Algebra 2

Schriftliche Unterlagen zur Vorlesung
im Sommersemester 2013

Franz Pauer

Institut für Mathematik
Universität Innsbruck

KAPITEL 1

Moduln über $\mathbb{Z}$ und $K[x]$

In diesem Kapitel werden u.a. die folgenden Fragen beantwortet: Wie beschreibt man die Menge der ganzzahligen Lösungen eines Systems linearer Gleichungen mit ganzzahligen Koeffizienten? Wie kann man entscheiden, ob zwei Matrizen ähnlich sind?

Mit R wird immer ein kommutativer Ring und mit K immer ein Körper bezeichnet.

§1. Zur Beschreibung von endlich erzeugten Moduln

Definition 1 :

- $R^{m\times n}$:= Menge der $m \times n$-Matrizen mit Koeffizienten in R.
- $GL(n, R)$:= Menge der Matrizen in $R^{n\times n}$, die invertierbar sind.
- Für $A \in R^{n\times n}$ sei $\det(A) := \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) A_{1\sigma(1)} \cdots A_{n\sigma(n)}$ (Determinante von A).
- Zwei Matrizen $A, B \in R^{m\times n}$ sind genau dann *äquivalent*, wenn es Matrizen $P \in GL(m, R),\ Q \in GL(n, R)$ gibt so, dass
$$B = P \circ A \circ Q\ .$$
- Zwei Matrizen $A, B \in R^{n\times n}$ sind genau dann *ähnlich*, wenn es eine Matrix $P \in GL(n, R)$ gibt so, dass
$$B = P^{-1} \circ A \circ P\ .$$

Satz 1 : *Je zwei Basen eines endlich erzeugten freien Moduls über einem kommutativen Ring haben gleich viele Elemente. Die Anzahl der Elemente einer Basis heißt* Dimension *des Moduls.*

Definition 2 : Ein R-Modul M ist *durch Erzeugende und Relationen* gegeben, wenn eine surjektive R-lineare Abbildung $f : R^n \longrightarrow M$ und ein Erzeugendensystem des Kerns von f gegeben sind. Die Elemente $f(e_1), \ldots, f(e_n)$ sind dann die Erzeugenden, die Elemente des Erzeugendensystems von $\operatorname{Kern}(f)$ die Relationen.

Beispiel 1 : Die Spalten einer Matrix $A \in R^{m\times n}$ sind die Erzeugenden ihres Spaltenraums ($\leq_R R^m$), die Relationen dieses $R-$Moduls sind ein

Erzeugendensystem des Lösungsraums ($\leq_R R^n$) des durch A definierten homogenen Systems linearer Gleichungen.

§2. Matrizen mit Koeffizienten in $\mathbb{Z}$ oder $K[x]$

Satz 2 : *Jede ganzzahlige $m \times n$-Matrix A ist zu genau einer Diagonalmatrix $Diag(c_1, \ldots, c_k, 0, \ldots, 0)$ mit $c_1|c_2|\ldots|c_k$ und $c_1 > 0, \ldots, c_k > 0$ äquivalent.*

Jede $m \times n$-Matrix A mit Koeffizienten in $K[x]$ ist zu genau einer Diagonalmatrix $Diag(c_1, \ldots, c_k, 0, \ldots, 0)$ mit $c_1|c_2|\ldots|c_k$ und $lk(c_1) = \ldots = lk(c_k) = 1$ äquivalent.

Die Elemente $c_1, \ldots, c_k$ heißen Elementarteiler *von A. Sie können (natürlich unter Verwendung der Division mit Rest!) in endlich vielen Schritten berechnet werden und sind durch A eindeutig bestimmt. Insbesondere sind zwei $m \times n$- Matrizen mit Koeffizienten in $\mathbb{Z}$ oder $K[x]$ genau dann äquivalent, wenn ihre Elementarteiler gleich sind.*

§3. Endlich erzeugte Moduln über $\mathbb{Z}$ oder $K[x]$

Satz 3 : *Es seien R ein noetherscher Ring und M ein endlich erzeugter R-Modul. Dann ist M ein noetherscher R-Modul, das heißt: Jeder Untermodul von M ist endlich erzeugt.*

Satz 4 : *Es sei $R = \mathbb{Z}$ oder $R = K[x]$. Für jeden Untermodul U eines endlich erzeugten freien R-Moduls V gibt es eine Basis $(v_1, \ldots, v_n)$ von V und Elemente $c_1, \ldots, c_k \in R$ so, dass $c_1|c_2|\ldots|c_k$ und $c_1v_1, \ldots, c_kv_k$ eine R-Basis von U ist. Insbesondere ist jeder Untermodul eines endlich erzeugten freien R-Moduls frei.*

Satz 5 : *Es seien $R = \mathbb{Z}$ oder $R = K[x]$ und M ein endlich erzeugter R-Modul. Dann gibt es natürliche Zahlen k, ℓ und Elemente $c_1, \ldots, c_k \in R$ mit $c_1|c_2|\ldots|c_k$ so, dass M zu*

$$R/Rc_1 \times R/Rc_2 \times \ldots \times R/Rc_k \times R^\ell$$

isomorph ist.

Satz 6 : *(Klassifikation der endlich erzeugten abel'schen Gruppen) Jede endlich erzeugte abel'sche Gruppe ($\mathbb{Z}$-Modul) ist isomorph zu*

$$\mathbb{Z}_{c_1} \times \mathbb{Z}_{c_2} \times \ldots \times \mathbb{Z}_{c_k} \times \mathbb{Z}^{\ell},$$

wobei $k, \ell \in \mathbb{N}, c_1, \ldots, c_k \in \mathbb{N}_{>0}$ und $c_1|c_2|\ldots|c_k$.

Die Zahlen $k, \ell, c_1, \ldots, c_k$ sind eindeutig bestimmt.

§4. Ähnlichkeitsinvarianten

Satz 7 : *Es seien V ein K-Vektorraum und f eine K-lineare Abbildung von V nach V. Dann ist V mit*

$$K[x] \times V \longrightarrow V \ , \ (g, v) \longmapsto g \circ v := g(f)(v)$$

ein $K[x]$-Modul. Ein Untervektorraum U von V ist genau dann ein $K[x]$-Untermodul, wenn U stabil unter f ist, d.h.: $f(U) \subseteq U$.

Sei umgekehrt V ein $K[x]$-Modul. Dann ist V insbesondere ein K-Vektorraum und die Abbildung

$$f : V \longrightarrow V \ , \ v \longmapsto x \circ v \ ,$$

ist K-linear.

„Ein K-Vektorraum mit einer linearen Abbildung ist ein $K[x]$-Modul (und umgekehrt).“

Satz 8 : *Zwei Matrizen $A, B \in K^{n \times n}$ sind genau dann ähnlich, wenn die Matrizen $A - x \cdot I_n$ und $B - x \cdot I_n$ in $K[x]^{n \times n}$ äquivalent sind.*

KAPITEL 2

Endliche Körper

§1. Endliche Körper

In diesem Abschnitt seien p eine positive Primzahl und L ein endlicher Körper der Charakteristik p. Durch

$$\mathbb{Z}_p \longrightarrow L\,,\ \bar{n} \longmapsto n \cdot 1_L\,,$$

fassen wir $\mathbb{Z}_p$ als Unterkörper von L auf. Wir bezeichnen mit r die Dimension von L als Vektorraum über $\mathbb{Z}_p$, dann ist $q := p^r$ die Anzahl der Elemente von L.

Beispiel 2 : Das Polynom $x^2 + x + 1$ ist über $\mathbb{Z}_2$ irreduzibel, also ist $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ ein Körper der Charakteristik 2 mit 4 Elementen. Seine Elemente sind $\bar{0}, \bar{1}, \bar{x}$ und $\overline{x+1}$. Es ist $\bar{x} \cdot \overline{(1+x)} = \bar{1}$.

Satz 9 : *Die multiplikative Gruppe $L \setminus \{0\}$ ist zyklisch, d.h.: es gibt ein Element $a \in L$ so, dass*

$$L \setminus \{0\} = \{1, a, a^2, \ldots, a^{q-2}\}\,.$$

Ein Element mit dieser Eigenschaft heißt primitives Element *des Körpers L.*

Satz 10 : *Es gibt bis auf Isomorphie genau einen Körper L mit $q = p^r$ Elementen. Er wird häufig als* Galoiskörper *$GF(q)$ bezeichnet. Das Polynom $x^q - x$ hat keine mehrfachen Nullstellen und zerfällt über L in Linearfaktoren, insbesondere ist L die Menge der Nullstellen von $x^q - x$.*

Satz 11 : *Es gibt genau r Ringhomomorphismen von L nach L. Diese sind $\mathbb{Z}_p$-linear und haben die Form*

$$L \longrightarrow L\,,\ z \longmapsto z^{p^m}\,,\ 0 \le m \le r-1\,.$$

Satz 12 : *Das Polynom $x^{p^r} - x$ ist das Produkt aller irreduziblen normierten Polynome in $\mathbb{Z}_p[x]$, deren Grad die Zahl r teilt. Der Körper*

L enthält genau dann einen Unterkörper mit p^m Elementen, wenn m die Zahl r teilt.

Beispiel 3 : Ein *linearer (n,k)-Code* ist ein k-dimensionaler Untervektorraum eines n-dimensionalen Vektorraums über einem endlichen Körper L. Seine Elemente heißen *Worte* des Codes. Ein linearer Code ist *zyklisch*, wenn er mit jedem Wort $(a_0, \ldots, a_{n-1})$ auch das Wort $(a_1, \ldots, a_{n-1}, a_0)$ enthält. Wir betrachten ein Wort $(a_0, \ldots, a_{n-1})$ in L^n als Restklasse eines Polynoms

$$\overline{\sum_{i=0}^{n-1} a_i x^i} \in L[x]/\langle x^n - 1\rangle \ .$$

Dann ist ein (n, k)-Code genau dann zyklisch, wenn er ein Ideal in $L[x]/\langle x^n - 1\rangle$ ist. Dieses Ideal wird von der Restklasse eines normierten Polynoms vom Grad $n - k$ erzeugt, welches das Polynom $x^n - 1$ teilt. Also entspricht jedem solchen Polynom in $L[x]$ genau ein zyklischer (n, k)-Code und umgekehrt.

§2. Ein Verfahren zur Faktorisierung von Polynomen in $\mathbb{Z}_p[x]$

Es seien p eine positive Primzahl und f ein Polynom in $\mathbb{Z}_p[x]$ mit positivem Grad. In $\mathbb{Z}_p[x]$ ist

$$x^p - x = \prod_{a \in \mathbb{Z}_p} (x - a)\,,$$

daher gilt für alle $g \in \mathbb{Z}_p[x]$:

$$g^p - g = \prod_{a \in \mathbb{Z}_p} (g - a)\,.$$

Die Polynome $g - a$, $a \in \mathbb{Z}_p$, sind paarweise teilerfremd, denn: Ist für $a, b \in \mathbb{Z}_p$ mit $a \neq b$ ein Polynom $h \in \mathbb{Z}_p[x]$ ein gemeinsamer Teiler von $g - a$ und $g - b$, dann ist h auch ein Teiler von $(g - a) - (g - b) = b - a \in \mathbb{Z}_p \setminus \{0\}$, also $h \in \mathbb{Z}_p$. Daher ist

$$\mathrm{ggT}(f, g^p - g) = \prod_{a \in \mathbb{Z}_p} \mathrm{ggT}(f, g - a).$$

Die Idee des "Algorithmus von Berlekamp" zur Zerlegung von f ist: Finde ein Polynom $g \in \mathbb{Z}_p[x]$ so, dass

$$f \text{ das Polynom } g^p - g \text{ teilt}$$

und

$$0 < \deg(g) < \deg(f)$$

ist. Dann ist

$$f = \mathrm{ggT}(f, g^p - g) = \prod_{a \in \mathbb{Z}_p} \mathrm{ggT}(f, g - a).$$

eine nicht triviale Zerlegung von f.

Satz 13: *Die Abbildung*

$$\pi : \mathbb{Z}_p[x]/\langle f\rangle \to \mathbb{Z}_p[x]/\langle f\rangle \ , \quad \bar{h} \longmapsto \bar{h}^p \ ,$$

ist $\mathbb{Z}_p$-linear, die Menge

$$\{\bar{g} \in \mathbb{Z}_p[x]/\langle f\rangle \mid g \in \mathbb{Z}_p[x],\ f \text{ teilt } g^p - g\}$$

ist ihr Eigenraum zum Eigenwert 1.

Beweis: Für $0 < i < p$ ist $\binom{p}{i} \in \mathbb{Z}$ ein Vielfaches von p. Daher ist

$$\begin{aligned} \pi(\bar{h}_1 + \bar{h}_2) &= (\bar{h}_1 + \bar{h}_2)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} \bar{h}_1^{p-i} \bar{h}_2^i \\ &= \bar{h}_1^p + \bar{h}_2^p. \end{aligned}$$

Für $c \in \mathbb{Z}_p$ ist $c^p = c$, also $\pi(c\bar{h}) = c\pi(\bar{h})$. Somit ist π $\mathbb{Z}_p$-linear.
Das Polynom f teilt $g^p - g$ genau dann, wenn $\overline{g^p - g} = \bar{0}$, also $\pi(\bar{g}) = \bar{g}$ ist.

Definition 3: Ein Polynom $\neq 0$ mit Koeffizienten in einem Körper K ist *quadratfrei*, wenn seine irreduziblen Faktoren paarweise nicht assoziiert sind.

Nach dem folgenden Satz genügt es, ein Verfahren für die Zerlegung von *quadratfreien* Polynomen in irreduzible Faktoren zu suchen.

Satz 14: *Mit dem folgenden Verfahren kann das Produkt aller (paarweise nicht assoziierten) irreduziblen Faktoren von f berechnet werden:*

- *Setze $h := 1$.*
- *Solange $g := \mathrm{ggT}\left(f, D(f)\right) \neq 1$:*
  - *Wenn $D(f) \neq 0$, ersetze h durch $\frac{f}{g} \cdot h$ und f durch*

$$\frac{f}{\mathrm{ggT}(f, (\frac{f}{g})^{\deg(f)})} \ .$$

  - *Wenn $D(f) = 0$, ersetze f durch das Polynom f_1 mit $f_1^p = f$.*

Dann ist $f \cdot h$ quadratfrei und wird von jedem irreduziblen Faktor des anfangs gegebenen Polynoms f geteilt.

Beweis: Sei $f = \mathrm{lk}(f) f_1^{e_1} f_2^{e_2} \cdot \ldots \cdot f_k^{e_k}$, wobei $f_1, \ldots, f_k$ paarweise nicht assoziierte, normierte und irreduzible Polynome, sowie $e_1, \ldots, e_k$ positive ganze Zahlen sind.

Seien

$$\mathcal{M} := \{i \mid 1 \leq i \leq k,\ p \text{ teilt } e_i\}$$

und

$$\mathcal{N} := \{i \mid 1 \leq i \leq k,\ p \text{ teilt } e_i \text{ nicht}\}.$$

Es ist

$$D(f) = \sum_{i=1}^{k} e_i \frac{f}{f_i} D(f_i) = \sum_{i \in \mathcal{N}} e_i \frac{f}{f_i} D(f_i).$$

Daraus folgt

$$g := \mathrm{ggT}\left(f, D(f)\right) = \prod_{i \in \mathcal{N}} f_i^{e_i - 1} \prod_{i \in \mathcal{M}} f_i^{e_i}.$$

Daher ist $\frac{f}{g} = \prod_{i \in \mathcal{N}} f_i$,

$$\mathrm{ggT}\left(f, \left(\frac{f}{g}\right)^{\deg(f)}\right) = \prod_{i \in \mathcal{N}} f_i^{e_i}$$

und

$$\frac{f}{\mathrm{ggT}\left(f, \left(\frac{f}{g}\right)^{\deg(f)}\right)} = \prod_{i \in \mathcal{M}} f_i^{e_i} = \Big(\prod_{i \in \mathcal{M}} f_i^{\frac{e_i}{p}} \Big)^p.$$

Nun kann die Behauptung leicht nachgeprüft werden.

Beispiel 4: Es sei $f := x^8 + x^6 + 2x^5 + 2x^3 + x^2 + 1 \in \mathbb{Z}_3[x]$. Dann ist

$$\begin{aligned} D(f) &= 2x^7 + x^4 + 2x, \\ g &:= \mathrm{ggT}(f, D(f)) = x^6 + 2x^3 + 1, \\ h &:= \frac{f}{g} = x^2 + 1, \\ \mathrm{ggT}(f, h^8) &= x^2 + 1, \\ u &:= \frac{f}{x^2 + 1} = x^6 + 2x^3 + 1. \end{aligned}$$

Nun ist $D(u) = 0$ und $u = (x^2 + 2x + 1)^3$. Setze $u_1 := x^2 + 2x + 1$. Dann ist

$$\begin{aligned} D(u_1) &= 2x + 2, \\ \mathrm{ggT}\big(u_1, D(u_1)\big) &= x + 1, \\ h &:= (x^2+1)\frac{u_1}{x+1} = (x^2+1)(x+1), \\ \mathrm{ggT}\big(u_1, (x+1)^2\big) &= u_1. \end{aligned}$$

Also ist $(x^2 + 1)(x + 1)$ das Produkt der paarweise nicht assoziierten irreduziblen Faktoren von f.

Satz 15 : *Das Polynom $f \in \mathbb{Z}_p[x]$ sei quadratfrei. Dann gilt:*

(1) *Die Dimension des Eigenraums von*

$$\pi : \mathbb{Z}_p[x]/\langle f\rangle \to \mathbb{Z}_p[x]/\langle f\rangle, \quad \bar{h} \mapsto \bar{h}^p,$$

zum Eigenwert 1 ist gleich der Anzahl der irreduziblen Faktoren von f.

(2) *Sei B eine Teilmenge von $\mathbb{Z}_p[x]$ so, dass $(\bar{b})_{b\in B}$ eine $\mathbb{Z}_p$-Basis des Eigenraums von π zum Eigenwert 1 ist. Dann gibt es zu je zwei nicht assoziierten irreduziblen Faktoren f_i, f_j von f ein Element $a \in \mathbb{Z}_p$ und ein Polynom $b \in B$ so, dass $b - a$ ein Vielfaches von f_i, aber nicht von f_j ist.*

Beweis: Seien $f_1, \ldots, f_k$ die irreduziblen Faktoren von f. Dann ist

$$f = f_1 \cdot f_2 \cdot \ldots \cdot f_k$$

und die Abbildung

$$\begin{aligned} \chi : \quad \mathbb{Z}_p[x]/\langle f\rangle \quad &\to \quad \prod_{i=1}^k \mathbb{Z}_p[x]/\langle f_i\rangle \\ \bar{h} \quad &\mapsto \quad (\bar{h}, \ldots, \bar{h}) =: (\bar{h}_1, \ldots \bar{h}_k) \end{aligned}$$

ist ein Isomorphismus von $\mathbb{Z}_p$-Algebren.

(1) Es ist $\bar{h}^p = \bar{h} \in \mathbb{Z}_p[x]/\langle f\rangle$ genau dann, wenn $\bar{h}_i^p = \bar{h}_i \in \mathbb{Z}_p[x]/\langle f_i\rangle$, $1 \le i \le k$. Weil f_i irreduzibel, also $\mathbb{Z}_p[x]/\langle f_i\rangle$ ein Körper ist, ist $\bar{h}_i^p = \bar{h}_i$ genau dann, wenn $\bar{h}_i \in \mathbb{Z}_p \subseteq \mathbb{Z}_p[x]/\langle f_i\rangle$ ist, $1 \le i \le k$.
Somit ist $\chi\big(\mathrm{Kern}(\pi - \mathrm{Id})\big) = \mathbb{Z}_p^k \subseteq \prod_{i=1}^k \mathbb{Z}_p[x]/\langle f_i\rangle$.

(2) Seien $1 \le i < j \le k$. Dann gibt es ein $b \in B$ so, dass $\bar{b}_i \neq \bar{b}_j$. (Denn sonst wären für alle $\bar{h} \in \mathrm{Kern}(\pi - \mathrm{Id})$ die Komponenten $\bar{h}_i$ und $\bar{h}_j$ gleich, also $\chi\big(\mathrm{Kern}(\pi - \mathrm{Id})\big) \subsetneqq \mathbb{Z}_p^k$, Widerspruch zu (1)).

Sei $a := \bar{b}_i \in \mathbb{Z}_p$. Dann ist $\overline{(b-a)}_i = \bar{0}$ und $\overline{(b-a)}_j \neq \bar{0}$, das heißt: $b-a$ ist ein Vielfaches von f_i aber nicht von f_j.

Satz 16: *Das Polynom $f \in \mathbb{Z}_p[x]$ sei quadratfrei. Mit dem folgenden Verfahren ("Berlekamp-Algorithmus") können alle irreduziblen Faktoren von f berechnet werden:*

- *Berechne $g_1 := 1, g_2, \ldots, g_k \in \mathbb{Z}_p[x]$ so, dass $\bar{g}_1, \ldots \bar{g}_k$ eine $\mathbb{Z}_p$-Basis von $\mathrm{Kern}(\pi - \mathrm{Id})$ und $\deg(g_i) < \deg(f),\ 1 \leq i \leq k$, ist.*
- *Setze $i := 1$ und $IF := \{f\}$.*
- *Solange $\#(IF) < k$, ersetze i durch $i+1$ und IF durch*

$$\big\{\, \mathrm{ggT}(h, g_i - a) \mid h \in IF,\ a \in \mathbb{Z}_p \big\} \setminus \{1\}.$$

Dann ist IF die Menge der irreduziblen Faktoren von f.

Beweis: Wenn $i = k$ ist, enthält IF nur noch irreduzible Polynome. Denn sonst würde IF ein Polynom enthalten, das von zwei Polynomen $f_i, f_j,\ i \neq j$, geteilt wird. Dann würde aber für alle $\ell \in \{1, 2, \ldots, k\}$ und alle $a \in \mathbb{Z}_p$ gelten:

$g_\ell - a$ ist entweder ein gemeinsames Vielfaches von f_i und f_j, oder es wird weder von f_i noch von f_j geteilt.

Widerspruch zu (2) im Satz 15.

Beispiel 5: Seien $p = 3$ und $f := x^6 + x^4 + x^2 + 1 \in \mathbb{Z}_3[x]$. Dann ist f quadratfrei und $(1, \bar{x}^3 + \bar{x}, \bar{x}^4)$ ist eine $\mathbb{Z}_3$-Basis von $\mathrm{Kern}(\pi - \mathrm{Id})$. Es ist

$$\begin{aligned} \mathrm{ggT}(f, x^3 + x) &= x^2 + 1, \\ \mathrm{ggT}(f, x^3 + x - 1) &= x^2 - x - 1, \\ \mathrm{ggT}(f, x^3 + x + 1) &= x^2 + x - 1, \end{aligned}$$

also $IF = \{x^2+1, x^2-x-1, x^2+x-1\}$ ist die Menge der irreduziblen Faktoren von $x^6 + x^4 + x^2 + 1 \in \mathbb{Z}_3[x]$.

KAPITEL 3

Gruppen und Symmetrien

Mit G wird immer eine Gruppe und mit K immer ein Körper bezeichnet.

§1. Operationen von Gruppen (Wiederholung)

Mit M wird immer eine Menge bezeichnet.

Definition 4 : Eine Funktion $G \times M \longrightarrow M\,,\ (s,m) \longmapsto s \cdot x\,,$ heißt *Operation der Gruppe G auf der Menge M*, wenn gilt:
für alle $m \in M$ ist $e \cdot m = m$ (e ist das neutrale Element von G) und
für alle $s,t \in G$ und alle $m \in M$ ist $(st) \cdot m = s \cdot (t \cdot m)$.

Satz 17 : *Es sei $G \times M \longrightarrow M\,,\ (s,m) \longmapsto s \cdot m\,,$ eine Operation. Dann ist die Funktion $G \longrightarrow S(M)\,,\ s \longmapsto [m \longmapsto s \cdot m]\,,$ ein Gruppenhomomorphismus.*
Sei umgekehrt $f : G \longrightarrow S(M)$ ein Gruppenhomomorphismus. Dann ist $G \times M \longrightarrow M\,,\ (s,m) \longmapsto f(m)\,,$ eine Operation.

Satz 18 : *Jede endliche Gruppe mit n Elementen ist zu einer Untergruppe von S_n isomorph.*

Definition 5 : Es seien $G \times M \longrightarrow M\,,\ (s,m) \longmapsto s \cdot m\,,$ eine Operation, $s \in G$ und $m \in M$. Dann heißt

- $G \cdot m := \{s \cdot m \mid s \in G\}$ *G-Bahn durch m*,
- $G_m := \{s \in G \mid s \cdot m = m\}$ *Stabilisatorgruppe* oder *Isotropiegruppe* von G in m und
- M/G *Menge der G-Bahnen in M* (Sprechweise: M modulo G).

Enthält die Bahn von G durch m nur ein Element, dann heißt m *Fixpunkt von G in M*. Die Menge aller Fixpunkte von G in M wird mit ${}^{G}M$ bezeichnet.
Eine Teilmenge N von M ist *G-stabil*, wenn mit jedem Element von N auch die G-Bahn durch dieses Element in N enthalten ist.
Die Operation von G auf M ist *frei*, wenn die Stabilisatorgruppe jedes Elementes von M nur ein Element enthält.

Die Operation von G auf M ist *transitiv*, wenn es in M nur eine einzige G-Bahn gibt.

Beispiel 6 : Es seien V ein euklidischer Raum, G die Gruppe aller Isometrien von V und $Pot(V)$ die Potenzmenge von V. Zwei Teilmengen sind genau dann euklidisch kongruent, wenn sie in derselben Bahn der Operation

$$G \times Pot(V) \longrightarrow Pot(V)\,,\ (g, M) \longmapsto g(M)\ ,$$

liegen. Die Mengen aller Quadriken in V und aller affinen Unterräume von V sind G-stabile Teilmengen von $Pot(V)$.

Satz 19 : *Es sei* $G \times M \longrightarrow M\,,\ (s, m) \longmapsto s \cdot m\,,$ *eine Operation.*

- *M ist die disjunkte Vereinigung der G-Bahnen in M (dh.: durch „zwei Elemente von M sind genau dann äquivalent, wenn sie in der gleichen G-Bahn liegen“ wird eine Äquivalenzrelation definiert).*
- *Die Stabilisatorgruppe eines Elementes in M ist eine Untergruppe von G.*
- *Die Stabilisatorgruppen von zwei Elementen einer G-Bahn sind konjugiert, dh.: für $s \in G$ und $m \in M$ ist $G_{s\cdot m} = sG_m s^{-1} = \{sgs^{-1} \mid g \in G_m\}$.*

§2. Darstellungen von Gruppen

Es sei V ein Vektorraum über K.

Definition 6 : Eine Operation $G \times V \longrightarrow V\,,\ (s, v) \longmapsto s \cdot v\,,$ heißt *Darstellung oder lineare Operation*, wenn gilt:
für alle $c \in K$, $v, w \in V$, $s \in G$ ist $s \cdot (c(v + w)) = c(s \cdot v) + c(s \cdot w)$.

Satz 20 : *Es sei* $G \times V \longrightarrow V\,,\ (s, v) \longmapsto s \cdot v\,,$ *eine Darstellung. Dann ist die Funktion* $G \longrightarrow GL_K(V)\,,\ s \longmapsto [v \longmapsto s \cdot v]\,,$ *wohldefiniert und ein Gruppenhomomorphismus.*
Sei umgekehrt $f : G \longrightarrow GL_K(V)$ *ein Gruppenhomomorphismus. Dann ist* $G \times V \longrightarrow V\,,\ (s, v) \longmapsto f(s)(v)\,,$ *eine Darstellung.*

Beispiel 7 : Die Operation $G \times V \longrightarrow V\,,\ (s, v) \longmapsto v\,,$ ist linear und heißt *triviale Darstellung* von G in V.

Beispiel 8 : Es sei G eine Untergruppe von $GL_K(V)$. Die Operation

$$G \times V \longrightarrow V\,,\ (f,v) \longmapsto f(v)\,,$$

von G auf V ist linear und heißt *natürliche Darstellung* von G.

Beispiel 9 : Es seien M eine Menge, $G \times M \to M$, $(s,x) \mapsto s \cdot x$, eine Operation, $G \times V \longrightarrow V\,,\ (s,v) \longmapsto s \cdot v\,,$ eine Darstellung (zum Beispiel die triviale Darstellung von G in K) und $\mathcal{F}(M,V)$ der Vektorraum aller Funktionen von M nach V (mit punktweiser Addition und Skalarmultiplikation). Dann ist

$$G \times \mathcal{F}(M,V) \longrightarrow \mathcal{F}(M,V)\,,\ (s,f) \longmapsto [x \longmapsto s \cdot f(s^{-1} \cdot x)]\,,$$

eine Darstellung.

Beispiel 10 : Es seien $\varphi : G \times V \longrightarrow V\,,\ (s,v) \longmapsto s \cdot v\,,$ eine Darstellung und W ein G-stabiler Untervektorraum von V. Dann ist $G \times W \longrightarrow W\,,\ (s,v) \longmapsto s \cdot v\,,$ wohldefiniert und eine Darstellung von G. Diese heißt *Einschränkung* von φ auf W.
Sind $\varphi : G \times U \longrightarrow U$ und $G \times V \longrightarrow V$ Darstellungen von G, dann ist der Vektorraum $Lin_K(U,V)$ aller linearen Funktionen von U nach V ein G-stabiler Untervektorraum von $\mathcal{F}(U,V)$. Ist speziell $V = K$ und die Darstellung von G in K trivial, dann heißt die Darstellung

$$\varphi^* : G \times U^* := Lin_K(U,K) \longrightarrow U^*\,,\ (s,f) \longmapsto [u \longmapsto f(s^{-1} \cdot u)]\,,$$

die zur Darstellung φ *duale Darstellung*.

Definition 7 : Eine Darstellung von G in V heißt *einfach* oder *irreduzibel*, wenn $\{0\}$ und V die einzigen G-stabilen Untervektorräume von V sind.

Definition 8 : Es seien $G \times M \longrightarrow M$ und $G \times N \longrightarrow N$ Operationen der Gruppe G auf den Mengen M und N. Eine Funktion $f : M \longrightarrow N$ heißt *G-äquivariant* wenn gilt:

$$\text{für alle } s \in G,\ m \in M \text{ ist } f(s \cdot m) = s \cdot f(m)\,.$$

Es seien $G \times U \longrightarrow U$ und $G \times V \longrightarrow V$ Darstellungen der Gruppe G in den K-Vektorräumen U und V. Eine lineare und G-äquivariante Funktion $f : U \longrightarrow V$ heißt *Morphismus von Darstellungen*. Ein *Isomorphismus* von Darstellungen ist ein bijektiver Morphismus von Darstellungen. Zwei Darstellungen von G (in U und V) sind *isomorph*, wenn es einen Isomorphismus von Darstellungen von U nach V gibt.

Beispiel 11 : Es seien G eine kommutative Gruppe und V ein endlichdimensionaler komplexer Vektorraum. Eine Darstellung von G in V ist genau dann einfach, wenn V eindimensional ist.

Beispiel 12 : Es seine V ein euklidischer Raum und G die orthogonale Gruppe von V. Dann ist die Funktion

$$V \longrightarrow V^* \,,\; v \longmapsto \langle v, - \rangle$$

ein Isomorphismus von Darstellungen. Die natürliche Darstellung von $GL_{\mathbb{R}}(V)$ und die dazu duale sind jedoch nicht isomorph.

Satz 21 : *(„Lemma von Schur") V und W seien einfache Darstellungen von G.*

- *Jeder Morphismus von Darstellungen von V nach W ist entweder die Nullfunktion oder ein Isomorphismus.*
- *Ist V ein endlichdimensionaler komplexer Vektorraum, dann ist jeder Morphismus f von Darstellungen von V nach V ein skalares Vielfaches der Identität (und zwar: $f = \frac{Spur(f)}{\dim_{\mathbb{C}}(V)} id_V$.)*
- *Es seien V ein unitärer Raum und f eine $\mathbb{C}$-lineare Funktion, die mit jeder unitären Funktion von V nach V vertauschbar ist. Dann ist f ein skalares Vielfaches der Identität.*

§3. Zerlegbare Darstellungen

Es seien G eine Gruppe, V ein Vektorraum und $G \times V \longrightarrow V$ eine Darstellung.

Definition 9 :

- $(V_i)_{i \in I}$ sei eine Familie von Darstellungen von G. Dann ist

  $$G \times \bigoplus_{i \in I} V_i \longrightarrow \bigoplus_{i \in I} V_i \,,\; (v_i)_{i \in I} \longmapsto (s \cdot v_i)_{i \in I} \,,$$

  eine Darstellung und heißt *direkte Summe* der Darstellungen V_i, $i \in I$.
- Die Darstellung von G in V heißt *zerlegbar*, wenn V die direkte Summe zweier nichttrivialer G-stabiler Untervektorräume ist.
- Ein G-stabiler Untervektorraum W von V heißt *G-stabiles Komplement* eine G-stabilen Untervektorraums U von V, wenn V die direkte Summe $U \oplus W$ ist.
- Die Darstellung von G in V ist *vollständig reduzibel*, wenn jeder G-stabile Untervektorraum von V ein G-stabiles Komplement hat.

Beispiel 13 : Die Darstellung

$$GL(n, \mathbb{C}) \times \mathbb{C}^{n \times n} \longrightarrow \mathbb{C}^{n \times n}, (A, X) \longmapsto A \circ X \circ A^{-1},$$

ist die direkte Summe der $GL(n, \mathbb{C})$-stabilen Unterräume $\{X \in \mathbb{C}^{n \times n} \mid Spur(X) = 0\}$ und $\mathbb{C} \cdot I_n$.

Satz 22 : *(„Satz von Maschke") G sei eine endliche Gruppe, deren Ordnung von der Charakteristik des Körpers K nicht geteilt wird. Dann hat jeder G-stabile Untervektorraum von V ein G-stabiles Komplement.*

Satz 23 : *Ist V endlichdimensional, dann ist eine Darstellung von G in V genau dann vollständig reduzibel, wenn sie V direkte Summe von einfachen Darstellungen ist.*

Definition 10 : Es sei V mit $\langle -, - \rangle$ ein unitärer Raum. Das Skalarprodukt heißt *G-invariant*, wenn für alle $s \in G$ und alle $v, w \in V$ gilt:

$$\langle s \cdot v, s \cdot w \rangle = \langle v, w \rangle .$$

Satz 24 :

(1) *Es seien G eine endliche Gruppe und V ein komplexer Vektorraum. Dann gibt es auf V ein G-invariantes Skalarprodukt.*
(2) *Jede endliche Untergruppe von $GL(n, \mathbb{C})$ ist konjugiert zu einer Untergruppe der unitären Gruppe $U(n)$.*
(3) *Jede Matrix in $GL(n, \mathbb{C})$ mit endlicher Ordnung ist diagonalisierbar.*

Definition 11 : Ist τ eine einfache Darstellung von G, dann heißt die Summe aller zu τ isomorphen G-stabilen Untervektorräume von V die *isotypische Komponente von V vom Typ τ.*

Satz 25 : *Annahme: Die Darstellung von G in V ist vollständig reduzibel. Die Funktion $\tau : G \longrightarrow GL_K(U)$ sei eine einfache Darstellung von G.*

(1) *Jeder einfache G-stabile Untervektorraum der isotypischen Komponente von V vom Typ τ ist zu U isomorph.*
(2) *V ist die direkte Summe seiner isotypischen Komponenten. Diese* Zerlegung von V in isotypische Komponenten *ist eindeutig bestimmt.*

Satz 26: *Es sei $\tau : G \longrightarrow GL_K(U)$ eine einfache Darstellung von G, $\rho : G \longrightarrow GL_K(V)$ sowie $\sigma : G \longrightarrow GL_K(W)$ seien vollständig reduzible Darstellungen von G und $f : V \longrightarrow W$ sei ein Morphismus von Darstellungen von G.*
Dann: $f(V_\tau) \subseteq W_\tau$ (das Bild bezüglich f der isotypischen Komponente von V vom Typ τ ist in der isotypischen Komponente von W vom Typ τ enthalten).

§4. Symmetriegerechte Basen

Es seien G eine Gruppe, V ein komplexer Vektorraum und $G \times V \longrightarrow V$ eine vollständig reduzible endlich-dimensionale Darstellung.

Definition 12: Es sei $\sigma : G \longrightarrow GL_K(W)$ eine vollständig reduzible endlich-dimensionale Darstellung von G, die nur eine isotypische Komponente hat. $W = W_1 \oplus W_2 \oplus \ldots \oplus W_n$ sei eine Zerlegung von W in eine direkte Summe von G-stabilen einfachen Untervektorräumen von W. Die Darstellungen W_i sind paarweise isomorph, wir wählen Isomorphismen $g_i : W_1 \longrightarrow W_i$, $2 \leq i \leq n$. Weiters wählen wir eine Basis $(w_1, w_2, \ldots, w_d)$ von W_1. Dann heißt die Basis

$$(w_1, g_2(w_1), \ldots, g_n(w_1), w_2, g_2(w_2), \ldots, g_n(w_2), \ldots$$

$$\ldots, w_d, g_2(w_d), \ldots, g_n(w_d))$$

eine *symmetriegerechte Basis* von W.

Satz 27: *Es sei $\sigma : G \longrightarrow GL_K(W)$ eine vollständig reduzible endlichdimensionale Darstellung von G, die nur eine isotypische Komponente hat. $W = W_1 \oplus W_2 \oplus \ldots \oplus W_n$ sei eine Zerlegung von W in eine direkte Summe von G-stabilen einfachen Untervektorräumen von W. Die Dimension des Vektorraums W_1 sei d. Die Matrix einer G-äquivarianten linearen Funktion $f : W \longrightarrow W$ bezüglich einer symmetriegerechten Basis hat die Blockdiagonalgestalt*

$$\begin{pmatrix} C & & & & \\ & C & & & \\ & & C & & \\ & & & \ddots & \\ & & & & C \end{pmatrix}$$

mit d Blöcken. Die Matrix C ist eine komplexe $n \times n$-Matrix. Insbesondere sind die Eigenwerte von f dieselben wie die der Matrix C. Die Vielfachheit jedes Eigenwertes von f ist ein Vielfaches von d.

Definition 13 : Es sei $V = V_1 \oplus V_2 \oplus \ldots \oplus V_m$ die Zerlegung der Darstellung V in ihre isotypischen Komponenten. Wir wählen symmetriegerechte Basen

$$\underline{v}(1), \underline{v}(2), \ldots, \underline{v}(m)$$

der isotypischen Komponenten $V_1, V_2 \ldots, V_m$. Dann heißt die Basis

$$(\underline{v}(1), \underline{v}(2), \cdots, \underline{v}(m))$$

eine *symmetriegerechte Basis* von V.

Satz 28 : *Die Matrix einer G-äquivarianten linearen Funktion von V nach V bezüglich einer symmetriegerechten Basis von V hat die Blockdiagonalgestalt*

$$\begin{pmatrix} C_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & C_1 & & & & & & \\ & & & C_2 & & & & & \\ & & & & \ddots & & & & \\ & & & & & C_2 & & & \\ & & & & & & \ddots & & \\ & & & & & & & C_m & \\ & & & & & & & & \ddots \\ & & & & & & & & & C_m \end{pmatrix}$$

Dabei ist m die Anzahl der isotypischen Komponenten der Darstellung V.
(Eine symmetriegerechte Basis von V muss nur einmal *berechnet werden, dann kann sie zur Berechnung der Eigenwerte* jeder *linearen G-äquivarianten Funktion von V nach V verwendet werden).*

§5. Komplexe Darstellungen endlicher Gruppen

In diesem Abschnitt sei G eine endliche Gruppe, e ihr neutrales Element und $\rho : G \longrightarrow GL_K(V)$ eine komplexe endlich-dimensionale Darstellung von G. Nach dem Satz von Maschke ist ρ vollständig reduzibel.

Definition 14 : Die Funktion

$$\chi_\rho : G \longrightarrow \mathbb{C},\ s \longmapsto Spur(\rho_s)$$

heißt *Charakter von ρ.*

Die Funktion $\chi : G \longrightarrow \mathbb{C}$ ist ein *Charakter von G*, wenn χ der Charakter einer endlich-dimensionalen Darstellung von G ist. Ein *einfacher*

(oder irreduzibler) Charakter von G ist der Charakter einer einfachen Darstellung von G.

Satz 29 :

1.) *Ist ρ eindimensional, dann ist χ_ρ ein Gruppenhomomorphismus von G nach $\mathbb{C} \setminus \{0\}$.*
2.) *Sind zwei Darstellungen ρ und σ isomorph, so sind ihre Charaktere gleich.*
3.) $\chi_\rho(e) = dim_{\mathbb{C}}(V)$
4.) *Der Charakter der direkten Summe zweier endlichdimensionaler Darstellungen von G ist die Summe ihrer Charaktere.*
5.) *Für alle $s \in G$ ist $\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}$.*

Definition 15 : Eine Funktion f von G nach $\mathbb{C}$ heißt *zentral*, wenn sie auf den Konjugationsklassen von G konstant ist (also: für alle $s, t \in G$ ist $f(sts^{-1}) = f(t)$.). Die Menge aller zentralen Funktionen von G nach $\mathbb{C}$ bezeichnen wir mit $Zent(G, \mathbb{C})$.

Satz 30 :

1.) *Die Charaktere von Darstellungen sind zentrale Funktionen. $Zent(G, \mathbb{C})$ ist ein Untervektorraum des Vektorraums aller Funktionen von G nach $\mathbb{C}$, seine Dimension ist die Anzahl der Konjugationsklassen von G.*
2.) $Zent(G, \mathbb{C}) \times Zent(G, \mathbb{C}) \longrightarrow \mathbb{C}$, $(f, g) \longmapsto \frac{1}{|G|} \sum_{s \in G} f(s)\overline{g(s)}$ *ist ein hermite'sches Skalarprodukt auf $Zent(G, \mathbb{C})$.*

Definition 16 : Die Darstellung

$$reg : G \longrightarrow GL_{\mathbb{C}}(\mathcal{F}(G, \mathbb{C})),\ s \longmapsto reg_s$$

mit $reg_s(f)(t) := f(s^{-1}t)$ heißt *reguläre Darstellung von G.*

Satz 31 : *Der Charakter der regulären Darstellung ist die Funktion*

$$\chi_{reg} : G \longrightarrow \mathbb{C},\ \chi_{reg}(s) \longmapsto |G| \cdot \delta_{se}\,.$$

Satz 32 :

1.) *Die Familie der irreduziblen Charaktere von G ist eine Orthonormalbasis von $Zent(G, \mathbb{C})$.*
2.) *Zwei Darstellungen sind genau dann isomorph, wenn ihre Charaktere gleich sind.*

Satz 33 :

1.) *Die Anzahl der irreduziblen Charaktere von G ist gleich der Anzahl der Konjugationsklassen von G.*
2.) *Ist $\tau : G \longrightarrow GL_{\mathbb{C}}(W)$ eine irreduzible Darstellung von G und $V = V_1 \oplus \ldots \oplus V_\ell$ eine Zerlegung von V in einfache Summanden, dann ist $\langle \chi_\tau, \chi_\rho \rangle$ die Anzahl der zu W isomorphen Summanden (die* Vielfachheit von τ in ρ*).*
3.) *Sind $\chi_1, \ldots, \chi_k$ alle irreduziblen Charaktere von G und $n_1, \ldots, n_k$ die Dimensionen der entsprechenden irreduziblen Darstellungen, dann ist*

$$\sum_{i=1}^{k} n_i^2 = |G| \, .$$

4.) *Eine Darstellung τ von G ist genau dann irreduzibel, wenn sie endlichdimensional ist und $\langle \chi_\tau, \chi_\tau \rangle = 1$ ist.*

Beispiel 14 : Wenn G kommutativ ist, dann ist $Zent(G, \mathbb{C}) = \mathcal{F}(G, \mathbb{C})$. Alle einfachen Darstellungen von G sind eindimensional. Die Menge der einfachen Charaktere von G ist die Menge der Gruppenhomomorphismen von G nach $\mathbb{C} \setminus \{0\}$.
Wenn $G = \langle s \rangle$ zyklisch ist und $k := |G|$ ist, dann sind die Gruppenhomomorphismen

$$\chi_n : G \longrightarrow \mathbb{C}, \; s^\ell \longmapsto e^{\frac{2\pi i}{k} n\ell}$$

$0 \leq n \leq k-1$ alle irreduziblen Charaktere.
Für $f : G \longrightarrow \mathbb{C}$ ist dann

$$f = \sum_{n=0}^{k-1} \langle f, \chi_n \rangle \chi_n = \frac{1}{k} \sum_{n=0}^{k-1} \sum_{\ell=0}^{k-1} f(s^\ell) e^{\frac{2\pi i}{k} n\ell} \chi_n$$

(„Fouriertransformation“).

Satz 34 : *Es seien $\chi_1, \chi_2, \ldots, \chi_k$ die irreduziblen Charaktere von G. Die Funktion*

$$p_i := \frac{\chi_i(e)}{|G|} \sum_{s \in G} \overline{\chi_i(s)} \rho_s \in End_{\mathbb{C}}(V)$$

ist die Projektion von V auf die isotypische Komponente vom Typ χ_i längs der Summe der anderen isotypischen Komponenten, $1 \leq i \leq k$.

Satz 35 : *Es seien τ eine irreduzible komplexe Darstellung von G, $n := \chi_\tau(e)$ und $(T(s)_{ij})_{1 \leq i,j \leq n}$, $s \in G$, die Matrizen von τ_s, $s \in G$, bezüglich*

einer fest gewählten Basis. Für $1 \leq i \leq n$ *sei*

$$q_i := \frac{n}{|G|} \sum_{s \in G} T(s^{-1})_{1i} \cdot \rho_s \in End_{\mathbb{C}}(V)\,.$$

Es sei $(v_1, \ldots, v_m)$ *eine* $\mathbb{C}$*-Basis von* $q_1(V) \leq V$ *und* W_j *der von*

$$\{v_j, q_2(v_j), \ldots, q_n(v_j)\}$$

erzeugte Untervektorraum von V*,* $1 \leq j \leq m$*. Dann sind* $W_1, \ldots, W_m$ *irreduzible* G*-stabile Untervektorräume von* V *und*

$$V_\tau = W_1 \oplus \ldots \oplus W_m\,,$$

dabei ist V_τ *die isotypische Komponente von* V *vom Typ* τ*.*

KAPITEL 4

Tensoren

§1. Tensorprodukt von Moduln

In diesem Abschnitt seien R ein kommutativer Ring und M, N Moduln über R.

Definition 17 : Ein R-Modul T zusammen mit einer bilinearen Abbildung $b : M \times N \longrightarrow T$ heißt *Tensorprodukt* von M und N, wenn gilt:
Zu jeder R-bilinearen Abbildung $h : M \times N \longrightarrow V$ in einen R-Modul V gibt es genau eine R-lineare Abbildung $g : T \longrightarrow V$ so, dass $g \circ b = h$.
Die Elemente von T heißen dann Tensoren.
Schreibweise: $M \otimes_R N := T$, $v \otimes w := b(v, w)$.

Beispiel 15 : Es seien $M := Hom_R(R^m, R)$, $N := Hom_R(R^n, R)$ und T der R-Modul aller bilinearen Abbildungen von $R^m \times R^n$ nach R. Dann ist T mit

$$b : M \times N \longrightarrow T\,,\ (f, g) \longmapsto [(v, w) \longmapsto f(v) \cdot g(w)]\,,$$

ein Tensorprodukt von M und N.

Satz 36 : *Sind T mit b und T' mit b' Tensorprodukte von M und N, dann gibt es einen Isomorphismus $f : T \longrightarrow T'$ von R-Moduln so, dass $f \circ b = b'$. („Das Tensorprodukt ist bis auf Isomorphie eindeutig bestimmt“.)*
Das Bild von b ist ein R-Erzeugendensystem von T. Sind M und N freie R-Moduln mit Basen $(v_i)_{i\in I}$ und $(w_j)_{j\in J}$, dann ist auch $M \otimes N$ frei und $(v_i \otimes w_j)_{i\in I, j\in J}$ ist eine Basis von $M \otimes N$.

Satz 37 : *Das Tensorprodukt von M und N existiert.*

Beispiel 16 : Es seien m und n teilerfremde ganze Zahlen. Dann ist $\{0\}$ das Tensorprodukt der $\mathbb{Z}$-Moduln $\mathbb{Z}_n$ und $\mathbb{Z}_m$.

Satz 38: *Es seien $g : S \longrightarrow R$ ein Ringhomomorphismus und U ein S-Modul. Dann ist das Tensorprodukt (von S-Moduln) $R \otimes_S U$ mit*

$$R \times R \otimes_S U \longrightarrow R \otimes_S U\,,\ (r, \sum_{u \in U} t_u \otimes u) \longmapsto \sum_{u \in U} r \cdot t_u \otimes u\,,$$

ein R-Modul.
Sprechweise: Den R-Modul $R \otimes_S U$ erhält man durch Grundringerweiterung *mittels g aus U.*
Wenn U ein freier S-Modul mit Basis $(u_i)_{i \in I}$ ist, dann ist $R \otimes_S U$ ein freier R-Modul mit Basis $(1 \otimes u_i)_{i \in I}$.

Beispiel 17: Es seien A eine Menge und U bzw. V der reelle bzw. komplexe Vektorraum aller Abbildungen von A nach $\mathbb{R}$ bzw. $\mathbb{C}$. Dann ist die lineare Abbildung

$$\mathbb{C} \otimes_{\mathbb{R}} U \longrightarrow V\,, z \otimes f \longmapsto [a \longmapsto z \cdot f(a)]$$

ein Isomorphismus von Vektorräumen.

§2. Tensorprodukt von Algebren

Satz 39: *Es seien R ein kommutativer Ring und A und B R-Algebren. Mit der Abbildung*

$$A \otimes B \times A \otimes B \longrightarrow A \otimes B\,, (\sum_{a,b} r_{ab} a \otimes b, \sum_{c,d} s_{cd} c \otimes d) \longmapsto \sum r_{ab} s_{cd} ac \otimes bd\,,$$

ist $A \otimes B$ eine kommutative R-Algebra.
Es seien

$$u_A : A \longrightarrow A \otimes B\,,\ a \longmapsto a \otimes 1$$

und

$$u_B : B \longrightarrow A \otimes B\,,\ b \longmapsto 1 \otimes b\ .$$

Zu jedem Paar von R-Algebrenhomomorphismen $f_A : A \longrightarrow S$ und $f_B : B \longrightarrow S$ gibt es genau einen R-Algebrenhomomorphismus $f : A \otimes B \longrightarrow S$ so, dass $f \circ u_A = f_A$ und $f \circ u_B = f_B$.

Beispiel 18: Es seien R ein kommutativer Ring, S eine R-Algebra und $R[x_1, \ldots, x_n]$ der Polynomring in $x_1, \ldots x_n$. Dann ist

$$S \otimes_R R[x_1, \ldots, x_n] \longrightarrow S[x_1, \ldots, x_n]\,,\ s \otimes \sum_i c_i x^i \longmapsto \sum_i (c_i \cdot s) x^i\,,$$

ein Isomorphismus von S-Algebren.

§3. Tensorprodukt von Darstellungen

Es seien K ein Körper, G eine Gruppe und V, W K-Vektorräume, auf denen G linear operiert.

Satz 40 : *Die Abbildung*

$$G \times V \otimes W \longrightarrow V \otimes W\,,$$
$$(s, \sum_{v,w} c_{vw} v \otimes w) \longmapsto s \cdot (\sum_{v,w} c_{vw} v \otimes w) := \sum_{v,w} c_{vw} s \cdot v \otimes s \cdot w\ ,$$

ist wohldefiniert und eine lineare Operation von G auf $V \otimes W$.
Diese Darstellung heißt Tensorprodukt der Darstellungen *von G in V und W.*

Satz 41 : *Die Abbildungen*

$$V \longrightarrow (V^*)^*\,,\ v \longmapsto [f \longmapsto f(v)]\,,$$
$$V^* \otimes W \longrightarrow Hom_K(V, W)\,,\ f \otimes w \longmapsto [v \longmapsto f(v)w]\,,$$

und

$$V^* \otimes W^* \longrightarrow Bil_K(V \times W, K)\,,\ f \otimes g \longmapsto [(v, w) \longmapsto f(v)g(w)]\,,$$

sind Isomorphismen von Darstellungen der Gruppe G.
(„Lineare Abbildungen und Bilinearformen sind Tensoren“).

Beispiel 19 : Die Abbildung id_V ist ein Fixpunkt für die Operation von $G := GL_K(V)$ in $Hom_K(V, V)$. Seien $(v_1, \ldots, v_n)$ eine K-Basis von V und $(v^1, \ldots, v^n)$ die dazu duale Basis von V^*. Der Isomorphismus von $V^* \otimes V$ nach $Hom_K(V, V)$ bildet $\sum_{i=1}^n v^i \otimes v_i$ auf id_V ab, also ist $\sum_{i=1}^n v^i \otimes v_i$ ein Fixpunkt für die Operation von G in $V^* \otimes V$.

Beispiel 20 : Sei V ein dreidimensionaler Vektorraum. Dann haben die Vektorräume $V \times V \times V$, $Hom_K(V, V) \cong V^* \otimes V$, $Bil_K(V \times V, K) \cong V^* \otimes V^*$ und $Bil_K(V^* \times V^*, K) \cong V \otimes V$ dieselbe Dimension 9, also sind sie paarweise isomorph. Als Darstellungen von $GL_K(V)$ sind sie aber paarweise nicht isomorph. (Insbesondere: „Tripel von Punkten im Raum sind keine Tensoren“).

Tensorprodukt von mehreren Moduln: Es seien $M_1, \ldots, M_n$ R-Moduln. Ein R-Modul T zusammen mit einer multilinearen Abbildung $b : M_1 \times \cdots \times M_n \longrightarrow T$ heißt *Tensorprodukt* von $M_1, \ldots, M_n$, wenn gilt:
Zu jeder R-multilinearen Abbildung $h : M_1 \times \cdots \times M_n \longrightarrow V$ in einen

R-Modul V gibt es genau eine R-lineare Abbildung $g : T \longrightarrow V$ so, dass $g \circ b = h$.
Schreibweise: $T = M_1 \otimes \cdots \otimes M_n$, $b(v_1, \ldots, v_n) := v_1 \otimes \cdots \otimes v_n$.
Analog kann auch das Tensorprodukt von mehreren Algebren und von mehreren Darstellungen definiert werden.

Definition 18 : Elemente von

$$V \otimes V \otimes \cdots \otimes V \otimes V^* \otimes \cdots \otimes V^*$$

(p-mal V und q-mal V^*) heißen *p-fach kontravariante und q-fach kovariante Tensoren.*

Beispiel 21 : Lineare Abbildungen von V nach V sind einfach kontravariante und einfach kovariante Tensoren; Bilinearformen auf V sind zweifach kovariante Tensoren.

Es seien $(v_1, \ldots, v_n)$ eine K-Basis von V, $(v^1, \ldots, v^n)$ die dazu duale Basis von V^*, $s \in GL_K(V)$, $A = (A^i_j)_{1 \le i,j \le n} \in K^{n \times n}$ die Matrix von s bezüglich $(v_1, \ldots, v_n)$ und $B := A^{-1}$. Dann ist

$$s \cdot v_i := s(v_i) = \sum_{k=1}^{n} A^k_i v_k =: A^k_i v_k$$

und

$$s \cdot v^j := v^j \circ s^{-1} = \sum_{\ell=1}^{n} B^j_\ell v^\ell =: B^j_\ell v^\ell \ .$$

Die Menge

$$\{v_{i_1} \otimes \cdots \otimes v_{i_p} \otimes v^{j_1} \otimes \cdots \otimes v^{j_q} \mid 1 \le i_1, \ldots, i_p, j_1, \ldots, j_q \le n\}$$

ist eine Basis von

$$V \otimes V \otimes \cdots \otimes V \otimes V^* \otimes \cdots \otimes V^* \, ,$$

jeder p-fach kontravariante und q-fach kovariante Tensor kann daher eindeutig als Linearkombination

$$u^{i_1 \ldots i_p}_{j_1 \ldots j_q} v_{i_1} \otimes \cdots \otimes v_{i_p} \otimes v^{j_1} \otimes \cdots \otimes v^{j_q} :=$$

$$= \sum_{i_1 \ldots i_p, j_1 \ldots j_q} u^{i_1 \ldots i_p}_{j_1 \ldots j_q} v_{i_1} \otimes \cdots \otimes v_{i_p} \otimes v^{j_1} \otimes \cdots \otimes v^{j_q}$$

geschrieben werden. Dann ist

$$s \cdot u^{i_1 \ldots i_p}_{j_1 \ldots j_q} v_{i_1} \otimes \cdots \otimes v_{i_p} \otimes v^{j_1} \otimes \cdots \otimes v^{j_q} =$$

$$= u^{i_1 \ldots i_p}_{j_1 \ldots j_q} s \cdot v_{i_1} \otimes \cdots \otimes s \cdot v_{i_p} \otimes s \cdot v^{j_1} \otimes \cdots \otimes s \cdot v^{j_q} =$$

$$= u^{i_1 \ldots i_p}_{j_1 \ldots j_q} A^{k_1}_{i_1} \ldots A^{k_p}_{i_p} B^{j_1}_{\ell_1} \ldots B^{j_q}_{\ell_q} v_{k_1} \otimes \cdots \otimes v_{k_p} \otimes v^{\ell_1} \cdots \otimes v^{\ell_q} \ .$$