Inhaltsverzeichnis

October 3, 2010

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 beginnt man mit einer Aufteilung des Ideals in einen Teil, welcher keine Elemente aus R hat und einen Teil, der Elemente aus R hat. Den ersten Teil zerlegt man dann mit Hilfe einer Erweiterung nach dem Polynomring über $\mathbb{Q}$. Der zweite Teil wird zuerst in weitere Teile 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 deswegen vor der ersten Aufteilung des Ideals I 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. Sind zum Beispiel $Q_1, \ldots, Q_S$ Primärideale, deren Erzeuger benutzt werden um Daten zu kodieren, und I 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 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 3. Kapitel darstellen. Die im arithmetischen Fall auftretenden Unterschiede werden dann im 4. Kapitel ausführlich beschrieben.

2 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*

$$I = Q_1 \cap \cdots \cap Q_s$$

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 [GP0707, 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 $R[x_1, x_2, \dots]$ 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.