1 Einleitung

In dieser Diplomarbeit beschäftigen wir uns mit der algorithmischen Primärzerlegung von Idealen in $\mathbb{Z}[x_1, ..., x_n]$. Primärzerlegungen von Idealen sind das Analogon zu Primfaktorzerlegungen von einzelnen Zahlen. Jedes Ideal in einem Noetherschen Ring kann so als Schnitt von endlich vielen Primäridealen, das sind Verallgemeinerungen von Primidealen, dargestellt werden.
Die Radikale der gesuchten Primärideale sind die zu dem zu zerlegenden Ideal assoziierten Primideale und werden dessen Komponenten genannt. Ein Primideal P eines Noetherschen Ringes R heißt zu einem Ideal $I \subset R$ assoziiert, falls es ein $r \in R$ gibt mit $P = (I : \langle r \rangle)$. Nach der ursprünglichen Definition eines zu einem Modul assoziierten Primideals müsste man hier I durch R/I ersetzen und das assoziierte Primideal ist dann der Annulator eines Elementes aus R/I. Wir beschränken uns hier jedoch auf die Zerlegung von Idealen und brauchen Moduln nur als Werkzeuge dazu.
Wenn man in einem Polynomring über $\mathbb{Z}$ arbeitet, so gibt es zwei Herangehensweisen an die algorithmische Umsetzung einer Primärzerlegung. Ein Ideal, welches keine Elemnte aus $\mathbb{Z}$ enthält zerlegt man mit Hilfe einer Erweiterung nach dem Polynomring über $\mathbb{Q}$. Enthält ein Ideal Elemnte aus $\mathbb{Z}$, so wird es zuerst in den Schnitt weiterer Ideale verfeinert, die jeweils nur eine Potenz einer einzigen Primzahl enthalten. Bei diesen beginnt man dann damit die 0-dimensionalen assoziierten Primideale zu suchen und dann die höher dimensionalen. Das ist der aufwändigste Teil der ganzen Konstruktion. Er läuft über eine Lokalisierung nach dem multiplikativen System der Elemente $\not\equiv 0$ modulo der jeweiligen Primzahl p in $\mathbb{Z}[x]$. Hierbei ist x eine der Variablen $x_1, \ldots, x_n$. Der nächste Schritt ist dann die Konstruktion der zu diesen Primidealen korrespondierenden Primärideale.
In einem Polynomring über einem Körper ist es wesentlich einfacher. Dort kann man direkt über eine univariate Faktorisierung und einen geeigneten Koordinatenwechsel die gesuchten Primärideale konstruieren.

Bei der Performance von Algorithmen für Polynome mit Koeffizienten aus Ringen tauchen am häufigsten Schwierigkeiten bei Faktorisierungen auf. A. Seidenberg hat mittels Vergleich von Quotienten $(I : p_i)$ und I für gewisse Primzahlen p_i eine geeignete ganze Zahl $(p_1 \cdots p_k)^\varrho$, $\varrho \in \mathbb{N}$ konstruiert, deren Faktorisierung man dann schon kennt.
Primärzerlegungen sind nicht eindeutig, meist hat ein Ideal mehrere Zerlegungen. Bei einer irredundanten Primärzerlegung bleibt die Anzahl der Komponenten jedoch immer gleich und entspricht der Anzahl der zu dem Ideal I assoziierten Primideale.
Primärzerlegungen von Idealen sind in vielerlei Hinsicht interessant, da viele Eigenschaften von I zu seinen Komponenten korrespondieren. Oft ist es einfach viel übersichtlicher, die Zerlegung eines Ideals zu betrachten, wie

folgendes Beispiel aus *An Introduction to Gröbner Bases* von G-M. Greuel und G. Pfister demonstriert:

$$\mathbb{Z}[x] \supset I = \langle 45, 5x+10, x^3+6x^2+20x+15\rangle = \langle 9, x+2\rangle \cap \langle 5, x^2\rangle \cap \langle 5, x+1\rangle$$

Manchmal jedoch erscheint eine algebraisch betrachtete Zerlegung erst einmal komplizierter als das ursprüngliche Ideal und die Vereinfachung wird erst bei der geometrischen Betrachtung der Komponenten klar. Denn man kann sich auf der geometrischen Seite die Nullstellenmenge

$$V(I) = \{P \subset R : P \quad \text{Primideal und} \quad P \supset I\}$$

eines Ideals I als Vereinigung der Nullstellenmengen der Primärideale vorstellen. Diese Nullstellenmengen sind irreduzibel, denn für ein Primärideal Q ist $\sqrt{Q}$ ein Primideal.
Primärzerlegungen sind aber auch in der Kodierungstheorie nützlich. Betrachten wir zum Beispiel Primärideale $Q_1, \ldots, Q_S$, deren Erzeuger benutzt werden um Daten zu kodieren, und I sei deren Schnitt. Wenn wir nun annehmen, dass manche dieser Primärideale vergleichbare Radikale habe, mit anderen Worten soll I eingebette Komponenten haben, dann kann ein Primärzerlegungsprozess unter Umständen nicht alle Q_i entdecken, weil das jeweils von der Art des Zerlegungsprozesses abhängt. So kann man Daten vor denjenigen verstecken, die diesen Prozess nicht kennen.
Die konkrete Umsetzung der Konstruktionen wird mittlerweile mit Hilfe von Gröbner Basen gemacht, die sich dadurch auszeichnen, dass deren Leitideal, das heisst das Ideal der Leitterme, gleich dem Leitideal des tatsächlichen Ideals ist. Das gilt nicht für beliebige Erzeugendensysteme eines Ideals und ist eine Eigenschaft, die viele Algorithmen vereinfachen kann. A.Seidenberg hat 1974 noch ohne deren Hilfe gearbeitet. Obwohl er im Artikel *What is Noetherian?* auch schon den Begriff eines Leitideals im Sinne eines Ideals der Leitkoeffizienten eingeführt hat.
Sobald man von Leitkoeffizienten, -termen oder -exponenten spricht, wird klar, dass man erst mal eine Ordnung für die Terme eines Polynoms festlegen muss. Sonst sind diese Begriffe nicht wohldefiniert. Auf die genaue Ausführung solcher Ordnungen werden wir hier verzichten, wollen aber erwähnen, dass sie immer global sein müssen. In einigen Beispielen werden sie trotzdem angesprochen.
Da viele grundlegende Konstruktionen, die für unser Problem gebraucht werden schon in Singular implementiert sind, werden wir nicht immer auf die resultierenden Unterschiede der in den Konstruktionen benutzten Basen eingehen.

Für polynomiale Ringe über Körpern wurde das Problem der Berechnung einer solchen Zerlegung schon gelöst und die entsprechenden Algorithmen sind in Singular in der Bibliothek "primdec.lib" implementiert. Die Vorgehensweise in diesen Fällen werden wir im Kapitel 3.1 darstellen. Die im

arithmetischen Fall auftretenden Unterschiede werden dann im Kapitel 3.2 ausführlich beschrieben.

2 Theoretische Grundlagen

In diesem Kapitel werden die algebraischen Grundlagen für die kontruktivistische Primärzerlegung eines Ideals I eines Noetherschen Ringes R, speziell auch für $R = \mathbb{Z}$, erläutert. Da unser Interesse dem Polynomring über den ganzen Zahlen gehört, können wir uns sogar auf einen Ring $R[x_1, \ldots, x_n]$, mit R faktorieller Hauptidealring, konzentrieren.
Teilweise verzichten wir auf Beweise und verweisen stattdessen auf die Quellen.
Ringe werden jeweils als kommutativ mit 1 vorausgesetzt.
Zuerst betrachten wir für ein Ideal I in einem Polynomring $A = R[x_1, \ldots, x_n]$ die Zerlegung seines Radikals $\sqrt{I} = \{f \in A : f^r \in I \text{ für ein } r \in \mathbb{N}\}$.

Lemma 1 (AL94, Lemma 4.6.2) *Sei I ein Ideal in einem Noetherschen Ring A. Dann können wir das Radikal von I wie folgt darstellen:*

$$\sqrt{I} = \bigcap_{I \subset P} P, \quad P \quad \textit{Primideal}$$

Beweis: Dass auch $\sqrt{I}$ im Schnitt dieser Primideale enthalten ist, folgt daraus, dass in jedem Primideal, das I enthält auch $\sqrt{I}$ enthalten ist. Nun betrachten wir die andere Inklusion unter folgender Annahme:
Es gibt ein $f \in \bigcap_{I \subset P} P - \sqrt{I}$. Wir setzen $S := \{f^r : r \in \mathbb{N}_0\}$. $S \cap \sqrt{I} = \emptyset$, denn ist $f^r \in \sqrt{I}$ für ein $r \in \mathbb{N}$, so ist $f^{rs} \in I$ für ein $s \in \mathbb{N}$ und somit $f \in \sqrt{I}$.
Betrachte nun die Menge $\mathfrak{M}$ der Ideale in A, die $\sqrt{I}$ enthalten und mit S leeren Schnitt haben. $\sqrt{I} \in \mathfrak{M}$, also ist $\mathfrak{M}$ nicht leer und hat ein maximales Element M. $\sqrt{I} \subset M$ und $M \cap S = \emptyset$ und ausserdem ist M ein Primideal: Sei $gh \in M$ aber weder g noch h seien in M. Wegen der Maximalität von M gilt $\langle g, M\rangle \cap S \neq \emptyset$ und $\langle h, M\rangle \cap S \neq \emptyset$ Deswegen gibt es $r, r' \in \mathbb{N}$, $m, m' \in M$ und $a, a' \in A$ so dass gilt

$$ag + m = f^r \quad \text{und} \quad a'h + m' = f^{r'}$$

Aber dann ist

$$\underbrace{f^{r+r'}}_{\in S} = (ag + m)(a'h + m') = (aa')\underbrace{(gh)}_{\in M} + \underbrace{(ag + m)m' + (a'h)m}_{\in M} \in M \cap S$$

was ein Widerspruch zur Annahme ist. Also ist M ein Primideal, das $\sqrt{I}$ und somit auch I enthält. Somit ist $f \in \bigcap_{I \subset P} P \subset M$ laut Annahme, was ein Widerspruch zu $M \cap S = \emptyset$ ist.

q.e.d.

Geht man von der Primfaktorzerlegung einer Zahl in einem faktoriellen Ring aus, so könnte man nun auf die Idee kommen, dass im Falle eines Ideals in dessen Zerlegung Potenzen von Primidealen auftreten. Dem ist aber nicht so, wie folgendes Beispiel demonstriert:

Beispiel 1
Betrachten wir $Q = \langle 9, x^2 \rangle$ in $\mathbb{Z}[x]$. Jedes Primdeal, das Q enthält muss 3 und x enthalten und ist somit gleich $M = \langle 3, x \rangle$, da M ein maximales Ideal ist. $\mathbb{Z}[x]\ M = \mathbb{Z}_3$). Aber $M^3 \not\subset Q \not\subset M^2$, also kann Q keine Potenz eines Primideals sein.

Das korrekte Analogon zu einer Potenz einer Primzahl ist ein Primärideal:

Definition 2 (GP07, Def. 4.1.1.) *(1) Ein Ideal Q eines Ringes A heisst Primärideal, falls für $ab \in Q$ und $a \notin Q$ $b \in \sqrt{Q}$ liegt.*

(2) Ein Ideal Q eines Ringes A heisst P-primär, wenn $\sqrt{Q} = P$ ist für ein Primideal P.

Primideale sind natürlich auch Primärideale, aber Potenzen von Primidealen sind nicht immer Primärideale.

Beispiel 2 Wir betrachten den Ring $A = \mathbb{Z}[x, y, z]/\langle xy - z^2 \rangle$. Das Ideal $P = \langle x, z \rangle$ ist ein Primideal in A, denn $A/P = \mathbb{Z}[y]$ ist ein Integritätsbereich. Aber P^2 ist nicht primär, da $xy = z^2 \in P^2$ ist, aber $x \notin P^2$ und auch keine Potenz von y ist in P^2 enthalten.

Potenzen von maximalen Idealen sind jedoch immer primär, wie folgendes Lemma zeigt:

Lemma 3 (AL94, Lemma 4.6.13.) *Sei A ein Noetherscher Ring und M ein maximales Ideal von A. Sei $Q \subseteq M$ ein Ideal und für jedes $m \in M$ existiere ein $\nu \in \mathbb{N}$, so dass $m^\nu \in Q$ ist. Dann ist Q ein M-primäres Ideal.*

Beweis: M ist ein Primideal und Q ist darin enthalten, also ist $\sqrt{Q} \subseteq M$. Haben wir ein $m \in M$, so ist $m \in \sqrt{Q}$, da nach Vorraussetzung eine Potenz von m in Q ist. Somit ist $\sqrt{Q} = M$.
Es bleibt zu zeigen, dass Q primär ist: Sei $fg \in Q$ und $f \notin Q$. Wir nehmen an, dass g nicht in M ist. Dann gibt es wegen der Maximalität von M ein $h \in A$ und ein $m \in M$ so dass $hg + m = 1$. Sei $\nu \in \mathbb{N}$ so dass $m^\nu \in Q$ ist. Dann gilt

$$1 = 1^\nu = (hg + m)^\nu = h'g + m^\nu,$$

für ein $h' \in A$. So können wir schreiben $f = h' \underbrace{gf}_{\in Q} + \underbrace{m^\nu}_{\in Q} f \in Q$, was ein Widerspruch zu $f \notin Q$ ist.

q.e.d.

Bei der Konstruktion der Primärideale, nachdem man die zu einem Ideal assoziierten Primideale gefunden hat, ist diese Tatsache nützlich. Umgekehrt sind Radikale von Primäridealen jedoch immer Primideale:

Lemma 4 *(GP07, Lemma 4.1.3.)*

(1) Das Radikal eines Primärideals Q ist ein Primideal.

(2) Seien Q, Q' P-primäre Ideale. Dann ist $Q \cap Q'$ auch ein P-primäres Ideal.

Beweis:

Zu (1): Sei $a \cdot b \in \sqrt{Q}$. Dann ist $(ab)^r = a^r b^r \in Q$ Für ein $r \in \mathbb{N}$.
Also ist $a^r \in Q$ oder $b^{rs} \in Q$ für $r, s \in \mathbb{N}$ woraus folgt, dass $a \in Q$ oder $b \in Q$.

Zu (2): Sei $a \in \sqrt{Q \cap Q'}$. Dann gibt es ein $r \in \mathbb{N}$ mit $a^r \in Q \cap Q'$, woraus folgt, dass $a^r \in Q$ und $a^r \in Q'$.
Also ist $a \in \sqrt{Q} = P$ und $a \in \sqrt{Q'} = P$.

q.e.d.

Primärideale sind nicht immer irreduzibel, aber jedes irreduzible Ideal ist primär. Zum Beispiel ist in für einen Ring R in $R[x, y]$ das Ideal $Q = \langle x^2, xy, y^2 \rangle = \langle x^2, y \rangle \cap \langle x, y^2 \rangle$ ein reduzibles Primärideal. Aber die beiden rechten Ideale sind irreduzibel. Man erreicht eine Zerlegung in irreduzible Primärideale, indem man bei deren Konstruktion mit Quotienten arbeitet. Nun können wir definieren, was eine Primärzerlegung eines Ideals in einem Noetherschen Ring ist:

Definition 5 (AL94, Kap.4.6, Def. 4.6.8,Seite 261) *Sei $I = \bigcap_{i=1}^r Q_i$ wobei die Q_i P_i-primär seien für Primideale P_i. Wir nennen $\bigcap_{i=1}^r Q_i$ eine Primärzerlegung von I.*
Sind die P_i zusätzlich paarweise verschieden und ist $\bigcap_{i \neq j} Q_j \not\subset Q_i$, so nennen wir die Primärzerlegung irredundant. In diesem Fall heissen die Q_i die zu den P_i korrespondierenden primären Komponenten von I und die P_i heissen die Primkomponenten von I.

Hat man eine Primärzerlegung eines Ideals, so erhält man mit Punkt (2) vom letzten Lemma eine irredundante Primärzerlegung, indem man Primärideale mit gleichem Radikal durch deren Schnitt ersetzt. Dass jedes Ideal in einem Noetherschen Ring eine irredundante Primärzerlegung besitzt ist die Aussage des nächsten Theorems.

Theorem 6 (GP07, Theorem 4.1.4.) *Jedes echte Ideal I eines Noetherschen Ringes R besitzt eine irredundante Primärzerlegung*

$$I = Q_1 \cap \ldots \cap Q_s$$

in Primärideale Q_i, $i = 1, \cdots, s$ mit paarweise verschiedenen $\sqrt{Q_i}$ und kein Q_i enthält den Schnitt der anderen Q_j.

Beweis: Wegen dem Punkt (2) im letzten Lemma reicht es zu zeigen, dass jedes Ideal eines Noetherschen Ringes der Schnitt von endlich vielen Primäridealen ist.
Unter der Annahme, dass die Aussage nicht stimmt sei $\mathfrak{M}$ die Menge der Ideale, die kein Schnitt endlich vieler Primärideale sind.
R ist noethersch und $\mathfrak{M}$ hat ein maximales Element I bezüglich der Inklusion. Da I nicht primär ist, gibt es $a, b \in R$ mit $ab \in I$, $a \notin I$ und $b^r \notin I$ für alle $r \in \mathbb{N}$.
Betrachte nun die aufsteigende Kette von Idealen

$$(I : \langle b \rangle) \subset (I : \langle b^2 \rangle) \subset \cdots$$

Da R noethersch ist, gibt es ein $r \in \mathbb{N}$ mit $(I : \langle b^r \rangle) = (I : \langle b^{r+1} \rangle) = \cdots$.
Mit Lemma 3.3.6 aus [GP07, Kap.3.3] folgt, dass $I = (I : \langle b^r \rangle) \cap (I, b^r)$. Da $b^r \notin I$, ist $I \subseteq (I, b^r)$. Und da $a \notin I$ aber $ab^r \in I$ liegt, ist $I \subseteq (I : \langle b^r \rangle)$.
I ist maximal in $\mathfrak{M}$, also sind beide Ideale Schnitte von endlich vielen Primäridealen und somit ist auch I Schnitt von endlich vielen Primäridealen.

q.e.d.

Bemerkung 7 *In anderen Ringen können Ideale durchaus Schnitte von unendlich vielen Primäridealen sein. Betrachten wir zum Beispiel das Ideal $I = \langle x_1 x_2 \cdots \rangle = \langle x_1 \rangle \cap \langle x_2 \rangle \cdots$ im Polynomring $R[x_1, x_2, \ldots]$ in unendlich vielen Variablen.*

Da wir nun die theoretischen Grundlagen zur Existenz von Primärzerlegungen gesehen haben, wollen wir uns deren Konstruktion zuwenden. Im Text beschäftigen wir uns mit mit der algorithmischen Theorie und deren algorithmischer Umsetzung. Die Algorithmen werden in Pseudocode vereinfacht dargestellt.

3 Algorithmische Umsetzungen

Was uns nun interessiert, ist die algorithmische Umsetzung der Primärzerlegung eines Ideals I. Wir haben gesehen, dass wir es in Noetherschen Ringen dabei mit einer endlichen Anzahl von Primäridealen zu tun haben. Da die Grundlagen aus den Ergebnissen in Polynomringen über Körpern stammen, wenden wir uns zuerst der algorithmischen Umsetzung einer Primärzerlegung in $k[x_1, \ldots, x_n]$ zu. Hierbei ist k ein Körper der Charakteristik 0 oder genügend große p. Im arithmetischen Fall nutzen wir dann, was schon bekannt ist und nehmen Lokalisierungen und Homomorphismen zwischen $\mathbb{Z}[x_1, \ldots, x_n]$ und $k[x_1, \ldots, x_n]$, $k = \mathbb{Q}$ oder $k = \mathbb{Z}/p$ für eine Primzahl p zur Hilfe. Betrachten wir einen Homomorphismus zwischen zwei Ringen, so ist die Kontraktion eines Primideals dann immer auch ein Primideal in $\mathbb{Z}[x_1, \ldots, x_n]$, weswegen wir dann die mod p-irreduziblen Elemente suchen.

3.1 Primärzerlegung eines Ideals in $k[x_1, \ldots, x_n]$

Wir beschränken uns auf Noethersche Ringe und betrachten eine Primärzerlegung $I = \cap_{i=1}^{s} Q_i$ in P_i-primäre Ideale Q_i, wobei die P_i genau die zu I assoziierten Primideale sind. Dass das Ergebnis nicht eindeutig sein muss sieht man zum Beispiel bei der Zerlegung des Ideals $I = \langle x^2, xy \rangle \subset k[x, y]$ in $\langle x \rangle \cap \langle x^2, xy, y^2 \rangle$ oder in $\langle x \rangle \cap \langle x^2, y \rangle$. Die zu I assoziierten Primideale sind $\langle x \rangle$ und $\langle x, y \rangle$, wobei $\langle x, y \rangle$ zu $\langle x^2, y \rangle$ und zu $\langle x^2, xy, y^2 \rangle$ korrespondiert. Beide Zerlegungen sind irredundant.
Es gibt zwei wesentliche Vereinfachungen der Situation, die uns schrittweise zum Ziel führen. Die erste ist die Betrachtung eines nulldimensionalen Ideals, bei dem wir dann durch eine univariate Faktorisierung die gesuchten Primärideale finden.

3.1.1 Der nulldimensionale Fall

Wir gehen von einem Körper k der Charakteristik 0 aus und betrachten ein nulldimensionales Ideal I im Polynomring über k in einer Variablen. Wir haben es mit einem faktoriellen Hauptidealring zu tun und können jedes Ideal I als Hauptideal $\langle f \rangle = \langle f_1^{r_1} \cdots f_r^{n_r} \rangle$ eines Polynoms darstellen. Dann ist die Primärzerlegung von I gegeben durch

$$I = \bigcap_{i=1}^{r} \langle f_i \rangle^{r_i}$$

Bei polynomialen Idealen über k in mehreren Variablen benutzen wir nach einem geeigneten Koordinatenwechsel die univariate Faktorisierung eines Polynoms und nehmen erst einmal an, dass I nulldimensional ist. Alle

zu I assoziierten Primideale müssen dann maximal sein. Für die univariate Faktorisierung eines Polynoms brauchen wir den Begriff eines *Ideals in allgemeiner Lage*.

Definition 8 (GP07, Def. 4.2.1.) *(1) Sei $M \subset k[x_1, \cdots, x_n]$ ein maximales Ideal. M heisst in allgemeiner Lage bezüglich der Lexikografischen Ordnung mit $x_1 > \cdots > x_n$, falls es $g_1, \ldots, g_n \in k[x_n]$ gibt mit*

$$M = \langle x_1 + g_1(x_n), \ldots, x_{n-1} + g_{n-1}(x_n), g_n(x_n) \rangle$$

.

(2) Ein nulldimensionales Ideal $I \subset k[x_1, \ldots, x_n]$ heisst in allgemeiner Lage bezüglich der Lexikografischen Ordnung mit $x_1 > \cdots > x_n$, falls alle seine assoziierten Primideale P_i in allgemeiner Lage sind und falls $P_i \cap k[x_n] \neq P_j \cap k[x_n]$ für $i \neq j$.

Wir können jedes beliebige Ideal mit einem passenden Koordinatenwechsel in allgemeine Lage bringen. Wenn wir ein $\underline{a} = (a_1, \ldots, a_{n-1}) \in k^{n-1}$ wählen, so macht das z.B. der generische lineare Koordinatenwechsel

$\varphi_{\underline{a}} : k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$
$\varphi_{\underline{a}}(x_i) = x_i, \quad i = 1, \cdots, n-1$
$\varphi_{\underline{a}}(x_n) = x_n + \sum_{i=1}^{n-1} a_i x_i$

Für den Beweis dazu verweisen wir auf GP07, Proposition 4.2.2.

Ist ein nulldimensionales Ideal I in allgemeiner Lage, so betrachten wir $I \cap k[x_n] = \langle g \rangle$ und faktorisieren $g = g_1^{r_1} \cdots g_s^{r_s}$ mit monischen Primelementen und $g_i \neq g_j$ für $i \neq j$. Dann ist $I = \cap_{i=1}^{s} \langle I, g_i^{r_i} \rangle$ und die $\langle I, g_i^{r_i} \rangle$ sind Primärideale für alle i. In GP07, Proposition 4.2.3 können die Einzelheiten dazu nachgelesen werden.
Das $\underline{a}$ kann unter Umständen schlecht gewählt sein, deswegen muss für die $\langle I, g_i^{r_i} \rangle$ jeweils noch ein Primärtest durchgeführt werden. Es gibt 3 äquivalente Kriterien eines Ideals in allgemeiner Lage, die für die algorithmische Umsetzung dessen Zerlegung nützlich sind. Sie sind die Basis für einen Primärtest eines nulldimensionalen Ideals.

(1) I ist nulldimensional, primär und in allgemeiner Lage bezüglich lexikografischen Ordnung mit $x_1 > \cdots > x_n$.

(2) Es gibt $g_1, \ldots, g_n \in k[x_n]$ und positive ganze Zahlen $\nu_1, \ldots, \nu_n$, so dass

   a) $I \cap k[x_n] = \langle g_n^{\nu_n} \rangle$ ist mit irreduziblem g_n und

b) für jedes $j < n$ I das Element $(x_j + g_j)^{\nu_j}$ enthält.

(3) Wenn S eine reduzierte Gröbner Basis bezüglich der gewählten Ordnung von I ist, dann gibt es $g_1, \ldots, g_n \in k[x_n]$ und positive ganze Zahlen $\nu_1, \ldots, \nu_n$, so dass

a) $g_n^{\nu_n} \in S$ mit irreduziblem g_n

b) $(x_j+g_j)^{\nu_j}$ ist kongruent modulo einem Element in $S \cap k[x_j, \ldots, x_n]$ modulo $\langle x_{j+1} + g_{j+1}, \ldots, x_{n-1} + g_{n-1}, g_n\rangle \subset k[x_1, \ldots, x_n]$ für $j = 1, \ldots, n-1$.

Der Beweis dieser Behauptung wird in GP07 Criterion 4.2.4. ausgeührt und der daraus resultierende Algorithmus für die Primärzerlegung eines nulldimensionalen Ideals ist der Algorithmus 4.2.7. in [GP07]:

ALGORITHMUS (ZERODECOMP(I)):

INPUT: Ein nulldimensionales Ideal $I = \langle f_1, \ldots, f_k\rangle \subset k[x_1, \ldots, x_n]$.

OUTPUT: Paare (Q_i, P_i) von Idealen in $k[x_1, \ldots, x_n]$, $i = 1, \ldots, r$, mit

- $I = Q_1, \ldots, Q_r$ ist eine Primärzerlegung von I, und
- $P_i = \sqrt{Q_i}$, $i = 1, \ldots, r$.

- RESULT := $\emptyset$;
- Wähle ein $\underline{a} \in k^{n-1}$ und führe den Koordinatenwechsel $I' = \varphi_{\underline{a}}(I)$ durch.;
- Berechne eine Gröbnerbasis G von I' bzgl. der lexikografischen Ordnung mit $x_1 > \ldots > x_n$ und sei $g \in G$ das Element mit dem kleinsten führenden Monom (LM);
- Faktorisiere $g = g_1^{\nu_1} \cdots g_s^{\nu_s} \in k(x_n)$;
- FOR $i = 1, \ldots, s$ DO

  Setze $Q_i' := \langle I', g_i^{\nu_i}\rangle$ und $Q_i := \langle I, \varphi_{\underline{a}}^{-1}(g_i)^{\nu_i}\rangle$;
  Setze $P_i' :=$ PRIMARYTEST (Q_i');
  IF $P_i' \neq \langle 0\rangle$;
  Setze $P_i := \varphi_{\underline{a}}^{-1}(P_i')$;
  RESULT := RESULT $\cup\{(Q_i, P_i)\}$;

ELSE

RESULT := RESULT ∪ ZERODECOMPOSITION (Q_i);

- RETURN RESULT.

3.1.2 Der mehrdimensionale Fall

Zur Reduktion eines mehrdimensionalen Ideals I auf den 0-dimensionalen Fall brauchen wir den Begriff einer maximalen unabhängigen Menge bezüglich dieses Ideals. Eine Menge $u \subset \{x_1, \ldots, x_n\}$ heisst eine maximale unabhängige Menge bezüglich i, falls $I \cap k[u] = 0$ und dim $(k[x_1, \ldots, x_n]/I) = \#u$. Maximal unabhängige Mengen sind eine Anwendung der Noether Normalisierung. Die geometrische Bedeutung solcher Mengen ist, dass die Projektion von der Nullstellenmenge $V(I)$ des Ideals auf den affinen Raum in den Variablen von u surjektiv ist, denn $V(I \cap k[u]) = V(\langle 0 \rangle)$ ist der ganze affine Raum.

Beispiel 3

(1) Sei $I = \langle xy, xz \rangle \subset k[x, y, z]$. Dann ist $\{y, z\} \subset \{x, y, z\}$ eine maximale unabhängige Menge bezüglich I.
Denn $I \cap k[y, z] = 0$ und dim $(k[x, y, z]/I) = 2$. (Die Nullstellenmenge von I ist die Vereinigung der yz-Ebene und der x-Achse). Die Menge $\{z\}$ ist zwar unabängig und kann nicht vergrössert werden, aber sie ist dennoch nicht maximal.

(2) Sei $J = \langle x^2, yz \rangle \subset k[x, y, z]$. Dann sind $\{x\}, \{y\}$, und $\{z\} \subset \{x, y, z\}$ maximal unabhängige Mengen bezüglich J. denn $J \cap k[u] = 0$ für $u = x, y, z$ und dim $(k[x, y, z]/J) = 1$. (Die Nullstellenmenge von J ist die Vereinigung der y-Achse und der z-Achse).

Wir schreiben hier $(x_1, \ldots, x_n)$ als x. Nun ist $\emptyset \subset x \setminus u$ eine maximal unabhängige Menge bezüglich $Ik(u)[x \setminus u]$ und somit ist dieses ein nulldimensionales Ideal in $k(u)[x \setminus u]$. Aus einer irredundanten Primärzerlegung von diesem Ideal $Ik(u)[x \setminus u] = Q_1 \cap \cdots \cap Q_s$ erhalten wir dann mittels einer Kontraktion $Ik(u)[x \setminus u] \cap k[x] = (Q_1 \cap k[x]) \cap \cdots \cap (Q_s \cap k[x])$, ebenfalls eine irredundante Primärzerlegung, was in der folgenden Proposition nochmal erläutert wird.

Proposition 9 (GP07, Proposition 4.3.1.)

(1) $Ik(u)[x \setminus u] \subset k(u)[x \setminus u]$ ist ein nulldimensionales Ideal.

(2) Sei $S = \{g_1, \ldots, g_s\} \subset I \subset k[x]$ eine Gröbner Basis von $Ik(u)[x \setminus u]$ und sei $h := kgV(LC(g_1), \ldots, LC(g_s)) \in k[u]$. Dann ist

$$Ik(u)[x \setminus u] \cap k[x] = (I : \langle h^\infty \rangle)$$

und dieses Ideal ist equidimensional von der Dimension dim(I).

(3) $Ik(u)[x \setminus u] = Q_1 \cap \cdots \cap Q_s$ sei eine irredundante Primärzerlegung. Dann ist auch

$$Ik(u)[x \setminus u] \cap k[x] = (Q_1 \cap k[x]) \cap \cdots \cap (Q_s \cap k[x])$$

eine irredundante Primärzerlegung.

Hier ist mit "LC" jeweils der Leitkoeffizient, das heißt, der Koeffizient des Leitmonoms gemeint. Der erste Punkt ist auch eine Anwendung der Noether Normalisierung. Es gibt ein Theorem (GP07 5.3.1.(6)) das besagt, dass ein Ideal $I \subset A$ mit einer bezüglich I unabhängigen Menge v die folgenden zwei Eigenschaften hat:
Die Dimension des Faktorringes $(A/I) \geq \#v$ und es gibt ein $v \subset \{x_1, \ldots, x_n\}$ mit $I \cap k[u] = 0$, so dass die Dimension von $A/I = \#v$ ist. In unserem Fall setzen wir $k = k(u)$ und dann ist $u = v$. Beim zweiten Punkt ist es offensichtlich, dass $(I : \langle h^\infty \rangle) \subset Ik(u)[x \setminus u]$ ist. Die andere Inklusion zeigt man indem man für ein $f \in Ik(u)[x \setminus u] \cap k[x]$ zeigt, dass die Buchberger Normalform NF $(f \mid S) = 0$ ist mit einer Gröebner Basis S von I. Die Equidimensionalität erkannt man am besten wenn man das Ideal in $k[x]$ betrachtet. Wir nehmen an, dass $I = Q_1 \cap \ldots \cap Q_r$ eine Primärzerlegung ist mit $Q_i \cap k[u] = \langle 0 \rangle$ für alle $i = 1, \ldots, s$ und $Q_j \cap k[u] \neq \langle 0 \rangle$ für alle $j = s+1, \ldots, r$. Dann ist die Primärzerlegung unseres Ideals der Schnitt der $Q_i k(u)[x \setminus u]$. Aber da u eine maximal unabhängige Menge bezüglich der Ideale $\sqrt{Q_i k(u)[x \setminus u]}$ ist, folgt dass alle assoziierten Primideale von $Ik(u)[x \setminus u]$ mindestens die Dimension von I haben müssen.
Beim dritten Punkt kann man die Zerlegung von

$$Ik(u)[x \setminus u] \cap k[x] = (Q_1 \cap k[x]) \cap \cdots \cap (Q_s \cap k[x])$$

als Kontraktion von $Ik(u)[x \setminus u] = Q_1 \cap \cdots \cap Q_s$ unter einem Homomorphismus zwischen $k(u)[x \setminus u]$ und $k(u)[x \setminus u] \cap k[x]$ betrachten.

Nun ist aber $I = (I : \langle h^m \rangle) \cap (I, h^m)$ (GP07, Lemma 3.3.6.). $(I : \langle h^m \rangle)$ ist ein equidimensionales Ideal gleicher Dimension wie I, dessen Zerlegung wir schon berechnet haben. Also müssen wir nur noch $(I, \langle h^m \rangle)$ zerlegen. Das machen wir mittels Induktion, indem wir die Prozedur auf $(I, \langle h^m \rangle)$ anwenden. Wenn dim $(I, \langle h^m \rangle) <$ dim (I) ist oder die Anzahl der maximal unabhängigen Mengen bezgl. $(I, \langle h^m \rangle)$ kleiner geworden ist als die Anzahl der maximal unabhängigen Mengen bezgl. (I) endet der Vorgang.

Als Basis für eine allgemeine oder eine equidimensionale Primärzerlegung und die Berechnung eines Radikals wird der Algorithmus 4.3.2 in GP07, zur Reduktion auf den nulldimensionalen Fall, eingesetzt:

ALGORITHMUS (REDUCTIONTOZERO(I)):

INPUT: $I = \langle f_1, \ldots, f_k \rangle \subset k[x_1, \ldots, x_n]$.

OUTPUT: Eine Liste (u, G, h^m), so dass

- u eine maximale unabhängige Menge bezüglich I ist,
- $G = \{g_1, \ldots, g_s\} \subset I$ eine Gröbner Basis von $Ik(u)[x \setminus u]$ ist, und
- $h \in k[u]$ so dass $Ik(u)[x \setminus u] \cap k[x] = (I : \langle h^m \rangle)(I : \langle \langle h^\infty \rangle \rangle)$

- Berechne eine maximale unabhängige Menge bezüglich I;
- Berechne eine Gröbner Basis $G = \{g_1, \ldots, g_s\}$ von I bezüglich der lexikografischen Ordnung mit $x \setminus u > u$;
- $h := \prod_{i=1}^{s} \mathrm{LC}(g_i)$, wobei die g_i als Polynome in $k[x \setminus u]$ mit Koeffizienten aus $k(u)$ behandelt werden;
- Berechne $m \in \mathbb{N}$, so dass $(I : \langle h^m \rangle) = (I : \langle h^{m+1} \rangle)$;
- RETURN (u, G, h^m)

Bemerkung 10 *Da bezüglich der eingeführten lexikografischen Ordnung für jedes $f \in Ik(u)[x \setminus u]$ gilt, dass $LM(f) \in L(I) \cdot k(u)$, ist G tatsächlich eine Gröbner Basis von $Ik(u)[x \setminus u]$.*

Beispiel 4 Sei $I = \langle xz, xy \rangle$ wie im ersten Punkt des letzten Beispiels. Dann haben wir gesehen, dass $u = \{y, z\}$ eine maximale unabhängige Menge bezüglich I ist. Wählen wir somit die lexikografische Ordnung dp mit $x > y > z$, so erhalten wir $G = \{xz, xy\}$ und $h = yz$. $(I : \langle yz \rangle) = (I : \langle yz \rangle^2)$ und somit ist der Saturierungsexponent $m = 1$.

Nun ist die Vorbereitung für einen Algorithmus eines mehrdimensionalen Ideals komplett:

ALGORITHMUS (DECOMP(I)):

INPUT: $I = \langle f_1, \ldots, f_k \rangle \subset k[x_1, \ldots, x_n]$.

OUTPUT: Paare (Q_i, P_i) von Idealen in $k[x_1, \ldots, x_n]$, $i = 1, \ldots, r$, so dass

- $I = Q_1, \ldots, Q_r$ eine Primärzerlegung von I ist, und
- $P_i = \sqrt{Q_i}$, $i = 1, \ldots, r$.

- (u, G, h) = REDUCTIONTOZERO(I);
- Wechsle den Ring zu $k(u)[x \setminus u]$ und berechne dort qprimary:= ZERODECOMP(G);
- Wechsle den Ring zu $k[x]$ und berechne dort primary:= $\{(Q' \cap k[x], (P' \cap k[x]) \mid (Q', P') \in qprimary\}$;
- primary = primary $\cup$ DECOMP($\langle I, h \rangle$);
- RETURN primary.

3.2 Primärzerlegung eines Ideals in $\mathbb{Z}[x_1, \ldots, x_n]$

Die Hauptquelle zu diesem Kapitel ist der Artikel *Constructions in a polynomial ring over the ring of integers* den A. Seidenberg 1974 dem *American Journal of Mathematics* zukommen liess. Viele Definitionen und Eigenschaften von bekannten Objekten aus der kommutativen Algebra werden hier von einer anderen Seite aufgezogen.
Was jetzt neu dazu kommt sind Elemente aus $\mathbb{Z}$, die in den zu zerlegenden Idealen enthalten sein können. Da alle Elemente eines Körpers k invertierbar sind, hatten wir es damit vorher nicht zu tun. Ausserdem müssen einige Vorgänge wegen der nicht invertierbaren Koeffizienten modifiziert werden.

3.2.1 Vorbereitungen für die algorithmische Umsetzung

Es gibt zwei Herangehensweisen an ein Problem: Die klassische, bei der man die gesuchten Objekte nach deren Existenzbeweis konstruiert. Bei der zweiten, der algorithmischen Methode, werden die Objekte erst nach deren algorithmische Umsetzung als existent erklärt. Mit algorithmische Umsetzung ist hier ein Vorgang gemeint, der mit endlich vielen Schritten zum gewünschten Ergebnis führt, d.h. es kann eine obere Schranke für die Anzahl der benötigten Operationen angegeben werden.

Hier achten wir darauf, dass die Beweise, die direkt mit der Primärzerlegung zu tun haben schon in algorithmischer Form dargestellt werden, da wir einen Algorithmus für solche Zerlegungen entwickeln wollen.
Zum Beispiel können wir wie folgt ein $\varrho \in \mathbb{N}$ konstruieren, so dass für Ideale $A, B \subset k[x_1, \ldots, x_n]$ gilt $(A : B^{\varrho}) = (A : B^{\varrho+1})$. Ist die algorithmische Umsetzung von $(A : B)$ und der Vergleich von A und $(A : B)$ schon bekannt, so konstruiert man $(A : B)$ und vergleicht es mit A. Ist $A = (A : B)$, so ist $\varrho = 0$ eine Lösung, sie sogenannte Saturierung von $(A : B)$. Falls $A \subseteq (A : B)$ ist, so konstruieren wir $(A : B^2)$und vergleichen es mit $(A : B)$, etc.

Beispiel 5

(1) $A := \langle y \rangle$, $B := \langle x \rangle$ seien Ideale in $\mathbb{Z}[x, y]$
$(A : B) = (\langle y \rangle : \langle x \rangle) = \{r \in \mathbb{Z}[x, y] : r \cdot \langle y \rangle \subset \langle x \rangle\} = \langle y \rangle = A$
$\Rightarrow \varrho = 0.$

(2) Für $A := \langle x \rangle$, $B := \langle x^2 \rangle$ in $\mathbb{Z}[x, y]$ ist $(A : B) = \mathbb{Z}[x, y]$
Hier sieht man leicht, dass der Quotient gleich dem ganzen Ring ist, falls $B \subset A$.

(3) $A := \langle x^3z^3, xyz, 2yz^5 \rangle$, $B := \langle z \rangle$ seien Ideale in $\mathbb{Z}[x, y, z]$
$(A : B) = \langle x^3z^2, xy, 2yz^4 \rangle$
$(A : B^2) = \langle x^3z, xy, 2yz^3 \rangle$
$(A : B^3) = \langle x^3, xy, 2yz^2 \rangle$
$(A : B^4) = \langle x^3, xy, 2yz \rangle$
$(A : B^5) = \langle x^3, xy, 2yz \rangle$
$\Rightarrow \varrho = 4.$

In der klassischen Herangehensweise sind solche Versuchsmethoden durchaus erlaubt. Aber vom algorithmischen Gesichtspunkt her ist das keine Lösung, da sie vom Argument der Existenz von ϱ abhängt. Also werden wir ab jetzt die Versuchsmethoden auch im Klassischen ausschließen.

Auch im arithmetischen Fall gehen wir erst einmal von einem Polynomring in einer Variablen aus. Deswegen werden wir unseren Polynomring in mehreren Variablen wie folgt bezeichnen: $\mathbb{Z}[x_1, \cdots, x_n] := R[x_n]$ mit $R = \mathbb{Z}[x_1, \cdots, x_{n-1}]$. Mit "Grad" meinen wir den Grad in x_n.
William W. Adams und Philippe Loustaunau haben in *An Introduction to Gröbner Bases*, das 1994 von der American Mathematical Society herausgegeben wurde, die algorithmische Umsetzung einer Primärzerlegung mittels Gröbner Basen im univariaten Fall $A = R[x]$, R Hauptidealbereich beschrieben. Darauf kann man hier nur im univariaten Fall zurückgreifen. Für den interessierten Leser werden dort auch einige Beispiele Schritt für

Schritt mit Hilfe von Gröbner Basen durchgerechnet.
Ein grundlegendes Hilfsmittel, das in vielen algorithmische Umsetzungen der Kommutativen Algebra gebraucht wird sind Syzygienmoduln $syz(I)$ von Idealen I. Die Theorie dazu wird im Anhang dargestellt. In Singular gehört die Berechnung von Syzygien zu den wenigen Funktionen, die schon für den arithmetischen Fall implementiert sind. A. Seidenberg hat 1974 in *Constructions in Algebra* die algorithmische Umsetzung von $A \cap B$ wie folgt beschrieben: Seien $A = \langle f_1, \ldots, f_r \rangle$, $B = \langle f_{r+1}, \ldots, f_s \rangle$ zwei durch endlich viele Erzeugende gegebene Ideale. Dann reicht es, alle s-Tupel $(g_1, \ldots, g_s)$ zu finden, so dass gilt: $g_1 f_1 + \cdots + g_r f_r = g_{r+1} f_{r+1} + \cdots + g_s f_s$.
Also rechnen wir

$$g_1 f_1 + \cdots + g_r f_r - g_{r+1} f_{r+1} - \cdots - g_s f_s = 0$$

und erhalten $syz(\langle f_1, \ldots, f_r, -f_{r+1}, \ldots, -f_s \rangle)$.
In diesem Artikel hatte er allerdings keine Berechnung von Syzygien im arithmetischen Fall dargestellt. In *An Introduction to Gröbner Bases* haben W.W. Adams und P. Loustaunau erst die algorithmische Umsetzung von Schnitten und Quotienten und dann die algorithmische Umsetzung von Syzygien für Ideale eines Ringes $A = R[x_1, \cdots, x_n]$, R ein Ring, in dem lineare Gleichungsysteme lösbar sind, gezeigt. Da sowohl Schnitte als auch Quotienten von Idealen in unseren Algorithmen gebraucht werden, wollen wir hier die Ideen zu deren algorithmischer Umsetzung darstellen.

Proposition 11 (AL94, Proposition 4.3.9.) *Seien $I = \langle f_1, \ldots, f_s \rangle$ und $J = \langle g_1, \ldots, g_t \rangle$ Ideale in A und w eine neue Variable. Betrachte das Ideal*

$$\langle w f_1, \cdots, w f_s, (1-w) g_1, \cdots, (1-w) g_t \rangle \subset A[w]$$

Dann ist $I \cap J = L \cap A$.

Proposition 12 (AL94, Proposition 4.3.11.) *Seien $I = \langle f_1, \ldots, f_s \rangle$ und $J = \langle g_1, \ldots, g_t \rangle$ Ideale in A. Dann ist*

$$(I : J) = \{ f \in A \mid fJ \subseteq I \} = \bigcap_{j=1}^{t} (I : \langle g_j \rangle).$$

Ist $I \cap \langle g \rangle = \langle h_1 g, \ldots, h_l g \rangle$ mit einem Nichtnullteiler $g \in A$, so ist

$$(I : \langle g \rangle) = \langle h_1, \ldots, h_l \rangle$$

Wir verzichten hier auf die Beweise. Bei der vorletzten Proposition benutzt man eine Eliminierungsordnung für Variablen mit $w > x_1, \ldots, x_n$. Eliminierungsverfahren spielen auch in unserem angestrebten Algorithmus eine Rolle.

3.2.2 Primärzerlegung eines Ideals ohne Elemente aus $\mathbb{Z}$

Ist ein Polynom f in einem Ideal $I \subset R[x_n]$ enthalten, so ist trivialerweise $(I : f) = R[x_n]$. Betrachten wir nun das Ideal $(I : p)$ für eine Primzahl p. Ist $(I : p) = I$ so gibt es kein $f \notin I$ mit $f \cdot p \in I$. Im folgenden Theorem geht es darum, dass jedes Ideal $I \subseteq R[x_n]$ nur durch endlich viele Primzahlen teilbar ist.

Theorem 13 (Sei78) *Sei $I = (f_1, \cdots, f_q)$ ein Ideal in $R[x_n]$. Dann gibt es endlich viele Primzahlen p mit $(I : p) \supseteq I$.*

Beweis: $(h_1, \cdots, h_q) \subset \mathbb{Q}[x_1, \cdots, x_n]$ seien Lösungsmengen der Gleichung $h_1 f_1 + \cdots + h_q f_q = 0$. Die Menge der q-Tupel $\{(h_1, \cdots, h_q)\}$, Lösungen der Gleichung $h_1 f_1 + \cdots + h_q f_q = 0\}$ ist ein $\mathbb{Q}[x_1, \cdots, x_n]$-Modul, den wir mittels eines endlichen Erzeugendensystems angeben können, der sogenannte Syzygienmodul von I. Dies sei $(h_{i1}, \cdots, h_{iq})$, $i = 1, \cdots, M$.
Durch dessen Konstruktion erhält man ein $N \in \mathbb{N}$, so dass $(h_{i1}, \cdots, h_{iq})$ modulo p ein Erzeugendensystem ist für die Lösungen von $h_1 f_1 + \cdots + h_q f_q \equiv 0$ modulo p für $p > N$. Wir können annehmen, dass
$h_{ij} \in \mathbb{Z}[x_1, \cdots, x_n]$ liegt, indem man alle Erzeugenden mit dem Hauptnenner durchmultipliziert.
Sei $p > N$ und $f \in (I : p)$, d.h. $pf = g_1 f_1 + \cdots + g_q f_q \in I$.
Dann ist $(g_1, \cdots, g_q) \equiv \sum_{i=1}^{M} a_i (h_{i1}, \cdots, h_{iq}) \bmod p$, mit $a_i \in \mathbb{Z}[x_1, \cdots, x_n]$
$\Rightarrow pf = (\sum a_i h_{i1} + p g'_1) f_1 + \cdots + (\sum a_i h_{iq} + p g'_q) f_q$ für ein $(g'_1, \cdots, g'_q)$ in $(\mathbb{Z}[x_1, \cdots, x_n])^q$.
$\Rightarrow f = g'_1 f_1 + \cdots + g'_q f_q$ und $(I : p) = I$ für $p > N$ Also bleiben nur endlich viele Primzahlen p für die man testen muss, ob $(I : p) \supseteq I$ ist.

q.e.d.

Dieser Beweis läuft algorithmisch analog. Wie man testet, ob I in $(I : p)$ enthalten ist wird in den Artikeln *What is Noetherian?* von A. Seidenberg oder *Constructive Aspects of Noetherian Rings* von F. Richman erläutert. Dabei taucht die Eigenschaft der *detachability* von endlich erzeugten Idealen auf. Das heisst, dass man für ein Element $r \in R$ sagen kann, ob es in einem Ideal I enthalten ist. Genauso heisst eine Teilmenge A einer Menge B *detachable* von B, wenn man für ein $b \in B$ entscheiden kann, ob es auch in A enthalten ist. Dies ist ein Vorgang, der für Ideale schon in Singular

implementiert ist und auch im arithmetischen Fall funktioniert. Dort wird mit einer Normalform NF geprüft, ob $\mathrm{NF}(I \mid (I:p)) = 0$ ist. Wenn dem so ist, dann ist $(I:p) \supsetneq I$.

Nun wollen wir ein Ideal I wie folgt in zwei Teile $I = B \cap C$ zerlegen, so dass kein zu B assoziiertes Primideal eine ganze Zahl $\neq 0$ enthält und jedes zu C assoziierte Primideal eine ganze Zahl $\neq 0$ enthält. Ausserdem kann C als $C_1 \cap \cdots \cap C_s$ geschrieben werden, wobei alle assoziierten Primideale der C_i, $i = 1, \cdots, s$ dieselbe Primzahl p_i enthalten. Algorithmisch betrachtet formulieren wir das ein wenig anders.

Theorem 14 (Sei78) *Sei $I = (f_1, \cdots, f_q)$ ein Ideal in $R[x_n]$. Dann kann man Ideale B und C konstruieren mit $I = B \cap C$, so dass $(B:b) = B$ ist für jede ganze Zahl $b \neq 0$ und so dass C eine ganze Zahl $\neq 0$ enthält. Ausserdem kann C als $C_1 \cap \cdots \cap C_s$ geschrieben werden, wobei jedes C_i eine Potenz einer Primzahl p_i enthält.*

Beweis: Für gegebene Ideale I und J kann man den Saturierungsexponenten $\varrho \in \mathbb{N}$, von $(I:J)$ finden. Also gilt für positive Primzahlen $p_1, \cdots, p_s$ mit $(I:p_i) \supsetneq I$, dass $B = (I : \langle p_1 \cdots p_k \rangle^{\varrho})$ ist für ein genügend großes ϱ.
Ist für beliebiges $f \in A$ $(I:f^r) = (I:f^{r+1})$, so gilt $I = (I:f^r) \cap (I, f^r)$:
Aus $b \in (I:f^r) \cap (I, f^r)$ folgt $b = g + h \cdot f^r$ für $g \in I$, $h \in R[x_n]$
$\Rightarrow b \cdot f^r = g \cdot f^r + h \cdot f^{2r} \in I$ und somit folgt
$h \cdot f^{2r} \in I$ und $h \in (I:f^{2r}) = (I:f^r)$
$\Rightarrow h \cdot f^r \in I$ und $b \in I$
Also ist $C = (I, (p_1, \cdots, p_s)^{\varrho})$ und $I = (I : (p_1 \cdots p_k)^{\varrho})) \cap (I, (p_1 \cdots p_k)^{\varrho})$.
Analog kann man die C_i, $i = 1, \cdots, s$ konstruieren.

q.e.d.

Dies war die Beschreibung der ersten Zerlegung, die dann aber noch verfeinert werden muss. Das ϱ ist das Maximum aller Saturierungsexponenten der Ideale $(I : \langle p_j \rangle)$, $j = 1, \ldots, k$. Die Ideale C_i, $i = 1, \ldots, s$ enthalten zwar alle eine Potenz einer Primzahl, aber sie müssen dennoch keine Primärideale sein. Trotzdem wollen wir schon das erste Element unseres Algorithmus darstellen:

]
ALGORITHMUS (SPLITTING(I)):

INPUT: Ein Ideal $I = \langle f_1, \ldots, f_k \rangle \subset \mathbb{Z}[x_1, \ldots, x_n]$.

OUTPUT: Ideale $B, C \in \mathbb{Z}[x_1, \ldots, x_n]$, Primzahlen $p_1, \ldots, p_k$ und ein $\varrho \in \mathbb{N}$, so dass

- $I = B \cap C$ eine Zerlegung von I ist, und
- $B = (I : (p_1 \cdots p_k)^\varrho)$ und $C = (I, (p_1 \cdots p_k)^\varrho)$ ist.

- RESULT $:= \emptyset$;
- Berechne $N = n(d)^{2^{n-1}}$, wobei n die Anzahl der Variablen und $d \geq \max deg(h_{ij})$ der h_{ij} aus dem Beweis des Theorem 14 sind;
- Berechne alle Primzahlen $p_1, \ldots, p_r$ zwischen 1 und N;
- FOR $i = 1, \ldots, r$ DO

  Berechne NF$((I \mid (I : p_i))$;
  IF NF$((I \mid (I : p_i)) = 0$, setze RESULT=RESULT$\cup\{p_i\}$;
  ELSE setze RESULT=RESULT;

- Berechne die Saturierung von $(I : \langle p_1 \cdots p_k \rangle)$, $p_1, \ldots, p_k \in$ RESULT, d.h. finde ein $\varrho \in \mathbb{N}$, so dass $(I : \langle p_1 \cdots p_k \rangle^\varrho) = (I : \langle p_1 \cdots p_k \rangle^{\varrho+1})$;
- Setze $B = (I : (p_1 \cdots p_k)^\varrho)$ und $C = (I, (p_1 \cdots p_k)^\varrho)$;
- RESULT = RESULT $\cup \{B, C, \varrho\}$;
- RETURN RESULT.

Beispiel 6 Sei $I = \langle x^2, 5xy, 12 \rangle \subset \mathbb{Z}[x, y]$. Es gibt drei Primzahlen p mit $(I : p) \supsetneq I$: $(I : 2) = \langle x^2, 5xy, 6 \rangle$, $(I : 3) = \langle x^2, xy, 4 \rangle$ und $(I : 5) = \langle x^2, xy, 12 \rangle$. Es gilt: $(I : 2^2) = (I : 2^3)$, $(I : 3) = (I : 3^2)$ und $(I : 5) = (I : 5^2)$, also ist $\varrho = 2$. Also ist $(p_1 p_2 p_3)^2 = 900$ und wir teilen I wie folgt:

$$I = \langle x^2, 5xy, 12, 900 \rangle \cap (\langle x^2, 5xy, 12 \rangle : 900)$$
$$I = \langle x^2, 5xy, 12 \rangle \cap \langle x^2, xy, 1 \rangle = \mathbb{Z}[x, y]$$

Das Ideal $C = \langle x^2, 5xy, 12 \rangle$ kann geschrieben werden als der Schnitt der Ideale $\langle x^2, 5xy, 4 \rangle \cap \langle x^2, 5xy, 3 \rangle$, wobei die beiden rechten Ideale nur Potenzen der selben Primzahl enthalten. Beide Ideale sind aber keine Primärideale. Denn es ist $5xy \in \langle x^2, 5xy, 4 \rangle$ und $5x \notin \langle x^2, 5xy, 4 \rangle$, aber keine Potenz von y ist in $\langle x^2, 5xy, 4 \rangle$ enthalten.

Wir sehen, dass das Ideal $B = \mathbb{Z}[x_1, \ldots, x_n]$ ist, falls I eine ganze Zahl enthält. In dem Sinne ist das Wort "Aufteilung" eher als "Fallunterscheidung" zu verstehen. Enthält ein Ideal I keine ganze Zahl, so könnte man direkt mit einer Erweiterung nach $\mathbb{Q}[x_1, \ldots, x_n]$ arbeiten. Aber wenn man es mit komplexeren Idealen zu tun hat, sieht man nicht immer sofort, ob ein Ideal eine ganze Zahl enthält oder nicht. In Singular ist die Berechnung von Standardbasen, das sind nicht reduzierte Gröbnerbasen, für den arithmetischen Fall schon implementiert. Bei deren Berechnung wird ein Ideal, das ganze Zahlen enthält immer eine einzige ganze Zahl in der Standardbasis haben, weil bei ursprünglich mehreren ganzen Zahlen ja der größte gemeinsame Teiler immer als Linearkombination dieser Zahlen dargestellt werden kann. Die Zerlegung in die Ideale C_i hängt von der Faktorisierung dieser ganzen Zahl ab, was bei sehr großen Zahlen ein Problem bei der Effizienz des implementierten Algorithmus darstellen kann. Aufgrund unserer Konstruktion dieser Zahl kennen wir aber deren Faktorisierung schon.
Da ganze Zahlen in $\mathbb{Q}$ Einheiten sind, stören sie die Abbildung von Idealen aus $\mathbb{Z}[x_1, \ldots, x_n]$, d.h. das erweiterte Ideal ist dann in $\mathbb{Q}[x_1, \ldots, x_n]$ der ganze Ring. Das nächste Theorem beschreibt den Vorgang der Zerlegung mittels einer Erweiterung.

Theorem 15 (Sei78) *Sei das gegebene Ideal $I = B$ so, dass keines seiner assoziierten Primideale eine ganze Zahl $\neq 0$ enthält, mit anderen Worten gilt $(I : b) = I, \quad \forall b \in \mathbb{Z} \setminus \{0\}$. Dann kann man eine Primärzerlegung von I in Primärideale konstruieren.*

Beweis: Wir erweitern I nach $\mathbb{Q}[x_1, \ldots, x_n]$, wo wir eine Primärzerlegung von $I \cdot \mathbb{Q}[x_1 \cdots, x_n]$ bekommen können. [1] Diese sei $Q_1 \cap \cdots \cap Q_s$.
Nun konstruieren wir die $Q_i \cap \mathbb{Z}[x_1 \cdots, x_n]$, $i = 1, \ldots, s$:
Ist z.B. $Q_1 = \langle f_1, \ldots, f_q \rangle$ mit $f_i \in \mathbb{Z}[x_1 \cdots, x_n]$, was wir erreichen, indem wir die f_i mit dem Hauptnenner durchmultiplizieren. Nun setzen wir $I_1 := \langle f_1, \ldots, f_q \rangle \subset \mathbb{Z}[x_1 \cdots, x_n]$.
Dann ist Q_1 die Erweiterung von I_1 und die gesuchte Kontraktion ist die Kontraktion der Erweiterung von I_1.
Sei nun $I_1 = B_1 \cap C_1$ wie in Theorem 7. Dann ist B_1 die gesuchte Kontraktion.
$\Rightarrow I = B_1 \cap \cdots \cap B_s$

q.e.d.

[1] A. Seidenberg hat diesen Vorgang in *Constructions in Algebra* geschildert. Aber er wurde auch schon von G. Pfister, W. Decker, H. Schönemann und S. Laplagne nach der Theorie von Gianni, Trager und Zacharias und von Shimoyama-Yokohama in die Bibiliothek *primdec.lib* in Singular implementiert

Natürlich muss man das für alle Q_i betrachten. Etwas übersichtlicher kann man das wie folgt darstellen:

$$\begin{array}{rcl} f : \mathbb{Z}[x_1, \ldots, x_n] & \longrightarrow & \mathbb{Q}[x_1, \ldots, x_n] \\ I & \longmapsto & f(I) = Q_1 \cap \cdots \cap Q_s \\ \langle f_1, \ldots, f_q \rangle = I_1 & \longmapsto & Q_1 = \langle f_1, \ldots, f_q \rangle = I_1^e \end{array}$$

$Q_1^c = I_1^{ec} = B_1$ aus der Aufteilung $I_1 = B_1 \cap C_1$

Wir wissen, dass $I_1 \subset I_1^{ec}$ ist. Um sicher zu gehen, dass in der gesuchten Kontraktion von Q_1 keine ganze Zahl ist, teilt man hier I_1 nochmal auf. In Singular lösen wir das wie folgt:

ring $r = 0, (x_1, \ldots, x_n)$, lp;
ideal $I = B$;
$I = \mathsf{std}(I)$;
LIB "primdec.lib";
$\mathsf{primdecGTZ}(I)$;

Das Ergebnis $Q_1 \cap \cdots \cap Q_s$ wird angezeigt. Die Funktion "$\mathsf{std}(I)$" berechnet eine Standardbasis von I. Gegebenenfalls müssen wir die Erzeugenden der Ideale noch mit dem Hauptnenner durchmultiplizieren, um sie dann als Polynome in $\mathbb{Z}[x_1, \ldots, x_n]$ betrachten zu können. Das führt man mit der Funktion "cleardenom" aus:

for $(i = 1, i <= q, i++)$
{vector $v_i = Q_i$;
$\mathsf{cleardenom}(v_i)$;
ideal $Q_i = \mathsf{cleardenom}(v_i)$};

Nun wechseln wir den Ring:

ring $r =$ integer, $(x_1, \ldots, x_n)$, lp;
int $q = q$;
for $(i = 1, i <= q, i++)$
{Ideal $I_i = Q_i$;
$\mathsf{SPLITTING}(I_i)$;}

Die jeweils angezeigten B_i sind dann unsere gesuchten Primärideale. Die hier benutzte Ordnung "lp" kann durch eine andere globale Ordnung ersetzt werden.

3.2.3 Eliminierung von Variablen

Für die algorithmische Herangehensweise an unser Problem werden folgende Begrifflichkeiten sehr nützlich sein: Ein O-dimensionales Primideal P welches das Ideal I enthält nennen wir ein *zu I assoziiertes Primideal*, falls $(I : P) \supseteq I$ ist. Dementsprechend nennen wir ein c-dimensionales Primideal P ein *zu I assoziiertes Primideal*, falls $(I : P') = I$ ist für jedes Primideal $P' \supseteq I$ von kleinerer Dimension als c, und $(I : P) \supseteq I$. In diesen Definitionen steckt die Reduktion auf den nulldimensionalen Fall.

Im arithmetischen Fall führt die Konstruktion der assoziierten Primideale eines Ideals mit Elementen aus $\mathbb{Z}$ über einen langen Weg zum Ziel. Wie schon erwähnt spielen dabei Lokalisierungen von Ringen nach multiplikativen Systemen eine große Rolle. Ist S ein multiplikativ abgeschlossenes System in einem Ring A, so nennen wir $A_S := \{\frac{a}{b} : a \in A, b \in S\}$ die Lokalisierung von A nach S. Betrachten wir den Ringhomomorphismus $\varphi : A \to A_S$ mit $a \mapsto \frac{a}{1}$. Er setzt Primideale in A_S in 1 : 1-Beziehung zu Primidealen in A, die leeren Schnitt mit S haben. Ausserdem lokalisieren irredundante Primärzerlegungen wie folgt: Ist $I = \cap_{i=1}^{s} Q_i$ eine irredundante Primärzerlegung in A und $Q_1, \ldots, Q_r$ diejenigen Primärideale, die mit S leeren Schnitt haben, so ist $I_S = \cap_{j=1}^{r} Q_{j\,S}$ eine irredundante Primärzerlegung in A_S. Die Hintergründe dazu kann man in David Eisenbuds *Commutative algebra with a view toward algebraic geometry* im Theorem 3.10.d. nachlesen.
Die Saturierung eines Ideals $I \subset A$ bezüglich eines multiplikativ abgeschlossenen Systems S ist als $A_S I \cap A$ definiert. Tatsächlich ist zum Beispiel für $S = \{f^\nu \mid \nu \in \mathbb{N}\}$ die Saturierung $A_S I \cap A = I_f A \cap A = (I : \langle f \rangle^\infty)$.
Ein für uns interessantes multiplikatives System ist $A \setminus P$ wobei P ein Primideal ist. Die Lokalisierung $A_P = \{\frac{a}{b} : a \in A, b \notin P\}$ heisst die Lokalisierung von A nach P und ist ein lokaler Ring mit maximalem Ideal PA_P. Hier liegt die Schwierigkeit darin, dass S nur indirekt, als Komplement gegeben ist. Trotzdem können wir interessante Informationen aus dieser Lokalisierung ziehen:

Proposition 16 (Vas04, Prop. 3.56.(d)) *Sei I ein Ideal und P ein beliebiges Primideal. Ist $I = \cap_{i=1}^{s} Q_i$ eine Primärzerlegung von I, deren Komponenten Q_j, $j = 1, \ldots, r < s$ in P enthalten sind und die restlichen Komponenten nicht, dann ist*

$$I_P = Q_1 \cap \cdots \cap Q_r.$$

Ausserdem gilt für ein $f \in \sqrt{Q_{r+1} \cap \cdots \cap Q_s} \setminus P$:

$$I_P = (I : f^\infty).$$

Nun wenden wir uns der Konstruktion der assoziierten Primideale zu. Dazu betrachten wir das multiplikativ abgeschlossene System S der Elemente, die nicht in $\langle p\rangle$ für eine Primzahl p enthalten sind. Das Ideal $\langle p\rangle$ ist ein Primideal, also haben wir hier eine Lokalisierung wie es oben beschrieben wurde. Wir brauchen den Schnitt $A_S M \cap \sum AZ_i$ mit dem freien A-Modul $\sum AZ_i$. Dabei sei M ein Untermodul und es soll $p^b Z_i \in M$ sein $\forall\, i$. Diese algorithmische Umsetzung wird der komplexeste und aufwändigste Teil des angestrebten Algorithmus werden. Deswegen betrachten wir erst einmal den univariaten Fall. Das nächste Lemma wird zu dieser algorithmischen Umsetzung in $\mathbb{Z}[x]$, mit genau einer Variablen führen. Später werden wir aber die Situation für $\mathbb{Z}[y_1, \cdots, y_c]$ anstelle von $\mathbb{Z}$ an der Basis erweitern. Dann sei I ein Ideal in $\mathbb{Z}[y_1, \cdots, y_c, x]$ welches eine Potenz p^b einer Primzahl p enthält mit $(I : f) = I$ für jedes $f \not\equiv 0 \bmod p$ in $\mathbb{Z}[y_1, \cdots, y_c]$. Im Klassischen würde man sagen, dass dann die assoziierten Primideale von I von Dimension $\geq c$ sind. Aber aus der algorithmischen Sicht werden wir beobachten, dass $(I : P) = I$ ist für jedes Primideal $P \supset I$ kleinerer Dimension als c und suchen zuerst die c-dimensionalen Primideale, und dann diejenigen höherer Dimension.
Aber erst einmal zum einfachen Fall. Wir können immer annehmen, dass eine Potenz einer Primzahl in unserem Ideal ist, da uns von nun an nur noch die schon konstruierten C_i interessieren.

Lemma 17 (Sei78) *Sei $A = \mathbb{Z}[x]$ und $I \subset A$ ein Ideal, so dass $p^b \in I$ ist für eine gegebene Primzahl $p > 0$.(b kann konstruiert oder als gegeben angenommen werden). S sei das multiplikative System der Elemente in $\mathbb{Z}[x]$ die ungleich 0 mod p sind. Dann kann man $A_S I \cap A$ konstruieren.*

Beweis: Alle zu I assoziierten Primideale enthalten p. Ist $I = \langle f_1, \cdots, f_s\rangle$ mit $f_i = p^{r_i} f_i'$, $f_i' \not\equiv 0 \bmod p$, so erhalten wir $A_S I \cap A = (p^r)$ und r ist das Minimum der $\{r_i, i = 1, \ldots, s\}$

q.e.d.

Für die Konstruktion der assoziierten Primideale eines Ideals in einer Variablen werden wir die mod p-irreduziblen Elemente $s_j \in \mathbb{Z}[x]$ suchen, so dass $(I : s_j) \supseteq I$. Ist P ein Primideal, das p enthält, so definieren wir seine Dimension als die Dimension von $P/\langle p\rangle$ in $\mathbb{Z}[x]/\langle p\rangle$. Die 0-dimensionalen Primideale, die p enthalten sind dann von der Form $\langle p, f\rangle$ mit einem mod p-irreduziblen Polynom f. Das einzige andere Primideal das p enthält ist $\langle p\rangle$. Für $I \not\equiv 0 \bmod p$ sei $f \in I$, $f \not\equiv 0 \bmod p$. Seine Zerlegung in mod p-irreduzible Faktoren sei $f = f_1' \cdots f_q' \bmod p$. Dann enthält jedes 0-dimensionale Primideal $P \supset I$ auch eines der f_i'. Somit haben wir eine endliche Anzahl Kandidaten für assoziierte Primideale von I, die wir auch

finden können: Denn ist $(I : s_j) \supseteq I$, s_j irreduzibel mod p, so ist $s_j \equiv f_i'$ mod p für ein $i \in \{1, \ldots, q\}$
Ist $I \equiv 0$ mod p und $I = p^r \cdot I_1$ mit $I_1 \not\equiv$ mod p, so ist jedes 0-dimensionale assoziierte Primideal von I auch assoziiertes Primideal von I_1. Also können wir auch hier die Primideale finden.

Wir gehen von den Idealen C_i aus, die jeweils eine Potenz von p enthalten. Dann gibt es eine Standardbasis $\langle p^b, f\rangle$ von C_i, da wir es nur mit einer Variablen zu tun haben. Wir faktorisieren $f = f_1' \cdots f_q'$ mod p und bekommen die zu C_i assoziierten Primideale $\langle p, f_i'\rangle$, $i = 1, \ldots, q$.

Beispiel 7 Wir betrachten das Ideal $C_1 = \langle x^3 - 7x^2 + 3x - 21, 16\rangle$. Das ist schon eine Standardbasis. Also haben wir $p = 4$ und sehen, dass $C_1 \not\equiv 0$ mod p ist. Es ist $f = x^3 - 7x^2 + 3x - 21 = x^3 + x^2 + 3x + 3$ mod 4. Die Faktorisierung davon ist dann $(x^2 + 3)(x + 1)$ und wir haben die gesuchten s_j. Die zu C_1 assoziierten Primideale sind dann $\langle x^2 + 3, 4\rangle$, $\langle x + 1, 4\rangle$ und $\langle 4\rangle$.

Wir hätten hier $\langle x + 1, 4\rangle$ auch als $\langle x - 7, 4\rangle$ schreiben können, wenn wir f direkt faktorisiert hätten. Beide Basen sind Standardbasen. Aber da die Faktorisierung im arithmetischen Fall eine der größten Hürden ist, ist es sinnvoll, soviel wie möglich zu vereinfachen.
Nochmal zurück zu $\mathbb{Z}[y_1, \ldots, y_c]$ anstelle von $\mathbb{Z}$ an der Basis. Wenn wir nun die c-dimensionalen assoziierten Primideale von $I \not\equiv 0$ mod p suchen, so sind diese von der Form $\langle p, f_i'\rangle$ wobei f_i', $i = 1, \cdots, q$ ein mod p-irreduzibles Polynom in $\mathbb{Z}[y_1, \ldots, y_c]$ ist. S sei nun das multiplikative System der Polynome $\not\equiv 0$ mod p in $\mathbb{Z}[y_1, \ldots, y_c]$ und sei s_j ein mod-p-irreduzibles Polynom mit $(I : s_j) \supseteq I$. Wir kommen zu der Annahme, dass $s_j \equiv f_i'$ mod p für ein $i \in \{1, \ldots, q\}$ sein muss. Denn wir haben $(I : s_j) \supseteq I$ und auch $(I : \langle p, s_j\rangle) \supseteq I$. Also ist I in $\langle p, s_j\rangle$ enthalten:
Nehmen wir einmal an, dass $I \not\subset \langle p, s_j\rangle$. Dann betrachten wir $\langle p, s_j, I\rangle$ mod p und sehen, dass dieses Ideal ein $f \not\equiv 0$ mod $p \in \mathbb{Z}[y_1, \cdots, y_c]$ enthält. Sei nun $a \in (I : \langle p, s_j\rangle)$. Da $f \in \langle p, s_j, I\rangle$ ist folgt, dass $af \in I$ und somit auch $a \in I$ liegt. Was dann bedeuten würde, dass $(I : \langle p, s_j\rangle) = I$, was ein Widerspruch zu $I \not\subset \langle p, s_j\rangle$ ist.
Also wissen wir, dass $I \subseteq \langle p, s_j\rangle$ und dass $\langle p, s_j\rangle$ ein c-dimensionales assoziiertes Primideal von I ist. Ebenso muss $s_j \equiv f_i'$ sein für ein $i \in \{1, \ldots, q\}$ sein. Ist $I \equiv 0$ mod p und $I = p^r I_1$ mit $I_1 \not\equiv 0$ mod p. I_1 enthält auch eine Potenz von p und $(I_1 : f) = I_1$ für alle $f \not\equiv 0$ mod p aus $\mathbb{Z}[y_1, \ldots, y_c]$. Damit ist auch $(I_1 : P) = I_1$ für jedes Primideal P das p enthält und kleinere Dimension als c hat. Für jedes c-dimensionale assoziierte Primideal $P \supset I$ folgt wegen $(I : P) \supseteq I$ dass $(I_1 : P) \supseteq I_1$ und $I_1 \subset P$, also ist P ein c-dimensionales assoziiertes Primideal von I_1. So können wir die c-dimensionalen assoziierten Primideale von I_1 und auch von I finden und

ebenso die mod p irreduziblen Elemente s_j mit $(I : s_j) \supseteq I$.
Mit den eben erarbeiteten Ergebnissen können wir ein Korollar formulieren:

Korollar 18 (Sei78) *Das letzte Lemma gilt auch für $\mathbb{Z}[y_1, \cdots, y_c]$ an der Basis anstelle von $\mathbb{Z}$, mit der weiteren Annahme, dass $(I : f) = I$ ist für jedes $f \not\equiv 0$ mod p in $\mathbb{Z}[y_1, \cdots, y_c]$.*

In einer Variablen und mit einer einzelnen Erzeugenden war das noch sehr übersichtlich. Wir erinnern uns, dass auch ein endlich erzeugtes Ideal ein freier A-Modul ist. Sind mehrere Erzeugende gegeben, so wird die Betrachtung von $A_S M \cap \sum AZ_i$ schon etwas aufändiger:

Theorem 19 (Sei78) *Sei $A = \mathbb{Z}[x]$ und $AZ_1 + \cdots + AZ_t$ ein freier A-Modul mit freien Erzeugenden $Z_1, \ldots, Z_t$. Sei $M = (l_1, \ldots, l_s)$ mit $l_i = f_{i1}Z_1 + \cdots + f_{it}Z_t$ ein endlicher Untermodul, so dass $p^b Z_i \in M$ ist, $i = 1, \cdots, t$ für eine gegebene Primzahl $p > 0$ (die wie oben als gegeben angenommen oder konstruiert werden kann). Sei S das multiplikative System in $\mathbb{Z}[x]$ der Elemente $\not\equiv 0$ mod p. Dann kann man $A_S M \cap \sum AZ_i$ konstruieren.*

Beweis: Sei $t \geq 1$. Wir suchen hier die mod p irreduziblen Elemente $s_j \in \mathbb{Z}[x]$ so dass $((l_1, \cdots, l_s) : s_j) \supseteq (l_1, \cdots, l_s)$, also dass es ein $l \notin (l_1, \cdots, l_s)$ mit $s_j l \in (l_1, \cdots, l_s)$. Dieses Problem haben wir schon für $t = 1$ gelöst, also machen wir hier eine Induktion nach t:
Für $t = 1$ gibt es nur eine endliche Anzahl der Elemente $s_j \not\equiv 0$ mod p, und wir behaupten das auch für größere t:
Sei nun $l = f_1 Z_1 + \cdots + f_t Z_t$ so ein l. Ist $f_1 \in \langle f_{11}, \cdots, f_{s1} \rangle$ so können wir, indem wir ein Element aus $(l_1, \cdots, l_s)$ von l subtrahieren annehmen, dass $l \in AZ_2 + \cdots + AZ_t$ ist. Aber ein Element $r_1 l_1 + \cdots + r_s l_s$ liegt nur in $AZ_2 + \cdots + AZ_t$, falls $r_1 f_{11} + \cdots + r_s f_{s1} = 0$ ist. Also berechnen wir den Syzygienmodul von $\langle f_{11}, \cdots, f_{s1} \rangle$. Damit kann man $(l_1, \cdots, l_s) \cap (AZ_2 + \cdots + AZ_t)$ konstruieren.
Da l nicht in diesem Modul ist, aber $s_j l$ schon, können wir durch Induktion nach t endlich viele s_j finden, die mod p betrachtet unterschiedlich sind. Ist $f_1 \notin \langle f_{11}, \cdots, f_{s1} \rangle$, dann ist $f_1 \in (\langle f_{11}, \cdots, f_{s1} \rangle : s_j) \supseteq \langle f_{11}, \cdots, f_{s1} \rangle$, und wir erhalten eine endliche Anzahl mehr Kandidaten für die s_j.
Nun konstruieren wir $A_S M \cap \sum AZ_i$:
Angenommen $l \in A_S M \cap \sum AZ_i$, $l \notin M$. Dann gibt es ein $s \in S$ mit $sl \in M$. Faktorisieren wir s mod p als $s = s_1 \cdots s_k - pr = s' - pr$ wobei die s_i irreduzibel mod p sind.
Nun ist $(s' - pr)(s'^{b-1} + s'^{b-2} pr + \cdots + p^{b-1} r^{b-1}) = s'^b - p^b r^b$, und somit ist $s'^b l \in M$. Also können wir annehmen, dass s ein Produkt $s_1 \cdots s_k$ mod p irreduzibler Elemente ist.

Ist nun s_i nicht equivalent zu einem der s_j aus der Konstruktion der Primideale eines Ideals $\langle f, p^b \rangle$, so ist $(M : s_i) = M$ und wir können dieses s_i entfernen.
Also können wir annehmen, dass S das multiplikative System ist, das durch die s_j des letzten Abschnitts erzeugt wird. Sei nun s das Produkt dieser s_j. Dann ist $A_S M \cap \sum AZ_i = (M : s^\varrho)$ für ein genügend großes ϱ.

q.e.d.

Dies war die verallgemeinerte algorithmische Umsetzung der Saturierung, die in der Proposition 9 beschrieben wurde. Mit diesem Ergebnis können wir ein Korollar formulieren:

Korollar 20 (Sei78) *Man kann ein einziges $s \in S$ konstruieren, so dass $R_S M \cap \sum RZ_i = (M : s^\varrho)$ ist für ein genügend großes ϱ.*

Der Algorithmus zur Konstruktion dieser Saturierung sieht wie folgt aus:

ALGORITHMUS (UNIVARLOC(M)):

INPUT: Ein $\mathbb{Z}[x]$-Modul $M = (l_1, \ldots, l_s) \subset \sum_{i=1}^{t} \mathbb{Z}[x] Z_i$, und eine Primzahl p, mit $p^b Z_i \in M$ für $i = 1, \ldots, t$.

OUTPUT: Der Schnitt $\mathbb{Z}[x]_S M \cap \sum_{i=1}^{t} \mathbb{Z}[x] Z_i$, wobei

- $S = \mathbb{Z}[x] \setminus \langle p \rangle$ das multiplikative System der Elemente ungleich 0 mod p in $\mathbb{Z}[x]$ ist und
- $\sum_{i=1}^{t} \mathbb{Z}[x] Z_i$ ein freier $\mathbb{Z}[x]$-Modul ist.

- Berechne eine Standardbasis von $M = \langle l_1, \ldots, l_s \rangle$;
- Finde mod p-irreduzible Elemente s_j mit $(M : s_j) \supseteq M$, das heisst, faktorisiere die Elemente $f_i \neq 0$ der Standardbasis mod p und erhalte mod p-irreduzible Elemente s_j, für $j = 1, \ldots, k$;
- Setze $s = s_1 \cdots s_k$;
- Berechne die Saturierung von $(M : s)$;
- RESULT $= (M : s^\infty)$;
- RETURN RESULT.

Im Algorithmus wurde $M = \langle l_1, \ldots, l_s \rangle$ bewusst als Ideal geschrieben, da die $l_i = f_{i1}Z_1 + \cdots + f_{it}Z_t$ in unserem Fall als Erzeugende eines Ideals behandelt werden können.
Nun sind wir vorbereitet, diese Konstruktion auch für den Polynomring in mehreren Variablen über $\mathbb{Z}$ zu betrachten. Wir wählen nun eine der Variablen x_i aus und nennen sie x. Dann setzen wir $R = \mathbb{Z}[x, x_1, \ldots, \hat{x_i}, \ldots, x_n]$.

Theorem 21 (Sei78) *Sei $R = \mathbb{Z}[x, x_1, \ldots, \hat{x_i}, \ldots, x_n]$ und $RZ_1 + \cdots + RZ_t$ ein freier R-Modul mit freien Erzeugenden $Z_1, \ldots, Z_t$. Sei $M = (l_1, \ldots, l_s)$ mit $l_i = f_{i1}Z_1 + \cdots + f_{it}Z_t$ ein endlicher Untermodul, so dass $p^b Z_i \in M$ ist, $i = 1, \ldots, t$ für eine gegebene Primzahl $p > 0$ (die wie oben als gegeben angenommen oder konstruiert werden kann). Sei S das multiplikative System in $\mathbb{Z}[x]$ der Elemente $\not\equiv 0$ mod p. Dann kann man $R_S M \cap \sum RZ_i$ konstruieren.*

Beweis: Sei $n + 1 = n + 1$ und $t \geq 1$. Für $R = \mathbb{Z}[x_1, \ldots, x_n]$ machen wir eine Induktion nach n. Dafür brauchen wir allerdings noch einige andere algorithmische Umsetzungen.
Wir beginnen mit der Betrachtung von der Situation in Lemma 12 für $R = \mathbb{Z}[x, x_1, \ldots, x_n]$. Sei $l_i = f_{i1}Z_1 + \cdots + f_{it}Z_t$ und sei $q = \max\{total\ deg(f_{ij})\}$. Der totale Grad *total deg* bedeutet hier der Grad in den Variablen $x_1, \ldots, x_n$, wobei wir mit *Grad* den Grad in x_n meinen.
Nun wählen wir aus $l_1, \cdots, l_s$ eine maximale mod p linear unabhängige Teilmenge über $\mathbb{Z}[x, x_1, \ldots, x_n]$ aus. Diese seien $l_1, \ldots, l_r$.
Da aus $r = 0$ auch $M \equiv 0$ mod p folgt können wir annehmen, dass $r > 0$ ist. Sonst können wir M durch p teilen.
Eine $r \times r$ Unterdeterminante der Matrix $\|f_{ij}\|$, $i = 1, \ldots, r$, $j = 1, \ldots, t$ ist $\not\equiv 0$ mod p. Sei das z.B. die folgende Determinante

$$\Delta = \begin{vmatrix} f_{11} & \cdots & f_{1r} \\ \vdots & \ddots & \vdots \\ f_{r1} & \cdots & f_{rr} \end{vmatrix}$$

Dann ist $\Delta l_{r+i} \in (l_1, \cdots, l_r) + p\,(M : p)$, wobei der totale Grad von $\Delta \leq rq$ ist.
Sei nun $l \in R_S M \cap \sum RZ_i$, also gibt es ein $s(x) \in S$ mit $sl = a_1 l_1 + \cdots + a_s l_s$. Und sei $\Delta = \Delta_1 + \Delta_2 p$, wobei Δ_1 keinen Term $\neq 0$ enthält, der $\equiv 0$ mod p ist. Dann ist die Summe der Terme höchsten Grades in $D = \Delta_1^b \not\equiv 0$ mod p. Wir erinnern uns, dass $p^b Z_i \in M$ ist für jedes i. Dann liegt auch Dl_{r+i} in $(l_1, \cdots, l_r) + p(M : p)$ für jedes i, wobei der $total\ deg(D) := m \leq brq$ ist. Wir hätten gerne x_n^m mit Koeffizient 1 in D. Um das zu erreichen machen wir eine generische lineare Transformation $x_i = u_{i1}x_1' + \cdots + u_{in}x_n'$ und wählen dann die Koeffizienten $u_{ij} \in \mathbb{Z}[x]$ dementsprechend.
Der Koeffizient von ${x'_n}^m$ in D ist die Summe D_0 der Terme des Grades m

in $D(u_{1n}, \ldots, u_{nn})$ und somit $\not\equiv 0 \bmod p$.
Nun wollen wir die u_{ij} so wählen, dass $D_0\, det(u_{ij})$ ein Element $t \in S$ bestimmt. Da $\mathbb{Z}[x]/\langle p\rangle$ unendlich ist, stellt das keine Schwierigkeit dar.
Sei nun $T = \{t^k \mid k \in \mathbb{N}_0\}$ das durch t erzeugte multiplikative System. Es gilt, dass $\mathbb{Z}[x]_T[x_1, \ldots, x_n] = \mathbb{Z}[x]_T[x'_1, \cdots, x'_n]$ ist. Wir können also ab jetzt über $\mathbb{Z}[x]_T$ arbeiten, denn sobald wir $R_S M \cap R_T Z_i$ haben, bekommen wir auch $R_S M \cap R Z_i$. Denn für einen gegebenen Untermodul N von $\sum R_T Z_i$ können wir $N \cap \sum R Z_i$ konstruieren: Ist nämlich N^* ein Untermodul von $\sum R Z_i$ dessen Erweiterung $(N^*)^e = N$ ist, so ist die gesuchte Kontraktion die Saturierung $(N^* : t^\infty)$ von $(N^* : t)$. Also können wir, indem wir über $\mathbb{Z}[x]_T$ arbeiten annehmen, dass D ein Monom x_n^m enthält und nachdem wir dafür gesorgt haben, dass sein Koeffizient t war, ist dieser nun sogar 1.[2]

Nun müssen wir die Gleichungen $sl = a_1 l_1 + \cdots + a_s l_s$ als Kongruenzen mod p $(M : p^k)$ für $k = 1, \ldots, b-1$ betrachten, wobei kein Term $\neq 0$ in $a_i \equiv 0 \bmod p$ sein darf. Für jedes k muss eine passende lineare Transformation der Koordinaten gefunden werden. Leider können wir hier nicht iterativ vorgehen, da die späteren Arrangements die früheren stören. Wir brauchen eine einzige Transformation, die sowohl für M als auch für $(M : p), \ldots, (M : p^{b-1})$ nützlich ist:
Sei dann $\{l'_{1'}, \ldots, l'_{s'}\}$ eine berechnete Basis von $(M : p)$, $\{l''_1, \ldots, l''_{s''}\}$ eine für $(M : p^2)$; etc. Wir wollen im Allgemeinen die zu $(M : p)$, $(M : p^2)$; etc. gehörenden Objekte wie die Basen kennzeichnen. Auch hier wählen wir aus $\{l'_{1'}, \ldots, l'_{s'}\}$ eine Teilmenge $\{l'_{1'}, \ldots, l'_{r'}\}$ aus, die über $\mathbb{Z}[x, x_1, \ldots, x_n]$ modulo p linear unabhängig ist. Dasselbe machen wir mit $\{l''_1, \ldots, l''_{s''}\}$; etc. Seien dann $\Delta', \Delta'', \ldots, D', D'', \ldots$ wie im letzten Abschnitt.
Dann führen wir eine generische lineare Koordinatentransformation $x_i = u_{i1}x'_1 + \cdots + u_{in}x'_n$ durch und wählen dann die Koeffizienten u_{ij} so, dass $D_0 \cdot D'_0 \cdot D''_0 \cdots det(u_{ij})$ ein $t \in S$ bestimmt.
Dann sei T das multiplikative System, das durch dieses t erzeugt wird und wir arbeiten nun über $\mathbb{Z}[x]_T$.
Wir bemerken noch, dass die Determinanten $\Delta', \Delta'', \ldots$ nicht unbedingt von den ersten $r', r'', \ldots$ Spalten von $\|f'_{ij}\|$, $\|f''_{ij}\|$, etc. zu kommen brauchen. Dies könnte man aber auch durch eine weitere generische lineare Koordinatentransformation der Z_j erreichen.

Mit den vorhergehenden Vorbereitungen sei $R' = \mathbb{Z}[x, x_1, \ldots, x_{n-1}]$, wobei natürlich $n \geq 1$ sein muss. Sei dann N eine ganze Zahl und wir betrachten den R'-Modul M', der durch die $l_i x_n^j$, $i = 1, \ldots, s$, $j = 0, \ldots, N$ erzeugt wird. M' ist ein Untermodul des freien R'-Moduls $\mathcal{M} = \sum R'(Z_i x_n^j)$, $i = 1, \ldots, t$

[2] A. Seidenberg hat hier die Abbildung beschrieben, die in [GP07] bei der Primärzerlegung eines Ideals über einem Körper dazu benutzt wurde, das Ideal in allgemeine Lage zu bringen. Allerdings werden hier dabei noch mehr Faktoren berücksichtigt, welche die gesamte Situation vereinfachen.

und $j = 0, \ldots, N + q$ als freie Erzeugende hat.
Nun konstruieren wir ein N, so dass gilt:

$$R_S M \cap \sum R_T Z_i = R_T M + \left(R'_S M' \cap \sum R'_T Z_i X_n^j\right),$$

für $j = 0, \ldots, N + q$, um eine Variable zu eliminieren. Wir haben $sl = a_1 l_1 + \cdots + a_s l_s \bmod p\,(M : p)$, wobei kein Term $\neq 0$ in den $a_i \equiv 0 \bmod p$ ist. Da $D\, l_{r+i} \in (l_1, \ldots, l_r) + p\,(M : p)$ ist, können wir annehmen, dass $deg(a_i) < m \leq brq$ ist für $i = r + 1, \ldots, s$. Wir haben in M auch Elemente der Form $\Delta Z_i + b_{ir+1} Z_{r+1} + \cdots + b_{it} Z_t$, und Elemente der Form $DZ_i + b'_{ir+1} Z_{r+1} + \cdots + b'_{it} Z_t$ für $i = 1, \ldots, r$.
Sei nun $l = g_1 Z_1 + \cdots + g_t Z_t = l^{(0)} + l^{(1)} p + \cdots + l^{(b-1)} p^{b-1}$. Wir können annehmen, dass kein Term ungleich 0 in $l^{(0)}$ in $\langle p \rangle$ ist. Da wir $l \bmod M$ betrachten, indem wir die Elemente $DZ_i + b'_{ir+1} Z_{r+1} + \cdots + b'_{it} Z_t$ in M benutzen, können wir auch annehmen, dass die Koeffizienten von $Z_1, \ldots, Z_r$ in $l^{(0)}$ kleineren Grades als $deg(D)$ sind. Ausserdem gilt für die g_i, dass $sg_i \equiv a_1 f_{1i} + \cdots + a_s f_{si} \bmod p$ ist für $i = 1, \ldots, r$. Sei nun F_{ki} der Kofaktor von f_{ki} in Δ. Dann gilt:

$$\sum_{i=1}^{r} sg_i F_{ki} \equiv a_k \Delta + \sum_{i=1}^{r} \sum_{j>r} a_j f_{ji} F_{ki} \bmod p$$

Ersetzen wir die g_i durch $g_i^{(0)}$, die Summe der Terme der g_i in $l^{(0)}$. Dann ist $deg(a_k) < deg(D) + rq \leq (b+1)rq$ und somit $deg(a_i) < (b+1)rq$ für $i = 1, \ldots, s$.
Vergleichen wir nun die beiden Seiten von $sl \equiv a_1 l_1 + \cdots + a_s l_s \bmod p\,(M : p)$, erkennen wir, dass die Koeffizienten von $Z_1, \ldots, Z_t$ in $l^{(0)}$ von kleinerem Grad als $(b+1)\,rq + q$ in x_n sind.

Schreibe nun $sl \equiv a_1 l_1 + \cdots + a_s l_s + p(a'_1 l'_1 + \cdots + a'_{s'} l'_{s'}) \bmod p^2\,(M : p^2)$, wobei die Reduktionen des letzten Abschnitts immer noch gelten und kein Term in a'_i, der nicht gleich Null ist gleichzeitig $\equiv 0 \bmod p$ ist. Mit der gewählten Notation haben wir $D' l'_{r'+i} \in (l'_1, \cdots, l'_{r'}) + p\,(M : p^2)$. Wir können somit annehmen, dass $deg(a'_i) < deg(D') \leq br'q'$ ist für $i = r'+1, \ldots, s'$. Benutzen wir nun Elemente $D' Z_i + b'_{ir'+1} Z_{r'+1} + \cdots + b'_{it} Z_t$ für $i = 1, \cdots, r'$, so können wir annehmen, dass die Koeffizienten von $Z_1, \cdots, Z_{r'}$ kleineren Grad in x_n haben als $deg(D')$. Diese Reduktion ändert nichts an $l^{(0)}$ und wir erhalten

$$sg_i \equiv a_1 f_{1i} + \cdots + a_s f_{si} + p\,(a'_1 f'_{1i} + \cdots + a'_{s'} f'_{s'i}) \bmod p^2$$

Ist nun F'_{ki} der Kofaktor von f'_{ki} in Δ', so ist

$$\sum_{i=1}^{r'} s(g_i^{(0)} + p g_i^{(1)}) F'_{ki} \equiv \sum a_j f_{ji} F'_{ki} + p \left(a'_k \Delta' + \sum_{i=1}^{r'} \sum_{j>r'} a'_j f'_{ji} F'_{ki} \right) \bmod p^2$$

wobei die $g_i^{(0)}$ und die $g_i^{(1)}$ die Summe der Terme der g_i sind die in $l^{(0)}$ und $l^{(1)}$ erscheinen. Dann ist $deg(a'_k) < (b+1)rq + (b+1)r'q' + q$ und somit $deg(a'_i) < (b+1)(rq + r'q') + q$ für $i = 1, \cdots, s'$.
Sei nun $q* = max\{q, q', \cdots\}$. Vergleichen wir dann die beiden Seiten von $sl \equiv a_1 l_1 + \cdots + a_s l_s + p(a'_1 l'_1 + \cdots + a'_{s'} l'_{s'}) \bmod p^2 (M : p^2)$, so sehen wir, dass die Koeffizienten von $Z_{r'+1}, \ldots, Z_t$ sowie von $Z_1, \cdots, Z_{r'}$ in $l^{(1)}$ von kleinerem Grad als $(b+1)(rq + r'q') + 2q*$ sind. Wiederholen wir dasselbe Argument einige Male, so finden wir ein N_1 mit dem wir den Grad der $a_i^{(j)}$ in

$$sl \equiv a_1 l_1 + \cdots + a_s l_s + \sum_{i=1}^{b-1} p^i (a_1^i l_1^i + \cdots + a_s^i l_s^i) + p^b m$$

begrenzen können. Und ausserdem ist $deg(g_i) \leq N_1 + q*$. Dann ist der Grad des Koeffizienten h_i von Z_i in m ebenso $\leq N_1 + q*$.
Beziehen wir die $p^b Z_i$ unter den l_i mit ein, so können wir annehmen, dass $m = 0$ ist. So sind nun $deg(a_i^{(j)})$ und $deg(g_i) \leq N_1 + q*$.
Sei $p^i l_j^{(i)} = \sum_{k=1}^{s} h_{jk}^{(i)} l_k$ und sei $N_2 = max\{deg(h_{jk}^{(i)})\}$. Dann können wir einfach $sl = a_1 l_1 + \cdots + a_s l_s$ schreiben, wobei $N = N_1 + N_2 + q*$ den Grad der a_i begrenzt. Dann ist $N = N_1 + N_2 + q*$ unsere gesuchte ganze Zahl mit

$$R_S M \cap \sum R_T Z_i = R_T M + \left(R'_S M' \cap \sum R'_T Z_i x_n^j \right)$$

und wir haben n um eins reduziert.

q.e.d.

Korollar 22 (Sei78) *Die Theoreme* 19 *und* 21 *und das Korollar* 20 *gelten auch für* $\mathbb{Z}[y_1, \cdots, y_c]$ *an der Basis anstelle von* $\mathbb{Z}$*, mit der weiteren Annahme, dass* $(M : f) = M$ *ist für jedes* $f \not\equiv 0$ *mod* p *in* $\mathbb{Z}[y_1, \cdots, y_c]$.

Die Beweise sind fast dieselben wie für $c = 0$. Im Fall $n = 0$, $t = 1$ haben wir es mit einem Ideal A in $\mathbb{Z}[y_1, \cdots, y_c, x]$ zu tun. Seine assoziierten Primideale sind von der Dimension $\geq c$ und wir suchen die c-dimensionalen. Ist $A \not\equiv 0 \bmod p$, so läuft der Beweis fast gleich wie für $c = 0$. Ist $A \equiv 0 \bmod p$ und $A = p^r A_1$ mit $A_1 \not\equiv 0 \bmod p$, so werden wir zuerst beobachten, dass $(A_1 : f) = A_1$ ist für jedes $f \not\equiv 0 \bmod p$ in $\mathbb{Z}[y_1, \cdots, y_c]$ und dass dann auch jedes c-dimensionale assoziierte Primideal von A ein assoziiertes Primideal von A_1 ist. Alles weitere ist dann wie für $c = 0$, ausser dass wir $\mathbb{Z}$ durch $\mathbb{Z}[y_1, \cdots, y_c]$ ersetzen.

3.2.4 Assoziierte Primideale

Der nächste Schritt zur Primärzerlegung der Ideale C_i ist nun die Konstruktion ihrer assoziierten Primideale. In den theoretischen Grundlagen hatten wir gezeigt, dass ein Ideal in einem noetherschen Ring immer als Schnitt endlich vieler Primärideale dargestellt werden kann. Da wir unseren Algorithmus aber von einer anderen Seite aufgezogen haben, müssen wir hier noch zeigen, dass wir es auch bei den assoziierten Primidealen eines Ideals nur mit einer endlichen Anzahl tun haben. Also benötigen noch ein weiteres Lemma:

Lemma 23 (Sei78) *Sei $I \subset A = \mathbb{Z}[x_1, \ldots, x_n]$ ein Ideal, das eine Potenz einer Primzahl p enthält und so dass $(I : P) = I$ ist für jedes Primideal $P \supset I$ kleinerer Dimension als c. Dann hat I nur eine endliche Anzahl c-dimensionaler assoziierter Primideale.*

Beweis: Sei zuerst $c = 0$ und sei S_i die Menge der Elemente $\not\equiv 0 \bmod p$ in $\mathbb{Z}[x_i]$. Wir wissen nun, wie wir ein $s_i(x_i) \in S_i$ finden können, so dass $A_{S_i} I \cap A = (I : s_i)^\infty = (I : s_i)^\varrho$ ist.
Sei nun P ein 0-dimensionales assoziiertes Primideal von I, und sei $f_i(x_i)$ ein mod p irreduzibles Polynom aus P. Da $(I : P) \supseteq I$ ist, können wir ein $a \in (I : P)$ wählen das nicht in I liegt. Dann ist $af_i \in I$ und $as_i^\varrho \in I$ für ein großes ϱ. Daraus folgt, dass mod p betrachtet s_i durch f_i teilbar ist und dass $s_i \in P$.
Also ist $\langle p, s_1, \ldots, s_n \rangle \subset P$, womit für P nur eine endliche Anzahl Kandidaten in Frage kommen.
Sei P nun für $c > 0$ ein c-dimensionales Primideal. Da $\langle p \rangle$ das einzige n-dimensionale Primideal ist können wir annehmen, dass $c < n$ ist.
Irgendwelche c der x_i, zum Beispiel $x_1, \ldots, x_c$ sind algebraisch unabhängig über $\mathbb{Z}/\langle p \rangle$ mod $P/\langle p \rangle$. Sei S_{12} die Menge der Elemente $\not\equiv 0 \bmod p$ in $\mathbb{Z}[x_1, x_2]$. Laut Korollar 15 haben wir $I_1 = (I : s_1^\varrho) = A_{S_1} I \cap A$ für ein genügend großes ϱ und wenden wir das gleiche Korollar nun auf I_1 an, so finden wir ein $s_{12} \in S_{12}$ so dass $A_{12} I_1 \cap I = (I_1 : s_{12}^\varrho)$ ist für ein genügend großes ϱ. Also ist $A_{S_{12}} I \cap A = (I : (s_{12} s_1)^\varrho)$ für ein großes ϱ. Wenn wir auf diese Weise fortfahren erhalten wir ein $s = s_{12\cdots c} \in S_{12\cdots c}$, der Menge der Elemente $\not\equiv 0 \bmod p$ in $\mathbb{Z}[x_1, \cdots, x_c]$, so dass $A_{S_{12\cdots c}} I \cap A = (I : s_{12\cdots c}^\varrho)$ für ein großes ϱ ist.
Nun nehmen wir an, dass $I = (I : P^\varrho) \cap (I : s^\varrho)$ für jedes ϱ ist. Um das zu zeigen, sei nun ein $b \in (I : P^\varrho) \cap (I : s^\varrho)$. Dann ist $b\langle s^\varrho, P^\varrho \rangle \subset I$.
Das Ideal $\langle p, s^\varrho, P^\varrho \rangle / \langle p \rangle$ enthält in $\mathbb{Z}[x_1, \ldots, x_n]/\langle p \rangle$ eine Potenz des Produktes seiner minimalen assoziierten Primideale. Somit enthält $\langle s^\varrho, P^\varrho \rangle$ in $\mathbb{Z}[x_1, \ldots, x_n]$ ein Produkt $P_1 \cdots P_s$ von Primidealen, so dass jedes P_i von geringerer Dimension als c ist und I enthält. Dann ist $b \in (I : P_1 \cdots P_s) = I$ und die Behauptung gezeigt.

Da aus $(I : s^\varrho P') \supseteq (I : s^\varrho)$ folgt, dass $(I : P') \supseteq I$ ist, sehen wir, dass $(I : s^\varrho P') = (A : s^\varrho)$ gilt für jedes Primideal P' kleinerer Dimension als c. Für großes ϱ gilt aber auch $(I : P) = (I : P^\varrho) \cap (I : s^\varrho) : P$. Also ist für $(I : P) \supseteq I$ auch $((I : s^\varrho) : P) \supseteq (I : s^\varrho)$. Damit ist jedes c-dimensionale zu I assoziierte Primideal auch zu $(I : s^\varrho)$ assoziiert.
Nun folgern wir also genau wie für $c = 0$, dass $(I : s^\varrho)$ und somit auch I nur eine endliche Anzahl c-dimensionaler assoziierte Primideale P hat, für die $x_1, \ldots, x_c$ algebraisch unabhängig über $\mathbb{Z}/\langle p\rangle$ mod $P/\langle p\rangle$ sind. Da dies für jede beliebige Wahl von c der $x_1, \ldots, x_n$ gilt, ist das Lemma bewiesen.

q.e.d.

Nun können wir die Definition eines assoziierten Primideals eines gegebenen Ideals I wie folgt vervollständigen:

Definition 24 *Ein O-dimensionales Primideal P welches das Ideal I enthält heisst ein zu I assoziiertes Primideal, falls $(I : P) \supseteq I$ ist.*

Durch das vorhergehende Lemma wissen wir, dass es davon nur endlich viele gibt und nennen diese $P_1, \cdots, P_S$. Sei nun $I_1 = (I : \langle P_1 \cdots P_s\rangle^\varrho))$ für ein großes ϱ. Dann ist $(I_1 : P) = I_1$ für jedes 0-dimensionale I_1 enthaltende Ideal, da aus $(I_1 : P) \supseteq I_1$ folgt, dass $(I : P) \supseteq I$. Das würde dann wiederum heissen, dass P eines der P_i ist wobei $(I_1 : P_i) = I_1$. So sind die 1-dimensionalen assoziierten Primideale von I nun definiert als die 1-dimensionalen assoziierten Primideale von I_1. Laut dem Lemma 23 sind auch das endlich viele und wir nennen sie $P_{s+1}, \ldots, P_t$.
Dann setzen wir $I_2 = (I : \langle P_1 \cdots P_s\rangle^\varrho)$ für ein großes ϱ. Ist P ein 0-dimensionales Ideal, das I_2 und somit auch I enthält, so wissen wir, dass $(I : \langle P_1 \cdots P_s\rangle^\varrho P) = (I : \langle P_1 \cdots P_s\rangle^\varrho)$ für ein genügend großes ϱ ist und somit auch $(I_2 : P) = I_2$. Und ist P eines der $P_{s+1}, \cdots, P_t$, so gilt

$$(I_2 : P) = I : \langle P_1 \cdots P_t\rangle^\varrho P) \subset (I : \langle P_1 \cdots P_t\rangle^{\varrho+1} = (I : \langle P_1 \cdots P_t\rangle^\varrho = I_2,$$

da wir ϱ genügend groß gewählt haben. Also ist $(I_2 : P) = I_2$ für jedes 0- oder 1-dimensionale Primideal $P \supset I_2$. Damit sind die 2-dimensionalen assoziierten Primideale von I als die 2-dimensionalen assoziierten Primideale von I_2 definiert.
Fahren wir in dieser Art und Weise fort, so definieren wir die c-dimensionalen assoziierten Primideale von I für jedes $c \in \{0, \cdots, n\}$ und diese sind per Definition die assoziierten Primideale von I. Wir sehen leicht, dass es nur endlich viele sind. Dass wir sie auch konstruieren können ist die Aussage des folgenden Theorems.

Theorem 25 (Sei78) *Zu einem gegebenen Ideal I in $A = \mathbb{Z}[x_1, \ldots, x_n]$ kann man seine assoziierten Primideale konstruieren.*

Beweis: Wir können annehmen, dass I eine Potenz einer Primzahl p enthält.
Zuerst suchen wir die 0-dimensionalen assoziierten Primideale:
Sei S_i das multiplikative System der Elemente in $\mathbb{Z}[x_i]$ die $\not\equiv 0 \bmod p$ sind.
Nach dem Korollar 18 sei $s_i(x_i) \in S_i$ so, dass $A_{S_i} I \cap A = (I : s_i^{\varrho})$ ist für ein genügend großes ϱ.
Jedes 0-dimensionale assoziierte Primideal P von I enthält ein mod p irreduzibles Element $s(x_i)$. Dann gibt es ein $f \notin I$ mit $s(x_i)f \in I$, also ist $s_i^{\varrho}(x_i)f \in I$ für ein großes ϱ und es folgt, dass $s_i(x_i)$ mod p-teilbar ist durch $s(x_i)$. Also enthält auch P das $s_i(x_i)$.
Man kann also sagen, dass P das Ideal $\langle p, s_1(x_1), \ldots, s_n(x_n)\rangle$ enthält. Betrachten wir das mod p , so gibt es nur eine endliche Anzahl Kandidaten für P und wir haben die 0-dimensionalen assoziierten Primideale zu I gefunden.
Teilen wir nun I durch eine große Potenz des Produktes der 0-dimensionalen assoziierten Primideale, so können wir annehmen, dass I keine solchen hat.
Also suchen wir die 1-dimensionalen:
In jedem assoziierten Primideal P der Dimension ≥ 1 von I ist mindestens ein $s_i(x_i)$ nicht enthalten. P ist dann aber ein assoziiertes Primideal von $B_i = (I : s_i^{\varrho})$ für ein großes ϱ. Wenden wir nun das Korollar 22 zu den Lemmatas mit $\mathbb{Z}[x_i]$ an der Basis an, so finden wir die 1-dimensionalen assoziierten Primideale von B_i und somit auch von I.
Danach finden wir mit analogem Vorgehen die höher dimensionalen Primideale.

q.e.d.

ALGORITHMUS (ZASSPRIMES(I)):

INPUT: Ein Ideal $I = \langle f_1, \ldots, f_k\rangle \subset \mathbb{Z}[x_1, \ldots, x_n]$ mit $p^b \in I$ für eine Primzahl p.

OUTPUT: Primdeale $P_1, \ldots, P_S \in \mathbb{Z}[x_1, \ldots, x_n]$, so dass $\sqrt{I} = \bigcap P_i$ ist für für $i = 1, \ldots, s$.

- RESULT := $\emptyset$;
- WHILE $n \neq 0$ DO:

  FOR $i = 1, \ldots, n$ DO:

  Wähle das s_i aus UNIVARLOC(I) mit $A_{S_i} I \cap A = (I : s_i^{\infty})$;

  Berechne $M = \langle p, s_1(x_1), \ldots, s_n(x_n)\rangle$;

  Betrachte M modulo p und finde Primdeale $P_1, \ldots, P_r \supset M$ mit $(I : P_j) \supseteq I$ für $i = 1, \ldots, r$;

RESULT = RESULT $\cup \{P_1, \ldots, P_r\}$;

Setze $I = (I : \langle P_1 \cdots P_r \rangle^\infty)$;

Wähle das s_i mit $(I : s_i) \supseteq I$;

Setze $I = (I : s_i^\infty)$ und
$\{s_1(x_1), \ldots, s_n(x_n)\} = \{s_1(x_1), \ldots, s_n(x_n)\} \setminus s_i$;

Setze $n = \#\{s_1(x_1), \ldots, s_n(x_n)\}$;

- RETURN RESULT.

In diesem Algorithmus haben wir folgende Eigenschaften von assoziierten Primidealen benutzt:

Korollar 26 (Sei78) *Ist P ein zu einem Ideal I assoziiertes Primideal, so ist $I \subset P$ und $(I : P) \supseteq I$. Ist P ein Primideal mit $(I : P) \supseteq I$, so ist P in einem zu I assoziierten Primideal enthalten.*

Beweis: Die erste Behauptung folgt direkt aus der Definition der assoziierten Primideale.
Sei nun $(I : P) \supseteq I$ mit einem c-dimensionalen Primideal P. Wir nehmen an, dass die erste Behauptung für Primideale kleinerer Dimension als c richtig ist. Diese seien $P_1, \ldots, P_S$ und keines dieser P_i enthalte P. Dann ist $I = (I : P^\varrho) \cap (I : (P_1, \ldots, P_s)^\varrho)$ für jedes ϱ:
Sei $b \in (I : P^\varrho) \cap (I : (P_1, \cdots, P_s)^\varrho)$. Dann ist $b(P^\varrho, (P_1, \ldots, P_s)^\varrho)) \subset I)$. Das Ideal $(P^\varrho, (P_1, \ldots, P_s)^\varrho))$ enthält ein Produkt von Primidealen $P_1' \cdots P_t'$, wobei jedes der P_i' von kleinerer Dimension als c das Ideal I enthält. Ausserdem soll keines der P_i' in einem der $P_1, \ldots, P_s$ enthalten sein. Also ist $b \in (I : (P_1', \ldots, P_t')) = I$ und die behauptete Gleichung ist bewiesen.
Betrachte nun für ein großes ϱ

$$(I : P) = (I : P^\varrho) \cap (I : (P_1 \cdots P_s)^\varrho P)$$

wobei $(I : (P_1 \cdots P_s)^\varrho P) \supseteq (I : (P_1 \cdots P_s)^\varrho)$ ist. Dann ist P ein c-dimensionales Primideal von I und der Beweis ist vollständig.

q.e.d.

Korollar 27 (Sei78) *Ist $A \neq (1)$, so hat I mindestens ein assoziiertes Primideal. Hat I genau ein assoziiertes Primideal P und ist $(I : P^r) = (I : P^{r+1})$ für ein $r \in \mathbb{N}$, so ist $P^r \subset I$ und I ist ein Primärideal. Umgekehrt hat ein Primärideal nur ein assoziiertes Primideal.*

Beweis: Hier haben wir es mit einem Ideal zu tun, das eine Potenz einer Primzahl p enthält. $(I : \langle p \rangle) \supseteq I$ also folgt mit dem letzten Korollar, dass $\langle p \rangle$ in einem zu I assoziierten Primideal enthalten ist. Das beweist die erste Aussage.
Habe nun I nur ein assoziiertes Primideal P. Ist $(I : P^r) = (I : P^{r+1})$, so hat $(I : P^r)$ kein assoziiertes Primideal und $(I : P^r) = (1)$ und $P^r \subset I$.
Ist nun $ab \in I$ und $a \notin I$, so ist $b \in P$ und damit $b^r \in I$. Denn sonst wäre $(I : (P^r, b)) \supseteq I$. Da (P^r, b) ein Produkt von Primidealen $P_1' \cdots P_t'$ enthält, von denen jedes Primideal P echt enthält, erhalten wir $(I : (P_1' \cdots P_t') \supseteq I$ und $(I : P_i') \supseteq I$ für ein i, was unmöglich ist. Also haben wir die zweite Aussage bewiesen.
Umgekehrt sei I primär und $P_1, \ldots, P_s$ seine assoziierten Primideale. P_1 sei das maximale davon. Dann ist $(I : P_1) \supseteq I$. Sei nun $a \in (I : P_1)$, $a \notin I$. Dann ist $aP_1 \subset I$ und es folgt, dass $P_1^r \subset I$ für ein $r \in \mathbb{N}$. Da $I \subset P_i \ \forall i$ ist, muss $P_1 \subset P_i$ sein und somit $P_1 = P_i$ und $s = 1$.

q.e.d.

3.2.5 Die allgemeine Primärzerlegung

Nun haben wir die notwendigen Werkzeuge zur algorithmischen Umsetzung dessen was uns ursprünglich interessiert hat, die Primärzerlegung eines beliebigen Ideals I in $\mathbb{Z}[x_1, \ldots, x_n]$. Wir gehen dabei von der klassischen Definition aus. Eine Zerlegung eines Ideals $I = Q_1 \cap \cdots \cap Q_s$ ist eine unverkürzbare Primärzerlegung, falls die Q_i Primärideale mit unterschiedlichen assoziierten Primidealen P_i sind und keines der Q_i den Schnitt der anderen Q_j enthält. Kann I als endlicher Schnitt von Primäridealen $Q_1 \cap \cdots \cap Q_s$ geschrieben werden, so erhält man eine unverkürzbare Primärzerlegung, indem man die Q_i mit gemeinsamen Primidealen durch deren Schnitt ersetzt. Die Eindeutigkeit der Primideale in einer Primärzerlegung folgt dann auch auf die gleiche Art und Weise wie im Klassischen:
Sind $Q_1 \cap \cdots \cap Q_s$ und $Q_1' \cap \cdots \cap Q_t'$ zwei verschiedene Primärzerlegungen von I mit jeweiligen assoziierten Primidealen P_i bzw. P_j', dann nehmen wir ein maximales Element der Menge $\{P_1, \ldots, P_s, P_1', \ldots, P_t'\}$, sagen wir dies sei P_s. Ist dann $(I : P_s) \supseteq I$, so ist P_s in einem der P_j' enthalten und somit ist sogar $P_s = P_j'$ für ein j.[3] Sagen wir dies sei P_t'. Dividieren wir dann durch eine große Potenz von P_s, so erhalten wir $Q_1 \cap \cdots \cap Q_{s-1} = Q_1' \cap \cdots \cap Q_{t-1}'$ usw.
Nun wollen wir aber in dem Beweis zum nächsten Theorem die algorithmische Umsetzung einer Primärzerlegung vervollständigen.

[3] Das ist eine Eigenschaft, die unter dem Begriff *prime avoidance* in verschiedenen Werken zur kommutativen Algebra erläutert wird.

Theorem 28 (Sei78) *Kann man für ein gegebenes Ideal I seine assoziierten Primideale konstruieren, so kann man auch eine Primärzerlegung von ihm konstruieren.*
Also kann man für ein beliebiges Ideal $I \subset \mathbb{Z}[x_1, \ldots, x_n]$ eine Primärzerlegung konstruieren.

Beweis: Seien $P_1, \ldots, P_s$ maximale assoziierte Primideale des gegebenen Ideals I. Seien $P'_{i1}, \ldots, P'_{it_i}$ jeweils die zu I assoziierten Primideale, die nicht in P_i enthalten sind. Dann ist $I = \bigcap_i (I : (P'_{i1} \cdots P'_{it_i})^\varrho)$ für ein genügend großes ϱ. Also können wir annehmen, dass I ein einziges maximales assoziiertes Primideal hat, das heisst eines, welches die anderen enthält. Sei dies nun $P = (f_1, \ldots, f_s)$. Nun finden wir ein $r_1 \in \mathbb{N}$ mit $(I : f_1^{r_1}) = (I : f_1^{r_1+1})$. Dann ist $I = (I : f_1^{r_1}) \cap (A, f_1^{r_1})$.
Kein zu $(I : f_1^{r_1})$ assoziiertes Primideal enthält f_1 und jedes zu $(I, f_1^{r_1})$ assoziierte Primideal enthält f_1. Ist P' ein zu $(I, f_1^{r_1})$ assoziiertes Primideal, so ist $(I : f_1^{r_1}) : P' = (I : f_1^{r_1})$. Ist $P' \not\subset P$ so ist $(I : P') = I$. Dann können wir durch eine große Potenz von dem Produkt solcher P' teilen und schreiben $I = (I : f_1^{r_1}) \cap I_1$ wobei P das einzige maximale Ideal von I_1 ist und $f_1^{r_1} \in I_1$.
Nun wiederholen wir das Ganze mit I_1 und f_2. Dann können wir I als $(I : f_1^{r_1}) \cap (I_1 : f_2^{r_2}) \cap (I_1, f_2^{r_2})$ schreiben. Ist P' ein zu $(I_1, f_2^{r_2})$ assoziiertes Primideal, so ist $(I_1 : f_2^{r_2}) : P' = (I_1 : f_2^{r_2})$ und ist $P' \not\subset P$, dann ist $(I : P') = I$. Also dividieren wir durch eine Potenz solcher P' und erhalten $I = (I : f_1^{r_1}) \cap (I_1 : f_2^{r_2}) \cap I_2$ wobei P das einzige maximale Ideal von I_2 ist und $f_1^{r_1}, f_2^{r_2} \in I_2$.
So gehen wir weiter vor, bis wir folgende Zerlegung erhalten:

$$I = (I : f_1^{r_1}) \cap (I_1 : f_2^{r_2}) \cap \cdots \cap (I_{s-1} : f_s^{r_s}) \cap I_s$$

Jedes zu I_s assoziierte Primideal ist in P enthalten und enthält $f_1, \ldots, f_s$ womit es gleich P ist.
Also ist I_s laut Korollar 20 primär mit P als assoziiertem Primideal. Der Schnitt $B = (I : f_1^{r_1}) \cap (I_1 : f_2^{r_2}) \cap \cdots \cap (I_{s-1} : f_s^{r_s})$ hat Primideale, die echt in P enthalten sind. Also ist $B = (I : P^\varrho)$ für ein genügend großes ϱ.
Wir haben also $I = (I : P^\varrho) \cap I_s$. Nun wiederholen wir dieses Argument bis wir eine Primärzerlegung von I erhalten haben.

q.e.d.

Als Algorithmus in Pseudocode sieht das wie folgt aus:

ALGORITHMUS (ZpPRIMDEC(I)):

INPUT: Ein Ideal $I = \langle f_1, \ldots, f_k \rangle$ und Primideale $P_1, \ldots, P_S$ in $\mathbb{Z}[x_1, \ldots, x_n]$ mit $p^b \in I$ für eine Primzahl p.

OUTPUT: Primärideale $Q_1, \ldots, Q_S \in \mathbb{Z}[x_1, \ldots, x_n]$, so dass $I = \bigcap Q_i$ ist für $i = 1, \ldots, s$.

- RESULT $:= \emptyset$ und $S = \{I\}$;
- Setze $I = \bigcap_i (I : (P'_{i1} \cdots P'_{it_i})^\infty)$ wobei $P'_{i1}, \ldots, P'_{it_i}$ die assoziierten Primideale von I sind, die nicht in P_i enthalten sind für $i = 1, \ldots, s$;
- Finde nun das einzige assoziierte Primideal $P \supset I$ und berechne eine Standardbasis $f_1, \ldots, f_s$ von P;

  FOR $i = 1, \ldots, s$ DO:

  Berechne die Saturierung $(I : f_i^{r_i}) = (I : f_i^{r_i+1})$;

  Schreibe $I = (I : f_i^{r_i}) \cap (I, f_i^{r_i})$;

  Berechne ZASSPRIMES$((I, f_i^{r_i}))$ und erhalte Primideale P'_j;

  Setze $I_i = ((I, f_i^{r_i}) : \prod P'_j)^\infty$ und $S = S \cup \{I_i\}$;

  Setze $I = I_i$;
- Setze $I = (I : f_1^{r_1}) \cap (I_1 : f_2^{r_2}) \cap \cdots \cap (I_{s-1} : f_s^{r_s})$ und $I_s = Q_s$;
- RESULT = RESULT $\cup \{Q_s\}$;
- RETURN RESULT.

Der ganze Vorgang wird dann auf $(I : f_1^{r_1}) \cap (I_1 : f_2^{r_2}) \cap \cdots \cap (A_{s-1} : f_s^{r_s})$ angewandt, u.s.w., bis wir nur noch Primärideale haben.
Die Primärzerlegung eines beliebigen Ideals $I \subset \mathbb{Z}[x_1, \ldots, x_n]$ bekommen wir also, indem wir erst den Algorithmus SPLITTING(I) anwenden. Ist $B \neq \mathbb{Z}[x_1, \ldots, x_n]$, so zerlegen wir den Teil B aus $I = B \cap C$ mittels der beschriebenen Erweiterung nach $\mathbb{Q}[x_1, \ldots, x_n]$ in Primärideale $B_1 \cap \cdots \cap B_t$. Andernfalls teilen wir das Ideal C mit SPLITTING(C) in die C_i auf, die wir mit ZpPRIMDEC(C_i) in Primärideale C_{ij} zerlegen. Unsere gesuchte Primärzerlegung ist dann der Schnitt der C_{ij}.

Anhang

October 4, 2010

A Ideale und Moduln

Hier werden weitere Definitionen und Zusamenhänge zur Ring- und Modultheorie erwähnt, die zum Verständnis einer Primärzerlegung im arithmetischen Fall benötigt werden. Im ersten Teil gehen wir auf Quotienten von Idealen und deren Saturierungen ein, im zweiten Teil erinnern wir an assoziierte Primideale und Dimensionsbegriffe, im dritten Teil geht es um Moduln und im Speziellen Syzygienmoduln. Bei einigen Objekten betrachten wir auch deren geometrische Interpretation. Grundlegende Kenntnisse über Ringe und Moduln werden vorausgesetzt. Bei den fehlenden Beweisen verweisen wir auf die jeweils erwähnte Literatur.

A.1 Quotienten von Idealen und deren Saturierung

Bei der Konstruktion einer Primärzerlegung eines Ideals $I \subset R[x, \ldots, x_n]$ mit einem beliebigen Ring R wird zu einem großen Teil mit Quotienten von Idealen und Moduln und deren Saturierung gearbeitet. Deswegen wenden wir uns erst mal diesen Begriffen zu.

Definition 29 (GP07, Kap.1.8.8) *Seien I, J Ideale eines noetherschen Ringes R oder Untermoduln eines R-Moduls M. Dann ist der Quotient von I nach J definiert als*

$$(I : J) := \{r \in R : rJ \subset I\}$$

Offensichtlich gilt

$$(I : \langle b_1, \cdots, b_s\rangle) = \bigcap_{i=1}^{s} (I : \langle b_i\rangle)$$

Betrachten wir den Quotienten von I nach Potenzen von J

$$I = (I : J) \subset (I : J^2) \subset \cdots R$$

Da R noethersch ist, gibt es ein $s \in \mathbb{N}$ mit $(I : J^s) = (I : J^{s+i}) \quad \forall i \geq 0$. So ein s genügt

$$(I : J^\infty) := \bigcup_{i \geq 0} (I : J^i) = (I : J^s)$$

und $(I : J^s)$ nennt man die *Saturierung* von I nach J. Das minimale derartige s heisst *Saturierungsexponent*. Ist I ein Radikalideal, so ist der Saturierungsexponent 1.

Der Quotient und die Saturierung des Untermoduls eines Moduls werden analog definiert. Man kann die Erzeugenden eines Untermoduls eines freien R-Moduls R^k als Vektoren mit k Einträgen betrachten. Darauf werden wir aber nicht weiter eingehen. In [AL], Kapitel 3 und in [GP07], Kapitel 2 sind die Theorie und algorithmische Umsetzungen zu diesem Thema ausführlich beschrieben.

Beispiel 8 $R = \mathbb{Z}[x, y]$, $I := \langle xy^2, y^3 \rangle$, $J := \langle x, y \rangle$
$(I : J) = (I : J^\infty) = (\langle xy^2, y^3 \rangle : \langle x, y \rangle) = \langle y^2 \rangle$

Trotzdem ist I in diesem Fall kein Radikalideal, denn $\sqrt{I} = \langle xy^2, y \rangle \neq I$. Nun noch einige Eigenschaften von Idealquotienten:

Lemma 30 (GP07, Lemma 1.8.14.) *Sei R ein Ring und I, J, K Ideale in R. Dann gilt*

(1) $(I \cap J) : K = (I : K) \cap (J : K)$ *im Speziellen gilt* $(I : K) = (I \cap J) : K$, *falls* $K \subset J$ *ist.*

(2) $(I : J) : K = (I : J \cdot K)$

(3) Ist I ein Primideal und $J \not\subset I$, dann ist $(I : J^j) = I$ *für* $j > 0$.

(4) Ist $I = \bigcap_{i=1}^r P_i$ *mit Primidealen* P_i *, dann ist* $(I : J^\infty) = (I : J) = \bigcap_{J \not\subset P_i} P_i$.

Diese Punkte sind für die geometrische Betrachtung von Quotienten und Saturierungen interessant. Im Punkt (4) haben wir es mit der Zerlegung eines Radikalideals zu tun. Dann ist

$$V(I) = \cup_{i=1}^r V(P_i).$$

Ausserdem ist genau dann $J \subset P_i$, wenn $V(P_i)$ ein abgeschlossenes Unterschema von $V(J)$ ist. Somit ist die Varietät $V(I : J)$ definiert durch

$$V(I : J) = \bigcup_{V(P_i) \not\subset V(J)} V(P_i).$$

Mit anderen Worten ist dann $V(I:J)$ der Zariski-Abschluss von $V(I)\backslash V(J)$.

A.2 Assoziierte Primideale und Dimensionsbegriffe

Bei der algorithmischen Primärzerlegung im arithmetischen Fall werden die assoziierten Primideale des zu zerlegenden Ideals sukzessiv nach der Höhe deren Dimension gesucht. Was hier mit der Dimension eines Ringes oder eines Ideals gemeint ist, wird in der folgenden Definition erläutert.

Definition 31 (GP07, Def. 3.3.1.) *Sei A ein Ring*

(1) Die Menge aller Ketten von Primidealen in A wird definiert als

$$C(A) := \{\zeta = (P_0 \subsetneq \cdots \subsetneq P_m \subsetneq A) \mid P_i Primideal)\}$$

(2) Ist $\zeta = (P_0 \subsetneq \cdots \subsetneq P_m \subsetneq A) \in C(A)$, so ist $m := length(\zeta)$ die Länge von ζ.

(3) Die Dimension von A ist definiert als

$$dim(A) := sup\,\{length(\zeta)\} \mid \zeta \in C(A)$$

(4) Für ein Primideal $P \subset A$ sei

$$C(A,P) := \{\zeta = (P_0 \subsetneq \cdots \subsetneq P_m) \in C(A) \mid P_m = P\}$$

die Menge der Ketten von Primidealen, welche in P enden. Wir definieren die Höhe von P als $ht(P) = sup\{length(\zeta) \mid \zeta \in C(A,P)\}$.

(5) Für ein allgemeines Ideal $I \subset A$ sei die Höhe von I definiert al $ht(I) := inf\,\{ht(P) \mid I \subset P, Primideal\}$ und $dim\ (I) := dim(A/I)$ sei die Dimension von I.

Die so definierte Dimension von Ringen heisst auch *Krull-Dimension*. Betrachten wir einen Polynomialen Ring in mehreren Variablen über einem Körper, so sind diese Definitionen noch leicht zu veranschaulichen. Wir kennen einfache Beispiele aus der Algebraischen Geometrie in denen wir uns die Varietät $V(I)$ eines Ideals I vorstellen und dann die Komponente der höchsten Dimension auch die Dimension des Ideals verkörpert. Im Falle von $k[x_1, \cdots, x_n]$ haben maximale Ketten von Primidealen, das heisst Ketten, die nicht verfeinert werden können, alle die Länge n. Also ist es offensichtlich, dass $k[x_1, \cdots, x_n]$ die Dimension n hat. Aber schon bei

Lokalisierungen dieses Rings ist das nicht mehr so. Ein algebraisch abgeschlossener Körper, der nur zwei Ideale, sich selbst und das Nullideal hat, ist somit offensichtlich von Dimension 0. Ein Hauptidealbereich, also auch $\mathbb{Z}$ hat die Dimension 1. $\mathbb{Z}[x]$ hat die Dimension 2. Es hat sogar jeder Noethersche Ring $R[x]$ die Dimension $k+1$, wenn k die Dimension von R ist. Also folgt, dass $\mathbb{Z}[x_1, \cdots, x_n]$ die Dimension $n+1$ hat. Dass man vorsichtig mit diesen Dimensionbegriffen umgehen muss, zeigt folgendes Beispiel:

Beispiel 9 Im Ring $(\mathbb{Z}/8\mathbb{Z})[x, y, z]$ betrachten wir die Kette

$$\langle 2 \rangle \subsetneq \langle 2, x \rangle \subsetneq \langle 2, x, y \rangle \subsetneq \langle 2, x, y, z \rangle$$

Jedes dieser Ideale ist prim, und die Dimension von $(\mathbb{Z}/8\mathbb{Z})[x, y, z]$ ist 3. Da dieser Ring kein Integritätsbereich ist, ist das Nullideal hier kein Primideal.

In [Eis95] kann mehr zum Thema Dimension von Ringen und Idealen gelesen werden.
Da wir es mit dem Polynomialen Ring über den ganzen Zahlen zu tun haben, müssen wir auf der geometrischen Seite affine Schemata betrachten. Dort ist die Anschauung schon abstrakter. Anstelle eines affinen Raums betrachtet man $\mathrm{Spec}(A) = \{P \mid A \supset P \quad \text{Primideal}\}$ als umgebenden "Raum" von den Nullstellenmengen $V(I) = \{P \in \mathrm{Spec}(A) \mid I \subset P\}$. Während man im ersten Fall eine Topologie über abgeschlossene Mengen $V(I)$, $I \subset A$ Ideal, definiert hat (Zariski Topologie), macht man dies bei $\mathrm{Spec}(A)$ über die offenen Mengen $\mathrm{Spec}(A) \setminus V(f)$, $f \in A$, also diejenigen Primideale, die f nicht enthalten.
Nun interessieren uns aber Primideale, die in besonderer Beziehung zu einem bestimmten allgemeinen Ideal I stehen:

Definition 32 (GP07, Def. 4.1.1.) *Sei A ein Noetherscher Ring und $I \subsetneq A$ ein Ideal.*

(1) Die Menge der zu I assoziierten Primideale wird definiert als
$Ass(I) := \{P \subset A : P$ Primideal und $P = (I : \langle b \rangle)$ für ein $b \in A\}$
Elemente von $Ass(\langle 0 \rangle)$ heissen auch assoziierte Primideale von A.

(2) Seien $P, Q \in Ass(I)$ und $Q \subseteq P$, dann heisst P ein eingebettetes Primideal von I. Dieser Begriff ist geometrisch motiviert.
Wir definieren $Ass(I, P) := \{Q \mid Q \in Ass(I), Q \subset P\}$

(3) I heisst equidimensionales oder rein dimensionales Ideal, falls alle zu I assoziierten Primideale von gleicher Dimension sind.

Zum Beispiel sind alle zu einem 0-dimensionalen Ideal I assoziierten Primideale auch 0-dimensional, da sie alle auch I enthalten. Man kann sich das geometrisch so vorstellen, dass eine Menge von isolierten Punkten auch nur Teilmengen von isolierten Punkten enthalten kann.
Ein zu I assoziiertes Primideal P heisst minimal, wenn für jedes Primideal $Q \subset R$ mit $I \subset Q \subset P$ gilt, dass $Q = P$. Die Menge der minimalen assoziierten Primideale von I ist $minAss(I)$.
Da wir diejenigen Primärideale suchen, deren Radikale die zu dem Ideal assoziierten Primideale sind, ist folgender Zusammenhang interessant:

Lemma 33 (AL, Lemma 4.6.14.) *Sei $I \subset A$ ein Ideal eines noetherschen Ringes A und sei $I = \bigcap_{i=1}^{r} Q_i$ eine Primärzerlegung, so dass die Q_i P_i-primär sind mit maximalen Idealen P_i. Dann sind für $j = 1, \ldots, r$*

$$Q_j = \{f \in A \mid (I : \langle f \rangle) \not\subset P_j\}$$

Beweis: Sei $j \in \{1, \ldots, r\}$. Wir bezeichnen $\{f \in A : (I : \langle f \rangle) \not\subset P_j\}$ mit Q'_j. Für ein $f \in Q'_j$ gibt es dann ein $g \in A$, so dass $g \notin M_j$ aber $fg \in I \subset Q_j$ ist. Da Q_j primär ist, ist entweder f oder eine Potenz von g in Q_j. Da aber $g \notin M_j = \sqrt{Q_j}$ folgt, dass $f \in Q_j$.
Für die umgekehrte Inklusion betrachten wir $f \in Q_j$. Für jedes $i \in \{1, \ldots, r\}$, $i \neq j$ gibt es ein $s_i \in M_i - M_j$. Dann ist $s_i^{e_i} \in Q_i$. Nun sei s das Produkt dieser $s_i^{e_i}, i \neq j$ und liegt im Produkt der $Q_i, i \neq j$ aber nicht in M_j. Dann ist fs im Produkt aller Q_j und somit auch in I enthalten. Also ist $s \in I : \langle f \rangle$ und $s \notin M_j$, so dass $f \in Q'_j$ sein muss.

q.e.d.

In der Primärzerlegung wollen wir unnötige Primärideale ausschliessen, damit wir eine irredundante Zerlegung erhalten. Deswegen wollen wir keine eingebetteten Primideale miteinbeziehen.

Proposition 34 (GP07, Prop. 3.3.5.) *Sei R ein Noetherscher Ring und $I \subset R$ ein Ideal. Dann ist $minAss(I) = \{P_1, \cdots, P_n\}$ endlich und*

$$\sqrt{I} = P_1 \cap \cdots \cap P_n$$

Im Speziellen ist $\sqrt{I}$ der Schnitt von allen Primidealen die I enthalten.

Den zweiten Punkt hatten wir schon in der Einführung gezeigt. Auch in der Konstruktion der Primärzerlegung nach dem Finden der assoziierten Primideale in Theorem 25 schliesst man überflüssige Primideale aus. Somit schliesst sich hier der Kreis.

A.3 Endlich erzeugte und freie Moduln

Wir benötigen für die Konstruktion der assoziierten Primideale Informationen über Moduln und im Speziellen auch endlich erzeugte Moduln und freie Moduln endlichen Ranges. Dazu wollen wir erstmal an folgende Definition errinnern:

Definition 35 *Sei R ein Ring und M ein endlich erzeugter R-Modul. M heisst frei, falls M isomorph ist zu R^n für ein $n \in \mathbb{N}$. Genau dann gibt es eine R-Basis von M, d.h. ein R-linear unabhängiges Erzeugendensystem.*

Zum Beispiel ist ein endlich erzeugtes Ideal in einem Ring R ein freier R-Modul oder $\mathbb{Z}_p[x]/f(x)$ für ein Polynom $f(x) \in \mathbb{Z}_p[x]$.
Schon im Beweis des ersten Theorems taucht der Begriff von Lösungsmengen der Form $(h_{i1}, \cdots, h_{ik})$ von Gleichungen $h_1 f_1 + \cdots + h_k f_k = 0$ einer Basis $(f_1, \cdots, f_q)$ eines Ideals auf. Dass wir es dann auch wieder mit Untermoduln, den sogenannten *Syzygienmoduln* zu tun haben wird in folgender Definition erläutert. A. Seidenberg hat in den siebziger Jahren eine Konstruktion von Syzygienmoduln von polynomialen Idealen mit Koeffizienten aus Körpern der Charakteristik $n \leq 0$ veröffentlicht. Mit Hilfe von Gröbner Basen hat man dann auch Syzygienkonstruktionen im arithmetischen Fall entwickelt. Syzygien werden in vielen weiteren algebraischen Konstruktionen nützlich eingesetzt.

Definition 36 (GP07, Def. 2.5.1.) *Eine Syzygie oder eine Relation zwischen k Elementen $f_1, \cdots, f_k$ eines R-Moduls M ist ein k-Tupel $(g_1, \cdots, g_k) \in R^k$, welches folgender Gleichung genügt*

$$\sum_{i=1}^{k} g_i f_i = 0$$

Die Menge aller Syzygien zwischen $f_1, \cdots, f_k$ ist ein Untermodul von R^k. Dieser ist sogar der Kern des Ringhomomorphismus

$$\varphi : F_1 := \bigoplus_{i=1}^{k} R\varepsilon_i \to M, \varepsilon_i \to f_i$$

wobei $(\varepsilon_1, \cdots, \varepsilon_k)$ eine kanonische Basis von R^k ist.
φ bildet surjektiv auf den R-Modul $I := \langle f_1, \cdots, f_k \rangle_R$ ab und

$$syz(I) := syz(f_1, \cdots, f_k) := Ker(\varphi)$$

wird der Modul der Syzygien von I bezüglich der Erzeugenden $f_1, \cdots, f_k$ genannt.

Der zweite Teil dieser Definition ist eigentlich eine Proposition. Es ist jedoch leicht zu sehen, dass für die Menge aller dieser k-Tupel die Moduloperationen wie verlangt gelten und sie darunter auch abgeschlossen ist.
Ist R ein lokaler b.z.w. graduierter Ring und $\{f_1, \cdots, f_k\}$, $\{g_1, \cdots, g_k\}$ minimale homogene Erzeugendensysteme von I, so sind $syz(f_1, \cdots, f_k)$ und $syz(g_1, \cdots, g_k)$ zueinander isomorph. Dann ist also $syz(I)$ wohldefiniert bis auf graduierte Isomorphismen. Im Allgemeinen hängt $syz(I)$ von der Wahl der Basis des Ideals I ab. Es kann aber gezeigt werden, dass für $I = \langle f_1, \cdots, f_k \rangle = \langle g_1, \cdots, g_s \rangle$ gilt:

$$syz(f_1, \cdots, f_k) \oplus R^s \cong syz(g_1, \cdots, g_s) \oplus R^k$$

Die Syzygienkonstruktion nach A. Seidenberg im Falle eines Körpers ist eine Konstruktion, die hauptsächlich Elemente der linearen Algebra beinhaltet. Sie funktioniert zwar nicht im arithmetischen Fall, aber für endliche Körper mit genügend großer Charakteristik p. Genügend groß heisst hierbei, dass wir eine obere Grenze für den Grad der g_j, $j = 1, \ldots, s$ brauchen, damit wir ausschliessen können, dass die Grade der g_j eventuell von p geteilt werden. Er ging dabei von r Relationen der f_{ij}, $i = 1, \ldots, r$ aus und berechnete eine einfache rekursive Funktion $M(n, r, d)$ von n, r und $d \geq \max \deg(f_i)$:
Wir betrachten die Matrix des Linearen Gleichungssystems der r Gleichungen mit den g_j als Variablen und nehmen an, sie seien linear unabhängig. Sei Δ die Determinante dieser Matrix, die dann ungleich 0 sein muss. Wir stellen $\Delta g_1, \ldots, \Delta g_r$ als Linearkombination der $g_{r+1}, \ldots, g_s$ dar und erhalten so Lösungen

$$(g_{11}, \ldots, g_{1r}, \Delta, 0, \ldots, 0) \ldots (g_{s1}, \ldots, g_{sr}, 0, \ldots, 0, \Delta)$$

Wir hatten eine homogene lineare Transformation durchgeführt, so dass wir annehmen konnten, dass der Koeffizient der höchsten Potenz von x_n in Δ ein Element aus dem Körper k ist. Nun beobachten wir, dass $\deg_{x_n}(g_{ij})$ und $\deg(\Delta) \leq rd$ sein müssen. Die g_j sind Polynome $\sum g_{ij} x_n^j$ vom Grad $rd - 1$ in x_n mit Koeffizienten aus $k[x_1, \ldots, x_{n-1}]$. Jede der r Gleichungen erhöht rd und wir erhalten insgesamt $r^2 d$ Gleichungen.
$M(n, r, d) = M(n - 1, r^2 d, d) + rd$ ist eine mögliche rekursive Funktion für M. Da $M(o, r, d) = 0$ erlaubt ist, können wir schreiben:

$$M(n, r, d) = rd + (rd)^2 + (rd)^4 + \cdots + (rd)^{2^{n-1}} \leq n(rd)^{2^{n-1}}$$

Das ist das N, welches im Algorithmus SPLITTING(I) auftaucht. Die Quelle zu dieser Berechnung ist [Sei10.74].
In den Artikeln von A.Seidenberg taucht auch der Begriff eines *Moduls von endlicher Präsentation* auf. Ein R-Modul M heisst von endlicher Präsentation, wenn es einen Homomorphismus von einem freien R-Modul endlichen Ranges auf M gibt, so dass dessen Kern endlich erzeugt ist. Hier sollte "es

gibt" in Hinblick auf die konstruktivistische Intention heissen, dass M durch eine endliche Menge von Erzeugenden und durch eine endliche Anzahl von Relationen zwischen den Erzeugenden gegeben ist. Mit anderen Worten ist dann der Syzygienmodul endlich erzeugt.

Lemma 37 (Sei74, Lemma 2) *Ist ein Modul M von endlicher Präsentation, so hat jede Abbildung eines freien R-Moduls endlichen Ranges auf M einen endlich erzeugten Kern.*

Tatsächlich ist auch für einen Modul ein Erzeugendensystem so gut wie das andere. Mit anderen Worten kann man mit den gegebenen Relationen des einen Erzeugendensystems die Relationen jedes anderen Erzeugendensystems konstruieren. In [Ri74] und in [Sei74] sind viele weitere algorithmische Aspekte von Noetherschen Ringen beschrieben. Die meisten dieser Algorithmen wurden schon in verschiedene Computeralgebrasysteme implementiert.

B Abbildungen als "Übersetzungen"

Wir wollen noch die Begriffe von Erweiterungen und Kontraktionen von Idealen erläutern. Diese Definitionen sind für Moduln analog. Wir werden sie hier aber nur für Ideale formulieren.

B.1 Homomorphismen zwischen Polynomringen

Sie sind unentbehrlich für Zerlegungen von Idealen und Moduln über Ringen. Mit ihrer Hilfe können wir Informationen, welche schon in der Zerlegung von Idealen in $k[x_1, \ldots, x_n]$ für einen Körper k und Unterräumen von Vektorräumen erarbeitet wurden auf unseren Fall übertragen.
Wir betrachten also einen Homomorphismus $f : A \to B$ zwischen zwei Ringen A und B.

Definition 38 (AM69) *(1) Die Erweiterung oder Verlängerung I^e eines Ideals $I \subset A$ ist das Ideal $B\langle f(I)\rangle$ in B.*

(2) Die Kontraktion J^c eines Ideals $J \subset B$ ist das Ideal $f^{-1}(J)$ in A.

Die Kontraktion eines Primideals $P \subset B$ ist immer auch ein Primideal in A, eine Verlängerung eines Primideals $P \subset A$ ist jedoch nicht unbedingt ein Primideal in B. Diese Tatsache legt schon fest, dass wir bei Abbildungen immer $A = \mathbb{Z}[x_1, \ldots, x_n]$ setzen. Wir betrachten ein klassisches Beispiel aus der Zahlentheorie:

Beispiel 10 Sei $f : \mathbb{Z} \to \mathbb{Z}[i]$, $i = \sqrt{-1}$, ein Homomorphismus von zwei Hauptidealringen:

(1) Die Erweiterung des Primideals $\langle 2\rangle$ ist dann $\langle 2\rangle^e = \mathbb{Z}[i]\langle 2\rangle = \langle 2i\rangle = \langle (1+i)^2\rangle$, also das Quadrat eines Primideals.

(1) Ist eine Primzahl $p \equiv 1 \bmod 4$, so ist $\langle p\rangle^e$ das Produkt zweier unterschiedlicher Ideale. Zum Beispiel ist $\langle 5\rangle^e = \langle (2+i)(2-i)\rangle$.

Folgende Eigenschaften von Kontraktionen und Erweiterungen sind für uns interessant:

Proposition 39 (AM69, Prop. 1.17.) *Sei $f : A \to B$ ein Homomorphismus von Ringen und $I \subset A$, $J \subset B$ zwei Ideale. Dann gilt:*

(1) $I \subset I^{ec}$, $J^{ce} \subset J$

(2) $J^c = J^{cec}$, $I^e = I^{ece}$

(3) Setzen wir $C = \{J^c \mid J \in B\} \subset A$ *und* $E = \{I^e \mid I \in A\} \subset B$ *so gilt:*
$C = \{I \mid I^{ec} = I\}$ *und* $E = \{J \mid J^{ce} = J\}$.
$I \mapsto I^{ec}$ *definiert eine bijektive Abbildung von* C *nach* E*, deren Inverse durch* $J \mapsto J1c$ *gegeben ist.*

Damit haben wir einige grundlegende Hilfsmittel, die wir in unserem Algorithmus direkt oder indirekt angewandt haben erkärt. Es würde aber wie bei allen Dingen, die auf vielen anderen bereits erarbeiteten Prozessen aufbauen den Rahmen sprengen, diese Prozesse bis in die Wurzeln zu erläutern.

References

[AL94] WILLIAM W. ADAMS und PHILIPPE LOUSTAUNAU: *An Introduction to Gröbner bases*. Graduate Studies in Mathematics. 3. Providence, RI: American Mathematical Society (AMS), 1994.

[AM69] MICHAEL F. ATIYAH und I.G. MACDONALD: *Introduction to commutaive algebra*. Addison-Wesley Publishing Company, 1969.

[Eis95] DAVID EISENBUD: *Commutative algebra with a view toward algebraic geometry*. Graduate Texts in Mathematics. 150. Berlin, Springer-Verlag, 1995.

[GP07] GERT-MARTIN GREUEL und GERHARD PFISTER: *A Singular introduction to commutative algebra, 2nd extended edition*. Berlin, Springer-Verlag, 2007.

[Ri74] FRED RICHMAN: *Constructive Aspects of Noetherian Rings*. RI: American Mathematical Society (AMS), Proceedings of the AMS, Vol. 44, No. 2, pages 436-441, June 1974.

[Sei78] ABRAHAM SEIDENBERG: *Constructions in a polynomial ring over the ring of integers*. American Journal of Mathematics, 1978 (received 1974), 100(4): pages 685-703.

[Sei74] ABRAHAM SEIDENBERG: *What is Noetherian?*. Seminario Matematico e Fisico, Italy, May 1974.

[Sei10.74] ABRAHAM SEIDENBERG: *Constructions in algebra*. RI: American Mathematical Society (AMS), Transactions of the AMS, Vol. 197, pages 273-313, October 1974.

[Vas04] WOLMER VASCONCELOS: *Computational Methods in Commutative Algebra and Algebraic Geometry, 3rd Edition*. Berlin, Springer-Verlag, 2004.