Wolfgang K. Seiler
Tel. 2515

B6, B4.18

18. Mai 2020

11. Übungsblatt Computeralgebra

Aufgabe 1: *(6 Punkte)*
Finden Sie für die folgenden Ideale I in $\mathbb{Q}[X,Y]$ sowohl die Nullstellenmenge als auch Monome aus $\mathbb{Q}[X,Y]$, deren Restklassen eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}[X,Y]/I$ bilden:

a) $I = (X, Y)$

Lösung: Da sowohl die x- als auch die y-Koordinate jedes Punktes aus $V(I)$ verschwinden müssen, ist $V_K(I) = \{(0,0)\}$ für jeden Körper K, der $\mathbb{Q}$ enthält. Ein Polynom $f \in \mathbb{Q}[X,Y]$ verschwindet genau dann im Punkt $(0,0)$, wenn es keinen konstanten Term hat, und das ist genau dann der Fall, wenn jedes seiner Monome durch X oder durch Y teilbar ist, d.h. wenn das Polynom in I liegt. Somit ist I der Kern der Abbildung

$$\begin{cases} \mathbb{Q}[X,Y] \to Q \\ \qquad f \mapsto f(0,0) \end{cases},$$

so daß $\mathbb{Q}[X,Y]/I \cong \mathbb{Q}$ nach dem Homomorphiesatz eindimensional ist mit der Restklasse des konstanten Monoms 1 als Basis.

b) $I = (X^3 - X, Y^3 - Y)$

Lösung: $X^3 - X = X(X-1)(X+1)$ hat $0, 1$ und -1 als Nullstellen; für jeden Körper K, der $\mathbb{Q}$ enthält, ist also $V_K(I) = \{-1,0,1\} \times \{-1,0,1\}$.
Modulo I ist X^3 äquivalent zu X. Allgemein ist für jedes $a \in \mathbb{N}_0$

$$X^{a+3} - X^{a+1} = X^a(X^3 - X) \in I,$$

und daraus folgt sukzessive, daß jede Potenz X^a mit $a \geq 3$ für ungerades a äquivalent zu X ist und für gerades a zu X^2. Entsprechend ist auch Y^b für $b \geq 3$ im Falle eines ungeraden Exponenten äquivalent zu Y und für einen geraden zu Y^2. Somit ist jedes Monom X^aY^b äquivalent zu einem Monom X^cY^d mit $c, d \in \{0,1,2\}$. Diese neun Monome erzeugen also $\mathbb{Q}[X,Y]/I$. Wie wir wissen, ist die Dimension dieses $\mathbb{Q}$-Vektorraums größer oder gleich der Elementanzahl von $V_K(I)$, also mindestens neun. Somit müssen diese neun Erzeugenden linear unabhängig sein und bilden daher eine Basis.

Aufgabe 2: *(8 Punkte)*

a) Zeigen Sie, daß die angegeben Erzeugendensysteme der beiden Ideale aus der vorigen Aufgabe bezüglich jeder beliebigen Mononmordnung GRÖBNER-Basen sind!

Lösung: Im ersten Fall ist $I = (X, Y)$ ein monomiales Ideal und somit ist FM $I = I = (X, Y)$. Da beide Erzeugenden Monome sind, sind sie natürlich unabhängig von der Monomordnung ihre eigenen führenden Monome, so daß direkt aus der Definition folgt, daß sie eine GRÖBNER-Basis bilden.
Für $I = (X^3 - X, Y^3 - Y)$ sind die führenden Monome der Erzeugenden bezüglich jeder Monomordnung X^3 und Y^3, da ein echter Teiler eines Monoms bezüglich jeder Monomordnung kleiner ist als dieses. Da die beiden führenden Monome teilerfremd sind, läßt sich $S(X^3 - X, Y^3 - Y)$ auf Null reduzieren; die beiden Erzeugenden bilden also nach dem Kriterium von BUCHBERGER eine GRÖBNER-Basis.

b) Untersuchen Sie für beide Ideale, ob eine der Variablen separierend bezüglich $V_{\mathbb{C}}(I)$ ist!

Lösung: Für $I = (X, Y)$ ist $V_{\mathbb{C}}(I) = \{(0, 0)\}$ einelementig, so daß beide Variablen trivialerweise separierend sind.
Für $I = (X^3 - X, Y^3 - Y)$ ist $V_{\mathbb{C}}(I) = \{-1, 0, 1\} \times \{-1, 0, 1\}$, so daß keine der beiden Variablen separierend ist: Jede nimmt für jeweils drei der neun Nullstellen den gleichen Wert an.

c) Bestimmen Sie, falls dies nicht der Fall sein sollte, eine separierende Linearform in X und Y, und ersetzen Sie Y durch eine neue Variable Z derart, daß das Ideal eine GRÖBNER-Basis gemäß dem *Shape*-Lemma hat!

Lösung: Die Linearform muß so gewählt werden, daß ihre Nullstellenmenge keine Gerade definiert, die parallel ist zur Verbindungsgerade zweier Punkte aus $V_{\mathbb{C}}(I)$i ist. Waagrechte und senkrechte Geraden sowie solche mit Steigung ± 1 oder ± 2 sind daher ausgeschlossen. Eine offensichtlich separierende Linearform ist $3X + Y$; sie nimmt auf $V_K(I)$ alle ganzzahligen Werte zwischen -4 und 4 an. Ersetzen wir Y durch die neue Variable $Z = 3X + Y$, bleibt $f = X^3 - X$ unverändert; das Polynom $Y^3 - Y$ wird in den neuen Variablen zu $g = (Z - 3X)^3 - (Z - 3X) = Z^3 - 9XZ^2 + 27X^2Z - 27X^3 - Z + 3X$. Da $k[X, Y]/I$ nach Aufgabe eins die Dimension neun hat und $V_K(I)$ aus neun Punkten besteht, ist I ein Radikalideal, und damit natürlich auch das von f und g erzeugte Ideal in $k[X, Z]$. Da Z separierend auf der Nullstellenmenge ist, hat dieses Ideal bezüglich der lexikographischen Ordnung mit $X > Z$ eine GRÖBNER-Basis gemäß dem *Shape*-Lemma.

d) Bestimmen Sie diese Basis!

Lösung: Das Polynom nur in Z ist natürlich

$$p = \prod_{i=-4}^{4} (Z - i) = Z \prod_{i=1}^{4} (Z^2 - i^2) = Z^9 - 30Z + 273Z^5 - 820Z^3 + 576Z\,.$$

Das zweite Polynom aus der GRÖBNER-Basis ist $q = X - h$, wobei $h \in \mathbb{Q}[Z]$ das Interpolationspolynom vom Grad höchstens acht ist, das für $z = -4, \ldots, 4$ jeweils den Wert $x \in \{-1, 0, 1\}$ annimmt, für den es ein $y \in \{-1, 0, 1\}$ gibt, so daß $3x + y = z$ ist. $h(z)$ ist damit die am nächsten bei $z/3$ liegende ganze Zahl. Dies führt auf folgende Wertetabelle:

z	-4	-3	-2	-1	0	1	2	3	4
x	-1	-1	-1	0	0	0	1	1	1

Nach NEWTON (oder mit einem Computeralgebrasystem) ergibt sich dieses zu

$$h = \frac{1}{1680}\left(3Z^7 - 84Z^5 + 637Z^3 - 556Z\right)\,.$$

Die GRÖBNER-Basis gemäß *Shape*-Lemma ist also $\{p, X - h\}$, was hier nicht gerade einfacher ist als die Ausgangsbasis und die Nullstellenmenge auch nicht besser beschreibt.

Aufgabe 3: *(6 Punkte)*
Sei $f = 9X^2 + 16Y^2 - 144$, $g = 25X^2 + 4(Y+1)^2 - 100$ und I das von f und g erzeugte Ideal in $\mathbb{Q}[X, Y]$.

a) Lassen Sie ein Computeralgebrasystem GRÖBNER-Basen von I bestimmen bezüglich der lexikographischen Ordnungen mit $X > Y$ *bzw.* $Y > X$ sowie auch der entsprechenden graduiert lexikographischen Ordnungen! In welchen Fällen hat diese Basis bezüglich einer der beiden Variablen die Form aus dem Shape-Lemma?

Lösung: Für die lexikographische Ordnung mit $X > Y$ liefert Maple die Basis bestehend aus

$$91Y^2 - 18Y - 684 \quad \text{und} \quad 91X^2 + 32Y - 240\,,$$

die wegen des quadratischen Terms im zweiten Polynom nicht die gewünschte. Form hat. Für die mit $Y > X$ liefert es

$$8281X^4 - 43104X^2 + 48384 \quad \text{und} \quad 32Y + 91X^2 - 240\,,$$

was (bis auf die führenden Koeffizienten, durch die man natürlich jeweils dividieren kann) der Form gemäß *Shape*-Lemma entspricht.
Für die graduiert lexikographische Ordnung mit $X > Y$ und für die mit $Y > X$ erhalten wir

$$91X^2 + 32Y - 240 \quad \text{und} \quad 91Y^2 - 18Y - 684\,,$$

was nicht der Form gemäß *Shape*-Lemma entspricht.

b) Bestimmen Sie mit Hilfe einer der berechneten GRÖBNER-Basen die Nullstellenmenge $V_{\mathbb{C}}(I)$!

Lösung: Am einfachsten geht das wohl mit der GRÖBNER-Basis zur lexikographischen Ordnung mit $X > Y$. Das quadratische Polynom in Y hat die Nullstellen

$$\frac{9}{91} \pm \frac{15}{91}\sqrt{277}\,.$$

Wegen des zweiten Polynoms bestimmt y das Quadrat von x eindeutig als

$$x^2 = -\frac{32y - 240}{91}\,.$$

Dies führt auf die Lösungen

$$\left(\pm\sqrt{\frac{21552}{8281} - \frac{480}{8281}\sqrt{277}},\ \frac{9}{91} + \frac{15}{91}\sqrt{277}\right)$$

und

$$\left(\pm\sqrt{\frac{21552}{8281} + \frac{480}{8281}\sqrt{277}},\ \frac{9}{91} - \frac{15}{91}\sqrt{277}\right)\,,$$

die man noch ein bißchen einfacher schreiben kann, wenn man beachtet, daß $8281 = 91^2$ ist und 21552 und 480 beide durch 4^2 teilbar sind.

c) Interpretieren Sie die Nullstellenmenge geometrisch!

Lösung: Sowohl $V(f)$ als auch $V(g)$ sind Ellipsen, deren Halbachsen parallel zu den Koordinatenachsen liegen. Mittelpunkt der ersten Ellipse ist $(0, 0)$, Mittelpunkt der zweiten ist $(0, -1)$. Da beide symmetrisch zur y-Achse sind, haben je zwei der Schnittpunkte die gleiche y-Koordinate, so daß Y nicht separierend ist und die GRÖBNER-Basis bezüglich der lexikographischen Ordnung mit $X > Y$ keine Form gemäß *Shape*-Lemma haben kann.