Lineare Algebra II

SoSe 1999

Wiland Schmale

(Schreibfehler zuletzt berichtigt am 9. Mai 2003)

Inhaltsverzeichnis

Einleitung

Der Hauptteil meiner Linearen Algbra II ist eine Einführung in die lineare Algebra über Ringen und zwar insbesondere über euklidischen Ringen wie $\mathbb{Z}$ und $K[x]$, K ein Körper.

Statt K-Vektorräumen wie in der Linearen Algebra I betrachten wir jetzt R-Moduln.

Ein R-Modul ist genau wie ein K-Vektorraum eine abelsche Gruppe mit einer Skalarmultiplikation, wobei jetzt allerdings die Skalare aus einem Ring stammen. Vektorräume sind miterfaßt als K-Moduln, K ein Körper.

Bei der Beschäftigung mit Moduln stößt man auf ganz neuartige Phänomene, die stark geprägt sind von den Ringen, die man als Skalarbereiche zulassen will.

Bei uns sind es euklidische Ringe wie $\mathbb{Z}$ und $K[x]$, die im Vordergrund stehen werden. Diese erlauben eine schöne Theorie von großem praktischen Nutzen. Einige beispielhafte Anwendungen sollen dies unterstreichen.

Ein unerwartetes aber wesentliches Phänomen in der linearen Algebra über Ringen ist folgendes:

Ein n-dimensionaler Vektorraum über einem Körper K kann nach Einführung von Koordinaten bis auf Isomorphie durch K^n beschrieben werden. Ist R ein kommutativer Ring (z. B. $R = \mathbb{Z}$) und betrachtet man von R^n ausgehende lineare Abbildungen, so ist keineswegs sicher, ob der Bild-Modul bis auf Isomorphie durch einen Modul R^k, k geeignet, dargestellt werden kann. Dies ist schon für $n = 1$ der Untersuchung wert, wie folgende Beispiele zeigen:

Beispiel 1: Seien $R = \mathbb{Z}$ und $Z_2 = \{0, 1\}$ Körper mit 2 Elementen. Zu $z \in \mathbb{Z}$ sei

$$z \cdot 0 = 0 \text{ und } z \cdot 1 = \left\{ \begin{array}{cl} \overbrace{1 + \cdots + 1}^{z\text{-mal}} & \text{falls } z > 0 \\ 0 & \text{falls } z = 0 \\ -|z| \cdot 1 & \text{falls } z < 0 \end{array} \right\}$$

$\mathbb{Z}_2$ wird so zu einem $\mathbb{Z}$-Modul und die Abbildung

$$G : \mathbb{Z} \longrightarrow \mathbb{Z}_2 \quad \text{mit} \quad G(z) = \left\{ \begin{array}{ll} 0 & \text{wenn } z \text{ gerade} \\ 1 & \text{wenn } z \text{ ungerade} \end{array} \right\}$$

ist surjektiv und $\mathbb{Z}$-linear.

Beispiel 2: Seien jetzt K ein Körper, $R = K[x]$ und $\alpha \in K$. Auf folgende Weise wird K ein $K[x]$-Modul: Zu $k \in K$ und $p \in K[x]$ sei

$$\underset{\substack{\uparrow \\ \text{zu definierende} \\ \text{Skalarmultiplikation}}}{p \cdot k} := \underset{\substack{\uparrow \\ \text{Multiplikation} \\ \text{in } K}}{p(\alpha) \cdot k}$$

Die Abbildung $\pi_\alpha : K[x] \longrightarrow K$ mit $\pi_\alpha(p) = p(\alpha)$ ist eine $K[x]$-lineare Abbildung.

Für $n \geq 1$ ist in zahlreichen Anwendungen der linearen Algebra über Körpern folgendes Beispiel grundlegend:

Beispiel 3: Seien K ein Körper, V ein K-Vekorraum und F eine lineare Abbildung von V nach V. Zu $p = a_0 + \cdots + a_d x^d \in K[x]$ sei $p(F) = a_0 Id_V + \cdots + a_d F^d$ und zu $v \in V$ und $p \in K[x]$ sei $p \cdot v := p(F)(v)$. Man erkennt so die durch den Endomorphismus F hervorgerufene $K[x]$-Modulstruktur von V. Mit $R = K[x]$ kann i. A. nicht gelten: $V \cong R^n$ schon gar nicht, wenn V endlich dimensional ist. Läßt sich V trotzdem mit Hilfe von R beschreiben?

Während bei einem Körper K der eindimensionale K-Vektorraum $K = K^1$ durch eine K-lineare Abbildung nur auf 0 oder auf einen zu K isomorphen Raum abgebildet werden kann, gibt es bei Ringen noch viele Möglichkeiten "dazwischen". Allerdings sind die von 0 verschiedenen Bilder von $R = R^1$ stets nicht nur R-Moduln sondern auch Ringe und zwar i. A. durchaus von R sehr verschiedene Ringe.

Dieses Phänomen ist der Hauptgrund, warum in den Abschnitten 2 und 3 ganz ausführlich die möglichen homomorphen Bilder der Ringe $\mathbb{Z}$ und $K[x]$ untersucht werden.

Damit erweitern wir zugleich beträchtlich unseren Beispielvorrat an Ringen und Körpern. Insbesondere wird es um endliche Ringe und Körpern gehen, die in und außerhalb der Mathematik heute eine wichtige Rolle spielen.

Die Vorlesung beginnt in Kapitel I mit den Abschnitten 2, 3 und 4. Nachdem so der nötige Vorrat an Ringen erarbeitet ist und genügend Information über deren Struktur vorliegen, geht es in Kapitel II zunächst um Matrizen über euklidischen Ringen und deren äquivalenten Umformungen (Abschnitte 6, 9). In Abschnitt 7 lösen wir lineare Gleichungen mit z. B. ganzzahligen Koeffizienten. In den Abschnitten 10 und 11 wird gezeigt, wie auf Grund der Smith-Form für Polynommatrizen das Normalformenproblem aus der linearen Algebra elegant und vollständig gelöst werden kann. Behandelt werden die Frobenius-, Weierstraß-, Jacobson- und Jordan-Normalformen. Erst in Kapitel III geht es um lineare Algebra, wie sie vom ersten Semester her bei Vektorräumen vertraut ist. Allerdings nehmen jetzt Ringe und Moduln die Stellen ein von Körpern und Vektorräumen. Ansonsten beschäftigt man sich aber mit denselben Themen: Erzeugendensysteme, Basen, Dimension, lineare Abbildungen. Mit einigen Überraschungen ist bei dieser etwas verallgemeinerten Version der linearen Algebra allerdings zu rechnen. Die Matrizenkenntnisse aus Kapitel II gehen an wesentlichen Stellen ein. Neben den bereits in Kapitel III zu behandelnden

eher geometrischen Anwendungen, soll in Kapitel IV an wenigstens einem Beispiel ein etwas längerer Abstecher in einen Anwendungsbereich stattfinden. Gelegenheiten zur Benutzung von Maple o. Ä. entstehen im Zusammenhang mit dieser Linearen Algebra II reichlich. Anregungen und Hilfestellungen dazu werden in der Vorlesung gegeben werden. Das kürzlich erschienene Buch [KiSch] bietet in dieser Hinsicht einiges mehr, ist aber von der Stoffauswahl her (abgesehen von Linearer Algebra I) nur noch für Kapitel II relevant.

Motiviert durch Anwendungen in der Kontroll- oder Regelungstheorie habe ich zum erstenmal im SoSe 88 eine Lineare Algebra II mit einer ähnlichen Stoffauswahl durchgeführt. Unabhängig davon hat in den letzten Jahren dieser Stoff zunehmend Eingang in die Lehrbuchliteratur zur linearen Algebra gefunden. Die vorherrschende Motivation dabei ist der elegante Zugang zu Ähnlichkeitsnormalformen über einem Körper und der sogenannte Hauptsatz für endlich erzeugte abelsche Gruppen. Auf Anwendungen außerhalb der Algebra oder linearen Algebra wird selten hingewiesen, obwohl dies schon in dem Klassiker [Ga] angelegt ist.

Beispiele neuerer Lehrbücher, die die Theorie der Moduln über euklidischen oder Hauptideal-Ringen einbeziehen, sind [AdWe], [Lue1] und [KoMi] ab 10. Auflage. Ältere Werke sind [HaHa] und [Ga].

Inzwischen ist die mathematische Kodierungstheorie zu einem reizvollen Gebäude hochgewachsen. Dem wird am Schluß der Vorlesung mit einer kurzen Einführung zu wichtigen linearen fehlerkorrigierenden Code-Klassen Rechnung getragen.

Zur Benutzung dieses Skripts:

Beim Lesen des Skripts wird man feststellen, daß die Darstellungsweise uneinheitlich ist. Dies ist zu einem großen Teil Absicht. Es handelt sich nicht um eine Niederschrift einer Vorlesung sondern um einen Text, der in die Vorlesung mit einbezogen wird. Er enthält zwar fast alle Definitionen und Sätze der Vorlesung aber nur einen kleinen Teil der Beweise und auch nicht alle Beispiele. Einige Beweise sind allerdings in voller Ausführlichkeit enthalten. Diese können dem Selbststudium überlassen oder in der Vorlesung auf eine Leinwand projiziert werden und gemeinsam ohne Mitschreiben durchgegangen werden. Ähnlich kann man mit den zahlreichen Definitionen verfahren. Ein großer Teil der notwendigen Definitionen ist in Abschnitt 1 konzentriert, auf den im Verlauf der Vorlesung – die mit Abschnitt 2 beginnt – immer wieder zurückgegriffen werden kann.

Ich stelle mir vor, daß am Ende des Semesters die Studierenden neben diesem Skript ein "wohlnummeriertes" Paket an Vorlesungsmitschriften vorliegen haben. Beides zusammen sollte dann gemeinsam mit den Übungsmaterialien ausreichen, um selbständig den Stoff nachzuvollziehen und ihn auch später noch benutzen zu können.

Kapitel I

Ringe

0 Vorbemerkungen zu Kapitel I

Das Material der folgenden Paragraphen sollte nicht als Einführung in die Grundlagen der Ringtheorie gesehen werden. Übergeordnetes Ziel ist eine Einführung in die lineare Algebra über gewissen Ringen als Verallgemeinerung der linearen Algebra über Körpern. Die dabei ins Auge gefaáten Ringe sind in erster Linie $\mathbb{Z}$ und $K[x]$, K ein Körper. Beides sind euklidische Ringe (Abschnitt 4). Solche Ringe sind – was lineare Algebra angeht – noch relativ leicht beherrschbar. Insbesondere sind sie auch der Berechnung zugänglich und für zahlreiche Anwendungen von Bedeutung. Die wichtigsten Eigenschaften der uns im folgenden interessierenden Ringe sind daher der Gegenstand dieses Kapitels bis einschlieálich Abschnitt 4. In Abschnitt 5 sind ein paar Informationen über den Matrizenring $R^{n\times n}$ zusammengestellt.

Obwohl erst in Kapitel III Moduln und lineare Abbildungen im Vordergrund stehen, ist es zweckmääig ihre Definition frühzeitig zur Kenntnis zu nehmen (Abschnitt 1(B)). Der definitorische Unterschied zu Vektorräumen ist minimal und man kann dort, wo eine natürliche Modulstruktur vorliegt auch gleich darauf hinweisen.

1 Grundlegende Definitionen

Bemerkung. Nicht alle Definitionen werden – und schon gar nicht gleich zu Anfang – in der Vorlesung behandelt. Das Folgende ist eine Übersicht und zum Nachschlagen. Die Vorlesung beginnt mit Abschnitt 2.

(A) Ringaxiome, abgeleitete Grundregeln, Einheiten, Äquivalenz, Nullteiler

Definition 1.1. *Sei R eine Menge und seien $+,\cdot$ zwei Verknüpfungen ("Addition" und "Multiplikation") auf R (vgl. [Fi, S. 41]) R heiße* **Ring** *(bezüglich $+,\cdot$), wenn gilt:*

(a) *R ist abelsche Gruppe bzgl. $+$*

(b) *Für alle $r, s, t \in R$ gilt*

$$r \cdot (s + t) = r \cdot s + r \cdot t \quad \text{und} \quad (r + s) \cdot t = r \cdot t + s \cdot t$$

(c) *Für alle $r, s, t \in R$ gilt: $r \cdot (s \cdot t) = (r \cdot s) \cdot t$*

(d) *Es gibt ein $e \in R$ mit $e \cdot r = r \cdot e = r$ für alle $r \in R$.*

Bemerkung. Manche Autoren lassen bei der Definition eines Ringes die Forderungen (c), (d) weg, wie z. B. [Wa, S. 64]. Weithin üblich – und für die Ziele dieser Vorlesung allgemein genug – ist allerdings obige Definition 1.1. Wenn man die benutzten Verknüpfungen zweifelsfrei hervorheben möchte, dann ist $\boldsymbol{(R, +, \cdot)}$ die vollständige Bezeichnung für einen Ring. Dies wird nur gelegentlich notwendig sein.

Definition 1.2. *Ein Ring R heißt* **kommutativ**, *wenn für alle $r, s \in R$ gilt:*

$$r \cdot s = s \cdot r\,.$$

Schreibweisen. rs statt $r \cdot s$, 1 statt e, 0 für das neutrale Element bzgl. $+$, $-r$ für das additive Inverse zu r. Wenn zwei Ringe R, S gleichzeitig betrachtet werden: 1_R, 1_S, 0_R, 0_S.

Satz 1.3. *In jedem Ring R gelten folgende Regeln:*

(a) $|R| > 1 \Longleftrightarrow 1 \neq 0$

(b) $0r = r0 = 0$ *für alle $r \in R$*

(c) $(-1)r = -r$ *für alle $r \in R$*

(d) $(-1)(-1) = 1$

(e) $(-r)s = -(rs)$ *und* $(-r)(-s) = rs$ *für alle $r, s \in R$*

(f) *Assoziativgesetze bzgl. $+$ und $\cdot$ für endlich viele Elemente aus R*

(g) *Distributivgesetze für endlich viele Elemente aus R.*

Natürlich gelten alle für abelsche Gruppen gültigen Regeln auch in R bzgl. $+$. Siehe z. B. [Fi, S. 41ff].

Definition 1.4. *Sei R ein Ring. $r \in R$ heißt* **Einheit**, *wenn es $s \in R$ gibt mit $rs = sr = 1$. s heißt dann (multiplikatives)* **Inverses** *von r und ist eindeutig durch r bestimmt.*

Schreibweise. $s = r^{-1}$

Satz 1.5. *Sei R ein Ring. $G(R) = \{r \in R \mid r \text{ ist Einheit }\}$ ist eine Gruppe bezüglich der Multiplikation von R. Sie wird* **Einheitengruppe** *genannt. Es gilt für alle $a, b \in G(R) : (ab)^{-1} = b^{-1}a^{-1}$.*

Definition 1.6. *Sei R ein Ring und seien $r, s \in R$.*

(a) r, s heißen **äquivalent***, wenn es $u, v \in G(R)$ gibt mit $ur = sv$.*

Schreibweise. $r \sim s$

Bemerkung. Man rechnet leicht nach, dass " $\sim$ " eine Äquivalenzrelation ist. Im Falle $R = K^{n\times n}$, K Körper handelt es sich um die bereits aus Lineare Algebra I bekannte Matrizenäquivalenz, deren Äquivalenzklassen ausführlich untersucht wurden. Im Falle $R = \mathbb{Z}$ sind die Äquivalenzklassen einfach die Mengen $\{z, -z\}$ mit $z \in \mathbb{Z}$. Ist $R = K$ ein Körper, so gibt es nur die Äquivalenzklassen $\{0\}$, $K\backslash\{0\}$. $G(R)$ ist stets eine Äquivalenzklasse.

Fortsetzung von Definition 1.6:

(b) r, s heißen **linksäquivalent***, wenn es $u \in G(R)$ gibt mit $ur = s$.*

Schreibweise. $r \underset{\ell}{\sim} s$

(c) r, s heißen **rechtsäquivalent***, wenn es $u \in G(R)$ gibt mit $ru = s$.*

Schreibweise. $r \underset{r}{\sim} s$

Auch $\underset{r}{\sim}$, $\underset{\ell}{\sim}$ sind Äquivalenzrelationen und stets $G(R)$ eine Äquivalenzklasse.

Definition 1.7. *$r \in R\backslash\{0\}$ heißt* **Nullteiler***, wenn es ein $s \in R\backslash\{0\}$ gibt mit $rs = 0$ oder $sr = 0$. Im ersten Fall heißt r Links-Nullteiler im zweiten Fall Rechts-Nullteiler. Ein Ring $\neq \{0\}$ ohne Nullteiler heißt* **Bereich** *(wenn R kommutativ ist, oft auch: Integritätsbereich).*

Die bisher eingeführten Begriffe werden illustriert durch die **Beispiele:** $\{0\}$, Körper, $\mathbb{Z}$, $R^{n\times n}$, $\mathrm{Abb}(M, R)$. Weitere Beispiele von Ringen ergeben sich in den Abschnitten 2 und 3.

Eine für uns wichtige Eigenschaft von Bereichen ist die folgende **Kürzungsregel:** Seien R ein Bereich und $r, s, s' \in R$, $r \neq 0$. Dann gilt: $rs = rs' \Longrightarrow s = s'$.

(B) Moduln, Untermoduln, lineare Abbildungen

Die folgenden Definitionen sind fast identisch mit den Definitionen von Vektorraum, Untervektorraum und linearer Abbildung zwischen Vektorräumen. Einziger Unterschied: Der Skalarbereich ist jetzt ein kommutativer Ring.

Moduln und lineare Abbildungen sind erst in Kapitel III unser Hauptthema. Es lohnt sich aber, bereits vorher an einigen Stellen diese Begriffe zu benutzen.

Definition 1.8. *Sei R ein kommutativer Ring $\neq \{0\}$. Ein* **R-Modul** *(genauer : R-Links-Modul) oder:* **Modul über R** *ist ein Tripel $(M, +, \cdot)$, bestehend aus einer Menge M, einer Verknüpfung (Addition)*

$$\begin{aligned} + : M \times M &\longrightarrow M\,, \\ (v, w) &\longmapsto v + w\,, \end{aligned}$$

und einer Verknüpfung (Multiplikation mit Skalaren)

$$\begin{aligned} \cdot : R \times M &\longrightarrow M\,, \\ (\lambda, v) &\longmapsto \lambda \cdot v\,, \end{aligned}$$

so dass folgendes gilt:

M1: $(M, +)$ *ist eine abelsche Gruppe. Ihr neutrales Element 0 heißt "Nullvektor", das zu einem $v \in M$ inverse Element $-v$ heißt der zu v negative "Vektor".*

M2: *(a)* $(\lambda + \mu) \cdot v = (\lambda \cdot v) + (\mu \cdot v)$,

(b) $\lambda \cdot (v + w) = (\lambda \cdot v) + (\lambda \cdot w)$,

(c) $(\lambda \cdot \mu) \cdot v = \lambda \cdot (\mu \cdot v)$,

(d) $1 \cdot v = v$

Falls es nicht darauf ankommt, oder wenn es aus dem Kontext heraus klar ist, welche Addition und Multiplikation mit Skalaren eine Menge M zu einem Modul machen, so schreibt man auch kurz M statt $(M, +, \cdot)$.

Statt $\lambda \cdot v$ mit $\lambda \in R$, $v \in M$ schreibt man auch nur λv.

Nach einer üblichen Konvention sollen die Addition in M und die Addition in R weniger stark binden als die Multiplikation mit Skalaren. Das erspart viele Klammern.

Aus den Axiomen kann man leicht einige weitere oft verwendete Rechenregeln ableiten.

Bemerkung. M sei ein R-Modul. Dann gilt:

1. (a) $0 \cdot v = 0$ für alle $v \in M$ und $\lambda \cdot 0 = 0$ für alle $\lambda \in R$.

   (b) $\lambda \cdot v = 0$ für ein $\lambda \in R$ und ein $v \in M \quad \Longrightarrow \quad \lambda \notin G(R)$ oder $v = 0$.

2. $(-1) \cdot v = -v$ für alle $v \in M$.

3. M2 (c) und (d) für endlich viele Elemente aus R bzw. M.

Vergleiche mit [Fi, Bemerkung 1.4.1]!

I. Allg. schreiben wir die Skalare links entsprechend obiger Definition. Da R ein kommutativer Ring ist, kann man, ohne in Schwierigkeiten zu kommen, festlegen: $v\lambda := \lambda v$ für $\lambda \in R$ und $v \in M$. Es gelten dann automatisch die zu M1 und M2 analogen Regeln. Dies ist manchmal beim Rechnen mit Matrizen bequem.

Als **Beipiel** eines R-Moduls sei hier nur $\boldsymbol{R^n}$ erwähnt, $n \in \mathbb{N}_+$. Zahlreiche weitere Beispiele folgen später.

Definition 1.9. *Eine Teilmenge U eines R-Moduls M heißt* **Untermodul** *von M bzw. R-Untermodul von M, wenn gilt*

(UM1) $U \neq \varnothing$.

(UM2) *Für alle $v, w \in U$ ist $v + w \in U$.*

(UM3) *Für alle $v \in U$, $\lambda \in R$ ist $\lambda v \in U$.*

Beobachtung. Ein Untermodul des Moduls M ist selbst Modul bzgl. der in M vorliegenden Verknüpfungen.

Beispiel. $\mathbb{Z}^n$ und $U = \{v \in \mathbb{Z}^n$ mit geraden Einträgen$\}$.

Definition 1.10. *Die Menge der* **Torsionselemente** *von M ist $t(M) := \{v \in M :$ Es gibt ein $r \in R\backslash\{0\}$ mit $rv = 0\}$.*

Satz 1.11. *Sei R nullteilerfrei und M ein R-Modul. Dann ist $t(M)$ ein Untermodul von M.*

Definition 1.12. *Seien M, N R-Moduln und $F : M \longrightarrow N$ eine Abbildung. F heißt* **($\boldsymbol{R}$−)linear** *oder* **Modul***(-homo-)***morphismus**, *wenn gilt:*

(LA1) *Für alle $v, w \in M$ ist $F(v + w) = F(v) + F(w)$.*

(LA2) *Für alle $v \in M$, $\lambda \in R$ ist $F(\lambda v) = \lambda F(v)$.*

Beispiel. $M = \mathbb{Z}$, $\mathbb{N} = \mathbb{Z}_2$ und G wie in der Einleitung.

(C) Unterringe, Ideale, Hauptideale, Hauptidealringe

Definition 1.13. *Eine Teilmenge M des Ringes R heißt* **Unterring von $\boldsymbol{R}$**, *wenn gilt:*

(a) $1 \in M$

(b) Für alle $r, s \in M$ ist $r + s \in M$.

(c) Für alle $r, s \in M$ ist $rs \in M$.

(d) Für alle $r \in M$ ist $-r \in M$.

Insbesondere ist dann wegen (b) auch $\mathbf{0 \in M}$.

Sei jetzt M eine **nichtleere** Teilmenge von R. M heißt **Linksideal von R**, wenn (b) gilt und außerdem noch

(L) Für alle $\boldsymbol{r \in R}$ und alle $s \in M$ ist $rs \in M$.

M heißt **Rechtsideal** von R, wenn (b) gilt und außerdem noch

(R) Für alle $r \in M$ und $\boldsymbol{s \in R}$ ist $rs \in M$.

M heißt (zweiseitiges) **Ideal** von R, wenn (b), (L) und (R) gilt.

Sprechweisen. Ist M ein Unterring von R, so wird R manchmal auch Oberring von M oder Ring-**Erweiterung von $\boldsymbol{M}$** genannt.

Bemerkungen.

(a) Ist R kommutativ, dann ist jedes Links-Ideal und jedes Rechtsideal ein Ideal.

(b) Man überlegt sich leicht, dass ein Unterring von R ein Ring ist bezüglich der Addition und Multiplikation von R. Dies trifft für (Links-, Rechts-) Ideale J nicht zu, da i.A. $1 \notin J$. Wegen (L) oder (R) gilt ja sogar:

$$1 \in J \quad \Longleftrightarrow \quad J = R\,.$$

Alle Rechenregeln, die sich nicht auf 1_R beziehen, gelten allerdings auch in (Links-, Rechts-) Idealen. Insbesondere sind (Links-, Rechts-) Ideale Untergruppen von R bzgl. $+$.

(c) Man vergleiche die Definition von "Linksideal" mit der eines Untermoduls in (B): Die Linksideale eines Ringes R sind genau die R-Untermoduln von R.

Beispiele.

(a) In der Vorlesung konkrete Beispiele u. A. in den Fällen: $K =$ Körper, $R = \mathbb{Z}$, $R = \mathrm{Abb}(M, R)$, $R = K^{n\times n}$.

(b) Ein Rechtsideal, das $a \in R$ enthält, enthält auch $aR = \{ar \mid r \in R\}$. Da aR selbst schon Rechtsideal ist, ist aR das **"kleinste" Rechtsideal, das $\boldsymbol{a}$** enthält. Insbesondere für $a = 0$ ist $\{0\}$ ein Rechtsideal. Entsprechendes gilt für das Linksideal Ra.

(c) Ein Ideal, das $a \in R$ enthält, enthält auch

$$J(a) := \left\{ \sum_{i=1}^{n} r_i a s_i \mid n \in \mathbb{N}_+,\ r_i, s_i \in R \right\}.$$

Da $J(a)$ selbst schon Ideal ist, ist $J(a)$ das **kleinste Ideal, das $\boldsymbol{a}$ enthält**. $J(a)$ wird oft auch **das von $\boldsymbol{a}$ erzeugte Ideal** genannt.

(d) Verallgemeinerung von (c): das von $a_1, \ldots, a_n \in R$ erzeugte Ideal $J(a_1, \ldots, a_n)$, bzw. das von $\varnothing \neq M \subset R$ erzeugte Ideal $J(M)$.

Satz 1.14.

(a) Durchschnitt $J_1 \cap J_2$ und Summe $J_1 + J_2 = \{r+s \mid r \in J_1,\ s \in J_2\}$ von (Rechts-/Links-) Idealen J_1, J_2 eines Ringes sind wieder (Rechts-/Links-) Ideale.

(b) Der Durchschnitt $R_1 \cap R_2$ von Unterringen eines Ringes ist wieder ein Unterring.

Definition 1.15. *Sei R ein Ring und $a \in R$. Dann wird aR* **Rechts-Hauptideal** *und Ra* **Links-Haupideal** *genannt. Ist R kommutativ, spricht man von* **Hauptidealen**. *a heißt* **Erzeuger** *von aR bzw. Ra.*

Ein Ring heißt **Rechts-** *(bzw.* **Links-***)* **Hauptidealring**, *wenn jedes Rechts- (bzw. jedes Links-) Ideal ein Rechts- (bzw. Links-) Hauptideal ist. Ist R kommutativ, kann man den Zusatz "Rechts" oder "Links" weglassen.*

Bemerkung. Die meisten und die wichtigsten der in dieser Vorlesung auftretenden Ringe sind kommutative Hauptidealringe (Abschnitte 2-4) oder sie sind zugleich Rechts- und Links-Hauptidealringe. Zu letzterem siehe Abschnitt 5.

Im kommutativen Fall kann man wohl ohne Übertreibung noch sagen, dass alle praktisch wichtigen Hauptidealringe zusätzlich noch "euklidisch" sind, siehe Abschnitt 4. Letztere Bemerkung ließe sich auch auf den nicht kommutativen Fall ausweiten.

Satz 1.16. *Sei R ein Bereich und seien $a, b \in R$. Es gilt:*

$$aR = bR \Longleftrightarrow a \underset{r}{\sim} b \quad \text{und} \quad Ra = Rb \Longleftrightarrow a \underset{\ell}{\sim} b\,.$$

(D) Vielfache und Teiler, kglV, ggrT, Bézout-Identität

Folgende Definitionen verallgemeinern die Begriffe Vielfache, Teiler, "ggT" und "kgV".

Definition 1.17. *Sei R ein Ring und seien $a, b, k, g \in R$.*

(a) Sei $t = ab$, dann heißt

(i) t **Linksvielfaches** *von b und* **Rechtsvielfaches** *von a.*

(ii) a **Linksteiler** *von t, kurz $a|_\ell\, t$.*
b **Rechtsteiler** *von t, kurz $b|_r\, t$.*

(b) k ist **ein gemeinsames Linksvielfaches** *(glV) von a and b, wenn gilt:*

(i) $a|_r\, k$ und $b|_r\, k$

k ist **ein kleinstes** *gemeinsames Linksvielfaches (kglV) von a and b, wenn außerdem gilt:*

(ii) Gilt für ein $t \in R : a|_r\, t$ und $b|_r\, t$ dann gilt auch $k|_r\, t$.

(c) g ist **ein gemeinsamer Rechtsteiler** *(grT) von a und b, wenn gilt:*

(i) $g|_r\, a$ und $g|_r\, b$

g ist **ein größter** *gemeinsamer Rechtsteiler (ggrT) von a und b, wenn außerdem noch gilt:*

(ii) Gilt für ein $t \in R : t|_r\, a$ und $t|_r\, b$ dann gilt auch $t|_r\, g$.

(d) Die Definitionen lassen sich mühelos auch für mehr als 2 Ringelemente formulieren.

Analog wird "kgrV" und "gglT" definiert. **Ist R kommutativ, können die Attribute "r", "l" wegfallen (ggT, kgV).**

Der folgende elementare Satz ist unter strukturellen Gesichtspunkten interessant, siehe jedoch Bemerkung nach Satz 1.19. Auf jeden Fall bietet er eine gute Übungsmöglichkeit in abstrakter **linearer**(!) Algebra: Es geht um Summe und Durchschnitt spezieller Untermoduln von R.

Satz 1.18 (rechts). *Sei R ein Ring und seien $a, b \in R$.*

(a) $aR \cap bR \neq \{0\}$ genau dann, wenn a und b ein gemeinsames Rechtsvielfaches $\neq 0$ besitzen.

(b) Es gibt $k \in R$ mit $aR \cap bR = kR$ genau dann, wenn a und b ein kgrV besitzen.

(c) Mit einem $g \in R$ gilt $aR + bR \subset gR$ ganau dann, wenn g ein glT von a und b ist. Gibt es ein $g \in R$ mit $aR + bR = gR$, dann ist g ein ggT von a und b und es gibt $a', b' \in R$ mit

$$aa' + bb' = g \quad \textbf{Bézout-Identität} \tag{1}$$

(d) Analoge Aussagen sind für mehr als 2 Ringelemente möglich.

Bemerkung. Eine Bézout-Identität für g ist nichts anderes als eine Darstellung (1) von g als Linearkombination von a und b. Wenn R nicht kommutativ ist, dann ist es allerdings nicht gleichgültig, auf welcher Seite die Koeffizienten a', b' der Linearkombination stehen.

Satz 1.18 (links). *analog*

Eine unmittelbare Folgerung ist:

Satz 1.19. *Sei R ein Rechtshauptidealring, dann existiert zu vorgegebenen $a, b \in R$ stets ein kgrV und ein gglT.*

Ist g ein gglT von a und b, dann gibt es $a', b' \in R$, so dass (1) gilt.

Die letzte Aussage ist das sogenannte **Lemma von Bézout**. *Satz 1.19 ist "rechts-links symmetrisch".*

Bemerkung. Satz 1.19 zeigt, dass der Begriff "Hauptidealring" theoretisch sehr bequem ist. Kann man für einen Ring R nachweisen, dass er etwa Rechtshauptidealring ist, dann ist, wie der Beweis von Satz 1.18 zeigt, durch einfach idealtheoretische Überlegungen gesichert, dass ein gglT und ein kgrV für alle $a, b \in R$ existiert und dass (1) gilt. Dadurch ist aber nichts darüber ausgesagt, ob zu vorgegebenen a, b ein kgrV bzw. gglT und die Koeffizienten a', b' in (1) tatsächlich in endlich vielen Schritten gefunden werden können! Kurz: Die Sätze 1.18 und 1.19 sind nicht konstruktiv. Ringe bei denen ein Algorithmus bekannt ist, zur Berechnung eines ggrT bzw. kglV sind daher von besonderem Interesse. Im kommutativen Fall gehören dazu euklidische Ringe (Abschnitt 4) im nicht kommutativen Fall ist $K^{n\times n}$ (K geeigneter Körper) ein leicht zugängliches Beispiel (Abschnitt 5). Weitere Beispiele können Ihnen im weiteren Verlauf des Studiums begegnen. Es wird sich zeigen, dass die uns interessierenden Ringe alle auch (Rechts- und Links-) Hauptidealringe sind. Die Sätze 1.18 und 1.19 sind aber dann insofern überflüssig, als alle Existenzprobleme sich durch die explizite Möglichkeit der Berechnung in endlich vielen Schritten natürlich von selbst erledigen. Zur **Eindeutigkeit** von gglT und kgrV macht Satz 1.16 in Verbindung mit Satz 1.18 eine Aussage (!). Siehe auch Satz 5.4.

(E) Ringmorphismen, Kern, Bild, Charakteristik, Teil des Homomorphiesatzes

Definition 1.20. *Seien R und S Ringe und $f : R \longrightarrow S$ eine Abbildung. f heißt Ring-*__Morphismus__ *(oft auch nur Morphismus oder* __Homomorphismus__*, wenn klar ist, dass von Ringen die Rede ist), wenn gilt*

(a) $f(1_R) = 1_S$

(b) Für alle $r, s \in R$ *gilt:* $f(r + s) = f(r) + f(s)$

(c) Für alle $r, s \in R$ *gilt:* $f(rs) = f(r)f(s)$

Ein injektiver Ringmorphismus wird manchmal auch **Einbettung**, *ein bijektiver* **Isomorphismus** *genannt. Die Schreibweise* $\boldsymbol{R \cong S}$ *bedeutet: Es gibt einen Isomorphismus $f : R \longrightarrow S$. (b) und (c) lassen sich durch vollständige Induktion auf endlich viele Argumente ausdehnen.*

Satz 1.21. *Seien R, S Ringe und sei $f : R \longrightarrow S$ ein Ringmorphismus.*

(i) $\operatorname{Kern} f := \{r \in R \mid f(r) = 0_S\} = f^{-1}(\{0_s\})$ *ist ein zweiseitiges Ideal. Insbesondere gilt:* $f(0_R) = 0_S$ *und für alle* $r \in R : f(-r) = -f(r)$

(ii) $\text{Bild}\, f = \{s \in S \mid$ *Es gibt ein* $r \in R$ *mit* $f(r) = s\} = f(R)$ *ist ein Unterring von* S.

(iii) $f(G(R))$ *ist eine Untergruppe von* $G(S)$ *und es gilt* $f(r)^{-1} = f(r^{-1})$ *für* $r \in G(R)$.

(iv) f *injektiv* $\Longleftrightarrow \text{Kern}\, f = \{0\}$

(v) f *bijektiv* $\Longrightarrow$ *Umkehrabbildung bijektiver Morphismus*

Bemerkung. Satz 1.21 besagt u. A. dass die Möglichkeiten, einen Ring R "strukturverträglich" abzubilden "begrenzt" sind durch den "Vorrat" an Idealen in R. Weiter unten in Satz 1.23 wird sich zeigen, dass es einen noch viel engeren Zusammenhang zwischen den Idealen von R, den von R ausgehenden Ringmorphismen und den dabei entstehenden homomorphen Bildern des Ringes R gibt.

Ist R ein Körper ($\{0\}$ und K sind dann die einzigen Ideale), S ein Ring und $f : K \longrightarrow S$ ein Ringmorphismus, so ist wegen Satz 1.21 entweder f die Nullabbildung oder f injektiv. Im letzteren Falle ist der Unterring $f(K)$ von S ein zu K isomorpher Körper. Ähnliches lässt sich erstaunlicherweise auch für den Ring $K^{n\times n}$ sagen, da dieser ebenfalls nur die Ideale $\{0\}$ und $K^{n\times n}$ besitzt (siehe Abschnitt 5).

Beispiel. Sei R ein Ring. Die Abbildung $\pi_R : \mathbb{Z} \longrightarrow R$ mit

$$\pi_R(z) = \left\{ \begin{array}{ll} z \cdot 1_R := \overbrace{1_R + \ldots + 1_R}^{z\text{-mal}} & \text{falls } z > 0 \\ 0 & \text{falls } z = 0 \\ -((-z) \cdot 1) & \text{falls } z < 0 \end{array} \right\}$$

ist ein Ring-Morphismus. Wie Kern und Bild von $\pi_R(\mathbb{Z})$ aussehen können, wird sich in Abschnitt 2 ergeben. $\pi_R(\mathbb{Z})$ ist der kleinste Unterring von R und wird häufig (irreführenderweise) Primring von R genannt.

Definition 1.22. *Die* **Charakteristik eines Ringes** R, $\text{Char}(R)$, *ist definiert als*

$$\text{Char}(R) = \left\{ \begin{array}{ll} 0 & \textit{wenn } |\pi_R(\mathbb{Z})| = \infty \\ |\pi_R(\mathbb{Z})| & \textit{sonst} \end{array} \right\}$$

Ist $f : R \longrightarrow S$ *ein Ringmorphismus, dann ist* $f(1_R) = 1_S$ *nach Definition 1.20 und daher gilt* $f(z \cdot z_R) = z \cdot 1_S$ *für* $z \in \mathbb{Z}$ *und* $f(\pi_R(\mathbb{Z})) = f(\pi_S(\mathbb{Z}))$. *Definiert man für beliebige* $r \in R$, $s \in S$, $z \in \mathbb{Z}$ *ausgehend von obigem Beispiel* $zr = \pi_R(z)r$ *und* $zs = \pi_s(z)s$, *dann erhält man:* $f(zr) = z \cdot f(r)$. **Ringmorphismen sind demnach automatisch "$\mathbb{Z}$-linear"**. *Dies ist besonders interessant, wenn* $R = \mathbb{Z}$ *(siehe Abschnitt 2).*

Satz 1.23 (Teil des Homomorphiesatzes). *Seien* R, S, T *Ringe und* $f : R \longrightarrow S$, $g : R \longrightarrow T$ *Ringmorphismen. Dann gilt:*

$$\text{Ker}\, f = \text{Ker}\, g \Longrightarrow f(R) \cong g(R)\,.$$

(F) Kongruenzen

Definition 1.24. *Sei R ein Ring und M eine nichtleere Teilmenge und seien $r, s \in R$. Wir sagen* $\boldsymbol{r}$ **kongruent zu** $\boldsymbol{s}$ **modulo** $\boldsymbol{M}$*, wenn gilt $r - s \in M$.*

Schreibweise. $\boldsymbol{r \equiv s \mod M}$ oder nur $\boldsymbol{r \equiv s}$ wenn klar ist, welche Menge M gemeint ist.

Kongruenzen treten in der Vorlesung eher am Rande auf, z. B. in Kapitel II. Sie spielen jedoch nicht nur in der Algebra eine wichtige Rolle. Der folgende Satz dient mehr als Angebot zum Kennenlernen.

Satz 1.25. *Seien R, M wie in Definition 1.24. Dann gelten:*

(i) *Für alle $m \in M$ ist $m \equiv 0$ und $0 \equiv -m$*

(ii) *$\equiv$ reflexiv $\iff 0 \in M$*

(iii) *$\equiv$ symmetrisch $\iff$ Für alle $m \in M$ ist auch $-m \in M$*

(iv) *$\equiv$ transitiv $\iff$ Für alle $m_1, m_2 \in M$ ist $m_1 + m_2 \in M$*
$\iff$ [Für alle $r, s, r', s' \in R$ gilt: [$r \equiv r'$ und $s \equiv s'$] $\Longrightarrow r + s \equiv r' + s'$]

(v) *$\equiv$ Äquivalenzrelation $\iff M$ Untergruppe der additiven Gruppe R*

(vi) *[Für alle $r, s \in R$, $\lambda \in R$ gilt: $r \equiv s \Longrightarrow \lambda r \equiv \lambda s$]*
$\iff$ [Für alle $m \in M$, $\lambda \in R$ ist $\lambda m \in M$]

(vii) *wie (vi), aber λ von recht multipliziert*

(viii) *[Für alle $r, s, r', s' \in R$ gilt: [$r \equiv s$ und $r' \equiv s'$] $\Longrightarrow rr' \equiv ss'$]*
$\iff M$ ist Ideal

(ix) *Sei $r \in R$. Dann ist $\{s \in R \mid s \equiv r\} = r + M$ und $\{s \in R \mid r \equiv s\} = r - M$.*

Bemerkung. Am wichtigsten ist der Fall, wo $\equiv$ zumindest eine Äquivalenzrelation ist bzw. (wegen (v)) M eine additive Untergruppe von R ist. Die Teilmengen in (ix) fallen dann zusammen, werden Kongruenzklasse genannt und R ist disjunkte Vereinigung solcher Klassen.

Ist M ein Ideal, gelten alle in (ii) bis (vii) auftretenden Einzelaussagen.

(G) Vertretersysteme

Definition 1.26. *Seien M eine nichtleere Menge, $\sim$ eine Äquivalenzrelation auf M und $M/_\sim$ die Menge der Äquivalenzklassen bzgl. $\sim$. Eine Teilmenge $\boldsymbol{\mathcal{V}} \subseteq M$ heißt Vertretersystem (für die Äquivalenzklassen) bzgl. $\sim$, wenn für alle $K \in M/_\sim$ gilt: $K \cap \boldsymbol{\mathcal{V}}$ besteht aus genau einem Element.*

(H) Effektivität oder Berechenbarkeit

Für konkrete Anwendungen bis hin zum Ausrechnen eines Ergebnisses auf einem Computer ist es selbstverständlich notwendig, dass alle in die Berechnung eingehenden Größen auf einem Computer darstellbar und vergleichbar sind und die notwendigen Operationen durch Algorithmen realisiert werden können.

Definition 1.27. *Eine Abbildung $f : M \longrightarrow N$ heißt* **effektiv** *oder* **berechenbar**, *wenn*

(i) die Elemente von M und N in einem Computer dargestellt werden können und die Gleichheit zweier Elemente durch einen Algorithmus festgestellt werden kann.

(ii) es einen Algorithmus gibt, der zu $m \in M$ den Abbildungswert $f(m)$ berechnet.

Definition 1.28. *Eine algebraische Struktur (z. B. Ring, Gruppe, Vektorraum, Modul) heißt effektiv oder berechenbar, wenn ihre Verknüpfungen und die in den Axiomen auftretenden Forderungen effektiv sind. Bei einer Gruppe G bedeutet dies z. B., dass neben der Verknüpfungen auch die Abbildung $g \longmapsto g^{-1}$ für $g \in G$ effektiv sein muss.*

Die hier getroffene Definition von effektiv oder berechenbar liegt ungefähr zwischen der von "effective" in [CoCuSt, S. 1] und der von "computable" in [BeWe, S. 78].

In der Vorlesung wird bei mehreren Gelegenheiten die Berechenbarkeit der erreichten Ergebnisse thematisiert.

2 $\mathbb{Z}$ und die Ringe $\mathbb{Z}_d$

Zunächst geht es um Division mit Rest und die dabei entstehenden Restabbildungen. Danach werden die Restringe $\mathbb{Z}_d$ konstruiert und Morphismen $\varrho_d : \mathbb{Z} \longrightarrow \mathbb{Z}_d$; jedes Ideal $\neq \{0\}$ kommt als Kern eines ϱ_d vor (Satz 2.4). Als Anwendung erreichen wir eine konkrete Beschreibung der homomorphen Bilder von $\mathbb{Z}$.

Grundlegend ist dabei der folgende

Satz 2.1 (Division mit Rest). *Für alle $p, q \in \mathbb{Z}$ mit $q \neq 0$ gibt es* **genau** *ein Paar $(r, s) \in \mathbb{Z}^2$ mit*

$$p = sq + r \quad \textit{und} \quad 0 \leq r < |q|$$

r heißt (nichtnegativer) **Rest** *bei Division durch q.*

Anschaulich ist sofort klar, dass jede ganze Zahl in genau einem Intervall der Form $[\alpha q, (\alpha + 1)q)$ liegt.

Beweis von Satz 2.1 durch vollständige Induktion, wie z. B. auch in [La1, S. 12].

Bemerkung. Fast alle Eigenschaften von $\mathbb{Z}$, die wir benötigen, beruhen auf Satz 2.1 und werden in etwas abstrakterer Form in Abschnitt 4 gleich für die ganze Klasse derjenigen Ringe hergeleitet werden, bei denen "Division mit Rest" möglich ist. Auch der folgende Satz wird dort in etwas verallgemeinerter Form nochmals auftreten.

Satz 2.2. *$\mathbb{Z}$ ist ein Hauptidealring. Die Menge der Ideale von $\mathbb{Z}$ ist $\{d\mathbb{Z} : d \in \mathbb{N}\}$. Dies ist auch die Menge der $\mathbb{Z}$-Untermoduln von $\mathbb{Z}$.*

Die Restabbildungen von $\mathbb{Z}$. Sei $q \in \mathbb{Z}\backslash\{0\}$ und $d = |q|$. Sei weiter $\varrho_q : \mathbb{Z} \longrightarrow \mathbb{Z}_d := \{0, \ldots, d-1\} \subset \mathbb{Z}$ gegeben durch $\varrho_q(z) :=$ nichtnegativer Rest bei Division von z durch q. Wegen Satz 2.1 ist ϱ_q sinnvoll definiert und es gilt:

Satz 2.3.

(a) $\varrho_q = \varrho_d$. *Es genügt daher den Fall $q = d > 0$ zu betrachten.*

(b) $\varrho_d(z + \lambda d) = \varrho_d(z)$ *für alle $z, \lambda \in \mathbb{Z}$.*

(c) ϱ_d *ist surjektiv und es gilt $\varrho_d \circ \varrho_d = \varrho_d$.*

(d) Für alle $z, z' \in \mathbb{Z}$ gilt: $\varrho_d(z + z') = \varrho_d(\varrho_d(z) + \varrho_d(z'))$

(e) Für alle $z, z' \in \mathbb{Z}$ gilt: $\varrho_d(z \cdot z') = \varrho_d(\varrho_d(z) \cdot \varrho_d(z'))$

Satz 2.3 motiviert die Festlegung folgender **Verknüpfungen auf $\mathbb{Z}_d$**. Für alle $a, b \in \mathbb{Z}_d$:

$$a \oplus b := \varrho_d(a + b)\,, \quad a \odot b := \varrho_d(ab)$$

Satz 2.4. *Mit den eben eingeführten Verknüpfungen $\oplus$ und $\odot$ ist $\mathbb{Z}_d$ – genauer: $(\mathbb{Z}_d, \oplus, \odot)$ – ein kommutativer Ring und ϱ_d ein surjektiver Ringmorphismus mit* $\operatorname{Ker} \varrho_d = d\mathbb{Z}$. *Die Anzahl der Elemente des Ringes $\mathbb{Z}_d$ ist d. Es gilt $\mathbb{Z}_d \cong \mathbb{Z}_{d'}$ nur wenn $d = d'$, bzw. wenn $\mathbb{Z}_d = \mathbb{Z}_{d'}$. Außerdem ist ϱ_d $\mathbb{Z}$-linear (vgl. 1.22).*

Die Verbindung von Satz 2.2 und Satz 2.4 mit Satz 1.23 führt uns auf folgende konkrete **Beschreibung der homomorphen Bilder von $\mathbb{Z}$**:

Satz 2.5. *Sei R ein Ring und $f : \mathbb{Z} \longrightarrow R$ ein Ringmorphismus. Entweder ist f injektiv und somit $\mathbb{Z}$ in R eingebettet ($\mathbb{Z} \cong f(\mathbb{Z})$) oder $f(\mathbb{Z})$ ist isomorph zu einem der natürlichen Restringe $\mathbb{Z}_d$, die daher als "Modelle" für die homomorphen Bilder von $\mathbb{Z}$ dienen können.*

Wenn man schon weiß, was eine Primzahl ist, lässt sich leicht zeigen:

Satz 2.6. *$\mathbb{Z}_d$ ist genau dann ein Körper, wenn d eine Primzahl ist.*

Definition und einige Eigenschaften des Begriffes "prim" folgen erst später in Abschnitt 4. Da es unendlich viele Primzahlen gibt, sind unter den homomorphen Bildern von $\mathbb{Z}$ unendlich viele paarweise nicht isomorphe endliche Körper.

3 Polynome

In diesem Abschnitt werden folgende Themen behandelt: Konstruktion von $R[x]$, Division mit Rest, Konstruktion der Restringe $R[x]_d$ analog zu Abschnitt 2, Einsetzungsmorphismen, Nullstellen, Abspaltung von linearen Faktoren, konkrete Beschreibung der homomorphen Bilder von $K[x]$. **Dabei ist R stets ein kommutativer Ring.**

(A) Konstruktion von Polynomen

Polynome traten bereits in der Linearen Algebra I auf (charakteristische Polynome). Dort wurde aber nicht genau gesagt, was ein Polynom sein soll. Dies wird jetzt nachgeholt.

Definition 3.1. *$f \in \mathrm{Abb}(R, R)$ heißt* **Polynomfunktion**, *wenn es $n \in \mathbb{N}$ und $a_0, \ldots, a_n \in R$ gibt, so dass für alle $t \in R$ gilt:*

$$f(t) = a_n t^n + \ldots + a_1 t + a_0$$

$a_0, \ldots, a_n$ heißen **Koeffizienten** *der Polynomfunktion f.*

Beispiele.

1. Sei R ein endlicher Körper, als Beispiel nehmen wir den Körper $\mathbb{Z}_3$ der Reste bei Division durch 3. In diesem Körper betrachten wir die durch

   $$f(t) = t^3 + 2t + 1 \quad \text{für } t \in \mathbb{Z}_3$$

   gegebene Funktion $f : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$. Eine Wertetabelle lässt sich leicht ausrechnen. Es ist $f(0) = 1$ und $f(1) = 1$ und $f(2) = 1$, also $f = g$ für die durch

   $$g(t) = 1 \quad \text{für } t \in \mathbb{Z}_3$$

   gegebene Funktion $g : \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3$. Hier sehen wir, dass dieselbe Funktion sich durch verschiedene Koeffizientenfolgen darstellen lässt.

2. Sei $R = \mathbb{R}$. In der Analysis wird i. A. gezeigt, dass zwei reelle Polynomfunktionen nur dann für alle t dieselben Funktionswerte liefern, wenn sie dieselben Koeffizienten haben.

Bemerkung. Die in Beispiel 2 vorliegende Eindeutigkeit der Koeffizienten einer Polynomfunktion lässt sich für eine große Klasse von Ringen nachweisen (s. u. Satz 3.15) aber z. B. eben nicht für endliche Körper (Beispiel 1).

Diesen eventuellen Mehrdeutigkeiten kann aus dem Wege gegangen werden, indem die Koeffizientenfolgen an Stelle der Polynomfunktionen in den Vordergrund gestellt werden.

Sei $\boldsymbol{K} = \{(a_0, a_1, \ldots, a_n, 0, \ldots) : \ n \in \mathbb{N},\ a_i \in R\}$ und $PF_R := \{f \in \mathrm{Abb}(R, R) : f \text{ Polynomfunktion}\}$. Es liegt dann eine surjektive Abbildung $\varphi : \boldsymbol{K} \longrightarrow PF_R$ vor mit $\varphi(k) =$ Polynomfunktion mit Koeffizientenfolge k. PF_R ist ein Unterring von $\mathrm{Abb}(R, R)$. $\boldsymbol{K}$ wird zu einem Ring **gemacht** und zwar so, dass φ ein Ringmorphismus wird:

Addition in $\boldsymbol{K}$: komponentweise
Multiplikation (Faltung) in $\boldsymbol{K}$:

$$(a_0, \ldots, a_n, 0, \ldots,)(b_0, \ldots, b_m, 0, \ldots,) := (c_0, \ldots, c_{n+m}, 0, \ldots,)$$

mit $c_k = \sum\limits_{i+j=k} a_i b_j$ für $k \in \mathbb{N}$.

Man rechnet nach, dass $\boldsymbol{K}$ mit diesen Verknüpfungen ein kommutativer Ring wird. Das neutrale Element der Multiplikation ist $1 := (1, 0, \ldots)$. Die Abbildung mit der Vorschrift $a \longrightarrow a \cdot 1$ ist ein injektiver Ringmorphismus (Einbettung von R).

Sei $x = (0, 1, 0, \ldots)$. Dann ist $x^2 = (0, 0, 1, 0, 0, \ldots)$ und $x^3 = (0, 0, 0, 1, 0, \ldots)$ und mit vollständiger Induktion erhält man für $n \in \mathbb{N}$: $x^n = (0, \ldots, 0, 1, 0, \ldots)$ mit 1 an der $(n+1)$-ten Stelle.

Man setzt noch $x^0 := 1$ und erhält jetzt

$$(a_0, a_1, \ldots, a_n, 0, 0, \ldots) = a_0 x^0 + a_1 x^0 + \ldots + a_n x^n \,.$$

Dabei lässt man noch x^0 weg und hat somit die gewohnte Schreibweise für Polynome zurück, nur dass man es jetzt nicht mehr mit Funktionen zu tun hat. Konstruktionsbedingt gilt in $\boldsymbol{K}$:

$$\sum_{i=0}^{n} a_i x^i = 0 \Longleftrightarrow (a_0, \ldots, a_n, 0, \ldots) = 0 \Longleftrightarrow [a_0 = 0, a_1 = 0, \ldots, a_n = 0] \,.$$

M. a. W.: x kann nicht Nullstelle eines nichttrivialen Polynoms mit Koeffizienten aus R sein. Man nennt x eine **Unbestimmte** oder **transzendent** über R, $\boldsymbol{K}$ die Menge der (formalen) Polynome über R, und man schreibt $\boldsymbol{R[x]}$ an Stelle von $\boldsymbol{K}$.

Wie geplant, ist nun die oben eingeführte Abbildung $\varphi : R[x] \longrightarrow PF_R$ ein surjektiver Ringmorphismus. In der eben eingeführten Schreibweise ist

$$\left(\varphi\left(\sum_{i=0}^{n} a_i x^i\right)\right)(t) = \sum_{i=0}^{n} a_i t^i \quad \text{für alle } t \in R. \tag{1}$$

Für $R = \mathbb{R}$ (Beispiel 2) ist φ injektiv, also insgesamt ein Isomorphismus. Für $R = \mathbb{Z}_3$ (Beispiel 1) trifft dies nicht zu. Weiter unten werden weitere Ringe angegeben, bei denen φ ein Isomorphismus ist.

Definition 3.2. *Zu* $(a_0, \ldots, a_n, 0, \ldots) = \sum\limits_{i=0}^{n} a_i x^i =: p \in R[x]$ *mit* $a_n \neq 0$ *ist* **Grad von** $p := \deg p := n$. a_n *heißt* **höchster Koeffizient** *von* p. *Abkürzung:* $\boldsymbol{hK(p)}$. *Ist* $\deg p = 0, 1, 2$, *so heißt* p *konstant, linear, quadratisch. Für das* 0*-Polynom wird kein Grad festgesetzt.*

Satz 3.3.

(i) Für Polynome $p, q \in R[x]\backslash\{0\}$ mit $p+q \neq 0$ gilt: $\deg(p+q) \leq \max(\deg p, \deg q)$.

(ii) Für Polynome p, q aus $R[x]$ mit $pq \neq 0$ gilt: $\deg(pq) \leq \deg p + \deg q$. *Ist der höchste Koeffizient von p oder q kein Nullteiler so gilt $=$.*

(iii) $R[x]$ ist genau dann nullteilerfrei, wenn R dies ist.

(B) Division mit Rest

Der folgende Satz beschreibt die Division durch Polynome. Die Aussage ist ganz analog zur Division mit Rest bei den ganzen Zahlen. Ihr Beweis verläuft allerdings ganz anders.

Satz 3.4 (Division mit Rest für Polynome). *Es seien p, q Polynome aus $R[x]$, $q \neq 0$ und $hK(q) \in G(R)$. Dann gibt es Polynome $s, r \in R[x]$ mit*

$$p = sq + r \quad \textit{wobei} \quad r = 0 \textit{ oder } \deg r < \deg q\,. \tag{2}$$

Die Polynome s, r sind durch diese Bedingungen **eindeutig** *bestimmt.*

Beweis. Wir beweisen zuerst die Existenz von s und r.

Ist $p = 0$ oder $\deg p < \deg q$, so gilt

$$p = 0 \cdot q + p \quad \text{mit} \quad p = 0 \text{ oder } \deg p < \deg q\,. \tag{3}$$

Es existiert also eine Darstellung der gewünschten Art.

Für $p \neq 0$ und $\deg p \geq \deg q$ kommen wir mit vollständiger Induktion nach $n = \deg p$ zum Ziel. Wenn $n = 0$, dann ist $q = b_0 \in G(R)$, da $\deg p \geq \deg q$ gelten soll. Dann ist aber einfach $p = a_0 = sq + r$ mit $s = a_0 b_0^{-1}$ und $r = 0$. Nun nehmen wir an, dass für ein $n > 0$ jedes Polynom $p \neq 0$ mit $n > \deg p \geq \deg q$ eine Darstellung (2) besitzt. Nun seien

$$\begin{aligned} p &= a_n x^n + \ldots + a_n \\ q &= b_m x^m + \ldots + b_0 \quad \text{mit} \quad b_m \in G(R) \text{ und } n \geq m\,. \end{aligned}$$

Wir beseitigen nun den höchsten Koeffizienten von p mit dem Ansatz

$$\begin{aligned} p_1 &= p - a_n b_m^{-1} x^{n-m} q \\ &= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 - a_n x^n - \ldots\,. \end{aligned}$$

Wenn $p_1 = 0$, dann ist $p = sq + r$ mit $s = a_n b_m^{-1} x^{n-m}$ und $r = 0$. Wenn $p_1 \neq 0$, dann ist $\deg p_1 < n$. Nach Induktionsvoraussetzung oder nach (3) (falls $\deg p_1 < \deg q$) gibt es eine Darstellung

$$p_1 = s_1 q + r \quad \text{mit} \quad r = 0 \text{ oder } \deg r < \deg q$$

und man berechnet $p = a_n b_m^{-1} x^{n-m} q + p_1 = a_n b_m^{-1} x^{n-m} q + s_1 q + r$
$= (a_n b_m^{-1} x^{n-m} + s_1)\, q + r$ mit $r = 0$ oder $\deg r < \deg q$.

Wir müssen noch die Eindeutigkeit von s und r beweisen. Angenommen es ist

$$p_1 = s_1 q + r_1 = s_2 q + r_2$$

mit $r_1 = 0$ oder $\deg r_1 < \deg q$ und $r_2 = 0$ oder $\deg r_2 < \deg q$. Dann ist $(s_1 - s_2)q = r_2 - r_1$. Sei $r_2 \neq r_1$ und damit auch $s_2 \neq s_1$. Dann ist $\deg(r_2 - r_1) < \deg q$ und daher auch $\deg[(s_1 - s_2)q] < \deg q$. Das ist aber unmöglich nach Satz 3.3(ii). Also ist $s_1 = s_2$ und damit auch $r_1 = r_2$. □

Bemerkungen. (i) Der Beweis von Satz 3.4 zeigt uns einen algorithmischen Weg auf zur Berechnung von s und r in (2) bei gegebenem p, q. Dies lässt sich allerdings nur über solchen Koeffizientenringen R praktisch umsetzen in denen die Rechenoperationen in endlich vielen Schritten erledigt werden können. Siehe Abschnitt 1(H).

(ii) Ist in Satz 3.4 R ein Körper, so ist der höchste Koeffizient eines von 0 verschiedenen Polynoms stets eine Einheit, Division mit Rest "durch" ein $q \neq 0$ also uneingeschränkt möglich.

Satz 3.5. *Ist $R = K$ ein Körper, dann ist $K[x]$ ein Hauptidealring. Die Menge der Ideale in $K[x]$ ist $\{q \cdot K[x] : q = 0$ oder höchster Koeffizient von $q = 1\}$.*

(C) Die Restabbildungen von $R[x]$

Bemerkung. Ganz ähnlich wie im letzten Abschnitt; für den Ring $\mathbb{Z}$ lassen sich – wegen Satz 3.4, insbesondere wegen der Eindeutigkeit der Reste – auch für $R[x]$ mit Hilfe der Restabbildungen neue Ringe konstruieren als homomorphe Bilder von $R[x]$. Dies führt auf sogenannte (algebraische) Ringerweiterungen von R.

Anders als in Abschnitt 2, wo, ausgehend von dem unendlichen Ring $\mathbb{Z}$, sich eine ganze Klasse endlicher Ringe ergab, wird man ausgehend von $R[x]$ durch Übergang zu den Divisionsresten zu Ringen geführt, die "i. W." Unterringe uns schon bekannter Ringe sind. Näheres dazu am Ende dieses Abschnittes.

Sei $q \in R[x]\backslash\{0\}$, $d = \deg q$ und $\boldsymbol{hK(q) \in G(R)}$. Sei weiter $\varrho_q : R[x] \longrightarrow R[x]_d := \{p \in R[x] \mid \deg p < d$ oder $p = 0\}$ gegeben durch $\varrho_q(p) :=$ Rest bei Division von $p \in R[x]$ durch q. Wegen Satz 3.4 ist ϱ_q sinnvoll definiert, und es gilt:

Satz 3.6.

(a) Für alle $a \in G(R)$ ist $\varrho_q = \varrho_{aq}$. Es kann also o. E. vorausgesetzt werden, dass $hK(q) = 1$.

(b) ϱ_q ist surjektiv, und es gilt $\varrho_q \circ \varrho_q = \varrho_q$.

(c) Für alle $p, p' \in R[x]$ gilt:

$$\varrho_q(p + p') = \varrho_q(\varrho_q(p) + \varrho_q(p'))\,.$$

(d) Für alle $p, p' \in R[x]$ gilt:

$$\varrho_q(pp') = \varrho_q(\varrho_q(p)\varrho_q(p'))\,.$$

Obiger Satz motiviert die Festlegung folgender Verknüpfungen auf $R[x]_d$:

$$a \oplus b := \varrho_q(a+b) \stackrel{!}{=} a+b\,, \quad a \odot b = \varrho_q(ab)$$

für alle $a, b \in R[x]_d$.

Satz 3.7. *Mit den eingeführten von q abhängigen (!) Verknüpfungen ist $R[x]_d$ – genauer: $(R[x]_d, \oplus, \odot)$ – ein kommutativer Ring, der R als* **Unterring** *enthält. ϱ_q ist ein surjektiver Ringmorphismus mit* $\operatorname{Ker} \varrho_q = qR[x]$*. ϱ_q ist außerdem $R[x]$-linear, wenn man für $\lambda \in R[x]$ festlegt:*

$$\lambda\varrho_q(p) := \lambda \odot \varrho_q(p)$$

Um zu betonen, dass die Verknüpfungen auf $R[x]_d$ von q abhängen, schreiben wir auch $\boldsymbol{R[x]_{d,q}}$.

Bemerkung. Die Konstruktion des Ringes $R[x]_{d,q}$ verläuft nach dem gleichen Schema wie die Konstruktion des Ringes $\mathbb{Z}_d$ in Abschnitt 2. Da $R[x]_{d,q}$ den Ring R als Unterring enthält, ist $R[x]_{d,q}$ eine **Ringerweiterung** von R. $R[x]$ selbst ist natürlich auch ein Beispiel einer Ringerweiterung.

Die Verbindung von Satz 3.5 und Satz 3.13 mit unserer Version des Homomorphiesatzes (Satz 1.23) führt auf folgendes Ergebnis:

Satz 3.8. *Sei S ein Ring, K ein Körper, der zugleich Unterring von S ist, und $f : K[x] \longrightarrow S$ ein K-linearer Ringmorphismus. Entweder ist f injektiv und somit $K[x]$ in S eingebettet ($K[x] \cong f(K[x])$ oder $f(K[x])$ ist als K-Vektorraum und als Ring isomorph zu einem der natürlichen Restringe $K[x]_{d,q}$, die daher als "Modelle" für die homomorphen Bilder von $K[x]$ dienen können.*

Wenn man schon weiß, was ein Primpolynom ist, lässt sich leicht eine zu Satz 2.6 analoge Aussage herleiten:

Satz 3.9.

(i) $K[x]_{d,q}$ ist genau dann ein Körper, wenn q ein Primpolynom ist.

(ii) $K[x]_{d,q}$ ist ein $(\deg q)$-dimensionaler K-Vektorraum.

Beispiel. $K = \mathbb{Z}_2$, $q = x^2 + x + 1$, $\mathbb{F}_4 := K[x]_{2,q}$ ist ein Körper mit 4 Elementen.

Bemerkung. Interessant ist auch noch folgende Eigenschaft des Ringes $R[x]_d$ bzgl. q: Es gilt $\varrho_q(q) = 0$ bzw. $a_0 \oplus a_1 x \ldots \oplus a_n(x^d) = 0$. $\boldsymbol{x}$ **ist also eine Nullstelle von** $\boldsymbol{q}$ **in** $\boldsymbol{R' = R[x]_{d,q}}$ im Sinne der nachfolgenden Definitionen!

(D) Einsetzen in Polynome und Nullstellen

Definition und Beobachtung 3.10. *Sei R' ein nicht notwendig kommutativer Ring und R ein* **kommutativer** *Unterring von R'. Ein Element $\alpha \in R'$ mit der Eigenschaft*

$$\boxed{\alpha r = r\alpha \text{ für alle } r \in R}$$

heißt **einsetzbar** *(in ein Polynom aus $R[x]$). Ein $\alpha \in R$ ist stets einsetzbar, da R ja kommutativ ist.*

Die Abbildung $\pi_\alpha : R[x] \longrightarrow R'$ mit

$$\pi_\alpha \underbrace{\left(\sum_{i=0}^{n} a_i x^i\right)}_{=p} = \underbrace{\sum_{i=0}^{n} a_i \alpha^i}_{=:p(\alpha)}$$

*ist ein R-linearer Ringmorphismus (***Einsetzen von α / Einsetzungsmorphismus***).*

Das Bild von π_α wird oft mit $\boldsymbol{R[\alpha]}$ bezeichnet:

$$R[\alpha] := \pi_\alpha(R[x]) = \text{ Bild } \pi_\alpha$$

$R[\alpha]$ ist stets ein kommutativer (!) Unterring von R'!

Beachte. Falls $\alpha \in R$, dann ist $p(\alpha)$ nichts anderes als der Wert der zu p gehörigen Polynomfunktion an der Stelle α.

Beispiele.

(a) $R := \mathbb{Q}, R' := \mathbb{R}$. Für alle $\alpha \in \mathbb{R}$ und alle $q \in \mathbb{Q}$ gilt natürlich $\alpha q = q\alpha$. Für $p \in \mathbb{Q}[x]$ und $\alpha \in \mathbb{R}$ ist $p(\alpha)$ der Wert der Polynomfunktion p mit rationalen Koeffizienten an der reellen Stelle α.

(b) $R' := R^{n\times n}$, R kommutativer Ring. Wir können R als Unterring von R' auffassen, mit Hilfe der Einbettung

$$r \longrightarrow r \cdot E \quad \text{für alle} \quad r \in R\,.$$

Da für alle $A \in R'$ gilt: $(rE)A = rA = Ar = A(rE)$ kann im Sinne vorstehender Definition jedes $A \in R'$ in ein Polynom p aus $R[x]$ eingesetzt werden. Ist etwa $p(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$, so ist dann

$$\pi_A(p) = p(A) = \sum_{i=0}^{n} a_i A^i \in R'\,, \quad (A^0 := E)\,.$$

Ist speziell $R = K$ ein Körper, dann ist Bild $\pi_A = \pi_A(K[x]_d)$, denn wegen 3.5 ist $\operatorname{Ker} \pi_A = qK[x]$ mit einem $q \in K[x]$, und $d = \deg q$.

Definition 3.11. *Seien R, R' wie in der vorigen Definition. Ein einsetzbares Element $\alpha \in R'$ heißt* **Nullstelle aus $\boldsymbol{R'}$ von** *$p \in R[x]$, wenn gilt: $p(\alpha) = 0$. Nullstellen aus R von p nennen wir einfach* **Nullstellen**.

(E) Struktur von Polynomen, die Nullstellen besitzen

Satz 3.12. *Sei $\alpha \in R$ eine Nullstelle von $p \in R[x]$. Dann gibt es $s \in R[x]$, so dass $p = s \cdot (x - \alpha)$. Dabei ist s eindeutig bestimmt.*

Satz 3.13. *Sei R nullteilerfrei und $0 \neq p \in R[x]$. Dann hat entweder p keine Nullstelle (in R!) oder es gibt $r \in \mathbb{N}$ mit $r \geq 1, \alpha_1, \ldots, \alpha_r \in R$ und $\widetilde{p} \in R[x]$ ohne Nullstellen (alle eindeutig bestimmt), so dass gilt:*

$$p = \widetilde{p} \cdot (x - \alpha_1) \ldots (x - \alpha_r) \,.$$

Satz 3.14. *Sei R nullteilerfrei, dann hat jedes von 0 verschiedene Polynom p aus $R[x]$ höchstens* $\deg p$ *Nullstellen.*

Beispiel. $R = \mathbb{Z}_6$, $p(x) = (x-2)(x-3)$ hat 4 Nullstellen.

Nun können wir als Anwendung auch das Verhältnis zwischen Polynom und Polynomfunktion genauer beschreiben:

Satz 3.15 (Identitätssatz für Polynome). *Ist R nullteilerfrei und $|R|$ nicht endlich, dann sind die Koeffizienten der Polynomfunktionen eindeutig. M. a. W.: Dann ist die weiter oben (siehe* (1)*) betrachtete Abbdildung $\varphi : R[x] \longrightarrow PF_R$ ein Isomorphismus.*

Sucht man die Nullstellen eines nicht konstanten Polynoms $q \in R[x]$ mit $hK(q) = 1$ nicht nur in R, sondern auch in Ringerweiterungen R' von R, so findet man stets eine Nullstelle in $R[x]_{d,q}$ (siehe Bemerkung nach Satz 3.9), aber auch wie folgt:
Sei etwa $q = \sum_{i=0}^{d} a_i x^i$ mit $a_d = 1$, $A = \begin{bmatrix} 0 & \ldots & 0 & -a_0 \\ \vdots & \ddots & & \vdots \\ 0 & \ldots & 1 & -a_{d-1} \end{bmatrix}$ und $R' = R^{d \times d}$. Wie in (D) Beispiel (b) fassen wir R als Unterring von R' auf. Hier ist $\pi_A : R[x] \longrightarrow R^{d \times d}$ und $R[A] = \pi_A(R[x])$. A ist nun eine Nullstelle (aus R') von q, m. a. W. $q \in \operatorname{Ker} \pi_A$, denn es gilt sogar:

Satz 3.16. $\operatorname{Ker} \pi_A = q \cdot R[x]$.

Beispiel. $R = \mathbb{R}$, $q = x^2 + 1$, $A = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, $R[A]$ "=" $\mathbb{C}$.

Bemerkung. Auf Grund von Satz 1.23 ist $R[A] \approx R[x]_{d,q}$. Wir haben mit den Ringen $R[A]$ einen weiteren Typ von "Modellen" für homomorphe Bilder von $R[x]$ gefunden. Es ist vermutlich Geschmacksache, ob $R[x]_{d,q}$ oder $R[A]$ für übersichtlicher gehalten wird.

Das Einsetzen von Matrizen in Polynome und damit natürlich auch die Ringe $R[A]$ spielen in der linearen Algebra eine wichtige Rolle, siehe z. B. am Ende von Kapitel II.

4 Euklidische Ringe

Definition euklidischer Ringe, Division mit Rest, Zusammenhang mit Hauptidealringen und Zerlegung in Primelemente.

(A) Gemeinsame Verallgemeinerung von $\mathbb{Z}$ und $K[x]$

Die Beobachtung, dass Satz 4.2 sehr ähnlich ist zur Division mit Rest bei ganzen Zahlen, motiviert die weiter unten aufgeführte Definition euklidischer Ringe. Das Studium euklidischer Ringe ist für sich ein interessantes Teilgebiet der Algebra/Zahlentheorie. Für uns hat allerdings die Einführung dieses neuen Begriffes ganz pragmatische Gründe. Die für Anwendungen besonders wichtigen Ringe $\mathbb{Z}$ und $K[x]$, K ein Körper, sind beide Beispiele euklidischer Ringe. Da ein wichtiger Teil der noch folgenden Theorie sich mit demselben Aufwand und z. T. sogar durchsichtiger für euklidische Ring entwickeln lässt, ist eine beträchtliche Arbeitsersparnis möglich.

Definition 4.1. *Ein* **kommutativer** *Bereich heißt* **Ring mit Divisionsalgorithmus** *oder* **euklidischer Ring**, *wenn es eine Abbildung*

$$\delta : R\backslash\{0\} \longrightarrow \mathbb{N}$$

mit folgenden Eigenschaften gibt:

(i) *Für alle* $a, b \in R\backslash\{0\}$ *ist* $\delta(ab) \geq \delta(b)$.

(ii) *Für alle* $a, b \in R\backslash\{0\}$ *gilt:* $\delta(ab) = \delta(b) \iff a \in G(R)$.

(iii) *Für alle* $p, q \in R$ *mit* $q \neq 0$ *gibt es* $r, s \in R$ *mit* $p = sq + r$, *wobei* $r = 0$ *oder* $\delta(r) < \delta(q)$.

Auch hier heißt r *der* **Rest** *bei Division durch* q.

Beobachtung. Sei R ein euklidischer Ring und $d = \operatorname{Min} \delta(R\backslash\{0\})$ die kleinste Zahl im Bild von δ. Es gilt: $G(R) = \delta^{-1}(d)$.

Bemerkungen. (ii) folgt aus (i) und (iii). (i) wird nicht immer gefordert bei der Definition euklidischer Ringe; vergleiche z. B. [Koe]. Obige Definition ist angelehnt an [Lue2]. Fordert man nur (iii), so lässt sich zeigen, dass dann eine Abbildung $\delta' := R\backslash\{0\} \longrightarrow \mathbb{N}$ existiert, für die (i) bis (iii) gilt. (Siehe hierzu etwa [SchSt, Teil 2, S. 152]). Unsere oben getroffenen Definition ist also nur scheinbar spezieller. Der Beweis des nachfolgenden Satzes 4.4(a) wird unter Benutzung von (i) und (ii) wesentlich einfacher; insbesondere sind keine idealtheoretischen Überlegungen notwendig.

Beispiele.

(a) $R =$ Körper, $\delta(r) = 1$ für alle $r \in R\backslash\{0\}$.

(b) $R = \mathbb{Z}$ und $\delta = |\ |$.

(c) K ein Körper, $R = K[x]$, $\delta = \deg$.

(d) $R = \mathbb{Z}[i]$, $\delta(r) = r\overline{r}$.

Bemerkung. r und s in vorstehender Definition sind i. a. nicht eindeutig bestimmt. Z. B. ist im Falle des Beispiels (b) $7 = 2{\cdot}5{-}3 = 1{\cdot}5{+}2$. Erst die zusätzliche Forderung "nicht negativ" macht die Reste eindeutig. **Bei einem beliebigen euklidischen Ring ist daher die Konstruktion der Restringe wie in Abschnitt 2 oder 3 nicht ohne weiteres möglich**.

Um mit der Definition euklidischer Ringe vertraut zu machen, wird nun die folgende – für $\mathbb{Z}$ und $K[x]$ uns schon bekannte – Aussage bewiesen.

Satz 4.2. *Ein euklidischer Ring ist stets auch Hauptidealring.*

Beweis. Es handelt sich lediglich um eine "Übersetzung" des Beweises für $\mathbb{Z}$ oder $K[x]$. $\{0\}$ ist stets ein Hauptideal. Sei J ein Ideal $\neq \{0\}$ im euklidischen Ring R und sei $q \in J$, $q \neq 0$, ein Element bei dem δ eingeschränkt auf $J\backslash\{0\}$ den kleinsten Wert liefert. Für ein beliebiges $p \in J$ gibt es nun s und r aus R mit $p = sq + r$ und $\delta(r) < \delta(q)$ oder $r = 0$.

Da $p, q \in J$, ist $p - sq = r \in J$. Da $\delta(q)$ minimal, folgt $r = 0$. Alle Elemente von J sind also Vielfache von q. □

Bemerkung. Es hat Mühe gekostet bis man einen Hauptidealbereich entdeckt hat der nicht euklidsch ist. Beispiele sind in dem Buch von [SchSt, Teil 2, S. 157] angegeben.

Der Name "euklidisch" rührt daher, dass in einem euklidischen Ring der sogenannte **euklidische Algorithmus** zur Bestimmung eines ggT zur Verfügung steht. Siehe dazu Abschnitt 6. Dort wird ein Verfahren angegeben zur Bestimmung eines ggT, der Koeffizienten einer Bézout-Identität und eines kgV. Es wird erinnert an Satz 1.19 und die Bemerkungen danach.

(B) Zerlegung in Primelemente

Im weiteren Verlauf der Vorlesung wird ein paarmal die Zerlegung von Polynomen in Primpolynome eine Rolle spielen. **Zerlegung in Primelemente** ist über euklidischen Ringen nicht schwierig, sogar eher noch etwas durchsichtiger. Die folgenden Aussagen und Definitionen über euklidische Ringe wiederholen insbesondere Bekanntes (?) aus der Theorie ganzer Zahlen.

Definition 4.3. *Sei R ein kommutativer Ring.*

(a) Sind $a, b \in R$ und gilt $a|b$, dann sagen wir: a ist ein **echter** *Teiler von b, wenn a weder eine Einheit noch äquivalent zu b ist.*

(b) Sei $u \in R$ keine Einheit und $\neq 0$. u heißt **unzerlegbar (= irreduzibel)***, wenn eine Gleichung $u = ab$ mit $a, b \in R$ nur möglich ist, wenn a oder b eine Einheit ist; kurz wenn u keine echten Teiler hat.*

(c) $p \in R$ heißt **prim** *oder* **Primelement***, wenn p kein Nullteiler und keine Einheit ist und außerdem für alle $a, b \in R$ gilt: $[p|ab] \Longrightarrow [p|a$ oder $p|b]$.*

Beachte. Bei dieser Definition ist R ein beliebiger kommutativer Ring, sie ist also auch für $R[x]$ benutzbar.

Beobachtung. (i) p prim $\Longrightarrow$ p unzerlegbar (wenn R Bereich!).
(ii) Seien $p, a_1, \ldots, a_n \in R$ und p prim, dann gilt:

$$p \mid a_1 \cdots a_n \quad \Longrightarrow \quad p \mid a_i \quad \text{für ein } i \in \{1, \ldots, n\}.$$

Satz 4.4 (a). *Sei R ein euklidischer Ring. Jedes Element $r \in R$, das keine Einheit und $\neq 0$ ist, lässt sich als endliches Produkt von unzerlegbaren Elementen darstellen.*

Um auch die weitgehende Eindeutigkeit einer Zerlegung in Primelementen nachweisen zu können, benötigt man den folgenden

Satz 4.5. *In einem euklidischen Ring sind alle unzerlegbaren Elemente prim.*

Satz 4.5 ergibt sich mit Hilfe von Satz 1.18 sogar für Hauptidealringe oder als Anwendung von Ergebnissen in Abschnitt 6.

Es lässt sich dann zeigen:

Satz 4.4 (b). *Sei R ein euklidischer Ring und gelte für ein $r \in R$*

$$r = p_1 \ldots p_m = q_1 \ldots q_n$$

mit (nicht notwendig verschiedenen) Primelementen $p_1, \ldots, p_m, q_1, \ldots, q_n \in R$ und $m, n \geq 1$.

Dann ist notwendigerweise $m = n$ und (evtl. nach Umnumerierung etwa der q_i) $p_i = q_i e_i$ mit geeigneten Einheiten e_i.

Bemerkung. Fasst man Satz 4.4(a) und 4.4(b) zusammen, so erhält man für ein von 0 verschiedenes Element r aus einem euklidischen Ring zunächst eine Darstellung

$$r = p_1 \ldots p_n \,.$$

Dabei können die Primelemente mehrfach auftreten. Fasst man gleiche Primfaktoren zusammen, so ergibt sich, wenn o. E. etwa $p_1, \ldots, p_m$ paarweise nicht äquivalent sind, die Darstellung

$$r = p_1^{\alpha_1} \ldots p_m^{\alpha_m} \quad \text{mit } \alpha_i \in \mathbb{N},\ \alpha_i \geq 1 \text{ und } \sum_{i=1}^{n} \alpha_i = n\,.$$

Aufgrund von Satz 4.4(b) sind dabei (bis auf die Reihenfolge und eventueller Multiplikation mit Einheiten) $p_1, \ldots, p_m$ und die zugehörigen $\alpha_1, \ldots, \alpha_m$ eindeutig bestimmt.

Beweis von Satz 4.4(a) durch vollständige Induktion nach $\delta(r)$. O. E. sei vorausgesetzt: $M := R\backslash(G(R) \cup \{0\}) \neq \varnothing$, m. a. W., dass R kein Körper ist.

1) **Induktionsanfang:** Sei $n_0 = \text{Min}\{\delta(r) : r \in M\}$ und sei $r \in M$ mit $\delta(r) = n_0$. Wenn nun mit $a, b \in R$ gilt: $r = ab$ und wenn dabei b keine Einheit ist, dann folgt mit Def. 4.1(i) und der Minimalität von $\delta(r)$, dass gilt: $\delta(ab) = \delta(b)$. Nach Def. 4.1(ii) muss dann a eine Einheit sein. Man sieht so, dass ein $r \in M$ mit $\delta(r) = n_0$ unzerlegbar sein muss und dass daher für solche r die Behauptung von Satz 4.4(a) zutrifft.

2) **Induktionsschritt:** Sei $n > n_0$ und treffe Satz 4.4(a) für alle $r \in M$ mit $\delta(r) < n$ zu. Zu zeigen ist jetzt: Satz 4.4(a) trifft auch für $r \in M$ mit $\delta(r) = n$ zu. Wenn r unzerlegbar ist, ist dies der Fall. Wenn r zerlegbar ist, gibt es $a, b \in M$ mit $r = ab$ und $\delta(a) < \delta(r)$, $\delta(b) < \delta(r)$ (Def. 4.1(i), (ii)). Satz 4.4(a) kann also nach unserer Voraussetzung für a und b bereits angewendet werden. Sei etwa $a = u_1 \cdots u_m$ und $b = v_1, \ldots, v_n$ mit unzerlegbaren $u_1, \ldots, u_m$, $v_1, \ldots, v_n \in R$. Dann ist aber $r = u_1 \cdots u \cdot v_1 \cdots v_n$ Produkt endlich vieler unzerlegbarer Elemente aus R.

3) Wegen 1) und 2) ist nach dem Prinzip der vollständigen Induktion jedes $r \in M$ ein endliches Produkt unzerlegbarer Elemente. Satz 4.4(a) ist daher bewiesen.

□

Beweis von Satz 4.4(b) durch vollständige Induktion nach $\delta(r)$. Seien M, n_0 wie beim Beweis von Satz 4.4(a).

1) **Induktionsanfang:** Sei $r \in M$ mit $\delta(r) = n_0$. Dann ist (vgl. Induktionsanfang bei Satz 4.4(a) r unzerlegbar und es folgt $m = n = 1$ und $p_1 = q_1$.

2) **Induktionsschritt:** Sei $n > n_0$ und sei Satz 4.4(b) bewiesen für $r \in M$ mit $\delta(r) < n$. Zu zeigen ist: Die Aussage von Satz 4.4(b) gilt dann auch für $r \in M$ mit $\delta(r) = n$. Sei daher $r \in M$ und $\delta(r) = n$ und gelte $r = p_1 \cdots p_m = q_1 \cdots q_n$ mit Primelementen $p_1, \ldots, p_m,\ q_1, \ldots, q_n$. Ist r unzerlegbar, so folgt wieder

unmittelbar $m = n = 1$ und $p_1 = q_1$. Ist r zerlegbar, so muss gelten $m \geq 2$ **und** $n \geq 2$.

Da p_1 prim ist, und ein Teiler von $q_1 \cdots q_n$, gibt es ein $i \in \{1, \ldots, n\}$ derart, dass $p_1 | q_i$. Da q_i unzerlegbar ist, folgt $q_i = p_1 e$ mit $e \in G(R)$. Sei o. E. $i = 1$ (ggfs. umnumerieren). Wir haben dann: $r = p_1 \cdots p_m = p_1(eq_2) \cdots q_n = p_1 q_2' \cdots q_n'$ mit $q_2' = eq_2$ und $q_j' = q_j$ falls $3 \leq j \leq n$. Auch q_2' ist prim (selber nachweisen!). Da R nullteilerfrei ist, kann mit p_1 gekürzt werden und es gilt: $r' := p_2 \cdots p_m = q_2' \cdots q_n'$.

Wegen Def. 4.1(i), (ii) ist $\delta(r') < \delta(r) = n$. Für r' kann daher nach unserer Voraussetzung der Satz 4.4(b) benutzt werden und es folgt $m - 1 = n - 1$ und $p_i = q_i e_i$ für $2 \leq i \leq m = n$ mit $e_i \in G(R)$. Weiter oben ergab sich schon: $p_1 = q_1 e_1$ mit $e_1 = e^{-1} \in G(R)$. Für unser $r \in M$ mit $\delta(r) = n$ trifft demnach die Aussage von Satz 4.4(b) ebenfalls zu.

3) Ähnlich wie beim Beweis von Satz 4.4(a).

□

5 Matrizenringe

In einigen Beispielen tauchte der Ring $R^{n\times n}$ der quadratischen Matrizen mit Einträgen aus dem Ring R schon mehrfach auf. Hier werden nun in etwas systematischerer Form Eigenschaften dieses wichtigsten Beispiels eines nicht kommutativen Ringes zusammengetragen. Sei $R \neq \{0\}$.

Satz 5.1. *$R^{n\times n}$ kommutativ $\Longleftrightarrow$ R kommutativ* **und** *$n = 1$.*

Satz 5.2. *Die Teilmenge $\mathcal{M} \subset R^{n\times n}$ ist genau dann Ideal von $R^{n\times n}$, wenn $\mathcal{M} = J^{n\times n}$ mit einem Ideal J von R. Insbesondere gibt es keine Ideale $\neq \{0\}$, $R^{n\times n}$, wenn R ein Körper ist.*

Bemerkung. Erinnert man sich an Satz 1.21, dann ergibt sich aus Satz 5.2: Ist K ein Körper und φ ein von $K^{n\times n}$ ausgehender Ringmorphismus, dann ist $\operatorname{Kern}\varphi = \{0\}$ oder $\operatorname{Kern}\varphi = K^{n\times n}$; m. a. W., dann ist entweder φ injektiv oder die Nullabbildung.

Satz 5.3. *Sei K ein Körper, dann ist $K^{n\times n}$ ein Rechts- und Links-Hauptidealring.*

Bemerkung. Der Beweis von Satz 5.3 deutet an, dass die Verallgemeinerung von Satz 5.3 etwa schon für $\mathbb{Z}^{n\times n}$ zumindest nicht ohne zusätzliche Überlegungen möglich ist. Wir kommen darauf am Ende von Abschnitt 13 zurück.

Satz 5.4. *Sei K ein Körper, $R = K^{n\times n}$ und seien $A, B \in R$. Dann gilt*

$$\begin{aligned} AR &= BR \iff A \underset{r}{\sim} B \\ RA &= RB \iff A \underset{\ell}{\sim} B \end{aligned}$$

(vgl. Satz 1.16).

Satz 5.5. *Sei K ein Körper, dann kann man für $A, B \in K^{n\times n}$ einen "ggrT", die Koeffizienten einer Bézout-Identität und "kglV" in endlich viele Schritten berechnen. Alle ggrT (bzw. kglV) von A und B sind untereinander links-äquivalent. Die Aussagen sind links-rechts-symmetrisch.*

Wichtiger noch als Satz 5.5 insbesondere in Anwendungen ist dessen Verallgemeinerung für euklidische Ringe. Die Existenz etwa eines ggrT für zwei Matrizen $A, B \in R^{n\times n}$ und $\det B \neq 0$ erlaubt es, bei dem Ausdruck AB^{-1} zu einer gekürzten Darstellung überzugehen: $(A'G)(B'G)^{-1} = A'B'^{-1}$.

Der Vollständigkeit halber sei noch erinnert an die Ringe $R[A] \subset R^{n\times n}$, die am Ende von Abschnitt 3 eingeführt wurden. Allein die Klasse kommutativer Unterringe von $R^{n\times n}$, $n \in \mathbb{N}$, ist danach schon so reichhaltig, dass sie z. B. im Falle $R = K$ alle "endlichen" Körpererweiterungen "umfasst".

Kapitel II

Matrizen

Die Umformung von Matrizen war eines der wichtigsten Hilfsmittel in der Linearen Algebra I. In diesem Kapitel geht es zunächst darum, herauszufinden, was man mit elementaren Umformungen bei Matrizen über einem euklidischen Ring erreichen kann. Im weiteren Verlauf des Kapitels wenden wir die Ergebnisse unserer Untersuchungen an, um lineare Gleichungssysteme zu lösen. Eine weitere wichtige Anwendung führt uns zurück zum Normalformproblem aus der Linearen Algebra I, für das wir verschiedene vollständige Lösungen entwickeln.

6 Hermite und Smith-Form

Wichtiges Hilfsmittel bei der Gewinnung der Hermite- und Smith-Form ist die "Vereinfachung" von Ringelementen aus R bzw. $R^{n\times n}$ durch Multiplikation mit Einheiten aus $G(R)$ bzw. $G(R^{n\times n})$. Dies läuft darauf hinaus, dass in den Äquivalenzklassen bzgl. $\underset{r}{\sim}, \underset{\ell}{\sim}, \sim$ aber auch $\equiv$ nach möglichst "einfachen" Vertretern gesucht wird. Schon bekannte Beispiele von Vertretersystemen sind:

(a) $R = K$ Körper. $\boldsymbol{\mathcal{U}} = \{0, 1\}$ ist ein Vertretersystem für $\sim$.

(b) $R = \mathbb{Z}$. Durch Multiplikation mit $u \in G(\mathbb{Z})$ kann man stets zu nicht negativen Zahlen kommen. Es gilt $\mathbb{Z} = \{0\} \cup \{-1, 1\} \cup \{-2, 2\} \cup \ldots$. $\boldsymbol{\mathcal{U}} := \mathbb{N}$ ist ein Vertretersystem für diese Zerlegung in Äquivalenzklassen.

(c) $R = K[x]$, K ein Körper. Durch Multiplikation mit $u \in G(R) = G(K) = K\backslash\{0\}$ kann man stets erreichen, dass der höchste Koeffizient eines von 0 verschiedenen Polynoms 1 wird. Mit $\boldsymbol{\mathcal{U}} := \{p \in K[x]\backslash\{0\} : hK(p) = 1\} \cup \{0\}$ gilt: $K[x] = \bigcup_{p\in\boldsymbol{\mathcal{U}}} p \cdot (K\backslash\{0\})$. Dabei sind die Mengen $p \cdot (K\backslash\{0\})$, $p \in \boldsymbol{\mathcal{U}}$, paarweise disjunkt. $\boldsymbol{\mathcal{U}}$ ist ein Vertretersystem für die Äquivalenzrelation $\sim$ in $K[x]$.

(d) K ein Körper, $R = K^{n\times n}$. Die Gewinnung der Zeilenstufenform für eine quadratische Matrix A (Teil 1 der Linearen Algebra) ist nichts anderes als der

Übergang zu einem in gewissem Sinne einfacheren Vertreter der Klasse der zu A links-äquivalenten Matrizen. Der "rechteckige" Fall subsummiert sich, indem man mit "0-en" zu einer quadratischen Matrix auffüllt.

(e) Auch das folgende Resultat ist schon von der Linearen Algebra I her bekannt: $\boldsymbol{\mathcal{U}} := \{0, \mathrm{diag}(1,0,\ldots,0), \ldots, \mathrm{diag}(1,\ldots,1)\}$ ist ein Vertretersystem für $\sim$ in $K^{n\times n}$.

Beispiele von Vertretersysgem bzgl. $\equiv$ sind:

(e) $R = \mathbb{Z}$, $q \in \mathbb{Z}$, $|q| = d$. Die Menge $\boldsymbol{\mathcal{U}}_q = \mathbb{Z}_d$ ist ein Vertretersystem für $\equiv_q$.

(f) $R = K[x]$, K ein Körper. Für jedes Polynom $q \in K[x]\backslash\{0\}$ mit $d = \deg q$ ist die Menge $\boldsymbol{\mathcal{U}}_q := K[x]_d$ ein Vertretersystem für $\equiv_q$.

Die "einfachsten" Einheiten in $R^{n\times n}$ sind die **Elementarmatrizen**. Sie sind besonders wichtig wegen ihrer engen Beziehung zu den **elementaren Umformungen**.

Die Ausführungen in Linearer Algebra I bzw. in [Fi, S. 156] über Elementarmatrizen lassen sich mit einer Ausnahme ohne Änderung für beliebige Ringe übernehmen: **Bei den Matrizen $\boldsymbol{S_i(\lambda)} = \mathrm{diag}(1,\ldots,\lambda,\ldots,1)$ mit λ an der i-ten Stelle, ist jetzt $\boldsymbol{\lambda \in G(R)}$ zu fordern.**

Entsprechend ist bei den elementaren Zeilen- oder Spaltenoperationen die **Multiplikation einer Zeile oder Spalte nur mit $\boldsymbol{\lambda \in G(R)}$ zugelassen**. Nur dann sind auch diese Operationen "reversibel" wie alle übrigen auch.

Satz 6.1. *Sei R ein Ring. Produkte von Elementarmatrizen aus $R^{n\times n}$ sind stets invertierbar. Genauer: $\{P \in R^{n\times n} | P$ ist Produkt von Elementarmatrizen$\}$ ist eine Untergruppe von $\boldsymbol{GL_n(R) = G(R^{n\times n})}$.*

Bemerkung. Für euklidische Ringe wird sich weiter unten noch ergeben $GL_n(R) = \{P \in R^{n\times n} \mid P$ ist Produkt von Elementarmatrizen$\}$, ganz so, wie es für Körper schon aus der Linearen Algebra I bekannt ist. Dies liegt daran, dass über einem euklidischen Ring allein durch elementare Zeilenumformungen bei einer Matrix obere Dreiecksform erreicht werden kann, was schon über einem nicht euklidischen Hauptidealring nicht mehr möglich ist. Dieser Sachverhalt ist ein wichtiger mathematischer Anlass, lineare Algebra über euklidischen Ringen zu betreiben.

Satz 6.2 (a). *Sei R euklidisch, $A \in R^{m\times n}$. Dann ist A linksäquivalent zu einer Matrix der Form*

$$B = \begin{bmatrix} 0 & \ldots & 0|\underline{b_{1j_1}} & * & \ldots\ldots\ldots\ldots & * \\ 0 & \ldots\ldots\ldots & 0|\underline{b_{2j_2}} & * & \ldots\ldots\ldots\ldots & * \\ & & & & & \vdots \\ 0 & \ldots\ldots\ldots\ldots\ldots\ldots & & 0|\underline{b_{kj_k}} & & * \\ 0 & & & & & 0 \\ \vdots & & & & & \vdots \\ 0 & & & & & 0 \end{bmatrix} \tag{1}$$

und zwar kann A durch Multiplikation von links mit Elementarmatrizen bzw. durch elementare Zeilenumformungen in eine Matrix der Form B überführt werden.

Der **Beweis** ist algorithmisch und beruht wesentlich auf der Division mit Rest. Eine unmittelbare Folgerung ist:

Satz 6.2 (b). *$GL_n(R) = \{P \in R^{n\times n} | P$ ist Produkt von Elementarmatrizen$\}$.*

Nach Satz 6.2(a) liegt in der Linksäquivalenzklasse einer Matrix $A \in R^{n\times n}$ stets mindestens eine Matrix der Form B. Es können aber i. a. mehrere sein. Durch weitere "Normierung" lässt sich Eindeutigkeit erreichen. Sei dazu $\boldsymbol{\mathcal{U}}$ ein Vertretersystem für die Äquivalenz in R und für $0 \neq q \in R$ $\boldsymbol{\mathcal{U}}_q$ ein Vertretersystem für die Kongruenz $\mod qR$. Beispiele für solche Vertretersysteme wurden bereits weiter oben angegeben.

Satz 6.2(a) lässt sich nun wie folgt präzisieren:

Satz 6.2 (c). Hermite-Normalform *(Charles Hermite 1822-1901). Sei R euklidisch, $A \in R^{n\times n}$, $A \neq 0$, dann liegt in der Linksäquivalenzklasse von A* **genau eine** *Matrix der Form B in (1) mit folgenden zusätzlichen Spezifikationen.*

$$\begin{array}{lll} b_{ij_i} & \in \boldsymbol{\mathcal{U}}\backslash\{0\} & 1 \leq i \leq k \\ b_{\nu j_i} & \in \boldsymbol{\mathcal{U}}_{b_{ij_i}} & 1 \leq \nu < i \text{ und } 1 < i \leq k, \text{ sofern } k > 1. \end{array}$$

Die so spezifizierte Matrix B aus der Linksäquivalenzklasse von A heißt **Hermite-Form** *von A (bzgl. der gewählten Vertretersysteme). Der Übergang von A nach B ist durch elementare Zeilenumformungen möglich.*

Bemerkungen. (i) Für Matrizen $A \in R^{m\times n}$, $m \neq n$ gilt ein analoger Satz, den man erhält, indem man A mit 0-en zu einer quadratischen Matrix auffüllt. Als erste Anwendung von Satz 6.2 ergibt sich ein **Verfahren zur Berechnung eines ggrT und kglV für $\boldsymbol{A, B \in R^{n\times n}}$**, das im Sonderfall $n = 1$ zu einem Verfahren zur Berechnung von ggT, kgV für $a, b \in R$ wird (Details dieses wichtigen Verfahrens in der Vorlesung). Dabei werden die Koeffizienten einer Bézout-Identität für ggrT bzw. ggT gleich mitgeliefert. Das Verfahren lässt sich im Fall $n = 1$ so handhaben, dass es dem **"euklidischen Algorithmus"** entspricht.

Die Bestimmung eines ggrT endlich vieler $A_1, \ldots, A_r \in R^{n\times n}$ ist auf analoge Weise möglich.

(ii) Es sei erinnert an die Bemerkung nach Satz 1.19. Die Möglichkeit, mit obigem Verfahren in endlich vielen Schritten eine Bézout-Identität für ggT herzustellen, ist Grundlage für einen **Beweis von Satz 4.5** ohne Rückgriff auf die Sätze 1.18, 1.19. Es geht dabei um die Äquivalenz der Begriffe "prim" und "unzerlegbar", die ausschlaggebend ist bei der Eindeutigkeit von Primzerlegung.

Der folgende Satz gibt an, wie eine Matrix über einem euklidischen Ring "vereinfacht" werden kann, wenn Zeilen- **und** Spaltenumformungen zugelassen sind:

Satz 6.3. Smith-Form *(Henry John Steven Smith 1826-1883, Original für $\mathbb{Z}$ 1861). Sei R euklidisch und $\boldsymbol{U} \subset R$ ein Vertretersystem für die Äquivalenz in R. In der Äquivalenzklasse von $M \in R^{n\times n}$ liegt genau eine Matrix*

$$D = \operatorname{diag}(d_1, \ldots, d_n)$$
$$\text{mit } d_i \in \boldsymbol{U} \text{ für } 1 \le i \le n \text{ und } \boldsymbol{d_i | d_{i+1}} \text{ für } 1 \le i \le n-1\,.$$

Der Übergang von A zu D ist durch elementare Zeilen- und Spaltenumformungen bzw. durch Multiplikation mit Elementarmatrizen möglich. D heißt **Smith-Form von $\boldsymbol{M}$**, die d_i heißen **invariante Faktoren von $\boldsymbol{M}$**.

Beweis. Der Existenznachweis für die Smith-Form ist über einem euklidischen Ring konstruktiv möglich durch Angabe eines Algorithmus (siehe Vorlesung), der in endlich vielen Schritten zu einer vorgegebenen Matrix M deren Smith-Form liefert. Der **Eindeutigkeits**nachweis ergibt sich als Anwendung von Ergebnissen über die "Determinantenteiler" (siehe Abschnitt 9) und wird daher vorerst zurückgestellt. □

Bemerkung. Satz 6.3 ist die Verallgemeinerung des zu Beginn dieses Abschnittes in Beispiel (e) erwähnten Resultates. Für Matrizen $A \in R^{m\times n}$ gilt eine analoger Satz (s. o. Bemerkung (i)).

7 Lineare Gleichungssysteme

Zunächst sei R ein kommutativer Ring. Betrachtet wird das lineare Gleichungssystem

$$''Ax = b''\,.$$

Gegeben sind dabei $A \in R^{m\times n}$, $b \in R^m$ und gesucht ist $x \in R^n$. Die Lösungsmenge bezeichnen wir mit

$$\text{Lös}(A, b) := \{x \in R^n : Ax = b\}\,.$$

Völlig analog zur Linearen Algebra I gilt auch hier:

Satz 7.1. *Entweder ist $Lös(A, b) = \varnothing$ oder es ist $Lös(A, b) = Lös(A, 0) + x$ für alle $x \in Lös(A, b)$.*

Satz 7.2. *Mit $P \in GL_m(R)$ und $Q \in GL_n(R)$ gilt:*

$$Lös(A, b) = Q\, Lös(PAQ, Pb)\,.$$

Will man im konkreten Einzelfall die Lösungsmenge $\text{Lös}(A, b)$ bestimmen, so muss man ein Verfahren finden, das die Matrix A in eine Matrix PAQ überführt derart, dass $\text{Lös}(PAQ, Pb)$ einfach bestimmt werden kann.

Setzen wir R als euklidisch voraus, dann kennen wir ein solches Verfahren aus dem vorangehenden Abschnitt 6. Sei (o. E.!) zur Vereinfachung der Schreibweise $m = n$ und seien $P, Q \in GL_n(R)$ gefunden derart, dass

$$D := PAQ = diag(d_1, \ldots, d_n) \quad \text{mit } d_1, \ldots, d_n \in R.$$

Zu bestimmen bleibt, dann $\text{Lös}(D, c)$ mit $c := Pb$.

Satz 7.3.

(i) *Lös*$(D, c) \neq \varnothing$ *genau dann, wenn gilt*

$$d_i \mid c_i \quad \textit{für } 1 \leq i \leq n. \tag{1}$$

(ii) *Wenn* (1) *gilt, dann ist*

$$\textit{Lös}(D, c) = X^* + \mathrm{Span}_R((e_j)_{j \in K})$$

wobei

$$x_i^* = \left\{ \begin{array}{ll} 0 & \textit{falls } d_i = 0 \\ \dfrac{c_i}{d_i} & \textit{falls } d_i \neq 0 \end{array} \right\} \quad \textit{für } 1 \leq i \leq n\,,$$

e_j *ist* j*-ter Einheitsvektor in* $R^{n \times 1}$ *und*

$$K = \{i \in \{1, \ldots, n\} : d_i = 0\}\,.$$

Für effektivere Lösungsverfahren sei z. B. auf [Co] verwiesen.

8 Zur Determinante über einem kommutativen Ring

In der Vorlesung zur Linearen Algebra I wurde ausgehend vom Problem der Volumenbestimmung von Parallelflachen die Determinante eingeführt als homogene und scherungsinvariante Abbildung $(K^{n \times 1})^n \longrightarrow K$, wobei K ein Körper ist. Es wurde u. a. gezeigt, dass solche Abbildungen immer auch n-linear und alternierend sind (und umgekehrt). In einem weiteren Schritt ergab sich dann, dass es bis auf einen konstanten Normierungsfaktor genau **eine** n-lineare und alternierende Abbildung gibt: die Determinante.

Zwangsläufig erhält man für $A = (a_{ij})$ den folgenden Ausdruck (Leibniz'sche Formel):

$$\boxed{\begin{array}{l} \det A \;\; = \Sigma(sig\; n(\sigma) \cdot a_{1\sigma(1)} \ldots a_{n\sigma(n)}) \\ \qquad\qquad (\sigma \text{ Permutation von } \{1, \ldots, n\}) \end{array}} \tag{1}$$

und die durch (1) definierte Abbildung $\det : K^{n \times n} \longrightarrow K$ ist tatsächlich alternierend und n-fach linear bzw. homogen und scherungsinvariant und zwar sowohl bezüglich der Zeilen als auch der Spalten der Matrizen $A \in K^{n \times n} = (K^{n \times 1})^n$. Für Matrizen $A \in R^{n \times n}$, R mit Einträgen aus einem kommutativen Ring, gehen wir genau den **umgekehrten Weg**.

Der Ausdruck auf der rechten Seite von (1) kann auch in einem Ring R gebildet werden. Daher kann **$\det A$ für $A \in R^{n \times n}$ durch** (1) **definiert** werden. **Fast** alle wichtigen Eigenschaften der Determinante lassen sich in völliger Analogie zum Körper-Fall aus (1) herleiten. Es gilt:

Satz 8.1. *Sie R ein kommutativer Ring, $n \geq 1$, und* $\det : R^{n\times n} \longrightarrow R$ *definiert durch* (1) *und $A = (a_{ij}) \in R^{n\times n}$. Es gilt dann:*

(a) $\det E = 1$ *für die $n \times n$-Einheitsmatrix E.*

(b) det *ist n-fach linear in Zeilen und Spalten.*

(c) det *ist invariant bzgl. der folgenden elementaren Zeilenoperation: Addition des λ-fachen ($\lambda \in R$) einer Zeile zu einer* **anderen** *Zeile.*

(d) Aussage c) für Spalten

(e) Vertauschung zweier (verschiedener) Zeilen oder Spalten bewirkt Vorzeichenwechsel.

(f) $\det {}^tA = \det A$

(g)
$$\det \begin{bmatrix} a_{11} & * & \dots & * \\ 0 & & & \vdots \\ \vdots & \ddots & & * \\ 0 & \dots & 0 & a_{nn} \end{bmatrix} = a_{11} \cdots a_{nn}$$

(h)
$$\det \begin{bmatrix} \underline{A_{11}|} & & & * \\ 0 & \ddots & & \\ \vdots & & \ddots & \\ 0 & & & |\overline{A_{rr}} \end{bmatrix} = (\det A_{11}) \cdots (\det A_{rr})$$

wobei $A_{ii} \in R^{d_i \times d_i}$ $(d_i \geq 1)$ und $\sum_{i=1}^{r} d_i = n$.

(i) $\det(AB) = (\det A)(\det B)$.

(j) Für $i \in \{1, \dots, n\}$ gilt

$$\det A = \sum_{j=1}^{n} a_{ij} c_{ij} \quad \textit{mit} \quad c_{ij} = \det \begin{bmatrix} a_{11} & & \dots & & a_{1n} \\ 0 & \dots & 1 & \dots & 0 \\ a_{n1} & & & & a_{nn} \end{bmatrix}$$

wobei die 1 an der Position (i, j) steht. Die c_{ij} heißen **Kofaktoren** *von A, die behauptete Formel heißt* **Laplace'sche Entwicklung** *nach der i-ten Zeile.*

(k)
$$\widetilde{A}A = A\widetilde{A} = (\det A)E\,,$$

dabei ist $\widetilde{A} := {}^tC$ mit $C = (c_{ij})$ und c_{ij} definiert wie in (j). $\widetilde{A}$ wird häufig **adjungierte** *oder auch* **komplementäre** *Matrix zu A genannt.*

(l) **Cramer'sche Regel:** *Seien* $b, x \in R^{n\times 1}$ *und* $A_{i,b}$ *die Matrix, die aus* A *entsteht durch Ersetzen der* i*-ten Spalte durch* b*. Dann gilt:*

$$Ax = b \quad \Longrightarrow \quad \det A \cdot x_i = \det A_{i,b} \quad \textit{für } 1 \le i \le n.$$

Die Umkehrung gilt, wenn R *ein Bereich ist,* $\det A \neq 0$ *und* $\det A \mid \det A_{i,b}$ *für* $1 \le i \le n$*.*

(m) $A \in GL_n(R)$ *genau dann, wenn* $\det A \in G(R)$*.*

(n) $A^{-1} = \frac{1}{\det A}\widetilde{A}$*, falls* $\det A \in G(R)$*.*

Beweis. Alle behaupteten Eigenschaften lassen sich wie ein Körper-Fall direkt und elementar aus (1) ableiten! Nur j) – l) werden in der Vorlesung behandelt, da insbesondere j) in Linearen Algebra I nicht auftrat. □

Die Cramer'sche Regel in der obigen Form wird z. B. in [Lue1] für Körper und in [La2] für kommutative Ringe hergeleitet.

Die bereits bei Satz 8.1(h) in Sonderfällen aufgetretenen Determinanten von quadratischen Untermatrizen sind erste Beispiele von **Minoren**.

Definition 8.2 (Untermatrizen und Minoren). *Sei* $A = (a_{ij}) \in R^{m\times n}$ *und seien* $k, \ell, i_1, \ldots, i_k, j_1, \ldots, j_\ell \in \mathbb{N}_+$ *mit* $1 \le i_1 < \cdots < i_k \le m$ *und* $1 \le j_1 < \cdots < j_\ell \le n$ *also insbesondere* $1 \le k \le m$ *und* $1 \le \ell \le n$*. Die Matrix*

$$A^{j_1,\ldots,j_k}_{i_1,\ldots,i_k} := (a_{i_\varkappa j_\lambda})_{\substack{1\le\varkappa\le k\\ 1\le\lambda\le\ell}} \in R^{k\times\ell}$$

ist eine $\boldsymbol{k\times\ell}$**-Untermatrix** *(oder Teilmatrix) von* A *und wenn* $\boldsymbol{k=\ell}$*, dann ist*

$$\det\left(A^{j_1,\ldots,j_k}_{i_1,\ldots,i_k}\right) \in R$$

ein $\boldsymbol{k\times k}$**-Minor** *oder* **Minor der Ordnung** $\boldsymbol{k}$ *von* A*.*

9 Determinantenteiler und Eindeutigkeit der Smith-Form

Im Folgenden sei stets R ein euklidischer Ring und $\boldsymbol{\mathcal{U}}$ ein Vertretersystem für die Äquivalenz in R. Zur Vereinfachung setzen wir noch voraus: $\boldsymbol{\mathcal{U}}$ **sei multiplikativ abgeschlossen**. Beispiele hierfür sind a), b), c) auf S. 32.

Definition 9.1. *Seien* $M \in R^{n\times n}$*,* $1 \le r \le n$ *und* g *ein ggT aller Minoren der Ordnung* r*. Der eindeutig bestimmte, zu* g *äquivalente Vertreter* $\boldsymbol{g_r(M)} \in \boldsymbol{\mathcal{U}}$ *heißt* $\boldsymbol{r}$**-ter Determinantenteiler von** $\boldsymbol{M}$ *(bzgl.* $\boldsymbol{\mathcal{U}}$*).*

Bequem aber ungenau ist die Schreibweise:

$$\boxed{g_r(M) := \text{ ggT Minoren der Ordnung } r \text{ von } M}$$

Wenn Verwechslungen ausgeschlossen sind, wird g_r statt $g_r(M)$ geschrieben. Außerdem wird festgesetzt:

$$g_0(M) := 1$$

Aus der Definition ist ersichtlich, dass stets $g_r(M) = g_r(M')$ ist, wenn M' die transponierte Matrix zu M ist. Außerdem gilt die Regel

$$\boxed{g_{r-1} \mid g_r \quad \text{für} \quad 1 \leq r \leq n}$$

Man beachte, dass $g_r = 0$ zugelassen und möglich ist. Falls $r < n$ und $g_r = 0$, dann ist auch $g_i = 0$ für $r \leq i \leq n$.

Die Determinantenteiler spielen eine wichtige Rolle wegen folgender **Invarianzeigenschaft**:

Satz 9.2 (a). *Seien $M, N \in R^{n\times n}$. Es gilt:*

$$[M \sim N] \Longrightarrow [g_r(M) = g_r(N) \quad \textit{für } 1 \leq n \leq n]$$

Bemerkung zum **Beweis**. $M \sim N$ heißt ja $M = PNQ$ mit $P, Q \in Gl_n(R) = G(R^{n\times n})$. Nach Satz 6.2(b) ist jedes $P \in GL_n(R)$ Produkt von Elementarmatrizen. Also genügt es zu beweisen, dass die Determinantenteiler bei elementaren Zeilen- und Spaltenumformungen sich nicht ändern. Da **Transposition** die Determinantenteiler nicht ändert, genügt es z. B. zu zeigen: Elementare Spaltenumformungen ändern die Determinantenteiler nicht. □

Satz 9.2(a) besagt u. a.: wenn D eine Smith-Form der Matrix M ist, dann haben D und M dieselben Determinantenteiler (immer bezogen auf ein multiplikativ abgschlossenes Vertretersystem $\boldsymbol{\mathcal{V}}$ für die Äquivalenz in R). Daher ist es lohnend, **einmal** die Determantenteiler einer Smith-Form zu berechnen. Sei also $D = \operatorname{diag}(d_1, \ldots, d_n)$ mit $d_i \mid d_{i+1}$, $1 \leq i \leq n$.

Satz 9.3. *Es bestehen folgende* **Beziehungen zwischen Determinantenteilern und invarianten Faktoren***:*

(a) $g_i = d_1 \ldots d_i$ *für* $1 \leq i \leq n$

(b) $g_i = d_i \cdot g_{i-1}$ *für* $1 \leq i \leq n$

(c) $g_i = 0 \Longleftrightarrow d_i = 0$ *für* $\quad 1 \leq i \leq n$

(d) $g_i = 0 \Longrightarrow g_{i+1} = 0$ *für* $1 \leq i \leq n$

(e) $g_1^2 \mid g_2$, *falls* $n \geq 2$, *und*
$g_i^2 \mid g_{i-1}g_{i+1}$, *falls* $n \geq 3$ *und für* $2 \leq i < n$

Seien $g, d : R^{n\times n} \longrightarrow R^n$ definiert durch

$$\begin{aligned} g(M) := (g_1(M), \ldots, g_n(M)) &= \text{Vektor der Determinantenteiler von } M \text{ in } \boldsymbol{\mathcal{U}}. \\ d(M) := (d_1(M), \ldots, d_n(M)) &= \text{Vektor der invarianten Faktoren von } M \text{ in } \boldsymbol{\mathcal{U}}. \end{aligned}$$

Seien $I := \{(r_1, \ldots, r_n) \in \boldsymbol{\mathcal{U}}^n : r_1 | \ldots | r_n\}$ und

$$J := \left\{ (s_1, \ldots, s_n) \in \boldsymbol{\mathcal{U}}^n : \begin{array}{ll} s_1^2 \mid s_2, & \text{falls } n \geq 2, \text{ und} \\ s_i^2 \mid s_{i-1}s_{i+1}, & \text{falls } n \geq 3,\ 2 \leq i < n \end{array} \right\}$$

J ist eine Teilmenge von I (!) und $\gamma : I \longrightarrow J$ (!) sei gegeben durch

$$\gamma(r_1, \ldots, r_n) := (r_1, r_1r_2, \ldots, r_1 \cdots r_n)\,.$$

Auf Grund von Satz 9.3 lässt sich elementar bestätigen, dass in dem Diagramm

$$\begin{array}{ccc} & {\scriptstyle d} \searrow & I \\ R^{n\times n} & & \downarrow {\scriptstyle \gamma} \\ & {\scriptstyle g} \searrow & J \end{array}$$

alle Abbildungen **surjektiv** sind, γ **bijektiv** ist und dass außerdem gilt: $\gamma \circ d = g$.

Auf Grund dieses Zusammenhanges ergibt sich folgende **Umkehrung von Satz 9.2(a)**.

Satz 9.2 (b). $[g(M) = g(N)] \Longrightarrow [M \sim N]$

Beweis. Vorausgesetzt ist: $g(M) = g(N)$.
Seien $\operatorname{diag}(\underbrace{d_1(M), \ldots, d_n(M)}_{=:d(M)})$ und $\operatorname{diag}(\underbrace{d_1(N), \ldots, d_n(N)}_{=:d(N)})$ Smith-Formen von M und N. Wegen Satz 9.3 und Satz 9.2(a) folgt: $\gamma(d(M)) = g(M) = g(N) = \gamma(d(N))$ und, da γ invertierbar ist, $d(M) = \gamma^{-1}(g(M)) = \gamma^{-1}(g(N)) = d(N)$. Die Smith-Formen von M und N stimmen somit überein, was nur möglich ist, wenn $M \sim N$. □

Bemerkung. Aus Satz 9.2(a),(b) und 9.3 ergibt sich direkt die **Eindeutigkeit der Smith-Form** bezüglich eines multiplikativ abgeschlossenen Vertretersystems $\boldsymbol{\mathcal{U}}$ für die Äquivalenz in R.

Die invarianten Faktoren und die Deteminantenteiler sind Beispiele sogenannter **Invarianten** bzgl. $\sim$. Satz 9.2(a) besagt: $g_i(M)$ bleibt unverändert bei äquivalenten Umformungen, kurz: $g_i(M)$ ist invariant oder **eine Invariante** bzgl. $\sim$. Satz 9.2(a),(b) besagt: $g(M)$ ist ein **vollständiger Satz** (Vektor) **von Invarianten** bzgl. $\sim$. Damit ist gemeint, dass die Angabe der $g_i(M)$ genügt, um M bis auf

Äquivalenz festzulegen **und** dass die $g_i(M)$ Invarianten sind. M. a. W.: Die Abbildung

$$g^{-1} : J \longrightarrow \{\text{Äquivalenzklassen in } R^{n\times n}\}$$
$$x \longmapsto \{M \in R^{n\times n} : g(M) = x\}$$

ist bijektiv.

Da die Abbildung γ bijektiv ist, gilt für $\gamma^{-1}\circ g = d$ das Gleiche wie für g. Somit ist auch $d(M) = (d_1(M), \ldots, d_n(M))$ ein vollständiger Satz von Invarianten. Letztere Aussage beinhaltet die Eindeutigkeit der Smith-Form. Ein weiterer vollständiger Satz von Invarianten ergibt sich, wenn die Zerlegung der invarianten Faktoren in Primelemente berücksichtigt wird.

Ist $p \in \boldsymbol{\mathcal{U}}$ ein ("normiertes") Primelement und $r \in R$, $r \neq 0$, dann sei:

$$\alpha_p(r) := \max\{\ell \in \mathbb{N} : p^\ell \mid r\}$$

Wenn $p \nmid r$, ist $\alpha_p(r) = 0$ und $\alpha_p(0)$ ist nicht definiert. $p^{\alpha_p(r)}$ ist der **p-Anteil von r** (beachte die Abhängigkeit von $\boldsymbol{\mathcal{U}}$).

Sei jetzt $M \in R^{n\times n}$ und seien $d_1, \ldots, d_n$ die invarianten Faktoren ($\in \boldsymbol{\mathcal{U}}$) von M. Wegen der Teilbarkeitsbeziehungen zwischen den invarianten Faktoren teilt der p-Anteil von d_i den p-Anteil von d_k für $1 \leq i \leq k \leq n$, sofern er definiert ist.

Schreibt man daher die von 1 verschiedenen p-Anteile von $d_1, \ldots, d_n$ für alle vorkommenden Primelemente in irgendeiner Reihenfolge auf, so treten im allgemeinen einige Terme p^m mehrfach auf. Die Liste dieser Primelementpotenzen mit Wiederholungen (!) und beliebiger Anordnung heißt Liste oder **Familie der Elementarteiler von M**. Die Elementarteiler alleine bilden noch keinen vollständigen Satz von Invarianten. Hinzu tritt noch der Rang von M.

Definition 9.3. *Sei $M \in R^{n\times n}$ und seien $d_1, \ldots, d_n \in \boldsymbol{\mathcal{U}}$ die invarianten Faktoren von M.*

$$\operatorname{rang} M := \max\{i : d_i \neq 0\}\,.$$

Es gilt wegen der Eindeutigkeit der Smith-Form: $M \sim N \Longrightarrow \operatorname{rang} M = \operatorname{rang} N$.

In der Vorlesung wird erläutert, wie man bei gegebenem Rang aus einer Liste von Elementarteilern die invarianten Faktoren wieder zurückerhalten kann.

Da außerdem Rang und Elementarteiler invariant sind bei elementaren Zeilen- und Spaltenumformungen (also bei äquivalenten Umformungen, vgl. Satz 6.2(b), stellen sie einen weiteren vollständigen Satz von Invarianten bzgl. $\sim$ dar.

10 Charakteristische Matrizen

Dieser Abschnitt ist grundlegend in verschiedener Hinsicht. Zunächst wird gezeigt, wie man "vorsichtig" ein Matrixpolynom von links und rechts durch ein lineares

Matrixpolynom mit Rest dividieren kann. Man erkennt so den Unterschied zwischen Links- und Rechts-Einsetzung in ein Matrixpolynom. Als erste Anwendung ergibt sich direkt der Satz von Caylay Hamilton für beliebige kommutative Ringe. Als zweite Anwendung zeigen wir, dass zwei Matrizen $A, B \in R^{n\times n}$ genau dann ähnlich sind, wenn die Matrixpolynome $xE - A$, $xE - B$ äquivalent sind. Dieses Ergebnis ist der Angelpunkt für ein Verfahren zur Bestimmung verschiedener Ähnlichkeits-Normalformen für Matrizen über einem Körper in Abschnitt 11.

Sei R ein kommutativer Ring und $A \in R^{n\times n}$.

Definition 10.1.

$$(xE - A) = \begin{bmatrix} x - a_{11} & \dots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{n1} & \dots & x - a_{nn} \end{bmatrix} \in (R[x])^{n\times n}$$

heißt **charakteristische Matrix zu** A.

$(xE - A)$ ist das erste Beispiel für die **Polynomschreibweise für Matrizen aus $(R[x])^{n\times n}$**, die wir im folgenden öfter benutzen werden. Sei $M \in (R[x])^{n\times n}$, M ist dann eine sogenannte **Polynommatrix**, ihre Einträge sind Polynome.

Sei etwa $m_{ij} = \sum_{\nu=0}^{d} r_{ij\nu}x^\nu$. O. E. wurde $d \in \mathbb{Z}_{\geq 0}$ unabhängig von i, j gewählt, was stets möglich ist, da ja nicht $r_{ijd} \neq 0$ gefordert wird. Nun ist $M = \sum_{\nu=0}^{d} M_\nu x^\nu$ mit $M_\nu = (r_{ij\nu}) \in R^{n\times n}$. Dabei ist $M_\nu x^\nu = M_\nu(Ex^\nu) = (r_{ij\nu}x^\nu) = (x^\nu r_{ij\nu}) = (Ex^\nu)M_\nu = x^\nu M_\nu$. $\sum_{\nu=0}^{d} x^\nu M_\nu = \sum_{\nu=0}^{d} M_\nu x^\nu$ ist ein sogenanntes Matrix-Polynom, die **Darstellung von M als Matrixpolynom**. Letztere ist eindeutig durch M bestimmt.

Wichtig: Matrixpolynome sind für uns nur umgschriebene Polynommatrizen.

Satz 10.2. *Sei R ein kommutativer Ring, $M = \sum_{\nu=0}^{d} M_\nu x^\nu = \sum_{\nu=0}^{d} x^\nu M_\nu \in (R[x])^{n\times n}$, $M_\nu \in R^{n\times n}$ für $0 \leq \nu \leq d$. Es gilt:*

(a) $M = 0 \Longleftrightarrow M_\nu = 0, \quad 0 \leq \nu \leq d$

(b) $(xE - A)M = \sum_{\nu=0}^{d} N_\nu x^\nu \quad (N_\nu \in R^{n\times n}) \Longrightarrow M_d = 0$

(c) $(xE - A)M = 0 \Longleftrightarrow M = 0 \Longleftrightarrow M(xE - A) = 0$
Kurz: $(xE - A)$ ist kein Nullteiler in $R[x]^{n\times n}$.

(d) Es gibt $U, S \in (R[x])^{n\times n}$ und $R, V \in R^{n\times n}$ derart, dass

$$M = S(xE - A) + R = (xE - A)U + V\,.$$

Dabei sind R, S, U, V sind eindeutig bestimmt, und es gilt:

$$\begin{aligned} R &= \sum_{\nu=0}^{d} M_\nu A^\nu =: M^\bullet(A) \\ V &= \sum_{\nu=0}^{d} A^\nu M_\nu =: {}^\bullet M(A) \end{aligned}$$

$M^\bullet(A)$ bzw. ${}^\bullet M(A)$ ist das Ergebnis der Rechts- bzw. Links-Einsetzung von A in M.

Die Aussage (d) heißt: **Satz von Bézout** *(Étienne Bézout 1739-1783)*

Als erste Anwendung des Satzes von Bézout beweisen wir den Satz von Cayley-Hamilton:

Definition 10.3. *Sei R ein kommutativer Ring und $A \in R^{n\times n}$.*

$\varphi_A := \det(xE - A)$ *heißt* **charakteristisches Polynom der Matrix** A.

Offensichtlich ist $\varphi_A = x^n + \ldots + \det(-A) \in R[x]$; also $\deg \varphi_A = n$ und höchster Koeffizient von $\varphi_A = 1$.

Satz 10.4. Satz von Cayley-Hamilton *(Arthur Cayley 1821-1895, Willliam Rowan Hamilton 1805-1865). Sei R ein kommutativer Ring und $A \in R^{n\times n}$. Es gilt:*
A ist Nullstelle in $R^{n\times n}$ von φ_A.

Kurz: $\varphi_A(A) = 0$
oder: $\varphi_A \in \operatorname{Kern} \pi_A$. *(vgl. Abschnitt 3, S. 24 Beispiel (b))*

Beweis. Sei $N := (xE - A)$, $S := \widetilde{N}$ und $M := \widetilde{N}N = S(xE - A)$. Wegen Satz 8.1(k) gilt:

$$M = (\det N)E = S(xE - A) = \varphi_A \cdot E\,.$$

Auf Grund der Eindeutigkeitsaussage des Satzes von Bézout folgt: $M^\bullet(A) = 0$.
Im vorliegenden Spezialfall ist $M^\bullet(A) = \varphi_A(A)$, also $\varphi_A(A) = 0$. □

Auch bei dem folgenden Satz 10.5 ist der Satz von Bézout wichtigstes Beweishilfsmittel. Satz 10.5 ist das Hauptziel dieses Abschnitts 10. Er ist Grundlage für die Anwendung der Smith-Form (Satz 6.3) bei der Behandlung des Normalformenproblems der linearen Algebra über Körpern in Abschnitt 11.

Satz 10.5. *Sei R ein kommutativer Ring und seien $A, B \in R^{n\times n}$. Dann gilt:*

(a) $[\,(xE - A) \sim (xE - B)\,] \Longleftrightarrow [\,A \approx B\,]$

(b) Gilt mit $P, Q \in (R[x])^{n\times n}$

$$P(xE - A) = (xE - B)Q \tag{1}$$

dann ist zwangsläufig ${}^\bullet P(B) = Q^\bullet(A)$ und mit $T := {}^\bullet P(B) = Q^\bullet(A)$ gilt: $TA = BT$. Sind insbesondere $P, Q \in GL_n(R[x])$, dann ist $T \in GL_n(R)$.

Beweis. (i) Wir zeigen zuerst (b): Gelte (1) mit $P, Q \in (R[x])^{n\times n}$.
Nach Satz 10.2(d) gibt es $S, U \in (R[x])^{n\times n}$ und $R, V \in R^{n\times n}$ mit

$$P = (xE - B)U + V\,, \qquad V = {}^{\bullet}P(B) \tag{2a}$$
$$Q = S(xE - A) + R\,, \qquad R = Q^{\bullet}(A) \tag{2b}$$

Eingesetzt in (1) ergibt dies:

$$((xE - B)U + V)(xE - A) = (xE - B)(S(xE - A) + R)$$

bzw.:

$$\underbrace{(xE - B)(U - S)(xE - A)}_{\substack{\text{enthält Komponenten vom}\\ \text{Grad} \geq 2 \text{ sobald } U - S \neq 0}} = \underbrace{(xE - B)R - V(xE - A)}_{\substack{\text{enthält höchstens Komponenten}\\ \text{vom Grad 1, da } R, V \in R^{n\times n}.}}$$

Es folgt $U - S = 0$ und $(xE - B)R = V(xE - A)$, bzw.: $xR - BR = xV - VA$, bzw.: $R = V$ und $BR = VA$. Wir setzen $T := R = V = {}^{\bullet}P(B) = Q^{\bullet}(A)$.
Es bleibt zu zeigen:

wenn P, Q invertierbar sind, dann auch $T(= V = R)$.

Sei also $P \in GL(n, R[x])$. Wieder wegen Satz 10.2(d) gibt es $G \in (R[x])^{n\times n}$ und $H \in R^{n\times n}$ mit:

$$P^{-1} = (xE - A)G + H\,.$$

Damit ist (beachte (1), (2a)):

$$\begin{aligned} E = PP^{-1} &= P(xE - A)G + PH \\ &= (xE - B)QG + ((xE - B)U + V)H \\ &= (xE - B)(QG + UH) + VH\,. \end{aligned}$$

Mehrfache Anwendung von Satz 10.2(b) ergibt

$$QG + UH = 0 \quad \text{und} \quad E = VH\,.$$

Somit ist $\det V$ eine Einheit in R und damit V nach 8, Satz 8.1(m) invertierbar.

(ii) Nun zum Beweis von (a). "$\Longrightarrow$" ergibt sich mit (b). "$\Longleftarrow$:" Gelte mit $T \in GL_n(R)$: $TA = BT$, dann gilt auch

$$T(xE - A) = TxE - TA = xT - BT = (xE - B)T$$

und $T \in GL_n(R[x])$. □

11 Zum allgemeinen Normalformenproblem der linearen Algebra über Körpern

Sei K ein Körper.

Definition 11.1. *Eine Abbildung* $\boldsymbol{\mathcal{C}} : K^{n\times n} \longrightarrow K^{n\times n}$ *mit den Eigenschaften*

(i) $\boldsymbol{\mathcal{C}}(A) \approx A$ *für alle* $A \in K^{n\times n}$

(ii) $[\boldsymbol{\mathcal{C}}(A) = \boldsymbol{\mathcal{C}}(B)] \Longleftrightarrow [A \approx B]$ *für alle* $A, B \in K^{n\times n}$

heißt **kanonische Form bzgl.** $\approx$ *oder auch* **Normalform bzgl.** $\approx$.

Bemerkung. Es genügt in (ii) nur "$\Longleftarrow$" zu fordern. Wegen (i) gilt dann "$\Longrightarrow$" automatisch. Eine kanonische Form ist nach Definition 11.1 nichts anderes als eine Vertreterauswahlfunktion für $\approx$ (vgl. 1(G)).

Das allgemeine Normalformenproblem ist die Aufgabe, eine Normalform bzgl. $\approx$ anzugeben. Dieses Problem tauchte in der Linearen Algebra I auf im Zusammenhang mit der Suche nach möglichst einfachen Matrixdarstellungen für Endomorphismen endlich-dimensionaler Vektorräume.

Die Sätze 6.3 und 10.5 ermöglichen elementare Lösungen des Problems. Die wichtigsten behandeln wir im folgenden kurz.

Sei $A \in K^{n\times n}$ und sei $\boldsymbol{\mathcal{U}}$ das Vertretersystem aus Beispiel c) in Abschnitt 6 für die Äquivalenz in $K[x]$. Nach Satz 6.3 besitzt die charakteristische Matrix $(xE - A)$ eine bzgl. $\boldsymbol{\mathcal{U}}$ eindeutige Smith-Form. **Wir schreiben zur Abkürzung in diesem Paragraphen $\boldsymbol{d_i(A)}$ statt $\boldsymbol{d_i(xE - A)}$ für den $\boldsymbol{i}$-ten invarianten Faktor in der Smith-Form von $\boldsymbol{(xE - A)}$. Vorsicht:** $d_i(A)$ hat nichts mit "Einsetzen von A" zu tun! Es ist dann $(xE - A) \sim \operatorname{diag}(d_1(A), \ldots, d_n(A))$ mit

$$d_i(A) \in \boldsymbol{\mathcal{U}} \quad \text{für } 1 \le i \le n \quad \text{und} \quad d_i(A) \mid d_{i+1}(A) \quad \text{für } 1 \le i < n.$$

Zunächst stellt man fest:

(1) $\varphi_A = \det(xE - A) = d_1(A) \cdots d_n(A)$

(2) $d_i(A) \neq 0$ für $1 \le i \le n$

(3) $\sum_{i=1}^{n} \deg d_i(A) = n$ und $\deg d_i(A) \le \deg d_{i+1}(A)$ für $1 \le i < n$

(2) und (3) formulieren die zusätzlichen Beschränkungen, denen die invarianten Faktoren einer charakteristischen Matrix unterworfen sind. Ist z. B. $\deg d_1(A) = 1$, dann ist zwangsläufig $d_1(A) = \ldots = d_n(A)$.

Sei $s(A) := \min\{i : d_i \neq 1\}$ und

$$\boldsymbol{\mathcal{C}}(A) := \operatorname{diag}\left(C(d_{s(A)}(A)), \ldots, C(d_n(A))\right). \tag{1}$$

Dabei ist $C(d_i(A))$ die sogenannte **Begleitmatrix** zum Polynom $d_i(A)$.

Definition 11.2. *Die Begleitmatrix zu* $f = a_0 + \cdots + a_{n+1}x^{n-1} + x^n \in K[x]$ *ist:*

$$C(f) : \begin{bmatrix} 0 & \dots & 0 & -a_0 \\ 1 & & & \vdots \\ \vdots & \ddots & & \vdots \\ 0 & \dots & 1 & -a_{n-1} \end{bmatrix}$$

Satz 11.3. $\boldsymbol{\mathcal{C}}$*, wie in* (1) *definiert für* $A \in K^{n\times n}$*, ist eine Normalform bzgl.* $\approx$*, die sogenannte* **rationale kanonische Form** *oder* **erste kanonische Form** *oder auch* **Frobenius'sche Normalform** *(Georg Frobenius 1849-1917).*

Beweis. Zunächst bestätigt man mit vollständiger Induktion, dass gilt:

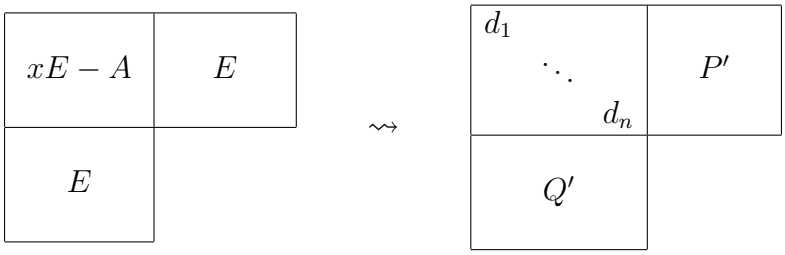
$$(xE - \boldsymbol{\mathcal{C}}(A)) \sim \operatorname{diag}(d_1(A), \dots, d_n(A)) .$$

Wegen Satz 10.5 folgt: $\boldsymbol{\mathcal{C}}(A) \approx A$. Die Eigenschaft (ii), in Definition 11.1 ergibt sich ebenfalls mit Hilfe von Satz 10.5 und der Eindeutigkeit der Smith-Form. □

Zur Organisation der Berechnung:

Gegeben ist $A \in K^{n\times n}$. **Gesucht** ist ein $T \in GL_n(K)$ mit $TAT^{-1} = \boldsymbol{\mathcal{C}}(A)$.

1. Schritt: **Äquivalente Umformung von $(xE - A)$ zur Smith-Form.**



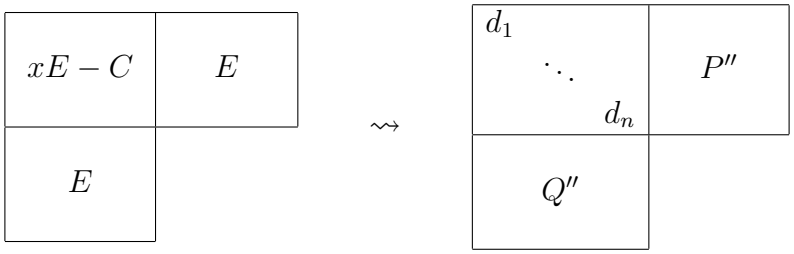
mit $d_i \mid d_{i+1}$ für $1 \le i < n$ und höchstem Koeffizienten 1. Es gilt dann:
$P'(xE - A)Q' = \operatorname{diag}(d_1, \dots, d_n)$ und $P', Q' \in GL_n(K[x])$. $\boldsymbol{\mathcal{C}}(A)$ kann jetzt angegeben werden:

$$\boldsymbol{\mathcal{C}}(A) = \operatorname{diag}(C(d_{s(A)}), \dots, C(d_n)) .$$

2. Schritt: **Bestimmung der Basiswechselmatrix T**

Völlig unabhängig vom jeweils vorgegebenen A können für beliebige
$d_1, \dots, d_n \in K[x]\backslash\{0\}$ mit höchstem Koeffizienten 1, mit $d_i \mid d_{i+1}$ für $1 \le i < n$ und mit $\sum_{i=1}^{n} \deg d_i = n$ Matrizen $P'', Q'' \in GL_n(K[x])$ bestimmt werden mit $P'' \operatorname{diag}(xE -$

$C)Q'' = \operatorname{diag}(d_1, \ldots, d_n)$, wobei $C = \operatorname{diag}(C(d_s), \ldots, C(d_n))$ und $s = \min\{i \mid d_i \neq 1\}$.



Insgesamt gilt dann – wenn $d_1, \ldots, d_n$ die invarianten Faktoren von $(xE - A)$ sind, d. h. wenn $C = \boldsymbol{\mathcal{C}}(A)$:

$$P'(xE - A)Q' = \operatorname{diag}(d_1, \ldots, d_n) = P''(xE - \boldsymbol{\mathcal{C}}(A))Q''$$

bzw.

$$\underbrace{(P''^{-1}P')}_{:=P}(xE - A) = (xE - \underbrace{\boldsymbol{\mathcal{C}}(A)}_{:=B})\underbrace{(Q''Q'^{-1})}_{:=Q} \tag{2}$$

Setze:

$$\boldsymbol{T := {}^{\bullet}P(B) = Q^{\bullet}(A)} \tag{3}$$

(vgl. Satz 10.5)

P'' ist formelmäßig aus den d_i bestimmbar und i. a. einfacher gebaut als Q'. Es gilt nun: $TA = \boldsymbol{\mathcal{C}}(A)T$. Letztere Beziehung kann als Rechenprobe benutzt werden.

Ein einfaches Rechenbeispiel: $K = \mathbb{Q}$

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \qquad (xE - A) = \begin{bmatrix} x-1 & -1 \\ 0 & x-1 \end{bmatrix}$$

$$\left[\begin{array}{cc|cc} x-1 & -1 & 1 & 0 \\ 0 & x-1 & 0 & 1 \\ \hline 1 & 0 & & \\ 0 & 1 & & \end{array}\right] \rightsquigarrow \left[\begin{array}{cc|cc} 1 & 0 & -1 & 0 \\ 0 & (x-1)^2 & x-1 & 1 \\ \hline 0 & 1 & \multicolumn{2}{c}{\multirow{2}{*}{$=P'$}} \\ 1 & x-1 & & \end{array}\right]$$

$=Q'$

Es gilt: $P'(xE - A)Q' = \operatorname{diag}(d_1, d_2)$ mit $d_1 = 1, d_2 = (x-1)^2 = x^2 - 2x + 1$. Nun ist $s(A) = 2$, $C(d_2) = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix}$ und $\boldsymbol{\mathcal{C}}(A) = C(d_2)$.

Mit $(xE - \boldsymbol{\mathcal{C}}(A))$ wird weiter gerechnet:

$$\left[\begin{array}{cc|cc} x & 1 & 1 & 0 \\ -1 & x-2 & 0 & 1 \\ \hline 1 & 0 & & \\ 0 & 1 & & \end{array}\right] \rightsquigarrow \left[\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & (x-1)^2 & x-2 & -1 \\ \hline 0 & 1 & \multicolumn{2}{c}{\multirow{2}{*}{$\underbrace{\qquad}_{=P''}$}} \\ 1 & -x & & \end{array}\right]$$

$$\underbrace{\qquad}_{=Q''}$$

Nun kann die Basiswechselmatrix T nach (2) und (3) bestimmt werden, z. B. so:

$$Q'^{-1} = \begin{bmatrix} 1-x & 1 \\ 1 & 0 \end{bmatrix}, Q = \begin{bmatrix} 1 & 0 \\ 1-2x & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ -2 & 0 \end{bmatrix} x + \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\text{und schließlich} \quad T = Q^{\bullet}(A) = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}$$

oder wie folgt:

$$P''^{-1} = P'' \quad \text{und} \quad P = \begin{bmatrix} -1 & 0 \\ -2x+3 & -1 \end{bmatrix} = x \begin{bmatrix} 0 & 0 \\ -2 & 0 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 3 & -1 \end{bmatrix}$$

$$\text{und dann ebenfalls} \quad T = {}^{\bullet}P(\boldsymbol{\mathcal{C}}(A)) = \begin{bmatrix} 1 & 0 \\ -1 & -1 \end{bmatrix}.$$

Weitere Normalformen: Sei $d \in K[x]$, d nicht konstant mit höchstem Koeffizienten 1. Es gibt dann eine Zerlegung

$$d = p_1^{\alpha_1} \dots p_m^{\alpha_m} \tag{4}$$

mit paarweise verschiedenen unzerlegbaren normierten Polynomen $p_1, \dots, p_m$ und $\alpha_i \in \mathbb{N}$. In den Übungsaufgaben können sie mit Hilfe Satz 10.5 bestätigen, daß gilt:

$$C(d) \approx \operatorname{diag}(C(p_1^{\alpha_1}), \dots, C(p_m^{\alpha_m})) \tag{5}$$

Die Darstellung (4) ist nur eindeutig bis auf die Reihenfolge der Faktoren $p_i^{\alpha_i}$. Entsprechend taucht bei (5) die Frage auf, in welcher Reihenfolge die Blöcke $C(p_i^{\alpha_i})$ aufgeführt werden sollen. Bei der rationalen kanonischen Form tauchte ein vergleichbares Problem **nicht** auf, da die normierten invarianten Faktoren durch ihre Teilungsbeziehung auf natürliche Weise geordnet sind. Will man die Elementarteiler zur Grundlage einer Normalform machen, muß zuerst eine Anordnung der Primpolynome gefunden werden, da sonst eine Eindeutigkeit nicht möglich ist. Dies hat ganz praktische Bedeutung. Jedes Hilfsprogramm zur Berechnung einer Normalform muß

das Ergebnis ja in einer wohl definierten Form ausgeben können! Wir setzen daher zusätzlich voraus:

LO: Auf der Menge der normierten Primpolynome in $K[x]$ sei eine lineare Anordnung vorgegeben.

Ist dies der Fall, dann kann die Familie der Elementarteiler von $(xE-A)$, $A \in K^{n\times n}$ auf eindeutige Weise angeordnet werden. Diese geordnete Liste der Elementarteiler von $(xE-A)$ sei $\varepsilon_1(A),\ldots,\varepsilon_t(A)$, wobei jedes ε_i Primpolynompotenz ist. Nun sei

$$\boldsymbol{\mathcal{E}}(A) := \operatorname{diag}(C(\varepsilon_1(A)),\ldots,C(\varepsilon_t(A))) \tag{6}$$

Satz 11.4. *Erfüllt $K[x]$ die Zusatzvoraussetzung LO, dann ist $\boldsymbol{\mathcal{E}} : K^{n\times n} \longrightarrow K^{n\times n}$ eine Normalform, die sogenannte* **2. Normalform** *oder auch* **Weierstraß'sche Normalform** *(Karl Theordor Wilhelm Weierstraß 1815-1897).*

Die Blöcke $C(p^\alpha)$ mit $\alpha > 1$ in (5) können noch weiter unterteilt werden. Es gilt nämlich:

$$C(p^\alpha) \approx \overbrace{\begin{bmatrix} C(p) & & 0 & 0 \\ E_{1\delta} & C(p) & & 0 \\ 0 & & E_{1\delta} & C(p) \end{bmatrix}}^{\alpha \text{ Blockspalten}} := J_\alpha(p) \tag{7}$$

wobei $\delta = \deg p$ und $C(p) \in K^{\delta\times\delta}$

$$E_{1\delta} = \begin{bmatrix} 0 & \ldots & \ldots & 1 \\ \vdots & & & \vdots \\ 0 & & & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix} \in K^{\delta\times\delta}\,.$$

Falls $\alpha = 1$ setzen wir $J_1(p) = C(p)$.

Sind nun

$$\varepsilon_1(A) = p_1^{\alpha_1},\ldots,\varepsilon_t(A) = p_t^{\alpha_t}$$

die (aufgrund von LO) angeordneten Elementarteiler von $(xE-A)$, so sei

$$\boldsymbol{\mathcal{J}}(A) := \operatorname{diag}(J_{\alpha_1}(p_1),\ldots,J_{\alpha_t}(p_t))$$

Satz 11.5. *Erfüllt $K[x]$ die Zusatzvoraussetzung, dann ist $\boldsymbol{\mathcal{J}} : K^{n\times n} \longrightarrow K^{n\times n}$ eine Normalform, die sogenannte* **Jacobson-Normalform** *(Nathan Jacobson 1910-1999).*

Bemerkungen. (i) Die **Jordan'sche Normalform** (Camille Jordan 1838-1922) ist der Sonderfall der Jacobson'schen Normalform, wenn in $K[x]$ jedes Polynom Produkt linearer Polynome ist (bzw. wenn in $K[x]$ jedes unzerlegbare Polynom linear ist), was z.B. für $K = \mathbb{C}$ der Fall ist. Die einzigen unzerlegbaren Polynome sind dann die Polynome $p = x - \lambda$, $\lambda \in K$. Für solche p ist $C(p) = C(x-\lambda) = (\lambda)$ eine 1×1-Matrix und jede(r) kann nun selbst feststellen, daß in diesem Sonderfall $J(A)$ in

Jordan'scher Form ist wie sie z. B. in [Fi] eingeführt wird. Satz 11.5 ergibt natürlich auch dafür die Normalform-Eigenschaft.

(ii) Die 2. Normalform setzt die Kenntnis der Primzerlegung der invarianten Faktoren voraus. Die Berechnung einer solchen Zerlegung ist zwar möglich (z. B. wenn $K = Q$ oder K endlich) aber meistens sehr aufwendig.

Bemerkungen zur geometrischen Interpretation der 1. u. 2. Normalform. Sei F Endomorphismus eines n-dimensionalen K-Vektorraumes V. Ein Vektor $v \in V$ heißt ***F*-zyklisch**, wenn $v, F(v), \ldots, F^{n-1}(v)$ eine Basis von V ist. Bezüglich einer solchen ***F*-zyklischen Basis** ist die Matrix von F eine Begleitmatrix. Nicht jeder Endomorphismus von V besitzt einen F-zyklischen Vektor. Dies folgt unmittelbar aus Satz 11.3! Andererseits besitzt zu jedem $v \in V$, $v \neq 0$, der Untervektorraum $\mathrm{Span}(F^i(v))_{i\geq 0}$ die F-zyklische Basis:

$$v, \ldots, F^{k-1}(v) \quad \text{mit } k = \min\{i \in \mathbb{N} : F^{(i)}(v) \in \mathrm{Span}\{v \ldots, F^{i-1}(v)\}\}.$$

Die Unterräume der Form $\mathrm{Span}(F^i(v))_{v\geq 0}$ für $v \in V$ heißen F-zyklisch.

Satz 11.6.

(i) Die rationale kanonische Form entspricht einer Zerlegung von V in eine direkte Summe von möglichst wenigen F-zyklischen Unterräumen:

$$V = V_1 \oplus \cdots \oplus V_S$$

(ii) Die zweite kanonische Form entspricht einer Zerlegung von V in eine direkte Summe von möglichst vielen F-zyklischen Unterräumen.

Diese geometrische Interpretation unserer Normalformen ist direkt verbunden mit der modultheoretischen, wie sie in Kapitel 3 gegeben werden kann.

Eine klassische Literaturstelle zu diesem Thema ist [Ga].

Kapitel III

Moduln über euklidischen Ringen

12 Grundbegriffe und erste Resultate

Sei R stets kommutativ und $\neq \{0\}$. Für die Definition von R-Moduln und Untermoduln wird auf Abschnitt 1(B) verwiesen.

Beispiele.

(a) Trivialfall: $M = \{0\}$;

(b) K-Vektorräume;

(c) $\mathbb{Q}$ als $\mathbb{Z}$-Modul, $\mathbb{Z}$-Untermoduln von $\mathbb{Q}^n$, "Gitter";

(d) $R[x]$ als R-Modul;

(e) R^n, $n \geq 1$;

(f) $R^{n \times n}$ als R-Modul;

(g) $Abb(X, R^n)$ mit einer nichtleeren Menge X;

(h) abelsche Gruppen, insbesondere $\mathbb{Z}_n$ sind $\mathbb{Z}$-Moduln (siehe Abschnitt 1);

(i) R-Moduln sind $\mathbb{Z}$-Moduln und für u. U. gewisse n auch $\mathbb{Z}_n$-Moduln;

(j) K-Vektorräume als $K[x]$-Moduln bzgl. eines Endomorphismus; siehe weiter unten in einem eigenen Abschnitt.

Wichtig: Ist $K = R$ ein Körper, dann ist der Begriff des K-Moduls identisch mit dem Begriff des K-Vektorraumes. Der Modulbegriff ist eine Verallgemeinerung des Vektorraumbegriffs.

Jeder R-Modul ist insbesondere auch ein $\mathbb{Z}$-Modul.

Definition 12.1. *(Z.T. Wiederholung) Sei M ein R-Modul.*

(a) $v \in M$ *heißt* **Torsionselement**, *wenn es ein* $r \in R$ *gibt mit* $rv = 0$ *und* $r \neq 0$.

(b) $\boldsymbol{t(M)} := \{v \in M : v \text{ Torsionselement } \}$

(c) *Gilt* $t(M) = M$, *heißt* M **Torsionsmodul.**

(d) *Gilt* $t(M) = \{0\}$, *heißt* M **torsionsfrei.**

Stets ist $0 \in t(M)$, *da* $R \neq \{0\}$.

Satz 12.2. *(Wiederholung) Sei* R *nullteilerfrei und* M *ein* R*-Modul. Dann ist* $t(M)$ *ein Untermodul von* M.

Beispiel. $t(\mathbb{Z}_6) = \{0, 2, 4, 3\}$ (mit $\mathbb{Z}_6$ als $\mathbb{Z}_6$-Modul), aber $4 \oplus 3 \notin t(\mathbb{Z}_6)$

Ein (Unter-) Modul muss mit je endlich vielen Elementen auch deren Linearkombinationen bzw. deren Aufspann enthalten:

Definition 12.3. *Sei* M *ein* R*-Modul und* $X = (X_\nu)_{\nu \in I}$ *eine nichtleere Familie von Elementen aus* M. *Der* **von** $\boldsymbol{X}$ **aufgespannte Untermodul von** $\boldsymbol{M}$ *ist*

$$\mathbf{Span_R(X)} := \left\{ \sum_{i=1}^{m} \lambda_i \, x_{\nu_i} : m \in \mathbb{N};\, \nu_1, \ldots, \nu_m \in I;\, \lambda_1, \ldots, \lambda_m \in R \right\}$$

Im Sonderfall: $X = (x_1, \ldots, x_m)$ *schreiben wir*

$$\mathrm{Span}_R(x_1, \ldots, x_m) := \mathrm{Span}_R(X) = \left\{ \sum_{i=1}^{m} \lambda_i \, x_i : \lambda_1, \ldots, \lambda_m \in R \right\}.$$

Man setzt fest: $\mathrm{Span}_R(\varnothing) = \{0\}$.

Beobachtung. $\mathrm{Span}_R(X)$ ist stets ein Untermodul. Stets gilt: $\mathrm{Span}_R(0) = \{0\}$ und $\mathrm{Span}_R(M) = M$.

Definition 12.4. *Sei* M *ein* R*-Modul und* X *eine nichtleere Familie von Elementen aus* M. X *heißt* **Erzeugendensystem von** $\boldsymbol{M}$, *wenn gilt:* $\mathrm{Span}_R(X) = M$. M *heißt* **endlich erzeugt** *oder* **endlich erzeugbar**, *wenn es ein endliches Erzeugendensystem von* M *gibt, d.h. wenn es* $m \in \mathbb{N}$ *und* $x_1, \ldots, x_m \in M$ *gibt mit* $M = \mathrm{Span}_R(x_1, \ldots, x_m)$. *Gilt* $\mathrm{Span}_R(X) = M$, *so sagt man auch:* $\boldsymbol{X}$ **erzeugt** $\boldsymbol{M}$. *Gilt* $\mathrm{Span}_R(x_1, \ldots, x_m) = M$, *so sagt man auch:* $\boldsymbol{x_1, \ldots, x_m}$ **erzeugen** $\boldsymbol{M}$.

Beispiele.

(a) $a \in R:\ aR = \mathrm{Span}_R(a)$

(b) $R^n = \mathrm{Span}_R(e_1, \ldots, e_n)$

(c) $\mathbb{Z}_6 = \mathrm{Span}_{\mathbb{Z}}(5)$

(d) $R[x]$, $X = (x^\nu)_{\nu\in\mathbb{N}}$, $R[x] = \mathrm{Span}_R(X)$

(e) $R^{n\times n} = \mathrm{Span}_R(E_{11}, \ldots, E_{nn})$

Auch die folgende Definition ist identisch zu derjenigen in der Linearen Algebra I.

Definition 12.5. *Sei M ein R-Modul. Eine endliche Familie $v_1, \ldots, v_r$ von "Vektoren" aus M (bzw. die Vektoren $v_1, \ldots, v_r \in M$ heißt (bzw. heißen)* **linear unabhängig** *(**über R** oder R-linear unabhängig), falls gilt: Sind $\lambda_1, \ldots, \lambda_r \in R$ und ist*

$$\lambda_1 v_1 + \cdots + \lambda_r v_r = 0$$

so folgt:

$$\lambda_1 = \cdots = \lambda_r = 0\,.$$

Die Familie bzw. die Vektoren heißen linear abhängig, wenn sie nicht linear unabhängig sind.

Definition 12.6. *Sei M ein R-Modul und X eine nichtleere Familie von Elementen aus M.*

(i) X heißt l.a., wenn X eine endliche l.a.-e Teilfamilie enthält.

(ii) X heißt l.u., wenn jede endliche Teilfamilie von X l.u. ist, m. a. W., wenn X nicht l.a. ist.

Beobachtung. Ist die Familie X l.a. (l.u.), dann ist auch jede durch Umordnung (Permutation) aus X hervorgehende Familie l.a. (l.u.).

Definition 12.7. *Sei M ein R-Modul und X eine nichtleere Familie von Elementen aus R. X heißt* **Basis** *von M, wenn gilt:*

(i) $\mathrm{Span}_R(X) = M$

(ii) X ist l.u.

Ein R-Modul, der eine Basis besitzt, heißt **frei.**

Satz 12.8. *Eine Basis ist eine unverkürzbares Erzeugendensystem und eine unverlängerbare linear unabhängige Familie. Anders als in der linearen Algebra über Körpern gelten jetzt die Umkehrungen i.A. nicht mehr.*

Beispiele.

(a) $(e_1, \ldots, e_n)$ ist eine Basis von R^n, insbesondere ist 1 eine Basis von R.

(b) Zwar ist in $\mathbb{Z}_d$ stets $\mathrm{Span}_{\mathbb{Z}}(1) = \mathbb{Z}_d$, da aber $d \cdot 1 = \underbrace{1 \oplus \ldots \oplus 1}_{d-\text{mal}} = 0$, ist 1 in $\mathbb{Z}_d$ (aufgefasst als $\mathbb{Z}$-Modul) ein unverkürzbares Erzeugendensystem aber keine Basis.

(c) X aus dem vorangehenden Beispiel (d) ist eine Basis von $R[x]$.

(d) $(E_{11}, \ldots, E_{nn})$ ist eine Basis von $R^{n\times n}$.

(e) $(2e_1, \ldots, 2e_n)$ ist eine nicht verlängerbare linear unabhängige Familie in $\mathbb{Z}^n$ aber keine Basis von $\mathbb{Z}^n$!

(f) Ein Torsionselement kann nicht Teil einer Basis sein!

Neben den $\mathbb{Z}$-Moduln spielen die $K[x]$-Moduln (K ein Körper) eine wichtige Rolle. Im folgenden Abschnitt wird gezeigt, wie solche Moduln auf natürliche Weise in der linearen Algebra und dadurch in deren Anfwendungen auftauchen:

K-Vektorräume als $K[x]$-Moduln bezüglich eines Endomorphismus.

Sei K ein Körper, V ein K-Vektorraum und $F : V \longrightarrow V$ eine lineare Abbildung, kurz: $F \in L(V) := Hom_K(V, V)$. $L(V)$ ist ein Ring bzgl. $+, \circ$ und ein K-Vektorraum. Zunächst einmal stellt man fest, daß K in den Ring $L(V)$ eingebettet werden kann durch die Vorschrift: $k \mapsto k \cdot \mathrm{id}_V$ (id_V = identische Abbildung von V). Jedes $F \in L(V)$ wird dadurch einsetzbar in Polynome aus $K[x]$ (vgl. Abschnitt 3, Beispiel (b), S. 24. Durch folgende Vorschrift wird jetzt eine Verknüpfung $K[x] \times V \longrightarrow V$ festgelegt:

Für alle $p \in K[x]$ und $v \in V$ sei:

$$pv := (p(F))(v)\,.$$

Ist etwa $p = \sum_{i=0}^{d} k_i x^i$, dann ist $pv = \left(\sum_{i=0}^{d} k_i F^i\right)(v) = \sum_{i=0}^{d} k_i (F^i)(v)$. Dabei ist $F^0 = id_V$. Man bestätigt leicht, dass K^n mit dieser Skalarmultiplikation zum $K[x]$-Modul wird.

Sprechweise. V ist $K[x]$-Modul bezüglich F.

Beispiele.

(a) $V = K^{n\times 1}$, $A \in K^{n\times n}$, $F : V \longrightarrow V$ mit $F(v) = Av$

Der $K[x]$-Modul $K^{n\times 1}$ bzgl. A ist ein endlich erzeugter Torsionsmodul, denn es ist

$$K^{n\times 1} = K[x]e_1 + \ldots + K[x]e_n$$

und wegen des Satzes von Cayley-Hamilton gilt: $\varphi_A v = 0$ für alle $v \in K^{n\times 1}$.

$$\text{Ist etwa } A = \begin{bmatrix} 0 & & \ldots & * \\ 1 & \ddots & & \vdots \\ \vdots & \ddots & 0 & * \\ 0 & \ldots & 1 & * \end{bmatrix}, \text{ dann gilt sogar:}$$

$$K^{n\times 1} = K[x]e_1\,. \tag{1}$$

(b) $V = C^\infty(\mathbb{R}), K = \mathbb{R}, D : V \longrightarrow V$ mit $Df = f'$.

Es ist $D \in L(V)$ und o.E. $\mathbb{R} \subset L(V)$. Mit obiger Skalarmultiplikation wird V zum $K[x]$-Modul bezüglich D. Man stellt fest: $f \in V$ ist Torsionselement genau dann, wenn f Lösung einer linearen Differentialgleichung mit konstanten Koeffizienten ist.

(c) Wie (b) aber mit zwei Variablen und mit partiellen Ableitungen.

Definition 12.9. *Ein R-Modul M heißt* **zyklisch**, *wenn mit einem $v \in M$ gilt $M = Rv$.*

Beispiele.

(a) R als R-Modul ist zyklisch: $R = R \cdot 1$.

Die zyklischen R-Untermoduln von R sind gerade die Hauptideale.

(b) siehe oben (1).

(c) $\mathbb{Z}_d$ ist zyklisch als $\mathbb{Z}_d$-Modul (vgl. (a)) aber auch als $\mathbb{Z}$-Modul.

Einige elementare (für beliebige kommutative Ringe $\neq \{0\}$ gültige) Ergebnisse der linearen Algebra:

Satz 12.10. *Sei R ein kommutativer Ring ($\neq \{0\}$) und M ein R-Modul.*

(a) Ist M endlich erzeugbar, dann enthält jedes Erzeugendensystem von M ein endliches Erzeugendensystem.

(b) Ist M endlich erzeugbar, dann kann M allenfalls eine endliche Basis besitzen.

(c) Ein endliches Erzeugendensystem von M ist stets mindestens so lang wie eine Basis, **falls** *eine solche existiert.*

(d) Besitzt M eine endliche Basis der Länge r, so hat jede weitere Basis ebenfalls die Länge r.

(e) Besitzt M eine endliche Basis der Länge r, so ist jedes Erzeugendensystem der Länge r eine Basis.

(f) Ist R Bereich und M endlich erzeugt, dann sind alle maximalen l.u. Familien gleich lang.

Bemerkung (zu (e)). Besitzt M eine (nicht notwendig) endliche Basis und läßt man ein Basiselement weg, so entsteht wieder eine l.u. Familie, die aber M nicht mehr erzeugt. In diesem Sinne ist eine Basis (sozusagen per Definition) minimal. Satz 12.10(e) besagt wesentlich mehr!

Beweis.

(a) Sei $(m_1, \ldots, m_r)$ ein endliches Erzeugendensystem von M und $(n_i)_{i\in I}$ ein weiteres Erzeugendensystem von M. Dann ist z.B̃. $m_1 \in \mathrm{Span}_R(n_i)_{i\in I}$ bzw. $m_1 = \sum_{\nu=1}^{s} \lambda_\nu\, n_{i_\nu} \quad (\lambda_\nu \in R)$ mit geeigneten **endlich vielen** Indizes $i_\nu \in I$.

Analog für $m_2, \ldots, m_r$. Es werden also insgesamt nur endlich viele Elemente der Familie $(n_i)_{i\in I}$ benötigt, um die m_i als Linearkombination darzustellen. Dies seien etwa $n_{i_1}, \ldots, n_{i_t}$. Es gilt dann:

$$M = \mathrm{Span}_R(n_i)_{i\in I} \supseteq \mathrm{Span}_R(n_{i_1}, \ldots, n_{i_t}) \supseteq \mathrm{Span}_R(m_1, \ldots, m_r) = M$$

Die $n_{i_1}, \ldots, n_{i_t}$ bilden daher ein endliches Teilerzeugendensystem.

(b) ergibt sich direkt aus (a).

(c) Sei $(m_1, \ldots, m_r)$ ein Erzeugendensystem von M und $(n_1, \ldots, n_s)$ eine Basis von M. Zu zeigen: $r \geq s$. Es gilt dann:

$$m_i = \sum_{\mu=1}^{s} a_{i\mu} n_\mu \quad \text{und} \quad n_j = \sum_{\nu=1}^{r} b_{j\nu} m_\nu \tag{2}$$

für $1 \leq i \leq r$ und $1 \leq j \leq s$ und mit geeigneten $a_{i\mu}, b_{i\nu} \in R$. Einsetzen ergibt für $1 \leq j \leq s$:

$$n_j = \sum_{\nu=1}^{r} b_{j\nu} \sum_{\mu=1}^{s} a_{\nu\mu} n_\mu = \sum_{\mu=1}^{s} \left(\sum_{\nu=1}^{r} b_{j\nu} a_{\nu\mu} \right) n_\mu$$

Da $(n_1, \ldots, n_s)$ eine Basis sein sollte, folgt

$$\sum_{\nu=1}^{r} b_{j\nu} a_{\nu\mu} = \left\{ \begin{array}{ll} 0 & j \neq \mu \\ 1 & j = \mu \end{array} \right\} \tag{3}$$

$A := (a_{i\mu})$ und $B := (b_{j\nu})$ ($A \in R^{r\times s}$ und $B \in R^{s\times r}$) genügen daher der Beziehung

$$B\,A = E$$

Wäre nun $s > r$, dann würde mit

$$\overline{B} := [\,B, 0\,] \quad \text{und} \quad \overline{A} := \left[\begin{array}{c} A \\ 0 \end{array} \right] \in R^{s\times s}$$

gelten:

$$\overline{B}\;\overline{A} = E$$

und damit auch:

$$det(\overline{B}\;\overline{A}) = det\,\overline{B} \cdot det\,\overline{A} = det\,E = 1$$

Offensichtlich ist aber $det\,\overline{B} = det\,\overline{A} = 0$. Da $R \neq \{0\}$ vorausgesetzt wurde, liegt ein Widerspruch vor. Der Fall $s > r$ kann also nicht eintreten.

(d) ergibt sich direkt aus (c).

(e) Im Beweis von (c) können wir jetzt von vorneherein $\nu = s$ annehmen. Dann sind $A, B \in R^{s\times s}$ und wegen der Beziehung $BA = E$ sogar $A, B \in GL_s(R)$. Wenn nun $0 = \sum_{i=1}^{s} \lambda_i m_i$ und $\lambda_1, \ldots, \lambda_s \in R$, dann folgt:

$$0 = \sum_{i=1}^{s} \lambda_i m_i = \sum_{i=1}^{s} \lambda_i \sum_{\mu=1}^{s} a_{i\mu} n_\mu = \sum_{\mu=1}^{s} \left(\sum_{i=1}^{s} \lambda_i a_{i\mu} \right) n_\mu \,.$$

Da $(n_1, \ldots, n_s)$ l.u. ist dies nur möglich, wenn ${}^t\lambda A = 0$. Da $A \in GL_n(R)$ folgt $\lambda = 0$.

(f) Beweis unter der Voraussetzung, dass eine Basis existiert:
Wenn im Beweis von (c) die Familie $(m_1, \ldots, m_r)$ maximal linear unabhängig ist, dann gibt es für $1 \le j \le s$ jeweils ein $\lambda_j \in R\backslash\{0\}$ derart, dass $\lambda_j n_j = \sum_{\nu=1}^{r} b_{j\nu} m_\nu$ mit geeigneten $b_{j\nu} \in R$. Die Beziehungen (2) gelten daher mit $\lambda_j n_j$ statt n_j vor der zweiten Gleichung. Folgt man nun dem Beweis von (c), so erhält man in (3) λ_j statt 1 und am Ende den gleichen Widerspruch, denn $\det \overline{BA} = \lambda_1 \cdot \cdots \cdot \lambda_s \neq 0$, da jetzt R als Bereich vorausgesetzt ist.
In der Vorlesung wird der Beweis ohne Zusatzvoraussetzung geführt.

□

Beispiele.

(a) (2) ist eine nicht verlängerbare (maximale) linear unabhängige Familie von $\mathbb{Z}$ als $\mathbb{Z}$-Modul. (2) ist keine Basis.

(b) $\left(\begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 2 \\ 4 \end{bmatrix} \right)$ ist l.u.: $\left(\begin{bmatrix} 1 \\ 3 \end{bmatrix}, \begin{bmatrix} 1 \\ 4 \end{bmatrix} \right)$ ist Basis in $\mathbb{Z}^2$.

(c) (2,3) ist ein unverkürzbares Erzeugendensystem von $\mathbb{Z}$.

Definition 12.11. *Besitzt der R-Modul M eine endliche Basis, dann sei:*

$$\begin{aligned} \dim_R M &:= \textbf{\textit{R}-Dimension von } \textbf{\textit{M}} \\ &:= \textbf{Länge einer Basis von } \textbf{\textit{M}} =: \textbf{Rang von } \textbf{\textit{M}} \end{aligned}$$

Wegen Satz 12.10 ist $\dim_R M$ *wohldefiniert.*

Beobachtung. Ist R nullteilerfrei und existiert im R-Modul M eine endliche Basis, so gilt wegen Satz 12.10(f):

$$\dim_R M = \text{ Länge einer maximalen l. u. Familie}$$

Beispiele.

(a) $\dim_R R^n = n$, insbesondere $\dim_R R = 1$;

(b) Sei $0 \neq a \in R$ und a kein Nullteiler, dann ist $\dim_R(aR^n) = n$.

Wichtigstes Hilfsmittel bei der Bestimmung von Basen sind auch bei Moduln die **elementaren Umformungen.** Das liegt **u.a.** an folgendem

Satz 12.12. *Seien $m_1, \ldots, m_t$ Elemente des R-Moduls M und $m'_1, \ldots, m'_t$ Elemente, die durch elementare Umformungen aus $m_1, \ldots, m_t$ hervorgehen, dann ist*

$$\mathrm{Span}_R(m_1, \ldots, m_t) = \mathrm{Span}_R(m'_1, \ldots, m'_t)$$

Im Falle $M = R^{1\times n}$ entsprechen die elementaren Umformungen bei $m_1, \ldots, m_t$ den elementaren Zeilenumformungen bei der Matrix $\begin{bmatrix} m_1 \\ \vdots \\ m_t \end{bmatrix}$, im Fall $M = R^{n\times 1}$ den elementaren Spaltenumformungen bei der Matrix $[m_1, \ldots, m_t]$.

Satz 12.12 nützt nur dann etwas, wenn durch elementare Umformungen das zu lösende Problem (z.B. Basisbestimmung für $\mathrm{Span}_R(m_1, \ldots, m_t)$) vereinfacht wird. So lange der Grundring R beliebig, läßt sich hierüber nicht viel aussagen.

13 R^n und Untermoduln von R^n, R euklidisch

Die schönen und elementaren Ergebnisse von 12 könnten zu der Annahme verleiten, daß generell über kommutativen Ringen doch alles so ähnlich verläuft wie in Linearer Albegra I über Körpern.

Daß dies ganz und gar nicht der Fall ist, wird an folgenden Beispielen (insbesondere (c) im Vergleich zu (a) und (b)) deutlich:

Beispiele (Untermoduln von R^n für $n = 1$).

(a) K Körper. $\{0\}$, K sind die einzigen K-Untermoduln (= K-Untervektorräume) von K; $\dim_K K = 1$.

(b) R euklidisch. Die einzigen R-Untermoduln (= Ideale) sind hier $\{0\}$, Ra mit $0 \neq a \in R$. Es gilt $\dim_R Ra = 1$, falls $a \neq 0$.

(c) $R = \mathrm{Abb}(\mathbb{N}, K) = \{(k_i)_{i\in\mathbb{N}} : k_i \in K\}$, K Körper, komponentenweise Addition und Multiplikation. Wie immer sind $\{0\}$, R Untermoduln und $\dim_R R = 1$. $U = \{(k_i)_{i\in\mathbb{N}} : k_i \neq 0$ nur für endlich viele $i\}$ ist ein R-Untermodul von R, der nicht endlich erzeugt werden kann.

(d) $R = K[x, y]$, $U = \mathrm{Span}_R(x, y)$.

Bei Moduln über euklidischen Ringen sind zumindest Untermoduln von R höchstens 1-dimensional (s.o. b)), und wie sich weiter unten zeigen wird (Satz 13.1) besitzen auch Untermoduln von R^n stets Basen und zwar höchstens der Länge n. Letzteres ließe sich allerdings auch noch für Hauptidealringe beweisen. Die besondere Bedeutung der euklidischen Ringe liegt auch hier wieder darin, dass nicht nur Existenzaussagen (z.B. für Basen) gemacht werden, sondern auch explizite Rechenverfahren angegeben werden können. Diese sind immer dann praktisch umsetzbar, wenn Division mit Rest, $+$ und $\cdot$ in endlich vielen Schritten durchgeführt werden kann, bzw. wenn der euklidische Ring effektiv ist.

Sei ab jetzt R **euklidisch.**

Satz 13.1. *R euklidisch, U Untermodul von R^n. Dann kann U von endlich vielen (genauer sogar von n Elementen) erzeugt werden.*

Beweis. Induktion nach n für $R^{n\times 1}$ bzw. in Spaltenschreibweise.
$n = 1$: siehe obiges Beispiel (b)
$n \geq 1$: Sei U ein Untermodul von $R^{(n+1)\times 1}$ und $U_0 := \{u \in U : u_{n+1} = 0\}$. U_0 ist ein Untermodul von U bzw. R^{n+1}, und es gilt:

$$U_0 \subset \{v \in R^{n+1} : v_{n+1} = 0\} = R^{n\times 1} \times \{0\}$$

Sei $U_0' = \{u' \in R^{n\times 1} : \left[\begin{smallmatrix} u' \\ 0 \end{smallmatrix}\right] \in U_0\}$. U_0' ist Untermodul von $R^{n\times 1}$. Nach Induktionsannahme ist U_0' von n Elementen erzeugbar, etwa von $u'^{(1)}, \ldots, u'^{(n)}$. Offensichtlich ist $u^{(1)}, \ldots, u^{(n)}$ mit $u^{(i)} = \left[\begin{smallmatrix} u'^{(i)} \\ 0 \end{smallmatrix}\right]$ ein Erzeugendensystem von U_0 der Länge n. (u.U.: $u^{(1)} = \ldots = u^{(n)} = 0$, wenn $U_0 = \{0\}$).

1. Fall: $U_0 = U$, dann ist also U selbst schon von n Elementen erzeugbar.

2. Fall: $U_0 \neq U$. Es gibt dann ein $u^* \in U$ mit den Eigenschaften:

$$u^*_{n+1} \neq 0$$

und für alle $u \in U$ mit $u_{n+1} \neq 0$ gilt $\delta(u^*_{n+1}) \leq \delta(u_{n+1})$ □

Beh.: $U = Ru^* + U_0$

Beweis. $\supseteq$ ist klar, da $U_0 \subset U$, $u^* \in U$.
$\subseteq$: Sei $u \in U$. Ist $u_{n+1} = 0$, dann ist $u \in U_0$. Ist $u_{n+1} \neq 0$, dann gibt es $r, s \in R$ mit

$$u_{n+1} = su^*_{n+1} + r\,, \quad \text{wobei} \quad r = 0 \quad \text{oder} \quad \delta(r) < \delta(u^*_{n+1})$$

Mit u ist auch $u - su^* = \begin{bmatrix} * \\ \vdots \\ * \\ r \end{bmatrix} \in U$. Es muß, wegen der Wahl von u^*, $r = 0$ sein. Also gilt: $u - su^* \in U_0$ bzw. $u \in Ru^* + U_0$.

Da U_0 von n Elementen erzeugt werden kann, genügen $n+1$, um U zu erzeugen. □

Satz 13.2. *R euklidisch, U Untermodul von R^n. Dann besitzt U eine endliche Basis und es gilt:* $\dim_R U \leq n$.

Zum **Beweis** wird Satz 13.1 und die Hermiteform (Abschnitt 6) herangezogen. **Beachte,** daß trotzdem etwa der **Basisergänzungssatz** i. A. **nicht** gilt. D.h., daß i.A. die aufgrund von Satz 13.1 stets existierende Basis eines Untermoduls U von R^n nicht zu einer Basis des R^n erweitert werden kann. Trotzdem kann u.U. eine Basis von U verlängert werden zu einer größeren l.u. Familie. Auch das sieht man direkt an der Hermiteform. Z. B. ist $(2e_2, 3e_3)$ l.u. in $\mathbb{Z}^3$, aber nicht zu einer Basis ergänzbar. Allgemein gilt, daß die Zeilen einer Matrix in Hermiteform stets zu einer Familie aus n l.u. Vektoren ergänzt werden können, diese ist dann maximal l.u. ohne i.A. Basis zu sein.

Ebenso gilt der **Basisaustauschsatz** i. A. **nicht**. Z.B. sind (e_1, e_2) und $([\begin{smallmatrix}2\\3\end{smallmatrix}], [\begin{smallmatrix}1\\2\end{smallmatrix}])$ Basen von $\mathbb{Z}^2$. Aber nur $(e_2, [\begin{smallmatrix}1\\2\end{smallmatrix}])$ ist auch noch Basis von $\mathbb{Z}^2$.

Erfreulicherweise hat man aber trotzdem die aus der Linearen Algebra I vertraute Dimensionsformel:

Satz 13.3. *R* euklidisch. *Seien U, W Untermoduln von R^n, dann gilt:* $\dim_R U + \dim_R W = \dim_R(U + W) + \dim_R(U \cap W)$.

Bemerkung. Mit Hilfe von Satz 13.2 lässt sich zeigen, dass Satz 5.3 auch für euklidische Ringe noch gilt.

14 Lösung der Grundaufgaben für Untermoduln

Wir haben jetzt alle Hilfsmittel zur Verfügung, um folgende Grundaufgaben der Linearen Algebra über euklidischen Ringen zu lösen:

(1) Sind $u_1, \ldots, u_r$ linear unabhängig?

(2) Liegt $u \in \mathrm{Span}(u_1, \ldots, u_r)$?

(3) Basisbestimmung für $\mathrm{Span}(u_1, \ldots, u_k)$ in R^n

(4) Basisbestimmung für $\mathrm{Span}(u_1, \ldots, u_k) + \mathrm{Span}(v_1, \ldots, v_l)$ in R^n

(5) Basisbestimmung von $\mathrm{Span}(u_1, \ldots, u_k) \cap \mathrm{Span}(v_1, \ldots, v_l)$ in R^n

(6) Entscheiden, ob eine Basis von $\mathrm{Span}(u_1, \ldots, u_k)$ in R^n ergänzt werden kann zu Basis von R^n.

(7) Bestimme $U \cap \mathbb{Z}^n$ für einen Untervektorraum U von $\mathbb{Q}^n$; analog für $K[x]$.

15 Lineare Abbildungen

Sei R ein kommutativer Ring $\neq \{0\}$. Lineare Abbildungen wurden bereits in Abschnitt 1(B) definiert.

Die Definition von Kern und Bild linearer Abbildungen können wir ohne Änderung aus der Linearen Algebra I übernehmen.

Satz 15.1. *Seien M, N R-Moduln und $F : M \longrightarrow N$ linear. Es gilt:*

(i) $\mathrm{Kern}\, F$ *ist Untermodul*

(ii) $\mathrm{Bild}\, F$ *ist Untermodul*

(iii) Urbild eines Untermoduls ist Untermodul.

(iv) F *ist injektiv* $\Longleftrightarrow \mathrm{Kern}\, F = \{0\}$

(v) F *ist surjektiv* $\Longleftrightarrow \mathrm{Bild}\, F = N$

Definition 15.2. *Eine bijektive lineare Abbildung heißt (Modul-)* **Isomorphismus**. *Ist $F : M \longrightarrow N$ ein Modulisomorphismus, so schreibt man $\boldsymbol{M \cong N}$.*

Ist $F : M \longrightarrow N$ ein Modulisomorphismus, so trifft dies auch für die Umkehrung zu.

Satz 15.3. *Sei $F : M \longrightarrow N$ linear. Äquivalent sind:*

(i) F *surjektiv*

(ii) F *bildet* **jedes** *Erzeugendensystem von M auf ein Erzeugendensystem von N ab.*

(iii) F *bildet* **ein** *Erzeugendensystem von M auf ein Erzeugendensystem von N ab.*

Satz 15.4. *$F : M \longrightarrow N$ linear. Es gilt:*

(i) $[(x_i)_{i\in I}$ *l.u. in M, F injektiv]* $\Longrightarrow (F(x_i))_{i\in I}$ *l.u. in N*

(ii) $(F(x_i))_{i\in I}$ *l.u. in* $N \Longrightarrow [(x_i)_{i\in I}$ *l.u. in M, $F\,|_{\mathrm{Span}(x_i)_{i\in I}}$ injektiv]*

(iii) $F(t(M)) \subseteq t(N)$

Satz 15.5. *$F, G : M \longrightarrow N$ beide R-linear; $(x_i)_{i\in I}$ ein Erzeugendensystem von M. Es gilt:*

$$[F(x_i) = G(x_i) \text{ für alle } i \in I] \Longrightarrow F = G$$

Satz 15.6. *Sei $F : M \longrightarrow N$ linear. Wenn M eine Basis $(x_i)_{i\in I}$ besitzt, dann ist F durch $(F(x_i))_{i\in I}$ eindeutig bestimmt.*

Satz 15.7. *Jeder endlich erzeugte R-Modul ist R-lineares Bild eines R^m (m geeignet).*

Dies führt uns auf die foldende **Problemstellung: Wie sehen die endlich erzeugten R-Moduln – d. h. die R-linearen Bilder von R^m aus? Insbesondere wenn $R = \mathbb{Z}$ oder $R = K[x]$?**

Satz 15.8 (Teil des Homomorphiesatzes für Moduln). *Seien $F_i : M \longrightarrow N_i$ R-linear $(i = 1, 2)$. Es gilt:*

$$\text{Kern } F_1 = \text{Kern } F_2 \Longrightarrow \text{Bild } F_1 \cong \text{Bild } F_2$$

(vgl. Satz 1.23).

Konsequenz aus Satz 15.8: Ist jeder Untermodul eines Moduls Kern einer schon bekannten R-linearen Abbildung, so sind bis auf Isomorphie die Bildmoduln die einzig möglichen homomorphen Bilder.

Ganz abstrakt kann man mit Hilfe einer Kongruenzrelation zu einem Untermodul U eine surjektive lineare Abbildung konstruieren die U als Kern hat.

Definition 15.9. *Sei U ein Untermodul des R-Moduls M. Zu $v, v' \in M$ definieren wir*

$$v \equiv v' \mod U :\Longleftrightarrow v - v' \in U \Longleftrightarrow: v \equiv_U v'$$

In Worten: u kongruent zu u' modulo U.

Beobachtung. $\equiv_U$ ist eine Äquivalenzrelation und für alle $v, w, v', w' \in M$ und $\lambda \in R$ gilt:

(i) $v \equiv_U v'$ und $w \equiv_U w' \quad \Longrightarrow \quad v + w \equiv_U v' + w'$.

(ii) $v \equiv_U v' \quad \Longrightarrow \quad \lambda v \equiv_U \lambda v'$

Aufgrund von (i), (ii) nennt man $\equiv_U$ eine Kongruenzrelation (bei Moduln, vgl. Abschnitt 1(F)) und die Menge der durch $\equiv_U$ gebildeten Kongruenzklassen wird mit M/U bezeichnet.

Satz 15.10.

(i) Die Kongruenzklassen bzgl. $\equiv_U$ *haben die Form* $v+U$ *mit* $v \in M$

(ii) Sind $\Gamma_1, \Gamma_2 \in M/U$ *und* $\lambda \in R$*, dann gilt für alle* $v, v' \in \Gamma_1$*,* $w, w' \in \Gamma_2$

$$\begin{array}{rcrcrcl} v+w & + & U & = & v' & + & w'+U \\ \lambda v & + & U & = & \lambda v' & + & U \end{array}$$

(iii) Zu $\Gamma_1, \Gamma_2 \in M/U$ *und* $\lambda \in R$ *sind*

$$\Gamma_1 + \Gamma_2 := v+w+U \quad \text{für ein } v \in \Gamma_1,\ w \in \Gamma_2, \tag{1}$$

$$\lambda\Gamma_1 := \lambda v_1 + U \quad \text{für ein } v \in \Gamma_1 \tag{2}$$

unabhängig von der speziellen Wahl von $v \in \Gamma_1$*,* $w \in \Gamma_2$*. Durch* (1)*,* (2) *lassen sich daher Verknüpfungen auf* M/U *festlegen.*

(iv) Mit den Verknüpfungen aus (iii) wird M/U *zum* R*-Modul.*

(v) Die Abbildung $F : M \longrightarrow M/U$ *mit* $F(v) = v+U$ *für* $v \in M$ *ist* R*-linear und surjektiv und es ist* $\operatorname{Kern} F = U$*.*

Die in Satz 15.10 durchgeführte abstrakte Konstruktion von M/U ist von grundsätzlicher Bedeutung für weite Teile der heutigen Mathematik. Für praktische Aufgaben ist M/U weniger geeignet. Immerhin sind i. A. die Elemente von M/U unendliche Mengen. Diesem Problem kann man aus dem Wege gehen, wenn es gelingt, ein Vertretersystem für die Kongruenzklassen zu konstruieren. Einen solchen Weg waren wir von vorneherein gegangen bei der Konstruktion von $\mathbb{Z}_d$ und $K[x]_{d,q}$.

Satz 15.11. *Sei* $\boldsymbol{\mathcal{V}} \subseteq M$ *ein Vertretersystem für* $\equiv_U$ *und* $(\varrho_{U,\boldsymbol{\mathcal{V}}} =)\varrho : M \longrightarrow \boldsymbol{\mathcal{V}}$ *die Abbildung mit* $\varrho(w) :=$ *einziges Element in* $(w+U) \cap \boldsymbol{\mathcal{V}}$*. Es gilt dann:*

(i) ϱ *ist surjektiv und* $\varrho \circ \varrho = \varrho$*.*

(ii) Für alle $w, w' \in M$*,* $\lambda \in R$*:*

$$\begin{array}{lcll} \varrho(w+w') & = & \varrho(\varrho(w)+\varrho(w')) & =: \ \varrho(w) \oplus \varrho(w') \\ \varrho(\lambda w) & = & \varrho(\lambda\varrho(w)) & =: \ \lambda \odot \varrho(w) \end{array}$$

(iii) Mit den durch (ii) festgelegten Verknüpfungen wird $\boldsymbol{\mathcal{V}}$ *ein* R*-Modul und* ϱ *eine* R*-lineare Abbildung mit* $\operatorname{Kern} \varrho = U$*.*

Vorsicht: *Der* R*-Modul* $\boldsymbol{\mathcal{V}}$ *bzgl.* $\oplus\odot$ *ist kein Untermodul von* M*. Allerdings ist* $\boldsymbol{\mathcal{V}}$ *Teilmenge von* M *und man kann wegen der* R*-Linearität von* ϱ *getrost in* M *rechnen und am Ende* ϱ *anwenden oder wann immer man dies (zur Vereinfachung) während einer Rechnung möchte.*

(iv) $(\boldsymbol{\mathcal{V}}, \oplus, \odot) \cong M/U$

Wenn $R = \mathbb{Z}$ oder $R = K[x]$, dann können wir mit Hilfe der Smith-Form ein Vertretersystem konstruieren. Dies sei am Beispiel $R = \mathbb{Z}$, $M = \mathbb{Z}^{n\times 1}$ illustriert: Sei $U = \mathrm{Span}(u_1, \ldots, u_r)$ und o. E. $r = n$. Setze $A = [u_1, \ldots, u_n]$. Wir schreiben $\mathrm{Span}\, A$ für den Aufspann der Spalten von A und beobachten, dass für alle $Q \in GL_n(\mathbb{Z})$ gilt: $\mathrm{Span}\, A = \mathrm{Span}\, AQ$. Seien nun $P, Q \in GL_n(\mathbb{Z})$ derart, dass $PAQ = \mathrm{diag}(d_1, \ldots, d_n) =: D$ in Smith-Form ist mit $d_1 \mid \cdots \mid d_n$ und $d_i \in \mathbb{N}$ für $1 \le i \le n$. Sei $X := \mathrm{Span}\, D$.

Satz 15.12.

(i) $\mathbb{Z}_D^n = \begin{bmatrix} \mathbb{Z}_{d_1} \\ \vdots \\ \mathbb{Z}_{d_n} \end{bmatrix} = \{z \in \mathbb{Z}^{n\times n} : z_i \in \mathbb{Z}_{d_i} \textit{ für } 1 \le i \le n\}$ *ist ein Vertretersystem für* $\equiv_X$

(ii) $P^{-1}\mathbb{Z}_D^n$ *ist ein Vertretersystem für* $\equiv_U$.

Ergänzung zu Abschnitt 13 unter Benutzung des Begriffes "lineare Abbildung":

Satz 15.13. *R euklidisch, M ein von n Elementen erzeugter R-Modul, U ein Untermodul von M. Dann kann auch U von n Elementen erzeugt werden.*

Beweis. Satz 15.7 benutzen, und zwar so:

Sei $M = \mathrm{Span}_R(m_1, \ldots, m_n)$. Es gibt dann genau eine surjektive lineare Abbildung $F : R^n \longrightarrow M$ mit $F(e_i) := m_i$, $1 \le i \le n$.

$F^{-1}(U) = \{v \in R^n : F(v) \in U\}$ ist ein Untermodul von R^n, besitzt also eine Basis der Länge k mit $k \le n$. Sei etwa $w_1, \ldots, w_k$ eine Basis von $F^{-1}(U) = \mathrm{Span}_R(w_1, \ldots, w_k)$. Nun gilt: $U = \mathrm{Span}_R(F(w_1), \ldots, F(w_k))$. □

Satz 15.14. $\boldsymbol{R}$ euklidisch, *M endlich erzeugt: $M = t(M) \oplus F$ mit einem freien Untermodul F von M.*

Beispiel. $\mathbb{Q}$ als $\mathbb{Z}$-Modul ist nicht endlich erzeugt, es ist $t(\mathbb{Q}) = \{0\}$ und jede maximale l.u. Familie hat die Länge 1.

16 Homomorphe Bilder von R^n, R euklidisch

Satz 15.7 besagt: jeder endlich erzeugte R-Modul ist homomorphes Bild eines R^n, n geeignet.

Es genügt also, die homomorphen Bilder von R^n zu übersehen, um einen Überblick über alle endlich erzeugten R-Moduln zu erhalten. Dies trifft für beliebige Ringe

zu. Für euklidische Ringe lassen sich vollständige **und** algorithmisch erschließbare Aussagen machen. Dies geschieht in diesem Abschnitt.

Für $R = \mathbb{Z}$ ergeben sich dabei interessante Darstellungen für "Faktorgitter" $\mathbb{Z}^n/U$.

Der Fall $R = K[x]$, K Körper, lässt sich bei linearen Differenzialgleichungssystemen und in der linearen Kontrolltheorie anwenden und ermöglicht einen weiteren Zugang (sogenannter geometrischer) zum Normalformenproblem. Beides wird hier im Skript nicht mehr dargestellt.

Sei M ein endlich erzeugter R-Modul und R zunächst noch ein beliebiger kommutativer Ring $\neq \{0\}$. Es gibt dann $k \in \mathbb{N}$ und eine surjektive lineare Abbildung $f : R^{k\times 1} \longrightarrow M$. Mit $m_i = f(e_i)$ ist $M = \mathrm{Span}_R(m_1, \ldots, m_k)$.

Sei nun $P \in Gl_k(R)$. P definiert eine bijektive lineare Abbildung $\pi : R^{k\times 1} \longrightarrow R^{k\times 1}$ mit $\pi(x) = Px$.

$$\begin{array}{ccc} R^{k\times 1} & \overset{f}{\longrightarrow} & M \\ & & \downarrow \\ {\scriptstyle \pi, P}\downarrow & & \\ & & {\scriptstyle g = f\circ\pi^{-1}} \\ R^{k\times 1} & & \end{array} \tag{1}$$

$g = f \circ \pi^{-1}$ ist eine **weitere** lineare Abbildung mit $\mathrm{Bild}\, g = M$.

Wir haben also einen ersten Ansatzpunkt gefunden zur Vereinfachung von f bzw. der Darstellung von M als homomorphem Bild von R^n.

Satz 16.1. *Ist in* (1) $g \circ \pi = f$ *und* π *bijektiv, dann gilt:*

$$\mathrm{Kern}\, g = \pi(\mathrm{Kern}\, f)$$

Sei nun R euklidisch. $\mathrm{Kern}\, f$ ist Untermodul von $R^{k\times 1}$. Falls $\mathrm{Kern}\, f = \{0\}$, ist $M \approx R^k$. Wir setzen daher voraus, daß $\mathrm{Kern}\, f \neq \{0\}$. Nach Satz 13.2 besitzt $\mathrm{Kern}\, f$ dann eine Basis von $1 \leq l \leq k$ Elementen. Es gibt also eine (sogar injektive) Abbildung

$$\alpha : R^{l\times 1} \longrightarrow R^{k\times 1}$$

mit $\mathrm{Bild}\, \alpha = \mathrm{Kern}\, f = \mathrm{Span}(\alpha(e_1), \ldots, \alpha(e_l))$.

Sei $A := [\alpha(e_1), \ldots, \alpha(e_l)] \in R^{k\times 1}$, dann gilt: $\alpha(x) = Ax$ für alle $x \in R^{l\times 1}$.

Wie bei f, so kann auch bei α versucht werden, durch Vorschalten einer bijektiven Abbildung (Basiswechsel) eine Vereinfachung der Beschreibung des Bildes von α (= $\mathrm{Kern}\, f$) zu erreichen. Beide Vereinfachungsmöglichkeiten werden wir jetzt ausnutzen, so daß insgesamt folgendes Diagramm entsteht:

$$\begin{array}{ccccc} R^{1\times 1} & \overset{\alpha, A}{\hookrightarrow} & R^{k\times 1} & \overset{f}{\longrightarrow} & M \\ \uparrow & & & & \downarrow \\ {\scriptstyle \kappa, Q} & & {\scriptstyle \pi, P}\downarrow & & {\scriptstyle g(=f\pi^{-1})} \\ R^{1\times 1} & \underset{\beta, B}{\hookrightarrow} & R^{k\times 1} & & \end{array} \tag{2}$$

(das Symbol "$\longrightarrow\!\!|$" soll Surjektivität, das Symbol "$\hookrightarrow$" Injektivität anzeigen).

Dabei sollen κ, π bijektiv sein, bzw. $P \in GL_k(R)$, $Q \in GL_l(R)$ und $\beta = \pi \circ \alpha \circ \kappa$ bzw. $B = PAQ$.

Wenn ***R* euklidisch** ist, gibt es $P \in GL_k(R)$ und $Q \in GL_l(R)$ mit

$$B = PAQ = \operatorname{diag}(d_1, \ldots, d_l) = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_l \\ \cdots & \cdots & \cdots \\ & 0 & \end{bmatrix}, (l \leq k) \tag{3}$$

wobei $d_1 \mid \ldots \mid d_l$ und die d_i eindeutig sind bis auf Einheiten.

Es bleibt zu klären, wie sich eine solche Diagonalisierung von A auf die Beschreibung von M auswirkt.

Satz 16.2. *In einem Diagramm der Form* (2) *mit*

(i) $\operatorname{Bild}\alpha = \operatorname{Kern} f$

(ii) κ, α *bijektiv*

(iii) $\pi\alpha\kappa = \beta$ *und* $g\pi = f$

gilt: $\operatorname{Bild}\beta = \operatorname{Kern} g$

Beweis. $\operatorname{Kern} G \overset{\text{Satz 1}}{=} \pi(\operatorname{Kern} f) = \pi(\operatorname{Bild}\alpha) = \operatorname{Bild}\pi\alpha \overset{\text{Surjektivität von } \kappa}{=} \operatorname{Bild}\pi\alpha\kappa = \operatorname{Bild}\beta$. □

Wenn nun (3) gilt, dann ist also

$$\operatorname{Kern} g = \operatorname{Span}_R(d_1 e_1, \ldots, d_l e_l) \tag{4}$$

Von Satz 15.8 her wissen wir, daß gilt: $M \approx R^{k\times 1}/\operatorname{Kern} g$.

Wegen der besonderen Form (4) von $\operatorname{Kern} g$ läßt sich noch mehr aussagen:

Satz 16.3. *Seien R ein kommutativer Ring, $d_1, \ldots, d_l \in R$ und $U = \operatorname{Span}_R(d_1 e_1, \ldots, d_l e_l)$. Dann ist*

$$R^{k\times 1}/_U \approx R/_{Rd_1} \times \ldots \times R/_{Rd_l} \times \underbrace{R^{k-l}}_{\substack{\text{tritt nicht auf,} \\ \text{falls } k=l}} \tag{5}$$

Dabei werden die $R/_{Rd_i}$ aufgefaßt als R-Moduln.

Beweis. Wir betrachten die R-lineare surjektive Abbildung $F : R^{k\times 1} \longrightarrow$ rechte Seite von (5) mit

$$F\left(\begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix}\right) = (x_1 + Rd_1, \ldots, x_l + Rd_l, \underbrace{x_{l+1}, \ldots, x_k}_{\text{falls } l<k}) .$$

und bestimmen ihren Kern. Es gilt:

$$F(x) = 0 \Longleftrightarrow \left\{ \begin{array}{l} x_i \in d_i R \text{ für } 1 \leq i \leq l \\ \text{und} \\ x_{l+1} = \ldots = x_k = 0 \text{ falls } l < k \end{array} \right\}$$

bzw. $\operatorname{Kern} F = \operatorname{Span}_R(d_1 e_1, \ldots, d_l e_l)$. Mit Satz 15.8 ergibt sich Satz 16.3. □

Die Moduln ${}^R/_{Rd_i}$ sind für konkrete Anwendungen immer noch zu abstrakt oder unbestimmt. Man möchte sie daher ersetzen durch einfache isomorphe Modelle.

Satz 16.4. *Seien R ein kommutativer Ring, $d_1, \ldots, d_l \in R$ und $M_1, \ldots, M_l$ R-Moduln.*

Wenn gilt $M_i \approx {}^R/_{Rd_i}$ für $1 \leq i \leq l$, dann gilt auch

$$M_1 \times \ldots \times M_l \approx {}^R/_{Rd_1} \times \ldots \times {}^R/_{Rd_l}$$

Beweis. Seien für $1 \leq i \leq l$ etwa $\varphi_i : M_i \longrightarrow {}^R/_{Rd_i}$ R-Modul-Isomorphismen, dann ist

$$\varphi : M_1 \times \ldots \times M_l \longrightarrow {}^R/_{Rd_1} \times \ldots \times {}^R/_{Rd_l}$$

mit $\varphi(m_1, \ldots, m_l) := (\varphi_1(m_1), \ldots, \varphi_l(m_l))$ ebenfalls ein Isomorphismus von R-Moduln. □

Zusamenfassung:

Satz 16.5. *Sei R euklidisch und $M = \operatorname{Span}_R(m_1, \ldots, m_k)$ ein endlich erzeugter R-Modul. Sei $F : R^{k\times 1} \longrightarrow M$ eine surjektive Abbildung; sei $\alpha_1, \ldots, \alpha_l$ eine Basis von* $\operatorname{Kern} F$ *und $A := [\alpha_1, \ldots, \alpha_l]$.*

Sei $\operatorname{diag}(d_1, \ldots, d_l)$ *eine Smith-Form von A und seien $M_1, \ldots, M_l$ Modelle für ${}^R/_{Rd_1}, \ldots, {}^R/_{Rd_l}$ (d.h.: $M_i \approx {}^R/_{Rd_i}$ als R-Moduln). Dann gilt:*

$$M \approx M_1 \times \ldots \times M_l \times \underbrace{R^{k-l}}_{\substack{\text{tritt nur auf,} \\ \text{wenn } k>l}} \tag{6}$$

Bemerkungen.

1.) Schon bei der Smith-Form sind die d_i nur eindeutig bis auf Einheiten. Hier sind allerdings jetzt die ${}^R/_{Rd_i}$ eindeutig bestimmt, denn es gilt $Rd_i = Rud_i$ für alle $u \in G(R)$.

2.) Die aus der Linearen Algebra I bekannte Aussage: "Jeder endlich erzeugte K-Vektorraum ist isomorph zu K^k, k geeignet" findet in (6) ihre Verallgemeinerung für euklidische Ringe.

3.) Im Falle $R = \mathbb{Z}$ heißt Satz 16.5 auch: "Hauptsatz über endlich erzeugte abelsche Gruppen". Insbesondere wird durch Satz 16.5 die Struktur einer beliebigen endlichen abelschen Gruppe genau beschrieben. Eine Verfeinerung der Aussage erhält man über die Elementarteiler und mit Hilfe des chinesischen Restsatzes. Siehe etwa [Ja].

Kapitel IV

Ein Anwendungsbeispiel

Schon relativ früh in der Linearen Algebra I wurden lineare Kontrollprozesse als Anwendungsbeispiel vorgestellt. Geometrische Anwendungen stehen meistens und naturgemäß im Mittelpunkt. Zum Abschluss der Vorlesung wurde als Kapitel IV eine weitere der zahlreichen Anwendungen linear-algebraischer Methoden ansatzweise vorgestellt: **lineare und zyklische fehlerkorrigierende Codes**. Im Einzelnen ging es um: Kodierung und Codes, Hammingabstand, Hamming Codes, Fehlerkorrektur, Syndrom-Dekodierung, diskrete Fourierformation, Reed-Solomon Codes.

Interessante Literatur zu diesem Thema ist u. A. [LiCo], [BFKWZ] und [CLS, Chapter 9].

Literaturverzeichnis

[AdWe] W. Adkins, S. Weintraub: *Algebra, An Approach via Module Theory*, Springer, 1992.

[BFKWZ] A. Betten, H. Fripertinger, A. Kerber, A. Wassermann, K.H. Zimmerman: *Codierungstheorie*, Springer, 1998.

[BeWe] E. Becker, V. Weispfennig: *Gröbner Bases, A Computational Approach to Commutative Algebra*, Springer, 1993.

[CLS] D. Cox, J. Little, D. O'Shea: *Using Algebraic Geometry*, Springer, 1998.

[Co] H. Cohen: *A Course in Computational Algebraic Member Theory*, Springer, 1993.

[CoCuSt] H. Cohen, H. Cuypers, H. Sterk (Hrsg.): *Some Tapas of Computer Algebra*, Springer, 1999.

[Fi] G. Fischer: *Lineare Algebra*, vieweg, 11. Auflage, 1997.

[Ga] F. Gantmacher: *Matrizenrechnung*, Springer, 1986.

[HaHa] B. Hartley, T. Hawkes: *Rings, Modules and Linear Algebra*, Chapman Hall, 1976.

[Ja] N. Jacobson: *Basic Algebra I*, Freeman, 1974.

[KiSch] K. Kiyek, F. Schwarz: *Lineare Algebra*, Teubner, 1999.

[KoMi] H. Kowalski, G. Michler: *Lineare Algebra*, deGruyter, 11. Auflage, 1998.

[Koe] O. Körner: *Algebra*, Akad. Verl. Ges., 1974.

[La1] S. Lang: *Algebraische Strukturen*, Vandenhoeck u. Ruprecht, 1979.

[La2] S. Lang: *Algebra*, Addison Wesley, 1965 (oder spätere Auflagen).

[LiCo] S. Lin, D. Costello: *Error Control Coding*, Prentice Hall, 1983.

[Lue1] H. Lüneburg: *Vorlesungen über lineare Algebra*, BI, 1993.

[Lue2] H. Lüneburg: *Einführung in die Algebra*, Springer, 1973.

[Ne] M. Newman: *Integral matrices*, Acad. Press, 1972.

[SchSt] G. Scheja, U. Storch: *Lehrbuch der Algebra*, Teubner, 1980 und 1988.

[Wa] R. Walter: *Einführung in die lineare Algebra*, vieweg, 2. Auflage, 1986.