Kapitel 8

Normalformen von Matrizen

Nachdem wir uns im vorigen Kapitel mit Moduln über einem Hauptidealring R und mit R-Modul-Homomorphismen $\varphi : N \longrightarrow M$ beschäftigt haben, wenden wir uns nun Vektorraum-Endomorphismen zu, d.h. Homomorphismen von einem Vektorraum in sich selbst. Bereits in der Linearen Algebra hatten wir gesehen, dass in diesem Fall das Auffinden von geeigneter Basen bzw. einer Normalform schwieriger ist, da nur eine Basis gewählt werden kann. Damals hatten wir den Begriff der Diagonalisierbarkeit eingeführt und diese Eigenschaft dann mittels Eigenwerttheorie genauer untersucht. Insbesondere war ein zentrales Ergebnis, dass ein K-Vektorraum-Endomorphismus φ genau dann diagonalisierbar ist, wenn V eine K-Basis aus Eigenvektoren von φ besitzt. Was geschieht jedoch, wenn keine solche Basis existiert, d.h. wenn der Endomorphismus nicht diagonalisierbar ist?

Genau an dieser Stelle setzen wir mit unseren Überlegungen ein und werden dabei auch die Ergebnisse aus dem vorigen Kapitel verwenden, um bei nicht diagonalisierbaren Vektorraum-Endomorphismen eine Normalform definieren und bestimmen zu können. Dazu werden wir bei gegebenem Körper K und K-Vektorraum V zuerst eine $K[t]$-Modulstruktur auf $End_K(V)$ einführen. mit deren Hilfe wir dann das Minimalpolynom eines K-Vektorraum-Endomorphismus definieren können, von dem wir später im Verlauf des Kapitels sehen werden, dass es stets Teiler des charakteristischen Polynoms des Endomorphismus ist, mit diesem aber bei weitem nicht immer übereinstimmt.

Die $K[t]$-Vektorraumstruktur auf $End_K(V)$ wird es uns erlauben, den Vektorraum V zu einem gegebenen K-Vektorraum-Endomorphismus in eine direkte Summe sogenannter zyklischer Unterräume zu zerlegen, so dass auf jedem Unterraum der Endomorphismus durch eine Matrix von einer bestimmten Struktur beschrieben wird und aus diesen Blöcken dann die Frobenius-Normalform des K-Vektorraum-Endomorphismus als Block-Diagonalmatrix zusammengesetzt werden kann. Eine weitere Verfeinerung der Kästenchen führt dann auf die Weierstraß-Normalform und die Jordan-Normalform, die wir zum Ende des Skripts (je nach verbleibender Zeit) noch kurz anreißen werden.

8.1 Minimalpolynom und zyklische Unterräume

Sei von hier an K stets ein Körper und V stets ein n-dimensionaler K-Vektorraum, auch wenn dies einmal nicht explizit mit erwähnt wird.

Wir wissen bereits aus der Linearen Algebra bzw. aus früheren Kapiteln, dass die K-Vektorraum-Endomorphismen sowohl die Struktur eines K-Vektorraums als auch eines Ringes tragen. Der Körper K selbst lässt sich mittels der folgenden Inklusion in $End_K(V)$ einbetten:

$$\begin{array}{rcl} \iota : K & \longrightarrow & End_K(V) \\ a & \longmapsto & a \cdot id_V . \end{array}$$

Wie in Aufgabe 10.2 bereits gezeigt, trägt $End_K(V)$ eine $K[t]$-Modulstruktur mittels der folgenden äußeren Verknüpfung:

$$\begin{array}{rcl} \cdot_F : K[t] \times V & \longrightarrow & V \\ (p = \sum_{i=0}^{d} a_i t^i, v) & \longmapsto & p \cdot_F v := \sum_{i=0}^{d} a_i F^i(v) \end{array}$$

Hier können wir auch die dazu eng verwandte Abbildung

$$\begin{array}{rcl} \Psi_F : K[t] & \longrightarrow & End_K(V) \\ p = \sum_{i=0}^{d} a_i t^i & \longmapsto & \Psi_F(p) := \sum_{i=0}^{d} a_i F^i \end{array}$$

betrachten, für die offensichtlich $\Psi_F(p) = p \ \cdot_F \ \_\_$ gilt. Aus einem leicht anderen Blickwinkel ist Ψ_F der Einsetzungshomomorphismus bzgl. des Einsetzens des Elementes F aus dem Ring $End_K(V)$ in Polynome aus $K[t]$.

Satz 8.1.1 *Mit den soeben eingeführten Bezeichnungen gilt:*

a) Ψ_F *ist sowohl* K*-Vektorraumhomomorphismus als auch Ring-Homomorphismus.*

b) $End_K(V) \cong K[t]/\langle g_F \rangle$ *für ein eindeutig bestimmtes normiertes Polynom* $g_F \in K[t]$.

c) *Jedes* $f \in K[t]$ *mit* $\Psi_F(f) = f(F) = 0_{End_K(V)}$ *ist ein Vielfaches von* g_F.

d) $\deg(g_F) \leq n^2$

Beweis: Nach Satz 2.5.12 ist Ψ_F ein Ringhomomorphismus. Die Eigenschaft, ebenfalls K-Vektorraumhomomorphismus zu sein, kann daher einfach als Verträglichkeit mit der Skalarmultiplikation über K nachgerechnet werden, was wir uns hier sparen, da es keine besonderen Schwierigkeiten bietet. Damit ist Aussage a) bewiesen.
Die Isomorphie in Aussage b) ergibt sich aus dem Homomorphiesatz für Ringe 4.5.1, wobei der Kern als Ideal im Hauptidealring $K[t]$ ein Hauptideal sein muss, dessen Erzeuger ein bis auf Assoziiertheit eindeutig bestimmtes Polynom ist. Da die Einheiten in $K[t]$ gerade die Elemente von $K \setminus \{0\}$ sind und die Bedingung der Normierung des Polynoms den Leitkoeffizienten eindeutig auf den Wert 1 festlegt, ist der Erzeuger eindeutig bestimmt und wird dann als g_F bezeichnet.
Die in c) betrachteten Element liegen in $\ker(\Psi_F) = \langle g_F \rangle$, was direkt die gewünschte Aussage liefert.
Zum Beweis von Aussage d) erinnern wir uns zuerst, dass $\dim_K(End_K(V)) = n^2$ für einen n-dimensionalen K-Vektorraum V. Damit ist die Familie von Endomorphismen $(id_V, F, F^2, \ldots, F^{n^2})$ sicher linear abhängig über K, was bedeutet, dass es ein Polynom f vom Grad n^2 in $K[t]$ gibt, so dass $f(F) = \Psi_F(f) = 0$. Nun muss nach c) das Minimalpolynom dieses f teilen, weswegen der Grad des Minimalpolynoms höchstens n^2 betragen kann.

□

Definition 8.1.2 *In der Notation des vorigen Satzes wird* g_F *als das* **Minimalpolynom** *von* F *bezeichnet.*

Nach unseren Überlegungen aus der Linearen Algebra sind der Ring der K-Vektorraum-Endomorphismen von V und der Ring $R^{\dim(V)\times\dim(V)}$ der quadratischen Matrizen passender Größe zueinander isomorph. Daher lassen sich die obigen Definitionen und Ergebnisse bzgl. des Minimalpolynoms genauso für quadratische Matrizen formulieren wie für Endomorphismen.

Gerade eben hatten wir bereits im Beweis von Satz 8.1.1,d) eine Familie von Endomorphismen $(id_V, F, F^2, \ldots)$ betrachtet. Was geschieht nun, wenn wir diese Endomorphismen auf einen festen Vektor $v \in V$ anwenden bzw. den Endomorphismus F immer wieder anwenden? In der Regel haben wir keine Kontrolle darüber, wohin v dabei abgebildet wird. Ist v ein Eigenvektor von F, dann wird v unter F^i immer auf Vielfache von sich selbst abgebildet. In der folgenden Definition werden wir noch eine Zwischenstufe zwischen den beiden Fällen einführen: F-zyklische Untervektorräume.

Definition 8.1.3 *Sei V ein K-Vektorraum und $F \in End_K(V)$. Sei $U \subseteq V$ ein Untervektorraum von V.*

a) U heißt F-invariant, falls $F(U) \subseteq U$, d.h.

$$\forall v \in U: \quad F(v) \in U.$$

b) U heißt F-zyklisch, falls

$$\exists v \in U: \quad U = \operatorname{span}_K(F^i(v) \mid i \in \mathbb{N}_0)$$

In diesem Fall schreibt man auch kurz $U = U(F, v)$.

Wie im Fall eines diagonalisierbaren Endomorphismus, wo wir eine Basis von V aus Eigenvektoren zum Erreichen einer Normalform verwendet haben, werden wir für die im nächsten Abschnitt folgende Frobenius-Normalform F-zyklische Unterräume als Bausteine verwenden. Dazu sollten wir diese nun noch ein wenig genauer kennenlernen.

Lemma 8.1.4 *Seien K, V und F wie zuvor und sei $U \subseteq V$ ein Untervektorraum. Dann ist U genau dann F-invarianter Untervektorraum von V, wenn U ein $K[t]$-Untermodul von V ist.*

Beweis: Da U nach Voraussetzung nicht leer ist und ebenfalls nach Voraussetzung die Addition abgeschlossen in U ist, ist die folgende Äquivalenz zu zeigen:

U ist F-invarianter Untervektorraum $\iff U$ abgeschlossen unter $K[t] \cdot_F \_\_$

Ist U F-invarianter Untervektorraum von V, so gilt $F(v) \in U$ und damit auch $t^i \cdot_F v = F^i(v) \in U$ für alle $v \in U$ und $i \in \mathbb{N}_0$. Damit ist die Abgeschlossenheit unter der Skalarmultiplikation gezeigt und damit die Untermodul-Eigenschaft bewiesen.
Ist andererseits U ein $K[t]$-Untermodul von V, so gilt insbesondere $F(v) = t \cdot_F v \in U$ für alle $v \in U$, was die F-Invarianz zeigt.

$\square$

Führen wir diese Überlegung noch ein wenig weiter, so sehen wir direkt, dass auch F-zyklisch sich als eine Untermoduleigenschaft formulieren läßt:

Bemerkung 8.1.5 *Seien K, V und F wie zuvor und sei $U \subseteq V$ ein Untervektorraum. Dann ist U genau dann F-zyklisch, wenn es ein $v \in U$ gibt mit $U = K[t] \cdot_F v$.*

Wie bereits vorher erwähnt sollen die F-zyklischen Unterräume uns bei der Konstruktion einer Normalform für Endomorphismen helfen. Dazu sollten wir noch einen Bezug zu Matrizen von 'besonders schöner Gestalt' herstellen. Überraschenderweise steigen wir dazu von einer anderen Seite ein: wir definieren eine Begleitmatrix zu einem gegebenen normierten Polynom und betrachten das charakteristische Polynom bzw. das Minimalpolynom dieser Matrix – mit sehr erfreulichem Ergebnis!

Definition 8.1.6 *Sei K ein Körper und $p \in K[t]$ ein normiertes Polynom vom Grad $\deg(p) = m > 0$, d.h.*

$$p = t^m + \sum_{i=0}^{m-1} c_i t^i.$$

Dann heißt die Matrix

$$B(p) := \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & 0 & -c_2 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & -c_{m-2} \\ 0 & 0 & 0 & \dots & 0 & 1 & -c_{m-1} \end{pmatrix} \in K^{m \times m}$$

die **Begleitmatrix** *zu p.*

Satz 8.1.7 *Sei K ein Körper und sei $g \in K[t]$ ein normiertes Polynom positiven Grades. Dann gilt:*

a) g ist das charakteristische Polynom zu $B(g)$.

b) g ist das Minimalpolynom zu $B(g)$.

Beweisidee: Für Teil a) ist die Aussage per Induktion über den Grad von p und direkte Berechnung der Determinante von $B(g) - tE_m$ direkt nachzurechnen. Für Teil b) verwendet der geschickteste Beweis den Satz von Cayley-Hamilton, den wir im folgenden Abschnitt kennenlernen werden.

($\square$)

Wichtig ist an dem Satz vor allem, dass es zu jedem normierten Polynom positiven Grades eine Matrix gibt, die es sowohl als charakteristisches Polynom als auch als Minimalpolynom besitzt.

Satz 8.1.8 *Sei V ein endlich-dimensionaler K-Vektorraum und $F \in End_K(V)$. Sei außerdem $v \in V$ und $U := U(F, v)$ der von v erzeugte F-zyklische Untervektorraum von V. Dann gilt:*

a) U ist F-invariant und $F_v = F\mid_U \in End_K(U)$

b) $\varphi_v = \_\_ \cdot_{F_v} v : K[t] \longrightarrow U$ ist ein K-Vektorraumhomomorphismus und $K[t]$-Modul-Homomorphismus.

c) $U \cong K[t]/\langle g \rangle$ für ein eindeutig bestimmtes normiertes Polynom $g \in K[t]$

d) Für jedes $f \in K[t]$ mit $f \cdot_{F_v} v = 0$ gilt $g \mid f$.

e) Setze $m := \deg(g)$. Dann ist $\mathcal{C} = (v, F(v), \ldots, F^{m-1}(v))$ eine K-Basis von U und

$$M_{\mathcal{C}}^{\mathcal{C}}(F_v) = B(g)$$

f) g ist Minimalpolynom von F_v und von $B(g)$.

Beweis: Nach Konstruktion ist $U = \{F^i(v) \mid i \in \mathbb{N}_0\}$, weswegen $F(U) = \{F^i(v) \mid i \in \mathbb{N}\} \subseteq U$ ist. Wegen der F-Invarianz von U ist dann offensichtlich auch $F\mid_U \in End_K(U)$. Damit ist Aussage a) bewiesen.
Aussage b) läßt sich durch direktes Überprüfen der Verträglichkeit mit den

Operationen nachweisen, was wir uns hier sparen, das es keine Schwierigkeiten bietet.
Nach dem Homomorphiesatz gilt $U \cong K[t]/\ker(\varphi_v)$, wobei $\ker(\varphi_v)$ ein Ideal im Hauptidealring $K[t]$ ist. Es kann also von einem einzigen Polynom erzeugt werden, welches bis auf Assoziiertheit eindeutig ist. Die Normierung legt g dann eindeutig fest, womit Aussage c) bewiesen ist.
Das Polynom f aus Aussage d) liegt in $\ker(\varphi_v)$ und ist daher ein Vielfaches des in c) eingeführten Polynoms g.
Da $\dim_K(U) = \deg(g) = m$ gilt, muss die gesuchte Basis $\mathcal{C}$ aus m Elementen bestehen. Andererseits ist $(F^i(v) \mid i \in \mathbb{N}_0)$ ein Erzeugendensystem von U. Wäre nun die Unterfamilie $(F^i(v) \mid 0 \leq i \leq m-1)$ linear abhängig, so gäbe es eine nicht-triviale Relation $0 = \sum_{i=0}^{m-1} \alpha_i F^i(v) = \phi_v(\sum_{i=0}^{m-1} \alpha_i t^i)$ und damit ein Polynom von positivem Grad höchstens $m-1$ in $\langle g \rangle$ im Widerspruch zum Grad von g. Die Gestalt der darstellenden Matrix ergibt sich dann durch direkte Rechnung, die man beim Nacharbeiten mal für ein konkretes, nicht zu großes m ausführen sollte.
Nach Satz 8.1.7 ist g das Minimalpolynom von $B(g)$ und damit das Minimalpolynom des Endomorphismus F_v, dessen darstellende Matrix bzgl. $\mathcal{C}$ die Begleitmatrix $B(g)$ ist.

$\square$