WOLFGANG K. SEILER
Tel. 2515

B6, B4.18

11. Mai 2020

10. Übungsblatt Computeralgebra

Aufgabe 1: *(4 Punkte)*
Finden Sie eine Menge von Polynomen, die die getwistete kubische Kurve

$$C = \{(t, t^2, t^3) \mid t \in \mathbb{R}\} \subset \mathbb{R}^3$$

als gemeinsame Nullstellenmenge haben! Ist hier C die vollständige Nullstellenmenge?

Lösung: Aus der Parametrisierung $x = t, y = t^2, z = t^3$ kann t leicht eliminiert werden, denn da $x = t$ ist, kann t einfach überall durch x ersetzt werden. Wir erhalten die Kurve daher als Nullstellenmenge der beiden Polynome $Y - X^2$ und $Z - X^3$.
Nach der aus der Vorlesung bekannten allgemeinen Methode könnten wir auch nach einer GRÖBNER-Basis des von $X - T, Y - T^2$ und $Z - T^3$ erzeugten Ideals von $k[T, X, Y, Z]$ suchen bezüglich einer Eliminationsordnung für T. In der lexikographischen Ordnung bezüglich $T > Z > Y > X$ ist

$$S(-T + X, -T^2 + Y) = -TX + Y = X(X - T) + Y - X^2\,;$$

das S-Polynom kann also auf $Y - X^2$ reduziert werden, und genauso kann

$$S(-T + X, -T^3 + Z) = -T^2X + Z = (XT + X^2)(X - T) + Z - X^3$$

auf $Z - X^3$ reduziert werden. Die drei Polynome $X - T, Y - X^2$ und $Z - X^3$ erzeugen offensichtlich das gleiche Ideal wie $X - T, Y - T^2$ und $Z - T^3$, und sie bilden eine GRÖBNER-Basis, denn ihre führenden Monome T, Y und Z sind teilerfremd, so daß sich alle S-Polynome auf Null reduzieren lassen. Wenn wir uns auf die beiden Polynome beschränken, die kein T enthalten, bekommen wir das gleiche Ergebnis wie oben.
Die lexikographische Ordnung mit $T > X > Y > Z$ allerdings würde auf ein komplizierteres Ergebnis führen: Hier bestünde die reduzierte GRÖBNER-Basis aus den fünf Polynomen $Y^3 - Z^2, XY - Y^2, XY - Z, X^2 - Y$ und $T - X$, wobei die ersten vier das Eliminationsideal erzeugen.
In allen Fällen ist wegen $X = T$ klar, daß jedes Element der Nullstellenmenge in der Form (t, t^2, t^3) dargestellt werden kann.

Aufgabe 2: *(6 Punkte)*
Das Ideal I in $\mathbb{Q}[X, Y]$ werde erzeugt von $f = X^2 + 2Y^2 - 3$ und $g = X^2 + XY + Y^2 - 3$.

a) Berechnen Sie die Durchschnitte $I \cap k[X]$ und $I \cap k[Y]$!

Lösung: Das sind die Eliminationsideale bezüglich Y *bzw.* X. Beginnen wir mit der lexikographischen Ordnung mit $X > Y$. Beide Polynome haben den führenden Term X^2, so daß $h = S(f, g) = f - g = -XY + Y^2$ ist. Da X^2 keinen der beiden Terme teilt, kann dies nicht weiter reduziert werden, muß also zur Basis dazu.
In $S(f, h) = -XY^2 - 2Y^3 + 3Y$ ist der führende Term $-XY^2$ ein Vielfaches des führenden Terms $-XY$ von h; Subtraktion von Yh führt auf $-3Y^3 + 3Y$, so daß wir $p = Y^3 - Y$ zum Erzeugendensystem dazunehmen müssen.
Auch in $S(g, h) = -2XY^2 - 3Y^3 + 3Y$ können wir durch Subtraktion von 2Yh reduzieren; das Ergebnis ist wieder $-3Y^3 + 3Y$.

Im nächsten Schritt müssen wir schauen, ob f, g, h, p das BUCHBERGER-Kriterium erfüllen: $S(f,p)$ und $S(g,p)$ können auf Null reduziert werden, da die führenden Monome X^2 und Y^3 teilerfremd sind, und $S(h,p) = Y^4 - XY$ wird durch Subtraktion von h zu $Y^4 - Y^2 = Yp$, so daß auch dies auf Null reduziert werden kann. Damit bilden f, g, h, p eine GRÖBNER-Basis, und p als einziges Element ohne X erzeugt das Eliminationsideal $I \cap k[Y] = (Y^3 - Y)$.

Wenn wir die lexikographische Ordnung mit $Y > X$ verwenden, haben f und g beide das führende Monom Y^2; um Nenner zu vermeiden berechnen wir das Doppelte davon, also $2S(f,g) = f - 2g = -2XY - X^2 - 3$, was nicht weiter reduziert werden kann. (Im folgenden werde ich S-Polynome meist kommentarlos mit geeigneten Konstanten multiplizieren, wenn dies Brüche vermeidet.) Wir nehmen daher $h' = 2XY + X^2 + 3$ zum Erzeugendensystem dazu.

$S(f,h') = Xf - Yh' = -YX^2 + 3Y + X^3 - 3X$ wird durch Addition von $\frac{1}{2}Xh'$ zu $3Y + \frac{3}{2}X^3 - \frac{9}{2}X$, was nicht weiter reduziert werden kann. Wir müssen also im nächsten Schritt das Polynom $p' = 6Y + 3X^3 - 9X$ dazunehmen.

$S(g,h') = Xg - Yh' = YX^2 + 3Y + 2X^3 - 6X$ wird durch Subtraktion von $\frac{1}{2}Xh'$ reduziert zu $3Y + \frac{3}{2}X^3 - \frac{9}{2}X$, was wir von $S(f,h')$ kennen, so daß wir auch hier auf p' kommen.

$S(f,p') = -3X^3Y + 9XY + 3X^3 - 9$ wird durch Addition von $\frac{3}{2}X^2h'$ und anschließende Subtraktion von $\frac{9}{2}h'$ zu $\frac{3}{2}X^4 - 6X^2 + \frac{9}{2}$, was nicht weiter reduziert werden kann. Wir müssen also im nächsten Schritt noch dieses Polynom mit betrachten, am besten, nachdem wir es mit $\frac{2}{3}$ multipliziert haben zu $q = X^4 - 4X^2 + 3$.

Auch $S(g,p') = -3X^3Y + 15XY + 6X^2 - 18$ wird zunächst durch Addition von $\frac{3}{2}X^2h'$ reduziert, danach durch Subtraktion von $\frac{15}{2}h'$ auf $\frac{3}{2}X^4 - 6X^2 + \frac{9}{2} = \frac{3}{2}q$

$S(h',p')$ führt direkt auf q.

Die vier Polynome f, g, h', p', q bilden eine GRÖBNER-Basis, denn wir müssen nur noch zeigen, daß sich die S-Polynome mit q auf Null reduzieren lassen, und das ist klar für $S(f,q)$ und $S((g,q)$, deren führendes Monom Y^2 teilerfremd zu $\mathrm{FM}\, q = X^4$ ist.

$S(h',q) = 8XY^2 - 6Y + X^5 - 3X^3$ wird durch Subtraktion von $4Xh'$ zu $-6Y + X^5 - 7X^3 + 12X$; Addition von p' macht daraus $X^5 - 4X^3 + 3X = 3q$, so daß dies auf Null reduziert werden kann.

$S(p',q) = 24XY^2 - 18Y - 9X^5 + 3X^7$ wird zunächst durch Subtraktion von $12Xh$ zu $-18Y + 3X^7 - 9X^5 - 12X^3 + 36X$; Addition von $3p'$ macht daraus $3X^7 - 9X^5 - 3X^3 + 9X$. Polynomdivision zeigt, daß dies gleich $3X(X^2+1)q$ ist, so daß $S(p',q)$ auf Null reduziert werden kann.

Da q das einzige Polynom ohne Y ist, erzeugt es das Eliminationsideal

$$I \cap k[X] = (X^4 - 4X^2 + 3)\,.$$

b) Bestimmen Sie alle gemeinsamen Nullstellen von f und g in $\mathbb{R}^2$!
GRÖBNER-*Basen können Sie von einen Computeralgebrasystem berechnen lassen.*

Lösung: Da $Y^3 - Y = Y(Y^2-1)$ im Ideal liegt, kann y nur die Werte Null und ± 1 annehmen. Setzt man Y auf drei, werden f und g zu $X^2 - 3$; also sind $(\pm\sqrt{3}, 0)$ die Lösungen mit $y = 0$.

$f(X,1) = X^2 - 1$ hat die Nullstellen ± 1, aber $g(X,1) = X^2 + X - 2$ verschwindet zwar an der Stelle $+1$, nicht aber bei -1. Also ist $(1,1)$ die einzige Lösung mit $y = 1$.

Auch $f(X,-1) = X^2 - 1$, aber $g(X,-1) = X^2 - X - 2$ verschwindet nur bei -1, nicht bei $+1$. Die vierte und letzte Lösung ist also $(-1,-1)$.

Aufgabe 3: *(7 Punkte)*

Finden Sie Ideale I in $\mathbb{Q}[X,Y,Z]$, für die $V(I)$ gleich der angegebenen Teilmenge von $\mathbb{Q}^3$ ist:

a) $\{-1,0,1\} \times \{3,5\} \times \{1,2,3\}$

Lösung: Da wir ein Produkt dreier Teilmengen von $\mathbb{Q}$ haben, können wir einfach für jede der drei Teilmengen ein Polynom betrachten, das genau diese Menge als Nullstellenmenge hat:
Mit den Polynomen $f = (X+1)X(X-1) = X^3 - X$, $g = (Y-3)(Y-5) = Y^2 - 8Y + 15$ und $h = (Z-1)(Z-2)(Z-3) = Z^3 - 6z^2 + 11z - 6$ ist $V(f) = \{-1,0,1\}$, $V(g) = \{3,5\}$ und $V(h) = \{1,2,3\}$, also $V(f,g,h) = \{-1,0,1\} \times \{3,5\} \times \{1,2,3\}$.

b) $\{(-2,-1,0),\ (-1,0,1),\ (0,1,2),\ (1,2,3),\ (2,3,4)\}$

Lösung: Alle Punkte sind von der Form $(x, x+1, x+2)$, wobei x die ganzzahligen Werte zwischen -2 und 2 annimmt.

$$f = (X+2)(X+1)X(X-1)(X-2) = (X^2-4)(X^2-1)X = X^5 - 5X^3 + 4X,$$

also ist die Menge Nullstellenmenge des Ideals $(X^5 - 5X^3 + 4X, Y - X - 1, Z - X - 2)$.

c) $\{(3,1,4),\ (1,5,9),\ (2,6,5),\ (3,5,8)\}$

Etwa notwendige GRÖBNER-Basen sollten mit einem Computeralgebrasystem berechnet werden; mit alternativen Ansätzen läßt sich zumindest manchmal allerdings viel Arbeit sparen.

Lösung: Hier sind die Koordinaten durch die Dezimalstellen von π gegeben, was zu keiner Vereinfachung des Problems führt. Daher bleibt nur die allgemeine Methode: Wir gehen in den Polynomring $\mathbb{Q}[T_1, T_2, T_3, T_4, X, Y, Z]$ und betrachten dort die Polynome

$$T_1(X-3), T_1(Y-1), T_1(Z-4), T_2(X-1), T_2(Y-5), T_2(Z-9), T_3(X-2), T_3(Y-6), T_3(Z-5),$$
$$T_4(X-3), T_4(Y-5), T_4(Z-8) \quad \text{und} \quad T_1 + T_2 + T_3 + T_4 - 1\,.$$

Die (bis auf führende Koeffizienten) reduzierte GRÖBNER-Basis bezüglich der lexikographischen Ordnung mit $T_1 > T_2 > T_3 > T_4 > X > Y > Z$ besteht aus sieben Polynomen, von denen vier jeweils genau ein T_i enthalten. Die restlichen vier Polynome

$$Z^4 - 26Z^3 + 245Z^2 - 988Z + 1440\,,$$
$$60Y - 17Z^3 + 369Z^2 - 2584Z + 5460\,,$$
$$60X + 11Z^3 - 207Z^2 + 1252Z - 2580$$

erzeugen das gesuchte Ideal.

Aufgabe 4: *(3 Punkte)*

a) Finden Sie alle Nullstellen des Polynoms $f = X^2Y + 2XY^2 \in \mathbb{F}_3[X,Y]$ in $\mathbb{F}_3^2$!

Lösung: $f = XY(X+2Y) = XY(X-Y)$; Nullstellen sind also alle Paare (x,y) mit $x = 0$ oder $y = 0$ oder $x = y$, d.h. $V(f) = \{(0,0),(0,1),(0,2),(1,0),(2,0),(1,1),(2,2)\}$.

b) Nun sei k ein unendlicher Körper, der $\mathbb{F}_3$ enthält. Zeigen Sie, daß $V_k(f)$ unendlich ist, und geben Sie diese Menge über Parameterdarstellung explizit an!

Lösung: $V_K(f) = \{(0,y) \mid y \in k\} \cup \{(x,0) \mid x \in k\} \cup \{(x,x) \mid x \in k\}$.

c) Nun sei $g = X^2 + 2Y^2$ und K sei ein algebraisch abgeschlossener Erweiterungskörper von $\mathbb{F}_3$. Bestimmen Sie $V_K(f,g)$!
(GRÖBER-Basen werden für diese Aufgabe nicht benötigt.)

Lösung: Für einen Punkt $(0,y)$ mit $y \in K$ ist $g(0,y) = 2y^2 = 0$ genau dann, wenn $y = 0$ ist; entsprechend verschwindet auch $g(x,0) = x^2$ nur für $x = 0$. $g(x,x) = x^2 + 2x^2 = x^2 - x^2$ verschwindet für alle $x \in K$. Somit ist $V_K(f,g) = \{(x,x) | x \in K\}$.