Wolfgang K. Seiler
Tel. 2515

B6, B4.18

26. März 2020

6. Übungsblatt Computeralgebra

Aufgabe 1: *(4 Punkte)*

k sei ein Körper, und $f, g \in k[X]$ seien zwei Polynome. Zeigen Sie:

a) f und g sind genau dann teilerfremd, wenn es zwei Polynome $a, b \in k[X]$ gibt mit

$$af + bg = 1 \quad \text{und} \quad \deg a < \deg g\,.$$

Lösung: Natürlich sind f und g teilerfremd, wenn es solche Polynome gibt, denn jeder gemeinsame Teiler von f und g muß auch $af + bg = 1$ teilen.
Umgekehrt liefert der erweiterte Euklidische Algorithmus für zwei teilerfremde Polynome $f, g \in k[X]$ Polynome $u, v \in k[X]$ mit $uf + vg = 1$. Polynomdivision mit Rest liefert eine Darstellung $u = qg + r$ mit $q, r \in k[X]$ und $\deg r < \deg g$. Damit wird die Darstellung zu

$$(qg + r)f + vg = rf + qgf + vg = rf + (v - qf)g = 1\,.$$

Die Polynome $a = r$ und $b = v - qf$ erfüllen also die Bedingung.
(Tatsächlich ist auch $\deg b < \deg f$, denn sonst wäre $\deg bg \geq \deg f + \deg g$, während $\deg af = \deg r + \deg f$ echt kleiner als $\deg g + \deg f$ ist. Somit müßte $1 = af + bg$ einen Grad von mindestens $\deg f + \deg g$ haben, was absurd ist.)

b) In diesem Fall sind a und b eindeutig bestimmt.

Lösung: $af + bg = uf + vg = 1$ seien zwei Darstellungen mit sowohl $\deg a < \deg g$ als auch $\deg u < \deg g$. Dann ist $(a - u)f + (b - v)g = 0$, also ist $(a - u)f = (b - v)g$ ein gemeinsames Vielfaches von f und g. Wegen der Teilerfremdheit von f und g muß daher g ein Teiler von $a - u$ sein. Da die Grade von a und u beide kleiner als der Grad von g sind, ist das nur möglich, wenn $a - u$ das Nullpolynom ist, also $a = u$. Die Polynome

$$b = \frac{1 - af}{g} \quad \text{und} \quad v = \frac{1 - vf}{g}$$

sind durch a und u eindeutig festgelegt, müssen also auch übereinstimmen.

Aufgabe 2: *(9 Punkte)*

a) Bestimmen Sie in $\mathbb{Q}[X]$ den ggT der beiden Polynome $f = 2X^2+3X+5$ und $g = 3X^2+5X+7$, und stellen Sie ihn als Linearkombination dieser Polynome dar!

Lösung: Wir wenden den erweiterten Euklidischen Algorithmus an:
$f : g = \frac{2}{3}$ Rest $-\frac{1}{3}X + \frac{1}{3} = f - \frac{2}{3}g$
$g : (-\frac{1}{3}X + \frac{1}{3}) = -9X - 24$ Rest 15 und
$15 = g + (9X + 24)(-\frac{1}{3}X + \frac{1}{3}) = g + (9X + 24)(f - \frac{2}{3}g) = (9X + 24)f - (6X + 15)g$.

Da 15 eine Einheit von $\mathbb{Q}[X]$ ist, sagen wir besser, der ggT sei eins, und

$$1 = \frac{9X+24}{15}f - \frac{6X+15}{15} = \left(\frac{3}{5}X + \frac{8}{5}\right)f - \left(\frac{2}{5}X + 1\right)g\,.$$

b) Was ist der ggT h von f und g in $\mathbb{Z}[X]$?

Lösung: Da beide Polynome primitiv sind, bleiben sie auch in $\mathbb{Z}[X]$ teilerfremd, d.h. $h = 1$.

c) Zeigen Sie, daß es keine Polynome $a, b \in \mathbb{Z}[X]$ gibt, für die $af + bg = h$ ist!

Lösung: Angenommen, es gäbe Polynome a und b aus $\mathbb{Z}[X]$ mit $h = af + bg$. Dann wäre auch für jedes $n \in \mathbb{Z}$

$$a(n)f(n) + b(n)g(n) = h(n) = 1\,.$$

Speziell für $n = 1$ ist $f(n) = 2 + 3 + 5 = 10$ und $g(n) = 3 + 5 + 7 = 15$, also müßte

$$10a(n) + 15b(n) = 1$$

sein, was natürlich unmöglich ist.
(Bei der Suche nach einem geeigneten n muß man natürlich probieren; $n = 0$ oder $n = 2$ beispielsweise hätten nichts gebracht.)

d) Zeigen Sie, daß es auch keine Polynome $a, b \in \mathbb{Z}[X]$ gibt, für die $af + bg \equiv h \bmod 5$ ist!

Lösung: Falls $f \bmod 5$ und $g \bmod 5$ teilerfremd wären, gäbe es solche Polynome; wir müssen also zeigen, daß diese Polynome nicht teilerfremd sind. In $\mathbb{F}_5$ sind die führenden Koeffizienten natürlich Einheiten, und am ggT ändert sich nichts, wenn wir zu den normierten Polynomen übergehen – außer daß die Rechnung (zumindest von Hand) einfacher wird.
Da $2 \cdot 3 \equiv 1 \bmod 5$ ist, müssen wir dazu f mit drei und g mit zwei multiplizieren; die neuen Polynome sind also

$$3f \equiv X^2 + 4X = X(X+4) \equiv X(X-1) \bmod 5$$

und

$$2g \equiv X^2 + 4 \equiv X^2 - 1 = (X+1)(X-1) \bmod 5\,.$$

Auch ohne EUKLIDischen Algorithmus sehen wir, daß der ggT von $f \bmod 5$ und $g \bmod 5$ gleich $X - 1 \equiv X + 4 \bmod 5$ ist. Für alle Polynome $a, b \in \mathbb{Z}[X]$ ist somit $af + bg$ modulo fünf ein Vielfaches von $X - 1$, und das ist die Eins natürlich nicht.

e) Finden Sie Polynome $a, b \in \mathbb{Z}[X]$, für die $af + bg \equiv h \bmod 7$ ist!

Lösung: Die Rechnung ist die gleiche wie in *a),* nur daß wir die Brüche mit Nenner fünf nun noch weiter ausrechnen können. Modulo sieben ist $5 \cdot 3 \equiv 1$, also entspricht Division durch fünf modulo sieben der Multiplikation mit drei, und wir erhalten

$$a = \frac{3}{5}X + \frac{8}{5} = 2X + 3 \quad \text{und} \quad b = -\left(\frac{2}{5}X + 1\right) = X + 6$$

in $\mathbb{F}_7[X]$, das heißt

$$(2X+3)f + (X+6)g \equiv 1 \bmod 7\,.$$

f) Finden Sie Polynome $a, b \in \mathbb{Z}[X]$, für die $af + bg \equiv h \bmod 49$ ist!

Lösung: Wir machen den Ansatz $a = 2X + 3 + 7u$ und $b = X + 6 + 7v$ mit höchstens linearen Polynomen $u, v \in \mathbb{Z}[X]$. Dann ist

$$af + bg = (2X + 3)f + (X + 6)g + 7(uf + fg)\,.$$

Ausmultiplizieren zeigt, daß

$$af + bg = 7X^3 + 35X^2 + 56X + 57 = 1 + 7(X^3 + 5X^2 + 8X + 8)$$

ist; wenn $af + bg \equiv 1 \bmod 49$ sein soll, muß also

$$(X^3 + 5X^2 + 8X + 8) + uf + vg \equiv 0 \bmod 7$$

sein, das heißt

$$uf + vg \equiv -(X^3 + 5X^2 + 8X + 8) \equiv 6X^3 + 2X^2 + 6X + 6 \bmod 7\,.$$

Wie wir bereits wissen, ist

$$(2X + 3)f + (X + 6)g \equiv 1 \bmod 7\,;$$

Multiplikation mit $6X^3 + 2X^2 + 6X + 6$ führt auf

$$(5X^4 + X^3 + 4X^2 + 2X + 4)f + (6X^4 + 3X^3 + 4X^2 + 1)g \equiv 1 \bmod 7\,.$$

Wir haben also eine erste Lösung

$$u_1 = 5X^4 + X^3 + 4X^2 + 2X + 4 \quad \text{und} \quad v_1 = 6X^4 + 3X^3 + 4X^2 + 1\,,$$

aber die Grade sind natürlich noch viel zu hoch. Um sie zu reduzieren, dividieren wir u_1 mit Rest durch g und erhalten

$$u_1 = 5X^4 + X^3 + 4X^2 + 2X + 4 \equiv (4X^2 + 3X + 1)g + (4X + 4) \bmod 7\,.$$

Mit

$$u = u_1 - (4X^2 + 3X + 1)g \bmod 7 = 4X + 4$$

und

$$v = v_1 + (4X^2 + 3X + 1)f \bmod 7 = 6X + 4$$

haben wir somit eine lineare Lösung gefunden. Nach unserem Ansatz ist

$$a = (2X + 3) + 7u = 30X + 31 \quad \text{und} \quad b = (X + 6) + 7v = 29X + 48\,.$$

Nachrechnen zeigt, daß in der Tat $af + bg \equiv 1 \bmod 49$ gilt.

Aufgabe 3: *(4 Punkte)*

Welche der folgenden Mengen sind Ideale im Polynomring $\mathbb{Q}[X, Y, Z]$?

a) $\mathbb{Z}[X, Y, Z]$ *b)* $\mathbb{Q}[X]$ *c)* $\mathbb{Q}[X, Y, Z]$ *d)* $\{f \in \mathbb{Q}[X, Y, Z] \mid f(1, 2, 3) = 0\}$

e) $\left\{f = \sum_{i=0}^{d} a_i X^i \;\middle|\; d \in \mathbb{N}_0, a_i \in \mathbb{Z} \text{ und } \sum_{i=0}^{d} a_i \text{ gerade}\right\}$

Lösung: $\mathbb{Z}[X, Y, Z]$ ist kein Ideal, denn $\mathbb{Q}$ liegt in $\mathbb{Q}[X, Y, Z]$, und das Produkt eines ganzzahligen Polynoms mit einer beliebigen rationalen Zahl hat im Allgemeinen keine ganzzahligen Koeffizienten.

Genauso ist auch $\mathbb{Q}[X]$ kein Ideal in $\mathbb{Q}[X,Y,Z]$, denn wenn wir ein Polynom in X zum Beispiel mit Y multiplizieren, liegt das Produkt nicht mehr in $\mathbb{Q}[X]$.

Der ganze Ring ist natürlich ein Ideal; schließlich liegen alle Summen und Produkte dort.

Auch $\{f \in \mathbb{Q}[X,Y,Z] \mid f(1,2,3) = 0\}$ ist ein Ideal, denn das Nullpolynom erfüllt die Bedingung, und ist $f(1,2,3) = g(1,2,3) = 0$, so ist auch $(f+g)(1,2,3) = 0$. Ist schließlich $g(1,2,3) = 0$ und f beliebig, so ist auch $(fg)(1,2,3) = f(1,2,3)g(1,2,3) = 0$.

$\left\{f = \sum_{i=0}^{d} a_i X^i \;\middle|\; d \in \mathbb{N}_0, a_i \in \mathbb{Z} \text{ und } \sum_{i=0}^{d} a_i \text{ gerade}\right\}$ ist wie auch $\mathbb{Z}[X,Y,Z]$ kein Ideal, da die Multiplikation mit einer rationalen Zahl im Allgemeinen zu einem Polynom führt, das nicht mehr in dieser Menge liegt. (Sie ist aber ein Ideal in $\mathbb{Z}[X,Y,Z]$.)

Aufgabe 4: *(3 Punkte)*

Schreiben Sie das Polynom $f = X^3 + 2XYZ - Y^2Z$ um als ein Polynom in $X, Y-1$ und $Z+2$!

Lösung: Mit $U = Y - 1$ und $V = Z + 2$ ist $Y = U + 1$ und $Z = V - 2$, also

$$\begin{aligned} f &= X^3 + 2X(U+1)(V-2) - (U+1)^2(V-2) \\ &= X^3 + 2XUV - 4XU + 2XC - 4X - U^2V + 2U^2 - 2UV + 4U - V + 2 \\ &= X^3 + 2X(Y-1)(Z+2) - 4X(Y-1) + 2XC - 4X - (Y-1)^2(Z+2) \\ &\quad +2(Y-1)^2 - 2(Y-1)(Z+2) + 4(Y-1) - (Z+2) + 2 \end{aligned}$$