2.44 Bem: (a) Wir wiederholen aus Linearer Algebra I.
Sei V ein K-Vektorraum. Dann ist $\mathrm{End}_K(V)$, die Menge aller Endomorphismen von V, ein K-Vektorraum und Ring, mit λT, $S+T$, $S\circ T$ definiert durch

$$(\lambda T)(x) := \underline{\lambda T(x)}$$
$$(S+T)(x) := \underline{S(x)+T(x)}$$
$$(S\circ T)(x) := \underline{S(T(x))},$$

für $\lambda \in K$, $S, T \in \mathrm{End}_K(V)$.

(b) Sei $A \in M_n(K)$ bzw $T: V \to V$ linear.
Sei $p \in K[X]$ Polynom. Wir können Polynome an Matrizen bzw Endomorphismen auswerten.
Für $p = a_0 + a_1 X + \dots + a_d X^d$ definieren wir:

$$p(A) := a_0 I_n + a_1 A + \dots + a_d A^d \in M_n(K)$$

bzw. $p(T) := a_0 \mathrm{id}_V + a_1 T + \dots + a_d T^d \in \mathrm{End}_K(V)$

mit $T^i := \underbrace{T\circ T\circ\dots\circ T}_{i \text{ mal}}$.

Das Auswerten von Polynomen an Matrizen bzw Endomorphismen ist ein Ringhomomorphismus

$$K[X] \longrightarrow M_n(K),\ p \mapsto p(A)$$

bzw $$K[X] \longrightarrow \mathrm{End}_K(V),\ p \mapsto p(T),$$

d.h. $$(p+q)(A) \overset{1.1}{=} \underline{p(A)+q(A)}$$
$$(p\cdot q)(A) \overset{1.1}{=} \underline{p(A)\cdot q(A)},$$

für $p, q \in K[X]$. Analog für T.

(c) Für $s,t \in \mathbb{N}_0$ gilt $A^s \cdot A^t = A^t \cdot A^s$
Für $\lambda \in K$ gilt $\lambda A = A\lambda$.
Also ist $p(A) \cdot q(A) = q(A) \cdot p(A)$,
für $p,q \in K[X]$. Beispielsweise gilt für $p = X^2+3$
und $q = X-2$:

$$p(A) \cdot q(A) = \underline{\qquad\qquad\qquad}$$
$$q(A) \cdot p(A) = \underline{\qquad\qquad\qquad}$$

(d) Angenommen $Av = \lambda v$, $\lambda \in K$, $v \in K^4$.

Beh: Dann gilt $p(A) \cdot v = p(\lambda) \cdot v$, für $p \in K[X]$.
Wir schauen uns dies zunächst am Beispiel an, für $p = X^2+3$:

$$p(A) \cdot v = (A^2 + 3I) \cdot v$$
$$=$$
$$= (\lambda^2+3)v = p(\lambda) \cdot v$$

Beweis: Wir zeigen die Behauptung zunächst für Polynome $p = X^i$, $i \in \mathbb{N}_0$ (mittels Induktion):

Also gilt $p(A) \cdot v = p(\lambda) \cdot v$ dh. $A^i v = \lambda^i v$.
Sei nun $p = \sum_{i=0}^{t} a_i X^i$. Dann folgt:

$$p(A) \cdot v = \left(\sum_{i=0}^{t} a_i A^i\right) v = \sum_{i=0}^{t} a_i \lambda^i v = p(\lambda) \cdot v.$$

Wir schauen uns einen Spezialfall an, bevor wir allgemeine Resultate beweisen:

2.45 Bsp:

Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(K)$. Dann ist:

$$\chi_A = \det \begin{pmatrix} X-a & -b \\ -c & X-d \end{pmatrix} = \underline{\hspace{6cm}}$$

$$= X^2 + (\underline{\hspace{1.5cm}}) \cdot X + \underline{\hspace{2cm}} = X^2 - Sp(A)X + \det A \cdot I_2$$

$$\Rightarrow \chi_A(A) =$$

$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Zu jeder 2×2-Matrix A existiert also ein normiertes Polynom $p \in K[X]$, nämlich zum Beispiel das charakteristische Polynom χ_A, mit $p(A) = 0$.

Ein solches Polynom minimalen Grades heißt Minimalpolynom von A:

2.46 Def: Sei $A \in M_n(K)$, $T: V \to V$ linear.

(a) Ein Polynom $m_A \in K[X]$ mit den Eigenschaften

(i) m_A ist normiert (siehe 1.13),

(ii) $m_A(A) = 0$,

(iii) für alle $f \in K[X]$ mit $f(A) = 0$, gibt es ein $q \in K[X]$ mit $f = q \cdot m_A$,

heißt Minimalpolynom von A.

(b) Ein Polynom $m_T \in K[X]$ mit den Eigenschaften

(i) m_T ist normiert,

(ii) $m_T(T) = 0$,

(iii) für alle $f \in K[X]$ mit $f(T) = 0$, gibt es ein $q \in K[X]$ mit $f = q \cdot m_T$,

heißt Minimalpolynom von T.

2.47 Thm: Das Minimalpolynom einer Matrix $A \in M_n(K)$ bzw eines Endomorphismus $T: V \to V$ existiert, und ist eindeutig bestimmt.

Beweis: Sei $n \in \mathbb{N}$, $A \in M_n(K)$.

(a) Wir zeigen die Existenz des Minimalpolynoms.

(i) $M_n(K)$ ist ein K-Vektorraum der Dimension ____. Die Menge $\{I_n = A^0, A, A^2, \dots, A^{n^2}\} \subseteq M_n(K)$ besteht aus ____ vielen Elementen.

$\overset{\text{LAI}}{\Longrightarrow}$ Diese Menge ist linear abhängig.

$\Rightarrow$ $\exists \lambda_i \in K$ mit $\lambda_0 A^0 + \lambda_1 A + \dots + \lambda_{n^2} A^{n^2} = 0$, und nicht alle λ_i sind Null.

Sei $p := \lambda_0 + \lambda_1 X + \ldots + \lambda_{n^2} X^{n^2} \in K[X]$. Dann ist $p \neq 0$ mit $p(A) = 0$. Es existiert also ein nicht-triviales Polynom p mit $p(A) = 0$.

(ii) Sei $m_A \in K[X]$ minimalen Grades mit $m_A(A) = 0$. Sei λ der Leitkoeffizient von m_A, dh. $\lambda \in K^\times$.

$\Rightarrow$ $\lambda^{-1} m_A \in K[X]$ ist normiert mit

$$(\lambda^{-1} m_A)(A) = \lambda^{-1} m_A(A) = \lambda^{-1} \cdot 0 = 0.$$

(iii) Sei $f \in K[X]$ mit $f(A) = 0$.

Wir machen Division mit Rest, siehe 1.17:

Es existieren $q, r \in K[X]$ mit

$$f = q \cdot m_A + r,$$

wobei $\deg r < \deg m_A$ ist.

Da Auswerten an A ein Ringhomomorphismus ist

$$\overset{2.44}{\Longrightarrow} \quad 0 = f(A) = q(A) \cdot \underbrace{m_A(A)}_{=0} + r(A) = r(A)$$

Da m_A minimalen Grades ist nach Definition

$\Rightarrow r = 0$. Also ist $f = q \cdot m_A$.

Dies zeigt, daß es zu jeder Matrix $A \in M_n(K)$ ein Minimalpolynom in $K[X]$ gibt.

(b) Wir zeigen die Eindeutigkeit des Minimalpolynoms.

Sei $\mu_A \in K[X]$ ein weiteres Polynom, welches die ~~in~~ Def 2.46 genannten Eigenschaften hat.

Da $m_A(A) = 0$ und μ_A ein Minimalpolynom ist

$\Rightarrow \exists\, 0 \neq q \in K[X]$ mit $m_A = q \cdot \mu_A$.

$$\Rightarrow \deg m_A = \deg q + \deg \mu_A$$
$$\geq \deg \mu_A$$
$$\geq \deg m_A,$$

da nach Konstruktion m_A minimalen Grades mit den Eigenschaften aus Def 2.46 ist.

$\Rightarrow \deg m_A = \deg \mu_A$, und beide Polynome sind normiert.

$\Rightarrow p := m_A - \mu_A$ erfüllt $\deg p < \deg m_A$

und $p(A) = m_A(A) - \mu_A(A) = 0 - 0 = 0$.

Nach Definition von m_A (minimaler Grad...)

$\Rightarrow p = 0$

$\Rightarrow m_A = \mu_A$.

Also ist das Minimalpolynom von A eindeutig bestimmt.

Bem: In der Sprache der Algebra ist dieser Beweis kürzer. Hierzu benötigt man die Begriffe Ideal, Hauptidealring. Der Kern jedes Ringhomomorphismus ist ein Ideal, insbesondere ist $I := \operatorname{Kern}(K[X] \to M_n(K))$ aus Bem 2.44 ein Ideal. Division mit Rest 1.17 zeigt, daß $K[X]$ ein Hauptidealring ist. Dies bedeutet, daß I von einem Element erzeugt wird. Die Erzeuger von I sind von der Form $\lambda \cdot m_A$, $\lambda \in K^\times$. Siehe beispielsweise Henke, Algebra-Skript SS2017, § 10 ff

2.48 Bem: Der Beweis in 2.47 zur Existenz des Minimalpolynoms ist konstruktiv:

- Berechne die Potenzen $A^0, A^1, A^2, \dots$ (soweit wie nötig)

- Durch das Lösen linearer Gleichungssysteme, bestimme die kleinste Zahl $d \in \mathbb{N}$ mit $\{A^0, A, A^2, \dots, A^d\}$ ist linear abhängig, d.h. finde $\lambda_j \in k$ mit
$$\sum_{j=0}^{d} \lambda_j A^j = 0, \text{ (nicht alle } \lambda_j \text{ Null).}$$
Dann ist $m_A = X^d + \sum_{j=0}^{d-1} \frac{a_j}{a_d} \cdot X^j \in k[X]$
das Minimalpolynom von A.

2.49 Bsp: (a) Sei $A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ wie in Bsp 2.1.
Dann ist $A^2 = \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix}$. Wir sehen $\{I_2, A\}$ sind linear unabhängig, aber $\{I_2, A, A^2\}$ ist linear abhängig:
$$\lambda_0 \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \lambda_1 \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 & -2 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

mit $\lambda_0 =$ _____, $\lambda_1 =$ _____, $\lambda_2 =$ _____.

Setze $p := \lambda_2 X^2 + \lambda_1 X + \lambda_0 \in k[X]$.
Normiere durch Multiplikation mit λ_2^{-1};
dann ist
$$m_A := X^2 + \underline{\qquad\qquad} \overset{\text{Faktorisieren}}{=} (X \quad)\cdot(X \quad)$$
das Minimalpolynom von A.
Wir beobachten $m_A = \chi_A$, siehe 2.26.
Wir zeigen m_A ist immer Teiler von χ_A.

(b) Sei $C = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ -1 & 4 & -1 \end{pmatrix}$. Dann sind die Potenzen von C:

$$C^2 = \begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ -1 & 4 & -1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ -1 & 4 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 4 & 0 \\ -4 & 8 & 0 \\ -4 & 7 & 1 \end{pmatrix}$$

$$C^3 = \begin{pmatrix} 0 & 4 & 0 \\ -4 & 8 & 0 \\ -4 & 7 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ -1 & 4 & -1 \end{pmatrix} = \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix}$$

Die Menge $\{I, C\}$ ist linear unabhängig.

Die Menge $\{I, C, C^2\}$ ist ________________

Die Menge $\{I, C, C^2, C^3\}$ ist ________________.

Hierbei finden wir die nicht triviale Linearkombination

$$\lambda_0 \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \lambda_1 \begin{pmatrix} 1 & 1 & 0 \\ -1 & 3 & 0 \\ -1 & 4 & -1 \end{pmatrix} + \lambda_2 \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} + \lambda_3 \begin{pmatrix} & & \\ & & \\ & & \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

mit $\lambda_0 =$ ______ $\lambda_1 =$ ______ $\lambda_2 =$ ______ $\lambda_3 =$ ______.

Also ist das Minimalpolynom von C gerade

$$m_C = X^3 + \_\_\_\_\_\_\_\_\_\_\_\_$$

$$\overset{\text{Faktorisieren}}{=} \_\_\_\_\_\_\_\_\_\_\_\_$$

Wie vergleicht sich m_C mit χ_C, siehe 2.37.

Wir bemerken: Das Ausrechnen von Minimalpolynomen ist mühsam. Gleichzeitig besteht in unseren Beispielen jeweils eine Beziehung zum charakteristischen Polynom. Das wollen wir genauer anschauen.