KAPITEL 3

Moduln über Ringen

1. Ringe

Wir wiederholen die Definition aus der Algebra-Vorlesung:

DEFINITION. *Ein* **Ring** R *ist eine Menge mit zwei Verknüpfungen* $+$ *und* $\cdot$*, die* **Addition** *und* **Multiplikation** *genannt werden, wobei folgende Eigenschaften erfüllt sind:*

(1) $(R,+)$ *ist eine abelsche Gruppe. Explizit:*
   (a) *Es gilt das Assoziativgesetz:* $a+(b+c)=(a+b)+c$ *für alle* $a,b,c\in R$.
   (b) *Es gibt ein neutrales Element* 0 *(Null):* $a+0=0+a=a$ *für alle* $a\in R$.
   (c) *Zu jedem* $a\in R$ *gibt es ein inverses Element* $-a$*:* $a+(-a)=(-a)+a=0$.
   (d) *Es gilt das Kommutativgesetz:* $a+b=b+a$ *für alle* $a,b\in R$.

(2) $(R,\cdot)$ *ist ein Monoid. (Statt* $a\cdot b$ *wird oft einfach* ab *geschrieben.) Explizit:*
   (a) *Es gilt das Assoziativgesetz:* $a(bc)=(ab)c$ *für alle* $a,b,c\in R$.
   (b) *Es gibt ein neutrales Element* 1 *(Eins):* $a\cdot 1=1\cdot a=a$ *für alle* $a\in R$.
   (c) *Eine* **Einheit** a *von* R *ist ein bzgl.* $\cdot$ *invertierbares Element. Das zu* a *inverse Element wird als* a^{-1} *geschrieben:* $a\cdot a^{-1}=a^{-1}\cdot a=1$.
   (d) *Die Einheiten von* R *bilden bzgl. der Multiplikation eine Gruppe, die als* **Einheitengruppe** *bezeichnet und als* R^* *geschrieben wird:* $R^*=\{a\in R: \text{es gibt ein } b\in R \text{ mit } ab=ba=1\}$.
   (e) *Ist die Multiplikation kommutativ, d.h.* $ab=ba$ *für alle* $a,b\in R$*, so spricht man von einem* **kommutativen Ring**.

(3) *Es gelten die Distributivgesetze:*

$$a(b+c)=ab+ac \quad \text{und} \quad (a+b)c=ac+bc \quad \text{für alle } a,b,c\in R.$$

Dabei wird die Konvention „Punkt vor Strich“ verwendet.

Ist G eine (multiplikativ geschriebene) Gruppe und k ein kommutativer Ring, so kann man die formalen (endlichen) Linearkombinationen der Gruppenelemente mit Koeffizienten aus k betrachten:

$$\sum_{g\in G} a_g g \quad \text{mit} \quad a_g\in k \text{ und } |\{g\in G: a_g\neq 0\}|<\infty.$$

Ähnlich wie bei Polynomen kann man eine Ringstruktur einführen:

DEFINITION. *Ist* k *ein kommutativer Ring und* G *eine (multiplikativ geschriebene) Gruppe, so ist der* **Gruppenring** *(oder die* **Gruppenalgebra***)* $k[G]$ *von* G *mit Koeffizienten in* k *die Menge der formalen (endlichen) Linearkombinationen der Gruppenelemente mit Koeffizienten aus* k*, also*

$$k[G]=\{\sum_{g\in G} a_g g : a_g\in k, |\{g: a_g\neq 0\}|<\infty\}.$$

Dabei gilt:

$$\sum_{g\in G} a_g g=\sum_{g\in G} b_g g \quad \Longleftrightarrow \quad a_g=b_g \text{ für alle } g\in G.$$

Durch

$$\left(\sum_{g\in G} a_g g\right)+\left(\sum_{g\in G} b_g g\right)=\sum_{g\in G}(a_g+b_g)g$$

wird eine Addition, durch

$$\left(\sum_{g\in G} a_g g\right)\cdot\left(\sum_{g\in G} b_g g\right)=\sum_{g\in G}\left(\sum_{\substack{g_1,g_2\in G\\ g_1g_2=g}} a_{g_1}b_{g_2}\right)g=\sum_{g\in G}\left(\sum_{h\in G} a_h b_{h^{-1}g}\right)g$$

eine Multiplikation auf $k[G]$ definiert.

LEMMA. *Ist k ein kommutativer Ring und G eine multiplikativ geschriebene Gruppe mit Einselement 1_G, so ist der Gruppenring $k[G]$ mit den angegebenen Eigenschaften ein Ring und es gilt:*

(1) *Das Nullelement ist $\sum_{g\in G} 0\cdot g$, wofür man auch 0 schreibt.*
(2) *Das Einselement ist $1\cdot 1_G+\sum_{g\in G\setminus\{1_G\}} 0\cdot g$, wofür man auch 1 schreibt.*

Bemerkungen:

(1) Ist die Schreibweise $\sum_{g\in G} a_g g$ missverständlich, so kann man beispielsweise auch $\sum_{g\in G} a_g[g]$ schreiben.
(2) Etwas abstrakter kann man den Gruppenring $k[G]$ auch so einführen: Man betrachtet die Menge von Abbildungen

$$K=\{\alpha: G\to k : |\{g\in G:\alpha(g)\neq 0\}|<\infty\}.$$

Man definiert Addition und Multiplikation wie folgt:

$$(\alpha+\beta)(g)=\alpha(g)+\beta(g)\quad\text{und}\quad(\alpha\beta)(g)=\sum_{\substack{g_1,g_2\in G\\ g_1g_2=g}}\alpha(g_1)\beta(g_2).$$

Das Nullelement ist die Abbildung $g\mapsto 0$, das Einselement ist die Abbildung $\varepsilon\in K$ mit

$$\varepsilon(g)=\begin{cases}1 & \text{für } g=1_G,\\ 0 & \text{sonst.}\end{cases}$$

Natürlich muss man nachrechnen, dass K auf diese Weise ein Ring wird. Ordnet man dann einem $\alpha\in K$ die formale Summe

$$\sum_{g\in G}\alpha(g)g$$

zu, so erhält man die ursprüngliche Darstellung.

Beispiele:

(1) Sei $G=\{1,g\}$ eine Gruppe der Ordnung 2, sodass insbesondere $g^2=1$ gilt. Dann ist

$$k[G]=\{a+bg : a,b\in k\}.$$

Es ist

$$(a+bg)(c+dg)=(ac+bd)+(ad+bc)g.$$

(2) Ist $G=S_3$, so betrachten wir

$$\Big(2(12)-3(132)\Big)\cdot\Big(3(1)-(13)+(123)\Big)=-3+9(12)+2(23)-11(132).$$

(3) Hat man eine additiv geschriebene Gruppe, so sollte man eine Schreibweise wie $\sum_{g\in G} a_g[g]$ benutzen. Dann gilt $[g]\cdot[h]=[g+h]$ in $k[G]$.

Wir erinnern an einen weiteren Begriff aus der Algebra:

DEFINITION. *Ist R ein Ring, so nennt man einen Teilmenge $S\subseteq R$ einen* **Unterring** *von R, falls S mit der Addition und der Multiplikation von R einen Ring bildet und die Eins von R in S enthalten ist.*

Bemerkungen:

(1) Eine Teilmenge S eines Rings R ist genau dann ein Unterring, wenn folgende Bedingungen erfüllt sind:
   - $0 \in S$,
   - $x, y \in S \Longrightarrow x + y \in S$,
   - $x \in S \Longrightarrow -x \in S$,
   - $1 \in S$,
   - $x, y \in S \Longrightarrow xy \in S$.

(2) Bei der Definition eines Unterrings S von R fordern wir, dass die Eins von R auch die Eins von S ist. Es kann Teilmengen von R geben, die Ringe sind, aber keine Unterringe. Beispielsweise enthält $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ die Teilmenge $\{0, 2, 4\}$, die wegen $2 \cdot 2 = 4$, $2 \cdot 4 = 2$, $4 \cdot 4 = 4$ einen Ring bildet mit Einselement 4.

DEFINITION. *Ist R ein Ring, so heißt*

$$Z(R) = \{a \in R : ab = ba \text{ für alle } b \in R\}$$

das **Zentrum** *von R. (Es besteht aus den Elementen, die mit allen anderen vertauschbar sind.)*

Bemerkung: $Z(R)$ ist ein kommutativer Unterring von R. Immer gilt $0, 1 \in Z(R)$.

Das Zentrum des Gruppenrings einer endlichen Gruppe können wir gut beschreiben:

SATZ. *Ist G eine (multiplikativ geschriebene) endliche Gruppe, ist $g_1, \ldots, g_h \in G$ ein Repräsentantensystem der Konjugationsklassen, definiert man für $i = 1, \ldots, h$*

$$c_i = \sum_{g \in c(g_i)} g \in k[G],$$

so gilt

$$Z(k[G]) = \{a_1 c_1 + \cdots + a_h c_h : a_1, \ldots, a_h \in k\}.$$

Definiert man

$$\ell_{ijk} = |\{(a, b) \in c(g_i) \times c(g_j) : ab = g_k\}|,$$

so gilt

$$c_i c_j = \sum_{k=1}^{h} \ell_{ijk} c_k.$$

Beweis: Sei $z = \sum_{g \in G} a_g g$ ein beliebiges Element aus $k[G]$. Wir wollen untersuchen, wann es im Zentrum liegt. Für $h \in G$ (Achtung! Hier ist h ein Gruppenelement, nicht die Anzahl der Konjugationsklassen.) haben wir

$$\begin{aligned} hz &= \sum_{g \in G} a_g hg = \sum_{g \in G} a_{h^{-1}g} h(h^{-1}g) = \sum_{g \in G} a_{h^{-1}g} g, \\ zh &= \sum_{g \in G} a_g gh = \sum_{g \in G} a_{gh^{-1}} (gh^{-1})h = \sum_{g \in G} a_{gh^{-1}} g. \end{aligned}$$

Daher gilt:

$$\begin{aligned} z \in Z(k[G]) &\iff hz = zh \text{ für alle } h \iff \\ &\iff a_{h^{-1}g} = a_{gh^{-1}} \text{ für alle } g, h \in G \iff \\ &\iff a_{h^{-1}hg} = a_{hgh^{-1}} \text{ für alle } g, h \in G \iff \\ &\iff a_{hgh^{-1}} = a_g \text{ für alle } g, h \in G \iff \\ &\iff a_g = a_{g_i} \text{ für alle } g \in c(g_i) \text{ und alle } i. \end{aligned}$$

Damit schreiben sich die Elemente des Zentrums in der Form

$$z = \sum_{g \in G} a_g g = \sum_{i=1}^{h} \sum_{g \in c(g_i)} a_g g = \sum_{i=1}^{h} \sum_{g \in c(g_i)} a_{g_i} g = \sum_{i=1}^{h} a_{g_i} \sum_{g \in c(g_i)} g = \sum_{i=1}^{h} a_{g_i} c_i.$$

Damit ist die Behauptung bewiesen.
Die Darstellung $c_i c_j = \sum_{k=1}^{h} \ell_{ijk} c_k$ beweist man genauso wie bei den Darstellungen. ■

Beispiel: In S_3 wählen wir $g_1 = (1)$, $g_2 = (12)$, $g_3 = (123)$ und erhalten dann

$$c_1 = (1), \quad c_2 = (12) + (13) + (23), \quad c_3 = (123) + (132).$$

Dann gilt

$$Z(k[S_3]) = k + k\,c_2 + k\,c_3.$$

Man findet die Beziehungen

$$c_2^2 = 3 + 3c_3, \quad c_2 c_3 = 2c_2, \quad c_3^2 = 2 + c_3.$$

Wir erinnern an die Definition eines Ringhomomorphismus:

DEFINITION. *Ein* **Ringhomomorphismus** *zwischen zwei Ringen R und S ist eine Abbildung $\phi : R \to S$, sodass für alle $x, y \in R$ gilt*

$$\phi(x + y) = \phi(x) + \phi(y), \quad \phi(xy) = \phi(x)\phi(y), \quad \phi(1) = 1.$$

Ein **Ringisomorphismus** *ist ein bijektiver Ringhomomorphismus.*

Ist k ein Körper, so ist der Gruppenring $k[G]$ offensichtlich auch ein k-Vektorraum. Diese Art von Struktur kommt häufiger vor und hat einen eigenen Namen:

DEFINITION. *Sei k ein kommutativer Ring, R ein Ring und*

$$\varepsilon_R : k \to Z(R)$$

ein Ringhomomorphismus. Dann nennt man R eine **k-Algebra**.

Bemerkungen:

(1) Es gibt auch noch andere Arten von k-Algebren, bei denen beispielsweise auf das Assoziativgesetz oder die Existenz eines Einselements verzichtet wird.
(2) Jeder Ring R lässt sich als $\mathbb{Z}$-Algebra auffassen mit $\varepsilon_R(1) = 1_R$.
(3) Ist $\lambda \in k$ und $r \in R$, so schreibt man gewöhnlich λr für $\varepsilon_R(\lambda) r$.
(4) Die Matrizenringe $\mathrm{M}_n(k)$ sind k-Algebren.
(5) Gruppenringe $k[G]$ sind k-Algebren.

Wir werden im Folgenden die k-Algebra-Struktur von Gruppenringen nicht besonders betonen.

Bemerkung: Ist k ein Körper und V ein Vektorraum, so ist

$$\mathrm{End}_k(V) = \{\alpha : V \to V \ k\text{-linear}\}$$

eine k-Algebra. Ist $e_1, \ldots, e_n$ eine Basis von V, so gibt es zu $\alpha \in \mathrm{End}_k(V)$ Zahlen $a_{ij} \in k$ mit

$$\alpha(e_j) = \sum_{i=1}^{n} a_{ij} e_i.$$

Durch

$$\mathrm{End}_k(V) \to \mathrm{M}_n(k), \quad \alpha \mapsto (a_{ij})$$

wird ein Ringisomorphismus definiert, der auch ein k-Algebra-Isomorphismus ist.

LEMMA. *Sei G eine Gruppe, k ein Körper und $\rho : G \to \mathrm{GL}(V)$ eine Darstellung von G auf dem k-Vektorraum V.*

(1) *Dann wird durch*

$$\widetilde{\rho} : k[G] \to \mathrm{End}_k(V), \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g \rho(g)$$

ein Ringhomomorphismus definiert, der auch k-linear ist.

(2) *Ist $e_1, \dots, e_n$ eine k-Basis von V, ist $A(g)$ die $\rho(g)$ beschreibende Matrix bezüglich der Basis $e_1, \dots, e_n$, so ist*

$$k[G] \mapsto \mathrm{M}_n(k), \quad \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g A(g)$$

ein Ringhomomorphismus, der auch k-linear ist.

Beweis: Den ersten Teil rechnet man einfach nach:

$$\begin{aligned}
\widetilde{\rho}(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g) &= \sum_{g\in G}(a_g+b_g)\rho(g) = \sum_{g\in G} a_g\rho(g) + \sum_{g\in G} b_g\rho(g) = \\
&= \widetilde{\rho}(\sum_{g\in G} a_g g) + \widetilde{\rho}(\sum_{g\in G} b_g g), \\
\widetilde{\rho}(\sum_{g\in G} a_g g \cdot \sum_{g\in G} b_g g) &= \widetilde{\rho}(\sum_{g\in G}(\sum_{\substack{g_1,g_2\in G\\ g_1g_2=g}} a_{g_1}b_{g_2})g) = \sum_{g\in G}(\sum_{\substack{g_1,g_2\in G\\ g_1g_2=g}} a_{g_1}b_{g_2})\rho(g) = \\
&= \sum_{g\in G} a_g\rho(g) \circ \sum_{g\in G} b_g\rho(g) = \widetilde{\rho}(\sum_{g\in G} a_g g) \circ \widetilde{\rho}(\sum_{g\in G} b_g g), \\
\widetilde{\rho}(1_{k[G]}) &= \widetilde{\rho}(1_G) = \rho(1_G) = \mathrm{id}_V, \\
\widetilde{\rho}(\lambda \sum_{g\in G} a_g g) &= \widetilde{\rho}(\sum_{g\in G} \lambda a_g g) = \sum_{g\in G} \lambda a_g\rho(g) = \lambda\widetilde{\rho}(\sum_{g\in G} a_g g).
\end{aligned}$$

Der zweite Teil folgt sofort aus dem ersten Teil. ■

Beispiel: In Aufgabe 12 wurden die beschreibenden Matrizen einer 2-dimensionalen Darstellung von S_3 bestimmt:

$$A((1)) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A((12)) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad A((13)) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \quad A((23)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$A((123)) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad A((132)) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Dann ist $\widetilde{\rho} : k[S_3] \to \mathrm{M}_2(k)$ mit

$$\widetilde{\rho}(a_1(1) + a_2(12) + a_3(13) + a_4(23) + a_5(123) + a_6(132)) = \begin{pmatrix} a_1 - a_2 + a_3 - a_5 & -a_2 + a_4 - a_5 + a_6 \\ -a_3 + a_4 + a_5 - a_6 & a_1 + a_2 - a_3 - a_6 \end{pmatrix}$$

ein Ringhomomorphismus.

Gruppenringe lassen sich häufig in ein Produkt von Ringen zerlegen.

LEMMA. *Sind $R_1, \dots, R_n$ Ringe, so wird das* **Produkt der Ringe** *$R_1, \dots, R_n$ definiert durch*

$$\prod_{i=1}^{n} R_i = R_1 \times \cdots \times R_n = \{(a_1, \dots, a_n) : a_i \in R_i\}$$

mit Addition

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n)$$

und Multiplikation

$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1b_1, \dots, a_nb_n).$$

Dadurch wird $R_1 \times \cdots \times R_n$ zu einem Ring mit Nullelement $(0, \dots, 0)$ und Einselement $(1, \dots, 1)$. Die Abbildungen

$$\pi_i : R_1 \times \cdots \times R_n \to R_i, \quad (a_1, \dots, a_n) \mapsto a_i$$

sind Ringhomomorphismen. Definiert man $e_i \in R_1 \times \cdots \times R_n$ durch $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ - an Position i soll $1 \in R_i$ stehen -, so gilt

$$e_i^2 = e_i, \quad e_ie_j = 0 \text{ für } i \neq j, \quad e_1 + \cdots + e_n = 1 \quad \text{und} \quad e_i \in Z(R_1 \times \cdots \times R_n).$$

DEFINITION. *Sei R ein Ring.*

(1) *$e \in R$ heißt* **idempotent**, *wenn $e^2 = e$ gilt.*
(2) *$e \in R$ heißt* **zentral idempotent**, *wenn $e^2 = e$ und $e \in Z(R)$ gilt.*
(3) *Idempotente Elemente $e_1, e_2 \in R$ heißen* **orthogonal**, *wenn gilt $e_1 e_2 = e_2 e_1 = 0$.*

Beispiele:

(1) In jedem Ring sind 0 und 1 zentral idempotent.
(2) Ist e idempotent, so auch $1 - e$ wegen

$$(1-e)^2 = (1-e)(1-e) = 1 - e - e + e^2 = 1 - e.$$

Außerdem sind e und $1 - e$ orthogonal:

$$e(1-e) = e - e^2 = 0 = e(1-e).$$

SATZ. *Für einen Ring R sind äquivalent:*

(1) *R ist isomorph zu einem Produkt $R_1 \times \cdots \times R_n$ von n Ringen.*
(2) *Es gibt paarweise orthogonale zentrale idempotente Elemente $e_1, \ldots, e_n \in R$ mit $1 = e_1 + \cdots + e_n$.*

Beweis:

- (1) $\Longrightarrow$ (2) Dies steht bereits im letzten Lemma.
- (2) $\Longrightarrow$ (1) Wir definieren

$$R_i = Re_i = \{ae_i : a \in R\} \text{ für } i = 1, \ldots, n$$

und

$$\phi : R_1 \times \cdots \times R_n \to R \text{ mit } (r_1, \ldots, r_n) \mapsto r_1 + \cdots + r_n.$$

  – *Behauptung:* $R_i \subseteq R$ ist ein Ring mit Eins e_i.
  Beweis: Die Abgeschlossenheit unter Multiplikation folgt unter Ausnutzung von $e_i \in Z(R)$ und $e_i^2 = e_i$ aus

$$(ae_i)(be_i) = ae_i be_i = abe_i^2 = abe_i.$$

  Dass e_i das Einselement in R_i ist, ersieht man aus

$$(ae_i) \cdot e_i = ae_i^2 = ae_i \quad \text{und} \quad e_i \cdot (ae_i) = e_i ae_i = ae_i^2 = ae_i.$$

  – *Behauptung:* ϕ ist ein Ringhomomorphismus.
  Beweis: Da für $r_i \in R_i$ die Gleichung $r_i e_i = r_i$ gilt, erhalten wir

$$\begin{aligned}
\phi((r_1, \ldots, r_n) + (s_1, \ldots, s_n)) &= \phi((r_1 + s_1, \ldots, r_n + s_n)) = \sum_{i=1}^{n} (r_i + s_i) = \\
&= \phi((r_1, \ldots, r_n)) + \phi((s_1, \ldots, s_n)), \\
\phi((r_1, \ldots, r_n) \cdot (s_1, \ldots, s_n)) &= \phi((r_1 s_1 + \cdots + r_n s_n)) = \sum_{i=1}^{n} r_i s_i = \\
&= \sum_{i=1}^{n} r_i e_i s_i e_i = \sum_{i=1}^{n} \sum_{j=1}^{n} r_i e_i s_j e_j = \\
&= \left(\sum_{i=1}^{n} r_i e_i \right) \left(\sum_{j=1}^{n} s_j e_j \right) = \\
&= \phi((r_1, \ldots, r_n)) \cdot \phi((s_1, \ldots, s_n)), \\
\phi((1_{R_1}, \ldots, 1_{R_n})) &= \phi((e_1, \ldots, e_n)) = e_1 + \cdots + e_n = 1.
\end{aligned}$$

– *Behauptung:* ϕ ist injektiv.
Beweis: Sei $(r_1, \dots, r_n) \in \mathrm{Kern}(\phi)$, d.h. $r_1 + \cdots + r_n = 0$. Dann gilt für $1 \le i \le n$

$$\begin{aligned} 0 &= 0e_i = (r_1 + \cdots + r_i + \cdots + r_n)e_i = (r_1e_1 + \cdots + r_ie_i + \cdots + r_ne_n)e_i = \\ &= r_ie_i^2 = r_i, \end{aligned}$$

also $r_i = 0$, und damit $(r_1, \dots, r_n) = (0, \dots, 0)$, was die Injektivität von ϕ beweist.
– *Behauptung:* ϕ ist surjektiv.
Dies folgt sofort aus

$$r = r(e_1 + \cdots + e_n) = re_1 + \cdots + re_n.$$

Damit ist ϕ ein Ringisomorphismus, was wir zeigen wollten. ■

Beispiel: Wir betrachten $R = \mathbb{Z}_{12} = \{0, 1, \dots, 11\}$ mit Addition und Multiplikation modulo 12. Durch Ausprobieren findet man die idempotenten Elemente:

$$0, \quad 1, \quad 4, \quad 9.$$

Wir betrachten $e = 4$ mit $1 - e = 9$. Es ist

$$R_1 = Re = \{0, 4, 8\} \quad \text{und} \quad R_2 = \{0, 3, 6, 9\}.$$

Man sieht, dass sich jedes $a \in R$ eindeutig als $a = a_1 + a_2$ mit $a_1 \in R_1$, $a_2 \in R_2$ schreiben lässt:

$a_1 + a_2$	a_1	a_2
0	0	0
1	4	9
2	8	6
3	0	3
4	4	0
5	8	9
6	0	6
7	4	3
8	8	0
9	0	9
10	4	6
11	8	3

Man überprüft auch, dass R_1 ein Ring mit Einselement 4 und R_2 ein Ring mit Einselement 9 ist.

Das Vorgehen beim letzten Beispiel funktioniert auch allgemein für endliche Ringe:

SATZ. *Sei R ein endlicher Ring der Ordnung $N = p_1^{m_1} \dots p_n^{m_n}$ (mit $n \ge 1$ paarweise verschiedenen Primzahlen $p_1, \dots, p_n$ und $m_1, \dots, m_n \in \mathbb{N}$).*

(1) *Es ist $N \cdot r = \underbrace{r + \cdots + r}_{N \text{ Summanden}} = 0$ für alle $r \in R$.*
(2) *Es gibt Zahlen $\widetilde{e}_1, \dots, \widetilde{e}_n \in \mathbb{Z}$ mit*

$$\widetilde{e}_i \equiv \begin{cases} 1 \bmod p_i^{m_i} \\ 0 \bmod p_j^{m_j} \quad \text{für } j \ne i. \end{cases}$$

Durch diese Bedingungen ist $\widetilde{e}_i$ eindeutig bestimmt modulo N.
(3) *Sei $e_i = \widetilde{e}_i \cdot 1_R$ (das Bild von $\widetilde{e}_i$ in R). e_i ist unabhängig von der Wahl von $\widetilde{e}_i$. Es gilt:*

$$e_i \in Z(R), \quad e_i^2 = e_i, \quad e_ie_j = 0 \text{ für } i \ne j, \quad e_1 + \cdots + e_n = 1.$$

($e_1, \dots, e_n$ sind also paarweise orthogonale zentrale idempotente Elemente von R, die sich zu 1 aufaddieren.)
(4) *Sei $R_i = Re_i = \{ae_i : a \in R\}$. Mit der Addition und Multiplikation von R wird R_i zu einem Ring mit Einselement e_i. Es gilt*

$$|R_i| = p_i^{m_i}.$$

(5)
$$\phi : R_1 \times \cdots \times R_n \to R, \quad (r_1, \ldots, r_n) \mapsto r_1 + \cdots + r_n$$
ist ein Ringisomorphismus.

Beweis:

(1) Die additive Gruppe $(R, +)$ hat Ordnung N, also gilt $N \cdot r = 0$ für alle $r \in R$.
(2) Dies liefert der chinesische Restsatz.
(3)
- Die $\widetilde{e}_i$ kann man um Vielfache von N abändern. Wegen $N \cdot r = 0$ für $r \in R$ erhält man trotzdem die gleichen Elemente $e_1, \ldots, e_n$.
- $Z(R)$ ist ein Unterring von R. Wegen $r_1 \in Z(R)$ und $e_i = \pm(\underbrace{1_R + \cdots + 1_R}_{|\widetilde{e}_i| \text{ Summanden}})$ gilt auch $e_i \in Z(R)$.
- Man sieht aus den Kongruenzen, dass gilt
$$\widetilde{e}_i^2 \equiv \widetilde{e}_i \bmod N, \quad \widetilde{e}_i\widetilde{e}_j \equiv 0 \bmod N \text{ für } i \neq j, \quad \widetilde{e}_1 + \cdots + \widetilde{e}_n \equiv 1 \bmod N.$$
Daraus ergeben sich dann sofort die für $e_1, \ldots, e_n$ behaupteten Eigenschaften.

(4) Dass R_i ein Ring mit Einselement e_i haben wir bereits im Allgemeinfall gesehen. Nun gilt aber $p_i^{m_i}\widetilde{e}_i \equiv 0 \bmod N$, woraus
$$p_i^{m_i} \cdot e_i = 0, \quad \text{und damit } p_i^{m_i} \cdot R_i = \{0\}$$
folgt. Daher ist die Ordnung der abelschen Gruppe $(R_i, +)$ eine p_i-Potenz. Wegen
$$p_1^{m_1} \ldots p_n^{m_n} = N = |R| = |R_1| \ldots |R_n|$$
bleibt dann nur die Möglichkeit
$$|R_i| = p_i^{m_i},$$
wie behauptet.
(5) Dies haben wir bereits allgemein gezeigt. ■

Der folgende Satz zeigt, wie man den Gruppenring $k[G]$ einer endlichen Gruppe zumindest in Charakteristik 0 und über einem algebraisch abgeschlossenen Körper in ein Produkt zerlegen kann.

Satz. *Sei G eine endliche Gruppe mit h Konjugationsklassen. Sei k ein algebraisch abgeschlossener Körper der Charakteristik 0. Seien $\chi_1, \ldots, \chi_h : G \to k$ die irreduziblen Charaktere von G und $\rho_i : G \to \mathrm{GL}(V_i)$ zu gehörige Darstellungen mit $n_i = \dim(V_i) = \chi_i(1)$. Dann ist*
$$\phi : k[G] \to \prod_{i=1}^{h} \mathrm{End}_k(V_i), \quad \sum_{g \in G} a_g g \mapsto \left(\sum_{g \in G} a_g \rho_i(g) \right)_{1 \leq i \leq h}$$
ein Ringisomorphismus, der auch k-linear ist. Wählt man Basen in den Vektorräumen V_i, so erhält man einen Isomorphismus
$$k[G] \xrightarrow{\simeq} \prod_{i=1}^{h} \mathrm{M}_{n_i}(k).$$
Die zugehörigen zentralen Idempotenten sind
$$e_i = \frac{n_i}{|G|} \sum_{g \in G} \chi_i(g^{-1}) g.$$

Beweis:

(1) Es ist (nach einem früheren Lemma) klar, dass
$$\phi : k[G] \to \prod_{i=1}^{h} \mathrm{End}_k(V_i), \quad \sum_{g \in G} a_k g \mapsto \Big(\sum_{g \in G} a_g \rho_i(g) \Big)_{1 \leq i \leq h}$$
ein Ringhomomorphismus ist, der auch k-linear ist.

(2) Was ist der Kern von ϕ? Sei $\sum_{g\in G} a_g g \in \mathrm{Kern}(\phi)$. Dann gilt

$$\sum_{g\in G} a_g \rho_i(g) = 0 \text{ für } i = 1, \ldots, h.$$

Da sich jede Darstellung $\rho : G \to \mathrm{GL}(V)$ als direkte Summe der Darstellungen $\rho_1, \ldots, \rho_h$ schreiben lässt, folgt

$$\sum_{g\in G} a_g \rho(g) = 0.$$

Insbesondere gilt dies dann für die reguläre Darstellung:

$$\sum_{g\in G} a_g R_G(g) = 0.$$

Ist $V = \oplus_{g\in G} k e_g$ der zugehörige Vektorraum, so ist $R_G(g)(e_a) = e_{ga}$. Wendet man die Relation auf e_1 an, so folgt

$$\sum_{g\in G} a_g e_g = 0,$$

und damit $a_g = 0$ für alle $g \in G$. Daher ist ϕ injektiv.

(3) Wir wissen, dass mit $n_i = \chi_i(1) = \dim(V_i)$ gilt

$$|G| = n_1^2 + \cdots + n_h^2.$$

Nun ist

$$\dim k[G] = |G| \quad \text{und} \quad \dim \prod_{i=1}^{h} \mathrm{End}_k(V_i) = \sum_{i=1}^{h} n_i^2,$$

woraus

$$\dim k[G] = \dim \prod_{i=1}^{h} \mathrm{End}_k(V_i)$$

folgt. Da ϕ injektiv ist, ist ϕ auch surjektiv, also ein Isomorphismus.

(4) Was sind die idempotenten Elemente. Wir haben bei „Zerlegung in isotypische Komponenten“ so etwas gesehen. Wir versuchen

$$e_i = \frac{n_i}{|G|} \sum_{g\in G} \chi_i(g^{-1}) g \in k[G].$$

Wir betrachten

$$\rho_j(e_i) = \frac{n_i}{|G|} \sum_{g\in G} \chi_i(g^{-1}) \rho_j(g) \in \mathrm{End}(V_j).$$

Für $a \in G$ gilt

$$\begin{aligned}
\rho_j(a) \circ \rho_j(e_i) &= \frac{n_i}{|G|} \sum_{g\in G} \chi_i(g^{-1}) \rho_j(ag) = \frac{n_i}{|G|} \sum_{g\in G} \chi_i(g^{-1}) \rho_j(aga^{-1}) \circ \rho_j(a) = \\
&= \frac{n_i}{|G|} \sum_{g\in G} \chi_i((a^{-1}ga)^{-1}) \rho_j(a(a^{-1}ga)a^{-1}) \circ \rho_j(a) = \\
&= \frac{n_i}{|G|} \sum_{g\in G} \chi_i(a^{-1}g^{-1}a) \rho_j(g) \circ \rho_j(a) = \frac{n_i}{|G|} \sum_{g\in G} \chi_i(g^{-1}) \rho_j(g) \circ \rho_j(a) = \\
&= \rho_j(e_i) \circ \rho_j(a).
\end{aligned}$$

Nach dem Lemma von Schur gibt es ein $\lambda \in k$ mit

$$\rho_j(e_i) = \lambda \mathrm{id}_{V_j}.$$

Spurbildung liefert

$$\lambda n_j = \mathrm{sp}(\rho_j(e_i)) = \frac{n_i}{|G|} \sum_{g\in G} \chi_i(g^{-1}) \chi_j(g) = n_i \langle \chi_i, \chi_j \rangle,$$

also

$$\rho_j(e_i) = \langle \chi_i, \chi_j \rangle \mathrm{id}_{V_j}.$$

Also gilt

$$\rho_j(e_i) = \langle \chi_i \chi_j \rangle \mathrm{id}_{V_j},$$

also

$$\rho_j(e_i) = \begin{cases} \mathrm{id}_{V_j} & \text{für } i = j, \\ 0 & \text{für } i \neq j. \end{cases}$$

Dies beweist, dass $e_1, \ldots, e_h$ die zentralen idempotenten Elemente sind. ■

Beispiel: Wir betrachten S_3. Über einem algebraisch abgeschlossenen Körper der Charakteristik 0 kennen wir drei irreduzible Darstellungen:

- Die triviale Darstellung $\rho_{\text{trivial}} : S_3 \to k^*$ mit $\rho_{\text{trivial}}(\sigma) = 1$, sie führt zu
  $\widetilde{\rho_{\text{trivial}}}(a_1(1) + a_2(12) + a_3(13) + a_4(23) + a_5(123) + a_6(132)) = a_1 + a_2 + a_3 + a_4 + a_5 + a_6.$
- Die Darstellung $\rho_{\text{Signum}} : S_3 \to k^*$ mit $\rho_{\text{Signum}}(\sigma) = \mathrm{sgn}(\sigma)$, sie führt zu
  $\widetilde{\rho_{\text{Signum}}}(a_1(1) - a_2(12) - a_3(13) - a_4(23) + a_5(123) + a_6(132)) = a_1 + a_2 + a_3 + a_4 + a_5 + a_6.$
- Die zuvor erwähnte 2-dimensionale Darstellung, die zu
  $\widetilde{\rho_2}(a_1(1) + a_2(12) + a_3(13) + a_4(23) + a_5(123) + a_6(132)) = \begin{pmatrix} a_1 - a_2 + a_3 - a_5 & -a_2 + a_4 - a_5 + a_6 \\ -a_3 + a_4 + a_5 - a_6 & a_1 + a_2 - a_3 - a_6 \end{pmatrix}$
  führt.

Fassen wir alle drei Darstellungen zusammen, so erhalten wir

$$\phi : k[S_3] \to k \times k \times M_2(k)$$

mit

$$\begin{aligned} &\phi(a_1(1) + a_2(12) + a_3(13) + a_4(23) + a5(123) + a_6(132)) = \\ = \quad &\left(a_1 + a_2 + a_3 + a_4 + a_5 + a_6 \quad | \quad a_1 - a_2 - a_3 - a_4 + a_5 + a_6 \quad | \quad \begin{pmatrix} a_1 - a_2 + a_3 - a_5 & -a_2 + a_4 - a_5 + a_6 \\ -a_3 + a_4 + a_5 - a_6 & a_1 + a_2 - a_3 - a_6 \end{pmatrix} \right) \end{aligned}$$

Die idempotenten Elemente sind

$$e_{\text{trivial}} = \frac{1}{6}(c_1 + c_2 + c_3), \quad e_{\text{Signum}} = \frac{1}{6}(c_1 - c_2 + c_3), \quad e_2 = \frac{1}{3}(2c_1 - c_3)$$

mit $c_1 = (1)$, $c_2 = (12) + (13) + (23)$, $c_3 = (123) + (132)$. Tatsächlich findet man:

$$\phi(e_{\text{trivial}}) = \left(1 \quad | \quad 0 \quad | \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right), \quad \phi(e_{\text{Signum}}) = \left(0 \quad | \quad 1 \quad | \quad \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right), \quad \phi(e_2) = \left(0 \quad | \quad 0 \quad | \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right).$$

Bemerkung: Man kann nachrechnen, dass durch die angegebenen Formeln für jeden kommutativen Ring k ein Ringhomomorphismus

$$\phi : k[S_3] \to k \times k \times \mathrm{M}_2(k)$$

definiert wird. Ist k ein Körper, so kann man mit den Methoden der Linearen Algebra die Dimension des Bildes ausrechnen. Man findet:

- **Fall** $\mathrm{char}(k) = 2$**:** Dann gilt $\dim_k(\phi(k[S_3]) = 5$, insbesondere ist ϕ kein Isomorphismus.
- **Fall** $\mathrm{char}(k) = 3$**:** Dann gilt $\dim_k(\phi(k[S_3])) = 3$. Auch hier ist ϕ kein Isomorphismus.
- **Fall** $\mathrm{char}(k) \neq 2, 3$**:** Dann ist $\dim_k(\phi(k[S_3])) = 6$, ϕ ist ein Isomorphismus.

Beispiel: Wir betrachten den Gruppenring $R = \mathbb{F}_2[S_3]$, der 64 Elemente hat. Indem wir mit dem Rechner alle Elemente durchgehen, findet man als zentrale idempotente Elemente

$$0, \quad (1), \quad (123) + (132), \quad (1) + (123) + (132).$$

Wir wählen

$$e = (1) + (123) + (132).$$

Man findet:

$$Re = \{0, (1) + (123) + (132), (12) + (13) + (23), (1) + (12) + (13) + (23) + (123) + (132)\}.$$

Dies ist ein Ring mit 4 Elementen. Das Einselement ist $e = (1) + (123) + (132)$. Wir schreiben $a = (1) + (12) + (13) + (23) + (123) + (132)$. Dann ist

$$Re = \{0, e, a, a + e\}.$$

Man findet

$$a^2 = 0, \quad (e + a)^2 = e.$$

Der Ring Re ist isomorph zu $\mathbb{F}_2[x]/(x^2)$.

Im folgenden Satz werden Produkte von Ringen durch eine universelle Eigenschaft charakterisiert:

SATZ. *Seien $R_i, i \in I$ Ringe.*

(1) *Dann wird*

$$R = \prod_{i \in I} R_i = \{(a_i)_{i\in} : a_i \in R_i \text{ für } i \in I\}$$

durch komponentenweise Addition und Multiplikation zu einem Ring und

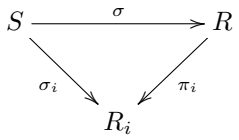
$$\pi_j : R \to R_i, \quad (a_i)_{i\in I} \mapsto a_j$$

sind Ringhomomorphismen.

(2) *Ist S ein Ring, sind $\sigma_i : S \to R_i$ Ringhomomorphismen, so gibt es genau einen Ringhomomorphismus $\sigma : S \to R$ mit*

$$\sigma_i = \pi_i \circ \sigma \text{ für alle } i \in I,$$

d.h. das Diagramm



ist kommutativ für alle $i \in I$.

Beweis: Teil (1) ist klar. Teil (2) ergibt sich aus der expliziten Konstruktion von $R = \prod_{i\in I} R_i$: Existiert ein σ wie angegeben und ist $\sigma(s) = (a_i)_{i\in I}$, so gilt

$$\sigma_j(s) = \pi_j(\sigma(s)) = \pi_j((a_i)_{i\in I}) = a_j,$$

und damit

$$\sigma_j(s) = (\sigma_i(s))_{i\in I}.$$

Nun muss man nur noch zeigen, dass durch diese Vorschrift ein Ringhomomorphismus definiert wird, was aber klar ist. ■

2. R-Moduln

DEFINITION. *Sei R ein Ring und M eine Menge mit zwei Abbildungen*

$$+ : M \times M \to M \quad \text{und} \quad \cdot : R \times M \to M,$$

sodass folgende Eigenschaften erfüllt sind:

(1) *$(M, +)$ ist eine abelsche Gruppe.*
(2) *Für $a, b \in R$ und $x, y \in M$ gilt:*
   (a) $1x = x$
   (b) $(a + b)x = ax + bx$
   (c) $a(x + y) = ax + ay$
   (d) $a(bx) = (ab)x$

*Dann heißt M ein R-**Modul**, genauer ein R-**Linksmodul**.*

Bemerkungen:

(1) Analog zu Linksmoduln kann man auch Rechtsmoduln betrachten. Wir werden uns aber auf Linksmoduln beschränken und sie einfach als Moduln bezeichnen.

(2) Man zeigt sofort: $0x = 0$ und $a(-x) = -(ax)$ für $a \in R$ und $x \in M$.
(3) Da ein R-Modul M eine additive Gruppe ist, hat man wie üblich die Multiplikation mit ganzen Zahlen:

$$n \cdot x = \begin{cases} \underbrace{x + \cdots + x}_{n \text{ Summanden}} & \text{für } n \in \mathbb{Z} \text{ mit } n \geq 1, \\ 0 & \text{für } n = 0, \\ \underbrace{(-x) + \cdots + (-x)}_{|n| \text{ Summanden}} & \text{für } n \in \mathbb{Z} \text{ mit } n \leq -1. \end{cases}$$

Beispiele:

(1) Ist k ein Körper, so ist ein k-Modul nichts anderes als ein k-Vektorraum.
(2) Ein $\mathbb{Z}$-Modul ist nichts anderes als eine abelsche Gruppe.
(3) Ist R ein Ring und $n \in \mathbb{N}$, so ist

$$R^n = \{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_1, \ldots, a_n \in R \}$$

in natürlicher Weise ein R-Modul.
(4) Für jeden Ring R ist $\{0\}$ ein R-Modul.
(5) Ist k ein Körper und $n \in \mathbb{N}$, so wird (der Spaltenraum) k^n zu einem $\mathrm{M}_n(k)$-Modul durch Matrizenmultiplikation:

$$\mathrm{M}_n(k) \times k^n \to k^n, \quad (A, b) \mapsto Ab.$$

(6) Ist k ein Körper, $n \in \mathbb{N}$ und $A \in \mathrm{M}_n(k)$, so wird k^n zu einem $k[x]$-Modul ($k[x]$ ist der Polynomring in der Unbestimmten x mit Koeffizienten aus k) durch

$$k[x] \times k^n \to k^n, \quad (f(x), v) \mapsto f(A)v.$$

Der folgende Satz zeigt, wie Darstellungen einer Gruppe G mit Moduln über dem Gruppenring $k[G]$ in natürlicher Verbindung stehen.

Satz. *Sei G eine (multiplikativ geschriebene) Gruppe und k ein Körper.*

(1) *Ist $\rho : G \to \mathrm{GL}(V)$ eine Darstellung von G auf einem k-Vektorraum V, so wird durch*

$$(\sum_{g \in G} a_g g) \cdot v = \sum_{g \in G} a_g \rho(g)(v)$$

V zu einem $k[G]$-Modul. (Insbesondere gilt $g \cdot v = \rho(g)(v)$ für $g \in G$ und $v \in V$.)
(2) *Ist V ein $k[G]$-Modul, so ist V ein k-Vektorraum und durch*

$$\rho : G \to \mathrm{GL}(V) \text{ mit } \rho(g)(v) = g \cdot v$$

wird eine Darstellung von G auf dem Vektorraum V definiert.
(3) *Die Konstruktionen in (1) und (2) sind invers zueinander.*

Beweis:

(1) Sei G eine Gruppe und $\rho : G \to \mathrm{GL}(V)$ eine Darstellung auf einem k-Vektorraum V. Natürlich ist $(V, +)$ eine abelsche Gruppe. Wir definieren nun

$$k[G] \times V \to V \text{ durch } (\sum_{g \in G} a_g g) \cdot v = \sum_{g \in G} a_g \rho(g)(v).$$

Wir überprüfen die in der Definition angegebenen Eigenschaften:

$$\begin{aligned}
1 \cdot v &= 1_G \cdot v = \rho(1_G)(v) = \mathrm{id}_V(v) = v, \\
(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g) \cdot v &= (\sum_{g\in G} (a_g + b_g) g) \cdot v = \sum_{g\in G} (a_g + b_g)\rho(g)(v) = \\
&= \sum_{g\in G} a_g \rho(g)(v) + \sum_{g\in G} b_g \rho(g)(v) = \\
&= (\sum_{g\in G} a_g g) \cdot v + (\sum_{g\in G} b_g g) \cdot v, \\
(\sum_{g\in G} a_g g) \cdot (v + w) &= \sum_{g\in G} a_g \rho(g)(v + w) = \sum_{g\in G} a_g \rho(g)(v) + \sum_{g\in G} a_g \rho(g)(w) = \\
&= (\sum_{g\in G} a_g g) \cdot v + (\sum_{g\in G} a_g g) \cdot w, \\
(\sum_{g\in G} a_g g)((\sum_{g\in G} b_g g) \cdot v) &= (\sum_{g_1\in G} a_{g_1} g_1)((\sum_{g_2\in G} b_{g_2} g_2) \cdot v) = \\
&= (\sum_{g_1\in G} a_{g_1} g_1) \cdot (\sum_{g_2\in G} b_{g_2} \rho(g_2)(v)) = \\
&= \sum_{g_1\in G} a_{g_1} \rho(g_1) \left(\sum_{g_2\in G} b_{g_2} \rho(g_2)(v) \right) = \\
&= \sum_{g_1\in G} \sum_{g_2\in G} a_{g_1} b_{g_2} \rho(g_1 g_2)(v) = \\
&= \sum_{g\in G} \left(\sum_{\substack{g_1, g_2\in G \\ g_1 g_2 = g}} a_{g_1} b_{g_2} \right) \rho(g)(v) = \\
&= \left(\sum_{g\in G} \left(\sum_{\substack{g_1, g_2\in G \\ g_1 g_2 = g}} a_{g_1} b_{g_2} \right) g \right) \cdot v = \\
&= \left((\sum_{g\in G} a_g g) \cdot (\sum_{g\in G} b_g g) \right) \cdot v.
\end{aligned}$$

Dies zeigt, dass V ein $k[G]$-Modul ist.

(2) Sei umgekehrt V ein $k[G]$-Modul. Dann ist V ein k-Vektorraum. Wir definieren für $g \in G$

$$\rho(g) : V \to V \quad \text{durch} \quad \rho(g)(v) = g \cdot v.$$

Wir zeigen zunächst, dass $\rho(g) \in \mathrm{End}_k(V)$ ist, d.h. dass $\phi(g)$ linear ist:

$$\begin{aligned}
\rho(g)(v + w) &= g \cdot (v + w) = g \cdot v + g \cdot w = \rho(g)(v) + \rho(g)(w), \\
\rho(g)(\lambda v) &= g \cdot (\lambda v) = (g \cdot \lambda) \cdot v = (\lambda \cdot g) \cdot v = \lambda \cdot (g \cdot v) = \lambda \rho(g).
\end{aligned}$$

Weiter gilt:

$$\begin{aligned}
\rho(gh)(v) &= (gh) \cdot v = g \cdot (h \cdot v) = g \cdot (\rho(h)(v) = \rho(g)(\rho(h)(v)) = (\rho(g) \circ \rho(h))(v), \\
\rho(1)(v) &= 1 \cdot v = v = \mathrm{id}_V(v),
\end{aligned}$$

also

$$\rho(gh) = \rho(g) \circ \rho(h) \quad \text{und} \quad \rho(1) = \mathrm{id}_V.$$

Daher ist $\rho : G \to \mathrm{GL}(V)$ eine Darstellung.

(3) Dies folgt sofort aus den angegebenen Formeln. ■

Definition. *Sei M ein R-Modul.*

(1) *Eine Teilmenge $U \subseteq M$ heißt ein* **Untermodul** *von M, wenn gilt:*
   - $0 \in U$,
   - $x, y \in U \Longrightarrow x + y \in U$,
   - $a \in R, x \in U \Longrightarrow ax \in U$.

   Dann ist U selbst ein R-Modul.
(2) *Der Modul M heißt* **einfach** *oder* **irreduzibel**, *wenn $M \neq \{0\}$ gilt und $\{0\}$ und M die einzigen Untermoduln von M sind.*

Bemerkungen:

(1) Ist R ein Ring, so ist R ein R-Modul durch Linksmultiplikation. Die Untermoduln von R sind genau die Linksideale.
(2) Ist k ein Körper, so sind die irreduziblen k-Moduln genau die 1-dimensionalen k-Vektorräume.
(3) Ein $\mathbb{Z}$-Modul A - also eine abelsche Gruppe - ist genau dann einfach, wenn A eine endliche abelsche Gruppe von Primzahlordnung ist.

Der folgende zeigt wieder, wie sich Begriffe aus der Darstellungstheorie mit $k[G]$-Moduln formulieren lassen:

Satz. *Sei G eine Gruppe und $\rho : G \to \mathrm{GL}(V)$ eine Darstellung von G auf einem k-Vektorraum V. Wir betrachten V als $k[G]$-Modul. Dann gilt:*

(1) *Die G-invarianten Unterräume von V sind genau die $k[G]$-Untermoduln von V.*
(2) *ρ ist genau dann irreduzibel, wenn V ein einfacher $k[G]$-Modul ist.*

Faktormoduln: Sei R ein Ring, M ein R-Modul und $N \subseteq M$ ein Untermodul.

(1) $(N, +)$ ist eine Untergruppe von $(M, +)$. Durch

$$x \equiv y \bmod N \quad \Longleftrightarrow \quad x - y \in N$$

wird eine Äquivalenzrelation auf M definiert. Die Äquivalenzklasse von $x \in M$ ist

$$\overline{x} = x + N = \{x + u : u \in N\}.$$

Die Menge der Äquivalenzklassen ist die **Faktorgruppe**

$$M/N = \{\overline{x} : x \in M\},$$

die durch

$$\overline{x} + \overline{y} = \overline{x + y} \quad \text{oder} \quad (x + N) + (y + N) = (x + y) + N$$

zu einer abelschen Gruppe wird.
(2) Ist $a \in R$, so gilt für $x, y \in M$

$$\begin{aligned} x \equiv y \bmod N \quad &\Longrightarrow \quad x - y \in N \quad \Longrightarrow \quad a(x - y) \in N \quad \Longrightarrow \quad ax - ay \in N \quad \Longrightarrow \\ &\Longrightarrow \quad ax \equiv ay \bmod N. \end{aligned}$$

Daher wird durch

$$R \times M/N \to M/N, \quad (a, \overline{x}) \mapsto \overline{ax}$$

eine Abbildung definiert. Man überprüft leicht, dass dadurch M/N zusammen mit obiger Addition zu einem R-Modul wird, dem Faktormodul M/N.

Beispiel: Der $\mathbb{Z}$-Modul $\mathbb{Z}$ hat die Untermoduln $n\mathbb{Z}$ (für $n \in \mathbb{N}_0$). Die Faktormoduln sind $\mathbb{Z}/n\mathbb{Z}$.

DEFINITION. *Seien M und N R-Moduln. Eine Abbildung $\alpha : M \to N$ heißt* **R-Modulhomomorphismus** *oder* **R-Homomorphismus** *oder* **R-linear**, *wenn gilt*

$$\alpha(x+y) = \alpha(x) + \alpha(y) \quad \text{und} \quad \alpha(rx) = r\alpha(x) \quad \text{für alle } x, y \in M \text{ und } r \in R.$$

(Ist der zugrundeliegende Ring R klar, so findet man statt R-linear auch linear etc.) **Kern** *und* **Bild** *werden durch*

$$\mathrm{Kern}(\alpha) = \alpha^{-1}(0) = \{x \in M : \alpha(x) = 0\} \quad \text{und} \quad \mathrm{Bild}(\alpha) = \alpha(M) = \{\alpha(x) : x \in M\}$$

definiert. Ein **R-Modulisomorphismus** *ist eine bijektive R-lineare Abbildung $\alpha : M \to N$.*

Bemerkungen:

(1) Ist $\alpha : M \to N$ eine R-lineare Abbildung zwischen R-Moduln M und N, so sind Kern und Bild Untermoduln von M bzw. N. Weiter gilt:

$$\alpha \text{ injektiv} \quad \Longleftrightarrow \quad \mathrm{Kern}(\alpha) = \{0\}$$

und

$$\alpha \text{ surjektiv} \quad \Longleftrightarrow \quad \mathrm{Bild}(\alpha) = N.$$

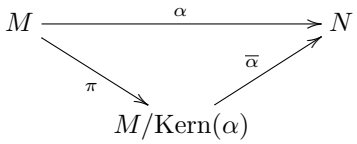
(2) Ist M ein R-Modul und N ein Untermodul, so ist die kanonische Abbildung

$$\pi : M \to M/N, \quad x \mapsto \overline{x}$$

ein surjektiver Modulhomomorphismus mit Kern N. Die N enthaltenden Untermoduln von M stehen in Bijektion zu den Untermoduln von M/N:

$$\begin{array}{rcl} \{U \text{ Untermodul} : N \subseteq U \subseteq M\} & \leftrightarrow & \{\overline{U} \text{ Untermodul} : \overline{U} \subseteq M/N\} \\ U & \to & \pi(U) \\ \pi^{-1}(\overline{U}) & \leftarrow & \overline{U} \end{array}$$

(3) Die aus der Gruppentheorie bekannten Isomorphiesätze übertragen sich auf auf Moduln. Wir geben ein Beispiel: Ist $\alpha : M \to N$ eine surjektive R-lineare Abbildung, so faktorisiert α über $M/\mathrm{Kern}(\alpha)$:



Dabei ist jetzt $\overline{\alpha}$ ein Isomorphismus.

DEFINITION. *Sei R ein Ring und M ein R-Modul. Ein Untermodul $U \subseteq M$ heißt* **maximal**, *wenn gilt*

- $U \subsetneq M$.
- *Ist V ein Untermodul von M mit $U \subseteq V \subseteq M$, so gilt $U = V$ oder $V = M$.*

Bemerkungen:

(1) Ist U ein Untermodul des R-Moduls M, so entsprechen die Untermoduln von M/U genau den Untermoduln von M, die U enthalten. Daher ergibt sich sofort folgende Charakterisierung:

$$U \subseteq M \text{ ist maximales Untermodul} \quad \Longleftrightarrow \quad M/U \text{ ist einfach.}$$

(2) Ist V ein k-Vektorraum der Dimension $n =\geq 1$, so sind die maximalen Unterräume genau die Unterräume der Dimension $n-1$.

(3) Ein Modul muss keine maximalen Untermoduln besitzen. (Der $\mathbb{Z}$-Modul $\mathbb{Q}$ besitzt keinen maximalen Untermodul.)

(4) In einem Ring R entsprechen die Untermoduln (nach unserer Konvention) den Linksidealen. Hier gilt der folgende wichtige Satz:

SATZ. *Ist R ein Ring und $\mathfrak{a} \subsetneq R$ ein von R verschiedenes Ideal, so gibt es ein maximales Linksideal (einen maximalen Untermodul) $\mathfrak{m}$, der $\mathfrak{a}$ enthält:*

$$\mathfrak{a} \subseteq \mathfrak{m} \subsetneq R.$$

Beweishinweis: Wie in der Algebra beweist man dies mit dem Zornschen Lemma. ■

Wir können jetzt einfache Moduln nochmals anders charakterisieren:

LEMMA. *Sei R ein Ring.*

(1) *Ist M ein einfacher Modul und $m \in M \setminus \{0\}$, definiert man*

$$f : R \to M \text{ mit } f(r) = rm,$$

so ist f surjektiv, der Kern ein maximales Linksideal in R und

$$R/\mathrm{Kern}(f) \simeq M.$$

(2) *Ist $\mathfrak{m}$ ein maximales Linksideal in R, so ist $R/\mathfrak{m}$ ein einfacher R-Modul.*

Beweis:

(1) Wegen $m \neq 0$ ist $\{0\} \subsetneq f(R) \subseteq M$, sodass mit der Einfachkeit von M sofort $f(R) = M$ folgt. Dann ist

$$R/\mathrm{Kern}(f) \simeq M.$$

Da die Untermoduln von M genau den zwischen $\mathrm{Kern}(f)$ und M gelegenen Moduln entsprechen, ist $\mathrm{Kern}(f)$ maximal.

(2) Dies folgt mit dem gleichen Argument wie in (1). ■

Bemerkung: Das Lemma garantiert mit dem vorangegangenen Satz, dass jeder Ring einfache Moduln besitzt.

Wir betrachten nun wieder die Situation von $k[G]$-Moduln.

LEMMA. *Sei G eine Gruppe. Seien $\rho_1 : G \to \mathrm{GL}(V_1)$ und $\rho_2 : G \to \mathrm{GL}(V_2)$ zwei Darstellungen von G über einem Körper k. Zugehörig betrachten wir V_1 und V_2 als $k[G]$-Moduln. Für eine $f : V_1 \to V_2$ sind dann folgende Aussagen äquivalent:*

(1) *f ist k-linear und für alle $g \in G$ gilt $f \circ \rho_1(g) = \rho_2(g) \circ f$.*

(2) *f ist ein $k[G]$-Modulhomomorphismus.*

Beweis:

- (1) $\Longrightarrow$ (2) Sei f k-linear mit $f \circ \rho_1(g) = \rho_2(g) \circ f$. Die k-Linearität impliziert $f(v_1 + v_2) = f(v_1) + f(v_2)$. Also müssen wir nur noch die Verträglichkeit mit der Multiplikation überprüfen:

$$\begin{aligned} f((\sum_{g\in G} a_g g) \cdot v) &= f(\sum_{g\in G} a_g \rho_1(g)(v)) = \sum_{g\in G} a_g f(\rho_1(g)(v)) = \\ &= \sum_{g\in G} a_g \rho_2(g)(f(v)) = (\sum_{g\in G} a_g g) \cdot f(v). \end{aligned}$$

  Dies zeigt, dass f $k[G]$-linear ist.

- (2) $\Longrightarrow$ (1) Sei f $k[G]$-linear. Dann ist f natürlich auch k-linear. Für $g \in G$ und $v \in V$ gilt daher

$$f(g \cdot v) = g \cdot f(v),$$

  was sich in

$$f(\rho_1(g)(v)) = \rho_2(g)(f(v))$$

  übersetzt, woraus sofort

$$f \circ \rho_1(g) = \rho_2(g) \circ f$$

  folgt, also die Behauptung. ■

LEMMA (Schur). *Sei R ein Ring, M und N zwei einfache R-Moduln und $f : M \to N$ eine R-lineare Abbildung. Dann gilt:*

(1) *Sind M und N nicht isomorph, so ist $f = 0$.*
(2) *Sind M und N isomorph, so ist $f = 0$ oder f ein Isomorphismus.*

Beweis: Da M als einfach vorausgesetzt war, $\mathrm{Kern}(f)$ ein Untermodul ist, gibt es genau zwei Möglichkeiten:

$$\mathrm{Kern}(f) = \{0\} \quad \text{oder} \quad \mathrm{Kern}(f) = M,$$

d.h.

$$f \text{ ist injektiv} \quad \text{oder} \quad f = 0.$$

Da N als einfach vorausgesetzt war und $\mathrm{Bild}(f)$ ein Untermodul von N ist, gibt es genau zwei Möglichkeiten:

$$\mathrm{Bild}(f) = \{0\} \quad \text{oder} \quad \mathrm{Bild}(f) = N,$$

d.h.

$$f = 0 \quad \text{oder} \quad f \text{ surjektiv.}$$

Natürlich ist $f = 0$ möglich. Ist $f \neq 0$, so folgt sofort die Bijektivität von f. Damit folgt das Lemma. ■

LEMMA. *Für einen Ring R und R-Moduln M und N sei*

$$\mathrm{Hom}_R(M, N) = \{f : M \to N \text{ ist } R\text{-linear}\}.$$

(1) *Sind $f, g \in \mathrm{Hom}_R(M, N)$ und definiert man $f + g : M \to N$ durch $(f + g)(x) = f(x) + g(x)$, so gilt auch $f + g \in \mathrm{Hom}_R(M, N)$.*
(2) *Mit der in (1) definierten Addition wird $\mathrm{Hom}_R(M, N)$ zu einer abelschen Gruppe.*
(3) *Ist R kommutativ und $f \in \mathrm{Hom}_R(M, N)$ und definiert man $af : M \to N$ durch $(af)(x) = af(x)$, so gilt auch $af \in \mathrm{Hom}_R(M, N)$.*
(4) *Ist R kommutativ, so wird $\mathrm{Hom}_R(M, N)$ mit den oben angegebenen Abbildungen zu einem R-Modul.*

Beweis: ■

Beispiele:

(1) Sei k ein Körper. Für $m, n \in \mathbb{N}$ betrachten wir die k-Vektorräume k^m und k^n. Ist $f : k^m \to k^n$, so gibt es eine Matrix $A \in \mathrm{M}(n \times m, k)$ mit

$$f(x) = Ax.$$

Man sieht, dass

$$\mathrm{M}(n \times n, k) \to \mathrm{Hom}_k(k^m, k^n), \quad A \mapsto (x \mapsto Ax)$$

eine Bijektion ist. Links und rechts stehen k-Vektorräume.

(2) Sei k ein Körper und $R = \mathrm{M}_2(k)$. Wir betrachten k^2 als R-Modul. Dann ist $f : k^2 \to k^2$ mit $f(x) = x$ R-linear:

$$f(x + y) = f(x) + f(y) \quad \text{und} \quad f(Ax) = Ax = Af(x).$$

Wir betrachten nun für eine Matrix A die Abbildung $g : k^2 \to k^2$ mit $g(x) = Ax$. Natürlich gilt $g(x + y) = g(x) + g(y)$. Für $B \in R$ gilt aber die Äquivalenz:

$$g(Bx) = Bg(x) \quad \Longleftrightarrow \quad ABx = BAx \quad \Longleftrightarrow \quad AB = BA.$$

Ist also A nicht mit allen Matrizen vertauschbar, so ist g nicht R-linear.

LEMMA. *Sei R ein Ring und M ein R-Modul. Sei*

$$\mathrm{End}_R(M) = \{f : M \to M \text{ ist } R\text{-linear}\}.$$

(1) *Mit der für $\mathrm{Hom}_R(M, M)$ definierten Addition wird $\mathrm{End}_R(M)$ zu einer abelschen Gruppe.*
(2) *Sind $f, g \in \mathrm{End}_R(M)$, so ist auch $f \circ g \in \mathrm{End}_R(M)$. (Statt $f \circ g$ schreibt man auch fg.)*
(3) *Mit $(f, g) \mapsto f + g$ und $(f, g) \mapsto f \circ g$ wird $\mathrm{End}_R(M)$ zu einem Ring mit Eins id_M, dem* **Endomorphismenring** *des R-Moduls M.*

Beweis:

(1) Dies wurde bereits bewiesen.
(2) Es gilt

$$(f \circ g)(x+y) = f(g(x+y)) = f(g(x)+g(y)) = f(g(x)) + f(g(y)) = (f \circ g)(x) + (f \circ g)(y)$$

und

$$(f \circ g)(ax) = f(g(ax)) = f(ag(x)) = af(g(x)) = a(f \circ g)(x).$$

Also ist auch $f \circ g$ R-linear.
(3) ■

LEMMA (Schur). *Ist M ein einfacher R-Modul, so ist $\mathrm{End}_R(M)$ ein Schiefkörper (oder Körper).*

Beweis: Ist $f \in \mathrm{End}_R(M) \setminus \{0\}$, so ist nach dem vorangegangenen Lemma von Schur f bijektiv, also ist f^{-1} ein Inverses von f in $\mathrm{End}_R(M)$. Damit gilt

$$\mathrm{End}_R(M)^* = \mathrm{End}_R(M) \setminus \{0\},$$

also ist $\mathrm{End}_R(M)$ ein Schiefkörper. ■

Bemerkung: Die Umkehrung des Lemmas von Schur gilt nicht. In den Aufgaben finden sich dazu Beispiele:

- Aufgabe 49 zeigt ein Beispiel eines nicht-einfachen Moduls M, für den $\mathrm{End}_R(M)$ ein Körper ist.
- In Aufgabe 53 wird gezeigt, dass der Endomorphismenring des (offensichtlich) nicht einfachen $\mathbb{Z}$-Moduls $\mathbb{Q}$ isomorph zu $\mathbb{Q}$, einem Körper ist.

Wir formulieren das Lemma von Schur nochmals für $k[G]$-Moduln:

LEMMA (Schur). *Sei k ein algebraisch abgeschlossener Körper, G eine Gruppe und V ein einfacher $k[G]$-Modul, der als k-Vektorraum endlich-dimensional ist. Dann gilt*

$$\mathrm{End}_{k[G]}(V) = \{\lambda \,\mathrm{id}_V : \lambda \in k\} \simeq k.$$

Beispiel: Wir betrachten die Darstellung ρ von $\mathbb{Z}_4 = \{0,1,2,3\}$ auf dem $\mathbb{Q}$-Vektorraum $V = \mathbb{Q}^2$, die durch

$$\rho(1)(v) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} v$$

definiert wird. Dann ist

$$\rho(0)(v) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} v, \quad \rho(1)(v) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} v, \quad \rho(2)(v) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} v, \quad \rho(3)(v) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} v$$

und für den zugehörigen Charakter χ gilt

$$\chi(0) = 2, \quad \chi(1) = 0, \quad \chi(2) = -2, \quad \chi(3) = 0$$

und

$$\langle \chi, \chi \rangle = \frac{1}{4}(\chi(0)\chi(0) + \chi(3)\chi(0) + \chi(2)\chi(2) + \chi(1)\chi(3)) = 2.$$

Wir betrachten V als $\mathbb{Q}[\mathbb{Z}_4]$-Modul. Da jedes Element von $\mathrm{End}_{\mathbb{Q}[\mathbb{Z}_4]}(V)$ auch eine $\mathbb{Q}$-lineare Abbildung des $\mathbb{Q}$-Vektorraums V ist, können wir die Elemente durch 2×2-Matrizen beschreiben. Sei als $f : V \to V$ gegeben durch $f(x) = Ax$ mit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Dann gilt:

$$\begin{aligned} f \in \mathrm{End}_{\mathbb{Q}[\mathbb{Z}_4]}(V) \quad &\Longleftrightarrow \quad f(Ax) = Af(x) \text{ für alle } x \in V \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad A\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} A \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \Longleftrightarrow \\ &\Longleftrightarrow \quad \begin{pmatrix} b & -a \\ d & -c \end{pmatrix} = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix} \quad \Longleftrightarrow \quad c = -b \text{ und } d = a. \end{aligned}$$

Wir erhalten also

$$A = \begin{pmatrix} a & -c \\ c & a \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + c\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

und damit

$$\mathrm{End}_{\mathbb{Q}[\mathbb{Z}_4]}(V) = \{x \mapsto Ax \text{ mit } A \in \mathbb{Q}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \mathbb{Q}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\}.$$

Mit $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ sieht man schnell, dass gilt

$$\mathrm{End}_{\mathbb{Q}[\mathbb{Z}_4]}(V) \simeq \mathbb{Q}(i) \text{ mit } i^2 = -1.$$

Hier gilt $\dim_{\mathbb{Q}}(\mathrm{End}_{\mathbb{Q}[\mathbb{Z}_4]}(V)) = 2 = \langle\chi,\chi\rangle$. Ein nachfolgender Satz besagt, dass dies ein allgemeines Phänomen ist.

Wir geben hier noch ein Beispiel, bei dem $\mathrm{End}_{k[G]}(V)$ ein „echter“, d.h. nichtkommutativer Schiefkörper ist.

Beispiel: Die Quaternionengruppe Q kann als Untergruppe von $\mathrm{GL}_2(\mathbb{C})$ durch

$$Q = \langle I, J\rangle \quad \text{mit} \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad \text{und} \quad J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

definiert werden. Mit $K = IJ$ und der 2×2-Einheitsmatrix $\mathbf{1}$ gilt

$$Q = \{\pm\mathbf{1}, \pm I, \pm J, \pm K\}.$$

Q hat also 8 Elemente. Zum Rechnen genügen die Relationen

$$I^2 = -\mathbf{1}, \quad J^2 = -\mathbf{1}, \quad JI = -IJ.$$

Ersetzen wir in den Matrizen I und J die komplexe Zahl i durch die Matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und die Zahl 0 durch die Matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, so erhalten wir 4×4-Matrizen, die wir mit i und j bezeichnen:

$$i = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Man rechnet nach, dass gilt $i^2 = j^2 = -\mathbf{1}_4$ und $ji = -ij$. Wir erhalten dadurch eine über $\mathbb{Q}$ definierte 4-dimensionale Darstellung von Q:

$$\rho : Q \to \mathrm{GL}(\mathbb{Q}^4) \text{ mit } \rho(I) = (x \mapsto ix) \text{ und } \rho(J) = (x \mapsto jx).$$

Für den zugehörigen Charakter findet man:

g	$\mathbf{1}$	$-\mathbf{1}$	$\pm I$	$\pm J$	$\pm K$
$\chi(g)$	4	-4	0	0	0

Damit erhält man $\langle \chi, \chi \rangle = 4$.
Wir betrachten nun $\mathbb{Q}^4$ als $\mathbb{Q}[Q]$-Modul. Die Elemente des Endomorphismenrings sind Abbildungen $f : \mathbb{Q}^4 \to \mathbb{Q}^4$, die durch 4×4-Matrizen $A \in \mathrm{M}_4(\mathbb{Q})$ gegeben werden, d.h. $f(x) = Ax$ und

$$Ai = iA \quad \text{und } Aj = jA$$

erfüllen. Setzt man allgemein an

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix},$$

so kann man mit $Ai = iA$ und $Aj = jA$ Parameter eliminieren und man erhält die Gestalt

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ -a_{12} & a_{11} & a_{14} & -a_{13} \\ -a_{13} & -a_{14} & a_{11} & a_{12} \\ -a_{14} & a_{13} & -a_{12} & a_{11} \end{pmatrix}.$$

Mit

$$\widetilde{i} \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \quad \widetilde{j} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad \widetilde{k} = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

gilt

$$A = a_{11}\mathbf{1}_4 + a_{12}\widetilde{i} + a_{13}\widetilde{j} - a_{14}\widetilde{k}.$$

Es ist also

$$\mathrm{End}_{\mathbb{Q}[Q]}(\mathbb{Q}^4) = \{a_{11}\mathbf{1}_4 + a_{12}\widetilde{i} + a_{13}\widetilde{j} - a_{14}\widetilde{k} : a_{11}, a_{12}, a_{13}, a_{14} \in \mathbb{Q}\}.$$

Man findet:

$$\widetilde{i}^2 = \widetilde{j}^2 = \widetilde{k}^2 = -\mathbf{1}_4, \quad \widetilde{k} = \widetilde{i} \cdot \widetilde{j}, \quad \widetilde{j} \cdot \widetilde{i} = -\widetilde{i} \cdot \widetilde{j}.$$

Dies beschreibt eine sogenannte Quaternionenalgebra. Sie ist 4-dimensional über $\mathbb{Q}$ und ein Schiefkörper.

Satz. *Sei k ein Körper der Charakteristik 0, $\rho_1 : G \to \mathrm{GL}(V_2)$ und $\rho_2 : G \to \mathrm{GL}(V_2)$ zwei endlichdimensionale Darstellungen von G über k mit zugehörigen Charakteren χ_1 und χ_2. Wir betrachten V_1 und V_2 als $k[G]$-Module. Dann gilt:*

$$\dim_k \mathrm{Hom}_{k[G]}(V_1, V_2) = \langle \chi_1, \chi_2 \rangle.$$

3. Direkte Produkte, direkte Summen und freie Moduln

Analog zum Produkt von Ringen definieren wir auch das Produkt von Moduln:

Definition. *Sei R ein Ring und $(M_i)_{i \in I}$ eine Familie von R-Moduln. Dann heißt*

$$\prod_{i \in I} M_i = \{(m_i)_{i \in I} : m_i \in M_i\}$$

das **direkte Produkt** *der R-Moduln M_i. Durch*

$$(m_i)_{i \in I} + (n_i)_{i \in I} = (m_i + n_i)_{i \in I} \quad \text{und} \quad a \cdot (m_i)_{i \in I} = (am_i)_{i \in I}$$

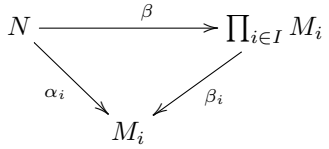
wird $\prod_{i \in I} M_i$ zu einem R-Modul. Die Projektionsabbildungen

$$\prod_{i \in I} M_i \to M_i, \quad (m_i)_{i \in I} \mapsto m_i$$

sind R-linear.

Der folgende Satz charakterisiert das direkte Produkt durch eine universelle Eigenschaft:

SATZ. *Sei $(M_i)_{i\in I}$ eine Familie von R-Moduln und $\prod_{i\in I} M_i$ das direkte Produkt mit den Projektionsabbildungen $\alpha_i : \prod_{i\in I} M_i \to M_i$. Ist N ein R-Modul und $\beta_i : N \to M_i$ eine Familie von R-linearen Abbildungen, so gibt es genau eine Abbildung $\beta : N \to \prod_{i\in I} M_i$, die das Diagramm*



kommutativ macht. Es ist

$$\beta(n) = (\alpha_i(n))_{i\in I}.$$

Beweis:

- *Eindeutigkeit:* Sei $\beta : N \to \prod_{i\in I} M_i$ mit $\alpha_i = \beta_i \circ \beta$. Sei $n \in N$ und $\beta(n) = (m_i)_{i\in I}$. Dann gilt
$$\alpha_i(n) = (\beta_i \circ \beta)(n) = \beta_i(\beta(n)) = \beta_i((m_j)_{j\in I}) = m_i,$$
also $m_i = \alpha_i(n)$, und damit
$$\beta(n) = (\alpha_i(n))_{i\in I}.$$
Dies beweist die Eindeutigkeit.
- *Existenz:* Wir definieren
$$\beta : N \to \prod_{i\in I} M_i \text{ durch } \beta(n) = (\alpha_i(n))_{i\in I}.$$
Natürlich ist β R-linear und erfüllt $\alpha_i = \beta_i \circ \beta$. Es folgt die Behauptung. ■

DEFINITION. *Sei R ein Ring und $(M_i)_{i\in I}$ eine Familie von R-Moduln. Dann heißt*

$$\bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} \in \prod_{i\in I} M_i : |\{i \in I : m_i \neq 0\}| < \infty\}$$

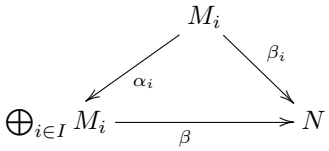
die **direkte Summe** *der Moduln M_i. (Die Elemente der direkten Summe sind also die Elemente des Produkts, die nur an endlich vielen Stellen von 0 verschiedene Komponenten haben.) Wir fassen hier die direkte Summe als Untermodul des direkten Produkts auf.*

Wir können die direkte Summe auch durch eine universelle Eigenschaft charakterisieren:

SATZ. *Sei R und Ring und $(M_i)_{i\in I}$ eine Familie von R-Moduln.*

(1) *Durch*
$$\alpha_i : M_i \to \bigoplus_{j\in I} M_j, \quad m_i \mapsto (\widetilde{m}_j)_{j\in I} \text{ mit } \widetilde{m}_j = \begin{cases} m_i & \text{für } j = i, \\ 0 & \text{für } j \neq i \end{cases}$$
wird eine injektive R-lineare Abbildung definiert.

(2) *Ist N ein R-Modul und ist $\beta_i : M_i \to N$, $i \in I$, eine Familie von R-linearen Abbildungen, so gibt es genau eine R-lineare Abbildung $\beta : \bigoplus_{i\in} M_i \to N$, das das Diagramm*



kommutativ macht. Es ist

$$\beta((m_i)_{i\in I}) = \sum_{i\in I} \beta_i(m_i).$$

Beweis:

- *Eindeutigkeit:* Für $\beta : \bigoplus_{i\in I} M_i \to N$ gelte $\beta \circ \alpha_i = \beta_i$. Sei $(m_i)_{i\in I}$. Dann gilt
$$\beta(\alpha_i(m_i)) = \beta_i(m_i).$$
Es folgt
$$\beta((m_i)_{i\in I}) = \beta(\sum_{\substack{i\in I\\ m_i\neq 0}} \alpha_i(m_i)) = \sum_{\substack{i\in I\\ m_i\neq 0}} \beta_i(m_i).$$
- *Existenz:* Man definiert $\beta : \bigoplus_{i\in I} M_i \to N$ durch
$$\beta((m_i)_{i\in I}) = \sum_{i\in I} \beta_i(m_i),$$
wobei zu beachten ist, dass in der Summe rechts nur endlich viele von 0 verschiedene Summanden vorkommen. Natürlich ist β R-linear. Die Eigenschaft $\beta(\alpha_i(m_i)) = \beta_i(m_i)$ ist dann trivialerweise erfüllt. ■

Bemerkung: Nach unserern Definition stimmen direktes Produkt und direkte Summe überein, wenn die Indexmenge I endlich ist.

Sei M ein R-Modul und $(M_i)_{i\in I}$ eine Familie von Untermoduln. Die Inklusion können wir als Modulhomomorphismus $\beta_i : M_i \to M$ deuten. Es gibt dann einen Modulhomomorphismus
$$\beta : \bigoplus_{i\in I} M_i \to M \quad \text{ mit } \beta((m_i)_{i\in I}) = \sum_{i\in I} m_i.$$
Ist β ein Isomorphismus, so sagt man $(M_i)_{i\in I}$ ist eine **direkte Summenzerlegung** von M. Dies ist äquivalent damit, dass sich jedes Elemente $m \in M$ eindeutig schreiben lässt als
$$m = \sum_{i\in I} m_i \text{ mit } m_i \in M_i,$$
wobei natürlich nur endlich viele m_i von 0 verschieden sind. Wir schreiben in diesem Fall auch
$$M = \bigoplus_{i\in I} M_i.$$
Im Allgemeinen ist
$$\sum_{i\in I} M_i = \{\sum_{i\in I} m_i : m_i \in M_i, |\{i \in I : m_i \neq 0\}| < \infty\}$$
ein Untermodul von M.

Beispiel: Sei k ein Körper, G eine Gruppe und $\rho_i : G \to \mathrm{GL}(V_i)$, $i \in I$ eine Familie von Darstellungen von G über k. Dann können wir V_i als $k[G]$-Modul betrachten, und damit auch die direkte Summe
$$\bigoplus_{i\in I} V_i.$$

Bemerkung: Sei k ein Körper und G eine endliche Gruppe mit $\mathrm{char}(k) \nmid |G|$. Sei $\rho : G \to \mathrm{GL}(V)$ eine Darstellung von G über k. Dann können wir V als $k[G]$-Modul betrachten. Ist $W \subseteq V$ ein G-invarianter Unterraum, so gibt es nach dem Satz von Maschke einen G-invarianten Unterraum W' mit
$$V = W \oplus W'.$$
Nun sind W und W' auch $k[G]$-Untermoduln von V. Wir erhalten dann
$$V = W \oplus W'$$
auch als $k[G]$-Moduln.

Ohne Beweis erwähnen wir noch folgende Eigenschaft (Bourbaki, A II.13, Corollaire 1):

Satz. *Sind $(M_i)_{i\in I}$ und $(N_j)_{j\in J}$ Familien von R-Moduln, so gilt*
$$\mathrm{Hom}_R(\bigoplus_{i\in I} M_i, \prod_{j\in J} N_j) \simeq \prod_{(i,j)\in I\times J} \mathrm{Hom}_R(M_i, N_j).$$

SATZ. *Sei k ein algebraisch abgeschlossener Körper der Charakteristik 0, G eine endliche Gruppe und $\rho_V : G \to \mathrm{GL}(V)$ und $\rho_W : G \to \mathrm{GL}(W)$ zwei endlich-dimensionale Darstellungen mit Charakteren χ_V und χ_W. Wir betrachten V und W als $k[G]$-Moduln. Dann gilt*

$$\dim_k \mathrm{Hom}_{k[G]}(V,W) = \langle \chi_V, \chi_W \rangle.$$

Beweis: Seien $\rho_i : G \to \mathrm{GL}(V_i)$, $i = 1, \ldots, h$ Repräsentanten der Isomorphieklassen irreduzibler Darstellungen und $\chi_1, \ldots, \chi_h$ die zugehörige Charaktere. Wir betrachten V_i als $k[G]$-Modul. Dann gibt es Zahlen $m_i, n_i \in \mathbb{N}_0$ mit

$$V \simeq m_1 V_1 \oplus \cdots \oplus m_h V_h, \quad W \simeq n_1 V_1 \oplus \cdots \oplus n_h V_h.$$

Wir wollen $\mathrm{Hom}_{k[G]}(V,W)$ mit der Formel des vorangegangenen Satzes auswerten. Da für $i \neq j$ die $k[G]$-Moduln V_i und V_j einfach und nicht isomorph sind, folgt $\mathrm{Hom}_{k[G]}(V_i, V_j) = \{0\}$. Es kommen $m_i n_i$ Faktoren $\mathrm{Hom}_{k[G]}(V_i, V_i)$ vor. Daher gilt:

$$\dim_k \mathrm{Hom}_{k[G]}(V,W) = \sum_{i=1}^{h} m_i n_i \dim_k \mathrm{Hom}_{k[G]}(V_i, V_i).$$

Da k als algebraisch abgeschlossen vorausgesetzt war, besteht $\mathrm{Hom}_{k[G]}(V_i, V_i)$ nur aus $\lambda \,\mathrm{id}_{V_i}$ mit $\lambda \in k$, also ist

$$\dim_k \mathrm{Hom}_{k[G]}(V_i, V_i) = 1.$$

Damit folgt nun

$$\dim_k \mathrm{Hom}_{k[G]}(V,W) = \sum_{i=1}^{h} m_i n_i = \sum_{i=1}^{h} m_i n_i \langle \chi_i, \chi_i \rangle = \langle \sum_{i=1}^{h} m_i \chi_i, \sum_{j=1}^{h} n_j \chi_j \rangle = \langle \chi_V, \chi_W \rangle.$$

Dies wollten wir beweisen. ■

Wir übertragen Begriffe von Vektorräumen auf Moduln.

DEFINITION. *Sei R ein Ring.*

(1) *Ist M ein R-Modul und $S \subseteq M$ eine Teilmenge von M, so heißt ein Ausdruck der Form*

$$\sum_{s \in S} a_s s \quad \text{mit } a_s \in R \text{ und } |\{s \in S : a_s \neq 0\}| < \infty$$

eine **Linearkombination** *von Elementen aus S mit Koeffizienten aus R. Wenn wir solche Linearkombinationen anschreiben, wird immer vorausgesetzt, dass nur endlich viele a_s von 0 verschieden sind, auch wenn dies nicht explizit angegeben wird.*

(2) *Die Menge aller Linearkombinationen von Elementen aus S, also*

$$\{\sum_{s \in S} a_s s : a_s \in R, |\{s \in S : a_s \neq 0\}| < \infty\}$$

ist offensichtlich ein Untermodul von M. Man nennt ihn den **von S erzeugten R-Untermodul**.

(3) *Ein Modul M heißt* **endlich erzeugt**, *wenn es eine endliche Teilmenge $S \subseteq M$ gibt, sodass der von S erzeugte Untermodul ganz M ist.*

(4) *Eine Teilmenge $S \subseteq M$ heißt* **linear unabhängig**, *wenn aus $\sum_{s \in S} a_s s = 0$ schon $a_s = 0$ für alle $s \in S$ folgt. In diesem Fall gilt auch:*

$$\sum_{s \in S} a_s s = \sum_{s \in S} b_s s \quad \Longleftrightarrow \quad a_s = b_s \text{ für alle } s \in S.$$

DEFINITION. *Sei M ein R-Modul und $S \subseteq M$ eine Teilmenge. S heißt eine* **Basis** *von M, wenn $S \neq \emptyset$, S linear unabhängig ist und M erzeugt, d.h. jedes $m \in M$ lässt sich eindeutig schreiben als*

$$m = \sum_{s \in S} a_s s \text{ mit } a_s \in R.$$

Ein Modul heißt **frei**, *wenn er eine Basis besitzt oder $\{0\}$ ist.*

Beispiele:

(1) Der Ring R als R-Modul besitzt die Basis $\{1\}$.
(2) Allgemeiner ist für $n \in \mathbb{N}$

$$R^n = \underbrace{R \oplus \cdots \oplus R}_{n \text{ Summanden}} = \{(x_1, \ldots, x_n) : x_i \in R\}$$

frei. Eine Basis ist $e_1, \ldots, e_n$ mit

$$e_i = (0, \ldots, 0, 1, 0, \ldots, 0),$$

wo an der Stelle i eine 1 steht und sonst lauter Nullen.
(3) Sei I eine nichtleere Menge. Für jedes $i \in I$ sei $R_i = R$ als R-Modul. Sei

$$F = \bigoplus_{i \in I} R_i.$$

Dann besitzt F eine Basis, nämlich $\{e_i : i \in I\}$, wobei e_i an der Stelle i 1, sonst aber 0 ist.

Ein zentraler Satz der Linearen Algebra ist:

SATZ. *Jeder Vektorraum V über einem Körper k ist ein freier k-Modul, d.h. $V = \{0\}$ oder V besitzt eine Basis. Außerdem sind zwei Basen eines Vektorraums gleichmächtig.*

Bemerkungen: Die Aussage des letzten Satzes verallgemeinert sich nicht auf Moduln über Ringen.

(1) Moduln über Ringen sind im Allgemeinen nicht frei. Manchmal ist dies einfach zu sehen, wie beim $\mathbb{Z}$-Modul $\mathbb{Z}/2\mathbb{Z}$, manchmal nicht, wie beim $\mathbb{Z}$-Modul $\prod_{i \in \mathbb{N}} \mathbb{Z}$.
(2) Bei Vektorräumen über Körpern sind alle Basen gleichmächtig. Dies muss bei einem freien Modul über einem Ring R nicht der Fall sein, wie Aufgabe 54 zeigt. Eine wichtige Ausnahme bilden kommutative Ringen, was im nächsten Satz erwähnt wird.

SATZ. *Ist R ein kommutativer Ring und M ein freier R-Modul, so haben alle Basen die gleiche Mächtigkeit. Man nennt diese Mächtigkeit auch den* **Rang** $\operatorname{rang}(M)$ *von M.*

Beweisidee: Sei $\mathfrak{m}$ ein maximales Ideal von R. Dann ist $R/\mathfrak{m}$ ein Körper. $\mathfrak{m}F = \{\sum_i a_i x_i : a_i \in \mathfrak{m}, x_i \in F\}$ ist ein Untermodul von F. Den Faktormodul $F/\mathfrak{m}F$ kann man als $R/\mathfrak{m}$-Vektorraum auffassen. Dann ist $\dim_{R/\mathfrak{m}}(F/\mathfrak{m}F)$ gerade die Mächtigkeit einer Basis von F. ■

Im nichtkommutativen Fall können wir folgendes Ergebnis beweisen:

SATZ. *Sei R ein Ring und M ein freier R-Modul mit einer Basis $e_1, \ldots, e_n$. Dann hat auch jede andere Basis nur endlich viele Elemente.*

Beweis: Sei $f_i, i \in I$ eine beliebige Basis von M. Um e_i als Linearkombination von $f_i, i \in I$ auszudrücken, genügen endlich viele f_i. Es gibt also eine endliche Teilmenge $J \subseteq I$, sodass für alle $i = 1, \ldots, n$ eine Darstellung

$$e_i = \sum_{j \in J} a_{ij} f_j \text{ mit } a_{ij} \in R$$

existiert. Nun ist aber $e_1, \ldots, e_n$ ein Erzeugendensystem von M. Wäre $I \neq J$ und $i \in I \setminus J$, so könnte man f_i als Linearkombination von $e_1, \ldots, e_n$ und daher als Linearkombination von $f_j, j \in J$ darstellen. Dann wären aber f_i und $f_j, j \in J$ linear abhängig, was nicht der Fall ist. Also gilt $I = J$, insbesondere ist I endlich. ■

Der folgende Satz spielt eine wichtige Rolle in nachfolgenden Anwendungen.

SATZ. *Sei M ein R-Modul mit einer Basis $(x_i)_{i \in I}$. Ist N ein R-Modul und $(y_i)_{i \in I}$ eine Familie von Elementen von N, so gibt es genau eine R-lineare Abbildung*

$$f : M \to N \text{ mit } f(x_i) = y_i \text{ für alle } i \in I.$$

Beweis: Wir müssen definieren

$$f(\sum_{i\in I} a_i x_i) = \sum_{i\in I} a_i y_i.$$

Nun bleibt noch zu zeigen, dass f wohldefiniert und R-linear ist. Diese Eigenschaften sind aber klar. ■

Der von einer nichtleeren Menge S erzeugte freie R-Modul $R\langle S\rangle$: Wir bilden

$$R\langle S\rangle = \{\sum_{s\in S} a_s s : a_s \in R, |\{s \in S : a_s \neq 0\}| < \infty\}$$

und definieren Addition und Linksmultiplikation mit Elementen aus R durch

$$(\sum_{s\in S} a_s s) + (\sum_{s\in S} b_s s) = \sum_{s\in S}(a_s + b_s)s$$

und

$$a \cdot (\sum_{s\in S} b_s s) = \sum_{s\in S} a b_s s.$$

Wir werden die vorangegangene Konstruktion nutzen um neue Moduln zu definieren.

4. Das Tensorprodukt über kommutativen Ringen

Wir haben früher das Tensorprodukt $V \otimes W$ zweier k-Vektorräume V und W eingeführt. Dies wird nun verallgemeinert.

Sei R ein Ring und $E_1, \ldots, E_n$ und F seien R-Moduln. Eine Abbildung

$$f : E_1 \times \cdots \times E_n \to F$$

heißt **n-multilinear**, wenn f in jeder Komponente R-linear ist, d.h. wenn gilt

$$f(x_1, \ldots, x_i + x_i', \ldots, x_n) = f(x_1, \ldots, x_i, \ldots, x_n) + f(x_1, \ldots, x_i', \ldots, x_n)$$

und

$$f(x_1, \ldots, a x_i, \ldots, x_n) = a f(x_1, \ldots, x_i, \ldots, x_n)$$

für alle i und alle $x_i, x_i' \in E_i$ und $a \in R$.
Im Fall $n = 2$ spricht man auch von einer **bilinearen Abbildung**.

Beispiele:

(1) Ist k ein Körper und $V_i = k^n$ für $i = 1, \ldots, n$, so ist die Determinante

$$\det : V_1 \times \cdots \times V_n \to k, \quad (v_1, \ldots, v_n) \mapsto \det(v_1 | \ldots | v_n)$$

eine multilineare Abbildung.

(2) Für $k = \mathbb{R}$ definiert das Kreuzprodukt eine bilineare Abbildung

$$\mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3, \quad (v, w) \mapsto v \times w.$$

(3) Ist R ein kommutativer Ring und $E_i = F = R$, so definiert

$$R \times \cdots \times R \to R, \quad (a_1, \ldots, a_n) \mapsto a_1 \ldots a_n$$

eine multilineare Abbildung. (Die Kommutativität der Multiplikation ist hier wichtig.)

Bemerkungen:

(1) Ist R ein Ring, sind E, F, M drei R-Moduln und ist

$$f : E \times F \to M$$

bilinear, so gilt für $a, b \in R$ und $x \in E$, $y \in F$

$$abf(x, y) = af(x, by) = f(ax, by) = bf(ax, y) = baf(x, y),$$

und damit

$$(ab - ba)f(x, y) = 0.$$

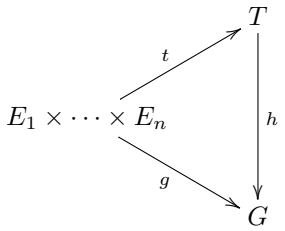
Ist R nicht kommutativ, so ergeben sich daraus offensichtlich deutliche Einschränkungen für bilineare Abbildungen.

(2) In Aufgabe 47 wird gezeigt, dass die einzige bilineare Abbildung für den Matrizenring $R = \mathrm{M}_2(k)$ (über einem Körper k) die Nullabbildung ist.
(3) Wir werden daher in diesem Abschnitt nur das Tensorprodukt für kommutative Ringe betrachten.

DEFINITION. *Sei R ein kommutativer Ring und $E_1, \dots, E_n$ seien R-Moduln. Ein R-Modul T zusammen mit einer multilinearen Abbildung $t : E_1 \times \cdots \times E_n \to T$ heißt ein* **Tensorprodukt** *von $E_1, \dots, E_n$, wenn es für jede multiplineare Abbildung*

$$g : E_1 \times \cdots \times E_n \to G$$

genau eine R-lineare Abbildung $h : T \to G$ gibt, sodass folgendes Diagramm kommutativ ist:



Konstruktion des Tensorprodukts: Seien $E_1, \dots, E_n$ R-Moduln.

(1) Sei M der freie R-Modul mit Basis $(x_1, \dots, x_n)$, $(x_1, \dots, x_n) \in E_1 \times \cdots \times E_n$. (Jedes n-Tupel $(x_1, \dots, x_n)$ liefert also ein Basiselement.) Jedes Element aus M lässt sich also eindeutig als R-Linearkombination schreiben:

$$\sum_{(x_1,\dots,x_n) \in E_1 \times \cdots \times E_n} a_{(x_1,\dots,x_n)}(x_1, \dots, x_n) \quad \text{mit} \quad a_{(x_1,\dots,x_n)} \in R,$$

wobei nur endlich viele $a_{(x_1,\dots,x_n)}$ von 0 verschieden sind. Wir haben eine natürliche Abbildung

$$f : E_1 \times \cdots \times E_n \to M, \quad (x_1, \dots, x_n) \mapsto 1 \cdot (x_1, \dots, x_n),$$

die aber nicht multilinear ist.

(2) Sei N der Untermodul von M, der von allen Elementen folgenden Typs erzeugt wird:
- $(x_1, \dots, x_i + x_i', \dots, x_n) - (x_1, \dots, x_i, \dots, x_n) - (x_1, \dots, x_i', \dots, x_n)$,
- $(x_1, \dots, ax_i, \dots, x_n) - a(x_1, \dots, x_i, \dots, x_n)$.

(3) Trivialerweise gilt dann
- $(x_1, \dots, x_i + x_i', \dots, x_n) \equiv (x_1, \dots, x_i, \dots, x_n) + (x_1, \dots, x_i', \dots, x_n) \bmod N$,
- $(x_1, \dots, ax_i, \dots, x_n) \equiv a(x_1, \dots, x_i, \dots, x_n) \bmod N$.

(4) Definieren wir also $T = M/N$ und t als $E_1 \times \cdots \times E_n \xrightarrow{f} M \xrightarrow{\pi} M/N = T$, schreiben wir

$$x_1 \otimes \cdots \otimes x_n = t(x_1, \dots, x_n),$$

so ist t offensichtlich multilinear, d.h.

$$x_1 \otimes \cdots \otimes (x_i + x_i') \otimes \cdots \otimes x_n = (x_1 \otimes \cdots \otimes x_i \otimes \cdots \otimes x_n) + (x_1 \otimes \cdots \otimes x_i' \otimes \cdots \otimes x_n)$$

und

$$x_1 \otimes \cdots \otimes ax_i \otimes \cdots \otimes x_n = a(x_1 \otimes \cdots \otimes x_i \otimes \cdots \otimes x_n).$$

Die Elemente von T schreiben sich in der Form

$$\sum_{(x_1,\dots,x_n) \in E_1 \times \cdots \times E_n} a_{(x_1,\dots,x_n)}(x_1 \otimes \cdots \otimes x_n).$$

(5) Sei $g : E_1 \times \cdots \times E_n \to G$ eine beliebige multilineare Abbildung.
   (a) Die Eigenschaft von M als freier R-Modul impliziert, dass es genau eine R-lineare Abbildung $\ell : M \to G$ gibt mit

$$\ell(\sum a_{(x_1,\dots,x_n)}(x_1, \dots, x_n)) = \sum a_{(x_1,\dots,x_n)} g(x_1, \dots, x_n).$$

   Da g multilinear ist, folgt $N \subseteq \mathrm{Kern}(\ell)$. Wir erhalten also eine induzierte Abbildung

$$h : T \to G \text{ mit } h(\sum a_{(x_1,\dots,x_n)}(x_1 \otimes \cdots \otimes x_n)) = \sum a_{(x_1,\dots,x_n)} g(x_1, \dots, x_n).$$

(b) Die Eindeutigkeit von h folgt sofort aus der Forderung
$$h(x_1 \otimes \cdots \otimes x_n) = g(x_1, \ldots, x_n).$$

(6) Wir schreiben
$$E_1 \otimes \cdots \otimes E_n = T,$$
wobei der zugrundeliegende Ring R oft durch $\otimes_R$ angedeutet wird.

Das konstruierte Tensorprodukt verallgemeinert das Tensorprodukt für Vektorräume, das wir zuvor konstruiert haben.

Beispiel: Wir betrachten die $\mathbb{Z}$-Moduln $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Q}$. Für $\overline{a} \in \mathbb{Z}/2\mathbb{Z}$ und $b \in \mathbb{Q}$ gilt in $\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$
$$\overline{a} \otimes b = \overline{a} \otimes (2 \cdot \frac{b}{2}) = 2 \cdot (\overline{a} \otimes \frac{b}{2}) = \overline{2a} \otimes \frac{b}{2} = \overline{0} \otimes \frac{b}{2} = \overline{0 \cdot 0} \otimes \frac{b}{2} = 0 \cdot (\overline{0} \otimes \frac{b}{2}) = 0.$$
Da das Tensorprodukt von Ausdrücken der Gestalt $\overline{a} \otimes b$ erzeugt wird, folgt
$$\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} = \{0\}.$$

Für freie Moduln verhält sich das Tensorprodukt etwas vorhersehbarer:

Satz. *Sei R ein kommutativer Ring, sei E ein freier R-Modul mit Basis e_i, $i \in I$ und F ein (beliebiger) R-Modul. Dann gilt: Jedes Element von $E \otimes_R F$ hat eine eindeutige Darstellung*
$$\sum_{i \in I} e_i \otimes f_i \quad \textit{mit} \quad f_i \in F,$$
wobei natürlich nur endlich viele f_i von 0 verschieden sind.

Beweis:

- Ist $a \in E$, so gibt es eine Darstellung
$$a = \sum_{i \in I} a_i e_i \text{ mit } a_i \in R,$$
wobei nur endlich viele a_i von 0 verschieden sind. Für $f \in F$ gilt dann
$$a \otimes f = \left(\sum_{i \in I} a_i e_i \right) \otimes f = \sum_{i \in I} a_i e_i \otimes f = \sum_{i \in I} e_i \otimes (a_i f).$$
Da $E \otimes_R F$ von Ausdrücken $a \otimes f$ erzeugt wird, folgt schnell, dass sich jedes Element in der Form
$$\sum_{i \in I} e_i \otimes f_i \text{ mit } f_i \in F$$
schreiben lässt.
- Sei nun $\sum_{i \in I} e_i \otimes f_i = 0$. Sei $i_0 \in I$. Dann gibt es eine R-lineare Abbildung $\ell : E \to R$ mit
$$\ell(e_i) = \begin{cases} 1 & \text{für } i = i_0, \\ 0 & \text{für } i \neq i_0. \end{cases}$$
Die Abbildung
$$h : E \times F \to F \text{ mit } h(a, f) = \ell(a) f$$
ist bilinear, faktorisiert also über das Tensorprodukt:
$$\overline{h}(a \otimes f) = \ell(a) f.$$
Es folgt
$$0 = \overline{h}(\sum_{i \in I} e_i \otimes f_i) = \sum_{i \in I} \ell(e_i) f_i = f_{i_0}.$$
Da $i_0 \in I$ beliebig gewählt werden konnte, folgt $f_i = 0$ für alle $i \in I$. Daraus folgt sofort die Eindeutigkeit der Darstellung. ■

Aus dem letzten Satz ergibt sich leicht folgende Folgerung:

FOLGERUNG. *Sei R ein kommutativer Ring, E ein freier R-Modul mit Basis $e_i, i \in I$ und F ein freier R-Modul mit Basis $f_j, j \in J$. Dann ist $E \otimes_R F$ ein freier R-Modul mit Basis*

$$e_i \otimes f_j, \quad (i,j) \in I \times J.$$

Insbesondere gilt also

$$\operatorname{rang}(E \otimes_R F) = \operatorname{rang}(E) \cdot \operatorname{rang}(F).$$

5. Halbeinfache Moduln

DEFINITION. *Sei R ein Ring. Ein R-Modul E heißt* **halbeinfach** *(engl: semisimple), wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

(1) *E ist die Summe einer Familie von einfachen Untermoduln, d.h. es gibt eine Familie $(E_i)_{i\in I}$ von einfachen Untermoduln E_i mit*

$$E = \sum_{i\in I} E_i.$$

(2) *E ist direkte Summe einer Familie von einfachen Untermoduln, d.h. es gibt eine Familie $(E_i)_{i\in I}$ von einfachen Untermoduln E_i mit*

$$E = \bigoplus_{i\in I} E_i.$$

(3) *Jeder Untermodul F von E ist direkter Summand, d.h. es gibt einen Untermodul F' mit*

$$E = F \oplus F'.$$

Beweis der Äquivalenz der Bedingungen (1), (2), (3)*:*

- (1) $\Longrightarrow$ (2) Sei also $E = \sum_{i\in I} E_i$. Sei $J \subseteq I$ eine maximale Teilmenge, sodass die Summe $\sum_{j\in J} E_j$ direkt ist. Sei nun $i \in I$ ein beliebiges Element. Dann ist

  $$(\sum_{j\in J} E_j) \cap E_i$$

  ein Untermodul von E_i. Da E_i einfach ist, gibt es zwei Möglichkeiten:
  Falls $(\sum_{j\in J} E_j) \cap E_i = \{0\}$, dann ist $i \notin J$, aber die Summe $\sum_{j\in J\cup\{i\}} E_j$ direkt. Dann wäre aber J nicht maximal. Also kann dieser Fall nicht eintreten.
  Es bleibt also nur die Möglichkeit $(\sum_{j\in J} E_j) \cap E_i = E_i$, d.h.

  $$E_i \subseteq \sum_{j\in J} E_j.$$

  Da $i \in I$ beliebig gewählt werden konnte, sind also alle E_i in $\sum_{j\in J} E_j$ enthalten. Damit gilt aber $E = \sum_{j\in J} E_j$. E ist also direkte Summe von einfachen Untermoduln.
- (2) $\Longrightarrow$ (3) Sei $E = \bigoplus_{i\in I} E_i$ und $F \subseteq E$ irgendein Untermodul. Wir wählen wieder eine maximale Teilmenge $J \subseteq I$, sodass die Summe $F + \bigoplus_{j\in J} E_j$ direkt ist. Nun betrachten wir ein beliebiges $i \in I$ und den Schnitt $(F + \bigoplus_{j\in J} E_j) \cap E_i$. Dies ist ein Untermodul des einfachen Moduls E_i, sodass es nur zwei Möglichkeiten gibt:
  Ist $(F+\bigoplus_{j\in J} E_j)\cap E_i = \{0\}$, so wäre die Summe $F+\bigoplus_{j\in J\cup\{i\}} E_j$ direkt, J also nicht maximale gewählt gewesen. Daher kann dieser Fall nicht eintreten.
  Es gilt also $E_i \subseteq F + \bigoplus_{j\in J} E_j$. Da dies für alle $i \in I$ gilt, folgt

  $$E = F + \bigoplus_{j\in J} E_j.$$

  Es folgt die Behauptung.
- (3) $\Longrightarrow$ (1)

– Wir zeigen zunächst, dass unter der angegebenen Voraussetzung jeder von 0 verschiedene Untermodul von E einen einfachen Untermodul enthält.
Es reicht, dies für Untermoduln der Gestalt Rv mit $v \in E\backslash\{0\}$ zu zeigen. Sei L der Kern des Modulhomomorphismus $R \to Rv$, $r \mapsto rv$. Sei M ein maximales Linksideal mit $L \subseteq M \subsetneq R$ (Zorn-Lemma). Dann ist Mv ein Untermodul von E, also gibt es nach Voraussetzung einen Untermodul M' mit $E = Mv \oplus M'$. Ist $x \in Rv \subseteq E$, so gibt es $a \in M$ und $x' \in M'$ mit $x = av + x'$. Dann ist aber $x' = x - av \in Rv$. Es folgt

$$Rv = Mv \oplus (M' \cap Rv).$$

Nun muss man sehen, dass Mv maximal in Rv ist. Dann ist $M' \cap Rv$ ein einfacher Modul.
– Sei nun E_0 die Summe der einfachen Untermoduln von E. Nach Voraussetzung gibt es einen Untermodul F mit $E = E_0 \oplus F$. Wäre $F \neq \{0\}$, so würde F einen einfachen Untermodul enthalten, was aber der Definition von E_0 widersprechen würde. Also ist $F = \{0\}$ und damit $E = E_0$, was wir zeigen wollten. ■

Beispiele:

(1) Ist k ein Körper, so sind alle k-Vektorräume halbeinfach: Ist $e_i, i \in I$ eine Basis von V, so ist

$$V = \bigoplus_{i \in I} ke_i$$

mit den einfachen Moduln ke_i.
(2) Die einfachen $\mathbb{Z}$-Moduln sind die zu den Moduln $\mathbb{Z}/p\mathbb{Z}$ (für eine Primzahl p) isomorphen Moduln. So sind

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3$$

und

$$\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

halbeinfache $\mathbb{Z}$-Moduln.
(3) Der $\mathbb{Z}$-Modul $\mathbb{Z}/4\mathbb{Z}$ ist nicht halbeinfach, da es beispielsweise zum Untermodul $\{\overline{0}, \overline{2}\}$ kein Komplement gibt.
(4) Ist G eine endliche Gruppe und k ein Körper mit $\mathrm{char}(k) \nmid |G|$, ist $\rho : G \to \mathrm{GL}(V)$ eine Darstellung von G über k, so ist V als $k[G]$-Modul nach dem Satz von Maschke halbeinfach.

Satz. *Sei R ein Ring. Dann gilt:*

(1) *Direkte Summen von halbeinfachen Moduln sind halbeinfach.*
(2) *Untermoduln halbeinfacher Moduln sind halbeinfach.*
(3) *Faktormoduln halbeinfacher Moduln sind halbeinfach.*

Beweis:

(1) Sind $(E_i)_{i \in I}$ halbeinfache Moduln mit $E = \bigoplus_{i \in I} E_i$, so gibt es einfache Moduln $E_{i,j}$ mit $E_i = \bigoplus E_{i,j}$. Dann ist

$$E = \bigoplus_{i,j} E_{i,j},$$

also E halbeinfach.
(2) Sei E ein halbeinfacher Modul und F ein Untermodul von E. Sei F_0 die Summe der einfachen Untermoduln von F. Da E halbeinfach ist, gibt es einen Untermodul F_0' mit $E = F_0 \oplus F_0'$.
Behauptung: $F = F_0 \oplus (F \cap F_0')$.
Natürlich ist die Summe direkt, und auch $\supseteq$ ist klar. Sei $x \in F$. Dann gibt es $x_0 \in F_0$ und $x_0' \in F_0'$ mit $x = x_0 + x_0'$. Dann ist aber $x_0' = x - x_0 \in F \cap F_0'$, also $F \subseteq F_0 \oplus (F \cap F_0')$. Dann ist $F \cap F_0'$ ein Untermodul von E. Wäre er von 0 verschieden, so würde er einen einfachen Untermodul enthalten, was aber der Definition von F_0 widersprechen würde. Es folgt $F = F_0$. Daher ist F halbeinfach.

(3) Sei F ein Untermodul von E. Wir wollen den Faktormodul E/F anschauen. Da E halbeinfach ist, können wir zerlegen $E = F \oplus F'$. Nun ist aber E/F isomorph zu F'. F' ist halbeinfach nach dem ersten Teil, also ist auch E/F halbeinfach. ■

Nochmals eine Aussage, die schon in obigem Beweis vorkam:

FOLGERUNG. *Ist E ein halbeinfacher R-Modul, so enthält jeder von 0 verschiedene Untermodul einen einfachen Modul.*

6. Halbeinfache Ringe

DEFINITION. *Ein Ring R mit $1 \neq 0$ heißt* **halbeinfach**, *wenn R ein halbeinfacher R-Modul ist.*

SATZ. *Ist R ein halbeinfacher Ring, so ist jeder R-Modul halbeinfach.*

Beweis: Jeder Modul M ist Faktormodul eines freien Moduls. Da freie Moduln die Gestalt $F = \bigoplus_{i \in I} R$ haben, ist F nach einem vorangegangenen Satz halbeinfach. Da Faktormoduln halbeinfacher Moduln halbeinfach sind, ist schließlich auch M halbeinfach. ■

Beispiele:

(1) Körper sind halbeinfache Ringe.
(2) Sei G eine endliche Gruppe und k ein Körper mit $\mathrm{char}(k) \nmid |G|$. Dann ist der Gruppenring $k[G]$ halbeinfach (nach dem Satz von Maschke).

LEMMA. *Sei k ein Körper und $R = \mathrm{M}_n(k)$ für ein $n \in \mathbb{N}$. Wir betrachten den R-Modul R. Sei*

$$L_i = \left\{ \begin{pmatrix} 0 & \dots & 0 & a_{1i} & 0 & \dots & 0 \\ 0 & \dots & 0 & a_{2i} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & a_{ni} & 0 & \dots & 0 \end{pmatrix} : a_{1i}, \dots, a_{ni} \in k \right\}.$$

Dann gilt:

(1) *L_i ist ein einfacher R-Modul. (L_i ist einfaches Linksideal.)*
(2) *$R = L_1 \oplus \dots \oplus L_n$.*
(3) *$R = \mathrm{M}_n(k)$ ist ein halbeinfacher Ring.*

Beweis:

(1) Natürlich ist L_i unter Addition abgeschlossen. Nach Definition der Matrizenmultiplikation ist L_i auch unter Matrizenmultiplikation abgeschlossen. Also ist L_i ein R-Untermodul von R. Sind $v, w \in k^n$ mit $(0|\dots|v|\dots|0), (0|\dots|w|\dots|0) \in L_i \setminus \{0\}$, so gibt es eine Matrix A mit $Av = w$. Dann gilt
$$A(0|\dots|v|\dots|0) = (0|\dots|w|\dots|0).$$
Daraus folgt sofort, dass L_i ein einfacher R-Modul ist.
(2) Die Zerlegung ist klar.
(3) Nach (2) ist der R-Modul R direkte Summe von einfachen Moduln. Also ist R halbeinfach als Modul. Damit ist nach Definition auch R als Ring halbeinfach. ■

Im folgenden Satz werden alle einfachen Linksideale des Matrizenrings $\mathrm{M}_n(k)$ angegeben.

SATZ. *Sei k ein Körper und $R = \mathrm{M}_n(k)$ mit $n \in \mathbb{N}$. Für $\ell \in \mathrm{M}(1 \times n, k) \setminus \{0\}$ sei*

$$L_\ell = \{a\ell : a \in k^n\} \subseteq R.$$

(Dabei fassen wir $a \in k^n$ als $n \times 1$-Matrix auf, sodass $a\ell$ eine $n \times n$-Matrix ist, also in R liegt.) Dann gilt:

(1) *Mit* $\ell_1 = (\ell_1, \dots, \ell_n)$ *gilt*

$$L_\ell = \{ \begin{pmatrix} a_1\ell_1 & a_1\ell_2 & \dots & a_1\ell_n \\ a_2\ell_1 & a_2\ell_2 & \dots & a_2\ell_n \\ \vdots & \vdots & & \vdots \\ a_n\ell_1 & a_n\ell_2 & \dots & a_n\ell_n \end{pmatrix} : a_1, \dots, a_n \in k\} = \{ \begin{pmatrix} a_1\ell \\ a_2\ell \\ \vdots \\ a_n\ell \end{pmatrix} : a_1, \dots, a_n \in k\}.$$

(2) *Für jedes* $\ell \in k^n \setminus \{0\}$ *ist* L_ℓ *ein einfaches Linksideal.*

(3) *Ist* L *ein einfaches Linksideal und* ℓ *eine von* 0 *verschiedene Zeile eines Elements von* L*, so gilt*

$$L = L_\ell.$$

Insbesondere haben alle einfachen Linksideale die Gestalt L_ℓ*.*

(4) *Für* $\ell, \ell' \in \mathrm{M}(1 \times n, k) \setminus \{0\}$ *gilt:*

$$L_\ell = L_{\ell'} \quad \Longleftrightarrow \quad \ell' = \lambda\ell \text{ für ein } \lambda \in k^*.$$

(5) *Sind* $\ell, \ell' \in \mathrm{M}(1 \times n, k) \setminus \{0\}$*, ist* $T \in \mathrm{M}_n(k)$ *mit*

$$\ell' = \ell T,$$

so ist

$$f : L_\ell \to L_{\ell'}, \quad x \mapsto xT$$

ein R*-Isomorphismus. Insbesondere gibt es nur eine Isomorphieklasse einfacher Linksideale.*

Beweis:

(1) Mit

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

erhält man

$$a\ell = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} (\ell_1, \ell_2, \dots, \ell_n) = \begin{pmatrix} a_1\ell_1 & a_1\ell_2 & \dots & a_1\ell_n \\ a_2\ell_1 & a_2\ell_2 & \dots & a_2\ell_n \\ \vdots & \vdots & & \vdots \\ a_n\ell_1 & a_n\ell_2 & \dots & a_n\ell_n \end{pmatrix} = \begin{pmatrix} a_1\ell \\ a_2\ell \\ \vdots \\ a_n\ell \end{pmatrix}.$$

(2) Natürlich ist $L_\ell = \{a\ell : a \in k^n\}$ abgeschlossen unter Addition. Wegen

$$A \cdot (a\ell) = (Aa)\ell$$

ist L_ℓ auch abgeschlossen unter R-Multiplikation, also ein Linksideal. Ist $a_1\ell \in L_\ell \setminus \{0\}$, so folgt aus $Ra_1 = k^n$, dass

$$R \cdot a_1\ell = L_\ell$$

gilt. Also ist L_ℓ ein einfaches Linksideal.

(3) Sei L ein einfaches Linksideal. Sei $A \in L \setminus \{0\}$ und ℓ eine von 0 verschiedene Zeile von A. Durch Multiplikation mit einer geeigneten Matrix von links können wir annehmen, dass die erste Zeile von A die Matrix ℓ ist. Sei Dann gilt

$$E_{11}A = \begin{pmatrix} \ell \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \ell \in L_\ell \cap L.$$

Durch Matrizenmultiplikation erhält man daraus alle Elemente von L_ℓ. Also folgt $L_\ell \subseteq L$. Da L als einfach vorausgesetzt war, folgt $L = L_\ell$.

(4) Wir zeigen zunächst $\Longrightarrow$: Es ist

$$\begin{pmatrix} \ell' \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in L_{\ell'},$$

also gibt es $a_1, \ldots, a_n \in k$ mit

$$\begin{pmatrix} \ell' \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_1\ell \\ a_2\ell \\ \vdots \\ a_n\ell \end{pmatrix}.$$

Es folgt $\ell' = a_1\ell$, und damit die Behauptung.
Die Richtung $\Longleftarrow$ ist klar.

(5) Sei also $\ell' = \ell T$. Ist $a\ell \in L_\ell$ (mit $a \in k^n$), so ist $a\ell T = a\ell' \in L_{\ell'}$. Daher ist die Abbildung wohldefiniert und natürlich R-linear. Wegen

$$f\left(\begin{pmatrix} \ell \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right) = \begin{pmatrix} \ell' \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

ist f von 0 verschieden, also nach dem Lemma von Schur bereits ein Isomorphismus. ■

Beispiel: Wir betrachten das Produkt $R = k \times k$, wo k ein Körper ist.

$$L_1 = \{(x, 0) : x \in k\} \quad \text{und} \quad L_2 = \{(0, y) : y \in k\}$$

sind zwei (offensichtlich) einfache Linksideale. Wegen $R = L_1 + L_2$ ist R ein halbeinfacher Ring. Sind die Linksideale L_1 und L_2 isomorph?

- Wir definieren
$$f : L_1 \to L_2, \quad (x, 0) \mapsto (0, x).$$
Offensichtlich ist f bijektiv und additiv. Ist f R-linear?
$$f((a, b) \cdot (x, 0)) = f((ax, 0)) = (0, ax), \quad \text{aber} \quad (a, b) \cdot f((x, 0)) = (a, b) \cdot (0, x) = (0, bx).$$
Da sich immer $a, x, y \in k$ finden lassen mit $ax \neq bx$, ist f nicht R-linear.
- Sei $g : L_1 \to L_2$ eine R-lineare Abbildung. Sei $f((1, 0)) = (0, c)$. Dann gilt:
$$g((x, 0)) = g((x, 0) \cdot (1, 0)) = (x, 0) \cdot g((1, 0)) = (x, 0) \cdot (0, c) = (0, 0) = 0.$$
Also ist $g = 0$. Insbesondere sind also L_1 und L_2 nicht isomorph.

LEMMA. *Sei R ein Ring.*

(1) *Sind L_1, L_2 zwei einfache, nichtisomorphe Linksideale von R, so gilt*
$$b_1 b_2 = b_2 b_1 = 0 \text{ für alle } b_1 \in L_1 \text{ und } b_2 \in L_2.$$
Man schreibt auch $L_1 L_2 = \{0\}$.

(2) *Ist L ein einfaches Linksideal von R und $a \in R$, so ist $La = \{0\}$ oder ein einfaches, zu L isomorphies Linksideal.*

Beweis:

(1) Sei $b_2 \in L_2$ ein beliebiges Element. Dann ist
$$f : L_1 \to L_2, \quad x \mapsto x b_2$$
R-linear. Nach dem Lemma von Schur ist $f = 0$ oder ein Isomorphismus. Da L_1 und L_2 nicht isomorph sein sollten, folgt $f = 0$, also
$$b_1 b_2 = 0 \text{ für alle } b_1 \in L_1.$$

Der Rest folgt daraus.

(2) Natürlich ist La ein Linksideal. Wir betrachten den surjektiven R-Homomorphismus

$$f : L \to La, \quad x \mapsto xa.$$

Da L einfach ist, ist $\mathrm{Kern}(f) = L$, also $f = 0$ und damit $La = 0$, oder $\mathrm{Kern}(f) = \{0\}$, also f injektiv und damit f ein Isomorphismus. Das wollten wir zeigen. ■

SATZ. *Sei R ein halbeinfacher Ring.*

(1) *Bis auf Isomorphie gibt es nur endlich viele einfache Linksideale. Sei $L_1, \ldots, L_h$ ein Repräsentantensystem. (Jedes einfache Linksideal ist also zu einem L_i isomorph. Für $i \neq j$ sind L_i und L_j nichtisomorph, insbesondere gilt $L_iL_j = L_jL_i = \{0\}$ für $i \neq j$.)*

(2) *Sei*

$$R_i = \sum_{L \simeq L_i} L,$$

also die Summe aller zu L_i isomorphen einfachen Linksideale. R_i ist ein zweiseitiges Ideal von R und es gilt $R_iR_j = R_jR_i = \{0\}$ für $i \neq j$.

(3) *Es gibt $e_i \in R_i$ mit*

$$1 = e_1 + \cdots + e_h, \quad e_i^2 = e_i, \quad e_ie_j = e_je_i = 0 \text{ für } i \neq j.$$

(4) *R_i ist ein Ring mit Einselement e_i. Es ist $R_i = Re_i = e_iR$.*

(5) *R_i ist ein halbeinfacher Ring und besitzt bis auf Isomorphie genau ein einfaches Linksideal, nämlich L_i.*

(6) *Durch*

$$R \to \prod_{i=1}^{h} R_i, \quad a \mapsto (ae_1, \ldots, ae_h)$$

wird ein Ringisomorphismus definiert.

Beweis:

- Sei $(L_i)_{i \in I}$ ein Repräsentantensystem der einfachen Linksideale von R bis auf Isomorphie. Sei

$$R_i = \sum_{L \simeq L_i} L$$

die Summe aller zu L_i isomorphen Linksideale. Natürlich ist R_i ein Linksideal. Nach dem letzten Lemma können wir aber auch von rechts mit Elementen aus R multiplizieren und bleiben in R_i. Also ist R_i auch ein Rechtsideal, und damit ein beidseitiges Ideal.

- Nach dem letzten Lemma gilt $L_iL_j = L_jL_i = \{0\}$ für $i \neq j$. Damit folgt dann schnell

$$R_iR_j = R_jR_i = \{0\} \text{ für } i \neq j.$$

- Da R als halbeinfach vorausgesetzt war, ist R Summe von Linksidealen, woraus insbesondere

$$R = \sum_{i \in I} R_i$$

folgt.

- Aus $R = \sum_{i \in I} R_i$ folgt, dass es Elemente $e_i \in R_i$ gibt mit

$$1 = \sum_{i \in I} e_i.$$

Für $x_i \in R_i$ folgt mit $R_iR_j = R_jR_i = \{0\}$ für $i \neq j$

$$x_i = x_i \cdot 1 = x_i \sum_{j \in I} e_j = x_ie_i \quad \text{und} \quad x_i = 1 \cdot x_i = (\sum_{j \in I} e_j) \cdot x_i = e_ix_i,$$

also

$$e_ix_i = x_ie_i = x_i \text{ für alle } x_i \in R_i.$$

Daher ist e_i das Einselement in R_i, insbesondere also R_i ein Ring. Da die Summe $\sum_{i \in I} e_i = 1$ endlich ist, ist auch die Indexmenge I endlich. Wir können also $I = \{1, \ldots, h\}$ annehmen.

- Da $e_1, \ldots, e_h$ zentrale Idempotente sind mit $1 = e_1 + \cdots + e_h$, folgt die Produktzerlegung

$$R \xrightarrow{\simeq} R_1 \times \cdots \times R_h$$

wie früher. ■

Bemerkungen:

(1) Wir erinnern an folgenden Satz von zuvor: Ist G eine endliche Gruppe und k ein algebraisch abgeschlossener Körper der Charakteristik 0, so gibt es einen Isomorphismus

$$k[G] \simeq \prod_{i=1}^{h} \mathrm{M}_{n_i}(k).$$

(2) Wir haben auch früher folgendes Ergebnis erwähnt: Ist k ein Körper der Charakteristik $\neq 2, 3$, so gibt es einen (explizit gegebenen) Isomorphismus

$$k[S_3] \simeq k \times k \times \mathrm{M}_2(k).$$

Beispiel: Wir betrachten die Quaternionengruppe $Q = \{\pm\mathbf{1}, \pm I, \pm J, \pm K\}$ (Aufgabe 4). Sei L ein beliebiger Körper mit $\mathrm{char}(L) \neq 2$. Den Gruppenring schreiben wir in der Form

$$L[Q] = \{a_1[\mathbf{1}] + a_2[-\mathbf{1}] + a_3[I] + a_4[-I] + a_5[J] + a_6[-J] + a_7[K] + a_8[-K] : a_1, \ldots, a_8 \in L\}.$$

Im Folgenden sei für $a_1, \ldots, a_8 \in L$

$$\alpha = a_1[\mathbf{1}] + a_2[-\mathbf{1}] + a_3[I] + a_4[-I] + a_5[J] + a_6[-J] + a_7[K] + a_8[-K].$$

Die 1-dimensionalen Charaktere liefern 4 Ringhomomorphismen $\varphi_i : L[Q] \to L$ (Aufgabe 13):

$$\begin{aligned}
\varphi_1(\alpha) &= a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8, \\
\varphi_2(\alpha) &= a_1 + a_2 - a_3 - a_4 + a_5 + a_6 - a_7 - a_8, \\
\varphi_3(\alpha) &= a_1 + a_2 - a_3 - a_4 - a_5 - a_6 + a_7 + a_8, \\
\varphi_4(\alpha) &= a_1 + a_2 + a_3 + a_4 - a_5 - a_6 - a_7 - a_8.
\end{aligned}$$

Nun betrachten wir noch die Quaternionenalgebra A, die über L definiert ist durch

$$A = L + L\,i + L\,j + L\,k \text{ mit } i^2 = -1, j^2 = -1, ij = -ji, k = ij.$$

Durch

$$Q \to \{\pm 1, \pm i, \pm j, \pm k\} \subseteq A^*$$

mit

$$\mathbf{1} \mapsto 1, \quad -\mathbf{1} \mapsto -1, \quad I \mapsto i, \quad -I \mapsto -i,$$

$$J \mapsto j, \quad -J \mapsto -j, \quad K \mapsto k, \quad -K \mapsto -k$$

wird ein Gruppenisomorphismus definiert. Der Gruppenhomomorphismus $Q \to A^*$ liefert dann den Ringhomomorphismus $\varphi_5 : L[Q] \to A$ mit

$$\varphi_5(\alpha) = a_1 - a_2 + (a_3 - a_4)i + (a_5 - a_6)j + (a_7 - a_8)k.$$

Wir erhalten den Ringhomomorphismus

$$\varphi : L[Q] \to L \times L \times L \times L \times A, \quad \alpha \mapsto (\varphi_1(\alpha), \varphi_2(\alpha), \varphi_3(\alpha), \varphi_4(\alpha), \varphi_5(\alpha)).$$

Offensichtlich ist φ auch eine L-lineare Abbildung. Wählt man in $L[Q]$ die L-Basis

$$[\mathbf{1}], [-\mathbf{1}], [I], [-I], [J], [-J], [K], [-K]$$

und in $L \times L \times L \times L \times A$ die L-Basis

$$(1,0,0,0,0), (0,1,0,0,0), (0,0,1,0,0), (0,0,0,1,0), (0,0,0,0,1), (0,0,0,0,i), (0,0,0,0,j), (0,0,0,0,k),$$

so wird φ durch die Matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

(mit Determinante $-256 = -2^8$) beschrieben. Da wir $\mathrm{char}(L) \neq 2$ vorausgesetzt haben, ist φ ein Isomorphismus.

Der Abschnitt hört hier unvollendet auf.

Wenn man die Theorie in der angefangenen Richtung weiterentwickelt, kommt man schließlich zu folgendem wichtigen Satz:

Satz (Wedderburn-Artin). *Jeder halbeinfache Ring R ist isomorph zu einem Produkt*

$$R \simeq \prod_{i=1}^{h} M_{n_i}(D_i),$$

wobei D_i ein Schiefkörper und $M_{n_i}(D_i)$ der Ring der $n_i \times n_i$-Matrizen mit Einträgen aus dem Schiefkörper D_i ist.