Kapitel 6
Gröbner-Basen

§ 1: Gauß und Euklid

Wir haben bereits ziemlich am Anfang der Vorlesung ein Verfahren zur Lösung nichtlinearer Gleichungssysteme kennengelernt, die Elimination von Variablen durch Resultanten. Hier im letzten Kapitel soll es um ein alternatives Verfahren gehen, dessen Bedeutung in der Computeralgebra – genau wie im Falle der Resultanten – weit über die Lösung nichtlinearer Gleichungssysteme hinausgeht.

Ausgangspunkt sind der GAUSS-Algorithmus zur Lösung linearer Gleichungssysteme und der Algorithmus zur Polynomdivision, wie er im EUKLIDischen Algorithmus zur Berechnung des ggT zweier Polynome verwendet wird:

Wenn wir ein lineares Gleichungssystem durch GAUSS-Elimination lösen, bringen wir es zunächst auf eine Treppengestalt, indem wir die erste vorkommende Variable aus allen Gleichungen außer der ersten eliminieren, die zweite aus allen Gleichungen außer den ersten beiden, uns so weiter, bis wir schließlich Gleichungen haben, deren letzte entweder nur eine Variable enthält oder aber eine Relation zwischen Variablen, für die es sonst keine weiteren Bedingungen mehr gibt. Konkret sieht ein Eliminationsschritt folgendermaßen aus: Wenn wir im Falle der beiden Gleichungen

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = r \qquad (1)$$
$$b_1x_1 + b_2x_2 + \cdots + b_nx_n = s \qquad (2)$$

die Variable x_1 mit Hilfe von (1) aus (2) eliminieren wollen, ersetzen wir die zweite Gleichung durch ihre Summe mit $-b_1/a_1$ mal der ersten. Die theoretische Rechtfertigung für diese Umformung besteht darin, daß das Gleichungssystem bestehend aus (1) und (2) sowie das neue Gleichungssystem dieselbe Lösungsmenge haben, und daran ändert sich auch dann nichts, wenn noch weitere Gleichungen dazukommen.

Ähnlich können wir vorgehen, wenn wir ein nichtlineares Gleichungssystem in nur einer Variablen betrachten: Am schwersten sind natürlich die Gleichungen vom höchsten Grad, also versuchen wir, die zu reduzieren auf Polynome niedrigeren Grades. Das kanonische Verfahren dazu ist die Polynomdivision: Haben wir zwei Polynome

$$f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \quad \text{und}$$
$$g = b_mx^n + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$$

mit $m \le n$, so dividieren wir f durch g, d.h. wir berechnen einen Quotienten q und einen Rest r derart, daß $f = qg + r$ ist und r kleineren Grad als g hat. Konkret: Bei jedem Divisionsschritt haben wir ein Polynom

$$f = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0\,,$$

das wir mit Hilfe des Divisors

$$g = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$$

reduzieren, indem wir es ersetzen durch

$$f - \frac{b_m}{a_n}x^{n-m}g\,,$$

und das führen wir so lange fort, bis f auf ein Polynom von kleinerem Grad als g reduziert ist: Das ist dann der Divisionsrest r. Auch hier ist klar, daß sich nichts an der Lösungsmenge ändert, wenn man die beiden Gleichungen f, g ersetzt durch g, r, denn

$$f = qg + r \quad \text{und} \quad r = f - qg\,,$$

d.h. f und g verschwinden genau dann für einen Wert x, wenn g und r an der Stelle x verschwinden.

In beiden Fällen ist die Vorgehensweise sehr ähnlich: Wir vereinfachen das Gleichungssystem schrittweise, indem wir eine Gleichung ersetzen durch ihre Summe mit einem geeigneter Vielfachen einer anderen Gleichung.

Dieselbe Strategie wollen wir auch anwenden Systeme von Polynomgleichungen in mehreren Veränderlichen. Erstes Problem dabei ist, daß wir nicht wissen, wie wir die Monome eines Polynoms anordnen sollen und damit, was der führende Term ist. Dazu gibt es eine ganze Reihe verschiedener Strategien, von denen je nach Anwendung mal die eine, mal die andere vorteilhaft ist. Wir wollen uns daher zunächst damit beschäftigen.

§ 2: Monomordnungen

Wir betrachten Polynome in n Variablen $x_1, \ldots, x_n$ und setzen zur Abkürzung

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \quad \text{mit} \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0 \, .$$

Eine Anordnung der Monome ist offensichtlich äquivalent zu einer Anordnung auf $\mathbb{N}_0^n$, und es gibt sehr viele Möglichkeiten, diese Menge anzuordnen. Für uns sind allerdings nur Anordnungen interessant, die einigermaßen kompatibel sind mit der algebraischen Struktur des Polynomrings $k[x_1, \ldots, x_n]$; beispielsweise wollen wir sicherstellen, daß der führende Term des Produkts zweier Polynome das Produkt der führenden Terme der Faktoren ist – wie wir es auch vom Eindimensionalen her gewohnt sind. Daher definieren wir

Definition: *a)* Eine Monomordnung ist eine Ordnungsrelation $<$ auf $\mathbb{N}_0^n$, für die gilt

1. $<$ ist eine Linear- oder Totalordnung, d.h. für zwei Elemente $\alpha, \beta \in \mathbb{N}_0^n$ ist entweder $\alpha < \beta$ oder $\beta < \alpha$ oder $\alpha = \beta$.
2. Für $\alpha, \beta, \gamma \in \mathbb{N}_0^n$ gilt $\alpha < \beta \Longrightarrow \alpha + \gamma < \beta + \gamma$.
3. $<$ ist eine Wohlordnung, d.h. jede Teilmenge $I \subseteq \mathbb{N}_0^n$ hat ein kleinstes Element.

b) Für $f = \sum_{\alpha \in I} c_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ mit $c_\alpha \neq 0$ für alle $\alpha \in I \subset \mathbb{N}_0$ sei γ das größte Element von I bezüglich einer fest gewählten Monomordnung. Dann bezeichnen wir bezüglich dieser Monomordnung

- γ = multideg f als Multigrad von f
- x^γ = FM f als führendes Monom von f
- c_γ = FK f als führenden Koeffizienten von f
- $c_\gamma x^\gamma$ = FT f als führenden Term von f

Der Grad deg f von f ist, wie in der Algebra üblich, der höchste Grad eines Monoms von f; je nach gewählter Monomordnung muß das nicht unbedingt der Grad des führenden Monoms sein.

Beispiele von Monomordnungen sind

1) Die lexikographische Ordnung: Hier ist $\alpha < \beta$ genau dann, wenn für den ersten Index i, in dem sich α und β unterscheiden, $\alpha_i < \beta_i$ ist. Betrachtet man Monome x^α als Worte über dem (geordneten) Alphabet $\{x_1, \ldots, x_n\}$, kommt hier ein Monom x^α genau dann vor x^β, wenn die entsprechenden Worte im Lexikon in dieser Reihenfolge gelistet werden. Die ersten beiden Forderungen an eine Monomordnung sind klar, und auch die Wohlordnung macht keine großen Probleme: Man betrachtet zunächst die Teilmenge aller Exponenten $\alpha \in I$ mit kleinstmöglichem α_1, unter diesen die Teilmenge mit kleinstmöglichem α_2, *usw.*, bis man bei α_n angelangt ist. Spätestens hier ist die verbleibende Teilmenge einelementig, und ihr einziges Element ist das gesuchte kleinste Element von I.

2) Die graduierte lexikographische Ordnung: Hier ist der Grad eines Monoms erstes Ordnungskriterium: Ist deg $x^\alpha <$ deg x^β, so definieren wir $\alpha < \beta$. Falls beide Monome gleichen Grad haben, soll $\alpha < \beta$ genau dann gelten, wenn α im lexikographischen Sinne kleiner als β ist. Auch hier sind offensichtlich alle drei Forderungen erfüllt.

3) Die inverse lexikographische Ordnung: Hier ist $\alpha < \beta$ genau dann, wenn für den *letzten* Index i, in dem sich α und β unterscheiden. Das entspricht offensichtlich gerade der lexikographischen Anordnung bezüglich des rückwärts gelesenen Alphabets $x_n, \ldots, x_1$. Entsprechend

läßt sich natürlich auch bezüglich jeder anderen Permutation des Alphabets eine Monomordnung definieren, so daß diese Ordnung nicht sonderlich interessant ist – außer als Bestandteil der im folgenden definierten Monomordnung:

4) Die graduierte inverse lexikographische Ordnung: Wie bei der graduierten lexikographischen Ordnung ist hier der Grad eines Monoms erstes Ordnungskriterium: Falls $\deg x^\alpha < \deg x^\beta$, ist $\alpha < \beta$, und nur falls beide Monome gleichen Grad haben, soll $\alpha < \beta$ genau dann gelten, wenn α im Sinne der inversen lexikographischen Ordnung *größer* ist als β. Man beachte, daß wir hier also nicht nur die Reihenfolge der Variablen invertieren, sondern auch die Ordnungsrelation im Fall gleicher Grade. Es ist nicht schwer zu sehen, daß auch damit eine Monomordnung definiert wird; siehe Übungsblatt.

Für das folgende werden wir noch einige Eigenschaften einer Monomordnung benötigen, die in der Definition nicht erwähnt sind.

Als erstes wollen wir uns überlegen, daß bezüglich jeder Monomordnung auf $\mathbb{N}_0^n$ kein Element kleiner sein kann als $(0, \ldots, 0)$: Wäre nämlich $\alpha < (0, \ldots, 0)$, so wäre wegen der zweiten Eigenschaft auch

$$2\alpha = \alpha + \alpha < \alpha + (0, \ldots, 0) = \alpha$$

und so weiter, so daß wir eine unendliche Folge

$$\alpha > 2\alpha > 3\alpha > \cdots$$

hätten, im Widerspruch zur dritten Forderung.

Daraus folgt nun sofort, daß das Produkt zweier Monome größer ist als jeder der beiden Faktoren und damit auch, daß ein echter Teiler eines Monoms immer kleiner ist als dieses. Außerdem folgt, daß für ein Produkt von Polynomen stets $\mathrm{FM}(fg) = \mathrm{FM}(f) \cdot \mathrm{FM}(g)$ ist.

§3: Der Divisionsalgorithmus

Die Eliminationsschritte beim GAUSS-Algorithmus können auch als Divisionen mit Rest verstanden werden, und beim EUKLIDischen Algorithmus ist ohnehin alles Division mit Rest. Für ein Verallgemeinerung der

beiden Algorithmen auf Systeme nichtlinearer Gleichungssysteme brauchen wir also auch einen Divisionsalgorithmus für Polynome in mehreren Veränderlichen, der die eindimensionale Polynomdivision mir Rest und die Eliminationsschritte beim GAUSS-Algorithmus verallgemeinert.

Beim GAUSS-Algorithmus brauchen wir im allgemeinen mehr als nur einen Eliminationsschritt, bis wir eine Gleichung auf eine Variable reduziert haben; entsprechend wollen wir auch hier einen Divisionsalgorithmus betrachten, der gegebenenfalls auch mehrere Divisoren gleichzeitig behandeln kann.

Wir gehen also aus von einem Polynom $R = f \in k[x_1, \ldots, x_n]$, wobei k irgendein Körper ist, in dem wir rechnen können, meistens also $k = \mathbb{Q}$ oder $k = \mathbb{F}_p$. Dieses Polynom wollen wir dividieren durch die Polynome $f_1, \ldots, f_s \in R$, d.h. wir suchen Polynome $a_1, \ldots, a_s, r \in R$, so daß

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

ist, wobei r in irgendeinem noch zu präzisierenden Weise kleiner als die f_i sein soll.

Da es sowohl bei GAUSS als auch bei EUKLID auf die Anordnung der Terme ankommt, legen wir als erstes eine Monomordnung fest; wenn im folgenden von führenden Termen *etc.* die Rede ist, soll es sich stets um die führenden Terme *etc.* bezüglich dieser Ordnung handeln.

Mit dieser Konvention geht der Algorithmus dann folgendermaßen:

Gegeben sind $f, f_1, \ldots, f_s \in R$
Berechnet werden $a_1, \ldots, a_s, r \in R$ mit $f = a_1 f_1 + \cdots + a_s f_s + r$

1. Schritt (Initialisierung): Setze $a_1 = \cdots = a_s = r = 0$. Falls $f = 0$ endet der Algorithmus damit; andernfalls setzen wir $p = f$.

2. Schritt: Falls keiner der führenden Terme FT f_i den führenden Term FT p teilt, wird p ersetzt durch $p - \mathrm{FT}\, p$ und r durch $r + \mathrm{FT}\, p$.

3. Schritt (Divisionsschritt): Andernfalls sei i der kleinste Index, für den FT f_i Teiler von FT r ist; der Quotient sei q. Dann wird a_i ersetzt durch $a_i + q$ und p durch $p - qf_i$. Weiter geht es mit dem 2. Schritt.

Offensichtlich ist die Bedingung $f - p = a_1 f_1 + \cdots + a_s f_s + r$ nach der Initialisierung im ersten Schritt erfüllt, und sie bleibt auch bei jeder Anwendung des zweiten oder dritten Schritts erfüllt. Außerdem endet der Algorithmus nach endlich vielen Schritten: Bei jedem Divisionsschritt wird der führende Term von p eliminiert, und alle Monome, die eventuell neu dazukommen, sind kleiner oder gleich dem führenden Monom von f_i. Da letzteres das (alte) führende Monom von p teilt, kann es nicht größer sein als dieses, d.h. der führende Term des neuen p ist kleiner als der des alten. Wegen der Wohlordnungseigenschaft einer Monomordnung folgt daraus, daß der Algorithmus nach endlich vielen Schritten abbrechen muß.

Um den Algorithmus besser zu verstehen, betrachten wir zunächst zwei Beispiele:

Als erstes dividieren wir $f = x^2y + xy^2 + y^2$ durch $f_1 = xy - 1$ und $f_2 = y^2 - 1$.

Zur Initialisierung setzen wir $a_1 = a_2 = r = 0$ und $p = f$. Wir verwenden die lexikographische Ordnung; bezüglich derer ist der führende Term von p gleich x^2y und der von f_1 gleich xy. Letzteres teilt x^2y, wir setzen also

$$p \leftarrow p - xf_1 = xy^2 + x + y^2 \quad \text{und} \quad a_1 \leftarrow a_1 + x = x\,.$$

Neuer führender Term von p ist xy^2; auch das ist ein Vielfaches von xy, also setzen wir

$$p \leftarrow p - yf_1 = x + y^2 + y \quad \text{und} \quad a_1 \leftarrow a_1 + y = x + y\,.$$

Nun ist x der führende Term von p, und der ist weder durch xy noch durch y^2 teilbar, also kommt er in den Rest:

$$p \leftarrow p - x = y^2 + y \quad \text{und} \quad r \leftarrow r + x = x\,.$$

Der nun führende Term y^2 von p ist gleichzeitig der führende Term von f_2 und nicht teilbar durch xy, also wird

$$p \leftarrow p - f_2 = y + 1 \quad \text{und} \quad a_2 \leftarrow a_2 + 1 = 1\,.$$

Die verbleibenden Terme von p sind weder durch xy noch durch y^2 teilbar, kommen also in den Rest, so daß wir als Ergebnis erhalten

$$f = a_1 f_1 + a_2 f_2 + r \quad \text{mit} \quad a_1 = x + y, \quad a_2 = 1 \quad \text{und} \quad r = x + y + 1\,.$$

Wenn wir statt durch das Paar (f_1, f_2) durch (f_2, f_1) dividiert hätten, hätten wir im ersten Schritt zwar ebenfalls x^2y durch xy dividiert, denn durch y^2 ist es nicht teilbar. Der neue führende Term xy^2 ist aber durch beides teilbar, und wenn f_2 an erster Stelle steht, nehmen wir im Zweifelsfall dessen führenden Term. Man rechnet leicht nach, daß man hier mit folgendem Ergebnis endet:

$$f = a_1 f_1 + a_2 f_2 + r \quad \text{mit} \quad a_1 = x + 1, \quad a_2 = x \quad \text{und} \quad r = x + 1\,.$$

Wie wir sehen, sind also sowohl die „Quotienten“ a_i als auch der „Rest“ r von der Reihenfolge der f_i abhängig. Sie hängen natürlich im allgemeinen auch ab von der verwendeten Monomordnung; deshalb haben wir die schließlich eingeführt.

Als zweites Beispiel wollen wir $f = xy^2 - x$ durch die beiden Polynome $f_1 = xy + 1$ und $f_2 = y^2 - 1$ dividieren. Im ersten Schritt dividieren wir xy^2 durch xy mit Ergebnis y, ersetzen also f durch $-x - y$. Diese beiden Terme sind weder durch xy noch durch y^2 teilbar, also ist unser Endergebnis

$$f = a_1 f_1 + a_2 f_2 + r \quad \text{mit} \quad a_1 = y, \quad a_2 = 0 \quad \text{und} \quad r = -x - y\,.$$

Hätten wir stattdessen durch (f_2, f_1) dividiert, hätten wir als erstes xy^2 durch y^2 dividiert mit Ergebnis x; da $f = xf_2$ ist, geht die Division hier ohne Rest auf. Der Divisionsalgorithmus erlaubt uns also nicht einmal die sichere Feststellung, ob f als Linearkombination der f_i darstellbar ist oder nicht; als alleiniges Hilfsmittel zur Lösung nichtlinearer Gleichungssysteme reicht er offenbar nicht aus. Daher müssen wir in den folgenden Paragraphen noch weitere Werkzeuge betrachten.

§ 4: Der Hilbertsche Basissatz

Die Grundidee des Algorithmus von BUCHBERGER besteht darin, das Gleichungssystem so abzuändern, daß möglichst viele seiner Eigenschaften bereits an den führenden Termen der Gleichungen ablesbar sind.

Angenommen, wir haben ein nichtlineares Gleichungssystem

$$f_1(x_1, \ldots, x_n) = \cdots = f_r(x_1, \ldots, x_n) = 0 \;\text{ mit } f_i \in R = k[x_1, \ldots, x_n]\,;$$

seine Lösungsmenge sei $\mathcal{L} \subseteq k^n$.

Ist $g = g_1 f_1 + \cdots + g_r f_r$ mit $g_i \in R$ ein beliebiges Element des von $f_1, \ldots, f_r$ erzeugten Ideals $I \lhd R$, so ist für jede Lösung $(x_1, \ldots, x_r)$ aus $\mathcal{L}$ offensichtlich auch $g(x_1, \ldots, x_r) = 0$. Ist $I = (h_1, \ldots, h_s)$ eine andere Erzeugung von I, so hat das obige Gleichungssystem daher dieselbe Lösungsmenge wie das System

$$h_1(x_1, \ldots, x_n) = \cdots = h_s(x_1, \ldots, x_n) = 0\,.$$

Zur Lösung des Systems sollten wir daher versuchen, ein möglichst „einfaches“ Erzeugendensystem für das Ideal I zu finden.

Ganz besonders einfach (wenn auch selten ausreichend) sind Ideale, die von Monomen erzeugt werden:

Definition: Ein Ideal $I \lhd R = k[x_1, \ldots, x_n]$ heißt *monomial*, wenn es von (nicht notwendigerweise endlich vielen) Monomen erzeugt wird.

Nehmen wir an, I werde erzeugt von den Monomen x^α mit α aus einer Indexmenge A. Ist dann x^β irgendein Monom aus I, kann es als endliche Linearkombination

$$x^\beta = \sum_{i=1}^{r} f_i x^{\alpha_i} \quad \text{mit} \quad \alpha_i \in A$$

geschrieben werden, wobei die f_i irgendwelche Polynome aus R sind. Da sich jedes Polynom als Summe von Monomen schreiben läßt, können wir f_i als k-Linearkombination von Monomen x^γ schreiben und bekommen damit eine neue Darstellung von x^β als Summe von Termen der Form $cx^\gamma x^\alpha$ mit $\alpha \in A, \beta \in \mathbb{N}_0^n$ und $c \in k$. Sortieren wir diese Summanden nach den resultierenden Monomen $x^{\gamma+\alpha}$, entsteht eine k-Linearkombination verschiedener Monome, die insgesamt gleich x^β ist. Das ist aber nur möglich, wenn diese Summe aus dem einen Summanden x^β besteht, d.h. β läßt sich schreiben in der Form $\beta = \alpha + \gamma$ mit einem $\alpha \in A$ und einem $\gamma \in \mathbb{N}_0^n$.

Dies zeigt, daß ein Monom x^β genau dann in I liegt, wenn $\beta = \alpha + \gamma$ ist mit einem $\alpha \in A$ und einem $\gamma \in \mathbb{N}_0^n$; das Ideal I selbst besteht

also genau aus den Polynomen f, die sich als k-Linearkombinationen solcher Monome schreiben lassen.

Damit folgt insbesondere, daß ein Polynom f genau dann in einem monomialen Ideal I liegt, wenn jedes seiner Monome dort liegt.

Lemma von Dickson: Jedes monomiale Ideal in $R = k[x_1, \ldots, x_n]$ kann von endlich vielen Monomen erzeugt werden.

Der *Beweis* wird durch vollständige Induktion nach n geführt. Im Fall $n = 1$ ist alles klar, denn da sind die Monome gerade die Potenzen der einzigen Variable, und natürlich erzeugt jede Menge von Potenzen genau dasselbe Ideal wie die Potenz mit dem kleinsten Exponenten aus dieser Menge. Hier kommt man also sogar mit einem einzigen Monom aus.

Für $n > 1$ bezeichnen wir für $\alpha \in \mathbb{N}_0^n$ mit x'^α das Monom $x_1^{\alpha_1} \cdots x_{n-1}^{\alpha_{n-1}}$ und betrachten das Ideal

$$J = \left(x'^\alpha \;\middle|\; x^\alpha \in I\right) \lhd k[x_1, \ldots, x_{n/1}]\,.$$

Nach Induktionsvoraussetzung wird J erzeugt von endlich vielen Monomen x'^α

Jedes Monom aus aus dem endlichen Erzeugendensystem von J läßt sich in der Form x'^α schreiben mit einem $\alpha \in \mathbb{N}_0^n$, für das x^α in I liegt. Unter den Indizes α_n, die wir dabei jeweils an das $(n-1)$-tupel $(\alpha_1, \ldots, \alpha_{n-1})$ anhängen, sei r der größte. Dann liegt $x'^{\alpha'} x_n^r$ für jedes Monom aus dem Erzeugendensystem von J in I und damit für jedes Monom aus J. Die endlich vielen Monome $x^{\alpha'} x_n^r$ erzeugen also zumindest ein Teilideal von I.

Es gibt aber natürlich auch noch Monome in I, in denen x_n mit einem kleineren Exponenten als r auftritt. Um auch diese Elemente zu erfassen, betrachten wir für jedes $s < r$ das Ideal $J_s \lhd k[x_1, \ldots, x_{n-1}]$, das von allen jeden Monomen x'^α erzeugt wird, für die $x'^\alpha x_n^s$ in I liegt. Auch jedes der J_s wird nach Induktionsannahme erzeugt von endlich vielen Monomen x'^α, und wenn wir die sämtlichen Monome $x'^\alpha x_n^s$ zu unserem Erzeugendensystem hinzunehmen (für alle $s = 0, 1, \cdots, r-1$),

haben wir offensichtlich ein Erzeugendensystem von I aus endlich vielen Monomen gefunden.

■

Beliebige Ideale sind im allgemeinen nicht monomial; schon das von $x+1$ erzeugte Ideal in $k[x]$ ist ein Gegenbeispiel, denn es enthält weder das Monom x noch das Monom 1, im Widerspruch zu der oben gezeigten Eigenschaft eines monomialen Ideals, zu jedem seiner Elemente auch dessen sämtliche Monome zu enthalten.

Um monomiale Ideale auch für die Untersuchung solcher Ideale nützlich zu machen, wählen wir eine Monomordnung auf R und definieren für ein beliebiges Ideal $I \lhd R \underset{\text{def}}{=} k[x_1, \ldots, x_n]$ das monomiale Ideal

$$\text{FM}(I) = \Big(\text{FM}(f) \;\Big|\; f \in I \setminus \{0\}\Big)\,,$$

das von den führenden Monomen *aller* Elemente von I erzeugt wird – außer natürlich dem nicht existierenden führenden Term der Null.

Nach dem Lemma von DICKSON ist FM(I) erzeugt von endlich vielen Monomen. Jedes dieser Monome ist, wie wir eingangs gesehen haben, ein Vielfaches eines der erzeugenden Monome, also eines führenden Monoms eines Elements von I. Ein Vielfaches des führenden Monoms ist aber das führende Monom des entsprechenden Vielfachen des Elements von I, denn FM($x^\gamma f$) = x^γ FM(f), da für jede Monomordnung gilt $\alpha < \beta \Longrightarrow \alpha+\beta < \alpha+\gamma$. Somit wird FM($I$) erzeugt von endlich vielen Monomen der Form FM(f_i), wobei die f_i Elemente von I sind. Wir wollen sehen, daß die Elemente f_i das Ideal I erzeugen; damit folgt insbesondere

Hilbertscher Basissatz: Jedes Ideal $I \lhd R = k[x_1, \ldots, x_n]$ hat ein endliches Erzeugendensystem.

Beweis: Wie wir bereits wissen, gibt es Elemente $f_1, \ldots f_m \in I$, so daß FM(I) von den Monomen FM(f_i) erzeugt wird. Um zu zeigen, daß die Elemente f_i das Ideal I erzeugen, betrachten wir ein beliebiges Element $f \in I$ und versuchen, es als R-Linearkombination der f_i zu schreiben. Division von f durch $f_1, \ldots, f_m$ zeigt, daß es Polynome $a_1, \ldots, a_m$ und r in R gibt derart, daß

$$f = a_1 f_1 + \cdots + a_m f_m + r\,.$$

Wir sind fertig, wenn wir zeigen können, daß der Divisionsrest r verschwindet.

Falls r *nicht* verschwindet, zeigt der Divisionsalgorithmus, daß das führende Monom FM(r) von r durch kein führendes Monom FM(f_i) eines der Divisoren f_i teilbar ist. Andererseits ist aber

$$r = f - (a_1 f_1 + \cdots + a_m f_m)$$

ein Element von I, und damit liegt FM(r) im von den FM(f_i) erzeugten Ideal FM(I). Somit muß FM(r) Vielfaches eines FM(f_i) sein, ein Widerspruch. Also ist $r = 0$.

■

§5: Gröbner-Basen und der Buchberger-Algorithmus

Angesichts der Rolle der führenden Monome im obigen Beweis bietet sich folgende Definition an für eine Idealbasis, bezüglich derer möglichst viele Eigenschaften bereits an den führenden Monomen abgelesen werden können:

Definition: Eine endliche Teilmenge $G = \{g_1, \ldots, g_m\} \subset I$ eines Ideals $I \lhd R = k[x_1, \ldots, x_n]$ heißt Standardbasis oder GRÖBNER-Basis von I, falls die Monome FM(g_i) das Ideal FM(I) erzeugen.

Wie der obige Beweis des HILBERTschen Basissatzes zeigt, erzeugt eine GRÖBNER-Basis das Ideal, und jedes Ideal im Polynomring hat eine GRÖBNER-Basis. Bevor wir uns damit beschäftigen, wie man diese berechnen kann, wollen wir zunächst eine wichtige Eigenschaften betrachten.

Sei $g_1, \ldots, g_m$ GRÖBNER-Basis eines Ideals $I \lhd R$. Wir wollen ein beliebiges Element $f \in R$ durch $g_1, \ldots, g_m$ dividieren. Dies liefert als Ergebnis

$$f = a_1 g_1 + \cdots + a_m g_m + r\,,$$

wobei kein Monom von r durch eines der Monome FM(g_i) teilbar ist. Wie wir wissen, sind allerdings bei der Polynomdivision weder der Divisionsrest r noch die Koeffizienten a_i auch nur im entferntesten

eindeutig. Sei etwa $f = a_1g_1 + \cdots + a_mg_m + r = b_1g_1 + \cdots + b_mg_m + s$; dann ist $(a_1 - b_1)g_1 + \cdots + (a_m - b_m)g_m = s - r$.

Links steht ein Element von I, also auch rechts. Andererseits enthält aber weder r noch s ein Monom, das durch eines der Monome $\mathrm{FM}(g_i)$ teilbar ist, d.h. $r - s = 0$. Somit ist bei der Division durch die Elemente einer GRÖBNER-Basis der Divisionsrest eindeutig bestimmt. Insbesondere ist f genau dann ein Element von I, wenn der Divisionsrest verschwindet. Wenn wir eine GRÖBNER-Basis haben, können wir also leicht entscheiden, ob ein gegebenes Element $f \in R$ im Ideal I liegt.

Nachdem im Fall einer GRÖBNER-Basis der Divisionsrest nicht von der Reihenfolge der Basiselemente abhängt, können wir ihn durch ein Symbol bezeichnen, das nur von der *Menge* $G = \{g_1, \ldots, g_m\}$ abhängt; wir schreiben $\overline{f}^G$.

Als nächstes wollen wir uns überlegen, wie sich eine GRÖBNER-Basis eines vorgegebenen Ideals I finden läßt.

Dazu müssen wir uns als erstes überlegen, *wie* das Ideal vorgegeben sein soll. Wenn wir damit rechnen wollen, müssen wir irgendeine Art von endlicher Information haben; was sich anbietet ist natürlich ein endliches Erzeugendensystem.

Wir gehen also aus von einem Ideal $I = (f_1, \ldots, f_m)$ und suchen eine GRÖBNER-Basis. Das Problem ist, daß die Monome $\mathrm{FM}(f_i)$ im allgemeinen nicht ausreichen, um das monomiale Ideal $\mathrm{FM}(I)$ zu erzeugen, denn dieses enthält ja *jedes* Monom eines jeden Elements von I und nicht nur das führende. Wir müssen daher neue Elemente produzieren, deren führende Monome in den gegebenen Elementen f_i oder auch anderen Elementen von I erst weiter hinten vorkommen.

BUCHBERGERS Idee dazu war die Konstruktion sogenannter S-Polynome: Seien $f, g \in R$ zwei Polynome; $\mathrm{FM}(f) = x^\alpha$ und $\mathrm{FM}(g) = x^\beta$ seien ihre führenden Monome, und x^γ sei das kgV von x^α und x^β, d.h. $\gamma_i = \max(\alpha_i, \beta_i)$ für alle $i = 1, \ldots, n$. Das S-Polynom von f und g ist

$$S(f,g) = \frac{x^\gamma}{\mathrm{FT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{FT}(g)} \cdot g\,.$$

Da $\frac{x^\gamma}{\mathrm{FT}(f)} \cdot f$ und $\frac{x^\gamma}{\mathrm{FT}(g)} \cdot g$ beide nicht nur dasselbe führende Monom x^γ haben, sondern es wegen der Division durch den führenden *Term* statt nur das führende Monom auch beide mit Koeffizient eins enthalten, fällt es bei der Bildung von $S(f,g)$ weg, d.h. $S(f,g)$ hat ein kleineres führendes Monom. Das folgende Lemma ist der Kern des Beweises, daß S-Polynome alles sind, was wir brauchen, um GRÖBNER-Basen zu berechnen.

Lemma: Für die Polynome $f_1, \ldots, f_m \in R$ sei

$$S = \sum_{i=1}^m \lambda_i x^{\alpha_i} f_i \quad \text{mit} \quad \lambda_i \in k \quad \text{und} \quad \alpha_i \in \mathbb{N}_0^n$$

eine Linearkombination zu der es ein $\delta \in \mathbb{N}_0^n$ gebe, so daß alle Summanden x^δ als führendes Monom haben, d.h. $\alpha_i + \text{multideg } f_i = \delta_i$ für $i = 1, \ldots, n$. Falls multideg $S < \delta$ ist, gibt es Elemente $\lambda_{ij} \in k$, so daß

$$S = \sum_{i=1}^m \sum_{j=1}^m \lambda_{ij} x^{\gamma_{ij}} S(f_i, f_j)$$

ist mit $x^{\gamma_{ij}} = \mathrm{kgV}\big(\mathrm{FM}(f_i), \mathrm{FM}(f_j)\big)$.

Beweis: Der führende Koeffizient von f_i sei μ_i; dann ist $\lambda_i\mu_i$ der führende Koeffizient von $\lambda_i x^{\alpha_i} f_i$. Somit ist multideg S genau dann kleiner als δ wenn $\sum_{i=1}^m \lambda_i\mu_i$ verschwindet. Wir normieren alle $x^{\alpha_i} f_i$ auf führenden Koeffizienten eins, indem wir $p_i = x^{\alpha_i} f_i/\mu_i$ betrachten; dann ist

$$\begin{aligned} S = \sum_{i=1}^m \lambda_i\mu_i p_i = {} & \lambda_1\mu_1(p_1 - p_2) + (\lambda_1\mu_1 + \lambda_2\mu_2)(p_2 - p_3) + \cdots \\ & + (\lambda_1\mu_1 + \cdots + \lambda_{m-1}\mu_{m-1})(p_{m-1} - p_m) \\ & + (\lambda_1\mu_1 + \cdots + \lambda_m\mu_m)p_m\,. \end{aligned}$$

Da alle p_i denselben Multigrad δ und denselben führenden Köeffizienten eins haben, kürzen sich in den Differenzen $p_i - p_j$ die führenden Terme weg, genau wie in den S-Polynomen. In der Tat: Bezeichnen wir den Multigrad von $\mathrm{kgV}\big(\mathrm{FM}(f_i), \mathrm{FM}(f_j)\big)$ mit γ_{ij}, so ist

$$p_i - p_j = x^{\delta - \gamma_{ij}} S(f_i, f_j)\,.$$

Damit hat die obige Summendarstellung von S die gewünschte Form. ∎