

# II. Ringe und Moduln für etwas Fortgeschrittene

## II.1 Algebren

### 2.1.1 Definition/Bemerkung (*Die Kategorie der $R$ -Algebren*)

a) Es sei  $R$  ein Ring. Eine  $R$ -Algebra ist ein  $R$ -Modul  $A$ , der gleichzeitig ein Ring ist (natürlich mit derselben Addition), und dessen Multiplikation  $R$ -bilinear ist, das heißt, dass zusätzlich zum Distributivgesetz auch noch gilt:

$$\forall r_1, r_2 \in R, a_1, a_2 \in A : (r_1 a_1) \cdot (r_2 a_2) = r_1 r_2 (a_1 a_2).$$

b) Wenn  $A$  eine  $R$ -Algebra ist, dann ist die Abbildung

$$\iota_A : R \ni r \mapsto \iota_A(r) := r \cdot 1_A \in A$$

ein Ringhomomorphismus. Wegen der Bilinearität der Multiplikation liegt das Bild von  $\iota_A$  im Zentrum  $Z(A)$  von  $A$ :

$$Z(A) := \{a \in A \mid \forall x \in A : ax = xa\}.$$

Dies folgt aus

$$\forall r \in R, a \in A : \iota_A(r) \cdot a = (r 1_A) a = r \cdot (1_A a) = r \cdot (a 1_A) = a \cdot (r 1_A) = a \cdot \iota_A(r).$$

Insbesondere ist das Bild von  $R$  unter  $\iota_A$  ein kommutativer Ring.

c) Wenn umgekehrt  $R$  und  $A$  Ringe sind und wir einen Ringhomomorphismus  $\iota : R \rightarrow Z(A)$  haben, so definiert dieser auf  $A$  die Struktur eines  $R$ -Moduls und macht  $A$  zu einer  $R$ -Algebra.

d) Wenn  $A$  und  $B$  zwei  $R$ -Algebren sind, so sind die  $R$ -Algebren-Homomorphismen zwischen  $A$  und  $B$  genau die Ringhomomorphismen, die auch noch  $R$ -linear sind. Das definiert die Menge  $\text{Hom}_{R\text{-Alg}}(A, B)$ . Die  $R$ -Algebren sind damit eine Kategorie, die Verknüpfung zweier Homomorphismen ist die Komposition der Abbildungen.

e) Es sei  $[R, R]$  das Ideal in  $R$ , das von den Kommutatoren  $rs - sr$ ,  $r, s \in R$ , erzeugt wird. Dieses heißt das Kommutatorideal von  $R$ . Dann ist  $R/[R, R]$  kommutativ, und jeder Homomorphismus von  $R$  in einen kommutativen Ring faktorisiert über  $R/[R, R]$ . Die Vorgabe einer  $R$ -Algebra ist also äquivalent zur Vorgabe einer  $R/[R, R]$ -Algebra.

Wir werden im Weiteren meistens voraussetzen, dass  $R$  kommutativ ist.

### 2.1.2 Beispiele (ein paar Algebren)

a) Für einen kommutativen Ring  $R$  ist der Polynomring  $R[X]$  eine  $R$ -Algebra. Hierbei braucht man, dass  $R$  kommutativ ist, da  $R$  ja isomorph zu einem Teilring des Zentrums von  $R[X]$  sein soll.

Der Polynomring über einem nicht kommutativen Ring  $R$  lässt sich natürlich auch definieren, aber das Rechnen mit ihm ist tückisch. Er ist nur noch eine Algebra über dem Zentrum von  $R$ .

b) Allgemeiner ist für einen kommutativen Ring  $R$  und ein Monoid  $M$  der Monoidring  $R[M]$  eine  $R$ -Algebra.

Zur Erinnerung:  $R[M] := \text{Abb}(M, R)_0$  ist die Menge aller Abbildungen von  $M$  nach  $R$  mit endlichem Träger. Dies ist ein freier  $R$ -Modul mit einer Basis  $\{\delta_m \mid m \in M\}$ , wobei

$$\forall x \in M : \delta_m(x) = \begin{cases} 0, & \text{falls } x \neq m, \\ 1, & \text{falls } x = m. \end{cases}$$

Die Multiplikation in  $R[M]$  ist durch  $R$ -bilineare Fortsetzung der Vorschrift  $\delta_m \cdot \delta_n := \delta_{mn}$  gegeben.

Dies liefert einen Funktor von der Kategorie der Monoide in die Kategorie der  $R$ -Algebren, wobei für eine Abbildung  $f : M \rightarrow N$  zwischen Monoiden die Abbildung  $R[M] \ni \sum_{m \in M} r_m \delta_m \mapsto \sum_{m \in M} r_m \delta_{f(m)} \in R[N]$  ein  $R$ -Algebren-Homomorphismus ist.

c) Auch der Matrizenring  $R^{n \times n} =: M_n(R)$  ist eine  $R$ -Algebra, wenn  $R$  ein kommutativer Ring ist.

d) Jeder Ring ist eine Algebra über seinem Zentrum (bezüglich der Einbettung). Jeder Ring  $A$  ist eine  $\mathbb{Z}$ -Algebra bezüglich des einzigen Ringhomomorphismus von  $\mathbb{Z}$  nach  $A$ . Die Kategorie der  $\mathbb{Z}$ -Algebren ist natürlich äquivalent zur Kategorie aller Ringe.

e) Wenn  $K$  ein Körper und  $L$  ein Erweiterungskörper von  $K$  ist, dann ist  $L$  insbesondere eine  $K$ -Algebra. In der Galoistheorie wird das implizit immer so gehandhabt. So betrachtet man dort ja für zwei Erweiterungskörper gerade die  $K$ -linearen Ringhomomorphismen, also die  $K$ -Algebrenhomomorphismen. Genauso betrachtet man die  $K$ -linearen Automorphismen eines Erweiterungskörpers, also die  $K$ -Algebren Automorphismen (die wir nicht gesondert definiert haben – es sind die Automorphismen in der Kategorie der  $K$ -Algebren).

### 2.1.3 Definition (freie Algebra)

Es sei  $R$  ein kommutativer Ring. Jede  $R$ -Algebra ist auch eine Menge, und das gibt einen Vergiss-Funktor von  $\underline{R-Alg}$  nach  $\underline{Men}$ . Gibt es einen dazu linksadjungierten Funktor? Das wäre ein Funktor, der jeder Menge  $S$  eine  $R$ -Algebra

$R[S]$  zuordnet, sodass man für jede  $R$ -Algebra  $A$  natürliche Isomorphismen

$$\eta_{S,A} : \text{Abb}(S, A) \longrightarrow \text{Hom}_{R\text{-Alg}}(R[S], A)$$

erhält. Solch eine Algebra  $R[S]$  ist die *freie  $R$ -Algebra über dem Alphabet  $S$* ; sie lässt sich so konstruieren:

Zu  $S$  gehört das freie Monoid

$$M := S^0 \cup S^1 \cup S^2 \cup \dots = \bigcup_{n \in \mathbb{N}_0} S^n \quad (\text{disjunkte Vereinigung}).$$

Dabei ist  $S^n$  das  $n$ -fache kartesische Produkt von  $S$ , also die Menge aller Abbildungen von  $\{1, \dots, n\}$  nach  $S$ . Speziell ist  $S^0$  eine Menge, die aus einem Element (dem *leeren Wort*) besteht. Die Verknüpfung in  $M$  ist das Hintereinandersetzen von Tupeln:

$$S^n \times S^k \ni ((s_1, \dots, s_n), (t_1, \dots, t_k)) \mapsto (s_1, \dots, s_n, t_1, \dots, t_k) \in S^{n+k}.$$

Wir haben eine offensichtliche Identifikation von  $S$  mit  $S^1 \subseteq M$ . Dieses freie Monoid erfüllt eine universelle Abbildungseigenschaft: Für alle Monoide  $(N, \circ)$  und alle Abbildungen  $f : S \rightarrow N$  gibt es genau einen Monoidhomomorphismus  $\tilde{f}$  von  $M$  nach  $N$ , der  $f$  von  $S^1$  nach  $M$  fortsetzt:

$$\tilde{f}((s_1, \dots, s_n)) := f(s_1) \circ f(s_2) \circ \dots \circ f(s_n).$$

Zu guter Letzt bilden wir den Monoidring  $R[M]$  (siehe 2.1.2 b)). Wir schreiben  $R\{S\} := R[M]$  und nennen dies die *freie  $R$ -Algebra über  $S$* .

Nun sei  $A$  eine beliebige  $R$ -Algebra und  $f : S \rightarrow A$  eine Abbildung von Mengen. Dann gehört dazu eine multiplikative Abbildung vom freien Monoid  $M$  nach  $(A, \cdot)$ , nämlich

$$(s_1, \dots, s_n) \mapsto f(s_1) \cdot f(s_2) \cdot \dots \cdot f(s_n).$$

Die  $R$ -lineare Fortsetzung hiervon liefert einen  $R$ -Algebren-Homomorphismus von  $R\{S\}$  nach  $A$ . Damit haben wir eine Abbildung

$$\eta_{S,A} : \text{Abb}(S, A) \longrightarrow \text{Hom}_{R\text{-Alg}}(R\{S\}, A)$$

definiert. Diese ist injektiv, da die Elemente  $\delta_m$ ,  $m \in M$ , eine  $R$ -Basis von  $R\{S\}$  bilden. Sie ist surjektiv, da sich ein  $R$ -Algebren-Homomorphismus  $\Phi : R\{S\} \rightarrow A$  aus der Abbildung  $f : S \rightarrow A$ ,  $s \mapsto \Phi(\delta_s)$ , zurückgewinnen lässt.

Man rechnet nach (z.B. mit Yoneda), dass diese Abbildungen  $\eta_{S,A}$  zeigen, dass die Funktoren  $S \rightsquigarrow R\{S\}$  und  $(A \text{ als Algebra}) \rightsquigarrow (A \text{ als Menge})$  zueinander adjungiert sind.

### 2.1.4 Definition/Bemerkung (*K*-Algebren)

Es seien  $K$  ein Körper und  $A \neq \{0\}$  eine  $K$ -Algebra. Dann ist für jedes  $a \in A$  die Abbildung

$$\mu_a : A \longrightarrow A, \quad \mu_a(x) := ax,$$

ein Endomorphismus der additiven Gruppe von  $A$ . Da die Multiplikation  $K$ -bilinear ist, ist dieser Endomorphismus sogar  $K$ -linear. Da  $A$  außerdem ein Einselement hat, ist die Abbildung

$$\mu : A \longrightarrow \text{End}_{K\text{-VR}}(A), \quad a \mapsto \mu_a,$$

injektiv. Sie ist ein injektiver  $K$ -Algebren-Homomorphismus, und das sagt, dass  $A$  sich auffassen lässt als  $K$ -Unteralgebra (es ist klar, wie das zu definieren ist!) der Algebra  $\text{End}_{K\text{-VR}}(A)$ .

Das ist wieder einmal ein Analogon zum Satz von Cayley, dass jede Gruppe isomorph zu einer Untergruppe einer symmetrischen Gruppe ist.

Wenn  $A$   $n$ -dimensional ist, so ist also  $A$  isomorph zu einer Unteralgebra von  $M_n(K)$ . Mit dieser Methode lässt sich oft entscheiden, ob es eine endlichdimensionale Algebra mit vorgegebenen Eigenschaften gibt oder nicht.

Außerdem sind damit für eine endlichdimensionale  $K$ -Algebra  $A$  folgende Begriffe für  $a \in A$  definierbar:

$$\text{Spur}(a) := \text{Spur}(\mu_a), \quad \mathcal{N}(a) := \text{Norm}(a) := \det(\mu_a).$$

Die Spur ist eine Linearform auf dem Vektorraum  $A$ , die Norm ist multiplikativ und homogen vom Grad  $\dim_K(A)$ , was heißt:

$$\forall r \in K, a, b \in A : \mathcal{N}(rab) = r^{\dim_K(A)} \mathcal{N}(a) \mathcal{N}(b).$$

Wenn  $a \in A$  invertierbar ist, dann folgt  $\mathcal{N}(a)\mathcal{N}(a^{-1}) = 1$ , also ist die Norm von  $a$  eine Einheit in  $K$ . Ist umgekehrt die Norm von  $a$  eine Einheit in  $K$ , so ist  $\mu_a$  im Endomorphismenring invertierbar, aber diese Inverse ist – wegen Cayley-Hamilton – ein Polynom in  $\mu_a$ , also selbst im Bild von  $\mu$ , und damit ist  $a$  in  $A$  invertierbar.

### 2.1.5 Bemerkung (*Verkettungsoperatoren*)

Die Homomorphismen zwischen zwei  $A$ -Moduln  $M$  und  $N$  heißen oft auch *Verkettungsoperatoren*. So ein Homomorphismus  $\Phi$  muss für alle  $a \in A$  das folgende Diagramm kommutativ machen:

$$\begin{array}{ccc} M & \xrightarrow{m \mapsto am} & M \\ \Phi \downarrow & & \downarrow \Phi \\ N & \xrightarrow{n \mapsto an} & N \end{array}$$

Im Englischen sind das die *intertwining operators*.

Wenn  $A$  eine  $K$ -Algebra ist, darf man sich bei der Suche nach solchen  $\Phi$  auf  $K$ -Vektorraum Homomorphismen beschränken, was die Sache manchmal übersichtlicher macht. Und dann langt es, das obige Diagramm für alle  $a$  in einem fest gewählten Algebren-Erzeugendensystem von  $A$  auf seine Kommutativität zu überprüfen. Wenn zum Beispiel  $A = K[G]$  ein Gruppenring ist, dann besteht  $\text{End}_A(M)$  genau aus den  $K$ -linearen Abbildungen von  $M$  nach  $M$ , die zusätzlich  $G$ -äquivariant sind.

Für jeden endlich erzeugten Modul  $M$  über einer endlich dimensionalen  $K$ -Algebra  $A$  (d.h. Vorgabe eines Ringhomomorphismus  $\rho : A \longrightarrow \text{End}(M)$ ) gibt es die Linearform

$$S_\rho : A \longrightarrow K, \quad a \mapsto \text{Spur}(\rho(a)).$$

Hierbei wird benutzt, dass jeder  $A$ -Modul ein  $K$ -Vektorraum ist, und bei unseren Voraussetzungen endlichdimensional sein muss. Ist nämlich  $\{a_1, \dots, a_n\}$  eine  $K$ -Basis von  $A$  und  $\{m_1, \dots, m_l\}$  ein  $A$ -Erzeugendensystem von  $M$ , dann enthält

$$\{\rho(a_i)(m_j) \mid 1 \leq i \leq n, 1 \leq j \leq l\}$$

eine  $K$ -Basis von  $M$ .

Diese Linearform liefert eine Bilinearform  $\tau_\rho$  auf  $A$  vermöge

$$\tau_\rho(a_1, a_2) := S_\rho(a_1 \cdot a_2).$$

Wir werden später auf diese sogenannte *Spurform* ( $\tau$  steht für *trace*) zu sprechen kommen.

### 2.1.6 Definition/Bemerkung (*halbeinfach*)

Es seien  $A$  ein Ring und  $M$  ein  $A$ -Modul.

a)  $M$  heißt *einfach*, wenn  $M \neq \{0\}$  gilt und wenn  $M$  und  $\{0\}$  die einzigen  $A$ -Untermodule von  $M$  sind.

b)  $M$  heißt *halbeinfach*, wenn es zu jedem Untermodul  $U$  von  $M$  einen komplementären Untermodul  $V$  gibt, für den also

$$M = U \oplus V$$

gilt. Jeder einfache Modul zum Beispiel ist halbeinfach.

c) Wenn man eine Zerlegung von  $M$  als  $M = U \oplus V$  mit Untermoduln  $U$  und  $V$  hat, so sind die Projektionen von  $M$  auf  $U$  längs  $V$  und auf  $V$  längs  $U$  jeweils  $A$ -Modul-Homomorphismen.

d) Ein Ring  $A$  heißt *halbeinfach*, wenn er als  $A$ -Modul halbeinfach ist.

*Vorsicht:* Ein einfacher Ring ist einer ohne zweiseitige Ideale; das ist nicht dasselbe wie die Forderung, dass er als  $A$ -Modul einfach sei.

### 2.1.7 Beispiel

a) Es sei  $K$  ein Körper. Der Ring  $A := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in K \right\} \subseteq M_2(K)$  ist eine  $K$ -Algebra. Sie ist nicht halbeinfach, denn zu dem Linksideal  $K \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$  gibt es kein komplementäres Linksideal.

Ein Körper hingegen ist immer halbeinfach.

Der Matrizenring  $A = K^{n \times n}$  über einem Körper  $K$  ist einfach als Ring; aber als Modul ist er die direkte Summe von  $n$  einfachen  $A$ -Moduln (Übung!).

b) Ein einfacher  $A$ -Modul  $M$  ist immer von einem beliebigen Element  $m \in M \setminus \{0\}$  erzeugt. Die Abbildung

$$A \longrightarrow M, \quad a \mapsto a \cdot m$$

ist dann ein surjektiver  $A$ -Modulhomomorphismus, und der Kern ist ein maximales Linksideal in  $A$ . Umgekehrt liefert jedes maximale Linksideal  $I$  in  $A$  einen irreduziblen  $A$ -Modul, nämlich  $A/I$ .

### 2.1.8 Hilfssatz (Summen und Quotienten von halbeinfachen Moduln)

Es seien  $A$  ein Ring und  $M$  ein halbeinfacher  $A$ -Modul. Dann gelten:

a) Wenn  $U$  ein Untermodul von  $M$  ist, so sind auch  $U$  und der Faktormodul  $M/U$  halbeinfach.

b) Ist  $N$  ein weiterer halbeinfacher  $A$ -Modul, dann auch ist  $M \times N$  halbeinfach.

*Beweis.* a) Es sei  $V$  ein Untermodul von  $U$ . Zu  $U$  gibt es in  $M$  einen komplementären Untermodul  $W$ . Da  $V \subseteq U$  gilt, ist  $V \oplus W$  ein Untermodul von  $M$ , und dazu gibt es einen komplementären Untermodul  $S$ . Betrachte nun die Projektion  $\pi$  von  $M$  auf  $U$  längs  $W$ . Dieses ist ein surjektiver Modulhomomorphismus, und es gilt für alle  $v \in V$ :  $\pi(v) = v$ . Da  $W$  der Kern von  $\pi$  ist, folgt  $U = V \oplus \pi(S)$ , und wir haben einen zu  $V$  komplementären Untermodul in  $U$  gefunden.

$M/U$  ist zum Modul  $W$  isomorph, also zu einem Untermodul von  $M$ , und damit auch wieder halbeinfach.

b) Es sei nun  $V$  ein Untermodul von  $M \times N$ . Weiter seien

$$\pi_1 : M \times N \longrightarrow M, \quad \pi_2 : M \times N \longrightarrow N,$$

die Projektionen auf die erste bzw. zweite Koordinate. Wir bezeichnen mit  $M_V$  und  $N_V$  die Bilder von  $V$  unter  $\pi_1$  und  $\pi_2$ .

Dann ist  $V \subseteq M_V \times N_V$ .

Schließlich seien

$$V_1 := \{m \in M \mid (m, 0) \in V\}, \quad \text{und} \quad V_2 := \{n \in N \mid (0, n) \in V\}.$$

Dann ist  $V_1 \times V_2 \subseteq V$ .

Nun ist aber  $V_1 \subseteq M_V$ , und  $M_V$  ist wegen Teil a) halbeinfach. Also gibt es einen komplementären Untermodul  $U_1$  zu  $V_1$  in  $M_V$ . Analog gibt es einen komplementären Untermodul  $U_2$  zu  $V_2$  in  $N_V$ .

Für jedes  $u_1 \in U_1$  gibt es ein  $(u_1, n) \in V$ , und  $n$  lässt sich eindeutig als  $n_V + u_2$  zerlegen mit  $n_V \in N_V, u_2 \in U_2$ . Also gibt es ein eindeutig bestimmtes  $u_2 \in U_2$  mit  $(u_1, u_2) \in V$ .

Die Zuordnung  $U_1 \ni u_1 \mapsto u_2 \in U_2$  ist ein Isomorphismus  $\varphi$  zwischen  $U_1$  und  $U_2$ . Damit gilt

$$V = (M_V \times \{0\}) \oplus (\{0\} \times N_V) \oplus \{(u_1, \varphi(u_1)) \mid u_1 \in U_1\}.$$

Wenn  $C_V$  ein Komplement zu  $M_V$  in  $M$  und  $D_V$  ein Komplement in  $N$  zu  $N_V$  sind, dann ist damit

$$(C_V \times D_V) \oplus (U_1 \times \{0\})$$

ein zu  $V$  komplementärer Untermodul in  $M \times N$ . ○

### 2.1.9 Hilfssatz (Kriterium der Halbeinfachheit)

Es seien  $K$  ein Körper,  $A$  eine endlichdimensionale  $K$ -Algebra, und  $M$  ein endlich erzeugter  $A$ -Modul. Dann sind äquivalent:

- i)  $M$  ist halbeinfach
- ii)  $M$  ist eine direkte Summe von einfachen Moduln.

*Beweis.* i)  $\Rightarrow$  ii)

Wir machen vollständige Induktion nach  $d := \dim_K(M)$ . Im Falle  $d = 0$  ist  $M$  die leere Summe, was wir als Induktionsanfang nehmen.

Nun sei die Behauptung wahr für alle Moduln mit kleinerer Dimension als  $\dim(M)$ . Wenn  $M$  nicht einfache ist, dann gibt es einen nichttrivialen Untermodul  $U$  von  $M$ . Zu diesem gibt es – wegen der Halbeinfachheit – einen komplementären Untermodul  $V$ .

Aber sowohl  $U$  als auch  $V$  sind nach Induktionsvoraussetzung direkte Summen von einfachen Moduln. Damit stimmt dies auch für  $U \oplus V = M$ .

ii)  $\Rightarrow$  i)

Dies ist wegen Proposition 2.1.8 klar. ○

### 2.1.10 Bemerkung

Eine endlichdimensionale  $K$ -Algebra  $A$  ist also genau dann halbeinfach, wenn jeder endlich erzeugte  $A$ -Modul halbeinfach ist.

Vielleicht ist jetzt ein guter Zeitpunkt für ein Beispiel?

Dabei werden wir uns gleich die Schwerpunktbildung zunutze machen. Wenn eine endliche Gruppe  $G$  auf einer abelschen Gruppe  $V$  über Gruppenautomorphismen operiert, dann ist für jedes  $v \in V$  das Element  $\sum_{g \in G} g(v)$  invariant unter der Gruppenoperation. Denn für jedes  $h \in G$  gilt:

$$h\left(\sum_{g \in G} g(v)\right) = \sum_{g \in G} (hg)(v) = \sum_{g \in G} g(v).$$

An welcher Stelle und für welche Gruppe wird dies im nächsten Satz benützt?

### 2.1.11 Anwendung (Satz von Maschke)

Es seien  $K$  ein Körper,  $G$  eine endliche Gruppe und die Charakteristik von  $K$  kein Teiler der Ordnung  $|G|$  von  $G$ . Dann ist der Gruppenring  $K[G]$  halbeinfach.

*Beweis.* Wir zeigen sogar direkt mehr: jeder endlich erzeugte  $K[G]$ -Modul ist halbeinfach.

Es sei  $M$  ein endlichdimensionaler  $K[G]$ -Modul, also ein endlichdimensionaler  $K$ -Vektorraum  $M$ , auf dem die Gruppe  $G$  über  $K$ -lineare Automorphismen operiert, das heißt über einen Gruppenhomomorphismus

$$\rho : G \longrightarrow \text{Aut}_{K\text{-VR}}(M).$$

Weiter sei  $U$  ein  $K[G]$ -Untermodul. Schließlich sei  $\pi : M \longrightarrow U$  irgendeine  $K$ -lineare Projektion (mit einem Vektorraumkomplement zu  $U$  als Kern).

Dann definieren wir

$$\tilde{\pi} : M \longrightarrow U, \quad m \mapsto \tilde{\pi}(m) := \sum_{g \in G} \rho(g)(\pi(\rho(g^{-1})m)).$$

Dieses  $\tilde{\pi}$  ist  $K$ -linear, und für jedes  $h \in G$  und jedes  $m \in M$  gilt:

$$\begin{aligned} \rho(h) \circ \tilde{\pi}(m) &= \sum_{g \in G} \rho(hg)(\pi(\rho(g^{-1})m)) \\ &= \sum_{hg \in G} \rho(hg)(\pi(\rho((hg)^{-1}h)m)) \\ &= \tilde{\pi}(\rho(h)(m)) = \tilde{\pi} \circ \rho(h)(m). \end{aligned}$$

Also ist  $\tilde{\pi}$  ein  $K[G]$ -Modulhomomorphismus von  $M$  nach  $U$ . Für  $u \in U$  gilt

$$\tilde{\pi}(u) = \sum_{g \in G} \rho(g)(\pi(\rho(g^{-1})u)) = \sum_{g \in G} \rho(g)(\rho(g^{-1})u) = |G| \cdot u.$$

Da  $|G|$  eine Einheit in  $K$  ist, ist das Bild von  $\tilde{\pi}$  gleich  $U$ , und der Kern ist ein zu  $U$  komplementärer Untermodul.  $\circ$

### 2.1.12 Bemerkung (Bezeichnungen für $K[G]$ -Moduln)

Statt von  $K[G]$ -Moduln spricht man auch von ( $K$ -)linearen Darstellungen der Gruppe  $G$ . Ein einfacher  $K[G]$ -Modul heißt auch eine *irreduzible Darstellung* von  $G$ . Nach dem Satz 2.1.8 ist jede endlichdimensionale Darstellung von  $G$  eine direkte Summe von irreduziblen Darstellungen, wenn die Charakteristik von  $K$  kein Teiler der Gruppenordnung ist.

Wir werden das später in Charakteristik 0 noch genauer untersuchen.

Welche irreduziblen Darstellungen gibt es?

Da nach 2.1.7 b) die irreduziblen Darstellungen isomorph sind zu Quotienten von  $K[G]$  nach maximalen Linksideal, diese aber wegen der Halbeinfachheit ein komplementäres Linksideal besitzen, ist in Charakteristik 0 jede irreduzible  $K$ -lineare Darstellung einer endlichen Gruppe  $G$  isomorph zu einer Teildarstellung der sogenannten *regulären Darstellung* von  $G$ . Das ist  $K[G]$  aufgefasst als  $K[G]$ -Linksmodul. Wenn man  $K[G]$  in irreduzible Summanden zerlegt hat und einen irreduziblen Modul untersucht, sieht man, dass er (als Quotient der regulären Darstellung) zu einem der ausgewählten irreduziblen Moduln isomorph ist. Insbesondere gibt es nur endlich viele Typen von irreduziblen Darstellungen von  $G$ .

Wie sehen Endomorphismen von einfachen Moduln aus?

### 2.1.13 Proposition (Lemma von Schur)

a) Es seien  $A$  ein Ring und  $M$  ein einfacher  $A$ -Modul. Dann ist  $\text{End}_A(M)$  ein Schiefkörper.

b) Ist  $A$  eine endlichdimensionale Algebra über einem algebraisch abgeschlossenen Körper  $K$  und  $M$  ein einfacher  $A$ -Modul, so ist  $\text{End}_A(M) = K \cdot \text{Id}_M$ .

*Beweis.* a) Dass  $M$  ein einfacher  $A$ -Modul ist bedeutet, dass  $M \neq \{0\}$  gilt und dass es in  $M$  keine Untermoduln außer  $M$  und  $\{0\}$  gibt. Natürlich bilden die Endomorphismen von  $M$  einen Ring. Zu zeigen ist nur, dass dieser Ring nicht der Nullring ist, und dass jedes von 0 verschiedene Element invertierbar ist.

Da  $M$  nicht 0 ist, ist  $\text{Id}_M$  ein Endomorphismus von  $M$ , der nicht die Nullabbildung ist. Da auch die Nullabbildung ein Endomorphismus ist, ist der Endomorphismenring nicht der Nullring.

Nun sei  $\Phi \in \text{End}_A(M)$  ein von Null verschiedener Endomorphismus. Dann ist der Kern von  $\Phi$  ein  $A$ -Untermodul von  $M$ , denn für alle  $m, n \in \text{Kern}(\Phi)$  und alle  $a \in A$  gilt

$$\Phi(am + n) = a\Phi(m) + \Phi(n) = 0.$$

Da  $\Phi$  nicht die Nullabbildung ist, ist der Kern von  $M$  verschieden, also – wegen der Einfachheit –  $\text{Kern}(\Phi) = \{0\}$ . Damit ist  $\Phi$  injektiv.

Auch das Bild von  $\Phi$  ist ein Untermodul von  $M$ , aber eben nicht der Nullmodul, da  $\Phi$  nicht die Nullabbildung ist. Daher ist – wegen der Einfachheit –  $\text{Bild}(\Phi) = M$ , und  $\Phi$  ist surjektiv.

Insgesamt ist  $\Phi$  bijektiv und damit invertierbar, die Inverse ist aber selbstverständlich auch ein  $A$ -Modul-Homomorphismus. Also gilt für  $\Phi \neq 0$ :  $\Phi^{-1} \in \text{End}_A(M)$ .

b) Nun ist  $A$  eine endlichdimensionale  $K$ -Algebra. Für  $m \in M$  ist sicher  $A \cdot m := \{am \mid a \in A\} \subseteq M$  ein  $A$ -Untermodul von  $M$ . Da  $M$  einfach ist, ist dieser Untermodul gleich  $M$ , wenn  $m \neq 0$ . Damit ist  $M$  ein endlichdimensionaler  $K$ -Vektorraum, denn für eine Basis  $a_1, \dots, a_d$  von  $A$  erzeugen  $a_1m, \dots, a_dm$  den  $K$ -Vektorraum  $Am = M$ .

Wenn jetzt  $\Phi$  ein  $A$ -Endomorphismus von  $M$  ist, dann ist  $\Phi$  insbesondere  $K$ -linear. Da  $M$  endlichdimensional und  $K$  algebraisch abgeschlossen ist, hat  $\Phi$  einen Eigenwert  $\lambda$  in  $K$ . Der Endomorphismus

$$\Phi - \lambda \text{Id}_M \in \text{End}_A(M)$$

ist nicht invertierbar, da er einen nichttrivialen Kern hat. Somit ist er nach Teil a) die Nullabbildung, und wir finden

$$\Phi = \lambda \text{Id}_M.$$

Da umgekehrt die Abbildungen in  $K \cdot \text{Id}_M$  alle  $A$ -linear sind (hier braucht man  $\iota_A(K) \subseteq Z(A)$ ), folgt die Behauptung.  $\circ$

## II.2 Noethersche Ringe und Moduln

Hier lernen wir einen hilfreichen Endlichkeitsbegriff kennen.

**2.2.1 Definition/Bemerkung** a) Es seien  $R$  ein kommutativer Ring und  $M$  ein  $R$ -Modul. Dann heißt  $M$  *noethersch*, falls jeder  $R$ -Untermodul von  $M$  endlich erzeugt ist.

Der Ring  $R$  selbst heißt *noethersch*, wenn jedes Ideal in  $R$  endlich erzeugt ist, wenn er also ein noetherscher  $R$ -Modul ist.

b) Wenn  $R$  nicht kommutativ ist, dann unterscheiden sich im Allgemeinen Links- $R$ -Moduln (mit der Eigenschaft  $(rs)m = r(sm)$ ) und Rechts- $R$ -Moduln (mit der Eigenschaft  $(rs)m = s(rm)$ ). Entsprechend gibt es linksnoethersche Ringe und rechtsnoethersche Ringe.

**2.2.2 Beispiele** (*alles sieht so noethersch aus!*)

a) Der Ring  $\mathbb{Z}$  der ganzen Zahlen ist noethersch, wie überhaupt jeder Hauptidealring noethersch ist. Dazu gehören auch die Körper.

b) Ist  $R$  ein noetherscher Ring und  $\Phi : R \longrightarrow S$  ein surjektiver Ringhomomorphismus, so ist auch  $S$  noethersch. Denn für jedes Ideal  $I$  in  $S$  ist  $\Phi^{-1}(I)$  ein Ideal in  $R$  und somit endlich erzeugt. Die Bilder eines Erzeugendensystems von  $\Phi^{-1}(I)$  unter  $\Phi$  erzeugen aber  $\Phi(\Phi^{-1}(I)) = I$ .

c) Jede endlichdimensionale  $K$ -Algebra  $A$  über einem Körper  $K$  ist noethersch. Die Ideale in  $A$  sind ja insbesondere Untervektorräume, und als solche endlichdimensional über  $K$ . Also sind sie erst Recht als  $A$ -Moduln endlich erzeugt. Für so eine Algebra ist auch jeder endlich erzeugte Modul ein noetherscher  $A$ -Modul, und zwar aus demselben Grund.

Aber auch der Polynomring über einem Körper ist noethersch, er ist ja ein Hauptidealring.

### 2.2.3 Definition / Bemerkung (*exakte Sequenzen*)

Es seien  $R$  ein Ring und  $M_i, i \in \mathbb{Z}$ , ein paar  $R$ -Moduln. Weiterhin sei für jedes  $i \in \mathbb{Z}$  ein  $R$ -Modulhomomorphismus

$$\Phi_i : M_i \longrightarrow M_{i+1}$$

gegeben. Dann heißt die Sequenz

$$\dots \xrightarrow{\Phi_{i-1}} M_i \xrightarrow{\Phi_i} M_{i+1} \xrightarrow{\Phi_{i+1}} M_{i+2} \dots$$

eine *exakte Sequenz* von  $R$ -Moduln, wenn das Folgende für alle  $i$  gilt:

$$\text{Kern}(\Phi_{i+1}) = \text{Bild}(\Phi_i).$$

Anstelle von  $\mathbb{Z}$  kann hier auch der Durchschnitt von  $\mathbb{Z}$  mit einem reellen Intervall als Indexmenge dienen, wobei die Bedingung dann nur für alle  $i$  zu prüfen ist, für die sowohl  $i$  als auch  $i + 1$  als Index vorkommen.

Eine exakte Sequenz der Gestalt

$$0 \longrightarrow M \xrightarrow{\Phi} N \xrightarrow{\Psi} Q \longrightarrow 0$$

heißt eine *kurze exakte Sequenz* (*keS*). Das ist gleichbedeutend damit, dass  $\Phi$  injektiv ist,  $\text{Kern}(\Psi) = \text{Bild}(\Phi)$  gilt, und  $\Psi$  surjektiv ist. Man könnte dann auch  $M$  durch den isomorphen Modul  $\Phi(M)$  ersetzen,  $\Phi$  durch die Einbettung,  $Q$  durch  $N/\Phi(M)$  und  $\Psi$  durch die kanonische Abbildung.

Zum Beispiel ist für zwei Moduln  $M$  und  $Q$  die Sequenz

$$0 \longrightarrow M \xrightarrow{m \mapsto (m,0)} M \times Q \xrightarrow{(m,q) \mapsto q} Q \longrightarrow 0$$

eine kurze exakte Sequenz.

### 2.2.4 Hilfssatz (Sequenzen von noetherschen Moduln)

Es seien  $R$  ein Ring und  $M, N, Q$  drei  $R$ -Moduln. Weiterhin sei

$$0 \longrightarrow M \xrightarrow{\Phi} N \xrightarrow{\Psi} Q \longrightarrow 0$$

eine kurze exakte Sequenz von  $R$ -Moduln.

Dann ist  $N$  genau dann noethersch, wenn sowohl  $M$  als auch  $Q$  noethersch sind.

*Beweis.* Zunächst sei  $N$  noethersch. Wenn  $U \subseteq M$  ein Untermodul ist, dann ist  $U$  isomorph zu  $\Phi(U)$ , das ist ein Untermodul von  $N$ , also endlich erzeugt, und damit ist auch  $U$  endlich erzeugt, also  $M$  noethersch.

Wenn  $V$  ein Untermodul von  $Q$  ist, dann ist  $V = \Psi(\Psi^{-1}(V))$ , da  $\Psi$  surjektiv ist. Da  $N$  noethersch ist, wird  $\Psi^{-1}(V)$  von endlich vielen Elementen  $n_1, \dots, n_k$  erzeugt, aber dann ist  $V$  von  $\Psi(n_1), \dots, \Psi(n_k)$  erzeugt, und damit auch  $Q$  noethersch.

Sind umgekehrt  $M$  und  $Q$  noethersch und  $U$  ein Untermodul von  $N$ , dann ist  $\Phi^{-1}(U)$  ein Untermodul von  $M$  und damit endlich erzeugt. Es seien  $m_1, \dots, m_r$  endlich viele Erzeuger von  $\Phi^{-1}(U)$ . Weiterhin ist  $\Psi(U)$  ein Untermodul von  $Q$  und damit endlich erzeugt. Es seien  $q_1, \dots, q_s$  Erzeuger von  $\Psi(U)$  und  $u_1, \dots, u_s$  Urbilder von ihnen unter  $\Psi$ .

Nun sei  $u \in U$ . Dann lässt sich  $\Psi(u)$  schreiben als

$$\Psi(u) = \sum_{i=1}^s r_i q_i,$$

und damit liegt

$$u - \sum_{i=1}^s r_i u_i \in \text{Kern}(\Psi) \cap U = \Phi(\Phi^{-1}(U)).$$

Es gibt also  $a_1, \dots, a_r \in R$ , sodass

$$u - \sum_{i=1}^s r_i u_i = \sum_{j=1}^r a_j \Phi(m_j).$$

Damit haben wir ein endliches Erzeugendensystem von  $U$  gefunden, nämlich

$$\{\Phi(m_1), \dots, \Phi(m_r), u_1, \dots, u_s\}.$$

Da dies für jeden Untermodul  $U$  von  $N$  geht, ist  $N$  noethersch. ○

### 2.2.5 Hilfssatz

Es sei  $R$  ein linksnoetherscher Ring und  $M$  ein endlich erzeugter  $R$ -Linksmodul. Dann ist  $M$  noethersch.

*Beweis.* Es seien  $m_1, \dots, m_d$  Erzeuger von  $M$ . Dann ist die Abbildung

$$\Phi : R^d \longrightarrow M, \quad \Phi((a_i)) := a_1 m_1 + a_2 m_2 + \dots + a_d m_d,$$

ein surjektiver Morphismus von Links- $R$ -Moduln. Dann ist aber nach 2.2.4  $M$  noethersch, wenn  $R^d$  dies ist, was wiederum induktiv aus 2.2.4 folgt, es gibt ja eine offensichtliche kurze exakte Sequenz

$$0 \longrightarrow R \longrightarrow R^{d+1} \longrightarrow R^d \longrightarrow 0.$$

○

### 2.2.6 Satz (Hilberts Basissatz)

Es sei  $R$  ein kommutativer noetherscher Ring. Dann ist auch der Polynomring  $R[X]$  noethersch.

*Beweis.* Es sei  $I \subseteq R[X]$  ein Ideal. Wir müssen zeigen, dass es endlich erzeugt ist.

Für  $n \in \mathbb{N}_0$  definieren wir

$$C_n := \{r \in R \mid \exists f \in I : f = rX^n + \sum_{i=0}^{n-1} a_i X^i, a_i \in R\}.$$

Insbesondere ist  $C_n = \{0\}$ , wenn es kein Polynom vom Grad  $n$  in  $I$  gibt.

Die Multiplikation mit  $X$  führt  $I$  in sich über. Dies zeigt, dass

$$C_n \subseteq C_{n+1}.$$

Außerdem ist  $C_n$  für jedes  $n$  ein Ideal in  $R$ .

Damit ist auch die (aufsteigende) Vereinigung  $C_0 \cup C_1 \cup C_2 \cup \dots =: C$  ein Ideal in  $R$ . Da  $C$  als Ideal in  $R$  endlich erzeugt ist und diese endlich vielen Erzeuger schon in einem der  $C_n$  liegen müssen, gibt es ein  $N \in \mathbb{N}$ , sodass gilt:

$$\forall n \geq 0 : C_N = C_{N+1} = \dots = C_{N+n}.$$

Wir wählen ein großes  $K \in \mathbb{N}$ , sodass für  $0 \leq i \leq N$  das Ideal  $C_i$  von Elementen  $\alpha_{i,1}, \dots, \alpha_{i,K}$  erzeugt wird. Weiter wählen wir für jedes solche  $i$  und  $1 \leq j \leq K$  ein Polynom

$$f_{i,j} \in I : f_{i,j} = \alpha_{i,j} X^i + \text{niedrigere Terme.}$$

Dann gilt: Die Menge  $\{f_{i,j} \mid 0 \leq i \leq N, 1 \leq j \leq K\}$  ist ein Erzeugendensystem des Ideals  $I$ .

Um das einzusehen machen wir vollständige Induktion nach dem Grad von  $f \in I$ . Wenn  $f$  Grad  $\leq 0$  hat, dann ist es eine Konstante, liegt also in  $C_0$ , das als  $R$ -Modul von den Elementen  $f_{0,j} = \alpha_{0,j}$ ,  $1 \leq j \leq K$ , erzeugt wird.

Hat  $f$  Grad  $d > 0$ , so ist entweder  $d \leq N$ , und  $f$  lässt sich durch Subtraktion einer geeignete  $R$ -Linearkombination der  $f_{d,j}$ ,  $1 \leq j \leq K$ , zu einem Polynom kleineren Grades machen, das in  $I$  liegt und damit – nach Induktionsvoraussetzung – im  $R[X]$ -Modulerzeugnis der  $f_{i,j}$ .

Oder  $f$  hat Grad  $d > N$ ; dann lässt sich  $f$  durch Subtraktion des  $X^{d-N}$ -fachen einer  $R$ -Linearkombination der  $f_{N,j}$ ,  $1 \leq j \leq K$ , zu einem Polynom in  $I$  von kleinerem Grad machen, und damit auch zu einer  $R[X]$ -Linearkombination der  $f_{i,j}$ .  $\circ$

### 2.2.7 Folgerung (endlich erzeugte kommutative $R$ -Algebren)

Es sei  $R$  ein kommutativer noetherscher Ring und  $A$  eine (als Ring) endlich erzeugte kommutative  $R$ -Algebra. Dann ist auch  $A$  noethersch.

*Beweis.* Es sei

$$\{a_1, \dots, a_d\} \subseteq A$$

ein Erzeugendensystem, das heißt

$$A = \left\{ \sum_{i_1, \dots, i_d} r_{i_1, \dots, i_d} a_1^{i_1} \cdots a_d^{i_d} \mid r_{i_1, \dots, i_d} \in R, \text{ endliche Summe} \right\}.$$

Dann ist der Homomorphismus

$$\Phi : R[X_1, \dots, X_d] \longrightarrow A, \quad f(X_1, \dots, X_d) \mapsto f(a_1, \dots, a_d),$$

ein surjektiver Ringhomomorphismus.

Da aber  $R$  noethersch ist, ist es (dank Hilbert) auch  $R[X_1]$ , und damit auch  $R[X_1][X_2] = R[X_1, X_2]$ , und damit ... auch  $R[X_1, \dots, X_d]$ . Wegen 2.2.2b) ist auch  $A$  selbst noethersch.  $\circ$

### 2.2.8 Bemerkung/Definition (Kettenbedingung)

Im Beweis von Hilberts Basissatz haben wir benutzt (und begründet), dass eine aufsteigende Kette von Idealen in einem noetherschen Ring stationär wird. Genauer:

a) Es sei  $R$  ein Ring und  $M$  ein  $R$ -Modul. Weiter sei

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \dots$$

eine aufsteigende Folge von Untermoduln. Dann sagt man, diese Folge werde *stationär*, wenn es ein  $N \in \mathbb{N}$  gibt mit:

$$\forall k \geq N : U_k = U_N.$$

Der Modul erfüllt die *aufsteigende Kettenbedingung*, wenn jede aufsteigende Folge von Untermoduln stationär wird.

b) Analog gibt es die *absteigende Kettenbedingung*, die besagt, dass jede absteigende Folge von Untermoduln stationär wird.

c) Diese zwei Bedingungen lassen sich direkt auf beliebige geordnete Mengen übertragen. Statt zu sagen, sie erfüllten die aufsteigende Kettenbedingung, sagt man auch: sie sind *noethersch*. Statt zu sagen, sie erfüllten die absteigende Kettenbedingung, sagt man auch: sie sind *artinsch*.

Insbesondere haben wir jetzt eine neue Definition für noethersche Moduln und Ringe. Das ist aber nicht problematisch, denn die neue und die alte Definition stimmen überein, wie uns der folgende Hilfssatz lehrt.

### 2.2.9 Hilfssatz (*noethersch ist noethersch*)

Es sei  $R$  ein Ring und  $M$  ein Links- $R$ -Modul. Dann ist  $M$  genau dann linksnoethersch, wenn  $M$  die aufsteigende Kettenbedingung für Links- $R$ -Untermoduln erfüllt.

*Beweis.* Wenn  $M$  linksnoethersch ist und

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \dots$$

eine aufsteigende Folge von Links- $R$ -Untermoduln, dann ist die Vereinigung

$$U := \bigcup_{i \in \mathbb{N}} U_i$$

auch ein Links- $R$ -Untermodul von  $M$ , also endlich erzeugt. Wenn  $S \subseteq U$  ein endliches Erzeugendensystem ist, dann gibt es ein  $N \in \mathbb{N}$ , sodass bereits  $S \subseteq U_N$  gilt. Dann ist aber  $U_N = U$  und damit für alle  $K \geq N$  offensichtlich  $U_N = U_K$ .

Wenn umgekehrt  $M$  nicht noethersch ist, dann wählen wir einen Untermodul  $U \subseteq M$ , der nicht endlich erzeugt ist.

Mit seiner Hilfe konstruieren wir eine aufsteigende, nicht stationär werdende Folge von (endlich erzeugten) Links- $R$ -Untermoduln.

Wir wählen ein  $u_1 \in U$  und setzen  $U_1 := R \cdot u_1$ . Wenn  $U_i$  bereits definiert ist, so ist es ungleich  $U$ , da  $U_i$  endlich erzeugt ist. Wir wählen ein  $u_{i+1} \in U \setminus U_i$  und definieren  $U_{i+1}$  als den kleinsten Untermodul, der  $U_i$  und  $u_{i+1}$  enthält. Dieser wird von  $\{u_1, \dots, u_{i+1}\}$  erzeugt und ist ungleich  $U_i$ . Die Folge

$$U_1 \subset U_2 \subset U_3 \dots$$

lehrt, dass die aufsteigende Kettenbedingung in  $M$  verletzt ist. ○

### 2.2.10 Bemerkung (doch nicht alles noethersch!)

Es gibt tatsächlich Ringe, die nicht noethersch sind. Wenn zum Beispiel  $K$  ein Körper ist und  $X_1, X_2, \dots$  unendlich viele Unbestimmte über  $K$  sind, so gibt es den Polynomring

$$K[X_1, X_2, \dots].$$

Dieser ist nicht noethersch, denn wenn wir für  $n \in \mathbb{N}$  das Ideal  $I_n$  definieren als das von  $X_1, \dots, X_n$  erzeugte, so ist  $X_{n+1}$  nicht in  $I_n$  und damit

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

eine aufsteigende Folge von Idealen, die die aufsteigende Kettenbedingung verletzt.

## II.3 Bilineares

In diesem Abschnitt sei  $R$  immer ein kommutativer Ring. Wir werden verschiedene Gründe kennenlernen, bilineare Abbildungen zu untersuchen.

### 2.3.1 Definition/Beispiele (Bilineare Abbildung)

a) Es seien  $U, V, W$  drei  $R$ -Moduln. Eine *bilineare Abbildung*

$$\beta : U \times V \longrightarrow W$$

ist (wie in der LA) dadurch definiert, dass für alle  $r, s \in R, u_1, u_2 \in U, v_1, v_2 \in V$  gilt:

$$\beta(ru_1 + u_2, sv_1 + v_2) = rs\beta(u_1, v_1) + r\beta(u_1, v_2) + s\beta(u_2, v_1) + \beta(u_2, v_2).$$

b) An Beispielen kennen wir die aus der Linearen Algebra. In 2.1.1 haben wir schon die Bilinearität der Multiplikation in einer  $R$ -Algebra hingeschrieben. Für einen  $R$ -Modul  $M$  und für  $N := \text{Hom}_{R\text{-Mod}}(M, R)$  ist die Abbildung

$$\langle \cdot, \cdot \rangle : N \times M \longrightarrow R, \quad \langle \Phi, m \rangle := \Phi(m),$$

eine Bilinearform (das heißt: bilinear mit Werten im Grundring).

c) Wenn  $K$  ein Körper und  $A$  eine endlichdimensionale  $K$ -Algebra sind, dann ist die Abbildung

$$A \times A \longrightarrow K, \quad (a, b) \mapsto \text{Spur}_A(a \cdot b)$$

eine symmetrische Bilinearform auf  $A$ .

Wenn allgemeiner  $M$  ein endlichdimensionaler  $A$ -Modul ist,  $\rho : A \longrightarrow \text{End}_{K\text{-VR}}(M)$  der zugehörige Ringhomomorphismus, dann ist auch

$$T_\rho : A \times A \longrightarrow K, \quad T(a, b) := \text{Spur}_M(\rho(ab)),$$

eine symmetrische Bilinearform auf  $A$ .

### 2.3.2 Fragestellung/Definition (*Tensorprodukt kategoriell*)

Wir bezeichnen mit  $\text{Bil}(M \times N, V)$  die Menge aller bilinearen Abbildungen von  $M \times N$  nach  $V$ .

Für festes  $M, N$  ist dann durch  $\mathcal{B}(V) := \text{Bil}(M \times N, V)$  ein Funktor von  $\underline{R-Mod}$  nach  $\underline{Men}$  definiert. Dabei ist für einen  $R$ -Modulhomomorphismus  $\Phi : V \rightarrow W$  die Abbildung  $\mathcal{B}(\Phi)$  definiert, indem man für eine bilineare Abbildung  $\beta : M \times N \rightarrow V$  setzt:

$$\mathcal{B}(\Phi)(\beta) := \Phi \circ \beta.$$

Gesucht ist nun nach einem universellen Element für diesen Funktor, das heißt nach einem  $R$ -Modul  $T$  und einer bilinearen Abbildung

$$\otimes : M \times N \rightarrow T, \quad (m, n) \mapsto m \otimes n \in T,$$

sodass für alle bilinearen Abbildung  $\beta : M \times N \rightarrow V$  ein eindeutig bestimmter  $R$ -Modulhomomorphismus  $\Phi : T \rightarrow V$  existiert, für den

$$\beta = \Phi \circ \otimes$$

gilt.

Wenn es so einen Modul  $T$  gibt, dann heißt er ein *Tensorprodukt von  $M$  und  $N$* . Dieses Tensorprodukt ist dann bis auf einen Isomorphismus eindeutig bestimmt, und man schreibt dafür  $T =: M \otimes N$ . Genauer müsste man eigentlich sogar  $M \otimes_R N$  schreiben, was ich bisweilen tun werde.

### 2.3.3 Konstruktion (*Es gibt ein Tensorprodukt*)

Wir werden nun ein Tensorprodukt für zwei  $R$ -Moduln  $M$  und  $N$  konstruieren. Dazu sei erst einmal  $F$  der freie  $R$ -Modul mit Basis  $M \times N$ , wir schreiben Elemente von  $F$  als formale endliche Linearkombinationen

$$F = \left\{ \sum_{(m,n)} a_{(m,n)} \cdot (m, n) \mid a_{(m,n)} \in R, \text{ endliche Summe} \right\}.$$

Zwei solche formalen Linearkombinationen stimmen genau dann überein, wenn die Koeffizienten  $a_{(m,n)}$  für alle  $(m, n) \in M \times N$  übereinstimmen. Addition und skalare Multiplikation werden komponentenweise vorgenommen.

Die Abbildung

$$M \times N \ni (m, n) \mapsto (m, n) \in F$$

ist natürlich nicht bilinear. Um sie bilinear zu machen, müssen wir in  $F$  geeignete Relationen fordern. Dazu betrachten wir den Untermodul  $B$  von  $F$ , der von den Ausdrücken

$$(rm_1 + m_2, sn_1 + n_2) - rs(m_1, n_1) - r(m_1, n_2) - s(m_2, n_2) - (m_2, n_2)$$

mit  $r, s \in R, m_1, m_2 \in M, n_1, n_2 \in N$  erzeugt wird. Wir setzen

$$T := F/B, \quad \pi : F \longrightarrow F/B \quad \text{die kanonische Projektion.}$$

Dann ist

$$\otimes : M \times N \longrightarrow T, \quad (m, n) \mapsto \pi((m, n)),$$

eine bilineare Abbildung.

Wir müssen noch zeigen, dass  $T$  die universelle Abbildungseigenschaft hat. Dazu seien  $V$  ein  $R$ -Modul und  $\beta : M \times N \longrightarrow V$  irgendeine bilineare Abbildung. Dazu gibt es einen Modulhomomorphismus

$$\tilde{\Phi} : F \longrightarrow V, \quad \sum_{(m,n)} a_{(m,n)} \cdot (m, n) \mapsto \sum_{(m,n)} a_{(m,n)} \cdot \beta(m, n).$$

Da  $\beta$  bilinear ist, liegt  $B$  im Kern von  $\tilde{\Phi}$ , also faktorisiert  $\tilde{\Phi}$  über  $T = F/B$ , das heißt wir erhalten einen eindeutig bestimmten Modulhomomorphismus

$$\Phi : T \longrightarrow V, \quad \text{sodass } \tilde{\Phi} = \Phi \circ \pi.$$

Aber  $\Phi$  ist nun gerade so gemacht, dass

$$\beta = \Phi \circ \otimes$$

gilt. ○

### 2.3.4 Beispiele (für Tensorprodukte)

a) Für jeden  $R$ -Modul  $M$  gilt  $R \otimes_R M \simeq M$ .

b) Wenn  $M$  von  $\{m_i \mid i \in I\}$  und  $N$  von  $\{n_j \mid j \in J\}$  erzeugt werden, dann wird  $M \otimes_R N$  von der Menge  $\{m_i \otimes n_j \mid i \in I, j \in J\}$  erzeugt. Denn  $M = \{\sum_{i \in I} a_i m_i \mid a_i \in R, \text{ endliche Summe}\}$ , und  $N = \{\sum_{j \in J} b_j n_j \mid b_j \in R, \text{ endliche Summe}\}$ , und es gilt

$$m = \sum_{i \in I} a_i m_i, \quad n = \sum_{j \in J} b_j n_j \Rightarrow m \otimes n = \sum_{(i,j) \in I \times J} a_i b_j (m_i \otimes n_j).$$

Aber diese „Elementartensoren“ erzeugen  $M \otimes N$  nach Konstruktion.

c) Wenn  $\Phi : M \longrightarrow P$  und  $\Psi : N \longrightarrow Q$  zwei  $R$ -Modulhomomorphismen sind, dann ist die Abbildung

$$\beta : M \times N \longrightarrow P \otimes Q, \quad (m, n) \mapsto \Phi(m) \otimes \Psi(n),$$

bilinear. Sie induziert also einen Homomorphismus

$$\Phi \otimes \Psi : M \otimes N \longrightarrow P \otimes Q, \quad m \otimes n \mapsto \Phi(m) \otimes \Psi(n).$$

d) Wenn  $U$  ein Untermodul von  $M$  ist und  $\iota$  die Einbettung von  $U$  nach  $M$ , dann ist für jeden  $R$ -Modul  $N$

$$(M/U) \otimes N \simeq (M \otimes N) / (\iota \otimes \text{Id}_N)(U \otimes N).$$

Wieso? Übung!

### 2.3.5 Ringwechsel (*Ein Hochzeitsmärchen*)

Aus der linearen Algebra sieht man vielleicht ein, dass es manchmal sinnvoll ist, Aussagen über rationale Matrizen zu erhalten, indem man sie als reelle Matrizen auffasst, oder gar als komplexe. Dabei macht man implizit den rationalen Standardvektorraum zu einer Teilmenge des reellen Standardvektorraums (oder des komplexen). Wie man das ohne Basiswahl machen kann, lernt man durch die allgemeine Konstruktion des Ringwechsels (Skalarerweiterung).

Dazu seien  $R$  ein kommutativer Ring,  $M$  ein  $R$ -Modul und  $A$  eine  $R$ -Algebra. Dann ist  $A \otimes M$  erst einmal ein  $R$ -Modul.

Für jedes  $a \in A$  ist die Abbildung

$$\mu_a : A \times M \longrightarrow A \otimes M, \quad (t, m) \mapsto at \otimes m,$$

bilinear. Also gibt es eine eindeutig bestimmte  $R$ -lineare Abbildung

$$\tilde{\mu}_a : A \otimes M \longrightarrow A \otimes M, \quad \sum a_i \otimes m_i \mapsto \sum (aa_i) \otimes m_i.$$

Wir erhalten also insgesamt eine Abbildung

$$\tilde{\mu} : A \times (A \otimes M) \longrightarrow A \otimes M,$$

und man rechnet leicht nach, dass diese Abbildung aus  $A \otimes M$  einen  $A$ -Modul macht.

Wenn  $\Phi : M \longrightarrow N$  eine  $R$ -lineare Abbildung ist, dann ist die Abbildung

$$\tilde{\Phi} : A \times M \longrightarrow A \otimes N, \quad \tilde{\Phi}(a, m) := a \otimes \Phi(m),$$

bilinear, definiert also einen Modulhomomorphismus

$$\omega(\Phi) : A \otimes M \longrightarrow A \otimes N.$$

Man rechnet leicht nach, dass durch  $M \rightsquigarrow \omega(M) := A \otimes M$  und  $\Phi \rightsquigarrow \omega(\Phi)$  ein kovarianter Funktor  $\omega$  von  $\underline{R-Mod}$  nach  $\underline{A-Mod}$  definiert wird.

Man nennt diesen Funktor die *Skalarerweiterung* (oder *Ringerweiterung*) von  $R$  nach  $A$ .

### 2.3.6 Algebren unter sich

Wenn  $A$  und  $B$  zwei  $R$ -Algebren sind, dann ergibt sich analog zu 2.3.5, dass für feste  $a \in A, b \in B$  die Abbildung

$$\nu_{a,b} : A \times B \longrightarrow A \otimes B, \quad (x, y) \mapsto ax \otimes by,$$

bilinear ist, also eine Abbildung  $\tilde{\nu}_{a,b}$  von  $A \otimes B$  in sich selbst induziert. Für festes  $t \in A \otimes B$  ist aber auch

$$\nu^t : A \times B \longrightarrow A \otimes B, \quad (a, b) \mapsto \tilde{\nu}_{a,b}(t),$$

bilinear und definiert damit eine Abbildung  $\tilde{\nu}^t$  von  $A \otimes B$  nach  $A \otimes B$ .

Schließlich erhalten wir eine Abbildung

$$\nu : (A \otimes B) \times (A \otimes B) \longrightarrow A \otimes B, (s, t) \mapsto s \cdot t := \tilde{\nu}^t(s),$$

und man sieht, dass  $A \otimes B$  damit eine  $R$ -Algebra ist.

In der Kategorie der kommutativen  $R$ -Algebren ist  $A \otimes B$  das Koproduct von  $A$  und  $B$ . (Wieso? Übung!)

### 2.3.7 Hilfssatz (Assoziativität des Tensorprodukts)

Es seien  $L, M, N$  drei  $R$ -Moduln. Dann gibt es einen eindeutig bestimmten Isomorphismus von  $R$ -Moduln

$$\Phi : (L \otimes M) \otimes N \longrightarrow L \otimes (M \otimes N),$$

der für alle  $l \in L, m \in M, n \in N$  die Vorgabe

$$\Phi((l \otimes m) \otimes n) = l \otimes (m \otimes n)$$

erfüllt.

*Beweis.* Für festes  $n \in N$  ist die Abbildung

$$\psi_n : L \times M \longrightarrow L \otimes (M \otimes N), \quad \psi_n(l, m) := l \otimes (m \otimes n),$$

bilinear. Also gibt es einen eindeutig bestimmten Modulhomomorphismus

$$\Psi_n : L \otimes M \longrightarrow L \otimes (M \otimes N) \quad \text{mit} \quad \Psi_n(l \otimes m) = l \otimes (m \otimes n).$$

Die Abbildung

$$\psi : (L \otimes M) \times N \longrightarrow L \otimes (M \otimes N), \quad \psi(x, n) := \Psi_n(x),$$

ist bilinear, und deshalb gibt es einen eindeutig bestimmten  $R$ -Modulhomomorphismus

$$\Phi : (L \otimes M) \otimes N \longrightarrow L \otimes (M \otimes N) \quad \text{mit} \quad \Phi((l \otimes m) \otimes n) = l \otimes (m \otimes n).$$

Es ist klar, dass man analog einen Homomorphismus

$$\tilde{\Phi} : L \otimes (M \otimes N) \longrightarrow (L \otimes M) \otimes N \quad \text{mit} \quad \tilde{\Phi}(l \otimes (m \otimes n)) = (l \otimes m) \otimes n$$

erhält, und dass  $\Phi$  und  $\tilde{\Phi}$  zueinander invers sind.

Die Eindeutigkeit von  $\Phi$  folgt daraus, dass  $(L \otimes M) \otimes N$  von den Elementen  $(l \otimes m) \otimes n$  erzeugt wird. ○

### 2.3.8 Konstruktion (die Tensoralgebra)

a) Für einen  $R$ -Modul  $M$  definieren wir rekursiv  $M^{\otimes n}$  durch

$$M^{\otimes 0} := R, M^{\otimes n+1} := M \otimes M^{\otimes n}.$$

Wir bilden die direkte Summe dieser  $R$ -Moduln:

$$T(M) := \bigoplus_{n=0}^{\infty} M^{\otimes n}.$$

Ein typisches Element dieser Menge ist eine endliche Summe von Ausdrücken der Gestalt  $r \cdot (m_1 \otimes m_2 \otimes \cdots \otimes m_n)$  mit  $r \in R$  und  $m_1, \dots, m_n \in M$ . Ähnlich wie in 2.3.6 zeigt man, dass die Abbildung

$$M^{\otimes k} \times M^{\otimes l} \ni (x, y) \mapsto x \otimes y \in M^{\otimes(k+l)}$$

für alle  $k, l \in \mathbb{N}_0$  wohldefiniert ist. Durch bilineare Fortsetzung erhalten wir eine Abbildung

$$T(M) \times T(M) \longrightarrow T(M).$$

Diese Abbildung verwenden wir als Multiplikation auf  $T(M)$ , das dadurch zu einer  $R$ -Algebra wird. Die Assoziativität erhalten wir wieder aus 2.3.7.

Wenn  $A$  irgendeine  $R$ -Algebra ist und  $\varphi : M \longrightarrow A$  eine  $R$ -lineare Abbildung, dann setzt sich diese auf eindeutig bestimmte Art zu einem  $R$ -Algebren Homomorphismus  $\Phi : T(M) \longrightarrow A$  fort. Dies liefert eine Bijektion

$$\eta_{M,A} : \text{Hom}_{R\text{-Mod}}(M, A) \longrightarrow \text{Hom}_{R\text{-Alg}}(T(M), A),$$

denn  $T(M)$  wird als Algebra ja von  $M$  erzeugt. Diese Bijektionen zeigen, dass die Funktoren ( $A$  als  $R$ -Algebra)  $\rightsquigarrow$  ( $A$  als  $R$ -Modul) und  $M \rightsquigarrow T(M)$  zueinander adjungiert sind.

b) Beispiel: Es sei  $M$  ein freier  $R$ -Modul vom Rang 1, das heißt:  $M$  hat eine Basis aus einem Element:  $\{b\}$ .

Dann ist  $M^{\otimes n} = R \cdot b^{\otimes n}$  auch jeweils frei, und die Definition des Produkts in  $T(M) = \bigoplus R \cdot b^{\otimes n}$  ist gegeben durch

$$\sum_i r_i b^{\otimes i} \cdot \sum_j s_j b^{\otimes j} = \sum_k \left( \sum_{0 \leq i \leq k} r_i s_{k-i} \right) b^{\otimes k}.$$

Wir erhalten ein neues Modell des Polynomrings in einer Variablen.

Wenn wir einen freien Modul von höherem Rang verwenden, dann bekommen wir einen nichtkommutativen Ring, und nicht direkt den Polynomring in mehreren Variablen. Wenn  $\{b_1, \dots, b_n\} =: B$  eine Basis von  $M$  ist, dann ist  $T(M)$  isomorph zur freien  $R$ -Algebra  $R\{B\}$ , siehe 2.1.3. Beide  $R$ -Algebren stellen den Funktor  $A \rightsquigarrow \text{Hom}_{\text{Mengen}}(B, A)$  dar.

Ähnlich wie der Polynomring für kommutative Ringe lässt sich diese Tensoralgebra benutzen, um beliebige (nicht nur endlich erzeugte)  $R$ -Algebren durch Quotientenbildung zu erhalten. Allerdings ist diese Tensoralgebra manchmal nicht sehr „benutzerfreundlich“.

### 2.3.9 Zwei Beispiele (*Clifford-Algebren und noch eine*)

a) Es seien  $K$  ein Körper mit Charakteristik  $\neq 2$ ,  $V$  ein endlichdimensionaler Vektorraum, und  $q$  eine quadratische Form auf  $V$ , d.h. es gibt eine symmetrische Bilinearform  $\beta$  auf  $V$  mit  $q(v) = \beta(v, v)$  für alle  $v \in V$ .

Weiter sei  $A$  eine  $K$ -Algebra und  $\Phi : V \rightarrow A$  eine  $K$ -lineare Abbildung, sodass für alle  $v \in V$  gilt:

$$\Phi(v)^2 = \beta(v) \cdot 1_A.$$

Schließlich sei  $C(q)$  die  $K$ -Algebra, die sich ergibt, indem aus der Tensoralgebra  $T(V)$  das zweiseitige Ideal  $I$  herausgeteilt wird, das von den Ausdrücken  $v \otimes v - q(v)$  erzeugt wird. Die offensichtliche Abbildung  $V \ni v \mapsto v + I \in C(q)$  erfüllt dann auch die Bedingung

$$(v + I)^2 = q(v) \cdot 1_{C(q)}.$$

$\Phi$  induziert einen Algebrenhomomorphismus  $T(V) \rightarrow A$  wie in 2.3.8, und wegen der Bedingung an  $\Phi$  ist  $I$  im Kern von diesem Algebrenhomomorphismus enthalten. Also erhalten wir einen Algebrenhomomorphismus  $\Psi : C(q) \rightarrow A$ , sodass für alle  $v \in V$  gilt:

$$\Phi(v) = \Psi(v + I).$$

Die Algebra  $C(q)$  zusammen mit der Abbildung  $v \mapsto v + I$  erfüllt also eine universelle Eigenschaft. (Was ist der zugehörige Funktor?) Sie heißt die *Cliffordalgebra* zur quadratischen Form  $q$ .

Wenn etwa  $V = K$  ist und  $q(v) = dv^2$ , dann ist  $C(V) = K[x]/(x^2 - d)$ , das sieht man direkt an der Konstruktion.

Wenn  $V = K^2$  gilt und die quadratische Form  $q$  durch  $q(v, w) := av^2 + bw^2$  gegeben ist, dann gilt für die Standardbasis  $I := e_1, J := e_2$  in  $C(q)$ :

$$I^2 = a, J^2 = b, (I + J)^2 = a + b.$$

Dies impliziert  $IJ = -JI$ , und für dieses Element gilt

$$(IJ)^2 = IJIJ = -(IIJJ) = -ab.$$

Da  $C(q)$  als Algebra von  $I$  und  $J$  erzeugt wird, und da sich jedes Wort in  $I$  und  $J$  modulo der Relationen in  $C(q)$  auf ein Wort der Länge  $\leq 2$  reduzieren lässt, hat  $C(q)$  als  $K$ -Basis die Elemente  $1, I, J, IJ$ .  $C(q)$  ist die zu  $a$  und  $b$  gehörige Quaternionenalgebra.

Jetzt können wir Quaternionenalgebren etwas flexibler definieren: eine Quaternionenalgebra ist die Cliffordalgebra zu einer nicht ausgearteten quadratischen Form auf einem zweidimensionalen Vektorraum. Die Theorie der quadratischen Formen sagt (mittels eines leicht modifizierten E. Schmidt-Verfahrens), dass jede nicht ausgeartete quadratische Form zu einer „Diagonaleform“ äquivalent ist. Eine feinere Klassifikation ist im Allgemeinen schwierig; für interessante Körper kennt man das natürlich.

b) Nun sei  $M = \mathbb{Z}^2$  und  $T(M)$  die Tensoralgebra davon. Sie wird frei erzeugt von einer Basis  $\{x, y\}$  von  $M$ . Wir betrachten in  $T(M)$  das zweiseitige Ideal  $I$ , das von  $\{xy, yy\}$  erzeugt wird. Dann ist der (nicht-kommutative!) Ring

$$T(M)/I \cong \mathbb{Z}[x] \oplus \curvearrowright \mathbb{Z}[x].$$

Mit Multiplikation von Rechts wird ist das ein endlich erzeugter  $\mathbb{Z}[x]$ -Modul.

Wenn  $J$  ein Rechtsideal hierin ist, dann ist es insbesondere auch ein Rechts- $\mathbb{Z}[x]$ -Untermodul, und damit als solcher endlich erzeugt, weil  $\mathbb{Z}[x]$  noethersch ist. Also ist  $T(M)/I$  rechtsnoethersch.

Hingegen ist die Kette

$$\mathbb{Z}y \subseteq \mathbb{Z}y \oplus \mathbb{Z}yx \subseteq \mathbb{Z}y \oplus \mathbb{Z}yx \oplus \mathbb{Z}yx^2 \subseteq \dots$$

eine aufsteigende Folge von  $T(M)/I$ -Linksidealien, die nicht stationär wird. Also ist  $T(M)/I$  nicht linksnoethersch.

## II.4 Ordnung und Ganzheit

Ausgehend von Ordnungen in endlichdimensionalen  $\mathbb{Q}$ -Algebren wollen wir die algebraische Theorie der Ganzheit entwickeln.

### 2.4.1 Definition (*Ordnung*)

Es sei  $A$  eine endlichdimensionale  $\mathbb{Q}$ -Algebra. Eine *Ordnung* in  $A$  ist ein Teilring  $\mathcal{O} \subseteq A$ , der als  $\mathbb{Z}$ -Modul endlich erzeugt ist und der eine  $\mathbb{Q}$ -Basis von  $A$  enthält.

### 2.4.2 Bemerkung / Beispiele (*Matrizen und so weiter*)

a) Im Matrizenring  $\mathbb{Q}^{d \times d}$  gibt es mindestens eine Ordnung, nämlich  $\mathbb{Z}^{d \times d}$ .

Da jede  $d$ -dimensionale Algebra  $A$  sich auffassen lässt als Teilalgebra von  $\mathbb{Q}^{d \times d}$ , findet sich auch in  $A$  eine Ordnung, nämlich

$$\mathcal{O} := A \cap \mathbb{Z}^{d \times d}.$$

Es gibt also in jeder endlichdimensionalen  $\mathbb{Q}$ -Algebra mindestens eine Ordnung.

b) Eine Ordnung  $\mathcal{O}$  in einer  $\mathbb{Q}$ -Algebra ist immer eine Untergruppe des Vektorraums  $A$ , also torsionsfrei. Da  $\mathcal{O}$  auch endlich erzeugt ist, greift der Struktursatz für endlich erzeugte abelsche Gruppen:  $\mathcal{O}$  ist eine freie abelsche Gruppe.

Da  $\mathcal{O}$  eine Basis von  $A$  enthält, ist der Rang mindestens so groß wie die Dimension  $d$  von  $A$ . Umgekehrt sind mehr als  $d$  Element aus  $A$  immer  $\mathbb{Q}$ -linear abhängig, und diese Abhängigkeit lässt sich ganz machen durch Multiplikation mit einem gemeinsamen Nenner der Koeffizienten. Also ist der Rang von  $\mathcal{O}$  genau gleich  $d$  und es gibt eine Basis  $\{b_1, \dots, b_d\}$  von  $A$ , sodass gilt:

$$\mathcal{O} = \mathbb{Z}b_1 \oplus \dots \oplus \mathbb{Z}b_d.$$

Da dies ein Ring sein soll, muss das Produkt zweier Basisvektoren eine ganzzahlige Linearkombination von Basisvektoren sein:

$$\forall i, j : \exists c_{ijk} \in \mathbb{Z} : b_i \cdot b_j = \sum_{k=1}^d c_{ijk} b_k.$$

c) Nun sei  $x \in \mathcal{O}$  für eine Ordnung  $\mathcal{O}$  der  $d$ -dimensionalen  $\mathbb{Q}$ -Algebra  $A$ . Beschreibt man die Multiplikation mit  $x$  bezüglich einer Basis der Ordnung, so erhält man eine ganzzahlige Abbildungsmatrix. Dann sagen Hamilton und Cayley unisono, dass  $x$  als Nullstelle des charakteristischen Polynoms dieser Matrix ein normiertes ganzzahliges Polynom als annullierendes Polynom hat.

Diese Eigenschaft werden wir in Kürze Ganzheit nennen.

d) Die einzige Ordnung in  $\mathbb{Q}$  ist  $\mathbb{Z}$ . Denn eine Ordnung muss ja die 1 enthalten, also sicherlich  $\mathbb{Z}$  umfassen; und wenn ein echter Bruch  $p/q$  in der Ordnung liegt, dann auch alle Potenzen davon, aber deren Nenner wären dann unbeschränkt, und damit wäre die Ordnung nicht endlich erzeugt als  $\mathbb{Z}$ -Modul.

Alternativ: Wenn  $q \in \mathbb{Q}$  eine Nullstelle eines normierten ganzzahligen Polynoms  $f$  ist, dann ist  $q$  selbst ganz.

e) Nun seien  $\zeta \in \mathbb{C}$  eine primitive  $n$ -te Einheitswurzel und  $K = \mathbb{Q}(\zeta)$  der zugehörige Kreisteilungskörper. Da  $\zeta$  eine Nullstelle von  $X^n - 1$  ist, ist  $\mathbb{Z}[\zeta]$  als abelsche Gruppe von  $1, \zeta, \dots, \zeta^{n-1}$  erzeugt, worin eine Basis von  $K$  liegt. Daher ist  $\mathbb{Z}[\zeta]$  eine Ordnung in  $K$ . Jede Ordnung von  $K$  ist darin enthalten, aber das zu zeigen ist etwas aufwändiger.

f)  $\mathbb{R} \otimes_{\mathbb{Q}} A$  ist eine endlichdimensionale  $\mathbb{R}$ -Algebra. Insbesondere ist das ein endlichdimensionaler reeller Vektorraum, und darauf kann man Normen betrachten. All diese Normen induzieren dieselbe Topologie auf  $\mathbb{R} \otimes_{\mathbb{Q}} A$ , und bezüglich dieser Topologie ist  $\{1 \otimes z \mid z \in \mathcal{O}\}$  eine diskrete Untergruppe von  $\mathbb{R} \otimes_{\mathbb{Q}} A$ . Auf diese Art lassen sich geometrische Argumente ins Rechnen mit Algebren einbeziehen. Das ist der Ursprung der „Geometrie der Zahlen“, die etwa in der algebraischen Zahlentheorie Anwendung findet im Rahmen der Minkowski-Theorie.

### 2.4.3 Definition (*Diskriminante, Maximalordnung*)

a) Auf jeder endlichdimensionalen  $\mathbb{Q}$ -Algebra  $A$  gibt es die Spurform

$$A \times A \ni (a, b) \mapsto \text{Spur}(ab).$$

Diese Bilinearform ist symmetrisch. Wenn  $\mathcal{O} \subseteq A$  eine Ordnung ist, so wählen wir eine Basis  $\{b_1, \dots, b_n\}$  von  $\mathcal{O}$ , und betrachten die zugehörige Fundamentalmatrix der Spurform:

$$F := (\text{Spur}(b_i b_j))_{1 \leq i, j}.$$

Dies ist eine ganzzahlige Matrix, denn die Multiplikation mit  $b_i b_j$  beschreibt sich durch eine ganzzahlige Matrix bezüglich der gewählten Basis. Die Determinante von  $F$  heißt die *Diskriminante* von  $\mathcal{O}$ . Sie ist wohldefiniert, da eine andere Basis von  $\mathcal{O}$  aus der gewählten durch eine ganzzahlige Basiswechselmatrix mit Determinante  $\pm 1$  hervorgeht.

Die Spurform heißt *nicht ausgeartet*, wenn die Diskriminante nicht 0 ist. Hierbei könnte man auch die Fundamentalmatrix der Spurform bezüglich einer beliebigen anderen Basis nehmen. Äquivalent dazu ist auch, dass es zu jedem  $a \in A \setminus \{0\}$  ein  $b \in A$  gibt mit  $\text{Spur}(ab) \neq 0$ .

b) Eine Ordnung  $\mathcal{O}$  von  $A$  heißt eine *Maximalordnung* von  $A$ , wenn sie in keiner größeren Ordnung enthalten ist. (Etwas pathetisch könnte man sagen, sie sei nicht zur Unterordnung fähig.)

### 2.4.4 Beispiel

Es sei  $A$  der Ring der rationalen  $d \times d$ -Matrizen. Darin betrachten wir die Ordnung  $\mathcal{O}$ , die aus den ganzzahligen Matrizen besteht. Sie hat als Basis die Menge  $B$  der Elementarmatrizen  $E_{ij}$ ,  $1 \leq i, j \leq d$ . Was ist hiervon die Diskriminante?

Für zwei Elementarmatrizen  $E_{i,j}$  und  $E_{k,l}$  gilt:

$$E_{i,j} \cdot E_{k,l} = \begin{cases} E_{i,l} & \text{falls } j = k, \\ 0 & \text{sonst.} \end{cases}$$

Die Spur von  $E_{i,l}$  wiederum ist  $d$ , wenn  $i = l$  ist, und sonst 0. Wenn  $i \neq l$  gilt, dann ist  $E_{i,l}^2 = 0$ , also die Multiplikation mit  $E_{i,l}$  nilpotent, und ansonsten ist die Multiplikation mit  $E_{i,i}$  eine Projektion auf den Raum aller Matrizen, die außerhalb der  $i$ -ten Zeile 0 sind.

Damit ist die Fundamentalmatrix der Spurform bezüglich  $B$  gegeben durch  $d \cdot P$ , wobei  $P$  die Matrix ist, die die Transposition als lineare Abbildung von  $A$  nach  $A$  beschreibt.

$P$  ist diagonalisierbar, und die Eigenwerte sind 1 und  $-1$ . Die zugehörigen Eigenräume sind die Räume der symmetrischen bzw. antisymmetrischen Matrizen und haben Dimension  $d(d+1)/2$  bzw.  $d(d-1)/2$ .

Das zeigt, dass die Diskriminante von  $\mathcal{O}$  die Zahl

$$(-1)^{d(d-1)/2} \cdot d^{d^2}$$

ist.

#### 2.4.5 Hilfssatz (*manchmals gibt es eine Maximalordnung*)

Es seien  $A$  eine endlichdimensionale  $\mathbb{Q}$ -Ordnung, deren Spurform nicht ausgeartet ist, und  $\mathcal{O}$  eine Ordnung in  $A$ . Dann ist  $\mathcal{O}$  in einer Maximalordnung von  $A$  enthalten.

*Beweis.* Wenn  $\mathcal{O}$  noch nicht maximal ist, dann ist es enthalten in einer größeren Ordnung  $\tilde{\mathcal{O}}$ , und hat darin endlichen Index  $m$ . Dann gilt für die Diskriminanten  $D$  und  $\tilde{D}$  dieser Ordnungen:

$$\tilde{D} = D/m^2,$$

denn aus einer Basis von  $\tilde{\mathcal{O}}$  macht man eine Basis von  $\mathcal{O}$  durch eine ganzzahlige Basiswechsellmatrix mit Determinante  $\pm m$ . (Hier darf man entweder geometrisch argumentieren: Determinanten sind Volumina und Indizes irgendwie auch; oder algebraisch: über den Elementarteilersatz.)

Da aber alle Zahlen ganz und nicht Null sind (hier brauche ich, dass die Spurform nicht ausgeartet ist), kann man  $\mathcal{O}$  nur endlich oft vergrößern und gelangt auf diese Art schließlich zu einer Maximalordnung.  $\circ$

#### 2.4.6 Beispiele

a) Wenn die Diskriminante einer Ordnung quadratfrei ist, dann ist die Ordnung maximal, wie man am Beweis von 2.4.5 sieht.

b) Der Matrizenring  $\mathbb{Q}^{d \times d}$  besitzt eine Maximalordnung. Zum Beispiel ist  $\mathbb{Z}^{d \times d}$  eine Maximalordnung. Wenn nämlich  $\tilde{\mathcal{O}}$  eine Maximalordnung ist, die die ganzzahligen Matrizen umfasst, und wenn die Matrix  $M = (a_{ij}) \in \tilde{\mathcal{O}}$  nicht ganzzahlig wäre, dann kann man durch Multiplikation mit Permutationsmatrizen (die ganzzahlig sind) erzwingen, dass zum Beispiel  $a_{11}$  nicht ganzzahlig ist. Dann ist aber auch  $E_{11} \cdot M \cdot E_{11} = a_{11}E_{11} \in \tilde{\mathcal{O}}$ . Diese Matrix hat aber kein ganzzahliges charakteristisches Polynom, und ist damit nicht in einer Ordnung enthalten.

Für jede invertierbare Matrix  $M$  ist  $M\mathbb{Z}^{d \times d}M^{-1}$  ebenfalls eine Maximalordnung in  $\mathbb{Q}^{d \times d}$ , Maximalordnungen sind also meistens nicht eindeutig bestimmt.

c) Wenn  $K$  eine endliche Körpererweiterung von  $\mathbb{Q}$  ist, dann ist die Spurform nicht ausgeartet: es gibt zu  $x \in K \setminus \{0\}$  ein  $y \in K$ , sodass  $xy$  von 0 verschiedene Spur hat, zum Beispiel  $y = x^{-1}$ . Daher gibt es in  $K$  eine Maximalordnung. Wir werden später sehen, dass diese eindeutig bestimmt ist. Sie heißt der Ganzheitsring von  $K$  und spielt eine übergeordnete Rolle in der algebraischen Zahlentheorie.

d) Die Algebra  $A := \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\}$  enthält für jedes  $q \in \mathbb{Q}$  die Ordnung

$$\mathcal{O}_q := \left\{ \begin{pmatrix} a & bq \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}.$$

Jede Ordnung von  $A$  ist in einer solchen enthalten. Daher besitzt  $A$  keine Maximalordnung. Tatsächlich ist die Spurform von  $A$  bezüglich der Basis  $B := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \right\}$  durch die Fundamentalmatrix

$$F = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$$

beschrieben, ist also ausgeartet.

#### 2.4.7 Definition (*Ganzheit*)

Es seien  $R$  ein kommutativer Ring und  $S$  eine  $R$ -Algebra.

- a) Ein Element  $s \in S$  heißt *ganz über  $R$* , falls ein normiertes Polynom  $f \in R[X]$  existiert mit  $f(s) = 0$ .
- b) Wenn  $S$  kommutativ ist, so heißt die Menge aller über  $R$  ganzen Elemente in  $S$  der *ganze Abschluss* von  $R$  in  $S$ .
- c) Wenn  $R$  nullteilerfrei ist und  $S$  der Quotientenkörper von  $R$ , so heißt  $R$  *ganz abgeschlossen*, wenn der ganze Abschluss von  $R$  in  $S$  gleich  $R$  ist. Beispielsweise Hauptidealringe sind ganz abgeschlossen.
- d) Eine Ringerweiterung  $R \subseteq S$  heißt *ganz*, wenn jedes Element von  $S$  ganz über  $R$  ist.

#### 2.4.8 Hilfssatz (*Kriterium der Ganzheit*)

Es seien  $R$  ein kommutativer Ring und  $S$  eine  $R$ -Algebra. Dann sind für  $s \in S$  äquivalent:

- a)  $s$  ist ganz über  $R$ .
- b) Die Unteralgebra  $R[s]$  von  $S$  ist als  $R$ -Modul endlich erzeugt.
- c)  $R[s]$  ist in einer Unteralgebra  $A$  von  $S$  enthalten, die als  $R$ -Modul endlich erzeugt ist.

*Beweis:*

a)  $\Rightarrow$  b)

Es sei  $f(X) = X^d + \sum_{i=0}^{d-1} r_i X^i$  ein Polynom, wie es nach Voraussetzung existiert: normiert mit  $f(s) = 0$ . Dann gilt:

$$R[s] = \left\{ \sum_{i=0}^{d-1} a_i s^i \mid a_i \in R \right\}.$$

Die Inklusion  $\supseteq$  ist hierbei klar, die andere Inklusion folgt, da  $s^d, s^{d+1}, \dots$  sich induktiv durch kleinere Potenzen von  $s$  ausdrücken lassen, die linker Hand enthalten sind.

b)  $\Rightarrow$  c) sollte klar sein.

c)  $\Rightarrow$  a)

Es sei  $m_1, \dots, m_d$  ein endliches Erzeugendensystem des  $R$ -Moduls  $A$ . Die ( $R$ -lineare!) Multiplikation mit  $s$  ist dann auf  $A$  gegeben durch

$$s \cdot m_j = \sum_{i=0}^d a_{ij} m_j, \quad a_{ij} \in R.$$

Wir machen den freien  $R$ -Modul  $R^d$  zu einem  $R[X]$ -Modul, indem wir  $X$  als Multiplikation mit  $D := (a_{ij})$  wirken lassen. Außerdem machen wir  $A$  zu einem  $R[X]$ -Modul, indem wir  $X$  als Multiplikation mit  $s$  wirken lassen. Dann ist die Abbildung

$$\pi : R^d \longrightarrow A, \quad (r_i) \mapsto \sum_i r_i m_i$$

ein surjektiver Homomorphismus von  $R[X]$ -Moduln. Da das charakteristische Polynom von  $D$  den Modul  $R^d$  annulliert, muss es auch  $R[s]$  annullieren. Das aber heißt, dass  $s$  eine Nullstelle davon ist.

Aber das charakteristische Polynom von  $D$  ist ein normiertes Polynom in  $R[X]$ . Daher ist  $s$  ganz über  $R$ .  $\circ$

#### 2.4.9 Folgerung (Der ganze Abschluss)

Es sei  $R$  ein kommutativer Ring und  $S$  eine kommutative  $R$ -Algebra. Dann ist der ganze Abschluss von  $R$  in  $S$  eine Teilalgebra von  $S$ .

*Beweis.* Es seien  $s, t \in S$  ganz über  $R$ . Dann ist  $t$  auch ganz über  $R[s]$ , (an dieser Stelle geht ein, dass  $S$  kommutativ ist). Also ist  $R[s, t]$  als  $R[s]$ -Modul endlich erzeugt, und damit auch als  $R$ -Modul, denn  $R[s]$  ist endlich erzeugter  $R$ -Modul. Damit liegen  $st$  und  $s + t$  in einem endlich erzeugten  $R$ -Modul, der eine Algebra ist, sind also ganz über  $R$ . Das zeigt die Behauptung.  $\circ$

#### 2.4.10 Folgerung (Der Ganzheitsring)

Es sei  $K$  eine endliche Körpererweiterung von  $\mathbb{Q}$ . Dann ist der ganze Abschluss von  $\mathbb{Z}$  in  $K$  die eindeutig bestimmte Maximalordnung  $\mathcal{O}$  in  $K$ .

*Beweis.* Es seien  $R$  der ganze Abschluss von  $\mathbb{Z}$  in  $K$ , und  $\mathcal{O}$  eine Maximalordnung. Dann ist  $\mathcal{O}$  in  $R$  enthalten (wegen 2.4.2 c)). Wenn  $r \in R$  liegt, so ist es ganz über  $\mathbb{Z}$  und damit auch ganz über  $\mathcal{O}$ . Daher ist  $\mathcal{O}[r]$  ein endlich erzeugter  $\mathcal{O}$ -Modul und (da  $\mathcal{O}$  endlich erzeugter  $\mathbb{Z}$ -Modul ist) auch endlich erzeugter  $\mathbb{Z}$ -Modul. Daher ist  $\mathcal{O}[r]$  eine Ordnung, folglich  $r \in \mathcal{O}$ , da dies eine Maximalordnung ist.

Es folgt  $R = \mathcal{O}$ . Daher kann es auch nur eine Maximalordnung geben.  $\circ$

## II.5 Darstellungstheorie endlicher Gruppen

In diesem Abschnitt wollen wir die grundlegenden Aussagen aus der Darstellungstheorie der endlichen Gruppen herleiten. Wir kennen schon einige Definitionen (siehe 2.1.12), und den Satz von Maschke sowie das Lemma von Schur (2.1.11, 2.1.13).

### 2.5.1 Definition (*Der Darstellungsring*)

Es seien  $K$  ein Körper und  $G$  eine endliche Gruppe. Wir bezeichnen die Menge aller Isomorphieklassen von endlichdimensionalen  $K[G]$ -Moduln mit  $\mathcal{H}_K(G)$ . Wenn  $V, W$  zwei Darstellungen von  $G$  sind, dann operiert  $G$  auch auf  $V \oplus W := \{(v, w) \mid v \in V, w \in W\}$  vermöge

$$g \bullet (v, w) := (gv, gw)$$

und auf  $V \otimes_K W$  vermöge

$$g \bullet (v \otimes w) := gv \otimes gw.$$

Das heißt: Darstellungen lassen sich addieren und multiplizieren. Natürlich ist dies mit dem Bilden der Isomorphieklassen verträglich. Damit haben wir auf  $\mathcal{H}_K(G)$  die Struktur eines Halbrings (insbesondere ist das Multiplizieren assoziativ: siehe 2.3.7). Das Distributivgesetz folgt aus den Regeln des Tensorrechnens.

Das Einselement ist die triviale eindimensionale Darstellung, das Nullelement ist die nulldimensionale Darstellung.

Durch Einführung von formalen inversen (wie von  $\mathbb{N}$  nach  $\mathbb{Z}$ ) bezüglich der Addition macht man aus  $\mathcal{H}_K(G)$  einen Ring:

$$\mathcal{R}_K(G) := (\mathcal{H}_K(G) \times \mathcal{H}_K(G)) / \sim,$$

wobei  $(\rho_1, \rho_2) \sim (\sigma_1, \sigma_2) : \iff \exists \pi : \pi \oplus \sigma_2 \oplus \rho_1 \cong \pi \oplus \sigma_1 \oplus \rho_2$ . (Das ist eine Äquivalenzrelation...)

Wir schreiben dann auch  $\rho_1 - \rho_2$  für die Äquivalenzklasse von  $(\rho_1, \rho_2)$ . So etwas ist eine *virtuelle Darstellung*. Die Dimension einer virtuellen Darstellung ist  $\dim_K(V_1) - \dim_K(V_2)$ , wobei  $V_1$  und  $V_2$  die  $K$ -Vektorräume sind, die als Darstellungsräume für  $\rho_1$  und  $\rho_2$  dienen. Diese Dimension ist auf den Äquivalenzklassen wohldefiniert, und  $\dim$  ist ein Ringhomomorphismus von  $\mathcal{R}_K(G)$  nach  $\mathbb{Z}$ .

Die Abbildung

$$\mathcal{H}_K(G) \ni \rho \mapsto (\rho, 0)_{\sim} \in \mathcal{R}_K(G)$$

muss im Allgemeinen nicht injektiv sein.

Dafür bräuchte man eine Kürzungsregel in  $\mathcal{H}_K(G)$ , die gilt, wenn die Charakteristik von  $K$  kein Teiler der Gruppenordnung ist. *Das setzen wir nun voraus.*

In diesem Fall ist ja jede endlichdimensionale Darstellung eine direkte Summe von irreduziblen, und diese Zerlegung ist eindeutig. Es gibt nur endlich viele Isomorphieklassen von irreduziblen Darstellungen (alles wegen Maschke, siehe 2.1.11 und 2.1.12).

Wenn  $\rho_1, \dots, \rho_k$  ein Representativesystem der irreduziblen  $K$ -linearen Darstellungen von  $G$  ist, dann sind sie eine  $\mathbb{Z}$ -Basis von  $\mathcal{R}_K(G)$ , denn die Zerlegung einer Darstellung in irreduzible Unterdarstellungen ist (bis auf die Reihenfolge) eindeutig. Wir schreiben dann für eine Darstellung oft

$$\rho = \bigoplus_{i=1}^k m_i \rho_i, \quad m_i \in \mathbb{N}_0.$$

Die Zahl  $m_i$  heißt die *Multiplizität* von  $\rho_i$  in  $\rho$ .

Der Ring  $\mathcal{R}_K(G)$  ist eine Ordnung in der endlichdimensionalen  $\mathbb{Q}$ -Algebra  $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{R}_K(G)$ .

Die Darstellungstheorie hat das Ziel, diesen kommutativen Ring zu verstehen. Dazu betrachtet man den leichter verständlichen Ring der Klassenfunktionen, der nun eingeführt wird.

### 2.5.2 Definition (*Charaktere, Klassenfunktionen, $\kappa_G$* )

a) Es seien  $K$  ein Körper,  $G$  eine endliche Gruppe und  $V$  ein endlichdimensionaler  $K$ -Vektorraum. Weiter sei  $\rho : G \rightarrow \text{Aut}_K(V)$  eine  $K$ -lineare Darstellung von  $G$  auf  $V$ . (Erinnerung: alternativ könnten wir das durch einen  $K$ -Algebrenhomomorphismus  $K[G] \rightarrow \text{End}_K(V)$  beschreiben.)

Dann definieren wir die Abbildung

$$\chi_\rho : G \rightarrow K, \chi_\rho(g) := \text{Spur}(\rho(g)).$$

Sie heißt der *Charakter* von  $\rho$ .

Dann gilt für alle  $g, h \in G$  :

$$\chi_\rho(hgh^{-1}) = \text{Spur}(\rho(h)\rho(g)\rho(h)^{-1}) = \chi_\rho(g).$$

Den Charakter einer virtuellen Darstellung  $\rho - \sigma$  definieren wir als

$$\chi_{\rho - \sigma} := \chi_\rho - \chi_\sigma.$$

Das ist wohldefiniert auf  $\mathcal{R}_K(G)$ .

b) Wegen der vorletzten Gleichung ist  $\chi_\rho$  auf den Konjugationsklassen von  $G$  konstant. Eine Funktion  $f : G \rightarrow K$  heißt eine *Klassenfunktion*, wenn sie auf den Konjugationsklassen von  $G$  konstant ist, also alle  $g, h \in G$  die Gleichung

$$f(hgh^{-1}) = f(g)$$

erfüllt. Den Vektorraum aller Klassenfunktionen bezeichnen wir mit  $\mathcal{C}_K(G)$ .

Dies ist eine  $K$ -Algebra, wobei wir argumentweise addieren und multiplizieren. Insbesondere ist dieser Ring kommutativ.

Die  $K$ -Dimension von  $\mathcal{C}_K(G)$  ist gleich der Anzahl  $\kappa_G$  der Konjugationsklassen von  $G$ .

c) Nun definieren wir noch das Ziel dieses Abschnitts: wir werden im Wesentlichen zeigen, dass

$$\mathbb{C} \otimes_{\mathbb{Z}} \mathcal{R}_{\mathbb{C}}(G) \cong \mathcal{C}_{\mathbb{C}}(G).$$

Im Klartext: eine komplex lineare Darstellung ist bis auf Isomorphie eindeutig durch ihren Charakter bestimmt, und es gibt genau  $\kappa_G$  Isomorphieklassen irreduzibler Darstellungen über  $\mathbb{C}$ .

Dazu brauchen wir zunächst einmal eine Aussage über Charaktere.

### 2.5.3 Hilfssatz (ein Ringhomomorphismus)

Die Abbildung

$$\chi : \mathcal{R}_K(G) \rightarrow \mathcal{C}_K(G), \rho \mapsto \chi_\rho,$$

ist ein Ringhomomorphismus.

*Beweis.* Die triviale eindimensionale Darstellung hat als Charakter die konstante Einsabbildung. Das ist das Einselement von  $\mathcal{C}_K(G)$ .

Wir müssen Additivität und Multiplikativität nur für „echte“ Darstellungen zeigen, dann folgen sie auch für virtuelle. Das erleichtert das  $\text{\TeX}$ . Es seien also  $\rho : G \rightarrow \text{Aut}_K(V)$  und  $\sigma : G \rightarrow \text{Aut}_K(W)$  zwei endlichdimensionale Darstellungen. Weiter seien Basen  $B$  und  $C$  von  $V$  und  $W$  gewählt, sodass sich  $\rho(g)$  bezüglich  $B$  durch die Abbildungsmatrix  $A(g)$  beschreibt, und  $\sigma(g)$  bezüglich  $C$  durch  $\tilde{A}(g)$ .

Dann beschreibt aber die Blockmatrix  $\begin{pmatrix} A & 0 \\ 0 & \tilde{A} \end{pmatrix}$  die Abbildung  $\rho(g) \oplus \sigma(g)$  auf  $V \oplus W$  bezüglich einer geeignet gewählten Basis, und offensichtlich ist damit

$$\text{Spur}(\rho(g) \oplus \sigma(g)) = \text{Spur}(\rho(g)) + \text{Spur}(\sigma(g)).$$

Das ist die gewünschte Additivität.

Ähnlich wird die Abbildung  $\rho(g) \otimes \sigma(g)$  bezüglich einer geeignet gewählten Basis

durch das Kroneckerprodukt

$$\begin{pmatrix} a_{11}(g)\tilde{A}(g) & a_{12}(g)\tilde{A}(g) & \dots & a_{1n}(g)\tilde{A}(g) \\ a_{21}(g)\tilde{A}(g) & a_{22}(g)\tilde{A}(g) & \dots & a_{2n}(g)\tilde{A}(g) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}(g)\tilde{A}(g) & \dots & a_{n,n-1}(g)\tilde{A}(g) & a_{nn}(g)\tilde{A}(g) \end{pmatrix}$$

beschrieben, dessen Spur offensichtlich

$$a_{11}(g)\text{Spur}(\tilde{A}(g)) + \dots + a_{nn}(g)\text{Spur}(\tilde{A}(g)) = \text{Spur}(A(g)) \cdot \text{Spur}(\tilde{A}(g))$$

ist. ○

#### 2.5.4 Bemerkung

In Charakteristik  $p > 0$  ist die Abbildung  $\chi$  nicht injektiv. Denn die triviale  $p$ -dimensionale Darstellung hat Spur konstant gleich 0, wie auch die nulldimensionale Darstellung. Wir werden in Kürze sicherstellen, dass die Abbildung in Charakteristik 0 injektiv ist. Das ist ein allgemeines Phänomen für halbeinfache  $K$ -Algebren  $A$  in Charakteristik 0: ein endlichdimensionaler Modul  $M$  ist bis auf Isomorphie durch die zugehörige Spurabbildung (siehe 2.1.5) eindeutig bestimmt. Wir werden das aber nur in der Situation des Gruppenrings weiterverfolgen.

#### 2.5.5 Definition / Frage (eine Bilinearform)

Es seien  $K$  ein Körper und  $G$  eine endliche Gruppe. Dann führen wir auf dem Raum  $\text{Abb}(G, K)$  aller Abbildungen von  $G$  nach  $K$  die folgende Bilinearform ein:

$$\beta_G(f_1, f_2) := \sum_{g \in G} f_1(g) \cdot f_2(g^{-1}).$$

NB: Wenn  $K = \mathbb{C}$  gilt und  $f_2$  der Charakter einer Darstellung von  $G$  ist, dann gilt  $f_2(g^{-1}) = \overline{f_2(g)}$ . Es ist ja  $\rho(g)$  diagonalisierbar, da es endliche Ordnung hat, und die Eigenwerte sind Einheitswurzeln, also sind die Eigenwerte von  $\rho(g^{-1})$  gerade die zu den Eigenwerten von  $\rho(g)$  konjugiert komplexen Zahlen.

Man führt daher im Falle  $K = \mathbb{C}$  anstelle der obigen Bilinearform das komplexe Skalarprodukt

$$\langle f_1, f_2 \rangle_G := \frac{1}{\#G} \sum_{g \in G} f_1(g) \cdot \overline{f_2(g)}$$

ein, das für Charaktere im zweiten Argument denselben Wert liefert wie  $\beta$ .

Genauso ist im Falle  $K \subseteq \mathbb{R}$  für einen Charakter  $f_2$  die Gleichung  $f_2(g) = f_2(g^{-1})$  richtig. Das liegt letztlich daran, dass eine reelle Matrix endlicher Ordnung zu ihrer inversen ähnlich ist.

b) Wieso haben wir  $\beta$  eingeführt?

### 2.5.6 Hilfssatz

Es seien  $\rho : G \longrightarrow \text{Aut}_K(V)$  und  $\sigma : G \longrightarrow \text{Aut}_K(W)$  zwei irreduzible Darstellungen der endlichen Gruppe  $G$ . Weiter sei  $\Phi : V \longrightarrow W$  eine  $K$ -lineare Abbildung. Dann ist die Abbildung

$$\tilde{\Phi} := \sum_{g \in G} \sigma(g) \circ \Phi \circ \rho(g)^{-1}$$

die Nullabbildung, wenn  $\rho$  und  $\sigma$  nicht isomorph sind.

Wenn  $K$  algebraisch abgeschlossen ist,  $\dim_K(V)$  in  $K$  invertierbar ist und  $\rho = \sigma$  gilt, ist  $\tilde{\Phi}$  die Multiplikation mit dem Skalar

$$\lambda := \#G \cdot \text{Spur}(\Phi) / \dim_K(V).$$

*Beweis.* Wie im Beweis von Maschkes Theorem sieht man, dass  $\tilde{\Phi}$  ein Homomorphismus von  $K[G]$ -Moduln ist. ( $K$ -linear ist klar,  $G$ -Äquivarianz muss man nachrechnen...)

Daher ist  $\tilde{\Phi} = 0$ , wenn  $\rho$  und  $\sigma$  nicht isomorph sind, denn der Kern ist ein Untermodul von  $V$ , und das Bild ein Untermodul von  $W$ .

Wenn  $\rho = \sigma$  gilt und  $K$  algebraisch abgeschlossen ist, dann sagt uns das Lemma von Schur, dass  $\tilde{\Phi}$  die Multiplikation mit einem Skalar  $\lambda \in K$  ist. Es gilt wegen der Ähnlichkeitsinvarianz der Spur

$$\dim_K(V) \cdot \lambda = \text{Spur}(\tilde{\Phi}) = \sum_{g \in G} \text{Spur}(\Phi) = \#G \cdot \text{Spur}(\Phi),$$

woraus sich der angegebene Wert von  $\lambda$  berechnet. ○

### 2.5.7 Konkretisierung (mit „Matrixkoeffizienten“)

Wir wählen nun in der Situation des vorangegangenen Hilfssatzes Basen der Vektorräume und erhalten daraus Abbildungsmatrizen  $A(g) := (a_{ij}(g))_{1 \leq i, j \leq d}$  für  $\rho$  und  $B(g) := (b_{ij}(g))_{1 \leq i, j \leq e}$  für  $\sigma$ , wobei  $d := \dim_K(V)$ ,  $e := \dim_K(W)$  gelte. Wenn  $\Phi$  durch die Elementarmatrix  $(E_{j,k})$  beschrieben wird, dann wird  $\tilde{\Phi}$  durch die Matrix

$$\sum_{g \in G} B(g) E_{j,k} A(g^{-1})$$

beschrieben, die an der Stelle  $(i, l)$  den Eintrag

$$\sum_{g \in G} b_{ij}(g) a_{kl}(g^{-1})$$

hat. Es gilt also im ersten Fall:

$$\forall i, j, k, l : \sum_{g \in G} b_{ij}(g) a_{kl}(g^{-1}) = 0.$$

Wenn hingegen  $\rho = \sigma$  gilt, so folgt durch eine analoge Rechnung, wenn  $K$  algebraisch abgeschlossen ist und die Charakteristik von  $K$  kein Teiler der Dimension von  $V$  ist:

$$\forall i, j, k, l : \sum_{g \in G} a_{ij}(g) a_{kl}(g^{-1}) = \begin{cases} \lambda, & \text{falls } j = k \text{ und } i = l, \\ 0, & \text{sonst.} \end{cases}$$

Dabei ist  $\lambda$  wie in 2.5.6 durch  $\lambda = \#G / \dim_K(V)$  gegeben, der Fall  $j = k$  entspricht ja einer Elementarmatrix mit Spur 1.

### 2.5.8 Folgerung (Orthogonalitätsrelation)

Es seien  $\rho, \sigma$  irreduzible Darstellungen der endlichen Gruppe  $G$  über einem algebraisch abgeschlossenen Körper  $K$  der Charakteristik 0. (Dasselbe geht auch für  $\text{char}(K) > \#G$ .) Dann gilt für die Charaktere  $\chi_\rho$  und  $\chi_\sigma$ :

$$\beta_G(\chi_\rho, \chi_\sigma) = \begin{cases} 0, & \text{falls } \rho \text{ und } \sigma \text{ nicht isomorph sind,} \\ \#G, & \text{sonst.} \end{cases}$$

*Beweis:* Wir wählen Matrizenmodelle von  $\rho$  und  $\chi$  und verwenden die Regeln aus 2.5.7 beim Berechnen der Bilinearform.  $\circ$

### 2.5.9 Folgerung (Injektivität von $\chi$ , Kriterium der Irreduzibilität)

Es seien  $K$  ein algebraisch abgeschlossener Körper der Charakteristik 0 und  $G$  eine endliche Gruppe. Dann gelten:

- a) Der Ringhomomorphismus  $\chi : \mathcal{R}_K(G) \longrightarrow \mathcal{C}_K(G)$  ist injektiv.
- b) Eine endlichdimensionale  $K$ -lineare Darstellung  $\rho$  von  $G$  ist genau dann irreduzibel, wenn  $\beta_G(\chi_\rho, \chi_\rho) = \#G$  gilt.

*Beweis.* a) Der Darstellungsring wird als  $\mathbb{Z}$ -Modul von den irreduziblen Darstellungen von  $G$  erzeugt. Es langt also zu zeigen, dass die Charaktere von paarweise verschiedenen irreduziblen Darstellungen über  $K$  linear unabhängig sind. Das folgt offensichtlich aus der Orthogonalitätsrelation: die Charaktere bilden ein Orthogonalsystem im Raum der Klassenfunktionen.

b) Wir schreiben  $\rho = \bigoplus_{i=1}^k m_i \rho_i$  wie in 2.5.1. Aufgrund der Orthogonalitätsrelation ist dann

$$\beta_G(\chi_\rho, \chi_\rho) = \#G \cdot \sum_{i=1}^k m_i^2.$$

Diese Summe ist genau dann 1, wenn  $\rho$  irreduzibel ist.  $\circ$

### 2.5.10 Bemerkung

a) Wenn  $K$  nicht algebraisch abgeschlossen ist, aber immer noch Charakteristik 0 hat, dann ist  $\chi$  immer noch injektiv. Wenn nämlich  $\overline{K}$  der algebraische Abschluss

von  $K$  ist, dann erhalten wir ein kommutatives Diagramm

$$\begin{array}{ccc} \mathcal{R}_K(G) & \longrightarrow & \mathcal{C}_K(G) \\ \downarrow & & \downarrow \\ \mathcal{R}_{\overline{K}}(G) & \longrightarrow & \mathcal{C}_{\overline{K}}(G) \end{array}$$

wobei von oben nach unten die offensichtlichen Inklusionen stehen. Da  $\chi$  in der unteren Zeile kommutativ ist, gilt dies also auch in der oberen.

Das Kriterium für die Irreduzibilität gilt allerdings nicht für beliebiges  $K$ ! So ist etwa die vierdimensionale Standarddarstellung der Quaternionengruppe  $Q_8$  über  $\mathbb{R}$  irreduzibel, hat aber den Charakter

$$\chi_\rho : 1 \mapsto 4, -1 \mapsto -4, \pm I, \pm J, \pm K \mapsto 0.$$

Es gilt

$$\beta_{Q_8}(\chi_\rho, \chi_\rho) = 32.$$

Über den komplexen Zahlen zerfällt diese Darstellung in zwei isomorphe zweidimensionale, d.h.  $\rho = 2\tilde{\rho}$ , und es folgt

$$\beta_{Q_8}(\chi_{\tilde{\rho}}, \chi_{\tilde{\rho}}) = \frac{1}{4}\beta_{Q_8}(\chi_\rho, \chi_\rho) = 8 = \#Q_8.$$

Daher ist  $\tilde{\rho}$  irreduzibel.

b) Mit dem Satz sieht man auch, wieso im Fall  $K = \mathbb{C}$  im Skalarprodukt  $\langle \cdot, \cdot \rangle_G$  der Normierungsfaktor  $1/\#G$  eingebaut wird. Er sorgt dafür, dass die Charaktere der irreduziblen Darstellungen ein Orthonormalsystem im Raum der Klassenfunktionen sind.

c) Wenn die Charakteristik von  $K$  nicht 0, aber größer als  $\#G$  ist, dann gilt der Satz 2.5.9 fast auch noch:  $\chi$  ist zwar nicht mehr injektiv, aber der Kern von  $\chi$  ist so klein, wie er nur sein kann:  $\text{Kern}(\chi) = p \cdot \mathcal{R}_K(G)$ . Der Beweis ist analog zu dem in Charakteristik 0, die Charaktere der irreduziblen Darstellungen sind immer noch linear unabhängig über  $K$ .

### 2.5.11 Folgerung (Zerlegung einer gegebenen Darstellung)

Es sei  $\rho$  eine endlichdimensionale Darstellung der endlichen Gruppe  $G$  über dem algebraisch abgeschlossenen Körper  $K$  der Charakteristik 0. Weiter seien  $\rho_1, \dots, \rho_k$  die Typen irreduzibler  $K[G]$ -Moduln. Dann gilt

$$\rho \cong \bigoplus_{i=1}^k m_i \cdot \rho_i,$$

wobei die Multiplizitäten  $m_i$  gegeben sind durch  $m_i = \frac{1}{\#G}\beta_G(\chi_\rho, \chi_{\rho_i})$ .

*Beweis.* Klar. ○

### 2.5.12 Folgerung

Wenn  $K$  algebraisch abgeschlossen von Charakteristik 0 ist, dann ist die Multiplizität der irreduziblen Darstellung  $\rho$  in der regulären Darstellung gleich  $\dim(\rho)$ . Es ist ja der Charakter  $\chi_{\rho_{\text{reg}}}$  der regulären Darstellung gegeben durch

$$e_G \mapsto \#G, \quad g \mapsto 0 \text{ falls } g \neq e_G.$$

Nun ist nur der Wert  $\frac{1}{\#G}\beta_G(\chi_{\rho_{\text{reg}}}, \chi_{\rho_i})$  zu berechnen, dieser ist  $\chi_{\rho_i}(e_G) = \dim(\rho_i)$ .

Nun sollten wir noch sehen, wie viele irreduzible Darstellungen es gibt. Es können höchstens  $\kappa_G$  sein, womit wieder die Anzahl der Konjugationsklassen in  $G$  gemeint ist. Dass für algebraisch abgeschlossene Körper der Charakteristik 0 dieser Wert auch wirklich angenommen wird, wird sich nun zeigen.

### 2.5.13 Satz

*Es sei  $K$  ein algebraisch abgeschlossener Körper der Charakteristik 0 und  $G$  eine endliche Gruppe. Dann bilden die Charaktere  $\chi_i$ ,  $1 \leq i \leq k$ , der irreduziblen Darstellungen von  $G$  eine Basis des Raums  $\mathcal{C}_K(G)$  der Klassenfunktionen.*

*Beweis.* Wir wissen schon, dass die  $\chi_i$  linear unabhängig sind. Wir müssen noch zeigen, dass sie den Raum der Klassenfunktionen erzeugen.

Es sei  $\rho$  die reguläre Darstellung von  $G$  auf  $K[G]$ . Weiter sei  $f$  eine beliebige Klassenfunktion. Wir bilden die Abbildung

$$\Phi := \sum_{g \in G} f(g)\rho(g^{-1}) \in \text{End}_K(K[G]).$$

Weil  $f$  eine Klassenfunktion ist, gilt hierbei

$$\forall h \in G : \rho(h)^{-1} \circ \Phi \circ \rho(h) = \sum_{g \in G} f(g)\rho(h^{-1}g^{-1}h) = \Phi.$$

$K[G]$  ist eine direkte Summe von irreduziblen  $K[G]$ -Untermoduln, und jeder solche ist zu einem  $\rho_i$  isomorph. Wegen des Lemmas von Schur ist die Einschränkung von  $\Phi$  auf solch einen irreduziblen Teilraum die Multiplikation mit einem Skalar  $\lambda_i$ ; dieser berechnet sich durch

$$\dim \rho_i \cdot \lambda_i = \sum_{g \in G} f(g)\text{Spur} \rho_i(g^{-1})$$

als

$$\lambda_i = \frac{1}{\dim \rho_i} \beta_G(f, \chi_i).$$

Für die Funktion

$$\tilde{f} := \frac{1}{\#G} \sum_{i=1}^k \beta(f, \chi_i) \chi_i$$

hat die zugehörige Abbildung  $\tilde{\Phi}$  auf den irreduziblen Summanden von  $K[G]$  aber dieselben Eigenwerte, und deshalb stimmen  $\Phi$  und  $\tilde{\Phi}$  überein.

Da  $f$  sich vermöge

$$\Phi(\delta_{e_G}) = \sum_{g \in G} f(g) \delta_g$$

aus  $\Phi$  zurückgewinnen lässt, folgt

$$f = \tilde{f} = \frac{1}{\#G} \sum_{i=1}^k \beta(f, \chi_i) \chi_i.$$

Damit erzeugen die  $\chi_i$  den Raum der Klassenfunktionen als  $K$ -Vektorraum.  $\circ$

### 2.5.14 Bemerkung

a) Wir wissen jetzt, dass es (im algebraisch abgeschlossenen Fall in Charakteristik 0) genau  $\kappa_G$  Isomorphietypen von irreduziblen Darstellungen einer endlichen Gruppe  $G$  mit  $\kappa_G$  Konjugationsklassen gibt. Dies lässt sich zusammen mit der Gleichung

$$\#G = \sum_{i=1}^{\kappa_G} (\dim \rho_i)^2$$

und der Orthogonalitätsrelation oft benutzen, um die Suche nach den irreduziblen Darstellungen zu erleichtern.

Beispiel: Wir nehmen  $G = S_4$ . Die Gruppe  $G$  hat 24 Elemente, und die Konjugationsklassen entsprechen bijektiv den (aufsteigenden) Partitionen von 4, wobei einer Partition eben ein Typ von Zykelzerlegung zugeordnet wird. Wir wählen Repräsentanten der Konjugationsklassen:

$$\text{Id}, (1\ 2), (1\ 2) \circ (3\ 4), (1\ 2\ 3), (1\ 2\ 3\ 4).$$

Wir haben 5 Klassen, also auch 5 irreduzible Darstellungen über  $\mathbb{C}$ . Zwei eindimensionale Darstellungen kennen wir schon lange: die triviale und die Signatur.

Gesucht sind nun noch die Dimensionen  $d_3, d_4, d_5$  der übrigen irreduziblen Darstellungen von  $S_4$ ; es muss gelten

$$1^2 + 1^2 + d_3^2 + d_4^2 + d_5^2 = 24, \text{ also } d_3^2 + d_4^2 + d_5^2 = 22.$$

Mit ein bisschen Herumprobieren sieht man, dass die einzige Möglichkeit, dies mit natürlichen Zahlen zu bewerkstelligen, die folgende ist:

$$d_3 = 2, d_4 = d_5 = 3.$$

Nun wollen wir versuchen, die Charaktere dieser Darstellungen zu bestimmen. Da es nur eine zweidimensionale irreduzible Darstellung gibt und diese nach Tensorieren mit der Signatur wieder eine zweidimensionale irreduzible Darstellung gibt, muss die Spur von  $\rho_3$  auf den ungeraden Permutationen verschwinden.  $\chi_2(e_G) = 2$  gilt aus Dimensionsgründen. Eine  $2 \times 2$ -Matrix der Ordnung 1 oder 2 hat Spur 2, 0 oder  $-2$ . Das gilt also für  $\chi_3((1\ 2)(3\ 4))$ . Die Orthogonalität von  $\chi_3$  mit dem trivialen Charakter sagt

$$2 + 3 \cdot \chi_3((1\ 2)(3\ 4)) + 8\chi_3((1\ 2\ 3)) + 6 \cdot 0 + 6 \cdot 0 = 0.$$

Weiter sagt die Formel  $\beta_G(\chi_3, \chi_3) = 24$ , dass

$$4 + 3\chi_3((1\ 2)(3\ 4))^2 + 8\chi_3((1\ 2\ 3))^2 = 24.$$

Ausprobieren der möglichen Werte des Charakters bei  $(1\ 2)(3\ 4)$  liefert

$$\chi_3((1\ 2)(3\ 4)) = 2, \chi_3((1\ 2\ 3)) = -1.$$

Damit kennen wir  $\chi_3$ .

Nun brauchen wir noch  $\chi_4$  und  $\chi_5$ . Dies sind Charaktere von dreidimensionalen Darstellungen, und die Spuren von Matrizen der Ordnung 1 oder 2 im Dreidimensionalen sind 3, 1,  $-1$ , oder  $-3$ . Die Spur von  $\rho_4((1\ 2))$  ist nicht 3, denn sonst wäre  $\rho((1\ 2))$  die Einheitsmatrix, also  $(1\ 2)$  im Kern von  $\rho$ , und damit  $\rho$  trivial, weil die einzige normale Untergruppe der  $S_4$ , die  $(1\ 2)$  enthält, eben  $S_4$  selbst ist. Also ist  $\chi_4((1\ 2)) = \pm 1$ , und weil das Tensorieren mit der Signatur  $\rho_4$  und  $\rho_5$  vertauscht, darf man sich das Vorzeichen aussuchen: ohne Einschränkung gilt  $\chi_4((1\ 2)) = 1$ .

Da  $\chi_4$  sowohl auf  $\chi_1$  als auch auf  $\chi_2$  senkrecht steht, sieht man, dass  $\chi_4((1\ 2\ 3\ 4)) = -1$  gelten muss. Es folgt mit ähnlichen Rechnungen wie für  $\chi_3$  die folgende Charaktertafel für  $S_4$ :

Klasse	$\chi_1$	$\chi_2$	$\chi_3$	$\chi_4$	$\chi_5$
$e_G$	1	1	2	3	3
$(1\ 2)$	1	$-1$	0	1	$-1$
$(1\ 2)(3\ 4)$	1	1	2	$-1$	$-1$
$(1\ 2\ 3)$	1	1	$-1$	0	0
$(1\ 2\ 3\ 4)$	1	$-1$	0	$-1$	1

Damit kennen wir die Charaktere der irreduziblen Darstellungen von  $S_4$ , was aber noch fehlt, sind die Darstellungen selber! Zum Beispiel  $\rho_2$  bekommt man so: weil  $\chi_2((1\ 2)(3\ 4)) = 3$  gilt, ist diese  $2 \times 2$ -Matrix endlicher Ordnung die Einheitsmatrix. Es ist also  $(1\ 2)(3\ 4)$  im Kern und damit jedes Produkt von 2 disjunkten 2-Zykeln: Diese drei Matrizen bilden zusammen mit der Einheitsmatrix die Kleinsche Vierergruppe  $V_4$ , und  $S_4/V_4 \cong S_3$ . Wir erhalten  $\rho_3$  auf den

Erzeugern  $(1\ 2), (1\ 2\ 3), (3\ 4)$  durch

$$\rho((1\ 2)) := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} =: \rho((3\ 4)), \quad \rho((1\ 2\ 3)) := \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Die Darstellung  $\rho_4$  ergibt sich aus der vierdimensionalen Standarddarstellung von  $S_4$  auf  $\mathbb{C}^4$ , die durch die Permutationsmatrizen gegeben ist. Darin ist der Teilraum

$$V_0 := \{(x_i)_{1 \leq i \leq 4} \mid \sum_{i=1}^4 x_i = 0\}$$

ein invarianter Unterraum, und man rechnet nach, dass  $\rho_4$  gerade die Operation auf diesem Raum ist. Schließlich setzen wir  $\rho_5(g) := \text{sgn}(g)\rho_4(g)$  und erhalten die zweite irreduzible Darstellung von  $S_4$  in Dimension 3.

### 2.5.15 Definition / Bemerkung (die induzierte Darstellung)

Nun sei in der endlichen Gruppe  $G$  eine Untergruppe  $H$  gegeben.

a) Die Zuordnung  $\rho \mapsto \rho|_H$  liefert einen Vergissfaktor von der Kategorie der  $K[G]$ -Moduln in die Kategorie der  $K[H]$ -Moduln. Er heißt  $\text{Res}_H^G$ : die Restriktion von  $G$  nach  $H$ .

b) Nun wollen wir in die umgekehrte Richtung. Wir nehmen also einen  $K[H]$ -Modul  $W$  und wollen diesem einen  $K[G]$ -Modul zuordnen. Dazu nehmen wir hilfsweise den Vektorraum

$$\widetilde{W} := K[G] \otimes_K W,$$

der zwar ein  $K[G]$ -Modul ist, aber nichts von der  $K[H]$ -Modulstruktur von  $W$  merkt. Um dies zu ändern benutzen wir eine Operation von  $H$  auf  $\widetilde{W}$ , die durch

$$h \bullet (g \otimes w) := (gh^{-1}) \otimes hw$$

gegeben ist. Diese vertauscht mit der  $K[G]$ -Multiplikation. Also ist der Modul der  $H$ -invarianten hierin ein  $K[G]$ -Untermodul von  $\widetilde{W}$ . Wir nennen ihn  $\text{Ind}_H^G W$ .

Ein schönes konkretes Modell erhalten wir wie folgt:

Es ist

$$K[G] \otimes_K W = \text{Abb}(G, K) \otimes_K W = \text{Abb}(G, W),$$

das ist ein  $K$ -Vektorraum, und  $H$  operiert darauf durch

$$\forall f \in \text{Abb}(G, W), \forall h \in H : (h \bullet f)(g) := h(f(gh)).$$

Wir suchen die Invarianten unter dieser Operation, das heißt die Menge aller Funktionen  $f \in \text{Abb}(G, W)$ , für die gilt:

$$\forall h \in H, g \in G : f(gh) = h^{-1}f(g).$$

In Zukunft denken wir uns  $\text{Ind}_H^G W$  als die Menge

$$\{f : G \longrightarrow W \mid \forall g \in G, h \in H : f(gh) = h^{-1}(f(g))\},$$

wobei  $h^{-1}(f(g))$  die gegebene Operation von  $H$  auf  $W$  ist. Auf diesem Raum operiert die Gruppe  $G$  durch

$$(g * f)(x) := f(g^{-1}x).$$

Rechnen Sie nach, dass wir tatsächlich einen  $K[G]$ -Linksmodul erhalten!

c) Konkretisierung:

Um diese Funktionen  $f$  mit  $f(gh) = h^{-1}(f(g))$  zu finden, wählen wir ein System von Nebenklassenvertretern von  $H$  in  $G$ , das heißt wir wählen für  $r := (G : H)$  Elemente  $g_1, \dots, g_r \in G$ , sodass

$$G = \bigcup_{i=1}^r g_i H.$$

Dann ist durch die Vorgabe von  $w_1, \dots, w_r \in W$  eine  $H$ -invariante Abbildung von  $G$  nach  $W$  gegeben durch

$$f(g_i h) := h^{-1}(w_i).$$

Wir erhalten somit eine Bijektion von  $\text{Ind}_H^G W$  mit  $W^r$  als  $K$ -Vektorräume, und die Operation von  $G$  darauf lässt sich auch hinschreiben: Für  $g \in G$  und  $1 \leq i \leq r$  gibt es  $1 \leq \sigma(i) \leq r$  und  $h \in H$ , sodass  $g^{-1}g_i = g_{\sigma(i)}h$  gilt. Dann macht die Operation von  $g$  aus dem  $r$ -Tupel  $(w_1, \dots, w_r)$  das Tupel

$$g * (w_i)_{1 \leq i \leq r} := (h_i^{-1}w_{\sigma(i)})_{1 \leq i \leq r}.$$

Es ist klar, was man mit Morphismen  $\Phi$  zwischen  $K[H]$ -Moduln zu tun hat, um aus  $\text{Ind}_H^G$  einen Funktor von der Kategorie der  $K[H]$ -Moduln in die Kategorie der  $K[G]$ -Moduln zu machen: man schränkt  $\text{Id}_{K[G]} \otimes \Phi$  auf die  $H$ -invarianten ein.

### 2.5.16 Rechnung (Der Charakter eines induzierten Moduls)

Es seien  $W$  ein endlichdimensionaler  $K[H]$ -Modul (Darstellung  $\rho : H \longrightarrow \text{Aut}_J(W)$ ),  $H$  eine Untergruppe der endlichen Gruppe  $G$ , und  $V := \text{Ind}_H^G(W)$  der durch  $W$  auf  $G$  induzierte Modul. Wie hängt der Charakter von  $V$  mit dem von  $W$  zusammen?

Naja, wenn wir uns die Formel für die Operation von  $G$  auf  $W^r$  aus dem letzten Abschnitt ansehen, dann beschreiben wir dabei die Operation durch Blockmatrizen (wenn wir einen Basis von  $W$  gewählt haben), und zwar Blöcke der Größe

$\dim_K(W) \times \dim_K(W)$ , und an der Stelle  $(i, \sigma(i))$  steht die Matrix, die die Operation von  $h_i^{-1}$  auf  $W$  beschreibt. Das bedeutet:

$$\text{Spur}(g|_{\text{Ind}_H^G(\rho)}) = \sum_{\substack{i=1 \\ g^{-1}g_i=g_ih_i}}^r \text{Spur}(\rho(h_i^{-1})) = \frac{1}{\#H} \sum_{\substack{x \in G \\ x^{-1}g^{-1}x \in H}} \text{Spur}(\rho(x^{-1}gx)).$$

Dabei wird ab dem zweiten Gleichheitszeichen vorausgesetzt, dass die Charakteristik von  $K$  kein Teiler der Ordnung von  $\#H$  ist.

Hierbei kann man nun nicht viel weiter vereinfachen, da  $\rho$  ja eine Darstellung von  $H$  ist, und nicht von  $G$ !

Grundsätzlich aber kennen wir damit den Charakter von  $\text{Ind}_H^G(\rho)$ .

Wenn nun  $\sigma : G \rightarrow \text{Aut}_K(V)$  eine endlichdimensionale Darstellung von  $G$  ist, dann hat die auch einen Charakter. Wir berechnen (wenn die Charakteristik von  $K$  nicht gerade ungünstig ist...)

$$\begin{aligned} \beta_G(\chi_{\text{Ind}_H^G(\rho)}, \chi_\sigma) &= \frac{1}{\#H} \sum_{g \in G} \sum_{\substack{x \in G \\ x^{-1}gx \in H}} \text{Spur}(\rho(x^{-1}gx)) \cdot \text{Spur}(\sigma(g^{-1})) \\ &= \frac{1}{\#H} \sum_{h \in H} \sum_{x \in G} \text{Spur}(\rho(h)) \cdot \text{Spur}(\sigma(xh^{-1}x^{-1})) \\ &= \frac{\#G}{\#H} \beta_H(\chi_\rho, \chi_{\text{Res}_H^G(\sigma)}). \end{aligned}$$

Nun betrachten wir uns die  $K$ -linearen Abbildungen

$$\text{Res}_H^G : \mathcal{C}_K(G) \rightarrow \mathcal{C}_K(H), \quad \text{Ind}_H^G : \mathcal{C}_K(H) \rightarrow \mathcal{C}_K(G),$$

deren erste durch Einschränken der Funktionen nach  $H$  gegeben ist, und deren zweite durch die Formel definiert wird, die den Charakter der induzierten Darstellung aus dem Charakter eines  $H$ -Moduls berechnet.

Dann zeigt die letzte Rechnung im Falle, dass die Charakteristik von  $K$  kein Teiler von  $\#G$  ist:

$$\frac{1}{\#G} \beta_G(\text{Ind}_H^G v, w) = \frac{1}{\#H} \beta_H(v, \text{Res}_H^G w).$$

Die linearen Abbildungen  $\text{Res}$  und  $\text{Ind}$  sind adjungiert bezüglich der (richtig normierten) betrachteten Bilinearformen auf den Klassenfunktionen.

Dies ist doch nett, denn es gilt der folgende Satz:

**2.5.17 Satz** (*Nun adjungiert was zusammengehört – Frobeniusreziprozität*)

Wenn  $H \subseteq G$  endliche Gruppen sind und  $K$  ein Körper ist, dann ist der Funktor  $\text{Ind}_H^G$  zum Funktor  $\text{Res}_H^G$  linksadjungiert.

*Beweis.* Wir brauchen für jeden  $K[G]$ -Modul  $V$  und jeden  $K[H]$ -Modul  $W$  intelligente Isomorphismen

$$\text{Hom}_{K[G]}(\text{Ind}_H^G W, V) \longrightarrow \text{Hom}_{K[H]}(W, \text{Res}_H^G V).$$

Diese müssen durch ein geeignetes universelles Element für den richtigen Funktor zustande kommen, z.B. für den Funktor  $V \rightsquigarrow \text{Hom}_{K[H]}(W, \text{Res}_H^G V)$ . Die gewünschte Adjungiertheit legt nahe, dass wir einen  $H$ -Morphismus von  $W$  nach  $\text{Res}_H^G \text{Inf}_H^G W$  angeben sollten. Das tun wir nun; wir ordnen dem Element  $w \in W$  die Funktion  $f_w : G \longrightarrow W$  zu, die durch

$$\forall x \in G : f_w(x) := \begin{cases} x^{-1}w, & \text{falls } x \in H, \\ 0, & \text{sonst.} \end{cases}$$

Dies definiert eine  $K$ -lineare Abbildung  $F : W \longrightarrow \text{Ind}_H^G W$ , und man rechnet nach, dass

$$\forall w \in W, h \in H, x \in G : f_{hw}(x) = x^{-1}hw = f_w(h^{-1}x) = (h * (f_w))(x).$$

Es ist also  $F : w \mapsto f_w$  ein Homomorphismus von  $K[H]$ -Moduln. Dann definiert die Abbildung

$$\eta_{V,W} : \text{Hom}_{K[G]}(\text{Ind}_H^G W, V) \ni \Phi \mapsto \Phi \circ F \in \text{Hom}_{K[H]}(W, \text{Res}_H^G V)$$

eine natürliche Transformation der entsprechenden Hom-Funktoren (bei festem  $W$ ;  $V$  läuft).

In der umgekehrten Richtung erinnern wir uns an die Zerlegung  $G = \bigcup g_i H$  und betrachten für einen festen  $K[G]$ -Modul  $V$  die Abbildung

$$M : \text{Ind}_H^G \text{Res}_H^G V \longrightarrow V, \quad f \mapsto \sum_{i=1}^r g_i(f(g_i)).$$

Das ist sinnvoll, da die Funktionswerte von  $f$  ja in einem  $K[G]$ -Modul liegen. Es hängt außerdem nicht von der Wahl der Nebenklassenvertreter ab, da für alle  $g \in G$  und  $h \in H$  gilt:

$$ghf(gh) = gh h^{-1} f(g) = gf(g).$$

Wir sind ja im induzierten Modul!

Nun definieren wir die Abbildung

$$\tilde{\eta}_{W,V} : \text{Hom}_{K[H]}(W, \text{Res}_H^G V) \ni \Psi \mapsto M \circ \text{Ind}_H^G(\Psi) \in \text{Hom}_{K[G]}(\text{Ind}_H^G W, V),$$

und man rechnet nach, dass  $\eta_{V,W}$  und  $\tilde{\eta}_{W,V}$  für jeden  $K[G]$ -Modul  $V$  und jeden  $K[H]$ -Modul  $W$  zueinander invers sind.  $\circ$

### 2.5.18 Bemerkung

Der Prozess der Induktion führt manchmal dazu, dass Aussagen über Darstellungen von weniger komplizierten Gruppen benutzt werden können, um Aussagen über die eigentlich gerade interessierende Darstellung zu machen. Stichwort: Die Sätze von Artin und Brauer. Diese sind zum Beispiel in der Theorie der  $L$ -Reihen in der Zahlentheorie wichtig.

Zu guter Letzt soll nun noch eine Anwendung der Darstellungstheorie in der Gruppentheorie selbst vorgeführt werden. Vorbereitender Weise brauchen wir noch einen Hilfssatz über Einheitswurzeln in  $\mathbb{C}$ .

### 2.5.19 Hilfssatz (ein Satz von Kronecker)

a) Es sei  $\alpha \in \mathbb{C}$  algebraisch ganz (d.h. ganz über  $\mathbb{Z}$ ) und so, dass alle Nullstellen des Minimalpolynoms von  $\alpha$  Betrag  $\leq 1$  haben. Dann ist  $\alpha = 0$  oder  $\alpha$  ist eine Einheitswurzel.

b) Es seien  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  Einheitswurzeln und

$$\alpha := (\lambda_1 + \dots + \lambda_n)/n.$$

Wenn  $\alpha$  algebraisch ganz ist, dann ist es 0 oder eine Einheitswurzel.

*Beweis.*

a) Es seien  $\alpha_1, \dots, \alpha_n$  die Nullstellen des Minimalpolynoms  $f$  von  $\alpha$ . Dann gilt

$$f = \prod_{i=1}^n (X - \alpha_i).$$

Die Koeffizienten von  $f$  sind die Ausdrücke

$$\sum_{1 \leq j_1 < j_2 < \dots < j_k \leq n} \prod_{l=1}^k \alpha_{j_l}, \quad 0 \leq k \leq n.$$

Diese Koeffizienten sind also betragsmäßig alle  $\leq 2^n$ .

Es sei  $P := \{\sum_{i=0}^n a_i X^i \in \mathbb{Z}[X] \mid -2^n \leq a_i \leq 2^n\}$ . Das ist eine endliche Menge, in der auch  $f$  liegt, da  $\alpha$  algebraisch ganz ist.

Die Potenzen  $\alpha^k$ ,  $k \in \mathbb{N}_0$ , erfüllen alle dieselbe Voraussetzung wie  $\alpha$  selbst: sie sind ganz (denn die ganzen Zahlen bilden einen Ring) und alle Nullstellen ihrer Minimalpolynome haben Betrag  $\leq 1$  (denn diese sind  $\{\alpha_i^k \mid 1 \leq i \leq n\}$ ). Außerdem ist der Grad ihrer Minimalpolynome nicht größer als  $n$ . Demnach liegt das Minimalpolynom von  $\alpha^k$  also in  $P$ , und es gibt nur endlich viele Möglichkeiten

für die Werte von  $\alpha^k$ . Speziell gibt es natürliche Zahlen  $k < l$ , sodass  $\alpha^k = \alpha^l$  gilt, und die Behauptung folgt.

b) Wenn  $\alpha$  ganz ist, dann erfüllt es alles, was in a) verlangt wird.  $\circ$

### 2.5.20 Hilfssatz

Es sei  $\rho : G \rightarrow \text{GL}_n(\mathbb{C})$  eine irreduzible Darstellung der endlichen Gruppe  $G$  mit Charakter  $\chi$ . Weiter sei  $g \in G$  ein Element,  $C$  seine Konjugationsklasse in  $G$  und  $\eta = \#C$ . Wenn dann  $\eta$  und  $n$  teilerfremd sind, dann ist  $\chi(g)/n$  entweder 0 oder eine Einheitswurzel.

*Beweis:* Wir schreiben

$$1 = kn + l\eta$$

mit  $k, l \in \mathbb{Z}$ . Nach Multiplikation mit  $\chi(g)/n$  wird daraus

$$\chi(g)/n = k\chi(n) + l\eta\chi(g)/n.$$

$\chi(g)$  ist eine Summe von  $n$  Einheitswurzeln, und die Behauptung folgt aus 2.5.19, wenn wir wissen, dass  $\chi(g)/n$  ganz algebraisch ist. Das wiederum folgt daraus, dass  $\eta\chi(g)/n$  ganz algebraisch ist, was wir nun noch zeigen müssen.

Dazu sei  $\Phi := \sum_{x \in C} \rho(x)$ . Die Summe  $s := \sum_{x \in C} x$  liegt im Zentrum des Gruppenrings  $\mathbb{Z}[G]$ . Dieses Zentrum wird (nach dem Lemma von Schur) von  $\rho$  auf  $\mathbb{C} \cdot I_n = Z(\mathbb{C}^{n \times n})$  abgebildet ( $I_n$  ist die  $n \times n$ -Einheitsmatrix). Dabei geht  $s$  auf die Matrix  $\lambda I_n$ , deren Spur  $n\lambda$  gleich  $\sum_{x \in C} \text{Spur}(\rho(x)) = \eta \cdot \chi(g)$  ist. Da  $s$  als Element einer Ordnung in  $\mathbb{Q}[G]$  ganz ist, muss auch  $\lambda = \eta\chi(g)/n$  ganz sein.  $\circ$

### 2.5.21 Satz (Nicht-Einfachheitskriterium)

Es seien  $G$  eine endliche Gruppe,  $p$  eine Primzahl und  $g \in G$  ein Element, sodass die Mächtigkeit der Konjugationsklasse von  $g$  eine  $p$ -Potenz  $> 1$  ist.

Dann ist  $G$  nicht einfach.

*Beweis:* Es sei  $X$  die Menge der Charaktere der irreduziblen komplexen Darstellungen von  $G$ ,  $X' = X \setminus \{1\}$ . Die Orthogonalitätsrelation impliziert dann (weil mit den Spalten einer unitären Matrix auch deren Zeilen orthogonal sind)

$$\sum_{\chi \in X} \chi(e_G)\chi(g) = 0, \quad \text{also} \quad 1 = - \sum_{\chi \in X'} \chi(g)\chi(e_G).$$

Dann gibt es aber einen Charakter  $\chi \in X'$ , sodass  $\chi(g) \neq 0$  und  $p \nmid \chi(1) = \dim(\chi)$ . Anderenfalls wäre ja  $p^{-1}$  ganz algebraisch, was aber nicht stimmt.

Es sei  $\chi$  so ein Charakter und  $\rho$  die zugehörige irreduzible Darstellung. Dann gilt  $\chi(e_G) = \dim(\rho)$ , und nach 2.5.20 folgt  $\chi(g)/\chi(1) =: \lambda$  ist eine Einheitswurzel. Das impliziert  $\rho(g) = \lambda I_n$  (alle Eigenwerte müssen gleich sein, da sonst die Summe der Beträge nicht  $n$  sein könnte). Damit gilt  $\rho(g) \in Z(\rho(G))$ , und somit ist  $G$  nicht einfach.  $\circ$

**2.5.22 Folgerung** (*Burnside's  $p^a q^b$ -Satz*)

Es seien  $p$  und  $q$  Primzahlen und  $G$  eine Gruppe, deren Ordnung gleich  $p^a q^b$  für natürliche Zahlen  $a, b$  ist

Dann ist  $G$  auflösbar.

*Beweis:* Wir zeigen, dass  $G$  nicht einfach ist, wenn es nicht zyklisch von Primzahlordnung ist. Dann folgt rekursiv nach  $a, b$ , dass in der Kompositionsreihe für  $G$  nur zyklische Gruppen von Primzahlordnung als Faktoren auftauchen, dass also  $G$  eine Normalreihe mit abelschen Quotienten hat, und damit auflösbar ist.

Da  $p$ -Gruppen nilpotent sind (siehe Algebra I; Sylowsätze und Folgerungen), dürfen wir  $a, b > 0$  annehmen. Dann wählen wir im Zentrum einer  $p$ -Sylowgruppe  $S$  ein Element  $g \neq e_G$ . Das geht wiederum, weil  $S$  nilpotent ist.

Wenn dann  $s$  im Zentrum von  $G$  liegt, sind wir fertig ( $g$  erzeugt einen nichttrivialen Normalteiler), und ansonsten ist die Mächtigkeit der Konjugationsklasse von  $s$  eine  $q$ -Potenz  $> 1$  und mit Satz 2.5.21 sind wir wieder fertig.  $\circ$