l7
- 1 -

Vorlesung Lineare Algebra II

SoSe'20 hhu
K. Halupczok

§2: Normalformentheorie

l7: Die Polynomalgebra

Stichworte: K-Algebra, Beispiele $\underbrace{\mathrm{Hom}(U,U)}_{=\mathrm{End}(U)}$ und $K^{m\times m}$, freie von einem Element erzeugte K-Algebra $K[T]$ = Polynomalgebra, Einsetzhomomorphismus, Endo in Polynom einsetzen

Die Motivation aus l6 zeigte uns, dass wir Endomorphismen f gerne in Polynome "einsetzen" möchten: Durch Bilden von $(f-\lambda\,\mathrm{id}_V)^t$, d.h. Einsetzen von f in $(T-\lambda)^t$, kommen wir zu den HVen in der Jordanschen Normalform. Um dahinzukommen, muss dieses "Einsetzen" genau erklärt/definiert werden, weswegen wir erst etwas ausholen müssen und hier in l7 ersteinmal die Polynomalgebra sauber einführen, die bisher als "Polynomring" $K[T]$ in LA I, L8.19 eingeführt wurde. Einiges in l7, l8 ist daher eine Wiederholung von Stoff aus LA I, L8, vertieft und erweitert diesen aber auch.

Beginnen wir erst mit der Def. einer Algebra, vgl. auch LA I, L15.4, L14.10/11.

7.1. Def. (K-Algebra): Ein K-Vektorraum A, in dem noch eine weitere Operation "Multiplikation" $\cdot : A\times A\to A$ erklärt ist, heißt eine K-Algebra, wenn gilt:
1.) $\cdot$ ist assoziativ, 2.) es gelten die Distributivgesetze (für alle $a,b,c\in A$, $\alpha,\beta,\gamma\in K$):

$$(\alpha a+\beta b)\cdot c=\alpha(a\cdot c)+\beta(b\cdot c)$$
$$a(\beta b+\gamma c)=\beta(a\cdot b)+\gamma(a\cdot c).$$

- Gibt es ein Element $1\in A$ mit $\forall a\in A: 1\cdot a=a\cdot 1=a$, so heißt A eine K-Algebra mit 1 ("mit Eins"). 1_A
- Ist die Multiplikation kommutativ, so heißt A eine kommutative K-Algebra.

7.2. Vereinbarung: Im weiteren betrachten wir nur K-Algebren mit 1-Element.

7.3. Bsp.: K selbst ist K-Algebra, im Fall $K=\mathbb{R}$ die Polynome $\mathbb{R}[T]$.
Beide sind kommutative Algebren mit 1.

7.4. Bem.: Eine Algebra ist mit $+,\cdot$ ein Ring, der gleichzeitig K-Vektorraum ist.

Noch weitere Beispiele liefert folgendes Lemma:

l7
-2-

$(f\circ g \neq g\circ f)$

$A :=$ $\operatorname{End}(U)$

7.5 Lemma: Sei U ein K-VR. Dann ist $\operatorname{Hom}(U,U)$ mit der üblichen Addition und dem Hintereinanderausführen (=Komposition "$\circ$") von Homomorphismen als Multiplikation eine i.a. nicht kommutative K-Algebra mit id_U als 1-Element.

7.6 Bem.: Wegen $\operatorname{Hom}(U,U) \cong K^{m\times m}$ für $m = \dim U$, vgl. LAI L15.5, bilden auch die quadratischen Matrizen der Dimension m eine K-Algebra. ("$\cong$" ist Algebren-Isomorphismus, vgl. 7.11). Das gibt uns noch mehr Beispiele für Algebren (die i.a. nicht kommutativ sind).

Ü Warum ist $K^{m\times n}$ mit $m\neq n$ keine K-Algebra?

Produkt: $\prod_{i\in\mathbb{N}_0} K$

Coprodukt: $\coprod_{i\in\mathbb{N}_0} K$

7.7 Def.: Zu einem Körper K bilden wir das Coprodukt über "$\mathbb{N}_0$" viele Exemplare von K, d.h. $P := \coprod_{i\in\mathbb{N}_0} K := \{(\alpha_0, \alpha_1, \alpha_2, \ldots);\ \alpha_i \in K,\ \alpha_i \neq 0 \text{ nur endl. oft}\}$

$\rightsquigarrow$ Folgen, deren Einträge nur endlich oft $\neq 0$ sind

- Klar, dass P (zunächst) ein K-VR ist.
- In Analogie zu den Einheitsvektoren in K^n bezeichnen wir die Folgen $(0,\ldots,0,\overset{i\text{-te Stelle}}{1},0,\ldots)$, die genau an der i-ten Stelle eine 1 und sonst nur 0en haben, mit e_i.

Offensichtlich ist $(e_i \mid i\in\mathbb{N}_0)$ eine Basis von P.

Wir definieren nun in P eine Multiplikation $\cdot$ aus der Festsetzung

$$\boxed{e_i\cdot e_j := e_{i+j}}$$

Wegen der Distributivgesetze führt dies zwangsläufig zu

$$\left(\sum_{i=0}^{n}\alpha_i e_i\right)\cdot\left(\sum_{j=0}^{m}\beta_j e_j\right) = \sum_{k=0}^{n+m}\gamma_k e_k \quad\text{mit}\quad \gamma_k = \sum_{i+j=k}\alpha_i\beta_j .$$

⌈Z.B. $(-2e_2+e_1-11e_0)\cdot(5e_3+13e_2-e_0) = -10e_5+(-26+5)e_4+(-55+13)e_3+(2+11)e_2-e_1+11e_0$⌋

7.8 Satz und Definition: Mit der eben eingeführten Multiplikation ist $P = \coprod_{i\in\mathbb{N}_0} K$ eine kommutative K-Algebra mit 1-Element e_0. Man nennt P die freie von einem Element erzeugte K-Algebra, oder auch Algebra der Polynome in einer Veränderlichen/Unbestimmten über K und wird mit $K[T]$ (gelesen: K adjungiert T) bezeichnet. Die Elemente von $K[T]$ heißen Polynome in einer Veränderlichen/Unbestimmten über K.

$T := e_1$

7.9 Beweis, dass $K[T]$ Algebra ist: Nachrechnen der Axiome ... Ü

7.10. **Bem.:** • Schreiben wir in P statt e_0 das Symbol 1,
statt e_1 das Symbol T.
Dann ist wegen $e_i \cdot e_j = e_{i+j}$ offenbar $e_2 = e_1 \cdot e_1 = T \cdot T = T^2$, $e_3 = T^3$, usw.
• Jedes Element von P lässt sich also statt $p = \alpha_0 e_0 + \alpha_1 e_1 + \ldots + \alpha_m e_m$ schreiben als $p = \alpha_0 \cdot 1 + \alpha_1 \cdot T + \alpha_2 \cdot T^2 + \ldots + \alpha_m \cdot T^m$,
und die Multiplikation ist so, wie wir es von Polynomen "naiv" gewöhnt sind.
⌜z.B. $(-2T^2 + T - 11) \cdot (5T^3 + 13T^2 - 1) = -10T^5 + (-26+5)T^4 + (-55+13)T^3 + (2+11)T^2 - T + 11$⌟
• Wir bemerken nur noch, dass $T^0 = 1$ ist.
• Die freie, von einem Element erzeugte K-Algebra hat eine universelle Eigenschaft über die Existenz und Eindeutigkeit gewisser Homomorphismen (die sie bis auf Isomorphie charakterisiert):

7.11. **Def. (K-Algebra-Homomorphismen):** Sind A, A' K-Algebren mit 1-Elementen $1_A, 1_{A'}$, so heißt eine Abb. $f: A \to A'$ ein K-Algebren-Homomorphismus, wenn gilt: 1.) f ist K-Vektorraumhomomorphismus,
2.) $\forall a, b \in A: f(\underset{\text{in } A}{a \cdot b}) = f(a) \underset{\text{in } A'}{\cdot} f(b)$, $(\in A')$
3.) $f(1_A) = 1_{A'}$.

7.12. **Bem.:** Eine solche Abb. ist also verträglich mit der Struktur von A und A'.
Für die freie Algebra $K[T]$ gilt nun:

7.13. **Satz:** Ist A eine K-Algebra mit 1-Element 1_A, so gibt es zu jedem $a \in A$ genau einen K-Algebra-Homomorphismus $f_a: K[T] \to A$ mit $f_a(T) = a$. ⌜$T \overset{f_a}{\mapsto} a$⌟
(Genannt "Einsetzhomomorphismus": a wird anstelle T "eingesetzt".)

univ. Eigenschaft

!

Bew.: • Ist f ein solcher Homomorphismus, so ist notwendig für $p = \sum_{i=0}^{m} \alpha_i T^i \in K[T]$, dass $f(p) = f(\sum_{i=0}^{m} \alpha_i T^i) = \sum_{i=0}^{m} \alpha_i f(T^i)$

$$= \sum_{i=0}^{m} \alpha_i (f(T))^i = \sum_{i=0}^{m} \alpha_i a^i \quad (\text{wo } a^0 := 1_A \text{ gesetzt wird}).$$

• Andererseits prüft man leicht, dass die Abb. $f_a: \sum_{i=0}^{m} \alpha_i T^i \mapsto \sum_{i=0}^{m} \alpha_i a^i$ tatsächlich ein Homomorphismus mit den gewünschten Eigenschaften ist. □

7.14. **Def.:** Für den Einsetzhomomorphismus schreiben wir jetzt auch abkürzend

$$f_a(p) =: p(a).$$

7.15. **Bsp.:** $p(a) = a^3 - 2a + 1_A$ für $p = T^3 - 2T + 1 \in K[T]$, $a \in A$, A sei bel. K-Algebra.

7.16. **Bem.:** Ist speziell $A = K = \mathbb{R}$, so ist dies das übliche Auswerten eines reellen Polynomes an der reellen Stelle a. Auf diesen Spezialfall sind wir jetzt aber nicht mehr beschränkt: Ist U ein K-VR, so ist $Hom(U,U)$ eine K-Algebra, und wir können Satz 7.13 hierauf anwenden. Ist dann $h \in Hom(U,U)$, $p = \sum_{i=0}^{n} \alpha_i T^i$, so ist $f_h(p) = p(h) = \sum_{i=0}^{n} \alpha_i h^i$ ein Element aus $Hom(U,U)$. Da f_h die 1-Elemente in sich überführt, ist insbesondere für jedes $h \in Hom(U,U)$: $f_h(1) = id_U$.

7.17. **Wichtige Bem.:** Die Algebra $Hom(U,U)$ ist im allgemeinen nicht kommutativ. Die durch Einsetzen eines h in verschiedene Polynome p, q entstehenden Endomorphismen sind jedoch stets vertauschbar, da $K[T]$ kommutativ ist:

$$p(h) \circ q(h) = f_h(p) \circ f_h(q) = f_h(p \cdot q) = f_h(qp) = f_h(q) \circ f_h(p) = q(h)p(h)$$

7.18. **Bsp.:** $p = T^2 - 2$, $q = T^3 + T \in \mathbb{R}[T]$, $h \in Hom(\mathbb{R}^2, \mathbb{R}^2)$, $x \mapsto h(x) = \underbrace{\begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}}_{=H} x$, dann können wir diese Gleichung auch direkt im Beispiel nachrechnen:

$$p(h)q(h) = (h^2 - 2id) \circ (h^3 + h) = h^2 \circ (h^3 + h) - 2id \circ (h^3 + h) = h^5 + h^3 - 2h^3 - 2h$$
$$= h^5 - 2h^3 + h^3 - 2h = (h^3 + h) \circ (h^2 - 2id) = q(h)p(h) \checkmark$$

Als Matrixprodukt:

$$p(H)q(H) = \left(\underbrace{\begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}^2}_{= \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ -5 & 8 \end{pmatrix}} - 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \cdot \left(\underbrace{\begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}^3}_{= \begin{pmatrix} 3 & 5 \\ -5 & 8 \end{pmatrix} \cdot \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 18 \\ -18 & 19 \end{pmatrix}} + \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} \right)$$

$$= \begin{pmatrix} 1 & 5 \\ -5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 3 & 19 \\ -19 & 22 \end{pmatrix} = \begin{pmatrix} 3 - 5 \cdot 19 & 19 + 5 \cdot 22 \\ -15 - 6 \cdot 19 & -5 \cdot 19 + 6 \cdot 22 \end{pmatrix},$$

das kommt auch raus für $\left(\begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}^3 + \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} \right) \cdot \left(\begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix}^2 - 2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right)$

$$q(H) \cdot p(H) = \left(\begin{pmatrix} 1 & 18 \\ -18 & 19 \end{pmatrix} + \begin{pmatrix} 2 & 1 \\ -1 & 3 \end{pmatrix} \right) \cdot \left(\begin{pmatrix} 3 & 5 \\ -5 & 8 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right)$$
$$= \begin{pmatrix} 3 & 19 \\ -19 & 22 \end{pmatrix} \cdot \begin{pmatrix} 1 & 5 \\ -5 & 6 \end{pmatrix} = \begin{pmatrix} 3 - 5 \cdot 19 & 15 + 6 \cdot 19 \\ -19 - 5 \cdot 22 & -5 \cdot 19 + 22 \cdot 6 \end{pmatrix},$$

da $15 + 6 \cdot 19 = 19 + 5 \cdot 22 = 129$ ✓

Bsp.: $p(a) = a^3 - 2a + 1_A$ für $p = T^3 - 2T + 1 \in K[T]$, $a \in A$, A sei bel. K-Algebra.

1. Bsp.: $A = K^{3\times 3}$, sei $a \in A$, etwa $a = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in A$

Dann:

$$p(a) = a^3 - 2a + 1_A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}^3 - 2\cdot\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 8 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \ldots$$

2. Bsp.: $A = \mathrm{End}(K^2)$, sei $f \in A$, $f(x) = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} x$

Dann $p(f) = f^3 - 2f + id_{K^2} = f \circ f \circ f - 2\cdot f + id_{K^2} \in A$

3. Bsp.: Sei $p = (T-\lambda)^m \in K[T]$, $\lambda \in K$, $m \in \mathbb{N}_0$

- Sei $A := \mathrm{End}(K^n)$, $f \in A$

$$\rightsquigarrow p(f) = (f - \lambda\, id_{K^n})^m$$

$$= \underbrace{(f - \lambda\, id) \circ (f - \lambda\, id) \circ \ldots \circ (f - \lambda\, id)}_{m\text{ mal}}$$

- Sei $A := K^{n\times n}$, $F \in A$

$$\rightsquigarrow p(F) = (F - \lambda \cdot I_n)^m$$

$$= \underbrace{(F - \lambda I_n) \cdots (F - \lambda I_n)}_{m\text{ mal}}$$