Gröbner-Basen

Angenommen, wir suchen die gemeinsamen Nullstellen der beiden Polynome

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

und

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

Zumindest auf den ersten Blick ist es schwer, einen Ansatz dafür zu erkennen, und auf den zweiten Blick sieht man auch nicht viel mehr. Erheblich einfacher ist es bei den beiden Polynomen

$$g_1 = X^4 + 2X^2Y + 9 \qquad \text{und} \qquad g_2 = Y^2 - 5Y + 6\,,$$

denn g_2 ist ein Polynom nur in Y, dessen Nullstellen 2 und 3 sich einfach bestimmen lassen. Setzen wir die in g_1 ein, erhalten wir die beiden Polynome X^4+4X^2+9 und X^4+6X^2+9 in nur der einen Variablen X, und deren Nullstellen können wir berechnen: Beide sind quadratische Polynome in X^2; das erste hat die Lösungen $x^2 = -2 \pm \sqrt{-5}$, also $x = \pm\sqrt{-2 \pm \sqrt{-5}}$ oder, wenn wir die Wurzel ausrechnen, $x = \pm\frac{1}{2}\sqrt{2} \pm \frac{1}{2}\sqrt{-10}$. Das zweite Polynom ist $(X^2+3)^2$, hat also $\pm\sqrt{-3}$ als doppelte Nullstellen. Die gemeinsamen Nullstellen von g_1 und g_2 sind somit $\left(\pm\frac{1}{2}\sqrt{2} \pm \frac{1}{2}\sqrt{-10},\ 2\right)$ und $\left(\pm\sqrt{-3},\ 3\right)$.

Tatsächlich sind das auch die gemeinsamen Nullstellen von f_1 und f_2, denn $f_1 = 2g_1 + 3g_2$ und $f_2 = 5g_1 - 7g_2$ sind einfach ganzzahlige Linearkombinationen von g_1 und g_2, und g_1, g_2 sind entsprechend (rationale) Linearkombinationen von f_1 und f_2. Im Allgemeinen läßt sich ein nichtlineares Gleichungssystem nicht schon durch skalare Linearkombinationen derart vereinfachen; GRÖBNER-Basen liefern aber eine Methode, mit der man jedes nichtlineare Gleichungssystem, dessen Lösungsmenge auch noch über einem algebraisch abgeschlossenen Körper endlich bleibt, auf eine ähnliche Form bringen kann.

Wir arbeiten über einem beliebigen Körper k.

Wenn $(x_1, \ldots, x_n)$ eine gemeinsame Nullstelle von m Polynomen $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ ist, verschwindet auch jedes Polynom

$$f = h_1 f_1 + \cdots + h_m f_m \ \text{ mit } \ h_1, \ldots, h_m \in k[X_1, \ldots, X_n]$$

im Punkt $(x_1, \ldots, x_n)$. Die Polynome, die sich so darstellen lassen, sind genau die aus dem von $f_1, \ldots, f_m$ erzeugten Ideal. Wenn wir irgendwelche andere Polynome $g_1, \ldots, g_r \in k[X_1, \ldots, X_n]$ finden, die dasselbe Ideal erzeugen, sind natürlich die gemeinsamen Nullstellen von $f_1, \ldots, f_m$ in k^n genau die gleichen wie die von $g_1, \ldots, g_r$, aber bei geschickter Wahl der g_j lassen sie sich über diese vielleicht einfacher bestimmen.

Die wesentliche Philosophie bei GRÖBNER-Basen besteht darin, so viel wie möglich mit den führenden Monome zu arbeiten. Wir wählen daher eine feste Monomordnung auf $\mathbb{N}_0^n$ und definieren:

Definition: *a)* I sei ein Ideal in $k[X_1, \ldots, X_n]$. Das Ideal der führenden Monome von I bezüglich einer vorgegebenen Monomordnung ist das Ideal FM I in $k[X_1, \ldots, X_n]$, das von den führenden Monomen FM f der Elemente $f \in I \setminus \{0\}$ erzeugt wird.
b) Eine Teilmenge $\{g_1, \ldots, g_r\}$ eines Ideals I heißt eine GRÖBNER-Basis von I bezüglich einer vorgegebenen Monomordnung, wenn die führenden Monome FM $g_1, \ldots,$ FM g_r das Ideal FM I erzeugen.

(WOLFGANG GRÖBNER (1899-1980) war der Lehrer von BRUNO BUCHBERGER; er beschäftigte sich zwar intensiv mit Idealen in Polynomringen, betrachte aber nie die von BUCHBERGER zu seinen Ehren als GRÖBNER-Basen bezeichneten Teilmengen und ahnte auch nicht, welch große Bedeutung diese hauptsächlich erst nach seinem Tod in der Mathematik bekommen würden.)

Im obigen Beispiel ist $\{f_1, f_2\}$ offensichtlich keine GRÖBNER-Basis von $I = (f_1, f_2)$ bezüglich der lexikographischen Ordnung, denn bezüglich dieser Ordnung haben sowohl f_1 als auch f_2 das führende Monom X^4. Das Ideal enthält aber auch das Polynom g, und FM $g = Y^2$ liegt nicht im von X^4 erzeugten Ideal. $\{g_1, g_2\}$ ist eine GRÖBNER-Basis, allerdings können wir mit unseren bisherigen Methoden noch nicht beweisen, daß wirklich *jedes* Polynom aus dem von f_1 und f_2 (oder g_1 und g_2) erzeugten Ideal bezüglich der lexikographischen Ordnung ein führendes Monom hat, das im von FM $g_1 = X^4$ und FM $g_2 = Y^2$ erzeugten Ideal liegt. Außerdem ist im Augenblick noch völlig unklar, ob und wie GRÖBNER-Basen bei der Lösung nichtlinearer Gleichungssysteme helfen können,

auch wenn das Beispiel nahelegt, daß die Lösung möglicherweise einfacher ist, wenn die Gleichungen viele verschiedene führende Monome haben.

Um solche Fragen zu klären, müssen wir uns zunächst Ideale, die von Monomen erzeugt werden, etwas genauer betrachten. Die Darstellung hier folgt weitgehend der im ersten Kapitel des Buchs

TAKAYUKI HIBI [Hrsg.]: Gröbner Bases – Statistics and Software Systems, *Springer,* 2013,

das über die Universitätsbibliothek auch elektronisch zur Verfügung steht.

Definition: Ein Ideal I im Polynomring $k[X_1, \ldots, X_n]$ heißt *monomiales Ideal,* wenn es von einer Menge von Monomen in $X_1, \ldots, X_n$ erzeugt werden kann.

In diesem Sinne ist also das Ideal (X^4, Y^2) in $k[X, Y]$ ein monomiales Ideal, aber auch das Ideal FM(f_1, f_2), das von den führenden Monomen aller Polynome aus (f_1, f_2) erzeugt wird. Wie schon erwähnt, stimmen die beiden monomialen Ideale überein, aber das können wir noch nicht beweisen.

Lemma: Ein Monom u aus $k[X_1, \ldots, X_n]$ liegt genau dann im von den Monomen $u_1, \ldots, u_r$ erzeugten monomialen Ideal, wenn es durch mindestens eines der u_i teilbar ist.

Beweis: Wenn u durch ein u_i teilbar ist, ist ein Vielfaches von u_i und liegt daher natürlich in $(u_1, \ldots, u_r)$.

Von einem beliebigen Monom aus $(u_1, \ldots, u_r)$ wissen wir zunächst nur, daß es sich irgendwie in der Form

$$u = h_1 u_1 + \cdots + h_r u_r \quad \text{mit} \quad h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$$

schreiben läßt. Die Polynome h_i lassen sich als Linearkombinationen

$$h_i = \sum_{j=1}^{m_i} c_{ij} v_{ij}$$

schreiben mit Monomen v_{ij} aus $k[X_1, \ldots, X_n]$ und Elementen $c_{ij} \in k$, von denen wir voraussetzen können, daß keines davon verschwindet.

(Falls ein h_i das Nullpolynom ist, setzen wir $m_i = 0$ und haben dann eine leere Summe, die nach üblicher mathematischer Konvention den Wert Null hat.) Einsetzen zeigt, daß

$$u = \sum_{i=1}^{r} h_i u_i = \sum_{i=1}^{r} \sum_{j=1}^{m_i} c_{ij} v_{ij} u_i$$

ist. Das kann nur gelten, wenn es Indizes i, j gibt, für die $u = v_{ij} u_i$ ist; u muß also durch mindestens ein u_i teilbar sein.

■

Definition: $M \subset k[X_1, \ldots, X_n]$ sei eine Menge von Monomen. Ein Element $u \in M$ heißt *minimal,* falls es in M keinen echten Teiler hat.

In $M = \{X^2, XY, Y^3, X^2Y, X^5\}$ beispielsweise sind die Monome X^2, XY und Y^3 minimal; X^2Y hat X^2 und XY als echte Teiler, und X^5 ist durch X^2 teilbar. Man beachte, daß dieser Minimalitätsbegriff natürlich nichts mit einer Monomordnung zu tun hat! Bezüglich einer Monomordnung hat jede Menge genau ein kleinstes Element. Im Beispiel wäre das im Falle der lexikographischen Ordnung mit $X < Y$ das Monom X^2, im Falle derer mit $Y < X$ wäre es Y^3, für die graduierte lexikographische Ordnung mit $X < Y$ wieder X^2, für die mit $Y < X$ wäre es XY. In jedem Fall allerdings ist es ein auch bezüglich der Teilbarkeit minimales Monom, denn ein echter Teiler eines Monoms ist ja bezüglich jeder Monomordnung kleiner als das Monom selbst.

Lemma von Dickson: *a)* Die Teilmenge der minimalen Monome ist in jeder Menge M von Monomen endlich.
b) Jedes monomiale Ideal kann von endlich vielen Monomen erzeugt werden.

Beweis: a) Wir beweisen die Behauptung durch Induktion nach der Variablenanzahl n. Für $n = 1$ ist jedes Monom eine Potenz der einen Variablen, und in jeder Menge von Monomen ist offensichtlich die Potenz mit dem kleinsten Exponenten das einzige minimale Element.

Für $n > 1$ betrachten wir die Menge M' aller Monome $X_1^{e_1} \cdots X_{n-1}^{e_{n-1}}$ in $X_1, \ldots, X_{n-1}$ mit der Eigenschaft, daß für irgendein $e \in \mathbb{N}_0$ das Monom $X_1^{e_1} \cdots X_{n-1}^{e_{n-1}} X_n^e$ in M liegt. Nach Induktionsannahme enthält

diese Menge nur endlich viele Monome; diese seien $u_1, \ldots, u_r$. Für jedes u_i gibt es (mindestens) einen Exponenten f_i, so daß $u_i X_n^{f_i}$ in M liegt; wir wählen jeweils ein solches f_i aus. Das Maximum aller f_i sei f. Für jedes $e < f$ sei M'_e die Menge aller Monome $X_1^{e_1} \cdots X_{n-1}^{e_{n-1}}$, für die $X_1^{e_1} \cdots X_{n-1}^{e_{n-1}} X_n^e$ in M liegt. Auch jede dieser Mengen enthält nach Induktionsannahme höchstens endlich viele Elemente; sei etwa $M'_e = \{u_1^{(e)}, \ldots, u_{s_e}^{(e)}\}$.

Jedes Monom aus M kann geschrieben werden als uX_n^e, wobei u ein Monom aus M' ist. Falls $e \geq f$ ist, hat es eines der endliche vielen Monome $u_i X_n^{f_i}$ als Teiler, ist also nicht minimal. Andernfalls ist es eines der endlich vielen Monome $u_i^{(e)} X_n^e$ mit $e < f$. Somit liegen alle minimalen Monome aus M in der endlichen Menge bestehend aus den $u_i X_n^{f_i}$ und den $u_i^{(e)} X_n^e$ mit $e < f$, bilden also selbst eine endliche Teilmenge.

b) ist nun klar: Nach Definition kann jedes monomiale Ideal durch eine Menge M von Monomen erzeugt werden. Da jedes Monom aus M Vielfaches eines der endlich vielen minimalen Monome aus M ist, reichen diese zur Erzeugung aus.

■

Korollar: Jedes Ideal I in $k[X_1, \ldots, X_n]$ hat bezüglich jeder Monomordnung eine GRÖBNER-Basis.

Beweis: Wir betrachten die Menge $M = \{\mathrm{FM}\, f \mid f \in I \setminus \{0\}\}$ aller führender Monome von Polynomen aus I. Nach dem Lemma von DICKSON bilden die minimalen Monome aus M eine endliche Menge; diese sei $\{\mathrm{FM}\, g_1, \ldots, \mathrm{FM}\, g_r\}$. Da das Ideal $\mathrm{FM}\, I$ von M erzeugt wird, wird es auch von dieser Teilmenge der minimalen Elemente erzeugt, und damit ist $\{g_1, \ldots, g_r\}$ eine GRÖBNER-Basis bezüglich der gewählten Monomordnung.

■

In der linearen Algebra hat eine Basis eines Vektorraums die Eigenschaft, daß sich jeder Vektor eindeutig als eine skalare Linearkombination der Basisvektoren darstellen läßt. Eine eindeutige Darstellung können wir bei Erzeugendensystemen von Idealen natürlich nicht erwarten: Da Ideal $I = (X, Y)$ aus $k[X, Y]$ enthält beispielsweise das Polynom

$X^2 + XY + Y^2$, das wir unter anderem als $(X + Y) \cdot X + Y \cdot Y$ oder als $X \cdot X + (X + Y) \cdot Y$ schreiben können.

Bei der Definition einer GRÖBNER-Basis haben wir nicht einmal vorausgesetzt, daß diese überhaupt das Ideal I erzeugt; in der Definition wird nur verlangt, daß die führenden Monome der Basiselemente das monomiale Ideal erzeugen, das alle führenden Monome von Elementen aus I enthält. Eine GRÖBNER-Basis, die nicht das gleiche Ideal wie die Ausgangspolynome erzeugt, ist natürlich nutzlos für die Lösung nichtlinearer Gleichungssysteme, und zum Glück gilt

Satz: Ist $\{g_1, \ldots, g_r)$ eine GRÖBNER-Basis des Ideals I in einem Polynomring $k[X_1, \ldots, X_n]$, so wird $I = (g_1, \ldots, g_r)$ von den g_i erzeugt.

Beweis: Nach Definition einer GRÖBNER-Basis erzeugen die führenden Monome $\mathrm{FM}\, g_1, \ldots, \mathrm{FM}\, g_r$ das Ideal $\mathrm{FM}\, I$. Wir müssen zeigen, daß jedes Elemente $f \in I$ als Linearkombination (mit Koeffizienten aus dem Polynomring) der g_i geschrieben werden kann. Für $f = 0$ ist das klar, und ein $f \neq 0$ aus I hat einen führenden Term $\mathrm{FM}\, f$, der im monomialen Ideal $\mathrm{FM}\, I$ liegt, das von $\mathrm{FM}\, g_1, \ldots, \mathrm{FM}\, g_r$ erzeugt wird. Nach dem ersten Lemma der heutigen Vorlesung ist $\mathrm{FM}\, f$ daher ein Vielfaches eines der Monome $\mathrm{FM}\, g_i$; konkret sei $\mathrm{FM}\, f = u_1\, \mathrm{FM}\, g_{i_1}$ mit einem Monom u_1. Wegen der zweiten Eigenschaft aus der Definition einer Monomordnung ist dann auch $\mathrm{FM}\, f = \mathrm{FM}(u_1 g_{i_1})$. Wir können daher den führenden Term von f eliminieren, indem wir ein geeignetes Vielfaches $c_1 u_1 g_{i_1}$ subtrahieren und erhalten ein Polynom

$$f_1 = f - c_1 u_1 g_{i_1} \quad \text{mit} \quad f_1 = 0 \quad \text{oder} \quad \mathrm{FM}\, f_1 < \mathrm{FM}\, f\,.$$

Da f und g_{i_1} beide in I liegen, ist auch $f_1 \in I$. Falls f_1 verschwindet, liegt $f = c_1 u_1 g_{i_1}$ im von den g_i erzeugten Ideal; andernfalls ist $\mathrm{FM}\, f_1$ als Element von $\mathrm{FM}\, I$ Vielfaches eines führenden Monoms $\mathrm{FM}\, g_{i_2}$, etwa $\mathrm{FM}\, f_1 = u_2\, \mathrm{FM}\, g_{i_2}$. Wieder folgt, daß es ein $c_2 \in k$ gibt, so daß

$$f_2 = f_1 - c_2 u_2 g_{i_2} = f - c_1 u_1 g_{i_1} - c_2 u_2 g_{i_2}$$

mit $f_2 = 0$ oder $\mathrm{FM}\, f_2 < \mathrm{FM}\, f_1$.

Wenn f_2 verschwindet, haben wir f als Linearkombination der g_i dargestellt; andernfalls machen wir genauso weiter und konstruieren

sukzessive neue Polynome

$$f_j = f - c_1 u_1 g_{i_1} - \cdots - c_j u_j g_{i_j} \in I$$

mit $f_j = 0$ oder $\mathrm{FM}\, f_j < \mathrm{FM}_{j-1}$

Sobald ein f_j verschwindet, haben wir f als Linearkombination dargestellt. Falls kein f_j verschwindet, haben wir eine unendliche Folge von Monomen

$$\mathrm{FM}\, f > \mathrm{FM}\, f_1 > \mathrm{FM}\, f_2 > \cdots ,$$

im Widerspruch zur dritten Eigenschaft aus der Definition einer Monomordnung, wonach die Menge aller FM f_j ein kleinstes Element enthalten muß. Somit bricht die Konstruktion ab mit einem $f_j = 0$, und wir haben f als Linearkombination der g_i dargestellt.

■

Als Korollar erhalten wir einen berühmten Satz, den DAVID HILBERT (1862–1943) 1890 in den Mathematischen Annalen veröffentlichte:

Hilbertscher Basissatz: Jedes Ideal I im Polynomrings $k[X_1, \ldots, X_n]$ hat ein endliches Erzeugendensystem.

Beweis: Nach obigem Korollar hat jedes Ideal eine GRÖBNER-Basis, die nach Definition endlich ist. Nach dem gerade bewiesenen Satz ist diese ein Erzeugendensystem des Ideals.

■

HILBERT bewies diesen Satz natürlich nicht über GRÖBNER-Basen, allerdings war auch sein Beweis nicht konstruktiv. Da damals noch fast alle Beweise zumindest im Prinzip konstruktiv waren, veranlaßte dies PAUL GORDAN (1837–1912), einen der bedeutendsten Invariantentheoretiker dieser Zeit, zu der (bewundernden) Bemerkung, dieser Beweis sei nicht Mathematik, sondern Theologie.