WOLFGANG K. SEILER
Tel. 2515

A5, C201

8. Januar 2018

Modulklausur Computeralgebra

Aufgabe 1: (*10 Punkte*)

a) Zeigen Sie: Ist $\varphi\colon R \to S$ ein Homomorphismus zwischen den kommutativen Ringen R und S, so ist $\operatorname{Kern}\varphi = \{x \in R \mid \varphi(x) = 0\}$ ein Ideal von R.

Lösung: Da $\varphi(0) = 0$ ist, liegt die Null im Kern, der somit nicht leer ist. Für $x, y \in \operatorname{Kern}\varphi$ ist $\varphi(x+y) = \varphi(x) + \varphi(y) = 0 + 0 = 0$, so daß auch die Summe im Kern liegt. Für $x \in \operatorname{Kern}\varphi$ und $r \in R$ schließlich ist $\varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0$, d.h. $rx \in \operatorname{Kern}\varphi$.

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

$$M_1 = \mathbb{Z}, \quad M_2 = 2\mathbb{Z}, \quad M_3 = \mathbb{Z}[X], \quad M_4 = \mathbb{Z}[X^2], \quad M_5 = \bigl\{f \in \mathbb{Z}[X] \bigm| f(5) = 0\bigr\},$$
$$M_6 = \bigl\{f \in \mathbb{Z}[X] \bigm| f(5) = 1\bigr\}, \quad M_7 = \bigl\{f \in \mathbb{Z}[X] \bigm| f\bigl(\sqrt{5}\bigr) = 0\bigr\},$$
$$M_8 = \left\{\sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X] \;\middle|\; \sum_{i=0}^{d} a_i = 0\right\}, \quad M_9 = \left\{\sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X] \;\middle|\; \sum_{i=0}^{d} 2^i a_i = 0\right\}$$

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

Lösung: M_1 enthält die Eins; wäre es ein Ideal müßte $M_1 = \mathbb{Z}[X]$ sein, was nicht der Fall ist. M_2 ist auch kein Ideal, denn $2 \in M_2$, aber das Produkt $X \cdot 2$ liegt nicht dort. M_3 als der ganze Ring ist natürlich ein Ideal; es wird erzeugt von der Eins. M_4 ist kein Ideal, da beispielsweise $X^2 \in M_4$, aber $X \cdot X^2 = X^3$ nicht.

M_5 ist ein Ideal, denn die Summe zweier Polynome, die an der Stelle fünf verschwinden, verschwindet auch dort, genauso wie das Produkt eines solchen Polynoms mit einem beliebigen Polynom. Da die Polynome mit Nullstelle fünf genau die durch $X - 5$ teilbaren sind, ist M_5 das Hauptideal $(X - 5)$. M_6 ist kein Ideal, denn für $f(5) = g(5) = 1$ ist $(f + g)(5) = 2$.

M_7 ist wieder ein Ideal, denn das Argument für M_5 gilt genauso, wenn wir anstelle der Fünf ihre Wurzel einsetzen. Schwieriger wird es mit dem Erzeugendensystem: In $\mathbb{R}[X]$ ist ein Polynom, das bei $\sqrt{5}$ verschwindet, durch $X - \sqrt{5}$ teilbar, aber dieses Polynom liegt nicht in $\mathbb{Z}[X]$. Für ein Polynom $f = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ verschwindet

$$f\bigl(\sqrt{5}\bigr) = \sum_{\substack{i=0 \\ i \text{ gerade}}}^{d} a_i \cdot 5^{i/2} + \sqrt{5} \cdot \sum_{\substack{i=0 \\ i \text{ ungerade}}}^{d} a_i \cdot 5^{(i-1)/2}$$

genau dann, wenn beide Summen verschwinden; dann verschwindet auch

$$f\bigl(-\sqrt{5}\bigr) = \sum_{\substack{i=0 \\ i \text{ gerade}}}^{d} a_i \cdot 5^{i/2} - \sqrt{5} \cdot \sum_{\substack{i=0 \\ i \text{ ungerade}}}^{d} a_i \cdot 5^{(i-1)/2}$$

Somit ist f teilbar durch $\bigl(X - \sqrt{5}\bigr)\bigl(X + \sqrt{5}\bigr) = X^2 - 5$, d.h. M_7 ist das Hauptideal $(X^2 - 5)$.

M_8 läßt sich einfacher beschreiben als Menge aller $f \in \mathbb{Z}[X]$ mit $f(1) = 0$, ist also das Hauptideal $(X-1)$. Entsprechend ist $M_9 = \big\{f \in \mathbb{Z}[X] \bigm| f(2) = 0\big\} = (X-2)$.

Aufgabe 2: *(10 Punkte)*

Welche der folgenden Vorschriften definiert eine Monomordnung auf $\mathbb{Q}[X,Y,Z]$?

a) $X^aY^bZ^c >_1 X^\alpha Y^\beta Z^\gamma$ falls $c > \gamma$ oder $c = \gamma$ und $b > \beta$ oder $c = \gamma$, $b = \beta$ und $a > \alpha$

Lösung: Das ist die lexikographische Ordnung für die Variablenanordnung $Z > Y > X$, also eine Monomordnung.

b) $X^aY^bZ^c >_2 X^\alpha Y^\beta Z^\gamma$ falls $a+2b+3c > \alpha+2\beta+3\gamma$ oder $a+2b+3c = \alpha+2\beta+3\gamma$ und $X^aY^bZ^c >_1 X^\alpha Y^\beta Z^\gamma$

Lösung: Auch das definiert eine Monomordnung: Es ist eine Totalordnung, denn im Fall $a+2b+3c = \alpha+2\beta+3\gamma$ sorgt die Monomordnung $>_1$ dafür, daß genau eine der Relationen größer, kleiner oder gleich erfüllt ist. Multipliziert man die Ungleichung $X^aY^bZ^c >_2 X^\alpha Y^\beta Z^\gamma$ mit $X^uY^vZ^w$, so wird beim Vergleich von $a+2b+3c$ mit $\alpha+2\beta+3\gamma$ auf beiden Seiten $u+2v+3w$ addiert, was nichts an der Ordnungsrelation ändert, und im Falle der Gleichheit wird die Monomordnung $>_1$ angewandt. Schließlich ist $>_2$ eine Wohlordnung, denn die Menge aller Tripel (a,b,c) mit $a+2b+3c = M$ ist für jede natürliche Zahl M endlich und hat daher wegen der Totalordnungseigenschaft ein kleinstes Element.

c) $X^aY^bZ^c >_3 X^\alpha Y^\beta Z^\gamma$ falls $a+2b+3c > \alpha+2\beta+3\gamma$ oder $a+2b+3c = \alpha+2\beta+3\gamma$ und $X^\alpha Y^\beta Z^\gamma >_1 X^aY^bZ^c$

Lösung: Das gleiche Argument wie bei *b)* zeigt, daß auch dies eine Monomordnung ist.

d) $X^aY^bZ^c >_4 X^\alpha Y^\beta Z^\gamma$ falls $a-2b+3c > \alpha-2\beta+3\gamma$ oder $a-2b+3c = \alpha-2\beta+3\gamma$ und $X^aY^bZ^c >_1 X^\alpha Y^\beta Z^\gamma$

Lösung: Dies ist keine Monomordnung, denn $Y >_4 Y^2 >_4 Y^3 >_4 \cdots$, so daß die Menge aller Y-Potenzen kein kleinstes Element enthält und $>_4$ keine Wohlordnung ist.

e) $X^aY^bZ^c >_5 X^\alpha Y^\beta Z^\gamma$ falls $abc > \alpha\beta\gamma$ oder $abc = \alpha\beta\gamma$ und $X^aY^bZ^c >_1 X^\alpha Y^\beta Z^\gamma$

Lösung: Das ist keine Monomordnung: Beispielsweise ist $XYZ^6 >_5 XY^2Z^3$, denn das Produkt der drei Exponenten ist in beiden Fällen sechs, so daß XYZ^6 wegen seiner höheren Z-Potenz größer ist. Multipliziert man aber beide Monome mit Z^5, so ist das Produkt der Exponenten in XYZ^{11} gleich elf, das in XY^2Z^8 aber sechzehn, so daß das zweite Monom größer ist.

Aufgabe 3: *(8 Punkte)*

a) Dividieren Sie in $\mathbb{Q}[X,Y]$ das Polynom $f = X^3Y^2 + 2X^3Y + 3X^2Y^3 + 4XY - 6Y + 3X - 9$ bezüglich der lexikographischen Ordnung durch die beiden Polynome $g = X^2 + 1$ und $h = Y + 1$!

Lösung: Die führenden Monome von g und h sind X^2 und Y, das von f ist X^3Y^2. Dies ist durch X^2 teilbar; also subtrahieren wir im ersten Schritt XY^2g und erhalten

$$2X^3Y + 3X^2Y^3 - XY^2 + 4XY - 6Y + 3X - 9\,.$$

Der führende Term $2X^3Y$ ist wieder durch X^2 teilbar; wir subtrahieren also $2XYg$ und erhalten
$$3X^2Y^3 - XY^2 + 2XY - 6Y + 3X - 9\,.$$
Auch hier ist der führende Term $3X^2Y^3$ durchX^2 teilbar; Subtraktion von $3Y^3g$ führt auf
$$-XY^2 + 2XY - 3Y^3 - 6Y + 3X - 9\,.$$
Nun ist der führende Term $-XY^2$ nicht mehr durch X^2 teilbar, aber durch Y; wir addieren also XYh und erhalten
$$3XY - 3Y^3 - 6Y + 3X - 9\,.$$
Auch $3XY$ ist durch Y teilbar; Subtraktion von $3Xh$ ergibt
$$-3Y^3 - 6Y - 9\,.$$
Der führende Term $-3Y^3$ ist durch Y teilbar; Addition von $3Y^2h$ ergibt $3Y^2 - 6Y - 9$. Subtraktion von $3Yh$ macht daraus $-9Y - 9$, was durch Addition von $9h$ zu Null wird. Somit ist
$$f = (XY^2 + 2XY + 3Y^3)g + (-XY + 3X - 3Y^2 + 3Y - 9)h\,.$$

b) Können Sie sicher entscheiden, ob f im von g und h erzeugten Ideal liegt?

Lösung: Natürlich, denn die letzte Formel stellt f als Linearkombination von g und h dar; somit liegt f in (g, h).

c) Bestimmen Sie $V_{\mathbb{C}}(f, g, h)$!

Lösung: Da f im Ideal (g, h) liegt, verschwindet f automatisch, wenn g und h verschwinden, d.h. $V_{\mathbb{C}}(f, g, h) = V_{\mathbb{C}}(g, h) = \big\{(i, -1), (-i, -1)\big\}$.

Aufgabe 4: *(15 Punkte)*

a) Beschreiben Sie die Nullstellenmengen $V_{\mathbb{R}}(f)$ und $V_{\mathbb{R}}(g)$ der beiden Polynome
$$f = X^2 + Y^2 - 4Y - 12 \quad \text{und} \quad X^2 + Y^2 - 2X - 8$$
geometrisch!

Lösung: $f = X^2 + (Y - 2)^2 - 16$ und $g = (X - 1)^2 + Y^2 - 9$; somit ist $V_{\mathbb{R}}(f)$ der Kreis mit Radius vier um den Punkt $(0, 2)$ und $V_{\mathbb{R}}(g)$ der mit Radius drei um $(1, 0)$.

b) Zeigen Sie, daß die führenden Terme von f und g bezüglich jeder Monomordnung übereinstimmen!

Lösung: Bezüglich jeder Monomordnung ist ein Monom größer als seine Teiler; daher kann der führende Term von f und g nur X^2 oder Y^2 sein. Falls $X^2 > Y^2$, ist er in beiden Fällen X^2, sonst Y^2.

c) Bilden f und g bezüglich irgendeiner Monomordnung eine GRÖBNER-Basis des Ideals $I = (f, g)$?

Lösung: Da f und g denselben führenden Term haben, ist $S(f, g) = f - g = 2X - 4Y - 4$. Je nach Monomordnung haben f und g entweder X^2 oder Y^2 als führenden Term, und damit kann dieses lineare Polynom nicht nach dem Divisionsalgorithmus modulo f und g weiter reduziert werden. Nach BUCHBERGERS Kriterium bilden f, g daher keine GRÖBNER-Basis.

d) Finden Sie ein lineares Polynom $h \in \mathbb{Q}[X,Y]$, das auf ganz $V_{\mathbb{C}}(f,g)$ verschwindet!

Lösung: Das gerade berechnete S-Polynom $f-g = 2X-4Y-4$ ist linear und verschwindet natürlich in allen Punkten $(x,y) \in \mathbb{C}^2$, in denen sowohl f als auch g verschwindet. Da alle seine Koeffizienten gerade sind, empfiehlt es sich, es noch durch zwei zu dividieren und $h = X - 2Y - 2$ zu setzen

e) Finden Sie in $I = (f,g)$ nichttriviale Polynome $p \in \mathbb{Q}[X]$ und $q \in \mathbb{Q}[Y]$!

Lösung: $h = 0$ läßt sich sowohl nach X als auch nach Y auflösen zu

$$X = 2Y + 2 \quad \text{und} \quad Y = \frac{X}{2} - 1 .$$

Einsetzen in f oder g führt zu

$$q = (2Y+2)^2 + Y^2 - 4Y - 12 = 5Y^2 + 4Y - 8 \quad \text{und} \quad p = X^2 + \left(\frac{X}{2} - 1\right)^2 - 2X - 8 = \frac{5}{4}X^2 - 4X - 7 .$$

f) Ist $I = (p,q)$?

Lösung: Nein, denn $V_{\mathbb{C}}(p,q) = V_{\mathbb{C}}(p) \times V_{\mathbb{C}}(q)$ enthält vier Punkte, $V_{\mathbb{C}}(I) = V_{\mathbb{C}}(f,h)$ aber nur zwei.

g) Zeigen Sie, daß die Polynome h und q eine reduzierte GRÖBNER-Basis von I bezüglich der lexikographischen Ordnung bilden!

Lösung: Zunächst bilden h und q ein Erzeugendensystem, denn $I = (f,g) = (f,h)$, und das ist gleich (q,h), da $q \equiv f \bmod h$.
Zum Nachweis, daß wir eine GRÖBNER-Basis haben, berechnen und reduzieren wir das S-Polynom

$$5S(q,h) = Xq - 5Y^2h = 4XY - 8X + 10Y^3 + 10Y^2 .$$

Der führende Term $4XY$ ist nicht durch Y^2, aber durch X teilbar; Subtraktion von $4Yh$ führt auf

$$-8X + 10Y^3 + 10Y^2 + 8Y^2 + 8Y = -8X + 10Y^3 + 18Y^2 + 8Y .$$

Der neue führende Term $-8X$ kann durch Addition von $8h$ eliminiert werden; übrig bleibt $10Y^3 + 18Y^2 - 8Y - 16$.
Der führende Term ist durch $5Y^2$ teilbar; Subtraktion von $2Yq$ führt auf $10Y^2 + 8Y - 16$. Der führende Term ist das Doppelte dessen von q, und Subtraktion von $2q$ reduziert dies zu Null.

h) Hat diese Basis eine Gestalt gemäß dem Shape-Lemma?

Lösung: Ja, denn q ist ein Polynom nur in Y, und h ist von der Form X plus (lineares) Polynom in Y.

Aufgabe 5: (*12 Punkte*)

a) Zeigen Sie: Besteht das Polynom $q \in k[X_1, \dots, X_n]$ nur aus einem Monom und ist der führende Term von $p \in k[X_1, \dots, X_n]$ teilerfremd zu diesem Monom, so läßt sich $S(p,q)$ mit dem Divisionsalgorithmus bezüglich q und p auf Null reduzieren.

Lösung: Da q teilerfremd zum führenden Monom von p ist, ist

$$\mathrm{FK}(p) \cdot S(p,q) = qp - \mathrm{FT}(p)q = \big(p - \mathrm{FT}(p)\big)q .$$

Somit sind alle Monome durch q teilbar, das S-Polynom kann also durch den Divisionsalgorithmus auf Null reduziert werden.

b) Bestimmen Sie möglichst einfach alle komplexen Nullstellen des von $f = X^2 + 2XY + Y^2$ und $g = Y^2 - 2XY + X^2$ in $\mathbb{Q}[X, Y]$ erzeugten Ideals I!

Lösung: Offensichtlich ist $f = (X+Y)^2$ und $g = (X-Y)^2$. Die Nullstellen von I sind daher die von $X + Y$ und $X - Y$, also nur der Nullpunkt.

c) Bestimmen Sie das Radikal von I!

Lösung: Da $(X \pm Y)^2 \in I$, liegen $X \pm Y$ in $\sqrt{I}$, also auch X und Y. Da (X, Y) als maximales Ideal insbesondere prim ist, ist es ein Radikalideal, also, da es in $\sqrt{I}$ liegt, gleich dem Radikal von I.

d) Finden Sie eine GRÖBNER-Basis von $\sqrt{I}$!

Lösung: Die angegebene Basis X, Y ist nach dem Kriterium von BUCHBERGER eine GRÖBNER-Basis, denn $S(X, Y) = YX - XY = 0$.

e) Wenden Sie den BUCHBERGER-Algorithmus an, um eine GRÖBNER-Basis von I bezüglich der graduiert-lexikographischen Ordnung zu bestimmen!

Lösung: f und g haben beide den führenden Term X^2; daher ist $S(f, g) = f - g = 4XY$. Da dies nicht durch X^2 teilbar ist, kann es nicht weiter reduziert werden; wir nehmen also $h = XY$ in die Basis auf.

$S(f, h) = Yf - Xh = 2XY^2 + Y^3 - X^2Y$ hat den führenden Term $-X^2Y$; Addition von Yf führt auf $4XY + 4Y^3$. Der neue führende Term $4XY$ wird durch Subtraktion von $4h$ eliminiert, und übrig bleibt $4Y^3$. Das läßt sich nicht weiter reduzieren; also müssen wir Y^3 in die Basis aufnehmen.

Genauso läßt sich auch $S(g, h)$ auf $4Y^3$ reduzieren.

$S(f, Y^3)$ und $S(g, Y^3)$ lassen sich nach *a)* auf Null reduzieren, und $S(h, Y^3)$ ist als S-Polynom zweier Monome ohnehin Null. Also bilden f, g, h und Y^3 eine GRÖBNER-Basis.

f) Bestimmen Sie die reduzierte GRÖBNER-Basis dazu!

Lösung: Die führenden Terme der Basiselemente sind X^2, X^2, XY und Y^3. Daher kann eines der beiden Polynome f, g eliminiert werden, und beim anderen kann mit h der XY-Term eliminiert werden. Übrig bleibt eine reduzierte Basis aus $X^2 + Y^2, XY$ und Y^3.

g) Bestimmen Sie die Vielfachheiten der Nullstellen aus $V_{\mathbb{C}}(I)$!

Lösung: Die Standardmonome bezüglich der gerade berechneten GRÖBNER-Basis sind X, Y, XY und Y^2; somit ist $\mathbb{Q}[X, Y]/I$ ein vierdimensionaler Vektorraum. Einzige Nullstelle ist $(0, 0)$. Da die Summe aller Vielfachheiten gleich der Dimension des Faktorrings ist, hat der Nullpunkt somit Multiplizität vier.

Aufgabe 6: *(6 Punkte)*

a) Welche Nullstellen hat das Polynom $f = X^4 - X^3 - 5X^2 + 3X + 6$, und welche Vielfachheiten haben sie?

Lösung: Das Produkt aller Nullstellen ist nach VIÈTE gleich sechs (vier ist gerade), und die Summe ist eins.

$f(1) = 1 - 1 - 5 + 3 + 6 = 4$, also ist eins keine Nullstelle.

$f(-1) = 1 + 1 - 5 + 3 - 6 = 0$, also ist minus eins eine Nullstelle.

$f(2) = 16 - 8 - 20 + 6 + 6 = 0$, also ist auch zwei eine Nullstelle

Das Produkt der restlichen beiden Nullstellen ist minus drei, und ihre Summe ist Null, d.h. die restlichen Nullstellen sind $\pm\sqrt{3}$ und müssen einfach sein, da die Summe aller Vielfachheiten gleich dem Grad ist.

b) Das Polynom $g = X^5 + X^4 - 2X^3 - 2X^2 + X + 1$ wurde so konstruiert, daß es nur ganzzahlige Nullstellen hat. Bestimmen Sie diese sowie auch ihre Vielfachheiten, und finden Sie ein quadratfreies Polynom, das die gleichen Nullstellen hat!

Lösung: Das Produkt aller Nullstellen ist -1 und ihre Summe auch. Falls alle Nullstellen ganzzahlig sind, kommen also nur ± 1 in Frage, wobei die Vielfachheit von -1 ungerade und um eins größer als die von eins sein muß. Bei nur ganzzahligen Nullstellen heißt dies, daß -1 eine dreifache und 1 eine doppelte Nullstelle sein muß.

Aufgabe 7: *(4 Punkte)*

Finden Sie eine separierende Linearform für $\{(0,2), (-1,1), (1,1), (-2,0), (0,0), (2,0)\}$!

Lösung: Die sechs Punkte sind die Ecken und Seitenmitten des Dreiecks mit Ecken $(-2,0)$, $(2,0)$ und $(0,2)$. Eine Gerade, die durch zwei der sechs Punkte geht, kann waagrecht oder senkrecht sein; die durch $(-2,0)$ und $(0,2)$ hat Steigung eins, die durch $(2,0)$ und $(0,2)$ minus eins. Bleiben noch die Geraden durch $(-2,0)$ und $(1,1)$ sowie $(2,0)$ und $(-1,1)$; die haben Steigung $\pm\frac{1}{3}$. Eine Gerade mit Steigung zwei kann somit nicht durch zwei dieser Punkte gehen, d.h. die Linearform $Y - 2X$ nimmt auf jedem der sechs Punkte einen anderen Wert an.

Aufgabe 8: *(5 Punkte)*

a) Für welche reellen Zahlen p haben die beiden quadratischen Gleichungen $x^2 + px + 1 = 0$ und $x^2 + x + p = 0$ mindestens eine gemeinsame Lösung?

Lösung: Die Resultante der beiden Polynome $X^2 + pX + 1$ und $X^2 + X + p$ ist

$$\begin{vmatrix} 1 & p & 1 & 0 \\ 0 & 1 & p & 1 \\ 1 & 1 & p & 0 \\ 0 & 1 & 1 & p \end{vmatrix} = \begin{vmatrix} 1 & p & 1 & 0 \\ 0 & 1 & p & 1 \\ 0 & 1-p & p-1 & 0 \\ 0 & 1 & 1 & p \end{vmatrix}$$

(Subtraktion der ersten Zeile von der dritten.) Entwicklung nach der ersten Spalte macht dies zu

$$\begin{vmatrix} 1 & p & 1 \\ 1-p & p-1 & 0 \\ 1 & 1 & p \end{vmatrix} = (p-1)\begin{vmatrix} 1 & p & 1 \\ -1 & 1 & 0 \\ 1 & 1 & p \end{vmatrix} = (p-1)(p+0-1-1+p^2) = (p-1)(p^2+p-2)$$

nach SARRUS. p^2+p-2 hat die beiden Nullstellen $p = 1$ und $p = -2$; die beiden Polynome haben also genau in diesen beiden Fällen gemeinsame Nullstellen.

b) Wie viele gemeinsame Lösungen haben sie für diese Werte von p jeweils?

Lösung: Für $p = 1$ sind beide Gleichungen identisch, haben also die gleichen beiden Lösungen. Für $p = -2$ sind die Gleichungen verschieden und haben beide den führenden Koeffizienten eins; daher können sie nur eine gemeinsame Nullstelle haben.

Abgabe bis zum Donnerstag, dem 8. Januar 2018, um 12.00 Uhr