Kap. VI Eigenwerte und Diagonalisierbarkeit

M ↓

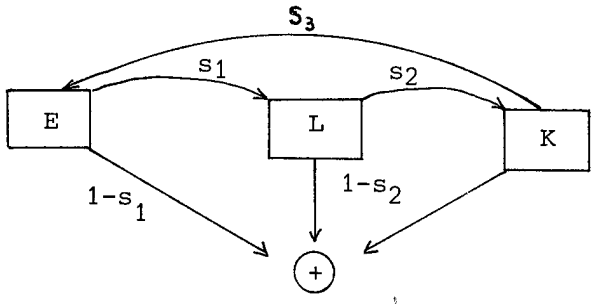
Zur Einleitung diene folgendes Beispiel aus der Populationsdynamik (vgl. J. Lighthill (Hrsg.): Newer uses of mathematics, Penguin 1978, Chap. 2 Mathematics and the Biological Environment

H.L. Le Roy: Prinzipien der linearen Algebra, UTB 1980, Kap. VIII

E. Lehmann: Computereinsatz in Kursen der linearen Algebra, in: K.-D. Graf: Mathematikunterricht und Informatik, FU Berlin, Zentralinstitut f. Unterrichtswissenschaften und Curriculumentwicklung, 1982, S. 123 -152):

Wie im Beispiel (10.4 Anm 4) (s. LAI p.130) sehe ein Modell für die Entwicklung einer Käferpopulation folgendermaßen aus: Aus den Eiern eines Käfers schlüpfen nach einem Monat Larven, nach einem weiteren Monat werden diese zu Käfern, die dann wieder Eier legen und anschließend sterben.

Der Übergang von einer Generation zur nächsten geschehe (im Durchschnitt) folgendermaßen: Aus a% der Eier werden Larven, von den Larven werden d% Käfer. Pro Käfer werden im Mittel c% Eier gelegt (vgl. folgendes Schema mit den Bezeichnungen: E : Eier, L : Larven, K : Käfer und mit $s_1 := \frac{a}{100}$, $s_2 := \frac{d}{100}$ als Überlebendsraten und $s_3 = \frac{c}{100}$ als Geburtenrate):



Die Übergangsmatrix

$$T := \begin{array}{c} \begin{matrix} E & L & K \end{matrix} \\ \begin{pmatrix} 0 & 0 & \frac{c}{100} \\ \frac{a}{100} & 0 & 0 \\ 0 & \frac{d}{100} & 0 \end{pmatrix} \end{array} \begin{matrix} E \\ L \\ K \end{matrix}$$

beschreibt die Entwicklung der Population:

$$v_m = \begin{pmatrix} n_E \\ n_L \\ n_K \end{pmatrix} \longmapsto v_{m+1} = \begin{pmatrix} n'_E \\ n'_L \\ n'_K \end{pmatrix} = T \cdot \begin{pmatrix} n_E \\ n_L \\ n_K \end{pmatrix} = Tv_m$$

(mit n_E, n_L, n_K bzw. n'_E, n'_L, n'_K Anzahl der Eier, Larven, Käfer vor und nach dem "Generationswechsel"; v_i Verteilung nach i Generationswechseln, v_o Anfangsverteilung).

Es interessiert nun, (i) ob es eine Verteilung $v \neq \mathfrak{O}$ gibt, bei der (theoretisch) der prozentuale Anteil der Eier, Larven und Käfer bei jedem Generationswechsel konstant bleibt, und dabei:

(ii) unter welcher Bedingung (an a,c,d) eine solche Verteilung (bei konstantem Anteil der Generationen) wächst oder gleich bleibt.

Diese Problemstellung führt zu der Frage

Existiert ein $v \neq \mathfrak{O}$ mit (*) $Tv = \lambda v$ (d.h. $(T - \lambda E_n)v = \mathfrak{O}$)

und (i) $\lambda \geq 0$

↑ M (ii) $\lambda > 1$ (Wachstum) bzw. $\lambda = 1$ (Gleichgewicht).

Wie am Ende des § 24 stößt man auch hier auf die (allgemeine) Frage: Gegeben sei die Matrix $A \in K^{(n,n)}$; für welche $\lambda \in K$ ist die Matrix $A - \lambda E_n$ (bzw. der Endomorphismus $f - \lambda id_V$) singulär?

Dieses Problem läßt sich nun nach Kenntnis der Determinanten und ihrer Eigenschaften folgendermaßen formulieren:

Für welche $\lambda \in K$ gilt

$$\det(A - \lambda E_n) = 0 \quad \text{(bzw.} \quad \det(f - \lambda id_V) = 0)?$$

Spezialfall n = 2

Sei $A = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \in K^{(2,2)}$. Für jedes $\lambda \in K$ gilt

dann

$$\det(A - \lambda E_2) = \det\left(\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right) = \begin{vmatrix} \alpha_{11}-\lambda & \alpha_{12} \\ \alpha_{21} & \alpha_{22}-\lambda \end{vmatrix} =$$

$$(\alpha_{11}-\lambda)(\alpha_{22}-\lambda) - \alpha_{21}\alpha_{12} = \lambda^2 - (\alpha_{11} + \alpha_{22})\lambda + (\alpha_{11}\alpha_{22} - \alpha_{21}\alpha_{12}).$$

$\det(A - \lambda E_2)$ ist also für solche $\lambda \in K$ gleich Null, die Nullstellen des "Polynoms" $x^2 - (\alpha_{11}+\alpha_{22})x + \det A$ sind.

Spezialfall n = 3

Analog ist für $A = (\alpha_{ij})_{i,j\in\{1,2,3\}}$ jede Nullstelle von

$$\det(A-\lambda E_3) = \begin{vmatrix} \alpha_{11}-\lambda & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22}-\lambda & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33}-\lambda \end{vmatrix}$$ Nullstelle eines Polygnoms vom Grad 3

Beispiel (Fortsetzung des obigen Beispiels):

$$0 = \begin{vmatrix} -\lambda & 0 & c/100 \\ \frac{a}{100} & -\lambda & 0 \\ 0 & \frac{d}{100} & -\lambda \end{vmatrix} = -\lambda^3 + \frac{acd}{10^6}$$ hat die Lösung $\lambda = \frac{\sqrt[3]{acd}}{100}$ (Nullstelle-

stelle des Polynoms $(-x^3 + acd\cdot 10^{-6})$. Also ist die obige Problemstellung (i) lösbar, falls $a\cdot c\cdot d > 0$ gilt; ferner ist (ii) erfüllt, wenn $\sqrt[3]{acd} > 100$ bzw. $\sqrt[3]{acd} = 100$ gilt.

Wir fügen einen Exkurs über Polynome ein, bevor wir die Frage nach 1-dim invarianten UR'e eines Endomorphismus allgemein weiter verfolgen.

---

§ 27 Polynome (Exkurs)

M ↓ Es ist in der Elementarmathematik üblich, unter einem Polynom einen Ausdruck der Gestalt

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n$$

zu verstehen, wobei x Unbestimmte heißt. Diese Definition ist jedoch unbefriedigend, da nicht definiert wird, was eine Unbestimmte ist. Man hilft sich, indem man Polynomabbildungen heranzieht (vgl. LAI p. 104) oder folgendermaßen vorgeht:
Ein Polynom sollte durch die Koeffizienten $\alpha_0, \alpha_1, \ldots, \alpha_n$ bestimmt sein, also durch die Folge $(\alpha_0, \alpha_1, \ldots, \alpha_n, 0, 0, \ldots) \in K^{(\mathbb{N}_0)}$

(mit endlichem Träger). Zu x gehört dabei die (definierte!) Folge (0,1,0,...). Addition (S-Multplikation) der Polynome entspricht dabei der bereits definierten komponentenweise Addition (S-Multiplikation) der entsprechenden Koeffizientenfolgen:

$(\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n) + (\beta_0 + \beta_1 x + \ldots + \beta_m x^m) = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1) x + \ldots$

$\lambda\ (\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n) = \lambda\alpha_0 + (\lambda\alpha_1) x + \ldots + (\lambda\alpha_n) x^n$

↑ Für das Produkt soll gelten: $(\alpha_0 + \ldots + \alpha_n x^n)(\beta_0 + \ldots + \beta_m x^m) =$

M $\alpha_0\beta_0 + (\alpha_0\beta_1 + \alpha_1\beta_0) x + \ldots + (\sum_{j=0}^{i} \alpha_j \beta_{i-j}) x^i + \ldots$

Generalvoraussetzung: Sei weiterhin K Körper.

(27.1) Definition :

Auf $K^{(\mathbb{N}_0)} = \{(\alpha_i)_{i\in\mathbb{N}_0} \mid (\alpha_i)_{i\in\mathbb{N}_0}$ Folge aus K mit endlichem Träger$\}$ definieren wir zusätzlich zu der (bereits definierten) Addition +

$$(\alpha_i)_{i\in\mathbb{N}_0} + (\beta_i)_{i\in\mathbb{N}_0} := (\alpha_i + \beta_i)_{i\in\mathbb{N}_0}$$

und S-Multiplikation $\dot{K}$

$$(\alpha_i)_{i\in\mathbb{N}_0} \cdot \lambda = (\alpha_i \lambda)_{i\in\mathbb{N}_0}$$

eine Multiplikation · durch

$$(\alpha_i)_{i\in\mathbb{N}_0} \cdot (\beta_i)_{i\in\mathbb{N}_0} := (\sum_{j=0}^{i} \alpha_j \beta_{i-j})_{i\in\mathbb{N}_0}$$

Anmerkung: Die Multiplikation ist eine innere Verknüpfung; denn definitionsgemäß existieren $n,m \in \mathbb{N}_0$ mit $\alpha_j = 0$ für alle $j > n$ und $\beta_k = 0$ für alle $k > m$. Für $i \geq m + n$ ist $\sum_{j=0}^{i} \alpha_j \beta_{i-j} = 0$, weil $\alpha_j = 0$ oder $j \leq n$ und damit $i - j > m + n - n$, also $\beta_{i-j} = 0$ ist.

(27.2) Hilfssatz

(a) $(K^{(\mathbb{N}_o)}, +, \cdot_K)$ ist K-VR.

(b) $(K^{(\mathbb{N}_o)}, +, \cdot)$ ist ein kommutativer Ring mit Einselement

(c) $\forall a,b \in K^{(\mathbb{N}_o)} \; \forall \lambda \in K$:

$$(a \cdot b) \cdot_K \lambda = (a \cdot_K \lambda) \cdot b = a \cdot (b \cdot_K \lambda)$$

Beweis: (a) vgl. LAI p.104 (b) und (c) durch Nachprüfen;
Einselement ist $(1,0,0,\ldots)$

Anmerkung:
$(K^{(\mathbb{N}_o)}, +, \cdot_K, \cdot)$ ist also eine kommutative K-Algebra.

Wir wollen nun zu einer der vertrauten Gestalt von Polynomen ähnlichen Form gelangen. Dazu definieren wir:

(27.3) Definition

$$X := (0,1,0,\ldots,0,\ldots) = (\delta_{1i})_{i \in \mathbb{N}_o}$$

und

$$X^\circ := (1,0,\ldots,0,\ldots) = (\delta_{0i})_{i \in \mathbb{N}_o} .$$

Damit zeigen wir

(27.4) Hilfssatz

(i) $X^n = (\delta_{ni})_{i \in \mathbb{N}_o} = (0,\ldots,0,\underset{\substack{\uparrow \\ n\text{-te} \\ \text{Stelle}}}{1},0,\ldots,0,\ldots)$

(ii) Jedes $(\alpha_i)_{i \in \mathbb{N}_o} \in K^{(\mathbb{N}_o)}$ hat eine Darstellung der Form

$$(\alpha_i)_{i \in \mathbb{N}_o} = \sum_{i \in \mathbb{N}_o} \alpha_i X^i = \sum_{i=0}^{n} \alpha_i X^i \quad \text{(für geeignetes } n \in \mathbb{N}_o)$$

(iii) Diese Darstellung ist eindeutig in folgendem Sinne:
Ist $\sum_{i=0}^{n} \alpha_i X^i = \sum_{j=0}^{m} \beta_j X^j$ und $\alpha_n \neq 0 \neq \beta_m$, so gilt
$n = m$ und $\alpha_i = \beta_i$ für alle $i \in \{1,\dots,n\}$.

Beweis:

(i) durch vollständige Induktion[1]:

Induktions-Verankerung: $n = 0$; Behauptung richtig.

Induktions-Voraussetzung: $X^n = (\delta_{ni})$

Induktions-Schritt:

$$X^{n+1} = X \cdot X^n = (\delta_{1i})_i \cdot (\delta_{ni})_i \underset{\text{def.}}{=} \Big(\sum_{j=0}^{i} \underbrace{\delta_{1j}\delta_{ni-j}}_{\neq 0 \text{ nur für } j=1 \text{ und } i-j=n}\Big)_{i \in \mathbb{N}_0}$$

$$= (\delta_{n+1\ i})_{i \in \mathbb{N}_0}$$

(ii) $(\alpha_i)_{i \in \mathbb{N}_0} = \sum_{i \in \mathbb{N}_0} \alpha_i \underbrace{(0,\dots,0,1,0,\dots)}_{\substack{i\text{-te} \\ \text{Stelle}}} = \sum_{i \in \mathbb{N}_0} \alpha_i X^i$, wobei fast alle $\alpha_i = 0$ sind.

(iii) folgt, da $\{X^0, X^1, \dots, X^n, \dots\}$ l.u. sind (vgl. LA I p. 117). □

Anmerkung:

Die Abbildung $\begin{cases} K \longrightarrow K^{(\mathbb{N}_0)} \\ \alpha \longmapsto \alpha X^0 \end{cases}$ ist ein Algebren-Monomorphismus.

Da X^0 das neutrale Element der Multiplikation in $K^{(\mathbb{N}_0)}$ ist, folgt aus 27.2(c)

$$\alpha \cdot \sum_{i=1}^{n} \alpha_i X^i = (\alpha X^0) \cdot \sum_{i=1}^{n} \alpha_i X^i.$$ Aus diesen Gründen können wir K in $K^{(\mathbb{N}_0)}$ einbetten, d.h. α und αX^0 für $\alpha \in K$ identifizieren. Damit hat jedes Element aus $K^{(\mathbb{N}_0)}$ eine Darstellung der Form

---

1) Statt von $n = 1$ aus startend (wie in 2.7.1) kann eine vollständige Induktion auch mit beliebigem $z_0 \in \mathbb{Z}$ beginnen. Die Aussage gilt dann für alle $z \in \mathbb{Z}$ mit $z \geq z_0$.

$$\alpha_o + \alpha_1 X + \ldots + \alpha_n X^n,$$

die uns aus der Elementarmathematik gewohnt ist.

(27.5) Bezeichnungen

(a) $K[X] := (K^{(\mathbb{N}_o)}, +, \cdot_K, \cdot)$ heißt Polynom-Algebra über K.

Jedes Element von K[X] heißt Polynom in der "Umbestimmten" X mit Koeffizienten aus K.

(b) Ist $P = \sum_{i=0}^{n} \alpha_i X^i \in K[X]$ und $\alpha_n \neq 0$, so definieren wir

grad P := n (Grad von P)

grad (0,0,...) := $-\infty$ (damit grad (P·Q) = grad P + grad Q gilt).

(27.6) Satz (Zusammenfassung)

K[X] ist eine K-Algebra; $\{X^n \mid n \in \mathbb{N}_o\}$ ist eine Basis von K[X]

Beweis: (27.2), (27.4)

Anmerkung: Es gilt also dim $K[X] = |\mathbb{N}_o| = \aleph_o$ und damit (vgl. z.B. Satz 25.7 in Schęja, Storch, Lehrbuch der Algebra, Stuttgart 1980), $|K[X]| = |K| \cdot \dim K[X] = \sup\{|K|, |\mathbb{N}_o|\}$.

Wir wollen nun das Einsetzen eines Elementes aus einer K-Algebra mit 1 $\mathfrak{A}$ in ein Polynom behandeln: Für $a \in \mathfrak{A}$ und

$$P = \sum_{i=0}^{n} \alpha_i X^i \in K[X] \quad \text{definieren wir} \quad P(a) := \sum_{i=0}^{n} \alpha_i a^i$$

Beispiel (i) $\mathfrak{A} = K^{(n,n)}$, $A \in \mathfrak{A}$, $\lambda \in K$, $P = X^2 - \lambda$

$P(A) = A^2 - \lambda A^\circ = A^2 - \lambda E_n$

(ii) $\mathfrak{A} = \mathrm{End}_K V$, $f \in \mathfrak{A}$, $P = X^2 - \lambda$

$P(f) = f \circ f - \lambda \mathrm{id}_V$.

(27.7) Hilfssatz

Seien $P,Q \in K[X]$, sei ferner $\mathfrak{A}$ eine K-Algebra mit 1 und $a \in \mathfrak{A}$.

Dann gilt

(i) $(P+Q)(a) = P(a) + Q(a)$

(ii) $(\lambda P)(a) = \lambda P(a)$

(iii) $(P \cdot Q)(a) = P(a) \cdot Q(a)$

Beweis durch Nachrechnen ...

Anmerkung: Die Abbildung $\begin{cases} K[X] \longrightarrow \mathfrak{A} \\ P \longmapsto P(a) \end{cases}$

ist (für $a \in \mathfrak{A}$) also ein Algebren-Homomorphismus.

Ersetzt man bei festem $P = \sum \alpha_i X^i$ die Unbestimmte speziell durch ein Element α aus der K-Algebra K, so erhält man

$$P(\alpha) = \sum_{i=0}^{n} \alpha_i \alpha^i = [\sum_{i=0}^{n} \alpha_i (id_K)^i](\alpha), \text{ das Bild von } \alpha$$

unter der Polynomabbildung $\sum_{i=0}^{n} \alpha_i (id_K)^i : \begin{cases} K \longrightarrow K \\ \alpha \longmapsto P(\alpha) \end{cases}$

Diese steht in engem Zusammenhang mit P und lässt sich durch Einsetzen von id_K in P gewinnen:

Sei $\mathfrak{A} = \mathfrak{P}(K)$ die Algebra der Polynomabbildungen über K. Für $a = id_K \in \mathfrak{A}$ ist nach (27.7) die Abbildung

$$\varphi : \begin{cases} K[X] \longrightarrow \mathfrak{P}(K) \\ P = \sum_{i=0}^{n} \alpha_i X^i \longrightarrow P(id_K) = \sum_{i=0}^{n} \alpha_i (id_K)^i \end{cases}$$

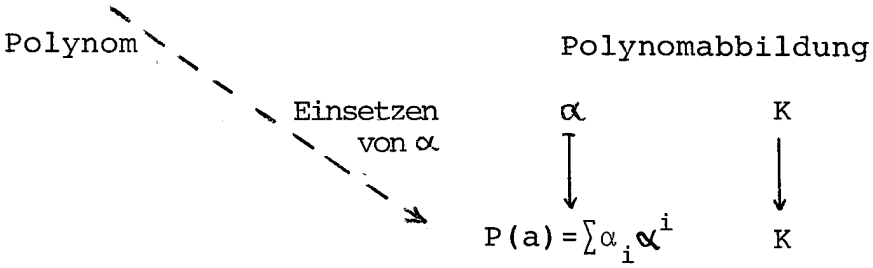
ein surjektiver Algebren-Homomorphismus:

(27.7) Satz

Ist K ein Körper, so ist $\mathfrak{P}(K)$ homomorphes Bild von K[X]

Schema: $K[X] \xrightarrow{\varphi} \mathcal{P}(K)$

$P = \sum_{i=0}^{n} \alpha_i X^i \longmapsto P(id_K) = \sum_{i=0}^{n} \alpha_i (id_K)^i$



I.a. ist φ jedoch kein Isomorphimus, d.h. zwei verschiedene Polynome können zur gleichen Polynomabbildung führen:

Beispiel: $K = GF(2)$

$P = X^2 + X \in K[X]$

$f := P(id_K) = id_K^2 + id_K$ bildet 0 auf $P(0) = 0^2 + 0 = 0$

und 1 auf $P(1) = 1^2 + 1 = 0$

ab, ist also gleich der 0-Abbildung, zu der auch das 0-Polynom gehört.

Insbesondere ist $\{id^j \mid j \in \mathbb{N}_0\}$ keine Basis von $\mathcal{P}(K)$ (vgl. auch die Anmerkung zu (7.2) Bsp. (d), s. LA I p.108)

Jedoch gilt

(27.8) Satz

Ist K unendlicher Körper, so gilt $K[X] \cong \mathcal{P}(K)$

Beweis: Nach 27.7 ist $\varphi: K[X] \longrightarrow \mathcal{P}(K)$ mit $P \longmapsto P(id_K)$ ein surjektiver Algebren-Homomorphismus. Wir zeigen, daß φ injektiv ist, wenn $|K|$ unendlich ist.

Sei $P \in \text{Kern } \varphi$, also $P \in K[X]$ und $P(id_K) = 0$; dann gilt $P(x) = 0$ für alle $x \in K$; wäre $P \neq 0$, also Grad $P = m \geq 0$, so hätte P nach folgendem Satz 27.9 höchstens m Nullstellen. Aus $|K| > m$ folgt $P = 0$. Also ist φ injektiv und damit Isomorphismus. □

(27.9) Satz

Sei K ein Körper und $P \in K[X] - \{0\}$ mit Grad $P = n$. Dann hat P höchstens n Nullstellen.

Dabei benutzen wir folgende Definition:

(27.10) Definition

$\alpha \in K$ heißt Nullstelle des Polynoms $P \in K[X]$ (bzw. der zugehörige Polynomabbildung $\varphi(P)$), wenn gilt $P(\alpha) = 0$.

Zum Beweis von (27.9) (Übungsaufgabe) kann man folgenden Hilfssatz heranziehen:

(27.11) Hilfssatz

Ist $P \in K[X]$ und α Nullstelle von P, so gibt es ein Polynom $Q \in K[X]$ mit

$$P = (X - \alpha) \cdot Q \qquad \text{(d.h. } (X - \alpha) \text{ teilt } P\text{)}$$

Letzterer ergibt sich mit Hilfe des Euklidischen Algorithmus.

(27.12) Satz "Teilen mit Rest" bei Polynomen (Grundlagen für den "Euklidischen Algorithmus")

Seien $P, Q \in K[X]$ mit $Q \neq 0$. Dann existieren $R, S \in K[X]$ mit

(i) $P = Q \cdot S + R$ und

(ii) Grad $R <$ Grad Q

Beweis: .....

Beispiel: $K = \mathbb{Q}$; $P = X^5 - 3X^4 + X^2 - 7$; $Q = X^3 + 5X^2 + X - 2$

$$(X^5 - 3X^4 + X^2 - 7) : (X^3 + 5x^2 + X - 2) = X^2 - 8X + 39 + \frac{R}{Q}$$

$$\underline{X^5 + 5X^4 + X^3 - 2X^2}$$

$$-8X^4 - X^3 + 3X^2 - 7$$

$$\underline{-8X^4 - 40X^3 - 8X^2 + 16X}$$

$$39X^3 + 11\ X^2 - 16\ X - 7$$

$$\underline{39X^3 + 195\ X^2 + 39\ X - 78}$$

$$-184\ X^2 - 55\ X + 71$$

$$\underbrace{X^5 - 3X^4 + X^2 - 7}_{P} = \underbrace{(X^3 + 5X^2 + X - 2)}_{Q} \cdot \underbrace{(X^2 - 8X + 39)}_{S} + \underbrace{(-184X^2 - 55X + 71)}_{R}$$

Auch sonst finden sich viele Übereinstimmungen zwischen $(\mathbb{Z},+,\cdot)$ und $(K[X],+,\cdot)$:

$\mathbb{Z}$	$K[X]$ (für K Körper)
	(27.13) Def. Teiler
$p,q \in \mathbb{Z}$	$P,Q \in K[X]$
$p \mid q$ (p Teiler von q) $:\Leftrightarrow \exists s \in \mathbb{Z} : q = s \cdot p$	$P \mid Q$ (P Teiler von Q) $:\Leftrightarrow \exists S \in K[X] : Q = S \cdot P$
Unzerlegbare Elemente	
Eine Primzahl p ist in $\mathbb{Z}$ dadurch gekennzeichnet, daß sie ungleich ± 1 ist und keine echten Teiler besitzt, also keinen Teiler außer $\pm p$ und ± 1. $+1$ und -1 sind stets Teiler, da sie (bzgl. der Multiplikation) invertierbar sind. $p = p \cdot 1 = (-p)(-1) = p \cdot (-1)(-1)$	In $K[X]$ ist jedes $\beta = \beta \cdot X^0$ mit $\beta \in K - \{0\}$ invertierbar: $(\beta X^0)^{-1} = \beta^{-1} X^0$, also Teiler jedes Polynoms, z.B. $X - \alpha = (\beta X^0)(\beta^{-1} X - \beta^{-1} \alpha X^0)$.
	(27.14) Definition
	(i) $P \in K[X]$ heißt echter Teiler von $Q \in K[X]$ wenn $P \mid Q$ und $0 < \operatorname{grad} P < \operatorname{grad} Q$
	(ii) $P \in K[X]$ heißt irreduzibel, falls P keine echten Teiler hat, anderenfalls reduzibel.
	Ein reduzibles Polynom läßt sich in ein Produkt ($q = S \cdot p$) von Polynomen kleinerenen (positiven) Grades zerlegen. Ein irreduzibles Polynom vom Grad größer als 1 kann nach (27.11) keine Nullstelle haben.
	Bsp.: $\mathbb{R}[X]$: $X^2 + 1$ ist irreduzible (über $\mathbb{R}$)
	$\mathbb{C}[X]$: $X^2 + 1$ ist reduzibel (über $\mathbb{C}$) $X^2 + 1 = (X + i)(X - i)$

$\mathbb{Z}$	$K[X]$

Primfaktorzerlegung

Jedes $z \in \mathbb{Z} - \{0\}$ läßt sich (bis auf die Reihenfolge der Faktoren) eindeutig darstellen als

$z = \varepsilon \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_k$

mit $\varepsilon \in \{+1, -1\}$ und positiven Primzahlen $p_1, \ldots, p_k$.

(Das Produkt $p_1 \cdots p_k$ kann "leer" sein. Durch die Forderung "positiv", also eine gewisse Normierung, wird ε eindeutig festgelegt).

Bsp.: $-60 = (-1) \cdot 2 \cdot 2 \cdot 3 \cdot 5$

Um auch in $K[X]$ eine Zerlegung auszuzeichnen, müssen wir berücksichtigen, daß - so wie ± 1 in $\mathbb{Z}$ - die Polynome βX^0 mit $\beta \in K - \{0\}$ Teiler jedes anderen Polynoms sind. Wir vereinbaren daher

(27.15) Definition

$P = \sum_{i=0}^{m} \alpha_i X^i \in K[X]$ mit grad $P = m \geq 0$ heißt normiert, wenn $\alpha_m = 1$ gilt.

Anmerkung: Ist P nicht normiert, so ist es $\alpha_m^{-1} P$.

(27.16) Satz

Jedes $P \in K[X] - \{0\}$ läßt sich (bis auf die Reihenfolge der Faktoren) eindeutig darstellen als $P = \alpha \cdot P_1 \ldots P_k$ mit $\alpha \in K - \{0\}$ und normierten irreduziblen Polynomen $P_1, \ldots, P_k$ vom grad ≥ 1.
(Das Produkt $P_1 \cdot \cdots \cdot P_k$ kann leer sein: $P = \alpha$)

Beweis: s. z.B. Guber II p.150f.

Bsp.: $P = 2X^3 - 4X^2 + 2X - 4$

(i) in $\mathbb{R}[X]$: $P = 2 \cdot (X^2 + 1) \cdot (X - 2)$

(ii) in $\mathbb{C}[X]$ $P = 2 \cdot (X + i) \cdot (X - i) \cdot (X - 2)$

Anm.: Nach dem Fundamentalsatz der Algebra (Gauss, s.z.B. Lüneburg p.245) besitzt jedes Polynom vom Grad größer gleich 1 aus $\mathbb{C}[X]$ mindestens eine Nullstelle

"$\mathbb{C}$ ist algebraisch abgeschlossen"

sodaß nach (27.11) die irreduziblen Polynome einen Grad kleiner gleich 1 haben. Jedes Polynom über $\mathbb{C}$ zerfällt (bei der obigen Zerlegung) in "Linearfaktoren" (Polynome v. Grad ≤ 1)

$\mathbb{Z}$ | $K[X]$

Struktur der Ideale

Den Normalteilern bei Gruppen und den UR'en bei VR'en entsprechen bei Ringen spezielle Unterringe , die Ideale:

Sei $(R,+,\cdot)$ ein kommutativer Ring. Dann heißt $J \subseteq R$ Ideal in R, wenn J UG von $(R,+)$ ist und $R \cdot J \subseteq J$ gilt. In einem kommutativen Ring $(R,+,\cdot)$ mit 1 ist $(a) := Ra$ ein Ideal, das von $a \in R$ erzeugte Ideal. Ein Ideal J heißt Hauptideal, wenn es ein $a \in R$ gibt mit $J = (a)$.

Beispiele

$(2) = 2\mathbb{Z}$ Ideal der geraden ganzen Zahlen; $(n) = n\mathbb{Z}$ Ideal der durch n teilbaren Zahlen; $(1) = (-1) = \mathbb{Z}$

$4\mathbb{Z} + 6\mathbb{Z} = (2)$

(denn $4\mathbb{Z} + 6\mathbb{Z} \subseteq 2\mathbb{Z}$ und, wegen $ggT(4,6) = 2 = 1 \cdot 6 + (-1) \cdot 4$, $2\mathbb{Z} \subseteq 4\mathbb{Z} + 6\mathbb{Z}$)

$((X-1)) = (X-1) \cdot K[X]$

$(2) \neq (1) = K[X]$ (falls $2 \neq 0$)

$P \in K[X] \Rightarrow (P) = \{P \cdot Q \mid Q \in K[X]\}$ Ideal der durch P teilbaren Polynome

$(0) = \{0\}$ Nullideal

(27.17) Satz

In $\mathbb{Z}$ und in $K[X]$ ist jedes Ideal Hauptideal (Ringe dieser Eigenschaft heißen Haupidealringe.)

Genauer:

Zu jedem Ideal J in $K[X]$ existiert ein (bis auf einen Skalar $\alpha \in K$) eindeutig bestimmtes Polynom $P \in K[X]$ mit $J = (P)$.
Ist $J \neq \{0\}$, so ist P ein Polynom minimalen nicht-negativen Grades in J.

$\mathbb{Z}$	K[X]
Beweis für $\mathbb{Z}$ ähnlich wie für K[X], aber mit "Betrag" statt "Grad".	Beweis (a) Existenz Ist $J = \{0\}$, so setze man $P = 0$. Sei also $J - \{0\} \neq \emptyset$. Dann hat $\{\text{grad } P \mid P \in J - \{0\}\}$ ein kleinstes Element m. Sei $P \in J - \{0\}$ mit grad $P = m$. Da J Ideal ist, gilt $(P) \subseteq J$. Sei umgekehrt $Q \in J$; z.z. $Q \in (P)$. Nach (27.12) existieren $R,S \in K[X]: Q = SP + R$ mit grad $R <$ grad P. Da J Ideal ist und $P,Q \in J$ gilt, folgt $R = Q - SP \in J$. Weil P minimalen Grad in $J - \{0\}$ hat, muß $R = 0$ sein, woraus sich $Q \in (P)$ ergibt. (b) Eindeutigkeit Sei $(P) = (Q) \neq (0)$. Aus $Q \in (P)$ folgt $\exists S \in K[X]$ mit $Q = PS$; aus $P \in (Q)$ die Existenz eines Polynoms $R \in K[X]$ mit $P = QR$. Es ergibt sich $P = QR = P \cdot (SR)$, also $P(SR - 1) = 0$. Da K[X] nullteilerfrei ist (s.u.) und $P \neq 0$, muß $SR = 1$ sein, woraus man grad R + grad S = grad 1 = 0 erhält. Damit ist grad R = grad S = 0 und es existiert $\alpha \in K: S = \alpha X^0$. $Q = PS = \alpha \cdot P$ zeigt die Behauptung. □

(27.18) Satz

$\mathbb{Z}$ und K[X] sind nullteilerfrei.

Beweis für K[X]: Seien $P,Q \in K[X] - \{0\}$; dann gilt grad $P \geq 0$ und grad $Q \geq 0$; daher grad$(P \cdot Q)$ = grad P + grad $Q \geq 0$ und $P \cdot Q \neq 0$.

Bew. für $\mathbb{Z}$ s.z.B. A. Oberschelp, Aufbau des Zahlensystems, Göttingen 1968, S. 72 f.

(27.19) Anmerkung

Da beide Ringe außerdem kommutativ sind und mindestens 2 Elemente enthalten, sind sie sogar Integritätsbereiche (vgl. Def.(5.2)). Man kann zeigen (s.z.B. A. Oberschelp l.c., p.80 ff) , daß gilt:

Jeder Integritätsbereich lässt sich in einen Körper einbetten

Beispiele: $\mathbb{Z} \subseteq \mathbb{Q} = \{\frac{m}{n} | m,n \in \mathbb{Z},\ n \neq 0\}$ mit $\frac{m_1}{n_1} = \frac{m_2}{n_2} \Leftrightarrow m_1 n_2 = n_1 m_2$

$K[X] \subseteq K(X)$ mit $K(X) = \{\frac{P}{Q} | P,Q \in K[X],\ Q \neq 0\}$ und $\frac{P_1}{Q_1} = \frac{P_2}{Q_2} \Leftrightarrow P_1 Q_2 = Q_1 P_2$

Insbesonder gelten die von uns angeführten Definitionen und Rechengesetze auch für Matrizen, deren Einträge Polynome sind.