Wolfgang K. Seiler A5, C201
Tel. 2515

18. Dezember 2017

Modulklausur Computeralgebra

Aufgabe 1: *(10 Punkte)*

a) Welche Bedingungen muß eine Teilmenge $I \subseteq R$ eines Rings erfüllen, um ein Ideal zu sein?

Lösung: I darf nicht leer sein und muß zu je zwei Elementen auch deren Summe enthalten. Außerdem muß das Produkt eines jeden Elements mit einem beliebigen Ringelement in I liegen.

b) Welche der folgenden Mengen sind Ideale in $\mathbb{R}[X]$? (Bei den angegebenen Polynomen soll stets d beliebig und $a_d \neq 0$ sein.)

$$M_1 = \mathbb{Z}, \quad M_2 = \mathbb{Q}, \quad M_3 = \mathbb{R}, \quad M_4 = \mathbb{C}, \quad M_5 = \left\{ f \in \mathbb{R}[X] \;\middle|\; f(1) = 0 \right\}$$

$$M_6 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{R}[X] \;\middle|\; \sum_{i=0}^{d} a_i = 0 \right\}, \quad M_7 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{R}[X] \;\middle|\; \sum_{i=0}^{d} a_i = 1 \right\}$$

$$M_8 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{R}[X] \;\middle|\; \sum_{i=0}^{d} (-1)^i a_i = 0 \right\}, \quad M_9 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{R}[X] \;\middle|\; a_0 = 0 \right\}$$

c) Geben Sie in allen Fällen, in denen M_i ein Ideal ist, ein möglichst einfaches Erzeugendensystem von M_i an!

Lösung: M_1 bis M_3 enthalten die Eins; wären Sie Ideale müßten sie ganz $\mathbb{R}[X]$ sein, was nicht der Fall ist. M_4 liegt nicht einmal in $\mathbb{R}[X]$, kann also auch kein Ideal sein.

M_5 ist ein Ideal, denn die Summe zweier Polynome, die an der Stelle eins verschwinden, verschwindet auch dort, genauso wie das Produkt eines solchen Polynoms mit einem beliebigen Polynom. Da die Polynome mit Nullstelle eins genau die durch $X - 1$ teilbaren sind, ist M_5 das Hauptideal $(X-1)$. Offensichtlich ist $M_6 = M_5$, also dasselbe Hauptideal.

M_7 besteht aus allen Polynomen, die am der Stelle eins den Wert eins annehmen; die Summe zweier solcher Polynome nimmt dort den Wert zwei an, liegt also nicht in M_7, das somit kein Ideal ist.

M_8 läßt sich einfacher beschreiben als Menge alle $f \in \mathbb{R}[X]$ mit $f(-1) = 0$, ist also das Hauptideal $(X + 1)$. Entsprechend ist $M_9 = \left\{ f \in \mathbb{R}[X] \;\middle|\; f(0) = 0 \right\} = (X)$.

Aufgabe 2: *(6 Punkte)*

a) Welche Bedingungen muß eine Monomordnung auf $k[X_1, \dots, X_n]$ erfüllen?

Lösung: 1.) Es ist eine Totalordnung, d.h. für je zwei Monome X^d und X^e gilt genau eine der drei Aussagen $X^d < X^e$, $X^d = X^e$ und $X^d > X^e$.
2.) Ist $X^d > X^e$, so ist $X^{d+a} > X^{e+a}$ für alle Monome X^a.
3.) Jede nichtleere Menge von Monomen enthält ein kleinstes Element *(Wohlordnung)*.

b) Zeigen Sie: Ist $>$ eine Monomordnung auf $k[X_1, \dots X_n]$, und ist $X_i > X_j$, so ist auch $X_i^n > X_j^n$ für alle $n \in \mathbb{N}$.

Lösung: Beweis durch vollständige Induktion. Der Fall $n = 1$ ist die Voraussetzung, also erfüllt.
Für $n > 1$ nehmen wir an, daß $X_i^{n-1} > X_j^{n-1}$ bereits gezeigt sei; nach der obigen Eigenschaft 2.) ist dann $X_i^n = X_i^{n-1}X_i > X_i^{n-1}X_j > X_j^{n-1}X_j = X_j^n$.

Aufgabe 3: (*11 Punkte*)

a) Beschreiben Sie die Nullstellenmengen $V_\mathbb{R}(f)$ und $V_\mathbb{R}(g)$ der beiden Polynome

$$f = X^2 + Y^2 - 6X - 8 \quad \text{und} \quad X^2 + Y^2 - 6Y - 8$$

geometrisch!

Lösung: $f = (X-3)^2 + Y^2 - 17$ und $g = X^2 + (Y-3)^2 - 17$; somit sind $V_\mathbb{R}(f)$ und $V_\mathbb{R}(g)$ Kreise mit Radius $\sqrt{17}$ um die Punkte $(3, 0)$ *bzw.* $(0, 3)$.

b) Finden Sie Ideale I, J in $\mathbb{Q}[X, Y]$, so daß $V_\mathbb{C}(I) = V_\mathbb{C}(f) \cap V_\mathbb{C}(g)$ und $V_\mathbb{C}(J) = V_\mathbb{C}(f) \cup V_\mathbb{C}(g)$ ist, und geben Sie jeweils Erzeugendensysteme dafür an!

Lösung: Da das Polynom fg genau in den Punkten verschwindet, in denen f oder g verschwindet, können wir für J das Hauptideal (fg) nehmen; für I nehmen wir natürlich das von f und g erzeugte Ideal (f, g).

c) Finden Sie ein Hauptideal von $\mathbb{R}[X, Y]$, dessen Nullstellenmenge in $\mathbb{R}^2$ gleich $V_\mathbb{R}(f) \cap V_\mathbb{R}(g)$ ist!

Lösung: Die Summe zweier Quadrate reeller Zahlen verschwindet genau dann, wenn beide Zahlen verschwinden; somit können wir das von $f^2 + g^2$ erzeugte Hauptideal nehmen.

d) Finden Sie eine Gerade in $\mathbb{R}^2$, die durch alle gemeinsamen Nullstellen von f und g geht, sowie auch ein Polynom $h \in \mathbb{Q}[Y]$ aus I mit möglichst kleinem Grad!

Lösung: Die Schnittpunkte der beiden Kreise liegen auf der Mittelsenkrechten der Verbindungsstrecke der beiden Mittelpunkte; das ist hier aus Symmetriegründen gerade die Winkelhalbierende $y = x$. Das Polynom $X - Y$ liegt in $I = (f, g)$, denn $f - g = -6X + 6Y$, d.h. $X - Y = (g - f)/6$. Da $g = f + 6(X - Y)$ ist, erzeugen f und g das gleiche Ideal wie f und $X - Y$.
Einsetzen von $Y = X$ in f führt auf das Polynom $2Y^2 - 6Y - 8$, das auf ganz $V_\mathbb{C}(I)$ verschwinden muß, da $I = (f, X - Y)$. Da alle Koeffizienten gerade sind, bietet sich an, stattdessen $h = Y^2 - 3Y - 4$ zu betrachten.

e) Zeigen Sie, daß das Polynom h zusammen mit der Gleichung der gefundenen Geraden eine reduzierte GRÖBNER-Basis von I bezüglich der lexikographischen Ordnung bildet!

Lösung: Zunächst sind h und $X - Y$ ein Erzeugendensystem, denn $I = (f, g) = (f, X - Y)$, und das ist gleich $(h, X - Y)$, denn

$$f - 2h = X^2 - Y^2 - 6X + 6Y = (X + Y)(X - Y) - 6(X - Y) = (X + Y - 6)(X - Y) ,$$

so daß sich f und $2h$ um ein Vielfaches von $X - Y$ unterscheiden.
Zum Nachweis, daß wir eine GRÖBNER-Basis haben, berechnen und reduzieren wir das S-Polynom

$$S(h, X - Y) = Xh - Y^2(X - Y) = -3XY - 4X + Y^3 .$$

Der führende Term $-3XY$ ist nicht durch X^2, aber durch X teilbar; Addition von $3Y(X-Y)$ führt auf $-4X+Y^3-3Y^2$. Der neue führende Term ist wieder durch X teilbar; Addition von $4(X-Y)$ führt auf Y^3-3Y^2-4Y. Jetzt ist der führende Term Y^3; Subtraktion von Yh reduziert den verbliebenen Ausdruck auf Null.

f) Analog gibt es ein Polynom $h^* \in \mathbb{Q}[X]$, das zusammen mit der Geradengleichung ein Erzeugendensystem von I bildet. Finden Sie dieses!

Lösung: Einsetzen von $X=Y$ in f führt auf $2X^2-6X-8$, wir können also $h^*=X^2-3X-4$ nehmen.

g) Geben Sie $V_{\mathbb{C}}(I)$ explizit an!

Lösung: Die Nullstellen von $h=Y^2-3Y-4$ haben Summe drei und Produkt -4, sind also vier und minus eins. Somit besteht $V_{\mathbb{C}}(I)$ aus den beiden Punkten $(-1,-1)$ und $(4,4)$.

h) Bilden h und h^* bezüglich irgendeiner Monomordnung eine GRÖBNER-Basis von I?

Lösung: *Nein,* denn sie bilden nicht einmal ein Erzeugendensystem: Das von ihnen erzeugte Ideal hat die vier Nullstellen $(-1,-1)$, $(-1,4)$, $(4,-1)$ und $(4,4)$, ist also kleiner als I und enthält insbesondere nicht das Element $X-Y$.

Aufgabe 4: *(11 Punkte)*

a) Berechnen Sie eine GRÖBNER-Basis des von

$$f = X^2+2XY+Y^2 \quad \text{und} \quad g = Y^2+2XY+X$$

erzeugten Ideals I von $\mathbb{Q}[X,Y]$ bezüglich der graduiert lexikographischen Ordnung!

Lösung: Die führenden Terme von f und g sind X^2 und $2XY$; daher ist

$$2S(f,g) = 2Yf - Xg = 3XY^2 + 2Y^3 - X^2 .$$

Dieses Polynom muß modulo f und g reduziert werden.
Sein führender Term $3XY^2$ ist durch XY teilbar; subtrahieren wir vom Doppelten $3Yg$, erhalten wir Y^3-2X^2-3XY. Der neue führende Term Y^3 ist weder durch den führenden Term von f noch den von g teilbar, geht also in den Rest. Neuer führender Term ist $-2X^2$, ein Vielfaches von X^2. Addition von $2f$ führt auf $XY+2Y^2$ mit führendem Term XY. Das Doppelte minus g ist $3Y^2-X$, wobei kein Term mehr durch X^2 oder XY teilbar ist. Ein Vielfaches des Rests ist somit $h=2Y^3+3Y^2-X$. Dieses Polynom muß zur Basis hinzugenommen werden.

$$2S(f,h) = 2Y^3f - X^2h = 4Y^6+6Y^5-2XY^3-X^4-2X^3Y-X^2Y^2$$

hat Y^6 als führendes Monom; bei der Reduktion modulo f,g,h subtrahieren wir daher als erstes $2Y^3h$ und erhalten $-X^4-2X^3Y-X^2Y=-X^2f$. Somit läßt sich das S-Polynom auf Null reduzieren.
$S(g,h)=Y^2g-Xh=Y^4-2XY^2+X^2$ hat führenden Term Y^4; Multiplikation mit zwei und Subtraktion von Yh macht daraus $-4XY^2+2X^2-3Y^3+XY$. Der führende Term $-4XY^2$ ist durch XY teilbar; Addition von $2g$ führt auf $2X^2-Y^3+3XY$, was nach Subtraktion von $2f$ zu $-Y^3-XY-2Y^2$ wird. Multiplikation mit zwei und Addition von h macht daraus $-2XY-Y^2-X=-g$. Somit lassen sich beide S-Polynome auf Null reduzieren und $\{f,g,h\}$ ist nach dem Kriterium von BUCHBERGER eine GRÖBNER-Basis.

b) Ist die berechnete GRÖBNER-Basis reduziert? Ersetzen Sie sie gegebenenfalls durch eine reduzierte. Falls Sie keine Brüche als Koeffizienten wollen, können Sie dabei die Bedingung, daß alle führenden Koeffizienten eins sein sollen, ignorieren.

Lösung: Der führende Term $2XY$ von g kommt auch in f vor, also müssen wir f ersetzen durch $f - g = X^2 - X$. Weitere Reduktionen sind nicht möglich, die reduzierte GRÖBNER-Basis besteht also aus $X^2 - X, g$ und h.

b) Hat die gefundene reduzierte Basis für irgendeine Anordnung der Variablen die Form gemäß Shape-Lemma?

Lösung: Nein; sie enthält zwar ein Polynom nur in X, aber keines der Form Y plus Polynom in X.

c) Bestimmen Sie $V_{\mathbb{C}}(I)$ und die Vielfachheiten aller Nullstellen!

Lösung: $X^2 - X$ hat die beiden Nullstellen $x = 0$ und $x = 1$. Setzen wir $x = 0$ in g ein, erhalten wie die Bedingung $Y^2 = 0$, so daß auch $y = 0$ sein muß. Auch $h(0, Y) = 2Y^3 - 3Y^2$ verschwindet im Nullpunkt, so daß $(0, 0)$ eine Lösung ist.

$$g(1, Y) = Y^2 + 2Y + 1 = (Y + 1)^2 \quad \text{und} \quad h(1, Y) = 2Y^3 + 3Y^2 - 1$$

verschwinden beide bei $y = -1$. Der Restklassenring hat die Standardmonome $1, X, Y$ und Y^2 als Basis und ist damit vierdimensional; die Summe der Vielfachheiten der beiden Nullstellen muß also vier sein. Offensichtlich ist $(0, 0)$ mindestens eine doppelte Nullstelle, denn sowohl $g(0, Y)$ als auch $h(0, Y)$ sind durch Y^2 teilbar. $g(1, Y) = (Y + 1)^2$, und $h(1, Y)$ ist durch $(Y + 1)^2$ teilbar mit Quotient $2Y - 1$. Somit sind sowohl $(0, 0)$ als auch $(1, -1)$ doppelte Nullstellen.

d) Finden Sie eine Basis von $\sqrt{I}$ in einer Form gemäß dem Shape-Lemma!

Lösung: Da $f = (X + Y)^2$ in I liegt, muß $X + Y$ im Radikal liegen. Da die Nullstellen y-Koordinaten 0 und -1 haben, muß auch $Y^2 + Y$ in $\sqrt{I}$ liegen. Beide zusammen bilden wegen der Shape-Lemma-Form bezüglich der lexikographischen Ordnung eine GRÖBNER-Basis des von ihnen erzeugten Ideals $J \subseteq \sqrt{I}$. Die Standardmonome dazu sind 1 und Y, also ist der Restklassenring zweidimensional. Da $V_{\mathbb{C}}(I) = V_{\mathbb{C}}(\sqrt{I})$ ist, kann der Restklassenring modulo $\sqrt{I}$ nicht kleiner sein, also ist $\sqrt{I} = J = (X + Y, Y^2 + Y)$.

Aufgabe 5: *(8 Punkte)*

a) Das Ideal I in $\mathbb{Q}[X, Y]$ werde erzeugt von den beiden Polynomen $f = X - Y - Y^2$ und $g = X - Y^2 - Y^3$. Finden Sie ein Polynom aus $\mathbb{Q}[Y]$ in diesem Ideal, das zusammen mit einem der beiden Polynome f oder g ein Erzeugendensystem von I in der Form gemäß dem Shape-Lemma bildet!

Lösung: $h = f - g = Y^3 - Y$ liegt in $\mathbb{Q}[Y]$, und natürlich ist $(f, g) = (f, h) = (g, h)$. Da h den Grad drei hat, bildet es nur zusammen mit f eine Basis gemäß Shape-Lemma.

b) Bezüglich welcher Monomordnung ist dieses Erzeugendensystem sicher eine GRÖBNER-Basis?

Lösung: Wie in der Vorlesung gezeigt, ist es eine GRÖBNER-Basis bezüglich der lexikographischen Ordnung mit $X > Y$.

c) Bestimmen Sie $V_{\mathbb{C}}(I)$!

Lösung: h hat die drei Nullstellen $-1, 0, 1$. Da auch f verschwinden muß, ist $x = y + y^2$ für jedes $(x, y) \in V_{\mathbb{C}}(I)$. Wir haben somit die drei Lösungen $(0, -1)$, $(0, 0)$ und $(2, 1)$, *d)* Welche Multiplizitäten haben die einzelnen Lösungen?

Lösung: Da f und h eine GRÖBNER-Basis bilden, sind die Standardmonome $1, Y, Y^2$ dazu eine Vektorraumbasis des Restklassenrings. Somit ist die Summe aller Vielfachheiten gleich drei, d.h. alle Nullstellen sind einfach.

Aufgabe 6: *(6 Punkte)*

a) Welche Nullstellen hat das Polynom $f = X^4 - 2X^3 - 4X^2 + 10X - 5$, und welche Vielfachheiten haben sie?
Hinweis: Bestimmen Sie für jede gefundene Nullstelle gleich deren Vielfachheit!

Lösung: Das Produkt aller Nullstellen ist nach VIÈTE gleich minus fünf (vier ist gerade), und die Summe ist zwei. $f(1) = 1 - 2 - 4 + 10 - 5 = 0$, also ist eins eine Nullstelle. $f' = 4X^3 - 6X^2 - 8X + 10$ verschwindet ebenfalls dort, $f'' = 12X^2 - 12X - 8$ aber nicht. Also ist eins eine doppelte Nullstelle. Das Produkt der restlichen beiden Nullstellen ist immer noch minus fünf, aber ihre Summe ist nun Null, d.h. die restlichen Nullstellen sind $\pm\sqrt{5}$ und müssen einfach sein, da die Summe aller Vielfachheiten gleich dem Grad ist.

b) Finden Sie ein quadratfreies Polynom mit denselben Nullstellen!

Lösung: Da nur die Eins eine doppelte Nullstelle ist, müssen wir f durch $X - 1$ dividieren; das Ergebnis ist $X^3 - X^2 - 5X + 5$.

Aufgabe 7: *(4 Punkte)*

Finden Sie eine separierende Linearform aus $\mathbb{Q}[X, Y]$ für die Menge $\{0, 1\} \times \{1, 2\}$!

Lösung: Eine Gerade, die durch zwei der vier Punkte $(0, 1)$, $(0, 2)$, $(1, 1)$ und $(1, 2)$ geht, hat als Steigung die Differenz der y-Koordinaten durch die Differenz der x-Koordinaten, ist also entweder parallel zur y-Achse, oder hat ganzzahlige Steigung. Für die Gerade $y = x/2$ ist beides nicht der Fall; also ist $X - 2Y$ eine separierende Linearform.

Aufgabe 8: *(4 Punkte)*

a) Berechnen Sie die Resultante des Polynoms $f = X^2 + pX + q \in \mathbb{R}[X]$ und seiner Ableitung bezüglich der Variablen X!

Lösung: $f' = 2X + p$; die Resultante ist daher

$$\operatorname{Res}_X(f, f') = \begin{vmatrix} 1 & p & q \\ 2 & p & 0 \\ 0 & 2 & p \end{vmatrix} = \begin{vmatrix} p & 0 \\ 2 & p \end{vmatrix} - 2\begin{vmatrix} p & q \\ 2 & p \end{vmatrix} = p^2 - 2(p^2 - 2q) = -p^2 + 4q\,.$$

b) Was bedeutet es für die Lösungen der quadratischen Gleichung $x^2 + px + q = 0$, wenn diese Resultante positiv, negativ *bzw.* Null ist?

Lösung: Die Nullstellen sind $-\frac{p}{2} \pm \frac{1}{2}\sqrt{p^2 - 4q} = -\frac{p}{2} \pm \frac{1}{2}\sqrt{-\operatorname{Res}_X(f, f')}$. Bei negativer Resultante gibt es daher zwei reelle Lösungen, bei positiver zwei konjugiert komplexe, und bei verschwindender Resultante gibt es eine doppelte (reelle) Nullstelle.

Abgabe bis zum Montag, dem 18. Dezember 2017, um 10.00 Uhr