Operationen auf Idealen von $K[X]$ (wie Produkt, Durchschnitt, Quotient, Bildung des Radikals) algorithmisch durchführen. Geometrisch gesehen erhält man somit - mit Hilfe des Hilbertschen Nullstellensatzes - ein algorithmisches Kriterium dafür, ob es im algebraischen Abschluß $\overline{K}$ von K eine gemeinsame Nullstelle von $f_1, \ldots, f_m$ gibt, an der weitere Polynome $g_1, \ldots, g_k \in K[X]$ nicht verschwinden.

In univariaten formalen Potenzreihenringen über einem Körper sind die entsprechenden Probleme fast trivial zu lösen: Eine Potenzreihe f teilt eine andere g genau dann, wenn für die entsprechenden Ordnungen gilt, $ord(f)$ teilt $ord(g)$. Damit ist der größte gemeinsame Teiler einer Menge von Potenzreihen einfach ein Element dieser Menge von minimaler Ordnung. Allerdings sind Potenzreihen, algorithmisch gesehen, unendliche Objekte; demgemäß läßt sich der Quotient von zwei Potenzreihen nur bis auf beliebige, aber endliche Genauigkeit berechnen. Solche Berechnungen lassen sich realisieren z. B. durch Modellierung von Potenzreihen als *Ströme*, siehe Abschnitt 2.1.2.

Volker Weispfenning (Passau)

2.2.2 Faktorisieren von Polynomen

Seit Carl Friedrich Gauß wissen wir, daß sich ein Polynom (in mehreren Variablen) über einem Körper (im wesentlichen) eindeutig in ein Produkt von irreduziblen Polynomen faktorisieren läßt. Die Frage, wie man diese Zerlegung effizient durchführt, ist eines der hübschesten und erfolgreichsten Gebiete der Computeralgebra.

Im folgenden gehe ich zunächst auf die Berechnung von größten gemeinsamen Teilern (ggTs), der quadratfreien Zerlegung und der Partialbruchzerlegung ein. Dann berichte ich über das Faktorisieren von Polynomen in einer Variablen über endlichen Körpern, über den rationalen Zahlen und über algebraischen Zahlkörpern, und schließlich über Polynome in mehreren Variablen. Eine ausführlichere Darstellung und Referenzen findet man in den drei Übersichtsartikeln von Kaltofen [12, 14, 15].

Der erweiterte Euklidische Algorithmus für Polynome in einer Variablen über einem Körper hat zahlreiche wichtige Anwendungen: Chinesischer Restsatz, Interpolation, Inversion in Erweiterungsringen, linear rekurrente Folgen, lineare Algebra für schwach besetzte Matrizen à la Krylov, Dekodieren von BCH-Kodes (Berlekamp-Massey Algorithmus). Die Subresultantentheorie liefert theoretische Einsichten, Strategien zum Vermeiden von zu großen Zwischenresultaten und vor allem die wichtigen modularen Algorithmen für Polynome in mehreren Variablen über $\mathbb{Q}$.

Der quadratfreie Teil $f_1 \dots f_r$ eines Polynoms $f = f_1^{e_1} \dots f_r^{e_r}$, mit $f_1, \dots, f_r$ irreduzibel und paarweise nichtassoziiert, berechnet sich als $f/\mathrm{ggT}(f, f')$. In Charakteristik $p > 0$ muß man noch gewisse p-te Wurzeln ziehen. Durch Iteration des Algorithmus erhält man die *quadratfreie Zerlegung* $f = g_1^1 \cdot g_2^2 \cdot \dots \cdot g_n^n$, wobei die $g_i \in K[X]$ quadratfrei und paarweise teilerfremd sind. Die quadratfreie Zerlegung wird speziell auch zum Integrieren von rationalen Funktionen f/g (mittels Partialbruchzerlegung) verwendet (siehe Abschnitt 2.8.2). Für die übliche Partialbruchzerlegung benötigt man hingegen die vollständige Faktorisierung des Nennerpolynoms g.

Der grundlegende Fall beim Faktorisieren ist der eines Polynoms vom Grad n in einer Variablen über einem endlichen Körper $\mathbb{F}_q$ mit q Elementen, wobei q eine Primzahlpotenz ist. Berlekamp (cf. [3, 4]) hat einen deterministischen Algorithmus mit Laufzeit (= Operationen in $\mathbb{F}_q$) $O^\sim(n^3 + nq)$ angegeben, wobei das *weiche* $O^\sim$ bedeutet, daß wir Faktoren $\log n$ vernachlässigen. Ein Meilenstein ist sein Zufallsalgorithmus mit polynomialer Laufzeit $O^\sim(n^3 + n \log q)$; dies war die erste bedeutende Anwendung dieses Berechnungsmodus in der Computeralgebra, und bis heute ist keine deterministische Methode mit polynomialer Laufzeit bekannt. Eine wichtige Idee war der Algorithmus von Cantor und Zassenhaus [9] mit $O^\sim(n^2 \log q)$ Operationen, und die schnellste bekannte Methode braucht $O^\sim(n^2 + n \log q)$ Operationen [24]. Ein Computeralgebra-System wie MAPLE faktorisiert Polynome vom Grad $n \approx 200$ über einem Körper mit $q \approx 2^{200}$ Elementen in einem Tag auf einer gängigen Workstation (1992), und mit $n \approx 400$ und $q \approx 2^{400}$ in einem Monat; es wird erwartet, daß die neuen Methoden diese Grenzen verbessern [23].

Für Polynome über $\mathbb{Q}$ oder algebraischen Zahlkörpern benutzt man die *Hensel-lifting*-Methode von Zassenhaus [25] – die in gewissen Fällen exponentielle Laufzeit braucht – oder die *kurzen Vektoren in Gittern* von Lenstra *et al.* (siehe [18] und 2.3.6) mit polynomialer Laufzeit, aber oft langsamer. Diese Algorithmen sind erheblich aufwendiger als die über endlichen Körpern. Schönhage hat sehr schnelle Algorithmen zum „numerischen" Faktorisieren über $\mathbb{R}$ und $\mathbb{C}$, d. h. dem Finden von Näherungen der Wurzeln [21].

Für Polynome in mehreren Variablen ist die Wahl der „richtigen" Datenstruktur entscheidend. Bei „wenigen" Variablen führt eine Variante des *Hensel-lifting* zum Ziel, aber bei vielen Variablen muß man eine *dünn besetzte Darstellung* benutzen. Die entscheidenden weitreichenden Konzepte sind effektive Versionen des Hilbertschen Irreduzibilitätssatzes und die „Darstellung durch einen Schaltkreis". Kaltofens Faktorisierungsalgorithmus [13] in diesem Modell zählt zu einem der Höhepunkte auf dem Gebiet der Faktorisierung.

Ein verschiedenes, aber verwandtes Problem ist das der funktionalen Zerlegung $f = g \circ h$ eines Polynoms f. Dies galt zunächst als schwierig und wurde als

Grundlage für ein Kryptosystem vorgeschlagen. Dieser Hoffnung machte aber ein hübscher Algorithmus mit polynomialer Laufzeit von Kozen und Landau [17] den Garaus. Die schnellsten Algorithmen hierzu sind in [22] enthalten.

Joachim von zur Gathen (Toronto)

2.2.3 Gröbnerbasen

Multivariate Polynomringe $R = K[X_1, \ldots, X_n]$ über Körpern sind für $n \geq 2$ keine Hauptidealringe. In solchen Ringen übernimmt die Konstruktion von *Gröbnerbasen* die Rolle, die der Euklidische Algorithmus in $K[X]$ spielt. Das gilt sowohl im Hinblick auf den methodischen Ansatz als auch auf die Anwendungen für Ideale in R und ihre Nullstellen in algebraisch abgeschlossenen Erweiterungskörpern von K. Die Methode wurde von B. Buchberger 1965 begründet (siehe [5, 6]); sie hat sich seit den siebziger Jahren rapide weiterentwickelt und stellt heute eine der wichtigen grundlegenden Techniken der Computeralgebra dar.

Man fixiert eine *Termordnung* $<$ auf dem Monoid T der Terme (Potenzprodukte der Unbestimmten) von R. Dann kann man analog zum Divisionsalgorithmus bei univariaten Polynomen den Begriff der *Reduktion* eines Polynoms f mittels einer Menge P weiterer Polynome erklären. Die Iteration solcher Reduktionen führt schließlich auf eine *Normalform* von f bezüglich P.

Eine endliche Menge $G \subseteq R$ ist eine *Gröbnerbasis* (des von G erzeugten Ideals I), falls für jedes Polynom $0 \neq f \in I$ gilt, daß der höchste Term von f Vielfaches des höchsten Terms eines Polynoms aus G ist. Das bedeutet anschaulich, daß bei den Linearkombinationen der Polynome aus G zwar Auslöschungen zwischen Monomen in der Darstellung vorkommen können, diese aber nicht wesentlich sind.

Die Konstruktion einer Gröbnerbasis G aus einer vorgegebenen endlichen Idealbasis F wurde 1965 von Buchberger angegeben. Sie iteriert die Hinzunahme von Normalformen von *S-Polynomen* (kritischen Paaren) zu F. Die Terminierung des Algorithmus wird duch das *Dicksonsche Lemma* garantiert. Da die Konstruktion von Gröbnerbasen doppelt exponentiell in der Anzahl der Variablen sein kann, stößt sie bei Problemen mit vielen Variablen auf erhebliche Schwierigkeiten. Dabei spielt die Wahl der Termordnung oft eine entscheidende Rolle.

Mit Hilfe von Gröbnerbasen (teilweise in Kombination mit anderen Polynomalgorithmen wie etwa Faktorisierung) lassen sich eine Fülle von algorithmischen Problemen für multivariate Polynome und deren Nullstellen (in algebraisch abgeschlossenen Körpern) lösen. Dazu gehören etwa: das Idealmitgliedschaftsproblem, Inklusion zwischen Idealen, Berechnung von Durchschnit-

ten und Quotienten von Idealen, Berechnung des Radikals und der Primäridealzerlegung, eine Erweiterung des chinesischen Restesatzes (vgl. Abschnitt 2.1.4), Bestimmung der Dimension eines Ideals und der Vektorraumdimension des entsprechenden Restklassenrings $\bar{R}$, explizite Angabe einer Basis von $\bar{R}$ sowie der Strukturkonstanten von $\bar{R}$, Berechnung eines Erzeugendensystems für den Syzygienmodul einer Idealbasis, Lösen linearer Gleichungssysteme über R, Rechnen in endlichen algebraischen Körpererweiterungen, Überführung eines algebraischen Gleichungssystems in Dreiecksform, die eine exakte, symbolische Lösung in einer geeigneten Erweiterung des Grundkörpers ermöglicht (vergl. Abschnitt 2.4.1).

Die von Buchberger entwickelte Gröbnerbasen-Methode für multivariate Polynome über einem Körper ist in den meisten universell anwendbaren Computeralgebra-Systemen implementiert sowie in vielen Spezialsystemen wie CoCoA, FELIX, MACAULAY und MAS. Sie ist auf eine Reihe anderer Ringe und auf endlich erzeugte Moduln über diesen Ringen ausgedehnt worden. Dazu gehören: multivariate Polynomringe über Hauptidealringen und über kommutativen von Neumann-regulären Ringen, sowie gewisse Typen von nichtkommutativen Polynomringen über Schiefkörpern (vgl. auch Abschnitt 2.5).

Die Konstruktion *umfassender Gröbnerbasen* für multivariate Polynome mit parametrischen Koeffizienten ist von Bedeutung für die Eliminationstheorie, insbesondere für die Quantorenelimination in algebraisch abgeschlossenen Körpern (siehe Abschnitt 2.4.1).

Eine detaillierte Übersicht über das Gebiet bieten der Übersichtsartikel von Buchberger [7] sowie das Lehrbuch [2].

Volker Weispfenning (Passau)

2.2.4 Standardbasen

In formalen Potenzreihenringen $K[[X_1, \ldots, X_n]]$ über einem Körper K entspricht der Begriff einer *Standardbasis* dem einer Gröbnerbasis im Polynomring $K[X_1, \ldots, X_n]$. Dabei wird die Rolle der höchsten Terme in Polynomen übernommen von den niedrigsten Termen in einer Potenzreihe (bezüglich einer festen Termordnung). Die Existenz von Standardbasen und Gröbnerbasen bezüglich gewisser Termordnungen wurde von Hironaka (1964) nichtkonstruktiv bewiesen. Ähnlich wie Gröbnerbasen lassen sich Standardbasen bezüglich einer mit dem Totalgrad verträglichen Termordnung aus einer gegebenen endlichen Idealbasis F bis auf beliebige Genauigkeit (im Sinne der natürlichen Topologie auf $K[[X_1, \ldots, X_n]]$) berechnen [11]. Besteht F nur aus Polynomen, so läßt sich eine Standardbasis (in Form von Polynomen) sogar exakt berechnen (Tangentialkegel-Algorithmus von Mora [20]). Das ist von großer Bedeu-

tung für die algorithmische Untersuchung von Singularitäten von algebraischen Varietäten (vgl. Abschnitt 2.4.2). Einen Überblick über Standardbasen bietet [1].

Volker Weispfenning (Passau)

2.2.5 Charakteristische Mengen

Charakteristische Mengen wurden von Ritt 1950 als ein wichtiges Hilfsmittel zur strukturellen Untersuchung von algebraischen Differentialgleichungen eingeführt (vgl. die Abschnitte 2.9.1 und 2.9.2). Wu übertrug 1984 die algorithmischen Aspekte der Methode auf algebraische Gleichungen mit dem Ziel, eine effektive Methode zum automatischen Beweisen von geometrischen Sätzen zu finden. Dieser Ansatz ist seitdem intensiv weiterverfolgt worden [10].

Sei F eine Menge von Polynomen in einem multivariaten Polynomring R über einem Körper. Eine *charakteristische Menge* von F ist dann eine minimale aufsteigende Teilmenge von F im Sinne von Ritt. Die Existenz einer solchen charakteristischen Menge ist stets durch die Fundiertheit der entsprechenden Ordnung zwischen aufsteigenden Ketten gesichert; ist F endlich, so kann eine charakteristische Teilmenge leicht algorithmisch bestimmt werden.

Der Algorithmus von Wu besteht aus einer Kombination einer Vervollständigungsprozedur für endliche charakteristische Mengen mit einem sukzessiven Aufspalten der erhaltenen Mengen in endlich viele Bestandteile. Bei der Vervollständigung werden die charakteristischen Mengen ergänzt um Reste von Polynomen in F unter Pseudodivisionen nach geeignet ausgewählten Variablen. Das Aufspalten geschieht durch Fallunterscheidungen über das mögliche Verschwinden von Initialen der Polynome, mit denen Pseudodivisionen durchgeführt werden.

Das Ergebnis kann als eine Aufspaltung der Nullstellenmenge V von F in endlich viele paarweise disjunkte Boolesche Kombinationen von Varietäten (*konstruktible Mengen*) aufgefaßt werden, die in der Praxis in vielen Fällen genügt, um die gewünschten Informationen über V zu erhalten. Im allgemeinen läßt sich damit jedoch nicht entscheiden, ob ein gegebenes Polynom g auf V verschwindet oder nicht. Trotz dieser Unvollständigkeit ist diese Methode in der Praxis für geometrische Untersuchungen oft effektiver als entsprechende Gröbnerbasis-Methoden. Allerdings liefert sie nicht immer eine definitive Antwort. Die Methode kann ergänzt werden durch sukzessive Faktorisierung von Polynomen in der charakteristischen Menge über dem algebraischen Erweiterungskörper, der durch die vorhergehenden Polynome der charakteristischen Menge definiert wird. Dadurch gewinnt die Methode an Informationsgehalt, verliert aber gleichzeitig erheblich an Effektivität.

Einen Überblick über die Methode liefert der Anhang von [2], eine detaillierte Beschreibung [10].

Volker Weispfenning (Passau)

Literatur

[1] Th. Becker. Standard bases and some computations in rings of power series. *Journal of Symbolic Computation*, 10(2):165–178, 1990.

[2] Th. Becker and V. Weispfenning in cooperation with H. Kredel. *Gröbner Bases, A Computational Approach to Commutative Algebra*, volume 141 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, Berlin, Heidelberg, 1993.

[3] E.R. Berlekamp. Factoring polynomials over finite fields. *Bell System Techn. Journal*, 46:1853–1859, 1967.

[4] E.R. Berlekamp. Factoring polynomials over large finite fields. *Mathematics of Computation*, 24:713–735, 1970.

[5] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Dissertation, Mathematisches Institut der Universität Innsbruck, Innsbruck, Österreich, 1965.

[6] B. Buchberger. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems. *Aequ. Math.*, 4:374–383, 1970.

[7] B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In N.K. Bose, editor, *Multidimensional Systems Theory*, pages 184–232. K. Reidel Publishing Company, Dordrecht, 1985.

[8] B. Buchberger, G.E. Collins, and R. Loos, editors. *Computer Algebra, Symbolic and Algebraic Computation.* Springer-Verlag, Wien - New York, second edition, 1983.

[9] D.G. Cantor and H. Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Mathematics of Computation*, 36:587–592, 1981.

[10] Shang-Ching Chou. *Mechanical Geometry Theorem Proving.* K. Reidel Publishing Company, Dordrecht, 1988.

[11] P. Ebner-Altunay. Standardbasen in Potenzreihenringen. Diplomarbeit, Universität Passau, Passau, 1991.

[12] E. Kaltofen. Factorization of polynomials. In Buchberger et al. [8], pages 95–113.

[13] E. Kaltofen. Factorization of polynomials given by straight-line programs. In S. Micali, editor, *Randomness and Computation*, pages 375–412. JAI Press, Greenwhich CT, 1989.

[14] E. Kaltofen. Polynomial factorization 1982-1986. In D.V. Chudnovsky and R.D. Jenks, editors, *Computers in Mathematics*, pages 285–300. Marcel Dekker, New York, 1990.

[15] E. Kaltofen. Polynomial factorization 1987-1991. In I. Simon, editor, *Proc. Latin '92*, volume 583 of *Lecture Notes in Computer Science*, pages 294–313. Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[16] D.E. Knuth. *Seminumerical Algorithms*, volume 2 of *The Art of Computer Programming*. Addison-Wesley, Reading, Massachusetts, second edition, 1981.

[17] D. Kozen and S. Landau. Polynomial decomposition algorithms. *Mathematische Annalen*, 7:445–456, 1989.

[18] A.K. Lenstra, H.W. Lenstra Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[19] R. Loos. Generalized polynomial remainder sequences. In Buchberger et al. [8], pages 115–137.

[20] T. Mora. An algorithm to compute the equations of tangent cones. In J. Calmet, editor, *Computer Algebra, EUROCAM'82, European Computer Algebra Conference, Marseille, France, 5–7 April 1982*, volume 144 of *Lecture Notes in Computer Science*, pages 158–165. Springer-Verlag, Berlin-Heidelberg-New York, 1982.

[21] A. Schönhage. Equation solving in terms of computational complexity. In A.M. Gleason, editor, *Proceedings of the International Congress of Mathematicians 1986, Vol. I*, pages 131–153. AMS, Providence, 1987.

[22] J. von zur Gathen. Functional decomposition of polynomials: the tame case. *Journal of Symbolic Computation*, 9(3):281–299, 1990.

[23] J. von zur Gathen. A polynomial factorization challenge. *SIGSAM Bulletin*, 26:22–24, 1992.

[24] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Computational Complexity*, 2, 1992.

[25] H. Zassenhaus. On Hensel factorization I. *Journal of Number Theory*, 1:291–311, 1969.

2.3 Konstruktive Methoden in der Zahlentheorie

2.3.1 Primzahlnachweise

Ein wichtiges Problem der algorithmischen Zahlentheorie besteht darin, zu entscheiden, ob eine natürliche Zahl n eine Primzahl ist oder nicht. Üblicherweise geht man so vor, daß man zunächst einen probabilistischen *Primzahltest* anwendet. Dieser zeigt entweder, daß n zusammengesetzt ist oder daß n mit hoher Wahrscheinlichkeit eine Primzahl ist. Im letzteren Fall verwendet man deterministische Primzahlnachweisverfahren um zu zeigen, daß n tatsächlich eine Primzahl ist.

Ein erster Primzahltest basiert auf dem *kleinen Satz von Fermat*: Sei n eine Primzahl. Dann gilt für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ die Kongruenz $a^{n-1} \equiv 1 \bmod n$.