HT = HT \cup HT(r)$;

P :=addpairs(r, P); // neue Paare hinzufügen und ordnen

if($\deg^W(r) > d$)

{

// der Grad ist größer, also das nächste Paar

}else

{

// der Grad ist gleich, also die Anzahl korrigieren

$c := c - 1$;

if($c = 0$) // alle Fehlenden wurden gefunden

{

$HS^W_{k[X]/G}(t) = \sum_{i=0}^{\infty} b_i t^i$;// Berechnen der neuen temporären Hilbertreihe

if($HS^W_{k[X]/G}(t)$==$HS^W_{k[X]/GB}(t)$){break();} //wir haben nun unsere Gröbnerbasis

d := minimalDegree($HS^W_{k[X]/G}(t)$, $HS^W_{k[X]/GB}(t)$); // neuer kleinster Grad

$c := b_d - a_d$;

$P := \{(i, j) \mid i < j \wedge i, j = 1, ..., s \wedge \mathrm{LCM}_{f_i, f_j} > d\}$;

};

};

};};

3.2.2. Hilbertreihen bzgl. einem System von Gewichtsvektoren

Behandeln wir nun den Fall der Multigraduierung. Es wird vorausgesetzt, dass eine Menge von Gewichtsvektoren W existiert, die selbst kein Gewichtssystem sind, die aber ein Gewichtssystem enthalten.

SATZ 3.2.3. ***Reduktion des Gewichtssystems***

Sei $W = \{W_1, ..., W_r\}$ eine Menge von Gewichtsvektoren auf $k[X]$ derart, dass das Untersystem $(W_1, ..., W_s)$ minimale Länge besitzt (reduziert ist). Ferner sei $I \subset k[X]$ ein homogenes Ideal bzgl. W und die entsprechenden Hilbertreihen haben die Form

$$\begin{aligned} HS^{W}_{k[X]/I}(t) &= \sum_{i \in \mathbb{Z}^r_{\geq 0}} a_i t^i \\ HS^{W_1,...,W_s}_{k[X]/I}(t) &= \sum_{j \in \mathbb{Z}^s_{\geq 0}} b_j t^j. \end{aligned}$$

Dann haben die Koeffizienten bzgl. des reduzierten Gewichtssystems die Form

$$b_j = \sum_{i \in \mathbb{Z}^{r-s}_{\geq 0}} a_{(j,i)} \tag{3.2.1}$$

und die Reihe

$$HS^{W_1,...,W_s}_{k[X]/I}(t) = HS^{W}_{k[X]/I}(t_1, ..., t_s, 1, ..., 1).$$

BEWEIS. Ein einzelner Teilraum bezüglich der einzelnen Unbekannten zerlegt hat die Form

$$H_j^{W_1,...,W_s}(k[X]/I) = \sum_{i_{s+1}=0}^{\infty} \cdots \sum_{i_r=0}^{\infty} H^{W_1,...,W_s,W_{s+1},...,W_r}_{j,i_{s+1},...,i_r}(k[X]/I) \text{ für alle } j \in \mathbb{Z}^s_{\geq 0}. \tag{3.2.2}$$

Die einzelnen Teilräume bzgl. $(W_1, ..., W_s)$ werden bzgl. der restlichen $r - s$ Gewichtsvektoren in direkter Summe zerlegt. Da $(W_1, ..., W_s)$ ein Gewichtssystem ist, folgt, dass $H_j^{W_1,...,W_s}(k[X]/I)$ endlich dimensional ist (es existieren nur endlich viele Monome x^α mit $\text{multideg}_{W_1,...,W_s}(x^\alpha) = j$). Also ist für jedes obige j die Summenbildung der rechten Seiten endlicher Natur. Setzt man nun einfach als Koeffizienten der obigen beiden Reihen die Dimensionen der Teilräume ein:

$$\begin{aligned} b_j &= \dim(H_j^{W_1,...,W_s}(k[X]/I)) \\ a_{j,i} &= \dim(H^{W}_{j,i}(k[X]/I)), \end{aligned}$$

so folgt die Behauptung. Durch das 1-Setzen der Unbekannten $t_{s+1}, ..., t_r$werden die entsprechenden Unterräume $H_{j,i}$ nur zum Raum H_j gefaltet. ■

Jetzt wissen wir, wie man aus einer vorhandenen Hilbertreihe bzgl. eines Gewichtssystems die Reihe bzgl. eines reduzierten Systems einfach berechnet. Durch die Berechnung bezüglich des reduzierten Gewichtssystems kann man ebenfalls Rechenzeit sparen, weil schon hier erkannt werden kann, ab welchem Grad S-Polynome berechnet werden müssen oder nicht. Dann kann

man hieraus die entsprechenden Grade bezüglich des Gesamtsystems bestimmen.
Das folgende Theorem spiegelt nun schon die Grundzüge des erweiterten Algorithmus wider.

SATZ 3.2.4. ***Satz über die fehlenden S-Polynome*** *(Multigradversion)* [4, S.25]

Sei $W = \{W_1, ..., W_r\}$ eine Menge von Gewichtsvektoren auf $k[X]$ mit einem Untersystem $W' = (W_1, ..., W_S)$. Ferner sei $I \subset k[X]$ ein homogenes Ideal bzgl. W und von den W-homogen Elementen $F = \{f_1, ...f_m\}$ erzeugt. Zu einer gegebenen Monomordnung $>$ sei $J := \langle LT(f_1), ..., LT(f_m)\rangle \subset \langle LT(I)\rangle$. Die folgenden Hilbertreihen von J und $\langle LT(I)\rangle$ seien gegeben mit $t' := (t_1, ..., t_s)$ (und $t := (t_1, ..., t_r)$)

$$\begin{aligned} HS^{W}_{k[X]/\langle LT(I)\rangle}(t) &= \sum_{i\in\mathbb{Z}^r_{\geq 0}} c_i t^i \\ HS^{W}_{k[X]/J}(t) &= \sum_{i\in\mathbb{Z}^r_{\geq 0}} d_i t^i \\ HS^{W'}_{k[X]/\langle LT(I)\rangle}(t') &= \sum_{i\in\mathbb{Z}^s_{\geq 0}} a_i t^i \\ HS^{W'}_{k[X]/J}(t') &= \sum_{i\in\mathbb{Z}^s_{\geq 0}} b_i t^i. \end{aligned}$$

Sei $d \in \mathbb{Z}^s_{\geq 0}$ ein beliebiger aber fester Grad. Wenn für alle $i \leq d$ gilt, dass $a_i = b_i$, dann ist F eine d-beschränkte Gröbnerbasis von I bzgl. W' und $>$.

Sei nun $\delta \in \mathbb{Z}^s_{\geq 0}$ ein größerer Grad als d, dass $\forall i = 1, ..., s-1$ gilt: $\delta_i = d_i$ und $\delta_s = d_s + 1$. Wenn nun für $i \leq d$ gilt $a_i = b_i$ aber $a_\delta < b_\delta$, dann existiert eine endliche Anzahl von Graden $E = \{e \in \mathbb{Z}^{r-s}_{\geq 0}\}$ mit folgenden Eigenschaften.

(1) Es fehlen $b_\delta - a_\delta$ linear unabhängige Polynome vom Grad δ bzgl. W' , damit F eine δ-beschränkte Gröbnerbasis von I ist.
(2) Für jeden Grad $e \in E$ existieren $d_{\delta,e} - c_{\delta,e}$ linear unabhängige Polynome des Grades (δ, e) bzgl. W, damit F eine (δ, e)-beschränkte Gröbnerbasis von I ist.
(3) Angenommen die Gröbnerbasis enthält homogene Polynome bzgl. W. So besitzt jedes fehlende Polynom vom Grad δ einen Grad (δ, e) bzgl. W mit $e \in E$ und

$$b_\delta - a_\delta = \sum_{e\in E} d_{\delta,e} - c_{\delta,e}.$$

BEWEIS. Stimmen die Koeffizienten $a_i = b_i$ überein bis zu einem Grad d. So gilt ja, dass die Teilräume $H_i^{W'}(\langle \mathrm{LT}(I)\rangle) = H_i^{W'}(J)$ gleich sind für $i \leq d$. Daraus folgt, dass nach (3.2.2) $H_i^{W}(\langle \mathrm{LT}(I)\rangle) = H_i^{W}(J)$ gilt. Damit ist F sogar eine d-beschränkte Gröbnerbasis bzgl. W. ■

BEMERKUNG. Die bei Frau Gatermann vorgesehene zusätzliche Graduierung für die Beschränkung der Gröbnerbasis, bzw. der Gewichtung der Unbekannten, kann im Algorithmus leicht eingebaut werden. Sie ist in der Implementierung nicht enthalten. Auch ist eine Graduierung der

Monomordnung selbst als zusätzlicher Parameter nicht eingeführt. Diese kann aber dadurch angegeben werden, dass die Monomordnung vermöge einer Matrix übergeben wird.

Fazit

Um die verschiedenen Fälle des Laufzeitverhaltens des Algorithmus darzulegen, wurden entsprechende prototypische Tests ausgesucht. (Die Namen der Tests werden in Klammern vorangestellt und korrespondieren dabei mit den Mathematica-Testdateien.)

(SimplePositiveExample) Man sieht, dass die Hilbertreihenvariante 25 von 55 kritischen Paaren von der Berechnung ausschließt. Das bringt eine bessere Laufzeit von 0.69 sec gegenüber 1.301 sec.

(SecondPositiveExample) An diesem Beispiel erkennt man die mögliche doppelte Wirkungsweise des Ansatzes. Es werden nicht nur 10 von 36 kritischen Paaren ausgeschlossen. Der Algorithmus mit Hilbertreihen bricht die Berechnung auch insgesamt früher ab. So kommt die normale Berechnung mit 45 Paaren auf zusätzliche Reduktionsschritte.

(NegativeExample) Bei diesem Test erkennt man, dass die Hilbertreihen zwar helfen, 19 von 120 Paaren von der Berechnung auszuschließen. Aber die Zeit für die zusätzlichen Berechnungen, z.B. der temporären Hilbertreihen, heben diesen Vorteil wieder auf. Die Variante ohne Hilbertreihe ist mit 0.461 sec schneller als die 0.751 sec mit Hilbertreihenberechnung.

(BigSystem) Hier wird eine kompliziertere Gröbnerbasis berechnet. Von 3570 Paaren werden immerhin ganze 970 durch die Hilbertreihen ausgeschlossen.

Da der Algorithmus in der Interpretersprache von Mathematica geschrieben ist, ist er der internen Mathematica-Funktion selbstverständlich stark unterlegen und nicht vergleichbar. Außerdem finden beim vorliegenden Algorithmus außer den klassischen Kriterien nur die Hilbertreihe ihre Anwendung, während die interne Funktion sicher viel differenzierter vorgeht. Da ich für das Einbinden der Sugar-Strategie den Divisionsalgorithmus selbst implementiert habe und er der Hauptkonsument der Rechenzeit ist, gehen an dieser entscheidenden Stelle auch die Vorteile der schon vorhandenen internen Division verloren.

Allerdings wurde gerade hier offenbar, welche allgemeinen Probleme sich ergeben. So war ich einerseits damit konfrontiert, komplizierte Darstellungen der Null bei Koeffizienten aufzulösen, da dies Mathematica nicht immer automatisch gelingt. Weiterhin wurden die ganzzahligen Koeffizienten selbst schnell sehr groß und dies schien eine der Hauptbremsen bei der Berechnung zu sein.

Trotz dessen konnte mit den Beispielrechnungen gezeigt werden, dass bei günstiger Struktur des Problems (Polynomsystem und Graduierung), Vorteile bei der Berechnung zu erreichen sind. Es

wäre vielleicht weitergehend zu untersuchen, wie die Struktur des Problems mit der Güte der Verbesserung zusammenhängt. Es scheint so zu sein, dass dünn besetzte Polynome und insgesamt hohe Grade bessere Voraussetzungen sind, damit der Hilbertreihenansatz eine Verbesserung der Laufzeit bringt.

Anhang

Es folgt die Beschreibung der wichtigsten Funktionen der Implementation des Buchbergeralgorithmus. Eine vollständige Übersicht und Dokumentation befindet sich auf der beiliegenden CD in der Mathematica-Notebook-Datei 'HBuchberger.Documentation.nb'. Beispielrechnungen sind jeweils in einem eigenen Notebook gegeben. Die Implementierung selbst ist sowohl in Form von Nootebooks, als auch als Mathematica-Pakete gegeben.

HBuchberger

HBuchberger ist die Hauptfunktion des Buchbergeralgorithmus mit Hilbertreihenunterstützung. Die Funktion ist definiert mit *HBuchberger[P_,vars_, ord_,grads_,HSI_,indets_]*.

- P ist eine Menge von Polynomen $\{f_1, ..., f_s\}$. Zu dem von ihnen erzeugten Ideal $I \subset k[X]$ berechnet die Funktion eine reduzierte Gröbnerbasis. Wenn die Hilbertreihen benutzt werden sollen, dann ist es notwendig, dass diese Polynome homogen sind.
- vars gibt eine Menge von Symbolen an, die die Unbekannten des Polynomrings darstellen. Das wäre z.B. $X = \{x, y, z\}$.
- ord ist eine Monomordnung. Diese kann als Symbol angegeben werden, z.B. 'Lexicographic', 'DegreeLexicographic', 'DegreeReverseLexicographic'. Es besteht auch die Möglichkeit, eine Matrix als Repräsentant der Monomordnung zu übergeben. Bezüglich dieser Monomordnung werden die Leitterme bestimmt und die kritischen Paare geordnet.
- grads betrifft die Graduierung. Entweder man übergibt einen Vektor. Dieser muss dann für jede Unbekannte in X das Gewicht enthalten. Hier wäre die natürliche Gewichtung mit {1, 1, 1} für $\{x, y, z\}$ angegeben. Oder man übergibt eine Matrix, die mit der Anzahl der Variablen konform ist, z.B. auf obige 3 Unbekannte bezogen:
  {{1, 1, 1}, {1, 3, 4}, {2, 1, 5}, {2, 0, 3}}. Diese Graduierung wird ausschließlich bei der Hilbertreihenberechnung benutzt.
- HSI_ ist die übergebene Referenz-Hilbertreihe des Ideals I. Wird an ihrer Stelle keine Reihe übergeben, dann läuft der Algorithmus ohne die Hilbertreihenunterstützung und der Benutzer bekommt bei entsprechender Einstellung eine Warnung ausgegeben.
- indets ist eine Menge von Symbolen, bezüglich derer die Hilbertreihen gebildet werden. Hat man r Gewichtsvektoren, dann muss man hier ebenfalls r Symbole übergeben. Im Standardfall ist das $\{\lambda_1, ..., \lambda_r\}$.

ReducePolynomial

Der Divisionsalgorithmus musste neu implementiert werden, um die Sugar-Berecnungen der S-Polynome zu integrieren: *ReducePolynomial[SPoly_,lowest_, i_, j_ , G_, LTList_, SugarList_, PairSugarList_, vars_ ,ord_].*

Das gegebene S-Polynom SPoly wird durch die Elemente der Polynommenge G reduziert. Die Indizes *i* und *j* sind die Indizes der Elemente aus *G*, aus denen das gegebene S-Polynom gebildet wurde. Der Parameter lowest ist der kleinste Leitterm ohne Koeffizient der Polynome aus *G*.

Innerhalb des Divisionsalgorithmus wird der Sugar neu berechnet und der kleinste LT beachtet. D. h., ein Schritt wird nicht ausgeführt, wenn der aktuelle LT kleiner gleich dem Kleinsten (lowest) ist.

Zurückgegeben wird eine Liste. Diese enthält die Liste der Koeffizienten entsprechend der Elemente in *G*, den möglichen Rest der Division dividiert durch seinen Content, den Sugar dieses Restes und den Content selbst.

ReducePolynomial

SPolynomial[G_, i_, j_, LTList_, PairLCMList_, vars_] gibt das S-Polynom des *i*-ten und des *j*-ten Elementes in *G* zurück.

ReduceBase

ReduceBase[P_,LTList_,RedundantList_, vars_]

Eine gegebene Gröbnerbasis *P* wird über eine minimale in eine reduzierte Gröbnerbasis transformiert. RedundantList sammelt schon während der Berechnungen die Indizes in *P*, deren zugehörige Elemente aus *P* für die Transformation überhaupt in Frage kommen.

HilbertSeriesNumerator

HilbertSeriesNumerator[M_,vars_,grads_,indets_,deep_]

Der Numerator der Hilbertreihe des Ideals $\langle M \rangle$ wird sukzessiv berechnet. Diese Funktion ruft sich selbst auf. Intern wird für jede Quotientenmodulberechnung ReduceBase aufgerufen. Über die Funktion GetLinearMonomials werden die linearen Monome beachtet.

HilbertSeries

HilbertSeries[M_,vars_,grads_,indets_]

Berechnet die Hilbertreihe des Ideals $\langle M \rangle$ mit M einer Menge von Polynomen in $k[X]$ mit den Unbekannten der Potenzreihe aus der Menge idets. Die Menge der Unbkannten X wird wieder

im Parameter vars übergeben. Wird keine Graduierung übergeben, so wird implizit die natürliche angenommen. Wenn die Monome den ganzen Ring $k[X]$ aufspannen, die Graduierung kein Gewichtssystem ist oder die Anzahl der Unbekannte aus indets entspricht nicht dem Gewichtssystem, dann wird die Berechnung abgebrochen.

Literaturverzeichnis

[1] D. Bayer and M. Stillman: *Computation of Hilbert Functions*, J. Symb. Comp. 14:31-50, 1992.

[2] Bronstein, Semendjajew: *Taschenbuch der Mathematik*, Teubner, 1991.

[3] D. Cox, J. Little, D. O'Shea: *Ideal, Varieties und Algorithms, An Introduction to Computational Algebraic Geometrie and Commutativ Algebra,* Springer, 2nd edition, 1998.

[4] K. Gatermann: *Computer Algebra Methods for Equivariant Dynamical Systems,* Lecture Notes in Mathematics No.:1728, 2000.

[5] K. Gatermann: *The moregroebner Package Version 3.2 an improvement of grobner package* (Maple), Konrad-Zuse-Zentrum für Informationstechnik Berlin, *http://www.zib.de.*

[6] Ernst Kunz: *Einführung in die Algebraische Geometrie*, vieweg studium,1997.

[7] H. Matsamura: *Commutative Ring Theorie*, Cambridge University Press, 1986.

[8] Wolfram Koepf: Gröbner bases and triangles, *International Journal of Computer Algebra in Mathematics Education*, 4:371-386, 1997.

[9] Wolfram Research, Mathematica 4.1 Dokumentation.

Ich versichere hiermit, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Hendrik Spiewok, Kassel, 2006