LINEARE ALGEBRA II

JÜRGEN HAUSEN

Fassung vom 9. Juni 2023

Vorwort zur ersten Auflage

Der vorliegende Text entstand aus einer Vorlesung “Lineare Algebra II” im Rahmen des Mathematikstudiums. Er führt das Skriptum [1] fort. Ich habe mich wieder um knappe Darstellung bemüht, ohne dabei auf vollständige Beweise und Beispiele zu verzichten. Jeder Textabschnitt lässt sich in einer Vorlesungsdoppelstunde (90 min.) behandeln.

Tübingen im April 2013 Jürgen Hausen

Vorwort zur geplanten zweiten Auflage

Beim vorliegenden Text handelt es sich um die Vorabversion einer zweiten Auflage des Skriptums “Lineare Algebra II”. In den beiden ersten Abschnitten wird nun auch auf nicht-abelsche Gruppen eingegangen. Darüberhinaus wird das Skriptum um zwei einführende Kapitel zur Darstellungstheorie endlicher Gruppen ergänzt. Nach wie vor lässt sich jeder Textabschnitt in einer Vorlesungsdoppelstunde (90 min.) behandeln.

Für Korrekturen, Hinweise und Anregungen, insbesondere in der Entstehungsphase dieses Textes, bin ich sehr dankbar.

Tübingen im Sommer 2021 Jürgen Hausen

Inhaltsverzeichnis

1. Gruppen und Ringe

1.1. **Gruppen.**

Erinnerung 1.1.1. Eine *Gruppe* ist eine nichtleere Menge G zusammen mit einer inneren Verknüpfung

$$\mu\colon G \times G \;\to\; G, \qquad (g_1, g_2) \;\mapsto\; \mu(g_1, g_2) =: g_1 * g_2,$$

sodass folgendes gilt:

(G1) Die Verknüpfung "$*$" auf G ist assoziativ, d.h., für je drei $g_1, g_2, g_3 \in G$ hat man

$$g_1 * (g_2 * g_3) \quad = \quad (g_1 * g_2) * g_3.$$

(G2) Die Verknüpfung "$*$" auf G besitzt ein neutrales Element, d.h., es gibt ein Element $e \in G$, sodass für jedes $g \in G$ gilt

$$e * g \;=\; g \;=\; g * e.$$

(G3) Jedes $g \in G$ besitzt ein inverses Element bezüglich "$*$", d.h., zu jedem $g \in G$ gibt es ein $g' \in G$ mit

$$g' * g \;=\; e \;=\; g * g'.$$

Eine Gruppe G mit Verknüpfung "$*$" heisst *abelsch*, auch *kommutativ*, falls sie zusätzlich zu (G1), (G2) und (G3) die folgende Eigenschaft besitzt:

(Ab) Die Verknüpfung "$*$" auf G ist kommutativ, d.h., für je zwei $g_1, g_2 \in G$ hat man

$$g_1 * g_2 \quad = \quad g_2 * g_1.$$

Will man die Verknüpfung einer Gruppe G näher bezeichnen, so schreibt man auch $(G, *)$ anstatt G. Wir werden oft abkürzend $g_1 g_2 := g_1 * g_2$ verwenden.

Das neutrale Element einer Gruppe G ist stets eindeutig bestimmt; man bezeichnet es auch mit e_G. Ebenso ist das Inverse eines Elements $g \in G$ eindeutig bestimmt; man bezeichnet es mit g^{-1}.

Eine abelsche Gruppe G schreiben wir im folgenden meistens additiv, d.h., die Verknüpfung wird bezeichnet durch

$$\alpha\colon G \times G \;\to\; G, \qquad (g_1, g_2) \;\mapsto\; \alpha(g_1, g_2) =: g_1 + g_2.$$

Das neutrale Element bezeichnen wir dann mit 0_G, das Inverse zu gegebenem $g \in G$ mit $-g$ und für $g_1 + (-g_2)$ schreiben wir kurz $g_1 - g_2$.

Beispiel 1.1.2. Die Menge $\mathbb{Z}$ der ganzen Zahlen zusammen mit der üblichen Addition ist eine abelsche Gruppe.

Definition 1.1.3. Die *Ordnung* einer Menge X ist die Anzahl ihrer Elemente und wird mit $|X|$ bezeichnet.

Beispiel 1.1.4. Zu jedem $n \in \mathbb{Z}_{\geq 1}$ gibt es eine abelsche Gruppe der Ordnung n: Die Menge

$$C_n \;:=\; \{\overline{0}, \ldots, \overline{n-1}\}$$

besitzt genau n Elemente und wird zu einer abelschen Gruppe durch die Verknüpfung

$$\overline{a} + \overline{b} \quad := \quad \overline{r(a+b; n)},$$

wobei man für $c \in \mathbb{Z}$ mit $r(c;n) \in \{0, \ldots n-1\}$ den *Rest von c modulo n* bezeichnet, d.h., man hat

$$c \;=\; k(c;n)n + r(c;n), \quad k(c;n), r(c;n) \in \mathbb{Z}, \quad 0 \leq r(c;n) \leq n-1.$$

Das neutrale Element in C_n ist $\overline{0}$ und für $1 \leq a \leq n-1$ ist das Inverse zu $\overline{a}$ gegeben durch $-\overline{a} = \overline{n-a}$.

Beispiel 1.1.5 (Permutationen)**.** Für eine beliebige Menge X betrachten wir die Menge ihrer *Permutationen*:

$$S(X) \;:=\; \{\sigma\colon X \to X;\ \sigma \text{ ist bijektiv}\}.$$

Zusammen mit der Hintereinanderausführung von Abbildungen wird die Menge $S(X)$ zu einer Gruppe:

$$S(X) \times S(X) \;\to\; S(X), \qquad (\sigma, \tau) \;\mapsto\; \sigma \circ \tau.$$

Ein wichtiger Spezialfall ist die n-elementige Menge $X_n := \{1, 2, \ldots, n\}$. Sie liefert die *symmetrische Gruppe*:

$$S_n \;:=\; S(X_n).$$

Die Elemente von S_n stellen wir durch Wertetabellen dar; beispielsweise haben wir in S_3 das Element

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \colon X_3 \;\to\; X_3, \qquad 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1.$$

Eine *Transposition* ist eine Bijektion aus S_n, die lediglich zwei Elemente i, j von X_n vertauscht; dafür verwendet man auch die Notation

$$(i,j)\colon X_n \;\to\; X_n, \qquad i \mapsto j,\ j \mapsto i,\ k \mapsto k \text{ für } k \neq i, j.$$

Die symmetrische Gruppe S_n besitzt genau $|S_n| = n!$ viele Elemente. Für $n \geq 3$ ist S_n nicht abelsch. Beispielsweise haben wir in S_3:

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \;=\; \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \;=\; \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}.$$

Beispiel 1.1.6. Die Menge $\mathrm{GL}(n;\mathbb{K}) \subset \mathrm{Mat}(n,n;\mathbb{K})$ aller invertierbaren $(n \times n)$-Matrizen über einem Körper $\mathbb{K}$ ist zusammen mit der Matrizenmultiplikation

$$\mathrm{GL}(n;\mathbb{K}) \times \mathrm{GL}(n;\mathbb{K}) \;\to\; \mathrm{Mat}(n,n;\mathbb{K}), \qquad (A,B) \;\mapsto\; AB$$

eine Gruppe, die *allgemeine lineare Gruppe*. Für $n \geq 2$ ist $\mathrm{GL}(n;\mathbb{K})$ nicht abelsch. Beispielsweise haben wir in $\mathrm{GL}(2;\mathbb{Q})$:

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

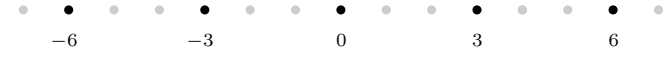
$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \;=\; \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Erinnerung 1.1.7. Es sei G eine Gruppe. Eine *Untergruppe* von G ist eine Teilmenge $H \subseteq G$ mit den Eigenschaften

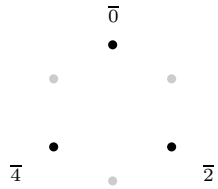
$$e_G \in H, \qquad h_1, h_2 \in H \;\Rightarrow\; h_1 h_2 \in H, \qquad h \in H \;\Rightarrow\; h^{-1} \in H$$

und der *induzierten Verknüpfung* $(h_1, h_2) \mapsto h_1 h_2$; wir schreiben dafür $H \leq G$. Jede Untergruppe $H \leq G$ ist eine Gruppe mit neutralem Element $e_H = e_G$.

Beispiel 1.1.8. Für jede ganze Zahl $n \in \mathbb{Z}$ ist $n\mathbb{Z} = \{nk;\ k \in \mathbb{Z}\}$ eine Untergruppe von $\mathbb{Z}$. Für $n = 3$ erhält man folgendes Bild:



Beispiel 1.1.9. Die Teilmenge $\{\overline{0}, \overline{2}, \overline{4}\}$ ist eine Untergruppe der Gruppe $C_6 = \{\overline{0}, \ldots, \overline{5}\}$.



Erinnerung 1.1.10. Es seien $(G, *)$ und $(H, \star)$ Gruppen. Eine Abbildung $\varphi\colon G \to H$ heisst *Gruppenhomomorphismus*, falls für je zwei $g_1, g_2 \in G$ gilt:

$$\varphi(g_1 * g_2) \;=\; \varphi(g_1) \star \varphi(g_2).$$

Ist $\varphi\colon G \to H$ ein Gruppenhomomorphismus, so gilt $\varphi(e_G) = e_H$ und für jedes $g \in G$ gilt $\varphi(g^{-1}) = \varphi(g)^{-1}$.

Die Komposition zweier Gruppenhomomorphismen ist stets wieder ein Gruppenhomomorphismus.

Beispiel 1.1.11. Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann hat man einen surjektiven Gruppenhomomorphismus

$$\pi\colon \mathbb{Z} \;\to\; C_n, \qquad a \;\mapsto\; \overline{r(a;n)}.$$

Beispiel 1.1.12. Wir betrachten die Gruppe S_n. Das *Signum* einer Permutation $\sigma \in S_n$ ist gegeben als

$$\mathrm{sg}(\sigma) \;:=\; \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \;=\; (-1)^{m(\sigma)},$$

wobei $m(\sigma)$ die Zahl der *Fehlstände*, also die Zahl der Paare i, j mit $i < j$ und $\sigma(i) > \sigma(j)$ ist. Das Signum definiert einen Gruppenhomomorphismus

$$\mathrm{sg}\colon S_n \;\to\; \{\pm 1\}, \qquad \sigma \;\mapsto\; \mathrm{sg}(\sigma).$$

Beispiel 1.1.13. Es sei $\mathbb{K}$ ein Körper. Die Determinante definiert einen Gruppenhomomorphismus

$$\det\colon \mathrm{GL}(n;\mathbb{K}) \;\to\; \mathbb{K}^*, \qquad A \;\mapsto\; \det(A).$$

Definition 1.1.14. Ein Gruppenhomomorphismus $\varphi\colon G \to H$ heisst *Isomorphismus*, falls es einen Gruppenhomomorphismus $\psi\colon H \to G$ gibt mit

$$\psi \circ \varphi \;=\; \mathrm{id}_G, \qquad\qquad \varphi \circ \psi \;=\; \mathrm{id}_H.$$

Wir nennen zwei Gruppen G und H *isomorph* zueinander, in Zeichen $G \cong H$, falls es einen Isomorphismus $G \to H$ gibt.

Satz 1.1.15. *Es seien G und H Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann sind folgende Aussagen äquivalent:*

(i) *$\varphi\colon G \to H$ ist ein Isomorphismus.*
(ii) *$\varphi\colon G \to H$ ist bijektiv.*

Beweis. Die Implikation "(i)⇒(ii)" ist klar. Zu "(ii)⇒(i)". Da $\varphi\colon G \to H$ bijektiv ist, gibt es eine Umkehrabbildung $\psi\colon H \to G$. Für je zwei $h_1, h_2 \in H$ gilt

$$h_1 h_2 \;=\; \varphi\left(\psi(h_1)\right) \varphi\left(\psi(h_2)\right) \;=\; \varphi\left(\psi(h_1)\, \psi(h_2)\right).$$

Wendet man ψ auf diese Identität an, so erhält man $\psi(h_1 h_2) = \psi(h_1)\psi(h_2)$ für je zwei Elemente $h_1, h_2 \in H$. □

Definition 1.1.16. Es seien G und H Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus. *Kern* und *Bild* von φ sind definiert als

$$\begin{aligned} \operatorname{Kern}(\varphi) &:= \{g \in G;\ \varphi(g) = e_H\} &&= \varphi^{-1}(e_H), \\ \operatorname{Bild}(\varphi) &:= \{\varphi(g);\ g \in G\} &&= \varphi(G). \end{aligned}$$

Beispiel 1.1.17. Der Gruppenhomomorphismus $\pi\colon \mathbb{Z} \to C_n,\ a \mapsto \overline{r(a;n)}$ besitzt die Untergruppe $n\mathbb{Z} \subseteq \mathbb{Z}$ als Kern.

Beispiel 1.1.18. Der Kern des Signums $\operatorname{sg}\colon S_n \to \{\pm 1\}$ ist eine Untergruppe der symmetrischen Gruppe S_n, die *alternierende Gruppe*

$$\ker(\operatorname{sg}) \ = \ A_n \ := \ \{\sigma \in S_n;\ \operatorname{sg}(\sigma) = 1\}.$$

Beispiel 1.1.19. Der Kern der Determinante $\det\colon \mathrm{GL}(n;\mathbb{K}) \to \mathbb{K}^*$ ist eine Untergruppe von $\mathrm{GL}(n;\mathbb{K})$, die *spezielle lineare Gruppe*

$$\ker(\det) \ = \ \mathrm{SL}(n;\mathbb{K}) \ := \ \{A \in \mathrm{GL}(n;\mathbb{K});\ \det(A) = 1\}.$$

Bemerkung 1.1.20. Es sei $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt:

(i) Für jede Untergruppe $H' \leq H$ ist das Urbild $\varphi^{-1}(H')$ eine Untergruppe von G; insbesondere ist $\operatorname{Kern}(\varphi) = \varphi^{-1}(e_H)$ eine Untergruppe von G.
(ii) Für jede Untergruppe $G' \leq G$ ist das Bild $\varphi(G')$ eine Untergruppe von H; insbesondere gilt $\operatorname{Bild}(\varphi) \leq H$.

Satz 1.1.21. *Es sei $\varphi\colon G \to H$ ein Homomorphismus von Gruppen. Dann sind folgende Aussagen äquivalent:*

(i) *φ ist injektiv.*
(ii) *Es gilt* $\operatorname{Kern}(\varphi) = \{e_G\}$.

Beweis. Die Implikation "(i)⇒(ii)" ist klar: Wegen der Injektivität von φ kann es höchstens ein Element $g \in G$ geben mit $\varphi(g) = e_H$, und e_G hat diese Eigenschaft.

Zur Implikation "(ii)⇒(i)". Es seien $g_1, g_2 \in G$ mit $\varphi(g_1) = \varphi(g_2)$ gegeben. Dann gilt

$$e_H \ = \ \varphi(g_2)^{-1}\varphi(g_1) \ = \ \varphi(g_2^{-1}g_1).$$

Das bedeutet $g_2^{-1}g_1 \in \operatorname{Kern}(\varphi)$ und somit, nach Voraussetzung, $g_2^{-1}g_1 = e_G$. Multiplikation mit g_2 von links ergibt $g_1 = g_2$. □

Konstruktion 1.1.22. Es seien $G_1, \ldots, G_r$ Gruppen. Das *direkte Produkt*dieser Gruppen ist $G_1 \times \ldots \times G_r$ zusammen mit der komponentenweisen Verknüpfung

$$(g_1, \ldots, g_r) * (h_1, \ldots, h_r) \quad := \quad (g_1 * h_1, \ldots, g_r * h_r).$$

Das direkte Produkt von $G_1, \ldots, G_r$ ist wieder eine Gruppe; neutrales Element und Inversenbildung sind gegeben durch

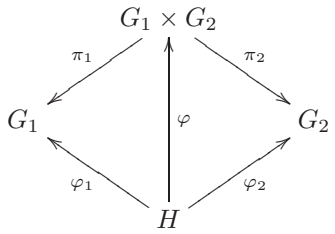
$$e_{G_1 \times \ldots \times G_r} \ = \ (e_{G_1}, \ldots, e_{G_r}), \qquad (g_1, \ldots, g_r)^{-1} \ = \ (g_1^{-1}, \ldots, g_r^{-1}).$$

Weiter hat man für jeden Index $1 \leq i \leq r$ einen surjektiven Gruppenhomomorphismus

$$\pi_i\colon G_1 \times \ldots \times G_r \ \to \ G_i, \qquad (g_1, \ldots, g_r) \ \mapsto \ g_i.$$

Bemerkung 1.1.23. Es seien $G_1, \ldots, G_r$ Gruppen. Die Gruppe $G_1 \times \ldots \times G_r$ ist genau dann abelsch, wenn alle G_i, $1 \leq i \leq r$, abelsch sind.

Bemerkung 1.1.24. Es seien G_i, H Gruppen und $\varphi_i := H \to G_i$ Gruppenhomomorphismen, wobei $i = 1, 2$. Dann hat man ein kommutatives Diagramm



mit einem eindeutig bestimmten Gruppenhomomorphismus $\varphi\colon H \to G_1 \times G_2$, gegeben durch $h \mapsto (\varphi_1(h), \varphi_2(h))$.

Aufgaben zu Abschnitt 1.1.

Aufgabe 1.1.25. Es seien G eine Gruppe und $H_i \subseteq G$, $i \in I$, Untergruppen. Zeige: Der Durchschnitt $\bigcap_{i\in I} H_i$ ist wieder eine Untergruppe von G.

Aufgabe 1.1.26. Beweise Bemerkung 1.1.20: Es sei $\varphi\colon G \to H$ ein Homomorphismus von Gruppen. Dann gilt:

(i) Für jede Untergruppe $H' \leq H$ ist das Urbild $\varphi^{-1}(H')$ eine Untergruppe von G.
(ii) Für jede Untergruppe $G' \leq G$ ist das Bild $\varphi(G')$ eine Untergruppe von H.

Aufgabe 1.1.27. Es seien $m, l \in \mathbb{Z}_{\geq 1}$ und $n := ml$. Zeige, dass die folgenden Abbildungen wohldefinierte Gruppenhomomorphismen sind:

(i) $\varphi\colon C_m \to C_n$, $\overline{a} \mapsto \overline{la}$,
(ii) $\psi\colon C_n \to C_m$, $\overline{a} \mapsto \overline{r(a;m)}$.

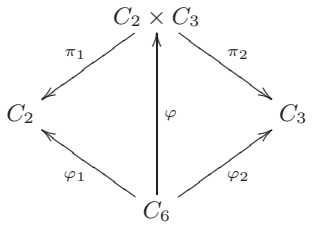
Aufgabe 1.1.28. Bestimme Kern und Bild für die beiden Gruppenhomomorphismen $\varphi\colon C_3 \to C_6$, $\overline{a} \mapsto \overline{2a}$ und $\psi\colon C_6 \to C_3$, $\overline{a} \mapsto \overline{r(a;3)}$.

Aufgabe 1.1.29. Betrachte die symmetrische Gruppe S_3 und den Homomorphismus $\mathrm{sg}\colon S_3 \to \{\pm 1\}$. Zeige:

$$\begin{aligned} \mathrm{sg}^{-1}(1) &= \left\{ \mathrm{id}_{X_3}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\}, \\ \mathrm{sg}^{-1}(-1) &= \{(1,2),\, (1,3),\, (2,3)\}\,. \end{aligned}$$

Aufgabe 1.1.30. Beweise die Aussagen aus der Konstruktion 1.1.22 und Bemerkung 1.1.23.

Aufgabe 1.1.31. Zeige: Mit den Gruppenhomomorphismen $\varphi_1\colon C_6 \to C_2$, $\overline{a} \mapsto \overline{r(a;2)}$ und $\varphi_1\colon C_6 \to C_3$, $\overline{a} \mapsto \overline{r(a;3)}$ erhält man ein kommutatives Diagramm



Zeige weiter, dass $\varphi\colon C_6 \to C_2 \times C_3$ ein Isomorphismus ist. Das bedeutet dann insbesondere $C_6 \cong C_2 \times C_3$.

Aufgabe 1.1.32. Zeige: Die Gruppen C_4 und $C_2 \times C_2$ sind nicht isomorph zueinander. *Hinweis*: Für jedes Element aus $C_2 \times C_2$ gilt $(\overline{a}, \overline{b}) + (\overline{a}, \overline{b}) = (\overline{0}, \overline{0})$, aber in C_4 haben wir $\overline{1} + \overline{1} = \overline{2} \neq \overline{0}$.

1.2. **Homogene Räume und Faktorgruppen.**

Erinnerung 1.2.1. Es sei X eine Menge. Eine *Relation* auf X ist eine Teilmenge $R \subseteq X \times X$. Man schreibt $x \sim y$, falls $(x, y) \in R$ gilt.

Eine *Äquivalenzrelation* auf X ist eine Relation $R \subseteq X \times X$ mit folgenden Eigenschaften

(i) R ist *reflexiv*, d.h., für alle $x \in X$ gilt $x \sim x$.
(ii) R ist *symmetrisch*, d.h., für alle $x, y \in X$ gilt $x \sim y \implies y \sim x$.
(iii) R ist *transitiv*, d.h., für alle $x, y, z \in X$ gilt $x \sim y$ und $y \sim z \implies x \sim z$.

Es sei $R \subseteq X \times X$ eine Äquivalenzrelation auf X. Die *Äquivalenzklasse* eines Elementes $x \in X$ ist die Menge

$$[x] \quad := \quad \{x' \in X;\ x' \sim x\}.$$

Man nennt das Element $x \in X$ auch einen *Repräsentanten* der Äquivalenzklasse $[x] \subseteq X$. Für je zwei Elemente $x, y \in X$ hat man folgende Aussagen:

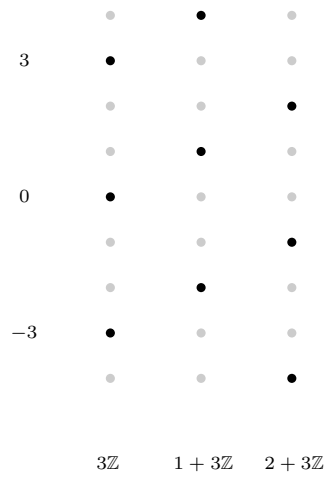
(i) Es gilt genau dann $[x] = [y]$ wenn $x \sim y$ gilt.
(ii) Es gilt entweder $[x] = [y]$ oder $[x] \cap [y] = \emptyset$.

Insbesondere erhält man die Menge X als disjunkte Vereinigung aller Äquivalenzklassen von R.

Beispiel 1.2.2. Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann ist $n\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$. Wir erhalten eine Äquivalenzrelation auf $\mathbb{Z}$ durch

$$a \sim_{n\mathbb{Z}} b : \iff \quad a - b \in n\mathbb{Z} \quad \iff \quad r(a; n) - r(b; n) \in n\mathbb{Z} \quad \iff \quad r(a; n) = r(b; n).$$

Die zugehörigen Äquivalenzklassen sind $n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}$ und wir haben die disjunkte Vereinigung $\mathbb{Z} = n\mathbb{Z} \sqcup 1 + n\mathbb{Z} \sqcup \ldots \sqcup (n-1) + n\mathbb{Z}$; etwa für $n = 3$:



Definition 1.2.3. Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Für ein Element $g \in G$ nennt man

$$gH \quad := \quad \{gh;\ h \in H\}$$

die zugehörige *(Links-)Nebenklasse*. Der durch die Untergruppe $H \leq G$ gegebene *homogene Raum* ist die Menge aller Nebenklassen:

$$G/H \quad := \quad \{gH;\ g \in G\}.$$

Satz 1.2.4. *Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann erhält man eine Äquivalenzrelation auf G durch:*

$$g_1 \ \sim_H \ g_2 \quad :\Longleftrightarrow \quad g_2^{-1} g_1 \ \in \ H.$$

Die Äquivalenzklasse $[g] \subseteq G$ eines Elements $g \in G$ ist genau seine Nebenklasse $gH \subseteq G$. Insbesondere hat man eine Darstellung als disjunkte Vereinigung

$$G \ = \ \bigsqcup_{gH \in G/H} gH.$$

Beweis. Zunächst weisen wir die Eigenschaften einer Äquivalenzrelation für "$\sim_H$" nach. Zur Reflexivität: Für jedes $g \in G$ gilt

$$g^{-1} g \ = \ e_G \ = \ e_H \ \in \ H$$

und somit $g \sim_H g$. Zur Symmetrie: Gilt $g_1 \sim_H g_2$, so haben wir $g_2^{-1} g_1 \in H$. Das impliziert

$$g_1^{-1} g_2 \ = \ \left(g_2^{-1} g_1\right)^{-1} \ \in \ H$$

und es folgt $g_2 \sim_H g_1$. Zur Transitivität: Gilt $g_1 \sim_H g_2$ und $g_2 \sim_H g_3$, so erhält man $g_1 \sim_H g_3$ mit

$$g_3^{-1} g_1 \ = \ \underbrace{g_3^{-1} g_2}_{\in H} \underbrace{g_2^{-1} g_1}_{\in H} \ \in \ H.$$

Wir zeigen nun, dass für jedes Element $g \in G$ die zugehörige Äquivalenzklasse $[g]$ gerade die Linksnebenklasse gH ist: Für jedes Element $g' \in G$ gilt

$$g' \in [g] \iff g' \sim_H g \iff g^{-1} g' \in H \iff g' \in gH.$$

Somit gilt $[g] = gH$ für jedes $g \in G$. Insbesondere sehen wir, dass G die disjunkte Vereinigung der Linksnebenklassen gH ist. □

Definition 1.2.5. Es sei G eine Gruppe. Der *Index* einer Untergruppe $H \leq G$ ist die Ordnung des homogenen Raumes G/H; in Zeichen $[G : H] := |G/H|$.

Satz 1.2.6 (Satz von Lagrange)**.** *Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt*

$$|G| \ = \ [G : H] \cdot |H|.$$

Insbesondere ist im Fall einer endlichen Gruppe G die Ordnung $|H|$ ein Teiler der Ordnung $|G|$.

Lemma 1.2.7. *Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann gilt $|gH| = |H|$ für jedes $g \in G$.*

Beweis. Jedes $g \in G$ definiert eine Bijektion $L_g \colon H \to gH$, $h \mapsto gh$; die zugehörige Umkehrabbildung ist dabei gegeben durch $L_g^{-1} = L_{g^{-1}} \colon gH \to H$, $gh \mapsto g^{-1}(gh)$. Insbesondere gilt $|gH| = |H|$. □

Beweis von Satz 1.2.6. Nach Satz 1.2.4, Lemma 1.2.7 und der Definition des Index haben wir

$$G \ = \ \bigsqcup_{gH \in G/H} gH, \qquad |gH| \ = \ |H|, \qquad |G/H| \ = \ [G : H].$$

Gilt $|G| = \infty$, so muss also mindestens eine der Mengen H und G/H unendlich sein, was die Behauptung in diesem Fall beweist. Gilt $|G| < \infty$, so erhalten wir

$$|G| \ = \ \sum_{gH \, \in \, G/H} |gH| \ = \ \sum_{gH \, \in \, G/H} |H| \ = \ |G/H||H| \ = \ [G : H]|H|.$$

□

Folgerung 1.2.8. *Es sei G eine endliche Gruppe. Ist $|G|$ eine Primzahl, so sind $\{e_G\}$ und G die einzigen Untergruppen von G.*

Definition 1.2.9. Es sei G eine Gruppe und es sei $g \in G$. Die von g in G *erzeugte Untergruppe* ist

$$\langle g \rangle \ := \ \{g^n;\, n \in \mathbb{Z}\} \ \leq \ G.$$

Die *Ordnung* $\operatorname{ord}(g)$ des Elements $g \in G$ ist die Ordnung $|\langle g \rangle|$ der von $\langle g \rangle$ erzeugten Untergruppe.

Folgerung 1.2.10. *Es sei G eine endliche Gruppe. Dann ist für jedes $g \in G$ die Ordnung $\operatorname{ord}(g)$ ein Teiler der Gruppenordnung $|G|$.*

Folgerung 1.2.11. *Es sei G eine endliche Gruppe. Ist $|G|$ eine Primzahl, so gilt $G = \langle g \rangle$ für jedes $g \in G$ mit $g \neq e_G$.*

Definition 1.2.12. Eine Untergruppe $H \leq G$ einer Gruppe G heißt *Normalteiler*, notiert $H \trianglelefteq G$, falls $gHg^{-1} = H$ für alle $g \in G$, wobei $gHg^{-1} := \{ghg^{-1};\ h \in H\}$.

Bemerkung 1.2.13. Ist G eine abelsche Gruppe, so ist jede Untergruppe $H \leq G$ ein Normalteiler.

Bemerkung 1.2.14. Eine Untergruppe $H \leq G$ einer Gruppe G ist genau dann Normalteiler in G, wenn $gH = Hg$ für alle $g \in G$ gilt, wobei $Hg := \{hg;\ h \in H\}$.

Beispiel 1.2.15. In der nichtabelschen Gruppe $\mathrm{GL}(2;\mathbb{Q})$ haben wir die Menge aller oberen Dreiecksmatrizen mit Diagonaleinträgen Eins:

$$U(2;\mathbb{Q}) \ := \ \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix};\ a \in \mathbb{Q} \right\}.$$

Die Menge $U(2;\mathbb{Q})$ ist eine Untergruppe von $\mathrm{GL}(2;\mathbb{Q})$, aber kein Normalteiler: Für jedes $a \in \mathbb{Q}$ haben wir

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \ = \ \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}, \qquad \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ = \ \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}.$$

Somit haben wir ein Element $A \in \mathrm{GL}(2;\mathbb{Q})$ gefunden mit $AU(2;\mathbb{Q}) \neq U(2;\mathbb{Q})A$. Nach Bemerkung 1.2.14 ist $U(2;\mathbb{Q})$ kein Normalteiler in $\mathrm{GL}(2;\mathbb{Q})$.

Konstruktion 1.2.16 (Faktorgruppe)**.** Es seien G eine Gruppe und $H \trianglelefteq G$ ein Normalteiler. Dann besitzt der homogene Raum G/H eine Verknüpfung

$$G/H \times G/H \ \to \ G/H, \qquad (g_1H, g_2H) \ \mapsto \ g_1g_2H.$$

Zusammen mit dieser Verknüpfung ist G/H eine Gruppe, die *Faktorgruppe* von G nach H. Neutrales Element und Inversenbildung sind gegeben durch

$$e_{G/H} \ = \ e_GH, \qquad\qquad (gH)^{-1} \ = \ g^{-1}H.$$

Weiter hat man einen surjektiven Gruppenhomomorphismus von G auf die Faktorgruppe G/H mit Kern H, nämlich

$$\pi\colon G \ \to \ G/H, \qquad\qquad g \ \mapsto \ gH.$$

Beweis. Wir zeigen zunächst, dass die Verknüpfung wohldefiniert ist. Dazu betrachten wir zwei Nebenklassen

$$g_1H \ = \ g_1'H, \qquad g_2H \ = \ g_2'H.$$

Wir müssen $g_1g_2H = g_1'g_2'H$ nachweisen. Zunächst liefert die Normalteilereigenschaft $g_2'H = Hg_2'$. Damit erhalten wir

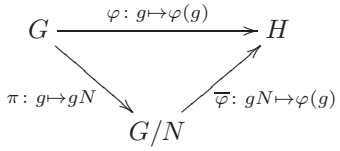
$$g_1g_2H \ = \ g_1g_2'H \ = \ g_1Hg_2' \ = \ g_1'Hg_2' \ = \ g_1'g_2'H.$$

Die Gruppenaxiome für G/H und die Homomorphieeigenschaft von π ergeben sich dann unmittelbar. Offensichtlich ist π surjektiv und $\operatorname{Kern}(\pi) = H$ folgt mit

$$\pi(g) = e_{G/H} \iff gH = e_G H \iff g \in H.$$

□

Satz 1.2.17 (Homomorphiesatz)**.** *Es seien $\varphi\colon G \to H$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ ein Normalteiler mit $N \subseteq \operatorname{Kern}(\varphi)$. Dann gibt es ein kommutatives Diagramm*



wohldefinierter Gruppenhomomorphismen. Dabei ist $\overline{\varphi}\colon G/N \to H$ durch dieses kommutative Diagramm eindeutig bestimmt. Es gilt weiter

(i) *$\overline{\varphi}$ ist injektiv $\Leftrightarrow$ $N = \operatorname{Kern}(\varphi)$;*
(ii) *$\overline{\varphi}$ ist surjektiv $\Leftrightarrow$ φ ist surjektiv.*

Beweis. Wir zeigen zunächst, dass $\overline{\varphi}\colon gN \mapsto \varphi(g)$ wohldefiniert ist. Dazu sei $g' \in G$ mit $g'N = gN$. Dann gilt $g' = gn$ mit einem $n \in N$. Wegen $N \subseteq \operatorname{Kern}(\varphi)$ gilt $\varphi(n) = e_H$, und es folgt

$$\varphi(g') \;=\; \varphi(gn) \;=\; \varphi(g)\varphi(n) \;=\; \varphi(g).$$

Somit ist $\overline{\varphi}$ ein wohldefiniert Abbildung. Die Kommutativität des Diagrammes ist dann nach Konstruktion gegeben. Weiter ist $\overline{\varphi}$ ein Homomorphismus, denn für $g_1N, g_2N \in G/N$ erhalten wir

$$\overline{\varphi}(g_1Ng_2N) \;=\; \overline{\varphi}(g_1g_2N) \;=\; \varphi(g_1g_2) \;=\; \varphi(g_1)\varphi(g_2) \;=\; \overline{\varphi}(g_1N)\overline{\varphi}(g_2N).$$

Die Eindeutigkeit von $\overline{\varphi}$ ist eine Folge der Kommutativität des Diagramms: Für jede Nebenklasse $gN \in G/N$ haben wir $\overline{\varphi}(gN) = \varphi(g)$, was den Homomorphismus $\overline{\varphi}$ bereits festlegt.

Wir kommen zur Charakterisierung der Injektivität. Der Homomorphismus $\overline{\varphi}$ ist genau dann injektiv, wenn $\operatorname{Kern}(\overline{\varphi}) = \{e_G N\}$ gilt. Wir müssen also zeigen:

$$\operatorname{Kern}(\overline{\varphi}) = \{e_G N\} \quad\Longleftrightarrow\quad \operatorname{Kern}(\varphi) = N.$$

Zur Implikation "⇒": Aufgrund der Kommutativität des Diagramms erhalten wir:

$$\operatorname{Kern}(\varphi) \;=\; \varphi^{-1}(e_H) \;=\; \pi^{-1}(\overline{\varphi}^{-1}(e_H)) \;=\; \pi^{-1}(\operatorname{Kern}(\overline{\varphi})) \;=\; \pi^{-1}(e_G N) \;=\; N.$$

Zur Implikation "⇐". Wir erhalten $\operatorname{Kern}(\overline{\varphi}) = \{e_G N\}$ mit

$$\overline{\varphi}(gN) = e_H \iff \varphi(g) = e_H \iff g \in N \iff gN = e_G N.$$

Die Charakterisierung der Surjektivität ergibt sich sofort aus der Identität $\operatorname{Bild}(\overline{\varphi}) = \operatorname{Bild}(\varphi)$. □

Satz 1.2.18. *Es sei $\varphi\colon G \to G'$ ein Gruppenhomomorphismus. Dann ist* $\operatorname{Kern}(\varphi)$ *ein Normalteiler in G.*

Beweis. Nach Bemerkung 1.1.20 ist $H := \operatorname{Kern}(\varphi)$ eine Untergruppe von G. Für jedes $h \in H$ und jedes $g \in G$ erhalten wir

$$\varphi(ghg^{-1}) \;=\; \varphi(g)\varphi(h)\varphi(g^{-1}) \;=\; \varphi(g)e_{G'}\varphi(g)^{-1} \;=\; e_{G'}.$$

Folglich gilt $ghg^{-1} \in H$ für alle $h \in H$ und $g \in G$. Wir schließen $gHg^{-1} = H$ für jedes $g \in G$. □

Satz 1.2.19. *Es sei $\varphi\colon G \to G'$ ein surjektiver Gruppenhomomorphismus. Mit $H := \mathrm{Kern}(\varphi)$ hat man einen Isomorphismus von Gruppen:*

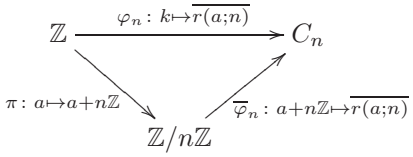
$$\overline{\varphi}\colon G/H \;\to\; G', \qquad gH \;\mapsto\; \varphi(g).$$

Beweis. Satz 1.2.17 garantiert zunächst, dass $\overline{\varphi}$ ein wohldefinierter Gruppenhomomorphismus ist. Weiter erhalten wir wegen $H = \mathrm{Kern}(\varphi)$ die Injektivität von $\overline{\varphi}$ und die Surjektivität von φ impliziert Surjektivität von $\overline{\varphi}$. □

Beispiel 1.2.20. Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann ist $n\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$. Die Elemente der Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ sind

$$0_{\mathbb{Z}/n\mathbb{Z}} \;=\; n\mathbb{Z}, \quad 1 + n\mathbb{Z}, \quad \ldots, \quad (n-1) + \mathbb{Z}.$$

Wir betrachten den Epimorphismus $\varphi_n\colon \mathbb{Z} \to C_n$, $a \mapsto \overline{r(a;n)}$. Nach dem Homomorphiesatz 1.2.17 gibt es ein kommutatives Diagramm



Wegen $\mathrm{Kern}(\varphi_n) = n\mathbb{Z}$ ist der induzierte Homomorphismus $\overline{\varphi}_n\colon \mathbb{Z}/n\mathbb{Z} \to C_n$ ein Isomorphismus. Es gilt also

$$C_n \;\cong\; \mathbb{Z}/n\mathbb{Z}.$$

Schreibweise 1.2.21. Es sei $n \in \mathbb{Z}_{\geq 1}$. Die Elemente der Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$ bezeichnet man häufig mit

$$\overline{a} \;:=\; a + n\mathbb{Z} \;\in\; \mathbb{Z}/n\mathbb{Z}.$$

Aufgaben zu Abschnitt 1.2.

Aufgabe 1.2.22. Bestimme sämtliche Untergruppen der Gruppen $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/4\mathbb{Z}$.

Aufgabe 1.2.23. Bestimme sämtliche Untergruppen, Normalteiler und Faktorgruppen der symmetrischen Gruppe S_3.

Aufgabe 1.2.24. Betrachte die Untergruppe $H := \{\overline{0}, \overline{2}, \overline{4}\}$ der Gruppe $\mathbb{Z}/6\mathbb{Z}$. Zeige: Es gilt $(\mathbb{Z}/6\mathbb{Z})/H \cong \mathbb{Z}/2\mathbb{Z}$.

Aufgabe 1.2.25. Es seien $m, l \in \mathbb{Z}_{\geq 1}$ und $n := ml$. Beweise die folgenden Aussagen.

(i) Man hat ein kommutatives Diagramm von Gruppenhomomorphismen

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\lambda\colon a \mapsto la} & \mathbb{Z} \\ {\scriptstyle \pi_m}\downarrow & & \downarrow{\scriptstyle \pi_n} \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow[\overline{a} \mapsto \overline{la}]{} & \mathbb{Z}/n\mathbb{Z} \end{array}$$

(ii) Für den Homomorphismus $\varphi := \pi_n \circ \lambda\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ gilt $\mathrm{Kern}(\varphi) = m\mathbb{Z}$.
(iii) $\overline{\varphi}\colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\overline{a} \mapsto \overline{la}$ definiert einen injektiven Homomorphismus.

Aufgabe 1.2.26. Es seien $m, l \in \mathbb{Z}_{\geq 1}$ und $n := ml$. Beweise die folgenden Aussagen.

(i) Man hat ein kommutatives Diagramm von Gruppenhomomorphismen

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{a \mapsto a} & \mathbb{Z} \\ {\scriptstyle \pi_n}\downarrow & & \downarrow{\scriptstyle \pi_m} \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow[\overline{a} \mapsto \overline{a}]{} & \mathbb{Z}/m\mathbb{Z} \end{array}$$

(ii) Der Homomorphismus $\varphi := \pi_m \circ \mathrm{id}_{\mathbb{Z}}$ ist surjektiv und es gilt $n\mathbb{Z} \subseteq \mathrm{Kern}(\varphi)$.
(iii) $\overline{\varphi}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $\overline{a} \mapsto \overline{a}$ definiert einen surjektiven Homomorphismus.

Aufgabe 1.2.27. Es seien G eine endliche Gruppe und $g \in G$.

(i) Es gilt $\mathrm{ord}(g) = \max(n \in \mathbb{Z}_{\geq} 1;\ g^n = e_G)$.
(ii) Es gilt $g^{|G|} = e_G$.

Aufgabe 1.2.28. Es sei G eine Gruppe. Zeige: Ist $|G|$ eine Primzahl, so gilt $G \cong \mathbb{Z}/p\mathbb{Z}$.

1.3. **Kommutative Ringe.**

Erinnerung 1.3.1. Ein *kommutativer Ring mit Eins*, im folgenden kurz *K1-Ring* genannt ist eine Menge R mit Verknüpfungen

$$\begin{aligned} \text{add}\colon R \times R \to R, &\qquad (a,b) \mapsto a+b, \\ \text{mult}\colon R \times R \to R, &\qquad (a,b) \mapsto ab \end{aligned}$$

(üblicherweise Addition und Multiplikation genannt), sodass folgende Bedingungen erfüllt sind:

(i) (R, add) ist eine abelsche Gruppe, d.h.,
- es gilt stets $a+(b+c)=(a+b)+c$,
- es gilt stets $a+b=b+a$,
- es gibt ein Element $0_R \in R$ mit $0_R + a = a$ für alle $a \in R$,
- zu jedem $a \in R$ gibt es ein Element $-a \in R$ mit $a+(-a)=0_R$.

(ii) (R, mult) ist ein abelsches Monoid, d.h.,
- es gilt stets $a(bc)=(ab)c$,
- es gilt stets $ab=ba$,
- es gibt ein Element $1_R \in R$ mit $1_R a = a$. für alle $a \in R$,

(iii) Es gilt $a(b+c)=ab+ac$ für alle $a,b,c \in R$.

Eine *Einheit* eines K1-Ringes R ist ein Element $a \in R$, sodass $ab = 1_R$ mit einem $b \in R$ gilt; in diesem Fall ist b eindeutig bestimmt und man schreibt $b = a^{-1}$. Die Menge aller Einheiten von R bezeichnet man mit R^*. Zusammen mit der Multiplikation bildet R^* eine abelsche Gruppe mit neutralem Element 1_R.

Einen K1-Ring nennt man *Integritätsring*, falls $1_R \neq 0_R$ gilt und $ab = 0_R$ stets $a = 0_R$ oder $b = 0_R$ impliziert. In Integritätsringen R hat man folgende *Kürzungsregel*: Es seien $a,b,c \in R$. Gilt $ab = ac$ und $a \neq 0$, so gilt $b = c$. Ein *Körper* ist ein K1-Ring $\mathbb{K}$ mit $1_\mathbb{K} \neq 0_\mathbb{K}$ und $\mathbb{K}^* = \mathbb{K} \setminus \{0_\mathbb{K}\}$.

Beispiel 1.3.2. Die ganzen Zahlen $\mathbb{Z}$ mit der üblichen Addition und Multiplikation bilden einen Integritätsring. Es gilt $\mathbb{Z}^* = \{\pm 1\}$.

Beispiel 1.3.3. Es sei $\mathbb{K}$ ein Körper. Ein *Polynom* über $\mathbb{K}$ in der Variablen T ist ein formaler Ausdruck

$$\sum_{\nu \in \mathbb{N}} a_\nu T^\nu, \qquad \text{wobei } a_\nu \neq 0_\mathbb{K} \text{ für nur endlich viele } \nu \in \mathbb{N}.$$

Auf der Menge $\mathbb{K}[T]$ aller Polynome über $\mathbb{K}$ in der Variablen T definiert man eine Addition und eine Multiplikation durch:

$$\begin{aligned} \left(\sum_{\nu\in\mathbb{N}} a_\nu T^\nu\right) + \left(\sum_{\nu\in\mathbb{N}} b_\nu T^\nu\right) &:= \sum_{\nu\in\mathbb{N}} (a_\nu + b_\nu) T^\nu, \\ \left(\sum_{\nu\in\mathbb{N}} a_\nu T^\nu\right) \cdot \left(\sum_{\nu\in\mathbb{N}} b_\nu T^\nu\right) &:= \sum_{\nu\in\mathbb{N}} c_\nu T^\nu, \qquad \text{wobei } c_\nu := \sum_{\nu=\mu+\kappa} a_\mu b_\kappa. \end{aligned}$$

Damit wird $\mathbb{K}[T]$ zu einem K1-Ring. Der *Grad* eines Polynoms $f = \sum_{\nu\in\mathbb{N}} a_\nu T^\nu$ ist definiert als

$$\deg(f) := \begin{cases} \max(\nu \in \mathbb{N};\ a_\nu \neq 0_\mathbb{K}) & \text{falls } f \neq 0_{\mathbb{K}[T]}, \\ -\infty & \text{falls } f = 0_{\mathbb{K}[T]}. \end{cases}$$

Gilt $\deg(\sum a_\nu T^\nu) = n \geq 0$, so nennt man $a_n \in \mathbb{K}^*$ den *Leitkoeffizienten* des Polynoms $\sum a_\nu T^\nu$. Für je zwei $f, g \in \mathbb{K}[T]$ gilt

$$\deg(f+g) \leq \max(\deg(f), \deg(g)), \qquad \deg(fg) = \deg(f) + \deg(g).$$

Damit sieht man, dass $\mathbb{K}[T]$ ein Integritätsring ist, und dass die Gruppe seiner Einheiten gegeben ist durch $\mathbb{K}[T]^* = \mathbb{K}^* T^0 = \mathbb{K}^*$.

Beispiel 1.3.4. Für $n \geq 1$ wird die Menge $C_n := \{\overline{0}, \ldots, \overline{n-1}\}$ zu einem K1-Ring durch

$$\overline{a} + \overline{b} \ := \overline{r(a+b;n)}, \qquad \overline{a} \cdot \overline{b} \ := \overline{r(ab;n)},$$

wobei $r(c;n) \in \{0, \ldots, n-1\}$ wie üblich den Rest von c modulo n bezeichnet, d.h., man hat $c = k(c;n)n + r(c;n)$. Die Einheitengruppe von C_n ist

$$C_n^* \quad = \quad \{\overline{a} \in C_n;\ \mathrm{ggT}(a,n) = 1\}.$$

Insbesondere ergibt sich daraus, dass C_n genau dann ein Körper ist, wenn n eine Primzahl ist.

Definition 1.3.5. Es seien R ein K1-Ring, und $S \subseteq R$ eine Teilmenge mit folgenden Eigenschaften:

$$0_R, 1_R \in S, \qquad a, b \in S \ \Rightarrow \ a \pm b \in S, \qquad a, b \in S \ \Rightarrow \ ab \in S.$$

Man nennt S zusammen mit den Verknüpfungen $(a,b) \mapsto a+b$ und $(a,b) \mapsto ab$ einen *Unterring* von R und bezeichnet das Paar $S \subseteq R$ auch als *Ringerweiterung*.

Bemerkung 1.3.6. Es sei R ein K1-Ring. Dann ist jeder Unterring $S \subseteq R$ wieder ein K1-Ring; für $a \in S$ erhält man das additive Inverse durch $-a = 0_R - a \in S$.

Beispiel 1.3.7. Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Unterring des Körpers $\mathbb{Q}$ der rationalen Zahlen. Insbesondere ist $\mathbb{Z} \subset \mathbb{Q}$ eine Ringerweiterung.

Bemerkung 1.3.8. Ist R ein Integritätsring, so ist auch jeder Unterring $S \subseteq R$ ein Integritätsring.

Konstruktion 1.3.9. Es seien R ein K1-Ring, $S \subseteq R$ ein Unterring und $A \subseteq R$ eine Teilmenge. Dann *erzeugt* A einen Unterring über S:

$$S[A] \quad := \quad \left\{ \sum_{i=1}^{n} s_{i1} \cdots s_{im_i},\ n \in \mathbb{Z}_{\geq 1},\ s_{ij} \ \in \ S \cup A \right\}$$

mit $S \cup A \subseteq S[A]$. Gilt $A = \{a_1, \ldots, a_r\}$ mit Ringelementen $a_1, \ldots, a_r \in R$, so schreibt man auch $S[a_1, \ldots, a_r]$ anstelle von $S[A]$.

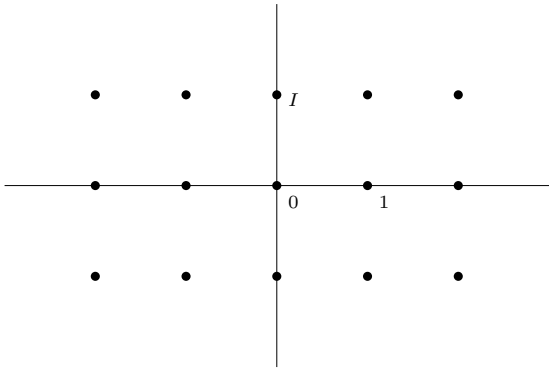
Beweis. Die Elemente aus $S[A]$ sind genau die möglichen Summen von Produkten aus Elementen von $S \cup A$ und bilden somit einen Unterring von R. □

Beispiel 1.3.10 (Ring der ganzen Gaußschen Zahlen)**.** Wir betrachten die Ringerweiterung $\mathbb{Z} \subset \mathbb{C}$ und die imaginäre Einheit $I \in \mathbb{C}$. Dann hat man

$$\mathbb{Z}[I] \quad = \quad \{m + nI;\ m, n \in \mathbb{Z}\},$$

denn die möglichen Produkte von Elementen aus $\mathbb{Z} \cup \{I\}$ sind alle von der Form m bzw. nI mit $m, n \in \mathbb{Z}$ und die möglichen Summen solcher Produkte sind daher von der Form $m + nI$ mit $m, n \in \mathbb{Z}$.

Man nennt $\mathbb{Z}[I]$ den Ring der *ganzen Gaußschen Zahlen*. Als Unterring des Integritätsringes $\mathbb{C}$ ist $\mathbb{Z}[I]$ ein Integritätsring.



Die Einheitengruppe $\mathbb{Z}[I]^*$ des Ringes $\mathbb{Z}[I]$ der ganzen Gaußschen Zahlen ist gegeben durch

$$\mathbb{Z}[I]^* \;=\; \{\pm 1, \pm I\}.$$

Es ist klar, das $\pm 1, \pm I$ Einheiten in $\mathbb{Z}[I]$ sind. Um zu sehen, dass es keine weiteren gibt, verwenden wir das Quadrat des komplexen Absolutbetrags

$$\delta\colon \mathbb{Z}[I] \;\to\; \mathbb{Z}_{\geq 0}, \qquad m + In \;\mapsto\; m^2 + n^2 = (m+nI)\overline{(m+nI)} = |m+nI|^2,$$

wobei $\overline{(m+nI)} = m - nI$. Für je zwei komplexe Zahlen $a, b \in \mathbb{C}$ gilt $ab\overline{ab} = a\overline{a}b\overline{b}$ und somit $|ab|^2 = |a|^2|b|^2$. Folglich leistet jede Einheit $m + nI \in \mathbb{Z}[I]$:

$$1 \;=\; |(m+nI)(m+nI)^{-1}|^2 \;=\; |(m+nI)|^2|(m+nI)^{-1}|^2 \;=\; (m^2+n^2)c$$

mit einem $c \in \mathbb{Z}_{\geq 0}$. Das impliziert bereits $m^2 + n^2 = 1$ und somit erhält man entweder $m = \pm 1$ und $n = 0$ oder $m = 0$ und $n = \pm 1$.

Definition 1.3.11. Ein *Homomorphismus* von K1-Ringen R und S ist eine Abbildung $\varphi\colon R \to S$ mit folgender Eigenschaft: Für alle $a, b \in R$ gilt:

$$\varphi(a+b) \;=\; \varphi(a) + \varphi(b), \qquad \varphi(ab) \;=\; \varphi(a)\varphi(b), \qquad \varphi(1_R) \;=\; 1_S.$$

Man nennt einen Homorphismus von K1-Ringen $\varphi\colon R \to S$ einen *Isomorphismus*, falls es einen Homomorphismus von K1-Ringen $\psi\colon S \to R$ gibt mit

$$\psi \circ \varphi \;=\; \mathrm{id}_R, \qquad\qquad \varphi \circ \psi \;=\; \mathrm{id}_S.$$

Weiter definiert man *Kern* und *Bild* eines Homomorphismus von K1-Ringen $\varphi\colon R \to S$ als

$$\mathrm{Kern}(\varphi) \;:=\; \{a \in R;\; \varphi(a) = 0_S\}, \qquad \mathrm{Bild}(\varphi) \;:=\; \{\varphi(a);\; a \in R\}.$$

Beispiel 1.3.12. Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann hat man einen surjektiven Homomorphismus von K1-Ringen

$$\pi\colon \mathbb{Z} \;\to\; C_n, \qquad a \;\mapsto\; \overline{r(a;n)};$$

dieser Homomorphismus besitzt $n\mathbb{Z} \subseteq \mathbb{Z}$ als Kern und C_n als Bild. Man beachte, dass $\mathrm{Kern}(\pi)$ für $n \geq 2$ kein Unterring von $\mathbb{Z}$ ist.

Satz 1.3.13. *Es sei $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen.*

(i) *Es gilt $\varphi(0_R) = 0_S$.*
(ii) *Ist $R' \subseteq R$ ein Unterring, so ist $\varphi(R') \subseteq S$ wieder ein Unterring. Insbesondere ist* $\mathrm{Bild}(\varphi)$ *ist ein Unterring von S.*
(iii) *Ist $S' \subseteq S$ ein Unterring, so ist das Urbild $\varphi^{-1}(S') \subseteq R$ wieder ein Unterring.*
(iv) *Der Homomorphismus $\varphi\colon R \to S$ ist genau dann injektiv, wenn* $\mathrm{Kern}(\varphi) = \{0_R\}$ *gilt.*
(v) *Der Homomorphismus $\varphi\colon R \to S$ ist genau dann ein Isomorphismus, wenn er bijektiv ist.*

Beweis. Aussage (i) folgt bereits aus der Tatsache, das $\varphi\colon R \to S$ ein Homomorphismus der zugrunde liegenden Gruppen $(R,+)$ und $(S,+)$ ist.

Zu (ii). Wegen $1_R \in R'$ und $\varphi(1_R) = 1_S$ haben wir $1_S \in \varphi(R')$. Zu $b_1, b_2 \in \varphi(R')$ wählen wir $a_i \in R'$ mit $\varphi(a_i) = b_i$ und erhalten

$$b_1 \pm b_2 \;=\; \varphi(a_1) \pm \varphi(a_2) \;=\; \varphi(a_1 \pm a_2) \;\in\; \varphi(R'),$$
$$b_1 b_2 \;=\; \varphi(a_1)\varphi(a_2) \;=\; \varphi(a_1 a_2) \;\in\; \varphi(R').$$

Zu (iii). Wegen $1_S \in S'$ und $\varphi(1_R) = 1_S$ erhalten wir $1_R \in \varphi^{-1}(S')$. Sind weiter $a_1, a_2 \in \varphi^{-1}(S)$ gegeben, so erhalten wir $a_1 \pm a_2, a_1 a_2 \in \varphi^{-1}(S')$ wegen

$$\varphi(a_1 \pm a_2) \;=\; \varphi(a_1) \pm \varphi(a_2) \;\in\; S', \qquad \varphi(a_1 a_2) \;=\; \varphi(a_1)\varphi(a_2) \;\in\; S'.$$

Aussage (iv) erhalten wir mit der entsprechenden Aussage 1.1.21 über Gruppenhomomorphismen.

Zu (iv). Es ist klar, dass die Existenz eines Umkehrhomomorphismus $\psi\colon S \to R$ die Bijektivität impliziert. Ist $\varphi\colon R \to S$ bijektiv, so liefert 1.1.15 einen Umkehrhomomorphismus $\psi\colon S \to R$ der zu Grunde liegenden additiven Gruppen. Es gilt

$$\psi(1_S) \;=\; \psi(\varphi(1_R)) \;=\; 1_R.$$

Wir müssen also nur noch zeigen, dass ψ mit der Multiplikation verträglich ist. Das geht wie im Beweis von 1.1.15: Für je zwei $b_1, b_2 \in S$ gilt

$$b_1 b_2 \;=\; \varphi(\psi(b_1))\varphi(\psi(b_2)) \;=\; \varphi(\psi(b_1)\psi(b_2)).$$

Wendet man nun ψ auf diese Gleichung an, so ergibt sich die gewünschte Homomorphieeigenschaft. □

Konstruktion 1.3.14. Es seien K1-Ringe $R_1, \ldots, R_s$ gegeben. Das *direkte Produkt* dieser Ringe ist $R_1 \times \ldots \times R_s$ zusammen mit den komponentenweisen Verknüpfungen

$$(a_1, \ldots, a_s) + (b_1, \ldots, b_s) \;:=\; (a_1 + b_1, \ldots, a_s + b_s),$$
$$(a_1, \ldots, a_s) \cdot (b_1, \ldots, b_s) \;:=\; (a_1 b_1, \ldots, a_s b_s).$$

Das direkte Produkt von $R_1, \ldots, R_s$ ist wieder ein K1-Ring; die neutrale Elemente sind gegeben durch

$$0_{R_1 \times \ldots \times R_s} \;=\; (0_{R_1}, \ldots, 0_{R_s}), \qquad 1_{R_1 \times \ldots \times R_s} \;=\; (1_{R_1}, \ldots, 1_{R_s}).$$

Weiter hat man für jeden Index $1 \le i \le n$ einen surjektiven Ringhomomorphismus

$$\pi_i\colon R_1 \times \ldots \times R_s \;\to\; R_i, \qquad (a_1, \ldots, a_s) \;\mapsto\; a_i.$$

Aufgaben zu Abschnitt 1.3.

Aufgabe 1.3.15. Es sei $\mathbb{K}$ ein Körper.

(i) Zeige: Jedes Polynom $f \in \mathbb{K}[T]$ mit $n := \deg(f) > -\infty$ besitzt höchstens n Nullstellen.
(ii) Zeige: Besitzt $\mathbb{K}$ unendlich viele Elemente, so gilt für je zwei $f, g \in \mathbb{K}[T]$:
$$f = g \iff f(a) = g(a) \text{ für jedes } a \in \mathbb{K}.$$
(iii) Gib ein Beispiel mit einem endlichen Körper $\mathbb{K}$, in welchem Aussage (ii) nicht erfüllt ist.

Aufgabe 1.3.16. Es sei R ein K1-Ring. Zeige:

(i) Ist S_i, $i \in I$, eine Familie von Unterringen $S_i \subseteq R$, so ist $\bigcap_{i\in I} S_i$ wieder ein Unterring in R
(ii) Ist $S \subseteq R$ ein Unterring und ist $A \subseteq R$ eine Teilmenge, so gilt
$$S[A] = \bigcap_{S'\subseteq R \text{ Unterring, } S\cup A\subseteq S'} S'.$$

Aufgabe 1.3.17. Es sei $p \in \mathbb{Z}_{\geq}1$ eine Primzahl. Zeige:

(i) Es gilt $(p-1)! \equiv -1 \mod p$. *Hinweis:* Betrachte das entsprechende Produkt in dem Körper C_p.
(ii) Gilt $p = 4m+1$ mit $m \in \mathbb{Z}_{\geq 0}$, so gibt es ein $c \in \mathbb{Z}$ mit $c^2 \equiv -1 \mod p$. *Hinweis:* Betrachte $c := (2m)!$.

Aufgabe 1.3.18. Es sei $d \in \mathbb{Z}$ quadratfrei, d.h., ohne Teiler der Form k^2 mit $k \in \mathbb{Z}_{\geq 2}$. Weiter bezeichne $\sqrt{d} \in \mathbb{R}_{\geq 0}$ wie üblich die Quadratwurzel, und für $d \in \mathbb{Z}_{<0}$ setzen wir $\sqrt{d} := I\sqrt{|d|} \in \mathbb{C}$. Zeige:
$$\mathbb{Z}[\sqrt{d}] = \{m + n\sqrt{d};\ m, n \in \mathbb{Z}\}.$$
Betrachte weiter die Abbildung $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}$, $m + n\sqrt{d} \mapsto m^2 - n^2 d$ und zeige:

(i) Für je zwei $a, b \in \mathbb{Z}[\sqrt{d}]$ gilt $N(ab) = N(a)N(b)$.
(ii) Es gilt $N(a) = 0 \iff a = 0$ für alle $a \in \mathbb{Z}[\sqrt{d}]$.
(iii) Die Einheitengruppe des Ringes $\mathbb{Z}[\sqrt{d}]$ ist $\mathbb{Z}[\sqrt{d}]^* = \{a \in \mathbb{Z}[\sqrt{d}];\ N(a) = \pm 1\}$.

1.4. **Ideale und Faktorringe.**

Definition 1.4.1. Es sei R ein K1-Ring. Eine nichtleere Teilmenge $\mathfrak{a} \subseteq R$ heißt *Ideal*, geschrieben $\mathfrak{a} \leq_R R$, falls sie folgende Eigenschaften besitzt:

(i) Für je zwei $a, a' \in \mathfrak{a}$ gilt $a + a' \in \mathfrak{a}$.
(ii) Für jedes $r \in R$ und jedes $a \in \mathfrak{a}$ gilt $ra \in \mathfrak{a}$.

Beispiel 1.4.2. Es sei R ein K1-Ring. Dann sind die Teilmengen $\{0_R\} \subseteq R$ und $R \subseteq R$ Ideale in R.

Beispiel 1.4.3. Die Menge $2\mathbb{Z} \subseteq \mathbb{Z}$ der geraden Zahlen ist ein Ideal im Ring $\mathbb{Z}$ der ganzen Zahlen. Allgemeiner gilt $n\mathbb{Z} \leq_{\mathbb{Z}} \mathbb{Z}$ für jedes $n \in \mathbb{Z}_{\geq 1}$. Für $n \geq 2$ ist $n\mathbb{Z} \leq_{\mathbb{Z}} \mathbb{Z}$ kein Unterring in $\mathbb{Z}$.

Satz 1.4.4. *Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal. Dann ist $\mathfrak{a}$ eine Untergruppe von $(R, +)$*

Beweis. Da $\mathfrak{a}$ nicht leer ist, gibt es ein $r \in \mathfrak{a}$. Damit erhalten wir $0_R = 0_r \cdot r \in \mathfrak{a}$. Nach Definition des Ideals gilt $a_1 + a_2 \in \mathfrak{a}$ für alle $a_1, a_2 \in \mathfrak{a}$. Ist weiter $a \in \mathfrak{a}$ gegeben, so haben wir $-a = (-1_r) \cdot a \in \mathfrak{a}$. □

Satz 1.4.5. *Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal. Dann sind folgende Aussagen äquivalent:*

(i) *Es gilt $\mathfrak{a} = R$.*
(ii) *Es gilt $\mathfrak{a} \cap R^* \neq \emptyset$.*

Beweis. Die Implikation "(i)⇒(ii)" ist klar, denn $1_R \in R = \mathfrak{a}$ impliziert $\mathfrak{a} \cap R^* \neq \emptyset$. Zu "(ii)⇒(i)". Ist $r \in R$ gegeben, so wählen wir ein $c \in \mathfrak{a} \cap R^*$ und erhalten $r = (rc^{-1})c \in \mathfrak{a}$. □

Folgerung 1.4.6. *Ein Ideal $\mathfrak{a} \leq_R R$ eines K1-Ringes R ist genau dann ein Unterring von R, wenn $\mathfrak{a} = R$ gilt.*

Konstruktion 1.4.7. Es sei R ein K1-Ring. Jede nichtlere Teilmenge $A \subseteq R$ *erzeugt* ein Ideal

$$\langle A \rangle \;:=\; \left\{ \sum_{i=1}^{n} r_i a_i;\; n \in \mathbb{Z}_{\geq 1},\; r_i \in R,\; a_i \in A \right\} \;\leq_R\; R$$

mit $A \subseteq \langle A \rangle$. Gilt $A = \{a_1, \ldots, a_n\}$, so schreibt man auch $\langle a_1, \ldots, a_n \rangle$ für $\langle A \rangle$. Der Vollständigkeit halber setzt man $\langle \emptyset \rangle := \{0_R\}$.

Das von einem einzigen Element $a \in R$ erzeugte Ideal, auch das von a erzeugte *Hauptideal* genannt, ist gegeben durch

$$\langle a \rangle \;=\; Ra \;=\; \{ra;\; r \in R\}.$$

Beweis. Wegen $A = 1_R \cdot A$ gilt $A \subseteq \langle A \rangle$; insbesondere haben wir $\langle A \rangle \neq \emptyset$. Weiter hat man

$$\Big(\sum r_i a_i\Big) + \Big(\sum r_j a_j\Big) \;\in\; \langle A \rangle, \qquad r \cdot \Big(\sum r_i a_i\Big) \;=\; \Big(\sum r r_i a_i\Big) \;\in\; \langle A \rangle$$

für je zwei $\sum r_i a_i$ und $\sum r_j a_j$ aus $\langle A \rangle$ sowie alle $r \in R$. Also ist $\langle A \rangle \subseteq R$ ein Ideal mit $A \subseteq \langle A \rangle$. □

Beispiel 1.4.8. Für das von den ganzen Zahlen 4 und 6 erzeugte Ideal $\langle 4,6\rangle \leq_{\mathbb{Z}} \mathbb{Z}$ haben wir

$$\langle 4,6\rangle \;=\; \langle 2\rangle \;=\; 2\mathbb{Z}.$$

Dabei gilt offensichtlich $\langle 4,6\rangle \subseteq 2\mathbb{Z}$. Umgekehrt erhält man $2 = 6 - 4 \in \langle 4,6\rangle$, was $2\mathbb{Z} \subseteq \langle 4,6\rangle$ impliziert.

Konstruktion 1.4.9. Es seien R ein K1-Ring und $\mathfrak{a}_i$, $i \in I$, eine Familie von Idealen. Dann erhält man neue Ideale in R:

(i) Den *Durchschnitt* der Ideale $\mathfrak{a}_i$:

$$\bigcap_{i\in I} \mathfrak{a}_i \quad \leq_R \quad R,$$

(ii) Die *Summe* der Ideale $\mathfrak{a}_i$:

$$\sum_{i\in I} \mathfrak{a}_i \quad := \quad \left\{ \sum_{j\in J} a_j;\ J \subseteq I \text{ endlich},\ a_j \in \mathfrak{a}_j \right\} \quad \leq_R \quad R.$$

(iii) Falls I endlich ist, das *Produkt* der Ideale $\mathfrak{a}_i$:

$$\prod_{i\in I} \mathfrak{a}_i \quad := \quad \left\langle \prod_{i\in I} a_i;\ a_i \in \mathfrak{a}_i \right\rangle \quad \leq_R \quad R.$$

Bemerkung 1.4.10. Es seien R ein K1-Ring und $\mathfrak{a}_i$, $i \in I$, eine (erforderlichenfalls endliche) Familie von Idealen in R. Dann gilt

$$\sum_{i\in I} \mathfrak{a}_i \;=\; \left\langle \bigcup_{i\in I} \mathfrak{a}_i \right\rangle, \qquad \prod_{i\in I} \mathfrak{a}_i \;\subseteq\; \bigcap_{i\in I} \mathfrak{a}_i.$$

Beispiel 1.4.11. Für die von den ganzen Zahlen 4 bzw. 6 erzeugten Ideale $\langle 4\rangle$ bzw. $\langle 6\rangle$ in $\mathbb{Z}$ haben wir

$$\langle 4\rangle + \langle 6\rangle \;=\; \langle 4,6\rangle \;=\; \langle 2\rangle, \qquad \langle 4\rangle\langle 6\rangle \;=\; \langle 24\rangle \;\subsetneq\; \langle 12\rangle \;=\; \langle 4\rangle \cap \langle 6\rangle$$

Man beachte dabei, dass $\langle 4\rangle + \langle 6\rangle$ von $2 = \mathrm{ggT}(4,6)$ erzeugt wird und $\langle 4\rangle \cap \langle 6\rangle$ von $12 = \mathrm{kgV}(4,6)$

Satz 1.4.12. *Es sei $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen.*

(i) *Ist $\mathfrak{b} \subseteq S$ ein Ideal, so ist das Urbild $\varphi^{-1}(\mathfrak{b})$ ein Ideal in R; insbesondere ist $\mathrm{Kern}(\varphi) = \varphi^{-1}(0)$ ein Ideal in R.*

(ii) *Ist $\mathfrak{a} \subseteq R$ ein Ideal und ist $\varphi\colon R \to S$ surjektiv, so ist das Bild $\varphi(\mathfrak{a})$ ein Ideal in S.*

Beweis. Zu (i). Aus $\varphi(0_R) = 0_S \in \mathfrak{b}$ folgt $0_R \in \varphi^{-1}(\mathfrak{b})$ und somit $\varphi^{-1}(\mathfrak{b}) \neq \emptyset$. Sind $a_1, a_2 \in \varphi^{-1}(\mathfrak{b})$ und $r \in R$ gegeben, so erhalten wir $a_1 + a_2 \in \varphi^{-1}(\mathfrak{b})$ und $ra_1 \in \varphi^{-1}(\mathfrak{b})$ mit

$$\varphi(a_1 + a_2) \;=\; \varphi(a_1) + \varphi(a_2) \;\in\; \mathfrak{b}, \qquad \varphi(ra_1) \;=\; \varphi(r)\varphi(a_1) \;\in\; \mathfrak{b}.$$

Zu (ii). Wegen $\mathfrak{a} \neq \emptyset$ gilt auch $\mathfrak{b} \neq \emptyset$. Es seien $b_1, b_2 \in \varphi(\mathfrak{a})$ und $s \in S$ gegeben. Wir wählen $a_1, a_2 \in \mathfrak{a}$ mit $\varphi(a_i) = b_i$ und $r \in R$ mit $\varphi(r) = s$. Dann erhalten wir

$$b_1 + b_2 \;=\; \varphi(a_1) + \varphi(a_2) \;=\; \varphi(a_1 + a_2) \;\in\; \varphi(\mathfrak{a}),$$
$$sb_1 \;=\; \varphi(r)\varphi(a_1) \;=\; \varphi(ra_1) \;\in\; \varphi(\mathfrak{a}).$$

□

Beispiel 1.4.13. Die Inklusionsabbildung $\varphi\colon \mathbb{Z}\ to\mathbb{Q}$ ist ein Homomorphismus von K1-Ringen. Für $\mathbb{Z} \leq_{\mathbb{Z}} \mathbb{Z}$ ist das Bild $\varphi(\mathbb{Z}) = \mathbb{Z}$ kein Ideal in $\mathbb{Q}$.

Konstruktion 1.4.14 (Faktorring)**.** Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal. Wir betrachten die (additive) Faktorgruppe

$$R/\mathfrak{a} \quad := \quad \{r + \mathfrak{a};\ r \in R\}$$

und definieren eine Multiplikation auf $R/\mathfrak{a}$, indem wir für zwei Äquivalenzklassen $r + \mathfrak{a}$ und $s + \mathfrak{a}$ setzen:

$$(r + \mathfrak{a})(s + \mathfrak{a}) \quad := \quad rs + \mathfrak{a}.$$

Damit wird $R/\mathfrak{a}$ zu einem K1-Ring, dem *Faktorring* von R nach $\mathfrak{a}$. Die neutralen Elemente bezüglich Addition und Multiplikation in $R/\mathfrak{a}$ sind

$$0_R + \mathfrak{a} \ \in \ R/\mathfrak{a}, \qquad 1_R + \mathfrak{a} \ \in \ R/\mathfrak{a}.$$

Weiter hat man einen surjektiven Homomorphismus $\pi\colon R \to R\mathfrak{a}$ mit $\mathrm{Kern}(\pi) = \mathfrak{a}$, nämlich

$$\pi\colon R \ \to \ R/\mathfrak{a}, \qquad r \ \mapsto \ r + \mathfrak{a}.$$

Beweis. Wir zeigen zunächst, dass die Multiplikation in $R/\mathfrak{a}$ wohldefiniert ist. Dazu betrachten wir $r, r' \in R$ und $s, s' \in R$ mit

$$r + \mathfrak{a} \ = \ r' + \mathfrak{a}, \qquad s + \mathfrak{a} \ = \ s' + \mathfrak{a}.$$

Wir müssen zeigen, dass $rs + \mathfrak{a}$ und $r's' + \mathfrak{a}$ übereinstimmen. Es gilt $r - r' \in \mathfrak{a}$ und $s - s' \in \mathfrak{a}$. Weiter erhalten wir

$$\begin{aligned} rs &= (r' + (r - r'))(s' + (s - s')) \\ &= r's' + r'(s - s') + s'(r - r') + (r - r')(s - s'). \end{aligned}$$

Die letzten drei Summanden liegen alle im Ideal $\mathfrak{a}$. Es folgt $rs - r's' \in \mathfrak{a}$ und somit $rs + \mathfrak{a} = r's' + \mathfrak{a}$.

Die Axiome 1.3.1 (ii) ergeben sich direkt aus den entsprechenden Eigenschaften von R: Es gilt stets

$$\begin{aligned} ((r + \mathfrak{a})(r' + \mathfrak{a}))(r'' + \mathfrak{a}) &= ((r + r') + \mathfrak{a})(r'' + \mathfrak{a}) \\ &= ((rr')r'') + \mathfrak{a} \\ &= ((r(r'r'')) + \mathfrak{a} \\ &= (r + \mathfrak{a})((r' + r'') + \mathfrak{a}) \\ &= (r + \mathfrak{a})((r' + \mathfrak{a})(r'' + \mathfrak{a})). \end{aligned}$$

Es ist klar, dass $1_R + \mathfrak{a} \in R/\mathfrak{a}$ neutrales Element der Multiplikation ist. Weiter hat man stets

$$\begin{aligned} (r + \mathfrak{a})(r' + \mathfrak{a}) &= (rr') + \mathfrak{a} \\ &= (r'r) + \mathfrak{a} \\ &= (r' + \mathfrak{a})(r + \mathfrak{a}). \end{aligned}$$

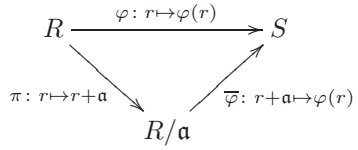
Ebenso erhält man das Axiom 1.3.1 (iii) direkt aus der entsprechenden Eigenschaft von R: Es gilt stets

$$\begin{aligned} (s + \mathfrak{a})((r' + \mathfrak{a}) + (r'' + \mathfrak{a})) &= (s + \mathfrak{a})((r' + r'') + \mathfrak{a}) \\ &= (s(r + r')) + \mathfrak{a} \\ &= (sr + sr') + \mathfrak{a} \\ &= (sr + \mathfrak{a}) + (sr' + \mathfrak{a}) \\ &= (s + \mathfrak{a})(r + \mathfrak{a}) + (s + \mathfrak{a})(r' + \mathfrak{a}). \end{aligned}$$

□

Beispiel 1.4.15. Für jedes $n \in \mathbb{Z}$ hat man ein Ideal $n\mathbb{Z} \leq_{\mathbb{Z}} \mathbb{Z}$ und einen zugehörigen Faktorring $\mathbb{Z}/n\mathbb{Z}$.

Satz 1.4.16 (Homomorphiesatz)**.** *Es sei $\varphi\colon R \to S$ ein Homomorphismus von K1-Ringen, und es sei $\mathfrak{a} \leq_R R$ ein Ideal mit $\mathfrak{a} \subseteq \mathrm{Kern}(\varphi)$. Dann gibt es ein kommutatives Diagramm*



von wohldefinierten Homomorphismen zwischen K1-Ringen. Dabei ist der Homomorphismus $\overline{\varphi}\colon R/\mathfrak{a} \to S$ durch $\varphi\colon R \to S$ und das obige Diagramm eindeutig bestimmt. Es gilt weiter

(i) *$\overline{\varphi}$ ist injektiv $\Leftrightarrow$ $\mathfrak{a} = \mathrm{Kern}(\varphi)$;*
(ii) *$\overline{\varphi}$ ist surjektiv $\Leftrightarrow$ φ ist surjektiv.*

Beweis. Da φ und π Homomorphismen der zu Grunde liegenden additiven (abelschen) Gruppen sind, besagt der Homomorphiesatz 1.2.17, dass

$$\overline{\varphi}\colon R/\mathfrak{a} \;\to\; S, \qquad r+\mathfrak{a} \;\mapsto\; \varphi(r)$$

ein (wohldefinierter) Gruppenhomomorphismus mit den entsprechenden Eigenschaften ist. Die noch fehlenden Eigenschaften eines Ringhomomorphismus lassen sich leicht nachweisen:

$$\overline{\varphi}(1_{R/\mathfrak{a}}) \;=\; \varphi(1_R) \;=\; 1_S.$$
$$\overline{\varphi}((r+\mathfrak{a})(r'+\mathfrak{a})) \;=\; \overline{\varphi}(rr'+\mathfrak{a}) \;=\; \varphi(rr') \;=\; \varphi(r)\varphi(r') \;=\; \overline{\varphi}(r+\mathfrak{a})\overline{\varphi}(r'+\mathfrak{a}).$$

□

Folgerung 1.4.17. *Es sei $\varphi\colon R \to S$ ein surjektiver Homomorphismus von K1-Ringen. Dann hat man einen Isomorphismus von K1-Ringen*

$$\overline{\varphi}\colon R/\mathrm{Kern}(\varphi) \;\to\; S, \qquad r+\mathrm{Kern}(\varphi) \;\mapsto \varphi(r).$$

Folgerung 1.4.18. *Es sei $n \in \mathbb{Z}_{\geq 1}$. Dann hat man einen kanonischen Isomorphismus von K1-Ringen:*

$$\mathbb{Z}/n\mathbb{Z} \;\to\; C_n, \qquad a+n\mathbb{Z} \;\mapsto\; \overline{r(a;n)}.$$

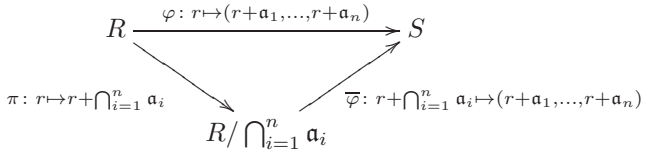
Satz 1.4.19 (Chinesischer Restsatz)**.** *Es sei R ein K1-Ring, und es seien $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Ideale in R mit $\mathfrak{a}_i + \mathfrak{a}_j = R$ für alle i, j mit $i \neq j$. Dann hat man einen Isomorphimus*

$$R\Big/\bigcap_{i=1}^{n} \mathfrak{a}_i \quad\to\quad R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n,$$
$$r+\bigcap_{i=1}^{n} \mathfrak{a}_i \quad\mapsto\quad (r+\mathfrak{a}_1, \ldots, r+\mathfrak{a}_n).$$

Beweis. Man hat einen kanonischen Homomorphismus von R auf das direkte Produkt der Faktorringe $R/\mathfrak{a}_i$:

$$\varphi\colon R \;\to\; R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n, \qquad r \;\mapsto\; (r+\mathfrak{a}_1, \ldots, r+\mathfrak{a}_n).$$

Der Kern dieses Homomorphismus ist gegeben durch $\mathrm{Kern}(\varphi) = \bigcap_{i=1}^{n} \mathfrak{a}_i$. Der Homomorphiesatz 1.4.16 liefert daher ein kommutatives Diagramm



Nach 1.4.17 ist nur noch die Surjektivität von φ nachzuweisen. Dafür wählen wir zu jedem $j \neq i$ Elemente $a_j \in \mathfrak{a}_i$ und $b_j \in \mathfrak{a}_j$ mit $a_j + b_j = 1$. Damit erhalten wir

$$\begin{aligned} 1_R &= \prod_{j \neq i} (a_j + b_j) \\ &\in \mathfrak{a}_i + \prod_{j \neq i} b_j \\ &\subseteq \mathfrak{a}_i + \bigcap_{j \neq i} \mathfrak{a}_j. \end{aligned}$$

Das liefert uns für jedes i Elemente $c_i \in \mathfrak{a}_i$ und $d_i \in \bigcap_{j \neq i} \mathfrak{a}_j$ mit $c_i + d_i = 1_R$. Damit ergibt sich

$$\varphi(d_i) = (0_{R/\mathfrak{a}_1}, \ldots, 0_{R/\mathfrak{a}_{i-1}}, 1_{R/\mathfrak{a}_i}, 0_{R/\mathfrak{a}_{i+1}}, \ldots, 0_{R/\mathfrak{a}_n}).$$

Damit sehen wir, dass jedes Element $(r_1 + \mathfrak{a}_1, \ldots, r_n + \mathfrak{a}_n) \in R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_n$ im Bild von φ liegt: Es gilt

$$(r_1 + \mathfrak{a}_1, \ldots, r_n + \mathfrak{a}_n) = \varphi(r_1 d_1 + \ldots + r_n d_n).$$

□

Aufgaben zu Abschnitt 1.4.

Aufgabe 1.4.20. Es sei R ein K1-Ring. Zeige: R ist genau dann ein Körper, wenn $\{0_R\} \leq_R R$ und $R \leq_R R$ die einzigen Ideale in R sind.

Aufgabe 1.4.21. Zeige, dass die Ringe $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ keine Integritätsringe sind. Zeige weiter, dass sie nicht isomorph zueinander sind.

Aufgabe 1.4.22. Es seien R ein K1-Ring und $A \subseteq R$ eine Teilmenge. Zeige: Es gilt

$$\langle A \rangle \quad = \quad \bigcap_{A \subseteq \mathfrak{a} \leq_R R} \mathfrak{a}.$$

Aufgabe 1.4.23. Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal in R. Das *Radikal* von $\mathfrak{a}$ ist definiert als

$$\sqrt{\mathfrak{a}} \quad := \quad \{b \in R;\, b^n \in \mathfrak{a} \text{ für ein } n \in \mathbb{Z}_{\geq 0}\}.$$

Zeige: Das Radikal $\sqrt{\mathfrak{a}} \subseteq R$ ist wieder ein Ideal in R. *Hinweis:* Verwende den binomischen Lehrsatz.

Aufgabe 1.4.24. Es seien $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ Ideale in einem K1-Ring R. Zeige:

(i) $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$,
(ii) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supseteq (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})$; Gleichheit gilt, falls $\mathfrak{b} \subseteq \mathfrak{a}$ oder $\mathfrak{c} \subseteq \mathfrak{a}$ gilt,
(iii) $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b}$.

Aufgabe 1.4.25 (Erster Isomorphiesatz für Ringe)**.** Es seien R ein K1-Ring, $S \subseteq R$ ein Unterring und $\mathfrak{a} \leq_R R$ ein Ideal. Zeige: $S \cap \mathfrak{a}$ ist ein Ideal in S, und es gilt

$$(S + \mathfrak{a})/\mathfrak{a} \quad \cong \quad S/(S \cap \mathfrak{a}).$$

Aufgabe 1.4.26 (Zweiter Isomorphiesatz für Ringe)**.** Es seien R ein K1-Ring, und $\mathfrak{a}, \mathfrak{b} \leq_R R$ Ideale mit $\mathfrak{a} \subseteq \mathfrak{b}$. Zeige: $\mathfrak{b}/\mathfrak{a}$ ist ein Ideal in $R/\mathfrak{a}$, und es gilt

$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \quad \cong \quad R/\mathfrak{b}.$$

Aufgabe 1.4.27. Für $n \in \mathbb{Z}_{\geq 1}$ bezeichne $\varphi(n)$ die Anzahl aller ganzen Zahlen a mit $1 \leq a \leq n$ und $\mathrm{ggT}(a, n) = 1$. Zeige: Für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ gilt $a^{\varphi(n)} \equiv 1 \mod n$. *Hinweis*: Verwende Aufgabe 1.2.27 und Beispiel 1.3.4.

2. Teilbarkeitstheorie

2.1. **Teilbarkeit in Integritätsringen.**

Definition 2.1.1. Es seien R ein Integritätsring und $a, b \in R$. Man sagt *a ist ein Teiler von b*, auch *a teilt b*, geschrieben $a \mid b$, falls es ein $r \in R$ gibt mit $b = ra$.

Bemerkung 2.1.2. Es seien R ein Integritätsring und $a \in R$. Dann gilt $a \mid a$ sowie $a \mid 0_R$ und weiter $c \mid a$ für jedes $c \in R^*$, denn man hat

$$a \;=\; 1_R a, \qquad 0_R \;=\; 0_R a, \qquad a \;=\; (ac^{-1})c.$$

Beispiel 2.1.3. Die Teiler von 12 im Ring $\mathbb{Z}$ der ganzen Zahlen sind ± 1, ± 2, ± 3, ± 4, ± 6 und ± 12.

Beispiel 2.1.4. Die Teiler des Polynoms $f := T^2 - 1 \in \mathbb{Q}[T]$ sind genau die Polynome

$$a, \quad b(T-1), \quad c(T+1), \quad d(T^2-1), \qquad \text{wobei } a, b, c, d \in \mathbb{Q}^*.$$

Dazu beachte man, dass $f = gh$ nur für $\deg(g) + \deg(h) = 2$ möglich ist. Die darin enthaltenen Fälle lassen sich dann schnell durchspielen.

Satz 2.1.5. *Es sei R ein Integritätsring, und es seien $a, b \in R$. Dann gilt:*

$$a \mid b \iff b \in \langle a \rangle \iff \langle b \rangle \subseteq \langle a \rangle.$$

Weiter gilt:

$$a \mid b \text{ und } b \mid a \iff \langle a \rangle = \langle b \rangle \iff b = ca \text{ mit einem } c \in R^*.$$

Beweis. Die erste Reihe von Äquivalenzen folgt sofort aus der Definition von $a \mid b$ und $\langle a \rangle = Ra$. In der zweiten Reihe ist lediglich zur Implikation "$\Rightarrow$" der letzten Äquivalenz etwas zu vermerken: Aus $a \in \langle b \rangle$ schliessen wir $a = rb$ mit einem $r \in R$. Aus $b \in \langle a \rangle$ schliessen wir $b = r'a$ mit einem $r' \in R$. Es folgt $a = rb = rr'a$. Da R Integritätsring ist, erhalten wir $rr' = 1_R$ und somit $r' \in R^*$. □

Definition 2.1.6. Es sei R ein Integritätsring. Wir nennen zwei Elemente $a, b \in R$ *assoziiert zueinander*, in Zeichen $a \sim b$, falls $b = ca$ mit einer Einheit $c \in R^*$ gilt.

Beispiel 2.1.7. In dem Ring $\mathbb{Z}$ der ganzen Zahlen gilt genau dann $m \sim n$, wenn man $m = \pm n$ hat.

Beispiel 2.1.8. Es sei $\mathbb{K}$ ein Körper. Zwei Polynome $f, g \in \mathbb{K}[T]$ sind genau dann assoziiert zueinander, wenn $g = af$ mit einem $a \in \mathbb{K}^*$ gilt.

Satz 2.1.9. *Es sei R ein Integritätsring.*

(i) *Durch "$a \sim b$", d.h., a assoziiert zu b, wird eine Äquivalenzrelation auf R definiert.*
(ii) *Für je zwei Elemente $a, b \in R$ gilt $a \sim b$ genau dann, wenn man $a \mid b$ und $b \mid a$ hat.*
(iii) *Gilt $a \sim b$ für zwei $a, b \in R$, so haben a und b dasselbe Teilbarkeitsverhalten, d.h., für jedes $r \in R$ gilt*

$$a \mid r \iff b \mid r, \qquad r \mid a \iff r \mid b.$$

Sind umgekehrt $a, b \in R$ zwei Elemente in R, die dasselbe Teilbarkeitsverhalten in obigem Sinne aufweisen, so gilt $a \sim b$.

Beweis. Aussage (ii) ist bereits in Satz 2.1.5 bewiesen worden. Zu (i). Die Reflexivität von "$\sim$" ist klar mit $a = 1_R a$. Zur Symmetrie: Gilt $b = ca$ mit $c \in R^*$, so gilt $a = c^{-1}b$. Zur Transitivität: Gelten $b = ca$ und $d = c'b$ mit $c, c' \in R^*$, so hat man $d = c'ca$ und $cc' \in R^*$.

Zu (iii). Sind a und b assoziiert zueinander, etwa $b = ca$ mit $c \in R^*$, so hat man für jedes $r \in R$:

$$a \mid r \iff r = r'a \iff r = r'c^{-1}b \iff b \mid r,$$
$$r \mid a \iff a = a'r \iff b = ca'r \iff r \mid b.$$

Weisen umgekehrt a und b dasselbe Teilbarkeitsverhalten auf, so erhalten wir $a \mid b$ und $b \mid a$ aus $a \mid a$. Satz 2.1.5 liefert dann $a \sim b$. □

Definition 2.1.10. Es seien R ein Integritätsring und $a_1, \ldots, a_n \in R$.

(i) Ein *größter gemeinsamer Teiler* von $a_1, \ldots, a_n$ ist ein $a \in R$ mit
- $a \mid a_i$ für $i = 1, \ldots, n$;
- $a' \mid a_i$ für $i = 1, \ldots, n \Rightarrow a' \mid a$.

(ii) Die Menge aller größten gemeinsamen Teiler von $a_1, \ldots, a_n$ bezeichnen wir mit $\mathrm{ggT}(a_1, \ldots, a_n)$.

(iii) Die Elemente $a_1, \ldots, a_n \in R$ heißen *teilerfremd*, falls $1_R \in \mathrm{ggT}(a_1, \ldots, a_n)$ gilt.

(iv) Ein *kleinstes gemeinsames Vielfaches* von $a_1, \ldots, a_n$ ist ein $b \in R$ mit
- $a_i \mid b$ für $i = 1, \ldots, n$;
- $a_i \mid b'$ für $i = 1, \ldots, n \Rightarrow b \mid b'$.

(v) Die Menge aller kleinsten gemeinsamen Vielfachen von $a_1, \ldots, a_n$ bezeichnen wir mit $\mathrm{kgV}(a_1, \ldots, a_n)$.

Beispiel 2.1.11. In dem Ring $\mathbb{Z}$ der ganzen Zahlen gilt $\mathrm{ggT}(12, 18) = \{\pm 6\}$ und $\mathrm{kgV}(12, 18) = \{\pm 36\}$.

Bemerkung 2.1.12. Es seien R ein Integritätsring und $a_1, \ldots, a_n \in R$.

(i) Es sei $a \in \mathrm{ggT}(a_1, \ldots, a_n)$. Dann gilt $a' \sim a$ für jedes $a' \in \mathrm{ggT}(a_1, \ldots, a_n)$. Umgekehrt gilt $a' \in \mathrm{ggT}(a_1, \ldots, a_n)$ für jedes $a' \in R$ mit $a' \sim a$.

(ii) Es sei $b \in \mathrm{kgV}(a_1, \ldots, a_n)$. Dann gilt $b' \sim b$ für jedes $b' \in \mathrm{kgV}(a_1, \ldots, a_n)$. Umgekehrt gilt $b' \in \mathrm{kgV}(a_1, \ldots, a_n)$ für jedes $b' \in R$ mit $b' \sim b$.

Definition 2.1.13. Ein *Hauptidealring* ist ein Integritätsring R, sodass jedes Ideal $\mathfrak{a} \leq_R R$ ein Hauptideal ist, d.h., von der Form $\mathfrak{a} = \langle a \rangle = Ra$ mit einem $a \in R$.

Satz 2.1.14. *Es sei R ein Hauptidealring, und es seien $a_1, \ldots, a_n \in R$. Für jedes $a \in R$ gilt:*

$$a \in \mathrm{ggT}(a_1, \ldots, a_n) \iff \langle a \rangle = \langle a_1, \ldots, a_n \rangle,$$
$$a \in \mathrm{kgV}(a_1, \ldots, a_n) \iff \langle a \rangle = \langle a_1 \rangle \cap \ldots \cap \langle a_n \rangle.$$

Insbesondere gibt es stets größte gemeinsame Teiler und kleinste gemeinsame Vielfache für $a_1, \ldots, a_n$.

Beweis. Es sei zunächst $a \in \mathrm{ggT}(a_1, \ldots, a_n)$. Dann gilt $a \mid a_i$ und somit $a_i \in \langle a \rangle$. Es folgt $\langle a_1, \ldots, a_n \rangle \subseteq \langle a \rangle$. Da R Hauptidealring ist, gilt weiter $\langle a_1, \ldots, a_n \rangle = \langle b \rangle$ mit einem $b \in R$. Das impliziert $a_i \in \langle b \rangle$ und somit $b \mid a_i$. Wegen $a \in \mathrm{ggT}(a_1, \ldots, a_n)$ erhalten wir $b \mid a$ und somit $\langle a \rangle \subseteq \langle b \rangle = \langle a_1, \ldots, a_n \rangle$.

Es sei nun $\langle a \rangle = \langle a_1, \ldots, a_n \rangle$. Dann gilt $a_i \in \langle a \rangle$ und somit $a \mid a_i$. Ist $a' \in R$ ein weiterer gemeinsamer Teiler von $a_1, \ldots, a_n$, so folgt $a_i \in \langle a' \rangle$. Das impliziert $\langle a_1, \ldots, a_n \rangle \subseteq \langle a' \rangle$, und wir erhalten $a \in \langle a' \rangle$. Folglich gilt $a' \mid a$. Wir haben also $a \in \mathrm{ggT}(a_1, \ldots, a_n)$ nachgewiesen.

Die Aussage über die kleinsten gemeinsamen Vielfachen läßt sich mit ähnlichen Argumenten beweisen — die Ausführung wird als Übungsaufgabe gestellt. □

Folgerung 2.1.15. *Es seien R ein Hauptidealring und $a_1, \ldots, a_n \in R$. Die Elemente $a_1, \ldots, a_n$ sind genau dann teilerfremd, wenn man $1_R \in R$ als "Linearkombination" aus ihnen erhält:*

$$1_R \;=\; r_1 a_1 + \ldots + r_n a_n \quad \textit{mit } r_i \in R.$$

Definition 2.1.16. Es sei R ein Integritätsring.

(i) Ein Element $q \in R$ heißt *irreduzibel*, falls gilt:
- $q \neq 0_R$ und $q \notin R^*$,
- $q = ab$ mit $a, b \in R$ impliziert stets $a \in R^*$ oder $b \in R^*$.

(ii) Ein Element $p \in R$ heißt *prim*, falls gilt:
- $p \neq 0_R$ und $p \notin R^*$,
- $p \mid ab$ mit $a, b \in R$ impliziert stets $p \mid a$ oder $p \mid b$.

Bemerkung 2.1.17. Ein Element $0_R \neq q \in R \setminus R^*$ eines Integritätsringes R ist genau dann irreduzibel, wenn es keine "echten" Teiler besitzt, d.h., wenn $a \mid q$ stets $a \in R^*$ oder $a \sim q$ impliziert.

Beispiel 2.1.18. Eine Zahl $p \in \mathbb{Z}_{\geq 1}$ nennt man bekanntlich Primzahl, falls 1 und p die einzigen Teiler von p sind. Nach Bemerkung 2.1.17 sind Primzahlen irreduzible Elemente in $\mathbb{Z}$.

Beispiel 2.1.19. Es sei $\mathbb{K}$ ein Körper. Dann besteht $\mathbb{K}[T]^* = \mathbb{K}^*$ genau aus den Elementen vom Grad Null. Ein Polynom $f \in \mathbb{K}[T]$ vom Grad 1 ist hingegen irreduzibel: Es ist offensichtlich keine Einheit, und für jede Zerlegung $f = gh$ in $\mathbb{K}[T]$ muss entweder g oder h aus Gradgründen eine Einheit sein.

Satz 2.1.20. *Es sei R ein Integritätsring. Dann ist jedes Primelement $p \in R$ irreduzibel.*

Beweis. Wir müssen nur die zweite Bedingung der Irreduzibilität nachprüfen. Dazu sei $p = ab$ mit $a, b \in R$. Da p prim ist, gilt $p \mid a$ oder $p \mid b$. Wir dürfen $p \mid a$ annehmen. Dann haben wir $a = rp$ mit einem $r \in R$. Folglich erhalten wir $p = ab = rpb$. Da $p \neq 0$ gilt und R ein Integritätsring ist, folgt $rb = 1$, d.h., b ist eine Einheit. □

Satz 2.1.21. *Es sei R ein Hauptidealring, und es sei $q \in R$. Dann sind folgende Aussagen äquivalent.*

(i) *q ist prim.*
(ii) *q ist irreduzibel.*

Beweis. Die Implikation "(i)⇒(ii)" ist Satz 2.1.20. Zur Implikation "(ii)⇒(i)". Wir zeigen zunächst, dass für jedes Ideal $\mathfrak{a} \leq_R R$ gilt

$$\langle q \rangle \;\subsetneq\; \mathfrak{a} \quad\Longrightarrow\quad \mathfrak{a} \;=\; R.$$

Da R Hauptidealring ist, gilt $\mathfrak{a} = \langle a \rangle$ mit einem $a \in R$. Also haben wir $\langle q \rangle \subsetneq \langle a \rangle$ und somit $q = ab$ mit einem $b \in R$, wobei b keine Einheit sein kann. Da q irreduzibel ist, muss a eine Einheit sein. Das impliziert $\mathfrak{a} = R$.

Wir müssen zeigen, dass aus $q \mid ab$ bereits $q \mid a$ oder $q \mid b$ folgt. Nehmen wir an, dass $q \nmid a$ und $q \nmid b$ gelten. Dann gilt $a \notin \langle q \rangle$ und $b \notin \langle q \rangle$. Die Vorüberlegung liefert

$$\langle q \rangle \;\subsetneq\; \langle a, q \rangle \;=\; R \;=\; \langle b, q \rangle \;\supsetneq\; \langle q \rangle.$$

Es folgt

$$R \;=\; \langle a, q \rangle \langle b, q \rangle \;=\; \langle ab, aq, bq, q^2 \rangle \;\subseteq\; \langle q \rangle.$$

Wobei die letzte Inklusion auf $q \mid ab$ zurückgeht. Es folgt $\langle q \rangle = R$. Insbesondere ergibt sich $1_R = cq$ mit einem $c \in R$. Widerspruch zu $q \notin R^*$. □

Satz 2.1.22. *Es sei R ein Integritätsring.*

(i) *Es seien $p \in R$ prim, $a, b \in R$ und $\nu \in \mathbb{Z}_{\geq 0}$. Gilt $p^\nu \mid ab$ und $p \nmid b$, so gilt bereits $p^\nu \mid a$.*
(ii) *Es seien $p_1, \ldots, p_k \in R$ paarweise nichtassoziierte Primelemente, und es sei $a \in R$ ein beliebiges Element. Gilt $p_i^{\nu_i} \mid a$ mit $\nu_i \in \mathbb{Z}_{\geq 0}$ für $1 \leq i \leq k$, so gilt bereits $p_1^{\nu_1} \cdots p_k^{\nu_k} \mid a$.*
(iii) *Es seien $p_1, \ldots, p_k \in R$ Primelemente, und es sei $a \in R$ ein beliebiges Element. Gilt $a \mid p_1^{\nu_1} \cdots p_k^{\nu_k}$, so gilt bereits $a \sim p_1^{n_1} \cdots p_k^{n_k}$ mit $0 \leq n_i \leq \nu_i$.*

Beweis. Aussage (i) erhält man durch Induktion über ν. Für $\nu = 1$ liefert die definierende Eigenschaft des Primelements $p \mid a$. Gilt $\nu > 1$, so gilt insbesondere $p \mid ab$ und somit $a = a'p$ mit einem $a' \in R$. Es folgt $p^\nu \mid a'pb$ und somit $p^{\nu-1} \mid a'b$. Die Induktionsvoraussetzung liefert $p^{\nu-1} \mid a'$. Das impliziert $p^\nu \mid a$.

Aussage (ii) beweisen wir mittels Induktion über $m := \nu_1 + \ldots + \nu_k$. Für $m = 0, 1$ ist nichts zu zeigen. Gilt $m > 1$, so gibt es ein i mit $\nu_i > 0$. Das bedeutet $p_i \mid a$ und somit $a = a'p_i$ mit einem $a' \in R$. Offensichtlich gilt $p_i^{\nu_i - 1} \mid a'$. Mit (i) erhalten wir weiter $p_j^{\nu_j} \mid a'$ für jedes $j \neq i$. Die Induktionsvoraussetzung liefert $p_1^{\mu_1} \cdots p_k^{\mu_k} \mid a'$, wobei $\mu_j = \nu_j$, falls $j \neq i$ und $\mu_i = \nu_i - 1$. Es folgt $p_1^{\nu_1} \cdots p_k^{\nu_k} \mid a$.

Aussage (iii) beweisen wir ebenfalls per Induktion über $m := \nu_1 + \ldots + \nu_k$. Im Falle $m = 0$ ist nichts zu zeigen. Für $m > 0$ haben wir $p_1^{\nu_1} \cdots p_k^{\nu_k} = ab$ mit einem $b \in R$, und es gilt $\nu_i \geq 1$ für ein i. Da p_i ein Primelement ist, sind die folgenden beiden Fälle möglich.

Fall 1. Es gilt $p_i \mid a$. Dann haben wir $a = a'p_i$ mit $a' \in R$. Es folgt $a' \mid p_1^{\mu_1} \cdots p_k^{\mu_k}$, wobei $\mu_j = \nu_j$, falls $j \neq i$ und $\mu_i = \nu_i - 1$. Nach Induktionsvoraussetzung haben wir $a' \sim p_1^{m_1} \cdots p_k^{m_k}$ mit $0 \leq m_i \leq \mu_i$. Es folgt $a \sim p_1^{n_1} \cdots p_k^{n_k}$ mit $0 \leq n_i \leq \nu_i$.

Fall 2. Es gilt $p_i \mid b$. Dann haben wir $b = b'p_i$ mit $b' \in R$. Es folgt $a \mid p_1^{\mu_1} \cdots p_k^{\mu_k}$, wobei $\mu_j = \nu_j$, falls $j \neq i$ und $\mu_i = \nu_i - 1$. Nach Induktionsvoraussetzung haben wir $a \sim p_1^{m_1} \cdots p_k^{m_k}$ mit $0 \leq m_i \leq \mu_i$. □

Aufgaben zu Abschnitt 2.1.

Aufgabe 2.1.23. Es sei R ein Integritätsring, und es seien Elemente $a, a_1, \ldots, a_n \in R$ gegeben. Zeige: Es gilt

$$a \in \mathrm{kgV}(a_1, \ldots, a_n) \iff \langle a \rangle = \langle a_1 \rangle \cap \ldots \cap \langle a_n \rangle.$$

Aufgabe 2.1.24. Zeige: Zu jedem Tripel (a_1, a_2, a_3) ganzer Zahlen gibt es eine ganze Zahl a mit

$$a \equiv a_1 \mod 35, \qquad a \equiv a_2 \mod 44, \qquad a \equiv a_3 \mod 57,$$

wobei die Schreibweise "$a \equiv b \mod c$" wie üblich bedeutet, dass c ein Teiler der Differenz $b - a$ ist.

Aufgabe 2.1.25. Betrachte den Ring $\mathbb{Z}[I\sqrt{5}] \subseteq \mathbb{C}$. Zeige, dass die Elemente $3 \in \mathbb{Z}[I\sqrt{5}]$ und $2 \pm I\sqrt{5} \in \mathbb{Z}[I\sqrt{5}]$ irreduzibel, aber nicht prim sind.

2.2. **Euklidische Ringe.**

Beispiel 2.2.1. Wir betrachten den Ring $\mathbb{Z}$ der ganzen Zahlen und den Absolutbetrag $\mathbb{Z} \mapsto \mathbb{Z}_{\geq 0}$, $a \mapsto |a|$. Dann gilt:

(i) Für je zwei ganze Zahlen $a, b \in \mathbb{Z}$ mit $a \neq 0 \neq b$ hat man die Abschätzung
$$|a| \ \leq \ |a||b| \ = \ |ab|.$$
(ii) Division mit Rest liefert für je zwei $a, b \in \mathbb{Z}$ mit $b \neq 0$ eine Darstellung
$$a \ = \ qb + r, \qquad \text{mit } q, r \in \mathbb{Z},\ |r| < |b|.$$

Definition 2.2.2. Ein *euklidischer Ring* ist ein Integritätsring R zusammen mit einer Abbildung $\delta\colon R \setminus \{0_R\} \to \mathbb{Z}_{\geq 0}$, sodass folgendes gilt:

(i) Für je zwei Elemente $a, b \in R \setminus \{0\}$ hat man $\delta(a) \leq \delta(ab)$.
(ii) Zu jedem $a \in R$ und jedem $0 \neq b \in R$ gibt es $q, r \in R$ mit
$$a \ = \ qb + r, \qquad \text{wobei } \delta(r) < \delta(b) \text{ oder } r = 0_R.$$

Man nennt $\delta\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ dann eine *Gradabbildung* auf R und die Darstellung $a = qb + r$ aus (ii) nennt man eine *Division mit Rest* in R.

Satz 2.2.3. *Der Ring $\mathbb{Z}[I] \subseteq \mathbb{C}$ der ganzen Gaußschen Zahlen ist zusammen mit $\delta(m + In) := m^2 + n^2$ ein euklidischer Ring.*

Beweis. Wir vermerken zunächst, dass $\delta(a) = a\overline{a}$ für jedes $a \in \mathbb{Z}[I]$ gilt. Insbesondere hat man für alle $a = m + nI$ und $b = k + lI$ aus $\mathbb{Z}[I]$:
$$\delta(a) \ \leq \ \delta(a)(k^2 + l^2) \ = \ \delta(a)\delta(b) \ = \ \delta(ab).$$
Um die im Falle $b \neq 0$ benötigte Darstellung $a = qb + r$ zu erhalten, betrachten wir zunächst die komplexe Zahl
$$ab^{-1} \ = \ u + vI \ \in \ \mathbb{C}, \quad \text{wobei } u, v \in \mathbb{R}$$
und wählen $s, t \in \mathbb{Z}$ mit $|u - s| \leq 1/2$ sowie $|v - t| \leq 1/2$. Dann setzen wir $q := s + tI$ und erhalten $a = qb + r$ mit $r := a - qb = b(ab^{-1} - q)$. Es folgt
$$\delta(r) \ = \ \delta(b)\delta(ab^{-1} - q) \ = \ \delta(b)\left((u - s)^2 + (v - t)^2\right) \ \leq \ \frac{\delta(b)}{2} \ < \ \delta(b).$$
□

Satz 2.2.4. *Es sei $\mathbb{K}$ ein Körper, und es sei $\mathbb{K}[T]$ der Polynomring in der Variablen T über $\mathbb{K}$. Dann gilt:*

(i) *Für je zwei nichttriviale Polynome $f, g \in \mathbb{K}[T]$ hat man*
$$\deg(f) \ \leq \ \deg(f) + \deg(g) \ = \ \deg(fg).$$
(ii) *Für je zwei $f, g \in \mathbb{K}[T]$ mit $g \neq 0_{\mathbb{K}[T]}$ hat man eine Darstellung*
$$f \ = \ qg + r \qquad \textit{mit } q, r \in \mathbb{K}[T],\ \deg(r) < \deg(g).$$
Dabei sind die Polynome $q, r \in \mathbb{K}[T]$ eindeutig bestimmt.

Insbesondere ist der Polynomring $\mathbb{K}[T]$ zusammen mit der Gradabbildung $\delta(f) := \deg(f)$ ein euklidischer Ring.

Beweis. Aussage (i) ist offensichtlich. Die Existenz der Darstellung aus (ii) ist bereits in [1, Satz 8.2.5] gezeigt worden. Zur Eindeutigkeit seien zwei Darstellungen
$$f \ = \ qg + r \ = \ q'g + r'.$$
gegeben. Dann gilt $(q - q')g + (r - r') = 0$. Dabei ist $r - r'$ dem Grade nach kleiner als $(q - q')g$. Das impliziert $q = q'$ und $r = r'$. □

Konstruktion 2.2.5 (Polynomdivision)**.** Es seien $\mathbb{K}$ ein Körper und $f, g \in \mathbb{K}[T]$ mit $g \neq 0_{\mathbb{K}[T]}$. Weiter seien $m := \deg(g)$ und $b \in \mathbb{K}$ der Leitkoeffizient von g.

Das folgende Verfahren ermöglicht es, eine Darstellung $f = qg + r$ wie in Satz 2.2.4 (ii) explizit zu bestimmen.

- Schritt 0. Setze $q_0 := 0$ und $f_0 := f$. Falls $n_0 := \deg(f_0) < \deg(g)$: Abbrechen mit $q := q_0$ und $r := f_0$.
- Schritt 1. Es sei a_0 der Leitkoeffizient von f_0. Bestimme die Polynome
$$q_1 := \frac{a_0}{b} T^{n_0 - m}, \qquad f_1 := f_0 - q_1 g.$$
Falls $n_1 := \deg(f_1) < \deg(g)$: Abbrechen mit $q := q_0 + q_1$ und $r := f_1$.

$$\vdots$$

- Schritt k. Es sei a_{k-1} der Leitkoeffizient von f_{k-1}. Bestimme die Polynome
$$q_k := \frac{a_{k-1}}{b} T^{n_{k-1} - m}, \qquad f_k := f_{k-1} - q_k g.$$
Falls $n_k := \deg(f_k) < \deg(g)$: Abbrechen mit $q := q_0 + \ldots + q_k$ und $r := f_k$.

$$\vdots$$

Da der Grad von f_k in jedem Schritt echt veringert wird, bricht das Verfahren bei irgendeinem $k = n$ ab. Dann hat man

$$\begin{aligned} f_{n-1} &= q_n g + r, \\ f_{n-2} &= f_{n-1} + q_{n-1} g = (q_{n-1} + q_n) g + r \\ &\vdots \\ f = f_0 &= (q_0 + q_1 + \ldots + q_n) g + r = qg + r. \end{aligned}$$

Beispiel 2.2.6. Für die Polynome $f = T^3 + 2T + 1$ und $g = T - 1$ aus $\mathbb{Q}[T]$ erhält man die Darstellung $f = qg + r$ mittels Polynomdivision wie folgt.

$$\begin{aligned} \underbrace{T^3 + 2T + 1}_{f_0 = f} &= \underbrace{(T - 1)}_{g} \cdot \underbrace{(\underbrace{T^2}_{q_1} + \underbrace{T}_{q_2} + \underbrace{3}_{q_3})}_{q} + \underbrace{4}_{r} \\ &\quad -(\underbrace{T^3 - T^2}_{q_1 g}) \\ &= \underbrace{T^2 + 2T + 1}_{f_1 = f_0 - q_1 g} \\ &\quad -(\underbrace{T^2 - T}_{q_2 g}) \\ &= \underbrace{3T + 1}_{f_2 = f_1 - q_2 g} \\ &\quad -(\underbrace{3T - 3}_{q_3 g}) \\ &= \underbrace{4}_{r = f_3 = f_2 - q_3 g} \end{aligned}$$

Satz 2.2.7. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Es sei R ein euklidischer Ring mit Gradabbildung δ. Zu einem gegebenen Ideal $\mathfrak{a} \neq \langle 0 \rangle$ betrachten wir ein Element $0 \neq b \in \mathfrak{a}$ mit minimalem Grad $\delta(b)$. Wir zeigen $\mathfrak{a} = \langle b \rangle$. Ist $a \in \mathfrak{a}$ ein beliebiges Element, so haben wir eine Darstellung

$$a \;=\; qb + r, \qquad \text{wobei } \delta(r) < \delta(b) \text{ oder } r = 0.$$

Man beachte, dass dabei $r = a - qb \in \mathfrak{a}$ gilt. Da b minimalen Grad unter den Elementen von $\mathfrak{a}$ besitzt, muss $r = 0$ gelten. Folglich erhalten wir $a = qb$. Mit anderen Worten, es gilt $a \in \langle b \rangle$. □

Folgerung 2.2.8. *Die Ringe $\mathbb{Z}$ und $\mathbb{Z}[I]$ sind Hauptidealringe. Weiter ist für jeden Körper $\mathbb{K}$ der Polynomring $\mathbb{K}[T]$ ein Hauptidealring.*

Folgerung 2.2.9. *Für den Ring $\mathbb{Z}$ der ganzen Zahlen erhält man:*

(i) *Die Primzahlen sind genau die positiven Primelemente in $\mathbb{Z}$.*
(ii) *Jede Untergruppe $H \leq \mathbb{Z}$ ist von der Form $H = n\mathbb{Z}$ mit einem $n \in \mathbb{Z}$.*

Beweis. Zu (i). Die Primzahlen sind genau die irreduziblen Elemente in $\mathbb{Z}_{\geq 0}$. Da die Begriffe irreduzibel und prim in Hauptidealringen zusammenfallen, ergibt sich die Behauptung. Zu (ii). Jede Untergruppe $H \leq \mathbb{Z}$ ist bereits ein Ideal in $\mathbb{Z}$. Damit ergibt sich die Behauptung. □

Konstruktion 2.2.10 (Euklidischer Algorithmus)**.** Es sei R ein euklidischer Ring mit Gradabbildung δ, und es seien $a, b \in R$, wobei $b \neq 0$.

- *Schritt 0.* Setze $c_{-1} := a$ und $c_0 := b$.
- *Schritt 1.* Wähle $c_1, q_1 \in R$ mit

  $$c_{-1} \;=\; q_1 c_0 + c_1, \qquad \text{wobei } \delta(c_1) < \delta(c_0) \text{ oder } c_1 = 0.$$

  Falls $c_1 = 0$: Verfahren abbrechen.
- *Schritt 2.* Wähle $c_2, q_2 \in R$ mit

  $$c_0 \;=\; q_2 c_1 + c_2, \qquad \text{wobei } \delta(c_2) < \delta(c_1) \text{ oder } c_2 = 0.$$

  Falls $c_2 = 0$: Verfahren abbrechen.

  $\vdots$

- *Schritt n.* Wähle $c_n, q_n \in R$ mit

  $$c_{n-2} \;=\; q_n c_{n-1} + c_n, \qquad \text{wobei } \delta(c_n) < \delta(c_{n-1}) \text{ oder } c_n = 0.$$

  Falls $c_n = 0$: Verfahren abbrechen.

  $\vdots$

Das Verfahren bricht bei einem $n \in \mathbb{Z}_{>0}$ mit $c_n = 0$ ab. Dabei ist c_{n-1} ein größter gemeinsamer Teiler von a und b, und man erhält eine Darstellung

$$c_{n-1} \;=\; ua + vb, \qquad \text{mit } u, v \in R.$$

Beweis. Da im euklidischen Algorithmus $\delta(c_{i+1}) < \delta(c_i)$ für jedes $i \geq 0$ gilt, muss das Verfahren irgendwann mit $c_n = 0$ abbrechen. Um zu sehen, dass c_{n-1} dann ein gemeinsamer Teiler von a und b ist, betrachten wir das Schema

$$\begin{aligned} c_{n-2} &= q_n c_{n-1} \\ c_{n-3} &= q_{n-1} c_{n-2} + c_{n-1} \\ c_{n-4} &= q_{n-2} c_{n-3} + c_{n-2} \\ &\vdots \\ c_1 &= q_3 c_2 - c_3 \\ b = c_0 &= q_2 c_1 + c_2 \\ a = c_{-1} &= q_1 c_0 + c_1 \end{aligned}$$

Indem wir Darstellung von c_{n-2} in die von c_{n-3} einsetzen, sehen wir, dass c_{n-3} ein Vielfaches von c_{n-1} ist. Es folgt, dass c_{n-4} Vielfaches von c_{n-1} ist, usw., und schließlich sieht man, dass b und a Vielfache von c_{n-1} sind.

Um zu sehen, dass jeder gemeinsame Teiler c von a und b auch ein Teiler von c_{n-1} ist, schreiben wir das obige Schema um. In jeder Gleichung lösen wir nach dem c_i mit größtem i auf:

$$\begin{aligned} c_{n-1} &= c_{n-3} - q_{n-1} c_{n-2} \\ c_{n-2} &= c_{n-4} - q_{n-2} c_{n-3} \\ c_{n-3} &= c_{n-5} - q_{n-3} c_{n-4} \\ &\vdots \\ c_2 &= c_0 - q_2 c_1 \\ c_1 &= c_{-1} - q_1 c_0 \\ &= a - q_1 b. \end{aligned}$$

Die unterste Gleichung liefert, dass mit a und b auch c_1 ein Vielfaches von c ist. Geht man eine Gleichung höher, so erhält man, dass c_2 Vielfaches von c ist usw..

Weiter liefert die oberste Gleichung, dass man c_{n-1} linear aus c_{n-3} und c_{n-2} kombinieren kann. Entsprechend liefert die zweite Gleichung, dass man c_{n-2} linear aus c_{n-3} und c_{n-4} kombinieren kann. Durch sukzessives Einsetzen erhält man so eine Darstellung $c_{n-1} = ua + vb$. □

Beispiel 2.2.11. Wir führen den euklidischen Algorithmus in $\mathbb{Z}$ mit $a := 60$ und $b := 42$ durch. Er bricht im dritten Schritt ab:

$$60 \;=\; 1 \cdot 42 + 18, \qquad 42 \;=\; 2 \cdot 18 + 6, \qquad 18 \;=\; 3 \cdot 6$$

Folglich ist 6 ein größter gemeinsamer Teiler von 60 und 42. Weiter erhalten wir die Vielfachsummendarstellung

$$6 \;=\; 42 - 2 \cdot 18 \;=\; 42 - 2 \cdot (60 - 42) \;=\; 3 \cdot 42 - 2 \cdot 60.$$

Aufgaben zu Abschnitt 2.2.

Aufgabe 2.2.12. Es sei (R, δ) ein euklidischer Ring. Zeige: Ein Element $a \in R$ ist genau dann eine Einheit, wenn $\delta(a) = \delta(1_R)$ gilt.

Aufgabe 2.2.13. Finde eine explizite Darstellung $f = qg + r$ mit $\deg(r) \leq \deg(g)$ in $\mathbb{Q}[T]$ für die Polynome

$$f := 3T^5 - 6T^4 + 19T^3 - 25T^2 + 15T - 8, \qquad g := T^3 + 5T + 1.$$

Aufgabe 2.2.14. Bestimme mittels euklidischem Algorithmus einen größten gemeinsamen Teiler für die Polynome

$$f := 6T^5 + 2T^4 - T^3 - 4T^2 + 3, \qquad g := 2T^4 + 2T^3 - T^2 - T - 1.$$

Aufgabe 2.2.15. Es seien $p \in \mathbb{Z}$ eine Primzahl und $c \in \mathbb{Z}$ mit $\mathrm{ggT}(p, c) = 1$, sodass $cp = m^2 + n^2$ mit ganzen Zahlen m, n gilt. Zeige:

(i) $p = p + I \cdot 0$ ist kein Primelement in dem Ring $\mathbb{Z}[I]$ der ganzen Gaußschen Zahlen.
(ii) Es gibt ganze Zahlen a, b mit $p = a^2 + b^2$.

Aufgabe 2.2.16. Es sei $p \in \mathbb{Z}$ eine Primzahl der Form $p = 4m + 1$ mit einem $m \in \mathbb{Z}$. Zeige: Es gibt ganze Zahlen a, b mit $p = a^2 + b^2$. *Hinweis:* Es gibt ein $x \in \mathbb{Z}$ mit $|x| \leq p/2$, sodass $x^2 \equiv -1 \mod p$ gilt. Verwende dann Aufgaben 1.3.17 und 2.2.15.

Aufgabe 2.2.17. Zeige: Der Ring $\mathbb{Z}[\sqrt{d}]$ ist euklidisch für $d = \pm 2$ und $d = 3$. Wie verhält es sich mit $\mathbb{Z}[\sqrt{-3}]$?

2.3. **Primfaktorzerlegung.**

Bemerkung 2.3.1. Der *Hauptsatz der elementaren Zahlentheorie* besagt, dass man jede Zahl $n \in \mathbb{Z}_{>1}$ auf eindeutige Weise zerlegen kann als

$$n \;=\; p_1^{\nu_1} \cdots p_r^{\nu_r}$$

mit Primzahlen $p_1 < \ldots < p_r$ und $\nu_i \in \mathbb{Z}_{\geq 0}$; beispielsweise $60 = 2^2 \cdot 3 \cdot 5$. Wir werden diesen Satz als Folgerung allgemeinerer Überlegungen erhalten.

Definition 2.3.2. Einen Integritätsring R nennt man *faktoriell*, falls jedes $a \in R$ mit $0_R \neq a \notin R^*$ eine Zerlegung $a = p_1 \cdots p_n$ mit Primelementen $p_1, \ldots, p_n \in R$ besitzt.

Satz 2.3.3. *Jeder euklidische Ring ist faktoriell.*

Beweis. Es sei R ein euklidischer Ring mit Gradabbildung $\delta\colon R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$. Nach Satz 2.2.7 ist R ein Hauptidealring. Somit ist jedes irreduzible Element von R bereits prim, siehe Satz 2.1.21. Es genügt daher, zu zeigen, dass jedes Element $0_R \neq a \in R$ entweder eine Einheit oder ein Produkt irreduzibler Elemente ist.

Wir verwenden Induktion über den Grad $\delta(a)$. Gilt $\delta(a) = 0$, so erhalten wir eine Darstellung $1_R = ca + r$ mit $r = 0$. Folglich ist a eine Einheit.

Zum Induktionsschritt. Ist a Einheit oder irreduzibel, so ist nichts zu zeigen. Andernfalls gilt $a = bc$ mit Nichteinheiten b, c. Wir zeigen $\delta(b) < \delta(a)$. Dazu schreiben wir

$$b \;=\; qbc + r, \quad \text{wobei } q, r \in R,\ \delta(r) < \delta(bc) \text{ oder } r = 0_R.$$

Der Fall $r = 0_R$ ist dabei ausgeschlossen, denn dann hätte man $b = qbc$ und somit $1_R = qc$; Widerspruch zu c Nichteinheit. Also gilt

$$0_R \;\neq\; r \;=\; b - qbc \;=\; b(1_R - qc).$$

Es folgt

$$\delta(b) \;\leq\; \delta(r) \;<\; \delta(bc) \;=\; \delta(a).$$

Analog verifiziert man, dass $\delta(c) < \delta(a)$ gilt. Nach Induktionsvoraussetzung sind b sowie c und Produkte irreduzibler Elemente. Also ist auch $a = bc$ ein Produkt irreduzibler Elemente. □

Folgerung 2.3.4. *Die Ringe $\mathbb{Z}$ und $\mathbb{Z}[I]$ sind faktoriell. Weiter ist für jeden Körper $\mathbb{K}$ der Polynomring $\mathbb{K}[T]$ faktoriell.*

Definition 2.3.5. Es sei R ein Integritätsring. Unter einem *Primsystem* für R verstehen wir eine Teilmenge $P \subset R$ von Primelementen, sodass folgendes gilt:

(i) Ist $q \in R$ ein Primelement, so gilt $q \sim p$ mit einem $p \in P$.
(ii) Sind zwei verschiedene $p, p' \in P$ gegeben, so gilt $p \not\sim p'$.

Bemerkung 2.3.6. Ein Primsystem $P \subset R$ ist ein Repräsentantensystem für die Assoziiertheit "$\sim$" auf der Menge aller Primelemente von R.

Beispiel 2.3.7. Die Primzahlen $2, 3, 5, 7, \ldots$ bilden ein Primsystem in dem Ring $\mathbb{Z}$ der ganzen Zahlen.

Satz 2.3.8. *Es seien R ein faktorieller Ring und $P \subset R$ Primsystem. Dann besitzt jedes $a \in R \setminus \{0_R\}$ eine eindeutige Primfaktorzerlegung bezüglich P, d.h., eine Darstellung*

$$a \;=\; c \prod_{p \in P} p^{\nu_p(a)}$$

mit einer eindeutig bestimmten Einheit $c \in R^*$ und eindeutig bestimmten "Vielfachheiten" $\nu_p(a) \in \mathbb{Z}_{\geq 0}$, von denen höchstens endlich viele von Null verschieden sind.

Lemma 2.3.9. *Es sei R ein Integritätsring. Sind $p, q_1, \ldots, q_k \in R$ Primelemente mit $p \mid q_1 \cdots q_k$, so gilt bereits $p \sim q_i$ für ein i.*

Beweis. Wir beweisen die Aussage durch Induktion über k. Zum Fall $k = 1$. Wegen $p \mid q_1$ haben wir $q_1 = cp$ mit einem $c \in R$. Als Primelement ist q_1 nach Satz 2.1.20 irreduzibel. Folglich muß c eine Einheit sein. Das bedeutet $p \sim q_1$. Zum Induktionsschritt. Gilt $p \mid q_1 \cdots q_k$, so gilt $p \mid q_1 \cdots q_{k-1}$ oder $p \mid q_k$, da p prim ist. Folglich liefert die Induktionsvoraussetzung $p \sim q_i$ für ein i. □

Beweis von Satz 2.3.8. Im Falle $a \in R^*$ ist nichts zu zeigen. Es sei nun $a \in R \setminus R^*$. Da R faktoriell ist, haben wir $a = q_1 \cdots q_l$ mit Primelementen $q_j \in R$. Jedes q_i ist assoziiert zu einem $p_i \in P$; wir haben also $q_i = c_i p_i$ mit $c_i \in R^*$. Zusammenfassen gleicher p_i ergibt die gewünschte Darstellung für a mit $c := c_1 \cdots c_l$.

Es bleibt die Eindeutigkeit der Primfaktorzerlegung nachzuweisen. Dazu vergleichen wir zwei Darstellungen

$$c \prod_{p \in P} p^{\nu_p} \quad = \quad c' \prod_{p \in P} p^{\mu_p}.$$

Wir betrachten $k := \sum \nu_p$ und $l := \sum \mu_p$ und zeigen durch Induktion über k, dass $c = c'$ sowie $\nu_p = \mu_p$ für alle $p \in P$ gelten.

Gilt $k = 0$, so hat man $\nu_p = 0$ für alle $p \in P$ und auf der linken Seite steht eine Einheit. Folglich muss auch auf der rechten Seite eine Einheit stehen, was $\mu_p = 0$ für alle $p \in P$ und $c = c'$ impliziert.

Gilt $k > 0$, so muss auch $l > 0$ gelten. Weiter hat man $\nu_{p_0} \neq 0$ für ein $p_0 \in P$. Nach Lemma 2.3.9 findet man auf der rechten Seite ein $q_0 \in P$ mit $q_0 \sim p_0$. Da P ein Primsystem ist, folgt $p_0 = q_0$, d.h., wir haben $\mu_{p_0} > 0$. Kürzt man durch p_0, so liefert die Induktionsvoraussetzung $c = c'$ sowie $\nu_p = \mu_p$ für alle $p \in P$. □

Beispiel 2.3.10. Bezüglich des Primsystems $P = \{2, 3, 5, 7, \ldots\}$ ist die Primfaktorzerlegung von $-360 \in \mathbb{Z}$ gegeben durch

$$-360 \quad = \quad -1 \cdot 2^3 \cdot 3^2 \cdot 5.$$

Weiter erhält man den *Hauptsatz der elementaren Zahlentheorie*: Jede natürliche Zahl $n \geq 2$ lässt sich auf eindeutige Weise darstellen als

$$n \quad = \quad p_1^{\nu_1} \cdots p_r^{\nu_r}$$

mit $r \in \mathbb{Z}_{\geq 1}$, paarweise verschiedenen Primzahlen $p_1 < \ldots < p_r$ und Exponenten $\nu_1, \ldots, \nu_r \in \mathbb{Z}_{\geq 1}$.

Satz 2.3.11. *Es seien R ein faktorieller Ring und $P \subset R$ ein Primsystem. Weiter seien $a_1, \ldots, a_n \in R$ und*

$$a_i \quad = \quad c_i \prod_{p \in P} p^{\nu_p(a_i)}$$

die zugehörigen Primfaktorzerlegungen Mit Einheiten $c_i \in R^*$ und Vielfachheiten $\nu_p(a_i) \in \mathbb{Z}_{\geq 0}$. Die Teilbarkeit $a_i \mid a_j$ wird charakterisiert durch

$$a_i \mid a_j \quad \Longleftrightarrow \quad \nu_p(a_i) \leq \nu_p(a_j) \text{ für alle } p \in P.$$

Weiter hat man immer einen größten gemeinsamen Teiler und ein kleinstes gemeinsames Vielfaches für $a_1, \ldots, a_n$, nämlich

$$\prod_{p\in P} p^{\min(\nu_p(a_i))} \ \in\ \mathrm{ggT}(a_1,\ldots,a_n), \qquad \prod_{p\in P} p^{\max(\nu_p(a_i))} \ \in\ \mathrm{kgV}(a_1,\ldots,a_n).$$

Beweis. Falls $a_i \mid a_j$ gilt, haben wir $a_j = ba_i$ mit einem Element $b \in R$. Es sei $b = c\prod p^{\nu_p(b)}$ die zugehörige Primfaktorzerlegung. Dann gilt

$$c_j \prod_{p\in P} p^{\nu_p(a_j)} \ =\ \left(c\prod_{p\in P} p^{\nu_p(b)}\right)\left(c_j\prod_{p\in P} p^{\nu_p(a_i)}\right) \ =\ cc_j\prod_{p\in P} p^{\nu_p(b)+\nu_p(a_i)}$$

Mit der Eindeutigkeit der Primfaktorzerlegung ergibt sich $\nu_p(a_i) \le \nu_p(a_j)$ für alle $p \in P$. Umgekehrt impliziert letztere Bedingung offensichtlich, dass a_i ein Teiler von a_j ist. Die weiteren Aussagen sind direkte Folgerungen. □

Beispiel 2.3.12. Wir betrachten das Primsystem $P \subseteq \mathbb{Z}$ bestehend aus allen Primzahlen. Dann hat man die Primfaktorzerlegungen

$$12 \ =\ 2^2\cdot 3, \qquad\qquad 18 \ =\ 2\cdot 3^2.$$

Gemäß Satz 2.3.11 erhalten wir dann den größten gemeinsamen Teiler sowie das kleinste gemeinsame Vielfache als

$$\mathrm{ggT}(12,18) \ =\ \{\pm 2\cdot 3\} \ =\ \{\pm 6\}, \qquad \mathrm{kgV}(12,18) \ =\ \{\pm 2^2\cdot 3^2\} \ =\ \{\pm 36\}.$$

Satz 2.3.13. *Es seien R ein euklidischer Ring und $a = cp_1^{\nu_1}\cdots p_n^{\nu_n} \in R$ mit einer Einheit $c \in R^*$ und paarweise nichtassoziierte Primelementen $p_i \in R$. Dann hat man einen Isomorphismus von Ringen*

$$R/\langle a\rangle \ \cong\ R/\langle p_1^{\nu_1}\rangle \ \times\ \ldots\ \times\ R/\langle p_n^{\nu_n}\rangle.$$

Beweis. Wir dürfen annehmen, dass $p_1, \ldots, p_n$ Elemente eines Primsystems $P \subset R$ sind. Weiter genügt es, den Fall $c = 1$ zu behandeln. Nach Satz 2.3.11 sind $p_i^{\nu_i}$ und $p_j^{\nu_j}$ für $i \ne j$ teilerfremd. Nach Satz 2.1.14 bedeutet dies

$$\langle p_i^{\nu_i}\rangle + \langle p_j^{\nu_j}\rangle \ =\ \langle p_i^{\nu_i}, p_j^{\nu_j}\rangle \ =\ \langle 1_R\rangle \ =\ R.$$

Damit können wir den Chinesischen Restsatz 1.4.19 ins Spiel bringen; er liefert im vorliegenden Fall einen Isomorphismus von Ringen

$$R/\left(\langle p_1^{\nu_1}\rangle \ \cap\ \ldots\ \cap\ \langle p_n^{\nu_n}\rangle\right) \ \cong\ R/\langle p_1^{\nu_1}\rangle \ \times\ \ldots\ \times\ R/\langle p_n^{\nu_n}\rangle.$$

Zum Beweis der Aussage müssen wir also nur noch $\langle a\rangle = \langle p_1^{\nu_1}\rangle \cap \ldots \cap \langle p_n^{\nu_n}\rangle$ nachweisen. Die Inklusion "$\subseteq$" ist dabei offensichtlich. Die Inklusion "$\supseteq$" ergibt sich wie folgt. Liegt $b \in R$ in der rechten Seite, so erhält man insbesondere $p_i^{\nu_i} \mid b$ für jedes i. Satz 2.3.11 liefert dann $p_1^{\nu_1}\cdots p_n^{\nu_n} \mid b$ und somit $b \in \langle a\rangle$. □

Bemerkung 2.3.14. Es sei $n \in \mathbb{Z}_{\ge 1}$, und es sei $n = p_1^{\nu_1}\ldots p_r^{\nu_r}$ die zugehörige Primfaktorzerlegung. Satz 2.3.13 liefert einen Isomorphismus von K1-Ringen

$$\mathbb{Z}/n\mathbb{Z} \ \cong\ \mathbb{Z}/\langle p_1^{\nu_1}\rangle \ \times\ \ldots\ \times\ \mathbb{Z}/\langle p_r^{\nu_r}\rangle.$$

Dieser ist insbesondere ein Isomorphismus der zu Grunde liegenden abelschen Gruppen. Weiter erhält man für die Einheiten

$$(\mathbb{Z}/n\mathbb{Z})^* \ \cong\ (\mathbb{Z}/\langle p_1^{\nu_1}\rangle)^* \ \times\ \ldots\ \times\ (\mathbb{Z}/\langle p_r^{\nu_r}\rangle)^*.$$

Satz 2.3.15. *Die Menge $\{T-a;\ a\in\mathbb{C}\}$ ist ein Primsystem in dem Polynomring $\mathbb{C}[T]$. Jedes nichtkonstante $f\in\mathbb{C}[T]$ lässt sich eindeutig schreiben als*

$$f \;=\; c\prod_{a\in\mathbb{C}}(T-a)^{\nu_a(f)},$$

wobei $c\in\mathbb{C}^*$. Die Vielfachheit $\nu_a(f)$ des Primfaktors $T-a$ in f ist dabei genau die Ordnung der Nullstelle a von f.

Beweis. Jedes Polynom $T-a$ besitzt den Grad 1 und ist somit irreduzibel. Da $\mathbb{C}[T]$ ein Hauptidealring ist, muss $T-a$ bereits prim sein, siehe Satz 2.1.21. Weiter gilt

$$(T-a)\sim(T-b) \iff (T-b)=c(T-a) \text{ mit } c\in\mathbb{C}^* \iff b=a.$$

Insbesondere sind keine zwei verschiedenen Polynome $T-a$ und $T-b$ assoziiert zueinander.

Um zu sehen, dass die Polynome $T-a$ ein Primsystem bilden, müssen wir noch zeigen, dass jedes Primelement $f\in\mathbb{C}[T]$ assoziiert zu einem $T-a$ ist. Nach dem Fundamentalsatz der Algebra gilt $f=c\cdot(T-a_1)\cdots(T-a_r)$ mit $c\in\mathbb{C}^*$ und $a_1,\ldots,a_r\in\mathbb{C}$. Da f irreduzibel ist, folgt $f\sim T-a_1$. □

Satz 2.3.16. *Die normierten Primpolynome in dem Polynomring $\mathbb{R}[T]$ sind genau die Polynome der Form*

$$T-a,\ \text{wobei } a\in\mathbb{R}, \qquad T^2+bT+c,\ \text{wobei } b,c\in\mathbb{R},\ b^2<4c.$$

Lemma 2.3.17. *Es sei $f=\sum a_\nu T^\nu\in\mathbb{C}[T]$ mit nur reellen Koeffizienten a_ν. Ist $\lambda\in\mathbb{C}$ eine Nullstelle von f, so ist auch $\overline{\lambda}$ eine Nullstelle von f.*

Beweis. Die Aussage ergibt sich sofort aus der Tatsache, dass die komplexe Konjugation ein Körperhomomorphismus ist und die reellen Zahlen fest lässt: Es gilt

$$f(\overline{\lambda}) \;=\; \sum a_\nu\overline{\lambda}^\nu \;=\; \overline{\sum a_\nu\lambda^\nu} \;=\; \overline{f(\lambda)} \;=\; 0.$$

□

Lemma 2.3.18. *Es sei eine Zerlegung $f=gh$ mit drei nichtverschwindenden Polynomen $f,g,h\in\mathbb{C}[T]$ gegeben. Sind zwei dieser Polynome reell, so ist auch das dritte reell.*

Beweis. Falls g und h reell sind, so ist offensichtlich auch f reell. Es bleibt also nur der Fall, dass f und g reell sind zu diskutieren. Wir verwenden Induktion über $n:=\deg(f)$. Der Fall $n=0$ ist klar.

Für den Induktionsschritt verwenden wir Division mit Rest in $\mathbb{R}[T]$ und schreiben $f=qg+r$ mit Polynomen $q,r\in\mathbb{R}[T]$, wobei $\deg(r)<\deg(g)$. Mit $f=gh$ ergibt sich

$$gh \;=\; qg+r \;\Longrightarrow\; r \;=\; (h-q)g.$$

Ist r das Nullpolynom, so ergibt sich $h=q\in\mathbb{R}[T]$. Andernfalls verwenden wir die Abschätzung

$$\deg(r) \;<\; \deg(g) \;\leq\; \deg(f)$$

und erhalten mittels Induktionsvoraussetzung, dass $h-q\in\mathbb{R}[T]$ gilt. Das impliziert $h\in\mathbb{R}[T]$. □

Beweis von Satz 2.3.16. Die angegebenen Polynome sind offensichtlich irreduzibel und somit prim. Ausserdem sind sie paarweise nichtassoziiert zueinander. Wir zeigen nun, dass jedes normierte Primpolynom $f \in \mathbb{R}[T]$ bereits erfasst ist.

Besitzt f eine Nullstelle $a \in \mathbb{R}$, so können wir f schreiben als $f = (T-a)g$ mit einem Polynom $g \in \mathbb{R}[T]$. Die Irreduzibilität von f impliziert $g = 1_{\mathbb{R}[T]}$.

Gilt $f(a) \neq 0$ für alle $a \in \mathbb{R}$, so verwenden wir den Fundamentalsatz der Algebra. Dieser liefert ein $\lambda \in \mathbb{C}$ mit $f(\lambda) = 0$. Nach Lemma 2.3.17 ist auch $\overline{\lambda}$ eine Nullstelle von f. Folglich gilt

$$f \;=\; (T-\lambda)(T-\overline{\lambda})g \;=\; (T^2 - (\lambda+\overline{\lambda})T + \lambda\overline{\lambda})g.$$

mit einem Polynom $g \in \mathbb{C}[T]$. Lemma 2.3.18 garantiert, dass g ein reelles Polynom ist. Da f irreduzibel in $\mathbb{R}[T]$ ist, muss g eine Einheit in $\mathbb{R}[T]$ sein. Da f normiert ist, erhalten wir $g = 1_{\mathbb{R}[T]}$. Mit $\lambda = x + Iy$ folgt schliesslich

$$(-\lambda - \overline{\lambda})^2 \;=\; 4x^2 \;<\; 4x^2 + 4y^2 \;=\; 4\lambda\overline{\lambda}.$$

□

Aufgaben zu Abschnitt 2.3.

Aufgabe 2.3.19. Es sei R ein faktorieller Ring, und es sei $q \in R$. Beweise die Äquivalenz folgender Aussagen:

(i) q ist irreduzibel.
(ii) q ist prim.

Aufgabe 2.3.20. Die *Eulersche* Φ*-Funktion* ordnet jeder Zahl $n \in \mathbb{Z}_{\geq 1}$ die Anzahl $\Phi(n)$ der zu n teilerfremden ganzen Zahlen m mit $1 \leq m \leq n$ zu:

$$\Phi(n) \quad = \quad |\{m \in \mathbb{Z}_{\geq 1};\ m \leq n,\, 1 \in \mathrm{ggT}(m,n)\}|.$$

Für $n \in \mathbb{Z}_{\geq 2}$ sei $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ eine Darstellung mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$. Zeige: Es gilt

$$\Phi(n) \ = \ \Phi(p_1^{\nu_1}) \cdots \Phi(p_r^{\nu_r}) \ = \ n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Aufgabe 2.3.21. Es seien $m, n \in \mathbb{Z}_{\geq 1}$ zwei teilerfremde ganze Zahlen. Zeige: Es gilt $m^{\Phi(n)} \equiv 1 \mod n$.

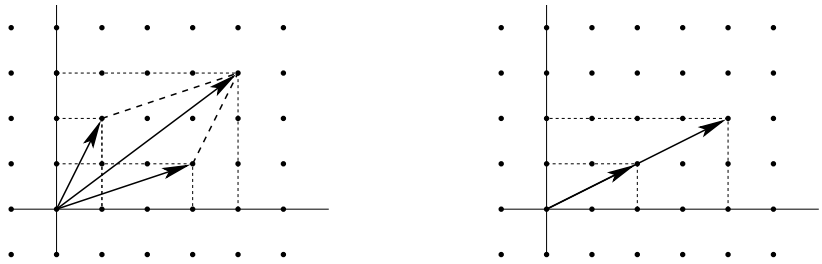
Aufgabe 2.3.22. Bestimme die Primfaktorzerlegungen jeweils in $\mathbb{C}[T]$ und in $\mathbb{R}[T]$ für die Polynome $T^2 + 1$, $T^3 + 1$ sowie $T^4 + 1$.

Aufgabe 2.3.23. Zeige: Der Polynomring $\mathbb{Q}[T]$ besitzt irreduzible Polynome beliebig hohen Grades.

3. Moduln

3.1. **Grundbegriffe.**

Beispiel 3.1.1. Die Teilmenge $\mathbb{Z}^2 \subseteq \mathbb{R}^2$ ist eine Untergruppe der additiven Gruppe $\mathbb{R}^2$, und wir haben Skalarmultiplikation mit ganzen Zahlen auf $\mathbb{Z}^2$:



Definition 3.1.2. Es sei R ein K1-Ring. Ein *(unitärer) R-Modul* ist eine abelsche Gruppe $(M,+)$ zusammen mit einer Abbildung

$$R \times M \;\to\; M, \qquad (r,u) \;\mapsto\; r\cdot u,$$

genannt *Skalarmultiplikation*, sodass für $r, r' \in R$ und $u, u' \in M$ stets folgendes gilt:

$$1_R \cdot u \;=\; u, \quad (r'r)\cdot u \;=\; r'\cdot(r\cdot u), \quad (r'+r)\cdot u \;=\; r'\cdot u + r\cdot u, \quad r\cdot(u+u') \;=\; r\cdot u + r\cdot u'.$$

Bemerkung 3.1.3. Der Begriff des Moduls verallgemeinert den Begriff des Vektorraumes: Die Moduln über einem Körper $\mathbb{K}$ sind genau die Vektorräume über $\mathbb{K}$.

Beispiel 3.1.4. Es sei R ein K1-Ring. Dann wird die Menge R^n zu einem R-Modul durch komponentenweise Addition und komponentenweise Skalarmultiplikation

$$\begin{aligned}(r_1,\ldots,r_n) \;+\; (s_1,\ldots,s_n) \;&:=\; (r_1+s_1,\ldots,r_n+s_n),\\ a\cdot(r_1,\ldots,r_n) \;&:=\; (ar_1,\ldots,ar_n).\end{aligned}$$

Konstruktion 3.1.5. Jede abelsche Gruppe $(G,+)$ ist auf kanonische Weise ein $\mathbb{Z}$-Modul: Man definiert eine Skalarmultiplikation $\mathbb{Z} \times G \to G$ durch

$$n\cdot g \;:=\; ng \;=\; \begin{cases} \underbrace{g+\ldots+g}_{n\text{-mal}} & \text{falls } n>0,\\ 0 & \text{falls } n=0,\\ \underbrace{-g-\ldots-g}_{|n|\text{-mal}} & \text{falls } n<0.\end{cases}$$

Konstruktion 3.1.6. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ eine lineare Abbildung. Dann wird V zu einem $\mathbb{K}[T]$-Modul durch

$$\Big(\sum a_\nu T^\nu\Big)\cdot v \;:=\; \sum a_\nu \varphi^\nu(v),$$

wobei wir, wie üblich, φ^ν für die ν-fache Hintereinanderausführung $\varphi\circ\ldots\circ\varphi$ von $\varphi\colon V\to V$ schreiben.

Beweis. Mit $\varphi^0 = \mathrm{id}_V$ ergibt sich sofort $1_{\mathbb{K}[T]} \cdot v = v$. Die weiteren Modulaxiome erhalten wir mit

$$\begin{aligned}
\textstyle\sum a_\nu T^\nu \cdot \big(\big(\sum b_\mu T^\mu\big) \cdot v\big) &= \textstyle\sum a_\nu \varphi^\nu \big(\sum b_\mu \varphi^\mu(v)\big) \\
&= \textstyle\sum\limits_\kappa \Big(\sum\limits_{\nu+\mu=\kappa} a_\nu b_\mu \varphi^\kappa(v) \Big) \\
&= \big(\big(\textstyle\sum a_\nu T^\nu\big) \cdot \big(\sum b_\mu T^\mu\big)\big) \cdot v, \\
\big(\textstyle\sum a_\nu T^\nu + \sum b_\nu T^\nu\big) \cdot v &= \big(\textstyle\sum (a_\nu + b_\nu) T^\nu\big) \cdot v \\
&= \textstyle\sum (a_\nu + b_\nu) \varphi^\nu(v) \\
&= \textstyle\sum a_\nu \varphi^\nu(v) \; + \; \sum b_\nu \varphi^\nu(v) \\
&= \big(\textstyle\sum a_\nu T^\nu\big) \cdot v \; + \; \big(\sum b_\mu T^\mu\big) \cdot v, \\
\big(\textstyle\sum a_\nu T^\nu\big) \cdot (v + v') &= \textstyle\sum a_\nu \varphi^\nu(v + v') \\
&= \textstyle\sum a_\nu \varphi^\nu(v) \; + \; \sum a_\nu \varphi^\nu(v') \\
&= \big(\textstyle\sum a_\nu T^\nu\big) \cdot v \; + \; \big(\sum b_\mu T^\mu\big) \cdot v.
\end{aligned}$$

□

Definition 3.1.7. Es seien R ein K1-Ring, M ein R-Modul, und $N \subseteq M$ eine nichtleere Teilmenge mit

$$v, v' \in N \implies v + v' \in N, \qquad v \in N, r \in R \implies r \cdot v \in N.$$

Dann nennen wir N zusammen mit den induzierten Verknüpfungen $(v, v') \mapsto v + v'$ sowie $(r, v) \mapsto r \cdot v$ einen *(R-)Untermodul von M*; wir schreiben dafür auch $N \leq_R M$.

Bemerkung 3.1.8. Es seien R ein K1-Ring, M ein R-Modul und $N \leq_R M$ ein Untermodul. Dann ist N eine Untergruppe der additiven Gruppe M und N ist bezüglich der induzierten Verknüpfungen wieder ein R-Modul.

Bemerkung 3.1.9. Es sei G eine abelsche Gruppe. Dann ist G ein $\mathbb{Z}$-Modul gemäß 3.1.5. Die $\mathbb{Z}$-Untermoduln von G sind genau die Untergruppen von G.

Bemerkung 3.1.10. Es sei R ein K1-Ring. Dann wird $(R, +)$ ein R-Modul durch $r \cdot u := ru$. Die R-Untermoduln von R sind genau die Ideale des Ringes R.

Definition 3.1.11. Es seien R ein K1-Ring, M ein R-Modul und $\mathcal{F} = (u_i)_{i \in I}$ eine Familie in M, wobei $I \neq \emptyset$. Eine *(R-)Linearkombination über $\mathcal{F}$* ist ein Element der Form

$$\sum_{i \in I} a_i \cdot u_i \in M, \qquad \text{wobei } a_i \in R,\ a_i \neq 0_R \text{ für höchstens endlich viele } i \in I.$$

Konstruktion 3.1.12. Es seien R ein K1-Ring, M ein R-Modul und $\mathcal{F} = (u_i)_{i \in I}$ eine Familie in M, wobei $I \neq \emptyset$.

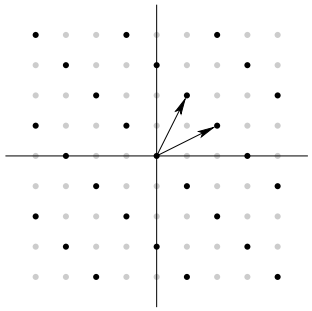
Der von $\mathcal{F}$ *erzeugte Untermodul* (auch die *lineare Hülle*, das *Erzeugnis*, der *Aufspann*) von $\mathcal{F}$ in M ist definiert

$$\mathrm{Lin}(\mathcal{F}) := \{u \in M;\ u \text{ ist Linearkombination über } \mathcal{F}\} \leq_R M.$$

Für $\mathcal{F} = (u_1, \ldots, u_k)$ schreiben wir auch $\mathrm{Lin}(u_1, \ldots, u_k)$ anstelle von $\mathrm{Lin}(\mathcal{F})$. Weiter definiert man die lineare Hülle der leeren Familie durch $\mathrm{Lin}(\,) := \{0_M\}$. Für eine Teilmenge $A \subseteq M$ setzt man auch

$$\langle A \rangle := \mathrm{Lin}(A) := \mathrm{Lin}((u)_{u \in A}) \leq_R M.$$

Beispiel 3.1.13. Für den von $v_1 := (2,1)$ und $v_2 := (1,2)$ erzeugten Untermodul $\mathrm{Lin}(v_1, v_2)$ in $\mathbb{Z}^2$ erhält man folgendes Bild;



Konstruktion 3.1.14. Es seien R ein K1-Ring, M ein R-Modul und $N_i \leq_R M$, $i \in I$, Untermoduln. Dann ist die *Summe* dieser Untermoduln der Untermodul

$$\sum_{i\in I} N_i \;:=\; \left\langle \bigcup_{i\in I} N_i \right\rangle \;=\; \left\{ \sum u_i;\; u_i \in N_i \right\} \;\leq_R\; M.$$

Definition 3.1.15. Es sei R ein K1-Ring. Ein *Homomorphismus* (auch *lineare Abbildung*) von R-Moduln M und N ist eine Abbildung $\varphi\colon M \to N$ mit

$$\varphi(u+u') \;=\; \varphi(u)+\varphi(u'), \qquad \varphi(r\cdot u) \;=\; r\cdot\varphi(u)$$

für alle $u, u' \in M$ und $r \in R$. Man nennt einen Modulhomomorphismus $\varphi\colon M \to N$ einen *Isomorphismus*, falls es einen Modulhomomorphismus $\psi\colon N \to M$ gibt mit

$$\psi \circ \varphi \;=\; \mathrm{id}_M, \qquad \varphi \circ \psi \;=\; \mathrm{id}_N;$$

man nennt M und N dann *isomorph* zueinander und schreibt dafür $M \cong N$. Weiter definiert man *Kern* und *Bild* eines Modulhomomorphismus $\varphi\colon M \to N$ als

$$\mathrm{Kern}(\varphi) \;:=\; \{u \in M;\; \varphi(u) = 0_N\}, \qquad \mathrm{Bild}(\varphi) \;:=\; \{\varphi(u);\; u \in M\}.$$

Bemerkung 3.1.16. Es seien G und H abelsche Gruppen.

(i) Eine Abbildung $\varphi\colon G \to H$ ist genau dann ein Homomorphismus der $\mathbb{Z}$-Moduln G und H, wenn sie ein Gruppenhomomorphismus ist.
(ii) G und H sind genau dann isomorph als $\mathbb{Z}$-Moduln, wenn sie als Gruppen isomorph sind.

Bemerkung 3.1.17. Die Komposition zweier Homomorphismen von R-Moduln ist stets wieder ein Homomorphismus von R-Moduln.

Bemerkung 3.1.18. Es seien R ein K1-Ring und $\varphi\colon M \to N$ ein Homomorphismus von R-Moduln.

(i) Für jeden Untermodul $M' \leq_R M$ ist das Bild $\varphi(M')$ ein Untermodul von N; insbesondere ist $\mathrm{Bild}(\varphi)$ ein Untermodul von N.
(ii) Für jeden Untermodul $N' \leq_R N$ ist das Urbild $\varphi^{-1}(N')$ ein Untermodul von M; insbesondere ist $\mathrm{Kern}(\varphi)$ ein Untermodul von M.
(iii) Der Homomorphismus $\varphi\colon M \to N$ ist genau dann injektiv, wenn $\mathrm{Kern}(\varphi) = \{0_M\}$ gilt.
(iv) Der Homomorphismus $\varphi\colon M \to N$ ist genau dann ein Isomorphismus, wenn er bijektiv ist.

Konstruktion 3.1.19. Es seien R ein K1-Ring und M_i, $i \in I$, eine Familie von R-Moduln und

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

das (mengentheoretische) direkte Produkt. Dann ist $\prod_{i\in I} M_i$ zusammen mit den komponentenweisen Verknüpfungen

$$\begin{aligned}(u_i)_{i\in I} \;+\; (u_i')_{i\in I} &:= (u_i + u_i')_{i\in I},\\ r\cdot(u_i)_{i\in I} &:= (r\cdot u_i)_{i\in I}\end{aligned}$$

ein R-Modul, das *direkte Produkt* der R-Moduln M_i, $i \in I$. Die *direkte Summe* der R-Moduln M_i, $i \in I$, ist der Untermodul

$$\begin{aligned}\bigoplus_{i\in I} M_i \;&:=\; \left\{(u_i)_{i\in I} \in \prod_{i\in I} M_i;\ u_i \neq 0 \text{ für höchstens endlich viele } i \in I\right\}\\ &\leq_R \prod_{i\in I} M_i.\end{aligned}$$

Die Projektionen auf die Faktoren liefern kanonische surjektive Modulhomomorphismen

$$\pi_j\colon \prod_{i\in I} M_i \to M_j,\quad (u_i)_{i\in I} \mapsto u_j, \qquad\qquad \pi_j\colon \bigoplus_{i\in I} M_i \to M_j,\quad (u_i)_{i\in I} \mapsto u_j.$$

Ist die Indexmenge I endlich, so stimmen direkte Summe und Produkt der Moduln M_i, $i \in I$, überein.

Konstruktion 3.1.20. Es seien R ein K1-Ring, M ein R-Modul und $N \leq_R M$ ein Untermodul. Dann hat man eine wohldefinierte Skalarmultiplikation

$$R \times M/N \;\to\; M/N, \qquad r\cdot(u+N) \;:=\; r\cdot u + N$$

Damit wird die Faktorgruppe M/N zu einem R-Modul, dem *Faktormodul* von M nach N.

Weiter hat man einen surjektiven Modulhomomorphismus $\pi\colon M \to M/N$ mit $\mathrm{Kern}(\pi) = N$, nämlich

$$\pi\colon M \;\to\; M/N, \qquad u \;\mapsto\; u + N.$$

Beweis. Wir wissen bereits, dass M/N eine abelsche Gruppe ist, und dass $\pi\colon M \to M/N$ ein surjektiver Gruppenhomomorphismus mit $\mathrm{Kern}(\pi) = N$ ist.

Um zu zeigen, dass die Skalarmultiplikation wohldefiniert ist, betrachten wir zwei $u, u' \in N$ mit $u + N = u' + N$. Dann gilt $u - u' \in N$. Für jedes $r \in R$ erhält man $r\cdot(u - u') = r\cdot u - r\cdot u' \in N$. Das bedeutet $r\cdot(u + N) = r\cdot(u' + N)$.

Es bleiben die Modulaxiome für die Skalarmultiplikation zu verifizieren. Offensichtlich gilt $1_R\cdot(u + N) = u + N$ für alle $u + N \in M/N$. Weiter haben wir für alle

$u, u' \in M$ und alle $r, r' \in R$:

$$\begin{aligned}
(r'r)\cdot(u+N) &= ((r'r)\cdot u)+N \\
&= (r'\cdot(r\cdot u))+N \\
&= r'\cdot((r\cdot u)+N) \\
&= r'\cdot(r\cdot(u+N)).
\end{aligned}$$

$$\begin{aligned}
(r+r')\cdot(u+N) &= ((r+r')\cdot u)+N \\
&= (r\cdot u + r'\cdot u)+N \\
&= (r\cdot u+N) \;+\; (r'\cdot u+N) \\
&= r\cdot(u+N) \;+\; r'\cdot(u+N).
\end{aligned}$$

$$\begin{aligned}
r\cdot((u+N)+(u'+N)) &= r\cdot((u+u')+N) \\
&= (r\cdot(u+u'))+N \\
&= (r\cdot u + r\cdot u')+N \\
&= (r\cdot u+N) \;+\; (r\cdot u'+N) \\
&= r\cdot(u+N) \;+\; r\cdot(u'+N).
\end{aligned}$$

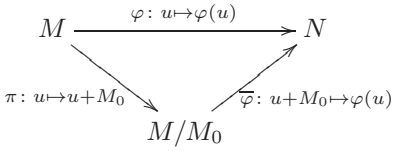
Es bleibt zu zeigen, dass die Abbildung $\pi\colon M \to M/N$ mit der Skalarmultiplikation verträglich ist. Für alle $u, u' \in v$ und alle $r, r' \in R$ gilt

$$\begin{aligned}
\pi(r\cdot u + r'\cdot u') &= (r\cdot u + r'\cdot u')+N \\
&= (r\cdot u+N)+(r'\cdot u'+N) \\
&= r\cdot(u+N)+r'\cdot(u'+N) \\
&= r\cdot\pi(u)+r'\cdot\pi(u').
\end{aligned}$$

□

Beispiel 3.1.21. Es seien R ein K1-Ring und $\mathfrak{a} \leq_R R$ ein Ideal. Dann ist der Faktorring $R/\mathfrak{a}$ ein R-Modul.

Satz 3.1.22 (Homomorphiesatz)**.** *Es seien R ein K1-Ring, $\varphi\colon M \to N$ ein Homomorphismus von R-Moduln, und $M_0 \leq_R M$ ein Untermodul mit $M_0 \subseteq \mathrm{Kern}(\varphi)$. Dann gibt es ein kommutatives Diagramm*



von wohldefinierten R-Modulhomomorphismen. Dabei ist der Modulhomomorphismus $\overline{\varphi}\colon M/M_0 \to N$ durch $\varphi\colon M \to N$ und das obige Diagramm eindeutig bestimmt. Es gilt weiter

(i) *$\overline{\varphi}$ ist injektiv $\Leftrightarrow$ $M_0 = \mathrm{Kern}(\varphi)$;*
(ii) *$\overline{\varphi}$ ist surjektiv $\Leftrightarrow$ φ ist surjektiv.*

Beweis. Der Homomorphiesatz 1.2.17 liefert die entsprechenden Aussagen für die abelschen Gruppen M, N und M/M_0. Es ist daher nur noch zu zeigen, dass $\overline{\varphi}\colon M/M_0 \to N$ mit der Skalarmultiplikation verträglich ist. Das ergibt sich jedoch sofort mit

$$\overline{\varphi}(r\cdot(u+M_0)) \;=\; \varphi(r\cdot u) \;=\; r\cdot\varphi(u) \;=\; r\cdot\overline{\varphi}(u+M_0).$$

□

Folgerung 3.1.23. *Es seien R ein K1-Ring und $\varphi\colon M \to N$ ein surjektiver Homomorphismus von R-Moduln. Dann hat man einen Isomorphismus von R-Moduln*

$$\overline{\varphi}\colon M/\mathrm{Kern}(\varphi) \;\to\; N, \qquad u+\mathrm{Kern}(\varphi) \;\mapsto\; \varphi(u).$$

Aufgaben zu Abschnitt 3.1.

Aufgabe 3.1.24. Es seien $\mathbb{K}$ ein Körper, $V := \mathbb{K}^n$ und $A \in \mathrm{Mat}(n,n;\mathbb{K})$. Betrachte die durch $\varphi\colon V \to V$, $v \mapsto A\cdot v$ definierte $\mathbb{K}[T]$-Modulstruktur auf V und zeige:

(i) Es seien ein Polynom $\sum a_\nu T^\nu \in \mathbb{K}[T]$ und ein Vektor $v \in V$ gegeben. Dann gilt
$$\Big(\sum a_\nu T^\nu\Big)\cdot v \;=\; \sum a_\nu (A^\nu \cdot v)$$

(ii) Ist A diagonalisierbar mit den Eigenwerten $\lambda_1,\ldots,\lambda_k$, wobei $\lambda_i \neq \lambda_j$ für $i \neq j$ und $k \leq n$, so gilt
$$((T-\lambda_1)\cdots(T-\lambda_k))\cdot v \;=\; 0_V \quad \text{für alle } v \in V.$$

Aufgabe 3.1.25. Es seien $\mathbb{K}$ ein Körper und $V := \mathbb{K}^3$, und es sei $A \in \mathrm{Mat}(3,3;\mathbb{K})$ gegeben durch
$$A \;:=\; \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$
Betrachte die durch $\varphi\colon V \to V$, $v \mapsto A\cdot v$ definierte $\mathbb{K}[T]$-Modulstruktur auf V und bestimme die Vektoren
$$(T-1)\cdot e_1, \qquad (T-1)\cdot e_2, \qquad (T-1)^2\cdot e_2, \qquad (T-2)\cdot e_3.$$

Aufgabe 3.1.26. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ eine lineare Abbildung. Betrachte die zugehörige $\mathbb{K}[T]$-Modulstruktur auf V und zeige, dass für jede Teilmenge $U \subseteq V$ die folgenden Aussagen äquivalent sind:

(i) U ist ein Untermodul des $\mathbb{K}[T]$-Moduls V,
(ii) U ist ein Untervektorraum des $\mathbb{K}$-Vektorraumes V, und es gilt $\varphi(U) \subseteq U$.

Aufgabe 3.1.27. Es seien R ein K1-Ring und $\varphi\colon M \to N$ ein Homomorphismus von R-Moduln. Beweise die Aussagen aus Bemerkung 3.1.18:

(i) Für jeden Untermodul $M' \leq_R M$ ist das Bild $\varphi(M')$ ein Untermodul von N; insbesondere ist Bild(φ) ein Untermodul von N.
(ii) Für jeden Untermodul $N' \leq_R N$ ist das Urbild $\varphi^{-1}(N')$ ein Untermodul von M; insbesondere ist Kern(φ) ein Untermodul von M.
(iii) Der Homomorphismus $\varphi\colon M \to N$ ist genau dann injektiv, wenn Kern$(\varphi) = \{0\}$ gilt.
(iv) Der Homomorphismus $\varphi\colon M \to N$ ist genau dann ein Isomorphismus, wenn er bijektiv ist.

Aufgabe 3.1.28. Es seien $v_1 := (2,1)$ und $v_2 := (1,2)$ und $N := \mathrm{Lin}(v_1,v_2) \leq_{\mathbb{Z}} \mathbb{Z}^2$. Zeige: Es gilt $\mathbb{Z}^2/N \cong \mathbb{Z}/3\mathbb{Z}$.

Aufgabe 3.1.29. Es sei M ein $\mathbb{Z}$-Modul, sodass $M = \mathbb{Z}\cdot u$ für ein $u \in M$ gilt. Zeige:

(i) Es gilt $M \cong \mathbb{Z}/n\mathbb{Z}$ mit einem eindeutig bestimmten $n \in \mathbb{Z}_{\geq 0}$. *Hinweis:* Konstruiere einen surjektiven Homomorphismus $\mathbb{Z} \to M$ mit $1 \mapsto u$.
(ii) Ist n wie in (i) und gilt $n = p_1^{\nu_1}\cdots p_r^{\nu_r}$ mit paarweise verschiedenen Primzahlen $p_1,\ldots,p_r \in \mathbb{Z}_{\geq 2}$, so hat man einen $\mathbb{Z}$-Modulisomorphismus
$$M \;\cong\; \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_r^{\nu_r}\mathbb{Z}.$$

Aufgabe 3.1.30. Es sei M ein $\mathbb{Z}$-Modul. Zeige: Ist $p := |M|$ eine Primzahl, so gilt $M \cong \mathbb{Z}/p\mathbb{Z}$.

Aufgabe 3.1.31 (Isomorphiesätze für Moduln)**.** Es seien R ein K1-Ring und M ein R-Modul. Zeige:

(i) Für je zwei Untermoduln $L \leq_R M$ und $N \leq_R M$ hat man einen kanonischen Isomorphismus
$$N/(N\cap L) \;\to\; (N+L)/L, \qquad v+(N\cap L) \;\mapsto\; v+L.$$

(ii) Für jede Schachtelung $L \leq_R N \leq_R M$ von Untermoduln hat man einen kanonischen Isomorphismus

$$M/L\Big/N/L \;\to\; M/N, \qquad (u+L)+(N/L) \;\mapsto\; u+N.$$

3.2. **Freie Moduln.**

Definition 3.2.1. Es seien R ein K1-Ring und M ein R-Modul.

(i) Eine Familie $\mathcal{F} = (u_i)_{i\in I}$ in M heißt *Erzeugendensystem für M*, falls jedes $u \in M$ eine R-Linearkombination über $\mathcal{F}$ ist.
(ii) Eine Familie $\mathcal{F} = (u_i)_{i\in I}$ in M heißt *linear unabhängig*, falls für jede R-Linearkombination $\sum r_i u_i$ über $\mathcal{F}$ gilt

$$\sum r_i u_i \;=\; 0_M \quad\Longrightarrow\quad r_i \;=\; 0_R \text{ für alle } i \in I.$$

(iii) Der R-Modul M heißt *endlich erzeugt*, falls er ein endliches Erzeugendensystem besitzt.
(iv) Der R-Modul M heißt *frei*, falls $M = \{0_M\}$ gilt oder M eine *Basis*, d.h., ein linear unabhängiges Erzeugendensystem, besitzt.

Beispiel 3.2.2. Es seien R ein K1-Ring und $I \neq \emptyset$ eine Menge. Dann ist der R-Modul $R^I_\oplus := \bigoplus_{i\in I} R$ frei; er besitzt eine kanonische Basis $(e_i)_{i\in I}$, wobei

$$e_i \;:=\; (\delta_{ij})_{j\in I} \quad \text{mit } \delta_{ij} \;:=\; \begin{cases} 1_R & \text{falls } j = i, \\ 0_R & \text{falls } j \neq i. \end{cases}$$

Beispiel 3.2.3. In $\mathbb{Z}^2$ betrachten wir die Elemente $v_1 := (2, 1)$ und $v_2 := (1, 2)$. Dann ist $\mathcal{F} := (v_1, v_2)$ linear unabhängig aber nicht erzeugend; beispielsweise kann man $(1, 0)$ nicht als $\mathbb{Z}$-Linearkombination über $\mathcal{F}$ darstellen.

Beispiel 3.2.4. Der $\mathbb{Z}$-Modul $\mathbb{Z}/2\mathbb{Z}$ ist nicht frei. Es gilt $2 \cdot \overline{1} = \overline{0}$ in $\mathbb{Z}/2\mathbb{Z}$, aber wir haben $2 \neq 0$ in $\mathbb{Z}$.

Satz 3.2.5. *Es seien R ein K1-Ring und M ein R-Modul mit Basis $\mathcal{B} = (u_i)_{i\in I}$. Dann besitzt jedes $u \in M$ eine eindeutige Darstellung*

$$u \;=\; \sum_{i\in I} r_i \cdot u_i \quad \textit{mit } r_i \in R. \tag{3.2.5.1}$$

Beweis. Da $\mathcal{B}$ ein Erzeugendensystem für M ist, besitzt jedes $u \in M$ eine Darstellung (3.2.5.1).

Zum Nachweis der Eindeutigkeit seien zwei Darstellungen $u = \sum_{i\in I} r_i \cdot u_i$ und $u = \sum_{i\in I} s_i \cdot u_i$ gegeben. Dann erhalten wir

$$\begin{aligned} 0_M &= u - u \\ &= \sum_{i\in I} r_i \cdot u_i \;-\; \sum_{i\in I} s_i \cdot u_i \\ &= \sum_{i\in I} (r_i - s_i) \cdot u_i. \end{aligned}$$

Da $\mathcal{B}$ linear unabhängig ist, muss $r_i = s_i$ für jedes $i \in I$ gelten. Folglich stimmen die Darstellungen von u überein. □

Definition 3.2.6. Es seien R ein K1-Ring und M ein R-Modul mit Basis $\mathcal{B} = (u_i)_{i\in I}$. Für jedes $u \in M$ nennt man die Darstellung

$$u \;=\; \sum_{i\in I} r_i \cdot u_i$$

die *Entwicklung* von u nach der Basis $\mathcal{B}$, und man nennt $x_\mathcal{B}(u) := (r_i)_{i\in I} \in R^I_\oplus$ den *Koordinatenvektor* von u bezüglich $\mathcal{B}$.

Satz 3.2.7. *Es seien R ein K1-Ring und M ein freier R-Modul mit einer Basis $B = (u_i)_{i\in I}$. Weiter seien und N ein R-Modul und $(v_i)_{i\in I}$ eine Familie in N.*

(i) *Es gibt einen eindeutig bestimmten Homomomorphismus $\varphi\colon M \to N$ mit $\varphi(u_i) = v_i$ für alle $i \in I$, nämlich*

$$\varphi\left(\sum_{i\in I} r_i\cdot u_i\right) \ := \ \sum_{i\in I} r_i\cdot v_i.$$

(ii) *Der Homomorphismus $\varphi\colon M \to N$ aus (ii) ist genau dann ein Isomorphismus, wenn $(v_i)_{i\in I}$ eine Basis für N ist.*

Beweis. Zu (i). Wegen der Eindeutigkeit des Koordinatenvektors ist die Abbildung $\varphi\colon M \to N$ wohldefiniert. Weiter haben wir $\varphi(u_i) = v_i$.

Zum Nachweis der Linearität seien $u, u' \in M$ und $a, a' \in \mathbb{K}$ gegeben. Wir betrachten die Entwicklungen

$$u \ = \ \sum_{i\in I} r_i\cdot u_i, \qquad\qquad u' \ = \ \sum_{i\in I} r'_i\cdot u_i$$

bezüglich der Basis $\mathcal{B} = (u_i)_{i\in I}$ von M. Gemäß unserer Definition von φ erhalten wir dann

$$\begin{aligned}
\varphi(a\cdot u + a'\cdot u') &= \varphi\left(\sum_{i=1}^{n}(ar_i + a'r'_i)\cdot u_i\right)\\
&= \sum_{i=1}^{n}(ar_i + a'r'_i)\cdot v_i\\
&= \sum_{i=1}^{n}(ar_i)\cdot v_i \ + \ \sum_{i=1}^{n}(a'r'_i)\cdot v_i\\
&= a\cdot\sum_{i=1}^{n} r_i\cdot v_i \ + \ a'\cdot\sum_{i=1}^{n} r'_i\cdot v_i\\
&= a\cdot\varphi(v) \ + \ a'\cdot\varphi(v').
\end{aligned}$$

Es bleibt zu zeigen, dass φ durch die Vorgabe der Werte v_i auf den u_i eindeutig bestimmt ist. Ist $\varphi'\colon M \to N$ eine weitere lineare Abbildung mit $\varphi'(u_i) = v_i$, so erhalten wir für jedes $u = \sum r_i\cdot u_i$:

$$\varphi'(u) \ = \ \varphi'\left(\sum r_i\cdot u_i\right) \ = \ \sum r_i\cdot\varphi'(u_i) \ = \ \sum r_i\cdot\varphi(u_i) \ = \ \varphi\left(\sum r_i\cdot u_i\right) \ = \ \varphi(u).$$

Zu (ii). Es sei zunächst $\varphi\colon M \to N$ ein Isomorphismus. Wir zeigen, dass $\mathcal{C} := (v_i)_{i\in I}$ ein Erzeugendensystem für N ist. Dazu sei $v \in N$ gegeben. Da φ surjektiv ist, gibt es ein $u \in M$ mit $\varphi(u) = v$. Ist $u = \sum r_i\cdot u_i$ die Etwicklung von u bezüglich $\mathcal{B}$, so erhalten wir

$$v \ = \ \varphi(u) \ = \ \varphi\left(\sum_{i\in I} r_i\cdot u_i\right) \ = \ \sum_{i\in I} r_i\cdot v_i \ \in \ \mathrm{Lin}(\mathcal{C})$$

Zum Nachweis der linearen Unabhängigkeit von $\mathcal{C} = (v_i)_{i\in I}$ sei eine Linearkombination $\sum r_i\cdot v_i = 0_N$ gegeben. Dann erhalten wir

$$0_M \ = \ \varphi^{-1}(0_N) \ = \ \varphi^{-1}\left(\sum_{i\in I} r_i\cdot v_i\right) \ = \ \sum_{i\in I} r_i\cdot u_i,$$

wobei $\varphi^{-1}\colon N \to M$ den Umkehrhomomorphismus bezeichnet. Da $(u_i)_{i\in I}$ linear unabhängig ist, ergibt sich $r_i = 0_R$ für alle $i \in I$.

Es sei nun $(v_i)_{i\in I}$ eine Basis für N. Dann erhält man nach (i) einen Homomorphismus $\psi\colon N \to M$ mit $\psi(v_i) = u_i$ für alle $i \in I$. Wir zeigen, dass ψ eine Umkehrabbildung zu φ ist: Es gilt stets

$$\varphi \circ \psi \left(\sum_{i\in I} r_i \cdot v_i \right) \;=\; \varphi \left(\sum_{i\in I} r_i \cdot u_i \right) \;=\; \sum_{i\in I} r_i \cdot v_i,$$

$$\psi \circ \varphi \left(\sum_{i\in I} r_i \cdot u_i \right) \;=\; \psi \left(\sum_{i\in I} r_i \cdot v_i \right) \;=\; \sum_{i\in I} r_i \cdot u_i.$$

□

Folgerung 3.2.8. *Es seien R ein $K1$-Ring und M eine freier R-Modul mit Basis $\mathcal{B} = (u_i)_{i\in I}$. Dann hat man einen Isomorphismus*

$$\varphi_{\mathcal{B}}\colon M \;\to\; R^I_{\oplus}, \qquad u \;\mapsto\; x_{\mathcal{B}}(u).$$

Folgerung 3.2.9. *Ein freier R-Modul M ist genau dann endlich erzeugt, wenn er eine endliche Basis besitzt.*

Beweis. Besitzt M eine endliche Basis, so ist M auch endlich erzeugt. Es sei nun M endlich erzeugt. Als freier Modul besitzt M dann eine Basis $\mathcal{B} = (u_i)_{i\in I}$. Nach Folgerung 3.2.8 ist M isomorph zu $R^I_{\oplus}$; insbesondere ist letzterer Modul ebenfalls endlich erzeugt. Das geht nur, wenn I endlich ist. □

Satz 3.2.10. *Es sei R ein Integritätsring und M ein freier R-Modul. Dann besitzen je zwei Basen von M die gleiche Länge.*

Beweis. Da M frei ist, dürfen wir annehmen, dass $M = \bigoplus_{i\in I} R$ gilt. Es sei $\mathbb{K} := Q(R)$ der Quotientenkörper von R. Dann hat man einen injektiven Homomorphismus von R-Moduln

$$\Phi\colon \bigoplus_{i\in I} R \;\to\; \bigoplus_{i\in I} \mathbb{K}, \qquad (a_i) \;\mapsto\; \left(\frac{a_i}{1_R} \right)$$

Da je zwei Vektorraumbasen dieselbe Länge besitzen, genügt es zu zeigen, dass für jede Basis $(u_j)_{j\in J}$ für M die Bildfamilie $\mathcal{C} := (\Phi(u_j))_{j\in J}$ eine Basis für den $\mathbb{K}$-Vektorraum $V := \bigoplus_{i\in I} \mathbb{K}$ ist.

Um zu sehen, dass $\mathcal{C}$ ein Erzeugendensystem für V ist, betrachten wir ein beliebiges Element $v \in V$. Dieses ist von der Form

$$v \;=\; \left(\frac{a_i}{b_i} \right)_{i\in I}, \quad a_i \neq 0_R \text{ für nur endlich viele } i \in I.$$

Bezeichnet $b \in R$ das Produkt über alle b_i mit $a_i \neq 0_R$, so gilt $b{\cdot}v \in \Phi(M)$. Folglich gibt es eine Darstellung

$$v \;=\; \frac{1_R}{b}\cdot(b\cdot v) \;=\; \frac{1_R}{b}\cdot\Phi \left(\sum_{j\in J} c_j \cdot u_j \right) \;=\; \sum_{j\in J} \frac{c_j}{b}\cdot(\Phi(u_j)).$$

Wir kommen zur linearen Unabhängigkeit. Dazu betrachten wir eine Darstellung des Nullvektors als Linearkombination

$$0_V \;=\; \sum_{j\in J} \frac{a_j}{b_j}\cdot\Phi(u_j).$$

Ähnlich wie vorhin sei $b \in R$ das Produkt über alle b_j mit $a_j \neq 0_R$. Dann erhalten wir mit $b'_j := b/b_j$:

$$0_V \;=\; \frac{b}{1_R}\cdot\sum_{j\in J}\frac{a_j}{b_j}\cdot\Phi(u_j) \;=\; \sum_{j\in J}\frac{b'_j a_j}{1_R}\cdot\Phi(u_j) \;=\; \Phi\left(\sum_{j\in J} b'_j a_j\cdot u_j\right).$$

Da Φ injektiv ist, muss der Ausdruck in der letzten Klammer gleich 0_M sein. Die lineare Unabhängigkeit von $\mathcal{B}$ liefert $b'_j a_j = 0_R$ für alle $j \in J$. Mit $b'_j \neq 0_R$ folgt $a_j = 0_R$ und somit $a_j/b_j = 0_{\mathbb{K}}$ für alle $j \in J$. □

Definition 3.2.11. Es seien R ein Integritätsring und M ein freier R-Modul. Dann definiert man den *Rang* von M durch

$$\operatorname{rg}(M) \;:=\; \begin{cases}\infty & \text{falls } M \text{ keine endliche Basis besitzt,}\\ n & \text{falls } M \text{ eine Basis } (u_1,\ldots,u_n) \text{ besitzt.}\end{cases}$$

Beispiel 3.2.12. Der freie $\mathbb{Z}$-Modul $\mathbb{Z}^2$ besitzt den Rang 2. Der durch $v_1 = (2,1)$ und $v = (1,2)$ erzeugte Untermodul $M \leq_{\mathbb{Z}} \mathbb{Z}^2$ besitzt ebenfalls den Rang 2. Man beachte, dass $M \neq \mathbb{Z}^2$ gilt.

Satz 3.2.13. *Es seien R ein Hauptidealring und F ein endlich erzeugter freier R-Modul. Ist $M \leq_R F$ ein Untermodul, so ist M frei und es gilt* $\operatorname{rg}(M) \leq \operatorname{rg}(F)$.

Beweis. Es ist nur für $F \neq \{0_F\}$ etwas zu zeigen. Es sei $(v_1,\ldots,v_r)$ eine Basis für F. Für $0 \leq n \leq r$ betrachten wir die Untermoduln

$$M_n \;:=\; M \,\cap\, \operatorname{Lin}(v_1,\ldots,v_n).$$

Es gilt also $M_r = M$. Wir zeigen durch Induktion über n, dass M_n frei ist mit $\operatorname{rg}(M_n) \leq n$.

Im Fall $n = 0$ haben wir $M_n = \{0_F\}$ und die Aussage ist offensichtlich. Im Induktionsschritt betrachten wir die Teilmenge

$$\mathfrak{a} \;:=\; \{a \in R;\; a_1\cdot v_1 + \ldots + a_{n-1}\cdot v_{n-1} + a\cdot v_n \in M \text{ für } a_1,\ldots,a_{n-1} \in R\} \;\subseteq\; R.$$

Offensichtlich ist $\mathfrak{a}$ ein Ideal in R. Da R ein Hauptidealring ist, haben wir $\mathfrak{a} = \langle a_n\rangle$ mit einem $a_n \in R$.

Falls $a_n = 0_R$ gilt, erhalten wir $M_n = M_{n-1}$. Nach Induktionsvoraussetzung ist M_n dann frei mit $\operatorname{rg}(M_n) \leq n$. Gilt $a_n \neq 0_R$, so wählen wir ein

$$v \;=\; a_1\cdot v_1 + \ldots + a_{n-1}\cdot v_{n-1} + a_n\cdot v_n \;\in\; M_n.$$

Weiter sei $(\widetilde{v}_1,\ldots,\widetilde{v}_k)$ eine Basis für M_{n-1}. Wir zeigen, dass $(\widetilde{v}_1,\ldots,\widetilde{v}_k, v)$ eine Basis für M_n ist. Für jedes $w \in M_n$ erhalten wir eine Darstellung

$$\begin{aligned} w &= b_1\cdot v_1 + \ldots + b_{n-1}\cdot v_{n-1} + b_n\cdot v_n\\ &= b_1\cdot v_1 + \ldots + b_{n-1}\cdot v_{n-1} + ba_n\cdot v_n\\ &= (b_1 - ba_1)\cdot v_1 + \ldots + (b_{n-1} - ba_{n-1})\cdot v_{n-1} + b\cdot v\\ &\in \operatorname{Lin}(\widetilde{v}_1,\ldots,\widetilde{v}_k, v). \end{aligned}$$

Zum Nachweis der linearen Unabhängigkeit sei $b_1\cdot\widetilde{v}_1 + \ldots + b_k\cdot\widetilde{v}_k + b\cdot v = 0_M$ gegeben. Dann hat man

$$b_1\cdot\widetilde{v}_1 + \ldots + b_k\cdot\widetilde{v}_k + ba_1\cdot v_1 + \ldots + ba_{n-1}\cdot v_{n-1} + ba_n\cdot v_n \;=\; 0_M.$$

Die lineare Unabhängigkeit von $(v_1,\ldots,v_n)$ liefert zunächst $ba_n = 0_R$ und somit $b = 0_R$. Da $(\widetilde{v}_1,\ldots,\widetilde{v}_k)$ linear unabhängig ist, ergibt sich $b_1 = \ldots = b_k = 0_R$. □

Aufgaben zu Abschnitt 3.2.

Aufgabe 3.2.14. Es sei R ein K1-Ring. Zeige: Zu jedem R-Modul M gibt es einen surjektiven Modulhomomorphismus $F \to M$ mit einem freien R-Modul F. *Hinweis:* Betrachte $F := \oplus_M R$.

Aufgabe 3.2.15. Es seien $a_1, \ldots, a_n \in \mathbb{Z}$, und es sei $v := (a_1, \ldots, a_n)$. Beweise die Äquivalenz folgender Aussagen:

(i) Es gibt eine Basis $(v, v_2, \ldots, v_n)$ für $\mathbb{Z}^n$.
(ii) Die Zahlen $a_1, \ldots, a_n$ sind teilerfremd.

3.3. **Matrizen und lineare Abbildungen.**

Definition 3.3.1. Es sei R ein K1-Ring. Eine $(m \times n)$-*Matrix über* R ist eine Anordnung von Elementen $a_{ij} \in R$ in ein Schema

$$A \;=\; (a_{ij})_{\substack{1\le i\le m\\ 1\le j\le n}} \;=\; \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}.$$

Die Menge aller $m \times n$-Matrizen über R bezeichnen wir mit $\mathrm{Mat}(m,n;R)$. Die i-te Zeile A_{i*} und die j-te Spalte A_{*j} von $A \in \mathrm{Mat}(m,n;R)$ sind gegeben durch

$$A_{i*} \;:=\; (a_{i1},\dots,a_{in}), \qquad A_{*j} \;:=\; \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}.$$

Für $(m\times n)$-Matrizen $A=(a_{ij})$ und $B=(b_{ij})$ über R erklären wir die Summe und das skalare Vielfache mit $r \in R$ komponentenweise durch

$$(a_{ij}) + (b_{ij}) \;:=\; (a_{ij}+b_{ij}), \qquad\qquad r\cdot(a_{ij}) \;:=\; (ra_{ij}).$$

Sind eine Matrix $A=(a_{ij}) \in \mathrm{Mat}(m,n;R)$ und ein Element $x=(x_1,\dots,x_n) \in R^n$ gegeben, so definiert man das Das *Matrix-Vektor-Produkt* von A und x als

$$A\cdot x \;:=\; \begin{pmatrix} A_{1*}\cdot x \\ \vdots \\ A_{m*}\cdot x \end{pmatrix} \;=\; \begin{pmatrix} a_{11}x_1+\ldots+a_{1n}x_n \\ \vdots \\ a_{m1}x_1+\ldots+a_{mn}x_n \end{pmatrix} \;\in\; R^m.$$

Sind $A=(a_{ij})$ eine $(m\times n)$-Matrix und $B=(b_{jk})$ eine $(n\times l)$-Matrix über R, so ist das *Matrizenprodukt* von A und B die $(m\times l)$-Matrix

$$A\cdot B \;:=\; (c_{ik})_{\substack{1\le i\le m\\ 1\le k\le l}} \;\in\; \mathrm{Mat}(m,l;R), \qquad \text{wobei } c_{ik} \;:=\; \sum_{j=1}^{n} a_{ij}b_{jk} \;=\; A_{i*}\cdot B_{*k}.$$

Die *Transponierte* A^t der Matrix $A=(a_{ij}) \in \mathrm{Mat}(m,n;R)$ besitzt genau die Zeilen von A als Spalten, d.h., sie ist definiert durch

$$A^t \;:=\; (a_{ji})_{\substack{1\le i\le n\\ 1\le j\le m}} \;\in\; \mathrm{Mat}(n,m;R).$$

Satz 3.3.2. *Es sei R ein K1-Ring.*

(i) *Die Menge* $\mathrm{Mat}(m,n;R)$ *ist zusammen mit der komponentenweise definierten Addition und Skalarmultiplikation ein R-Modul.*

(ii) *Für je zwei Matrizen $A,B \in \mathrm{Mat}(m,n;R)$ und je zwei Elemente $x,y \in R^n$ gilt*

$$\begin{aligned} A\cdot(x+y) &= A\cdot x + A\cdot y, & A\cdot(r\cdot x) &= r\cdot(A\cdot x),\\ (A+B)\cdot x) &= A\cdot x + B\cdot x, & (r\cdot A)\cdot x &= r\cdot(A\cdot x). \end{aligned}$$

(iii) *Für je drei Matrizen $A \in \mathrm{Mat}(m,n;R)$, $B \in \mathrm{Mat}(n,l;R)$ und $C \in \mathrm{Mat}(l,k;R)$ hat man*

$$(A\cdot B)\cdot C \;=\; A\cdot(B\cdot C).$$

Für alle Matrizen $A \in \mathrm{Mat}(m,n;R)$, $B,C \in \mathrm{Mat}(n,l;R)$ und $D \in \mathrm{Mat}(l,k;R)$ hat man

$$\begin{aligned} A\cdot(B+C) &= A\cdot B + A\cdot C,\\ (B+C)\cdot D &= B\cdot D + C\cdot D. \end{aligned}$$

(iv) *Die Einheitsmatrix* $E_n \in \mathrm{Mat}(n,n;R)$ *verhält sich neutral, d.h., für* $A \in \mathrm{Mat}(m,n;R)$ *und* $B \in \mathrm{Mat}(n,l;R)$ *gilt stets*

$$A \cdot E_n \;=\; A, \qquad\qquad E_n \cdot B \;=\; B.$$

(v) $\mathrm{Mat}(n,n;R)$ *ist zusammen mit der komponentenweisen Addition und der Matrizenmultiplikation ein Ring; es gilt* $1_{\mathrm{Mat}(n,n;R)} = E_n$ *und*

$$\mathrm{Mat}(n,n;R)^* \;=\; \{A \in \mathrm{Mat}(n,n;R);\ A \text{ ist invertierbar}\}.$$

(vi) *Für je zwei Matrizen* $A, B \in \mathrm{Mat}(m,n;R)$ *und jedes* $\lambda \in R$ *gilt*

$$(A+B)^t \;=\; A^t + B^t, \qquad (\lambda \cdot A)^t \;=\; \lambda \cdot A^t, \qquad (A^t)^t \;=\; A.$$

(vii) *Für je zwei Matrizen* $A \in \mathrm{Mat}(m,n;R)$ *und* $B \in \mathrm{Mat}(n,l;R)$ *gilt*

$$(A \cdot B)^t \;=\; B^t \cdot A^t.$$

Beweis. In den Beweisen der entsprechenden Aussagen für Matrizen über einem Körper $\mathbb{K}$ aus [1, §§ 4.2 und 4.4] wurden von $\mathbb{K}$ nur die Eigenschaften eines K1-Ringes verwendet. □

Bemerkung 3.3.3. Es sei R ein Integritätsring. Dann besitzt R einen Quotientenkörper

$$Q(R) \;=\; \left\{\frac{a}{b};\ a,b \in R,\, b \neq 0_R\right\}, \qquad \text{wobei} \quad \frac{a_1}{b_1} = \frac{a_2}{b_2} \iff a_1 b_2 = b_1 a_2.$$

Dabei kann man R als Unterring seines Quotientenkörpers auffassen vermöge des kanonischen Homomorphismus

$$\imath\colon R \;\to\; Q(R), \qquad a \;\mapsto\; \frac{a}{1_R}.$$

Darüber kann man R^n als Teilmenge von $Q(R)^n$ und $\mathrm{Mat}(m,n;R)$ als Teilmenge von $\mathrm{Mat}(m,n;Q(R))$ auffassen; konkret sind die Identifikationen gegeben durch

$$\imath\colon R^n \;\to\; Q(R)^n, \qquad (x_1,\ldots,x_n) \;\mapsto\; \left(\frac{x_1}{1_R},\ldots,\frac{x_n}{1_R}\right),$$

$$\imath\colon \mathrm{Mat}(m,n;R) \;\to\; \mathrm{Mat}(m,n;Q(R)), \qquad (a_{ij}) \;\mapsto\; \left(\frac{a_{ij}}{1_R}\right).$$

Diese Identifikationen sind verträglich mit der Matrix-Vektor-Multiplikation sowie der Matrizenmultiplikation; es gilt

$$\imath(A \cdot x) \;=\; \begin{pmatrix} \frac{a_{11}x_1+\ldots+a_{1n}x_n}{1_R} \\ \vdots \\ \frac{a_{m1}x_1+\ldots+a_{mn}x_n}{1_R} \end{pmatrix} \;=\; \begin{pmatrix} \frac{a_{11}}{1_R}\frac{x_1}{1_R} + \ldots + \frac{a_{1n}}{1_R}\frac{x_n}{1_R} \\ \vdots \\ \frac{a_{m1}}{1_R}\frac{x_1}{1_R} + \ldots + \frac{a_{mn}}{1_R}\frac{x_n}{1_R} \end{pmatrix} \;=\; \imath(A) \cdot \imath(x).$$

$$\imath(A \cdot B) \;=\; \left(\frac{\sum a_{ij}b_{jk}}{1_R}\right) \;=\; \left(\sum \frac{a_{ij}}{1_R}\frac{b_{jk}}{1_R}\right) \;=\; \imath(A) \cdot \imath(B).$$

Satz 3.3.4. *Es seien* R *ein K1-Ring und* M *sowie* N *freie* R*-Moduln mit Basen* $\mathcal{B} := (u_1,\ldots,u_n)$ *sowie* $\mathcal{C} := (v_1,\ldots,v_m)$.

(i) *Zu jeder Matrix* $A \in \mathrm{Mat}(m,n;R)$ *gibt es einen eindeutig bestimmten Modulhomomorphismus* $\mu_{\mathcal{C}}^{\mathcal{B}}(A)\colon M \to N$ *mit der das folgende Diagramm kommutativ wird*

$$\begin{array}{ccc} M & \xrightarrow{\mu_{\mathcal{C}}^{\mathcal{B}}(A)} & N \\ {\scriptstyle \varphi_{\mathcal{B}}\colon u \mapsto x_{\mathcal{B}}(u)}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \varphi_{\mathcal{C}}\colon v \mapsto x_{\mathcal{C}}(v)} \\ R^n & \xrightarrow[\mu_A\colon x \mapsto A\cdot x]{} & R^m \end{array}$$

(ii) *Zu jedem Modulhomomorphismus $\varphi\colon M \to N$ hat man ein kommutatives Diagramm*

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & N \\ {\scriptstyle \varphi_{\mathcal{B}}\colon u\mapsto x_{\mathcal{B}}(u)}\downarrow{\scriptstyle \cong} & & {\scriptstyle \cong}\downarrow{\scriptstyle \varphi_{\mathcal{C}}\colon v\mapsto x_{\mathcal{C}}(v)} \\ R^n & \xrightarrow[x\mapsto M_{\mathcal{C}}^{\mathcal{B}}(\varphi)\cdot x]{} & R^m \end{array}$$

mit einer eindeutig bestimmten Matrix $M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \in \mathrm{Mat}(m,n;R)$; diese ist gegeben durch $M_{\mathcal{C}}^{\mathcal{B}}(\varphi) = (x_{\mathcal{C}}(\varphi(u_1)), \ldots, x_{\mathcal{C}}(\varphi(u_n)))$

Beweis. Zu (i). Die Abbildung $\mu_A\colon R^n \to R^m$, $x \mapsto A\cdot x$ ist linear. Der Homomorphismus $\mu_{\mathcal{C}}^{\mathcal{B}}(A)$ ist dann gegeben (und festgelegt) durch $\mu_{\mathcal{C}}^{\mathcal{B}}(A) = \varphi_{\mathcal{C}}^{-1} \circ \mu_A \circ \varphi_{\mathcal{B}}$.

Zu (ii). Der Homomorphismus $x \mapsto M_{\mathcal{C}}^{\mathcal{B}}(\varphi)\cdot x$ macht das Diagramm kommutativ, da er auf den Basisvektoren $e_1, \ldots, e_n \in R^n$ dieselben Werte annimmt wie $\varphi_{\mathcal{C}} \circ \varphi \circ \varphi_{\mathcal{B}}^{-1}$; siehe Satz 3.2.7. Dies legt die Spalten der Matrix $M_{\mathcal{C}}^{\mathcal{B}}(\varphi)$ auch schon fest: Es gilt

$$M_{\mathcal{C}}^{\mathcal{B}}(\varphi)_{*j} \;=\; M_{\mathcal{C}}^{\mathcal{B}}(\varphi)\cdot e_i \;=\; x_{\mathcal{C}}(\varphi(u_j)).$$

□

Konstruktion 3.3.5. Es seien R ein K1-Ring und M sowie N zwei R-Moduln. Dann wird Menge $\mathrm{Hom}(M,N)$ aller Modulhomomorphismen von M nach N zu einem R-Modul durch die punktweisen Verknüpfungen:

$$(\varphi+\psi)(u) \;:=\; \varphi(v)+\psi(u), \qquad (r\cdot\varphi)(u) \;:=\; r\cdot\varphi(u).$$

Das Nullelement in $\mathrm{Hom}(M,N)$ ist die Nullabbildung $M \to N$, $u \mapsto 0_N$. Weiter wird die Menge $\mathrm{End}(M) := \mathrm{Hom}(M,M)$ der Endomorphismen von M zu einem Ring durch

$$(\varphi+\psi)(u) \;:=\; \varphi(u)+\psi(u), \qquad \varphi\cdot\psi \;:=\; \varphi\circ\psi.$$

Der Endomorphismenring $\mathrm{End}(M)$ besitzt die Identität id_M als Einselement, und die Gruppe seiner Einheiten ist gegeben durch

$$\mathrm{End}(M)^* \;=\; \{\varphi \in \mathrm{End}(M);\ \varphi \text{ ist Isomorphismus}\}.$$

Satz 3.3.6. *Es seien R ein K1-Ring, L, M und N endlich erzeugte freie R-Moduln mit Basen $\mathcal{A}$, $\mathcal{B}$ bzw. $\mathcal{C}$.*

(i) *Es seien $n := \mathrm{rg}(M)$ und $m := \mathrm{rg}(N)$. Dann hat hat man zueinander inverse R-Modulisomorphismen*

$$\begin{array}{rcl} \mathrm{Mat}(m,n;R) & \longleftrightarrow & \mathrm{Hom}(M,N) \\ A & \mapsto & \mu_{\mathcal{C}}^{\mathcal{B}}(A) \\ M_{\mathcal{C}}^{\mathcal{B}}(\varphi) & \leftarrow\!\shortmid & \varphi. \end{array}$$

(ii) *Sind $\varphi\colon L \to M$ und $\psi\colon M \to N$ Modulhomomorphismen, so gilt für die zugehörigen darstellenden Matrizen*

$$M_{\mathcal{C}}^{\mathcal{A}}(\psi\circ\varphi) \;=\; M_{\mathcal{C}}^{\mathcal{B}}(\psi)\cdot M_{\mathcal{B}}^{\mathcal{A}}(\varphi)$$

(iii) *Man hat zueinander inverse Ringhomomorphismen*

$$\begin{array}{rcl} \mathrm{Mat}(n,n;R) & \longleftrightarrow & \mathrm{End}(V) \\ A & \mapsto & \mu_{\mathcal{B}}^{\mathcal{B}}(A) \\ M_{\mathcal{B}}^{\mathcal{B}}(\varphi) & \leftarrow\!\shortmid & \varphi. \end{array}$$

Insbesondere hat man für jede Matrix $A \in \mathrm{Mat}(n,n;R)$ und jeden Modulhomomorphismus $\varphi\colon V \to V$:

$$\begin{aligned} A \text{ ist invertierbar} &\iff \mu_{\mathcal{C}}^{\mathcal{B}}(A) \text{ ist Isomorphismus},\\ \varphi \text{ ist Isomorphismus} &\iff M_{\mathcal{B}}^{\mathcal{B}}(\varphi) \text{ ist invertierbar}, \end{aligned}$$

Ist dabei eine beiden Bedingungen erfüllt, so gilt $\mu_{\mathcal{C}}^{\mathcal{B}}(A)^{-1} = \mu_{\mathcal{C}}^{\mathcal{B}}(A^{-1})$, beziehungsweise $M_{\mathcal{B}}^{\mathcal{B}}(\varphi^{-1}) = M_{\mathcal{B}}^{\mathcal{B}}(\varphi)^{-1}$.

Definition 3.3.7. Es seien R ein K1-Ring und $A \in \mathrm{Mat}(n,n;R)$ eine Matrix. Die *Determinante* von A ist

$$\det(A) \;:=\; \sum_{\sigma\in S_n} \mathrm{sg}(\sigma)\cdot a_{1\sigma(1)}\cdots a_{n\sigma(n)} \;\in\; R.$$

Die zu der Matrix $A \in \mathrm{Mat}(n,n;R)$ *komplementäre Matrix* $A^{\#} \in \mathrm{Mat}(n,n;R)$ ist definiert als

$$A^{\#} \;:=\; \begin{pmatrix} \det(A_{11}) & \dots & \det(A_{1n}) \\ \vdots & & \vdots \\ \det(A_{n1}) & \dots & \det(A_{nn}) \end{pmatrix}^t \;\in\; \mathrm{Mat}(n,n;R),$$

wobei

$$A_{ij} \;:=\; \begin{pmatrix} a_{11} & \dots & a_{1j-1} & 0 & a_{1j+1} & \dots & a_{1n} \\ & \vdots & & & & \vdots & \\ a_{i-11} & \dots & a_{i-1j-1} & 0 & a_{i-1j+1} & \dots & a_{i-1n} \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ a_{i+11} & \dots & a_{i+1j-1} & 0 & a_{i+1j+1} & \dots & a_{i+1n} \\ & \vdots & & & & \vdots & \\ a_{n1} & \dots & a_{nj-1} & 0 & a_{nj+1} & \dots & a_{nn} \end{pmatrix} \;\in\; \mathrm{Mat}(n,n;R).$$

Satz 3.3.8. *Es seien R ein Integritätsring und $A, B \in \mathrm{Mat}(n,n;R)$.*

(i) *Es gilt* $\det(A\cdot B) = \det(A)\det(B)$.
(ii) *Es gilt* $\det(A^t) = \det(A)$.
(iii) *Es gilt* $A^{\#}\cdot A = \det(A)\cdot E_n = A\cdot A^{\#}$.

Beweis. Wir betrachten wieder den Quotientenkörper $Q(R)$ von R und die Einbettungen

$$\begin{aligned} \imath\colon R \;&\to\; Q(R), \qquad a \;\mapsto\; a/1_R,\\ \imath\colon \mathrm{Mat}(n,n;R) \;&\to\; \mathrm{Mat}(n,n,Q(R)), \qquad (a_{ij}) \;\mapsto\; \left(\frac{a_{ij}}{1_R}\right). \end{aligned}$$

Die Determinante ist verträglich mit diesen Einbettungen; es gilt

$$\begin{aligned} \det(\imath(A)) &= \sum_{\sigma\in S_n} \mathrm{sg}(\sigma)\cdot \frac{a_{1\sigma(1)}}{1_R}\cdots\frac{a_{n\sigma(n)}}{1_R}\\ &= \frac{\sum_{\sigma\in S_n}\mathrm{sg}(\sigma)\cdot a_{1\sigma(1)}\cdots a_{n\sigma(n)}}{1_R}\\ &= \imath(\det(A)). \end{aligned}$$

Das erlaubt es uns, die Aussagen in $\mathrm{Mat}(n,n;Q(R))$ zu beweisen; dies wurde bereits in [1, §§ 6.2 und 6.3] durchgeführt. □

Satz 3.3.9. *Es seien R ein Integritätsring und $A \in \mathrm{Mat}(n,n;R)$. Dann sind folgende Aussagen äquivalent:*

(i) *A ist invertierbar, d.h., es gilt $A \in \mathrm{Mat}(n,n;R)^*$.*
(ii) *Die Spalten von A bilden eine Basis des R^n.*
(iii) *Die Zeilen von A bilden eine Basis des R^n.*
(iv) *Die Determinante von A ist invertierbar, d.h., es gilt $\det(A) \in R^*$.*

Beweis. Zu "(i)⇒(iv)". Es sei A^{-1} die Inverse zu A. Dann liefert uns der Determinantenmultiplikationssatz

$$\det(A)\det(A^{-1}) \;=\; \det(A\cdot A^{-1}) \;=\; \det(E_n) \;=\; 1_R.$$

Zu "(iv)⇒(i)". Wir betrachten die zu A komplementäre Matrix $A^{\#} \in \mathrm{Mat}(n,n;R)$. Dann gilt

$$A^{\#}\cdot A \;=\; A\cdot A^{\#} \;=\; \det(A)\cdot E_n.$$

Folglich ist die Matrix $\det(A)^{-1}\cdot A^{\#}$ invers zu A; insbesondere ist die Matrix A invertierbar.

Zu "(i)⇒(ii)". Wir haben einen Isomorphismus $\mu_A\colon R^n \to R^n$, $x \mapsto A\cdot x$. Dieser bildet die Basis $(e_1,\ldots,e_n)$ auf die Basis $(A_{*1},\ldots,A_{*n})$ ab.

Zu "(ii)⇒(i)". Für jedes $1 \le i \le n$ stellen wir $e_i \in R^n$ als Linearkombination über den Spalten von A dar: Mit geeigneten $b_{i1},\ldots,b_{in} \in R$ gilt

$$e_i \;=\; b_{i1}\cdot A_{*1} + \ldots + b_{in}\cdot A_{*n} \;=\; A\cdot b_i,$$

wobei $b_i = (b_{i1},\ldots,b_{in})$. Die Matrix $B := (b_1,\ldots,b_n)$ leistet $A\cdot B = E_n$. Der Determinantenmultiplikationssatz zeigt $\det(A) \in R^*$. Somit ist A invertierbar.

Zur Äquivalenz von (i) und (iii). Die Matrix A ist genau dann invertierbar, wenn ihre Transponierte A^t invertierbar ist. Letzteres ist nach (ii) äquivalent zu der Tatsache, dass die Zeilen von A eine Basis für R^n bilden. □

Bemerkung 3.3.10. Es sei $\mathbb{K}$ ein Körper. In [1, 5.2.15] hatten wir gezeigt dass eine Matrix $A \in \mathrm{Mat}(n,n;\mathbb{K})$ genau dann invertierbar ist, wenn $\mathrm{rg}(A) = n$ gilt.

Eine entsprechende Aussage für Matrizen über Integritätsringen ist nicht möglich: Die Matrix

$$A \;:=\; \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \;\in\; \mathrm{Mat}(2,2;\mathbb{Z}) \;\subset\; \mathrm{Mat}(2,2;\mathbb{Q})$$

besitzt den Rang 2, ist jedoch nicht invertierbar in $\mathrm{Mat}(n,n;\mathbb{Z})$, denn es gilt $\det(A) = 4 \notin \mathbb{Z}^*$.

Aufgaben zu Abschnitt 3.3.

Aufgabe 3.3.11. In welchem der folgenden Fälle ist die Matrix $A \in \mathrm{Mat}(n,n;R)$ invertierbar in $\mathrm{Mat}(n,n;R)$:

(i) $R = \mathbb{Z}$ und $A = \begin{pmatrix} 1 & 0 & -1 \\ -2 & 1 & 2 \\ -2 & 3 & 3 \end{pmatrix}$

(ii) $R = \mathbb{Q}[T]$ und $A = \begin{pmatrix} T^2+1 & T+1 \\ T-1 & 1 \end{pmatrix}$

Berechne gegebenenfalls die zugehörige Inverse $A^{-1} \in \mathrm{Mat}(n,n;R)$.

Aufgabe 3.3.12. Es seien R ein Hauptidealring und $a, b \in R$. Beweise die Äquivalenz folgender Aussagen:

(i) Es gibt $c, d \in R$, sodass (a,b) und (c,d) eine Basis des R^2 bilden.
(ii) Die Elemente $a, b \in R$ sind teilerfremd.

Aufgabe 3.3.13. Es seien R ein K1-Ring und M ein freier R-Modul mit einer Basis $(u_1, \ldots, u_n)$. Dann ist auch der duale Modul $M^* := \mathrm{Hom}(M,R)$ frei, und man hat eine eine duale Basis $(u_1^*, \ldots, u_n^*)$ für M^* mit

$$u_i^*(u_j) \quad = \quad \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$$

Aufgabe 3.3.14. Es seien $p, q \in \mathbb{Z}_{\geq 0}$ Primzahlen. Zeige: Für die Menge aller Homomorphismen zwischen den $\mathbb{Z}$-Moduln $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}/q\mathbb{Z}$ gilt

$$\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/q\mathbb{Z}) \quad \cong \quad \begin{cases} \mathbb{Z}/p\mathbb{Z} & \text{falls } p = q, \\ \{0\} & \text{falls } p \neq q. \end{cases}$$

3.4. **Torsion und Länge.**

Beispiel 3.4.1. Für $n \in \mathbb{Z}_{\geq 2}$ betrachten wir den $\mathbb{Z}$-Modul $\mathbb{Z}/n\mathbb{Z}$. Für jedes Element $\overline{a} = a + n\mathbb{Z}$ hat man

$$n \cdot \overline{a} \;=\; (na) \cdot \overline{1} \;=\; (an) \cdot \overline{1} \;=\; a \cdot \overline{n} \;=\; \overline{0}.$$

Insbesondere ist die Familie $(\overline{a})$ linear abhängig. Somit kann $\mathbb{Z}/n\mathbb{Z}$ kein freier $\mathbb{Z}$-Modul sein.

Definition 3.4.2. Es seien R ein Integritätsring und M ein R-Modul.

(i) Man nennt $u \in M$ ein *Torsionselement*, falls $r \cdot u = 0_M$ für ein $0_R \neq r \in R$ gilt. Die Menge aller Torsionselemente in M bezeichnen wir mit $T(M)$.
(ii) Man nennt M einen *Torsionsmodul*, falls $M = T(M)$ gilt, und man nennt M *torsionsfrei*, falls $T(M) = \{0_M\}$ gilt.

Beispiel 3.4.3. Es seien R ein Integritätsring und $0_R \neq a \in R$. Dann ist $R/\langle a \rangle$ ein Torsionsmodul über R.

Satz 3.4.4. *Es seien R ein Integritätsring und M ein R-Modul.*

(i) *Die Menge $T(M) \subseteq M$ der Torsionselemente ist ein Untermodul von M.*
(ii) *Ist M frei, so ist M torsionsfrei.*
(iii) *Ist M torsionsfrei, so ist auch jeder Untermodul $N \leq_R M$ torsionsfrei.*

Beweis. Zu (i). Es gilt stets $0_M \in T(M)$. Sind $u, u' \in T(M)$ gegeben, so gibt es $0_R \neq r, r' \in R$ mit $r \cdot u = 0_M = r' \cdot u'$. Da R ein Integritätsring ist, gilt $rr' \neq 0_R$. Weiter haben wir

$$(rr') \cdot (u + u') \;=\; r' \cdot (r \cdot u) + r \cdot (r' \cdot u') \;=\; 0_M$$

Das bedeutet $u + u' \in T(M)$. Sind $u \in M$ und $s \in R$ gegeben, so wählen wir wieder $0_R \neq r \in R$ mit $r \cdot u = 0_M$. Dann ergibt sich $s \cdot u \in T(M)$ mit

$$r \cdot (s \cdot u) \;=\; s \cdot (r \cdot u) \;=\; 0_M.$$

Zu (ii). Wir zeigen, dass $T(M) = \{0_M\}$ gilt. Dazu sei $(u_i)_{i \in I}$ eine Basis für M. Ist $u \in T(M)$, gegeben, so besitzt u eine Entwicklung $\sum r_i \cdot u_i$. Man hat

$$0_M \;=\; r \cdot \sum_{i \in I} r_i \cdot u_i \;=\; \sum_{i \in I} (rr_i) \cdot u_i.$$

Die lineare Unabhängigkeit von $(u_i)_{i \in I}$ liefert $rr_i = 0_R$ für alle $i \in I$. Da R Integritätsring ist, erhalten wir $r_i = 0_R$ für alle $i \in I$. Das bedeutet $u = 0_M$. □

Definition 3.4.5. Es seien R ein K1-Ring und M ein R-Modul. Die *Länge* $l_R(M)$ von M ist das Supremum über alle Längen r von Untermodulketten der Form

$$\{0_M\} \;\subsetneq\; M_1 \;\subsetneq\; M_2 \;\subsetneq\; \ldots \;\subsetneq\; M_r \;=\; M, \qquad M_i \leq_R M.$$

Bemerkung 3.4.6. Es seien R ein K1-Ring und M ein R-Modul. Dann gilt:

$$l_R(M) \;=\; 0 \quad \Longleftrightarrow \quad M \;=\; \{0_M\}.$$

Beispiel 3.4.7.
(i) Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Dann gilt $l_{\mathbb{K}}(V) = \dim(V)$.
(ii) Es gilt $l_{\mathbb{Z}}(\mathbb{Z}) = \infty$, denn mit jedem $a \in \mathbb{Z}_{\geq 2}$ kann man beliebig lange Untermodulketten konstruieren:

$$\{0\} \;\subsetneq\; \langle a^n \rangle \;\subsetneq\; \langle a^{n-1} \rangle \;\subsetneq\; \ldots \;\subsetneq\; \langle a \rangle \;\subsetneq\; \mathbb{Z}.$$

(iii) Für jede Primzahl $p \in \mathbb{Z}$ hat man $l_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}) = 1$, da $\{0\}$ und $\mathbb{Z}/p\mathbb{Z}$ die einzigen Untermoduln von $\mathbb{Z}/p\mathbb{Z}$ sind.

Satz 3.4.8. *Es sei R ein K1-Ring, und es seien M, N zwei R-Moduln. Dann gilt*

$$l_R(M \oplus N) \quad = \quad l_R(M) + l_R(N).$$

Beweis. Wir verifizieren zunächst die Abschätzung "$\geq$". Dazu betrachten wir zwei aufsteigende Untermodulketten

$$\{0\} \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = M, \qquad \{0\} \subsetneq N_1 \subsetneq \ldots \subsetneq N_s = N.$$

Daraus gewinnt man eine echt aufsteigende Kette der Länge $r+s$ in der direkten Summe $M \oplus N$, nämlich

$$\{0\} \subsetneq M_1 \oplus \{0\} \subsetneq \ldots \subsetneq M_r \oplus \{0\} \subsetneq M_r \oplus N_1 \subsetneq \ldots \subsetneq M_r \oplus N_s = M \oplus N.$$

Beim Nachweis der Abschätzung "$\leq$" arbeiten wir mit den kanonischen Homomorphismen

$$\imath\colon M \to M \oplus N,\ u \mapsto (u,0), \qquad \pi\colon M \oplus N \to N,\ (u,v) \mapsto v.$$

Man hat also $\imath(M) = \operatorname{Kern}(\pi)$. Es sei $\{0\} \subsetneq U_1 \subsetneq \ldots \subsetneq U_r = M \oplus N$ eine aufsteigende Kette von Untermoduln. Wir zeigen, dass dann für jedes j gilt:

$$(*) \qquad \imath^{-1}(U_j) \subsetneq \imath^{-1}(U_{j+1}) \qquad \text{oder} \qquad \pi(U_j) \subsetneq \pi(U_{j+1}).$$

Nehmen wir an, es wäre für ein j in beiden Fällen Gleichheit gegeben. Wir führen dies zum Widerspruch, indem wir zeigen, dass dann $U_{j+1} \subseteq U_j$ und somit $U_j = U_{j+1}$ gelten müsste.

Dazu sei $(u,v) \in U_{j+1}$ gegeben. Wegen $\pi(U_j) = \pi(U_{j+1})$ gibt es dann ein Element $(u',v) \in U_j$. Offensichtlich gilt

$$(u-u',0) \ = \ (u,v) - (u',v) \ \in \ U_{j+1}.$$

Folglich hat man $u - u' \in \imath^{-1}(U_{j+1}) = \imath^{-1}(U_j)$. Das impliziert $(u-u',0) \in U_j$, und wir erhalten

$$(u,v) \ = \ (u',v) + (u-u',0) \ \in \ U_j.$$

Damit haben wir $(*)$ verifiziert. Folglich kann man aus den Untermoduln $\imath^{-1}(U_j) \subseteq M$ und $\pi(U_j) \subseteq N$ echt aufsteigende Ketten in M bzw. N bilden, sodass die Summe der Kettenlängen mindestens r beträgt. □

Satz 3.4.9. *Es sei R ein euklidischer Ring, und es seien $q_1, \ldots, q_n \in R$ Primelemente. Dann gilt*

$$l_R(R/\langle q_1 \cdots q_n \rangle) \quad = \quad n.$$

Lemma 3.4.10. *Es seien R ein euklidischer Ring und $a \in R$ von der Form $a = cp_1^{\nu_1} \cdots p_n^{\nu_n}$, wobei $c \in R^*$ gelte und die p_i paarweise nichtassoziierte Primelemente seien. Dann erhält man einen Isomorphismus von R-Moduln*

$$R/\langle a \rangle \quad \cong \quad R/\langle p_1^{\nu_1} \rangle \ \times \ \ldots \ \times \ R/\langle p_n^{\nu_n} \rangle.$$

Beweis. Nach Satz 2.3.13 hat man sogar einen Isomorphismus der entsprechenden Faktorringe. Das liefert insbesondere den gewünschten Isomorphismus der Faktormoduln. □

Beweis von Satz 3.4.9. Wir behandeln zunächst den Fall $q_1 = \ldots = q_n =: q$. Wir arbeiten mit dem surjektiven Homomorphismus $\pi\colon R \to R/\langle q^n \rangle$.

Die Ungleichung $l_R(R/\langle q^n \rangle) \geq n$ ist leicht einzusehen: Man hat eine echt aufsteigende Kette der Länge n von Idealen in R, nämlich

$$\{0\} \subsetneq \langle q^{n-1} \rangle \subsetneq \ldots \subsetneq \langle q \rangle \subsetneq \langle 1_R \rangle = R.$$

Die Inklusionen sind jeweils echt, da wir sonst $q^{i+1} \mid q^i$ für ein i hätten. Als Ideale in R sind die $\langle q^i \rangle$ auch Untermoduln von R.

Die Bilder $\pi(\langle q^i \rangle)$ der Untermoduln $\langle q^i \rangle \leq_R R$ liefern eine aufsteigende Untermodulkette in $R/\langle q^n \rangle$:

$$\{0\} \subsetneq \pi(\langle q^{n-1} \rangle) \subsetneq \ldots \subsetneq \pi(\langle q \rangle) \subsetneq \pi(\langle 1_R \rangle) = R/\langle q^n \rangle.$$

Diese Kette ist tatsächlich echt aufsteigend, denn sonst hätte man $\pi(\langle q^{i+1} \rangle) = \pi(\langle q^i \rangle)$ für ein i, was sofort zu einem Widerspruch führt:

$$q^i \in \pi^{-1}(\pi(\langle q^{i+1} \rangle)) = \langle q^{i+1} \rangle + \langle q^n \rangle = \langle q^{i+1} \rangle.$$

Zum Nachweis der Ungleichung $l_R(R/\langle q^n \rangle) \leq n$ betrachten wir eine aufsteigende Kette

$$\{0\} \subsetneq M_1 \subsetneq \ldots \subsetneq M_r = R/\langle q^n \rangle$$

von Untermoduln in $R/\langle q^n \rangle$ Die Urbilder $\pi^{-1}(M_i)$ sind Ideale in dem Ring R, und sie bilden eine echt aufsteigende Kette

$$\{0\} \subsetneq \langle q^n \rangle \subsetneq \pi^{-1}(M_1) \subsetneq \pi^{-1}(M_2) \subsetneq \ldots \subsetneq \pi^{-1}(M_r) = R.$$

Da R Hauptidealring ist, wird jedes Ideal $\pi^{-1}(M_i)$ von einem Element $s_i \in R$ erzeugt, und wir erhalten $s_i | q^n$, d.h., es gilt $s_i = c_i q^{n_i}$ mit $c_i \in R^*$. Da die Kette echt aufsteigt, muss $n > n_1 > \ldots > n_1 = 0$ gelten. Folglich kann die Kette höchstens die Länge n besitzen.

Für den allgemeinen Fall schreiben wir $q_1 \cdots q_n = c p_1^{\nu_1} \cdots p_m^{\nu_m}$ mit paarweise nichtassoziierten Primelementen p_i. Lemma 3.4.10 liefert einen Isomorphismus von R-Moduln

$$R/\langle c p_1^{\nu_1} \cdots p_m^{\nu_m} \rangle \cong \bigoplus_{i=1}^{m} R/\langle p_i^{\nu_i} \rangle.$$

Die gewünschte Aussage über die Längen ergibt sich dann aus dem bereits behandelten Fall und Satz 3.4.8: Es gilt

$$\begin{aligned} l_R\left(R/\langle c p_1^{\nu_1} \cdots p_m^{\nu_m} \rangle\right) &= l_R\left(R/\langle p_1^{\nu_1} \rangle \oplus \ldots \oplus R/\langle p_m^{\nu_m} \rangle\right) \\ &= l_R\left(R/\langle p_1^{\nu_1} \rangle\right) + \ldots + \left(R/\langle p_m^{\nu_m} \rangle\right) \\ &= \nu_1 + \ldots + \nu_m \\ &= n. \end{aligned}$$

□

Satz 3.4.11. *Es seien R ein euklidischer Ring und $a_1, \ldots, a_n, b_1, \ldots, b_m \in R$ Nichteinheiten mit $a_{i+1} | a_i$ für $i = 1, \ldots, n-1$ bzw. $b_{j+1} | b_j$ für $j = 1, \ldots, m-1$. Gilt*

$$\bigoplus_{i=1}^{n} R/\langle a_i \rangle \cong \bigoplus_{j=1}^{m} R/\langle b_j \rangle$$

als Isomorphie von R-Moduln, so hat man bereits $m = n$, und es gilt $b_i = c_i a_i$ mit Einheiten $c_i \in R$.

Beweis. Wir zeigen zunächst $\langle a_i \rangle = \langle b_i \rangle$ für $i \leq \min(m, n)$. Nehmen wir einmal an es existierten $k \leq \min(m, n)$ mit $\langle a_k \rangle \neq \langle b_k \rangle$. Dann wählen wir k minimal mit dieser Eigenschaft. Für $l \geq 0$ hat man $a_{k+l} | a_k$, somit $a_k R \subseteq \langle a_{k+l} \rangle$, und wir erhalten

$$M' := a_k \cdot \bigoplus_{i=1}^{n} R/\langle a_i \rangle \cong \bigoplus_{i=1}^{k-1} a_k \cdot (R/\langle a_i \rangle).$$

Andererseits erhalten wir mit $\langle a_i\rangle = \langle b_i\rangle$ für $i = 1, \ldots, k-1$ die folgende Darstellung für den R-Modul M':

$$M' \;\cong\; a_k \cdot \bigoplus_{j=1}^{m} R/\langle b_j\rangle \;=\; \bigoplus_{i=1}^{k-1} a_k \cdot (R/\langle a_i\rangle) \;\oplus\; \bigoplus_{j=k}^{m} a_k \cdot (R/\langle b_j\rangle).$$

Verwendet man nun die Additivität 3.4.8 der Länge $l_R(M')$, so ergibt ein Vergleich dieser beiden Darstellungen

$$l_R\left(\bigoplus_{j=k}^{m} a_k \cdot (R/\langle b_j\rangle)\right) \;=\; 0.$$

Folglich muss der Modul auf der linken Seite trivial sein. Insbesondere erhalten wir $a_k R \subseteq \langle b_k\rangle$. Analog sieht man $b_k R \subseteq \langle a_k\rangle$. Das ergibt $\langle a_k\rangle = \langle b_k\rangle$; Widerspruch zu unserer Annahme. Bis $\min(n, m)$ muss also $\langle a_i\rangle = \langle b_i\rangle$ gelten.

Wir nehmen nun an, dass m und n voneinander verschieden sind, etwa $m < n$. Nach Voraussetzung und wegen $\langle b_j\rangle = \langle a_j\rangle$ für $1 \le j \le m$ gilt

$$\bigoplus_{i=1}^{m} R/\langle a_i\rangle \oplus \bigoplus_{i=m+1}^{n} R/\langle a_i\rangle \;\cong\; \bigoplus_{j=1}^{m} R/\langle b_j\rangle \;=\; \bigoplus_{j=1}^{m} R/\langle a_j\rangle.$$

Wiederum kann man mit Satz 3.4.8 eine Längenberechnung durchführen, und erhält $R/\langle a_n\rangle = \{0\}$; Widerspruch zu $a_n \notin R^*$. □

Aufgaben zu Abschnitt 3.4.

Aufgabe 3.4.12. Als abelsche Gruppe ist $(\mathbb{Q}, +)$ ist ein $\mathbb{Z}$-Modul. Zeige: $(\mathbb{Q}, +)$ ist torsionsfrei, aber nicht frei.

Aufgabe 3.4.13. Es sei R ein Integritätsring. Beweise folgende Aussagen:

(i) Die direkte Summe $\bigoplus_{i \in I} M_i$ von R-Torsionsmoduln M_i ist wieder ein R-Torsionsmodul.
(ii) Das direkte Produkt $\prod_{i \in I} M_i$ von R-Torsionsmoduln M_i ist im allgemeinen kein R-Torsionsmodul.

Aufgabe 3.4.14. Berechne die Länge des $\mathbb{Z}$-Moduls $\mathbb{Z}/36\mathbb{Z}$. Gib eine Kette maximaler Länge in $\mathbb{Z}/36\mathbb{Z}$ an.

4. Moduln über euklidischen Ringen

4.1. **Matrizen über euklidischen Ringen.**

Bemerkung 4.1.1. Eine Matrix A über einem Körper kann durch Zeilenoperationen auf normierte Zeilenstufenform bringen, wendet man zusätzlich Spaltenoperationen an, so kommt man sogar auf die Gestalt

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix},$$

wobei r der Rang der Matrix A ist. Elementare Zeilen- und Spaltenoperationen sind auch bei Matrizen über Ringen möglich; wir betrachten dafür die Matrix

$$A := \begin{pmatrix} 3 & 3 & 0 \\ -3 & -1 & 2 \\ -3 & -3 & 2 \end{pmatrix} \in \mathrm{Mat}(3,3;\mathbb{Z})$$

Wir wollen zunächst schauen, inwieweit man A durch ganzzahlige Zeilenumformungen auf eine möglichst einfache Gestalt bringen kann:

$$\begin{pmatrix} 3 & 3 & 0 \\ -3 & -1 & 2 \\ -3 & -3 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(1;1,2)} \quad \begin{pmatrix} 3 & 3 & 0 \\ 0 & 2 & 2 \\ -3 & -3 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(1;1,3)} \quad \begin{pmatrix} 3 & 3 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(-1;3,2)} \quad \begin{pmatrix} 3 & 3 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(-1;2,1)} \quad \begin{pmatrix} 3 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Mit weiteren Zeilenoperationen läßt sich nun nichts mehr ausrichten. Nimmt man jedoch zusätzlich Spaltenoperationen zur Hilfe, so kann weiter vereinfachen:

$$\begin{pmatrix} 3 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{SpOp}(1,2)} \quad \begin{pmatrix} 1 & 3 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(-2;1,2)} \quad \begin{pmatrix} 1 & 3 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{SpOp}(-3;1,2)} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -6 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(-1;2)} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(2,3)} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 2 \\ 0 & 6 & 0 \end{pmatrix}$$

$$\xrightarrow{\mathrm{SpOp}(2,3)} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 6 \end{pmatrix}$$

Bemerkung 4.1.2. Es seien R ein Integritätsring und $n \in \mathbb{N}_{\geq 2}$. Für $\lambda \in R$ und $1 \leq i, j \leq n$ mit $i \neq j$ hat man eine *Elementarmatrix*

$$E(n;\lambda;j,i) \quad := \quad \begin{pmatrix} e_1 \\ \vdots \\ e_i + \lambda \cdot e_j \\ \vdots \\ e_j \\ \vdots \\ e_n \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 0 & & & & & 0 \\ & \ddots & & & & & \\ 0 & & 1 & & \lambda & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & 0 \\ 0 & & & & & 0 & 1 \end{pmatrix}$$

$$= \quad (e_1, \ldots, e_i, \ldots, e_j + \lambda \cdot e_i, \ldots, e_n).$$

Multiplikation von links mit $E(n;\lambda;j,i)$ entspricht dem Addieren des λ-fachen der j-ten Zeile zur i-ten Zeile, d.h., für $A \in \mathrm{Mat}(n,m;R)$ gilt

$$E(n;\lambda;j,i) \cdot A \quad = \quad \mathrm{ZOp}(\lambda;j,i)(A).$$

Multiplikation von rechts mit $E(n;\lambda;j,i)$ entspricht dem Addieren des λ-fachen der i-ten Spalte zur j-ten Spalte, d.h., für $B \in \mathrm{Mat}(m,n;R)$ gilt

$$B \cdot E(n;\lambda;j,i) \quad = \quad \mathrm{SpOp}(\lambda;i,j)(B).$$

Die Matrix $E(n;\lambda;j,i)$ ist invertierbar in $\mathrm{Mat}(n,n;R)$, und ihre Inverse ist gegeben durch

$$E(n;\lambda;j,i)^{-1} \quad = \quad E(n;-\lambda;j,i).$$

Bemerkung 4.1.3. Es seien R ein Integritätsring und $n \in \mathbb{N}_{\geq 2}$. Für jedes $1 \leq i < j \leq n$ hat man eine *Elementarmatrix*

$$E(n;i,j) \quad := \quad \begin{pmatrix} e_1 \\ \vdots \\ e_j \\ \vdots \\ e_i \\ \vdots \\ e_n \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 0 & & & & & 0 \\ & \ddots & & & & & \\ 0 & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & 0 \\ 0 & & & & & 0 & 1 \end{pmatrix}$$

$$= \quad (e_1, \ldots, e_j, \ldots, e_i, \ldots, e_n).$$

Multiplikation von links mit $E(n;i,j)$ entspricht dem Vertauschen der i-ten Zeile mit der j-ten Zeile, d.h., für $A \in \mathrm{Mat}(n,m;R)$ gilt

$$E(n;i,j) \cdot A \quad = \quad \mathrm{ZOp}(i,j)(A).$$

Multiplikation von rechts mit $E(n;i,j)$ entspricht dem Vertauschen der i-ten Spalte mit der j-ten Spalte, d.h., für $B \in \mathrm{Mat}(m,n;R)$ gilt

$$B \cdot E(n;i,j) \quad = \quad \mathrm{SpOp}(i,j)(B).$$

Die Matrix $E(n;i,j)$ ist invertierbar in $\mathrm{Mat}(n,n;R)$, und ihre Inverse ist gegeben durch

$$E(n;i,j)^{-1} \quad = \quad E(n;i,j).$$

Bemerkung 4.1.4. Es seien R ein Integritätsring und $n \in \mathbb{N}_{\geq 2}$. Zu $\lambda \in R^*$ und $1 \leq i \leq n$ hat man eine *Elementarmatrix*

$$E(n;\lambda;i) \quad := \quad \begin{pmatrix} e_1 \\ \vdots \\ \lambda \cdot e_i \\ \vdots \\ e_n \end{pmatrix} \quad = \quad \begin{pmatrix} 1 & 0 & & & & & 0 \\ & \ddots & & & & & \\ 0 & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & & & 0 & 1 \end{pmatrix}$$

$$= \quad (e_1, \ldots, \lambda \cdot e_i, \ldots, e_n).$$

Multiplikation von links mit $E(n;\lambda;i)$ entspricht dem Multiplizieren der i-ten Zeile mit dem Faktor λ, d.h., für $A \in \mathrm{Mat}(n,m;R)$ gilt

$$E(n;\lambda;i) \cdot A \quad = \quad \mathrm{ZOp}(\lambda;i)(A).$$

Multiplikation von rechts mit $E(n;\lambda;i)$ entspricht dem Multiplizieren der i-ten Spalte mit dem Faktor λ, d.h., für $B \in \mathrm{Mat}(m,n;R)$ gilt

$$B \cdot E(n;\lambda;i) = \mathrm{SpOp}(\lambda;i)(B).$$

Die Matrix $E(n;\lambda;i)$ ist invertierbar in $\mathrm{Mat}(n,n;R)$, und ihre Inverse ist gegeben durch

$$E(n;\lambda;i)^{-1} \quad = \quad E(n;\lambda^{-1};i).$$

Satz 4.1.5 (Hermite-Normalform)**.** *Es seien (R,δ) ein euklidischer Ring und $A \in \mathrm{Mat}(m,n;R)$. Dann gibt es Elementarmatrizen $S_1, \ldots, S_k \in \mathrm{Mat}(m,m;R)$, sodass $B := S_k \cdots S_1 \cdot A$ von folgender Gestalt ist*

$$B \quad = \quad \begin{pmatrix} 0 & \cdots & 0 & b_{1j_1} & * & \cdots & * & \star & * & \cdots & \cdots & * & \star & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & b_{2j_2} & * & \cdots & \cdots & * & \star & * & \cdots & * \\ & & \vdots & & & & & & & & & & & & \vdots & \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & b_{rj_r} & * & \cdots & * \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0 \\ & & \vdots & & & & & & & & & & & & \vdots & \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

wobei $b_{lj_l} \in R \setminus \{0_R\}$ für $1 \leq l \leq r$ gilt, "$*$" für beliebige Elemente aus R steht, und $b_{ij_l} = 0_R$ oder $\delta(b_{ij_l}) < \delta(b_{lj_l})$ für alle $2 \leq l \leq r$ und $1 \leq i < l$ gilt.

Beweis. Es ist zu zeigen, dass man A durch elementare Zeilenoperationen auf die gewünschte Gestalt bringen kann. Wir bringen A zunächst auf Zeilenstufenform.

Schritt 1: Wir suchen das kleinste j_1, sodass A_{*j_1} keine Nullspalte ist und wählen ein i_1 mit $a_{i_1 j_1} \neq 0$, sodass $\delta(a_{i_1 j_1})$ minimal unter den Graden der nichttrivialen Einträge von A_{*j_1} ist. Dann vertauschen wir die erste mit der i_1-ten Zeile. Für die resultierende Matrix A' gilt $a'_{1j_1} = a_{i_1 j_1}$, und sie besitzt die Gestalt

$$A' \quad = \quad \begin{pmatrix} 0 & \ldots & 0 & a'_{1j_1} & * & \ldots & * \\ 0 & \ldots & 0 & \star & * & \ldots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & \star & * & \ldots & * \end{pmatrix}$$

Schritt 2: Da R ein euklidischer Ring ist, hat jedes a'_{ij_1}, wobei $i \geq 2$, eine Darstellung $a'_{ij_1} = q_i a'_{1j_1} + r_i$ mit $r_i = 0_R$ oder $\delta(r_i) < \delta(a'_{ij_1})$. Durch Addieren des $-q_i$-Fachen der ersten Zeile zur i-ten Zeile erreichen wir also, dass unter a'_{1j_1} nur noch Einträge stehen, die entweder verschwinden oder dem Grade nach echt kleiner sind als a'_{1j_1}.

Durch Iteration dieser beiden Schritte bringen wir die Matrix B schließlich auf die Gestalt

$$\begin{pmatrix} 0 & \ldots & 0 & b_{1j_1} & * & \ldots & * \\ 0 & \ldots & 0 & 0 & \bullet & \ldots & \bullet \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \ldots & 0 & 0 & \bullet & \ldots & \bullet \end{pmatrix} \quad = \quad \begin{pmatrix} B_{1*} \\ D \end{pmatrix}$$

Wiederholt man die beiden Schritte mit der Matrix D, so ist auch die zweite Zeile in die gewünschte Form gebracht — man beachte dabei, dass Zeilenoperationen an D auch Zeilenoperationen an C sind. Nach m derartigen Durchläufen hat man A auf Zeilenstufenform gebracht.

Um schließlich die Bedingungen $b_{ij_l} = 0_R$ oder $\delta(b_{ij_l}) < \delta(b_{lj_l})$ für alle $2 \leq l \leq r$ und $1 \leq i < l$ sicherzustellen, muss man nur noch entsprechende Vielfache der l-ten Zeile von den darüberliegenden abziehen. □

Satz 4.1.6 (Smith-Normalform)**.** *Es seien (R, δ) ein euklidischer Ring und $A \in \mathrm{Mat}(m, n; R)$ eine Matrix. Dann gibt es Elementarmatrizen $S_1, \ldots, S_k \in \mathrm{Mat}(m, m; R)$, und $T_1, \ldots, T_l \in \mathrm{Mat}(n, n; R)$ mit*

$$S_k \cdots S_1 \cdot A \cdot T_1 \cdots T_l \quad = \quad \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix},$$

wobei $D \in \mathrm{Mat}(s, s; R)$ eine Diagonalmatrix mit nichtverschwindenden Diagonaleinträgen $a_1, \ldots, a_s \in R$ ist, die den Teilbarkeitsbedingungen $a_1 | a_2, \ldots, a_{s-1} | a_s$ genügen.

Beweis. Ist A die Nullmatrix, so ist nichts zu zeigen. Für nichttriviales A müssen wir zeigen, dass man A durch elementare Zeilen- und Spaltenoperationen auf die gewünschte Gestalt bringen kann. Dies geschieht durch ein geschachteltes Iterationsverfahren; wir bezeichnen die aus den einzelnen Umformungschritten resultierende Matrix stets wieder mit $A = (a_{ij})$.

Schritt 1. Wir erreichen durch Zeilen- und Spaltenvertauschungen, dass a_{11} ein Element minimalen Grades ist, d.h., dass $\delta(a_{11}) \leq \delta(a_{ij})$ für alle $a_{ij} \neq 0_R$ gilt.

Schritt 2. Wir wählen Darstellungen $a_{i1} = q_i a_{11} + r_i$ mit $r_i = 0_R$ oder $\delta(r_i) < \delta(a_{11})$ und erreichen durch Addieren des $-q_i$-Fachen der ersten zur i-ten Zeile, dass a_{i1} durch r_i ersetzt wird, d.h., wir haben nach diesem Schritt $a_{i1} = 0_R$ oder $\delta(a_{i1}) < \delta(a_{11})$ für alle $2 \leq i \leq m$.

Schritt 3. Wir wählen Darstellungen $a_{1j} = q_j a_{11} + r_j$ mit $r_j = 0_R$ oder $\delta(r_i) < \delta(a_{11})$ und erreichen durch Addieren des $-q_j$-Fachen der ersten zur j-ten Spalte, dass a_{1j} durch r_j ersetzt wird, d.h., wir haben nach diesem Schritt $a_{1j} = 0_R$ oder $\delta(a_{1j}) < \delta(a_{11})$ für alle $2 \leq j \leq n$.

Falls $\delta(a_{11})$ nicht mehr minimal unter den $\delta(a_{ij})$ ist, so steigen wir wieder bei Schritt 1 ein. Da $\delta(a_{11})$ im neuen Durchlauf echt verringert wird, terminiert das Verfahren nach endlich vielen Iterationen der Schritte 1, 2 und 3 mit einer Matrix A der Form

$$A \quad = \quad \begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & * & \ldots & * \\ \vdots & \vdots & & \vdots \\ 0 & * & \ldots & * \end{pmatrix}, \qquad \text{wobei } \delta(a_{11}) \leq \delta(a_{ij}), \text{ sobald } a_{ij} \neq 0_R.$$

Schritt 4. Falls der Eintrag a_{11} nicht alle anderen Einträge der Matrix A teilt, etwa $a_{11} \nmid a_{ij}$, so können wir durch Addieren der 1-ten zur j-ten Spalte und anschließendes Addieren eines geeigneten Vielfachen der 1-ten zur i-ten Zeile erreichen, dass $\delta(a_{ij}) < \delta(a_{11})$ gilt.

Iteration der Schritte 1,2,3 und 4 bringt A auf die obige Blockgestalt, wobei a_{11} nun jeden weiteren Eintrag a_{ij} teilt. Man beachte, dass bei jeder Iteration $\delta(a_{11})$ echt verringert wird; die Iteration der Schritte 1,2,3 und 4 bricht also spätestens dann ab, wenn $\delta(a_{11})$ minimal unter allen $\delta(r)$, $r \in R$, ist, was $a_{11} \in R^*$ impliziert.

Jetzt kann man das bisherige Verfahren auf den rechten unteren Block anwenden. Da die in den einzelnen Schritten neu gewonnenen Einträge stets Summen von Vielfachen der alten sind, ist sichergestellt, dass a_{11} auch weiterhin alle anderen Einträge teilt.

So reduziert man Schritt für Schritt die Größe des noch zu behandelnden Blocks und kommt schließlich zu dem Fall, dass dieser nur noch aus eine Zeile oder einer Spalte besteht. In diesem Fall führt Iteration der Schritte 1,2 und 3 dann zum gewünschten Ergebnis. □

Folgerung 4.1.7. *Es seien R ein euklidischer Ring und $A \in \mathrm{Mat}(n,n;R)$. Dann sin folgende Aussagen äquivalent.*

(i) *Die Matrix A ist invertierbar in* $\mathrm{Mat}(n,n;R)$.
(ii) *Die Matrix A ist ein Produkt von Elementarmatrizen aus* $\mathrm{Mat}(n,n;R)$.

Satz 4.1.8. *Es seien R ein euklidischer Ring, F ein freier R-Modul von endlichem Rang und $M \leq_R F$ ein Untermodul. Dann gibt es eine Basis $(v_1,\ldots,v_m)$ von F und Elemente $a_1,\ldots,a_s \in R$ mit*

(i) *$(a_1v_1,\ldots,a_sv_s)$ ist eine Basis für M,*
(ii) *es gilt $a_i | a_{i+1}$ für $1 \leq i \leq s-1$.*

Lemma 4.1.9. *Es seien R ein Integritätsring und $A \in \mathrm{Mat}(m,n;R)$ eine Matrix.*

(i) *Es gilt $\mathrm{Lin}(A_{*1},\ldots,A_{*n}) = \mathrm{Lin}((A\cdot T)_{*1},\ldots,(A\cdot T)_{*n})$ für jede Matrix $T \in \mathrm{Mat}(n,n;R)^*$.*
(ii) *Sind invertierbare Matrizen $S \in \mathrm{Mat}(m,m;R)^*$ und $T \in \mathrm{Mat}(n,n;R)^*$ gegeben mit*

$$S\cdot A\cdot T \;=\; \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix},$$

wobei D eine Diagonalmatrix mit Einträgen $a_1,\ldots,a_r \neq 0_R$ ist, so ist $(a_1\cdot S^{-1}\cdot e_1,\ldots,a_r\cdot S^{-1}\cdot e_r)$ eine Basis für $\mathrm{Lin}(A_{*1},\ldots,A_{*n})$.

Beweis. Zu (i). Um zu sehen, dass die Inklusion "$\supseteq$" gilt, genügt es zu zeigen, dass stets $(A\cdot T)_{*j} \in \mathrm{Lin}(A_{*1},\ldots,A_{*n})$ gilt. Das ergibt sich mit

$$(A\cdot T)_{*j} \;=\; \begin{pmatrix} a_{11}t_{1j}+\ldots+a_{1n}t_{nj} \\ \vdots \\ a_{m1}t_{1j}+\ldots+a_{mn}t_{nj} \end{pmatrix} \;=\; t_{1j}\cdot A_{*1}+\ldots+t_{nj}\cdot A_{*n}.$$

Die Inklusion "$\subseteq$" ergibt sich durch Anwenden der eben durchgeführten Überlegung auf die Matrizen $A\cdot T$ und $(A\cdot T)\cdot T^{-1}$: Es gilt

$$\begin{aligned} \mathrm{Lin}(A_{*1},\ldots,A_{*n}) &= \mathrm{Lin}((A\cdot T\cdot T^{-1})_{*1},\ldots,(A\cdot T\cdot T^{-1})_{*n}) \\ &\subseteq \mathrm{Lin}((A\cdot T)_{*1},\ldots,(A\cdot T)_{*n}). \end{aligned}$$

Zu (ii). Die Familie ist $(a_1 \cdot e_1, \ldots, a_r \cdot e_r)$ ist offensichtlich eine Basis für den Untermodul

$$\mathrm{Lin}((S \cdot A \cdot T)_{*1}, \ldots, (S \cdot A \cdot T)_{*n}) \;=\; \mathrm{Lin}((S \cdot A)_{*1}, \ldots, (S \cdot A)_{*n}),$$

wobei die Gleichung nach Aussage (i) gilt. Somit ist $(a_1 \cdot S^{-1} \cdot e_1, \ldots, a_r \cdot S^{-1} \cdot e_r)$ eine Basis für den Untermodul

$$S^{-1} \cdot \mathrm{Lin}((S \cdot A)_{*1}, \ldots, (S \cdot A)_{*n}) \;=\; \mathrm{Lin}(A_{*1}, \ldots, A_{*n}).$$

□

Beweis von Satz 4.1.8. Wir dürfen annehmen, dass $F = R^m$ gilt. Nach Satz 3.2.13 ist M endlich erzeugt, etwa durch $u_1, \ldots, u_n$. Wir betrachten die Matrix

$$A \;:=\; (u_1, \ldots, u_n).$$

Satz 4.1.6 liefert uns invertierbare Matrizen $S = S_k \cdots S_1$ und $T = T_1 \cdots T_l$, mit

$$S \cdot A \cdot T \;=\; \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix},$$

wobei D Diagonalgestalt mit nichtrivialen Diagonaleinträgen $a_1, \ldots, a_s \neq 0_R$ besitzt und stets $a_i | a_{i+1}$ gilt.

Nach Lemma 4.1.9 (ii) besitzt die Basis $(S^{-1} \cdot e_1, \ldots, S^{-1} \cdot e_m)$ die gewünschten Eigenschaften. □

Bemerkung 4.1.10. Ist eine Matrix A über einem euklidischen Ring gegeben, so sucht man bisweilen invertierbare Matrizen $S = S_k \cdots S_1$ und $T = T_1 \cdots T_l$, sodass $S \cdot A \cdot T$ Smith-Normalform annimmt. Als Beispiel betrachten wir

$$A \;:=\; \begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix} \;\in\; \mathrm{Mat}(2,3;\mathbb{Z}).$$

Wie im entsprechenden Verfahren für Matrizen über Körpern verschafft man sich S und T, indem man die benötigten Zeilen- und Spaltenoperationen durch sukzessives Anwenden auf Einheitsmatrizen mitführt:

$$\begin{aligned}
&\left(\begin{pmatrix} 1 & -1 & 1 \\ 1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) \\
\xrightarrow{\mathrm{ZOp}(-1;1,2)} \quad &\left(\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) \\
\xrightarrow{\mathrm{ZOp}(1;2,1)} \quad &\left(\begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) \\
\xrightarrow{\mathrm{SpOp}(1;1,3)} \quad &\left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right) \\
\xrightarrow{\mathrm{SpOp}(2;2,3)} \quad &\left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}\right)
\end{aligned}$$

Damit haben wir Matrizen S und T gefunden, sodass $S \cdot A \cdot T$ Smith-Normalform besitzt, nämlich

$$S \;:=\; \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \qquad T \;:=\; \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Analog erhält man eine invertierbare Matrix S, sodass $S \cdot A$ Hermite-Normalform besitzt, indem man wie oben die benötigten Zeilenoperationen mitführt.

Aufgaben zu Abschnitt 4.1.

Aufgabe 4.1.11. Bestimme Hermite- und Smith-Normalform der ganzzahligen Matrix A in den folgenden Fällen:

$$A := \begin{pmatrix} 12 & -4 & 8 \\ -6 & 4 & -2 \end{pmatrix}, \qquad A := \begin{pmatrix} 3 & 4 & 0 \\ -3 & -2 & 2 \\ -3 & -4 & 2 \end{pmatrix}$$

Gib ganzzahlige Matrizen S und T an, sodass $S{\cdot}A$ bzw. $S{\cdot}A{\cdot}T$ die jeweilige Hermite- bzw. Smith-Normalform annimmt.

Aufgabe 4.1.12. Es seien R ein Integritätsring, $A \in \mathrm{Mat}(m,n;R)$ und $S \in \mathrm{Mat}(n,n;R)^*$, sodass $B := S{\cdot}A^t$ Zeilenstufenform mit r Pivoteinträgen besitzt. Betrachte die zu A gehörige lineare Abbildung $\mu_A\colon R^n \to R^m$, $v \mapsto A{\cdot}v$ und zeige:

(i) Die Zeilen $B_{1*}, \ldots, B_{r*}$ bilden eine Basis für $\mathrm{Bild}(\mu_A) \leq_R R^m$.
(ii) Die Zeilen $S_{r+1*}, \ldots, S_{n*}$ bilden eine Basis für $\mathrm{Kern}(\mu_A) \leq_R R^n$.

Aufgabe 4.1.13. Bestimme Basen für Kern und Bild der linearen Abbildung $\mu_A\colon \mathbb{Z}^4 \to \mathbb{Z}^4$, $v \mapsto A{\cdot}v$, wobei

$$A = \begin{pmatrix} -2 & 2 & 4 & 4 \\ -2 & 3 & 2 & 2 \\ -3 & 3 & 2 & -1 \\ -3 & 3 & 2 & -1 \end{pmatrix}$$

4.2. **Die Struktursätze.**

Satz 4.2.1. *Es seien R ein euklidischer Ring und M ein endlich erzeugter R-Modul. Dann gibt es eine direkte Zerlegung*

$$M \;\cong\; F \,\oplus\, T(M)$$

mit einem endlich erzeugten freien Untermodul $F \leq_R M$ und dem Torsionsmodul $T(M) \leq_R M$. Es gilt weiter

$$F \;\cong\; R^l, \qquad\qquad T(M) \;\cong\; \bigoplus_{i=1}^{m} R/\langle a_i\rangle$$

mit $l \in \mathbb{Z}_{\geq 0}$ und $0_R \neq a_1, \ldots, a_m \in R \setminus R^*$, sodass $a_i | a_{i+1}$ gilt; dabei ist l eindeutig und $a_1, \ldots, a_m \in R$ sind eindeutig bis auf Assoziiertheit.

Lemma 4.2.2. *Es seien R ein K1-Ring, M_i, $i \in I$, R-Moduln und $N_i \leq_R M_i$ Untermoduln. Dann gilt*

$$\left(\bigoplus_{i\in I} M_i\right) \Big/ \left(\bigoplus_{i\in I} N_i\right) \;\cong\; \bigoplus_{i\in I} M_i/N_i.$$

Beweis. Man hat einen kanonischen surjektiven Homomorphismus von R-Moduln:

$$\varphi\colon \bigoplus_{i\in I} M_i \;\to\; \bigoplus_{i\in I} M_i/N_i, \qquad (u_i)_{i\in I} \;\mapsto\; (u_i + N_i)_{i\in I}$$

mit $\ker(\varphi) = \bigoplus_{i\in I} N_i$. Der Homomorphiesatz 3.1.22 liefert die Behauptung. □

Beweis von Satz 4.2.1. Es seien $u_1, \ldots, u_n \in M$ Erzeugende für M. Dann erhalten wir einen surjektiven Homomorphismus von R-Moduln:

$$\pi\colon R^n \;\to\; M, \qquad (r_1, \ldots, r_n) \;\mapsto\; r_1u_1 + \ldots + r_nu_n.$$

Der Homomorphiesatz 3.1.22 liefert $M \cong R^n/N$ mit $N := \mathrm{Kern}(\pi)$. Nach Satz 4.1.8 gibt es eine Basis $(v_1, \ldots, v_n)$ für R^n und $a_1, \ldots, a_s \in R \setminus \{0_R\}$ mit $a_i | a_{i+1}$ und

$$N \;=\; R{\cdot}a_1{\cdot}v_1 \,\oplus\, \ldots \,\oplus\, R{\cdot}a_s{\cdot}v_s.$$

Mit Hilfe von Lemma 4.2.2 können wir also den Modul $M \cong R^n/N$ gut beschreiben: Sind $a_1, \ldots, a_k$ die Einheiten unter den a_i, so erhalten wir

$$\begin{aligned}
M \;&\cong\; R^n/N \\
&\cong\; (R{\cdot}v_1 \oplus \ldots \oplus R{\cdot}v_n) \,/ (R{\cdot}a_1{\cdot}v_1 \,\oplus\, \ldots \,\oplus\, R{\cdot}a_s{\cdot}v_s, R{\cdot}v_{s+1} \oplus \ldots \oplus R{\cdot}v_n) \\
&\cong\; \bigoplus_{i=1}^{k} R/\langle a_i\rangle \,\oplus\, \bigoplus_{i=k+1}^{s} R/\langle a_i\rangle \,\oplus\, R^{n-s} \\
&\cong\; R^{n-s} \,\oplus\, \bigoplus_{i=k+1}^{s} R/\langle a_i\rangle.
\end{aligned}$$

Dabei ist der erste Summand ein freier R-Modul, und der zweite Summand ist der Torsionsmodul; er wird durch das Element $0 \neq a_{k+1} \cdots a_s$ annulliert.

Die Zahl l ist als Rang von $M/T(M)$ eindeutig. Die Eindeutigkeitsaussage über $a_{k+1}, \ldots, a_s \in R$ ist eine direkte Anwendung von Satz 3.4.11. □

Definition 4.2.3. Es seien R ein euklidischer Ring, M ein R-Modul und $p \in R$ ein Primelement.

(i) Ein Element $v \in M$ heißt *p-Torsionselement*, falls $p^n \cdot v = 0$ mit einem $n \in \mathbb{Z}_{\geq 0}$ gilt.

(ii) Der *p-Torsionsmodul von M* ist der Untermodul $M_p \leq_R M$ aller p-Torsionselemente von M.
(iii) Falls $M = M_p$ gilt, so nennt man den Modul M selbst einen *p-Torsionsmodul*.

Satz 4.2.4. *Es seien R ein euklidischer Ring, $P \subset R$ ein Primsystem und M ein endlich erzeugter R-Modul. Dann gibt es eine Zerlegung*

$$M \quad \cong \quad F \ \oplus \ T(M).$$

mit einem endlich erzeugten freien Untermodul $F \leq_R M$ und dem Torsionsmodul $T(M) \leq_R M$. Nur endlich viele p-Torsionsmoduln $M_p \leq_R M$ sind nichttrivial und man hat

$$F \ \cong \ R^l, \qquad T(M) \ \cong \ \bigoplus_{p \in P} M_p, \qquad M_p \ \cong \ \bigoplus_{i=1}^{d(p)} R/\langle p^{\nu_{p,i}} \rangle$$

mit ganzen Zahlen l und $1 \leq \nu_{p,1} \leq \ldots \leq \nu_{p,d(p)}$. Die Zahlen l sowie $d(p)$ und $\nu_{p,1}, \ldots, \nu_{p,d(p)}$ sind dabei durch den Isomorphietyp von M eindeutig bestimmt.

Beweis. Satz 4.2.1 liefert eine Zerlegung $M \cong F \oplus T(M)$ in einen freien Anteil und den Torsionsmodul sowie $0_R \neq a_1, \ldots, a_m \in R \setminus R^*$ mit $a_i | a_{i+1}$ und

$$T(M) \quad \cong \quad \bigoplus_{i=1}^{m} R/\langle a_i \rangle.$$

Wir müssen den Torsionsmodul $T(M)$ auf geeignete Weise als direkte Summe seiner p-Torsionsmoduln darstellen. Dazu betrachten wir die Primfaktorzerlegungen

$$a_i \quad = \quad c_i \prod_{p \in P} p^{\nu(p,i)}$$

mit Einheiten $c_i \in R^*$ und Exponenten $\nu(p,i) \in \mathbb{Z}_{\geq 0}$. Mit der Variante 3.4.10 des Chinesischen Restsatzes erhalten wir eine Zerlegung von R-Moduln:

$$R/\langle a_i \rangle \quad \cong \quad \bigoplus_{p \in P} R/\langle p^{\nu(p,i)} \rangle. \tag{4.2.4.1}$$

Damit gehen wir in die Zerlegung von $T(M)$ und fassen für jedes $p \in P$ alle Terme der Form $R/\langle p^{\nu(p,i)} \rangle$ zu einem Summanden zusammen. Das ergibt

$$\begin{aligned} \bigoplus_{i=1}^{m} R/\langle a_i \rangle \quad &\cong \quad \bigoplus_{i=1}^{m} \left(\bigoplus_{p \in P} R/\langle p^{\nu(p,i)} \rangle \right) \\ &\cong \quad \bigoplus_{p \in P} \left(\bigoplus_{i=1}^{m} R/\langle p^{\nu(p,i)} \rangle \right) \\ &=: \quad \overline{M}. \end{aligned}$$

Man beachte, dass wegen der Teilbarkeitsrelationen $a_i | a_{i+1}$ stets $\nu(p,i) \leq \nu(p,i+1)$ gelten muss. Für jedes $p \in P$ setzen wir

$$d(p) \quad := \quad |\{i;\ \nu_{p,i} > 0\}|,$$

und für p mit $d(p) \neq 0$ definieren wir $\nu_{p,i} := \nu(p, i + m_p)$, wobei m_p die erste Zahl mit $\nu(p, 1 + m_p) > 0$ bezeichne. Dann haben wir

$$\overline{M} \quad = \quad \bigoplus_{p \in P} \left(\bigoplus_{i=1}^{d(p)} R/\langle p^{\nu_{p,i}} \rangle \right).$$

Zum Beweis der Existenzaussage müssen wir also nur noch zeigen, dass wir den p-Torsionsmodul $\overline{M}_p \leq_R \overline{M}$ erhalten als

$$\overline{M}_p \;=\; M'_p \;:=\; \bigoplus_{i=1}^{d(p)} R/\langle p^{\nu_{p,i}}\rangle.$$

Jedes M'_p enthält nur p-Torsionselemente. Ist ein p-Torsionselement $v \in \overline{M}_p$ gegeben, so haben wir eine eindeutige Darstellung mit Elementen $v_p \in M'_p$ und $v_q \in M'_q$:

$$v \;=\; v_p + \sum_{p\neq q\in P} v_q.$$

Da v ein p-Torsionselement ist, gibt es ein $\nu \in \mathbb{Z}_{\geq 1}$ mit $p^\nu \cdot v_q = 0$ für alle $q \in P$. In jedem M'_q erhalten wir mit geeigneten $r_{q,i} \in R$:

$$0 \;=\; p^\nu \cdot v_q \;=\; p^\nu \sum_{i=1}^{d(q)} r_{q,i} + \langle q^{\nu_{q,i}}\rangle \;=\; \sum_{i=1}^{d(q)} p^\nu r_{q,i} + \langle q^{\nu_{q,i}}\rangle$$

Das bedeutet $p^\nu r_{q,i} \in \langle q^{\nu_{q,i}}\rangle$. Falls $q \neq p$ gilt, muss also $q^{\nu_{q,i}}$ stets ein Teiler von $r_{q,i}$ sein. Das bedeutet $v_q = 0$ und somit $v = v_p \in M'_p$.

Zur Eindeutigkeitsaussage: Es ist klar, dass der Isomorphietyp des p-Torsionsmoduls $M_p \leq M$ durch den von M festgelegt ist. Die Eindeutigkeit der Zahlen $d(p)$ und $\nu_{p,i}$ ergibt sich daher mit Lemma 3.4.11. □

Definition 4.2.5. Wir nennen eine abelsche Gruppe *endlich erzeugt*, wenn sie als $\mathbb{Z}$-Modul endlich erzeugt ist.

Folgerung 4.2.6 (Hauptsatz für endlich erzeugte abelsche Gruppen)**.** *Es sei G eine endlich erzeugte abelsche Gruppe. Dann hat man eine eindeutige Darstellung*

$$G \;\cong\; \mathbb{Z}^d \;\times\; \prod_{p\in P}\left[\prod_{i=1}^{d(p)} \mathbb{Z}/p^{\nu_{p,i}}\mathbb{Z}\right]$$

wobei $P \subset \mathbb{Z}_{\geq 2}$ die Menge der Primzahlen bezeichnet, $d(p) > 0$ für höchstens endlich viele p gilt und für diese p stets $1 \leq \nu_{p,1} \leq \ldots \leq \nu_{p,d(p)}$ erfüllt ist.

Beweis. Als endlich erzeugte abelsche Gruppe ist G ein endlich erzeugter $\mathbb{Z}$-Modul, siehe Beispiel 3.1.5. Satz 4.2.4 liefert daher die gewünschte Zerlegung von G. □

Beispiel 4.2.7. Mit Hilfe der Eindeutigkeitsaussage von Satz 4.2.6 kann man oft schnell entscheiden, ob zwei gegebene abelsche Gruppen isomorph zueinander sind oder nicht, etwa

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \;\ncong\; \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Definition 4.2.8. Es seien R ein euklidischer Ring, M ein endlich erzeugter R-Modul und $T(M) \leq_R M$ der zugehörige Torsionsmodul.

(i) *Elementarteiler* für M sind nichttriviale Nichteinheiten $a_1, \ldots, a_m \in R$ mit $a_i | a_{i+1}$ für $i = 1, \ldots, m-1$, sodass

$$T(M) \;\cong\; \bigoplus_{i=1}^{m} R/\langle a_i\rangle.$$

(ii) *Primäre Elementarteiler* für M sind $p_i^{\nu_{ij}} \in R$ mit paarweise nichtassoziierten Primelementen $p_1, \ldots, p_r \in R$ und $1 \leq \nu_{i1} \leq \ldots \leq \nu_{id_i}$, sodass

$$T(M) \quad \cong \quad \bigoplus_{i=1}^{r} \left(\bigoplus_{j=1}^{d_i} R/\langle p_i^{\nu_{ij}} \rangle \right).$$

Beispiel 4.2.9. Wir betrachten den $\mathbb{Z}$-Modul $M := \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ und wollen Elementarteiler sowie primäre Elementarteiler dafür bestimmen. Mit der Variante 3.4.10 des Chinesischen Restsatzes erhalten wir

$$M \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

Die letzte Darstellung ist wie in Satz 4.2.4. Folglich sind $2^1, 2^2, 3^1$ primäre Elementarteiler für M. Um Elementarteiler zu gewinnen schreiben wir die primären Elementarteiler in ein Schema

$$\begin{array}{ll} p = 2: & 2, \quad 2^2, \\ p = 3: & 1, \quad 3. \end{array}$$

Aufmultiplizieren der Spalten ergibt dann Elementarteiler $a_1 = 2 \cdot 1 = 2$ und $a_2 = 2^2 \cdot 3 = 12$ für M. Um dies zu verifizieren, verwenden wir nochmals Variante 3.4.10 des Chinesischen Restsatzes: Sie liefert

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong M.$$

Bemerkung 4.2.10. Es seien R ein euklidischer Ring, M ein endlich erzeugter R-Modul.

(i) Elementarteiler für M sind bis auf Assoziiertheit eindeutig bestimmt. Sie legen den Torsionsmodul $T(M)$ bis auf Isomorphie fest.

(ii) Primäre Elementarteiler von M sind bis auf Assoziiertheit eindeutig bestimmt. Sie legen den Torsionsmodul $T(M)$ sowie die p-Torsionsmoduln M_p bis auf Isomorphie fest.

(iii) Hat man Elementarteiler $a_1, \ldots, a_m$ für M vorliegen, so wählt man ein Primsystem $P \subset R$ und betrachtet die Primfaktorzerlegungen

$$a_1 = c_1 \cdot p_1^{\nu_{11}} \cdots p_r^{\nu_{r1}}, \quad \ldots, \quad a_m = c_m \cdot p_1^{\nu_{1d_1}} \cdots p_r^{\nu_{rd_r}}.$$

Die darin auftretenden Primpotenzen $p_i^{\nu_{ij}}$ sind dann primäre Elementarteiler für M, wobei die $p_i^{\nu_{ij}} = 1$ jeweils zu entfernen sind.

(iv) Hat man primäre Elementarteiler $p_i^{\nu_{ij}}$, wobei $1 \leq i \leq r$ und $1 \leq \nu_{i1} \leq \ldots \leq \nu_{id_i}$, für M vorliegen, so betrachtet man das Schema

$$\begin{array}{ccccccc} 1 & \ldots & 1 & p_1^{\nu_{11}} & \ldots & p_1^{\nu_{1d_1}} \\ & & \vdots & & & \\ p_m^{\nu_{m1}} & \ldots & & & \ldots & p_m^{\nu_{md_m}} \\ & & \vdots & & & \\ 1 & \ldots & 1 & p_r^{\nu_{r1}} & \ldots & p_r^{\nu_{rd_r}} \end{array}$$

wobei d_m maximal unter den d_i. Aufmultiplizieren der Einträge aus den Spalten liefert dann Elementarteiler $a_r = p_1^{\nu_{1d_1}} \cdots p_r^{\nu_{rd_r}}$, etc., für M.

Aufgaben zu Abschnitt 4.2.

Aufgabe 4.2.11. Bestimme Elementarteiler und primäre Elementarteiler für die folgenden $\mathbb{Z}$-Moduln:

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \qquad \mathbb{Z}/4\mathbb{Z}, \qquad \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \qquad \mathbb{Z}/72\mathbb{Z}.$$

Aufgabe 4.2.12. Es seien $m, n \in \mathbb{Z}_{\geq 1}$. Beweise die Äquivalenz folgender Aussagen:

(i) Es gilt $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
(ii) Die Zahlen m und n sind teilerfremd.

Aufgabe 4.2.13. Es seien R ein euklidischer Ring und $A \in \mathrm{Mat}(m, n; R)$. Beweise die Eindeutigkeit der Smith-Normalform: Sind S, T und S', T' invertierbare Matrizen, sodass

$$S \cdot A \cdot T = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \qquad S' \cdot A \cdot T' = \begin{pmatrix} D' & 0 \\ 0 & 0 \end{pmatrix}$$

jeweils Smith-Normalform besitzen, so gilt $d'_{ii} \sim d_{ii}$ für die Diagonaleinträge der Matrizen D bzw. D'.

Aufgabe 4.2.14. Es seien R ein euklidischer Ring, F ein freier R-Modul vom Rang n und $M \leq_R F$ ein Untermodul. Beweise die Äquivalenz folgender Aussagen:

(i) F/M ist frei.
(ii) F/M ist torsionsfrei.
(iii) Es gibt eine Basis $(v_1, \ldots, v_n)$ mit $M = \mathrm{Lin}(v_1, \ldots, v_m)$ für ein $m \leq n$.
(iv) Für je zwei Elemente $v \in M$ und $0_R \neq r \in R$ gilt: $r \cdot v \in M \implies v \in M$.

5. Normalformentheorie

5.1. **Das Minimalpolynom.**

Erinnerung 5.1.1. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Dann wird V zu einem $\mathbb{K}[T]$-Modul durch

$$\left(\sum a_\nu T^\nu\right) \cdot v \quad := \quad \sum a_\nu \varphi^\nu(v).$$

Gilt $V = \mathbb{K}^n$, so ist φ von der Form $v \mapsto A \cdot v$ mit einer Matrix $A \in \mathrm{Mat}(n, n; \mathbb{K})$ und die $\mathbb{K}[T]$-Modulstruktur auf V ist gegeben durch

$$\left(\sum a_\nu T^\nu\right) \cdot v \quad = \quad \left(\sum a_\nu A^\nu\right) \cdot v.$$

Definition 5.1.2. Es seien R ein K1-Ring und M ein R-Modul. Das *Annullatorideal* $\mathfrak{a}_M \leq_R R$ von M besteht aus allen Ringelementen, die M annullieren:

$$\mathfrak{a}_M \quad := \quad \{a \in R;\ a \cdot v = 0_V \text{ für alle } v \in M\}.$$

Satz 5.1.3. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Dann wird das Annullatorideal*

$$\mathfrak{a}_V \ = \ \{f \in \mathbb{K}[T];\ f \cdot V = \{0_V\}\} \ \leq_{\mathbb{K}[T]} \ \mathbb{K}[T]$$

des $\mathbb{K}[T]$-Moduls V durch ein eindeutig bestimmtes normiertes Polynom $q_\varphi \in \mathbb{K}[T]$ erzeugt; es gilt $q_\varphi \neq 0_{\mathbb{K}[T]}$ und man hat $\deg(q_\varphi) > 0$, sobald $V \neq \{0_V\}$ gilt.

Beweis. Wir zeigen zunächst, dass $\mathfrak{a}_V$ nicht das Nullideal ist. Dazu betrachten wir den folgenden Homomorphismus von Vektorräumen:

$$\mathbb{K}[T] \ \to \ \mathrm{Hom}_{\mathbb{K}}(V, V), \qquad \sum a_\nu T^\nu \ \mapsto \ \sum a_\nu \varphi^\nu.$$

Der Kern dieses Homomorphismus ist genau das Annullatorideal $\mathfrak{a}_V$, denn für jedes Polynom $\sum a_\nu T^\nu$ und jedes $v \in V$ gilt

$$\left(\sum a_\nu \varphi^\nu\right)(v) \ = \ 0_V \quad \Longleftrightarrow \quad \left(\sum a_\nu T^\nu\right) \cdot v \ = \ 0_V.$$

Wäre $\mathfrak{a}_V$ trivial, so wäre $\mathbb{K}[T] \to \mathrm{Hom}(V, V)$ injektiv und somit $\mathbb{K}[T]$ als Vektorraum isomorph zu einem Untervektorraum von $\mathrm{Hom}_{\mathbb{K}}(V, V)$; das ist jedoch unmöglich wegen

$$\dim(\mathbb{K}[T]) \ = \ \infty \ > \ \dim(\mathrm{Hom}(V, V)) \ = \ \dim(V)^2.$$

Da $\mathbb{K}[T]$ ein Hauptidealring ist, gilt $\mathfrak{a}_V = \langle q_\varphi \rangle$ mit einem Polynom $q_\varphi \in \mathbb{K}[T]$. Wegen $\mathfrak{a}_V \neq \{0_{\mathbb{K}[T]}\}$ muss $\deg(q_\varphi) \geq 0$ gelten. Weiter darf man annehmen, dass q_φ normiert ist. Wegen $\mathbb{K}[T]^* = \mathbb{K}^*$ ist q_φ dadurch eindeutig bestimmt.

Es bleibt zu zeigen, dass q_φ positiven Grad besitzt, falls $V \neq \{0_V\}$ gilt. Wäre $\deg(q_\varphi) = 0$, so hätte man $q_\varphi = T^0$ und somit $q_\varphi \cdot v = v$ für jedes $v \in V$. Das ist wegen $q_\varphi \cdot V = \{0_V\} \neq V$ aber nicht möglich. □

Folgerung 5.1.4. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Dann ist der zugehörige $\mathbb{K}[T]$-Modul V ein Torsionsmodul.*

Definition 5.1.5. Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Das *Minimalpolynom* von φ ist der normierte Erzeuger $q_\varphi \in \mathbb{K}[T]$ des Annullatorideals $\mathfrak{a}_V \leq_{\mathbb{K}[T]} \mathbb{K}[T]$.

Beispiel 5.1.6. Wir betrachten den $\mathbb{R}$-Vektorraum $V := \mathbb{R}^2$ und für beliebiges $\lambda \in \mathbb{R}$ die reelle (2×2)-Matrix

$$A \;:=\; \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

und den zugehörigen Endomorphismus $\varphi\colon V \to V$, $v \mapsto A \cdot v$. Für das Polynom $T - \lambda \in \mathbb{R}[T]$ erhalten wir

$$(T-\lambda)\cdot v \;=\; (A - \lambda E_2)\cdot v \;=\; (0,0) \qquad \text{für jedes } v \in \mathbb{R}^2.$$

Somit gilt $T - \lambda \in \mathfrak{a}_M$. Da $\mathfrak{a}_V$ durch ein normiertes Polynom positiven Grades erzeugt wird, muss $T - \lambda$ bereits ein Erzeuger von $\mathfrak{a}_M$ sein, d.h., es gilt

$$q_\varphi \;=\; T - \lambda.$$

Beispiel 5.1.7. Wir betrachten den $\mathbb{R}$-Vektorraum $V := \mathbb{R}^2$ und für beliebiges $\lambda \in \mathbb{R}$ die reelle (2×2)-Matrix

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

und den zugehörigen Endomorphismus $\psi\colon V \to V$, $v \mapsto B \cdot v$. Für jedes Polynom der Form $T - \lambda'$ hat man

$$(T-\lambda')\cdot v \;=\; (B-\lambda'\cdot E_2)\cdot v \;=\; \begin{pmatrix} \lambda-\lambda' & 0 \\ 1 & \lambda-\lambda' \end{pmatrix}\cdot\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \;=\; \begin{pmatrix} (\lambda-\lambda')v_1 \\ v_1 + (\lambda-\lambda')v_2 \end{pmatrix}.$$

Insbesondere kann kein Polynom ersten Grades den gesamten Vektorraum V annullieren. Für das Polynom $(T-\lambda)^2$ gilt jedoch

$$(T-\lambda)^2\cdot v \;=\; \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}^2 \cdot \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \;=\; \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Folglich gilt $(T-\lambda)^2 \in \mathfrak{a}_V$, und wir erhalten, dass $(T-\lambda)^2$ sogar ein Erzeuger für $\mathfrak{a}_V$ ist, d.h., es gilt

$$q_\varphi \;=\; (T-\lambda)^2.$$

Definition 5.1.8. Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Der Vektorraum V heisst *φ-zyklisch*, falls es ein $v \in V$ und ein $k \in \mathbb{Z}_{\geq 1}$ gibt, sodass $(v, \varphi(v), \varphi^2(v), \ldots, \varphi^{k-1}(v))$ eine Basis von V ist.

Bemerkung 5.1.9. Es seien V ein eindimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Dann ist V ein φ-zyklischer Vektorraum: Für $k = 1$ und jedes $0_V \neq v$ ist $(v) = (\varphi^0(v))$ eine Basis für V.

Beispiel 5.1.10. Wir betrachten den $\mathbb{R}$-Vektorraum $V := \mathbb{R}^2$ und für beliebiges $\lambda \in \mathbb{R}$ die beiden reellen (2×2)-Matrizen

$$A \;:=\; \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}, \qquad\qquad B \;:=\; \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}.$$

Mit $\varphi\colon V \to V, v \mapsto A\cdot v$ ist V kein φ-zyklischer Vektorraum, denn es gilt $\varphi(v) \in \mathbb{R}\cdot v$ für jedes $v \in V$.

Mit $\psi\colon V \to V, v \mapsto B\cdot v$ wird V zu einem ψ-zyklischen Vektorraum; für $v := (1,0)$ gilt $\varphi(v) = (\lambda, 1)$ und somit ist $(v, \varphi(v))$ eine Basis für $\mathbb{R}^2$.

Satz 5.1.11. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Dann sind äquivalent:*

(i) *V ist φ-zyklisch.*

(ii) *Man hat einen Isomorphismus von $\mathbb{K}[T]$-Moduln $\mathbb{K}[T]/\langle q\rangle \cong V$ mit einem normierten Polynom $q \in \mathbb{K}[T]$.*

Gilt eine der beiden Aussagen, so ist das Polynom $q \in \mathbb{K}[T]$ aus (ii) das Minimalpolynom von φ und man hat $\deg(q) = \dim(V)$.

Lemma 5.1.12. *Es seien R ein K1-Ring und M ein R-Modul. Dann sind folgende Aussagen äquivalent:*

(i) *Der R-Modul M ist monogen, d.h., es gibt ein $v \in M$ mit $M = R \cdot v$.*
(ii) *Es gibt einen Isomorphismus $R/\mathfrak{b} \cong M$ von R-Moduln mit einem $\mathfrak{b} \leq_R R$.*

Gilt eine der beiden Aussagen, so ist $\mathfrak{b} \leq_R R$ aus (ii) bereits das Annullatorideal des R-Moduls M.

Beweis. Zu "(i)⇒(ii)". In der Situation von (i) haben wir einen surjektiven Homomorphismus von R-Moduln

$$\varepsilon\colon R \;\to\; M, \qquad r \;\mapsto\; r \cdot v.$$

Der Kern dieses Homomorphismus ist genau das Annullatorideal $\mathfrak{a}_M \leq_R R$ von M, denn es gilt

$$\begin{aligned} \varepsilon(r) \;=\; 0_R \quad &\Longleftrightarrow \quad r \cdot v \;=\; 0_M \\ &\Longleftrightarrow \quad r \cdot (r' \cdot v) \;=\; r' \cdot (r \cdot v) \;=\; 0_M \text{ für alle } r' \in R \\ &\Longleftrightarrow \quad r \cdot v' \;=\; 0_M \text{ für alle } v' \in M. \end{aligned}$$

Somit liefert der Homomorphiesatz 3.1.22 einen wohldefinierten Isomorphismus von R-Moduln

$$\overline{\varepsilon}\colon R/\mathfrak{a}_M \;\to\; M, \qquad r + \mathfrak{a}_M \;\mapsto\; r \cdot v.$$

Zu "(ii)⇒(i)". Es sei $\varphi\colon R/\mathfrak{b} \to M$ ein Isomorphismus von R-Moduln. Mit $v := \varphi(1_R + \mathfrak{b})$ erhalten wir dann

$$R \cdot v \;=\; \varphi(R \cdot (1_R + \mathfrak{b})) \;=\; \varphi(R/\mathfrak{b}) \;=\; M.$$

Wir kommen zum Zusatz. Es seien $\mathfrak{a}_M \leq_R R$ das Annullatorideal und $\varphi\colon R/\mathfrak{b} \to M$ ein Isomorphismus von R-Moduln mit einem weiteren Ideal $\mathfrak{b} \leq_R R$. Wir zeigen

$$\mathfrak{a}_M \quad = \quad \mathfrak{b}.$$

Zu "$\subseteq$". Es sei $r \in \mathfrak{a}_M$ gegeben. Dann gilt $0_M = r \cdot \varphi(1_R + \mathfrak{b}) = \varphi(r + \mathfrak{b})$. Da φ injektiv ist, muss $r + \mathfrak{b}$ das Nullelement in $R/\mathfrak{b}$ sein. Das bedeutet $r \in \mathfrak{b}$.

Zu "$\supseteq$". Es sei $r \in \mathfrak{b}$ gegeben. Dann annulliert r jedes Element aus $R/\mathfrak{b}$ und somit erhalten wir für jedes $v \in M$:

$$r \cdot v \;=\; r \cdot (\varphi(\varphi^{-1}(v))) \;=\; \varphi(r \cdot \varphi^{-1}(v)) \;=\; \varphi(0_{R/\mathfrak{b}}) \;=\; 0_M.$$

□

Lemma 5.1.13. *Es seien $\mathbb{K}$ ein Körper und $q \in \mathbb{K}[T]$ ein Polynom positiven Grades. Dann hat man zueinander inverse Isomorphismen von $\mathbb{K}$-Vektorräumen*

$$\begin{aligned} \bigoplus_{\nu=0}^{\deg(q)-1} \mathbb{K} \cdot T^\nu \quad &\longleftrightarrow \quad \mathbb{K}[T]/\langle q\rangle \\ f \quad &\mapsto \quad f + \langle q\rangle \\ r_f \quad &\mapsfrom \quad f + \langle q\rangle, \end{aligned}$$

wobei $r_f \in \mathbb{K}[T]$ durch die eindeutige Darstellung $f = g_f q + r_f$ mit $g_f, r_f \in \mathbb{K}[T]$ und $\deg(r_f) < \deg(f)$ oder $r_f = 0_{\mathbb{K}[T]}$ definiert ist. Insbesondere gilt

$$\dim(\mathbb{K}[T]/\langle q\rangle) \quad = \quad \deg(q).$$

Beweis. Die Abbildung $f \mapsto f + \langle q \rangle$ ist die Einschränkung der kanonischen linearen Abbildung $\mathbb{K}[T] \to \mathbb{K}[T]/\langle q \rangle$. Weiter haben wir

$$f = r_f \text{ falls } \deg(f) < \deg(q), \qquad f - r_f = g_f q \in \langle q \rangle \text{ für alle } f \in \mathbb{K}[T].$$

Damit ergibt sich, dass beide Abbildungen invers zueinander sind. Es folgt weiter, dass sie Isomorphismen sind. □

Beweis von Satz 5.1.11. Zu "(i)⇒(ii)". Nach Lemma 5.1.12 genügt es zu zeigen, dass der $\mathbb{K}[T]$-Modul V monogen ist. Dazu wählen wir einen Vektor $v \in V$, sodass $(v, \varphi(v), \ldots, \varphi^{k-1}(v))$ eine Basis von V ist. Dann ist jedes Element $w \in V$ von der Gestalt

$$w \;=\; \sum_{\nu=0}^{k-1} a_\nu \cdot \varphi^\nu(v) \;=\; \left(\sum_{\nu=0}^{k-1} a_\nu T^\nu \right) \cdot v.$$

Zu "(ii)⇒(i)". Es sei $k := \deg(q)$. Nach Lemma 5.1.13 erhalten wir eine Basis $(w_0, \ldots, w_{k-1})$ für den $\mathbb{K}$-Vektorraum $\mathbb{K}[T]/\langle q \rangle$ durch

$$w_i \;:=\; T^i + \langle q \rangle \;=\; T^i \cdot w_0.$$

Es sei nun $\imath\colon \mathbb{K}[T]/\langle q \rangle$ ein Isomorphismus von $\mathbb{K}[T]$-Moduln. Wir setzen $v := \imath(w_0)$ und erhalten

$$\imath(w_i) \;=\; \imath(T^i \cdot w_0) \;=\; T^i \cdot \imath(w_0) \;=\; \varphi^i(v).$$

Als Isomorphismus von $\mathbb{K}[T]$-Moduln ist $\imath$ insbesondere ein Isomorphismus von $\mathbb{K}$-Vektorräumen und somit ist $(v, \varphi(v), \ldots, \varphi^{k-1}(v))$ eine Basis für V.

Wir kommen zum Zusatz. In der Situation von (ii) garantiert der Zusatz in Lemma 5.1.12, dass $\langle q \rangle$ das Annullatorideal des $\mathbb{K}[T]$-Moduls V ist. Somit gilt $q = q_\varphi$. Mit Lemma 5.1.13 erhalten wir weiter $\dim(V) = \deg(q_\varphi)$. □

Aufgaben zu Abschnitt 5.1.

Aufgabe 5.1.14. Es seien $n_1, \ldots, n_k \in \mathbb{Z}_{\geq 2}$. Zeige, dass das Annullatorideal des $\mathbb{Z}$-Moduls $\mathbb{Z}/n_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/n_k\mathbb{Z}$ durch $\mathrm{kgV}(n_1, \ldots, n_k)$ erzeugt wird.

Aufgabe 5.1.15. Betrachte den Körper $\mathbb{K} := \mathbb{Z}/2\mathbb{Z}$. Bestimme alle $A \in \mathrm{Mat}(2, 2; \mathbb{K})$, sodass $\mathbb{K}^2$ ein φ-zyklischer Vektorraum ist, wobei $\varphi\colon \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto A \cdot v$.

Aufgabe 5.1.16. Es seien $\mathbb{K}$ ein Körper, $A \in \mathrm{Mat}(n, n; \mathbb{K})$ und $\varphi\colon \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto A \cdot v$ die zu A gehörige lineare Abbildung. Für $C \in \mathrm{Mat}(n, n; \mathbb{K}[T])$ setze

$$C \cdot (e_1, \ldots, e_n) \;:=\; \left(\sum_{j=1}^{n} c_{1j} * e_j, \ldots, \sum_{j=1}^{n} c_{nj} * e_j \right),$$

wobei "$*$" für die Skalarmultiplikation in dem durch φ definierten $\mathbb{K}[T]$-Modul steht. Betrachte nun die Matrix

$$B \;:=\; T \cdot E_n - A \;\in\; \mathrm{Mat}(n, n; \mathbb{K}[T])$$

und das zu A gehörige charakteristische Polynom $p_A = \det(B)$. Beweise die folgenden Aussagen:

(i) Es gilt $B \cdot (e_1, \ldots, e_n) = (0, \ldots, 0)$.
(ii) Es gibt eine Matrix $B^{\#} \in \mathrm{Mat}(n, n; \mathbb{K}[T])$ mit $B^{\#} \cdot B = p_A E_n$.
(iii) Es gilt $p_A * v = (0, \ldots, 0)$ für jedes $v \in \mathbb{K}^n$.

Folgere daraus, dass das charakteristische Polynom eines Endomorphismus $V \to V$ stets ganz V annulliert.

5.2. **Rationale Normalform und Elementarteiler.**

Bemerkung 5.2.1. Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Um $\varphi\colon V \to V$ gut zu verstehen, versucht man, V in möglichst einfache "φ-invariante Bausteine" zu zerlegen, d.h.,

$$V \;=\; V_1 \oplus \ldots \oplus V_r, \quad \text{wobei } V_i \leq_{\mathbb{K}} V \text{ mit } \varphi(V_i) \subseteq V_i.$$

Gelingt dies, so genügt es, die Einschränkungen $\varphi_{|V_i}\colon V_i \to V_i$ zu untersuchen. Der Weg hierzu führt über die durch $\varphi\colon V \to V$ definierte $\mathbb{K}[T]$-Modulstruktur auf V und die Hauptsätze für Moduln über euklidischen Ringen.

Zur Erinnerung: Jeder endlich erzeugte Torsionsmodul M über einem euklidischen Ring R ist von der Gestalt

$$M \;\cong\; \bigoplus_{i=1}^{m} R/\langle a_i\rangle$$

mit Elementarteilern $0_R \neq a_1, \ldots, a_m \in R\backslash R^*$ des Moduls M; diese erfüllen $a_i | a_{i+1}$ für $1 \leq i \leq m-1$ und bis auf Assoziiertheit eindeutig bestimmt.

Definition 5.2.2. Es seien $\mathbb{K}$ ein Körper und V ein endlichdimensionaler $\mathbb{K}$-Vektorraum. Die *Elementarteiler* eines Endomorphismus $\varphi\colon V \to V$ sind die normierten Elementarteiler $q_1, \ldots, q_r \in \mathbb{K}[T]$ des durch φ definierten $\mathbb{K}[T]$-Moduls V.

Satz 5.2.3. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi, \psi\colon V \to V$ zwei Endomorphismen. Dann sind folgende Aussagen äquivalent:*

(i) *Es gibt einen Vektorraumisomorphismus $\kappa\colon V \to V$ mit $\psi = \kappa \circ \varphi \circ \kappa^{-1}$.*
(ii) *φ und ψ definieren isomorphe $\mathbb{K}[T]$-Modulstrukturen auf V.*
(iii) *φ und ψ haben dieselben Elementarteiler.*

Beweis. Die Äquivalenz der Aussagen (ii) und (iii) ist eine direkte Folge der Eindeutigkeit der Elementarteiler eines Moduls über einem euklidischen Ring.

Zu "(i)⇒(ii)". Wir zeigen, dass κ bereits ein Isomorphismus der durch φ und ψ definierten $\mathbb{K}[T]$-Moduln ist. Als lineare Abbildung ist κ mit der Addition dieser $\mathbb{K}[T]$-Moduln verträglich. Weiter gilt

$$\begin{aligned}
\kappa\left(\left(\sum a_\nu T^\nu\right)\cdot v\right) &= \kappa\left(\sum a_\nu \varphi^\nu(v)\right)\\
&= \kappa\left(\sum a_\nu (\kappa^{-1}\circ\psi\circ\kappa)^\nu(v)\right)\\
&= \kappa\left(\sum a_\nu (\kappa^{-1}\circ\psi^\nu\circ\kappa)(v)\right)\\
&= \sum a_\nu \psi^\nu(\kappa(v))\\
&= \left(\sum a_\nu T^\nu\right)\cdot\kappa(v).
\end{aligned}$$

Zu "(ii)⇒(i)". Es sei $\kappa\colon V \to V$ eine Isomorphismus von dem durch φ definierten $\mathbb{K}[T]$-Modul in den durch ψ definierten $\mathbb{K}[T]$-Modul. Dann gilt für jedes $v \in V$:

$$\kappa(\varphi(v)) \;=\; \kappa(T\cdot v) \;=\; T\cdot\kappa(v) \;=\; \psi(\kappa(v)).$$

Damit erhalten wir $\kappa\circ\varphi = \psi\circ\kappa$ und somit, wie gewünscht, die Beziehung $\psi = \kappa\circ\varphi\circ\kappa^{-1}$. □

Satz 5.2.4. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus mit Elementarteilern $q_1, \ldots, q_r \in \mathbb{K}[T]$. Dann gibt es eine direkte Zerlegung*

$$V \;=\; V_1 \oplus \ldots \oplus V_r$$

in Untervektorräume $V_i \leq_{\mathbb{K}} V$ mit $\dim(V_i) = \deg(q_i)$, sodass $\varphi(V_i) \subseteq V$ gilt und die Einschränkungen $\varphi_i := \varphi_{|V_i} \colon V_i \to V_i$ folgende Eigenschaften besitzen:

(i) *Jedes V_i ist φ_i-zyklisch,*
(ii) *q_i ist das Minimalpolynom von $\varphi_i \colon V_i \to V_i$,*
(iii) *q_r ist das Minimalpolynom von $\varphi \colon V \to V$.*

Beweis. Nach Folgerung 5.1.4 ist der durch $\varphi \colon V \to V$ definierte $\mathbb{K}[T]$-Modul V ein Torsionsmodul. Der Hauptsatz 4.2.1 liefert daher einen Isomorphismus von $\mathbb{K}[T]$-Moduln

$$\Phi \colon \bigoplus_{i=1}^{r} \mathbb{K}[T]/\langle q_i \rangle \ \to \ V,$$

wobei $q_1, \ldots, q_r \in \mathbb{K}[T]$ die Elementarteiler des $\mathbb{K}[T]$-Moduls V sind. Wir betrachten den i-ten Faktor $V_i = \Phi(\mathbb{K}[T]/\langle q_i \rangle)$. Dann gilt $V = V_1 \oplus \ldots \oplus V_r$ und jedes V_i ist φ-invariant wegen

$$\varphi(V_i) \ = \ T \cdot V_i \ = \ \Phi(T \cdot (\mathbb{K}[T]/\langle q_i \rangle)) \ \subseteq \ \Phi(\mathbb{K}[T]/\langle q_i \rangle) \ = \ V_i.$$

Jeder Faktor V_i ist dabei φ_i-zyklisch und q_i ist das Minimalpolynom von φ_i, siehe Satz 5.1.11; insbesondere folgt $\dim(V_i) = \deg(q_i)$.

Wir zeigen nun, dass q_r das Minimalpolynom φ ist. Zunächst weisen wir $q_\varphi | q_r$ nach. Für jedes $v \in V$ betrachten wir die Zerlegung $v = v_1 + \ldots + v_r$ mit $v_i \in V_i$. Weiter schreiben wir $p_i q_i = q_r$ mit $p_i \in \mathbb{K}[T]$, was wegen $q_i | q_{i+1}$ möglich ist. Es folgt

$$q_r \cdot v \ = \ q_r \cdot (v_1 + \ldots + v_r) \ = \ q_r \cdot v_1 + \ldots + q_r \cdot v_r \ = \ p_1 q_1 \cdot v_1 + \ldots + p_r q_r \cdot v_r \ = \ 0_V.$$

Also liegt das Polynom q_r im Annullatorideal des $\mathbb{K}[T]$-Moduls V und ist somit ein Vielfaches des Minimalpolynoms q_φ. Umgekehrt annuliert q_φ den Untervektorraum V_r und ist somit ein Vielfaches von dessen Minimalpolynom q_r. Es folgt $q_\varphi = q_r$. □

Definition 5.2.5. Es seien $\mathbb{K}$ ein Körper und $q = T^k + a_{k-1}T^{k-1} + \ldots + a_1 T + a_0$ ein Polynom über $\mathbb{K}$. Die zu q gehörige *Begleitmatrix* ist

$$B(q) \quad := \quad \begin{pmatrix} 0 & & & & & -a_0 \\ 1 & 0 & & & & -a_1 \\ & 1 & \cdot & & & -a_2 \\ & & \cdot & \cdot & & \cdot \\ & & & \cdot & \cdot & \cdot \\ & & & & 0 & \cdot \\ & & & & 1 & -a_{k-2} \\ & & & & & -a_{k-1} \end{pmatrix} \quad \in \quad \operatorname{Mat}(k,k;\mathbb{K}).$$

Beispiel 5.2.6. Für das Polynom $q = T^2 + 1 \in \mathbb{Q}[T]$ erhalten wir die Begleitmatrix

$$B(q) \ = \ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Satz 5.2.7. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi \colon V \to V$ ein Endomorphismus mit den Elementarteilern $q_1, \ldots, q_r \in \mathbb{K}[T]$. Dann besitzt V eine Basis $\mathcal{B}$ mit*

$$M_{\mathcal{B}}^{\mathcal{B}}(\varphi) \ = \ \begin{pmatrix} B(q_1) & & 0 \\ & \ddots & \\ 0 & & B(q_r) \end{pmatrix}$$

Beweis. Wir betrachten zunächst den Fall eines φ-zyklischen $\mathbb{K}$-Vektorraumes V. Das Minimalpolynom von φ sei gegeben als

$$q \;=\; T^k + a_{k-1}T^{k-1} + \ldots + a_1 T + a_0.$$

Wählt man weiter eine Basis der Form $\mathcal{B} = (v, \varphi(v), \varphi^2(v), \ldots, \varphi^{k-1}(v))$ für V, so ergibt sich für das Bild des letzten Basisvektors

$$\begin{aligned}\varphi(\varphi^{k-1}(v)) &= T^k \cdot v \\ &= \big(q_\varphi - a_{k-1}T^{k-1} - \ldots - a_1 T - a_0\big) \cdot v \\ &= -a_{k-1} \cdot \varphi^{k-1}(v) - \ldots - a_1 \cdot \varphi(v) - a_0 \cdot v.\end{aligned}$$

Nach Definition der darstellenden Matrix von φ und der Begleitmatrix zu q_φ hat man daher

$$M_{\mathcal{B}}^{\mathcal{B}}(\varphi) \;=\; B(q_\varphi)$$

Um den Satz zu beweisen wählen wir nun eine direkte Zerlegung wie in Satz 5.2.4. Dann erhält man die Aussage durch Anwenden der Vorüberlegung auf die Einschränkungen $\varphi_i \colon V_i \to V_i$. □

Erinnerung 5.2.8. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum der Dimension $n \geq 1$. Das *charakteristische Polynom* eines Endomorphismus $\varphi \colon V \to V$ ist

$$p_\varphi \;:=\; \det(T \cdot E_n - M_{\mathcal{B}}^{\mathcal{B}}(\varphi)) \;\in\; \mathbb{K}[T],$$

wobei $\mathcal{B}$ eine beliebige Basis von V ist; dabei garantieren die Transformationsformel und der Determinantenmultiplikationssatz die Unabhängigkeit von der Basiswahl.

Satz 5.2.9 (Cayley-Hamilton)**.** *Es seien $\mathbb{K}$ ein Körper, ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi \colon V \to V$ ein Endomorphismus mit den Elementarteilern $q_1, \ldots, q_r \in \mathbb{K}[T]$. Dann ist das charakteristische Polynom von φ gegeben durch*

$$p_\varphi \;=\; q_1 \cdots q_r.$$

Insbesondere teilt das Minimalpolynom $q_\varphi = q_r$ das charakteristische Polynom p_φ, die Polynome q_φ und p_φ besitzen dieselben Primteiler, und es gilt $\deg(p_\varphi) = \deg(q_1) + \ldots + \deg(q_r)$.

Beweis. Es sei $\mathcal{B}$ eine Basis für V wie in Satz 5.2.7. Dann besitzt die zugehörige darstellende Matrix $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ Blockdiagonalgestalt, mit Blöcken $B(q_i)$, und es gilt

$$p_\varphi \;=\; \det(T \cdot E_n - M_{\mathcal{B}}^{\mathcal{B}}(\varphi)) \;=\; \det(T \cdot E_{n_1} - B(q_1)) \cdots \det(T \cdot E_{n_r} - B(q_r))$$

mit $n_i := \deg(q_i) = \dim(V_i)$. Wir bestimmen nun die Determinante der Matrix $T \cdot E_{n_i} - B(q_i)$. Dazu sei q_i gegeben als

$$q_i \;=\; T^k + a_{k-1}T^{k-1} + \ldots + a_1 T + a_0,$$

wobei wir $k := n_i$ setzen. Dann haben wir

$$T \cdot E_{n_i} - B(q_i) \;=\; \begin{pmatrix} T & & & & & & a_0 \\ -1 & T & & & & & a_1 \\ & -1 & \cdot & & & & a_2 \\ & & \cdot & \cdot & & & \cdot \\ & & & \cdot & \cdot & & \cdot \\ & & & & \cdot & T & \cdot \\ & & & & & -1 & T \quad a_{k-2} \\ & & & & & & -1 \quad T + a_{k-1} \end{pmatrix}$$

Die Determinante dieser Matrix berechnet man durch Entwickeln nach der letzten Spalte und erhält

$$\begin{aligned}\det(T \cdot E_{n_i} - B(q_i)) &= (-1)^{k+1}(-1)^{k-1}a_0 \ + \ (-1)^{k+2}(-1)^{k-2}a_1 T \\ &\quad + \ \ldots \ + \\ &\quad (-1)^{2k-1}(-1)a_{k-2}T^{k-2} \ + \ (T + a_{k-1})T^{k-1} \\ &= T^k + a_{k-1}T^{k-1} + \ldots + a_1 T + a_0.\end{aligned}$$

Das bedeutet $\det(T \cdot E_{n_i} - B(q_i)) = q_i$. Folglich ist das charakteristische Polynom von φ gegeben durch $p_\varphi = q_1 \cdots q_r$. □

Definition 5.2.10. Es seien $\mathbb{K}$ ein Körper und $A \in \mathrm{Mat}(n, n; \mathbb{K})$ eine Matrix. Die *Elementarteiler* von A sind die Elementarteiler des Endomorphismus $\mu_A \colon \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto A \cdot v$.

Satz 5.2.11 (Rationale Normalform)**.** *Es sei $\mathbb{K}$ ein Körper.*

(i) *Besitzt $A \in \mathrm{Mat}(n, n; \mathbb{K})$ die Elementarteiler $q_1, \ldots, q_r \in \mathbb{K}[T]$, so gibt es eine Matrix $S \in \mathrm{GL}(n, \mathbb{K})$ mit*

$$S \cdot A \cdot S^{-1} \ = \ \begin{pmatrix} B(q_1) & & 0 \\ & \ddots & \\ 0 & & B(q_r) \end{pmatrix}$$

(ii) *Für je zwei Matrizen $A, B \in \mathrm{Mat}(n, n; \mathbb{K})$ sind folgende Aussagen äquivalent:*
- *Es gilt $B = S \cdot A \cdot S^{-1}$ mit einer Matrix $S \in \mathrm{GL}(n, \mathbb{K})$.*
- *Die Matrizen A und B besitzen dieselben Elementarteiler.*

Beweis. Zu (i). Wir betrachten $\mu_A \colon \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto A \cdot v$. Satz 5.2.7 liefert eine Basis $\mathcal{B}$ für $\mathbb{K}^n$, sodass $M_{\mathcal{B}}^{\mathcal{B}}(\mu_A)$ die gewünschte Gestalt hat. Nach der Transformationsformel gilt $M_{\mathcal{B}}^{\mathcal{B}}(\mu_A) = S \cdot A \cdot S^{-1}$ mit einem $S \in \mathrm{GL}(n, \mathbb{K})$.

Zu (ii). Wir betrachten die Endomorphismen $\varphi := \mu_A$ und $\psi := \mu_B$ von $\mathbb{K}^n$. Nach Satz 5.2.3 besitzen φ und ψ genau dann dieselben Elementarteiler, wenn

$$\psi \ = \ \kappa \circ \varphi \circ \kappa^{-1}.$$

mit einem Isomorphismus $\kappa \colon \mathbb{K}^n \to \mathbb{K}^n$ gilt. Letztere Aussage ist äquivalent zu $B = S \cdot A \cdot S^{-1}$ mit einem $S \in \mathrm{GL}(n, \mathbb{K})$. □

Aufgaben zu Abschnitt 5.2.

Aufgabe 5.2.12. Bestimme die Elementarteiler und das Minimalpolynom für den Endomorphismus $\varphi\colon \mathbb{R}^3 \to \mathbb{R}^3$, $v \mapsto A \cdot v$ in den Fällen

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \qquad A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 2 & -1 \\ -1 & 0 & 3 \end{pmatrix}.$$

Begründe die Ergebnisse jeweils. *Hinweis:* Betrachte das charakteristische Polynom und verwende den Satz von Cayley-Hamilton.

Aufgabe 5.2.13. Bestimme Elementarteiler, Minimalpolynom und rationale Normalform der Matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 11 & 7 & 0 & -3 \end{pmatrix} \in \mathrm{Mat}(4,4;\mathbb{Q}).$$

Aufgabe 5.2.14. Es sei $\mathbb{K} := \mathbb{Z}/2\mathbb{Z}$ der Körper mit zwei Elementen. Betrachte die folgende Äquivalenzrelation auf $\mathrm{Mat}(2,2;\mathbb{K})$:

$$B \sim A \quad :\Longleftrightarrow \quad B = S \cdot A \cdot S^{-1} \text{ mit einem } S \in \mathrm{GL}(2,\mathbb{K})$$

Wieviele Äquivalenzklassen gibt es? *Hinweis:* Wieviel verschiedene Matrizen in rationaler Normalform besitzt $\mathrm{Mat}(2,2;\mathbb{K})$?

5.3. **Jordansche Normalform.**

Bemerkung 5.3.1. Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. In Abschnitt 5.2 hatten wir die Elementarteiler des zugehörigen $\mathbb{K}[T]$-Moduls verwendet, um φ zu untersuchen. Hier wollen wir die primären Elementarteiler zur Hilfe nehmen.

Zur Erinnerung: Sind R ein euklidischer Ring, $P \subset R$ ein Primsystem und M ein endlich erzeugter Torsionsmodul über R, so gibt es eine Zerlegung

$$M \;\cong\; \bigoplus_{p\in P} M_p,$$

mit den p-Torsionsmoduln $M_p \leq M$; nur endlich viele M_p sind nichttrivial, und jedes nichttriviale M_p besitzt eine Darstellung

$$M_p \;\cong\; \bigoplus_{i=1}^{d(p)} R/\langle p^{\nu_{p,i}}\rangle$$

mit den primären Elementarteilern $p^{\nu_{p,i}}$ des R-Moduls M; diese sind durch den Isomorphietyp von M und $1 \leq \nu_{p,1} \leq \ldots \leq \nu_{p,d(p)}$ eindeutig bestimmt.

Definition 5.3.2. Es seien $\mathbb{K}$ ein Körper und V ein endlichdimensionaler $\mathbb{K}$-Vektorraum. Die *primären Elementarteiler* eines Endomorphismus $\varphi\colon V \to V$ sind die normierten primären Elementarteiler des durch φ definierten $\mathbb{K}[T]$-Moduls V.

Satz 5.3.3. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus mit den primären Elementarteilern $p_i^{\nu_{ij}}$, wobei $1 \leq i \leq r$ und $1 \leq \nu_{i1} \leq \ldots \leq \nu_{id_i}$. Dann besitzt V eine direkte Zerlegung*

$$V \;=\; V_1 \oplus \ldots \oplus V_r, \quad \text{wobei } V_i \;=\; V_{i1} \oplus \ldots \oplus V_{id_i},$$

in Untervektorräume $V_{ij} \leq_{\mathbb{K}} V_i \leq_{\mathbb{K}} V$ mit $\varphi(V_{ij}) \subseteq V_{ij}$ und $\dim(V_{ij}) = \deg(p_i^{\nu_{ij}})$, sodass für die Einschränkungen $\varphi_{ij} := \varphi_{|V_{ij}}$ und $\varphi_i := \varphi_{|V_i}$ gilt:

(i) *Jedes V_{ij} ist φ_{ij}-zyklisch.*
(ii) *$p_i^{\nu_{ij}}$ ist das Minimalpolynom von φ_{ij}.*
(iii) *$p_i^{\nu_{id_i}}$ ist das Minimalpolynom von φ_i.*
(iv) *Man hat $V_i = \mathrm{Kern}(p_i^{\nu_{id_i}}(\varphi))$.*
(v) *$p_1^{\nu_{1d_1}} \cdots p_r^{\nu_{rd_r}}$ ist das Minimalpolynom von φ.*

Beweis. Nach Folgerung 5.1.4 ist der durch $\varphi\colon V \to V$ definierte $\mathbb{K}[T]$-Modul V ein Torsionsmodul. Satz 4.2.4 liefert daher einen Isomorphismus von $\mathbb{K}[T]$-Moduln

$$\Phi\colon \bigoplus_{i=1}^{r} \left(\bigoplus_{j=1}^{d_i} \mathbb{K}[T]/\langle p_i^{\nu_{ij}}\rangle \right) \quad\to\quad V,$$

wobei $p_i^{\nu_{ij}}$ die primären Elementarteiler des des $\mathbb{K}[T]$-Moduls V sind. Wir definieren Untervektorräume $V_{ij} \leq_{\mathbb{K}} V_i \leq_{\mathbb{K}} V$ durch

$$V_{ij} \;:=\; \Phi\left(\mathbb{K}[T]/\langle p_i^{\nu_{ij}}\rangle\right), \qquad V_i \;:=\; \Phi\left(\bigoplus_{j=1}^{d_i} \mathbb{K}[T]/\langle p_i^{\nu_{ij}}\rangle \right).$$

Dann gilt $V = V_1 \oplus \ldots \oplus V_r$ und $V_i = V_{i1} \oplus \ldots \oplus V_{id_i}$. Alle V_{ij} sind φ-invariant, denn wir haben

$$\varphi(V_{ij}) \;=\; T \cdot V_{ij} \;=\; \Phi(T \cdot (\mathbb{K}[T]/\langle p_i^{\nu_{ij}}\rangle)) \;\subseteq\; \Phi(\mathbb{K}[T]/\langle p_i^{\nu_{ij}}\rangle) \;=\; V_{ij}.$$

Nach Satz 5.1.11 ist jedes V_{ij} ein φ_{ij}-zyklischer Vektorraum, $p_i^{\nu_{ij}}$ ist das Minimalpolynom von φ_{ij}, und es gilt $\dim(V_{ij}) = \deg(p_i^{\nu_{ij}})$.

Zu (iii). Offensichtlich annulliert $q_i := p_i^{\nu_{id_i}}$ ganz V_i. Also gilt $q_i \in \mathfrak{a}_{V_i} = \langle q_{\varphi_i} \rangle$. Das impliziert $q_{\varphi_i} | q_i$. Umgekehrt gilt $q_{\varphi_i} \in \mathfrak{a}_{V_{id_i}} = \langle q_i \rangle$. Also gilt $q_i | q_{\varphi_i}$ und wir erhalten $q_i = q_{\varphi_i}$.

Aussage (iv) ergibt sich direkt aus der Tatsache, dass V_i genau der p_i-Torsionsmodul des $\mathbb{K}[T]$-Moduls V ist: Es gilt

$$\begin{aligned} V_i &= \{v \in V;\ p_i^n \cdot v = 0_V \text{ für ein } n \geq 0\} \\ &= \left\{v \in V;\ p_i^{\nu_{id_i}} \cdot v = 0_V\right\} \\ &= \operatorname{Kern}(p_i^{\nu_{id_i}}(\varphi)). \end{aligned}$$

Für (v) vermerken wir zunächst, dass $q := p_1^{\nu_{1d_1}} \cdots p_r^{\nu_{rd_r}}$ jedes $v \in V$ annulliert. Somit gilt $q \in \mathfrak{a}_V = \langle q_\varphi \rangle$, d.h., q_φ teilt q. Weiter annulliert q_φ jedes V_i. Somit ist jedes $p_i^{\nu_{id_i}}$ ein Teiler von V. Da die Primelemente p_i paarweise nichtassoziiert sind, erhalten wir, dass q ein Teiler von q_φ ist. Es folgt $q = q_\varphi$. □

Satz 5.3.4. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus mit den primären Elementarteilern $p_i^{\nu_{ij}}$, wobei $1 \leq i \leq r$ und $1 \leq \nu_{i1} \leq \ldots \leq \nu_{id_i}$. Dann besitzt V eine Basis $\mathcal{B}$ mit*

$$M_{\mathcal{B}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} B_1 & & 0 \\ & \ddots & \\ 0 & & B_r \end{pmatrix}, \qquad B_i = \begin{pmatrix} B(p_i^{\nu_{i1}}) & & 0 \\ & \ddots & \\ 0 & & B(p_i^{\nu_{id_i}}) \end{pmatrix}$$

Beweis. Wir zerlegen V gemäß Satz 5.3.3 in φ-invariante Untervektorräume V_{ij}. Nach Satz 5.2.7 besitzt jedes V_{ij} eine Basis $\mathcal{B}_{ij}$, bezüglich derer $\varphi|_{V_{ij}}$ durch die Begleitmatrix $B(p_i^{\nu_{ij}})$ dargestellt wird. Zusammensetzen der $\mathcal{B}_{ij}$ ergibt dann die gewünschte Basis. □

Folgerung 5.3.5. *Es sei $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ eine Endomorphismus. Dann sind folgende Aussagen äquivalent:*

(i) *Der Endomorphismus $\varphi\colon V \to V$ ist diagonalisierbar, d.h., V besitzt eine Basis aus Eigenvektoren für φ*
(ii) *Das Minimalpolynom $q_\varphi \in \mathbb{K}[T]$ zerfällt in paarweise verschiedene Linearfaktoren, d.h., $q_\varphi = (T - \lambda_1) \cdots (T - \lambda_k)$ mit $\lambda_i \neq \lambda_j$ für $i \neq j$.*

Beweis. Die Implikation "(i)⇒(ii)" erhält man durch eine explizite Berechnung des Minimalpolynoms. Für "(ii)⇒(i)" beachte man, dass φ nur primäre Elementarteiler der Form $T - \lambda_i$ besitzen kann. Somit sind alle Begleitmatrizen in Satz 5.3.4 von der Gestalt $B(p_i^{\nu_{ij}}) = (\lambda_i)$. Das bedeutet, dass φ diagonalisierbar ist. □

Folgerung 5.3.6. *Es seien $\mathbb{K}$ ein Körper und $A \in \operatorname{Mat}(n, n; \mathbb{K})$. Dann sind folgende Aussagen äquivalent:*

(i) *Die Matrix A ist diagonalisierbar, d.h., es gibt eine Matrix $S \in \operatorname{GL}(n, \mathbb{K})$, sodass $S \cdot A \cdot S^{-1}$ Diagonalgestalt besitzt.*
(ii) *Das Minimalpolynom $q_A \in \mathbb{K}[T]$ zerfällt in paarweise verschiedene Linearfaktoren, d.h., $q_A = (T - \lambda_1) \cdots (T - \lambda_k)$ mit $\lambda_i \neq \lambda_j$ für $i \neq j$.*

Definition 5.3.7. Es seien $\mathbb{K}$ ein Körper, $n \in \mathbb{Z}_{\geq 1}$ und $\lambda \in \mathbb{K}$. Das zugehörige *Jordankästchen* ist die Matrix

$$J(n,\lambda) \quad := \quad \begin{pmatrix} \lambda & & & & & & 0 \\ 1 & \lambda & & & & & \\ & 1 & \cdot & & & & \\ & & \cdot & \cdot & & & \\ & & & \cdot & \cdot & & \\ & & & & \cdot & \cdot & \\ & & & & & 1 & \lambda \\ 0 & & & & & 1 & \lambda \end{pmatrix} \in \mathrm{Mat}(n,n;\mathbb{K}).$$

Satz 5.3.8. *Es seien $\mathbb{K}$ ein Körper und V ein endlichdimensionaler φ-zyklischer $\mathbb{K}$-Vektorraum für einen Endomorphismus $\varphi\colon V \to V$ mit Minimalpolynom*

$$q_\varphi \;=\; q^n \;\in\; \mathbb{K}[T], \quad \text{wobei } q := (T-\lambda).$$

Ist $v \in V$ mit $q^{n-1} \cdot v = (\varphi - \lambda \cdot \mathrm{id}_V)^{n-1}(v) \neq 0_V$, so ist $\mathcal{B} := (v, q\cdot v, \ldots, q^{n-1}\cdot v)$ eine Basis für V und die zugehörige darstellende Matrix ist

$$M_{\mathcal{B}}^{\mathcal{B}}(\varphi) \quad = \quad J(n,\lambda).$$

Beweis. Nach Satz 5.1.11 gilt $\dim(V) = \deg(q_\varphi) = n$. Um zu sehen, dass $\mathcal{B}$ eine Basis für V ist, genügt es daher die lineare Unabhängigkeit nachzuweisen. Dazu sei

$$a_0 \cdot v + a_1 \cdot q \cdot v + \ldots + a_{n-1} \cdot q^{n-1} \cdot v \quad = \quad 0_V.$$

Anwenden von q^{k-1} auf diese Gleichung ergibt $a_0 \cdot q^{n-1} \cdot v = 0_V$. Das impliziert $a_0 = 0_{\mathbb{K}}$. Durch Anwenden von q^{n-2} erhält man dann $a_1 \cdot q^{n-1} \cdot v = 0_V$, was $a_2 = 0_{\mathbb{K}}$ liefert. So verfährt man weiter und erhält $a_i = 0_{\mathbb{K}}$ für alle $1 \leq i \leq n-1$. Das beweist die lineare Unabhängigkeit von $\mathcal{B}$.

Um die darstellende Matrix $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ zu erhalten, müssen wir die Bilder der Basisvektoren bestimmen. Mit $q^{i+1} \cdot v = (\varphi - \lambda \cdot \mathrm{id}_V) \cdot (q^i \cdot v)$ ergibt sich

$$\varphi(q^i \cdot v) \quad = \quad \lambda \cdot (q^i \cdot v) + q^{i+1} \cdot v$$

für $0 \leq i \leq n-2$. Das Bild von $q^{n-1} \cdot v$ ist ein Eigenvektor zum Eigenwert λ von φ, denn es gilt

$$(\varphi - \lambda \cdot \mathrm{id}_V)(q^{n-1} \cdot v) \;=\; q^n \cdot v \;=\; 0_V.$$

Somit sind die Bilder der Basisvektoren $v, \ldots, q^{n-1} \cdot v$ bestimmt und wir erhalten die darstellende Matrix wie behauptet. □

Satz 5.3.9. *Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\varphi\colon V \to V$ ein Endomorphismus. Hat man eine Zerlegung*

$$q_\varphi \quad = \quad (T-\lambda_1)^{m_1} \cdots (T-\lambda_r)^{m_r}$$

des Minimalpolynoms von $\varphi\colon V \to V$ in Linearfaktoren mit $\lambda_i \neq \lambda_j$ für $i \neq j$, so besitzt V eine Basis $\mathcal{B}$ mit

$$M_{\mathcal{B}}^{\mathcal{B}}(\varphi) \quad = \quad \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_r \end{pmatrix}, \qquad J_i \;=\; \begin{pmatrix} J(k_{i1},\lambda_i) & & 0 \\ & \ddots & \\ 0 & & J(k_{id_i},\lambda_i) \end{pmatrix},$$

wobei $1 \leq k_{i1} \leq \ldots \leq k_{id_i} = m_i$ gilt und die Polynome $(T-\lambda_i)^{k_{ij}}$ die primären Elementarteiler des Endomorphismus $\varphi\colon V \to V$ sind.

Beweis. Da q_φ in Linearfaktoren $T - \lambda_i$ zerfällt, sind die primären Elementarteiler von φ alle von der Gestalt $(T-\lambda_i)^{k_{ij}}$. Wir zerlegen V in Untervektorräume $V_{ij} \leq_{\mathbb{K}} V_i \leq_{\mathbb{K}} V$ wie in Satz 5.3.3 und wenden dann Satz 5.3.8 auf jedes V_{ij} an. Damit ergibt sich die Behauptung. □

Definition 5.3.10. Es seien $\mathbb{K}$ ein Körper und $A \in \mathrm{Mat}(n,n;\mathbb{K})$. Die *primären Elementarteiler* von A sind die primären Elementarteiler des Endomorphismus $\mu_A\colon \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto A \cdot v$.

Satz 5.3.11 (Jordansche Normalform)**.** *Es sei $\mathbb{K}$ ein Körper.*

(i) *Es sei $A \in \mathrm{Mat}(n,n;\mathbb{K})$ eine Matrix, deren Minimalpolynom in Linearfaktoren zerfällt. Dann gibt es eine Matrix $S \in \mathrm{GL}(n,\mathbb{K})$ mit*

$$S \cdot A \cdot S^{-1} \;=\; \begin{pmatrix} J_1 & & 0 \\ & \ddots & \\ 0 & & J_r \end{pmatrix},$$

$$J_i \;:=\; \begin{pmatrix} J(k_{i1},\lambda_i) & & 0 \\ & \ddots & \\ 0 & & J(k_{id_i},\lambda_i) \end{pmatrix}.$$

Dabei sind $(T-\lambda_i)^{k_{ij}}$, wobei $\lambda_i \in \mathbb{K}$ und $1 \le k_{i1} \le \ldots \le k_{id_i}$, die primären Elementarteiler von A.

(ii) *Für je zwei Matrizen $A, B \in \mathrm{Mat}(n,n;\mathbb{K})$ sind folgende Aussagen äquivalent:*
- *Es gilt $B = S \cdot A \cdot S^{-1}$ mit einer Matrix $S \in \mathrm{GL}(n,\mathbb{K})$.*
- *Die Matrizen A und B besitzen dieselben primären Elementarteiler.*

Beweis. Zu (i). Wir betrachten den Endomorphismus $\varphi\colon \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto A \cdot v$. Satz 5.3.9 liefert eine Basis $\mathcal{B}$ für $\mathbb{K}^n$, sodass $M^{\mathcal{B}}_{\mathcal{B}}(\varphi)$ die gewünschte Gestalt hat. Nach der Transformationsformel gilt $M^{\mathcal{B}}_{\mathcal{B}}(\varphi) = S \cdot A \cdot S^{-1}$ mit einem $S \in \mathrm{GL}(n,\mathbb{K})$.

Zu (ii). Die Matrizen A und B besitzen genau dann dieselben primären Elementarteiler, wenn sie dieselben Elementarteiler besitzen. Letzteres ist nach Satz 5.2.11 äquivalent zu $B = S \cdot A \cdot S^{-1}$ mit einer Matrix $S \in \mathrm{GL}(n,\mathbb{K})$. □

Bemerkung 5.3.12. Nach dem Fundamentalsatz der Algebra zerfällt für jede Matrix $A \in \mathrm{Mat}(n,n;\mathbb{C})$ das Minimalpolynom $q_A \in \mathbb{C}[T]$ in Linearfaktoren. Insbesondere besitzt A eine Jordansche Normalform.

Definition 5.3.13. Es sei $\mathbb{K}$ ein Körper. Eine Matrix $N \in \mathrm{Mat}(n,n;\mathbb{K})$ nennt man *nilpotent*, falls es ein $k \in \mathbb{Z}_{\ge 0}$ gibt, sodass N^k die Nullmatrix ist.

Beispiel 5.3.14. Es sei $\mathbb{K}$ ein Körper. Ist $N \in \mathrm{Mat}(n,n;\mathbb{K})$ mit $n_{ij} = 0_{\mathbb{K}}$ für alle $j \ge i$, so ist N nilpotent.

Folgerung 5.3.15 (Jordan-Zerlegung)**.** *Jede Matrix $A \in \mathrm{Mat}(n,n;\mathbb{C})$ besitzt eine Zerlegung $A = C + N$ mit einer diagonalisierbaren Matrix $C \in \mathrm{Mat}(n,n;\mathbb{C})$ und einer nilpotenten Matrix $N \in \mathrm{Mat}(n,n;\mathbb{C})$.*

Beweis. Ist $A \in \mathrm{Mat}(n,n;\mathbb{C})$ in Jordanscher Normalform, so ist die Aussage offensichtlich. Für beliebiges $A \in \mathrm{Mat}(n,n;\mathbb{C})$ liefern Bemerkung 5.3.12 und Satz 5.3.11 ein $S \in \mathrm{GL}(n,\mathbb{C})$, sodass $A' := S \cdot A \cdot S^{-1}$ Jordansche Normalform besitzt.

Ist $A' = C' + N'$ eine Zerlegung mit einer diagonalisierbaren Matrix C' und einer nilpotenten Matrix $N' \in \mathrm{Mat}(n,n;\mathbb{C})$, so ist

$$A \;=\; S^{-1} \cdot C' \cdot S + S^{-1} \cdot N' \cdot S$$

die gewünschte Zerlegung: Die Matrix $S^{-1} \cdot C' \cdot S$ ist offensichtlich diagonalisierbar und $S^{-1} \cdot N' \cdot S$ ist nilpotent, denn für jedes $k \in \mathbb{Z}_{\ge 0}$ gilt

$$(S^{-1} \cdot N' \cdot S)^k \;=\; S^{-1} \cdot N' \cdot S \;\cdots\; S^{-1} \cdot N' \cdot S \;=\; S^{-1} \cdot (N')^k \cdot S.$$

□

Aufgaben zu Abschnitt 5.3.

Aufgabe 5.3.16. Bestimme jeweils rationale und Jordansche Normalform der folgenden reellen (2×2)-Matrizen

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Aufgabe 5.3.17. Es sei $\mathbb{K}$ ein Körper. Betrachte die untenstehenden Matrizen $A, B \in \mathrm{Mat}(n, n; \mathbb{K})$ und zeige, dass es ein $S \in \mathrm{GL}(n, \mathbb{K})$ gibt mit $B = S \cdot A \cdot S^{-1}$.

$$A := \begin{pmatrix} \lambda & & & & & & & 0 \\ 1 & \lambda & & & & & & \\ & 1 & \ddots & & & & & \\ & & \ddots & \ddots & & & & \\ & & & \ddots & \ddots & & & \\ & & & & \ddots & \ddots & & \\ & & & & & 1 & \lambda & \\ 0 & & & & & & 1 & \lambda \end{pmatrix}, \qquad B := \begin{pmatrix} \lambda & 1 & & & & & & 0 \\ 0 & \lambda & 1 & & & & & \\ & & \ddots & \ddots & & & & \\ & & & \ddots & \ddots & & & \\ & & & & \ddots & \ddots & 1 & \\ & & & & & & \lambda & 1 \\ 0 & & & & & & & \lambda \end{pmatrix}$$

Aufgabe 5.3.18. Es sei $A \in \mathrm{Mat}(3, 3; \mathbb{R})$ eine Matrix, deren charakteristisches Polynom über $\mathbb{R}$ nicht in Linearfaktoren zerfällt. Zeige: Es gibt eine Matrix $S \in \mathrm{GL}(3, \mathbb{R})$ mit

$$S \cdot A \cdot S^{-1} = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & -c \\ 0 & 1 & -b \end{pmatrix}, \qquad \text{wobei } \lambda, b, c \in \mathbb{R},\ b^2 < 4c.$$

Aufgabe 5.3.19. Zeige: Ist $A \in \mathrm{Mat}(n, n; \mathbb{C})$ eine invertierbare Matrix, so gibt es ein Polynom $f \in \mathbb{C}[T]$ mit $\deg(f) \leq n$ und $f(A) = A^{-1}$.

Aufgabe 5.3.20. Bestimme alle Matrizen $A \in \mathrm{Mat}(5, 5; \mathbb{C})$ mit den beiden folgenden Eigenschaften:

- Es gilt $p_A = (T - 3)^5$,
- A besitzt Jordansche Normalform.

Bestimme von jeder dieser Matrizen die Elementarteiler und die primären Elementarteiler. Gibt es unter den obigen Matrizen Paare A, A', sodass $A' = S \cdot A \cdot S^{-1}$ mit einem $S \in \mathrm{GL}(5, \mathbb{C})$ gilt?

5.4. **Normalformenberechnung.**

Bemerkung 5.4.1. Will man die rationale bzw. die Jordansche Normalform einer gegebenen Matrix bestimmen, so benötigt man ihre Elementarteiler bzw. ihre primären Elementarteiler.

Bei kleinen Matrizen kommt man häufig mit dem Satz von Cayley-Hamilton zum Erfolg. Als Beispiel betrachten wir die Matrix

$$A \;=\; \begin{pmatrix} 3 & -1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in \mathrm{Mat}(3,3;\mathbb{C}).$$

Das charakteristische Polynom $p_A = \det(T \cdot E_3 - A)$ kann man hier leicht berechnen, etwa durch Entwicklen nach der letzten Zeile:

$$\begin{aligned} p_A &= (T-2) \cdot \det \begin{pmatrix} T-3 & 1 \\ -1 & T-1 \end{pmatrix} \\ &= (T-2)((T-3)(T-1)+1) \\ &= (T-2)(T^2-4T+4) \\ &= (T-2)^3. \end{aligned}$$

Da das Minimalpolynom q_A von A, d.h., der letzte Elementarteiler von A, dieselben Primteiler wie p_A besitzt, gibt es zunächst folgende Möglichkeiten:

$$q_A \;=\; T-2, \qquad q_A \;=\; (T-2)^2, \qquad q_A \;=\; (T-2)^3.$$

Die erste Möglichkeit entfällt, da A in diesem Fall Diagonalgestalt besitzen müsste. Wir müssen also prüfen, ob $(T-2)^2$ die Matrix A bereits annulliert. Es gilt

$$(A-2)^2 \;=\; \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \;=\; \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Also ist $(T-2)^2$ das Minimalpolynom. Da das Produkt über die Elementarteiler das charakteristische Polynom ergibt, muss A die Elementarteiler

$$q_1 \;=\; T-2, \qquad q_2 \;=\; q_A \;=\; (T-2)^2$$

besitzen. Durch Primfaktorzerlegung der Elementarteiler und sortieren der Primfaktoren erhält man die primären Elementarteiler; in unserem Falle sind das

$$p_{11} \;=\; T-2, \qquad p_{12} \;=\; (T-2)^2$$

Damit können wir die rationale Normalform und die Jordansche Normalform der Matrix A bereits hinschreiben:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & 4 \end{pmatrix}, \qquad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$

Bei größeren Matrizen A sind, selbst bei einfachem charakteristischem Polynom, schnell deutlich mehr Konstellationen für Elementarteiler und primäre Elementarteiler möglich. Eine explizite Bestimmung erfordert dann zusätzlichen Aufwand.

Satz 5.4.2. *Es seien $\mathbb{K}$ ein Körper und $A \in \mathrm{Mat}(n,n;\mathbb{K})$ eine Matrix. Die Elementarteiler $q_1,\ldots,q_r \in \mathbb{K}[T]$ von A sind bis auf Normierung die nicht konstanten Diagonaleinträge der Smith-Normalform von $T \cdot E_n - A \in \mathrm{Mat}(n,n;\mathbb{K}[T])$.*

Lemma 5.4.3. *Es sei $\mathbb{K}$ ein Körper. Wir betrachten eine Matrix $A \in \mathrm{Mat}(n,n;\mathbb{K})$ und die zu $\mu_A\colon \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto A \cdot v$, gehörige $\mathbb{K}[T]$-Modulstruktur auf $\mathbb{K}^n$. Dann ist*

$$\pi\colon \mathbb{K}[T]^n \ \to\ \mathbb{K}^n, \qquad (p_1,\ldots,p_n) \ \mapsto\ p_1(A)\cdot e_1 + \ldots + p_n(A)\cdot e_n.$$

ein surjektiver Homomorphismus von $\mathbb{K}[T]$-Moduln. Der Kern dieses Homomorphismus wird von den Spalten der Matrix $T \cdot E_n - A \in \mathrm{Mat}(n,n;\mathbb{K}[T])$ erzeugt:

$$\mathrm{Kern}(\pi) \ =\ \langle (T\cdot E_n - A)_{*1},\ldots,T\cdot E_n - A)_{*n}\rangle \ \leq_{\mathbb{K}} \mathbb{K}[T]^n.$$

Beweis. Nach Satz 3.2.7 (i) ist die oben definierte Abbildung π der (eindeutig bestimmte) $\mathbb{K}[T]$-Modulhomomorphismus, welcher $e_i \in \mathbb{K}[T]^n$ auf $e_i \in \mathbb{K}^n$ abbildet.

Wir zeigen nun, dass der von den Spalten $(T \cdot E_n - A)_{*j}$ erzeugte Untermodul $W \leq_{\mathbb{K}[T]} \mathbb{K}[T]^n$ mit dem Untermodul $\mathrm{Kern}(\pi) \leq_{\mathbb{K}[T]} \mathbb{K}[T]^n$ übereinstimmt. Die Inklusion $W \subseteq \mathrm{Kern}(\pi)$ ergibt sich aus

$$\pi((T\cdot E_n - A)_{*j}) \ =\ \pi(T\cdot e_j) - \pi\left(\sum_{i=1}^n a_{ij}\cdot e_j\right) \ =\ A\cdot e_j - \sum_{i=1}^n a_{ij}\cdot e_j \ =\ 0_{\mathbb{K}^n}.$$

Für die Inklusion $W \supseteq \mathrm{Kern}(\pi)$ zeigen wir zunächst, dass jedes $u \in \mathbb{K}[T]^n$ eine Darstellung $u = w + v$ mit $w \in W$ und $v \in \mathbb{K}^n$ besitzt. Mittels Induktion über ν zeigen wir, dass dies für alle $T^\nu \cdot e_i$ gilt. Der Fall $\nu = 0,1$ ist klar mit

$$T^0\cdot e_i \ =\ e_i \ \in\ \mathbb{K}^n, \qquad T^1\cdot e_i \ =\ (T\cdot E_n - A)_{*i} + A_{*i} \ \in\ W + \mathbb{K}^n.$$

Ist $\nu > 1$ gegeben, so schreiben wir $T^\nu \cdot e_i = T\cdot(T^{\nu-1}\cdot e_i)$. Nach Induktionsvoraussetzung haben wir $T^{\nu-1}\cdot e_i = w + v$ mit $w \in W$ und $v \in \mathbb{K}^n$. Es folgt

$$T^\nu\cdot e_i \ =\ T\cdot(w+v) \ =\ T\cdot w + \sum_{i=1}^n v_i \cdot T\cdot e_i \ \in\ W + \mathbb{K}^n.$$

Da man jedes $u \in \mathbb{K}[T]^n$ als Linearkombination mit konstanten Koeffizienten über den $T^\nu\cdot e_i$ darstellen kann, sehen wir dass jedes $u \in \mathbb{K}[T]^n$ eine Darstellung $u = w+v$ mit $w \in W$ und $v \in \mathbb{K}^n$ erlaubt.

Damit können wir $W \supseteq \mathrm{Kern}(\pi)$ nachweisen. Ist $u \in \mathrm{Kern}(\pi)$ gegeben, so schreiben wir $u = w + v$ mit $w \in W$ und $v \in \mathbb{K}^n$. Wir müssen also $v = 0_{\mathbb{K}^n}$ zeigen. Das ergibt sich durch Anwenden von π:

$$0_{\mathbb{K}^n} \ =\ \pi(u) \ =\ \pi(w+v) \ =\ \pi(w) + \pi(v) \ =\ \pi(v) \ =\ v.$$

□

Beweis von Satz 5.4.2. Wir betrachten den Homomorphismus $\pi\colon \mathbb{K}[T]^n \to \mathbb{K}^n$ aus Lemma 5.4.3. Der Homomorphiesatz 3.1.22 liefert uns dann einen Isomorphismus von $\mathbb{K}[T]$-Moduln

$$\mathbb{K}^n \ \cong\ \mathbb{K}[T]^n/\mathrm{Kern}(\pi).$$

Wie im Beweis von Satz 4.2.1 arbeiten wir mit einer an $\mathrm{Kern}(\pi)$ angepassten Basis für $\mathbb{K}[T]^n$. Lemma 5.4.3 liefert, dass $\mathrm{Kern}(\pi)$ von den Spalten von $B := T\cdot E_n - A$ erzeugt wird.

Es seien $S, S' \in \mathrm{Mat}(n,n;\mathbb{K}[T])$ invertierbar, sodass $D := S \cdot B \cdot S'$ die Smith-Normalform für B in $\mathrm{Mat}(n,n;\mathbb{K}[T])$ ist; wegen $\det(D) = \det(B) \neq 0_{\mathbb{K}[T]}$ sind dabei alle Diagonaleinträge d_{ii} von Null verschieden. Die Elemente $v_i := S^{-1} \cdot e_i$, $1 \leq i \leq n$, bilden dann eine Basis für $\mathbb{K}[T]^n$, und Lemma 4.1.9 (ii) garantiert, dass $(d_{11} \cdot v_1, \ldots, d_{nn} \cdot v_n)$ eine Basis für $\mathrm{Kern}(\pi)$ ist.

Sind $d_{ll}, \ldots, d_{nn}$ die nicht konstanten Polynome unter den d_{ii}, so erhält man einen Isomorphismus von $\mathbb{K}[T]$-Moduln

$$\mathbb{K}^n \;\cong\; \mathbb{K}[T]^n/\mathrm{Kern}(\pi) \;\cong\; \mathbb{K}[T]/\langle d_{ll}\rangle \oplus \ldots \oplus \mathbb{K}[T]/\langle d_{nn}\rangle.$$

Da sich die d_{ii} aufsteigend teilen, sehen wir, dass $d_{ll}, \ldots, d_{nn}$ die Elementarteiler des $\mathbb{K}[T]$-Moduls $\mathbb{K}^n$ und somit der Matrix A sind. □

Bemerkung 5.4.4. Satz 5.4.2 liefert uns ein konkretes Verfahren zur Bestimmung der Elementarteiler und primären Elementarteiler einer gegebenen Matrix $A \in \mathrm{Mat}(n,n;\mathbb{K})$ und somit zur Normalformenberechnung:

- Man überführe $T \cdot E_n - A \in \mathrm{Mat}(n,n;\mathbb{K}[T])$ durch elementare Zeilen- und Spaltenumformungen in eine Matrix D in Smith-Normalform.
- Die Elementarteiler von A erhält man durch Normieren der nichtkonstanten Diagonaleinträge d_{ii} und die rationale Normalform von A ist die Matrix mit den zugehörigen Begleitmatrizen $B(d_{ii})$ als Diagonalblöcken, siehe Satz 5.2.11.
- Die primären Elementarteiler $p_i^{\nu_{ij}}$ von A erhält man gemäß 4.2.10 mittels Primfaktorzerlegung der Elementarteiler $q_1, \ldots, q_r$ (wobei die $p_i^{\nu_{ij}}$ mit $\nu_{ij} = 0$ jeweils wegzulassen sind);

  $$q_1 \;= p_1^{\nu_{11}} \cdot \ldots \cdot p_r^{\nu_{r1}}, \quad \ldots, \quad q_r \;= p_1^{\nu_{1d_1}} \cdot \ldots \cdot p_r^{\nu_{rd_r}}.$$

  Zerfällt das Minimalpolynom q_A in Linearfaktoren, so sind die primären Elementarteiler von der Form $p_i^{\nu_{ij}} = (T - \lambda_i)^{\nu_{ij}}$, und die Jordansche Normalform von A ist die Matrix mit den zugehörigen Jordankästchen als Diagonalblöcken, siehe Satz 5.3.11.

Beispiel 5.4.5. Wir erproben das Verfahren aus Bemerkung 5.4.4 an der bereits in Bemerkung 5.4.1 diskutierten Matrix

$$A \;=\; \begin{pmatrix} 3 & -1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in \mathrm{Mat}(3,3;\mathbb{C}).$$

Zunächst benötigt man die Smith-Normalform von $T \cdot E_n - A$; man kann sie wie folgt durch elementare Zeilen- und Spaltenumformungen gewinnen:

$$\begin{pmatrix} T-3 & 1 & -1 \\ -1 & T-1 & -1 \\ 0 & 0 & T-2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(1,2)} \quad \begin{pmatrix} -1 & T-1 & -1 \\ T-3 & 1 & -1 \\ 0 & 0 & T-2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(T-3;1,2)} \quad \begin{pmatrix} -1 & T-1 & -1 \\ 0 & (T-3)(T-1)+1 & -T+2 \\ 0 & 0 & T-2 \end{pmatrix}$$

$$\xrightarrow{=} \quad \begin{pmatrix} -1 & T-1 & -1 \\ 0 & T^2-4T+4 & -T+2 \\ 0 & 0 & T-2 \end{pmatrix}$$

$$\xrightarrow{=} \quad \begin{pmatrix} -1 & T-1 & -1 \\ 0 & (T-2)^2 & -T+2 \\ 0 & 0 & T-2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{SpOp}(T-1;1,2)} \quad \begin{pmatrix} -1 & 0 & -1 \\ 0 & (T-2)^2 & -T+2 \\ 0 & 0 & T-2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{SpOp}(-1;1,3)} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & (T-2)^2 & -T+2 \\ 0 & 0 & T-2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(1;3,2)} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & (T-2)^2 & 0 \\ 0 & 0 & T-2 \end{pmatrix}$$

$$\xrightarrow{\mathrm{ZOp}(2,3)} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & T-2 \\ 0 & (T-2)^2 & 0 \end{pmatrix}$$

$$\xrightarrow{\mathrm{SpOp}(2,3)} \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & T-2 & 0 \\ 0 & 0 & (T-2)^2 \end{pmatrix}$$

Folglich besitzt A die Polynome $q_1 = T-2$ und $q_2 = (T-2)^2$ als Elementarteiler. Als primäre Elementarteiler ergeben sich $p_{11} = T-2$ und $p_{12} = (T-2)^2$. Rationale und Jordansche Normalform von A sind daher

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -4 \\ 0 & 1 & 4 \end{pmatrix}, \qquad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix}.$$

Bemerkung 5.4.6. Es seien $\mathbb{K}$ ein Körper und $A \in \mathrm{Mat}(n,n;\mathbb{K})$, deren Minimalpolynom q_A in Linearfaktoren zerfällt. Bisweilen benötigt man eine Matrix $S \in \mathrm{GL}(n,\mathbb{K})$, sodass $S \cdot A \cdot S^{-1}$ Jordansche Normalform besitzt. Dabei ist das folgende Vorgehen empfehlenswert:

- Man bestimme das Minimalpolynom q_A von A und zerlege es in Linearfaktoren:
$$q_A \quad = \quad (T-\lambda_1)^{m_1} \cdots (T-\lambda_r)^{m_r}.$$
- Bestimme die zu den Eigenwerten $\lambda_1, \ldots, \lambda_r$ der Matrix A gehörigen *Haupträume* V_i; diese sind mit $B_i := A - \lambda_i \cdot E_n$ gegeben durch
$$V_i \ := \ \mathrm{Kern}(B_i^{m_i}) \ \leq_{\mathbb{K}} \ \mathbb{K}^n.$$
- Bestimme für jedes V_i eine Basis $\mathcal{B}_i = (v_{i1}, \ldots, v_{in_i})$ bezüglich derer $\mu_A|_{V_i}$ durch eine Matrix in Jordanscher Normalform dargestellt wird.
- Die aus den Basen $\mathcal{B}_1, \ldots, \mathcal{B}_r$ zusammengesetzte Matrix definiert die gewünschte Transformationsmatrix S, es gilt
$$S \ = \ (v_{11}, \ldots, v_{1n_1}, \ldots, v_{r1}, \ldots, v_{rn_r})^{-1}.$$

Für die Bestimmung der Basen $\mathcal{B}_i$ der Haupträume V_i liefert Bemerkung 5.4.7 ein allgemeines Verfahren; gilt jedoch $\dim(V_i) = m_i$, so ist V_i bereits φ_i-zyklisch, und jedes $v \in V_i \setminus \mathrm{Kern}(B^{m_i-1})$ liefert eine Basis $\mathcal{B}_i = (v, B \cdot v, \ldots B^{m_i-1} \cdot v)$ mit den gewünschten Eigenschaften.

Bemerkung 5.4.7. Es seien $\mathbb{K}$ ein Körper, V ein endlichdimensionaler Vektorraum, und $\varphi\colon V \to V$ ein Endomorphismus mit Minimalpolynom

$$q_\varphi \;=\; q^m, \quad \text{mit } q \;=\; T - \lambda \;\in \mathbb{K}[T].$$

Dann sind die Elementarteiler von φ von der Form q^{k_j} mit aufsteigend angeordneten Exponenten k_j:

$$1 \;\leq\; k_1 = \ldots = k_{s_1} \;<\; \ldots \;<\; k_{s_{r-1}+1} = \ldots = k_{s_r} \;=\; m.$$

Das folgende schrittweise Vorgehen liefert eine Basis $\mathcal{B}$ für V, sodass $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ Jordansche Normalform besitzt. Wir setzen $U_j := \mathrm{Kern}(q^j)$ und $W^{r+1} := \{0_V\}$.

- Bestimme Vektoren $v_1^r, \ldots, v_{s_r}^r \in U_{k_{s_r}}$, sodass die zugehörigen Klassen $(\overline{v}_1^r, \ldots, \overline{v}_{s_r}^r)$ eine Basis bilden für

  $$U_{k_{s_r}} / (U_{k_{s_r}-1} + (W^{r+1} \cap U_{k_{s_r}})).$$

  Dann erhält man Basen $\mathcal{B}_j^r \;=\; (v_j^r, q(\varphi)(v_j^r), \ldots, q^{k_{s_r}-1}(\varphi)(v_j^r))$ für φ-zyklische Untervektorräume $W_j^r := \mathrm{Lin}(\mathcal{B}_j^r)$. Setze

  $$W^r \;:=\; W^{r+1} + W_1^r + \ldots + W_{s_r}^r.$$

- Bestimme Vektoren $v_1^{r-1}, \ldots, v_{s_{r-1}}^{r-1} \in U_{k_{s_{r-1}}}$, sodass die zugehörigen Klassen $(\overline{v}_1^{r-1}, \ldots, \overline{v}_{s_{r-1}}^{r-1})$ eine Basis bilden für

  $$U_{k_{s_{r-1}}} / (U_{k_{s_{r-1}}-1} + (W^r \cap U_{k_{s_{r-1}}}).$$

  Dann erhält man Basen $\mathcal{B}_j^{r-1} = (v_j^{r-1}, q(\varphi)(v_j^{r-1}), \ldots, q^{k_{s_{r-1}}-1}(\varphi)(v_j^{r-1}))$ für φ-zyklische Untervektorräume $W_j^{r-1} := \mathrm{Lin}(\mathcal{B}_j^{r-1})$. Setze

  $$W^{r-1} \;:=\; W^r + W_1^{r-1} + \ldots + W_{s_{r-1}}^{r-1}.$$

- usw., bis

- Bestimme Vektoren $v_1^1, \ldots, v_{s_1}^1 \in U_{k_{s_1}}$, sodass die zugehörigen Klassen $(\overline{v}_1^1, \ldots, \overline{v}_{s_1}^1)$ eine Basis bilden für

  $$U_{k_{s_1}} / (U_{k_{s_1}-1} + (W^2 \cap U_{k_{s_1}})).$$

  Dann erhält man Basen $\mathcal{B}_j^1 \;=\; (v_j^1, q(\varphi)(v_j^1), \ldots, q^{k_{s_1}-1}(\varphi)(v_j^1))$ für φ-zyklische Untervektorräume $W_j^1 := \mathrm{Lin}(\mathcal{B}_j^1)$.

Bezüglich jeder Basis $\mathcal{B}_j^i$ besitzt die Einschränkung $\varphi|_{W_j^i}$ das Jordankästchen $J(\lambda, k_{s_i})$ als darstellende Matrix. Zusammensetzen der $\mathcal{B}_j^i$ liefert eine Basis $\mathcal{B}$ für V mit den gewünschten Eigenschaften.

Beispiel 5.4.8. Wir wollen das Verfahren aus Bemerkung 5.4.7 auf die Matrix A aus Bemerkung 5.4.1 anwenden; zur Erinnerung:

$$A \;=\; \begin{pmatrix} 3 & -1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} \in \mathrm{Mat}(3,3;\mathbb{C}).$$

Die Elementarteiler von A sind $T-2$ und $(T-2)^2$. Das Verfahren 5.4.7 beginnt also mit $r=2$; wir vermerken zunächst

$$U_1 \;=\; \operatorname{Kern}(A-2\cdot E_3) \;=\; \operatorname{Kern}\begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \;=\; \operatorname{Lin}\left(\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}\right)$$

Wegen $U_2=\mathbb{C}^3$ ist U_2/U_1 eindimensional; es wird beispielsweise erzeugt durch die Klasse von $v_1^2 := (0,1,0)$. Das Verfahren liefert also folgende Basis für $W_1^2=W^2$:

$$\mathcal{B}_1^2 \;=\; (v_1^2, (A-2\cdot E_3)\cdot v_1^2) \;=\; \left(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ -1 \\ 0 \end{pmatrix}\right).$$

Im zweiten (und letzten) Schritt haben wir $r=1$ und $U_1/(U_0+(W^2\cap U_1))$ wird z.B., erzeugt durch die Klasse von $v_1^1=(0,1,1)$. Das liefert uns die Basis $\mathcal{B}_1^1=(v_1^1)$ für $W_1^1=W_1^1$.

Eine Transformationsmatrix $S\in \mathrm{GL}(3,\mathbb{C})$, für die $S\cdot A\cdot S^{-1}$ Jordansche Normalform besitzt, ist daher gegeben durch

$$S \;=\; (v_1^1, v_1^2, (A-2\cdot E_3)\cdot v_1^2)^{-1} \;=\; \begin{pmatrix} 0 & 0 & -1 \\ 1 & 1 & -1 \\ 1 & 0 & 0 \end{pmatrix}^{-1} \;=\; \begin{pmatrix} 0 & 0 & 1 \\ -1 & 1 & -1 \\ -1 & 0 & 0 \end{pmatrix}.$$

Aufgaben zu Abschnitt 5.4.

Aufgabe 5.4.9. Bestimme rationale und Jordansche Normalform für die folgende Matrix

$$A := \begin{pmatrix} 0 & 0 & 4 & -1 \\ 4 & 3 & 0 & -4 \\ 0 & 0 & 3 & 0 \\ 1 & 0 & 4 & -2 \end{pmatrix} \in \mathrm{Mat}(4,4;\mathbb{C})$$

Bestimme eine Matrix $S \in \mathrm{GL}(4,\mathbb{C})$, sodass $S \cdot A \cdot S^{-1}$ Jordansche Normalform besitzt.

Aufgabe 5.4.10. Es sei $A \in \mathrm{Mat}(n,n;\mathbb{K})$ eine Matrix in Jordanscher Normalform, und es sei $A = D + N$, wobei $D \in \mathrm{Mat}(n,n;\mathbb{K})$ eine Diagonalmatrix ist und $N \in \mathrm{Mat}(n,n;\mathbb{K})$ höchstens auf der (unteren) Nebendiagonalen nichttriviale Einträge besitzt. Zeige:

(i) Es gilt $D \cdot N = N \cdot D$.
(ii) Es gilt $(D+N)^k = \sum_{i=0}^{k} \binom{k}{i} D^i N^{k-i}$.

Aufgabe 5.4.11. Bestimme A^{1234} für die reelle (3×3)-Matrix

$$A := \begin{pmatrix} 0 & -1 & 1 \\ -2 & -1 & 2 \\ -3 & 1 & 0 \end{pmatrix}.$$

6. Multilineare Algebra

6.1. **Bilinearformen.**

Definition 6.1.1. Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Eine *Bilinearform* auf V ist eine Abbildung

$$\beta\colon V\times V \;\to\; \mathbb{K}, \qquad (v,v) \;\mapsto\; \beta(v,v),$$

die linear in jeder Komponente ist, d.h., für alle $v,v',w,w'\in V$ und alle $a,a',b,b'\in\mathbb{K}$ gilt:

$$\begin{aligned}\beta(a\cdot v+a'\cdot v',w) &= a\beta(v,w)+a'\beta(v',w),\\ \beta(v,b\cdot w+b'\cdot w') &= b\beta(v,w)+b'\beta(v,w').\end{aligned}$$

Beispiel 6.1.2. Es sei $\mathbb{K}$ ein Körper.

(i) Die Multiplikation in $\mathbb{K}$ liefert eine Bilinearform

$$\mathbb{K}\times\mathbb{K} \;\to\; \mathbb{K}, \qquad (x,y) \;\mapsto\; xy.$$

(ii) Anwenden von Zeilen- auf Spaltenvektoren liefert eine Bilinearform:

$$\mathbb{K}^n\times\mathbb{K}^n \;\to\; \mathbb{K}, \qquad (x,y) \;\mapsto\; x^t\cdot y = x_1y_1+\ldots+x_ny_n.$$

(iii) Jede Matrix $A\in \mathrm{Mat}(n,n;\mathbb{K})$ definiert eine Bilinearform:

$$\beta_A\colon \mathbb{K}^n\times\mathbb{K}^n \;\to\; \mathbb{K}, \qquad (x,y) \;\mapsto\; x^t\cdot A\cdot y.$$

Beispiel 6.1.3. Es sei V ein euklidischer Vektorraum. Dann ist das Skalarprodukt auf V eine Bilinearform:

$$V\times V \;\to\mathbb{R}, \qquad (v,w) \;\mapsto\; \langle v,w\rangle.$$

Beispiel 6.1.4. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum und $V^*:=\mathrm{Hom}(V,\mathbb{K})$ der zugehörige Dualraum. Sind $u,u'\in V^*$ gegeben, so gewinnt man daraus eine Bilinearform

$$V\times V \;\to\; \mathbb{K}, \qquad (v,w) \;\mapsto\; u(v)\cdot u'(w).$$

Konstruktion 6.1.5. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum. Für Bilinearformen β,β' auf V und $a\in\mathbb{K}$ erhält man neue Bilinearformen durch

$$(\beta+\beta')(v,w) \;:=\; \beta(v,w)+\beta'(v,w), \qquad (a\cdot\beta) \;:=\; a\cdot\beta(v,w).$$

Zusammen mit der so definierten Addition und Skalarmultiplikation ist die Menge $\mathrm{BiLin}(V)$ aller Bilinearformen $V\times V\to\mathbb{K}$ ein $\mathbb{K}$-Vektorraum.

Beweis. Wir wissen bereits, dass die Menge $\mathrm{Abb}(V\times V,\mathbb{K})$ zusammen mit der punktweise erklärten Addition und Skalarmultiplikation ein $\mathbb{K}$-Vektorraum ist. Es genügt also, zu zeigen, dass $\mathrm{BiLin}(V)\subseteq\mathrm{Abb}(V\times V,\mathbb{K})$ ein Untervektorraum ist.

Offensichtlich gehört die Nullabbildung zu $\mathrm{BiLin}(V)$. Es bleibt zu zeigen, dass Summen und skalare Vielfache von Bilinearformen wieder bilinear sind. Es gilt

$$\begin{aligned}(\beta+\beta')(a\cdot v+a'\cdot v',w) &= a\cdot\beta(v,w)+a'\cdot\beta(v',w)+a\cdot\beta'(v,w)+a'\cdot\beta'(v',w)\\ &= a\cdot(\beta+\beta')(v,w)+a'\cdot(\beta+\beta')(v',w),\\ (\beta+\beta')(v,b\cdot w+b'\cdot w') &= b\cdot\beta(v,w)+b'\cdot\beta(v,w')+b\cdot\beta'(v,w)+b'\cdot\beta'(v,w')\\ &= b\cdot(\beta+\beta')(v,w)+a'\cdot(\beta+\beta')(v,w'),\\ (c\cdot\beta)(a\cdot v+a'\cdot v',w) &= c\cdot(a\cdot\beta(v,w)+a'\cdot\beta(v',w))\\ &= a\cdot((c\cdot\beta)(v,w))+a'\cdot((c\cdot\beta)(v',w)),\\ (c\cdot\beta)(v,b\cdot w+b'\cdot w') &= c\cdot(b\cdot\beta(v,w)+b'\cdot\beta(v,w'))\\ &= b\cdot((c\cdot\beta)(v,w))+b'\cdot((c\cdot\beta)(v,w')).\end{aligned}$$

□

Erinnerung 6.1.6. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum und $V^* := \mathrm{Hom}(V, \mathbb{K})$ der zugehörige Dualraum. Ist $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis für V, so ist die zugehörige *duale Basis* $\mathcal{B}^* = (v_1^*, \ldots, v_n^*)$ für V^* gegeben durch

$$v_i^*(v_j) \quad = \quad \begin{cases} 1_{\mathbb{K}} & \text{falls } i = j, \\ 0_{\mathbb{K}} & \text{falls } i \neq j. \end{cases}$$

Satz 6.1.7. *Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum. Ist $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis für V und $\mathcal{B}^* = (v_1^*, \ldots, v_n^*)$ die zugehörige duale Basis für V^*, so erhält man eine Basis $(\beta_{ij};\ 1 \leq i, j \leq n)$ für $\mathrm{BiLin}(V)$ durch*

$$\beta_{ij}(v, w) \quad := \quad v_i^*(v) \cdot v_j^*(w).$$

Lemma 6.1.8. *Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum mit einer Basis $\mathcal{B} = (v_1, \ldots, v_n)$. Weiter sei $\beta \in \mathrm{BiLin}(V)$ eine Bilinearform. Dann gilt für je zwei Vektoren $v = x_1 \cdot v_1 + \ldots + x_n \cdot v_n$ und $w = y_1 \cdot v_1 + \ldots + y_n \cdot v_n$ aus V:*

$$\beta(v, w) \ = \ \sum_{1 \leq i, j \leq n} x_i y_j \beta(v_i, v_j).$$

Beweis von Satz 6.1.7. Wir zeigen zunächst, dass die Familie (β_{ij}) linear unabhängig in $\mathrm{BiLin}(V)$ ist. Dazu betrachte wir eine Linearkombination

$$\beta \ = \ \sum_{1 \leq i, j \leq n} a_{ij} \cdot \beta_{ij} \ = \ 0_{\mathrm{BiLin}(V)}.$$

Dann ergibt sich für jedes a_{ij}:

$$0_{\mathbb{K}} \ = \ \beta(v_i, v_j) \ = \ \sum_{1 \leq k, l \leq n} a_{kl} \beta_{kl}(v_i, v_j) \ = \ a_{ij}.$$

Wir zeigen nun, dass die Familie (β_{ij}) den Vektorraum $\mathrm{BiLin}(V)$ erzeugt. Dazu sei $\beta \in \mathrm{BiLin}(V)$ gegeben. Mit $c_{ij} := \beta(v_i, v_j)$ erhalten wir für je zwei Vektoren $v = x_1 \cdot v_1 + \ldots + x_n \cdot v_n$ und $w = y_1 \cdot v_1 + \ldots + y_n \cdot v_n$ aus V:

$$\begin{aligned} \beta(v, w) &= \sum_{1 \leq i, j \leq n} x_i y_j c_{ij} \\ &= \sum_{1 \leq i, j \leq n} x_i y_j c_{ij} \beta_{ij}(v_i, v_j) \\ &= \sum_{1 \leq i, j \leq n} c_{ij} \beta_{ij}(v, w) \\ &= \left(\sum_{1 \leq i, j \leq n} c_{ij} \beta_{ij} \right)(v, w). \end{aligned}$$

□

Definition 6.1.9. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum und $\beta \colon V \times V \to \mathbb{K}$ eine Bilinearform. Ist $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis für V, so definieren wir die zu β und $\mathcal{B}$ gehörige *Gramsche Matrix* als

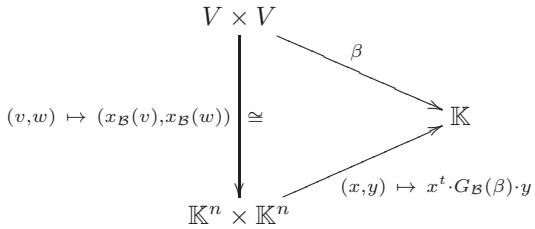
$$G_{\mathcal{B}}(\beta) \ := \ (\beta(v_i, v_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \ \in \ \mathrm{Mat}(n, n; \mathbb{K}).$$

Beispiel 6.1.10. Es seien $\mathbb{K}$ ein Körper und $\mathcal{E} = (e_1, \ldots, e_n)$ die kanonische Basis für $\mathbb{K}^n$.

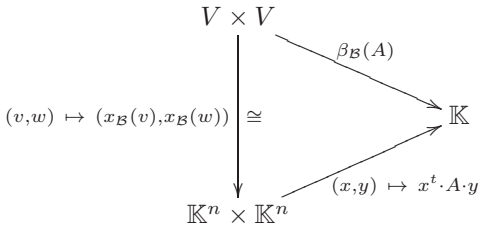
(i) Für $\beta \colon (x, y) \mapsto x^t \cdot y$ gilt $G_{\mathcal{E}}(\beta) = E_n$.
(ii) Für $\beta \colon (x, y) \mapsto x^t \cdot A \cdot y$ mit $A \in \mathrm{Mat}(n, n; \mathbb{K})$ gilt $G_{\mathcal{E}}(\beta) = A$.

Satz 6.1.11. *Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum und $\mathcal{B} = (v_1, \ldots, v_n)$ eine Basis für V.*

(i) *Ist $\beta\colon V \times V \to \mathbb{K}$ eine Bilinearform und $G_{\mathcal{B}}(\beta)$ die zugehörige Gramsche Matrix, so hat man ein kommutatives Diagramm*



(ii) *Zu jedem $A \in \mathrm{Mat}(n,n;\mathbb{K})$ gibt es eine eindeutig bestimmte Bilinearform $\beta_{\mathcal{B}}(A)\colon V \times V \to \mathbb{K}$ mit der das folgende Diagramm kommutativ wird:*



(iii) *Man hat zueinander inverse Isomorphismen von $\mathbb{K}$-Vektorräumen*

$$\begin{array}{rcl} \mathrm{BiLin}(V) & \longleftrightarrow & \mathrm{Mat}(n,n;\mathbb{K}) \\ \beta & \mapsto & G_{\mathcal{B}}(\beta) \\ \beta_{\mathcal{B}}(A) & \leftarrow\!\shortmid & A. \end{array}$$

Insbesondere ist $G_{\mathcal{B}}(\beta)$ die einzige Matrix in $\mathrm{Mat}(n,n;\mathbb{K})$, mit der das Diagramm aus (i) kommutativ wird.

Beweis. Zu (i). Sind $v = x_1 \cdot v_1 + \ldots + x_n \cdot v_n$ und $w = y_1 \cdot v_1 + \ldots + y_n \cdot v_n$ aus V gegeben, so erhalten wir

$$\beta(v,w) \;=\; \sum_{1 \le i,j \le n} x_i \beta(v_i, v_j) y_j \;=\; x_{\mathcal{B}}(v)^t G_{\mathcal{B}}(\beta) x_{\mathcal{B}}(w).$$

Zu (ii). Die gewünschte Linearform ist gegeben und festgelegt durch $\beta_{\mathcal{B}}(A) = \beta_A \circ \Phi$, wobei $\Phi\colon (v,w) \mapsto (x_{\mathcal{B}}(v), x_{\mathcal{B}}(w))$.

Zu (iii). Zunächst zeigen wir, dass die Abbildung $\varphi\colon \mathrm{BiLin}(V) \to \mathrm{Mat}(n,n;\mathbb{K})$, $\beta \to G_{\mathcal{B}}(\varphi)$ linear ist. Das lässt sich direkt nachprüfen: Es gilt

$$\begin{array}{rcl} G_{\mathcal{B}}(a \cdot \beta + a' \cdot \beta') & = & ((a \cdot \beta + a' \cdot \beta')(v_i, v_j))_{i,j} \\ & = & (a \cdot (\beta(v_i, v_j)) + a' \cdot (\beta'(v_i, v_j)))_{i,j} \\ & = & a \cdot G_{\mathcal{B}}(\beta) + a' \cdot G_{\mathcal{B}}(\beta'). \end{array}$$

Nach (i) und (ii) gilt $\beta_{\mathcal{B}}(G_{\mathcal{B}}(\beta)) = \beta$. Für $\psi\colon \mathrm{Mat}(n,n;\mathbb{K}) \to \mathrm{BiLin}(V)$, $A \mapsto \beta_{\mathcal{B}}(A)$ gilt daher $\psi \circ \varphi = \mathrm{id}$. Insbesondere ist φ injektiv. Satz 6.1.7 liefert

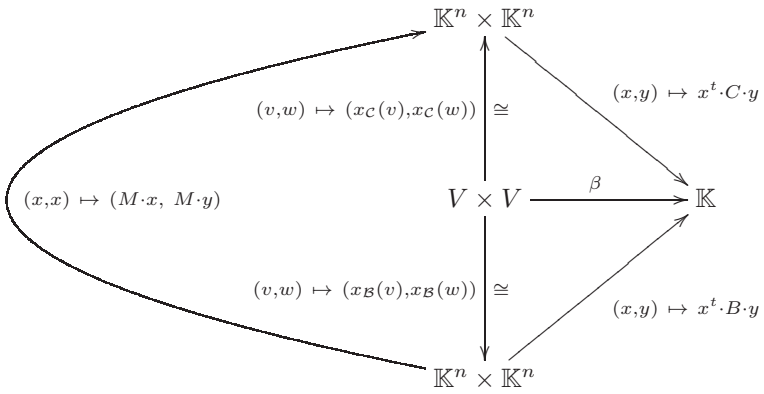
$$\dim(\mathrm{BiLin}(V)) \;=\; n^2 \;=\; \dim(\mathrm{Mat}(n,n;\mathbb{K})).$$

Folglich ist $\varphi\colon \mathrm{BiLin}(V) \to \mathrm{Mat}(n,n;\mathbb{K})$ ein Isomorphismus. Ist $\psi'\colon \mathrm{Mat}(n,n;\mathbb{K}) \to \mathrm{BiLin}(V)$ der zugehörige Umkehrisomorphismus, so folgt $\psi = \psi \circ \varphi \circ \psi' = \psi'$. $\square$

Satz 6.1.12. *Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum, $\mathcal{B} = (v_1, \ldots, v_n)$ sowie $\mathcal{C} = (w_1, \ldots, w_n)$ Basen für V und $M_{\mathcal{C}}^{\mathcal{B}}(\mathrm{id}_V)$ die zugehörige Transformationsmatrix. Ist $\beta\colon V \to V$ eine Bilinearform, so gilt für die durch $\mathcal{B}$ bzw. $\mathcal{C}$ definierten Gramschen Matrizen:*

$$G_{\mathcal{B}}(\beta) \;=\; M_{\mathcal{C}}^{\mathcal{B}}(\mathrm{id}_V)^t \cdot G_{\mathcal{C}}(\beta) \cdot M_{\mathcal{C}}^{\mathcal{B}}(\mathrm{id}_V).$$

Beweis. Wir schreiben abkürzend $C := G_{\mathcal{C}}(\beta)$ und $G_{\mathcal{B}}(\beta)$ für die Gramschen Matrizen sowie $M := M_{\mathcal{C}}^{\mathcal{B}}(\mathrm{id}_V)$ für die Transformationsmatrix. Dann erhalten wir ein kommutatives Diagramm:



Mit der Eindeutigkeit der Gramschen Matrix erhalten wir daraus die Behauptung: Setzen wir $x := x_{\mathcal{B}}(v)$ und $y := x_{\mathcal{B}}(w)$ für $(v, w) \in V \times V$, so ergibt sich

$$\beta(v,w) \;=\; x^t \cdot B \cdot y \;=\; (M \cdot x)^t \cdot C \cdot (M \cdot y) \;=\; x^t \cdot (M^t \cdot C \cdot M) \cdot y.$$

□

Folgerung 6.1.13. *Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum mit Basis $\mathcal{B} = (v_1, \ldots, v_n)$. Weiter seien $\beta \in \mathrm{BiLin}(V)$ mit Gramscher Matrix $A := G_{\mathcal{B}}(\beta)$ und $B \in \mathrm{Mat}(n, n; \mathbb{K})$ gegeben. Dann sind folgende Aussagen äquivalent.*

(i) *Es gibt eine Basis $\mathcal{C}$ für V mit $B = G_{\mathcal{C}}(\beta)$.*
(ii) *Es gibt eine Matrix $S \in \mathrm{GL}(n, \mathbb{K})$ mit $A = S^t \cdot B \cdot S$.*

Beweis. Die Implikation "(i)⇒(ii)" ergibt sich mit $S := M_{\mathcal{C}}^{\mathcal{B}}(\mathrm{id}_V)$ sofort aus der Transformationsformel 6.1.12.

Zu "(ii)⇒(i)". Es sei $w_j \in V$, sodass $x_{\mathcal{B}}(w_j) = S_{*j}^{-1}$. Dann ist $\mathcal{C} := (w_1, \ldots, w_n)$ eine Basis für V mit $M_{\mathcal{C}}^{\mathcal{B}}(\mathrm{id}_V) = S$. Die Transformationsformel 6.1.12 liefert

$$S^t \cdot B \cdot S \;=\; A \;=\; G_{\mathcal{B}}(\beta) \;=\; S^t \cdot G_{\mathcal{C}}(\beta) \cdot S.$$

Mit S ist auch S^t invertierbar. Multipliziert man die obige Gleichung von links mit $(S^t)^{-1}$ und von rechts mit S^{-1}, so ergibt sich $B = G_{\mathcal{C}}(\beta)$. □

Aufgaben zu Abschnitt 6.1.

Aufgabe 6.1.14. Es sei $\mathbb{K}$ ein Körper. Betrachte den $\mathbb{K}$-Vektorraum $V := \mathbb{K}^2$. Zeige, dass man die Bilinearform

$$\beta\colon V \times V \;\to\; \mathbb{K}, \qquad ((x_1, x_2), (y_1, y_2)) \;\mapsto\; x_1y_2 + x_2y_1.$$

nicht als Produkt von Linearformen darstellen kann, d.h., dass es kein Paar $u, u' \in V^*$ gibt mit $\beta(x, y) = u(x)u'(y)$ für alle $x, y \in V$.

Aufgabe 6.1.15. Es sei $\mathbb{K}$ ein Körper. Zeige: Man erhält eine Äquivalenzrelation "$\sim$" auf $\mathrm{Mat}(n, n; \mathbb{K})$ durch

$$A \sim B \quad :\Longleftrightarrow \quad \text{es gibt ein } S \in \mathrm{GL}(n\mathbb{K}) \text{ mit } A = S^t \cdot B \cdot S$$

6.2. **Symmetrische Bilinearformen.**

Definition 6.2.1. Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Eine Bilinearform $\beta \in \mathrm{BiLin}(V)$ nennt man *symmetrisch*, falls $\beta(v,w) = \beta(w,v)$ für alle $v, w \in V$ gilt.

Beispiel 6.2.2. Es sei V ein euklidischer Vektorraum. Dann ist das Skalarprodukt auf V eine symmetrische Bilinearform:

$$V \times V \ \to \mathbb{R}, \qquad (v,w) \ \mapsto \ \langle v, w\rangle.$$

Satz 6.2.3. *Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum mit Basis $\mathcal{B} = (v_1, \ldots, v_n)$ und $\beta \in \mathrm{BiLin}(V)$. Dann sind folgende Aussagen äquivalent:*

(i) *Die Bilinearform β ist symmetrisch.*
(ii) *Die Gramsche Matrix $G_{\mathcal{B}}(\beta) = (\beta(v_i, v_j))$ ist symmetrisch.*

Beweis. Ist β symmetrisch, so haben wir stets $\beta(v_i, v_j) = \beta(v_j, v_i)$ und somit ist $G_{\mathcal{B}}(\beta)$ symmetrisch. Ist $A := G_{\mathcal{B}}(\beta)$ symmetrisch, so gilt

$$x_{\mathcal{B}}(v)^t \cdot A \cdot x_{\mathcal{B}}(w) \ = \ (x_{\mathcal{B}}(v)^t \cdot A \cdot x_{\mathcal{B}}(w))^t \ = \ x_{\mathcal{B}}(w)^t \cdot A^t \cdot x_{\mathcal{B}}(v) \ = \ x_{\mathcal{B}}(w)^t \cdot A \cdot x_{\mathcal{B}}(v)$$

für alle $v, w \in V$. Das bedeutet $\beta(v,w) = \beta(w,v)$ für alle $v, w \in V$. Folglich ist β symmetrisch. □

Definition 6.2.4. Es sei R ein K1-Ring. Für $r \in R$ und $k \in \mathbb{Z}_{>0}$ setzen wir $k \cdot r := \sum_{i=1}^{k} r$. Die *Charakteristik* des Ringes R ist dann definiert als

$$\mathrm{Char}(R) \quad := \quad \begin{cases} 0, & \text{falls } k \cdot 1_R \neq 0_R \text{ für alle } k \in \mathbb{Z}_{>0}, \\ \min(k \in \mathbb{Z}_{>0};\ k \cdot 1_R = 0_R), & \text{sonst.} \end{cases}$$

Beispiel 6.2.5. Es gilt $\mathrm{Char}(\mathbb{Z}) = \mathrm{Char}(\mathbb{Q}) = \mathrm{Char}(\mathbb{R}) = \mathrm{Char}(\mathbb{C}) = 0$. Weiter hat man $\mathrm{Char}(\mathbb{Z}/n\mathbb{Z}) = n$ für jede ganze Zahl $n \in \mathbb{Z}_{>0}$.

Satz 6.2.6. *Es sei $\mathbb{K}$ ein Körper mit $\mathrm{Char}(\mathbb{K}) \neq 2$ und $A \in \mathrm{Mat}(n,n;\mathbb{K})$ eine symmetrische Matrix. Dann gibt es $a_1, \ldots, a_n \in \mathbb{K}$ und Elementarmatrizen $S_1, \ldots, S_k \in \mathrm{Mat}(n,n;\mathbb{K})$ der Typen $E(n;\lambda;j,i)$ und $E(n;i,j)$, sodass*

$$S_k^t \cdots S_1^t \cdot A \cdot S_1 \cdots S_k \quad = \quad \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

Beweis. Multipliziert man $E(n;\lambda;j,i)$ von rechts an die Matrix A heran, so entspricht dies der Spaltenoperation $\mathrm{SpOp}(\lambda;i,j)$, d.h., das λ-fache der i-ten Spalte wird zur j-ten addiert. Weiter haben wir

$$E(n;\lambda;j,i)^t \quad = \quad E(n;\lambda;i,j).$$

Multipliziert man also $E(n;\lambda;j,i)^t$ von links an die Matrix A, so entspricht dies dem Anwenden der Zeilenoperation $\mathrm{ZOp}(\lambda;i,j)$, d.h., das λ-fache der i-ten Zeile wird zur j-ten addiert.

Heranmultiplizieren von $E(n;i,j)$ von rechts an A entspricht $\mathrm{SpOp}(i,j)$, dem Vertauschen der i-ten mit der j-ten Spalte wir haben

$$E(n;i,j)^t \quad = \quad E(i,j)$$

und somit entspricht Heranmultiplizieren von $E(n;i,j)^t$ von links an A dem Vertauschen $\mathrm{ZOp}(i,j)$ der i-ten mit der j-ten Zeile.

Schließlich vermerken wir noch, dass für jedes $S \in \mathrm{GL}(n,\mathbb{K})$ die Matrix $S^t \cdot A \cdot S$ wieder symmetrisch ist, denn es gilt

$$(S^t \cdot A \cdot S)^t \ = \ S^t \cdot A^t \cdot (S^t)^t \ = \ S^t \cdot A \cdot S.$$

Aufgrund dieser Vorbemerkungen genügt es, die Matrix A durch paarweises Anwenden elementarer Operationen $\mathrm{ZOp}(\lambda; i, j)$ und $\mathrm{SpOp}(\lambda; i, j)$ bzw. $\mathrm{ZOp}(i, j)$ und $\mathrm{SpOp}(i, j)$ auf Diagonalgestalt zu bringen. Dazu steigen wir in eine Iterationsschleife mit den folgenden drei Schritten ein:

Schritt 0. Falls A_{1*} keine Nullzeile ist, gehen wir zu Schritt 1. Andernfalls ist A_{*1} eine Nullspalte, und wir brechen den aktuellen Schleifendurchlauf ab mit

$$A \;=\; \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 0 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \ldots & * \end{pmatrix}$$

Schritt 1. Gilt $a_{11} \neq 0_{\mathbb{K}}$, so gehen wir direkt zu Schritt 2. Gilt $a_{11} = 0_{\mathbb{K}}$, so unterscheiden zwei Fälle:

Gibt es ein i mit $a_{ii} \neq 0_{\mathbb{K}}$, so wenden wir $\mathrm{ZOp}(i, 1)$ und $\mathrm{SpOp}(i, 1)$ auf die Matrix A an und setzen $a := a_{ii} \neq 0_{\mathbb{K}}$.

Gilt $a_{ii} = 0_{\mathbb{K}}$ für $i = 1, \ldots, n$, so wählen wir i mit $a_{i1} \neq 0_{\mathbb{K}}$, wenden $\mathrm{ZOp}(1_{\mathbb{K}}; i, 1)$ und $\mathrm{SpOp}(1_{\mathbb{K}}; i, 1)$ auf die Matrix A an und setzen $a := 2 \cdot 1_{\mathbb{K}} \cdot a_{i1} \neq 0_{\mathbb{K}}$.

In jedem der beiden Fälle bringen die genannten Operationen die Matrix A auf die Gestalt

$$\begin{pmatrix} a & * & \ldots & * \\ * & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \ldots & * \end{pmatrix}$$

Schritt 2. Anwenden von $\mathrm{ZOp}(-a_{j1}/a; 1, j)$ und $\mathrm{SpOp}(-a_{1j}/a; 1, j)$ für $j = 2, \ldots, n$ bringt das Ergebnis aus Schritt 1 auf die Gestalt

$$\begin{pmatrix} a & 0 & \ldots & 0 \\ 0 & * & \ldots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \ldots & * \end{pmatrix} \;=\; \begin{pmatrix} a & 0 \\ 0 & A' \end{pmatrix}$$

Nach dem ersten Durchlauf der drei Schritte gehen wir mit der (kleineren, ebenfalls symmetrischen) Matrix A' in die Schleife. Nach n Durchläufen haben wir A auf Diagonalgestalt gebracht. □

Folgerung 6.2.7. *Es seien $\mathbb{K}$ ein Körper mit $\mathrm{Char}(\mathbb{K}) \neq 2$ und V ein endlichdimensionaler $\mathbb{K}$-Vektorraum. Dann gibt es zu jeder symmetrischen Bilinearform $\beta \in \mathrm{BiLin}(V)$ eine Basis $\mathcal{B}$ von V, sodass $G_{\mathcal{B}}(\beta)$ ein Diagonalmatrix ist.*

Beweis. Es sei $\mathcal{C}$ eine beliebige Basis für V. Nach Satz 6.2.3 ist die zugehörige Gramsche Matrix $A := G_{\mathcal{B}}(\beta)$ symmetrisch. Nach Satz 6.2.6 gibt es eine Matrix $S \in \mathrm{GL}(n, \mathbb{K})$, sodass $S^t \cdot A \cdot S$ Diagonalgestalt besitzt. Folgerung 6.1.13 liefert dann eine Basis $\mathcal{B}$ für V, sodass $G_{\mathcal{B}}(\beta)$ Diagonalgestalt besitzt. □

Bemerkung 6.2.8. Der Beweis von Satz 6.2.6 liefert ein konkretes Verfahren, um eine symmetrische Matrix A durch paarweise Zeilen- und Spaltenumformungen in eine Diagonalmatrix D zu überführen. Als Beispiel betrachten wir die Matrix

$$A \;:=\; \begin{pmatrix} 1 & 2 & 1 \\ 2 & -1 & 2 \\ 1 & 2 & 2 \end{pmatrix}$$

Neben der Diagonalmatrix D bestimmen wir eine invertierbare Matrix S, sodass $S^t \cdot A \cdot S = D$ gilt. Dazu führen wir die jeweils verwendeten Spaltenoperationen mit, indem wir sie sukzessive auf eine Einheitsmatrix anwenden:

$$\left(\begin{pmatrix} 1 & 2 & 1 \\ 2 & -1 & 2 \\ 1 & 2 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right)$$

$$\xrightarrow{\text{ZOp}(-2;1,2)} \quad \left(\begin{pmatrix} 1 & 2 & 1 \\ 0 & -5 & 0 \\ 1 & 2 & 2 \end{pmatrix}, \quad\right)$$

$$\xrightarrow{\text{SpOp}(-2;1,2)} \quad \left(\begin{pmatrix} 1 & 0 & 1 \\ 0 & -5 & 0 \\ 1 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right)$$

$$\xrightarrow{\text{ZOp}(-1;1,3)} \quad \left(\begin{pmatrix} 1 & 0 & 1 \\ 0 & -5 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad\right)$$

$$\xrightarrow{\text{SpOp}(-1;1,3)} \quad \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -2 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\right)$$

Manchmal möchte man noch die Diagonaleinträge sortieren. Dies ist durch paarweise Zeilen- und Spaltenvertauschungen machbar:

$$\xrightarrow{\text{ZOp}(2,3)} \quad \left(\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & -5 & 0 \end{pmatrix}, \quad\right)$$

$$\xrightarrow{\text{SpOp}(2,3)} \quad \left(\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -5 \end{pmatrix}, \begin{pmatrix} 1 & -1 & -2 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\right)$$

Damit haben wir, wie gewünscht, eine Diagonalmatrix D und eine invertierbare Matrix S gefunden, sodass $S^t \cdot A \cdot S = D$ gilt, nämlich

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -5 \end{pmatrix}, \qquad S = \begin{pmatrix} 1 & -1 & -2 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Bemerkung 6.2.9. Es sei $\mathbb{K}$ ein Körper. Im Allgemeinen kann es grundsätzlich verschiedene Diagonalmatrizen D, D' geben, sodass $D' = S^t \cdot D \cdot S$ mit einer Matrix $S \in \mathrm{GL}(n, \mathbb{K})$ gilt. Für $\mathbb{K} = \mathbb{Q}$ hat man beispielsweise

$$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

Insbesondere kann man nicht ohne weiteres von einer "Normalform" $D = S^t \cdot A \cdot S$ in Diagonalgestalt für symmetrischen Matrizen A sprechen.

Definition 6.2.10. Es seien V ein $\mathbb{R}$-Vektorraum und $\beta \in \mathrm{BiLin}(V)$ symmetrisch.

(i) Man nennt β *positiv definit*, falls $\beta(v, v) > 0$ für alle $0_V \neq v \in V$ gilt.
(ii) Man nennt β *negativ definit*, falls $\beta(v, v) < 0$ für alle $0_V \neq v \in V$ gilt.
(iii) Der *Ausartungsraum* der Bilinearform β ist der Untervektorraum

$$V^0 := \{v \in V;\ \beta(v, w) = 0 \text{ für alle } w \in V\} \leq_{\mathbb{R}} V.$$

Satz 6.2.11 (Sylvestersches Trägheitsgesetz)**.** *Es seien V ein n-dimensionaler $\mathbb{R}$-Vektorraum, und es sei $\beta \in \mathrm{BiLin}(V)$ symmetrisch. Weiter seien*

$$V = V_1^+ \oplus V_1^- \oplus V^0 = V_2^+ \oplus V_2^- \oplus V^0$$

zwei direkte Zerlegungen, sodass β positiv definit auf den V_i^+ und negativ definit auf den V_i^+ ist. Dann gilt

$$\dim(V_1^+) \;=\; \dim(V_2^+), \qquad \dim(V_1^-) \;=\; \dim(V_2^-), \qquad \dim(V_1^0) \;=\; \dim(V_2^0).$$

Beweis. Die Dimensionen der beteiligten Untervektorräume bezeichnen wir mit $n^0 := \dim(V^0)$ sowie $n_i^+ := \dim(V_i^+)$ und $n_i^- := \dim(V_i^-)$, wobei $i = 1, 2$.

Wir zeigen zunächst, dass $\beta(v, v) \leq 0$ für alle $v \in V_i^- \oplus V_i^0$ gilt. Dazu schreiben wir $v = v^- + v^0$ mit $v^- \in V_i^-$ und $v^0 \in V_i^0$. Dann ergibt sich

$$\beta(v, v) \;=\; \beta(v^-, v^-) + \beta(v^-, v^0) + \beta(v^0, v^-) + \beta(v^0, v^0) \;\leq\; 0.$$

Damit erhalten wir $V_1^+ \cap (V_2^- \oplus V_2^0) = \{0_V\}$. Die Dimensionsformel liefert uns

$$\begin{aligned} n_1^+ + n_2^- + n^0 &= \dim(V_1^+ + (V_2^- \oplus V_2^0)) \\ &\leq \dim(V) \\ &= n_2^+ + n_2^+ + n^0. \end{aligned}$$

Das bedeutet $n_1^+ \leq n_2^+$ Analog sieht man $n_2^+ \leq n_1^+$. Also gilt $n_1^+ = n_2^+$. Mit $n = n_i^+ + n_i^- + n^0$ erhalten wir daraus $n_1^- = n_2^-$. □

Satz 6.2.12. *Für den Körper $\mathbb{R}$ der reellen Zahlen gilt:*

(i) *Ist $A \in \mathrm{Mat}(n, n; \mathbb{R})$ symmetrisch, so gibt es eine Matrix $S \in \mathrm{GL}(n, \mathbb{R})$ mit*

$$S^t \cdot A \cdot S \;=\; \begin{pmatrix} E_{n^+} & & 0 \\ 0 & E_{n^-} & 0 \\ 0 & & 0_{n^0} \end{pmatrix},$$

Dabei sind die Zahlen n^+ und n^- sowie $n^0 = n - \mathrm{Rang}(A)$ eindeutig bestimmt.

(ii) *Es seien V ein n-dimensionaler $\mathbb{R}$-Vektorraum, und es sei $\beta \in \mathrm{BiLin}(V)$ symmetrisch. Dann gibt es seine Basis $\mathcal{B}$ für V mit*

$$G_{\mathcal{B}}(\beta) \;=\; \begin{pmatrix} E_{n^+} & & 0 \\ 0 & E_{n^-} & 0 \\ 0 & & 0_{n^0} \end{pmatrix},$$

Dabei sind die Zahlen n^+ und n^- sowie $n^0 = n - \mathrm{Rang}(G_{\mathcal{B}}(\beta))$ eindeutig bestimmt.

Beweis. Nach Folgerung 6.1.13 genügt es, Aussage (i) zu beweisen. Nach Satz 6.2.6 gibt es eine invertierbare Matrix $S_0 \in \mathrm{GL}(n, \mathbb{R})$ mit

$$S_0^t \cdot A \cdot S_0 \;=\; \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{pmatrix}$$

Durch symmetrisches Vertauschen von Zeilen und Spalten erreichen wir dabei, dass die ersten n^+ Diagonaleinträge positiv, die folgenden n^- negativ sind und die letzten n^0 alle verschwinden. Mit

$$S \;:=\; S_0 \cdot \begin{pmatrix} \frac{1}{\sqrt{|a_1|}} & & 0 & 0 \\ & \ddots & & \\ 0 & & \frac{1}{\sqrt{|a_{n^+ + n^-}|}} & \\ 0 & & & E_{n^0} \end{pmatrix}$$

besitzt $S^t \cdot A \cdot S$ die gewünschte Gestalt. Nach der Transformationsformel 6.1.12 besitzt die Basis $\mathcal{B}$ für V mit Transformationsmatrix $M_{\mathcal{C}}^{\mathcal{B}}(\mathrm{id}_V) = S$ die gewünschte Eigenschaft.

Für die Zusatzaussage betrachten wir die symmetrische Bilinearform $\beta\colon (x, y) \mapsto x^t \cdot A \cdot y$ auf $\mathbb{R}^n$. Ist $\mathcal{B}$ eine Basis für $\mathbb{R}^n$, sodass $G_{\mathcal{B}}(\beta) = S^t \cdot A \cdot S$ gilt, sind die Zahlen n^+, n^-, n^0 aus der Behauptung genau die Dimensionen n^+, n^-, n^0 einer Zerlegung wie im Sylvesterschen Trägheitsgesetz. Das liefert ihre Eindeutigkeit. □

Bemerkung 6.2.13. Es sei $A \in \mathrm{Mat}(n, n; \mathbb{R})$ eine symmetrische Matrix. In [1, § 9.4] hatten wir gesehen, dass man immer eine *orthogonale* Matrix $S \in \mathrm{Mat}(n, n; \mathbb{R})$ findet, d.h., eine invertierbare Matrix S mit $S^{-1} = S^t$, sodass

$$S^t \cdot A \cdot S \quad = \quad \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

mit den *Eigenwerten* $\lambda_1, \ldots, \lambda_n$ gilt. Das Sylvestersche Trägheitsgesetz liefert, dass die Zahlen der positiven bzw. negativen Eigenwerte von A genau die Zahlen n^+ bzw. n^- aus Satz 6.2.12 sind.

Aufgaben zu Abschnitt 6.2.

Aufgabe 6.2.14. Es sei $\mathbb{K} := \mathbb{Z}/2\mathbb{Z}$. Bestimme ein Repräsentantensystem der folgenden Äquivalenzrelation auf $\mathrm{Mat}(2,2;\mathbb{K})$:

$$A \sim B :\Longleftrightarrow\ B = S^t \cdot A \cdot S \text{ mit } S \in \mathrm{GL}(2,\mathbb{K}).$$

Aufgabe 6.2.15. Zeige, dass man die Aussage von Satz 6.2.6 stets mit Elementarmatrizen $S_1, \ldots, S_k$ vom Typ $E(\lambda; j, i)$ erreichen kann.

Aufgabe 6.2.16. Es sei $A \in \mathrm{Mat}(n,n;\mathbb{C})$ eine symmetrische Matrix vom Rang r. Zeige: Es gibt eine Matrix $S \in \mathrm{GL}(n,\mathbb{C})$ mit

$$S^t \cdot A \cdot S \quad = \quad \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}.$$

Aufgabe 6.2.17. Es seien $A \in \mathrm{Mat}(n,n;\mathbb{R})$ symmetrisch und $S \in \mathrm{GL}(n,\mathbb{R})$ mit

$$S^t \cdot A \cdot S \quad = \quad \begin{pmatrix} E_{n^+} & 0 \\ 0 & -E_{n^-} \end{pmatrix}.$$

Zeige: Es gilt $\det(S) = \pm\sqrt{|\lambda_1 \cdots \lambda_n|}$, wobei $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ die Eigenwerte von A sind.

6.3. **Tensorprodukte.**

Definition 6.3.1. Es seien $\mathbb{K}$ ein Körper, und es seien $\mathbb{K}$-Vektorräume $V_1, \ldots, V_r$ sowie W gegeben. Eine Abbildung $\Phi\colon V_1 \times \ldots \times V_r \to W$ heisst *multilinear*, falls sie linear in jeder Komponente ist, d.h., falls stets gilt

$$\begin{aligned}\Phi(v_1,\ldots,v_{i-1}, a\cdot v_i + a'\cdot v_i', v_{i+1},\ldots,v_r) \quad &= \quad a\cdot\Phi(v_1,\ldots,v_{i-1}, v_i, v_{i+1},\ldots,v_r)\\ &\quad + a'\cdot\Phi(v_1,\ldots,v_{i-1}, v_i', v_{i+1},\ldots,v_r).\end{aligned}$$

Beispiel 6.3.2. Es sei $\mathbb{K}$ ein Körper und $n \in \mathbb{Z}_{\geq 1}$. Dann erhält man eine multilineare Abbildung

$$\mathbb{K}^n = \mathbb{K} \times \ldots \times \mathbb{K} \;\to\; \mathbb{K}, \qquad (a_1, \ldots, a_r) \;\mapsto\; a_1 \cdots a_r.$$

Insbesondere sieht man, dass eine multilineare Abbildung im allgemeinen keine lineare Abbildung ist.

Beispiel 6.3.3. Es seien $\mathbb{K}$ ein Körper, $V_1, \ldots, V_r$ Vektorräume über $\mathbb{K}$, und es seien $V_i^* := \mathrm{Hom}(V_i, \mathbb{K})$ die zugehörigen Dualräume. Sind Linearformen $u_i \in V_i^*$ gegeben, so erhält man eine multilineare Abbildung

$$V_1 \times \ldots \times V_r \;\to\; \mathbb{K}, \qquad (v_1, \ldots, v_r) \;\mapsto\; u_1(v_1) \cdots u_r(v_r).$$

Beispiel 6.3.4. Es seien $\mathbb{K}$ ein Körper und $V_1 := \ldots := V_r := \mathbb{K}^n$. Dann liefert die Determinante eine multilineare Abbildung

$$V_1 \times \ldots \times V_r \;\to\; \mathbb{K}, \qquad (v_1, \ldots, v_n) \;\mapsto\; \det(v_1, \ldots, v_n).$$

Konstruktion 6.3.5. Es seien $\mathbb{K}$ ein Körper, und es seien $\mathbb{K}$-Vektorräume $V_1, \ldots, V_r$ sowie W gegeben. Dann machen die punktweisen Verknüpfungen

$$\begin{aligned}(\Phi + \Psi)(v_1, \ldots, v_r) \quad &:= \quad \Phi(v_1, \ldots, v_r) \;+\; \Psi(v_1, \ldots, v_r),\\ (a\cdot\Phi)(v_1, \ldots, v_r) \quad &:= \quad a\cdot(\Phi(v_1, \ldots, v_r))\end{aligned}$$

die Menge $\mathrm{MultLin}(V_1, \ldots, V_r; W)$ der multilinearen Abbildungen $V_1 \times \ldots \times V_r \to W$ zu einem $\mathbb{K}$-Vektorraum.

Konstruktion 6.3.6. Es seien ein Körper $\mathbb{K}$ und $\mathbb{K}$-Vektorräume $V_1, \ldots, V_r$ gegeben. Das Tensorprodukt von $V_1, \ldots, V_r$ wird in drei Schritten konstruiert:

Schritt 1. Man bildet den freien $\mathbb{K}$-Vektorraum $F(V_1 \times \ldots \times V_r)$ über der Menge $V_1 \times \ldots \times V_r$, d.h.:

$$F(V_1 \times \ldots \times V_r) \quad := \quad \bigoplus_{(v_1,\ldots,v_r) \in V_1 \times \ldots \times V_r} \mathbb{K}\cdot(v_1, \ldots, v_r).$$

Man beachte dabei, dass die Elemente der Form $1_{\mathbb{K}}\cdot(v_1, \ldots, v_r) \in F(V_1 \times \ldots \times, V_r)$ mit $(v_1, \ldots, v_r) \in V_1 \times \ldots \times V_r$ eine Basis für $F(V_1, \ldots, V_r)$ bilden.

Schritt 2. Es sei $R(V_1 \times \ldots \times V_r) \leq_{\mathbb{K}} F(V_1 \times \ldots \times V_r)$ der Aufspann von allen Elementen der Form

$$\begin{aligned}1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1}, v_i + v_i', v_{i+1},\ldots,v_r) \quad &- \quad 1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1}, v_i, v_{i+1},\ldots,v_r)\\ &- \quad 1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1}, v_i', v_{i+1},\ldots,v_r),\end{aligned}$$

$$1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1}, av_i, v_{i+1},\ldots,v_r) \quad - \quad a\cdot(v_1,\ldots,v_{i-1}, v_i, v_{i+1},\ldots,v_r).$$

Schritt 3. Das *Tensorprodukt* der Vektorräume $V_1, \ldots, V_r$ ist definiert als der Quotientenvektorraum

$$V_1 \otimes \ldots \otimes V_r \quad := \quad F(V_1 \times \ldots \times V_r)/R(V_1 \times \ldots \times V_r).$$

Für $1_{\mathbb{K}} \cdot (v_1, \ldots, v_r) \in F(V_1 \times \ldots \times V_r)$ bezeichnet $v_1 \otimes \ldots \otimes v_r \in V_1 \otimes \ldots \otimes V_r$ die zugehörige Äquivalenzklasse. Die Restklassenabbildung ist dann festgelegt durch

$$\pi\colon F(V_1 \times \ldots \times V_r) \ \to \ V_1 \otimes \ldots \otimes V_r, \qquad 1_{\mathbb{K}} \cdot (v_1, \ldots, v_r) \ \to \ v_1 \otimes \ldots \otimes v_r$$

Bemerkung 6.3.7. Es seien $\mathbb{K}$ ein Körper und $V_1, \ldots, V_r$ Vektorräume über $\mathbb{K}$. Dann gelten folgende Rechenregeln in $V_1 \otimes \ldots \otimes V_r$:

$$\begin{aligned} & v_1 \otimes \ldots \otimes v_{i-1} \otimes (v_i + v_i') \otimes v_{i+1} \otimes \ldots \otimes v_r \\ = \ & v_1 \otimes \ldots \otimes v_{i-1} \otimes v_i \otimes v_{i+1} \otimes \ldots \otimes v_r \ + \ v_1 \otimes \ldots \otimes v_{i-1} \otimes v_i' \otimes v_{i+1} \otimes \ldots \otimes v_r, \end{aligned}$$

$$\begin{aligned} & v_1 \otimes \ldots \otimes v_{i-1} \otimes a \cdot v_i \otimes v_{i+1} \otimes \ldots \otimes v_r \\ = \ & a \cdot (v_1 \otimes \ldots \otimes v_{i-1} \otimes v_i \otimes v_{i+1} \otimes \ldots \otimes v_r). \end{aligned}$$

Bemerkung 6.3.8. Es seien $\mathbb{K}$ ein Körper und $V_1, \ldots, V_r$ Vektorräume über $\mathbb{K}$. Ein Element der Form $v_1 \otimes \ldots \otimes v_r \in V_1 \otimes \ldots \otimes V_r$ mit $v_i \in V_i$ nennt man auch *zerlegbar*. Es gilt

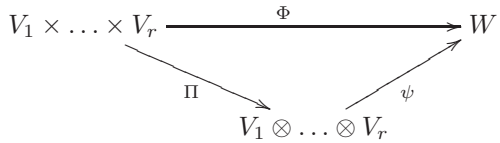
(i) Jedes Element von $V_1 \otimes \ldots \otimes V_r$ ist eine (endliche) Summe von zerlegbaren Elementen.
(ii) Im allgemeinen ist nicht jedes Element in $V_1 \otimes \ldots \otimes V_r$ zerlegbar; ein Beispiel für ein nicht zerlegbares Element ist

$$e_1 \otimes e_2 \ + \ e_2 \otimes e_1 \quad \in \quad \mathbb{R}^2 \ \otimes \mathbb{R}^2.$$

Satz 6.3.9. *Es seien ein Körper $\mathbb{K}$ und $\mathbb{K}$-Vektorräume $V_1, \ldots, V_r$ gegeben. Dann hat man eine kanonische multilineare Abbildung*

$$\Pi\colon V_1 \times \ldots \times V_r \ \to \ V_1 \otimes \ldots \otimes V_r, \qquad (v_1, \ldots, v_r) \ \mapsto \ v_1 \otimes \ldots \otimes v_r.$$

Zu jeder weiteren multilinearen Abbildung $\Phi\colon V_1 \times \ldots \times V_r \to W$ gibt es ein kommutatives Diagramm



mit einer linearen Abbildung $\psi\colon V_1 \otimes \ldots \otimes V_r \to W$; diese Abbildung ist eindeutig bestimmt, und es gilt stets

$$\psi(v_1 \otimes \ldots \otimes v_r) \quad = \quad \Phi(v_1, \ldots, v_r).$$

Beweis. Zunächst beachte man, dass es eine kanonische Abbildung von Mengen gibt

$$\imath\colon V_1 \times \ldots \times V_r \ \to \ F(V_1 \times \ldots \times V_r), \qquad (v_1, \ldots, v_r) \ \mapsto \ 1_{\mathbb{K}} \cdot (v_1, \ldots, v_r).$$

Wir setzen $\Pi := \pi \circ \imath$, wobei $\pi\colon F(V_1 \times \ldots \times V_r) \to V_1 \otimes \ldots \otimes V_r$ die Restklassenabbildung bezeichnet. Nach Konstruktion liegen die Elemente der Form

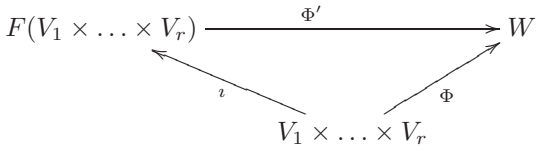
$$\begin{aligned} A \ &:= \ \imath(*,\ldots,*, v_i + v_i', *,\ldots,*) \ - \ (\imath(*,\ldots,*, v_i, *,\ldots,*) \ + \ \imath(*,\ldots,*, v_i', *,\ldots,*)), \\ B \ &:= \ \imath(*,\ldots,*, a \cdot v_i, *,\ldots,*) \ - \ a \cdot \imath(*,\ldots,*, v_i', *,\ldots,*) \end{aligned}$$

in $R(V_1 \times \ldots \times V_r)$ und werden daher durch π auf den Nullvektor abgebildet. Mit der Linearität von π ergibt sich dann die Multilinearität von Π: Es gilt

$$\begin{aligned}
\Pi(*,\ldots,*, v_i + v_i', *,\ldots,*) &= \pi(\imath(*,\ldots,*, v_i + v_i', *,\ldots,*) - A) \\
&= \pi(\imath(*,\ldots,*, v_i, *,\ldots,*) \ + \ \imath(*,\ldots,*, v_i', *,\ldots,*)) \\
&= \pi(\imath(*,\ldots,*, v_i, *,\ldots,*)) \ + \ \pi(\imath(*,\ldots,*, v_i', *,\ldots,*)) \\
&= \Pi(*,\ldots,*, v_i, *,\ldots,*) \ + \ \Pi(*,\ldots,*, v_i', *,\ldots,*)
\end{aligned}$$

$$\begin{aligned}
\Pi(*,\ldots,*, a\cdot v_i, *,\ldots,*) &= \pi(\imath(*,\ldots,*, a\cdot v_i, *,\ldots,*) - B) \\
&= \pi(a\cdot\imath(*,\ldots,*, v_i, *,\ldots,*)) \\
&= a\cdot\pi(\imath(*,\ldots,*, v_i, *,\ldots,*)) \\
&= a\cdot\Pi(*,\ldots,*, v_i, *,\ldots,*).
\end{aligned}$$

Es sei nun $\Phi\colon V_1 \times \ldots \times V_r \to W$ eine multilineare Abbildung. Dann erhalten wir zunächst ein kommutatives Diagramm



indem wir eine lineare Abbildung $\Phi'\colon F(V_1 \times \ldots \times V_r) \to W$ durch Vorgabe von Werten auf einer Basis definieren:

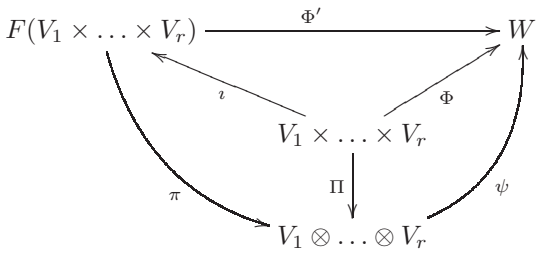
$$\Phi'(1_{\mathbb{K}}\cdot(v_1, \ldots, v_r)) \quad := \quad \Phi(v_1, \ldots, v_r).$$

Dann stellen wir fest, das der Untervektorraum $R(V_1, \ldots, V_r) \leq_{\mathbb{K}} F(V_1, \ldots, V_r)$ in $\mathrm{Kern}(\Phi')$ enthalten ist: Es gilt

$$\begin{aligned}
& \Phi'(1_{\mathbb{K}}\cdot(*,\ldots,*, v_i + v_i', *,\ldots,*) \ - \ 1_{\mathbb{K}}\cdot(*,\ldots,*, v_i, *,\ldots,*) \ - \ 1_{\mathbb{K}}\cdot(*,\ldots,*, v_i', *,\ldots,*)), \\
= \ & \Phi'(\imath(*,\ldots,*, v_i + v_i', *,\ldots,*)) \ - \ \Phi'(\imath(*,\ldots,*, v_i, *,\ldots,*)) \ - \ \Phi'(\imath(*,\ldots,*, v_i', *,\ldots,*)) \\
= \ & \Phi(*,\ldots,*, v_i + v_i', *,\ldots,*) \ - \ \Phi(*,\ldots,*, v_i, *,\ldots,*) \ - \ \Phi(*,\ldots,*, v_i', *,\ldots,*) \\
= \ & \Phi(*,\ldots,*, 0_{V_i}, *,\ldots,*) \\
= \ & 0_W.
\end{aligned}$$

$$\begin{aligned}
& \Phi'(1_{\mathbb{K}}\cdot(*,\ldots,*, av_i*,\ldots,*) \ - \ a\cdot(*,\ldots,*, v_i, *,\ldots,*)) \\
= \ & \Phi'(\imath(*,\ldots,*, av_i*,\ldots,*)) \ - \ \Phi'(\imath(a\cdot(*,\ldots,*, v_i, *,\ldots,*))) \\
= \ & \Phi(*,\ldots,*, av_i*,\ldots,*) \ - \ \Phi(a\cdot(*,\ldots,*, v_i, *,\ldots,*)) \\
= \ & \Phi(*,\ldots,*, 0_{V_i}, *,\ldots,*) \\
= \ & 0_W.
\end{aligned}$$

Wegen $R(V_1 \times \ldots \times V_r) \subseteq \mathrm{Kern}(\pi)$ liefert uns der Homomorphiesatz eine lineare Abbildung $\psi\colon V_1 \otimes \ldots \otimes V_r \to W$ mit der das Diagramm



kommutativ wird. Die Eindeutigkeit von ψ ergibt sich sofort aus der Tatsache, dass $V_1 \otimes \ldots \otimes V_r$ durch die Elemente aus $\Pi(V_1 \times \ldots \times V_r)$ erzeugt wird. □

Folgerung 6.3.10. *Es seien $\mathbb{K}$ ein Körper und $V_1, \ldots, V_r$ sowie W Vektorräume über $\mathbb{K}$. Dann hat man kanonische Isomorphismen von $\mathbb{K}$-Vektorräumen*

$$\begin{array}{rcl} \operatorname{MultLin}(V_1, \ldots, V_r; W) & \longleftrightarrow & \operatorname{Hom}(V_1 \otimes \ldots \otimes V_r, W) \\ \varphi & \mapsto & [v_1 \otimes \ldots \otimes v_r \mapsto \varphi(v_1, \ldots, v_r)] \\ [(v_1, \ldots, v_r) \mapsto \psi(v_1 \otimes \ldots \otimes v_r)] & \leftarrow\!\shortmid & \psi \end{array}$$

Folgerung 6.3.11. *Es seien $\mathbb{K}$ ein Körper und $\varphi\colon V_i \to V_i'$, $1 \le i \le r$, lineare Abbildungen von $\mathbb{K}$-Vektorräumen. Dann hat man ein kommutatives Diagramm*

$$\begin{array}{ccc} V_1 \times \ldots \times V_r & \xrightarrow[\varphi_1 \times \ldots \times \varphi_r]{(v_1,\ldots,v_r) \mapsto (\varphi(v_1),\ldots,\varphi(v_r))} & V_1' \times \ldots \times V_r' \\ \Big\downarrow \Pi & & \Big\downarrow \Pi' \\ V_1 \otimes \ldots \otimes V_r & \xrightarrow[v_1 \otimes \ldots \otimes v_r \mapsto \varphi(v_1) \otimes \ldots \otimes \varphi(v_r)]{\varphi_1 \otimes \ldots \otimes \varphi_r} & V_1' \otimes \ldots \otimes V_r' \end{array}$$

mit den kanonischen multilinearen Abbildungen Π, Π' und einer eindeutig bestimmten linearen Abbildung $\varphi_1 \otimes \ldots \otimes \varphi_r\colon V_1 \otimes \ldots \otimes V_r \to V_1' \otimes \ldots \otimes V_r'$

Beweis. Die Komposition $\Pi' \circ (\varphi_1 \times \ldots \times \varphi_r)\colon V_1 \times \ldots \times V_r \to V_1' \otimes \ldots \otimes V_r'$ ist multilinear. Existenz und Eindeutigkeit der linearen Abbildung $\varphi_1 \otimes \ldots \otimes \varphi_r$ folgen daher aus Satz 6.3.9. □

Satz 6.3.12. *Es seien ein Körper $\mathbb{K}$ und $\mathbb{K}$-Vektorräume $V_1, \ldots, V_r$ gegeben. Sind $\mathcal{B}_i = (v_1^i, \ldots, v_{n_i}^i)$ Basen für V_i, so ist*

$$\mathcal{B} \;:=\; (v_{j_1}^1 \otimes \ldots \otimes v_{j_r}^r;\ 1 \le j_i \le n_i)$$

eine Basis für das Tensorprodukt $V_1 \otimes \ldots \otimes V_r$. Insbesondere erhält man für die Dimension des Tensorproduktes

$$\dim(V_1 \otimes \ldots \otimes V_r) \;=\; \dim(V_1) \cdots \dim(V_r).$$

Beweis. Um zu sehen, dass $\mathcal{B}$ ein Erzeugendensystem ist, genügt es zu sehen, dass man jedes Element der Form $v_1 \otimes \ldots \otimes v_r$ mit $v_i \in V_i$ als Linearkombination über den $v_{j_1}^1 \otimes \ldots \otimes v_{j_r}^r$ darstellen kann. Dazu betrachten wir die Entwicklungen

$$v_i \;=\; a_1^i \cdot v_1^i + \ldots + a_{n_i}^i \cdot v_{n_i}^i.$$

Durch multilineares Ausmultiplizieren ergibt sich

$$\begin{array}{rcl} v_1 \otimes \ldots \otimes v_r & = & \Big(\sum a_j^1 \cdot v_j^1\Big) \otimes \ldots \otimes \Big(\sum a_j^r \cdot v_j^r\Big) \\ & = & \displaystyle\sum_{j_1, \ldots, j_r} (a_{j_1}^1 \cdots a_{j_r}^r) \cdot v_{j_1}^1 \otimes \ldots \otimes v_{j_r}^r \end{array}$$

Um zu sehen, dass $\mathcal{B}$ linear unabhängig ist, betrachten wir zunächst die Dualräume $V_i^* = \operatorname{Hom}(V_i, \mathbb{K})$ und die dualen Basen $\mathcal{B}_i^* = (u_1^i, \ldots, u_{n_i}^i)$ zu den $\mathcal{B}_i = (v_1^i, \ldots, v_{n_i}^i)$. Man hat multilineare Abbildungen

$$\beta_{j_1,\ldots,j_r}\colon V_1 \times \ldots \times V_r \;\to\; \mathbb{K}, \qquad (v_1, \ldots, v_r) \;\mapsto\; u_{j_1}^1(v_{j_1}) \cdots u_{j_r}^r(v_{j_r}).$$

Diese Abbildungen leisten

$$\beta_{j_1,\ldots,j_r}(v_{k_1}^1, \ldots, v_{k_r}^r) \;=\; \begin{cases} 1_{\mathbb{K}} & \text{falls } (j_1, \ldots, j_r) = (k_1, \ldots, k_r), \\ 0_{\mathbb{K}} & \text{falls } (j_1, \ldots, j_r) \ne (k_1, \ldots, k_r). \end{cases}$$

Nach Satz 6.3.9 gibt es lineare Abbildungen

$$\varphi_{j_1,\ldots,j_r} : V_1 \otimes \ldots \otimes V_r \ \to \ \mathbb{K}, \qquad v_1 \otimes \ldots \otimes v_r \ \mapsto \ \beta_{j_1,\ldots,j_r}(v_1,\ldots,v_r).$$

Zum Nachweis der linearen Unabhängigkeit von $\mathcal{B}$ sei eine Darstellung des Nullvektors als Linearkombination gegeben:

$$0 \ = \ \sum_{k_1,\ldots,k_r} a_{k_1,\ldots,k_r} \cdot v^1_{k_1} \otimes \ldots \otimes v^r_{k_r}.$$

Wenden wir die lineare Abbildung $\varphi_{j_1,\ldots,j_r}$ auf diese Gleichung an, so erhalten wir

$$\begin{aligned} 0 \ &= \ \varphi_{j_1,\ldots,j_r} \left(\sum_{k_1,\ldots,k_r} a_{k_1,\ldots,k_r} \cdot v^1_{k_1} \otimes \ldots \otimes v^r_{k_r} \right) \\ &= \ \sum_{k_1,\ldots,k_r} a_{k_1,\ldots,k_r} \varphi_{j_1,\ldots,j_r}(v^1_{k_1} \otimes \ldots \otimes v^r_{k_r}) \\ &= \ a_{j_1,\ldots,j_r}. \end{aligned}$$

□

Aufgaben zu Abschnitt 6.3.

Aufgabe 6.3.13. Es sei $V := \mathbb{R}^2$. Betrachte das Tensorprodukt $V \otimes V$ und den Vektor

$$u \;:=\; (1,1) \otimes (2,3) - (2,1) \otimes (1,-1) \;\in\; V \otimes V$$

Entwickle den Vektor u nach der Basis $(v_1 \otimes w_1, v_1 \otimes w_2, v_2 \otimes w_1, v_2 \otimes w_2)$, wobei

$$v_1 \;:=\; (1,2), \quad v_2 \;:=\; (0,1), \qquad\qquad w_1 \;:=\; (2,1), \quad w_2 \;:=\; (3,1).$$

Aufgabe 6.3.14. Zeige, dass das Element $e_1 \otimes e_2 + e_2 \otimes e_1 \in \mathbb{R}^2 \otimes \mathbb{R}^2$ nicht zerlegbar ist.

Aufgabe 6.3.15. Es sei $V := \mathbb{R}^2$. Bestimme die darstellende Matrix $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ der linearen Abbildung

$$\varphi := \mu_A \otimes \mu_B \colon V \otimes V \;\to\; V \otimes V$$

bezüglich der Basis $\mathcal{B} \;=\; (e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2)$, wobei die Matrizen A und B gegeben seien als

$$A \;:=\; \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}, \qquad\qquad B \;:=\; \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

Aufgabe 6.3.16. Das *Kronecker-Produkt* zweier Matrizen $A \in \mathrm{Mat}(m,n;\mathbb{K})$ und $B \in \mathrm{Mat}(k,l;\mathbb{K})$ ist die Matrix

$$A \otimes B \;:=\; \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix} \;\in\; \mathrm{Mat}(mk, nl; \mathbb{K}).$$

Betrachte die lineare Abbildung $\mu_A \otimes \mu_B \colon V \colon \mathbb{K}^n \otimes \mathbb{K}^l \to \mathbb{K}^m \otimes \mathbb{K}^k$ Zeige: $A \otimes B$ ist die darstellende Matrix der linearen Abbildung bezüglich der Basen

$$(e_i \otimes e_j;\; i = 1, \dots, n,\; j = 1, \dots, l), \qquad (e_\imath \otimes e_\jmath;\; \imath = 1, \dots, m,\; \jmath = 1, \dots, k).$$

Aufgabe 6.3.17. Es seien $\mathbb{K}$ ein Körper und es seien $\mathbb{K}$-Vektorräume U, V, W gegeben. Beweise folgende Aussagen:

(i) Es gilt $V \otimes W \;\cong\; W \otimes V$.
(ii) Es gilt $(U \otimes V) \otimes W \;\cong\; U \otimes (V \otimes W)$.

Aufgabe 6.3.18. Es seien $\mathbb{K}$ ein Körper und V, W zwei $\mathbb{K}$-Vektorräume. Zeige: Es gilt $(V \otimes W)^* \;\cong\; V^* \otimes W^*$.

6.4. **Äußere Potenzen.**

Definition 6.4.1. Es seien $\mathbb{K}$ ein Körper, und V, W zwei $\mathbb{K}$-Vektorräume. Eine multilineare Abbildung $\Phi\colon V^r \to W$ heisst *alternierend*, falls

$$\Phi(v_1,\ldots,v_r) \;=\; 0, \quad \text{sobald } v_i = v_j \text{ mit } 1 \le i < j \le r.$$

Beispiel 6.4.2. Es seien $\mathbb{K}$ ein Körper und $V := \mathbb{K}^n$. Dann liefert die Determinante eine alternierende multilineare Abbildung

$$V^n \;\to\; \mathbb{K}, \qquad (v_1,\ldots,v_n) \;\mapsto\; \det(v_1,\ldots,v_n).$$

Beispiel 6.4.3. Das *Kreuzprodukt* auf $\mathbb{R}^3$ ist definiert eine alternierende bilineare Abbildung

$$\mathbb{R}^3 \times \mathbb{R}^3 \;\to\; \mathbb{R}^3, \qquad (x,y) \;\mapsto\; x \times y \;:=\; \begin{pmatrix} x_2y_3 - y_3x_2 \\ x_3y_1 - x_1y_3 \\ x_1y_2 - x_2y_1 \end{pmatrix}.$$

Bemerkung 6.4.4. Es seien $\mathbb{K}$ ein Körper, und V, W zwei $\mathbb{K}$-Vektorräume. Die Menge $\mathrm{AltLin}(V^r;W)$ der alternierenden multilinearen Abbildungen $V^r \to W$ ist ein Untervektorraum des Vektorraumes $\mathrm{MultLin}(V,\ldots,V;W)$ aller multilinearen Abbildungen $V^r \to W$.

Konstruktion 6.4.5. Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Die r-fache äußere Potenz von V wird in drei Schritten konstruiert:

Schritt 1. Man bildet den freien $\mathbb{K}$-Vektorraum $F(V^r)$ über der Menge V^r, d.h.:

$$F(V^r) \;:=\; \bigoplus_{(v_1,\ldots,v_r)\in V^r} \mathbb{K}\cdot(v_1,\ldots,v_r).$$

Schritt 2. Es sei $R^a(V^r) \le_{\mathbb{K}} F(V^r)$ der Aufspann von allen Elementen der Form

$$\begin{aligned} 1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1},v_i+v_i',v_{i+1},\ldots,v_r) \;&-\; 1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1},v_i,v_{i+1},\ldots,v_r) \\ &-\; 1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1},v_i',v_{i+1},\ldots,v_r), \end{aligned}$$

$$1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1},av_i,v_{i+1},\ldots,v_r) \;-\; a\cdot(v_1,\ldots,v_{i-1},v_i,v_{i+1},\ldots,v_r),$$

$$1_{\mathbb{K}}\cdot(v_1,\ldots,v_{i-1},v,v_{i+1},\ldots,v_{j-1},v,v_{j+1},\ldots,v_r).$$

Schritt 3. Die *r-fache äußere Potenz* von V, auch *r-faches Dachprodukt* genannt, ist der Quotientenvektorraum

$$\bigwedge^r V \;:=\; F(V^r)/R^a(V^r).$$

Für $1_{\mathbb{K}}\cdot(v_1,\ldots,v_r) \in F(V^r)$ bezeichnet $v_1 \wedge \ldots \wedge v_r \in V^r$ die zugehörige Äquivalenzklasse. Die Restklassenabbildung ist dann festgelegt durch

$$\pi^a\colon F(V^r) \;\to\; \bigwedge^r V, \qquad 1_{\mathbb{K}}\cdot(v_1,\ldots,v_r) \;\to\; v_1 \wedge \ldots \wedge v_r$$

Bemerkung 6.4.6. Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Dann gelten folgende Rechenregeln in $\bigwedge^r V$:

$$\begin{aligned}
& v_1\wedge\ldots\wedge v_{i-1}\wedge(v_i+v_i')\wedge v_{i+1}\wedge\ldots\wedge v_r \\
= \;& v_1\wedge\ldots\wedge v_{i-1}\wedge v_i\wedge v_{i+1}\wedge\ldots\wedge v_r \;+\; v_1\wedge\ldots\wedge v_{i-1}\wedge v_i'\wedge v_{i+1}\wedge\ldots\wedge v_r, \\
& v_1\wedge\ldots\wedge v_{i-1}\wedge av_i\wedge v_{i+1}\wedge\ldots\wedge v_r \\
= \;& a\cdot(v_1\wedge\ldots\wedge v_{i-1}\wedge v_i\wedge v_{i+1}\wedge\ldots\wedge v_r), \\
& v_1\wedge\ldots\wedge v_{i-1}\wedge v\wedge v_{i+1}\wedge\ldots\wedge v_{j-1}\wedge v\wedge v_{j+1}\wedge\ldots\wedge v_r \\
= \;& 0 \\
& v_1\wedge\ldots\wedge v_{i-1}\wedge v_j\wedge v_{i+1}\wedge\ldots\wedge v_{j-1}\wedge v_i\wedge v_{j+1}\wedge\ldots\wedge v_r \\
= \;& -(v_1\wedge\ldots\wedge v_{i-1}\wedge v_i\wedge v_{i+1}\wedge\ldots\wedge v_{j-1}\wedge v_j\wedge v_{j+1}\wedge\ldots\wedge v_r).
\end{aligned}$$

Bemerkung 6.4.7. Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Ein Element der Form $v_1\wedge\ldots\wedge v_r\in\bigwedge^r V$ nennt man *zerlegbar*. Es gilt

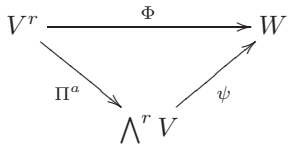
(i) Jedes Element von V^r ist eine (endliche) Summe von zerlegbaren Elementen.
(ii) Im allgemeinen ist nicht jedes Element in $\bigwedge^r V$ zerlegbar; ein Beispiel für ein nicht zerlegbares Element ist

$$e_1\wedge e_2 \;+\; e_3\wedge e_4 \quad\in\quad \mathbb{R}^4\;\wedge\mathbb{R}^4.$$

Satz 6.4.8. *Es seien ein Körper $\mathbb{K}$ und V ein $\mathbb{K}$-Vektorraum. Dann hat man eine kanonische alternierende multilineare Abbildung*

$$\Pi^a\colon V^r \;\to\; \bigwedge^r V, \qquad (v_1,\ldots,v_r) \;\mapsto\; v_1\wedge\ldots\wedge v_r.$$

Zu jeder weiteren alternierenden multilinearen Abbildung $\Phi\colon V^r\to W$ gibt es ein kommutatives Diagramm



mit einer linearen Abbildung $\psi\colon\bigwedge^r V\to W$; diese Abbildung ist eindeutig bestimmt, und sie ist gegeben durch

$$\psi(v_1\wedge\ldots\wedge v_r) \quad=\quad \Phi(v_1,\ldots,v_r).$$

Beweis. Das Vorgehen ist analog zu dem im Beweis von Satz 6.3.9. Zunächst haben wir eine kanonische Abbildung von Mengen

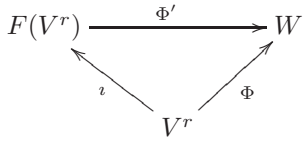
$$\imath\colon V^r \;\to\; F(V^r), \qquad (v_1,\ldots,v_r) \;\mapsto\; 1_{\mathbb{K}}\cdot(v_1,\ldots,v_r).$$

Wir setzen $\Pi^a:=\pi^a\circ\imath$, wobei $\pi^a\colon F(V^r)\to\bigwedge V^r$ die Restklassenabbildung bezeichnet. Nach Konstruktion liegen

$$\begin{gathered}
\imath(*,\ldots,*,v_i+v_i',*,\ldots,*) \;-\; (\imath(*,\ldots,*,v_i,*,\ldots,*) \;+\; \imath(*,\ldots,*,v_i',*,\ldots,*)), \\
\imath(*,\ldots,*,a\cdot v_i,*,\ldots,*) \;-\; a\cdot\imath(*,\ldots,*,v_i',*,\ldots,*), \\
\imath(*,\ldots,*,v,*,\ldots,*,v,*,\ldots,*)
\end{gathered}$$

in $R^a(V^r)$ und werden daher durch π^a auf den Nullvektor abgebildet. Mit der Linearität von π^a ergibt sich, dass Π^a alternierend und multilinear ist.

Es sei nun $\Phi\colon V^r \to W$ eine alternierende multilineare Abbildung. Dann erhalten wir zunächst ein kommutatives Diagramm



indem wir eine lineare Abbildung $\Phi'\colon F(V^r) \to W$ durch Vorgabe von Werten auf einer Basis definieren:

$$\Phi'(1_{\mathbb{K}}\cdot(v_1,\ldots,v_r)) \quad := \quad \Phi(v_1,\ldots,v_r).$$

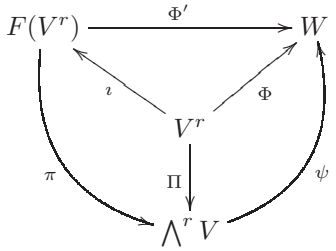
Dann stellen wir fest, das der Untervektorraum $R^a(V^r) \leq_{\mathbb{K}} F(V^r)$ in $\mathrm{Kern}(\Phi')$ enthalten ist: Es gilt

$$\begin{aligned}
& \Phi'(1_{\mathbb{K}}\cdot(*,\ldots,*,v_i+v_i',*,\ldots,*) \;-\; 1_{\mathbb{K}}\cdot(*,\ldots,*,v_i,*,\ldots,*) \;-\; 1_{\mathbb{K}}\cdot(*,\ldots,*,v_i',*,\ldots,*)),\\
= \;& \Phi'(\imath(*,\ldots,*,v_i+v_i',*,\ldots,*)) \;-\; \Phi'(\imath(*,\ldots,*,v_i,*,\ldots,*)) \;-\; \Phi'(\imath(*,\ldots,*,v_i',*,\ldots,*))\\
= \;& \Phi(*,\ldots,*,v_i+v_i',*,\ldots,*) \;-\; \Phi(*,\ldots,*,v_i,*,\ldots,*) \;-\; \Phi(*,\ldots,*,v_i',*,\ldots,*)\\
= \;& \Phi(*,\ldots,*,0_V,*,\ldots,*)\\
= \;& 0_W.
\end{aligned}$$

$$\begin{aligned}
& \Phi'(1_{\mathbb{K}}\cdot(*,\ldots,*,av_i*,\ldots,*) \;-\; a\cdot(*,\ldots,*,v_i,*,\ldots,*))\\
= \;& \Phi'(\imath(*,\ldots,*,av_i*,\ldots,*)) \;-\; \Phi'(\imath(a\cdot(*,\ldots,*,v_i,*,\ldots,*)))\\
= \;& \Phi(*,\ldots,*,av_i*,\ldots,*) \;-\; \Phi(a\cdot(*,\ldots,*,v_i,*,\ldots,*))\\
= \;& \Phi(*,\ldots,*,0_V,*,\ldots,*)\\
= \;& 0_W.
\end{aligned}$$

$$\begin{aligned}
& \Phi'(1_{\mathbb{K}}\cdot(*,\ldots,*,v,*,\ldots,*,v,*,\ldots,*))\\
= \;& \Phi'(\imath(*,\ldots,*,v,*,\ldots,*,v,*,\ldots,*))\\
= \;& \Phi(*,\ldots,*,v,*,\ldots,*,v,*,\ldots,*)\\
= \;& 0_W.
\end{aligned}$$

Wegen $R^a(V^r) \subseteq \mathrm{Kern}(\pi^a)$ liefert uns der Homomorphiesatz eine lineare Abbildung $\psi\colon V^r \to W$ mit der das Diagramm



kommutativ wird. Die Eindeutigkeit von ψ ergibt sich sofort aus der Tatsache, dass $\bigwedge^r V$ durch die Elemente aus $\Pi^a(V_1 \times \ldots \times V_r)$ erzeugt wird. $\square$

Folgerung 6.4.9. *Es seien ein Körper $\mathbb{K}$ und V ein $\mathbb{K}$-Vektorraum. Dann hat man ein kommutatives Diagramm*

$$\begin{array}{ccc} V^r & \xrightarrow{\quad\Pi^a\quad} & \bigwedge^r V \\ & {\scriptstyle\Pi}\searrow \quad \nearrow{\scriptstyle\psi} & \\ & \bigotimes^r V & \end{array}$$

mit einer linearen Abbildung $\psi\colon \bigotimes^r V \to \bigwedge^r$; diese Abbildung ist eindeutig bestimmt, und sie ist gegeben durch stets

$$\psi(v_1 \otimes \ldots \otimes v_r) \quad = \quad v_1 \wedge \ldots \wedge v_r.$$

Folgerung 6.4.10. *Es seien $\mathbb{K}$ ein Körper und V sowie W Vektorräume über $\mathbb{K}$. Dann hat man zu einander inverse Isomorphismen von $\mathbb{K}$-Vektorräumen*

$$\begin{array}{rcl} \mathrm{AltLin}(V^r; W) & \longleftrightarrow & \mathrm{Hom}(\bigwedge^r V, W) \\ \varphi & \mapsto & [v_1 \wedge \ldots \wedge v_r \mapsto \varphi(v_1, \ldots, v_r)] \\ [(v_1, \ldots, v_r) \mapsto \psi(v_1 \wedge \ldots \wedge v_r)] & \mapsfrom & \psi \end{array}$$

Folgerung 6.4.11. *Es seien $\mathbb{K}$ ein Körper und $\varphi\colon V \to W$ eine lineare Abbildungen von $\mathbb{K}$-Vektorräumen. Dann hat man ein kommutatives Diagramm*

$$\begin{array}{ccc} V^r & \xrightarrow[\varphi\times\ldots\times\varphi]{(v_1,\ldots,v_r)\mapsto(\varphi(v_1),\ldots,\varphi(v_r))} & W^r \\ {\scriptstyle\Pi_V^a}\downarrow & & \downarrow{\scriptstyle\Pi_W^a} \\ \bigwedge^r V & \xrightarrow[v_1\wedge\ldots\wedge v_r\mapsto\varphi(v_1)\wedge\ldots\wedge\varphi(v_r)]{\varphi\wedge\ldots\wedge\varphi} & \bigwedge^r W \end{array}$$

mit den kanonischen Abbildungen Π_V^a, Π_W^a und einer eindeutig bestimmten linearen Abbildung $\varphi \wedge \ldots \wedge \varphi\colon \bigwedge^r V \to \bigwedge^r W$.

Lemma 6.4.12. *Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum mit einer Basis $(v_1, \ldots, v_n)$, und es sei $(v_1^*, \ldots, v_n^*)$ die duale Basis in $V^* = \mathrm{Hom}(V, \mathbb{K})$. Dann ist*

$$\beta_{i_1,\ldots,i_r}\colon V^r \to \mathbb{K}, \qquad (w_1, \ldots, w_r) \mapsto \sum_{\sigma\in S_r} \mathrm{sg}(\sigma) v_{i_{\sigma(1)}}^*(w_1) \cdots v_{i_{\sigma(r)}}^*(w_r)$$

für jedes Tupel $1 \le i_1 < \ldots < i_r \le n$ eine alternierende multilineare Abbildung. Für jedes weitere Tupel $1 \le j_1 < \ldots < j_r \le n$ gilt

$$\beta_{i_1,\ldots,i_r}(v_{j_1}, \ldots, v_{j_r}) \quad = \quad \begin{cases} 1_{\mathbb{K}} & \textit{falls } (j_1, \ldots, j_r) = (i_1, \ldots, i_r), \\ 0_{\mathbb{K}} & \textit{falls } (j_1, \ldots, j_r) \ne (i_1, \ldots, i_r). \end{cases}$$

Beweis. Als Summe von multilinearen Abbildungen ist $\beta_{i_1,\ldots,i_r}$ wieder multilinear. Weiter erhalten wir

$$\begin{array}{rcl} \beta_{i_1,\ldots,i_r}(v_{j_1}, \ldots, v_{j_r}) & = & v_{i_1}^*(v_{j_1}) \cdots v_{i_r}^*(v_{j_r}) \\ & & \quad + \sum_{\mathrm{id}\ne\sigma\in S_r} \mathrm{sg}(\sigma) v_{i_{\sigma(1)}}^*(v_{j_1}) \cdots v_{i_{\sigma(r)}}^*(v_{j_r}) \\ & = & v_{i_1}^*(v_{j_1}) \cdots v_{i_r}^*(v_{j_r}) \\ & = & \begin{cases} 1_{\mathbb{K}} & \text{falls } (j_1, \ldots, j_r) = (i_1, \ldots, i_r), \\ 0_{\mathbb{K}} & \text{falls } (j_1, \ldots, j_r) \ne (i_1, \ldots, i_r). \end{cases} \end{array}$$

Hierbei gilt $v_{i_{\sigma(1)}}^*(v_{j_1}) \cdots v_{i_{\sigma(r)}}^*(v_{j_r}) = 0_{\mathbb{K}}$ sobald $\sigma \ne \mathrm{id}$, weil $i_{\sigma(1)}, \ldots, i_{\sigma(r)}$ in diesem Fall nicht strikt aufsteigend und somit von $(j_1, \ldots, j_r)$ verschieden ist.

Es bleibt zu zeigen, dass $\beta_{i_1,\ldots,i_r}$ alternierend ist. Dazu sei $(w_1,\ldots,w_r)\in V^r$ gegeben mit $w_i=w_j$ für $i\neq j$. Die Transposition $\tau=(i,j)\in S_r$ liefert eine Zerlegung

$$S_r \;=\; A_r \cup A_r\circ\tau$$

in disjunkte Teilmengen, wobei $A_r=\operatorname{Kern}(\mathrm{sg})\subseteq S_r$ die alternierende Gruppe bezeichnet, siehe [1, Satz 6.1.8]. Damit ergibt sich

$$\begin{aligned}\beta_{i_1,\ldots,i_r}(w_1,\ldots,w_r) &= \sum_{\sigma\in S_r}\operatorname{sg}(\sigma)v^*_{i_{\sigma(1)}}(w_1)\cdots v^*_{i_{\sigma(r)}}(w_r)\\ &= \sum_{\sigma\in A_r} v^*_{i_{\sigma(1)}}(w_1)\cdots v^*_{i_{\sigma(r)}}(w_r)\\ &\quad - \sum_{\sigma\in A_r\circ\tau} v^*_{i_{\sigma(1)}}(w_1)\cdots v^*_{i_{\sigma(r)}}(w_r)\\ &= 0_{\mathbb{K}}.\end{aligned}$$

□

Satz 6.4.13. *Es seien $\mathbb{K}$ ein Körper, V ein Vektorraum mit Basis $(v_1,\ldots,v_n)$ und $1\leq r\leq n$ gegeben. Dann ist*

$$\mathcal{C} \;=\; (v_{i_1}\wedge\ldots\wedge v_{i_r};\ 1\leq i_1<\ldots<i_r\leq n).$$

eine Basis für die r-fache äußere Potenz $\bigwedge^r V$. Insbesondere ist dessen Dimension gegeben durch

$$\dim\left(\bigwedge^r V\right) \;=\; \binom{n}{r} \;=\; \frac{n!}{r!(n-r)!}.$$

Beweis. Um zu sehen, dass $\mathcal{C}$ ein Erzeugendensystem ist, genügt es zu zeigen, dass man jedes Element $w_1\wedge\ldots\wedge w_r$ mit $w_i\in V$ als Linearkombination über den $v_{i_1}\wedge\ldots\wedge v_{j_r}$ erhält. Dazu betrachten wir die Entwicklungen $w_i=a^i_1\cdot v_1+\ldots+a^i_n\cdot v_n$. Multilineares Ausmultiplizieren liefert zunächst

$$\begin{aligned}w_1\wedge\ldots\wedge w_r &= \left(\sum a^1_j\cdot v_j\right)\wedge\ldots\wedge\left(\sum a^r_j\cdot v_j\right)\\ &= \sum_{j_1,\ldots,j_r}(a^1_{j_1}\cdots a^r_{j_r})\cdot v_{j_1}\wedge\ldots\wedge v_{j_r}\end{aligned}$$

Hier können auch nicht streng aufsteigende Indextupel $j_1,\ldots,j_r$ vorkommen. Gilt dabei $j_k=j_{k+1}$ für ein k, so verschwindet $v_{j_1}\wedge\ldots\wedge v_{j_r}$. Andernfalls ordnen wir $j_1,\ldots,j_r$ steng aufsteigend um zu $l_1,\ldots,l_r$ und haben dann

$$v_{j_1}\wedge\ldots\wedge v_{j_r} \;=\; \pm 1_{\mathbb{K}} v_{l_1}\wedge\ldots\wedge v_{l_r}$$

Nun können wir die Terme mit in der obigen Gleichung nach $v_{l_1}\wedge\ldots\wedge v_{l_r}$ mit sreng aufsteigenden Indextupel $l_1,\ldots,l_r$ zusammenfassen und erhalten so die gewünschte Darstellung.

Um zu sehen, dass die Familie $\mathcal{C}$ linear unabhängig ist, arbeiten wir mit den Linearformen

$$\beta_{i_1,\ldots,i_r}\colon V^r\to\mathbb{K},\qquad (w_1,\ldots,w_r)\mapsto\sum_{\sigma\in S_r}\operatorname{sg}(\sigma)v^*_{i_{\sigma(1)}}(w_1)\cdots v^*_{i_{\sigma(r)}}(w_r)$$

aus Lemma 6.4.12. Satz 6.4.8 liefert uns dann zu jedem $\beta_{i_1,\ldots,i_r}$ eine lineare Abbildung

$$\varphi_{i_1,\ldots,i_r}\colon \bigwedge^r V \;\to\; \mathbb{K},\qquad w_1\wedge\ldots\wedge w_r \;\mapsto\; \beta_{i_1,\ldots,i_r}(w_1,\ldots,w_r).$$

Es sei nun eine Darstellung des Nullvektors als Linearkombination über der Familie $\mathcal{C}$ gegeben:

$$0 \quad = \quad \sum_{k_1,\ldots,k_r} a_{k_1,\ldots,k_r} \cdot v_{k_1} \wedge \ldots \wedge v_{k_r}.$$

Wenden wir die lineare Abbildung $\varphi_{i_1,\ldots,i_r} \colon \bigwedge^r V \to \mathbb{K}$ auf diese Gleichung an, so erhalten wir

$$\begin{aligned} 0 &= \varphi_{i_1,\ldots,i_r}\left(\sum_{k_1,\ldots,k_r} a_{k_1,\ldots,k_r} \cdot v_{k_1} \wedge \ldots \wedge v_{k_r}\right) \\ &= \sum_{k_1,\ldots,k_r} a_{k_1,\ldots,k_r} \varphi_{i_1,\ldots,i_r}(v_{k_1} \wedge \ldots \wedge v_{k_r}) \\ &= a_{i_1,\ldots,i_r}. \end{aligned}$$

□

Aufgaben zu Abschnitt 6.4.

Aufgabe 6.4.14. Zeige: Das Element $e_1 \wedge e_2 \ + \ e_3 \wedge e_4 \in \mathbb{R}^4 \wedge \mathbb{R}^4$ ist nicht zerlegbar. *Hinweis* Sonst hätte man $e_1 \wedge e_2 \ + \ e_3 \wedge e_4 = u \wedge v$ mit Vektoren $u, v \in \mathbb{R}^4$. Schreibe nun $u = u_1 \cdot e_1 + \ldots + u_4 \cdot e_4$ und verwende $u \wedge u \wedge v = 0$.

Aufgabe 6.4.15. Es seien $\mathbb{K}$ ein Körper, V ein $\mathbb{K}$-Vektorraum und $v_1, \ldots, v_k \in V$. Beweise die Äquivalenz folgender Aussagen:

(i) Die Familie $(v_1, \ldots, v_k)$ ist linear abhängig.
(ii) Es gilt $v_1 \wedge \ldots \wedge v_k = 0$.

Aufgabe 6.4.16. Es seien $\mathbb{K}$ ein Körper und $v_1, \ldots, v_n \in \mathbb{K}^n$. Zeige: Es gilt

$$v_1 \wedge \ldots \wedge v_n \quad = \quad \det(v_1, \ldots, v_n) \cdot e_1 \wedge \ldots \wedge e_n.$$

Aufgabe 6.4.17. Es sei $V := \mathbb{R}^3$. Bestimme die darstellende Matrix $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ der linearen Abbildung

$$\varphi := \mu_A \wedge \mu_A \colon V \wedge V \ \to \ V \wedge V$$

bezüglich der Basis $\mathcal{B} \ = \ (e_1 \wedge e_2, \, e_1 \wedge e_3, \, e_2 \wedge e_3)$, wobei die Matrix A gegeben sei als

$$A \quad := \quad \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & 1 \\ -1 & 0 & 2 \end{pmatrix}.$$

7. Gruppenoperationen und Darstellungen

7.1. **Gruppenoperationen.**

Beispiel 7.1.1. Es sei $\mathbb{K}$ ein Körper. Die Gruppe $\mathrm{GL}(n,\mathbb{K})$ der invertierbaren $(n\times n)$-Matrizen "operiert" auf $\mathbb{K}^n$ durch Matrix-Vektor-Multiplikation

$$\mathrm{GL}(n,\mathbb{K})\times\mathbb{K}^n \;\to\; \mathbb{K}^n, \qquad (A,x) \;\mapsto\; A\cdot x.$$

Für jedes $x\in\mathbb{K}^n$ gilt dabei $E_n\cdot x = x$, und für je zwei Matrizen $A,B\in\mathrm{GL}(n;\mathbb{K})$ hat man $A\cdot(B\cdot x)=(AB)\cdot x$.

Definition 7.1.2. Es seien G eine Gruppe und X eine Menge. Eine *Operation* (auch *Wirkung*) von G auf X ist eine Abbildung

$$\mu\colon G\times X \;\to\; X, \qquad (g,x) \;\mapsto\; \mu(g,x) =: g\cdot x$$

mit folgenden Eigenschaften: Für jedes Element $x\in X$ und je zwei Gruppenelemente $g_1,g_2\in G$ gilt

$$e_G\cdot x \;=\; x, \qquad\qquad g_2\cdot(g_1\cdot x) \;=\; (g_2g_1)\cdot x.$$

Beispiel 7.1.3. Es seien X eine Menge und $S(X)=\{\sigma\colon X\to X;\sigma \text{ ist bijektiv}\}$ die Gruppe der zugehörigen Permutationen. Dann operiert $S(X)$ auf X durch

$$S(X)\times X \;\to\; X, \qquad \sigma\cdot x \;:=\; \sigma(x).$$

Bemerkung 7.1.4. Die Gruppe G operiere auf der Menge X. Dann definiert jedes $g\in G$ eine bijektive Abbildung

$$T_g\colon X \;\to\; X, \qquad x \;\mapsto\; g\cdot x,$$

die *Translation* um g. Die Umkehrabbildung von T_g ist gegeben durch $T_g^{-1}=T_{g^{-1}}$; man hat stets

$$\begin{aligned} T_{g^{-1}}(T_g(x)) \;&=\; g^{-1}\cdot(g\cdot x) \;=\; (g^{-1}g)\cdot x \;=\; e_G\cdot x \;=\; x,\\ T_g(T_{g^{-1}}(x)) \;&=\; g\cdot(g^{-1}\cdot x) \;=\; (gg^{-1})\cdot x \;=\; e_G\cdot x \;=\; x. \end{aligned}$$

Bemerkung 7.1.5. Es sei $\mu\colon G\times X\to X$ eine Operation einer Gruppe G auf einer Menge X.

(i) Ist $H\le G$ eine Untergruppe, so erhält man eine H-Operation auf X durch

$$H\times X \;\to\; X, \qquad (h,x) \;\mapsto\; \mu(h,x).$$

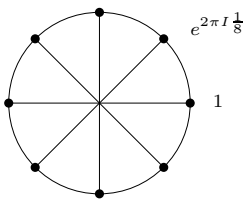
(ii) Ist G' eine Gruppe und $\varphi\colon G'\to G$ ein Gruppenhomomorphismus, so erhält man eine G'-Operation auf X durch

$$G'\times X \;\to\; X, \qquad (g',x) \;\mapsto\; g'\cdot x := \varphi(g')\cdot x.$$

Beispiel 7.1.6 (Einheitswurzeln)**.** Es sei $n\in\mathbb{Z}_{\ge 1}$. Die Gruppe der n-ten komplexen Einheitswurzeln ist die Untergruppe

$$\mathrm{EW}_n \;:=\; \{\zeta\in\mathbb{C}^*;\ \zeta^n=1\} \;=\; \left\{e^{2\pi I\frac{k}{n}};\ k=0,\dots,n-1\right\} \;\le\; \mathbb{C}^*.$$

Die Elemente von EW_n bilden die Eckpunkte eines regelmäßigen n-Ecks in der komplexen Ebene; hier der Fall $n=8$:



Die Abbildung $\mathbb{Z} \to \mathrm{EW}_n$, $k \mapsto e^{2\pi I \frac{k}{n}}$ ist ein surjektiver Gruppenhomomorphismus mit Kern $n\mathbb{Z}$. Der Homomorphiesatz liefert somit einen Gruppenisomorphismus

$$\mathbb{Z}/n\mathbb{Z} \;\to\; \mathrm{EW}_n, \qquad \overline{k} \;\mapsto\; e^{2\pi I \frac{k}{n}}.$$

Als Untergruppe von $\mathbb{C}^*$ operiert EW_n durch Multiplikation auf $\mathbb{C}$. Somit haben wir eine Operation von $\mathbb{Z}/n\mathbb{Z}$ auf $\mathbb{C}$:

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{C} \;\to\; \mathbb{C}, \qquad \overline{k} \cdot z \;:=\; e^{2\pi I \frac{k}{n}} z.$$

Weiter definiert jedes $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ einen Gruppenhomomorphismus $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\overline{k} \mapsto \overline{m}\overline{k}$. Damit erhält man neue Operationen

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{C} \;\to\; \mathbb{C}, \qquad \overline{k} \cdot z \;:= e^{2\pi I \frac{mk}{n}} z.$$

Die Abbildung $T_{\overline{k}} \colon \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{k} \cdot z$ ist dabei gerade die Drehung um den Winkel $2\pi mk/n$.

Definition 7.1.7. Es seien G eine Gruppe, X eine Menge und $\mu \colon G \times X \to X$ eine Operation von G auf X.

(i) Die *Bahn* eines Punktes $x \in X$ ist $G \cdot x := \{g \cdot x;\ g \in G\}$
(ii) Ein Punkt $x \in X$ heisst *Fixpunkt*, falls $G \cdot x = \{x\}$ gilt.
(iii) Die *Fixpunktmenge* der Operation ist $X^G := \{x \in X;\ x \text{ ist Fixpunkt}\}$.
(iv) Die *Isotropiegruppe* eines Punktes $x \in X$ ist $G_x := \{g \in G;\ g \cdot x = x\}$.

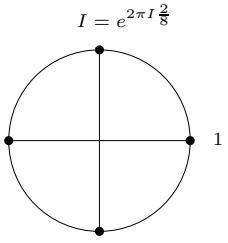
Bemerkung 7.1.8. Es seien G eine Gruppe, X eine Menge und $\mu \colon G \times X \to X$ eine Operation von G auf X.

(i) Für jedes $x \in X$ ist G_x eine Untergruppe von G.
(ii) Ein Element $x \in X$ ist genau dann ein Fixpunkt, wenn $G_x = G$ gilt.

Beispiel 7.1.9. Wir betrachten wieder die Gruppe $\mathbb{Z}/8\mathbb{Z}$ und ihre Operation auf $\mathbb{C}$ gegeben durch

$$\overline{k} \cdot z \quad := \quad e^{2\pi I k \frac{2}{8}} z.$$

Dann ist $0 \in \mathbb{C}$ ein Fixpunkt dieser Operation. Die Bahn von $1 \in \mathbb{C}$ ist gegeben als $\{\overline{k} \cdot 1;\ k = 0, \ldots, 7\}$ und besteht genau aus den vierten Einheitswurzeln.



Die Isotropiegruppe des Punktes 0 ist $\mathbb{Z}/8\mathbb{Z}$ und die Isotropiegruppe von $1 \in \mathbb{C}$ ist gegeben durch

$$\{\overline{k} \in \mathbb{Z}/8\mathbb{Z};\ \overline{k} \cdot 1 = 1\} \quad = \quad \{\overline{0}, \overline{4}\}.$$

Erinnerung 7.1.10. Es seien G eine Gruppe und $H \leq G$ eine Untergruppe.

(i) Die *Nebenklasse* von $g \in G$ bezüglich H ist $gH = \{gh;\ h \in H\}$.
(ii) Der zu $H \leq G$ gehörige *homogene Raum* ist $G/H = \{gH;\ g \in G\}$.
(iii) Der *Index* von $H \in G$ ist $[G : H] := |G/H|$.
(iv) Der Satz von Lagrange besagt $|G| = [G : H]|H|$.

Satz 7.1.11. *Die Gruppe G operiere auf der Menge X. Weiter seien $g \in G$ und $x \in X$ gegeben.*

(i) *Für die Isotropiegruppe von $g \cdot x$ gilt $G_{g\cdot x} = gG_xg^{-1}$.*
(ii) *Man hat eine bijektive Abbildung $\beta_x \colon G/G_x \to G \cdot x$, $gG_x \mapsto g \cdot x$.*
(iii) *Es gelten $|G \cdot x| = [G : G_x]$ und $|G| = |G \cdot x| \cdot |G_x|$.*

Beweis. Wir verifizieren (i). Für jedes Element $h \in G$ ist Mitgliedschaft in $G_{g\cdot x}$ charakterisiert durch

$$h \cdot (g \cdot x) = g \cdot x \;\Leftrightarrow\; g^{-1}hg \cdot x = x \;\Leftrightarrow\; g^{-1}hg \in G_x \;\Leftrightarrow\; h \in gG_xg^{-1}.$$

Zu (ii). Die Abbildung β_x ist offensichtlich wohldefiniert und surjektiv. Zur Injektivität: Es gilt

$$\beta_x(gG_x) = \beta_x(hG_x) \;\Rightarrow\; g \cdot x = h \cdot x \;\Rightarrow\; h^{-1}g \in G_x \;\Rightarrow\; gG_x = hG_x.$$

Zu (iii). Nach Definition haben wir $[G : G_x] = |G/G_x|$. Die Aussagen ergeben sich somit aus (ii) und dem Satz von Lagrange. □

Definition 7.1.12. Es seien G eine Gruppe, X eine Menge und $\mu \colon G \times X \to X$ eine Operation von G auf X.

(i) Das *Translat* einer Teilmenge $Y \subseteq X$ um $g \in G$ ist $g \cdot Y := \{g \cdot y;\ y \in Y\}$
(ii) Eine Teilmenge $Y \subseteq X$ heisst *invariant*, falls $g \cdot Y = Y$ für alle $g \in G$ gilt.
(iii) Der *Stabilisator* einer Teilmenge $Y \subseteq X$ ist $G_Y := \{g \in G;\ g \cdot Y = Y\}$

Bemerkung 7.1.13. Es seien G eine Gruppe, X eine Menge, $\mu \colon G \times X \to X$ eine Operation von G auf X und $Y \subseteq X$.

(i) Es gilt $G_Y \leq G$ und man hat eine Operation $G_Y \times Y \to Y$, $g \cdot y = \mu(g, y)$.
(ii) Die Teilmenge $Y \subseteq X$ ist genau dann invariant, wenn $G_Y = G$ gilt.

Erinnerung 7.1.14. Auf dem reelle Vektorraum $\mathbb{R}^n$ wird ein euklidischer Vektorraum, indem wir ihn mit dem Standardskalarprodukt versehen:

$$\langle x, y\rangle \;:=\; x_1y_1 + \ldots + x_ny_n.$$

Man nennt $A \in \mathrm{Mat}(n, n; \mathbb{R})$ *orthogonal*, falls A invertierbar ist mit $A^{-1} = A^t$. Für jede Matrix $A \in \mathrm{Mat}(n, n; \mathbb{R})$ sind folgende Aussagen äquivalent:

(i) A ist orthogonal.
(ii) $\mu_A \colon \mathbb{R}^n \to \mathbb{R}^n$ ist eine *Isometrie*, d.h., man hat stets $\langle A \cdot x, A \cdot y\rangle = \langle x, y\rangle$.
(iii) Die Spalten von A bilden eine Orthonormalbasis für $\mathbb{R}^n$.
(iv) Die Zeilen von A bilden eine Orthonormalbasis für $\mathbb{R}^n$.

Bemerkung 7.1.15. Die Menge aller orthogonalen $(n \times n)$-Matrizen ist eine Untergruppe der allgemeinen linearen Gruppe, die *orthogonale Gruppe*:

$$O(n) \;:=\; \{A \in \mathrm{GL}(n, \mathbb{R});\ A \text{ is orthogonal }\} \;\leq\; \mathrm{GL}(n, \mathbb{R}).$$

Offenbar haben wir $O(n) \subseteq \mathrm{GL}(n, \mathbb{R})$ und $E_m \in O(n)$. Die Charakterisierungen aus Erinnerung 7.1.14 liefern uns

$$A \in O(n) \;\Longrightarrow\; A^{-1} = A^t \in O(n)$$

Sind zwei Matrizen $A, B \in O(n)$ gegeben, so ist AB invertierbar und wir erhalten $AB \in O(n)$ mit

$$(A \cdot B)^{-1} \;=\; B^{-1} \cdot A^{-1} \;=\; B^t \cdot A^t \;=\; (A \cdot B)^t.$$

Beispiel 7.1.16. Die orthogonale Gruppe $O(2) \leq \mathrm{GL}(2, \mathbb{R})$ ist explizit gegeben durch:

$$O(2) \;=\; \left\{ \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix};\ 0 \leq \alpha < 2\pi \right\} \cup \left\{ \begin{pmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{pmatrix};\ 0 \leq \alpha < 2\pi \right\}.$$

Definition 7.1.17. Wir versehen $\mathbb{R}^n$ mit dem Standardskalarprodukt $\langle\ ,\ \rangle$. Die *Einheitssphäre* in $\mathbb{R}^n$ ist

$$S^{n-1} \ := \ \{x \in \mathbb{R}^n;\ \langle x, x\rangle = 1\} \ = \ \{x \in \mathbb{R}^n;\ x_1^2 + \ldots + x_n^2 = 1\}$$

Satz 7.1.18. *Die Gruppe* $\mathrm{GL}(n, \mathbb{R})$ *operiere durch Matrix-Vektor-Multiplikation auf* $\mathbb{R}^n$*. Dann ist* $O(n)$ *der Stabilisator der Einheitssphäre* $S^{n-1} \subset \mathbb{R}^n$*.*

Beweis. Nach 7.1.15 definiert jedes $A \in O(n)$ eine Isometrie; insbesondere überführt es Elemente von S^{n-1} in Elemente von S^{n-1} und gehört daher zum Stabilisator von S^{n-1}.

Ist umgekehrt ein $A \in \mathrm{GL}(n, \mathbb{R})$ ein Element des Stabilisators von S^{n-1}, so erhalten wir für jedes vom Nullvektor verschiedene Element $v \in \mathbb{R}^n$:

$$\langle A \cdot v, A \cdot v\rangle = \|v\|^2 \left\langle A \cdot \frac{1}{\|v\|} \cdot v, A \cdot \frac{1}{\|v\|} \cdot v \right\rangle = \|v\|^2 = \langle v, v\rangle.$$

Damit können wir zeigen, dass die Abbildung μ_A eine Isometrie ist. Für je zwei $x, y \in \mathbb{R}^n$ erhalten wir

$$\begin{aligned}
\langle A \cdot x, A \cdot y\rangle &= \frac{1}{2}\left(\langle A \cdot x + A \cdot y, A \cdot x + A \cdot y\rangle - \langle A \cdot x, A \cdot x\rangle - \langle A \cdot y, A \cdot y\rangle\right) \\
&= \frac{1}{2}\left(\langle x + y, x + y\rangle - \langle x, x\rangle - \langle y, y\rangle\right) \\
&= \langle x, y\rangle
\end{aligned}$$

□

Aufgaben zu Abschnitt 7.1.

Aufgabe 7.1.19. Es sei G eine Gruppe. Beweise die folgenden Aussagen:

(i) Die Gruppe G operiert auf sich selbst durch $G \times G \to G$, $(g,h) \mapsto gh$.
(ii) Man hat einen injektiven Gruppenhomomorphismus $\varphi\colon G \to S(G)$, $g \mapsto T_g$.
(iii) Jede Gruppe der Ordung n ist isomorph zu einer Untergruppe von $S_{n!}$.

Aufgabe 7.1.20. Zeige: Die Gruppe $O(n) \leq \mathrm{GL}(n,\mathbb{R})$ orthogonalen $(n \times n)$-Matrizen operiert transitiv auf der Einheitssphäre S^{n-1}, d.h., zu je zwei $x, y \in S^{n-1}$ gibt es eine orthogonale Matrix A mit $y = A \cdot x$.

Aufgabe 7.1.21. Betrachte die Menge der Eckpunkte des folgenden regelmäßigen n-Ecks in $\mathbb{R}^2$:

$$Y \;=\; \left\{(1,0),\; \left(\cos\left(\tfrac{2\pi}{n}\right), \sin\left(\tfrac{2\pi}{n}\right)\right),\; \ldots,\; \left(\cos\left(\tfrac{2\pi(n-1)}{n}\right), \sin\left(\tfrac{2\pi(n-1)}{n}\right)\right)\right\} \;\subseteq\; S^1.$$

Zeige: Der Stabilisator der Teilmenge $Y \subseteq S^1$ unter der Operation von $O(2)$ auf S^1 ist gegeben durch

$$O(2)_Y \quad = \quad \{d_n^0, \ldots, d_n^{n-1}\} \;\cup\; \{d_n^0 \cdot s, \ldots, d_n^{n-1} \cdot s\},$$

wobei die Matrix d_n die Drehung um den Winkel $2\pi/n$ darstellt und s die Spiegelung an der x_1-Achse, d.h., wir haben

$$d_n^k \;:=\; \begin{pmatrix} \cos\left(\frac{2\pi k}{n}\right) & -\sin\left(\frac{2\pi k}{n}\right) \\ \sin\left(\frac{2\pi k}{n}\right) & \cos\left(\frac{2\pi k}{n}\right) \end{pmatrix}, \qquad s \;:=\; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

7.2. **Konjugationsklassen.**

Definition 7.2.1. Die Gruppe G operiere auf der Menge X. Der *Bahnenraum* ist die Menge aller G-Bahnen in X, in Zeichen $X/G := \{G \cdot x;\ x \in X\}$.

Beispiel 7.2.2. Es seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann operiert H auf G durch

$$H \times G \ \to\ G, \qquad h \cdot g \ :=\ gh^{-1}.$$

Die Bahnen dieser Operation sind genau die Nebenklassen gH und der Bahnenraum ist der homogene Raum G/H.

Satz 7.2.3. *Die Gruppe G operiere auf der Menge X. Dann hat man eine Äquivalenzrelation auf X:*

$$x_1 \ \sim_G\ x_2 \quad :\Longleftrightarrow \quad x_2 \ =\ g \cdot x_1 \text{ mit einem } g \in G.$$

Die zugehörigen Äquivalenzklassen sind genau die G-Bahnen in X. Insbesondere erhält man eine disjunkte Zerlegung von X in G-Bahnen

$$X \ =\ \bigsqcup_{G\cdot x \in X/G} G \cdot x \ =\ \bigsqcup_{i\in I} G \cdot x_i,$$

die Bahnzerlegung*, wobei $\{x_i;\ i \in I\}$ ein vollständiges Repräsentantensystem der Äquivalenzrelation "$\sim_G$" bezeichnet.*

Beweis. Die Relation "$\sim_G$" ist reflexiv, da stets $x = e_G \cdot x$ gilt. Weiter ist "$\sim_G$" symmetrisch, denn wir haben stets

$$x_2 \ =\ g \cdot x_1 \quad \Longleftrightarrow \quad x_1 \ =\ g^{-1} \cdot x_2.$$

Zum Nachweis der Transitivität, seien $x_1 \sim_G x_2$ und $x_2 \sim_G x_3$. Dann gibt es $g, h \in G$ mit $x_2 = h \cdot x_1$ und $x_3 = g \cdot x_2$. Es folgt $x_3 = (gh) \cdot x_1$ und somit $x_1 \sim_G x_3$.

Nach Definition sind die Äquivalenzklassen von "$\sim_G$" genau die G-Bahnen in X. Damit erhält man die disjunkte Zerlegung von X in G-Bahnen. □

Satz 7.2.4 (Bahnengleichung)**.** *Es sei $G \times X \to X$ eine Operation einer Gruppe G auf einer Menge X, und es sei $\{x_i; i \in I\}$ ein vollständiges Repräsentantensystem für "$\sim_G$". Dann gilt*

$$|X| \ =\ \sum_{i\in I} |G \cdot x_i| \ =\ \sum_{i\in I} [G : G_{x_i}].$$

Beweis. Nach Satz 7.2.3 ist X die disjunkte Vereinigung aller G-Bahnen in X, d.h., es gilt

$$X \quad =\quad \bigsqcup_{i\in I} G \cdot x_i.$$

Das beweist die erste Gleichung. Nach Satz 7.1.11 (ii) gilt $|G \cdot x_i| = [G : G_{x_i}]$ für jedes $i \in I$. Das beweist die zweite Gleichung. □

Bemerkung 7.2.5. Es sei G eine Gruppe. Dann operiert G auf sich selbst vermöge *Konjugation*:

$$G \times G \ \to\ G, \qquad (g, h) \ \mapsto\ g \cdot h \ :=\ ghg^{-1}.$$

Die Bahnen dieser Operation nennt man auch die *Konjugationsklassen* von G; sie sind für gegebenes $h \in G$ von der Form

$$G \cdot h \quad =\quad \{ghg^{-1};\ g \in G\}.$$

Beispiel 7.2.6. Wir betrachten $G = \mathrm{GL}(2, \mathbb{C})$. Nach dem Satz über die Jordansche Normalform erhält man alle Konjugationsklassen $\{SAS^{-1};\ S \in G\}$ mit den Matrizen A der Gestalt

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \quad \lambda_1, \lambda_2 \in \mathbb{C}^*, \qquad \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}, \quad \lambda \in \mathbb{C}^*.$$

Definition 7.2.7. Es sei G eine Gruppe. Der *Zentralisator* Z_h eines Elements $h \in G$ und das *Zentrum* Z_G von G sind definiert als

$$Z_h \ := \ \{g \in G;\ gh = hg\}, \qquad Z_G \ := \ \{g \in G;\ gh = hg \text{ für alle } h \in G\}.$$

Bemerkung 7.2.8. Es sei G eine Gruppe. Dann ist jeder Zentralisator Z_h, wobei $h \in G$, eine Untergruppe von G. Weiter ist das Zentrum Z_G eine abelsche Untergruppe von G und es gilt

$$Z_G \ = \ \bigcap_{h \in G} Z_h.$$

Satz 7.2.9 (Klassengleichung)**.** *Es sei G eine Gruppe. Wir betrachten die Operation von G auf sich selbst vermöge Konjugation:*

$$G \times G \ \to \ G, \qquad g \cdot h \ = \ ghg^{-1}.$$

Für jedes $h \in G$ gilt $G_h = Z_h$. Weiter ist $h \in G$ genau dann Fixpunkt, wenn $h \in Z_G$ gilt. Gilt $G = G \cdot h_1 \sqcup \ldots \sqcup G \cdot h_r$ mit $h_i \in G$ so gilt

$$|G| \ = \ |Z_G| + \sum_{[G:Z_{h_i}] \geq 2} [G : Z_{h_i}].$$

Beweis. Die ersten beiden Aussagen sind offensichtlich. Die dritte Aussage ergibt sich dann mit der Bahnengleichung:

$$\begin{aligned} |G| \ &= \ \sum_{i=1}^{r} |G \cdot h_i| \\ &= \ \sum_{|G \cdot h_i| = 1} |G \cdot h_i| + \sum_{|G \cdot h_i| \geq 2} |G \cdot h_i| \\ &= \ |Z_G| + \sum_{[G:G_{h_i}] \geq 2} [G : G_{h_i}] \\ &= \ |Z_G| + \sum_{[G:Z_{h_i}] \geq 2} [G : Z_{h_i}]. \end{aligned}$$

□

Erinnerung 7.2.10. Es sei $n \in \mathbb{Z}_{\geq 1}$. Wir schreiben $X_n = \{1, \ldots, n\}$. Die zugehörige *symmetrische Gruppe* ist

$$S_n \ := \ \{\sigma \colon X_n \to X_n;\ \sigma \text{ ist bijektiv}\}$$

mit der Verknüpfung $\sigma_1 \sigma_2 := \sigma_1 \circ \sigma_2$. Die symmetrische Gruppe S_n besitzt genau $n!$ Elemente.

Definition 7.2.11. Ein Element $\vartheta \in S_n$ heißt *k-Zykel*, falls es paarweise verschiedene $i_1, \ldots, i_k \in X_n$ gibt mit

$$\vartheta(i_1) = i_2, \quad \vartheta(i_2) = i_3, \quad \ldots, \quad \vartheta(i_{k-1}) = i_k, \quad \vartheta(i_k) = i_1$$

und $\vartheta(j) = j$ für alle $j \in X_n \setminus \{i_1, \ldots, i_k\}$. Wir bezeichnen einen solchen k-Zykel ϑ dann mit $(i_1, \ldots, i_k)$.

Beispiel 7.2.12. Die Elemente der symmetrischen Gruppe S_3 sind genau ihre k-Zykel mit $k = 1, 2, 3$, nämlich

$$\mathrm{id}_{X_3} = (1), \qquad (1,2),\ (1,3),\ (2,3), \qquad (1,2,3),\ (1,3,2).$$

In den symmetrischen Gruppen S_n mit $n \geq 4$ gibt es hingegen Elemente, die keine Zykel sind, etwa

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \;=\; (1,2)(3,4) \;\in\; S_4.$$

Bemerkung 7.2.13. Wir betrachten einen k-Zykel $\vartheta = (i_1, \ldots, i_k)$ in S_n. Für das Tupel $(i_1, \ldots, i_k) \in X_n^k$ haben wir

$$(i_1, i_2, \ldots, i_k) \;=\; (\vartheta^0(i_1), \vartheta^1(i_1), \ldots, \vartheta^{k-1}(i_1)).$$

Insbesondere ist das Element $\vartheta \in S_n$ von der Ordnung k und wir erhalten einen Gruppenisomorphismus

$$\mathbb{Z}/k\mathbb{Z} \;\to\; \langle\sigma\rangle, \qquad \bar{a} \;\mapsto\; \vartheta^a(i_1).$$

Bemerkung 7.2.14. Die Schreibweise $(i_1, \ldots, i_k)$ für einen k-Zykel in S_n ist nicht eindeutig; beispielsweise hat man

$$(1,2) \;=\; (2,1) \;\in\; S_3.$$

Für $k \geq 2$ hat jeder k-Zykel eine eindeutige Darstellung $(i_1, \ldots, i_k)$ mit $i_1 < i_j$ für $j = 2, \ldots, k$. Im trivialen Fall $k = 1$ wird die Notation (i_1) nicht verwendet.

Definition 7.2.15. Zwei Zykel $(i_1, \ldots, i_k)$ und $(j_1, \ldots, j_l)$ in S_n heißen *elementfremd*, falls

$$\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} \;=\; \emptyset.$$

Bemerkung 7.2.16. Je zwei elementfremde Zykeln ϑ_1 und ϑ_2 in S_n kommutieren, d.h., es gilt $\vartheta_1\vartheta_2 = \vartheta_2\vartheta_1$.

Satz 7.2.17. *Jedes Element $\sigma \in S_n$ lässt sich schreiben als $\sigma = \vartheta_1 \cdots \vartheta_s$ mit elementfremden Zykeln $\vartheta_1, \ldots, \vartheta_s$; dabei gilt $\vartheta_j(i) = i$ wann immer $\sigma(i) = i$.*

Beweis. Es sei $\sigma \in S_n$ gegeben. Wir verwenden Induktion über die Anzahl m aller $i \in X_n$ mit $\sigma(i) \neq i$. Für $m = 0$ haben wir $\sigma = \mathrm{id}_{X_n}$ und es ist nichts zu zeigen.

Es sei nun $m > 0$. Dann gibt es ein $i_1 \in X_n$ mit $\sigma(i_1) \neq i_1$. Da X_n endlich ist, gibt es $l_1 > l_2 \in \mathbb{Z}_{\geq 1}$ mit $\sigma^{l_1}(i_1) = \sigma^{l_2}(i_1)$. Das bedeutet $\sigma^{l_1 - l_2}(i_1) = i_1$. Insbesondere gibt es ein minimales $k \in \mathbb{Z}_{\geq 1}$ mit $\sigma^k(i_1) = i_1$. Damit haben wir einen k-Zykel

$$\vartheta_1 \;:=\; (i_1, \ldots, i_k) \;=:\; (\sigma^0(i_1), \ldots, \sigma^{k-1}(i_1)).$$

Für die Permutation $\sigma' := \vartheta_1^{-1}\sigma \in S_n$ ergibt sich

$$\sigma'(i) \;=\; \vartheta_1^{-1}(\sigma(i)) \;=\; \begin{cases} i, & i \in \{i_1, \ldots, i_k\}, \\ \sigma(i), & i \notin \{i_1, \ldots, i_k\}. \end{cases}$$

Insbesondere lässt σ' mehr Elemente aus X_n fest als σ. Nach Induktionsvoraussetzung ist σ' ein Produkt elementfremder Zykel $\vartheta_2, \ldots, \vartheta_s$ wie in der Behauptung des Satzes. Somit ist $\sigma = \vartheta_1 \cdots \vartheta_s$ die gewünschte Darstellung. □

Satz 7.2.18. *Es seien $\sigma \in S_n$ und $\sigma = \vartheta_1 \cdots \vartheta_s$ eine Zerlegung in elementfremde Zykel $\vartheta_\iota = (i_{\iota 1}, \ldots, i_{\iota k_\iota})$. Weiter sei $X_n^\sigma = \{j \in X_n;\ \sigma(j) = j\}$. Dann gilt*

$$m \;:=\; \mathrm{ord}(\sigma) \;=\; \mathrm{kgV}(k_1, \ldots, k_s), \qquad\qquad \langle\sigma\rangle \;=\; \{e_G, \sigma, \ldots, \sigma^{m-1}\},$$

wobei $\langle\sigma\rangle \leq S_n$ die von σ erzeugte Untergruppe ist. Die Bahnzerlegung der Operation von $\langle\sigma\rangle$ auf S_n ist gegeben durch

$$X_n \;=\; \bigsqcup_{j\in X_n^\sigma} \{j\} \sqcup \bigsqcup_{\iota=1}^{s} \{i_{\iota 1}, \ldots, i_{\iota k_\iota}\}.$$

Für die nichttrivialen Bahnen $B_\iota = \{i_{\iota 1}, \ldots, i_{\iota k_\iota}\}$ der Operation von $\langle\sigma\rangle$ auf X_n haben wir dabei $|B_\iota| = k_\iota$.

Beweis. Da die paarweise elementfremden Zykel $\vartheta_1, \ldots, \vartheta_s$ kommutieren, erhalten wir $\sigma^k = \vartheta_1^k \cdots \vartheta_s^k$ für jedes $k \in \mathbb{Z}_{\geq 1}$. Damit ergibt sich $\operatorname{ord}(\sigma) = \operatorname{kgV}(k_1, \ldots, k_s)$. Weiter haben wir $\sigma^k \cdot i = \vartheta_1^k \cdots \vartheta_s^k \cdot i$ für jedes $i \in X_n$. Damit erhalten wir die Aussagen über die Bahnen von $\langle\sigma\rangle$. □

Definition 7.2.19. Der *Typ* einer Permutation $\sigma \in \Sigma$ ist das Tupel $(k_1, \ldots, k_s)$ der Mächtigkeiten der nichtrivialen Bahnen $B_1, \ldots, B_s$ von $\langle\sigma\rangle$ in X_n nach Größe geordnet, d.h., man hat $k_1 \leq \ldots \leq k_s$.

Lemma 7.2.20. *Es sei $(i_1, \ldots, i_k) \in S_n$ ein k-Zykel. Für jede Permutation $\sigma \in S_n$ haben wir*

$$\sigma\,(i_1, \ldots, i_k)\,\sigma^{-1} \;=\; (\sigma(i_1), \ldots, \sigma(i_k)).$$

Beweis. Wir vergleichen die Werte der beiden Zykel auf einem gegebenem Element $a \in X_n$. Es gilt

$$\sigma\,(i_1, \ldots, i_k)\,\sigma^{-1}(a) \;=\; \begin{cases} \sigma(\sigma^{-1}(a)), & \sigma^{-1}(a) \notin \{i_1, \ldots, i_k\}, \\ \sigma(i_{j+1}), & \sigma^{-1}(a) = i_j,\ 1 \leq j < k, \\ \sigma(i_1), & \sigma^{-1}(a) = i_k, \end{cases}$$

$$(\sigma(i_1), \ldots, \sigma(i_k))(a) \;=\; \begin{cases} a, & a \notin \{\sigma(i_1), \ldots, \sigma(i_k)\}, \\ \sigma(i_{j+1}), & a = \sigma(i_j),\ 1 \leq j < k, \\ \sigma(i_1), & a = \sigma(i_k). \end{cases}$$

□

Satz 7.2.21. *Zwei Permutationen $\tau, \tau' \in S_n$ sind genau dann konjugiert zueinander, wenn sie vom gleichem Typ sind.*

Beweis. Es sei $\tau' = \sigma\tau\sigma^{-1}$ mit $\sigma \in S_n$. Wir wählen eine Darstellung als Produkt elementfremder Zykeln $\tau = (i_{11}, \ldots, i_{1k_1}) \cdots (i_{s1}, \ldots, i_{sk_s})$. Lemma 7.2.20 liefert

$$\begin{aligned} \tau' &= \sigma(i_{11}, \ldots, i_{1k_1}) \cdots (i_{s1}, \ldots, i_{sk_s})\sigma^{-1} \\ &= \sigma(i_{11}, \ldots, i_{1k_1})\sigma^{-1} \cdots \sigma(i_{s1}, \ldots, i_{sk_s})\sigma^{-1} \\ &= (\sigma(i_{11}), \ldots, \sigma(i_{1k_1})) \cdots (\sigma(i_{s1}), \ldots, \sigma(i_{sk_s})). \end{aligned}$$

Somit haben wir auch τ' als Produkt elementfremder Zykel dargestellt. Nach Satz 7.2.18 sind τ und τ' vom gleichen Typ.

Es seien nun τ und τ' vom gleichen Typ. Dann erhalten wir Darstellungen als Produkte elementfremder Zykel

$$\tau \;=\; (i_{11}, \ldots, i_{1k_1}) \cdots (i_{s1}, \ldots, i_{sk_s}), \qquad \tau' \;=\; (i'_{11}, \ldots, i'_{1k_1}) \cdots (i'_{s1}, \ldots, i'_{sk_s}),$$

wobei Satz 7.2.18 die Gleichheit der Längen garantiert. Wir wählen ein $\sigma \in S_n$ mit $\sigma(i_{lj}) = i'_{lj}$. Nach Lemma 7.2.20 gilt dann $\tau' = \sigma\tau\sigma^{-1}$. □

Folgerung 7.2.22. *Die Konjugationsklassen der symmetrischen Gruppe S_n sind genau die Mengen $C_{k_1,\ldots,k_s}$ aller Permutationen eines gegebenen Typs $(k_1,\ldots,k_s)$:*

$$C_{k_1,\ldots,k_s} \;:=\; \{\sigma \in S_n;\ \sigma \textit{ ist vom Typ } (k_1,\ldots,k_s)\} \;\subseteq\; S_n.$$

Beispiel 7.2.23. Die Konjugationsklassen der symmetrischen Gruppe S_4 sind gegeben durch

$$\begin{aligned}
C_1 &:= \{\mathrm{id}_{X_4}\},\\
C_2 &:= \{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\},\\
C_3 &:= \{(1,2,3),(1,2,4),(1,3,2),(1,3,4),(1,4,2),(1,4,3),(2,3,4),(2,4,3)\},\\
C_4 &= \{(1,2,3,4),(1,2,4,3),(1,3,2,4),(1,3,4,2),(1,4,2,3),(1,4,3,2)\},\\
C_{2,2} &= \{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}.
\end{aligned}$$

Aufgaben zu Abschnitt 7.2.

Aufgabe 7.2.24. Zeige: Die symmetrischen Gruppe S_3 besitzt triviales Zentrum, d.h., es gilt $Z_{S_3} = \{\mathrm{id}_{X_3}\}$.

Aufgabe 7.2.25. Zeige, dass das Zentrum der allgemeinen linearen Gruppe $\mathrm{GL}(2,\mathbb{K})$ gegeben ist durch

$$Z_{\mathrm{GL}(2,\mathbb{K})} \;=\; \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix};\ \lambda \in \mathbb{K}^* \right\}.$$

Aufgabe 7.2.26. Es sei p eine Primzahl. Zeige: Jede Gruppe der Ordnung p^k mit $k \in \mathbb{Z}_{\geq 1}$ besitzt ein nichttriviales Zentrum.

Aufgabe 7.2.27. Es sei $n \in \mathbb{Z}_{\geq 3}$. Betrachte die Permutationsgruppe S_n und die beiden Permutationen

$$\delta \;:=\; \begin{bmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{bmatrix}, \qquad \sigma \;:=\; \begin{bmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{bmatrix}.$$

Verifiziere die folgenden Aussagen:

$$\sigma^2 = \mathrm{id}_{X_n}, \qquad \delta^n = \mathrm{id}_{X_n}, \qquad \delta^k \neq \mathrm{id}_{X_n} \text{ für } k = 1 \dots, n-1, \qquad \sigma\delta = \delta^{-1}\sigma.$$

Die *Diedergruppe* $D_n \leq S_n$ ist die von δ und σ erzeugte Untergruppe von S_n, d.h., die kleinste Untergruppe, die δ und σ enthält. Zeige:

$$D_n \;=\; \{\delta^k \circ \sigma^j;\ k = 0, \dots, n-1,\ j = 0, 1\}, \qquad |D_n| \;=\; 2n.$$

Aufgabe 7.2.28. Es sei $n \in \mathbb{Z}_{\geq 3}$. Betrachte die Diedergruppe $D_n \leq S_n$ und die Permutationen $\delta, \sigma \in D_n$ aus Aufgabe 7.2.27. Beweise folgende Aussagen: Es gilt

$$\delta \;=\; (1, \dots, n), \qquad \sigma \;=\; \begin{cases} (1,n-1)(2,n-2)\cdots(\frac{n}{2}-1, \frac{n}{2}+1), & n \text{ gerade}, \\ (1,n-1)(2,n-2)\cdots(\frac{n-1}{2}, \frac{n+1}{2}), & n \text{ ungerade}. \end{cases}$$

Für ungerades n besitzt D_n die Konjugationsklassen

$$\{\mathrm{id}_{X_n}\}, \quad \{\delta^l, \delta^{n-l}\},\ l = 1, \dots, \frac{n-1}{2}, \quad \{\sigma, \sigma\delta, \dots, \sigma\delta^{n-1}\}.$$

Für gerades n besitzt D_n die Konjugationsklassen

$$\{\mathrm{id}_{X_n}\},\ \{\delta^{\frac{n}{2}}\},\ \{\delta^l, \delta^{n-l}\},\ l = 1, \dots, \frac{n-2}{2},\ \{\sigma, \sigma\delta^2, \dots, \sigma\delta^{n-2}\},\ \{\sigma\delta, \sigma\delta^3, \dots, \sigma\delta^{n-1}\}.$$

Aufgabe 7.2.29. Eine *Partition* von $n \in \mathbb{Z}_{\geq 1}$ ist eine Darstellung $n = n_1 + \ldots + n_r$ mit natürlichen Zahlen $1 \leq n_1 \leq \ldots \leq n_r \leq n$. Zeige: Die Anzahl der Konjugationsklassen in S_n ist genau die Anzahl der Partitionen von n.

7.3. **Darstellungen.**

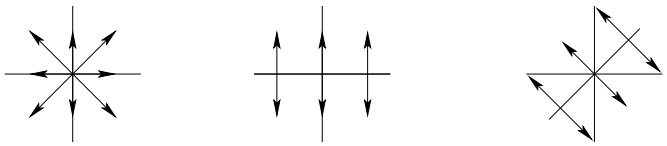
Definition 7.3.1. Es seien G eine Gruppe und $\mathbb{K}$ ein Körper. Eine *Matrixdarstellung* von G ist ein Homomorphismus $\varrho\colon G \to \mathrm{GL}(n;\mathbb{K})$.

Beispiel 7.3.2. Man erhält verschiedene Matrixdarstellungen $\varrho_i\colon G \to \mathrm{GL}(2;\mathbb{R})$ der Gruppe $G := \mathbb{Z}/2\mathbb{Z}$ durch

$$\varrho_1\colon \quad \overline{0} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \overline{1} \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\varrho_2\colon \quad \overline{0} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \overline{1} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\varrho_3\colon \quad \overline{0} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \overline{1} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$



$\varrho_1(\overline{1})$ $\varrho_2(\overline{1})$ $\varrho_3(\overline{1})$

Bemerkung 7.3.3. Es sei $\varrho\colon G \to \mathrm{GL}(n;\mathbb{K})$ eine Matrixdarstellung. Dann hat man eine Operation von G auf $\mathbb{K}^n$:

$$G \times \mathbb{K}^n \;\to\; \mathbb{K}^n, \qquad (g,v) \;\mapsto\; g \cdot v := \varrho(g) \cdot v,$$

wobei "$\cdot$" die Matrix-Vektor-Multiplikation bezeichnet. Für jedes $g \in G$ ist die Translation $T_g\colon \mathbb{K}^n \to \mathbb{K}^n$, $v \mapsto g \cdot v$ linear.

Beispiel 7.3.4. Die zu den Matrixdarstellungen $\varrho_i\colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{GL}(2,\mathbb{R})$ aus Beispiel 7.3.2 gehörigen Operationen μ_i von $\mathbb{Z}/2\mathbb{Z}$ auf $\mathbb{R}^2$ sind

$$\mu_1\colon \quad \overline{0} \cdot (x_1,x_2) = (x_1,x_2), \quad \overline{1} \cdot (x_1,x_2) = (-x_1,-x_2),$$

$$\mu_2\colon \quad \overline{0} \cdot (x_1,x_2) = (x_1,x_2), \quad \overline{1} \cdot (x_1,x_2) = (x_1,-x_2),$$

$$\mu_3\colon \quad \overline{0} \cdot (x_1,x_2) = (x_1,x_2), \quad \overline{1} \cdot (x_1,x_2) = (x_2,x_1).$$

Erinnerung 7.3.5. Die *Automorphismengruppe* eines $\mathbb{K}$-Vektorraumes V ist die Menge $\mathrm{Aut}(V)$ aller Vektorraumisomorphismen $V \to V$ mit der Komposition als Verknüpfung.

Definition 7.3.6. Es seien $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Eine *Darstellung* einer Gruppe G auf V ist ein Gruppenhomomorphismus $\varrho\colon G \to \mathrm{Aut}(V)$.

Bemerkung 7.3.7. Ist V ein n-dimensionaler $\mathbb{K}$-Vektorraum mit Basis $\mathfrak{B}$, so liefert der Übergang zur darstellenden Matrix einen Gruppenisomorphismus

$$\psi_{\mathcal{B}}\colon \mathrm{Aut}(V) \;\to\; \mathrm{GL}(n,\mathbb{K}), \qquad \alpha \;\mapsto\; M_{\mathcal{B}}^{\mathcal{B}}(\alpha).$$

Insbesondere erhalten wir eine Bijektion zwischen den Darstellungen $G \to \mathrm{Aut}(V)$ einer Gruppe G und ihren Matrixdarstellungen $G \to \mathrm{GL}(n;\mathbb{K})$ vermöge $\varrho \mapsto \psi_{\mathcal{B}} \circ \varrho$.

Definition 7.3.8. Es sei G eine Gruppe.

(i) Eine Operation von G auf einem $\mathbb{K}$-Vektorraum V heißt *linear*, falls jede Translation $T_g\colon V \to V$, $v \mapsto g \cdot v$ linear ist.
(ii) Ein *G-Modul* ist ein $\mathbb{K}$-Vektorraum V zusammen mit einer linearen Operation der Gruppe G.

Satz 7.3.9. *Es seien G eine Gruppe, $\mathbb{K}$ ein Körper und V ein $\mathbb{K}$-Vektorraum. Dann hat man zueinander inverse bijektive Abbildungen*

$$\begin{array}{rcl} \left\{ \begin{array}{l} \text{Darstellungen} \\ \varrho\colon G \to \operatorname{Aut}(V) \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{l} \text{Lineare Operationen} \\ \mu\colon G \times V \to V \end{array} \right\} \\ \varrho & \mapsto & \mu_\varrho\colon g \cdot v := \varrho(g)(v) \\ \varrho_\mu\colon g \mapsto [T_g\colon v \mapsto g \cdot v] & \leftarrow\!\shortmid & \mu \end{array}$$

Beweis. Wir zeigen zunächst, dass die Zuordnungen wohldefiniert sind. Ist ein Homomorphismus $\varrho\colon G \to \operatorname{Aut}(V)$ gegeben, so müssen wir zeigen, dass

$$\mu_\varrho\colon G \times V \;\to\; V, \qquad (g,v) \;\mapsto\; g \cdot v := \varrho(g)(v).$$

eine lineare G-Operation auf V ist. Für den Nachweis der Eigenschaften einer Operation sei $v \in V$ gegeben. Dann erhalten wir

$$e_G \cdot v \;=\; \varrho(e_G)(v) \;=\; \mathrm{id}_V(v) \;=\; v$$

und für je zwei $g_1, g_2 \in G$ gilt

$$g_2 \cdot (g_1 \cdot v) \;=\; \varrho(g_2)(\varrho(g_1)(v)) \;=\; (\varrho(g_2) \circ \varrho(g_1))(v) \;=\; \varrho(g_2 g_1)(v) \;=\; (g_2 g_1) \cdot v.$$

Damit ist gezeigt, dass μ_ϱ eine G-Operation auf V ist. Wegen $T_g = \varrho(g)$ sind dabei alle Translationen linear.

Es sei nun eine lineare Operation $\mu\colon G \times V \to V$ von G auf V gegeben. Wir müssen zeigen, dass

$$\varrho_\mu\colon G \;\to\; \operatorname{Aut}(V), \qquad g \;\mapsto\; T_g$$

ein Homomorphismus ist. Dazu seien $g_1, g_2 \in G$ gegeben. Dann erhalten wir für jedes $v \in V$:

$$T_{g_2 g_1}(v) \;=\; (g_2 g_1) \cdot v \;=\; g_2 \cdot (g_1 \cdot v) \;=\; T_{g_2}(T_{g_1}(v)) \;=\; (T_{g_2} \circ T_{g_1})(v).$$

Folglich gilt $T_{g_2 g_1} = T_{g_2} \circ T_{g_1}$. Das ist genau die Homomorphieeigenschaft für die Abbildung $\varrho_\mu\colon G \to \operatorname{Aut}(V)$.

Es bleibt zu zeigen, dass die Zuordnungen $\varrho \mapsto \mu_\varrho$ und $\mu \mapsto \varrho_\mu$ invers zueinander sind, d.h., dass gilt

$$\mu_{\varrho_\mu} \;=\; \mu, \qquad\qquad \varrho_{\mu_\varrho} \;=\; \varrho.$$

Das geschieht wiederum durch einfaches Nachrechnen: Für jedes $g \in G$ und jedes $v \in V$ erhalten wir

$$\begin{aligned} \mu_{\varrho_\mu}(g,v) \;&=\; \varrho_\mu(g)(v) \;=\; T_g(v) \;=\; \mu(g,v), \\ \varrho_{\mu_\varrho}(g)(v) \;&=\; T_g(v) \;=\; \mu_\varrho(g,v) \;=\; \varrho(g)(v). \end{aligned}$$

□

Definition 7.3.10. Es seien $G \times V \to V$ und $G \times V' \to V'$ lineare Operationen.

(i) Eine lineare Abbildung $\varphi\colon V \to V'$ heißt *äquivariant*, falls $\varphi(g \cdot v) = g \cdot \varphi(v)$ für alle $g \in G$ und alle $v \in V$ gilt.
(ii) Die Menge aller äquivarianten linearen Abbildungen $V \to V'$ bezeichnet man mit $\operatorname{Hom}_G(V, V')$.
(iii) Man nennt eine äquivariante lineare Abbildung $V \to V'$ auch *G-äquivariant* oder einen *G-Modulhomomorphismus*.

Definition 7.3.11. Es sei G eine Gruppe.

(i) Zwei Darstellungen $\varrho\colon G \to \operatorname{Aut}(V)$ und $\varrho'\colon G \to \operatorname{Aut}(V')$ heißen *äquivalent*, in Zeichen $\varrho \sim \varrho'$, falls ein Isomorphismus $\varphi\colon V \to V'$ existiert mit $\varrho'(g) = \varphi \circ \varrho(g) \circ \varphi^{-1}$ für alle $g \in G$.

(ii) Zwei Matrixdarstellungen $\varrho, \varrho' \colon G \to \mathrm{GL}(n;\mathbb{K})$ heißen *äquivalent*, in Zeichen $\varrho \sim \varrho'$, falls eine Matrix $S \in \mathrm{GL}(n;\mathbb{K})$ existiert mit $\varrho'(g) = S\varrho(g)S^{-1}$ für alle $g \in G$.

Bemerkung 7.3.12. Es sei V ein eindimensionaler $\mathbb{K}$-Vektorraum. Dann ist $\mathrm{Aut}(V)$ abelsch, denn wir haben Gruppenisomorphismen

$$\mathrm{Aut}(V) \;\cong\; \mathrm{GL}(1;\mathbb{K})^* \;\cong\; \mathbb{K}^*.$$

Für zwei Darstellungen $\varrho, \varrho' \colon G \to \mathrm{Aut}(V)$ einer Gruppe G auf V gilt also im vorliegenden Fall

$$\varrho \sim \varrho' \iff \varrho = \varrho'.$$

Beispiel 7.3.13. Die drei Matrixdarstellungen $\varrho_i \colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{GL}(2;\mathbb{R})$ aus Beispiel 7.3.2 waren gegeben durch

$$\varrho_1(\overline{1}) \;=\; \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \varrho_2(\overline{1}) \;=\; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \varrho_3(\overline{1}) \;=\; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Wir wollen sehen, welche dieser Darstellungen äquivalent zueinander sind. Wegen $G = \mathbb{Z}/2\mathbb{Z}$ haben wir

$$\varrho_i \sim \varrho_j \iff \varrho_j(\overline{1}) = S \cdot \varrho_i(\overline{1}) \cdot S^{-1} \text{ mit } S \in \mathrm{GL}(2;\mathbb{R}).$$

Letztere Bedingung lässt sich anhand der Eigenwerte prüfen. Für $\varrho_1(\overline{1})$ sind Eigenwerte $-1, -1$ und für $\varrho_2(\overline{1})$, $\varrho_3(\overline{1})$ jeweils $1, -1$. Wir schliessen

$$\varrho_1 \;\not\sim\; \varrho_2, \qquad \varrho_1 \;\not\sim\; \varrho_3, \qquad \varrho_2 \;\sim\; \varrho_3.$$

Satz 7.3.14. *Es seien $\varrho \colon G \to \mathrm{Aut}(V)$ und $\varrho' \colon G \to \mathrm{Aut}(V')$ zwei Darstellungen einer Gruppe G auf $\mathbb{K}$-Vektorräumen V bzw. V'. Dann hat man*

$$\varrho \sim \varrho' \quad\iff\quad \text{es gibt einen } G\text{-Modulisomorphismus } \varphi \colon V \to V'.$$

Beweis. Zu "⇒". Es sei $\varphi \colon V \to V'$ ein Vektorraumisomorphismus mit $\varrho'(g) = \varphi \circ \varrho(g) \circ \varphi^{-1}$ für alle $g \in G$. Dann haben wir stets $\varrho'(g) \circ \varphi = \varphi \circ \varrho(g)$. Es folgt

$$\varphi(g \cdot v) \;=\; \varphi(\varrho(g)(v)) \;=\; \varrho'(g)(\varphi(v)) \;=\; g \cdot \varphi(v).$$

Zu "⇐". Es sei $\varphi \colon V \to V'$ ein Isomorphismus der G-Moduln V und V'. Dann erhalten wir für jedes $g \in G$

$$\varrho'(g)(\varphi(v)) \;=\; g \cdot \varphi(v) \;=\; \varphi(g \cdot v) \;=\; \varphi(\varrho(g)(v))$$

Also gilt $\varrho'(g) \circ \varphi = \varphi \circ \varrho(g)$ für jedes $g \in G$. Das impliziert $\varrho'(g) = \varphi \circ \varrho(g) \circ \varphi^{-1}$ für alle $g \in G$. □

Satz 7.3.15. *Es seien $G = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$ und $\varrho \colon G \to \mathbb{C}^*$ eine Darstellung. Dann gibt es Einheitswurzeln $\zeta_i \in \mathrm{EW}_{n_i}$ mit*

$$\varrho(\overline{k}_1, \ldots, \overline{k}_r) \;=\; \zeta_1^{k_1} \cdots \zeta_r^{k_r}.$$

Die zur Darstellung $\varrho \colon G \to \mathbb{C}^*$ gehörige lineare G-Operation auf $\mathbb{C}$ ist damit gegeben durch

$$(\overline{k}_1, \ldots, \overline{k}_r) \cdot z \;=\; \zeta_1^{k_1} \cdots \zeta_r^{k_r} z.$$

Lemma 7.3.16. *Es sei $\varrho \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$ ein Gruppenomomorphismus. Dann gibt es eine n-te Einheitswurzel $\zeta \in \mathbb{C}^*$ mit $\varrho(\overline{k}) = \zeta^k$ für alle $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$.*

Beweis. Es sei $\zeta := \varrho(\overline{1})$. Dann ergeben sich die Behauptungen direkt aus der Tatsache, dass ϱ ein Gruppenhomomorphismus ist: Es gilt

$$\zeta^n \;=\; \varrho(n\overline{1}) \;=\; \varrho(\overline{0}) \;=\; 1, \qquad\qquad \varrho(\overline{k}) \;=\; \varrho(k\overline{1}) \;=\; \zeta^k.$$

□

Beweis von Satz 7.3.15. Für $1 \leq i \leq r$ betrachten wir die injektiven Gruppenhomomorphismen

$$\varphi_i \colon \mathbb{Z}/n_i\mathbb{Z} \ \to \ G, \qquad \overline{k}_i \ \mapsto \ (\overline{0}, \ldots, \overline{0}, \overline{k}_i, \overline{0} \ldots, \overline{0}).$$

Damit erhält man Gruppenhomomorphismen $\varrho \circ \varphi_i \colon \mathbb{Z}/n_i\mathbb{Z} \to \mathbb{C}^*$. Diese sind nach Lemma 7.3.16 von der Form $\overline{k}_i \mapsto \zeta_i^{k_i}$ mit n_i-ten Einheitswurzeln $\zeta_i \in \mathbb{C}$. Es folgt

$$\begin{aligned} \varrho(\overline{k}_1, \ldots, \overline{k}_r) &= \varrho(\varphi_1(\overline{k}_1) + \ldots + \varphi_r(\overline{k}_r)) \\ &= \varrho(\varphi_1(\overline{k}_1)) \cdot \ldots \cdot \varrho(\varphi_r(\overline{k}_r)) \\ &= \zeta_1^{k_1} \cdot \ldots \cdot \zeta_r^{k_r}. \end{aligned}$$

□

Satz 7.3.17. *Es seien $G = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$ und $\varrho, \sigma \colon G \to \mathbb{C}^*$ Darstellungen. Sind $\zeta_1, \ldots, \zeta_r$ bzw. $\eta_1, \ldots, \eta_r$ Einheitswurzeln zu ϱ bzw. σ wie in 7.3.15, so gilt*

$$\varrho \ \sim \ \sigma \quad \Longleftrightarrow \quad \zeta_1 = \eta_1, \ldots, \zeta_r = \eta_r.$$

Beweis. Nur zur Implikation "$\Rightarrow$" ist etwas zu zeigen. Wegen $\varrho \sim \sigma$ gibt es ein $a \in \mathbb{C}^*$, sodass für alle $(\overline{k}_1, \ldots, \overline{k}_r) \in G$ gilt:

$$\sigma(\overline{k}_1, \ldots, \overline{k}_r) \ = \ a\varrho((\overline{k}_1, \ldots, \overline{k}_r) \cdot 1)a^{-1}.$$

Das impliziert jeweils $\zeta_1^{k_1} \cdots \zeta_r^{k_r} = \eta_1^{k_1} \cdots \eta_r^{k_r}$. Setzt man dabei $k_i = 1$ und $k_j = 0$ für $j \neq i$, so ergibt sich $\eta_i = \zeta_i$. □

Folgerung 7.3.18. *Es sei G eine endliche abelsche Gruppe, dann gibt es genau $|G|$ nicht äquivalente Darstellungen $\varrho \colon G \to \mathbb{C}^*$.*

Beweis. Als endliche abelsche Gruppe ist G von der Form $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$; siehe Satz 4.2.6. Nach Sätzen 7.3.15 und 7.3.17 werden die Darstellungen $\varrho \colon G \to \mathbb{C}^*$ eindeutig durch Tupel $(\zeta_1, \ldots, \zeta_r)$ mit $\zeta_i \in \mathrm{EW}_{n_i}$ bestimmt. Wegen $|\mathrm{EW}_{n_i}| = n_i$ gibt es genau $n_1 \cdots n_r = |G|$ viele nichtäquivalante Darstellungen $\varrho \colon G \to \mathbb{C}^*$. □

Aufgaben zu Abschnitt 7.3.

Aufgabe 7.3.19. Es seien $\mathbb{K}$ ein Körper, $\mathcal{E} = (e_1, \ldots, e_n)$ die Standardbasis für $\mathbb{K}^n$ und S_n die symmetrische Gruppe. Beweise folgende Aussagen:

(i) Zu jedem $\sigma \in S_n$ gibt es einen Isomorphismus $\varphi_\sigma \colon \mathbb{K}^n \to \mathbb{K}^n$ mit

$$\varphi_\sigma(e_i) \;=\; e_{\sigma(i)} \qquad \text{für } 1 \leq i \leq n.$$

Dabei ist φ_σ eindeutig bestimmt und für je zwei Permutationen $\sigma, \tau \in S_n$ gilt

$$\varphi_{\sigma\circ\tau} \;=\; \varphi_\sigma \circ \varphi_\tau.$$

(ii) Die darstellende Matrix A_σ von φ_σ bezüglich der Standardbasis ist gegeben als

$$A_\sigma \;=\; M_{\mathcal{E}}^{\mathcal{E}}(\varphi_\sigma) \;=\; (e_{\sigma(1)}, \ldots, e_{\sigma(n)}).$$

Dabei ist A_σ stets invertierbar mit $A_\sigma^{-1} = A_\sigma^t$ und für alle $\sigma, \tau \in S_n$ gilt

$$A_{\sigma\circ\tau} \;=\; A_\sigma \cdot A_\tau.$$

(iii) Man erhält eine injektive Matrixdarstellung durch

$$\varrho_n \colon S_n \;\to\; \mathrm{GL}(n, \mathbb{K}), \qquad \sigma \;\mapsto\; A_\sigma.$$

Für jedes $\sigma \in S_n$ und jeden Vektor $x = (x_1, \ldots, x_n) \in \mathbb{K}^n$ gilt dabei

$$\varrho_n(\sigma) \cdot x \;=\; (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

(iv) Man hat ein kommutatives Diagramm von Gruppenhomomorphismen

$$\begin{array}{ccc} S_n & \xrightarrow{\;\sigma \mapsto A_\sigma\;} & \mathrm{GL}(n, \mathbb{K}) \\ {\scriptstyle \sigma \mapsto \mathrm{sg}(\sigma)}\downarrow & & \downarrow{\scriptstyle A \mapsto \det(A)} \\ \{\pm 1\} & \xrightarrow[\pm 1 \mapsto \pm 1_{\mathbb{K}}]{} & \mathbb{K}^* \end{array}$$

Aufgabe 7.3.20. Es seien $\mathbb{K}$ ein Körper, G eine Gruppe der Ordnung n und $m := n!$. Zeige: Es gibt eine injektive Darstellung $G \to \mathrm{GL}(m; \mathbb{K})$. *Hinweis*: Verwende Aufgabe 7.1.19 und Aufgabe 7.3.19.

Aufgabe 7.3.21. Zeige, dass es eine eindeutig bestimmte injektive Matrixdarstellung $\varrho \colon D_n \to \mathrm{GL}(2, \mathbb{R})$ gibt mit

$$\varrho(\delta) \;=\; \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}, \qquad \varrho(\sigma) \;:=\; \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Aufgabe 7.3.22. Es seien V ein $\mathbb{K}$-Vektorraum und G eine Gruppe. Zeige: Ist $G \times V \to V$ eine lineare Operation, so ist ihre Fixpunktmenge $V^G \subseteq V$ ein Untervektorraum von V.

7.4. **Darstellungen und lineare Algebra.**

Konstruktion 7.4.1. Es seien G eine Gruppe, V ein G-Modul und $V_0 \subseteq V$ ein *G-Untermodul*, d.h., wir haben

$$V_0 \ \leq_{\mathbb{K}} \ V, \qquad G \cdot V_0 \ = \ V_0.$$

Dann wird der Quotientenvektorraum V/V_0 zu einem G-Modul, indem wir für $g \in G$ und $v \in V$ setzen

$$g \cdot (v + V_0) \ := \ g \cdot v + V_0.$$

Beweis. Es ist lediglich die Wohldefiniertheit von $g \cdot (v + V_0)$ nachzuweisen. Dazu seien $v, v' \in V$ mit $v + V_0 = v' + V_0$ gegeben. Dann erhalten wir

$$g \cdot v' + V_0 \ = \ g \cdot (v - v + v') + V_0 \ = \ g \cdot v + g \cdot (v' - v) + V_0 \ = \ g \cdot v + V_0.$$

Man beachte, dass dabei für die zweite Gleichung die Linearität der Operation und für die dritte Gleichung die Invarianz von V_0 verwendet wurden. □

Konstruktion 7.4.2. Es seien eine Gruppe G und G-Moduln $V_1, \ldots, V_r$ gegeben. Dann wird die direkte Summe $V_1 \oplus \ldots \oplus V_r$ ein G-Modul durch

$$g \cdot (v_1, \ldots, v_r) \ = \ (g \cdot v_1, \ldots, g \cdot v_r).$$

Beispiel 7.4.3. Wir betrachten die Gruppe $G := \mathbb{Z}/2\mathbb{Z}$, die beiden eindimensionalen G-Moduln

$$V_1 = \mathbb{R} \text{ mit } \overline{1} \cdot x := x, \qquad V_2 = \mathbb{R} \text{ mit } \overline{1} \cdot x := -x$$

und den zweidimensionalen G-Modul

$$V = \mathbb{R}^2 \text{ mit } \overline{1} \cdot (x, y) := (y, x).$$

Dann ist der G-Modul $V_1 \oplus V_2$ isomorph zum G-Modul V; ein expliziter Isomorphismus ist gegeben durch

$$V_1 \oplus V_2 \ \to \ V, \qquad (x, y) \ \mapsto \ (x + y, x - y).$$

Bemerkung 7.4.4. Es seien G eine Gruppe und $\varrho_i \colon G \to \mathrm{Aut}(V_i)$ Darstellungen, wobei $1 \leq i \leq r$. Wir schreiben

$$\varrho_1 \oplus \ldots \oplus \varrho_r \colon G \ \to \ \mathrm{Aut}(V_1 \oplus \ldots \oplus V_r)$$

für die zum G-Modul $V_1 \oplus \ldots \oplus V_r$ gehörige Darstellung. Im Fall von Matrixdarstellungen $\varrho_i \colon G \to \mathrm{GL}(n_i; \mathbb{K})$ schreiben wir

$$\varrho_1 \oplus \ldots \oplus \varrho_r \colon G \ \to \ \mathrm{GL}(n; \mathbb{K}), \qquad g \ \mapsto \ \begin{pmatrix} \varrho_1(g) & & 0 \\ & \ddots & \\ 0 & & \varrho_r(g) \end{pmatrix},$$

wobei $n := n_1 + \ldots + n_r$. Der G-Modul $\mathbb{K}^n$ zu $\varrho_1 \oplus \ldots \oplus \varrho_r$ ist dann isomorph zur direkten Summe $\mathbb{K}^{n_1} \oplus \ldots \oplus \mathbb{K}^{n_r}$ der G-Moduln $\mathbb{K}^{n_i}$ zu ϱ_i.

Konstruktion 7.4.5. Es seien eine Gruppe G und G-Moduln $V_1, \ldots, V_r$ gegeben. Dann wird das Tensorprodukt $V_1 \otimes \ldots \otimes V_r$ ein G-Modul durch

$$g \cdot (v_1 \otimes \ldots \otimes v_r) \ := \ g \cdot v_1 \otimes \ldots \otimes g \cdot v_r.$$

Beweis. Es ist zu zeigen, dass wir eine wohldefinierte G-Modulstruktur vorliegen haben. Folgerung 6.3.11 liefert für jedes $g \in G$ ein kommutatives Diagramm

$$\begin{array}{ccc} V_1 \times \ldots \times V_r & \xrightarrow[T_g \times \ldots \times T_g]{(v_1,\ldots v_r) \,\mapsto\, (g\cdot v_1,\ldots,g\cdot v_r)} & V_1 \times \ldots \times V_r \\ \Big\downarrow \Pi & & \Big\downarrow \Pi \\ V_1 \otimes \ldots \otimes V_r & \xrightarrow[T_g \otimes \ldots \otimes T_g]{v_1 \otimes \ldots \otimes v_r \,\mapsto\, g\cdot v_1 \otimes \ldots \otimes g\cdot v_r} & V_1 \otimes \ldots \otimes V_r \end{array}$$

mit einer linearen Abbildung $T_g \otimes \ldots \otimes T_g \colon V_1 \otimes \ldots \otimes V_r \to V_1 \otimes \ldots \otimes V_r$. Diese ist die zu $g \in G$ gehörige Translation. □

Beispiel 7.4.6. Es seien $G := \mathbb{Z}/n\mathbb{Z}$ und $\zeta, \eta \in \mathbb{C}$ zwei n-te Einheitswurzeln. Dann hat man eindimensionale G-Moduln

$$V_1 = \mathbb{C} \text{ mit } \overline{k} \cdot z := \zeta^k z, \qquad\qquad V_2 = \mathbb{C} \text{ mit } \overline{k} \cdot w := \eta^k w.$$

Wir betrachten das Tensorprodukt $V_1 \otimes V_2$ Für jedes Elemenent $g = \overline{k}$ haben wir

$$g \cdot (z \otimes w) \;=\; g \cdot z \otimes g \cdot w \;=\; \zeta^k z \otimes \eta^k w \;=\; \zeta^k \eta^k \, z \otimes w.$$

Nun ist $V_1 \otimes V_2 = \mathbb{C} \otimes \mathbb{C}$ eindimensional mit Basis $(1 \otimes 1)$. Somit erhalten wir einen Vektorraumisomorphismus

$$\varphi \colon V_1 \otimes V_2 \;\to\; \mathbb{C}, \qquad \sum z_i \otimes w_i \;\mapsto\; \sum z_i w_i.$$

Durch $\overline{k} \cdot z := (\zeta\eta)^k z$ wird $V = \mathbb{C}$ zu einem G-Modul und $\varphi \colon V_1 \otimes V_2 \to V$ ein Isomorphismus von G-Moduln.

Bemerkung 7.4.7. Es seien G eine Gruppe und $\varrho_i \colon G \to \mathrm{Aut}(V_i)$ Darstellungen, wobei $1 \le i \le r$. Wir schreiben

$$\varrho_1 \otimes \ldots \otimes \varrho_r \colon G \;\to\; \mathrm{Aut}(V_1 \otimes \ldots \otimes V_r)$$

für die zum G-Modul $V_1 \otimes \ldots \otimes V_r$ gehörige Darstellung. Im Fall von Matrixdarstellungen $\varrho_i \colon G \to \mathrm{GL}(n_i; \mathbb{K})$ mit $i = 1, 2$, liefert

$$\varrho_1 \otimes \varrho_2 \colon G \;\to\; \mathrm{GL}(n_1 n_2; \mathbb{K}), \qquad g \;\mapsto\; \varrho_1(g) \otimes \varrho_2(g).$$

die Matrixdarstellung des Tensorproduktes $\mathbb{K}^{n_1} \otimes \mathbb{K}^{n_2}$ der G-Moduln $\mathbb{K}^{n_i}$ zu ϱ_i, wobei $\varrho_1(g) \otimes \varrho_2(g)$ das *Kronecker-Produkt* von $A = \varrho_1(g)$ und $B = \varrho_2(g)$ ist:

$$A \otimes B \;:=\; \begin{bmatrix} a_{11}B & \ldots & a_{1n_1}B \\ \vdots & & \vdots \\ a_{n_1 1}B & \ldots & a_{n_1 n_1}B \end{bmatrix} \;\in\; \mathrm{GL}(n_1 n_2; \mathbb{K}).$$

Konstruktion 7.4.8. Es seien G eine Gruppe und V, W zwei G-Moduln. Dann wird $\mathrm{Hom}(V, W)$ ein G-Modul durch

$$G \times \mathrm{Hom}(V,W) \;\to\; \mathrm{Hom}(V,W), \qquad (g \cdot \varphi)(v) \;:=\; g \cdot \varphi(g^{-1} \cdot v).$$

Beweis. Wir zeigen zunächst, dass die Vorschrift eine Operation definiert. Ist $\varphi \in \mathrm{Hom}(V, W)$ gegeben, so erhalten wir für jedes $v \in V$:

$$(e_G \cdot \varphi)(v) \;=\; e_G \cdot \varphi(e_G^{-1} \cdot v) \;=\; \varphi(v).$$

Das bedeutet $e_G \cdot \varphi = \varphi$. Sind weiter $g_1, g_2 \in G$ gegeben, so erhalten wir für jedes Element $v \in V$:

$$\begin{aligned} ((g_1 g_2) \cdot \varphi)(v) &= (g_1 g_2) \cdot \varphi((g_1 g_2)^{-1} \cdot v) \\ &= g_1 \cdot (g_2 \cdot \varphi(g_2^{-1} \cdot (g_1^{-1} \cdot v))) \\ &= g_1 \cdot (g_2 \cdot \varphi)(g_1^{-1} \cdot v) \\ &= (g_1 \cdot (g_2 \cdot \varphi))(v). \end{aligned}$$

Das impliziert $(g_1g_2)\cdot\varphi = g_1\cdot(g_2\cdot\varphi)$. Die Linearität der G-Operation auf $\mathrm{Hom}(V,W)$ lässt sich direkt nachweisen: Für $\varphi,\psi\in\mathrm{Hom}(V,W)$ und $a,b\in\mathbb{K}$ ergibt sich

$$\begin{aligned}(g\cdot(a\varphi+b\psi))(v) &= g\cdot((a\varphi+b\psi)(g^{-1}\cdot v))\\ &= g\cdot(a\varphi(g^{-1}\cdot v)+b\psi(g^{-1}\cdot v))\\ &= a(g\cdot\varphi(g^{-1}\cdot v))+b(g\cdot\psi(g^{-1}\cdot v))\\ &= a((g\cdot\varphi)(v))+b((g\cdot\psi)(v))\\ &= (a(g\cdot\varphi)+b(g\cdot\psi))(v).\end{aligned}$$

□

Satz 7.4.9. *Es seien G eine Gruppe und V, W zwei G-Moduln. In* $\mathrm{Hom}(V,W)$ *gilt dann*

$$\mathrm{Hom}_G(V,W) \;=\; \mathrm{Hom}(V,W)^G.$$

Beweis. Zum Nachweis der Inklusion "$\subseteq$" sei ein G-Modulhomomorphismus $\varphi\colon V\to W$ gegeben. Dann erhalten wir für jedes $g\in G$ und jedes $v\in V$:

$$(g\cdot\varphi)(v) \;=\; g\cdot\varphi(g^{-1}\cdot v) \;=\; g\cdot(g^{-1}\cdot\varphi(v)) \;=\; \varphi(v).$$

Zum Nachweis der Inklusion "$\supseteq$", sei $\varphi\in\mathrm{Hom}(V,W)$ ein Fixpunkt der G-Operation auf $\mathrm{Hom}(V,W)$. Dann ergibt sich für jedes $g\in G$ und jedes $v\in V$:

$$\varphi(g\cdot v) \;=\; (g\cdot\varphi)(g\cdot v) \;=\; g\cdot\varphi(g^{-1}\cdot(g\cdot v)) \;=\; g\cdot\varphi(v).$$

□

Konstruktion 7.4.10. Es seien G eine Gruppe und V ein G-Modul. Der zugehörige *duale G-Modul* ist $V^*:=\mathrm{Hom}(V,\mathbb{K})$ mit der G-Operation

$$(g\cdot u)(v) \;:=\; u(g^{-1}\cdot v).$$

Dies ist ein Spezialfall von Konstruktion 7.4.8, wobei man $W=\mathbb{K}$ mit der trivialen Operation $g\cdot z=z$ versieht.

Bemerkung 7.4.11. Es seien G eine Gruppe und $\varrho\colon G\to\mathrm{GL}(n;\mathbb{K})$ eine Matrixdarstellung. Die zugehörige *duale Matrixdarstellung* ist

$$\varrho^*\colon G \;\to\; \mathrm{GL}(n;\mathbb{K}), \qquad g \;\mapsto\; (\varrho(g)^{-1})^t.$$

Den durch ϱ^* definierten G-Modul $\mathbb{K}^n$ kann man mit dem dualen G-Modul $(\mathbb{K}^n)^*$ des durch ϱ definierten G-Moduls identifizieren; man hat einen Isomorphismus

$$\mathbb{K}^n \;\to\; (\mathbb{K}^n)^*, \qquad e_i \;\mapsto\; e_i^*.$$

Satz 7.4.12. *Es seien $\mathbb{K}$ ein Körper und V,W zwei eindlichdimensionale $\mathbb{K}$-Vektorräume. Dann hat man einen Isomorphismus von $\mathbb{K}$-Vektorräumen*

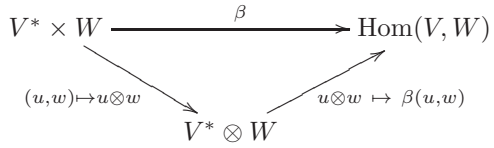
$$\Phi\colon V^*\otimes W \;\to\; \mathrm{Hom}(V,W), \qquad \sum u_i\otimes w_i \;\mapsto\; \Big[v\mapsto\sum u_i(v)w_i\Big].$$

Sind dabei V und W beides G-Moduln, so ist die lineare Abbildung Φ ein Isomorphismus der G-Moduln $V^*\otimes W$ und $\mathrm{Hom}(V,W)$.

Beweis. Wir zeigen zunächst, dass Φ eine wohldefinierte Abbildung ist. Dazu betrachten wir die bilineare Abbildung

$$\beta\colon V^*\times W \;\to\; \mathrm{Hom}(V,W), \qquad (u,w) \;\mapsto\; [v\mapsto u(v)w].$$

Nach der universellen Eigenschaft des Tensorproduktes 6.3.9 erhalten wir dann ein kommutatives Diagramm



wobei die Abbildung $V^* \otimes W \to \mathrm{Hom}(V,W)$ linear ist. Wegen $\Phi(u \otimes w) = \beta(u,w)$ ist damit gezeigt, dass Φ eine wohldefinierte lineare Abbildung ist.

Es bleibt zu zeigen, dass Φ bijektiv ist. Dazu seien $(b_1, \ldots, b_n)$ eine Basis für V und $(b_1^*, \ldots, b_n^*)$ die zugehörige duale Basis. Wir betrachten die lineare Abbildung

$$\Psi\colon \mathrm{Hom}(V,W) \ \to \ V^* \otimes W, \qquad \varphi \ \mapsto \ \sum b_i^* \otimes \varphi(b_i)$$

und zeigen, dass dies eine Umkehrabbildung zu Φ ist. Für den Nachweis von $\Psi \circ \Phi = \mathrm{id}$ sei $u \otimes w \in V^* \otimes W$ gegeben. Wir setzen

$$\varphi := \Phi(u \otimes w)\colon V \ \to \ W, \qquad v \ \mapsto \ u(v)w$$

und verwenden die Entwicklung $u = \sum u(b_i) \cdot b_i^*$ bezüglich der Basis $(b_1^*, \ldots, b_r^*)$. Dann erhalten wir

$$\Psi(\varphi) \ = \ \sum b_i^* \otimes \varphi(b_i) \ = \ \sum b_i^* \otimes u(b_i)w \ = \ \Big(\sum u(b_i) b_i^*\Big) \otimes w \ = \ u \otimes w.$$

Zum Nachweis von $\Phi \circ \Psi = \mathrm{id}$ sei eine lineare Abbildung $\varphi\colon V \to W$ gegeben. Dann haben wir

$$\Phi(\Psi(\varphi))\colon V \ \to \ W, \qquad v \ \mapsto \ \sum b_i^*(v)\varphi(b_i).$$

Insbesondere sehen wir, dass $\Phi(\Psi(\varphi))(b_j) = \varphi(b_j)$ gilt. Da beide Abbildungen linear sind, folgt $\Phi(\Psi(\varphi)) = \varphi$.

Es seien nun G-Modulstrukturen auf V sowie W gegeben. Weiter seien $g \in G$ und $u \otimes w \in V^* \otimes W$ gegeben. Dann erhalten wir für jedes $v \in V$:

$$\begin{aligned}
\Phi(g \cdot (u \otimes w))(v) &= \Phi(g \cdot u \otimes g \cdot w)(v) \\
&= (g \cdot u)(v)(g \cdot w) \\
&= u(g^{-1} \cdot v)(g \cdot w) \\
&= g \cdot (u(g^{-1} \cdot v)w) \\
&= g \cdot (\Phi(u \otimes w)(g^{-1} \cdot v)) \\
&= (g \cdot \Phi(u \otimes w))(v).
\end{aligned}$$

Somit ist Φ ein G-Modulhomomorphismus. Damit muss auch die Umkehrabbildung Ψ ein G-Modulhomomorphismus sein, denn wir haben stets

$$\Psi(g \cdot v) \ = \ \Psi(g \cdot \Phi(\Psi(v))) \ = \ \Psi(\Phi(g \cdot \Psi(v))) \ = \ g \cdot \Psi(v).$$

□

Aufgaben zu Abschnitt 7.4.

Aufgabe 7.4.13. Es sei $\varphi\colon V \to W$ ein G-Modulhomomorphismus. Beweise folgende Aussagen.

(i) $\mathrm{Kern}(\varphi)$ ist ein G-Untermodul von V.
(ii) $\mathrm{Bild}(\varphi)$ ist ein G-Untermodul von W.
(iii) Ist φ bijektiv, so ist φ ein G-Modulisomorphimus.

Aufgabe 7.4.14. Beweise die in den Bemerkungen 7.4.4, 7.4.7 und 7.4.11 getroffenen Aussagen.

Aufgabe 7.4.15. Es seien $A \in \mathrm{Mat}(n,n;\mathbb{K})$ und $B \in \mathrm{Mat}(m,m;\mathbb{K})$. Beweise folgende Aussagen über das Kronecker-Produkt:

$$\begin{aligned} \mathrm{Spur}(A \otimes B) &= \mathrm{Spur}(A)\mathrm{Spur}(B), \\ \mathrm{Rang}(A \otimes B) &= \mathrm{Rang}(A)\mathrm{Rang}(B), \\ \det(A \otimes B) &= \det(A)^m \det(B)^n. \end{aligned}$$

Zeige weiter: Das Kronecker-Produkt $A \otimes B$ ist genau dann invertierbar, wenn A und B invertierbar sind. In diesem Fall gilt

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

Aufgabe 7.4.16. Es sei $G := \mathbb{Z}/2\mathbb{Z}$. Berechne die direkte Summe $\varrho_1 \oplus \varrho_2$ und das Tensorprodukt $\varrho_1 \otimes \varrho_2$ der beiden Matrixdarstellungen $\varrho_1, \varrho_2\colon G \to \mathrm{GL}(2,\mathbb{R})$, wobei

$$\varrho_1(\bar{1}) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \varrho_2(\bar{1}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

8. Komplexe Darstellungen endlicher Gruppen

8.1. **Zerlegung in irreduzible Darstellungen.**

Definition 8.1.1. Es sei G eine Gruppe.

(i) Ein G-Modul V heißt *einfach*, falls $\{0_V\}$ und V die einzigen G-Untermoduln von V sind.
(ii) Eine Darstellung $G \to \mathrm{Aut}(V)$ heißt *irreduzibel*, falls der zugehörige G-Modul V einfach ist.

Beispiel 8.1.2. Es sei G eine Gruppe. Dann ist jeder eindimensionale G-Modul einfach.

Beispiel 8.1.3. Es sei $G = \mathbb{Z}/2\mathbb{Z}$. Dann wird der $\mathbb{R}$-Vektorraum $\mathbb{R}^2$ zu einem G-Modul durch

$$\overline{0} \cdot (x_1, x_2) := (x_1, x_2), \qquad \overline{1} \cdot (x_1, x_2) := (x_2, x_1).$$

Der G-Modul $\mathbb{R}^2$ ist nicht einfach, denn er besitzt nichttriviale echte G-Untermoduln, nämlich

$$\mathbb{R} \cdot (1, 1), \qquad \mathbb{R} \cdot (-1, 1).$$

Lemma 8.1.4 (Schur)**.** *Es seien G eine Gruppe, V sowie W einfache G-Moduln und $\varphi\colon V \to W$ ein G-Modulhomomorphismus.*

(i) *Es gilt $\varphi = 0$ oder φ ist ein Isomorphismus.*
(ii) *Gilt $V = W$ und besitzt φ einen Eigenwert λ, so gilt $\varphi = \lambda \cdot \mathrm{id}_V$.*

Insbesondere hat man $\varphi = \lambda \cdot \mathrm{id}_V$ mit $\lambda \in \mathbb{C}$ für jeden G-Modulendomorphismus $\varphi\colon V \to V$ eines endlichdimensionalen komplexen G-Moduls V.

Beweis. Zu (i). Wir betrachten die beiden G-Untermoduln $\mathrm{Kern}(\varphi) \subseteq V$ und $\mathrm{Bild}(\varphi) \subseteq W$. Da V und W einfache G-Moduln sind, haben wir folgende Möglichkeiten:

$$\mathrm{Kern}(\varphi) = \{0_V\},\ \mathrm{Kern}(\varphi) = V, \qquad \mathrm{Bild}(\varphi) = \{0_W\},\ \mathrm{Bild}(\varphi) = W.$$

Gilt $\mathrm{Kern}(\varphi) = V$, so gilt $\varphi = 0$. Es sei $\mathrm{Kern}(\varphi) = \{0_V\}$. Gilt $\mathrm{Bild}(\varphi) = \{0_W\}$, so haben wir wieder $\varphi = 0$. Gilt $\mathrm{Bild}(\varphi) = W$, so ist φ injektiv und surjektiv. Folglich ist φ ein Isomorphismus von G-Moduln.

Zu (ii). Es sei λ ein Eigenwert von φ. Dann ist $\psi := \varphi - \lambda \cdot \mathrm{id}_V$ ein G-Modulhomomorphismus und ψ ist nicht injektiv. Nach (i) gilt daher $\psi = 0$. Es folgt $\varphi = \lambda \cdot \mathrm{id}_V$. □

Definition 8.1.5. Es sei G eine Gruppe.

(i) Ein G-Modul V heißt *halbeinfach*, falls $V = V_1 \oplus \ldots \oplus V_r$ mit einfachen G-Untermoduln $V_1, \ldots, V_r \subseteq V$ gilt.
(ii) Eine Darstellung $G \to \mathrm{Aut}(V)$ heißt *vollständig reduzibel* falls der zugehörige G-Modul V halbeinfach ist.

Satz 8.1.6. *Es seien G eine Gruppe und V ein endlichdimensionaler G-Modul. Dann sind folgende Aussagen äquivalent:*

(i) *Der G-Modul V ist halbeinfach.*
(ii) *Jeder G-Untermodul $U \subseteq V$ erlaubt einen G-Untermodul $U' \subseteq V$ mit $V = U \oplus U'$.*

Beweis. Zur Implikation "(i)⇒(ii)". Es sei $U \subseteq V$ ein G-Untermodul. Wir führen den Existenznachweis von U' aus (ii) durch Induktion über

$$d \;:=\; \dim(V) \;-\; \dim(U).$$

Für $d = 0$ ist $U' = \{0_V\}$ wie gewünscht. Für den Induktionsschritt sei $d > 0$. Wir schreiben

$$V \;=\; V_1 \oplus \ldots \oplus V_r.$$

mit einfachen G-Untermoduln $V_i \subseteq V$. Dabei dürfen wir $V_1 \not\subseteq U$ annehmen. Da V_1 einfach ist, haben wir dann $U \cap V_1 = \{0_V\}$. Das bedeutet

$$W \;:=\; U + V_1 \;=\; U \oplus V_1.$$

Die Induktionsvoraussetzung liefert einen G-Untermodul $W' \subseteq V$ mit $V = W \oplus W'$. Mit $U' := V_1 + W'$ erhalten wir dann

$$V \;=\; W \oplus W' \;=\; U \oplus V_1 \oplus W' \;=\; U \oplus U'.$$

Zur Implikation "(ii)⇒(i)". Wir wählen einen halbeinfachen G-Untermodul $U \subseteq V$ maximaler Dimension. Weiter sei $U' \subseteq V$ ein G-Untermodul mit

$$V \;=\; U \oplus U'.$$

Wir zeigen $U' = \{0_V\}$. Dazu wählen wir einen G-Untermodul $\{0_V\} \neq U'' \subseteq U'$ minimaler Dimension. Dann ist U'' einfach. Damit ist

$$U + U'' \;=\; U \oplus U''$$

ein halbeinfacher G-Untermodul von V mit $\dim(U + U'') > \dim(U)$. Das widerspricht der Wahl von $U \subseteq V$. □

Satz 8.1.7 (Maschke)**.** *Es seien G eine endliche Gruppe, $\mathbb{K}$ ein Körper mit* $\mathrm{Char}(\mathbb{K}) \not| \, |G|$ *und V ein endlichdimensionaler $\mathbb{K}$-Vektorraum. Dann ist jede Darstellung $\varrho\colon G \to \mathrm{Aut}(V)$ vollständig reduzibel.*

Beweis. Nach Satz 8.1.6 genügt es zu zeigen, dass zu jedem G-Untermodul $U \subseteq V$ ein G-Untermodul $U' \subseteq V$ existiert, sodass

$$V \;=\; U \;\oplus\; U'.$$

Da V endlichdimensional ist, finden wir zunächst einen Untervektorraum $V' \subseteq V$, mit dem wir eine direkte Zerlegung erhalten:

$$V \;=\; U \;\oplus\; V'.$$

Die zugehörige lineare Projektion $P\colon V \to U, (u, v') \mapsto u$ erfüllt insbesindere $P|_U = \mathrm{id}_U$ Wir betrachten nun die lineare Abbildung

$$\overline{P}\colon V \;\to\; U, \qquad v \;\mapsto\; \frac{1}{|G|} \sum_{g \in G} g \cdot P(g^{-1} \cdot v).$$

Da $U \subseteq V$ ein G-Untermodul ist, haben wir dabei tatsächlich $\overline{P}(V) \subseteq U$. Für jedes $u \in U$ gilt weiter

$$\overline{P}(u) \;=\; \frac{1}{|G|} \sum_{g \in G} g \cdot P(g^{-1} \cdot u) \;=\; \frac{1}{|G|} \sum_{g \in G} g \cdot (g^{-1} \cdot u) \;=\; \frac{1}{|G|} \sum_{g \in G} u \;=\; u.$$

Das bedeutet $\overline{P}|_U = \mathrm{id}_U$. Insbesondere folgen $\overline{P}(V) = U$ und $\overline{P}^2 = \overline{P}$. Mit $U' := \mathrm{Kern}(\overline{P})$ hat man daher eine direkte Zerlegung

$$V \;=\; \mathrm{Bild}(\overline{P}) \oplus \mathrm{Kern}(\overline{P}) \;=\; U \oplus U'.$$

Um zu sehen, dass $U' \subseteq V$ ein G-Untermodul ist, zeigen wir dass $\overline{P}$ ein G-Modulhomomorphismus ist. Für alle $h \in G$ und $v \in V$ gilt

$$\begin{aligned}
\overline{P}(h \cdot v) &= \frac{1}{|G|} \sum_{g \in G} g \cdot P(g^{-1} \cdot h \cdot v) \\
&= \frac{1}{|G|} \sum_{g \in G} hgh^{-1} \cdot P((hgh^{-1})^{-1} \cdot h \cdot v) \\
&= h \cdot \left(\frac{1}{|G|} \sum_{g \in G} gh^{-1} \cdot P(hg^{-1} \cdot v) \right) \\
&= h \cdot \left(\frac{1}{|G|} \sum_{g \in G} g \cdot P(g^{-1} \cdot v) \right) \\
&= h \cdot \overline{P}(v).
\end{aligned}$$

□

Beispiel 8.1.8. Wir betrachten $G = \mathbb{Z}/2\mathbb{Z}$ und $\mathbb{R}^2$ mit der G-Modulstruktur

$$\overline{0} \cdot (x_1, x_2) \ := \ (x_1, x_2), \qquad \overline{1} \cdot (x_1, x_2) \ := \ (x_2, x_1).$$

Dann ist der G-Modul $\mathbb{R}^2$ halbeinfach. Eine explizite Zerlegung in einfache G-Untermoduln ist gegeben durch

$$\mathbb{R}^2 \ = \ \mathbb{R} \cdot (1,1) \oplus \mathbb{R} \cdot (-1,1).$$

Beispiel 8.1.9. Wir betrachten den Körper $\mathbb{K} := \mathbb{Z}/2\mathbb{Z}$ und die Gruppe $G := \mathbb{Z}/2\mathbb{Z}$. Dann wir $\mathbb{K}^2$ zu einem G-Modul durch

$$\overline{0} \cdot (x_1, x_2) \ := \ (x_1, x_2), \qquad \overline{1} \cdot (x_1, x_2) \ := \ (x_2, x_1).$$

Der G-Modul $\mathbb{K}^2$ ist nicht einfach. Wir betrachten den eindimensionalen G-Untermodul

$$U \ := \ \mathbb{K}(\overline{1}, \overline{1}) \ = \ \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1})\} \ \subseteq \ \mathbb{K}^2.$$

Dazu gibt es keinen G-Untermodul $U' \subseteq \mathbb{K}^2$ mit $\mathbb{K}^2 = U \oplus U'$. Wir haben zwar

$$\mathbb{K}(\overline{1}, \overline{0}) \ = \ \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0})\}, \qquad \mathbb{K}(\overline{0}, \overline{1}) \ = \ \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1})\}$$

als weitere mögliche eindimensionale Untervektorräume von $\mathbb{K}^2$, aber keiner davon ist ein G-Untermodul.

Lemma 8.1.10. *Es seien G eine abelsche Gruppe und V ein nichttrivialer, endlichdimensionaler, einfacher, komplexer G-Modul. Dann gilt* $\dim(V) = 1$

Beweis. Wir zeigen zunächst, dass jede Translation $T_g \colon V \to V$ ein G-Modulhomomorphismus ist. Da G abelsch ist, haben wir für alle $h \in G$ und $v \in V_\lambda$:

$$T_g(h \cdot v) \ = \ g \cdot h \cdot v \ = \ gh \cdot v \ = \ hg \cdot v \ = \ h \cdot g \cdot v \ = \ h \cdot T_g(v)$$

Nach dem Lemma von Schur ist daher jedes T_g ein Vielfaches von id_V. Somit ist jede Gerade $\mathbb{C}v \subseteq V$ ein G-Untermodul. Da V einfach ist, gilt $V = \mathbb{C}v$. □

Satz 8.1.11. *Es seien G eine endliche abelsche Gruppe, und V ein nichttrivialer, endlichdimensionaler, komplexer G-Modul. Dann ist V eine direkte Summe von eindimensionalen G-Untermoduln.*

Beweis. Nach Satz 8.1.7 ist V halbeinfach und somit eine direkte Summe einfacher G-Untermoduln $V_1, \ldots, V_r$. Nach Lemma 8.1.10 ist jedes V_i eindimensional. □

Folgerung 8.1.12. *Es seien $G = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$ und $\varrho\colon G \to \mathrm{GL}(m;\mathbb{C})$ eine Matrixdarstellung. Dann gibt es Einheitswurzeln $\zeta_{ji} \in \mathrm{EW}_{n_i}$, wobei $j = 1, \ldots m$, und $i = 1, \ldots, r$, sodass ϱ äquivalent ist zu der Matrixdarstellung*

$$G \;\to\; \mathrm{GL}(m;\mathbb{C}), \qquad (\overline{k}_1, \ldots, \overline{k}_r) \;\mapsto\; \begin{pmatrix} \zeta_{11}^{k_1} \cdots \zeta_{1r}^{k_r} & & 0 \\ & \ddots & \\ 0 & & \zeta_{m1}^{k_1} \cdots \zeta_{mr}^{k_r} \end{pmatrix}.$$

Beweis. Nach Satz 8.1.11 ist der zugehörige G-Modul $\mathbb{K}^n$ eine direkte Summe eindimensionaler G-Moduln $V_1, \ldots, V_n$. Nach Satz 7.3.15 operiert G auf jedem V_j durch $(\overline{k}_1, \ldots, \overline{k}_r) \cdot v_j = \zeta_{j1}^{k_1} \cdots \zeta_{jr}^{k_r}$ mit Einheitswurzeln ζ_{ji} wie in der Behauptung. □

Aufgaben zu Abschnitt 8.1.

Aufgabe 8.1.13. Es sei $\mathbb{K}$ ein Körper mit $\mathrm{Char}(\mathbb{K}) = 0$. Betrachte die Matrixdarstellung der symmetrischen Gruppe

$$\varrho\colon S_n \ \to\ \mathrm{GL}(n;\mathbb{K}), \qquad \sigma \ \mapsto\ A_\sigma := (e_{\sigma(1)},\ldots,e_{\sigma(n)})$$

aus Aufgabe 7.3.19. Zeige dass man eine Zerlegung $\mathbb{K}^n = U \oplus V$ in einfache G-Untermoduln erhält mit

$$U \ :=\ \mathbb{K}\cdot(1_\mathbb{K},\ldots,1_\mathbb{K}), \qquad V \ :=\ \{x \in \mathbb{K}^n;\ x_1 + \ldots + x_n = 0_\mathbb{K}\}.$$

Hinweis: Es sei $\{0_V\} \neq U \subseteq V$ ein S_n-Untermodul. Wähle $0_V \neq (x_1,\ldots,x_n) \in U$ und zeige:

- Es gibt ein $2 \leq i \leq n$ mit $x_i \neq x_1$,
- es gilt $e_1 - e_i \in U$,
- es gilt $e_1 - e_j \in U$ für $j = 2,\ldots,n$.

Schliesse daraus $U = V$. Wo wird in dieser Aufgabe überall die Voraussetzung $\mathrm{Char}(\mathbb{K}) = 0$ verwendet?

Aufgabe 8.1.14. Betrachte die Gruppe $\mathrm{B}(2;\mathbb{C}) \leq \mathrm{GL}(2;\mathbb{C})$ aller invertierbaren oberen Dreiecksmatrizen und die Operation

$$\mathrm{B}(2;\mathbb{C}) \times \mathbb{C}^2 \ \to\ \mathbb{C}^2, \qquad (A,v) \ \mapsto A\cdot v$$

mittels Matrix-Vektormultiplikation. Zeige, dass der so definierte $\mathrm{B}(2;\mathbb{C})$-Modul $\mathbb{C}^2$ nicht halbeinfach ist.

8.2. **Der Charakter einer komplexen Darstellung.**

Erinnerung 8.2.1. Es seien $\mathbb{K}$ ein Körper und $A = (a_{ij}) \in \mathrm{Mat}(n,n;\mathbb{K})$ eine Matrix. Die *Spur* von A ist die Summe ihrer Diagonalelemente:

$$\mathrm{Spur}(A) \;:=\; a_{11} + \ldots + a_{nn}.$$

Die Spur ist invariant unter Konjugation mit invertierbaren Matrizen: Für jedes $S \in \mathrm{GL}(n,\mathbb{K})$ gilt

$$\mathrm{Spur}(S \cdot A \cdot S^{-1}) \;=\; \mathrm{Spur}(A).$$

Damit kann man auch Endomorphismen $\varphi\colon V \to V$ endlichdimensionaler $\mathbb{K}$-Vektorräume eine *Spur* zuordnen: Man wählt eine Basis $\mathcal{B}$ von V und setzt

$$\mathrm{Spur}(\varphi) \;:=\; \mathrm{Spur}(M_{\mathcal{B}}^{\mathcal{B}}(\varphi)),$$

wobei $M_{\mathcal{B}}^{\mathcal{B}}(\varphi)$ die darstellende Matrix von φ bezüglich $\mathcal{B}$ bezeichnet. Nach obiger Anmerkung hängt die Spur nicht von der Wahl der Basis $\mathcal{B}$ ab.

Definition 8.2.2. Es sei G eine endliche Gruppe.

(i) Der *Charakter* einer Matrixdarstellung $\varrho\colon G \to \mathrm{GL}(n;\mathbb{C})$ ist die Abbildung

$$\chi_\varrho\colon G \;\to\; \mathbb{C}, \qquad g \;\mapsto\; \mathrm{Spur}(\varrho(g)).$$

(ii) Es sei V ein endlichdimensionaler $\mathbb{C}$-Vektorraum. Der *Charakter* einer Darstellung $\varrho\colon G \to \mathrm{Aut}(V)$ ist die Abbildung

$$\chi_\varrho\colon G \;\to\; \mathbb{C}, \qquad g \;\mapsto\; \mathrm{Spur}(\varrho(g)).$$

Beispiel 8.2.3. Wir betrachten die Gruppe $G := \mathbb{Z}/2\mathbb{Z}$ und die Matrixdarstellungen $\varrho_i\colon G \to \mathrm{GL}(2;\mathbb{C})$, wobei

$$\varrho_1\colon \quad \overline{0} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \overline{1} \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\varrho_2\colon \quad \overline{0} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \overline{1} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\varrho_3\colon \quad \overline{0} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \overline{1} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Die zu diesen Matrixdarstellungen gehörigen Charaktere $\varrho_i\colon G \to \mathbb{C}$ sind gegeben durch

$$\chi_{\varrho_1}(\overline{0}) \;=\; 2, \qquad \chi_{\varrho_1}(\overline{1}) \;=\; -2,$$

$$\chi_{\varrho_2}(\overline{0}) \;=\; 2, \qquad \chi_{\varrho_2}(\overline{1}) \;=\; 0,$$

$$\chi_{\varrho_3}(\overline{0}) \;=\; 2, \qquad \chi_{\varrho_3}(\overline{1}) \;=\; 0.$$

Satz 8.2.4. *Es seien $\varrho\colon G \to \mathrm{Aut}(V)$ und $\sigma\colon G \to \mathrm{Aut}(W)$ Darstellungen einer endlichen Gruppe G auf endlichdimensionalen $\mathbb{C}$-Vektorräumen. Dann gilt:*

$$\varrho \;\sim\; \sigma \quad\Longrightarrow\quad \chi_\varrho \;=\; \chi_\sigma.$$

Beweis. Sind ϱ und σ äquivalente Darstellungen, so existiert ein Isomorphismus $\varphi\colon V \to W$ der zugehörigen G-Moduln. Das bedeutet

$$\sigma(g) \;=\; \varphi \circ \varrho(g) \circ \varphi^{-1}$$

für jedes $g \in G$. Wählt man nun Basen $\mathcal{B}$ für V sowie $\mathcal{C}$ für W, so ergibt sich für die zugehörigen darstellenden Matrizen

$$M_{\mathcal{C}}^{\mathcal{C}}(\sigma(g)) \;=\; M_{\mathcal{C}}^{\mathcal{C}}(\varphi \circ \varrho(g) \circ \varphi^{-1}) \;=\; M_{\mathcal{C}}^{\mathcal{B}}(\varphi) \cdot M_{\mathcal{B}}^{\mathcal{B}}(\varrho(g)) \cdot M_{\mathcal{C}}^{\mathcal{B}}(\varphi)^{-1}.$$

Wie in Erinnerung 8.2.1 vermerkt, ist die Spur invariant unter Konjugation. Damit erhalten wir $\chi_\sigma = \chi_\varrho$. □

Satz 8.2.5. *Es seien G eine endliche Gruppe, V ein endlichdimensionaler $\mathbb{C}$-Vektorraum und $\varrho\colon G \to \mathrm{Aut}(V)$ eine Darstellung. Dann gilt für alle $g, h \in G$:*

$$\chi_\varrho(e_G) \;=\; \dim(V), \qquad \chi_\varrho(g^{-1}) \;=\; \overline{\chi_\varrho(g)}, \qquad \chi_\varrho(hgh^{-1}) \;=\; \chi_\varrho(g).$$

Lemma 8.2.6. *Es seien G eine endliche Gruppe, V ein n-dimensionaler $\mathbb{C}$-Vektorraum und $\varrho\colon G \to \mathrm{Aut}(V)$ eine Darstellung. Zu jedem $g \in G$ gibt es m-te Einheitswurzeln $\zeta_1, \ldots, \zeta_n \in \mathbb{C}$, wobei $m := \mathrm{ord}(g)$, und eine Basis $\mathcal{B}$ für V mit*

$$M_{\mathcal{B}}^{\mathcal{B}}(\varrho(g)) \;=\; \begin{pmatrix} \zeta_1 & & 0 \\ & \ddots & \\ 0 & & \zeta_n \end{pmatrix}.$$

Beweis. Wir betrachten die von g erzeugte Untergruppe $H \leq G$. Es gilt $H \cong \mathbb{Z}/m\mathbb{Z}$ und Einschränken von ϱ liefert eine Darstellung $H \to \mathrm{Aut}(V)$. Nach Satz 8.1.11 ist V eine direkte Summe eindimensionaler H-Moduln $V_1, \ldots, V_r$ und auf jedem V_i haben wir $g \cdot v_i = \zeta_i v_i$ mit einer m-ten Einheitswurzel ζ_i; siehe Lemma 7.3.16. □

Beweis. Wir setzen $n := \dim(V)$ und $m := |G|$. Die erste Gleichung erhalten wir sofort mit

$$\chi_\varrho(e_G) \;=\; \mathrm{Spur}(\mathrm{id}_V) \;=\; \mathrm{Spur}(E_n) \;=\; n.$$

Für die zweite Gleichung wählen wir zu gegebenem $g \in G$ eine Basis $\mathcal{B}$ für V wie in Lemma 8.2.6. Damit erhalten wir

$$\begin{aligned} \chi_\varrho(g^{-1}) &= \mathrm{Spur}(\varrho(g^{-1})) \\ &= \mathrm{Spur}(\varrho(g)^{-1}) \\ &= \zeta_1^{-1} + \ldots + \zeta_n^{-1} \\ &= \overline{\zeta_1} + \ldots + \overline{\zeta_n} \\ &= \overline{\zeta_1 + \ldots + \zeta_n} \\ &= \overline{\mathrm{Spur}(\varrho(g))} \\ &= \overline{\chi_\varrho(g)}. \end{aligned}$$

Die dritte Gleichung erhält man wieder durch eine leichte Rechnung. Für je zwei $g, h \in G$ ergibt sich

$$\chi_\varrho(hgh^{-1}) \;=\; \mathrm{Spur}(\varrho(h)\varrho(g)\varrho(h)^{-1}) \;=\; \mathrm{Spur}(\varrho(g)) \;=\; \chi_\varrho(g).$$

□

Satz 8.2.7. *Es seien $\varrho\colon G \to \mathrm{GL}(V)$ und $\sigma\colon G \to \mathrm{GL}(W)$ Darstellungen einer endlichen Gruppe auf komplexen Vektorräumen V bzw. W.*

(i) *Der Charakter $\chi_{\varrho\oplus\sigma}$ der direkten Summe $\varrho \oplus \sigma\colon G \to \mathrm{Aut}(V \oplus W)$ ist gegeben durch*

$$\chi_{\varrho\oplus\sigma}(g) \;=\; \chi_\varrho(g) + \chi_\sigma(g).$$

(ii) *Der Charakter $\chi_{\varrho\otimes\sigma}$ des Tensorproduktes $\varrho \otimes \sigma\colon G \to \mathrm{Aut}(V \otimes W)$ ist gegeben durch*

$$\chi_{\varrho\otimes\sigma}(g) \;=\; \chi_\varrho(g) \cdot \chi_\sigma(g).$$

(iii) *Der Charakter χ_{ϱ^*} der zu ϱ dualen Darstellung $\varrho^*\colon G \to \mathrm{Aut}(V^*)$ ist gegeben durch*

$$\chi_{\varrho^*}(g) \;=\; \overline{\chi_\varrho(g)}.$$

(iv) *Der Charakter χ_τ der durch ϱ und σ definierten Darstellung $\tau\colon G \to \mathrm{Aut}(\mathrm{Hom}(V,W))$ ist gegeben durch*

$$\chi_\tau(g) \;=\; \overline{\chi_\varrho(g)}\chi_\sigma(g).$$

Beweis. Es sei $g \in G$ gegeben. Lemma 8.2.6 liefert uns Basen $(v_1,\ldots,v_n)$ für V und $(w_1,\ldots,w_m)$ für W, sodass

$$\varrho(g)(v_i) \;=\; \zeta_i v_i, \qquad \sigma(g)(w_j) \;=\; \eta_j w_j$$

gilt mit komplexen Einheitswurzeln $\zeta_1,\ldots,\zeta_n$ und $\eta_1,\ldots,\eta_m$. Damit können wir die Aussagen beweisen.

Zu (i). Für die Elemente der Basis $((v_1,0_W),\ldots,(v_n,0_W),(0_V,w_1),\ldots,(0_V,w_m))$ der direkten Summe $V \oplus W$ haben wir

$$g\cdot(v_i,0_W) \;=\; \zeta_i(v_i,0_W), \qquad g\cdot(0_V,w_j) \;=\; \eta_j(0_V,w_j).$$

Somit besitzt $\varrho\oplus\sigma(g)$ bezüglich der obigen Basis Diagonalgestalt mit den Diagonaleinträgen $\zeta_1,\ldots,\zeta_n,\eta_1,\ldots,\eta_m$. Es folgt

$$\chi_{\varrho\oplus\sigma}(g) \;=\; \zeta_1+\ldots+\zeta_n+\eta_1+\ldots+\eta_m \;=\; \chi_\varrho(g)+\chi_\sigma(g).$$

Zu (ii). Die Vektoren der Form $v_i\otimes w_j$ mit $1\le i\le n$ und $1\le j\le m$ bilden eine Basis für das Tensorprodukt $V\otimes W$. Es gilt

$$g\cdot(v_i\otimes w_j) \;=\; g\cdot v_i\otimes g\cdot w_j \;=\; \zeta_i v_i\otimes\eta_j w_j \;=\; (\zeta_i\eta_j)(v_i\otimes w_j).$$

Also besitzt die darstellende Matrix von $(\varrho\otimes\sigma)(g)$ bezüglich der oben angegebenen Basis Diagonalgestalt mit Diagonaleinträgen $\zeta_i\eta_j$. Es folgt

$$\chi_{\varrho\otimes\sigma}(g) \;=\; \sum_{i,j}\zeta_i\eta_j \;=\; \left(\sum_i\zeta_i\right) \;=\; \chi_\varrho(g)\chi_\sigma(g).$$

Zu (iii). Nach Satz 8.2.5 gilt $\chi_\varrho(g^{-1}) = \overline{\chi_\varrho(g)}$ für jedes $g\in G$. Mit $A := M_{\mathcal{B}}^{\mathcal{B}}(\varrho(g))$ erhalten wir

$$\chi_{\varrho^*}(g) \;=\; \mathrm{Spur}(\varrho^*(g)) \;=\; \mathrm{Spur}((A^{-1})^t) \;=\; \mathrm{Spur}(A^{-1}) \;=\; \chi_\varrho(g^{-1}) \;=\; \overline{\chi_\varrho(g)}.$$

Aussage (iv) ergibt sich sofort aus den Aussagen (ii) und (iii) sowie der Tatsache, dass $\mathrm{Hom}(V,W)$ nach Satz 7.4.12 als G-Modul isomorph zu $V^*\otimes W$ ist. □

Erinnerung 8.2.8. Es sei X eine endliche Menge. Durch punkteweise Addition und Skalarmultiplikation wird die Menge

$$V_X \;:=\; \mathrm{Abb}(X,\mathbb{C})$$

der komplexwertigen Funktionen auf X zu einem $\mathbb{C}$-Vektorraum. Es gilt $\dim(V_X) = |X|$; eine Basis bilden beispielsweise die charakteristischen Funktionen

$$f_x\colon X \;\to\; \mathbb{C}, \qquad x' \;\mapsto\; \delta_{x,x'} \;=\; \begin{cases}1, & \text{falls } x'=x,\\ 0, & \text{falls } x'\neq x.\end{cases}$$

Konstruktion 8.2.9. Es sei $G\times X\to X$ eine Operation einer endlichen Gruppe G auf einer endlichen Menge X. Dann V_X zu einem G-Modul durch

$$G\times V_X \;\to\; V_X, \qquad (g\cdot f)(x) \;:=\; f(g^{-1}\cdot x).$$

Die zugehörige Darstellung $\varrho_X\colon G\to \mathrm{GL}(V_X)$ nennt man die durch die Operation $G\times X\to X$ definierte *Permutationsdarstellung*.

Satz 8.2.10. *Es sei $G \times X \to X$ eine Operation einer endlichen Gruppe G auf einer endlichen Menge X. Dann ist der Charakter $\chi_X\colon G \to \mathbb{C}$ der zugehörigen Permutationsdarstellung $\varrho_X\colon G \to \mathrm{GL}(V_X)$ gegeben durch*

$$\chi_X(g) \quad = \quad |\{x \in X;\ g \cdot x = x\}|.$$

Beweis. Es sei $g \in G$ gegeben. Wir wollen die darstellende Matrix von $\varrho_X(g)$ bezüglich einer Basis aus charakteristischen Funktionen bestimmen. Für die charakteristische Funktion f_x eines Punktes $x \in X$ gilt:

$$(g \cdot f_x)(x') \ = \ f_x(g^{-1} \cdot x') \ = \ \delta(x, g^{-1} \cdot x') \ = \ \delta(g \cdot x, x') \ = \ f_{g \cdot x}(x').$$

Das bedeutet $g \cdot f_x = f_{g \cdot x}$. Wir bezeichnen nun mit $x_1, \ldots, x_r \in X$ diejenigen Punkte, sodass $g \cdot x_i = x_i$ gilt und $y_1, \ldots, y_s \in X$ diejenigen Punkte, die $g \cdot y_j \neq y_j$ erfüllen. Dann haben wir eine disjunkte Zerlegung

$$X \quad = \quad \{x_1, \ldots, x_r\} \ \cup \ \{y_1, \ldots, y_s\}.$$

Mit den zugehörigen charakteristischen Funktionen f_{x_i} und f_{y_j} erhalten wir dann eine Basis $\mathcal{B} = (f_{x_1}, \ldots, f_{x_r}, f_{y_1}, \ldots, f_{y_s})$ für V_X. Wie oben gesehen, gilt stets

$$g \cdot f_{x_i} = f_{g \cdot x_i} = f_{x_i}, \qquad g \cdot f_{y_j} = f_{g \cdot y_j} = f_{y_k},\ k \neq j.$$

Damit sehen wir, dass die darstellende Matrix von $\varrho_X(g)$ bezüglich der Basis $\mathcal{B}$ die folgende Blockdiagonalgestalt besitzt. Genauer gilt

$$M_{\mathcal{B}}^{\mathcal{B}}(\varrho_X(g)) \quad = \quad \begin{pmatrix} E_r & 0 \\ 0 & A \end{pmatrix}$$

mit einer $(s \times s)$-Matrix A. Wegen $g \cdot f_{y_j} = f_{y_k}$ mit $k \neq j$ verschwinden alle Diagonaleinträge der Matrix A. Damit erhalten wir

$$\chi_X(g) \ = \ \mathrm{Spur}(M_{\mathcal{B}}^{\mathcal{B}}(\varrho_X(g))) \ = \ r \ = \ |\{x \in X;\ g \cdot x = x\}|.$$

□

Definition 8.2.11. Es sei G eine endliche Gruppe. Die *reguläre Darstellung* von G ist die Permutationsdarstellung $\varrho_G\colon G \to \mathrm{GL}(V_G)$ der Operation

$$G \times G \ \to \ G, \qquad h \cdot g \ := \ hg.$$

Satz 8.2.12. *Es sei G eine endliche Gruppe. Dann ist der Charakter χ_G der regulären Darstellung $\varrho_G\colon G \to \mathrm{GL}(V_G)$ gegeben durch*

$$\chi_G(g) \quad = \quad \begin{cases} |G| & \text{falls } g = e_G, \\ 0 & \text{falls } g \neq e_G. \end{cases}$$

Beweis. Die Aussage ist eine direkte Folgerung aus Satz 8.2.10: Das neutrale Element leistet $e_G \cdot g = g$ für alle $g \in G$, und für jedes von e_G verschiedene $h \in G$ hat man $h \cdot g \neq g$ für alle $g \in G$. □

Aufgaben zu Abschnitt 8.2.

Aufgabe 8.2.13. Zeige: Für jede eindimensionale Darstellung ϱ gilt $\chi_\varrho(g) = \varrho(g)$. Insbesondere ist χ_ϱ ein Gruppenhomomorphismus.

Aufgabe 8.2.14. Die symmetrische Gruppe S_n operiert auf der Menge $X_n = \{1, \ldots, n\}$ durch $\sigma \cdot i = \sigma(i)$. Betrachte $V_n := V_{X_n}$ und die zugehörige Permutationsdarstellung $\varrho_n \colon G \to \mathrm{Aut}(V_n)$. Zeige: Für jedes $\sigma \in S_n$ gilt

$$\mathcal{M}_{\mathcal{B}}^{\mathcal{B}}(\varrho_n(\sigma)) \;=\; A_\sigma,$$

wobei die Basis $\mathcal{B} = (f_1, \ldots, f_n)$ von V_n aus den charakteristischen Funktionen f_i zu $i \in X_n$ besteht und die Matrix $A_\sigma = (e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ wie in Aufgabe 7.3.19 definiert ist. Zeige weiter: Die Matrixdarstellungen $\sigma \mapsto \mathcal{M}_{\mathcal{B}}^{\mathcal{B}}(\varrho_n(\sigma))$ und $\sigma \mapsto A_\sigma$ sind äquivalent.

Aufgabe 8.2.15. Bestimme explizit die Charaktere der Permutationsdarstellungen von S_3 und S_4. *Hinweis:* Zur Bestimmung eines Charakters genügt es, ihn auf je einem Element pro Konjugationsklasse auszuwerten; siehe Satz 8.2.5.

8.3. **Orthogonalitätsrelationen.**

Erinnerung 8.3.1. Es sei G eine Gruppe. Die *Konjugationsklasse* eines Elements $g \in G$ ist die Teilmenge

$$\{hgh^{-1};\ h \in G\} \ \subseteq\ G.$$

Es bezeichne $\mathrm{C}(G)$ die Menge aller Konjugationsklassen von G. Dann haben wir eine surjektive Abbildung

$$\pi\colon G \ \to\ \mathrm{C}(G), \qquad g \ \mapsto\ \{hgh^{-1}; h \in G\}.$$

Definition 8.3.2. Es sei G eine endliche Gruppe. Eine *Klassenfunktion* auf G ist eine Abbildung $f\colon G \to \mathbb{C}$ mit $f(hgh^{-1}) = f(g)$ für alle $g, h \in G$. Die Menge aller Klassenfunktionen auf G bezeichnen wir mit $\mathrm{CF}(G)$.

Bemerkung 8.3.3. Es sei $\varrho\colon G \to \mathrm{Aut}(V)$ eine Darstellung einer endlichen Gruppe G auf einem endlichdimensionalen $\mathbb{C}$-Vektorraum V. Dann ist der Charakter $\chi_\varrho\colon G \to \mathbb{C}$, $g \mapsto \mathrm{Spur}(g)$ eine Klassenfunktion auf G; siehe Satz 8.2.5.

Bemerkung 8.3.4. Durch punktweise definierte Addition und Skalarmultiplikation gewinnt man die $\mathbb{C}$-Vektorräume

$$\mathrm{Abb}(\mathrm{C}(G), \mathbb{C}), \qquad \mathrm{CF}(G)\ \leq_{\mathbb{C}}\ \mathrm{Abb}(G, \mathbb{C}).$$

Mit der kanonischen Abbildung $\pi\colon G \to \mathrm{C}(G)$ erhalten wir einen Vektorraumisomorphismus

$$\mathrm{Abb}(\mathrm{C}(G), \mathbb{C})) \ \to\ \mathrm{CF}(G), \qquad \tilde{f} \ \mapsto\ \tilde{f} \circ \pi.$$

Insbesondere ist die Dimension von $\mathrm{CF}(G)$ gleich der Anzahl der Konjugationsklassen in G:

$$\dim(\mathrm{CF}(G)) \ =\ \dim(\mathrm{Abb}(\mathrm{C}(G), \mathbb{C})) \ =\ |\,\mathrm{C}(G)|.$$

Konstruktion 8.3.5. Es sei G eine endliche Gruppe. Dann erhält man ein hermitesches Skalarprodukt auf $\mathrm{CF}(G)$ durch

$$\langle f', f\rangle \ :=\ \frac{1}{|G|}\sum_{g\in G} f'(g)\overline{f(g)}.$$

Satz 8.3.6. *Es seien G eine endliche Gruppe, V, W endlichdimensionale komplexe Vektorräume und $\varrho\colon G \to \mathrm{Aut}(V)$ sowie $\sigma\colon G \to \mathrm{Aut}(W)$ irreduzible Darstellungen. Dann gilt:*

$$\langle \chi_\sigma, \chi_\varrho\rangle \ =\ \begin{cases} 1, & \text{falls } \varrho \sim \sigma, \\ 0, & \text{sonst.} \end{cases}$$

Lemma 8.3.7. *Es seien G eine endliche Gruppe und V ein eindlicimensionaler komplexer G-Modul. Dann ist*

$$P\colon V \ \to\ V, \qquad v \ \mapsto\ \frac{1}{|G|}\sum_{g\in G} g\cdot v$$

eine lineare Abbildung mit $P(V) = V^G$ und $P|_{V^G} = \mathrm{id}_{V^G}$. Insbesondere hat man die Zerlegung $V = V^G \oplus \mathrm{Kern}(P)$.

Beweis. Wir zeigen zunächst, dass tatsächlich $P(v) \in V^G$ für jedes $v \in V$ gilt. Für $h \in G$ erhält man

$$h\cdot P(v) \ =\ h\cdot\left(\frac{1}{|G|}\sum_{g\in G} g\cdot v\right) \ =\ \frac{1}{|G|}\sum_{g\in G} hg\cdot v \ =\ \frac{1}{|G|}\sum_{g\in G} g\cdot v \ =\ P(v).$$

Weiter ist P offensichtlich linear und auf V^G ist P die Identität. Damit ergibt sich $P(V) = V^G$ und $V = V^G \oplus \mathrm{Kern}(P)$. □

Beweis von Satz 8.3.6. Das Skalarprodukt der Charaktere zu den Darstellungen ϱ und σ ist gegeben durch

$$\langle \chi_\sigma, \chi_\varrho \rangle \;=\; \frac{1}{|G|} \sum_{g \in G} \chi_\sigma(g) \overline{\chi_\varrho(g)} \;=\; \frac{1}{|G|} \sum_{g \in G} \chi_\tau(g),$$

mit dem Charakter $\chi_\tau \colon G \to \mathbb{C}$, $g \mapsto \overline{\chi_\varrho(g)} \chi_\sigma(g)$ der durch ρ und σ induzierten Darstellung $\tau \colon G \to \mathrm{GL}(\mathrm{Hom}(V,W))$; siehe Satz 8.2.7. Wir erhalten

$$\langle \chi_\sigma, \chi_\varrho \rangle \;=\; \frac{1}{|G|} \sum_{g \in G} \mathrm{Spur}(\tau(g)) \;=\; \mathrm{Spur}\left(\frac{1}{|G|} \sum_{g \in G} \tau(g) \right) \;=\; \dim(\mathrm{Hom}(V,W)^G).$$

Die letzte Gleichung ergibt sich mit Lemma 8.3.7 angewandt auf den G-Modul $\mathrm{Hom}(V,W)$. Satz 7.4.12 liefert

$$\mathrm{Hom}(V,W)^G \;\cong\; \mathrm{Hom}_G(V,W).$$

Aussagen über den Vektorraum $\mathrm{Hom}_G(V,W)$ aller G-Modulhomomorphismen gibt das Lemma von Schur Auskunft. Damit erhalten wir

$$\langle \chi_\sigma, \chi_\varrho \rangle \;=\; \dim(\mathrm{Hom}_G(V,W)) \;=\; \begin{cases} 1, & \text{falls } \varrho \sim \sigma, \\ 0, & \text{sonst.} \end{cases}$$

□

Definition 8.3.8. Es sei G eine endliche Gruppe.

(i) Mit $\Omega(G)$ bezeichnen wir die Menge aller Äquivalenzklassen irreduzibler endlichdimensionaler komplexer Darstellungen von G.
(ii) Für jedes $\omega \in \Omega(G)$ fixieren wir eine irreduzible endlichdimensionale komplexe Darstellungen $\varrho_\omega \colon G \to \mathrm{Aut}(V_\omega)$ aus ω.
(iii) Wir schreiben $\chi_\omega \colon G \to \mathbb{C}$ für den Charakter von $\varrho_\omega \colon G \to \mathrm{Aut}(V_\omega)$, wobei $\omega \in \Omega(G)$. Wir sprechen auch von dem irreduziblen Charakter χ_ω.

Beispiel 8.3.9. Wir betrachten die Gruppe $G = \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_r\mathbb{Z}$. Dann ist jede irreduzible Darstellung von G eindimensional und haben wir eine Bijektion

$$\begin{aligned} \mathrm{EW}_{n_1} \times \ldots \times \mathrm{EW}_{n_r} &\to \Omega(G), \\ (\zeta_1, \ldots, \zeta_r) &\to [\varrho_{\zeta_1,\ldots,\zeta_r} \colon \overline{k}_1, \ldots, \overline{k}_r) \to (\zeta_1^{k_1} \cdots \zeta_r^{k_r})]. \end{aligned}$$

Bemerkung 8.3.10. Es sei G eine endliche Gruppe. Für je zwei Äquivalenzklassen $\omega_1, \omega_2 \in \Omega(G)$ haben wir

$$\omega_1 = \omega_2 \iff \varrho_{\omega_1} \sim \varrho_{\omega_2}.$$

Mit Satz 8.3.6 ergibt sich

$$\langle \chi_{\omega_1}, \chi_{\omega_2} \rangle \;=\; \begin{cases} 1, & \omega_1 = \omega_2, \\ 0, & \omega_1 \neq \omega_2. \end{cases}$$

Folglich ist Familie $(\chi_\omega;\ \omega \in \Omega(G))$ linear unabhängig im Vektorraum $\mathrm{CF}(G)$ der Klassenfunktionen. Es folgt

$$|\Omega(G)| \;\leq\; \dim(\mathrm{CF}(G)) \;=\; |\,\mathrm{C}(G)|.$$

Satz 8.3.11. *Es seien G eine endliche Gruppe, V ein endlichdimensionaler G-Modul und $\varrho \colon G \to \mathrm{Aut}(V)$ die zugehörige Darstellung. Dann hat man einen Isomorphismus von G-Moduln*

$$V \;\cong\; \bigoplus_{\omega \in \Omega(G)} V_\omega^{\langle \chi_\omega, \chi_\varrho \rangle}.$$

Beweis. Nach dem Satz von Maschke ist der G-Modul V halbeinfach. Man hat also eine direkte Zerlegung

$$V \;=\; V_1 \oplus \ldots \oplus V_r$$

mit einfachen G-Untermoduln $V_i \subseteq V$. Bezeichnen wir mit $\varrho_i \colon G \to \mathrm{Aut}(V_i)$ die zugehörigen Darstellungen, so hat man entsprechend

$$\chi_\varrho \;=\; \chi_{\varrho_1} + \ldots + \chi_{\varrho_r}.$$

Jedes der V_i ist isomorph zu einem V_ω mit $\omega \in \Omega(G)$. Wir müssen nun zu gegebenem $\omega \in \Omega$ die Anzahl s_ω der ϱ_i mit $\varrho_i \sim \omega$ bestimmen. Nach Satz 8.3.6 gilt

$$s_\omega \;=\; \langle \chi_\omega, \chi_{\varrho_1} \rangle + \ldots + \langle \chi_\omega, \chi_{\varrho_r} \rangle \;=\; \langle \chi_\omega, \chi_\varrho \rangle.$$

□

Definition 8.3.12. Es seien G eine endliche Gruppe und $\varrho \colon G \to \mathrm{Aut}(V)$ eine Darstellung auf einem endlichdimensionalen $\mathbb{C}$-Vektoraum V. Man nennt

$$V \;\cong \bigoplus_{\omega \in \Omega(G)} V_\omega^{\langle \chi_\omega, \chi_\varrho \rangle}$$

aus Satz 8.3.11 die *isotypische Zerlegung* des G-Moduls V; dabei heißt $\langle \chi_\omega, \chi_\varrho \rangle$ die *Vielfachheit*, auch *Multiplizität* der isotypischen Komponente V_ω in V.

Folgerung 8.3.13. *Es sei G eine endliche Gruppe. Für je zwei endlichimensionale komplexe Darstellungen $\varrho \colon G \to \mathrm{Aut}(V)$ und $\varrho' \colon G \to \mathrm{Aut}(V')$, gilt*

$$\varrho' \sim \varrho \iff \chi_{\varrho'} = \chi_\varrho.$$

Beweis. Falls $\varrho' \sim \varrho$ gilt, so liefert Satz 8.2.4 die Gleichheit der zugehörigen Charaktere. Gilt $\chi_{\varrho'} = \chi_\varrho$, so besitzen die G-Moduln V' und V dieselbe isotypische Zerlegung und sind daher isomorph zueinander. □

Erinnerung 8.3.14. Es sei G eine endliche Gruppe. Der Vektorraum $V_G = \mathrm{Abb}(G, \mathbb{C})$ aller komplexwertigen Funktionen auf G wird zu einem G-Modul durch

$$(h \cdot f)(g) \;:=\; f(h^{-1}g).$$

Die zugehörige Darstellung $\varrho_G \colon G \to \mathrm{Aut}(V_G)$ nennt man die *reguläre Darstellung* von G auf V_G. Für die charakteristischen Funktionen f_g zu $g \in G$ haben wir.

$$(h \cdot f_g)(g') \;=\; f_g(h^{-1}g') \;=\; \delta(g, h^{-1}g') \;=\; \delta(hg, g') \;=\; f_{hg}(g').$$

Das bedeutet $h \cdot f_g = f_{hg}$. Die reguläre Darstellung permutiert also die charakteristischen Funktionen. Der Charakter con ϱ_G ist gegeben durch

$$\chi_G(g) \;=\; \begin{cases} |G|, & \text{falls } g = e_G, \\ 0, & \text{falls } g \neq e_G. \end{cases}$$

Satz 8.3.15. *Es sei G eine endliche Gruppe. Betrachte die reguläre Darstellung $\varrho_G \colon G \to \mathrm{Aut}(V_G)$ aus 8.2.11.*

(i) *Für jede Darstellung $\varrho \colon G \to \mathrm{Aut}(V)$ auf einem endlichdimensionalen komplexen Vektorraum gilt*

$$\langle \chi_\varrho, \chi_G \rangle \;=\; \dim(V).$$

(ii) *Die isotypische Zerlegung der regulären Darstellung $\varrho_G \colon G \to \mathrm{Aut}(V_G)$ ist gegeben durch*

$$V_G \;\cong \bigoplus_{\omega \in \Omega(G)} V_\omega^{\dim(V_\omega)}.$$

(iii) *Für die Ordnung von G und die Dimensionen der einfachen G-Moduln V_ω ergibt sich*

$$|G| \;=\; \chi_G(e_G) \;=\; \sum_{\omega\in\Omega(G)} \dim(V_\omega)\chi_\omega(e_G) \;=\; \sum_{\omega\in\Omega(G)} \dim(V_\omega)^2.$$

Beweis. Aussage (i) ergibt sich direkt aus Satz 8.2.12 und der Definition des Skalarproduktes:

$$\begin{aligned}\langle \chi_\varrho, \chi_G\rangle &= \frac{1}{|G|}\sum_{g\in G} \chi_\varrho(g)\overline{\chi_G(g)} = \frac{1}{|G|}\chi_\varrho(e_G)\overline{\chi_G(e_G)}\\ &= \frac{1}{|G|}\mathrm{Spur}(\mathrm{id}_V)|G| = \dim(V).\end{aligned}$$

Aussage (ii) folgt direkt aus Aussage (i) mit $\langle \chi_\omega, \chi_G\rangle = \dim(V_\omega)$. Aussage (iii) ergibt sich aus Aussage (ii) mit

$$\chi_G \;=\; \sum_{\omega\in\Omega(G)} \dim(V_\omega)\chi_\omega, \qquad \chi_\omega(e_G) \;=\; \dim(V_\omega).$$

□

Satz 8.3.16. *Es sei G eine endliche Gruppe. Dann bilden die Charaktere χ_ω, wobei $\omega \in \Omega(G)$, eine Orthonormalbasis des Vektorraumes $\mathrm{CF}(G)$ der Klassenfunktionen.*

Lemma 8.3.17. *Es seien G eine endliche Gruppe, V ein endlichdimensionaler komplexer G-Modul und $\alpha\colon G \to \mathbb{C}$ eine Klassenfunktion. Wir betrachten*

$$\varphi_{\varrho,\alpha}\colon V \;\to\; V, \qquad v \;\mapsto\; \sum_{g\in G} \overline{\alpha(g)}\, g\cdot v,$$

wobei $\varrho\colon G \to \mathrm{Aut}(V)$ die zum G-Modul V gehörige Darstellung bezeichnet. Dann ist $\varphi_{\varrho,\alpha}$ ein G-Modulhomomorphismus und seine Spur ist gegeben durch

$$\mathrm{Spur}(\varphi_{\varrho,\alpha}) \;=\; |G|\langle \chi_\varrho, \alpha\rangle.$$

Beweis. Offensichtlich ist $\varphi_{\varrho,\alpha}$ eine lineare Abbildung. Für jedes $h \in G$ und jedes $v \in V$ haben wir zudem

$$\begin{aligned}\varphi_{\varrho,\alpha}(h\cdot v) &= \sum_{g\in G} \overline{\alpha(g)}\, g\cdot h\cdot v = \sum_{g\in G} \overline{\alpha(hgh^{-1})}\, hgh^{-1}\cdot h\cdot v\\ &= \sum_{g\in G} \overline{\alpha(g)}\, hg\cdot v = h\cdot\sum_{g\in G} \overline{\alpha(g)}\, g\cdot v = h\cdot\varphi_{\varrho,\alpha}(v).\end{aligned}$$

Somit ist $\varphi_{\varrho,\alpha}$ ein G-Modulhomomorphismus. Die Formel für die Spur lässt sich ebenfalls direkt verifizieren:

$$\begin{aligned}\mathrm{Spur}(\varphi_{\varrho,\alpha}) &= \mathrm{Spur}\left(\sum_{g\in G} \overline{\alpha(g)}\varrho(g)\right) = \sum_{g\in G} \overline{\alpha(g)}\mathrm{Spur}(\varrho(g))\\ &= \sum_{g\in G} \overline{\alpha(g)}\chi_\varrho(g) = \langle \chi_\varrho, \alpha\rangle.\end{aligned}$$

□

Beweis von Satz 8.3.16. Nach Satz 8.3.6 ist die Familie $\mathcal{B} := (\chi_\omega;\ \omega \in \Omega(G))$ eine Orthonormalbasis für den Untervektorraum

$$U \ := \ \mathrm{Lin}(\mathcal{B}) \ \subseteq \ \mathrm{CF}(G).$$

Wegen $\mathrm{CF}(G) = U \oplus U^\perp$ genügt es zu zeigen, dass das orthogonale Komplement $U^\perp$ trivial ist. Dazu sei eine Klassenfunktion $\alpha \in U^\perp$ gegeben. Dann gilt

$$\langle \chi_\omega, \alpha \rangle \ = \ 0 \quad \text{für alle } \omega \in \Omega(G).$$

Wir betrachten nun eine irreduzible Darstellung $\varrho \in \omega \in \Omega(G)$ und den G-Modulhomomorphismus

$$\varphi_{\varrho,\alpha} \colon V \ \to \ V, \qquad v \ \mapsto \ \sum_{g \in G} \overline{\alpha(g)}\, g \cdot v$$

aus Lemma 8.3.17. Nach dem Lemma von Schur haben wir $\varphi_{\varrho,\alpha} = \lambda \cdot \mathrm{id}_V$ mit einem $\lambda \in \mathbb{C}$. Mit Lemma 8.3.17 erhalten wir

$$\lambda \dim(V) \ = \ \mathrm{Spur}(\varphi_{\varrho,\alpha}) \ = \ |G| \langle \chi_\varrho, \alpha \rangle \ = \ |G| \langle \chi_\omega, \alpha \rangle \ = \ 0.$$

Das bedeutet $\lambda = 0$ und somit $\varphi_{\varrho,\alpha} = 0$. Ist $\varrho = \varrho_1 \oplus \ldots \oplus \varrho_r$ eine direkte Summe irreduzibler Darstellungen $\varrho_i \in \omega \in \Omega(G)$, so erhalten wir

$$\begin{aligned} \varphi_{\varrho,\alpha}(v) \ &= \ \sum_{g \in G} \overline{\alpha(g)}\, g \cdot v \ = \ \sum_{g \in G} \overline{\alpha(g)}\, g \cdot v_1 + \ldots + \sum_{g \in G} \overline{\alpha(g)}\, g \cdot v_r \\ &= \ \varphi_{\varrho_1,\alpha}(v_1) + \ldots + \varphi_{\varrho_r,\alpha}(v_r) \ = \ 0 \end{aligned}$$

für jedes Element $v = v_1 + \ldots + v_r$ des zugehörigen G-Moduls $V = V_1 \oplus \ldots \oplus V_r$. Das bedeutet $\varphi_{\varrho,\alpha} = 0$.

Insbesondere gilt $\varphi_{\varrho_G,\alpha} = 0$ für die reguläre Darstellung $\varrho_G \colon G \to \mathrm{Aut}(V_G)$. Für die charakteristische Funktion $f_{e_G} \in V_G$ des neutralen Elements $e_G \in G$ ergibt sich

$$0 \ = \ \varphi_{\varrho_G,\alpha}(f_{e_G}) \ = \ \sum_{g \in G} \overline{\alpha(g)}\, g \cdot f_{e_G} \ = \ \sum_{g \in G} \overline{\alpha(g)} f_g.$$

Da die charakteristischen Funktionen f_g, wobei $g \in G$ eine Basis für V_G bilden, folgt $\overline{\alpha(g)} = 0$ und somit $\alpha(g) = 0$ für alle $g \in G$. Das bedeutet $\alpha = 0$. □

Folgerung 8.3.18. *Für jede endliche Gruppe G ist $|\Omega(G)|$ die Anzahl der Konjugationsklassen von G. Insbesondere besitzt G genauso viele irreduzible Charaktere wie Konjugationsklassen.*

Aufgaben zu Abschnitt 8.3.

Aufgabe 8.3.19. Beweise die Aussagen aus Bemerkung 8.3.4 und Konstruktion 8.3.5.

Aufgabe 8.3.20. Es sei $G = S_3$. Betrachte die Permutationsdarstellung von G sowie den zugehörigen Charakter dieser Darstellung. Ist diese Darstellung irreduzibel? Bestimme die isotypische Zerlegung des zugehörigen G-Moduls.

Aufgabe 8.3.21. Betrachte die regulären Darstellungen für $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und $G = \mathbb{Z}/4\mathbb{Z}$ und bestimme die isotypische Zerlegung der zugehörigen G-Moduln.

Aufgabe 8.3.22. Es sei $\varrho\colon G \to \mathrm{GL}(V)$ eine Darstellung von G mit $\varrho = \sum_{i=1}^{r} n_i \varrho_i$ für irreduzible Darstellungen $\varrho_i\colon G \to \mathrm{GL}(V_i)$. Dann gilt für jede irreduzible Darstellung $\sigma\colon G \to \mathrm{GL}(W)$:

$$\langle \chi_\varrho, \chi_\sigma \rangle \;=\; \begin{cases} n_i & \text{falls } \sigma \sim \varrho_i \\ 0 & \text{sonst} \end{cases}.$$

Aufgabe 8.3.23. Jeder Charakter ist Linerakombination von irreduziblen Cahrakteren

$$\chi = \sum_{i=1}^{r} m_i \chi_i \quad \text{und es gilt} \quad \langle \chi, \chi \rangle \;=\; \sum_{i=1}^{r} m_i^2.$$

Literatur

[1] J. Hausen: Lineare Algebra I. 3. korrigierte Auflage. Aachen: Shaker. vi + 217 p. (2017). ISBN 978-3-8322-8616-3