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.)*

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

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

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

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

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

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

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 $\mathbb{F}_p[X]$?

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

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!

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!

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

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

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!

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

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 $g_0 - h_0$!)*

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 $f \equiv \widetilde{g}\widetilde{h} \bmod 9$!

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?

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

• • • B I T T E W E N D E N ! • • •

Aufgabe 4: (*10 Punkte*)

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

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!

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!

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

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

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!

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 $f_2 = XY^2 + XY + Y$!

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

d) Dividieren Sie f nun durch f_2 und f_1 !

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!

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

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 $f_4 \neq 0$.

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

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!

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!

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

l) Ist (f_1, f_2) 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 $c < f$

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 $c < f$

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 $c < f$

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 $c > f$

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 $c < f$

Abgabe bis zum Dienstag, dem 15. September 2020, um 10.00 Uhr