Die Jordansche Normalform und endlich erzeugte Torsionsmoduln über Hauptidealringen

Zu den Vorlesungen *Lineare Algebra I,II* von Florian Pop
Bonn, Wintersemester 2002/2003 — Sommersemester 2003
Jakob Stix — im Mai 2003

Inhaltsverzeichnis

Die Jordannormalform stellt das erste interessante Strukturtheorem der linearen Algebra dar. Es beantwortet die Frage nach der Klassifikation von Endomorphismen eines endlich dimensionalen Vektorraums. Zwar hat man üblicherweise, wenn man in der Vorlesung über lineare Algebra auf diese Fragestellung trifft, schon andere Strukturaussagen angetroffen: alle Vektorräume sind frei und über ihre Dimension klassifiziert; lineare Abbildungen entsprechen Matrizen; der Raum der Determinantenfunkionen hat Dimension 1. Jedoch fällt die Antwort im Fall der Jordannormalform deutlich vielfältiger aus. Es verwundert daher nicht, daß auch der Beweis und die algebraischen Hilfsmittel aufwendiger sind.

Der vorliegende Text leitet die Jordannormalform aus dem Elementarteilersatz ab. Dies entspricht dem Vorgehen der Vorlesung. Ist man an diesem Ansatz interessiert, so braucht man nur die Kapitel 1 & 4 zu lesen. Allerdings befinden sich die wesentlichen Beispiele, die insbesondere den 'Jordanblock' einführen in Kapitel 2. Dort wird man auch auf einen anderen Zugang zum Struktursatz vorbereitet, der dann in Kapitel 3 verfolgt wird. Der Struktursatz wird in Kapitel 3 in seinem schwierigsten Abschnitt mit drei unterschiedlichen Argumenten bewiesen. Aus dieser Perspektive ist die Jordannormalform ein Korollar aus dem Struktursatz.

Mein Dank gilt Armin Holschbach und Igor Ronkine für eine kritische Durchsicht einer ersten Version dieses Textes.

1 Algebraische Grundlagen

Alle Ringe seien kommutativ und mit 1.

1.1 Quotienten

Sei R ein Ring und M ein R-Modul. Zu einem Untermodul $N \subset M$ kann man den Quotienten M/N bilden. Dieser ist über die folgende Eigenschaft charakterisiert.

Definition 1.1. (1) Eine Abbildung von R-Modulen $\mathrm{pr} : M \to \overline{M}$ heißt **Quotient von M nach dem R-Untermodul $N \subset M$**, falls: (i) $\mathrm{pr}(N) = 0$ und (ii) jeder Morphismus $\varphi : M \to T$ in einen R-Modul T mit $\varphi(N) = 0$ eindeutig zu einem Morphismus $\overline{\varphi} : \overline{M} \to T$ faktorisiert, dh. $\varphi = \overline{\varphi} \circ \mathrm{pr}$. Die Abbildung pr heißt **Quotientenabbildung**.

(2) Eine Abbildung von R-Moduln $p : M \to \overline{M}$ heißt **Kokern** des R-Modulhomomorphismus $f : N \to M$, falls: (i) $p \circ f = 0$ und (ii) jeder Morphismus $\varphi : M \to T$ in einen R-Modul T mit $\varphi \circ f = 0$ eindeutig zu einem Morphismus $\overline{\varphi} : \overline{M} \to T$ faktorisiert, dh. $\varphi = \overline{\varphi} \circ p$. Die Abbildung p heißt **Quotientenabbildung**. Nachlässigerweise nennt man oft $\overline{M}$ einfach $coker(f)$ oder den Kokern von f.

Wie üblich kontrolliert die universelle Eigenschaft Quotienten und Kokerne. Etwa folgt aus der Definition leicht, daß Quotienten und Kokerne eindeutig sind bis auf eindeutigen Isomorphismus und daß $coker(f)$ der Quotient von M nach dem Bild $f(N)$ ist. Beide Begriffe müssen aber durch eine Konstruktion, welche ihre Existenz zeigt, zum Leben erweckt werden.

Sei $N \subset M$ ein Untermodul. Auf M wird durch $m \sim m' \iff m' - m \in N$ eine Äquivalenzrelation definiert. Die Menge der Äquivalenzklassen bezeichnen wir mit M/N. Die Abbildung $\mathrm{pr} : M \to M/N$ ordne jedem m seine Klasse $\overline{m} := m + N$ zu. Man mache sich klar, daß auf M/N eine eindeutige R-Modulstruktur existiert, so daß pr ein R-Modulhomomorphismus ist. Man hat nur zu beobachten, daß die Summe zweier Klassen und das a-fache einer Klasse für $a \in R$ wieder nur in **einer** Klasse in M/N sind:

$$(m + N) + (m' + N) = (m + m') + N, \qquad a(m + N) = am + aN \subset am + N \ .$$

Die Axiome für diese Operationen sowie die Eigenschaft, daß pr ein Abbildung von R-Moduln ist, folgen automatisch. Offensichtlich ist $\mathrm{pr} : M \to M/N$ ein Quotient von M nach N. Denn sei $\varphi : M \to T$ gegeben, so kann eine Faktorisierung $\overline{\varphi} : M/N \to T$ nur durch

$$\overline{\varphi} : m + N \mapsto \varphi(m)$$

definiert werden. Das einzige Problem ist die Wohldefiniertheit, ein Morphismus ist $\overline{\varphi}$ automatisch. Dieses $\overline{\varphi}$ ist genau dann wohldefiniert, wenn für alle $m \in M$ und $n \in N$ schon $\varphi(m + n) = \varphi(m)$ gilt. Dies ist offenbar äquivalent mit $\varphi(N) = 0$.

Die Konstruktion zeigt auch, daß Quotientenabbildungen surjektiv sind.

Definition/Satz 1.2 (Homomorphiesatz). Ist $f : M \twoheadrightarrow \overline{M}$ eine surjektive Abbildung von R-Moduln, dann heißt nachlässigerweise $\overline{M}$ auch Quotient von M, denn es gilt kanonisch $\overline{M} \cong M/\ker(f)$. Es ist also in der Tat f ein Quotient von M nach dem Untermodul $\ker(f)$.

Beweis: Gemäß der universellen Eigenschaft induziert f wegen $f\big(\ker(f)\big) = 0$ eine Abbildung $M/\ker(f) \to \overline{M}$ von R-Moduln. Diese ist injektiv und surjektiv. □

Die Notation M/N deutet an, daß man die Information aus N vernachlässigt hat und nur noch betrachtet, was in M zwischen 'M und N' oder 'modulo N' passiert.

Die Untermoduln des Rings R aufgefaßt als R-Modul über sich selbst heißen **Ideale** des Rings. Das von Elementen $a_i \in R, i \in I$ erzeugte Ideal bezeichnet man mit $(a_i; i \in I)$. Es

enthält alle endlichen (d.h. fast alle $r_i = 0$) Summen $\sum_i r_i a_i$ mit $r_i \in R$. Sei $\mathfrak{a} \subset R$ ein Ideal von R. Dann ist $R/\mathfrak{a}$ nicht nur ein R-Modul, sondern sogar ein Ring und $\mathrm{pr} : R \to R/\mathfrak{a}$ ein Ringhomomorphismus. Die Multiplikation auf $R/\mathfrak{a}$ wird wieder durch

$$(r + \mathfrak{a}) \cdot (r' + \mathfrak{a}) = rr' + r\mathfrak{a} + r'\mathfrak{a} + \mathfrak{a}^2 \subset rr' + \mathfrak{a}$$

auf ihre Wohldefiniertheit überprüft. Die Axiome eines Rings gelten für $R/\mathfrak{a}$ automatisch. Sie folgen aus den entsprechenden Eigenschaften von R. Es gilt nun der Satz:

Satz 1.3. *$R/\mathfrak{a}$-Moduln entsprechen eindeutig R-Moduln, auf denen $\mathfrak{a}$ trivial operiert. Für solche Moduln M, N gilt* $\mathrm{Hom}_R(M, N) = \mathrm{Hom}_{R/\mathfrak{a}}(M, N)$.

Beweis: Die Aussage des Satzes muß wie folgt präzisiert werden: (1) ein $R/\mathfrak{a}$-Modul M wird vermöge $r \cdot m = (r+\mathfrak{a})m, \forall r \in R, m \in M$ ein R-Modul, (2) gilt in einem R-Modul N, daß $\mathfrak{a}N = 0$ verschwindet, so trägt N eine $R/\mathfrak{a}$-Modulstruktur vermöge $(r + \mathfrak{a}) \cdot n = rn, \forall r \in R, n \in N$.

Man hat nur die Wohldefiniertheit nachzuweisen. Die Aussage über die Hom's ergibt sich unmittelbar. □

Definition 1.4. (1) Sei $x \in M$ ein Element eines R-Moduls. Das **Annulatorideal** von x ist das Ideal

$$\mathrm{Ann}(x) = \{r \in R \,|\, rx = 0\}.$$

(2) Sei M ein R-Modul. Das **Annulatorideal** von M ist

$$\mathrm{Ann}(M) = \{r \in R \,|\, \forall x \in M : \; rx = 0\} = \bigcap_{x \in M} \mathrm{Ann}(x).$$

Damit ist $\mathrm{Ann}(x)$ nichts anderes als der Kern der Abbildung $R \to M, r \mapsto rx$. Man erhält eine Injektion

$$\iota : R/\mathrm{Ann}(x) \hookrightarrow M, \qquad \overline{r} \mapsto rx \; . \tag{1.1}$$

Das Annulatorideal ist gerade so definiert, daß ι wohldefiniert und injektiv ist. Das Bild von ι ist der von x erzeugte R-Untermodul $\langle x \rangle_R$ für den wir deshalb auch $\big(R/\mathrm{Ann}(x)\big) \cdot x = Rx \subseteq M$ schreiben.

1.2 Hauptidealringe

Ordnet man einem mathematischen Objekt einen linearen Raum als Invariante zu, so erbt dieser zu jeder Symmetrie des Objekts einen Endomorphismus. Die Frage nach der Klassifikation von Endomorphismen liegt daher auf der Hand. Der algebraische Gehalt dieser Frage wird durch die folgende Beobachtung anvisiert, siehe auch [ArtinM, Kap. 12 §7].

Satz 1.5 (Übersetzungssatz).

(1) Sei K ein Körper. Dann entsprechen sich folgende Daten:

- *(a) $K[X]$-Moduln M.*
- *(b) K-Vektorräume V zusammen mit einem Endomorphismus $\varphi \in \mathrm{End}_K(V)$.*

(2) Entsprechen sich M und (V, φ) nach (1), so gibt es folgende Beziehungen ihrer Struktur:

- *(a) Die Multiplikation mit X auf M entspricht dem Endomorphismus φ von V.*
- *(b) Untermoduln von M entspechen φ-invarianten Unterräumen von V.*
- *(c) Eine Zerlegung von M als direkte Summe von $K[X]$-Moduln entspricht einer Zerlegung von V als direkte Summe von φ-invarianten Unterräumen.*

(d) *Zyklische, d.h. von einem Element erzeugte Moduln M entsprechen φ-zyklischen V, d.h. V wird aufgespannt von $v, \varphi(v), \varphi^2(v), \ldots$ für ein Element $v \in V$.*

(e) *Das Annulatorideal von M wird vom Minimalpolynom von φ auf V erzeugt.*

(f) *Es ist M endlich erzeugt als $K[X]$-Modul und Torsion, d.h. jedes $m \in M$ wird von einem von 0 verschiedenen Element $f \in K[X]$ annulliert ($fm = 0$), genau dann wenn V endliche K-Dimension hat.*

Beweis: (1) Dies muß wieder präzisiert werden. Sei (V, φ) ein Paar wie in (b). Dann wird für $v \in V$ und $a_0 + a_1X + \ldots + a_nX^n \in K[X]$ durch

$$(a_0 + a_1X + \ldots + a_nX^n)v := a_0v + a_1\varphi(v) + \ldots a_n\varphi^n(v)$$

auf V eine $K[X]$-Modulstruktur erklärt ($\varphi^n = \varphi \circ \ldots \circ \varphi$ mit n-Faktoren φ).

Sei andererseits M ein $K[X]$-Modul, so operiert $K \subset K[X]$ durch die konstanten Funktionen auf M und macht aus dem Modul einen K-Vektorraum. Als K-Vektoraum trägt M einen Endomorphismus $\varphi : m \mapsto Xm$, die Multiplikation mit X. Diese verträgt sich mit der K-Vektorraumstruktur, da im Polynomring $aX = Xa$ für $a \in K$ gilt.

Diese beiden Konstruktionen sind invers zueinander und liefern nur unterschiedliche Betrachtungsweisen der algebraischen Struktur auf der Menge $V = M$.

(2) Der Beweis der Aussagen (a)–(d) sollte unmittelbar klar sein. Die Aussage (e) gilt per Definition des Minimalpolynoms. Daß man überhaupt ein Minimalpolynom definieren kann, folgt aus der Eigenschaft des Polynomrings, ein Hauptidealring zu sein.

Bei (f) schließe man wie folgt. Ist M erzeugt von $m_1, \ldots, m_s$, welche jeweils von $f_i(X) \in K[X]$ annulliert werden, dann gibt es eine surjektive Abbildung

$$\bigoplus_{i=1}^{s} K[X]/\big(f_i(X)\big) \twoheadrightarrow M, \quad \big(\overline{h_i(X)}\big)_{1\le i\le s} \mapsto \sum_{i=1}^{s} h_i(X)m_i \ .$$

Der Modul $K[X]/\big(f(X)\big)$ hat eine K-Basis $1, X, \ldots, X^{\deg(f)-1}$ und ist somit als K-Vektorraum endlich dimensional. Dies gilt dann auch für den Quotienten M.

Ist andererseits V von endlicher Dimension, so folgt nach dem Satz von Cayley–Hamilton, siehe Satz A.1, daß die Auswertung in $X = \varphi$ des charakteristischen Polynoms $\mathrm{chr}_\varphi(X)$ des Endomorphismus φ die Nullabbildung ist. Mit anderen Worten $\mathrm{chr}_\varphi(X)V = 0$. Somit liefert die $K[X]$-Modulstruktur auf V einen Torsionsmodul. Er ist endlich erzeugt, da dies bereits für V gilt, wo man zum Erzeugen ja nur den Teilring $K \subset K[X]$ zur Verfügung hat. □

Das Studium von Endomorphismen von K-Vektorräumen wird nach Satz 1.5 auf das Studium von Moduln unter $K[X]$ reduziert.

Beispiel 1.6. (1) Sei V ein endlich dimensionaler Vektorraum mit Endomorphismus φ. Der entsprechende $K[X]$-Modul M zerfalle als direkte Summe $M = M_1 \oplus M_2$. Dann hat φ in einer geeigneten Basis Blockdiagonalgestalt. In der Tat hat man nur die Basis von V aus Basen der den Moduln M_i zugrundeliegenden Vektorräumen zusammenzusetzen. Aus $\varphi(M_i) \subseteq M_i$ und der Art und Weise, wie man Endomorphismen Matrizen zuordnet, folgt die Blockdiagonalform glasklar. Wem dies nicht so geht, der oder die wiederhole das Thema Endomorphismen und Matrizen.

(2) Sei V ein φ-zyklischer Modul mit Erzeuger $v \in V$. Sei $(f) \subset K[X]$ das Annulatorideal von $v \in V$, wobei wir V als $K[X]$-Modul auffassen. Wir nehmen oBdA an, daß $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ normiert und vom Grad n ist. Die Abbildung (1.1) liefert einen Isomorphismus $K[X]/(f) \cong V$ von $K[X]$-Moduln. Wir studieren daher das Beispiel $K[X]/(f)$, wobei φ durch die Multiplikation mit X gegeben ist.

Die bevorzugte Basis ist nun $\mathscr{B} = (1, X, X^2, \ldots, X^{n-1})$. Es ergibt sich folgende Matrix, die **Begleitmatrix** zu f. (Zur Klarheit dieses Fakts siehe (1)).

$$\Lambda(f) := \mathscr{M}^{\mathscr{B}}_{\mathscr{B}}(\varphi) = \mathscr{M}^{\mathscr{B}}_{\mathscr{B}}(X\cdot) = \begin{pmatrix} 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & \ddots & & 0 & -a_1 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{n-2} \\ 0 & \ldots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

Ist speziell $f(X) = X - \lambda$ für ein $\lambda \in K$, so ist $K[X]/(X - \lambda)$ von Dimension 1 und die Begleitmatrix ist $\Lambda(X - \lambda) = (\lambda) \in \mathscr{M}_1(K)$. Es operiert X durch Multiplikation mit λ.

(3) Eine **(fallende) Filtration** der Länge n eines Moduls M ist eine Folge von Untermoduln F^iM für $0 \leq i \leq n$ mit

$$M = F^0M \supseteq F^1M \supseteq \ldots \supseteq F^iM \supseteq F^{i+1}M \supseteq \ldots \supseteq F^nM = 0 \ .$$

Besitzt der endlich erzeugte Torsions-$K[X]$-Modul M eine solche fallende Filtrierung, so gilt $XF^iM \subset F^iM$ und die Matrix des zugehörigen Endomorphismus hat untere Blockdreiecksgestalt. Man wählt für die Quotienten $F^iM/F^{i+1}M$ Basen als K-Vektorräume und liftet diese zu Systemen $\mathscr{B}_i$ von Elementen in F^iM. Dann ist $\mathscr{B} = (\mathscr{B}_0, \mathscr{B}_1, \ldots, \mathscr{B}_{n-1})$ eine geeignete Basis für die untere Blockdiagonalgestalt. Auch dies sollte glasklar sein, siehe (1).

Natürlich ist die Richtung der Nummerierung in der Filtration willkürlich. Dreht man sie um, so erhält man eine **(steigende) Filtration** der Länge n auf dem Modul M als eine Folge von Untermoduln F_iM für $0 \leq i \leq n$ mit

$$0 = F_0M \subseteq F_1M \subseteq \ldots \subseteq F_iM \subseteq F_{i+1}M \subseteq \ldots \subseteq F_nM = M \ .$$

Jetzt ergibt sich analog mit den Lifts $\mathscr{B}_i$ von Basen der $F_iM/F_{i-1}M$ als K-Vektorräume eine Basis $\mathscr{B} = (\mathscr{B}_1, \ldots, \mathscr{B}_n)$ von M als K-Vektorraum, in dem die Multiplikation mit X obere Blockdreiecksgestalt annimmt.

Der Ring $K[X]$ ist ein Hauptidealring und dies ist für die weitere algebraische Betrachtung seine wesentliche Eigenschaft:

Definition 1.7. Ein **Hauptidealring** ist ein Integritätsring R, in dem jedes Ideal von **einem** Element aus R erzeugt wird. Jedes Ideal ist also ein Hauptideal.

Wir erinnern an folgende Fakten:

Satz 1.8. *Hauptidealringe sind faktoriell.*

Beweis: [Meyb, Satz 3.6.14]. □

Das bedeutet: In einem Hauptidealring sind irreduzible Elemente prim und es gilt die eindeutige Primfaktorzerlegung. Es heißen zwei Elemente assoziiert, wenn sie sich nur um eine Einheit unterscheiden. In Primfaktorzerlegungen gelten assoziierte Primelemente als gleich.

Satz 1.9. *Euklidische Ringe sind Hauptidealringe.*

Beweis: [Meyb, Satz 3.6.18]. □

In der Tat kann man mit Hilfe der euklidischen Gradfunktion und der geforderten/axiomatisierten Eigenschaft 'Teilen mit kleinerem Rest' feststellen, daß jedes Ideal $\mathfrak{a}$ eines euklidischen Rings R von einem Element kleinsten Grades in $\mathfrak{a}$ erzeugt wird. Beispiele für euklidische Ringe und damit Hauptidealringe sind $\mathbb{Z}$ und $K[X]$.

In einem Hauptidealring kann man aufgrund der Faktorialität vom kleinsten gemeinsamen Vielfachen oder dem größten gemeinsamen Teiler von endlich vielen Elementen sprechen. Diese sind auch wieder nur bis auf Einheiten wohldefiniert. Ein zentrales Motiv der Strukturtheorie von Moduln über Haupidealringen ist der folgende Satz.

Satz 1.10 (Satz von Bézout). *Sei R ein Hauptidealring und $a_1, \ldots, a_n \in R$ mit größtem gemeinsamen Teiler d. Dann gilt $(a_1, \ldots, a_n) = (d)$. Insbesondere gibt es $\alpha_i \in R, 1 \leq i \leq n$ mit $\sum_i \alpha_i a_i = d$.*

Beweis: Das von $a_1, \ldots, a_n$ erzeugte Ideal ist ein Hauptideal (d'). Da alle a_i von d geteilt werden, gilt $(d') \subseteq (d)$.

Andererseits liegt $a_i \in (d')$ und somit teilt d' alle a_i und damit auch deren größten gemeinsamen Teiler d, ergo $(d) \subseteq (d')$.

Aus $(d) = (d') = (a_1, \ldots, a_n)$ folgt, daß d eine R-Linearkombination der a_i ist. □

Dem Satz von Bézout folgend vereinbaren wir für den größten gemeinsamen Teiler d von Elementen $a_1, \ldots, a_n$ eines Hauptidealrings R die Notation $d = (a_1, \ldots, a_n)$, also die gleiche, wie für das von den Elementen erzeugte Ideal. Elemente $a_1, \ldots, a_n$ heißen **teilerfremd**, wenn $(a_1, \ldots, a_n) = 1$.

Der euklidische Algorithmus führt für euklidische Ringe, etwa für $\mathbb{Z}$ und $K[X]$, zu einer effektiven Version des Satzes von Bézout, siehe Aufgabe 15, LA2, SoSe 2003.

Satz 1.11 (Chinesischer Restsatz). *Seien $a, b \in R$ teilerfremde Elemente eines Hauptidealrings R. Dann gilt kanonisch $R/(ab) \cong R/(a) \times R/(b)$.*

Korollar 1.12. *Ist speziell $R = K[X]$ und $f = \prod_{i=1}^{n} p_i^{e_1}$ die Zerlegung in (paarweise verschiedene) Primfaktoren p_i von f, so gilt kanonisch*

$$K[X]/(f) \cong \prod_{i=1}^{n} K[X]/(p_i^{e_i}) \ .$$

Zunächst ein paar Anmerkungen: (a) Das Korollar 1.12 gilt natürlich auch für beliebige Hauptidealringe und folgt per Induktion über die Anzahl der verschiedenen Primfaktoren, die in f auftauchen, sofort aus Satz 1.11. Wir haben hier auf den Fall $K[X]$ spezialisiert, damit der Fall, der uns interessiert, besonders hervorgehoben wird. Zyklische Moduln wie in Beispiel 1.6(2) sind also nur dann Kandidaten für einen unzerlegbaren, quasi atomaren Bestandteil unseres Klassifikationsproblems, wenn das Annulatorideal (f) von einer Primpotenz erzeugt wird. Man überlege sich, daß dann in der Tat der Modul $K[X]/(p^e)$ keine weitere Zerlegung als direkte Summe von $K[X]$-Moduln zuläßt.

(b) Der Chinesische Restsatz limitiert Eindeutigkeitsaussagen für Zerlegungen von Moduln über Hauptidealringen als Summe zyklischer Moduln.

(c) In der obigen Formulierung tauchen direkte Produkte statt direkter Summen auf. Da nur endlich viele Summanden/Faktoren auftreten, sind beide Konstruktionen als Moduln kanonisch isomorph, vgl. Aufgabe 5, LA 2, SoSe 2003. Die natürlichen Abbildungen $R/(ab) \twoheadrightarrow R/(a)$ und $R/(ab) \twoheadrightarrow R/(b)$ liefern allerdings (i) eine Abbildung in das Produkt und sind (ii) überdies auch Abbildungen von Ringen. Für Ringe sind Produkte wieder Ringe, während man für Objekte mit der universellen Eigenschaft der Summe das Tensorprodukt bemühen muß.

Beweis von Satz 1.11: Nach dem Satz von Bézout gibt es $\alpha, \beta \in R$ mit $1 = \alpha a + \beta b$. Wir setzen $e_a := \beta b$ und $e_b = \alpha a$. Damit gilt $e_a + e_b = 1$ und in $R/(ab)$ auch $e_a e_b = \alpha\beta ab = 0$, woraus $e_a^2 = e_a(e_a + e_b) = e_a$ und $e_b^2 = e_b$ in $R/(ab)$ folgt. Des weiteren gilt in $R/(a)$, daß $e_b = 0$ und $e_a = 1 - e_b = 1$. Analog gilt $e_a = 0$ und $e_b = 1$ in $R/(b)$.

Damit erhält man zur kanonischen Abbildung $\mathrm{pr} : R/(ab) \to R/(a) \times R/(b), r \mapsto \big(r, r\big)$ das folgende Inverse $\psi : (r, s) \mapsto re_a + se_b$. Dazu muß man nachrechnen, daß die Abbildungen pr und ψ wohldefiniert sind und

- $\psi(\mathrm{pr}(r)) = re_a + re_b = r(e_a + e_b) = r$ in $R/(ab)$,
- $\mathrm{pr}(\psi(r,s)) = \big(re_a + se_b, re_a + se_b\big) = (r,s)$ in $R/(a) \times R/(b)$.

Damit ist tatsächlich ψ ein Inverses zu pr und der Satz bewiesen. □

Alternativer Beweis: Wir bestimmen den Kern der Abbildung $\mathrm{pr} : R \to R/(a) \times R/(b)$, welche $r \in R$ nach $(\overline{r}, \overline{r})$ abbildet. Es gilt $r \in \ker(\mathrm{pr})$ genau dann, wenn $r \in (a)$ und $r \in (b)$, also r sowohl Vielfaches von a als auch von b ist. Da a und b teilerfremd sind, folgt aus der endeutigen Primfaktorzerlegung in R, daß r ein Vielfaches des Produktes ab sein muß. Daher ist $\ker(\mathrm{pr}) = (ab)$. Nach der universellen Eigenschaft des Quotienten $R/(ab)$ faktorisiert pr zu einer Abbildung $\overline{\mathrm{pr}} : R/(ab) \to R/(a) \times R/(b)$. Da $\ker(\mathrm{pr}) = (ab)$ gilt ist $\overline{\mathrm{pr}}$ injektiv. Bis jetzt haben wir nur die eindeutige Primfaktorzerlegung ausgenutzt (dies reicht nicht für die Surjektivität, wie das Beispiel $\mathbb{Z}[X]$ mit $a = X$ und $b = 2$ zeigt).

Wir verwenden entweder die Idempotente e_a, e_b aus dem vorherigen Beweis und finden mit $r_e a + se_b$ ein Urbild von (r,s) oder wir spezialisieren uns auf den Fall $R = K[X]$. In diesem Fall sind $R/(ab), R/(a)$ und $R/(b)$ auch K-Vektorräume der Dimension $\deg(ab), \deg(a)$ und $\deg(b)$. Aus der Additivität des Grades bei Multiplikation ergibt sich, daß $\overline{\mathrm{pr}}$ eine injektive K-lineare Abbildung zwischen Vektorräumen der gleichen endlichen Dimension ist. Es muß daher $\overline{\mathrm{pr}}$ ein Isomorphismus sein. □

Zu einer Zerlegung als direkte Summe gehören Idempotente in den Endomorphismen, vgl. Aufgabe 45, LA1, WS 2002/2003, und dies sind e_a, e_b aufgefaßt via Multiplikation als Endomorphismen von $R/(ab)$. In der Tat gilt dann $R/(ab) = e_a R/(ab) \oplus e_b R/(ab)$. Diese Zerlegung stimmt mit der obigen überein, da $e_a R/(ab) \cong R/(a), e_a r \mapsto e_a r = r$ und $e_b R/(ab) \cong R/(b), e_b r \mapsto e_b r = r$ Isomorphismen sind. Die Wohldefiniertheit aller verwendeten Abbildungen möge der Leser zur Übung kontrollieren.

Satz 1.13 (Restklassenkörper). *Sei p ein Primelement eines Hauptidealrings R. Dann ist der Restklassenring $R/(p) =: \kappa(p)$ ein Körper, der* **Restklassenkörper** *bei (p).*

Beweis: Sei $r \in R/(p)$ von 0 verschieden. Dann teilt p nicht r und folglich kann der größte gemeinsame Teiler von p und r nur 1 sein. Nach dem Satz von Bézout gibt es dann $\pi, \rho \in R$ mit $\pi p + \rho r = 1$. Dies bedeutet, daß ρ ein Inverses zu r in $R/(p)$ darstellt. □

Als Beispiel sei $\mathbb{F}_p$ als Quotient von $\mathbb{Z}$ nach dem von der Primzahl p erzeugten Ideal genannt. Des weiteren gehört zu einem irreduziblen Polynom $p \in K[X]$ der Restklassenkörper $\kappa(p) = K[X]/(p)$. Er enthält den Körper K als Unterkörper, denn eine Basis als K-Vektorraums des Quotienten $K[X]/(p)$ ist durch $(1, X, \ldots, X^{\deg(p)-1})$ gegeben. Wir stellen fest: ein Körper mit vielen irreduziblen Polynomen p hat viele interessante Körpererweiterungen $K \subset \kappa(p)$.

Satz 1.14. *Sei $p \in K[X]$ irreduzibel. Der Körper $\kappa(p)$ hat folgende Eigenschaft. Das Polynom $p(X)$ hat eine Nullstelle in $\kappa(p)$ und für jede K-Algebra A gilt*

$$\mathrm{Hom}_{K-Algebren}\big(\kappa(p), A\big) = \{\alpha \in A \,|\, p(\alpha) = 0\} \ .$$

Beweis: Das '=' bedeutet hier wie so oft eine kanonische Identifikation. Die Gleichung $p(\alpha) = 0$ ist dabei so aufzufassen, daß vermöge der K-Algebrastruktur $K \subseteq A$ eine polynomiale Gleichung in A entsteht, deren Lösungen mit K-Morphismen $\kappa(p) \to A$ identifiziert werden sollen.

Wir schreiben $x \in \kappa(p)$ für das Element $X + (p) \in K[X]/(p)$. Dann gilt $p(x) = p(X) + (p) = 0$ in $\kappa(p)$. Damit hat das Polynom $p(X)$ über dem Körper $\kappa(p)$ die Nullstelle x.

Sei α eine Nullstelle von $p(X)$ in der K-Algebra A. Dann ist $\kappa(p) = K[X]/(p) \to A$, $f(X) \mapsto f(\alpha)$ eine wohldefinierte Abbildung von K-Algebren. Umgekehrt sei $\varphi : \kappa(p) \to A$ ein Morphismus von K-Algebren, dann ist $\alpha = \varphi(x)$ eine Lösung von $p(X) = 0$ in A, denn $p(\alpha) = p(\varphi(x)) = \varphi(p(x)) = \varphi(0) = 0$. Diese beiden Konstruktionen sind invers zueinander. □

Korollar 1.15 (Existenz von Zerfällungskörpern). *Zu einem Polynom $f \in K[X]$ gibt es eine Körpererweiterung $K \subseteq L$, so daß f aufgefaßt als Polynom in $L[X]$ in Linearfaktoren zerfällt.*

Beweis: Nach dem vorherigen Satz wissen wir, wie man zu einem irreduziblen Faktor von f eine Nullstelle in einer Körpererweiterung findet. Eine Nullstelle läßt sich als Linearfaktor abspalten, so daß wir den Beweis durch Induktion über den Grad von f abschließen können. □

Ein minimales L wie in Korollar 1.15 heißt **Zerfällungskörper** von $f \in K[X]$.

2 Die Primärzerlegung von Torsionsmoduln

Die Dimension ist eine wichtige Invariante von K-Vektorräumen. So kann ein endlich dimensionaler K-Vektorraum nicht beliebig lange Filtrationen durch Untervektorräume beinhalten. Dies liefert eine Endlichkeitsaussage, die in der Strukturtheorie von $K[X]$-Moduln ausgenutzt werden kann. In der Algebra wird dieser Begriff als 'noethersch' und 'artinsch' axiomatisiert. Für unsere Zwecke der Analyse der Struktur von Moduln über Hauptidealringen reicht es aus, sich auf endlich erzeugte Torsionsmoduln zu beschränken, um eine analoge Endlichkeitseigenschaft verwenden zu können. Wir erinnern an die folgende Definition.

Definition 2.1. (1) Auf einem R-Modul M operiert ein Element $f \in R$ durch Multiplikation als R-Modulhomomorphismus, dessen Kern wir die **f-Torsion von** M nennen und mit $M[f]$ bezeichnen. Es ist $M[f] = \{m \in M \mid fm = 0\}$. Sind f und f' assoziiert, d.h. unterscheiden sich nur um eine Einheit, so gilt $M[f] = M[f']$.

(2) Ein R-Modul M heißt **Torsionsmodul**, falls $M = \bigcup_{0 \neq f \in R} M[f]$.

(3) Sei R ein Integritätsring. Der R-Untermodul $M_{\text{tors}} = \bigcup_{0 \neq f \in R} M[f]$ von M heißt **Torsion von** M und ist der maximale Torsionsuntermodul von M. In der Tat ist M_{tors} ein Untermodul, denn aus $f_i m_i = 0$ für $i = 1, 2$ mit $f_i \neq 0$ folgt $f_1 f_2 (m_1 + m_2) = 0$ und $f_1 f_2 \neq 0$.

(4) Sei nun R ein Hauptidealring und $p \in R$ ein Primelement. Die Elemente eines R-Moduls M, welche von einer Potenz von p annulliert werden, nennt man **p-primär** und dem R-Untermodul ihrer Vereinigung $M[p^\infty] := \bigcup_n M[p^n]$ nennt man die **p-primäre Komponente** von M. Gilt $M = M[p^\infty]$, so nennt man M **p-primär**.

In unserem leitenden Beispiel eines Vektorraums V mit Endomorphismus φ, den wir so als $K[X]$-Modul auffassen, indem X durch φ operiert, können wir in einem Spezialfall Torsion und p-Primärkomponente angeben. Sei V von endlicher Dimension. Dann handelt es sich nach dem Satz von Cayley–Hamilton, Satz A.1, bei V um einen endlich erzeugten $K[X]$-Torsionsmodul, siehe Satz 1.5(f). Der Eigenraum V_λ zum Eigenwert $\lambda \in K$ ist nichts anderes als die $(X - \lambda)$-Torsion $V[X - \lambda]$. Ist überdies φ diagonalisierbar, so ist sogar $V_\lambda = V[(X - \lambda)^\infty]$ die entsprechende Primärkomponente und es gilt $V = \bigoplus_\lambda V_\lambda$. Der Modul ist also die direkte Summe seiner Primärkomponenten. Dies ist kein Zufall.

Satz 2.2 (Primärzerlegung). *Sei M ein endlich erzeugter Torsionsmodul über dem Hauptidealring R. Dann gilt:*

(1) $M = \bigoplus_{p \text{ prim}} M[p^\infty]$, und nur endlich viele Primärkomponenten verschwinden nicht.

(2) Es gibt ein (minimales bezüglich Teilbarkeit) $f \in R$ mit $fM = 0$, und wenn $f = \prod p^{\alpha(p)}$ seine Zerlegung in Primfaktoren ist, so gilt genauer $M = \bigoplus_{p \text{ teilt } f} M[p^{\alpha(p)}]$.

(3) Sei $r \in R$. Die Multiplikation mit r auf der p-Primärkomponente $M[p^\infty]$ ist

$$\begin{aligned} \text{ein Isomorphismus} &\iff p \text{ teilt } r \text{ nicht}, \\ \text{nilpotent} &\iff p \text{ teilt } r. \end{aligned}$$

(4) *Mit* $M[p'] := \bigoplus_{q \neq p} M[q^\infty]$ *erhalten wir die eindeutige direkte Zerlegung von* $M = M[p^\infty] \oplus M[p']$ *in einen Summanden, auf dem die Multiplikation mit* p *nilpotent ist, und einen zweiten Summanden, auf dem die Multiplikation mit* p *ein Isomorphismus ist.*

Beweis: Wir zeigen (2). Seien $m_1, \ldots, m_s$ Erzeuger von M und $f_i \in R$ von 0 verschiedene Elemente mit $f_i m_i = 0$, $1 \leq i \leq s$. Dann annulliert $f_1 \cdot \ldots \cdot f_s \neq 0$ den Modul M. Somit ist $\mathrm{Ann}(M) := \{f \in R \mid fM = 0\}$ ein von 0 verschiedenes Ideal von R. Da R ein Hauptidealring ist, gilt $\mathrm{Ann}(M) = (f)$ für ein geeignetes $f \neq 0$. Dieses f ist minimal bezüglich Teilbarkeit mit der Eigenschaft $fM = 0$.

Sei nun $f = \prod_{i=1}^n p_i^{\alpha_i}$ die Zerlegung in Primfaktoren. Für $n = 0, 1$ ist nichts zu tun. Sei daher $n > 1$. Der größte gemeinsame Teiler der Elemente $p_i' = \prod_{j \neq i} p_j^{\alpha_j}$ für $1 \leq i \leq n$ ist 1. Gemäß des Satzes von Bézout, Satz 1.10, wählen wir $a_i \in R$ mit $1 = \sum_{i=1}^n a_i p_i'$. Setzen wir $e_i = a_i p_i'$, so gilt in $\mathrm{End}_R(M)$ für die Multiplikationsabbildungen $e_i e_j = 0$ für $i \neq j$. In der Tat ist f ein Teiler von $e_i e_j$, ergo $e_i e_j \in \mathrm{Ann}(M)$. Des weiteren sind die e_i in $\mathrm{End}_R(M)$ Idempotente:

$$e_i = e_i(\sum_{j=1}^n e_j) = e_i^2.$$

Wir definieren die Untermoduln $e_i M = \{e_i m \mid m \in M\}$ von M. Die Inklusionen definieren eine Abbildung

$$\chi : \bigoplus_{i=1}^n e_i M \to M, \quad (m_1, \ldots, m_n) \mapsto \sum m_i$$

welche die Abbildung $\psi : m \mapsto (e_1 m, \ldots, e_n m)$ als Inverses hat, denn

- $\chi(\psi(m)) = \sum_i e_i m = \big(\sum_i e_i\big) m = m$, und
- $\psi(\chi(m_1, \ldots, m_n)) = \big(\ldots, e_i(\sum_j m_j), \ldots\big) = (m_1, \ldots, m_n)$.

Es gilt nämlich für $x = e_j y \in e_j M$, daß $e_i x = e_i e_j y = 0$, falls $i \neq j$, oder $e_i x = e_i e_i y = e_i y = x$ für $i = j$. Daraus folgt die Rechnung für $\psi \circ \chi$.

Wir haben jetzt noch $e_i M = M[p_i^{\alpha_i}]$ nachzuweisen. Da f das Element $e_i p_i^{\alpha_i}$ teilt, gilt $e_i M \subseteq M[p_i^{\alpha_i}]$. Um die umgekehrte Inklusion nachzuweisen, nehmen wir ein Element $m \in M[p_i^{\alpha_i}]$ und zerlegen es in Komponenten $e_j m$ bezüglich der Zerlegung $M = \bigoplus e_i M$. Für $j \neq i$ teilt $p_i^{\alpha_i}$ das Idempotent e_j und somit ist diese Komponente $e_j m =$ (anderer Faktor) $\cdot\, p_i^{\alpha_i} m = 0$. Somit gilt $m = e_i m$ und $m \in e_i M$.

Für (1) ist jetzt nur noch nachzuweisen, daß schon $M[p^\infty] = M[p^{\alpha(p)}]$ gilt und für Primelemente, die f nicht teilen, die entsprechende Primärkomponente von M verschwindet. Dies folgt beides aus (3) und dem Folgenden.

Zu (3). Teilt p nicht r, so ist $(r, p^n) = 1$ $\forall n \in \mathbb{N}$, und es gibt nach Satz 1.10 eine Relation $1 = \rho_n r + \pi_n p^n$. Somit operiert r auf $M[p^n]$ mit Inversem ρ_n. Damit ist auch in der Vereinigung $M[p^\infty]$ über alle n die Multiplikation mit r bijektiv (man beachte, daß $M[p^n] \subseteq M[p^{n+k}]$ für $k \geq 0$).

Ist hingegen p ein Teiler von r, so reicht es, sich mit dem Fall $r = p$ auseinanderzusetzen. Für jedes Element $m \in M[p^\infty]$ gibt es per Definition ein *a priori* von m abhängendes $N \in \mathbb{N}$, so daß $p^N m = 0$. Wir wollen aber die Multiplikation mit p als nilpotent erkennen und müssen so ein für alle $m \in M[p^\infty]$ uniform geltendes N finden.

Wir zerlegen ein Element $m \in M[p^\infty]$ gemäß (2) in Komponenten $e_i m \in M[p_i^{\alpha_i}]$. Sei $p_i \neq p$, so ist nach dem eben Bewiesenen die Multiplikation mit p ein Isomorphismus auf $M[p_i^{\alpha_i}]$. Damit verschwindet die entsprechende Komponente von $p^N m$, nämlich $e_i p^N m$, nur, wenn schon $e_i m = 0$. Somit liegt $M[p^\infty]$ schon in $M[p^{\alpha(p)}]$ und stimmt deswegen mit $M[p^{\alpha(p)}]$ überein. Dies zeigt (3) und damit auch (1).

Für (4) bemerken wir nur, daß in einer derartigen Zerlegung der nilpotente Teil in $M[p^\infty]$ enthalten sein muß. Der Anteil, auf dem p Isomorphismus ist, hingegen muß im Schnitt der Bilder der Multiplikation mit p^n über alle n liegen. Mit den Erkenntnissen aus (3) ist dieser Schnitt gerade $M[p']$. Die Zerlegung $M = M[p^\infty] \oplus M[p']$ gilt nach (1). Die Summe eines p-nilpotenten und eines p-isomorphen Teils kann also nur dann ganz M sein, wenn es die in (4) beschriebene ist. □

Der wichtige Teil des obigen Beweises, der Punkt (2), erinnert an den Beweis des Chinesischen Restsatzes. Dies ist nicht verwunderlich, denn man kann den Chinesischen Restsatz leicht aus Satz 2.2 ableiten.

Korollar 2.3. *Sei V ein endlich dimensionaler K-Vektorraum mit einem Endomorphismus φ. Sei $\operatorname{chr}_\varphi(X) = \prod p^{\alpha(p)}$ die Primfaktorzerlegung des charakteristischen Polynoms in $K[X]$. Dann gilt:*

(1) $V = \bigoplus_{p \text{ teilt } \operatorname{chr}_\varphi(X)} V_p$ mit $V_p = \ker(p^{\alpha(p)}) \subseteq V$,

(2) Die Projektoren $V \twoheadrightarrow V_p \subseteq V$ der Zerlegung als direkte Summe in (1) sind gegeben durch Polynome in φ. Insbesondere kommutieren die Projektoren mit allen Endomorphismen von V, die mit φ vertauschen, die deshalb auch die Zerlegung $V = \bigoplus V_p$ respektieren.

(3) Das charakteristische Polynom von $\varphi|_{V_p}$ ist $\operatorname{chr}_{\varphi|_{V_p}}(X) = p^{\alpha(p)}$.

Beweis: (1) Wir fassen wieder V als $K[X]$-Modul auf. Nach dem Satz von Cayley–Hamilton, Satz A.1, wird V vom charakteristische Polynom $\operatorname{chr}_\varphi(X)$ annulliert. Damit folgt (1) aus Satz 2.2(2).

(2) Genauer zeigt der obige Beweis von Satz 2.2 das Folgende. Sei

$$1 = \sum_{p \text{ teilt } \operatorname{chr}_\varphi(X)} \big(a_p \prod_{q \neq p} q^{\alpha(q)}\big)$$

in $K[X]$, so sind die $e_p = a_p \prod_{q\neq p} q^{\alpha(q)}$ paarweise orthogonale (d.h. $e_p e_q = 0$ für $p \neq q$) Idempotente in $K[X]/\big(\operatorname{chr}_\varphi(X)\big)$ und $e_p(\varphi) \in \operatorname{End}_K V$ ist der Projektor $V \to V_p$. Vertauscht ein $\psi \in \operatorname{End}_K V$ mit φ, so gilt mit $f(X) = a_0 + a_1 X + \ldots + a_n X^n$, $a_i \in K$:

$$\psi \circ \big(f(\varphi)\big) = \psi \circ \big(a_0 + a_1\varphi + \ldots a_n\varphi^n\big) = \big(a_0 + a_1\varphi + \ldots a_n\varphi^n\big) \circ \psi = \big(f(\varphi)\big) \circ \psi.$$

Die Komponente in V_p von $\psi(v), v \in V$ ist daher $e_p(\varphi)\big(\psi(v)\big) = \psi\big(e_p(\varphi)(v)\big)$, also das Bild der Komponente in V_p von v. Damit ist $\psi(V_p) \subseteq V_p$ und ψ respektiert die Zerlegung aus (1).

(3) Es kommutiert φ mit sich selbst und daher respektiert φ die Zerlegung $V = V_p$. Wir schreiben φ_p für die Einschränkung $\varphi|_{V_p}$ als Endomorphismus von V_p. Die Notation $\varphi = \bigoplus \varphi_p$ deutet an, daß sich φ in blockdiagonaler Form aus den φ_p zusammensetzt. Für die charakteristischen Polynome gilt daher

$$\operatorname{chr}_\varphi(X) = \prod_{p \text{ teilt } \operatorname{chr}_\varphi(X)} \operatorname{chr}_{\varphi_p}(X). \tag{2.1}$$

Es annulliert $p^{\alpha(p)}$ die Einschränkung φ_p. Das Minimalpolynom von φ_p muß daher eine Potenz von p sein. Nach Satz A.2 gilt dies dann auch für das charakteristische Polynom $\operatorname{chr}_{\varphi_p}(X)$. Damit folgt (3) aus (2.1) und der eindeutigen Primfaktorzerlegung in $K[X]$. □

Sei nun M ein p-primärer endlich erzeugter Torsionsmodul des Hauptidealrings R. Dann haben wir die folgende steigende **Kernfiltrierung** $K_i M := M[p^i]$

$$(0) \subseteq M[p] \subseteq \cdots \subseteq M[p^{i-1}] \subseteq M[p^i] \subseteq \ldots \subseteq M[p^n] = M.$$

Es annulliert p die Filtrationsquotienten $M[p^i]/M[p^{i-1}]$, welche deshalb nach Satz 1.3 Moduln unter $R/(p)$ sind. Nach Satz 1.13 handelt es sich also bei den Filtrationsquotienten um $\kappa(p)$-Vektorräume. Sei nun speziell $R = K[X]$ und M der Modul zum Vektorraum V mit Endomorphismus φ. Die Wahl einer Basis der Filtrationsquotienten der Kernfiltration als $\kappa(p)$-Vektorräume entspricht einem $K[X]$-Modulisomorphismus $M[p^i]/M[p^{i-1}] \cong \big(K[X]/(p)\big)^{e_i}$. Daraus folgert man die Existenz einer Basis so daß φ einer Matrix der oberen Blockdreiecksgestalt entspricht, auf deren Blockdiagonale ausschließlich die Begleitmatrix $\Lambda(p)$ zum irreduziblen Polynom p auftritt. Dies sieht man deutlich

Beispiel 2.4. Als Beispiel sehen wir uns den Fall $M = K[X]/(p^e)$ und $\varphi =$ Multiplikation mit X an. Die Filtration ist gegeben durch $M[p^i] = p^{e-i}K[X]/(p^e)$ und die Filtrationsquotienten sind gegeben durch $M[p^i]/M[p^{i-1}] \cong K[X]/(p)$, wobei der inverse Isomorphismus durch Multiplikation mit p^{e-i} gegeben ist. Sei $\deg(p) = d$. Wir beschreiben die Multiplikation mit X in der Basis $\mathscr{B} = \big(p(X)^i X^j : 0 \le i < e, 0 \le j < d\big)$. Dabei ordnen wir die Elemente lexikographisch nach dem Index (i, j). Das System $\mathscr{B}$ ist tatsächlich eine Basis, denn für festes i stellt $\mathscr{B}_i = \big(p(X)^i X^j : 0 \le j < d\big)$ einen Lift nach $K[X]/(p^e)$ der Standardbasis von $M[p^i]/M[p^{i-1}]$ via des obigen Isomorphismus mit $K[X]/(p)$ dar. Damit wissen wir schon, daß auf der Blockdiagonalen von $\mathscr{M}^{\mathscr{B}}_{\mathscr{B}}$ die Begleitmatrix $\Lambda(p)$ von p steht. Genauer ist in $K[X]/(p^e)$ mit $p(X) = a_0 + a_1X^1 + \ldots + a_{d-1}X^{d-1} + X^d$

$$X \cdot p(X)^i X^j = \begin{cases} p(X)^i X^{j+1} & \text{für } 0 \le i < e, 0 \le j \le d-2 \\ p(X)^{i+1}X^0 - p(X)^i\big(a_0 + \ldots + a_{d-1}X^{d-1}\big) & \text{für } 0 \le i < e-1, j = d-1 \\ -p(X)^{e-1}\big(a_0 + \ldots + a_{d-1}X^{d-1}\big) & \text{für } i = e-1, j = d-1 \end{cases}$$

Bis auf die Terme mit den a_i, welche für das Erscheinen der Begleitmatrix verantwortlich zeichnen, shiftet also die Multiplikation mit X die Basis um einen Index weiter in der lexikographischen Anordnung:

$$\mathscr{M}^{\mathscr{B}}_{\mathscr{B}}(\varphi) = \mathscr{M}^{\mathscr{B}}_{\mathscr{B}}(X\cdot) = \begin{pmatrix} \boxed{\Lambda(p)} & & & & \\ 1 & \boxed{\Lambda(p)} & & & \\ & 1 & \ddots & & \\ & & 1 & \boxed{\Lambda(p)} & \\ & & & 1 & \boxed{\Lambda(p)} \end{pmatrix}$$

Diese Matrix nennen wir das **Jordankästchen** $J(p^e)$ zur Potenz p^e des Primelements p.

Es drängt sich einem die Frage auf, in wieweit die Primärzerlegung verfeinert werden kann. Bezüglich der Zerlegung als direkte Summe suggeriert das obige Beispiel, daß zyklische Moduln vom Typ $R/(p^e)$ zu einem Primelement p die 'atomaren' Bestandteile sind, denn $R/(p^e)$ ist p-primär und seine Filtrationsquotienten der Kernfiltration sind kleinstmöglich. Wir fragen also: Ist jeder endlich erzeugte Torsionsmodul eine direkte Summe von zyklischen p-primären Moduln? Wie eindeutig ist eine solche Zerlegung?

3 Der Strukturatz

In diesem Kapitel beweisen wir den folgenden Struktursatz.

Satz 3.1 (Struktursatz für endlich erzeugte Torsionsmoduln I). *Sei R ein Haupidealring und M ein endlich erzeugter Torsions-R-Modul. Dann gilt:*

(1) M ist isomorph zu einer direkten Summe zyklischer Moduln.

(2) Es gibt nicht notwendig verschiedene Primelemente $p_i, i = 1, \ldots, s$ und natürliche Zahlen $e_i, i = 1, \ldots, s$, so daß

$$M \cong \bigoplus_{i=1}^{s} R/(p_i^{e_i}).$$

Es folgen drei Beweise dieses Satzes.

Beweis 1: Offenbar ist (1) eine Folge von der präziseren Strukturaussage (2). Um (2) zu beweisen, dürfen wir nach der Primärzerlegung, Satz 2.2, den Modul M durch seine p-Primärkomponente $M[p^e]$ zu einer uniformen Potenz p^e mit einem Primelement p ersetzen. Ein zunächst subtiler Punkt ist hier die endliche Erzeugtheit der p-Primärkomponente, welche aus dem folgenden Lemma folgt (oder aber aus dem grundlegenden Begriff 'noethersch' sofort; im Fall $R = K[X]$ folgt dies sofort aus dem Begriff der Dimension in der Theorie der Vektorräume).

Lemma 3.2. *Direkte Summanden endlich erzeugter Moduln sind endlich erzeugt.*

Beweis: Sei $M = M_1 \oplus M_2$ eine direkte Summe von Moduln und M endlich erzeugt. Die Projektionsabbildung $M \to M_1$ ist surjektiv. Damit erzeugen die Bilder von Erzeugern von M den Modul M_1. □

Sei also nun oBdA $\mathrm{Ann}(M) = (p^e)$. Es reicht dann eine direkte Zerlegung $M = \bigoplus_i Rx_i$ mit endlich vielen Elementen $x_i \in M$ zu finden, in der die Summanden von einem Element x_i erzeugt werden. In der Tat gilt $\mathrm{Ann}(x_i) \subseteq (p^e)$ und daher $\mathrm{Ann}(x_i) = (p^{e_i})$ für geeignete e_i, und $Rx_i \cong R/\mathrm{Ann}(x_i)$ gemäß (1.1). Wir wollen eine Zerlegung in zyklische Moduln $R/(p^{e_i})$ induktiv beweisen. Dazu müssen wir ein Maß dafür finden, daß M kleiner geworden ist, wenn wir das Problem teilweise gelöst haben.

Der erste Beweis führt eine Induktion über die Anzahl der Erzeuger von M. Der Induktionsanfang mit einer leeren Erzeugermenge führt zum Modul $M = 0$, der die leere direkte Summe zyklischer Moduln ist. (Wem das suspekt ist, der analysiere den Fall mit nur einem Erzeuger.)

Behandeln wir nun den Induktionsschritt. Besitze M ein Erzeugendensystem aus n Elementen. Unter diesen gibt es ein Element $x_1 \in M$ mit $\mathrm{Ann}(x_1) = (p^e)$ und e maximal, denn sonst annullierte schon p^{e-1} den Modul M. Der Quotient $\mathrm{pr} : M \to \overline{M} = M/Rx_1$ kann mit $n-1$ Elementen erzeugt werden. Per Induktion ist $\overline{M} = \bigoplus_{i=2}^{s} R\overline{y}_i$. Wir werden versuchen diese Zerlegung nach M zu liften, das heißt wir suchen eine Spaltung σ (Rechtsinverses der Projektion $M \to \overline{M}$) von der exakten Sequenz

$$0 \longrightarrow Rx_1 \longrightarrow M \overset{\sigma}{\underset{\curvearrowleft}{\longrightarrow}} \bigoplus_{i=2}^{s} R\overline{y}_i \longrightarrow 0\,.$$

Dazu liften wir zunächst die $\overline{y}_i$ beliebig zu $y_i \in \mathrm{pr}^{-1}(\overline{y}_i)$ nach M. Es sei $\mathrm{Ann}(\overline{y}_i) = (p^{e_i})$. Dann gilt $e_i \le e$ und $p^{e_i} y_i \in Rx_1$. Es gibt also $a_i \in R$ mit $p^{e_i} y_i = a_i x_1$. Jetzt verwenden wir die Extremalität von x_1. Da $p^{e-e_i} a_i x_1 = p^e y_i = 0$ muß p^{e_i} ein Teiler von a_i sein. Wir setzen $a_i = p^{e_i} b_i$ und modifizieren y_i ohne sein Bild in $\overline{M}$ zu ändern durch $x_i = y_i - b_i x_1$. Damit annulliert p^{e_i} den Lift x_i und $\sigma(\sum_{i=2}^{s} \lambda_i \overline{y}_i) = \sum_{i=2}^{s} \lambda_i x_i$ ist wohldefiniert und die gesuchte Spaltung (folgt aus der universellen Eigenschaft der direkten Summe und (1.1)). Wir schließen mit dem folgenden Lemma den ersten Beweis des Struktursatzes ab. □

Lemma 3.3. *Sei* $0 \longrightarrow M' \xrightarrow{i} M \xrightarrow{\mathrm{pr}} M'' \longrightarrow 0$ *eine kurze exakte Sequenz von R-Moduln, d.h. i ist injektiv,* pr *ist surjektiv und* $M'' = coker(i)$ *oder äquivalent* $M' = \ker(\mathrm{pr})$. *Läßt die Sequenz eine Spaltung* $\sigma : M'' \to M$ *zu, d.h. ein Rechtsinverses zu* pr, *also* $\mathrm{pr} \circ \sigma = \mathrm{id}_{M''}$, *so ist kanonisch*

$$M \cong M' \oplus M'', \quad m \mapsto \big(m - \sigma(\mathrm{pr}(m)), \mathrm{pr}(m)\big)$$

eine direkte Summe.

Beweis: Die inverse Abbildung zu der gegebenen ist $(m', m'') \mapsto (m' + \sigma(m''))$. Dies muß man zur Übung selbst nachrechnen. □

Beweis 2: Wir steigen im ersten Beweis an der Stelle ein, an dem die Induktion beginnt. Wir führen wieder Induktion nach der Anzahl der Erzeuger von M. Wir wählen wieder einen Erzeuger $x \in M$ mit minimalem Annulatorideal $\mathrm{Ann}(x) = \mathrm{Ann}(M) = (p^e)$. Wir konstruieren eine Retraktion $\rho : M \to R/(p^e) \cdot x$ der Inklusion $i : R/(p^e) \cdot x \subseteq M$, also $\rho \circ i = \mathrm{id}$. Die Konstruktion geht über Induktion nach der Anzahl der Erzeugenden von M. Ist M von einem Element erzeugt, so folgt aus der Maximalität von e, daß bereits $R/(p^e) \cdot x = M$ und ρ ist einfach die Identität. Sei nun $M' \subseteq M$ ein Untermodul mit $R/(p^e) \cdot x \subseteq M'$ und einer schon konstruierten Retraktion $\rho' : M' \to R/(p^e) \cdot x$, so daß $M = \langle M', y \rangle_R$ mit einem Element $y \in M$. Für die Konstruktion von ρ wollen wir ρ' auf M fortsetzen und müssen y derart einen Wert $\rho(y)$ zuweisen, daß es nicht zu Konflikten kommt. Wir betrachten die kurze exakte Sequenz

$$0 \longrightarrow M' \cap Ry \xrightarrow{(-,+)} M' \oplus Ry \xrightarrow{\sum} M \longrightarrow 0\,,$$

in der die Abbildung $(-,+) : m \mapsto (-m, m)$ offensichtlich der Kern der surjektiven Abbildung $\sum : (m', \lambda y) \mapsto m' + \lambda y$ ist. Ferner ist $\oplus$ hier eine formale (nicht innere) direkte Summe und $\sum$ surjektiv, da M von M' und y erzeugt wird. Die Retraktion ρ' läßt sich durch

$$\tilde{\rho} : M' \oplus Ry \to Rx, \qquad (m', \lambda y) \mapsto \rho'(m') + \lambda \rho(y)$$

nach Wahl von $\rho(y) \in Rx$ fortsetzen. Eine Retraktion $\rho : M \to Rx$ erhalten wir genau dann nach der universellen Eigenschaft des Kokern, wenn $\tilde{\rho}$ auf $M' \cap Ry$ verschwindet.

Der Schnitt $M' \cap Ry$ ist ein Untermodul von $Ry = R/(p^f) \cdot y$ mit $f \leq e$, nach Extremalität von e. Untermoduln von $R/(p^f)$ entsprechen Idealen $\mathfrak{a} \subseteq R$ mit $(p^f) \subseteq \mathfrak{a} \subseteq R$. Da R ein Haupidealring ist, folgt $\mathfrak{a} = (p^g)$ mit $0 \leq g \leq f$, oder $M' \cap Ry = Rp^g y$. Es gilt nun

$$p^{e-g} \rho'(p^g y) = \rho'(p^e y) = \rho'(0) = 0$$

und daher $\rho'(p^g y) \subseteq Rx[p^{e-g}] = Rp^g x$, denn x wird erst von p^e annulliert und R ist ein Hauptidealring. Es gibt also ein $a \in R$ mit $\rho'(p^g y) = ap^g x$. In der obigen Konstruktion von $\tilde{\rho}$ wählen wir jetzt $\rho(y) := ax$. Man überzeugt sich sofort, daß jetzt $\tilde{\rho}$ zu der gesuchten Retraktion $\rho : M \to Rx$ faktorisiert, denn für $m = \lambda p^g y \in M' \cap Ry$ gilt

$$\tilde{\rho}\big(-m, m\big) = \rho'(-\lambda p^g y) + \lambda p^q \rho(y) = -\lambda \rho'(p^g y) + \lambda p^g a x = 0.$$

Wir schließen mit dem folgenden Lemma, daß $M = Rx \oplus \ker(\rho)$ ist. Es war x ein Erzeuger von M aus dem gewählten Erzeugendensystem der Größe n, welches den Induktionsparameter darstellt. Somit ist $\ker(\rho)$ als Quotient M/Rx von einem Element weniger erzeugbar, ergo per Induktion schon eine direkte Summe zyklischer Moduln und der Satz ist ein zweites Mal bewiesen. □

Lemma 3.4. *Sei* $M' \subseteq M$ *ein Untermodul und* $\rho : M \to M'$ *eine Retraktion. Dann ist kanonisch* $M' \oplus \ker(\rho) = M$ *eine direkte Summe.*

Beweis: Die Abbildung ρ ist ein Linksinverses zur Inklusion $i : M' \to M$. Die Inklusionen von M' und $\ker(\rho)$ definieren eine Abbildung $M' \oplus \ker(\rho) \to M$, deren Inverses durch $m \mapsto \big(\rho(m), m - i(\rho(m))\big)$ gegeben ist. Dies muß man zur Übung selbst nachrechnen. □

Bemerkung: Der zweite Beweis zeigt eigentlich, daß $R/(p^e)$ ein injektiver $R/(p^e)$-Modul ist, siehe irgendein Buch über homologische Algebra von Artinschen Ringen.

Beweis 3: Bis zum Beginn der Induktion wiederholen wir Beweis (1). Allerdings verwenden wir nun Induktion nach dem Exponenten e in $\mathrm{Ann}(M) = (p^e)$. Wir werden auch die Eigenschaft noethersch verwenden. Dies ließe sich vermeiden, erscheint aber unnatürlich. Daher sei auch erwähnt, daß man diesen Ansatz als noethersche Induktion nach dem Annulatorideal von M bezeichnen kann.

Für $e = 0$ ist $M = 0$ und sonst nichts weiter zu tun. Für den Induktionsschritt arbeiten wir mit der kurzen exakten Sequenz

$$0 \longrightarrow M[p] \longrightarrow M \xrightarrow{p\cdot} pM \longrightarrow 0\,,$$

wobei pM das Bild der Multiplikation mit p auf M ist. Es gilt $\mathrm{Ann}(pM) = (p^{e-1})$ und daher gibt es eine Zerlegung $pM = \bigoplus R/(p^{e_i})y_i$. Dabei sind die $y_i \in pM$ also von der Form $y_i = px_i$ mit $\mathrm{Ann}(y_i) = (p^{e_i})$. Es folgt $\mathrm{Ann}(x_i) = (p^{e_i+1})$. Wir betrachten nun den Kern der surjektiven von den Inklusionen und der universellen Eigenschaft der direkten Summe induzierten Abbildung

$$\psi : M[p] \oplus \bigoplus_i R/(p^{e_i+1})x_i \twoheadrightarrow M.$$

Die Surjektivität folgt, da mit $m \in M$ und $pm = \sum_i \lambda_i y_i$ die Differenz $m - \sum_i \lambda_i x_i$ im Kern der Multiplikation mit p liegt. Sei $(-m, \sum_i \lambda_i x_i)$ ein Element des Kerns von ψ, also $\sum_i \lambda_i x_i = m \in M[p]$. Es folgt $0 = pm = \sum_i \lambda_i y_i$ und demnach wird λ_i von p^{e_i} geteilt, wenigstens aber $\lambda_i = p\mu_i$ für geeignete μ_i. Damit ist $m = \sum_i \lambda_i x_i = \sum_i \mu_i y_i \in pM$. Nach Satz 1.3 und Satz 1.13 ist $M[p]$ ein $\kappa(p) = R/(p)$-Vektorraum. Darin wählen wir zum R-Untermodul $M[p] \cap pM \subseteq M[p]$, der deshalb auch ein $\kappa(p)$-Unterraum ist, ein $\kappa(p)$-Vektorraumkomplement $M' \subseteq M$, also $M' \oplus \big(M[p] \cap pM\big) = M[p]$. Wir schränken ψ ein auf

$$\psi' : M' \oplus \bigoplus_i R/(p^{e_i+1})x_i \twoheadrightarrow M.$$

Diese Abbildung ist immer noch surjektiv, da $pM \subset \bigoplus_i R/(p^{e_i+1})x_i$ und $pM + M' \supset M[p]$. Jetzt allerdings gilt mit der obigen Argumentation und Notation für ein Element $(-m, \sum_i \lambda_i x_i)$ des Kerns von ψ', daß $m \in M' \cap pM = 0$. Demnach gilt $0 = \sum_i \lambda_i x_i = \sum_i \mu_i y_i$, und damit ist p^{e_i} ein Teiler von μ_i, bzw. p^{e_i+1} ein Teiler von λ_i. Damit ist gezeigt, daß $\ker(\psi')$ verschwindet und ψ' ist der gesuchte Isomorphismus mit einer Summe zyklischer Moduln. Der $\kappa(p)$-Vektorraum ist nämlich nach Wahl einer Basis isomorph zu einer Summe von Moduln der Form $R/(p)$. □

Wo haben wir im dritten Beweis die Eigenschaft noethersch verwendet? A priori wissen wir nicht, daß $M[p]$ und damit M' endlich dimensionale $\kappa(p)$-Vektorräume sind. Wir müßten dazu wissen, daß Untermoduln von endlich erzeugten Moduln selbst endlich erzeugt sind (noethersch). Investiert man den Begriff 'noethersch' nicht, so können im letzten Schritt unendlich viele Summanden $R/(p)$ hinzukommen (und, man kann mit einer Basis von M' als $\kappa(p)$-Vektorraum nur argumentieren, wenn man auch für unendlich dimensionale Vektorräume die Existenz von einer Basis gezeigt hat). In einer Zerlegung als direkte Summen des endlich erzeugten Moduls M können nur endlich viele Summanden auftreten, da die endlich vielen Erzeuger von M nur in endlich vielen (im Unterschied zum Produkt!) Summanden nicht verschwindende Komponenten haben dürfen. Das Problem eines unendlich dimensionalen Vektorraums tritt also nicht auf.

Als vertiefende Quellen zu den gegebenen Beweisen des Strukturs atzes sei auf [Lieb, Satz 1.2], [Lang, Kap. III §7] für Beweis 1 und auf [Meyb, §5.5] für Beweis 2 verwiesen.

Satz 3.5 (Eindeutigkeit). *Sei M ein p-primärer endlich erzeugter Torsionsmodul über dem Hauptidealring R. Sei $M \cong \bigoplus_i R/(p^{e_i})$ mit $e_i > 0$ eine Zerlegung in eine direkte Summe zyklischer Moduln (wie im Struktursatz). Dann gilt:*

(1) $\#\{i\} = \dim_{\kappa(p)}(M/pM)$,

(2) $\#\{i \mid e_i = e\} = \dim_{\kappa(p)}\big(M[p^e]/M[p^{e-1}]\big) - \dim_{\kappa(p)}\big(M[p^{e+1}]/M[p^e]\big)$,

(3) insbesondere sind die Anzahl der Summanden und genauer die Anzahl der Summanden mit Annulator (p^e) unabhängig von der gewählten Zerlegung. Nach der Eindeutigkeit der Primärzerlegung gilt dies auch für allgemeine endlich erzeugte Torsionsmoduln über R.

Beweis: Aus $M = M' \oplus M''$ folgt $pM = pM' \oplus pM''$ und $M[p^e] = M'[p^e] \oplus M''[p^e]$. Da Quotienten nehmen mit direkten Summen verträglich ist, vgl. Aufgabe 17(a) LA 2, SoSe 2003, und die Dimension eines Vektorraums additiv auf direkten Summen ist, gelten die Formeln in (1) und (2) für M genau dann, wenn sie für M' und M'' gelten. Wir haben also nur den Fall $M = R/(p^\alpha), \alpha > 0$ zu analysieren. Dieser Fall jedoch ist klar. □

Beispiel 3.6. Viel mehr an Eindeutigkeit läßt sich nicht erwarten. Wir betrachten zu $0 < e \in \mathbb{N}$ den R-Modul $M = R/(p) \oplus R/(p^e)$. Für $e = 1$ handelt es sich um einen $\kappa(p)$-Vektorraum der Dimension 2. Eine Zerlegung wie im Struktursatz entspricht der Wahl einer Basis als $\kappa(p)$-Vektorraum. Die Mehrdeutigkeit einer Basiswahl wird parametrisiert durch ein Element in $\mathrm{GL}_2(\kappa(p))$, der Basiswechselmatrix.

Sei $e > 1$. Die Beweise des Struktursatzes lehren, daß jedes Element mit Annulator (p^e) ein direkter Summand von M ist. Diese sind gegeben durch $f \in \mathrm{Hom}\big(R/(p^e), R/(p)\big) \cong \kappa(p)$ als $M_f := \{(f(x), x) \mid x \in R/(p^e)\} \subset R/(p) \oplus R/(p^e)$. Zu M_f kann man auf vielfache Weise ein Komplement finden. Man muß nur gemäß des dritten Beweises in $M[p] = R/(p) \oplus p^{e-1}R/(p^e)$ ein Komplement von $pM_f \cap M[p]$ finden. Diese Wahl wird ebenso von einem Element aus $\kappa(p)$ parametrisiert.

Satz 3.7 (Struktursatz für endlich erzeugte Torsionsmoduln II). *Sei M ein endlich erzeugter Torsionsmodul über dem Hauptidealring R.*

(1) Es gibt eine Folge sich aufsteigend teilender Elemente $d_1|d_2|\ldots|d_s$ des Rings R, so daß

$$M \cong \bigoplus_{i=1}^{s} R/(d_i).$$

(2) Die natürliche Zahl s und die Ideale (d_i) zu den Elementen d_i aus (1) sind eindeutig durch den R-Modul M bestimmt.

Beweis: Es folgt (1) aus dem ersten Struktursatz, Satz 3.1, und dem Chinesischen Restsatz, Satz 1.11. Die Eindeutigkeitsaussage (2) folgt aus Satz 3.5. □

Korollar 3.8 (Jordannormalform). *Sei K ein Körper.*

(1) Sei $\varphi : V \to V$ ein Endomorphismus eines endlich dimensionalen K-Vektorraums. Dann gibt es eine Basis von V, bezüglich der die Matrix von φ aus Jordankästchen besteht, die längs der Diagonale angeordnet sind.

(2) Eine quadratische Matrix $A \in \mathscr{M}_n(K)$ über K ist ähnlich zu einer Matrix aus Jordankästchen, die längs der Diagonale angeordnet sind.

(3) In (1) und (2) hängen die Anzahl der Kästchen sowie die auftretenden Primpotenzen inklusive ihrer Häufigkeit, zu denen Jordankästchen vorkommen, nicht von der Basiswahl ab.

Diese Matrix aus Jordankästchen heißt die **Jordannormalform** *des Endomorphismus/der Matrix.*

Beweis: Die Matrix eines Jordankästchens wurde in Beispiel 2.4 vorgestellt. Die Jordannormalform behauptet also die Existenz einer Basis $\mathscr{B}$ bzw. einer invertierbaren Matrix $S \in \mathrm{GL}_n(K)$ mit:

$$\mathscr{M}_{\mathscr{B}}^{\mathscr{B}}(\varphi) = SAS^{-1} = \begin{pmatrix} \boxed{J(p_1^{e_1})} & & \\ & \ddots & \\ & & \boxed{J(p_s^{e_s})} \end{pmatrix}$$

Dies folgt für (1) aus Satz 3.1 für den Spezialfall $R = K[X]$ mittels des Übersetzungssatzes, Satz 1.5, und der Diskussion des Beispiels $K[X]/(p^e)$ in 2.4. Die Aussage (2) folgt aus der Aussage (1) für den von der Matrix auf K^n induzierten Endomorphismus. Die Eindeutigkeitsaussage (3) ist die Übersetzung von Satz 3.5 in die Situation des Korollars. □

Korollar 3.9 (Zerfallende Jordannormalform). *Sei K ein Körper.*

(1) Sei $\varphi : V \to V$ ein Endomorphismus eines endlich dimensionalen K-Vektorraums mit in $K[X]$ zerfallendem charakteristischen Polynom. Dann gibt es eine Basis von V, bezüglich der die Matrix von φ aus Jordankästchen zu linearen Primpolynomen besteht, die längs der Diagonale angeordnet sind.

(2) Eine quadratische Matrix $A \in \mathscr{M}_n(K)$ mit in $K[X]$ zerfallendem charakteristischen Polynom ist ähnlich zu einer Matrix aus Jordankästchen zu linearen Primpolynomen, die längs der Diagonale angeordnet sind.

Es treten also nur Jordankästchen der Form

$$J\big((X-\lambda)^e\big) = \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & \ddots & \ddots & & \\ & & \ddots & \lambda & \\ & & & 1 & \lambda \end{pmatrix} \in \mathscr{M}_e(K)$$

zu Eigenwerten λ auf.

Beweis: Die in der Jordannormalform auftretenden irreduziblen Polynome sind nach dem Satz über die Primärzerlegung, 2.2, gerade die Teiler des charakteristischen Polynoms. □

4 Der Elementarteilersatz

Satz 4.1 (Elementarteilersatz). *Sei R ein Hauptidealring. Sei $A \in \mathscr{M}_{m\times n}(R)$ eine Matrix über R.*

(1) Dann gibt es invertierbare Matrizen $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$, so daß

$$S^{-1}AT = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_s \\ & & \end{pmatrix}$$

mit $s \leq \min\{n, m\}$ und sich steigend teilenden Elementen $d_1|d_2|\ldots|d_r$ des Rings R. (Alle restlichen Einträge der Matrix sind 0.)

(2) Die natürliche Zahl s und die d_i bis auf Assoziertheit hängen nicht von den Matrizen S, T ab, d.h. sind eindeutig.

Dies beweisen wir später. Natürlich könnten wir anstatt S^{-1} auch S schreiben, aber theoretisch ist das egal und in der Anwendung auf die Jordannormalform entfällt dann ein Vorzeichen.

Korollar 4.2.

(1) Untermoduln von freien Moduln (endlichen Rangs) über einem Hauptidealring sind frei.

(2) Sei $N \subseteq M \cong R^m$ ein Untermodul eines freien Moduls über dem Hauptidealring R, so gibt es eine Basis $x_1, \ldots, x_m$ von M und sich aufsteigend teilende Elemente $d_1|d_2|\ldots|d_s$ für ein $s \leq m$ so daß N von den $d_1x_1, \ldots, d_sx_s$ frei erzeugt wird.

(3) Der Rang eines Untermoduls eines freien Moduls über einem Hauptidealring ist kleiner als der des umgebenden Moduls.

Beweis: Wir behandeln nur den Fall, daß der freie Modul endlichen Rang hat. Dann folgt (1) und (3) unmittelbar aus (2), worum wir uns also zu kümmern haben.

Ohne Einschränkung sei $M = R^m$. Wir zeigen zunächst, daß $N \subset R^m$ endlich erzeugt ist. Dies geschieht per Induktion nach m. Wir betrachten R^{m-1} als den Untermodul derjenigen Elemente von R^m, bei denen die letzte Koordinate 0 ist. Sei $\overline{N}$ das Bild von N bei Projektion auf die letzte Koordinate von R^m. Dies ist ein Untermodul von R, also ein Ideal, also von einem Element erzeugt. Wir betrachten die exakte Sequenz

$$0 \to N \cap R^{m-1} \to N \to \overline{N} \to 0.$$

Hierin ist $N \cap R^{m-1}$ per Induktion und $\overline{N}$ nach eben gesagtem endlich erzeugt. Damit aber auch N durch einen Lift des Erzeugers von $\overline{N}$ und die Erzeuger von $N \cap R^{m-1}$.

Sei nun $R^n \twoheadrightarrow N$ eine Surjektion, welche von der Wahl eines Erzeugendensystems von N der Kardinalität n herrührt. Dann entspricht der Verkettung $R^n \twoheadrightarrow N \subset R^m$ eine Matrix, auf die wir Satz 4.1 anwenden können. Das Komponieren mit S^{-1}, T entspricht einer anderen Basiswahl von R^m und R^n. Dies ändert am Bild N der Abbildung nichts, welches daher die behauptete Form hat. □

Korollar 4.3 (Struktursatz für endlich erzeugte Moduln über Hauptidealringen). *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul.*

(1) Es gibt eine kanonische exakte Sequenz

$$0 \to M_{\text{tors}} \to M \to M/\text{tors} \to 0 \tag{4.1}$$

mit dem maximalen Torsionsuntermodul $M_{\text{tors}} \subseteq M$ und einem freien, endlich erzeugten Quotienten $M/\text{tors} \cong R^r$. Die Sequenz (4.1) spaltet unkanonisch. Somit gilt unkanonisch $M \cong M_{\text{tors}} \oplus M/\text{tors}$ und es ist M_{tors} auch endlich erzeugt.

(2) Es gibt eine nicht kanonische Zerlegung als direkte Summe

$$M \cong R^r \oplus \bigoplus_{i=1}^{s} R/(d_i)$$

mit sich aufsteigend teilenden Elementen $d_1|d_2|\ldots|d_s$ des Rings R. Die Zahlen r und s sowie die Elemente d_i bis auf Assoziierung sind eindeutig.

Beweis: Wir beweisen zunächst (2). Wir wählen Erzeuger $x_1, \ldots, x_m$ von M und damit eine Surjektion $\mathrm{pr} : R^m \to M$. Wir wenden Korollar 4.2 auf den Kern $\ker(\mathrm{pr}) \subset R^m$ dieser Abbildung an. Ohne Einschränkung sei $x_1, \ldots, x_m$ bereits die Basis von R^m, die das Korollar uns verspricht, so daß $\ker(\mathrm{pr})$ von $d_1x_1, \ldots, d_sx_s$ erzeugt wird. Es gilt nun nach dem Homomorphiesatz und Aufgabe 17(a) LA 2, SoSe 2003, daß

$$M \cong R^m/\ker(\mathrm{pr}) \cong \left(\bigoplus_{i=1}^{m} Rx_i\right) / \left(\bigoplus_{i=1}^{s} Rd_ix_i\right) = R^{m-s} \oplus \bigoplus_{i=1}^{s} Rx_i/Rd_ix_i.$$

Damit ist $r = m - d$ und wegen $Rx_i/Rd_ix_i \cong R/(d_i)$ haben wir (2) bis auf die Eindeutigkeitsaussage bewiesen. Zur Eindeutigkeit bemerken wir, daß diese nicht aus der entsprechenden Eindeutigkeit der d_i aus dem Elementarteilersatz folgt, denn wir müssen über alle Matrizen A variieren, die zu einer endlichen **Präsentation**, also einer kurzen exakten Sequenz

$$R^n \xrightarrow{A} R^m \to M \to 0$$

gehören. Die Eindeutigkeit aus dem Elementarteilersatz garantiert nur für jede fixierte Matrix die Eindeutigkeit der diagonalen Form. Die Eindeutigkeit über alle Präsentationen wird durch die Theorie der Fittingideale geleistet, siehe [Eis, Kap. 20]. Wir begnügen uns mit einem unnatürlichen Rückgriff auf Satz 3.7, den wir auf den Torsionsanteil von M anwenden, siehe Beweis von Teil (1). Die Zahl r ist charakterisiert als $\dim_{\mathrm{Quot}(R)} M \otimes_R \mathrm{Quot}(R)$ beziehungsweise als der Rang des freien Quotienten M/M_{tors}.

(1) Sei M_{tors} der Torsionsuntermodul. Dann ist $M/\mathrm{tors} := M/M_{\mathrm{tors}}$ torsionsfrei und endlich erzeugt. Denn wäre $\overline{m} \in M/\mathrm{tors}$ Torsion, etwa $f\overline{m} = 0$, so gilt für ein Urbild $m \mapsto \overline{m}$, daß $fm \in M_{\mathrm{tors}}$ und somit m selbst Torsion. Damit ist $\overline{m} = 0$.

Wenden wir (2) auf M/tors an, so erkennen wir, daß alle Summanden $R/(d)$ verschwinden müssen, da sie aus R-Torsion bestehen. Ergo ist M/tors frei. Um eine Spaltung von (4.1) zu finden, muß man nun nur eine Basis von M/tors liften und die universelle Eigenschaft von freien Moduln anwenden. Damit folgt aus Lemma 3.3, daß $M \cong M_{\mathrm{tors}} \oplus M/\mathrm{tors}$. Nach Lemma 3.2 ist somit auch M_{tors} endlich erzeugt. □

Wir spezialisieren nun auf den Fall $R = K[X]$ und damit einen endlich erzeugten K-Vektorraum mit einem Endomorphismus φ. Das Korollar 4.3 zusammen mit dem Chinesischen Restsatz, Satz 1.11, impliziert den Satz über die Jordannormalform, Satz 3.8. Der Ansatz über den Elementarteilersatz liefert allerdings noch etwas mehr, wenn man eine effektive Form des Elementarteilersatzes zur Verfügung hat. Es sei $\mathscr{A} = (v_1, \ldots, v_m)$ eine Basis von V. Dann definiert $\mathrm{pr} : K[X]^m \to V$, $(f_1, \ldots, f_m) \mapsto \sum_i f_iv_i$ eine Surjektion, deren Kern wir gut berechnen können. Sei dazu $\tilde{A} = X \cdot I_m - \mathscr{M}_{\mathscr{A}}^{\mathscr{A}}(\varphi) \in \mathscr{M}_m(K[X])$. Wir betrachten die zugehörige Abbildung freier $K[X]$-Moduln und stellen fest, daß

$$K[X]^m \xrightarrow{\tilde{A}} K[X]^m \xrightarrow{\mathrm{pr}} V \to 0 \tag{4.2}$$

exakt ist. In der Tat ergibt die Verkettung $\mathrm{pr} \circ \tilde{A}$ die Nullabbildung, da ein Standardbasiselement $e_i \in K[X]^m$ zu $\mathrm{pr}(Xe_i - \mathscr{M}_{\mathscr{A}}^{\mathscr{A}}(\varphi)e_i) = Xv_i - \varphi(v_i) = 0$ abgebildet wird. Dann gibt es nach der universellen Eigenschaft des Kokerns einen $K[X]$-Modulhomomorphismus $coker(\tilde{A}) \to V$, der weiterhin surjektiv ist. Es ist $\dim_K V = m$ und $\dim_K coker(\tilde{A}) \leq m$, denn der Kokern wird als K-Vektorraum durch die Bilder der e_i erzeugt (vermöge der Relationen $Xe_i = \mathscr{M}_{\mathscr{A}}^{\mathscr{A}}(\varphi)e_i$ kann man induktiv über den Grad zeigen, daß man in $coker(\tilde{A})$ zum Erzeugen mit konstanten Polynomen auskommt). Aus Dimensionsgründen ist also $coker(\tilde{A}) \cong V$. Wir haben also durch (4.2) eine endliche Präsentation des $K[X]$-Moduls V zur Hand.

Wir wenden den Elementarteilersatz, Satz 4.1, auf die Matrix $\tilde{A}$ an. Wir erhalten invertierbare Matrizen $T, S \in \mathrm{GL}_m(K[X])$ so daß $D = S^{-1}\tilde{A}T$ diagonale Form hat, deren diagonale

Einträge sich steigend teilende Polynome $d_1|d_2|\dots|d_s$ sind. Da V Torsion ist als $K[X]$-Modul, kommt in der Zerlegung nach Korollar 4.3 kein freier Anteil vor. Es ist daher $r = m-s = 0$. Es ist also tatsächlich D eine Diagonalmatrix mit von 0 verschiedenen Einträgen auf der Diagonalen. Das Diagramm mit exakten Zeilen

$$\begin{array}{ccccccc} K[X]^m & \xrightarrow{\tilde{A}} & K[X]^m & \xrightarrow{\text{pr}} & V & \longrightarrow & 0 \\ \uparrow{\scriptstyle T} & & \uparrow{\scriptstyle S} & & \uparrow{\scriptstyle \sigma} & & \\ K[X]^m & \xrightarrow{D} & K[X]^m & \longrightarrow & \bigoplus_{i=1}^{m} K[X]/(d_i) & \longrightarrow & 0 \end{array}$$

hat mit T, S zwei isomorphe Spalten. Die universelle Eigenschaft des Kokern zeigt, daß es die Abbildung σ gibt, und daß σ ein Isomorphismus von $K[X]$-Moduln ist. Investiert man jetzt noch den Chinesischen Restsatz, Satz 1.11, so folgt erneut die Jordannormalform, Korollar 3.8.

Hat man S (effektiv) berechnet, so kann man die Bilder unter σ der Erzeuger der zyklischen Moduln $K[X]/(d_i)$ als $\text{pr}\big(S(e_i)\big) = \sum_{j=1}^{s} S_{j,i}(\varphi)v_j$ explizit (und effektiv) berechnen. Da auch der Chinesische Restsatz mit Projektoren auskommt, die durch effektive Rechnung in $K[X]$ mittels des Euklidischen Algorithmus erhalten werden können, gelangt man so tatsächlich effektiv zu einer Basis der Jordannormalform.

Beweis des Elementarteilersatzes Satz 4.1: Wir beweisen zunächst Teil (1). Es bezeichne $\text{ggT}(A)$ den größten gemeinsamen Teiler der Einträge der Matrix A. Wir werden versuchen, durch Multiplikation mit invertierbaren Matrizen von links und rechts die Matrix A auf die Blockform

$$\left(\begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \tag{4.3}$$

zu bringen, wobei $d_1 = \text{ggT}(A)$ gelten soll. Somit teilt d_1 jeden Eintrag der Matrix A'. Wir schließen dann per Induktion nach der Größe $n+m$ der Matrix indem wir den Induktionsschritt auf die Matrix $\frac{1}{d_1}A' \in \mathscr{M}_{(m-1)\times(n-1)}(R)$ anwenden.

Zunächst einmal beweisen wir, daß sich in unserer Zielvorgabe durch Multiplikation mit invertierbaren Matrizen von links und rechts nichts ändert.

Lemma 4.4. *Sei R ein Hauptidealring und $A \in \mathscr{M}_{m\times n}(R)$, $S \in \mathscr{M}_m(R)$ und $T \in \mathscr{M}_n(R)$. Dann gilt:*

(1) $\text{ggT}(A)$ *teilt* $\text{ggT}(SA)$ *und* $\text{ggT}(AT)$.

(2) Sind S, T invertierbar, so gilt $\text{ggT}(A) = \text{ggT}(SA) = \text{ggT}(AT)$.

Beweis: Es folgt (2) sofort aus (1) und (1) ist auch klar. □

Für den Induktionsanfang ($n = 1$ oder $m = 1$) beweisen wir das folgende Lemma, welches auch im Induktionsschritt Verwendung finden wird.

Lemma 4.5. *(1) Sei $w = (a_1, \dots, a_n) \in R^n$ ein Zeilenvektor mit größtem gemeinsamen Teiler der Koordinaten $d = \text{ggT}(w)$. Dann gibt es eine invertierbare Matrix $T \in \text{GL}_n(R)$ mit $wT = (d, 0 \dots, 0)$.*

(2) Analog gibt es für einen Spaltenvektor v der Länge m eine invertierbare Matrix $S \in \text{GL}_m(R)$ so, daß in Sv die erste Zeile d ist und alle anderen Einträge verschwinden.

Beweis: Offenbar sind die Aussagen (1) und (2) äquivalent. Man hat nur alle Matrizen und Vektoren zu transponieren. Daher beweisen wir nur (2). Wir verwenden Induktion nach der Größe m des Vektors. Für $m = 1$ ist nichts zu zeigen. Des weiteren ist die Behauptung des Lemmas für Vektoren v und Bv äquivalent, wenn B eine invertierbare Matrix ist, denn nach Lemma 4.4 gilt $\mathrm{ggT}(v) = \mathrm{ggT}(Bv)$.

Sei $v = \binom{a_1}{v'}$ mit einem Spaltenvektor v' der Länge $m-1$. Per Induktionsvoraussetzung gibt es eine Matrix $S' \in \mathrm{GL}_{(m-1)}(R)$ so daß $S'v'$ nur noch einen nichtverschwindenden Eintrag d' in der ersten Zeile hat. Dann ist die Blockmatrix $B = \begin{pmatrix} 1 & 0 \\ 0 & S' \end{pmatrix}$ invertierbar, und es hat Bv nur noch nichtverschwindende Einträge in den ersten beiden Zeilen. Jetzt reicht es offenbar, den Fall $m = 2$ zu beherrschen.

Sei $m = 2$ und $v = \binom{a_1}{a_2}$. Nach dem Satz von Bézout, Satz 1.10, gibt es in R eine Relation $\alpha_1 a_1 + \alpha_2 a_2 = d$. Damit erfüllt die Matrix $S = \begin{pmatrix} \alpha_1 & \alpha_2 \\ -a_2/d & a_1/d \end{pmatrix}$ das Gewünschte: $Sv = \binom{d}{0}$. Es ist $d = \mathrm{ggT}(Sv) = \mathrm{ggT}(v)$ nach Lemma 4.4. □

Daß man die Matrix A in eine Matrix der Form (4.3) bringen kann, beweisen wir per Induktion nach der minimalen Anzahl von Primfaktoren (mit Vielfachheit), die in einem nicht verschwindenden Eintrag von A vorkommt. Zum Induktionsanfang müssen wir eine Matrix behandeln, in der ein Eintrag eine Einheit ist. Dies geschieht später nebenbei.

Durch Permutationsmatrizen können wir immer annehmen, daß ein Eintrag mit minimaler Anzahl der Primfaktoren in der ersten Spalte der ersten Zeile steht. Das sei a_{11}. Wenden wir das Lemma 4.5 auf die erste Spalte von A an, so finden wir ein $S \in \mathrm{GL}_n(R)$, so daß in SA die erste Spalte, welche ja nichts anderes ist als das Produkt von S mit der ersten Spalte von A, nur ein Eintrag in der ersten Zeile findet und der Rest verschwindet:

$$\left(\begin{array}{c|ccc} d & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \tag{4.4}$$

Die Matrix nennen wir wieder A. Falls in A ein Eintrag existiert, der weniger Primfaktoren enthält als das vorherige Minimum, so sind wir per Induktion fertig. Nun verwenden wir diese Konstruktion nach Lemma 4.5 transponiert angewandt auf die erste Zeile, so daß eine Matrix der Form

$$\left(\begin{array}{c|ccc} d & 0 & \cdots & 0 \\ \hline * & & & \\ \vdots & & A' & \\ * & & & \end{array}\right) \tag{4.5}$$

entsteht. Falls jetzt in A ein Eintrag existiert, der weniger Primfaktoren enthält als das vorherige Minimum, so sind wir wieder per Induktion fertig.

Andernfalls und auch beim Induktionsanfang (ein Eintrag ist eine Einheit) muß der Eintrag a_{11} links oben in der ersten Zeile und ersten Spalte der Ausgangsmatrix schon der größte gemeinsame Teiler aller Elemente der ersten Spalte und Zeile gewesen sein, denn $d|a_{11}$ und d hat, da wir nicht in der Induktion eine Etage tiefer rutschen, die selbe Anzahl von Primfaktoren. Daher sind a_{11} und d assoziiert.

In diesem Fall teilt a_{11} alle Einträge der ersten Zeile (nach dem letzten Schritt sind diese bis auf $d = a_{11}$ schon 0) und der ersten Spalte. Man kann nun mittels elementarer Zeilenoperationen ein entsprechendes Vielfaches der ersten Zeile von den anderen Zeilen abziehen und erhält eine

Matrix der Gestalt

$$\left(\begin{array}{c|ccc} d & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right) \tag{4.6}$$

Damit sind wir fast am Ziel. Falls d nicht alle Einträge von A' teilt (äquivalent $d \neq \mathrm{ggT}(A)$), so kann man die erste Zeile zu der entsprechenden Zeile addieren, in welcher der schlechte Eintrag sitzt. Dann entsteht dort eine Zeile, deren größter gemeinsamer Teiler weniger Primfaktoren hat als das bisherige Minimum. Durch Anwendung von Lemma 4.5(1) auf diese Zeile, können wir die Matrix so manipulieren, daß dieser ggT als Eintrag erscheint. Wir schließen dann per Induktion nach der minimalen Anzahl der Primfaktoren eines Eintrags.

Zum Teil (2). Jetzt kümmern wir uns um die Eindeutigkeit der Elemente $d_1|d_2|\ldots|d_s$ und der Zahl s. Dazu bemühen wir im Wesentlichen die Theorie der Fittingideale, siehe [Eis, Kap. 20.2]. Sei $\mathrm{Fitt}_\nu(A)$ dasjenige Ideal von R, welches von den Minoren der Größe $m-\nu$ der Matrix $A \in \mathscr{M}_{m\times n}(R)$, also den Determinanten von quadratischen $(m-\nu)\times(m-\nu)$-Untermatrizen, erzeugt wird. Man nennt $\mathrm{Fitt}_\nu(A)$ das **νte Fittingideal von** A.

Lemma 4.6 (Fitting's Lemma). *Sei R ein Ring, $A \in \mathscr{M}_{m\times n}(R)$ und $S \in \mathrm{GL}_m(R)$ und $T \in \mathrm{GL}_n(R)$. Dann gilt $Fitt_\nu(A) = \mathrm{Fitt}_\nu(SA) = \mathrm{Fitt}_\nu(AT)$.*

Beweis: Man hat nur $\mathrm{Fitt}_\nu(SA) \subseteq \mathrm{Fitt}_\nu(A)$ bzw. $\mathrm{Fitt}_\nu(AT) \subseteq \mathrm{Fitt}_\nu(A)$ nachzuweisen, und das ist klar: Berechnen wir etwa den Minor derjenigen Untermatrix $(SA)_{IJ}$ von SA deren Zeilenindizes nur $i \in I$ und Spaltenindizes nur $j \in J$ durchlaufen ($\#I = \#J$). Wir stellen zunächst fest, daß die Zeilenvektoren von $(SA)_{IJ}$ Linearkombinationen der auf den Indexbereich $j \in J$ eingeschränkten Zeilenvektoren von A (alle Zeilen, nicht nur $i \in I$) sind. Dies folgt unmittelbar aus der Definition der Matrizenmultiplikation. Die Koeffizienten der Linearkombination stehen in der entsprechenden Zeile von S. Sodann berechnen wir die Determinate von $(SA)_{IJ}$ vermöge der Multilinearität in jeder Zeile als eine Linearkombination von Determinaten von auf den Bereich $j \in J$ eingeschränkten Zeilenvektoren von A, also entsprechende Minoren von A. Terme, in denen eine Zeile doppelt auftritt, verschwinden. Damit liegt $\det(SA)_{IJ}$ im entsprechenden Fittingideal von A. Die Aussage für AT erhält man analog durch Transposition. Genaueres findet man in [Eis, Kap 20.2]. □

Wir berechnen die Fittingideale von A wie im Elementarteilersatz Teil (1) daher mittels der diagonalen Form. Wir erhalten:

$$\mathrm{Fitt}_\nu(A) = \begin{cases} (\prod_{i=1}^{m-\nu} d_i) & \text{falls } m-\nu \leq s \\ (0) & \text{falls } m-\nu > s \end{cases}$$

Da dies Invarianten der Matrix und nicht nur der diagonalen Form sind, schließen wir, daß sich s und die Elemente d_i bis auf Assoziiertheit aus den Fittingidealen und damit der Matrix A eindeutig rekonstruieren lassen. Dies zeigt die Eindeutigkeit der Parameter der diagonalen Form. □

Als Literatur zum Elementarteilersatz sei auf [ArtinM, Kap. 12 §4] oder vom Vater des Autors der ersten Quelle und damit etwas älter [ArtinE, Kap. II] verwiesen.

A Der Satz von Cayley–Hamilton

Satz A.1 (Cayley–Hamilton). *Sei K ein Körper. Das charakteristische Polynom einer $n\times n$-Matrix bzw. eines Endomorphismus eines endlich dimensionalen K-Vektorraums annulliert die Matrix bzw. den Endomorphismus.*

Das Ziel des Appendix A besteht darin, zwei Beweise des Satzes von Cayley–Hamilton anzugeben, die der Tatsache Rechnung tragen, daß der Satz für Diagonalmatrizen und deshalb auch diagonalisierbare Matrizen trivial ist. In der Tat gilt folgende Überlegung: Sei D eine Diagonalmatrix mit Einträgen $\lambda_1, \ldots, \lambda_n$. Es gilt $\mathrm{chr}_D(X) = \prod_i (X - \lambda_i)$. Andererseits gilt für ein Polynom $f \in K[X]$ wie man einfach sieht, daß $f(D)$ eine Diagonalmatrix mit Einträgen $f(\lambda_1), \ldots, f(\lambda_n)$ ist. Daraus folgt Cayley–Hamilton für Diagonalmatrizen. Ist A diagonalisierbar, also $A = SDS^{-1}$ mit D diagonal und S invertierbar, so gilt

$$\mathrm{chr}_A(A) = \mathrm{chr}_D(SDS^{-1}) = S\big(\mathrm{chr}_D(D)\big)S^{-1} = 0,$$

und auch dieser Fall war nicht schwerer.

Beweis 1: Wir brauchen nur die Matrixversion zu beweisen. Die Aussage des Satzes wird vom Übergang zu einem Erweiterungskörper nicht tangiert: ist $K \subset L$ eine Körpererweiterung, so kann man die Matrix $A \in \mathscr{M}_n(K)$ via $\mathscr{M}_n(K) \subseteq \mathscr{M}_n(L)$ als L-wertige Matrix auffassen. Das charakteristische Polynom ändert sich nicht und auch nicht die Frage, ob seine Auswertung in A verschwindet.

Nach Korollar 1.15 können wir uns oBdA wünschen, daß das charakteristische Polynom $\mathrm{chr}_A(X)$ von A schon in $K[X]$ in Linearfaktoren zerfällt. Wir brauchen nur zu einem Zerfällungskörper von $\mathrm{chr}_A(X)$ überzugehen. Jetzt folgt aus dem Fahnensatz, siehe Aufgabe 20 LA 2, SoSe 2003, daß A ähnlich ist zu einer oberen Dreiecksmatrix. Da die Gültigkeit von Cayley–Hamilton wie oben bereits benutzt nur von der Ähnlichkeitsklasse abhängt, darf man oBdA annehemn, daß A obere Dreiecksgestalt hat.

Jetzt betreiben wir Induktion nach der Größe n der Matrix. Den Fall $n = 1$ haben wir bei der Diskussion der diagonalisierbaren Matrizen bereits erledigt. Sei

$$A = \begin{pmatrix} \lambda & * \\ 0 & A' \end{pmatrix}$$

eine Blockbeschreibung von A mit $\lambda \in K$ und $A' \in \mathscr{M}_{n-1}(K)$ in oberer Dreiecksform und $*$ für unbekannte Einträge. Dann gilt $\mathrm{chr}_A(X) = (X - \lambda) \cdot \mathrm{chr}_{A'}(X)$ und

$$\mathrm{chr}_{A'}(A) = \begin{pmatrix} \mathrm{chr}_{A'}(\lambda) & * \\ 0 & \mathrm{chr}_{A'}(A') \end{pmatrix} = \begin{pmatrix} \mathrm{chr}_{A'}(\lambda) & * \\ 0 & 0 \end{pmatrix}$$

per Induktion mit Cayley–Hamilton für A'. Es gilt also $\mathrm{chr}_{A'}(A)\big(K^n\big) \subseteq Ke_1$, wobei e_1 der erste Standardbasisvektor ist. Aber e_1 ist ein Eigenvektor von A zum Eigenwert λ und daher gilt

$$\mathrm{chr}_A(A)\big(K^n\big) = (A - \lambda)\mathrm{chr}_{A'}(A)\big(K^n\big) \subseteq (A - \lambda)Ke_1 = 0$$

und der Satz von Cayley–Hamilton ist bewiesen. □

Beweis 2: Der zweite Beweis verwendet das 'Prinzip der universellen Gültigkeit', siehe [ArtinM, Kap. 12 §3]. Sei $\mathrm{Mat}_n = \mathbb{Z}[X_{i,j} : 1 \leq i, j \leq n]$ der Polynomring in n^2 Variablen, welche wie die Einträge einer $n \times n$-Matrix nummeriert werden. Dann gilt für jeden Ring R

$$\mathrm{Hom}_{\mathrm{Ringe}}(\mathrm{Mat}_n, R) = \mathscr{M}_n(R)$$

als Gleichheit von Mengen. Dabei gehört zur Matrix $A = (a_{i,j})$ der Homomorphismus φ_A, welcher die Variable $X_{i,j}$ in $a_{i,j}$ auswertet. Zur Identität $\mathrm{id} : \mathrm{Mat}_n \to \mathrm{Mat}_n$ gehört die **universelle $n \times n$-Matrix** $\underline{X} = (X_{i,j}) \in \mathscr{M}_n(\mathrm{Mat}_n)$.

Zu einem Ringhomomorphismus $\varphi : R \to S$ gibt es ein kommutatives Diagramm von Mengen

$$\begin{array}{ccc} \mathscr{M}_n(R) & \xrightarrow{\varphi} & \mathscr{M}_n(S) \\ \downarrow & & \downarrow \\ R[T] & \xrightarrow{\varphi[T]} & S[T] \end{array}$$

in dem die vertikalen Pfeile einer Matrix ihr charakteristisches Polynom zuordnen und die horizontalen Pfeile den Morphismus φ auf die Matrix- bzw. Polynomkoeffizienten anwenden. Dieses Diagramm erlaubt uns zwei Argumentationen: (i) gilt Cayley–Hamilton für $A \in \mathscr{M}_n(R)$, so gilt er auch für $\varphi(A) \in \mathscr{M}_n(S)$, und (ii) ist φ injektiv und gilt Cayley–Hamilton für $\varphi(A), A \in \mathscr{M}_n(R)$, so auch schon für A.

Gegeben sei nun ein Ring R und eine beliebige Matrix $A \in \mathscr{M}_n(R)$. Dann ist $A = \varphi_A(\underline{X})$ und nach (i) haben wir Cayley–Hamilton nur für die universelle Matrix $\underline{X}$ zu zeigen, um den Satz von Cayley–Hamilton sogar über jedem Ring (!) zu beweisen.

Jetzt machen wir eine Anleihe bei der Theorie des Transzendenzgrades: Es gibt eine injektive Abbildung $\mathrm{Mat}_n \hookrightarrow \mathbb{C}$ in den Körper der komplexen Zahlen. Nach (ii) reicht es also, den Fall $K = \mathbb{C}$ zu betrachten.

Die Koeffizienten des charakteristischen Polynoms einer komplexen Matrix sind Polynome in den Matrixeinträgen und daher stetige Funktionen auf dem Vektorraum $\mathscr{M}_n(\mathbb{C}) = \mathbb{C}^{n^2}$ mit der üblichen metrischen Topologie. Damit liefert $\mathscr{M}_n(\mathbb{C}) \ni A \mapsto \mathrm{chr}_A(A) \in \mathscr{M}_n(\mathbb{C})$ eine stetige Selbstabbildung von $\mathbb{C}^{n^2}$. Da wir den Satz von Cayley–Hamilton für diagonalisierbare Matrizen schon aus dem Vorspann kennen, reicht es aufgrund der Stetigkeit jetzt aus, solche Matrizen als dicht in allen Matrizen zu erkennen.

Eine Matrix, deren Minimalpolynom lauter verschiedene Nullstellen hat, ist sicher diagonalisierbar. Wir zeigen, daß auch schon diese dicht liegen. Dazu bemerken wir, daß es ein Polynom in den Koeffizienten a_i eines (normierten) Polynoms $f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ vom Grad n gibt, die Diskriminante $\Delta(f) = \Delta(a_0, \ldots, a_{n-1})$, siehe Lemma A.3, das genau dann verschwindet, wenn das zugehörige Polynom $f(X)$ eine mehrfache Nullstelle besitzt. Für eine Matrix A ist $\Delta = \Delta(\mathrm{chr}_A(X))$ ein Polynom in den Matrixeinträgen und der 'schlechte Ort' in $\mathscr{M}_n(C) = \mathbb{C}^{n^2}$ ist genau das Nullstellengebilde von Δ. Sicher ist Δ nicht das 0-Polynom, denn seiner Bedeutung nach wäre sonst keine Matrix über $\mathbb{C}$ mit lauter verschiedenen Eigenwerten diagonalisierbar. Dies ist sicher nicht richtig, da wir etwa aus $1, 2, \ldots, n$ eine Diagonalmatrix bilden können.

Wenn aber $\Delta \neq 0$ gilt als Polynom, dann liegt der Ort, an dem es nicht verschwindet, dicht in $\mathbb{C}^{n^2}$. Ansonsten hätte der Ort $\{A \in \mathscr{M}_n(\mathbb{C}) \,|\, \Delta(A) = 0\}$ innere Punkte, das heißt Δ verschwindet auf einem kleinen Ball. Jetzt machen wir Analysis. Dann verschwinden nämlich auch alle Ableitungen an einem Punkt in diesem Ball und damit auch die Taylorreihe von Δ um diesen Punkt. Es ist Δ ein Polynom und damit sicher identisch mit seiner Taylorreihe; es verschwindet vielmehr, wenn dies die Taylorreihe tut. Somit verschwindet Δ als Polynom, und dies ist ein Widerspruch. □

Die Menge der Polynome, welche eine Matrix/einen Endomorphismus annullieren, ist ein Ideal des Polynomrings und somit von einem Element, welches wir **Minimalpolynom** nennen, erzeugt. Dieses Annulatorideal ist nicht (0), da der Raum der Matrizen/Endomorphismen von endlicher Dimension ist und somit nicht alle Potenzen der Matrix/des Endomorphismus linear unabhängig sein können.

Satz A.2. *Sei K ein Körper.*

(1) Das Minimalpolynom einer $n \times n$-Matrix bzw. eines Endomorphismus eines endlichdimensionalen K-Vektorraums teilt das charakteristische Polynom der Matrix bzw. des Endomorphismus.

(2) Jeder Primfaktor des charakteristischen Polynoms teilt das Minimalpolynom.

Beweis: (1) ist nur eine Umformulierung des Satzes von Cayley–Hamilton. Bei (2) brauchen wir nur den Fall einer Matrix zu betrachten. Teilt ein Primteiler p des charakteristischen Polynoms das Minimalpolynom m nicht, so muß der größte gemeinsame Teiler von p und m gleich 1 sein. Nach dem Satz von Bézout, Satz 1.10, gibt es Polynome $\mu, \pi \in K[X]$ mit $\pi p + \mu m = 1$.

Diese Relation geht nach Übergang zu einem Erweiterungskörper $K \subseteq L$ in $L[X]$ nicht verloren. Wir dürfen also wegen Satz 1.14 nach einer Erweiterung annehmen, daß p zwar nicht mehr irreduzibel ist, dafür aber eine Nullstelle λ in L hat. Dazu gehört ein Eigenvektor v. Es annulliert weiterhin m die Matrix A. Somit gilt $m(A)v = m(\lambda)v = 0$. Aus $v \neq 0$ folgt, daß λ eine Nullstelle von m ist. Damit gilt aber $0 = \pi(\lambda)p(\lambda) + \mu(\lambda)m(\lambda) = 1(\lambda) = 1$. Dies ist ein Widerspruch zur Annahme p teile m nicht. □

Wir haben noch das Folgende Nachzutragen. Literatur darüber findet man etwa in [Lang, IV §8].

Lemma A.3 (Diskriminante — Resolvente). *Sei K ein Körper, und seien $f(X) = a_nX^n + \cdots + a_0$ und $g(X) = b_mX^m + \cdots + b_0$ Polynome in $K[X]$.*

(1) Es gibt ein Polynom $\mathrm{Res}_{n,m}$ in Variablen A_i, B_j für $0 \leq i \leq n, 0 \leq j \leq m$, welches genau dann in $A_i = a_i$, $B_j = b_j$ verschwindet, wenn die zugehörigen Polynome f, g eine gemeinsame Nullstelle in einem Erweiterungskörper haben. Das Polynom $\mathrm{Res}_{n,m}$ heißt **Resolvente** *und sein Wert $\mathrm{Res}_{n,m}(a_i, b_j) = \mathrm{Res}(f, g)$ heißt* **Resolvente von** *f, g.*

(2) Sei $a_n = 1$. Dann ist $f \mapsto \Delta(f) = \mathrm{Res}(f, f')$ ein Polynom in Varaiablen A_i, $0 \leq i < n$, welches genau dann in $A_i = a_i$ verschwindet, wenn das zugehörige Polynom f eine doppelte Nullstelle in einem Erweiterungskörper hat. Das Polynom Δ heißt **Diskriminante** *n***ter Ordnung**.

(3) Ein normiertes Polynom $f \in \mathbb{C}[X]$ zerfällt in paarweise verschiedene Linearfaktoren, genau wenn $\Delta(f) \neq 0$.

Beweis: (1) Wir definieren die Resolvente $\mathrm{Res}_{n,m}(A_i, B_j)$ als Determinante im Polynomring $K[A_i, B_j]$ von

$$\begin{pmatrix} A_n & A_{n-1} & \cdots & A_0 & & & \\ & A_n & \ddots & & \ddots & & \\ & & \ddots & \ddots & & \ddots & \\ & & & A_n & A_{n-1} & \cdots & A_0 \\ B_m & B_{m-1} & \cdots & B_0 & & & \\ & B_m & \ddots & & \ddots & & \\ & & \ddots & \ddots & & \ddots & \\ & & & B_m & B_{m-1} & \cdots & B_0 \end{pmatrix} \in \mathscr{M}_{n+m}(K[A_i, B_j]).$$

Wir verwenden Lemma 1.15, um oBdA davon auszugehen, daß f und g über K in Linearfaktoren zerfallen. Wir betrachten $\mathrm{Res}(f, g) = \mathrm{Res}_{n,m}(a_i, b_j)$. Dies ist die Determinante der Matrix, wenn man in die Variablen A_i, B_j jeweils a_i, b_j einsetzt. Haben f und g eine gemeinsame Nullstelle x, so liegt der Spaltenvektor $(x^{n+m}, \ldots, x, 1)$ im Kern der Matrix aufgefaßt als Endomorphismus von K^{n+m}. Damit verschwindet die Determinante und somit auch $\mathrm{Res}(f, g)$.

Jetzt müssen wir noch sehen, daß aus $\mathrm{Res}(f, g) = 0$ folgt, daß f und g eine gemeinsame Nullstelle haben. Sei $f(X) = a_n \prod_i (X - \alpha_i)$ und $g(X) = b_m \prod_j (X - \beta_j)$ die Zerlegung in Linearfaktoren. Nach Lemma A.4 gilt für die Resolvente von f, g die Formel $\mathrm{Res}(f, g) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j)$. Damit folgt die Behauptung.

(2) Sei $f(x_0) = 0$. Dann ist $f(X) = (X - x_0)g(X)$ und nach der Produktregel $f'(X) = (X - x_0)g'(X) + g(X)$. Damit gilt $f'(x_0) = g(x_0)$ und somit verschwindet die Ableitung von f in x_0 genau dann, wenn sich aus f ein weiterer Linearfaktor $(X - x_0)$ abspalten läßt. Der Rest folgt aus (1).

(3) Nach dem Fundamentalsatz der Algebra, [Meyb, 6.10], zerfällt jedes Polynom über den komplexen Zahlen in Linearfaktoren. Damit folgt (3) aus (2). □

Lemma A.4. *Sei K ein Körper und seien $f(X) = a_n \prod_i (X - \alpha_i)$ und $g(X) = b_m \prod_j (X - \beta_j)$ zerfallende Polynome aus $K[X]$. Dann gilt die Formel* $\operatorname{Res}(f, g) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j)$.

Beweis: [Lang, IV Prop 8.3]. Man kann dies mittels des 'Prinzips der universellen Gültigkeit' zeigen. Wir führen für die Nullstellen α_i und β_j und die führenden Koeffizienten a_n, b_m Variablen ein und stellen fest, daß die behauptete Formel eine Polynomidentität in diesen Variablen wird. Diese gilt dann, wenn sie für Belegungen mit komplexen Zahlen gültig ist. Wir haben damit auf den Fall $K = \mathbb{C}$ reduziert, der uns in der Anwendung im Beweis des Satzes von Cayley-Hamilton auch ausschließlich interessiert.

Wir berechnen das folgende Matrixprodukt, wobei die a_i wie oben die Koeffizienten von f und die b_j diejenigen von g bezeichnen:

$$\begin{pmatrix} a_n & \cdots & a_0 & & \\ & \ddots & & \ddots & \\ & & a_n & \cdots & a_0 \\ b_m & \cdots & b_0 & & \\ & \ddots & & \ddots & \\ & & b_m & \cdots & b_0 \end{pmatrix} \begin{pmatrix} \beta_1^{n+m-1} & \cdots & \beta_m^{n+m-1} & \alpha_1^{n+m-1} & \cdots & \alpha_n^{n+m-1} \\ \vdots & & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & & \vdots \\ \beta_1 & \cdots & \beta_m & \alpha_1 & \cdots & \alpha_n \\ 1 & \cdots & 1 & 1 & \cdots & 1 \end{pmatrix}$$

Das Ergebnis ist die folgende Blockmatrix

$$= \left(\begin{array}{ccc|ccc} f(\beta_1)\beta_1^{m-1} & \cdots & f(\beta_m)\beta_m^{m-1} & & & \\ \vdots & & \vdots & & 0 & \\ f(\beta_1)\beta_1 & \cdots & f(\beta_m)\beta_m & & & \\ f(\beta_1) & \cdots & f(\beta_m) & & & \\ \hline & & & g(\alpha_1)\alpha_1^{n-1} & \cdots & g(\alpha_n)\alpha_n^{n-1} \\ & 0 & & \vdots & & \vdots \\ & & & g(\alpha_1)\alpha_1 & \cdots & g(\alpha_n)\alpha_n \\ & & & g(\alpha_1) & \cdots & g(\alpha_n) \end{array}\right)$$

Ein Vergleich der Determinanten liefert das Folgende (man denke an die Vandermondedeterminante):

$$\operatorname{Res}(f,g) \cdot \prod_{j<j'} (\beta_j - \beta_{j'}) \prod_{i<i'} (\alpha_i - \alpha_{i'}) \prod_{j,i} (\beta_j - \alpha_i) = \prod_j f(\beta_j) \prod_i g(\alpha_i) \prod_{j<j'} (\beta_j - \beta_{j'}) \prod_{i<i'} (\alpha_i - \alpha_{i'}).$$

Verwendet man nun

$$f(\beta_j) = a_n \prod_i (\beta_j - \alpha_i) \quad \text{und} \quad g(\alpha_i) = b_m \prod_j (\alpha_i - \beta_j),$$

so haben wir in der Determinantengleichung die gesuchte Formel bis auf einen zusätzlichen Faktor $\prod_{j<j'} (\beta_j - \beta_{j'}) \prod_{i<i'} (\alpha_i - \alpha_{i'}) \prod_{j,i} (\beta_j - \alpha_i)$ bewiesen. Dieser Faktor ist von 0 verschieden, falls die α_i und β_j alle paarweise verschieden sind, also insgesamt $n + m$ Zahlen sind.

Hätten wir nicht nach $\mathbb{C}$ spezialisiert, wären wir jetzt fertig, denn im Polynomring mit Variablen α_i, β_j sind diese sicherlich paarweise verschieden. Da wir aber speziell den komplexen Fall $K = \mathbb{C}$ benötigen, fahren wir im Beweis fort.

Wir stören unsere Nullstellen ein wenig. Dazu wählen wir $n+m$ paarweise verschiedene ε_i, η_j für $1 \le i \le n$ und $1 \le j \le m$. Zum Parameter $t \in \mathbb{C}$ betrachten wir die Polynome

$$f_t(X) = a_n \prod_i \big(X - (\alpha_i + \varepsilon_i t)\big) \quad \text{und} \quad g_t(X) = b_m \prod_j \big(X - (\beta_j + \eta_j t)\big).$$

Fassen wir t als in t ausgewertete Variable T auf, so wird die zu beweisende Identität eine Identität von Polynomen in T mit Koeffizienten aus $\mathbb{C}$. Da ein nichtverschwindendes Polynom über einem Körper nur endlich viele Nullstellen haben kann, sind wir fertig, wenn wir für unendlich viele $T = t$ unsere Formel beweisen können.

Aufgrund der Wahl der ε_i, η_j ist die Menge der deformierten Nullstellen $\{\alpha_i + \varepsilon_i t, \beta_j + \eta_j t\}$ nur für endlich viele Werte von t nicht von Mächtigkeit $n + m$. In der Tat verbietet Jede der Gleichungen einer Koinzidenz von Nullstellen nur einen Parameterwert t. Für alle anderen Parameterwerte haben wir die Formel aber oben schon nachgewiesen, da man dann den störenden Faktor kürzen darf.

Bei genauer Betrachtung benötigt man für das letzte Argument nur, daß es unendlich viele komplexe Zahlen gibt. Das Argument funktioniert also auch über jedem anderen unendlichen Körper. □

B Strukturtheorie endlich erzeugter abelscher Gruppen

In diesem Abschnitt spezialisieren wir die Aussagen der Kapitel 3 und 4 auf den Fall $R = \mathbb{Z}$. Moduln unter $\mathbb{Z}$ sind nichts anderes als abelsche Gruppen. Wir behandeln also die Klassifikation endlich erzeugter abelscher Gruppen. Die Primelemente von $\mathbb{Z}$ sind nichts anderes als die Primzahlen.

Satz B.1 (Struktursatz endlich erzeugter abelscher Gruppen). *Sei A eine endlich erzeugte abelsche Gruppe.*

(1) Es gibt eine kanonische exakte Sequenz

$$0 \to A_{\text{tors}} \to A \to A/\text{tors} \to 0 \tag{B.1}$$

mit einer endlichen Untergruppe $A_{\text{tors}} \subseteq A$ der Torsionselemente und einem freien endlich erzeugten Quotienten $A/\text{tors} \cong \mathbb{Z}^r$. Die Sequenz (B.1) spaltet unkanonisch. Somit gilt unkanonisch $A \cong A_{\text{tors}} \oplus A/\text{tors}$.

(2) Sei $A = A_{\text{tors}}$ eine endlich erzeugte Torsionsgruppe. Dann zerfällt A kanonisch in Primärkomponenten

$$A = \bigoplus_{p|\#A} A[p^\infty]$$

und es gibt eine nichtkanonische Zerlegung $A[p^\infty] \cong \bigoplus_i \mathbb{Z}/(p^{e_i})$ als endliche direkte Summe, wobei die Anzahlen $\#\{i\}$ und $\#\{i \mid e_i = e\}$ unabhängig von der Zerlegung sind.

(3) Es gibt eine nicht kanonische Zerlegung als direkte Summe

$$A \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{s} \mathbb{Z}/(d_i)$$

mit sich aufsteigend teilenden natürlichen Zahlen $d_1|d_2|\ldots|d_s$. Die Zahlen r und s sowie die d_i sind eindeutig.

Beweis: (1) Dies ist Korollar 4.3(1) für den Fall $R = \mathbb{Z}$. Wegen $A \cong A_{\text{tors}} \oplus A/\text{tors}$ und Lemma 3.2 ist auch A_{tors} endlich erzeugt, somit ein Quotient von $\big(\mathbb{Z}/(\#A)\big)^n$ für $n \gg 0$ und damit endlich.

(2) Nach dem Satz von Lagrange annulliert die Gruppenordnung $\#A$ jedes einzelne Element und damit A. Jetzt folgt (2) aus Satz 2.2 und Satz 3.1 für $R = \mathbb{Z}$.

(3) Dies ist Korollar 4.3(2) für den Fall $R = \mathbb{Z}$. Es ist $r = \dim_{\mathbb{Q}} A \otimes_{\mathbb{Z}} \mathbb{Q}$ beziehungsweise der Rang von A/tors. □

Literatur

[ArtinE] Artin, E., *Algebra II*, Ausarbeitung der von Prof. Emil Artin im WS 1961/62 an der Universität Hamburg gehaltenen Vorlesung.

[ArtinM] Artin, M., *Algebra*, Birkhäuser advanced texts, dt. Auflage (1993).

[Eis] Eisenbud, D., *Commutative Algebra with a View Toward Algebraic Geometry*, Springer GTM **150** (1994).

[Lang] Lang, S., *Algebra*, Revidierte dritte Auflage, Springer GTM **211** (2002).

[Lieb] Lieb, I., *Endlich erzeugte Moduln über Hauptidealringen*, `http://www.math.uni-bonn.de/people/hefer/LAII/torsionsmoduln.ps`

[Meyb] Meyberg, K., *Algebra, Teil 1+2*, Carl Hanser Verlag (1975).