Wolfgang K. Seiler
Tel. 2515

A5, C201

13. Dezember 2014

Modulklausur Computeralgebra

Aufgabe 1: (*9 Punkte*)

a) Stellen Sie den größten gemeinsamen Teiler von 301 und 259 als Linearkombination dieser beiden Zahlen dar!

Lösung: Der Euklidische Algorithmus führt auf

$$\begin{aligned} 301 : 259 = 1 \quad \text{Rest } 42 &\Longrightarrow 42 = 301 - 259 \\ 259 : 42 = 6 \quad \text{Rest } 7 &\Longrightarrow 7 = 259 - 6 \cdot 42 = 259 - 6 \cdot (301 - 259) = 7 \cdot 259 - 6 \cdot 301 \,. \end{aligned}$$

Da 42 durch sieben teilbar ist, ist das die gesuchte Darstellung des ggT.

b) Berechnen Sie die Resultante der beiden Polynome $f = X^2 + \lambda$ und $g = X^2 - \lambda X + \lambda$ bezüglich X, und interpretieren Sie das Ergebnis!

Lösung: Die Resultante ist die Determinante

$$\begin{vmatrix} 1 & 0 & \lambda & 0 \\ 0 & 1 & 0 & \lambda \\ 1 & -\lambda & \lambda & 0 \\ 0 & 1 & -\lambda & \lambda \end{vmatrix} .$$

Subtraktion der vierten von der zweiten Zeile macht daraus

$$\begin{vmatrix} 1 & 0 & \lambda & 0 \\ 0 & 0 & \lambda & 0 \\ 1 & -\lambda & \lambda & 0 \\ 0 & 1 & -\lambda & \lambda \end{vmatrix} ,$$

und durch Subtraktion der zweiten Zeile von der ersten können wir dort auch noch das λ zum Verschwinden bringen. Somit stehen in der ersten und der zweiten Zeile jeweils nur noch ein Element; Entwicklung nach diesen Zeilen führt auf

$$\mathrm{Res}_X(f, g) = 1 \cdot (-\lambda) \cdot \begin{vmatrix} -\lambda & 0 \\ 1 & \lambda \end{vmatrix} = \lambda^3 \,.$$

Die Polynome haben also nur für $\lambda = 0$ einen gemeinsamen Faktor positiven Grades, was auch so klar war, da ein solcher Faktor die Differenz λX teilen muß, und für $\lambda \neq 0$ teilt X keines der beiden Polynome. Für $\lambda = 0$ ist natürlich $f = g = X^2$ der gemeinsame Faktor.

Aufgabe 2: (*7 Punkte*)

Geben Sie für jeden der folgenden Ringe an, ob er ein Integritätsbereich, Euklidisch und/oder faktoriell ist! Begründen Sie Ihre Antwort jeweils durch einen kurzen Verweis aus einen Satz oder eine Definition der Vorlesung oder zeigen Sie an einem Beispiel, daß der Ring die betrachtete Eigenschaft nicht haben kann:

a) $\mathbb{Z}$, *b)* $\mathbb{Z}[X]$ *c)* $(\mathbb{Z}/6)[X]$, *d)* $\mathbb{Q}[X]$ *e)* $\mathbb{Q}[X, Y]$ *f)* $\mathbb{Q}[X, Y]/(XY)$!

Lösung: Der Körper $\mathbb{Q}$ und damit auch sein Teilring $\mathbb{Z}$ sind Integritätsbereiche, und damit sind es nach einem Satz aus der Vorlesung auch alle Polynomringe darüber, also insbesondere $\mathbb{Z}[X]$ und $\mathbb{Q}[X,Y]$, Dagegen ist $\mathbb{Z}/6$ kein Integritätsbereich, denn $2 \cdot 3 = 0$, was natürlich auch in $(\mathbb{Z}/6)[X]$ gilt. Entsprechend ist $\mathbb{Q}[X,Y]/(XY)$ kein Integritätsbereich, denn das Produkt der Restklassen von X und Y verschwindet, obwohl keiner der Faktoren null ist. Da EUKLIDische und faktorielle Ringe nach Definition Integritätsbereiche sein müssen, sind $(\mathbb{Z}/6)[X]$ und $\mathbb{Q}[X,Y]/(XY)$ keines von beiden.

$\mathbb{Z}$ und $\mathbb{Q}[X]$ sind EUKLIDische Ringe, da wir in beiden eine Division mit Rest haben; als EUKLIDische Ringe sind sie insbesondere faktoriell.

$\mathbb{Z}[X]$ und $\mathbb{Q}[X,Y]$ sind nicht EUKLIDisch, denn sonst müßten sich die größten gemeinsamen Teiler linear kombinieren lassen, was weder für $1 = \mathrm{ggT}(2,X) \in \mathbb{Z}[X]$ noch für $1 = \mathrm{ggT}(X,Y) \in \mathbb{Q}[X,Y]$ der Fall ist. Beide sind aber faktoriell, da nach GAUSS jeder Polynomring über einem faktoriellen Ring selbst faktoriell ist.

Aufgabe 3: (*6 Punkte*)

Wir betrachten das Polynom $f = X^2Y^2 + XY^3 + X^2Y + X^3 \in \mathbb{Z}[X,Y]$.

a) Schreiben Sie f als Polynom aus $\mathbb{Z}[X][Y]$ bzw. $\mathbb{Z}[Y][X]$ und geben Sie jeweils den Inhalt und den primitiven Anteil an!

Lösung: $f = XY^3 + X^2Y^2 + X^2Y + X^3 \in \mathbb{Z}[X][Y]$ hat den Inhalt X, da X alle Koeffizienten teilt und der Koeffizient von Y^3 gleich X ist, so daß der Inhalt nicht größer sein kann. Der primitive Anteil in $\mathbb{Z}[X][Y]$ ist $f^* = Y^3 + XY^2 + XY + X^2$.

In $\mathbb{Z}[Y][X]$ hat $f = X^3 + (Y^2+Y)X^2 + Y^3X$ den Inhalt eins, da der Koeffizient von X^3 gleich eins ist. Somit ist f hier ein primitives Polynom.

b) Bestimmen Sie die führenden Terme von f bezüglich der lexikographischen und der graduiert-lexikographischen Ordnung sowohl für den Fall $X > Y$ als auch für $Y > X$!

Lösung: Zunächst sei $X > Y$. Dann ist bezüglich der lexikographischen Ordnung der führende Term der mit der höchsten X-Potenz, also X^3. Bezüglich der graduiert-lexikographischen Ordnung müssen wir die Terme höchsten Grades betrachten, also X^2Y^2 und XY^3; der führende Term ist wegen des höheren X-Grads X^2Y^2.

Nun sei $Y > X$. Dann ist bezüglich der lexikographischen Ordnung der führende Term der mit der höchsten Y-Potenz, also XY^3, und auch bezüglich der graduiert-lexikographischen Ordnung ist nun wegen des höheren Y-Grads XY^3 der führende Term.

c) Gibt es eine Monomordnung, bezüglich derer X^2Y das führende Monom ist?

Lösung: *Nein,* denn da X^2Y ein Teiler von X^2Y^2 ist, muß X^2Y bezüglich jeder Monomordnung kleiner als X^2Y^2 sein.

d) Ist f irreduzibel?

Lösung: *Nein,* denn wie wir in *a)* gesehen haben, ist X ein nichttrivialer Faktor.

Aufgabe 4: (*18 Punkte*)

Wir arbeiten mit der lexikographischen Ordnung (mit $X > Y$) im Polynomring $\mathbb{Q}[X,Y]$ und betrachten dort das Ideal $I = (f,g)$ mit

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

a) Zeigen Sie, daß f und g keine GRÖBNER-Basis von I sind.

Lösung: Ausmultipliziert ist $f = X^2 - 2X + 2Y^2 - 4Y$ und $g = X^2 - 2X - Y^2$; der führende Term ist in beiden Fällen X^2, und somit ist $S(f,g) = f - g = 3Y^2 - 4Y$. Wenden wir darauf den Divisionsalgorithmus an, müssen offensichtlich alle Terme in den Rest, denn f und g haben führenden Term X^2, und kein Term von $S(f,g)$ ist dadurch teilbar. Also können f und g nach BUCHBERGERS Kriterium keine Gröbnerbasis bilden.

b) Zeigen Sie, daß g und $f - g$ eine GRÖBNER-Basis bilden!

Lösung: Der führende Term von $f - g = 3Y^2 - 4Y$ ist $3Y^2$, der von g weiterhin X^2; also ist

$$S(g, f-g) = Y^2 g - \frac{X^2}{3}(f-g) = (X^2Y^2 - 2XY^2 - Y^4) - X^2Y^2 + \frac{4}{3}X^2Y = \frac{4}{3}X^2Y - 2XY^2 - Y^4 \,.$$

Das müssen wir mit dem Divisionsalgorithmus durch g und $f-g$ dividieren. Der führende Term $\frac{4}{3}X^2Y$ ist durch den führenden Term X^2 von g teilbar; Subtraktion von $\frac{4}{3}Yg$ läßt

$$-2XY^2 - Y^4 + \frac{8}{3}XY + \frac{4}{3}Y^3$$

übrig. Der führende Term davon ist $-2XY^2$; er ist durch den führenden Term $3Y^2$ von $f-g$ teilbar. Addition von $\frac{2}{3}X(f-g)$ führt zu

$$-Y^4 + \frac{4}{3}Y^3 = -\frac{1}{3}(f-g)\,.$$

Somit ist $S(g, f-g)$ modulo g und $f-g$ auf Null reduzierbar; nach BUCHBERGERS Kriterium haben wir also eine GRÖBNER-Basis.

c) Zeigen Sie ohne weitere Rechnung: Wenn g und $f-g$ eine GRÖBNER-Basis von I bilden, gilt dasselbe für f und $f-g$.

Lösung: Nach Definition ist eine Menge GRÖBNER-Basis eines Ideals I, wenn ihre führenden Monome das Ideal der führenden Monome von I erzeugen. Da f und g beide den führenden Term X^2 haben, erzeugen die führenden Monome in beiden Fällen das gleiche Ideal (X^2, Y^2).

d) Geben Sie eine reduzierte GRÖBNER-Basis von I an!

Lösung: Zunächst müssen die Elemente der vorhandenen GRÖBNER-Basis auf führenden Koeffizienten eins normiert werden. Bei g ist das bereits der Fall; $f-g$ muß durch drei dividiert werden. Die entstehende Basis aus

$$X^2 - 2X - Y^2 \quad \text{und} \quad Y^2 - \frac{4}{3}Y$$

ist minimal, da keiner der beiden führenden Terme den anderen teilt, aber noch nicht reduziert, da der führende Term Y^2 des zweiten Basiselement im ersten vorkommt. Wir müssen dieses daher ersetzen durch seine Summe mit dem zweiten und erhalten die neue, reduzierte Basis aus

$$X^2 - 2X - \frac{4}{3}Y \quad \text{und} \quad Y^2 - \frac{4}{3}Y\,.$$

e) Auf welche reduzierte GRÖBNER-Basis hätte die Basis aus f und $f-g$ geführt?

Lösung: Da die reduzierte GRÖBNER-Basis eines Ideals bei vorgegebener Monomordnung eindeutig ist, auf dieselbe.

f) Bestimmen Sie die Nullstellenmenge $V(I)$!

Lösung: Das zweite Basispolynom $Y^2 - \frac{4}{3}Y = Y(Y - \frac{4}{3})$ verschwindet für $Y = 0$ und $Y = \frac{4}{3}$. Setzen wir im ersten Basispolynom $Y = 0$, erhalten wir $X^2 - 2X = X(X-2) = 0$; also liegen $(0,0)$ und $(2,0)$ in $V(I)$.
Einsetzen von $Y = \frac{4}{3}$ führt auf das Polynom

$$X^2 - 2X - \frac{16}{9} = (X-1)^2 - \frac{25}{9};$$

es verschwindet für $x = 1 \pm \frac{5}{3}$, so daß wir die weiteren Nullstellen $(\frac{8}{3}, \frac{4}{3})$ und $(-\frac{2}{3}, \frac{4}{3})$ erhalten. Somit ist

$$V(I) = \left\{ (0,0), (0,2), \left(\frac{8}{3}, \frac{4}{3}\right), \left(-\frac{2}{3}, \frac{4}{3}\right) \right\}.$$

g) Interpretieren Sie das Ergebnis geometrisch!

Lösung: Die Nullstellenmenge von f ist eine Ellipse, die von g eine Hyperbel; die beiden Kurven schneiden sich in den vier berechneten Punkten.

Aufgabe 5: (*12 Punkte*)
Gegeben seien die beiden Polynome

$$f = 3X^3 + 2X^2 - X + 1 \quad \text{und} \quad g = X^2 + 2X + 2$$

aus $\mathbb{Z}[X]$; für jede Primzahl p seien $f^{(p)}, g^{(p)} \in \mathbb{F}_p[X]$ die entsprechenden Polynome mit Koeffizienten modulo p.

a) Geben Sie eine obere Schranke an für den Betrag von $\mathrm{Res}_X(f,g)$!

Lösung: Die Resultante ist die Determinante einer 5×5-Matrix, deren erste beiden Zeilen Koeffizienten von f enthalten; ihr Betrag ist höchstens drei. Dann kommen drei Zeilen mit Koeffizienten von g; ihr Betrag ist höchstens zwei. Daher ist der Betrag der Determinante nach dem LAPLACEschen Entwicklungssatz höchstens gleich $5! \cdot 3^2 \cdot 2^3 = 120 \cdot 9 \cdot 8 = 8640$.

b) Für welche Primzahlen können Sie sicher sein, daß $\mathrm{Res}_X(f,g) \bmod p = \mathrm{Res}_X(f^{(p)}, g^{(p)})$?

Lösung: Das gilt auf jeden Fall modulo aller Primzahlen, die keinen der beiden führenden Koeffizienten teilen, also für alle außer der Drei. (Anders als bei der modularen ggT-Berechnung reicht hier nicht, daß die Primzahl nicht *beide* führenden Koeffizienten teilt; auch wenn sie nur einen teilt, ändert sich schon die Größe der SYLVESTER-Matrix.)

c) Tatsächlich ist der Betrag der Resultante von f und g kleiner als hundert, und wie man nachrechnen kann (aber nicht muß), ist $\mathrm{Res}_X(f^{(59)}, g^{(59)}) = 6$ und $\mathrm{Res}_X(f^{(61)}, g^{(61)}) = 4$. Berechnen Sie $\mathrm{Res}_X(f,g)$!

Lösung: Nach *b)* und den hier gegebenen Informationen ist $\mathrm{Res}_X(f,g) \equiv 6 \bmod 59$ und $\mathrm{Res}_X(f,g) \equiv 4 \bmod 61$. 59 und 61 sind teilerfremd; also können wir den chinesischen Restesatz anwenden, um $\mathrm{Res}_X(f,g) \bmod (59{\cdot}61)$ zu berechnen. Der erweiterte EUKLIDische Algorithmus zeigt, daß

$$2 = 61 - 59 \quad \text{und} \quad 1 = 59 - 29 \cdot 2 = 59 - 29 \cdot (61 - 59) = 30 \cdot 59 - 29 \cdot 61$$

ist. Somit ist

$$30 \cdot 59 = 1770 \equiv \begin{cases} 0 & \bmod 59 \\ 1 & \bmod 61 \end{cases} \quad \text{und} \quad -29 \cdot 61 = -1769 \equiv \begin{cases} 1 & \bmod 59 \\ 0 & \bmod 61 \end{cases}.$$

Daher ist $\mathrm{Res}_X(f,g) \equiv 1770 \cdot 4 - 1769 \cdot 6 = -3534 \bmod 59 \cdot 61 = 3599$. Da die Resultante höchstens Betrag hundert hat, folgt $\mathrm{Res}_X(f,g) = -3534 + 3599 = 65$.

d) Für welche Primzahlen p haben $f^{(p)}$ und $g^{(p)}$ einen gemeinsamen Faktor?

Lösung: $65 = 5 \cdot 13$; da beide Primzahlen keinen der führenden Koeffizienten teilen, ist also $\mathrm{Res}(f^{(5)}, g^{(5)}) = 0$ in $\mathbb{F}_5$ und $\mathrm{Res}(f^{(13)}, g^{(13)}) = 0$ in $\mathbb{F}_{13}$. Über den Fall $p = 3$ sagt uns die berechnete Resultante nichts; hier müssen wir uns die Polynome direkt anschauen:

$$f^{(3)} = 2X^2 + 2X + 1 \quad \text{und} \quad g^{(3)} = X^2 + 2X + 2$$

haben die Summe X; jeder gemeinsame Teiler, muß also auch X teilen. Da X weder f noch g teilt, gibt es keinen echten gemeinsamen Teiler.

Aufgabe 6: *(8 Punkte)*

a) Schreiben Sie das Polynom $f = X^4 + X^2 + 1 \in \mathbb{F}_2[X]$ als Produkt zweier nichttrivialer Faktoren!

Lösung: $X^4 + X^2 + 1 = (X^2 + X + 1)^2$, denn in $\mathbb{F}_p[X]$ ist $\left(\sum_{i=0}^{d} a_i X^i\right)^p = \sum_{i=0}^{d} a_i X^{ip}$.

b) Haben Sie damit die Zerlegung von f in irreduzible Faktoren gefunden?

Lösung: *Ja,* denn wäre X^2+X+1 nicht irreduzibel, müßte es einen linearen Faktor haben, d.h. also eine Nullstelle in $\mathbb{F}_2$. Das Polynom nimmt aber sowohl an der Stelle eins als auch an der Stelle null den Wert eins an.

c) Finden Sie einen Linearfaktor des Polynoms $g = X^4 + 2X^3 + 2X^2 + 1 \in \mathbb{F}_3[X]$!

Lösung: $g(0) = 1 \neq 0$, aber $g(1) = 1 + 2 + 2 + 1 = 0$. Also ist das Polynom durch $X - 1 = X + 2$ teilbar.

d) Zerlegen Sie g in seine irreduziblen Faktoren!

Lösung:

$$\begin{aligned}(X^4 + 2X^3 + 2X^2 + 1) : (X + 2) &= X^3 + 2X + 2 = X^2 + 2X + 2\\ 2X^2 + 1&\\ 2X \ \ + 1&\end{aligned}$$

Letzteres Polynom ist irreduzibel, denn sonst müßte es einen linearen Faktor, also eine Nullstelle in $\mathbb{F}_3$ haben. Seine Werte an den Stellen $0, 1, 2 \in \mathbb{F}_3$ sind aber $2, 2$ und 1. Somit ist $g = (X + 2)(X^3 + 2X + 2)$ die Zerlegung von g in irreduzible Faktoren in $\mathbb{F}_3[X]$.

e) Zeigen Sie, daß das Polynom $h = X^4 - 4X^3 + 5X^2 + 6X + 7 \in \mathbb{Z}[X]$ irreduzibel ist!

Lösung: Offensichtlich ist $h^{(2)} = f$ und $h^{(3)} = g$. Hätte h einen echten irreduziblen Faktor $k \in \mathbb{Z}[X]$ vom Grad $d > 0$, so wäre $k^{(2)}$ ein Faktor von f und $k^{(3)}$ einer von g. Da h den führenden Koeffizienten eins hat, hätten $k^{(2)}$ und $k^{(3)}$ den gleichen Grad wie k. Für $k^{(2)}$ ist aber nur Grad zwei möglich, und für $k^{(3)}$ nur Grad eins oder drei. Beides gleichzeitig geht nicht.

Abgabe bis zum Samstag, dem 13. Dezember 2014, um 13.00 Uhr