Prof. Dr. H. Brenner **Osnabrück WS 2015/2016**

Lineare Algebra und analytische Geometrie I

Vorlesung 20

Kultur ist Reichtum an Problemen.

Egon Friedell

Der Interpolationssatz

Satz 20.1. *Es sei K ein Körper und es seien n verschiedene Elemente $a_1, \ldots, a_n \in K$ und n Elemente $b_1, \ldots, b_n \in K$ gegeben. Dann gibt es ein eindeutiges Polynom $P \in K[X]$ vom Grad $\leq n-1$ derart, dass $P(a_i) = b_i$ für alle i ist.*

Beweis. Wir beweisen die Existenz und betrachten zuerst die Situation, wo $b_j = 0$ ist für alle $j \neq i$. Dann ist

$$(X - a_1) \cdots (X - a_{i-1})(X - a_{i+1}) \cdots (X - a_n)$$

ein Polynom vom Grad $n-1$, das an den Stellen $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ den Wert 0 hat. Das Polynom

$$\frac{b_i}{(a_i - a_1) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)} (X - a_1) \cdots (X - a_{i-1})(X - a_{i+1}) \cdots (X - a_n)$$

hat an diesen Stellen ebenfalls eine Nullstelle, zusätzlich aber noch bei a_i den Wert b_i. Nennen wir dieses Polynom P_i. Dann ist

$$P = P_1 + P_2 + \cdots + P_n$$

das gesuchte Polynom. An der Stelle a_i gilt ja

$$P_j(a_i) = 0$$

für $j \neq i$ und $P_i(a_i) = b_i$.

Die Eindeutigkeit folgt aus Korollar 19.9. □

Eine Beweisvariante bzw. Interpretationsvariante besteht darin, die durch $a_1, \ldots, a_n \in K$ insgesamt definierte Abbildung

$$K[X] \longrightarrow K^n,\ P \longmapsto (P(a_1), \ldots, P(a_n)),$$

zu betrachten. Diese Abbildung ist K-linear, da nach Bemerkung 19.8 die Komponenten linear sind. Der Interpolationssatz besagt, dass diese Abbildung surjektiv ist, was wie im Beweis bewiesen werden kann. Er besagt

sogar, dass diese Abbildung, wenn man sie auf den Untervektorraum aller Polynome vom Grad $\leq n-1$ einschränkt, ein Isomorphismus ist.

Einsetzen von Endomorphismen

Zu einer linearen Abbildung

$$f\colon V \longrightarrow V$$

auf einem K-Vektorraum kann man die Iterationen f^n, also die n-fache Hintereinanderschaltung von f mit sich selbst, betrachten. Ferner kann man lineare Abbildungen addieren und mit Skalaren aus dem Körper multiplizieren. Insgesamt sind somit Ausdrücke der Form

$$a_n f^n + a_{n-1} f^{n-1} + \cdots + a_2 f^2 + a_1 f + a_0$$

selbst wieder lineare Abbildungen von V nach V. Dabei ist

$$a_0 \, = \, a_0 f^0 \, = \, a_0 \operatorname{Id}_V$$

zu interpretieren. Es ist eine von vornherein keineswegs selbstverständliche Tatsache, dass die Untersuchung solcher polynomialer Kombinationen aus f bei der Untersuchung von f selbst hilfreich ist. Den beschriebenen Ausdruck kann man so auffassen, dass in das Polynom $a_n X^n + a_{n-1} X^{n-1} + \cdots + a_2 X^2 + a_1 X + a_0$ für die Variable X die lineare Abbildung f eingesetzt wird. Diese Zuordnung durch Einsetzen besitzt die folgenden strukturellen Eigenschaften.

Lemma 20.2. *Sei K ein Körper, V ein K-Vektorraum und*

$$f\colon V \longrightarrow V$$

eine lineare Abbildung. Dann erfüllt die Abbildung

$$K[X] \longrightarrow \operatorname{End}(V), \; P \longmapsto P(f),$$

die folgenden Eigenschaften.

(1) *Für konstante Polynome $P = a_0$ ist*

$$P(f) \, = \, a_0(f) \, = \, a_0 f^0 \, = \, a_0 \operatorname{Id}_V .$$

Insbesondere wird das Nullpolynom auf die Nullabbildung und das konstante 1-Polynom auf die Identität abgebildet.

(2) *Es ist*

$$(P+Q)(f) \, = \, P(f) + Q(f) \, = \, Q(f) + P(f)$$

für alle Polynome $P, Q \in K[X]$.

(3) *Es ist*

$$(P \cdot Q)(f) \, = \, P(f) \circ Q(f) \, = \, Q(f) \circ P(f)$$

für alle Polynome $P, Q \in K[X]$.

(4) *Es ist*

$$(X^n)(f) = f^n$$

für alle $n \in \mathbb{N}$.

Beweis. (1) und (4) stecken in der Definition des Einsetzungshomomorphismus drin. Daraus ergeben sich auch (2) und (3). □

Wenn V endlichdimensional ist, sagen wir die Dimension d besitzt, so sind sämtliche Potenzen f^k, $k \in \mathbb{N}$, Elemente im d^2-dimensionalen Vektorraum

$$\operatorname{Hom}_K(V,V) = \operatorname{End}(V)$$

aller linearen Abbildungen von V nach V. Wegen der Endlichkeit des Homomorphismenraumes müssen daher diese Potenzen linear abhängig sein, d.h. es gibt ein $m \in \mathbb{N}$ und Koeffizienten a_i, $0 \leq i \leq m$, die nicht alle 0 sind, mit

$$a_m f^m + a_{m-1} f^{m-1} + \cdots + a_2 f^2 + a_1 f + a_0 = 0$$

(dabei ist $m \leq d^2$ unmittelbar klar, wir werden später sehen, dass sogar stets $m \leq d$ ist). Das entsprechende Polynom $a_m X^m + a_{m-1} X^{m-1} + \cdots + a_2 X^2 + a_1 X + a_0$ hat also die Eigenschaft, dass es selbst nicht das Nullpolynom ist, dass aber, wenn man überall X durch f ersetzt, die Nullabbildung auf V herauskommt. Wir fragen uns:

- Gibt es eine Struktur auf der Menge aller Polynome $P \in K[X]$ mit $P(f) = 0$?
- Gibt es ein besonders einfaches Polynom $P_0 \in K[X]$ mit $P_0(f) = 0$?
- Wie kann man es finden?
- Welche Eigenschaften von f kann man aus der Faktorzerlegung von diesem Polynom P_0 ablesen?

Bemerkung 20.3. Sei K ein Körper, V ein endlichdimensionaler K-Vektorraum und

$$f\colon V \longrightarrow V$$

eine lineare Abbildung. Es sei $v_1, \ldots, v_n$ eine Basis von V und es sei M die zugehörige Matrix. Nach Lemma 11.9 entsprechen sich die Verknüpfung von linearen Abbildungen und die Matrixmultiplikation. Insbesondere entsprechen sich f^n und M^n. Ebenso entsprechen sich die Skalarmultiplikation und die Addition auf dem Endomorphismenraum $\operatorname{End}(V)$ und dem Matrizenraum. Daher kann man statt mit der Zuordnung $P \mapsto P(f)$ genauso gut mit der Zuordnung $P \mapsto P(M)$ arbeiten.

Ideale

Definition 20.4. Eine nichtleere Teilmenge $\mathfrak{a}$ eines kommutativen Ringes R heißt *Ideal*, wenn die beiden folgenden Bedingungen erfüllt sind:

(1) Für alle $a, b \in \mathfrak{a}$ ist auch $a + b \in \mathfrak{a}$.
(2) Für alle $a \in \mathfrak{a}$ und $r \in R$ ist auch $ra \in \mathfrak{a}$.

Die Eigenschaft, nichtleer zu sein, kann man durch die Bedingung $0 \in \mathfrak{a}$ ersetzen.

DEFINITION 20.5. Zu einer Familie von Elementen $a_1, a_2, \ldots, a_n \in R$ in einem kommutativen Ring R bezeichnet $(a_1, a_2, \ldots, a_n)$ das von diesen Elementen *erzeugte Ideal*. Es besteht aus allen *Linearkombinationen*

$$r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \,,$$

wobei $r_1, r_2, \ldots, r_n \in R$ sind.

DEFINITION 20.6. Ein Ideal $\mathfrak{a}$ in einem kommutativen Ring R der Form

$$\mathfrak{a} = (a) = Ra = \{ra : r \in R\}.$$

heißt *Hauptideal*.

Das Nullelement bildet in jedem Ring das sogenannte *Nullideal*, das wir einfach als $0 = (0) = \{0\}$ schreiben. Die 1 und überhaupt jede Einheit erzeugt als Ideal schon den ganzen Ring. Eine *Einheit* in einem kommutativen Ring R ist ein Element $x \in R$, für das es ein $y \in R$ mit $xy = 1$ gibt. Ein kommutativer Ring ist genau dann ein Körper, wenn alle Elemente außer der 0 Einheiten sind.

DEFINITION 20.7. Das *Einheitsideal* in einem kommutativen Ring R ist der Ring selbst.

In einem Körper gibt es nur diese beiden Ideale.

LEMMA 20.8. *Es sei R ein kommutativer Ring. Dann sind folgende Aussagen äquivalent.*

(1) *R ist ein Körper.*
(2) *Es gibt in R genau zwei Ideale.*

Beweis. Wenn R ein Körper ist, so gibt es das Nullideal und das Einheitsideal, die voneinander verschieden sind. Sei I ein von 0 verschiedenes Ideal in R. Dann enthält I ein Element $x \neq 0$, das eine Einheit ist. Damit ist $1 = xx^{-1} \in I$ und damit $I = R$.

Sei umgekehrt R ein kommutativer Ring mit genau zwei Idealen. Dann kann R nicht der Nullring sein. Sei nun x ein von 0 verschiedenes Element in R. Das von x erzeugte Hauptideal Rx ist $\neq 0$ und muss daher mit dem anderen Ideal, also mit dem Einheitsideal übereinstimmen. Das heißt insbesondere, dass $1 \in Rx$ ist. Das bedeutet also $1 = xr$ für ein $r \in R$, so dass x eine Einheit ist. □

Ideale in $K[X]$

Satz 20.9. *In einem Polynomring über einem Körper ist jedes Ideal ein Hauptideal.*

Beweis. Sei I ein von 0 verschiedenes Ideal in $K[X]$. Betrachte die nicht-leere Menge

$$\{\operatorname{grad}(P) |\, P \in I,\, P \neq 0\}\ .$$

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \operatorname{grad}(F)$. Wir behaupten, dass $I = (F)$ ist. Sei hierzu $P \in I$ gegeben. Aufgrund von Satz 19.4 gilt

$$P = FQ + R \text{ mit } \operatorname{grad}(R) < \operatorname{grad}(F) \text{ oder } R = 0\,.$$

Wegen $R \in I$ und der Minimalität von $\operatorname{grad}(F)$ kann der erste Fall nicht eintreten. Also ist $R = 0$ und P ist ein Vielfaches von F. □

Das Minimalpolynom

Definition 20.10. Sei V ein endlichdimensionaler K-Vektorraum und

$$f\colon V \longrightarrow V$$

eine lineare Abbildung. Dann heißt das eindeutig bestimmte normierte Polynom $\mu_f \in K[X]$ minimalen Grades mit

$$\mu_f(f) = 0$$

das *Minimalpolynom* von f.

Korollar 20.11. *Es sei V ein endlichdimensionaler Vektorraum über einem Körper K und es sei*

$$f\colon V \longrightarrow V$$

eine lineare Abbildung. Dann ist die Menge

$$\{P \in K[X] |\, P(f) = 0\}$$

ein Hauptideal im Polynomring $K[X]$, das vom Minimalpolynom μ_f erzeugt wird.

Beweis. Siehe Aufgabe 20.8. □

Beispiel 20.12. Zur Identität Id_V auf einem K-Vektorraum ist das Minimalpolynom gleich $X-1$. Dieses geht ja unter dem Einsetzungshomomorphismus auf

$$\mathrm{Id}_V - \mathrm{Id}_V = 0.$$

Ein konstantes Polynom a_0 geht auf $a_0\,\mathrm{Id}$, was, außer bei $a_0 = 0$ oder $V = 0$, nicht die Nullabbildung ist.

Für eine Streckung, also eine Abbildung der Form $\lambda\,\mathrm{Id}_V$, ist das Minimalpolynom, vorausgesetzt $\lambda \neq 0$ und $V \neq 0$, gleich $X - \lambda$. Für die Nullabbildung

auf $V \neq 0$ ist X das Minimalpolynom, bei $V = 0$ ist es das konstante Polynom 1.

Beispiel 20.13. Zur einer Diagonalmatrix

$$M = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & d_n \end{pmatrix}$$

mit verschiedenen Einträgen d_i ist das Minimalpolynom gleich

$$P = (X - d_1)(X - d_2) \cdots (X - d_n).$$

Dieses Polynom geht unter der Einsetzung auf

$$(M - d_1 E_n) \circ (M - d_2 E_n) \circ (M - d_n E_n)\,.$$

Wenden wir darauf den Standardvektor e_i an, so wird er von dem Faktor $(M - d_j E_n)$ auf $(d_i - d_j)e_i$ abgebildet. Der i-te Faktor sichert also, dass e_i insgesamt annulliert wird. Da somit eine Basis zu 0 gemacht wird, muss es sich insgesamt um die Nullabbildung handeln.

Angenommen, es würde ein Polynom Q kleineren Grades geben mit

$$Q(M) = 0.$$

Dann ist nach Korollar 20.11

$$P = QS$$

und nach Lemma 19.8 muss Q ein Teilprodukt der Linearfaktoren von P sein. Sobald man aber einen Faktor von P weglässt, sagen wir $X - d_i$, so wird e_i durch die zugehörige Abbildung nicht mehr annulliert.

Beispiel 20.14. Zur Matrix

$$M = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

ist X^2 das Minimalpolynom. Dieses Polynom wird beim Einsetzen zur Nullabbildung, wegen

$$M^2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Die Teiler von X^2 von kleinerem Grad sind konstante Polynome $\neq 0$ und $a_1 X$ mit $a_1 \neq 0$, aber diese Polynome annullieren nicht M.