§10.2 Begleitmatrix, Satz von Cayley-Hamilton und Minimalpolynom

[Arthur Cayley *1821 †1895;
William Rowan Hamilton *1805, †1865]

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ *mit* $g \neq 0$*. Dann gibt es genau ein Paar* $(q, r) \in K[X]^2$ *mit* $\deg r < \deg g$ *und* $f = gq + r$*.*

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ *mit* $g \neq 0$*. Dann gibt es genau ein Paar* $(q, r) \in K[X]^2$ *mit* $\deg r < \deg g$ *und* $f = gq + r$*. Man nennt* q *den* ***Quotienten*** *und* r *den* ***Rest*** *bei Division von* f *durch* g*.*

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ *mit* $g \neq 0$. *Dann gibt es genau ein Paar* $(q, r) \in K[X]^2$ *mit* $\deg r < \deg g$ *und* $f = gq + r$. *Man nennt* q *den* *Quotienten* *und* r *den* *Rest* *bei Division von* f *durch* g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$.

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ *mit* $g \neq 0$. *Dann gibt es genau ein Paar* $(q, r) \in K[X]^2$ *mit* $\deg r < \deg g$ *und* $f = gq + r$. *Man nennt* q *den Quotienten und* r *den Rest bei Division von* f *durch* g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$. Dann gilt $r_1 - r_2 = g(q_2 - q_1) \in (g)$ und wegen $\deg(r_1 - r_2) < \deg g$ daher $r_1 - r_2 = 0$.

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es genau ein Paar $(q, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f = gq + r$. Man nennt q den Quotienten und r den Rest bei Division von f durch g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$. Dann gilt $r_1 - r_2 = g(q_2 - q_1) \in (g)$ und wegen $\deg(r_1 - r_2) < \deg g$ daher $r_1 - r_2 = 0$. Also $r_1 = r_2$.

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es genau ein Paar $(q, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f = gq + r$. Man nennt q den Quotienten und r den Rest bei Division von f durch g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$. Dann gilt $r_1 - r_2 = g(q_2 - q_1) \in (g)$ und wegen $\deg(r_1 - r_2) < \deg g$ daher $r_1 - r_2 = 0$. Also $r_1 = r_2$. Folglich $g(q_1 - q_2) = 0$ und schließlich $q_1 = q_2$.

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es genau ein Paar $(q, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f = gq + r$. Man nennt q den Quotienten und r den Rest bei Division von f durch g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$. Dann gilt $r_1 - r_2 = g(q_2 - q_1) \in (g)$ und wegen $\deg(r_1 - r_2) < \deg g$ daher $r_1 - r_2 = 0$. Also $r_1 = r_2$. Folglich $g(q_1 - q_2) = 0$ und schließlich $q_1 = q_2$.

Die Existenz beweisen wir durch Induktion nach dem Grad von f:

Induktionsanfang: Ist $\deg f < \deg g$, so setzen wir $(q, r) := (0, f)$.

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es genau ein Paar $(q, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f = gq + r$. Man nennt q den Quotienten und r den Rest bei Division von f durch g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$. Dann gilt $r_1 - r_2 = g(q_2 - q_1) \in (g)$ und wegen $\deg(r_1 - r_2) < \deg g$ daher $r_1 - r_2 = 0$. Also $r_1 = r_2$. Folglich $g(q_1 - q_2) = 0$ und schließlich $q_1 = q_2$.

Die Existenz beweisen wir durch Induktion nach dem Grad von f:

Induktionsanfang: Ist $\deg f < \deg g$, so setzen wir $(q, r) := (0, f)$.

Induktionsschritt: Sei $\deg f \geq \deg g$ und die Behauptung schon bewiesen, wenn f durch ein Polynom von kleinerem Grad ersetzt wird.

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es genau ein Paar $(q, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f = gq + r$. Man nennt q den Quotienten und r den Rest bei Division von f durch g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$. Dann gilt $r_1 - r_2 = g(q_2 - q_1) \in (g)$ und wegen $\deg(r_1 - r_2) < \deg g$ daher $r_1 - r_2 = 0$. Also $r_1 = r_2$. Folglich $g(q_1 - q_2) = 0$ und schließlich $q_1 = q_2$.

Die Existenz beweisen wir durch Induktion nach dem Grad von f:

Induktionsanfang: Ist $\deg f < \deg g$, so setzen wir $(q, r) := (0, f)$.

Induktionsschritt: Sei $\deg f \geq \deg g$ und die Behauptung schon bewiesen, wenn f durch ein Polynom von kleinerem Grad ersetzt wird. Wähle $a \in K^\times$ und $k \in \mathbb{N}_0$ derart, dass f und $aX^k g$ denselben Grad und denselben Leitkoeffizienten haben.

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es genau ein Paar $(q, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f = gq + r$. Man nennt q den Quotienten und r den Rest bei Division von f durch g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$. Dann gilt $r_1 - r_2 = g(q_2 - q_1) \in (g)$ und wegen $\deg(r_1 - r_2) < \deg g$ daher $r_1 - r_2 = 0$. Also $r_1 = r_2$. Folglich $g(q_1 - q_2) = 0$ und schließlich $q_1 = q_2$.

Die Existenz beweisen wir durch Induktion nach dem Grad von f:

Induktionsanfang: Ist $\deg f < \deg g$, so setzen wir $(q, r) := (0, f)$.

Induktionsschritt: Sei $\deg f \geq \deg g$ und die Behauptung schon bewiesen, wenn f durch ein Polynom von kleinerem Grad ersetzt wird. Wähle $a \in K^\times$ und $k \in \mathbb{N}_0$ derart, dass f und $aX^k g$ denselben Grad und denselben Leitkoeffizienten haben. Dann hat $f_0 := f - aX^k g$ einen kleineren Grad als f und es gibt nach Induktionsvoraussetzung $(q_0, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f_0 = gq_0 + r$.

Proposition und Sprechweise (Polynomdivision mit Rest)

Seien $f, g \in K[X]$ mit $g \neq 0$. Dann gibt es genau ein Paar $(q, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f = gq + r$. Man nennt q den Quotienten und r den Rest bei Division von f durch g.

Beweis.

Um die Eindeutigkeit zu beweisen, seien $(q_i, r_i) \in K[X]^2$ mit $\deg r_i < \deg g$ und $f = gq_i + r_i$ für $i \in \{1, 2\}$. Dann gilt $r_1 - r_2 = g(q_2 - q_1) \in (g)$ und wegen $\deg(r_1 - r_2) < \deg g$ daher $r_1 - r_2 = 0$. Also $r_1 = r_2$. Folglich $g(q_1 - q_2) = 0$ und schließlich $q_1 = q_2$.

Die Existenz beweisen wir durch Induktion nach dem Grad von f:

Induktionsanfang: Ist $\deg f < \deg g$, so setzen wir $(q, r) := (0, f)$.

Induktionsschritt: Sei $\deg f \geq \deg g$ und die Behauptung schon bewiesen, wenn f durch ein Polynom von kleinerem Grad ersetzt wird. Wähle $a \in K^\times$ und $k \in \mathbb{N}_0$ derart, dass f und $aX^k g$ denselben Grad und denselben Leitkoeffizienten haben. Dann hat $f_0 := f - aX^k g$ einen kleineren Grad als f und es gibt nach Induktionsvoraussetzung $(q_0, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f_0 = gq_0 + r$. Es folgt $f = f_0 + aX^k g = g(q_0 + aX^k) + r = gq + r$ für $q := q_0 + aX^k$. $\square$

Satz

Im Polynomring $K[X]$ ist jedes Ideal ein Hauptideal.

Satz

Im Polynomring $K[X]$ ist jedes Ideal ein Hauptideal.

Beweis.

Sei I ein Ideal von $K[X]$. Ist $I = \{0\}$, so ist $I = (0)$. Also bleibt nur der Fall zu betrachten, dass es ein $g \in K[X] \setminus \{0\}$ gibt mit $g \in I$.

Satz

Im Polynomring $K[X]$ ist jedes Ideal ein Hauptideal.

Beweis.

Sei I ein Ideal von $K[X]$. Ist $I = \{0\}$, so ist $I = (0)$. Also bleibt nur der Fall zu betrachten, dass es ein $g \in K[X] \setminus \{0\}$ gibt mit $g \in I$. Wir wählen ein solches g von kleinstmöglichem Grad und behaupten $I = (g)$.

Satz

Im Polynomring $K[X]$ ist jedes Ideal ein Hauptideal.

Beweis.

Sei I ein Ideal von $K[X]$. Ist $I = \{0\}$, so ist $I = (0)$. Also bleibt nur der Fall zu betrachten, dass es ein $g \in K[X] \setminus \{0\}$ gibt mit $g \in I$. Wir wählen ein solches g von kleinstmöglichem Grad und behaupten $I = (g)$. Die Inklusion $I \supseteq (g)$ ist klar.

Satz

Im Polynomring $K[X]$ ist jedes Ideal ein Hauptideal.

Beweis.

Sei I ein Ideal von $K[X]$. Ist $I = \{0\}$, so ist $I = (0)$. Also bleibt nur der Fall zu betrachten, dass es ein $g \in K[X] \setminus \{0\}$ gibt mit $g \in I$. Wir wählen ein solches g von kleinstmöglichem Grad und behaupten $I = (g)$. Die Inklusion $I \supseteq (g)$ ist klar. Um $I \subseteq (g)$ zu beweisen, sei $f \in I$. Zu zeigen ist $f \in (g)$.

Satz

Im Polynomring $K[X]$ ist jedes Ideal ein Hauptideal.

Beweis.

Sei I ein Ideal von $K[X]$. Ist $I = \{0\}$, so ist $I = (0)$. Also bleibt nur der Fall zu betrachten, dass es ein $g \in K[X] \setminus \{0\}$ gibt mit $g \in I$. Wir wählen ein solches g von kleinstmöglichem Grad und behaupten $I = (g)$. Die Inklusion $I \supseteq (g)$ ist klar. Um $I \subseteq (g)$ zu beweisen, sei $f \in I$. Zu zeigen ist $f \in (g)$. Wähle $q, r \in K[X]$ mit $\deg r < \deg g$ und $f = gq + r$.

Satz

Im Polynomring $K[X]$ ist jedes Ideal ein Hauptideal.

Beweis.

Sei I ein Ideal von $K[X]$. Ist $I = \{0\}$, so ist $I = (0)$. Also bleibt nur der Fall zu betrachten, dass es ein $g \in K[X] \setminus \{0\}$ gibt mit $g \in I$. Wir wählen ein solches g von kleinstmöglichem Grad und behaupten $I = (g)$. Die Inklusion $I \supseteq (g)$ ist klar. Um $I \subseteq (g)$ zu beweisen, sei $f \in I$. Zu zeigen ist $f \in (g)$. Wähle $q, r \in K[X]$ mit $\deg r < \deg g$ und $f = gq + r$. Dann gilt $r = f - gq \in I$ und nach Wahl von g muss $r = 0$ gelten. Dann aber $f = gq \in (g)$. $\square$

Definition

Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Definition

Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Korollar

Sei I ein Ideal von $K[X]$ mit $I \neq \{0\}$. Dann gibt es genau ein normiertes $p \in K[X]$ mit $I = (p)$.

Definition

Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Korollar

Sei I ein Ideal von $K[X]$ mit $I \neq \{0\}$. Dann gibt es genau ein normiertes $p \in K[X]$ mit $I = (p)$.

Beweis.

Die Existenz ist klar.

Definition

Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Korollar

Sei I ein Ideal von $K[X]$ mit $I \neq \{0\}$. Dann gibt es genau ein normiertes $p \in K[X]$ mit $I = (p)$.

Beweis.

Die Existenz ist klar. Zur Eindeutigkeit: Seien $p, q \in K[X]$ normiert mit $(p) = I = (q)$.

Definition

Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Korollar

Sei I ein Ideal von $K[X]$ mit $I \neq \{0\}$. Dann gibt es genau ein normiertes $p \in K[X]$ mit $I = (p)$.

Beweis.

Die Existenz ist klar. Zur Eindeutigkeit: Seien $p, q \in K[X]$ normiert mit $(p) = I = (q)$. Dann $\deg p \geq \deg(q)$ wegen $p \in (q)$ und

Definition
Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Korollar
Sei I ein Ideal von $K[X]$ mit $I \neq \{0\}$. Dann gibt es genau ein normiertes $p \in K[X]$ mit $I = (p)$.

Beweis.
Die Existenz ist klar. Zur Eindeutigkeit: Seien $p, q \in K[X]$ normiert mit $(p) = I = (q)$. Dann $\deg p \geq \deg(q)$ wegen $p \in (q)$ und $\deg q \geq \deg(p)$ wegen $q \in (p)$,

Definition

Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Korollar

Sei I ein Ideal von $K[X]$ mit $I \neq \{0\}$. Dann gibt es genau ein normiertes $p \in K[X]$ mit $I = (p)$.

Beweis.

Die Existenz ist klar. Zur Eindeutigkeit: Seien $p, q \in K[X]$ normiert mit $(p) = I = (q)$. Dann $\deg p \geq \deg(q)$ wegen $p \in (q)$ und $\deg q \geq \deg(p)$ wegen $q \in (p)$, also $\deg p = \deg q$.

Definition

Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Korollar

Sei I ein Ideal von $K[X]$ mit $I \neq \{0\}$. Dann gibt es genau ein normiertes $p \in K[X]$ mit $I = (p)$.

Beweis.

Die Existenz ist klar. Zur Eindeutigkeit: Seien $p, q \in K[X]$ normiert mit $(p) = I = (q)$. Dann $\deg p \geq \deg(q)$ wegen $p \in (q)$ und $\deg q \geq \deg(p)$ wegen $q \in (p)$, also $\deg p = \deg q$. Weiter gilt $p - q \in (p)$ und daher $p - q = 0$ oder $\deg(p - q) \geq \deg p$.

Definition

Ein Polynom $p \in K[X]$ heißt normiert, wenn $p \neq 0$ und der Leitkoeffizient von p gleich 1 ist.

Korollar

Sei I ein Ideal von $K[X]$ mit $I \neq \{0\}$. Dann gibt es genau ein normiertes $p \in K[X]$ mit $I = (p)$.

Beweis.

Die Existenz ist klar. Zur Eindeutigkeit: Seien $p, q \in K[X]$ normiert mit $(p) = I = (q)$. Dann $\deg p \geq \deg(q)$ wegen $p \in (q)$ und $\deg q \geq \deg(p)$ wegen $q \in (p)$, also $\deg p = \deg q$. Weiter gilt $p - q \in (p)$ und daher $p - q = 0$ oder $\deg(p - q) \geq \deg p$. Letzteres ist unmöglich, also gilt $p = q$. □

Proposition

Sei $p \in K[X]$ ein Polynom vom Grad $n \in \mathbb{N}_0$. Dann ist das Ideal (p) des kommutativen Ringes $K[X]$ ein UR des VRs $K[X]$ und $(\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}})$ eine Basis des QuotVRs $K[X]/(p)$.

Proposition

Sei $p \in K[X]$ ein Polynom vom Grad $n \in \mathbb{N}_0$. Dann ist das Ideal (p) des kommutativen Ringes $K[X]$ ein UR des VRs $K[X]$ und $(\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}})$ eine Basis des QuotVRs $K[X]/(p)$.

Beweis.

Zu zeigen:

(a) $\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}$ sind linear unabhängig in $K[X]/(p)$.

(b) $\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}$ erzeugen $K[X]/(p)$.

Proposition

Sei $p \in K[X]$ ein Polynom vom Grad $n \in \mathbb{N}_0$. Dann ist das Ideal (p) des kommutativen Ringes $K[X]$ ein UR des VRs $K[X]$ und $(\overline{1}, \overline{X}, \dots, \overline{X^{n-1}})$ eine Basis des QuotVRs $K[X]/(p)$.

Beweis.

Zu zeigen:

(a) $\overline{1}, \overline{X}, \dots, \overline{X^{n-1}}$ sind linear unabhängig in $K[X]/(p)$.

(b) $\overline{1}, \overline{X}, \dots, \overline{X^{n-1}}$ erzeugen $K[X]/(p)$.

Zu (a). Seien also $a_0, \dots, a_{n-1} \in K$ mit $\sum_{k=0}^{n-1} a_k \overline{X^k} = 0$. Zu zeigen ist $a_0 = \dots = a_{n-1} = 0$. Schreibt man $h := \sum_{k=0}^{n-1} a_k X^k \in K[X]$, so ist $h = 0$ zu zeigen. Nun gilt $\overline{h} = \sum_{k=0}^{n-1} a_k \overline{X^k} = 0$ und daher $h \in (p)$. Wegen $\deg h < n = \deg p$ folgt $h = 0$.

Proposition

Sei $p \in K[X]$ ein Polynom vom Grad $n \in \mathbb{N}_0$. Dann ist das Ideal (p) des kommutativen Ringes $K[X]$ ein UR des VRs $K[X]$ und $(\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}})$ eine Basis des QuotVRs $K[X]/(p)$.

Beweis.

Zu zeigen:

(a) $\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}$ sind linear unabhängig in $K[X]/(p)$.

(b) $\overline{1}, \overline{X}, \ldots, \overline{X^{n-1}}$ erzeugen $K[X]/(p)$.

Zu (a). Seien also $a_0, \ldots, a_{n-1} \in K$ mit $\sum_{k=0}^{n-1} a_k \overline{X^k} = 0$. Zu zeigen ist $a_0 = \ldots = a_{n-1} = 0$. Schreibt man $h := \sum_{k=0}^{n-1} a_k X^k \in K[X]$, so ist $h = 0$ zu zeigen. Nun gilt $\overline{h} = \sum_{k=0}^{n-1} a_k \overline{X^k} = 0$ und daher $h \in (p)$. Wegen $\deg h < n = \deg p$ folgt $h = 0$.

Zu (b). Sei $f \in K[X]$. Zu zeigen ist, dass es ein $r \in K[X]$ mit $\deg r < n$ und $\overline{f} = \overline{r}$ in $K[X]/(p)$ gibt. Man findet $(q, r) \in K[X]^2$ mit $\deg r < \deg g$ und $f = pq + r$. Dann $f - r \in (p)$ und daher $\overline{f} = \overline{r}$ in $K[X]/(p)$ wie gewünscht. □

Proposition und Definition

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$ mit $a_0, \ldots, a_{n-1} \in K$ ein normiertes Polynom. Dann ist

$$f\colon K[X]/(p) \to K[X]/(p),\ \overline{q} \mapsto \overline{Xq} \quad (q \in K[X])$$

wohldefiniert und linear.

Proposition und Definition

Sei $p = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0 \in K[X]$ mit $a_0, \dots, a_{n-1} \in K$ ein normiertes Polynom. Dann ist

$$f\colon K[X]/(p) \to K[X]/(p),\ \overline{q} \mapsto \overline{Xq} \quad (q \in K[X])$$

wohldefiniert und linear. Die Darstellungsmatrix $C_p := M(f, \underline{v})$ von f bezüglich der Basis $\underline{v} := (\overline{1}, \overline{X}, \dots, \overline{X^{n-1}})$ von $K[X]/(p)$ nennen wir die Begleitmatrix von p.

Proposition und Definition

Sei $p = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \in K[X]$ mit $a_0, \dots, a_{n-1} \in K$ ein normiertes Polynom. Dann ist

$$f \colon K[X]/(p) \to K[X]/(p),\ \overline{q} \mapsto \overline{Xq} \quad (q \in K[X])$$

wohldefiniert und linear. Die Darstellungsmatrix $C_p := M(f, \underline{v})$ von f bezüglich der Basis $\underline{v} := (\overline{1}, \overline{X}, \dots, \overline{X^{n-1}})$ von $K[X]/(p)$ nennen wir die Begleitmatrix von p. Es gilt

$$C_p = \begin{pmatrix} 0 & 0 & \cdots & & 0 & -a_0 \\ 1 & 0 & & & \vdots & -a_1 \\ 0 & 1 & \ddots & & \vdots & -a_2 \\ 0 & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & & \ddots & 0 & \vdots \\ 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

Satz

Sei $p \in K[X]$ ein normiertes Polynom vom Grad n. Dann ist p bis auf das Vorzeichen das charakteristische Polynom seiner eigenen Begleitmatrix, das heißt

$$p = (-1)^n \chi_{C_p}.$$

Definition

(a) Ist f eine Selbstabbildung der Menge M, so definiert man

$$f^k := \underbrace{f \circ \cdots \circ f}_{k\text{-mal}} \in M^M$$

für jedes $k \in \mathbb{N}_0$, wobei $f^0 := \mathrm{id}_M$. Insbesondere ist $f^k \in \mathrm{End}(V)$ für jeden VR V und jedes $f \in \mathrm{End}(V)$ erklärt.

Definition

(a) Ist f eine Selbstabbildung der Menge M, so definiert man

$$f^k := \underbrace{f \circ \cdots \circ f}_{k\text{-mal}} \in M^M$$

für jedes $k \in \mathbb{N}_0$, wobei $f^0 := \mathrm{id}_M$. Insbesondere ist $f^k \in \mathrm{End}(V)$ für jeden VR V und jedes $f \in \mathrm{End}(V)$ erklärt.

(b) Ist $n \in \mathbb{N}_0$ und $A \in K^{n \times n}$, so definiert man

$$A^k := \underbrace{A \cdots A}_{k\text{-mal}} \in K^{n \times n},$$

wobei $A^0 := I_n$.

Definition

(a) Ist f eine Selbstabbildung der Menge M, so definiert man

$$f^k := \underbrace{f \circ \cdots \circ f}_{k\text{-mal}} \in M^M$$

für jedes $k \in \mathbb{N}_0$, wobei $f^0 := \mathrm{id}_M$. Insbesondere ist $f^k \in \mathrm{End}(V)$ für jeden VR V und jedes $f \in \mathrm{End}(V)$ erklärt.

(b) Ist $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$, so definiert man

$$A^k := \underbrace{A \cdots A}_{k\text{-mal}} \in K^{n\times n},$$

wobei $A^0 := I_n$.

Beispiel

Ist $\varphi \in \mathbb{R}$ und $k \in \mathbb{N}_0$, so gilt für die Drehung $R_\varphi \in \mathrm{End}(\mathbb{R}^2)$

$$(R_\varphi)^k = R_{k\varphi}.$$

Erinnerung

Sei V ein K-VR. Dann ist $\mathrm{End}(V) := \mathrm{Hom}(V, V)$ ein K-VR und für alle $f, g, h \in \mathrm{End}(V)$ und $\lambda \in K$ gilt

$$\begin{aligned} f \circ (g + h) &= f \circ g + f \circ h, \\ (f + g) \circ h &= f \circ h + g \circ h \quad \text{und} \\ (\lambda f) \circ g &= \lambda(f \circ g) = f \circ (\lambda g). \end{aligned}$$

Definition und Proposition

(a) Sei V ein K-VR und $f \in \mathrm{End}(V)$. Dann ist

$$K[f] := \left\{ \sum_{k=0}^{n} a_k f^k \mid n \in \mathbb{N}_0, a_0, \ldots, a_n \in K \right\}$$

zusammen mit der punktweisen Addition und der Hintereinanderschaltung als Multiplikation ein kommutativer Ring.

Definition und Proposition

(a) Sei V ein K-VR und $f \in \mathrm{End}(V)$. Dann ist

$$K[f] := \left\{ \sum_{k=0}^{n} a_k f^k \mid n \in \mathbb{N}_0, a_0, \ldots, a_n \in K \right\}$$

zusammen mit der punktweisen Addition und der Hintereinanderschaltung als Multiplikation ein kommutativer Ring.

(b) Sei $n \in \mathbb{N}_0$ und $A \in K^{n \times n}$. Dann ist

$$K[A] := \left\{ \sum_{k=0}^{n} a_k A^k \mid n \in \mathbb{N}_0, a_0, \ldots, a_n \in K \right\}$$

zusammen mit der Addition und Multiplikation von Matrizen ein kommutativer Ring.

Satz und Definition

(a) *Sei V ein K-VR und $f \in \mathrm{End}(V)$. Dann gibt es genau einen Ringhomomorphismus $\psi\colon K[X] \to K[f]$ mit*

$$\psi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} a_k f^k$$

für alle $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in K$. Ist $p \in K[X]$, so schreibt man auch $p(f)$ statt $\psi(p)$ („p ausgewertet in f“). Dass ψ ein Ringhomomorphismus ist, heißt dann $(p+q)(f) = p(f) + q(f)$, $1(f) = \mathrm{id}_V$ und $(pq)(f) = p(f) \circ q(f)$ für alle $p, q \in K[X]$.

Satz und Definition

(a) *Sei V ein K-VR und $f \in \mathrm{End}(V)$. Dann gibt es genau einen Ringhomomorphismus $\psi\colon K[X] \to K[f]$ mit*

$$\psi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} a_k f^k$$

für alle $n \in \mathbb{N}_0$ und $a_0, \ldots, a_n \in K$. Ist $p \in K[X]$, so schreibt man auch $p(f)$ statt $\psi(p)$ („p ausgewertet in f"). Dass ψ ein Ringhomomorphismus ist, heißt dann $(p+q)(f) = p(f) + q(f)$, $1(f) = \mathrm{id}_V$ und $(pq)(f) = p(f) \circ q(f)$ für alle $p, q \in K[X]$.

Beweis.

(a) Überprüfe zunächst, dass $\varphi\colon K \to K[f],\ a \mapsto a\,\mathrm{id}_V$ ein Ringhomomorphismus ist. Dann erhält man $\psi\colon K[X] \to K[f]$ mit

$$\psi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} \varphi(a_k) f^k = \sum_{k=0}^{n} \underbrace{(a_k\,\mathrm{id}_V) \circ f^k}_{=a_k(\mathrm{id}_V \circ f^k) = a_k f^k} .$$

Satz und Definition

(b) *Sei* $n \in \mathbb{N}_0$ *und* $A \in K^{n\times n}$*. Dann gibt es genau einen Ringhomomorphismus* $\psi\colon K[X] \to K[A]$ *mit*

$$\psi\left(\sum_{k=0}^{n} a_k X^k\right) = \sum_{k=0}^{n} a_k A^k$$

für alle $n \in \mathbb{N}_0$ *und* $a_0, \dots, a_n \in K$*. Ist* $p \in K[X]$*, so schreibt man auch* $p(A)$ *statt* $\psi(p)$ *(„p ausgewertet in A“). Dass* ψ *ein Ringhomomorphismus ist, heißt dann* $(p+q)(A) = p(A) + q(A)$*,* $1(A) = I_n$ *und* $(pq)(A) = (p(A))(q(A))$ *für alle* $p, q \in K[X]$*.*

Satz (Cayley-Hamilton)

(a) *Für jeden Endomorphismus f eines endlichdimensionalen VRs gilt $\chi_f(f) = 0$.*

(b) *Für jede quadratische Matrix A über einem Körper gilt $\chi_A(A) = 0$.*

Satz (Cayley-Hamilton)

(a) *Für jeden Endomorphismus f eines endlichdimensionalen VRs gilt $\chi_f(f) = 0$.*

(b) *Für jede quadratische Matrix A über einem Körper gilt $\chi_A(A) = 0$.*

Beweis.

(a) Sei V ein endlichdimensionaler VR, $f \in \mathrm{End}(V)$ und $v \in V$. Zu zeigen ist $(\chi_f(f))(v) = 0$.

Satz (Cayley-Hamilton)

(a) *Für jeden Endomorphismus f eines endlichdimensionalen VRs gilt $\chi_f(f) = 0$.*

(b) *Für jede quadratische Matrix A über einem Körper gilt $\chi_A(A) = 0$.*

Beweis.

(a) Sei V ein endlichdimensionaler VR, $f \in \mathrm{End}(V)$ und $v \in V$. Zu zeigen ist $(\chi_f(f))(v) = 0$. Wir wählen das kleinste $m \in \mathbb{N}_0$ derart, dass $v, f(v), \ldots, f^m(v)$ linear abhängig sind. Dann gibt es $a_0, \ldots, a_{m-1} \in K$ mit $f^m(v) + a_{m-1}f^{m-1}(v) + \cdots + a_1 f(v) + a_0 v = 0$.

Satz (Cayley-Hamilton)

(a) *Für jeden Endomorphismus f eines endlichdimensionalen VRs gilt $\chi_f(f) = 0$.*

(b) *Für jede quadratische Matrix A über einem Körper gilt $\chi_A(A) = 0$.*

Beweis.

(a) Sei V ein endlichdimensionaler VR, $f \in \mathrm{End}(V)$ und $v \in V$. Zu zeigen ist $(\chi_f(f))(v) = 0$. Wir wählen das kleinste $m \in \mathbb{N}_0$ derart, dass $v, f(v), \ldots, f^m(v)$ linear abhängig sind. Dann gibt es $a_0, \ldots, a_{m-1} \in K$ mit $f^m(v) + a_{m-1}f^{m-1}(v) + \cdots + a_1 f(v) + a_0 v = 0$. Da $v, f(v), \ldots, f^{m-1}(v)$ linear unabhängig sind, findet man eine Basis $\underline{v} = (v, f(v), \ldots, f^{m-1}(v), v_m, \ldots, v_n)$ von V.

Satz (Cayley-Hamilton)

(a) *Für jeden Endomorphismus f eines endlichdimensionalen VRs gilt $\chi_f(f) = 0$.*

(b) *Für jede quadratische Matrix A über einem Körper gilt $\chi_A(A) = 0$.*

Beweis.

(a) Sei V ein endlichdimensionaler VR, $f \in \mathrm{End}(V)$ und $v \in V$. Zu zeigen ist $(\chi_f(f))(v) = 0$. Wir wählen das kleinste $m \in \mathbb{N}_0$ derart, dass $v, f(v), \ldots, f^m(v)$ linear abhängig sind. Dann gibt es $a_0, \ldots, a_{m-1} \in K$ mit $f^m(v) + a_{m-1}f^{m-1}(v) + \cdots + a_1 f(v) + a_0 v = 0$. Da $v, f(v), \ldots, f^{m-1}(v)$ linear unabhängig sind, findet man eine Basis $\underline{v} = (v, f(v), \ldots, f^{m-1}(v), v_m, \ldots, v_n)$ von V. Setzt man nun $p := X^m + a_{m-1}X^{m-1} + \cdots + a_1 X + a_0$, so ist

$$M(f, \underline{v}) = \left(\begin{array}{c|c} C_p & * \\ \hline 0 & A \end{array}\right)$$

für ein $A \in K^{(n-m)\times(n-m)}$ ... □

Bemerkung

(a) Im Beweis von Cayley-Hamilton haben wir Teil (b) sofort aus Teil (a) gewonnen. Geht man umgekehrt von Teil (b) aus, so gewinnt man daraus sofort Teil (a).

Bemerkung

(a) Im Beweis von Cayley-Hamilton haben wir Teil (b) sofort aus Teil (a) gewonnen. Geht man umgekehrt von Teil (b) aus, so gewinnt man daraus sofort Teil (a).

(b) Was ist mit folgendem „Beweis“? Ist $n \in \mathbb{N}_0$ und $A \in K^{n \times n}$, so setzen wir in die Gleichung $\chi_A = \det(A - XI_n)$ für X die Matrix A ein und erhalten $\chi_A(A) = \det(A - AI_n) = \det(A - A) = \det(0) = 0$

Definition

(a) Sei V ein K-Vektorraum und $f \in \mathrm{End}(V)$. Dann heißt der Kern $I_f := \ker \psi$ des Ringhomomorphismus $\psi\colon K[X] \to K[f],\ p \mapsto p(f)$ das Ideal der algebraischen Identitäten von f.

Definition

(a) Sei V ein K-Vektorraum und $f \in \mathrm{End}(V)$. Dann heißt der Kern $I_f := \ker \psi$ des Ringhomomorphismus $\psi\colon K[X] \to K[f],\ p \mapsto p(f)$ das Ideal der algebraischen Identitäten von f.

(b) Sei $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$. Dann heißt der Kern $I_A := \ker \psi$ des Ringhomomorphismus $\psi\colon K[X] \to K[A],\ p \mapsto p(A)$ das Ideal der algebraischen Identitäten von A.

Definition

(a) Sei V ein K-Vektorraum und $f \in \mathrm{End}(V)$. Dann heißt der Kern $I_f := \ker \psi$ des Ringhomomorphismus $\psi\colon K[X] \to K[f],\ p \mapsto p(f)$ das Ideal der algebraischen Identitäten von f.

(b) Sei $n \in \mathbb{N}_0$ und $A \in K^{n\times n}$. Dann heißt der Kern $I_A := \ker \psi$ des Ringhomomorphismus $\psi\colon K[X] \to K[A],\ p \mapsto p(A)$ das Ideal der algebraischen Identitäten von A.

Bemerkung

Der Satz von Cayley-Hamilton besagt:

(a) Ist f ein Endomorphismus eines endlichdimensionalen Vektorraums, so gilt $\chi_f \in I_f$ und daher insbesondere $I_f \neq \{0\}$.

Definition

(a) Sei V ein K-Vektorraum und $f \in \mathrm{End}(V)$. Dann heißt der Kern $I_f := \ker \psi$ des Ringhomomorphismus $\psi\colon K[X] \to K[f],\ p \mapsto p(f)$ das Ideal der algebraischen Identitäten von f.

(b) Sei $n \in \mathbb{N}_0$ und $A \in K^{n \times n}$. Dann heißt der Kern $I_A := \ker \psi$ des Ringhomomorphismus $\psi\colon K[X] \to K[A],\ p \mapsto p(A)$ das Ideal der algebraischen Identitäten von A.

Bemerkung

Der Satz von Cayley-Hamilton besagt:

(a) Ist f ein Endomorphismus eines endlichdimensionalen Vektorraums, so gilt $\chi_f \in I_f$ und daher insbesondere $I_f \neq \{0\}$.

(b) Ist $A \in K^{n \times n}$, so gilt $\chi_A \in I_A$ und daher insbesondere $I_A \neq \{0\}$.

Definition

(a) Sei V ein K-Vektorraum und $f \in \operatorname{End}(V)$ mit $I_f \neq \{0\}$. Dann heißt das eindeutig bestimmte normierte Polynom $\mu_f \in K[X]$ mit $I_f = (\mu_f)$ das Minimalpolynom von f.

Definition

(a) Sei V ein K-Vektorraum und $f \in \mathrm{End}(V)$ mit $I_f \neq \{0\}$. Dann heißt das eindeutig bestimmte normierte Polynom $\mu_f \in K[X]$ mit $I_f = (\mu_f)$ das Minimalpolynom von f.

(b) Sei $n \in \mathbb{N}_0$ und $A \in K^{n \times n}$. Dann heißt das eindeutig bestimmte normierte Polynom $\mu_A \in K[X]$ mit $I_A = (\mu_A)$ das Minimalpolynom von A.

Definition

(a) Sei V ein K-Vektorraum und $f \in \mathrm{End}(V)$ mit $I_f \neq \{0\}$. Dann heißt das eindeutig bestimmte normierte Polynom $\mu_f \in K[X]$ mit $I_f = (\mu_f)$ das Minimalpolynom von f.

(b) Sei $n \in \mathbb{N}_0$ und $A \in K^{n \times n}$. Dann heißt das eindeutig bestimmte normierte Polynom $\mu_A \in K[X]$ mit $I_A = (\mu_A)$ das Minimalpolynom von A.

Bemerkung

(a) Sei V ein Vektorraum mit $n := \dim V < \infty$ und $f \in \mathrm{End}(V)$. Dann gibt es $r \in K[X]$ mit $\chi_f = \mu_f r$. Insbesondere gilt $\deg(\mu_f) \leq n$.

Definition

(a) Sei V ein K-Vektorraum und $f \in \mathrm{End}(V)$ mit $I_f \neq \{0\}$. Dann heißt das eindeutig bestimmte normierte Polynom $\mu_f \in K[X]$ mit $I_f = (\mu_f)$ das Minimalpolynom von f.

(b) Sei $n \in \mathbb{N}_0$ und $A \in K^{n \times n}$. Dann heißt das eindeutig bestimmte normierte Polynom $\mu_A \in K[X]$ mit $I_A = (\mu_A)$ das Minimalpolynom von A.

Bemerkung

(a) Sei V ein Vektorraum mit $n := \dim V < \infty$ und $f \in \mathrm{End}(V)$. Dann gibt es $r \in K[X]$ mit $\chi_f = \mu_f r$. Insbesondere gilt $\deg(\mu_f) \leq n$.

(b) Sei $n \in \mathbb{N}_0$ und $A \in K^{n \times n}$. Dann gibt es $r \in K[X]$ mit $\chi_A = \mu_A r$. Insbesondere gilt $\deg(\mu_A) \leq n$.

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \,\mathrm{id}_V \,.$$

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \,\mathrm{id}_V \,.$$

(a) Sei $\varphi \in \mathbb{R}$. Dann gilt

$$\begin{aligned} \chi_{R_\varphi} &= X^2 - 2(\cos\varphi)X + 1 \qquad \text{und} \\ \mu_{R_\varphi} &= \begin{cases} \chi_{R_\varphi} & \text{falls } \varphi \notin \{n\pi \mid n \in \mathbb{Z}\} \\ X - 1 & \text{falls } \varphi = n\pi \text{ für ein gerades } n \in \mathbb{Z} \\ X + 1 & \text{falls } \varphi = n\pi \text{ für ein ungerades } n \in \mathbb{Z} \end{cases} \,. \end{aligned}$$

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \,\mathrm{id}_V \,.$$

(a) Sei $\varphi \in \mathbb{R}$. Dann gilt

$$\begin{aligned} \chi_{R_\varphi} &= X^2 - 2(\cos\varphi)X + 1 \qquad \text{und} \\ \mu_{R_\varphi} &= \begin{cases} \chi_{R_\varphi} & \text{falls } \varphi \notin \{n\pi \mid n \in \mathbb{Z}\} \\ X - 1 & \text{falls } \varphi = n\pi \text{ für ein gerades } n \in \mathbb{Z} \\ X + 1 & \text{falls } \varphi = n\pi \text{ für ein ungerades } n \in \mathbb{Z} \end{cases} . \end{aligned}$$

Nach Cayley-Hamilton gilt

$$\begin{aligned} (R_\varphi)^2 - 2(\cos\varphi)R_\varphi + \mathrm{id}_{\mathbb{R}^2} &= 0, \quad \text{also} \\ R_{2\varphi}(v) - 2(\cos\varphi)R_\varphi(v) + v &= 0 \quad \text{für alle } v \in \mathbb{R}^2. \end{aligned}$$

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \operatorname{id}_V .$$

(b) Es gilt $\mu_S = \chi_S = (X-1)(X+1) = X^2 - 1$ und Cayley-Hamilton besagt $S^2 = \operatorname{id}_{\mathbb{R}^2}$ („zweimal spiegeln ist keinmal spiegeln“).

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \operatorname{id}_V .$$

(b) Es gilt $\mu_S = \chi_S = (X-1)(X+1) = X^2 - 1$ und Cayley-Hamilton besagt $S^2 = \operatorname{id}_{\mathbb{R}^2}$ („zweimal spiegeln ist keinmal spiegeln“).

(c) Es gilt $\mu_P = \chi_P = X(X-1) = X^2 - X$ und Cayley-Hamilton besagt $P^2 = P$ („zweimal projizieren ist einmal projizieren“).

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \, \mathrm{id}_V \, .$$

(b) Es gilt $\mu_S = \chi_S = (X-1)(X+1) = X^2 - 1$ und Cayley-Hamilton besagt $S^2 = \mathrm{id}_{\mathbb{R}^2}$ („zweimal spiegeln ist keinmal spiegeln").

(c) Es gilt $\mu_P = \chi_P = X(X-1) = X^2 - X$ und Cayley-Hamilton besagt $P^2 = P$ („zweimal projizieren ist einmal projizieren").

(d) Sei $a \in \mathbb{R}$. Dann gilt

$$\begin{aligned} \chi_{T_a} &= (X-1)^2 = X^2 - 2X + 1 \qquad \text{und} \\ \mu_{T_a} &= \begin{cases} \chi_{T_a} & \text{falls } a \neq 0 \\ X - 1 & \text{falls } a = 0 \end{cases} . \end{aligned}$$

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \, \mathrm{id}_V \, .$$

(b) Es gilt $\mu_S = \chi_S = (X-1)(X+1) = X^2 - 1$ und Cayley-Hamilton besagt $S^2 = \mathrm{id}_{\mathbb{R}^2}$ („zweimal spiegeln ist keinmal spiegeln").

(c) Es gilt $\mu_P = \chi_P = X(X-1) = X^2 - X$ und Cayley-Hamilton besagt $P^2 = P$ („zweimal projizieren ist einmal projizieren").

(d) Sei $a \in \mathbb{R}$. Dann gilt

$$\begin{aligned} \chi_{T_a} &= (X-1)^2 = X^2 - 2X + 1 \qquad \text{und} \\ \mu_{T_a} &= \begin{cases} \chi_{T_a} & \text{falls } a \neq 0 \\ X - 1 & \text{falls } a = 0 \end{cases} . \end{aligned}$$

Cayley-Hamilton sagt hier $T_a^2 = 2T_a - \mathrm{id}_{\mathbb{R}^2}$ („zweimal scheren ist scheren, verdoppeln und Ausgangsvektor abziehen").

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \operatorname{id}_V .$$

(e) Ist $A \in K^{n \times n}$, so ist $\chi_{f_A} = \chi_A$ und $\mu_{f_A} = \mu_A$.

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \, \mathrm{id}_V \, .$$

(e) Ist $A \in K^{n \times n}$, so ist $\chi_{f_A} = \chi_A$ und $\mu_{f_A} = \mu_A$.

(f) Sei $d \in \mathbb{N}_0$. Wegen $\chi_{D^{(d)}} = (-X)^{d+1}$ besagt Cayley-Hamilton hier, dass $D^{d+1}(p) = (D^{(d)})^{d+1}(p) = 0$ für alle $p \in K[X]_d$, das heißt ein Polynom vom Grad $\leq d$ wird nach $(d+1)$-maligem Ableiten das Nullpolynom.

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \, \mathrm{id}_V \, .$$

(e) Ist $A \in K^{n \times n}$, so ist $\chi_{f_A} = \chi_A$ und $\mu_{f_A} = \mu_A$.

(f) Sei $d \in \mathbb{N}_0$. Wegen $\chi_{D^{(d)}} = (-X)^{d+1}$ besagt Cayley-Hamilton hier, dass $D^{d+1}(p) = (D^{(d)})^{d+1}(p) = 0$ für alle $p \in K[X]_d$, das heißt ein Polynom vom Grad $\leq d$ wird nach $(d+1)$-maligem Ableiten das Nullpolynom.

(g) $E_{a_1,\ldots,a_n}$ ist kein Endomorphismus!

Beispiel

In den folgenden Beispielen benutzen wir, dass für einen Endomorphismus f eines zweidimensionalen K-VRs V offensichtlich gilt:

$$\chi_f \neq \mu_f \iff \exists \lambda \in K : f = \lambda \, \mathrm{id}_V \, .$$

(e) Ist $A \in K^{n \times n}$, so ist $\chi_{f_A} = \chi_A$ und $\mu_{f_A} = \mu_A$.

(f) Sei $d \in \mathbb{N}_0$. Wegen $\chi_{D^{(d)}} = (-X)^{d+1}$ besagt Cayley-Hamilton hier, dass $D^{d+1}(p) = (D^{(d)})^{d+1}(p) = 0$ für alle $p \in K[X]_d$, das heißt ein Polynom vom Grad $\leq d$ wird nach $(d+1)$-maligem Ableiten das Nullpolynom.

(g) $E_{a_1,\ldots,a_n}$ ist kein Endomorphismus!

(h) Es gilt $\mu_C = \chi_C = X^2 - 1$ und Cayley-Hamilton besagt $C^2 = \mathrm{id}_{\mathbb{C}}$ („zweimal komplex konjugieren ist keinmal komplex konjugieren“).