Diss. ETH No. 11013

Algebraic, Combinatorial and Algorithmic Issues Related to the Theory of Gröbner Bases of Polynomial Ideals

A dissertation submitted to the
SWISS FEDERAL INSTITUTE OF TECHNOLOGY
ZURICH

for the degree of
Dr. Sc. Math.

presented by
STÉPHANE COLLART
dipl. Math. ETH
born March 12^{th} 1961
citizen of Genève

accepted on the recommendation of
Prof. Dr. E. Engeler, examiner
Prof. Dr. U. Stammbach, co-examiner

1995

Summary.

In chapter 2, we develop a formal / structural framework for deciding the membership problem in algebraic structures; we show that a number of well known algorithms, such as Buchberger's algorithm for polynomial ideals, Sim's Schreier algorithm for permutation groups, Gauss elimination for vector spaces, and the Nielsen algorithm for subgroups of free groups are all analogous manifestations of a common formal procedure. This procedure can be applied to a broad class of algebraic structures satisfying sufficient requirements; we describe in detail the steps and requirements. Finally, we enunciate the thesis that this general procedure, in its varied manifestations, is basic to the decision procedure for a category of arbitrarily defined algebraic structures.

In chapter 3, we take on the problem of classifying the so-called admissible orders on the set of monomial terms, which may be viewed basically as the collection of semi-group orders on the set of monic monomials. This 'problem' is not new, and has been 'solved' a number of times over again up into the recent past (cf. [Rob85], [Wei87a]). The author gives here his own home-made 'solution', which uses order-preserving embeddings in ordered real additive spaces, by means of which the inner structure of these orders become particularly evident. In addition, these constructions make it immediately evident which orders are computable, and how to represent and compute with them. Of particular interest is the immediate decomposition of the term orders into their various archimedian types.

In chapter 4 an algebraic and algorithmic framework is assembled in which amongst other things Gröbner bases find a natural place, but is less determined at the outset by such arbitrarily imposed notions as that of 'admissible order'. The first step to this end is the investigation of the *monomialisation* of a polynomial ideal. We show that there is only a *finite* number of monomial ideals which satisfy a minimal incidence property with the original ideal. With each such minimally incidental ideal, we show that there is a uniquely defined associated system of (canonically oriented) polynomials from the ideal; not all of these systems are bases, as is shown in later examples. By orientation of a polynomial we mean the — arbitrary — designation of one of its monomials as its associated initial monomial. The next step is the investigation of a general scheme of polynomial reduction by means of oriented systems of polynomials. A simple calculus of reduction chains is developed, in which a notion of 'surfeitness' plays a certain rôle. Two equivalent conditions for such reduction systems to be noetherian are given, one of them being of combinatorial, the other of geometric nature. We distinguish further with respect to an ideal I among polynomial reduction systems those which are I-complete, i.e. they reduce by repeated application exactly the polynomials of I to 0. We show that the incidental systems distinguished thus are bases, and these are given the name of M-bases. Finally we further distinguish those M-bases which possess a 'self-reducedness' property, and correspondingly call these minimal M-bases. Finally we show that every M-base is a Gröbner base, and vice versa. Every initial ideal is a minimal incidental monomial ideal of I, but not the other way around: some of the latter are not initial ideals. The main product of this exhaustive approach is threefold:

(1) Starting with natural notions of reduction, one arrives by logical steps to the objects which constitute Gröbner bases; the framework itself represents a proper extension of the ordinary theory of Gröbner bases.
(2) A 'best-possible' result is achieved for Gröbner bases, i.e. every polynomial reduction system with reduction properties like Gröbner bases must be itself a Gröbner base.
(3) An original proof of the finiteness of the Gröbner system of a polynomial ideal — the set of its oriented reduced Gröbner bases — is obtained via the stronger result of the finiteness of the collection of minimal incidental monomial ideals belonging to that ideal.

Chapter 5, 6, 7 and chapter 8 are part of a series of joint investigations with D. Mall in the combinatorial and algorithmic theory of polynomial ideals. The results of these chapters will be published jointly.

In chapter 5 we prove a theorem on the *regularity* of the Gröbner fan of a polynomial ideal which sharpens a theorem of Mora and Robbiano in [MR88]. More precisely, we show that the Gröbner fan constitutes a conic polyhedral *decomposition* of the positive orthant, i.e. a fan in the sense of the theory of toric varieties (and not simply a tessalation). The proof is obtained by an original method which exploits the interplay between Gröbner bases, admissible orders, and Gröbner cones. The same method is used in the final section of the chapter to show that it is necessary and sufficient for the unrestricted Gröbner fan of a polynomial ideal to be complete that the ideal be quasi-homogeneous. This is sketched in the final section of the chapter, with a few further properties of the Gröbner fan, while the first sections develop all the circumstances of the main theorem.

In chapter 6 we enter into the question of the computation of the Gröbner system of a polynomial ideal. Some existing proposals for this object are discussed, and the problem of redundancies in the computation of the Gröbner system is evidenced with a few examples. For this reason we propose the *Gröbner filling algorithm*, which exploits the regularity derived in the preceding chapter to obtain a direct enumeration without redundancies of the Gröbner system.

In chapter 7 we give a direct proof that the set of initial degenerations of a polynomial ideal constitutes a complex. A generalisation in [CM94e] of the notion of initial ideal of a polynomial ideal permits the construction of the set of initial (or toric) degenerations. In [CM94e] it is shown that this set is dual to the Gröbner complex (more precisely, to a part of the complex), the facial complex of the Gröbner fan. This shows that the initial degenerations themselves constitute a complex. We develop here a direct proof of this complex structure (as an abstract complex), without reference to the Gröbner fan. This is done in three principal steps. First a simple calculus of *admissible* partial orders is developped. Then we show that the initial degenerations of a polynomial ideal constitute a modular lattice. Finally we show that this lattice satisfies an interpolation property which abstractly models the structure of a polytopal complex.

Chapter 8 returns to the original problem of the computation of a Gröbner base with respect to a given admissible term order, with however an approach quite different from all proposed up to now. We propose here a highly structured algorithm, the *Gröbner stripping algorithm*, which is based on the notion of toric (or initial) degeneration of a polynomial ideal. Essentially, a given base is completed to a Gröbner base by repeated recursive 'stripping' of toric degenerations, ensuing completion, and back-substitution in corresponding polynomial combinations. One obtains in this way a structurally explicit way of computing Gröbner bases. An advantage is that at any point of time one computes only with 'fragments' of polynomials of the objective ideal; from this one must on the other hand discount the overhead of back-substitution. This algorithm inherently computes the polynomial combinations expressing the new base in the original base.

Zusammenfassung.

In Kapitel 2 wird gezeigt, dass einige bekannte Algorithmen aus der Computational Algebra, als Beispiele werden nämlich der Buchberger Algorithmus, der Schreier Algorithmus, der Nielsen

Reduktionsalgorithmus und der Gauss'sche Eliminationsalgorithmus genommen, eine gemeinsame formale Beschreibung zulassen. Es handelt sich um ein allgemeines formales Verfahren zur Lösung des Mitgliedschaftsproblems in einer breiten Klasse von algebraischen Strukturen mit hinreichenden Voraussetzungen; das Verfahren und die Voraussetzungen werden im Detail aufgezogen. Es wird schliesslich die These aufgestellt, dass dieses allgemeine Verfahren, in seinen sehr verschiedenen Manifestationen, den eigentlichen empirischen Grundstein für praktische Berechnungen in beliebigen algebraischen Strukturen bildet.

In Kapitel 3 wird das Problem der Klassifikation aller sogenannten zulässigen Ordnungen auf die Menge der monomialen Termen, im Grunde genommen der fundierten Halbgruppenordnungen auf die Menge der monischen Monomen, angegangen. Dieses 'Problem' ist grundsätzlich kein Neues, und ist eine Anzahl von Malen bis in die jüngste Vergangenheit von Neuem 'gelöst' worden (cf. [Rob85], [Wei87a]). Der Autor gibt hier seine eigene hausgemachte 'Lösung', mit der Begründung, dass sie einen besonders einsichtlichen Charakter besitzt, indem sie sich zur Charakterisierung natürlichen ordnungstreuen additiven Einbettungen in geordnete reelle Räume bedient, die die innere Struktur der untersuchten Ordnungen ersichtlich machen. Zusätzlich lässt sich direkt aus den gegebenen Konstruktionen ableiten, welche Ordnungen berechenbar sind, und wie sie praktisch darzustellen und auszurechnen sind. Von besonderer Interesse in der hier gegebenen Konstruktion ist die Offenlegung der verschiedenen archimedischen Typen der Ordnungen.

In Kapitel 4 wird ein theoretischer Zugang aufgezogen, der unter anderem den herkömmlichen Begriff von Gröbner Basis umfasst, aber weniger von willkürlichen Voraussetzungen, wie zum Beispiel die Vorgabe von 'zulässigen Termordnungen', geprägt ist. Zu diesem Zweck wird zunächst die *Monomialisierung* eines Ideals untersucht. Es wird gezeigt, dass eine *endliche* Anzahl von monomialen Idealen existiert, die eine minimale Inzidenz Eigenschaft mit dem gegebenen Ideal besitzen. Assoziert mit diesen minimalen inzidentalen monomialen Idealen sind eineindeutige endliche Systeme von (canonisch orientierten) Polynomen aus dem Ideal; nicht alle solche Systeme konstituieren Basen, wie in späteren Beispielen gezeigt wird. Durch Orientierung eines Polynom wird die — willkürliche — Auszeichnung eines seiner Monomen als Initialmonom verstanden. In einem zweiten Schritt wird ein allgemeiner Begriff von polynomialer Reduktion anhand Systemen von orientierten Polynomen untersucht. Ein einfacher Kalkulus mit Reduktionsketten wird entwickelt, in dem ein Begriff von 'Übersättigung' eine Rolle spielt. Zwei äquivalente Bedingungen werden für die Noetherzität von Reduktionsketten angegeben, die eine kombinatorischer, die andere geometrischer Natur. Weiter werden für ein Ideal I solche Reduktionssysteme unterschieden, die I-vollständig sind, d.h. sie reduzieren durch wiederholte Anwendung genau die Polynome von I auf 0. Es wird gezeigt, dass dadurch inzidentale Systeme ausgezeichnet werden, die auch Basen sind, und M-Basen genannt werden. Schliesslich werden noch diejenigen ausgezeichnet, welche eine 'Selbst-Reduziertheitseigenschaft' besitzen, und dann entsprechend minimale M-Basen genannt werden. Schliesslich wird gezeigt, dass jede M-Basis eine Gröbner Basis ist, und umgekehrt; jedes Initialideal ist ein minimal inzidentales monomiale Ideal von I, aber nicht umgekehrt: es gibt welche der letzteren, die keine Initialideale sind. Durch diesen ausschöpfenden Vorgang sind drei Hauptsachen erreicht worden:

(1) Ausgehend von natürlichen Reduktionsbegriffen stösst man auf eine logische Weise zu den Gegenständen, die Gröbner Basen bilden. Der theoretische Rahmen dazu bildet eine echte Erweiterung des Üblichen.
(2) Ein 'Best-möglich' Beweis ist mitgeliefert, dass der Begriff von Gröbner Basen ausschöpfend ist, d.h. jedes polynomiale Reduktionssystem, welches die Reduktionseigenschaften von Gröbner Basen erfüllt, fällt bereits unter die Gröbner Basen.
(3) Ein origineller Beweis für die Endlichkeit des Gröbner Systems eines polynomialen Idealen — die Menge seiner orientierten reduzierten Gröbner Basen — ist durch das stärkere Resultat der Endlichkeit der Menge der zum Idealen zugehörigen minimalen inzidentalen monomialen Idealen gegeben.

Kapitel 5, Kapitel 6, Kapitel 7 und Kapitel 8 fügen sich ein in eine Reihe von fortlaufenden gemeinsamen Untersuchungen mit D. Mall in die kombinatorische und algorithmische Theorie

von Polynomidealen. Die Ergebnisse aus diesen Kapiteln werden gemeinsam veröffentlicht.

In Kapitel 5 wird ein Satz über die *Regularität* des Gröbner Fächers (= *en.* fan) eines Polynomideals bewiesen, der einen Satz von Mora und Robbiano aus [MR88] verschärft; genauer, es wird gezeigt, dass der Gröbner Fächer eines Ideals eine konische polyhedrale *Dekomposition* des positiven Orthants bildet, d.h. ein Fächer im Sinne der Theorie der torischen Varietäten bildet (und nicht bloss eine Parkettierung). Zum Beweis dieses Satzes wird eine originelle Beweismethode angewandt, die das Wechselspiel zwischen Gröbner Basen, zulässigen Ordnungen, und den Gröbner Koni ausbeutet; dieselbe Methode erlaubt es, im letzten Abschnitt des Kapitels zu zeigen, dass es zur Vollständigkeit des unrestringierten Gröbner Fächers notwendig- und hinreichenderweise der Quasi-Homogenität des Ideals bedarf. Während die ersten Abschnitte des Kapitels zum Beweis des Hauptsatzes aufbauen, wird Letzteres im letzten Abschnitt des Kapitels skizziert, wo auch ein paar weitere Eigenschaften des Gröbner Fächers diskutiert werden.

In Kapitel 6 wird auf die Frage der Berechnung des Gröbner Systems eines Ideals eingegangen. Nachdem bestehende Vorschläge für mögliche Verfahren dazu diskutiert werden, wird das Problem der Redundanz (und daher Effizienzverlustes) in der Berechnung des Gröbner Systems anhand von Beispielen erörtert. Deshalb wird der *Gröbner Filling Algorithmus* vorgeschlagen, ein Vorgang der die im vorigen Kapitel ermittelte Regularität des Gröbner Fächers ausbeutet, um die direkte Aufzählung des Gröbner Systems zu erlangen.

In Kapitel 7 wird ein direkter Beweis geliefert, dass die Menge der Initialdegerationen eines Polynomideals ein Komplex bildet. Eine Verallgemeinerung in [CM94e] des Begriffs von Initialideal eines Polynomideals gibt Anlass zur Bildung der (endlichen) Menge der Initial- (oder torischen) degenerationen. In [CM94e] wurde gezeigt, dass diese Menge dual ist zum Gröbner Komplex (genauer, einem Teil des Gröbner Komplexes), dem Seitenkomplex des Gröbner Fächers. Daraus folgt, dass die Initialdegenerationen selber ein Komplex bilden. Hier wird nun ein direkter Beweis der komplexen Struktur (als abstraktes Komplex) der Initialdegenerationen geliefert, ohne Bezug zum Gröbner Fächer. Dies geschiet im Wesentlichen in drei Schritten. Zunächst wird ein Kalkül von *zulässigen* partiellen Termordnungen erstellt. Dann wird gezeigt, dass die Initialdegenerationen eines Polynomideals einen modularen Verband bilden. Schliesslich wird gezeigt, dass dieser eine Interpolationseigenschaft erfüllt, welche die komplexe Struktur eines polytopalen Komplexes abstrakt modelliert.

Kapitel 8 kehrt gewissermassen zum ursprünglichen Problem der Berechnung einer Gröbner Basis bezüglich einer vorgegebenen zulässigen Termordnung zurück, mit jedoch einer Betrachtungsweise ganz anderer Art als die bisher vorgeschlagenen Verfahren. Wir schlagen hier ein hochstrukturiertes Verfahren vor, den *Gröbner Stripping Algorithmus*, das sich völlig an den Begriff von torischer (oder Initial-) Degeneration eines Polynomialideals orientiert. Es geht im wesentlichen darum, vorgegebene Basen zu Gröbnerbasen durch wiederholtes und rekursives 'Abschälen' von torischen Degenerationen, Vervollständigung, und Wiedereinsetzen in Polynomialkombinationen zu vervollständigen. Gewonnen wird dadurch eine strukturell erfassbare Berechnungsweise von Gröbnerbasen. Vorteilhaft ist, dass zu jedem Zeitpunkt nur mit 'Bruchstücken' von Polynomonen aus dem Zielideal gerechnet wird; dagegen muss der Aufwand des Wiedereinsetzens gehalten werden. Inhärent berechnet dieser Algorithmus die Polynomialkombinationen mit, die die neue Basis durch die alte ausdrücken.