Wolfgang K. Seiler
Tel. 2515

B6,26, A4.18

15. September 2020

Modulklausur Computeralgebra

Aufgabe 1: (*13 Punkte*)

a) Bestimmen Sie für jedes $x \in \mathbb{F}_7 \setminus \{0\}$ das Element x^{-1}! *(Hinweis: Das ist mit sehr geringem Rechenaufwand möglich.)*

Lösung: 1 und $-1 = 6$ sind zu sich selbst invers, und das sind die beiden einzigen Elemente mit dieser Eigenschaft, da das Polynom $X^2 - 1$ nicht mehr als zwei Nullstellen haben kann. Da $2 \cdot 4 = 8 \equiv 1 \bmod 7$, sind 2 und 4 invers zueinander; daher müssen auch die beiden verbleibenden Elemente 3 und 5 zueinander invers sein. In der Tat ist $3 \cdot 5 = 15 \equiv 1 \bmod 7$.

b) Bestimmen Sie die Inhalte und primitiven Anteile von $f = 6X^4 - 12X^2 - 18X - 12$ und $g = 20X^3 - 50X^2 + 50X - 60$!

Lösung: Da alle Koeffizienten von f durch sechs teilbar sind und X^4 den Koeffizienten sechs hat, ist der Inhalt von f gleich sechs. Der Inhalt von g ist der ggT von 20, 50 und 60, also zehn. Die primitiven Anteile sind dementsprechend $f^* = \frac{1}{6}f = X^4 - 2X^2 - 3X - 2$ und $g^* = \frac{1}{10}g = 2X^3 - 5X^2 + 5X - 6$.

c) Bestimmen Sie den ggT mit führendem Koeffizienten eins von f mod 3 und g mod 3!

Lösung: Da alle Koeffizienten von f durch drei teilbar sind, ist $f \bmod 3 = 0$, d.h. der ggT ist $g \bmod 3$. Da g allerdings den führenden Koeffizienten zwanzig hat, müssen wir $g \bmod 3$ noch durch zwanzig dividieren (oder g^* durch zwei) und erhalten $X^3 + 2X^2 + 2X$ als den ggT mit führendem Koeffizienten eins in $\mathbb{F}_3[X]$.

d) Bestimmen Sie den ggT mit führendem Koeffizienten eins von f mod 7 und g mod 7!

Lösung: $f \bmod 7 = 6X^4 + 2X^2 + 3X + 2$ und $g \bmod 7 = 6X^3 + 6X^2 + X + 3$. Da $6 \equiv -1 \bmod 7$ ist, können wir die Anwendung des Euklidischen Algorithmus vereinfachen, wenn wir zu $-f \bmod 7 = X^4 + 5X^2 + 4X + 5$ und $-g \bmod 7 = X^3 + X^2 + 6X + 4$ übergehen.

$$(X^4 + 5X^2 + 4X + 5) : (X^3 + X^2 + 6X + 2) = X + 6 \text{ Rest } 6X + 2$$
$$(X^3 + X^2 + 6X + 2) : (6X + 2) = 6X^2 + 4X + 2 \text{ Rest } 0$$

Somit ist $6X + 2$ ein ggT; um den mit führendem Koeffizienten eins zu bekommen, müssen wir mit sechs multiplizieren und erhalten $X + 5$.

e) Was können Sie auf Grund der bisherigen Ergebnisse *sicher* über den Grad des ggT von f und g in $\mathbb{Z}[X]$ aussagen?

Lösung: Weder fünf noch sieben teilen beide führenden Koeffizienten; daher ist der Grad des gesuchten ggT höchstens gleich dem des modularen. Der ggT hat also höchstens den Grad eins; er könnte aber auch Grad Null haben.

f) Erraten Sie den ggT von f und g in $\mathbb{Q}[X]$, und beweisen Sie, daß Sie richtig geraten haben!

Lösung: Wenn der ggT linear ist, muß er modulo sieben kongruent zu $X+5$ sein. $X+5$ teilt allerdings keines der beiden Polynome, denn sonst müßte der konstante Koeffizient jeweils durch fünf teilbar sein. Tatsächlich sind die konstanten Koeffizienten der primitiven Anteile -2 und -6; dies spricht eher für $X-2$ als ggT. Einsetzen zeigt, daß beide Polynome an der Stelle zwei verschwinden; daher ist der ggT in $\mathbb{Q}[X]$ gleich $X-2$.

g) Bestimmen Sie den ggT von f und g in $\mathbb{Z}[X]$!

Lösung: Jetzt müssen wir noch die Inhalte sechs und zehn der beiden Polynome betrachten; der ggT dieser beiden Zahlen ist zwei, so daß der ggT $2(X-2) = 2X-4$ ist.

Aufgabe 2: (*12 Punkte*)
Nun sei $f = 2X^3 - 9X^2 + 7X + 6$.

a) Für welche Primzahlen p können Sie *a priori* nicht ausschließen, daß der ggT von f und f' in $\mathbb{Z}[X]$ einen größeren Grad hat als der von $f \bmod p$ und $f' \bmod p$ in $\mathbb{F}_p[X]$?

Lösung: Wenn der ggT von f und f' einen größeren Grad hat als der von $f \bmod p$ und $f' \bmod p$, muß p den führenden Koeffizienten sowohl von f als auch von $f' = 6X^2 - 18X + 7$ teilen. Dies ist nur für $p = 2$ der Fall; hier kann der modulare ggT eventuell einen kleineren Grad haben als der ggT in $\mathbb{Z}[X]$.

b) Bestimmen Sie für jede dieser Primzahlen den ggT von $f \bmod p$ und $f' \bmod p$ in $\mathbb{F}_p[X]$!

Lösung: $f \bmod 2 = X^2 + 1$ und $f' \bmod 2 = 1$. Somit ist der ggT in $\mathbb{F}_2[X]$ gleich eins.

c) Zeigen Sie, ohne Informationen über die Nullstellen von f oder f' zu verwenden, daß f keine mehrfachen Nullstellen hat, und bestimmen Sie alle Primzahlen p, für die $f \bmod p$ und $f' \bmod p$ einen gemeinsamen Faktor positiven Grades haben!

Lösung: Dazu betrachtet man am einfachsten die Resultante von f und f':

$$\operatorname{Res}(f,f') = \begin{vmatrix} 2 & -9 & 7 & 6 & 0 \\ 0 & 2 & -9 & 7 & 6 \\ 6 & -18 & 7 & 0 & 0 \\ 0 & 6 & -18 & 7 & 0 \\ 0 & 0 & 6 & -18 & 7 \end{vmatrix} = 2\cdot \begin{vmatrix} 2 & -9 & 7 & 6 \\ -18 & 7 & 0 & 0 \\ 6 & -18 & 7 & 0 \\ 0 & 6 & -18 & 7 \end{vmatrix} + 6\cdot \begin{vmatrix} -9 & 7 & 6 & 0 \\ 2 & -9 & 7 & 6 \\ 6 & -18 & 7 & 0 \\ 0 & 6 & -18 & 7 \end{vmatrix}.$$

Die Determinante im ersten Summanden können wir zum Beispiel durch Entwicklung nach der zweiten Zeile berechnen; wir erhalten

$$18\cdot \begin{vmatrix} -9 & 7 & 6 \\ -18 & 7 & 0 \\ 6 & -18 & 7 \end{vmatrix} + 7\cdot \begin{vmatrix} 2 & 7 & 6 \\ 6 & 7 & 0 \\ 0 & -18 & 7 \end{vmatrix} = 18\cdot 2\,133 + 7\cdot(-844) = 32\,486\,.$$

Für die Determinante im zweiten Summanden können wir nach der letzten Spalte entwickeln:

$$6\cdot \begin{vmatrix} -9 & 7 & 6 \\ 6 & -18 & 7 \\ 0 & 6 & -18 \end{vmatrix} + 7\cdot \begin{vmatrix} -9 & 7 & 6 \\ 2 & -9 & 7 \\ 6 & -18 & 7 \end{vmatrix} = 6\cdot(-1\,566) + 7\cdot(-263) = -11\,237\,.$$

Die gesuchte Resultante ist somit $\operatorname{Res}_X(f,f') = 2\cdot 32\,486 - 7\cdot 11\,237 = -2\,450$. Da sie nicht verschwindet, sind f und f' in $\mathbb{Z}[X]$ teilerfremd. Die Primzerlegung von $2\,450$ ist $2\,450 = 2\cdot 5\cdot 245 = 2\cdot 5^2\cdot 49 = 2\cdot 5^2\cdot 7^2$, was modulo der Primzahlen $2, 5$ und 7 verschwindet. Zwei teilt allerdings die führenden Koeffizienten von f und f', so daß die Resultante von $f \bmod 2$ und $f' \bmod 2$ nicht gleich $-2\,450 \bmod 2 = 0$ sein muß, und wir

wissen ja auch bereits aus *b)*, daß $f \bmod 2$ und $f' \bmod 2$ teilerfremd sind. 5 und 7 teilen die führenden Koeffizienten nicht; daher haben $f \bmod p$ und $f' \bmod p$ genau modulo dieser beiden Primzahlen einen gemeinsamen Faktor positiven Grades.

d) Die Nullstellen von f sind $-\frac{1}{2}$, 2 und 3. Bestimmen Sie den ggT von $f \bmod p$ und $f' \bmod p$ für die in *c)* gefundenen Primzahlen!

Lösung: $f' \bmod 5 = X^2 + 2X + 2$, und in $\mathbb{F}_5$ ist $-\frac{1}{2} = 2$. Weiter ist dort $f'(2) = 0$ und $f'(3) = 2$; daher ist der ggT in $\mathbb{F}_5[X]$ gleich $X - 2 = X + 3$.
$f' \bmod 7 = 6X^2 + 3X$, und in $\mathbb{F}_7$ ist $-\frac{1}{2} = 3$, $f'(2) = 6$ und $f'(3) = 0$; in $\mathbb{F}_7[X]$ ist der ggT daher $X - 3 = X + 4$.
(Alternativ hätte man auch argumentieren können, daß modulo fünf die Zwei und modulo sieben die Drei eine doppelte Nullstelle von f ist.)

e) Bestimmen Sie die L^1-Norm, die L^2-Norm, die Höhe und das Maß von f!

Lösung: Die L^1-Norm eines Polynoms ist die Summe der Beträge der Koeffizienten, hier also gleich $2+9+7+6 = 24$. Die L^2-Norm ist die Wurzel aus den (Betrags-)Quadraten der Koeffizienten, also $\sqrt{4 + 81 + 49 + 36} = \sqrt{170} \approx 13{,}0384$. Die Höhe ist der größte Betrag eines Koeffizienten, also neun, und das Maß ist das Produkt der Beträge aller Nullstellen vom Betrag größer eins mal dem Betrag des führenden Koeffizienten, also $2 \cdot 3 \cdot 2 = 12$.

f) Bei welcher dieser vier Größen können Sie sicher sein, daß sie für keinen Teiler eines Polynoms größer ist als für das Polynom selbst?

Lösung: Nur beim Maß, denn jede Nullstelle eines Teilers ist auch Nullstelle des Polynoms, und der führende Koeffizient eines Teiler teilt den des Ausgangspolynoms.

Aufgabe 3: (*10 Punkte*)
Für das Polynom $f = X^4 + 2X^3 - 14X^2 - 36X - 16 \in \mathbb{Z}[X]$ ist $f \equiv g_0 h_0 \bmod 3$ mit $g_0 = X^2 + X + 1$ und $h_0 = X^2 + X - 1$.

a) Angenommen, es gibt Polynome $g, h \in \mathbb{Z}[X]$ mit $f = gh$, $g \equiv g_0 \bmod 3$ und $h \equiv h_0 \bmod 3$. Zeigen Sie, daß g und h dann quadratische Polynome mit führendem Koeffizient eins sind!

Lösung: Wegen der beiden Kongruenzen müssen g und h beide mindestens den Grad zwei haben; da $f = gh$ Grad vier hat, haben beide genau den Grad zwei. Das Produkt ihrer führenden Koeffizienten ist der führende Koeffizient eins von f. Daher sind entweder beide führenden Koeffizienten gleich eins oder beide gleich minus eins. Im letzteren Fall wären aber g und h modulo drei nicht kongruent zu g_0 und h_0, so daß nur die führenden Koeffizienten eins möglich sind.

b) Können Sie auch etwas über die konstanten Koeffizienten von g und h sagen?

Lösung: Offensichtlich muß ihr Produkt gleich dem konstanten Koeffizienten -16 von f sein. Außerdem ist der von g kongruent eins modulo drei, also $1, -2, 4, -8$ oder 16, und der von h ist kongruent minus eins, also $-1, 2, -4, 8$ oder -16.

c) Zeigen Sie, daß $g_0 \bmod 3$ und $h_0 \bmod 3$ teilerfremd sind, und stellen Sie die Eins in $\mathbb{F}_3[X]$ als Linearkombination von g_0 und h_0 dar! *(Hinweis: Betrachten Sie* $g_0 - h_0$ *!)*

Lösung: $g_0 - h_0 = 2$, und jeder gemeinsame Teiler von g_0 und h_0 muß auch diese Differenz teilen. Da diese in $\mathbb{F}_3[X]$ eine Einheit ist, sind $g_0 \bmod 3$ und $h_0 \bmod 3$ teilerfremd. Das Inverse zur Zwei in $\mathbb{F}_3$ ist sie selbst, so daß $1 \equiv 2g_0 - 2h_0 \equiv 2g_0 + h_0 \bmod 3$ ist.

d) Finden Sie Polynome $\widetilde{g}, \widetilde{h} \in \mathbb{Z}[X]$ mit führendem Koeffizienten eins derart, daß $\widetilde{g} \equiv g_0$ und $\widetilde{h} \equiv h_0 \bmod 3$ ist und $f \equiv \widetilde{g}\widetilde{h} \bmod 9$!

Lösung: Da die Polynome modulo drei teilerfremd sind, können wir das HENSELsche Lemma anwenden. Da die gesuchten Polynome den führenden Koeffizienten eins haben sollen und modulo drei gleich g_0, h_0 sein sollen, haben Sie die Form g_0+3g_1 und h_0+3h_1, wobei $g1, h_1$ Polynome vom Grad höchstens eins sind derart, daß

$$(g_0 + 3g_1)(h_0 + 3h_1) = g_0h_0 + 3(g_1h_0 + h_1g_0) + 9g_1h_1 \equiv f \bmod 9$$

ist. Dies ist äquivalent zur Kongruenz $f - g_0h_0 \equiv 3(g_1h_0 + h_1g_0) \bmod 9$.
Da $f - g_0h_0 = -15X^2 - 36X - 15$ (natürlich) durch drei teilbar ist, ist dies wiederum äquivalent zur Kongruenz $-5X^2-12X-5 \equiv g_1h_0+h_1g_0 \bmod 3$ oder, einfacher geschrieben,

$$X^2 + 1 \equiv g_1h_0 + h_1g_0 \bmod 3\,.$$

Wie wir in *c)* gesehen haben, ist $2g_0 + h_0 \equiv 1 \bmod 3$; Multiplikation mit $X^2 + 1$ macht daraus $(2X^2 + 2)g_0 + (X^2 + 1)h_0 \equiv X^2 + 1 \bmod 3$.
Damit haben wir aber g_1 und h_1 noch nicht gefunden, denn wir wollen ja höchstens lineare Polynome, um die führenden Koeffizienten eins zu erhalten. Diese erhalten wir, indem wir ein geeignetes Vielfaches der Gleichung $h_0g_0 - g_0h_0 = 0$ addieren. Hier reicht es schon, diese Gleichung selbst zu addieren; dies führt zu $(X + 1)g_0 - Xh_0 \equiv X^2 + 1 \bmod 3$. Somit können wir $g_1 = -X$ und $h_1 = X + 1$ setzen. Damit ist

$$\widetilde{g} = g_0 + 3g_1 = X^2 - 2X + 1 \quad \text{und} \quad \widetilde{h} = h_0 + 3h_1 = X^2 + 4X + 2\,.$$

In der Tat ist $\widetilde{g}\widetilde{h} = X^4 + 2X^3 - 5X^2 + 2$, und das unterscheidet sich um das durch neun teilbare Polynom $-9X^2 - 36X - 18$ von f, so daß $f \equiv \widetilde{g}\widetilde{h} \bmod 9$ ist.

e) Angenommen, $f = gh$ wie in *b)* und $g \equiv \widetilde{g} \bmod 9$ sowie $h \equiv \widetilde{h} \bmod 9$. Was können Sie jetzt über die konstanten Koeffizienten von g und h sagen?

Lösung: Das Produkt muß natürlich immer noch -16 sein, aber jetzt muß der von g kongruent eins modulo neun sein und der von h kongruent zwei. Da beide Teiler von -16 sind, kommt für g nur -8 und für h nur 2 in Frage.

f) Finden Sie quadratische Polynome $g, h \in \mathbb{Z}[X]$ mit $f = gh$ und $g \equiv \widetilde{g} \bmod 9$ sowie $h \equiv \widetilde{h} \bmod 9$!

Lösung: Wenn es solche Polynome gibt, haben Sie nach dem, was wir bereits wissen, die Form $g = X^2 + aX - 8$ und $h = X^2 + bX + 2$ mit $a \equiv -2 \bmod 9$ und $b \equiv 4 \bmod 9$. Schon der Versuch mit $a = -2$ und $b = 4$ führt auf das Produkt f.

Aufgabe 4: (*10 Punkte*)

a) Wann bezeichnet man eine Teilmenge I eines (kommutativen) Rings R als ein Ideal von R?

Lösung: Eine Teilmenge I eines Rings R heißt ein *Ideal* von R, wenn sie nicht leer ist, mit je zwei Elementen auch deren Summe enthält, und wenn für ein Element $g \in I$ für jedes $f \in R$ das Produkt fg in I liegt.

b) Zeigen Sie oder widerlegen Sie durch ein Gegenbeispiel, daß für zwei Ideale I und J von R auch deren Vereinigung ein Ideal von R ist!

Lösung: Die Vereinigung muß kein Ideal sein; beispielsweise bilden in $\mathbb{Z}$ sowohl die geraden Zahlen als auch die Dreierzahlen ein Ideal, aber $2+3 = 5$ liegt nicht in der Vereinigung dieser beiden Ideale.

c) Zeigen Sie oder widerlegen Sie durch ein Gegenbeispiel, daß für zwei Ideale I und J von R auch deren Durchschnitt ein Ideal von R ist!

Lösung: $I \cap J$ ist ein Ideal, denn als Ideale enthalten sowohl I als auch J die Null, so daß $I \cap J \neq \emptyset$ ist. Für zwei Elemente $f, g \in I \cap J$ liegen f und g sowohl in I als auch in J, also liegt auch $f + g$ sowohl in I als auch in J und damit in $I \cap J$. Für $g \in I \cap J$ und $f \in R$ liegt analog fg sowohl in I als auch in J, also in $I \cap J$.

d) Sind Kern und Bild eines Ringhomomorphismus $\varphi\colon R \to S$ Ideale von R *bzw.* S?

Lösung: Der Kern ist ein Ideal von R, denn $\varphi(0) = 0$, so daß er die Null enthält. Weiter ist für $f, g \in \operatorname{Kern}\varphi$ das Bild von $f+g$ gleich $\varphi(f+g) = \varphi(f)+\varphi(g) = 0+0 = 0$, so daß $f+g$ im Kern liegt. Für $f \in R$ und $g \in \operatorname{Kern}\varphi$ ist schließlich $\varphi(fg) = \varphi(f)\cdot\varphi(g) = \varphi(f)\cdot 0 = 0$, so daß auch fg im Kern liegt.
Das Bild von φ muß aber kein Ideal von S sei; beispielsweise ist die Einbettung von $\mathbb{Z}$ in $\mathbb{Q}$ ein Ringhomomorphismus, aber ihr Bild, die ganzen Zahlen in $\mathbb{Q}$, ist kein Ideal.

e) Wie ist das Radikal eines Ideals definiert, und warum ist es ein Ideal?

Lösung: Das Radikal $\sqrt{I}$ eines Ideals I eines Rings R besteht aus allen Elementen $f \in R$, für die eine Potenz f^n mit $n \in \mathbb{N}$ in I liegt. Es ist ein Ideal von R: Es enthält natürlich I, so daß es nicht leer ist. Für $f, g \in \sqrt{I}$ gibt es natürliche Zahlen n, m derart, daß f^n und g^m in I liegen. Dann ist

$$(f+g)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} f^i g^{n+m-i},$$

und hier liegen alle Summanden in I: Für $i \geq n$ ist $f^i \in I$, also auch $\binom{n+m}{i} f^i g^{n+m-i}$, und für $i < n$ ist $n+m-i > m$, so daß g^{n+m-i} in I liegt. Für $f \in R$ und $g \in I$ schließlich gibt es ein $m \in \mathbb{N}$, so daß $g^m \in I$; damit ist auch $(fg)^m = f^m \cdot g^m$ ein Element von I.

Aufgabe 5: (*25 Punkte*)

a) Welche Terme von $f = XY + X^2Y^2 + 2X^2Y + X^3Y + X^2$ kommen bezüglich irgendeiner Monomordnung auf $\mathbb{Q}[X, Y]$ als führende Terme in Frage? Geben Sie für jede dieser Möglichkeiten eine Monomordnung an, bezüglich derer der betreffende Term führend ist!

Lösung: Nur X^3Y und X^2Y^2 kommen in Frage, denn jedes andere Monom ist ein Teiler dieser beiden und daher bezüglich jeder Monomordnung kleiner als diese. X^3Y ist führender Term beispielsweise bezüglich der lexikographischen Ordnung mit $X > Y$, X^2Y^2 bezüglich derer mit $Y > X$.

b) Im folgenden verwenden wir die lexikographische Ordnung mit $X > Y$. Dividieren Sie f durch die beiden Polynome $f_1 = X^2Y + XY + X$ und $f_2 = XY^2 + XY + Y$!

Lösung: Der führende Term von f_1 ist X^2Y, der von f_2 ist XY^2. Der führende Term X^3Y von f ist durch X^2Y teilbar, also wird Xf_1 von f subtrahiert. Als Ergebnis erhalten wir die Differenz $X^2Y^2 + X^2Y + XY$. Wieder ist der führende Term durch X^2Y teilbar; also wird Yf_1 subtrahiert, was auf $X^2Y - XY^2$ führt. Der führende Term ist gleich dem von f_1, also wird dieses Polynom subtrahiert mit Ergebnis $-XY^2 - XY - X$. Jetzt ist der führende Term das Negative dessen von f_2; also wird f_2 addiert mit Ergebnis $-X + Y$. Keiner der verbleibenden Terme ist durch einen führenden Term von f_1 oder f_2 teilbar. Also ist $f = (X + Y + 1)f_1 + f_2 - X + Y$.

c) Können Sie damit entscheiden, ob f im Ideal $I = (f_1, f_2)$ des Polynomrings $\mathbb{Q}[X, Y]$ liegt?

Lösung: Da der Divisionsrest von Null verschieden ist, konnte nicht gezeigt werden, daß f im Ideal (f_1, f_2) liegt. Andererseits kann bei der Division durch eine Menge, die keine GRÖBNER-Basis ist, ein Divisionsrest ungleich Null auftreten, obwohl der Dividend im Ideal liegt. Wir können also keine sichere Aussage machen.

d) Dividieren Sie f nun durch f_2 und f_1 !

Lösung: $\mathrm{FM}(f)$ ist nur durch $\mathrm{FM}(f_1)$ teilbar; der erste Schritt ist also wie in *b)*. Der führende Term X^2Y^2 von $X^2Y^2 + X^2Y + XY$ ist aber auch durch $\mathrm{FM}(f_2)$ teilbar, also wird nun Xf_2 subtrahiert mit Ergebnis Null. Somit ist $f = X(f_1 + f_2)$ und liegt damit im Ideal (f_1, f_2).

e) Folgern Sie aus den bisherigen Ergebnissen, daß f_1 und f_2 keine GRÖBNER-Basis des Ideals (f_1, f_2) bezüglich der lexikographischen Ordnung bilden!

Lösung: Bei der Division durch die Elemente einer GRÖBNER-Basis ergibt jedes Element des Ideals unabhängig von der Anordnung der Elemente den Rest Null. Da dies in *b)* nicht der Fall war, können f_1 und f_2 keine GRÖBNER-Basis bilden.

f) Bestimmen Sie das S-Polynom $S(f_1, f_2)$ sowie seinen Divisionsrest f_3 bei der Division durch f_1, f_2 !

Lösung: $S(f_1, f_2) = Yf_1 - Xf_2 = -X^2Y + XY^2$. Der Divisionsalgorithmus addiert zunächst f_1 mit Ergebnis $XY^2 + XY + X$ und subtrahiert dann f_2, wobei $X - Y$ übrig bleibt. Dies läßt sich nicht weiter reduzieren, d.h. $f_3 = X - Y$.

g) Bestimmen Sie auch die S-Polynome $S(f_1, f_3)$ und $S(f_2, f_3)$ und dividieren Sie beide durch f_1, f_2, f_3. Zeigen Sie, daß eines der beiden Polynome auf Null reduziert werden kann, das andere aber nur auf einen Rest $f_4 \neq 0$.

Lösung: $S(f_1, f_3) = f_1 - XYf_3 = X^2Y + XY + X - X^2Y + XY^2 = XY^2 + XY + X$. Der führende Term XY^2 ist durch $\mathrm{FT}(f_3) = X$ teilbar; Subtraktion von XYf_3 führt auf $X^2Y + XY + X = f_1$, was durch Subtraktion von f_1 auf Null reduziert werden kann.
$S(f_2, f_3) = f_2 - Y^2f_3 = XY^2 + XY + Y - XY^2 + Y^3 = XY + Y^3 + Y$. Wieder ist der führende Term XY durch $\mathrm{FT}(f_3) = X$ teilbar; hier führt die Subtraktion von Yf_3 auf $Y^3 + Y^2 + Y$, was nicht weiter reduziert werden kann; denn die führenden Terme von f_1, f_2 und f_3 sind alle durch X teilbar. Somit bleibt $f_4 = Y^3 + Y^2 + Y$ übrig.

h) Was müßten Sie tun um zu beweisen, daß f_1, f_2, f_3 und f_4 eine GRÖBNER-Basis bilden?

Lösung: Wir müßten zeigen, daß $S(f_i, f_j)$ für jedes Paar (i, j) mit $1 \leq i < j \leq 4$ modulo f_1, f_2, f_3, f_4 auf Null reduziert werden können. (Tatsächlich müßten wir das „nur“ noch für die drei S-Polynome $S(f_i, f_4)$ mit $i \in \{1, 2, 3\}$ zeigen.) Wenn ja, folgt aus dem Satz von BUCHBERGER, daß wir eine GRÖBNER-Basis haben.

i) Tatsächlich bilden diese Polynome eine GRÖBNER-Basis. (Das müssen Sie nicht zeigen.) Bestimmen Sie die zugehörige reduzierte GRÖBNER-Basis, und entscheiden Sie, ob diese eine Form gemäß dem *Shape*-Lemma hat!

Lösung: Die führenden Monome von f_1 und f_2 sind durch $\mathrm{FM}(f_3) = X$ teilbar, so daß f_1 und f_2 gestrichen werden können. Kein Term von f_4 ist durch X teilbar, und kein Term von f_3 ist durch $\mathrm{FM}(f_4) = Y^3$ teilbar; damit bilden f_3 und f_4 eine reduzierte GRÖBNER-Basis. Sie hat eine Form gemäß dem *Shape*-Lemma, denn f_4 ist ein Polynom nur in Y, und $f_3 = X - Y$ hat die Form X minus Polynom in Y.

j) Zeigen Sie daß diese reduzierte Basis auch eine GRÖBNER-Basis von (f_1, f_2) bezüglich der graduiert-lexikographischen Ordnung mit $X > Y$ ist!

Lösung: Auch bezüglich dieser Ordnung ist $\mathrm{FM}(f_3) = X$ und $\mathrm{FM}(f_4) = Y^3$, und diese beiden Monome sind teilerfremd. Somit kann $S(f_3, f_4)$ modulo f_3, f_4 auf Null reduziert werden, so daß wir nach dem Satz von BUCHBERGER eine GRÖBNER-Basis haben.

k) Bestimmen Sie die Nullstellenmenge des Ideals (f_1, f_2) in $\mathbb{Q}^2$ und in $\mathbb{C}^2$!

Lösung: Wie wir inzwischen wissen, ist $(f_1, f_2) = (f_3, f_4)$. Falls ein Punkt (x, y) Nullstelle des Ideals ist, muß also $x = y$ sein und $y^3 + y^2 + y = y(y^2 + y + 1) = 0$. Somit ist $(0, 0)$ eine Nullstelle sowie alle Punkte (y, y) mit $y^2 + y + 1 = 0$. In $\mathbb{Q}$ hat diese quadratische Gleichung keine Lösung, so daß in $\mathbb{Q}^2$ die Nullstellenmenge nur aus $(0, 0)$ besteht. In $\mathbb{C}^2$ kommen noch die beiden Punkte (y, y) mit $y = -\frac{1}{2} \pm \frac{i}{2}\sqrt{3}$, d.h. die beiden primitiven dritten Einheitswurzeln, mit dazu.

l) Ist (f_1, f_2) ein Radikalideal?

Lösung: Ja, denn $\mathbb{Q}[X, Y]/(f_1, f_2) = \mathbb{Q}[X, Y]/(f_3, f_4)$ wird erzeugt von den Restklassen der Standardmonome. Bezüglich f_3 und f_4 sind das die drei Monome $1, Y$ und Y^2; die Dimension des Restklassenrings ist also drei. Da es in $\mathbb{C}^2$ genau drei Nullstellen gibt, sind alle Nullstellen einfach, und damit das Ideal ein Radikalideal.

Aufgabe 6: (*10 Punkte)*

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

a) $X^aY^bZ^c <_1 X^dY^eZ^f$ genau dann, wenn $a + b + c < d + e + f$ oder $a + b + c = d + e + f$ und entweder $a < d$ oder $a = d$ und $b < e$ oder $a = d$, $b = e$ und $c < f$

Lösung: Das ist gerade die graduiert-lexikographische Ordnung.

b) $X^aY^bZ^c <_2 X^dY^eZ^f$ genau dann, wenn $a+2b+3c < d+2e+3f$ oder $a+2b+3c = d+2e+3f$ und entweder $a < d$ oder $a = d$ und $b < e$ oder $a = d$, $b = e$ und $c < f$

Lösung: Auch das ist eine Monomordnung: Für zwei Monome ist $a+2b+3c$ größer, gleich oder kleiner als $d+2e+3f$. Nur im Falle der Gleichheit ist dann noch nicht entschieden, ob $X^aY^bZ^c$ größer, gleich oder kleiner $X^dY^eZ^f$ ist, aber dann entscheidet die lexikographische Ordnung, die bekanntlich eine Totalordnung ist.
Nun sein $X^aY^bZ^c <_2 X^dY^eZ^f$, und $X^uY^vZ^w$ sei ein weiteres Monom. Ist $a + 2b + 3c < d + 2e + 3f$, so ist auch $(a + u) + 2(b + v) + 3(c + w) < (d + u) + 2(e + v) + 3(f + w)$, also $X^uY^vZ^w \cdot X^aY^bZ^c <_2 X^uY^vZ^w \cdot X^dY^eZ^f$. Bei gleichen Exponentensummen haben auch die Produkte gleiche Exponentensummen, so daß nach der lexikographischen Ordnung entschieden wird, wonach zwischen den Produkten die gleiche Relation besteht wie zwischen den Ausgangsmonomen.
Die Wohlordnungseigenschaft ist klar, denn da $<$ eine Wohlordnung auf $\mathbb{N}_0$ ist, gibt es in jeder Menge von Monomen welche, für die $a+2b+3c$ minimal ist. Davon gibt es höchstens endlich viele, denn für jedes $n \in \mathbb{N}_0$ gibt es nur endlich viele Tripel $(a, b, c) \in \mathbb{N}_0^3$ mit $a+2b+3c = n$. In einer endlichen Menge gibt es aber bezüglich jeder Totalordnung stets ein kleinstes Element.

c) $X^aY^bZ^c <_3 X^dY^eZ^f$ genau dann, wenn $a+2b-3c < d+2e-3f$ oder $a+2b-3c = d+2e-3f$ und entweder $a < d$ oder $a = d$ und $b < e$ oder $a = d$, $b = e$ und $c < f$

Lösung: Das ist keine Monomordnung, denn $Z^n <_3 Z^m$ genau dann, wenn $n > m$ ist, Somit bilden die Monome $Z > Z^2 > Z^3 \cdots$ eine unendliche absteigende Folge, d.h. die Menge aller Z-Potenzen hat kein kleinstes Element.

d) $X^aY^bZ^c <_4 X^dY^eZ^f$ genau dann, wenn $a+2b+3c < d+2e+3f$ oder $a+2b+3c = d+2e+3f$ und entweder $a > d$ oder $a = d$ und $b > e$ oder $a = d$, $b = e$ und $c > f$

Lösung: Der einzige Unterschied zu *b)* ist, daß im Falle der Summengleichheit nun „lexikographisch größer“ statt „lexikographisch kleiner“ entscheidet. Mit dieser Veränderung

kann die Argumentation aus *b)* wörtlich übernommen werden, so daß auch $<_4$ eine Monomordnung definiert.

e) $X^aY^bZ^c <_5 X^dY^eZ^f$ genau dann, wenn $abc < def$ oder $abc = def$ und entweder $a < d$ oder $a = d$ und $b < e$ oder $a = d$, $b = e$ und $c < f$

Lösung: Das ist keine Monomordnung: Beispielsweise ist X größer als Y^2, da die Produkte der Exponenten in beiden Fällen Null sind und X lexikographisch größer als Y^2 ist. Multipliziert man aber beide Monome mit XYZ, so ist $X^2YZ <_5 XY^3Z$, denn links ist das Exponentenprodukt zwei, rechts aber drei.