Wolfgang K. Seiler
Tel. 2515

B6,26, A4.18

13. Dezember 2011

Modulklausur Computeralgebra

Aufgabe 1: (*8 Punkte*)

Bestimmen Sie Real- und Imaginärteil einer komplexen Zahl mit

a) $z^2 = 1 + 2i$ *b)* $z^3 = 10 + 9\sqrt{-3}$

Lösung:

a) Sei $z = x + iy$. Dann ist $z^2 = (x^2 - y^2) + 2xy \cdot i$; somit müssen wir reelle Zahlen x, y finden mit $xy = 1$ und $x^2 - y^2 = 1$. Einsetzen von $y = 1/x$ in die zweite Gleichung führt auf

$$x^2 - \frac{1}{x^2} = 1 \quad \text{oder} \quad x^4 - x^2 - 1 = 0\,.$$

Dies ist eine quadratische Gleichung für x^2; in der gewohnten Weise löst man sie und erhält $x^2 = \frac{1}{2} \pm \frac{1}{2}\sqrt{5}$. Damit ist $y^2 = x^2 - 1 = -\frac{1}{2} \pm \frac{1}{2}\sqrt{5}$. Da wir reelle Lösungen x und y suchen, ist jeweils nur das positive Vorzeichen sinnvoll; somit ist

$$x = \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{5}} \quad \text{und} \quad y = \sqrt{-\frac{1}{2} + \frac{1}{2}\sqrt{5}}$$

eine Lösung.

b) Wir versuchen unser Glück mit einem Ansatz der Form $z = a + b\sqrt{-3}$ mit $a, b \in \mathbb{Z}$. Dann ist

$$z^3 = a^3 + 3a^2b\sqrt{-3} - 9ab^2 - 3b^3\sqrt{-3} = (a^3 - 9ab^2) + (3a^2b - 3b^3)\sqrt{-3}\,.$$

Wir suchen also ganze Zahlen a, b mit

$$a(a^2 - 9b^2) = 10 \quad \text{und} \quad b(a^2 - b^2) = 3\,.$$

Wegen der zweiten Gleichung kommen für $b \in \mathbb{Z}$ nur die Werte ± 1 und ± 3 in Frage; für $b = \pm 1$ muß $a^2 - 1 = \pm 3$ sein, was für $b = 1$ und $a = \pm 2$ erfüllbar ist. Einsetzen in die erste Gleichung führt auf $\pm 2(4-9) = 10$, was mit dem Minuszeichen auch tatsächlich gilt. Also ist $a = -2$ und $b = 1$ eine Lösung, d.h. $z = -2 + \sqrt{3} \cdot i$.

c) Wie können Sie daraus die sämtlichen Lösungen dieser Gleichungen bestimmen? (Eventuell notwendige Rechnungen müssen nicht durchgeführt werden.)

Lösung: Bei *a)* ist die zweite Lösung natürlich einfach $-z$; Real- und Imaginärteil sind also $-x$ und $-y$. Bei *b)* gibt es zwei weitere Lösungen, nämlich $z\rho$ und $z\bar{\rho}$, wobei ρ eine primitive dritte Einheitswurzel ist, d.h. ρ und $\bar{\rho}$ sind $-\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$.

Aufgabe 2: (*12 Punkte*)

a) Das Polynom $x^2 + ax + b$ mit $a, b \in \mathbb{Z}$ verschwinde für $x = \sqrt{3}$. Welche Möglichkeiten gibt es für a und b ?

Lösung: Bezeichnet x_2 die zweite Lösung, so sind nach dem Wurzelsatz von Viète sowohl $x_2\sqrt{3} = b$ als auch $x_2 + \sqrt{3} = -a$ ganze Zahlen. Daher muß $x_2 = \frac{b}{\sqrt{3}}$ ein ganzzahliges Vielfaches von $1/\sqrt{3}$ sein. Weiter muß auch

$$-a = \sqrt{3} + \frac{b}{\sqrt{3}} = \sqrt{3} + \frac{b}{2}\sqrt{3} = \left(1 + \frac{b}{3}\right)\sqrt{3}$$

eine ganze Zahl sein; das ist wegen der Irrationalität von $\sqrt{3}$ nur möglich, wenn die Klammer verschwindet, d.h. $b = -3$ und $a = 0$. Somit ist $x_2 = -\sqrt{3}$.

b) Das Polynom $f(x) = x^{12} + a_{11}x^{11} + \cdots + a_1x + a_0$ mit a_i aus $\mathbb{Z}$ habe zehn ganzzahlige Nullstellen; die elfte ist $\sqrt{3}$. Was ist die zwölfte?

Lösung: In der Faktorisierung von f führen die zehn ganzzahligen Nullstellen zu linearen Faktoren der Form $x - c_i$; da $\sqrt{3}$ wegen ihrer Irrationalität keine Nullstelle eines linearen Polynoms aus $\mathbb{Z}[x]$ sein kann, kommt zu diesen zehn linearen Faktoren noch ein quadratischer. Da f den führenden Koeffizienten eins hat, ist dieser von der Form $x^2 + ax + b$ mit $a, b \in \mathbb{Z}$ und hat $\sqrt{3}$ als Nullstelle. Wie wir in *a)* gesehen haben, ist dann $-\sqrt{3}$ die zweite Nullstelle dieses Faktors und damit auch die zwölfte Nullstelle von f.

c) Finden Sie die sämtlichen Nullstellen des Polynoms $g = x^4 + x^3 - 5x^2 - 3x + 6$!

Lösung: Nach VIÈTE ist das Produkt aller Nullstellen gleich sechs, also probieren wir die Teiler von sechs aus: $g(1) = 0, g(-1) = 4, g(2) = 4, g(-2) = 0, g(3) = 60, g(-3) = 24$. Da 1 und -2 Nullstellen sind, ist das Produkt der beiden verbleibenden gleich -3, ± 6 kommen somit nicht in Frage und müssen daher auch nicht getestet werden. Die beiden verbleibenden Nullstellen sind somit nicht ganzzahlig, haben des Produkt drei und ihre Summe ergibt zusammen mit 1 und -2 den Wert -1, ist also Null. Dies geht nur, wenn die noch fehlenden Nullstellen $\pm\sqrt{3}$ sind.

Aufgabe 3: (*10 Punkte*)

a) Stellen Sie den größten gemeinsamen Teiler von 299 und 247 als Linearkombination dieser Zahlen dar!

Lösung: Wir berechnen den ggT nach dem Erweiterten EUKLIDischen Algorithmus:

$$\begin{aligned}
299 : 247 &= 1 \text{ Rest } 52 &&\Longrightarrow 52 = 299 - 247\\
247;\ 52 &= 4 \text{ Rest } 39 &&\Longrightarrow 39 = 247 - 4(295 - 247) = 5 \cdot 247 - 4 \cdot 299\\
52 :\ 39 &= 1 \text{ Rest } 13 &&\Longrightarrow 13 = (299 - 247) - (5 \cdot 247 - 4 \cdot 299) = 5 \cdot 299 - 6 \cdot 247\\
39 :\ 13 &= 3 \text{ Rest } 0
\end{aligned}$$

Der ggT ist also $13 = 5 \cdot 299 - 6 \cdot 247$.

b) Beweisen Sie, daß es höchstens endlich viele Primzahlen p gibt, für die der ggT zweier Polynome $f, g \in \mathbb{Z}[X]$ einen anderen Grad hat als der ggT der beiden Polynome $f \bmod p$ und $g \bmod p$ in $\mathbb{F}_p[x]$!

Lösung: Der Grad des modularen ggT kann nur dann kleiner sein als der des ggT in $\mathbb{Z}[x]$, wenn letzterer einen durch p teilbaren führenden Koeffizienten hat. Dann müssen auch die führenden Koeffizienten sowohl von f als auch von g durch p teilbar sein; das ist für höchstens endlich viele Primzahlen der Fall.
Wenn der modulare ggT einen höheren Grad hat als $h = \mathrm{ggT}(f, g)$, sind zwar die Polynome f/h und $g/h \in \mathbb{Z}[x]$ teilerfremd, nicht aber ihre Reduktionen modulo p. Somit ist die Resultante von f/h und g/h zwar nicht Null, aber durch p teilbar. Da eine ganze Zahl ungleich Null höchstens endlich viele Primteiler hat, gibt es auch hier nur endlich viele Möglichkeiten.

c) Berechnen Sie für eine feste, aber beliebige ganze Zahl $a \in \mathbb{Z}$ die Resultante der beiden Polynome $f = 5x^5 + 4x^4 + 3x^3 + 2x^2 + x + a$ und $g = x$, und interpretieren Sie das Ergebnis!

Lösung: Da f den Grad fünf und g den Grad eins hat, stehen die Koeffizienten von f einmal und die von g fünfmal in den Zeilen der SYLVESTER-Matrix, die Resultante ist also

$$\begin{vmatrix} 5 & 4 & 3 & 2 & 1 & a \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{vmatrix} = -a \cdot \begin{vmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix} = -a\,,$$

wobei die Determinante hier nach der letzten Zeile entwickelt wurde. Das Ergebnis bedeutet, daß f und g nur für $a = 0$ einen gemeinsamen Faktor haben, was natürlich auch ohne Resultante klar war.

Aufgabe 4: (*15 Punkte*)

a) Die LANDAU-MIGNOTTE-Schranke des Polynoms $f \in \mathbb{Z}[x]$ sei M. Was bedeutet das für die Faktoren $g \in \mathbb{Z}[x]$ von f?

Lösung: Jeder Koeffizient eines Faktors $g \in \mathbb{Z}[x]$ von f hat höchstens den Betrag M.

b) Sei $f = x^4 - 2x^3 - 2x + 15$. Die irreduziblen Faktoren von f mod 23 in $\mathbb{F}_{23}[x]$ sind $x^2 + 19x + 5$ und $x^2 + 2x + 3$. Was können Sie bereits ohne jede Rechnung über die irreduziblen Faktoren von $f \in \mathbb{Z}[x]$ und ihre Grade aussagen?

Lösung: Da der führende Koeffizient eins von f nicht durch 23 teilbar ist, führt jeder Faktor von f zu einem Faktor desselben Grads von f mod 23. Daher ist f entweder irreduzibel oder das Produkt zweier quadratischer Polynome, die modulo 23 gleich den beiden angegebenen sind.

c) Die LANDAU-MIGNOTTE-Schranke von f ist knapp 245; faktorisieren Sie f in $\mathbb{Z}[x]$! Brauchen Sie dazu unbedingt das HENSELsche Lemma?

Lösung: Falls f Produkt zweier quadratischer Faktoren aus $\mathbb{Z}[x]$ ist, müssen diese beide den führenden Koeffizienten eins (oder beide -1) haben. Außerdem muß das Produkt ihrer konstanten Terme gleich 15 sein, und modulo 23 sind sie drei und fünf. Damit kommen nur drei und fünf in Frage. Somit ist

$$f = (x^2 + ax + 5)(x^2 + bx + 3) = x^4 + (a + b)x^3 + (8 + ab)x^2 + (3a + 5b)x + 15$$

mit $a \equiv 19 \bmod 23$ und $b \equiv 2 \bmod 23$. Der Koeffizient von x^2 zeigt, daß $ab = -8$ sein muß; somit ist $a = -4$ und $b = 2$. Einsetzen zeigt, daß dann auch alle anderen Koeffizienten den richtigen Wert haben; somit ist

$$f = (x^2 - 4x + 5)(x^2 + 2x + 3)\,.$$

d) Falls Sie bei *c)* das HENSELsche Lemma nicht benutzt haben: Welchen Ansatz würden Sie machen, um mit seiner Hilfe die Faktorisierung aus $\mathbb{F}_{23}[x]$ zu einer Faktorisierung modulo 23^2 hochzuheben? (Konkrete Rechnungen müssen nicht ausgeführt werden.)

Lösung: Der Ansatz wäre folgender: Wir setzen

$$g = x^2 + 19x + 5, \quad g_1 = g + 23\widetilde{g} \quad h = x^2 + 2x + 3 \quad \text{und} \quad h_1 = h + 23\widetilde{h}\,.$$

Dann multiplizieren wir gh aus und berechnen $f - gh$. Dies ist durch 23 teilbar, denn $f \equiv gh \bmod 23$. Wir dividieren durch 23 und erhalten eine Gleichung der Form

$$g\widetilde{h} + h\widetilde{g} \equiv \frac{f - gh}{23} \bmod 23\,.$$

Da g und h teilerfremd sind, können wir entsprechende Polynome $\widetilde{g}$ und $\widetilde{h}$ aus $\mathbb{F}_{23}[x]$ über den erweiterten EUKLIDischen Algorithmus bestimmen; ersetzen wir sie durch Repräsentanten aus $\mathbb{Z}[x]$, ist $f \equiv g_1 h_1 \bmod 23^2$.

Aufgabe 5: (*15 Punkte*)

a) Zeigen Sie, daß die Polynome $f = 4y - 2x - 3$ und $g = y^2 - 2y - 3$ bezüglich der lexikographischen Ordnung eine GRÖBNER-Basis des Ideals (f, g) in $\mathbb{Q}[x, y]$ bilden!

Lösung: Bezüglich der lexikographischen Ordnung ist der führende Term von f gleich $-2x$, der von g ist y^2. Das S-Polynom ist somit

$$S(f, g) = y^2 f + 2xg = 4y^3 - 3y^2 - 4xy - 6x$$

mit führendem Term $-4xy$. Dieses Polynom dividieren wir durch f und g nach dem Divisionsalgorithmus: Da der führende Term $-2x$ von f ein Teiler von $-4xy$ ist, subtrahieren wir als erstes $2yf = 4y^2 - 4xy - 6y$; wir erhalten $4y^3 - 11y^2 - 6x + 6y$ als neues Polynom. Sein führender Term $-6x$ ist das Dreifache dessen von f, also subtrahieren wir $3f$ und erhalten $4y^3 - 11y^2 - 6y + 9$. Nun haben wir ein Polynom, das nur noch von y abhängt; ab hier wird der Divisionsalgorithmus also zur gewöhnlichen Polynomdivision mir Rest in $\mathbb{Q}[y]$. Sie liefert das Ergebnis $4y - 3$ ohne Rest. Somit hat $S(f, g)$ bei der Division durch f, g den Rest Null; nach BUCHBERGERS Kriterium ist f, g daher eine GRÖBNER-Basis.

b) Machen Sie daraus eine reduzierte GRÖBNER-Basis!

Lösung: Von den führenden Termen von f und g teilt keiner den anderen; wir können also keines der beiden Polynome eliminieren. Außerdem ist kein Term von f durch den führenden Term y^2 von g teilbar und kein Term von g durch den führenden Term $-2x$ von f; die Polynome können also nicht weiter vereinfacht werden. Somit müssen wir nur die führenden Koeffizienten auf Eins normieren; die reduzierte GRÖBNER-Basis besteht also aus den beiden Polynomen

$$x - 2y + \frac{3}{2} \quad \text{und} \quad y^2 - 2y - 3\,.$$

c) Bestimmen Sie $\{(x, y) \in \mathbb{Q}^2 \mid f(x, y) = g(x, y) = 0\}$!

Lösung: $g = (y - 1)^2 - 4$ verschwindet für $y = 3$ und $y = -1$. Da auch f verschwinden soll, muß jeweils $x = 2y - \frac{3}{2}$ sein; die Lösungsmenge besteht also aus den beiden Punkten $\left(\frac{9}{2}, 3\right)$ und $\left(-\frac{7}{2}, -1\right)$.