ALGEBRA

Tammo tom Dieck

Mathematisches Institut
Georg-August-Universität
Götingen

Version vom 28. April 2004

Inhaltsverzeichnis

1 Kategorien

1 Kategorien

Die Kategorientheorie liefert eine allgemeine Begriffssprache, ähnlich wie die Mengenlehre. In der Algebra dient sie unter anderem dazu, immer wieder auftretende Begriffe und Konstruktionen auf ihre wesentliche Struktur zurückzuführen. Für Beispiele verwenden wir Material aus späteren Kapiteln.

(1.1) Kategorie. Eine *Kategorie* $\mathcal{C}$ besteht aus den folgenden Daten:

(1) Einer Klasse (Menge) $\mathrm{Ob}(\mathcal{C})$ von *Objekten*.

(2) Einer Menge $\mathrm{Mor}(C, D)$ zu jedem geordneten Paar (C, D) von Objekten C, D von $\mathcal{C}$. Die Elemente von $\mathrm{Mor}(C, D)$ heißen *Morphismen* der Kategorie *von* C *nach* D. Ein Morphismus von C nach D wird oft in der Form $f\colon C \to D$ geschrieben und *Pfeil* der Kategorie genannt. In diesem Fall heißt C die *Quelle* und D das *Ziel* von f. Ein Morphismus bestimmt Quelle und Ziel, d. h. aus $\mathrm{Mor}(C, D) \cap \mathrm{Mor}(E, F) \neq \emptyset$ folgt $C = E$ und $D = F$.

(3) Einem Morphismus $\mathrm{id}(C) = \mathrm{id}_C = 1_C \in \mathrm{Mor}(C, C)$ für jedes Objekt C, genannt *Identität* von C.

(4) Einer Abbildung

$$\mathrm{Mor}(B, C) \times \mathrm{Mor}(A, B) \to \mathrm{Mor}(A, C), \quad (g, f) \mapsto g \circ f = gf$$

für jedes geordnete Tripel (A, B, C) von Objekten, genannt *Komposition, Verknüpfung* oder *Verkettung* von Morphismen.

Diese Daten sollen die folgenden Axiome erfüllen:

(5) Die Komposition ist assoziativ, d. h. für Morphismen $f\colon A \to B$, $g\colon B \to C$ und $h\colon C \to D$ gilt immer $(hg)f = h(gf)$.

(6) Für jeden Morphismus $f\colon A \to B$ gilt $f = f \circ \mathrm{id}(A) = \mathrm{id}(B) \circ f$.

Statt $\mathrm{Mor}(C, D)$ wird zur Verdeutlichung auch $\mathrm{Mor}_{\mathcal{C}}(C, D)$ oder $\mathcal{C}(C, D)$ geschrieben. Auch $\mathrm{Hom}(C, D)$ oder $\mathrm{Hom}_{\mathcal{C}}(C, D)$ ist für diese Menge in Gebrauch, in Anlehnung an die Homomorphismenmengen der Algebra. ◇

Das Musterbeispiel einer Kategorie ist die Kategorie MEN der Mengen. Die Objekte sind die Mengen. Die Morphismen sind die Mengenabbildungen. Die Identität ist die identische Abbildung. Die Komposition ist die Nacheinanderausführung von Abbildungen.

Viele weitere Kategorien werden aus Mengen mit zusätzlichen Strukturen gewonnen. Wir geben einige Standardbeispiele.

Die Kategorie GRU der Gruppen (Objekte) und Gruppenhomomorphismen (Morphismen). Die Kategorie K-Vek der Vektorräume über einem Körper K (Objekte) und K-linearen Abbildungen (Morphismen). Die Kategorie AB der abelschen Gruppen und Homomorphismen.

In allen vorstehend genannten Kategorien und weiteren analogen, denen Mengen mit weiterer Struktur zugrundeliegen, ist, wenn nichts anderes gesagt wird,

die Komposition diejenige der Mengenabbildungen. Die Axiome einer Kategorie sind dann offenbar erfüllt.

Wir haben anfangs von einer *Klasse* von Objekten gesprochen, weil Bildungen wie die Menge aller Mengen nicht erlaubt sind. Ist $\mathrm{Ob}(\mathcal{C})$ eine Menge, so sprechen wir von einer *kleinen* Kategorie. Wir gehen auf die mengentheoretischen Grundlagenprobleme nicht ein.

Die Sprache der Kategorien dient dazu, die in vielen mathematischen Zweigen auftretenden Begriffe in eine einheitliche Begriffssprache einzugliedern. Hierzu gleich ein einfaches Beispiel.

Ein Morphismus $f\colon C \to D$ einer Kategorie heißt *Isomorphismus*, wenn er einen Umkehrmorphismus $g\colon D \to C$ mit den Eigenschaften $g \circ f = \mathrm{id}(C)$ und $f \circ g = \mathrm{id}(D)$ besitzt. Dieser ist dann eindeutig durch f bestimmt (Beweis!) und wird auch mit f^{-1} bezeichnet. Gibt es einen Isomorphismus $f\colon C \to D$, so heißen die Objekte C und D *isomorph*. Ein Morphismus $f\colon C \to C$ heißt *Endomorphismus* von C. Ein Isomorphismus $f\colon C \to C$ heißt *Automorphismus* von C.

Die Morphismen einer Kategorie sind nicht immer Mengenabbildungen, wie die folgenden Beispiele zeigen.

(1.2) Monoide und Gruppen. Eine Kategorie mit einem einzigen Objekt C ist durch die Menge $M = \mathrm{Mor}(C, C)$ und eine assoziative Verknüpfung mit neutralem Element auf M gegeben. Die Angabe eines Objektes ist in diesem Falle überflüssig, es genügt M zusammen mit der Verknüpfung. Eine Menge M zusammen mit einer assoziativen Verknüpfung mit neutralem Element heißt *Monoid*.

Eine Kategorie mit einem Objekt C, in der jeder Morphismus ein Isomorphismus ist, wird durch eine Gruppenstruktur auf $M = \mathrm{Mor}(C, C)$ gegeben, denn die Existenz des Umkehrmorphismus besagt die Existenz des Inversen.

Eine Kategorie, in der jeder Morphismus ein Isomorphismus ist, heißt *Gruppoid*.

Für jede Kategorie und jedes ihrer Objekte A ist $\mathrm{Hom}(A, A)$ mit der Komposition ein Monoid. ◇

(1.3) Teilweise geordnete Mengen. Sei $\mathcal{C}$ eine kleine Kategorie, in der zwischen je zwei Objekten höchstens ein Morphismus existiert. Sei P die Menge der Objekte. Wir definieren auf P eine Relation $\leq$ durch

$$x \leq y \quad \Leftrightarrow \quad \mathrm{Mor}(x, y) \neq \emptyset.$$

Diese Relation hat die Eigenschaft

$$x \leq y,\ y \leq z \quad \Rightarrow \quad x \leq z$$

und heißt deshalb *Präordnung* auf P. Gilt außerdem

$$x \leq y,\ y \leq x \quad \Rightarrow \quad x = y,$$

so sprechen wir von einer (teilweisen oder partiellen) *Ordnung* auf P.

Im Sinne der Kategorien bedeutet das gleichzeitige Bestehen von $x \leq y$ und $y \leq x$, daß die Objekte x und y isomorph sind. $\diamond$

(1.4) Duale Kategorie. Sei $\mathcal{C}$ eine Kategorie. Die *duale Kategorie* $\mathcal{C}^\circ$ entsteht aus $\mathcal{C}$ durch „Umkehren der Pfeile“. Das bedeutet: Die Objektklassen beider Kategorien sind gleich. Es ist $\mathcal{C}^\circ(C, D) = \mathcal{C}(D, C)$. Die Identitäten bleiben dieselben. Die Komposition $*$ in $\mathcal{C}^\circ$ ist durch Umkehrung der Reihenfolge definiert: $f * g$ ist genau dann definiert, wenn $g \circ f$ definiert ist, und gleich dem zu $g \circ f$ in $\mathcal{C}^\circ$ gehörenden Morphismus. $\diamond$

(1.5) Produktkategorie. Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. Die *Produktkategorie* $\mathcal{C} \times \mathcal{D}$ hat als Objekte die Paare (C, D) von Objekten C aus $\mathcal{C}$ und D aus $\mathcal{D}$. Die Morphismen $(C_1, D_1) \to (C_2, D_2)$ sind die Paare von Morphismen $f\colon C_1 \to C_2$, $g\colon D_1 \to D_2$. $\diamond$

Aus einer Kategorie kann man in vielerlei Weise neue Kategorien konstruieren. Wir geben einige Beispiele.

(1.6) Kategorie der Pfeile. Sei $\mathcal{C}$ eine Kategorie. Die Kategorie $P\mathcal{C}$ der Pfeile von $\mathcal{C}$ hat als Objekte die Morphismen von $\mathcal{C}$. Ein Morphismus von $f\colon C_1 \to C_2$ nach $g\colon D_1 \to D_2$ ist ein Paar von Morphismen $\varphi_j\colon C_j \to D_j$, die $g\varphi = \varphi_2 f$ erfüllen. $\diamond$

(1.7) Kategorie der Endomorphismen. Die Objekte von $\mathrm{END}(\mathcal{C})$ sind die Endomorphismen $f\colon C \to C$ in $\mathcal{C}$. Ein Morphismus von f nach $g\colon D \to D$ ist ein Morphismus $\varphi\colon C \to D$, der $g\varphi = \varphi f$ erfüllt. $\diamond$

(1.8) Objekte über und unter B. Sei B ein Objekt aus $\mathcal{C}$. Ein Morphismus $f\colon E \to B$ heißt *Objekt über* B. Die Kategorie $\mathcal{C}_B$ habe als Objekte die Objekte über B. Ein Morphismus von $f\colon E \to B$ nach $g\colon F \to B$ ist ein Morphismus $\varphi\colon E \to F$, der $g\varphi = f$ erfüllt. Ebenso für *Objekte* $f\colon B \to E$ *unter* B. $\diamond$

Allgemein kann man in analoger Weise offenbar aus Diagrammen fester Form Kategorien bilden.

2 Funktoren

Seien $\mathcal{C}$ und $\mathcal{D}$ Kategorien. Ein *Funktor* $F\colon \mathcal{C} \to \mathcal{D}$ von $\mathcal{C}$ nach $\mathcal{D}$ ist eine Vorschrift, die jedem Objekt C von $\mathcal{C}$ ein Objekt $F(C)$ von $\mathcal{D}$ und jedem Morphismus $f\colon C \to D$ von $\mathcal{C}$ einen Morphismus $F(f)\colon F(C) \to F(D)$ von $\mathcal{D}$ zuordnet. Diese Daten sollen die folgenden Eigenschaft haben:

$$\textbf{(2.1)} \qquad F(\mathrm{id}(C)) = \mathrm{id}(F(C)), \qquad F(g \circ f) = F(g) \circ F(f).$$

Ein *kontravarianter Funktor* $U\colon \mathcal{C} \to \mathcal{D}$ ist eine Vorschrift, die jedem Objekt C von $\mathcal{C}$ ein Objekt $U(C)$ von $\mathcal{D}$ zuordnet und jedem Morphismus $f\colon C \to D$ von $\mathcal{C}$ einen Morphismus $U(f)\colon U(D) \to U(C)$ von $\mathcal{D}$. Diese Daten sollen die folgende Eigenschaft haben:

(2.2) $$U(\mathrm{id}(C)) = \mathrm{id}(U(C)), \qquad U(g \circ f) = U(f) \circ U(g).$$

Funktoren nennt man zur Unterscheidung auch *kovariante Funktoren*. ◇

Man sagt: Ein kontravarianter Funktor dreht die Richtung der Pfeile um. Eine unmittelbare Folgerung aus den Axiomen (2.1) und (2.2) ist:

(2.3) Notiz. *Ein (kontravarianter) Funktor bildet Isomorphismen auf Isomorphismen ab.* □

Ein kontravarianter Funktor $F\colon \mathcal{C} \to \mathcal{D}$ ist im wesentlichen dasselbe wie ein Funktor $\mathcal{C} \to \mathcal{D}^\circ$ in die duale Kategorie oder wie ein Funktor $\mathcal{C}^\circ \to \mathcal{D}$. Ein Funktor $F\colon \mathcal{C} \times \mathcal{D} \to \mathcal{E}$ von einer Produktkategorie wird auch als Funktor in zwei Variablen angesehen. Wir geben einige Beispiele für Funktoren.

(2.4) Dualraum. Jedem Vektorraum V über dem Körper K werde der Dualraum $V^* = \mathrm{Hom}_K(V, K)$ der K-linearen Abbildungen $V \to K$ zugeordnet und jeder linearen Abbildung $f\colon V \to W$ die duale Abbildung $f^*\colon W^* \to V^*$, $\alpha \mapsto \alpha \circ f$. Dadurch wird ein kontravarianter Funktor *Dualraum* von der Kategorie K-Vek in sich definiert. Zweimalige Anwendung liefert den Funktor *Bidualraum*. ◇

(2.5) Vergißfunktoren. Die in Rede stehenden Funktoren lassen Struktur weg (vergessen sie). Wird einer Gruppe G die ihr zugrundeliegende Menge G und jedem Homomorphismus dieselbe Mengenabbildung zugeordnet, so erhalten wir einen Vergißfunktor GRU $\to$ MEN. ◇

(2.6) Gruppen. Wir fassen eine Gruppe als Kategorie mit einem Objekt auf. Ein Funktor $G \to H$ ist dann dasselbe wie ein Gruppenhomomorphismus $f\colon G \to H$. Durch $g \mapsto g^{-1}$ wird ein kontravarianter Funktor $G \to G$ definiert. ◇

(2.7) Hom-Funktoren. Jede Kategorie produziert durch ihre Morphismenmengen Funktoren. Sei D ein Objekt der Kategorie $\mathcal{C}$. Der kontravariante Hom-Funktor

$$\mathrm{Hom}(-, D) = \mathrm{Hom}(?, D)\colon \mathcal{C} \to \text{ MEN}$$

ordnet einem Objekt C die Morphismenmenge $\mathrm{Hom}(C, D)$ zu und einem Morphismus $\varphi\colon C_1 \to C_2$ die Abbildung

$$\mathrm{Hom}(\varphi, D)\colon \mathrm{Hom}(C_2, D) \to \mathrm{Hom}(C_1, D), \quad f \mapsto f \circ \varphi.$$

Die Funktoraxiome sind leicht nachzurechnen. Analog gibt es zu jedem Objekt C den kovarianten Hom-Funktor $\mathrm{Hom}(C, -)\colon \mathcal{C} \to$ MEN. Betrachtet man beide Variablen gleichzeitig, so wird der Hom-Funktor ein Funktor

$$\mathrm{Hom}(-, -)\colon \mathcal{C}^\circ \times \mathcal{C} \to \mathrm{MEN}$$

in zwei Variablen. ◇

Sind $F\colon \mathcal{A} \to \mathcal{B}$ und $G\colon \mathcal{B} \to \mathcal{C}$ Funktoren, so ist die Komposition $G \circ F$ der Funktor $\mathcal{A} \to \mathcal{C}$, der durch

(2.8) $$(G \circ F)(C) = G(F(C)), \qquad (G \circ F)(f) = G(F(f))$$

auf Objekten C und Morphismen f definiert ist. Es gibt den identischen Funktor $\mathrm{Id}_{\mathcal{C}}\colon \mathcal{C} \to \mathcal{C}$, der auf Objekten und Morphismen die Identität ist. Komposition von Funktoren ist assoziativ. Sind $\mathcal{A}$ und $\mathcal{B}$ kleine Kategorien, so bilden die Funktoren von $\mathcal{A}$ nach $\mathcal{B}$ eine Menge, denn ein Funktor ist durch eine Abbildung der Objektmengen und Morphismenmengen gegeben. Deshalb bilden die kleinen Kategorien zusammen mit den Funktoren zwischen ihnen und der eben genannten Komposition selbst wieder eine Kategorie KAT.

Die Komposition zweier kontravarianter Funktoren ist analog definiert und liefert einen kovarianten Funktor. Auch lassen sich ko- und kontravariante Funktoren komponieren.

Da KAT eine Kategorie ist, haben wir den Begriff einer Isomorphie von (kleinen) Kategorien. Es stellt sich jedoch heraus, daß dieser Begriff zum Vergleich zweier Kategorien zu starr ist. Wir werden alsbald den Begriff einer Äquivalenz von Kategorien erklären.

(2.9) Natürliche Transformation. Seien $F, G\colon \mathcal{C} \to \mathcal{D}$ Funktoren. Eine *natürliche Transformation* $\Phi\colon F \to G$ von F nach G besteht aus einer Familie $\Phi_C\colon F(C) \to G(C)$ von Morphismen in $\mathcal{D}$, indiziert durch die Objekte C von $\mathcal{C}$, so daß für jeden Morphismus $f\colon C \to D$ in $\mathcal{C}$ das Diagramm

$$\begin{array}{ccc} F(C) & \xrightarrow{\Phi_C} & G(C) \\ \downarrow{\scriptstyle F(f)} & & \downarrow{\scriptstyle G(f)} \\ F(D) & \xrightarrow{\Phi_D} & G(C) \end{array}$$

in $\mathcal{D}$ kommutativ ist. Sind alle Φ_C Isomorphismen in $\mathcal{D}$, so heißt Φ *natürlicher Isomorphismus*, in Zeichen $\Phi\colon F \simeq G$. Analog wird eine natürliche Transformation und ein natürlicher Isomorphismus zwischen kontravarianten Funktoren definiert. Die Inversen Φ_C^{-1} eines natürlichen Isomorphismus bilden ebenfalls einen.$\diamond$

(2.10) Beispiel. Seien D und E Objekte einer Kategorie, und sei $f\colon D \to E$ ein Morphismus. Durch Komposition mit f erhalten wir eine natürliche Transformation $f_*\colon \mathrm{Hom}(?, D) \to \mathrm{Hom}(?, E)$ zwischen Hom-Funktoren, indem

$$f_{*C}\colon \mathrm{Hom}(C, D) \to \mathrm{Hom}(C, E), \quad g \mapsto f \circ g$$

gesetzt wird, und eine natürliche Transformation $f^*\colon \mathrm{Hom}(E, ?) \to \mathrm{Hom}(D, ?)$, indem

$$f_C^*\colon \mathrm{Hom}(E, C) \to \mathrm{Hom}(D, C), \quad h \mapsto h \circ f$$

gesetzt wird. $\diamond$

(2.11) Bidualraum. Zu jedem K-Vektorraum V und jedem $v \in V$ gehört $D_V(v) \in V^{**}$, wobei

$$D_V(v)\colon V^* \to K, \quad \varphi \mapsto \varphi(v)$$

ist. Die durch

$$D_V\colon V \to V^{**}, \quad v \mapsto D_V(v)$$

gegebenen linearen Abbildungen liefern eine natürliche Transformation des identischen Funktors von K-Vek in den Funktor Bidualraum. Beschränkt man diese Konstruktion auf die Kategorie K-vek der endlichdimensionalen K-Vektorräume, so wird D ein natürlicher Isomorphismus. $\diamond$

Sind $\Phi\colon F \to G$ und $\Psi\colon G \to H$ natürliche Transformationen zwischen Funktoren $\mathcal{C} \to \mathcal{D}$, so wird durch

$$(\Psi \circ \Phi)_C = \Psi_C \circ \Phi_C \tag{2.12}$$

eine natürliche Transformation $\Psi \circ \Phi\colon F \to H$ definiert. Diese Komposition von natürlichen Transformationen ist assoziativ. Es gibt immer die identische natürliche Transformation $\mathrm{Id}_F\colon F \to F$.

Sind $\mathcal{C}$ und $\mathcal{D}$ kleine Kategorien, so bilden wir die *Funktorkategorie* $[\mathcal{C}, \mathcal{D}]$: Deren Objekte sind die Funktoren $\mathcal{C} \to \mathcal{D}$, und die Morphismen von F nach G sind die natürlichen Transformationen $\Phi\colon F \to G$. Die Komposition haben wir durch (2.12) definiert.

Ein Funktor $F\colon \mathcal{C} \to \mathcal{D}$ heißt *Äquivalenz* von diesen Kategorien, wenn es einen Funktor $G\colon \mathcal{D} \to \mathcal{C}$ und natürliche Isomorphismen $GF \simeq \mathrm{Id}_{\mathcal{C}}$ und $FG \simeq \mathrm{Id}_{\mathcal{D}}$ gibt. Es ist dann auch G eine Äquivalenz von Kategorien. Kategorien $\mathcal{C}$ und $\mathcal{D}$ heißen *äquivalent*, wenn es eine Äquivalenz zwischen ihnen gibt.

(2.13) Aufgaben und Ergänzungen.

1. Eine *Unterkategorie* einer Kategorie $\mathcal{C}$ besteht aus einer Teilmenge von Objekten und Morphismen, so daß mit der gegebenen Komposition diese Teilmengen eine Kategorie bilden. Eine Unterkategorie heißt *voll*, wenn für je zwei ihrer Objekte die Hom-Menge dieselbe ist wie in der großen Kategorie. Eine volle Unterkategorie $\mathcal{D}$ ist genau dann äquivalent zur ganzen Kategorie $\mathcal{C}$, wenn zu jedem ihrer Objekte ein isomorphes in $\mathcal{D}$ existiert.

2. (Yoneda-Lemma) Sei $\mathcal{C}$ eine Kategorie. Eine natürliche Transformation des Hom-Funktors $\mathrm{Hom}(-, D)$ in einen kontravarianten Funktor $G\colon \mathcal{C} \to \mathrm{MEN}$ ist durch den Wert auf $\mathrm{id}(C) \in G(C)$ bestimmt und dieser Wert kann beliebig vorgeschrieben werden. Die Funktoren $\mathrm{Hom}(-, D)$ und $\mathrm{Hom}(-, E)$ sind genau dann natürlich isomorph, wenn D und E isomorph sind.

3. Sind $F\colon \mathcal{C} \to \mathcal{D}$ und $G\colon \mathcal{D} \to \mathcal{E}$ Äquivalenzen von Kategorien, so ist auch $G \circ F$ eine Äquivalenz.

3 Summen und Produkte

Wir kommen jetzt zu kategoriellen Begriffsbildungen, die in sämtlichen algebraischen Kategorien immer wieder eine wichtige Rolle spielen. Hier bewährt sich der Formalismus der allgemeinen Begriffssprache.

Sei $\mathcal{X} = (X_j \mid j \in J)$ eine Familie von Objekten der Kategorie $\mathcal{C}$. Eine Familie $(p_j \colon X \to X_j \mid j \in J)$ von Morphismen in $\mathcal{C}$ heißt *Produkt* der Familie $\mathcal{X}$, wenn für jedes Objekt Y von $\mathcal{C}$ die Abbildung

$$\textbf{(3.1)} \qquad \mathrm{Hom}(Y, X) \to \prod_{j \in J} \mathrm{Hom}(Y, X_j), \quad f \mapsto (p_j \circ f \mid j \in J)$$

bijektiv ist. In (3.1) ist $\prod$ das mengentheoretische Produkt. Das Urbild von (f_j) bei (3.1) werde ebenfalls mit (f_j) bezeichnet.

Ein Produkt ist, wenn es existiert, im wesentlichen eindeutig bestimmt. Sei nämlich $(q_j \colon X' \to X_j \mid j \in J)$ ein weiteres Produkt von $\mathcal{X}$. Dann gibt es genau einen Morphismus $\alpha \colon X' \to X$ mit $p_j \circ \alpha = q_j$ (indem wir (3.1) auf $Y = X'$ anwenden) und genau einen Morphismus $\beta \colon X \to X'$ mit $q_j \circ \beta = p_j$. Wegen $p_j \circ \alpha \circ \beta = p_j$ und der Bijektivität in (3.1) ist $\alpha \circ \beta = \mathrm{id}$. Ebenso folgt $\beta \circ \alpha = \mathrm{id}$. Also sind α und β eindeutig bestimmte Isomorphismen.

Ein Produkt ist also bis auf die genannte Isomorphie eindeutig durch eine Eigenschaft, nämlich die Bijektivität von (3.1), bestimmt. Wir sprechen deshalb von der *universellen Eigenschaft* des Produktes.

Ein Produkt bezeichnen wir häufig wie in der Mengensprache durch das Symbol

$$\textbf{(3.2)} \qquad X = \prod_{j \in J} X_j,$$

nehmen also die p_j nicht mit in die Notation auf, und nennen $p_j = \mathrm{pr}_j$ die *Projektion* auf den *Faktor* X_j. Ebenso wird ein Produkt der Objekte X_1, X_2 durch $X_1 \times X_2$ bezeichnet.

Ist $\mathcal{Y} = (Y_j \mid j \in J)$ eine weitere Familie, $(q_j \colon Y \to Y_j)$ ein Produkt von $\mathcal{Y}$ und $(f_j \colon X_j \to Y_j)$ eine Familie von Morphismen, so gibt es genau einen Morphismus $f \colon X \to Y$ mit der Eigenschaft $q_j \circ f = f_j \circ p_j$, $j \in J$. Wir wählen dafür die Bezeichung

$$\textbf{(3.3)} \qquad f = \prod_{j \in J} f_j$$

und nennen f das *Produkt* der Morphismen f_j. Die eindeutige Existenz von f folgt mit der universellen Eigenschaft von Y, angewendet auf die Familie $(f_j p_j)$. Universelle Eigenschaften liefern auch Rechenregeln wie

$$\textbf{(3.4)} \qquad (\prod_j f_j) \circ (\prod_j g_j) = \prod_j (f_j \circ g_j).$$

Wir bemerken, daß das übliche cartesische Produkt von Mengen ein Produkt im eben genannten Sinne in der Kategorie der Mengen MEN ist.

Wir sagen, eine Kategorie besitze (endliche) Produkte, wenn zu jeder (endlichen) Familie von Objekten ein Produkt existiert. Die Kategorie der endlichen Mengen hat endliche Produkte aber nicht beliebige, denn das Produkt einer

unendlichen Familie von Mengen mit mehr als zwei Elementen müßte eine unendliche Menge sein.

Haben je zwei Objekte ein Produkt, so auch je endlich viele. Die Produktbildung ist assoziativ. Diese Aussagen folgen daraus, daß Produkte von Produkten wieder Produkte sind. Genauer:

(3.5) Satz. *Sei $(\mathcal{X}_k = (X_j \mid j \in J(k)) \mid k \in K)$ eine Familie von Familien von Objekten von $\mathcal{C}$. Seien die $J(k)$ paarweise disjunkt, und sei $\mathcal{X} = (X_j \mid j \in \bigcup_{k\in K} J(k))$. Hat jede der Familien $\mathcal{X}_k$ ein Produkt $Y_k = \prod_{j\in J(k)} X_j$ und haben die $(Y_k \mid k \in K)$ ein Produkt, so ist*

$$\mathrm{pr}_{X_j} \circ \mathrm{pr}_{Y_k} \colon \prod_{k\in K} Y_k \to \prod_{j\in J(k)} X_j \to X_j$$

ein Produkt von $\mathcal{X}$.

Beweis. Argumentation mit den universellen Eigenschaften. □

Insbesondere läßt sich ein Produkt von drei Objekten durch $(X_1 \times X_2) \times X_3$ und $X_1 \times (X_2 \times X_3)$ gewinnen, und es gibt einen eindeutigen Isomorphismus zwischen diesen Produkten, der mit den Projektionen auf die Faktoren verträglich ist. Das ist die Assoziativität (analog für beliebige Klammerungen). In fast allen praktisch vorkommenden Kategorien weiß man, wie man mit eventuellen Produkten umgehen muß. Deshalb wollen wir hier die formellen Überlegungen, zum Beispiel zur Assoziativität, nicht vertiefen. Sie sind übrigens komplizierter, als es zunächst den Anschein hat.

Wird ein kategorientheoretischer Begriff nur durch Eigenschaften von Pfeilen definiert, so erhält man einen neuen Begriff, indem man die Richtungen aller Pfeile umkehrt (Dualitätsprinzip; Verwendung desselben Begriffs in der dualen Kategorie). Der duale Begriff zum Produkt ist die *Summe*, zur Betonung der Dualität auch *Koprodukt* genannt. (Ein dualer Begriff wird oft mit der Vorsilbe Ko- gekennzeichnet.)

Eine *Summe* einer Familie $\mathcal{X} = (X_j \mid j \in J)$ ist eine Familie $(i_j \colon X_j \to Z \mid j \in J)$ von Morphismen, so daß für alle Objekte Y die Abbildung

$$\textbf{(3.6)} \qquad \mathrm{Hom}(Z, Y) \to \prod_{j\in J} \mathrm{Hom}(X_j, Y), \quad f \mapsto (f \circ i_j \mid j \in J)$$

bijektiv ist (universelle Eigenschaft der Summe). Das Urbild von (f_j) bei (3.6) werde mit $\langle f_j \rangle$ bezeichnet. Wir schreiben

$$\textbf{(3.7)} \qquad Z = \coprod_{j\in J} X_j$$

und nennen i_j die Injektion des j-ten *Summanden*. Die Aussagen und Notationen (3.3), (3.4) und (3.5) übertragen sich durch Dualisierung: Sind $f_j \colon X_j \to Y_j$ Morphismen, so wird der Summenmorphismus mit

(3.8)
$$\coprod_{j\in J} f_j \colon \coprod_{j\in J} X_j \to \coprod_{j\in J} Y_j$$

bezeichnet. Er ist durch die Eigenschaft

$$(\coprod f_j) \circ i_j = i_j \circ f_j$$

charakterisiert. Eine Summe von Summen ist eine Summe. Die Summenbildung ist assoziativ.

Ist eine Menge X die disjunkte Vereinigung der Teilmengen $(X_j \mid j \in J)$, so bilden die Inklusionen $i_j \colon X_j \subset X$ ein Summe in MEN. Um eine Summe in MEN einer beliebigen Familie von Mengen $(X_j \mid j \in J)$ zu erhalten, muß man die Mengen künstlich disjunkt machen und sie dann vereinigen, etwa wie durch $\bigcup_{j\in J}\{j\} \times X_j$ angedeutet.

Mit den Begriffen Produkt und Summe eng zusammen hängen die Begriffe Pullback (= cartesisches Quadrat) und Pushout (= kocartesisches Quadrat).

Seien $f \colon X \to B$ und $g \colon Y \to B$ Morphismen einer Kategorie $\mathcal{C}$. Ein kommutatives Diagramm in $\mathcal{C}$

(3.9)
$$\begin{array}{ccc} P & \xrightarrow{F} & Y \\ \downarrow{\scriptstyle G} & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{f} & B \end{array}$$

heißt *Pullback* von (f, g) (oder *cartesisches Quadrat*), wenn es die folgende universelle Eigenschaft hat: Zu jedem Paar von Morphismen $F' \colon Z \to Y$, $G' \colon Z \to X$ mit $gF' = fG'$ gibt es genau einen Morphismus $\varphi \colon Z \to P$ mit den Eigenschaften $G\varphi = G'$ und $F\varphi = F'$.

Durch die universelle Eigenschaft ist ein Pullback in der folgenden Weise bis auf eindeutige Isomorphie bestimmt: Ist $F_* \colon P_* \to Y$ und $G_* \colon P \to X$ eine weitere Ergänzung von (f, g) zu einem Pullback, so gibt es genau einen Isomorphismus $\Phi \colon P \to P_*$ mit $F_*\Phi = F$ und $G_*\Phi = G$.

Die Definition eines Pushout ergibt sich durch Dualisierung (Umdrehen der Pfeile): Das kommutative Quadrat (3.9) heißt *Pushout* (oder *kocartesisches Quadrat*) von (G, F), wenn es die folgende universelle Eigenschaft hat: Zu jedem Paar $g' \colon Y \to T$ und $f' \colon X \to T$ von Morphismen mit $f'G = g'F$ gibt es genau einen Morphismus $\Psi \colon B \to T$ mit $\Psi f = f'$ und $\Psi g = g'$.

Es ist denkbar, daß ein Quadrat (3.9) sowohl Pushout als auch Pullback ist: Es heißt dann *bicartesisch*.

(3.10) Beispiel. Ein Quadrat der Form

$$\begin{array}{ccc} A \cap B & \xrightarrow{\subset} & A \\ \downarrow{\scriptstyle \cap} & & \downarrow{\scriptstyle \cap} \\ B & \xrightarrow{\subset} & A \cup B \end{array}$$

ist ein Pushout in MEN. Seien $f\colon X \to B$ und $g\colon Y \to B$ Mengenabbildungen. Sei (Sprachmißbrauch)

$$P := X \times_B Y = \{(x, y) \in X \times Y \mid f(x) = g(y)\}.$$

Wir haben Abbildungen

$$F\colon P \to Y, \quad (x, y) \mapsto y, \qquad G\colon P \to X, \quad (x, y) \mapsto x.$$

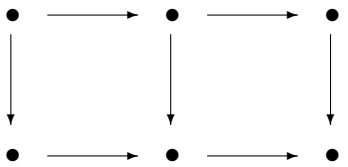
Mit diesen Daten ist (3.9) ein Pullback in MEN. ◇

Noch ein Wort zur universellen Eigenschaft: Bei einem Produkt bestimmt sie Abbildungen „hinein“, bei einer Summe Abbildungen „heraus“. Darin liegt auch eine Beweismethode.

(3.11) Aufgaben und Ergänzungen.

1. Ist (3.9) ein Pullback, so kann $gF = fG\colon P \to B$ zusammen mit F und G als ein Produkt von f und g in der Kategorie der Objekte über B angesehen werden. Dual für Pushout und Summe in der Kategorie der Objekte unter P.

2. Die Pushoutbildung ist transitiv: Sind in einem kommutativen Diagramm



die beiden Quadrate Pushouts, so auch das Rechteck. Dual für Pullbacks.

3. Beweis für (3.4) und (3.5).

2 Die ganzen Zahlen

1 Teilbarkeit

Wir bezeichnen die Menge der ganzen Zahlen $\{0, \pm 1, \pm 2, \ldots\}$ mit $\mathbb{Z}$. Die Teilbarkeitseigenschaften der ganzen Zahlen sind für die gesamte Mathematik wichtig. Wir stellen in diesem Abschnitt grundlegende Begriffe und Aussagen zur Teilbarkeit zusammen. Sie werden uns später in vielen analogen Situationen begegnen.

Gewissen Teilmengen von $\mathbb{Z}$ geben wir einen eigenen Namen. Die Zahlen in $\mathbb{Z}^* = \{\pm 1\}$ bezeichnen wir als *Einheiten*. Eine nichtleere Menge $I \subset \mathbb{Z}$ heißt *Ideal* von $\mathbb{Z}$, wenn mit je zwei Elementen $x, y \in I$ die Differenz $x - y$ und jedes skalare Vielfache λx für $\lambda \in \mathbb{Z}$ wieder in I liegt.[1]

Seien a und b ganze Zahlen. Wir sagen: a *teilt* b oder a ist ein *Teiler* von b oder b ist *Vielfaches* von a (in Zeichen $a|b$), wenn für ein $c \in \mathbb{Z}$ die Relation $b = ac$ besteht. Wir notieren einige einfache Eigenschaften.

(1.1) Regeln über Teilbarkeit.
(1) $1|a$, $a|a$, $a|0$.
(2) $a|b$, $b|c \Rightarrow a|c$.
(3) $a|b_1$, $a|b_2 \Rightarrow a|r_1b_1 + r_2b_2$.
(4) $a|b$, $c|d \Rightarrow ac|bd$.

Falls a das Element b nicht teilt, so schreiben wir dafür $a \not| b$. □

Die Menge $(a) := \{ac \mid c \in \mathbb{Z}\}$ aller Zahlen, die a als Teiler haben, ist das von a erzeugte *Hauptideal*. Wir stellen leicht fest:

(1.2) Notiz. *Es gelten die Äquivalenzen:*
(1) $a|b \Leftrightarrow (a) \supset (b)$.
(2) $(a) = (b) \Leftrightarrow$ *es gibt eine Einheit* $u \in \mathbb{Z}^*$, *so daß* $a = ub$ *ist.*

Beweis. Wir zeigen nur (2). Sei $(a) = (b)$. Dann gibt es Gleichheiten $ac = b$, $bd = a$. Folglich gilt $acd = a$ und $a(1 - cd) = 0$. Ist $a = 0$, so ist auch $b = 0$, und folglich ist wegen $a = 0 = 1 \cdot b$ die Behauptung richtig. Ist $a \neq 0$, so folgt $1 - cd = 0$, und damit ist c als Einheit erkannt. Ist umgekehrt $a = ub$ und $u^{-1}a = b$, so gelten nach (1) die Inklusionen $(a) \subset (b) \subset (a)$. □

Zahlen a und b heißen *assoziiert*, wenn $(a) = (b)$ ist. Assoziierte Zahlen haben dieselben Teilbarkeitseigenschaften.

Theorie und Praxis der Teilbarkeit beruht auf der bekannten *Division mit Rest*: Sind $a, q \in \mathbb{Z}$, und ist $q > 0$, so gibt es ein eindeutig bestimmtes Paar (b, r) ganzer Zahlen mit den Eigenschaften: $a = bq + r$, $0 \leq r < q$. Damit schließen wir leicht:

(1.3) Satz. *Ein von* $\{0\}$ *verschiedenes Ideal* $I \subset \mathbb{Z}$ *besteht genau aus den Vielfachen der kleinsten positiven Zahl in* I. *Insbesondere ist jedes Ideal von* $\mathbb{Z}$ *ein Hauptideal.*

[1] Dieser Begriff ist der Gruppen- und Ringtheorie angepaßt; die erste Bedingung besagt, daß I eine *Untergruppe* von $\mathbb{Z}$ ist; die zweite folgt in diesem Fall aus der ersten.

BEWEIS. Hat I von Null verschiedene Elemente, so auch positive und genau ein kleinstes q. Ist $a \in I$, so dividieren wir durch q mit Rest $a = bq + r$ und erkennen $r = a - bq \in I$. Wegen der Minimalität von q muß $r = 0$ sein. □

Sei $A \subset \mathbb{Z}$ nicht leer. Ein *größter gemeinsamer Teiler* (= GGT) von A ist eine Zahl d mit den Eigenschaften:

(1) d teilt jedes $a \in A$.

(2) Teilt f jedes $a \in A$, so teilt f auch d.

Aus dieser Definition folgt mittels (1.2) sofort, daß ein Element d durch diese beiden Eigenschaften bis auf Multiplikation mit einer Einheit eindeutig bestimmt ist, da sich zwei Zahlen mit diesen Eigenschaften gegenseitig teilen.

Das von A *erzeugte* Ideal $I(A)$ besteht aus allen endlichen Summen der Form $\sum_j \lambda_j a_j$ mit $\lambda_j \in \mathbb{Z}$ und $a_j \in A$ (*ganzzahlige Linearkombination*). Nach (1.3) ist $I(A)$ ein Hauptideal $(d(A))$. Das von $a_1, \ldots, a_n$ erzeugte Ideal wird mit $(a_1, \ldots, a_n)$ bezeichnet. Der Durchschnitt einer Menge von Idealen ist wieder ein Ideal.

(1.4) Satz. *Sei $A \subset \mathbb{Z}$ und $I(A) = (d(A))$. Dann ist $d(A)$ ein* GGT *von A. Es gibt insbesondere eine Darstellung als Linearkombination $d(A) = \sum_j \lambda_j a_j$.*

BEWEIS. Die Elemente von A liegen in $I(A)$ und sind deshalb Vielfache von $d(A)$. Teilt f jedes Element von A, so auch jede Linearkombination, also auch $d(A)$. □

Hat eine Menge den GGT 1, so heißt sie *teilerfremd*. Für ganze Zahlen $a_1, \ldots, a_k$ schreiben wir $(a_1, \ldots, a_k) = d$, wenn $d \geq 0$ der GGT der Familie $a_1, \ldots, a_k$ ist. Insbesondere heißen zwei Zahlen a_1 und a_2 *teilerfremd zueinander* oder *relativ prim*, wenn 1 ihr GGT ist.

Sei $A \subset \mathbb{Z}$ eine endliche nichtleere Teilmenge. Ein *kleinstes gemeinsames Vielfaches* (= KGV) von A ist eine Zahl m mit den Eigenschaften:

(1) Jedes $a \in A$ teilt m.

(2) Teilt jedes $a \in A$ eine Zahl f, so teilt m auch f.

Wieder ist m durch diese Eigenschaften bis auf Multiplikation mit einer Einheit eindeutig bestimmt.

(1.5) Satz. *Sei $A \subset \mathbb{Z}$ eine endliche nichtleere Menge. Der Durchschnitt der Ideale (a) für $a \in A$ ist ein Ideal (m). Das Element m ist ein* KGV *von A und teilt das Produkt $\prod_{a \in A} a$.*

BEWEIS. Wegen $(m) \subset (a)$ ist m ein Vielfaches von a. Ist f ein Vielfaches aller a, so ist (f) im Durchschnitt der (a) enthalten. □

(1.6) Euklidischer Algorithmus. Er besteht in einer fortgesetzten Division mit Rest bis die Teilung „aufgeht“, also $a_1 = q_1 a_2 + a_3$, $a_2 = q_2 a_3 + a_4, \ldots$. Das Verfahren muß abbrechen, da die Reste $a_3, a_4, \ldots$ immer kleiner werden. Der kleinste von Null verschiedene Rest ist der GGT von a_1 und a_2; das folgt induktiv mit Hilfe von Relationen des Typs $(a_1, a_2) = (a_2, a_3)$ (Beweis?). Durch Rückwärtsrechnen mit den Gleichungen des Algorithmus erhalten wir eine Darstellung

des GGT zweier Zahlen als Linearkombination nach (1.4). Ein Beispiel genügt für das Verständnis. ◇

Beispiel. $638 = 1 \cdot 511 + 127$, $511 = 4 \cdot 127 + 3$, $127 = 42 \cdot 3 + 1$, also $(638, 511) = (1)$. Durch Rückwärtsrechnen im Euklidischen Algorithmus erhalten wir eine Darstellung $1 = \lambda_1 \cdot 638 + \lambda_2 \cdot 511$ wie in (1.4): $127 - 42 \cdot 3 = 1$, $127 - 42 \cdot (511 - 4 \cdot 127) = 169 \cdot 127 - 42 \cdot 511 = 1$, $169 \cdot 638 - 211 \cdot 511 = 1$. ◇

2 Primzahlen

Wir beweisen in diesem Abschnitt die eindeutige Zerlegbarkeit einer Zahl in Primfaktoren. Dazu fixieren wir zwei Eigenschaften einer Zahl, die sich dann alsbald als gleichwertig erweisen werden.

Eine Zahl $p \in \mathbb{Z}$ heiße *unzerlegbar*, wenn $p \neq 0$ ist, p keine Einheit ist und aus $p = ab$ folgt, daß a oder b eine Einheit ist. Mit anderen Worten: Eine unzerlegbare Zahl hat keine Produktzerlegung in Nichteinheiten.

Es heiße $p \in \mathbb{Z}$ *Primelement* von $\mathbb{Z}$, wenn $p \neq 0$ ist und keine Einheit und wenn gilt: aus $p|ab$ folgt $p|a$ oder $p|b$. Die definierende Eigenschaft eines Primelementes kann im allgemeinen nicht direkt dazu benutzt werden, um ein Element als Primelement zu erkennen, denn dazu müßten unendlich viele Bedingungen nachgeprüft werden. Deshalb notieren wir zunächst als wichtigstes Hilfsmittel:

(2.1) Satz. *Eine ganze Zahl ist genau dann Primelement, wenn sie unzerlegbar ist.*

Beweis. Sei p Primelement und $p = ab$. Dann gilt also $p|a$ (oder $p|b$). Mit $pc = a$ schließen wir nacheinander $a = pc = abc$, $1 = bc$, $b \in \mathbb{Z}^*$. Mithin ist p unzerlegbar.

Sei p unzerlegbar. Es gelte $p|ab$, aber p teile nicht a. Es gilt immer $(p) \subset (p, a)$. Aus $(p) = (p, a)$ folgt $a \in (p)$, also $p|a$, was ausgeschlossen war. Also ist $(p) \neq (p, a)$. Das Ideal (p, a) ist ein Hauptideal (d), und nach (1.2) besteht deshalb eine Relation der Form $p = dc$. Da p unzerlegbar ist, gilt $d \in \mathbb{Z}^*$ oder $c \in \mathbb{Z}^*$. Ist $c \in \mathbb{Z}^*$ so ist $(d) = (p)$, und das hatten wir ausgeschlossen. Also ist $(d) = (1)$. Es gibt deshalb eine Darstellung der Form $1 = ep + fa$. Wir multiplizieren mit b. In der Gleichung $b = bep + fab$ sind wegen $p|ab$ beide Summanden der rechten Seite durch p teilbar; also folgt $p|b$. □

Von nun an nennen wir die positiven Primelemente von $\mathbb{Z}$ wie üblich *Primzahlen*.

(2.2) Satz. *Sei $a \in \mathbb{Z}$ von Null verschieden und keine Einheit. Dann ist a Produkt von unzerlegbaren Elementen. Sind $a = p_1 \dots p_r = q_1 \dots q_s$ Produktdarstellungen mit unzerlegbaren p_i und q_j, so ist $r = s$, und mit einer geeigneten Permutation π von $\{1, \dots, r\}$ gilt $(p_i) = (q_{\pi(i)})$.*

Beweis. Existenz einer Zerlegung. Wir führen einen Widerspruchsbeweis, der zunächst etwas umständlich anmuten mag, der aber den Vorteil hat, später auf

allgemeinere Situationen übertragbar zu sein, weil er nur allgemeine Teilbarkeitseigenschaften benutzt. Wir nehmen also an, a sei nicht Produkt unzerlegbarer Elemente. Wir zeigen damit zunächst durch Induktion: Es gibt eine Folge $a_0, a_1, a_2, \ldots$ von Nichteinheiten mit den Eigenschaften:

$$(a_0) \subset (a_1) \subset (a_2) \subset \ldots \subset (a_n),$$
$$(a_i) \neq (a_{i+1}),$$
$$a_i \text{ ist kein Produkt unzerlegbarer Elemente.}$$

Als a_0 wählen wir das Element a. Seien $a_0, \ldots, a_n$ mit den genannten Eigenschaften gegeben. Da a_n kein Produkt unzerlegbarer Elemente ist, besitzt a_n eine Zerlegung $a_n = a_{n+1}b_{n+1}$ in Nichteinheiten, und mindestens einer der Faktoren, etwa a_{n+1}, ist kein Produkt unzerlegbarer Elemente. Aus $(a_n) = (a_{n+1})$ würde $a_n = ua_{n+1}$ mit einer Einheit u folgen, was wir ausgeschlossen hatten.

Für eine Folge der genannten Art ist $\bigcup_{i=1}^{\infty}(a_i)$ ein Ideal, also ein Hauptideal (d). Es gibt deshalb einen Index i, so daß d in (a_i) liegt. Es folgt $(d) \subset (a_i) \subset (a_{i+1}) \subset (d)$. Damit haben wir einen Widerspruch deduziert.

Eindeutigkeit einer Zerlegung. Sei $a = p_1 \ldots p_r = q_1 \ldots q_s$. Da p_1 Primelement ist, teilt p_1 entweder q_1 oder $q_2 \ldots q_s$. Induktiv erkennt man: Es gibt ein j, so daß p_1 das Element q_j teilt. Da q_j unzerlegbar ist, gilt $(p_1) = (q_j)$. Sei $j = 1$. Wir dividieren durch p_1 und erhalten eine Gleichung $p_2 \ldots p_r = uq_2 \ldots q_s$ mit $u \in \mathbb{Z}^*$. Induktion nach der Anzahl der Faktoren liefert die Behauptung. □

Eine Produktzerlegung $a = up_1p_2 \cdots p_n$ einer ganzen Zahl a mit einer Einheit u und Primzahlen p_i heißt ihre *Primfaktorzerlegung* in die *Primfaktoren* p_i. Die Primfaktorzerlegung regelt die Teilbarkeitseigenschaften. Am besten faßt man dazu die gleichen Primfaktoren zu Primpotenzen zusammen und spricht dann von der *Primpotenzzerlegung*. Wir schreiben das in (2.3) formal auf.

(2.3) Teilbarkeit und Primfaktorzerlegung. Sei $x \in \mathbb{Z}$ von Null verschieden und p eine Primzahl. Es gibt genau ein $\nu \in \mathbb{N}_0$, so daß gilt: $p^\nu | x$ aber $p^{\nu+1} \not| x$. Wir setzen $\nu = \nu_p(x)$.

(1) Für eine Einheit x gilt $\nu_p(x) = 0$ für alle Primzahlen p.

(2) Es gilt $x|y$ genau dann, wenn für alle Primzahlen die Relation $\nu_p(x) \leq \nu_p(y)$ besteht.

(3) Der GGT der Familie $(a_j \mid j \in J)$ ist eine Zahl d, die durch die Bedingungen
$$\nu_p(d) = Min\{\nu_p(a_j) \mid j \in J\}$$
bis auf Assoziierte bestimmt ist.

(4) Das KGV der endlichen Familie $(a_j \mid j \in J)$ ist eine Zahl m, die durch die Bedingungen
$$\nu_p(m) = Max\{\nu_p(a_j) \mid j \in J\}$$
bis auf Assoziierte bestimmt ist. ◇

3 Ganzzahlige Matrizen

Sei $M(m,n;\mathbb{Z})$ die Menge der (m,n)-Matrizen $(a_{ij} \mid 1 \le i \le m,\ 1 \le j \le n)$ mit Eintragungen $a_{ij} \in \mathbb{Z}$. Zwei solche Matrizen werden komponentenweise addiert, und das Produkt von Matrizen wird nach der bekannten Formel definiert. Wir setzten $M_n(\mathbb{Z}) = M(n,n;\mathbb{Z})$.

(3.1) Notiz. *Eine Matrix $A \in M_n(\mathbb{Z})$ hat genau dann ein Inverses in $M_n(\mathbb{Z})$, wenn* $\det(A) \in \mathbb{Z}^*$ *ist.*

Beweis. Ist $AB = I$ die Einheitsmatrix, so ist nach dem Produktsatz $1 = \det(AB) = \det(A)\det(B)$, also $\det(A) \in \mathbb{Z}^*$. Ist $\det(A) \in \mathbb{Z}^*$, so läßt sich eine inverse Matrix $B = (b_{ij})$ durch die Formel der Cramerschen Regel

$$b_{ij} = (-1)^{i+j} \det(A_{ij}) \det(A)^{-1}$$

gewinnen (A_{ij} ist die durch Streichung der i-ten Zeile und j-ten Spalte entstehende Untermatrix, wie üblich). Da $\det(A)$ eine Einheit ist, wird durch die Formel wirklich ein Element $b_{ij} \in \mathbb{Z}$ definiert. □

Die Menge der ganzzahlig invertierbaren Matrizen in $M_n(\mathbb{Z})$ bezeichnen wir mit $GL(n,\mathbb{Z})$ und mit $SL(n,\mathbb{Z})$ darin die Teilmenge der Matrizen mit der Determinante 1. Diese Mengen bilden bezüglich der Matrizenmultiplikation eine Gruppe.

Wir wollen im folgenden das grobe Normalformenproblem für Matrizen aus $M(m,n;\mathbb{Z})$ behandeln. Dazu definieren wir: $U, V \in M(m,n;\mathbb{Z})$ heißen *äquivalent*, wenn mit geeigneten $A \in GL(m,\mathbb{Z})$ und $B \in GL(n,\mathbb{Z})$ eine Gleichung $U = AVB$ gilt. Dadurch wird eine Äquivalenzrelation definiert, wie eine leichte Überlegung lehrt. Wir bezeichnen eine Matrix aus $M(m,n;\mathbb{Z})$ als Diagonalmatrix $\mathrm{Dia}(a_1, a_2, \ldots)$, wenn a_j der Eintrag an der Stelle (j,j) ist und alle anderen Einträge Null sind.

(3.2) Satz. *Eine ganzzahlige Matrix $U \in M(m,n;\mathbb{Z})$ ist zu einer Diagonalmatrix* $\mathrm{Dia}(d_1, \ldots, d_r, 0, \ldots, 0)$ *äquivalent, in der $d_i \neq 0$ ist und $d_i | d_{i+1}$ für $1 \le i < r$.*

Beweis. Wir geben zwei Beweise. Zunächst einen etwas theoretischen, der sich aber auf allgemeinere Fälle übertragen läßt, weil er nur allgemeine Teilbarkeitseigenschaften benutzt. Später einen, der sogar ein Rechenverfahren liefert. Ein Element $0 \neq x \in \mathbb{Z}$ besitzt eine Darstellung $x = up_1p_2 \ldots p_r$, worin u eine Einheit und jedes p_j unzerlegbar ist. Die Zahl r ist durch x eindeutig bestimmt. Wir setzen $L(x) = r$ und nennen r die *Länge* von x (mit $L(u) = 0$ für eine Einheit u). Ist d ein Teiler von x und gilt $L(d) = L(x)$, so sind d und x assoziiert; für jeden Teiler d von x gilt $L(d) \le L(x)$.

Wir bemerken, daß Vertauschung von Zeilen oder Spalten und Addition des Vielfachen einer Zeile (Spalte) zu einer anderen Zeile (Spalte) durch Multiplikation von links (rechts) mit einer invertierbaren Matrix bewirkt wird, also zu einer äquivalenten Matrix führt (elementare Zeilen- und Spaltenumformungen).

Wir betrachten die Länge $L(a'_{11})$ aller Elemente, die in zu A äquivalenten Matrizen $A' = (a'_{ij})$ auftreten. Wir wählen ein A' aus, für das diese Länge minimal ist, und nennen A' wieder A. Falls a_{11} die Elemente $a_{12}, \dots, a_{1n}$ und $a_{21}, \dots, a_{m1}$ teilt, können wir aus A durch elementare Zeilen- und Spaltenumformungen eine Matrix der folgenden Form gewinnen:

(3.3) Bis auf die Stelle (1,1) stehen in der ersten Zeile und Spalte nur Nullen.

Falls a_{11} etwa a_{12} nicht teilt, so sei $(d) = (a_{11}, a_{12})$. Dann ist d ein Teiler von a_{11} und hat kleinere Länge als a_{11}, da aus $L(d) = L(a_{11})$ folgt, daß d zu a_{11} assoziiert und deshalb a_{11} ein Teiler von a_{12} ist. Sei $d = \lambda a_{11} + \mu a_{12}$, $a_{11} = da'_{11}$, $a_{12} = da'_{12}$. Dann ist die Matrix

$$V = \begin{pmatrix} \lambda & -a'_{12} & & & \\ \mu & a'_{11} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

invertierbar, denn sie hat die Determinante 1, und AV hat an der Stelle $(1,1)$ das Element d.

Das widerspricht der Minimaleigenschaft von a_{11}. Also können wir in jedem Fall die Form (3.3) erreichen. Addieren wir dann eine andere Zeile zur ersten, so sehen wir, daß a_{11} auch alle anderen Elemente teilt. Man behandelt jetzt die durch Streichen der ersten Zeile und Spalte entstehende Matrix analog. Man beachte dabei, daß ein Element, welches alle Elemente einer Matrix teilt, auch alle Elemente jeder äquivalenten Matrix teilt. □

Der nächste Satz zeigt, wie man die Größen $d_1, \dots, d_r$ aus A berechnen kann. Er zeigt außerdem, daß diese Elemente bis auf Multiplikation mit Einheiten durch A und die im Satz (3.2) genannten Teilbarkeitseigenschaften eindeutig bestimmt sind. Wir nennen die in (3.2) gewonnene Diagonalmatrix eine *Normalform* von U.

(3.4) Satz. *Sei U eine Matrix wie in* (3.2) *mit der dort angegebenen Normalform. Sei $\delta_k = d_1 d_2 \dots d_k$. Dann ist δ_k ein* GGT *aller Determinanten von (k,k)-Untermatrizen von U.*

Beweis. Die Behauptung ist offenbar richtig, wenn U eine Matrix in Normalform ist. Wie verändert sich der GGT der Determinanten aller (k,k)-Untermatrizen, wenn man von einer Matrix U zu einer äquivalenten übergeht? Gar nicht! Sei nämlich $U = (u_{ij})$ und $B = (b_{ij})$. Dann ist UB eine Matrix, deren Spalten Linearkombinationen der Spalten von U sind. Wegen der multilinearen Eigenschaft der Determinante sind die (k,k)-Unterdeterminanten von UB also Linearkombinationen derjenigen von U. Diese Tatsache impliziert $\delta_k(U) \mid \delta_k(UB)$. Ist B invertierbar, so gilt deshalb auch $\delta_k(UB) \mid \delta_k(U)$, d. h. in

diesem Fall gilt $(\delta_k(UB)) = (\delta_k(U))$. Entsprechendes gilt bei Linksmultiplikation von U mit einer invertierbaren Matrix. □

Die durch (3.2) gegebenen Ideale $(d_1), \ldots, (d_r)$ heißen die *Äquivalenz-Faktoren* oder *Äquivalenz-Ideale* der Matrix U.

Zweiter Beweis von (3.2). Der Beweis von (3.2) ist nicht konstruktiv. Wir geben jetzt ein Rechenverfahren an, das auf der Division mit Rest beruht. Falls alle $a_{ij} = 0$ sind, ist nichts zu beweisen. Andernfalls können wir durch elementare Umformungen bewirken, daß an die Stelle (1,1) das Element mit dem kleinsten von Null verschiedenen absoluten Betrag kommt. Wir nennen die neue Matrix wieder A. Die Elemente $a_{12}, \ldots, a_{1n}$ dividieren wir mit Rest durch a_{11}

$$a_{1r} = q_i a_{11} + r_i, \quad 0 \leq |r_i| < |a_{11}|.$$

Wir subtrahieren das q_i-fache der ersten Spalte von der i-ten für $i = 2, \ldots, n$ und erhalten eine Matrix mit der ersten Zeile $a_{11}, r_2, \ldots, r_n$. Ebenso verfahren wir mit der ersten Spalte. Sind danach nicht alle Elemente (außer a_{11}) der ersten Zeile und Spalte gleich Null, so wiederholen wir die Prozedur (kleinstes Element an die Stelle $(1,1)$, Division mit Rest, ...). Da bei diesem Verfahren die Elemente der ersten Zeile und Spalte absolut kleiner werden, bricht das Verfahren dadurch ab, daß wir bei einer Matrix der Form

$$\begin{pmatrix} x_{11} & 0 & \ldots & 0 \\ 0 & c_{22} & \ldots & c_{2n} \\ \vdots & & \ldots & \vdots \\ 0 & c_{m2} & \ldots & c_{mn} \end{pmatrix}$$

ankommen. Wir wiederholen mit dem Block (c_{ij}) dieses Verfahren. Schließlich erhalten wir eine Diagonalmatrix mit Diagonale $(c_1, \ldots, c_r, 0, \ldots, 0)$. Gilt $c_i = q_i c_1 + r_i$, $0 < r_i < |c_1|$, so formen wir um zu

$$\begin{pmatrix} c_1 & & c_i & \\ & \ddots & \vdots & \\ & & c_i & \\ & & & \ddots \end{pmatrix} \quad \text{und dann zu} \quad \begin{pmatrix} c_1 & & r_i & \\ & \ddots & \vdots & \\ & & c_i & \\ & & & \ddots \end{pmatrix}.$$

Mit dieser Matrix wiederholen wir den oben beschriebenen Prozeß und erhalten eine Diagonalmatrix mit Diagonale $(e_1, e_2, \ldots)$ und $|e_1| < |c_1|$. Dieses Verfahren bricht ab, wenn die im Satz genannten Teilbarkeitsbedingungen erfüllt sind.

4 Gitter

Wir wollen die im letzten Abschnitt beschriebene Transformation auf Normalform als Basiswechsel interpretieren. Dazu brauchen wir ganzzahlige Basen. Das führt auf den Begriff eines Gitters.

Wir betrachten die Menge $\mathbb{Z}^n$ der ganzzahligen n-Tupel mit komponentenweiser Addition und Multiplikation mit ganzzahligen Skalaren. Eine Teilmenge $N \subset \mathbb{Z}^n$ heißt *Gitter*, wenn mit $x, y \in N$ auch $x - y \in N$ und $\lambda x \in N$ ist ($\lambda \in \mathbb{Z}$). [2] Ein System $e_1, \ldots, e_m$ von Elementen in N heißt *Basis* des Gitters, wenn jedes x in N eine eindeutige Linearkombination $x = \sum_{j=1}^{m} \lambda_j e_j$ mit ganzzahligen Koeffizienten λ_j ist. Der Schnitt zweier Gitter ist wieder eines. Das nur aus dem Nullelement bestehende Gitter ist das *Nullgitter* 0.

(4.1) Notiz. *Seien $e_1, \ldots, e_k$ und $f_1, \ldots, f_l$ Basen eines Gitters $N \subset \mathbb{Z}$. Dann ist $k = l$.*

Beweis. Wir betrachten alles im Vektorraum $\mathbb{Q}^n$. Der von $e_1, \ldots, e_k$ erzeugte Unterraum hat die Dimension k. Gäbe es nämlich eine echte lineare Relation $\sum_j r_j e_j = 0$ zwischen diesen Elementen, so könnten wir durch Multiplikation mit dem Hauptnenner der $r_j \in \mathbb{Q}$ daraus eine echte ganzzahlige Relation machen, im Widerspruch zur Basiseigenschaft. Die Behauptung folgt jetzt aus der Wohldefiniertheit der Vektorraumdimension. □

(4.2) Notiz. *Sei $e_1, \ldots, e_k$ Basis eines Gitters $N \subset \mathbb{Z}$ und $f_1, \ldots, f_k$ ein System von Elementen aus N. Dann ist dieses System genau dann eine Basis des Gitters, wenn die durch $f_l = \sum_k a_{kl} e_k$ bestimmte Matrix (a_{kl}) in $GL(k, \mathbb{Z})$ liegt.*

Beweis. Nach den Regeln der linearen Algebra und der Definition einer Gitterbasis ist $f_1, \ldots, f_k$ genau dann eine Basis, wenn die Matrix ganzzahlige Einträge hat und als ganzzahlige Matrix invertierbar ist. □

(4.3) Satz. *Jedes Gitter hat eine Basis.*

Beweis. Sei $N \subset \mathbb{Z}^n$ ein Gitter und $x_1, \ldots, x_n$ eine beliebige Basis von $\mathbb{Z}^n$, zum Beispiel die Standardbasis aus den Einheitsvektoren. Sei $[x_1, \ldots, x_r]$ das von $\{x_1, \ldots, x_r\}$ *erzeugte* Gitter, das definitionsgemäß aus allen ganzzahligen Linearkombinationen dieser Elemente besteht, und $N_r = N \cap [x_1, \ldots, x_r]$. Wir zeigen, daß N_r eine Basis hat. Sei dazu

$$I_r = \{a_r \mid \text{ es gibt } c = a_1 x_1 + \cdots + a_r x_r \in N_r;\ a_i \in \mathbb{Z}\}.$$

Dann ist $I_r \subset \mathbb{Z}$ ein Ideal, etwa $I_r = (\lambda_r)$.

Wir wählen ein Element der Form $b_r = a_1 x_1 + \cdots + \lambda_r x_r \in N_r$, falls $\lambda_r \neq 0$ ist; andernfalls sei $b_r = 0$ gesetzt. Als Zwischenbehauptung zeigen wir durch Induktion nach r die Gleichheit $N_r = [b_1, \ldots, b_r]$. Für $r = 1$ ist entweder $b_1 = 0$, also $N_1 = 0$, oder $b_1 = \lambda_1 x_1$ und dann jedes $y = \lambda x_1 \in N_1$ ein Vielfaches von b_1, da λ ein Vielfaches von λ_1 ist. Ist $x \in N_r$ gegeben, so gibt es nach Wahl von b_r ein $\mu \in \mathbb{Z}$ mit $x - \mu b_r \in N_{r-1}$. Damit ist die Zwischenbehauptung gezeigt.

Wir beenden den Beweis, indem wir zeigen, daß die von Null verschiedenen unter den b_j linear unabhängig sind. Sei also $\sum \alpha_j b_j = 0$, sei k maximal mit

[2] Diese Definition ist der Gruppen- und Modultheorie angepaßt. Wird $\mathbb{Z}^n$ als additive Gruppe aufgefaßt, so besagt die erste Bedingung, daß N eine Untergruppe ist. Die zweite folgt in diesem Fall aus der ersten und besagt, daß N ein $\mathbb{Z}$-Untermodul von $\mathbb{Z}^n$ ist.

$\alpha_k \neq 0$ und $b_k \neq 0$. Dann ist der Koeffizient von x_k in dieser Summe gleich $\alpha_k\lambda_k$. Da die x_j eine Basis bilden, ist folglich $\alpha_k\lambda_k = 0$, im Widerspruch zu den Annahmen über α_k und λ_k. □

(4.4) Satz. *Sei M ein Gitter und $N \subset M$ ein Teilgitter. Dann gibt es eine Basis $e_1, \ldots, e_m$ von M und Elemente $d_1, \ldots, d_k$ mit $d_1 | \ldots | d_k$ aus $\mathbb{Z}$ derart, daß $f_1 = d_1e_1, \ldots, f_k = d_ke_k$ eine Basis von N ist.*

Beweis. Nach (4.3) haben M und N eine Basis. Wir schreiben die Basis von N Basis als Linearkombination einer Basis von M und bringen die resultierende Matrix nach (3.2) auf Normalform. Die Transformationsmatrizen werden wie in der Vektorraumtheorie als Basiswechselmatrizen interpretiert, wobei (4.2) verwendet wird. □

Basen mit den in (4.4) genannten Eigenschaften heißen der Inklusion $N \subset M$ *angepaßt*.

In der ebenen Geometrie lassen sich Gitter wie folgt veranschaulichen. Man betrachte zwei verschiedene Geraden durch den Nullpunkt und zu beiden jeweils eine Schar paralleler Geraden mit jeweils gleichem Abstand. Dadurch wird die Ebene in Parallelogramme aufgeteilt. Die Eckpunkte der Parallelogramme, d. h. die Schnittpunkte der Parallelenscharen bilden ein sogenanntes Gitter in $\mathbb{R}^2$. Haben alle Gitterpunkte ganzzahlige Koordinaten, so ist die Menge der Gitterpunkte ein Gitter im hier betrachteten Sinne. Nach (4.2) gibt es viele verschiedene Parallelogrammaufteilungen des rechtwinkligen Gitters aus Einheitsquadraten. Die Geraden der Scharen durch den Nullpunkt sind die von den Basisvektoren aufgespannten. Angepaßte Basen bedeuten in dieser Veranschaulichung, daß die Parallelogramme des kleinen Gitters sich aus Parallelogrammen des großen zusammensetzen. Es empfiehlt sich, einige Beispiele zu zeichnen. Im Dreidimensionalen kann man entsprechende Schnitte dreier Ebenenscharen betrachten.

3 Gruppen

1 Grundbegriffe

Eine *Verknüpfung* auf einer Menge G ist eine Abbildung $m\colon G \times G \to G$. Sie heißt *assoziativ*, wenn für je drei Elemente a, b, c aus G die Gleichheit $m(a, m(b, c)) = m(m(a, b), c)$ besteht. Ist m assoziativ, so sagen wir auch, m erfüllt das *Assoziativgesetz*. Der besseren Lesbarkeit halber notieren wir eine Verknüpfung abgekürzt meist als Multiplikation: $m(a, b) = a \cdot b = ab$. Statt verknüpfen sagen wir bei dieser Bezeichnungsweise auch multiplizieren. Das Assoziativgesetz lautet dann einfach $a(bc) = (ab)c$. Ist eine Verknüpfung assoziativ, so ist das Resultat einer Multiplikation von beliebig vielen Elementen $(a_1, \ldots, a_n)$ in dieser Reihenfolge unabhängig von der Auswahl der Klammerung, und wir schreiben dafür $a_1 \ldots a_n$ oder $a_1 \cdot a_2 \cdot \ldots \cdot a_n$.

Eine Verknüpfung m heißt *kommutativ* oder *abelsch*, wenn für je zwei Elemente a, b aus G die Gleichheit $ab = ba$ besteht, wenn also das *Kommutativgesetz* für m gilt. Ist eine Verknüpfung sowohl assoziativ als auch kommutativ, so ist das Resultat einer Verknüpfung von beliebig vielen Elementen sowohl von der Klammerung als auch von der Reihenfolge der Elemente unabhängig.

Ein Element $e \in G$ heißt *linksneutrales Element* einer Verknüpfung m auf G, wenn für alle $x \in G$ die Gleichung $m(e, x) = ex = x$ gilt, und *rechtsneutrales Element*, wenn immer $m(x, e) = xe = x$ gilt. Ist ein Element sowohl rechts- als auch linksneutral, so heißt es *neutrales Element*. Ist e linksneutral und f rechtsneutral, so folgt $e = ef = f$. Insbesondere hat eine Verknüpfung höchstens ein neutrales Element. Gilt $ab = e$, so heißt a *linksinvers* zu b und b *rechtsinvers* zu a. Aus $ab = e$ und $bc = e$ folgt $a = a(bc) = (ab)c = c$; in diesem Fall nennt man a ein *Inverses* von b und schreibt $a = b^{-1}$. Es ist dann b ein Inverses von b^{-1}, d. h. es gilt $(b^{-1})^{-1} = b$. Ein Paar (G, m) aus einer Menge G und einer assoziativen Verknüpfung m auf G mit neutralem Element heißt ein *Monoid* oder eine *Halbgruppe*.

Der Begriff einer Verknüpfung läßt viele Verallgemeinerungen zu. So wird jede Abbildung $m\colon A \times B \to C$ eine *zweistellige Verknüpfung* genannt und allgemein $A_1 \times \cdots \times A_n \to B$ eine *n-stellige Verknüpfung*.

(1.1) Gruppe. Eine *Gruppe* besteht aus einer Menge G und einer Verknüpfung m auf G, so daß die folgenden Axiome gelten:

(1) Die Verknüpfung ist assoziativ.
(2) Die Verknüpfung besitzt ein linksneutrales Element $e \in G$.
(3) Jedes $a \in G$ hat ein Linksinverses.

Ist (G, m) eine Gruppe, so heißt m eine *Gruppenstruktur* auf der Menge G. Wenn die Verknüpfung als Multiplikation geschrieben wird, so nennen wir m auch *Gruppenmultiplikation*. Eine Gruppe mit einer kommutativen Multiplikation wird *kommutative Gruppe* oder *abelsche Gruppe* genannt. In einer kommutativen Gruppe wird die Verknüpfung oft als Addition geschrieben, $m(a, b) = a+b$; in diesem Fall sprechen wir natürlich von der *Gruppenaddition*. Wir unterscheiden

diese beiden Notationen auch dadurch, daß wir von *additiven* und *multiplikativen* Gruppen reden. Es ist üblich, eine Gruppe (G, m) nur durch die zugrundeliegende Menge G zu bezeichnen, insbesondere dann, wenn man nicht mehrere Verknüpfungen unterscheiden muß. ◇

Wir leiten einige Folgerungen aus den Gruppenaxiomen her. Sie werden im weiteren stillschweigend verwendet.

(1.2) Satz. *Sei G eine multiplikative Gruppe. Dann gelten:*

(1) Linkskürzung. *Aus $ax = ay$ folgt $x = y$.*
(2) e rechtsneutral. *Für alle $x \in G$ gilt $xe = x$.*
(3) Rechtsinvers=Linksinvers. *Aus $ba = e$ folgt $ab = e$.*
(4) Rechtskürzung. *Aus $xa = ya$ folgt $x = y$.*
(5) Inverses eindeutig. *Aus $ba = ca = e$ folgt $b = c$.*

Beweis. (1) Sei $ba = e$. Wir schließen der Reihe nach $ax = ay,\ b(ax) = b(ay),\ (ba)x = (ba)y,\ ex = ey,\ x = y$.

(2) Wir wählen ein y, so daß $yx = e$ gilt. Dann folgt $y(xe) = (yx)e = ee = e = xy$, und wegen (1) gilt deshalb $xe = x$.

(3) Wir schließen der Reihe nach $b(ab) = (ba)b = eb = b = be$, und mit (1) folgt dann $ab = e$.

(4) Mit (3) wie für (1).

(5) folgt schließlich unmittelbar aus (4). □

In einer multiplikativen Gruppe schreiben wir das neutrale Element oft als 1 und nennen es das *Einselement* der Gruppe. Das bei gegebenem $a \in G$ eindeutig bestimmte Element b mit der Eigenschaft $ab = 1 = ba$ nennen wir das *Inverse* von a und bezeichnen es mit a^{-1}. Mit diesen Bezeichnungen gelten dann die Rechenregeln $1 \cdot a = a = a \cdot 1$ und $a^{-1} \cdot a = a \cdot a^{-1} = 1$. Ferner ist $(a^{-1})^{-1} = a$, und es gilt $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. In einer additiv geschriebenen abelschen Gruppe bezeichnen wir das neutrale Element mit 0 und nennen es das *Nullelement* der Gruppe. In einer additiv geschriebenen Gruppe ist das Inverse b von a durch die Gleichung $a + b = 0$ bestimmt; wir schreiben in diesem Fall $b = -a$ und $a - c$ statt $a + (-c)$.

(1.3) Die symmetrische Gruppe. Eine bijektive Abbildung $s\colon M \to M$ einer Menge M auf sich wird *Permutation* von M genannt. Sei $S(M)$ die Menge aller Permutationen von M. Verkettung von Abbildungen liefert eine Verknüpfung

$$\circ\colon S(M) \times S(M) \to S(M), \quad (s, t) \mapsto s \circ t,$$

da die Verkettung bijektiver Abbildungen wieder bijektiv ist. Verkettung von Abbildungen ist assoziativ. Die identische Abbildung von M ist ein neutrales Element. Das Inverse von s ist die Umkehrabbildung s^{-1}. Damit haben wir auf $S(M)$ eine Gruppenstruktur gewonnen. Wir nennen diese Gruppe die *symmetrische Gruppe* von M. Enthält M mehr als zwei Elemente, so ist $S(M)$ nicht kommutativ.

Ist $M = \{1, 2, \ldots, n\} =: [n]$, so schreiben wir $S(n)$ oder S_n statt $S(M)$. Bekanntlich hat $S(n)$ $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ (gelesen: n-Fakultät) Elemente.

Eine *Transposition* von $[n]$ ist eine Permutation, die zwei benachbarte Elemente vertauscht und die anderen festläßt. (Manchmal auch: Vertauschung zweier beliebiger Elemente, da dann der Begriff von der Anordnung unabhängig ist.) Jedes Element von $S(n)$ ist ein Produkt von Transpositionen; steht nämlich die 1 nicht an der ersten Stelle, so kann man sie so oft mit ihrem linken Nachbarn vertauschen, bis sie dort steht; sodann bringt man, ohne die 1 noch weiter zu behelligen, die 2 durch ebensolche Transpositionen an die zweite Stelle; und so weiter (vollständige Induktion nach n). ◇

Für das Rechnen in Gruppen verwenden wir die folgenden Bezeichnungen. Ist $S \subset G$, so sei $S^{-1} = \{s^{-1} \mid s \in S\}$. Sind H und K Teilmengen einer Gruppe G, so sei $HK = \{hk \mid h \in H, k \in K\}$. Ist $a \in G$, so setzen wir $aK = \{ak \mid k \in K\}$. Sinngemäß verwenden wir analoge Bezeichungen; so ist etwa $HaK^{-1} = \{hak^{-1} \mid h \in H, k \in K\}$ und $H^2 = HH$. Für additive Gruppen verwenden wir Bezeichnungen wie $H + K = \{h + k \mid h \in H, k \in K\}$ und $a + H = \{a + h \mid h \in H\}$.

Eine nichtleere Teilmenge H einer Gruppe G heißt *Untergruppe* von G (*echte* Untergruppe, falls $H \neq G$), in Zeichen $H < G$, wenn aus $x, y \in H$ immer $xy \in H$ und $x^{-1} \in H$ folgt. Dann ist nämlich die Einschränkung $H \times H \to H$, $(x, y) \mapsto xy$ definiert und eine Gruppenstruktur auf H. Der Durchschnitt einer beliebigen Menge von Untergruppen von G ist wieder eine Untergruppe von G. Ist S eine Teilmenge von G, so wird der Durchschnitt $\langle S \rangle$ aller S enthaltenden Untergruppen die *von S erzeugte* Untergruppe genannt; wegen $S \subset G$ gibt es jedenfalls S umfassende Untergruppen. Es besteht $\langle S \rangle$ aus dem Einselement von G und allen Elementen, die sich als Produkt $s_1 \cdot \ldots \cdot s_n$ von Elementen $s_j \in S \cup S^{-1}$ schreiben lassen, denn die Menge dieser Elemente ist eine Untergruppe und in jeder S umfassenden Untergruppe enthalten. Zum Beispiel erzeugen die Transpositionen die symmetrische Gruppe. Eine von einem Element erzeugte Gruppe heißt *zyklische* Gruppe. Jede Gruppe hat die nur aus dem neutralen Element bestehende *triviale* Untergruppe, die im Falle multiplikativer (oder additiver) Gruppen auch mit 1 (oder 0) bezeichnet wird.

Wir betrachten die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen. Ist $n \in \mathbb{Z}$, so ist die Menge $n\mathbb{Z} = \{kn \mid k \in \mathbb{Z}\} =: (n)$ aller ganzzahligen Vielfachen von n eine Untergruppe.

(1.4) Satz. *Sei H eine Untergruppe von $\mathbb{Z}$, die nicht nur die Null enthält. Dann gibt es in H positive Zahlen. Ist n die kleinste positive Zahl in H, so ist $H = (n)$.*

Beweis. Ist $x \in H$ gegeben, so dividieren wir x durch n mit Rest $x = qn + r$, $0 \leq r < n$. Da H eine Untergruppe ist, folgt $x - qn \in H$. Wegen der Minimalität von n ist $r = 0$. □

Seien (G, m) und (H, n) Verknüpfungen. Eine Abbildung $f\colon G \to H$ heißt *Homomorphismus* von (G, m) nach (H, n), wenn für alle $x, y \in G$ die Gleichung

$f(m(x,y)) = n(f(x), f(y))$ gilt. Schreiben wir beide Verknüpfungen als Multiplikation, so lautet diese Gleichung $f(x \cdot y) = f(x) \cdot f(y)$. Wir sagen für diesen Sachverhalt: f ist mit den beiden Verknüpfungen *verträglich* oder *vertauschbar* (erst multiplizieren dann abbilden = erst abbilden dann multiplizieren). Sind $f\colon L \to M$ und $g\colon M \to N$ Homomorphismen, so ist auch $g \circ f$ ein Homomorphismus. Ein Homomorphismus $f\colon M \to M$ heißt *Endomorphismus* der Verknüpfung. Ein bijektiver Homomorphismus heißt *Isomorphismus*; und *Automorphismus*, wenn er außerdem ein Endomorphismus ist. Ein injektiver Homomorphismus heißt *Monomorphismus*, ein surjektiver *Epimorphismus*. Die Umkehrabbildung eines bijektiven Homomorphismus ist selbst wieder einer. Zwei Verknüpfungen heißen *isomorph*, wenn es einen Isomorphismus zwischen ihnen gibt. Isomorphe Verknüpfungen sind algebraisch (d. h. von ihren Recheneigenschaften her) als gleich anzusehen.

(1.5) Notiz. *Sei $f\colon G \to H$ ein Gruppenhomomorphismus. Dann gilt:*

(1) $f(1) = 1$, $f(x^{-1}) = f(x)^{-1}$.

(2) *Ist G_1 Untergruppe von G, so ist $f(G_1)$ Untergruppe von H. Ist H_1 Untergruppe von H, so ist $f^{-1}(H_1)$ Untergruppe von G.*

Beweis. $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$. Es folgt $f(1) = 1$; wir sagen dafür: ein Homomorphismus von Gruppen respektiert die Einselemente. Damit ergibt sich $1 = f(1) = f(xx^{-1}) = f(x)f(x^{-1})$, und das ist nur möglich, wenn $f(x^{-1}) = f(x)^{-1}$ ist; wir sagen dafür: ein Gruppenhomomorphismus respektiert die Inversen. (2) folgt unmittelbar aus den Definitionen. □

Sei $f\colon G \to H$ ein Homomorphismus. Das Urbild der trivialen Untergruppe $\{1\}$, also die Menge aller Elemente von G, die auf das neutrale Element von H abgebildet werden, heißt der *Kern* von f. Eine Sequenz von Gruppen und Homomorphismen $f_i\colon G_i \to G_{i+1}$, $m \le i \le n$, heißt *exakt*, wenn das Bild eines Homomorphismus f_i gleich dem Kern des nächsten f_{i+1} ist. Eine exakte Sequenz der Form

$$1 \longrightarrow A \xrightarrow{a} B \xrightarrow{b} C \longrightarrow 1$$

heißt *kurze exakte Sequenz*; darin ist dann insbesondere a injektiv (siehe (2.5.)) und b surjektiv.

Ist $a \in G$ ein beliebiges Element einer Gruppe G, so definieren wir induktiv $a^0 = 1$, $a^1 = a$, $a^2 = a \cdot a$, $a^{n+1} = a^n \cdot a$ für $n \in \mathbb{N}$. Ferner setzen wir $a^{-n} = (a^n)^{-1}$ für $n \in \mathbb{N}$. In kommutativen Gruppen verwenden wir eine entsprechende additive Notation: Wir haben dann für $n \in \mathbb{Z}$ das n-fache na eines Gruppenelementes a zur Verfügung. Wir notieren ohne Beweis:

(1.6) Notiz. *Für beliebige ganze Zahlen m, n gilt $a^m a^n = a^{m+n}$. Mit anderen Worten: $\pi\colon \mathbb{Z} \to G$, $n \mapsto a^n$ ist ein Homomorphismus der additiven Gruppe $\mathbb{Z}$ in die multiplikative Gruppe G. Analog für die additive Notation.* □

Die *Ordnung der Gruppe* ist als ihre Elementanzahl definiert. Erzeugt ein Element a eine Untergruppe der Ordnung n, so heißt n die *Ordnung des Elementes*

a ($n = \infty$ erlaubt). Das Bild von π in der letzten Notiz ist die von a erzeugte zyklische Untergruppe.

(1.7) Lineare Gruppen. Wichtige Gruppen sind die aus der linearen Algebra bekannten Matrizengruppen. Sei K ein Körper. Dann bezeichnen wir die Gruppe der invertierbaren (n,n)-Matrizen mit Einträgen aus K bezüglich Matrizenmultiplikation als Verknüpfung mit $GL(n,K)$ oder $GL_n(K)$ und nennen sie *allgemeine lineare Gruppe* über K.

Die Determinante $\det\colon GL(n,K) \to K^*$ ist ein Homomorphismus. Der Kern ist die *spezielle* lineare Gruppe $SL(n,K)$. Wichtige Untergruppen von $GL(n,\mathbb{R})$ sind die *orthogonale Gruppe* $O(n)$ der orthogonalen (n,n)-Matrizen und die *spezielle* orthogonale Gruppe $SO(n) = O(n) \cap SL(n,\mathbb{R})$. Analog gibt es die *unitäre* Gruppe $U(n)$ der unitären Matrizen in $GL(n,\mathbb{C})$ und die *spezielle* unitäre Gruppe $SU(n) = U(n) \cap SL(n,\mathbb{C})$. ◇

Sei G eine Gruppe und $\varphi\colon G \to H$ eine bijektive Abbildungen zwischen Mengen. Dann gibt es auf H genau eine Gruppenstruktur, bezüglich der φ ein Isomorphismus ist. Wir sagen, die so auf H gewonnene Struktur entstehe durch *Strukturtransport* vermöge φ. In analogen Situationen verwenden wir diese mengentheoretische Bemerkung meist stillschweigend. Eine Anwendung besteht in der folgenden Konstruktion: Sei $i\colon U \to G$ ein injektiver Homomorphismus. Wir wählen eine Menge V, die U als Teilmenge enthält, und eine bijektive Abbildung $I\colon V \to G$, die auf U mit i übereinstimmt. Wir transportieren mit I die Struktur und erhalten eine zu G isomorphe Gruppe, die U als Untergruppe enthält.

Sei (G,m) eine Gruppe. Dazu gibt es die *Gegengruppe* $G^\circ = (G, m^\circ)$ mit der Multiplikation $m^\circ(a,b) = m(b,a)$. Ein *Antihomomorphismus* $f\colon G \to H$ zwischen Gruppen erfüllt $f(gh) = f(h)f(g)$; das ist dasselbe wie ein Homomorphismus in die Gegengruppe.

Sei $(G_j \mid j \in J)$ eine Familie von Gruppen. Auf dem mengentheoretischen Produkt $G = \prod_j G_j$ definieren wir durch komponentenweise Multiplikation eine Gruppenstruktur. Die Projektionen auf die Faktoren $\mathrm{pr}_j\colon G \to G_j$ sind dann Homomorphismen. Die Gruppe G heißt *Produkt* der Familie der G_j. Das ist ein Produkt im Sinne der Kategorientheorie. Sind $f_j\colon G_j \to H_j$ Homomorphismen, so ist das mengentheoretische Produkt $\prod_j f_j$ ein Homomorphismus. Die Elemente, die außerhalb der Stelle j das neutrale Element haben, bilden in G eine zu G_j isomorphe Untergruppe. Das Produkt zweier Gruppen G_1, G_2 bezeichnen wir durch $G_1 \times G_2$; analog für endlich viele Faktoren. Produkte werden auch *direkte Produkte* genannt.

(1.8) Aufgaben und Ergänzungen.

1. Haben alle Elemente einer Gruppe höchstens die Ordnung zwei, so ist die Gruppe kommutativ.

2. Die invertierbaren Elemente in einem Monoid M bilden mit der induzierten Verknüpfung eine Gruppe M^*.

3. Seien A, B und C Untergruppen von G und gelte $A < C$. Dann ist $AB \cap C =$

$A(B \cap C)$.

4. Ist $f\colon M \to N$ ein Monoidhomomorphismus, so gilt nicht notwendig $f(1) = 1$. Ist f surjektiv und M eine Gruppe, so ist auch N eine Gruppe.

5. Wieviele sinnvolle Klammerungen gibt es für ein Produkt von n Faktoren?

6. Die additive Gruppe $\mathbb{R}$ und die multiplikative Gruppe der positiven reellen Zahlen sind isomorph (Logarithmus und Exponentialfunktion).

7. Sei eine assoziative multiplikative Verknüpfung auf der Menge M gegeben. Seien $a_1, \ldots, a_n$ Elemente aus M. Ein Produkt $\prod_{j=1}^{n} a_j$ wird induktiv durch

$$\prod_{j=1}^{n+1} a_j = (\prod_{j=1}^{n} a_j) a_{n+1}$$

definiert. Durch Induktion nach n beweise man mit dem Assoziativgesetz

$$\prod_{\mu=1}^{m} a_\mu \cdot \prod_{\nu=1}^{n} a_{m+\nu} = \prod_{\sigma}^{m+n} a_\sigma.$$

Damit zeige man dann (1.6). Ist die Verknüpfung außerdem kommutativ, so zeige man induktiv nach n für jede Permutation φ die Gleichheit

$$\prod_{\nu=1}^{n} a_{\varphi(\nu)} = \prod_{\nu=1}^{n} a_\nu.$$

8. Eine Permutation in S_n ist ein Produkt von Transpositionen. Ein Element läßt sich im allgemeinen in verschiedener Weise als ein solches Produkt schreiben; nicht einmal die Anzahl der gebrauchten Transpositionen ist eindeutig. Dagegen ist für jedes Element festgelegt, ob man eine gerade oder ungerade Anzahl von Transpositionen braucht. Es gibt nämlich den Vorzeichenhomomorphismus *Signum* $\varepsilon\colon S_n \to \{\pm 1\}$, der dieses festlegt. Eine Permutation heißt *gerade*, wenn ihr Vorzeichen gleich 1 ist, andernfalls *ungerade*. Die geraden Permutationen bilden als Kern von ε eine Untergruppe von S_n, die *alternierende Gruppe* A_n.

9. Sei ein Diagramm

$$\begin{array}{ccccc} A & \xrightarrow{a} & B & \xrightarrow{b} & C \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \\ A' & \xrightarrow{a'} & B' & \xrightarrow{b'} & C' \end{array}$$

von Gruppen und Homomorphismen mit den folgenden Eigenschaften gegeben: Bild A=Kern b, b ist surjektiv, $\beta a = a'\alpha$, $b'a'$ ist der triviale Homomorphismus. Dann gibt es genau einen Homomorphismus $\gamma\colon C \to C'$, der $\gamma b = b'\beta$ erfüllt. Ist b' surjektiv, so ist γ surjektiv. Ist α surjektiv, β injektiv und Bild a'= Kern b', so ist γ injektiv.

2 Faktorgruppen

Für jede Untergruppe H von G ist die Relation

$$a \sim b \quad \Leftrightarrow \quad aH = bH \quad \Leftrightarrow \quad \text{es gibt } h \in H \text{ mit } ah = b \quad \Leftrightarrow \quad a^{-1}b \in H$$

eine Äquivalenzrelation auf G. Der linke Doppelpfeil dient dabei zur Definition und die beiden anderen werden leicht als gleichwertig erkannt. Die Äquivalenzklassen sind die Mengen der Form aH, $a \in G$. Die Menge aH heißt die *Rechtsnebenklasse* von a bezüglich H. Ebenso hat man die *Linksnebenklassen* Ha zur Verfügung. Wir bezeichnen mit G/H die Menge der Rechtsnebenklassen von G bezüglich H und mit $H\backslash G$ die Menge der Linksnebenklassen. Wir nennen die Restklassenabbildung $p\colon G \to G/H$, $g \mapsto gH$ die kanonische *Faktorabbildung* oder *Quotientabbildung*. Da wegen der Kürzungseigenschaft einer Gruppe jede Rechtsnebenklasse die Mächtigkeit von H hat, gilt die Gleichung

$$|G| = |H| \cdot |G/H|, \tag{2.1}$$

die hauptsächlich für endliches G interessant ist. Die Mächtigkeit $|G/H|$ heißt *Index* von H in G und wird auch mit $[G : H]$ bezeichnet. Insbesondere liefert (2.1) den *Satz von Lagrange*:

(2.2) Notiz. *Die Ordnung eines Elementes einer endlichen Gruppe teilt die Gruppenordnung. Die Ordnung einer Untergruppe teilt die Gruppenordnung.* □

Aus (2.2) folgt leicht: Eine Gruppe von Primzahlordnung ist zyklisch, denn ein vom neutralen Element verschiedenes kann keine echte Untergruppe erzeugen.

Sei G eine Gruppe und H eine Untergruppe. Dann ist für jedes $g \in G$ die Menge $gHg^{-1} := \{ghg^{-1} \mid h \in H\}$ wieder eine Untergruppe. Untergruppen der Form $K = gHg^{-1}$ heißen zu H *konjugiert*. Wir schreiben $H \sim K$, falls K zu H konjugiert ist. Konjugation von Untergruppen ist eine Äquivalenzrelation. Die Gesamtheit der Elemente

$$N(H) := N_G(H) := \{g \in G \mid gHg^{-1} = H\}$$

ist wiederum eine, H enthaltende, Untergruppe, die *Normalisator* von H in G genannt wird.

(2.3) Satz. *Sei H eine Untergruppe von G. Folgende Aussagen sind äquivalent:*

(1) $N_G(H) = G$.
(2) *Jede Rechtsnebenklasse gH ist eine Linksnebenklasse Hk.*
(3) *Jede Linksnebenklasse ist eine Rechtsnebenklasse.*
(4) *Für alle $g \in G$ gilt $gH = Hg$.*

Beweis. (1) ⇒ (4). Sei $gx \in gH$. Da $g^{-1}Hg = H$ ist, gibt es ein $y \in H$ mit $x = g^{-1}yg$. Also ist $gx = yg \in Hg$, und folglich gilt $gH \subset Hg$. Analog folgt $gH \supset Hg$ und damit insgesamt (4).

(4) ⇒ (2) und (3). Klar.

(2) ⇒ (4). Sei $gH = Hk$, also $g = hk$ für ein $h \in H$. Es folgt $Hg = H(hk) =$

$(Hh)k = Hk$ und damit (4).
(4) $\Rightarrow$ (1). Aus $gH = Hg$ folgt $(gH)g^{-1} = (Hg)g^{-1} = H(gg^{-1}) = H$. □

Gilt für eine Untergruppe H von G eine der Aussagen des letzten Satzes, so heißt H ein *Normalteiler* von G. Wir schreiben dafür $H \lhd G$.

(2.4) Satz. *Sei $H \lhd G$. Es gibt genau eine Gruppenstruktur auf G/H, so daß $p\colon G \to G/H$, $g \mapsto gH$ ein Homomorphismus wird.*

Beweis. Da p surjektiv ist, gibt es jedenfalls höchstens eine Gruppenstruktur auf G/H mit der genannten Eigenschaft. Falls es eine gibt, so muß sie $(g_1H)(g_2H) = (g_1g_2)H$ erfüllen. Damit durch die Vorschrift $(g_1H, g_2H) \mapsto g_1g_2H$ eine wohldefinierte Verknüpfung gegeben wird, muß folgendes gezeigt werden: Aus $g_iH = f_iH$ folgt $g_1g_2H = f_1f_2H$. Zunächst gibt es $h_i \in H$, so daß $g_i = f_ih_i$ ist. Da H Normalteiler ist, also $Hf_2 = f_2H$ gilt, besteht für ein geeignetes $k \in H$ die Gleichung $h_1f_2 = f_2k$. Insgesamt folgt $g_1g_2 = f_1h_1f_2h_2 = f_1f_2kh_2$ und, wegen $kh_2 \in H$, also $g_1g_2H = f_1f_2H$. □

Wir nennen G/H mit der durch (2.4) gegebenen Gruppenstruktur die *Faktorgruppe* oder *Quotientgruppe* von G nach dem Normalteiler H und lesen G/H als G *modulo* H. Ist von der Gruppe G/H die Rede, so ist damit immer die Faktorgruppe gemeint. Der Kern der Faktorabbbildung $p\colon G \to G/H$ ist H. Man bestätigt sofort, daß der Kern eines beliebigen Homomorphismus ein Normalteiler ist. Wir notieren noch:

(2.5) Notiz. *Ein Gruppenhomomorphismus ist genau dann injektiv, wenn sein Kern nur aus dem neutralen Element besteht.*

Beweis. Die Urbilder eines Elementes sind genau die Nebenklassen nach dem Kern des Homomorphismus. □

(2.6) Satz. *Sei H Normalteiler von G. Sei $f\colon G \to L$ ein Gruppenhomomorphismus mit dem Kern K. Es gibt genau dann einen Homomorphismus $F\colon G/H \to L$, der die Gleichung $Fp = f$ erfüllt, wenn $H \subset K$ ist. Genau dann ist F injektiv, wenn $H = K$ ist.*

Beweis. Es gelte $Fp = f$. Dann ist $K = f^{-1}(1) = p^{-1}(F^{-1}(1)) \supset p^{-1}(1) = H$. Sei umgekehrt $H \subset K$. Wir wollen F durch $(gH) := f(g)$ definieren und müssen zeigen, daß dadurch eine wohldefinierte Abbildung gegeben wird. Sei $g_1H = g_2H$, also $g_1 = g_2h$ für ein $h \in H$. Weil h im Kern von f liegt, folgt $f(g_1) = f(g_2h) = f(g_2)f(h) = f(g_2)$. □

Für viele Überlegungen ist der folgende einfache *Entsprechungssatz* nützlich.

(2.7) Satz. *Sei $p\colon G \to L$ ein surjektiver Homomorphismus mit dem Kern K. Die Zuordnung $H \mapsto p^{-1}(H)$ liefert eine Bijektion zwischen den Untergruppen von L und denjenigen Untergruppen von G, die K enthalten. Bei dieser Zuordnung entsprechen sich auch die jeweiligen Normalteiler.*

Beweis. Die Umkehrabbildung wird durch $A \mapsto p(A)$ geliefert. □

(2.8) Notiz. (2.6) *hat die folgende Konsequenz: In einer exakten Sequenz*

$$1 \to H \xrightarrow{i} G \xrightarrow{j} L \to 1$$

von Gruppen und Homomorphismen induziert j einen Isomorphismus $G/K \cong L$, $gK \mapsto j(g)$, wobei $K = i(H)$ gesetzt wurde. □

Die Automorphismen einer Gruppe G bilden bezüglich Verkettung eine Gruppe, die *Automorphismengruppe* $\mathrm{Aut}(G)$ von G. Für jedes $g \in G$ ist

$$c_g \colon G \to G, \quad x \mapsto gxg^{-1}$$

ein Automorphismus, genannt *Konjugation* mit g. Elemente h und ghg^{-1} heißen *konjugiert*. Konjugiertheit ist eine Äquivalenzrelation auf G. Die Automorphismen der Form c_g heißen *innere* Automorphismen von G. Die inneren Automorphismen bilden einen Normalteiler $\mathrm{In}(G)$ von $\mathrm{Aut}(G)$ (Beweis!). Die Faktorgruppe $\mathrm{Aut}(G)/\mathrm{In}(G) =: \mathrm{Out}(G)$ heißt Gruppe der *äußeren* Automorphismen von G. Die Normalteiler von G sind die Untergruppen, die bei allen inneren Automorphismen in sich abgebildet werden. Eine Untergruppe, die sogar bei allen Automorphismen in sich abgebildet wird, heißt *charakteristische* Untergruppe.

(2.9) Zyklische Gruppen. Sei $m > 0$ eine natürliche Zahl. Die Faktorgruppe $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m = \mathbb{Z}/(m)$ ist eine zyklische Gruppe der Ordnung m, genannt die Gruppe der Restklassen modulo m, weil zwei ganze Zahlen genau dann dasselbe Element in dieser Gruppe repräsentieren, wenn sie bei Division mit m denselben Rest ergeben. Man schreibt für $a - b \in (m)$ auch $a \equiv b \bmod m$ und sagt dazu, a ist *kongruent zu* b modulo m. In dieser Schreibweise besagt $a \equiv 0 \bmod m$, daß a durch m teilbar ist. Ist C eine von $a \in C$ erzeugte Gruppe der Ordnung m, so ist $\pi \colon \mathbb{Z} \to C$, $k \mapsto a^k$ ein surjektiver Homomorphismus. Der Kern hat nach (1.7) die Form (n), und nach (2.8) ist $\mathbb{Z}/(n) \cong C$. Also ist $n = m$. Eine zyklische Gruppe der Ordnung n ist zu $\mathbb{Z}/n$ isomorph. Eine Untergrupe einer zyklischen Gruppe ist zyklisch, ebenso eine Faktorgruppe. Zu jedem Teiler m von n gibt es genau eine Untergruppe (Faktorgruppe) der Ordnung m von $\mathbb{Z}/n$.

Sei S^1 die multiplikative Gruppe der komplexen Zahlen vom Betrag eins. Sie kann mit $U(1)$ identifiziert werden und ist zu $SO(2)$ isomorph. Ist $m \in \mathbb{N}$, so besteht die von $\exp(2\pi i/m) = \zeta_m$ erzeugte Untergruppe C_m von S^1 aus den Elementen $1, \zeta_m, \ldots, \zeta_m^{m-1}$, ist also eine zyklische Gruppe der Ordnung m. Durch $k \mapsto \zeta_m^k$ wird ein Isomorphismus $\mathbb{Z}/m \to C_m$ vermittelt. Eine komplexe Zahl, die die Gleichung $x^m = 1$ erfüllt, heißt m-te *Einheitswurzel*. Die Gruppe C_m ist die Gruppe der m-ten Einheitswurzeln. ◇

Eine zyklische Gruppe hat im allgemeinen verschiedene Erzeuger. Eine m-te Einheitswurzel heißt *primitiv*, wenn sie C_m erzeugt.

(2.10) Satz. *Die Restklasse von $k \in \mathbb{Z}$ erzeugt genau dann $\mathbb{Z}/m$, wenn k zu m teilerfremd ist.*

Beweis. Sei k zu m teilerfremd. Dann gibt es ganze Zahlen a, b, die der Gleichung $ak = 1 + bm$ genügen, und folglich ist das a-fache der Klasse von k die

Klasse von 1. Haben andererseits k und m einen gemeinsamen Teiler $d > 1$, so ist das m/d-fache von $k \bmod m = k + m\mathbb{Z}$ das neutrale Element von $\mathbb{Z}/m$, so daß $k \bmod m$ eine Untergruppe kleinerer Ordnung als m erzeugt. Analog ist ζ_m^k genau dann eine primitive m-te Einheitswurzel, wenn k zu m teilerfremd ist. □

(2.11) Kommutatorgruppe. Sind g, h Elemente einer Gruppe G, so heißt $[g,h] := ghg^{-1}h^{-1}$ ihr *Kommutator*. Die von allen Kommutatoren erzeugte Untergruppe $[G,G]$ ist ein Normalteiler von G, genannt die *Kommutatorgruppe* von G. Die Kommutatorgruppe ist sogar eine charakteristische Untergruppe. Der Quotient $G^{ab} = G/[G,G]$ ist abelsch und heißt die *abelsch gemachte* Gruppe G. Die Faktorabbildung $p\colon G \to G^{ab}$ hat die folgende universelle Eigenschaft: Zu jedem Homomorphismus $\varphi\colon G \to A$ in eine abelsche Gruppe gibt es genau einen Homomorphismus $\Phi\colon G^{ab} \to A$ mit $\Phi \circ p = \varphi$. Ein Beweis wird mit (2.6) geführt.◇

Wir benutzen im folgenden meist stillschweigend den Entsprechungssatz (2.7) sowie (2.8). Ist H Normalteiler von G und gilt $H \subset K \subset G$ für eine Untergruppe K, so ist H auch Normalteiler in K. Wir erhalten eine Untergruppe $K/H \subset G/H$. Ist auch K Normalteiler von G, so liefert (2.6) einen Homomorphismus $G/H \to G/K$, $gH \mapsto gK$. Dieser hat den Kern K/H. Insgesamt erhalten wir den *ersten Isomorphiesatz*:

(2.12) Satz. *Seien H und K Normalteiler von G und sei $H \subset K$. Dann ist K/H Normalteiler von G/H, und es gibt einen kanonischen Isomorphismus $(G/H)/(K/H) \cong G/K$, der auf Repräsentanten die Identität ist.* □

(2.13) Notiz. *Seien H und K Untergruppen von G. Dann gilt: Genau dann ist HK eine Untergruppe, wenn $HK = KH$ ist. Ist $K < N_G(H)$, so gilt $HK = KH$, und H ist Normalteiler in HK.*

Beweis. Sei $h_1k_1, h_2k_2 \in HK$. Dann ist $k_1h_2 = hk$, da $HK = KH$. Folglich ist $h_1k_1h_2k_2 = h_1hkk_2 \in HK$. Ebenso sieht man $(h_1k_1)^{-1} \in HK$. Also ist HK Untergruppe von G. Die Inklusion $K < N_G(H)$ besagt, daß für jedes $k \in K$ die Gleichung $kH = Hk$ gilt; somit gilt $HK = KH$. Ferner gilt $hkH = hHk = Hk = Hhk$, und deshalb ist $H \lhd HK$. □

(2.14) Notiz. *Sei $H \lhd K < G$ und $L < G$. Dann ist $H \cap L \lhd K \cap L$.*

Beweis. Die Abbildung $K \cap L \to K/H$, $x \mapsto xH$ hat den Kern $H \cap L$. □

Wir beweisen den *zweiten Isomorphiesatz*.

(2.15) Satz. *Seien H und K Untergruppen von G und gelte $K < N_G(H)$. Dann induziert die Inklusion $K \subset HK$ induziert Isomorphismus $K/(H \cap K) \cong HK/H$.*

Beweis. Wir verwenden (2.13). Der Kern von $K \to (HK)/H$, $k \mapsto kH$ besteht aus den k mit $kH = H$, ist also gleich $H \cap K$. Also wird nach (2.6) eine Injektion $K/(H \cap K) \to HK/H$ induziert. Nach Konstruktion ist die Abbildung auch surjektiv. □

Als kleine Verallgemeinerung des Satzes von Lagrange haben wir:

(2.16) Notiz. *Seien H und K Untergruppen von G. Dann gilt $|HK|\cdot|H\cap K| = |H|\cdot|K|$.*

BEWEIS. Auf $H\times K$ wird durch $(h,k)\sim(hu,u^{-1}k)$, $u\in H\cap K$ eine Äquivalenzrelation definiert. Die Äquivalenzklassen sind genau die Urbilder der Abbildung $H\times K\to HK$, $(h,k)\mapsto hk$. □

Sind H und K vertauschbare Untergruppen von G, d. h. gilt $hk=kh$ für alle $h\in H, k\in K$, so ist $p\colon H\times K\to HK$, $(h,k)\mapsto hk$ ein surjektiver Homomorphismus. Der Kern besteht aus den Paaren (h,k) mit $k=h^{-1}$. Durch $i\colon H\cap K\to H\times K$, $x\mapsto(x,x^{-1})$ wird eine Injektion auf den Kern von p gegeben. Man beachte, daß wegen der Vertauschbarkeit $H\cap K$ abelsch ist. Wir haben also für vertauschbare H,K ein exakte Sequenz:

$$\textbf{(2.17)}\qquad 1\to H\cap K\xrightarrow{\ i\ } H\times K\xrightarrow{\ p\ } HK\to 1.$$

(2.18) Satz. *Sei $H\lhd G$ und $K\lhd G$. Dann ist $HK\lhd G$. Wir haben eine exakte Sequenz*

$$1\to HK/H\to G/H\to G/HK\to 1,$$

in der die zweite und dritte Abbildung auf Repräsentanten durch die Identität gegeben ist.

BEWEIS. Nach (2.13) ist $HK<G$. Sei $hk\in HK$ und $g\in G$. Dann ist wegen $ghkg^{-1}=ghg^{-1}gkg^{-1}$ und der Voraussetzung $ghkg^{-1}\in HK$. Das zeigt $HK\lhd G$. Der Kern der surjektiven Abbildung $G/H\to G/HK$ ist offenbar gleich HK/H.□

(2.19) Satz. *Seien A,B,C Untergruppen von G und gelte $A\lhd B$ und $B<N_G(C)$. Dann ist $AC\lhd BC$.*

BEWEIS. Wegen $A<B<N_G(C)$ sind nach (2.15) AC und BC Untergruppen von G. Sei $bc\in BC$ und $ac_1\in AC$. Für $a\in A$ gilt $aC=Ca$. Also hat cac_1c^{-1} die Form ac_2 mit $c_2\in C$. Es folgt

$$y:=(bc)(ac_1)(bc)^{-1}=bac_2b^{-1}=bab^{-1}bc_2b^{-1}.$$

Nach den Voraussetzungen ist $bab^{-1}\in A$ und $bc_2b^{-1}\in C$. Folglich ist $y\in AC$. Das zeigt die Behauptung. □

(2.20) Satz. *Sei U,u,V,v Untergruppen von G und sei $u\lhd U, v\lhd V$. Dann ist $u(U\cap v)\lhd u(U\cap V)$.*

BEWEIS. Sei $A=U\cap v$, $B=U\cap V$ und $C=u$. Nach (??.3) ist $A\lhd B$ und nach Voraussetzung $B=U\cap V<U<N_G(u)=N_G(C)$. Die Behauptung folgt nun aus (2.19). □

(2.21) Satz. *Die Inklusion $U\cap V\to u(U\cap V)$ induziert einen Isomorphismus*

$$u(U\cap V)/u(U\cap v)\cong U\cap V/(u\cap V)(U\cap v).$$

Indem wir die Rolle von U und V vertauschen erhalten wir insgesamt den Isomorphismus von Zassenhaus

$$u(U \cap V)/u(U \cap v) \cong (U \cap V)v/(u \cap V)v.$$

BEWEIS. Die Zusammensetzung der genannten Inklusion und der Quotientabbildung liefert $U \cap V \to u(U \cap V)/u(U \cap v)$ mit dem Kern $(U \cap V) \cap u(U \cap v)$. Diese letztere Gruppe ist aber gleich $(u \cap V)(U \cap v)$, wie eine leichte Umrechnung zeigt. □

3 Produkte

Sei $(G_j \mid j \in J)$ eine Familie von Gruppen. Das Produkt $G = \prod_j G_j$ haben wir schon im ersten Abschnitt definiert. Der folgende Satz zeigt, unter welchen Umständen eine Gruppe das Produkt von Untergruppen ist.

(3.1) Satz. *Seien $G_1, \ldots, G_n$ Untergruppen der Gruppe G. Folgende Aussagen sind äquivalent:*

(1) *Die Abbildung*

$$\pi\colon \prod_{j=1}^{n} G_j \to G, \quad (g_1, \ldots, g_n) \mapsto g_1 \ldots g_n$$

ist ein Isomorphismus.

(2) *Die G_i sind Normalteiler, G wird von $\bigcup_j G_j$ erzeugt und für alle j gilt: G_j hat mit dem Erzeugnis der G_i, $i \neq j$ den Schnitt 1.*

(3) *Die G_i sind Normalteiler, und die Abbildung π aus (1) ist bijektiv.*

BEWEIS. Offenbar impliziert (1) die Aussagen (2) und (3). Und offenbar impliziert (3) die Aussage (2). Gelte also (2). Da die G_i Normalteiler sind, gilt $G_iG_j = G_jG_i$, und damit sieht man, daß π surjektiv ist. Aus $\pi(g_1, \ldots, g_n) = \pi(u_1, \ldots, u_n)$ folgt nach (2) zunächst $g_1 = u_1$ und dann induktiv $g_j = u_j$. Also ist π bijektiv. Ist $i \neq j$, $x \in G_i$ und $y \in G_j$, so folgt $xyx^{-1}y^{-1} \in G_i \cap G_j$, weil beide Gruppen Normalteiler sind. Also sind Elemente in verschiedenen Gruppen miteinander vertauschbar, und deshalb ist π ein Homomorphismus. □

Ist eine der Aussagen in (3.1) erfüllt, so sagen wir, G sei das *interne* (direkte) Produkt der Untergruppen $G_1, \ldots, G_n$.

(3.2) Satz. *Seien H und G Gruppen, und sei $\tau\colon G \to \mathrm{Aut}(H)$, $g \mapsto \tau_g$ ein Homomorphismus. Auf der Menge $H \times G$ wird durch die Vorschrift*

$$(x, g) \cdot (y, h) = (x \cdot \tau_g(y), gh)$$

eine Gruppenstruktur mit dem Inversen $(x, g)^{-1} = (\tau_{g^{-1}}(x^{-1}), g^{-1})$ und dem neutralen Element $(1, 1)$ definiert.

BEWEIS. Es ist die Assoziativität nachzurechnen, das neutrale Element und die Formel für das Inverse. □

Die so konstruierte Gruppe wird mit $H \times_\tau G$ bezeichnet und *semidirektes Produkt* von H mit G vermöge τ genannt. Durch $(x, g) \mapsto g$ wird ein surjektiver Homomorphismus $H \times_\tau G \to G$ gegeben. Der Kern $\{(x, 1) \mid x \in H\}$ ist ein zu H isomorpher Normalteiler. Die Menge $\{(1, g) \mid g \in G\}$ ist eine zu G isomorphe Untergruppe, aber im allgemeinen kein Normalteiler (3.3). Es gilt

$$(1, g)(x, 1)(1, g)^{-1} = (\tau_g(x), 1).$$

Damit werden die Automorphismen τ_g in der größeren Gruppe $H \times_\tau G$ durch innere Automorphismen induziert.

(3.3) Notiz. *Sei G Untergruppe und H Normalteiler einer Gruppe K. Die Abbildung*

$$\mu\colon H \times G \to K, \quad (h, g) \mapsto hg$$

sei bijektiv. Konjugation mit Elementen aus G liefert einen Homomorphismus $\tau\colon G \to \mathrm{Aut}(H)$. Dann ist μ, aufgefaßt als Abbildung von $H \times_\tau G$, ein Isomorphismus. □

Die vorstehende Notiz liefert eine *interne* Beschreibung von semidirekten Produkten.

(3.4) Die affine Gruppe. Sei K ein Körper. Wir betrachten die Gesamtheit der Abbildungen $K^n \to K^n$ der Form $\varphi_{a,A}\colon x \mapsto Ax + a$ mit $A \in GL(n, K)$ und $a \in K^n$. Es gilt

$$\varphi_{b,B} \circ \varphi_{a,A} = \varphi_{Ba+b,BA}.$$

Durch die Abbildung $\varphi_{a,A}$ sind a und A bestimmt. Die Menge dieser Abbildungen ist mit der Verkettung eine Gruppe, die *affine Gruppe* $A(n, K)$. Die Untergruppe der Abbildungen $x \mapsto x + a$ ist zur additiven Gruppe K^n isomorph. Sie ist ein Normalteiler in $A(n, K)$, und ihre Elemente heißen *Translationen*. Wir haben einen surjektiven Homomorphismus $A(n, K) \to GL(n, K)$, $\varphi_{a,A} \mapsto A$. Die Gruppe $GL(n, K)$ ist eine Automorphismengruppe der additiven Gruppe K^n, und zwar ist $\tau(A)$ der Automorphismus $a \mapsto Aa$. Die Abbildung

$$K^n \times_\tau GL(n, K) \to A(n, K), \quad (a, A) \mapsto \varphi_{a,A}$$

ist ein Isomorphismus. ◇

(3.5) Kranzprodukt. Sei G eine Gruppe und G^n ihr n-faches Produkt Ist $\pi \in S_n$, so erhalten wir einen Automorphismus τ_π von G^n durch Vertauschung der Faktoren

$$\tau_\pi\colon (g_1, \ldots, g_n) \mapsto (g_{\pi^{-1}(1)}, \ldots, g_{\pi^{-1}(n)}).$$

Es gilt $\tau_{\pi\rho} = \tau_\pi \tau_\rho$. Das zugehörige semidirekte Produkt $G^n \times_\tau S_n$ wird das *Kranzprodukt* $G \int S_n$ von G mit S_n genannt. Für eine Untergruppe H von S_n wird analog $G \int H$ gebildet. ◇

Manchmal ist es zweckmäßig, das semidirekte Produkt etwas anders zu definieren. Sei $\tau\colon G \to \mathrm{Aut}(H)$ ein Antihomomorphismus. Damit wird das semidirekte Produkt $G \,{}_\alpha\!\times H$ mit der Multiplikation

$$(g,h)(u,v) = (gu, \tau_u(h)v)$$

definiert.

(3.6) Diedergruppen. Die Gruppe $\mathbb{Z}/2$ ist eine Automorphismengruppe von $\mathbb{Z}/n$, indem das nichttriviale Element durch $\tau\colon x \mapsto -x$ wirkt. Das semidirekte Produkt $D_{2n} := \mathbb{Z}/n \times_\tau \mathbb{Z}/2$ heißt *Diedergruppe* der Ordnung $2n$. Die Gruppe D_{2n} ist isomorph zur Symmetriegruppe eines regelmäßigen n-Ecks, d. h. zur Untergruppe der orthogonalen Gruppe $O(2)$, die ein regelmäßiges n-Eck in der Ebene mit dem Nullpunkt als Zentrum in sich abbildet. Wird $\mathbb{Z}/n$ durch $\mathbb{Z}$ ersetzt, so entsteht die unendliche Diedergruppe $D_\infty := \mathbb{Z} \times_\tau \mathbb{Z}/2$. Die Gruppe D_∞ ist isomorph zu einer Untergruppe der affinen Gruppe $A(1,\mathbb{R})$. ◇

(3.7) Notiz. *Seien $(G_j \mid j \in J)$ Gruppen und $H_j \lhd G_j$ Normalteiler. Das Produkt der Faktorabbildungen $p_j\colon G_j \to G_j/H_j$ hat den Kern $\prod_j H_j$. Also besteht nach* (2.8) *ein kanonischer Isomorphismus $(\prod_j G_j)/(\prod_j H_j) \cong \prod_j (G_j/H_j)$.* □

(3.8) Aufgaben und Ergänzungen.

1. Die orthogonale Gruppe $O(n)$ ist für ungerades n isomorph zu einem Produkt von $SO(n)$ und $\mathbb{Z}/2$ und für gerades n isomorph zu einem semidirekten Produkt dieser Gruppen.

2. Sei $B_2(K)$ die Gruppe der invertierbaren oberen Dreiecksmatrizen mit Einträgen aus dem Körper K, $D_2(K)$ die Untergruppe der Diagonalmatrizen und $U_2(K)$ die Untergruppe mit Einsen auf der Diagonale. Dann gibt es ein semidirektes Produkt

$$1 \to U_2(K) \to B_2(K) \to D_2(K) \to 1.$$

Die Gruppe $U_2(K)$ ist isomorph zur additiven Gruppe K. Wie wirkt in diesem Kontext ein Element von $D_2(K)$ als Automorphismus auf K?

3. In einer exakten Sequenz von Gruppen

$$1 \to H \to G \xrightarrow{\ p\ } K \to 1$$

ist G genau dann das semidirekte Produkt von H und einer zu K isomorphen Untergruppe, wenn p einen *Schnitt* $s\colon K \to G$ hat, welchletzteres ein Homomorphismus mit der Eigenschaft $ps = \mathrm{id}$ ist.

4. Die Homomorphismen $H \times_\tau G \to A$ entsprechen bijektiv den Paaren von Homomorphismen $\varphi\colon H \to A$, $\psi\colon G \to A$ mit der Eigenschaft $\varphi(\tau_g(h)) = \psi(g)\varphi(h)\psi(g)^{-1}$. Dem Paar φ, ψ wird dabei $(h,g) \mapsto \varphi(h)\psi(g)$ zugeordnet.

5. Verifikation von (3.3).

4 Gruppenoperationen

Gruppen wurden dazu erfunden, Symmetrien zu beschreiben. Der Symmetriebegriff wird im Begriff der Transformationsgruppe formalisiert.

(4.1) Transformationsgruppe. Eine *Operation* der Gruppe G auf der Menge X ist eine Abbildung $\rho\colon G \times X \to X$ mit den folgenden Eigenschaften:

(1) Für alle $g, h \in G$ und $x \in X$ gilt $\rho(g, \rho(h, x)) = \rho(gh, x)$.

(2) Für das neutrale Element $e \in G$ und $x \in X$ gilt $\rho(e, x) = x$.

Oft schreiben wir statt $\rho(g, x)$ einfach gx. Dann nehmen die Eigenschaften (1) und (2) die vertrautere Form $g(hx) = (gh)x$ und $ex = x$ an.

Eine *Transformationsgruppe* ist ein Tripel (G, ρ, x), das aus einer Gruppe G, einer Menge X und einer Operation ρ von G auf X besteht. Wir sagen kurz, X ist eine *G-Menge*, wenn die Operation von G auf X gegeben ist oder unterstellt wird. ◇

Für jedes $g \in G$ wird die Abbildung $L_g\colon X \to X,\ x \mapsto gx$ als *Linkstranslation* mittels g bezeichnet. Die Eigenschaften (1) und (2) besagen dann $L_g L_h = L_{gh}$ und $L_e = \mathrm{id}(X)$. Wegen $L_g L_{g^{-1}} = L_{gg^{-1}} = L_e = \mathrm{id}(X)$ ist L_g bijektiv. Die Zuordnung $g \mapsto L_g$ ist ein Homomorphismus von G in die symmetrische Gruppe von X.

Sei (G, ρ, X) eine G-Menge. Ist $x \in X$ gegeben, so heißt $Gx := \{gx \mid g \in G\}$ die *Bahn* der Operation *durch* x. Die Menge X zerfällt in Bahnen: Durch

$$x \sim y \quad \Leftrightarrow \quad x = gy \quad \text{für ein} \quad g \in G$$

wird eine Äquivalenzrelation auf X gegeben, deren Äquivalenzklassen die Bahnen sind. Die Menge der Äquivalenzklassen wird mit $G\backslash X$, gelesen X modulo G, bezeichnet und *Bahnenmenge* (= *Bahnenraum, Orbitmenge, Orbitraum*) genannt. Statt Bahn sagen wir auch *Orbit*. Die Mächtigkeit einer Bahn heißt auch ihre *Länge*.

Wir können Gruppenoperationen auch durch Abbildungen $X \times G \to X$, $(x, g) \mapsto xg$ mit den Eigenschaften $x(g_1 g_2) = (xg_1)g_2$, $xe = x$ definieren. Wir sprechen dann von einer *Rechtsoperation*, im Gegensatz zur anfangs definierten *Linksoperation*. Den Orbitraum bezeichnen wir in diesem Fall mit X/G. Dieselbe Bezeichnung wird allerdings oft auch für den Orbitraum einer Linksoperation verwendet.

(4.2) Beispiel. Ist H eine Untergruppe von G, so haben wir eine Linksoperation $H \times G \to G,\ (h, g) \mapsto hg$ von H auf G. Die Bahnenmenge ist die schon früher definierte Menge von Linksnebenklassen. Indem wir jedem Element $g \in G$ die Permutation l_g der Menge G zuordnen, erhalten wir einen injektiven Homomorphismus von G in die symmetrische Gruppe von G (*Satz von Cayley*). ◇

Eine Operation von G auf X heißt *transitiv*, wenn X nur aus einer einzigen Bahn besteht. Eine Operation heißt *effektiv*, wenn aus $L_g = \mathrm{id}$ folgt, daß $g = e$ ist. Eine Operation heißt *trivial*, wenn für $g \in G$ immer $gx = x$ gilt.

Für jedes $x \in X$ ist $G_x := \{g \in G \mid gx = x\}$ eine Untergruppe von G, die *Standgruppe* oder *Isotropiegruppe* oder *Stabilisator* der Operation im Punkt x genannt wird. Es gilt $G_{gx} = gG_xg^{-1}$. Eine Operation heißt *frei*, wenn alle Standgruppen nur aus dem neutralen Element bestehen.

(4.3) Beispiel. Die Gruppe $GL(n, K)$ operiert durch Matrizenmultiplikation auf dem Vektorraum K^n von links

$$GL(n, K) \times K^n \to K^n, \quad (A, x) \mapsto Ax.$$

Alle Linkstranslationen sind sogar lineare Abbildungen.

Die Gruppe $SO(n)$ operiert in dieser Weise transitiv auf der *Einheitssphäre* $S^{n-1} = \{(x_i) \in \mathbb{R}^n \mid \sum_i x_i^2 = 1\}$. Die Standgruppe eines Punktes ist zu $SO(n-1)$ isomorph. ◇

Ist X eine G-Menge und $H \subset G$ eine Untergruppe, so heißt

$$X^H = \{x \in X \mid \text{für alle } h \in H \text{ ist } hx = x\}$$

die *H-Fixpunktmenge* von X.

Sind X und Y G-Mengen, so bezeichnen wir eine Abbildung $f\colon X \to Y$ als *G-Abbildung* oder als *G-äquivariant*, wenn für $g \in G$ und $x \in X$ immer $f(gx) = gf(x)$ gilt. Eine bijektive äquivariante Abbildung ist ein *Isomorphismus* von G-Mengen. Für eine äquivariante Abbildung f gilt $f(X^H) \subset Y^H$ und $G_x \subset G_{f(x)}$.

Sind $(X_j \mid j \in J)$ G-Mengen, so definieren wir auf dem mengentheoretischen Produkt $\prod_{j\in J} X_j$ eine G-Operation durch komponentenweise Operation (auch *Diagonaloperation* genannt) $g(x_j) := (gx_j)$.

Ist X eine G-Menge, Y eine Teilmenge von X und gilt für $g \in G$ und $y \in Y$ immer $gy \in Y$, so wird durch $G \times Y \to Y$ $(g, y) \mapsto gy$ eine G-Operation auf Y definiert. In diesem Fall heißt Y eine *G-invariante* oder *G-stabile* Teilmenge von X.

Jede Bahn ist eine G-invariante Teilmenge und jede G-invariante Teilmenge ist disjunkte Vereinigung von Bahnen.

Die Gruppe G operiert in natürlicher Weise auf G/H vermöge

$$G \times G/H \to G/H, \ (u, gH) \mapsto ugH.$$

Die Menge G/H mit dieser Operation heißt *homogener Raum* von G bezüglich H oder *homogene G-Menge*.

Sei (G, s, X) eine transitive Operation. Für $x \in X$ betrachten wir die Abbildung $F\colon G \to X, \ \ g \mapsto gx$, die nach Voraussetzung surjektiv ist. Sei $H = G_x$ die Standgruppe im Punkt x. Für $h \in H$ gilt dann $F(g) = F(gh)$. Also gibt es eine Abbildung $f\colon G/H \to X$, die mit der Restklassenabbildung $p\colon G \to G/H$ die Gleichung $fp = F$ erfüllt. Wir verifizieren:

(4.4) Lemma. *Die Abbildung f ist ein Isomorphismus von G-Mengen.*

Beweis. Da F surjektiv ist, so auch f. Nach Konstruktion ist f äquivariant. Sei $f(g_1H) = f(g_2H)$, also $g_1x = g_2x$, $g_2^{-1}g_1x = x$, $g_2^{-1}g_1 =: g \in H$. Wegen $g_1 = g_2h$

gilt $g_1H = g_2H$. Folglich ist f bijektiv und damit ein G-Isomorphismus, da die Umkehrabbildung wiederum eine G-Abbildung ist. □

Wir haben damit transitive G-Mengen, also Bahnen, als homogene Räume erkannt.

(4.5) Beispiel. Sei G endlich und X eine endliche G-Menge. Sei $A \subset X$ eine Teilmenge, die aus jeder Bahn genau ein Element enthält. Da X Vereinigung von Bahnen ist, gilt wegen (8.2) die *Bahngleichung*

$$|X| = \sum_{x \in A} |G/G_x| = \sum_{x \in A} |G|/|G_x|$$

für die Kardinalität von X. ◇

(4.6) Satz. *Seien H und K Untergruppen von G. Dann gilt:*

(1) *Es gibt genau dann eine G-Abbildung $G/H \to G/K$, wenn H zu einer Untergruppe von K konjugiert ist.*

(2) *Ist $a \in G$ und gilt $a^{-1}Ha \subset K$, so ist $R_a\colon G/H \to G/K$, $gh \mapsto gaK$ eine G-Abbildung. Jede G-Abbildung $G/H \to G/K$ hat diese Form.*

Beweis. Sei $f\colon G/H \to G/K$ eine G-Abbildung und gelte $f(eH) = aK$. Aus der Äquivarianz von f folgt $haK = aK$ für alle $h \in H$, und letzteres ist zu $a^{-1}Ha \subset K$ äquivalent. Ferner zeigt die Äquivarianz, daß $f = R_a$ ist. Umgekehrt wird R_a leicht als wohldefinierte äquivariante Abbildung verifiziert. □

(4.7) Beispiel. Eine Gruppe operiert auf sich selbst durch Konjugation

$$G \times G \to G, \quad (g,h) \mapsto ghg^{-1}.$$

Gruppenelemente heißen *konjugiert*, wenn sie in derselben Bahn bezüglich dieser Operation liegen. Ist $G = GL(n,\mathbb{C})$, so werden die Konjugationsklassen durch die Jordansche Normalform beschrieben.

Ist $P(G)$ die Menge aller Teilmengen von G, so operiert G durch Konjugation auf $P(G)$

$$G \times P(G) \to P(G), \quad (g,A) \mapsto gAg^{-1}.$$

Ist H eine Untergruppe von G, so auch gHg^{-1}. Wir nennen H und gHg^{-1} konjugierte Untergruppen von G. Die Isotropiegruppe von H bei dieser Operation ist der Normalisator NH. Also gibt es $|G/NH|$ zu H konjugierte Untergruppen. Eine Untergruppe $K \in P(G)$ ist genau dann Fixpunkt unter dieser Operation, wenn sie Normalteiler ist. Die Konjugationsklasse von H werde mit (H) bezeichnet. Auf der Menge $\mathrm{Kon}(G)$ der Konjugationsklassen von Untergruppen wird eine teilweise Ordnung gegeben durch die Festlegung: $(H) \leq (K) \iff$ H ist konjugiert zu einer Untergruppe von K (= H ist *subkonjugiert* zu K). ◇

Ist X eine rechte und Y eine linke H-Menge, so wird durch die Orbitmenge der Operation

$$H \times (X \times Y) \to X \times Y, \quad (h,(x,y)) \mapsto (xh^{-1}, hy)$$

die Menge $X \times_H Y$ definiert. Ist H eine Untergruppe von G, und wird G mit der H-Operation durch Rechtsmultiplikation versehen, so haben wir $G \times_H Y$. Durch Linksmultiplikation auf dem linken Faktor wird $G \times_H Y$ eine G-Menge. Ist Y eine G-Menge, so ist

$$G \times_H Y \to G/H \times Y, \quad (g, y) \mapsto (g, gy)$$

ein Isomorphismus von G-Mengen. Die G-Bahnen von $G \times_H Y$ entsprechen den H-Bahnen von Y. Aus den letzten beiden Aussagen erhalten wir, daß die G-Bahnen von $G/H \times G/K$ den Doppelnebenklassen HgK entsprechen, also der Menge $H\backslash G/K$.

Sei X eine G-Menge. Die Standgruppen der Punkte einer Bahn bilden eine Konjugationsklasse von Untergruppen. Zwei Bahnen sind genau dann isomorph, wenn die zugehörigen Konjugationsklassen gleich sind. Sei

$$X(H) = \{x \in X \mid (G_x) = (H)\}.$$

Zwei G-Mengen X und Y sind genau dann isomorph, wenn für alle $H < G$ die Mengen $X(H)/G$ und $Y(H)/G$ gleichmächtig sind. Einen Isomorphismus erhält man nämlich dadurch, daß isomorphe Bahnen aufeinander abgebildet werden. Isomorphie läßt sich auch durch Fixpunktdaten feststellen.

(4.8) Satz. *Endliche G-Mengen S und T einer endlichen Gruppe G sind genau dann isomorph, wenn für alle $H < G$ die Gleichheit $|S^H| = |T^H|$ besteht.*

Beweis. Die genannte Fixpunktbedingung ist offenbar notwendig. Sei sie erfüllt. Wir verwenden Induktion über die Anzahl der Konjugationsklassen von Isotropiegruppen. Sind $A \subset S$ und $B \subset T$ isomorphe G-Teilmengen, so sind S und T genau dann isomorph, wenn $S \setminus A$ und $T \setminus B$ isomorph sind. Aus der Gleichheit der H-Fixpunktdaten für S und T folgt diejenige für die Differenzmengen. Sei (K) maximal mit der Bedingung $|S^K| \neq 0$. Dann ist $|S^K| = |S(K)^K| = |S(K)/G||G/K^K|$. Also gibt es gleichviele Bahnen vom Typ G/K in S und T. Wir betrachten deshalb $S \setminus S(K)$ und $T \setminus T(K)$ und haben damit die Anzahl der Konjugationsklassen von Isotropiegruppen reduziert. □

(4.9) Satz. *Für eine G-Menge S gilt $|G||S/G| = \sum_{g \in G} |S^g|$.*

Beweis. Wir betrachten $U = \{(g, s) \mid gs = s\}$. Sortieren wir die Menge nach g, so erhalten wir $\bigcup_{g \in G} \{g\} \times S^g$. Sortieren wir nach s, so erhalten wir als Mächtigkeit $\sum_{s \in S} |G_s|$. Da aber $|G_s|$ nur von der Bahn von s abhängt und diese die Länge $|G|/|G_s|$ hat, ergibt sich $\sum_{x \in S/G} |G|$ wie gewünscht. □

Ist A Teilmenge von B, so fassen wir die symmetrische Gruppe $S(A)$ als Untergruppe von $S(B)$ auf, indem wir eine Permutation von A außerhalb von A durch die Identität fortsetzen. Ist A die disjunkte Vereinigung nichtleerer Teilmengen $A_1, \ldots, A_r$ und bezeichnet $S(A; A_1, \ldots, A_r) \subset S(A)$ die Untergruppe derjenigen Permutationen, die jedes A_j in sich abbilden, so ist in diesem Sinne

(4.10) $$S(A; A_1, \dots, A_r) = \prod_{j=1}^{r} S(A_j).$$

Sei $\pi \in S_n$. Die von π erzeugte zyklische Untergruppe habe die Ordnung $m = m(\pi)$. Die Operation von $\mathbb{Z}/m$ auf $[n]_\pi = \{1, \dots, n\}$, bei der $1 \bmod m$ durch π wirkt, habe die Bahnen $A_1, \dots, A_r$. Eine Bahn hat die Form einer geordneten Menge

(4.11) $$A_j = (x, \pi(x), \dots, \pi^{t-1}(x)), \qquad \pi^t(x) = x,$$

wenn t ihre (von j abhängige) Länge ist. Dabei kann für x irgendein Element der Bahn gewählt werden. (Siehe dazu auch Aufgabe 6.) Die Permutation zerfällt gemäß (5.10) in Permutationen π_j von A_j, die die *Zyklen* von π heißen. Die Schreibweise (5.11) als geordnete Menge sagt, um welche Permutation es sich handelt: Ein Element wird auf das rechts danebenstehende und das letzte auf das erste abgebildet. Beispielsweise hat

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 8 & 4 & 9 & 6 & 5 & 2 & 7 \end{pmatrix}$$

die Zyklen $(1, 3, 8, 2)$, (4), $(5, 9, 7)$.

(4.12) Notiz. *Permutationen $\pi, \rho \in S_n$ sind genau dann konjugiert, wenn sie für jedes $k \in \mathbb{N}$ dieselbe Anzahl von Zyklen der Länge k haben.*

Beweis. Seien π und ρ konjugiert durch $h \in S_n$ in der Form $\pi h = h\rho$. Dann ist $m(\pi) = m = m(\rho)$ und h ein Isomorphismus von $\mathbb{Z}/m$-Mengen $[n]_\rho \to [n]_\pi$.

Seien umgekehrt $A_1, \dots, A_r$ und $B_1, \dots, B_r$ die geordneten Bahnen von $[n]_\pi$ und $[n]_\rho$ so aufgeschrieben, daß A_j und B_j gleichmächtig sind. Die Konjugation von π und ρ wird dann durch die Bijektion bewirkt, die die Elemente von B_j der Reihe nach auf die Elemente von A_j abbildet. □

5 Sylow-Gruppen

Sei $n \in \mathbb{N}$ und $p \in \mathbb{N}$ ein Primteiler von n. Dann gibt es eine Zerlegung der Form $n = p^e m$ mit zu p teilerfremdem $m \in \mathbb{N}$. Wir nennen p^e den p-primären Anteil von n und $n = p^e m$ die p-primäre Zerlegung von n.

Wir betrachten in diesem Abschnitt nur endliche Gruppen. Ist G eine Gruppe der Ordnung $|G| = n$, so heißt eine Untergruppe P der Ordnung p^e von G eine *p-Sylowgruppe* von G. Die Sätze (5.1), (5.3) und (5.4) heißen die *Sylow-Sätze* der Gruppentheorie.

(5.1) Satz. *Eine Gruppe G besitzt zu jedem Primteiler ihrer Ordnung eine p-Sylowgruppe.*

Beweis. Sei X die Menge aller Teilmengen von G, die p^e Elemente haben. Auf X operiert G durch Linksmultiplikation $(g, U) \mapsto gU$. Wir zerlegen X in Bahnen

bezüglich dieser Operation. Die Menge X hat

$$\binom{n}{p^e} = \frac{n(n-1)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots 1}, \qquad n = |G|$$

Elemente. Diese Zahl ist zu p teilerfremd (Aufgabe). Es gibt deshalb eine Bahn, deren Mächtigkeit nicht durch p teilbar ist, etwa die Bahn B_U der Menge $U \in X$. Es gilt die Bahngleichung $|G| = |G_U| \cdot |B_U| = p^e m$. Die Ordnung der Standgruppe G_U teilt $|U|$, da allgemein für eine Untergruppe H und eine Teilmenge U genau dann $HU \subset U$ ist, wenn U aus Linksnebenklassen von H besteht. Da also demnach $|G_U|$ die Anzahl $|U| = p^e$ teilt und $|B_U|$ teilerfremd zu p ist, folgt aus der Bahngleichung $|G_U| = p^e$, d. h. G_U ist eine p-Sylowgruppe. □

Als leichte Folgerung erhalten wir den folgenden *Satz von Cauchy*

(5.2) Folgerung. *Ist p ein Primteiler der Gruppenordnung $|G|$, so enthält G ein Element der Ordnung p.*

Beweis. Ein Element $x \neq 1$ einer p-Sylowgruppe hat eine Ordnung p^k, $k > 0$. Die p^{k-1}-te Potenz von x hat dann die Ordnung p. □

(5.3) Satz. *Sei K eine Untergruppe von G, deren Ordnung durch p teilbar ist, und sei H eine p-Sylowgruppe von G. Dann gibt es $g \in G$, so daß $K \cap gHg^{-1}$ eine Sylowgruppe von K ist. Insbesondere sind alle p-Sylowgruppen von G konjugiert.*

Beweis. Wir betrachten die G-Menge G/H durch Einschränkung als K-Menge. Da $|G/H|$ teilerfremd zu p ist, so gibt es auch eine K-Bahn KgH mit dieser Eigenschaft. Die Standgruppe von gH ist $K \cap gHg^{-1}$. Also ist die Bahnenlänge $|K/K \cap gHg^{-1}|$ teilerfremd zu p. Folglich ist $K \cap gHg^{-1}$ eine Sylowgruppe von K. Ist K selbst eine Sylowgruppe, so ist also $K \cap gHg^{-1} = K \subset gHg^{-1}$, und aus Anzahlgründen besteht Gleichheit. □

Wegen des letzten Satzes ist eine p-Sylowgruppe in einer abelschen Gruppe eindeutig bestimmt. Es folgt dann leicht, daß die Gruppe direktes Produkt ihrer Sylowgruppen ist.

(5.4) Satz. *Sei s die Anzahl der p-Sylowgruppen einer Gruppe G mit p-primärer Zerlegung $|G| = p^e m$. Dann gilt $s|m$ und $s \equiv 1 \bmod p$.*

Da alle p-Sylowgruppen konjugiert zu einer festen H sind, ist $s = |G/NH|$. Wegen $m = |G/H| = |G/NH||NH/H|$ ist s ein Teiler von m. Auf der Menge S der p-Sylowgruppen operiert H durch Konjugation. Sei $K \in S^H$. Das bedeutet $H \subset NK$. Also sind H und K Sylowgruppen von NK und deshalb in NK konjugiert. Da K Normalteiler von NK ist, ist $H = K$. Also ist $|S^H| = 1$. Mit $|S| \equiv |S^H| \bmod p$ folgt $s \equiv 1 \bmod p$. □

(5.5) Beispiel. Sei $|G| = p^e q, e \geq 1$, mit Primzahlen $p > q$. Nach (5.4) ist s ein Teiler von q, und wegen $s \equiv 1 \bmod p$ und $p > q$ ist $s = 1$. Folglich ist die p-Sylowgruppe H von G ein Normalteiler. Es gibt in G ein Element der

Ordnung q. Die davon erzeugte Untergruppe sei K. Nach Abschnitt 3 ist G ein semidirektes Produkt $H \times_c K$, wobei $c\colon K \to \mathrm{Aut}(H)$ das Element k auf den inneren Automorphismus c_k abbildet. Ist $e = 1$, so ist H zyklisch und $\mathrm{Aut}(H) = (\mathbb{Z}/p)^*$. Diese Gruppe hat die Ordnung $p-1$. Wir werden später sehen, daß diese Gruppe zyklisch ist. Wenn q kein Teiler von $p-1$ ist, so ist α trivial und damit G zyklisch. Andernfalls erhalten wir eine nichtabelsche Gruppe. Damit haben wir einen Überblick über Gruppen der Ordnung pq für verschiedene Primzahlen p und q gewonnen. ◇

Das *Zentrum* einer Gruppe besteht aus den Elementen, die mit allen Gruppenelementen vertauschbar sind. Jede Untergruppe des Zentrums ist ein Normalteiler. Allgemeiner ist der *Zentralisator* einer Menge X in einer Gruppe G die Menge

$$Z(X) = \{g \in G \mid \text{ für alle } x \in X \text{ gilt } gx = xg\}.$$

Eine Gruppe der Ordnung p^e für eine Primzahl p heißt *p-Gruppe*.

(5.6) Satz. *Sei G eine nichttriviale p-Gruppe. Dann hat G ein nichtriviales Zentrum.*

Beweis. Wir betrachten die Operation von G auf $X = G$ durch Konjugation. Dann ist X^G das Zentrum. Wegen $|X^G| \equiv |X| \bmod p$, $|X| \equiv 0 \bmod p$ und $X^G \neq \emptyset$ ist $|X^G| > 1$. □

(5.7) Satz. *Sei G eine p-Gruppe. Dann gibt es eine Sequenz $1 = G_0 \subset G_1 \subset \ldots \subset G_n = G$ von Normalteilern G_i von G, so daß G_i/G_{i-1} zyklisch von der Ordnung p ist.*

Beweis. Induktion nach $|G|$. Ist $|G| > 1$, so gibt es im Zentrum eine Untergruppe G_1 der Ordnung p. Man wende die Induktionsvoraussetzung auf G/G_1 an, erhält dadurch eine Sequenz von Normalteilern $1 = H_1 \subset H_2 \subset \ldots \subset H_n = G/G_1$ mit sukzessiven Quotienten der Ordnung p darin und betrachte die Urbilder G_j von H_j bei der Quotientabbildung $G \to G/H$. □

(5.8) Beispiel. Eine Gruppe G der Ordnung p^2 ist abelsch. Hat sie nämlich ein Element der Ordnung p^2, so ist sie zyklisch. Andernfalls haben alle nichtneutralen Elemente die Ordnung p. Es gibt eine zentrale Untergruppe H der Ordnung p, und jedes Element im Komplement von H erzeugt eine Untergruppe K, mit der $G = H \times K$ gilt. ◇

6 Abelsche Gruppen

In diesem Abschnitt stellen wir einige Aussagen über abelsche Gruppen zusammen. Insbesondere klassifizieren wir die endlich erzeugten abelschen Gruppen.

Eine *Basis* einer (additiven) abelschen Gruppe A ist eine Teilmenge C mit der folgenden Eigenschaft: Jedes Element $a \in A$ besitzt eine eindeutige Darstellung als ganzzahlige Linearkombination

(6.1) $$a = \sum_{c \in C} n_c c, \qquad n_c \in \mathbb{Z}.$$

Zum Beispiel bilden die Einheitsvektoren $e_i = (0, \dots, 1, \dots, 0)$ mit einer 1 an der i-ten Stelle eine Basis von $\mathbb{Z}^n$. Eine abelsche Gruppe hat genau dann eine Basis der Mächtigkeit n, wenn sie zu $\mathbb{Z}^n$ isomorph ist. Ein Isomorphismus wird dadurch gegeben, daß die Basiselemente bijektiv auf die Standardbasis abgebildet werden. Besitzt A eine Basis, so heißt A eine *freie* abelsche Gruppe. Ist B eine weitere abelsche Gruppe, so ist ein Homomorphismus $f\colon A \to B$ einer freien abelschen Gruppe A durch die Werte auf einer Basis bestimmt, und diese Werte können beliebig vorgegeben werden. Homomorphismen zwischen freien abelschen Gruppen werden deshalb in Analogie zur Vektorraumtheorie durch ganzzahlige Matrizen beschrieben.

(6.2) Notiz. *Die Gruppe A habe eine Basis der Mächtigkeit n. Dann hat jede andere Basis ebenfalls die Mächtigkeit n.*

Beweis. Wir verwenden die bekannte lineare Algebra über dem Körper $\mathbb{Q}$. Wir können ohne wesentliche Einschränkung $A = \mathbb{Z}^n$ annehmen. Dann sind für $k > n$ jeweils k Elemente $y_1, \dots, y_k$ über $\mathbb{Q}$ linear abhängig. Nach Multiplikation einer linearen Relation mit dem Hauptnenner der Koeffizienten erhalten wir eine lineare Relation über $\mathbb{Z}$. Deshalb können die y_j keine Basis bilden. □

Die Mächtigkeit einer Basis heißt der *Rang* der Gruppe. Wir formalisieren im weiteren noch den Begriff einer freien abelschen Gruppe. Sei S eine Menge. Eine *freie abelsche Gruppe über S* ist eine Mengenabbildung $i\colon S \to F$ in eine abelsche Gruppe F mit der folgenden universellen Eigenschaft: Zu jeder Mengenabbildung $\varphi\colon S \to A$ in eine abelsche Gruppe A gibt es genau einen Homomorphismus $\Phi\colon F \to A$ mit $\Phi \circ i = \varphi$. Durch die universelle Eigenschaft ist $i\colon S \to F$ bis auf eindeutige Isomorphie bestimmt: Hat $j\colon S \to G$ ebenfalls die universelle Eigenschaft, so gibt es genau einen Isomorphismus $\alpha\colon F \to G$ mit $\alpha i = j$. Ist C eine Basis von A, so ist $i\colon C \subset A$ eine freie abelsche Gruppe über C. Zu jeder Menge S gibt es eine freie abelsche Gruppe: Sei $F(S)$ die Menge aller Funktionen $f\colon S \to \mathbb{Z}$, die nur an endlich vielen Stellen von Null verschiedene Werte annehmen. Durch Addition von Funktionswerten wird $F(S)$ eine Gruppe. Für $s \in S$ sei i_s die Funktion $i_s(t) = \delta_{s,t}$ (Kronecker-Symbol). Dann ist $i\colon S \to F(S)$, $s \mapsto i_s$ eine freie abelsche Gruppe über S. In einer solchen Gruppe ist nämlich das Bild $i(S)$ eine Basis von F.

Ist A eine abelsche Gruppe, so bilden die Elemente endlicher Ordnung von A eine Untergruppe $T(A)$, genannt die *Torsionsuntergruppe* von A. Ein Homomorphismus $f\colon A \to B$ bildet TA nach TB ab, induziert also $Tf\colon TA \to TB$, $a \mapsto f(a)$. Ist $A = TA$ so heißt A *Torsionsgruppe*, ist $TA = 0$, so heißt A *torsionsfrei*. Eine endliche abelsche Gruppe ist eine Torsionsgruppe.

(6.3) Satz. *Für jedes A ist A/TA torsionsfrei.*

Beweis. Sei $x \in A/TA$ ein Element der Ordnung n und $y \in A$ ein Urbild von x. Dann liegt ny in TA. Folglich hat auch y endliche Ordnung und liegt in TA,

was $x = 0$ zur Folge hat. □

Der folgende Satz wurde in I.4 bewiesen, und zwar für den Standardfall $A = \mathbb{Z}^n$.

(6.4) Satz. *Sei A eine freie abelsche Gruppe vom Rang n und B eine Untergruppe. Dann gibt es ein Paar $(a_1, \dots, a_n)$ und $(b_1, \dots, b_k)$ von Basen von A und B mit der Eigenschaft: Es gibt natürliche Zahlen $n_1, \dots, n_k$ mit $n_j a_j = b_j$. Diese Zahlen können überdies so gewählt werden, daß n_j ein Teiler von n_{j+1} ist.* □

Ein Paar von Basen mit den in (6.4) genannten Eigenschaften heißt der Inklusion $B \subset A$ *angepaßt*.

Aus dem voranstehenden Satz folgt jetzt leicht der *Struktursatz für endlich erzeugte abelsche Gruppen*:

(6.5) Satz. *Eine endlich erzeugte abelsche Gruppe G ist isomorph zu einem Produkt der Form*

$$\mathbb{Z}^r \times \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_k)$$

mit von Null verschiedenen n_j, die der Teilbarkeitsbedingung $n_1 | n_2 | \cdots | n_k$ genügen.

Beweis. Da die Gruppe G endlich erzeugt ist, gibt es einen surjektiven Homomorphismus $\varphi\colon \mathbb{Z}^n \to G$, der die Standardbasis von $A = \mathbb{Z}^n$ auf ein Erzeugendensystem abbildet. Sei B sein Kern. Wir wählen angepaßte Basen für $B \subset A$ wie im letzten Satz. Wir benutzen diese Basen, um φ durch eine ganzzahlige Diagonalmatrix zu beschreiben, d. h. wir erhalten ein Diagramm

$$\begin{array}{ccccc} B & \xrightarrow{\subset} & A & \xrightarrow{\varphi} & G \\ \downarrow\cong & & \downarrow\cong & & \\ \mathbb{Z}^k & \xrightarrow{\Phi} & \mathbb{Z}^n, & & \end{array}$$

in dem Φ durch $(x_1, \dots, x_k) \mapsto (n_1 x_1, \dots, n_k x_k, 0 \dots, 0)$ gegeben ist. Die Faktorgruppe nach dem Bild von Φ hat aber die behauptete Form. Die Zahl r ist der Rang von $G/T(G)$. □

(6.6) Notiz. *Sei $a \in \mathbb{N}$. Der Kern der Multiplikation $l_a\colon \mathbb{Z}/n \to \mathbb{Z}/n$, $x \mapsto ax$ hat die Ordnung (a, n).*

Beweis. Wir setzten $a = dm$ mit $d = (a, n)$. Da m zu n teilerfremd ist, so ist l_m ein Automorphismus, siehe (2.10). Es genügt also die Aussage für l_d zu zeigen. Im Kern liegen dann aber genau die Vielfachen von n/d. □

(6.7) Folgerung. *Der Endomorphismus l_a von $\mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$ hat die Ordnung $\prod_{j=1}^{r} (a, n_j)$.* □

(6.8) Satz. *Sei A eine endliche abelsche Gruppe der Ordnung n. Die Zahl n besitze die Primzahlzerlegung*

$$n = p_1^{n(1)} p_2^{n(2)} \dots p_r^{n(r)}$$

*mit paarweise verschiedenen Primzahlen p_j und $n(j) > 0$. Dann gibt es in A eine eindeutig bestimmte Untergruppe $A(p_j)$ der Ordnung $p_j^{n(j)}$ für $j = 1, \dots r$. Sie wird der p_j-*primäre *Anteil von A genannt. Es gilt*

$$A = \prod_{j=1}^{r} A(p_j) \tag{6.9}$$

(internes Produkt).

Beweis. Sei $A(j) = \{x \in A \mid p_j^{n(j)} x = 0\}$. Die Untergruppe $A(j)$ hat nach der letzten Folgerung die Ordnung $p_j^{n(j)}$. Jede Untergruppe H dieser Ordnung muß aber in $A(j)$ enthalten sein, da jedes Element von H eine Ordnung hat, die $p_j^{n(j)}$ teilt. Wir setzten $q_j = \prod_{i \neq j} p_i^{n(i)}$. Die Menge dieser Zahlen ist teilerfremd. Es gibt deshalb eine Darstellung $1 = \sum_j m_j q_j$. Für jedes $x \in A$ liegt $q_j x$ in $A(j)$. Wegen $x = \sum_j m_j q_j x$ ist die Abbildung

$$\prod_j A(j) \to A, \quad (a_1, \dots, a_r) \mapsto a_1 + \dots + a_r$$

surjektiv und aus Anzahlgründen bijektiv. □

(6.10) Satz. *Eine endliche abelsche Gruppe A ist Produkt zyklischer Gruppen von Primzahlpotenzordnung. Die Anzahl der zu $\mathbb{Z}/p^t$ isomorphen Faktoren einer Produktdarstellung ist durch A eindeutig bestimmt (p Primzahl).*

Beweis. Die Existenz folgt aus (6.5) und (6.8). Sei eine Zerlegung mit $a(j)$ Faktoren $\mathbb{Z}/p^j$ gegeben. Sei $b(k) = \sum_{k \geq j} a(j)$. Wir setzen $U_t(A) = \{x \in A \mid p^t x = 0\}$. Nach (6.7) hat $U_1(A)$ die Ordnung $p^{b(1)}$. Wir bilden $A/U_1(A)$. Dann hat $U_1(A/U_1(A)) \cong U_2(A)/U_1(A)$ die Ordnung $p^{b(2)}$. Induktiv sieht man, daß $U_k(A)/U_{k-1}(A)$ die Ordnung $p^{b(k)}$ hat. Die Zahlen $b(k)$ — und damit auch die Zahlen $a(k)$ — sind also durch die Gruppenstruktur bestimmt. □

Eine zu $(\mathbb{Z}/p)^n$ isomorphe abelsche Gruppe heißt *elementar abelsche* p-Gruppe vom Rang n. Die Gruppe $\mathbb{Z}/2 \times \mathbb{Z}/2$ wird manchmal *Kleinsche Vierergruppe* genannt.

7 Universelle Gruppen

Ein *abelsches Monoid* ist eine Menge H zusammen mit einer assoziativen und kommutativen Verknüpfung $H \times H \to H$, $(a, b) \mapsto a + b$ mit neutralem Element 0. Ein *Homomorphismus* $\alpha \colon H \to K$ zwischen Monoiden ist eine Abbildung mit den Eigenschaften $\alpha(h_1 + h_2) = \alpha(h_1) + \alpha(h_2)$ und $\alpha(0) = 0$. Ein *Untermonoid*

U eines Monoids H ist eine Teilmenge, die die Null enthält und mit a und b auch deren Summe. Sind H und K Monoide, so ist $H \times K$ mit komponentenweiser Verknüpfung das *Produktmonoid*. Sei $U \subset H$ ein Untermonoid. Durch

$$x \sim y \quad \Leftrightarrow \quad \text{es gibt } a, b \in U \text{ mit} x + a = y + b$$

wird auf H eine Äquivalenzrelation definiert. Sei H/U die Menge der Äquivalenzklassen und $p\colon H \to H/U$, $x \mapsto [x]$ die Faktorabbildung. Durch $[x] + [y] = [x + y]$ wird auf H/U eine wohldefinierte Verknüpfung gegeben; sie macht p zu einem Homomorphismus. Die Abbildung p auf das *Faktormonoid* H/U hat die folgende universelle Eigenschaft: Ist $f\colon H \to K$ ein Monoidhomomorphismus, der U im Kern $f^{-1}(0)$ enthält, so gibt es genau einen Homomorphismus $F\colon H/U \to K$ mit $Fp = f$. Ist H eine abelsche Gruppe und U eine Untergruppe, so ist H/U die übliche Faktorgruppe. Die Teilmenge H^* eines Monoids H der Elemente, die ein Inverses haben, ist eine Untergruppe.

(7.1) Definition. Eine *universelle Gruppe* eines abelschen Monoids H ist ein Homomorphismus $i\colon H \to K(H)$ in eine abelsche Gruppe $K(H)$ mit der folgenden universellen Eigenschaft: Zu jedem Homomorphismus $\varphi\colon H \to A$ in eine abelsche Gruppe A gibt es genau einen Homomorphismus $\Phi\colon K(H) \to A$ mit der Eigenschaft $\Phi \circ i = \varphi$. ◇

Wie üblich bestimmt die universelle Eigenschaft das Objekt eindeutig. Ist $i'\colon H \to K'(H)$ eine zweite universelle Gruppe, so gibt es nämlcih Homomorphismen $\alpha\colon K(H) \to K'(H)$ und $\beta\colon K'(H) \to K(H)$ mit $\alpha i = i'$ und $\beta i' = i$. Wegen $\beta\alpha i = i$ und $\alpha\beta i' = i'$ sind dann $\beta\alpha$ und $\alpha\beta$ Identitäten.

Ist $S \subset H$ ein Untermonoid, so ist $D(S) = \{(s, s) \mid s \in S\}$ ein Untermonoid von $H \times S$. Wir setzen

$$i_S\colon H \to H \times S/D(S) = K_S(H), \quad x \to [x, 0].$$

(7.2) Satz. *Der Homomorphismus i_S hat die folgenden Eigenschaften:*

(1) *Zu jedem Homomorphismus $\varphi\colon H \to A$ in ein Monoid A mit $\varphi(S) \subset A^*$ gibt es genau einen Homomorphismus $\Phi\colon K_S(H) \to A$ mit $\Phi i_S = \varphi$.*
(2) *Die Klasse von $(s, t) \in S^2$ in $K_S(H)$ hat das Inverse (t, s). Insbesondere besteht $i_S(S)$ aus invertierbaren Elementen.*
(3) *Im Fall $H = S$ ist i_H eine universelle Gruppe für H.*

Beweis. Wegen $\varphi(S) \subset A^*$ ist

$$\tilde{\Phi}\colon H \times SA, \quad (x, s) \mapsto \varphi(x) - \varphi(s)$$

definiert und ein Homomorphismus. Er enthält $D(S)$ im Kern und induziert deshalb einen Homomorphismus Φ mit $\Phi i = \varphi$.

Das Element $(s, t) + (t, s) = (s + t, t + s) \in D(S)$ ist für $(s, t) \in S^2$ äquivalent zur Nullklasse. Das belegt (2). Außerdem liefert $[x, s] = [x, 0] - [s, 0]$, daß Φ eindeutig durch die angegebenen eigenschaften bestimmt ist.

Die Aussage (3) ist ein Spezialfall von (1). □

(7.3) Beispiel. Die Inklusion $i\colon \mathbb{N}_0 \subset \mathbb{Z}$ ist eine universelle Gruppe. Die Konstruktion in (1.2) verallgemeinert die Konstruktion von $\mathbb{Z}$ aus $\mathbb{N}_0$ als Klassen von Paaren. ◇

Sei $f\colon A \to B$ ein Monoidhomomorphismus. Es gibt genau einen Gruppenhomomorphismus $K(f)$, der das Diagramm

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle i_A} & & \downarrow{\scriptstyle i_B} \\ K(A) & \xrightarrow{K(f)} & K(B) \end{array}$$

kommutativ macht. Die Existenz folgt aus der universellen Eigenschaft von i_A, angewendet auf $i_B \circ f$. Es gilt $K(fg) = K(f)K(g)$ und $K(\mathrm{id}) = \mathrm{id}$. Damit wird K zu einem Funktor von abelschen Monoiden zu abelschen Gruppen. Ferner gilt $K(f_1 + f_2) = K(f_1) + K(f_2)$ für $f_1, f_2\colon A \to B$. Auch diese Regeln sind fast unmittelbare Konsequenzen aus der universellen Eigenschaft.

(7.4) Satz. *Sei $f\colon A \times B \to C$ eine biadditive Abbildung für abelsche Monoide A, B, C. Es gibt genau eine biadditive Abbildung $K(f)$, die das Diagramm*

$$\begin{array}{ccc} A \times B & \xrightarrow{f} & C \\ \downarrow{\scriptstyle i_A \times i_B} & & \downarrow{\scriptstyle i_C} \\ K(A) \times K(B) & \xrightarrow{K(f)} & K(C) \end{array}$$

kommutativ macht.

Beweis. Daß f biadditiv ist, besagt: Für jedes $b \in B$ ist $f_b\colon a \mapsto f(a, b)$ ein Homomorphismus; ebenso für die andere Variable. Wegen des universellen Eigenschaft von i_A gibt es $K(f_b)$. Die Zuordnung

$$B \to \mathrm{Hom}(K(A), K(C)), \quad b \mapsto K(f_b)$$

ist ein Homomorphismus, der nach der universellen Eigenschaft von i_B einen Homomorphismus

$$\tilde{K}(f)\colon K(B) \to \mathrm{Hom}(KA), K(C))$$

liefert. Die adjungierte biadditive Abbildung $K(f)$ zu $\tilde{K}(f)$ hat die gewünschten Eigenschaften. □

Die universelle Gruppe $K(H)$ zu H wird manchmal auch *Grothendieck-Gruppe* von H genannt.

(7.5) Aufgaben und Ergänzungen.

1. Die Äquivalenzrelation auf $H \times S$ zur Definition von $KS(X)$ lautet: $(x, s) \sim (y, t)$ genau dann wenn es ein $u \in S$ mit $x + t + u = y + s + v$ gibt.

2. Es gilt genau dann $i_S(a) = i_S(b)$, wenn ein $u \in S$ mit $a + u = b + u$ existiert.
3. Ist $i\colon H \to K(H)$, $x \to [x]$ eine universelle Gruppe, so hat jedes Element von $K(H)$ die Form $[x] - [y]$.
4. Was ist $K(H)$, wenn H selbst schon eine Gruppe ist?

8 Präsentation von Gruppen

Sei M ein Monoid und $\sim$ eine Äquivalenzrelation auf M mit der Eigenschaft

$$\textbf{(8.1)} \qquad x \in M,\, y \sim z \quad \Rightarrow \quad xy \sim xz,\, yx \sim zx.$$

Dann wird auf der Menge $\overline{M} = M/\sim$ der Äquivalenzklassen $\overline{x}$ durch $\overline{y} \cdot \overline{z} = \overline{yz}$ die Struktur eines Monoids erklärt (Quotientmonoid), da (8.1) gerade die Unabhängigkeit vom Repräsentanten liefert. Die Quotientabbildung $p\colon M \to \overline{M}$, $x \mapsto \overline{x}$ ist ein Monoidhomomorphismus.

Sei S eine Menge. Ein *Wort* der Länge $n \in \mathbb{N}_0$ über S ist eine Sequenz $(x_1, \ldots, x_n)$ von Elementen $x_i \in S$ (leere Sequenz für $n = 0$). Sei $M(S)$ die Menge aller Worte über S. Durch die Verknüpfung

$$(x_1, \ldots, x_m) \cdot (y_1, \ldots, y_n) = (x_1, \ldots, x_m, y_1, \ldots, y_n)$$

wird auf $M(S)$ die Struktur eines Monoids definiert. Die leere Sequenz ist das neutrale Element. Die Abbildung $\iota\colon S \to M(S)$, die jedem $x \in S$ die Sequenz (x) zuordnet, hat die folgende universelle Eigenschaft: Ist $\alpha\colon S \to M$ eine beliebige Abbildung in ein Monoid M, so gibt es genau einen Monoidhomomorphismus $A\colon M(S) \to M$ mit $A \circ \iota = \alpha$, und zwar ist $A(x_1, \ldots, x_n) = \alpha(x_1)\alpha(x_2)\cdots\alpha(x_n)$, $A(\,) = 1$. Aus diesem Grunde heißt $M(S)$ (genauer $\iota\colon S \to M(S)$) das *freie Monoid* über S.

Eine *Involution* auf einer Menge S ist eine Abbildung $*\colon S \to S$, $x \mapsto x^*$ mit $x^{**} = x$ für alle x. Die Involution heißt *frei*, wenn immer $x \neq x^*$ ist. Sei $(S, *)$ eine Menge mit freier Involution. Auf $M(S)$ betrachten wir die Äquivalenzrelation, die von

$$\textbf{(8.2)} \qquad u \cdot x \cdot x^* \cdot v \quad \sim \quad u \cdot v$$

erzeugt wird (u, v Worte über S und $x \in S$). Zwei Worte x, y über S sind genau dann äquivalent, wenn es eine Sequenz $x = x_0, x_1, \ldots, x_m = y$ von Worten gibt, so daß x_{i+1} und x_i in einer Beziehung (8.2) stehen. Diese Äquivalenzrelation hat die Eigenschaft (8.1), die zur Bildung des Quotientmonoids gebraucht wird. Sei $F(S, *)$ das Quotientmonoid und

$$i\colon S \xrightarrow{\ \iota\ } M(S) \xrightarrow{\ p\ } F(S, *)$$

die kanonische Abbildung. Wegen (8.2) gilt

$$p(x_1, \ldots, x_m) \cdot p(x_m^*, \cdots, x_1^*) = p(x_1, \ldots, x_m, x_m^*, \ldots, x_1^*) = p(\,) = 1.$$

Deshalb gibt es in $F(S, *)$ Inverse, es handelt sich also um eine Gruppe. Ist $x \in S$, so bezeichnen wir $i(x)$ auch einfach mit x. Jedes Element von $F(S, *)$ hat dann

die Form eines Produktes $x_1 \cdots x_m$ mit $x_j \in S$. Es gilt dann übrigens $x^* = x^{-1}$, was in diesem Zusammenhang der Sinn der freien Involution ist.

(8.3) Satz. *Die Abbildung $i\colon S \to F(S,*)$ hat die folgende universelle Eigenschaft: Zu jeder Mengenabbildung $\alpha\colon S \to G$ in eine Gruppe G mit $\alpha(x^*) = \alpha(x)^{-1}$ gibt es genau einen Gruppenhomomorphismus $A\colon F(S,*) \to G$ mit $A \circ i = \alpha$. Für $x_1 \cdots x_m = x$ wie eben gilt $A(x) = \alpha(x_1) \cdots \alpha(x_m)$.*

Beweis. Sei $A_1\colon M(S) \to G$ der Monoidhomomorphismus mit $A_1 \circ \iota = \alpha_1$. Die Abbildung A_1 faktorisiert über die Quotientabbildung $p\colon M(S) \to F(S,*)$ und liefert einen Gruppenhomomorphismus A mit $A \circ p = A_1$. Es gilt dann $A \circ i = \alpha$. Da das Bild von i die Gruppe $F(S,*)$ erzeugt, ist A eindeutig bestimmt und hat die angegebene Form. □

Wie immer ist $i\colon S \to F(S,*)$ durch die universelle Eigenschaft bis auf eindeutige Isomorphie bestimmt. Ist S die disjunkte Vereinigung von X und Y und liefert $*$ eine Bijektion $X \to Y$, $x \mapsto x^*$, so setzen wir $F(X) = F(S,*)$ und nennen die Einschränkung $i\colon X \to F(X)$ die *freie* Gruppe über X. Die Gruppe $F(X)$ heißt einfach freie Gruppe. Der Grund ist die folgende universelle Eigenschaft, die sich unmittelbar aus dem vorigen Satz ergibt.

(8.4) Satz. *Zu jeder Mengenabbildung $\alpha\colon X \to G$ in eine Gruppe G gibt es genau einen Homomorphismus $A\colon F(X) \to G$ mit $A \circ i = \alpha$.* □

Indem wir als X ein Erzeugendensystem von G nehmen, sehen wir, daß jede Gruppe Faktorgruppe einer freien ist (bis auf Isomorphie).

Da $i\colon X \to F(X)$ injektiv ist (Aufgabe 1), betrachten wir i als Inklusion. Ein Element von $F(X)$ ist dann Produkt von Elementen aus X und deren Inversen. Im folgenden wollen wir wegen der gruppentheoretischen Bedeutung die freie Involution meist mit der Menge $S = X \amalg X^{-1}$ verwenden und die Involution als Übergang zum Inversen $X \to X^{-1}$, $x \mapsto x^{-1}$ mit $(x^{-1})^{-1} = x$ ansehen.

Sei R eine Menge von Worten in $S = X \amalg X^{-1}$ und $\overline{R}$ das Bild dieser Menge in $F(X)$. Sei $N(R)$ der Normalteiler in $F(X)$, der von $\overline{R}$ erzeugt wird. Die Gruppe $G = F(X)/N(R)$ heißt die von X mit den Relationen R erzeugte Gruppe. Sie wird durch $\langle X|R \rangle$ bezeichnet. Das Paar X, R heißt eine *Präsentation* von G durch *Erzeugende* X und *Relationen* R. Das Bild eines Wortes $(x_1, \ldots, x_n)$ über $X \amalg X^{-1}$ schreiben wir als Produkt $x_1 \cdots x_n$, obgleich $X \to \langle X|R \rangle$ nicht notwendig injektiv ist.

(8.5) Satz. *Die Gruppe $\langle X|R \rangle = G$ hat die folgende universelle Eigenschaft: Sei $\alpha\colon X \to H$ eine Mengenabbildung in eine Gruppe H. Für jedes Wort $(x_1, \ldots, x_n) \in R$ gelte $\alpha(x_1) \cdots \alpha(x_n) = 1$. Dann gibt es genau einen Gruppenhomomorphismus $A\colon G \to H$ mit $A(x) = \alpha(x)$ für $x \in X$.*

Beweis. Zunächst erhalten wir einen Homomorphismus aus der universellen Eigenschaft der freien Gruppe. Die Voraussetzung besagt, daß die Elemente aus $\overline{R}$ im Kern dieses Homomorphismus liegen. Dann liegt aber der ganze Normalteiler

$N(R)$ im Kern (Aufgabe 2), und der auf der Faktorgruppe induzierte Homomorphismus ist der gesuchte. □

(8.6) Notiz. *Jede Gruppe besitzt eine Präsentation, d. h. ist isomorph zu einer Gruppe der Form* $\langle X|R\rangle$.

Beweis. Sei (G, m) ein Gruppe. Wir setzen $X = G$. Die Menge R bestehe aus den Worten $\{(x, y, (xy)^{-1}) \mid x, y \in X\}$. Die Mengenabbildung $\alpha\colon X \to G$ sei die Identität. Dann gilt $\alpha(x)\alpha(y)\alpha((xy)^{-1}) = 1$, und folglich gibt es einen Homomorphismus $j\colon \langle X|R\rangle \to G$ mit $j(x) = \alpha(x) = x$ für $x \in X$. Nach Konstruktion von $\langle X|R\rangle$ ist die kanonische Abbildung $i\colon G = X \to \langle X|R\rangle$ ein Homomorphismus. Nach Konstruktion ist ij die Identität, und ji ist auf einem Erzeugendensystem die Identität. □

In praktischen Fällen verwenden wir für die Präsentationen auch weniger formale Bezeichnungen. Ein Beispiel macht die Handhabe klar. Sei $X = \{x, y\}$. Wir betrachten das Wort $(x, x, y^{-1}, y^{-1}, y^{-1})$. Für die Gruppe $\langle X|R\rangle$ schreiben wir in diesem Fall $\langle x, y|x^2y^{-3}\rangle$ oder $\langle x, y|x^2 = y^3\rangle$, weil die universelle Eigenschaft besagt, daß die Homomorphismen nach G genau den Mengenabbildungen $\alpha\colon \{x, y\} \to G$ mit $\alpha(x)^2 = \alpha(y)^3$ entsprechen.

(8.7) Diedergruppen. Die Diedergruppe D_{2n} war im dritten Abschnitt als das semidirekte Produkt $\mathbb{Z}/n \times_\tau \mathbb{Z}/2$ definiert worden. Diese Gruppe hat die beiden Präsentationen

$$G = \langle A, B|A^n, B^2, BAB^{-1} = A^{-1}\rangle, \quad H = \langle S, T|S^2, T^2, (ST)^n\rangle.$$

Um das einzusehen, zeigen wir zunächst, daß die beiden Präsentationen isomorphe Gruppen liefern. Isomorphismen werden durch die folgenden Zuordnungen induziert:

$$A \mapsto ST,\ B \mapsto S, \qquad S \mapsto B,\ T \mapsto BA.$$

Man hat nach der universellen Eigenschaft der Präsentationen zu verifizieren, daß diese Vorschriften Homomorphismen induzieren, was eine leichte Rechnung ist; sie sind dann offenbar invers zueinander. Man erhält inverse Isomorphismen $G \to D_{2n}$ durch $A \mapsto (1, 0)$, $B \mapsto (0, 1)$ und $D_{2n} \to G$ durch $(a, b) \mapsto A^aB^b$. ◇

(8.8) Satz. *Die symmetrische Gruppe* S_n *wird durch* $x(n-1) := \{x_1, \ldots, x_{n-1}\}$ *mit den Relationen*

$$\begin{array}{lrcll} (1) & x_ix_j & = & x_jx_i, & |i-j| \geq 2 \\ (2) & x_ix_jx_i & = & x_jx_ix_j, & |i-j| = 1 \\ (3) & x_i^2 & = & 1. & \end{array}$$

erzeugt.

Beweis. Sei G_n die Gruppe mit dieser Präsentation. Wegen der Relationen (3) ist jedes Element von G_n ein Produkt der Form $a_1a_2\cdots a_r$, wobei $a_j \in x(n-1)$ ist. Wir nennen ein formales Wort dieser Art ein Produkt über $x(n-1)$. Wir zeigen zunächst durch Induktion nach n:

(8.9) Lemma. *Jedes Wort über $x(n-1)$ kann auf Grund der Relationen in die Form $ax_{n-1}\cdots x_j$, $1 \le j \le n$ gebracht werden, wobei a ein Wort über $x(n-2)$ ist und im Fall $j = n$ rechts von a nichts steht.*

Beweis. Zunächst überlegen wir, daß es genügt, höchstens ein x_{n-1} zu verwenden. Angenommen, das Wort habe die Form $z = ax_{n-1}bx_{n-1}c$, worin b kein x_{n-1} enthält. Nach Induktionsvoraussetzung können wir annehmen, daß b höchstens ein x_{n-2} enthält. Da jedes Wort über $x(n-3)$ mit x_{n-1} vertauschbar ist, läßt sich z in die Form $ux_{n-1}x_{n-2}x_{n-1}v$ oder ux_{n-1}^2v bringen. Mittels (2) und (3) erhalten wir die gewünschte Form.

Wir gehen nun von einem Wort der Form $ax_{n-1}b$ aus, worin a und b Worte über $x(n-2)$ sind. Auf b wenden wir die Induktionsvoraussetzung an und gelangen mittels (1) zum behaupteten Ergebnis. □

Aus dem Lemma schließen wir $|G_n| \le n|G_{n-1}|$, also $|G_n \le n!$. Wir haben einen Homomorphismus $\rho\colon G_n \to S_n$, der x_j auf die Transposition $(j, j+1)$ abbildet. Eine leichte Überlegung zeigt die Relationen (1) – (3) für diese Transpositionen. Damit ist ρ wohldefiniert. Außerdem ist ρ surjektiv, da die Transpositionen S_n erzeugen. Wegen $|G_n| \le n!$ muß ρ ein Isomorphismus sein. □

Wir bemerken, daß auf Grund des letzten Lemmas jedes Element von S_n eine Normalformendarstellung durch die x_j hat.

(8.10) Satz. *Zu jeder Familie von Gruppen gibt es eine Summe.*

Beweis. Sei $(\langle X_j|R_j\rangle \mid j \in J)$ eine Familie von Gruppen, die durch eine Präsentation gegeben sind. Wir setzen die X_j als disjunkt voraus und nennen X ihre Vereinigung. Die R_j sind dann Worte über $X \amalg X^{-1}$. Sei $R = \bigcup_j R_j$. Wir haben Homomorphismen $i_j\colon \langle X_j|R_j\rangle \to \langle X|R\rangle$, die durch die Inkusion $X_j \subset X$ induziert sind. Diese i_j bilden eine Summe. Das folgt aus den universellen Eigenschaften der beteiligten Gruppen. □

Aus historischen Gründen wird die Summe in GRU auch das *freie Produkt* der beteiligten Gruppen genannt. Für das freie Produkt von G und H wird dabei $G * H$ geschrieben. Aus der Summe erhält man auch ein Pushout in GRU. Seien $i_1\colon G \to G * H$ und $j_1\colon H \to G * H$ die kanonischen Inklusionen in die Summe. Seien $J\colon P \to G$ und $I\colon P \to H$ Homomorphismen. Sei N der Normalteiler von $G * H$, der von den Elementen $\{i_1J(x) \cdot j_1I(x) \mid x \in P\}$ erzeugt wird. Wir setzen $Q = (G * H)/N$ und bezeichnen die Komposition von i_1 und j_1 mit der Quotientabbildung durch $i\colon G \to Q$, $j\colon H \to Q$. Dann bildet (i, j) ein Pushout von (J, I). Die universelle Eigenschaft wird unmittelbar mit der universellen Eigenschaft der Summe hergeleitet (Aufgabe).

Sind I und J Inklusionen von Untergruppen, so wird der Pushout mit $G *_P H$ bezeichnet und freies Produkt mit *amalgamierter* Untergruppe P genannt.

Wir behandeln zu diesen Begriffen ein Beispiel.

(8.11) Beispiel. Sei $SL(2,\mathbb{Z})$ die Gruppe der $(2,2)$-Matrizen mit ganzzahligen Einträgen und der Determinante 1. Darin gibt es die Elemente

$$B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad A = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

mit

$$B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A^3.$$

Wir betrachten die von A und B erzeugten zyklischen Untergruppen. Dadurch wird ein Homomorphismus

$$\kappa\colon \mathbb{Z}/6 *_{\mathbb{Z}/2} \mathbb{Z}/4 \to SL(2,\mathbb{Z})$$

gegeben. Man kann zeigen, daß κ ein Isomorphismus ist. Das liefert also die Präsentation

$$SL(2,\mathbb{Z}) = \langle\, A, B | A^2 = B^3, A^6, B^4 \,\rangle.$$

Elementare Zeilen und Spaltenumformungen zeigen, daß κ surjektiv ist. $\diamond$

(8.12) Aufgaben und Ergänzungen.

1. Die kanonische Abbildung $i\colon X \to F(X)$ ist injektiv, weil die analoge Abbildung in die freie abelsche Gruppe injektiv ist. Die abelsch gemachte freie Gruppe $F(X)$ ist die freie abelsche Gruppe über X. Die Gruppe $\mathbb{Z}$ ist die freie Gruppe über einer einelementigen Menge.

2. Sei C eine Teilmenge einer Gruppe G. Sei C^* die Menge, die aus C und C^{-1} und allen Konjugierten dieser Elemente besteht. Dann ist der von C erzeugte Normalteiler N die von C^* erzeugte Untergruppe. Damit folgt: Liegt C im Kern eines Homomorphismus, so auch N.

3. Die unendliche Diedergruppe D_∞ hat die Präsentation $\langle\, S, T | S^2, T^2 \,\rangle$. Diese Gruppe ist also das freie Produkt $\mathbb{Z}/2 * \mathbb{Z}/2$.

4. Es gilt $\mathbb{Z}/n \cong \langle\, A | A^n \,\rangle$.

5. Die *Quaternionengruppe* Q_{4n} wird durch die Präsentation

$$\langle\, A, B | A^n = B^2, BAB^{-1} = A^{-1} \,\rangle$$

definiert. Aus den Relationen folgere man: $BA^nB^{-1} = A^{-n}$, $B^4 = 1$, $A^{2n} = 1$. Demnach erzeugt A einen zyklischen Normalteiler der Ordnung $2n$, und die Faktorgruppe hat die Ordnung 2. Also hat Q_{4n} die Ordnung $4n$. Durch die Zuordnung $A \mapsto \exp(2\pi i/2n)$, $B \mapsto j$ wird ein injektiver Homomorphismus von Q_{4n} in die Gruppe der Quaternionen der Norm 1 definiert. Die Gruppe Q_8 ist die durch die Standardeinheiten $\{\pm 1, \pm i, \pm j, \pm k\}$ in $\mathbb{H}$ gegebene Gruppe.

6. Wird ein Element von $z \in S_n$ als ein Produkt von möglichst wenig Faktoren x_j dargestellt, so nennt man die Darstellung *reduziert* und die Anzahl der Faktoren die *Länge* $l(z)$ von z. Die Länge der Permutation z ist gleich der Anzahl der *Fehlstände*

$$l(z) = \{(i,j) \mid i < j, z(i) > z(j)\}.$$

Die maximale Länge eine Elementes von S_n ist $n(n-1)/2$. Es gibt genau ein Element w_0 dieser Länge, nämlich die Permutation $i \mapsto n-i+1$. Das Element w_0 hat viele reduzierte Darstellungen. Eine davon ist

$$a_1 a_2 \cdots a_{n-1}, \qquad a_j = x_j x_{j-1} \cdots x_1.$$

Die Anzahl der reduzierten Darstellungen von $w_0 \in S_4$ ist 12. Die im Beweis von (8.9) gewonnene Normalform ist reduziert. Damit zeigt man induktiv, daß das sogenannte *Poincaré-Polynom* $P_n(t) = \sum_{x \in S_n} t^{l(x)}$ die Form

$$P_n(t) = \prod_{j=1}^{n} \frac{x^j - 1}{x - 1}$$

hat.

7. Verifikation, daß die im Text beschriebene Konstruktion ein Pushout in GRU liefert.

4 Ringe

1 Grundbegriffe

Ein *Ring* ist ein Tripel (R, a, m), das aus einer Menge R und zwei Verknüpfungen $a\colon R \times R \to R, \quad (r,s) \mapsto a(r,s) =: r+s$ und $m\colon R \times R \to R, \quad (r,s) \mapsto m(r,s) =: rs$ auf R besteht. Die Verknüpfung a heißt *Addition*, die Verknüpfung m *Multiplikation* des Ringes. Diese Daten sollen den folgenden Axiomen genügen:

(1) (R,a) ist eine abelsche Gruppe mit neutralem Element 0.
(2) (R,m) ist ein Monoid mit neutralem Element 1.
(3) Es gelten die beiden *Distributivgesetze* $a(b+c) = ab+ac$ und $(b+c)d = bd+cd$.

Wir nennen (R,a) die *additive Gruppe* und (R,m) das *multiplikative Monoid* des Ringes. Das neutrale Element der Addition (Multiplikation) heißt *Nullelement (Einselement)* des Ringes. Das Distributivgesetz besagt in anderen Worten: Die Multiplikation $m\colon R \times R \to R$ ist eine biadditive (oder bilineare) Abbildung. Ist die Multiplikation kommutativ, so heißt der Ring *kommutativ*. Meist wird der Ring (R,a,m) nur durch R bezeichnet.

Für $x \in R$ gilt $x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$, also $x \cdot 0 = 0$. Gibt es ein $x \neq 0$, so ist auch $1 \neq 0$, da andernfalls $x = x \cdot 1 = x \cdot 0 = 0$ folgen würde. Der *triviale Ring* $R = \{0\}$ soll ausgeschlossen werden; dennoch betonen wir gelegentlich die Bedingung $0 \neq 1$.

Beispiele. (1) Ein *Körper* ist ein kommutativer Ring R, in dem jedes von Null verschiedene Element ein Inverses bezüglich der Multiplikation hat (und für den $1 \neq 0$ ist). Verzichtet man auf die Bedingung der Kommutativität, so spricht man von einem *Divisionsring* oder von einem *Schiefkörper*. Die Quaternionen $\mathbb{H}$ bilden einen Schiefkörper.

(2) Der Ring $\mathbb{Z}$ der ganzen Zahlen mit der üblichen Addition und Multiplikation. Die Teilmenge der geraden Zahlen trägt auch Verknüpfungen Addition und Multiplikation; da es aber kein Einselement gibt, liegt kein Ring vor.

(3) Die (n,n)-Matrizen $M(n,n;K) = M_n(K)$ über einem Körper K bilden bezüglich Addition und Multiplikation von Matrizen einen Ring. Für $n \geq 2$ ist dieser Ring nicht kommutativ.

(4) Für jeden Ring R wird die Menge der (n,n)-Matrizen mit Einträgen aus R durch die üblichen Regeln der Addition und Multiplikation von Matrizen wie in (3) einen *Matrizenring* $M_n(R)$. ◇

Im allgemeinen hat ein Element eines Ringes R bezüglich der Multiplikation kein Inverses. Wir betrachten die Teilmenge der Elemente mit Inversem. Ein $x \in R$ heißt *Einheit* des Ringes R, wenn für geeignete $y, z \in R$ die Relationen $xy = 1 = zx$ gelten. Durch Multiplikation mit z folgt dann $z = zxy = y$. Natürlich schreiben wir meist x^{-1} für das Inverse der Einheit x. Sei R^* die Menge der Einheiten von R. Bezüglich der Multiplikation ist R^* eine Gruppe, die *Einheitengruppe* von R. Beispiele: $\mathbb{Z}^* = \{\pm 1\}$. $M(n,n;K)^* = GL(n,K)$.

Das Produkt zweier von Null verschiedener Elemente eines Ringes kann Null sein. Dieses Phänomen tritt zum Beispiel bei Matrizen auf. Wir definieren deshalb: Ein Element $a \neq 0$ eines Ringes R heißt rechter (linker) *Nullteiler*, wenn es ein $b \neq 0$ so gibt, daß $ba = 0$ ($ab = 0$) ist. Der Ring heißt *nullteilerfrei*, wenn er weder rechte noch linke Nullteiler enthält, wenn also aus $ab = 0$ folgt, daß a oder b Null ist. Ein kommutativer, nullteilerfreier Ring heißt *Intergritätsring* oder *Integritätsbereich*.

Eine Abbildung $f\colon R \to S$ zwischen Ringen R und S heißt *(Ring)-Homomorphismus*, wenn für alle $x, y \in R$ die Relationen $f(x+y) = f(x)+f(y)$, $f(xy) = f(x)f(y)$, $f(1) = 1$ gelten. Damit haben wir die Kategorie der Ringe. Die Menge $f^{-1}(0)$ heißt *Kern* des Homomorphismus f. Ein Ringhomomorphismus bildet Einheiten in Einheiten ab.

Ein Kern I ist sicherlich eine Untergruppe der additiven Gruppe des Ringes. Ferner gelten für alle $r \in R$ und $x \in I$ die Relationen $rx \in I$ und $xr \in I$. Eine Teilmenge $I \subset R$ heißt *Ideal* von R, wenn I eine additive Untergruppe ist und mit $r \in R$, $x \in I$ auch immer $rx \in I$, $xr \in I$ gilt. Verlangt man nur, daß immer $rx \in I$ für die additive Untergruppe I gilt, so heißt I *Linksideal*; analog *Rechtsideal*. Zur Betonung heißt ein Ideal auch *zweiseitig*. Für kommutative Ringe ist diese Unterscheidung unnötig; wir sprechen dann nur von Idealen eines Ringes.

Sind $a_1, \ldots, a_n$ Elemente eines Ringes, so ist die Gesamtheit aller Summen (Linearkombinationen) der Form $\sum_{i=1}^{n} r_i a_i$ mit $r_i \in R$ ein Linksideal: das von $a_1, \ldots, a_n$ *erzeugte* oder *aufgespannte Linksideal*; ist R kommutativ, so bezeichnen wir es mit $(a_1, \ldots, a_n)$. Wir nennen (a) das von $a \in R$ erzeugte *Hauptideal* des kommutativen Ringes. Analog bilden die Summen der Form $\sum_{i=1}^{n} a_i r_i$ das von $a_1, \ldots, a_n$ aufgespannte Rechtsideal. Es sind $\{0\}$, das *Nullideal*, und R selbst immer Ideale von R. Der Durchschnitt einer Familie von (linken, rechten, zweiseitigen) Idealen ist wieder ein (linkes, rechtes, zweiseitiges) Ideal. Ist S eine Teilmenge von R, so ist das von S erzeugte Linksideal der Durchschnitt aller S umfassenden Linksideale; es besteht aus allen linken Linearkombinationen von Elementen aus S. Analog für rechte und zweiseitige Ideale.

Ist R ein Ring, so heißt eine Teilmenge S von R ein *Unterring* von R, wenn S eine Untergruppe der additiven Gruppe ist, mit $a, b \in S$ auch $ab \in S$ gilt, und wenn das Einselement von R in S liegt. Die Inklusionsabbildung $S \subset R$ ist dann ein Ringhomomorphismus. Wir nennen in einer solchen Situation auch R einen *Erweiterungsring* von S. Ein Durchschnitt von Unterringen ist wieder einer. Deshalb läßt sich wie üblich der von einer Teilmenge $X \subset R$ erzeugte Unterring als der Durchschnitt aller X umfassenden Unterringe definieren.

Beispiel. Der Ring $\mathbb{Z}\times\mathbb{Z}$ bestehe aus allen Paaren ganzer Zahlen mit komponentenweiser Addition und Multiplikation. Das Einselement ist $(1, 1)$. Die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$, $n \mapsto (n, 0)$ erfüllt $f(m+n) = f(m)+f(n)$ und $f(mn) = f(m)f(n)$, ist aber kein Ringhomomorphismus, da das Bild des Einselementes nicht das Einselement ist. Das Bild S von f ist bezüglich Addition und Multiplikation selbst ein Ring mit seinem eigenen Einselement $(1, 0)$. Weil $(1, 1)$ nicht in S liegt, ist jedoch S kein Unterring von $\mathbb{Z} \times \mathbb{Z}$. $\diamond$

Ist $(R_j \mid j \in J)$ eine Familie von Ringen, so wird auf dem mengentheoretischen Produkt $\prod_{j\in J} R_j$ durch komponentenweise Addition und Multiplikation eine Ringstruktur definiert. Die Projektionen auf die Faktoren sind Ringhomomorphismen.

(1.1) Satz. *Ist R ein Ring und I ein Ideal, so gibt es auf der abelschen Gruppe R/I genau eine Multiplikation, mit der R/I ein Ring und die kanonische Abbildung $p\colon R \to R/I$ ein Ringhomomorphismus wird.*

Beweis. Die Eindeutigkeit ist klar, da p surjektiv ist. Die Multiplikation soll durch $(r_1 + I) \cdot (r_2 + I) = r_1 r_2 + I$ definiert werden. Es ist die Unabhängigkeit von den Repräsentanten zu zeigen. Sei $r_j + I = s_j + I$, also $r_i = s_j + a_j$ mit $a_j \in I$. Es folgt $r_1 r_2 = s_1 s_2 + (s_1 a_2 + a_1 s_2 + a_1 a_2)$. Da I ein Ideal ist, liegt die umklammerte Summe in I, und deshalb ist $r_1 r_2 + I = s_1 s_2 + I$. □

Der durch (1.1) gelieferte Ring R/I heißt *Faktorring* oder *Restklassenring* der *Restklassen $r + I$ modulo I*. Es ist $r + I = s + I$ genau dann, wenn $r - s \in I$ ist; in diesem Fall nennen wir r und s *kongruent modulo I*, in Zeichen $r \equiv s \bmod I$. Ist $I = (p)$ ein Hauptideal, so schreibt man stattdessen auch $\bmod p$. Satz (1.1) liefert in dieser Schreibweise die Rechenregeln: Aus $x \equiv y \bmod I$ und $a \equiv b \bmod I$ folgt $x + a \equiv y + b \bmod I$ und $xa \equiv yb \bmod I$. Insbesondere für das Zahlenrechnen ist die Kongruenzschreibweise gang und gäbe.

Die kanonische Abbildung $p\colon R \to R/I$ hat die folgende *universelle Eigenschaft* (siehe II(2.6)):

(1.2) Satz. *Sei $f\colon R \to S$ ein Ringhomomorphismus. Es gibt genau dann einen Ringhomomorphismus $F\colon R/I \to S$, der die Relation $Fp = f$ erfüllt, wenn I im Kern von f liegt. Es ist F genau dann injektiv, wenn $I = \operatorname{Kern} f$ ist.* □

Fast selbstverständlich und häufig nützlich ist der folgende *Entsprechungssatz*:

(1.3) Satz. *Sei R ein Ring, $I \neq R$ ein Ideal und $p\colon R \to R/I$ die kanonische Faktorabbildung. Dann gilt: Vermöge $\bar{J} \mapsto p^{-1}(\bar{J})$ entsprechen die (rechten, linken, zweiseitigen) Ideale von R/I umkehrbar eindeutig den (rechten, linken, zweiseitigen) Idealen J von R, die I enthalten.*

Beweis. Ist $\bar{J}$ ein Ideal, so wird die Teilmenge $p^{-1}(\bar{J})$ leicht als Ideal nachgewiesen. Sei J ein Ideal und gelte $I \subset J$. Dann haben wir die Untergruppe J/I von R/I zur Verfügung; sie wird leicht als Ideal nachgewiesen. □

Sei M eine abelsche Gruppe und $\operatorname{End}(M)$ die Menge ihrer Endomorphismen. Die folgenden beiden Verknüpfungen auf $\operatorname{End}(M)$ definieren eine Ringstruktur. Addition: $(f + g)(m) := f(m) + g(m)$; Multiplikation: Verkettung von Abbildungen. Dieser Ring heißt der *Endomorphismenring* von M.

Zu jedem Ring R gibt es den *Gegenring* R^0, der dieselbe Addition wie R hat, jedoch die umgekehrte Multiplikation $(a, b) \mapsto ba$.

2 Produkte

Sind I und J Linksideale von R, so wird mit $I + J$ das von $I \cup J$ erzeugte Linksideal bezeichnet *Summe* genannt. Es besteht aus allen Summen $x + y$ mit $x \in I$ und $y \in J$. Entsprechend für eine beliebige Familie von Linksidealen. Die Summenbildung von Linksidealen ist assoziativ und kommutativ.

Mit IJ wird das von allen Produkten xy aufgespannte Linksideal bezeichnet und *Produkt* genannt. Es besteht aus allen Summen der Form $\sum_s x_s y_s$ mit $x_s \in I$ und $y_s \in J$. Für diese Produktbildung gilt das Assoziativgesetz $I(JK) = I(JK)$.

Entsprechend haben wir Summe und Produkt von rechten und zweiseitigen Idealen.

Für Ideale wirkt der Ring R bei dieser Produktbildung als neutrales Element. Die Ideale von R bilden mit diesem Produkt ein Monoid. Für Ideale I und J gilt immer $IJ \subset I \cap J$, was direkt aus der Idealeigenschaft folgt; entsprechend für mehrfache Produkte. Ideale I und J heißen *teilerfremd*, wenn $I + J = R$ ist. Für Hauptideale in $\mathbb{Z}$ etwa entspricht dies dem bekannten Begriff.

(2.1) Notiz. *Seien I und J Ideale von R. Die Abbildung*

$$\alpha\colon R/(I+J) \to R/I \times R/J, \quad x + I \cap J \mapsto (x + I, x + J)$$

ist ein injektiver Ringhomomorphismus. Das Bild besteht genau aus den Paaren $(x + I, y + J)$ mit $x \equiv y \bmod I + J$. Insbesondere ist α genau dann surjektiv, wenn I und J teilerfremd sind.

Beweis. Nach Konstruktion ist α ein injektiver Ringhomomorphismus, dessen Bild in der angegebenen Menge von Paaren liegt. Sei $x \equiv y \bmod I + J$, also $x - y = a + b$ mit $a \in I$ und $b \in J$. Dann ist $z = x - a = y + b$ ein Element mit $x \equiv z \bmod I$ und $y \equiv z \bmod J$. Also liegt (x, y) im Bild von α. □

Der folgende Satz über die Lösbarkeit simultaner Kongruenzen ist unter dem Namen *chinesischer Restsatz* bekannt.

(2.2) Satz. *Seien $I_1, \ldots, I_n$ Ideale von R. Der Ringhomomorphismus*

$$R \to \prod_{j=1}^{n} R/I_j, \quad x \mapsto (x + I_j \mid j = 1, \ldots, n)$$

ist genau dann surjektiv, wenn für $k \neq l$ die Ideale I_k und I_l immer teilerfremd sind.

Beweis. Die Notwendigkeit der Teilerfremdheit folgt aus der vorstehenden Notiz. Für $j \neq k$ gelte $I_j + I_k = R$. Die Behauptung ist äquivalent zu der Aussage: Zu jedem n-Tupel $x_1, \ldots, x_n$ von Elementen von R gibt es ein $x \in R$, das die Kongruenzen $x \equiv x_j \bmod I_j$ für alle j erfüllt (Lösbarkeit simultaner Kongruenzen). Wir zeigen diese Aussage durch Induktion nach n. Der Fall $n = 2$ ist die vorige Notiz. Im Fall $n \geq 2$ wählen wir zunächst eine Darstellung $1 = a_j + b_j$ mit $a_j \in I_1$ und $b_j \in I_j$ für jedes $j \geq 2$. Wenn wir das Produkt $1 = (a_2 + b_2) \cdots (a_n + b_n)$

ausmultiplizieren, sind alle Summanden, die einen Faktor a_j haben, in I_1 enthalten, und der Summand $b_2 \dots b_n$ in $I_2 \cap \cdots I_n$. Da also diese Summe die 1 enthält, ist sie als Ideal gleich R. Nach dem Satz für $n = 2$ gibt es also ein Element e_1 mit $e_1 \equiv 1 \bmod I_1$ und $e_1 \equiv 0 \bmod \bigcap_{j=2}^{n} I_j$. Ebenso finden wir Elemente e_j mit $e_j \equiv 1 \bmod I_j$, die in $\bigcap_{k \neq j} I_k$ enthalten sind. Das Element $x = x_1 e_1 + \cdots + x_n e_n$ hat dann die gewünschte Eigenschaft. □

Der chinesische Restsatz führt in natürlicher Weise zu Produkten von Ringen. Wir untersuchen die Situation abstrakt. Seien $A_1, \dots, A_n$ Ringe. Auf dem cartesischen Produkt $A = A_1 \times \cdots \times A_n$ wird durch komponentenweise Addition und Multiplikation die Struktur eines Ringes definiert. Dieser Ring zusammen mit den Projektionen auf die Faktoren ist das *Produkt* der Ringe $A_1, \dots, A_n$ im Sinne der Kategorientheorie. Sei $I_j \in A$ die Menge der n-Tupel, die außerhalb der Stelle j gleich Null sind. Dann gilt offenbar:

(1) I_j ist eine Untergruppe der additiven Gruppe von A, und diese ist die interne direkte Summe der I_j.
(2) Für alle j ist $I_j I_j \subset I_j$.
(3) Für $i \neq j$ ist $I_i I_j = 0$.

Für den Begriff der internen direkten Summe siehe IV.2. Es handelt sich um die additive Form von II(3.1). Der nächste Satz untersucht eine Umkehrung dieser Situation.

(2.3) Satz. *Sei A ein Ring. Sei $(I_j \mid j \in J)$ eine Familie von nichttrivialen Untergruppen der additiven Gruppe von A. Es gelte:*

(1) *Die additive Gruppe von A ist die interne direkte Summe der I_j.*
(2) *Für alle j ist $I_j I_j \subset I_j$.*
(3) *Für $i \neq j$ ist $I_i I_j = 0$.*

Dann gilt: Die I_j sind zweiseitige Ideale von A. Mit der von A induzierten Addition und Multiplikation sind die I_j Ringe. Die Menge J ist endlich. Die Abbildung

$$\sigma \colon \prod_{j \in J} I_j \to A, \quad (x_j) \mapsto \sum x_j$$

ist ein Isomorphismus von Ringen.

Beweis. Da A die interne direkte Summe der I_j ist, hat jedes $x \in A$ die Form $x = \sum_{j \in S} x_j$, wobei $S \subset J$ endlich ist und $x_j \in I_j$ ist. Sei $u \in I_k$. Wegen (2) und (3) ist $xu = x_k u \in I_k$. Also ist I_k ein Linksideal.

Es gibt eine endliche Menge $S \subset J$ und eine Darstellung $1 = \sum_{j \in S} e_j$ mit $e_j \in I_j$. Sei $k \notin S$ und $x \in I_k$. Dann ist $x = x \cdot 1 = \sum_j x e_j = 0$ nach (3). Also ist $S = J$.

Die Abbildung σ ist ein additiver Isomorphismus, weil A die interne direkte Summe der I_j ist. Wegen (3) ist σ mit der Multiplikation verträglich. Aus der Gleichung $x_k = x_k \cdot 1 = \sum_j x_k e_j = x_j e_j$ folgt, daß $e_j \in I_j$ ein Einselement von I_j ist. Wegen $1 = \sum_j e_j$ ist σ mit Einselementen verträglich und damit insgesamt ein Isomorphismus von Ringen. □

Wir sagen unter der Voraussetzung von (2.3): Die I_j bilden eine *interne Produktzerlegung* von A. Eine interne Produktzerlegung wird vollständig durch die zugehörige Zerlegung des Einselementes bestimmt.

(2.4) Satz. *Sei A ein Ring. Seien $e_1, \dots, e_n$ Ringelemente mit den folgenden Eigenschaften:*

(1) $1 = e_1 + \cdots + e_n$.
(2) $e_j^2 = e_j \neq 0$.
(3) $e_j e_k = 0$, *falls* $j \neq k$.
(4) *Für alle $x \in A$ gilt $xe_j = e_j x$.*

Dann bilden die Mengen $I_j = Ae_j$ eine interne Produktzerlegung von A.

Beweis. Nach Konstruktion ist I_j eine additive Untergruppe. Wegen der Voraussetzungen (2) und (3) gelten die Bedingungen (2) und (3) des letzten Satzes. Wegen (1) ist die Abbildung σ aus dem letzten Satz surjektiv. Aus (3) folgt $I_j \cap \sum_{k \neq j} I_k = 0$. Deshalb ist die Summe direkt. □

Ein System $e_1, \dots, e_n$ mit den Eigenschaften (1) – (4) des letzten Satzes nennen wir eine *zentrale Einszerlegung* des Ringes A.

Wir verallgemeinern die vorstehenden Betrachtungen auf andere Zerlegungen. Sei A ein Ring. Eine Familie $(I_1, \dots, I_n)$ von (nichtrivialen) Linksidealen von A heißt *Linksidealzerlegung* von A, wenn A als additive Gruppe (= als A-Linksmodul) die direkte Summe $A = I_1 \oplus \cdots \oplus I_n$ ist. Ebenso werden *Rechtsidealzerlegungen* und *Idealzerlegungen* definiert. Eine (n, n)-*Matrixzerlegung* von A ist eine Familie $(A_{ij} \mid 1 \leq i, j \leq n)$ von additiven Untergruppen von A, so daß $A = \bigoplus_{i,j} A_{ij}$ ist und ferner gilt: $A_{ij}A_{kl} = 0$ für $j \neq k$ und $A_{ij}A_{jk} \subset A_{ik}$. In einer Matrixzerlegung dürfen einige der Gruppen A_{ij} Null sein.

Wir werden zeigen, daß Zerlegungen der genannten Art Zerlegungen des Einselementes entsprechen. Dazu definieren wir:

Ein Element $e \in A$ heißt *idempotent*, wenn $e^2 = e$ ist. Ein Idempotent heißt *zentral*, wenn es im Zentrum von A liegt. Idempotente e, f heißen *orthogonal*, wenn $ef = fe = 0$ ist. Eine (zentrale) *Zerlegung der Eins* oder *Einszerlegung* des Ringes A ist eine Familie $(e_1, \dots, e_n)$ von paarweise orthogonalen, von Null verschiedenen (zentralen) Idempotenten e_i mit der Summe $1 = e_1 + \cdots + e_n$. Ein Idempotent heißt *primitiv*, wenn es nicht die Summe zweier orthogonaler Idempotenter ist.

(2.5) Satz. *Die Zuordnung $(e_1, \dots, e_n) \mapsto (Ae_1, \dots, Ae_n)$ ist eine Bijektion zwischen Einszerlegungen und Linksidealzerlegungen von A. Die Zuordnung $(e_1, \dots, e_n) \mapsto (e_1A, \dots, e_nA)$ ist eine Bijektion zwischen Einszerlegungen und Rechtsidealzerlegungen von A. Die zu $(e_1, \dots, e_n)$ gehörenden Zerlegungen stimmen genau dann überein, wenn die Zerlegung zentral ist. Die Zuordnung $(e_1, \dots, e_n) \mapsto (Ae_1, \dots, Ae_n)$ ist eine Bijektion zwischen zentralen Einszerlegungen und Idealzerlegungen von A.*

BEWEIS. Sei $A = L_1 \oplus \cdots \oplus L_n$ eine Linksidealzerlegung und $1 = e_1 + \cdots + e_n$ mit $e_j \in L_j$. Aus

$$e_j = e_j \cdot 1 = e_j e_1 + \cdots + e_j e_n \in L_j, \qquad e_j e_i \in L_i$$

folgt $e_j e_i = 0$ für $j \neq i$ und $e_j^2 = e_j$. Aus $e_j = 0$ würde wegen $x = x \cdot 1 = \sum_{i \neq j} x e_i$ folgen, daß x in der Summe der $L_i, i \neq j$, enthalten wäre, was nicht für alle x gelten kann, da $L_j \neq 0$ vorausgesetzt war. Also ist $(e_1, \ldots, e_n)$ eine Einszerlegung.

Sei umgekehrt $(e_1, \ldots, e_n)$ eine Einszerlegung. Dann ist Ae_j ein Linksideal. Wegen $x = \sum_j x e_j$ ist $\sum_j Ae_j = A$. Sei $x \in Ae_j \cap (\sum_{i \neq j} Ae_i)$. Da x in der Summe liegt, ist $xe_j = 0$. Da x in Ae_j liegt, ist $xe_j = x$. Also ist $x = 0$. Das zeigt $A = \bigoplus_j Ae_j$. Die beiden Prozesse sind zueinander invers. Analog für Rechtsidealzerlegungen.

Sei nun $Ae_j = e_j A$ für alle j. Dann folgt zunächst $e_i a_j = 0$ für $i \neq j$ und alle $a \in A$. Aus $a = \sum_j a e_j = \sum_j e_j a$ folgt dann $e_j a = e_j a e_j = a e_j$. Also liegt e_j im Zentrum von A. Liegt es im Zentrum, so gilt natürlich $Ae_j = e_j A$.

Ist $(e_1, \ldots, e_n)$ eine zentrale Einszerlegung, so sind die $Ae_j = e_j A$ zweiseitige Ideale. Seien die Ae_j zweiseitige Ideale. Dann bilden die Ae_j eine Rechtsidealzerlegung mit $(e_1, \ldots, e_n)$ als zugehöriger Einszerlegung, so daß $Ae_j = e_j A$ ist und somit die e_j zentral sind. □

(2.6) Satz. *Die Zuordnung $(e_1, \ldots, e_n) \mapsto (e_i A e_j \mid 1 \leq i, j \leq n)$ ist eine Bijektion zwischen Einszerlegungen der Länge n und (n,n)-Matrixzerlegungen von A. Eine Matrixzerlegung (A_{ij}) stammt dabei genau dann von einer zentralen Einszerlegung, wenn für $i \neq j$ immer $A_{ij} = 0$ ist.*

BEWEIS. Sei (A_{ij}) eine (n,n)-Matrixzerlegung. Wir setzen $1 = \sum_{i,j} e_{ij}$ mit $e_{ij} \in A_{ij}$. Wir zeigen:

(1) $e_{ij} = 0$ für $i \neq j$.
(2) $(e_{11}, \ldots, e_{nn})$ ist eine Einszerlegung.
(3) $e_{ii} A e_{jj} = A_{ij}$.

Aus $A_{ij} A_{kl} = 0$ für $j \neq k$ folgt $e_{ij} e_{kl} = 0$ für $j \neq k$. Damit ergibt sich

$$e_{kl} = 1 \cdot e_{kl} = \sum_{\alpha\beta} e_{\alpha\beta} e_{kl} = \sum_{\alpha} e_{\alpha k} e_{kl}$$

und durch Vergleich der Seiten $e_{\alpha k} e_{kl} = 0$ für $\alpha \neq k$ und $e_{kk} e_{kl} = e_{kl}$. Diese Relationen zeigen $(\sum_k e_{kk}) e_{\alpha\beta} = e_{\alpha\beta}$ für alle α, β. Ebenso sieht man, daß $e_{\alpha\beta}(\sum_k e_{kk}) = e_{\alpha\beta}$ ist. Folglich ist $\sum_k e_{kk}$ das Einselement des Ringes A und deshalb $e_{jk} = 0$ für $j \neq k$. Mittels $e_{kk} e_{ll} = 0$ für $k \neq l$ folgt

$$\sum_k e_{kk} = 1 = 1 \cdot 1 = (\sum_k e_{kk})(\sum_l e_{ll}) = \sum_k e_{kk}^2$$

und deshalb $e_{kk}^2 = e_{kk}$. Damit liegt liegt die behauptete Einszerlegung vor. Die Inklusion $e_{ii} A e_{jj} \subset A_{ij}$ folgt aus der Definition einer Matrixzerlegung. Sei $x \in A_{ij}$. Wegen $x = 1 \cdot x \cdot 1$ folgt $x = e_{ii} x e_{jj} \in e_{ii} A e_{jj}$.

Sei umgekehrt $(e_1, \ldots, e_n)$ eine Einszerlegung. Sei $A_{ij} = e_i A e_j$. Dann gilt sicherlich $A_{ij}A_{jk} \subset A_{ik}$ und $A_{ij}A_{kl} = 0$ für $j \neq k$. Ferner ist wegen $a = \sum_{i,j} e_i a e_j$ der Ring A die Summe der A_{ij}. Sei $x \in A_{ij}(\sum_{(i,j)} \neq (k,l)A_{kl})$. Dann folgt $e_i x e_j = x = 0$. Also ist die Summe direkt.

Ist die Zerlegung zentral, so folgt $e_i A e_j = e_i e_j A = 0$ für $i \neq j$. Ist umgekehrt $A_{ij} = 0$ für $i \neq j$, so hat jedes x die Gestalt $x = \sum_j e_j x e_j$, woraus sich sofort ergibt, daß die e_j zentral sind. □

Ist (A_{ij}) eine Matrixzerlegung von A, so können wir einem $x = \sum_{ij} x_{ij}$, $x_{ij} \in A_{ij}$ die Matrix (x_{ij}) zuordnen. Addition und Multiplikation von Elementen gehorchen dann den üblichen Regeln der Matrizenrechnung.

3 Kommutative Ringe

In diesem Abschnitt seien alle Ringe kommutativ. Wichtige kommutative Ringe sind die Körper. Wir notieren deshalb:

(3.1) Notiz. *Ein Ring R mit $0 \neq 1$ ist genau dann ein Körper, wenn er nur die Ideale $\{0\}$ und R hat.*

Beweis. Sei R ein Körper und $I \neq \{0\}$ ein Ideal. Dann enthält I ein Element $\lambda \neq 0$, also auch jedes Element $\mu = (\mu\lambda^{-1})\lambda$. Also ist $I = R$.

Sei umgekehrt R mit den genannten Eigenschaften gegeben. Wir müssen nur zeigen, daß jedes $x \in R \setminus \{0\}$ ein multiplikatives Inverses hat. Das Hauptideal (x) ist nach Voraussetzung gleich R, enthält also das Element 1 in der Form $1 = yx$. □

Eine unmittelbare Folge dieser Notiz: Ein Homomorphismus $f\colon K \to L$ zwischen Körpern ist injektiv. In einem solchen Fall identifizieren wir oft K mit seinem Bild $f(K)$ und betrachten L als Erweiterungskörper von K.

Ein Ideal I in R heißt *maximal*, wenn es von R verschieden ist und nicht in einem größeren Ideal $J \neq R$ enthalten. Nach (1.3) und (3.1) können wir deshalb sagen:

(3.2) Satz. *R/I ist genau dann ein Körper, wenn I maximal ist.* □

Ein nullteilerfreier Ring, in dem $0 \neq 1$ ist, heißt *Integritätsring*. Der Quotient R/I nach einem maximalen Ideal ist insbesondere nullteilerfrei. Ein Ideal $I \neq R$ heißt *Primideal* von R, wenn R/I nullteilerfrei ist. Mit anderen Worten: Das Ideal $I \neq R$ ist genau dann ein Primideal, wenn aus $ab \in I$ entweder $a \in I$ oder $b \in I$ folgt. Ein Ursprung für diese Wortwahl: In vielen zahlentheoretisch interessanten Ringen ist die Eindeutigkeit der Primfaktorzerlegung verletzt; man erfindet weitere „ideale“ Elemente, nämlich gewisse Primideale, die die Eindeutigkeit wiederherstellen.

Wir zeigen, daß ein kommutativer Ring R immer maximale Ideale besitzt. Genauer gilt:

(3.3) Satz. *Sei $I \neq R$ ein Ideal. Es gibt ein maximales Ideal von R, das I umfaßt.*

Der Beweis benutzt das *Zornsche Lemma* der Mengenlehre (siehe (3.7)). Sei X die Menge der Ideale J von R mit $I \subset J \neq R$. Durch $J_1 \leq J_2 :\Leftrightarrow J_1 \subset J_2$ wird auf X eine Halbordnung erklärt. Wegen $I \in X$ ist $X \neq \emptyset$. Es ist X induktiv geordnet: Sei K Kette von X. Sei L die Vereinigung der Ideale aus K. Wir zeigen: $L \in X$. Es ist $I \subset L$ klar. Es ist L ein Ideal, denn ist $b, c \in L$, so gibt es $J_1, J_2 \in K$ mit $b \in J_1$, $c \in J_2$ und etwa $J_1 \subset J_2$ (da K Kette ist); also ist $b - c \in J_2 \subset L$; ebenso folgt für $b \in L$ und $r \in R$, daß $rb \in L$ ist. Es ist $L \neq R$, denn aus $L = R$ würde $1 \in L$ folgen. Also gäbe es ein $J \in K$ mit $1 \in J$, also $J = R$; Widerspruch.

Ein nach dem Zornschen Lemma existierendes maximales Element in X ist ein maximales Ideal von R und umfaßt I. □

(3.4) Bemerkung. Mit demselben Beweis findet man in einem beliebigen Ring maximale linke, rechte und zweiseitige Ideale. ◇

Hier noch eine Ergänzung zum chinesischen Restsatz.

(3.5) Satz. *Seien $I_1, \ldots, I_n$ paarweise teilerfremde Ideale. Dann gilt $I_1 \cap \ldots \cap I_n = I_1 I_2 \ldots I_n$.*

Beweis. Das Produkt von Idealen ist immer in ihrem Schnitt enthalten. Ein Element x im Schnitt stellen wir in der Form $x = xe_1 + \cdots + xe_n$ dar. Dann verwenden wir, daß e_j im Produkt der I_k für $k \neq j$ enthalten ist, wie im Beweis von (2.2) gezeigt wurde. □

Sei R ein Unterring von S und X eine Teilmenge von S. Der von R und X erzeugte Unterring $R[X]$ von S heißt der durch *Adjunktion* von X an R entstehende Ring. Ist $X = \{x_1, \ldots, x_n\}$, so wird dieser Ring mit $R[x_1, \ldots, x_n]$ bezeichnet.

(3.6) Beispiel. Hier ein Beispiel, um die Wirkungsmacht der Algebra zu demonstrieren: Sei F der Ring aller Cauchy-Folgen (x_j) rationaler Zahlen mit komponentenweiser Addition und Multiplikation und C die Teilmenge aller Nullfolgen. Dann ist C ein Ideal in F und F/C isomorph zum Körper der reellen Zahlen. ◇

Ein *kommutativer Halbring* besteht aus einem abelschen Monoid H zusammen mit einer assoziativen und kommutativen Multiplikation $H \times H \to H$, $(a, b) \mapsto ab$, die biadditiv ist und ein neutrales Element 1 hat.

Sei $i\colon H \to K(H)$ die universelle Gruppe für das additive Monoid eines Halbringes. Nach (1.4) läßt sich die Multiplikation von H zu einer biadditiven Multiplikation $K(H) \times K(H) \to K(H)$ erweitern. Man bestätigt, daß diese Multiplikation wieder assoziativ und kommutativ ist und $i(1)$ als neutrales Element hat. Damit ist $K(H)$ ein kommutativer Ring und i ein Homomorphismus von Halbringen. Er hat die folgende universelle Eigenschaft: Zu jedem Homomorphismus $\varphi\colon H \to R$ von Halbringen in einen kommutativen Ring R (mit $\varphi(0) = 0$ und $\varphi(1) = 1$) gibt es genau einen Ringhomomorphismus $\Phi\colon K(H) \to R$ mit $\Phi i = \varphi$.

Wir nennen $K(H)$ den *Grothendieck-Ring* von H. Wie bei Monoiden wird K zu einem Funktor von Halbringen zu Ringen gemacht.

Die rationalen Zahlen entstehen aus den ganzen Zahlen durch die Bruchrechnung. Ein Bruch p/q wird dabei durch das Paar (p, q) bestimmt. Das Kürzen von Brüchen entspricht einer Äquivalenzrelation auf der Menge dieser Paare. Dieser Prozess soll auf beliebige kommutative Ringe verallgemeinert werden.

Ein multiplikatives Untermonoid $S \subset R$ eines Ringes R sei gegeben, d. h. S enthalte die 1 und mit je zwei Elementen das Produkt. Auf der Menge $R \times S$ wird durch

$$(a, s) \sim (b, t) \iff \text{es gibt } u \in S \text{ mit } atu = bsu \tag{3.7}$$

eine Äquivalenzrelation gegeben. In Abweichung von der gewöhnlichen Bruchrechnung braucht man die Multiplikation mit geeigneten u, um sicherzustellen, daß eine Äquivalenzrelation vorliegt. Die Klasse von (a, s) werde mit a/s oder $\frac{a}{s}$ bezeichnet. Die Menge der Klassen sei $S^{-1}R$ (das ist $K_S(R)$ im Sinne des ersten Abschnittes, wei R hier für das multiplikative Monoid steht). Auf dieser Menge definieren wir eine *Bruchrechnung* durch die Addition *Hauptnennerregel*

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} \tag{3.8}$$

und die Multiplikation

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}. \tag{3.9}$$

Es ist nachzurechnen, daß Addition und Multiplikation wohldefiniert sind. Ferner ist leicht nachzurechnen:

(3.10) Satz. *Mit den Verknüpfungen* (3.9) *und* (3.10) *ist $S^{-1}R$ ein kommutativer Ring und $b_S\colon R \to S^{-1}R$, $a \mapsto a/1$ ein Ringhomomorphismus.* □

(3.11) Satz. *Der Kern von b_S ist das Ideal $\{x \in R \mid$ es gibt $s \in S$ mit $sx = 0\}$.*

Beweis. Sei $sx = 0$. Dann gilt $(x, 0) \sim (0, s) \sim (0, 1)$. Also ist $b_S(x) = b_S(0)$. Sei $b_S(x) = 0$, also $(x, 1) \sim (0, 1)$. Dann gibt es $u \in S$ mit $x \cdot 1 \cdot u = 0 \cdot 1 \cdot u = 0$.□

(3.12) Folgerung. *Ist R nullteilerfrei, so ist b_S injektiv.* □

Die Elemente von S werden bei b_S auf Einheiten von $S^{-1}R$ abgebildet. Es gilt nämlich $s/1 \cdot 1/s = s/s$ und $(s, s) \sim (1, 1)$.

Die vorstehende Konstruktion hat die folgende universelle Eigenschaft:

(3.13) Satz. *Sei $f\colon R \to L$ ein Ringhomomorphismus, der die Elemente von S auf Einheiten von L abbildet. Dann gibt es genau einen Ringhomomorphismus $F\colon S^{-1}R \to L$ mit $F \circ b_S = f$.*

Beweis. Die Abbildung $R \times S \to L$, $(a, s) \mapsto f(a)f(s)^{-1}$ faktorisiert über $S^{-1}R$ und liefert ein F, das als Ringhomomorphismus verifiziert wird und die behauptete Eigenschaft hat. Da $(s/1)^{-1} = (1/s)$ ist und $a/s = (a/1) \cdot (s/1)^{-1}$, gilt notwendig $F(a/s) = f(a)f(s)^{-1}$, falls F wie behauptet existiert. □

(3.14) Satz. *Sei R ein Integritätsring und $S = R \setminus 0$. Dann ist $S^{-1}R$ ein Körper.*

BEWEIS. Sei $a/s \neq 0$. Dann ist $a \neq 0$ und deshalb s/a definiert und ein multiplikatives Inverses von a/s. □

Der durch (3.15) hergestellte Körper heißt der *Quotientenkörper* von R. Wegen (3.13) können wir R als Unterring seines Quotientenkörpers auffassen. Ist K ein Körper und $R = K[x]$ der Polynomring, so heißt der Quotientenkörper $K(x)$ von $K[x]$ der *Funktionenkörper* in einer Unbestimmten über K. Entsprechend erhalten wir für $K[x_1, \ldots, x_n]$ den Quotientenkörper $K(x_1, \ldots, x_n)$ in n Unbestimmten. (Siehe den Abschnitt über Polynomringe.)

Der Übergang $R \mapsto S^{-1}R$ wird wegen gewisser Anwendungen in der algebraischen Geometrie *Lokalisierung* genannt. Sei $\mathfrak{p} \subset R$ ein Primideal; das ist nach Definition genau dann der Fall, wenn $\mathfrak{p}$ ein Ideal und $R \setminus \mathfrak{p} = S$ ein Untermonoid ist. In diesem Fall wird $S^{-1}R$ mit $R_{\mathfrak{p}}$ bezeichnet und *Lokalisierung bei* $\mathfrak{p}$ genannt. Zum Beispiel besteht $\mathbb{Z}_{(p)}$ aus allen Brüchen der Form a/s, worin s teilerfremd zu p ist. Übrigens ist $\mathbb{Z}_{(0)} = \mathbb{Q}$.

4 Teilbarkeit

In diesem Abschnitt sei R ein Integritätsring. Ein kommutativer Ring ist genau dann ein Integritätsring, wenn das Nullideal ein Primideal ist. Die Teilbarkeitslehre läßt sich fast wörtlich aus den Abschnitten II.1 und II.2 übernehmen.

Für Elemente $a, b \in R$ sagen wir: *a teilt b* oder a ist ein *Teiler* von b oder b ist *Vielfaches* von a (in Zeichen $a|b$), wenn für ein $c \in R$ die Relation $b = ac$ besteht. Es gelten dann die Regeln II(1.1) über die Teilbarkeit, sowie die Notiz II(1.2). Die Menge $(a) := \{ac \mid c \in R\}$ aller Elemente, die a als Teiler haben, ist das von a erzeugte *Hauptideal*.

Ringelemente a und b heißen *assoziiert*, wenn $(a) = (b)$ ist. Assoziierte Elemente haben dieselben Teilbarkeitseigenschaften.

Wir wollen die bekannte Primzahlzerlegung der ganzen Zahlen verallgemeinern. Dazu definieren wir: Ein Element $p \in R$ heißt *unzerlegbar*, wenn $p \neq 0$ ist, p keine Einheit ist und aus $p = ab$ folgt, daß a oder b eine Einheit ist. Mit anderen Worten: Ein unzerlegbares Element hat keine Produktzerlegung in Nichteinheiten. Statt unzerlegbar sagt man (insbesondere bei Polynomringen) auch *irreduzibel*. Die Teilbarkeitslehre der ganzen Zahlen liefert in der neuen Terminologie:

(4.1) Satz. *Folgende Aussagen über $1 < p \in \mathbb{Z}$ sind äquivalent:*

(1) *p ist Primzahl.*
(2) *(p) ist ein Primideal.*
(3) *(p) ist ein maximales Ideal.*

BEWEIS. Wir wissen schon, daß ein maximales Ideal prim ist. Ist $p = ab$ eine Zerlegung in Nichteinheiten, so sind a und b nicht in (p) enthalten, wohl aber ihr

Produkt, so daß (p) nicht prim ist. Ist p Primzahl und $(p) \subset (d) \neq R$, so ist d ein Teiler von p aber keine Einheit, also zu p assoziert, d. h. $(p) = (d)$, und (p) ist maximal. □

Ist R ein beliebiger kommutativer Ring, so gibt es genau einen Ringhomomorphismus $c\colon \mathbb{Z} \to R$ mit $c(1) = 1$. Sein Kern wird von einer ganzen Zahl $d \geq 0$ erzeugt. Wir nennen d die *Charakteristik* von R. Ist R ein Integritätsring, zum Beispiel ein Körper, so ist nach dem letzten Satz die Charakteristik eine Primzahl oder Null. Nach dem letzten Satz haben wir für jede Primzahl p den Körper $\mathbb{Z}/p = \mathbb{F}_p$ mit p Elementen zur Verfügung. Ein Körper der Charakteristik $p > 0$ enthält als minimalen Körper einen zu $\mathbb{F}_p$ isomorphen. Ein Körper der Charakteristik Null enthält als minimalen Körper einen zu $\mathbb{Q}$ isomorphen. Diese minimalen Körper heißen *Primkörper*. Ist $n > 1$ keine Primzahl, so hat $\mathbb{Z}/n$ Nullteiler und ist somit kein Körper.

Ein Integritätsring heißt *Hauptidealring*, wenn jedes seiner Ideale ein Hauptideal ist. Für den Rest dieses Abschnittes sei R ein Hauptidealring. Unser Ziel ist der Beweis des Satzes über die Existenz und Eindeutigkeit der Primfaktorzerlegung in Hauptidealringen.

Es heiße $p \in R$ *Primelement*, wenn gilt: $p \neq 0$, $p \notin R^*$ und: aus $p|ab$ folgt $p|a$ oder $p|b$. Mit anderen Worten: p ist Primelement, wenn (p) ein von Null verschiedenes Primideal ist. Der Beweis der folgenden Notiz und des anschließenden Satzes wird wörtlich genauso geführt wie für I(2.2).

(4.2) Notiz. *Ein Element ist genau dann Primelement, wenn es unzerlegbar ist.* □

(4.3) Satz. *Sei $a \in R$ von Null verschieden und keine Einheit. Dann ist a Produkt von unzerlegbaren Elementen. Sind $a = p_1 \dots p_r = q_1 \dots q_s$ Produktdarstellungen mit unzerlegbaren p_i und p_j, so ist $r = s$, und mit einer geeigneten Permutation π von $\{1, \dots, r\}$ gilt $(p_i) = (q_{\pi(i)})$.* □

Die Begriffe GGT und KGV werden genauso wie in II.1 definiert. Die Sätze II(1.4) und II(1.5) übertragen sich einschließlich ihres Beweises wortwörtlich. Die Teilbarkeitseigenschaften lassen sich wie im ersten Kapitel durch die Primpotenzzerlegung beschreiben; eine Wiederholung ist unnötig.

(4.4) Aufgaben und Ergänzungen.

1. Sei R ein Intergritätsring. Folgende Aussagen sind äquivalent:

(1) Jedes Element $a \neq 0$ aus R, das keine Einheit ist, ist Produkt unzerlegbarer Elemente.

(2) Der Ring enthält keine unendliche echt aufsteigende Hauptidealkette $(a_1) \subset (a_2) \subset \dots$.

2. Ein Integritätsring R heißt *faktoriell*, wenn jedes Element ein Produkt unzerlegbarer Elemente ist und eine Produktzerlegung bis auf die Reihenfolge und Assoziiertheit eindeutig ist. Ein Integritätsring, in dem es Faktorzerlegungen gibt, ist genau dann faktoriell, wenn jedes unzerlegbare Element ein Primelement ist.

3. In einem faktoriellen Ring gibt es zu je zwei von Null verschiedenen Elementen einen größten gemeinsamen Teiler. Er ist bis auf Assoziiertheit eindeutig. Ebenso für endlich viele Elemente. (Er ist aber, im Gegensatz zu Hauptidealringen, nicht immer als Linearkombination der Elemente darstellbar.) In einem faktoriellen Ring lassen sich die Teilbarkeiten ebenfalls durch Primpotenzzerlegungen beschreiben.

5 Die Restklassenringe der ganzen Zahlen

Algebraische Ergebnisse über die Ringe $\mathbb{Z}/(m)$ haben zahlentheoretische Interpretationen.

Die Restklassenabbildung $\mathbb{Z} \to \mathbb{Z}/(m)$ wird *Reduktion* modulo m genannt. Der Ring $\mathbb{Z}/(m)$ hat nur endlich viele Elemente, er ist viel einfacher als $\mathbb{Z}$. Ein zahlentheoretisches Problem wird durch Reduktion oft vereinfacht oder verdeutlicht. Zum Beispiel sind 0 und 1 die einzigen Restklassen modulo 4, die Quadrate sind. Also kommen für $x^2 + y^2$ nur die Restklassen $0, 1, 2 \bmod 4$ in Frage. Eine natürliche Zahl $y \equiv 3 \bmod 4$ ist somit niemals die Summe zweier ganzzahliger Quadrate. Ist n ein Teiler von m, so haben wir ebenfalls die Reduktion $\mathbb{Z}/(m) \to \mathbb{Z}/(n)$, die auf Repräsentanten die Identität ist.

Ist $m = m_1 \dots m_r$ eine Zerlegung in paarweise teilerfremde Faktoren m_k, so ist die Abbildung

$$\mathbb{Z}/(m) \to \prod_{k=1}^{r} \mathbb{Z}/(m_k), \tag{5.1}$$

deren Komponenten die Reduktionen sind, nach (2.5) ein Isomorphismus von Ringen. Es genügt deshalb, die Ringe der Form $\mathbb{Z}/(p^t)$ für eine Primzahl p genauer zu untersuchen.

(5.2) Notiz. *Eine Zahl $a \in \mathbb{Z}$ repräsentiert genau dann eine Einheit von $\mathbb{Z}/(m)$, wenn a zu m teilerfremd ist.*

Beweis. Genau dann ist a Einheit, wenn es b mit $ab \equiv 1 \bmod m$ gibt. Letzteres besagt aber: Es gibt eine Darstellung der Form $ab + km = 1$, und das ist zu $(a, m) = 1$ gleichwertig. □

Wegen dieser Notiz nennt man die Einheitengruppe $(\mathbb{Z}/m)^*$ auch die *prime Restklassengruppe* modulo m. Da die Einheiten mit Produktbildung verträglich sind, liefert die Reduktion (5.1) einen Isomorphismus

$$(\mathbb{Z}/m)^* \cong \prod_{k=1}^{r} (\mathbb{Z}/m_k)^*. \tag{5.3}$$

Die Ordnung von $(\mathbb{Z}/m)^*$ wird oft mit $\varphi(m)$ bezeichnet und *Eulersche Funktion* genannt. Nach (5.3) gilt $\varphi(m) = \prod_k \varphi(m_k)$. Offenbar ist $\varphi(p^t) = p^t - p^{t-1}$. Damit haben wir φ ausgerechnet.

Wir haben schon bemerkt, daß $\mathbb{Z}/p$ ein Körper ist. Er wird auch mit $\mathbb{F}_p$ bezeichnet. Seine multiplikative Gruppe wird durch den nächsten Satz bestimmt.

(5.4) Satz. *Sei K ein Körper und G eine endliche Untergruppe der multiplikativen Gruppe K^*. Dann ist G zyklisch.*

Beweis. Nach der Strukturtheorie abelscher Gruppen ist G isomorph zu einem Produkt $G_1 \times \cdots \times G_r$ zyklischer Gruppen G_j, wobei die Ordnung von G_{j-1} die von G_j teilt. Dann genügt aber jedes Element von x der Gleichung $x^n = 1$ mit $n = |G_r|$. Da ein Polynom n-ten Grades höchstens n Nullstellen hat (siehe den Abschnitt über Polynomringe), folgt $G = G_r$. □

Eine Zahl $n \in \mathbb{N}$, die ein erzeugendes Element der primen Restklassengruppe $\bmod p$ liefert, heißt in der Zahlentheorie manchmal *Primitivwurzel* $\bmod p$. Es ist ein Mysterium, welche Zahlen diese Eigenschaft haben. Hier einige Beispiele für Primitivwurzeln $w \bmod p$.

p	3	5	7	11	13	17	19	23
w	2	2	3	2	2	3	3	5

Allein aus der Tatsache, daß $\mathbb{F}_p^*$ die Ordnung $p-1$ hat, folgt für jede zu p teilerfremde Zahl a nach III(2.3) die Kongruenz

$$a^{p-1} \equiv 1 \bmod p \tag{5.5}$$

(*kleiner Fermatscher Satz*) und folglich für jede ganze Zahl a die Kongruenz $a^p \equiv a \bmod p$. Die folgende Aussage besagt, daß für einen Ring der Primzahlcharakteristik p die Zuordnung $x \mapsto x^p$ ein Ringendomorphismus ist.

(5.6) Notiz. *Für Elemente x, y eines kommutativen Ringes gilt*

$$(x+y)^p \equiv x^p + y^p \bmod(p).$$

Beweis. Die Binomialkoeffizienten $\binom{p}{i}$ sind für $1 \le i \le p-1$ durch p teilbar. Deshalb liefert die binomische Formel die Kongruenz. □

(5.7) Notiz. *Aus $a \equiv b \bmod(p^t)$ folgt $a^p \equiv b^p \bmod(p^{t+1})$.*

Beweis. Wegen der vorausgesetzten Kongruenz gibt es eine Relation $a = b + kp^t$. Wir potenzieren und wenden die binomische Formel an. Es ergibt sich $a^p = b^p + \binom{p}{1} a^{p-1}(kp) + \ldots$; darin sind rechts alle Summanden außer b^p durch p^{t+1} teilbar. □

(5.8) Notiz. *Sei $t \ge 2$ und $p \ne 2$ eine Primzahl. Dann gilt für alle $a \in \mathbb{Z}$*

$$(1+ap)^{p^{t-2}} \equiv 1 + ap^{t-1} \bmod p^t.$$

BEWEIS. Induktion nach t. Der Anfang $t = 2$ ist klar. Aus der Kongruenz für t folgt nach (5.7)

$$(1 + ap)^{p^{t-1}} \equiv (1 + ap^{t-1})^p \bmod p^{t+1}.$$

Wir entwickeln die rechte Seite nach der binomischen Formel

$$1 + \binom{p}{1} ap^{t-1} + \sum_{j=2}^{p} \binom{p}{j} a^j p^{j(t-1)}.$$

Die Summanden für $2 \leq j \leq p-1$ sind durch $p^{1+2(t-1)}$ teilbar und der letzte Summand durch $p^{p(t-1)}$. Wegen $t \geq 2$ und $p \geq 3$ ist $1 + 2(t-1) \geq t+1$ und $p(t-1) \geq t+1$. Damit ergibt sich das Gewünschte. □

(5.9) Notiz. *Sei $p \neq 2$ eine Primzahl und $a \not\equiv 0 \bmod p$. Dann hat $1 + ap \in (\mathbb{Z}/p^t)^*$ die Ordnung p^{t-1}.*

BEWEIS. Es gilt $(1 + ap)^{p^{t-1}} \equiv 1 \bmod p^t$ (Induktion nach t mittels (5.8)). Also hat $1 + ap$ eine Ordnung, die p^{t-1} teilt. Die vorige Notiz zeigt, daß $1 + ap$ nicht die Ordnung p^{t-2} hat. □

(5.10) Satz. *Sei $p \neq 2$ eine Primzahl. Dann ist $(\mathbb{Z}/p^t)^*$ zyklisch. Genau dann repräsentiert $a \in \mathbb{Z}$ ein erzeugendes Element, wenn a ein erzeugendes Element von $(\mathbb{Z}/p)^*$ repräsentiert und wenn ferner $a^{p-1} \not\equiv 1 \bmod p^2$ ist.*

BEWEIS. Die Reduktion $r\colon (\mathbb{Z}/p^t)^* \to (\mathbb{Z}/p)^*$ ist nach (5.2) surjektiv. Wegen (5.8) wird durch $a \mapsto a^{p^{t-1}}$ ein wohldefinierter Homomorphismus $j\colon (\mathbb{Z}/p)^* \to (\mathbb{Z}/p^t)^*$ geliefert, für den überdies $jr = \mathrm{id}$ gilt. Repräsentiert g ein erzeugendes Element von $(\mathbb{Z}/p)^*$, so ist $j(g) = h$ ein Element der Ordnung $p-1$. Nach (5.10) hat $1+p$ in $(\mathbb{Z}/p^t)^*$ die Ordnung p^{t-1}. Das Produkt $h(1+p)$ hat dann die Ordnung $(p-1)p^{t-1}$, erzeugt also die Einheitengruppe.

Sei $a \bmod p^2$ erzeugendes Element. Dann ist $a^{p-1} \equiv 1 + bp \bmod p^2$ mit $b \not\equiv 0 \bmod p$, da a die Ordnung $p(p-1)$ hat. Mittels (5.9) folgt $a^{(p-1)p^{t-2}} \equiv 1 + bp^{t-1} \not\equiv 1 \bmod p^t$. Reduktion modulo p zeigt, daß $p-1$ die Ordnung von $a \bmod p^t$ teilt. Aus beiden Aussagen über die Ordnung folgt, daß $a \bmod p^t$ die Einheitengruppe erzeugt. Erfüllt schließlich a die letzten beiden Bedingungen des Satzes, so hat $a \bmod p^2$ die Ordnung $(p-1)p$, erzeugt also die Einheitengruppe $\bmod p^2$. □

(5.11) Satz. *Für $t \geq 3$ ist $(\mathbb{Z}/2^t)^*$ direktes Produkt von $\{\pm 1\}$ mit der durch $5 \bmod 2^t$ erzeugten zyklischen Untergruppe der Ordnung 2^{t-2}.*

BEWEIS. Daß $5 \bmod 2^t$ die angegebene Ordnung hat folgt aus $5^{2^{t-3}} \equiv 1 + 2^{t-1} \bmod 2^t$, was durch Induktion nach t leicht durch Quadrieren folgt. Da schon $5^u \equiv -1 \bmod 8$ unmöglich ist, handelt es sich um ein direktes Produkt. □

Insgesamt liefern die vorstehenden Sätze die Struktur der Einheitengruppe von $\mathbb{Z}/m$.

(5.12) Endomorphismen von $\mathbb{Z}/n$. Wir bestimmen den Endomorphismenring der abelschen Gruppe $\mathbb{Z}/n$. Ein Endomorphismus ist durch den Wert an der

Stelle $1 + n\mathbb{Z}$ bestimmt. Die Abbildung

$$a_k \colon \mathbb{Z}/n \to \mathbb{Z}/n, \quad r + n\mathbb{Z} \mapsto k \cdot r + n\mathbb{Z}$$

ist ein wohldefinierter Homomorphismus; aus $k \equiv l \bmod n$ folgt $a_k = a_l$. Es gelten die Regeln $a_{k+l} = a_k + a_l$ und $a_{kl} = a_k a_l$. Also ist $k + n\mathbb{Z} \mapsto a_k$ ein wohldefinierter Isomorphismus $\mathbb{Z}/n \cong \mathrm{End}(\mathbb{Z}/n)$. Die Einheiten des Ringes $\mathbb{Z}/n$ liefern genau die Automorphismen der abelschen Gruppe $\mathbb{Z}/n$. $\diamond$

Sei p eine Primzahl und $r_j \colon \mathbb{Z}/p^j \to \mathbb{Z}/p^{j-1}$ der Reduktionshomomorphismus. Die Menge

$$\mathbb{Z}_p = \{(x_j) \in \prod_{j=1}^{\infty} \mathbb{Z}/p^j \mid r_j(x_j) = x_{j-1}\}$$

ist ein Unterring. Dieser Ring heißt der *Ring der ganzen p-adischen Zahlen*. Jede natürliche n besitzt eine eindeutig bestimmte Darstellung der Form

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_t p^t, \qquad \text{mit } 0 \le a_j \le p - 1.$$

Dazu braucht p nicht einmal eine Primzahl zu sein, zum Beispiel liefert $p = 10$ die Dezimaldarstellung und $p = 2$ die Nulleinsfolgen der Maschinenwelt. Die Darstellung nennt man die *p-adische Darstellung* von n. Die p-adische Darstellung erhält man, indem man nacheinander die Bilder von n in $\mathbb{Z}/p^j$ anschaut. Wir erhalten einen injektiven Ringhomomorphismus $i \colon \mathbb{Z} \to \mathbb{Z}_p$, indem wir $n \in \mathbb{Z}$ auf die Folge $(n \bmod p^j)$ abbilden. Ein Beispiel einer Folge, die nicht im Bild von i liegt, ist durch $x_j = 1 + p + \cdots + p^{j-1}$ gegeben. Wegen der Formel für die geometrische Reihe ist $x_j \in \mathbb{Z}/p^j$ ein Inverses von $1 - p$ für alle j. Die Folge liefert also ein Inverses von $1 - p$ in $\mathbb{Z}_p$. Wir können diesen Sachverhalt suggestiv (mit Eulerschem Mut) durch die geometrische Reihe

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \cdots$$

beschreiben, jedoch hat die Summe keinen Sinn als *reelle* Zahl. Jedes Element von $\mathbb{Z}_p$ können wir *formal* durch eine Potenzreihe der Form

$$a_0 + a_1 p + a_2 p^2 + \cdots, \qquad \text{mit } \ 0 \le a_j \le p - 1$$

eindeutig beschreiben, indem wir festlegen, daß die k-te Partialsumme das Folgenelement in $\mathbb{Z}/p^{k+1}$ ist.

5 Moduln

1 Grundbegriffe

Moduln über Ringen verallgemeinern Vektorräume über Körpern. In der Modultheorie erfahren die Methoden der linearen Algebra eine weitreichende Ausdehnung. Ringe werden durch ihre modultheoretischen Eigenschaften untersucht.

(1.1) Modul. Ein *Linksmodul* über einem Ring R besteht aus einer additiven abelschen Gruppe M und einer Abbildung $R \times M \to M$, $(r, m) \mapsto rm$ mit folgenden Eigenschaften:

(1.2) Für $1, r, r_1, r_2 \in R$ und $m, m_1, m_2 \in M$ gilt:

$$\begin{aligned} r(m_1 + m_2) &= rm_1 + rm_2 \\ (r_1 + r_2)m &= r_1 m + r_2 m \\ r_1(r_2 m) &= (r_1 r_2)m \\ 1 \cdot m &= m. \end{aligned}$$

Die Abbildung $R \times M \to M$ heißt *Multiplikation mit Skalaren*. Sie definiert die *Struktur eines R-Moduls* auf der abelschen Gruppe M.

Wir sprechen von *Rechtsmoduln*, wenn eine Abbildung $M \times R \to M$, $(m, r) \mapsto mr$ mit zu (1.2) analogen Eigenschaften gegeben ist. Wenn nichts anderes gesagt wird, verwenden wir im folgenden Linksmoduln. ◇

Ist M ein R-Modul, so ist $L_r \colon M \to M$, $m \mapsto rm$ (die *Linkstranslation* mit r) ein Endomorphismus der abelschen Gruppe M. Die Eigenschaften (1.2) besagen, daß $r \mapsto L_r$ ein Ringhomomorphismus $R \to \mathrm{End}(M)$ ist. Umgekehrt liefert jeder Ringhomomorphismus $L \colon R \to \mathrm{End}(M)$ durch $R \times M \to M$, $(r, m) \mapsto (L(r))(m)$ eine R-Modulstruktur auf M. Rechtsmoduln werden dagegen durch Antihomomorphismen $R \to \mathrm{End}(M)$ gegeben. Insbesondere ist jede abelsche Gruppe ein Modul über ihrem Endomorphismenring.

Beispiele. (1) Ein Modul über einem Körper ist dasselbe wie ein Vektorraum über einem Körper.
(2) Durch $M_n(K) \times K^n \to K^n$, $(A, x) \mapsto Ax$ wird K^n zu einem Modul über dem Ring der (n, n)-Matrizen.
(3) Eine abelsche Gruppe M ist im wesentlichen dasselbe wie ein $\mathbb{Z}$-Modul. Die $\mathbb{Z}$-Modulstruktur wird so definiert: Für $n \in \mathbb{N}$ und $x \in M$ setzen wir $nx = (1 + \cdots + 1)x = x + \cdots + x$ (jeweils n Summanden) und $(-n)x = -(nx)$.
(4) Die additive Gruppe eines Ringes R wird durch Linksmultiplikation ein R-Linksmodul, zur Unterscheidung vom Ring R auch mit ${}_\ell R$ bezeichnet. Er heißt der *linksreguläre* Modul. Analog liefert R einen R-Rechtsmodul R_r, den *rechtsregulären* Modul. ◇

Sei M ein R-Modul. Eine Teilmenge $N \subset M$ heißt *Untermodul* von M, wenn N additive Untergruppe ist und $r \in R$, $n \in N$ immer $rn \in N$ impliziert. Mit der durch M induzierten Addition und mit $R \times N \to N$, $(r, n) \mapsto rn$ wird dann N

selbst zu einem R-Modul. Ein Untermodul des linksregulären Moduls ist dasselbe wie ein Linksideal.

Der Durchschnitt beliebig vieler Untermoduln ist wieder ein Untermodul. Ist $S \subset M$, so ist der Durchschnitt aller S enthaltenden Untermoduln, der von S *erzeugte Untermodul*, durch die Menge aller R-Linearkombinationen endlicher Länge

$$\langle S\rangle = \{\sum_{i=1}^{n} a_i x_i \mid n \in \mathbb{N},\ a_i \in R,\ x_i \in S\} \tag{1.3}$$

gegeben. Ist S endlich, so heißt $\langle S\rangle$ *endlich erzeugt*.

Seien M und N R-Moduln. Eine Abbildung $f\colon M \to N$ heißt *R-linear*, *R-Homomorphismus*, oder *Homomorphismus von R-Moduln*, wenn für $m, m_1, m_2 \in M$ und $r \in R$ immer gilt:

$$f(m_1 + m_2) = f(m_1) + f(m_2), \quad f(rm) = rf(m).$$

Wie üblich heißt $f^{-1}(0)$ der *Kern* einer R-linearen Abbildung. Bild und Kern einer R-linearen Abbildung sind Untermoduln. Allgemeiner: Bilder und Urbilder von Untermoduln bei einer linearen Abbildung sind wieder Untermoduln. In analoger Weise werden *R-bilineare* Abbildungen $f\colon M_1 \times M_2 \to N$ definiert: R-linear in jeder Variablen.

Die Verkettung von R-linearen Abbildungen ist wieder eine. Damit haben wir die Kategorie R-Mod der R-Moduln erklärt und damit wie üblich Begriffe wie Isomorphismus, Endomorphismus, Automorphismus von R-Moduln zur Verfügung. Eine Sequenz

$$\ldots \longrightarrow M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} M_{i+2} \longrightarrow \ldots$$

heißt *exakt an der Stelle M_{i+1}*, wenn Bild $f_i =$ Kern f_{i+1} ist und *exakt*, wenn sie an jeder Stelle exakt ist. Eine *kurze exakte Sequenz* ist eine exakte Sequenz der Form

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0.$$

Dabei bezeichnen wir mit 0 auch den *Nullmodul*, dessen additive Gruppe nur aus dem Nullelement besteht. Eine R-lineare Abbildung $f\colon A \to B$ ist genau dann injektiv, wenn ihr Kern der Nullmodul ist. In einer kurzen exakten Sequenz ist also insbesondere α injektiv und β surjektiv.

Sei S Teilmenge eines R-Moduln M. Dann heißt S *linear unabhängig*, wenn für je endlich viele paarweise verschiedene Elemente $s_1, \ldots, s_n$ aus S und $\lambda_1, \ldots, \lambda_n \in R$ aus $\lambda_1 s_1 + \cdots + \lambda_n s_n = 0$ immer $\lambda_1 = \ldots = \lambda_n = 0$ folgt. Man nennt S *Basis* von M, wenn $\langle S\rangle = M$ und S linear unabhängig ist. Besitzt M eine Basis, so heißt M ein *freier* R-Modul.

Ein freier Modul M mit Basis S hat die folgende universelle Eigenschaft: Ist $f\colon M \to N$ R-linear, so ist f durch die Werte auf Elementen aus S bestimmt. Zu jeder Wahl von Elementen $n_s \in N$, $s \in S$ gibt es genau eine R-lineare Abbildung f mit $f(s) = n_s$.

Zu jeder Menge S gibt es einen freien R-Modul mit Basis S (*freier Modul über S*). Er läßt sich folgendermaßen konstruieren: Sei $R^{(S)}$ die Menge aller Abbildungen $S \to R$, die nur an endlich vielen Stellen von Null verschiedene Werte annehmen. Die Menge $R^{(S)}$ wird durch Addition und Skalarmultiplikation von Funktionswerten zu einem R-Modul. Zu jedem $s \in S$ sei $\bar{s} \in R^{(S)}$ die durch $\bar{s}(t) = 1$ für $t = s$ und $\bar{s}(t) = 0$ für $t \neq s$ definierte Abbildung. Eine kurze Überlegung zeigt: $\bar{S} = \{\bar{s} \mid s \in S\}$ ist eine Basis von $R^{(S)}$. Wir lassen deshalb Querstriche weg. Elemente von $R^{(S)}$ sind *formale Linearkombinationen* $\Sigma r_i s_i$, $r_i \in R$, $s_i \in S$ (endliche Summen).

Indem wir den freien Modul über einem Erzeugendensystem eines Moduls N und die universelle Eigenschaft benutzen, sehen wir: Zu jedem Modul N gibt es eine Surjektion $M \to N$ eines freien Moduls M.

Der typische freie R-Modul ist der R-Modul R^n aller n-Tupel $(r_1, \ldots, r_n)$ von Elementen $r_i \in R$ mit komponentenweiser Addition und Skalarmultiplikation. Die *Standardbasis* ist $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$. Hat ein freier R-Modul F eine n-elementige Basis, so heißt n der *Rang* von F. Ein freier Modul vom Rang n ist isomorph zu R^n. Wir zeigen im *Rangsatz* (1.6), daß der Rang wohldefiniert ist, sofern R kommutativ ist. Allgemein gilt das leider nicht.

Eine Untergruppe N einer abelschen Gruppe M ist immer Normalteiler und deshalb M/N immer definiert. Ist M ein Modul über einem Ring R und N ein Untermodul, so ist deshalb zunächst M/N als abelsche Gruppe definiert. Sei $p\colon M \to M/N$ die kanonische Abbildung. Für jedes $r \in R$ induziert die Linkstranslation $L_r\colon M \to M$ mit r genau einen Homomorphismus $l_r\colon M/N \to M/N$, der das Diagramm

$$\begin{array}{ccc} M & \xrightarrow{L_r} & M \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} \\ M/N & \xrightarrow{l_r} & M/N \end{array}$$

kommutativ macht. Definieren wir l_r als Linkstranslation von r auf M/N, so wird, wie man leicht nachweist, auf diese Weise eine R-Modulstruktur auf M/N definiert. Wir nennen den so definierten Modul M/N den *Faktormodul* (*Quotientmodul*) M modulo N. Ist $f\colon M \to N$ R-linear, so heißt der Quotient $N/f(M)$ der *Kokern* von f.

(1.4) Satz. *Die Faktorabbildung $p\colon M \to M/N$ hat die universelle Eigenschaft: Sei $f\colon M \to A$ ein R-Homomorphismus zwischen R-Moduln. Es gibt genau dann einen R-Homomorphismus $F\colon M/N \to A$, der die Relation $Fp = f$ erfüllt, wenn N im Kern von f liegt. Genau dann ist F injektiv, wenn $N = \operatorname{Kern} f$ ist.* □

Sei I ein Linksideal von R und M ein Linksmodul. Die Menge aller endlichen Summen der Form $\sum_j a_j x_j$ mit $a_j \in I$ und $x_j \in M$ ist ein Untermodul IM von M. Das Ideal I liegt im Kern der Linkstranslation $L\colon R \to \operatorname{End}(M/IM)$. Ist I ein Ideal, so macht der induzierte Homomorphismus M/IM zu einem R/I-Modul.

(1.5) Notiz. *Ist S eine Basis des R-Moduls M und I ein Ideal von R, so ist die Bildmenge $\overline{S}$ von S in M/IM eine Basis des R/I-Moduls M/IM. Ferner gilt $|S| = |\overline{S}|$.*

Beweis. Offenbar ist $\overline{S}$ ein Erzeugendensystem. Seien $p\colon R \to R/I$ und $q\colon M \to M/IM$ die Quotientabbildungen. Sei $\varphi\colon \overline{S} \to Z$ eine Mengenabbildung in einen R/I-Modul Z. Wir fassen Z vermöge p als R-Modul auf (Aufgabe 2). Es gibt dann genau eine R-lineare Abbildung $\Phi'\colon M \to Z$ mit $\varphi \circ q|S = \Phi'|S$. Da Skalarmultiplikation mit $a \in I$ auf Z die Nullabbildung ist, liegt IM im Kern von Φ'. Deshalb wird $\Phi\colon M/IM \to Z$ mit $\Phi \circ q = \Phi'$ induziert, und es gilt $\varphi = \Phi|\overline{S}$. Damit haben wir die universelle Eigenschaft eines freien Moduls verifizert.

Die Abbildung $q\colon S \to \overline{S}$ ist injektiv. Aus $q(s) = q(t)$ folgt nämlich $s - t = \sum_{u\in S} a_u u$ mit $a_u \in I$, was wegen $I \neq R$ eine echte Linearkombination zwischen Basiselementen ist, wenn $s \neq t$ ist. □

(1.6) Satz. *Sei $R \neq 0$ ein kommutativer Ring. Je zwei Basen eines freien R-Moduls sind gleichmächtig.*

Beweis. Wir wenden die vorstehende Notiz auf ein maximales Ideal I an. Die Behauptung folgt dann aus dem Spezialfall für den Körper R/I. □

Seien M und N Moduln über dem kommutativen Ring R. Die Menge $\mathrm{Hom}_R(M, N)$ aller R-linearen Abbildungen $M \to N$ wird durch die folgenden Festsetzungen zu einem R-Modul *Homomorphismenmodul*:

$$(f_1 + f_2)(m) := f_1(m) + f_2(m), \quad (rf)(m) := r(f(m)).$$

(Woran scheitert diese Definition bei einem nichtkommutativen Ring R?) Ist $f\colon M_1 \to M_2$ R-linear, so erklären wir R-lineare Abbildungen (Hom-Funktor)

$$f^*\colon \mathrm{Hom}_R(M_2, N) \to \mathrm{Hom}_R(M_1, N), \quad \alpha \mapsto \alpha \circ f$$

$$f_*\colon \mathrm{Hom}_R(N, M_1) \to \mathrm{Hom}_R(N, M_2), \quad \beta \mapsto f \circ \beta.$$

Den Index R an Hom lassen wir weg, wenn R aus dem Kontext erkenntlich ist.

Dualmoduln sind wichtige Spezialfälle der Hom-Moduln. Ist R ein kommutativer Ring und M ein R-Modul, so heißt der R-Modul $M^* := \mathrm{Hom}_R(M, R)$ der *Dualmodul* von M. Eine R-lineare Abbildung $f\colon M \to N$ induziert eine R-lineare Abbildung $f^*\colon N^* \to M^*$, $\alpha \mapsto f \circ \alpha$. Es gelten die Regeln $(gf)^* = f^*g^*$, $\mathrm{id}^* = \mathrm{id}$. Wir bemerken, daß die Komposition

$$\mathrm{Hom}(N, P) \times \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, P), \quad (g, f) \mapsto g \circ f$$

bilinear ist.

Sei $f\colon R \to S$ ein Ringhomomorphismus und M ein S-Modul. Durch $R \times M \to M$, $(r, m) \mapsto f(r)m$ wird die abelsche Gruppe M zu einem R-Modul. Spezialfall: R Unterring von S; dann ist S ein linker R-Modul. Ist R ein Körper, so wird S ein R-Vektorraum. Das gilt erst recht, wenn R und S Körper sind, in welchem

Fall man S eine *Körpererweiterung* von R nennt. Im Falle von Körpern heißt die Dimension $\dim_R S$ der *Grad* der Erweiterung und wird mit $[S : R]$ bezeichnet. Ein Körper der Charakteristik $p > 0$ vom Grad n über seinem Primkörper hat p^n Elemente.

Sei R kommutativ. Es gibt eine kanonische Abbildung $\kappa\colon M \to (M^*)^*$ eines R-Moduls M in den doppelten Dualmodul (*Bidualmodul*), nämlich $x \mapsto (\alpha \mapsto \alpha(x))$. Ist M ein endlich erzeugter freier R-Modul, so ist κ ein Isomorphismus.

Für nichtkommutative Ringe R hat man keinen natürlichen Begriff eines Dualmoduls. Jedoch ist $\mathrm{Hom}_R(M, R)$ in kanonischer Weise ein Rechtsmodul, wenn M ein Linksmodul ist, und zwar mit der Skalarmultiplikation $(\varphi \cdot a)(x) = \varphi(x) \cdot a$. Man muß hier von rechts multiplizieren, damit $\varphi \cdot a$ wieder R-linear ist.

(1.7) Aufgaben und Ergänzungen.

1. Sei R ein kommutativer Ring. Jeder R-Modul ist genau dann frei, wenn R ein Körper ist.

2. Sei $\varphi\colon R \to S$ ein Ringhomomorphismus. Ist M ein S-Modul, so wird er durch die Skalarmultiplikation $(r, x) \mapsto \varphi(r)x$ zu einem R-Moduln. Aus S-linearen Abbildungen werden R-lineare. Damit haben wir einen Funktor $R\text{-}\,\mathrm{Mod} \to S\text{-}\,\mathrm{Mod}$.

2 Summen und Produkte

Sei $(M_j \mid j \in J)$ eine Familie von R-Moduln. Ihr *Produkt* $M = \prod_{j\in J} M_j$ ist derjenige R-Modul, dessen zugrundeliegende additive Gruppe das Produkt der additiven Gruppen ist. Die Skalarmultiplikation wird wieder komponentenweise definiert: $r(m_j \mid j \in J) = (rm_j \mid j \in J)$. Die Projektionen $p_k\colon \prod_j M_j \to M_k$ auf die Faktoren sind R-linear. Die Abbildung

$$\textbf{(2.1)} \qquad \mathrm{Hom}(N, M) \to \prod_j \mathrm{Hom}(N, M_j), \quad f \mapsto (p_j \circ f)$$

ist für jeden R-Modul bijektiv. Das ist die universelle Eigenschaft des Produktes. Wir nennen allgemein eine Familien $p_j\colon M \to M_j$ ein *Produkt* der M_j, wenn (2.1) für alle N bijektiv ist. Ist $q_j\colon M' \to M_j$ eine zweite Familie mit der entsprechenden universellen Eigenschaft, so gibt es genau einen Isomorphismus $\varphi\colon M' \to M$ mit $p_j \circ \varphi = q_j$. Zum Beweis wendet man (2.1) mit $N = M'$ an und vertauscht dann die Rollen von M und M', um einen inversen Homomorphismus $\psi\colon M \to M'$ mit $q_j \circ \psi = p_j$ zu erhalten. Wegen $p_j \circ \varphi \circ \psi = p_j$ folgt aus (2.1) $\varphi \circ \psi = \mathrm{id}$ und analog $\psi \circ \varphi = \mathrm{id}$. Damit bestimmt also die universelle Eigenschaft die Situation bis auf eindeutige Isomorphie. Das mengentheoretische Produkt $\prod_j f_j$ R-linearer Abbildungen f_j ist R-linear. Statt Produkt wird auch *direktes* Produkt gesagt.

Die *Summe* $M = \bigoplus_{j\in J} M_j$ der Familie von R-Moduln M_j ist der folgende R-Modul. Elemente sind alle Familien $(m_j \mid j \in J)$, die nur an endlich vielen Stellen j von Null verschieden sind. Addiert und skalarmultipliziert wird komponentenweise wie beim Produkt. Die *Injektion des k-ten Summanden* $i_k\colon M_k \to \bigoplus_{j\in J} M_j$ bildet $m_k \in M_k$ auf die Familie ab, die an der Stelle k das Element m_k und sonst überall die Null hat. Das Bild von i_k wird oft mit M_k identifiziert; in dieser Weise

betrachten wir M_k als Untermodul der Summe. Statt Summe wird auch *direkte* Summe gesagt. Die Abbildung

$$\textbf{(2.2)} \qquad \operatorname{Hom}(M,N) \to \prod_j \operatorname{Hom}(M_j,N), \quad f \mapsto (f \circ i_j)$$

ist für jeden R-Modul N bijektiv. Das ist die universelle Eigenschaft der direkten Summe. Das Urbild von (f_j) bei (2.2) wird mit $\langle f_j \rangle$ bezeichnet; manchmal auch suggestiv aber ungenau mit $\sum_j f_j$. Eine Familie $i_j\colon M_j \to M$ von R-linearen Abbildungen heißt eine *Summe* der M_j, wenn die Abbildung (2.2) immer bijektiv ist. Wie beim Produkt sieht man, daß dadurch die Situation bis auf eindeutige Isomorphie festgelegt ist.

Für endliche Indexmengen J sind Summe und Produkt von Moduln nicht verschieden. Wir unterscheiden sie trotzdem begrifflich, weil die Summe für Abbildungen „heraus“ und das Produkt für Abbildungen „hinein“ zuständig ist. Die Summe zweier Moduln M_1 und M_2 wird mit $M_1 \oplus M_2$ bezeichnet.

Sind M_j, $j \in J$, Untermoduln von M, so bezeichne $\sum_{j\in J} M_j$ den von $\bigcup_j M_j$ erzeugten Untermodul (oder $M_1 + M_2 + \cdots + M_n$ falls $J = \{1,2,\dots,n\}$). Er besteht aus allen Summen der Form $\Sigma_j m_j$, in denen alle bis auf endlich viele $m_j \in M_j$ gleich Null sind. In dieser Situation nennen wir $\sum_j M_j$ die *Summe* der Untermuduln. Diese ist dann sorgsam von der direkten Summe $\bigoplus_{j\in J} M_j$ zu unterscheiden.

Seien M, N Untermoduln eines R-Moduls E. Wir definieren Abbildungen und Sequenzen

$$\textbf{(2.3)} \qquad 0 \to M \cap N \xrightarrow{u} M \oplus N \xrightarrow{p} M + N \to 0$$

$$\textbf{(2.4)} \qquad 0 \to E/(M \cap N) \xrightarrow{v} (E/M) \oplus (E/N) \xrightarrow{q} E/(M+N) \to 0$$

durch: $u(x) = (x,x)$, $p(m,n) = m - n$, $v(y) = (y,y)$, $q(y,z) = y - z$; bei v und q sind $y, z \in E$ und bezeichnen die jeweils zugehörigen Restklassen.

(2.5) Satz. *Die Sequenzen* (2.3) *und* (2.4) *sind exakt.*

Beweis. Offenbar ist u injektiv und p surjektiv. Es ist $pu(x,x) = x - x = 0$. Sei $p(m,n) = m - n = 0$. Dann ist $m = n \in M \cap N$. Damit ist (2.3) als exakt erkannt.

Es ist q surjektiv, da etwa $E/M \to E(N+N)$ surjektiv ist. Sei $v(y) = 0$. Das bedeutet: $y \in M$ und $y \in N$, also $y \in M \cap N$. Somit ist die Restklasse von y in $E/(M \cap N)$ die Nullklasse. Folglich ist v injektiv. Offenbar ist qv die Nullabbildung. Sei schließlich $q(y,z) = 0$. Das bedeutet: $y - z \in M + N$. Wir setzen deshalb an: $y - z = n - m$, $m \in M$, $n \in N$. Dann ist $y + m = z + n =: x$ und $y + m \equiv y \bmod M$, $z + n \equiv z \bmod N$. Also ist $v(x) = (y,z)$. □

Seien M_j, $j \in J$, Untermoduln von E, und sei $f_j\colon M_j \to E$ die Inklusion. Wir nennen E die (*interne*) *direkte Summe* der M_j, wenn die (kanonisch genannte) Abbildung $\langle f_j \rangle\colon \bigoplus_{j\in J} M_j \to E$, $(x_j) \mapsto \sum_j x_j$ ein Isomorphismus ist.

(2.6) Satz. *Seien M_j, $j \in J$, Untermoduln von E. Folgende Aussagen sind äquivalent:*

(1) *$\sum_j M_j$ ist direkte Summe der M_j .*
(2) *Für jedes $i \in J$ ist $M_i \cap \sum_{j,j\neq i} M_j = \{0\}$.*
(3) *Aus $\sum_j x_j = 0$, $x_j \in M_j$, fast alle $x_j = 0$, folgt $x_j = 0$ für alle j.*

Beweis. (2) $\Rightarrow$ (1). Liege $(x_j) \in \bigoplus_j M_j$ im Kern der kanonischen Abbildung $\bigoplus_j M_j \to \Sigma_j M_j$. Dann ist also $\sum x_j = 0$ und folglich

$$x_i = -\sum_{j,j\neq i} x_j \in M_i \cap \sum_{j,j\neq i} M_j.$$

Wegen (2) ist $x_j = 0$. Die kanonische Abbildung ist somit injektiv. Sie ist nach Definition surjektiv.

(1) $\Rightarrow$ (2). Wäre $M_i \cap \sum_{j,j\neq i} M_j \neq \{0\}$, so würden wir ein von Null verschiedenes Element im Kern der kanonischen Abbildung finden.

(1) $\Leftrightarrow$ (3). Eine Familie (x_j) mit den in (3) angegebenen Eigenschaften ist ein Element im Kern der kanonischen Abbildung. □

Eine R-lineare Abbildung $p\colon M \to M$ heißt *Projektion*, wenn $p \circ p = p$ ist.

(2.7) Satz. *Sei $p\colon M \to M$ eine Projektion. Dann ist M direkte Summe von* Kern(p) *und* Bild(p). *Es ist* id $- p = q$ *ebenfalls eine Projektion.*

Beweis. Sei $p(x) = 0$ und $x = p(y)$. Dann ist $0 = p(x) = p^2(y) = p(y) = x$. Also haben Kern und Bild den Schnitt Null. Es liegt $x - p(x)$ immer im Kern von p. Aus $x = p(x) + (x - p(x))$ sehen wir, daß Kern und Bild zusammen M erzeugen. Nun wenden wir (2.6) an. □

Ein Untermodul F von E heißt *direkter Summand* von E, wenn es einen Untermodul G von E so gibt, daß $E = F \oplus G$ ist. Es heißt dann G ein *Komplement* von F in E.

(2.8) Satz. *Sei* $0 \to E \xrightarrow{f} F \xrightarrow{g} G \to 0$ *eine exakte Folge von R-Moduln. Folgende Aussagen sind äquivalent:*

(1) *$f(E)$ ist direkter Summand von F.*
(2) *Es gibt eine R-lineare Abbildung $r\colon F \to E$ mit $rf = \mathrm{id}$.*
(3) *Es gibt eine R-lineare Abbildung $s\colon G \to F$ mit $gs = \mathrm{id}$.*

Gilt (1) – (3), so sagen wir: Die Sequenz spaltet auf. Wir nennen r, s *Aufspaltungen* und s einen *Schnitt* von g.

Beweis. (1) $\Rightarrow$ (2). Sei $F = f(E) \oplus U$, und sei $p\colon F \to f(E)$ die dadurch gegebene Projektion auf den Summanden $f(E)$. Da f injektiv ist, so ist $E \to f(E)$, $\alpha \mapsto f(x)$ ein Isomorphismus, etwa mit Inversem α. Wir setzen $r = \alpha p$. Dann ist $rf(x) = \alpha p f(x) = \alpha f(x) = x$.

(2) $\Rightarrow$ (1). Sei $q = fr$. Dann ist q eine Projektion. Bild$(q) \subset$ Bild(f) ist klar. Sei $y = f(x) \in$ Bild(f). Dann ist $y = f(x) = frf(x) = qf(x) \in$ Bild(q). Jetzt wenden wir (2.7) an.

(3) $\Rightarrow$ (1). Sei $p = sg$. Dann ist p eine Projektion. Wegen $gf = 0$ ist $\mathrm{Bild}(f) \subset \mathrm{Kern}(p)$. Sei $y = \mathrm{Kern}\, p$. Dann ist $g(y) = gsg(y) = gp(y) = 0$, also wegen Exaktheit $y \in \mathrm{Bild}(f)$. Jetzt wenden wir (2.7) an.
(1) $\Rightarrow$ (3). Sei $F = f(E) \oplus U$. Aus der Exaktheit folgt, daß $g|U$ einen Isomorphismus $U \to G$ liefert, etwa mit Inversem β. Wir setzen s als Verkettung von β mit $U \subset F$ fest. □

(2.9) Folgerung. *Ist G in* (2.8) *frei, so spaltet die Sequenz auf.*

Beweis. Sei $(x_j \mid j \in J)$ Basis von G. Wir erhalten einen Schnitt, indem wir x_j auf ein Element von $g^{-1}(x_j)$ abbilden und linear fortsetzen. □

Seien M_j R-Moduln und $N_j \subset M_j$ Untermoduln $(j \in J)$. Dann kann $\bigoplus_j N_j$ als Untermodul von $\bigoplus_j M_j$ aufgefaßt werden. Die Summe $\bigoplus p_j$ der Faktorabbildungen $p_j \colon M_j \to M_j/N_j$ hat den Kern $\bigoplus N_j$ und induziert deshalb einen Isomorphismus

$$(\bigoplus_j M_j)/(\bigoplus_j N_j) \xrightarrow{\cong} \bigoplus_j (M_j/N_j). \tag{2.10}$$

(2.11) Beispiel. Sei p eine Primzahl. Es gibt eine exakte Sequenz

$$0 \to \mathbb{Z}/p \xrightarrow{f} \mathbb{Z}/p^2 \xrightarrow{g} \mathbb{Z}/p \to 0,$$

worin $g \colon x \bmod p^2 \mapsto x \bmod p$ und $f \colon x \bmod p \mapsto px \bmod p^2$. Die Sequenz spaltet nicht auf, denn andernfalls wäre $\mathbb{Z}/p^2$ zu $\mathbb{Z}/p \times \mathbb{Z}/p$ isomorph, und jedes Element von $\mathbb{Z}/p^2$ würde durch p annulliert. ◇

(2.12) Beispiel. Ein Untermodul von $M_1 \oplus M_2$ hat im allgemeinen *nicht* die Form $N_1 \oplus N_2$ für Untermoduln $N_j \subset M_j$. So hat $\mathbb{Z}/p \times \mathbb{Z}/p$ genau $p+1$ Untergruppen der Ordnung p (= eindimensionale Unterräume in einem zweidimensionalen Vektorraum über dem Körper $\mathbb{Z}/p$). ◇

(2.13) Satz. *Seien $M, M_1, \ldots, M_n$ Moduln und $i_k \colon M_k \to M$, $p_k \colon M \to M_k$ lineare Abbildungen mit den folgenden Eigenschaften:*
(1) $p_k i_k = \mathrm{id}(M_k)$; $p_l i_k = 0$, *für* $l \neq k$
(2) $\sum_k i_k p_k = \mathrm{id}(M)$.
Dann bilden die (i_k) eine Summe und die (p_k) ein Produkt.

Beweis. Sind nämlich

$$i \colon \bigoplus_k M_k \to M, \qquad p \colon M \to \prod M_k$$

die Abbildungen mit den Komponenten (i_k) und (p_k), so besagt (1), daß pi die Identität ist, und (2), daß ip die Identität ist. □

Sei $M = M_1 \oplus \cdots \oplus M_n$ eine interne Zerlegung eines A-Moduls. Die Projektionen $e_i \colon M \to M_i \subset M$, $\sum m_j \mapsto m_i$ sind Elemente des Endomorphismenringes $\mathrm{End}_A(M)$, die offenbar eine Einszerlegung dieses Ringes bilden. Ist umgekehrt

eine Einszerlegung (e_j) in $\mathrm{End}_A(M)$ gegeben und setzen wir $M_i = \mathrm{Bild}(e_i)$, so bilden die M_i eine direkte Zerlegung von M als A-Modul. Damit haben wir:

(2.14) Satz. *Es besteht eine bijektive Beziehung zwischen internen Summenzerlegungen $(M_1, \ldots, M_n)$ eines A-Moduls M und Einszerlegungen $(e_1, \ldots, e_n)$ von $\mathrm{End}_A(M)$. Dabei ist e_i die Projektion auf M_i.* □

Direkte Summen sind die Grundlage der *Matrizenrechnung*. Wir gehen von $M = \bigoplus_{k=1}^m M_k$ aus und verwenden die Inklusionen i_k und die Projektionen p_k wie eben. Weiter sei $N = \bigoplus_{l=1}^n N_l$ mit Inklusionen j_l und Projektionen q_l gegeben. Einer linearen Abbildung $f\colon M \to N$ ordnen wir die $n \times m$-Matrix f_{lk} mit $f_{lk} = q_l f i_k$ zu. Die Einträge an der Stelle (l,k) stammen also aus $\mathrm{Hom}(M_k, N_l)$. Wir erhalten eine Bijektion zwischen $\mathrm{Hom}(M,N)$ und der Menge derartiger Matrizen. Fassen wir m-Tupel aus $\bigoplus_k M_k$ als Spaltenvektoren auf, so wird die lineare Abbildung f in der Matrizenform durch die gewohnte Formel $(f_{lk})(x_k) = (\sum_k f_{lk}(x_k))$ gegeben. Der Komposition von Abbildungen entspricht ein Matrizenprodukt, das durch die gewohnte Formel $(g_{ml})(f_{lk}) = (g_{ml} \circ f_{lk})$ gegeben ist.

Äußerlich hat sich also in dieser allgemeinen Situation nichts gegenüber der elementaren linearen Algebra geändert. Trotzdem ist Vorsicht angebracht. Denn wie wird eine lineare Abbildung $f\colon M \to N$ beschrieben, wenn M ein freier Modul mit Basis $x_1, \ldots, x_m$ und N ein freier Modul mit Basis $y_1, \ldots, y_n$ ist? Dann ist M_k der von x_k aufgespannte Untermodul und N_l der von y_l aufgespannte. Ist $f(x_k) = \sum_l a_{kl} y_l$, so ist f_{lk} die Abbildung

$$\lambda_k x_k \mapsto \lambda_k a_{kl} y_l.$$

Hier findet gegenüber dem Üblichen ein Vertauschung der Faktoren statt. Die linearen Abbildungen $R \to R$ des regulären Linksmoduls werden durch Rechtsmultiplikation mit Elementen aus R gegeben. Der Komposition solcher Abbildungen entspricht die Multiplikation im Gegenring R°.

3 Diagramme

Größere Komplexe von Moduln oder Gruppen und Homomorphismen werden oft übersichtlich in Sequenzen und Diagrammen notiert. Wir geben in diesem Abschnitt einige typische Beispiele dafür an, wie mit diesen Hilfsmitteln gearbeitet wird.

(3.1) Satz. *Sei R ein kommutativer Ring und $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ eine Sequenz von R-Moduln. Diese Sequenz ist genau dann exakt, wenn für jeden R-Modul N die induzierte Sequenz*

$$0 \to \mathrm{Hom}(C,N) \xrightarrow{g^*} \mathrm{Hom}(B,N) \xrightarrow{f^*} \mathrm{Hom}(A,N)$$

exakt ist.

Beweis. Sei die Sequenz $A \to B \to C \to 0$ exakt. Rechenregeln wie $f^* g^* = (gf)^*$ und $0^* = 0$ zeigen, daß in der induzierten Sequenz, die Verkettung je zweier

Morphismen Null ist. Ist $g^*(\alpha) = \alpha \circ g = 0$, so ist $\alpha = 0$, weil g surjektiv ist. Also ist g^* injektiv. Sei $f^*(\beta) = \beta \circ f = 0$. Dann bildet also β den Kern von g auf Null ab. Durch $\alpha(c) = \beta(b)$ für $b \in g^{-1}(c)$ wird deshalb eine wohldefinierte Abbildung $\alpha\colon C \to N$ definiert, die leicht als R-linear nachgewiesen wird. Nach Konstruktion gilt $g^*(\alpha) = \beta$. Damit ist auch die Exaktheit an der Stelle $\mathrm{Hom}(B, N)$ gezeigt.

Sei die induzierte Sequenz immer exakt. Die kanonische Abbildung $\alpha\colon C \to \mathrm{Kokern}(g)$ wird bei g^* auf Null abgebildet. Da g^* injektiv ist, so ist $\alpha = 0$, was nur möglich ist, wenn g surjektiv ist. Es ist $0 = f^*g^*(\mathrm{id}) = gf$, also gilt $\mathrm{Bild}(f) \subset \mathrm{Kern}(g)$. Die kanonische Abbildung $\beta\colon B \to \mathrm{Kokern}(f)$ wird bei f^* auf Null bgebildet. Also gibt es ein $\alpha\colon C \to \mathrm{Kokern}(f)$, für das $\alpha g = \beta$ gilt. Wegen $\mathrm{Bild}(f) \subset \mathrm{Kern}(g)$ gibt es aber auch ein $\alpha'\colon \mathrm{Kokern}(f) \to C$, so daß $\alpha'\beta = g$ ist. Es folgt $\alpha\alpha'\beta = \beta$ und $\alpha'\alpha g = g$. Da β und g surjektiv sind, folgt $\alpha\alpha' = \mathrm{id}$ und $\alpha'\alpha = \mathrm{id}$. Der Isomorphismus α zeigt uns: $\mathrm{Kern}(g) \subset \mathrm{Bild}(f)$. Damit ist die Exaktheit an der Stelle B gezeigt. □

Es gibt eine analoge Exaktheitseigenschaft für die erste Veränderliche.

(3.2) Satz. *Sei R ein kommutativer Ring und $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ eine Sequenz von R-Moduln. Diese Sequenz ist genau dann exakt, wenn für jeden R-Modul N die induzierte Sequenz*

$$0 \to \mathrm{Hom}(N, A) \xrightarrow{f_*} \mathrm{Hom}(N, B) \xrightarrow{g_*} \mathrm{Hom}(N, C)$$

exakt ist. □

(3.3) Bemerkung. Die Kommutativität von R wird in (3.1) und (3.2) nicht benutzt. Im allgemeinen Fall sind jedoch die Hom-Mengen keine R-Moduln sondern nur abelsche Gruppen. ◇

(3.4) Das Fünfer-Lemma. *Das Diagramm*

$$\begin{array}{ccccccccc}
M_1 & \xrightarrow{a_1} & M_2 & \xrightarrow{a_2} & M_3 & \xrightarrow{a_3} & M_4 & \xrightarrow{a_4} & M_5 \\
\downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \downarrow{\scriptstyle f_4} & & \downarrow{\scriptstyle f_5} \\
N_1 & \xrightarrow{b_1} & N_2 & \xrightarrow{b_2} & N_3 & \xrightarrow{b_3} & N_4 & \xrightarrow{b_4} & N_5
\end{array}$$

aus R-Moduln und linearen Abbildungen sei kommutativ und habe exakte Zeilen.

(1) *Sind f_2, f_4 surjektiv und f_5 injektiv, so ist f_3 surjektiv.*
(2) *Sind f_2, f_4 injektiv und f_1 surjektiv, so ist f_3 injektiv.*
(3) *Sind f_1, f_2, f_4, f_5 bijektiv, so ist f_3 bijektiv.*

Beweis. Der Beweis besteht in einer sogenannten „Diagrammjagd“: Einzelne Elemente werden im Diagramm herumgejagt, bis sie vor Erschöpfung den gewünschten Nachweis liefern. Wir führen den Beweis für (1); derjenige für (2) verläuft analog, und (3) ist eine Folge von (1) und (2).

Sei $y_3 \in N_3$ gegeben. Es gibt $x_4 \in M_4$ mit $f_4(x_4) = b_3(y_3)$. Da $f_3a_4(x_4) = b_4f_4(x_4) = b_4b_3(y_3) = 0$ ist und f_5 injektiv, ist $a_4(x_4 = 0$ und folglich gibt es x_3 mit $a_3(x_3) = x_4$. Es gilt $b_3f_3(x_3) = f_4a_3(x_3) = f_4(x_4) = b_3(y_3)$. Demnach gibt es

ein $y_2 \in N_2$ mit $b_2(y_2) = y_3 - f_3(x_3)$, und da f_2 surjektiv ist, gibt es $x_2 \in M_2$ mit $f_2(x_2) = y_2$. Für das Element $x_3 - a_2(x_2)$ gilt somit

$$\begin{aligned} f_3(x_3 + a_2(x_2)) &= f_3(x_3) + f_3a_2(x_2) \\ &= f_3(x_3) + b_2f_2(x_2) \\ &= f_3(x_3) + b_2(y_2) \\ &= f_3(x_3) + y_3 - f_3(x_3) \\ &= y_3. \end{aligned}$$

Folglich liegt y_3 im Bild von f_3, und damit ist f_3 als surjektiv erkannt. □

(3.5) Kern-Kokern-Lemma. *Seien $f\colon A \to B$ und $g\colon B \to C$ lineare Abbildungen. Dann gibt es eine kanonische exakte Sequenz*

$$0 \to \operatorname{Kern} f \to \operatorname{Kern} gf \xrightarrow{\beta} \operatorname{Kern} g \xrightarrow{\partial} \operatorname{Kokern} f \xrightarrow{\gamma} \operatorname{Kokern} gf \to \operatorname{Kokern} g \to 0.$$

Beweis. Wir beschreiben zunächst die Abbildungen in der Sequenz. Die zweite ist eine Inklusion, die dritte wird durch f und die fünfte wird durch g induziert. Die sechste ist eine Faktorabbildung. Die vierte ist auf Repräsentanten die Identität. Wir weisen nur die Exaktheit an den mit ∂ beteiligten Stellen nach.

Ist $g(x) = 0$ und $\partial x = 0$, so gibt es y mit $x = f(y)$. Es ist dann $y \in \operatorname{Kern} gf$ und $\beta(y) = x$. Die Gleichung $\partial\beta = 0$ folgt unmittelbar aus den Definitionen.

Wir verwenden für Restklassen und ihre Repräsentanten dieselben Symbole. Sei $\gamma(z) = 0$. Dann liegt $g(z)$ im Bild von gf, etwa $g(z) = gf(a)$. Folglich liegt $u = z - f(a)$ im Kern von g und im Kokern von f gilt $\partial(u) = z$. Die Relation $\gamma\partial = 0$ folgt wieder unmittelbar aus den Definitionen. □

(3.6) Das Dreimaldrei-Lemma. *Gegeben sei ein kommutatives Diagramm von R-Moduln und linearen Abbildungen*

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & C_1 & \xrightarrow{\gamma_1} & C_2 & \xrightarrow{\gamma_2} & C_3 & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

(1) *Sind alle Spalten exakt und die beiden letzten Zeilen, so ist auch die erste Zeile exakt.*

(2) *Sind alle Spalten exakt und die erste und dritte Zeile, und gilt $\beta_2\beta_1 = 0$, so ist auch die mittlere Zeile exakt.*

BEWEIS. (1) Das Fünfer-Lemma zeigt, daß α_1 injektiv und α_2 surjektiv ist. Das Diagramm zeigt fast unmittelbar, daß $\alpha_2\alpha_1 = 0$ ist. Jetzt wird das Fünfer-Lemma auf die durch $\alpha_2, \beta_1, \gamma_2$ induzierte Abbildung der Kokerne von $\alpha_1, \beta_1, \gamma_1$ nach A_3, B_3, C_3 angewendet.
(2) analog wie (1) durch Zurückführung auf das Fünfer-Lemma. □

(3.7) Aufgaben und Ergänzungen.

1. Man belege durch ein Beispiel, daß auf die Voraussetzung $\beta_2\beta_1 = 0$ in (3.6.2) nicht verzichtet werden kann, wenn auf die Exaktheit der mittleren Zeile geschlossen werden soll.
2. Ein Modul N heißt *projektiv*, wenn für jede Surjektion $g\colon B \to C$ auch $g_*\colon \mathrm{Hom}(N, B) \to \mathrm{Hom}(N, C)$ surjektiv ist. Ein Modul N heißt *injektiv*, wenn für jede Injektion $f\colon A \to B$ die Abbildung $f^*\colon \mathrm{Hom}(B, N) \to \mathrm{Hom}(A, N)$ surjektiv ist. Daraus folgt: Für einen projektiven Modul N werden bei Anwendung von $\mathrm{Hom}(N, ?)$ beliebige exakte Sequenzen wieder in exakte Sequenzen überführt. Für einen injektiven Modul N transformiert $\mathrm{Hom}(?, N)$ exakte Sequenzen wieder in exakte. Ein freier Modul ist projektiv. Ein direkter Summand eines projektiven Moduls ist projektiv. Ein projektiver Modul ist direkter Summand eines geeigneten freien.

4 Moduln über Hauptidealringen

Dieser Abschnitt ist der Strukturbeschreibung der endlich erzeugten Moduln über einem Hauptidealring gewidmet. Wenn nichts anderes gesagt wird, ist R ein Hauptidealring. Wir formulieren zunächst zwei Hauptsätze. Die Aussagen und ihre Beweise sind völlig analog zu den entsprechenden über endlich erzeugte abelsche Gruppen.

(4.1) Struktursatz. *Jeder endlich erzeugte R-Modul M ist zu einem Modul der folgenden Form isomorph:*

$$R^t \oplus R/(d_1) \oplus \cdots \oplus R/(d_k).$$

Dabei können die Elemente $d_i \in R \setminus \{0\}$ zusätzlich der Teilbarkeitsrelation $d_1|d_2|\ldots|d_k$ unterworfen werden. Die Zahl t und die Ideale $(d_1), \ldots, (d_k)$ mit der Bedingung $(d_1) \supset \ldots \supset (d_k)$ sind durch M eindeutig bestimmt.

(4.2) Basissatz. *Sei M ein endlich erzeugter freier R-Modul und N ein Untermodul. Dann gibt es eine Basis $e_1, \ldots, e_n$ von M und Elemente $d_1, \ldots, d_k$ mit $d_1|\ldots|d_k$ aus R derart, daß $f_1 = d_1e_1, \ldots, f_k = d_ke_k$ eine Basis von N ist.*

Die Beweise beruhen auf dem Normalformensatz für Matrizen mit Einträgen aus R und der Existenz einer Basis in einem Untermodul eines freien Moduls.

(4.3) Satz. *Sei N Untermodul eines freien Moduls vom Rang n. Dann ist N frei vom Rang höchstens n.*

BEWEIS. Wörtlich genauso wie für I(4.1) im Fall der Gitter. □

(4.4) Folgerung. *Sei M ein R-Modul, der von n Elementen erzeugt wird. Dann wird jeder Untermodul N von höchstens n Elementen erzeugt.*

BEWEIS. Die Voraussetzung besagt: Es existiert eine surjektive R-lineare Abbildung $f\colon F \to M$ eines freien Moduls F mit einer Basis von n Elementen. Dann ist $f^{-1}N$ frei und hat nach dem Beweis von (4.3) eine Basis von k Elementen, wobei $k \leq n$ ist. Also wird $N = f(f^{-1}N)$ von k Elementen erzeugt. □

Wir betrachten die Menge $M(m,n;R)$ der (m,n)-Matrizen $(a_{ij} \mid 1 \leq i \leq m,\ 1 \leq j \leq n)$ mit Eintragungen a_{ij} aus dem Ring R. Zwei solche Matrizen werden komponentenweise addiert, und die Multiplikation von Matrizen wird nach der bekannten Formel definiert. Diese Addition und Multiplikation machen die Menge $M_n(R)$ der (n,n)-Matrizen über R zu einem Ring. Mit Hilfe der Cramerschen Regel wird bewiesen, daß eine Matrix $A \in M_n(R)$ genau dann invertierbar ist, wenn ihre Determinante in R^* liegt. Die Determinante $\det(A) \in R$ von $A \in M_n(R)$ wird nach der Leibnizschen Formel definiert:

$$\det A = \sum_{\sigma \in S(n)} \operatorname{sign}(\sigma) a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)}.$$

Die bekannten Rechenregeln über Determinanten gelten immer noch, nämlich der Produktsatz und die Formel für die Entwicklung nach Zeilen und Spalten.

Wir wollen im folgenden wieder das grobe Normalformenproblem für Matrizen aus $M(m,n;R)$ behandeln. Dazu definieren wir: $U, V \in M(m,n;R)$ heißen *äquivalent*, wenn mit geeigneten $A \in GL(m,R)$ und $B \in GL(n,R)$ eine Gleichung $U = AVB$ gilt. Dadurch wird eine Äquivalenzrelation definiert.

(4.5) Satz. *Sei R ein Hauptidealring. Eine Matrix $U \in M(m,n;R)$ ist zu einer Diagonalmatrix* $\operatorname{Dia}(d_1,\ldots,d_r,0,\ldots,0)$ *äquivalent, in der $d_i \neq 0$ ist und $d_i | d_{i+1}$ für $1 \leq i < r$.*

BEWEIS. Wörtlich wie der erste Beweis derselben Aussage über ganzzahlige Matrizen in I.3. □

Beweis von (4.2). Nach (4.3) hat N eine Basis. Wir schreiben diese Basis als Linearkombination einer Basis von M und bringen die resultierende Matrix nach dem letzten Satz auf Normalform. Die Transformationsmatrizen werden wie in der Vektorraumtheorie als Basiswechselmatrizen interpretiert. □

Basen mit den in (4.2) genannten Eigenschaften heißen der Inklusion $N \subset M$ oder dem Paar (M,N) *angepaßt*.

Beweis von (4.1). Wir wählen eine R-lineare Surjektion $p\colon F \to M$ eines freien, endlich erzeugten R-Moduls F auf M. Sei $K \subset F$ der Kern von p. Dann ist also M isomorph zu F/K. Wir wählen nach (4.2) angepaßte Basen $e_1,\ldots,e_n$ von F und $f_1,\ldots,f_k$ von K. Durch diese Basen werden Isomorphismen $\alpha\colon R^k \to K$ und

$\beta\colon R^n \to F$ geliefert (Standardbasis $\leftrightarrow$ Basis). Wir erhalten ein kommutatives Diagramm

$$\begin{array}{ccccc} K & \longrightarrow & F & \xrightarrow{p} & M \\ \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle\beta} & & \uparrow{\scriptstyle\gamma} \\ R^k & \xrightarrow{i} & R^n & \xrightarrow{q} & L, \end{array}$$

worin $i(\lambda_1,\dots,\lambda_k) = (\lambda_1 d_1,\dots,\lambda_k d_k, 0,\dots,0)$ und q die kanonische Abbildung auf den Kokern L von i ist. Dieser Kokern hat die in (4.1) behauptete Gestalt.

Die Eindeutigkeit der Darstellung wird später im Abschnitt über äußere Potenzen von Moduln bewiesen. □

Ist R ein beliebiger Ring, so heißt ein Element x eines R-Moduls M *Torsionselement*, wenn es ein $r \in R \setminus 0$ gibt, das x *annulliert*: $rx = 0$. Ein Modul heißt *Torsionsmodul*, wenn er nur Torsionselemente enthält, er heißt *torsionsfrei*, wenn $M \setminus 0$ keine Torsionselemente enthält.

Fassen wir eine abelsche Gruppe als $\mathbb{Z}$-Modul auf, so sind die Torsionselemente darin die Elemente endlicher Ordnung.

(4.6) Satz. *Sei M ein R-Modul. Dann gilt:*

(1) *Die Menge M_t der Torsionselemente von M ist ein Untermodul. Der Quotient M/M_t ist torsionsfrei.*

(2) *Ein endlich erzeugter torsionsfreier R-Modul M ist frei.*

Beweis. (1) Aus $x_1, x_2 \in M_t$, $r_1, r_2 \in R \setminus 0$, $r_1x_1 = 0 = r_2x_2$ folgt $r_1r_2(x_1 + x_2) = 0$. Also ist $x_1 + x_2 \in M_t$. Analog: $x \in M_t$, $r \in R$ impliziert $rx \in M_t$.

Sei $x \in M/M_t$ die Restklasse von $z \in M$. Sei $rx = 0$, also $rz \in M_t$, also $srz = 0$ für ein $s \in R \setminus 0$. Es ist $sr \neq 0$, da R keine Nullteiler hat. Also ist $z \in M_t$ und damit x die Nullrestklasse.

(2) Sei M von $\{y_1,\dots,y_m\}$ erzeugt und $\{v_1,\dots,v_n\} \subset \{y_1,\dots,y_m\}$ eine maximale linear unabhängige Teilmenge. Zu jedem y_i gibt es ein $\lambda_i \in R \setminus 0$ derart, daß $\lambda_i y_i \in [v_1,\dots,v_n]$. Das ist klar, falls $y_i = v_j$ für ein j, und für die anderen y_i folgt es, weil $\{v_1,\dots,v_n\}$ maximal linear unabhängig ist. Wir setzen $\lambda = \lambda_1\lambda_2\dots\lambda_m$. Dann gilt $\lambda M \subset [v_1,\dots,v_n]$. Der Untermodul λM des freien Moduls $[v_1,\dots,v_n]$ ist frei. Da M torsionsfrei ist, ist die Abbildung $M \to \lambda M$, $x \mapsto \lambda x$ ein Isomorphismus. □

In dem Modul in (4.1) ist die Summe der $R/(d_j)$ der Torsionsuntermodul. Im allgemeinen läßt sich ein Modul der Form $R/(d)$ noch weiter in eine direkte Summe zerlegen. Das beschreiben wir nun.

Sei $\alpha \in R$ und M ein R-Modul. Wir definieren zwei zugehörige Untermoduln:

$$\textbf{(4.7)} \qquad M(\alpha) = \{m \in M \mid \alpha m = 0\}.$$

$$\textbf{(4.8)} \qquad M_\alpha = \{m \in M \mid \text{ es gibt } n \in \mathbb{N} \text{ mit } \alpha^n m = 0\}.$$

Für jeden Untermodul N gilt $N_\alpha = N \cap M_\alpha$. Ist $p \in R$ ein Primelement, so

heißt M p-Modul oder *p-primär*, wenn $M = M_p$ ist. Wir notieren die folgenden Regeln, die unmittelbar aus den Definitionen folgen:

(4.9) Für $\alpha|\beta$ gilt $M(\alpha) \subset M(\beta)$.

(4.10) Für je zwei Elemente $\alpha, \beta \in R$ gilt $M(\alpha\beta) \cap M_\beta = M(\alpha\beta)_\beta$.

(4.11) $M(\alpha) \subset M_\alpha$.

(4.12) Satz. *Seien $\alpha, \beta \in R \setminus 0$. Wir wählen einen* GGT *δ und ein* KGV *γ von α, β, so daß $\alpha\beta = \gamma\delta$ gilt. Dann gilt*

$$M(\alpha) + M(\beta) = M(\gamma), \quad M(\alpha) \cap M(\beta) = M(\delta).$$

Es gibt also eine exakte Sequenz

$$0 \to M(\delta) \to M(\alpha) \oplus M(\beta) \to M(\gamma) \to 0.$$

Sind α und β teilerfremd, so gilt $M(\alpha) \oplus M(\beta) = M(\gamma)$; in diesem Fall hat die Projektion $M(\gamma) \to M(\alpha)$ auf den direkten Summanden $M(\alpha)$ die Form $x \mapsto rx$ für ein geeignetes $r \in R$.

Beweis. Wir setzen $\alpha = \delta\alpha'$ und $\beta = \delta\beta'$. Wegen $\alpha\beta = \gamma\delta$ ist dann $\gamma = \alpha'\beta = \alpha\beta'$. Wir wählen eine Darstellung $1 = \mu\alpha' + \lambda\beta'$, die dann $\delta = \mu\alpha + \lambda\beta$ impliziert. Sei $x \in M(\gamma)$. Es ist $x = 1 \cdot x = \mu\alpha' x + \lambda\beta' x$. Wegen $\beta\alpha' = \gamma$ ist $\beta(\mu\alpha' x) = \mu\gamma x = 0$, also $\mu\alpha' x \in M(\beta)$; und wegen $\alpha\beta' = \gamma$ ist $\lambda\beta' x \in M(\alpha)$. Folglich ist $x \in M(\alpha) + M(\beta)$.

Sei $x \in M(\alpha) \cap M(\beta)$. Aus $\alpha x = 0 = \beta x$ folgt dann $\delta x = (\mu\alpha + \lambda\beta)x = 0$ und damit $x \in M(\delta)$.

Aus (4.9) folgt $M(\delta) \subset M(\alpha)$ und $M(\delta) \subset M(\beta)$, also die umgekehrte Inlusion $M(\delta) \subset M(\alpha) \cap M(\beta)$. Ist $\delta = 1$, so ist die Projektion $M(\gamma) \to M(\alpha)$ durch $x \mapsto \lambda\beta x$ gegeben. □

(4.13) Satz. *Seien α und β teilerfremd. Dann gilt:*

$$M(\beta) = M(\alpha\beta) \cap M_\beta = M(\alpha\beta)_\beta.$$

Beweis. Die rechte Gleichheit gilt für je zwei Elemente $\alpha, \beta \in R$. Zur linken: Aus $M(\beta) \subset M_\beta$ und $M(\beta) \subset M(\alpha\beta)$ folgt $M(\beta) \subset M(\alpha\beta) \cap M_\beta$. Nach (4.12) gilt $M(\alpha) \oplus M(\beta) = M(\alpha\beta)$. Wir setzen ein Element von $M(\alpha\beta)$ deshalb in der Form $x + y$ mit $x \in M(\alpha)$ und $y \in M(\beta)$ an. Werde $x + y$ durch β^m annulliert. Dann werden auch x und y durch β^m annulliert (direkte Summe!). Da α, β teilerfremd sind, so auch α, β^m. Deshalb gibt es eine Darstellung der Form $\lambda\beta^m + \mu\alpha = 1$. Es folgt $x = \lambda\beta^m x + \mu\alpha x = 0$, da $\beta^m x = 0$ ist und $x \in M(\alpha)$. Also liegt $x + y = y$ in $M(\beta)$. □

(4.14) Satz. *Sei M ein Torsionsmodul über R. Sei P die Menge der maximalen Ideale von R, also der von Primelementen erzeugten Hauptideale. Dann ist M die direkte Summe der M_p für $(p) \in P$.*

BEWEIS. Da M ein Torsionsmodul ist, liegt jedes $x \in M$ in einem geeigneten $M(\alpha)$, $\alpha \in R \setminus 0$. Sei $\alpha = u \prod_{i=1}^{r} p_i^{n(i)}$ eine Zerlegung in Primfaktoren p_i und eine Einheit u. Da $p_i^{n(i)}$ teilerfremd zu $\prod_{j \neq i} p_j^{n(j)}$ ist, folgt aus (4.12) durch vollständige Induktion nach r, daß $M(\alpha)$ direkte Summe der Untermoduln $M(p_i^{n(i)})$ ist. Wegen $M(p_i^{n(i)}) \subset M_{p_i}$ ist also $x \in M(\alpha)$ in der Summe der M_p enthalten.

Sei nun $\sum_{(p) \in P} x_p = 0$, $x_p \in M_p$, fast alle x_p gleich Null. Für ein $x_p \neq 0$ gibt es ein $n(p) \in \mathbb{N}$, so daß $x_p \in M(p^{n(p)})$. Wegen $\bigoplus M(p^{n(p)}) = M(\prod p^{n(p)})$ folgt aus (4.12), daß alle $x_p = 0$ sind. Aus (2.6) folgt die Behauptung. □

Der direkte Summand M_p in (4.14) heißt *p-primäre Komponente* von M, die zugehörige direkte Zerlegung die *Primärzerlegung* des Moduls. Ist M in (4.14) endlich erzeugt, so gibt es nur endlich viele von Null verschiedene primäre Komponenten von M. Die Projektion $M \to M_p$ hat in diesem Fall die Form $x \mapsto r_p x$ für ein geeignetes $r_p \in R$.

Ein R-Modul M heißt *zyklisch*, wenn er von einem Element erzeugt wird. Sei $x \in M$ ein erzeugendes Element. Dann ist $R \to M$, $r \mapsto rx$ surjektiv. Der Kern ist ein Hauptideal (d). Zyklische Moduln sind also isomorph zu solchen der Form $R/(d)$. Die kleinsten derartigen Moduln sind die primären. Wir wenden (4.12) bzw. (4.14) auf einen Modul $R/(d)$ an. Sei $d = p_1^{n(1)} \dots p_r^{n(r)}$ eine Zerlegung in Primfaktoren. Dann haben wir einen Isomorphismus

$$R/(d) \cong \bigoplus_{j=1}^{r} R/(p_j^{n(j)}),$$

der übrigens auch aus dem chinesischen Restsatz folgt. Wir verwenden derartige Zerlegungen in (4.1). Das liefert die Existenzaussage im nächsten Satz.

(4.15) Satz. *Sei M ein endlich erzeugter Torsionsmodul. Dann ist M die direkte Summe von primären zyklischen Moduln. Die Anzahl der Summanden, die zu $R/(p^t)$ isomorph sind, ist durch M eindeutig bestimmt.*

BEWEIS. Es bleibt die Eindeutigkeit zu zeigen. Das geschieht wie bei den analogen Aussagen über endliche abelsche Gruppen. Sei eine direkte Zerlegung in zyklische Primärmoduln gegeben und $a(t)$ die Anzahl der zu $R/(p^t)$ isomorphen Summanden. Wir setzen $b(t) = \sum_{k \geq t} a(k)$. Dann ist $M(p)$ ein Vektorraum über dem Körper $R/(p)$ der Dimension $b(1)$. Die entsprechende Dimension von $M(p^2)/M(p)$ ist $b(2)$ etc. Also sind $b(t)$ und $a(t)$ aus der Modulstruktur berechenbar. □

5 Algebren

Wir stellen einen weiteren Grundbegriff bereit, der im weiteren gebraucht wird. Das Distributivgesetz, das die Addition und Multiplikation miteinander verbindet, besagt, daß die Multiplikation $(a, b) \mapsto ab$ bilinear, oder besser, biadditiv ist. Im Rahmen der Modultheorie liegt es nahe, wirklich bilineare Multiplikationen zu betrachten.

Sei also R ein kommutativer Ring und A ein R-Modul. Eine bilineare Abbildung $m\colon A \times A \to A$ heißt *Multiplikation* auf A und das Paar (A, m) heißt *R-Algebra* (Plural: *Algebren*).

Wie üblich verlangt man von der Multiplikation meist noch weitere Eigenschaften. Sie heißt *assoziativ*, wenn immer $m(a, m(b, c)) = m(m(a, b), c)$ gilt und *kommutativ*, wenn immer $m(a, b) = m(b, a)$ gilt. Ein *Einselement* $1 \in A$ für die Multiplikation ist durch die Eigenschaften $m(1, a) = a = m(a, 1)$ gekennzeichnet. Einmal formal definiert, kehren wir natürlich meist zur gewohnten Notation $m(a, b) = ab$ für die Multiplikation zurück. Ein Homomorphismus $f\colon A \to B$ der R-Algebra A in die R-Algebra B ist eine R-lineare Abbildung f, die mit den Multiplikationen verträglich ist, $f(ab) = f(a)f(b)$. Falls die Algebren beide Einselemente haben, wird meistens verlangt, daß auch $f(1) = 1$ gilt; von selbst ist das leider nicht richtig.

Im folgenden seien, solange nichts anderes gesagt wird, Algebren assoziativ mit Einselement und Homomorphismen von Algebren sollen 1 auf 1 abbilden.

Wir geben einige einfache Beispiele. Fassen wir die additive Gruppe eines Ringes als $\mathbb{Z}$-Modul auf, so ist in dieser Terminologie ein Ring im wesentlichen dasselbe wie eine assoziative $\mathbb{Z}$-Algebra mit Einselement. Die (n, n)-Matrizen über dem kommutativen Ring R bilden eine R-Algebra $M_n(R)$, die R-Modulstruktur ist die Übliche: Skalarmultiplikation jedes Matrixeintrags. Ist R kommutativ und M ein R-Modul, so ist der Endomorphismenring $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ sogar eine R-Algebra. Sei R Unterring des Ringes S. Dann wird S durch Linksmultiplikation mit Elementen aus R zu einem R-Modul, und die Multiplikation von S ist damit R-bilinear.

Typische und wichtige Beispiele von Algebren sind die *Monoidalgebren* und ihre Spezialfälle die *Gruppenalgebren* und *Polynomalgebren*.

Sei R ein kommutativer Ring und M ein multiplikatives Monoid. Wir bezeichnen mit RM oder $R[M]$ den freien R-Modul über der Menge M. Eine bilineare Abbildung $m\colon RM \times RM \to RM$ läßt sich einduetig dadurch definieren, daß ihr Wert auf Paaren (x, y) von Basiselementen $x, y \in M$ spezifiziert wird. Wir definieren m durch die Monoidmultiplikaton $m(x, y) = xy$. Da die Monoidmultiplikation assoziativ ist, so ist auch m assoziativ. Das neutrale Element von M wird das Einselement der Algebra RM.

Das additive Monoid der natürlichen Zahlen $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ schreiben wir in multiplikativer Form durch Potenzschreibweise $M = \{1 = x^0, x = x^1, x^2, \ldots\}$ mit der Multiplikaton $x^m x^n = x^{m+n}$. Elemente in RM sind dann endliche formale Linearkombinationen der Gestalt $r_0 + r_1 x + \cdots + r_n x^n$, $r_j \in R$. Wir bezeichnen die damit gewonnene Monoidalgebra mit $R[x]$ und nennen sie die *Polynomalgebra* in einer *Unbestimmten* x über R. Die Elemente von $R[x]$ heißen *Polynome* mit Koeffizienten in R. Ein Polynom ist keine Funktion, sondern ein formales Objekt, das durch seine Koeffizienten eindeutig bestimmt ist. Gerechnet wird mit Polynomem nach den üblichen Regeln des „Buchstabenrechnens“.

In ähnlicher Weise werden Polynomalgebren in mehreren Unbestimmten definiert. So wird $R[x, y]$ aus dem multiplikativen Monoid $\{x^i y^j \mid i, j \in \mathbb{N}_0\}$ mit der

Multiplikation $x^iy^j \cdot x^ky^l = x^{i+k}y^{j+l}$ gewonnen.

Eine Monoidalgebra $R[M]$ hat die folgende *universelle Eigenschaft*: Sei A eine beliebige R-Algebra und $\varphi\colon M \to A$ ein Homomorphismus von M in das multiplikative Monoid der Algebra A. Dann gibt es genau einen Homomorphismus $\Phi\colon R[M] \to A$ von R-Algeben, der auf den Basiselementen mit φ übereinstimmt, denn die eindeutige R-lineare Erweiterung von φ ist ein Homomorphismus von Algebren.

Für Polynomalgebren stellt sich die *universelle Eigenschaft* noch etwas anders dar: Die Monoidhomomorphismen von $\{x^0, x^1, x^2, \ldots\}$ sind eindeutig durch den Wert auf x bestimmet, und dieser Wert läßt sich auch beliebig vorgeben. Also entsprechen die Algebrahomomorphismen $\Phi\colon R[x] \to A$ umkehrbar eindeutig den Elementen von A vermöge $\Phi \mapsto \Phi(x)$. Ist zum Beispiel $A = R$ und $\Phi(x) = u \in R$, so wird der zugehörige Homomorphismus *Einsetzen* von u in Polynome genannt. Auf diese Weise wird jedem Polynom $f \in R[x]$ eine Funktion $R \to R$ zugeordnet, die wir in üblicher Notation $u \mapsto f(u)$ schreiben. Statt f wird deshalb auch $f(x)$ geschrieben, denn für A können wir auch $R[x]$ verwenden und somit Polynome in Polynome einsetzen. Das entspricht der Verkettung der Funktionen.

Ein *Linksmodul* M über einer R-Algebra A ist ein R-Linksmodul M zusammen mit einer R-bilinearen Skalarmultiplikation $A \times M \to M$. Homomorphismen $f\colon M \to N$ von A-Moduln sind dann R-lineare Abbildungen f, die mit der Skalarmultiplikation verträglich sind.

Wir beschreiben nun das Verhältnis von Ringen zu Algebren. Vergessen wir in einer R-Algebra A die R-Modulstruktur und behalten nur die Addition und Multiplikation, so bleibt ein Ring übrig. Eine R-Algebra ist also ein Ring mit Zusatzstruktur. Welcher?

Sei A eine R-Algebra. Wir bezeichnen die Skalarmultiplikation des R-Moduls A durch einen Punkt $x \cdot a$. Die Bilinearität der Multiplikation besagt unter anderem $(x \cdot a)(y \cdot b) = xy \cdot ab$. Insbesondere ist $e\colon R \to A$, $x \mapsto x \cdot 1_A$ ein Ringhomomorphismus. Dieser erfüllt $x \cdot a = x \cdot (1_A a) = (x \cdot 1_A)a = e(x)a$. Wegen $(x \cdot a)b = x \cdot (ab) = a(x \cdot b)$ ist $e(x)$ mit allen Ringelementen vertauschbar, d. h. $e\colon R \to A$ ist ein Homomorphismus in das *Zentrum* $Z(A) = \{x \in A \mid \forall a \in A\, xa = ax\}$ des Ringes A.

Ist umgekehrt A ein Ring und $\varepsilon\colon R \to A$ ein Homomorphismus in das Zentrum, so wird durch $R \times A \to A$, $(x, a) \mapsto x \cdot a = \varepsilon(x)a$ die additive Gruppe A zu einem R-Modul, und damit ist die Multiplikation von A R-bilinear.

Diese beiden Prozesse sind zueinander invers. Damit haben wir:

(5.1) Notiz. *R-Algebren A entsprechen umkehrbar eindeutig Ringen A zusammen mit einem Ringhomomorphismus $e_A\colon R \to A$ in das Zentrum von A.* □

Bei dieser Entsprechung sind Homomorphismen von Algebren dasselbe wie Ringhomomorphismen $f\colon A \to B$, die $fe_A = e_B$ erfüllen. Ist M ein Modul über der R-Algebra A, so gilt für $x \in R$ und $m \in M$ und der R-Modulstruktur $(x, m) \mapsto x * m$ auf M

$$e(x)m = (x \cdot 1_A)m = x * (1_A m) = x * m,$$

d. h. die A-Modulstruktur zusammen mit e bestimmt die R-Modulstruktur.

Die vorstehenden Überlegungen erwecken vielleicht den Eindruck, als sei es überflüssig, Algebren überhaupt als Begriff einzuführen. Der Vorteil dieser Begriffsbildung springt bei den wichtigen Algebren über Körpern $R = K$ ins Auge. Dann ist zum einen $e\colon K \to A$ injektiv, und wir betrachten damit ohne wesentliche Einschränkung K als Teilkörper im Zentrum von A. Zum anderen sind alle Moduln K-Vektorräume und die Linksmultiplikationen mit Elementen von A sind K-lineare Abbildungen, so daß wir uns in der vertrauten Welt der linearen Algebra befinden.

Ein Modul über $K[x]$ etwa ist dasselbe wie ein K-Vektorraum V zusammen mit einem Endomorphismus von V, der der Skalaroperation von x entspricht. Dieser Gesichtspunkt wird im sechsten Kapitel ausgenutzt.

Ein Modul über einem Gruppenring KG der Gruppe G ist dasselbe wie ein K-Vektorraum V zusammen mit einem Homomorphismus von G in die lineare Gruppe $GL(V)$. Diese Objekte heißen *Darstellungen* von G.

Wichtige Beispiele für Algebren, die nicht assoziativ sind, findet man in den sogenannten Lie-Algebren. Wir erwähnen sie nur am Rande. In Fall der Lie-Algebren schreibt man die Multiplikation meist als *Lie-Klammer* $(a, b) \mapsto [a, b]$. Eine *Lie-Algebra* liegt vor, wenn die so geschriebene Multiplikation die *Jacobi-Identität*

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$$

erfüllt (Merkregel: zyklische Vertauschung). Ist A eine assoziative R-Algebra, so definieren wir eine neue Verknüpfung durch

$$[a, b] = ab - ba.$$

Eine leichte Rechnung zeigt, daß die Jacobi-Identität gilt. Die so gewonnenen Lie-Algebren sind besonders wichtig, wenn sie aus $M(n, n; R)$ oder Unteralgebren entstehen, weil sie die infinitesimale Struktur der Matrizengruppen (Lie-Gruppen) beschreiben.

(5.2) Beispiel. Der Vektorraum $\mathbb{R}^3$ ist zusammen mit dem Vektorprodukt $(x, y) \mapsto x \times y$ eine Lie-Algebra (über $\mathbb{R}$). Diese Lie-Algebra ist isomorph zur Algebra der schiefsymmetrischen reellen $(3, 3)$-Matrizen mit der Lie-Klammer $[A, B] = AB - BA$. Ein Isomorphismus wird durch

$$(x, y, z) \mapsto \begin{pmatrix} 0 & -z & y \\ z & 0 & -x \\ -y & x & 0 \end{pmatrix}$$

gegeben. ◇

6 Der Satz von Jordan-Hölder

Wir betrachten A-Linksmoduln über einem beliebigen Ring A. Ein A-Modul M heißt *einfach*, wenn er von Null verschieden ist und nur die Untermoduln 0 und

M hat. Eine Sequenz

$$M = M_0 \supset M_1 \supset \ldots \supset M_r = 0$$

von Untermoduln M_j eines Moduls M heißt *Kompositionsreihe* von M, wenn alle Faktoren M_j/M_{j+1} einfach sind.

Zum Studium von Kompositionsreihen brauchen wir den folgenden *Isomorphiesatz von Zassenhaus*, den wir in gruppentheoretischer Form schon früher formuliert hatten.

(6.1) Satz. *Seien $V \subset U$ und $V' \subset U'$ Untermoduln eines Moduls. Dann gibt es kanonische Isomorphismen*

$$\frac{(U+V')\cap U'}{(V+V')\cap U'} \cong \frac{U\cap U'}{(U'\cap V)+(U\cap V')} \cong \frac{(U'+V)\cap U}{(V'+V)\cap U}.$$

Beweis. Der Kern der Abbildung

$$U\cap U' \xrightarrow{\subset} (U+V')\cap U' \longrightarrow (U+V')\cap U'/(V+V')\cap U'$$

ist gleich $X := (U\cap U')\cap((V+V')\cap U') = U\cap(V+V')\cap U'$. Es ist zu zeigen, daß X gleich $Y := U'\cap V + U\cap V'$ ist. Sei $x \in X$. Dann ist $x = v + v' \in V + V'$ und $x \in U \cap U'$, also

$$v = x - v' \in U\cap U' + V' \subset U', \qquad v \in V$$

und insgesamt $v \in U'\cap V$. Ebenso $v' \in U\cap V'$ und damit $x \in Y$.

Umgekehrt ist $U'\cap V \subset U$ und $U'\cap V \subset U'\cap(V+V')$, also $U'\cap V \subset X$. Ebenso $U\cap V' \subset X$ und damit $Y \subset X$. Der zweite Isomorphismus ergibt sich genauso. □

Auf das folgende Resultat wird unter dem Namen *Satz von Jordan-Hölder* verwiesen.

(6.2) Satz. *Seien zwei Sequenzen*

$$M = M_0 \supset M_1 \supset \ldots \supset M_r = 0, \quad M = M_0' \supset M_1' \supset \ldots \supset M_s' = 0$$

von Untermoduln gegeben. Dann lassen sich diese Sequenzen durch Dazwischenschalten weiterer Untermoduln zu Sequenzen gleicher Länge

$$M = L_0 \supset \ldots \supset L_n = 0, \quad M = L_0' \supset \ldots \supset L_n' = 0$$

so verfeinern, daß die Faktoren L_j/L_{j+1} bis auf Isomorphie eine Permutation der Faktoren L_i'/L_{i+1}' sind. Insbesondere haben je zwei Kompositionsreihen eines Moduls dieselbe Länge, und ihre Faktoren sind bis auf Permutation und Isomorphie gleich.

BEWEIS. Zwischen M_i und M_{i+1} setzen wir die Untermoduln

$$(M_{i+1} + M'_j) \cap M_i, \qquad j = 0, \dots s$$

und zwischen M'_i und M'_{i+1} die Untermoduln

$$(M'_{i+1} + M_j) \cap M'_i, \qquad j = 0, \dots, r.$$

Die Isomorphismen von Zassenhaus

$$\frac{(M_{i+1} + M'_j) \cap M_i}{(M_{i+1} + M'_{j+1}) \cap M_i} \cong \frac{(M'_{j+1} + M_i) \cap M'_j}{(M'_{j+1} + M_{i+1}) \cap M'_j}$$

liefern die Behauptung. □

Natürlich haben nicht alle Moduln eine Kompositionsreihe. Vielmehr gilt:

(6.3) Satz. *Folgende Aussagen über einen Modul M sind äquivalent:*

(1) *M hat eine Kompositionsreihe.*
(2) *Jede Sequenz von Untermoduln läßt sich zu einer Komposionsreihe verfeinern.*
(3) *Jede aufsteigende $M_0 \subset M_1 \subset M_2 \subset \dots$ und jede absteigende $N_0 \supset N_1 \supset N_2 \supset \dots$ Sequenz von Untermoduln ist schließlich konstant.*

BEWEIS. (3) $\Rightarrow$ (1). Sei $B \subset M$ ein Untermodul. Falls es keinen Untermodul $B_0 \subset B$ gibt, so daß B/B_0 einfach ist, so finden wir in B eine echt aufsteigende unendliche Sequenz von Untermoduln, was (3) widerspricht. Also gibt es eine Sequenz $M = N_0 \supset N_1 \supset \dots$, so daß N_i/N_{i+1} einfach ist. Sie muß abbrechen und liefert eine Kompositionsreihe.

(1) $\Rightarrow$ (2) gilt nach dem vorigen Satz.

(2) $\Rightarrow$ (3). Sei $M_0 \subset M_1 \subset \dots$ eine aufsteigende Sequenz. Falls sie nicht schließlich konstant ist, gibt es wegen (2) Kompositionsreihen beliebig großer Länge, was dem vorigen Satz widerspricht. □

(6.4) Bemerkung. Den Isomorphiesatz von Zassenhaus haben wir früher schon im Kontext der Gruppentheorie formuliert. Eine Sequenz von Untergruppen

$$0 = G_n \lhd G_{n-1} \lhd \dots \lhd G_1 \lhd G_0 = G$$

heißt *Normalreihe* in der Gruppe G. Wie für (1.2) wird gezeigt, daß je zwei Normalreihen so verfeinert werden können, daß die sukzessiven Quotienten beider Verfeinerungen bis auf die Reihenfolge isomorph sind. Eine Gruppe G heißt *einfach*, wenn sie nur 1 und G als Normalteiler hat. Eine Normalreihe heißt *Kompositionsreihe*, wenn die sukzessiven Quotienten einfach sind. Es gilt die Eindeutigkeit der Kompositionsreihen im Sinne von (1.2). Ebenso läßt sich (1.3) übertragen. ◇

Sei M ein A-Modul und $x \in M$. Dann ist $m_x \colon A \to M$, $a \mapsto ax$ eine A-lineare Abbildung mit dem Kern $\mathrm{Ann}(x) = \{a \in A \mid a = 0\}$, dem *Annullator*

des Elementes x. Der Modul M ist genau dann einfach, wenn $\mathrm{Ann}(x)$ für jedes $x \in M \setminus 0$ ein maximales Linksideal von A ist. Ein Modul M ist genau dann einfach, wenn es zu je zwei Elementen $x, y \in M \setminus 0$ ein $a \in A$ mit $ax = y$ gibt.

Der Satz von Jordan-Hölder verallgemeinert den Satz von der eindeutigen Bestimmtheit der Länge einer Basis in Vektorräumen. Wir erläutern das am Beispiel von Moduln über Schiefkörpern.

Sei D ein Schiefkörper und M ein D-Modul mit einem endlichen Erzeugendensystem T. Der übliche Beweis der linearen Algebra ist auch in dieser Situation durchführbar und liefert: Eine maximale, linear unabhängige Teilmenge B von T ist eine Basis von M; ist S linear unabhängig in M, so läßt sich S zu einer Basis von M ergänzen. Also ist ein (endlicherzeugter) D-Modul frei. Hat eine Basis die Länge n, so ist M zu D^n isomorph. Da D ein einfacher D-Modul ist (als linksregulärer), so ist durch $M \cong D^n$ nach dem Satz von Jordan-Hölder n eindeutig durch M bestimmt. Jeder von Null verschiedene Vektor von D^n ist linear unabhängig und läßt sich zu einer Basis ergänzen. Sind deshalb x und y zwei von Null verschiedene Vektoren von D^n, so gibt es einen Isomorphismus von D^n, der x auf y abbildet. Der Endomorphismenring von D^n ist $M_n(D)$. Aus dem eben Gesagten folgt:

(6.5) Notiz. *Der $M_n(D)$-Modul D^n ist einfach.* □

Im linksregulären $M_n(D)$-Modul ist die Untergruppe S_k der Matrizen, die außerhalb der k-ten Spalte nur Nullen haben, ein Linksideal. Als Modul ist S_k isomorph zu D^n. Also gilt:

(6.6) Satz. *Der linksreguläre Modul $M_n(D)$ für einen Schiefkörper D ist direkte Summe von n einfachen, zu D^n isomorphen Untermoduln.* □

7 Kettenbedingungen

Wir betrachten Linksmoduln über einem Ring A. Wir sagen, der Modul M erfüllt die *absteigende Kettenbedingung* (die *Minimalbedingung*), wenn jede absteigende Kette von Untermoduln $M_1 \supset M_2 \supset \ldots$ von einer Stelle an konstant ist, d. h. wenn es ein n so gibt, daß $M_n = M_{n+k}$ für alle $k \geq 0$. Wir sagen, ein Modul M erfüllt die *aufsteigende Kettenbedingung* (die *Maximalbedingung*), wenn jede aufsteigende Kette von Untermoduln $M_1 \subset M_2 \subset \ldots$ schließlich konstant ist. Ein Modul mit Minimalbedingung heißt *artinsch* ein Modul mit Maximalbedingung heißt *noethersch*. Ein Ring heißt (links-)*artinsch* oder *noethersch*, wenn der linksreguläre Modul diese Eigenschaft hat. Eine kleine Überlegung zeigt:

(7.1) Notiz. *Ein Modul ist genau dann artinsch (noethersch), wenn jede nichtleere Menge von Untermoduln bezüglich Inklusion mindestens ein minimales (maximales) Element hat.* □

(7.2) Satz. *Sei $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ eine exakte Sequenz von A-Moduln. Dann gilt: M ist genau dann noethersch (artinsch), wenn M' und M'' noethersch (artinsch) sind.*

BEWEIS. Wir behandeln den noetherschen Fall; der artinsche ist analog. Eine aufsteigende Kette von Untermoduln von M' (oder M'') liefert vermöge α (oder β^{-1}) eine ebensolche in M und ist deshalb schließlich konstant. Sei umgekehrt $(L_n \mid n \geq 1)$ eine aufsteigende Kette in M. Dann sind $(\alpha^{-1}(L_n))$ und $(\beta(L_n))$ aufsteigende Ketten in M' und M''. Seien beide ab der Stelle k konstant. Mittels Exaktheit folgt sofort $L_k = L_{k+1}$. □

(7.3) Satz. *Ein Modul M ist genau dann noethersch, wenn jeder Untermodul endlich erzeugt ist.*

BEWEIS. Sei $(M_j \mid j \geq 1)$ eine aufsteigende Kette und N deren Vereinigung. Dann ist N endlich erzeugt und ein Erzeugendensystem etwa in M_k enthalten. Dann folgt aber $M_k = N$.

Sei N ein Untermodul und $\mathcal{U}$ die Menge der endlich erzeugten Untermoduln von N. Diese Menge ist nicht leer und hat deshalb ein maximales Element P. Ist $P \neq N$ und $x \in N \setminus P$, so ist $P + Ax$ echt größer als P und endlich erzeugt. Widerspruch. □

(7.4) Satz. *Sei A noethersch (artinsch) und M ein endlich erzeugter A-Modul. Dann ist M noethersch (artinsch).*

BEWEIS. Sei A noethersch. Nach (7.2) ist der Modul A^n noethersch und damit M als Quotient eines solchen. Analog im artinschen Fall. □

(7.5) Korollar. *Sei A noethersch (artinsch) und $I \subset A$ ein Ideal. Dann ist A/I noethersch (artinsch).* □

Wir haben schon früher gezeigt, daß ein Modul genau dann eine Kompositionsreihe hat, wenn er sowohl artinsch als auch noethersch ist.

8 Lokale Ringe

Ein Ring A heißt *lokaler Ring*, wenn er ein eindeutig bestimmtes maximales Linksideal hat.

(8.1) Satz. *Sei A ein lokaler Ring mit maximalem Linksideal J. Dann gilt:*

(1) *J ist ein zweiseitiges Ideal.*
(2) *$A \setminus J$ ist die Menge der Elemente mit Linksinversem (Rechtsinversem, Inversem).*
(3) *A hat genau ein maximales Rechtsideal, und dieses ist gleich J.*
(4) *A/J ist ein Divisionsring.*
(5) $1 + J \in A^*$.

BEWEIS. (1) A/J ist ein einfacher A-Modul M. Für jedes $x \in M \setminus 0$ ist deshalb der Annullator $\mathrm{Ann}(x)$ ein maximales Linksideal, also gleich J. Das Ideal $\mathrm{Ann}(M) = \bigcup_{x \in M} \mathrm{Ann}(x)$ ist deshalb ebenfalls gleich J. Der Annullator eines Moduls ist ein zweiseitiges Ideal.

(2) Ein Element in einem zweiseitigen Ideal kann kein Rechts- oder Linksinverses

haben. Sei $x \notin J$. Das Linksideal Ax enthält x und ist deshalb nicht in J enthalten. Also ist $Ax = A$ und x hat ein Linksinverses. Sei $yx = 1$. Dann ist $y \notin J$, da J zweiseitig ist. Also gibt es z mit $zy = 1$. Folglich ist y ein Inverses von x.

(3) Sei I ein maximales Rechtsideal. Falls I nicht in J liegt, so enthält I eine Einheit. Unmöglich.

(4) folgt aus (2).

(5) Sei $x \in J$. Es ist $1 = x + (1 - x)$. Also liegt $1 - x$ nicht in J und hat demnach ein Inverses. □

(8.2) Satz. *Sei A ein Ring und A^* (A^{*l}, A^{*r}) die Menge der Elemente mit Inversem (Linksinversem, Rechtsinversem). Dann sind äquivalent:*

(1) *$A \setminus A^*$ ist ein Linksideal.*
(2) *$A \setminus A^{*l}$ ist ein Linksideal.*
(3) *$A \setminus A^*$ ist ein Rechtsideal.*
(4) *$A \setminus A^{*r}$ ist ein Rechtsideal.*

Gilt eine dieser Aussagen, so sind alle Ideale gleich und A ist ein lokaler Ring mit maximalem Ideal $A \setminus A^*$.

Beweis. Ein Linksideal enthält kein Element mit einem Linksinversen. Also ist im Falle (1) und (2) die Differenzmenge ein maximales Linksideal. Analog für (3) und (4). Alles Weitere folgt aus dem vorigen Satz. □

Ein A-Modul M heißt *unzerlegbar*, wenn er nicht direkte Summe zweier von 0 und M verschiedener Untermoduln ist. Ein Modul M heißt *eindeutig zerlegbar*, wenn er endliche direkte Summe unzerlegbarer Moduln ist und aus Zerlegungen

$$M = \bigoplus_{i=1}^{m} M_i = \bigoplus_{j=1}^{n} N_j$$

mit von Null verschiedenen unzerlegbaren M_i und N_j folgt, daß $m = n$ ist und nach Umordnung $M_i = N_i$. Wir wollen zeigen, daß endlich erzeugte Moduln über artinschen Ringen eindeutig zerlegbar sind (8.7). Das folgende Lemma läuft unter dem Namen *Lemma von Fitting*

(8.3) Lemma. *Der Modul M sei artinsch und noethersch. Für jedes $f \in \mathrm{End}_A(M)$ gibt es ein n, so daß $M = \mathrm{Bild}(f^n) \oplus \mathrm{Kern}(f^n)$.*

Beweis. Es gilt $f^n(M) \supset f^{n+1}(M)$ und $\mathrm{Kern}(f^n) \subset \mathrm{Kern}(f^{n+1})$. Wegen der Maximal- und Minimalbedingung gibt es ein n mit $f^n(M) = f^{2n}(M)$ und $\mathrm{Kern}(f^n) = \mathrm{Kern}(f^{2n})$. Für $x \in M$ gibt es dann ein y mit $f^n(x) = f^{2n}(y)$. Also ist $x - f^n(y) \in \mathrm{Kern}(f^n)$ und folglich $x = f^n(y) + (x - f^n(y)) \in \mathrm{Bild}(f^n) + \mathrm{Kern}(f^n)$. Sei $z \in \mathrm{Bild}(f^n) \cap \mathrm{Kern}(f^n)$, also $z = f^n(x)$ für ein $x \in M$ und dann $0 = f^n(z) = f^{2n}(x)$. Wegen $x \in \mathrm{Kern}(f^{2n}) = \mathrm{Kern}(f^n)$ ist $z = 0$. Also ist die Summe direkt. □

(8.4) Notiz. *Sei M unzerlegbar, artinsch und noethersch. Dann ist $E = \mathrm{End}_A(M)$ ein lokaler Ring.*

BEWEIS. Sei I ein maximales Linksideal von E und $a \notin I$. Dann ist $E = Ea + I$ und etwa $1 = \lambda a + \mu$ mit $\lambda \in E$ und $\mu \in I$. Da $\mu \in I$ kein Inverses hat, ist μ kein Isomorphismus. Wir wählen n nach (8.3) für μ. Da M unzerlegbar ist, gilt $\text{Bild}(f^n) = M$ oder $\text{Kern}(f^n) = M$. Wäre $\text{Bild}(f^n) = M$, so wäre $\text{Kern}(f^n) = 0$ und μ ein Isomorphismus. Also ist $\mu^n = 0$. Es folgt

$$(1 + \mu + \cdots + \mu^{n-1})\lambda a = (1 + \mu + \cdots + \mu^{n-1})(1 - \mu) = 0.$$

Also ist a invertierbar. □

Ist M zerlegbar, so ist $A = \text{End}(M)$ kein lokaler Ring, denn dann gibt es in A nichttriviale Idempotente e. Es sind aber e und $1 - e$ keine Einheiten, was in einem lokalen Ring nicht sein kann.

(8.5) Lemma. *Seien $M = M_1 \oplus M_2 = N_1 \oplus N_2$ Zerlegungen mit Inklusionen $i_k \colon M_k \to M$, $j_k \colon N_k \to N$ und Projektionen $p_l \colon M \to M_l$, $q_l \colon N \to N_l$. Sei $p_1 j_1 \colon N_1 \to M_1$ ein Isomorphismus. Dann sind M_2 und N_2 isomorph.*

BEWEIS. Wir benutzen die Inklusionen und Projektionen, um die Identität von M in Matrizenform zu schreiben, nämlich $\alpha = (p_k j_l) = \text{id}$ und $\beta = q_r i_s) = \text{id}$. Es sind $p_1 j_1$ und $q_1 i_1$ zueinander inverse Isomorphismen. Es gilt wegen $\alpha\beta = \text{id}$ die Gleichung $(p_2 j_1)(q_1 i_1) + p_2 j_2)(q_2 i_1) = 0$ und folglich $p_2 j_1 = -(p_2 j_2)(q_2 i_1)(p_1 j_1)$. Der Isomorphismus

$$\begin{pmatrix} \text{id} & 0 \\ p_2 j_2 q_2 i_1 & \text{id} \end{pmatrix} \begin{pmatrix} p_1 j_1 & p_1 j_2 \\ p_2 j_1 & p_2 j_2 \end{pmatrix} = \begin{pmatrix} p_1 j_1 & p_1 j_2 \\ 0 & p_2 j_2 q_2 i_1 p_1 j_2 + p_2 j_2 \end{pmatrix}$$

bildet N_2 isomorph auf M_2 ab. □

(8.6) Satz. *Sei $M = M_1 \oplus \cdots \oplus M_m$ mit unzerlegbaren M_j. Sei $\text{End}_A(M_j)$ für alle j ein lokaler Ring. Dann ist M eindeutig zerlegbar.*

BEWEIS. Sei $M = N_1 \oplus \cdots \oplus N_n$ eine zweite Zerlegung in unzerlegbare Moduln. Wir wenden Induktion nach m an. Sei $m > 1$. Wir setzen mit den kanonischen Injektionen und Projektionen

$$\alpha_i \colon N_i \to M \to M_1, \qquad \beta_i \colon M_1 \to M \to N_i.$$

Dann ist $\sum_i \alpha_i \beta_i = \text{id}(M_1)$. Da $\text{End}_A(M_1)$ ein lokaler Ring ist, muß eine der Abbildungen, etwa $\alpha_1 \beta_1$ ein Isomorphismus sein. Wir verwenden nun (8.5), um M_1 und N_1 zu kürzen. □

Als Satz von *Krull-Schmidt* bezeichnen wir:

(8.7) Satz. *Ein endlich erzeugter Modul M über einem artinschen Ring A ist eindeutig zerlegbar.*

BEWEIS. Sei N unzerlegbarer A-Modul. Dann ist N nach (3.11) artinsch und noethersch und deshalb $\text{End}(N)$ nach (8.4) ein lokaler Ring. Weil M artinsch ist,

hat M jedenfalls eine Zerlegung in unzerlegbare Moduln. Nun wenden wir (8.6) an. □

Hier ist eine wichtige Anwendung des Satzes von Krull-Schmidt.

(8.8) Satz. *Seien M und N endlichdimensionale Moduln über der endlichdimensionalen K-Algebra A. Sei $L|K$ eine endliche Körpererweiterung. Sind die $L \otimes_K A$-Moduln $L \otimes_K M$ und $L \otimes_K N$ isomorph, so sind M und N isomorph.*

Beweis. Sei $\dim_K L = t$. Wir betrachten $L \otimes_K M$ vermöge $A \to L \otimes_K A$, $a \mapsto 1 \otimes a$ als A-Modul. Als solcher ist er isomorph zur t-fachen direkten Summe M^t. Die Voraussetzung liefert also einen Isomorphismus $M^t \cong N^t$. Wir zerlegen M und N in unzerlegbare Moduln $M = M_1 \oplus \ldots \oplus M_n$, $N = N_1 \oplus \ldots \oplus N_n$ und erhalten

$$M_1^t \oplus \ldots \oplus M_m^t \cong N_1^t \oplus \ldots \oplus N_n^t.$$

Aus dem Eindeutigkeitssatz folgt durch Gruppierung nach Isomorphietypen der M_i und N_j, daß M und N aus isomorphen Summanden aufgebaut werden, also isomorph sind. □

Der vorstehende Satz läßt sich insbesondere auf Gruppendarstellungen anwenden.

6 Multilineare Algebra

1 Das Tensorprodukt

Wir betrachten in diesem Abschnitt nur kommutative Ringe R und R-Linksmoduln.

Seien E, F und G Moduln. Eine Abbildung $s\colon E \times F \to G$ heißt *R-bilinear* (kurz bilinear), wenn für jedes $e \in E$ und jedes $f \in F$ die Abbildungen

$$\textbf{(1.1)} \qquad s(e,?)\colon F \to G,\ f \mapsto s(e,f) \quad \text{und} \quad s(?,f)\colon E \to G,\ e \mapsto s(e,f)$$

R-linear sind. Die Menge $\mathrm{Bil}(E \times F, G)$ der bilinearen Abbildungen ist ein R-Modul mit der üblichen Struktur: Addition und skalare Multiplikation der Funktionswerte.

In derselben Weise werden *multilineare* Abbildungen definiert. Sind E_j und G Moduln, so heißt $f\colon E_1 \times \cdots \times E_n \to G$ *n-linear*, wenn f in jeder Variablen $e_j \in E_j$ linear ist.

(1.2) Tensorprodukt. Eine bilineare Abbildung $s\colon E \times F \to G$ heißt *Tensorprodukt* von E und F über R, wenn sie die folgende *universelle Eigenschaft* hat: Zu jeder bilinearen Abbildung $\varphi\colon E \times F \to H$ gibt es genau eine lineare Abbildung $f\colon G \to H$, so daß $f \circ s = \varphi$ ist. $\diamond$

Ist in (1.2) φ ebenfalls ein Tensorprodukt, so gibt es genau eine lineare Abbildung $g\colon H \to G$ mit $g\varphi = s$. Es folgt $gfs = s$, $fg\varphi = \varphi$. Wegen der Eindeutigkeitsaussage in (1.2) ist also $gf = \mathrm{id}(G)$, $fg = \mathrm{id}(H)$. Deshalb sind g und f zueinander inverse Isomorphismen. Der damit bewiesene Sachverhalt besagt: Das Tensorprodukt ist durch die universelle Eigenschaft eindeutig bis auf eindeutige Isomorphie bestimmt.

Wir bezeichnen das Tensorprodukt von E, F mit $s\colon E \times F \to E \otimes_R F$ und nennen $E \otimes_R F$ das Tensorprodukt über R des Paares E, F (gelesen: E Tensor F) mit den *Tensorfaktoren* E und F. Den Index R am *Tensorproduktzeichen* $\otimes$ lassen wir weg, wenn R aus dem Kontext erkenntlich ist. Einen Übergang $E \mapsto E \otimes F$ bezeichnen wir als *tensorieren* mit F. Das Element $s(e,f)$ wird mit $e \otimes f$ bezeichnet. Wegen der Bilinearität gelten die Rechenregeln

$$\textbf{(1.3)} \qquad \begin{aligned} (e_1 + e_2) \otimes f &= e_1 \otimes f + e_2 \otimes f \\ e \otimes (f_1 + f_2) &= e \otimes f_1 + e \otimes f_2 \\ (re) \otimes f &= e \otimes (rf) = r(e \otimes f) \end{aligned}$$

für $e, e_1, e_2 \in E$, $f, f_1, f_2 \in F$ und $r \in R$.

(1.4) Satz. *Zu je zwei R-Moduln E, F gibt es ein Tensorprodukt.*

Beweis. Sei C der von der *Menge* $E \times F$ erzeugte freie R-Modul. Sei D der Untermodul, der von den folgenden Linearkombinationen der Basiselemente erzeugt wird ($r \in R$, $e_1, e_2, e \in E$, $f_1, f_2, f \in F$)

$$(e_1 + e_2, f) - (e_1, f) - (e_2, f)$$

$$(e, f_1 + f_2) - (e, f_1) - (e, f_2)$$

$$r(e, f) - (re, f), \quad r(e, f) - (e, rf).$$

Wir haben eine kanonische Abbildung $i\colon E \times F \to C$, die (e, f) auf das ebenso bezeichnete Basiselement abbildet. Sei $p\colon C \to C/D$ die Faktorabbildung. Die Abbildung $pi = s\colon E \times F \to C/D$ ist nach Konstruktion bilinear. Wir verifizieren die universelle Eigenschaft des Tensorprodukts. Sei $\varphi\colon E \times F \to H$ bilinear. Wegen der universellen Eigenschaft des freien Moduls über einer Menge gibt es genau eine lineare Abbildung $F\colon C \to H$ mit $Fi = \varphi$. Da φ bilinear ist, liegt D im Kern von F, und deshalb gibt es eine lineare Abbildung $f\colon C/D \to H$ mit $fp = F$ und folglich $fs = \varphi$. Durch $fp = F$ ist f eindeutig bestimmt, denn F ist eindeutig bestimmt und p ist surjektiv. □

Als Folgerung aus der Konstruktion des Tensorprodukts ergibt sich:

(1.5) Notiz. *Die Elemente $e \otimes f$ für $e \in E$ und $f \in F$ erzeugen den R-Modul $E \otimes F$.* □

Wir leiten im folgenden einige formale Eigenschaften des Tensorprodukts her. Die schwerfällige Konstruktion des Tensorproduktes im Beweis von (1.4) wird niemals wieder verwendet. Die weitere Analyse des Tensorproduktes geschieht über die universelle Eigenschaft und die daraus gewonnenen formalen Regeln. Seien $\lambda\colon E \to E'$ und $\mu\colon F \to F'$ lineare Abbildungen. Wir betrachten das Diagramm

$$\begin{array}{ccc} E \times F & \xrightarrow{\lambda \times \mu} & E' \times F' \\ \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s'} \\ E \otimes F & \xrightarrow{\lambda \otimes \mu} & E' \otimes F' \end{array}$$

mit Tensorprodukten s und s'. Da $(\lambda \times \mu)s'$ bilinear ist, gibt es genau eine lineare Abbildung $\lambda \otimes \mu\colon E \otimes F \to E' \otimes F'$, genannt das *Tensorprodukt* von (λ, μ), die das Diagramm kommutativ macht. Speziell gilt

$$(\lambda \otimes \mu)(e \otimes f) = \lambda(e) \otimes \mu(f). \tag{1.6}$$

Diese Eigenschaft charakterisiert $\lambda \otimes \mu$. Für Verkettungen bestätigt man damit die Rechenregeln

$$(\lambda \otimes \mu) \circ (\lambda' \otimes \mu') = (\lambda\lambda') \otimes (\mu\mu'), \quad \mathrm{id} \otimes \mathrm{id} = \mathrm{id}\,. \tag{1.7}$$

(1.8) Satz. *Das Tensorprodukt ist assoziativ: Seien E, F und G Moduln. Es gibt genau einen Isomorphismus $\alpha\colon (E \otimes F) \otimes G \to E \otimes (F \otimes G)$ von R-Moduln mit der Eigenschaft $\alpha((e \otimes f) \otimes g) = e \otimes (f \otimes g)$.*

Beweis. Mit Tensorprodukten $\varphi, \varphi', \psi, \psi'$ und der universellen Eigenschaft wird

α aus dem folgenden Diagramm konstruiert

$$\begin{array}{ccc}
(E\times F)\times G & \xrightarrow{=} & E\times(F\times G)\\
\downarrow{\scriptstyle \varphi\times \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}\times\psi}\\
(E\otimes F)\times G & \longrightarrow & E\times(F\otimes G)\\
\downarrow{\scriptstyle \varphi'} & \searrow^{\alpha'} & \downarrow{\scriptstyle \psi'}\\
(E\otimes F)\otimes G & \xrightarrow{\alpha} & E\otimes(F\otimes G).
\end{array}$$

Für jedes $g\in G$ ist die Abbildung $(e,f)\mapsto \psi'(e,\psi(f,g))$ bilinear. Es gibt deshalb genau eine lineare Abbildung $\alpha_g\colon E\otimes F\to E\otimes(F\otimes G)$ mit

$$\alpha_g(e\otimes f)=\psi'(e,\psi(f,g))=e\otimes(f\otimes g).$$

Die Abbildung α' mit $\alpha'(e\otimes f,g)=\alpha_g(e\otimes f)$ ist ebenfalls bilinear: Es ist nämlich

$$\begin{aligned}
\alpha_{r_1g_1+r_2g_2}(e\otimes f) &= \psi'(e,\psi(f,r_1g_1+r_2g_2))\\
&= r_1\psi'(e,\psi(f,g_1))+r_2\psi'(e,\psi(f,g))\\
&= (r_1\alpha_{g_1}+r_2\alpha_{g_2})(e\otimes f);
\end{aligned}$$

da die Elemente $e\otimes f$ den Modul $E\otimes F$ erzeugen, gilt also

$$\alpha_{r_1g_1+r_2g_2}=r_1\alpha_{g_1}+r_2\alpha_{g_2}.$$

Damit ist α' als linear in der zweiten Veränderlichen erkannt. Ferner ist α' wegen der Linearität von α_g auch in der ersten Veränderlichen linear. Nach der universellen Eigenschaft von φ' gibt es α mit $\alpha\varphi'=\alpha'$, und speziell gilt

$$\alpha((e\otimes f)\otimes g)=\alpha\varphi'(e\otimes f,g)=\alpha'(e\otimes f,g)=\alpha_g(e\otimes f)=e\otimes(f\otimes g).$$

Ebenso verschafft man sich ein β mit der Eigenschaft $\beta(e\otimes(f\otimes g))=(e\otimes f)\otimes g$. Es sind dann α und β invers zueinander. □

(1.9) Satz. *Das Tensorprodukt ist kommutativ: Es gibt genau eine lineare Abbildung $\tau\colon E\otimes F\to F\otimes E$ mit der Eigenschaft $\tau(e\otimes f)=f\otimes e$. Diese Abbildung ist ein Isomorphismus.*

Beweis. Wir haben mit der Vertauschung $t\colon E\times F\to F\times E$, $(e,f)\mapsto(f,e)$ ein kommutatives Diagramm

$$\begin{array}{ccc}
E\times F & \xrightarrow{t} & F\times E\\
\downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi}\\
E\otimes F & \xrightarrow{\tau} & F\otimes E
\end{array}$$

mit Tensorprodukten φ und ψ. Die Existenz von τ folgt aus der universellen Eigenschaft von φ. □

Die Definition des Tensorprodukts läßt sich auf multilineare Abbildungen erweitern. Eine n-lineare Abbildung $s\colon E_1 \times \cdots \times E_n \to E_1 \otimes \cdots \otimes E_n$ heißt *Tensorprodukt* von $(E_1, \ldots, E_n)$, wenn zu jeder n-linearen Abbildung $\varphi\colon E_1 \times \cdots \times E_n \to G$ genau eine lineare Abbildung $f\colon E_1 \otimes \cdots \otimes E_n \to G$ mit $f \circ s = \varphi$ existiert. Der Beweis von (1.4) läßt sich auf diesen Fall übertragen. Man bestätigt aber auch leicht, daß die im Beweis von (1.8) auftretende Abbildung $(\varphi \times \mathrm{id})\varphi'\colon (E \times F) \times G \to (E \otimes F) \otimes G$ ein trilineares Tensorprodukt ist. Auf diese Weise erhält man durch Iteration ein n-lineares Tensorprodukt. Satz (1.8) folgt dann übrigens aus der universellen Eigenschaft des trilinearen Tensorprodukts. Auch gelten analoge Assoziativitäten und Kommutativitäten für mehrere Faktoren und beliebige Klammerungen.

Das Tensorprodukt $E \otimes E \otimes \cdots \otimes E$ von p Exemplaren E wird auch mit $\otimes^p E$ bezeichnet. Ähnlich ist die Bezeichnung

$$\bigotimes_{j=1}^{p} E_j := E_1 \otimes E_2 \otimes \cdots \otimes E_p.$$

Elemente von $\bigotimes_{j=1}^{p} E_j$ heißen *Tensoren*. Tensoren der Form $e_1 \otimes \cdots \otimes e_p$ heißen *zerlegbar*.

Die folgenden Beispiele von Tensorprodukten über $\mathbb{Z}$ zeigen schon eine Besonderheit dieses Begriffs.

(1.10) Beispiel. $\mathbb{Z}/(n) \otimes \mathbb{Q} = 0$ für $n > 0$.

Beweis. Die Rechenregeln für das Tensorzeichen liefern

$$x \otimes 1 = x \otimes \frac{n}{n} \otimes 1 = nx \otimes \frac{1}{n} = 0 \otimes \frac{1}{n} = 0.$$

(1.11) Beispiel. $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

Beweis. Die Rechenregeln für das Tensorzeichen liefern die Kette

$$\frac{p}{q} \otimes \frac{r}{s} = \frac{p}{q} \cdot \frac{s}{s} \otimes \frac{r}{s} = \frac{p}{q} \cdot \frac{1}{s} \otimes s\frac{r}{s} = \frac{p}{qs} \otimes r = \frac{p}{qs} \otimes 0 = 0.$$

($\frac{p}{q}$ bezeichne auch die Restklasse $\frac{p}{q} + \mathbb{Z}$). ◇

Aus der Definition des Tensorprodukts entnehmen wir einen kanonischen Isomorphismus von R-Moduln

$$\mathrm{Bil}(E \times F, G) \cong \mathrm{Hom}(E \otimes F, G). \tag{1.12}$$

Er ordnet jeder bilinearen Abbildung die nach der universellen Eigenschaft zugehörige lineare Abbildung zu. Da auch $\mathrm{Hom}(E, \mathrm{Hom}(F, G)) \to \mathrm{Bil}(E \times F, G)$, $\varphi \mapsto ((e, f) \mapsto (\varphi(e))(f))$ ein Isomorphismus ist, so erhalten wir einen kanonischen Isomorphismus (*Adjunktionsformel*)

(1.13) $$\mathrm{Hom}(E, \mathrm{Hom}(F, G)) \cong \mathrm{Hom}(E \otimes F, G).$$

Der Isomorphismus (1.13) ist mit induzierten linearen Abbildungen in den drei Variablen E, F, G verträglich.

Seien $(E_i \mid i \in I)$ und $(F_j \mid j \in J)$ Familien von R-Moduln. Seien

$$\alpha_i \colon E_i \to \bigoplus_{k \in I} E_k, \qquad \beta_j \colon F_j \to \bigoplus_{\ell \in J} F_\ell$$

die kanonischen Injektionen. Aus den Abbildungen

$$\alpha_i \otimes \beta_j \colon E_i \otimes F_j \to (\bigoplus_k E_k) \otimes (\bigoplus_\ell F_\ell)$$

erhalten wir eine Abbildung nach der universellen Eigenschaft der Summe

$$\gamma = \langle \alpha_i \otimes \beta_j \mid (i,j) \in I \times J \rangle \colon \bigoplus_{i,j} (E_i \otimes F_j) \to (\bigoplus_k E_k) \otimes (\bigoplus_\ell F_\ell).$$

(1.14) Satz. *Das Tensorprodukt ist mit direkten Summen verträglich: Die voranstehende Abbildung γ ist ein Isomorphismus.*

Beweis. Die kanonischen Projektionen $p_i \colon \bigoplus E_k \to E_i$ und $q_j \colon \bigoplus F_\ell \to F_j$ liefern Abbildungen $p_i \otimes q_j$ und

$$\delta' = (p_i \otimes q_j \mid (i,j) \in I \times J) \colon (\bigoplus E_k) \otimes (\bigoplus F_\ell) \to \prod_{i,j} (E_i \otimes F_j).$$

Das Bild von δ' liegt in der direkten Summe, aufgefaßt als Untermodul des Produkts, und deshalb definiert δ' einen Homomorphismus

$$\delta \colon (\bigoplus E_k) \otimes (\bigoplus F_\ell) \to \bigoplus (E_i \otimes F_j),$$

den wir als invers zu γ erkennen. □

(1.15) Notiz. *Die Abbildung $\varepsilon \colon R \otimes_R M \to M, \quad r \otimes m \mapsto rm$ ist ein wohldefinierter Isomorphismus von R-Moduln.*

Beweis. Sie entsteht aus der bilinearen Abbildung $R \times M \to M$, $(r, m) \mapsto rm$ durch die universelle Eigenschaft. Eine inverse Abbildung wird durch $m \mapsto 1 \otimes m$ gegeben. □

(1.16) Satz. *Ist E ein freier R-Modul mit Basis $(x_i \mid i \in I)$ und F ein freier R-Modul mit Basis $(y_j \mid j \in J)$, so ist $E \otimes F$ ein freier R-Modul mit Basis $(x_i \otimes y_j \mid (i,j) \in I \times J)$. Das Tensorprodukt projektiver Moduln ist projektiv.*

Beweis. Wir haben Isomorphismen

$$\varphi \colon \bigoplus_{i \in I} R \to E, \quad (\lambda_i) \mapsto \sum_i \lambda_i x_i$$

$$\psi\colon \bigoplus_{j\in J} R \to F, \quad (\mu_j) \mapsto \sum_j \mu_j y_j.$$

Mit Hilfe von (1.14) und (1.15) ergibt sich daraus

$$\bigoplus_{i,j} R \cong \bigoplus_{i,j} (R \otimes R) \cong (\bigoplus_i R) \otimes (\bigoplus_j R) \cong E \otimes F.$$

Das Bild der Standardbasis in $\bigoplus_{i,j} R$ ist die behauptete Basis. Die zweite Aussage folgt, wenn wir benutzen, daß projektive Moduln direkte Summanden von freien sind und das Tensorprodukt mit direkten Summen verträglich ist. □

Die im folgenden Satz niedergelegte Eigenschaft wird *Rechtsexakheit* des Tensorprodukt bezeichnet. Leider ist das Tensorprodukt nicht mit beliebigen exakten Sequenzen verträglich (1.19).

(1.17) Satz. *Sei $E' \xrightarrow{u} E \xrightarrow{v} E'' \to 0$ eine exakte Sequenz von R-Moduln. Für jeden R-Modul F ist die Sequenz*

$$E' \otimes F \xrightarrow{u \otimes \mathrm{id}} E \otimes F \xrightarrow{v \otimes \mathrm{id}} E'' \otimes F \to 0$$

exakt.

Beweis. Grundlage ist das kommutative Diagramm

$$\begin{array}{ccccccc}
0 & \to & \mathrm{Hom}(E'' \otimes F, B) & \to & \mathrm{Hom}(E \otimes F, B) & \to & \mathrm{Hom}(E' \otimes F, B) \\
 & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong \\
0 & \to & \mathrm{Hom}(E'', \mathrm{Hom}(F, B)) & \to & \mathrm{Hom}(E, \mathrm{Hom}(F, B)) & \to & \mathrm{Hom}(E', \mathrm{Hom}(F, B)),
\end{array}$$

in dem die senkrechten Abbildungen die kanonischen Isomorphismen (1.13) sind und die waagerechten durch u und v induziert werden. Ferner ist B ein beliebiger weiterer Modul. Nach IV(3.1) genügt es zu zeigen, daß für jedes B die obere Zeile exakt ist. Nach IV(3.1) ist aber die untere Zeile exakt. □

(1.18) Satz. *Sei $u\colon E' \to E$ injektiv und F ein freier Modul. Dann ist die Abbildung $u \otimes \mathrm{id}\colon E' \otimes F \to E \otimes F$ injektiv. Ebenso, falls F projektiv ist.*

Beweis. Da F frei ist, setzen wir F ohne wesentliche Einschränkung als $\bigoplus_{j\in J} R_j$ mit $R_j = R$ an. Nach (1.14) und (1.15) haben wir dann Isomorphismen $E' \otimes F \cong \bigoplus_j E \otimes R \cong \bigoplus_j E'$. Es ist leicht zu sehen, daß diese Isomorphismen $u \otimes \mathrm{id}$ in die Summe $\bigoplus_j u$ transformieren, und diese Abbildung ist offenbar injektiv. □

(1.19) Erste Warnung. Die Abbildung $u \otimes \mathrm{id}$ in (1.18) ist nicht immer injektiv, siehe Beispiel (1.24). Für $e \in E' \subset E$ kann also $e \otimes f \in E' \otimes F$ von Null verschieden sein, während $e \otimes f \in E \otimes F$ aber gleich Null ist. Hier ist eine Situation erreicht, die zu sorgfältiger Notation zwingt. Insbesondere ist zwischen einer Teilmenge und der Abbildung, die die Inklusion dieser Teilmenge ist, zu unterscheiden. ◇

(1.20) Beispiel. Sei $R \subset S$ ein Unterring. Für jeden R-Modul M ist $S \otimes_R M$ in kanonischer Weise ein S-Modul: Die Skalarmultiplikation wird durch

$$S \times (S \otimes_R M) \to S \otimes_R M, \quad (s, t \otimes m) \mapsto st \otimes m$$

definiert. Aus jeder R-linearen Abbildung $f\colon M \to N$ wird eine S-lineare

$$\mathrm{id} \otimes_R f\colon S \otimes_R M \to S \otimes_R N.$$

Der dadurch gewonnene Übergang (Funktor) von R-Moduln zu S-Moduln heißt *Skalarerweiterung* von R nach S. Die Skalarerweiterung ist transitiv: Sind $R \subset S \subset T$ jeweils Unterringe, so haben wir einen kanonischen Isomorphismus

$$T \otimes_R M \cong T \otimes_S (S \otimes_R M), \quad t \otimes x \mapsto t \otimes (1 \otimes x).$$

(1.21) Satz. *Sei $I \subset R$ ein Ideal. Die Abbildung*

$$\alpha\colon R/I \otimes_R M \to M/IM, \quad (r + I) \otimes m \mapsto rm + IM$$

ist wohldefiniert und ein Isomorphismus.

Beweis. Wir betrachten das Diagramm

$$\begin{array}{ccccccc} I \otimes_R M & \xrightarrow{\delta} & R \otimes_R M & \longrightarrow & R/I \otimes_R M & \longrightarrow & 0 \\ & & \beta \downarrow \cong & & \downarrow \alpha & & \\ & & M & \xrightarrow{\gamma} & M/IM. & & \end{array}$$

Die obere Zeile ist nach (1.17) exakt. Die Abbildung β ist der Isomorphismus (1.15). Das Bild von δ liegt im Kern von $\gamma\beta$. Deshalb gibt es α wie angegeben. Da β und γ surjektiv sind, so ist auch α surjektiv. Sei $\beta'\colon M \to R/I \otimes_R M$ die Abbildung $m \mapsto 1 \otimes m$. Es handelt sich um eine R-lineare Abbildung. Ist $a \in I$ und $m \in M$, so ist $\beta'(am) = 1 \otimes am = a \otimes m = 0$. Also induziert β' eine Abbildung $\alpha'\colon M/IM \to R/I \otimes_R M$, die als invers zu α verifiziert wird. □

(1.22) Satz. *Seien $E' \xrightarrow{u} E \xrightarrow{v} E'' \to 0$ und $F' \xrightarrow{s} F \xrightarrow{t} F'' \to 0$ exakte Sequenzen. Dann ist die folgende Sequenz exakt.*

$$(E' \otimes F) \oplus (E \otimes F') \xrightarrow{u \otimes \mathrm{id} + \mathrm{id} \otimes s} E \otimes F \xrightarrow{v \otimes t} E'' \otimes F'' \longrightarrow 0.$$

Beweis. Wir betrachten das durch u, v, s, t induzierte Diagramm mit nach (1.17) exakten Zeilen und Spalten.

$$\begin{array}{ccccccc} E' \otimes F' & \to & E' \otimes F & \to & E' \otimes F'' & \to & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ E \otimes F' & \to & E \otimes F & \to & E \otimes F'' & \to & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ E'' \otimes F' & \to & E'' \otimes F & \to & E'' \otimes F'' & \to & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ 0 & & 0 & & 0 & & \end{array}$$

Die Behauptung folgt mittels Diagrammjagd (Aufgabe). □

(1.23) Satz. *Seien I, J Ideale von R. Dann ist*

$$R/I \otimes_R R/J \to R/(I+J), \quad (r_1+I)\otimes(r_2+J) \mapsto r_1 r_2 + (I+J)$$

ein wohldefinierter kanonischer Isomorphismus.

Beweis. Wir wenden (1.22) auf die Sequenzen $I \to R \to R/I$ und $J \to R \to R/J$ an. Sodann benutzen wir (1.15) $R \otimes_R R \cong R$ und bemerken, daß das Bild von $I \otimes R \oplus R \otimes J$ in $R \otimes_R R$ bei diesem Isomorphismus in $I+J$ übergeht. □

(1.24) Beispiel. Wir tensorieren die exakte Sequenz von $\mathbb{Z}$-Moduln

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/(m) \to 0$$

mit $\mathbb{Z}/(n)$ und erhalten nach (1.15), (1.17) und (1.23) eine exakte Sequenz

$$\begin{array}{ccccccc} \mathbb{Z}\otimes\mathbb{Z}/(n) & \xrightarrow{m} & \mathbb{Z}\otimes\mathbb{Z}/(n) & \longrightarrow & \mathbb{Z}/(m)\otimes\mathbb{Z}/(n) & \longrightarrow & 0 \\ \| & & \| & & \| & & \\ \mathbb{Z}/(n) & & \mathbb{Z}/(n) & & \mathbb{Z}/(m,n) & & \end{array}$$

Das Ideal (m,n) wird vom GGT von m und n erzeugt. Sind m und n teilerfremd, so ist $\mathbb{Z}/(m)\otimes\mathbb{Z}/(n)$ der Nullmodul, obgleich die beteiligten Moduln im allgemeinen von Null verschieden sind. Ist $m=n$, so ist

$$\mathbb{Z}/(m) \xrightarrow{m} \mathbb{Z}/(m)$$

die Nullabbildung. Also induziert die Multiplikation $m\colon \mathbb{Z} \to \mathbb{Z}$, $u \mapsto mu$ nach Tensorieren mit $\mathbb{Z}/(m)$ keine injektive Abbildung. Mittels (1.14) können wir jetzt das Tensorprodukt beliebiger endlich erzeugter abelscher Gruppen (betrachtet als $\mathbb{Z}$-Moduln) ausrechnen. (In (1.24) immer $\otimes = \otimes_{\mathbb{Z}}$.) ◇

(1.25) Tensorprodukt von Matrizen. Seien E, E', F, F' freie R-Moduln mit Basen $(b_j \mid j \in J)$, $(b'_j \mid j \in J')$, $(c_k \mid k \in K)$, $(c'_k \mid k \in K')$. Seien $f\colon E \to F$ und $f'\colon E' \to F'$ R-lineare Abbildungen. Wir setzen wie üblich

$$f(b_i) = \sum_{k\in K} a_{ki} c_k, \quad f'(b'_i) = \sum_{k\in K'} a'_{ki} c'_k.$$

Dann ist

$$(f\otimes f')(b_\mu \otimes b'_\nu) = f(b_\mu)\otimes f'(b'_\nu) = \sum_{k,\ell} a_{k\mu} a'_{\ell\nu} (c_k \otimes c'_\ell).$$

Die Matrix von $f\otimes f'$ bezüglich der Basen $(b_\mu \otimes b'_\nu)$ und $(c_k \otimes c'_\ell)$ ist also die Matrix aller Produkte $a_{k\mu}a'_{\ell\nu}$. Ist $A = (a_{k\mu})$ eine (m,n)-Matrix und $A' = (a'_{\ell\nu})$ eine (m',n')-Matrix, so ist

$$A \otimes A' = (a_{k\mu} a'_{\ell\nu})$$

eine (mm', nn')-Matrix. Die voranstehende Bildung ist natürlich viel älter als das Tensorprodukt und wird auch *Kronecker-Produkt* von Matrizen genannt. ◇

2 Anwendungen des Tensorprodukts

(2.1) Satz. *Seien A, A', B, B' Moduln, seien $f_1, f_2 \colon A \to A'$ und $g_1, g_2 \colon B \to B'$ lineare Abbildungen, und sei $r \in R$. Dann gilt*

$$\begin{aligned}(f_1 + f_2) \otimes g_1 &= f_1 \otimes g_1 + f_2 \otimes g_1 \\ f_1 \otimes (g_1 + g_2) &= f_1 \otimes g_1 + f_2 \otimes g_2 \\ (rf_1) \otimes g_1 &= f_1 \otimes (rg_1) \,=\, r(f_1 \otimes g_1).\end{aligned}$$

Diese Regeln besagen: Die Abbildung

$$\mathrm{Hom}_R(A, A') \times \mathrm{Hom}_R(B, B') \to \mathrm{Hom}_R(A \otimes B, A' \otimes B'),\ (f, g) \mapsto f \otimes g$$

ist bilinear.

Beweis. Beide Seiten einer behaupteten Gleichheit werden durch Einsetzen nach (1.6) als gleich erwiesen. □

Die bilineare Abbildung des letzten Satzes liefert eine lineare Abbildung

(2.2) $$T \colon \mathrm{Hom}_R(A, A') \otimes \mathrm{Hom}_R(B, B') \to \mathrm{Hom}_R(A \otimes B, A' \otimes B'),$$

die $f \otimes g$ auf $f \otimes g$ abbildet. Sie heiße *tautologische* Abbildung. Diese Abbildung ist tückisch, weil das Symbol $f \otimes g$ für den Definitions- und Bildbereich von T verschiedene Bedeutung hat: Links Tensorprodukt von Elementen und rechts Tensorprodukt von linearen Abbildungen. Die Tücke wird belegt durch:

(2.3) Zweite Warnung. Die tautologische Abbildung ist im allgemeinen weder injektiv noch surjektiv, siehe (2.5). ◇

Wir behandeln eine Art Spezialfall der tautologischen Abbildung. Zu R-Moduln E, F und dem Dualmodul E^* gibt es eine lineare Abbildung

(2.4) $$\Theta \colon E^* \otimes_R F \to \mathrm{Hom}_R(E, F), \quad \varphi \otimes y \mapsto (x \mapsto \varphi(x)y).$$

(2.5) Beispiel. Für $R = \mathbb{Z}/4$ und $E = \mathbb{Z}/2 = R/2R$ ist Θ weder injektiv noch surjektiv. Es ist $E^* = \mathrm{Hom}_R(R/2R, R) \cong \mathbb{Z}/2$, wobei das nichttriviale Element x die $1 \in R/2R$ auf $2 \in R$ abbildet. Es ist $E^* \otimes E \cong R/2R \otimes R/2R \cong R/2R \cong \mathbb{Z}/2$. Das nichttriviale Element $x \otimes 1$ wird bei Θ auf $(1 \mapsto x(1) \cdot 1 = 2 \cdot 1 = 0)$, also auf die Nullabbildung geworfen. ◇

Die Abbildung Θ ist im wesentlichen ein Spezielfall der tautologischen Abbildung. Um das einzusehen, verwendet man die kanonischen Isomorphismen $R \otimes E \cong E$ und $\mathrm{Hom}(R, F) \cong F$ und das kommutative Diagramm

$$\begin{array}{ccc} \mathrm{Hom}(E, R) \otimes F & \xrightarrow{\Theta} & \mathrm{Hom}(E, F) \\ \downarrow \cong & & \downarrow \cong \\ \mathrm{Hom}(E, R) \otimes \mathrm{Hom}(R, F) & \xrightarrow{T} & \mathrm{Hom}(E \otimes R, R \otimes F). \end{array}$$

Ein anderer Spezialfall der tautologischen Abbildung ist das Tensorprodukt von Dualmoduln

$$\begin{array}{ccc} \mathrm{Hom}(E,R)\otimes\mathrm{Hom}(F,R) & \xrightarrow{T} & \mathrm{Hom}(E\otimes F, R\otimes R) \\ \downarrow\cong & & \downarrow\cong \\ E^*\otimes F^* & \xrightarrow{D} & (E\otimes F)^*. \end{array} \tag{2.6}$$

Auch diese Abbildung ist mit den Daten aus (2.5) weder injektiv noch surjektiv.

(2.7) Satz. *Die tautologische Abbildung ist unter den folgenden Voraussetzungen ein Isomorphismus: Eines der Paare (A,A'), (B,B'), (A,B) besteht aus endlich erzeugten projektiven Moduln. Falls E oder F ein endlich erzeugter projektiver Modul ist, so sind Θ und D Isomorphismen.*

Beweis. Die Aussage $T(A,A',B,B')$ bedeute: T ist für (A,A',B,B') ein Isomorphismus. Da Hom und $\otimes$ mit endlichen direkten Summen verträglich sind, folgt aus $T(A_j,A',B,B')$ für $j=1,2$ die Aussage $T(A_1\oplus A_2,A',B,B')$. Entsprechend für die Variable A'. Ebenso folgt aus $T(A,A',B,B')$ die Aussage $T(P,A',B,B')$ für einen direkten Summanden P von A. Wegen dieser formalen Eigenschaften von T müssen nur die Fälle $(A,A')=(R,R)$ und $(A,B)=(R,R)$ betrachtet werden. Im ersten Fall haben wir ein kommutatives Diagramm

$$\begin{array}{ccc} \mathrm{Hom}(R,R)\otimes\mathrm{Hom}(B,B') & \xrightarrow{T} & \mathrm{Hom}(R\otimes B, R\otimes B') \\ \downarrow\cong & & \downarrow\cong \\ \mathrm{Hom}(B,B') & \xrightarrow{\mathrm{id}} & \mathrm{Hom}(B,B'), \end{array}$$

in dem die senkrechten Pfeile durch kanonische Isomorphismen $\mathrm{Hom}(R,E)\cong E$ und $R\otimes E\cong E$ gegeben sind. Analog für den Fall $(A,B)=(R,R)$. Die Aussagen über die Abbildungen Θ und D sind im wesentlichen Spezialfälle, wie wir oben erläutert haben. □

(2.8) Die Spur. Sei E endlich erzeugt und projektiv. Sei ε die Evaluation $\varphi\otimes x\mapsto\varphi(x)$. Dann ist definitionsgemäß

$$\mathrm{Sp}\colon \mathrm{Hom}(E,E)\xrightarrow{\Theta^{-1}} E^*\otimes E\xrightarrow{\varepsilon} R$$

die Abbildung, die jedem Endomorphismus seine *Spur* zuordnet. Ist E ein freier Modul mit Basis $e_1,\dots,e_n$ und wird der Endomorphismus f durch eine Matrix $f(e_k)=\sum_l a_{lk}e_l$ beschrieben, so ist $\mathrm{Sp}(f)=\sum_k a_{kk}$, wie aus der elementaren linearen Algebra geläufig. Wegen der Linearität von Sp genügt es, diese Aussage für $\Theta(e^i\otimes e_j)$ zu beweisen, wobei (e^i) die Dualbasis zu (e_j) ist. Es ist

$$\Theta(e^i\otimes e_j)(e_k)=\delta^i_k e_j,$$

woraus die behauptete Gleichheit sofort folgt. ◇

Die fundamentale Eigenschaft der Spur ist ihre *Kommutativität*.

(2.9) Satz. *Seien $u\colon E \to F$ und $v\colon F \to E$ lineare Abbildungen zwischen endlich erzeugten projektiven Moduln. Dann ist* $\mathrm{Sp}(uv) = \mathrm{Sp}(vu)$.

Beweis. Die Abbildungen $(u,v) \mapsto \mathrm{Sp}(uv)$ und $(u,v) \mapsto \mathrm{Sp}(vu)$ sind bilineare Abbildungen $\mathrm{Hom}(E,F) \times \mathrm{Hom}(F,E) \to R$. Es genügt deshalb, die Gleichheit auf Elementen der Form $u = \Theta(\varphi, x)$ und $v = \Theta(\psi, y)$ für $\varphi \in E^*$, $x \in F$, $\psi \in F^*$, $y \in E$ nachzuweisen. Dafür ist

$$(vu)(e) = v(\varphi(e)x) = \varphi(e)\psi(x)y$$

$$(uv)(e) = u(\psi(e)y) = \psi(e)\varphi(y)x.$$

Also ist $vu = \Theta(\psi(x)\varphi \otimes y)$ und $uv = \Theta(\varphi(y)\psi \otimes x)$ und somit die Spur in beiden Fällen gleich $\psi(x)\varphi(y)$. □

Weiterhin ist die Spur *multiplikativ*.

(2.10) Satz. *Seien $u_j\colon E_j \to E_j$ Endomorphismen endlich erzeugter projektiver Moduln E_1 und E_2. Dann gilt* $\mathrm{Sp}(u_1 \otimes u_2) = \mathrm{Sp}(u_1)\,\mathrm{Sp}(u_2)$.

Beweis. Das folgt aus der Definition der Spur und dem folgenden kommutativen Diagramm

$$\begin{array}{ccc} E_1^* \otimes E_1 \otimes E_2^* \otimes E_2 & \xrightarrow{(D \otimes \mathrm{id})\tau_{23}} & (E_1 \otimes E_2)^* \otimes E_1 \otimes E_2 \\ \downarrow{\scriptstyle \Theta \otimes \Theta} & & \downarrow{\scriptstyle \Theta} \\ \mathrm{Hom}(E_1, E_1) \otimes \mathrm{Hom}(E_2, E_2) & \xrightarrow{T} & \mathrm{Hom}(E_1 \otimes E_2, E_1 \otimes E_2), \end{array}$$

worin τ_{23} den zweiten und dritten Tensorfaktor vertauscht. □

Wir definieren das *Tensorprodukt von Algebren*. Seien A und B R-Algebren. Auf dem Modul $A \otimes_R B$ wird die Struktur einer R-Algebra definiert durch die Multiplikation

$$(A \otimes B) \times (A \otimes B) \to A \otimes B, \quad (a \otimes b, a' \otimes b') \mapsto aa' \otimes bb'.$$

Die Multiplikation ist assoziativ (kommutativ), wenn die Multiplikationen von A und B assoziativ (kommutativ) sind. Die Abbildung $i_A\colon A \to A \otimes B$, $a \mapsto a \otimes 1$ ist ein Homomorphismus von Algebren (analog für B). Sind $\varphi\colon A \to C$ und $\psi\colon B \to C$ Homomorphismen von R-Algebren mit der Eigenschaft $\varphi(a)\psi(b) = \psi(b)\varphi(a)$, so gibt es genau einen Homomorphismus von R-Algebren

$$\Phi\colon A \otimes B \to C, \quad a \otimes b \mapsto \varphi(a)\psi(b).$$

Zum Beweis wird die universelle Eigenschaft des Tensorprodukts auf $(a,b) \mapsto \varphi(a)\psi(b)$ angewendet.

Gewisse Sorten von Tensorprodukten lassen sich auch für Moduln über nichtkommutativen Ringen definieren. Sei also jetzt A ein beliebiger Ring. Sei M ein

A-Rechtsmodul und N ein A-Linksmodul. Eine Abbildung $f\colon M \times N \to A$ in eine abelsche Gruppe C heißt *mittellinear*, wenn für $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, $\lambda \in A$ gilt

$$\begin{aligned} f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n) \\ f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2) \\ f(m\lambda, n) &= f(m, \lambda n). \end{aligned}$$

Wir bezeichnen die universelle mittellineare Abbildung mit

$$M \times N \to M \otimes_A N, \quad (x, y) \mapsto x \otimes y$$

und nennen sie das *Tensorprodukt* von (M, N). Die Konstruktion erfolgt genauso wie in (1.4): Man bildet den freien $\mathbb{Z}$-Modul über der Menge $M \times N$ und dividiert den Untermodul heraus, der von den Linearkombinationen der Form

$$\begin{aligned} (m_1 + m_2, n) &- (m_1, n) - (m_2 + n) \\ (m, n_1 + n_2) &- (m, n_1) - (m, n_2) \\ (m\lambda, n) &- (m, \lambda n) \end{aligned}$$

erzeugt wird.

Um dem Tensorprodukt $M \otimes_A N$ eine weitere Struktur zu geben, braucht man Bimoduln. Sei B ein weiterer Ring. Ein *B-A-Bimodul* ist eine abelsche Gruppe M zusammen mit der Struktur eines B-Linksmoduls und der Struktur eines A-Rechtsmoduls, so daß diese Modulstrukturen verträglich sind: $b(xa) = (bx)a$ für alle $b \in B$, $x \in M$ und $a \in A$. Sind A und B R-Algebren über einem kommutativen Ring R, so setzt man M als R-Modul voraus, d. h. die von A und B induzierten R-Modulstrukturen sollen übereinstimmen, wenn wir die R-Algebrastruktur durch einen Homomorphismus in das jeweilige Zentrum definieren. Einen B-A-Bimodul M kann man auch als Linksmodul über der Algebra $B \otimes_R A^\circ$ auffassen, vermöge der Definition $(b \otimes a)x = bxa$ (hier ist A° die Gegenalgebra von A), und umgekehrt.

Ist nun M ein B-A-Bimodul und N ein A-Linksmodul, so trägt $M \otimes_A N$ die Struktur eines B-Linksmoduls vermöge der Vorschrift

$$b \cdot (x \otimes y) = bx \otimes y.$$

Ein Homomorphismus zwischen B-A-Bimoduln ist eine Abbildung, die sowohl B- als auch A-linear ist. Ist $\varphi\colon M \to M'$ eine Homomorphismus von B-A-Moduln und $\psi\colon N \to N'$ einer von A-Moduln, so ist $\varphi \otimes \psi\colon M \otimes N \to M' \otimes N'$ einer von B-Moduln. Eine Anwendung dieser Konstruktion ist wieder der *Ringwechsel*. Sei A ein Unterring von B. Dann ist B ein B-A-Bimodul vermöge Multiplikation von links und rechts. Aus einem A-Linksmodul N wird dann der B-Linksmodul $B \otimes_A N$. Diese Bildung ist auch assoziativ: Für Unterringe $A \subset B \subset C$ gilt $C \otimes_B B \otimes_A N \cong C \otimes_A N$. Es gilt auch eine *Adjunktionsformel* für den Ringwechsel:

(2.11) $$\mathrm{Hom}_B(B \otimes_A N, P) \cong \mathrm{Hom}_A(N, P)$$

für A-Moduln N und B-Moduln N, wobei wir auf der rechten Seite P durch Strukturvergessen als A-Modul auffassen.

Seien A und B Algebren über dem kommutativen Ring R. Wir betrachten A- und B-Linksmoduln und Tensorprodukte über R. Aus einem A-Modul M und einem B-Modul N wird durch die Vorschrift

(2.12) $$(a \otimes b) \cdot (x \otimes y) = ax \otimes by$$

ein $A \otimes B$-Modul $M \otimes N$. Ist $\psi\colon M \otimes M'$ A-linear und $\psi\colon N \otimes N'$ B-linear, so ist $\varphi \otimes \psi$ $A \otimes B$-linear. Die tautologische Abbildung

(2.13) $$T\colon \mathrm{Hom}_A(M, M') \otimes \mathrm{Hom}_B(N, N') \to \mathrm{Hom}_{A\otimes B}(M \otimes N, M' \otimes N')$$

ist R-linear; und für $M = M'$ und $N = N'$ erhält man einen Homomorphismus von Endomorphismenalgebren

(2.14) $$\mathrm{End}_A(M) \otimes \mathrm{End}_B(N) \to \mathrm{End}_{A\otimes B}(M \otimes N).$$

Ist M eine freier A-Modul und N ein freier B-Modul, beide mit endlicher Basis, so sind die beiden letzten Abbildungen Isomorphismen. Wegen der Verträglichkeit des Tensorprodukts mit direkten Summen führt man diese Aussage auf den Fall $M = A$ und $N = B$ zurück, wo sie leicht nachgerechnet wird. Eine kanonische Isomorphie

(2.15) $$M_m(A) \otimes M_n(B) \cong M_{mn}(A \otimes B)$$

erhalten wir durch Übersetzung in Matrizen.

3 Äußere Potenzen

Seien E und F Moduln über dem kommutativen Ring R. Eine n-lineare Abbildung $f\colon E^n = E \times \cdots \times E \to F$ heißt *alternierend*, wenn aus $x_i = x_j$ für $i \neq j$ immer $f(x_1, \ldots, x_n) = 0$ folgt.

(3.1) Äußere Potenz. Eine n-lineare alternierende Abbildung

$$\lambda\colon E^n \to \Lambda^n(E), \qquad n \geq 1$$

heißt n-te *äußere Potenz* des R-Moduls E, wenn sie folgende *universelle Eigenschaft* hat: Zu jeder n-linearen alternierenden Abbildung $\varphi\colon E^n \to F$ gibt es genau eine lineare Abbildung $\Phi\colon \Lambda^n(E) \to F$ mit der Eigenschaft $\Phi\lambda = \varphi$. Oft wird auch nur der Modul $\Lambda^n(E)$ n-te äußere Potenz von E genannt. ◇

Wie beim Tensorprodukt folgt aus der universellen Eigenschaft, daß eine n-te äußere Potenz bis auf eindeutige Isomorphie bestimmt ist. Wir setzen $\lambda(e_1, \ldots, e_n) = e_1 \wedge e_2 \wedge \ldots \wedge e_n$. Als erste äußere Potenz können und wollen wir $\Lambda^n(E) = E$ und $\lambda = \mathrm{id}$ nehmen.

(3.2) Satz. *Zu jedem $n \in \mathbb{N}$ und jedem R-Modul E gibt es eine n-te äußere Potenz.*

Beweis. In dem n-fachen Tensorprodukt von E mit sich selbst $\bigotimes^n E$ betrachten wir den Untermodul N, der von allen Tensoren $e_1 \otimes e_2 \otimes \cdots \otimes e_n$ erzeugt wird, die an mindestens zwei Stellen $i \neq j$ gleiche Elemente $e_i = e_j$ haben. Wir setzen $\Lambda^n(E) = (\bigotimes^n E)/N$ und definieren $\lambda\colon E^n \to \bigotimes^n E \to \Lambda^n(E)$ als die Zusammensetzung des Tensorprodukts und der kanonischen Quotientabbildung. Nach Konstruktion ist dann λ eine n-lineare alternierende Abbildung. Ist $\varphi\colon E^n \to F$ alternierend und n-linear, so gibt es zunächst ein $\varphi'\colon \bigotimes^n E \to F$ als lineare Abbildung nach der universellen Eigenschaft des Tensorproduktes. Da φ alternierend ist, liegt N im Kern von φ' und deshalb induziert φ eine lineare Abbildung $\Phi\colon \Lambda^n(E) \to F$, die wie gewünscht $\Phi\lambda = \varphi$ erfüllt. Die Eindeutigkeit von Φ folgt daraus, daß $\lambda(E^n)$ den Modul $\Lambda^n(E)$ erzeugt. □

Ist $\varphi\colon E \to F$ eine lineare Abbildung, so gibt es genau eine lineare Abbildung $\Lambda^n(\varphi)\colon \Lambda^n(E) \to \Lambda^n(F)$, auch als n-te äußere Potenz von φ bezeichnet, die das Diagramm

$$\begin{array}{ccc} E^n & \xrightarrow{\varphi^n} & F^n \\ \downarrow{\scriptstyle\lambda} & & \downarrow{\scriptstyle\lambda} \\ \Lambda^n(E) & \xrightarrow{\Lambda^n(\varphi)} & \Lambda^n(F) \end{array}$$

kommutativ macht. Wie beim Tensorprodukt folgt das unmittelbar aus der universellen Eigenschaft. Es gelten die Regeln

$$\Lambda^n(\mathrm{id}) = \mathrm{id}, \quad \Lambda^n(\varphi \circ \psi) = \Lambda^n(\varphi) \circ \Lambda^n(\psi).$$

(3.3) Satz. *Es gibt genau eine bilineare Abbildung*

$$\Lambda^r(E) \times \Lambda^s(E) \to \Lambda^{r+s}(E),$$

die $(e_1 \wedge \ldots \wedge e_r,\ f_1 \wedge \ldots \wedge f_s)$ auf $e_1 \wedge \ldots \wedge e_r \wedge f_1 \wedge \ldots \wedge f_s$ abbildet. Sie wird mit $(x, y) \mapsto x \wedge y$ bezeichnet und äußeres Produkt *genannt.*

Beweis. Für gegebene $f_1, \ldots, f_s$ ist die Abbildung

$$(e_1, \ldots, e_r) \mapsto e_1 \wedge \ldots \wedge e_r \wedge f_1 \wedge \ldots \wedge f_s$$

alternierend. Also gibt es

$$\Lambda^r(E) \times E^s \to \Lambda^{r+s}(E), \quad (e_1 \wedge \ldots \wedge e_r, f_1, \ldots, f_s) \mapsto e_1 \wedge \ldots \wedge e_r \wedge f_1 \wedge \ldots \wedge f_s$$

linear in der ersten Variablen. Bei fester erster Komponente ist die Abbildung alternierend, also gibt es $\Lambda^r(E) \times \Lambda^s(E) \to \Lambda^{r+s}(E)$, linear in der zweiten Variablen, wie im Satz behauptet. □

Das äußere Produkt wird auch *Graßmann-Produkt* genannt.

(3.4) Eigenschaften des äußeren Produkts.

(1) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$
(2) $x \wedge y = (-1)^{rs} y \wedge x$, *falls* $x \in \Lambda^r$ *und* $y \in \Lambda^s$.
(3) $\Lambda^{r+s}(\varphi)(x \wedge y) = \Lambda^r(\varphi)(x) \wedge \Lambda^s(\varphi)(y)$, *falls* $x \in \Lambda^r$, $y \in \Lambda^s$ *und* $\varphi: E \to F$ *linear ist.*

Diese Aussagen folgen fast unmittelbar aus den Definitionen. □

Wir konstruieren jetzt mit Hilfe des äußeren Produkts einen Ring. Dazu müssen wir nur künstlich sicherstellen, daß das äußere Produkt nicht aus der betrachteten Menge herausführt. Wir setzen $\Lambda^0(E) = R$ und definieren das äußere Produkt $\Lambda^0(E) \times \Lambda^n(E) \to \Lambda^n(E) \leftarrow \Lambda^n(E) \times \Lambda^0(E)$ als skalare Multiplikation. Sodann setzen wir

$$\Lambda(E) := \bigoplus_{r \geq 0} \Lambda^r(E).$$

Aus der Addition und dem äußeren Produkt erhalten wir auf $\Lambda(E)$ eine Ringstruktur. Die Multiplikation von Summen von Elementen, die in verschiedenen $\Lambda^r(E)$ liegen, wird durch das Distributivgesetz definiert. Außerdem ist $\Lambda(E)$ ein R-Modul und die Multiplikation mit einem Element (von links oder rechts) ist R-linear. Solche Strukturen nennt man R-Algebren, und wir sprechen deshalb von der *äußeren Algebra* $\Lambda(E)$. Der nächste Satz stellt die *universelle Eigenschaft* der äußeren Algebra bereit. Er verwendet die kanonische Inklusion

$$i: E = \Lambda^1(E) \to \Lambda(E);$$

sie ist R-linear und hat die Eigenschaft $i(e)^2 := i(e) \wedge i(e) = 0$ für alle $e \in E$.

(3.5) Satz. *Sei A eine R-Algebra mit Einselement und $\varphi: E \to A$ eine R-lineare Abbildung mit der Eigenschaft $\varphi(e)^2 = 0$ für alle $e \in E$. Dann gibt es genau einen Homomorphismus $h: \Lambda(E) \to A$ von R-Algebren mit $hi = \varphi$.*

Beweis. Für $p \geq 2$ ist die Abbildung

$$E^p \to A, \quad (x_1, \ldots, x_p) \mapsto \varphi(x_1)\varphi(x_2) \ldots \varphi(x_p)$$

p-linear und alternierend, weil aus $\varphi(e)^2 = 0$ nämlich zunächst für beliebige $x, y \in E$ die Relation $\varphi(x)\varphi(y) + \varphi(y)\varphi(x) = 0$ folgt. Sie induziert eine lineare Abbildung $h^p: \Lambda^p(E) \to A$. Wir definieren h^0 und h^1 durch $h^0(r) = r \cdot 1$ und $h^1 = \varphi$. Sei $h: \Lambda(E) \to A$ als lineare Abbildung dadurch festgelegt, daß die Einschränkung auf $\Lambda^p(E)$ gerade h^p ist. Die Abbildung h ist auch mit der Multiplikation verträglich. Das zeigt man zunächst für Elemente der Form $u = x_1 \wedge \ldots \wedge x_p$ und $v = y_1 \wedge \ldots \wedge y_q$, und dann folgt die Verträglichkeit wegen der Linearität für Summen solcher Elemente. Damit ist die Existenz von h mit den angegebenen Eigenschaften gezeigt. Die Eindeutigkeit folgt daraus, daß $i(E)$ die Algebra $\Lambda(E)$ vermöge Addition und Multiplikation erzeugt. □

Seien E und F zwei R-Moduln. Auf dem Tensorprodukt $\Lambda(E) \otimes \Lambda(F)$ definieren wir eine Multiplikation wie folgt: Ist $u \in \Lambda^p(E)$, so schreiben wir $p = |u|$. Dann setzen wir

(3.6) $$(u \otimes v)(a \otimes b) = (-1)^{|v||a|}(u \wedge a) \otimes (v \wedge b).$$

Für Summen von *homogenen Elementen*, d. h. solchen, die in $\Lambda^p(E) \otimes \Lambda^q(F)$-Teilen liegen, wird die Multiplikation über das Distributivgesetz definiert. Damit wird $\Lambda(E) \otimes \Lambda(F)$ zu einer assoziativen R-Algebra mit Einselement.

Wir verwenden die kanonischen Inklusionen i, j und Projektionen p, q

$$i\colon E \to E \oplus F, \quad j\colon F \to E \oplus F, \quad p\colon E \oplus F \to E, \quad q\colon e \oplus F \to F.$$

Wir definieren $\varphi\colon \Lambda(E) \times \Lambda(F) \to \Lambda(E \oplus F)$ durch $\varphi(u, v) = (\Lambda i)(u) \wedge (\Lambda j)(v)$. Dann induziert φ eine lineare Abbildung

(3.7) $$f\colon \Lambda(E) \otimes \Lambda(F) \to \Lambda(E \oplus F)$$

mit der Eigenschaft $f(u \otimes v) = \varphi(u, v)$. Diese Abbildung ist sogar ein Homomorphismus von Algebren. Sei nämlich $u \in \Lambda(E),\ v \in \Lambda^q(F), u' \in \Lambda^r(E), v' \in \Lambda(F)$. Dann gilt:

$$\begin{aligned} f((u \otimes v)(u' \otimes v') &= (-1)^{rq} f((u \wedge u') \otimes (v \wedge v')) \\ &= (-1)^{rq} \Lambda i(u \wedge u') \wedge \Lambda j(v \wedge v') \\ &= (-1)^{rq} \Lambda i(u) \wedge \Lambda i(u') \wedge \Lambda j(v) \wedge \Lambda j(v') \\ &= \lambda i(u) \wedge \Lambda i(v) \wedge \Lambda i(u') \wedge \Lambda j(v) \wedge \Lambda j(v') \\ &= f(u \otimes v) \wedge f(u' \otimes v'). \end{aligned}$$

Um diese Gleichheit zu beweisen, war es nötig, auf $\Lambda(E) \otimes \Lambda(F)$ die Produktbildung mit dem Vorzeichen in (8.6) zu definieren.

(3.8) Satz. *Die Abbildung* (8.7) *ist ein Isomorphismus von Algebren. Für jedes* $n \geq 0$ *liefert er einen Isomorphismus*

(3.9) $$\Lambda^n(E \oplus F) \cong \bigoplus_{p+q=n} \Lambda^p(E) \otimes \Lambda^q(F).$$

Beweis. Wir konstruieren eine Umkehrabbildung. Sei $\eta\colon E \oplus F \to \Lambda(E) \otimes \Lambda(F)$ definiert durch

$$\eta(x, y) = x \otimes 1 + 1 \otimes y \in (\Lambda^1(E) \otimes \Lambda^0(F)) \oplus (\Lambda^0(E) \otimes \Lambda^1(E))$$

für $(x, y) \in E \times F$. Dann gilt $\eta(x, y)^2 = (x \otimes 1 + 1 \otimes y)^2 = x \wedge x \otimes 1 + x \otimes y - x \otimes y + 1 \otimes y \wedge y$. Es ist aber $x \wedge x = 0 = y \wedge y$.

Nach (8.5) induziert η einen Homomorphismus von Algebren $h\colon \Lambda(E \oplus F) \to \Lambda(E) \otimes \Lambda(F)$, der η fortsetzt. Es gilt $fh(x, y) = f(x \otimes 1 + 1 \otimes y) = (x, y)$; wegen der universellen Eigenschaft von $\Lambda(E \otimes F)$ ist also $fh = \mathrm{id}$. Es gilt $hf(x \otimes 1) = hi(x) = x \otimes 1$, $hf(1 \otimes y) = hj(y) = 1 \otimes y$. Da die Elemente aus $E \otimes R$ und $R \otimes F$ die Algebra $\Lambda(E) \otimes \Lambda(F)$ erzeugen, ist auch $hf = \mathrm{id}$. □

(3.10) Satz. *Sei E ein freier R-Modul mit Basis $b_1, \ldots, b_n$. Dann ist $\Lambda^r(E)$ ein freier R-Modul mit Basis $b_{i_1} \wedge \ldots \wedge b_{i_r}$, $i_1 < i_2 < \ldots < i_r$, hat also den Rang $\binom{n}{r}$.*

BEWEIS. Sei $n = 1$. Dann ist $\Lambda^0(E) = R$ und $\Lambda^1(E) = E$. Für $p \geq 2$ wird $\Lambda^p(E)$ von $b \wedge \ldots \wedge b$ (p Faktoren) erzeugt, ist also der Nullmodul ($b = b_1$). Ist E frei vom Rang n, so gilt $E = E' \otimes F'$, wobei E' von $b_1, \ldots, b_{n-1}$ und F' von b_n erzeugt wird. Wir erhalten aus (8.9)

$$\Lambda^n(E) \cong \Lambda^{n-1}(E') \otimes \Lambda^1(F'), \tag{3.11}$$

wenn wir induktiv annehmen, daß für einen Modul E' mit $n-1$ Basiselementen $\Lambda^p(E')$ für $p \geq n$ der Nullmodul ist. Nehmen wir ferner induktiv an, daß $\Lambda^{n-1}(E')$ frei vom Rang 1 ist, so folgt aus (8.11) dasselbe für $\Lambda(E)$. Man erkennt leicht, wegen der alternierenden Eigenschaft der äußeren Muliplikation, daß $\Lambda^r(E)$ von den Elementen $b_{i_1} \wedge \ldots \wedge b_{i_r}$ erzeugt wird. Ist aber eine lineare Relation

$$\sum_{i_1 < \ldots < i_r} \alpha(i_1, \ldots, i_r) b_{i_1} \wedge \ldots \wedge b_{i_r} = 0$$

gegeben, so führt zum Beispiel äußere Multiplikation mit $b_{n-r+1} \wedge \ldots \wedge b_n$ zu $\alpha(1, \ldots, r) = 0$, da wir schon wissen, daß $b_1 \wedge \ldots \wedge b_n$ Basiselement von $\Lambda^n(E)$ ist. Also sind die fraglichen Elemente linear unabhängig. □

(3.12) Beispiel. (8.10) liefert einen Beweis für die Invarianz der Basislänge eines freien Moduls, da $\Lambda^n(E)$ unabhängig von einer Basis definiert ist. ◇

(3.13) Beispiel. Sei E ein freier Modul vom Rang n. Da $\Lambda^n(E)$ den Rang 1 hat, ist auch der Modul der n-linearen alternierenden Abbildungen $E^n \to R$ frei vom Rang 1. Das ist die Existenz und Eindeutigkeit der Determinantenfunktion, hier für beliebige kommutative Ringe formuliert und bewiesen. Insbesondere ist es jetzt leicht, in bekannter Weise den Produktsatz für Determinanten zu beweisen und die Determinante eines linearen Endomorphismus eines freien endlich erzeugten Moduls basisfrei zu definieren. ◇

Als weitere Anwendung zeigen wir die Eindeutigkeit der Ideale, die bei der Zerlegung von Torsionsmoduln über Hauptidealringen auftraten. Ist M ein R-Modul, so heißt das Ideal

$$\operatorname{Ann}(M) = \{r \in R \mid \quad \text{für alle} \quad m \in M \quad \text{ist} \quad rm = 0\}$$

der *Annullator* des Moduls M. Es gilt offenbar

$$\operatorname{Ann}(M_1 \oplus M_2) = \operatorname{Ann}(M_1) \cap \operatorname{Ann}(M_2)$$

und $\operatorname{Ann}(R/I) = I$ für ein Ideal I.

(3.14) Satz. *Seien $I_1 \subset I_2 \subset \ldots \subset I_n \neq R$ Ideale von R. Sei E die direkte Summe der Moduln R/I_j, $j = 1, \ldots, n$. Dann it I_p der Annullator des Moduls $\Lambda^p(E)$.*

BEWEIS. Es ist $\Lambda^0(R/I_j) = R$, $\Lambda^1(R/I_j) = R/I_j$ und $\Lambda^p(R/I_j) = 0$ für $p \geq 2$. Nach (8.8) gilt deshalb

$$\Lambda(E) = \Lambda(\bigotimes_j R/I_j) = \bigotimes_j \Lambda(A/I_j) = \bigotimes_j (A \oplus A/I_j).$$

Es folgt speziell

$$\Lambda^p(E) \cong \bigoplus_{H\subset\{1,\dots,n\},|H|=p} (\bigotimes_{j\in H} R/I_j) \cong \bigoplus_{H\subset\{1,\dots,n\},|H|=p} (R/\bigcup_{j\in H} I_j),$$

letzteres nach (1.23). Der Durchschnitt der Ideale $\bigcup_{j\in H} I_j$ für $H \subset \{1,\dots,n\}$, $|H| = p$ ist I_p. Es folgt die Behauptung. □

7 Polynome

1 Polynomalgebren

Sei K ein kommutativer Ring. Die Polynomalgebra $K[x]$ ist additiv der freie K-Modul über der Menge $N = \{1 = x^0, x = x^1, x^2, x^3, \ldots\}$. Die bilineare assoziative Multiplikation mit Eins wird durch das Produkt $(x^k, x^l) \mapsto x^{k+l}$ auf den Basiselementen definiert. Die Elemente von $K[x]$ heißen *Polynome* über K in der Unbestimmten x. Ist $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = f$ ein Polynom mit $a_n \neq 0$, so heißt $n = d(f)$ der *Grad* von f und $\ell(f) = a_n$ der *Leitkoeffizient* von f. Für das Nullpolynom setzt man $d(0) = -\infty$. Ist $\ell(f) = 1$, so heißt f *normiert*. Wir fassen K als Unterring von $K[x]$ der sogenannten konstanten Polynome, d. h. der Polynome vom Grad höchsten Null, auf. Es gelten offenbar die folgenden Regeln, wobei wir bei (1) voraussetzen, daß $\ell(f)$ und $\ell(g)$ keine Nullteiler sind.

(1.1)
$$\begin{array}{ll} (1) & d(f \cdot g) = d(f) + d(g). \\ (2) & d(f + g) \leq \mathrm{Max}(d(f), d(g)). \\ (3) & \ell(fg) = \ell(f)\ell(g). \end{array}$$

Damit (1.1.1) ausnahmslos gilt, ist die zunächst überraschende Festsetzung $d(0) = -\infty$ nötig (mit der üblichen Vereinbarung $-\infty + a = -\infty$ für alle $a \in \mathbb{R}$).

Sei K nullteilerfrei. Dann ist auch $K[x]$ nullteilerfrei, denn aus (3) entnimmt man, daß aus $f \cdot g = 0$ folgt: $f = 0$ oder $g = 0$.

Ist K Unterring von L, so wird $K[x]$ in kanonischer Weise als Unterring von $L[x]$ angesehen. Diese Tatsache verwenden wir meist stillschweigend. Grad und Leitkoeffizient ändern sich bei diesem Standpunktwechsel nicht.

(1.2) Satz. *Der Polynomring $K[x]$ hat die folgende universelle Eigenschaft: Zu jedem Ringhomomorphismus $\varphi\colon K \to L$ und jedem Element $y \in L$ gibt es genau einen Ringhomomorphismus $\Phi\colon K[x] \to L$ mit $\Phi(x) = y$ und $\Phi|K = \varphi$. Fassen wir $K[x]$ als K-Algebra auf, so entsprechen die unitalen K-Algebra-Homomorphismen $\varphi\colon K[x] \to S$ in eine K-Algebra S vermöge $\varphi \mapsto \varphi(x)$ den Elementen von S.*

Beweis. Es bleibt keine andere Wahl, als Φ durch

$$\Phi(a_0 + a_1x + a_2x^2 + \cdots) = \varphi(a_0) + \varphi(a_1)y + \varphi(a_2)y^2 + \cdots$$

zu definieren. Die Homomorphie ist leicht nachzurechnen. □

Eine Anwendung dieser universellen Eigenschaft ist das „Einsetzen von Werten“ in ein Polynom, also die Betrachtung eines Polynoms als Funktion: Ist L ein Erweiterungsring von K, so erhalten wir zu jedem $y \in L$ einen Homomorphismus $K[x] \to L$, der x auf y abbildet und die Koeffizienten beläßt. Insbesondere kann man $K[x] = L$ wählen und Polynome in Polynome einsetzen. Durch $x \mapsto x - a$ für $a \in K$ wird ein Automorphismus von $K[x]$ gegeben: Jedes Polynom läßt sich nach Potenzen von $x - a$ entwickeln.

Durch Wiederholung der Konstruktion erhalten wir Polynomringe in mehreren Unbestimmten $(K[x_1])[x_2] := K[x_1, x_2]$ und $K[x_1, \ldots, x_n]$. Die universelle Eigenschaft des letzteren ist: Sei $\varphi\colon K \to L$ ein Homomorphismus in einen kommutativen Ring L und seien $y_1, \ldots, y_n$ beliebige Elemente aus L. Dann gibt es genau einen Homomorphismus $\Phi\colon K[x_1, \ldots, x_n] \to L$, der auf K mit φ übereinstimmt und x_j auf y_j abbildet.

Mit Polynomen kann man ähnlich wie mit ganzen Zahlen rechnen. Wir demonstrieren diesen Sachverhalt durch die elementare Teilbarkeitslehre für Polynome.

(1.3) Division mit Rest. *Sei K nullteilerfrei. Für $f, g \in K[x]$ mit $\ell(g) \in K^*$ gibt es genau eine Darstellung der Form $f = qg + r, \quad d(r) < d(g)$. Das gilt insbesondere für Körper K und $g \neq 0$.*

Beweis. Eindeutigkeit. Sind $f = q_1 g + r_1 = q_2 g + r_2$ zwei solche Darstellungen, so folgt $(q_1 - q_2)g = r_2 - r_1$. Wegen $d(r_2 - r_1) < d(g)$ und (1.1) kann die letzte Gleichheit nur bestehen, wenn $q_1 - q_2 = 0$ ist. Dann ist aber auch $r_2 - r_1 = 0$.
Existenz. Induktion nach $d(f)$. Ist $d(f) < d(g)$, so setzen wir $g = 0$ und $r = f$. Andernfalls sei $f = ax^{n+k} + \cdots$, $g = bx^n + \cdots$ und $a = \ell(f)$, $b = \ell(g)$. Dann hat $f - ab^{-1}x^k g$ einen kleineren Grad als f und besitzt deshalb eine Darstellung

$$f - ab^{-1}x^k g = q_1 g + r, \quad d(r) < d(g).$$

Wir rechnen um und erhalten wie gewünscht $f = (ab^{-1}x^k + q_1)g + r$. □

(1.4) Folgerung. *Sei K nullteilerfrei. Ist $\alpha \in K$ eine* Wurzel (= Nullstelle) *des Polynoms $f \in K[x]$, d. h. ist $f(\alpha) = 0$, so gilt $f = g \cdot (x - \alpha)$ für ein $g \in K[x]$.*

Beweis. Ist $f = 0$, so setzen wir $g = 0$. Andernfalls ist f nicht konstant, also $d(f) \geq 1$. Wir können nach (1.3) $f = g \cdot (x - \alpha) + r$ mit $d(r) < 1$ schreiben. Dann ist aber r konstant, und Einsetzen von α in die Gleichung liefert $r = 0$. □

In einer Produktzerlegung $f = g \cdot (x - \alpha)$ heißt $x - \alpha$ *Linearfaktor* von f. Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes nichtkonstante Polynom aus $K[x]$ eine Wurzel in K hat. Ist K algebraisch abgeschlossen, so kann man das Abspalten von Linearfaktoren immer durchführen und wiederholen und erhält für ein nichtkonstantes Polynom $f \in K[x]$ eine Produktdarstellung

$$\textbf{(1.5)} \qquad f = a(x - \alpha_1)^{n(1)}(x - \alpha_2)^{n(2)} \ldots (x - \alpha_r)^{n(r)},$$

worin die $\alpha_1, \ldots, \alpha_r$ die verschiedenen Wurzeln von f sind, a der Leitkoeffizient ist und $n = n(1) + n(2) + \cdots + n(r)$ der Grad von f. Man nennt $n(j)$ die *Vielfachheit* der Wurzel α_j. Von einem Polynom der Form (1.5) sagt man, es *zerfalle in Linearfaktoren*. Mit Vielfachheiten gezählt, hat ein Polynom vom Grad n über einem Körper also höchstens n Nullstellen. Anzahl und Art der Linearfaktoren ist durch f eindeutig bestimmt. Das wird sich sogleich in allgemeinerem Zusammenhang aus der eindeutigen Primfaktorzerlegung zeigen.

(1.6) Satz. *Der Polynomring $K[x]$ über einem Körper K ist ein Hauptidealring. Ist $I \neq 0$ ein Ideal und $p \in I$ ein Element minimalen Grades, so ist $I = (p)$.*

BEWEIS. Sei $f \in I$ gegeben. Man dividiert f durch p mit Rest $f = ap + r$. Falls die Division nicht aufgeht, ergibt sich ein Widerspruch zur Minimaleigenschaft von p, denn $r = f - ap \in I$. □

Nach diesem Satz können wir Ergebnisse aus der Theorie der Hauptidealringe anwenden (??). Die Primelemente in $K[x]$ heißen *irreduzible Polynome*. Wir haben also insbesondere Existenz und Eindeutigkeit der Zerlegung in irreduzible Faktoren, ferner größte gemeinsame Teiler GGT und kleinste gemeinsame Vielfache KGV. Wir bemerken dazu:

(1.7) Notiz. *Sei $K \subset L$ eine Körpererweiterung. Sei $d \in K[x]$ ein* GGT *der Polynome $f, g \in K[x]$. Wenn wir f und g als Polynome in $L[x]$ auffassen, so ist immer noch d der* GGT.

BEWEIS. Es gibt eine Darstellung $d = pf + qg$ mit $p, q \in K[x]$. Ein gemeinsamer Teiler von f und g in $L[x]$ teilt deshalb d. Umgekehrt ist d auch ein gemeinsamer Teiler von f und g in $L[x]$ und teilt deshalb den darin gebildeten GGT. □

Die praktische Berechnung des GGT erfolgt wie bei den ganzen Zahlen mit Hilfe des Euklidischen Algorithmus.

(1.8) Euklidischer Algorithmus. Seien $f_1, f_2 \in K[x]$ beide von Null verschieden, und sei $d(f_2) \leq d(f_1)$. Der *Euklidische Algorithmus* ist die folgende Sequenz von Divisionen mit Rest

$$\begin{aligned} f_1 &= q_1 f_2 + f_3 \qquad && d(f_3) < d(f_2), \\ f_2 &= q_2 f_3 + f_4 \qquad && d(f_4) < d(f_3), \\ &\vdots \\ f_{n-1} &= q_{n-1} f_n + 0. \end{aligned}$$

Weil die Grade abnehmen, muß irgendwann der Rest Null auftreten, womit der Algorithmus dann endet. Durch Rückwärtsrechnen in diesem Algorithmus findent man eine Darstellung des GGT d von f_1 und f_2 als Linearkombination $d = a_1 f_1 + a_2 f_2$ mit $a_i \in K[x]$. ◇

2 Potenzreihen

Sei R ein kommutativer Ring und $R[[x]]$ der R-Modul aller Funktionen $f\colon \mathbb{N}_0 \to R$. Wir schreiben eine Funktion f in form einer Potenzreihe $\sum_{n\geq 0} f(n)x^n$. Wir multiplizieren Potenzreihen nach der Formel

$$(\sum a_n x^n)(\sum b_n x^n) = \sum c_n x^n, \qquad c_n = \sum_{u+v=n} a_u b_v,$$

wie man es aus der Analysis gewohnt ist. Das Produkt ist assoziativ und R-bilinear. Damit wird $R[[x]]$ zu einer R-Algebren, genannt Algebra der *formalen Potenzreihen* über R. Die Polynomalgebra $R[x]$ ist darin enthalten. Ist das konstante Glied a_0 einer Potenzreihe $u = \sum a_n x^n$ in R eine Einheit, so kann man

die Gleichungen $(\sum a_n x^n)(\sum b_n x^n) = 1$ induktiv nach den b_n auflösen; also ist u eine Einheit in $R[[x]]$. Zum Beispiel hat $1 - x$ das Inverse $1 + x + x^2 + x^3 + \cdots$, wie gewohnt.

3 Symmetrische Polynome

Sei R ein kommutativer Ring und $S = R[x_1, \ldots, x_n]$ der Polynomring darüber in n Unbestimmten $x_1, \ldots, x_n$. Eine Permutation der Unbestimmten liefert einen Automorphismus von S. Dadurch erhalten wir eine Operation der symmetrischen Gruppe S_n auf S. Ein Polynom $f \in S$ heißt *symmetrisch*, wenn es in der Fixpunktmenge von S_n liegt.

Die *elementarsymmetrischen Polynome* $\sigma_1, \ldots, \sigma_n \in S$ sind definiert als

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + \cdots + x_n \\ \sigma_2 &= x_1x_2 + x_1x_3 + x_2x_3 + \cdots = \sum_{i<j} x_ix_j \\ \sigma_k &= \sum_{i_1<\cdots<i_k} x_{i_1}x_{i_2}\ldots x_{i_k}.\end{aligned}$$

Das Polynom $(x - x_1)(x - x_2)\cdots(x - x_n) \in S[x]$ hat die Form

$$x^n - \sigma_1 x^{n-1} + \sigma_2^{n-2} - \cdots + (-1)^n\sigma_n.$$

Die elementarsymmetrischen Polynome liefern also die Koeffizienten eines Polynoms aus seinen Nullstellen.

Es stellt sich heraus, daß jedes symmetrische Polynom in eindeutiger Weise ein Polynom in den elementarsymmetrischen Polynomen ist. Mit anderen Worten:

(3.1) Satz. *Der durch $s_i \mapsto \sigma_i$ bestimmte Homomorphismus $R[s_1, \ldots, s_n] \to R[x_1, \ldots, x_n]$ ist ein Isomorphismus auf den Unterring der symmetrischen Polynome.*

Beweis. Induktion nach n. Für $n = 1$ ist nichts zu zeigen. Sei $f \in S$ symmetrisch. Wir setzen darin $x_n = 0$ und erhalten ein Polynom f^0 in $x_1, \ldots, x_{n-1}$, das symmetrisch in diesen Unbestimmten ist und deshalb nach Induktionsvoraussetzung ein Polynom $g(\sigma_1^0, \ldots, \sigma_{n-1}^0)$ in den elementarsymmetrischen Polynomen σ_j^0 von $x_1, \ldots, x_{n-1}$. Das Polynom

$$p(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - g(\sigma_1, \ldots, \sigma_{n-1})$$

ist als Differenz symmetrischer Polynome symmetrisch. Da $p(x_1, \ldots, x_{n-1}, 0) = 0$ ist, ist jedes Monom, das in p vorkommt, ein Vielfaches von x_n. Wegen der Symmetrie kommen in p mit jedem Monom auch alle durch Permutation der Unbestimmten gewonnenen vor. Also ist jedes Monom durch s_n teilbar, d.h. wir haben eine Darstellung

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, s_{n-1}) + s_n h(x_1, \ldots, s_n)$$

mit symmetrischem h. Durch eine weitere Induktion über den Grad können wir annehmen, daß h ein Polynom in den σ_j ist. Damit ist die Surjektivität gezeigt.

Sei $\varphi \in R[s_1, \ldots, s_n]$ und $\varphi(\sigma_1, \ldots, \sigma_n) = 0$. Setzen wir $x_n = 0$, so ist also $\varphi(\sigma_1^0, \ldots, \sigma_{n-1}^0, 0) = 0$. Durch Induktion nach n haben wir $\varphi(s_1, \ldots, s_{n-1}, 0) = 0$. Also gilt $\varphi(s_1, \ldots, s_{n-1}, s_n) = s_n\psi(s_1, \ldots, s_n)$. Aus $\sigma_n\psi(\sigma_1, \ldots, \sigma_n) = 0$ folgt aber $\psi(\sigma_1, \ldots, \sigma_n) = 0$, und durch eine weitere Induktion über den Grad haben wir $\psi = 0$ und damit auch $\varphi = 0$. □

Wir geben dem elementarsymmetrischen Polynom σ_j das Gewicht j und einem Monom

$$\sigma_1^{a(1)}\sigma_2^{a(2)} \ldots \sigma_n^{a(n)}$$

das *Gewicht* $k = \Sigma_j ja(j)$; als Polynom in $x_1, \ldots, x_n$ hat es dann den Grad k. Die homogenen Komponenten eines symmetrischen Polynoms sind ebenfalls symmetrisch. Wird ein homogenes symmetrisches Polynom vom Grad k durch die σ_j ausgedrückt, so hat darin jedes Monom das Gewicht k.

Das Polynom $\prod_{i<j}(x_i - x_j)^2$ ist symmetrisch. Wir nennen es die *Diskriminante* $\Delta(x_1, \ldots, x_n)$ von $x_1, \ldots, x_n$. Sind die x_j nicht Unbestimmte, sondern irgendwelche Elemente eines Integritätsbereiches, so ist $\Delta \neq 0$ genau dann, wenn die $x_1, \ldots, x_n$ paarweise verschieden sind. Sei $\Delta(x_1, \ldots, x_n)$ als Polynom in den σ_j gleich $D(\sigma_1, \ldots, \sigma_n)$.

Sei $f = x^n - a_1x^{n-1} + a_2x^{n-2} - \ldots (-1)^n a_n \in k[x]$ ein Polynom über dem Körper k. Genau dann hat f mehrfache Nullstellen in einem Erweiterungskörper, wenn $D(a_1, \ldots, a_n) = 0$ ist.

Es ist $(x_1 - s_2)^2 = \sigma_1^2 - 4\sigma_2$. Für $n = 3$ ist das Resultat schon kompliziert.

(3.2) Satz. *Es gilt*

$$D(\sigma_1, \sigma_2, \sigma_3) = \sigma_1^2\sigma_2^2 - 4\sigma_2^3 - 4\sigma_1^3\sigma_3 - 27\sigma_3^2 + 18\sigma_1\sigma_2\sigma_3.$$

Beweis. Wir betrachten $\Delta(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$. Haben wir $D(s_1, \ldots, s_n) \in \mathbb{Z}[s_1, \ldots, s_n]$ bestimmt, so gilt das Resultat über jedem Ring. Da $\Delta(x_1, x_2, x_3)$ den Totalgrad 6 hat, muß $D(s_1, s_2, s_3)$ eine Linearkombination der Monome vom Gewicht 6

$$s_1^6,\ s_1^4s_2,\ s_1^3s_3,\ s_1^2s_2^2,\ s_1s_2s_3,\ s_2^3, s_3^2$$

sein. Wir setzen an

$$D(0, s_2, s_3) = \alpha s_2^3 + \beta s_3^2.$$

Das Polynom $x^3 - 1$ hat die Nullstellen $1, \zeta, \zeta^2$ mit $\zeta = \exp(2\pi i/3)$. Es ist

$$\begin{aligned}(1-\zeta)^2(1-\zeta^2)^2(\zeta-\zeta^2)^2 &= (1-\zeta)^2\zeta^4(1-\zeta)(\zeta^2(1-\zeta)^2 \\ &= (1-\zeta)^6 = (1-2\zeta+\zeta^2)^3 = (1+\zeta+\zeta^2-3\zeta)^3 \\ &= (-3\zeta)^3 = -27.\end{aligned}$$

Also ist $D(0,0,1) = \beta \cdot 1^3 = -27$. Das Polynom $x^3 - x$ hat die Nullstellen $0, 1, -1$. Es ist

$$(1-0)^2(-1-0)^2(1+1)^2 = -4.$$

Also ist $D(0,1,0) = -\alpha = 4$.

Ist $x^3 + ax^2 + bx + c$ gegeben, so liefert die Substitution $x = y + u$

$$\begin{array}{lllllll} y^3 & + & 3uy^2 & + & 3u^2y & + & u^3 \\ & + & ay^2 & + & 2auy & + & au^2 \\ & & & + & by & + & bu \\ & & & & & + & c \end{array}$$
$$= y^3 + (3u+a)y^2 + (3u^2 + 2au + b)y + u^3 + au^2 + bu + c.$$

Für $u = -\frac{a}{3}$ verschwindet also der lineare Term. Die Diskriminante ändert sich bei dieser Substitution nicht, da nur die Differenzen von Nullstellen eingehen. Also ist die Diskriminante nach dem schon Gezeigten gleich

$$-4\left(-\frac{a^2}{3} + b\right)^3 - 27\left(\frac{2a^3}{27} - \frac{ab}{3} + c\right)^2.$$

Darin ist der Koeffizient von c gleich $-4a^3 + 18ab$. Das liefert zwei weitere Glieder von D. Der Koeffizient von b^2 ist a^2; das liefert den letzten Term von D. Man sieht, daß a^6 und a^4b nicht vorkommen. □

Wir betrachten verschiedene Sorten von symmetrischen Polynomen. Dazu setzen wir

$$E(t) = \prod_{i=1}^{n}(1 + x_i t) = \sum_{r=0}^{n} s_i t^r,$$

wobei $s_0 = 1$ und s_i das i-te elementarsymmetrische Polynom ist. Sei

$$H(t) = \prod_{i=1}^{n} \frac{1}{1 - x_i t} = \prod_{i=1}^{n}(1 + x_i t + x_i^2 t^2 + \cdots) = \sum_{r \geq 0} h_r t^r.$$

Wir sehen, daß h_r die Summe aller Monome vom Totalgrad r ist. Wegen $E(t)H(-t) = 1$ folgt

$$\sum_{r=0}^{t} (-1)^r h_r e_{t-r} = 0, \qquad t \geq 1.$$

Die logarithmische Ableitung von $H(t)$ ist

$$\frac{H'(t)}{H(t)} = \sum_{i=1}^{n} \frac{x_i}{1 - x_i t} = \sum_{i=1}^{n} x_i \left(\sum_{k \geq 0} x_i^k t^k\right) = \sum_{k \geq 0} p_{k+1} t^k$$

mit der Potenzsumme $p_k = \sum_{i=1}^{n} x_i^k$.

Die logarithmische Ableitung der Identität $E(t)H(-t) = 1$ liefert

$$\frac{E'(t)}{E(t)} = \frac{H'(-t)}{H(t)} = P(-t).$$

Die Identität $E'(t) = E(t)P(-t)$ liefert durch Koeffizientenvergleich die *Newtonschen Formeln*

$$\textbf{(3.3)} \qquad \sum_{i+j=r} (-1)^{i-1} p_i \sigma_j = r s_r$$

wobei $\sigma_t = 0$ für $t > n$ gesetzt wird. Das ist eine Rekursionsformel zur Berechnung der p_k. Es ist $p_1 = s_1$, und $p_2 - p_1 s_1 + 2s_2 = 0$ liefert $p_2 = s_1^2 - 2s_2$.

(3.4) Satz. *Sei K ein Körper der Charakteristik Null. Für Familien $(a_i | 1 \leq i \leq n)$ und $(b_i | i \leq i \leq n)$ von Elementen aus K gelte $\sum_i a_i^t = \sum_i b_i^t$ für $1 \leq t \leq n$. Dann gibt es eine Permutation $\sigma \in S_n$ mit $a_i = b_{\sigma(i)}$.*

Beweis. Aus der Newtonschen Formel folgt induktiv, daß die elementarsymmetrischen Funktionen der a_i und der b_i gleich sind. Also sind die Polynome $\Pi_i(x - a_i)$ und $\Pi_i(x - b_i)$ gleich. □

(3.5) Satz. *Sei V ein n-dimensionaler Vektorraum über einem Körper K der Charakteristik Null. Für die Endomorphismen $f, g: V \to V$ gelte $\mathrm{Sp}(f^k) = \mathrm{Sp}(g^k)$ für $1 \leq k \leq n$. Dann haben f und g dasselbe charakteristische Polynom.*

Beweis. Sei $L|K$ eine Erweiterung, über der das charakteristische Polynom in Linearfaktoren zerfällt. Eine Matrix A von f läßt sich dann über L in eine obere Dreiecksmatrix B transformieren: $B = UAU^{-1}$, $U \in GL(n, L)$. Auf der Diagonale von B stehen die Nullstellen $\lambda_1, \ldots, \lambda_n$ des charakteristischen Polynoms. Es gilt $\mathrm{Sp}(B^k) = \mathrm{Sp}(A^k) = \sum_i \lambda_i^l$. Die Behauptung folgt aus (3.4). □

(3.6) Folgerung. *Gilt unter den Voraussetzungen von* (3.5) $\mathrm{Sp}(f^k) = 0$, $1 \leq k \leq n$, *so ist f nilpotent.* □

4 Teilbarkeit

Die Kreisteilungskörper entstehen aus $\mathbb{Q}$ durch Adjunktion von Einheitswurzeln. Sei $\Phi_n(x) \in \mathbb{C}[x]$ das normierte Polynom, dessen Nullstellen die primitiven n-ten Einheitswurzeln aus $\mathbb{C}$ sind. Wir nennen Φ_n das n-te *Kreisteilungspolynom*. Eine n-te Einheitswurzel heißt *primitiv*, wenn ihre multiplikative Ordnung gleich n ist. Die primitiven n-ten Einheitswurzeln sind $\exp(2\pi a i/n)$ für zu n teilerfremdes a. Eine n-te Einheitswurzel ist primitive d-te Einheitswurzel für genau einen Teiler d von n. Also gilt:

$$\textbf{(4.1)} \qquad x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Der Grad von Φ_n wird durch die Eulersche Funktion $\varphi(n)$ der zu n primen Restklassen $a \bmod n$ gegeben. Es ist $\Phi_1(x) = x - 1$ und deshalb $\Phi_p(x) = (x^p -$

$1)/(x-1) = 1 + x + \cdots + x^{p-1}$ für eine Primzahl p. Induktiv sieht man für eine Primzahlpotenz $q = p^n$ und $r = p^{n-1}$:

$$\Phi_q(x) = 1 + x^r + x^{2r} + \cdots + x^{(p-1)r}. \tag{4.2}$$

(4.3) Satz. *Für alle $n \in \mathbb{Z}$ ist $\Phi_n(x) \in \mathbb{Z}[x]$.*

Beweis. Induktion nach n. Nach Induktionsvoraussetzung liegt das Produkt der Φ_d mit $d|n$, $d \neq n$ in $\mathbb{Z}[x]$. Die Division von $x^n - 1$ durch ein normiertes Polynom aus $\mathbb{Z}[x]$ liefert wieder ein Polynom in $\mathbb{Z}[x]$. □

(4.4) Lemma. *Sei $f \in \mathbb{Z}[x]$ normiert. Ist $h \in \mathbb{Q}[x]$ ein normierter Teiler von f, so liegt h in $\mathbb{Z}[x]$.*

Beweis. Sei $f = g \cdot h$ eine Zerlegung von f in $\mathbb{Q}[x]$ durch nichtkonstante normierte Polynome. Wir können g derart mit einer ganzen Zahl a multiplizieren, daß $g^* = ag$ ganze teilerfremde Koeffizienten hat. Ebenso verfahren wir mit $h^* = bh$. Es gilt dann $abf = g^*h^*$. Sei $g^* = a_0 + a_1x + \ldots$ und $h^* = b_0 + b_1x + \ldots$. Falls $ab \neq \pm 1$ ist, sei p ein Primteiler von ab. Sei a_r der erste nicht durch p teilbare Koeffizient von g^* und b_s der erste nicht durch p teilbare von h^*. Solche gibt es, da die Koeffizienten als teilerfremd vorausgesetzt wurden. Der Koeffizient von x^{r+s} in g^*h^* ist dann

$$a_rb_s + a_{r+1}b_{s-1} + a_{r-1}b_{s+1} + \ldots.$$

Alle Summanden außer dem ersten sind durch p teilbar. Wegen $g^*h^* = abf$ ist aber auch die Summe durch p teilbar. Also teilt p auch a_rb_s. Widerspruch. □

(4.5) Satz. *Die Kreisteilungspolynome sind über $\mathbb{Q}$ irreduzibel.*

Beweis. Sei ζ eine primitive n-te Einheitswurzel und $f \in \mathbb{Q}[x]$ ihr Minimalpolynom. Dann ist f ein normierter Teiler von Φ_n und liegt nach (4.3) und (4.4) in $\mathbb{Z}[x]$. Wir haben nach (4.4) eine Zerlegung $x^n - 1 = fg$ in $\mathbb{Z}[x]$ mit normiertem g. Die primitiven n-ten Einheitswurzeln haben die Form ζ^a für zu n teilerfremdes a. Wenn wir zeigen, daß für jede zu n teilerfremde Primzahl p auch ζ^p eine Nullstelle von f ist, so sind alle primitiven Einheitswurzeln Nullstellen von f, und damit ist $f = \Phi_n$ gezeigt.

Angenommen $f(\zeta^p) \neq 0$, also $g(\zeta^p) = 0$. Dann ist ζ eine Nullstelle von $g(x^p)$. Da f Minimalpolynom von ζ ist, teilt f das Polynom $g(x^p)$. Nach (4.4) gibt es eine Zerlegung $g(x^p) = fh$ in $\mathbb{Z}[x]$. Wir reduzieren die Koeffizienten der Polynome modulo p. Das liefert einen Ringhomomorphismus $\mathbb{Z}[x] \to \mathbb{Z}/p[x]$, $f \mapsto \bar{f}$. In $\mathbb{Z}/p[x]$ gilt $\bar{g}(x^p) = (\bar{g}(x))^p$. Da g normiert ist, gilt $\bar{g}^p \neq 0$. Die Gleichung $\bar{g}^p = \bar{f}\bar{h}$ zeigt, daß $\bar{g}$ und $\bar{f}$ einen gemeinsamen irreduziblen Teiler haben. Folglich hat $x^n - 1 = \bar{f} \cdot \bar{g}$ in einem Erweiterungskörper mehrfache Nullstellen. Das widerspricht aber den Ergebnissen des siebenten Abschnittes. □

(4.6) Aufgaben und Ergänzungen.

1. Sei q Potenz einer Primzahl p. Dann ist $\Phi_q(1) = p$.

2. Sei n keine Primzahlpotenz. Dann gilt $\Phi_n(1) = 1$. Zum Beweis folgere man wegen

$$n = \prod_{d|n, d\neq 1} \Phi_d(1)$$

mittels der vorigen Aufgabe, daß das Produkt der $\Phi_d(1)$ für die Teiler d von n, die keine Primzahlpotenzen sind, gleich 1 ist; und dann durch Induktion die Behauptung.

8 Körper

1 Körpererweiterungen und Nullstellen

Ein Körper k sei vorgegeben. Er heiße der *Grundkörper*. Ist k ein Teilkörper von K, so nennen wir das Paar $k \subset K$ eine *Körpererweiterung* von k. Für diese Situation wird das Symbol $K|k$ verwendet. Ist $K|k$, so ist K mit seiner Addition und der Skalarmultiplikation $k \times K \to K$, $(a, u) \mapsto au$ ein Vektorraum über k. Die Dimension $\dim_k K$ heißt *Grad* $[K : k]$ der Erweiterung $K|k$. Wir erinnern daran, daß eine nichtleere Teilmenge $k \subset K$ genau dann ein Teilkörper ist, wenn mit $a, b \in k$ auch $a - b$, ab und (falls $b \neq 0$) b^{-1} in k liegen.

Der Durchschnitt von Teilkörpern ist wieder einer. Deshalb enthält jeder Körper einen eindeutig bestimmten kleinsten Teilkörper. Er ist entweder zum Körper $\mathbb{F}_p = \mathbb{Z}/(p)$ für eine Primzahl p oder zum Körper $\mathbb{Q}$ isomorph. Dieser kleinste Körper wird *Primkörper* genannt. Jeder Körper ist also ein Vektorraum über seinem Primkörper. Die *Charakteristik* eines Körpers ist p, wenn $\mathbb{F}_p$ der Primkörper ist, und 0 sonst. Ein Körper mit endlich vielen Elementen hat eine Charakteristik $p > 0$ und als Vektorraum über $\mathbb{F}_p$ deshalb als Elementanzahl eine Potenz von p.

Sei eine Erweiterung $K|k$ gegeben. Ein Element $a \in K$ heißt *algebraisch* über k, wenn es Nullstelle eines Polynoms aus $k[x]$ ist. Sei a Nullstelle von $f(x) = x^n + a_1x^{n-1} + \cdots + a_n \in k[x]$. Wir bezeichnen mit $k[a]$ die Gesamtheit der Linearkombinationen $c_0 + c_1a + \cdots + c_{n-1}a^{n-1}$, $c_j \in k$. Wir sagen, $k[a]$ entstehe aus k durch *Adjunktion* von a. Es gilt:

(1.1) Notiz. *$k[a]$ ist ein Teilkörper von K.*

Beweis. Sicherlich ist $k[a]$ eine additive Untergruppe, die auch die $1 \in k$ enthält. Um zu zeigen, daß Produkte wieder in $k[a]$ liegen, genügt es zu zeigen: Für alle $t \geq n$ liegt a^t in $k[a]$. Induktion nach t. Für $t = n$ folgt das aus der Gleichung $f(a) = 0$. Für den Induktionsschritt multiplizieren wir diese Gleichung mit a^{t-n}. Damit ist $k[a]$ als Teilring erkannt. Die Multiplikation mit $0 \neq x \in k[a]$ ist eine injektive k-lineare Abbildung des endlichdimensionalen k-Vektorraums $k[a]$ in sich und deshalb surjektiv. Folglich hat jedes von Null verschiedene Element ein multiplikatives Inverses. □

Wir haben den Einsetzungshomomorphismus $\varepsilon\colon k[x] \to K$, $x \mapsto a$. Das Bild ist $k[a]$ und der Kern ist ein Hauptideal $I(a) \subset k[x]$, das von einem eindeutig bestimmten normierten Polynom f erzeugt wird. Wir nennen f das *Minimalpolynom* von a. Durch ε wird ein kanonischer Isomorphismus

$$k[x]/(f) \cong k[a] \tag{1.2}$$

induziert. Zum Beispiel ist $\mathbb{C} \cong \mathbb{R}/(x^2 + 1)$.

(1.3) Satz. *Sei f das Minimalpolynom des über k algebraischen Elementes $a \in K$. Dann gilt:*

(1) *f ist irreduzibel.*
(2) $[k(a) : k] = \mathrm{Grad}(f)$.
(3) *Ist $m = \mathrm{Grad}(f)$, so ist $\{1, a, a^2, \ldots, a^{m-1}\}$ eine Basis des k-Vektorraums $k[a]$.*

Beweis. Wir verwenden (1.2). Ein Faktorring nach einem Ideal ist bekanntlich genau dann ein Körper, wenn das Ideal maximal ist. Da $k[a]$ ein Körper ist, ist also (f) ein maximales Ideal. Ein erzeugendes Element eines maximalen Ideals ist irreduzibel.

Die Elemente $1, a, \ldots, a^{m-1}$ erzeugen $k[a]$ als k-Vektorraum (1.1). Sie sind linear unabhängig, weil sonst a Nullstelle eines Polynoms von kleinerem Grad wäre. □

In Satz (1.3) haben wir die Existenz einer Nullstelle vorausgesetzt. Wir können den Spieß umdrehen und die linke Seite von (1.2) zur Definition benutzen. Das liefert die für alles Folgende fundamentale Konstruktion von Körpererweiterungen und Nullstellen:

(1.4) Satz. *Sei $p \in k[x]$ irreduzibel. Dann ist $k[x]/(p) =: K$ ein Körper. Sei $q\colon k[x] \to K$ die Quotientabbildung. Die Zusammensetzung mit der Inklusion der konstanten Polynome ist ein injektiver Körperhomomorphismus $k \to K$. Wir betrachten ihn vermöge Strukturtransport als Einbettung und dadurch K als Erweiterungskörper von k. Dann gilt: Das Element $\overline{x} := q(x) \in K$ ist eine Nullstelle von p, und p ist das Minimalpolynom von $\overline{x}$.*

Beweis. Sei $p = a_0 + a_1 x + \cdots + a_n x^n$. Da q ein Homomorphismus ist, gilt $q(p) = a_0 + a_1\overline{x} + \cdots + a_n\overline{x}^n$. Andererseits ist nach Konstruktion p ein Element im Kern von q. Da p irreduzibel ist und $\overline{x}$ als Nullstelle hat, ist es das Minimalpolynom.□

Ein irreduzibles Polynom $p \in \mathbb{Q}[x]$ hat in $\mathbb{C}$ im allgemeinen mehrere Nullstellen. Welche davon wurde in (1.4) konstruiert? Irgendeine! Die Nullstellen lassen sich algebraisch nicht unterscheiden! Diese Aussage wird alsbald deutlich werden; sie ist die Grundlage der Galois-Theorie.

3 Quadratische Gleichungen

Eine quadratische Gleichung $x^2 + ax + b = 0$ wird bekanntlich durch quadratische Ergänzung gelöst

$$x^2 + ax + b = (x + \frac{a}{2})^2 + b - \frac{a^2}{4}.$$

Der Wert $a^2 - 4b$ heiße *Diskriminante* des Polynoms $x^2 + ax + b$.

Sei k ein Körper und K eine zweidimensionale k-Algebra (assoziativ mit 1) über k, zum Beispiel eine Körpererweiterung vom Grad 2. Dazu gehört der injektive Homomorphismus $\varepsilon\colon k \to K$, $x \mapsto x \cdot 1$. Da wir uns im folgenden für

Isomorphieklassen von Algebren interessieren, nehmen wir ohne wesentliche Einschränkung ε als Inklusion an.

Sei $x \in K \setminus k$. Dann bilden 1 und x eine k-Basis von K. Folglich genügt x^2 einer Gleichung der Form $x^2 + ax + b = 0$. Wir setzen $D(x) = a^2 - 4b$.

(3.1) Notiz. *Ist $y \in K \setminus k$, so gilt $y = ux + v$ mit $u \neq 0$ und damit*

$$D(y) = u^2 D(x).$$

Beweis. Wir rechnen die quadratische Gleichung für y aus.

$$\begin{aligned} y^2 &= (ux+v)^2 = u^2x^2 + 2uvx + v^2 \\ &= u^2(-ax - b) + 2uvx + v^2 \\ &= ux(2v + ua) + v^2 - u^2b \\ &= (y - v)(2v - ua) + v^2 - u^2b \\ &= (2v - ua)y - v^2 + uva - u^2b. \end{aligned}$$

Durch Einsetzen verifiziert man dann $D(y) = u^2(a^2 - 4b)$. □

Wir bezeichnen mit $k^{*2} = \{u^2 \mid u \in k^*\}$ die multiplikative Untergruppe von k^* aller Quadrate. Durch Multiplikation operiert k^{*2} auf k, und wir haben die Bahnenmenge

$$Q(k) = k/k^{*2}.$$

Wegen (2.1) können wir jeder Algebra K ein Element $D(k) \in Q(k)$ zuordnen, nämlich die Bahn von $D(x)$ für $x \in K \setminus k$. Wir nennen auch $D(K)$ die *Diskriminante* von K. Sie hängt nur vom Isomorphietyp von K ab. Ist nämlich $\alpha\colon K \to L$ ein Isomorphismus von k-Algebren, so folgt aus $x^2 + ax + b = 0$ die Gleichung $y^2 + ay + b = 0$ für $y = \alpha(x)$.

(3.2) Satz. *Habe k nicht die Charakteristik 2. Dann liefert $K \mapsto D(K)$ eine Bijektion zwischen Isomorphieklassen zweidimensionaler k-Algebren und $Q(k)$. Genau dann ist K ein Körper, wenn $D(K) \neq [0], [1]$ ist.*

Beweis. Sei $b \in k$ gegeben. Wir betrachten die Faktoralgebra $K_b = k[X]/(X^2 - b)$. Die Restklasse x von X erfüllt die Gleichung $x^2 - b = 0$. Also ist $D(K_b) = [4b]$. Da k nicht die Charakteristik 2 hat, ist $4 \in k^{*2}$ und folglich $[4b] = [b]$ in $Q(k)$. Wir sehen, die Zuordnung ist surjektiv.

Sei K gegeben. Erfüllt $x \in K \setminus k$ die Gleichung $x^2 + ax + b = 0$, so erfüllt $y = x + \frac{a}{2}$ die Gleichung $y^2 = \frac{1}{4}D(x) := c$. Durch $k[Y]/(Y^2 - c) \to K, Y \mapsto y$ wird ein Isomorphismus gegeben. Also ist jede Algebra isomorph zu einer vom Typ K_c. Ist $[c] = [d]$, also $d = u^2c$, $u \neq 0$, so wird durch $Y \mapsto uZ$ ein Isomorphismus $k[Y] \to k[Z]$ geliefert, der $(Y^2 - d)$ auf $(uZ^2 - u^2c) = (Z^2 - c)$ abbildet, und deshalb einen Isomorphismus $K_c \cong K_d$ induziert. Wir sehen, die Zuordnung ist injektiv.

Die Algebren $k[X]/(X^2)$ und $k[X]/(X^2 - 1)$ sind keine Körper. Im ersten Fall hat die Restklasse $x \neq 0$ von X das Quadrat Null. Im zweiten Fall haben die von Null verschiedenen Elemente $x - 1$ und $x + 1$ das Produkt Null.

Ist $b \neq 0$ und $b \notin k^{*2}$, so ist $X^2 - b$ irreduzibel, denn andernfalls zerfiele es in Linearfaktoren $(X - a_1)(X - a_2)$, und dann wäre aber $a_1 = a_2$ und $a_1^2 = b$. □

Wir behandeln nun Algebren über einem Körper der Charakteristik zwei. Der folgende Satz zeigt, daß es zwei wesentlich verschiedene Fälle gibt.

(3.3) Satz. *Sei K eine zweidimensionale Algebra über dem Körper k der Charakteristik 2. Erfüllt ein Element $x \in K \setminus k$ eine Gleichung $x^2 = b$ ohne linearen Term, so gilt dieses für alle $y \in K \setminus k$.*

Beweis. Ist $y = ux+v$, so zeigt die Rechnung im Beweis von (2.1) $y^2 = u^2b+v^2$. □

Wir nennen Algebren mit der im Satz (2.3) genannten Eigenschaft *inseparabel*. Der Grund: Ist c eine Nullstelle von $x^2 - b$ in einem Erweiterungskörper, so ist $x^2-b = (x-c)^2$; es handelt sich um eine doppelte Nullstelle; die beiden Nullstellen sind nicht separiert.

Wir haben wieder die multiplikative Gruppe k^{*2}. Im Falle der Charakteristik 2 gilt $(x + y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$. Demnach ist $k^{(2)} = \{x^2 \mid x \in k\}$ eine additive Untergruppe von $(k, +)$. Die Gruppe k^{*2} ist vermöge Multiplikation eine Automorphismengruppe von $k^{(2)}$, nämlich $\tau\colon k^{*2} \to \mathrm{Aut}(k^{(2)})$, $u \mapsto (a \mapsto ua)$. Wir können also das semidirekte Produkt $A^2(k) = k^{(2)} \times_\tau k^{*2}$ bilden. Das ist eine Untergruppe der affinen Gruppe $A(k) = k \times_\tau k^*$. Die affine Gruppe operiert auf k durch $(v, u) \cdot x = ux + v$. Wir setzen für den Bahnenraum

$$Q_i(k) = k/A^2(k).$$

Erfüllt $y \in K \setminus k$ die Gleichung $y^2 = b$, so sei $D_i(y) \in Q_i(k)$ die Klasse von b. Im Beweis von (2.3) haben wir gesehen, daß $D_i(y)$ unabhängig von $y \in K \setminus k$ ist. Der Wert wurde deshalb mit $D_i(K)$ bezeichnet und *Diskriminante* von K genannt.

(3.4) Satz. *Die Zuordnung $K \mapsto D_i(K)$ liefert eine Bijektion zwischen Isomorphieklassen inseparabler Algebren und $Q_i(k)$. Genau dann ist K ein Körper, wenn $D_i(K) \neq [0]$ ist.*

Beweis. Die Algebra $k[Y]/(Y^2 - b) = K_b$ hat Diskriminante b. Also ist die Zuordnung surjektiv. Jede inseparable Algebra ist isomorph zu einer vom Typ K_b. Sei $[b] = [c]$ in $Q_i(k)$, also $c = u^2b+v^2$, $u \neq 0$. Der durch $Y \mapsto uZ+v$ gegebene Homomorphismus $k[Y] \to k[Z]$ ist ein Isomorphismus und bildet $(Y^2 - c)$ auf $(u^2Z^2 + v^2 - c) = (u^2Z - u^2b) = (Z^2 - b)$ ab und induziert einen Isomorphismus $K_c \cong K_b$. Also ist die Zuordnung injektiv.

Die Algebra K_0 ist kein Körper. Sei K_b ein Körper. Dann ist Y^2-b irreduzibel. Wäre $[b] = [0]$, also $u^2b + v^2 = 0$ für ein $u \neq 0$, so wäre $Y^2 - b = Y^2 + u^{-2}v^2 = (Y + u^{-1}v)^2$ reduzibel. □

Wir betrachten nun die Algebren K, bei denen ein $x \in K \setminus k$ eine Gleichung $x^2 + ax + b = 0$ mit $a \neq 0$ erfüllt. Wir wollen sie *separabel* nennen. Ist $y = ux + v$,

so gilt

$$y^2 = uay + uav + u^2b + v^2.$$

Wir wählen $u = a^{-1}$ und sehen, daß dann y einer Gleichung $y^2+y+c = 0$ genügt.

Die Menge $\mathfrak{p}(k) = \{x^2 + x \mid x \in k\}$ ist eine additive Untergruppe von k. Wir setzen

$$Q_s(k) = k/\mathfrak{p}(k).$$

Ist $y \in K \setminus k$ ein Element mit $y^2 + y + b = 0$, so setzen wir $D_s(K) \in Q_s(k)$ als die Klasse von b in $Q_s(k)$ fest. Aus der obigen Rechnung ($a = 1 = u$) sehen wir, daß die *Diskriminante* $D_s(K)$ wohldefiniert ist.

(3.5) Satz. *Die Zuordnung $K \mapsto D_s(K)$ liefert eine Bijektion zwischen Isomorphieklassen separabler Algebren und $Q_s(k)$. Genau dann ist K ein Körper, wenn $D_s(K) \neq [0]$ ist.*

Beweis. Die Algebra $K_b = K[Y]/(Y^2 + Y + b)$ hat die Diskriminante b. Die Zuordnung ist surjektiv. Sei $[b] = [c]$ in $Q_s(k)$, also $b = c+u^2+u$. Die Zuordnung $k[Y] \to k[Z]$, $Y \mapsto Z + u$ ist ein Isomorphismus und bildet $(Y^2 + Y + c)$ auf $(Z^2+u^2+Z+u+c) = (Z^2+Z+b)$ ab und liefert einen Isomorphismus $K_b \cong K_c$. Die Zuordnung ist injektiv.

Die Algebra K_0 ist kein Körper, da $Y^2 + Y$ reduzibel ist. Ist $Y^2 + Y + b$ reduzibel, etwa gleich $(Y + a_1)(Y + a_2)$, so ist $1 = a_1 + a_2$, $b = a_1a_2$, also $b = a_1(1 + a_1) \in \mathfrak{p}(k)$. □

(3.6) Beispiel. Sei $k = \mathbb{Q}$. Jedes $x \in \mathbb{Q}$ läßt sich durch Multiplikation mit einem Quadrat ganzzahlig machen. Jedes Element von $Q(\mathbb{Q})$ hat also einen Repräsentanten in $\mathbb{Z}$. Ist $x = a^2y$, so ist $[x] = [y]$ in $Q(\mathbb{Q})$. Also reichen als Repräsentanten die *quadratfreien* ganzen Zahlen, die also jede Primzahl höchstens in erster Potenz enthalten. Zwei solche sind aber niemals in $Q(\mathbb{Q})$ äquivalent. Die verschiedenen Körpererweiterungen von $\mathbb{Q}$ vom Grad zwei sind also genau die $\mathbb{Q}[\sqrt{d}]$, worin $d \neq 1$ eine quadratfreie ganze Zahl ist. Diese Körper heißen *quadratische Zahlkörper.* ◇

(3.7) Beispiel. $Q(\mathbb{R})$ hat drei Elemente $[0], [1], [-1]$. Es gibt genau eine quadratische Körpererweiterung von $\mathbb{R}$: Die komplexen Zahlen. ◇

(3.8) Beispiel. Sei $\mathbb{F}_p$ ein Körper mit p Elementen ($p \neq 2$ Primzahl). Die Gruppe $\mathbb{F}_p^*$ ist zyklisch von der Ordnung $p - 1$, siehe (??). Die Quadrate bilden darin die eindeutig bestimmte Untergruppe vom Index 2. Also hat $\mathbb{F}_p^*/\mathbb{F}_p^{*2}$ genau zwei Elemente. Folglich gibt es bis auf Isomorphie genau eine quadratische Erweiterung von $\mathbb{F}_p$, also genau einen Körper mit p^2 Elementen. Den surjektiven Homomorphismus $(\mathbb{Z}/p\mathbb{Z}^*) \to \{\pm 1\}$ bezeichnet man mit

$$a \mapsto (\frac{a}{p}) \qquad (a, p) = 1,$$

wobei $(\frac{a}{p}) = (\frac{b}{p})$ für $a \equiv b \bmod p$ ist, und nennt ihn *Legendre-Symbol.* Im Fall $\mathbb{F}_2$ gibt es genau eine separable Erweiterung vom Grad 2. ◇

4 Algebraische Erweiterungen

Sei $k \subset K$ eine Körpererweiterung. Ein Element $a \in K$ heißt *algebraisch* über K, wenn es einer Gleichung der Form $a^n + a_1 a^{n-1} + \cdots + a_n = 0$ mit Koeffizienten $a_j \in k$ genügt, wenn es also Nullstelle eines Polynoms aus $k[x]$ ist. Andernfalls heißt a *transzendent* über k. Die Erweiterung $k \subset K$ heißt *algebraisch*, wenn jedes Element von K algebraisch über k ist. Die über $\mathbb{Q}$ algebraischen komplexen Zahlen heißen *algebraische Zahlen*. Algebraische Erweiterungen von $\mathbb{Q}$, die in $\mathbb{C}$ liegen, heißen *algebraische Zahlkörper*. Das Element x des Funktionenkörpers $k(x)$ ist transzendent über k; es ist $k[x] \neq k(x)$. Genau dann ist a transzendent, wenn $k[x] \to k[a]$, bestimmt durch $x \mapsto a$, ein Isomorphismus ist. Dann ist auch der von a und k erzeugte Unterkörper $k(a)$ isomorph zum Funktionenkörper $k(x)$.

Wir brauchen einige Bezeichungen. Sei $k \subset K$ eine Körpererweiterung, $A \subset K$ eine Teilmenge und $R \subset K$ ein Unterring. Wir betrachten $R[A]$, den Schnitt aller Unterringe von K, die $R \cup A$ enthalten, und $k(A)$, den Schnitt aller Unterkörper, die $k \cup A$ enthalten. Wir sagen, der Körper $k(A)$ (oder der Ring $R[A]$) entstehe durch *Adjunktion* der Elemente aus A an k (oder R). Ist $A = \{a_1, \ldots, a_n\}$, so schreiben wir stattdessen $R[a_1, \ldots, a_n]$ und $k(a_1, \ldots, a_n)$. Ist $K = k(a)$, so heiße die Erweiterung $k \subset K$ *einfach* und a ein *primitives Element* der Erweiterung. Eine Erweiterung $K|k$ heißt endlich, wenn der Körpergrad $[K : k]$ endlich ist. Der Beweis der beiden folgenden Notizen kann als Aufgabe gelten.

(4.1) Notiz. *Über diese Symbole gelten die folgenden Rechenregeln:*

(1) $(R[A])[B] = R[A \cup B]$.
(2) $(k(A))(B) = k(A \cup B)$.
(3) $k[a_1, \ldots, a_n]$ *ist das Bild des Polynomringes* $k[x_1, \ldots, x_n]$ *bei dem durch* $x_j \mapsto a_j$ *gegebenen Homomorphismus.*
(4) $k(A)$ *ist Quotientenkörper von* $k[A]$.
(5) *Ist* $k[A]$ *ein Körper, so ist* $k[A] = k(A)$.
(6) $k(A) = \bigcup k(E)$, *Vereinigung über alle endlichen* $E \subset A$.
(7) $R[A] = \bigcup R[E]$, *Vereinigung über alle endlichen* $E \subset A$. □

Elementare lineare Algebra liefert das folgende Resultat. Es wird immer wieder stillschweigend verwendet.

(4.2) Notiz. *Seien* $k \subset K \subset L$ *Körpererweiterungen. Dann gilt*

$$[L : K][K : k] = [L : k].$$

Insbesondere ist $k \subset L$ *genau dann endlich, wenn* $k \subset K$ *und* $K \subset L$ *endlich sind. Ist* $(x_i \in L \mid i \in I)$ *eine Basis des* K*-Vektorraumes* L *und* $(y_j \in K \mid j \in J)$ *eine Basis des* k*-Vektorraumes* K*, so ist* $(x_i y_j \mid i \in I, j \in J)$ *eine Basis des* k*-Vektorraumes* L. □

(4.3) Korollar. *Ist* $L|K|k$ *und* $[L : k] = [K : k] < \infty$*, so gilt* $K = L$*. Ist* $[L : k] = [L : K] < \infty$*, so gilt* $k = K$*. Ist* $[L : k]$ *eine Primzahl, so ist* $K = k$ *oder* $K = L$. □

Wir haben nun Bezeichnungen und Hilfsmittel, um einige grundlegende Eigenschaften algebraischer Erweiterungen herleiten zu können.

(4.4) Satz. *Sei $k \subset K$ eine Körpererweiterung. Dann gelten:*

(1) *Ist die Erweiterung endlich, so ist sie algebraisch, und es gibt $a_1, \ldots, a_m \in K$ mit $K = k(a_1, \ldots, a_m) = k[a_1, \ldots, a_m]$.*

(2) *Ist $K = k(a_1, \ldots, a_m)$ mit algebraischen a_j, so ist die Erweiterung endlich und algebraisch.*

(3) *Ist $A \subset K$ eine Menge von über k algebraischen Elementen, so ist $k[A] = k(A)$.*

Beweis. (1) In einer endlichen Erweiterung können nicht alle Potenzen eines Elementes $a \in K$ über k linear unabhängig sein. Also ist jedes $a \in K$ algebraisch über k. Sei $\{a_1, \ldots, a_m\}$ eine k-Basis von K. Dann enthält $k[a_1, \ldots, a_m]$ alle Linearkombinationen der a_j, also K.

(2) Beweis durch Induktion nach m. Der Fall $m = 1$ ist (2.3). Der Induktionsschritt folgt mittels

$$[k(a_1, \ldots, a_{n+1}) : k] = [k(a_1, \ldots, a_n)(a_{n+1}) : k(a_1, \ldots, a_n)][k(a_1, \ldots, a_n) : k].$$

(3) Ist A endlich, so verwenden wir (1) und für beliebiges A danach (3.1). □

(4.5) Satz. *Seien $k \subset K \subset L$ Körpererweiterungen. Dann ist $k \subset L$ genau dann algebraisch, wenn $k \subset K$ und $K \subset L$ algebraisch sind.*

Beweis. Ist $k \subset L$ algebraisch, so auch $k \subset K$ und $K \subset L$, wie unmittelbar aus den Definitionen folgt. Seien umgekehrt $k \subset K$ und $K \subset L$ algebraisch, und sei $a \in L$. Dann gibt es $b_1, \ldots, b_n \in K$ mit $a^n + b_1 a^{n-1} + \cdots + b_n = 0$, da a über K algebraisch ist. Also ist a sogar algebraisch über $k(b_1, \ldots, b_n)$. Da $k \subset K$ algebraisch ist, sind die b_j algebraisch über k. Also ist nach (3.4) $k_n := k(b_1, \ldots, b_n)$ algebraisch über k. Es folgt

$$[k(a) : k] \leq [k_n(a) : k] = [k_n(a) : k_n][k_n : k] < \infty,$$

letzteres wieder mittels (3.4). □

(4.6) Satz. *Sei $k \subset K$ Körpererweiterung und L die Menge aller über k algebraischen Elemente von K. Dann gilt:*

(1) *L ist ein Zwischenkörper von $k \subset K$.*

(2) *L ist algebraisch über k.*

(3) *Ist a algebraisch über L, so gilt $a \in L$.*

Beweis. (1) Offenbar gilt $k \subset L$. Seien $a, b \in L$. Nach (3.4) ist $k(a, b)$ algebraisch über k. Also gilt $k(a, b) \subset L$. Da $a - b$ und (falls $b \neq 0$) auch ab^{-1} in $k(a, b)$ liegen und also auch in L, sehen wir, daß L ein Unterkörper ist.

(2) ist (1) und die Definition einer algebraischen Erweiterung.

(3) Sei $a \in K$ algebraisch über L. Dann ist nach (3.4) $L \subset L(a)$ algebraisch und nach (1) und (3.5) auch $k \subset L(a)$ algebraisch. Also ist a algebraisch über k, und deshalb liegt a in L. □

Wir bezeichen den Körper L im letzten Satz als den *algebraischen Abschluß* von k in K. Die Menge $\overline{\mathbb{Q}}$ aller über $\mathbb{Q}$ algebraischen Zahlen von $\mathbb{C}$ ist ein Körper, der *Körper aller algebraischen Zahlen*. Die Menge $\overline{\mathbb{Q}}$ ist abzählbar, da es nur abzählbar viele Polynome mit rationalen Koeffizienten gibt. Da $\mathbb{R}$ nicht abzählbar ist, gibt es transzendente Zahlen über $\mathbb{Q}$. Man kann beweisen, daß e und π transzendent sind. Der Körper $\overline{\mathbb{Q}}$ ist *algebraisch abgeschlossen*, das heißt jedes Polynom mit Koeffizienten in $\overline{\mathbb{Q}}$ zerfällt in Linearfaktoren: Da nämlich $\mathbb{C}$ algebraisch abgeschlossen ist, könnte man andernfalls noch weitere über $\overline{\mathbb{Q}}$ algebraische Elemente in $\mathbb{C}$ finden.

(4.7) Aufgaben und Ergänzungen.

1. Beweis von (3.1) und (3.2).

2. Untersuchung von $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})|\mathbb{Q}$. Die Menge $1, \sqrt{3}, \sqrt{5}, \sqrt{15}$ ist eine $\mathbb{Q}$-Basis von K. Wie lautet das Inverse von $1 + \sqrt{3} + \sqrt{5} + \sqrt{15}$ in dieser Basis? Es gilt $K = \mathbb{Q}(\sqrt{3} + \sqrt{5})$. Wie lautet das Minimalpolynom von $\sqrt{3} + \sqrt{5} = \delta$ über $\mathbb{Q}, \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$ und $\mathbb{Q}(\sqrt{15})$? Wie lautet $\sqrt{3}$ in der $\mathbb{Q}$-Basis $1, \delta, \delta^2, \delta^3$? Für welche rationalen Zahlen r ist $K = \mathbb{Q}(\sqrt{3} + r\sqrt{5})$?

5 Morphismen

Sei $K|k$ eine Körpererweiterung und $\varphi\colon k \to L$ ein Körperhomomorphismus. Ein φ-Morphismus ist ein Körperhomomorphismus $\Phi\colon K \to L$, der auf k mit φ übereinstimmt. Sei $\mathrm{Mor}_\varphi(K, L)$ die Menge der φ-Morphismen. Ist φ eine Inklusion, also L eine Erweiterung von k, so sprechen wir stattdessen auch von k-Morphismen und schreiben $\mathrm{Mor}_k(K, L)$ für die Morphismenmenge. Ein Körperhomomorphismus ist bekanntlich immer injektiv und heißt deshalb auch *Einbettung*. Ist $\ell = \varphi(k)$, so ist L eine Erweiterung von ℓ. Im Falle $[K : k] = [L : \ell] < \infty$ besteht also $\mathrm{Mor}_\varphi(K, L)$ aus Isomorphismen. Ist außerdem $K = L$, so ist $\mathrm{Mor}_k(K, K)$ die Automorphismengruppe der Erweiterung, die auch mit $G(K|k)$ bezeichnet werde.

Wir untersuchen $\mathrm{Mor}_\varphi(K, L)$ und beginnen mit der Adjunktion einer Nullstelle. Dazu noch eine Notation. Ist $\varphi\colon k \to L$ gegeben, so können wir φ auf die Koeffizienten von Polynomen anwenden und erhalten einen induzierten Ringhomomorphismus $\varphi_*\colon k[x] \to L[x]$. Ist φ eine Inklusion, so betrachten wir auch φ_* als Inklusion. Wir bezeichnen mit $N(g, L)$ die Menge der in L gelegenen Nullstellen eines Polynoms $g \in L[x]$.

(5.1) Notiz. *Sei $\Phi \in \mathrm{Mor}_\varphi(K, L)$, $f \in k[x]$ und $a \in N(f, K)$. Dann ist $\Phi(a) \in N(\varphi_* f, L)$. Insbesondere permutiert $\Phi \in G(K|k)$ die Nullstellen von f in K.*

Beweis. Ist $f(x) = \sum_j c_j x^j$, so folgt mit der Kette

$$0 = \Phi(\sum_j c_j a^j) = \sum_j \Phi(c_j)\Phi(a)^j = \sum_j \varphi(c_j)\Phi(a)^j = (\varphi_* f)(\Phi(a))$$

die Behauptung. □

Viele Aussagen über Morphismen werden durch wiederholte Anwendung der Standardsituation des folgenden Satzes gewonnen.

(5.2) Satz. *Sei $\varphi\colon k \to L$ gegeben und $k(a)|k$ eine algebraische Erweiterung von k mit Minimalpolynom $f \in k[x]$ von a. Die Zuordnung $\Phi \mapsto \Phi(a)$ liefert eine Bijektion $\varepsilon_a\colon \mathrm{Mor}_\varphi(k(a), L) \to N(\varphi_* f, L)$.*

Beweis. Nach (4.1) handelt es sich um eine Abbildung in die angegebene Menge. Da $k(a) = k[a]$ als Ring von k und a erzeugt wird, ist ein φ-Morphismus durch den Wert $\Phi(a)$ bestimmt und somit ε_a injektiv.

Sei $b \in N(\varphi_* f, L)$. Wir betrachten das Diagramm

$$\begin{array}{ccc} k[x] & \xrightarrow{\varphi_*} & L[x] \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ k[a] & \xrightarrow{\Phi} & L, \end{array}$$

worin α das Einsetzen von a und β das Einsetzen von b ist. Der Kern von α ist (f). Das Element f liegt im Kern von $\beta \circ \varphi_*$. Auf Grund der universellen Eigenschaft von α gibt es einen Homomorphismus Φ mit $\Phi \circ \alpha = \beta \circ \varphi_*$. Nach Konstruktion ist Φ ein k-Morphismus, der a auf b abbildet. Also ist ε_a auch surjektiv. □

(5.3) Folgerung. *Unter den Voraussetzungen von* (4.2) *ist*

$$|\mathrm{Mor}_\varphi(k(a), L)| \leq [k(a) : k].$$

Gleichheit gilt genau dann, wenn $\varphi_* f$ in paarweise verschiedene Linearfaktoren zerfällt. Sei $k' = \varphi(k)$ und $a' \in L$ eine Nullstelle von $\varphi_*(f)$. Dann gibt es genau einen Isomorphismus $\Phi\colon k(a) \to k'(a')$, der φ erweitert und a auf a' abbildet. Insbesondere gibt es genau einen k-Automorphismus von $k(a)$, der eine Nullstelle des Minimalpolynoms von a auf eine andere abbildet. Die Gruppe $G(k(a)|k)$ wirkt also transitiv auf der Menge $N(f, k(a))$ und ist eine Untergruppe der symmetrischen Gruppe dieser Menge. □

(5.4) Satz. (1) *Sei $\varphi\colon k \to L$ gegeben und $K|k$ eine endliche Erweiterung. Sei $K = k(a_1, \ldots, a_m)$ und $f_j \in k[x]$ das Minimalpolynom von a_j. Dann gilt $|\mathrm{Mor}_\varphi(K, L)| \leq [K : k]$. Die Morphismenmenge ist nicht leer, wenn alle $\varphi_*(f_j)$ in L wenigstens eine Nullstelle haben.*
(2) *Zerfallen die Polynome $\varphi_*(f_j)$ alle in paarweise verschiedene Linearfaktoren, so gilt die Gleichheit $|\mathrm{Mor}_\varphi(K, L)| = [K : k]$.*

Beweis. (1) Induktion nach m. Der Fall $m = 1$ ist (4.2). Wir betrachten das Diagramm

$$\begin{array}{ccccc} k & \xrightarrow{\subset} & k(a_1) & \xrightarrow{\subset} & K \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi(t)} & & \downarrow{\scriptstyle \Phi} \\ L & \xrightarrow{=} & L & \xrightarrow{=} & L. \end{array}$$

Sei $\Phi \in \mathrm{Mor}_\varphi(K, L)$. Seien $a_1 = a(1), \ldots, a(r)$ die verschiedenen Nullstellen von $\varphi_* f_1$ in L. Dann gibt es nach (4.2) genau ein $t \in \{1, \ldots, r\}$ mit $\Phi(a_1) = a(t)$. Wir haben eine disjunkte Zerlegung $\mathrm{Mor}_\varphi(K, L) = \coprod_t M_t$, worin M_t die Φ mit $\Phi(a_1) = a(t)$ enthält. Wir schreiben dann $\Phi | k(a_1) = \varphi(t)$. Nach Induktionsvoraussetzung ist $|M_t| \leq [K : k(a_1)]$. Da nach (4.3) $r \leq [k(a_1) : k]$ ist, folgt der Induktionsschritt.

(2) Wir müssen nur die konstruktive Seite von (4.2) sorgfältig betrachten. Da $\varphi_* f_1$ in verschiedene Linearfaktoren zerfällt, so ist $|\mathrm{Mor}_\varphi(k(a_1) : k)|$ nach (4.3) gleich $[k(a_1) : k] = r$. Sei $\varphi(j) \colon k(a_1) \to L$ durch $\varphi_j(a_1) = a(j)$ festgelegt. Wir betrachten nun $\mathrm{Mor}_{\varphi(j)}(K, L)$. Das Minimalpolynom $g_j \in k(a_1)[x]$ von a_j, $j \geq 2$, ist ein Teiler von $f_j \in k[x]$ und folglich ist $\varphi(t)_* g_j$ ein Teiler von $\varphi_* f_j$. Es zerfällt dann insbesondere in verschiedene Linearfaktoren. Also ist für $K | k(a_1)$ die Induktionsvoraussetzung erfüllt. Deshalb gilt $|\mathrm{Mor}_{\varphi(j)}(K, L)| = [K : k(a_1)]$ für alle j. □

Speziell gilt im Fall $K = L$ und $\varphi \colon k \subset K$:

(5.5) Folgerung. *Sei $K|k$ eine endliche Erweiterung. Dann ist $|G(K|k)| \leq [K : k]$, und Gleichheit gilt, falls $K = k(a_1, \ldots, a_m)$ mit Elementen a_j, deren Minimalpolynome über K in verschiedene Linearfaktoren zerfallen. Ist $K = k(a_1, \ldots, a_m)$ und sind alle a_j Nullstellen eines Polynoms aus $k[x]$, so liefert jedes $\Phi \in G(K|k)$ eine Permutation von $\{a_1, \ldots, a_m\}$; die Gruppe ist deshalb isomorph zu einer Untergruppe der symmetrischen Gruppe S_m.* □

Der folgende Satz sagt unter anderem, daß endliche Erweiterungen von $\mathbb{Q}$ zu Teilkörpern der komplexen Zahlen isomorph sind. Der Beweis von (4.4) liefert nämlich:

(5.6) Satz. *Sei $L|k$ gegeben und L algebraisch abgeschlossen. Dann ist jede endliche Erweiterung $K|k$ isomorph zu einem Zwischenkörper von $L|k$.* □

(5.7) Aufgaben und Ergänzungen.

1. Sei $K|k$ eine algebraische Erweiterung. Dann ist jeder k-Morphismus $K \to K$ ein Automorphismus.

2. Mit Hilfe des Zornschen Lemmas zeige man, daß (4.6) für beliebige algebraische Erweiterungen $K|k$ gilt. Genauer zeige man: Sei $\varphi \colon k \to L$ ein Morphismus in einen algebraisch abgeschlossenen Körper L. Man betrachte alle Paare (F, Φ), worin F ein Zwischenkörper von $K|k$ ist und $\Phi \in \mathrm{Mor}_\varphi(F, L)$. Auf diesen Paaren führe man eine teilweise Ordnung ein durch $(F_1, \Phi_1) \leq (F_2, \Phi_2)$ genau wenn $F_1 \subset F_2$ und $\Phi_2 | F_1 = \Phi_1$ ist. Nach dem Zornschen Lemma gibt es ein maximales Element (M, Ψ). Wäre $M \neq K$, so könnte man Ψ auf einen Körper $M(a)$ erweitern.

3. Sei $K|k$ eine algebraische Erweiterung. Jeder k-Endomorphismus von K ist ein Automorphismus.

4. Ein *algebraischer Abschluss* von k ist eine algebraische Erweiterung $K|k$ mit

algebraisch abgeschlossenem K. Aus den voranstehenden Aufgaben folgt, daß ein algebraischer Abschluß bis auf Isomorphie eindeutig bestimmt ist.

6 Zerfällungskörper und normale Erweiterungen

Eine Körpererweiterung $k \subset K$ heißt *Zerfällungskörper* eines nichtkonstanten Polynoms $f \in k[x]$, wenn f über K in Linearfaktoren zerfällt und wenn eine derartige Zerfällung über keinem kleineren Körper zwischen k und K möglich ist.

(6.1) Satz. *Sei $f \in k[x]$ nicht konstant. Ist $k \subset K$ eine Körpererweiterung, über der f in Linearfaktoren zerfällt, $f = c(x-a_1)(x-a_2)\cdots(x-a_n)$, so ist $L = k(a_1, \ldots, a_n)$ ein Zerfällungskörper von f.*

Beweis. Angenommen, f zerfällt über einem Zwischenkörper $k \subset M \subset L$ in Linearfaktoren. Dann gibt es also eine Darstellung $f = d(x-b_1)\cdots(x-b_n)$ mit $b_j \in M$. Wegen der eindeutigen Primfaktorzerlegung in $L[x]$ folgt $\{b_1, \ldots, b_n\} = \{a_1, \ldots, a_n\}$ und damit wegen $L = k(a_1, \ldots, a_n) = k(b_1, \ldots, b_n) \subset M \subset L$ die Behauptung. □

(6.2) Notiz. *Jedes nichtkonstante Polynom $f \in k[x]$ besitzt einen Zerfällungskörper.*

Beweis. Induktion nach dem Grad von f. Hat f den Grad 1, so ist k selbst Zerfällungskörper. Sei p ein irreduzibler Faktor von f. Wir haben in (2.4) gezeigt, daß es eine Erweiterung $K|k$ gibt, über der p und somit f wenigstens eine Nullstelle hat. In $K[x]$ gibt es also eine Zerlegung der Form $f = (x-a)g$. Auf $g \in K[x]$ wenden wir die Induktionsvoraussetzung an. □

(6.3) Beispiel. Eine Nullstelle von $x^3 - 2 \in \mathbb{Q}$ ist $\delta = \sqrt[3]{2} \in \mathbb{R}$. Es hat $\mathbb{Q}(\delta)|\mathbb{Q}$ den Grad 3 (ebenso für die beiden anderen Nullstellen). Über $K = \mathbb{Q}(\delta)$ spaltet $x^3 - 2$ nur einen Linearfaktor ab, da die beiden anderen Nullstellen nicht reell sind. Um auch den quadratischen Faktor von $x^3 - 2$ in $K[x]$ zu zerlegen, braucht man noch einmal eine quadratische Erweiterung $L|K$. Dann hat $L|k$ den Grad 6, und L ist ein Zerfällungskörper. ◇

(6.4) Notiz. *Ist $K|k$ ein Zerfällungskörper von $f \in k[x]$ und $k \subset L \subset K$ ein Zwischenkörper, so ist $L \subset K$ ein Zerfällungskörper von $f \in L[x]$. Ferner ist $K(a)|k(a)$ Zerfällungskörper von $f \in k(a)[x]$.*

Beweis. Es gilt mit den Nullstellen $a_1, \ldots, a_n$ von $f \in k[x]$

$$K = k(a_1, \ldots, a_n) \subset L(a_1, \ldots, a_n) \subset K,$$

also überall die Gleichheit. Ferner gilt

$$K(a) = k(a_1, \ldots, a_n)(a) = k(a)(a_1, \ldots, a_n),$$

was die zweite Aussage belegt. □

Die Eindeutigkeit des Zerfällungskörpers ist der Spezialfall $\varphi = \mathrm{id}$ des nächsten Satzes.

(6.5) Satz. *Sei $\varphi\colon k \to k'$ ein Isomorphismus. Sei $f \in k[x]$ nicht konstant. Sei $k \subset K$ ein Zerfällungskörper von f und $k' \subset K'$ einer von $\varphi_*(f) = f'$. Dann gibt es einen Isomorphismus $\Phi\colon K \to K'$, der auf k mit φ übereinstimmt und die Menge der Nullstellen von f in K auf die Menge der Nullstellen von f' in K' abbildet.*

Beweis. Induktion über die Anzahl r der Nullstellen in $K \setminus k$. Ist $r = 0$, also $K = k$, so gibt es $a_1, \dots, a_n, c \in k$ und eine Zerlegung

$$f = c(x - a_1)(x - a_2) \cdots (x - a_n).$$

Es folgt

$$f' = \varphi_*(f) = \varphi(c)(x - \varphi(a_1)) \cdots (x - \varphi(a_n)).$$

Wir setzen deshalb $\Phi = \varphi$.

Sei $r \geq 1$. Seien $a_1, \dots, a_r$ die in $K \setminus k$ liegenden Nullstellen von f. Sei $p \in k[x]$ das Minimalpolynom von a_1. Es teilt jedes andere Polynom mit der Nullstelle a_1, also insbesondere f. Folglich ist $p' = \varphi_*(p)$ Teiler von $f' = \varphi_*(f)$. Da f' über K' in Linearfaktoren zerfällt, hat p' eine Nullstelle in K', etwa a'_1. Nach Satz (5.3) gibt es einen Isomorphismus $\varphi_1\colon k(a_1) \to k'(a'_1)$, der auf k mit φ übereinstimmt und a_1 auf a'_1 abbildet. Wir wenden nun die Induktionsannahme auf $k(a_1), k'(a'_1), \varphi_1, f, K, K'$ an und erhalten den Induktionsschritt. □

(6.6) Zusatz. *Ist a Nullstelle eines irreduziblen Faktors g von f und a' Nullstelle des irreduziblen Faktors $g' := \varphi_*(g)$ von f', so kann man Φ im vorigen Satz so finden, daß $\Phi(a) = a'$ ist.*

Beweis. Zunächst haben wir wie im voranstehenden Beweis $\varphi_1\colon k(a) \to k'(a')$ mit $\varphi_1(a) = a'$. Wir können sodann den vorigen Satz auf φ_1 anwenden, da $k(a) \subset$ ein Zerfällungskörper von $f \in k(a)[x]$ ist. □

Ein Zerfällungskörper eines Polynoms $f \in k[x]$ wird durch Adjunktion aller Nullstellen von f an k erhalten. Verschiedene Polynome können jedoch denselben Zerfällungskörper haben. Um sich von der Auswahl eines Polynoms zu befreien, erhebt sich die Frage: Gibt es eine Eigenschaft, die Zerfällungskörper charakterisiert? Zur Beantwortung dienen die folgenden Definitionen.

Eine algebraische Erweiterung $K|k$ heißt *normal*, wenn jedes irreduzible Polynom $f \in k[x]$, das in K wenigstens eine Nullstelle hat, über K in Linearfaktoren zerfällt, wenn also die Minimalpolynome der Elemente $a \in K$ über K in Linearfaktoren zerfallen. Wir haben schon gesehen, daß Galois-Erweiterungen normal sind.

Wir wollen auch Adjunktion von unendlich vielen Nullstellen zulassen und definieren deshalb: Sei $S \subset k[x]$ eine Menge von nichtkonstanten Polynomen. Ein *Zerfällungskörper* von S ist eine Körpererweiterung $K|k$, über der jedes $f \in S$ in

Linearfaktoren zerfällt, bei der aber kein echter Zwischenkörper diese Eigenschaft hat.

(6.7) Satz. *Eine algebraische Erweiterung $K|k$ ist genau dann normal, wenn sie Zerfällungskörper einer geeigneten Menge $S \subset k[x]$ ist. Eine endliche Erweiterung ist genau dann normal, wenn sie Zerfällungskörper eines Polynoms ist.*

Beweis. Sei $K|k$ normal. Wir wählen eine Menge $A \subset K$, mit der $K = k(A)$ gilt (Erzeugendensystem). Das Minimalpolynom f_a von $a \in A$ zerfällt über K in Linearfaktoren, da $K|k$ normal ist. Also ist $K|k$ Zerfällungskörper von $S = \{f_a \mid a \in A\}$. Ist A endlich, so ist $K|k$ auch Zerfällungskörper des Produkts $\prod_{a\in A} f_a$.

Sei umgekehrt $K|k$ Zerfällungskörper von S. Sei $g \in k[x]$ ein irreduzibles Polynom, das in K eine Nullstelle a_1 hat. Da K von den Nullstellen der Polynome in S über k erzeugt wird, gibt es eine endliche Teilmenge E von S, so daß a_1 in dem Zerfällungskörper L von E liegt. Wir können dann annehmen, daß L Zerfällungskörper eines Polynoms f ist (Produkt der Polynome in E). Wir zeigen, daß g schon über L in Linearfaktoren zerfällt. Die Erweiterung $L|k$ ist endlich.

Falls g noch nicht zerfällt, wählen wir einen Zerfällungskörper $M|L$ von g. Sei a_2 eine weitere Nullstelle von g in M. Wir zeigen:

$$[L(a_1) : L] = [L(a_2) : L]. \tag{6.8}$$

Falls das gezeigt ist, folgt wegen $a_1 \in L$, daß $[L(a_2) : L] = 1$ ist, also $L(a_2) = L$ und $a_2 \in L$. Bleibt also (5.8) zu zeigen.

Für $j = 1, 2$ gilt:

$$[L(a_j) : L][L : k] = [L(a_j) : k] = [L(a_j) : k(a_j)][k(a_j) : k]. \tag{6.9}$$

Also genügt es, in (5.9) die Gleichheit der rechten Seiten zu zeigen. Da a_1, a_2 Nullstellen des irreduziblen Polynoms g sind, gibt es einen k-Isomorphismus $\varphi\colon k(a_1) \to k(a_2)$, siehe (5.3). Deshalb gilt schon einmal $[k(a_1) : k] = [k(a_2) : k]$. Da $L|k$ Zerfällungskörper von $f \in k[x]$ ist, so ist $L(a_j)|k(a_j)$ Zerfällungskörper von $f \in k(a_j)[x]$, siehe (5.4). Nach (5.5) läßt sich φ zu einem Isomorphismus $L(a_1) \to L(a_2)$ fortsetzen. Insbesondere ist $[L(a_1) : k(a_1)] = [L(a_2) : k(a_2)]$. □

Aus (5.4) und (5.7) ergibt sich:

(6.10) Folgerung. *Ist $L|k$ normal und $L|K|k$, so ist $L|K$ normal.* □

(6.11) Aufgaben und Ergänzungen.

1. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist Zerfällungskörper von x^4-10x^2+1 und von $(x^2-2)(x^2-3)$ über $\mathbb{Q}$. Das eine Polynom ist irreduzibel, das andere nicht.

7 Separable Erweiterungen

Kann ein irreduzibles Polynom in einem Erweiterungskörper mehrfache Nullstellen haben? In der Analysis lassen sich mehrfache Nullstellen durch die Nullstellen

der Ableitung finden. Die Formeln für die Ableitung werden formal auf Polynome übertragen.

Ist $f = a_0 + a_1 x + \cdots + a_n x^n \in k[x]$, so setzen wir

$$Df = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \in k[x].$$

Da ein Polynom eindeutig durch seine Koeffizienten bestimmt ist, wird durch diese Vorschrift eine k-lineare Abbildung $D\colon k[x] \to k[x]$ gegeben, die wir *formale Differentiation* nennen. Die Definition von D läßt sich für jeden kommutativen Ring k geben. Ist $k \subset K$, so ist D mit der Inklusion $k[x] \subset K[x]$ verträglich. Die Differentiation erfüllt auch die übliche Produktregel:

(7.1) Notiz. *Für $f, g \in k[x]$ gilt $D(fg) = fD(g) + D(f)g$.*

Beweis. Sei $f = \sum_i a_i x^i$ und $g = \sum_j b_j x^j$. Dann ist $fg = \sum_k c_k x^k$ mit $c_k = \sum_{i+j=k} a_i b_j$. Man berechnet die Koeffizienten von x^k in $D(fg)$, $fD(g)$ und $D(f)g$ der Reihe nach zu $(k+1)c_{k+1}$, $\sum_{i+j=k} a_i (j+1) b_{j+1}$ und $\sum_{i+j=k} (i+1) a_{i+1} b_j$, woraus die behauptete Gleichheit folgt. □

Es ist zu beachten, daß in einem Körper der Charakteristik $p > 0$ die Werte pm gleich Null sind, so daß zum Beispiel $D(x^p) = p x^{p-1} = 0$ ist. Wir notieren diesen Sachverhalt für späteren Gebrauch:

(7.2) Notiz. *Sei $f \in k[x]$. Hat k die Charakteristik Null, so gilt $Df = 0$ genau dann, wenn f konstant ist. Hat k die Charakteristik $p > 0$, so gilt $Df = 0$genau dann, wenn $f(x) = g(x^p)$ für ein $g \in k[x]$.* □

(7.3) Notiz. *Sei $f \in k[x]$ ein nichtkonstantes Polynom, das in einem Erweiterungskörper K eine n-fache Nullstelle $a \in K$ habe ($n \geq 1$). Dann gilt:*

(1) $n = 1 \iff (Df)(a) \neq 0$.

(2) $n > 1 \iff (Df)(a) = 0$.

Beweis. Es gibt über K eine Zerlegung $f = (x-a)^n \cdot g$ mit $g(a) \neq 0$. Mit (6.1) folgt

$$Df = n(x-a)^{n-1} \cdot g + (x-a)^n \cdot Dg.$$

Ist $n = 1$, so folgt $(Df)(a) = g(a) \neq 0$. Ist $n > 1$, so folgt $(Df)(a) = 0$. □

Aus der vorstehenden Notiz leiten wir nun ein Kriterium her, im dem der Zerfällungskörper nicht bekannt sein muß. Entscheidend dafür ist, daß D und der GGT mit Körpererweiterungen verträglich sind (1.7).

(7.4) Satz. *Ein nichtkonstantes Polynom $f \in k[x]$ hat genau dann in einem geeigneten Erweiterungskörper mehrfache Nullstellen, wenn f und Df einen nichtkonstanten gemeinsamen Teiler haben.*

Beweis. Sei a mehrfache Nullstelle von f im Erweiterungskörper K. Nach (6.3) gilt dann $f(a) = 0 = Df(a)$. Das Minimalpolynom $g \in K[x]$ von a ist ein gemeinsamer Teiler von f und Df als Polynom in $K[x]$. Der GGT von f und Df in $k[x]$ hat dann über K jedenfalls g als Teiler und ist somit nicht konstant.

Sei umgekehrt g ein gemeinsamer Teiler von f und Df von positivem Grad. Für eine Nullstelle a von g in einem Erweiterungskörper gilt dann $f(a) = 0 = Df(a)$, also nach (6.3) $n > 1$. □

Ein irreduzibles Polynom $f \in k[x]$ heißt *separabel*, wenn es in keinem Erweiterungskörper mehrfache Nullstellen hat. Ein Polynom heißt *separabel*, wenn alle irreduziblen Faktoren separabel sind. Ein $a \in K \supset k$ heißt *separabel* über k, wenn das Minimalpolynom $f \in k[x]$ von a separabel ist. Eine algebraische Erweiterung $K|k$ heißt *separabel*, wenn jedes $a \in K$ separabel ist. Ein Körper k heißt *vollkommen* oder *perfekt*, wenn jedes irreduzible Polynom $f \in k[x]$ separabel ist.

(7.5) Satz. *Ein irreduzibles Polynom $f \in k[x]$ ist genau dann separabel, wenn $Df \neq 0$ ist.*

Beweis. Sei $Df \neq 0$. Da Df einen kleineren Grad als f hat und f irreduzibel ist, gilt $(f, Df) = (1)$ und nach (6.4) ist f separabel. Ist $Df = 0$, so ist f nach (6.4) nicht separabel. □

Zusammen mit (6.2) ergibt sich:

(7.6) Folgerung. *Ein Körper der Charakteristik Null ist vollkommen.* □

(7.7) Satz. *Ein Körper k der Charakteristik $p > 0$ ist genau dann vollkommen, wenn $k \to k$, $a \mapsto a^p$ surjektiv ist. Das ist insbesondere für endliche Körper der Fall.*

Beweis. Wir zeigen zunächst: Ist $a \mapsto a^p$ surjektiv, so ist jedes Polynom, das nur Potenzen von x^p enthält, selbst eine p-te Potenz. Nach Voraussetzung können wir nämlich in dem Polynom $a_0 + a_p x^p + \cdots + a_{mp} x^{mp}$ das Element $a_{jp} = b_j^p$ schreiben. Dann benutzen wir

$$(\sum_j b_j x^j)^p = \sum_j b_j^p x^{jp}.$$

Ist f irreduzibel und $Df = 0$, so wäre also mittels (6.2) f eine p-te Potenz, im Widerspruch zur Irreduzibilität. Also ist jedes irreduzible Polynom separabel und somit der Körper vollkommen.

Sei umgekehrt $a \in k$ keine p-te Potenz. Sei $b \in K \supset k$ eine Nullstelle von $x^p - a \in k[x]$. Dann ist $x^p - a = x^p - b^p = (x - b)^p$. Sei f ein irreduzibler Faktor von $x^p - a$. Dann zerfällt f als Teiler von $x^p - a$ über K ebenfalls in Faktoren $x - b$. Wäre $f = x - b$, so wäre $b \in k$, also a in k eine p-te Potenz, was wir ausgeschlossen hatten. Mithim ist $f = (x - b)^t$ mit $t > 1$ ein inseparables irreduzibles Polynom über k und damit k nicht vollkommen.

Die Abbildung $a \mapsto a^p$ ist ein Körperhomomorphismus, also injektiv. Im Falle eines endlichen Körper ist sie also auch surjektiv. □

(7.8) Beispiel. Wir konstruieren eine inseparable Erweiterung. Dazu muß man einen Körper k der Charakteristik p angeben, für den $a \mapsto a^p$ nicht surjektiv ist.

Sei $K = \mathbb{F}_p(x)$ der Funktionenkörper. Darin ist x keine p-te Potenz. Aus $x = (f/g)^p$ mit $(f, g) = 1$ würde der Reihe nach folgen: $g^p = xf^p$, $x|g$, $x|f$. Widerspruch zu $(f, g) = 1$. ◇

8 Endliche Körper

In diesem Abschnitt klassifizieren wir die endlichen Körper.

(8.1) Satz. *Sei p eine Primzahl und $q = p^n$, $n \geq 1$. Dann gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ mit q Elementen. Er ist der Zerfällungskörper von $x^q - x \in \mathbb{F}_p[x]$.*

Beweis. Ein endlicher Körper $\mathbb{F}$ der Charakteristik p hat $q = p^n$ Elemente, für ein geeignetes $n \in \mathbb{N}$. Die multiplikative Gruppe $\mathbb{F}^*$ ist zyklisch. Deshalb gilt für $a \in \mathbb{F}$ die Gleichung $x^{q-1} - 1 = 0$. Folglich erfüllen alle Elemente von $\mathbb{F}^*$ die Gleichung $x^q - x = 0$. Dieses Polynom hat also q verschiedene Nullstellen und zerfällt deshalb über dem Primkörper $\mathbb{F}_p \subset \mathbb{F}$ in Linearfaktoren. Also ist nach Satz (5.1) $\mathbb{F}$ der Zerfällungskörper dieses Polynoms. Nach dem Eindeutigkeitssatz für Zerfällungskörper gibt es deshalb höchstens einen Körper mit q Elementen.

Sei umgekehrt $\mathbb{F}(q)$ der Zerfällungskörper des Polynoms $x^q - x$ über $\mathbb{F}_p$. Sei $M \subset \mathbb{F}(q)$ die Menge der Nullstellen des Polynoms. Aus $a, b \in M$ folgt $(a-b)^q - (a-b) = a^q - b^q - (a-b) = 0$, sowie $(ab)^q - ab = a^q b^q - ab = ab - ab = 0$ und (falls $b \neq 0$) $(b^{-1})^q - b^{-1} = (b^q)^{-1} - b^{-1} = b^{-1} - b^{-1} = 0$, d. h. $a-b, ab, b^{-1} \in M$. Also ist M ein Unterkörper von $\mathbb{F}(q)$, der sämtliche Nullstellen von $x^q - x$ enthält, folglich selbst schon der Zerfällungskörper, weshalb $M = \mathbb{F}(q)$ sein muß. Das Polynom $x^q - x \in \mathbb{F}_p[x]$ hat q *verschiedene* Nullstellen. Das folgt aus den Ergebnisssen des letzten Abschnittes, weil es teilerfremd zu seiner formalen Ableitung $qx^{q-1} - 1 = -1$ ist. Also hat der Körper $\mathbb{F}(q)$ wirklich q Elemente. □

Ist $\alpha \in \mathbb{F}_q$ ein erzeugendes Element von $\mathbb{F}_q^*$, so ist $\mathbb{F}_q = \mathbb{F}_p(\alpha)$. Das Minimalpolynom von α hat den Grad n. Also gibt es in $\mathbb{F}_p[x]$ irreduzible Polynome beliebigen Grades.

9 Darstellungen von Gruppen

1 Grundbegriffe

Sei G eine Gruppe und V ein Vektorraum über dem Körper K. Eine *Darstellung* von G mit dem *Darstellungsraum* V oder eine *Darstellung* von G *auf* V ist eine Operation $G \times V \to V$ von G auf V, so daß für jedes $g \in G$ die Linkstranslation $l_g: V \to V$, $v \mapsto gv$ eine K-lineare Abbildung ist. Wir sagen dann auch, V ist eine Darstellung von G oder eine *G-Darstellung* und nennen V einen *G-Vektorraum*. Die Dimension von V heißt *Dimension* der Darstellung. Sind V und W G-Darstellungen, so ist ein *Morphismus* oder *Homomorphismus* $f: V \to W$ zwischen den Darstellungen eine K-lineare G-äquivariante Abbildung f, also eine lineare Abbildung, für die $f(gv) = gf(v)$ für $g \in G$ und $v \in V$ gilt. Wir bezeichnen mit $\mathrm{Hom}_G(V, W)$ den K-Vektorraum der Morphismen $V \to W$. Darstellungen und ihre Morphismen bilden eine Kategorie. Damit sind auch die Begriffe Isomorphismus, Endomorphismus und Automorphismus definiert. Die *direkte Summe* zweier G-Darstellungen V, W ist die direkte Summe $V \oplus W$ von Vektorräumen mit der komponentenweisen Operation $g(v, w) = (gv, gw)$. Analog für beliebig viele Summanden. Ein Unterraum U einer Darstellung V, der G-stabil ist (also $g \in G, u \in U \Rightarrow gu \in U$ erfüllt), heißt *Unterdarstellung*. Der Quotientraum V/U nach einer Unterdarstellung trägt genau eine Struktur einer Darstellung, für die die Quotientabbildung $V \to V/U$ ein Morphismus ist. Eine Darstellung $V \neq 0$ heißt *einfach* oder *irreduzibel*, wenn sie nur 0 und V als Unterdarstellungen hat. Eine Darstellung V heißt *unzerlegbar*, wenn sie keine direkte Zerlegung $V = U_1 \oplus U_2$ in von Null verschiedene Unterdarstellungen U_j hat. Eine irreduzible Darstellung ist offenbar unzerlegbar. Eine Darstellung heißt *trivial*, wenn jedes Gruppenelement als die Identität operiert.

Die Axiome einer Darstellung besagen, daß $g \mapsto l_g$ ein Homomorphismus $l: G \to GL(V)$ von G in die Gruppe $GL(V)$ der linearen Automorphismen von V ist. Ist V n-dimensional, so wird l nach Wahl einer Basis durch einen Homomorphismus $G \to GL(n, K)$ gegeben. Ein solcher Homomorphismus heißt *Matrixdarstellung* von G. Eine Darstellung heißt *treu*, wenn l injektiv ist. Jeder Homomorphismus $G \to GL(V)$ entsteht auf diese Weise aus einer Darstellung auf V. Nach dem Basiswechselsatz der linearen Algebra liefern zwei Homomorphismen $f, g: G \to GL(n, K)$ genau dann isomorphe Darstellungen, wenn sie *konjugiert* sind, d. h. wenn es ein $A \in GL(n, K)$ so gibt, daß für alle $x \in G$ die Gleichung $f(x) = Ag(x)A^{-1}$ gilt.

Die *Standarddarstellung* von $GL(n, K)$ ist durch die Matrizenmultiplikation $GL(n, K) \times K^n \to K^n$, $(A, x) \mapsto Ax$ gegeben. Die *Determinantendarstellung* wird durch den Homomorphismus $\det: GL(n, K) \to K^*$ vermittelt.

Der folgende Satz ist unter dem Namen *Lemma von Schur* bekannt.

(1.1) Satz. *Seien E und F irreduzible Darstellungen. Ein Homomorphismus*

$f: E \to F$ ist entweder Null oder ein Isomorphismus. Der Endomorphismenring $R = \mathrm{Hom}_G(E, E)$ ist ein Schiefkörper. Ist K algebraisch abgeschlossen, so ist $K \to R$, $\lambda \mapsto \lambda \cdot \mathrm{id}$ ein Isomorphismus.

Beweis. Sei f von Null verschieden. Dann hat f trivialen Kern, da E irreduzibel ist. Also ist f injektiv; und das Bild ist gleich F, weil F irreduzibel ist. Das zeigt die erste Aussage und außerdem, daß jedes von Null verschiedene Element von R eine Einheit ist. Ist K algebraisch abgeschlossen, so hat f einen Eigenwert λ. Sei $E(\lambda)$ der zugehörige Eigenraum. Für $g \in G$ und $v \in E(\lambda)$ gilt $f(gv) = gf(v) = \lambda(gv)$. Also ist $gv \in E(\lambda)$ und somit $E(\lambda)$ eine Unterdarstellung. Da E irreduzibel ist, gilt $E = E(\lambda)$ und also $f = \lambda \cdot \mathrm{id}$. □

(1.2) Permutationsdarstellungen. Sei S eine G-Menge und $K(S) = KS$ der freie K-Vektorraum über S. Die Linksoperation von G auf S wird linear fortgesetzt und liefert eine Darstellung auf KS, die *Permutationsdarstellung* von S heißt, weil die Gruppenelemente die Basiselemente permutieren. Ist $S = G$ mit der G-Operation durch Linkstranslation, so heißt die zugehörige Darstellung die *reguläre Darstellung*. Die reguläre Darstellung ist offenbar treu. ◇

Bekannte Konstruktionen der linearen Algebra liefern neue Darstellungen aus gegebenen. Die direkte Summe haben wir schon erwähnt. Sind V und W Darstellungen von G, so wird das Tensorprodukt $V \otimes W$ eine G-Darstellung, indem $g \in G$ durch die lineare Abbildung $l_g \otimes l_g$ wirkt. Wir nennen $V \otimes W$ das *Tensorprodukt* der gegebenen Darstellungen. Auf dem Dualraum $V^* = \mathrm{Hom}_K(V, K)$ operiert $g \in G$ durch $(g \cdot \varphi)(v) = \varphi(g^{-1}v)$. Damit wird V^* die *duale* Darstellung. Auf $\mathrm{Hom}_K(V, W)$ operiert $g \in G$ durch $(g \cdot \varphi)(v) = g\varphi(g^{-1}v)$, und damit wird eine Darstellung gegeben.

Kanonische Isomorphismen zwischen Vektorraumkonstruktionen liefern Isomorphismen der zugehörigen Darstellungen. Zum Beispiel haben wir einen kanonischen Isomorphismus

$$\mathrm{Hom}_K(V, W) \cong V^* \otimes W \tag{1.3}$$

zwischen Darstellungen. Direkte Summen und Tensorprodukte sind assoziativ und kommutativ, bis auf natürliche Isomorphie. Es gilt das Distributivgesetz:

$$(U \oplus V) \otimes W \cong (U \otimes W) \oplus (V \otimes W). \tag{1.4}$$

Wir behandeln im folgenden nur endlichdimensionale Darstellungen endlicher Gruppen. Unser Ziel ist eine Zerlegung von Darstellungen in irreduzible und eine Übersicht über irreduzible Darstellungen.

(1.5) Eindimensionale Darstellungen. Sei V eine eindimensionale Darstellung von G. Dann ist $l_g: V \to V$ die Multiplikation mit einem Skalar $\lambda(g) \in K^*$. Die Zuordnung $\chi_V: G \to K^*$, $g \mapsto \lambda(g)$ ist ein Homomorphismus. Allgemein heißt ein Homomorphismus $\chi: G \to K^*$ *Charakter* von G. Jeder Charakter χ liefert eine eindimensionale Darstellung auf $V = K$ durch $l_g(v) = \chi(g)v$. Da K^* abelsch ist, sind zwei eindimensionale Darstellungen genau dann isomorph, wenn

ihre Charaktere gleich sind. Das Produkt zweier Charaktere χ und φ ist durch $(\chi \cdot \varphi)(g) = \chi(g)\varphi(g)$ erklärt und wieder ein Charakter. Mit dieser Verknüpfung wird die Menge $X(G, K)$ der Charaktere mit Werten in K^* eine abelsche Gruppe, die *Charaktergruppe* von G mit Werten in K heißt.

Da ein Charakter $\chi\colon G \to K^*$ ein Homomorphismus in eine abelsche Gruppe ist, faktorisiert er über die Projektion $G \to G^{ab}$ auf die abelsch gemachte Gruppe.

Es gibt n verschiedene eindimensionale Darstellungen der zyklischen Gruppe $\mathbb{Z}/n$ über den komplexen Zahlen. Ist $\zeta = \exp(2\pi i/n)$, so sind sie durch

$$\chi^k\colon t \bmod n \mapsto \zeta^{kt}$$

gegeben $(0 \le k \le n-1)$. ◇

(1.6) Satz. *Eine endlichdimensionale irreduzible Darstellung einer abelschen Gruppe über einem algebraisch abgeschlossenen Körper ist eindimensional.*

Beweis. Für abelsches G ist jede Linkstranslation l_g ein Endomorphismus von Darstellungen. Nach (1.1) ist l_g ein Vielfaches der Identität. Dann ist aber jeder Untervektorraum eine Unterdarstellung. □

Eine allgemeine Eigenschaft von Charakteren ist ihre lineare Unabhängigkeit.

(1.7) Satz. *Seien $\chi_1, \dots, \chi_n$ paarweise verschiedene Charaktere einer beliebigen Gruppe G mit Werten in K^*. Dann sind sie im K-Vektorraum aller Funktionen $G \to K$ linear unabhängig.*

Beweis. Induktion nach n. Sei eine echte lineare Relation

$$a_1\chi_1 + \cdots + a_n\chi_n = 0, \qquad a_j \in K$$

gegeben. Wir nehmen an, n mit dieser Eigenschaft sei minimal. Dann ist $n \ge 2$, und alle a_j sind von Null verschieden. Da χ_1 und χ_2 verschieden sind, gibt es eine Stelle $z \in G$, an der sie sich unterscheiden. Aus der für alle $x \in G$ bestehenden Relation

$$a_1\chi_1(xz) + \cdots + a_n\chi_n(xz) = 0$$

folgt, weil die χ_j Charaktere sind,

$$a_1\chi_1(z)\chi_1 + \cdots + a_n\chi_n(z)\chi_n = 0.$$

Wir multiplizieren die Ausgangsrelation mit $\chi_1(z)$, subtrahieren von der letzten und erhalten

$$(a_2\chi_2(z) - a_2\chi_1(z))\chi_2 + \cdots = 0.$$

Der erste Koeffizient ist von Null verschieden und deshalb die Relation kürzer. Widerspruch. □

Der Beweis des letzten Satzes benutzt übrigens nur, daß die χ_j Homomorphismen einer Menge G mit Verknüpfung sind; Assoziativität, sowie Existenz des neutralen Elementes und der Inversen wird nicht verwendet.

Wir ordnen nun die Darstellungstheorie in die Modultheorie ein. Wir erinnern an die Gruppenalgebra KG der Gruppe G über dem Körper K. Additiv handelt es sich um die freie abelsche Gruppe über G. Die Multiplikation ist durch bilineare Fortsetzung der Gruppenmultiplikation gegeben, das Produkt zweier Elemente ist also durch die folgende Formel definiert

$$(\sum_{g\in G}\lambda_g g)\cdot(\sum_{h\in G}\mu_h h)=\sum_{g,h\in G}\lambda_g\mu_h gh.$$

Ist V eine Darstellung von G über K, so wird V ein KG-Modul, wenn wir $\sum_{g\in G}\alpha_g g$ durch $(\sum_{g\in G}\alpha_g g)(v)=\sum_g \alpha_g(gv)$ operieren lassen, d. h. wir betrachten nicht nur die Linkstranslationen der Gruppenelemente sondern auch beliebige Linearkombinationen davon. Ist umgekehrt ein KG-Modul gegeben, so erhalten wir daraus eine G-Darstellung, indem wir $g\in G$ durch die Skalarmultiplikation des Basiselementes $g\in KG$ definieren. Auf diese Weise entsprechen sich KG-Moduln und G-Darstellungen. Morphismen von G-Darstellungen gehen bei dieser Entsprechung in KG-lineare Abbildungen über. Die Kategorie der G-Darstellungen ist äquivalent zur Kategorie KG-Mod der KG-Moduln. Direkte Summen entsprechen sich.

Übrigens kann man KG-Moduln natürlich auch betrachten, wenn K ein beliebiger kommutativer Ring ist. Das führt zu der allgemeineren Darstellungstheorie über K-Moduln.

Die in den folgenden Abschnitten entwickelte Darstellungstheorie ist in weiten Teilen unabhängig von der Modultheorie. Es ist jedoch hilfreich, sie in die Modultheorie einzuordnen.

(1.8) Aufgaben und Ergänzungen.

1. Sei G^* die Charaktergruppe von G über den komplexen Zahlen. Es gibt einen kanonischen Isomorphismus $(G\times H)^*\cong G^*\times H^*$. Für endliche abelsche Gruppen ist G zu G^* isomorph.

2. Ein Homomorphismus $\alpha\colon A\to B$ induziert durch Zusammensetzung mit Charakteren einen dualen Homomorphismus $\alpha^*\colon B^*\to A^*$. Sei

$$A \xrightarrow{\ \alpha\ } B \xrightarrow{\ \beta\ } C$$

eine exakte Sequenz von endlichen abelschen Gruppen. Dann ist auch die duale Sequenz

$$A^* \xleftarrow{\ \alpha^*\ } B^* \xleftarrow{\ \beta^*\ } C^*$$

exakt.

3. Die Darstellung

$$(\mathbb{R},+)\to GL(2,\mathbb{R}),\quad t\to\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}$$

ist unzerlegbar aber nicht irreduzibel.

4. Durch $(A, X) \to AXA^{-1}$ wird eine Darstellung von $GL(n, K)$ auf dem Vektorraum $M_n(K)$ der (n, n)-Matrizen über K definiert (

adjungierte Darstellung von $GL(n, K)$). Die Matrizen mit der Spur Null bilden eine Unterdarstellung. Ist letztere irreduzibel?

5. Sei V eine G-Darstellung und W eine H-Darstellung über K. Dann wird $\mathrm{Hom}_K(V, W)$ eine $G \times H$-Darstellung durch die Vorschrift $((g, h) \cdot \varphi)(v) = g\varphi(h^{-1}v)$. Durch die Vorschrift $(g, h) \cdot (v \otimes w) = (gv, hw)$ wird $V \otimes W$ eine $G \times H$-Darstellung, die wir zur Unterscheidung vom Tensorprodukt weiter oben auch *äußeres* Tensorprodukt von V und W nennen. Der Isomorphismus (1.3) von K-Vektorräumen wird durch

$$\varphi \otimes w \mapsto (v \mapsto \varphi(v)w)$$

gegeben. Er ist mit den soeben definierten Darstellungen ein Isomorphismus von $G \times H$-Darstellungen.

6. Ist $\varphi\colon G \to H$ eine Gruppenhomomorphismus, so wird aus einer H-Darstellung V eine G-Darstellung φ^*V mit demselben Vektorraum aber der Operation $(g, v) \mapsto \varphi(g)v$. Ist φ die Inklusion einer Untergruppe, so nennen wir φ^*V auch die *Restriktion* $\mathrm{res}^G_H V$ von V auf H. Die Zuordnung $V \mapsto \varphi^*V$ ist mit Homomorphismen verträglich, wir erhalten also einen Funktor

$$\varphi^*\colon KH\text{-}\,\mathrm{Mod} \to KG\text{-}\,\mathrm{Mod}\,.$$

7. Für Permutationsdarstellungen von G gibt es kanonische Isomorphismen

$$K(S \amalg T) \cong K(S) \oplus K(T), \qquad K(S \times T) \cong K(S) \otimes K(T).$$

8. Sei V eine G-Darstellung über K und α ein K-wertiger Charakter. Durch die Operation $g \cdot v := \alpha(g)gv$ wird eine Darstellung von G auf dem Vektorraum V definiert. Ist W ein Darstellungsraum von α, so ist diese Darstellung zu $W \otimes V$ isomorph.

9. Der Gruppenring KC_n der zyklischen Gruppe C_n der Ordnung n ist isomorph zu $K[x]/(x^n - 1)$.

2 Direkte Zerlegungen

Wir legen einen festen Körper K zugrunde. Er habe die Eigenschaft, daß die Gruppenordnung $|G|$ in ihm invertierbar sei. Das bedeutet: Es gibt ein $x \in K$, so daß $|G|x = 1$ ist. Wir schreiben $x = \frac{1}{|G|}$. Die Bedingung an K ist genau dann erfüllt, wenn die Charakteristik von K die Ordnung $|G|$ nicht teilt. Zur Erinnerung: Für $n \in \mathbb{N}$ und $y \in K$ wird unter ny die Summe $y + \cdots + y$ von n Summanden y verstanden. Unter der genannten Voraussetzung ist jede Darstellung direkte Summe irreduzibler. Der folgende Satz ist unter dem Namen *Satz von Maschke* bekannt.

(2.1) Satz. *Jede Unterdarstellung einer Darstellung ist ein direkter Summand. Insbesondere ist jede G-Darstellung direkte Summe irreduzibler Darstellungen.*

BEWEIS. Die zweite Aussage folgt offenbar sofort aus der ersten durch Induktion nach der Dimension. Sei W Unterdarstellung von V. Genau dann ist W ein direkter Summand, wenn es einen Projektionsoperator $q\colon V \to V$ mit dem Bild W gibt. Ein Projektionsoperator ist ein Morphismus q mit der Eigenschaft $q^2 = q$. Für eine Projektion gilt immer $V = \operatorname{Bild} q \oplus \operatorname{Kern} q$.

Es gibt sicherlich eine K-lineare Projektion $p\colon V \to V$ mit dem Bild W. Wir machen sie durch Mittelwertbildung künstlich G-äquivariant, indem wir definieren

$$q(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1} p(gv).$$

An dieser Stelle wird gebraucht, daß die Ordnung $|G|$ in K invertierbar ist. Als Linearkombination K-linearer Abbildungen ist q wieder K-linear. Für $h \in G$ rechnen wir

$$q(hv) = \frac{1}{|G|} \sum g^{-1} p(ghv) = \frac{1}{|G|} h \sum h^{-1} g^{-1} p(ghv) = hq(v).$$

Das ist die Äquivarianz. Für $w \in W$ ist $p(w) = w$, also $p(gw) = gw$ und folglich $q(w) = w$. Nach Konstruktion liegt $q(v)$ immer in W. □

Der folgende Satz liefert die Eindeutigkeit der Zerlegung in irreduzible Summanden.

(2.2) Satz. *Sei $V = V_1 \oplus \cdots \oplus V_r$ eine direkte Zerlegung in irreduzible Darstellungen V_j und W irreduzibel. Sei $d(W) = \dim \operatorname{Hom}_G(W, W)$. Die Anzahl $n(W, V)$ der V_j, die zu W isomorph sind, ist gleich $d(W)^{-1} \dim \operatorname{Hom}_G(W, V)$ und auch gleich $d(W)^{-1} \dim \operatorname{Hom}_G(V, W)$.*

BEWEIS. Es gilt allgemein für eine endliche direkte Summe wie im Satz

$$\operatorname{Hom}_G(W, V) \cong \prod_j \operatorname{Hom}_G(W, V_j).$$

Die Behauptung ist damit eine direkte Folge aus dem Schurschen Lemma (1.1). Analog für die zweite Aussage. □

Wir verwenden im weiteren die folgenden Bezeichnungen: $I = \operatorname{Irr}(G, K)$ sei ein vollständiges System paarweise nichtisomorpher irreduzibler Darstellungen von G über K. Mit nW bezeichnen wir die n-fache direkte Summe von W mit sich selbst. Ist

$$V = \bigoplus_{W \in I} n_W W,$$

so heißt n_W die *Multiplizität* von W in V. Ist $n_W \neq 0$, so sagen wir auch, W (oder jede dazu isomorphe Darstellung) kommt in V vor. Wir notieren an dieser Stelle schon ein vorläufiges Ergebnis:

(2.3) Notiz. *Die Menge I ist endlich. Jede irreduzible Darstellung kommt in der regulären Darstellung vor.*

BEWEIS. Für jedes U ist $\mathrm{Hom}_G(KG, U) \to U$, $\varphi \mapsto \varphi(e)$ ein Isomorphismus. Wird KG direkt zerlegt, so gibt es also in KG nach dem Schurschen Lemma einen zu U isomorphen Summanden. Da KG endlichdimensional ist, gibt es darin nach (2.2) nur endlich viele verschiedene irreduzible Summanden. □

Für $W \in I$ sei $V(W)$ die Summe aller zu W isomorphen Unterdarstellungen von V. Eine Summe von Unterdarstellungen $(U_j \mid j \in J)$ ist dabei die kleinste Unterdarstellung, die alle U_j enthält; als Vektorraum ist sie gleich der Summe der Unterräume U_j. Wir nennen $V(W)$ den *W-isotypischen* Anteil von V, falls $V(W) \neq 0$ ist, und die Zerlegung aus dem nächsten Satz die *isotypische Zerlegung* von V.

(2.4) Lemma. *Sei V Summe irreduzibler Unterdarstellungen $(A_j \mid j \in J)$ und B eine irreduzible Unterdarstellung von V. Dann ist B zu einem A_j isomorph.*

BEWEIS. Nach dem Satz von Maschke gibt es einen surjektiven Homomorphismus $\beta: V \to B$. Ist B zu keinem A_j isomorph, so ist die Einschränkung von β auf alle A_j nach dem Schurschen Lemma gleich Null, also β überhaupt Null. Widerspruch. □

(2.5) Satz. *Jede Darstellung ist direkte Summe ihrer isotypischen Bestandteile.* □

BEWEIS. Nach (2.1) ist V direkte Summe irreduzibler Unterdarstellungen, also jedenfalls Summe der isotypischen Bestandteile. Sei W die Summe der von $V(A)$ verschiedenen isotypischen Bestandteile $V(A_j)$. Wir haben zu zeigen: $V(A) \cap W = 0$. Wäre dem nicht so, so gäbe es in dem Durchschnitt eine irreduzible Unterdarstellung, die nach dem letzten Lemma zu A und zu einem A_j isomorph wäre. Widerspruch. □

Wir geben der isotypischen Zerlegung noch eine präziesere Gestalt. Sei $D(U) = \mathrm{Hom}_G(U, U)$ die Endomorphismenalgebra von U. Dann ist U ein $D(U)$-Linksmodul durch $(\varphi, u) \mapsto \varphi(u)$ und $\mathrm{Hom}_G(U, V)$ ein $D(U)$-Rechtsmodul durch $(\alpha, \varphi) \mapsto \alpha \circ \varphi$. Auf dem Tensorprodukt $\mathrm{Hom}_G(U, V) \otimes_{D(U)} U$ operiert G durch $(g, \alpha \otimes v) \mapsto \alpha \otimes gv$ und macht daraus eine G-Darstellung. Die Abbildung

$$\iota_U: \mathrm{Hom}_G(U, V) \otimes_{D(U)} U \to V, \quad \varphi \otimes u \mapsto \varphi(u)$$

ist dann ein Morphismus von G-Darstellungen. Sei

$$\iota: \bigoplus_{U \in I} \mathrm{Hom}_G(U, V) \otimes_{D(U)} U \to V$$

die Summe dieser Abbildungen ι_U.

(2.6) Satz. *Abbildung ι ist ein in der Variablen V natürlicher Isomorphismus. Das Bild von ι_U ist der U-isotypische Bestandteil.*

BEWEIS. Zur Abkürzung bezeichnen wir die Quelle von ι mit $S(V)$. Ist $\psi: V \to W$ ein Homomorphismus, so haben wir einen induzierten Homomorphismus von

G-Darstellungen $S(\psi)\colon S(V) \to S(W)$, indem wir $\mathrm{Hom}_G(U,V) \to \mathrm{Hom}_G(U,W)$ durch Zusammensetzung mit ψ bilden und auf dem Faktor U die Identität verwenden. Dadurch wird S ein Funktor. Das Diagramm

$$\begin{array}{ccc} S(V) & \xrightarrow{\iota} & V \\ \downarrow{\scriptstyle S(\psi)} & & \downarrow{\scriptstyle \psi} \\ S(W) & \xrightarrow{\iota} & W \end{array}$$

ist kommutativ, d. h. ι ist eine natürliche Transformation. Ist $i_j\colon V_j \to V$ eine direkte Summe von V, so ist $S(i_j)$ eine direkte Summe von $S(V)$. Damit und mit der Kommutativität des letzten Diagrammes folgert man leicht: Ist ι für V_1 und V_2 ein Isomorphismus, so auch für die direkte Summe $V_1 \oplus V_2$. Es genügt deshalb, die Isomorphie für irreduzibles V nachzuweisen. Dann handelt es sich um eine einfache Verifikation aus den Definitionen mit Hilfe des Schurschen Lemmas. □

Wir bezeichnen mit $R^+(G,K)$ die Menge der Isomorphieklassen von G-Darstellungen über K. Auf dieser Menge wird durch die direkte Summe von Darstellungen die Struktur eines abelschen Monoids gegeben. Die Menge $I = \mathrm{Irr}(G,K)$ ist in folgendem Sinne eine Basis von $R^+(G,K)$: Jedes Element x hat eine eindeutige Darstellung der Form

$$x = \sum_{A \in I} n_A A, \qquad n_A \in \mathbb{N}_0.$$

Das ist eine Umformulierung der eindeutigen Zerlegung in irreduzible Summanden. Wir setzen für G-Darstellungen U und V

$$\langle\, U, V \,\rangle = \dim \mathrm{Hom}_G(U,V).$$

Diese natürliche Zahl häng nur von den Isomorphieklassen von U und V ab. Aus dem Schurschen Lemma folgt die *Orthogonalitätsrelation*:

(2.7) Notiz. *Sind U und V nichtisomorphe irreduzible Darstellungen, so ist* $\langle\, U, V \,\rangle = 0$. □

Wir notieren die folgenden Eigenschaften der Form $\langle\, -, - \,\rangle$:

$$\textbf{(2.8)} \qquad \begin{aligned} \langle V, W\rangle &= \langle W, V\rangle \\ \langle U \oplus V, W\rangle &= \langle U, W\rangle + \langle V, W\rangle. \end{aligned}$$

Die zweite Aussage folgt direkt aus der Definition; ebenso die analoge für direkte Zerlegungen des rechten Arguments. Sind $U = \bigoplus_{W \in I} u_W W$ und $V = \bigoplus_{W \in I} v_W W$ direkte Zerlegungen, so folgt mit (2.7)

$$\textbf{(2.9)} \qquad \langle\, U, V \,\rangle = \sum_W u_W v_W \langle\, W, W \,\rangle.$$

Daraus ergibt sich insbesondere die Symmetrie der Form. Wir erhalten somit eine symmetrische biadditive Form

$$\langle -, - \rangle \colon R^+(G,K) \times R^+(G,K) \to \mathbb{Z}, \quad (U,V) \mapsto \langle U, V \rangle.$$

(2.10) Folgerung. *Ist $\langle V, V \rangle = 1$, so ist V irreduzibel.* □

(2.11) Satz. *Seien S und T endliche G-Mengen. Dann gilt $\langle K(S), K(T) \rangle = |(S \times T)/G|$.*

Beweis. Beide Seiten sind additiv bezüglich disjunkter Summen in S. Es genügt deshalb, den Fall einer Bahn $S = G/A$ zu behandeln. Es gilt immer

$$\mathrm{Hom}_G(K(G/A), KT) \cong \mathrm{Abb}_G(G/A, KT) \cong (KT)^A.$$

Der erste Isomorphismus ist durch die universelle Eigenschaft des freien Vektorraums gegeben, der zweite ist durch $\alpha \mapsto \alpha(eA)$ induziert. Sei $T = \coprod_{j \in J} T_j$ die Zerlegung von T in A-Bahnen. Dann ist $KT \cong \bigoplus_{j \in J} KT_j$ als A-Darstellung. Ist $T_j = A/B$, so liegt ein Element $\sum_{aB \in A/B} n(aB)aB$ genau dann in der Fixpunktmenge von A, wenn die $n(aB)$ alle untereinander gleich sind. Also ist $(K(A/B))^A$ eindimensional. Es folgt $\langle K(G/A), KT \rangle = |J| = |T/A|$. □

(2.12) Aufgaben und Ergänzungen.

1. Die symmetrische Gruppe S_n operiert durch Permutation auf $T = \{1, \ldots, n\}$. Die Standgruppe von 1 ist isomorph zu S_{n-1} und besteht aus den Permutationen von $\{2, \ldots, n\}$. Bezüglich dieser S_{n-1}-Operation hat $\{1, \ldots, n\}$ zwei Bahnen. Ist KT die Permutationsdarstellung, so gilt $\langle KT, KT \rangle = 2$.

Wir stellen uns KT als K^n vor, und S_n operiert durch Permutation der Koordinaten. Sei V die Unterdarstellung $\{(x_1, \ldots, x_n) \mid \sum_j x_j = 0\}$ und W die Unterdarstellung $\{(x, \ldots, x) \mid x \in K\}$. Dann ist W eine triviale Darstellung. Ist n in K invertierbar, so ist KT die direkte Summe $V \oplus W$. Aus $\langle KT, KT \rangle = 2$ folgt dann $\langle V, V \rangle = 1$. Also ist V irreduzibel.

2. Ein Homomorphismus $G \to O(n)$ in die orthogonale Gruppe heißt *orthogonale* Darstellung. Eine orthogonale Darstellung ist direkte Summe irreduzibler. Analog für *unitäre* Darstellungen $G \to U(n)$.

3. Ein *invariantes Skalarprodukt* auf einer reellen Darstellung V ist ein Skalarprodukt auf V, das $\langle gv, gw \rangle = \langle v, w \rangle$ für alle $g \in G$ erfüllt. Eine Darstellung zusammen mit einem invarianten Skalarprodukt heißt ebenfalls orthogonale Darstellung. Ist G endlich und b ein beliebiges Skalarprodukt, so ist durch

$$c(v,w) = \frac{1}{|G|} \sum_{g \in G} b(gv, gw)$$

ein invariantes Skalarprodukt c gegeben. Analog für hermitesche Formen auf komplexen Darstellungen.

4. Sei $\mathbb{F}$ ein endlicher Körper der Charakteristik p und G eine p-Gruppe. Ist V

eine Darstellung von G über $\mathbb{F}$, so ist $|V| \equiv |V^G| \bmod p$, also V^G eine von Null verschiedene Unterdarstellung. Die einzige irreduzible Darstellung ist deshalb in diesem Fall die triviale eindimensionale. Die reguläre Darstellung $\mathbb{F}G$ hat eine eindimensionale Fixpunktmenge und ist deshalb unzerlegbar.

3 Charaktere

Wir setzen in diesem Abschnitt voraus, daß K die Charakteristik Null hat.

Ist V eine G-Darstellung, so ordnen wir ihr einen *Charakter* $\chi_V\colon G \to K$ zu. Der Wert $\chi_V(g)$ an der Stelle g ist die Spur von $l_g\colon V \to V$. Die Charaktere eindimensionaler Darstellungen wurden im ersten Abschnitt schon erwähnt. Weil konjugierte Matrizen dieselbe Spur haben, sind die Charaktere isomorpher Darstellungen gleich. Der Charakter ist also eine Invariante des Isomorphietyps. Die Konjugationsinvarianz der Spur liefert ferner für je zwei Gruppenelemente g und h:

$$\chi_V(hgh^{-1}) = \chi_V(g). \tag{3.1}$$

Wir nennen eine Funktion auf G, die auf Konjugationsklassen konstant ist, eine *Klassenfunktion*. Dazu gehören also die Charaktere. Charaktere haben die folgenden weiteren Eigenschaften:

$$\chi_{V\oplus W} = \chi_V + \chi_W, \quad \chi_{V\otimes W} = \chi_V \cdot \chi_W, \quad \chi_{V^*}(g) = \chi(g^{-1}). \tag{3.2}$$

Für die direkte Summe ist das klar. Für die duale Darstellung verwenden wir, daß ein Endomorphismus und sein dualer dieselbe Spur haben. Für das Tensorprodukt zeigt man allgemein $\mathrm{Spur}(f \otimes g) = \mathrm{Spur}(f) \cdot \mathrm{Spur}(g)$ für Endomorphismen f und g. Für die weiteren Anwendungen heben wir hervor:

(3.3) Satz. *Der Charakter von* $\mathrm{Hom}_K(V, W)$ *ist* $g \mapsto \chi_V(g^{-1})\chi_W(g)$.

Beweis. Das folgt aus (3.2) zusammen mit der Identität (1.3). Wir rechnen es aber zusätzlich direkt aus. Wir schreiben alle gebrauchten Daten in Matrizenform auf. Sei $v_1, \ldots, v_m$ eine Basis von V und $w_1, \ldots, w_n$ eine Basis von W. Wir setzen $l_g^{-1}(v_i) = \sum_j a_{ji}v_j$ und $l_g(w_k) = \sum_l b_{lk}w_l$. Eine Basis von $\mathrm{Hom}_K(V, W)$ wird durch $e_{rs}\colon v_i \mapsto \delta_{si}w_r$ gegeben. Damit rechnen wir:

$$\begin{aligned}
(g \cdot e_{rs})(v_i) &= ge_{rs}(g^{-1}v_i) \\
&= ge_{rs}(\sum_j a_{ji}v_j) \\
&= g(\sum_j a_{ji}\delta_{sj}w_r) \\
&= \sum_{j,l} \delta_{sj}a_{ji}b_{lr}w_l \\
&= \sum_l a_{si}b_{lr}w_l
\end{aligned}$$

$$= \sum_l a_{si} b_{lr} e_{li}(v_i).$$

Die Spur ergibt sich als Summe über die Diagonalelemente damit zu $\sum_{r,s} a_{ss} b_{rr} = \chi_V(g^{-1})\chi_W(g)$. □

(3.4) Satz. *Die im zweiten Abschnitt eingeführte Form läßt sich mit Charakteren durch*

$$\langle V, W\rangle = \frac{1}{|G|}\sum_{g\in G} \chi_V(g^{-1})\chi_W(g)$$

ausrechen.

Beweis. Die lineare Abbildung

$$p\colon U \mapsto U, \quad u \mapsto \frac{1}{|G|}\sum_{g\in G} gu$$

ist ein G-äquivarianter Projektor auf die Fixpunktmenge U^G. Die Spur eines Projektionsoperators p ist gleich dem Rang von p. Also ist

$$\textbf{(3.5)} \qquad \dim U^G = \operatorname{Spur} p = \frac{1}{|G|}\sum_{g\in G} \operatorname{Spur}(l_g).$$

Wir wenden diese Relation auf $U = \operatorname{Hom}(V, W)$ an und bedenken $\operatorname{Hom}(V, W)^G = \operatorname{Hom}_G(V, W)$ □

(3.6) Satz. *Zwei Darstellungen von G sind genau dann isomorph, wenn ihre Charaktere gleich sind.*

Beweis. Haben V und V' gleichen Charakter, so sind nach dem letzten Satz für alle W die Werte $\langle W, V\rangle$ und $\langle W, V'\rangle$ gleich. Nach (2.2) sind dann die Multiplizitäten von $W \in \operatorname{Irr}(G, K)$ in V und V' gleich. □

(3.7) Notiz. *Sei $V = KS$ die Permutationsdarstellung der endlichen Menge S. Dann gilt $\chi_V(g) = |S^g|$. Dabei ist S^g die Fixpunktmenge der Linkstranslation l_g.*

Beweis. Wir betrachten die Matrix von l_g bezüglich der Basis S. Ein Basiselement $s \in S$ liefert genau dann einen von Null verschiedenen Eintrag auf der Diagonale, wenn $gs = s$ ist. Dieser Eintrag ist dann 1. □

Das *Zentrum* $Z(A)$ einer Algebra A ist $\{z \in A \mid \forall x \in A, zx = xz\}$.

(3.8) Notiz. *Sei $\alpha\colon G \to K$ gegeben. Das Element $\sum_{g\in G} a(g)g \in KG$ liegt genau dann im Zentrum von KG, wenn α eine Klassenfunktion ist.*

Beweis. Die Gleichheit

$$\sum_u \alpha(uh^{-1})u = \sum_g \alpha(g)gh = \sum_g \alpha(g)hg = \sum_u \alpha(h^{-1}u)u$$

gilt genau dann für alle $h \in G$, wenn für alle $u, h \in G$ die Gleichheit $\alpha(uh^{-1}) = \alpha(h^{-1}u)$ besteht, und letzteres ist äquivalent dazu, daß α eine Klassenfunktion ist. □

(3.9) Folgerung. *Sei $\alpha: G \to K$ gegeben. Die Linearkombination*

$$\alpha^\wedge = \sum_{g \in G} \alpha(g) l_g : V \to V$$

ist genau dann für jede Darstellung V ein Morphismus, wenn α eine Klassenfunktion ist.

Beweis. Ist $\alpha^\wedge$ für die reguläre Darstellung ein Morphismus, so liegt $\sum \alpha(g)g$ im Zentrum von KG. Die Umkehrung folgt unmittelbar aus (3.8). □

(3.10) Notiz. *Sei*

$$KG = \bigoplus_{W \in I} n_W W$$

die Zerlegung der regulären Darstellung. Dann ist $\dim_K W = n_W \langle W, W \rangle$.

Beweis. Für $W \in I$ ist

$$\dim W = \dim \mathrm{Abb}_G(G, W) = \langle KG, W \rangle = \sum_{U \in I} n_U \langle W, U \rangle = n_W \langle W, W \rangle,$$

letzteres wegen (2.7). Wir berechnen die linke Seite mittels (4.3) und (4.6):

$$\langle W, KG \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{\mathrm{reg}}(g) \chi_W(g^{-1}) = \chi_W(1) = \dim W.$$

Damit ist alles gezeigt. □

(3.11) Folgerung. *Sei K algebraisch abgeschlossen. Dann ist die Multiplizität von $W \in I$ in KG gleich* $\dim W$. *Es folgt* $|G| = \sum_{W \in I} (\dim W)^2$. □

Die letzte Gleichung liefert eine Methode, um festzustellen, ob ein System von paarweise verschiedenen irreduziblen Darstellungen vollständig ist.

(3.12) Satz. *Eine endliche Gruppe G ist genau dann abelsch, wenn alle irreduziblen Darstellungen über den komplexen Zahlen eindimensional sind.*

Beweis. Eine eindimensionale komplexe Darstellung wird durch einen Homomorphismus $G \to \mathbb{C}^* = GL(1, \mathbb{C})$ gegeben. Die reguläre Darstellung ist treu. Läßt sie sich in eindimensionale Darstellungen zerlegen, so besitzt G einen injektiven Homomorphismus in eine abelsche Gruppe.

Die umgekehrte Implikation haben wir schon in (1.6) bewiesen. □

(3.13) Beispiel. Wir betrachten komplexe Darstellungen der symmetrischen Gruppe S_3. Es gibt die triviale eindimensionale Darstellung und die Signum-Darstellung. Da S_3 nicht abelsch ist, sind nicht alle Darstellungen eindimensional.

Wegen $6 = 1^2 + 1^2 + 2^2$ bleibt noch eine zweidimensionale zu finden. Sie wird durch Permutation der Koordinaten in $W = \{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid \sum x_i = 0\}$ gegeben. Wir berechnen den Charakter von W. Die Vektoren $e_1 = (1, -1, 0)$ und $e_2 = (0, 1, -1)$ bilden eine Basis von W. Sei in Zyklenschreibweise $t = (12)$ und $c = (123)$. Dann ist $te_1 = -e_1$ und $te_2 = e_1 + e_2$, also $\chi(t) = 0$. Ferner ist $ce_1 = -e_1 - e_2$ und $ce_2 = e_1$, also $\chi(c) = -1$. Die Elemente $1, t, c$ sind Repräsentanten der drei Konjugationsklassen. Es folgt

$$\langle \chi, \chi \rangle = \frac{1}{6}\left(2^2 + 0 + 0 + 0 + (-1)^2 + (-1)^2\right) = 1.$$

Also ist W irreduzibel. Die Irreduzibilität von W wurde auch in (2.12.1) gezeigt.$\diamond$

(3.14) Aufgaben und Ergänzungen.

1. Die symmetrische Gruppe hat eine zu $\mathbb{Z}/2 \times \mathbb{Z}/2$ isomorphen Normalteiler N, der von der Permutation (12)(34) in Zyklenschreibweise erzeugt wird. Die Untergruppe S_3 der Permutationen von $\{1, 2, 3\}$ hat mit N den Schnitt 1. Also ist S_4 das semidirekte Produkt von N und S_3.

4 Komplexe Darstellungen

In diesem Abschnitt sei K ein algebraisch abgeschlossener Körper der Charakteristik Null, vorzugsweise aber $\mathbb{C}$.

Sei $Kl(G)$ der Ring der Klassenfunktionen $G \to K$. Wir definieren auf $Kl(G)$ eine symmetrische Bilinearform durch

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha(g^{-1})\beta(g).$$

Sind V und W Darstellungen, so gilt nach (3.4) $\langle V, W \rangle = \langle \chi_V, \chi_W \rangle$. Die Charaktere irreduzibler Darstellungen sind orthogonal bezüglich dieser Form, also linear unabhängig. Wir werden gleich sehen, daß sie eine Orthonormalbasis von $Kl(G)$ bilden.

(4.1) Satz. *Sei V irreduzibel und $f \in \mathrm{Hom}(V, V)$. Dann ist*

$$\frac{1}{|G|} \sum_{g \in G} g \cdot f = \frac{\mathrm{Sp}(f)}{\dim V} \cdot \mathrm{id}\,.$$

Beweis. Die linke Seite ist als G-Abbildung nach dem Schurschen Lemma gleich dem λ-fachen der Identität. Durch Anwenden der Spur

$$\lambda \dim V = |G|^{-1} \sum \mathrm{Sp}(\mathrm{lg} \circ f \circ l_g^{-1}) = |G|^{-1} \sum \mathrm{Sp}(f) = \mathrm{Sp}(f)$$

berechnen wir λ. $\square$

(4.2) Satz. *Sei $\alpha \in Kl(G)$ und V irreduzibel. Dann ist $p_\alpha = \sum_{g\in G} \alpha(g^{-1})l_g$ auf V die Multiplikation mit $|G|(\dim V)^{-1}\langle\, \alpha, \chi_V \,\rangle$.*

Beweis. Da α eine Klassenfunktion ist, so ist nach (3.9) p_α ein Endomorphismus von V, nach dem Schurschen Lemma also die Multiplikation mit einem Skalar λ. Durch die Rechnung

$$\begin{aligned} \lambda \dim V &= \operatorname{Sp}(\lambda \cdot \mathrm{id}) = \operatorname{Sp}\Big(\sum \alpha(g^{-1})l_g\Big) \\ &= \sum \alpha(g^{-1}) \operatorname{Sp}(l_g) = \sum \alpha(g^{-1})\chi_V(g) \\ &= |G|\langle\, \alpha, \chi_V \,\rangle. \end{aligned}$$

wird λ bestimmt. □

(4.3) Satz. *Sei $\alpha \in Kl(G)$ orthogonal zu allen Charakteren irreduzibler Darstellungen. Dann ist $\alpha = 0$.*

Beweis. Wenden wir die Voraussetzung über α in (4.2) an, so sehen wir, daß p_α in allen irreduziblen Darstellungen als Nullabbildung wirkt, also überhaupt in allen. In der regulären Darstellung gilt dann $0 = p_\alpha(e) = \sum \alpha(g^{-1})g$. Da die $g \in G$ eine Basis von KG bilden, folgt $\alpha(g) = 0$ für alle $g \in G$. □

(4.4) Satz. *Die irreduziblen Charaktere von G bilden eine Orthonormalbasis von $Kl(G)$. Die Anzahl der irreduziblen Darstellungen ist gleich der Anzahl der Konjugationsklassen von G.*

Beweis. Sei $U \subset Kl(G)$ ein Unterraum. Ist $U \neq Kl(G)$, so ist das orthogonale Komplement $U^\perp$ bezüglich der Form $\langle\, -, - \,\rangle$ von Null verschieden. Ist U der von den Charakteren erzeugte Unterraum, so sagt (4.3), daß $U^\perp = 0$ ist. Also erzeugen die Charaktere $Kl(G)$. Es is klar, daß die Dimension von $Kl(G)$ gleich der Anzahl der Konjugationsklassen ist. □

Sei W irreduzibel. Wir bilden dazu

$$\textbf{(4.5)} \qquad e_W = \frac{\dim W}{|G|} \sum_{g\in G} \chi_W(g^{-1})g \in KG.$$

(4.6) Satz. *Die Multiplikation mit e_W ist in jeder Darstellung die Projektion auf den W-isotypischen Bestandteil. Es gilt $e_W^2 = e_W$. Sind V und W nicht isomorph, so ist $e_V e_W = 0$.*

Beweis. Nach (4.2) wirkt e_W auf einer zu W isomorphen Darstellung V als Identität und auf einer anderen irreduziblen Darstellung als Null. Daraus folgt die erste Behauptung. Außerdem folgt, daß e_W^2 und e_W in jeder Darstellung gleich wirken. Anwendung auf die reguläre Darstellung zeigt $e_W^2 = e_W$. Da $e_V e_W$ in jeder Darstellung als Null wirkt, gilt ebenso $e_V e_W = 0$. □

Ein Element e einer Algebra heißt *idempotent*, wenn $e^2 = e$ ist. Idempotente e, f heißen *orthogonal*, wenn $ef = fe = 0$ ist. Sie heißen *zentral*, wenn sie im Zentrum liegen. Nach dieser Terminologie bilden die $(e_W \mid W \in \operatorname{Irr}(G, K))$ ein

System von zentralen, paarweise orthogonalen Idempotenten von KG. Außerdem gilt offenbar

$$1 = \sum_{W \in I} e_W,$$

da die Summe in jeder Darstellung als Identität wirkt.

(4.7) Orthogonalitätsrelation. Seien V und W irreduzibel. Dann gilt

$$\frac{1}{|G|} \sum_{g \in G} \chi_V(g^{-1}) \chi_W(xg) = \langle V, W \rangle \frac{\chi_V(x)}{\dim V}.$$

Beweis. Die Gleichung $e_V e_W = \langle V, W \rangle e_V$ nach (4.6) lautet ausgeschrieben

$$\frac{\dim V \dim W}{|G|^2} \sum_{g,h} \chi_V(g^{-1}) \chi_W(h^{-1}) gh = \langle V, W \rangle \frac{\dim V}{|G|} \sum_x \chi_V(x^{-1}) x.$$

Indem man auf beiden Seiten den Koeffizienten von x^{-1} vergleicht, ergibt sich die Behauptung. □

Für komplexe Klassenfunktionen definieren wir eine hermitesche Form auf $Kl(G)$ durch

$$(\alpha, \beta) = \frac{1}{|G|} \sum_{g \in G} \overline{\alpha(g)} \beta(g).$$

Wegen der Relation $\chi_V(g^{-1}) = \overline{\chi_V(g)}$ gilt für Charaktere $(\chi_V, \chi_W) = \langle V, W \rangle$. Die irreduziblen Charaktere bilden also auch eine Orthonormalbasis von $Kl(G)$ bezüglich dieser Form.

Sei $C \subset G$ ein Repräsentantensystem der Konjugationsklassen. Wegen $|C| = |I|$ nach (4.4) ist $X\colon C \times I \to K,\ (c, V) \mapsto \chi_C(c)$ eine quadratische Matrix. Sie heißt *Charaktertafel* von G. Wir schreiben die Orthogonalitätsrelation als eine Aussage über diese Matrix um. Dazu sei $X^*\colon I \times C \to \mathbb{C},\ (V, c) \mapsto \overline{\chi_V(c)}$ die transponiert-konjugierte Matrix und $D\colon C \times C \to \mathbb{C}$ die Diagonalmatrix $(c, d) \mapsto \delta_{c,d}|c|$, worin $|c|$ die Mächtigkeit der Konjugationsklasse von c bezeichnet.

Die Orthogonalitätsrelation $(\chi_V, \chi_W) = \delta_{V,W}$ kann dann als

$$\sum_{c \in C} |c| \overline{\chi_V(c)} \chi_W(c) = |G| \delta_{V,W}$$

geschrieben werden, oder in Matrizenform $X^* D X = |G| E$ (mit der Einheitsmatrix E). Es folgt

$$X X^* D = X X^* D X X^{-1} = X(|G|E) X^{-1} = |G| E$$

und damit $X X^* = |G| D^{-1}$. Sei $Z(c) = \{g \in G \mid gcg^{-1} = c\}$ der Zentralisator von c in G. Dann ist $|c| = |G : Z(c)|$. Die letzte Matrizengleichung besagt damit:

(4.8) Zweite Orthogonalitätsrelation. *Für je zwei Konjugationsklassen c, d gilt* $\sum_{V \in I} \overline{\chi_V(c)} \chi_V(d) = \delta_{c,d} |Z(c)|$. □

5 Darstellungen von Produkten

Sei V eine Darstellung von G und W eine von H über K. Auf dem Tensorprodukt $V \otimes W$ erhalten wir eine Darstellung von $G \times H$ durch

$$(g,h) \cdot (v \otimes w) = gv \otimes hw.$$

Hat K die Charakteristik Null, so gilt für diese, wieder $V \otimes W$ bezeichnete, Darstellung von $G \times H$

$$\chi_{V\otimes W}(g,h) = \chi_V(g)\chi_W(h).$$

Den Vektorraum $\mathrm{Hom}(V,W)$ machen wir zu einer $G \times H$-Darstellung durch

$$((g,h) \cdot \varphi)(v) = h\varphi(g^{-1}v).$$

Damit wird der kanonische Isomorphismus $V^* \otimes W \to \mathrm{Hom}(V,W)$ ein Isomorphismus von $G \times H$-Darstellungen.

Sind V_1, V_2 G-Darstellungen und W_1, W_2 H-Darstellungen, so ist der kanonische Isomorphismus

$$\textbf{(5.1)} \qquad \mathrm{Hom}(V_1,V_2) \otimes \mathrm{Hom}(W_1,W_2) \to \mathrm{Hom}(V_1 \otimes W_1, V_1 \otimes W_2)$$

ebenfalls einer von $G \times H$-Darstellungen; denn diese Abbildung ist tautologisch als $\alpha \otimes \beta \mapsto \alpha \otimes \beta$ definiert; die $G \times H$-Operation links ist durch $(g,h)(\alpha \otimes \beta) = l_g \alpha l_{g^{-1}} \otimes l_h \beta l_{h^{-1}}$ definiert und rechts durch $(g,h)(\alpha \otimes \beta) = l_{(g,h)}(\alpha \otimes \beta) l_{(g,h)^{-1}}$, was aber eben dasselbe ist.

(5.2) Notiz. *Seien $|G|$ und $|H|$ in K invertierbar. Dann gilt*

$$\langle\, V_1 \otimes W_1,\, V_2 \otimes W_2 \,\rangle_{G\times H} = \langle\, V_1, v_2 \,\rangle_G \langle\, W_1, W_2 \,\rangle_H.$$

(wir haben die verwendete Gruppe als Index geschrieben.)

Beweis. Die linke Seite ist der Rang von

$$\frac{1}{|G \times H|} \sum_{(g,h)\in G\times H} l_{(g,h)}$$

in $\mathrm{Hom}(V_1 \otimes W_1, V_2 \otimes W_2)$. Vermöge des Isomorphismus (5.1) entspricht diesem Operator aber

$$\frac{1}{|G|}\sum_{g\in G} l_g \otimes \frac{1}{|H|}\sum_{h\in H} l_h,$$

und dieser hat die rechte Seite der behaupteten Gleichheit als Rang. □

(5.3) Satz. *Sei K algebraisch abgeschlossen. Dann ist*

$$\mathrm{Irr}(G,K) \times \mathrm{Irr}(H,K) \to \mathrm{Irr}(G \times H, K), \quad (V,W) \mapsto V \otimes W$$

definiert und bijektiv.

BEWEIS. Sind V und W irreduzibel, so ist nach (5.2) $\langle V \otimes W, V \otimes W \rangle = \langle V, V \rangle \langle W, W \rangle = 1$, damit $V \otimes W$ irreduzibel und die genannte Abbildung definiert. Wegen der Orthogonalität der Charaktere ist sie auch injektiv. Die Anzahlformel (3.11) zeigt, daß es nicht mehr irreduzible Darstellungen von $G \times H$ geben kann, als diese Konstruktion liefert. □

6 Die Struktur der Gruppenalgebra

Sei $C(G, K)$ der Vektorraum aller Abbildungen $G \to K$. Er wird zu einer linken G-Darstellung durch $(g \cdot \alpha)(x) = \alpha(x, g)$ und zu einer rechten G-Darstellung durch $(\alpha \cdot h)(x) = \alpha(hx)$. Diese beiden Operationen von G sind miteinander vertauschbar: $(g \cdot \alpha) \cdot h = g \cdot (\alpha \cdot h)$.

Allgemein sei eine (G, H)-Darstellung V ein H-Vektorraum V mit einer linken G-Darstellung und einer rechten H-Darstellung, so daß für $g \in G$, $v \in V$ und $h \in H$ immer $g \cdot (v \cdot h) = (g \cdot v) \cdot h$ gilt. Aus einer (G, H)-Darstellung V erhalten wir eine linke $G \times H$-Darstellung auf V durch $(g, h) \cdot v = gvh^{-1}$. Auf diese Weise entsprechen die (G, H)-Darstellungen den $G \times H$-Darstellungen.

Sei V eine linke G-Darstellung. Wir machen den Dualraum V^* durch $(\varphi \cdot g)(v) = \varphi(gv)$ zu einer rechten G-Darstellung.

Einem Paar $(\varphi, v) \in V^* \times V$ ordnen wir die Funktion $d_{\varphi,v} \colon g \mapsto \varphi(gv)$ in $C(G, K)$ zu. Die Zuordnung $\varphi, v \mapsto d_{\varphi,v}$ ist linear in φ und v und induziert deshalb eine lineare Abbildung

$$s_V \colon V^* \otimes V \to C(G, K), \varphi \otimes v \mapsto d_{\varphi,v}.$$

Wir machen $V^* \otimes V$ zu einer (G, G)-Darstellung, indem g von links durch $1 \otimes l_g$ und von rechts durch $l_g \otimes 1$ operiert. Aus den Definitionen verifiziert man:

(6.1) Notiz. *Die Abbildung s_V ist ein Homomorphismus von (G, G)-Darstellungen.* □

Wir definieren eine lineare Abbildung $t_V \colon \mathrm{Hom}(V, V) \to C(G, K)$ durch $t_V\alpha \colon g \mapsto Sp(l_g \circ \alpha) = Sp(\alpha \circ l_g)$. Wir machen $\mathrm{Hom}(V, V)$ zu einer (G, G)-Darstellung durch $(g \cdot \alpha \cdot h)(v) = g\alpha(hv)$. Es ist

$$t_V(g \cdot \alpha \cdot h)(x) = Sp(l_g \alpha l_h l_x) = Sp(l_h l_x l_g \alpha)$$

und

$$(g \cdot t_V\alpha \cdot h)(x) = t_V\alpha(hxg) = Sp(l_{hxg}\alpha).$$

Also gilt:

(6.2) Notiz. *t_V ist ein Homomorphismus von (G, G)-Darstellungen.* □

Wir haben einen linearen Isomorphismus $\delta \colon KG \to C(G, K)$, $\sum \alpha(g)g \mapsto \alpha$. Wir übertragen damit die Multiplikation von KG. Das Produkt in $C(G, K)$ bezeichnen wir mit $(\alpha, \beta) \mapsto \alpha * \beta$ und nennen es *Faltung*. Wegen

$$\left(\sum_g \alpha(g)g\right)\left(\sum_h \beta(h)h\right) == \sum_u \left(\sum_g \alpha(g)\beta(g^{-1}u)\right) u = \sum_u \left(\sum_h \alpha(uh^{-1})\beta(h)\right) u$$

ist die Faltung durch

$$(\alpha * \beta)(u) = \sum_g \alpha(g)\beta(g^{-1}u) = \sum_h \alpha(uh^{-1})\beta(h) \tag{6.3}$$

definiert. Wir betrachten $C(G,K)$ mit dem Faltungsprodukt als ein Modell für die reguläre Darstellung.

(6.4) Satz. *Sei K algebraisch abgeschlossen und habe die Charakteristik Null. Sei V irreduzibel. Dann ist*

$$\tau_V = \frac{\dim V}{|G|} t_V \colon \mathrm{Hom}(V,V) \to C(G,K)$$

ein Antihomomorphismus von Algebren.

Beweis. Wir benutzen, daß für jedes $\beta \in \mathrm{Hom}(V,V)$ die Gleichung

$$\frac{|V|}{|G|} \sum_{g\in G} l_g \beta l_{g^{-1}} = \mathrm{Sp}(\beta)\,\mathrm{id}_V \tag{$*$}$$

gilt (4.1). Damit rechnen wir

$$\frac{|V|^2}{|G|^2} \sum_{g,u\in G} l_g \beta l_u l_{g^{-1}} l_{u^{-1}} \alpha$$

auf zweierlei Weise aus. Indem wir $(*)$ auf $\sum_u l_u l_{g^{-1}} l_{u^{-1}}$ anwenden und (4.6) einsetzen, erhalten wir

$$\frac{|V|}{|G|} \sum_g \chi_V(g^{-1}) l_g \beta\alpha = \beta\alpha.$$

Indem wir $(*)$ auf $\sum_g l_g \beta l_u l_{g^{-1}}$ anwenden, erhalten wir

$$\frac{|V|}{|G|} \sum_u \mathrm{Sp}(\beta l_u) l_{u^{-1}} \alpha.$$

Auf die damit gewonnene Gleichheit wenden wir die Spur an und erhalten

$$\mathrm{Sp}(\beta\alpha) = \frac{|V|}{|G|} \sum_u \mathrm{Sp}(l_u\beta)\,\mathrm{Sp}(l_{u^{-1}}\alpha).$$

Wir ersetzen β durch $l_g\beta$ und erkennen in

$$t_V(\beta\alpha) = \frac{|V|}{|G|} t_V\alpha * t_V\beta$$

die Behauptung. □

(6.5) Satz. *Das Bild von τ_V ist der V-isotypische Bestandteil von $C(G,K)$ bezüglich der linken G-Operation und der V^*-isotypische Bestandteil bezüglich der rechten G-Operation. Als (G,G)-Darstellung ist* $\mathrm{Hom}(V,V)$ *irreduzibel und das Bild von τ_V der* $\mathrm{Hom}(V,V)$*-isotypische Bestandteil der (G,G)-Darstellung.*

Beweis. Die kanonische Abbildung $V^* \otimes V \to \mathrm{Hom}(V,V)$ ist ein Isomorphismus von (G,G)-Darstellungen. Nach (5.3) ist deshalb $\mathrm{Hom}(V,V)$ als (G,G)-Darstellung irreduzibel. Da $\tau_V \neq 0$ ist, ist τ_V injektiv. Das Bild von τ_V liegt sicherlich im V-isotypischen Teil. Wir wissen schon, daß dieser die Dimension $|V|^2$ hat. Also ist τ_V ein Isomorphismus wie angegeben. □

(6.6) Bemerkung. Das Bild des Einselementes, also der Identität von V, bei τ_V ist die Funktion $g \mapsto \mathrm{Sp}(l_g) = \chi_V(g)$. Bei dem Isomorphismus $KG \cong C(G,K)$ entspricht das dem Idempotenten e_{V^*}. Wenn wir statt τ_V mit Homomorphismen arbeiten wollen, können wir den Antihomomorphismus $\mathrm{Hom}(V^*,V^*) \to \mathrm{Hom}(V,V)$, $\beta^* \mapsto \beta$ davorschalten. Dann wird die Identität auf das entsprechende Idempotente abgebildet. ◇

Als Algebra ist $\mathrm{Hom}(V,V)$ isomorph zur Matrixalgebra der $(|V|,|V|)$-Matrizen über K. Wir haben damit die reguläre Darstellung in das Produkt solcher Matrixalgebren zerlegt. Genauer

$$\bigoplus_{V \in \mathrm{Irr}(G,K)} \mathrm{Hom}(V,V) \to C(G,K), \quad (x_V) \mapsto \sum_{V \in I} \tau_V(x_V)$$

ist ein Antiisomorphismus von Algebren. In dieser Aussage steckt noch die Orthogonalität $\tau_V(x)\tau_W(y) = 0$ für $V \ncong W$. Das ist aber eine Folge aus $e_V e_W = 0$.

7 Darstellungsringe

Sei $R^+(G,k)$ die Menge der Isomorphieklassen von endlichdimensionalen Darstellungen von G über k. Durch direkte Summe von Darstellungen wird daraus ein abelsches Monoid mit universeller Gruppe $R(G,k)$.

(7.1) Satz. *Sei $|G|$ in k invertierbar. Dann ist $R(G,k)$ die freie abelsche Gruppe über den Isomorphieklassen irreduzibler Darstellungen.*

Beweis. Sei $R(G,k)$ die besagte freie abelsche Gruppe. Wir erhalten einen Homomorphismus $i\colon R^+(G,k) \to R(G,k)$ durch $i(V) = \sum_{A \in I} n_A A$, worin n_A die Multiplizität von $A \in \mathrm{Irr}(G,k)$ in V ist. Für diesen Homorphismus wird die universelle Eigenschaft direkt mit der universellen Eigenschaft einer Basis verifiziert. □

Das Tensorprodukt von Darstellungen liefert auf $R^+(G,k)$ eine weitere assoziative und kommutative Verknüpfung mit der trivialen eindimensionalen Darstellung als Einselement. Die Verträglichkeit (1.4) des Tensorprodukts mit direkten Summen besagt, daß daß diese Multiplikation $\otimes$ bezüglich der Addition biadditiv ist. Damit wird $R^+(G,k)$ ein Halbring, und der zugehörige Grothendieck-Ring heiße *Darstellungsring* von G über k.

Habe k die Charakteristik Null. Die Zuordnung $V \mapsto \chi_V$, die jeder Darstellung ihren Charakter zuordnet, ist wegen (3.2) ein Homomorphismus $\chi^+ \colon R^+(G,k) \to Kl(G,k)$ in den Ring der Klassenfunktionen. Wir erhalten einen induzierten Homomorphismus $\chi \colon R(G,k) \to Kl(G,k)$. Da die Charaktere irreduzibler Darstellungen linear unabhängig sind, ist χ injektiv. Das Bild heißt der *Charakterring* von G.

(7.2) Aufgaben und Ergänzungen.

1. Für eine endliche abelsche Gruppe G ist $R(G,\mathbb{C})$ isomorph zum Gruppenring $\mathbb{Z}G^*$ der Charaktergruppe G^* über den ganzen Zahlen. (Letztere ist isomorph zu G.)

8 Burnside-Ringe

Sei $A^+(G)$ die Menge der Isomorphieklassen endlicher G-Mengen. Durch disjunkte Summe (Addition) und cartesisches Produkt (Multiplikation) wird $A^+(G)$ zu einem kommutativen Halbring. Der Grothendieck-Ring dazu heiße *Burnside-Ring* von G und werde mit $A(G)$ bezeichnet. Sei $[S]$ das Bild der G-Menge S in $A(G)$.

Ist $H < G$ eine Untergruppe, so gelten für die Anzahlen der H-Fixpunkte offenbar die Regeln

$$|(S \amalg T)^H| = |S^H| + |T^H|, \qquad |(S \times T)^H| = |S^H||T^H|.$$

Die Zuordnung $S \mapsto |S^H|$ ist deshalb ein Homomorphismus $A^+(G) \to \mathbb{Z}$ von Halbringen und liefert nach der universellen Eigenschaft des Grothendieck-Ringes einen Homomorphismus von Ringen

$$\varphi_H \colon A(G) \to \mathbb{Z}, \tag{8.1}$$

der *H-Marke* von $A(G)$ heiße. Seien H und K in G konjugiert, d. h. es gebe $g \in G$ mit $gHg^{-1} = K$. Für jede G-Menge S induziert dann die Linkstranslation l_g eine Bijektion $l_g \colon S^H \to S^K$. Deshalb hängt die H-Marke nur von der Konjugationsklasse (H) von H ab. Wir nennen H *subkonjugiert* zu K, wenn H zu einer Untergruppe von K konjugiert ist. Wir erinnern daran, daß G/H und G/K genau dann isomorph sind, wenn H und K konjugiert sind. Aus $G/H^L \neq \emptyset$ folgt, daß L zu H subkonjugiert ist. Die G-Automorphismenmenge von G/H ist isomorph zur Gruppe $NH/H = WH$; darin ist $NH = \{g \in G \mid gHg^{-1} = H\}$ der *Normalisator* von H in G. Der Quotient WH wird auch *Weyl-Gruppe* von H in G genannt — wegen dieser Bezeichnung für den Fall, daß H der maximale Torus einer kompakten Lieschen Gruppe G ist.[3]

Sei $\Phi(G)$ die Menge der Konjugationsklassen von Untergruppen von G und $C(G)$ der Ring aller Abbildungen $\Phi(G) \to \mathbb{Z}$. Subkonjugation induziert eine teilweise Ordnung auf $\Phi(G)$. Wir sammeln die H-Marken zu einem Homomorphismus von Ringen

[3] Siehe Th. Bröcker, T. tom Dieck: Representations of compact Lie groups. Springer-Verlag.

(8.2) $$\varphi\colon A(G) \to C(G),$$

der $x \in A(G)$ auf die Funktion $(H) \mapsto \varphi_H(x)$ abbildet.

(8.3) Satz. *Additiv ist $A(G)$ die freie abelsche Gruppe über den Isomorphieklassen von homogenen Mengen G/H. Der Homomorphismus φ ist injektiv.*

Beweis. Da eine G-Menge disjunkte Summe von Bahnen ist und eine Bahn isomorph zu einer homogenen Menge der Form G/H, erzeugen die $[G/H]$ die Gruppe $A(G)$. Sei $\sum_{(H)} a_H[G/H] = 0$ eine echte lineare Relation mit ganzzahligen Koeffizienten a_H. Unter den (H) mit $a_h \neq 0$ sei L maximal bezüglich Subkonjugation. Aus $G/H^L \neq \emptyset$ folgt, daß L zu H subkonjugiert ist. Also gilt

$$0 = \varphi(\sum_{(H)} a_H[G/H]) = a_L|G/L^L| = a_L|WL| \neq 0.$$

Widerspruch. Das zeigt die lineare Unabhängigkeit der $[G/H]$. In derselben Weise folgt auch die Injektivität von φ. □

Für Permutationsdarstellungen gelten die Regeln

$$k(S \amalg T) \cong k(S) \oplus k(T), \quad k(S \times T) \cong k(S) \otimes k(T).$$

Die Zuordnung $S \mapsto \mathbb{Q}(S)$ induziert deshalb einen Ringhomomorphismus

(8.4) $$\pi_G\colon A(G) \to R(G, \mathbb{Q}).$$

Er ist im allgemeinen weder injektiv noch surjektiv.

Um die Multiplikation in $A(G)$ zu bestimmen, muß man die Produkte der Form $[G/H][G/K]$ kennen. Die G-Bahnen der Menge $G/H \times G/K$ entsprechen den Doppelnebenklassen HgK, siehe (??). Damit erhält man:

(8.5) Notiz. *Die Multiplikation in $A(G)$ ist durch*

$$[G/H] \times [G/K] = \sum_{HgK \in H\backslash G/K} [G/H \cap gHg^{-1}]$$

gegeben. □

Ist speziell G abelsch, so ist $[G/H][G/K] = c[G/H \cap K]$, wobei sich c aus einer Anzahlbestimmung ergibt. Dieselbe Formel ergibt sich, wenn K Normalteiler von G ist.

Die Abbildung (8.2) ist ein injektiver Homomorphismus zwischen freien abelschen Gruppen von gleichem Rang. Der Kokern ist also eine endliche abelsche Gruppe. Im nächsten Satz bestimmen wir angepaßte Basen für diese Inklusion.

(8.6) Satz. *Für jede Konjugationsklasse (H) gibt es ein Element $x_{(H)} \in C(G)$, das der Gleichung $\varphi(G/H) = |WH|x_{(H)}$ genügt. Die Menge $\{x_{(H)} \mid (H) \in \Phi(G)\}$ ist eine $\mathbb{Z}$-Basis von $C(G)$.*

BEWEIS. Die Automorphismengruppe WH von G/H operiert frei auf G/H durch $(gH, nH) \mapsto gnH$. Deshalb operiert WH frei auf allen Fixpunktmengen G/H^K. Mit anderen Worten: Die Funktionswerte von $\varphi(G/H)$ sind alle durch $|WH|$ teilbar. Das liefert $x_{(H)}$. Der Wert von $x_{(H)}$ an der Stelle (H) ist 1. Für alle (K) mit $(K) \not\leq (H)$ ist der Wert Null. Also ist die Wertetabelle $(H), (K) \mapsto x_{(H)}(K)$ eine Dreiecksmatrix (bezüglich der Partialordnung „subkonjugiert“) mit Einsen auf der Diagonale. Daraus folgt, daß die $x_{(H)}$ eine Basis bilden. □

(8.7) Folgerung. *Der Kokern von φ ist isomorph zu*

$$\prod_{(H)\in\Phi(G)} \mathbb{Z}/|WH|.$$

10 Galois-Theorie

1 Die Galois-Korrespondenz

In der Galois-Theorie werden Körpererweiterungen mit Hilfe ihrer Symmetriegruppen untersucht. Es gibt zwei Standpunkte: Entweder geht man von Körpererweiterungen oder von Symmetriegruppen aus. In diesem Abschnitt formulieren wir die Struktursätze der Galois-Theorie.

Eine *Galois-Symmetrie* (K, G) besteht aus einem Körper K zusammen mit einer endlichen Gruppe $G \subset \mathrm{Aut}(K)$ von Automorphismen von K.

Eine Erweiterung $K|k$ heißt *Galois-Erweiterung*, wenn sie endlich ist und die Gruppe $G = G(K|k)$ der k-Automorphismen von K die Ordnung $[K : k]$ hat. Die Gruppe G heißt dann die *Galois-Gruppe* von $K|k$. Die beiden Standpunkte sind äquivalent, wie im dritten Abschnitt gezeigt wird:

(1.1) Satz. *Folgende Aussagen über eine Erweiterung $K|k$ sind äquivalent:*
(1) *$K|k$ ist eine Galois-Erweiterung.*
(2) *Es gibt eine Galois-Symmetrie (K, G) mit der Fixpunktmenge $k = K^G$.*
Gelten diese Aussagen, so ist G die Galois-Gruppe von $K|k$.

Sei eine Galois-Symmetrie gegeben. Wir haben dann eine effektive Operation von G auf K durch $G \times K \to K$, $(\sigma, x) \mapsto \sigma(x)$. Jede Untergruppe $H < G$ hat einen Unterkörper K^H von K als Fixpunktmenge. Zu jedem $F \subset K$ gibt es die Standgruppe $G_F = \{\sigma \in G \mid \forall x \in F, \sigma(x) = x\}$. Wir betrachten $k = K^G$ als *Grundkörper* der Galois-Symmetrie. Mit $\mathrm{Un}(G)$ bezeichnen wir die Menge der Untergruppen von G und mit $\mathrm{Zw}(K)$ die Menge der Zwischenkörper von $K|k$.

Die Hauptresultate der Galois-Theorie sind die beiden folgenden *Korrespondenzsätze*. Sie werden im dritten Abschnitt bewiesen.

(1.2) Satz. *Sei (K, G) eine Galois-Symmetrie. Die Zuordnungen $\Phi\colon U \mapsto K^U$ und $\Sigma\colon F \mapsto G_F$ sind zueinander inverse Bijektionen $\Phi\colon \mathrm{Un}(G) \to \mathrm{Zw}(K)$ und $\Sigma\colon \mathrm{Zw}(K) \to \mathrm{Un}(G)$. Ferner gelten für $U \in \mathrm{Un}(G)$ und $F \in \mathrm{Zw}(K)$ die folgenden Anzahlrelationen*

$$[K : K^U] = |U|,\ [K^U : k] = |G/U|,\ [K : F] = |G_F|,\ [K : k] = |G/G_F|.$$

Ein zweiter Korrespondenzsatz betrifft Morphismen. Für $L, M \in \mathrm{Zw}(K)$ bezeichen wir mit $\mathrm{Mor}_k(L, M)$ die Menge der Homomorphismen $L \to M$ von k-Algebren (k-Morphismen). Für $A, B \in \mathrm{Un}(G)$ bezeichen wir mit $\mathrm{Abb}_G(G/B, G/A)$ die Menge der G-Abbildungen $G/B \to G/A$. Die Auswertung $\mathrm{Abb}_G(G/B, G/A) \to G/A^B$, $\alpha \mapsto \alpha(eB)$ ist bijektiv. Genau dann liegt σA in G/A^B, wenn $\sigma^{-1}B\sigma \subset A$ ist.

(1.3) Satz. *Wir fixieren Paare $L, M \in \mathrm{Zw}(K)$ und $A, B \in \mathrm{Un}(G)$ mit $L = K^A$ und $M = K^B$, die sich nach (1.2) eindeutig entsprechen.*

(1) *Genau dann bildet $\sigma \in G$ den Körper L in den Körper K ab, wenn $\sigma A \in G/A^B$ ist. Aus $\sigma A = \tau A$ folgt $\sigma|L = \tau|L$. Die Zuordnung*

$$\Phi\colon \mathrm{Abb}_G(G/B, G/A) \cong G/A^B \to \mathrm{Mor}_k(K^A, K^B), \quad \sigma \mapsto \sigma|A$$

ist bijektiv.

(2) *Zu jedem $\varphi \in \mathrm{Mor}_k(L, M)$ gibt es ein $\sigma_\varphi \in G$ mit $\sigma_\varphi|L = \varphi$. Aus $\sigma|L = \tau|L$ folgt $\sigma A = \tau A$. Die Zuordnung*

$$\mathrm{Mor}_k(L, M) \to G/A^B \cong \mathrm{Abb}_G(G/B, G/A), \quad \varphi \mapsto \sigma_\varphi A$$

ist bijektiv und invers zu Φ.

Wir formulieren nun (1.2) und (1.3) als eine Isomorphie von Kategorien um. Die Zwischenkörper zusammen mit den k-Morphismen bilden nämlich eine Kategorie $\mathrm{Zw}(K)$. Die Untergruppen von G zusammen mit $\mathrm{Abb}_G(G/B, G/A)$ als Morphismenmenge von B nach A bilden eine Kategorie $\mathrm{Un}(G)$. Verwendet man nicht die Objekte A sondern G/A, so erhält man die Orbitkategorie $\mathrm{Or}(G)$, die vom Standpunkt der Kategorientheorie natürlicher als $\mathrm{Un}(G)$ ist.

Wir definieren kontravariante Funktoren $\Phi\colon \mathrm{Un}(G) \to \mathrm{Zw}(K)$ und $\Sigma\colon \mathrm{Zw}(K) \to \mathrm{Un}(G)$. Auf den Objekten wurden die Funktoren in (1.2) definiert, auf den Morphismen in (1.3). Um die Funktoreigenschaften besser zu erkennen, zeigen wir, daß beide Funktoren im wesentlichen Hom-Funktoren sind.

Sei $\alpha \in \mathrm{Abb}_G(G/B, G/A)$. Damit definieren wir $\Phi(\alpha) \in \mathrm{Mor}_k(K^A, K^B)$ durch das folgenden kommutative Diagramm.

$$\begin{array}{ccc} \mathrm{Abb}_G(G/B, K) & \xrightarrow{\alpha^*} & \mathrm{Abb}_G(G/A, K) \\ \downarrow \cong & & \downarrow \cong \\ K^B & \xrightarrow{\Phi(\alpha)} & K^A \end{array}$$

Darin ist α^* die Zusammensetzung $f \mapsto f \circ \alpha$ (Hom-Funktor). Die senkrechten Isomorphismen sind durch die Auswertung am neutralen Element gegeben.

Für jedes $F \in \mathrm{Zw}(K)$ trägt $\mathrm{Mor}_k(F, K)$ eine G-Operation $(\sigma, \beta) \mapsto \sigma \circ \beta$. Indem wir $\sigma \in G \subset \mathrm{Mor}_k(K, K)$ auf F einschränken, erhalten wir eine Abbildung $G \to \mathrm{Mor}_k(F, G)$, die nach Konstruktion eine injektive G-Abbildung

$$\mathbf{(1.4)} \qquad i_F\colon G/G_F \to \mathrm{Mor}_k(F, K)$$

liefert. Nach (1.3) ist diese Abbildung auch surjektiv.

Sei $\beta \in \mathrm{Mor}_k(L, M)$ gegeben. Wir definieren $\Sigma(\beta) \in \mathrm{Abb}_G(G/G_M, G/G_L)$ durch die Kommutativität des folgenden Diagrammes.

$$\begin{array}{ccc} \mathrm{Mor}_k(M, K) & \xrightarrow{\beta^*} & \mathrm{Mor}_k(L, K) \\ \uparrow i_M & & \uparrow i_L \\ G/G_M & \xrightarrow{\Sigma(\beta} & G/G_L \end{array}$$

Darin ist β^* die Zusammensetzung $f \mapsto f \circ \beta$ (Hom-Funktor). Nach Konstruktion ist $\Sigma(\beta)$ eine G-Abbildung. Der folgende Satz ist nur noch eine Zusammenfassung von (1.2) und (1.3). Davon möge man sich überzeugen.

(1.5) Satz. *Die Funktoren* $\Phi\colon \mathrm{Un}(G) \to \mathrm{Zw}(K)$ *und* $\Sigma\colon \mathrm{Zw}(K) \to \mathrm{Un}(G)$ *sind zueinander inverse kontravariante Isomorphismen von Kategorien.* □

(1.6) Satz. *Sei* (K, G) *ein Galois-Symmetrie. Die* G*-Operation macht* K *zu einer* G*-Darstellung über* k*. Diese Darstellung ist isomorph zur regulären Darstellung.*

Nach diesem Satz gibt es insbesondere ein Element $a \in K$, so daß $\{\sigma(a) \mid \sigma \in G\}$ eine k-Basis von K ist. Eine Basis dieser Form nennt man *Normalbasis* der Erweiterung $K|k$. Deshalb heißt der letzte Satz auch Satz von der Normalbasis.

2 Verschränkte Darstellungen

Wir legen eine Galois-Symmetrie (K, G) mit Grundkörper $k = K^G$ zugrunde. Eine *verschränkte* (K, G)*-Darstellung* besteht aus einem K-Vektorraum W und einer Operation von G auf W mit den folgenden Eigenschaften

(1) Die Linkstranslation $l_\sigma\colon W \to W$, $w \mapsto \sigma(w)$ mit $\sigma \in G$ ist k-linear.
(2) Für $\lambda \in K$, $\sigma \in G$ und $w \in W$ gilt $\sigma(\lambda w) = \sigma(\lambda)\sigma(w)$.

Ist W eine verschränkte (K, G)-Darstellung, so ist W insbesondere eine G-Darstellung über k und $V = W^G$ ein k-Unterraum. Das Standardbeispiel einer verschränkten (K, G)-Darstellung ist $W = K$ mit der durch $G \subset \mathrm{Aut}(K)$ vorgegebenen Operation. Der nächste Hauptsatz über verschränkte Darstellungen besagt, daß es nur direkte Summen des Standardbeispiels gibt.

(2.1) Satz. *Sei* W *eine verschränkte* (K, G)*-Darstellung. Dann ist eine* k*-Basis von* V *eine* K*-Basis von* W*.*

Im Beweis dieses Satze brauchen wir das nächste sogenannte *Dedekindsche Lemma* über die lineare Unabhängigkeit von Algebrenhomomorphismen. Ist A eine k-Algebra, so bezeichnen wir mit $\mathrm{Alg}_k(A, K)$ die Menge der Homomorphismen $A \to K$ von k-Algebren.

(2.2) Satz. *Die Menge* $\mathrm{Alg}_k(A, k) \setminus \{0\}$ *ist im* K*-Vektorraum* $\mathrm{Hom}_k(A, K)$ *linear unabhängig.*

Beweis. Seien $\varphi_1, \ldots, \varphi_n \in \mathrm{Alg}_k(A, K)$ paarweise verschiedene Elemente (von Null verschieden). Seien je $n-1$ davon linear unabhängig (Induktion nach n). Sei eine lineare Relation $\sum_j \lambda_j \varphi_j(a) = 0$ für alle $a \in A$ mit gewissen $\lambda_j \in K$ gegeben. Weil die φ_j Homomorphismen sind, gilt dann auch für alle $a, b \in A$ die Relation $0 = \sum_j \lambda_j \varphi_j(a)\varphi_j(b)$. Wir subtrahieren von dieser Gleichung die mit $\varphi_1(b)$ multiplizierte erste und erhalten

$$\sum_{j=2}^{n} \lambda_j(\varphi_j(b) - \varphi_1(b))\varphi_j(a) = 0.$$

Aus der linearen Unabhängigkeit folgt $\lambda_j(\varphi_j(b) - \varphi_1(b)) = 0$ für alle b. Wegen $\varphi_j \neq \varphi_1$ zeigt das $\lambda_j = 0$. □

Im vorstehenden Satz wird von A nicht verlangt, daß ein Einselement existiert oder daß A assoziativ ist.

(2.3) Folgerung. *Es ist* $\dim_K \mathrm{Hom}_k(A, K) = \dim_k(A)$. *Also gilt*

$$|\mathrm{Alg}_k(A, K)| \leq \dim_k(A).$$

Insbesondere gilt die Abschätzung

$$|\mathrm{Mor}_k(F, K)| \leq \dim_k F = [F : k]$$

für alle $F \in \mathrm{Zw}(K)$. □

(2.4) Folgerung. *Die Menge* $G \subset \mathrm{Alg}_k(K, K)$ *ist in* $\mathrm{Hom}_k(K, K)$ K*-linear unabhängig.* □

Beweis von (2.1). Seien $v_1, \ldots, v_n \in V$ k-linear unabhängig. Je $n-1$ seien linear unabhängig über K in W. Sei $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ eine echte lineare Relation über K. Dann ist $\lambda_n \neq 0$, und wir nehmen deshalb ohne Schaden $\lambda_n = 1$ an. Durch Anwendung von σ wird aus der linearen Relation $\sum_j \sigma(\lambda_j)v_j = 0$, da $v_j \in W^G$ ist. Wir subtrahieren beide Relationen und erhalten wegen $\sigma(\lambda_n) = \sigma(1) = 1$ aus der linearen Unabhängigkeit von $v_1, \ldots, v_{n-1}$, daß $\sigma(\lambda_j) = \lambda_j$ ist. Da dieses für alle σ gilt, liegen die λ_j in $k = K^G$. Damit haben wir eine lineare Relation über k, im Widerspruch zur Annahme.

Wir müssen noch zeigen, daß V den K-Vektorraum W erzeugt. Falls dem nicht so ist, gibt es eine K-lineare Abbildung $f\colon W \to K$, die auf V verschwindet, aber nichttrivial ist. Das Element $\sum_{\sigma \in G} \sigma(\lambda w)$ liegt für alle $\lambda \in K$ und $w \in W$ in $W^G = V$. Also gilt

$$0 = f(\sum_\sigma \sigma(\lambda w)) = \sum_\sigma \sigma(\lambda) f(\sigma(w)).$$

Diese Gleichung ist eine lineare Relation zwischen den Elementen von G. Nach (2.4) ist $f\sigma(w) = 0$ und speziell $f(w) = 0$ für alle $w \in W$, im Widerspruch zu $f \neq 0$. □

Wir definieren nun die für unsere Zwecke wichtigen verschränkten Darstellungen. Sei S eine endliche G-Menge. Der K-Vektorraum $\mathrm{Abb}(S, K)$ aller Abbildungen $S \to K$ ist eine K-Algebra vermöge Addition und Multiplikation von Funktionswerten. Sie trägt die G-Operation $(\sigma, f) \mapsto \sigma * f$ mit $(\sigma * f)(s) = \sigma f(\sigma^{-1}s)$. Die Fixpunktmenge ist die Menge $\mathrm{Abb}_G(S, K)$ aller G-Abbildungen.

(2.5) Notiz. *Der* K*-Vektorraum* $A = \mathrm{Abb}(S, K)$ *zusammen mit der eben definierten* G*-Operation ist eine verschränkte* (K, G)*-Darstellung. Jedes Element von* G *wirkt auf* A *als ein Automorphismus von* k*-Algebren. Speziell ist* $\mathrm{Abb}_G(S, K) = \mathrm{Abb}(S, K)^G$ *eine* k*-Algebra.*

BEWEIS. Für $\sigma \in G$, $\lambda \in K$, $f \in A$ und $s \in S$ gilt

$$(\sigma * (\lambda f))(s) = \sigma(\lambda f(\sigma^{-1}s)) = \sigma(\lambda) \cdot \sigma f(\sigma^{-1}s)$$

und besagt die Regel (2) einer verschränkten Darstellung $\sigma*(\lambda f) = \sigma(\lambda)\cdot(\sigma * f)$. Die Aussagen $\sigma * (f_1 + f_2) = \sigma * f_1 + \sigma * f_2$ und $\sigma * (f_1 f_2) = (\sigma * f_1) \cdot (\sigma * f_2)$ folgen unmittelbar durch Einsetzen der Definitionen. Da jedes Element von G als Automorphismus von k-Algebren wirkt, ist die Fixpunktmenge eine k-Algebra.□

Wegen (2.5) können wir auf $A = \mathrm{Abb}(S, K)$ den Satz (2.1) anwenden und erhalten:

(2.6) Notiz. *Für jede endliche G-Menge S gilt*

$$|S| = \dim_K \mathrm{Abb}_K(S, K) = \dim_k \mathrm{Abb}_G(S, K).$$

3 Beweis der Korrespondenzsätze

Wir beweisen die Sätze (1.2) und (1.3) für eine Galois-Symmetrie. Wir verwenden die Bezeichungen der vorigen Abschnitte.

Beweis von (1.2). Für jede Untergruppe U von G gilt

$$\dim_k K^U = |G/U|. \tag{3.1}$$

BEWEIS. Wir haben einen Isomorphismus von k-Algebren

$$\mathrm{Abb}_G(G/U, K) \to K^U, \quad f \mapsto f(eU).$$

Nach (2.6) ist die k-Dimension der linken Seite gleich $|G/U|$. □

Sei $F \in \mathrm{Zw}(K)$. Wir haben die Ungleichungen

$$\dim_k F \geq |\operatorname{Mor}_k(F, K)| \geq |G/GF| = \dim_k K^{G_F} \geq \dim_k F.$$

Die erste Ungleichung wird durch (2.3) gegeben; die zweite durch die Injektivität der Abbildung i_F aus (1.4); die Gleichheit ist (3.1); die letzte Ungleichung gilt wegen der Inklusion $F \subset K^{G_F}$, die aus der Definition von G_F folgt. In der Kette steht also überall die Gleichheit. Das bedeutet:

$$\Phi\Sigma(F) = F. \tag{3.2}$$

$$\dim_k F = |G/G_F|. \tag{3.3}$$

$$G/G_F \cong \operatorname{Mor}_k(F, K). \tag{3.4}$$

Mit (3.1) und (3.3) sind die Anzahlrelationen von (1.2) gezeigt. Mit (3.4) ist die Bijektivität von i_F in (1.4) bewiesen.

Sei $F = K^U$ für $U \in \mathrm{Un}(G)$. Wir haben die Gleichungen

$$|G/U| = \dim_k K^U = \dim_k F = |G/G_F|.$$

Die erste ist (3.1), die zweite die Definition von F und die dritte (3.3). Nach Definition von F gilt $U < G_F$; also folgt die Gleichheit $U = G_F$, d. h.

(3.5) $$\Sigma\Phi(U) = U.$$

Mit (3.2) und (3.5) sind die Aussagen über Φ und Σ in (1.2) gezeigt. □

Beweis von (1.3). Sei $\sigma \in G$ und $\sigma(L) \subset M$. Wegen $M = K^B$ gilt für jedes $b \in B$ die Gleichheit $b\sigma|L = \sigma|L$. Demnach bildet $\sigma^{-1}b\sigma$ den Körper L in sich ab und liegt nach (1.2) in A. Also gilt $\sigma A \in G/A^B$. Ist $\sigma a = \tau$ für ein $a \in A$, so gilt wegen $L = K^A$ die Gleichheit $\sigma|L = \tau|L$. Damit ist Φ als wohldefiniert und injektiv erkannt.

Sei $\varphi \in \mathrm{Mor}_k(L, M)$. Wegen (3.4) gibt es ein σ_φ mit $\sigma_\varphi|L = \varphi$. Ist $\sigma|L = \tau|L$, so bildet $\tau^{-1}\sigma$ den Körper L in sich ab und liegt deshalb in A. Damit ist Σ als wohldefiniert erkannt.

Nach Konstruktion sind Σ und Φ zueinander invers. □

Beweis von (1.1). (1) ⇒ (2). Sei $G = G(K|k) = Mor_k(K, K)$ die Automorphismengruppe der Erweiterung $K|k$. Die Gruppe $G(K|K^G)$ enthält G nach Konstruktion. Nach (2.3) ist $|G(K|K^G)| \leq [K : K^G]$. Aus der Kette

$$[K : k] = |G| \leq |G(K|K^G)| \leq [K : K^G] \leq [K : k]$$

folgt die Gleichheit $k = K^G$. Also ist (K, G) eine Galois-Symmetrie mit Grundkörper k.
(2) ⇒ (1). Nach (1.2) ist $[K : k] = |G|$. Nach Definition ist $G < G(K|k)$. Wegen $|G(K|k)| \leq [K : k]$ ist $G = G(K|k)$ und damit $K|k$ eine Galois-Erweiterung mit Gruppe G. □

4 Der Existenzsatz

(4.1) Satz. *Eine endliche Erweiterung $K|k$ ist genau dann ein Galois-Erweiterung, wenn sie normal und separabel ist.*

Im Beweis dieses Existenzsatzes verwenden wir den folgenden Satz.

(4.2) Satz. *Sei (K, G) eine Galois-Symmetrie, sei $a \in K$ und sei Ga die G-Bahn von a. Dann ist*

$$f_a = \prod_{u \in Ga} (x - u)$$

das Minimalpolynom von a über k.

Beweis. Wir wenden $\sigma \in G$ auf f_a an und erhalten $\sigma_* f_a = \prod_u (x - \sigma(u))$. In diesem Produkt sind gegenüber f_a die Faktoren nur vertauscht. Also ist $\sigma_* f_a = f_a$. Da $\sigma_* f_a$ durch Anwendung von σ auf die Koeffizienten von f_a entsteht, sehen

wir, daß diese in $K^G = k$ liegen. Folglich ist $f_a \in k[x]$ ein Polynom mit der Nullstelle a. Mit einer Nullstelle b muß auch $\sigma(b)$ Nullstelle des Minimalpolynoms sein. Also ist f_a das Minimalpolynom. □

Beweis von (4.1). Sei (K, G) eine Galois-Symmetrie. Nach (4.2) ist dann jedes $a \in K$ Nullstelle eines Polynoms $f \in k[x]$, das über K in verschiedene Linearfaktoren zerfällt. Das bedeutet aber gerade, daß $K|k$ normal und separabel ist. Die Umkehrung wurde in VI(4.5) gezeigt; dazu beachte man die Definitionen aus VI.5 und VI.6. □

Eine Erweiterung $K|k$ ist genau dann normal und separabel, wenn sie Zerfällungskörper eines separablen Polynoms $f \in k[x]$ ist. In solchem Fall nennen wir $G(Kk)$ auch die *Galois-Gruppe von* f.

5 Reine Gleichungen

Ein Polynom der Form $x^n - a \in k[x]$ heißt *reines Polynom*. Ein Element b einer Erweiterung $K|k$ heißt *n-Radikal* oder n-te *Wurzel* von a, wenn $b^n = a$ ist. Wir setzen im folgenden voraus, daß $n \in \mathbb{N}$ teilerfremd zur Charakteristik von k ist. Für $a \neq 0$ haben dann $x^n - a$ und nx^{n-1} keinen gemeinsamen Teiler. Das Polynom $x^n - a$ ist separabel.

Sei $k_n|k$ der Zerfällungskörper von $x^n - 1$. Er entsteht aus k durch Adjunktion der n-ten Einheitswurzeln.

Sei K der Zerfällungskörper von $x^n - a$ für $a \in k^*$. Es gibt n verschiedene n-Radikale $b_1, \ldots, b_n$ von a in K. Die Elemente $1, b_2/b_1, \ldots, b_n/b_1$ sind dann n verschiedene n-te Einheitswurzeln. Also gilt $k_n \subset K$. Ist b ein n-Radikal von a und sind $\zeta_1, \ldots, \zeta_n \in K$ die n-ten Einheitswurzeln, so sind $b\zeta_1, \ldots, b\zeta_n$ die n Nullstellen von $x^n - a$. Ferner gilt $K = k_n(b)$. Die Erweiterungen $K|k$, $K|k_n$, $k_n|k$ sind als Zerfällungskörper separabler Polynome Galois-Erweiterungen.

(5.1) Satz. *Sei $k = k_n$ und $K|k$ Zerfällungskörper von $x^n - a$, $a \in k^*$. Sei $b^n = a$. Die kleinste Zahl $t \in \mathbb{N}$, so daß $b^t \in k$ ist, ist unabhängig von der Auswahl des n-Radikals b von a und ein Teiler von n. Die Galois-Gruppe von $K|k$ ist isomorph zu $\mathbb{Z}/t$. Ferner ist K Zerfällungskörper von $x^t - b^t \in k[x]$.*

Beweis. Da $k = k_n$ ist, so haben wir eben gesehen, daß $K = k(b)$ ist. Ist $b^t \in k$, so ist b Nullstelle von $x^t - b^t$. Sei $n = qt + r$ mit $0 \leq r < t$. Dann ist $b^n b^{-qt} = b^r \in k$ im Widerspruch zur Minimalität von t. Ebenso sieht man, daß b^s genau dann in k liegt, wenn t ein Teiler von s ist. Wegen $t|n$ ist $x^t - b^t$ ein Teiler von $x^n - b^n = x^n - a$ und zerfällt in K in Linearfaktoren. Also ist K auch Zerfällungskörper von $x^t - b^t$.

Sei $\varphi \in G(K|k)$. Mit b ist auch $\varphi(b)$ eine Nullstelle von $x^t - b^t$. Folglich gilt $\varphi(b) = \xi^{r(\varphi)} b$ mit einer primitiven t-ten Einheitswurzel ξ, die nach Voraussetzung in $k = k_n$ liegt. Es ist $r(\varphi) \bmod t$ durch φ eindeutig bestimmt, und $\varphi \mapsto r(\varphi)$ ist ein injektiver Homomorphismus $\gamma\colon G(K|k) \to \mathbb{Z}/t$. Insbesondere ist $G(K|k)$ zyklisch. Sei φ ein erzeugendes Element von $G(K|k)$. Dann ist $\varphi(u) = u$ äquivalent zu $u \in k$. Wir haben also die folgenden Äquivalenzen: $t|s$ genau wenn $b^s \in k$

genau wenn $b^s = \varphi(b^s) = \xi^{r(\varphi)s}b^s$ genau wenn $\xi^{r(\varphi)s} = 1$. Also muß $\xi^{r(\varphi)}$ eine primitive t-te Einheitswurzel sein. Somit hat φ die Ordnung t, und γ ist ein Isomorphismus. □

(5.2) Satz. *Sei $k = k_n$ und $K|k$ eine Galois-Erweiterung mit Gruppe $\mathbb{Z}/n$. Dann gibt es ein $b \in K$ mit $b^n \in k$ und $K = k(b)$. Es ist dann K der Zerfällungskörper von $x^n - b^n \in k[x]$.*

Beweis. Sei $\varphi \in G(K|k)$ ein erzeugendes Element, sei $c \in K$ und $\zeta \in K$ eine primitive n-te Einheitswurzel. Das Element $b = b(c) = c + \zeta^{-1}\varphi(c) + \cdots + \zeta^{-(n-1)}\varphi^{n-1}(c)$ erfüllt $\varphi(b) = \zeta b$. Es gibt ein $c \in K$, so daß $b(c) \neq 0$ ist, weil die Elemente von $G(K|k)$ linear unabhängig in $\mathrm{Hom}_k(K, K)$ sind (2.4).

Die Automorphismen $1, \varphi, \ldots, \varphi^{n-1}$ sind wegen $\varphi^j(b) = \zeta^j b$ auf $k(b)$ alle verschieden. Also ist $[k(b)\colon k] \geq n$ und demnach $K = k(b)$. Ferner ist wegen $\varphi(b^n) = (\zeta b)^n = b^n$ das Element b^n invariant unter der Galois-Gruppe und liegt deshalb in k. □

6 Konsequenzen aus den Hauptsätzen

(6.1) Satz. *Eine Galois-Erweiterung hat nur endlich viele Zwischenkörper, da jeder Zwischenkörper Fixpunktmenge einer Untergruppe der Galois-Gruppe ist.* □

(6.2) Satz. *Sei $K|k$ Galois-Erweiterung und L ein Zwischenkörper. Dann ist $K|L$ Galois-Erweiterung mit Galois-Gruppe G_L.* □

(6.3) Satz. *Sei $L|k$ eine endliche separable Erweiterung. Dann ist L Zwischenkörper einer Galois-Erweiterung $K|k$.*

Beweis. Ist nämlich $L = k(a_1, \ldots, a_m)$, so wähle man als K den Zerfällungskörper der Minimalpolynome der a_j. □

(6.4) Satz. *Eine endliche separable Erweiterung $L|k$ besitzt ein primitives Element, d. h. es gilt $L = k(a)$ mit einem $a \in L$.*

Beweis. Die Erweiterung hat nur endlich viele Zwischenkörper. Ein Vektorraum über einem unendlichen Körper ist nicht Vereinigung endlich vieler echter Unterräume. Ein Element a, das in keinem echten Zwischenkörper liegt, liefert $L = k(a)$. Ist L endlich, so gilt die Aussage, weil L^* zyklisch ist. □

(6.5) Folgerung. *Eine Galois-Erweiterung ist Zerfällungskörper eines geeigneten irreduziblen Polynoms.* □

(6.6) Satz. *Erweiterungen $L|k$ und $M|k$ in $\mathrm{Zw}(K|k)$ sind genau dann k-isomorph, wenn G_L und G_M in G konjugiert sind.* □

(6.7) Satz. *Sei $L \subset M$ eine Inklusion von Zwischenkörpern von $K|k$. Dann ist $G(M|L)$ isomorph zu $(N_G G_M \cap G_L)/G_M$. Genau dann ist $M|L$ galoissch, wenn $G_M \lhd G_L$ ist; in diesem Fall ist $G(M|L) \cong G_L/G_M$.*

BEWEIS. Da $K|L$ eine Galois-Erweiterung mit Gruppe G_L ist, genügt es, den Fall $L = k$ zu betrachten. Nach (1.3) ist dann $N_G G_M/G_M$ die Automorphismengruppe von $M|k$. Die Erweiterung ist genau dann galoissch, wenn diese Gruppe die Ordnung G/G_M hat, wenn also $G = N_G G_M$ ist. □

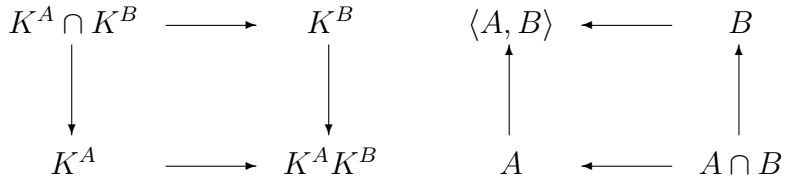
Die Mengen $\mathrm{Zw}(K|k)$ und $\mathrm{Un}(G)$ tragen eine weitere Struktur, nämlich eine durch Inklusion gegebene teilweise Ordnung. Die Zuordnungen Φ und Γ kehren die Ordnung um. Ordnungstheoretische Begriffe übertragen sich also. Dafür einige Beispiele.

Der Schnitt zweier Untergruppen A, B ist die Untergruppe C mit den beiden Eigenschaften: (1) $C \leq A$, $C \leq B$ und (2) $D \leq A$, $D \leq B$ impliziert $D \leq C$ (Infimum von A und B). Die von A, B erzeugte Untergruppe $C = \langle A, B\rangle$ ist dual als Supremum charakterisiert: (1) $A \leq C$, $B \leq C$ und (2) $A \leq D$, $B \leq D$ impliziert $C \leq D$. Für die Zwischenkörper gilt Entsprechendes. Aus dem Satz (1.2) folgt demnach:

$$\textbf{(6.8)} \qquad K^A \cap K^B = K^{\langle A,B\rangle}, \quad \langle K^A, K^B\rangle = K^{A\cap B}$$

$$\textbf{(6.9)} \qquad \langle G_L, G_M\rangle = G_{L\cap M}, \quad G_{\langle L,M\rangle} = G_L \cap G_M.$$

Der von Zwischenkörpern L und M erzeugte Körper $\langle L, M\rangle$ wird auch mit LM bezeichnet und *Kompositum* von L und M (in K) genannt. Die Situation (6.8) veranschaulichen wir durch die folgenden Diagramme.



(6.10) Lemma. *Genau dann ist $A \lhd \langle A, B\rangle$, wenn $B \subset N_G(A)$. In diesem Fall ist $\langle A, B\rangle = AB$, und wir haben dann nach einem Isomorphiesatz $AB/A \cong B/A \cap B$.* □

(6.11) Satz. *Sei $L, M \in \mathrm{Zw}(K)$ und $L \cap M \subset L$ eine Galois-Erweiterung. Dann ist auch $M \subset LM$ eine Galois-Erweiterung. Ein $\sigma \in G(LM|M)$ induziert durch Einschränkung $\sigma|L \in G(L|L \cap M)$, und $\sigma \mapsto \sigma|L$ ist ein Isomorphismus $G(LM|M) \cong G(L|L \cap M)$.*

BEWEIS. Sei $L = K^A$ und $M = K^B$. Wegen $K^A \cap K^B = K^{\langle a,b\rangle}$ und der Voraussetzung ist $A \lhd \langle\, A, B\,\rangle$. Nach dem Lemma ist $A \cap B \lhd B$ und deshalb $K^B \subset K^{A\cap B} = K^A K^B$ eine Galois-Erweiterung. Ein $\sigma \in G(LM|M) = G_M/G_L \cap G_M = B/A \cap B$ bildet genau dann L in sich ab, wenn $\sigma \in N_G(G_L) = N_G(A)$, was aber der Fall ist. Der behauptete Isomorphismus entspricht dann genau dem kanonischen $B/A \cap B \to AB/B$ des Isomorphiesatzes. □

In einem Kompositum von Galois-Erweiterungen kann man die Gruppe des Kompositums aus den Gruppen der beteiligten Körper aufbauen.

(6.12) Satz. *Seien $L_1|k$ und $L_2|k$ Galois-Erweiterungen in $\mathrm{Zw}(K|k)$. Die Inklusionen $L_1 \cap L_2 \subset L_j \subset L_1L_2$ induzieren durch Einschränkung von Automorphismen das Diagramm*

$$\begin{array}{ccc} G(L_1L_2|k) & \xrightarrow{\alpha_1} & G(L_1|k) \\ \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \beta_1} \\ G(L_2|k) & \xrightarrow{\beta_2} & G(L_1 \cap L_2|k) \end{array}$$

Die Abbildung

$$(\alpha_1, \alpha_2)\colon G(L_1L_2|k) \to G(L_1|k) \times G(L_2|k).$$

ist injektiv und ihr Bild besteht genau aus den Paaren (x, y) mit $\beta_1(x) = \beta_2(y)$, d. h. das Diagramm ist ein Pullback von Gruppen.

Beweis. Sind $L \subset M$ Galois-Erweiterungen in $\mathrm{Zw}(K|k)$ mit $G_M = A \subset G_L = B$, so ist die durch Einschränkung von Automorphismen gegebene Abbildung die Faktorabbildung $G/A \to G/B$. Sei L_j die Fixpunktmenge von A_j. Dann entspricht das obige Diagramm dem kanonischen Diagramm

$$\begin{array}{ccc} G/(A_1 \cap A_2) & \longrightarrow & G/A_1 \\ \downarrow & & \downarrow \\ G/A_2 & \longrightarrow & G/A_1A_2 \end{array}$$

und für dieses ist die Behauptung klar. □

Die Injektivität von (α_1, α_2) bedeutet: Ist $\varphi \in G(L_1L_2|k)$ auf L_1 und L_2 die Identität, so auch auf L_1L_2, denn $L_1 \cup L_2$ erzeugt L_1L_2.

Der Satz enthält die interessante Aussage, daß man Automorphismen von L_1 und L_2 zu einem von L_1L_2 zusammensetzen kann, wenn sie auf $L_1 \cap L_2$ übereinstimmen.

Man muß in (7.12) übrigens nur voraussetzen, daß L_1 und L_2 in einem Körper $K|k$ liegen. Dann ist $L_1L_2|k$ eine Galois-Erweiterung.

(6.13) Aufgaben und Ergänzungen.

1. Sind $L|K$ und $K|k$ Galois-Erweiterungen, so ist $L|k$ nicht notwendig eine Galois-Erweiterung. Beispiele, in denen beide Erweiterungen quadratisch sind?

2. Der Körper $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ hat über $\mathbb{Q}$ höchstens den Grad 4. Es gibt 4 verschiedene Automorphismen, die durch $(\sqrt{2}, \sqrt{3}) \mapsto (\pm\sqrt{2}, \pm\sqrt{3})$ bestimmt sind. Also ist $K|\mathbb{Q}$ eine Galois-Erweiterung mit Gruppe $\mathbb{Z}/2 \times \mathbb{Z}/2$. Die Bahn des Elementes $\sqrt{2} + \sqrt{3}$ hat die Länge 4. Deshalb ist $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Nach dem Verfahren von (4.2) errechnet sich das Minimalpolynom von $\sqrt{2} + \sqrt{3}$ zu $x^4 - 10x^2 + 1$.

7 Radikalerweiterungen

Eine Körpererweiterung $K|k$ heißt *Radikalerweiterung*, wenn es eine Kette

$$k = L_0 \subset L_1 \subset \ldots \subset L_m = K$$

von Zwischenkörpern L_j gibt, so daß jeweils L_j aus L_{j-1} durch Adjunktion einer Nullstelle eines reinen Polynoms erhalten wird. Eine Erweiterung $L|k$ heiße durch *Radikale auflösbar*, wenn L Zwischenkörper einer Radikalerweiterung ist. Ein Polynom $f \in k[x]$ heiße durch *Radikale auflösbar*, wenn dieses für seinen Zerfällungskörper gilt.

Der Einfachheit halber arbeiten wir im folgenden nur mit Körpern der Charakteristik Null.

Eine endliche Gruppe G heißt *auflösbar*, wenn es eine Sequenz

$$1 = G_0 < G_1 < \ldots < G_m = G$$

von Untergruppen so gibt, daß jeweils $G_j \lhd G_{j+1}$ und der Quotient G_{j+1}/G_j zyklisch ist. Wir benutzen im folgenden, daß in einer exakten Sequenz

$$1 \to H \to G \to G/H \to 1$$

G genau dann auflösbar ist, wenn dieses für H und G/H gilt (siehe die Aufgaben).

Der folgende Satz gibt eine gruppentheoretische Charakterisierung von Radikalerweiterungen.

(7.1) Satz. *Eine Galois-Erweiterung $L|k$ ist genau dann durch Radikale auflösbar, wenn ihre Galois-Gruppe auflösbar ist.*

Beweis. (1) Sei $K|k$ eine galoissche Radikalerweiterung, die L als Zwischenkörper enthält. Dann ist $G(L|k)$ Quotient von $G(K|k)$, und es genügt, letztere als auflösbar nachzuweisen. Es gibt also eine Kette

$$k = L_0 \subset L_1 \subset \ldots \subset L_m = K,$$

worin $L_{j+1} = L_j(b_j)$ und $b_j^{n(j)} = c_j \in L_j$ ist. Sei $n = n(1)n(2)\ldots n(m-1)$ und ζ eine primitive n-te Einheitswurzel in einer Erweiterung von K. Wir adjungieren ζ zu allen Körpern der Kette. Dann sind auch

$$L_{j+1}(\zeta) \supset L_j(\zeta),\ K(\zeta) \supset k,\ k(\zeta) \supset k$$

Galois-Erweiterungen. Ist nämlich $K|k$ Zerfällungskörper von g, so ist $K(\zeta) \supset k$ Zerfällungskörper von $(x^n - 1) \cdot g$. Ferner enthält $L_j(\zeta)$ eine primitive $n(j)$-te Einheitswurzel, und deshalb ist $L_{j+1}(\zeta) \supset L_j(\zeta)$ nach Abschnitt 10 Zerfällungskörper von $x^{n(j)} - e_j$. Da $K|k$ Galois-Erweiterung ist, so ist $G(K|k)$ Faktorgruppe von $G(K(\zeta)|k)$. Es genügt also, letztere als auflösbar nachzuweisen. In der Kette

$$1 \subset G(K(\zeta) \mid L_{m-1}(\zeta)) \subset \ldots \subset G(K(\zeta)|L_0(\zeta)) \subset G(K(\zeta)|k)$$

ist $G(K(\zeta)|L_{j+1}(\zeta))$ Normalteiler von $G(K(\zeta)|L_j(\zeta))$ mit der Faktorgruppe $G(L_{j+1}(\zeta)|L_j(\zeta)) := G_j$, weil alle drei Erweiterungen Galois-Erweiterungen sind. Die Gruppe G_j ist aber zyklisch, wie wir im letzten Abschnitt gesehen haben. Ebenso ist $G(K(\zeta)|k(\zeta))$ Normalteiler in $G(K(\zeta)|k)$ mit zyklischer Faktorgruppe $G(k(\zeta)|k)$. Damit ist $G(K(\zeta)|k)$ als auflösbar nachgewiesen.

(2) Wir müssen im allgemeinen die Voraussetzung des ersten Beweisschrittes sicherstellen. Wir zeigen dazu: Eine Radikalerweiterung ist in einer galoisschen Radikalerweiterung enthalten. Der Beweis wird durch Induktion nach dem Körpergrad geführt. Sei zunächst $K = k(a)$ und a Nullstelle von $x^n - a$. Der Zerfällungskörper dieses Polynoms ist dann durch $k_n(a) \supset k_n \supset k$ gegeben, und beide Schritte sind Radikalerweiterungen.

Sei nun $K|L|k$ und $K = L(b)$ mit $b^n \in L$. Wir wählen eine galoissche Radikalerweiterung $L'|L|k$ mit Gruppe $G = G(L'|k)$. Der Zerfällungskörper K' von

$$g = \prod_{\varphi \in G} (x^n - \varphi(b^n))$$

über L' ist eine Radikalerweiterung. Da g Koeffizienten in k hat, ist $K'|k$ eine Galois-Erweiterung.

Sei umgekehrt $G(K|k) = G$ auflösbar. Wir wählen eine Reihe

$$1 = G_m \lhd G_{m-1} \lhd \ldots \lhd G_0 = G$$

mit zyklischen Faktoren G_j/G_{j+1}. Sei L_j die G_j-Fixpunktmenge in K. Wir haben dann eine Kette von Zwischenkörpern

$$K = L_m \supset L_{m-1} \supset \ldots \supset L_0 = k,$$

worin $L_{j+1}|L_j$ eine Galois-Erweiterung mit Gruppe G_j/G_{j+1} ist.

Wir adjungieren zu dieser Kette wieder eine primitive n-te Einheitswurzel ζ für $n = |G|$. Es genügt dann zu zeigen, daß

$$K(\zeta) = L_m(\zeta) \supset L_{m-1}(\zeta) \supset \ldots \supset L_0(\zeta) = k(\zeta) \supset k$$

eine Radikalerweiterung ist. Wieder ist mit $L_{j+1}|L_j$ auch $L_{j+1}(\zeta)|L_j$ eine Galois-Erweiterung. Wenn wir zeigen, daß $L_{j+1}(\zeta)|L_j(\zeta)$ eine Radikalerweiterung ist, sind wir fertig. Nach (6.2) müssen wir dazu die Galois-Gruppe als zyklisch nachweisen. Der Homomorphismus in eine zyklische Gruppe

$$G(L_{j+1}(\zeta)|L_j(\zeta)) \xrightarrow{\subset} G(L_{j+1}(\zeta)|L_j) \to G(L_{j+1}|L_j)$$

ist aber injektiv, denn ein Element im Kern ist auf $L_{j+1} \cup L_j(\zeta)$ die Identität, also auf dem Erzeugnis $L_{j+1}(\zeta)$. □

(7.2) Aufgaben und Ergänzungen.

1. Sei $G^{(1)}$ die Kommutatorgruppe von G und induktiv $G^{(n)}$ die Kommutatorgruppe von $G^{(n-1)}$. Aus dem Entsprechungssatz folgt, daß es eine Sequenz

$$H = H_0 \lhd H_1 \lhd \ldots \lhd H_t = G$$

mit zyklischen Quotienten H_j/H_{j-1} gibt, wenn $G^{(1)} < H$ ist.

2. Aus $B < A$ folgt $B^{(n)} < A^{(n)}$.

3. Ein surjektiver Homomorphismus $A \to C$ induziert surjektive Homomorphismen $A^{(n)} \to C^{(n)}$.

4. Hat die Sequenz

$$H = H_t \lhd H_{t-1} \lhd \ldots \lhd H_0 = G$$

abelsche Quotienten H_j/H_{j+1}, so gilt $G^{(j)} < H_j$.

5. G ist genau dann auflösbar, wenn es ein $n \in \mathbb{N}$ mit $G^{(n)}$ gibt.

6. In einer Sequenz

$$1 \to H \to G \to G/H \to 1$$

ist G genau dann auflösbar, wenn H und G/H auflösbar sind.

7. Eine p-Gruppe ist auflösbar.

8 Beispiele

Kreisteilungskörper.

(8.1) Satz. *Sei $\zeta \in \mathbb{C}$ eine primitive n-te Einheitswurzel. Dann ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ eine Galois-Erweiterung. Die Galois-Gruppe G ist isomorph zur Einheitengruppe $(\mathbb{Z}/n)^*$.*

Beweis. Wir fixieren $\zeta = \zeta_n = \exp(2\pi i/n)$. Wir wissen, daß $\mathbb{Q}(\zeta)$ der Zerfällungskörper des Kreisteilungspolynoms Φ_n ist. Folglich ist $\mathbb{Q}(\zeta)|\mathbb{Q}$ eine Galois-Erweiterung. Ein Element σ der Galois-Gruppe G von $\mathbb{Q}(\zeta)|\mathbb{Q}$ bildet ζ auf ein ζ^a mit $(a, n) = 1$ ab, da G die Nullstellen von Φ_n permutiert. Indem wir $\sigma \in G$ die zugehörige Restklasse a zuordnen, erhalten wir einen kanonischen Homomorphismus $G(\mathbb{Q}(\zeta)|\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/n)^*$, der bijektiv ist, da beide Gruppen dieselbe Ordnung haben. □

Sei p eine ungerade Primzahl. Die Gruppe $(\mathbb{Z}/p)^* = G$ ist zyklisch und hat deshalb genau eine Untergruppe H vom Index 2. Somit ist $\mathbb{Q}(\zeta)^H = K$ eine quadratische Erweiterung von $\mathbb{Q}$, die im Kreisteilungskörper der p-ten Einheitswurzeln liegt. Wir wollen sie bestimmen.

Der Homomorphismus $G \to \{\pm 1\}$ mit dem Kern H wird $a \bmod p \mapsto (\frac{a}{p})$ bezeichnet und $(\frac{a}{p})$ *Legendre-Symbol* genannt.

(8.2) Satz. *In $\mathbb{Q}(\zeta_p)$ liegt die durch $x^2 = (-1)^{(p-1)/2}p$ bestimmte quadratische Erweiterung.*

BEWEIS. Um K zu bestimmen, müssen wir ein Element $u \in K \backslash \mathbb{Q}$ angeben und feststellen, welcher quadratischen Gleichung es genügt. Für jedes $a \in \mathbb{Q}(\zeta)$ liegen die Elemente

$$\Sigma(a) = \sum_{\sigma \in H} \sigma(a), \quad \Sigma^-(a) = \sum_{\tau \in G \backslash H} \tau(a)$$

in der H-Fixpunktmenge und folglich auch jede Linearkombination $\alpha\Sigma(a) + \beta\Sigma^-(a)$ über $\mathbb{Q}$. Ferner liegt $\Sigma(a) + \Sigma^-(a)$ in der G-Fixpunktmenge, also in $\mathbb{Q}$. Wegen

$$\alpha\Sigma(a) + \beta\Sigma^-(a) = \frac{\alpha - \beta}{2}(\Sigma(a) - \Sigma^-(a)) + \frac{\alpha + \beta}{2}(\Sigma(a) + \Sigma^-(a))$$

sind also die Elemente $\Sigma(a) - \Sigma^-(a)$ die einzig Betrachtenswerten. Diese gehen aber im wesentlichen aus dem Fall $a = \zeta$ hervor. Das Element

$$\textbf{(8.3)} \qquad S = \sum_{u \in G} (\frac{u}{p}) \zeta^u$$

muß also K erzeugen. Es heißt *Gaußsche Summe*. Wir zeigen:

$$\textbf{(8.4)} \qquad S^2 = (\frac{-1}{p}) p.$$

Zunächst gilt

$$S^2 = \left(\sum_u (\frac{u}{p}) \zeta^u \right)^2 = \sum_{u,v} (\frac{uv}{p}) \zeta^{u+v}.$$

Mit v durchläuft für festes u auch uv alle Elemente von $(\mathbb{Z}/p)^*$ genau einmal. Damit erhalten wir:

$$\begin{aligned}
S^2 &= \sum_{u,v} (\frac{uuv}{p}) \zeta^{u+uv} = \sum_{u,v} (\frac{v}{p}) \zeta^{u(1+v)} \\
&= \sum_v (\frac{-1}{p}) \zeta^0 + \sum_{v \neq -1} (\frac{v}{p}) \sum_u \zeta^{u(1+v)} \\
&= (\frac{-1}{p})(p-1) + \sum_{v \neq -1} (\frac{v}{p}) \sum_u \zeta^u \\
&= (\frac{-1}{p})(p-1) + \sum_{v \neq -1} (\frac{v}{p})(-1) \\
&= (\frac{-1}{p})(p-1) + (\frac{-1}{p}) - \sum_v (\frac{v}{p}) \\
&= (\frac{-1}{p}) p
\end{aligned}$$

Es ist $(\frac{-1}{p}) = (-1)^{(p-1)/2}$, da $a \mapsto a^{(p-1)/2}$ ein Homomorphismus $(\mathbb{Z}/p)^* \mapsto (\mathbb{Z}/p)^*$ mit Bild $\{\pm 1\}$ ist. □

Gleichungen dritten Grades.

(8.5) Satz. *Sei $f = x^3+ax^2+bx+c \in k[x]$ ein irreduzibles separables Polynom. Der Zerfällungskörper K von f hat den Grad 3 oder 6 über k. Im ersten Fall ist die Galois-Gruppe isomorph zu $\mathbb{Z}/3$, im zweiten isomorph zu S_3.*

Beweis. Sei $\alpha \in K$ eine Nullstelle von f. Dann hat $k(\alpha)$ über k den Grad 3. Ist $k(\alpha) \neq K$, so zerfällt f über $k(\alpha)$ in einen linearen und einen quadratischen Faktor. Der Zerfällungskörper $K|k(\alpha)$ des quadratischen Faktors hat den Grad 2. Insgesamt hat $K|k$ den Grad 6. Im letzteren Fall ist die Galois-Gruppe eine Untergruppe der Permutationsgruppe der drei Nullstellen von f, folglich isomorph zu S_3. □

Seien x_1, x_2, x_3 die drei Nullstellen von f in (5.5). Sei

$$\delta(f) = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1), \quad D(f) = \delta^2.$$

Da die Diskriminante $D(f)$ bei allen Permutationen der x_j invariant ist, liegt sie in k.

(8.6) Satz. *Habe k nicht die Charakteristik zwei. Die Galois-Gruppe von f aus (5.5) ist genau dann $\mathbb{Z}/3$, wenn $D(f)$ in k ein Quadrat ist.*

Beweis. Das Produkt δ ist bei zyklischen Permutationen der x_j invariant. Hat $K|k$ den Grad 3, so besteht die Galois-Gruppe aus den zyklischen Permutationen. Folglich liegt dann δ in k und D ist ein Quadrat.

Sei umgekehrt $D = u^2$, $u \in k$. Dann ist $\delta = \pm u \in k$ und folglich δ invariant unter der Galois-Gruppe. Da aber eine Transposition das Vorzeichen ändert, wenn k nicht die Charakteristik zwei hat, ist die Galois-Gruppe isomorph zu $\mathbb{Z}/3$. □

Hat k nicht die Charakteristik 3, so wird f durch die Substitution $x = y - \frac{a}{3}$ in ein Polynom der Form $g = y^3+py+q$ verwandelt. Es gilt $D(g) = -4p^3-27q^2$. Die Diskriminante von $h = x^3 - 3x + 1$ ist 9^2. Dieses Polynom hat also über $\mathbb{Q}$ einen Zerfällungskörper vom Grad 3. Ist $u = \exp(2\pi i/9)$, so hat h die Nullstellen $x_1 = u + u^{-1}$, $x_2 = u^2 + u^{-2}$, $x_3 = u^4 + u^{-4}$. Es gilt $x_1^2 = x_2 + 2$ und $x_2^2 = x_3 + 2$. Man sieht also direkt, daß $\mathbb{Q}(x_1)$ der Zerfällungskörper ist.

Endliche Körper.

Sei p ein Primzahl und $q = p^n$. Dann ist $\mathbb{F}_q$ der Zerfällungskörper des separablen Polynoms $x^q - x \in \mathbb{F}_p[x]$. Folglich ist $\mathbb{F}_q|\mathbb{F}_p$ eine Galois-Erweiterung vom Grad n. Die Abbildung $\sigma\colon \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^p$ ist ein Automorphismus. Ist $\sigma^k = \mathrm{id}$, so muß für alle $x \in \mathbb{F}_q$ die Gleichung $x^{p^k} = x$ gelten. Das ist genau für $k \equiv 0 \bmod n$ der Fall. Also erzeugt σ die Galois-Gruppe von $\mathbb{F}_q|\mathbb{F}_p$.

Polynome mit symmetrischer Galois-Gruppe. Wir konstruieren Polynome mit symmetrischer Galois-Gruppe. Dazu verwenden wir die

(8.7) Notiz. *Sei p eine Primzahl und G eine Untergruppe von S_p, die einen Zweierzyklus und ein Element der Ordnung p enthält. Dann ist $G = S_p$.*

Beweis. Wird eine Permutation in Zyklen zerlegt, so ist ihre Ordnung das KGV der Zyklenlängen. Ein Element der Ordnung p ist deshalb ein p-Zyklus. Wir setzen ihn in der Form $\sigma = (1, 2, \ldots, p)$ an. Der Zweierzyklus sei $\tau = (k, l)$. Dann ist $\sigma\tau\sigma^{-1} = (k+1, l+1)$. Durch Iteration sehen wir, daß alle $(k+t, l+t)$ in G liegen (Einträge $\bmod n$). Ferner gilt $(k,l)(l,m)(k,l) = (k,m)$. Ist $l = k+t$, so ist $t \not\equiv 0 \bmod p$. Es liegen deshalb alle $(k, k+rt)$ in G. Wir wählen $rt \equiv 1 \bmod p$ und sehen, daß $(k, k+1)$ für alle k in G liegt. Diese Transpositionen erzeugen aber S_p. □

(8.8) Satz. *Sei p eine Primzahl und $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad p mit genau zwei nichtreellen Nullstellen. Dann ist die Galois-Gruppe von f gleich S_p.*

Beweis. Mit $a \in \mathbb{C}$ ist auch $\overline{a}$ Nullstelle von f. Komplexe Konjugation ist also ein Element der Galois-Gruppe. Nach Voraussetzung werden dadurch genau zwei Nullstellen vertauscht; also enthält G, aufgefaßt als Permutationsgruppe der Nullstellen, einen Zweierzyklus. Ferner teilt p den Grad des Zerfällungskörpers über $\mathbb{Q}$. Also teilt p auch die Ordnung der Galois-Gruppe; sie enthält demnach ein Element der Ordnung p. Nun wende man (8.7) an. □

(8.9) Beispiel. Die Polynome $x^5 - 4x + 2$ oder $x^5 - 16x + 2 = x(x^2-4)(x^2+2)+2$ haben drei reelle Nullstellen. Mit Hilfe des Kriteriums von Eisenstein sieht man, daß sie irreduzibel sind. ◇

(8.10) Satz. *Die symmetrische Gruppe S_n ist für $n \geq 5$ nicht auflösbar.*

Beweis. Sei H die von allen Dreierzyklen erzeugte Untergruppe. Sind i, j, k, l, m paarweise verschieden und setzen wir $\sigma = (ijk)$, $\tau = (klm)$, so errechnen wir $\sigma^{-1}\tau^{-1}\sigma\tau = (kjl)$. Jeder Dreierzyklus ist also ein Kommutator, d. h. H ist gleich seiner Kommutatorgruppe und deshalb nicht auflösbar. Die Kommutatorreihe $G^{(n)}$ einer Gruppe G endet aber genau dann nicht bei 1, wenn G eine Gruppe H enthält, die gleich ihrer Kommutatorgruppe ist, wie aus den Aufgaben des vorigen Abschnittes sofort folgt. □

11 Halbeinfache Algebren

1 Halbeinfache Moduln

Sei A ein Ring. Wir betrachten Linksmoduln über A. Die folgende einfache Bemerkung ist als *Schursches Lemma* bekannt.

(1.1) Notiz. *Seien E und F einfache Moduln. Ein Homomorphismus $f\colon E \to F$ ist entweder Null oder ein Isomorphismus. Der Endomorphismenring von E ist ein Divisionsring.*

Beweis. Der Kern von f ist 0 oder E. Ist $f \neq 0$, so ist der Kern also Null und deshalb das Bild von Null verschieden, also gleich F. Ist $E = F$ und $f \neq 0$, so ist f ein Automorphismus, hat also im Endomorphismenring $\mathrm{End}_A(E)$ ein Inverses. □

Ist M ein Modul und $(M_j \mid j \in J)$ eine Familie von Untermoduln, so ist die *Summe* $\sum_{j\in J} M_j$ der von $\bigcup_j M_j$ erzeugte Untermodul. Er besteht aus allen Elementen, die sich als endliche Summe von Elementen aus $\bigcup_j M_j$ darstellen lassen. Für direkte Summenzerlegungen sei auf V(2.6) verwiesen; wir verwenden diesen Satz stillschweigend.

(1.2) Satz. *Sei der Modul M Summe einer Familie $(M_j \mid j \in J)$ einfacher Untermoduln. Sei N ein Untermodul von M. Dann gibt es eine Teilmenge $I \subset J$, so daß M direkte Summe von N und $(M_i \mid\in I)$ ist.*

Beweis. Für $I \subset J$ setzen wir $M_I = \sum_{i\in I} M_i$. Wir wählen $I \subset J$ maximal mit der Eigenschaft, daß $N + M_I$ direkte Summe von $(N, M_i \mid i \in I)$ ist. Wir zeigen, daß $N + M_I = M$ ist. Sei $j \in J$. Der Schnitt $M_j \cap (N + M_I)$ ist ein Untermodul von M_j, also gleich Null oder M_j. Ist der Durchschnitt Null, so ist $N + M_I + M_j$ direkte Summe von $N + M_I$ und M_j, also I nicht maximal. Deshalb ist M_j für jedes j in $N + M_I$ enthalten und folglich dieser Modul gleich M. □

Im vorstehenden Beweis gibt es eine maximale Menge nach dem Zornschen Lemma. Ist nämlich $I_\alpha, \alpha \in A$, eine total geordnete Menge von Teilmengen von J derart, daß $M_\alpha = \sum(M_i \mid i \in I_\alpha)$ direkte Summe der $M_i, i \in I_\alpha$ ist und ist I^* die Vereinigung der I_α, so ist auch $\sum(M_i \mid i \in I^*)$ direkte Summe der M_i, $i \in I^*$. Folglich hat jede total geordnete Menge eine obere Schranke, und das Lemma von Zorn läßt sich anwenden. Der Fall endlicher J in (1.2) ist für uns allerdings meist ausreichend.

(1.3) Satz. *Folgende Aussagen über einen A-Modul M sind äquivalent:*

(1) *M ist Summe einer Familie einfacher Untermoduln.*
(2) *M ist direkte Summe einer Familie einfacher Untermoduln.*
(3) *Jeder Untermodul N von M ist direkter Summand in M.*

BEWEIS. (1) $\Rightarrow$ (2) und (1) $\Rightarrow$ (3) wurde in (1.2) gezeigt, und (2) $\Rightarrow$ (1) ist trivial.
(3) $\Rightarrow$ (1). Wir zeigen zunächst, daß jeder von Null verschiedene Untermodul F einen einfachen Untermodul enthält. Sei $0 \neq x \in F$. Wir betrachten die Menge aller Untermoduln F' von F, die x nicht enthalten. Diese Menge enthält den Nullmodul, ist also nicht leer. Nach dem Zornschen Lemma gibt es in ihr einen maximalen Untermodul F_0. Nach Voraussetzung gibt es eine Zerlegung $F_0 \oplus F^* = M$. Wir setzen $F_1 = F^* \cap F$. Aus $F_0 \cap F^* = 0$ folgt $F_0 \cap F_1 = 0$. Ist $y = y_0 + y_1 \in F$ die Zerlegung mit $y_0 \in F_0$ und $y_1 \in F^*$, so ist $y_1 = y - y_0 \in F$, also $y_1 \in F^* \cap F = F_1$. Folglich ist $F = F_0 \oplus F_1$. Wir behaupten: F_1 ist einfach. Andernfalls gäbe es nach Voraussetzung eine Zerlegung $F_1 = F_2 \oplus F_3$ mit von Null verschiedenen F_2 und F_3. Aus $F = F_0 \oplus F_2 \oplus F_3$ folgt $x \notin F_0 \oplus F_2$ oder $x \notin F_0 \oplus F_3$, da andernfalls $x \in (F_0 \oplus F_2) \cap (F_0 \oplus F_3) = F_0$ wäre. Das widerspricht aber der Maximalität von F_0. Damit ist die Einfachheit von F_1 gezeigt.

Sei nun M_0 der Untermodul von M, der von allen einfachen Untermoduln erzeugt wird. Wäre $M_0 \neq M$, so gäbe es eine Zerlegung $M = M_0 \oplus M_1$ und einen einfachen Untermodul in M_1, im Widerspruch zur Definition von M_0. □

Ein A-Modul, für den eine der Eigenschaften (1) – (3) aus (1.3) gilt, heißt *halbeinfach*.

(1.4) Satz. *Untermoduln und Faktormoduln eines halbeinfachen Moduls sind wieder halbeinfach.*

BEWEIS. Sei M halbeinfach und $N \subset M$. Ist $F \subset N$ Untermodul, so gibt es eine Zerlegung $M = F \oplus E$. Wir setzen $F' = N \cap E$ und haben wie im Beweis des vorigen Satzes $N = F \oplus F'$. Damit ist für N die Eigenschaft (1.3.3) nachgewiesen. □

Ein Modul über einem Körper K ist ein Vektorraum. Ein einfacher K-Modul ist ein eindimensionaler Vektorraum. Jeder Vektorraum ist also ein halbeinfacher K-Modul.

(1.5) Satz. *Der Modul M besitze direkte Zerlegungen*

$$M = U_1 \oplus \cdots \oplus U_m = V_1 \oplus \cdots \oplus V_n$$

in einfache Moduln U_i und V_j. Dann ist $m = n$, und mit einer Permutation σ von $\{1, \ldots, n\}$ gilt $U_j \cong V_{\sigma(j)}$.

BEWEIS. Wir setzen $M_j = \bigoplus_{i>j} U_i$. Dann gilt $M = M_0 \supset M_1 \supset \ldots \supset M_m = 0$ und $M_{j-1}/M_j \cong U_j$. Wir haben damit eine Kompositionsreihe, und die Behauptung folgt aus dem Satz von Jordan-Hölder. □

(1.6) Notiz. *Sei M Summe einfacher Untermoduln $(M_j \mid j \in J)$. Dann ist jeder einfache Untermodul U von M zu einem M_j isomorph.*

BEWEIS. Nach (1.3) gibt es eine Projektion $p\colon M \to U$. Ist U zu keinem M_j isomorph, so ist die Einschränkung von p auf M_j nach (1.1) die Nullabbildung, also p selbst die Nullabbildung. □

Sei $\mathrm{Irr}(A)$ ein vollständiges System paarweise nichtisomorpher einfacher A-Moduln. Für $W \in \mathrm{Irr}(A)$ und einen halbeinfachen Modul M bezeichne $M(W)$ die Summe der zu W isomorphen Untermoduln von M. Wir nennen $M(W)$ den *W-isotypischen* Anteil von M. Es gilt die *isotypische Zerlegung*:

(1.7) Notiz. *Jeder halbeinfache A-Modul ist direkte Summe seiner isotypischen Anteile.*

Beweis. Er ist sicher die Summe dieser Anteile. Aus (1.6) folgt, daß ein isotypischer Anteil mit der Summe der weiteren den Schnitt Null hat, weshalb die Summe direkt ist. □

Wir beschreiben die Endomorphismenringe halbeinfacher Moduln, falls sie direkte Summe von endlich vielen einfachen sind. Sei M direkte Summe von Untermoduln $M_1, \ldots, M_n$. Jeder Modul M_j sei direkte Summe von einfachen Moduln, die zu einem festen S_j isomorph sind. Für $i \neq j$ sei $S_i \ncong S_j$. Ein Endomorphismus f von M bildet nach dem Schurschen Lemma jeweils M_j nach M_j ab; sei $f_j \colon M_j \to M_j$ die dadurch induzierte Einschränkung. Die Abbildung

$$\mathbf{(1.8)} \qquad \mathrm{End}(M) \to \prod_{j=1}^{n} \mathrm{End}(M_j), \quad f \mapsto (f_j)$$

ist offenbar ein Isomorphismus von Ringen. Die Struktur von $\mathrm{End}(M_j)$ wird im folgenden Satz bestimmt.

(1.9) Satz. *Sei $M = S_1 \oplus \cdots \oplus S_k$ direkte Summe von zu S isomorphen einfachen Moduln S_j. Sei $D = \mathrm{End}(S)$ der zu S gehörende Divisionsring. Dann ist $\mathrm{End}(M)$ isomorph zum Ring der (k,k)-Matrizen $M_k(D)$.*

Beweis. Wir wählen einen Isomorphismus $M \cong S^k$. Es genügt, $\mathrm{End}(S^k)$ zu beschreiben. Seien $i_j \colon S \to S^k$ und $p_j \colon S^k \to S$ die Inklusion des j-ten und die Projektion auf den j-ten Summanden. Einem $f \in \mathrm{End}(S^k)$ wird die Matrix $(f_{\mu\nu}) \in M_k(D)$ mit $f_{\mu\nu} = p_\mu f i_\nu$ zugeordnet. Diese Zuordnung ist der behauptete Isomorphismus. □

Wir betrachten eine Inklusion $A \subset B$ von halbeinfachen Ringen. Durch Skalarerweiterung wird aus einem A-Modul M ein B-Modul $B \otimes_A M$. Dieser Modul wird auch der induzierte Modul $\mathrm{ind}_A^B M$ genannt. Aus einem B-Modul wird durch Restriktion der Skalarmultiplikation auf A ein A-Modul $\mathrm{res}_A^B N$. Für B-Moduln N und A-Moduln M gilt die kanonische Adjunktionsisomorphie

$$\mathrm{Hom}_B(\mathrm{ind}_A^B M, N) \cong \mathrm{Hom}_A(M, \mathrm{res}_A^B N)$$

Wir haben eine Inklusion von A-Moduln $M \to \mathrm{res}(\, {}_A B \otimes_A M)$, $x \mapsto 1 \otimes x$. Da M als halbeinfacher A-Modul projektiv ist, so ist $\otimes_A M$ ein exakter Funktor. Sei M ein einfacher A-Modul. Wir zerlegen $B \otimes_A M$ in einfache Moduln $B \otimes_A M = \bigoplus_j N_j$. Diese Zerlegung restringieren wir auf A und sehen aus (1.6):

(1.10) Satz. *Sei $A \subset B$ eine Inklusion von halbeinfachen Ringen. Zu jedem einfachen A-Modul M gibt es einen einfachen B-Modul N, so daß M isomorph zu einem direkten Summanden von $\operatorname{res}_A^B N$ ist.* □

Sei $A \subset B$ eine Inklusion von endlichdimensionalen halbeinfachen Algebren über dem Körper K. Ein einfacher B-Modul N wird dann als A-Modul in eine endliche direkte Summe $\bigoplus_j m_j M_j$ paarweise nichtisomorpher einfacher A-Moduln zerlegt. Die Art und Weise, wie sich einfache B-Moduln bei Restriktion auf A zerlegen, ist eine wichtige Invariante der Inklusion $A \subset B$. Die Situation wird manchmal im sogenannten *Bratteli-Diagramm* notiert. Das Bratteli-Diagramm ist ein Graph mit den Eckenmengen $\operatorname{Iso}(B)$ und $\operatorname{Iso}(A)$. Eine Ecke N in $\operatorname{Iso}(B)$ wird durch m Kanten mit der Ecke $M \in \operatorname{Iso}(A)$ verbunden, wenn in $\operatorname{res}_A^B N$ genau m Summanden M auftreten. Wir werden später untersuchen, inwiefern $A \subset B$ durch das Bratteli-Diagramm bestimmt ist.

2 Halbeinfache Ringe

Ein Ring A heißt *halbeinfach*, wenn jeder A-Linksmodul halbeinfach ist.

(2.1) Satz. *Ein Ring A ist genau dann halbeinfach, wenn der linksreguläre Modul A halbeinfach ist.*

Beweis. Sei der linksreguläre Modul halbeinfach. Ein beliebiger Modul ist Quotient eines freien. Ein freier Modul ist aber die direkte Summe von Linksregulären. Nun wende man (1.4) an. □

Die Untermoduln des linksregulären Moduls sind die Linksideale. Ein solcher Modul ist genau dann einfach, wenn das Ideal minimal ist, d. h. außer dem Nullideal kein echt kleineres enthält.

Sei A ein halbeinfacher Ring. Zu jedem einfachen Linksideal L betrachten wir die Summe $A(L)$ aller zu L isomorphen einfachen Linksideale, den *L-isotypischen Bestandteil* von A. Sei $\operatorname{Iso}(A)$ ein vollständiges System paarweise nichtisomorpher einfacher Linksideale. Nach (1.7) ist $A = \bigoplus A(L)$, zunächst als Zerlegung des linksregulären Moduls.

(2.2) Satz. *Sei A ein halbeinfacher Ring. Dann gilt:*

(1) $\operatorname{Iso}(A)$ *ist eine endliche Menge.*
(2) *Für jedes $L \in \operatorname{Iso}(A)$ ist $A(L)$ ein zweiseitiges Ideal.*
(3) *A ist direkte Summe der $A(L)$ für $L \in \operatorname{Iso}(A)$ und als Ring das Produkt der Ringe $A(L)$.*

Beweis. Wegen III(2.3) müssen wir nur zeigen: $A(L)A(M) = 0$ für $M \neq L$ und $A(L)A(L) \subset A(L)$. Das Zweite ist aber klar, da $A(L)$ ein Linksideal ist. Seien L und M nichtisomorphe einfache Linksideale. Wir zeigen: $LM = 0$. Es ist LM ein Untermodul von M. Also gilt entweder $LM = 0$ oder $LM = M$, da M einfach ist. Angenommen $LM = M$. Wir wählen $m \in M$, so daß $Lm \neq 0$ ist. Dann ist $L \to M$, $l \mapsto lm$ nach dem Schurschen Lemma ein Isomorphismus. Widerspruch.

Aus dem Gezeigten folgt $A(L_1)A(L_2) = 0$, sofern L_1, L_2 verschiedene Elemente aus $\mathrm{Iso}(A)$ sind. □

(2.3) Satz. *Sei A halbeinfach und seien L, M isomorphe einfache Linksideale. Dann gibt es $\alpha \in A$ mit $L\alpha = M$.*

Beweis. Da A halbeinfach ist, ist L direkter Summand. Es gibt also einen A-linearen Projektionsoperator $f\colon A \to L$. Sei $s\colon L \to M$ ein Isomorphismus. Die Verkettung

$$h\colon A \xrightarrow{f} L \xrightarrow{s} M \xrightarrow{\subset} A$$

ist ein Endomorphismus h des A-Moduls A. Es gilt für $x \in A$

$$h(x) = h(x \cdot 1) = x \cdot h(1) = x \cdot \alpha, \qquad \alpha = h(1).$$

Für $x \in L$ gilt $h(x) = s(x) = x \cdot \alpha$, da f ein Projektionsoperator ist. □

(2.4) Satz. *Sei B ein zweiseitiges Ideal in dem halbeinfachen Ring A. Dann ist B ein Produkt von isotypischen Bestandteilen von A.*

Beweis. Da B ein Untermodul des linksregulären ist, so gibt es in B einfache Untermoduln L. Ist M ein einfacher Untermodul von $A(L)$, so ist nach (2.3) $M = L\alpha$. Da B auch ein Rechtsideal ist, so ist $M \subset B$. Also ist $A(L) \subset B$. □

(2.5) Folgerung. *Für einen halbeinfachen Ring sind äquivalent:*
(1) *Alle Linksideale sind isomorph.*
(2) *A hat nur die zweiseitigen Ideale A und 0.* □

Eine Ring A heiße *einfach*, wenn er halbeinfach ist und 0 und A die einzigen zweiseitigen Ideale sind.

(2.6) Satz. *Die isotypischen Bestandteile $A(L)$ eines halbeinfachen Ringes A sind einfache Ringe.*

Beweis. Sei U ein einfacher A-Untermodul von $A(L)$. Sei $0 \neq V \subset U$ ein $A(L)$-Untermodul. Wegen $A(L)A(M) = 0$ für $L \ncong M$ ist V auch ein A-Untermodul. Also ist $V = U$ und U auch als $A(L)$-Modul einfach. Damit ist $A(L)$ als linksregulärer $A(L)$-Modul direkte Summe einfacher $A(L)$-Moduln, die zudem alle isomorph sind. □

(2.7) Satz. *Ein Produkt $A = A_1 \times \cdots \times A_r$ halbeinfacher Ringe A_j ist halbeinfach.*

Beweis. Wir schreiben A_j als Summe einfacher A_j-Linksideale; vermöge der Projektion $A \to A_j$ sind diese dann einfache A-Moduln. □

(2.8) Satz. *Sei A ein einfacher Ring. Dann gibt es einen Divisionsring D und eine natürliche Zahl n, so daß A zum Matrizenring $M_n(D)$ isomorph ist.*

Beweis. Wir wissen nach (2.5), daß A direkte Summe einfacher Linksideale ist, die alle zu einem festen A-Modul S isomorph sind. Die Zuordnung

$$A \to \mathrm{Hom}_A(A, A), \quad x \mapsto (r_x\colon z \mapsto zx)$$

ist ein Antiisomorphismus von Ringen. Wir wissen nach (2.9), daß $\mathrm{Hom}_A(A,A)$ zu $M_n(\Delta)$ mit $\Delta = \mathrm{End}(S)$ isomorph ist. Also ist A isomorph zum Gegenring $M_n(\Delta)^\circ$. Man bestätigt, daß der Übergang zur transponierten Matrix ein Isomorphismus $M_n(\Delta)^\circ \cong M_n(\Delta^\circ)$ ist. Also kann $D = \Delta^\circ$ gewählt werden. □

Wir tragen jetzt die Resultate zum *Klassifikationssatz von Wedderburn* für halbeinfache Ringe zusammen:

(2.9) Satz. *Sei A ein halbeinfacher Ring. Dann ist A isomorph zu einem Produkt*

$$M_{n(1)}(D_1) \times \cdots \times M_{n(r)}(D_r)$$

von Matrixringen über Schiefkörpern D_j. Das System von Paaren $(n(j), D_j)$ ist durch A bis auf Permutation bestimmt. Jeder Ring dieser Form ist halbeinfach.

Beweis. Wegen (1.6) und (2.7) ist jedes Produkt von Matrixringen über Schiefkörpern halbeinfach. Sei A halbeinfach. Nach (2.2), (2.6) und (2.8) ist A Produkt von Matrixringen über Schiefkörpern. In einem Produkt von einfachen Ringen sind die einfachen Faktoren die isotypischen Bestandteile und als solche durch das Produkt bestimmt. Es bleibt zu zeigen: Aus $M_n(D) \cong M_m(E)$ folgt $n = m$ und $D \cong E$. Es ist D° isomorph zum Endomorphismenring eines einfaches $M_n(D)$-Moduls. Es folgt $D \cong E$ und dann $n = m$ mittels (1.6) und dem Satz von Jordan-Hölder. □

Ist ein halbeinfacher Ring gegeben, so besteht natürlich das Problem, die durch (2.9) gegebene Zerlegung explizit zu verstehen, insbesondere die Schiefkörper D_j und die Ränge n_j zu bestimmen.

Halbeinfache Ringe A treten häufig als endlichdimensionale Algebren über Körpern K auf; das bedeutet, daß K ein Unterring im Zentrum von A ist. Ist K algebraisch abgeschlossen, so sind alle D_j in(2.9) gleich K:

(2.10) Satz. *Eine endlichdimensionale Divisionsalgebra D über einem algebraisch abgeschlossenen Körper ist gleich K.*

Beweis. Die Linkstranslation $l_a\colon D \to D$, $x \mapsto ax$ ist K-linear. Da K algebraisch abgeschlossen ist, gibt es einen Eigenvektor v von l_a, etwa zum Eigenwert $\lambda \in K$. Die Gleichung $av = \lambda v$ liefert nach Rechtsmultiplikation mit v^{-1} die Gleichheit $a = \lambda$, d. h. jedes $a \in D$ liegt schon in K. □

Ist A eine halbeinfache endlichdimensionale Algebra über dem algebraisch abgeschlossenen Körper K und sind $V_1, \ldots, V_r$ die verschiedenen einfachen A-Moduln, so gilt wegen (2.9) und (2.10) die Gleichheit

$$\textbf{(2.11)} \qquad \dim_k = \sum_{j=1}^{k} (\dim_k V_j)^2.$$

Damit kann man manchmal feststellen, ob man alle einfachen Moduln gefunden hat.

Eine Matrix aus $M_n(D)$, die mit allen Matrizen daraus vertauschbar ist, muß notgedrungen ein Vielfaches der Einheitsmatrix sein. Das Zentrum eines Schiefkörpers ist ein Körper. Das Zentrum eines halbeinfachen Ringes ist also ein Produkt von Körpern. Da $M_n(D)$ für $n > 1$ nicht kommutativ ist, sehen wir aus dem Struktursatz:

(2.12) Folgerung. *Ein kommutativer Ring ist genau dann halbeinfach, wenn er endliches Produkt von Körpern ist. Er ist genau dann einfach, wenn er ein Körper ist.* □

Im Vorangehenden haben wir immer mit Linksmoduln gearbeitet. Deshalb müßten wir eigentlich von *links-halbeinfachen* Ringen sprechen. Die Ringe $M_n(D)$ sind aber auch rechts-halbeinfach; die Zerlegung des rechtsregulären Moduls in einfache Rechtsideale wird durch Betrachtung der Zeilenvektoren gewonnen. Wir sehen: Ein Ring ist genau dann links-halbeinfach, wenn er rechts-halbeinfach ist.

3 Tensorprodukte von Algebren

Ein einfacher Ring ist isomorph zu einem Matrizenring $M_n(D)$ über einem Schiefkörper D. Das Zentrum eines Ringes A bezeichnen wir mit $Z(A)$. Für jeden Ring A gilt:

(3.1) Notiz. *Die Zuordnung $\lambda \mapsto \lambda \cdot I_n$ liefert einen Isomorphismus $Z(A) \cong Z(M_n(A))$.* □

Das Zentrum von D ist ein Körper K. Wir können deshalb $M_n(D)$ als K-Algebra auffassen. Es ist ratsam, die Algebren nach ihrem Zentrum zu sortieren.

Wir betrachten im folgenden endlichdimensionale K-Algebren A. Durch $\lambda \mapsto \lambda \cdot 1$ fassen wir K als Unterkörper des Zentrums $Z(A)$ auf. Ist $K = Z(A)$, so heißt A eine *zentrale* K-Algebra. Unbezeichnete Tensorprodukte seien im folgenden über K gebildet. Sind $A' \subset A$ und $B' \subset B$ Unteralgebren, so fassen wir $A' \otimes B'$ kanonisch als Unteralgebra von $A \otimes B$ auf. Wir haben injektive Homomorphismen von K-Algebren

$$A \to A \otimes B,\ a \mapsto a \otimes 1, \qquad B \to A \otimes B,\ b \mapsto 1 \otimes b,$$

die gelegentlich als Inklusionen angesehen werden.

Für eine Teilmenge $X \subset A$ definieren wir den *Zentralisator von X in A* durch

$$Z_A(X) = \{z \in A \mid zx = xz \quad \text{für alle } x \in X\}.$$

Das ist eine Unteralgebra von A. Falls X selbst eine Unteralgebra ist, so gilt

$$Z \cap Z_A(X) = Z(X).$$

(3.2) Notiz. *Seien $A' \subset A$ und $B' \subset B$ Unteralgebren, so gilt*

$$Z_{A \otimes B}(A' \otimes B') = Z_A(A') \otimes Z_B(B').$$

BEWEIS. Die eine Inklusion $Z_A(A') \otimes Z_B(B') \subset Z_{A\otimes B}(A' \otimes B')$ ist aus den Definitionen unmittelbar klar.

Ist $b_1, \ldots, b_n$ eine K-Basis von B, so ist $1\otimes b_1, \ldots, 1\otimes b_n$ eine A-Basis von $A\otimes B$ bezüglich der linksregulären Modulstruktur $u \cdot (a \otimes b) := ua \otimes b$. Ist $\Sigma_j a_j \otimes b_j \in Z_{A\otimes B}(A' \otimes B')$, so gilt für alle $a \in A'$ die Gleichheit $\Sigma_j aa_j \otimes b_j = \Sigma a_j a \otimes b_j$, und durch Koeffizientenvergleich folgt $a_j \in Z_A(A')$. Ebenso argumentieren wir mit einer K-Basis von A und erhalten in

$$Z_{A\otimes B}(A' \otimes B') \subset (A \otimes Z_B(B')) \cap (Z_A(A') \otimes B) = Z_A(A') \otimes Z_B(B')$$

die andere Inklusion. □

(3.3) Folgerung. *Das Tensorprodukt zentraler K-Algebren ist wieder eine zentrale K-Algebra.* □

(3.4) Satz. *Sei A eine zentrale einfache und B eine einfache Algebra. Dann ist $A \otimes B$ einfach.*

BEWEIS. Sei $I \neq 0$ ein Ideal von $A \otimes B$. Wir haben $I = A \otimes B$ zu zeigen.

Angenommen I enthält ein Element der Form $a \otimes b \neq 0$. Da A einfach ist, so ist das von a erzeugte zweiseitige Ideal gleich A. Es gilt deshalb eine Darstellung

$$1 = \sum a_i a a_i', \quad a_i, a_i' \in A.$$

Also ist

$$\Sigma(a_i \otimes 1)(a \otimes b)(a_i' \otimes 1) = 1 \otimes b$$

ein Element von I. Indem wir dasselbe Argument auf $1 \otimes b$ anwenden, sehen wir $1 \otimes 1 \in I$.

Im allgemeinen Fall wählen wir in I ein Element der Form

$$0 \neq x = a_1 \otimes b_1 + \cdots + a_k \otimes b_k, \quad a_j \in A,\ b_j \in B$$

mit möglichst kleinem k. Dann sind die $b_1, \ldots, b_k$ K-linear unabhängig, da eine lineare Relation zu einer kürzeren Darstellung führen würde. Es ist $a_k \neq 0$, und wir können wie im Anfang des Beweises ein Element dieser Form finden, für das $a_k = 1$ ist.

Angenommen $k > 1$. Dann sind a_{k-1} und a_k über K linear unabhängig, denn eine Relation $a_{k-1} = \lambda a_k$ würde wegen $a_{k-1} \otimes b_{k-1} + a_k \otimes b_k = a_k \otimes (\lambda b_{k-1} + b_k)$ ein kürzeres Element in I liefern.

Da A zentral ist und $a_k = 1$, würde aus $a_{k-1} \in Z(A)$ eine lineare Relation der Form $a_{k-1} = \lambda a_k$ folgen. Also gibt es $a \in A$ mit $aa_{k-1} - a_{k-1}a \neq 0$. Das Element

$$(a \otimes 1)x - x(a \otimes 1) = (aa_1 - a_1 a) \otimes b_1 + \cdots + (aa_{k-1} - a_{k-1}a) \otimes b_{k-1}$$

liegt in I. Es ist ungleich Null, da die b_j K-linear unabhängig, also die $1 \otimes b_j$ A-linear unabhängig sind, und der Koeffizient von b_{k-1} von Null verschieden ist. □

Sei A eine K-Algebra und A^0 ihre Gegenalgebra. Wir erhalten einen Homomorphismus von Algebren

(3.5) $$\varphi\colon A \otimes A^0 \to \mathrm{End}_K(A),$$

indem wir $a \otimes b \in A \otimes A^0$ den Endomorphismus $\psi_{a,b}\colon x \mapsto axb$ zuordnen.

(3.6) Inversionssatz. *Sei A einfach und zentral. Dann ist φ ein Isomorphismus. Es gilt $Z_{A\otimes A^0}(A \otimes 1) = 1 \otimes A^0$, $Z_{A\otimes A^0}(1 \otimes A^0) = A \otimes 1$.*

Beweis. Nach (3.4) ist $A \otimes A^0$ einfach. Da φ nicht die Nullabbildung ist, so ist der Kern von φ als zweiseitiges Ideal das Nullideal. Aus Dimensionsgründen ist φ bijektiv. Die Aussagen über den Zentralisator folgen aus (3.2). □

(3.7) Notiz. *Die tautologische Abbildung*

$$T\colon \mathrm{Hom}_A(M, M') \otimes \mathrm{Hom}_B(N, N') to \mathrm{Hom}_{A\otimes B}(M \otimes N, M' \otimes N')$$

ist ein Isomorphismus, wenn M ein endlich erzeugter freier A-Modul und N ein endlich erzeugter freier B-Modul ist.

Beweis. Wir betrachten zunächst den Fall $M = A$ und $N = B$. Wir haben kanonische Isomorphismen

$$\varepsilon\colon \mathrm{Hom}_A(A, M') \to M', \quad \varphi \mapsto \varphi(1)$$

und ebenso für B und N'. Damit ist das Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_A(A, M') \otimes \mathrm{Hom}_B(B, N') & \xrightarrow{T} & \mathrm{Hom}_{A\otimes B}(A \otimes B, M' \otimes N') \\ \downarrow{\scriptstyle \varepsilon \otimes \varepsilon} & & \downarrow{\scriptstyle \varepsilon} \\ M' \otimes N' & \xrightarrow{\mathrm{id}} & M' \otimes N' \end{array}$$

kommutativ. Das beweist die Notiz in diesem Fall. Der allgemeine Fall folgt aus der Verträglichkeit von T mit endlichen direkten Summen in den Variablen M und N. □

Die tautologische Abbildung liefert speziell einen Homomorphismus von Endomorphismenalgebren

$$T\colon \mathrm{End}_A(M) \otimes_K \mathrm{End}_A(N) \to \mathrm{End}_{A\otimes B}(M \otimes N).$$

Im Fall $M = A^m$ und $N = B^n$ ist diese Abbildung nach (3.7) ein Isomorphismus. Er läßt sich dann in Matrizenform übersetzen und liefert:

(3.8) Notiz. *Es gibt einen kanonischen Isomorphismus von Algebren*

$$M_m(A) \otimes_K M_n(B) \cong M_{mn}(A \otimes_K B).$$

Er wirft $(a_{ij}) \otimes (b_{kl})$ auf $(c_{ik,jl})$ mit $c_{ik,jl} = a_{ij} \otimes b_{kl}$. □

Im Fall $m = 1$ erhalten wir aus (3.8) speziell

$$A \otimes_K M_n(B) \cong M_n(A \otimes_K B). \tag{3.9}$$

Ist $L|K$ eine Körpererweiterung und C eine K-Algebra, so ist $L \otimes_K C$ eine L-Algebra, denn $L \otimes 1$ liegt offenbar im Zentrum. Der Übergang von C zu $L \otimes_K C$ heißt *Skalarerweiterung*. Im Lichte von (3.9) gilt kanonisch $L \otimes_K M_n(B) \cong M_n(L \otimes_K B)$.

4 Die Hauptsätze.

Der folgende Satz ist als Satz von *Skolem-Noether* bekannt.

(4.1) Konjugationssatz. *Sei A eine zentrale einfache K-Algebra und seien $\sigma, \tau\colon B \to A$ zwei Homomorphismen der einfachen Algebra B nach A. Dann gibt es ein Element $g \in A$ mit $\tau(b) = g^{-1}\sigma(b)g$ für alle $b \in B$.*

Beweis. Wir betrachten zunächst den Fall $A = \mathrm{End}_K(V)$ für einen Vektorraum V. Dann ist V wie üblich durch Evaluation ein A-Modul. Wir benutzen σ und τ dazu, V zu B-Moduln V_σ und V_τ zu machen. Da B einfach ist, gibt es bis auf Isomorphie nur einen einfachen B-Modul. Aus Dimensionsgründen sind V_σ und V_τ direkte Summe gleichvieler einfacher B-Moduln und deshalb isomorph. Ein Isomorphismus $f\colon V_\tau \to V_\sigma$ erfüllt für alle $b \in B$ und $v \in V$ die Gleichung $f(\tau(b)v) = \sigma(b)f(v)$ oder $T(b) = f^{-1}\sigma(b)f$.

Im allgemeinen Fall betrachten wir

$$\sigma \otimes \mathrm{id},\ \tau \otimes \mathrm{id}\colon B \otimes A^0 \to A \otimes A^0 \cong \mathrm{End}_K(A),$$

wobei wir (1.6) verwenden. Nach (1.4) ist $B \otimes A^0$ einfach. Der Beweisanfang liefert ein $f \in A \otimes A^0$, so daß immer

$$\tau(b) \otimes a = f^{-1}(\sigma(b) \otimes a)f$$

gilt. Wir setzen $b = 1$ und stellen fest, daß f mit allen Elementen aus $1 \otimes A^0$ vertauschbar ist. Nach (1.6) hat deshalb f die Form $g \otimes 1 \in A \otimes 1$. Wir setzen nun $a = 1$ und erhalten $\tau(b) = g^{-1}\sigma(b)g$ für alle $b \in B$ wie gewünscht. □

(4.2) Folgerung *Jeder Automorphismus einer zentralen einfachen Algebra ist ein innerer Automorphismus. Isomorphe einfache Unteralgebren sind konjugiert.* □

(4.3) Zentralisatorsatz. *Sei A eine zentrale einfache K-Algebra und B eine einfache Unteralgebra mit Zentrum $L \supset K$. Sei $C = Z_A(B)$ der Zentralisator von B in A. Dann gilt:*

(1) *C ist einfach.*
(2) $\dim_K(A) = \dim_K(B)\dim_K(C)$.
(3) *Ist $L = K$, so ist $A \cong B \otimes_K C$.*

BEWEIS. (1) Wir wissen, daß $T = B \otimes A^0$ einfach ist. Wir betrachten A als T-Modul vermöge

$$(b \otimes a)x = bxa, \quad b \in B,\ x \in A,\ a \in A^0.$$

Die T-linearen Endomorphismen von A sind die Elemente von $\mathrm{End}_K(A) \cong A \otimes A^0$, die mit $B \otimes A^0$ kommutieren; also nach (3.4)

$$\mathrm{End}_T(A) \cong Z_{A\otimes A^0}(B \otimes A^0) = Z_A(B) \otimes Z_{A^0}(A^0) = C \otimes K.$$

Da A als T-Modul direkte Summe isomorpher einfacher ist, etwa $A \cong M^k$, so ist

$$C \cong \mathrm{End}_T(A) \cong M_k(D), \qquad D = \mathrm{End}_T(M)$$

eine einfache Algebra.

(2) Wir betrachten die K-Dimensionen $a, b, c, \ldots$ von $A, B, C, \ldots$. Es gelten:

$$\begin{array}{ll} a = mk & A \cong M^k \\ t = ba & T \cong B \otimes A^0 \\ m = sd & M \cong D^s \\ t = s^2 d & T \cong \mathrm{End}_D(M)^0 \cong M_s(D) \\ c = k^2 d & C \cong M_k(D). \end{array}$$

Durch Elimination folgt

$$c = k^2 d = \frac{a^2}{m^2} d = \frac{a^2}{s^2 d^2} d = \frac{a^2}{t} = \frac{a^2}{ab} = \frac{a}{b}$$

wie gewünscht.

(3) Die Abbildung $B \otimes C \to A$, $\beta \otimes \gamma \mapsto \beta\gamma$ ist ein Homomorphismus von Algebren; sie ist injektiv, weil $B \otimes C$ einfach ist, und surjektiv aus Dimensionsgründen. □

(4.4) Satz vom doppelten Zentralisator. *Sei B einfache Unteralgebra der zentralen einfachen Algebra A. Dann gilt $Z_A(Z_A(B)) = B$. Die Algebren B und $Z_A(B)$ haben dasselbe Zentrum.*

BEWEIS. Nach Definition von $Z_A(B)$ sind die Elemente von B und $Z_A(B)$ vertauschbar, so daß $B \subset Z_A(Z_A(B))$ ist. Aus der Dimensionsformel (2.3.2) folgt die Gleichheit.

Das Zentrum von $Z_A(B)$ ist danach $Z_A(B) \cap Z_A(Z_A(B)) = Z_A(B) \cup B$, und letzteres ist das Zentrum von B. □

Wir bemerken, daß (2.3.2) insbesondere sagt:

(4.5) Folgerung. *Die Dimension einer einfachen Unteralgebra B einer zentralen einfachen Algebra teilt* $\dim A$. □

(4.6) Satz vom maximalen Körper. *Sei A eine Dimensionsalgebra mit Zentrum K und B ein maximaler Unterkörper von A. Dann gilt:*

(1) $Z_A(B) = L$.
(2) $\dim_K A = (\dim_K B)^2$.
(3) $B \otimes_K A \cong M_b(B), \quad b = \dim_K B$.

BEWEIS. (1) Da B kommutativ ist, so ist $B \subset Z_A(B)$. Wäre $x \in Z_A(B) \setminus B$, so wäre $B[x]$ ein echt größerer Unterkörper.
(2) Nach (2.3.2) ist $\dim A = \dim B \dim Z_A(B) = b^2$.
(3) Im Beweis von (2.3) für diese Situation ist A ein einfacher $T = B \otimes_K A^0$-Modul, also $k = 1$, $B \cong D$, $D = \mathrm{End}_{B\otimes A^0}(A) = B$, $T \cong M_s(B)$ und aus Dimensionsgründen, da $\dim_B(T) = \dim_B(B \otimes A^0) = b^2$, $s = b$. □

Sei A eine zentrale einfache K-Algebra. Eine Körpererweiterung $L|K$ heißt *Zerfällungskörper* von A, wenn $L \otimes_K A$ ein Matrixring über L ist. Aus dem letzten Satz entnehmen wir: Ein maximaler Unterkörper einer Divisionsalgebra D ist ein Zerfällungskörper von D. Ist $A = M_r(D)$, so ist wegen $L \otimes_K M_r(D) \cong M_r(K \otimes_K D)$ ein Zerfällungskörper von D auch einer von A.

(4.7) Beispiel. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong M_2(\mathbb{C})$. ◇

5 Anwendungen

Der folgende Satz ist ein berühmter *Satz von Wedderburn*:

(5.1) Satz. *Ein Schiefkörper D mit endlich vielen Elementen ist kommutativ.*

BEWEIS. Sei K das Zentrum von D. Jedes Element von D ist in einem maximalen Körper enthalten. Nach (4.6) haben alle diese Körper dieselbe Dimension über K und sind deshalb nach der Strukturtheorie der endlichen Körper isomorph. Isomorphe Unterkörper sind nach dem Satz von Skolem-Noether konjugiert. Insgesamt ergibt sich die folgende gruppentheoretische Situation, wenn D nicht kommutativ ist: Die multiplikative endliche Gruppe $G = D^*$ ist Vereinigung der Konjugierten einer echten Untergruppe $H = L^*$. Das kann aber nicht sein. Es gibt nämlich $|G/NH|$ zu H konjugierte Untergruppen. Da diese alle das neutrale Element gemeinsam haben, liefern sie höchstens

$$|G/NH|(|H| - 1|) + 1$$

Elemente, und diese Zahl ist kleiner als $|G|$. □

Die Divisionsalgebren über $\mathbb{R}$ werden durch den *Satz von Frobenius* geliefert.

(5.2) Satz. *Eine endlichdimensionale Divisionsalgebra D über $\mathbb{R}$ ist isomorph zu $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$.*

BEWEIS. Ist D kommutativ, so ist $D = \mathbb{R}, \mathbb{C}$. Ist D nicht kommutativ, so ist $Z(D) = \mathbb{R}$, da eine Divisionsalgebra über $\mathbb{C}$ gleich $\mathbb{C}$ ist, wie wir früher gesehen haben.

Im nichtkommutativen Fall sind also die maximalen kommutativen Körper in D als Erweiterungen von $\mathbb{R}$ gleich $\mathbb{C}$. Folglich ist nach (4.6) $\dim_{\mathbb{R}} D = 4$.

Wir untersuchen daher zunächst überhaupt vierdimensionale zentrale Divisionsalgebren D über einem Körper K der Charakteristik $\neq 2$.

Sei $D \supset L \supset K$, $L|K$ quadratische Erweiterung. Da Char $K \neq 2$ gibt es $e_1 \in L \setminus K$ mit $e_1^2 = a \in K$. Der Automorphismus $e_1 \mapsto -e_1$ von L ist nach Skolem-Noether durch Konjugation mit einem e_2 gegeben, d. h. es gibt e_2 mit $e_2 e_1 e_2^{-1} = -e_1$ oder $e_2 e_1 = -e_1 e_2$. Es ist dann $e_2 \notin L$ und folglich als L-Vektorraum $D = L \oplus L e_2$. Das Element e_2^2 ist mit e_1 vertauschbar ($e_2^2 e_1 = -e_2 e_1 e_2 = e_1 e_2^2$), also mit allen Basiselementen von D, also im Zentrum von D enthalten: $e_2^2 = b \in K$. Demnach hat D eine Basis $1, e_1, e_2, e_1 e_2$; die Multiplikationstabelle der Basis ist durch $e_1^2 = a$, $e_2^2 = b$, $e_1 e_2 = -2_2 e_1$ bestimmt. Eine Divisionsalgebra dieser Form heißt *Quaternionenalgebra* $Q(a, b)$.

Im Fall $K = \mathbb{R}$ müssen a und b negativ sein, da andernfalls $x^2 - a$ und $x^2 - b$ nicht irreduzibel wäre. ($L = K[e_1]$). Dann können wir e_1 und e_2 durch

$$i = \frac{e_1}{\sqrt{|a|}}, \qquad j = \frac{e_2}{\sqrt{|b|}}$$

ersetzen und erhalten die klassische Quaternionenalgebra $\mathbb{H} = Q(-1, -1)$. □

Sei A eine zentrale einfache Algebra über K der Dimension n^2 und sei L ein Unterkörper von A der Dimension n. Wir setzen voraus:

(5.3) *$L|K$ ist eine Galois-Erweiterung mit zyklischer Galois-Gruppe G.*

Sei $\sigma \in G$ ein erzeugendes Element. Nach dem Satz von Skolem-Noether ist der Automorphismus σ von L durch Konjugation mit einem Element $e \in A^*$ gegeben:

$$\sigma(\lambda) = e\lambda e^{-1}, \quad l \in L.$$

Da $\sigma^n = \mathrm{id}$ ist, gilt $e^n \in Z_A(L) = L$. Wegen $\sigma(e^n) = e e^n e^{-1} = e^n$ ist e^n in der Fixpunktmenge von G enthalten, liegt also in K; etwa $e^n = a \in K$. Es gilt:

(5.4) *Die Elemente $1, e, \ldots, e^{n-1}$ sind über L linear unabhängig.*

Beweis. Sei

$$r = \lambda_0 + \lambda_1 e + \cdots + \lambda_k e^k = 0$$

eine Relation mit minimalem k. Sei $L = K[\mu]$. Dann ist $\sigma^i \mu \neq \mu$ für $\sigma^i \neq \mathrm{id}$, da μ den Körper L erzeugt. Es folgt

$$\begin{aligned} & (\mu r) - r\mu)e^{-1} \\ = \; & \mu\lambda_0 e^{-1} + \mu\lambda_1 + \mu\lambda_2 e + \cdots + \mu\lambda_k e^{k-1} \\ & \lambda_0\mu e^{-1} - \lambda_1 e\mu e^{-1} - \lambda_2 e^2\mu e^{-1} - \cdots \lambda_k e^k \mu e^{-1} \\ = \; & \lambda_1(\mu - \sigma(\mu)) + \lambda_2(\mu - \sigma^2(\mu))e + \cdots \lambda_k(\mu - \sigma^k(\mu))e^{k-1}, \end{aligned}$$

und das ist eine echte und kürzere Relation.

Damit haben wir also als L-Vektorraum

$$A = L \oplus Le \oplus \cdots \oplus Le^{n-1}.$$

Die Multiplikation wird durch

$$(\lambda e^i)(\mu e^j) = \lambda e^i \mu e^{-i} e^{i+j} = \lambda \sigma^i(\mu) e^{i+j}$$

und $e^n = a \in K$ gegeben.

Aus diesen Daten kann man umgekehrt eine K-Algebra-Struktur auf $L \oplus Le \oplus \cdots \oplus Le^{n-1}$ definieren. Die resultierende Algebra $A = (L|L, \sigma, a)$ heißt eine *zyklische Algebra*. Man überlegt sich, daß eine solche Algebra immer eine zentrale einfache K-Algebra ist.

6 Die Brauer-Gruppe.

Zwei zentrale einfache Algebren A, B über K heißen *ähnlich*, wenn sie zu isomorphen Divisionsalgebren gehören: $A \sim B \Leftrightarrow A \cong M_m(D), \quad B \cong M_n(D)$. Ähnlichkeit ist eine Äquivalenzrelation auf der Menge $Br(K)$ der Isomorphieklassen von zentralen einfachen K-Algebren. In jeder Klasse gibt es genau einen Isomorphietyp einer Divisionsalgebra (definitionsgemäß).

(6.1) Satz. *Das Tensorprodukt von K-Algebren induziert auf $Br(K)$ die Struktur einer kommutativen Gruppe, genannt die* Brauer-Gruppe *von K.*

Beweis. Zunächst einmal ist das Tensorprodukt zentraler einfacher Algebren wieder eine Algebra dieses Types. Sei $A \sim B$, etwa wie oben $A \cong M_m(D), \quad B \cong M_n(D)$. Sei $C = M_p(E)$ und $D \otimes E \cong M_k(F)$. Dann ist

$$A \otimes C \cong M_m(D) \otimes M_p(E) \cong M_{mp}(D \otimes E) \cong M_{mpk}(F), \quad B \otimes C \cong M_{npk}(F),$$

also $A \otimes C \sim B \otimes C$. Folglich ist $\sim$ mit dem Tensorprodukt verträglich und $\otimes$ induziert auf $Br(K)$ eine wohldefinierte Verknüpfung, die offenbar assoziativ und kommutativ ist. Die Existenz des Inversen folgt aus $A \otimes A^0 \cong \mathrm{End}_K(A) \cong M_n(K)$, $n = \dim_K A$. Das neutrale Element wird durch K repräsentiert. □

(6.2) Beispiel. $Br(\mathbb{R}) \cong \mathbb{Z}/2$. Es gibt nur die beiden zentralen Divisionsalgebren $\mathbb{R}$ und $\mathbb{H}$. Es ist $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$ das neutrale Element, also $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong M_4(\mathbb{R})$. Es ist $Br(\mathbb{C})$ trivial. ◇

(6.3) Beispiel. Ist K ein endlicher Körper, so ist $Br(K)$ trivial (Satz 5.1). ◇

12 Artinsche Ringe

1 Halbeinfache artinsche Ringe

Im letzten Kapitel haben wir die halbeinfachen Ringe modultheoretisch behandelt. Wir wollen sie jetzt ringtheoretisch charakterisieren.

(1.1) Notiz. *Ein halbeinfacher Ring ist artinsch.*

Beweis. Sei I ein Linksideal des Ringes. Es ist direkte Summe von einfachen Linksidealen. Nach dem Satz von Jordan-Hölder ist die Anzahl $l(I)$ der einfachen direkten Summanden eindeutig bestimmt. Ist $J \subset I$ ein echter Untermodul, so ist $l(J) < l(I)$. Also kann es keine echt absteigenden unendlichen Idealsequenzen geben. □

Das nächste Lemma wird zu einer genaueren Beschreibung halbeinfacher Ringe gebraucht.

(1.2) Notiz. *Sei $I \neq 0$ ein minimales Linksideal eines Ringes A. Dann ist entweder $I^2 = 0$ oder es gilt $I = Ae$ mit einem Idempotenten e.*

Beweis. Sei $I^2 \neq 0$. Es gibt dann Elemente x, y in I, deren Produkt $yx \neq 0$ ist. Da ein minimales Linksideal ein einfacher Modul ist, so ist deshalb der Homomorphismus $f\colon I \to I$, $a \mapsto ax$ nach dem Schurschen Lemma ein Isomorphismus. Für ein geeignetes $e \in I$ ist somit $x = ex$ und dann auch $ex = e^2x$. Das heißt aber $f(e) = f(e^2)$; und es folgt $e = e^2$, weil f bijektiv ist. Da Ae ein von Null verschiedener Untermodul von I ist, gilt $Ae = I$. □

(1.3) Satz. *Folgende Aussagen über einen artinschen Ring sind äquivalent:*

(1) *A ist halbeinfach.*
(2) *Jedes Linksideal hat die Form Ae mit einem Idempotenten e.*
(3) *Jedes von Null verschiedene zweiseitige Ideal enthält ein von Null verschiedenes Idempotentes.*
(4) *Es gibt kein von Null verschiedenes nilpotentes zweiseitiges Ideal.*
(5) *Es gibt kein von Null verschiedenes nilpotentes Linksideal.*

Beweis. (1) ⇒ (2). Sei $I \subset A$ ein Linksideal. Dann gibt es eine Linksidealzerlegung $A = I \oplus I'$ nach Definition von halbeinfach, und nach (VII.5) ist $I = Ae$ mit einem Idempotenten e.

(2) ⇒ (3) ist klar.

(3) ⇒ (4). Sei I nilpotent. Wäre $0 \neq e \in I$ nilpotent, so würde $e = e^k \in I^k$ für alle $k \in \mathbb{N}$ gelten.

(4) ⇒ (5). Sei I ein nilpotentes Linksideal. Dann ist IA ein zweiseitiges Ideal und wegen $(IA)^n = I^nA$ nilpotent.

(5) ⇒ (1). Sei I ein einfaches Linksideal. Dann ist $I^2 \neq 0$ und nach (1.2) $I = Ae$.

Es gibt also eine Zerlegung $A = Ae \oplus A(1-e)$, d. h. jeder einfache Untermodul ist direkter Summand. Weil A artinsch ist, enthält jeder Untermodul einen einfachen. Wir können also von $A(1-e)$ wiederum einen einfachen direkten Summanden abspalten. Dieser Prozess muß nach endlich vielen Schritten abbrechen, weil A artinsch ist. Folglich ist A direkte Summe einfacher Linksideale. □

Ein Element a eines Ringes heißt *nilpotent*, wenn $a \neq 0$ ist und für ein $n \in \mathbb{N}$ die Relation $a^n = 0$ gilt.

(1.4) Satz. *Ein kommutativer artinscher Ring ist genau dann halbeinfach, wenn er kein nilpotentes Element enthält.*

Beweis. Enthält der Ring A ein nilpotentes Element a, so ist das von a erzeugte Hauptideal Aa wegen der Kommutativität von A nilpotent, also A nach (1.3) nicht halbeinfach. Und umgekehrt. □

In der allgemeinen Ringtheorie heißt ein Ring A *einfach*, wenn er nur die zweiseitigen Ideale 0 und A hat. Wir zeigen, daß ein solcher Ring halbeinfach ist und damit einfach im bisher definierten Sinne, wenn er ein minimales Linksideal I besitzt. In diesem Fall ist nämlich IA ein zweiseitiges Ideal, also gleich A. Es gibt deshalb eine Darstellung

$$1 = x_1a_1 + \cdots + x_na_n, \quad x_j \in I, \quad a_j \in A.$$

Wir wählen eine solche mit minimalem n und behaupten, daß dann

$$A = Ia_1 \oplus \cdots \oplus Ia_n$$

ist. Wegen $a = ax_1a_1 + \cdots + ax_na_n$ ist sicherlich $A = \sum_j Ia_j$. Sei andererseits $0 = \sum_j y_ja_j$, $y_j \in I$, etwa mit $y_na_n \neq 0$. Dann ist $Ay_n = I$, da I ein minimales Linksideal ist. Wegen

$$Ia_n = Ay_na_n = A(-y_1a_1 - \cdots - y_{n-1}a_{n-1} \subset \sum_{j=1}^{n-1} Ia_j$$

würden wir eine kürzere Darstellung der Eins finden. Also ist die Summe der Ia_j direkt. Die Ia_j sind zu I isomorphe einfache Moduln.

2 Das Radikal

Ein Ziel dieses Abschnittes ist zu zeigen, daß ein artinscher Ring einen größten halbeinfachen Quotienten hat. Das ausdividierte Ideal ist das Radikal.

(2.1) Lemma. *Seien $I_1, \ldots, I_n$ Ideale eines Ringes A und J ein maximales Ideal. Ist $\bigcap_j I_j \subset J$, so gibt es ein k mit $I_k \subset J$.*

Beweis. Angenommen I_k liegt für alle k nicht in J. Dann ist $I_k + J = A$, weil J maximal ist. Wir wählen eine Darstellung $1 = a_k + b_k$ mit $a_k \in I_k$ und $b_k \in J$.

Wir multiplizieren $1 = (a_1 + b_1) \cdots (a_n + b_n)$ aus. Der Summand $a_1 \cdots a_n$ liegt dann nach Voraussetzung in J. Die anderen Summanden enthalten einen Faktor b_j und liegen deshalb in J. Insgesamt folgt $1 \in J$. Widerspruch. □

(2.2) Satz. *Ein artinscher Ring hat nur endlich viele maximale Ideale.*

Beweis. Seien $I_1, I_2, \ldots$ paarweise verschiedene maximale Ideale. Wir setzen $J_k = I_1 \cap I_2 \cap \ldots \cap I_k$. Dann gilt $J_k \supset J_{k+1}$. Es gibt also ein n mit $J_n = J_{n+1}$ und das besagt $J_n \subset I_{n+1}$. Nach dem letzten Lemma gilt für ein $k \leq n$ die Inklusion $I_k \subset I_{n+1}$, was der Maximalität von I_k widerspricht. □

Wir bezeichnen den Durchschnitt der maximalen Ideale von A mit $\operatorname{rad}(A)$ und nennen dieses Ideal das *Radikal* von A.

(2.3) Satz. *Sei J ein maximales Ideal eines artinschen Ringes A. Dann ist A/J ein einfacher Ring.*

Beweis. Als Quotient eines artinschen Ringes ist A/J artinsch. Gäbe es in A/J ein von Null verschiedenes nilpotentes Ideal, so wäre J nicht maximal in A. Also ist A/J nach (2.3) halbeinfach und dann auch einfach, weil es keine echten Ideale gibt. □

(2.4) Satz. *Sei A artinsch. Dann ist $A/\operatorname{rad}(A)$ halbeinfach.*

Beweis. Seien $I_1, \ldots, I_n$ die maximalen Ideale von A. Nach dem chinesischen Restsatz ist $A/\operatorname{rad}(A) \cong \prod_{j=1}^{n} A/I_j$. Nach (2.3) sind die A/I_j einfach. Also ist $A/\operatorname{rad}(A)$ als Produkt einfacher Ringe halbeinfach. □

(2.5) Satz. *Ein artinscher Ring A ist genau dann halbeinfach, wenn $\operatorname{rad}(A) = 0$ ist.*

Beweis. Ist $\operatorname{rad}(A) = 0$, so ist A nach (2.4) halbeinfach. Ist A halbeinfach, so folgt aus dem Struktursatz über halbeinfache Ringe, daß der Schnitt der maximalen Ideale Null ist. □

(2.6) Satz. *Sei A artinsch. Sei J ein Ideal, für das A/J halbeinfach ist. Dann ist $\operatorname{rad}(A) \subset J$.*

Beweis. Die maximalen Ideale von A/J haben die Form I/J mit maximalen Idealen I von A. Sind $I_1/J, \ldots, I_r/J$ die maximalen Ideale von A/J, so ist nach (2.5)

$$0 = \operatorname{rad}(A/J) = I_1/J \cap \ldots \cap I_k/J = (I_1 \cap \ldots \cap I_k)/J,$$

also $J = I_1 \cap \ldots \cap I_k$. □

(2.7) Satz. *Das Radikal eines artinschen Ringes ist der Schnitt der maximalen Linksideale.*

Beweis. Sei J der Schnitt der maximalen Linksideale. Wegen der Minimalbedingung ist J der Schnitt endlich vieler maximaler Linksideale $I_1, \ldots, I_n$. Die

kanonische Abbildung

$$A/J \to \prod_{j=1}^{n} A/I_j$$

ist ein injektiver Homomorphismus von A-Moduln in ein Produkt von einfachen Moduln. Also ist A/J ein halbeinfacher A-Modul, also auch ein halbeinfacher A/J-Modul und dehalb A/J ein halbeinfacher Ring. Es folgt nach dem letzten Satz $\operatorname{rad}(A) \subset J$. Da $A/\operatorname{rad}(A)$ halbeinfach ist, so ist nach demselben Argument jedenfalls $\operatorname{rad}(A)$ Schnitt einiger maximaler Linksideale und somit $J \subset \operatorname{rad}(A)$.□

Wir bemerken, daß in einem Ring A ein maximales Ideal J immer Schnitt von maximalen Linksidealen ist. Sei nämlich $J \subset I$ ein maximales Linksideal. Dann enthält der Annullator des Moduls $M = A/I$ das Ideal J. Wegen der Maximalität von J ist also $J = \operatorname{Ann}(M)$, da $\operatorname{Ann}(M)$ zweiseitig ist. Andererseits ist $\operatorname{Ann}(M) = \cap_{x \neq 0} \operatorname{Ann}(x)$, und weil M einfach ist, ist $\operatorname{Ann}(x)$ für jedes $0 \neq x \in M$ ein maximales Linksideal.

(2.8) Satz. *Sei M einfacher Modul des artinschen Ringes A. Dann ist der Annullator von M ein maximales Ideal von R.*

Beweis. Der Annullator J ist ein zweiseitiges Ideal, und M kann als treuer Modul über $B = A/J$ aufgefaßt werden. Es genügt zu zeigen, daß B einfach ist. Sei I ein minimales Linksideal von B. Dann ist $IM \neq 0$, weil andernfalls I im Annullator von M liegt, was der Treue von M widerspricht. Sei $x \in M$ so gewählt, daß $Ix \neq 0$ ist. Dann ist $f\colon I \to M$, $\lambda \mapsto \lambda x$ nach dem Schurschen Lemma ein Isomorphismus. Also sind alle minimalen Linksideale von B isomorph. Ferner ist $I^2 \neq 0$, denn wegen $Ix = M$ gibt es ein $a \in I$ mit $ax = x$, also $a^2x = x \neq 0$, also $a^2 \neq 0$. Nach (2.3) ist B halbeinfach und nach VII(2.5) einfach. □

(2.9) Folgerung. *Die einfachen Moduln eines artinschen Ringes A sind Moduln über dem halbeinfachen Quotienten $A/\operatorname{rad}(A)$.* □

(2.10) Lemma. *Sei $a \in \operatorname{rad}(A)$. Dann hat $1 - a$ ein Linksinverses in A.*

Beweis. Angenommen $A(1-a) \neq A$. Dann gibt es ein maximales Linksideal I, das $A(1-a)$ umfaßt. Es ist $1 = a + (1-a)$, also $A = \operatorname{rad}(A) + A(1-a) \subset \operatorname{rad}(A) + I \subset I$, da $\operatorname{rad}(A)$ Schnitt maximaler Linksideale ist. Widerspruch. □

(2.11) Satz. *Das Radikal J eines artinschen Ringes ist nilpotent.*

Beweis. Wegen der Minimalbedingung gibt es ein n, sodaß $J^n = J^{2n}$ ist. Angenommen $J^n \neq 0$. Wir betrachten die Linksideale I mit $J^nI \neq 0$. Unter diesen gibt es ein bezüglich Inklusion minimales I. Sei $x \in I$ so gewählt, daß $J^nx \neq 0$ ist. Insbesondere ist dann $x \neq 0$. Es ist $J^nx \subset I$ ein Linksideal, und $J^n(J^nx)) = J^{2n}x = J^nx \neq 0$. Wegen der Minimalität von I ist $J^nx = I$. Es gibt ein $a \in J^n$ mit $ax = x$. Aus $(1-a)x = 0$ und dem vorigen Lemma folgt aber $x = 0$. Widerspruch. □

(2.12) Satz. *Sei M ein endlich erzeugter Modul über dem artinschen Ring A. Dann ist M noethersch und artinsch.*

BEWEIS. Sei J das Radikal von A. Wir setzen $M_i = J^i M$. Dann wird M_i/M_{i+1} durch J annulliert und ist deshalb nach (2.9) halbeinfach. Nach (1.2) und (1.4) ist M_i/M_{i+1} artinsch und hat deshalb eine Kompositionsreihe. Dann hat aber auch M eine Kompositionsreihe. □

(2.13) Folgerung. *Ein linker artinscher Ring ist ein linker noetherscher Ring.*

BEWEIS. Anwendung des vorstehenden Satzes auf den linksregulären Modul. □

Ein artinscher Ring ist genau dann halbeinfach, wenn er einen treuen halbeinfachen Modul besitzt.

3 Anwendungen auf die Galois-Theorie

Wir betrachten die Galois-Theorie vom Standpunkt der Algebren, verschärfen sie dadurch und geben einen neuen Beweis für den Hauptsatz der Galois-Theorie.

Seien $K|k$ und $L|k$ endliche Körpererweiterungen, und sei $\sigma\colon K \to L$ ein k-Morphismus. Wir betrachten L als (K, L)-Bimodul vermöge

$$k \cdot x = \sigma(k)x, \quad x \cdot l = xl$$

für $k \in K$, $x \in L$, $l \in L$. Äquivalent dazu betrachten wir L als $K \otimes_k L$-Linksmodul vermöge

$$(\alpha \otimes \beta) \cdot x = \sigma(\alpha)x\beta$$

für $\alpha \in K$, $\beta \in L$, $x \in L$. Diesen Modul nennen wir L_σ. Er ist als L-Rechtsmodul eindimensional.

Sei umgekehrt ein (K, L)-Bimodul M gegeben, der als L-Modul eindimensional ist. Für $x \in M \setminus 0$ und $\alpha \in K$ gibt es genau ein $\sigma(\alpha) \in L$ mit

$$\alpha \cdot x = x \cdot \sigma(\alpha).$$

Die Zuordnung $\alpha \mapsto \sigma(\alpha)$ ist ein von der Wahl von x unabhängiger k-Morphismus $\sigma = \sigma_M\colon K \to L$. Zwei Moduln M und N dieser Art sind genau dann isomorph, wenn $\sigma_M = \sigma_N$ ist. Demnach besteht eine Bijektion zwischen $\mathrm{Mor}_k(K, L)$ und den Isomorphieklassen von (K, L)-Bimoduln, die als L-Moduln eindimensional sind (bzw. solchen $K \otimes_k L$-Moduln).

Ein $K \otimes_k L$-Modul, der als L-Modul eindimensional ist, ist sicherlich einfach. Da er einfach ist, gehört er zur L-Algebra $K \otimes_k L/\mathrm{rad}(K \otimes_k L) = A$. Es gibt höchstens $\dim_L(A)$ verschiedene eindimensionale Moduln. Es ist $\dim_L(A) \leq [K : k]$. Im Fall $K = L$ erhalten wir den schon anderweitig bewiesenen Satz:

(3.1) Folgerung. *Für jede Galois-Erweiterung $L|k$ gilt $|G(L|k)| \leq [L : k]$.* □

Eine Galois-Erweiterung war durch die Bedingung $[L : k] = |G(L|k)|$ definiert, und $G = G(L|k)$ hieß ihre Galois-Gruppe. Das Tensorprodukt $M \otimes_L N$ zweier (L, L)-Bimoduln ist wieder einer: Das Tensorprodukt wird bezüglich der rechten

L-Struktur von M und der linken L-Struktur von N definiert und die (L,L)-Modulstruktur bezüglich der linken von M und der rechten von N. Seien $\sigma, \tau \in G$. In $L_\sigma \otimes_L L_\tau$ gilt

$$\begin{aligned} \alpha \cdot (x \otimes y) &= \sigma(\alpha)x \otimes y \\ &= x \otimes \sigma(\alpha) \cdot y \\ &= x \otimes \tau\sigma(\alpha)y \\ &= (x \otimes y) \cdot \tau\sigma(\alpha). \end{aligned}$$

Das bedeutet:

$$L_\sigma \otimes_L L_\tau \cong L_{\tau\sigma}.$$

Die Isomorphieklassen von (L,L)-Bimoduln, die als L-Rechtsmoduln eindimensional sind, bilden also bezüglich Tensorprodukt eine Gruppe, die zur Galois-Gruppe $G(L/k)$ isomorph ist.

Aus den Vorbetrachtungen ergibt sich jetzt unmittelbar:

(3.2) Satz. *Genau dann ist $L|k$ eine Galois-Erweiterung, wenn $L \otimes_k L$ halbeinfach ist und in über L eindimensionale einfache Bestandteile zerfällt. Diese einfachen Bestandteile sind die isotypischen Summanden und zu den L_σ isomorph. Es gibt demnach eine direkte Zerlegung $L \otimes_k L = \bigoplus_{\sigma \in G} L_\sigma$.* □

Wir schildern die Zerlegung des vorstehenden Satzes genauer im Lichte der früheren Untersuchungen zur Galois-Theorie.

Seien $K|k$ und $L|k$ Körpererweiterungen. Die Algebra $K \otimes_k L$ ist kommutativ. Der Homomorphismus $L \to K \otimes_k L$, $y \mapsto 1 \otimes y$ macht daraus eine L-Algebra, der Homomorphismus $K \to K \otimes_k L$, $x \mapsto x \otimes 1$ eine K-Algebra.

Sei $L|k$ eine Galois-Erweiterung mit Gruppe G. Die Gruppe G operiert auf der k-Algebra $L \otimes_k L$ durch die Automorphismen

$$g \cdot (x \otimes y) = x \otimes gy$$

für $g \in G$. Bezüglich der linken L-Modulstruktur operiert g L-linear, nicht aber bezüglich der rechten L-Modulstruktur.

Ein Automorphismus einer halbeinfachen Algebra bildet einen isotypischen Bestandteil wieder auf einen ab.

Sei dazu $L = k[\alpha]$ mit Minimalpolynom p von α. Über L zerfalle p in paarweise verschiedene Faktoren $p(x) = \prod_{j=1}^{n}(x - \alpha_j)$. Wir haben einen Isomorphismus

$$k[x]/(p) \to L, \quad x \mapsto \alpha.$$

Er liefert einen Isomorphismus

$$L \otimes_k L \cong L \otimes_k k[x]/(p).$$

Ferner ist

$$L \otimes_k k[x]/(p) \cong L[x]/(p),$$

wobei $\lambda \otimes 1$ der Klasse von λ und $1 \otimes x$ der Klasse von x entspricht. Vermöge des gesamten Isomorphismus

$$L \otimes_k L \cong L[x]/(p)$$

ist die linke L-Modulstruktur durch die übliche Skalarmultiplikation mit Elementen aus L gegeben. Bei der rechten entspricht die Multiplikation mit α derjenigen mit x und Elemente aus k wirken wie üblich.

Die Zerlegung von p in Linearfaktoren liefert nach dem chinesischen Restsatz einen Isomorphismus

$$L[x]/(p) \to \prod_{j=1}^{n} L[x]/(x - \alpha_j).$$

Das ist ein Isomorphismus von k-Algebren, L-linear bezüglich der linken Modulstruktur.

Wir haben einen Isomorphismus

$$\gamma_j \colon L[x]/(x - \alpha_j) \to L, \quad x \mapsto \alpha_j,$$

der bezüglich der linken Struktur wieder L-linearist. Das Element $\alpha \in L$ operiert in $L[x]/(x - \alpha_j)$ durch Multiplikation mit x von rechts und im Bild von γ_j durch Multiplikation mit α_j. Wir setzen zur Unterscheidung der verschiedenen Operationen $L = L_j$.

Insgesamt erhalten wir auf diese Weise eine Zerlegung von k-Algebren

$$L \otimes_k L \cong \prod_{j=1}^{n} L_j. \tag{3.3}$$

Das ist außerdem eine Zerlegung von (L, L)-Bimoduln, wobei L von links überall wie gewöhnlich operiert, während $\alpha \in L$ in L_j durch Multiplikation mit α_j operiert. Es gibt aber einen k-Morphismus $\sigma_j \colon L \to L$ mit $\alpha_j x = x \cdot \alpha = \sigma_j(\alpha)x$. Demnach ist σ_j durch $\sigma_j(\alpha) = \alpha_j$ bestimmt.

Wir betrachten L in üblicher Weise als Modul über dem Gruppenring kG, wobei $g \in G$ als der gegebene k-Morphismus wirkt. Durch Skalarerweiterung wird $L \otimes_k L$ ein Modul über $L \otimes_k kG \cong LG$. Wir behaupten:

(3.4) Satz. *Der LG-Modul $L \otimes_k L$ ist isomorph zum regulären LG-Modul.*

Beweis. Sei $1 = \sum_{\sigma \in G} e_\sigma$ die zu (3.3) gehörende Einszerlegung. Für jedes $g \in G$ ist $x \otimes y \mapsto g \cdot (x \otimes y) = x \otimes gy$ ein Automorphismus der k-Algebra $L \otimes_k L$. Deshalb ist $g \cdot e_\sigma$ wieder eines der Idempotenten e_τ. Bezüglich der linken L-Modulstruktur ist die G-Operation L-linear. Es folgt mittels (3.3) und der Definition von L_σ

$$\begin{aligned} e_\tau \tau(a) &= a \cdot e_\tau = a(g \cdot e_\sigma) = g(a \cdot e_\sigma) \\ &= g(e_\sigma \sigma(a)) = (g \cdot e_\tau)(g\sigma(a)) = e_\tau g\sigma(a) \end{aligned}$$

und demnach $\tau = g\sigma$. Diese Rechnung belegt, daß $LG \to L \otimes_k L$, $\Sigma_g \lambda_g g \mapsto \Sigma \lambda_g e_g$ ein Isomorphismus von LG-Moduln ist. Aus (6.4) und (??) folgt:

(3.5) Satz. *Ist $L|k$ eine endliche Galois-Erweiterung mit Gruppe G, so ist L als kG-Modul zu kG isomorph. Ist $\alpha\colon kG \to L$ ein solcher Isomorphismus und ist $\alpha(1) = z \in L$, so ist $\{\sigma(z) \mid \sigma \in G\}$ eine k-Basis von L. (Eine Basis dieser Art heißt* Normalbasis*.* □

(3.6) Folgerung. *Für eine Galois-Erweiterung $L|k$ mit Gruppe G gilt $L^G = k$.* □

(3.7) Folgerung. *Ist $\{\sigma(z) \mid \sigma \in G\}$ eine Normalbasis, so ist $L = k[z]$. Denn $f(x) = \prod_{\sigma \in G} (x - \sigma(z))$ ist das Minimalpolynom von z über k.* □

Ist $L|K|k$ und $L|k$ Galoiserweiterung, so ist auch $L|K$ Galoiserweiterung, denn $L \otimes_k L$ ist ein Quotient von $L \otimes_k L$ und deshalb mit $L \otimes_k L$ halbeinfach mit als L-Modul eindimensionalen einfachen Moduln.

(3.8) Folgerung. *Für jeden Zwischenkörper K von $G|k$ gilt $L^{G(L|K)} = K$ und $|G(L|K)| = [L : K]$.* □

Sei $L|k$ Galois-Erweiterung und $H < G(L|k)$. Für die reguläre Darstellung gilt $|kG^H : k| = |G : H|$, also $|kG : kG^H| = |H|$. Also gilt $|L : L^H| = |H|$. Wegen $H < G(L|L^H)$ folgt $|H| \le |G(L|L^H)| = |L : L^H| = H$, also

$$H = G(L|L^H). \tag{3.9}$$

Mit (6.8) und (6.9) haben wir den Hauptsatz der Galois-Theorie von neuem bewiesen, jedenfalls soweit die Objekte betroffen sind.

Um auch die Morphismen zu behandeln, muß man sich überlegen, daß für $L|K|k$ jeder k-Morphismus $\sigma\colon K \to L$ zu einem k-Morphismus $L \to L$ erweitert werden kann.

Ein k-Morphismus $\sigma\colon K \to L$ entspricht aber einem gewissen einfachen $K \otimes_k L$-Modul M. Es ist zu zeigen, daß dieser als Restriktion eines $L \otimes_k L$-Moduls vorkommt. Das ist aber eine in (1.10) bewiesene allgemeine Tatsache über halbeinfache Algebren.

Der Isomorphismus $L \otimes_k L \cong LG$ läßt sich auch etwas anders begründen als im Beweis von Satz (6.4). Wir definieren eine Abbildung

$$f\colon L \otimes_k L \to LG, \quad x \otimes y \mapsto \sum_{g \in G} x g^{-1}(y) g.$$

Das ist eine G-äquivariante lineare Abbildung. Sie ist invers zu der in (6.4) angegebenen Isomorphie. Die Isomorphie folgt auch aus dem Satz von der linearen Unabhängigkeit von Charakteren.