Wolfgang K. Seiler
Tel. 2515

A5, C201

3. Februar 2015

Modulklausur Computeralgebra

Aufgabe 1: (*7 Punkte*)

a) Stellen Sie den größten gemeinsamen Teiler von 2015 und 1989 als Linearkombination dieser beiden Zahlen dar!

Lösung: Der Euklidische Algorithmus führt auf

$$2015 : 1989 = 1 \quad \text{Rest } 26 \Longrightarrow 26 = 2015 - 1989$$
$$1989 : 26 = 76 \quad \text{Rest } 13 \Longrightarrow 13 = 1989 - 76\cdot 26 = 1989 - 76\cdot(2015 - 1989) = 77\cdot 1989 - 76\cdot 2015\,.$$

Da 26 durch 13 teilbar ist, ist das die gesuchte Darstellung des ggT.

b) Bestimmen Sie alle Paare $(x, y) \in \mathbb{Z}^2$, für die $2015x + 1989y = 65$ ist!

Lösung: Um die Zahlen handhabbarer zu machen, empfiehlt es sich, zunächst durch den ggT 13 zu dividieren; die neue Gleichung ist $155x + 153y = 5$. Die in *a)* berechnete Darstellung des ggT wird nach Division durch 13 zu $1 = 153 \cdot 77 - 155 \cdot 76$; Multiplikation mit fünf macht daraus

$$153 \cdot 385 - 155 \cdot 380 = 5\,,$$

d.h. $x = -380$ und $y = 385$ ist eine Lösung. Die homogene Gleichung $155u - 153v = 0$ hat, da 153 und 155 teilerfremd sind, die Paare $(153k, -155k)$ mit $k \in \mathbb{Z}$ als Lösung; die Lösungsmenge der Ausgangsgleichung ist also

$$\{(153k - 380, 385 - 155k) \mid k \in \mathbb{Z}\} = \{(153n - 74, 75 - 155n) \mid n \in \mathbb{Z}\}\,.$$

c) Bestimmen Sie alle Paare $(u, v) \in \mathbb{Z}^2$, für die $2015u + 1989v = 165$ ist!

Lösung: Da 165 kein Vielfaches von $13 = \mathrm{ggT}(2015, 1989)$ ist, hat diese Gleichung keine ganzzahligen Lösungen.

d) Finden Sie eine natürliche Zahl $z \in \mathbb{N}$ mit $z \equiv 82 \bmod 153$ und $z \equiv 79 \bmod 155$. *(Hinweis: Auch dafür können Sie a) verwenden.)*

Lösung: Wie wir aus *a)* und *b)* wissen, ist $1 = 153 \cdot 77 - 155 \cdot 76$, d.h.

$$153 \cdot 77 = 11781 \equiv \begin{cases} 1 & \bmod 155 \\ 0 & \bmod 153 \end{cases} \quad \text{und} \quad -155 \cdot 76 = -11780 \equiv \begin{cases} 0 & \bmod 155 \\ 1 & \bmod 153 \end{cases}.$$

Somit ist

$$x = 79 \cdot 11781 - 82 \cdot 11780 = -35261$$

eine Lösung. Die kleinste positive Lösung ist $x + 2 \cdot 153 \cdot 155 = 12169$.

Aufgabe 2: (*7 Punkte*)

a) Für welche Werte von Y haben die beiden Polynome $f = X^2 + XY + Y$ und $g = X^2 - Y^2$ aus $\mathbb{Q}[X, Y]$ einen gemeinsamen Faktor positiven Grades?

Lösung: Das ist genau dann der Fall, wenn die Resultante

$$\begin{aligned}\mathrm{Res}_X(f,g) &= \begin{vmatrix} 1 & Y & Y & 0 \\ 0 & 1 & Y & Y \\ 1 & 0 & -Y^2 & 0 \\ 0 & 1 & 0 & -Y^2 \end{vmatrix} = Y^2 \begin{vmatrix} 1 & Y & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & -Y & 0 \\ 0 & 1 & 0 & -Y \end{vmatrix} \\ &= Y^2 \left(\begin{vmatrix} 1 & 1 & 1 \\ 0 & -Y & 0 \\ 1 & 0 & -Y \end{vmatrix} + \begin{vmatrix} Y & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & -Y \end{vmatrix} \right) \\ &= Y^2 \Big(\big(Y^2 - (-Y)\big) + \big(-Y^2 + 1 - (-Y)\big) \Big) = Y^2(2Y+1)\,. \end{aligned}$$

verschwindet, d.h. für $Y = 0$ und $Y = -\frac{1}{2}$.

b) Geben Sie diesen Faktor jeweils an!

Lösung: Für $Y = 0$ werden beide Polynome zu X^2, und das ist der gemeinsame Faktor. Für $Y = -\frac{1}{2}$ wird f zu $X^2 - \frac{1}{2}X - \frac{1}{2} = (X-1)(X+\frac{1}{2})$ und g zu $X^2 - \frac{1}{4} = (X+\frac{1}{2})(X-\frac{1}{2})$; der gemeinsame Faktor ist also $X + \frac{1}{2}$.

c) Bestimmen Sie alle Paare $(x,y) \in \mathbb{R}^2$, für die $f(x,y) = g(x,y) = 0$ ist!

Lösung: Wenn (x,y) eine Lösung ist, müssen $f(X,y)$ und $g(X,y)$ beide durch $X-x$ teilbar sein, d.h. entweder ist $y = 0$ und $x = 0$ oder $y = x = -\frac{1}{2}$.

Aufgabe 3: (*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 Teilmengen sind Ideale in $\mathbb{Z}[X]$? (Bei den angegebenen Polynomen soll stets d beliebig und $a_d \neq 0$ sein.)

$$M_1 = \mathbb{Z}, \quad M_2 = \mathbb{Z}[X^2], \quad M_3 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X] \;\middle|\; \text{alle } a_i \text{ sind gerade} \right\},$$

$$M_4 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X] \;\middle|\; \sum_{i=0}^{d} a_i \text{ ist gerade} \right\}, \quad M_5 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X] \;\middle|\; \sum_{i=0}^{d} a_i \text{ ist ungerade} \right\}$$

$$M_6 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X] \;\middle|\; a_0 \text{ ist gerade} \right\}, \quad M_7 = \left\{ \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X] \;\middle|\; a_d \text{ ist gerade} \right\},$$

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

Lösung: M_1, M_2 und M_5 enthalten die Eins. Wenn ein Ideal die Eins enthält, muß es gleich dem gesamten Ring sein; dies ist hier nicht der Fall. Somit sind diese drei Mengen keine Ideale.

M_3 besteht aus allen Vielfachen der Zwei, ist also das Hauptideal (2).

Wenn die Summe aller Koeffizienten eines Polynoms gerade ist, läßt sich durch Addition eines Polynoms mit geraden Koeffizienten (z.B. einer geraden Konstanten) erreichen, daß die Summe zu Null wird; umgekehrt führt die Addition eines Polynoms mit Koeffizientensumme Null und eines Polynoms mit lauter geraden Koeffizienten stets zu einem Polynom

mit gerader Koeffizientensumme. Ein Polynom hat genau dann Koeffizientensumme Null, wenn es an der Stelle Eins verschwindet, wenn es also durch $X-1$ teilbar ist. Somit ist M_4 das von 2 und $X-1$ erzeugte Ideal.

Entsprechend ist M_6 das von 2 und X erzeugte Ideal, denn die Polynome mit geradem a_0 sind genau die Summen aus Polynomen mit lauter geraden Koeffizienten und Polynomen mit $a_0 = 0$, und letztere sind genau die Vielfachen von X.

M_7 ist kein Ideal, denn es enthält zwar die Polynome $X+1$ und $X+2$, nicht aber deren Summe $2X+3$.

Aufgabe 4: (*9 Punkte*)

Wir betrachten das Polynom $f = 12X^3 + 30X^2 + 18X + 6 \in \mathbb{Z}[X]$.

a) Bestimmen Sie den Inhalt und den primitiven Anteil von f!

Lösung: Der Inhalt $I(f)$ ist der ggT der Koeffizienten, also sechs; der primitive Anteil ist somit $f^* = f/6 = 2X^3 + 5X^2 + 3X + 1$.

b) Zeigen Sie, daß $f^{(5)} = f \bmod 5 \in \mathbb{F}_5[X]$ irreduzibel ist!

Lösung: Wenn $f^{(5)} = 2X^3+3X+1 \in \mathbb{F}_5[X]$ nicht irreduzibel wäre, müßte es einen linearen Faktor geben, also eine Nullstelle. $f^{(5)}(0) = 1$, $f^{(5)}(1) = 1$, $f^{(5)}(2) = 3$, $f^{(5)}(3) = 4$ und $f^{(5)}(4) = f^{(5)}(-1) = 1$ sind aber allesamt von Null verschieden.

c) Zerlegen Sie f in $\mathbb{Z}[X]$ in seine irreduziblen Faktoren!

Lösung: Hätte f einen linearen oder quadratischen Faktor, so auch $f^{(5)}$; daher gibt es nur Faktoren vom Grad 0 oder 3. Der primitive Anteil ist durch keine Primzahl teilbar; daher ist $f = 2 \cdot 3 \cdot f^*$ die Zerlegung von f in irreduzible Faktoren.

d) Zerlegen Sie f in $\mathbb{Q}[X]$ in seine irreduziblen Faktoren!

Lösung: Ließe sich f in $\mathbb{Q}[X]$ als Produkt zweier Polynome positiven Grades schreiben, so nach GAUSS auch in $\mathbb{Z}[X]$. Da dies nach *c)* nicht der Fall ist, ist f in $\mathbb{Q}[X]$ irreduzibel. (2 und 3 sind dort natürlich Einheiten.)

e) Für welche Primzahlen p ist die SYLVESTER-Matrix von $f^{(p)}$ und $f^{(p)\prime}$ gleich der SYLVESTER-Matrix von f und f' modulo p?

Lösung: Dies gilt genau dann, wenn die führenden Koeffizienten der beiden Polynome modulo p nicht verschwinden. Da diese 12 und $3 \cdot 12$ sind, stimmt es also für alle Primzahlen $p \geq 5$.

Aufgabe 5: (*18 Punkte*)

Wir betrachten das Ideal $I = (f, g)$ mit

$$f = (X-1)^2 + Y^2 - 25 \quad \text{und} \quad g = (X-1)Y - 12$$

im Polynomring $\mathbb{Q}[X, Y]$.

a) Zeigen Sie, daß g bezüglich jeder Monomordnung (auch solcher, die nicht in der Vorlesung behandelt wurden) denselben führenden Term hat!

Lösung: $g = XY - Y - 12$ besteht aus den drei Monomen XY, Y und 1; da diese allesamt Teiler von XY sind und ein Vielfaches eines Monoms bezüglich jeder Monomordnung größer sein muß als das Monom selbst, ist XY stets führend.

b) Geben Sie für jeden Term von f, der als führender Term bezüglich einer Monomordnung auftreten kann, eine entsprechende Monomordnung an!

Lösung: $f = X^2-2X+1+Y^2-25 = X^2-2X+Y^2-24$ ist Linearkombination der Monome $1, X, X^2$ und Y^2. Da 1 und X Teiler von X^2 sind, können sie nie führend werden. X^2 *bzw.* Y^2 sind führend z.B. bezüglich der lexikographischen Ordnung mit $X > Y$ *bzw.* $Y > X$.

Im folgenden arbeiten wir mit der lexikographischen Ordnung mit $X > Y$.

c) Berechnen Sie das S-Polynom von f und g und bestimmen Sie seinen Rest h bei der Division durch f und g!

Lösung: Der führende Term von f ist X^2, der von g ist XY; somit ist

$$S(f,g) = Y\cdot f - X\cdot g = (X^2Y-2XY+Y^3-24Y)-(X^2Y-XY-12X) = -XY+12X+Y^3-24Y\,.$$

Der führende Term $-XY$ ist durch den führenden Term XY von g teilbar; Addition von g führt auf

$$(-XY+12X+Y^3-24Y)+(XY-Y-12) = 12X+Y^3-25Y-12\,.$$

Da keiner der Terme durch X^2 oder XY teilbar ist, ist dies der Divisionsrest h.

d) Berechnen Sie das S-Polynom k von g und h!

Lösung: Der führende Term von g ist XY, der von h ist $12X$; also ist

$$12S(g,h) = 12g - Yh = (12XY-12Y-144)-(12XY+Y^4-25Y^2-12Y) = -Y^4+25Y^2-144$$

und $k = -\dfrac{1}{12}Y^4 + \dfrac{25}{12}Y^2 - 12.$

e) Zeigen Sie, daß h und k eine GRÖBNER-Basis des Ideal (h,k) in $\mathbb{Q}[X,Y]$ bilden, und bestimmen Sie die zugehörige reduzierte Basis!

Lösung: Wir verwenden BUCHBERGERs Kriterium, müssen also das S-Polynom von h und k berechnen. An diesem S-Polynom ändert sich nichts, wenn wir der Übersichtlichkeit halber die beiden Polynome auf höchsten Koeffizienten eins normieren, wenn wir also mit

$$h^* = X + \frac{1}{12}Y^3 - \frac{25}{12}Y - 1 \quad \text{und} \quad k^* = Y^4 - 25Y^2 + 144$$

arbeiten. Die führenden Terme sind dann X und Y^4, d.h.

$$\begin{aligned} S(h,k) = S(h^*,k^*) = Y^4h^* - Xk^* &= \left(XY^4 + \frac{1}{12}Y^7 - \frac{25}{12}Y^5 - Y^4\right) - (XY^4 - 25XY^2 + 144X) \\ &= 25XY^2 - 144X + \frac{1}{12}Y^7 - \frac{25}{12}Y^5 - Y^4\,. \end{aligned}$$

Der führende Term $25XY^2$ ist durch den führenden Term X von h^* teilbar; Subtraktion von $25X^2h^*$ führt auf

$$-144X + \frac{1}{12}Y^7 - \frac{25}{6}Y^5 - Y^4 + \frac{625}{12}Y^3 + 25Y^2\,.$$

Wieder ist der führende Term durch X teilbar; Addition von $144h^*$ führt auf

$$\frac{1}{12}Y^7 - \frac{25}{12}Y^5 - Y^4 + \frac{769}{12}Y^3 + 25Y^2 - 300Y - 144\,.$$

Jetzt ist der führende Term durch Y^4 teilbar; Subtraktion von $\frac{1}{2}Y^3k^*$ liefert

$$-\frac{25}{12}Y^5 - Y^4 + \frac{625}{12}Y^3 + 25Y^2 - 300Y - 144\,.$$

Auch hier ist der führende Term durch Y^4 teilbar; addieren wir dazu $\frac{25}{12}Yk^*$, ergibt sich $-Y^4+25Y^2-144=-k^*$, was durch Addition von k^* zur Null reduziert wird. Also ist das S-Polynom ohne Rest durch h und k teilbar, und damit bilden h und k nach BUCHBERGER eine GRÖBNER-Basis. Die zugehörige minimale GRÖBNER-Basis ist h^*, k^*, und die ist sogar schon reduziert.

f) Warum ist $(h,k)\subseteq(f,g)$?

Lösung: Das S-Polynom von f und g ist eine Linearkombination von f und g über $\mathbb{Q}[X,Y]$, liegt also in (f,g). Damit liegt auch der Divisionsrest h bei der Division durch f und g dort. Entsprechend ist $k=S(g,h)\in(f,g)$.

g) Zeigen Sie, daß sogar $(h,k)=(f,g)$ ist!

Lösung: Dazu muß gezeigt werden, daß f und g in $(h,k)=(h^*,k^*)$ liegen. Da h^* und k^* eine GRÖBNER-Basis bilden, ist dies genau dann der Fall, wenn f und g sich ohne Rest durch h^* und k^* dividieren lassen.
Beginnen wir mit f. Der führende Term X^2 ist durch den führenden Term X von h^* teilbar und

$$f-Xh^*=-\frac{1}{12}XY^3+\frac{25}{12}XY-X-24+Y^2\,.$$

Wieder ist der führende Term durch X teilbar; Addition von $\frac{1}{12}Y^3h$ führt auf

$$\frac{25}{12}XY-X-\frac{1}{144}Y^6-\frac{25}{144}Y^4-\frac{1}{12}Y^3+Y^2-24\,,$$

was durch Subtraktion von $\frac{25}{12}Yh^*$ zu

$$-X+\frac{1}{144}Y^6-\frac{25}{72}Y^4-\frac{1}{12}Y^3+\frac{769}{144}Y^2+\frac{25}{12}Y-24$$

wird. Eine letzte Addition von f eliminiert X vollständig und läßt

$$\frac{1}{144}Y^6-\frac{25}{72}Y^4+\frac{769}{144}Y^2-25=\frac{1}{144}\left(Y^6-50Y^4+769Y^2-3600\right)$$

zurück. Ab hier kommt für die weitere Reduktion nur noch k^* in Frage; da wir es nur noch mit Polynomen in Y zu tun haben, wird der Divisionsalgorithmus zur altbekannten Polynomdivision in einer Veränderlichen. Uns geht es nur um darum, ob die Division ohne Rest aufgeht; daher können wir auf den Vorfaktor verzichten und erhalten

$$(Y^6-50Y^4+769Y^2-3600):(Y^4-25Y^2+144)=Y^2-25\quad\text{Rest }0\,.$$

Also liegt f in $(h^*,k^*)=(h,k)$.
Der führende Term von g ist XY; auch er ist durch X teilbar und

$$g-Y*h^*=-\frac{1}{12}Y^4+\frac{25}{12}Y^2-12=-\frac{k^*}{12}\,.$$

Damit liegt auch g in (h^*,k^*) und $(f,g)=(h^*,k^*)=(h,k)$.

h) Bestimmen Sie die Nullstellenmenge von f und g!

Lösung: Das ist die Nullstellenmenge von h und k oder auch von h^* und k^*.

$$Y^4-25Y^2+144=\left(Y^2-\frac{25}{2}\right)^2-\frac{625}{4}+144=\left(Y^2-\frac{25}{2}\right)^2-\frac{625-576}{4}=\left(Y^2-\frac{25}{2}\right)^2-\frac{49}{625}$$

verschwindet genau dann, wenn $Y^2 - \frac{25}{2} = \pm\frac{7}{2}$ ist, also wenn Y^2 gleich 9 oder 16 ist. Damit kann Y in den Nullstellen nur die Werte ± 3 und ± 4 annehmen. Wenn auch h^* in (x, y) verschwindet, ist

$$x = -\frac{1}{12}y^3 + \frac{25}{12}y + 1\,;$$

wir erhalten also die vier Punkte $(-3,-3)$, $(5,3)$, $(-2,-4)$ und $(4,4)$.

i) Interpretieren Sie das Ergebnis geometrisch!

Lösung: Die Nullstellenmenge von f ist der Kreis um $(1, 0)$ mit Radius fünf, die von g ist eine Hyperbel. Die beiden Kurven schneiden sich in den vier berechneten Punkten.

Aufgabe 6: *(9 Punkte)*

Wir betrachten $f = X^4 - 5X^3 - 12X^2 + 22X - 8 \in \mathbb{Z}[X]$.

a) Man kann zeigen, daß $f \equiv (X^2 + 2X + 3)(X^2 + 3X + 4) \bmod 5$ ist, wobei beide Faktoren in $\mathbb{F}_5[X]$ irreduzibel sind. Was folgt daraus über die Anzahl und den Grad möglicher Faktoren von f in $\mathbb{Z}[X]$?

Lösung: Da f den Inhalt eins hat, ist f entweder irreduzibel oder zerfällt in zwei quadratische Faktoren.

b) Wie lassen sich Polynome $g, h \in \mathbb{Z}[X]$ konstruieren, für die $f \equiv g \cdot h \bmod 25$ ist? (Die Beschreibung des Rechengangs genügt!)

Lösung: Nach dem Hensel*schen* Lemma können wir die Faktorisierung modulo 5 hochheben zu einer Faktorisierung modulo 25: Sei $g_0 = X^2 + 2X + 3$ und $h_0 = X^2 + 3X + 4$; wir setzen

$$g = X^2 + 2X + 3 + 5g_1 \quad \text{und} \quad h = X^2 + 3X + 4 + 5h_1$$

mit $g_1, h_1 \in \mathbb{Z}[X]$. Dann ist $g_0h_0 = X^4 + 5X^3 + 13X^2 + 17X + 12$ und

$$gh - f = g_0h_0 + 5g_0h1 + 5h_0g_1 + 25g_1h_1 - f = 10X^3 + 25X^2 - 5X + 20 + 5g_0h1 + 5h_0g_1 + 25g_1h_1\,.$$

Das soll modulo 25 verschwinden, was äquivalent ist zur Kongruenz

$$2X^3 - X + 4 + g_0h_1 + h_0g_1 \equiv 0 \bmod 5\,.$$

Wir müssen daher g_1 und h_1 so wählen, daß $h_1g_0 + g_1h_0 \equiv 3X^3 + X + 1 \bmod 5$ ist. Wenn g_0 und h_0 in $\mathbb{F}_5[X]$ teilerfremd sind, können wir die Eins linear aus ihnen kombinieren und damit auch jedes andere Polynom. Durch Reduktion modulo der Gleichung $g_0h_0 - h_0g_0 = 0$ können wir erreichen, daß die Koeffizienten dabei kleineren Grad als h_0 *bzw.* g_0 haben.

c) Wie sich zeigt, ist $f \equiv (X^2 + 2X + 23)(X^2 + 18X + 4) \bmod 25$. Zerlegen Sie f in $\mathbb{Z}[X]$ in seine irreduziblen Faktoren!

Lösung: Wenn es eine echte Zerlegung gibt, dann sind die Faktoren wegen der Primitivität von f und wegen der bekannten Zerlegung modulo fünf normierte quadratische Polynome. Das Produkt der konstanten Terme muß -8 sein, und modulo 25 sind die beiden Terme 23 und 4. Somit müssen die konstanten Terme -2 und 4 sein. Damit ist

$$f = (X^2 + aX - 2)(X^2 + bX + 4) \quad \text{mit} \quad a \equiv 2 \bmod 25 \quad \text{und} \quad b \equiv 18 \bmod 25\,.$$

Da die Koeffizienten von f eher klein sind, können wir es mit $a = 2$ und $b = -7$ probieren und erhalten mit $(X^2 + 2X - 2)(X^2 - 7X + 4) = X^4 - 5X^3 - 12X^2 + 22X - 8 = f$ die gewünschte Faktorisierung.

Abgabe bis zum Dienstag, dem 3. Februar 2015, um 17.30 Uhr