Grundlagen der Darstellungstheorie

Prof. Dr. A. Henke

Wintersemester 2020/21

Inhaltsverzeichnis

Kapitel 1

Algebren

In diesem Kapitel definieren wir Algebren. Wie bei anderen algebraischen Objekten (beispielsweise Gruppen, Ringen, Körpern) behandeln wir Unterobjekte sowie strukturerhaltende Abbildungen. Wir benutzen hierbei typischerweise die folgende Notation:

- K Körper,
- R Ring, Einselement 1_R,
- G Gruppe,
- A Algebra.

Es ist in der Darstellungstheorie wichtig, dass Algebren ein Einselement haben. Aus diesem Grund haben Ringe in dieser Vorlesung immer eine Eins.

1.1 Definition und Beispiele

In dieser Vorlesung wollen wir Algebren durch konkrete Objekte darstellen. In diesem Abschnitt wollen wir daher zunächst den Begriff der Algebra einführen und an Beispieln aufzeigen, dass Algebren zu den zentralen mathematischen Strukturen gehören.

Definition 1.1. Sei K ein Körper. Eine Menge $A = (A, +, \cdot_m, \cdot_s)$ heisst *Algebra über K* oder *K-Algebra*, falls gilt:

a) $(A, +, \cdot_m)$ ist ein Ring.

b) $(A, +, \cdot_s)$ ist ein K-Vektorraum.

c) Es gilt für alle $a, b \in A$ und $\lambda \in K$, dass $\lambda \cdot (a \cdot b) = (\lambda \cdot a) \cdot b = a \cdot (\lambda \cdot b)$.
In saloppen Worten: Skalare, also Elemente aus dem Körper, kommutieren mit allen anderen Elementen. Beachten Sie, in der angegebenen Gleichung schreiben wir nur einen Punkt; ob es sich bei dem Punkt um Skalarmultiplikation oder Ringmultiplikation handelt, ergibt sich aus dem Zusammenhang.

Die Vektorraumdimension von A, also $\dim_K A$, heisst die *Dimension* von A. Insbesondere ist A *endlich-dimensional*, falls $\dim_K A < \infty$. Eine Algebra A ist *kommutativ*, falls der Ring A kommutativ ist.

Bemerkung 1.2. Die Abbildung $K \to A$, definiert durch $\lambda \mapsto \lambda \cdot_s 1_A$, ist injektiv. Deshalb betrachten wir K als Teilmenge von A, mittels der Einbettung $\lambda \mapsto \lambda \cdot_s 1_A$. Insbesondere ist dann Skalarmultiplikation in A ein Spezialfall von Multiplikation: $\lambda \cdot_s a = (\lambda \cdot 1_A) \cdot_m a$.

Aufgabe 1.1. Zeigen Sie, dass die Abbildung $\lambda \mapsto \lambda \cdot_s 1_A$ in Bemerkung 1.2 injektiv ist. Machen Sie hierbei in jedem Schritt deutlich, warum er folgt.

Algebren sind also im wesentlichen Ringe, die gleichzeitig Vektorräume sind. Wir kennen bereits viele Beispiele von Algebren aus der Linearen Algebra oder Algebra-Vorlesung. Im Folgenden wiederholen wir diese. Überprüfen Sie in jedem Beispiel, dass es sich hierbei sowohl um einen Ring als auch um einen Vektorraum handelt.

Beispiel 1.3. Sei K ein Körper. Dann ist K eine kommutative K-Algebra der Dimension Eins. Sei n eine natürliche Zahl. Dann ist der Polynomring in n Variablen eine kommutative K-Algebra. All diese Algebren haben unendliche Dimension. Zur Erinnerung, der Polynomring $K[X]$ in einer Variablen X ist definiert durch:

$$K[X] = \{a_0 + a_1 X + \ldots + a_m X^m \mid m \in \mathbb{N}, a_0, a_1, \ldots a_m \in K\}.$$

Die Menge $\{1, X, X^2, \ldots\}$ ist eine Basis des K-Vektorraumes $K[X]$. Induktiv definiert man den Polynomring in n Variablen durch

$$K[X_1, \ldots, X_n] := K[X_1, \ldots, X_{n-1}][X_n].$$

Das nicht-kommutative Analogon zum Polynomring ist die *freie Algebra*

$$K\langle X_1, \ldots, X_n\rangle.$$

Die Basis des zugrundeliegenden Vektorraumes besteht aus allen Wörtern in $X_1, \ldots, X_n$. Multiplikation ist das Zusammenhängen von Wörtern, linear erweitert auf alle Elemente aus $K\langle X_1, \ldots, X_n\rangle$.

Beispiel 1.4. Als nächstes betrachten wir Beispiele, bei denen die Elemente Matrizen beziehungsweise lineare Abbildungen sind.

a) Die Menge $M_n(K)$ bestehend aus allen $n \times n$-Matrizen mit Einträgen im Körper K, zusammen mit Matrixaddition und Matrixmultiplikation bildet eine K-Algebra. Das Einselement ist die Diagonalmatrix $\mathrm{diag}(1, \ldots, 1)$, bei der alle Einträge auf der Diagonale Eins sind. Diese Algebra hat Dimension n^2. Für $n \geq 2$ ist sie nicht kommutativ. An diesem Beispiel kann man sich auch gut Bemerkung 1.2 verdeutlichen: Skalarmultiplikation von Matrizen ist ein Spezialfall von Matrixmultiplikation mittels der Einbettung

$$K \to M_n(K), \text{ definiert durch } \lambda \mapsto \lambda \cdot 1_{M_n(K)}.$$

Man kann ebenfalls sehr leicht nachprüfen, dass die folgenden Mengen Algebren über dem Körper K sind:

$$\begin{aligned} T_n(K) &:= \{(a_{ij} \in M_n(K)) \mid a_{ij} = 0 \text{ für } i > j\}, \\ D_n(K) &:= \{(a_{ij} \in M_n(K)) \mid a_{ij} = 0 \text{ für } i \neq j\}. \end{aligned}$$

Bei $T_n(K)$ handelt es sich um die Menge aller oberen Dreiecksmatrizen; diese Algebra ist nicht-kommutativ und hat die Dimesnion $n(n+1)/2$. Bei $D_n(K)$ handelt es sich um die Menge aller Diagonalmatrizen; dies ist eine kommutative Algebra der Dimension n.

b) Sei V ein endlich-dimensionaler K-Vektorraum. Dann ist die Menge $\mathrm{End}_K(V)$ aller K-linearen Abbildungen $f : V \to V$ eine K-Algebra. Die Addition von linearen Abbildungen wird definiert mittels

$$(f + g)(v) := f(v) + g(v).$$

Die Multiplikation von Elementen dieser Algebra ist definiert als die Komposition von Abbildungen:

$$(f \circ g)(v) := f(g(v)).$$

Die Skalarmultiplikation ist definiert durch

$$(\lambda \cdot f)(v) := \lambda \cdot f(v).$$

Bei den Definitionen ist jeweils $\lambda \in K$ und $f, g \in \mathrm{End}_K(V)$ und $v \in V$. Beachten Sie wiederum, wie die Skalarmultiplikation in diesem Fall als Spezialfall der Multiplikation gegeben ist. Die Algebra $\mathrm{End}_K(V)$ ist im Allgemeinen nicht kommutativ. Es gilt $\dim \mathrm{End}_K(V) = (\dim_K V)^2$.

Beispiel 1.5. Seien K und L Körper mit $K \subseteq L$ Teilkörper. Dann ist L eine kommutative K-Algebra. Die Addition in der Algebra L entspricht der Addition im Körper L; die Multiplikation in der Algebra L entspricht der Multiplikation im Körper L. Beispielsweise ist also $\mathbb{R}$ eine kommutative $\mathbb{Q}$-Algebra unendlicher Dimension; beispielsweise ist $\mathbb{C}$ eine kommutative $\mathbb{R}$-Algebra der Dimension zwei.

Aufgabe 1.2. Sei K ein Körper. Diskutieren Sie die folgenden Fragen:

a) Bilden die ganzen Zahlen $\mathbb{Z}$ eine Algebra über irgendeinem Körper?

b) Bilden die echten oberen Dreiecksmatrizen mit Einträgen in einem Körper K eine Algebra über K?

c) Bilden die stetigen Funktionen $\mathbb{R} \to \mathbb{R}$ eine Algebra über $\mathbb{R}$?

d) Bilden die 3×3-Diagonalmatrizen $\mathrm{diag}(a, b, c)$ mit $a + b + c = 1$ eine Algebra über K?

Wie auch bei Ringen und Vektorräumen kann man aus Beispielen von algebraischen Objekten mittels abstrakter Konstruktionen weitere Beispiele solcher Objekte konstruieren. Für uns relevant ist hierbei das direkte Produkt von Algebren, die entgegengesetzte Algebra sowie Quotientenalgebren. Dass es sich beim direkten Produkt beziehungsweise bei der Quotientenalgebra um eine Algebra handelt, folgt jeweils aus entsprechenden Aussagen für Ringe und Vektorräume aus der Algebra beziehungsweise der Linearen Algebra Vorlesung.

Beispiel 1.6. Seien A_1 und A_2 Algebren über demselben Körper K. Das *direkte Produkt* der Algebren A_1 und A_2 ist definiert durch

$$A_1 \times A_2 = \{(a_1, a_2) \mid a_i \in A_i, i = 1, 2\}.$$

Mit komponentenweiser Addition und Multiplikation wird $A_1 \times A_2$ zu einer K-Algebra:

$$\begin{aligned} (a_1, a_2) + (b_1, b_2) &:= (a_1 + b_1, a_2 + b_2), \\ (a_1, a_2) \cdot (b_1, b_2) &:= (a_1 \cdot b_1, a_2 \cdot b_2). \end{aligned}$$

Hierbei sind $a_i, b_i \in A_1$ für $i = 1, 2$. Die (innere) direkte Summe zweier Algebren ist entsprechend wie bei Ringen und Vektorräumen definiert – und ist natürlich wiederum isomorph zur (externen) direkten Summe, also dem hier definierten direkten Produkt von Algebren.

Beispiel 1.7. Sei A eine K-Algebra. Definiere A^{op} als den K-Vektorraum A mit der Multiplikation $a * b := b \cdot_A a$, für alle $a, b \in A$. Dann ist A^{op} eine K-Algebra mit Dimension $\dim A^{\mathrm{op}} = \dim A$. Die Algebra A^{op} heisst *entgegengesetzte Algebra*, im Englischen *opposite algebra*. Das Einselement von A^{op} ist $1_{A^{\mathrm{op}}} = 1_A$.

Beispiel 1.8. Sei A eine Algebra über dem Körper K. Ist I ein links-, rechts- oder zweiseitiges Ideal in A, so ist I ein Unterraum im Vektorraum A. Damit folgt: Ist I ein zweiseitiges Ideal von A, dann ist der Quotientenring A/I nach Linearer Algebra eine K-Algebra. Für zweiseitige Ideale I in A schreiben wir $I \trianglelefteq A$. Wird ein Ideal von einem Element $a \in A$ erzeugt, so schreiben wir für dieses Ideal (a).

Aufgabe 1.3. Sei n eine natürliche Zahl. Bestimmen Sie Basen für die folgenden Vektorräume: $K[X]/(X^2)$ und $K[X]/(X^n)$ und $K[X]/(f)$, mit $f \in K[X]$.

Beispiel 1.9. Sei $(G, \cdot)$ eine multiplikativ geschriebene Gruppe. Die *Gruppenalgebra* erhält die Notation KG. Sie ist definiert als der K-Vektorraum mit Basis

$$\{v_g \mid g \in G\},$$

also mit einer Basis, die durch die Elemente der Gruppe indiziert ist. Die Multiplikation auf diesem Vektorraum wird durch lineare Erweiterung der Gruppenmultiplikation definiert. Genauer bedeutet dies, dass ein allgemeines Element der Gruppenalgebra KG die Form $\sum_{g \in G} \alpha_g v_g$ mit $\alpha_g \in K$ hat, und die Multiplikation mit einem Element $\sum_{h \in G} \beta_h v_h \in KG$ ist definiert durch:

$$\Big(\sum_{g \in G} \alpha_g v_g\Big) \cdot \Big(\sum_{h \in G} \beta_h v_h\Big) := \sum_{u \in G} \gamma_u v_u \tag{1.1}$$

mit Koeffizienten

$$\gamma_u := \sum_{g,h \in G \ \text{mit } g \cdot h = u} \alpha_g \beta_h.$$

Bemerkung 1.10. Sei 1 das neutrale Element der Gruppe G. Die Abbildung $G \to KG$, definiert durch $g \mapsto v_g$, ist injektiv und multiplikativ, erfüllt also

$$g \cdot h \mapsto v_{g \cdot h} \overset{(1.1)}{=} v_g \cdot v_h \text{ und } 1 \mapsto v_1 = 1_{KG},$$

wobei die zweite Gleichung mittels der Multiplikation in (1.1) nachgerechnet werden kann: $g = 1 \cdot g \mapsto v_1 \cdot v_g = v_g$, für alle $g \in G$, also gilt auch $v_1 \cdot a = a$ für alle $a \in KG$. Wir betrachten also G als Teilmenge der Algebra KG. Statt v_g schreibt man für den durch g indizierten Basisvektor einfach g selber. Dann ist also die Gruppenalgebra KG definiert als der Vektorraum mit Basis $\{g \mid g \in G\}$ und Multiplikation

$$\Big(\sum_{g \in G} \alpha_g g\Big) \cdot \Big(\sum_{h \in G} \beta_h h\Big) := \sum_{u \in G} \gamma_u u$$

mit Koeffizienten

$$\gamma_u := \sum_{g,h \in G \quad \text{mit } g \cdot h = u} \alpha_g \beta_h.$$

Beispiel 1.11. Sei $K = \mathbb{Q}$. Für eine natürliche Zahl n sei C_n die zyklische Gruppe mit n Elementen. Sei etwa $C_4 = \langle x \mid x^4 = 1 \rangle$. Dann ist

$$\mathbb{Q}C_4 = \{a_0 + a_1 x + a_2 x^2 + a_3 x^3 \mid a_i \in \mathbb{Q}, i = 0, 1, 2, 3\}.$$

Es wird im Prinzip wie bei Polynomen multipliziert, wobei $x^i = x^j$ mit $i \equiv j \mod 4$ benutzt wird. Beispielsweise ist

$$(1 + 2x^3) \cdot (-1 + 0,5x) = -1 + 0,5x - 2x^3 + x^4 = 0,5x - 2x^3.$$

Aufgabe 1.4. Ein Element $e \neq 0$ in einem Ring heisst ein *Idempotent*, falls $e^2 = e$ ist. Bestimmen Sie alle Idempotente in der Gruppenalgebra $\mathbb{C}C_2$ beziehungsweise $\mathbb{C}C_3$. (Je nach Zusammenhang oder Autor wird auch $e = 0$ als Idempotent bezeichnet.)

Aufgabe 1.5. Diskutieren Sie die folgenden Fragen:

a) In einer Gruppe G sind alle Elemente multiplikativ invertierbar. Sind in einer Gruppenalgebra KG alle Elemente ungleich Null invertierbar?

b) Sei R ein Ring und $e \in R$ ein Idempotent. Ist dann $1 - e$ ein Idempotent? Welche Idempotente sind invertierbar?

1.2 Teilalgebren und Homomorphismen

Im ersten Abschnitt dieses Kapitels haben wir Algebren kennengelernt. Algebren sind spezielle Ringe, nämlich solche, die gleichzeitig auch Vektorräume sind. Wie bei allen algebraischen Objekten gibt es Unterobjekte und strukturerhaltende Abbildungen zwischen gleichartigen Objekten. Diese wollen wir in diesem zweiten Abschnitt einführen.

Definition 1.12. Sei A eine Algebra über dem Körper K. Eine *Unteralgebra* oder *Teilalgebra* von A ist ein Unterraum $B \leq A$ mit den folgenden Eigenschaften:

a) Wenn immer $b_1, b_2 \in B$, dann ist $b_1 \cdot b_2 \in B$.
Der Unterraum B ist also multiplikativ abgeschlossen.

b) Das Einselement 1_A liegt in B.

Wir schreiben $B \leq A$, falls B eine Unteralgebra von A ist.

Ein multiplikativ abgeschlossener Unterraum einer Algebra A, der das Einselement von A enthält, ist ein Teilring von A. Da B Teilmenge von A ist, kommutieren natürlich weiterhin die Skalare mit allen anderen Elementen von B. Eine Unteralgebra B von A ist damit natürlich wieder eine Algebra im Sinne von Definition 1.1.

Beispiel 1.13. a) Mit der Notation in Beispiel 1.4 gilt:

$$D_n(K) \leq T_n(K) \leq M_n(K).$$

b) Ist H eine Untergruppe von G, dann ist KH eine Unteralgebra von KG.

Aufgabe 1.6. Sei A eine Algebra über einem Körper K. Wir definieren

$$Z(A) := \{z \in A \mid az = za \text{ für alle } a \in A\},$$

genannt *Zentrum von A*.

a) Zeigen Sie, dass $Z(A)$ eine Unteralgebra von A ist.

b) Sei $A = A_1 \times A_2$ direktes Produkt von Algebren wie in Beispiel 1.6. Bestimmen Sie das Zentrum $Z(A)$ in Abhängigkeit von den Zentren $Z(A_1)$ und $Z(A_2)$.

Aufgabe 1.7. Sei K ein Körper. Diskutieren Sie, ob die folgenden Mengen Teilalgebren sind von $M_n(K)$ für eine geeignete natürliche Zahl n:

$$A_1 := \begin{pmatrix} K & 0 \\ 0 & K \end{pmatrix},\ A_2 := \begin{pmatrix} 0 & 0 \\ 0 & K \end{pmatrix},\ A_3 := \begin{pmatrix} K & K & 0 \\ 0 & K & 0 \\ 0 & K & K \end{pmatrix},\ A_4 := \begin{pmatrix} K & 0 & 0 & 0 \\ K & K & 0 & 0 \\ K & 0 & K & 0 \\ K & 0 & 0 & K \end{pmatrix}.$$

Hierbei definieren wir beispielsweise

$$\begin{pmatrix} K & K & 0 \\ 0 & K & 0 \\ 0 & K & K \end{pmatrix} := \left\{ \begin{pmatrix} a & b & 0 \\ 0 & c & 0 \\ 0 & d & e \end{pmatrix} \mid a,b,c,d,e \in K \right\}.$$

Definition 1.14. Seien A und B Algebren über demselben Körper K. Eine Abbildung $\phi : A \to B$ ist ein *K-Algebrenhomomorphismus* oder kurz *Homomorphismus*, falls gilt:

a) ϕ ist K-linear;

b) $\phi(ab) = \phi(a)\phi(b)$, für alle $a, b \in K$;

c) $\phi(1_A) = 1_B$.

Wir nennen ϕ einen *(Algebren-)Isomorphismus*, falls ϕ zusätzlich bijektiv ist. Die Algebren A und B heissen in diesem Fall *isomorph*, kurz $A \simeq B$, gesprochen A isomorph zu B.

Bemerkung 1.15. Seien A, B und C Algebren über demselben Körper K.

a) Sei $\varphi : A \to B$ ein Algebrenhomomorphismus. Dann ist $\ker(\varphi) \trianglelefteq A$ ein Ideal und $\operatorname{im}(\varphi) \leq B$ eine Unteralgebra.

b) Seien $\phi : A \to B$ und $\psi : B \to C$ Algebrenhomomorphismen. Dann ist $\psi \circ \phi : A \to C$ ein Algebrenhomomorphismus.

Beide Aussagen folgen direkt aus den entsprechenden Aussagen für Vektorräume beziehungsweise für Ringe. Der Beweis ist Ihnen als Übungsaufgabe überlassen.

Beispiel 1.16. Seien A und B Algebren über demselben Körper K.

a) Sei $I \trianglelefteq A$ ein Ideal. Dann ist die *kanonische Projektion* $\pi : A \to A/I$, definiert durch $a \mapsto a + I$, ein surjektiver Algebrenhomomorphismus.

b) Sei $b \in B$. Der sogenannte *Einsetzungshomomorphismus* $\psi : K[X] \to B$, definiert durch $f \mapsto f(b)$ ist ein Algebrenhomomorphismus.

Beide Aussagen folgen analog wie für Ringe, siehe Algebravorlesung.

Beispiel 1.17. Sei V ein K-Vektorraum mit $\dim V = n$. Aus Resultaten der Linearen Algebra I folgt: $\operatorname{End}_K(V) \simeq M_n(K)$, als Algebren. Wir wiederholen den Beweis hierzu: Nach Beispiel 1.4 sind $M_n(K)$ und $\operatorname{End}_K(V)$ Algebren über dem Körper K. Sei $B := \{v_1, \ldots, v_n\}$ eine Basis des Vektorraumes V. Definiere die Abbildung

$$\epsilon_B : \operatorname{End}_K(V) \to M_n(K), \quad T \mapsto M_B(T),$$

wobei zu einer linearen Abbildung T die darstellende Matrix $M_B(T)$ definiert ist mittels der Gleichungen

$$v_i \overset{T}{\mapsto} T(v_i) = a_{1i}v_1 + \ldots + a_{ni}v_n$$

für $1 \leq i \leq n$. Wir verwenden hier also die Spaltenkonvention zur Definition der darstellenden Matrix einer linearen Abbildung. Die Abbildung $\epsilon := \epsilon_B$ ist abhängig von der gewählten Basis B von V. Wir konstruieren also viele verschiedene Algebrenisomorphismen. Seien $S, T \in \operatorname{End}_K(V)$ und sei $\lambda \in K$. Resultate aus Linearer Algebra I ergeben:

a) $\epsilon(S + T) = M_B(S + T) = M_B(S) + M_B(T) = \epsilon(S) + \epsilon(T)$,

b) $\epsilon(\lambda T) = M_B(\lambda T) = \lambda M_B(T) = \lambda\epsilon(T)$,

c) $\epsilon(S \circ T) = M_B(S \circ T) = M_B(S) \cdot M_B(T) = \epsilon(S) \cdot \epsilon(T)$,

d) $\epsilon(\mathrm{id}_V) = I_n$.

Damit ist ϵ ein Algebrenhomomorphismus. Da ϵ bijektiv ist, folgt ϵ ist ein Isomorphismus von Algebren.

Aufgabe 1.8. Zeigen Sie, dass die Abbildung $\epsilon = \epsilon_B$ aus Beispiel 1.17 bijektiv ist.

Algebren sind spezielle Ringe. Wie in der Algebravorlesung erhält man nun diverse Struktursätze für Algebren direkt aus der entsprechenden Aussage über Ringe:

Theorem 1.18 (Homomorphiesatz)**.** *Seien A und B Algebren über demselben Körper K. Sei $\phi : A \to B$ ein Algebrenhomomorphismus. Dann ist $A/\ker\phi \simeq \operatorname{im}\phi$, als Algebren.*

Theorem 1.19 (Isomorphiesätze)**.** *Sei A eine Algebra über einem Körper K.*

1. *Sind $I, J \trianglelefteq A$ Ideale, so sind auch $I + J, I \cap J \trianglelefteq A$ Ideale, und es gilt:*

$$I + J/I \simeq J/I \cap J.$$

2. *Seien $I \subseteq J \subseteq L$ Ideale von A. Dann sind auch $J/I \subseteq L/I$ Ideale von A/I mit*

$$(L/I)/(J/I) \simeq L/J.$$

Bei den Algebren im letzten Theorem handelt es sich ausnahmsweise um Algebren ohne Eins. Beide Sätze sind Anwendungen des Homomorphiesatzes. Der Isomorphismus in der Aussage des ersten Isomorphiesatzes kann auch direkt zum Nachrechnen angegeben werden: $x + I \leftarrow x + I \cap J$. Zum Beweis des zweiten Isomorphiesatzes sei $f : L/I \to L/J$ definiert durch $a + I \mapsto a + J$. Dann ist $\ker f = J/I$. Jetzt wendet man den Homomorphiesatz an. Die folgende wichtige (leicht zu beweisende) Bijektion aus der Ringtheorie (Algebravorlesung) wird als Idealkorrespondenz bezeichnet, und spielt eine wichtige Rolle in der Darstellungstheorie:

Theorem 1.20 (Idealkorrespondenz)**.** *Sei A eine Algebra über einem Körper K und sei $I \trianglelefteq A$ ein Ideal, sowie $\pi : A \to A/I$ die kanonische Projektion, siehe Beispiel 1.16.*

a) Wenn J ein Ideal in A/I ist, dann ist $\pi^{-1}(J)$ ein Ideal in A, das I enthält.

b) Umgekehrt, ist $J' \trianglelefteq A$ mit $I \subseteq J'$, dann ist das Bild $\pi(J')$ ein Ideal in A/I.

Durch diese beiden Abbildungen wird eine inklusionserhaltende Bijektion zwischen den Idealen von A, die I enthalten, und den Idealen von A/I beschrieben.

Aufgabe 1.9. Beweisen Sie die Idealkorrespondenz.

Aufgabe 1.10. Diskutieren Sie die folgenden Aussagen:

a) Ist die Algebra der oberen $n \times n$-Dreiecksmatrizen isomorph zur Algebra der unteren $n \times n$-Dreiecksmatritzen?

b) Ist die Algebra der oberen $n \times n$-Dreiecksmatrizen isomorph zu ihrer entgegengesetzten Algebra?

c) Sind die oberen $n \times n$-Dreiecksmatrizen eine Quotientenalgebra der oberen $(n+1) \times (n+1)$-Dreiecksmatrizen?

d) Ist $M_n(K)$ isomorph zu einer Quotientenalgebra von $M_{n+1}(K)$?

1.3 Die Wegealgebra

In diesem Abschnitt geht es um die *Wegealgebra* von Köchern (bisweilen auch *Köcheralgebren*), einer wichtigen Klasse von Algebren, die uns in dieser Vorlesung begleiten werden. Um diese Algebren zu definieren, benötigen wir zunächst den Begriff eines Köchers.

Definition 1.21. Ein *Köcher* ist ein endlicher gerichteter Graph, also ein Quadrupel $Q = (Q_0, Q_1, s, t)$ mit endlichen Mengen Q_0 und Q_1 und Funktionen $s, t : Q_1 \to Q_0$, wobei $Q_0 \neq \emptyset$ mit

$$\begin{aligned} Q_0 &= \text{Menge der Ecken (auch } \textit{Punkte} \text{ oder } \textit{Knoten} \text{ genannt)},\\ Q_1 &= \text{Menge der (gerichteten) Kanten (auch } \textit{Pfeile} \text{ genannt)}, \end{aligned}$$

und für einen Pfeil $\alpha \in Q_1$ ist

$$\begin{aligned} s(\alpha) &= \textit{Startpunkt} \text{ (source) von Pfeil } \alpha,\\ t(\alpha) &= \textit{Endpunkt} \text{ (target) von Pfeil } \alpha. \end{aligned}$$

Beispiel 1.22. Statt Punkte- und Kantenmengen anzugeben, definieren wir Köcher in der Regel durch ein Bild eines gerichteten Graphs. Wir demonstrieren an einigen Beispielen den Zusammenhang zwischen einem gezeichneten Köcher und Definition 1.21:

a) Der Köcher Q_a : $\begin{tikzcd} 1 \arrow[loop above, "\alpha"] \end{tikzcd}$ entspricht der Punktmenge $Q_0 = \{1\}$ und der Kantenmenge $Q_1 = \{\alpha\}$ mit $s(\alpha) = 1$ und $t(\alpha) = 1$.

b) Der Köcher Q_b : $2 \xleftarrow{\alpha} 1$ entspricht der Punktmenge $Q_0 = \{1, 2\}$ und der Kantenmenge $Q_1 = \{\alpha\}$ mit $s(\alpha) = 1$ und $t(\alpha) = 2$.

c) Der Köcher Q_c : $1 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3$ entspricht der Punktmenge $Q_0 = \{1, 2, 3\}$ und der Kantenmenge $Q_1 = \{\alpha, \beta\}$ mit $s(\alpha) = 1$ und $t(\alpha) = 2$ und $s(\beta) = 2$ und $t(\beta) = 3$.

Bemerkung 1.23. Wir benötigen diverse weitere sprachliche Konzepte für Köcher: Hintereinanderausführen von Pfeilen, Wege, faule Wege, Länge von Wegen, sowie die Erweiterung der Funktionen s, t auf Wege beliebiger Länge. Wir erkären diese Begriffe an den Köchern in Beispiel 1.22.

a) Die Punkte in einem Köcher Q betrachten wir im Folgenden als Wege der Länge Null, auch *faule/triviale/leere* Wege genannt. Wir schreiben e_i (oder einfach nur i) für den faulen Weg am Punkt i.

b) Die Pfeile im Köcher Q betrachten wir als Wege der Länge Eins.

c) Sei n eine natürliche Zahl mit $n \geq 1$. Sei Q ein Köcher mit Pfeilen $\alpha_i \in Q_1$ für $1 \leq i \leq n$. Ein *Weg der Länge n* ist die Hintereinanderausführung der Pfeile $\alpha_1, \alpha_2, \ldots, \alpha_n$, wobei gelten muss $t(\alpha_i) = s(\alpha_{i+1})$, für $1 \leq i \leq n-1$. Wir schreiben für diesen Weg $\alpha_1\alpha_2 \ldots \alpha_n$. Wir definieren den *Startpunkt* eines Weges $p := \alpha_1\alpha_2 \ldots \alpha_n$ durch $s(p) = s(\alpha_1)$, den *Endpunkt* des Weges p durch $t(p) = t(\alpha_n)$.

d) Längere Wege entstehen durch Hintereinanderausführung kürzerer Wege. Sind p und q zwei Wege im Köcher Q, so lassen sich diese nur hintereinander ausführen (oder komponieren) als Weg pq, falls der Endpunkt $t(p)$ von p gleich dem Anfangspunkt $s(q)$ von q ist.

e) Da Q_0 und Q_1 endliche Mengen sind, gibt es in Q genau dann unendlich viele Wege, falls es einen Weg positiver Länge (also ≥ 1) gibt, dessen Endpunkt mit dem Startpunkt übereinstimmt. Ein Weg $\alpha_1 \ldots \alpha_n$ mit $\alpha_i \in Q_1$ für $1 \leq i \leq n$ und $s(\alpha_1) = t(\alpha_n)$ und $n \geq 2$ heisst ein *Zykel*; genauer spricht man auch von einem *orientierten Zykel*, um klarzustellen, dass wir orientierte Wege betrachten. Ein Weg α der Länge Eins mit $s(\alpha) = t(\alpha)$ heisst eine *Schleife*.

Der Köcher Q_a in Beispiel 1.22 a) hat eine Schleife, besitzt also unendlich viele Wege. Diese sind $\alpha, \alpha^2, \alpha^3, \ldots$ sowie der faule Weg am Punkt 1, also e_1. Der Weg α^n (mit $n \in \mathbb{N}$) besteht hierbei aus der Hintereinanderausführung von n Pfeilen und ist damit ein Weg der Länge n. Der Köcher Q_c in Beispiel 1.22 c) hat die Wege $\alpha, \beta, \alpha\beta, e_1, e_2, e_3$. Der Weg $\alpha\beta$ bedeutet hierbei, gehe erst α, dann β. Im Köcher Q_c gibt es also insgesamt sechs verschiedene Wege. Im Köcher Q_c gilt also $\alpha\beta$ ist ein Weg der Länge zwei, während $\beta\alpha$ keinen Sinn macht, da $t(\beta) = 3 \neq 1 = s(\alpha)$.

Ähnlich wie die Gruppenalgebra definieren wir nun die Wegealgebra KQ eines Köchers Q:

Definition 1.24. Sei $Q = (Q_0, Q_1, s, t)$ ein Köcher und K ein Körper. Die *Wegealgebra KQ* ist ein K-Vektorraum mit Basis alle Wege im Köcher Q. Wege p und q werden multipliziert durch Hintereinanderausführung von Wegen, falls dies definiert ist, ansonsten ist das Produkt Null:

$$p \cdot q := \begin{cases} pq & \text{falls } t(p) = s(q), \\ 0 & \text{sonst.} \end{cases}$$

Diese Multiplikation von Wegen wird linear (man sagt hierzu auch distributiv) fortgesetzt zu einer Multiplikation auf dem Vektorraum KQ.

Beispiel 1.25. Sei K ein Körper. Der Köcher $Q_b: \; 2 \xleftarrow{\alpha} 1$ aus Beispiel 1.22 definiert also den K-Vektorraum mit Basis $\{e_1, e_2, \alpha\}$, das heisst die Wegealgebra

$$KQ_b = \{\lambda_1 e_1 + \lambda_2 e_2 + \lambda_\alpha \alpha \mid \lambda_1, \lambda_2, \lambda_\alpha \in K\}$$

ist drei-dimensional. Die Multiplikation auf der Basis dieses Vektorraumes ist gegeben durch

$\cdot$	e_1	e_2	α
e_1	e_1	0	α
e_2	0	e_2	0
α	0	α	0

Es gilt beispielsweise $(e_1+\alpha)\cdot(e_2-\alpha) = e_1e_2 - e_1\alpha + \alpha e_2 - \alpha\alpha = 0 - \alpha + \alpha - 0 = 0$.

Bemerkung 1.26.

a) Die Beispiele zeigen, dass die Multiplikation in der Wegealgebra KQ im allgemeinen nicht kommutativ ist. Das letzte Beispiel zeigt auch, dass Köcheralgebren Nullteiler haben können.

b) Im Vektorraum KQ gilt für die Multiplikation der faulen Wege:

   i) $e_i^2 = e_i$, für alle $i \in Q_0$; insbesondere ist e_i mit $i \in Q_0$ ein Idempotent.

   ii) $e_ie_j = 0$ für $i \neq j$; man sagt hierzu, dass die Idempotente $\{e_i \mid i \in Q_0\}$ paarweise *orthogonal* sind.

   iii) $\alpha \cdot e_i = \left\{ \begin{array}{ll} \alpha & \text{falls } t(\alpha)\text{=i} \\ 0 & \text{sonst,} \end{array} \right\}$ und genauso $e_i \cdot \alpha = \left\{ \begin{array}{ll} \alpha & \text{falls } s(\alpha)\text{=i} \\ 0 & \text{sonst.} \end{array} \right.$

Aufgabe 1.11. Bestimmen Sie die in Definition 1.24 definierte Basis der Wegealgebra KQ für Köcher Q mit:

a) $Q = Q_c: \; 1 \xrightarrow{\alpha} 2 \xrightarrow{\beta} 3$

b) $Q = Q_d:$
$$\begin{tikzcd} 1 \arrow[r, bend left, "\alpha"] \arrow[r, bend right, "\beta"] & 2 \end{tikzcd}$$

c) $Q = Q_e:$
$$\begin{tikzcd} & 3 \arrow[dr, "\beta"] & \\ 1 \arrow[ur, "\alpha"] \arrow[rr, "\gamma"] & & 2 \end{tikzcd}$$

Bestimmen Sie auch eine Multiplikationstafel für die angegebenen Basiselemente von KQ_e.

Proposition 1.27. *Sei K ein Körper und Q ein Köcher.*

a) Die Wegealgebra KQ ist eine K-Algebra mit Einselement $1_{KQ} = \sum_{l \in Q_0} e_l$.

b) Die Algebra KQ ist endlich-dimensional über K genau dann, wenn es keinen Weg p positiver Länge gibt mit $t(p) = s(p)$, also genau dann wenn Q keine Schleifen und keine orientierten Zykel hat.

Beweis: Nach Definition 1.24 ist KQ ein K-Vektorraum. Aneinanderhängen von Wegen ist assoziativ, also ist die in Definition 1.24 definierte Multiplikation assoziativ. Beachten Sie, hier muss man eine Fallunterscheidung machen: Wege sind komponierbar, oder eben nicht. Da Multiplikation von Wegen linear fortgesetzt wird, gilt in KQ das Distributivgesetz.

Für einen Weg p aus Q mit $s(p) = i$ und $t(p) = j$ gilt nach Bemerkung 1.26, dass $e_i \cdot p = p$ und $e_h \cdot p = 0$ für $h \neq i$. Es folgt, dass $1_{KQ} \cdot p = (\sum_{l \in Q_0} e_l) \cdot p = e_i \cdot p = p$ ist, und analog $p \cdot 1_{KQ} = p$. Dies impliziert, dass für ein Element $a \in KQ$ gilt: $1_{KQ} \cdot a = a = a \cdot 1_{KQ}$. Also ist $1_{KQ} = \sum_{l \in Q_0} e_l$ das Einselement in KQ.

Sei $\alpha \in KQ$ eine Schleife, sei $p := \alpha_1 \ldots \alpha_m$ ein orientierter Zykel in KQ. Dann ist α^n beziehungsweise p^n ein Vektor in der Basis von KQ, für alle $n \in \mathbb{N}$. Es folgt, dass $\dim_K KQ$ unendlich ist.

Umgekehrt, sei $\dim_K KQ$ unendlich. Da nach Definition 1.21 die Mengen Q_0 und Q_1 beide endlich sind, muss es in Q Wege geben, die denselben Punkt mehrmals durchlaufen. Es folgt daraus, dass der Köcher Q eine Schleife oder einen orientierten Zykel hat. $\square$

Bemerkung 1.28. Erlaubt man in Definition 1.21, dass die Punktemenge Q_0 unendlich viele Elemente hat, so sind die Elemente e_i weiterhin Idempotente, allerdings lässt sich kein Einselement in KQ definieren. Aus diesem Grund fordern wir in Definition 1.21, dass die Punktemenge Q_0 endlich ist.

Aufgabe 1.12. Diskutieren Sie die folgenden Aussagen:

a) Seien Q und $\tilde{Q}$ Köcher mit der gleichen Punkt- und Pfeilmenge, wobei die Pfeile in Q beziehungsweise $\tilde{Q}$ verschiedene Orientierung haben. Sind dann die Dimensionen der Algebren KQ und $K\tilde{Q}$ gleich?

b) Sei Köcher Q die *disjunkte Vereinigung* von Köchern Q' und Q'' – das heisst, dass Q_0 und Q_1 jeweils disjunkte Vereinigungen von Q'_0 und Q''_0 beziehungsweise Q'_1 und Q''_1 sind. Ist KQ isomorph zur direkten Summe von KQ' und KQ''?

Die Wegealgebren liefern viele Beispiele von Algebren. Wir wollen uns einige genauer anschauen und feststellen, dass wir manche diese Algebren bereits kennen.

Beispiel 1.29. Sei KQ Wegealgebra mit Köcher Q_a : $\begin{tikzcd} 1 \arrow[loop above, "\alpha"] \end{tikzcd}$ Dann hat KQ_a die Basis $\{e_1, \alpha, \alpha^2, \ldots\}$ mit Multiplikation $\alpha^i \cdot \alpha^j = \alpha^{i+j}$, für $i, j \in \mathbb{N}_0$ und mit $\alpha^0 = e_1$. Es folgt, dass die Abbildung $KQ \to K[X]$, definiert durch $\alpha \mapsto X$ ein Algebrenisomorphismus ist.

Beispiel 1.30. Für den Köcher Q_b : $1 \xrightarrow{\alpha} 2$ ist die Abbildung $\psi : KQ_b \to T_2(K)$ definiert durch

$$e_1 \mapsto E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_2 \mapsto E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad \alpha \mapsto E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},$$

und linear erweitert, ein Algebrenisomorphismus: die Abbildung bildet Basisvektoren auf Basisvektoren ab; hierbei entspricht die Multiplikation auf der Basis von KQ_b gerade der Multiplikation der Basis von $T_2(K)$:

$$\begin{array}{c|ccc} \cdot & e_1 & e_2 & \alpha \\ \hline e_1 & e_1 & 0 & \alpha \\ e_2 & 0 & e_2 & 0 \\ \alpha & 0 & \alpha & 0 \end{array} \quad \text{entspricht mittels } \psi \text{ gerade} \quad \begin{array}{c|ccc} \cdot & E_{11} & E_{22} & E_{12} \\ \hline E_{11} & E_{11} & 0 & E_{12} \\ E_{22} & 0 & E_{22} & 0 \\ E_{12} & 0 & E_{12} & 0 \end{array}.$$

Der Isomorphismus ψ wird also durch die folgende symbolische Matrix beschrieben:

$$\begin{pmatrix} e_1 & \alpha_1 \\ 0 & e_2 \end{pmatrix}.$$

Allgemeiner: Der Köcher A_n : $1 \xrightarrow{\alpha_1} 2 \xrightarrow{\alpha_2} 3 \overset{\cdots}{- - - - -} n{-}1 \xrightarrow{\alpha_{n-1}} n$ ist definiert durch Punktemenge $(A_n)_0 = \{1, \ldots, n\}$ mit Pfeilen $\alpha_i : i \to i+1$ für $1 \leq i \leq n-1$. Dann ist die Wegealgebra KA_n isomorph zur Algebra $T_n(K)$ der oberen Dreiecksmatrizen mit

$$e_i \quad \mapsto \quad E_{ii}, (\text{für } 1 \leq i \leq n), \qquad \alpha_i \mapsto E_{i,i+1}, (\text{für } 1 \leq i \leq n-1).$$

Für $n = 3$ beispielsweise ist dieser Isomorphismus also durch die folgende symbolische Matrix beschrieben:

$$\begin{pmatrix} e_1 & \alpha_1 & \alpha_1\alpha_2 \\ 0 & e_2 & \alpha_2 \\ 0 & 0 & e_3 \end{pmatrix},$$

die angibt wie der Isomorphismus Basiselemente der beiden Algebren identifiziert. Wir benutzen in diesem Beispiel, dass $E_{12} \cdot E_{23} = E_{13}$ ist. Vergleichen Sie mit Aufgabe 1.10 a).

Aufgabe 1.13. a) Sei Q der Köcher mit $Q_0 = \{1\}$ und $Q_1 = \{\}$. Zeigen Sie, dass $KQ \simeq K$ ist.

b) Bestimmen Sie für den Köcher Q_f : $1 \xrightarrow{\alpha} 2 \xleftarrow{\beta} 3$ eine Unteralgebra A von $M_3(K)$ mit $A \simeq KQ_f$, als Algebren.

c) Konstruieren Sie einen Köcher Q, so dass KQ als Algebra isomorph ist zur Algebra A_4 aus Aufgabe 1.7.

d) Ist die Algebra der 2×2-Matrizen über dem Körper K isomorph zur Wegealgebra eines Köchers? Begründen Sie Ihre Antwort.

Lemma 1.31. *Sei* $= (Q_0, Q_1, s, t)$ *Köcher und* $A = KQ$ *die zugehörige Wegealgebra. Definiere den sogenannten entgegengesetzten Köcher* Q^{op} *durch* $Q_0^{op} := Q_0$ *und*

$$Q_1^{op} := \{\alpha^{op} : j \to i \mid \alpha : i \to j \text{ in } Q_1\}.$$

Dann gilt $A^{op} \simeq K(Q^{op})$*, als Algebren.*

Wir haben hierbei eine Klammer in $K(Q^{\mathrm{op}})$ gesetzt, um zu verdeutlichen, dass sich das op auf Q bezieht, und nicht auf KQ.

Beweis: Definiere die Abbildung $\mathrm{op} : A^{\mathrm{op}} \to K(Q^{\mathrm{op}})$ durch die Vorschrift:

$$e_i \quad \mapsto \quad e_i^{\mathrm{op}} = e_i, \quad \alpha \mapsto \alpha^{\mathrm{op}},$$

für $\alpha \in Q_1$ und erweitere multiplikativ und linear. Insbesondere bedeutet dies, dass per Definition für Wege α_1, α_2 in Q gilt: $\mathrm{op}(\alpha_1 * \alpha_2) = \mathrm{op}(\alpha_1) \cdot \mathrm{op}(\alpha_2) = \alpha_1^{\mathrm{op}} \alpha_2^{\mathrm{op}}$, wobei $*$ die Multiplikation in A^{op} ist. Nach Definition bildet die Abbildung op eine Basis von A^{op} auf eine Basis von $K(Q^{\mathrm{op}})$ ab. Daher ist op ein Vektorraumisomorphismus. Das Einselement von A^{op} ist $1_{A^{\mathrm{op}}} = 1_A$. Das Einselement von $K(Q^{\mathrm{op}})$ ist $1_{K(Q^{\mathrm{op}})} = \sum_{i \in Q_0} e_i^{\mathrm{op}} = \sum_{i \in Q_0} e_i$. Die Abbildung op bildet Einselement auf Einselement ab:

$$\mathrm{op}(1_{A^{\mathrm{op}}}) = \mathrm{op}(\sum_{i \in Q_0} e_i) = \sum_{i \in Q_0} e_i = 1_{K(Q^{\mathrm{op}})}.$$

Nach Definition ist die Abbildung multiplikativ. Damit ist die Abbildung op ein Algebrenisomorphismus. □

Aufgabe 1.14. Diskutieren Sie die folgenden Aussagen:

a) Ist KQ_c isomorph zu $K(Q_c^{\mathrm{op}})$? Wie sieht dieselbe Frage aus für Köcher Q_d beziehungsweise Köcher Q_e?

b) Sei $n \in \mathbb{N}$ und I die Menge der Linearkombinationen von Wegen mit Länge mindestens n. Dann ist I ein zweiseitiges Ideal in KQ. Geben Sie Beispiele von Algebren an, die man als KQ/I schreiben kann. Geben Sie insbesondere solche Beispiele an, bei denen KQ unendlich-dimensional ist und KQ/I endlich-dimensional, und solche, bei denen KQ/I selbst keine Wegealgebra ist.

1.4 Weitere Beispiele von Algebren

Im letzten Abschnitt dieses Kapitels behandeln wir weitere Beispiele, insbesondere klassifizieren wir die zwei-dimensionalen Algebren über dem Körper $K = \mathbb{R}$ der reellen Zahlen. Dieser Abschnitt pausiert in der Weiterentwicklung der Theorie, und wir wollen an Beispieln ganz explizit sehen, wie man mit Algebren arbeitet. Algebren sind Vektorräume und gleichzeitig Ringe: achten Sie bei den folgenden Argumenten jeweils darauf, ob Argumente aus Linearer Algebra oder aus Ringtheorie benutzt werden, und welche.

Sei A eine zwei-dimensionale Algebra über den reellen Zahlen. Dann hat A eine Basis bestehend aus zwei Elementen. Wir wählen hierzu zunächst das Einselement $1 \neq 0$ aus. Ein Vektor ungleich dem Nullvektor ist linear unabhängig, und nach dem Basisergänzungssatz existiert ein Element $x \in A$, so dass $\{1, x\}$ Basis von

A ist. Wir zeigen, dass das Element x immer so gewählt werden kann, dass $x^2 \in \{0, \pm 1\}$ liegt. Dies nutzen wir dann, um die zwei-dimensionalen reellen Algebren zu klassifizieren; bis auf Isomorphie sind diese: $\mathbb{R} \times \mathbb{R}$, die komplexen Zahlen $\mathbb{C}$ sowie die Quotientenalgebra $\mathbb{R}[X]/(X^2)$ des Polynomrings $\mathbb{R}[X]$.

Aufgabe 1.15. Machen Sie sich die Algebrenstruktur der drei genannten Objekte, also von $\mathbb{R} \times \mathbb{R}$, $\mathbb{C}$ beziehungsweise $\mathbb{R}[X]/(X^2)$ klar, und diskutieren Sie in jedem Fall, ob die genannte Algebra isomorph zu einer Wegealgebra oder einem Quotienten einer Wegealgebra ist.

Bemerkung 1.32. Wir zeigen als erstes, dass wir die Basis $\{1, x\}$ von A so wählen können, dass gilt $x^2 \in \{0, \pm 1\}$. Sei also $\{1, y\}$ Basis von A. Die Algebra A ist multiplikativ abgeschlossen, also ist $y^2 \in A$. Da $\{1, y\}$ eine Basis von A ist, existieren nach Linearer Algebra Skalare $\alpha, \beta \in K$ mit $y^2 = \alpha 1 + \beta y$. Quadratische Ergänzung ergibt:

$$0 = y^2 - \beta y - \alpha 1 = (y - \beta/2)^2 - (\alpha 1 + (\beta/2)^2). \tag{1.2}$$

Wir unterscheiden nun drei verschiedene Fälle.

a) Sei $\alpha = 0 = \beta$. Dann ist $y^2 = 0$ und $\{1, y\}$ Basis von A. In diesem Fall wählen wir also $x = y$ und die Behauptung folgt.

b) Sei $\beta = 0$ und $\alpha \neq 0$. Dann ist $y^2 = \alpha 1$ ein Skalar. Setze $x = (1/\sqrt{|\alpha|}) \cdot y$. Dann ist $x^2 = (1/|\alpha|)y^2 = \pm 1$. Hierbei ist x ein skalares Vielfaches von y mit $x \neq 0$, und damit ist $\{1, x\}$ eine Basis von A.

c) Sei $\beta \neq 0$ und $\alpha \neq 0$. Setze $x' = y - (\beta/2)1$. Mit dem Austausch-Lemma aus Linearer Algebra folgt, dass $\{1, x'\}$ Basis von A ist. Hierbei ist $(x')^2 = (y - \beta/2)^2 = \alpha + (\beta/2)^2$ ein Skalar. Ist dieses Skalar ungleich Null, so rechnet man weiter wie im zweiten Fall und setzt $x = \frac{1}{\sqrt{|\alpha + (\beta/2)^2|}} x'$. Ist hingegen das Skalar $\alpha + (\beta/2)^2 = 0$, so wähle $x = x' = y - (\beta/2)1$ mit $x^2 = 0$.

In allen Fällen existiert also ein Element $x \in A$, so dass $\{1, x\}$ Basis von A ist mit $x^2 \in \{0, \pm 1\}$.

Aufgabe 1.16. Diskutieren Sie die Aussage: Bemerkung 1.32 impliziert, dass es bis auf Isomorphie maximal drei zwei-dimensionale Algebren über dem Körper der reellen Zahlen gibt.

Wir führen die folgende Notation ein:

Notation 1.33. Wir schreiben A_j für die zwei-dimensionale Algebra über den reellen Zahlen mit Basis $\{1, x\}$ mit $x^2 = j \cdot 1$. Mit dieser speziellen Basis werden wir im Folgenden arbeiten, ohne sie explizit jedesmal erneut einzuführen.

Bemerkung 1.34. Da die Basiselemente $\{1, x\}$ kommutativ sind bezüglich der Multiplikation und da reelle Zahlen kommutieren, folgt, dass die Algebren A_0, A_1 und A_{-1} kommutativ sind:

$$(\alpha 1 + \beta x) \cdot (\gamma 1 + \delta x) = \alpha\gamma 1 + \alpha\delta x + \beta\gamma x + \beta\delta x^2 = (\gamma 1 + \delta x) \cdot (\alpha 1 + \beta x)$$

für $\alpha, \beta, \gamma, \delta \in \mathbb{R}$.

Im Folgenden zeigen wir, dass die drei Algebren A_0, A_1 und A_{-1} paarweise nicht-isomorph sind. Ausserdem analysieren wir die Struktur der drei Algebren.

Beispiel 1.35. Sei A_1 Algebra mit Basis $\{1, x\}$ mit $x^2 = 1$. Angenommen es existiert ein Element $a \in A_1$ mit $a^2 = 0$. Schreibe Element a in der Vektorraumbasis, also als $a = \alpha 1 + \beta x$ mit $\alpha, \beta \in \mathbb{R}$. Dann ist

$$0 = a^2 = (\alpha 1 + \beta x)^2 = \alpha^2 + 2\alpha\beta x + \beta^2 x^2 = (\alpha^2 + \beta^2) + 2\alpha\beta x.$$

Da $\{1, x\}$ eine Basis von A_1 ist, folgt $\alpha^2 + \beta^2 = 0$ sowie $\alpha\beta = 0$. In den reellen Zahlen existieren keine Nullteiler. Also ist $\alpha = \beta = 0$, und damit $a = 0$. In der Algebra A_1 existiert also keine Basis $\{1, a\}$ mit $a^2 = 0$. Insbesondere folgt, dass die Algebren A_0 und A_1 nicht isomorph sind.

Wir beobachten weiterhin, dass beide Algebren Nullteiler besitzen: im Fall von A_0 ist der Basisvektor x ein Nullteiler wegen $x^2 = 0$. Im Fall A_1 gilt für den speziell gewählten Basisvektor x stattdessen: $(x - 1)(x + 1) = x^2 - 1 = 1 - 1 = 0$. Wir zeigen in Bemerkung 1.38, dass die Algebra A_{-1} ein Körper ist. Da Körper keine Nullteiler haben, folgt dass A_{-1} weder isomorph zu A_0, noch isomorph zu A_1 ist.

Beispiel 1.36. Sei A_0 Algebra mit Basis $\{1, x\}$ mit $x^2 = 0$. Sei $I = (X^2)$ Ideal in der Algebra $\mathbb{R}[X]$, erzeugt durch X^2. Definiere die Abbildung

$$\psi : A_0 \to \mathbb{R}[X]/I, \text{ durch } 1 \mapsto 1 + I \text{ und } X \mapsto X + I,$$

und erweitere linear. Man prüft leicht, dass ψ ein Algebrenisomorphismus ist. Beispielsweise ist die Abbildung ψ multiplikativ:

$$\begin{aligned}
\psi((\alpha 1 + \beta x)(\gamma 1 + \delta x)) &= \psi(\alpha\gamma 1 + (\alpha\delta + \beta\gamma)x) \\
&= \alpha\gamma 1 + (\alpha\delta + \beta\gamma)X + I \\
&= (\alpha 1 + \beta X)(\gamma 1 + \delta X) + I \\
&= (\alpha 1 + \beta X + I)(\gamma 1 + \delta X + I) \\
&= \psi(\alpha 1 + \beta x)\psi(\gamma 1 + \delta x).
\end{aligned}$$

Nach Definition bildet ψ Basiselemente von A_0 auf Basiselemente von $\mathbb{R}[X]/I$ ab, also ist die Abbildung ψ bijektiv.

Beispiel 1.37. Sei A_1 Algebra mit Basis $\{1, x\}$ mit $x^2 = 1$. Definiere die Abbildung $\psi : A_1 \to \mathbb{R} \times \mathbb{R}$ durch $1 \mapsto (1, 1)$ und $x \mapsto (-1, 1)$, und erweitere linear. Dann ist $\psi(\alpha 1 + \beta x) = (\alpha - \beta, \alpha + \beta)$. Nach Definition ist also ψ eine lineare Abbildung, die das Einselement von A_1 auf das Einselement $(1, 1)$ von $\mathbb{R} \times \mathbb{R}$ schickt. Wie in Beispiel 1.36 folgt leicht, dass ψ multiplikativ ist. Die Vektoren $(1, 1)$ und $(-1, 1)$ sind linear unabhängig in $\mathbb{R} \times \mathbb{R}$. Da sowohl A_1 als auch $\mathbb{R} \times \mathbb{R}$ zwei-dimensionale $\mathbb{R}$-Algebren sind, bildet ψ Basis auf Basis ab, also ist ψ ein Algebrenisomorphismus.

Beispiel 1.38. Die komplexen Zahlen bilden einen Vektorraum der Dimension zwei über den reellen Zahlen. Ausserdem besitzen die komplexen Zahlen als Körper eine Ringstruktur; es ist also $\mathbb{C}$ eine $\mathbb{R}$-Algebra mit Basis $\{1, i\}$ mit $i^2 = -1$. Dann ist nach Aufgabe 1.16 die Algebra A_{-1} isomorph zur $\mathbb{R}$-Algebra $\mathbb{C}$. Ein Isomorphismus zwischen den beiden Algebren wird realisiert, indem man Basis auf Basis abbildet: $1 \mapsto 1$ und $i \mapsto x$. Das multiplikative Inverse zu einer komplexen Zahl $0 \neq \alpha + \beta i$ ist $\frac{\alpha - \beta i}{\alpha^2 + \beta^2}$. Entsprechend ist das multiplikative Inverse zu $0 \neq \alpha 1 + \beta x \in A_{-1}$ das Element $\frac{\alpha 1 - \beta x}{\alpha^2 + \beta^2}$. Zusammen mit Beispiel 1.35 haben wir damit gesehen, dass die drei Algebren A_0, A_1 und A_{-1} paarweise nicht-isomorph sind.

Wir beenden das erste Kapitel mit einigen weiteren Aufgaben, um Konzepte aus diesem Kapitel zu vertiefen und den Chinesischen Restsatz zu wiederholen.

Aufgabe 1.17. Gegeben sei der Köcher $Q : 1 \underset{\beta}{\overset{\alpha}{\leftrightarrows}} 2$ und weiterhin in der Wegealgebra KQ die vier Ideale

$$\begin{aligned} I_1 &= (\alpha\beta), & I_2 &= (\alpha\beta, \beta\alpha), \\ I_3 &= (\alpha\beta, \beta\alpha\beta), & I_4 &= (\alpha\beta - e_2, \beta\alpha - e_1). \end{aligned}$$

a) Bestimmen Sie die Dimension der Algebra KQ/I_i für $1 \leq i \leq 4$.

b) Gibt es Indizes $i, j \in \{1, 2, 3, 4\}$ mit $i \neq j$, so dass die Algebren KQ/I_i und KQ/I_j isomorph sind?

c) Gibt es einen Index $1 \leq i \leq 4$ mit $KQ/I_i \simeq M_2(K)$?

d) Sei n eine gegebene natürliche Zahl. Gibt es zum gegebenen Köcher Q ein Ideal I, so dass KQ/I eine Algebra der Dimension $2n$ oder $2n + 1$ ist?

Begründen Sie jeweils Ihre Antwort.

Ist Q ein Köcher, so heisst eine Linearkombination von Wegen in Q, die alle denselben Start- und Endpunkt besitzen, eine *Relation* in Q. In der letzten Aufgabe ist also beispielsweise $\alpha\beta - e_2$ eine Relation im gegebenen Köcher Q: sowohl der Weg $\alpha\beta$ als auch der Weg e_2 haben den Startpunkt 2; sowohl der Weg $\alpha\beta$ als auch der Weg e_2 haben den Endpunkt 2; Startpunkt und Endpunkt der Wege müssen hierbei nicht gleich sein: $\beta - \beta\alpha\beta$ ist auch eine Relation. Ein Ideal I, welches von Relationen $R_1, \ldots, R_l$ in Q erzeugt wird, ist nach der Algebravorlesung gerade

$$I = (R_1, \ldots, R_l) = KQR_1KQ + \ldots + KQR_lKQ = (R_1) + \ldots + (R_l).$$

Aufgabe 1.18. Diskutieren Sie die folgenden Aussagen:

a) Sei KQ/I endlich-dimensional über K. Ist das Ideal I dann von endlich vielen Relationen erzeugt?

b) Sei KQ irgendeine Wegealgebra und I ein zweiseitiges Ideal in KQ, das von endlich vielen Elementen $a_1, \ldots, a_n$ erzeugt ist. Ist I dann auch von Relationen erzeugt, und sogar von endlich vielen?

Aufgabe 1.19. Sei n eine natürliche Zahl, sei K ein Körper und C_n die zyklische Gruppe der Ordnung n. Sei $V_4 = C_2 \times C_2$ die Kleinsche Vierergruppe.

a) Zeigen Sie, dass gilt $KC_4 \simeq K[X]/(X^4 - 1)$.

b) Zeigen Sie, dass gilt $KV_4 \simeq K[X,Y]/(X^2 - 1, Y^2 - 1)$.

c) Sei $K = \mathbb{C}$. Ist dann $KC_4 \simeq KV_4$? Begründen Sie Ihre Antwort.

Kapitel 2

Darstellungen und Moduln

2.1 Darstellungen

In diesem Kapitel ist K ein Körper und A eine Algebra über dem Körper K.

Definition 2.1. Eine *Darstellung* der Algebra A ist ein K-Vektorraum V zusammen mit einem Algebrenhomomorphismus $r : A \to \mathrm{End}_K(V)$. Der *Grad* der Darstellung r ist definiert als $\dim_K(V)$. Eine *(Matrix-)Darstellung* von A ist eine natürliche Zahl n zusammen mit einem Algebrenhomomorphismus $R : A \to M_n(K)$. Die natürliche Zahl n wird hierbei als der *Grad* der Matrixdarstellung bezeichnet. Die Darstellung r (oder R) von A heisst *treu*, falls ihr Kern trivial ist, also falls

$$\ker(r) := \{a \in A \mid r(a) = 0\} = \{0\} \text{ bzw. } \ker(R) := \{a \in A \mid R(a) = 0\} = \{0\}.$$

Darstellungen sind nach Definition 2.1 nichts anderes als Algebrenhomomorphismen $A \to \mathrm{End}_K(V)$, wobei V ein K-Vektorraum ist, beziehungsweise Algebrenhomomorphismus $A \to M_n(K)$, wobei n eine natürliche Zahl ist. Wir reden im Folgenden kurz von Homomorphismen statt Algebrenhomomorphismen. Es ergibt sich hierbei in der Regel aus dem Zusammenhang (welche Objekte betrachten wir gerade), um welche Art von Homomorphismus (Gruppen, Ringe, Algebren etc) es sich handelt. In Definition 2.1 haben wir zwei Arten von Darstellungen definiert, zum einen solche, deren Bild in $\mathrm{End}_K(V)$ ist, und zum anderen Matrixdarstellungen, deren Bild in $M_n(K)$ ist. Der Zusammenhang zwischen Darstellungen und Matrixdarstellungen wird mit Hilfe von Beispiel 1.17 erklärt:

Bemerkung 2.2. Sei $r : A \to \mathrm{End}_K(V)$ eine Darstellung der Algebra A, mit $n := \dim_K(V)$.

a) Sei B eine Basis des Vektorraumes V. Nach Beispiel 1.17 existiert ein Algebrenisomorphismus $\epsilon = \epsilon_B : \mathrm{End}_K(V) \to M_n(K)$, definiert durch $T \mapsto M_B(T)$. Definiere $R := \epsilon \circ r : A \to M_n(K)$. Die Komposition von Homomorphismen ist wieder ein Homomorphismus, siehe Bemerkung 1.15. Also ist R eine Matrixdarstellung von A. Wir sagen auch *Darstellung r induziert die Matrixdarstellung R.*

b) Basen von Vektorräumen sind nicht eindeutig. Sei also B' eine weitere Basis von V. Nach Beispiel 1.17 existiert dann wie in a) ein Algebrenisomorphismus

$\epsilon' = \epsilon'_B : \mathrm{End}_K(V) \to M_n(K)$, definiert durch $T \mapsto M_{B'(T)}$. Dann induziert r auch die Matrixdarstellung $R' := \epsilon' \circ r : A \to M_n(K)$.

c) Mit Hilfe von Linearer Algebra können wir klären, wie sich R und R' unterscheiden: Nach Linearer Algebra I existiert eine invertierbare Matrix $X := M_B^{B'}(\mathrm{id})$ mit

$$\epsilon'(T) = M_{B'}(T) = X^{-1}M_B(T)X = X^{-1}\epsilon(T)X, \tag{2.1}$$

für alle $T \in \mathrm{End}_K(V)$. Um die Notation für Matrix X zu erklären, erinnern wir kurz an die Details aus Linearer Algebra. Bei Matrix X handelt es sich um die Basiswechselmatrix von Basis B' zu Basis B. Die obige Gleichung (2.1) folgt also aus der folgenden Komposition von Abbildungen

$$V_{B'} \overset{\mathrm{id}}{\to} V_B \overset{T}{\to} V_B \overset{\mathrm{id}}{\to} V_{B'}$$

die mit Linearer Algebra in ein Produkt von Matrizen übersetzt wird; hierbei bedeutet V_B, dass wir den Vektorraum V mit der Basis B versehen betrachten, und entsprechend $V_{B'}$, dass wir den Vektorraum V mit der Basis B' versehen betrachten. Für $a \in A$ sind die Elemente $r(a)$ lineare Abbildungen in $\mathrm{End}_K(V)$. Also gilt:

$$R'(a) = \epsilon'(r(a)) = X^{-1}\epsilon(r(a))X = X^{-1}R(a)X,$$

für alle $a \in A$. Beachten Sie hierbei: Die Matrix X selber hängt nicht von wechselnden linearen Abbildungen ab, ist unabhängig von den Algebrenelementen $a \in A$. In der Linearen Algebra konjugiert man eine lineare Abbildung mit einer invertierbaren linearen Abbildung, und dies entspricht einem Basiswechsel. Hier konjugieren wir viele lineare Abbildungen $r(a)$ beziehungsweise Matrizen $R(a)$ simultan, mit derselben invertierbaren linearen Abbildung beziehungsweise invertierbaren Matrix X. Hier wird also ein Basiswechsel an vielen verschiedenen linearen Abbildungen simultan durchgeführt.

Die Betrachtungen in dieser Bemerkung motivieren die folgende Definition:

Definition 2.3. Darstellungen R und R' einer Algebra A heissen *äquivalent*, falls es eine invertierbare Abbildung X gibt mit $R'(a) = X^{-1}R(a)X$, für alle $a \in A$.

Proposition 2.4. *Seien R und R' Matrixdarstellungen derselben Algebra A. Dann sind R und R' äquivalente Darstellungen, genau dann, wenn es eine Darstellung r gibt, die (bezüglich verschiedener Basen) die Matrixdarstellungen R und R' im Sinne von Bemerkung 2.2 induziert.*

Beweis: Seien $R : A \to M_n(K)$ und $R' : A \to M_n(K)$ äquivalente Matrixdarstellungen. Dann existiert nach Definition 2.3 eine invertierbare Matrix $X \in M_n(K)$ mit

$$R'(a) = X^{-1}R(a)X$$

für alle $a \in A$. Jede invertierbare Matrix kann als eine Basiswechselmatrix aufgefasst werden. Wir interpretieren im Folgenden also $X = M_B^{B'}(\mathrm{id})$ für geeignete Basen B und B' von $V := K^n$.

a) Sei $V := K^n$ und $B := \{e_1, \ldots, e_n\}$ die Standardbasis von V. Definiere $r(a) : V \to V$ durch $v \mapsto R(a)v$. Multiplikation mit einer Matrix ist eine lineare Abbildung, also ist $r(a)$ eine lineare Abbildung in $\mathrm{End}_K(V)$. Definiere $r : A \to \mathrm{End}_K(V)$ durch $a \mapsto r(a)$. Da R ein Algebrenhomomorphismus ist, folgt nun leicht, dass Abbildung r ebenfalls ein Algebrenhomomorphismus ist. Diese Details zu prüfen, ist dem Leser überlassen.

b) Definiere Basis $B' := \{b'_1, \ldots, b'_n\}$ mit $b'_i := Xe_i$ für $1 \leq i \leq n$. Da X invertierbar ist, ist B' eine Basis von V mit $M_B^{B'}(\mathrm{id}) = X$. Mit diesem Set-up folgt die Behauptung nun durch Nachrechnen unter Benutzung von Linearer Algebra bezüglich des Basiswechsels $V_{B'} \xrightarrow{\mathrm{id}} V_B \xrightarrow{r(a)} V_B \xrightarrow{\mathrm{id}} V_{B'}$:

$$\begin{aligned} \epsilon_{B'}(r(a)) &= M_{B'}(r(a)) = M_{B'}^{B}(\mathrm{id}) \cdot M_B(r(a)) \cdot M_B^{B'}(\mathrm{id}) \\ &= X^{-1} \cdot R(a) \cdot X = R'(a). \end{aligned}$$

Also induziert die Darstellung r sowohl die Matrixdarstellung R als auch die Matrixdarstellung R' – im ersten Fall bezüglich Basis B, im zweiten Fall bezüglich Basis B'. Dies beweist die erste Richtung der Proposition. Die Rückrichtung der Proposition wurde bereits in Bemerkung 2.2 bewiesen. □

Beispiel 2.9 im nächsten Abschnitt enthält ein konkretes Beispiel zur Äquivalenz von Darstellungen.

Aufgabe 2.1. Sei K ein Körper und $A = K[X, Y]$ die Algebra aller Polynome in zwei kommutierenden Variablen über dem Körper K. Für $c \in K$ sei

$$J_c := \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}.$$

Für $\lambda \in K$ sei $\psi_\lambda : A \to M_2(K)$ Darstellung mit $\psi_\lambda(X) = J_1$ und $\psi_\lambda(Y) = J_\lambda$.

a) Warum definiert ψ_λ eine Darstellung von A?

b) Bestimmen Sie alle Matrizen $P \in M_2(K)$ mit $PJ_1 = J_1P$.

c) Für welche λ und μ sind die Darstellungen ψ_λ und ψ_μ äquivalent?

Bevor wir konkrete Darstellungen in Abschnitt 2.2 angeben, wollen wir zunächst Standardbeispiele von Darstellungen nennen.

Beispiel 2.5. Sei A eine K-Algebra.

a) Sei V ein K-Vektorraum mit $A \leq \mathrm{End}_K(V)$ Unteralgebra. Dann ist Inklusion $i : A \to \mathrm{End}_K(V), a \mapsto a$ ein Algebrenhomomorphismus, also eine Darstellung von A.

b) Die Algebra A ist nach Definition insbesondere ein Vektorraum. Sei in diesem Beispiel $V = A$. Definiere $\mathfrak{X} : A \to \mathrm{End}_K(V) = \mathrm{End}_K(A)$ durch $a \mapsto \mathfrak{X}(a)$, wobei $\mathfrak{X}(a)$ als die lineare Abbildung Multiplikation mit a von Links definiert sei. Dann ist $\mathfrak{X}$ ein Algebrenhomomorphimus, also eine Darstellung von A. Diese Darstellung heisst die *reguläre Darstellung* von A.

Aufgabe 2.2. Überprüfen Sie, dass die Abbildung $\mathfrak{X}$ aus Beispiel 2.5 b) eine Darstellung ist:

a) Zeigen Sie, dass $\mathfrak{X}(a)$ eine lineare Abbildung ist.

b) Zeigen Sie, dass $\mathfrak{X}$ ein Algebrenhomomorphismus ist.

Im nächste Beispiel geht es um die *Inflation* von Darstellungen, einem wichtigen und gleichzeitig einfachen Konzept zum Vergleichen von Darstellungen einer Algebra A und einer Quotientenalgebra A/I. Hierbei liefert jede Darstellung von A/I auch eine (nicht wirklich neue) Darstellung von A. Umgekehrt lässt sich aus einer gegebenen Darstellung einer Algebra A unter zu bestimmenden Umständen eine (nicht wirklich neue) Darstellung für die Quotientenalgebra A/I gewinnen. Dieses Beispiel ist später sehr wichtig bei der Weiterentwicklung der Theorie. Inflation bezeichnet einen genau bestimmten Prozess (bei dem nicht wirklich etwas passiert), der eine Darstellung von A/I zu einer Darstellung von A macht.

Beispiel 2.6. Sei A eine Algebra und I ein Ideal in A. Dann entsprechen die Darstellungen von A/I gerade denjenigen Darstellungen von A, welche I auf Null abbilden. Im Folgenden beweisen wir diese Aussage:

a) Sei $\rho : A \to \mathrm{End}_K(V)$ eine Darstellung von A mit $\rho(I) = 0$. Definiere die Abbildung

$$\bar{\rho} : A/I \to \mathrm{End}_K(V) \text{ durch } a + I \mapsto \rho(a). \tag{2.2}$$

Immer wenn wir eine Abbildung auf Nebenklassen definieren, müssen wir überprüfen, dass die Abbildung wohldefiniert ist. Sei also $a + I = a' + I$ mit $a, a' \in A$. Schreibe $a = a' + i$ für ein $i \in I$. Nach Voraussetzung ist ρ ein Homomorphismus von Algebren, damit ist ρ insbesondere linear und es gilt:

$$\bar{\rho}(a + I) = \rho(a) = \rho(a' + i) = \rho(a') + \rho(i) = \rho(a') = \bar{\rho}(a' + I).$$

Also ist $\bar{\rho}$ wohldefiniert. Beachte, am vierten Gleichheitszeichen haben wir die Voraussetzung $\rho(I) = 0$ benutzt. Diese Voraussetzung wird also benötigt, um zu zeigen, dass $\bar{\rho}$ wohldefiniert ist. Da ρ linear ist, folgt Abbildung $\bar{\rho}$ ist auch linear. Nach Voraussetzung ist ρ multiplikativ, also gilt für alle $a, b \in A$:

$$\bar{\rho}((a + I)(b + I)) = \bar{\rho}(ab + I) = \rho(ab) = \rho(a) \cdot \rho(b) = \bar{\rho}(a + I) \cdot \bar{\rho}(b + I).$$

Also ist Abbildung $\bar{\rho}$ multiplikativ. Mit $\bar{\rho}(1_A + I) = \rho(1_A) = \mathrm{id}$ folgt, dass $\bar{\rho}$ ein Algebrenhomomorphismus, also eine Darstellung von A/I ist.

b) Die umgekehrte Richtung geht wie folgt: Sei $\rho : A/I \to \mathrm{End}_K(V)$ eine Darstellung der Quotientenalgebra A/I. Sei $\pi : A \to A/I$ die natürliche Projektion. Sei weiterhin $\hat{\rho} := \rho \circ \pi$, also

$$\hat{\rho} : A \xrightarrow{\pi} A/I \xrightarrow{\rho} \mathrm{End}_K(V), \quad a \mapsto a + I \mapsto \rho(a + I), \tag{2.3}$$

für alle $a \in A$. Mit 1.15 folgt, dass $\hat{\rho}$ ein Algebrenhomomorphismus ist, also eine Darstellung der Algebra A/I. Aus der Linearität der Abbildung ρ folgt in diesem Fall:

$$\hat{\rho}(I) = \rho(\pi(I)) = \rho(0_{A/I}) = 0.$$

Man sagt zu dem hier beschriebenen Prozess, dass die Darstellung von A/I zu einer Darstellung von A *hochgehoben* wird, *mittels Inflation.*

2.2 Gruppendarstellungen

In Definition 2.1 haben wir Darstellungen von Algebren definiert; in diesem Abschnitt zeigen wir den Zusammenhang zu Darstellungen von Gruppen auf. Sei n eine natürliche Zahl und sei V ein K-Vektorraum. Wir definieren

$$\begin{aligned} \mathrm{GL}_n(K) &:= \{A \in M_n(K) \mid A \text{ invertierbar}\}, \\ \mathrm{GL}(V) &:= \{f \in \mathrm{End}_K(V) \mid f \text{ invertierbar}\}. \end{aligned}$$

Dann ist $\mathrm{GL}_n(K)$ mit Matrixmultiplikation und $\mathrm{GL}(V)$ mit Komposition von Abbildungen eine Gruppe.

Bemerkung 2.7. a) Sei $(G, \cdot)$ eine multiplikativ geschriebene Gruppe und sei KG die in Beispiel 1.9 definierte Gruppenalgebra. Wie in Bemerkung 1.10 erklärt, betrachten wir $G \subset KG$.

i) Sei $\rho : G \to \mathrm{GL}(V)$ ein Gruppenhomomorphismus. Definiere die Abbildung

$$\tilde{\rho} : KG \to \mathrm{End}_K(V) \text{ durch } \tilde{\rho}(\sum_{g \in G} \lambda_g g) = \sum_{g \in G} \lambda_g \rho(g).$$

Die Abbildung $\tilde{\rho}$ entsteht durch lineare Erweiterung des Gruppenhomomorphismus ρ von G auf die Gruppenalgebra KG. Da ρ multiplikativ ist, ist auch $\tilde{\rho}$ multiplikativ. Damit folgt aus der Definition der Abbildung $\tilde{\rho}$, dass $\tilde{\rho}$ ein Algebrenhomomorphismus, also eine Darstellung der Algebra KG ist. Jeder Gruppenhomomorphismus von einer Gruppe G in die Gruppe $\mathrm{GL}_n(K)$ oder $\mathrm{GL}(V)$ liefert also eine Darstellung der Gruppenalgebra KG.

ii) Umgekehrt, sei $\tilde{\rho} : KG \to \mathrm{End}_K(V)$ eine Darstellung der Algebra KG. Nach Definition 2.1 ist dann $\tilde{\rho}$ ein Algebrenhomomorphismus, schickt also insbesondere das Einselement auf das Einselement und ist multiplikativ. Damit folgt, dass $\rho := \tilde{\rho}_{|G} : G \to \mathrm{GL}(V)$, also die Einschränkung der Abbildung $\tilde{\rho}$, multiplikativ, also ein Gruppenhomomorphismus ist. Hierbei ist noch zu überprüfen, dass ρ wohldefiniert, also $\tilde{\rho}(G) \subseteq \mathrm{GL}(V)$ ist. Sei hierzu $g \in G$. Dann ist:

$$\mathrm{id} = \tilde{\rho}(1) = \begin{cases} \tilde{\rho}(gg^{-1}) = \tilde{\rho}(g) \cdot \tilde{\rho}(g^{-1}), \\ \tilde{\rho}(g^{-1}g) = \tilde{\rho}(g^{-1}) \cdot \tilde{\rho}(g). \end{cases}$$

Also ist $\tilde{\rho}(g)$ invertierbar mit Inversem $\tilde{\rho}(g)^{-1}$, und damit gilt insbesondere $\mathrm{im}(\rho) = \tilde{\rho}(G) \subseteq \mathrm{GL}(V)$. Jede Darstellung von KG liefert also einen Gruppenhomomorphismus von G in die Gruppe der invertierbaren Matrizen $\mathrm{GL}_n(K)$ oder invertierbaren linearen Abbildungen $\mathrm{GL}(V)$, für geeignete natürliche Zahl n beziehungsweise einen geeigneten Vektorraum V.

Die beiden beschriebenen Prozesse sind invers zueinander, was die folgende Definition rechtfertigt: Ein Gruppenhomomorphismus $\rho : G \to \mathrm{GL}(V)$ heisst *Gruppendarstellung* von G auf V. Gruppendarstellungen werden ebenfalls einfach nur kurz als Darstellungen bezeichnet.

Wir haben gesehen, dass wir zwischen Darstellungen einer Gruppe und Darstellungen der zugehörigen Gruppenalgebra durch Linearisierung beziehungsweise Einschränkung wechseln können. Wir wollen uns im Folgenden einige konkrete Beispiele von Gruppendarstellungen anschauen; jedes dieser Beispiele liefert dann also auch eine Darstellung der zugehörigen Gruppenalgebra.

Beispiel 2.8. Um eine Darstellung einer Gruppenalgebra KG zu definieren, genügt es nach Bemerkung 2.7, einen Gruppenhomomorphismus auf den Erzeugern der Gruppe G zu definieren, und zu überprüfen, ob die Relationen dieser Erzeuger nach Anwendung des Homomorphismus weiterhin erfüllt sind. Beispielsweise sei $G := C_p = \langle x \mid x^p = 1\rangle$ die zyklische Gruppe mit p Elementen, wobei p eine Primzahl sei. Wir bezeichnen mit $\mathbb{Z}_p$ oder $\mathbb{F}_p$ den Körper mit p Elementen. Definiere

$$\rho : C_p \to \mathrm{GL}_2(\mathbb{Z}_p), \quad x \mapsto \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Da ρ ein Homomorphismus ist, folgt für $1 \le r \le p$:

$$\rho(x^r) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^r = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}.$$

In der Gruppe G gilt für den Erzeuger x die Relation $x^p = 1$. Für das Element $\rho(x)$ gilt diese Relation ebenfalls:

$$\rho(x^p) = \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = \rho(1).$$

Damit definiert ρ einen Gruppenhomomorphismus.

Aufgabe 2.3. Sei $Q_8 = \langle a, b \mid a^2 = b^2 = a^{-1}b^{-1}ab,\ a^4 = 1\rangle$ die Quaternionengruppe der Ordnung acht. Diskutieren Sie, ob durch die Zuordnung

$$a \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad b \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

eine Gruppendarstellung $\mathfrak{X} : Q_8 \to \mathrm{GL}_2(\mathbb{C})$ definiert wird.

Aufgabe 2.4. Bestimmen Sie bis auf Äquivalenz alle Matrixdarstellungen vom Grad Eins der folgenden Gruppen über dem Körper $K = \mathbb{C}$ der komplexen Zahlen:

a) der zyklischen Gruppe C_n, mit n eine natürliche Zahl;

b) der Kleinschen Vierergruppe V_4;

c) der symmetrischen Gruppe S_3.

Darstellungen einer explizit gegebenen Algebra zu finden, ist in der Regel ein sehr schwieriges, und teilweise ungelöstes Problem. Beispielsweise kennt man bis heute nicht die Grade aller sogenannten irreduziblen Darstellungen der Gruppenalgebren KS_n von symmetrischen Gruppen S_n über Körpern K von Primcharakteristik. Über Symmetriegruppen G von geometrischen Objekten lassen sich aber zumindest für die Gruppen G und damit auch für die Gruppenalgebra KG wenige konkrete Darstellungen konstruieren. Das werden wir explizit im nächsten Beispiel durchführen.

Beispiel 2.9. Sei G die Symmetriegruppe des Quadrates. Dann ist G die Diedergruppe mit acht Elementen, also

$$G = \langle \sigma, \tau \mid \sigma^4 = 1 = \tau^2,\ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle = D_8.$$

Wir legen das Quadrat ins Koordinatensystem, mit Schwerpunkt im Nullpunkt, und mit Seiten parallel zu den Achsen des Koordinatensystems. Wir interpretieren die Erzeuger σ und τ als Symmetrien des Quadrates: σ als Rotation des Quadrates um 90 Grad um den Nullpunkt, gegen den Uhrzeigersinn, und τ als Spiegelung des Quadrates an der y-Achse. Sei $V = \mathbb{R}^2$. Rotation und Spiegelung in der Ebene sind lineare Abbildungen $\sigma : V \to V$ beziehungsweise $\tau : V \to V$. Wir bestimmen die darstellenden Matrizen $\rho_i(\sigma)$ und $\rho_i(\tau)$ zu diesen beiden linearen Abbildungen, bezüglich verschiedener Basen B_i von V, mit $i = 1, 2$.

a) Sei Basis $B_1 := \{e_1, e_2\}$ die Standardbasis von V. Dann wird die Rotation σ um 90 Grad, beziehungsweise die Spiegelung τ an der y-Achse, beschrieben durch:

$$\begin{aligned}\rho_1(\sigma) &: V \to V, \text{ mit } e_1 \mapsto e_2 \text{ und } e_2 \mapsto -e_1,\\ \rho_1(\tau) &: V \to V, \text{ mit } e_1 \mapsto -e_1, \text{ und } e_2 \mapsto e_2.\end{aligned}$$

Es ist also

$$\rho_1(\sigma) = M_{B_1}(\sigma) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \rho_1(\tau) = M_{B_1}(\tau) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

b) Als nächstes wählen wir die Basis $B_2 := \{b_1 := e_1, b_2 := e_1 + e_2\}$. Dann wird die Rotation σ um 90 Grad, beziehungsweise die Spiegelung τ an der y-Achse, beschrieben durch:

$$\begin{aligned}\rho_2(\sigma) &: V \to V, \text{ mit } b_1 \mapsto -b_1 + b_2 \text{ und } b_2 \mapsto -2b_1 + b_2,\\ \rho_2(\tau) &: V \to V, \text{ mit } b_1 \mapsto -b_1, \text{ und } b_2 \mapsto -2b_1 + b_2.\end{aligned}$$

Es ist also

$$\rho_2(\sigma) = M_{B_2}(\sigma) = \begin{pmatrix} -1 & -2 \\ 1 & 1 \end{pmatrix}, \qquad \rho_2(\tau) = M_{B_2}(\tau) = \begin{pmatrix} -1 & -2 \\ 0 & 1 \end{pmatrix}.$$

Wir haben hiermit die Abbildungen $\rho_i : G \to \mathrm{GL}_2(\mathbb{R})$ auf den Erzeugern σ, τ der Gruppe G definiert. Es gilt hierbei für die obigen Matrizen

$$\rho_i(\sigma)^4 = I_2 = \rho_i(\tau)^2, \qquad \rho_i(\tau)^{-1}\rho_i(\sigma)\rho_i(\tau) = \rho_i(\sigma)^{-1}, \text{ für } i = 1, 2.$$

Es folgt, dass die Abbildungen $\rho_i : G \to \mathrm{GL}_2(\mathbb{R})$ Darstellungen von G sind. Die beiden Darstellungen ρ_1 und ρ_2 unterscheiden sich hierbei lediglich dadurch, dass sie bezüglich verschiedener Basen aufgeschrieben wurden. Es ist also ρ_1 äquivalent zu ρ_2. Genauer gilt:

$$\begin{aligned} \rho_2(\sigma) &= M_{B_2}^{B_1}(\mathrm{id}) \cdot \rho_1(\sigma) \cdot M_{B_1}^{B_2}, \\ \rho_2(\tau) &= M_{B_2}^{B_1}(\mathrm{id}) \cdot \rho_1(\tau) \cdot M_{B_1}^{B_2}, \end{aligned}$$

wobei die Basiswechselmatrix und ihre Inverse gegeben sind durch

$$M_{B_2}^{B_1}(\mathrm{id}) = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad M_{B_1}^{B_2}(\mathrm{id}) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Beispiel 2.10. Wir geben eine zweite Möglichkeit an, Darstellungen zu konstruieren. Hierzu wiederholen wir aus der Algebravorlesung: Eine Menge $\Omega = \{\omega_1, \ldots, \omega_n\}$ heisst eine *G-Menge*, falls es eine Operation gibt

$$G \times \Omega \to \Omega, (g, \omega) \mapsto g \cdot \omega \text{ mit } 1_G \cdot \omega = \omega \text{ und } (g \cdot h) \cdot \omega = g \cdot (h \cdot \omega),$$

für alle $g, h \in G$ und alle $\omega \in \Omega$. Mit Hilfe von G-Mengen lassen sich Permutationsdarstellungen konstruieren:

a) Sei G eine Gruppe und Ω eine endliche G-Menge. Sei V ein Vektorraum der Dimension $|\Omega|$, etwa mit Basis $B = \{b_i \mid i \in \Omega\}$. Wir definieren $g \cdot b_i := b_{g \cdot i}$, für alle $i \in \Omega$. Wir definieren die *Permutationsdarstellung* $\rho : KG \to \mathrm{End}_K(V)$ durch die Abbildungen $\rho(g) : V \to V$, $b_i \mapsto g \cdot b_i$, für alle $i \in \Omega$ und alle $g \in G$. Nach Definition sind die Abbildungen $\rho(g)$ linear. Aufgrund der Axiome der G-Menge erhalten wir eine Darstellung der Gruppe G, durch Linearisierung wie in Bemerkung 2.7 eine Darstellung der Gruppenalgebra KG.

b) Beispielsweise sei $G = S_3 = \langle \tau, \sigma \rangle$ mit $\tau = (1, 2)$ und $\sigma = (1, 2, 3)$, und sei $\Omega = \{1, 2, 3\}$. Dann ist Ω eine G-Menge mit $\pi \cdot i := \pi(i)$ für alle $\pi \in S_3$ und $i \in \Omega$. Damit erhalten wir die linearen Abbildungen

$$\rho(\tau) : \begin{cases} b_1 \mapsto \tau \cdot b_1 = b_2 \\ b_2 \mapsto \tau \cdot b_2 = b_1 \\ b_3 \mapsto \tau \cdot b_3 = b_3 \end{cases} \qquad \rho(\sigma) : \begin{cases} b_1 \mapsto \sigma \cdot b_1 = b_2 \\ b_2 \mapsto \sigma \cdot b_2 = b_3 \\ b_3 \mapsto \sigma \cdot b_3 = b_1 \end{cases}.$$

Bezüglich der Basis B erhalten wir die Matrixdarstellung $\rho : KS_3 \to M_3(K)$ mit:

$$M_B(\rho(\tau)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad M_B(\rho(\sigma)) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Wir schliessen diesen Abschnitt mit einem Beispiel von schlechter mathematischer Sprache. Darstellungen von Gruppen verhalten sich meistens wie Darstellungen von Algebren. Allerdings gibt es Beispiele, wo die Sprache auseinanderfällt. Der Begriff der *treuen* Darstellung liefert ein solches Beispiel. Wiederholen Sie Definition 2.1 einer treuen Darstellung einer Algebra. Für Gruppendarstellungen definieren wir treu wie folgt:

Definition 2.11. Eine Gruppendarstellung $\rho : G \to \mathrm{GL}(V)$ der Gruppe G heisst *treu*, falls $\ker(\rho) = \{g \in G \mid \rho(g) = \mathrm{id}\} = \{1\}$ ist.

Beispiel 2.12. Wir benutzen die Darstellungen ρ und $\tilde{\rho}$ der Gruppe $G = C_p$ aus Beispiel 2.8 und zeigen, dass die Gruppendarstellung ρ eine treue Darstellung ist. Die Darstellung $\tilde{\rho}$ der Gruppenalgebra KG, die durch lineare Erweiterung aus ρ entsteht, siehe Bemerkung 2.7, ist hingegen nicht treu. Es ist

$$\ker(\rho) = \{g \in G \mid \rho(g) = \mathrm{id}\} = \{x^r \mid \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\} = \{x^0 = 1_G\}.$$

Der Homomorphismus $\tilde{\rho} : \mathbb{Z}_p C_p \to M_2(\mathbb{Z}_p)$ hat hingegen nicht-trivialen Kern. Beispielsweise ist

$$\tilde{\rho}(x^0 - 2x + x^2) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Also ist $a := x^0 - 2x + x^2 \neq 0$ Element in $\ker(\tilde{\rho}) = \{a \in \mathbb{Z}_p C_p \mid \tilde{\rho}(a) = 0\}$.

Aufgabe 2.5. Sei A eine Algebra, und sei $I \trianglelefteq A$ ein Ideal. Sei G eine Gruppe. Diskutieren Sie die folgenden Aussagen:

a) Die Darstellung $\rho : S_3 \to \mathrm{GL}_3(\mathbb{C})$ aus Beispiel 2.10 ist treu.

b) Die Darstellung $\rho : \mathbb{C}S_3 \to M_3(\mathbb{C})$ aus Beispiel 2.10 ist treu.

c) Ist $\rho : KG \to M_n(K)$ eine treue Darstellung von KG, dann ist auch die Einschränkung $\rho_{|G}$ eine treue Darstellung von G.

d) Falls $\rho : A/I \to \mathrm{End}_K(V)$ treue Darstellung von A/I ist, dann ist auch die mittels Inflation hochgehobene Darstellung $\hat{\rho} : A \to \mathrm{End}_K(V)$ treu.

e) Die reguläre Darstellung $A \to \mathrm{End}_K(A)$ ist eine treue Darstellung. Siehe Beispiel 2.5 b).

Was sagt der Satz von Cayley aus der Algebravorlesung über die Existenz von treuen Darstellungen endlicher Gruppen?

Aufgabe 2.6. Sei $D_{2n} = \langle \sigma, \tau \mid \sigma^n = 1 = \tau^2,\ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$ die Diedergruppe mit $2n$ Elementen. Es ist bekannt, dass D_{2n} die Symmetriegruppe des regulären n-Ecks ist. Nutzen Sie dies, um eine Darstellung $\rho : D_{2n} \to \mathrm{GL}_2(\mathbb{R})$ vom Grad zwei zu konstruieren.

2.3 Moduln über Ringen

Eine gute Definition zu finden, gehört zu den ganz schwierigen Dingen in der Mathematik. Der Begriff des Moduls ist in der Algebra – neben Gruppen, Ringen, Körpern, Vektorräumen – einer der ganz grossen Definitionen, und stammt aus dem letzten Jahrhundert. Wir definieren Moduln zunächst allgemein über Ringen und stellen in diesem Abschnitt die technischen Hilfsmittel aus der Modultheorie bereit: Untermoduln, Modulhomomorphismen, bekannte Struktursätze wie den Homomorphiesatz, die Isomorphiesätze und die Untermodulkorrespondenz. Unser spezielles Interesse gilt den Moduln über Algebren. Wir sehen im nächsten Abschnitt, dass Moduln über Algebren gerade den Darstellungen einer Algebra entsprechen, die wir in dieser Vorlesung studieren wollen.

Sei R ein Ring, wie üblich mit Einselement. Sei weiterhin K ein Körper. Der Axiomatik nach sind Moduln salopp gesagt nichts anderes als Vektorräume über einem Ring:

Definition 2.13. Ein *Linksmodul* über R ist eine abelsche Gruppe $(M, +)$, zusammen mit einer Abbildung $R \times M \to M$, mit $(r, m) \mapsto r \cdot m$, derart dass gilt:

(M1) $(r + s) \cdot m = r \cdot m + s \cdot m$,

(M2) $r \cdot (m + n) = r \cdot m + r \cdot n$,

(M3) $r \cdot (s \cdot m) = (r \cdot s) \cdot m$,

(M4) $1_R \cdot m = m$,

für alle $r, s \in R$ und alle $m, n \in M$. Häufig schreibt man rm statt $r \cdot m$. Statt von einem Linksmodul über R zu reden, sagt man auch *R-Linksmodul*.

Normalerweise sagt man nun, analog definieren wir Rechtsmoduln. Um Verwirrung vorzubeugen, ist es sinnvoll, dies einmal hinzuschreiben: Ein *Rechtsmodul* über R oder *R-Rechtsmodul* ist eine abelsche Gruppe $(M, +)$, zusammen mit einer Abbildung $R \times M \to M$, mit $(r, m) \mapsto m \cdot r$, derart dass gilt:

(M1) $m(r + s) = mr + ns$,

(M2) $(m + n)r = mr + nr$,

(M3) $m(rs) = (mr)s$,

(M4) $m1_R = m$,

für alle $r, s \in R$ und alle $m, n \in M$. Um die Modulstruktur anzudeuten schreiben wir statt M bisweilen auch ${}_RM$ oder M_R. Die Notation ${}_RM$ bedeutet, dass M ein R-Linksmodul ist, und analog bedeutet M_R, dass M ein R-Rechtsmodul ist. Meistens schreiben wir nur kurz *Modul* statt Linksmodul oder Rechtsmodul, und man entnimmt dem Zusammenhang, ob es sich um einen Linksmodul oder einen Rechtsmodul handelt.

In der Regel behandeln wir in dieser Vorlesung Linksmoduln. Beim Überprüfen der Modulaxiome ist (M3) typischerweise das wichtigste dieser Axiome. Aber ohne das unscheinbare Axiom (M4) liesse sich viel Theorie nicht entwickeln. Vergleichen Sie auch sorgfältig die Definition des Moduls mit Beispiel 2.17, das erklärt wie G-Mengen Beispiele von Moduln liefern. Noch ein sprachlicher Hinweis: es heisst *der* Modul im Singular, die Moduln im Plural – im Baumarkt findet man auch *das* Modul, die Module.

Aufgabe 2.7. Sei R eine Ring und sei M ein R-Linksmodul. Diskutieren Sie: Wird M zu einem R-Rechtsmodul durch die Definition $R \times M \to M$, mit $m \cdot r := r \cdot m$, für $r \in R$ und $m \in M$?

Einige Aussagen über Moduln entsprechen Aussagen über Vektorräumen, und werden ganz analog bewiesen – siehe beispielweise Bemerkung 2.14 oder Definition 2.23.

Bemerkung 2.14. Sei M ein R-Modul.

a) Es ist $0 \cdot m = 0$, für alle $m \in M$: Es ist $0 \cdot m = (0+0) \cdot m \overset{(M1)}{=} 0m + 0m$. Beim ersten Gleichheitszeichen haben wir die Ringaxiome benutzt. Addiere das additive Inverse $-(0m)$ zu dieser Gleichung, dann folgt die Behauptung aus den Gruppenaxiomen der abelschen Gruppe M.

b) Es ist $r \cdot 0 = 0$, für alle $r \in R$. Der Beweis ist dem Leser überlassen.

Wir betrachten als nächstes Beispiele von Moduln; bisweilen betrachten wir Moduln über Ringen allgemein, insofern es Relevanz zur Vorlesung hat und so allgemein formuliert werden kann; meistens beschränken wir uns aber auf Beispiele von Moduln über Algebren.

Beispiel 2.15. Sei R eine Ring.

a) Ist $R = K$ ein Körper, so entsprechen R-Moduln gerade K-Vektorräumen. In diesem Sinne verallgemeinert der Begriff des Moduls den Begriff des Vektorraumes.

b) Sei $S \leq R$ ein Teilring. Sei M ein R-Modul. Dann ist M auch ein S-Modul durch Einschränkung der Operation.

c) Sei $V = R$, also insbesondere ist V eine abelsche Gruppe. Definiere

$$R \times V \to V, \quad (r, s) \mapsto r \cdot s \text{ (Ringmultiplikation).}$$

Dann ist V ein R-Modul, genannt der *reguläre* Linksmodul über dem Ring R, geschrieben ${}_R R$. Wir zeigen in Abschnitt 2.4, dass die Begriffe Darstellung und Modul äquivalent sind, insbesondere korrespondiert danach die reguläre Darstellung in Beispiel 2.5 zum regulären Modul.

d) Sind N_1 und N_2 zwei R-Moduln, so ist das kartesische Produkt $N_1 \times N_2$ wieder ein R-Modul mit Operation

$$r \cdot (n_1, n_2) := (r \cdot n_1, r \cdot n_2),$$

für alle $r \in R$ und $n_i \in N_i$ mit $i = 1, 2$. Das kartesische Produkt $N_1 \times N_2$ wird als *äussere oder externe direkte Summe* von Moduln bezeichnet.

Iterieren wir, so ist das kartesische Produkt $M_1 \times \ldots \times M_n$ von R-Moduln M_i mit $1 \leq i \leq n$ wieder ein R-Modul mit Operation

$$r(m_1, \ldots, m_n) := (rm_1, \ldots, rm_n)$$

für alle $r \in R$ und $m_i \in M_i$, mit $1 \leq i \leq n$. Wir schreiben

$$R^n := R \times R \times \ldots \times R$$

für das kartesische Produkt des regulären Moduls n-mal mit sich selber.

Bemerkung 2.16. In dieser Vorlesung geht es um Moduln über speziellen Ringen, nämlich über Algebren. Sei A eine K-Algebra. Nach Bemerkung 1.2 ist $K \subseteq A$. Es folgt, dass jeder A-Modul M immer auch ein K-Vektorraum ist. Entsprechend können wir beispielsweise von der Dimension eines Moduls reden, und meinen die Vektorraumdimension; und natürlich stehen uns hiermit beim Studium von Moduln die Konzepte der Linearen Algebra zur Verfügung. Wir vereinbaren weiterhin, dass wir in dieser Vorlesung endlich-dimensionale A-Moduln betrachten..

Beispiel 2.17. Sei G eine endliche Gruppe.

a) Sei G eine Gruppe und Ω eine endliche G-Menge. Wir definieren V als Vektorraum der Dimension $|\Omega|$, etwa mit Basis $B = \{b_i \mid i \in \Omega\}$. Wir definieren den wichtigen *Permutationsmodul* $K\Omega := V$ mit der Operation $g \cdot b_i := b_{g \cdot i}$, für alle $i \in \Omega$ und alle $g \in G$, linear erweitert. Dann ist die Operation von G auf $K\Omega$ linear, also ist $K\Omega$ ein KG-Modul. Wir zeigen in Abschnitt 2.4, dass die Begriffe Darstellung und Modul äquivalent sind, insbesondere korrespondiert danach die Permutationsdarstellung in Beispiel 2.10 zum Permutationsmodul.

b) Ganz ähnlich gilt: Sei V ein Vektorraum über K und gleichzeitig eine G-Menge mit Operation $G \times V \to V, (g, v) \mapsto g \cdot v$, für alle $g \in G$ und $v \in V$. Dann ist V mittels Linearisierung ein KG-Modul, falls die Operation von G auf V linear ist, das heisst, falls $g \cdot (v + w) = gv + gw$ und $g(\lambda v) = \lambda(gv)$, für alle $\lambda \in K, g \in G$ und $v, w \in V$. *Man definiert bisweilen Moduln über Gruppen, statt über Ringen oder Algebren: Ein G-Modul ist hierbei eine G-Menge und Vektorraum V, bei der G linear auf V operiert.*

c) Ein Spezialfall der obigen Konstruktion (wähle Ω einelementig mit trivialer Operation) ist der folgende Modul: Sei V ein eindimensionaler K-Vektorraum. Definiere die Operation $G \times V \to V$ durch $(g, v) \mapsto g \cdot v := v$, für alle $g \in G$ und $v \in V$. Erweitere diese Operation linear zu einer Operation von $KG \times V \to V$. Dann ist V ein KG-Modul, genannt der *triviale Modul* der Gruppenalgebra KG.

Wie bei allen algebraischen Objekten haben wir Unterobjekte und strukturerhaltende Abbildungen zwischen gleichartigen Objekten.

Definition 2.18. Sei R ein Ring und M ein R-Modul. Eine Untergruppe $(U, +)$ von $(M, +)$ heisst *Untermodul*, falls U bezüglich der Operation von R abgeschlossen ist, also $r \cdot u \in U$ ist, für alle $u \in U$ und alle $r \in R$. Wir schreiben $U \leq M$, falls U ein Untermodul von M ist. Wie üblich heisst ein Untermodul $U \leq M$ ein *echter* Untermodul von M, falls $U \neq M$ ist.

Beispiel 2.19. a) Sei M ein R-Modul. Es sind $\{0\}$ (kurz aus Faulheit als 0 geschrieben, also ohne Klammern zu setzen) und M Untermoduln des Moduls M. Der Nulluntermodul $\{0\}$ heisst auch *trivialer* Untermodul. Er ist zu unterscheiden vom trivialen eindimensionalen Modul für Gruppenalgebren, siehe Beispiel 2.17 c).

b) Die Linksideale von R sind genau die Linksuntermoduln des regulären R-Moduls ${}_RR$ aus Beispiel 2.15 c).

c) In Beispiel 2.15 d) sind $\{0\} \times N_2$ und $N_1 \times \{0\}$ Untermoduln von $N_1 \times N_2$.

Mit den üblichen algebraischen Konstruktionen erhalten wir weitere abstrakte Beispiele von Untermoduln: der Schnitt und die Summe von Untermoduln bilden wieder einen Untermodul:

Beispiel 2.20. Sei M ein R-Modul und seien M_1 und M_2 zwei Untermoduln von M. Dann gilt:

a) Der Schnitt $M_1 \cap M_2$ ist ein Untermodul von M; wir kennen das Resultat bereits für abelsche Gruppen. Sei $x \in M_1 \cap M_2$. Dann ist $x \in M_i$ für $i = 1, 2$. Da M_1 und M_2 Moduln sind, ist auch $rx \in M_i$ für $i = 1, 2$, also ist $rx \in M_1 \cap M_2$.

b) Die Summe von Untermoduln $X := M_1 + M_2$ ist ein Untermodul von M. Wir sagen, der Modul X ist eine *(innere oder interne) direkte Summe* von Untermoduln, geschrieben $X = M_1 \oplus M_2$, falls für alle $x \in X$ eindeutige Elemente $m_i \in M_i$ mit $i = 1, 2$ existieren, sodass $x = m_1 + m_2$ ist. Äquivalent dazu ist $X = M_1 \oplus M_2$, falls $X = M_1 + M_2$ ist mit $M_1 \cap M_2 = 0$. Bewiesen wird diese äquivalente Aussage wie in der Linearen Algebra für Vektorräume. Wir sagen, ein Untermodul $M \leq X$ ist ein *direkter Summand* von Modul X, falls er ein *Komplement* hat, also falls es einen Untermodul $N \leq X$ gibt mit $X = M \oplus N$.

Bemerkung 2.21. Nach Bemerkung 2.16 sind Moduln über Algebren immer Vektorräume. Untermoduln dieser Moduln sind entsprechend Untervektorräume. Ist also A eine Algebra und M ein (nach unserer Vereinbarung in Bemerkung 2.16 endlich-dimensionaler) A-Modul mit echtem Untermodul $N < M$, so gilt insbesondere $\dim_K(N) < \dim_K(M)$.

Nachdem wir Unterobjekte definiert haben, können wir als nächstes Quotientenobjekte definieren und erhalten ein weiteres Beispiel eines Moduls:

Beispiel 2.22. Sei M ein R-Modul mit Untermodul U. Dann ist die als Menge von Restklassen definierte Quotientengruppe $M/U = \{m + U \mid m \in M\}$ ein R-Modul mittels $r \cdot (m+U) := r \cdot m + U$. Wir müssen zeigen, dass die Operation wohldefiniert ist Sei $m + U = m' + U$. Dann existiert ein $u \in U$ mit $m = m' + u$, und es folgt:

$$r(m+U) \overset{\text{Def}}{=} rm + U = r(m'+u) + U = rm' + ru + U = rm' + U \overset{\text{Def}}{=} r(m'+U),$$

denn $ru \in U$ wegen U Modul. Am dritten Gleichheitszeichen haben wir Modulaxiom (M2) für Modul M benutzt. Damit ist die Operation von R auf der Quotientengruppe M/U wohldefiniert. Die Modulaxiome für M/U folgen nun aus den Modulaxiomen für M. Beispielsweise gilt mit (M3) für Modul M, dass

$$r(s(m+U)) \overset{\text{Def}}{=} r(sm+U) \overset{\text{Def}}{=} r(sm) + U \overset{(M3)}{=} (rs)m + U \overset{\text{Def}}{=} (rs)(m+U).$$

Dies beweist, dass (M3) auch für den Quotienten M/U gilt. Wir nennen M/U den *Quotientenmodul von M modulo U.*

Als nächstes definieren wir die strukturerhaltenden Abbildungen zwischen unseren Objekten:

Definition 2.23. Seien M und N zwei R-Moduln. Die Abbildung $\phi : M \to N$ heisst *R-Modulhomomorphismus* oder kurz *Homomorphismus*, falls gilt:

i) $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2)$,

ii) $\phi(r \cdot m) = r \cdot \phi(m)$,

für alle $m_1, m_2, m \in M$ und alle $r \in R$. Falls zusätzlich ϕ bijektiv ist, so heisst ϕ (Modul-)isomorphismus. Zwei R-Moduln M und N heissen *isomorph*, falls es einen Modulisomorphismus $\varphi : M \to N$ gibt. Wir schreiben in diesem Fall $M \simeq N$. Wir schreiben

$$\begin{aligned} \mathrm{Hom}_R(M,N) &:= \{f : M \to N \mid f \text{ ist } R\text{-Modulhomomorphismus}\}, \\ \mathrm{End}_R(M) &:= \mathrm{Hom}_R(M,M). \end{aligned}$$

Aufgabe 2.8. Sei R eine Ring beziehungsweise eine Algebra, und seien M und N zwei R-Moduln. Diskutieren Sie: Welche algebraische Struktur (Gruppen, Vektorräume, Ringe, Algebren, Moduln) haben jeweils die Mengen $\mathrm{Hom}_R(M,N)$ und $\mathrm{End}_R(M)$?

Bemerkung 2.24. a) Die Komposition von Modulhomomorphismen ist wieder ein Modulhomomorphismus: Seien $f : M_1 \to M_2$ und $g : M_2 \to M_3$ Modulhomomorphismen. Modulhomomorphismen sind Gruppenhomomorphismen bezüglich der Addition. Also wird die additive Struktur von $g \circ f$ erhalten. Ausserdem ist

$$(g \circ f)(rm) = g(f(rm)) = g(rf(m)) = rg(f(m)) = r(g \circ f)(m),$$

für alle $r \in R$ und $m \in M_1$. Das Inverse eines Modulisomorphismus ist ein Modulisomorphismus.

b) Sei $f : M \to N$ Modulhomomorphismus. Dann ist das Bild $\operatorname{im} f$ ein Untermodul von N und das Urbild $f^{-1}(N)$ ein Untermodul von M. Insbesondere ist $\ker f = f^{-1}(0)$ ein Untermodul in M. Nach Definition ist f ein Gruppenhomomorphismus. Die analogen Aussagen für Gruppen sind bereits aus früheren Vorlesungen bekannt. Zusätzlich gilt:

   i) Sei $n \in \operatorname{im} \phi$. Dann existiert $m \in M$ mit $\phi(m) = n$. Es folgt $\phi(rm) = r\phi(m) = rn$, das heisst, $rn \in \operatorname{im} \phi$ für alle $r \in R$. Nach Definition 2.18 ist $\operatorname{im} \phi \leq N$ Untermodul.

   ii) Sei $m \in f^{-1}(N)$. Nach Definition des Urbildes ist also $f(m) \in N$. Nach Voraussetzung ist N ein Modul und f ein Homomorphismus, also gilt $f(rm) = rf(m) \in N$. Die Definition des Urbilds liefert $rm \in f^{-1}(N)$. Nach Definition 2.18 ist also $f^{-1}(N)$ ein Untermodul von M.

c) Wir interessieren uns für Moduln über Algebren. Sei A eine K-Algebra und $\phi : M \to N$ ein A-Modulhomomorphismus. Dann ist ϕ eine K-lineare Abbildung: Nach Bemerkung 2.16 ist jeder A-Modul insbesondere ein K-Vektorraum. Seien $m_1, m_2 \in M$ und $\lambda_1, \lambda_2 \in K$. Nach Bemerkung 1.2 ist $K \subseteq A$, also ist $\phi(\lambda_1 m_1 + \lambda_2 m_2) = \lambda_1\phi(m_1) + \lambda_2\phi(m_2)$, also ϕ linear.

Beispiel 2.25. Sei M ein R-Modul.

a) Sei $M = U \oplus V$ interne direkte Summe von R-Moduln U und V. Dann sind die Einbettung $\iota : U \to M$ und die Projektion $\pi : M \to U$ entlang V Modulhomomorphismen. Allgemeiner, sei $U \leq M$ ein R-Untermodul. Dann ist die natürliche Projektion $\pi : M \to M/U, m \mapsto m + U$, für alle $m \in M$, ein R-Modulhomomorphismus:

$$\pi(rm) = rm + U = r(m + U) = r\pi(m), \text{ für alle } r \in R \text{ und } m \in M.$$

b) Das nächste Beispiel wirkt unscheinbar, ist aber wichtig für später. Wir definieren vom regulären Modul ausgehende Abbildungen. Sei $m \in M$ fest gewählt. Dann ist Multiplikation von Rechts mit m

$$r_m : {}_RR \overset{\cdot m}{\to} M, \quad r \mapsto r \cdot m, \text{ für } r \in R$$

ein R-Modulhomomorphismus:

$$\begin{aligned} r_m(r_1 + r_2) &= (r_1 + r_2) \cdot m = r_1 m + r_2 m = r_m(r_1) + r_m(r_2), \\ r_m(r_1 r_2) &= (r_1 r_2) \cdot m = r_1(r_2 m) = r_1 \cdot r_m(r_2), \end{aligned}$$

für alle $r_1, r_2 \in R$. Dieses Beispiel verallgemeinern wir noch. Das kartesische Produkt von Moduln ist wieder ein Modul, siehe Beispiel 2.15 d). Seien $m_1, \dots m_n \in M$ fest gewählt. Dann ist die Abbildung

$$\phi : R^n \to M, \quad (r_1, \dots, r_n) \mapsto \sum_{i=1}^{n} r_i m_i,$$

mit $r_i \in R$ für $1 \leq i \leq n$ ein R-Modulhomomorphismus.

c) In Beispiel 2.15 d) gilt $N_1 \times \{0\} \simeq N_1$ und $\{0\} \times N_2 \simeq N_2$, als Moduln, und $(N_1 \times \{0\}) \oplus (\{0\} \times N_2) = N_1 \times N_2$. Falls $M_1, M_2 \leq M$ mit $M_1 \oplus M_2 = M$ ist, dann ist $M_1 \times M_2 \simeq M = M_1 \oplus M_2$. Oft schreibt man deshalb auch $\oplus$ statt $\times$, und unterscheidet nicht zwischen innerer und äusserer direkter Summe.

Aufgabe 2.9. Sei K ein Körper und $(A, +_A, \cdot_A)$ eine Algebra über K. Sei $a \in A$ fest gewählt. Sei wie in Beispiel 2.25 die Abbildung $r_a : A \to A$ definiert durch $r_a(x) = x \cdot_A a$, Rechtsmultiplikation mit dem Element a. Zeigen Sie, dass

$$\operatorname{End}_A(A) = \{r_a \mid a \in A\}$$

ist, und folgern Sie, dass die Algebren $\operatorname{End}_A(A)$ und A^{op} isomorph sind.

Auch für Moduln gelten der Homomorphiesatz und die Isomorphiesätze. Moduln sind abelsche Gruppen mit Zusatzstruktur. Den Homomorphiesatz und die Isomorphiesätze kennen wir bereits für Gruppen. Zu prüfen bleibt bei den folgenden Sätzen also nur, ob die Aussagen mit der Moduloperation verträglich sind.

Theorem 2.26. *[Homomorphiesatz und Isomorphiesätze]*

a) Sei $\phi : M \to N$ ein R-Modulhomomorphismus. Dann sind $\ker \phi \leq M$ und $\operatorname{im} \phi \leq N$ Untermoduln mit $M/\operatorname{Ker} \phi \simeq \operatorname{im} \phi$.

b) Seien $U, V \leq M$ Untermoduln. Dann sind $U + V, U \cap V \leq M$ Untermoduln mit $(U + V)/U \simeq V/U \cap V$.

c) Seien $U \leq V \leq M$ Untermoduln. Dann ist $V/U \leq M/U$ Untermodul mit $(M/U)/(V/U) \simeq M/V$.

Beweis. Die Beweise verlaufen wie die Beweise analoger Sätze anderer algebraischer Objekte. Insbesondere folgen die beiden Isomorphiesätze aus dem Homomorphiesatz.

a) Da ϕ ein Gruppenhomomorphismus ist, gilt die Aussage des Homomorphiesatzes bereits für die Gruppenstruktur: die Abbildung

$$\psi : M/\ker \phi \to \operatorname{im} \phi, m + \ker \phi \mapsto \phi(m),$$

für alle $m \in M$, ist wohldefiniert und ein Gruppenisomorphismus. Es bleibt zu prüfen, ob der Isomorphismus mit der Operation von R kompatibel ist. Für $r \in R$ und $m \in M$ gilt:

$$\begin{aligned} \psi(r(m + \ker \phi)) &\overset{2.22}{=} \psi(rm + \ker \phi) \overset{\text{Def } \psi}{=} \phi(rm) \\ &= r\phi(m) \overset{\text{Def } \psi}{=} r\psi(m + \ker \phi). \end{aligned}$$

Am dritten Gleichheitszeichen haben wir benutzt, dass ϕ ein Modulhomomorphismus ist. Mit dieser Rechnung haben wir gezeigt, dass ϕ ein Modulisomorphismus ist.

b) Der bereits von den Isomorphiesätzen für Gruppen bekannte Gruppenisomorphismus

$$\psi : V/(U \cap V) \to (U+V)/U, \quad v + (U \cap V) \mapsto v + U$$

ist verträglich mit der Operation des Rings:

$$\psi(r(v+U\cap V)) = \psi(rv+(U\cap V)) = rv+U = r(v+U) = r\psi(v+(U\cap V)).$$

Damit ist ψ ein Modulisomorphismus.

c) Der bereits für Gruppen bekannte surjektive Gruppenhomomorphismus

$$\psi : M/U \to M/V, \quad m + U \mapsto m + V,$$

für $m \in M$ ist kompatibel mit der Operation des Rings:

$$\psi(r(m+U)) = \psi(rm+U) = rm+V = r(m+V) = r\psi(m+U).$$

Damit ist ψ ein Modulhomomorphismus mit $\ker\psi = V/U$. Mit dem Homomorphiesatz folgt die Behauptung. □

Die Untermodulkorrespondenz, die genauso bewiesen wird wie die Idealkorrespondenz in Aufgabe 1.9, werden wir in Beispielen und der Theorie immer wieder benötigen; sie sollte deshalb gut verstanden werden.

Theorem 2.27 (Untermodulkorrespondenz)**.** *Sei M ein R-Modul und $U \leq M$ Untermodul. Dann gibt es eine Inklusions-erhaltende Bijektion zwischen der Menge aller Untermoduln von M/U und der Menge aller Untermoduln von M, die U enthalten.*

Beweis. In der einen Richtung ist die Bijektion durch modulo U rechnen gegeben. In der Rückrichtung nehmen wir das Urbild des Untermoduls $X \leq M/U$ unter der Projektion $\pi : M \to M/U$. Nach Bemerkung 2.24 ist $\pi^{-1}(X)$ ein Untermodul von M, der U enthält. Die beiden definierten Abbildungen sind invers zueinander. Insbesondere ist also $X = \pi^{-1}(X)/U$. Das Ausarbeiten weiterer Details ist dem Leser überlassen. □

Aufgabe 2.10. Betrachten Sie $\mathbb{C}$ als regulären Modul über sich selbst und durch Einschränkung als $\mathbb{R}$-Modul. Bestimmen Sie jeweils alle Untermoduln, alle Quotientenmoduln, alle Endomorphismen von $\mathbb{C}$ und einen Ringhomomorphismus zwischen den beiden Endomorphismenringen $\mathrm{End}_{\mathbb{R}}(\mathbb{C})$ und $\mathrm{End}_{\mathbb{C}}(\mathbb{C})$.

2.4 Äquivalenz von Moduln und Darstellungen

Wir werden als nächstes sehen, in welchem Sinne der Begriff der Darstellung äquivalent zum Begriff des Moduls ist. Mit den folgenden beiden Prozessen können wir Aussagen von Moduln in Aussagen über Darstellungen, und umgekehrt, Aussagen über Darstellungen in Aussagen über Moduln übersetzen.

Bemerkung 2.28. Sei A eine K-Algebra. Wir stellen den wichtigen und gleichzeitig einfachen Zusammenhang her zwischen Moduln und Darstellungen:

a) Sei $\rho : A \to \mathrm{End}_K(V)$ eine Darstellung von A auf einem Vektorraum V. Definiere die Operation

$$A \times V \to V \text{ durch } (a, v) \mapsto a \cdot v := \rho(a)(v), \text{ fur alle } a \in A \text{ und alle } v \in V$$

Es ist $\rho(a)$ ein Element in $\mathrm{End}_K(V)$, also eine lineare Abbildung. Entsprechend ist $\rho(a)(v)$ ein Element in V.
Dann ist V ein A-Linksmodul, der *zur Darstellung ρ korrespondierende Modul.*

b) Umgekehrt, sei V ein A-Linksmodul. Insbesondere ist also V ein K-Vektorraum, siehe Bemerkung 2.16. Wir definieren die Abbildung

$$\rho : A \to \mathrm{End}_K(V), \quad \rho(a)(v) := a \cdot v, \text{ für alle } a \in A \text{ und alle } v \in V.$$

Dann ist ρ ein Algebrenhomomorphismus, also eine Darstellung von A auf V, die *zum Modul V gehörige Darstellung von A auf V.*

Die beiden hier beschriebenen Prozesse sind invers zueinander.

Beweis. Sei ρ eine gegebene Darstellung von A auf V. Wir müssen prüfen, dass die Operation

$$A \times V \to V, \quad (a, v) \mapsto a \cdot v := \rho(a)(v), \text{ für } v \in V \text{ und } a \in A$$

die Modulgesetze in Definition 2.13 erfüllt. Beispielsweise gilt für das Einselement nach Definition der Operation:

$$1_A \cdot v = \rho(1_A)(v) = \mathrm{id}_V(v) = v.$$

Am zweiten Gleichheitszeichen haben wir benutzt, dass ρ als Homomorphismus das Einselement von A auf das Einselement von $\mathrm{End}_K(V)$ abbildet. Damit gilt also Modulaxiom (M4). Wir prüfen auch das Axiom (M3) nach. Die Definition der Operation liefert für $a, b \in A$ und $v \in V$:

$$(a \cdot b) \cdot v \overset{\text{Def}}{=} \rho(ab)(v) = (\rho(a) \circ \rho(b))(v) \overset{\text{Def}}{=} \rho(a)(b \cdot v) \overset{\text{Def}}{=} a \cdot (b \cdot v).$$

Die Multiplikation in $\mathrm{End}_K(V)$ ist Komposition von Abbildungen. Am zweiten Gleichheitszeichen haben wir benutzt, dass ρ ein Homomorphismus ist. Das Nachrechnen der Axiome (M1) und (M2) ist dem werten Leser überlassen. Der Beweis von Bemerkung 2.28 wird vervollständigt durch die folgende Übungsaufgabe:

Aufgabe 2.11. Vervollständigen Sie den Beweis zu Bemerkung 2.28:

a) Zeigen Sie, dass $\rho(a)$ eine lineare Abbildung ist, also die Operation von A auf V wohldefiniert ist.

b) Zeigen Sie, dass ρ ein Algebrenhomomorphismus ist.

c) Machen Sie sich klar, dass die beiden Prozesse invers zueinander sind.

Bemerkung 2.28 erlaubt uns das Übersetzen zwischen Darstellungen und Moduln. Es wird uns im Rest der Vorlesung begleiten. Zwei Beispiele haben wir bereits gesehen: Die reguläre Darstellung 2.5 entspricht dem regulären Modul 2.15 c); die Permutationsdarstellung 2.10 entspricht dem Permutationsmodul 2.17. Als Beispiel wollen wir das in Definition 2.3 definierte Konzept der äquivalenten Darstellung auf Moduln übertragen:

Proposition 2.29. *Zwei A-Moduln M_1 und M_2 sind isomorph, genau dann, wenn die zugehörigen Darstellungen ρ_1 und ρ_2 äquivalent sind.*

Beweis. Sei $\rho_i : A \to \mathrm{End}_K(M_i)$ die zum Modul M_i korrespondierende Darstellung, mit $i = 1, 2$. Angenommen ρ_1 und ρ_2 sind äquivalent. Wir wollen zeigen, dass dann die Moduln M_1 und M_2 isomorph sind. Nach Definition 2.3 existiert ein Vektorraumisomorphismus $\psi : M_1 \to M_2$ mit $\psi \circ \rho_1(a) \circ \psi^{-1} = \rho_2(a)$, für alle $a \in A$. Damit ist ψ linear, bijektiv und es gilt

$$\begin{aligned}\psi(a \cdot v) &\overset{2.28}{=} \psi(\rho_1(a)(v) = (\psi \circ \rho_1(a))(v)\\ &= (\rho_2(a) \circ \psi)(v) = \rho_2(a)(\psi(v)) \overset{2.28}{=} a \cdot \psi(v),\end{aligned}$$

für alle $a \in A$. Damit ist ψ ein A-Modulisomorphismus.

Um die Rückrichtung zu beweisen, sei $\psi : M_1 \to M_2$ ein A-Modulisomorphismus. Seien $\rho_i : A \to \mathrm{End}_K(M_i)$ die zu M_i korrespondierenden Darstellungen, mit $i = 1, 2$. Da ψ Modulhomomorphismus ist, folgt

$$(\psi \circ \rho_1(a))(v) = \psi(\rho_1(a)(v)) \overset{2.28}{=} \psi(a \cdot v) = a\psi(v) \overset{2.28}{=} \rho_2(a)(\psi(v)) = (\rho_2(a) \circ \psi)(v),$$

beziehungsweise wegen ψ bijektiv gilt $\psi \circ \rho_1(a) \circ \psi^{-1} = \rho_2(a)$ für alle $a \in A$. Damit sind ρ_1 und ρ_2 äquivalent. □

Aufgabe 2.12. Sei A eine K-Algebra. Übertragen Sie mittels Bemerkung 2.28 die beiden Konzepte A-Untermodul (siehe 2.18) und A-Modulhomomorphismus (siehe 2.23) auf Darstellungen, um eine passende Definition des Begriffs Unterdarstellung beziehungsweise Homomorphismus von Darstellungen zu erhalten.

Aufgabe 2.13. Sei A eine K-Algebra und sei V ein A-Modul mit korrespondierender Darstellung $\rho : A \to \mathrm{End}_K(V)$. Sei U ein Untermodul von V. Zeigen Sie:

a) Es gibt eine Basis von V, sodass für alle $a \in A$ die Matrix $\rho(a)$ die Blockgestalt hat:

$$\rho(a) = \begin{pmatrix} \rho_1(a) & \rho_2(a) \\ 0 & \rho_3(a) \end{pmatrix},$$

wobei ρ_1 beziehungsweise ρ_3 die Operation von A auf U beziehungsweise auf V/U beschreiben.

b) Existiert eine Basis von V, sodass $\rho_2(a)$ die Nullmatrix ist, dann existiert ein Untermodul $W \leq V$ mit $V = U \oplus W$.

Zeitlich gesehen wurden Darstellungen vor Moduln definiert und studiert. In der Theorie erweist sich die Sprache der Modultheorie als erheblich effizienter und eleganter – um mit dem Computer zu rechnen, hat die Sprache der Darstellungen ihre Vorteile. Es ist einer der grossen Verdienste von Emmy Noether einen durch die abstraktere Modultheorie erheblich einfacheren Zugang zu Darstellungstheorie gefunden zu haben. Kein Mathematiker sollte die Universiät verlassen, ohne einmal über das Leben von Emmy Noether gelesen zu haben. Das Internet bietet diverse Resourcen, mit unterschiedlicher Genauigkeit und Gewichtung, beispielsweise:

`https://www.fembio.org/biographie.php/frau/biographie/emmy-noether/`
`https://www.britannica.com/print/article/417132`
`https://mathshistory.st-andrews.ac.uk/Biographies/Noether_Emmy/`

Eine kurze Entwicklung des Begriffs des *Moduls* findet man in der Enzyklopedia of Mathematics, `https://encyclopediaofmath.org/wiki/Module`, wo aufgezeigt wird, wie spezielle Beispiele immer allgemeiner formuliert werden.

Aufgabe 2.14. Sei K ein Körper der Charakteristik p prim. Sei G eine endliche Gruppe und Ω eine G-Menge. Es operiere zusätzlich G transitiv auf Ω, das heisst, zu beliebigen Elementen $x, y \in \Omega$ existiert ein $g \in G$ mit $g \cdot x = y$. Wir definieren die folgenden beiden Teilmengen des Permutationsmoduls $M := K\Omega$:

$$M_1 \;:=\; \{\lambda \cdot (\sum_{\omega \in \Omega} b_\omega) \mid \lambda \in K\}, \quad M_2 := \left\{ \sum_{\omega\in\Omega} \lambda_\omega b_\omega \mid \sum_{\omega\in\Omega} \lambda_\omega = 0 \right\}.$$

a) Zeigen Sie, dass M_1 und M_2 Untermoduln von M sind. Bestimmen Sie die Dimensionen von M_1 und M_2. Bestimmen Sie die Matrixdarstellung korrespondierend zu M_1 beziehungsweise zu M/M_2.

b) Zeigen Sie, dass die Abbildung $\phi : M \to M_1$, definiert durch

$$\phi(\sum_{\omega\in\Omega} \lambda_\omega b_\omega) = (\sum_{\omega\in\Omega} \lambda_\omega)(\sum_{\omega\in\Omega} b_\omega)$$

ein KG-Modulhomomorphismus ist. Sei $\psi : M \to M_1$ ein surjektiver Modulhomomorphismus. Wie sieht die Abbildung ψ aus? Bestimmen Sie $\ker \psi$.

Aufgabe 2.14 (b) liefert einen möglichen Hinweis zum Lösen der etwas schwierigeren folgenden Aufgabe:

Aufgabe 2.15. Wir setzen Aufgabe 2.14 fort:

a) Zeigen Sie, dass M_1 ein direkter Summand von M ist, genau dann, wenn $\mathrm{ggT}(p, |\Omega|) = 1$ ist.

b) Sei nun p ein Teiler der Ordnung der Gruppe G. und sei $\Omega = G$. Zeigen Sie, dass Modul M_1 ein Untermodul des regulären Moduls KG ist. Zeigen Sie auch, dass M_1 kein Komplement in KG hat, das heisst, dass es keinen Untermodul $T \leq KG$ gibt mit $KG = M_1 \oplus T$.

2.5 Köcherdarstellungen

Wie üblich sei K ein Körper und B eine Algebra über dem Körper K. In diesem Kapitel treten auf natürliche Art und Weise Rechtsmoduln auf. In Aufgabe 2.7 haben wir gesehen, ist die Algebra B nicht kommutativ, so lässt sich die Struktur eines B-Rechtsmoduls in der Regel nicht naiv nutzen, um die Struktur eines B-Linksmoduls zu erhalten, oder umgekehrt. Allerdings können wir zwischen Links- und Rechtsmoduln wechseln, wenn wir mit der entgegengesetzten Algebra B^{op}, siehe Beispiel 1.7, arbeiten:

Bemerkung 2.30. Ist B eine Algebra, und M ein B-Rechtsmodul, so wird durch

$$B \times M \to M, (a, m) \mapsto a \cdot m := m \cdot a, \quad \text{mit } a \in B \text{ und } m \in M,$$

eine B^{op}-Linksmodulstruktur auf dem Vektorraum M definiert, denn es gilt für das wichtige Modulaxiom (M3):

$$a \cdot (b \cdot m) \overset{\text{Def}}{=} a \cdot (m \cdot b) \overset{\text{Def}}{=} (m \cdot b) \cdot a \overset{\text{(M3)}}{=} m \cdot (b \cdot a) = m \cdot (a * b) \overset{\text{Def}}{=} (a * b) \cdot m,$$

für alle $m \in M$ und alle $a, b \in B$. Die meisten Multiplikationszeichen in dieser letzten Gleichung entsprechen der Operation eines Algebraelementes auf einem Vektor, ausser im vierten Audruck, dort bedeutet der zweite Punkt Multiplikation in der Algebra B. Im fünften und sechsten Ausdruck steht $*$ für die Multiplikation in der entgegengesetzten Algebra B^{op}.

Wendet man die Konstruktion ein weiteres mal an, so wird aus dem B^{op}-Linksmodul M ein $(B^{\mathrm{op}})^{\mathrm{op}}$-Rechtsmodul M. Für die entgegengesetzte Algebra ist $(B^{\mathrm{op}})^{\mathrm{op}} \simeq B$, als Algebra, also erhält man den ursprünglichen B-Rechtsmodul M beim zweimaligen Anwenden der Konstruktion wieder zurück. Die Konstruktion ist also selbstinvers, und erlaubt es uns, zwischen Links- und Rechtsmoduln beliebig zu wechseln, wenn wir die Algebra entsprechend ändern.

Sei $Q = (Q_0, Q_1)$ ein Köcher, wie üblich mit endlicher Punktemenge Q_0. Wir schreiben $A = KQ$ für die Wegealgebra. Wir wollen verstehen, wie Moduln oder Darstellungen einer Wegealgebra aussehen. Die Operation von A auf V ist vollständig beschrieben, wenn wir verstehen, wie die Erzeuger der Algebra A auf dem Vektorraum V operieren. Wie bei Gruppendarstellungen oder Moduln der Gruppenalgebra ist diese Operation natürlich nur wohldefiniert, wenn hierbei die Relationen auf den Erzeugern respektiert werden. Daher bemerken wir zunächst für die Wegealgebra:

Bemerkung 2.31. Die Wegealgebra KQ eines Köchers Q wird als Algebra erzeugt von den faulen Wegen e_i mit $i \in Q_0$, sowie den Wegen der Länge Eins, also den Pfeilen. Sei $\alpha \in Q_1$ ein Pfeil, mit $\alpha : i \to j$. Auf den Algebra-Erzeugern der entgegengesetzten Wegealgebra haben wir die folgenden Relationen:

$$\begin{aligned} e_l \cdot e_t &= \begin{cases} e_l & \text{falls l=t,} \\ 0 & \text{sonst,} \end{cases} \\ e_l \cdot \alpha &= \begin{cases} \alpha & \text{falls } l = i, \\ 0 & \text{sonst,} \end{cases} \\ \alpha \cdot e_l &= \begin{cases} \alpha & \text{falls } l = j, \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

Wir wollen nun die Operation der Erzeuger der Wegealgebra KQ auf dem Vektorraum V des KQ-Moduls V analysieren. Dies motiviert dann unsere Definition einer Köcherdarstellung.

Bemerkung 2.32. Sei V ein (wie üblich endlich-dimensionaler) A-Rechtsmodul mit $A = KQ$. Im ersten Teil analysieren wir wie die faulen Wege auf dem Vektorraum V operieren, im zweiten Teil betrachten wir dann die Operation der Pfeile auf V. Nach Bemerkung 2.28 b) ist die Abbildung $V \to V, v \mapsto v \cdot a$ mit $a \in A$ eine K-lineare Abbildung.

a) Die faulen Wege e_i operieren von rechts auf dem Vektorraum V. Dies ist nach Bemerkung 2.28 eine lineare Abbildung. Definiere

$$V(i) := Ve_i = \{ve_i \mid v \in V\}, \text{ für } i \in Q_0.$$

Dann ist $V(i)$ als Bild einer linearen Abbildung ein Unterraum von V. Da e_i ein Idempotent ist (siehe 1.26), gilt für alle $w \in V(i)$, dass $we_i = w$ ist. Wir wollen zeigen, dass V eine direkte Summe der Unterräume $V(i)$ ist. Sei $v \in V$ beliebig. Dann gilt:

$$v = v \cdot 1 \overset{1.27}{=} v \cdot (\sum_{i \in Q_0} e_i) = \sum_{i \in Q_0} ve_i.$$

Damit ist also $V = \sum_{i \in Q_0} Ve_i = \sum_{i \in Q_0} V(i)$, das heisst V ist die Summe der Unterräume $V(i)$. Wir zeigen, dass diese Summe eine direkte Summe ist: Sei

$$v \in V(i) \cap \bigoplus_{j \neq i} V(j).$$

Wir müssen zeigen, dass $v = 0$ ist. Wie oben bemerkt, gilt für $v \in V(i)$, dass $v = ve_i$ ist. Ausserdem existieren Elemente $u_j \in V$ mit $v = \sum_{j \neq i} u_j e_j$. Jetzt nutzen wir, dass die Idempotente e_i paarweise orthogonal sind, siehe 1.26, und erhalten:

$$v = ve_i = (\sum_{j \neq i} u_j e_j)e_i = \sum_{j \neq i} u_j(e_j e_i) = \sum_{j \neq i} u_j \cdot 0 \overset{2.14}{=} 0.$$

Es folgt, dass $V = \bigoplus_{i \in Q_0} Ve_i = \bigoplus_{i \in Q_0} V(i)$ eine direkte Summe der Vektorräume $V(i)$ ist. Jedem Punkt des Köchers Q lässt sich also ein Vektorraum $V(i)$ zuordnen, sodass $V = \bigoplus V(i)$ gilt.

b) Als nächstes analysieren wir, wie die Wege der Länge Eins auf dem Vektorraum V operieren. Wir wollen jedem Pfeil des Köchers Q eine lineare Abbildung zuordnen. Sei $\alpha \in Q_1$ ein Pfeil mit Startpunkt $s(\alpha) = i$ und Endpunkt $t(\alpha) = j$. Wir definieren die Abbildung $V(\alpha) : V \to V$ durch $v \mapsto v\alpha$, also durch Operation von rechts mit α auf dem Vektorraum V. Nach Bemerkung 2.28 b) ist dies eine lineare Abbildung. Weiterhin ist $\alpha = e_i \alpha e_j$. Damit gilt für ein beliebiges Element $ve_l \in V(l)$:

$$(ve_l)\alpha = (ve_l)e_i\alpha e_j = v(e_l e_i)\alpha e_j = \begin{cases} (v\alpha)e_j & \text{falls } l = i, \\ 0 & \text{falls } l \neq i. \end{cases}$$

Das Element $v\alpha = (v\alpha)e_j$ liegt nach der letzten Rechnung also im Vektorraum $V(j)$. Und die Rechnung zeigt auch, dass jedes Element aus $V(l) \subseteq V$ mit $l \neq i$ durch die Abbildung $V(\alpha)$ auf das Nullelement geschickt wird. Damit ist die Einschränkung von $V(\alpha)$ auf den direkten Summanden $V(i)$ von V eine lineare Abbildung mit Bild in $V(j)$, und durch dieses Einschränken geht keinerlei Information der Operation von α auf V verloren. Jedem Pfeil α im Köcher Q haben wir damit eine eindeutige lineare Abbildung zugeordnet:

$$V(\alpha) : V(i) \to V(j), \text{ mit } v \mapsto v\alpha.$$

Definition 2.33. Sei K Körper und $Q = (Q_0, Q_1, s, t)$ ein Köcher. Eine *Darstellung*

$$V = (V(i), V(\alpha))_{i \in Q_0, \alpha \in Q_1}$$

des Köchers Q über dem Körper K ist eine Menge von Vektorräumen $V(i)$, einen für jedes $i \in Q_0$, zusammen mit einer Menge von linearen Abbildungen

$$V(\alpha) : V(s(\alpha)) \to V(t(\alpha)),$$

eine für jedes $\alpha \in Q_1$. Die Darstellung V heisst *endlich-dimensional*, falls jeder Vektorraum $V(i)$ endlich-dimensional ist. Der *Dimensionsvektor* von V ist definiert als $\underline{\dim} V := (\dim V(i))_{i \in Q_0}$. Ein *Element* von V ist definiert als ein Tupel $(v_i)_{i \in Q_0}$ mit $v_i \in V(i)$ für $1 \leq i \leq n$.

Bevor wir weiter klären, was dieser neue Begriff der Köcherdarstellung mit unseren bisherigen Darstellungen und Moduln zu tun hat, wollen wir uns Beispiele anschauen. Die Köcherdarstellungen werden in der Regel mit Hilfe der Köcher als Bilder angegeben, indem wir die Vektorräume $V(i)$ an die Punkte und die Abbildungen $V(\alpha)$ an die Pfeile des Köchers schreiben:

Beispiel 2.34. Wir betrachten den Köcher $Q_b : \; 1 \xrightarrow{\alpha} 2$ aus Beispiel 1.22, und geben für diesen Köcher vier verschiedene Köcherdarstellungen an:

$$\begin{aligned} V &: K \xrightarrow{\text{id}} K, \quad \underline{\dim} V = (1,1), \\ V' &: K \xrightarrow{0} K, \quad \underline{\dim} V = (1,1), \\ V'' &: K \longrightarrow 0, \quad \underline{\dim} V = (1,0), \end{aligned}$$

und

$$V''' : K^2 \xrightarrow{\begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix}} K^3, \quad \underline{\dim} V = (2,3)$$

sind Darstellungen des Köchers Q_b, mit jeweils angegebenem Dimensionsvektor. Im ersten Beispiel ist die lineare Abbildung die Identität auf K, im zweiten Beispiel ist es die Nullabbildung. Im dritten Beispiel ist nicht angegeben, was die Abbildung ist; dem Zusammenhang ist aber zu entnehmen, dass es sich um die Nullabbildung handeln muss. Die Matrix

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

im vierten Beispiel besagt, dass die Abbildung $K^2 \to K^3$ gegeben ist durch $x \mapsto Bx$, also durch Multiplikation mit der Matrix B.

Proposition 2.35. *Sei $A = KQ$ die Wegealgebra eines Köchers Q. Köcherdarstellungen eines Köchers Q korrespondieren zu A-Rechtsmoduln; im Sinne von Bemerkung 2.30 entsprechen also Köcherdarstellungen von Q gerade A^{op}-Linksmoduln, beziehungsweise nach Bemerkung 2.28 gerade Darstellungen der entgegengesetzten Algebra A^{op}.*

Beweis. Sei $V = (V(i), V(\alpha))_{i\in Q_0, \alpha\in Q_1}$ eine Köcherdarstellung des Köchers Q. Wir konstruieren aus der Köcherdarstellung V einen A-Rechtsmodul $\hat{V}$ mit

$$\hat{V} := \bigoplus_{i\in Q_0} V(i).$$

Da $\hat{V}$ eine direkte Summe ist, schreibe $v \in \hat{V}$ als $v = \sum_{j\in Q_0} v_j$ mit $v_j \in V(j)$. Diese Darstellung des Vektors v ist eindeutig. Wir definieren die Operation der Erzeuger von A auf $v \in \hat{V}$ wie folgt:

i) Die faulen Wege e_i operieren durch $v \cdot e_i := v_i$, mit $i \in Q_0$. Das sagt nichts anderes als dass Multiplikation mit e_i die Identitatsabbildung auf $V(i)$ ist, und die Nullabbildung auf $V(j)$ mit $j \neq i$; dies ist nichts anderes als die Projektion $\pi_{V(i)} : \hat{V} \to \hat{V}$ auf $V(i)$ entlang $\bigoplus_{j\neq i} V(j)$.

ii) Sei $\alpha \in Q_1$ ein Pfeil, mit $s(\alpha) = i$ und $t(\alpha) = j$. Dann operiert α durch $v \cdot \alpha := V(\alpha)(v_i)$. Das sagt, dass Multiplikation mit α, was nach Bemerkung 2.28 eine lineare Abbildung ist, gerade der Abbildung $V(\alpha) : V(i) \to V(j)$ entspricht, und der Nullabbildung auf allen $V(l)$ mit $l \neq i$.

Nachdem wir die Operation auf den Erzeugern der Algebra $A = KQ$ definiert haben, setzen wir die Operation so fort, dass das Modulaxiom (M3) gilt. Wir veranschaulichen das zunächst für zwei Pfeile $i \xrightarrow{\alpha} j \xrightarrow{\beta} h$ und definieren für $v \in \hat{V}$ mit Zerlegung wie oben:

$$v \cdot (\alpha\beta) := (v \cdot \alpha) \cdot \beta \overset{(ii)}{=} (V(\alpha)(v_i)) \cdot \beta \overset{(ii)}{=} V(\beta)(V(\alpha)(v_i)) = (V(\beta) \circ V(\alpha))(v_i).$$

Allgemeiner definieren wir für ein Produkt von Pfeilen $\alpha_i \in V$ die Operation

$$v \cdot (\alpha_1 \cdots \alpha_n) := (V(\alpha_n) \circ \ldots \circ V(\alpha_1))(v_{s(\alpha_1)}),$$

und setzen diese Operation dann linear zu einer Operation von $A = KQ$ auf $\hat{V}$ fort. Wir müssen nun prüfen, dass diese Operation wohldefiniert ist, also die Relationen der Erzeuger der Algebra A respektiert, siehe Bemerkung 2.31. Wir prüfen beispielsweise die Relation $e_i \cdot \alpha = \alpha$ für Pfeil α mit $s(\alpha) = i$ und $t(\alpha) = j$. Es gilt:

$$v \cdot (e_i\alpha) \overset{\text{Def}}{=} (v \cdot e_i) \cdot \alpha \overset{(i)}{=} v_i \cdot \alpha \overset{(ii)}{=} V(\alpha)(v_i) \overset{(ii)}{=} v \cdot \alpha.$$

Zu prüfen, dass die anderen Relationen gelten und zu prüfen, dass die Konstruktion in diesem Beweis invers zu der Konstruktion in Bemerkung 2.32 ist, überlassen wir dem Leser. Statt $\hat{V}$ schreiben wir typischerweise einfach nur V für den zur Köcherdarstellung V korrespondierenden A-Rechtsmodul. $\square$

Bemerkung 2.36. a) Warum erhalten wir keinen A-Linksmodul im Beweis von Proposition 2.35? Nachdem die Operation von A auf den Erzeugern definiert wurde, diesmal als Linksoperation, müssten wir die Operation des Produktes zweier Pfeile $\alpha\beta$ so definieren, dass gilt:

$$(\alpha\beta)v := \alpha(\beta v) = V(\alpha)(\beta v) = V(\alpha)(V(\beta)(v)).$$

Aber die Komposition der linearen Abbildungen $V(\alpha) \circ V(\beta)$ ist gar nicht definiert, denn es ist $V(\alpha) : V(i) \to V(j)$ und $V(\beta) : V(j) \to V(h)$. Wir müssen also im Beweis von Proposition 2.35 A-Rechtsmoduln definieren, oder aber entsprechend Bemerkung 2.30 Linksmoduln für die entgegengesetzte Algebra A^{op}.

b) Wie sieht die Linksmodulstruktur für die entgegengesetzte Algebra A^{op} aus? Nach Lemma 1.31 ist $A^{\mathrm{op}} = K(Q^{\mathrm{op}})$, wobei der entgegengesetzte Köcher Q^{op} aus Q durch das Herumdrehen von Pfeilen entsteht. Ist $\alpha \in Q_1$ ein Pfeil, mit $\alpha : i \to j$, so schreiben wir α^{op} für den Pfeil im Köcher Q^{op} mit entgegengesetzter Pfeilrichtung, also $\alpha^{\mathrm{op}} : j \to i$. Mit dieser Notation können wir auf $\hat{V}$ eine Linksmodulstruktur definieren. Nach Bemerkung 2.30 definieren wir $e_i \cdot v := v_i$ und $\alpha^{\mathrm{op}} \cdot v := V(\alpha)(v_i)$. Mit den Pfeilen α und β wie oben definieren wir weiter

$$(\beta^{\mathrm{op}} \cdot \alpha^{\mathrm{op}}) \cdot v := V(\beta)(V(\alpha)(v_i)).$$

Dann gilt Modulaxiom (M3):

$$\beta^{\mathrm{op}} \cdot (\alpha^{\mathrm{op}} \cdot v) = V(\beta)(\alpha^{\mathrm{op}} \cdot v) = V(\beta)(V(\alpha)(v_i)) = (\beta^{\mathrm{op}} \cdot \alpha^{\mathrm{op}}) \cdot v,$$

das heisst, wir erhalten mit diesen Definitionen einen A^{op}-Linksmodul.

Entsprechend wie im vorigen Abschnitt 2.4 lassen sich nun die weiteren Konzepte wie Untermoduln, Quotientenmoduln und Homomorphismen von Moduln mittels Proposition 2.35 auf Köcherdarstellungen übertragen.

Aufgabe 2.16. Sei Q ein Köcher.

a) Sei V ein KQ-Rechtsmodul mit korrespondierender Köcherdarstellung $V = (V(i), V(\alpha))$. Übersetzen Sie mittels Proposition 2.35 die Definition eines *Untermoduls* $U \leq V$ in die Sprache der Köcherdarstellungen, das heisst, definieren Sie den Begriff *Unterdarstellung* von $V = (V(i), V(\alpha))$. Wie sehen *direkte Summen* von Köcherdarstellungen aus?

b) Sei Köcher Q_b: $1 \xrightarrow{\alpha} 2$. Bestimmen Sie alle Untermoduln der folgenden drei Köcherdarstellungen:

$$V_1 : K \to 0, \quad V_2 : 0 \to K, \quad V_3 : K \xrightarrow{\mathrm{id}} K.$$

Lässt sich Darstellung V_3 als direkte Summe von Unterdarstellungen schreiben?

Begründen Sie jeweils Ihre Antworten.

Aufgabe 2.17. Sei Q ein Köcher. Wir setzen Aufgabe 2.16 fort. Definieren Sie korrespondierend zum Quotientenmodul, was mittels Proposition 2.35 unter einer *Quotientendarstellung* einer Köcherdarstellung zu verstehen ist. Finden Sie alle Quotientendarstellungen von V_3.

Wir übersetzen mittels Proposition 2.35 Modulhomomorphismen und definieren:

Definition 2.37. Seien $V = (V(i), V(\alpha))$ und $W = (W(i), W(\alpha))$ zwei Darstellungen eines Köchers Q über einem Körper K. Ein *Homomorphismus (von Köcherdarstellungen)* $f : V \to W$ besteht aus linearen Abbildungen $f(i) : V(i) \to W(i)$ für alle $i \in Q_0$, so dass das folgende Diagram kommutiert:

$$\begin{tikzcd} V(s(\alpha)) \arrow[r, "V(\alpha)"] \arrow[d, "f(s(\alpha))"'] & V(t(\alpha)) \arrow[d, "f(t(\alpha))"] \\ W(s(\alpha)) \arrow[r, "W(\alpha)"'] & W(t(\alpha)) \end{tikzcd}$$

Wir sagen f ist ein *Isomorphismus*, falls $f(i)$ ein Isomorphismus von K-Vektorräumen ist, für alle $i \in Q_0$. Zwei Darstellungen heissen *isomorph*, falls es einen Isomorphismus zwischen ihnen gibt. Isomorphie von Moduln oder Darstellungen ist eine Äquivalenzrelation, und die Äquivalenzklassen unter dieser Relation werden als *Isomorphieklassen* bezeichnet.

Beispiel 2.38. Sei Q der Köcher mit einem Punkt 1 und einem Pfeil α. Die Algebra KQ ist kommutativ, das heisst, die Algebra A und die entgegengesetzte Algebra stimmen nach Lemma 1.31 überein; also entsprechen A-Rechtsmoduln gerade A-Linksmoduln. Sei $V = (V(1), V(\alpha))$ eine Köcherdarstellung von V über einem Körper K. In diesem Fall ist also $V = V(1)$ und die Operation des Erzeugers α ist beschrieben durch $\alpha \cdot v := V(\alpha)(v)$, wobei $V(\alpha)$ einer beliebigen linearen Abbildung auf V entspricht. Nach Beispiel 1.29 entspricht KQ der Algebra $K[X]$. Dieses Beispiel beschreibt also, wie $K[X]$-Moduln aussehen: Ein $K[X]$-Modul ist ein Vektorraum V, zusammen mit einer linearen Abbildung, die angibt, wie X auf dem Vektorraum V operiert.

Sei K algebraisch abgeschlossen. Isomorphe Moduln verhalten sich im Sinne der Darstellungstheorie gleich. Wir suchen einen schönen Vertreter der Isomorphieklasse von V, beziehungsweise eine Klassifikation aller KQ-Moduln bis auf Isomorphie. Dies ist im Allgemeinen ein schwieriges Problem, das wir aber für diesen Köcher Q bereits in der Linearen Algebra gelöst haben: Sei $W = (W(1), W(\alpha))$ eine zu V isomorphe Darstellung des Köchers Q. Dann existiert nach Definition 2.37 ein Isomorphismus $T : V(1) \to W(1)$, sodass das folgende Diagram kommutiert:

$$\begin{tikzcd} V(1) \arrow[r, "V(\alpha)"] \arrow[d, "T"'] & V(1) \arrow[d, "T"] \\ W(1) \arrow[r, "W(\alpha)"'] & W(1) \end{tikzcd}$$

Somit gilt $W(\alpha) = TV(\alpha)T^{-1}$. Damit ist nach Linearer Algebra II die Darstellung $(V(1), J_{V(\alpha)})$ mit $J_{V(\alpha)}$ Jordan-Normalform von $V(\alpha)$ ein schöner Vertreter der Isomorphieklasse von $V = (V(1), V(\alpha))$. Die Jordan-Normalform liefert also eine Klassifikation aller Darstellungen von KQ oder KQ-Moduln bis auf Isomorphie. Beispielsweise sind also die folgenden beiden Darstellungen von KQ nicht-isomorph:

$$K^2 \xrightarrow{\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}} K^2, \quad K^2 \xrightarrow{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}} K^2.$$

Aufgabe 2.18. Am Ende von Beispiel 2.38 sind zwei Darstellungen der Dimension $(2, 2)$ angegeben. Rechnen Sie direkt nach, also mit Definition 2.37 und ohne das Argument zur Jordanschen Normalform zu nutzen, dass die beiden Darstellungen nicht-isomorph sind. Wieviele paarweise nicht-isomorphe Darstellungen der Form $K^2 \to K^2$ gibt es?

Aufgabe 2.19. Seien n, m natürliche Zahlen. Sei Köcher Q_b : $1 \xrightarrow{\alpha} 2$. Wieviele KQ_b-Darstellungen der Form $K^n \to K^m$ gibt es, bis auf Isomorphie? Geben Sie für jede Isomorphieklasse einen schönen Vertreter an.

Nachdem wir mit dem Arbeiten mit Homomorphismen von Köcherdarstellungen vertraut sind, wollen wir verstehen, dass Definition 2.37 von Homomorphismen zwischen Köcherdarstellungen mittels der Korrespondenz in Proposition 2.35 gerade Modulhomomorphismen entspricht. Definition 2.23 arbeitet mit Linksmoduln. Wir arbeiten hier mit Rechtsmoduln; Bedingung (ii) in Definition 2.23 umgeschrieben auf Rechtsmoduln ist $\phi(m \cdot r) = \phi(m) \cdot r$, für alle $m \in M$ und $r \in R$.

Bemerkung 2.39. Homomorphismen von Köcherdarstellungen von Q entsprechen genau den Homomorphismen von KQ-Rechtsmoduln.

Beweis. Seien $\hat{V} = \bigoplus_{i \in Q_0} V(i)$ und $\hat{W} = \bigoplus_{i \in Q_0} W(i)$ die zu den Köcherdarstellungen $V = (V(i), V(\alpha))$ beziehungsweise $W = (W(i), W(\alpha))$ korrespondierenden KQ-Rechtsmoduln. Sei $f : \hat{V} \to \hat{W}$ ein Modulhomomorphismus. Wir nutzen die direkte Summenstruktur von $\hat{V}$ aus: Schränken wir die Abbildung f auf den direkten Summanden $V(i)$ ein, so ist wegen e_i Idempotent und f Modulhomomorphismus: $f(ve_i) = f(ve_i^2) = f(ve_i)e_i \in W(i)$. Durch Einschränken von f erhalten wir also Abbildungen

$$f(i) := f_{|V(i)} : V(i) \to W(i), \text{ für } i \in Q_0.$$

Da f nach Voraussetzung K-linear ist, sind diese Abbildungen $f(i)$ ebenfalls K-linear. Umgekehrt lässt sich ein Tupel von linearen Abbildungen $(f(i))_{i \in Q_0}$ zu einer linearen Abbildung f zusammensetzen: Ist $v = \sum_{i \in Q_0} v_i$ mit eindeutigen $v_i \in V(i)$, so definieren wir

$$f(v) = \sum_{i \in Q_0} f(i)(v_i).$$

Wir zeigen, dass die zusammengesetzte Abbildung f genau dann ein Homomorphismus von Rechtsmoduln ist, wenn die Tupel von linearen Abbildungen $(f(i))_{i \in Q_0}$

einen Homomorphismus von Köcherdarstellungen bilden. Wir schreiben kurz auch $f = (f(i))_{i \in Q_0}$ oder $f = \operatorname{diag}(f(i)_{i \in Q_0})$ für die Diagonalmatrix mit Einträgen $f(i)$. Bis hierher haben wir lediglich die Homomorphismeneigenschaft (ii) in Definition 2.23 für die faulen Wege e_i benutzt. Die Algebra KQ hat weitere Erzeuger, die Pfeile. Sei $\alpha \in Q_1$ ein Pfeil mit Startpunkt $s(\alpha) = i$ und Endpunkt $t(\alpha) = j$. Mit Proposition 2.35 gilt:

$$f(i)((ve_i) \cdot \alpha) \overset{2.23(ii)}{=} f(i)(ve_i) \cdot \alpha \overset{2.35}{\Leftrightarrow} f(i)(V(\alpha)(ve_i)) = W(\alpha)(f(i)(ve_i)).$$

Die Äquivalenz der letzten beiden Gleichungen besagt nichts anderes, als dass die Kommutativität der folgenden beiden Diagramme äquivalent ist:

$$\begin{tikzcd} V(i) \arrow[r, "- \cdot \alpha"] \arrow[d, "f(i)"'] & V(j) \arrow[d, "f(j)"] \\ W(i) \arrow[r, "- \cdot \alpha"'] & W(j) \end{tikzcd} \quad \Leftrightarrow \quad \begin{tikzcd} V(i) \arrow[r, "V(\alpha)"] \arrow[d, "f(i)"'] & V(j) \arrow[d, "f(j)"] \\ W(i) \arrow[r, "W(\alpha)"'] & W(j) \end{tikzcd}$$

Modulhomomorphismen (linkes Diagram) entsprechen damit gerade Homomorphismen von Köcherdarstellungen (rechtes Diagram). $\square$

Wie im Beweis von Proposition 2.35 haben wir hier wiederum mit den Erzeugern der Algebra $A = KQ$ gearbeitet. Streng genommen müssen wir überprüfen, ob bei dieser Übersetzung auch die Relationen auf den Erzeugern respektiert werden. Diese folgt aber, weil die Kommutativität des zusammengesetzten Diagrams aus der Kommutativität der einzelnen Quadrate folgt, sowohl bei Homomorphismen von Köcherdarstellungen (siehe Diagram unten) als auch bei Modulhomomorphismen.

$$\begin{tikzcd} V(i) \arrow[r, "V(\alpha)"] \arrow[d, "f(i)"'] & V(j) \arrow[r, "V(\beta)"] \arrow[d, "f(j)"] & V(h) \arrow[d, "f(h)"] \\ W(i) \arrow[r, "W(\alpha)"'] & W(j) \arrow[r, "W(\beta)"'] & V(h) \end{tikzcd}$$

In den nächsten Vorlesungen beschäftigen wir uns mit der Struktur von Moduln, insbesondere welche kleinsten Bausteine gibt es, aus denen Moduln zusammengebaut werden. Die Moduln, die hier eine Rolle spielen, sind die *einfachen* Moduln und die *unzerlegbaren* Moduln. Die einfachen Moduln haben keine echten, nicht-trivialen Untermoduln; die unzerlegbaren Moduln lassen sich nicht als direkte Summe von zwei echten, nicht-trivialen Untermoduln schreiben. Um die Konzepte dieses Kapitels zu üben, betrachten wir ein Beispiel:

Beispiel 2.40. Sei Q der *Kroneckerköcher* aus Aufgabe 1.11, das heisst, $Q = Q_d : 1 \rightrightarrows 2$. Die *Kroneckeralgebra* KQ hat Basis $\{e_1, e_2, \alpha, \beta\}$, ist also vier-dimensional, und die Multiplikationstafel dieser Basiselemente ist

$\cdot$	e_1	e_2	α	β
e_1	e_1	0	α	β
e_2	0	e_2	0	0
α	0	α	0	0
β	0	β	0	0

a) Der Vorteil einer treuen Darstellung einer Algebra ist es, dass man eine äquivalente Definition der Algebra in den uns beim Rechnen vertrauten Matrizen erhält. Die erste Frage, die wir stellen wollen, ist entsprechend: Hat die Kroneckeralgebra KQ eine treue Darstellung $KQ \hookrightarrow M_n(K)$? Hierbei bedeutet der Pfeil $\hookrightarrow$, dass die Abbildung injektiv ist, siehe Definition 2.1. Falls eine treue Darstellung existiert, macht es Sinn dabei n möglichst klein zu wählen.

   i) Sei $n = 1$. Dann kann es aus Dimensionsgründen keine Einbettung des Vektorraumes KQ in die Matrizen $M_1(K)$ geben.

   ii) Sei $n = 2$. Die Algebra KQ besitzt echte, nicht-triviale Ideale, beispielsweise das zweiseitige Ideal $(\alpha, \beta) = K\text{-Span}\{\alpha, \beta\}$. Angenommen es existiert eine treue Abbildung $KQ \to M_2(K)$, dann ist diese ein Isomorphismus. Die Algbera $M_n(K)$ hat keine echten, nicht-trivialen zweiseitigen Ideale im Gegensatz zur Algebra KQ. Also ist $KQ \not\cong M_2(K)$.

   iii) Sei $n = 3$. In diesem Fall erhalten wir eine treue Darstellung, indem wir die Basisvektoren den folgenden linear unabhängigen Matrizen zuordnen:

$$e_1 \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; e_2 \mapsto \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; \alpha \mapsto \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \; \beta \mapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

   die sich analog zu obiger Multiplikationstabelle multiplizieren:

$\cdot$	E_{11}	$E_{22}+E_{33}$	E_{12}	E_{13}
E_{11}	E_{11}	0	E_{12}	E_{13}
$E_{22}+E_{33}$	0	$E_{22}+E_{33}$	0	0
E_{12}	0	E_{12}	0	0
E_{13}	0	E_{13}	0	0

   Damit ist die durch obige Zuordnung definierte Abbildung linear und multiplikativ, und schickt das Einselement von KQ auf das Einselement I_3 der Algebra

$$A := K\text{-Span}\{E_{11}, E_{22} + E_{33}, E_{12}, E_{13}\}.$$

   Die Kroneckeralgebra ist also eine Unteralgebra der Matrixalgebra $M_3(K)$.

b) Wir wollen als nächstes Beispiele von Köcherdarstellungen der Kroneckeralgebra geben. Gegeben seien die beiden folgenden Darstellungen:

$$K \underset{0}{\overset{0}{\rightrightarrows}} 0 \qquad \text{und} \qquad 0 \underset{0}{\overset{0}{\rightrightarrows}} K. \tag{2.4}$$

   Angenommen die beiden Darstellungen sind isomorph, so existieren nach Definition 2.37 Isomorphismen S, T, sodass das folgende Diagram kommutiert:

$$\begin{tikzcd} K \arrow[r, shift left, "0"] \arrow[r, shift right, "0"'] \arrow[d, "S"'] & 0 \arrow[d, "T"] \\ 0 \arrow[r, shift left, "0"] \arrow[r, shift right, "0"'] & K \end{tikzcd}$$

Wenn wir bei diesem Bild von einem kommutativen Diagram reden, so meinen wir, dass beide im Bild enthaltene Quadrate kommutieren. Das benötigen wir in diesem Fall aber gar nicht: Es gibt keine Vektorraumisomorphismen S und T zwischen K und 0. Also sind die Darstellungen nicht-isomorph. Beide Darstellungen korrespondieren zu eindimensionalen Moduln, und entsprechend können sie keine echten, nicht-trivialen Untermoduln haben. Moduln ungleich dem Nullmodul heissen *einfach* – beziehungsweise bei Darstellungen spricht man auch von *irreduziblen* Darstellungen – falls sie keinen echten nicht-trivialen Untermodul haben. Man sieht leicht, dass die in (2.4) angegebenen Darstellungen ein Vertretersystem der Isomorphieklassen der irreduziblen Darstellungen der Kroneckeralgebra sein müssen: Sei

$$\begin{tikzcd} V(1) \arrow[r, shift left, "V(\alpha)"] \arrow[r, shift right, "V(\beta)"'] & V(2) \end{tikzcd}$$

eine irreduzible Darstellung. Ist Vektorraum $V(2) \neq 0$, dann ist $0 \rightrightarrows K$ eine Teildarstellung von V. Schreibe ι für die Einbettungsabbildung. Dann ist das Diagram

$$\begin{tikzcd} V(1) \arrow[r, shift left, "0"] \arrow[r, shift right, "0"'] & V(2) \\ 0 \arrow[u, "\iota"] \arrow[r, shift left, "0"] \arrow[r, shift right, "0"'] & K \arrow[u, "\iota"'] \end{tikzcd}$$

ein kommutatives Diagram. Ist hingegen Vektorraum $V(2) = 0$, dann muss $V(1) \neq 0$ sein und so ist $K \rightrightarrows 0$ eine Teildarstellung:

$$\begin{tikzcd} V(1) \arrow[r, shift left, "0"] \arrow[r, shift right, "0"'] & 0 \\ K \arrow[u, "\iota"] \arrow[r, shift left, "0"] \arrow[r, shift right, "0"'] & 0 \arrow[u, "\iota"'] \end{tikzcd}$$

Die beiden oben angegebenen eindimensionalen Moduln sind also bis auf Isomorphie die einzigen einfachen Moduln der Kroneckeralgebra.

c) Wir betrachten den nächsteinfachen Fall: $V(1) = K = V(2)$. Wir wollen alle Darstellungen der Form $K \rightrightarrows K$ bis auf Isomorphie klassifizieren. Lineare Abbildungen zwischen den Vektorräumen K und K entsprechen Multiplikation mit einem Skalar. Eine solche Abbildung ist ein Isomorphismus, falls das Skalar ungleich Null ist. Seien $\lambda, \mu \in K$ mit $V(\alpha) = \lambda \cdot \mathrm{id}$ und $V(\beta) = \mu \cdot \mathrm{id}$. Angenommen es existieren Skalare $s, t \in K$ und $a, b \in K \backslash \{0\}$ mit

$$\begin{tikzcd} K \arrow[r, shift left, "\lambda"] \arrow[r, shift right, "\mu"'] \arrow[d, "a"] & K \arrow[d, "b"'] \\ K \arrow[r, shift left, "s"] \arrow[r, shift right, "t"'] & K \end{tikzcd} \tag{2.5}$$

Dann gilt also $sa = b\lambda$ und $ta = b\mu$. Wegen $b \neq 0$ erhalten wir

$$\begin{pmatrix} \lambda \\ \mu \end{pmatrix} = c \cdot \begin{pmatrix} s \\ t \end{pmatrix}. \tag{2.6}$$

mit $0 \neq c = a/b$. Somit sind die Darstellungen in der ersten und zweiten Zeile des Diagrams in (2.5) isomorph, genau dann, wenn es ein Skalar $0 \neq c \in K$ gibt, so dass Gleichung (2.6) erfüllt ist. Gegeben (λ, μ') mit $\lambda \neq 0$, dann ist die Darstellung zu den Abbildungen (λ, μ') nach (2.6) isomorph zur Darstellung zu $(1, \mu)$. Ist hingegen $\lambda = 0$, so ist die Darstellung zu den Abbildungen $(0, \mu')$ nach (2.6) isomorph zur Darstellung zu $(0, 1)$. Vertreter der Isomorphieklassen für Darstellungen der Kroneckeralgebra mit Dimensionsvektor $(1, 1)$, also eine *Normalform*, erhalten wir für $\mu \in K$ durch

$$K \overset{1}{\underset{\mu}{\rightrightarrows}} K \qquad \text{und} \qquad K \overset{0}{\underset{1}{\rightrightarrows}} K \tag{2.7}$$

Ist der Körper K unendlich, so gibt es insbesondere unendlich viele paarweise nicht-isomorphe Darstellungen von KQ mit Dimensionsvektor $(1, 1)$.

Die Klassifikation isomorpher Darstellungen mit Dimensionsvektor (m, n) der Kroneckeralgebra ist gelöst:

- `Weierstrass 1867:` Normalform für gewisse $V(\alpha)$ und $V(\beta)$;
- `Kronecker 1890:` allgemeine Lösung.

Die Lösung dieses Normalformenproblems ist ähnlich wie das Normalformenproblem in Beispiel 2.38 oder Aufgabe 2.19 mittels Linearer Algebra lösbar, aber länglich. Besser löst man es heute mit Auslander-Reiten Theorie.

Aufgabe 2.20. Sei Q der Kroneckerköcher. Wir setzen Beispiel 2.40 fort. Sind die Darstellungen in (2.7) unzerlegbar? Begründen Sie Ihre Antwort.

Aufgabe 2.21. Sei Q ein Köcher, sodass die Wegealgebra KQ endlich-dimensional ist mit Knotenmenge $Q_0 = \{1, \ldots, n\}$. Das sagt nichts anderes, als dass der Köcher Q keine Schleifen und Zykel hat. Für $i \in Q_0$ definieren wir die Darstellung S_i durch

$$S_i(j) = \begin{cases} K & \text{für } j = i, \\ 0 & \text{sonst.} \end{cases}$$

Zeigen Sie, dass die Darstellungen $S_1, \ldots, S_n$ bis auf Isomorphie ein Vertretersystem der irreduziblen KQ-Darstellungen bilden. Genauer, zeigen Sie:

a) Die Darstellungen S_i mit $i \in Q_0$ sind einfach;

b) Die Darstellung S_i ist nicht isomorph zur Darstellung S_j für $i \neq j$;

c) Ist S eine beliebige Darstellung von KQ, so ist für einen Index i_0 die Darstellung S_{i_0} eine Unterdarstellung von S.

Kapitel 3

Einfache Moduln und der Satz von Jordan-Hölder

Eine der Grundfragen der Darstellungstheorie ist es, die einfachen Moduln einer gegebenen Algebra zu parametrisieren und zu konstruieren, und dann in einem weiteren Schritt zu verstehen, wie ein beliebiger Modul aus einfachen Moduln zusammengebaut ist. Ganz in Analogie zum Satz von Jordan-Hölder für Gruppen, der zeigt, dass jede Gruppe aus einfachen Gruppen zusammengesetzt ist, geht es auch hier zunächst darum, dass jeder Moduln aus einfachen Moduln zusammengesetzt ist. Es ist dann eine weitere sehr schwierige Frage in der Darstellungstheorie, welche einfachen Moduln man wie miteinander verkleben kann, eine die dann weit über diese Vorlesung hinausgeht, und bei der noch viele Fragen offen sind. In diesem Kapitel sei R ein Ring, K ein Körper und A eine K-Algebra.

3.1 Einfache Moduln

3.1.1 Eigenschaften und Beispiele

Wir wollen in diesem Abschnitt einfache Moduln genauer charakterisieren und viele Beispiele einfacher Moduln kennenlernen. Wir haben bereits am Ende von Kapitel 2.5 einfache Moduln informell kennengelernt:

Definition 3.1. Sei M ein R-Modul mit $M \neq \{0\}$. Dann heisst der Modul M *einfach*, falls $\{0\}$ und M die einzigen Untermoduln von M sind.

Aufgabe 3.1. Ein $K[X]$-Modul ist nach Beispiel 2.38 ein Vektorraum V, zusammen mit einer linearen Abbildung, die angibt, wie X auf dem Vektorraum V operiert. Sei $V = K^2$ und X operiere auf V durch $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$. Ist der Modul V einfach? Begründen Sie Ihre Antwort.

Ist A eine K-Algebra, so ist jeder eindimensionale A-Modul einfach, da echte Untermoduln als Untervektorräume eine echt kleinere Vektorraumdimension haben. Wir sehen in Beispiel 3.4, dass die Umkehrung falsch ist: einfache Moduln können beliebig grosse Dimension haben. In der Praxis ist es häufig schwierig, nachzuweisen, dass ein gegebener Modul einfach ist. Eine erste äquivalente und aber in der Praxis sehr naive Charakterisierung von Einfachheit ist folgende:

Lemma 3.2. *Sei M ein R-Modul und $0 \neq m \in M$. Dann ist*

$$R \cdot m := \{rm \mid r \in R\}$$

ein Untermodul von Modul M. Es ist M einfach genau dann, wenn $M \neq \{0\}$ und $Rm = M$ für alle $0 \neq m \in M$.

Beweis. Seien $r, s \in R$.

a) Dann ist $rm \pm sm = (r \pm s)m \in Rm$, da der Ring R abgeschlossen ist bezüglich Addition und additiven Inversen. Damit ist $(Rm, +)$ eine abelsche Gruppe. Ausserdem ist $r \cdot (sm) = (rs) \cdot m \in Rm$, da Ring R multiplikativ abgeschlossen ist. Also ist Rm nach Definition 2.18 ein Untermodul von M.

b) Bei der zweiten Aussage der Bemerkung sind zwei Richtungen zu zeigen:

   i) Sei M einfach. Nach Definition 3.1 ist dann $M \neq \{0\}$. Sei $0 \neq m \in M$. Wegen $0 \neq m = 1 \cdot m \in R \cdot m \leq M$, ist also $Rm \neq 0$ ein nicht-trivialer Untermodul des einfachen Moduls M. Einfache Moduln haben aber nur sich selber und den trivialen Modul als Untermodul. Nach Definition 3.1 ist also $M = Rm$.

   ii) Umgekehrt, sei $0 \neq U \leq M$ ein nicht-trivialer Untermodul. Dann existiert ein Element $0 \neq m \in U$. Nach Annahme ist $M = Rm \leq U \leq M$, also gilt $U = M$. Nach Definition 3.1 ist also M einfach. □

Beispiel 3.3. Bekanntlich ist jede abelsche Gruppe ein $\mathbb{Z}$-Modul mit

$$z \cdot a := \begin{cases} \underbrace{a + \ldots + a}_{z\text{-mal}} & \text{falls } z > 0, \\ -\underbrace{(a + \ldots + a)}_{|z|\text{-mal}} & \text{falls } z < 0, \\ 0 & \text{falls } z = 0. \end{cases}$$

Sei $n \in \mathbb{N}$. Dann ist die abelsche Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ein $\mathbb{Z}$-Modul mit

$$\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (z, \bar{a}) \mapsto z \cdot \bar{a} := \overline{z \cdot a}.$$

Wir wollen bestimmen, welche $\mathbb{Z}$-Moduln $\mathbb{Z}/n\mathbb{Z}$ einfach sind.

a) Sei p eine Primzahl. Moduln sind nach Definition 2.13 insbesondere abelsche Gruppen; Untermoduln sind also insbesondere Untergruppen. Nach dem Satz von Lagrange besitzt $\mathbb{Z}/p\mathbb{Z}$ keine echten, nicht-trivialen Untergruppen, also auch keine echten, nicht-trivialen Untermoduln. Also ist der Modul $\mathbb{Z}/p\mathbb{Z}$ nach Definition 3.1 ein einfacher $\mathbb{Z}$-Modul.

b) Sei $n > 1$ nicht prim. Dann existiert $1 < m < n$ mit m teilt n. Nach dem ersten Teil von Lemma 3.2 ist damit $0 \neq \mathbb{Z}\bar{m} < \mathbb{Z}/n\mathbb{Z}$ mit $\bar{m} = m + n\mathbb{Z}$; nach dem zweiten Teil von Bemerkung 3.2 oder nach Definition 3.1 ist damit der Modul $\mathbb{Z}/n\mathbb{Z}$ nicht einfach.

Das nächste Beispiel ist zentral zu der in späteren Vorlesungen entwickelten Theorie. Es zeigt darüberhinaus auch, dass einfache Moduln beliebig grosse Dimension haben können. Einfachheit eines Moduls ist häufig nicht einfach nachzuweisen. Beachten Sie, wie im Beweis zur Einfachheit im nächsten Beispiel geschickt gerechnet wird.

Beispiel 3.4. Sei $A = M_n(K)$ Algebra und sei $V = K^n$. Dann ist V ein A-Modul mittels Matrixmultiplikation $A \times V \to V, (B, x) \mapsto Bx$, und dieser n-dimensionale A-Modul ist einfach.

Beweis. Sei $\{0\} \neq U < V$ ein Untermodul. Dann existiert ein Vektor $0 \neq u = (x_1, \ldots, x_n)^T \in U$. Wähle einen Index j mit $x_j \neq 0$. Da U ein Modul ist, folgt:

$$\underbrace{x_j^{-1} \cdot E_{ij}}_{\in M_n(K)} \cdot u = x_j^{-1}(x_j e_i) = e_i \in U, \text{ für } 1 \leq i \leq n.$$

Damit ist gezeigt, dass alle Basisvektoren $\{e_1, \ldots, e_n\}$ der Standardbasis von $V = K^n$ in U liegen. Also ist $U = V$. Wir haben also gezeigt, dass der Modul V keine echten, nicht-trivialen Untermoduln besitzt. Nach Definition 3.1 ist damit V einfach. □

Aufgabe 3.2. Sei K ein Körper der Charakteristik Null. Die Elemente $\tau = (1, 2)$ und $\pi = (1, 2, 3, 4)$ erzeugen die symmetrische Gruppe S_4 der Ordnung vier. Eine KS_4-Darstellung $\mathfrak{X}$ ist definiert durch

$$\mathfrak{X}(\tau) = \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ und } \mathfrak{X}(\pi) = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

Sei V der zur Darstellung $\mathfrak{X}$ korrespondierende Modul. Zeigen Sie, dass V ein einfacher Modul ist. (Der für die Darstellung benutzte Buchstabe $\mathfrak{X}$ ist eine Variante des Buchstabens X, im Latex-Schriftsatz \mathfrak.)

Ob ein Modul über einer Algebra einfach ist, hängt auch vom zugrundeliegenden Körper ab. Wir zeigen dies mit dem nächsten Beispiel.

Beispiel 3.5. Sei $G = D_8 = \langle \sigma, \tau \rangle$ die Symmetriegruppe des Quadrates, siehe Beispiel 2.9, wobei σ die Rotation um 90 Grad um den Nullpunkt ist und τ die Spiegelung an der y-Achse. Nach Beispiel 2.9 ist

$$\rho : \mathbb{R}G \to M_2(\mathbb{R}) \text{ mit } \sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ und } \tau \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

eine Darstellung der Algebra $\mathbb{R}G$. Sei V der zu ρ korrespondierende Modul, siehe Bemerkung 2.28. Angenommen V ist nicht einfach. Dann existiert ein nicht-trivialer Untermodul $U < V$. Da $\dim V = 2$ ist, muss gelten $\dim U = 1$. Sei $\{u\}$ Basis von U. Mit Definition 2.13 folgt, dann ist $\sigma \cdot u \in U$, also existiert $\lambda \in \mathbb{R}$ mit $\sigma \cdot u = \lambda \cdot u$, beziehungsweise $\rho(\sigma) \cdot u = \lambda \cdot u$. Nach Linearer Algebra ist als λ ein Eigenwert der Matrix $\rho(\sigma)$. Man sieht aber leicht, dass $\rho(\sigma)$ keine reellen Eigenwerte besitzt: Für das charakteristische Polynom der Matrix $\rho(\sigma)$ gilt:

$$0 = \chi_{\rho(\sigma)}(t) = \det \begin{pmatrix} t & 1 \\ -1 & t \end{pmatrix} = t^2 + 1 \Leftrightarrow t = \pm i.$$

Damit sind die Eigenwerte der Matrix $\rho(\sigma)$ nicht-reell. Dies ist ein Widerspruch, und es folgt, dass V keinen echten, nicht-trivialen Untermodul besitzt. Damit ist V nach Definition 3.1 ein einfacher $\mathbb{R}G$-Modul. Genauso könnten wir die Darstellung aus Beispiel 2.9 über dem Körper $\mathbb{C}$ betrachten. Der hierzu korrespondierende Modul ${}_{\mathbb{C}G}V$ ist ebenfalls ein einfacher Modul, dies muss aber in einer gesonderten Rechnung nachgewiesen werden. Es gibt Beispiele von Moduln von Gruppenalgebren, die über einem kleinen Körper wie $\mathbb{R}$ einfach sind, allerdings über $\mathbb{C}$ zerfallen.

Wir betrachten im nächsten Abschnitt *Kompositionsreihen* von Moduln, und bilden hierbei Quotientenmoduln. Wann ein Quotientenmodul einfach ist, wird durch das folgende Resultat charakterisiert, was aber häufig nicht von praktischem, wohl aber von theoretischem Nutzen ist.

Bemerkung 3.6. Sei R ein Ring und M ein Untermodul eines R-Moduls V. Dann ist V/M einfach genau dann, wenn M ein maximaler Untermodul von V ist.

Beweis: Der Beweis ist eine Anwendung der Untermodulkorrespondenz 2.27: Der Modul V/M ist nach Definition 3.1 einfach genau dann, wenn V/M keine echten, nicht-trivialen Untermoduln besitzt. Nach Theorem 2.27 passiert das genau dann, wenn es keinen Untermodul $W \leq V$ gibt mit $M \subsetneq W \subsetneq V$, also genau dann, wenn M maximaler Untermodul von V ist. □

Beispiel 3.7. Aus Algebra wissen wir, dass ein irreduzibles Polynom f im Hauptidealring $K[X]$ ein maximales Ideal (f) erzeugt. Ideale sind nach 2.19 b) Untermoduln des regulären Moduls $K[X]$. Der Quotientenmodul $K[X]/(f)$ ist damit ein einfacher $K[X]$-Modul. Es gibt irreduzible Polynome beliebig grossen Grades. Entsprechend gibt es einfache $K[X]$-Moduln beliebig grosser Dimension.

An das Arbeiten mit Quotientenmoduln muss man sich etwas gewöhnen. Wir geben deshalb noch ein weiteres Beispiel an, bei dem der Quotientenmodul einfach ist. Es zeigt auch, wie man neue einfache Moduln auffinden kann: Man sucht in einem bekannten Modul nach einem (maximalen oder beliebigem) Untermodul, und teilt diesen heraus. Ist der Quotient einfach, ist das Ziel erreicht. Unter Umständen muss man den Prozess wiederholen, bis man bei einem einfachen (Sub)quotienten endet. Es ist natürlich unklar dabei, ob wir einen neuen einfachen Modul dabei finden, also einen Modul, der nicht-isomorphen zu den bereits bekannten einfachen Moduln ist. Diese Grundidee nehmen wir aber in Kapitel 3.2 wieder auf, wo wir die Struktur von Moduln genauer verstehen wollen. Im nächsten Beispiel konstruieren wir nun erst einmal einen neuen einfachen zweidimensionalen Modul für die Gruppenalgebra KS_3.

Beispiel 3.8. Sei K ein Körper, sei $G = S_3 = \langle \tau, \sigma \rangle$ mit $\tau = (1,2)$ und $\sigma = (1,2,3)$, und sei M der KS_3-Modul korrespondierend zur Darstellung ρ aus Beispiel 2.10. Es ist also $\{b_1, b_2, b_3\}$ eine Basis von M und die Erzeuger operieren durch:

$$\begin{aligned} \tau \cdot b_1 &= b_2, & \sigma \cdot b_1 &= b_2, \\ \tau \cdot b_2 &= b_1, & \sigma \cdot b_2 &= b_3, \\ \tau \cdot b_3 &= b_3, & \sigma \cdot b_3 &= b_1. \end{aligned}$$

Nach Aufgabe 2.14 ist der triviale Modul in Form von $U := K\text{-Span}\{b_1+b_2+b_3\}$ ein Untermodul von M. Der Quotientenmodul M/U ist damit ein zweidimensionaler

KS_3-Modul. Wähle Basis $\mathcal{B}$ von Unterraum U, ergänze durch $\mathcal{C}$ zu einer Basis $\mathcal{B} \cup \mathcal{C}$ des Vektorraumes M, dann ist nach Linearer Algebra $\bar{\mathcal{C}} := \{m + U \mid m \in \mathcal{C}\}$ eine Basis des Quotientenvektorraumes M/U. In unserem Beispiel ist also $\{b_1 + U, b_2 + U\}$ eine Basis des Quotientenmoduls M/U mit Operation:

$$\begin{aligned} \tau \cdot (b_1 + U) &\overset{2.22}{=} \tau b_1 + U = b_2 + U, \\ \tau \cdot (b_2 + U) &\overset{2.22}{=} \tau b_2 + U = b_1 + U, \end{aligned}$$

und

$$\begin{aligned} \sigma \cdot (b_1 + U) &\overset{2.22}{=} \sigma b_1 + U = b_2 + U, \\ \sigma \cdot (b_2 + U) &\overset{2.22}{=} b_3 + U = b_3 - (b_1 + b_2 + b_3) + U = (-b_1 + U) + (-b_2 + U). \end{aligned}$$

Der Modul $W = M/U$ hat also eine Basis $\{w_1, w_2\}$ und die Operation der Algebra KS_3 ist gegeben durch

$$\begin{aligned} \tau \cdot w_1 &= w_2, & \sigma \cdot w_1 &= w_2 \\ \tau \cdot w_2 &= w_1, & \sigma \cdot w_2 &= -w_1 - w_2. \end{aligned}$$

Sei ρ_W die zu W korrespondierende Matrixdarstellung. Die darstellenden Matrizen sind also

$$\rho_W(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ und } \rho_W(\sigma) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Es ist

$$\det \begin{pmatrix} \lambda & -1 \\ -1 & \lambda \end{pmatrix} = \lambda^2 - 1 = (\lambda + 1)(\lambda - 1) = 0 \text{ genau dann, wenn } \lambda = \pm 1.$$

Die Matrix $\rho_W(\tau)$ hat also Eigenwerte ± 1, wobei die Matrix nur den Eigenwert Eins hat, falls die Charakteristik von K gerade zwei ist. Zum Eigenwert $\lambda = 1$ gehören die Eigenvektoren $(x, x)^T$ mit $x \in K$. Zum Eigenwert $\lambda = -1$ gehören die Eigenvektoren $(x, -x)^T$ mit $x \in K$. Es ist aber

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ x \end{pmatrix} = \begin{pmatrix} -x \\ 0 \end{pmatrix},$$

also ist $(x, x)^T$ kein Eigenvektor der Matrix $\rho_W(\sigma)$ für alle $x \in K$. Ganz analog haben wir

$$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ -x \end{pmatrix} = \begin{pmatrix} x \\ 2x \end{pmatrix},$$

also ist $(x, -x)^T$ kein Eigenvektor der Matrix $\rho_W(\sigma)$, für alle $x \in K$. Die Matrizen $\rho_W(\tau)$ und $\rho_W(\sigma)$ haben also keinen gemeinsamen Eigenvektor. Keinen gemeinsamen Eigenvektor zu besitzen bedeutet, dass der Modul W keinen eindimensionalen Untermodul hat. Da W zweidimensional ist, folgt, dass der Modul W einfach ist. Im Sinne von Bemerkung 3.6 haben wir gezeigt, dass der triviale Untermodul U ein maximaler Untermodul in M ist. Mit Aufgabe 2.15 folgt, dass der Modul $M = U \oplus W'$ eine direkte Summe von Untermoduln ist, falls die Charakteristik des Körpers ungleich drei ist. Mit Theorem 2.26 folgt, dass hierbei $W' \simeq W$ ist:

$$W = M/U = (U \oplus W')/U \simeq W'/(U \cap W') = W'/\{0\} = W'.$$

Aufgabe 3.3. Wir setzen Aufgabe 3.2 fort. Sei jetzt K ein Körper der Charakteristik zwei. Bestimmen Sie alle eindimensionalen Untermoduln von V, und konstruieren Sie mit deren Hilfe, falls möglich, einen zweidimensionalen einfachen KS_4-Modul.

3.1.2 Schurs Lemma und Anwendungen

Im letzten Teilabschnitt haben wir uns Charakterisierungen einfacher Moduln angeschaut. In diesem Teilabschnitt geht es um die Homomorphismen zwischen einfachen Moduln. Das folgende harmlos aussehende Lemma hat starke Konsequenzen in der Darstellungstheorie:

Lemma 3.9 (Schurs Lemma, allgemeine Form)**.** *Sei R ein Ring, seien S, T einfache R-Moduln und $\phi : S \to T$ ein R-Modulhomomorphismus. Dann ist entweder $\phi = 0$ oder ϕ ist ein Isomorphismus.*

Beweis. Wir müssen zeigen, ist $\phi \neq 0$, dann ist die Abbildung ϕ bijektiv.

a) Nach Bemerkung 2.24 b) ist $\ker \phi \leq S$ ein Untermodul. Nach Voraussetzung ist S ein einfacher Modul. Da $\phi \neq 0$, ist nach Definition 3.1 also $\ker \phi = 0$. Damit ist ϕ injektiv.

b) Nach Bemerkung 2.24 b) und da $\phi \neq 0$ ist, folgt $0 \neq \operatorname{im} \phi \leq T$ Untermodul. Nach Voraussetzung ist T ein einfacher Modul. Definition 3.1 impliziert also $\operatorname{im} \phi = T$, das heisst, die Abbildung ϕ ist surjektiv, also insgesamt bijektiv.

Über algebraisch abgeschlossenen Körpern wie beispielsweise dem Körper $\mathbb{C}$ können wir die Abbildung ϕ genau bestimmen:

Lemma 3.10 (Schurs Lemma über einem algebraisch abgeschlossenen Körper)**.** *Sei A eine Algebra über einem algebraisch abgeschlossenen Körper K. Sei $S = T$ ein einfacher A-Moduln und $\phi : S \to T$ ein A-Modulhomomorphismus. Dann existiert ein Skalar $\lambda \in K$ mit $\phi = \lambda \cdot \mathrm{id}_S$.*

Beweis. Sei χ_ϕ das charakteristische Polynom der linearen Abbildung ϕ. Da der Körper K algebraisch abgeschlossen ist, hat die Gleichung $\chi_\phi(t) = 0$ mindestens eine Lösung im Körper K. Nach Linearer Algebra hat damit die lineare Abbildung ϕ mindestens einen Eigenwert $\lambda \in K$. Sei $0 \neq v \in S$ ein zum Eigenwert λ gehöriger Eigenvektor, das heisst, es gilt $\phi(v) = \lambda v$. Die Abbildung $\lambda \cdot \mathrm{id}_S$ ist ein Modulhomomorphismus. Also ist auch $\phi - \lambda \cdot \mathrm{id}_S$ ein Modulhomomorphismus und nach Bemerkung 2.24 b) ist $0 \neq v \in \ker(\phi - \lambda \cdot \mathrm{id}_S) \leq S$ Untermodul. Da S nach Voraussetzung einfach ist, folgt mit Definition 3.1, dass $\ker(\phi - \lambda \cdot \mathrm{id}_S) = S$ ist. Damit ist aber $\phi - \lambda \cdot \mathrm{id}_S = 0$, also $\phi = \lambda \, \mathrm{id}_S$. □

Wir schauen uns eine erste kleinen Anwendung von Schurs Lemma an, und zeigen, dass für eine kommutativen Algebra über einem algebraisch abgeschlossenen Körper alle einfachen Moduln eindimensional sind, und sie damit mit den Methoden aus Aufgabe 2.4 leicht bestimmt werden können. Hierzu benötigen wir zunächst die folgende Bemerkung:

Bemerkung 3.11. Sei R ein Ring und $z \in Z(R) = \{r \in R \mid rs = sr \text{ für alle } s \in R\}$ ein Element im Zentrum von R. Sei M ein R-Modul. Dann ist die Abbildung $\phi : M \to M$, definiert durch $m \mapsto z \cdot m$ ein Modulhomomorphismus.

Beweis. Für alle $r \in R$ und $m \in M$ gilt:

$$\phi(rm) \overset{\text{Def}}{=} z(rm) \overset{\text{(M3)}}{=} (zr)m \overset{z \in Z(R)}{=} (rz)m \overset{\text{(M3)}}{=} r(zm) \overset{\text{Def}}{=} r\phi(m).$$

Also ist ϕ ein Modulhomomorphismus. $\square$

Lemma 3.12. *Sei A eine kommutative Algebra über einem algebraisch abgeschlossenen Körper K. Dann ist jeder einfache A-Modul eindimensional.*

Beweis. Sei S ein einfacher A-Modul.

a) Sei $a \in A$. Da die Algebra A kommutativ ist, liegt das Element a im Zentrum $Z(A) = A$. Nach Bemerkung 3.11 ist die Abbildung $\phi : S \overset{a\cdot-}{\to} S$, definiert durch $s \mapsto a \cdot s$ ein Modulhomomorphismus. Mit Schurs Lemma 3.10 existiert ein Skalar $\lambda_a \in K$ mit $\phi = \lambda_a \cdot \mathrm{id}$. Für alle $s \in S$ gilt also $a \cdot s = \phi(s) = \lambda \cdot s$.

b) Wähle $0 \neq s \in S$. Dann ist nach a) der Vektorraum $0 \neq K\text{-Span}\{s\}$ abgeschlossen unter der Operation von A, und damit ein Untermodul von S. Da S nach Voraussetzung einfach ist, gilt $K\text{-Span}\{s\} = S$. Also ist S ein eindimensionaler Modul. $\square$

Aufgabe 3.4. Entscheiden Sie jeweils, ob der gegebene Modul M einfach ist:

a) Modul $M = \mathbb{C}$ als Modul für die $\mathbb{R}$-Algebra $\mathbb{R}$;

b) Modul $M = \mathbb{C}$ als Modul für die $\mathbb{R}$-Algebra $\mathbb{C}$.

Folgern Sie, dass die Aussage in Lemma 3.12 falsch ist, falls der zugrundeliegende Körper K nicht algebraisch abgeschlossen ist.

Aufgabe 3.5. Sei A eine kommutative Algebra über einem algebraisch abgeschlossenem Körper K.

a) Zeigen Sie, dass ein A-Modul V die direkte Summe einfacher Moduln ist genau dann, wenn V eine Basis aus simultanen Eigenvektoren für alle $a \in A$ besitzt, bezüglich der Abbildung $v \mapsto av$, für $v \in V$.

b) Seien S, T zwei einfache A-Moduln. Zeigen Sie, dass $S \simeq T$ ist genau dann, wenn jedes Element $a \in A$ mit demselben Eigenwert auf S sowie T operiert.

Lassen sich die beiden Aussagen auf nicht-kommutative Algebren verallgemeinern?

Im nächsten Beispiel geben wir eine Anwendung von Lemma 3.12:

Beispiel 3.13. Sei $K = \mathbb{C}$ und $G = V_4 = \langle a, b \mid a^2 = 1 = b^2 = (ab)^2 \rangle$ die Kleinsche Vierergruppe. Da V_4 eine abelsche Gruppe ist, ist die Algebra KV_4 kommutativ. Nach Lemma 3.12 sind also alle einfachen KV_4-Moduln eindimensional. Wir haben also in Aufgabe 2.4 bis auf Isomorphie alle einfachen KV_4-Moduln bestimmt, und wiederholen hier der Vollständigkeit halber die Lösung:

a) Sei $\rho : KV_4 \to M_1(K)$ eine Darstellung vom Grad eins mit $\rho(a) = (x)$ und $\rho(b) = (y)$. Da ρ Algebrenhomomorphismus ist, gilt

$$(1) = \rho(1) = \rho(a^2) = \rho(a)^2 = (x)^2.$$

Damit ist $x^2 = 1$. Analog zeigt man, dass $y^2 = 1$ und $(xy)^2 = 1$ ist. Damit sind $x, y \in \{\pm 1\}$ und es gibt genau vier eindimensionale KV_4-Moduln:

$$\begin{aligned} S_1 &= K\text{-Span}\{v_1\} \text{ mit } av_1 = v_1 \text{ und } bv_1 = v_1, \\ S_2 &= K\text{-Span}\{v_2\} \text{ mit } av_2 = v_2 \text{ und } bv_2 = -v_2, \\ S_3 &= K\text{-Span}\{v_3\} \text{ mit } av_3 = -v_3 \text{ und } bv_3 = v_3, \\ S_4 &= K\text{-Span}\{v_4\} \text{ mit } av_4 = -v_4 \text{ und } bv_4 = -v_4. \end{aligned}$$

b) Wir zeigen diese vier einfachen Moduln sind paarweise nicht isomorph. Die eindimensionale Moduln S_i und S_j sind isomorph genau dann, wenn die zugehörigen Darstellungen ρ_i und ρ_j äquivalent sind, siehe Proposition 2.29. Dies passiert nach Definition 2.3 , wenn es eine invertierbare Matrix Z gibt mit

$$\begin{aligned} \rho_i(a) &= Z^{-1}\rho_j(a)Z = \rho_j(a), \\ \rho_i(b) &= Z^{-1}\rho_j(b)Z = \rho_j(b). \end{aligned}$$

Dies impliziert, dass $i = j$ ist. Damit sind die vier oben angegebenen Moduln paarweise nicht-isomorph, und die Gruppenalgebra KV_4 hat bis auf Isomorphie genau vier verschiedene einfache Moduln. In den letzten beiden Gleichungen gilt jeweils das zweite Gleichheitszeichen, weil wir mit 1×1-Matrizen arbeiten, also im kommutativen Körper K. Das in b) ausgeführte Argument ist natürlich für beliebige eindimensionale Moduln gültig.

3.1.3 Einfache Moduln für direkte Produkte von Algebren

In diesem Abschnitt studieren wir die einfachen Moduln eines direkten Produktes von Algebren $A = A_1 \times A_2$, siehe Beispiel 1.6. Hier sind die einfachen Moduln der Algebra A durch die einfachen Moduln der kleineren Algebren A_1 und A_2 gegeben, mittels Inflation. Dieses Beispiel ist wichtig für die Theorie in späteren Vorlesungen. Gleichzeitig können wir das wichtige und gleichzeitig einfache Konzept der Inflation aus Beispiel 2.6 üben. Wir benötigen zunächst die folgende Modulzerlegung:

Lemma 3.14. *Sei $A = A_1 \times A_2$ direktes Produkt von Algebren A_i, mit $i = 1, 2$. Sei M ein A-Modul. Definiere die Mengen*

$$\begin{aligned} M_1 &:= \{(1, 0) \cdot m \mid m \in M\}, \\ M_2 &:= \{(0, 1) \cdot m \mid m \in M\}. \end{aligned}$$

Dann sind M_1 und M_2 Moduln über der Algebra A, und es gilt $M = M_1 \oplus M_2$.

Beweis. Es ist $(M_1, +)$ eine abelsche Gruppe, die abgeschlossen ist unter der Operation der Algebra, denn

$$(a_1, a_2) \cdot (1, 0) \cdot m \quad = \quad (a_1, 0) \cdot m = (1, 0) \cdot \underbrace{(a_1, 0) \cdot m}_{\in M} \in M_1,$$

für alle $a_i \in A_i$, mit $i = 1, 2$. Also ist M_1 ein A-Modul. Analog sieht man, dass auch M_2 ein A-Modul ist. Sei jetzt $m \in M$ beliebig. Dann ist

$$m = (1, 1) \cdot m = ((1, 0) + (0, 1)) \cdot m = (1, 0) \cdot m + (0, 1) \cdot m \in M_1 + M_2.$$

Also ist $M = M_1 + M_2$. Sei $x \in M_1 \cap M_2$. Dann existieren $m_i \in M_i$, mit $i = 1, 2$, sodass $x = (1, 0)m_1 = (0, 1)m_2$ ist. Wir operieren von links mit dem Algebrenelement $(1, 0)$:

$$(1, 0) \cdot x = \begin{cases} (1, 0)(1, 0) \cdot m_1 = (1, 0)m_1 = x, \\ (1, 0)(0, 1) \cdot m_2 = (0, 0) \cdot m_2 = 0. \end{cases}$$

Also ist $x = 0$ und damit $M_1 \cap M_2 = \{0\}$. Der Modul M ist damit gleich der direkten Summe seiner Untermoduln M_1 und M_2. □

Bemerkung 3.15. Das im letzten Beweis verwandte Prinzip ist allgemeiner: Sind e_1 und e_2 zentrale orthogonale Idempotente einer Algebra A mit $1 = e_1 + e_2$ und ist M ein A-Modul, so sind e_1M und e_2M ebenfalls A-Moduln mit $M = M_1 \oplus M_2$. Hierbei heisst ein Idempotent e *zentral*, falls es im Zentrum der Algebra liegt. Die Zentralität der Idempotente garantiert, dass e_iM wieder ein A-Modul ist für $i = 1, 2$. Dass die Idempotente eine *Zerlegung der Eins* bilden, also $1 = e_1 + e_2$ ist, garantiert, dass $M = e_1M + e_2M$ ist. Die Orthogonalität der Idempotente, also dass $e_1e_2 = 0 = e_2e_1$ ist, liefert eine direkte Summenzerlegung, wir erhalten also $M = M_1 \oplus M_2$.

Um unser Resultat zu einfachen Moduln der Algebra $A = A_1 \times A_2$ zu beweisen, benötigen wir noch das folgende Resultat:

Bemerkung 3.16. Beispiel 2.6 erklärt das Konzept von Inflation für Darstellungen. Mittels Bemerkung 2.28 können wir dies übersetzen in eine Aussage über Moduln: Sei A eine Algebra mit Ideal $I \lhd A$. Ist M ein A/I-Modul, dann ist M ein A-Modul mit $I \cdot M = 0$ ist. Umgekehrt, ist M ein A-Modul mit $I \cdot M = 0$, dann ist M ein A/I-Modul.

Bei Inflation ändert sich nichts an der Moduloperation; entsprechend ändert Inflation nichts an der Modulstruktur:

Proposition 3.17. *Sei $A = A_1 \times A_2$ direktes Produkt von Algebren A_i, mit $i = 1, 2$. Die einfachen A-Moduln sind genau die Inflationen der einfachen A_1-Moduln zusammen mit den Inflationen der einfachen A_2-Moduln.*

Beweis. Wir haben zwei Richtungen zum Beweis der Aussage zu zeigen:

a) Die Menge $I := \{0\} \times A_2$ ist eine abelsche Gruppe bezüglich Addition. Da A_2 multiplikativ abgeschlossen ist, gilt $(a_1, a_2) \cdot (0, i) = (0, a_2 \cdot i) \in I$ und $(0, i) \cdot (a_1, a_2) = (0, i \cdot a_2) \in I$. Damit ist $I \lhd A$ ein zweiseitiges Ideal. Sei π_1 die

Projektion von A auf A_1, also $\pi : A \mapsto A_1$, mit $\pi(a_1, a_2) = a_1$. Dann ist π_1 ein surjektiver Algebrenhomomorphismus mit Kern $\{0\} \times A_2 = I$. Mit dem Homomorphiesatz 1.18 für Algebren, angewandt auf die Abbildung π_1 folgt, dass

$$A/I = (A_1 \times A_2)/(\{0\} \times A_2) \simeq \operatorname{im} \pi_1 = A_1.$$

Sei nun S ein einfacher A_1-Modul. Durch Inflation, siehe Bemerkung 3.16, ist dann S ein A-Modul mit $A \cdot s = A/I \cdot s = S$, für alle $0 \neq s \in S$. Lemma 3.2 impliziert, dass S ein einfacher A-Modul ist.

b) Umgekehrt, sei S ein einfacher A-Modul. Dann ist $S = S_1 \oplus S_2$ nach Lemma 3.14 mit Untermoduln $S_1 := (1,0)S$ und $S_2 := (0,1)S$. Da S ein einfacher Modul ist, ist entweder $S_1 = 0$ und $S_2 = S$, oder aber es ist $S_2 = 0$ und $S_1 = S$. Ohne Einschränkung ist $S = S_1$. Dann gilt

$$\underbrace{(0, a_2)}_{\in I}\underbrace{(1,0)s}_{\in S = S_1} = (0,0) \cdot s = 0, \text{ für alle } s \in S.$$

Das Ideal $I \lhd A$ operiert also auf dem Modul S durch Null, nach Bemerkung 3.16 ist S damit ein A/I-Modul. Da S ein einfacher Modul ist, folgt

$$S \overset{3.2}{=} A \cdot s \overset{3.16}{=} A/I \cdot s, \text{ für alle } 0 \neq s \in S.$$

Nach Lemma 3.2 ist damit S ein einfacher A_1-Modul. □

Aufgabe 3.6. Sei $K = \mathbb{C}$ der Körper der komplexen Zahlen. Bestimmen Sie mit Inflation alle einfachen Moduln der Algebra $KC_2 \times KC_2$. Was folgt für die Algebren KV_4 und $KC_2 \times KC_2$? (Vergleichen Sie mit Aufgabe 1.19.)

Aufgabe 3.7. Sei A eine Algebra und I ein zweiseitiges Ideal in A. Zeigen Sie, ist I nilpotent, also $I^n = 0$ für ein $n \in \mathbb{N}$, dann entsprechen einfache A-Moduln gerade einfachen A/I-Moduln, mittels Inflation. Hierbei ist für $I, J \lhd A$ das Produkt

$$I \cdot J := \{\sum_{t=1}^{m} i_t j_t \mid m \in \mathbb{N}, i_t \in I, j_t \in J, 1 \leq t \leq m\} \lhd A.$$

3.2 Der Satz von Jordan Hölder

In diesem Abschnitt wollen wir die Struktur von Moduln genauer verstehen und beweisen den Satz von Jordan-Hölder für Moduln. Seine Aussage und Beweis sind sehr ähnlich zu Aussage und Beweis des Satzes von Jordan-Hölder in der Gruppentheorie. Sei K ein Körper und A eine Algebra über K.

Definition 3.18. Sei V ein A-Modul. Eine *Kompositionsreihe* von V ist eine endliche Kette von Untermoduln

$$0 = V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_n = V \text{ mit } V_i/V_{i-1} \text{ einfach, für } 1 \leq i \leq n. \tag{3.1}$$

Die *Länge* der Kompositionsreihe ist n. Die Moduln V_i/V_{i-1} heissen *Kompositionsfaktoren*. Statt $\subsetneq$ schreiben wir auch $<$, oder salopp $\subseteq$ oder $\leq$.

Nach Definition der Kompositionsreihe sind die in ihr vorkommenden Subquotienten V_i/V_{i-1} von V einfache Moduln. Nach Bemerkung 3.6 ist also insbesondere der Modul V_{n-1} ein maximaler Untermodul von V.

Beispiel 3.19. a) Sei V ein einfacher Modul. Dann ist $0 = V_0 \subsetneq V_1 = V$ eine Kompositionsreihe von V, denn $V_1/V_0 = V_1 = V$ ist einfach. Es ist die einzige mögliche Kompositionsreihe von V.

b) Falls $0 = V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_n = V$ eine Kompositionsreihe von V ist, so ist $0 = V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_t$ eine Kompositionsreihe von V_t, für alle $1 \leq t \leq n$. Wir sagen in diesem Fall, dass der Modul V_t eine Kompositionsreihe von V erbt.

c) Sei Q der Kroneckerköcher. Wir betrachten den Modul

$$M(\mu) := \begin{tikzcd} K \arrow[r, shift left, "1"] \arrow[r, shift right, "\mu"'] & K \end{tikzcd}. \tag{3.2}$$

Der Modul $M(\mu)$ ist nach Aufgabe 2.20 unzerlegbar, also keine direkte Summe von einfachen Moduln. Er enthält genau einen Untermodul, den einfachen Modul S_2, siehe Notation in Aufgabe 2.21, denn beide in dem folgenden ersten Diagramm enthaltenen untere Quadrate sind kommutativ, das zweite Diagramm ist hingegen nicht kommutativ, und damit S_1 kein Untermodul von $M(\mu)$:

$$\begin{tikzcd} K \arrow[r, shift left, "0"] \arrow[r, shift right, "0"'] & 0 \\ K \arrow[u, two heads, "1"] \arrow[r, shift left, "1"] \arrow[r, shift right, "\mu"'] & K \arrow[u, two heads, "0"'] \\ 0 \arrow[u, hook, "0"] \arrow[r, shift left, "0"] \arrow[r, shift right, "0"'] & K \arrow[u, hook, "1"'] \end{tikzcd} \quad \text{ist kommutativ, nicht aber} \quad \begin{tikzcd} K \arrow[r, shift left, "1"] \arrow[r, shift right, "\mu"'] & K. \\ K \arrow[u, "1"] \arrow[r, shift left, "1"] \arrow[r, shift right, "\mu"'] & 0 \arrow[u, "0"'] \end{tikzcd}$$

Beim Bilden der Quotientendarstellung $M(\mu)/S_2$ bilden wir im ersten Diagramm in der obersten Zeile die Quotientenvektorräume $K/0 = K$ und $K/K = 0$, jeweils Vektorraum modulo Untervektorraum; die Abbildungen in der ersten Zeile des ersten Diagramms sind die auf den Restklassen (durch die Abbildungen in der zweiten Zeile) induzierten Abbildungen. Wir erhalten, dass $M(\mu)/S_2 \simeq S_1$ einfach ist. Damit ist $0 \leq S_2 \leq M(\mu)$ eine Kompositionsreihe, die einzige Kompositionsreihe des Moduls $M(\mu)$. Die Kompositionsfaktoren in dieser Kompositionsreihe sind (von links nach rechts) S_2 und S_1, jeweils mit Vielfachheit Eins.

d) In Beispiel 3.8 haben wir für den Modul M eine direkte Summenzerlegung bewiesen, nämlich $M = U \oplus W'$. Hier haben wir die beiden Kompositionsreihen $0 \leq U \leq M$ und $0 \leq W' \leq M$. Dass die Subquotienten M/U beziehungsweise M/W' einfach sind, folgt aus dem Isomorphiesatz 2.26, beispielsweise

$$M/U \simeq (U \oplus W')/U \simeq W'/(U \cap W') \simeq W'/\{0\} \simeq W'.$$

Wir beobachten, dass ein Modul bisweilen nur eine Kompositionsreihe hat, aber genauso kann er auch sehr viele verschiedene Kompositionsreihen haben – siehe auch Beispiel 3.22 b). Ein Modul, der genau eine Kompositionsreihe hat, heisst *uniseriell* oder *einreihig*.

Proposition 3.20. *Sei A eine Algebra über dem Körper K. Jeder nicht-triviale endlich-dimensionale A-Modul besitzt eine Kompositionsreihe.*

Beweis. Sei $0 \neq V$ ein endlich-dimensionaler A-Modul. Wir machen Induktion nach der Dimension von V. Ist $\dim V = 1$, so ist V einfach und hat Kompositionsreihe $0 < V$. Dasselbe gilt, falls V einfach ist. Sei also V nicht einfach. Nach Definition 3.1 existiert ein echter, nicht-trivialer Untermodul U in V. Wähle einen solchen Untermodul U maximaler Dimension in V. Dann ist V/U einfach nach Bemerkung 3.6. Da $\dim U < \dim V$ ist, hat U nach Induktionsvoraussetzung eine Kompositionsreihe, etwa $0 \leq U_1 \leq \ldots \leq U_{t-1} = U$. Wähle $U_t = V$. Dann ist $0 \leq U_1 \leq \ldots \leq U_t = V$ eine Kompositionsreihe von V. □

Theorem 3.21 (Satz von Jordan-Hölder)**.** *Sei A eine Algebra und sei V ein endlich-dimensionaler A-Modul. Angenommen die folgenden beiden Ketten von Untermoduln sind Kompositionsreihen der Länge n beziehungsweise m:*

$$0 = V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_n = V, \tag{3.3}$$

$$0 = W_0 \subsetneq W_1 \subsetneq \ldots \subsetneq W_m = V. \tag{3.4}$$

Dann ist $n = m$, und es existiert eine Permutation $\sigma \in S_n$ mit

$$V_i/V_{i-1} \simeq W_{\sigma(i)}/W_{\sigma(i)-1}, \text{ für } 1 \leq i \leq n. \tag{3.5}$$

Die Kompositionsreihen (3.3) *und* (3.4) *heissen in diesem Fall äquivalent.*

Äquivalente Kompositionsreihen haben also, inklusive Vielfachheiten, dieselben Kompositionsfaktoren, bis auf Isomorphie und Reihenfolge. Bevor wir diesen Satz beweisen, machen wir zur Veranschaulichung zwei Beispiele.

Beispiel 3.22. a) In Beispiel 3.19 d) sind zwei Kompositionsreihen des Moduls M angegeben. Beide Kompositionsreihen haben Länge zwei und die Kompositionsfaktoren, in verschiedener Reihenfolge, sind die einfachen Moduln U und W'. Die Permutation ist hier $\sigma = (1, 2)$.

b) Sei $A = M_n(K)$ die Matrixalgebra über dem Körper K. Sei V der reguläre A-Modul, siehe Beispiel 2.15. Wir definieren für $1 \leq i \leq n$ die abelschen Gruppen

$$C_i = \{\sum_{j=1}^{n} \lambda_j E_{ji} \mid \lambda_j \in K, 1 \leq j \leq n\} = \begin{pmatrix} 0 & \ldots & 0 & K & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & K & 0 & \ldots & 0 \end{pmatrix} \subseteq A.$$

Es ist hierbei

$$\begin{pmatrix} * & \ldots & * \\ \vdots & \ddots & \vdots \\ * & \ldots & * \end{pmatrix} \cdot \begin{pmatrix} 0 & \ldots & 0 & * & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & * & 0 & \ldots & 0 \end{pmatrix} = \begin{pmatrix} 0 & \ldots & 0 & * & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & * & 0 & \ldots & 0 \end{pmatrix}.$$

Also ist C_i ein A-(Links-)Modul und wir erhalten die direkte Summenzerlegung $V = C_1 \oplus \ldots \oplus C_n$, als Modul. Hierbei ist $C_1 \simeq C_2 \simeq \ldots \simeq C_n \simeq K^n$, und dieser Modul ist nach Beispiel 3.4 einfach. Hiermit lassen sich nun viele Kompositionsreihen von V hinschreiben. Beispielsweise, definieren wir $V_i = C_1 \oplus \ldots \oplus C_i$ für $1 \leq i \leq n$, dann ist

$$0 =: V_0 \underset{C_1}{<} V_1 \underset{C_2}{<} \cdots \underset{C_{n-1}}{<} V_{n-1} \underset{C_n}{<} V_n = V$$

eine Kompositionsreihe von V. Hierbei notieren wir den Subquotienten V_i/V_{i-1} am zugehörigen Kleiner-Symbol $<$ als Subindex. Den Subquotienten berechnen wir wie in Beispiel 3.20 d) mit Hilfe des Isomorphiesatzes 2.26:

$$\begin{aligned} V_i/V_{i-1} &= ((C_1 \oplus \ldots \oplus C_{i-1}) \oplus C_i)/(C_1 \oplus \ldots \oplus C_{i-1}) \\ &\simeq C_i/((C_1 \oplus \ldots \oplus C_{i-1}) \cap C_i) \simeq C_i/\{0\} \simeq C_i. \end{aligned}$$

Definieren wir hingegen $W_i = C_n \oplus \ldots \oplus C_{n-i+1}$, für $1 \leq i \leq n$, so ist auch

$$0 = W_0 \underset{C_n}{\leq} W_1 \underset{C_{n-1}}{\leq} \cdots \underset{C_2}{\leq} W_{n-1} \underset{C_1}{\leq} W_n = V$$

eine Kompositionsreihe von V. Die beiden Kompositionsreihen haben dieselbe Anzahl von Kompositionsfaktoren, und die Kompositionsfaktoren sind bis auf Isomorphie und Reihenfolge gleich. Es handelt sich also um zwei äquivalente Kompositionsreihen – wie der Satz von Jordan Hölder 3.21 behauptet. Die Permutation σ hinzuschreiben macht in diesem Beispiel nicht viel Sinn, da alle Kompositionsfaktoren isomorph sind zum einfachen Modul K^n.

Aufgabe 3.8. Sei A eine Algebra. Bestimmen Sie alle Kompositionsreihen der folgenden A-Moduln V:

a) $V = K \oplus K$ als K-Modul;

b) V der reguläre Modul der Algebra $A = T_2(K)$ der oberen Dreiecksmatrizen;

c) V der reguläre Modul der Kroneckeralgebra;

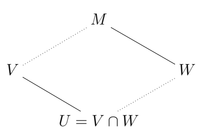
d) $V = K[X]/(X^n)$ als $K[X]$-Modul.

Für den Beweis des Satzes von Jordan-Hölder 3.21 benötigen wir das folgende Resultat, welches bisweilen als Schmetterlingslemma bezeichnet wird.

Lemma 3.23. *Sei M ein A-Modul und seien V und W maximale Untermoduln von M mit $V \neq W$. Sei $U := V \cap W$. Dann ist*

$$M/V \simeq W/U \text{ und } M/W \simeq V/U.$$

Es lohnt sich, sich dieses Lemma grafisch zu merken: Jeweils in der Grafik gegenüberliegende Quotientenmoduln sind isomorph zueinander.



Beweis. Wir zeigen, dass $V + W = M$ ist. Angenommen das gilt, dann folgt aus Theorem 2.26:

$$\begin{aligned} M/W &= (V+W)/W \simeq V/(V \cap W) = V/U, \\ M/V &= (V+W)/V \simeq W/(V \cap W) = W/U. \end{aligned}$$

Nach Voraussetzung ist $W \subseteq V + W \subseteq M$. Angenommen $V + W \neq M$. Da W maximal in M ist, folgt dann $W = V + W$, und wir erhalten $V \subseteq V + W = W \subsetneq M$. Da aber V maximal in M ist, erhalten wir $V = W$, ein Widerspruch zur Voraussetzung. Also ist $V + W = M$. □

Beweis des Satzes von Jordan-Hölder. Gegeben ist ein endlich-dimensionaler A-Modul V. Nach Proposition 3.20 hat V eine Kompositionsreihe. Wir machen Induktion nach der minimalen Länge n der Kompositionsreihe von V. Für den Induktionsanfang sei $n = 1$. Dann hat der Modul V eine Kompositionsreihe $0 = V_0 \subsetneq V_1 = V$ der Länge Eins. Nach Definition 3.18 ist V also ein einfacher Modul, und damit hat jede Kompositionsreihe von V die Länge eins. Damit ist der Induktionsanfang bewiesen. Die Induktionsbehauptung ist: Wenn V eine Kompositionreihe der Länge n hat, dann hat jede Kompositionsreihe von V die Länge n und alle diese Kompositionsreihen sind äquivalent.

Sei nun die minimale Länge $n > 1$. Gegeben seien die beiden Kompositionsreihen

$$0 = V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_n = V, \tag{3.6}$$

$$0 = W_0 \subsetneq W_1 \subsetneq \ldots \subsetneq W_m = V. \tag{3.7}$$

mit $n \leq m$. Wir wollen zeigen, dass die Kompositionsreihen (3.6) und (3.7) äquivalent sind. Im Induktionsschritt unterscheiden wir zwei Fälle:

a) Im ersten (und einfacheren) Fall nehmen wir an, dass $V_{n-1} = W_{m-1} =: U$ ist. Dann ist nach Beispiel 3.19 b)

$$0 = V_0 \subsetneq V_1 \subsetneq \ldots \subsetneq V_{n-1} = U \tag{3.8}$$

eine Kompositionsreihe von U der Länge $n - 1$. Wegen $n - 1 < n$ haben nach Induktionsannahme alle Kompositionsreihen von U die Länge $n - 1$. Da nach Beispiel 3.19 b) auch

$$0 = W_0 \subsetneq W_1 \subsetneq \ldots \subsetneq W_{m-1} = U \tag{3.9}$$

eine Kompositionsreihe von U ist, folgt $n-1 = m-1$, beziehungsweise $m = n$. Ebenfalls nach Induktionsannahme folgt, dass es eine Permutation $\sigma \in S_{n-1}$ gibt, so dass gilt:

$$V_i/V_{i-1} \simeq W_{\sigma(i)}/W_{\sigma(i)-1}, \text{ für } 1 \leq i \leq n-1.$$

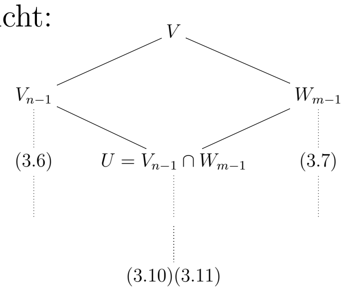
Da $V_{n-1} = W_{m-1}$ ist, folgt auch $V_n/V_{n-1} = W_n/W_{n-1}$. Es gibt also eine Permutation $\sigma \in S_n$, so dass (3.5) gilt.

b) Im zweiten Fall nehmen wir an, dass $V_{n-1} \neq W_{m-1}$ ist. Wir betrachten den Schnitt $U := V_{n-1} \cap W_{m-1}$. Modul U besitzt nach Proposition 3.20 eine Kompositionsreihe, etwa $0 = U_0 \subsetneq U_1 \subsetneq \ldots \subsetneq U_t = U$. Wir wollen zeigen, dass (3.6) und (3.7) äquivalente Kompositionsreihen sind. Hierzu benötigen wir drei Schritte:

i) Äquivalenz von Kompositionsreihen ist eine Äquivalenzrelation. Wir vergleichen die Kompositionsreihen (3.6) und (3.7), indem wir zwei weitere Kompositionsreihen dazwischen schieben: Betrachte die beiden Ketten von Untermoduln

$$0 = U_0 \subsetneq U_1 \subsetneq \ldots \subsetneq U_t = U \subsetneq V_{n-1} \subsetneq V_n = V, \qquad (3.10)$$
$$0 = U_0 \subsetneq U_1 \subsetneq \ldots \subsetneq U_t = U \subsetneq W_{m-1} \subsetneq W_m = V. \qquad (3.11)$$

Bildlich veranschaulicht:



Wir zeigen als erstes, dass (3.10) und (3.11) Kompositionsreihen sind, und dass diese äquivalent sind. Die beiden Ketten von Untermoduln stimmen, von links gelesen, in den ersten t Subquotienten U_i/U_{i-1} mit $1 \leq i \leq t$ überein, und all diese Subquotienten sind einfache Moduln, da sie Kompositionsfaktoren aus der Kompositionsreihe von U sind. Auch jeweils die ersten Subquotienten von rechts gelesen, also V/W_{m-1} und V/V_{n-1}, sind einfache Moduln, da sie als Kompositionsfaktoren in den Kompositionsreihen (3.6) und (3.7) vorkommen. Aus Definition 3.18 folgt, dass die beiden Moduln V_{n-1} und W_{m-1} in den Kompositionsreihen (3.6) und (3.8) maximale Untermoduln von V sind. Auf diese maximalen Untermoduln von V wenden wir Lemma 3.23 an und erhalten:

$$V_{n-1}/U \overset{3.23}{\simeq} V/W_{m-1} \text{ sowie } W_{m-1}/U \overset{3.23}{\simeq} V/V_{n-1},$$

und beide Quotienten sind einfache Moduln. Also sind die Untermodulketten (3.10) und (3.11) Kompositionsreihen, und sie haben die gleichen Kompositionsfaktoren, sind also äquivalent.

ii) Wir zeigen als nächstes, dass $n = m$ ist. Nach unserem Setup gilt $n \leq m$. Modul V_{n-1} erbt eine Kompositionsreihe aus (3.6), besitzt also eine Kompositionsreihe der Länge $n - 1$. Die Induktionsannahme besagt damit, dass jede Kompositionsreihe von V_{n-1} die Länge $n-1$ hat. Modul V_{n-1} erbt auch eine Kompositionsreihe aus (3.10). Diese hat Länge $t+1$. Also folgt, dass $n-1 = t+1$ ist. Modul W_{m-1} erbt eine Kompositionsreihe (3.11) über U. Diese hat also Länge $t + 1 = n - 1 < n$. Damit hat nach Induktionsvoraussetzung jede Kompositionsreihe von W_{m-1} die Länge $n - 1$, insbesondere auch die Kompositionsreihe (3.7) von W_{m-1}. Nach Konstruktion ist diese aber von Länge $m - 1$. Also ist $m - 1 = n - 1$, beziehungsweise $m = n$.

iii) Wir zeigen, dass die Kompositionsreihen (3.6) und (3.7) äquivalent sind. Hierzu vergleichen wir die Kompositionsreihen (3.6) und (3.10) des

Moduls V_{n-1}. Diese haben Länge $n-1$. Nach Induktionsvoraussetzung existiert eine Permutation $\sigma \in S_{n-1}$ mit

$$\begin{aligned} U_i/U_{i-1} &\simeq V_{\sigma(i)}/V_{\sigma(i)-1}, \text{ für } 1 \leq i \leq n-2, \\ V_{n-1}/U_t &\simeq V_{\sigma(n-1)}/V_{\sigma(n-1)-1}. \end{aligned}$$

Wir betrachten $\sigma \in S_{n-1} \subset S_n$. Dann folgt, dass (3.6) und (3.10) äquivalente Kompositionsreihen von V sind. Analog sieht man, dass (3.7) und (3.11) äquivalente Kompositionsreihen sind. Da Äquivalenz von Kompositionsreihen eine Äquivalenzrelation ist, folgt, dass die Kompositionsreihen (3.6) und (3.7) äquivalente Kompositionsreihen von V sind: (3.6) ist äquivalent zu (3.10), was wiederum äquivalent ist zu (3.11), was wiederum äquivalent zu (3.7) ist. □

Bemerkung 3.24. Kompositionsreihen lassen sich ganz analog für Moduln über beliebigen Ringen definieren. Zu diskutieren bleibt noch, warum wir in Definition 3.18 nur *endliche* Ketten und Untermoduln zulassen. Für natürliche Zahlen n ist $2^n\mathbb{Z}$ eine abelsche Gruppe, also ein $\mathbb{Z}$-Modul. Für den $\mathbb{Z}$-Modul $\mathbb{Z}$ haben wir die unendliche Kette von Untermoduln:

$$\ldots \subsetneq 16\mathbb{Z} \subsetneq 8\mathbb{Z} \subsetneq 4\mathbb{Z} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}, \tag{3.12}$$

wobei die Subquotienten $2^{n-1}\mathbb{Z}/2^n\mathbb{Z} = \{0 + 2^n\mathbb{Z}, 2^{n-1} + 2^n\mathbb{Z}\}$ jeweils isomorph zum einfachen $\mathbb{Z}$-Modul $\mathbb{Z}/2\mathbb{Z}$ sind, siehe Beispiel 3.3. Und genauso haben wir natürlich die unendliche Kette von Untermoduln

$$\ldots \subsetneq 81\mathbb{Z} \subsetneq 27\mathbb{Z} \subsetneq 9\mathbb{Z} \subsetneq 3\mathbb{Z} \subsetneq \mathbb{Z}, \tag{3.13}$$

mit Subquotienten $3^{n-1}\mathbb{Z}/3^n\mathbb{Z} = \{0 + 3^n\mathbb{Z}, 3^{n-1} + 3^n\mathbb{Z}, 2 \cdot 3^{n-1} + 3^n\mathbb{Z}\}$ jeweils isomorph zum einfachen $\mathbb{Z}$-Modul $\mathbb{Z}/3\mathbb{Z}$. Der Satz von Jordan-Hölder gilt also für den Modul ${}_{\mathbb{Z}}\mathbb{Z}$ nicht. Um strukturelle Resultate wie den Satz von Jordan-Hölder zu haben, ist es also sinnvoll, sich in Definition 3.18 auf *endliche* Ketten von Untermoduln zu beschränken.

Beispiel 3.25. Sei Q ein Köcher, sodass die Wegealgebra KQ endlich-dimensional ist mit Knotenmenge $Q_0 = \{1, \ldots, n\}$. Das sagt nichts anderes, als dass der Köcher Q keine Schleifen und Zykel hat. Für $i \in Q_0$ definieren wir die Darstellung S_i durch

$$S_i(j) = \begin{cases} K & \text{für } j = i, \\ 0 & \text{sonst.} \end{cases}$$

Die Darstellungen $S_1, \ldots, S_n$ sind eindimensional, also irreduzibel, und sie sind paarweise nicht-isomorph, denn $\mathrm{Hom}_{KQ}(S(i), S(j)) = 0$ für $i \neq j$. Wir wollen die Kompositionsfaktoren eines beliebigen KQ-Moduls bestimmen:

a) Sei $M \neq 0$ eine beliebige Darstellung von KQ. Definiere

$$\mathrm{Supp}(M) = \{i \in Q_0 \mid M(i) \neq 0\}.$$

Da nach Voraussetzung KQ endlich-dimensional ist, besitzt Q keine zyklischen Wege. Es gibt deshalb einen Index $i \in \mathrm{Supp(M)}$, von dem es keinen Pfeil von

Knoten i zu einem Knoten $j \in \operatorname{Supp}(M)$ gibt – andernfalls hätten wir eine Schleife konstruiert. Dann ist die Darstellung S_i eine Unterdarstellung von M. Insbesondere ist also M nicht einfach. Damit folgt, dass

$$\mathcal{R} := \{S_1, \ldots, S_n\}$$

ein Repräsentantensystem der einfachen KQ-Moduln bildet, sie also bis auf Isomorphie klassifiziert. Siehe Aufgabe 2.21.

b) Iterieren wir das letzte Argument aus a), so konstruieren wir eine Kompositionsreihe von M beziehungsweise bestimmen die Kompositionsfaktoren von M: Angenommen der in a) gefundene Modul M/S_i ist nicht einfach. Dann existiert ein Index $j \in Q_0$, so dass $S_j \leq M/S_i$ Untermodul ist. Und so weiter. Da $0 \neq M$ endlich-dimensional ist, endet dieser Prozess. Mit Hilfe der Untermodulkorrespondenz 2.27 folgt: Modul M besitzt eine Kompositionsreihe mit Kompositionsfaktoren aus der Menge $\mathcal{R}$, wobei der Modul S_t genau $\dim M(t)$ mal als Kompositionsfaktor in der Kompositionsreihe von M vorkommt. Nach dem Satz von Jordan-Hölder 3.21 sind diese Vielfachheiten eindeutig bestimmt.

Wir fassen das letzte Beispiel zusammen

Korollar 3.26. *Sei Q ein Köcher mit Knotenmenge $Q_0 = \{1, \ldots, n\}$ und so, dass die Wegealgebra KQ endlich-dimensional ist.*

a) Die Menge $\mathcal{R} := \{S_1, \ldots, S_n\}$, definiert in Beispiel 3.25, bildet ein Repräsentantensystem der einfachen KQ-Moduln.

b) Ist M ein KQ-Modul, so gibt der Dimensionsvektor $\underline{\dim} M = (\dim M(t))_{t \in Q_0}$ an, mit welcher Vielfachheit die einfachen Moduln $(S_t)_{t \in Q_0}$ jeweils als Kompositionsfaktoren im Modul M vorkommen.

Aufgabe 3.9. Sei A eine Algebra über einem Körper K, und sei V ein A-Modul mit zwei Kompositionsreihen $0 < U < V$ und $0 < W < V$, für $U \neq W$.

a) Zeigen Sie, dass $V = U \oplus W$ ist.

b) Angenommen $U \simeq W$. Sei $\psi : U \to W$ ein A-Modulisomorphismus. Wir definieren für $\lambda \in K$ die Menge $U_\lambda = \{u + \lambda\psi(u) \mid u \in U\}$. Zeigen Sie, dass U_λ ein Untermodul von V ist, und dass dieser isomorph zu U ist.

c) Folgern Sie, dass der Modul V unendlich viele Kompositionsreihen hat, falls der Körper K unendlich viele Elemente besitzt.

Aufgabe 3.10. Sei $A = K[X]$ und $V_\alpha = (V, \alpha)$ ein $K[X]$-Modul, das heisst, V ist ein K-Vektorraum und $\alpha : V \to V$ eine lineare Abbildung. Sei α eine nilpotente Abbildung, das heisst $\alpha^n = 0$ für eine natürliche Zahl n. Zeigen Sie, dass V_α uniseriell ist genau dann, wenn der Rang der Abbildung α gerade $\dim V - 1$ ist.

3.3 Konstruktion aller einfachen A-Moduln

Sei K ein Körper. Sei A eine endlich-dimensionale Algebra über dem Körper K. Wir haben diverse Beispiele von einfachen A-Moduln gesehen und dabei gelernt, dass es nicht trivial ist, zu einer gegebenen Algebra A die einfachen Moduln bis auf Isomorphie hinzuschreiben. In diesem Abschnitt wollen wir den folgenden Fragen nachgehen: Wieviele einfache A-Moduln bis auf Isomorphie gibt es? Können wir einfache A-Moduln bis auf Isomorphie klassifizieren? Können wir alle einfachen A-Moduln bis auf Isomorphie konstruieren? Für Wegealgebren haben wir diese Fragen bereits beantwortet, siehe Korollar 3.26. Wie üblich sind unsere Moduln endlich-dimensional, damit sie entsprechend Proposition 3.20 eine Kompositionsreihe besitzen. Wir benötigen zunächst zwei Hilfsresultate.

Lemma 3.27. *Sei V ein A-Modul und $N \leq V$ ein Untermodul. Dann existiert eine Kompositionsreihe von V, in welcher N als Untermodul vorkommt.*

Beweis. Nach Proposition 3.20 besitzt N eine Kompositionsreihe, etwa

$$0 = N_0 < N_1 < \ldots < N_t = N. \tag{3.14}$$

Auch der Modul V/N besitzt nach Proposition 3.20 eine Kompositionsreihe, etwa

$$0 = X_0 < X_1 < \ldots < X_s = V/N.$$

Nach der Untermodulkorrespondenz 2.27 existieren Moduln $N \subseteq U_i \subseteq V$ mit $X_i = U_i/N$, mit $0 \leq i \leq s$, das heisst,

$$0 = N/N = U_0/N < U_1/N < \ldots < U_s/N = V/N \tag{3.15}$$

ist eine Kompositionsreihe von V/N. Hierbei ist $U_i/N \subset U_{i+1}/N$ genau dann, wenn $U_i \subset U_{i+1}$ ist. Wir zeigen, dass die Kette von Untermoduln

$$0 = N_0 < N_1 < \ldots < N_t = N = U_0 < U_1 < \ldots < U_s = V \tag{3.16}$$

eine Kompositionsreihe von V ist. Hierzu müssen wir nach Definition 3.18 prüfen, dass alle in ihr vorkommenden Subquotienten N_i/N_{i-1} bzw. U_i/U_{i-1} einfache Moduln sind. Die Subquotienten N_i/N_{i-1} sind einfach, da sie Kompositionsfaktoren in der Kompositionsreihe (3.14) sind. Nach dem Isomorphiesatz 2.26 ist

$$U_i/U_{i-1} \simeq (U_i/N)/(U_{i-1}/N)$$

und dieser Modul ist einfach, da er als Kompositionsfaktor in der Kompositionsreihe (3.15) auftritt. Damit folgt, dass (3.16) eine Kompositionsreihe von V ist, in der N als Untermodul vorkommt. □

Definition 3.28. Sei M ein A-Modul und $m \in M$. Wir definieren die Annulatoren

$$\begin{aligned} \mathrm{Ann}_A(m) &:= \{a \in A \mid am = 0\} \trianglelefteq_l A \text{ (Linksideal)}, \\ \mathrm{Ann}_A(M) &:= \{a \in A \mid am = 0 \text{ für alle } m \in M\} \trianglelefteq_2 A \text{ (zweiseitiges Ideal)}, \end{aligned}$$

Lemma 3.29. *Sei M ein A-Modul und $m \in M$. Der Annulator $Ann_A(m)$ ist ein Linksideal in A. Ist S ein einfacher A-Modul und $0 \neq s \in S$, dann ist $Ann(s) \triangleleft_l A$ maximales Linksideal.*

Beweis.

a) Man sieht leicht, dass die Menge $\mathrm{Ann}(m)$ eine abelsche Gruppe ist. Darüber hinaus gilt für $b \in A$ und $a \in \mathrm{Ann}(m)$, dass $b \cdot (a \cdot m) \overset{3.28}{=} b \cdot 0 = 0$ ist, also ist $\mathrm{Ann}(m)$ ein Linksideal in A.

b) Sei S ein einfacher A-Modul und $0 \neq s \in S$. Dann ist $\psi : {}_AA \to {}_AS$, mit $a \mapsto as$ ein A-Modulhomomorphismus, siehe Beispiel 2.25. Es ist $\psi(1) = 1 \cdot s = s \neq 0$, also ist $\psi \neq 0$. Mit Bemerkung 3.2 und da S einfach ist, folgt dass $0 \neq A \cdot s = S$ ist. Damit ist ψ surjektiv mit

$$\ker \psi = \{a \in A \mid a \cdot s = 0\} = \mathrm{Ann}(s).$$

Nach dem Homomorphiesatz 2.26 folgt, dass $A/\mathrm{Ann}(s) \simeq S$ einfach ist. Die Untermodulkorrespondenz 2.27 beziehungsweise Bemerkung 3.6 impliziert, dass $\mathrm{Ann}(s) \leq {}_AA$ ein maximaler Untermodul ist. Nach Beispiel 2.19 entsprechen Links-Untermoduln genau den Linksidealen der Algebra A. Also ist $\mathrm{Ann}(s)$ in A ein maximales Linksideal. □

Aufgabe 3.11. Sei A eine Algebra und $I \trianglelefteq_2 A$ Ideal. Sei M ein A-Modul.

a) Zeigen Sie, dass $\mathrm{Ann}_A(M) \triangleleft_2 A$ ist mit $\mathrm{Ann}_A(M) = \bigcap_{m \in M} \mathrm{Ann}_A(m)$.

b) Zeigen Sie: Ist $M \simeq N$ als A-Modul, so ist $\mathrm{Ann}(N) = \mathrm{Ann}(M)$.

c) Bestimmen Sie $\mathrm{Ann}_{M_n(K)}(K^n)$ und $\mathrm{Ann}_A(A/I)$. Benötigen Sie hier, dass I ein zweiseitiges Ideal ist, oder genügt es, dass I ein Linksideal ist?

Theorem 3.30. *Sei A eine endlich-dimensionale Algebra über dem Körper K.*

a) Jeder einfache A-Modul kommt bis auf Isomorphie als Kompositionsfaktor des regulären Moduls ${}_AA$ vor.

b) Es existieren bis auf Isomorphie nur endlich viele einfache A-Moduln.

Beweis. Sei S ein einfacher A-Modul. Nach dem Beweis zu Lemma 3.29 gilt für $0 \neq s \in S$, dass $A/\mathrm{Ann}(s) \simeq S$ ist, also $\mathrm{Ann}(s)$ ein maximaler Untermodul in ${}_AA$ ist. Nach Lemma 3.27 existiert eine Kompositionsreihe des regulären Moduls ${}_AA$, in dem der Untermodul $\mathrm{Ann}(s)$ vorkommt, etwa

$$0 = I_0 < I_1 < \ldots < I_t := \mathrm{Ann}(s) \overset{3.29}{<} {}_AA.$$

Damit ist S ein Kompositionsfaktor von ${}_AA$. Da der reguläre Modul ${}_AA$ endlich-dimensional ist, hat er nach dem Satz von Jordan-Hölder bis auf Isomorphie nur endlich viele verschiedene Kompositionsfaktoren. Jeder einfache Modul kommt bis auf Isomorphie als einer dieser endlich vielen Kompositionsfaktoren des regulären Moduls vor. Also gibt es bis auf Isomorphie nur endliche viele einfache A-Moduln.
□

Beispiel 3.31. Wir klassifizieren die einfachen Moduln von einigen uns bekannten Algebren:

a) Sei $A = M_n(K)$ die Matrixalgebra über dem Körper K. Nach Beispiel 3.22 b) hat der reguläre Modul ${}_AA$ genau einen Kompositionsfaktor, bis auf Isomorphie. Dies ist der Modul $S := K^n$, wobei die Algebra A auf S durch Matrixmultiplikation operiert. Die Algebra $A = M_n(K)$ hat also bis auf Isomorphie genau einen einfachen A-Modul.

b) Seien $n_1, \ldots, n_t$ natürliche Zahlen und sei $A = M_{n_1}(K) \times \ldots \times M_{n_t}(K)$ das direkte Produkt von Matrixalgebren. Die einfachen A-Moduln sind – bis auf Isomorphie – nach 3.17 genau die Inflationen der einfachen $M_{n_i}(K)$-Moduln, für $1 \leq i \leq t$. Damit hat die Algebra A nach a) genau t paarweise nicht-isomorphe einfache A-Moduln: Sei $S_i = K^{n_i}$ der einfache Modul der Algebra $M_{n_i}(K)$. Dann ist S_i ein einfacher A-Modul, wobei der $i$te Faktor von A auf S_i durch Matrixmultiplikation operiert, und der j-te Faktor für $j \neq i$ operiert durch Null.

c) Die Algebra $B = T_n(K)$ der oberen Dreiecksmatrizen ist nach Beispiel 1.30 isomorph zu einer Wegealgebra mit n Punkten. Nach Beispiel 3.25 beziehungsweise Aufgabe 2.21 hat die Algebra B bis auf Isomorphie damit n verschiedene einfache B-Moduln. Diese sind alle eindimensional.

Aufgabe 3.12. Sei Q ein Köcher, so dass die Wegealgebra KQ endlich-dimensional ist. Wir definieren die Menge $(KQ)_{\geq 1}$ als den K-Vektorraum mit Basis alle Wege positiver Länge.

a) Zeigen Sie, dass $(KQ)_{\geq 1}$ ein nilpotentes zweiseitiges Ideal in KQ ist. Klassifizieren Sie die einfachen Moduln der Algebra $KQ/(KQ)_{\geq 1}$.

b) Sei $A = T_n(K)$ die Algebra der oberen Dreiecksmatrizen. Erklären Sie mit Hilfe von a), wie eine obere Dreiecksmatrix B auf den verschiedenen eindimensionalen einfachen A-Moduln operiert.

Theoretisch können wir also alle einfachen Moduln einer gegebenen Algebra konstruieren, indem wir die Kompositionsfaktoren des regulären Moduls bestimmen. In der Praxis hat der reguläre Modul eine grosse Dimension. Selbst mit Hilfe von Computern lassen sich solche Rechnungen bei Moduln grosser Dimension nicht durchführen: Für die Gruppenalgebra KS_n der symmetrischen Gruppe kennt man eine Parametrisierung ihrer einfachen Moduln – durch Partitionen von n beziehungsweise p-reguläre Partitionen von n; aber über einem Körper K von Primcharakteristik $p \leq n$ kennt man nicht einmal die Dimensionen der einfachen KS_n-Moduln. Hier sind schwere offene Fragen, auf die die Darstellungstheorie bisher keine Antworten gefunden hat.

Kapitel 4

Halbeinfache Algebren

Sei A eine Algebra über einem Körper K. Moduln in diesem Kapitel sind wie üblich endlich-dimensional. In diesem Kapitel geht es um die Klasse der *halbeinfachen* Algebren. Diese Algebren haben eine vergleichsweise einfache Darstellungstheorie: jeder Modul über einer halbeinfachen Algebra ist eine endliche direkte Summe einfacher Moduln. Solche Moduln werden als *halbeinfach* bezeichnet. Im ersten Abschnitt befassen wir uns mit diesen halbeinfachen Moduln. Ab dem zweiten Abschnitt geht es dann um die halbeinfachen Algebren.

4.1 Halbeinfache Moduln

In diesem Abschnitt geben wir verschiedene Charakterisierungen an, mit denen man entscheiden kann, ob ein Modul halbeinfach ist. Hier erst einmal die Definition:

Definition 4.1. Ein A-Modul $0 \neq V$ heisst *halbeinfach* genau dann, wenn für jeden Untermodul $W \leq V$ ein Untermodul $W' \leq V$ existiert mit $V = W \oplus W'$. Der Modul W' heisst hierbei ein *Komplement* zum Untermodul W in V.

Ob der Nullmodul als halbeinfacher Modul zugelassen wird, ist wieder einmal ein bisschen Geschmackssache. Später wollen wir beispielsweise sagen, jeder halbeinfache Modul ist die direkte Summe einfacher Moduln. Lassen wir den Nullmodul als halbeinfachen Modul zu, so müssen wir an dieser Stelle auch leere direkte Summen zulassen, da der Nullmodul – wiederum in Hinblick auf geltende Sätze – sinnvollerweise kein einfacher Modul ist. Aus solchen Gründen ist es sinnvoll, auch bei Halbeinfachheit von Moduln den Nullmodul auszuschliessen. Alternativ kann man bei späteren Sätzen voraussetzen, dass die Aussage nicht für den Nullmodul gilt.

Beispiel 4.2.

a) Ein einfacher Modul hat nach Definition 3.1 keine echten, nichttrivialen Untermoduln. Entsprechend hat jeder Untermodul eines einfachen Moduls V ein Komplement: Der Nullmodul hat das Komplement V; der Modul V hat als Komplement den Nullmodul. Also ist jeder einfache Modul halbeinfach.

b) Dass es Moduln gibt, die nicht halbeinfach sind, kennen wir bereits indirekt aus den letzten Kapiteln. Hier ein Beispiel dazu: Der reguläre Modul $V := \mathbb{Z}_2 C_2$

ist nicht halbeinfach. Um dies zu beweisen, müssen wir einen Untermodul dieses zwei-dimensionalen Moduls angeben, der kein Komplement im regulären Modul hat. Ein solcher Untermodul kann nur ein eindimensionaler Untermodul sein. Sei $G := C_2 = \langle x \mid x^2 = 1 \rangle = \{1, x\}$. Nach Aufgabe 2.14 ist der triviale Modul W ein Untermodul des regulären Moduls V; er wird erzeugt durch $v = 1 + x$, die Summe der Gruppenelemente aus C_2:

$$W := K\text{-Span}\{1 + x\} = \{0, 1 + x\} \leq V := K\text{-Span}\{1, x\} = \{0, 1, x, 1 + x\}.$$

Der Einfachheit halber arbeiten wir in diesem Beispiel mit einem endlichen Körper. Dadurch dass $K = \mathbb{Z}_2$ nur zwei Elemente hat, haben auch endlichdimensionale Vektorräume U über diesem Körper nur endlich viele Elemente: $|U| = |K|^{\dim U}$. Der Modul V in diesem Beispiel hat also nur $2^2 = 4$ Elemente. Es ist damit sehr einfach zu überprüfen, welche Untermoduln in V existieren. Diese erhalten wir, indem wir die Erzeugnisse einzelner Elemente $v \in V$ anschauen, also $A \cdot v = \{av \mid a \in A\}$ mit $A = KG$, und beispielsweise den Satz von Lagrange als Einschränkung an die Elementanzahl nutzen:

$$\begin{array}{rcl} KG \cdot 0 &=& 0, \\ KG \cdot 1 &=& KG, \\ KG \cdot x &\ni& x \cdot x = 1, \text{ also ist } KG \cdot x = KG, \\ KG \cdot (1 + x) &=& \{0, 1 + x\} = W. \end{array}$$

Erzeugnisse von mehr als einem Element ergeben in diesem Beispiel keine neuen Untermoduln von V. Der Modul W ist nach dieser Rechnung der einzige eindimensionale Untermodul von V. Ein Komplement von W in V müsste ein anderer eindimensionaler Untermodul sein. Da ein solcher nicht existiert, hat der Untermodul $W \leq V$ kein Komplement in V.

Aufgabe 4.1. Welche der folgenden Moduln sind halbeinfach? Begründen Sie jeweils Ihre Antwort.

a) Sei $K = \mathbb{Z}_3$ Körper mit drei Elementen. Ist der reguläre Modul $U := KC_2$ ein halbeinfacher Modul?

b) Sei $K = \mathbb{Z}_2$ der Körper mit zwei Elementen. Ist der KS_4-Modul V aus Aufgabe 3.3 ein halbeinfacher Modul?

Noch aus Vorsicht eine Anmerkung: Im gemachten Argument in Beispiel 4.2 zur Nicht-Halbeinfachheit des gegebenen Moduls betrachten wir nur Erzeugnisse eines einzigen Elementes. Dies liegt daran, dass das gesuchte Komplement eindimensional sein muss. Im Allgemeinen muss ein Komplement kein einfacher Modul sein, es muss auch nicht von einem Element erzeugt werden. Wollen wir eine Prüfung von Halbeinfachheit für einen Modul grösserer Dimension durchführen, so müssen wir bei der Suche nach Untermoduln auch Erzeugnisse von mehreren Elementen zulassen. Dies deutet natürlich an, dass der Nachweis von Halbeinfachheit durch Berechnung aller Untermoduln nur sehr beschränkt tauglich ist. Wir brauchen bessere Instrumente, um eine solche Frage anzugehen. In diesem Abschnitt entwickeln wir daher äquivalente Kriterien zu Definition 4.1.

Definition 4.3. Sei V ein A-Modul. Wir definieren das *Radikal* $\operatorname{rad}(V)$ und den *Sockel* $\operatorname{soc}(V)$ durch

$$\operatorname{rad}(V) := \bigcap_{W \leq V \text{maximal}} W, \quad \operatorname{soc}(V) := \sum_{W \leq V, W \text{ einfach}} W.$$

Klammern darf man hier auch weglassen: wir schreiben auch $\operatorname{rad} V$ und $\operatorname{soc} V$. Der Schnitt und die Summe von Untermoduln sind nach 2.20 wieder Untermoduln. Also bilden Sockel und Radikal eines Moduls V jeweils einen Untermodul von V. Wir sehen im Verlauf dieses Abschnittes, dass $\operatorname{soc}(V)$ und $V/\operatorname{rad}(V)$ halbeinfache Moduln sind, genauer handelt es sich um den grössten halbeinfachen Teilmodul und den grössten halbeinfachen Quotientenmodul von V.

Aufgabe 4.2. Bestimmen Sie jeweils den Untermodulverband, Sockel und Radikal der Moduln $U = \mathbb{Z}_3 C_2$ und V aus Aufgabe 4.1.

Der in der letzten Aufgabe erwähnte *Untermodulverband* eines Moduls W ist hierbei eine graphische Veranschaulichung der Menge aller Untermoduln $W' < W$ und der Inklusion zwischen Untermoduln in Form eines *Hasse Diagramms*: Der grösste Modul W steht ganz oben, der kleinste 0 ganz unten. Man zeichnet einen Strich zwischen den Untermoduln W' und W'', falls W' maximaler Untermodul in W'' ist. Hierbei steht der grössere Modul W'' oberhalb von W'. Die Ordnungsrelation „grösser“ ist hier durch Mengeninklusion gegeben.

Lemma 4.4. *Sei $W \leq V$ Untermodul. Sei weiterhin $U \leq V$ ein maximaler Untermodul von V. Dann ist entweder $U \cap W = W$ oder $U \cap W < W$ ist ein maximaler Untermodul von W. Insbesondere folgt, dass $\operatorname{rad}(W) \leq \operatorname{rad}(V)$ ist.*

Beweis.

a) Wir betrachten den Schnitt $U \cap W$ für maximale Untermoduln $U \leq V$ und unterscheiden zwei Fälle:

   i) Sei $U \cap W = W$. In diesem Fall ist $W \subseteq U$ und damit $\operatorname{rad}(W) \overset{4.3}{\subseteq} W \subseteq U$.

   ii) Sei $U \cap W \neq W$. Dann ist $W \not\subseteq U$. Also ist $U \subsetneq W + U \subseteq V$. Da U ein maximaler Untermodul von V ist, folgt $W + U = V$. Mit dem Isomorphiesatz 2.24 erhalten wir:

   $$W/(U \cap W) \simeq (U + W)/U = V/U,$$

   und nach Bemerkung 3.6 ist der Modul V/U einfach. Damit ist auch $W/(U \cap W)$ einfach, also nach Bemerkung 3.6 ist $U \cap W$ ein maximaler Untermodul von W. Damit gilt auch in diesem Fall $\operatorname{rad}(W) \overset{4.3}{\subseteq} U \cap W \subseteq U$. Wir benutzen hier, dass der Schnitt über alle maximalen Untermoduln von W enthalten ist in einem dieser maximalen Untermoduln von W.

b) Nach a) gilt also $\operatorname{rad}(W) \subseteq U$ für alle maximalen Untermoduln $U \leq V$. Dies zeigt, dass

$$\operatorname{rad}(W) \subseteq \bigcap_U U \overset{4.3}{=} \operatorname{rad}(V)$$

für $W \leq V$, wobei der Schnitt über alle maximalen $U \leq V$ läuft. $\square$

Aufgabe 4.3. Sei $W \leq V$ Untermodul. Ist jeder maximale Untermodul von W in einem maximalen Untermodul von V enthalten? Begründen Sie Ihre Antwort.

Hier nun das zentrale Resultat dieses Abschnittes.

Theorem 4.5. *Die folgenden Bedingungen sind für endlich-dimensionale Moduln V äquivalent:*

a) V *halbeinfach;*

b) $V = \mathrm{soc}(V)$*;*

c) $V = \sum V_\alpha$*, wobei die Summe über alle einfachen Untermoduln* $V_\alpha \leq V$ *läuft;*

d) $V = \bigoplus_{i=1}^t V_i$ *für eine natürliche Zahl* t*, mit* V_i *einfach für* $1 \leq i \leq t$*;*

e) $\mathrm{rad}(V) = 0$.

Beweis. Die Beweisstruktur ist folgende: *a)* $\Rightarrow$ *b)* $\Rightarrow$ *c)* $\Rightarrow$ *d)* $\Rightarrow$ *e)* $\Rightarrow$ *a)*.

a) $\Rightarrow$ *b)*: Sei V ein halbeinfacher Modul. Nach Definition 4.3 ist $\mathrm{soc}(V) \leq V$. Nach Voraussetzung (siehe Definition 4.1) existiert also ein Komplement zum Untermodul $\mathrm{soc}(V)$ in V, das heisst, es existiert ein Untermodul $W \leq V$ mit $V = \mathrm{soc}(V) \oplus W$. Angenommen $W \neq 0$. Dann existiert ein einfacher Untermodul $V_\alpha \leq W$. Wegen $W \leq V$ ist nach Definition 4.3 auch $V_\alpha \leq \mathrm{soc}(V)$, also $V_\alpha \leq \mathrm{soc}(V) \cap W = 0$. Es folgt $V_\alpha = 0$, was ein Widerspruch ist, siehe Definition 3.1. Also ist $W = 0$ und damit $V = \mathrm{soc}(V)$.

b) $\Rightarrow$ *c)*: Dies folgt direkt aus Definition 4.3.

c) $\Rightarrow$ *d)*: Sei W eine direkte Summe maximaler Dimension von einfachen Untermoduln V_α in V. Nach Voraussetzung ist $V = \sum V_\alpha$, Summe einfacher Moduln. Angenommen $W \neq V$. Dann existiert ein einfacher Modul $V_\alpha \leq V$ mit $V_\alpha \not\leq W$. Der Schnitt $V_\alpha \cap W \overset{2.20}{<} V_\alpha$ ist damit ein echter Untermodul des einfachen Moduls V_α. Nach Definition 3.1 ist damit $V_\alpha \cap W = 0$. Es folgt, dass $W \oplus V_\alpha \leq V$ direkte Summe einfacher Moduln ist mit $\dim(W \oplus V_\alpha) > \dim W$, ein Widerspruch zur Definition von W. Also ist $V = W$, das heisst, der Modul V ist eine direkte Summe einfacher Moduln, und diese ist endlich, da V endlich-dimensional ist.

d) $\Rightarrow$ *e)*: Sei $V = \oplus_{i=1}^t V_i$ eine endliche direkte Summe einfacher Moduln V_i. Setze $W_j := \oplus_{i \neq j} V_i$ für $1 \leq j \leq t$. Mit dem Isomorphiesatz 2.24 sieht man, dass die Moduln $W_j < V$ maximale Untermoduln in V sind. Der Schnitt von allen maximalen Untermoduln von V ist enthalten im Schnitt der maximalen Untermoduln W_j von V, und letzterer ist bereits Null. Mit Definition 4.3 des Radikals folgt, dass $\mathrm{rad}(V) = 0$ ist.

e) $\Rightarrow$ *a)*: Dieser Beweisschritt ist der schwierigste. Wir machen Induktion nach der Dimension von V. Ist $\dim V = 1$, so ist der Modul V einfach, und damit nach Beispiel 4.2 bereits halbeinfach. Sei also $\dim V > 1$. Sei $0 \neq W < V$ ein echter Untermodul von V. Wir konstruieren ein Komplement zu W in V. Hierzu müssen wir zunächst Vorarbeiten leisten:

i) Sei $S \leq W$ ein einfacher Untermodul von W. Angenommen $S \leq M$ für alle maximalen Untermoduln M von V. Dann ist

$$S \leq \bigcap M \overset{4.3}{=} \operatorname{rad}(V) \overset{\text{Vor}}{=} 0,$$

wobei der Schnitt über alle maximalen Untermoduln M in V läuft. Dies impliziert $S = 0$, ein Widerspruch zu Definition 3.1. Also existiert ein maximaler Untermodul M in V mit $S \not\subseteq M$. Damit ist $S \cap M < S$ echter Untermodul eines einfachen Moduls, also $S \cap M = 0$ nach Definition 3.1. Es folgt $M \leq S + M = S \oplus M \leq V$, und da M maximaler Untermodul von V ist, gilt

$$S \oplus M = V. \tag{4.1}$$

ii) Da M Untermodul von V ist, folgt $\operatorname{rad}(M) \overset{4.4}{\leq} \operatorname{rad}(V) \overset{\text{Vor}}{=} 0$, also $\operatorname{rad}(M) = 0$. Es ist $\dim M < \dim V$, also ist nach Induktionsvoraussetzung M ein halbeinfacher Modul. Nach Definition 4.1 existiert damit zum Untermodul $W \cap M \leq M$ ein Komplement W' in M, das heisst, es ist

$$M = (W \cap M) \oplus W'. \tag{4.2}$$

Mit dem hiermit konstruierten Modul W' können wir nun die Behauptung beweisen. Wir wollen zeigen, dass $V = W \oplus W'$ ist. Wir müssen also zeigen, dass $V = W + W'$ und $W \cap W' = 0$ ist. Sei $v \in V$ beliebig. Nach Gleichung (4.1) existieren Elemente $s \in S$ und $m \in M$ mit $v = s + m$. Nach Gleichung (4.2) existieren $w \in W \cap M$ und $w' \in W'$ mit $m = w + w'$. Also ist $v = s + m = (s + w) + w' \in W + W'$, da $S \leq W$ ist. Also ist $V = W + W'$. Als nächstes zeigen wir, dass der Schnitt $W \cap W' = 0$ ist. Es ist

$$0 \overset{(4.2))}{=} (W \cap M) \cap W' = W \cap (M \cap W') = W \cap W',$$

da $W' \leq M$ nach Konstruktion in ii). Also ist in der Tat $V = W \oplus W'$, der Modul W' ist also ein Komplement zu W in V. Mit Definition 4.1 folgt, dass der Modul V halbeinfach ist. □

Sockel und Radikal können allgemeiner auch für Moduln über Ringen definiert werden. Wir betrachten kurz unser Standardbeispiel: Die $\mathbb{Z}$-Moduln $p\mathbb{Z}$ mit p Primzahl sind maximale Untermoduln im $\mathbb{Z}$-Modul $\mathbb{Z}$, siehe Bemerkung 3.6. Damit ist der Schnitt aller maximalen Untermoduln von $\mathbb{Z}$, also das Radikal des $\mathbb{Z}$-Moduls $\mathbb{Z}$, gleich Null. Es ist aber $\mathbb{Z}$ keine direkte Summe einfacher Moduln wie in Theorem 4.5.

Aufgabe 4.4. Bestimmen Sie das Radikal des regulären $K[X]$-Moduls $K[X]$.

Lemma 4.6. *Untermoduln, Quotientenmoduln, homomorphe Bilder und (direkte) Summen von halbeinfachen Moduln sind halbeinfach.*

Beweis. Sei V halbeinfach. Nach Theorem 4.5 ist dann V eine endliche Summe einfacher Moduln, etwa $V = \sum_i S_i$ mit S_i einfach. Wir zeigen als erstes, dass homomorphe Bilder von halbeinfachen Moduln wieder halbeinfach sind. Aus dieser Aussage folgen dann die anderen Aussagen.

a) Sei $\varphi : V \to U$ ein Modulhomomorphismus. Dann ist $\varphi(V)$ ein homomorphes Bild des halbeinfachen Moduls V. Wir wollen mit Hilfe der Charakterisierungen von Halbeinfachheit in Theorem 4.5 zeigen, dass $\varphi(V)$ halbeinfach ist. Wir wenden den Homomorphiesatz 2.24 auf die eingeschränkte Abbildung $\varphi_{|S_i} : S_i \to \varphi(S_i)$ an. Dann gilt:
$$S_i/\ker(\varphi_{|S_i}) \simeq \varphi(S_i). \tag{4.3}$$
Da S_i einfach ist, folgt aus Gleichung (4.3), dass entweder $\varphi(S_i)$ einfach oder $\varphi(S_i) = 0$. Wir nutzen nun, dass φ ein Homomorphismus ist. Damit folgt, dass
$$\varphi(V) = \varphi(\sum_i S_i) = \sum_i \varphi(S_i)$$
eine Summe einfacher Moduln ist. Mit Theorem 4.5 folgt, dass der Modul $\varphi(V)$ halbeinfach ist. Homomorphe Bilder eines halbeinfachen Moduls sind also halbeinfach.

b) Sei $\pi : V \to V/U$ die natürliche Projektion. Dann ist $V/U \simeq \pi(V)$. Der Modul V/U ist also das homomorphe Bild des halbeinfachen Moduls V, und damit nach a) halbeinfach. Quotientenmoduln von halbeinfachen Moduln sind also halbeinfach.

c) Sei $U \leq V$ ein Untermodul. Da V halbeinfach ist, existiert nach Definition 4.1 ein Untermodul $W \leq V$ mit $V = U \oplus W$. Sei $\pi : V \to U$ die Projektion von V auf U entlang W. Dann ist nach dem Homomorphiesatz 2.24
$$U \simeq V/\ker\pi = V/W.$$
Damit ist U ein Quotientenmodul des halbeinfachen Moduls V und mit b) folgt, dass U halbeinfach ist. Untermoduln halbeinfacher Moduln sind also halbeinfach.

d) In einem Modul M seien die Untermoduln $V = \sum_i S_i$ und $W = \sum_j T_j$ jeweils endlichen Summen einfacher Moduln S_i beziehungsweise T_j. Dann ist $V + W = \sum_i S_i + \sum_j T_j$ eine Summe einfacher Moduln, und ist damit wieder halbeinfach nach Theorem 4.5. Damit ist die Summe halbeinfacher Moduln wieder halbeinfach. Analog folgt auch mit Theorem 4.5, dass die direkte Summe halbeinfacher Moduln wieder halbeinfach ist. □

Aufgabe 4.5. Sei $f : M \to N$ ein Modulhomomorphismus.

a) Zeigen Sie, dass $f(\operatorname{soc} M) \leq \operatorname{soc} N$.

b) Zeigen Sie, dass $f(\operatorname{rad} M) \leq \operatorname{rad} N$.

Hinweis: Betrachten Sie in b) Homomorphismen $g : N \to S$ mit S einfach, und zeigen Sie, dass $\operatorname{rad} M \leq \ker(g \circ f)$ *ist.*

Aus Theorem 4.5 wissen wir schon, dass der Sockel eines Moduls der grösste halbeinfache Untermodul des Moduls ist. Damit ist der Sockel ein Mass dafür wieweit ein Modul davon entfernt ist, halbeinfach zu sein. In Theorem 4.5 haben wir bereits gesehen, dass wir mit Hilfe des Radikals erkennen können, ob ein Modul halbeinfach ist. Es ist an dieser Stelle noch nicht offensichtlich, aber auch das Radikal eines Moduls misst, wieweit der Modul von Halbeinfachheit entfernt ist. Bildlich spricht man salopp davon, dass der Sockel den Modul von unten aus untersucht, durch Untermoduln; das Radikal hingegen arbeitet über Quotienten, bildlich gesehen untersucht es den Modul von oben. Um die Aussage über das Radikal genauer zu verstehen, benötigen wir zunächst eine Hilfsaussage:

Bemerkung 4.7. Für Untermoduln M_1, M_2 von V mit $W \subseteq M_i$ für $i = 1, 2$ gilt:

$$M_1/W \cap M_2/W = (M_1 \cap M_2)/W.$$

Bei dieser Gleichung handelt es sich um eine Mengengleichheit, wir müssen also zwei Inklusionen zeigen:

a) Sei $\bar{x} \in M_1/W \cap M_2/W$. Dann ist $\bar{x}$ sowohl Element in M_1/W als auch in M_2/W. Es existieren also $x_1 \in M_1$ und $x_2 \in M_2$ mit $\bar{x} = x_1 + W$ und $\bar{x} = x_2 + W$. Damit ist $x_1 \in x_2 + W$, das heisst, es existiert ein Element $w \in W \subseteq M_2$ mit $x_1 = x_2 + w \in M_2$. Es ist also $x_1 \in M_1 \cap M_2$, und damit ist $\bar{x} = x_1 + W \in (M_1 \cap M_2)/W$. Dies zeigt die erste Inklusion.

b) Sei $\bar{x} \in (M_1 \cap M_2)/W$. Dann existiert ein Element $m \in M_1 \cap M_2$ mit $\bar{x} = m + W$. Da nach Wahl $m \in M_1$ und $m \in M_2$ ist, folgt $\bar{x} \in M_1/W \cap M_2/W$. Dies zeigt die umgekehrte Inklusion. □

Proposition 4.8. *Sei V ein A-Modul.*

a) Der Quotientenmodul $V/\operatorname{rad}(V)$ ist halbeinfach.

b) Jeder Untermodul W von V mit V/W halbeinfach enthält $\operatorname{rad}(V)$ als Teilmodul. Also ist $\operatorname{rad}(V)$ der eindeutige kleinste Untermodul U von V mit V/U halbeinfach.

Beweis.

a) Nach der Untermodulkorrespondenz 2.26 hat jeder maximale Untermodul von $V/\operatorname{rad}(V)$ die Form $M/\operatorname{rad}(V)$ für einen maximalen Untermodul $M \leq V$. Damit folgt:

$$\begin{aligned} \operatorname{rad}(V/\operatorname{rad}(V)) &\overset{4.3}{=} \bigcap_{M \leq V \max} M/\operatorname{rad}(V) \overset{4.7}{=} \left(\bigcap_{M \leq V \max} M \right) / \operatorname{rad}(V) \\ &\overset{4.3}{=} \operatorname{rad}(V)/\operatorname{rad}(V) = 0. \end{aligned}$$

Nach Theorem 4.5 ist damit also der Modul $V/\operatorname{rad}(V)$ halbeinfach.

b) Sei nun $W \leq V$ Untermodul mit der Eigenschaft, dass V/W halbeinfach ist. Wir wollen zeigen, dass dann $\operatorname{rad}(V) \subseteq W$ ist, und in diesem Sinne ist damit $\operatorname{rad}(V)$ der kleinste Untermodul von V, so dass der Quotient halbeinfach ist. Nach Voraussetung ist der Modul V/W halbeinfach, also folgt:

$$0 \overset{4.5}{=} \operatorname{rad}(V/W) \overset{4.3}{=} \bigcap_M M/W \overset{4.7}{=} \left(\bigcap_M M\right)/W. \tag{4.4}$$

Hierbei laufen beide Schnitte über alle maximalen Untermoduln $M \leq V$ mit $W \subseteq M$. Es folgt, dass

$$\operatorname{rad}(V) \overset{4.3}{=} \bigcap_{M \leq V \max} M \subseteq \bigcap_{M \leq V \max \text{ mit } W \subseteq M} M \overset{(4.4)}{=} W.$$

Die Inklusion gilt, weil auf der rechten und grösseren Seite über weniger Mengen $M \leq V$ geschnitten wird als auf der linken Seite. $\square$

Aufgabe 4.6. Sei $A = T_3(K)$ die Algebra der oberen 3×3-Matrizen mit Einträgen im Körper K. Für $1 \leq i \leq 3$ definieren wir die Linksmoduln $M_i := AE_{ii}$. Bestimmen Sie jeweils Radikal und Sockel der Moduln M_i für $1 \leq i \leq 3$.

Aufgabe 4.7. Sei n eine natürliche Zahl und $A = K[X]/(X^n)$.

a) Zeigen Sie, dass der reguläre A-Linksmodul ${}_AA$ genau einen maximalen Untermodul hat.

b) Bestimmen Sie Sockel und Radikal von ${}_AA$.

Diese letzte Übungsaufgabe verdient einen Hinweis: Benutzen Sie die Idealkorrespondenz – analog zur Untermodulkorrespondenz 2.26 – aus der Algebravorlesung, siehe beispielsweise A.Henke, Skript zur Algebravorlesung SS 2017, verlinkt unter `http://info.mathematik.uni-stuttgart.de/algebrahenke18`, Theorem 11.1 (b). Alternativ können Sie zuerst zeigen: Sei das Polynom $f \in K[X]$ der Repräsentant eines Elements $a = f + (X^n)$ in A. Dann ist $a \in A$ invertierbar genau dann, wenn der konstante Koeffizient a_0 von f ungleich Null ist.

Wir beenden diesen Abschnitt mit einem Ihnen bereits vertrautem Beispiel, an dem wir die Konzepte aus Kapitel 3 auch nochmals üben. Dieses Beispiel ist wichtig, weil wir an ihm begreifen können, wie komplex die Struktur von nicht-halbeinfachen Moduln ist.

Beispiel 4.9. Sei $K = \mathbb{Z}_2$ der Körper mit zwei Elementen und $V_4 = C_2 \times C_2$ die Kleinsche Vierergruppe, erzeugt durch die Elemente x und y. Für $a, b \in K$, definieren wir Matrizen

$$\rho_{a,b}(x) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ und } \rho_{a,b}(y) = \begin{pmatrix} 1 & a & 1 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}. \tag{4.5}$$

a) Wir bestimmen als erstes alle Tupel (a, b), sodass $\rho_{a,b}$ eine Darstellung von KV_4 ist. Die Relationen der Gruppe V_4 sind $x^2 = 1 = y^2$ und $xy = yx$. Damit $\rho_{a,b} : KV_4 \to M_3(K)$ eine Darstellung von KV_4 ist, muss nach Bemerkung 2.7 also gelten: $\rho_{a,b}(x)^2 = I_3 = \rho_{a,b}(y)^2$ und $\rho_{ab}(x)\rho_{a,b}(y) = \rho_{a,b}(y)\rho_{a,b}(x)$. Nachrechnen ergibt, dass die erste und dritte Gleichung immer gilt:

$$\rho_{a,b}(x)^2 = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3 \text{ und } \rho_{a,b}(x)\rho_{a,b}(y) = \begin{pmatrix} 1 & a & 0 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = \rho_{a,b}(y)\rho_{a,b}(x).$$

Die zweite Gleichung liefert eine Bedingung an die Variablen a, b:

$$I_3 = \rho_{a,b}(y)^2 = \begin{pmatrix} 1 & 0 & ab \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Damit ist $\rho_{a,b}$ eine Darstellung von KV_4 genau dann, wenn $a \cdot b = 0$ ist, also für

$$(a, b) \in \{(0, 0), (0, 1), (1, 0)\}.$$

b) Sei nun (a, b) so, dass $\rho_{a,b}$ eine Darstellung von KV_4 ist. Wir schreiben $V_{a,b} := K\text{-Span}\{e_1, e_2, e_3\}$ für den zur Darstellung $\rho_{a,b}$ korrespondierenden Modul. Dann ist die Operation der Erzeuger nach Definition in (4.5) und Bemerkung 2.28 gegeben durch

$$\begin{aligned} xe_1 &= e_1, \quad xe_2 = e_2, \quad xe_3 = e_1 + e_3, \\ ye_1 &= e_1, \quad ye_2 = ae_1 + e_2, \quad ye_3 = e_1 + be_2 + e_3. \end{aligned} \tag{4.6}$$

Beachten Sie, wir lesen hier darstellende Matrizen bezüglich einer Basis ab, im Sinne der Linearen Algebra. Entsprechend kann die Menge $\{e_1, e_2, e_3\}$ als eine beliebige Basis gewählt werden, nicht-notwendigerweise die Standardbasis, und das Ergebnis ist immer noch wie in (4.6). Wir wollen bis auf Isomorphie alle eindimensionalen Untermoduln im Modul $V_{a,b}$ bestimmen. Sei U eindimensionaler Untermodul von $V_{a,b}$ mit Basisvektor u. Da U ein Modul ist, muss gelten $xu = \lambda u$ und $yu = \mu u$ für Skalare $\lambda, \mu \in K$. Damit ist u ein gemeinsamer Eigenvektor der Matrizen $\rho_{a,b}(x)$ und $\rho_{a,b}(y)$. Beide diese Matrizen sind obere Dreiecksmatrizen. Wir lesen also die Eigenwerte auf ihren jeweiligen Diagonalen ab: Beide Matrizen haben nur den Eigenwert Eins. Damit muss gelten $xu = u$ und $yu = u$, und es folgt, dass U isomorph zum trivialen Modul ist. Bis auf Isomorphie hat also $V_{a,b}$ nur den trivialen eindimensionalen Untermodul. Durch Berechnung der Eigenvektoren können wir nun alle solche Kopien des trivialen Moduls als Untermodul in $V_{a,b}$ bestimmen. Es ist hierbei $xu = u$ genau dann, wenn für $u = (u_1, u_2, u_3)^T$ gilt:

$$\begin{pmatrix} u_1 + u_3 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}.$$

Letzteres passiert genau dann, wenn $u_3 = 0$ ist. Die Eigenvektoren der Matrix $\rho_{a,b}(x)$ sind also genau die Vektoren $0 \neq (u_1, u_2, 0)^T$ mit $u_1, u_2 \in K$. Da wir einen simultanen Eigenvektor für beide erzeugenden Matrizen in (4.5) benötigen, rechnen wir gleich mit diesen gefundenen Eigenvektoren der ersten Matrix weiter. Dann ist $u = (u_1, u_2, 0)^T$ auch ein Eigenvektor von $\rho_{a,b}(y)$, wenn gilt:

$$\begin{pmatrix} u_1 + au_2 \\ u_2 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & a & 1 \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ 0 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \\ 0 \end{pmatrix}.$$

Wir benötigen hierzu, dass $au_2 = 0$ gilt. Damit müssen wir zwei Fälle unterscheiden: entweder ist $a = 0$ und u_2 beliebig oder aber $a \neq 0$ und $u_2 = 0$. Der Modul $V_{1,0}$ hat also nur einen eindimensionalen Untermodul, erzeugt durch den Vektor e_1. Die Moduln $V_{0,b}$ haben jeweils drei eindimensionale Untermoduln, erzeugt durch die Vektoren e_1, e_2 und $e_1 + e_2$. Sei $M_{a,b} := \sum_U U$ Untermodul von $V_{a,b}$, wobei die Summe über alle einfachen eindimensionalen Untermoduln $U < V_{a,b}$ läuft. Dann ist nach unserer Rechnung

$$M_{1,0} = K\text{-Span}\{e_1\} \text{ und } M_{0,0} = M_{0,1} = K\text{-Span}\{e_1, e_2\}.$$

c) Die beiden angegebenen Matrizen sind obere Dreiecksmatrizen, das heisst, die darstellenden Matrizen der Erzeuger x und y sind simultan trigonalisierbar. In einer solchen Situation lässt sich eine Kette von Untermoduln sofort ablesen: Sei $U_1 = K\text{-Span}\{e_1\}$ und $W_{a,b} := K\text{-Span}\{e_1, e_2\}$. Dann ist die Kette von Untermoduln

$$0 < U_1 < W_{a,b} < V_{a,b} \tag{4.7}$$

eine Kompositionsreihe von $V_{a,b}$ der Länge drei: die darstellenden Matrizen in Form oberer Dreiecksmatrizen in (4.5) garantieren, dass es sich um Untermoduln handelt; am besten liest man dies direkt an den Gleichungen der Operation in (4.6) ab. Ausserdem sind die Quotienten U_1, $W_{a,b}/U_1$ und $V_{a,b}/W_{a,b}$ eindimensional und damit einfach. Bestimmt man die Kompositionsfaktoren eines Moduls, so ist dies immer auch die Frage danach, welchen Isomorphietyp die Moduln haben, also insbesondere, ob manche dieser Kompositionsfaktoren isomorph zueinander sind. Wir rechnen in unserem Beispiel nach, dass alle Kompositionsfaktoren isomorph zum trivialen Modul sind, also gleichen Isomorphietyp haben: Modul $W_{a,b}/U_1$ hat Basis $e_2 + U_1$ mit der Operation

$$\begin{aligned} x \cdot (e_2 + U_1) &= xe_2 + U_1 = e_2 + U_1, \\ y \cdot (e_2 + U_1) &= ye_2 + U_1 = ae_1 + e_2 + U_1 = e_2 + U_1. \end{aligned}$$

Und ganz analog erhält man die Operation auf dem Basisvektor $e_3 + W_{a,b}$ von $V_{a,b}/W_{a,b}$:

$$\begin{aligned} x \cdot (e_3 + W_{a,b}) &= xe_3 + W_{a,b} = e_1 + e_3 + W_{a,b} = e_3 + W_{a,b}, \\ y \cdot (e_3 + W_{a,b}) &= ye_3 + W_{a,b} = e_1 + be_2 + e_3 + W_{a,b} = e_3 + W_{a,b}. \end{aligned}$$

Die Kompositionsfaktoren des Moduls $V_{a,b}$ sind also drei Kopien des trivialen Moduls. Alternativ zu dieser Rechnung kann man auch allgemeiner zeigen, dass jeder eindimensionale $\mathbb{Z}_2V_4$-Modul trivial ist: Ist $M = K$-Span$\{\mathrm{m}\}$ ein eindimensionaler $\mathbb{Z}_2V_4$-Modul, so existiert ein Skalar $\lambda \in \mathbb{Z}_2$ mit $x \cdot m = \lambda m$. Es folgt:

$$m = 1 \cdot m = x^2 \cdot m = \lambda^2 m, \text{ also wegn } m \neq 0 \text{ gilt } \lambda = \pm 1 = 1.$$

Es ist also $x \cdot m = m$. Analog folgt $y \cdot m = m$. Damit ist M der triviale Modul.

d) Mit dem Satz von Jordan-Hölder 3.21 folgt aus der angegebenen Kompositionsreihe in (4.7), dass auch alle einfachen Untermoduln von $V_{a,b}$ eindimensional sein müssen: Angenommen $V_{a,b}$ besitzt beispielsweise einen zweidimensionalen einfachen Untermodul W. Dann existiert nach Lemma 3.27 eine Kompositionsreihe von $V_{a,b}$, in der der Modul W vorkommt. Aus Dimensionsgründen ist damit $0 < W < V_{a,b}$ eine Kompositionsreihe von $V_{a,b}$ der Länge zwei, im Widerspruch zum Satz von Jordan-Hölder 3.21. Der Modul $M_{a,b}$ ist also nicht nur die Summe aller eindimensionalen einfachen Untermoduln, sondern sogar die Summe aller einfachen Untermoduln von $V_{a,b}$. Damit ist $M_{a,b} = \operatorname{soc} V_{a,b}$, siehe Definition 4.3.

e) Wir benutzen nun unter anderem den Sockel von $V_{a,b}$, um zu zeigen, dass die drei Moduln $V_{a,b}$ paarweise nicht-isomorph sind, oder dazu äquivalent, dass die drei Darstellungen $\rho_{a,b}$ nicht paarweise äquivalent sind, siehe Proposition 2.29. Aufgabe 4.5 impliziert, dass die Sockel zweier isomorpher Moduln ebenfalls isomorph sein müssen. Da der Sockel $M_{1,0}$ eindimensional ist, hingegen Sockel $M_{0,b}$ zweidimensional, ist der Modul $V_{1,0}$ nicht-isomorph zu einem der Moduln $V_{0,b}$. Wie sieht das für die Moduln $V_{0,0}$ und $V_{0,1}$ aus? Angenommen sie sind isomorph. Dann gibt es einen Isomorphismus $\varphi : V_{0,0} \to V_{0,1}$. Sei $\{e'_1, e'_2, e'_3\}$ die Basis von $V_{0,0}$ und $\{e_1, e_2, e_3\}$ die Basis von $V_{0,1}$. Der Isomorphismus φ bildet nach Aufgabe 4.5 Sockel auf Sockel ab; es ist also $\varphi(e'_i) \in \langle e_1, e_2 \rangle$ für $i = 1, 2$. Die beiden Moduln unterscheiden sich in der Variablen b. Diese kommt lediglich in der Operation auf dem dritten Basisvektor vor, den wir im folgenden daher betrachten. Seien $\alpha, \beta, \gamma \in K$ mit $\varphi(e'_3) = \alpha e_1 + \beta e_2 + \gamma e_3$. Da φ Homomorphismus ist, gilt

$$\begin{aligned} \alpha e_1 + \beta e_2 + \gamma(e_1 + e_2 + e_3) &= y(\alpha e_1 + \beta e_2 + \gamma e_3) = y\varphi(e'_3) \\ &= \varphi(ye'_3) \overset{b=0}{=} \varphi(xe'_3) = x\varphi(e'_3) \\ &= x(\alpha e_1 + \beta e_2 + \gamma e_3) \\ &= \alpha e_1 + \beta e_2 + \gamma(e_1 + e_3). \end{aligned}$$

Hierbei haben wir jeweils die passenden Werte für a und b eingesetzt; beim ersten Gleichheitszeichen ist das $a = 0$ und $b = 1$, da wir im Modul $V_{0,1}$ rechnen; beim vierten Gleichheitszeichen rechnen wir im Modul $V_{0,0}$, also ist $b = 0$. Koeffizientenvergleich der Basisvektoren ergibt, dass $\beta + \gamma = \beta$ ist; also ist $\gamma = 0$ beziehungsweise $\operatorname{im} \varphi = \langle e_1, e_2 \rangle$. Dies ist ein Widerspruch zu φ Isomorphismus. Also sind die Moduln $V_{0,0}$ und $V_{0,1}$ nicht isomorph.

Die drei Moduln $V_{a,b}$ sind also paarweise nicht-isomorphe dreidimensionale Moduln, auf verschiedene Art und Weise zusammengebaut aus jeweils drei Kopien des trivialen Moduls. Gerade in der Darstellungstheorie von nicht-halbeinfachen Objekten gibt es noch viele offene Fragen zu beantworten. Was Zusammenbauen von Moduln im Allgemeinen bedeutet, können Sie genauer in der derzeit parallel stattfindenden Master-Vorlesung Representation Theory of Algebras lernen. Im letzten Beispiel haben wir mittels recht formaler Argumente den Modul $V_{a,b}$ analysiert. Eigentlich wird hier ein bisschen mit Kanonen auf Spatzen geschossen: Benutzt man, dass $V_{a,b}$ lediglich aus acht verschiedenen Elementen besteht,

$$V_{a,b} = \{0, e_1, e_2, e_3, e_1 + e_2, e_1 + e_3, e_2 + e_3, e_1 + e_2 + e_3\},$$

so lasst sich die Modulstruktur von $V_{a,b}$ auch ad-hoc analysieren durch das relativ langweilige Auflisten aller Erzeugnisse einer Teilmenge von Elementen.

Wir wollen den Moduln $V_{a,b}$ alles Mysteriöse nehmen und betrachten daher noch die Fragen: welche verschiedene Kompositionsreihen haben wir? Welche Untermoduln gibt es? Den Sockel kennen wir bereits, was ist das Radikal?

Beispiel 4.10. Sei $V := V_{1,0}$. Nach Beispiel 4.9 ist der Sockel $U := \operatorname{soc}(V) = K\text{-Span}\{e_1\} =: \langle e_1\rangle_K$. Alle Kompositionsreihen von V müssen also U enthalten. Alle möglichen Fortsetzungen dieser Kompositionsreihen erhalten wir durch Hochheben von Kompositionsreihen des Quotientenmoduls V/U mittels der Untermodulkorrespondenz 2.27. Es ist $B := \{\bar{e}_2 := e_2 + U, \bar{e}_3 := e_3 + U\}$ Basis von V/U. Sei $\bar{\rho}$ die Matrixdarstellung korrespondierend zum Quotientenmodul V/U bezüglich der Basis B. Wir entnehmen der Operation in Gleichung (4.6):

$$\bar{\rho}(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ und } \bar{\rho}(y) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Alle Vektoren ungleich Null sind hier simultane Eigenvektoren der beiden Matrizen. Damit ergeben sich drei verschiedene Kompositionsreihen für den Quotienten V/U:

$$\begin{aligned} 0 &< \langle \bar{e}_2\rangle_K < V/U, \\ 0 &< \langle \bar{e}_3\rangle_K < V/U, \\ 0 &< \langle \bar{e}_2 + \bar{e}_3\rangle_K < V/U; \end{aligned}$$

diese heben wir zu Kompositionsreihen von V hoch. Damit erhalten wir insgesamt genau drei verschiedene Kompositionsreihen von $V = V_{1,0}$:

$$\begin{aligned} 0 &< \langle e_1\rangle_K < \langle e_1, e_2\rangle_K < V, \\ 0 &< \langle e_1\rangle_K < \langle e_1, e_3\rangle_K < V, \\ 0 &< \langle e_1\rangle_K < \langle e_1, e_2 + e_3\rangle_K < V. \end{aligned}$$

Der Untermodulverband (siehe Aufgabe 4.2) ergibt sich damit als:

$$\begin{tikzcd}[column sep=tiny] & V_{1,0} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \langle e_1, e_2\rangle_K \arrow[dr, dash] & \langle e_1, e_2 + e_3\rangle_K \arrow[d, dash] & \langle e_1, e_3\rangle_K \arrow[dl, dash] \\ & \langle e_1\rangle_K \arrow[d, dash] & \\ & 0 & \end{tikzcd}$$

Wir entnehmen diesem Bild auch alle maximalen Untermoduln von V und damit das Radikal von V:

$$\operatorname{rad} V = \langle e_1, e_2\rangle_K \cap \langle e_1, e_3\rangle_K \cap \langle e_1, e_2 + e_3\rangle_K = \langle e_1\rangle_K = \operatorname{soc} V.$$

Vielleicht ist es sinnvoll, sich bei der Besprechung der folgenden Aufgabe 4.8 in der Übung bei der Bildschirmteilung auf die vollständige Liste der Kompositionsreihe der Moduln $V_{0,b}$ und den Untermodulverband zu konzentrieren. Viele Rechnungen wiederholen sich beziehungsweise können auf einem Schmierblatt oder im Kopf direkt von Gleichung (4.6) abgelesen werden.

Aufgabe 4.8. Bestimmen Sie alle möglichen Kompositionsreihen, den Untermodulverband, sowie Radikal (und Sockel) der Moduln $V_{0,b}$ mit $b \in \{0, 1\}$.

Aufgabe 4.9. Nach Aufgabe 2.14 ist der triviale Modul K, erzeugt von der Summe aller Gruppenelemente aus V_4, ein Untermodul des regulären Moduls $M := \mathbb{Z}_2 V_4$.

a) Zeigen Sie, dass M/K isomorph zu $V_{0,1}$ ist. Bestimmen Sie den Untermodulverband des regulären Moduls $\mathbb{Z}_2 V_4$.

b) Beweisen Sie, dass die Gruppenalgebra $\mathbb{Z}_2 V_4$ bis auf Isomorphie genau einen einfachen Modul (den trivialen Modul) besitzt.

Die erste Behauptung in Aufgabe 4.9 a) sollten Sie bei Zeitknappheit vermutlich auslassen und bei Ihrer Lösung der anderen Aufgabenteile einfach benutzen.

Bemerkung 4.11. Am Ende von Beispiel 2.39 haben wir den Begriff unzerlegbar definiert. Sind die Moduln $V_{a,b}$ unzerlegbar? Nicht so schwer zu beweisen sind die beiden folgenden abstrakten Teilantworten:

a) Falls der Sockel eines Moduls einfach ist, so ist der Modul immer unzerlegbar. Aus diesem Grund ist der Modul $V_{1,0}$ unzerlegbar.

b) Falls $M/\operatorname{rad}(M)$ einfach ist, so ist der Modul M unzerlegbar. Aus diesem Grund ist $V_{0,1}$ unzerlegbar.

Man entnimmt (4.6), dass der Modul $V_{0,0}$ zerlegbar ist mit $V_{0,0} = \langle e_2 \rangle_K \oplus \langle e_1, e_3 \rangle_K$. Hierbei ist der erste Modul einfach und damit unzerlegbar, und der zweite Modul ist uniseriell, hat also einen einfachen Sockel und ist damit nach a) unzerlegbar. (Können Sie die direkte Summenzerlegung von $V_{0,0}$ am Untermodulverband in Aufgabe 4.8 erkennen?)

Beweis. Wir beweisen jeweils die Kontraposition der obigen Aussagen. Angenommen der Modul M ist zerlegbar mit echter Zerlegung $M = M_1 \oplus M_2$.

a) Diese Behauptung folgt aus der ganz unabhängig von der Behauptung nützliche Aussage, dass gilt

$$\operatorname{soc}(M_1 \oplus M_2) \quad = \quad \operatorname{soc}(M_1) \oplus \operatorname{soc}(M_2). \tag{4.8}$$

Nach Gleichung (4.8) hat der Sockel von $M = M_1 \oplus M_2$ mindestens zwei Kompositionsfaktoren. Umgekehrt gilt also, ist der Sockel von M einfach, so ist M unzerlegbar.

Zu zeigen bleibt noch Gleichung (4.8): Jeder einfache Untermodul von M_1 oder M_2 ist immer ein einfacher Untermodul von $M = M_1 \oplus M_2$. Nach Definition 4.3 ist also $\operatorname{soc}(M_1) \oplus \operatorname{soc}(M_2) \subseteq \operatorname{soc}(M_1 \oplus M_2) = \operatorname{soc}(M)$. Betrachte die natürlichen Projektionen $\pi_i : M \to M_i$ für $i = 1, 2$. Nach Aufgabe 4.5 ist

$$\operatorname{soc}(M) = (\pi_1 + \pi_2)(\operatorname{soc} M) = \pi_1(\operatorname{soc} M) + \pi_2(\operatorname{soc} M) \subseteq \operatorname{soc}(M_1) + \operatorname{soc}(M_2).$$

Wir erhalten zunächst nur eine Summe der beiden Sockel. Angenommen $\operatorname{soc} M_1 \cap \operatorname{soc} M_2 =: U \neq 0$. Dann existiert ein einfacher Modul $T \leq U$, und es folgt aus $T \leq \operatorname{soc} M_1 \leq M_1$ und $T \leq \operatorname{soc} M_2 \leq M_2$, ein Widerspruch zu $M_1 \cap M_2 = 0$.

b) Sei $U < M_1$ ein maximaler Untermodul von M_1. Dann ist $U \oplus M_2$ ein maximaler Untermodul von $M = M_1 \oplus M_2$. Es folgt aus Definition 4.3, dass $\operatorname{rad} M \leq U \oplus M_2$ ist. Da U beliebiger maximaler Untermodul von M_1 ist, folgt

$$\operatorname{rad} M \leq \bigcap_{U \leq M_1 \text{ max}} (U \oplus M_2) = \Big(\bigcap_{U \leq M_1 \text{ max}} U\Big) \oplus M_2 = \operatorname{rad}(M_1) \oplus M_2.$$

Ganz analog folgt auch $\operatorname{rad} M \leq M_1 \oplus \operatorname{rad}(M_2)$, und damit gilt die nützliche Inklusion

$$\operatorname{rad} M \leq (M_1 \oplus \operatorname{rad}(M_2)) \cap (\operatorname{rad}(M_1) \oplus M_2) = \operatorname{rad} M_1 \oplus \operatorname{rad} M_2. \quad (4.9)$$

Auch die Umkehrung dieser Inklusion gilt, ist aber an dieser Stelle noch schwer zu beweisen. Wir kommen später darauf zurück. Die Inklusion (4.9) impliziert zusammen mit Lemma 3.27 und der Untermodulkorrespondenz 2.27, dass es eine Kompositionsreihe gibt, in der die folgenden Moduln vorkommen

$$\operatorname{rad}(M_1 \oplus M_2) < \operatorname{rad} M_1 \oplus \operatorname{rad} M_2 < M_1 \oplus \operatorname{rad} M_2 < M,$$

und damit hat $M/\operatorname{rad} M$ nach der Untermodulkorrespondenz 2.27 mindestens zwei Kompositionsfaktoren. Wir haben also gesehen, ist $M/\operatorname{rad} M$ einfach, dann ist M unzerlegbar. $\square$

Nach all diesen Rechnungen beenden wir diesen Abschnitt mit einer abstrakten Aufgabe: Sei A eine Algebra. Ein *Subquotient* eines A-Moduls N ist ein Modul Y/X mit $0 \leq X \leq Y \leq N$ Untermoduln von N. Insbesondere muss Y/X nicht notwendigerweise einfach sein.

Aufgabe 4.10. Angenommen der Modul N hat eine Kompositionsreihe der Länge drei, und alle Subquotienten von N mit zwei Kompositionsfaktoren sind halbeinfach. Dann folgt, dass der Modul N halbeinfach ist.
Hinweis: Zeigen Sie, dass N mehr als einen maximalen Untermodul besitzt.

4.2 Halbeinfache Algebren

Wie üblich sind Algebren und Moduln über diesen Algebren in diesem Abschnitt endlich-dimensional. Im letzten Abschnitt haben wir uns mit halbeinfachen Moduln beschäftigt. In diesem Abschnitt studieren wir die Klasse der halbeinfachen Algebren:

Definition 4.12. Eine Algebra A heisst *halbeinfach*, falls jeder A-Modul ein halbeinfacher Modul ist.

Beispiel 4.13. Sei $A = K$ ein Körper. Dann entsprechen A-Moduln gerade K-Vektorräumen. Sei V ein A-Modul, und sei $\{b_1, \ldots, b_n\}$ eine Basis von V. Sei $S_i := K\text{-Span}\{b_i\}$ für $1 \leq i \leq n$. Dann ist S_i ein einfacher A-Modul mit $V = \oplus_{i=1}^n S_i$. Also ist V ein halbeinfacher Modul. Da V beliebig war, ist A nach Definition 4.12 eine halbeinfache Algebra.

In diesem letzten Beispiel sind Moduln nichts anderes als Vektorräume; im Allgemeinen sind A-Moduln aber Vektorräume, die unter der Operation der Algebra A abgeschlossen sind. Es wirkt im ersten Moment hoffnungslos zu überprüfen, ob jeder Modul über einer gegebenen Algebra A halbeinfach ist. Tatsächlich müssen wir nur einen einzigen Modul auf Halbeinfachheit überprüfen:

Theorem 4.14. *Eine Algebra A ist genau dann halbeinfach, wenn der reguläre Modul ${}_AA$ ein halbeinfacher Modul ist.*

Beweis. Ist A eine halbeinfache Algebra, so ist nach Definition 4.12 der reguläre Modul halbeinfach. Es ist also nichts weiter zu zeigen. Umgekehrt, sei nun der reguläre Modul ${}_AA$ ein halbeinfacher A-Modul. Sei M ein beliebiger A-Modul und sei $\{m_1, \ldots, m_n\}$ eine Vektorraumbasis von M. Sei $A^n = A \times \ldots \times A$ das kartesische Produkt von A mit sich selber, n mal. Die Algebra A operiert auf A^n durch $a(v_1, \ldots, v_n) := (av_1, \ldots, av_n)$ für $a \in A$ und $(v_1, \ldots, v_n) \in A^n$. Mit dieser Operation ist A^n ein A-Modul, nämlich die direkte Summe von n Kopien des regulären Moduls. Definiere

$$\psi : A^n \to M, \quad (a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i m_i.$$

Nach Beispiel 2.25 ist ψ ein A-Modulhomomorphismus. Da die Vektoren $m_1, \ldots, m_n$ eine Basis von M bilden und $K \subseteq A$, siehe Bemerkung 1.2, ist die Abbildung ψ surjektiv. Nach Voraussetzung ist der reguläre Modul ${}_AA$ ein halbeinfacher Modul. Nach Lemma 4.6 ist damit auch A^n als direkte Summe von n halbeinfachen Moduln ein halbeinfacher Modul. Da $M = \psi(A^n)$ ist, folgt mit Lemma 4.6, dass der Modul M als homomorphes Bild eines halbeinfachen Moduls wieder halbeinfach ist. Damit haben wir gezeigt, dass jeder A-Modul halbeinfach ist. Mit Definition 4.12 folgt, dass die Algebra A halbeinfach ist. $\square$

Beispiel 4.15. a) Sei $A = M_n(K)$ die Matrixalgebra der $n \times n$-Matrizen über dem Körper K. Nach Beispiel 3.4 ist der A-Modul K^n ein einfacher A-Modul, bis auf Isomorphie der einzige einfache A-Modul. Nach Beispiel 3.22 b) ist die reguläre Darstellung der Algebra $A = M_n(K)$ eine direkte Summe von n Kopien des einfachen A-Moduls K^n. Damit ist der reguläre A-Modul ${}_AA$ halbeinfach nach Definition 4.12. Nach Theorem 4.14 ist also die Matrixalgebra $A = M_n(K)$ eine halbeinfache Algebra.

b) Es existieren auch Algebren, die nicht halbeinfach sind. Die $\mathbb{Z}_2V_4$-Moduln $V_{a,b}$ in Beispiel 4.9 sind nicht halbeinfach, also ist die Algebra $\mathbb{Z}_2V_4$ nicht halbeinfach. Die Algebra $\mathbb{C}V_4$ ist hingegen halbeinfach.

Aufgabe 4.11. Sei $V = K^2$ der Vektorraum der Spaltenvektoren, auf dem die Algebra $T_2(K)$ durch Matrixmultiplikation von links operiert. Zeigen Sie, dass der $T_2(K)$-Modul V nicht halbeinfach ist, und damit $T_2(K)$ keine halbeinfache Algebra ist. Ist $T_n(K)$ halbeinfach für $n \geq 3$?

Wir lernen am letzten Beispiel (mit $T_n(K)$ Unteralgebra von $M_n(K)$) zusammen mit Aufgabe 4.11, dass Unteralgebren halbeinfacher Algebren nicht notwendigerweise wieder halbeinfach sind. Für Quotientenalgebren ist das anders:

Korollar 4.16. *a) Sei B eine Quotientenalgebra einer halbeinfachen Algebra A. Dann ist B halbeinfach.*

b) Die Algebren A_i mit $1 \leq i \leq n$ sind genau dann alle halbeinfach, wenn die Algebra $A_1 \times \ldots \times A_n$ halbeinfach ist.

Beweis.

a) Sei I Ideal in A mit $B = A/I$. Mittels Inflation, siehe Bemerkung 3.16, wird aus jedem B-Modul ein A-Modul M durch die Operation $A \times M \to M, (a, m) \mapsto a \cdot m := (a + I) \cdot m$, für $a \in A$ und $m \in M$. Hierbei gilt dann insbesondere $I \cdot M = 0$. Wir fassen in diesem Sinne den regulären B-Modul ${}_BB$ als A-Modul ${}_AB$ auf, wobei gilt $I \cdot B = 0$. Dann ist die Abbildung $\pi : {}_AA \to {}_AB$, definiert durch $\pi(a) = a + I$ ein surjektiver A-Modulhomomorphismus:

$$\pi(a \cdot v) = av + I = a(v + I) = a\pi(v), \text{ für } a, v \in A.$$

Da A eine halbeinfache Algebra ist, ist nach Definition 4.12 der reguläre Modul ${}_AA$ halbeinfach. Nach Lemma 4.6 ist somit der Modul ${}_AB$ als homomorphes Bild eines halbeinfachen Moduls wieder halbeinfach. Es ist also ${}_AB = \oplus_{j=1}^{t} S_i$ eine direkte Summe einfacher A-Moduln S_i. Da $I \cdot B = 0$ ist, gilt auch $I \cdot S_j = 0$ für alle $1 \leq j \leq t$. Nach Bemerkung 3.16 ist somit S_j ein einfacher B-Modul und der reguläre Modul ${}_BB = \oplus_t S_t$ ist eine direkte Summe einfacher B-Moduln. Nach Theorem 4.14 ist B also eine halbeinfache Algebra.

b) Wir schreiben $A := A_1 \times \ldots \times A_n$ und betrachten die Projektionen $\pi_j : A \to A_j$, für $1 \leq j \leq n$. Diese sind surjektive Algebrenhomomorphismen, und damit ist A_j eine Quotientenalgebra der Algebra A für $1 \leq j \leq n$. Ist A halbeinfache Algbebra, so folgt mit a), dass auch A_j eine halbeinfache Algebra ist, für $1 \leq j \leq n$.

Für die andere Beweisrichtung sei zur Vereinfachung $n = 2$, also $A = A_1 \times A_2$. Angenommen die Algebren A_1 und A_2 sind halbeinfache Algebren. Dann ist nach Definition 4.12 insbesondere der reguläre Modul ${}_{A_j}A_j$ ein halbeinfacher Modul, für $j = 1, 2$. Es existieren also einfache A_1-Moduln S_i, mit $1 \leq i \leq s$, und einfache A_2-Moduln T_i, mit $1 \leq i \leq t$, sodass gilt:

$${}_{A_1}A_1 = S_1 \oplus \ldots \oplus S_s \text{ und } {}_{A_2}A_2 = T_1 \oplus \ldots \oplus T_t.$$

Wende Inflation aus Bemerkung 3.16 an: Die Moduln S_i sind dann einfache $A_1 \times A_2$-Moduln mit $A_2 \cdot S_i = 0$, für $1 \leq i \leq s$. Und die Moduln T_i sind ebenfalls einfache $A_1 \times A_2$-Moduln mit $A_1 \cdot T_j = 0$, für $1 \leq i \leq t$. Es folgt, dass der reguläre Modul isomorph zu einem halbeinfachen Modul ist:

$$_A(A_1 \times A_2) = {}_A(A_1 \times \{0\}) \oplus {}_A(\{0\} \times A_2) \simeq {}_AA_1 \oplus {}_AA_2 = \bigoplus_i S_i \oplus \bigoplus_j T_j,$$

und damit ist $_AA$ nach Lemma 4.6 halbeinfach. Nach Theorem 4.14 ist die Algebra A also halbeinfach. Induktiv folgt nun die Behauptung für Algebren A_i mit $1 \leq i \leq n$. □

Beispiel 4.17. Nach Beispiel 4.15 sind Matrixalgebren beliebiger Grösse halbeinfache Algebren. Damit ist das kartesische Produkt $A = M_{n_1}(K) \times \ldots \times M_{n_t}(K)$ von t Matrixalgebren nach Korollar 4.16 eine halbeinfache Algebra. So unspektakulär dieses Beispiel an dieser Stelle ist: wir werden sehen, dass jede endlich-dimensionale halbeinfache Algebra über einem algebraisch abgeschlossenen Körper isomorph zu einem direkten Produkt von Matrixalgebren wie oben ist. Dieses Beispiel gibt also den Prototyp einer halbeinfachen Algebra an.

4.3 Der Satz von Wedderburn

In diesem Abschnitt klassifizieren wir die endlich-dimensionalen halbeinfachen Algebren über einem algebraisch abgeschlossenen Körper K. Dies benötigt einige Vorarbeiten.

Bemerkung 4.18. Sei M ein halbeinfacher A-Modul.

a) Zerlegungen halbeinfacher Moduln als direkte Summe einfacher Moduln sind eindeutig bis auf Isomorphie und Reihenfolge der Summanden: Angenommen es sind $M = U_1 \oplus \ldots \oplus U_m = T_1 \oplus \ldots \oplus T_n$ zwei verschiedene Zerlegungen des Moduls M als direkte Summe einfacher A-Moduln. Dann sind

$$0 \subsetneq U_1 \subsetneq U_1 \oplus U_2 \subsetneq \ldots \subsetneq U_1 \oplus \ldots \oplus U_{m-1} \subsetneq M,$$
$$0 \subsetneq T_1 \subsetneq T_1 \oplus T_2 \subsetneq \ldots \subsetneq T_1 \oplus \ldots \oplus T_{n-1} \subsetneq M$$

Kompositionsreihen von M der Länge m beziehungsweise n mit Kompositionsfaktoren $U_1, \ldots U_m$ beziehungsweise $T_1, \ldots, T_n$. Es folgt aus dem Satz von Jordan-Hölder 3.21, dass $n = m$ ist und nach Umsortierung ist $T_i \simeq U_i$, für $1 \leq i \leq n$.

b) Nach Theorem 3.30 hat eine endlich-dimensionale Algebra nur endlich viele einfache Moduln, und diese kommen als Kompositionsfaktor des regulären Moduls vor. Sei $\{S_1, \ldots, S_t\}$ ein Repräsentantensystem der Isomorphieklassen einfacher A-Moduln. Dann existieren nach a) für jeden halbeinfachen A-Modul M eindeutige natürliche Zahlen $n_i \in \mathbb{N}_0$, sodass $M \simeq S_1^{n_1} \oplus \ldots \oplus S_t^{n_t}$ ist. Für einen einfachen Modul S schreiben wir hierbei

$$S^n := \underbrace{S \oplus \ldots \oplus S}_{n\text{- mal}}.$$

Im Fall des regulären Moduls existieren nach Theorem 3.30 natürliche Zahlen n_i, sodass

$$_AA = S_1^{n_1} \oplus \ldots \oplus S_t^{n_t} \text{ mit } n_i > 0, \text{ für alle } 1 \leq i \leq t.$$

Bevor wir strukturell in den Beweis der Klassifikation einsteigen können, benötigen wir die folgende Algebra:

Lemma 4.19. *Sei A eine Algebra über dem Körper K. Gegeben seien weiter die A-Moduln $M_1, \ldots, M_n$. Dann ist die Menge der Matrizen*

$$B := \left\{ \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix} \mid f_{ij} \in \mathrm{Hom}_A(M_j, M_i) \right\}$$

eine K-Algebra.

Beweis. Seien (f_{ij}) und (g_{ij}) Matrizen in der Menge B. Um eine Algebrenstruktur auf der Menge B zu defininieren, müssen wir zunächst Addition, Skalarmultiplikation und Multiplikation angeben. Diese wählen wir als die übliche Matrixaddition, Matrix-Skalarmultiplikation und Matrixmultiplikation:

$$\begin{aligned} (f_{ij}) + (g_{ij}) &:= (f_{ij} + g_{ij}) & &\text{mit } (f_{ij} + g_{ij})(m_j) := f_{ij}(m_j) + g_{ij}(m_j), \\ \lambda \cdot (f_{ij}) &:= (\lambda f_{ij}) & &\text{mit } (\lambda \cdot f_{ij})(m_j) := \lambda \cdot f_{ij}(m_j), \\ (f_{ij}) \cdot (g_{ij}) &:= (h_{ij}) & &\text{mit } h_{ij} := \sum_{l=1}^{n} f_{il} \circ g_{lj}. \end{aligned}$$

Beachte hierbei, dass die Komposition der Modulhomomorphismen wohldefiniert ist: $f_{il} \circ g_{lj} \in \mathrm{Hom}_A(M_j, M_i)$. Damit ist Multiplikation von Matrizen in B wohldefiniert. Für diese Operationen müssen wir nun die Axiome aus Definition 1.1 für die Menge B nachprüfen. Da die Menge $\mathrm{Hom}_A(M_j, M_i)$ abgeschlossen ist bezüglich Addition und Skalarmultiplikation, ist $\mathrm{Hom}_A(M_j, M_i)$ ein K-Vektorraum. Dies impliziert, dass die Menge B ein K-Vektorraum (und damit auch abelsche Gruppe) ist. Da Komposition von Abbildungen assoziativ ist, hat die abelsche Gruppe B auch eine Multiplikation, die assoziativ ist, somit ist B ein Ring. Skalare kommutieren mit allen Elementen aus B, also ist B eine Algebra über dem Körper K. □

Theorem 4.20. *Sei A eine K-Algebra. Sei M ein A-Modul mit der Modulzerlegung $M = M_1 \oplus \ldots \oplus M_n$. Dann sind die beiden folgenden K-Algebren isomorph:*

$$\mathrm{End}_A(M) = \{f : M \to M \mid f \textit{ ist } A\textit{-Modulhomomorphismus}\} \simeq B,$$

mit Algebra B wie in Lemma 4.19.

Beweis. Der Beweis ist länglich, aber ohne Überraschungen.

a) Da M ein A-Modul ist, ist M ein K-Vektorraum und $\mathrm{End}_K(M)$ eine K-Algebra, siehe Beispiel 1.4 b). Es ist $\mathrm{End}_A(M) \leq \mathrm{End}_K(M)$ Unterraum mit $\mathrm{id}_M \in \mathrm{End}_A(M)$. Da Addition und Komposition von A-Modulhomomorphismen wieder ein A-Modulhomomorphismus ist, ist $\mathrm{End}_A(M)$ eine Teilalgebra der Algebra $\mathrm{End}_K(M)$, siehe Definition 1.12.

b) Wir betrachten Elemente $m \in M$ als n-Tupel: $m = (m_1, \ldots, m_n)$ mit $m_i \in M_i$ für $1 \leq i \leq n$. Sei $\pi_i : M \to M_i$ die natürliche Projektion mit $\pi_i(m) = m_i$ und $\kappa_i : M_i \to M$ Einbettung mit $\kappa_i(m_i) = (0, \ldots, 0, m_i, 0 \ldots, 0)$ mit m_i in der

$i$ten Koordinate. Nach Beispiel 2.25 sind π_i und κ_i A-Modulhomomorphismen und es gilt:

$$\sum_{i=1}^{n} \kappa_i \pi_i(m) = \sum_{i=1}^{n} \kappa_i(m_i) = \sum_{i=1}^{n} (0 \ldots 0, m_i, 0, \ldots 0) = (m_1, \ldots, m_n) = m.$$

Also ist $\sum_{i=1}^{n} \kappa_i \pi_i = \mathrm{id}_M$.

c) Definiere $\psi : \mathrm{End}_A(M) \to B$ durch $f \mapsto (f_{ij})$ mit $f_{ij} := \pi_i \circ f \circ \kappa_j$. Die Komposition von A-Modulhomomorphismen ist wieder ein A-Modulhomomorphismus. Damit ist $f_{ij} \in \mathrm{Hom}_A(M_j, M_i)$, das heisst, die Abbildung ψ ist wohldefiniert. Wir zeigen im Folgenden, dass ψ ein Isomorphismus von Algebren ist:

   Um die Abbildungen summieren zu können, fassen wir die Abbildungen $f_{ij} : M_j \to M_i$ auch auf als Abbildungen $f_{ij} : M \to M$, wobei Elemente aus M_l auf Null abgebildet werden für $l \neq j$. Dann gilt:

$$\begin{aligned} \sum_{i,j} f_{ij} &= \sum_i \sum_j \pi_i \circ f \circ \kappa_j = \sum_i \pi_i \circ f \circ (\sum_j \kappa_j) \\ &= \sum_i \pi_i \circ f \circ \mathrm{id}_M = (\sum_i \pi_i) \circ f = \mathrm{id}_M \circ f = f. \end{aligned} \tag{4.10}$$

   Damit können wir nun zeigen, dass ψ bijektiv ist. Sei $(f_{ij}) = \psi(f) = 0$. Dann sind die Abbildungen $f_{ij} = 0$. Mit (4.10) folgt $f = \sum_{ij} f_{ij} = 0$ ist. Also ist die Abbildung ψ injektiv. Um Surjektivität von ψ zu zeigen, wählen wir ein Element $(f_{ij}) \in B$. Die Abbildungen π_s beziehungsweise κ_t entsprechen der Identität auf M_s beziehungsweise M_t, und Null sonst. Daher ist

$$\pi_s \circ f_{ij} \circ \kappa_t = \begin{cases} 0 & \text{falls } t \neq j \text{ oder } i \neq s, \\ f_{ij} & \text{falls } t = j \text{ und } i = s. \end{cases}$$

   Definiere $g := \sum_{i,j} f_{ij}$. Nach (4.10) gilt $g = f$ mit $\psi(g) = (g_{ij}) = (f_{ij})$, das heisst die Abbildung ψ ist surjektiv.

d) Zu zeigen bleibt, dass die Abbildung ψ ein Algebrenhomomorphismus ist: Es ist $(\mathrm{id}_M)_{ij} = \pi_i \circ \mathrm{id}_M \circ \kappa_j$ gleich der Identität id_{M_i} falls $i = j$ ist, und die Abbildung ist gleich der Nullabbildung sonst. Damit ist $\psi(\mathrm{id}_M) = I_n = 1_B$. Die Abbildung ψ bildet also das Einselement aus der Algebra $\mathrm{End}_A(M)$ auf das Einselement von B ab. Ausserdem gilt:

$$\psi(\lambda f + g) = (\lambda \cdot f_{ij} + g_{ij}) = \lambda(f_{ij}) + (g_{ij}) = \lambda\psi(f) + \psi(g),$$

   für alle $f, g \in \mathrm{End}_A(M)$ und $\lambda \in K$. Damit ist ψ eine K-lineare Abbildung. Die Abbildung ist auch multiplikativ: es ist $\psi(f) \cdot \psi(g) = (f_{ij}) \cdot (g_{ij}) = (h_{ij})$ mit

$$\begin{aligned} h_{ij} &= \sum_l f_{il} \circ g_{lj} = \sum_l (\pi_i \circ f \circ \kappa_l) \circ (\pi_l \circ g \circ \kappa_j) \\ &= \pi_i \circ f \circ (\sum_l \kappa_l \circ \pi_l) \circ g \circ \kappa_j \overset{b)}{=} \pi_i \circ f \circ \mathrm{id}_M \circ g \circ \kappa_j = (f \circ g)_{ij}. \end{aligned}$$

   Damit ist $\psi(f \circ g) = \psi(f)\psi(g)$, also ψ ein Algebren-Isomorphismus. □

Ab dieser Stelle arbeiten wir mit einem algebraisch abgeschlossenen Körper K. Dies liegt daran, dass wir Schurs Lemma 3.10 anwenden wollen.

Korollar 4.21. *Sei K algebraisch abgeschlossen, beispielsweise $K = \mathbb{C}$. Sei A eine halbeinfache K-Algebra mit ${}_AA = S_1^{n_1} \oplus \ldots \oplus S_t^{n_t}$, wie in Bemerkung 4.18. Dann ist*

$$\mathrm{End}_A(A) \simeq M_{n_1}(K) \times \ldots \times M_{n_t}(K).$$

Beweis. Wir wenden Schurs Lemma 3.10 an, sowie Theorem 4.20. Nach Voraussetzung ist die Algebra A halbeinfach. Damit ist nach 4.12 der reguläre Modul halbeinfach, also eine direkte Summe von einfachen Moduln. Sei $\{S_1, \ldots, S_t\}$ ein Repräsentantensystem der Isomorphieklassen einfacher A-Moduln und sei ${}_AA = S_1^{n_1} \oplus \ldots \oplus S_t^{n_t}$ mit $n_i \in \mathbb{N}$ für $1 \le i \le t$, siehe Bemerkung 4.18. Nach Schurs Lemma 3.10 ist

$$\mathrm{Hom}_A(S_i, S_j) \simeq \begin{cases} K & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Damit ist

$$\begin{aligned} \mathrm{End}_A({}_AA) &= \mathrm{End}_A(\bigoplus_{i=1}^{t} S_i^{n_i}) \overset{4.20}{\simeq} \begin{pmatrix} M_{n_1}(K) & 0 & \ldots & 0 \\ 0 & M_{n_2}(K) & \ldots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & M_{n_t(K)} \end{pmatrix} \\ &= M_{n_1}(K) \times \ldots \times M_{n_t}(K). \end{aligned}$$

□

Wir erinnern an das Resultat in Aufgabe 2.9: Ist A eine K-Algebra mit beliebigem Körper K. Dann ist $A \simeq \mathrm{End}_A(A)^{\mathrm{op}}$, als Algebren. Damit erhalten wir:

Theorem 4.22 (Wedderburn's Theorem)**.** *Sei K ein algebraisch abgeschlossener Körper und A eine Algebra über dem Körper K. Dann ist A genau dann halbeinfache Algebra, wenn gilt*

$$A \simeq M_{n_1}(K) \times \ldots \times M_{n_t}(K).$$

Die Matrixalgebren $M_{n_i}(K)$ heissen die Wedderburnkomponenten *der Algebra A. Es ist hierbei*

$$t = \text{ Anzahl der Isomorphieklassen einfacher } A\text{-Moduln,}$$

und falls S_i einfacher A-Modul korrespondierend zur Wedderburnkomponente $M_{n_i}(K)$ ist, dann gilt $\dim S_i = n_i$ und ${}_AA \simeq S_1^{n_1} \oplus \cdots \oplus S_t^{n_t}$.

Beweis. Nach Beispiel 4.17 ist die Algebra $M_{n_1}(K) \times \ldots \times M_{n_t}(K)$ eine halbeinfache Algebra, und damit nach Korollar 4.16 a) auch jede zu ihr isomorphe Algebra A. Sei nun A eine halbeinfache Algebra, und sei $\{S_1, \ldots, S_t\}$ ein Repräsentantensystem der Isomorphieklassen der einfachen A-Moduln. Dann ist nach Definition 4.12 der reguläre Modul halbeinfach und nach Bemerkung 4.18 existieren eindeutige natürliche Zahlen $n_i > 0$ mit

$${}_AA = S_1^{n_1} \oplus \ldots \oplus S_t^{n_t}.$$

Die entgegengesetzte Algebra wurde in Beispiel 1.7 definiert. Transponieren von Matrizen liefert einen Algebrenisomorphismus $M_n(K)^{\mathrm{op}} \simeq M_n(K)$. Ausserdem gilt für das kartesische Produkt zweier Algebren $(A_1 \times A_2)^{\mathrm{op}} \simeq A_1^{\mathrm{op}} \times A_2^{\mathrm{op}}$. Es folgt die folgenden Folge von Algebrenisomorphismen:

$$\begin{aligned} A &\overset{1.7}{=} (A^{\mathrm{op}})^{\mathrm{op}} \overset{2.9}{\simeq} \mathrm{End}_A(A)^{\mathrm{op}} \\ &\overset{4.21}{\simeq} (M_{n_1}(K) \times \ldots \times M_{n_t}(K))^{\mathrm{op}} \\ &\simeq M_{n_1}(K)^{\mathrm{op}} \times \ldots \times M_{n_t}(K)^{\mathrm{op}} \\ &\simeq M_{n_1}(K) \times \ldots \times M_{n_t}(K). \end{aligned}$$

Die einfachen Moduln der Algebra $M_{n_1}(K) \times \ldots \times M_{n_t}(K)$ erhalten wir nach Proposition 3.17 gerade durch Inflation der einfachen $M_{n_i}(K)$-Moduln K^{n_i}. Für $1 \le i \le t$ existiert also jeweils ein einfacher A-Modul S_i der Dimension $\dim S_i = n_i$ korrespondierend zum einfachen $M_{n_i}(K)$-Modul K^{n_i}, und dieser kommt nach Beispiel 3.22 genau n_i-mal als direkter Summand von ${}_AA$ vor. □

Aufgabe 4.12. Eine halbeinfache Algebra A über einem algebraisch abgeschlossenen Körper K ist genau dann kommutativ, wenn die Anzahl der Kompositionsfaktoren des regulären Moduls ${}_AA$ mit der Anzahl der Isomorphieklassen einfacher A-Moduln übereinstimmt.

Bemerkung 4.23. Sei A eine Algebra und S ein einfacher A-Modul. Nach Lemma 3.9, dem Lemma von Schur in allgemeiner Form, ist der Endomorphismenring $\mathrm{End}_A(S)$ ein Schiefkörper, das heisst, alle Körperaxiome gelten, ausser, dass die Multiplikation nicht kommutativ sein muss. Arbeitet man in der obigen Klassifikation der halbeinfachen Algebren über einem beliebigen statt über einem algebraisch abgeschlossenen Körper K, so erhält man statt der Matrixalgebra $M_{n_i}(K)$ stattdessen die Matrixalgebra $M_{n_i}(\mathrm{End}_A(S_i))$, also eine Matrixalgebra über dem Schiefkörper $\mathrm{End}_A(S_i)$. Entsprechend kann man den Satz von Wedderburn auch allgemeiner formulieren und erhält: Jede halbeinfache Algebra über einem Körper K ist isomorph zu einem direkten Produkt von Matrixalgebren über Schiefkörpern $D_1, \ldots, D_t$, wobei $K \le D_i$ Teilring ist für alle $1 \le i \le t$.

Aufgabe 4.13. Ist $\mathbb{C}$ eine halbeinfache $\mathbb{R}$-Algebra? Ist $\mathbb{C}$ eine halbeinfache $\mathbb{C}$-Algebra? Wenn ja, wie sehen die Wedderburnkomponenten aus?

Mit dem Satz von Wedderburn 4.22 haben wir nun halbeinfache Algebren klassifiziert. Es bleibt die Frage offen, wann eine konkret gegebene Algebra halbeinfach ist. Im Fall der Gruppenalgebren gibt der Satz von Maschke eine schöne Antwort, siehe Vorlesung Algebra II beziehungsweise vielleicht bei Zeiten in einem Appendix zu diesem Skript.

Theorem 4.24 (Maschke)**.** *Sei K ein Körper und G eine endliche Gruppe. Dann ist die Algebra KG genau dann halbeinfach, wenn die Charakteristik des Körpers K kein Teiler der Ordnung der Gruppe G ist. In diesem Sinne sind also alle Gruppenalgebren $\mathbb{C}G$ halbeinfache Algebren.*

Aufgabe 4.14.

a) Bestimmen Sie die Wedderburnkomponenten der halbeinfachen Algebren $\mathbb{C}C_n$, $\mathbb{C}V_4$, $\mathbb{C}S_3$ und $\mathbb{C}D_8$. Beachten Sie hierzu die Korrektur des Skriptes am Ende von Beispiel 3.5.

b) Zeigen Sie, dass die Gruppe G abelsch ist, genau dann, wenn alle einfachen $\mathbb{C}G$-Moduln eindimensional sind.

Ein Ring R heisst *einfach*, wenn 0 und R die einzigen Ideale sind. Eine Algebra A heisst *einfach*, wenn A als Ring einfach ist.

Aufgabe 4.15. Zeigen Sie die folgenden Aussagen:

a) Die Wedderburnkomponenten einer Algebra A sind einfache Algebren.

b) Ein endliches Produkt endlich-dimensionaler einfacher K-Algebren ist halbeinfach.

Hinweis zu b): der Sockel des regulären Moduls ist ein zweiseitiges Ideal.

Aufgabe 4.16. Wahr oder falsch? Begründen Sie jeweils Ihre Antworten.

a) Ein Algebrenhomomorphismus zwischen einfachen K-Algebren ist immer injektiv.

b) Sei A halbeinfache Algebra, B eine K-Algebra und $f : A \to B$ ein surjektiver Algebrenhomomorphismus. Dann ist die Algebra B isomorph zu einem direkten Summanden der Algebra A und der Kern von f ist ebenfalls als Algebra ein direkter Summand der Algebra A.

c) Jede endlich-dimensionale Algebra über einem Körper K ist Teilalgebra einer einfachen K-Algebra.

4.4 Das Jacobson-Radikal einer Algebra

Definition 4.25. Sei A eine K-Algebra. Das *(Jacobson-)Radikal* $J(A)$ von A ist definiert als der Schnitt aller maximalen Linksideale von A:

$$J(A) := \bigcap_{I \triangleleft_l A \text{ max}} I.$$

Bemerkung 4.26. Zu dieser Definition gibt es einige Anmerkungen:

a) Das Jacobson-Radikal ist als Linksideal definiert. Wir zeigen in Theorem 4.29, dass das Jacobson-Radikal ein zweiseitiges Ideal ist. Ganz analog kann man das Jacobson-Radikal auch als Rechtsideal definieren. Die beiden Definitionen stimmen dann überein.

b) Das Jacobson-Radikal kann man ganz analog auch für Ringe definieren. Maximale Ideale existieren in Ringen und jedes Linksideal ist in einem maximalen Linksideal enthalten. Im Allgemeineren, bei Ringen, benötigt man für den Beweis Zorns Lemma, siehe Algebra-Skript Henke SS2017, Kapitel 15. Wir machen den Beweis hier für endlich-dimensionale Algebren:

   Ist J Linksideal in A, so ist entweder J maximal, oder es existiert ein Linksideal J_1 von A mit $J \subsetneq J_1 \subsetneq A$. Entweder J_1 ist maximales Linksideal in A, oder es existiert ein Linksideal J_2 in A mit $J \subsetneq J_1 \subsetneq J_2 \subsetneq A$. Und so weiter. Ideale in einer Algebra (anders als im Ring) haben eine Vektorraumstruktur. Da A eine endlich-dimensionale Algebra ist, sind alle Linksideale von A endlich-dimensionale Untervektorräume mit

$$\dim J < \dim J_1 < \dim J_2 < \ldots < \dim A < \infty.$$

   Da die Dimension des Ideals in jedem Schritt strikt wächst und nach oben durch $\dim A$ beschränkt ist, existiert ein maximales Linksideal J_n in A mit $J \subsetneq J_n \subsetneq A$. Vergleichen Sie mit der Lösung zu Aufgabe 4.3.

c) Nach Definition 4.3 des Radikals eines Linksmoduls entspricht das Radikal des regulären Moduls gerade dem Jacobson-Radikal:

$$\begin{aligned} \operatorname{rad}({}_A A) &= \bigcap \text{ aller maximalen Untermoduln des regulären Moduls } {}_A A \\ &\overset{2.19b)}{=} \bigcap \text{ aller maximalen Linksideale der Algebra A} \\ &= J(A). \end{aligned}$$

   Wir schreiben statt $J(A)$ daher auch $\operatorname{rad} A$.

d) Eine Algebra A ist genau dann halbeinfach, wenn $J(A) = 0$ ist: Angenommen A ist halbeinfache Algebra, so ist nach Definition 4.2 der reguläre A-Modul halbeinfach und mit Theorem 4.5 folgt, dass $J(A) = \operatorname{rad}({}_A A) = 0$ ist. Umgekehrt, sei $J(A) = 0$. Dann ist $\operatorname{rad}({}_A A) = 0$ und entsprechend ist nach Theorem 4.5 der reguläre A-Modul halbeinfach. Mit Theorem 4.14 folgt, dass A eine halbeinfache Algebra ist.

Aufgabe 4.17. Zeigen Sie mit Hilfe des Satzes von Jordan-Hölder, dass das Jacobson-Radikal ein Schnitt von endlich vielen maximalen Linksidealen ist.

Beispiel 4.27. Wir wollen einige Jacobson-Radikale berechnen:

a) Körper besitzen keine echten, nicht-trivialen Ideale. Da Körper kommutativ sind, entsprechen Linksideale gerade zweiseitigen Idealen. Also ist 0 das einzige maximale Ideal eines Körpers K und $\operatorname{rad} K = 0$.

b) Die Algebra $A = M_2(K)$ ist nach Beispiel 4.15 eine halbeinfache Algebra. Nach Definition 4.12 ist der reguläre A-Modul also halbeinfach. Nach Theorem 4.5 und Bemerkung 4.26 b) ist damit $J(A) = 0$.

c) Sei $A = T_2(K)$ die Algebra der oberen Dreiecksmatrizen. Die erste Zeile $KE_{11} + KE_{12} \subseteq A$ ist ein maximales Ideal in A, auch die zweite Spalte $KE_{12} + KE_{22} \subseteq A$ ist ein maximales Ideal in A, denn beides sind Ideale maximaler Dimension in A. Der Schnitt dieser beiden maximalen Ideale ist KE_{12}. Also ist das Radikal von A entweder Null oder diese rechte obere Ecke KE_{12}. Radikal Null bedeutet nach Theorem 4.5, dass ${}_AA$ halbeinfach ist. Aufgabe 3.8 b) impliziert aber, dass der reguläre A-Modul kein halbeinfacher Modul ist: In der zu A isomorphen Wegealgebra ist der einfache Modul $S(2)$ kein Untermodul des regulären Moduls, und damit erst recht kein direkter Summand des regulären Moduls. Aus dem Satz von Jordan-Hölder 3.21 sowie Theorem 3.30 folgt, dass der reguläre Modul nicht halbeinfach ist.

d) Wir lösen Aufgabe 4.4 und berechnen das Radikal von $K[X]$. Hierzu nutzen wir Resultate aus der Vorlesung Algebra I. Sei $A = K[X]$ der Polynomring in einer Variablen X. Für $\lambda \in K$ ist das Polynom $X - \lambda \in K[X]$ irreduzibel. Damit ist das von $X-\lambda$ erzeugte Ideal $(X-\lambda) \triangleleft K[X]$ maximal. Angenommen $f \in K[X]$ mit $f \in \bigcap_{\lambda \in K}(X - \lambda)$, dann ist $f \in (X - \lambda)$, also $X - \lambda$ ein Teiler von f, für jedes Element $\lambda \in K$. Hat der Körper K unendlich viele Elemente, so folgt aus Gradbetrachtungen des Polynoms f, dass $f = 0$. Damit folgt $J(K[X]) \subseteq \bigcap_{\lambda \in K}(X - \lambda) = 0$. Ist der Körper K endlich, so gilt ebenfalls $J(K[X]) = 0$. Hierzu muss man zeigen, dass der Polynomring $K[X]$ eines endlichen Körpers unendlich viele irreduzible Polynome enthält, und damit folgt dann die Behauptung analog wie im Fall K unendlich.

Bemerkung 4.28. Seien I, J Linksideale in einer Algebra A. Dann ist auch das Produkt $I \cdot J := K\text{-Span}\{ij \mid i \in I \text{ und } j \in J\}$ ein Linksideal in A. Ist M ein A-Linksmodul und I ein Linksideal in A, so ist $I \cdot M$ ein A-Untermodul von M und durch wiederholtes Multiplizieren erhält man eine Folge von Untermoduln $\ldots \subseteq I^2M \subseteq IM \subseteq M$. Der Modul M kann hierbei als Spezialfall natürlich selber auch ein Linksideal von A sein. Ist $M = J$ nun ein zweiseitiges Ideal, so heisst J *nilpotent*, falls es ein n gibt mit $0 = J^n = \{\sum i_1 \cdots i_n \mid i_j \in J\}$, wobei die Summen in der letzten Menge beliebige endliche Summen sind.

Theorem 4.29. *Sei A eine endlich-dimensionale Algebra über einem Körper K. Dann gilt:*

a) Es ist

$$\begin{aligned} J(A) &= \{a \in A \mid aS = 0 \text{ für alle einfachen } A\text{-Moduln } S\} \\ &= \bigcap_{S \text{ einfach}} Ann(S); \end{aligned}$$

insbesondere ist $J(A)$ ein Schnitt von endlich vielen maximalen Linksidealen beziehungsweise Untermoduln von A.

b) Das Jacobson-Radikal ist ein zweiseitiges Ideal: $J(A) \triangleleft_2 A$.

c) Das Jacobson-Radikal enthält jedes nilpotente Ideal und ist selber nilpotent, das heisst, $J(A)$ ist das grösste nilpotente Ideal in A.

Beweis.

a) Sei $a \in J(A)$. Angenommen es existiert ein einfacher Modul S mit $aS \neq 0$. Dann existiert ein Element $0 \neq s \in S$ mit $as \neq 0$. Nach Definition 4.25 ist $J(A) \triangleleft_l A$ ein Linksideal, insbesondere ist also $A \cdot J(A) \subseteq J(A)$. Hiermit folgt, dass $0 \neq J(A) \cdot s$ Untermodul von S ist. Da S ein einfacher Modul ist, folgt $J(A) \cdot s = S$. Es existiert also ein $x \in J(A)$ mit $x \cdot s = s$, beziehungsweise $(x-1)s = 0$. Auf der einen Seite ist $x - 1 \in \mathrm{Ann}(s) = \{a \in A \mid as = 0\} \triangleleft_l A$, und letzteres ist wegen $xs \neq 0$ ein echtes Ideal in A. Da jedes Linksideal nach 4.26 in einem maximalen Linksideal von A liegt, existiert ein maximales Linksideal M mit $x - 1 \in \mathrm{Ann}\{s\} \subseteq M$. Nach Konstruktion ist $x \in J(A)$. Mit Definition 4.25 folgt $x \in J(A) \overset{4.25}{\subseteq} M$. Es sind also x und $x-1$ Elemente in M, und da M als Linksideal insbesondere auch eine Gruppe bezüglich Addition ist, folgt $1 = x - (x-1) \in M$ und damit $M = A$. Dies ist ein Widerspruch zu M maximales Linksideal in A. Es folgt, für alle einfachen Moduln S gilt $a \cdot S = 0$. Damit haben wir $\subseteq$ in der ersten Mengengleichung in Aussage a) gezeigt.

Für die umgekehrte Inklusion $\supseteq$ nehmen wir an, dass $a \in A$ ist mit $aS = 0$ für alle einfachen A-Moduln S. Sei $M \triangleleft A$ maximales Linksideal. Dann ist nach Bemerkung 3.26 der Quotientenmodul A/M einfach und nach Voraussetzung ist damit $a \cdot A/M = 0$. Dies impliziert $a + M = a(1 + M) = 0 + M$, also ist $a \in M$. Da M in diesem Argument ein beliebiges maximales Ideal in A war, ist somit a im Schnitt aller maximalen Ideale von A, das heisst $a \in J(A)$. Damit ist die umgekehrte Inklusion $\supseteq$ in der ersten Mengengleichheit in Aussage a) gezeigt.

Die zweite Mengengleichung in Aussage a) folgt direkt aus Aufgabe 3.11. Isomorphe Modul haben den gleichen Annulator. Nach den Argumenten oben ist $a \in J(A)$ genau dann, wenn $a \in \mathrm{Ann}(S)$, für alle einfachen A-Moduln S ist. Das passiert also genau dann, wenn a im Schnitt aller Annulatoren ist.

b) Nach Definition ist $J(A)$ ein Linksideal in A. Sei S einfacher A-Modul, sei $a \in A$ und $x \in J(A)$. Dann ist $(xa)S = x(aS) \subseteq xS = 0$ nach a). Es folgt, dass $xa \in J(A)$ ist nach a). Also ist $J(A)$ auch ein Rechtsideal in A.

c) Sei $I \triangleleft_2 A$ ein zweiseitiges nilpotentes Ideal in A mit $I^n = 0$. Sei S ein einfacher A-Modul und $0 \neq s \in S$. Dann ist $Is \subseteq As \subseteq S$ mit $A(Is) = (AI)s \subseteq Is$, denn I ist ein Ideal in A. Also ist Is ein Untermodul des einfachen Moduls S. Angenommen $Is \neq 0$. Dann ist $Is = S$, das heisst, es existiert ein Element $x \in I$ mit $xs = s$. Es folgt, dass $x^n s = s$ ist, und damit ist $x^n \neq 0$, ein Widerspruch zu $I^n = 0$. Also ist $Is = 0$ für alle $s \in S$, beziehungsweise $IS = 0$. Da S ein beliebiger einfacher A-Modul ist, folgt $IS = 0$ für alle einfachen A-Moduln S. Nach a) ist damit $I \subseteq J(A)$.

Sei $0 = A_0 \subseteq A_1 \subseteq \ldots \subseteq A_t = {}_A A$ eine Kompositionsreihe des regulären A-Moduls. Die Kompositionsfaktoren A_i/A_{i-1} sind einfache A-Moduln, daher ist $x \cdot A_i/A_{i-1} = 0$ für alle $x \in J(A)$ nach a). Sei $a \in A_i$, dann ist

$$0 + A_{i-1} = x \underbrace{(a + A_{i-1})}_{\in A_i/A_{i-1}} = xa + A_{i-1}.$$

Es folgt $xa \in A_{i-1}$ beziehungsweise $xA_i \subseteq A_{i-1}$ für alle $1 \leq i \leq t$ und alle $x \in J(A)$. Wir wenden die letzte Inklusion mehrfach an. Beispielsweise ist $x_t A \subseteq A_{t-1}$. Es folgt für $x_1, \dots, x_t \in J(A)$:

$$x_1 \cdots x_{t-1}(x_t A) \subseteq x_1 \cdots x_{t-1} A_{t-1} \subseteq \ldots \subseteq x_1 A_1 \subseteq A_0 = 0.$$

Es ist also $x_1 \cdots x_t A = 0$, und benutzen wir $1 \in A$, so gilt insbesondere $x_1 \cdots x_t = 0$. Damit ist ein beliebiges Produkt von t Elementen aus $J(A)$ immer Null, das heisst $J(A)^t = 0$. Dies zeigt, dass das Jacobson-Radikal ein nilpotentes Ideal ist. Da wir oben gezeigt haben, dass jedes nilpotente Ideal im Jacobson-Radikal enthalten ist, folgt dass $J(A)$ das grösste nilpotente Ideal in A ist. □

Aufgabe 4.18. Berechnen Sie die Jacobson-Radikale für die Algebren $M_n(K)$ und $T_n(K)$ unter Benutzung von Theorem 4.29.

In Theorem 3.30 haben wir gesehen, dass wir – bis auf Isomorphie – alle einfachen A-Moduln konstruieren können, indem wir die Kompositionsfaktoren des regulären A-Moduls konstruieren. Das folgende Korollar gibt eine alternative Methode zur Konstruktion der Isomorphieklassen einfacher A-Moduln:

Korollar 4.30. *Sei A eine endlich-dimensionale K-Algebra. Definiere die Algebra $\bar{A} := A/J(A)$. Dann ist $\bar{A}$ eine halbeinfache Algebra. Der A-Modul $\bar{A}$ ist ein halbeinfacher A-Modul und jeder einfache A-Modul ist zu mindestens einem Summanden dieses Moduls isomorph.*

Beweis. Wir benutzen wiederholt Inflation zwischen A und $\bar{A}$-Moduln, siehe Bemerkung 3.16.

a) Das Jacobson-Radikal ist gleich dem Radikal des regulären Moduls, siehe Bemerkung 4.26. Es ist

$$J(\bar{A}) \overset{4.26}{=} \operatorname{rad}({}_{\bar{A}}\bar{A}) \overset{\text{Infl}}{=} \operatorname{rad}({}_{A}\bar{A}) = \operatorname{rad}({}_{A}(A/\operatorname{rad} A)) \overset{4.8}{=} 0,$$

denn der Untermodulverband der Moduln ${}_{\bar{A}}\bar{A}$ und ${}_{A}\bar{A}$ ist gleich. Die Algebra $\bar{A}$ ist nach Theorem 4.14 also halbeinfach. Nach Theorem 4.5 existieren also einfache $\bar{A}$-Moduln mit

$$\bar{A} = S_1 \oplus \ldots \oplus S_n, \tag{4.11}$$

und nach Theorem 3.30 und dem Satz von Jordan-Hölder 3.21 kommt – bis auf Isomorphie – jeder einfache $\bar{A}$-Modul in einer solchen Zerlegung vor. Mittels Inflation ist dies auch eine Zerlegung in einfache A-Moduln.

b) Sei nun S ein einfacher A-Modul. Es gilt $J(A) \cdot S = 0$ nach Theorem 4.29. Mittels Inflation folgt, dass S ein einfacher $\bar{A}$-Modul ist. Nach a) kommt damit ${}_{\bar{A}}S$ bis auf Isomorphie in der Zerlegung (4.11) vor, das heisst, es existiert ein Index i mit $S \simeq S_i$ als $\bar{A}$-Modul beziehungsweise A-Modul. □

Aufgabe 4.19. Nach Aufgabe 4.17 (oder Theorem 4.29) ist das Jacobson-Radikal der Schnitt von endlich vielen maximalen Linksidealen M_i, mit $1 \leq i \leq t$. Angenommen es gilt hierbei für alle i, dass $\bigcap_{j \neq i} M_j \nsubseteq M_i$ ist. Zeigen Sie, dass die Abbildung

$$\phi : A/J(A) \to A/M_1 \oplus \ldots \oplus A/M_t, \text{ mit } x + J(A) \mapsto (x + M_1, \ldots, x + M_t)$$

ein wohldefinierter A-Modulisomorphismus ist. Was folgt für die Algebra $\bar{A}$?

Wir wollen die Stärke der beschriebenen mathematischen Konzepte am Beispiel der endlich-dimensionalen Wegealgebren demonstrieren. Hierzu berechnen wir als erstes das Jacobson-Radikal mit Hilfe von Theorem 4.29:

Beispiel 4.31. Sei $A = KQ$ eine endlich-dimensionale Wegealgebra mit Köcher Q, das heisst der Köcher Q hat nach Proposition 1.27 keine Schleifen und Zykel. Dann ist das Jacobson-Radikal der Wegealgebra KQ gerade

$$\begin{aligned} J(A) &= K\text{-Span}\{\text{Wege in } Q \text{ der Länge} \geq 1\} \\ &= \text{Ideal in } KQ \text{ erzeugt von allen Wegen der Länge} \geq 1 =: KQ_{\geq 1}, \end{aligned}$$

siehe Aufgabe 3.12. Diese Aussage gilt nicht für unendlich-dimensionale Wegealgebren: Die Wegealgebra KQ_a ist nach Beispiel 1.29 isomorph zur Algebra $K[X]$, wobei Q_a der Köcher mit einem Punkt 1 und einem Pfeil α ist. Der Pfeil α entspricht also einer Schleife am Punkt 1. Das Radikal von $K[X]$ ist nach Beispiel 4.27 Null. Es gilt also Radikal $J(KQ_a) = 0 \neq (\alpha) = (KQ_a)_{\geq 1}$.

Beweis. Nach Definition ist $I := KQ_{\geq 1} := K\text{-Span}\{\text{Wege in } Q \text{ der Länge} \geq 1\}$ ein Vektorraum. Sei p ein Weg in $KQ_{\geq 1}$ der Länge l und sei a ein Element der Algebra KQ, so ist ap beziehungsweise pa entweder Null oder eine Summe von Wegen der Länge mindestens l, also sind ap und pa Elemente in $KQ_{\geq 1}$. Damit ist der Vektorraum $KQ_{\geq 1}$ ein zweiseitiges Ideal in der Wegealgebra KQ, nämlich das von allen Wegen positiver Länge erzeugte Ideal in KQ. Definiere für $i \in Q_0$ die zweiseitigen Ideale

$$M_i := K\text{-Span}\{\text{alle Wege in } Q, \text{ nicht aber der eine faule Weg } e_i\}.$$

Nach Konstruktion ist Dimension $\dim M_i = \dim(KQ) - 1$, also ist M_i ein maximales Ideal in A. Es folgt:

$$J(A) \overset{4.25}{=} \bigcap \text{aller maximaler Linksideale in } A \subseteq \bigcap_{i \in Q_0} M_i = I. \tag{4.12}$$

Da A eine endlich-dimensionale Algebra ist, enthält der Köcher Q keine Schleifen oder Zykel. Sei n die Länge des längsten Weges im Köcher Q. Dann ist $I^{n+1} = 0$. Also ist I ein nilpotentes Ideal. Nach Theorem 4.29 ist also $I \subseteq J(A)$, dem grössten nilpotenten Ideal von A. Mit der Inklusion in (4.12) folgt Gleichheit. □

Die Folgen für Wegealgebren, die sich aus dieser Rechnung ergeben, halten wir in einem Theorem fest. Vergleichen Sie diese Resultate auch mit Ihren Ergebnissen in Aufgabe 2.21, wo eine alternative Klassifikation und Beschreibung der einfachen KQ-Moduln gegeben wird.

Theorem 4.32. *Sei $A = KQ$ endlich-dimensionale Wegealgebra mit Köcher Q.*

a) Das Jacobson-Radikal der Wegealgebra ist das Ideal $KQ_{\geq 1}$.

b) Die Wegealgebra KQ ist genau dann halbeinfach, wenn die Menge Q_1 der Pfeile des Köchers Q leer ist.

c) Die Wegealgebra KQ hat bis auf Isomorphie genau $|Q_0|$ einfache Moduln S_i, mit $i \in Q_0$. Hierbei ist $\dim S_i = 1$, der faule Weg e_i operiert durch die Identität auf den Vektoren in S_i, alle anderen Wege operieren durch Null.

Beweis. Das Radikal der Wegealgebra wurde bereits in Beispiel 4.31 berechnet. Nach Bemerkung 4.26 b) ist die Wegealgebra $A = KQ$ genau dann halbeinfach, wenn $KQ_{\geq 1} \overset{4.31}{=} J(A) = 0$ ist, und das passiert genau dann, wenn die Pfeilmenge Q_1 des Köchers Q leer ist. Die Algebra $\bar{A} = KQ/KQ_{\geq 1}$ ist in Korollar 4.30 beschrieben. Sie ist isomorph als Algebra zum kartesischen Produkt $\bigtimes_{i \in Q_0} K$. Eine explizite Zerlegung in eine direkte Summe einfacher Moduln ist $\bar{A} = \bigoplus_{i \in Q_0} K(e_i + KQ_{\geq 1})$ wobei e_i als Idetität auf $S_i := K(e_i + KQ_{\geq 1})$ operiert und alle anderen Pfeile und Wege durch Null. □

Beispiel 4.33. Wir betrachten den Fall der Wegealgebra isomorph zu $A := T_n(K)$, siehe Beispiel 1.30. Nach Aufgabe 4.18 besteht das Radikal $J(A)$ genau aus allen strikten oberen Dreiecksmatrizen und $A/J(A) \simeq K \times \ldots \times K$, mit $C + J(A) \mapsto (c_{11}, \ldots, c_{nn})$, wobei c_{ii} der i-te Diagonaleintrag der Matrix C ist. Also operiert $C \in T_n(K)$ auf dem Modul $S_i := K\text{-Span}\{v\}$ durch $C \cdot v := c_{ii} \cdot v$. Siehe auch Aufgabe 3.12.

Aufgabe 4.20. Sei K ein Körper. Bestimmen Sie mit den Methoden dieses Abschnittes jeweils das Radikal der folgenden Algebren: $\mathbb{Z}_2 C_2$, $\mathbb{Z}_2 V_4$, $K[X]/(X^n)$ sowie der Algebren

$$A_1 := \begin{pmatrix} K & K & K \\ 0 & K & 0 \\ 0 & 0 & K \end{pmatrix}, \quad A_2 := \begin{pmatrix} K & 0 & K \\ 0 & K & 0 \\ K & 0 & K \end{pmatrix}.$$

Welche der Algebren sind halbeinfach? Was sind die Dimensionen der einfachen Moduln der gegebenen Algebren? Konstruieren Sie bis auf Isomorphie die einfachen Moduln der gegebenen Algebren.

In Kapitel 4.3 haben wir den Sockel und das Radikal eines Moduls kennengelernt. Diese Konzepte wollen wir nun iterieren, um einen gegebenen Modul sowohl von unten als auch von oben in Schichten zu zerlegen. Dazu benötigen wir zunächst die folgende Proposition:

Proposition 4.34. *Sei M ein A-Modul. Dann gilt:*

a) $\operatorname{rad}(M) = \operatorname{rad}(A) \cdot M$,

b) $\operatorname{soc}(M) = \{u \in M \mid \operatorname{rad} A \cdot u = 0\}$.

Beweis.

a) Sei M ein A-Modul und V ein Untermodul von M mit M/V halbeinfach. Da M/V eine direkte Summe einfacher Moduln ist, und das Radikal alle einfachen Moduln annuliert, folgt aus Theorem 4.29 a), dass $\operatorname{rad}(A)\cdot M/V = 0$ ist. Es ist also $0 = a(u+V) = au + V$ für alle $a \in \operatorname{rad}(A)$ und $u \in M$, das heisst $au \in V$ beziehungsweise $\operatorname{rad}(A)\cdot M \subseteq V$. Wir wählen nun $V = \operatorname{rad}(M)$. Dann ist $\operatorname{rad}(A)\cdot M \subseteq \operatorname{rad}(M)$. Dies zeigt eine der beiden zu zeigenden Inklusionen.

   Es ist $\operatorname{rad}(A)\cdot(M/\operatorname{rad}(A)M) = \operatorname{rad}(A)M/\operatorname{rad}(A)M = 0$. Mittels Inflation ist damit der A-Modul $M/\operatorname{rad}(A)M$ auch ein $\bar{A} = A/\operatorname{rad}(A)$-Modul. Da $\bar{A}$ halbeinfache Algebra ist, folgt $M/\operatorname{rad}(A)M$ ist ein halbeinfacher Modul. Nach Proposition 4.8 ist $\operatorname{rad}(M)$ der kleinste Untermodul von M, so dass $M/\operatorname{rad}(M)$ halbeinfach ist. Also folgt $\operatorname{rad}(M) \subseteq \operatorname{rad}(A)M$.

b) Definiere $W := \{u \in M \mid \operatorname{rad}(A)\cdot u = 0\}$. Nach Theorem 4.5 ist $\operatorname{soc}(M)$ ein halbeinfacher Modul. Nach Theorem 4.29 a) ist somit $\operatorname{rad}(A)\cdot\operatorname{soc}(M) = 0$. Also ist $0 \neq \operatorname{soc}(M) \subseteq W$. Seien $u, v \in W$. Dann ist $au = 0 = av$ beziehungsweise $a(u \pm v) = 0$ für alle $a \in \operatorname{rad}(A)$. Damit ist $u \pm v \in W$, also W eine abelsche Gruppe. Sei $b \in A$ und $a \in \operatorname{rad}(A)$. Dann ist $a(bu) = (ab)u = 0$, denn $ab \in \operatorname{rad}(A)$, weil $\operatorname{rad}(A)$ ein Ideal ist. Also ist $bu \in W$. Damit ist W ein Untermodul von M. Aus der Definition von W folgt $0 = \operatorname{rad}(A)\cdot W \overset{a)}{=} \operatorname{rad}(W)$. Nach Theorem 4.5 ist damit W ein halbeinfacher Untermodul von M. Es ist $\operatorname{soc}(M)$ der grösste halbeinfache Untermodul von M, also ist $W \subseteq \operatorname{soc}(M)$. Dies zeigt die Aussage in b). $\square$

Aufgabe 4.21. Seien U_1, U_2 zwei A-Moduln. Aus Gleichung (4.8) wissen wir, dass der Sockel additiv ist, also $\operatorname{soc}(U_1 \oplus U_2) = \operatorname{soc}(U_1) \oplus \operatorname{soc}(U_2)$. Zeigen Sie, dass auch das Radikal additiv ist, also $\operatorname{rad}(U_1 \oplus U_2) = \operatorname{rad}(U_1) \oplus \operatorname{rad}(U_2)$ ist.

Bemerkung 4.35. Sei M ein A-Modul. Wir definieren die Radikalreihe und die Sockelreihe des Moduls M:

a) Es ist $\operatorname{rad}(M) \leq M$ ein Untermodul mit $M/\operatorname{rad}(M)$ halbeinfach nach Proposition 4.8. Wir erhalten die Radikalreihe des Moduls M durch Iterieren: Bilde das Radikal von Modul $\operatorname{rad}(M)$:

   $$\operatorname{rad}^2(M) := \operatorname{rad}(\operatorname{rad} M) = \operatorname{rad}(A)\cdot(\operatorname{rad} M) = \operatorname{rad}(A)\cdot\operatorname{rad}(A)\cdot M =: \operatorname{rad}^2(A)\cdot M.$$

   Es ist $\operatorname{rad}^2(M) \leq \operatorname{rad}(M)$ Untermodul mit $\operatorname{rad}(M)/\operatorname{rad}^2(M)$ halbeinfach nach Proposition 4.8. Allgemein $\operatorname{rad}^k(M) := (\operatorname{rad} A)^k \cdot M = \operatorname{rad}(\operatorname{rad}^{k-1}(M))$. Nach Theorem 4.29 ist $\operatorname{rad}(A)$ ein nilpotentes Ideal; es existiert also eine natürliche Zahl n mit $\operatorname{rad}^n(A) = 0$. Damit existiert auch eine (möglicherweise andere) natürliche Zahl n mit $\operatorname{rad}^n(M) = 0$. Sei n die kleinste natürliche Zahl mit $\operatorname{rad}^{n-1}(M) \neq 0$ und $\operatorname{rad}^n(M) = 0$. Die endliche Folge von Untermoduln

   $$M =: \operatorname{rad}^0(M) \supseteq \operatorname{rad}^1(M) \supseteq \ldots \supseteq \operatorname{rad}^{n-1}(M) \supseteq 0$$

   heisst die *Radikalreihe* von M und n heisst die *Länge* der Radikalreihe von M. Die Subquotienten $\operatorname{rad}^i(M)/\operatorname{rad}^{i+1}(M)$ aus der Radikalreihe sind nach

Konstruktion halbeinfach. Wir schreiben sie als direkte Summen einfacher Moduln $S_{i,j}$:

$$\begin{array}{rcl} M/\operatorname{rad}(M) & = & S_{1,1} \oplus \ldots \oplus S_{1,t_1} \\ \operatorname{rad}(M)/\operatorname{rad}^2(M) & = & S_{2,1} \oplus \ldots \oplus S_{2,t_2} \\ & \vdots & \\ \operatorname{rad}^{n-2}(M)/\operatorname{rad}^{n-1}(M) & = & S_{n-1,1} \oplus \ldots \oplus S_{n-1,t_{n-1}} \\ \operatorname{rad}^{n-1}(M) & = & S_{n,1} \oplus \ldots \oplus S_{n,t_n} \end{array}$$

Wir beschreiben den Modul M daher auch mit dem Bild

$$M = \begin{array}{l} S_{1,1}S_{1,2}\ldots S_{1,t_1} \\ S_{2,1}S_{2,2}\ldots S_{2,t_2} \\ S_{n-1,1}S_{n-1,2}\ldots S_{n-1,t_{n-1}} \\ S_{n,1}S_{n,2}\ldots S_{n,t_n} \end{array}$$

und bezeichnen dies auch als die *Radikalreihe* von M.

b) Der Sockel $\operatorname{soc}(M)$ ist nach Proposition 4.8 der grösste halbeinfache Untermodul von M. Wir erhalten die Sockelreihe von M durch Iterieren: Wenn M nicht halbeinfach ist, ist der Sockel von $M/\operatorname{soc}(M)$ nicht trivial, und wir bilden in diesem Fall erneut den Sockel, jetzt von $M/\operatorname{soc}(M)$. Nach der Untermodulkorrespondenz 2.27 angewandt auf die Projektion $M \to M/\operatorname{soc}(M)$ existiert zum Modul $\operatorname{soc}(M/\operatorname{soc}(M)) \leq M/\operatorname{soc}(M)$ ein Untermodul $\operatorname{soc}(M) \leq \operatorname{soc}^2(M) \leq M$ mit

$$\operatorname{soc}^2(M)/\operatorname{soc}(M) = \operatorname{soc}(M/\operatorname{soc}(M)).$$

(Zeichnen Sie sich das entsprechende Bild der Untermodulkorrespondenz.) Sei bereits der Untermodul $\operatorname{soc}^{n-1}(M) \leq M$ definiert. Mit dem obigen Argument folgt, dann existiert ein Untermodul $\operatorname{soc}^n(M)$ mit $\operatorname{soc}^{n-1}(M) \leq \operatorname{soc}^n(M) \leq M$, sodass

$$\operatorname{soc}^n(M)/\operatorname{soc}^{n-1}(M) = \operatorname{soc}(M/\operatorname{soc}^{n-1}(M)) \tag{4.13}$$

ist. Wir zeigen mit Induktion nach n, dass

$$\operatorname{soc}^n(M) = \{m \in M \mid \operatorname{rad}^n(A) \cdot m = 0\} : \tag{4.14}$$

Der Induktionsanfang für $n = 2$ enthält genau dieselben Argumente wie wir sie im Induktionsschritt verwenden. Wir machen deshalb gleich den Induktionsschritt, und überlassen es der Leserin, die Details für den Induktionsanfang auszuarbeiten. Angenommen wir wissen, dass Gleichung (4.14) für $n - 1$ gilt.

i) Der Sockel eines Moduls ist nach Theorem 4.5 immer ein halbeinfacher Modul. Aus (4.13) folgt, dass $\operatorname{soc}^n(M)/\operatorname{soc}^{n-1}(M)$ halbeinfach ist, also ist $\operatorname{rad}(A) \cdot (\operatorname{soc}^n(M)/\operatorname{soc}^{n-1}(M)) \overset{4.34}{=} 0$. Das Rechnen mit Nebenklassen impliziert also $\operatorname{rad}(A) \cdot \operatorname{soc}^n(M) \subseteq \operatorname{soc}^{n-1}(M)$. Multiplikation von links mit $\operatorname{rad}^{n-1}(A)$ liefert

$$\operatorname{rad}^n(A) \cdot \operatorname{soc}^n(M) \subseteq \operatorname{rad}^{n-1}(A) \cdot \operatorname{soc}^{n-1}(M) \overset{\mathrm{IV}}{=} 0,$$

wobei beim letzten Gleichheitszeichen die Induktionsvoraussetzung benutzt wird. Es folgt, dass $\operatorname{soc}^n(M) \subseteq \{m \in M \mid \operatorname{rad}^n(A) \cdot m = 0\}$.

ii) Umgekehrt, sei nun $m \in M$ mit $0 = \operatorname{rad}^n(A) \cdot m = \operatorname{rad}^{n-1}(A) \cdot (\operatorname{rad}(A) \cdot m)$. Dann ist $\operatorname{rad}(A) \cdot m \overset{\mathrm{IV}}{\subseteq} \operatorname{soc}^{n-1}(M)$, das heisst im Quotientenmodul $M/\operatorname{soc}^{n-1}(M)$ gilt die Gleichung:

$$\operatorname{rad}(A) \cdot (m + \operatorname{soc}^{n-1}(M)) = \operatorname{rad}(A) \cdot m + \operatorname{soc}^{n-1}(M) = 0 + \operatorname{soc}^{n-1}(M).$$

Also ist $m + \operatorname{soc}^{n-1}(M) \overset{4.34}{\in} \operatorname{soc}(M/\operatorname{soc}^{n-1}(M)) \overset{(4.13)}{=} \operatorname{soc}^n(M)/\operatorname{soc}^{n-1}(M)$. Also ist $m \in \operatorname{soc}^n(M)$, das heisst $\operatorname{soc}^n(M) \supseteq \{m \in M \mid \operatorname{rad}^n(A) \cdot m = 0\}$.

Da das Radikal $J(A)$ der Algebra A nach Theorem 4.29 ein nilpotentes Ideal ist, impliziert Gleichung (4.14), dass es ein $m \in \mathbb{N}$ gibt mit $\operatorname{soc}^m(M) = M$. Die endliche Folge von Untermoduln

$$0 =: \operatorname{soc}^0(M) \subseteq \operatorname{soc}^1(M) \subseteq \operatorname{soc}^2(M) \subseteq \ldots \subseteq M$$

heisst die *Sockelreihe* von Modul M, und $m \in \mathbb{N}_0$ minimal mit $\operatorname{soc}^m(M) = M$ heisst die *Länge* der Sockelreihe von M. Die folgenden Moduln sind nach Gleichung (4.13) halbeinfach, und wir schreiben sie deshalb als direkte Summen einfacher Moduln $T_{i,j}$, siehe Theorem 4.5:

$$\begin{array}{rcl}
\operatorname{soc}^m(M)/\operatorname{soc}^{m-1}(M) & = & T_{m,1} \oplus \ldots \oplus T_{m,t_m} \\
\operatorname{soc}^{m-1}(M)/\operatorname{soc}^{m-2}(M) & = & T_{m-1,1} \oplus \ldots \oplus T_{m-1,t_{m-1}} \\
& \vdots & \\
\operatorname{soc}^2(M)/\operatorname{soc}(M) & = & T_{2,1} \oplus \ldots \oplus T_{2,t_2} \\
\operatorname{soc}(M) & = & T_{1,1} \oplus \ldots \oplus T_{1,t_1}
\end{array}$$

Wir beschreiben den Modul M daher auch mit dem Bild

$$M = \begin{array}{l}
T_{m,1} T_{m,2} \ldots T_{m,t_m} \\
T_{m-1,1} T_{m-1,2} \ldots T_{m-1,t_{m-1}} \\
T_{2,1} T_{2,2} \ldots T_{2,t_2} \\
T_{1,1} T_{1,2} \ldots T_{1,t_1}
\end{array}$$

Beispiel 4.36. Wir bestimmen die Sockelreihe des regulären Moduls der Algebra $A := T_3(K)$. Nach Aufgabe 4.18 ist das Radikal der Algebra der oberen 3×3-Matrizen gleich $J(A) = K\text{-Span}\{E_{12}, E_{13}, E_{23}\}$. Nach Beispiel 4.33 hat die Algebra A bis auf Isomorphie drei einfache Moduln $S_i = K\text{-Span}\{v_i\}$ mit $a \cdot v_i = a_{ii}$, für $a = (a_{st}) \in A$ und $1 \leq i \leq 3$. Wir berechnen $\operatorname{soc}({}_AA)$ mittels Proposition 4.34.

a) Die obere Dreiecksmatrix $b = (b_{ij}) \in A$ liegt im Sockel $\operatorname{soc}({}_AA)$ genau dann, wenn die drei Matrizen

$$E_{12} \cdot b = \begin{pmatrix} 0 & b_{22} & b_{23} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad E_{13} \cdot b = \begin{pmatrix} 0 & 0 & b_{33} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad E_{23} \cdot b = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & b_{33} \\ 0 & 0 & 0 \end{pmatrix}$$

jeweils Null sind, also genau dann, wenn $b_{22} = b_{23} = b_{33} = 0$ ist. Damit ist der Sockel ein drei-dimensionaler A-Modul mit Basis $\{E_{11}, E_{12}, E_{13}\}$ Da die einfachen Moduln alle eindimensional sind, lässt sich $\mathrm{soc}({}_AA)$ als direkte Summe von drei einfachen Moduln schreiben, und der Isomorphietyp dieser Moduln muss anhand der Operation der Algebra A bestimmt werden:

$$\begin{aligned}\mathrm{soc}({}_AA) &= K\text{-Span}\{E_{11}, E_{12}, E_{13}\} = K \cdot E_{11} \oplus K \cdot E_{12} \oplus K \cdot E_{13} \\ &\simeq S_1 \oplus S_1 \oplus S_1.\end{aligned}$$

Bei dieser Gleichung überliest man leicht, worum es geht. Deshalb ist es sinnvoll die Rechnung zu kommentieren: Es ist $K \cdot E_{1j}$ nicht nur ein K-Vektorraum, sondern jeweils ein A-Modul, da dieser Vektorraum abgeschlossen ist bezüglich der Operation der Algebra:

$$a \cdot E_{1j} = a_{11} E_{1j} \text{ für } 1 \leq j \leq 3 \text{ und } a = (a_{st}) \in A\ .$$

Diese letzte Gleichung gibt auch an, um welchen Isomorphietyp es sich jeweils bei den drei einfachen Moduln handelt, nämlich um Moduln isomorph zu S_1.

b) Um die zweite Sockelschicht zu berechnen, benutzen wir Gleichung (4.14). Es ist $\mathrm{rad}^2(A) = K\text{-Span}\{E_{ij} \cdot E_{st} \mid (i,j),(s,t) \in I\} = KE_{13}$ mit Indexset $I = \{(1,2),(1,3),(2,3)\}$. Wir berechnen $\mathrm{soc}^2(A)$ mit Hilfe von Gleichung (4.14): es ist $\mathrm{soc}^2({}_AA) = \{b \in A \mid 0 = E_{13} \cdot b = b_{33}E_{13}\} = \{b \in A \mid b_{33} = 0\}$, also

$$\mathrm{soc}^2(A)/\,\mathrm{soc}(A) = \begin{pmatrix} K & K & K \\ 0 & K & K \\ 0 & 0 & 0 \end{pmatrix} /\,\mathrm{soc}(A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & K & K \\ 0 & 0 & 0 \end{pmatrix} /\,\mathrm{soc}(A),$$

denn $\mathrm{soc}(A) = K\text{-Span}\{E_{11}, E_{12}, E_{13}\}$, besteht also genau aus den Einträgen in der ersten Zeile der Matrizen. Wir zeigen, dass dieser letzte Modul isomorph zu $S_2 \oplus S_2$ ist. Nach Gleichung (4.13) ist der Modul halbeinfach. Ausserdem handelt es sich um einen zweidimensionalen Vektorraum mit Basis

$$\{E_{22} + \mathrm{soc}(A), E_{23} + \mathrm{soc}(A)\}.$$

Da alle einfachen A-Moduln eindimensional sind, ist dieser Modul eine direkte Summe zweier einfacher Moduln. Hierbei ist für $a = (a_{ij}) \in A$ die Moduloperation auf dem ersten Summanden (zum ersten Basisvektor gehörend) gegeben durch:

$$\begin{aligned} a \cdot (E_{22} + soc(A)) &= \begin{pmatrix} 0 & a_{12} & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & 0 \end{pmatrix} + \mathrm{soc}(A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & 0 \end{pmatrix} + \mathrm{soc}(A) \\ &= a_{22}(E_{22} + \mathrm{soc}(A)) \simeq S_2. \end{aligned}$$

Ganz analog gilt für den zweiten direkten Summanden (zum zweiten Basisvektor gehörend):

$$\begin{aligned} a \cdot (E_{23} + \mathrm{soc}(A)) &= \begin{pmatrix} 0 & 0 & a_{12} \\ 0 & 0 & a_{22} \\ 0 & 0 & 0 \end{pmatrix} + \mathrm{soc}(A) = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & a_{22} \\ 0 & 0 & 0 \end{pmatrix} + \mathrm{soc}(A) \\ &= a_{22}(E_{23} + \mathrm{soc}(A)) \simeq S_2. \end{aligned}$$

c) Da jeder einfache Modul in einer Kompositionsreihe des regulären Moduls vorkommt, muss die dritte Sockelschicht, die eindimensional sein muss, gerade isomorph zu S_3 sein. Wir erhalten also die Sockelreihe

$$ {}_A A = \begin{matrix} S_3 \\ S_2 S_2 \\ S_1 S_1 S_1 \end{matrix} . $$

Aufgabe 4.22. Bestimmen Sie die Sockelreihe und die Radikalreihe der folgenden Moduln:

a) Moduln $V_{a,b}$ aus Beispiel 4.9;

b) reguläre Modul der Algebra $T_3(K)$ (nur die Radikalreihe);

c) reguläre Modul der Algebra $K[X]/(X^n)$.

Wir beobachten an diesen Beispielen, dass die Längen der Radikalreihen und die Längen der Sockelreihen jeweils übereinstimmen. Dies gilt im Allgemeinen, und diese gemeinsame Länge heisst die *Loewylänge* des gegebenen Moduls.

Aufgabe 4.23. Zeigen Sie, dass die Sockelreihe und die Radikalreihe eines gegebenen Moduls dieselbe Länge haben.

Kapitel 5

Quotientenalgebren von $K[X]$

Sei K ein Körper. In diesem Kapitel pausieren wir in der Weiterentwicklung der Theorie und wiederholen Konzepte aus den letzten Kapiteln, indem wir sie auf Quotientenalgebren des Polynomrings $K[X]$ anwenden. Ziel dieser Zwischeneinheit ist es, mehr Sicherheit im Umgang mit den Konzepten der Darstellungstheorie zu erhalten, und gleichzeitig mehr Zeit zu geben um die schwierigeren Konzepte in Kapitel 4 nachzuarbeiten. Wir erinnern zunächst an Resultate aus der Algebravorlesung: Der Polynomring $K[X]$ ist ein Hauptidealring, das heisst, jedes Ideal $I \triangleleft K[X]$ wird von einem Element erzeugt. Ausserdem wissen wir, dass der Ring $K[X]$ faktoriell ist, dass also Primelemente und irreduzible Elemente übereinstimmen, und die Faktorisierung von Polynomen aus $K[X]$ in irreduzible Polynome eindeutig ist, bis auf die Reihenfolge der irreduziblen Faktoren und bis auf Einheiten. Die Einheiten in $K[X]$ sind gerade Elemente aus $K^\times = K\backslash\{0\}$, und sie sind im Folgenden nicht relevant, weil $(f) = (\lambda f)$ ist, für Polynome $f \in K[X]$ und Einheiten $\lambda \in K$.

Bemerkung 5.1 (Inflation)**.** Wir wiederholen Inflation, siehe Beispiel 2.6 und Bemerkung 3.16. Seien A und B Algebren und $\varphi : A \to B$ ein surjektiver Algebrenhomomorphismus.

a) Ist M ein B-Modul, so ist M immer automatisch auch ein A-Modul mit der Operation $a \cdot m := \varphi(a) \cdot m$, für alle $m \in M$ und $a \in A$. Beispielsweise ist für $a_1, a_2 \in A$ und $m \in M$:

$$\begin{aligned}(a_1 \cdot a_2) \cdot m &\overset{\text{Def}}{=} \varphi(a_1 \cdot a_2) \cdot m \overset{(\varphi \text{ Homo})}{=} (\varphi(a_1) \cdot \varphi(a_2)) \cdot m \\ &\overset{(\text{M3})}{=} \varphi(a_1) \cdot (\varphi(a_2) \cdot m) \overset{\text{Def}}{=} a_1 \cdot (a_2 \cdot m).\end{aligned}$$

oder $1_A \cdot m \overset{\text{Def}}{=} \varphi(1_A) \cdot m = 1_B \cdot m \overset{(\text{M4})}{=} m$ für alle $m \in M$. Für den durch Inflation gewonnenen A-Modul M gilt $\ker(\varphi) \cdot M = 0$, denn $a \cdot m = \varphi(a) \cdot m = 0$ falls $\varphi(a) = 0$ ist.

b) Ist M ein A-Modul mit der zusätzlichen Eigenschaft, dass $\ker(\varphi) \cdot M = 0$ ist, so erbt M auch die Struktur eines B-Moduls mittels $b \cdot m := a \cdot m$, wobei das Element $a \in A$ im Urbild $\varphi^{-1}(b)$ gewählt wird. Die so definierte Operation von B auf der abelschen Gruppe M ist wohldefiniert: Seien $a_1, a_2 \in \varphi^{-1}(b)$. Dann gilt $\varphi(a_1) = \varphi(a_2)$ und es folgt mit der Additivität von φ, dass $0 =$

$\varphi(a_1) - \varphi(a_2) = \varphi(a_1 - a_2)$ ist, also $a_1 - a_2 \in \ker(\varphi)$ liegt. Sei $m \in M$. Nach Voraussetzung ist damit $(a_1 - a_2) \cdot m = 0$ und es folgt $a_1 \cdot m = a_2 \cdot m$. Die Operation von B auf M ist also wohldefiniert, und M wird mit dieser Operation zu einem B-Modul. Beispielsweise gilt $1_B \cdot m = 1_A \cdot m = m$ für alle $m \in M$, da $\varphi(1_A) = 1_B$ ist. Auch gilt für $m \in M$ und $b_1, b_2 \in B$, dass $(b_1 \cdot b_2) \cdot m = b_1 \cdot (b_2 \cdot m)$ ist, denn ist $\varphi(a_i) = b_i$ für $i = 1, 2$, dann folgt aus der Multiplikativität von φ, dass $\varphi(a_1 a_2) = \varphi(a_1)\varphi(a_2) = b_1 \cdot b_2$, und damit das Element $a_1 a_2$ im Urbild unter φ von $b_1 b_2$ ist. Also gilt

$$b_1 \cdot (b_2 \cdot m) \overset{\text{Def}}{=} a_1 \cdot (a_2 \cdot m) \overset{\text{(M3)}}{=} (a_1 \cdot a_2) \cdot m \overset{\text{Def}}{=} (b_1 b_2) \cdot m.$$

Deutlicher hätten wir in Kapitel 2 auch formulieren koennen, dass Inflation der Operation die Modulstruktur nicht ändert.

Lemma 5.2. *Sei $\varphi : A \to B$ ein surjektiver Algebrenhomomorphismus. Sei M ein A-Modul mit $\ker(\varphi) \cdot M = 0$. Dann stimmen der Untermodulverband von ${}_AM$ und ${}_BM$ überein. Insbesondere ist ${}_AM$ ein einfacher Modul, genau dann, wenn ${}_BM$ einfach ist.*

Beweis. Sei M ein einfacher A-Modul mit $\ker(\varphi) \cdot M = 0$. Nach Bemerkung 5.1 b) ist dann M auch ein B-Modul. Sei $U < M$ ein echter B-Untermodul. Nach Bemerkung 5.1 a) ist dann U auch ein A-Modul, genauer ein A-Untermodul des A-Moduls M. Und umgekehrt, ist ${}_AU <_A M$ Untermodul, dann folgt aus der Voraussetzung auch $\ker(\varphi) \cdot U \subseteq \ker(\varphi) \cdot M = 0$, also ist U auch als B-Modul ein Untermodul von ${}_BM$. Der Untermodulverband von ${}_AM$ stimmt also mit dem Untermodulverband von ${}_BM$ überein. □

Die Algebren, um die es in diesem Kapitel geht, sind Polynomringe in einer Variablen, beziehungsweise deren echte (und damit endlich-dimensionale) Quotienten. Ab jetzt sei also $A = K[X]$ der Polynomring. Ist I echtes, nicht-triviales Ideal in $K[X]$, so existiert ein Polynom f positiven Grades mit $I = (f)$. Sei $B := A/I = K[X]/(f)$. Die Quotientenalgebra $B := K[X]/I$ hat als Vektorraum die Basis $\{1 + I, X + I, \ldots, X^{\deg(f)-1} + I\}$, ist also eine Algebra der Dimension $\deg(f)$. Wir wollen im Laufe des Kapitels die einfachen B-Moduln klassifizieren und klassifizieren, wann die Algebra B halbeinfach ist. Um Antworten auf diese Fragen zu geben, müssen wir nach Theorem 3.30 und Theorem 4.14 den regulären Modul ${}_BB$ verstehen.

Bemerkung 5.3. Nach Konstruktion ist $\pi : A \to B = A/I$ mit $a \mapsto a + I$ für alle $a \in A$ ein surjektiver Algebrenhomomorphismus. Untermoduln des regulären Moduls ${}_BB$ entsprechen mittels Inflation genau den Untermoduln des Moduls ${}_AB$. Abbildung $\pi : {}_AA \to {}_AB$, definiert durch $a \mapsto a + I$ für $a \in A$ ist ein A-Modulhomomorphismus. Die Untermoduln von ${}_AB$ ergeben sich daher durch die Untermodulkorrespondenz 2.27 aus speziellen Untermoduln von ${}_AA$, wobei die Links-Untermoduln des regulären Moduls ${}_AA$ nach Beispiel 2.19 genau den Linksideale von A entsprechen. Im konkreten Fall der kommutativen Algebra $A = K[X]$ sind die Untermoduln von ${}_AA$ also zweiseitige Hauptideale (g), mit $g \in K[X]$. Die Untermoduln von ${}_AB$ beziehungsweise ${}_BB$ haben also die Form $(g)/(f)$, und wegen $(f) \subseteq (g)$ gilt Polynom g teilt Polynom f in $K[X]$. (Zeichnen Sie sich ein Bild der Untermodulkorrespondenz.)

Lemma 5.4. *Sei $0 \neq M = (g)/(f)$ ein echter Untermodul von ${}_BB$ mit $f = gh$ für $h \in K[X]$. Dann ist $M \simeq K[X]/(h)$, als B-Modul.*

Bemerkung. Es ist hier (h) Ideal in $A = K[X]$, also (h) ein A-Untermodul des regulären Moduls ${}_AA$. Damit ist $K[X]/(h)$ ein A-Quotientenmodul. Da Elemente aus (f) auf diesem Quotientenmodul durch Null operieren, ist nach Bemerkung 5.1 dieser Modul auch ein B-Modul. Für ein Polynom $t \in K[X]$ gilt:

$$f \cdot (t + (h)) = ft + (h) = ght + (h) = 0 + (h).$$

Beweis von Lemma 5.4. Sei $I = (f)$ und $0 \neq M$ ein echter Untermodul des regulären Moduls ${}_BB$. Nach Bemerkung 5.3 existiert ein Polynom $g \in K[X]$ mit g teilt f, so dass $M = (g)/(f)$ ist. Sei $h \in K[X]$ mit $f = gh$. Die Abbildung

$$\psi : {}_AA \to Ag = (g) \to Ag/Af = (g)/(f), \text{ definiert durch } t \mapsto tg \mapsto tg + I$$

ist Komposition zweier surjektiver A-Modulhomomorphismen (die erste Abbildung ist sogar ein Isomorphismus), und ist damit wieder ein surjektiver A-Modulhomomorphismus, von ${}_AA$ auf einen Subquotienten von ${}_AA$. Wir bestimmen den Kern der Abbildung ψ: Zunächst bemerken wir, dass

$$\psi(h) = hg + I = f + (f) = 0 + (f)$$

ist. Also ist $h \in \ker(\psi)$. Sei $0 = \psi(r) = rg + I$. Dann folgt $rg \in I = (f)$. Es existiert also ein Polynom $s \in K[X]$ mit $rg = sf = shg$. Da $K[X]$ ein nullteilerfreier Ring ist, folgt $r = sh$. Wir haben damit insgesamt gezeigt, dass $\ker(\psi) = (h)$ ist. Ist also $f = gh$ in $K[X]$, so folgt mit dem Homomorphiesatz 2.26 der A-Modulisomorphismus:

$$K[X]/(h) = K[X]/\ker(\psi) \simeq \operatorname{im}(\psi) = (g)/(f) = M.$$

Da $I = (f)$ auf M durch Null operiert, ist dies auch ein Isomorphismus von B-Moduln. □

Theorem 5.5. *Sei $B = K[X]/(f)$ mit $\deg(f) > 0$.*

a) Sei $h \in K[X]$ irreduzibel, derart, dass es ein Polynom $g \in K[X]$ gibt mit $f = gh$. Dann ist $K[X]/(h)$ ein einfacher B-Modul und jeder einfache B-Modul ist isomorph zu einem Modul dieser Form.

b) Schreibe $f = \prod_{i=1}^r f_i^{a_i}$ mit $f_i \in K[X]$ paarweise teilerfremd und irreduzibel und $a_i \in \mathbb{N}$. Dann hat B bis auf Isomorphie genau r paarweise verschiedene einfache Moduln. Diese sind

$$K[X]/(f_1), \ldots, K[X]/(f_r), \text{ wobei } \dim K[X]/(f_i) = \deg f_i, \text{ für } 1 \leq i \leq r.$$

Beweis. In diesem Beweis spielt es eine Rolle, dass $K[X]$ ein faktorieller Ring ist.

i) Seien $g, h \in K[X]$ mit $f = gh$ und h irreduzibel in $K[X]$. Da h irreduzibel ist, ist nach der Algebravorlesung $(h) \lhd K[X]$ ein maximales Ideal, also nach Beispiel 2.19 ein maximaler Untermodul von ${}_AA$. Der Modul $M = K[X]/(h)$ ist somit nach Bemerkung 3.6 ein einfacher A-Modul. Hierbei operiert (f) durch Null, da f ein Vielfaches von h ist: $f \cdot (t + (h)) = ft + (h) = 0 + (h)$. Nach Bemerkung 5.1 ist somit M ein B-Modul, und nach Lemma 5.2 ist M ein einfacher B-Modul.

ii) Sei S ein einfacher B-Modul (und damit nach Bemerkung 5.1 auch $K[X]$-Modul). Nach dem Beweis zu Lemma 3.29 ist somit S isomorph zu einem Quotientenmodul des regulären Moduls ${}_BB$, etwa $S \simeq B/J$. Hierbei ist der Untermodul $J \leq B$ maximal, da der Quotient B/J einfach ist, siehe Bemerkung 3.6. Mit der Untermodulkorrespondenz 2.27 folgt, dass es einen B-Untermodul $W \leq {}_BA$ gibt mit $I \subseteq W$ und $W/I \simeq J$. Als Untermodul in $K[X]$ hat W die Form $W = (h)$, für ein $h \in K[X]$. Aus $I = (f) \subseteq W = (h)$ folgt, dass h ein Teiler von f ist. Der Isomorphiesatz 2.26 impliziert, dass

$$S \simeq B/J \simeq (K[X]/(f))/((h)/(f)) \simeq K[X]/(h).$$

Da B/J einfach ist, ist auch der hierzu isomorphe Modul $K[X]/(h)$ einfach. Insbesondere ist $(h) \lhd K[X]$ ein maximales Ideal, also $h \in K[X]$ irreduzibel.

iii) Nach i) hat die Algebra B die einfachen Moduln

$$K[X]/(f_1), \ldots, K[X]/(f_r), \text{ wobei } \dim K[X]/(f_i) = \deg f_i, \text{ für } 1 \leq i \leq r.$$

Wir zeigen, sind f_i und f_j irreduzibel und teilerfremd, dann sind die zu den Polynomen korrespondierenden Moduln nicht isomorph. Angenommen $\psi : K[X]/(f_i) \to K[X]/(f_j)$ ist ein B-Modulhomomorphismus. Wir zeigen, dass $\ker(\psi) \neq 0$ ist, also ψ kein Isomorphismus sein kann. Sei $t + (f_j) = \psi(1 + (f_i))$. Dann ist

$$\begin{aligned} \psi(f_j + (f_i)) &= \psi(f_j(1 + (f_i))) = f_j\psi(1 + (f_i)) \\ &= f_j(t + (f_j)) = f_jt + (f_j) = 0 + (f_j). \end{aligned}$$

Damit ist $f_j + (f_i) \in \ker(\psi)$. Da $\mathrm{ggT}(f_j, f_i) = 1$, ist $f_j \notin (f_i)$, also ist $f_j + (f_i) \neq 0$, und damit ψ nicht injektiv. Damit ist die Klassifikation der einfachen B-Moduln bewiesen. □

Bemerkung 5.6. Kompositionsreihen von ${}_BB$ lassen sich einfach hinschreiben. Sei $f = \prod_{i=1}^r f_i$ mit $f_i \in K[X]$ irreduzible Polynome, nicht notwendigerweise paarweise teilerfremd. Betrachte

$$0 = I_1/(f) \subseteq I_2/(f) \subseteq \ldots \subseteq I_{r-1}/(f) \subseteq B \tag{5.1}$$

mit $I_t := (f_{t+1} \cdots f_r)$. Wegen $f_{t+1} \cdots f_r \mid f_t \cdot f_{t+1} \cdots f_r$ ist $I_{t-1} \subseteq I_t$, damit ist (5.1) eine Kette von Untermoduln und mit dem Isomorphiesatz 2.26 folgt

$$(I_t/(f))/(I_{t-1}/(f)) \simeq I_t/I_{t-1} \overset{5.4}{\simeq} K[X]/(f_t).$$

Nach Theorem 5.5 sind diese Quotientenmoduln einfach. Damit ist (5.1) eine Kompositionsreihe von ${}_BB$. Ändert man die Reihenfolge der Faktoren von f, so erhält man weitere Kompositionsreihen von ${}_BB$ und jede Kompositionsreihe von ${}_BB$ ist von der angegebenen Form. Der Untermodulverband von ${}_BB$ lässt sich an der Menge aller Kompositionsreihen von ${}_BB$ ablesen. Dass es für ${}_BB$ viele Kompositionsreihen gibt, wird später dadurch aufgeklärt, dass B als Algebra beziehungsweise als regulärer Modul zerfällt. Dieses Phänomen konnten wir bereits in Aufgabe 4.8 beim Modul V_{00} beobachten.

Aufgabe 5.1. Sei K Körper mit $K \in \{\mathbb{R}, \mathbb{C}, \mathbb{Z}_2\}$ und sei $B = K[X]/(f)$ mit $f \in K[X]$. Bestimmen Sie die Dimensionen der einfachen B-Moduln, falls

a) $f = X^3 - 1$;

b) $f = X^4 - X^2$.

Geben Sie auch jeweils die einfachen B-Moduln durch eine Vektorraumbasis und die Operation von X auf den Basisvektoren an.

Aufgabe 5.2. Wahr oder falsch? Begründen Sie jeweils Ihre Antwort.

a) Einfache Moduln der Algebra $\mathbb{C}[X]/(f)$ mit $f \in \mathbb{C}[X]$ sind immer eindimensional.

b) Einfache Moduln der Algebra $\mathbb{R}[X]/(f)$ mit $f \in \mathbb{R}[X]$ sind immer ein- oder zweidimensional.

c) Eine Algebra der Form $\mathbb{Q}[X]/(f)$ mit $f \in \mathbb{Q}[X]$ besitzt immer einen einfachen Modul der Dimension mindestens drei.

d) Zu jedem $n \in \mathbb{N}$ existiert ein Polynom $f_n \in \mathbb{Q}[X]$, so dass die Algebra $\mathbb{Q}[X]/(f_n)$ einen einfachen Modul der Dimension mindestens n besitzt.

Unsere erste Frage nach der Klassifikation der einfachen $B = K[X]/(f)$-Moduln ist hiermit beantwortet. Als nächstes wollen wir verstehen, wann die Algebren B halbeinfach sind. Hierzu benötigen wir die folgende Vorbereitung:

Lemma 5.7. *Sei $B = K[X]/(f)$ mit Polynom $f \in K[X]$ positiven Grades. Ist $f = gh$ Polynomfaktorisierung in $K[X]$ mit $\mathrm{ggT}(g, h) = 1$, dann gilt die folgende Zerlegung von B-Moduln:*

$$K[X]/(f) = (g)/(f) \oplus (h)/(f) \overset{5.4}{\simeq} K[X]/(h) \oplus K[X]/(g).$$

Beweis. Da die Polynome g und h teilerfremd sind, existieren nach dem Lemma von Bezout Polynome $q_1, q_2 \in K[X]$ mit $q_1 g + q_2 h = 1$. Damit ist also

$$1_B = 1 + (f) = q_1 g + q_2 h + (f) = (q_1 g + (f)) + (q_2 h + (f)),$$

also $B = B \cdot 1_B = B(q_1 g + (f)) + B(q_2 h + (f)) \subseteq (g)/(f) + (h)/(f) \subseteq B$, und damit gilt $B = (g)/(f) + (h)/(f)$. Angenommen es ist $r + (f)$ ein Element im Schnitt von $(g)/(f)$ und $(h)/(f)$. Dann existieren Polynome $p_1, p_2 \in K[X]$ mit $r + (f) = gp_1 + (f) = hp_2 + (f)$. Wir betrachten die erste der beiden Gleichungen. Diese impliziert, dass es ein Polynom $t \in K[X]$ gibt mit $r - gp_1 = tf = tgh$. Es folgt, dass g ein Teiler von r ist. Ganz analog sieht man, dass auch h ein Teiler von r ist. Da $\mathrm{ggT}(g, h) = 1$ ist, folgt $f = gh$ teilt r. Dies zeigt, dass $r + (f) = 0 + (f)$ ist. Der Schnitt der Moduln $(g)/(f)$ und $(h)/(f)$ ist also trivial. Damit folgt die behauptete Modulzerlegung. $\square$

Theorem 5.8. *Sei K ein Körper, sei $f \in K[X]$ Polynom positiven Grades mit Faktorisierung $f = \prod_{i=1}^{r} f_i^{a_i}$ (mit $a_i \in \mathbb{N}$) in paarweise teilerfremde irreduzible Polynome $f_i \in K[X]$. Dann ist die Algebra $B = K[X]/(f)$ genau dann halbeinfach, wenn $a_i = 1$ ist für $1 \leq i \leq r$.*

Beweis. Nach Theorem 4.14 ist die Algebra B halbeinfach, genau dann, wenn der reguläre Modul ${}_BB$ ein halbeinfacher Modul ist. Wir untersuchen deshalb den regulären Modul ${}_BB$.

a) Sei B eine halbeinfache Algebra. Angenommen einer der Exponenten erfüllt die Bedingung $a_i > 1$; ohne Einschränkung sei das a_1. Wir betrachten den B-Modul $M := K[X]/(f_1^2)$, siehe Lemma 5.4. Die Untermoduln von M haben die Form $(g)/(f_1^2)$ mit g teilt f_1^2. Da das Polynom f_1 irreduzibel ist, hat der Modul M genau einen nicht-trivialen echten Untermodul U, nämlich für den Teiler $g = f_1$ von f_1^2. Da M genau einen echten, nicht-trivialen Untermodul besitzt, kann der Modul $0 \neq U < M$ kein Kompliment in M haben. Das zeigt, dass der Modul M nicht halbeinfach ist. Dies ist ein Widerspruch zu B halbeinfache Algebra, siehe Definition 4.12. Es folgt, dass $a_i = 1$ ist für alle $1 \leq i \leq r$.

b) Sei nun umgekehrt das Polynom $f = \prod_{i=1}^{r} f_i$ Produkt paarweise teilerfremder irreduzibler Polynome f_i, die also ohne Vielfachheiten grösser als Eins als Teiler in f vorkommen. Sei M ein Untermodul von ${}_BB$. Dann existiert nach Bemerkung 5.3 ein Polynom $g \in K[X]$ mit g teilt f und $M = (g)/(f)$. Dies impliziert, dass es ein Polynom $h \in K[X]$ gibt mit $f = gh$. Aufgrund der Voraussetzung, dass kein irreduzibles Polynom f_i mit Vielfachheit als Teiler von f vorkommt, ist $\mathrm{ggT}(g, h) = 1$. Mit Lemma 5.7 erhalten wir die Modulzerlegung ${}_BB = (g)/(f) \oplus (h)/(f)$. Der Modul $M = (g)/(f)$ hat also in ${}_BB$ ein Komplement. Damit ist der reguläre Modul ${}_BB$ halbeinfach, und mit Theorem 4.14 ist die Algebra B halbeinfach. □

Aufgabe 5.3. Sei K ein Körper. Welche der folgenden Algebren sind halbeinfach?

a) $K[X]/(X^3 - X^2 + X - 1)$ mit $K = \mathbb{C}, \mathbb{R}$ oder $\mathbb{Q}$,

b) $\mathbb{C}[X]/(X^3 + X^2 - X - 1)$,

c) $\mathbb{Q}[X]/(X^4 - X^2 - 2)$,

d) $\mathbb{Z}_2[X]/(X^4 + X + 1)$.

Aufgabe 5.4. Wahr oder falsch? Begründen Sie jeweils Ihre Antwort.

a) Sei $f \in \mathbb{R}[X]$ ein Polynom positiven Grades. Die $\mathbb{R}$-Algebra $\mathbb{R}[X]/(f)$ ist genau dann halbeinfach, wenn die $\mathbb{C}$-Algebra $\mathbb{C}[X]/(f)$ halbeinfach ist.

b) Sei $f \in \mathbb{Q}[X]$ ein Polynom positiven Grades. Die $\mathbb{Q}$-Algebra $\mathbb{Q}[X]/(f)$ ist genau dann halbeinfach, wenn die $\mathbb{R}$-Algebra $\mathbb{R}[X]/(f)$ halbeinfach ist.

Kapitel 6

Unzerlegbare Moduln

6.1 Definition und Beispiele

Sei K ein Körper und A eine Algebra über K. Es gibt zwei elementare Bausteine, aus denen Moduln zusammengebaut sind. Der erste dieser Bausteine sind die einfachen Moduln, und wir haben gelernt, wie Moduln aus einfachen Moduln im Sinne des Jordan-Hölder-Theorems 3.21 zusammengesetzt sind, und diese Sichtweise in den Radikal- und Sockelschichten noch vertieft. Es stellt sich hierbei heraus, dass man einfache Moduln nicht beliebig zusammensetzen kann: gegeben zwei einfache Moduln S und T. Dann ist $S \oplus T$ ein Modul mit Kompositionslänge zwei und diesen beiden Kompositionsfaktoren. Es muss geklärt werden, ob es auch unzerlegbare Moduln M mit genau diesen beiden Kompositionsfaktoren gibt. Diese hätten dann die Form

$$M = \begin{matrix} S \\ T \end{matrix} \text{ beziehungsweise } M = \begin{matrix} T \\ S \end{matrix},$$

und man sagt, dass S eine *Erweiterung* von T, beziehungsweise T eine Erweiterung von S ist. Solche Erweiterungen müssen nicht immer existieren. Es ist Teil der derzeit gelesenen Vorlesung *Representation Theory of Algebras* im Masterbereich, Erweiterungen von Moduln zu verstehen, und wir werden hier dieses Thema nicht weiter vertiefen. Der zweite Baustein, aus dem Moduln zusammengesetzt sind, das sind die unzerlegbaren Moduln, und um diese geht es in den verbleibenden Vorlesungen. Wir wiederholen die Definition:

Definition 6.1. Ein A-Modul $M \neq 0$ heisst *unzerlegbar*, falls M nicht als direkte Summe $M = U \oplus V$ zweier echter, nicht-trivialer Untermoduln geschrieben werden kann. Andernfalls heisst $M \neq 0$ zerlegbar.

Bemerkung 6.2. Wie verhält sich unzerlegbar zu einfach?

a) Aus Definition 6.1 folgt direkt: Jeder einfache A-Modul ist unzerlegbar. Die Umkehrung ist im Allgemeinen falsch und wir geben in b) ein Gegenbeispiel an. Ist A eine halbeinfache Algebra, dann ist nach Definition 4.12 jeder A-Modul M halbeinfach und nach Theorem 4.5 eine direkte Summe einfacher Moduln. Es ist M in diesem Fall genau dann ein einfacher Modul, wenn M unzerlegbar ist. Unser Interesse gilt also im Folgenden den nicht halbeinfachen Algebren, wo die Konzepte einfach und unzerlegbar verschieden sind.

b) Ein unzerlegbarer A-Modul ist nicht notwendigerweise einfach: Sei $A = \mathbb{Z}_2 C_2$ mit $C_2 = \langle x \mid x^2 = 1 \rangle$. Dann ist der reguläre Modul ${}_A A$ zweidimensional mit Basis $\{1, x\}$ und den vier Elementen $\{0, 1, x, 1 + x\}$. Er besitzt genau einen einfachen Untermodul, den trivialen Modul $U := \{0, 1 + x\}$. Da A nur genau einen Untermodul besitzt, kann U kein Komplement in A haben. Wir haben hiermit alle Untermoduln von A aufgezählt und gleichzeitig gesehen, dass diese kein Komplement haben. Also folgt, dass U unzerlegbar ist, aber nicht einfach ist.

Algebren haben in der Regel viele unzerlegbare Moduln, bisweilen unendlich viele, selbst wenn es nur endlich viele einfache Moduln gibt.

Beispiel 6.3. Wir geben Beispiele unzerlegbarer Moduln.

a) Sei $A = K[X]$ der Polynomring. Wir zeigen, dass der reguläre Modul ${}_A A$ unzerlegbar ist. Untermoduln von ${}_A A$ sind Linksideale in A und damit erzeugt von einem Element. Angenommen es ist ${}_A A = (f) \oplus (g)$ eine Zerlegung in eine direkte Summe unzerlegbarer Untermoduln, für $f, g \in K[X]$. Wir schreiben das Einselement entsprechend dieser Zerlegung als $1_A = f_1 + g_1$ für $f_1 \in (f)$ und $g_1 \in (g)$. Dann ist f Teiler von f_1 und g Teiler von g_1, also ist fg Teiler von $f_1 g_1$, und damit das Produkt $f_1 g_1 \in (f) \cap (g) = \{0\}$, also ist $f_1 g_1 = 0$. Der Polynomring $K[X]$, als Polynomring über einem Körper K, hat keine Nullteiler, also ist $f_1 = 0$ oder $g_1 = 0$. Es folgt, dass der reguläre Modul ${}_A A$ unzerlegbar ist.

b) Der Modul ${}_A A$ in Bemerkung 6.2 b) ist uniseriell. Nach Aufgabe 3.8 (oder mit Hilfe von Bemerkung 5.3) folgt, dass die regulären Moduln $K[X]/(X^n)$ uniseriell sind, bestehend aus n Kompositionsfaktoren, jeweils isomorph zum trivialen eindimensionalen Modul. Mittels Inflation sind auch die $K[X]$-Moduln $K[X]/(X^n)$ uniseriell, siehe Lemma 5.2. Uniserielle Moduln haben einen einfachen Sockel. Nach Bemerkung 4.11 sind daher alle uniseriellen Moduln unzerlegbar.

Moduln der Form Ae mit A Algebra und $e \in A$ Idempotent spielen eine zentrale Rolle in der Darstellungstheorie. Für bestimmte Arten von Idempotenten ist Ae immer unzerlegbar. Wir zeigen dies am Beispiel von Wegealgebren und den faulen Wegen:

Beispiel 6.4. Sei Q ein Köcher ohne Schleifen und Zykel und sei $A = KQ$ die zugehörige endlich-dimensionale Wegealgebra, siehe Proposition 1.27. Wir arbeiten in diesem Beispiel zunächst mit Rechtsmoduln, da diese zu Köcherdarstellungen korrespondieren, siehe Proposition 2.35.

Für $i \in Q_0$ betrachten wir den A-Rechtsmodul $M := e_i A$ beziehungsweise die dazu korrespondierende Köcherdarstellung $M = (M(j), M(\alpha))$. Modul M hat als Basis alle Wege, die im Punkt i starten. Wegen $M(j) = Me_j$ haben die Vektorräume $M(j)$ als Basis alle Wege, die in i starten und in j enden. Da Q keine Schleifen und Zykel hat, gibt es genau einen Weg, der im Punkt i startet und endet, nämlich den faulen Weg e_i. Also ist $M(i) = K$. Angenommen der Modul M ist eine direkte Summe von Untermoduln, etwa $M = U \oplus V$. Seien $U = (U(j), U(\alpha))$ und $V = (V(j), V(\alpha))$ die zugehörigen Köcherdarstellungen. Dann ist also ohne Einschränkung $U(i) = K$ und $V(i) = 0$. Also ist $e_i \in U(i) \subseteq U$. Da U ein A-Rechtsmodul ist, folgt $M = e_iA \subseteq U$, das heisst $V = 0$. Damit ist der A-Rechtsmodul e_iA unzerlegbar.

Nach Proposition 2.35 und Lemma 1.31 entsprechen die A-Linksmoduln den Darstellungen des entgegengesetzten Köchers Q^{op}. Es hat Q genau dann keine Schleifen und Zykel, wenn Q^{op} keine Schleifen und Zykel hat. Da der Köcher Q beliebig war, sind also auch die A-Linksmoduln Ae_i unzerlegbar für die Wegealgebra $A = KQ$.

Bemerkung 6.5. Untermoduln und Quotientenmoduln von unzerlegbaren Moduln sind nicht notwendigerweise unzerlegbar. Die Moduln $V_{1,0}$ und $V_{0,1}$ der Algebra $\mathbb{Z}_2V_4$ sind nach Bemerkung 4.11 unzerlegbar. Nach Beispiel 4.9 ist $\operatorname{soc} V_{0,1} = \langle e_1\rangle_K \oplus \langle e_2\rangle_K$ ein zerlegbarer Untermodul des unzerlegbaren Moduls $V_{0,1}$. Nach Beispiel 4.10 ist

$$V_{1,0}/\operatorname{soc}(V_{1,0}) = \langle e_2\rangle_K \oplus \langle e_3\rangle_K$$

ein zerlegbarer Quotientenmodul des unzerlegbaren Moduls $V_{1,0}$.

Aufgabe 6.1. a) Der Modul $K[X]/(X^n)$ ist nach Beispiel 6.3 a) uniseriell und damit unzerlegbar. Geben Sie unter Benutzung von Kapitel 5 weitere uniserielle und damit unzerlegbare Moduln an.

b) Sei $A = K[X, Y]/(X^2, Y^2)$. Geben Sie einen unzerlegbaren A-Modul an, der einen zerlegbaren Quotientenmodul besitzt.

Unser Ziel in diesem Kapitel ist es, zu beweisen, dass die Zerlegung eines endlich-dimensionalen Moduls in eine direkte Summe unzerlegbarer Moduln immer existiert und dass sie eindeutig ist, bis auf Reihenfolge und Isomorphie der Summanden. Dieses zentrale Resultat der Darstellungstheorie ist als Satz von Krull-Remak-Schmidt bekannt. Die Existenz einer solchen Zerlegung lässt sich leicht beweisen:

Theorem 6.6. *Sei A eine Algebra und $M \neq 0$ ein endlich-dimensionaler A-Modul. Dann existieren unzerlegbare A-Moduln $U_1, \ldots, U_n$ mit $M = U_1 \oplus \ldots \oplus U_n$.*

Beweis. Wir machen Induktion nach der Dimension $\dim M$. Angenommen $\dim M = 1$, so ist M ein einfacher Modul und damit nach Bemerkung 6.2 unzerlegbar. Sei also $\dim M > 1$. Falls M unzerlegbar ist, dann sind wir fertig. Sei also M zerlegbar. Dann existieren echte, nicht-triviale Untermoduln $U, V < M$ mit $M = U \oplus V$. Da $\dim U, \dim V < \dim M$ sind, existiert nach Induktionsannahme eine Zerlegung von U und von V als direkte Summe unzerlegbarer Moduln, etwa $U = U_1 \oplus \ldots \oplus U_{n_1}$ und $V = V_1 \oplus \ldots \oplus V_{n_2}$. Damit folgt, dass M eine Zerlegung als direkte Summe unzerlegbarer Moduln besitzt:

$$M = U \oplus V = U_1 \oplus \ldots \oplus U_{n_1} \oplus V_1 \oplus \ldots \oplus V_{n_2}.$$

□

Es gibt viele unendlich-dimensionale Moduln für die eine solche Zerlegung nicht existiert. Dass eine solche Zerlegung von Moduln in eine direkte Summe von unzerlegbaren Untermoduln, falls sie existiert, nicht physisch eindeutig sein wird, kann man sich leicht am folgenden Beispiel klar machen:

Beispiel 6.7. Sei $A = K$ ein Körper. Dann sind A-Moduln gerade K-Vektorräume. Die unzerlegbaren Moduln der Algebra A sind eindimensionale K-Vektorräume. Der Modul $M = K^2$ besitzt nach Linearer Algebra viele verschiedene Zerlegungen als direkte Summe unzerlegbarer Moduln, sogar unendlich viele, falls $|K|$ unendlich ist. Beispielsweise ist:

$$M = \langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rangle_K \oplus \langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rangle_K = \langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rangle_K \oplus \langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \rangle_K.$$

Alle diese Zerlegungen bestehen aus genau zwei eindimensionalen Vektorräumen, und diese eindimensionalen K-Vektorräume sind natürlich nicht notwendigerweise gleich, sondern unter Umständen nur isomorph zueinander. Im Beispiel der Algebra $A = K$ wissen wir aber aus der Linearen Algebra: eine Zerlegung in unzerlegbare A-Moduln, also eindimensionale Vektorräume, ist immer eindeutig, bis auf Isomorphie und Reihenfolge der Summanden.

6.2 Idempotente und Zerlegungen

Ein gegebener endlich-dimensionale Modul $M \neq 0$ kann nach Beispiel 6.7 mehrere Zerlegungen als direkte Summe von unzerlegbaren Moduln besitzen. Um zu verstehen, wieviele solche Zerlegungen existieren, müssen wir verstehen, wie solche Zerlegungen entstehen. Wir wollen sie mit Hilfe von Idempotenten charakterisieren, und beginnen zunächst mit unzerlegbaren Moduln:

Lemma 6.8. *Ein A-Modul M ist genau dann unzerlegbar, wenn der Endomorphismenring* $\mathrm{End}_A(M)$ *keine Idempotente enthält ausser* 0 *und* id_M *. Insbesondere ist der reguläre Modul ${}_AA$ genau dann unzerlegbar, wenn* 0 *und* 1 *die einzigen Idempotente in A sind.*

Beweis. Es sind zwei Richtungen zu beweisen.

a) Sei M ein unzerlegbarer A-Modul, insbesondere ist also $M \neq 0$ nach Definition 6.1. Schreibe $1 = \mathrm{id}_M$ für das Einselement der Algebra $\mathrm{End}_A(M)$. Sei $\epsilon \in \mathrm{End}_A(M)$ ein Idempotent. Da ϵ ein A-Modulhomomorphismus ist, folgt

$$a \cdot \epsilon(m) = \epsilon(am) \in \epsilon(M), \text{ für alle } a \in A \text{ und } m \in M.$$

Es ist also $\epsilon(M) =: \epsilon M$ ein A-Untermodul von M. Analog folgt, dass auch $(1-\epsilon)M$ ein A-Untermodul von M ist, und da die Idempotente ϵ und $1-\epsilon$ eine Zerlegung der Eins $1 = \mathrm{id}_M$ bilden, folgt

$$M = \mathrm{id}_M(M) = (\epsilon + (1-\epsilon))(M) = \epsilon M + (1-\epsilon)M.$$

Die Idempotente ϵ und $1-\epsilon$ sind orthogonal, also $\epsilon(1-\epsilon) = 0$, die Nullabbildung. Angenommen es ist $x \in \epsilon M \cap (1-\epsilon)M$. Dann existieren $m_1, m_2 \in M$ mit $\epsilon(m_1) = x = (1-\epsilon)(m_2)$. Es folgt

$$x = \epsilon(m_1) = \epsilon^2(m_1) = \epsilon(x) = \underbrace{\epsilon(1-\epsilon)}_{=0}(m_2) = 0.$$

Damit ist der Schnitt der beiden Untermoduln trivial, also $M = \epsilon M \oplus (1-\epsilon)M$ eine Zerlegung als direkte Summe von Untermoduln. Da M unzerlegbar ist, folgt $\epsilon M = 0$ oder $(1-\epsilon)M = 0$. Da $M \neq 0$ ist, folgt $\epsilon = 0$ oder $1 - \epsilon = 0$, das heisst $\epsilon = 1$.

b) Für die umgekehrte Beweisrichtung nehmen wir an, dass der Modul M in eine direkte Summe von Untermoduln zerfällt. Sei also $M = U \oplus V$ eine direkte Summe von Untermoduln. Insbesondere ist dies also eine Vektorraumzerlegung von M. Solche Zerlegungen korrespondieren nach Linearer Algebra zu Idempotenten: Sei $\epsilon : M \to M$ Projektion von M auf U entlang V, also $\epsilon(u+v) = u$, für alle $u \in U$ und $v \in V$. Dann ist ϵ ein Idempotent in $\mathrm{End}_A(M)$:
$$\epsilon^2(u+v) = \epsilon(u) = u = \epsilon(u+v), \text{ also } \epsilon^2 = \epsilon.$$
Ist $U \neq 0$ und $V \neq 0$, dann ist ϵ ein Idempotent mit $\epsilon \neq 0, 1$. Nach Voraussetzung existieren im Endomorphismenring $\mathrm{End}_A(M)$ aber nur die Idempotente 0 und 1. Also ist entweder $U = 0$ oder $V = 0$ und damit der Modul M unzerlegbar. Dies beendet den Beweis der Hauptaussage von Lemma 6.8.

c) Wir betrachten nun den Spezialfall, dass $M = {}_AA$ der reguläre Modul ist und benutzen Aufgabe 2.9. Der reguläre Modul ${}_AA$ ist nach obigen Beweisen genau dann unzerlegbar, wenn der Endomorphismenring $\mathrm{End}_A(M) = A^{\mathrm{op}}$ nur die Idempotente 0 und 1 enthält. Idempotente in der Algebra A und der Algebra A^{op} stimmen aber überein. Somit folgt die letzte Behauptung. □

Vergleichen Sie die Argumente im letzten Beweis in Teil a) mit den Argumenten in Bemerkung 3.15. Beachten Sie, dass in Bemerkung 3.15 die Idempotente, anders als hier, zentrale Idempotente sind.

Aufgabe 6.2. Sei A eine Algebra. Wahr oder falsch? Begründen Sie jeweils Ihre Antwort.

a) Zerfällt A als Algebra in eine direkte Summe (das ist dasselbe wie direktes Produkt) zweier echter Unteralgebren, so zerfällt auch der reguläre Modul ${}_AA$ als direkte Summe zweier echter Untermoduln.

b) Zerfällt der regulärer Modul ${}_AA$ in eine direkte Summe von zwei echten Untermoduln, so zerfällt auch die Algebra A in eine direkte Summe zweier echter Unteralgebren.

Aus Bemerkung 3.15 aber genauso aus dem Beweis von Lemma 6.7 wissen wir, dass orthogonale Idempotente Objekte zerlegen können. In Lemma 6.7 haben wir gesehen, ist der Modul M unzerlegbar, so hat der Endomorphismenring $\mathrm{End}_A(M)$ ganz wenige Idempotente. Wir zeigen im Folgenden eine Korrespondenz zwischen Zerlegungen von M und Idempotenten im Endomorphismenring $\mathrm{End}_A(M)$. Hierzu benötigen wir die folgende Definition:

Definition 6.9. Sei A eine Algebra.

a) Ein Idempotent $e \neq 0$ heisst *primitiv*, falls e nicht als Summe $e = e_1 + e_2$ von orthogonalen Idempotenten $e_1, e_2 \in A$, beide ungleich Null, geschrieben werden kann.

b) Sind $e_1, \ldots, e_n \in A$ paarweise orthogonale Idempotente mit $1_A = e_1 + \ldots + e_n$, so sprechen wir von einer *Zerlegung der Eins in eine Summe paarweiser orthogonaler Idempotente.* Sind hierbei die Idempotente e_i zusätzlich alle primitiv, so sprechen wir von einer *Zerlegung der Eins als Summe primitiver und paarweise orthogonaler Idempotente.*

Beispiel 6.10. Wir pausieren, um durch Beispiele das Nachfolgende zu motivieren:

a) Algebren können sehr viele Idempotente haben. Beispielsweise gibt es in $M_2(K)$ die Idempotente:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 3 & -3 \\ 2 & -2 \end{pmatrix}, \ldots$$

Welche dieser Idempotente sind aber primitiv?

b) Man sieht leicht, warum es unzählige Idempotente in der Matrixalgebra $M_n(K)$ oder anderen Algebren gibt: Sei A eine Algebra und $a \in A$ invertierbar. Ist e_1 ein Idempotent, so ist auch ae_1a^{-1} ein Idempotent; sind die Idempotente e_1 und e_2 orthogonal, so gilt dies auch für ae_1a^{-1} und ae_2a^{-1}, denn für $i, j \in \{1, 2\}$ gilt:

$$(ae_ia^{-1}) \cdot (ae_ja^{-1}) = ae_ie_ja^{-1} = a \cdot \delta_{ij} \cdot a^{-1} = \begin{cases} ae_ia^{-1} & \text{falls } i = j \text{ ist,} \\ 0 & \text{sonst.} \end{cases}$$

c) Wir greifen Aufgabe 1.4 auf. Betrachte $A = K[X]/(X^2) = K\text{-Span}\{\bar{1}, \bar{X}\}$. Welche Idempotente besitzt die Algebra A? Sei $e = a + b\bar{X} \in A$ ein Idempotent. Dann ist

$$a + b\bar{X} = e = e^2 = (a + b\bar{X})^2 = a^2 + 2ab\bar{X} + b^2\bar{X}^2 = a^2 + 2ab\bar{X},$$

da $\bar{X}^2 = 0$ ist. Koeffizientenvergleich der Basisvektoren liefert $a^2 = a$ und $b = 2ab$, das heisst, es ist $a \in \{0, 1\}$. Falls $a = 0$ ist, so ist $b = 0$. Falls $a = 1$ ist, so ist $b = 2b$ also $b = 0$. Damit sind also 0 und 1 die einzigen Idempotente in A. Entsprechend ist 1_A ein primitives Idempotent. Mit dem unten aufgeführten Lemma 6.11 folgt, dass der Modul ${}_AA$ unzerlegbar ist – vergleiche auch mit Beispiel 6.3.

d) In Aufgabe 1.4 haben wir auch alle Idempotente in der Algebra $A = \mathbb{C}C_3$ bestimmt. Sei $C_3 = \langle g \mid g^3 = 1 \rangle$. Sei ζ eine primitive dritte Einheitswurzel. Dann hat die Algebra $\mathbb{C}C_3$ genau acht Idempotente, nämlich

$$\begin{aligned} e_1 &= \frac{1}{3}(1 + g + g^2) \\ e_2 &= \frac{1}{3}(1 + \zeta g + \zeta^2 g^2) \\ e_3 &= \frac{1}{3}(1 + \zeta^2 g + \zeta g^2), \end{aligned}$$

sowie die Elemente $0, e_1+e_2, e_1+e_3, e_2+e_3$ und 1. Da wir alle Idempotente der Algebra A aufgelistet haben, können wir daran ablesen: die Idempotente e_1, e_2 und e_3 sind primitive Idempotente und es ist $1 = e_1 + e_2 + e_3$ eine Zerlegung der Eins als Summe primitiver und paarweise orthogonaler Idempotente. Wir wissen vom Lösen von Aufgabe 1.4, dass es im Allgemeinen unangenehm ist, alle Idempotente einer Algebra zu berechnen. Bemerkung 6.13 und Theorem 6.14 geben an, wie man Aufgabe 1.4 mit Darstellungstheorie lösen kann.

e) Sei K ein Körper der Charakteristik ungleich zwei. Ist $B \leq A$ eine Unteralgebra (mit gleicher Eins, nach Definition 1.12) und $e \in B$ primitiv, dann ist $e \in A$ nicht notwendigerweise primitiv. Beispielsweise sei $H = \{1\}$ die triviale Untergruppe der Gruppe $G = \{1, x\} = \langle x \mid x^2 = 1 \rangle$. Dann ist 1 ein primitives Idempotent in $B := KH$, denn angenommen $\lambda \in KH$ ist Idempotent, dann ist $\lambda \in K$ mit $\lambda^2 = \lambda$, also $\lambda \in \{0, 1\}$. Aber 1 ist nicht primitiv in der grösseren Algebra $A := KG$: es sind $e_1 = \frac{1}{2}(1 + x)$ und $e_2 = \frac{1}{2}(1 - x)$ Idempotente in KG mit

$$1 = e_1 + e_2 \text{ und } e_1 \cdot e_2 = \frac{1}{2}(1 + x) \cdot \frac{1}{2}(1 - x) = \frac{1}{4}(1 - x^2) = 0.$$

Sind die Idemptente e_1 und e_2 primitiv in der Algebra KG?

Lemma 6.11. *Sei $0 \neq M$ ein A-Modul und $0 \neq e \in \mathrm{End}_A(M)$ Idempotent. Dann ist e genau dann primitiv, wenn $\mathrm{im}(e) \subseteq M$ ein unzerlegbarer Untermodul von M ist. Insbesondere ist ein Idempotent $0 \neq e \in A$ genau dann primitiv, wenn $Ae \leq {}_AA$ ein unzerlegbarer Untermodul ist.*

Beweis.

a) Sei $0 \neq e \in \mathrm{End}_A(M)$ ein primitives Idempotent. Nach Definition ist zunächst $e : M \to M$ ein Homomorphismus. Das Bild $\mathrm{im}(e)$ ist nach Beispiel 2.20 ein Untermodul von M. Angenommen $\mathrm{im}(e)$ zerfällt, das heisst, es existieren Untermoduln U, V von $\mathrm{im}(e)$ mit $\mathrm{im}(e) = U \oplus V$. Sei

$$\begin{aligned} e_U &: M \to M, \text{definiert als die Projektion von } M \text{ auf } U \text{ entlang } V, \\ e_V &: M \to M, \text{definiert als die Projektion von } M \text{ auf } V \text{ entlang } U. \end{aligned}$$

Wir erinnern an Lineare Algebra: ist $e(m) = u + v$ mit $m \in M$ und (eindeutigen) $u \in U$ und $v \in V$, so ist $e_U(m) = u$ und $e_V(m) = v$ nach Definition. Insbesondere ist also $e = e_U + e_V$, und e_U und e_V sind Idempotente (siehe zum Beispiel den Beweis von Lemma 6.8, Teil b)) und diese sind orthogonal:

$$(e_U \circ e_V)(m) = e_U(v) = 0, \text{ und } (e_V \circ e_U)(m) = e_V(u) = 0.$$

Da e primitiv ist, folgt $e_U = 0$ oder $e_V = 0$, siehe Definition 6.9. Wir erhalten also insgesamt $U = 0$ oder $V = 0$, das heisst, $\mathrm{im}(e)$ ist unzerlegbar.

b) Umgekehrt, sei nun $\mathrm{im}(e) \leq M$ ein unzerlegbarer Untermodul von M und es sei $e = e_1 + e_2$ eine Zerlegung von Idempotent e als Summe orthogonaler Idempotente $e_1, e_2 \in \mathrm{End}_A(M)$. Sei $e_2(m) \in \mathrm{im}(e_2)$ beliebig. Dann ist

$$e(e_2(m)) = (e \circ e_2)(m) = ((e_1 + e_2) \circ e_2)(m) = (\underbrace{e_1 \circ e_2}_{=0} + e_2^2)(m) = e_2(m).$$

Es ist also $e_2(m) \in \operatorname{im}(e)$ für alle $m \in M$, beziehungsweise $\operatorname{im}(e_2) \subseteq \operatorname{im}(e)$. Analog ist $\operatorname{im}(e_1) \subseteq \operatorname{im}(e)$ Untermodul, und damit ist auch die Summe der beiden Untermoduln im Bild von e enthalten: $\operatorname{im}(e_1) + \operatorname{im}(e_2) \subseteq \operatorname{im}(e)$. Da

$$e(m) = (e_1 + e_2)(m) = e_1(m) + e_2(m) \in \operatorname{im}(e_1) + \operatorname{im}(e_2), \text{ für alle } m \in M,$$

folgt Gleichheit, also $\operatorname{im}(e_1) + \operatorname{im}(e_2) = \operatorname{im}(e)$. Diese letzte Summenzerlegung ist eine Zerlegung als direkte Summe: Angenommen es ist $e_1x = e_2y$ ein Element im Schnitt $\operatorname{im}(e_1) \cap \operatorname{im}(e_2)$, so ist $e_1(x) = e_1^2(x) = e_1e_2(y) = 0$, und damit der Schnitt trivial, also $\operatorname{im}(e_1) \oplus \operatorname{im}(e_2) = \operatorname{im}(e)$. Da aber $\operatorname{im}(e)$ unzerlegbar ist, ist entweder $\operatorname{im}(e_1) = 0$ oder $\operatorname{im}(e_2) = 0$, also $e_1 = 0$ oder $e_2 = 0$.

c) Ist $M = {}_AA$ der reguläre Modul, so ist nach Aufgabe 2.9 die entgegengesetzte Algebra A^{op} isomorph zum Endomorphismenring $\operatorname{End}_A(A) = \{r_a \mid a \in A\}$, mittels der Bijektion $a \to r_a$, wobei r_a der Homomorphismus „Multiplikation mit a von rechts“ ist. Unter dieser Bijektion korrespondieren (primitive) Idempotente in A beziehungsweise A^{op} zu (primitiven) Idempotenten in $\operatorname{End}_A(A)$:

$$f = f^2 \text{ korrespondiert zu } r_f = r_{f^2} = r_f \circ r_f,$$

und eine Zerlegung $f = f_1 + f_2$ in orthogonale Idempotente korrespondiert zu einer Zerlegung $r_f = r_{f_1+f_2} = r_{f_1} + r_{f_2}$ in orthogonale Idempotente, denn

$$0 = f_1 \cdot f_2 \text{ genau dann, wenn } 0 = r_0 = r_{f_1f_2} = r_{f_1} \circ r_{f_2}.$$

Ist e ein Idempotent in $\operatorname{End}_A(A)$, so garantiert die Zuordnung $f \to r_f =: e$ ausserdem, dass $\operatorname{im}(e) = \operatorname{im}(r_f) = A \cdot f \subseteq A$ ist, und nach obigem Beweis ist e beziehungsweise f primitiv, genau dann, wenn $\operatorname{im}(e) = Af$ ein unzerlegbarer Untermodul von ${}_AA$ ist. □

Beispiel 6.12. Wir machen Beispiele zu Lemma 6.11.

a) Sei $A = M_n(K)$ die Matrixalgebra über dem Körper K. Dann sind die Matrizen E_{ii} für $1 \leq i \leq n$ paarweise orthogonale Idempotente in der Algebra A mit $1 = \sum_{i=1}^n E_{ii}$. Es ist $AE_{ii} \simeq K^n$ nach Beispiel 3.4 ein einfacher und damit nach Bemerkung 6.2 unzerlegbarer Modul. Also ist das Idempotent E_{ii} primitiv nach Lemma 6.11. Damit ist $1 = \sum_{i=1}^n E_{ii}$ eine Zerlegung der Eins in eine Summe primitiver und orthogonaler Idempotente.

b) Sei $A = KQ$ eine endlich-dimensionale Wegealgebra mit Köcher Q (ohne Schleifen und Zykel, siehe Proposition 1.27) über dem Körper K. Sei hierbei $Q_0 = \{1, \ldots, n\}$ die Punktemenge von Q, und sei e_i der faule Weg am Punkt i. Dann ist $1 = e_1 + \ldots + e_n$ eine Zerlegung der Eins in eine Summe primitiver und paarweise orthogonaler Idempotente: Nach Bemerkung 1.26 sind die faulen Wege e_i paarweise orthogonale Idempotente. Nach Beispiel 6.4 sind die Moduln Ae_i unzerlegbar. Nach Lemma 6.11 sind also die Idempotente e_i primitiv.

Aufgabe 6.3. a) Sei $A = M_n(K)$. Zeigen Sie, dass die Matrix $B = (b_{ij})$ mit $b_{ij} = \frac{1}{n}$ für $1 \leq i, j \leq n$ ein primitives Idempotent in der Algebra A ist. Welche der 2×2-Matrizen in Beispiel 6.10 a) sind primitive Idempotente in $M_2(K)$?

b) Sei $A = KQ$ eine endlich-dimensionale Wegealgebra über dem Körper K mit Punktemenge $Q_0 = \{1, \ldots, n\}$. Beweisen Sie ohne Verwendung von Beispiel 6.4 und Lemma 6.11, dass die faulen Wege e_i primitive Idempotente sind. Zeigen Sie hierzu zunächst: Ist $e_i = f + g$ eine Zerlegung in orthogonale Idempotente f, g, dann ist $f \in e_iAe_i$. Folgern Sie durch Nachrechnen, dass dann $f = e_i$ oder $f = 0$ ist.

Bemerkung 6.13. Sei A eine Algebra. Die Zerlegung der Eins als Summe primitiver, paarweise orthogonaler Idempotente, etwa $1_A = \sum_{i=1}^n e_i$, ist nicht eindeutig. Sei $a \in A$ invertierbar. Dann ist auch $1_A = a \cdot 1 \cdot a^{-1} = \sum_{i=1}^n (ae_ia^{-1})$ eine Zerlegung der Eins in primitive, paarweise orthogonale Idempotente. Beispielsweise gilt für $A = M_2(K)$, dass $1 = E_{11} + E_{22}$ eine solche Zerlegung ist, siehe Beispiel 6.12. Wähle

$$a = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \text{ das heisst } a^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

Dann ist

$$1 = I_2 = aE_{11}a^{-1} + aE_{22}a^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}$$

eine Zerlegung der Eins in primitive, paarweise orthogonale Idempotente. Ohne dass wir dies an dieser Stelle beweisen, es gilt: Jede Zerlegung der Eins in primitive, paarweise orthogonale Idempotente entsteht auf diese Weise. Wir kommen am Ende des Kapitels hierauf zurück.

Beweis. Für $1 \leq i \leq n$ sind nach Beispiel 6.10 b) die Elemente ae_ia^{-1} Idempotente und paarweise orthogonal zueinander, denn $afga^{-1} = 0$ genau dann, wenn $fg = 0$ ist. Also ist $e_i = f + g$ genau dann eine Summe orthogonaler Idempotente f, g, wenn $(ae_ia^{-1}) = afa^{-1} + aga^{-1}$ eine Summe orthogonaler Idempotente ist. Also ist e_i genau dann primitiv, wenn ae_ia^{-1} primitiv ist. □

Theorem 6.14. *Sei $0 \neq M$ ein A-Modul. Dann existiert eine Bijektion zwischen den folgenden Mengen:*

- *Zerlegungen $M = M_1 \oplus \ldots \oplus M_n$ als direkte Summe (unzerlegbarer) A-Moduln,*
- *Zerlegungen $1 = e_1 + \ldots + e_n$ in $\mathrm{End}_A(M)$ als Summe (primitiver) paarweise orthogonaler Idempotente.*

Insbesondere erhalten wir für den regulären Modul $M = {}_AA$ eine Bijektion zwischen

- *Zerlegungen $A = A_1 \oplus \ldots \oplus A_n$ als direkte Summe (unzerlegbarer) A-Moduln,*
- *Zerlegungen $1_A = e_1 + \ldots + e_n$ in A als Summe (primitiver) paarweise orthogonaler Idempotente.*

Beweis.

a) Sei $M = \bigoplus_{i=1}^n M_i$ eine Zerlegung von M als direkte Summe von Untermoduln M_i. Sei $e_i : M \to M$ die Projektion von M auf M_i entlang $\bigoplus_{j \neq i} M_j$. Dann ist $1 = \mathrm{id} = \sum_{i=1}^n e_i$ eine Zerlegung der Eins $1 \in \mathrm{End}_A(M)$ in paarweise orthogonaler Idempotente.

b) Umgekehrt, sei $1 = \sum_{i=1}^n e_i$ eine Zerlegung von $1 = \mathrm{id}$ im Endomorphismenring $\mathrm{End}_A(M)$ als Summe paarweiser orthogonaler Idempotente. Definiere die Untermodul $M_i := \mathrm{im}(e_i) \leq M$. Wir zeigen, dann ist $M = \bigoplus_{i=1}^n M_i$ eine Zerlegung des Moduls M als direkte Summe von Untermoduln:

   Nach 2.24 b) ist $\sum_{i=1}^n M_i \subseteq M$. Es gilt sogar Gleichheit, denn
   $$m = \mathrm{id}(m) = \sum_i e_i(m) \in \sum_i M_i, \text{für alle } m \in M.$$
   Angenommen es ist $x \in M_i \cap \bigoplus_{j \neq i} M_j$ für einen Index i mit $1 \leq i \leq n$. Dann existieren Elemente $m_1, \dots m_n \in M$ mit
   $$x = e_i(m_i) = e_i^2(m_i) = e_i(x) = e_i(\sum_{j \neq i} e_j(m_j)) = \sum_{j \neq i} (e_i \circ e_j)(m_j) = 0.$$
   Damit ist die Summe eine direkte Summe, also $M = \bigoplus_i M_i$.

c) Die beiden Zuordnungen in a) und b) sind invers zueinander und nach Lemma 6.11 ist e_i genau dann primitiv, wenn M_i unzerlegbar ist. Damit ist die erste der beiden Bijektionen bewiesen. Die zweite Bijektion folgt, indem wir $M = {}_A A$ wählen und die Korrespondenz in Aufgabe 2.9 benutzen. Siehe auch den Beweis von Lemma 6.11. $\square$

Aufgabe 6.4. Sei $A = \mathbb{R}[X]/(X^3 - X)$ und $B = \mathbb{R}[X]/(X^3 + X)$. Bestimmen Sie alle primitiven Idempotente der Algebren A und B, sowie jeweils eine Zerlegung der Eins in primitive paarweise orthogonale Idempotente.

Aufgabe 6.5. Sei $A = KQ$ Wegealgebra mit Köcher $Q = \{1, 2, 3, 4\}$ und Pfeilen wie in den Bildern unten angegeben. Bestimmen Sie für die folgenden A-Moduln (gegeben als Darstellungen von Q) jeweils den Endomorphismenring $\mathrm{End}_A(M_i)$ sowie eine Zerlegung von M_i, mit $i = 1, 2$, in unzerlegbare direkte Summanden für:

$$M_1 = \begin{tikzcd} K \arrow[dr, "\binom{1}{0}"] & & \\ & K^2 \arrow[r, "(1\ 1)"] & K \\ K \arrow[ur, "\binom{0}{1}"'] & & \end{tikzcd} \qquad M_2 = \begin{tikzcd} K \arrow[dr, "\binom{1}{0}"] & & \\ & K^2 \arrow[r, "(1\ 1)"] & K \\ K \arrow[ur, "\binom{1}{0}"'] & & \end{tikzcd}$$

Aufgabe 6.6. Sei A eine K-Algebra und $0 \neq M$ ein A-Modul mit Zerlegung $M = U_1 \oplus \ldots \oplus U_r$ in eine direkte Summe von Untermoduln. Sei $f : M \to M$ ein A-Modulisomorphismus. Zeigen Sie, dass dann $M = f(M) = f(U_1) \oplus \ldots \oplus f(U_r)$ eine Zerlegung von M in eine direkte Summe von Untermoduln ist.

6.3 Lokale Algebren

Lokale Ringe werden in der kommutativen Algebra beziehungsweise algebraischen Geometrie studiert, um lokales Verhalten von Funktionen auf algebraischen Varietäten zu studieren. Wir wollen sie nutzen, um unzerlegbare Moduln zu charakterisieren. Diese Zwischenresultate helfen uns dann, um in Abschnitt 6.4 unser Hauptresultat, den Satz von Krull-Remak-Schmidt beweisen zu können. Sei A eine Algebra über einem Körper K.

Das folgende Resultat ist unter Umständen bereits aus der Linearen Algebra bekannt. Es wird auch als Fitting Lemma bezeichnet.

Bemerkung 6.15. Sei V ein endlich-dimensionaler K-Vektorraum und $f : V \to V$ eine lineare Abbildung. Dann gibt es eine natürliche Zahl $n \in \mathbb{N}$ mit:

a) Für alle $t \geq 0$ ist $\ker(f^n) = \ker(f^{n+t})$ und $\operatorname{im}(f^n) = \operatorname{im}(f^{n+t})$.

b) Es gilt die Vektorraumzerlegung $V = \ker(f^n) \oplus \operatorname{im}(f^n)$.

Beweis.

a) Man sieht leicht, dass wir die folgenden aufsteigenden beziehungsweise abfallenden Ketten von Untervektorräumen haben:

$$0 \subseteq \ker(f) \subseteq \ker(f^2) \subseteq \ldots \subseteq V \text{ und } V \supseteq \operatorname{im}(f) \supseteq \operatorname{im}(f^2) \supseteq \ldots \supseteq 0.$$

Die Dimension von V ist endlich, also müssen diese beiden Ketten von Untervektorräumen endlich sein. Sie bestehen also aus strikten Inklusionen bis irgendwo an einer ersten Stelle in der Kette von Untermoduln ein Gleichheitszeichen auftaucht. Formal gesagt: Es existieren natürliche Zahlen n_1 und n_2 mit $\ker(f^{n_1}) = \ker(f^{n_1+1})$ und $\operatorname{im}(f^{n_2}) = \operatorname{im}(f^{n_2+1})$. Man sieht wiederum leicht, dass dann gilt $\ker(f^{n_1}) = \ker(f^{n_1+t})$ und $\operatorname{im}(f^{n_2}) = \operatorname{im}(f^{n_2+t})$ für alle $t \geq 0$. Man spricht davon, dass sich die beiden Ketten von Unterräumen stabilisieren. Es sei n das Maximum von n_1 und n_2. Dann ist also $\ker(f^n) = \ker(f^{n+t})$ und $\operatorname{im}(f^n) = \operatorname{im}(f^{n+t})$ für alle $t \geq 0$. Dies beweist die erste Behauptung.

b) Da Kern und Bild einer linearen Abbildung Unterräume von V sind, gilt

$$\ker(f^n) + \operatorname{im}(f^n) \leq V. \tag{6.1}$$

Wir müssen Gleichheit in dieser letzten Gleichung beweisen, und zeigen zunächst, dass der Schnitt der Unterräume $\ker(f^n)$ und $\operatorname{im}(f^n)$ trivial ist. Sei $x \in \ker(f^n) \cap \operatorname{im}(f^n)$. Dann ist zum einen $f^n(x) = 0$ und zum anderen existiert ein Element $y \in V$ mit $f^n(y) = x$. Es folgt

$$0 = f^n(x) = f^n(f^n(y)) = f^{2n}(y).$$

Nach Konstruktion ist $\ker(f^{2n}) = \ker(f^n)$, also ist $y \in \ker(f^{2n}) = \ker(f^n)$, was besagt, dass $x = f^n(y) = 0$ ist. Es ist also

$$\dim(\ker(f^n) \cap \dim \operatorname{im}(f^n)) = 0. \tag{6.2}$$

Bei der Modulsumme auf der linken Seite von Gleichung (6.1) handelt es sich also um eine direkte Summe. Mit den Dimensionsformeln aus der Linearen Algebra folgt:

$$\begin{aligned} \dim V &\overset{(6.1)}{\geq} \dim(\ker(f^n) + \operatorname{im}(f^n)) \\ &= \dim\ker(f^n) + \dim\operatorname{im}(f^n) - \dim(\ker(f^n) \cap \operatorname{im}(f^n)) \\ &\overset{(6.2)}{=} \dim\ker(f^n) + \dim\operatorname{im}(f^n) = \dim V, \end{aligned}$$

wobei am letzten Gleichheitszeichen der Rang-Defekt-Satz aus der Linearen Algebra für die lineare Abbildung f^n benutzt wird. Die Ungleichung in der Kette ist also Gleichheit, und damit folgt Gleichheit in Gleichung (6.1). □

Lemma 6.16 (Fitting Lemma)**.** *Sei A eine Algebra und $0 \neq M$ ein endlich-dimensionaler A-Modul.*

a) Ist $f : M \to M$ ein A-Modulhomomorphismus, so existiert eine natürliche Zahl $n \in \mathbb{N}$ mit $M = \ker(f^n) \oplus \operatorname{im}(f^n)$.

b) Es ist M genau dann unzerlegbar, wenn für alle Endomorphismen $f \in \operatorname{End}_A(M)$ gilt: entweder ist f ein Isomorphismus oder f ist nilpotent.

Beweis. Jeder Modulhomomorphismus über einer K-Algebra ist eine lineare Abbildung. Bemerkung 6.15 liefert also eine Vektorraumzerlegung. Die Zerlegung ist in diesem Fall sogar eine Modulzerlegung, da das Bild und der Kern eines Modulhomomorphismus jeweils Untermoduln sind, siehe Bemerkung 2.24.

Wenn der Modul M in der zweiten Behauptung unzerlegbar ist, muss in dieser Zerlegung gelten: entweder ist $\operatorname{im}(f^n) = 0$ und $\ker(f^n) = M$, in diesem Fall ist $f^n = 0$, also f nilpotent. Oder aber es ist $\ker(f^n) = 0$. In diesem Fall ist aber bereits $\ker(f) = 0$ und damit ist f injektiv. Jede injektive lineare Abbildung zwischen endlich-dimensionalen Vektorräumen ist aber auch surjektiv, und damit folgt in diesem Fall, dass f ein Isomorphismus ist.

In der zweiten Behauptung müssen wir noch die Rückrichtung beweisen. Sei jeder Homomorphismus im Endomorphismenring $\operatorname{End}_A(M)$ entweder ein Isomorphismus oder nilpotent. Wir zeigen, dass die Algebra $\operatorname{End}_A(M)$ nur die Idempotente 0 und 1 hat. Angenommen es ist $0 \neq \epsilon \in \operatorname{End}_A(M)$ ein Idempotent. Nach Voraussetzung ist dann ϵ entweder ein Isomorphismus oder nilpotent. Angenommen ϵ ist nilpotent. Dann existiert ein m mit $\epsilon^m = 0$. Es folgt aus $\epsilon = \epsilon^2$, dass

$$\epsilon = \epsilon^2 = \epsilon^3 = \ldots = \epsilon^m = 0.$$

Angenommen ϵ ist ein Isomorphismus. Dann gilt $\operatorname{im}\epsilon = M$. Es gibt also für ein beliebiges $m \in M$ ein Element $m' \in M$ mit $\epsilon(m') = m$. Es folgt:

$$m = \epsilon(m') = \epsilon^2(m') = \epsilon(\underbrace{\epsilon(m')}_{=m}) = \epsilon(m).$$

Ist also ϵ ein Isomorphismus, so ist $\epsilon = 1$, die Identitätsabbildung auf M. Damit hat die Algebra $\operatorname{End}_A(M)$ genau zwei Idempotente, nämlich 0 und 1. Mit Lemma 6.11 folgt, dass M unzerlegbar ist. □

Bemerkung 6.17. Wir arbeiten im Folgenden mit invertierbaren Elementen. Da unsere Algebren in der Regel nicht kommutativ sind, unterscheiden wir bei invertierbaren Elementen Links- und Rechtsinverse: Ein Element a in einem Ring R ist *links invertierbar*, falls es ein Element $b \in R$ gibt mit $ba = 1$. Das Element b heisst dann ein *Linksinverses* von a. Ein Element a heisst *rechts invertierbar*, falls es ein Element $c \in R$ gibt mit $ac = 1$. Das Element c heisst dann ein *Rechtsinverses* von a. Links- oder Rechtsinverse sind nicht notwendigerweise eindeutig bestimmt. Besitzt ein Element $a \in R$ sowohl ein Linksinverses b_1 als auch ein Rechtsinverses b_2, so stimmen Links- und Rechtsinverses überein:

$$b_2 = 1 \cdot b_2 = (b_1 a) b_2 = b_1 (a b_2) = b_1 \cdot 1 = b_1,$$

und nach Definition ist a in R invertierbar. In Linearer Algebra zeigen wir: wenn eine Matrix A eine Linksinverse besitzt, dann besitzt A auch eine Rechtsinverse. Im Matrizenring $M_n(K)$ wird man also keine Elemente finden, die nur ein Links- aber kein Rechtsinverses besitzen. Solche Beispiele finden wir aber unter Funktionen. Wir betrachten den Vektorraum V, bestehend aus allen Folgen (a_n) von Elementen $a_n \in K$, wobei nur endlich viele Folgenglieder ungleich Null sind. Im Endomorphismenring von V hat das Element

$$f : V \to V, \text{ definiert durch } (a_1, a_2, \ldots) \mapsto (a_2, a_3 \ldots)$$

mehrere Rechtsinverse. Beispielsweise sind

$$\begin{aligned} g : V \to V, &\text{ definiert durch } (a_1, a_2, \ldots) \mapsto (0, a_1, a_2, \ldots) \text{ oder} \\ g : V \to V, &\text{ definiert durch } (a_1, a_2, \ldots) \mapsto (a_1, a_1, a_2, \ldots) \end{aligned}$$

Rechtsinverse des Elements f, denn $f \circ g = \mathrm{id}_V$. Zum Element f existiert aber kein Linksinverses, da die Abbildung f nicht injektiv ist.

Aufgabe 6.7. Ist in einer endlich-dimensionalen Algebra A einseitig invertierbar dasselbe wie zweiseitig invertierbar? Begründen Sie Ihre Antwort.

Beispiel 6.18. Nilpotente Elemente kommen immer zusammen mit invertierbaren Elementen: Sei M ein A-Modul. Sei $f \in \mathrm{End}_A(M)$ ein nilpotenter Endomorphismus mit $f^n = 0$. Dann ist

$$\begin{aligned} (1 + f + \ldots + f^{n-1}) \cdot (1 - f) &= (1 + f + \ldots + f^{n-1}) - (f + f^2 + \ldots + f^n) \\ &= 1 - f^n = 1, \end{aligned}$$

und ganz analog gilt $(1 - f)(1 + f + \ldots + f^{n-1}) = 1$. Damit ist das Element $(1 - f) \in \mathrm{End}_A(M)$ invertierbar in der Algebra $\mathrm{End}_A(M)$.

Definition 6.19. Eine K-Algebra A heisst *lokal*, falls für alle $a \in A$ gilt: Ist das Element a nicht invertierbar, so ist das Element $1 - a$ invertierbar in A.

Beachten Sie, dass im Beweis des folgenden Lemmas keine Einschränkung an die Dimension der Algebra A benötigt wird.

Lemma 6.20. *Für eine K-Algebra gilt:*

a) Ist A eine lokale Algebra, so sind 0 und 1 die einzigen Idempotente in A.

b) Sind 0 und 1 die einzigen Idempotente in der Algebra A, so gilt für ein beliebiges Element $a \in A$: Element a hat ein Linksinverses, genau dann, wenn a invertierbar ist.

Beweis.

a) Sei e ein Idempotent in A. Angenommen e hat ein Linksinverses. Nach Definition bedeutet dies, es existiert ein Element $b \in A$ mit $be = 1_A$. Es folgt

$$1_A = be = be^2 = (be)e = 1 \cdot e = e.$$

Ist also $1 \neq e$ in A ein Idempotent, so hat e kein Linksinverses, ist also nicht invertierbar. Da A eine lokale Algebra ist, ist somit das Element $1 - e$ in A invertierbar. Mit e Idempotent ist aber auch $1 - e$ ein Idempotent. Mit obigem Argument folgt also, dass $1 - e = 1$, also $e = 0$ ist. Wir haben damit insgesamt gezeigt, dass die Algebra A nur die Idempotente 0 und 1 hat.

b) Seien $a, b \in A$ mit $ba = 1$, das heisst, das Element a hat ein Linksinverses b. Dann folgt, dass das Element ab ein Idempotent ist: $(ab)^2 = a(ba)b = a \cdot 1 \cdot b = ab$. Es ist hierbei $0 \neq a = a(ba) = (ab)a$, also ist $ab \neq 0$. Nach Voraussetzung hat die Algebra A nur die beiden Idempotente 0 und 1. Es folgt also $ab = 1$. Damit gilt also $ab = 1 = ba$; das Element ab ist somit invertierbar. □

Theorem 6.21. *Sei $0 \neq M$ ein endlich-dimensionaler A-Modul. Der Modul M ist genau dann unzerlegbar, wenn $\mathrm{End}_A(M)$ eine lokale Algebra ist.*

Beweis.

a) Ist M unzerlegbar, so ist nach Lemma 6.16 jeder Endomorphismus in $\mathrm{End}_A(M)$ entweder nilpotent oder invertierbar. Ist der Endomorphismus f nilpotent, so folgt mit Beispiel 6.18, dass $1 - f$ invertierbar ist. Damit ist aber $\mathrm{End}_A(M)$ nach Definition 6.19 eine lokale Algebra.

b) Umgekehrt, sei $\mathrm{End}_A(M)$ eine lokale Algebra. Dann sind 0 und 1 nach Lemma 6.20 die einzigen Idempotente im Endomorphismenring. Nach Lemma 6.8 ist der Modul M damit unzerlegbar. □

Theorem 6.22. *Sei A eine Algebra über einem Körper K. Die folgenden Aussagen sind äquivalent:*

a) Algebra A ist lokal.

b) Summen nicht invertierbarer Elemente in A sind nicht invertierbar.

c) Der reguläre Modul ${}_AA$ hat einen eindeutigen maximalen Untermodul.

Der eindeutige maximale Untermodul einer lokalen Algebra besteht genau aus den nicht-invertierbaren Elementen in A. Insbesondere haben lokale Algebren endlicher Dimension bis auf Isomorphie damit genau einen einfachen Modul.

Beweis.

i) Wir zeigen a) impliziert b). Sei also A eine lokale Algebra. Seien die Elemente $x, y \in A$ beide nicht invertierbar. Angenommen die Summe hat ein Linksinverses, es existiert also ein Element $b \in A$ mit $b(x+y) = 1$. Nach Voraussetzung und Definition 6.19 ist das Element bx oder das Element $1 - bx = by$ invertierbar. Damit hat x oder y ein Linksinverses. Nach Lemma 6.20 ist somit x oder y invertierbar, ein Widerspruch. Also ist $x + y$ nicht invertierbar.

ii) Wir zeigen b) impliziert a). Sei $a \in A$. Angenommen sowohl a als auch $1 - a$ sind nicht invertierbar. Nach Voraussetzung ist dann auch $1 = a + (1 - a)$ nicht invertierbar, ein Widerspruch. Mit Definition 6.19 folgt die Behauptung.

iii) Wir zeigen a) und b) implizieren c). Hierzu definieren wir die Menge

$$U := \{x \in A \mid x \text{ nicht invertierbar in } A\} \subsetneq A.$$

Da 0 nicht invertierbar ist, ist die Menge U nicht leer. Nach Voraussetzung b) ist U abgeschlossen unter Addition. Wir wollen zeigen, dass U ein A-Modul ist. Sei $a \in A$ und $x \in U$. Angenommen das Element ax hat ein Linksinverses. Dann hat auch x ein Linksinverses. Nach Voraussetzung a) ist die Algebra A lokal. Mit Lemma 6.20 folgt, dass x in A invertierbar ist, ein Widerspruch zu $x \in U$. Also ist das Element ax nicht invertierbar, das heisst $ax \in U$. Wir haben also gezeigt, dass U ein A-Linksuntermodul von ${}_AA$ beziehungsweise ein Linksideal in A ist. Als nächstes wollen wir zeigen, dass U der eindeutige maximale Untermodul von A ist. Sei also V ein weiterer echter Untermodul von ${}_AA$. Wir zeigen, dann ist $V \subseteq U$. Angenommen es existiert ein Element $y \in V \backslash U$. Dann ist y invertierbar, und da V ein A-Modul ist, folgt $1 = y^{-1}y \in V$, also $V = A$, ein Widerspruch. Damit ist U eindeutiger maximaler Untermodul von ${}_AA$.

iv) Wir zeigen c) impliziert a), und müssen hierzu zunächst einige Vorbereitungen zum Beweis machen. Sei U der eindeutige maximale Untermodul von ${}_AA$. Ist also V ein echter Untermodul von ${}_AA$, so ist $V \subseteq U$. Angenommen $e \neq 0, 1$ ist ein Idempotent in A. Sei $V_1 := Ae$ und $V_2 := A(1 - e)$. Dann liefert e die Modulzerlegung ${}_AA = Ae \oplus A(1 - e) = V_1 \oplus V_2$ mit $V_i \subsetneq A$ für $i = 1, 2$. Nach Voraussetzung gilt dann aber $V_i \subseteq U$, für $i = 1, 2$, und damit $A = V_1 \oplus V_2 \subset U \subsetneq A$, ein Widerspruch. Es folgt, dass die Algebra A nur die Idempotente 0 und 1 hat. Diese Aussage haben wir bewiesen, damit wir im Folgenden Lemma 6.20 b) nutzen können.

Als nächstes zeigen wir, dass die Menge U genau aus den nicht-invertierbaren Elementen aus A besteht. Angenommen $a \in U$. Wie schon zuvor, ist a invertierbar, so ist $1 = a^{-1}a \in U$ und es folgt $U = A$, ein Widerspruch. Damit ist also jedes Element in U nicht invertierbar. Umgekehrt, sei nun $a \in A$ nicht invertierbar. Dann hat a nach Lemma 6.20 b) kein Linksinverses in A. Das Linksideal Aa ist also ein echter Untermodul von ${}_AA$, und damit gilt nach Voraussetzung $Aa \subseteq U$. Insbesondere ist also $a \in U$. Die Menge U enthält also genau die nicht-invertierbaren Elemente in A.

Jetzt haben wir alle Vorbereitungen für den Beweis zusammen. Sei $a \in U$. Ist $1 - a$ nicht invertierbar, so ist $1 - a \in U$, und damit $a + (1 - a) = 1 \in U$, ein Widerspruch. Also ist $1 - a$ invertierbar, und damit die Algebra A lokal nach Definition 6.19.

v) Im letzten Schritt des Beweises brauchen wir, dass die Algebra A endlichdimensional ist, oder allgemeiner, dass der reguläre Modul ${}_AA$ eine endliche Kompositionsreihe besitzt. Nach Theorem 3.30 ist jeder einfache A-Modul S isomorph zu einem Quotienten des regulären Moduls: $S \simeq A/\mathrm{Ann}(s)$ für ein $0 \neq s \in S$. Hierbei ist nach Bemerkung 3.6 also $\mathrm{Ann}(s)$ ein maximaler Untermodul von ${}_AA$. Eine lokale Algebra hat genau einen maximalen Untermodul U. Also hat eine lokale Algebra bis auf Isomorphie genau einen einfachen Modul, den Modul A/U. □

Bemerkung 6.23. Die Algebra $A = M_n(K)$ hat nach Beispiel 3.31 bis auf Isomorphie genau einen einfachen A-Modul, aber A ist nicht lokal für $n \geq 2$. Beispielsweise ist der bis auf Isomorphie eindeutige einfache Modul von $M_2(K)$ zwei-dimensional, siehe Beispiel 3.4. Maximale Ideale in $M_2(K)$ haben also Dimension $4 - 2 = 2$. Die Algebra $M_2(K)$ hat beispielsweise die beiden maximalen Linksideale

$$\begin{pmatrix} K & 0 \\ K & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & K \\ 0 & K \end{pmatrix}.$$

Damit hat Algebra $M_2(K)$ mehr als ein maximales Linksideal, ist damit nach Theorem 6.22 nicht lokal. Es gibt also Algebren, die bis auf Isomorphie genau einen einfachen Modul haben, aber nicht lokal sind.

Beispiel 6.24. a) $A = K$ ist lokal nach Definition 6.19, denn ist $a \in K$ nicht invertierbar, dann ist $a = 0$ und es folgt $1 = 1 - a \in K$ ist invertierbar.

b) Sei $A = K[X]/(f)$ mit $f \in K[X]$ ein Polynom positiven Grades. Dann ist A genau dann eine lokale Algebra, wenn $f = g^n$ ist für ein irreduzibles Polynom $g \in K[X]$ und $n \in \mathbb{N}$: Ist $f = g^n$ mit g irreduzibel, so ist nach Bemerkungen 5.3 und 5.6 der reguläre Modul ${}_AA$ uniseriell und $(g)/(f)$ der eindeutige maximale Untermodul des regulären Moduls. Ist umgekehrt f das Produkt von mindestens zwei irreduziblen Polynomen, so folgt nach Theorem 5.5, dass die Algebra A mindestens zwei nicht-isomorphe einfache Moduln hat. Nach Theorem 6.22 ist sie somit nicht lokal.

c) Sei $A = KQ$ eine Wegealgebra mit Köcher Q. Angenommen die Punktemenge Q_0 besitzt mindestens zwei Elemente. Die faulen Wege in A sind Idempotente. Dann besitzt also A ein Idempotent $e \neq 0, 1$. Nach Lemma 6.20 a) ist also A nicht lokal. Sei also $Q_0 = \{1\}$ Menge mit einem Punkt. Angenommen $Q_1 = \{\alpha_1, \dots \alpha_n\}$ für ein $n \geq 1$. Dann ist $A \simeq K\langle X_1, \dots, X_n\rangle$, die freie Algebra in den n nicht kommutierenden Variablen $X_1, \dots, X_n$. Für jede Variable X_i folgt aus Gradbetrachtungen, dass weder X_i noch das Element $1 - X_i$ invertierbar ist. Nach Definition 6.19 ist also die Algebra A nicht lokal. Eine Wegealgebra $A = KQ$ ist also genau dann lokal, wenn $A = KQ \simeq K$ ist.

Aufgabe 6.8. Sei A eine endlich-dimensionale Algebra über einem Körper K. Zeigen Sie, dass A genau dann lokal ist, wenn 0 und 1 die einzigen Idempotente in A sind. Zeigen Sie auch mit Hilfe eines Gegenbeispiels, dass diese Äquivalenz falsch ist für unendlich-dimensionale Algebren.

Aufgabe 6.9. Sei K ein beliebiger Körper, sei L ein Körper von Primcharakteristik $p > 0$. Welche der folgenden Algebren sind lokal? Begründen Sie jeweils Ihre Antwort.

a) $\mathbb{Q}[X]/(X^n - 1)$ für $n \geq 2$;

b) $L[X]/(X^p - 1)$;

c) $K[X]/(X^3 - 9X^2 + 27X - 27)$;

d) A endlich dimensionale halbeinfache K-Algebra mit $\dim A > 1$;

e) $T_n(K)$ für $n \geq 2$;

f) $A = \{(a_{ij}) \in T_n(K) \mid a_{11} = a_{22} = \ldots = a_{nn}\}$;

g) $K[[X]] = \{\sum_{i=0}^{\infty} \lambda_i X^i\}$ der Ring der formalen Potenzreihen.

Aufgabe 6.10. Sei K ein Körper der Charakteristik $p > 0$. Sei G eine Gruppe der Ordnung p^n mit $n \in \mathbb{N}$. Zeigen Sie, dass die Algebra KG lokal ist.

6.4 Der Satz von Krull-Remak-Schmidt

Sei A eine Algebra über einem Körper K. Wir haben alle Vorbereitungen getroffen, um das Hauptresultat des Kapitels beweisen zu können. Nach Theorem 6.6 besitzt jeder Modul $0 \neq M$ eine Zerlegung als direkte Summe unzerlegbarer Summanden. Wir zeigen, dass diese eindeutig ist, bis auf Isomorphie und Reihenfolge der Summanden. Im Fall $A = K$ sind A-Moduln gerade Vektorräume, und das Resultat ist für uns so vertraut, dass es wenig erstaunlich wirkt. In der Darstellungstheorie ist es, wie der längliche Beweis andeutet, ein tieferes Resultat, und von grosser Bedeutung. Wir benötigen das folgende Resultat:

Lemma 6.25. *Sei A eine K-Algebra unf M, N, U nicht-triviale A-Moduln. Seien $f : M \to U$ und $g : U \to N$ Modulhomomorphismen, so dass $g \circ f : M \to N$ ein Isomorphismus ist. Dann ist f injektiv und g surjektiv und der Modul U zerfällt als $U = \mathrm{im}(f) \oplus \ker(g)$.*

Beweis. Die erste Behauptung ist aus der Linearen Algebra bekannt und der Leserin überlassen. Wir zeigen die zweite Behauptung. Es ist $\ker(g) + \mathrm{im}(f)$ Untermodul von U nach Bemerkung 2.24 und Beispiel 2.20. Sei $x \in \ker(g) \cap \mathrm{im}(f)$. Dann existiert ein $m \in M$ mit $f(m) = x$ und $g(x) = 0$. Es ist also $0 = g(x) = g(f(m))$, und da nach Voraussetzung $g \circ f$ injektiv ist, folgt $m = 0$, also auch $x = 0$. Also ist

$$\ker g \oplus \operatorname{im} f \leq U, \tag{6.3}$$

und wir zeigen, dass Gleichheit gilt. Sei $h : N \to M$ die Inverse zu $g \circ f$. Sei $x \in U$ beliebig. Dann ist $x = \underbrace{(f \circ h \circ g)(x)}_{\in \operatorname{im}(f)} + \underbrace{(x - (f \circ h \circ g)(x))}_{\in \ker(g)} \in \operatorname{im}(f) + \ker(g)$, denn

$$g(x - (f \circ h \circ g)(x)) = g(x) - (\underbrace{g \circ f \circ h}_{= \mathrm{id}_N} \circ g)(x) = g(x) - g(x) = 0.$$

Also folgt Gleichheit in Gleichung (6.3). $\square$

Theorem 6.26 (Krull-Remak-Schmidt). *Sei A eine Algebra und $0 \neq M$ ein endlich-dimensionaler A-Modul. Seien*

$$\begin{aligned} M &= M_1 \oplus \ldots \oplus M_s, \\ M &= N_1 \oplus \ldots \oplus N_t \end{aligned}$$

zwei Zerlegungen von M als direkte Summe unzerlegbarer Moduln. Dann gilt $s = t$ und es existiert eine Permutation $\sigma \in S_t$ mit $M_i \simeq N_{\sigma(i)}$, für $1 \leq i \leq t$.

Bemerkung. Wir beweisen die folgende allgemeinere Behauptung: Seien

$$M = \bigoplus_{i=1}^{s} M_i \text{ und } N = \bigoplus_{j=1}^{t} N_j$$

Zerlegungen von M beziehungsweise N als direkte Summe unzerlegbarer Untermoduln M_i beziehungsweise N_j. Sei $\varphi : M \to N$ ein Isomorphismus. Dann ist $s = t$ und es existiert eine Permutation $\sigma \in S_t$ mit $M_i \simeq N_{\sigma(i)}$. Der Satz von Krull-Remak-Schmidt folgt dann als Spezialfall mit $M = N$ und $\varphi = \mathrm{id}_M$.

Notation. Wir schreiben im Folgenden Modulhomomorphismen als Matrizen, in Analogie zu Theorem 4.20 und Lemma 4.19. Sei $\varphi : M \to N$ ein Isomorphismus. Wir identifizieren φ entsprechend der direkten Summenzerlegungen von $M = \bigoplus_{i=1}^{s} M_i$ und $N = \bigoplus_{j=1}^{t} N_j$ mit der $t \times s$-Matrix $(\varphi_{ij})_{1 \leq i \leq t, 1 \leq j \leq s}$. Damit ist also φ_{ij} definiert durch

$$\varphi_{ij} : M_j \xrightarrow{\iota_j} M \xrightarrow{\varphi} N \xrightarrow{\pi_i} N_i,$$

mit $\pi_i : N \to N_i$ der Projektion von M auf den direkten Summanden M_i, entlang $\bigoplus_{t \neq i} M_t$ und mit $\iota_j : M_j \to M$ der Einbettung von M_j in M, definiert durch $m \mapsto m$ für $m \in M_j$. Nach Voraussetzung ist φ bijektiv, besitzt also eine Inverse. Sei $\psi = \varphi^{-1}$. Wiederum identifizieren wir ψ in Analogie zu Theorem 4.20 mit einer Matrix. Dann entspricht ψ der $s \times t$-Matrix $(\psi_{ij})_{1 \leq i \leq s, 1 \leq j \leq t}$ und ψ_{ij} ist definiert durch:

$$\psi_{ij} : N_j \xrightarrow{\iota_j} N \xrightarrow{\varphi^{-1}} M \xrightarrow{\pi_i} M_i,$$

mit $\pi_i : M \to M_i$ der Projektion von M auf den direkten Summanden M_i, entlang $\bigoplus_{t \neq i} M_t$ und mit $\iota_j : N_j \to N$ der Einbettung von N_j in N, definiert durch $m \mapsto m$ für $m \in N_j$.

Beweis der Bemerkung. Wir machen Induktion über die Anzahl s der Summanden der Zerlegung von M. Ist $s = 1$, so ist $M = M_1$ unzerlegbar. Dann folgt, dass $\varphi(M) = N$ unzerlegbar ist, siehe Aufgabe 6.6. Es ist also $t = 1$ und $N_1 = N \simeq M = M_1$.

Sei nun $s > 1$ und die Behauptung bewiesen für Moduln mit einer Zerlegung in $s - 1$ unzerlegbare direkte Summanden.

a) Wir bestimmen im ersten Schritt einen Summanden N_l mit $N_l \simeq M_1$. Im Beweis werden wir sehen, dass wir ohne Einschränkung $l = 1$ wählen können.

   Wegen $\psi\varphi = \mathrm{id}_M$ gilt für die Matrizen das Matrixprodukt $(\psi_{ij}) \cdot (\varphi_{ij}) = \mathrm{diag}(\mathrm{id}_{M_1}, \ldots \mathrm{id}_{M_s})$. Nach Definition des Produktes von zwei Matrizen ist der Eintrag in Position $(1, 1)$ dieses Matrixproduktes gerade

$$\sum_{l=1}^{t} \psi_{1l}\varphi_{l1} = \mathrm{id}_{M_1} . \tag{6.4}$$

   Nach Theorem 6.21 ist der Endomorphismenring $\mathrm{End}_A(M_1)$ des unzerlegbaren Moduls M_1 lokal. Es ist $\psi_{1l}\varphi_{l1} \in \mathrm{End}_A(M_1)$ für alle $1 \leq l \leq t$. Da die Abbildung id_{M_1} auf der rechten Seite der Gleichung (6.4) invertierbar ist, ist nach Theoem 6.22 ist einer der Summanden $\psi_{1l}\varphi_{l1}$ auf der linken Seite der Gleichung (6.4) invertierbar. Durch Umsortieren der Summanden $N_1, \ldots, N_t$ erreichen wir, dass ohne Einschränkung $l = 1$ gewählt werden kann, also $\psi_{11}\varphi_{11}$ invertierbar ist.

b) Nach a) ist $\psi_{11}\varphi_{11}$ ein Isomorphismus. Mit Lemma 6.25 folgt, dass φ_{11} injektiv ist und ψ_{11} surjektiv, und $N_1 = \mathrm{im}(\varphi_{11}) \oplus \ker(\psi_{11})$. Da ψ_{11} ungleich der Nullabbildung ist und N_1 nach Voraussetzung unzerlegbar ist, folgt $N_1 = \mathrm{im}(\varphi_{11})$ und $\ker(\psi_{11}) = 0$. Damit sind φ_{11} und ψ_{11} Isomorphismen.

c) In diesem Schritt machen wir den eigentlichen Beweis der Bemerkung. Wir definieren dazu die folgenden beiden Homomorphismen

$$\alpha = \begin{pmatrix} \mathrm{id}_{N_1} & 0 & \ldots & 0 \\ -\varphi_{21}\varphi_{11}^{-1} & \mathrm{id}_{N_2} & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -\varphi_{t1}\varphi_{11}^{-1} & 0 & \ldots & \mathrm{id}_{N_t} \end{pmatrix}, \beta = \begin{pmatrix} \mathrm{id}_{M_1} & -\varphi_{11}^{-1}\varphi_{12} & \ldots & -\varphi_{11}^{-1}\varphi_{1s} \\ 0 & \mathrm{id}_{M_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \mathrm{id}_{M_s} \end{pmatrix}.$$

   Die beiden angegebenen Matrizen sind untere beziehungsweise obere Dreiecksmatrizen, ihre Determinanten entsprechen also gerade dem Produkt der Diagonaleinträge. Da die Determinanten beide ungleich der Nullabbildung sind, sind die Abbildungen α und β invertierbar. Wir definieren nun den Homomorphismus

$$\varphi' : M \xrightarrow{\beta} M \xrightarrow{\varphi} N \xrightarrow{\alpha} N.$$

   Da alle drei Abbildungen Isomorphismen sind, ist auch φ' ein Isomorphismus. Wir rechnen in b) nach, dass in Matrixschreibweise gilt:

$$\varphi' = \left(\begin{array}{c|c} \varphi_{11} & 0 \\ \hline 0 & \phi \end{array}\right) \tag{6.5}$$

Es ist hierbei $\phi : \bigoplus_{i=2}^s M_i \to \bigoplus_{j=2}^t N_j$. Da φ' ein Isomorphismus ist und φ_{11} Isomorphismus ist, folgt aus Gleichung (6.5) auch dass ϕ ein Isomorphismus ist. Mit der Induktionsvoraussetzung folgt dann die Richtigkeit der Bemerkung.

d) Wir müssen noch die Richtigkeit von Gleichung (6.5) bestätigen. Wir berechnen hierzu die Einträge für die erste Zeile und erste Spalte im Matrixprodukt $\varphi' = \alpha\varphi\beta$. Zu gegebener Matrix C bezeichnet C_{ij} den (i, j)-ten Eintrag von C. Aus der Definition von Matrixmultiplikation folgt:

$$(\alpha\varphi\beta)_{lu} = \sum_{a=1}^{s} (\alpha\varphi)_{la}\beta_{au} = \sum_{a=1}^{s}\sum_{b=1}^{t} \alpha_{lb}\varphi_{ba}\beta_{au}.$$

Wir nutzen in den folgenden Rechnungen, dass $\alpha_{1b} = 0$ ist für alle $b \geq 2$ und $\alpha_{11} = \mathrm{id}_{N_1}$ ist, sowie $\beta_{a1} = 0$ für $a \geq 2$. Dann gilt für die Einträge in der ersten Zeile der Matrix in Gleichung (6.5)

$$\begin{aligned} \varphi'_{1u} &= \sum_{a=1}^{s}\sum_{b=1}^{t} \alpha_{1b}\varphi_{ba}\beta_{au} = \sum_{a=1}^{s} \varphi_{1a}\beta_{au} \\ &= \begin{cases} \varphi_{11} & \text{für } u = 1, \\ -\varphi_{11}\varphi_{11}^{-1}\varphi_{1u} + \varphi_{1u}\,\mathrm{id} = 0 & \text{sonst.} \end{cases} \end{aligned}$$

Und analog gilt für die Einträge $(l, 1)$ mit $l \geq 2$ in der ersten Spalte von Matrix φ':

$$\varphi'_{l1} = \sum_{a=1}^{s}\sum_{b=1}^{t} \alpha_{lb}\varphi_{ba}\beta_{a1} = \sum_{b=1}^{t} \alpha_{lb}\varphi_{b1}\,\mathrm{id} = -\varphi_{l1}\varphi_{11}^{-1}\varphi_{11} + \mathrm{id}\,\varphi_{l1} = 0.$$

□

In Erdmann/Holm finden Sie in Kapitel 7.3 einen recht ähnlichen Beweis, ohne dass dort die Matrixschreibweise benutzt wird. Vielleicht lohnt sich der Vergleich. Wir merken an, dass der Satz von Krull-Remak-Schmidt 6.26 falsch ist, wenn Moduln unendlicher Dimension betrachtet werden:

Beispiel 6.27. Sei $A = \bigtimes_{\mathbb{N}} \mathbb{R}$ das direkte Produkt von abzählbar vielen Kopien der $\mathbb{R}$-Algebra $\mathbb{R}$. Dann ist A mit komponentenweiser Addition und Skalarmultiplikation eine $\mathbb{R}$-Algebra mit Einselement $(1, 1, \ldots)$. Wir zeigen, dass der reguläre Modul ${}_AA$ keine Zerlegung als direkte Summe unzerlegbarer Moduln besitzt:

Es ist $S(i) := \{(0, \ldots, 0, r, 0, \ldots) \mid r \in \mathbb{R}\} \leq {}_AA$ ein eindimensionaler und damit einfacher und unzerlegbarer A-Modul. Sei $U \leq {}_AA$ ein unzerlegbarer Untermodul. Sei $e_i = (0, \ldots, 0, 1, 0, \ldots) \in A$, wobei der Eintrag 1 in der $i$ten Koordinate steht. Es ist $e_i^2 = e_i$ ein Idempotent in der Algebra A. Da A kommutativ ist, ist $U_i := e_iU = Ue_i$ ein Untermodul von U. Genauso gilt $(1 - e_i)U = U(1 - e_i)$ ist Untermodul von U mit $U = e_iU \oplus (1 - e_i)U$. Existiert in U ein Element, das in der $i$ten Koordinate einen Eintrag ungleich Null hat, so ist $0 \neq Ue_i \leq Ae_i \simeq \mathbb{R}$, und es folgt, dass $Ue_i = Ae_i = S(i)$ ist. Da der Modul U unzerlegbar ist und Ue_i als direkten Summanden hat, ist also $U(1 - e_i) = 0$ und $U = S(i)$. Unzerlegbare Teilmoduln von ${}_AA$ sind also nicht nur isomorph zu $S(i)$, sondern physisch genau die Moduln $S(i)$, mit $i \in \mathbb{N}$, und jeder dieser Moduln kommt genau einmal vor.

Angenommen A ist eine Summe unzerlegbarer Teilmoduln. Dann muss also gelten ${}_AA = \bigoplus_{i\in\mathbb{N}} S(i)$. Dies ist ein Widerspruch: Nach der Definition von direkten Summen sind Elemente in $\bigoplus_{i\in\mathbb{N}}$ Folgen von reellen Zahlen, in denen nur endlich viele Einträge ungleich Null sind. Es ist also $1_A = (1, 1, \dots) \in {}_AA$, aber $1_A \notin \bigoplus_{i\in\mathbb{N}} S(i)$. Damit lässt sich ${}_AA$ nicht als direkte Summe unzerlegbarer Moduln schreiben.

Bemerkung 6.28. Wie häufig in der Mathematik üblich, gibt es verschiedene Wege zum Ziel. Wir haben sowohl aus Zeitgründen als auch, weil wir oft dem Buch von Erdmann/Holm folgen, den Beweis von Theorem 6.26 mit Hilfe von lokalen Algebren geführt. Ein anderer Beweis der Eindeutigkeitsaussage in Theorem 6.26 zeigt, dass die folgenden Zerlegungen jeweils in Bijektion zueinander stehen:

$$\begin{aligned}
&\text{Zerlegungen des Moduls } M \\
\overset{6.14}{\longleftrightarrow}\ &\text{Zerlegungen von } 1 = \mathrm{id}_M \in E := \mathrm{End}_A(M) \\
\overset{6.14}{\longleftrightarrow}\ &\text{Zerlegungen des regulären Moduls } {}_EE \\
\longleftrightarrow\ &\text{Zerlegungen des regulären Moduls } {}_{\bar{E}}\bar{E} \text{ mit } \bar{E} = E/\operatorname{rad} E.
\end{aligned}$$

Hierbei bedeutet Zerlegung eines Moduls immer Zerlegung in eine direkte Summe von unzerlegbaren Moduln. Und Zerlegung eines Einselementes bedeutet Zerlegung der Eins als Summe von primitiven, paarweise orthogonalen Idempotenten. Mit Theorem 6.14 haben wir also die ersten beiden Schritte in dieser Beweisskizze gezeigt. Überraschend in diesem Beweiszugang ist die dritte dieser drei Bijektionen. Angenommen diese gilt. Die Algebra $\bar{E}$ ist halbeinfach nach Korollar 4.30. Die Zerlegung von $\bar{E}$ in dieser Korrespondenz ist eindeutig, bis auf Isomorphie und Reihenfolge der Summanden nach Bemerkung 4.18. Damit folgt dann mittels der drei Bijektionen eine analoge Eindeutigkeitsaussage für die Zerlegung von M als direkte Summe unzerlegbarer Moduln.

Aufgabe 6.11. Sei A eine Algebra und seien $1_A = \sum_{i=1}^n e_i$ und $1_A = \sum_{j=1}^m f_j$ Zerlegungen von 1_A als Summe primitiver, paarweise orthogonaler Idempotente. Dann ist $n = m$ und es existiert ein invertierbares Element $a \in A$, so dass nach Umsortierung der Summanden gilt: $f_i = a^{-1}e_ia$, für $1 \le i \le n$.

E N D E