Musterlösung Serie 13

EUKLIDISCHER ALGORITHMUS, JORDAN BLÖCKE

1. *(Euklidischer Algorithmus)* Seien $0 \neq f, g \in K[t]$ Polynome. Der Euklidische Algorithmus ist beschrieben durch folgende Rekursion.

   (i) Setze $r_0 = f$ und $r_1 = Rest(g, f)$, wobei $Rest(g, f)$ der bei der Polynomdivision von g durch f auftretende Restterm ist, also $g = fh + Rest(g, f)$.

   (ii) Setze rekursiv
   $$r_{i+1} = Rest(r_{i-1}, r_i)\,, i = 1, 2, \dots .$$

   (iii) Sei $k+1$ der erste Index so dass $r_{k+1} = 0$ ist. Dann gilt
   $$\mathrm{ggT}(f, g) = c \cdot r_k\,,$$
   wobei $0 \neq c \in K$ so gewählt ist, dass die rechte Seite normiert ist.

   (a) Zeigen Sie die Korrektheit des Euklidischen Algorithmus, also dass tatsächlich $\mathrm{ggT}(f, g) = c \cdot r_k$.

   (b) Zeigen Sie, dass $a, b \in K[t]$ existieren, so dass
   $$\mathrm{ggT}(f, g) = af + bg\,.$$

   (c) Seien nun $f, g \in \mathbb{R}[t]$ folgende Polynome:
   $$f = t^5 - 7t^4 + 31t^3 - 133t^2 + 228t\,, \quad g = t^6 - 5t^5 + 22t^4 - 90t^3 + 53t^2 + 95t - 76\,.$$
   Berechnen Sie $\mathrm{ggT}(f, g)$ mit dem Euklidischen Algorithmus.

   Lösung:

   (a),(b) Siehe z.B. Kapitel 2.1 Satz 4 und Kapitel 2.4 Satz 15 Bosch, Algebra (per VPN mit Ihrem ETH Login sollte der Link verfügbar sein)

   (c) Polynomdivision von g durch f ergibt
   $$g = (t+2)f + r_1\,,$$
   mit $r_1 = 5t^4 - 19t^3 + 91t^2 - 361t - 76$. Wir fahren genau so fort:
   $$f = r_1 \frac{1}{25}(5t - 16) + r_2\,,$$

mit $r_2 = \frac{1}{25}(16t^3 - 64t^2 + 304t - 1216)$. Da nun aber

$$r_1 = r_2 \frac{25}{16}(5t-1)\,,$$

ist also $r_3 = 0$ und somit

$$\begin{aligned} \mathrm{ggT}(f,g) &= \frac{25}{16}\cdot r_2 \\ &= t^3 - 4t^2 + 19t - 76\,. \end{aligned}$$

Die Zerlegung in irreduzible Faktoren bestätigt obige Rechnung:

$$\begin{aligned} f &= (t^2+19)(t-4)(t-3)t\,, \\ g &= (t^2+19)(t-4)(t-1)^2(t+1)\,, \\ \mathrm{ggT}(f,g) &= (t^2+19)(t-4)\,. \end{aligned}$$

2. Seien $0 \neq f, g, \in K[t]$ und $I_f = fK[t], I_g = gK[t]$ die von f und g erzeugten Ideale. Zeigen Sie, dass

   (a)
   $$\mathrm{ggT}(f,g) = M_{I_f+I_g} \text{ und } \mathrm{kgV}(f,g) = M_{I_f \cap I_g}\,,$$
   wobei M_I das Minimalpolynom des Ideals $I \subset K[t]$ bezeichnet.

   (b) Zeigen Sie, dass $\mathrm{ggT}(-,-)$ und $\mathrm{kgV}(-,-)$ kommutative und assoziative Operationen sind und dass gilt
   $$\begin{aligned} \mathrm{ggT}(f_1,\dots,f_n) &= \mathrm{ggT}(f_1, \mathrm{ggT}(f_2, \dots \mathrm{ggT}(f_{n-1}, f_n)\dots))\,, \\ \mathrm{kgV}(f_1,\dots,f_n) &= \mathrm{kgV}(f_1, \mathrm{ggT}(f_2, \dots \mathrm{kgV}(f_{n-1}, f_n)\dots))\,. \end{aligned}$$

   Lösung:

   (a) Siehe Kapitel 2.4. Satz 2 und Satz 13 Bosch, Algebra

   (b) Siehe Kapitel 2.4. Satz 12 Bosch, Algebra

3. Seien V ein endlich dimensionaler K-Vektorraum und $F \in \mathrm{End}(V)$. Sei $p \in K[t]$ ein Polynom das zum charakteristischen Polynom P_F teilerfremd ist. Dann ist $p(F)$ invertierbar.

   Lösung:

   Da $\mathrm{ggT}(P_F, p) = 1$ gibt es $a, b \in K[t]$ so dass
   $$1 = aP_F + bp\,.$$
   Einsetzen von F ergibt mit Caley–Hamilton
   $$\mathrm{id}_V = a(F)\cdot 0 + b(F)p(F)\,,$$
   also ist $p(F)^{-1} = b(F)$.

4. Sei $p \in K[t]$ ein irreduzibles normiertes Polynom von Grad $n = \deg(p)$ mit Begleitmatrix $B_p \in \mathrm{M}(n \times n, K)$. Für $r \in \mathbb{N}$ sei

$$\tilde{J}_r(B_p) = \begin{pmatrix} B_p & \tilde{E}_n & & & \\ & B_p & \tilde{E}_n & & \\ & & \ddots & \ddots & \\ & & & \ddots & \tilde{E}_n \\ & & & & B_p \end{pmatrix} \in \mathrm{M}(nr \times nr, K)\,.$$

(a) Zeigen Sie, dass

$$M_{\tilde{J}_r(B_p)} = p^r$$

das Minimalpolynom von $\tilde{J}_r(B_p)$ ist.
Hinweis: Es gibt einen Vektor (zyklischer Vektor) $v \in K^{rn}$ so dass

$$K^{rn} = \mathrm{span}\big(v, Av, \dots, A^{rn-1}v\big)\,,$$

wobei $A = \tilde{J}_r(B_p)$. Also bilden $v, Av, \dots, A^{rn-1}v$ eine Basis des K^{rn}.

(b) Zeigen Sie, dass für $0 \leqslant s \leqslant r$ die Matrix $p(\tilde{J}_r(B_p))^s$ Rang $(r-s)n$ hat.

(c) Sei nun $F \in \mathrm{End}(V)$ und $\mathcal{B}$ eine Basis von V so dass $M_{\mathcal{B}}(F)$ in Jordanscher Normalform ist (im Sinne von Theorem 3.6 im Zusatzskript), wobei der Jordanblock $\tilde{J}_r(B_p)$ jeweils s_r mal vorkommt ($r = 1, 2, \dots$). Berechnen Sie dann

$$d_j = \dim \mathrm{Ker}(p(F)^j)\,, \quad j = 1, 2, \dots\,,$$

mittels Aufgabe 3 und (b). Rechnen Sie auch direkt nach, dass

$$s_r = \frac{1}{n}\left(2d_r - d_{r-1} - d_{r+1}\right)\,,$$

wobei $n = \deg(p)$.

Lösung:

(a) Das charakteristische Polynom ist $\pm p^r$, also muss das Minimalpolynom M_A die Form p^s haben mit $s \leqslant r$. Wir müssen also nur zeigen, dass $\deg(M_A) = rn$. Der zyklische Vektor wie im Hinweis ist $v = e_{rn}$, der 'letzte' Basisvektor. Ist $q(t)$ ein Polynom vom Grad k mit $q(A) = 0$, dann ist insbesondere $q(A)v = 0$, also sind $v, Av, \dots, A^k v$ linear abhängig. Dies steht im Widerspruch zur Aussage, dass $v, Av, \dots, A^{rn-1}v$ eine Basis des K^{rn} bilden, falls $k < rn$. Vergleiche auch mit LinAlg I, Serie 13, Aufgabe 4 und LinAlg II, Serie 12, Aufgabe 5.

(b) Für $r = s$ ist die Aussage klar, sei also $r > s$. Zunächst ist $p(A)$ Blockdiagonal mit Nullen auf der Blockdiagonalen. Also gilt $\operatorname{rang}(p(A)^s) \leqslant (r-s)n$. Wir müssen also nur noch '$\geqslant$' zeigen. Sei wieder $v = e_{rn}$ der zyklische Vektor von oben. Sei $w = p(A)^s v = e_{rn-sn}$. Dann ist aber (ersetze einfach r durch $r - s$ oben)

$$\operatorname{span}\bigl(w, Aw, \dots, A^{rn-sn-1}w\bigr) = K^{rn-sn} \subset K^{rn}\,.$$

Aber

$$A^j w = A^j p(A)^s v = p(A)^s A^j v \in \operatorname{Im}(p(A)^s)\,,$$

also gilt

$$\dim \operatorname{Im}(p(A)^s) \geqslant rn - sn\,,$$

also $\operatorname{rang}(p(A)^s) \geqslant rn - sn$.

(c) Wir können äquivalent ausrechnen, dass

$$d_j = \dim \operatorname{Ker}(p(B)^j)\,,$$

wobei $B = M_{\mathcal{B}}(F)$. Die Martrix B ist Blockdiagonal mit Jordanblöcken auf der Diagonalen. Also ist auch $p(B)^j$ Blockdiagonal, und der Rang ist die Summe der Ränge der Diagonalblöcke. Wegen Aufgabe 3 sind die Blöcke zu irreduziblen Faktoren $\neq p$ invertierbar, haben also vollen Rang. Wegen (b) trägt jeder Jordanblock der Grösse $r > j$ gerade $(rn - jn)$ zum Rang bei (und natürlich 0 falls $r \leqslant j$). Wir erhalten also, dass

$$d_j = \sum_{r=1}^{j} rns_r + \sum_{r \geqslant j+1} jns_r\,.$$

Betrachte nun

$$2d_j - d_{j-1} - d_{j+1}\,.$$

Hier kürzen sich alle Summanden mit $r \notin \{j, j+1\}$ gerade weg. Sammeln wir die Vorfaktoren der verbleibenden 2 Terme zusammen erhalten wir

$$\begin{aligned} 2d_j - d_{j-1} - d_{j+1} &= (2j - (j-1) - j)ns_j + (2j - (j-1) - (j+1))ns_{j+1} \\ &= ns_j\,. \end{aligned}$$

5. In der Vorlesung wurden zwei a priori verschiedene Versionen der Jordanschen Normalform für $K = \mathbb{R}$ betrachtet. Bei der einen waren die Jordanblöcke von der Form $J_r(\lambda)$ oder

$$J_r(A) = \begin{pmatrix} A & E_2 & & & \\ & A & E_2 & & \\ & & \ddots & \ddots & \\ & & & \ddots & E_2 \\ & & & & A \end{pmatrix} \in \mathrm{M}(2r \times 2r, \mathbb{R})\,,$$

mit

$$A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Bei der anderen waren die Jordanblöcke von der Form

$$\tilde{J}_r(A) = \begin{pmatrix} A & \tilde{E}_n & & & \\ & A & \tilde{E}_n & & \\ & & \ddots & \ddots & \\ & & & \ddots & \tilde{E}_n \\ & & & & A \end{pmatrix} \in \mathrm{M}(nr \times nr, K),$$

mit A der Begleitmatrix zu einem irreduziblen Faktor im charakteristischen Polynom des Endomorphismus F. Bestimmen Sie die Basistransformation, die die eine Jordansche Normalform in die andere überführt, für $r = 1$ und $r = 2$.

Lösung:

Seien

$$A_1 = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \quad A_2 = \begin{pmatrix} -a_1 & 1 \\ -a_0 & 0 \end{pmatrix},$$

das heißt A_2 ist die Begleitmatrix des Polynoms $p(t) = t^2 + a_1 t + a_0$. Falls A_1 und A_2 beide zum irreduziblen Faktor p korrespondieren (dann ist insbesondere $b \neq 0$), also $P_{A_1}(t) = p(t)$, dann ist

$$a_1 = -2a, \quad a_0 = a^2 + b^2.$$

Für allgemeines r betrachten wir nun die Matrix in (der ersten Form der) JNF

$$J := J_r(A_1) = D + N$$

wobei D Blockdiagonal ist und N die Matrix mit E_2's auf der ersten Blocknebendiagonalen. Es gilt dass $ND = DN$. Die Jordanbasis (f_j) in der zweiten Formulierung kann dann wie in der VL definiert werden als

$$f_{2k-i} = J^i p(J)^{r-k} e_{2r}$$

wobei $i = 0, 1$ und (e_j) die Standardbasis ist. Man kann noch vereinfachen:

$$p(J) = D^2 + 2DN + N^2 + a_1(D + N) + a_0 = \underbrace{p(D)}_{=0} + (2D + a_1)N + N^2.$$

Für den Fall $r = 1$ erhalten wir also

$$\begin{aligned} f_2 &= e_2 \\ f_1 &= A_1 e_2 = b e_1 + a e_2 \end{aligned}$$

Die entsprechende Basistransformationsmatrix ist also

$$S = \begin{pmatrix} b & 0 \\ a & 1 \end{pmatrix},$$

bzw. in die andere Richtung

$$S^{-1} = \frac{1}{b} \begin{pmatrix} 1 & 0 \\ -a & b \end{pmatrix},$$

Wir haben also

$$A_2 = S^{-1} A_1 S,$$

was man auch leicht direkt nachrechnet.

Für den Fall $r = 2$ erhalten wir entsprechend die Basis

$$\begin{aligned}
f_4 &= e_4 \\
f_3 &= J e_4 = b e_3 + a e_4 + e_2 \\
f_2 &= p(J) e_4 = (2D + a_1) N e_4 = 2(b e_1 + a e_2) + a_1 e_2 = b e_1 - a e_2 \\
f_1 &= J f_2 = -(a^2 + b^2) e_1.
\end{aligned}$$