## Das Kriterium von Buchberger

Aus der letzten Vorlesung wissen wir, daß jedes Ideal im Polynomring $R = k[X_1, \ldots, X_n]$ bezüglich jeder Monomordnung eine GRÖBNER-Basis hat. Leider war der Beweis dafür nicht konstruktiv, genau wie auch der Beweis des HILBERTschen Basissatzes, den wir ja aus der Existenz von GRÖBNER-Basen gefolgert haben.

Bei HILBERTschen Basissatz braucht uns das nicht weiter zu stören, denn die Ideale, die wir hier betrachten, kommen von nichtlinearen Gleichungssystemen, sind also ohnehin durch endlich viele Polynome definiert. Von den GRÖBNER-Basen hoffen wir, daß sie uns (zumindest für geeignete Monomordnungen) helfen, die Lösungsmenge des Gleichungssystems zu finden, und dazu brauchen wir sie natürlich explizit. Wir benötigen also ein Verfahren, das uns zu einem gegebenen endlichen Erzeugendensystem eines Ideals $I$ und einer vorgegebenen Monomordnung eine GRÖBNER-Basis von $I$ liefert. Dazu gibt es mittlerweile eine ganze Reihe von Möglichkeiten; die erste und auch einfachste ist der Algorithmus, den BRUNO BUCHBERGER 1966 in seiner Dissertation veröffentlicht hat.

Kehren wir noch einmal zurück zum Eingangsbeispiel der letzten Vorlesung mit

$$f_1 = 2X^4 + 3Y^2 + 4X^2Y - 15Y + 36$$

und

$$f_2 = 5X^4 - 7Y^2 + 10X^2Y + 35Y + 3$$

aus $\mathbb{Q}[X, Y]$. $f_1$ und $f_2$ bilden keine GRÖBNER-Basis bezüglich der lexikographischen Ordnung, denn sie haben beide das führende Monom $X^4$, während im von $f_1$ und $f_2$ erzeugten Ideal auch beispielsweise das Polynom $5f_1 - 2f_2 = 29Y^2 - 145Y + 66$ liegt, dessen führendes Monom $Y^2$ nicht im von $X^4$ erzeugten monomialen Ideal liegt. Um zu einer GRÖBNER-Basis zu kommen, müssen wir das Erzeugendensystem aus $f_1$ und $f_2$ daher noch ergänzen durch weitere Polynome, die zwar nicht zur Erzeugung des Ideals gebraucht werden, deren führende Monome wir aber brauchen, um das Ideal der führenden Monome von $(f_1, f_2)$

zu erzeugen. Dazu müssen wir, ähnlich wie wir es von der GAUSS-Elimination gewohnt sind, Linearkombinationen bilden, bei denen sich geeignete Vielfache der führenden Terme gegenseitig wegheben. Im Gegensatz zur Situation bei linearen Gleichungssystemen (und auch zum gerade betrachteten Beispiel $5f_1 - 2f_2$) genügen dabei allerdings skalare Linearkombinationen im Allgemeinen nicht: Falls etwa alle Ausgangspolynome verschiedene führende Monome haben, läßt sich so keines eliminieren. Wir müssen die Polynome daher noch mit geeigneten Monomen multiplizieren, um so zunächst zu erreichen, daß die Produkte das gleiche führende Monom bekommen. Im Falle zweier Polynome führt das zu BUCHBERGERs $S$-Polynomen:

**Definition:** $f, g \in R = k[X_1, \ldots, X_n]$ seien zwei Polynome; ihre führenden Monome seien $\mathrm{FM}\, f = X^\alpha$ und $\mathrm{FM}\, g = X^\beta$. Weiter sei $X^\gamma$ das kgV von $X^\alpha$ und $X^\beta$, d.h. $\gamma_i = \max(\alpha_i, \beta_i)$ für $i = 1, \ldots, n$. 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 $X^\gamma$ 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. Daher ist das führende Monom von $S(f,g)$ kleiner als $X^\gamma$. 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

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

eine Linearkombination, zu der es ein $\delta \in \mathbb{N}_0^n$ gebe, so daß alle Summanden $X^\delta$ als führendes Monom haben, d.h. $\alpha_i + \text{multideg}\, f_i = \delta_i$ für $i = 1, \ldots, m$. Falls $\text{multideg}\, S < \delta$ 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 $X^{\gamma_{ij}} = \text{kgV}(\text{FM}\, f_i, \text{FM}\, f_j)$.

*Beweis:* Der führende Koeffizient von $f_i$ sei $\mu_i$; 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 $\delta$, 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 können wir $S$ schreiben als eine Teleskopsumme

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

wobei der Summand in der letzten Zeile genau dann verschwindet, wenn multideg $S < \delta$ ist.

Da alle $p_i$ denselben Multigrad $\delta$ und denselben führenden Koeffizienten 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 $\text{kgV}(\text{FM}\, f_i, \text{FM}\, f_j)$ mit $\gamma_{ij}$, 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. ∎

Wenn wir also irgendeine Linearkombination der Polynome $f_i$ haben, in der sich die führenden Terme wegkürzen, so daß ein führendes Monom entsteht, das nicht automatisch Vielfaches eines der FM $f_i$ ist, können wir dieses neue führende Monom auch als führendes Monom eines $S$-Polynoms erzeugen.

**Definition:** Wir sagen, ein Polynom $f \in R$ kann bezüglich einer vorgegebenen Monomordnung modulo der Polynome $f_1, \ldots, f_m \in R$ auf Null reduziert werden, wenn es eine Darstellung

$$f = q_1 f_1 + \cdots + q_m f_m$$

gibt, bei der FM($q_i f_i$) $\leq$ FM $f$ ist für alle $i = 1, \ldots, m$.

Im ersten Beispiel dieser Vorlesung ist

$$f = 29Y^2 - 145Y + 66 = 5f_1 - 2f_2$$

zwar eine Linearkombination von $f_1$ und $f_2$, aber FM $f = Y^2$ ist kleiner als FM($5f_1$) = FM($-2f_2$) = $X^4$, so daß diese Darstellung $f$ nicht auf Null reduziert. In der Tat kann $f$ modulo $f_1$ und $f_2$ bezüglich der lexikographischen Ordnung nicht auf Null reduziert werden, denn wann immer ein Polynom $f$ modulo irgendwelcher Polynome $f_1, \ldots, f_m$ auf Null reduziert werden kann, muß FM $f$ gleich mindestens einem der FM($q_i f_i$) und damit Vielfaches eines der FM $f_i$ sein.

Wenn wir den Divisionsalgorithmus anwenden auf $f$ und $f_1, \ldots, f_m$, erhalten wir eine Darstellung $f = q_1 f_1 + \cdots + q_m f_m + r$, bei der nach Konstruktion rechts nur Monome stehen, die nicht größer als FM $f$ sein können. Falls der Divisionsrest $r$ verschwindet, kann $f$ also modulo $f_1, \ldots, f_m$ auf Null reduziert werden. Wie wir in der Vorlesung über den Divisionsalgorithmus gesehen haben, können wir aber gelegentlich auch einen von Null verschiedenen Divisionsrest erhalten, obwohl wir bei einer anderen Reihenfolge der Divisoren Rest Null erhalten und $f$ somit auf Null reduzierbar ist. Wenn $f_1, \ldots, f_m$ eine GRÖBNER-Basis bilden, kann das nicht passieren:

Angenommen, der Divisionsalgorithmus liefert uns bei verschiedenen Reihenfolgen der Divisoren zwei Darstellungen

$$f = a_1 f_1 + \cdots + a_m f_m + r = b_1 f_1 + \cdots + b_m f_m + s\,.$$

Dann ist

$$(a_1 - b_1) f_1 + \cdots + (a_m - b_m) f_m = s - r\,.$$

Links steht ein Element von $I$, also auch rechts. Andererseits enthält aber weder $r$ noch $s$ ein Monom, das durch eines der Monome FM($f_i$) teilbar ist, d.h. $r - s = 0$, da die FM($f_i$) ja das Ideal FM($I$) erzeugen. 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 oder nicht.

Daraus und aus dem letzten Lemma folgt nun ziemlich unmittelbar

**Buchbergers Kriterium:** Ein Erzeugendensystem $f_1, \ldots, f_m$ eines Ideals $I$ im Polynomring $R = k[X_1, \ldots, X_n]$ ist genau dann eine GRÖBNER-Basis, wenn jedes $S$-Polynom $S(f_i, f_j)$ modulo $f_1, \ldots, f_m$ auf Null reduziert werden kann.

*Beweis:* Als $R$-Linearkombination von $f_i$ und $f_j$ liegt das $S$-Polynom $S(f_i, f_j)$ im Ideal $I$; falls $f_1, \ldots, f_m$ eine GRÖBNER-Basis von $I$ ist, hat es also Rest Null bei der Division durch $f_1, \ldots, f_m$.

Umgekehrt sei $f_1, \ldots, f_m$ ein Erzeugendensystem von $I$ mit der Eigenschaft, daß alle $S(f_i, f_j)$ modulo $f_1, \ldots, f_m$ auf Null reduziert werden können. Wir wollen zeigen, daß $f_1, \ldots, f_m$ dann eine GRÖBNER-Basis ist, daß also die führenden Monome FM $f_1, \ldots,$ FM $f_m$ das Ideal FM $I$ erzeugen.

Sei dazu $f \in I$ ein beliebiges Element; wir müssen zeigen, daß FM $f$ im von den FM $f_i$ erzeugten Ideal liegt. Da $f$ in $I$ liegt, gibt es eine Darstellung

$$f = h_1 f_1 + \cdots + h_m f_m \quad \text{mit} \quad h_i \in R\,.$$

Falls sich hier bei den führenden Termen nichts wegkürzt, ist der führende Term von $f$ die Summe der führenden Terme gewisser Produkte $h_i f_i$, die allesamt dasselbe führende Monom FM $f$ haben. Wegen FM$(h_i f_i)$ = FM$(h_i)$ FM$(f_i)$ liegt FM $f$ daher im von den FM $f_i$ erzeugten Ideal.

Falls sich die maximalen unter den führenden Termen FT$(h_i f_i)$ gegenseitig wegkürzen, läßt sich die entsprechende Teilsumme der $h_i f_i$ nach dem vorigen Lemma auch als eine Summe von $S$-Polynomen schreiben. Diese wiederum lassen sich nach Voraussetzung modulo der $f_i$ auf Null reduzieren. Damit erhalten wir eine neue Darstellung

$$f = \widetilde{h}_1 f_1 + \cdots + \widetilde{h}_m f_m \quad \text{mit} \quad \widetilde{h}_i \in R\,,$$

in der der maximale Multigrad eines Summanden echt kleiner ist als in der obigen Darstellung, denn in der Darstellung als Summe von $S$-Polynomen sind die Terme mit dem maximalem Multigrad verschwunden.

Mit dieser Darstellung können wir wie oben argumentieren: Falls sich bei den führenden Termen nichts wegkürzt, haben wir FM $f$ als Element des von den FM $f_i$ erzeugten Ideals dargestellt, andernfalls erhalten wir wieder via $S$-Polynome und deren Reduktion eine neue Darstellung von $f$ als Linearkombination der $f_i$ mit noch kleinerem maximalem Multigrad der Summanden, und so weiter. Das Verfahren muß schließlich mit einer Summe ohne Kürzungen bei den führenden Termen enden, da es nach der Wohlordnungseigenschaft einer Monomordnung keine unendliche absteigende Folge von Multigraden geben kann. ∎

Um zu überprüfen, ob ein $S$-Polynom auf Null reduziert werden kann, bietet sich in erster Linie der Divisionsalgorithmus an, auch wenn der das, wie wir gesehen haben, nicht immer erkennt. Gelegentlich kann man aber auch ganz auf Divisionen verzichten; beispielsweise gilt:

**Lemma:** Falls die führenden Monome zweier Polynome $f, g \in R$ teilerfremd sind, kann $S(f, g)$ modulo $f, g$ (und damit auch modulo jedes Erzeugendensystems, das $f$ und $g$ enthält) auf Null reduziert werden.

*Beweis:* Der führende Term von $f$ sei $aX^\alpha$, der von $g$ sei $bX^\beta$. Wir schreiben $f = aX^\alpha + ap$ und $g = bX^\beta + bq$ mit $p, q \in R$. Da die führenden Monome $X^\alpha$ und $X^\beta$ teilerfremd sind, ist ihr kgV $X^\gamma = X^{\alpha+\beta}$, also ist

$$\begin{aligned} S(f,g) &= \frac{X^\gamma}{aX^\alpha} \cdot (aX^\alpha + ap) - \frac{X^\gamma}{bX^\beta} \cdot (bX^\beta + bq) = X^\beta \cdot p - X^\alpha \cdot q \\ &= \frac{g-q}{a} \cdot ap - \frac{f-p}{b} \cdot bq = (g-q)p - (f-p)q = pg - qf\,. \end{aligned}$$

Das führende Monom von $S(f, g)$ ist entweder $X^\beta$ FM $p$ oder $X^\alpha$ FM $q$, denn erstens sind alle anderen Monome, die in $X^\beta p$ und $X^\alpha q$ vorkommen, kleiner als eines dieser beiden, und zweitens können sich die Terme $X^\beta$ FT $p$ und $X^\alpha$ FT $q$ nicht wegheben, denn sonst wäre $X^\beta$ FM $p = X^\alpha$ FM $q$ ein gemeinsames Vielfaches von $X^\alpha$ und $X^\beta$, das kleiner wäre als das Produkt $X^\alpha \cdot X^\beta$, im Widerspruch zur Teilerfremdheit der beiden Monome. Somit reduziert die Darstellung $S(f, g) = pq - qf$ das $S$-Polynom auf Null. ∎