MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Dr. E. Schörner

SS 2013
Blatt 12
08.07.2013

Übungen zur Vorlesung „Grundlagen der Mathematik II“ — Lösungsvorschlag —

45. a) Wir betrachten die beiden Polynome

$$p = 2\,X^4 + 4\,X^3 + 3\,X^2 + 6\,X \quad \text{und} \quad q = 2\,X^3 + 3\,X \in \mathbb{R}[X].$$

- Für $p+q$ erhalten wir

$$\begin{aligned} p + q &= (2\,X^4 + 4\,X^3 + 3\,X^2 + 6\,X) + (2\,X^3 + 3\,X) = \\ &= 2\,X^4 + 6\,X^3 + 3\,X^2 + 9\,X. \end{aligned}$$

- Für $p-q$ erhalten wir

$$\begin{aligned} p - q &= (2\,X^4 + 4\,X^3 + 3\,X^2 + 6\,X) - (2\,X^3 + 3\,X) = \\ &= 2\,X^4 + 2\,X^3 + 3\,X^2 + 3\,X. \end{aligned}$$

- Für $p \cdot q$ erhalten wir

$$\begin{aligned} p \cdot q &= (2\,X^4 + 4\,X^3 + 3\,X^2 + 6\,X) \cdot (2\,X^3 + 3\,X) = \\ &= 4\,X^7 + 6\,X^5 + 8\,X^6 + 12\,X^4 + 6\,X^5 + 9\,X^3 + 12\,X^4 + 18\,X^2 = \\ &= 4\,X^7 + 8\,X^6 + 12\,X^5 + 24\,X^4 + 9\,X^3 + 18\,X^2. \end{aligned}$$

- Für $p : q$ erhalten wir

$$\begin{array}{rcl} p : q &=& (2\,X^4 + 4\,X^3 + 3\,X^2 + 6\,X) : (2\,X^3 + 3\,X) = X + 2 \\ && \underline{-(2\,X^4 + 3\,X^2)} \\ && 4\,X^3 + 6\,X \\ && \underline{-(4\,X^3 + 6\,X)} \\ && 0 \end{array}$$

b) Der euklidische Algorithmus ergibt für die Polynome $p = X^3 - 3\,X^2 + 5\,X - 3$ und $q = X^3 - 1 \in \mathbb{R}[X]$ als fortgesetzte Division mit Rest

$$\begin{aligned} X^3 - 3\,X^2 + 5\,X - 3 &= 1 \cdot (X^3 - 1) + \big(-3\,X^2 + 5\,X - 2\big) \\ X^3 - 1 &= (-\frac{1}{3}\,X - \frac{5}{9}) \cdot (-3\,X^2 + 5\,X - 23) + \\ &\qquad + \left(\frac{19}{9}\,X - \frac{19}{9}\right) \\ -3\,X^2 + 5\,X - 2 &= \left(-\frac{27}{19}\,X + \frac{18}{19}\right) \cdot \left(\frac{19}{9}\,X - \frac{19}{9}\right); \end{aligned}$$

damit ist $d = \frac{19}{9}\,X - \frac{19}{9} \in \mathrm{ggT}(p, q)$.

46. Das Polynom $p = X^5 - 3\,X^4 + 8\,X^3 - 14\,X^2 + 16\,X - 8 \in \mathbb{C}[X]$ besitzt wegen

$$f_p(1) = 1^5 - 3\cdot 1^4 + 8\cdot 1^3 - 14\cdot 1^2 + 16\cdot 1 - 8 = 0$$

die Nullstelle 1, und die Polynomdivision ergibt

$$\begin{array}{ll}
(X^5 - 3\,X^4 + 8\,X^3 - 14\,X^2 + 16\,X - 8) : (X-1) = & \\
\underline{-(X^5 - X^4)} & = X^4 - 2\,X^3 + 6\,X^2 - 8\,X + 8 \\
-2\,X^4 + 8\,X^3 - 14\,X^2 + 16\,X - 8 & \\
\underline{-(-2\,X^4 + 2\,X^3)} & \\
6\,X^3 - 14\,X^2 + 16\,X - 8 & \\
\underline{-(6\,X^3 - 6\,X^2)} & \\
-8\,X^2 + 16\,X - 8 & \\
\underline{-(-8\,X^2 + 8\,X)} & \\
8\,X - 8 & \\
\underline{-(8\,X - 8)} & \\
0, &
\end{array}$$

also $p = (X-1)\cdot s$ mit $s = X^4 - 2\,X^3 + 6\,X^2 - 8\,X + 8$. Wegen

$$f_s(2i) = (2i)^4 - 2\cdot(2i)^3 + 6\cdot(2i)^2 - 8\cdot(2i) + 8 = 16 + 16i - 24 - 16i + 8 = 0$$

besitzt s die Nullstelle $2i$ und folglich auch die Nullstelle $-2i$, und die Polynomdivision von s durch

$$(X-2i)(X+2i) = X^2 - (2i)^2 = X^2 - (-4) = X^2 + 4$$

liefert

$$\begin{array}{l}
(X^4 - 2\,X^3 + 6\,X^2 - 8\,X + 8) : (X^2 + 4) = X^2 - 2\,X + 2 \\
\underline{-(X^4 + 4\,X^2)} \\
-2\,X^3 + 2\,X^2 - 8\,X + 8 \\
\underline{-(-2\,X^3 - 8\,X)} \\
2\,X^2 + 8 \\
\underline{-(2\,X^2 + 8)} \\
0,
\end{array}$$

also $s = (X^2+4)\,(X^2 + 2\,X + 2)$ mit

$$X^2 - 2\,X + 2 = (X-1)^2 + 1 = (X - (1-i))\cdot(X - (1+i))\,.$$

Damit erhalten wir für das Polynom p die Faktorisierung

$$\begin{aligned}
p &= X^5 - 3\,X^4 + 8\,X^3 - 14\,X^2 + 16\,X - 8 \\
&= (X-1)\cdot\big(X^2+4\big)\cdot\big(X^2 + 2\,X + 2\big) \\
&= (X-1)\cdot(X-2\,i)\cdot(X+2\,i)\cdot(X-(1-i))\cdot(X-(1+i))\,.
\end{aligned}$$

Es ergeben sich für das Polynom p im Polynomring $\mathbb{C}[X]$ die fünf verschiedenen Nullstellen $1,\ 2\,i,\ -2\,i,\ 1-i,\ 1+i \in \mathbb{C}$.

Für $n \in \mathbb{N}$ betrachten wir das Polynom $q = X^n + X^{n-1} + \ldots + X^2 + X + 1 \in \mathbb{C}[X]$. Wegen

$$f_q(1) = 1^n + 1^{n-1} + \ldots + 1^2 + 1 + 1 = n + 1 \neq 0$$

ist $z = 1$ keine Nullstelle von q, und für alle $z \in \mathbb{C} \setminus \{1\}$ erhalten wir mit Hilfe der geometrischen Summenformel

$$f_q(z) = z^n + z^{n-1} + \ldots + z^2 + z + 1 = \sum_{j=0}^{n} z^j = \frac{z^{n+1} - 1}{z - 1};$$

damit ist $z \in \mathbb{C}$ genau dann eine Nullstelle von q, wenn $z \neq 1$ und $z^{n+1} = 1$ gilt. Die Polynomgleichung $z^{n+1} = 1$ besitzt genau die $n + 1$ verschiedenen Lösungen

$$z_k = E\left(k \cdot \frac{360°}{n+1}\right) \qquad \text{für} \quad k \in \{0, 1, \ldots, n\};$$

für $k = 0$ ist $z_0 = 1$, und damit ergeben sich für das Polynom q im Polynomring $\mathbb{C}[X]$ die n verschiedenen Nullstellen

$$E\left(k \cdot \frac{360°}{n+1}\right) \qquad \text{für} \quad k \in \{1, \ldots, n\}.$$

47. Sei $(K[X], +, \cdot)$ der Polynomring über dem Körper $(K, +, \cdot)$ sowie p, $q \in K[X]$ mit $q \neq 0$; dann gibt es eindeutig bestimmte r, $s \in K[X]$ mit

$$p = s \cdot q + r \qquad \text{und} \qquad \mathrm{Grad}(r) < \mathrm{Grad}(q).$$

Wir zeigen zunächst die Existenzbehauptung, indem wir für ein fest gewähltes

$$q = b_m X^m + b_{m-1} X^{m-1} + \ldots + b_1 X + b_0 \in K[X] \qquad \text{mit} \qquad b_m \neq 0$$

von $\mathrm{Grad}(q) = m \geq 0$ mit Hilfe vollständiger Induktion die Aussage

$A(n) =$ „Für alle $p \in K[X]$ mit $\mathrm{Grad}(p) < n$ gibt es
r, $s \in K[X]$ mit $p = s \cdot q + r$ und $\mathrm{Grad}(r) < \mathrm{Grad}(q)$.“

für alle $n \in \mathbb{N}_0$ mit $n \geq m$ nachweisen.

- Im Induktionsanfang „$n = m$“ ist $p \in K[X]$ mit $\mathrm{Grad}(p) < m$ zu betrachten, und wir können $s = 0$ und $r = p$ wählen; damit gilt $p = s \cdot q + r$ mit $\mathrm{Grad}(r) = \mathrm{Grad}(p) < m = \mathrm{Grad}(q)$.
- Im Induktionsschritt „$n \to n + 1$“ ist $p \in K[X]$ mit $\mathrm{Grad}(p) = n \geq m$ zu betrachten; dabei sei die Bezeichnung

$$p = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in K[X] \qquad \text{mit} \qquad a_n \neq 0$$

gewählt. Dann besitzt das Polynom $\widetilde{p} = b_m^{-1} \cdot a_n \cdot X^{n-m} \cdot q \in K[X]$ den

$$\mathrm{Grad}\left(\widetilde{p}\right) = \mathrm{Grad}\left(\underbrace{b_m^{-1} \cdot a_n}_{\neq 0} \cdot X^{n-m} \cdot q\right) = (n - m) + \mathrm{Grad}(q) = n$$

sowie den Leitkoeffizienten $b_m^{-1} \cdot a_n \cdot 1 \cdot b_m = a_n$, so daß für $p' = p - \widetilde{p} \in K[X]$ dann $\mathrm{Grad}(p') < n$ folgt. Gemäß der Induktionsvoraussetzung gibt es nun $r,\, s' \in K[X]$ mit $p' = s' \cdot q + r$ und $\mathrm{Grad}(r) < \mathrm{Grad}(q)$, und wir erhalten

$$\begin{aligned} p = \widetilde{p} + p' &= b_m^{-1} \cdot a_n \cdot X^{n-m} \cdot q + (s' \cdot q + r) \\ &= \left(b_m^{-1} \cdot a_n \cdot X^{n-m} + s'\right) \cdot q + r \\ &= s \cdot q + r \qquad \text{mit} \qquad s = b_m^{-1} \cdot a_n \cdot X^{n-m} + s' \in K[X]. \end{aligned}$$

48. Wir betrachten den Polynomring $K[X]$ über dem Körper $(K, +, \cdot)$ sowie für das Polynom

$$p = a_n\, X^n + a_{n-1}\, X^{n-1} + \ldots + a_1\, X + a_0 \in K[X]$$

die zugehörige Polynomabbildung

$$f_p : K \to K, \quad f_p(x) = a_n\, x^n + a_{n-1}\, x^{n-1} + \ldots + a_1\, x + a_0;$$

es bezeichne $\mathrm{Abb}(K, K)$ die Menge aller Selbstabbildungen $f : K \to K$ von K.

a) Für alle $p,\, q \in K[X]$ mit

$$p = \sum_{k=0}^{n} a_k X^k \qquad \text{und} \qquad q = \sum_{k=0}^{n} b_k X^k$$

gilt

$$p + q = \sum_{k=0}^{n} (a_k + b_k)\, X^k$$

und damit

$$\begin{aligned} f_{p+q}(x) = \sum_{k=0}^{n} (a_k + b_k)\, x^k &= \sum_{k=0}^{n} \left(a_k\, x^k + b_k\, x^k\right) = \\ &= \sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{n} b_k x^k = f_p(x) + f_q(x) = (f_p + f_q)(x) \end{aligned}$$

für alle $x \in K$, also $f_{p+q} = f_p + f_q$. Für alle $p,\, q \in K[X]$ mit

$$p = \sum_{k=0}^{n} a_k X^k \qquad \text{und} \qquad q = \sum_{\ell=0}^{m} b_\ell X^\ell$$

gilt

$$\begin{aligned} p \cdot q &= \sum_{j=0}^{n+m} c_j X^j \quad \text{mit} \quad c_j = a_j b_0 + \ldots + a_0 b_j \\ &= \sum_{k=0}^{n} \sum_{\ell=0}^{m} (a_k b_\ell) X^{k+\ell} \end{aligned}$$

und damit

$$
\begin{aligned}
f_{p\cdot q}(x) = \sum_{k=0}^{n}\sum_{\ell=0}^{m}(a_k b_\ell)x^{k+\ell} &= \sum_{k=0}^{n}\sum_{\ell=0}^{m}\left(a_k\,x^k\right)\left(b_\ell x^\ell\right) = \\
&= \left(\sum_{k=0}^{n} a_k\,x^k\right)\left(\sum_{\ell=0}^{m} b_\ell x^\ell\right) = f_p(x)\cdot f_q(x) = (f_p\cdot f_q)(x)
\end{aligned}
$$

für alle $x \in K$, also $f_{p\cdot q} = f_p \cdot f_q$. Für das Einspolynom 1 gilt schließlich $f_1(x) = 1$ für alle $x \in \mathbb{R}$, es ist also $f_1 = 1$ die konstante Einsfunktion.

b) Wir setzen nun voraus, daß K unendlich viele Elemente besitzt, und zeigen, daß dann die Abbildung

$$
g : K[X] \to \mathrm{Abb}(K,K), \quad p \mapsto f_p,
$$

injektiv, aber nicht surjektiv ist:

- Zum Nachweis der Injektivität von g seien $p, q \in K[X]$ mit $g(p) = g(q)$. Wegen $f_p = f_q$ gilt $f_{p-q}(x) = f_p(x) - f_q(x) = 0$ für alle $x \in K$, so daß das Polynom $p - q$ unendlich viele Nullstellen besitzt; dies kann über einem Körper nur dann erfüllt sein, wenn $p - q = 0$, also $p = q$ gilt. Damit ist g injektiv.
- Zum Nachweis, daß g nicht surjektiv ist, haben wir zu zeigen, daß nicht jede Selbstabbildung von K eine Polynomabbildung ist. Wir betrachten dazu die Abbildung

$$
h : K \to K, \quad h(x) = \begin{cases} 1, & \text{für } x = 0,\\ 0, & \text{sonst,} \end{cases}
$$

die wegen $h(x) = 0$ für alle $x \in K\setminus\{0\}$ zwar unendliche viele Nullstellen besitzt, wegen $h(0) = 1$ aber nicht die Nullabbildung ist; damit ist h nicht durch ein Polynom darstellbar, und g ist nicht surjektiv.

c) Wir setzen nun voraus, daß K nur endlich viele Elemente besitzt, und zeigen, daß dann die Abbildung $g : K[X] \to \mathrm{Abb}(K)$ surjektiv, aber nicht injektiv ist; es bezeichne $n = |K|$ die Anzahl der Elemente von K.

- Zum Nachweis, daß g nicht injektiv ist, betrachten wir das Polynom

$$
p = \prod_{k\in K}(X - k) \in K[X]
$$

mit $\mathrm{Grad}(p) = |K| = n$; damit gilt insbesondere $p \neq 0$. Da aber jedes Körperelement $x \in K$ eine Nullstelle von p ist, gilt $f_p(x) = 0 = f_0(x)$ für alle $x \in K$, also $f_p = f_0$; wegen $g(p) = g(0)$ ist g nicht injektiv.
- Zum Nachweis der Surjektivität von g betrachten wir eine beliebige Selbstabbildung $f : K \to K$ von K. Daneben betrachten wir für jedes Körperelement $a \in K$ die Hilfsabbildung

$$
h_a : K \to K, \quad h_a(x) = \begin{cases} 1, & \text{für } x = a,\\ 0, & \text{sonst,} \end{cases}
$$

und für alle $x \in K$ damit gilt

$$\left(\sum_{a\in K} f(a)\cdot h_a\right)(x) = \sum_{a\in K} f(a) \underbrace{h_a(x)}_{0 \text{ für } x\neq a} = f(x)h_x(x) = f(x)\cdot 1 = f(x),$$

also

$$f = \sum_{a\in K} f(a)\cdot h_a,$$

und damit reicht es gemäß a) zu zeigen, daß h_a für jedes $a \in K$ eine Polynomabbildung ist. Dazu betrachten wir das Polynom

$$p_a = \prod_{k\in K\setminus\{a\}} (X-k) \in K[X]$$

mit $\mathrm{Grad}(p_a) = |K \setminus \{a\}| = n-1$; für die zugehörige Polynomabbildung $f_{p_a} : K \to K$ gilt

$$f_{p_a}(x) = \prod_{k\in K\setminus\{a\}} (x-k) = \begin{cases} \prod_{k\in K\setminus\{a\}} (a-k)\,, & \text{für } x = a, \\ 0, & \text{für } x \neq a. \end{cases}$$

Da $(K,+,\cdot)$ ein Körper ist, gilt zudem $f_{p_a}(a) \neq 0$, und für das Polynom

$$\frac{1}{f_{p_a}(a)}\cdot p_a \in K[X] \qquad \text{gilt} \qquad g\left(\frac{1}{f_{p_a}(a)}\cdot p_a\right) = h_a;$$

damit ist g surjektiv.