8. Polynomringe

Das Umgehen mit Polynomen, d.h. mit Ausdrücken der Form

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

ist aus der Schule vertraut, falls die Koeffizienten $a_0, \ldots, a_n$ ganze oder rationale oder reelle Zahlen sind. In diesen Fällen kann man das Polynom mit einer Abbildung

$$\tilde{p} : \mathbb{R} \to \mathbb{R},\ \tilde{p}(x) := \sum_{i=0}^{n} a_i x^i$$

identifizieren. Es gilt dann $\tilde{p}(0) = a_0, (\tilde{p})'(0) = a_1, (\tilde{p})''(0) = 2a_2$ und die k'te Ableitung von $\tilde{p}$ ausgewertet an der Stelle $x = 0$ ist gerade $k!\,a_k$, d.h. die Funktion $\tilde{p}$ bestimmt die $a_0, \ldots, a_n$ eindeutig. Wenn man nun Polynome mit Koeffizienten a_i aus einem beliebigen Körper K betrachten will, entsteht im Fall von endlichen Körpern folgende Schwierigkeit: es „existieren" unendlich viele verschiedene Polynome, z.B. die „Monome" $1, x, x^2, \ldots, x^n, \ldots$, aber nur endlich viele verschiedene Abbildung $\tilde{p} : K \to K$. Ein Polynom $\sum\limits_{i=0}^{n} a_i x^i$ mit $a_i \in K$ kann also nicht durch die zugehörige Abbildung $\tilde{p} : K \to K$, $\tilde{p}(x) := \sum\limits_{i=0}^{n} a_i x^i$ eindeutig bestimmt sein. Diese Tatsache ruft die Frage hervor, was denn dann ein Polynom mit Koeffizienten $a_i \in K$ wirklich „ist" (oder besser „sein soll"), eine Frage, die wir eigentlich schon bei der Einführung des charakteristischen Polynoms (nach (5.24)) hätten stellen sollen. Das Ziel dieses Kapitels ist eine befriedigende Antwort auf diese Frage. Dann werden wir noch die Polynomdivision (mit Rest) kennenlernen und uns mit dem Zusammenhang zwischen Nullstellen von Polynomen und dem (multiplikativen) „Abspalten" von Linearfaktoren beschäftigen.

Zu einem beliebigen Körper K betrachten wir die Menge

$$K^{\mathbb{N}} := \{f \mid f : \mathbb{N} \to K\},$$

d.h. ein Element $f \in K^{\mathbb{N}}$ ist eine Folge $f = (f_0, f_1, \ldots, f_n, \ldots)$ mit $f_n \in K$ für alle $n \in \mathbb{N}$.

(8.1) Def.: Zu $f, g \in K^{\mathbb{N}}$, $a \in K$ definieren wir

(i) $f + g \in K^{\mathbb{N}}$ durch $f + g := (f_0 + g_0, f_1 + g_1, \ldots, f_n + g_n, \ldots)$
(ii) $af \in K^{\mathbb{N}}$ durch $af := (af_0, af_1, \ldots, af_n, \ldots)$
(iii) $f \cdot g \in K^{\mathbb{N}}$ durch $f \cdot g := ((f \cdot g)_0, (f \cdot g)_1, \ldots, (f \cdot g)_n, \ldots)$,
wobei $(f \cdot g)_0 := f_0 \cdot g_0, (f \cdot g)_1 := f_0 \cdot g_1 + f_1 \cdot g_0, (f \cdot g)_2 := f_0 \cdot g_2 + f_1 \cdot g_1 + f_2 \cdot g_0$
und $(f \cdot g)_n := \sum\limits_{j=0}^{n} f_j \cdot g_{n-j} = \sum\limits_{\substack{(j,k) \in \mathbb{N} \times \mathbb{N} \\ j+k=n}} f_j \cdot g_k$.

Bem.: 1) Die Ausdrücke in (iii) sind den Ausdrücken nachgebildet, die beim „schulmäßigen" Multiplizieren von Polynomen auftreten:

$$(a_0 + a_1x + \ldots + a_nx^n) \cdot (b_0 + b_1x + \ldots + b_mx^m) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \ldots$$

2) Für $a \in K$, $f \in K^{\mathbb{N}}$ gilt $af = (a, 0, \ldots, 0, \ldots) \cdot f$.

(8.2) Fakt.

(i) $(K^{\mathbb{N}}, +)$ ist ein ∞-dimensionaler K-Vektorraum mit dem Nullelement $0 = (0, \ldots, 0, \ldots) \in K^{\mathbb{N}}$.
(ii) $(K^{\mathbb{N}}, +, \cdot)$ ist ein kommutativer Ring mit $1 = (1, 0, \ldots, 0, \ldots) \in K^{\mathbb{N}}$.

Bem.: Die Definition des „kommutativen Rings mit 1“ unterscheidet sich von der des Körpers (vgl. (2.4)) nur dadurch, daß auf die Forderung der Existenz von multiplikativen Inversen verzichtet wird. (Man fordert üblicherweise auch <u>nicht</u>, daß $1 \neq 0$ gilt, aber das ist für $K^{\mathbb{N}}$ natürlich erfüllt).

Bez.: $(K^{\mathbb{N}}, +, \cdot)$ heißt der Ring der formalen Potenzreihen über K, meist bezeichnet durch $K[[x]]$.

Der Nachweis der in (8.2) behaupteten Eigenschaften ist leicht. Am längsten dauert der Nachweis der Assoziativität der Multiplikation, den man wie folgt durchführen kann:
Seien $f, g, h \in K^{\mathbb{N}}$ und $n \in \mathbb{N}$. Dann gilt:

$$\begin{aligned}
((f \cdot g) \cdot h)_n &= \sum_{j+k=n} (f \cdot g)_j h_k = \sum_{j+k=n} \left(\sum_{l+m=j} f_l \cdot g_m \right) \cdot h_k = \sum_{l+m+k=n} f_l \cdot g_m \cdot h_k \\
(f \cdot (g \cdot h))_n &= \sum_{l+j=n} f_l \cdot (g \cdot h)_j = \sum_{l+j=n} f_l \cdot \left(\sum_{m+k=j} g_m \cdot h_k \right) = \sum_{l+m+k=n} f_l \cdot g_m \cdot h_k
\end{aligned}$$

(8.3) Fakt. Die Teilmenge

$$K[x] = \{f \in K^{\mathbb{N}} \mid f_n \neq 0 \text{ nur für endlich viele } n \in \mathbb{N}\}$$

ist abgeschlossen bezüglich $+$ und $\cdot$ und enthält $1 = (1, 0, \ldots, 0, \ldots)$, und ist ein Unterring (mit 1) von $(K^{\mathbb{N}}, +, \cdot)$.

Die Abgeschlossenheit bzgl. $\cdot$ folgt aus dem Beweis zu (8.5).

(8.4) Def.:

(i) $(K[x], +, \cdot)$ heißt der Polynomring von K.
(ii) Ist $f \in K[x] \setminus \{0\}$, so heißt

$$\operatorname{grad} f := \max\{i \in \mathbb{N} \mid f_i \neq 0\} \in \mathbb{N}$$

der Grad von f. Ist $f = 0 \in K[x]$, so setzen wir $\operatorname{grad} f = -\infty$.

(8.5) Fakt. Für alle $f, g \in K[x]$ gilt:

$$\operatorname{grad}(f \cdot g) = \operatorname{grad} f + \operatorname{grad} g.$$

Speziell folgt: $f \cdot g = 0 \Rightarrow f = 0$ oder $g = 0$.

Zu letzterer Eigenschaft sagt man, $(K[x], +, \cdot)$ sei „nullteilerfrei“.

Bew.: Ist $f = 0$ oder $g = 0$, so $f \cdot g = 0$, also

$$\operatorname{grad}(f \cdot g) = -\infty = \operatorname{grad} f + \operatorname{grad} g.$$

Ist $\operatorname{grad} f = m \in \mathbb{N}$, $\operatorname{grad} g = n \in \mathbb{N}$, so gilt $f_m \neq 0$, $g_n \neq 0$ und $f_i = 0$ für $i > m$, $g_j = 0$ für $j > n$. Daraus folgt

$$(f \cdot g)_{m+n} = \sum_{\substack{(i,j) \in \mathbb{N} \times \mathbb{N} \\ i+j=m+n}} f_i g_j = f_m \cdot g_n \neq 0$$

und $(f \cdot g)_k = 0$ für $k > m + n$. Also

$$\operatorname{grad}(f \cdot g) = m + n = \operatorname{grad} f + \operatorname{grad} g.$$

Um zur üblichen Darstellung von Polynomen zu kommen, führen wir folgende <u>Bezeichnung</u> ein:

$$x := (0, 1, 0, \ldots, 0, \ldots) \in K[x].$$

Außerdem definieren wir wie üblich $x^0 := (1, 0, \ldots, 0, \ldots)$ und rekursiv $x^{n+1} := x \cdot x^n$ für $n \in \mathbb{N}$.

In diesem Zugang zu den Polynomen ist also x keine „Variable“, sondern ein festes Element des Rings $K[x]$.

(8.6) Fakt. Die Menge $\{x^n \mid n \in \mathbb{N}\}$ ist eine Basis des K-Vektorraums $K[x]$. Es gilt $x^n = (\underbrace{0, \ldots, 0}_{n\text{-mal}}, 1, 0, \ldots) \in K[x]$.

Bew.: Die erste Behauptung folgt aus der zweiten. Die zweite beweisen wir durch Induktion. Die Gleichung $x^0 = (1, 0, \ldots, 0, \ldots)$, die nach Definition von x^0 gilt, ist der Induktionsanfang. Mit der Bezeichnung $\delta_{ij} := 0$ für $i \neq j$ und $\delta_{ii} := 1$ können wir $x = (\delta_{01}, \delta_{11}, \delta_{21}, \ldots)$ und - nach Induktionsvoraussetzung - $x^n = (\delta_{0n}, \delta_{1n}, \ldots, \delta_{nn}, \ldots)$ schreiben. Also gilt für jedes $i \in \mathbb{N}$:

$$(x^{n+1})_i = (x \cdot x^n)_i = \sum_{j+k=i} \delta_{j1} \delta_{kn} = \begin{cases} 1 \text{ falls } i = n+1 \\ 0 \text{ falls } i \neq n+1. \end{cases}$$

(8.7) Folgerung. Jedes Polynom $f \in K[x] \setminus \{0\}$ besitzt genau eine Darstellung

$$f = f_0 + f_1 x + f_2 x^2 + \ldots + f_m x^m \text{ mit } f_m \neq 0.$$

Es gilt dann $\operatorname{grad} f = m$.

Bem.: Bezüglich dieser Darstellung gehen die in (8.1) definierten Operationen in die für Polynome „üblichen“ über.

(8.8) Satz (Division mit Rest). *Seien $f \in K[x]$, $g \in K[x]$, und es gelte* $\operatorname{grad} f \geq \operatorname{grad} g \geq 0$. *Dann existieren $h, r \in K[x]$, so daß*

$$f = gh + r$$

und

$$\operatorname{grad} r < \operatorname{grad} g \qquad \textit{(möglicherweise } r = 0\textit{)}$$

gelten.

Bew.: Durch Induktion nach $n := \operatorname{grad} f$.

Induktionsanfang: Gilt $\operatorname{grad} f = 0$, so auch $\operatorname{grad} g = 0$, also $f = f_0, g = g_0$, und wir können als $h := \frac{g_0}{f_0}$ und $r = 0$ nehmen. Für den Induktionsschritt betrachten wir $f = \sum\limits_{i=0}^{n} f_i x^i$, $g = \sum\limits_{j=0}^{m} g_j x^j$ mit $0 \leq m \leq n$, $f_n \neq 0, g_m \neq 0$. Wir definieren

$$r_1 := f - \frac{f_n}{g_m} x^{n-m} \cdot g.$$

Dann gilt:

$$(*) \qquad f = g \cdot \left(\frac{f_n}{g_m} x^{n-m} \right) + r_1 \text{ und } \operatorname{grad} r_1 < n.$$

1. Fall: $\operatorname{grad} r_1 < \operatorname{grad} g$. Dann erhalten wir die Behauptung, indem wir $h := \frac{f_n}{g_m} x^{n-m}$ und $r := r_1$ setzen.

2. Fall: $\operatorname{grad} r_1 \geq \operatorname{grad} g$. Wegen $n > \operatorname{grad} r_1 \geq \operatorname{grad} g \geq 0$ ist auf r_1 die Induktionsvoraussetzung anwendbar und wir erhalten $h_1, r \in K[x]$, so daß $r_1 = gh_1 + r$ und $\operatorname{grad} r < \operatorname{grad} g$ gelten.

Dann folgt mit $(*)$:

$$f = g \cdot \left(\frac{f_n}{g_m} x^{n-m} + h_1 \right) + r.$$

Setzen wir $h := \frac{f_n}{g_m} x^{n-m} + h_1$, so erhalten wir wegen $\operatorname{grad} r < \operatorname{grad} g$ die Behauptung.

Bem.: Der Beweis von (8.8) besteht in dem üblichen Rechenverfahren zur Polynomdivision, das in die Form eines Beweises gebracht wurde. Umgekehrt liefert der Beweis auch dieses Rechenverfahren, das man beherrschen muß.

Einem Polynom $p = \sum\limits_{i=0}^{n} a_i x^i \in K[x]$ ordnen wir die Abbildung

$$\tilde{p} : K \to K, \ \tilde{p}(b) := \sum_{i=0}^{n} a_i b^i \text{ zu.}$$

Dann gilt für alle $p, q \in K[x]$:

$$\begin{aligned} (p+q)^{\sim} &= \tilde{p} + \tilde{q} \\ (p \cdot q)^{\sim} &= \tilde{p} \cdot \tilde{q}. \end{aligned}$$

Dabei bedeuten $+$ und $\cdot$ auf der linken Seite die Addition und Multiplikation von Polynomen, auf der rechten Seite die Addition und Multiplikation von Abbildungen von K nach

K! Anders ausgedrückt: Die Abbildung $p \to \tilde{p}$ ist ein Ringhomomorphismus von $K[x]$ in den Ring der Selbstabbildungen von K.

Bez.: Ist $p \in K[x]$, $b \in K$, so schreibt man für $\tilde{p}(b)$ meist einfach $p(b)$.

<u>Wichtige Bemerkung</u>: Allgemeiner kann man in $p = \sum_{i=0}^{n} a_i x^i \in K[x]$ auch quadratische Matrizen $A \in K^{m \times m}$ für beliebiges $m \in \mathbb{N}$ einsetzen:

$$p(A) := \sum_{i=0}^{n} a_i A^i \in K^{m \times m}.$$

Es gilt wieder:
$$\begin{aligned} (p+q)(A) &= p(A) + g(A) \\ (p \cdot q)(A) &= p(A) \cdot g(A). \end{aligned}$$

Beweis der zweiten Gleichung: Ist $p = \sum_{i=0}^{m} a_i x^i$, $q = \sum_{j=0}^{n} b_j x^j$, so gilt nach (8.1)(iii): $p \cdot q = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k$, also $(p \cdot q)(A) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) A^k$. Andererseits berechnen wir in

$$\begin{aligned} K^{m \times m} : p(A) \cdot q(A) &= \left(\sum_{i=0}^{m} a_i A^i \right) \left(\sum_{j=0}^{n} b_j A^j \right) = \sum_{i=0}^{m} \sum_{j=0}^{n} (a_i A^i)(b_j A^j) \\ &= \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) A^k. \end{aligned}$$

(8.9) Def.: Ein $a \in K$ heißt Nullstelle eines Polynoms $p \in K[x]$, falls $p(a) = 0$ gilt.

(8.10) Lemma. $a \in K$ ist genau dann Nullstelle von $p \in K[x] \setminus \{0\}$, wenn ein $q \in K[x]$ existiert, so daß $p = (x-a)q$ gilt.

Bew.: Offenbar folgt aus $p = (x-a)q$, daß

$$\tilde{p}(a) \stackrel{!}{=} (a-a)\tilde{q}(a) = 0 \text{ gilt.}$$

Gilt $p(a) = 0$, so wenden wir (8.8) auf $f := p$ und $g := x - a$ an und erhalten $q \in K[x]$, $r \in K[x]$ mit $\operatorname{grad} r < \operatorname{grad} g = 1$, so daß

$$p = (x-a)q + r$$

gilt. Aus $0 = p(a) = (a-a)q(a) + r(a)$ folgt $r(a) = 0$ und daraus wegen $\operatorname{grad} r < 1$: $r = 0$.

Bez.: $(x-a)^0 := 1$.

(8.11) Def.: Sei $p \in K[x] \setminus \{0\}$, $a \in K$. Wir bezeichnen mit $k(p,a) \in \mathbb{N}$ das Maximum aller $k \in \mathbb{N}$, für die ein $q \in K[x]$ existiert, so daß $p = (x-a)^k q$ gilt. Ist $k(p,a) > 0$, so gilt $p(a) = 0$ und $k(p,a)$ heißt die Vielfachheit (oder Ordnung) der Nullstelle a von p.

Bem.: 1) $k(p,a) = 0 \Leftrightarrow p(a) \neq 0$.
2) $\exists q \in K[x]$: $p = (x-a)^{k(p,a)} q$ und $q(a) \neq 0$.
3) $k(p,a) \leq \operatorname{grad} p$, denn aus 2) folgt: $\operatorname{grad} p = k(p,a) + \operatorname{grad} q \geq k(p,a)$.

(8.12) Satz. *Seien $p, f, g \in K[x]$, $a \in K$ und es gelte $p = f \cdot g$. Dann gilt*

$$k(p,a) = k(f,a) + k(g,a).$$

Bew.:

(i) Ist $f = (x-a)^{k_1} q_1$, $g = (x-a)^{k_2} q_2$, so gilt

$$p = f \cdot g = (x-a)^{k_1+k_2} q_1 q_2.$$

Daraus folgt $k(p,a) \geq k(f,a) + k(g,a)$.

(ii) Ist $p = (x-a)^k q$ mit $k = k(p,a)$ und $f = (x-a)^{k_1} q_1$ mit $q_1(a) \neq 0$ ($\Rightarrow k_1 = k(f,a)$) und $g = (x-a)^{k_2} q_2$ mit $q_2(a) \neq 0$ ($\Rightarrow k_2 = k(g,a)$), so folgt

$$p = (x-a)^k q = f \cdot g = (x-a)^{k_1+k_2} q_1 q_2.$$

Wegen (i) gilt $k = k(p,a) \geq k_1 + k_2$, also

$$(x-a)^{k_1+k_2} \left((x-a)^{k-(k_1+k_2)} q - q_1 q_2 \right) = 0.$$

Da $K[x]$ nulleiterfrei ist, vgl. (8.5), und $(x-a)^{k_1+k_2} \in K[x] \setminus \{0\}$ gilt, folgt $(x-a)^{k-(k_1+k_2)} q - q_1 q_2 = 0$. Wenn $k > k_1 + k_2$ gelten würde, so folgte $q_1(a) q_2(a) = 0$, im Widerspruch zu $q_1(a) \neq 0, q_2(a) \neq 0$. Also gilt $k = k(p,a) \leq k_1 + k_2 = k(f,a) + k(g,a)$.

(8.13) Folgerung. Sind $a_1, \ldots, a_s$ verschiedene Nullstellen von $p \in K[x] \setminus \{0\}$ mit den Vielfachheiten $k_1 = k(p,a_1), \ldots, k_s = k(p,a_s)$, so existiert ein $q \in K[x]$ mit:

$$p = (x-a_1)^{k_1} \cdot \ldots \cdot (x-a_s)^{k_s} q.$$

Speziell gilt $\sum_{i=1}^{s} k_i \leq \operatorname{grad} p$.

Bew.: Induktion nach s. Der Induktionsanfang $s = 1$ ist gerade die Definition (8.11). Nach Induktionsvoraussetzung existiert $\overline{q} \in K[x]$ mit

$$p = (x-a_1)^{k_1} \cdot \ldots \cdot (x-a_{s-1})^{k_{s-1}} \overline{q}.$$

Aus (8.12) folgt $k_s = k(p,a_s) = k(\overline{q},a_s)$. Also existiert $q \in K[x]$ mit $\overline{q} = (x-a)^{k_s} q$. Daraus folgt die Behauptung

(8.14) Def.: Ein $p \in K[x] \setminus \{0\}$ zerfällt über K (in Linearfaktoren), falls ein $a \in K$ und $a_1, \ldots, a_s \in K$ und $k_1, \ldots, k_s \in \mathbb{N}$ existieren, so daß gilt

$$p = a(x-a_1)^{k_1} \cdot \ldots \cdot (x-a_s)^{k_s} =: a \prod_{i=1}^{s} (x-a_i)^{k_i}.$$

(8.15) Folgerung (aus (8.13)): $p \in K[x] \setminus \{0\}$ zerfällt genau dann über K, wenn verschiedene $a_1, \ldots, a_s \in K$ existieren, so daß

$$\operatorname{grad} p = \sum_{i=1}^{s} k(p, a_i)$$

gilt.

(8.16) Folgerung. Sind $p, f, g \in K[x] \setminus \{0\}$, gilt $p = f \cdot g$ und zerfällt p über K, so zerfallen auch f und g über K.

Bew.: Nach (8.15) existieren verschiedene $a_1, \ldots, a_s \in K$ mit $\operatorname{grad} p = \sum\limits_{i=1}^{s} k(p, a_i)$.

Nach (8.12) gilt $k(p, a_i) = k(f, a_i) + k(g, a_i)$ für $1 \leq i \leq s$, also

$$\operatorname{grad} f + \operatorname{grad} g = \operatorname{grad} p = \sum_{i=1}^{s} k(p, a_i) = \underbrace{\sum_{i=1}^{s} k(f, a_i)}_{\leq \operatorname{grad} f} + \underbrace{\sum_{i=1}^{s} k(g, a_i)}_{\leq \operatorname{grad} g}.$$

Daraus folgt $\sum\limits_{i=1}^{s} k(f, a_i) = \operatorname{grad} f$, $\sum\limits_{i=1}^{s} k(g, a_i) = \operatorname{grad} g$, so daß f und g nach (8.15) über K zerfallen.

Zum Abschluß wollen wir uns überlegen, wie nun eigentlich das charakteristische Polynom eines Endomorphismus oder einer quadratischen Matrix definiert wird. Das ist nicht unproblematisch, da wir in der Formel $P_L(x) = \det(L - x\,\mathrm{id})$ das x nicht einfach als Körperelement interpretieren können. Der zu diesem Zeitpunkt beste Weg ist zu erkennen, daß man natürlich auch die Determinante einer Matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ definieren kann, deren Einträge a_{ij} Elemente eines festen kommutativen Rings R mit 1 sind, nämlich durch die Leibnizformel $\det A = \sum\limits_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} \in R$. Für zwei solche Matrizen A und B ist das Matrizenprodukt AB definiert und es gilt $\det(AB) = \det A \det B$. Das kann man mit einer recht unangenehmen Rechnung direkt nachprüfen. Besser wäre es, wie in Kap. 4 und 5 vorzugehen, aber dabei den Körper K durch einen kommutativen Ring R mit 1 zu ersetzen. Den K-Vektorräumen entsprächen dann „freie R-Moduln“ und den Vektorraumhomomorphismen entsprächen „R-Modulhomomorphismen“, die (im Fall endlich erzeugter R-Moduln) gerade durch Matrizen mit Einträgen aus R zusammenhängen (für Interessierte sei auf Kapitel 9 des Buchs Kowalsky/Michler: Lineare Algebra, deGruyter 1995, verwiesen). Wir sehen hier ein schönes Beispiel dafür, wie man manchmal von der Mathematik zu allgemeineren Begriffen gezwungen wird.

Jedenfalls kann man dann für eine Matrix $A = (a_{ij})_{1 \leq i,j \leq n} \in K^{n \times n}$ die Matrix $A - xE_n$ als Matrix mit Einträgen im Ring $R = K[x]$ betrachten, und so ist das charakteristische

Polynom

$$P_A = \det(A - xE_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)(a_{1\sigma(1)} - x\delta_{1\sigma(1)}) \cdot \ldots \cdot (a_{n\sigma(n)} - x\delta_{n\sigma(n)})$$

von A definiert. Ist $B \in \mathrm{GL}_n(K)$, so gilt

$$\begin{aligned} P_{B^{-1}AB} &= \det(B^{-1}AB - xE_n) = \det(B^{-1}(A - xE_n)B) \\ &= \det B^{-1} P_A \det B = P_A. \end{aligned}$$

Ist nun L Endomorphismus eines n-dimensionalen K-Vektorraums, so wählen wir eine geordnete Basis $\mathcal{G}$ von V, setzen $A := \mathrm{Mat}_{\mathcal{G}}^{\mathcal{G}}(L)$ und definieren das charakteristische Polynom $P_L \in K[x]$ von L durch $P_L := P_A$. Aufgrund der vorangehenden Gleichung ist das unabhängig von der Wahl von $\mathcal{G}$, vgl. (4.19).