Kapitel 1

Kategorien

Wir wollen hier einen kleinen Einblick in die Welt der Kategorien geben. Insbesondere wollen wir nicht primär Kategorien um ihrer selbst willen untersuchen, sondern eben vor allem betonen, dass sie sehr gut als Sprache geeignet sind, in der sich parallele Entwicklungen aus verschiedensten Ecken und Winkeln der Mathematik in einem gemeinsamen Rahmen beschreiben lassen.

Die zentralen Akteure in den Kategorien sind die Morphismen. Alle Argumente aus den „üblichen“ Theorien, die Elemente von Mengen benutzen, treten in den Hintergrund. Oder man versucht, Ersatz für sie zu bekommen.

1.1 Liebe auf den ersten Blick

Definition 1.1.1 Kategorie, Morphismen

a) Eine *Kategorie* $\mathcal{K}$ besteht aus der Vorgabe einer Klasse $\mathrm{Ob}\,(\mathcal{K})$ von sogenannten *Objekten*, der Vorgabe einer Menge $\mathrm{Mor}\,(A,B)$ für je zwei dieser Objekte – die sogenannte *Morphismenmenge* –, und der Vorgabe von „Verknüpfungsabbildungen“

$$\circ : \mathrm{Mor}(A,B) \times \mathrm{Mor}(B,C) \longrightarrow \mathrm{Mor}(A,C), \quad (\Phi,\Psi) \mapsto \Psi \circ \Phi,$$

sodass die folgenden Bedingungen erfüllt sind:

- Wenn A,B,C,D Objekte von $\mathcal{K}$ sind und $(A,B) \neq (C,D)$ gilt, dann sind die Mengen $\mathrm{Mor}(A,B)$ und $\mathrm{Mor}(C,D)$ disjunkt.
- Die Verknüpfung $\circ$ ist assoziativ, d.h. für je vier Objekte A,B,C,D und Morphismen $\alpha \in \mathrm{Mor}(A,B),\ \beta \in \mathrm{Mor}(B,C),\ \gamma \in \mathrm{Mor}(C,D)$ gilt

$$\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha.$$

- Für jedes Objekt A von $\mathcal{K}$ gibt es im Magma $\mathrm{Mor}(A,A) =: \mathrm{End}(A)$ ein Einselement 1_A mit der Eigenschaft, dass für alle Objekte B von $\mathcal{K}$ gilt:

$$\forall \Phi \in \mathrm{Mor}(A,B) : \Phi \circ 1_A = \Phi, \forall \Psi \in \mathrm{Mor}(B,A) : 1_A \circ \Psi = \Psi.$$

$\mathrm{End}(A)$ ist daher ein Monoid, seine Elemente heißen die *Endomorphismen* von A.

b) Es sei $\mathcal{K} := (\mathrm{Ob}(\mathcal{K}), \mathrm{Mor}(-,-), \circ)$ eine Kategorie. Dabei steht $\mathrm{Mor}(-,-)$ abkürzend für die Gesamtheit aller Morphismenmengen. Dann heißt ein Morphismus $\alpha \in \mathrm{Mor}(A,B)$ ein *Isomorphismus*, wenn es einen Morphismus $\beta \in \mathrm{Mor}(B,A)$ gibt, sodass

$$\alpha \circ \beta = 1_B \quad \text{und} \quad \beta \circ \alpha = 1_A.$$

Der Morphismus β ist dann durch α eindeutig bestimmt, denn die Verknüpfung ist ja assoziativ, und aus $\alpha \circ \gamma = 1_B$ folgt zum Beispiel

$$\beta = \beta \circ 1_B = \beta \circ (\alpha \circ \gamma) = (\beta \circ \alpha) \circ \gamma = 1_A \circ \gamma = \gamma.$$

Wenn es so einen Isomorphismus gibt, dann heißen A und B isomorph.

Ein Isomorphismus $\alpha \in \mathrm{End}(A)$ heißt ein *Automorphismus* von A. Die Menge aller Automorphismen von A ist eine Gruppe, $\mathrm{Aut}(A)$.

c) Anstelle von Morphismen spricht man auch oft von *Homomorphismen* oder auch nur von *Pfeilen*. Statt $\Phi \in \mathrm{Mor}(A,B)$ schreibt man oft auch $\Phi : A \longrightarrow B$ oder $A \xrightarrow{\Phi} B$. Hier muss man natürlich höllisch aufpassen, dass man nicht zu sehr versucht ist zu meinen, dass Morphismen immer Abbildungen sein müssten.

Nach so einer schönen Definition will man sich eigentlich gar nicht mit den Niederungen der Beispiele abgeben... trotzdem:

Beispiel 1.1.2 für Kategorien

a) Die Kategorie *Men* aller Mengen hat als Objekte die Mengen, als Morphismen zwischen zwei Mengen einfach alle Abbildungen und als Verknüpfung die Komposition der Abbildungen. In der Literatur wird diese Kategorie auch mit *Sets* oder *Ens* (aus dem Französischen) bezeichnet. 1_A ist natürlich die Identität auf A.

Insbesondere sieht man an diesem Beispiel, dass $\mathrm{Mor}(A,B)$ auch leer sein darf: es gibt keine Abbildung von $A := \{0\}$ in die leere Menge.

b) Genauso wohlbekannt ist die Kategorie der Gruppen, *Gruppen*, deren Objekte eben die Gruppen sind, und die Morphismen die Gruppenhomomorphismen. Hier sind die Morphismenmengen immer nichtleer.

c) Die Kategorien $\underline{Ringe}$ aller Ringe, $\underline{R-Mod}$ aller R-Moduln (für einen festen Ring R) und $\underline{G-Men}$ aller G-Mengen (für eine feste Gruppe G) sind ebenso auf naheliegende Weise definiert.

Bemerkung 1.1.3 Rechtfertigung

a) Diese Beispiele, die man ja wirklich behandeln will, zeigen, dass es zu restriktiv wäre, zu verlangen, dass die „Gesamtheit“ aller Objekte einer Kategorie eine Menge bildet. Daher der vorsichtigere Ausdruck „Klasse“. Diesen wollen wir hier nicht näher präzisieren. Er verbietet eben einige Konstruktionen mit der Gesamtheit aller Objekte.

Eine Kategorie, deren Objekte eine Menge bilden, heißt eine *kleine Kategorie*.

b) Ein sehr krasses Beispiel ist die Kategorie aller nulldimensionalen K-Vektorräume. Die Objekte sind alle einelementigen Mengen, die eben insgesamt keine Menge bilden. Sonst gäbe es nämlich keine injektive Abbildung der Potenzmenge der Menge aller nulldimensionalen K-Vektorräume in diese Menge, obwohl sie sich angeben ließe. $X \to (\{X\}, +, \cdot)$ mit der einzig möglichen Addition und skalaren Multiplikation wäre nämlich solch eine verbotene Injektion.

Die gute Seite dieser Medaille ist: Auf jeder einelementigen Menge gibt es genau eine K-Vektorraumstruktur, und je zwei solche Vektorräume sind zueinander isomorph. Wenn man die Kategorie aller nulldimensionalen Vektorräume ersetzt durch die Kategorie, die nur noch einen Raum $\{0\}$ als Objekt hat, mit den offensichtlichen Morphismen, so hat man die Kategorie aller nulldimensionalen Vektorräume durch eine kleine Kategorie ersetzt ohne dabei wesentliche Information zu verlieren.

Dieses Glück ist uns natürlich nicht immer hold, aber manchmals ist es so, dass sich eine Kategorie durch eine kleine Kategorie ersetzen lässt, siehe Proposition 2.8.

Denken Sie nur an die Lineare Algebra, wo man statt mit der Kategorie aller endlichdimensionalen Vektorräume auch sehr lange mit der Kategorie aller Standardvektorräume K^n auskommt.

c) Jedes Monoid $(M, *)$ kann als Endomorphismenmenge in einer geeigneten Kategorie realisiert werden. Dazu nehmen wir einfach die Kategorie mit nur einem Objekt A, mit $\mathrm{Mor}(A, A) := M$, und mit $*$ als Verknüpfungsabbildung.

Insbesondere kann man eine Gruppe definieren als eine Kategorie mit nur einem Objekt, in der jeder Morphismus ein Isomorphismus ist. (Streng genommen ist die Gruppe dann die Menge all dieser Morphismen – siehe Ende der Definition 1.1.)

Eine kleine Kategorie, in der jeder Morphismus ein Isomorphismus ist, heißt ein *Gruppoid*. Dieser Begriff ist vielleicht in der Topologie wichtiger als in der Algebra.

Beispiel 1.1.4 geordnete Mengen als Kategorien

a) Es sei $(M, \leq)$ eine geordnete Menge. Dann kann man daraus eine Kategorie $\mathcal{M}$ machen, deren Objekte gerade die Elemente von M sind, und deren Morphismenmengen so aussehen:

$$\forall a, b \in M : \mathrm{Mor}(a, b) := \begin{cases} \{\leq (a, b)\}, & \text{falls } a \leq b, \\ \emptyset, & \text{sonst.} \end{cases}$$

Dabei ist $\leq (a, b)$ ein Element. Man würde vielleicht lieber einfach $\leq$ für dieses Element schreiben, aber dann wären die Morphismenmengen nicht disjunkt. Die Verknüpfung von $\leq (b, c)$ mit $\leq (a, b)$ ist $\leq (a, c)$. Dass es diesen Morphismus gibt, wenn es die ersten beiden gibt, folgt aus der Transitivität der Ordnungsrelation.

Auf diese Art haben wir die erste konkretere Kategorie konstruiert, in der die Morphismen nicht von vorneherein Abbildungen zwischen Mengen sind.

NB: Man kann jetzt den Spieß umdrehen und eine geordnete Menge als eine kleine Kategorie definieren, in der die Morphismenmengen alle leer oder einelementig sind und aus $\mathrm{Mor}(A, B) \neq \emptyset \neq \mathrm{Mor}(B, A)$ folgt, dass $A = B$.

b) Die Kategorie $\underline{Ord}$ hat als Objekte alle geordneten Mengen. Ein Morphismus zwischen zwei geordneten Mengen ist eine ordnungserhaltende Abbildung ($x \leq y \Rightarrow f(x) \leq f(y)$).

Definition 1.1.5 Unterkategorie, volle Unterkategorie

a) Es sei $\mathcal{K}$ eine Kategorie. Eine *Unterkategorie* $\mathcal{U}$ von $\mathcal{K}$ ist eine Kategorie,

- deren Objekte auch Objekte von $\mathcal{K}$ sind,
- deren Morphismenmengen Teilmengen der zugehörigen Morphismenmengen in $\mathcal{K}$ sind,
- für die mit jedem Objekt $A \in \mathrm{Ob}(\mathcal{U})$ auch das Einselement 1_A aus der Kategorie $\mathcal{K}$ ein Morphismus in $\mathrm{Mor}_{\mathcal{U}}(A, A)$ ist,

und

- deren Verknüpfungsvorschrift durch Einschränkung der Verknüpfungsvorschrift aus $\mathcal{K}$ entsteht.

b) Eine Unterkategorie heißt *voll*, wenn für alle Objekte A, B von $\mathcal{U}$ gilt:

$$\mathrm{Mor}_{\mathcal{U}}(A, B) = \mathrm{Mor}_{\mathcal{K}}(A, B).$$

Dabei markieren wir der Deutlichkeit halber als Index am Namen der Morphismenmengen, in welcher Kategorie wir gerade sind.

Beispiel 1.1.6 von Unterkategorien

a) Die Kategorie der Körper ist definiert als volle Unterkategorie der Kategorie der Ringe mit Eins: es gibt nichts, was ein Homomorphismus zwischen zwei Körpern zu erfüllen hätte, was nicht jeder Ringhomomorphismus auch tut.

b) Wenn man etwas zu viel Zeit hat und sich auch mit Ringen ohne Eins beschäftigt, dann ist die Kategorie der Ringe mit Eins eine Unterkategorie hiervon. Diese Unterkategorie ist nicht voll, denn zum Beispiel ist die Abbildung $\mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z},\ x \mapsto (x, 0)$ ein Morphismus in der Kategorie aller Ringe, aber nicht in der Kategorie der Ringe mit 1.

c) Für jede geordnete Menge $(M, \leq)$ und jede Teilmenge $N \subseteq M$ gibt es die offensichtliche Unterkategorie $\mathcal{N}$ der oben konstruierten Kategorie $\mathcal{M}$.

Wichtige Qualitäten von Abbildungen sind die der Injektivität und die der Surjektivität. Da Morphismen in beliebigen Kategorien im Allgemeinen keine Abbildungen zwischen zwei Mengen sind, muss man sich Eigenschaften überlegen, die rein kategorientheoretisch etwas ähnliches bedeuten wie Injektivität und Surjektivität in $\underline{Men}$.

Definition 1.1.7 Monomorphismen und Epimorphismen

Es sei $\mathcal{K}$ eine Kategorie und $\Phi \in \mathrm{Mor}(A, B)$ ein Morphismus in $\mathcal{K}$. Dann heißt Φ ein *Monomorphismus*, falls gilt:

Für alle Objekte C in $\mathcal{K}$ und alle Morphismen $\Psi_1, \Psi_2 \in \mathrm{Mor}(C, A)$ folgt aus $\Phi \circ \Psi_1 = \Phi \circ \Psi_2$, dass $\Psi_1 = \Psi_2$.

Φ heißt ein *Epimorphismus*, falls gilt:

Für alle Objekte C in $\mathcal{K}$ und alle Morphismen $\Psi_1, \Psi_2 \in \mathrm{Mor}(B, C)$ folgt aus $\Psi_1 \circ \Phi = \Psi_2 \circ \Phi$, dass $\Psi_1 = \Psi_2$.

Beispiel 1.1.8 Legitimitätsnachweis

a) In der Kategorie $\underline{Men}$ sind Monomorphismen genau die injektiven Abbildungen. Epimorphismen sind genau die surjektiven Abbildungen.

b) In der Kategorie $\underline{Gruppen}$ aller Gruppen ist ein surjektiver Homomorphismus sicher ein Epimorphismus. Die Umkehrung gilt auch.

Wenn nämlich $f : G \longrightarrow H$ ein nicht surjektiver Homomorphismus von Gruppen ist, so sei $B := f(G)$. Wir zeigen, dass f kein Epimorphismus ist.

Dazu sei $M := H/B \cup \{*\}$, wobei $*$ ein zusätzliches Element ist, das noch nicht in H/B liegt.

Die Gruppe H operiert auf H/B durch Linkstranslation, also

$$h \bullet (\eta B) := (h\eta)B.$$

Diese Operation wird auf S fortgesetzt durch $h \bullet * := *$. Das definiert einen Homomorphismus ρ nach $\mathrm{Sym}(M)$.

In dieser symmetrischen Gruppe liegt auch die Transposition $t := \tau_{B,*}$.

Für $b \in B$ gilt dann $t\rho(b)t^{-1} = \rho(b)$, denn t vertauscht ja nur die beiden Fixpunkte B und $*$ der Operation von B.

Für $h \in H \setminus B$ allerdings ist

$$t\rho(h)t^{-1}(*) = t(hB) = hB \neq *.$$

Das zeigt, dass die beiden Homomorphismen ρ und $t\rho t^{-1}$ zwar auf B übereinstimmen, aber doch auf ganz H verschieden sind. Damit ist f kein Epimorphismus.

Ein Monomorphismus in der Kategorie aller Gruppen ist dasselbe wie ein injektiver Gruppenhomomorphismus. Wenn nämlich (und das ist die „schwierigere“ Richtung) $\Phi : H \longrightarrow G$ ein Monomorphismus ist, dann betrachten wir für $C := \mathrm{Kern}(\Phi)$:

$$\Psi_1 : C \longrightarrow H : \ \Psi_1(c) := c, \quad \Psi_2 : C \longrightarrow H, \Psi_2(c) := e_H.$$

Dann ist $\Phi \circ \Psi_1 = \Phi \circ \Psi_2$ die triviale Abbildung von C nach G. Aber aus Monomorphismus folgt dann, dass $\Psi_1 = \Psi_2$, also sind alle $c \in C$ gleich dem neutralen Element, und damit $C = \{e_H\}$. Also ist Φ injektiv.

c) In der Kategorie der Ringe ist die Einbettung $\mathbb{Z} \subseteq \mathbb{Q}$ ein Monomorphismus und auch ein Epimorphismus, wenn auch nicht surjektiv. Wieso?

d) In der Kategorie aller Gruppen gibt es den Begriff des Unterobjekts. Den gibt es nicht in jeder Kategorie. Zum Beispiel ist eine echte Teilmenge eines Standardvektorraums niemals ein Standardvektorraum, also gibt es in der Kategorie aller Standardvektorräume keine Unterobjekte. Gleichwohl wissen wir aus der Linearen Algebra, dass sich jeder Untervektorraum eines Standardvektorraums als Bild eines Vektorraumhomomorphismus schreiben lässt. Man ersetzt also hier Untervektorräume des K^n durch Monomorphismen von K^d nach K^n und bekommt jedenfalls so etwas ähnliches wie den Begriff eines Unterobjektes.

Beispiel 1.1.9 noch ein paar Kategorien

a) Es sei X eine Menge. Dann ist die Potenzmenge $\mathcal{P}(X)$ durch Inklusion geordnet, und wir erhalten eine Kategorie wie in Beispiel 1.1.4. Jetzt dürfen wir uns den Morphismus $\leq (A, B)$ als die Inklusion von A nach B vorstellen, wenn $A \subseteq B$. Ansonsten gibt es ja keine Morphismen.

b) Die Struktur eines *topologischen Raumes* auf X wird vorgegeben durch Auszeichnung einer vollen Unterkategorie $\mathcal{T}(X)$ von $\mathcal{P}(X)$, die $\emptyset$ und X als Objekte

enthält und deren Objektemenge (als Unterkategorie von $\mathcal{P}(X)$ ist der topologische Raum natürlich eine kleine Kategorie) unter Bildung endlicher Durchschnitte und beliebiger Vereinigungen stabil ist.

$\mathcal{T}(X)$ heißt das System der offenen Mengen (der Topologie von X). Man kann die meisten Räume mit sehr vielen verschiedenen Topologien versehen.

So ist etwa die volle Unterkategorie von $\mathcal{P}((0,1))$, die aus allen offenen Teilmengen des offenen Einheitsintervalls $(0,1)$ besteht, eine Topologie auf $(0,1)$, die Standardtopologie aus der Analysis. Aber auch die Unterkategorie, die nur aus $\emptyset$ und $(0,1)$ besteht, oder die, die aus $\emptyset$ und den Komplementen endlicher Mengen besteht sind Topologien auf $(0,1)$.

Bitte fragen Sie sich hier, wieso ich das so kompliziert aufschreibe. Eigentlich interessiert man sich gar nicht für die Morphismen dieser Kategorie, beziehungsweise sind sie so naheliegend, dass man sich das Leben gerne erleichtern würde. Der Grund ist, dass man auf diese Art schon ein wenig sieht, wie sich der Begriff einer Topologie verallgemeinern lässt. Eine wichtige Verallgemeinerung dieses Begriffs findet sich im Begriff des *Situs*. Hier zeichnet man nicht von vorneherein die Teilmengen von X aus und benutzt Inklusionen, sondern man lässt als Objekte der Kategorie eine größere (von Fall zu Fall zu umreißende) Klasse von Abbildungen $Y \longrightarrow X$ zu, von der man eben irgendwie eine analoge Forderung wie „Abgeschlossenheit unter endlichen Durchschnitten und beliebigen Vereinigungen“ kategorientheoretisch formulieren muss. Diese Sichtweise von Topologien ist aus der modernen algebraischen (oder arithmetischen) Geometrie nicht wegzudenken.

c) Um nicht auf halbem Wege stehen zu bleiben definieren wir noch, was eine stetige Abbildung zwischen zwei topologischen Räumen X und Y ist. Es ist eine Abbildung $f : X \longrightarrow Y$, für die das Urbild jeder offenen Teilmenge von Y in X offen ist.

Die topologischen Räume bilden – mit stetigen Abbildungen als Morphismen und der üblichen Komposition von Abbildungen – eine Kategorie $\underline{Top}$.

Definition/Bemerkung 1.1.10 Anfang und Ende

a) Ein *initiales Objekt* A in einer Kategorie $\mathcal{K}$ ist durch die Eigenschaft definiert, dass für jedes Objekt B von $\mathcal{K}$ genau ein Morphismus von A nach B existiert.

Ein *terminales Objekt* A in einer Kategorie $\mathcal{K}$ ist durch die Eigenschaft definiert, dass für jedes Objekt B von $\mathcal{K}$ genau ein Morphismus von B nach A existiert.

b) Wenn $A, \tilde{A}$ zwei initiale Objekt sind, dann seien $\Phi \in \mathrm{Mor}(A, \tilde{A})$ und $\Psi \in \mathrm{Mor}(\tilde{A}, A)$ die jeweils eindeutig bestimmten Morphismen. Wegen

$$\Phi \circ \Psi \in \mathrm{Mor}(\tilde{A}, \tilde{A}) = \{1_{\tilde{A}}\}$$

und

$$\Psi \circ \Phi \in \mathrm{Mor}(A, A) = \{1_A\}$$

sind Φ und Ψ zueinander invers, also ist ein initiales Objekt – wenn es denn existiert – bis auf Isomorphismus eindeutig bestimmt.

c) Es folgt eine kleine Tabelle.

Kat.	initiales Ob.	terminales Ob.
Men	$\emptyset$	$\{\emptyset\}$
Gruppen	$(\{1\}, \cdot)$	$(\{1\}, \cdot)$
Ringe	$\mathbb{Z}$	$(\{0\}, +, \cdot)$
Körper	–	–

Die letzte Zeile zeigt, dass es weder das eine noch das andere geben muss.

1.2 Funktoren

Bei den Beispielen für Unterkategorien ist nicht das folgende aufgetaucht: die Kategorie der Ringe (ab jetzt wieder immer mit Eins) als Unterkategorie der Kategorie der Gruppen. Das liegt einfach daran, dass das keine Unterkategorie ist, denn es gibt ja in aller Regel wenn überhaupt dann mehr als eine Möglichkeit, aus einer abelschen Gruppe durch Definition der Multiplikation einen Ring zu machen. Trotzdem kann man jedem Ring seine additive Gruppe zuordnen und erhält dabei aus jedem Ring eine abelsche Gruppe. Ein Ringhomomorphismus lässt sich auch immer auffassen als Homomorphismus zwischen den additiven Gruppen. Dabei sind wir von einer Kategorie in eine andere gekommen. Dieser Sachverhalt wird verallgemeinert durch das Konzept des Funktors.

Definition 1.2.1 Funktor

Es seien $\mathcal{K}, \mathcal{L}$ zwei Kategorien. Ein *kovarianter Funktor* $\mathcal{F}$ von $\mathcal{K}$ nach $\mathcal{L}$ besteht aus der Vorgabe einer Zuordnung, die jedem Objekt A aus $\mathcal{K}$ ein Objekt $\mathcal{F}(A)$ in $\mathcal{L}$ zuordnet und der Vorgabe einer Abbildung

$$\mathcal{F}_{A,B} : \mathrm{Mor}_{\mathcal{K}}(A, B) \longrightarrow \mathrm{Mor}_{\mathcal{L}}(\mathcal{F}(A), \mathcal{F}(B))$$

für je zwei Objekte A, B in $\mathcal{K}$, sodass die folgenden Bedingungen erfüllt sind:

- $\forall A \in \mathrm{Ob}(\mathcal{K}) : \mathcal{F}_{A,A}(1_A) = 1_{\mathcal{F}(A)}$.
- $\forall A, B, C \in \mathrm{Ob}(\mathcal{K}), \forall \Phi \in \mathrm{Mor}(A, B), \Psi \in \mathrm{Mor}(B, C) : \mathcal{F}_{A,C}(\Psi \circ \Phi) = \mathcal{F}_{B,C}(\Psi) \circ \mathcal{F}_{A,B}(\Phi)$.

Analog gibt es einen *kontravarianten* Funktor von $\mathcal{K}$ nach $\mathcal{L}$. Dieser ordnet auch Objekten von $\mathcal{K}$ Objekte von $\mathcal{L}$ zu, aber dreht bei den Morphismen die Richtung um:

$$\mathcal{F}_{A,B}(\Phi) \in \mathrm{Mor}_{\mathcal{L}}(\mathcal{F}(B), \mathcal{F}(A)).$$

Man muss dann auch die Reihenfolge bei der zweiten Bedingung umdrehen.

Aus Bequemlichkeit lässt man die Indizes $_{A,B}$ im Allgemeinen weg.

Beispiel 1.2.2 Vergissfunktoren, Dualraum, Hom-Funktoren, Einheitengruppe, freie Moduln

a) Es seien R ein Ring und M ein R-Modul. Dann ist M immer auch eine Menge, und indem man einem Modul ihn selbst zuordnet und die Menge aller Modulhomomorphismen als Teilmenge der Menge aller Abbildungen zwischen zwei Moduln auffasst, hat man einen kovarianten Funktor von $\underline{R-Mod}$ nach $\underline{Men}$ definiert.

Solche und ähnliche Funktoren, die durch „Vergessen“ von Strukturen zustande kommen, nennt man Vergissfunktoren. Auch der eingangs beschriebene Funktor von $\underline{Ringe}$ nach $\underline{Gruppen}$ ist solch ein Vergissfunktor.

b) Nun betrachten wir die Kategorie $\underline{K-Mod}$ aller K-Vektorräume. Zu jedem K-Vektorraum V gibt es den Dualraum $V^* := \mathrm{Mor}_{\underline{K-Mod}}(V, K)$, und zu jedem K-Vektorraumhomomorphismus $\Phi : V \longrightarrow W$ gibt es den dualen Homomorphismus

$$\Phi^* : W^* \longrightarrow V^*,\ \lambda \mapsto \lambda \circ \Phi.$$

Auf diese Weise hat man einen kontravarianten Funktor * von der Kategorie der K-Vektorräume in sich selbst definiert.

c) Das Beispiel b) lässt sich leicht modifiziert verallgemeinern. Ist $\mathcal{K}$ eine beliebige Kategorie und A ein Objekt von $\mathcal{K}$, so bekommt man zwei Funktoren von $\mathcal{K}$ nach $\underline{Men}$, nämlich einerseits

$$\mathrm{Mor}(-, A) : \left\{ \begin{array}{rl} X & \rightsquigarrow \mathrm{Mor}(X, A), \\ \mathrm{Mor}(X, Y) \ni \Phi & \rightsquigarrow [\mathrm{Mor}(Y, A) \ni \Psi \mapsto \Psi \circ \Phi \in \mathrm{Mor}(X, A)], \end{array} \right.$$

das ist kontravariant, und andererseits

$$\mathrm{Mor}(A, -) : \left\{ \begin{array}{rl} X & \rightsquigarrow \mathrm{Mor}(A, X), \\ \mathrm{Mor}(X, Y) \ni \Phi & \rightsquigarrow [\mathrm{Mor}(A, X) \ni \Psi \mapsto \Phi \circ \Psi \in \mathrm{Mor}(A, Y)], \end{array} \right.$$

das ist kovariant.

Solche Funktoren heißen *Hom-Funktoren*. Man sollte dabei daran erinnern, dass Morphismen oft auch Homomorphismen genannt und mit $\mathrm{Hom}(A, B)$ notiert werden.

d) Einen wunderschönen Funktor von *Ringe* nach *Gruppen* erhält man, indem man einem Ring seine Einheitengruppe zuordnet. Dabei ordnen wir einem Homomorphismus $\Phi : R \longrightarrow S$ zwischen Ringen seine Einschränkung auf $R^\times$ zu, die bekanntlich Werte in $S^\times$ annimmt.

Das ist wieder nicht viel anders als der (kovariante) Hom-Funktor

$$R \rightsquigarrow \mathrm{Mor}(\mathbb{Z}[X, X^{-1}], R),$$

denn ein Ringhomomorphismus Φ von $\mathbb{Z}[X, X^{-1}]$ nach R ist eindeutig durch $\Phi(X) \in R^\times$ beschrieben, und dieses kann beliebig vorgeschrieben werden.

e) Als letztes Beispiel betrachten wir für einen festen Ring $R \neq \{0\}$ die Zuordnung, die einer Menge X den freien R-Modul mit Basis X zuordnet. Etwas präziser (wieso sollte X überhaupt in so einem Modul liegen?) nehmen wir den Funktor

$$\mathcal{F} : \begin{cases} \underline{Men} & \rightsquigarrow \underline{R-Mod}, \\ X & \rightsquigarrow \mathrm{Abb}(X, R)_0, \\ \mathrm{Abb}(X, Y) \ni \Phi & \rightsquigarrow [f \mapsto [y \mapsto \sum_{x:\Phi(x)=y} f(x)]]. \end{cases}$$

Dabei ist $\mathrm{Abb}\,(X, R)_0$ der R-Modul aller Abbildungen von X nach R mit endlichem Träger, was auch dafür sorgt, dass die Summe in der Definition endlich ist. Die Funktionen δ_{x_0}, die nur an einer Stelle $x_0 \in X$ den Wert 1 annehmen und sonst den Wert 0, bilden eine Basis von $\mathrm{Abb}(X, R)_0$, die mit X identifiziert wird. Der Homomorphismus $\mathcal{F}(\Phi)$ zu $\Phi : X \longrightarrow Y$ ist der, der durch lineare Fortsetzung der durch Φ induzierten Abbildung zwischen den Basen gehört.

Wir haben hier eine nette Eigenschaft, die zwei Funktoren miteinander verbindet. Wir kennen ja auch den Vergissfunktor $\mathcal{V}$, der einem R-Modul einfach die zugrunde liegende Menge zuordnet. Wir finden nun die folgende Formulierung des Satzes von der linearen Fortsetzung:

$$\mathrm{Mor}_{\underline{Men}}(X, \mathcal{V}(M)) \simeq \mathrm{Mor}_{\underline{R-Mod}}(\mathcal{F}(X), M).$$

Dabei ist X eine beliebige Menge, und M ein beliebiger R-Modul.

Auf diesen Zusammenhang zwischen zwei Funktoren werden wir noch eingehen.

Bemerkung 1.2.3 Wieso Funktoren?

Wie die Beispiele vielleicht schon gezeigt haben lässt es sich gar nicht vermeiden, mit Funktoren und Kategorien in Berührung zu kommen, auch wenn man natürlich alles ad hoc machen kann, ohne die abstrakte Sprache der Kategorien einzuführen.

Eine wesentliche Eigenschaft von Funktoren ist es, dass sie Isomorphismen in Isomorphismen überführen. Dies rechnet man ohne Weiteres mit den Eigenschaften aus Definition 1.2.1 nach. Es führt dazu, dass man vielleicht zeigen kann,

dass zwei Objekte einer Kategorie $\mathcal{K}$ nicht isomorph sind, indem man ihre Bilder unter einem geeigneten Funktor als nicht isomorph ausweist. Dies ist eine der Lieblingsanwendungen der Kategorientheorie in der Topologie. Die Frage, wann zwei topologische Räume isomorph sind (man sagt dann: homöomorph), ist sehr schwer zu beantworten, denn Topologie ist intrinsisch schwabbelig. Es gibt allerdings Funktoren in etwas rigidere Kategorien (Fundamentalgruppe, Kohomologiering), in denen Isomorphie leichter zu widerlegen ist.

Natürlich ist es nicht hinreichend, die Isomorphie zweier Objekte durch Untersuchung ihrer Bilder unter einem Funktor zu testen. Ein prominentes Beispiel, wo man so etwas untersucht und auch sieht, wie schwer diese Frage werden kann, ist die Poincaré-Vermutung. Hier wurde gut 100 Jahre vergeblich versucht zu zeigen, dass die dreidimensionale Sphäre unter allen dreidimensionalen Mannigfaltigkeiten durch den Wert eines bestimmten Funktors ausgezeichnet ist. Mittlerweile ist das auf einem weiteren langen Umweg gelungen.

Aufgabe: Finden Sie die triviale Kategorie, zu der es von jeder anderen Kategorie aus genau einen Funktor gibt.

Definition 1.2.4 natürliche Transformationen

Nun seien $\mathcal{K}$ und $\mathcal{L}$ zwei Kategorien und $\mathcal{F}, \mathcal{G}$ zwei kovariante Funktoren von $\mathcal{K}$ nach $\mathcal{L}$. Eine *natürliche Transformation* η von $\mathcal{F}$ nach $\mathcal{G}$ besteht aus der Vorgabe von Morphismen $\eta_A \in \mathrm{Mor}_{\mathcal{L}}(\mathcal{F}(A), \mathcal{G}(A))$, sodass das folgende Diagramm für beliebige Objekte $A, B \in \mathrm{Ob}(\mathcal{K})$ und Morphismen $f \in \mathrm{Mor}_{\mathcal{K}}(A, B)$ kommutativ ist:

$$\begin{array}{ccc} A & \mathcal{F}(A) & \xrightarrow{\eta_A} & \mathcal{G}(A) \\ f \downarrow & \mathcal{F}(f) \downarrow & & \downarrow \mathcal{G}(f) \\ B & \mathcal{F}(B) & \xrightarrow{\eta_B} & \mathcal{G}(B) \end{array}$$

Mit anderen Worten: $\eta_B \circ \mathcal{F}(f) = \mathcal{G}(f) \circ \eta_A$.

Wenn noch dazu jedes η_A ein Isomorphismus ist, dann ist η ein *natürlicher Isomorphismus* von Funktoren.

Beispiel 1.2.5 Bidual, und noch ein anderes Beispiel

a) In Beispiel 1.2.2b) hatten wir den kontravarianten Funktor * (Dualraum) von der Kategorie der K-Vektorräume in sich selbst. Diesen können wir zweimal ausführen und erhalten den kovarianten Funktor $V \rightsquigarrow V^{**}$.

Nun ist aus der Linearen Algebra bekannt, dass es einen natürlichen Homomorphismus von V nach V^{**} gibt, nämlich denjenigen, der $v \in V$ auf die Abbildung $\eta_V(v) = [V^* \ni \lambda \mapsto \lambda(v) \in K]$ schickt. Diese Abbildungen η_V definieren eine natürliche Transformation vom identischen Funktor zum Funktor **. Wenn man sich auf die Kategorie der endlichdimensionalen Vektorräume einschränkt, so bekommt man sogar einen natürlichen Isomorphismus von Funktoren.

b) Auf der Kategorie der Gruppen betrachten wir den Funktor $\mathcal{A}$, der einer Gruppe G den maximalen abelschen Quotienten $\mathcal{A}(G) := G/G'$ zuordnet. Dabei ist G' die Kommutatoruntergruppe, also die Untergruppe, die von den Elementen $ghg^{-1}h^{-1}$ (den sogenannten Kommutatoren) erzeugt wird. Jeder Gruppenhomomorphismus $\Phi : G \longrightarrow H$ bildet G' nach H' ab, wir erhalten also eine induzierte Abbildung $\mathcal{A}(\Phi) : G/G' \longrightarrow H/H'$.

Wenn nun $\pi_G : G \longrightarrow G/G'$ die natürliche Projektion ist, dann ist π eine natürliche Transformation von dem identischen Funktor zum Funktor $\mathcal{A}$. Das folgt aus dem Homomorphiesatz für Gruppen, oder besser gesagt: es liegt der Konstruktion von $\mathcal{A}(\Phi)$ zu Grunde.

Definition 1.2.6 Treue, Volltreue, Äquivalenz

Es sei $\mathcal{F}$ ein Funktor von der Kategorie $\mathcal{K}$ zur Kategorie $\mathcal{L}$.

a) Der Funktor $\mathcal{F}$ heißt *treu*, wenn für jedes Paar A, B von Objekten von $\mathcal{K}$ die Zuordnung

$$\mathcal{F}_{\mathcal{A},\mathcal{B}} : \mathrm{Mor}(\mathcal{A}, \mathcal{B}) \longrightarrow \mathrm{Mor}(\mathcal{F}(\mathcal{A}), \mathcal{F}(\mathcal{B}))$$

injektiv ist. Wenn diese Abbildung stets surjektiv ist, heißt $\mathcal{F}$ *voll*. Wenn sie eine Bijektion ist, heißt $\mathcal{F}$ *volltreu*.

b) Der Funktor $\mathcal{F}$ definiert eine *Äquivalenz* zwischen $\mathcal{K}$ und $\mathcal{L}$, wenn es einen Funktor $\mathcal{G}$ von $\mathcal{L}$ nach $\mathcal{K}$ gibt, sodass $\mathcal{FG}$ natürlich isomorph zur Identität auf $\mathcal{L}$ ist und $\mathcal{GF}$ natürlich isomorph zur Identität auf $\mathcal{K}$.

Vorsicht: $\mathcal{G}$ ist im Allgemeinen nicht eindeutig durch $\mathcal{F}$ festgelegt.

Beispiel 1.2.7 Nulldimensionales

Die Kategorie der nulldimensionalen K-Vektorräume ist äquivalent zur Kategorie des Nullraums. Aber die beiden Kategorien sind nicht isomorph im naheliegenden Sinne, denn die eine ist klein und die andere nicht.

Proposition 1.2.8 Kriterium für Äquivalenz

Es sei $\mathcal{F}$ ein Funktor zwischen den Kategorien $\mathcal{K}$ und $\mathcal{L}$. Dann sind gleichbedeutend:

i) $\mathcal{F}$ definiert eine Äquivalenz von Kategorien.

ii) $\mathcal{F}$ ist volltreu und für jedes Objekt C in $\mathcal{L}$ gibt es ein Objekt A in $\mathcal{K}$, sodass $\mathcal{F}(A)$ zu C isomorph ist.

Beweis.

i) $\Rightarrow$ ii) Wir wählen einen Funktor $\mathcal{G}$ wie in der Definition 1.2.6. Da $\mathcal{GF}$ natürlich isomorph zur Identität auf $\mathcal{K}$ ist, wählen wir einen natürlichen Isomorphismus

η von der Identität zu $\mathcal{GF}$, haben also für alle Morphismen $f : A \to B$ das folgende kommutative Diagramm:

$$\begin{array}{ccc} A & & A & \xrightarrow{\eta_A} & \mathcal{GF}(A) \\ f\downarrow & & f\downarrow & & \downarrow \mathcal{GF}(f) \\ B & & B & \xrightarrow{\eta_B} & \mathcal{GF}(B) \end{array}$$

Da die Morphismen η_A und η_B Isomorphismen sind, liefert dies eine Bijektion

$$\mathrm{Mor}(A,B) \ni f \mapsto \eta_B \circ f \circ \eta_A^{-1} \in \mathrm{Mor}(\mathcal{GF}(A), \mathcal{GF}(B)).$$

Diese Bijektion ist aber gerade das, was der Funktor $\mathcal{GF}$ mit den Morphismen macht, und das faktorisiert als

$$\mathrm{Mor}(A,B) \ni f \mapsto \mathcal{F}(f) \in \mathrm{Mor}(\mathcal{F}(A), \mathcal{F}(B)) \ni g \mapsto \mathcal{G}(g) \in \mathrm{Mor}(\mathcal{GF}(A), \mathcal{GF}(B)).$$

Damit ist $f \mapsto \mathcal{F}(f)$ injektiv und (wegen der analogen Überlegung für $\mathcal{FG}$ statt $\mathcal{GF}$) ist es auch surjektiv, zumindest für alle Objekte im Bildbereich von $\mathcal{G}$. Da aber jedes Objekt A zum Objekt $\mathcal{GF}(A)$ isomorph ist (via η_A), ist die Abbildung für je zwei Objekte surjektiv.

Da auch $\mathcal{FG}$ zur Identität auf $\mathcal{L}$ isomorph ist, ist ein Objekt C isomorph zu $\mathcal{FG}(C)$, also zu $\mathcal{F}(\mathcal{G}(C))$.

ii) $\Rightarrow$ i) Nun nehmen wir an, $\mathcal{F}$ sei volltreu und zu jedem Objekt C von $\mathcal{L}$ gebe es ein Objekt A von $\mathcal{K}$, sodass $\mathcal{F}(A)$ zu C isomorph ist. Wir wählen so ein A aus und nennen es $\mathcal{G}(C)$. Weiter wählen wir einen Isomorphismus $\xi_C \in \mathrm{Mor}_{\mathcal{L}}(C, \mathcal{F}(\mathcal{G}(C)))$.

Wenn D ein weiteres Objekt in $\mathcal{L}$ ist und Φ ein Morphismus von C nach D, dann betrachten wir das folgende Diagramm:

$$\begin{array}{ccccc} C & \xrightarrow{\xi_C} & \mathcal{FG}(C) & & A = \mathcal{G}(C) \\ \Phi\downarrow & & \downarrow \xi_D \circ \Phi \circ \xi_C^{-1} & & \downarrow \mathcal{G}(\Phi) \\ D & \xrightarrow{\xi_D} & \mathcal{FG}(D) & & B = \mathcal{G}(D) \end{array}$$

Hierbei ist $\mathcal{G}(\Phi)$ der eindeutig bestimmte ($\mathcal{F}$ ist ja volltreu!) Morphismus von A nach B mit $\mathcal{F}(\mathcal{G}(\Phi)) = \xi_D \circ \Phi \circ \xi_C^{-1}$.

Damit ist ein Funktor $\mathcal{G}$ von $\mathcal{L}$ nach $\mathcal{K}$ definiert (nachrechnen!). $\mathcal{G}$ ist so konstruiert, dass die Identität auf $\mathcal{L}$ zum Funktor $\mathcal{FG}$ natürlich isomorph ist. Um dies zu verifizieren verwende man die Morphismen ξ_C.

Nun ist noch zu zeigen, dass auch $\mathcal{GF}$ zur Identität auf $\mathcal{K}$ natürlich isomorph ist.

Es sei A ein Objekt von $\mathcal{K}$. Dann haben wir aus der Konstruktion von $\mathcal{G}$ den Morphismus

$$\xi_{\mathcal{F}(A)} : \mathcal{F}(A) \longrightarrow \mathcal{FGF}(A).$$

Da $\mathcal{F}$ volltreu ist, gibt es genau einen Morphismus

$$\eta_A \in \mathrm{Mor}(A, \mathcal{GF}(A)),$$

der unter $\mathcal{F}(A)$ auf $\xi_{\mathcal{F}(A)}$ abgebildet wird. Es ist klar (hier braucht man noch einmal die Volltreue von $\mathcal{F}$), dass η_A ein Isomorphismus ist.

Wenn nun $\Phi : A \longrightarrow B$ ein Morphismus in $\mathcal{K}$ ist, dann gilt nach Konstruktion von $\mathcal{G}$ für den Morphismus $\mathcal{F}(\Phi)$ die folgende Regel:

$$\mathcal{FGF}(\Phi) \circ \xi_{\mathcal{F}(A)} = \xi_{\mathcal{F}(B)} \circ \mathcal{F}(\Phi).$$

Da hier $\xi_{\mathcal{F}(A)} = \mathcal{F}(\eta_A)$ gilt und $\mathcal{F}$ volltreu ist, führt dies auf

$$\mathcal{GF}(\Phi) \circ \eta_A = \eta_B \circ \Phi.$$

Damit ist η ein natürlicher Isomorphismus von der Identität zu $\mathcal{GF}$. ◯

Anwendung 1.2.9 aus groß mach klein

Es sei $\mathcal{L}$ eine volle Unterkategorie der Kategorie $\mathcal{K}$, die für jedes Objekt A aus $\mathcal{K}$ mindestens eines enthält, das zu A isomorph ist. Dann ist die Inklusion von $\mathcal{L}$ nach $\mathcal{K}$ eine natürliche Äquivalenz von Kategorien.

So ist zum Beispiel die Kategorie aller endlichdimensionalen Vektorräume natürlich äquivalent zur Kategorie der endlich dimensionalen Standardvektorräume: man muss sich nicht mit so vielen Objekten herumschlagen.

Insbesondere kann oft – zum Beispiel im eben angeführten Beispiel – eine Kategorie durch eine äquivalente kleine Unterkategorie ersetzt werden, nämlich genau dann, wenn es eine Menge von Objekten gibt, die zu jedem Objekt ein isomorphes enthält.

Ein besonderes Augenmerk gilt bei Funktoren in die Kategorie *Men* den Hom-Funktoren aus Beispiel 1.2.2. Wir behandeln zunächst das weitberühmte

Hilfssatz 1.2.10 Yoneda-Lemma[1]

Es sei $\mathcal{F}$ ein kovarianter Funktor von der Kategorie $\mathcal{K}$ in die Kategorie Men. Weiter sei A ein Objekt von $\mathcal{K}$ und $h \in \mathcal{F}(A)$. Für ein Objekt B von $\mathcal{K}$ sei η_B die Abbildung

$$\eta_B : \mathrm{Mor}(A, B) \longrightarrow \mathcal{F}(B), \quad \Phi \mapsto (\mathcal{F}(\Phi))(h).$$

Dann ist $B \rightsquigarrow \eta_B$ eine natürliche Transformation η vom Hom-Funktor $\mathrm{Mor}(A, -)$ zum Funktor $\mathcal{F}$.

[1] Nobuo Yoneda, 1930-1996

Die Zuordnung $h \mapsto \eta$ ist eine Bijektion der Menge $\mathcal{F}(A)$ mit der Menge aller natürlichen Transformationen von $\mathrm{Mor}(A, -)$ *zum Funktor $\mathcal{F}$. Die Umkehrung wird durch*

$$\eta \mapsto \eta_A(1_A)$$

gegeben.

Beweis. Es seien B, C Objekte in $\mathcal{K}$ und Φ ein Morphismus von B nach C. Dann haben wir für $\Psi \in \mathrm{Mor}(A, B)$:

$$(\mathcal{F}(\Phi) \circ \eta_B)(\Psi) = \mathcal{F}(\Phi)(\mathcal{F}(\Psi)(h)) = \mathcal{F}(\Phi \circ \Psi)(h) = \eta_C(\Phi \circ \Psi).$$

Das zeigt die Gleichung

$$\mathcal{F}(\Phi) \circ \eta_B = \eta_C \circ \mathrm{Mor}(A, -)(\Phi),$$

und damit ist η tatsächlich eine natürliche Transformation der gewünschten Art.

Die Gleichung

$$h = \mathrm{Id}_{\mathcal{F}(A)}(h) = (\mathcal{F}(1_A))(h) = \eta_A(1_A)$$

zeigt, dass h sich aus η zurückgewinnen lässt, dass also die Zuordnung $h \rightsquigarrow \eta$ injektiv ist. Außerdem legt dies nahe, wie der Übergang von h zu η zu invertieren ist:

Wenn η eine beliebige Transformation vom Hom-Funktor zu $\mathcal{F}$ ist, so setze $h := \eta_A(1_A)$. Dann ist nachzuweisen, dass η die durch h definierte natürliche Transformation ist. Also sei $\Phi \in \mathrm{Mor}(A, B)$.

Wir betrachten das zur natürlichen Transformation gehörende kommutative Diagramm

$$\begin{array}{rcl} \mathrm{Mor}(A, A) & \xrightarrow{\eta_A} & \mathcal{F}(A) \\ M(\Phi) \downarrow & & \downarrow \mathcal{F}(\Phi) \\ \mathrm{Mor}(A, B) & \xrightarrow{\eta_B} & \mathcal{F}(B) \end{array}$$

Dabei steht $M(\Phi)$ für den Morphismus, der aus Φ unter dem Hom-Funktor wird, also die Komposition mit Φ.

Wir werten das Diagramm aus für die Identität $1_A \in \mathrm{Mor}(A, A)$ und erhalten

$$\eta_B(\Phi) = \eta_B(\Phi \circ 1_A) = (\eta_B \circ M_\Phi)(1_A) = \mathcal{F}(\Phi)(\eta_A(1_A)) = \mathcal{F}(\Phi)(h).$$

Also ist η die durch h definierte natürliche Transformation. ◯

Nun sind wir schon wieder sehr nah an einem Begriff aus der Algebra I. Um dies zu präzisieren starten wir einen neuen Abschnitt.

1.3 Darstellbare Funktoren

Definition/Bemerkung 1.3.1 Universelle Abbildungseigenschaft

a) Ein kovarianter Funktor $\mathcal{F}$ von $\mathcal{K}$ nach $\underline{Men}$ heißt *darstellbar*, wenn es ein Objekt A von $\mathcal{K}$ gibt, sodass $\mathcal{F}$ zum Hom-Funktor $\mathrm{Mor}(A,-)$ natürlich isomorph ist.

Nach dem Lemma von Yoneda heißt das, dass es ein Element $h \in \mathcal{F}(A)$ gibt, sodass für alle Objekte B von $\mathcal{K}$ die Abbildung

$$\mathrm{Mor}(A,B) \ni \varphi \mapsto (\mathcal{F}\varphi)(h) \in \mathcal{F}(B)$$

eine Bijektion ist: für alle $k \in \mathcal{F}(B)$ gibt es genau ein $\varphi \in \mathrm{Mor}(A,B)$ mit $k = (\mathcal{F}\varphi)(h)$.

Man sagt dann auch, dass das Paar (A,h) die *universelle Abbildungseigenschaft* für $\mathcal{F}$ hat, und dass (A,h) ein *universelles Element* für $\mathcal{F}$ ist.

Die Sprechweise der Abbildungseigenschaft kommt von Situationen her, wo $\mathcal{F}$ Mengen von Abbildungen als Werte annimmt (siehe unten).

b) Wenn (B,k) ein weiteres Paar mit der universellen Abbildungseigenschaft für $\mathcal{F}$ ist, dann gibt es genau einen Morphismus $\varphi \in \mathrm{Mor}(A,B)$ und genau einen Morphismus $\psi \in \mathrm{Mor}(B,A)$, sodass

$$k = (\mathcal{F}\varphi)(h) \quad \text{und} \quad h = (\mathcal{F}\psi)(k),$$

und das impliziert

$$h = (\mathcal{F}\psi)(\mathcal{F}\varphi)(h) = (\mathcal{F}\psi\varphi)(h).$$

Da aber die Identität auf A der $\underline{\text{einzige}}$ Morphismus $\kappa \in \mathrm{Mor}(A,A)$ ist, für den

$$h = (\mathcal{F}\kappa)(h)$$

gilt, folgt

$$\psi\varphi = 1_A.$$

Analog folgt $\varphi\psi = 1_B$.

Daher sind φ und ψ zueinander invers, A und B also isomorph, und die Isomorphismen sind dadurch eindeutig charakteristiert, dass sie die universellen Elemente aufeinander abbilden.

c) Ähnliche Definitionen und Sachverhalte hat man auch für kontravariante mengenwertige Funktoren $\mathcal{G}$, die man selbstverständlich mit den Funktoren $\mathrm{Mor}(-,A)$ vergleicht.

Ein universelles Element ist dann also ein Paar (A,h) mit $h \in \mathcal{G}(A)$, sodass für jedes Objekt B von $\mathcal{K}$ und jedes $k \in \mathcal{G}(B)$ genau ein $\varphi \in \mathrm{Mor}(B,A)$ existiert mit $k = (\mathcal{G}\varphi)(h)$.

Abgesehen davon, dass hier φ von B nach A geht und nicht umgekehrt, sieht diese Formel genauso aus wie im kovarianten Fall. Das kommt daher, dass man diese beiden Fälle durch Übergang zur opposiiten Kategorie ineinander umrechnen kann.

Beispiel 1.3.2 direktes Produkt, direkte Summe

Wir übertragen die Definitionen von direktem Produkt und direkter Summe (Koprodukt) aus der Algebra I in die Welt der Kategorien.

a) Um den Zusammenhang zu sehen schreiben wir das ganze funktoriell auf.

Es seien $\mathcal{K}$ eine Kategorie und A, B zwei fest gewählte Objekte in $\mathcal{K}$. Für ein Objekt X in $\mathcal{K}$ sei

$$\mathcal{F}(X) := \{(\alpha, \beta) \mid \alpha \in \mathrm{Mor}(X, A),\ \beta \in \mathrm{Mor}(X, B)\}.$$

Für einen Morphismus $\varphi : Y \to X$ in $\mathcal{K}$ sei dann

$$\mathcal{F}(\varphi) : \mathcal{F}(X) \to \mathcal{F}(Y), \quad (\mathcal{F}\varphi)(\alpha, \beta) := (\alpha \circ \varphi, \beta \circ \varphi).$$

Dann ist $\mathcal{F}$ ein kontravarianter Funktor von der Kategorie $\mathcal{K}$ in die Kategorie der Mengen.

Ein universelles Element für diesen Funktor ist ein Paar $(P, (\gamma, \delta))$ mit $\gamma \in \mathrm{Mor}(P, A), \delta \in \mathrm{Mor}(P, B)$, sodass es für jedes X und jedes $(\alpha, \beta) \in \mathcal{F}(X)$ genau einen Morphismus $\psi : X \to P$ gibt mit

$$(\alpha, \beta) = \mathcal{F}(\psi)(\beta, \delta).$$

Etwas plakativer kann man dies in einem kommutativen Diagramm aufmalen:

$$\begin{array}{ccc} P & \xrightarrow{\gamma} & A \\ \delta \downarrow & \overset{\psi}{\nwarrow} & \uparrow \alpha \\ B & \xleftarrow{\beta} & X \end{array}$$

Hierbei sind γ und δ fest, und für alle α und β gibt es genau ein ψ.

Statt P schreibt man gerne $A \,\Pi\, B$; dieses Objekt (zusammen mit den Morphismen) ist bis auf einen Isomorphismus eindeutig durch die universelle Abbildungseigenschaft bestimmt, wenn es denn existiert (was nicht immer der Fall ist). Es heißt dann das Produkt von A und B.

b) Nun drehen wir alle Pfeile um.

Die *Summe* (oder auch *Koprodukt* von A und B ist ein Objekt S zusammen mit zwei Morphismen $\alpha : A \longrightarrow S$ und $\beta : B \longrightarrow S$, sodass für jedes Objekt X mit

Morphismen $\varphi : A \longrightarrow X$ und $\psi : B \longrightarrow X$ genau ein Morphismus $\Phi : S \longrightarrow X$ existiert mit

$$\varphi = \Phi \circ \alpha, \quad \psi = \Phi \circ \beta.$$

Auch das gibt es als Diagramm:

$$\begin{array}{ccc} S & \xleftarrow{\alpha} & A \\ \beta \uparrow & \overset{\Phi}{\searrow} & \downarrow \varphi \\ B & \xrightarrow{\psi} & X \end{array}$$

Statt S schreibt man hier oft $A \amalg B$ und nennt das Objekt auch ein *Koprodukt* von A und B. Auch dieses stellt einen Funktor dar. Es wird nicht in jeder Kategorie für beliebige Objekte existieren.

Statt mit zwei Objekten kann man hier auch mit einer Familie von Objekten starten und analog direkte Produkte und Koprodukte definieren.

Wieso sind dann das direkte Produkt und das Koprodukt in der Kategorie der Vektorräume tatsächlich auch verschiedene Vektorräume? Das war eine Übungsaufgabe in der Algebra I...

Beispiel 1.3.3 Mengen

In der Kategorie $\underline{Men}$ aller Mengen ist das Produkt zweier Objekte M, N das kartesische Produkt $M \times N$ mit den Projektionen auf die Einträge als Morphismen.

Das Koprodukt ist die disjunkte Vereinigung $M \times \{0\} \cup N \times \{1\}$. Die zugehörigen Abbildungen sind $M \ni m \mapsto (m, 0)$ und $N \ni n \mapsto (n, 1)$.

Definition 1.3.4 adjungierte Funktoren

a) Es seien $\mathcal{F}$ eine Funktor von $\mathcal{K}$ nach $\mathcal{L}$ und $\mathcal{G}$ eine Funktor von $\mathcal{L}$ nach $\mathcal{K}$.

Dann heißt $\mathcal{G}$ *linksadjungiert* zu $\mathcal{F}$ (und $\mathcal{F}$ heißt *rechtsadjungiert* zu $\mathcal{G}$), wenn für jedes Paar (A, C) von Objekten in $\mathcal{K}$ und $\mathcal{L}$ eine Bijektion

$$\eta_{A,C} : \mathrm{Mor}(\mathcal{G}(C), A) \longrightarrow \mathrm{Mor}(C, \mathcal{F}(A))$$

gibt, die für festes A einen natürlichen Isomorphismus zwischen den Funktoren $\mathrm{Mor}(\mathcal{G}(-), A)$ und $\mathrm{Mor}(-, \mathcal{F}(A))$ vermittelt, sowie für festes C einen natürlichen Isomorphismus der Funktoren $\mathrm{Mor}(\mathcal{G}(C), -)$ und $\mathrm{Mor}(C, \mathcal{F}(-))$.

Diese Funktoren entstehen jeweils durch Komposition eines Homfunktors mit $\mathcal{F}$ beziehungsweise $\mathcal{G}$.

b) Das Yoneda-Lemma sagt uns, dass dies (für festes C) bedeutet, dass es ein Element $h_C \in \mathrm{Mor}(C, \mathcal{F}\mathcal{G}(C)$ gibt, sodass für jeden Morphismus $\varphi \in \mathrm{Mor}(\mathcal{G}(C), A)$

das folgende gilt:

$$\eta_{A,C}(\varphi) = \big(\mathrm{Mor}(C, \mathcal{F}(-))(\varphi)\big)(h_C) = \mathcal{F}(\varphi) \circ h_C.$$

Dabei wird benutzt, was der Funktor $\mathcal{F}$ mit φ macht und wie der Hom-Funktor $\mathrm{Mor}(C, -)$ dann mit $\mathcal{F}(\varphi)$ umgeht.

Das Pendant zum Yoneda-Lemma für den kontravarianten Hom-Funktor $\mathrm{Mor}(-, \mathcal{F}(A))$ (für festes A) sagt, dass es ein Element $k_A \in \mathrm{Mor}(\mathcal{G}\mathcal{F}(A), A)$ gibt, sodass für alle Morphismen $\psi : C \longrightarrow \mathcal{F}(A)$ das folgende gilt:

$$\eta^{-1}_{A,C}(\psi) = k_A \circ \mathcal{G}(\psi).$$

Um also zu zeigen, dass die Funktoren adjungiert sind, muss man Familien von Morphismen (h_C) und (k_A) wie gerade gesagt finden, sodass die Abbildungen

$$\mathrm{Mor}(\mathcal{G}(C), A) \longrightarrow \mathrm{Mor}(C, \mathcal{F}(A)), \quad \varphi \mapsto \mathcal{F}(\varphi) \circ h_C$$

und

$$\mathrm{Mor}(C, \mathcal{F}(A)) \longrightarrow \mathrm{Mor}(\mathcal{G}(C), A), \quad \psi \mapsto k_A \circ \mathcal{G}(\psi),$$

stets zueinander invers sind.

Beispiel 1.3.5 Gruppenring und Einheitengruppe

Dies ist genau der Sachverhalt (nur etwas präziser), den wir in Beispiel 1.2.2e) als Zusammenhang zwischen dem dortigen Vergissfunktor $\mathcal{V}$ und dem Bilden $\mathcal{F}$ des freien Moduls gesehen haben.

Um zu zeigen, dass es so etwas noch öfters gibt, machen wir noch ein Beispiel. Wir betrachten den Funktor aus Beispiel 1.2.2d), der einem Ring seine Einheitengruppe zuordnet. Nennen wir diesen Funktor $\mathcal{E}$.

Umgekehrt brauchen wir einen Funktor, der einer Gruppe einen Ring zuordnet. Dies leistet in universeller Weise der Gruppenring über $\mathbb{Z}$. Es sei also für eine (multiplikativ geschriebene) Gruppe G der Ring $\mathcal{R}(G)$ definiert als der Gruppenring

$$\mathbb{Z}[G] := \{\sum_{g \in G} a_g \cdot g \mid a_g \in \mathbb{Z}, \text{ nur endlich viele } a_g \neq 0\}.$$

Die Multiplikation ist definiert durch

$$(\sum_{g \in G} a_g \cdot g) \cdot (\sum_{h \in G} b_h \cdot h) := \sum_{g \in G} \left(\sum_{h \in G} a_h b_{h^{-1}g} \right) \cdot g.$$

Ein Gruppenhomomorphismus $\Phi : G \longrightarrow H$ setzt sich linear zu einem Ringhomomorphismus $\mathcal{R}(\Phi) : \mathcal{R}(G) \longrightarrow \mathcal{R}(H)$ fort, und damit ist $\mathcal{R}$ ein Funktor.

Ein Homomorphismus von diesem Gruppenring in einen anderen Ring ist eindeutig dadurch festgelegt, was mit der Gruppe G passiert (die als Untergruppe in der Einheitengruppe von $\mathbb{Z}[G]$ sitzt). Die lineare Fortsetzung

$$\eta_{R,G} : \mathrm{Mor}_{\underline{Gruppen}}(G, \mathcal{E}(R)) \longrightarrow \mathrm{Mor}_{\underline{Ringe}}(\mathcal{R}(G), R)$$

zeigt dann, dass $\mathcal{R}$ linksadjungiert zu $\mathcal{E}$ ist.

Kapitel 2

Ringe und Moduln

2.1 Algebren

Wir beginnen diese Kapitel mit einer Wiederholung einiger Sachverhalte aus Algebra I.

Definition 2.1.1 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 ι_A im *Zentrum $Z(A)$ von A*:

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

Dies folgt aus

$$\forall r \in R, a \in A : \iota_A(r) \cdot a = (r1_A)a = r \cdot (1_A a) = r \cdot (a1_A) = a \cdot (r1_A) = a \cdot \iota_A(r).$$

Insbesondere ist das Bild von R unter ι_A ein kommutativer Ring.

c) Wenn umgekehrt R und A Ringe sind und wir einen Ringhomomorphismus $\iota : R \longrightarrow Z(A)$ 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 $\mathrm{Hom}_{R-Alg}(A, B)$. 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.

Beispiel 2.1.2 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: $R[M] := \mathrm{Abb}(M, R)_0$ 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 $f : M \longrightarrow N$ 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).

Definition 2.1.3 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

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

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

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

Dabei ist S^n das n-fache kartesische Produkt von S, also die Menge aller Abbildungen von $\{1, \ldots, n\}$ 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:

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

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 $f : S \longrightarrow N$ gibt es genau einen Monoidhomomorphismus $\widetilde{f}$ von M nach N, der f von S^1 nach M fortsetzt:

$$\widetilde{f}((s_1, \ldots, s_n)) := f(s_1) \circ f(s_2) \circ \cdots \circ f(s_n).$$

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 $f : S \longrightarrow A$ eine Abbildung von Mengen. Dann gehört dazu eine multiplikative Abbildung vom freien Monoid M nach $(A, \cdot)$, nämlich

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

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

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

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 $\Phi : R\{S\} \longrightarrow A$ aus der Abbildung $f : S \longrightarrow A,\ \ s \mapsto \Phi(\delta_s)$, 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 als Algebra) $\rightsquigarrow$ (A als Menge) zueinander adjungiert sind.

Bemerkung 2.1.4 **K-Algebren**

Es seien K ein Körper und $A \neq \{0\}$ eine K-Algebra.

a) Für jedes $a \in A$ haben wir die Abbildung

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

Sie ist 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

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

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 $\mathrm{End}_{K-VR}(A)$.

Das war in Algebra I in einmal eine Übungsaufgabe und ist wieder einmal ein Analogon zum Satz von Cayley.

b) Wenn A als K-Vektorraum n-dimensional ist, so ist A via μ und Basiswahl in 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:

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

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 μ_a im Endomorphismenring invertierbar, aber diese Inverse ist – wegen Cayley-Hamilton – ein Polynom in μ_a, also selbst im Bild von μ, und damit ist a in A invertierbar.

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

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

Hierbei wird benutzt, dass jeder A-Modul ein K-Vektorraum ist, und bei unseren Voraussetzungen endlichdimensional sein muss. Ist nämlich $\{a_1, \ldots, a_n\}$ eine K-Basis von A und $\{m_1, \ldots, m_l\}$ 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 τ_ρ auf A vermöge

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

Wir werden später auf diese sogenante *Spurform* (τ steht für *trace*) zu sprechen kommen.

Bemerkung 2.1.5 Verkettungsoperatoren

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

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

Im Englischen sind das die *intertwining operators*.

Wenn A eine K-Algebra ist, darf man sich bei der Suche nach solchen Φ auf K-Vektorraum Homomorphismen beschränken, was die Sache manchmals 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 $\mathrm{End}_A(M)$ genau aus den K-linearen Abbildungen von M nach M, die zusätzlich G-äquivariant sind.

Jetzt kommt wieder ein neuer Begriff.

Definition 2.1.6 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-Untermoduln 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.

Beispiel 2.1.7 Seltenheit

a) Nicht einmal $\mathbb{Z}$ ist ein halbeinfacher Ring, denn zu $2\mathbb{Z}$ gibt es kein komplementäres Ideal in $\mathbb{Z}$. Halbeinfachheit ist demnach schon etwas spezielles.

b) Ein Körper K ist immer halbeinfach.

Die K-Algebra $A := \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in K\} \subseteq M_2(K)$ hingegen ist nicht halbeinfach, denn zu dem Linksideal $K \cdot \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ gibt es kein komplementäres Linksideal.

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!).

c) 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.

Hilfssatz 2.1.8 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 π 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 π 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 π_1 und π_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 $n \in N_V$, sodass $(u_1, n) \in V$. Dieses n lässt sich eindeutig als $v_2 + u_2$ zerlegen mit $v_2 \in V_2, u_2 \in U_2$. Da aber $(0, v_2)$ auch in V liegt, tut dies auch (u_1, u_2). Wenn es zwei solche u_2s gäbe, so läge ihre Differenz in V_2, was der Komplementarität widerspricht. Also ist dieses u_2 eindeutig durch u_1 festgelegt.

Diese Zuordnung $U_1 \ni u_1 \mapsto u_2 \in U_2$ ist aus Symmetriegründen ein Isomorphismus φ zwischen U_1 und U_2. Damit gilt

$$V = (V_1 \times \{0\}) \oplus (\{0\} \times V_2) \oplus \{(u_1, \varphi(u_1)) \mid u_1 \in U_1\}.$$

Außerdem ist $M_V \times N_V = V \oplus (U_1 \times \{0\})$.

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

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

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

Das liefert uns eine Folgerung:

Folgerung 2.1.9 Kriterium für 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 einfach 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. ◯

Bemerkung 2.1.10 Ein Spezialfall

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:

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

Diesen Prozess nennt man oft auch die Spurbildung.

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

Anwendung 2.1.11 Satz von Maschke[1]

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.

[1] Heinrich Maschke, 1853-1908

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

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

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

Weiter sei U ein $K[G]$-Untermodul. Schließlich sei $\pi : M \longrightarrow U$ irgendeine K-lineare Projektion (mit einem Vektorraumkomplement zu U als Kern). Diese gibt es wegen des Satzes von der Basisergänzung.

Dann definieren wir

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

Dieses Φ ist K-linear, und für jedes $h \in G$ und jedes $m \in M$ gilt:

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

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

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

Daher ist $\widetilde{\pi} := \frac{1}{|G|}\Phi$ eine Projektion auf U, und der Kern davon ist ein zu U komplementärer Untermodul. ◯

Bemerkung 2.1.12 Bezeichnungen für $K[G]$-Moduln

a) 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 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 c) die irreduziblen Darstellungen isomorph sind zu Quotienten von $K[G]$ nach maximalen Linksidealen, 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.

b) Wenn G eine endliche Gruppe ist und M ein endlich erzeugter $\mathbb{C}[G]$-Modul, dann ist M ein endlichdimensionaler $\mathbb{C}$-Vektorraum mit einem Homomorphismus $\rho : G \to \mathrm{Aut}_{\mathbb{C}-\mathrm{VR}}(M)$.

Ist $\langle \cdot, \cdot \rangle$ ein Skalarprodukt auf M, so kann man eines daraus gewinnen, für das die $\rho(g),\ g \in G,$ Isometrien sind, nämlich wieder durch Spurbildung:

$$\beta(v, w) := \sum_{g \in G} \langle \rho(g)(v), \rho(g)(w) \rangle.$$

Ist nun $U \leq M$ ein $\mathbb{C}[G]$-Untermodul, so ist das bezüglich β genommene orthogonale Komplement $U^\perp$ auch G-invariant, also sogar als $\mathbb{C}[G]$-Modul zu U komplementär. Das ist der LA-Beweis für den Satz von Maschke, wobei man sich hier auf endliche Dimension beschränken muss.

c) Ist G endlich und abelsch und M ein endlich erzeugter $\mathbb{C}[G]$-Modul, so ist zunächst jedes $\rho(g)$ diagonalisierbar, da es endliche Ordnung hat. (Oder man benutzt b) und die unitäre Normalform von Isometrien...)

Also ist $M = \oplus_{\lambda \in \mathrm{Spek}(\rho(g))} \mathrm{Eig}(\rho(g), \lambda)$. Da G abelsch ist, ist jeder dieser Eigenräume sogar G-invariant, also haben wir hier eine direkte Summenzerlegung in $\mathbb{C}[G]$-Untermoduln.

Ein Induktionsargument zeigt dann, dass die einfachen $\mathbb{C}[G]$-Moduln alle eindimensional sind, und damit ihre Isomorphieklassen bijektiv den Homomorphismen von G nach $\mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$ entsprechen.

d) Nun sei

$$M = \mathcal{P}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{C} \mid f \text{ stetig}, \ \forall x \in \mathbb{R} : \ f(x+1) = f(x)\}.$$

Das ist ein $\mathbb{C}$-Vektorraum, auf dem die Gruppe $S^1 := \mathbb{R}/\mathbb{Z}$ durch folgende Vorschrift operiert:

$$\forall r + \mathbb{Z} : (\tau_{r+\mathbb{Z}} f)(x) := f(x + r).$$

Die Gruppe S^1 ist kompakt, was fast so gut ist wie endlich, und abelsch. Nimmt man den Satz von Maschke und insbesondere Punkt c) dieser Bemerkung, so suggeriert das, dass $\mathcal{P}(\mathbb{R})$ so etwas wie die direkte Summe von irreduziblen $\mathbb{C}[S^1]$-Moduln sein könnte, die alle eindimensional sein sollten.

Ein (stetiger) Homomorphismus von S^1 nach $\mathbb{C}^\times$ ist immer von der Gestalt

$$\chi_k(r + \mathbb{Z}) := \exp(2\pi \mathrm{i} k r), \quad k \in \mathbb{Z}.$$

Es sollte also jede Funktion $f \in \mathcal{P}(\mathbb{R})$ im Wesentlichen eine Summe von Vielfachen dieser χ_k sein:

$$f = \sum_{k\in\mathbb{Z}} a_k \chi_k.$$

Inwieweit so etwas gilt wird durch die Fourier-Analysis geklärt. Die Gleichheit gilt im L^2-Sinn auf $\mathbb{R}/\mathbb{Z}$.

Dies ist eine der Stellen, wo sich Analysis, Geometrie, Algebra, Zahlentheorie, Maßtheorie und Numerik sehr nahe kommen. Die analytisch interessanten Eigenfunktionen χ_k des Laplace-Operators auf $\mathbb{R}/\mathbb{Z}$ spielen auch algebraisch eine ausgezeichnete Rolle.

Jetzt aber zurću zum Alltagsgeschäft.

Wie sehen Endomorphismen von einfachen Moduln aus?

Proposition 2.1.13 Lemma von Schur[2]

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

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

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

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

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

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

[2] Issai Schur, 1875-1941

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

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 $a_1, \ldots, a_d$ von A erzeugen $a_1m, \ldots, a_dm$ den K-Vektorraum $Am = M$.

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

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

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

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

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

2.2 Noethersche Ringe und Moduln

Hier lernen wir einen hilfreichen Endlichkeitsbegriff kennen.

Definition 2.2.1 Der Emmy-Award

a) Es seien R ein kommutativer Ring und M ein R-Modul. Dann heißt M *noethersch*[3], 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, wir wollen das aber nicht ausführlicher diskutieren.

Beispiel 2.2.2 alles sieht so noethersch aus!

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

[3] nach Amalie Emmy Noether, 1882-1935

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 Φ 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.

Definition 2.2.3 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

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

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 Φ injektiv ist, $\text{Kern}(\Psi) = \text{Bild}(\Phi)$ gilt, und Ψ surjektiv ist. Man könnte dann auch M durch den isomorphen Modul $\Phi(M)$ ersetzen, Φ durch die Einbettung, Q durch $N/\Phi(M)$ und Ψ 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.

Hilfssatz 2.2.4 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 Ψ surjektiv ist. Da N noethersch ist, wird $\Psi^{-1}(V)$ von endlich vielen Elementen $n_1, \ldots, n_k$ erzeugt, aber dann ist V von $\Psi(n_1), \ldots, \Psi(n_k)$ 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 $m_1, \ldots, m_r$ endlich viele Erzeuger von $\Phi^{-1}(U)$. Weiterhin ist $\Psi(U)$ ein Untermodul von Q und damit endlich erzeugt. Es seien $q_1, \ldots, q_s$ Erzeuger von $\Psi(U)$ und $u_1, \ldots, u_s$ Urbilder von ihnen unter Ψ.

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

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

Es gibt also $a_1, \ldots, a_r \in R$, 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

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

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

Hilfssatz 2.2.5 Vererbungslehre

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

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

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

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

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

◯

Satz 2.2.6 Hilberts[4] 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 $C_0 \cup C_1 \cup C_2 \cup \cdots =: C$ 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:

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

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

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

[4] David Hilbert, 1862-1943

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 ≤ 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 $f_{i,j}$. ◯

Folgerung 2.2.7 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

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

ein Erzeugendensystem, das heißt

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

Dann ist der Homomorphismus

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

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 $R[X_1, \ldots X_d]$. Wegen 2.2.2b) ist auch A selbst noethersch. ◯

Definition/Bemerkung 2.2.8 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

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \ldots$$

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*[5].

Eine geordnete Menge ist genau dann noethersch, wenn jede nichtleere Teilmenge ein maximales Element enthält.

Denn: Es sei $(M, \leq)$ noethersch und $S \subseteq M$ nichtleer. Nehmen wir an, es gebe in S kein maximales Element. Es sei $s_1 \in S$ irgendein Element. Wenn sukzessive $s_1 < s_2 < s_3 < \cdots < s_n \in S$ gewählt sind, dann ist auch s_n in S nicht maximal, und es gibt ein $s_{n+1} > s_n$. Auf diese Art konstruiert man eine unendliche, echt aufsteigende Kette in M, die es aber nach Voraussetzung nicht gibt. Also muss es ein maximales Element in M geben.

Wenn umgekehrt jede nichtleere Menge in M ein maximales Element besitzt und $m_1 \leq m_2 \leq \ldots$ eine aufsteigende Folge ist, dann besitzt auch

$$S := \{m_i \mid i \in \mathbb{N}\}$$

ein maximales Element. Das muss aber schon ein m_k sein (für geeignetes $k \in \mathbb{N}$), und es folgt $m_k = m_{k+1} = m_{k+2} \ldots$ Die Folge wird also stationär.

Analog ist eine geordnete Menge genau dann artinsch, wenn jede nichtleere Teilmenge ein minimales Element enthält.

d) Insbesondere haben wir in a) 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.

Hilfssatz 2.2.9 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.

[5]Emil Artin, 1898-1962

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. ◯

Bemerkung 2.2.10 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 Iealen, die die aufsteigende Kettenbedingung verletzt.

2.3 Bilineares

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

Definition/Bemerkung 2.3.1 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 der Definition des Begriffs Algebra haben wir schon die Bilinearität der Multiplikation in einer R-Algebra hingeschrieben. Für einen R-Modul M und für $N := \mathrm{Hom}_{R-Mod}(M, R)$ 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

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

eine symmetrische Bilinearform auf A.

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

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

eine symmetrische Bilinearform auf A.

Definition/Bemerkung 2.3.2 Tensorprodukt kategoriell

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

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

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

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

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

gilt.

Wenn es so einen Modul T gibt, dann heißt er ein *Tensorprodukt von M und N* (über dem Ring R). 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.

Konstruktion 2.3.3 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

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

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

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

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

$$\delta_{(rm_1+m_2,sn_1+n_2)} - rs\delta_{(m_1,n_1)} - r\delta_{(m_1,n_2)} - s\delta_{(m_2,n_2)} - \delta_{(m_2,n_2)}$$

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

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

Dann ist

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

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

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

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

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

Aber Φ ist nun gerade so gemacht, dass

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

gilt. Da die Werte der Abbildung Φ auf den Erzeugern $m \otimes n$ von T durch die gewünschte Beziehung zu β vorgeschrieben sind, gibt es auch nicht mehr als diese eine Abbildung Φ mit der gewünschten Eigenschaft. ◯

Beispiel 2.3.4 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

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

bilinear. Sie induziert also einen Homomorphismus

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

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

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

Wieso? Übung!

Bemerkung 2.3.5 Ringwechsel – Ein Hochzeitsmärchen

Aus der linearen Algebra sieht man vielleicht ein, dass es manchmals sinnvoll ist, Aussagen über rationale Matrizen zu begründen, 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

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

Wir erhalten also insgesamt eine Abbildung

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

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

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

bilinear, definiert also einen Modulhomomorphismus

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

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

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

Bemerkung 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

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

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

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

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

Schließlich erhalten wir eine Abbildung

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

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

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

Hilfssatz 2.3.7 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

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

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

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

Es ist klar, dass man analog einen Homomorphismus

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

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

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

Konstruktion 2.3.8 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 $m_1, \ldots, m_n \in M$. 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

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

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

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

Wir erhalten ein neues Modell des Polynomrings in einer Variablen.

Wenn wir einen freien Modul von höherem Rang verwenden, dann bekommen wir einen nichtkommutativem Ring, und nicht direkt den Polynomring in mehreren Variablen. Wenn $\{b_1, \ldots, b_n\} =: B$ 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 $A \rightsquigarrow \mathrm{Hom}_{Mengen}(B, A)$ 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 manchmals nicht sehr „benutzerfreundlich“.

Beispiel 2.3.9 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 β auf V mit $q(v) = \beta(v, v)$ für alle $v \in V$.

Weiter sei A eine K-Algebra und $\Phi : V \longrightarrow A$ 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

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

Φ induziert einen Algebrenhomomorphismus $T(V) \longrightarrow A$ wie in 2.3.8, und wegen der Bedingung an Φ ist I im Kern von diesem Algebrenhomomorphismus enthalten. Also erhalten wir einen Algebrenhomomorphismus $\Psi : C(q) \longrightarrow A$, 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 *Clifford-algebra* 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 eine Wort der Länge ≤ 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

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

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 $T(M)/I$-Linksidealen, die nicht stationär wird. Also ist $T(M)/I$ nicht linksnoethersch.

2.4 Ordnung und Ganzheit

Ausgehend von Ordnungen in endlichdimensionalen $\mathbb{Q}$-Algebren wollen wir die algebraische Theorie der Ganzheit entwickeln. Dies liefert einen ersten Einblick in eine wichtige Begriffsbildung der algebraischen Zahlentheorie.

Definition 2.4.1 Ordnung

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

Bemerkung 2.4.2 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 Strukturs atz 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 $\{b_1, \ldots, b_d\}$ von A, sodass gilt:

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

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 ζ eine Nullstelle von $X^n - 1$ ist, ist $\mathbb{Z}[\zeta]$ als abelsche Gruppe von $1, \zeta, \ldots, \zeta^{n-1}$ 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 aufwendiger.

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.

Definition 2.4.3 Diskriminante, Maximalordnung

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

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

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

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

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 ± 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 $\mathrm{Spur}\,(ab) \neq 0$.

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.)

Beispiel 2.4.4 Matrizenring

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.

Hilfssatz 2.4.5 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 $\widetilde{\mathcal{O}}$, und hat darin endlichen Index m. Dann gilt für die Diskriminanten D und $\widetilde{D}$ dieser Ordnungen:

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

denn aus einer Basis von $\widetilde{\mathcal{O}}$ macht man eine Basis von $\mathcal{O}$ durch eine ganzzahlige Basiswechselmatrix 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. ◯

Beispiel 2.4.6 Maximalforderung

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 $\widetilde{\mathcal{O}}$ eine Maximalordnung ist, die die ganzzahligen Matrizen umfasst, und wenn die Matrix $M = (a_{ij}) \in \widetilde{\mathcal{O}}$ 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 $E_{11} \cdot M \cdot E_{11} = a_{11}E_{11} \in \widetilde{\mathcal{O}}$. 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 $A := \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in \mathbb{Q}\}$ enthält für jedes $q \in \mathbb{Q}$ die Ordnung

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

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

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

beschrieben, ist also ausgeartet.

Definition 2.4.7 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.

Hilfssatz 2.4.8 Cayley-Hamilton

Es sei R ein beliebiger kommutativer Ring und $M \in R^{d\times d}$ eine quadratische Matrix mit Einträgen in R. Weiter sei

$$F := \det(XI_d - M)$$

das charakteristische Polynom.

Dann gilt $F(M) = 0$.

Beweis. Wir wissen, dass die Aussage für nullteilerfreies R gilt, denn dann liegt R in seinem Quotientenkörper, und man kann das entsprechende Faktum aus der Linearen Algebra benutzen.

Nun sei R ein beliebiger kommutativer Ring. Weiter sei

$$S := \mathbb{Z}[t_{i,j} \mid 1 \leq i, j \leq d]$$

der Polynomring über $\mathbb{Z}$ in d^2 Unbekannten.

Die Vorschrift $t_{i,j} \mapsto m_{i,j}$ (der (i,j)-te Eintrag in M) definiert per universeller Abbildungseigenschaft des Polynomrings einen Ringhomomorphismus $\varphi : S \to R$ vermöge

$$\varphi(g(t_{1,1}, \ldots, t_{d,d}) := g(m_{1,1}, \ldots, m_{d,d}).$$

Dieser liefert auch einen Ringhomomorphismus

$$\varphi^{d\times d} : S^{d\times d} \to R^{d\times d}, \quad (g_{i,j}) \mapsto (\varphi(g_{i,j})).$$

Die Matrix T mit den Einträgen $t_{i,j}$ wird hierbei auf unsere alte Matrix M abgebildet.

Als nächstes liefert uns φ auch noch einen Ringhomomorphismus $\varphi_* : S[X] \to R[X], \varphi_*(\sum g_i X^i) := \sum \varphi(g_i) X^i$.

Dieser bildet das charakteristische Polynom C von T auf das von M ab, denn beide werden über die Leibnizformel berechnet.

Es folgt insgesamt

$$F(M) = \varphi_*(C)(\varphi^{d\times d}(T)) = \varphi^{d\times d}(C(T)) = 0,$$

wobei wir am Ende ausnutzen, dass S nullteilerfrei ist. ◯

Hilfssatz 2.4.9 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:

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

Die Inklusion $\supseteq$ ist hierbei klar, die andere Inklusion folgt, da $s^d, s^{d+1}, \ldots$ 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 $a_1, \ldots, a_d$ ein endliches Erzeugendensystem des R-Moduls A. Die (R-lineare!) Multiplikation μ mit s (d.h. $\mu(x) = sx$) ist dann auf A gegeben durch

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

Auf dem freien R-Modul R^d betrachten wir den Endomorphismus Φ, der durch Multiplikation mit der Matrix $M := (m_{ij})$ gegeben ist. Außerdem machen wir A zu einem $R[X]$-Modul, indem wir X als Multiplikation mit s wirken lassen. Dann ist die Abbildung

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

ein surjektiver Homomorphismus, und es gilt $\pi \circ \Phi = \mu \circ \pi$, da dies auf den jeweils betrachteten Erzeugern stimmt. Man sieht schnell ein, dass für jedes Polynom $F \in R[X]$ auch $\pi \circ F(\Phi) = F(\mu) \circ \pi$ gilt.

Da das charakteristische Polynom F von M ausgewertet bei Φ die Nullabbildung ergibt, gilt $F(\mu) \circ \pi = 0$. Da π surjektiv ist, folgt $F(\mu) = 0$, aber $F(\mu)$ ist die Multiplikation mit $F(s)$, und daher ist

$$F(s) = F(\mu)(1) = 0.$$

Daher ist s ganz über R. ◯

Folgerung 2.4.10 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. ◯

Folgerung 2.4.11 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)). Jedes $r \in R$ ist 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. ◯

Definition/Bemerkung 2.4.12 Quadratische Zahlkörper, Gauß-Lemma

Es sei $\mathbb{Q} \subseteq K$ eine endliche Körpererweiterung.

a) Ein Element $s \in K$ ist genau dann ganz über $\mathbb{Z}$, wenn sein (wie immer: normiertes!) Minimalpolynom in $\mathbb{Q}[X]$ bereits ganzzahlige Koeffizienten hat.

Wenn dem ist, ist s ganz, das ist klar.

Ist umgekehrt s ganz, so sei $f \in \mathbb{Z}[X]$ ein normiertes Polynom mit $f(s) = 0$. Dies ist ein Vielfaches des Minimalpolynoms m von s, also gibt es ein Polynom $g \in \mathbb{Q}[X]$, sodass $f = m \cdot g$.

Da f ganzzahlig mit Leitkoeffizient 1 ist, ist sein Inhalt 1. Das Gauß-Lemma sagt, dass das Produkt der Inhalte von m und g dann auch 1 ist. Es folgt

$$f = \frac{m}{\mathrm{Inh}(m)} \cdot g\mathrm{Inh}(g),$$

aber die beiden Faktoren rechter Hand sind ganzzahlige Polynome. Da ihr Produkt normiert ist, sind sie beide (bis aufs Vorzeichen) normiert, das heißt aber, dass der Inhalt von m schon 1 ist, also liegt m in $\mathbb{Z}[X]$.

b) Insbesondere ist der ganze Abschluss von $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ für quadratfreies ganzes d die Menge aler Elemente, deren Norm und Spur ganz sind, und das ist $\mathbb{Z}[\omega]$ für

$$\omega = \begin{cases} \sqrt{d}, & \text{falls } d \equiv 2 \text{ oder } 3 \pmod 4, \\ \frac{1+\sqrt{d}}{2}, & \text{falls } d \equiv 1 \pmod 4. \end{cases}$$

c) Der ganze Abschluss von $\mathbb{Z}$ in K heißt der *Ganzheitsring* von K und wird meistens mit $\mathcal{O}_K$ notiert.

d) Die Kommutativität von S ist in 2.4.10 nicht nur hilfreich sondern tatsächlich essentiell. Zum Beispiel sind die beiden folgenden Elemente der $\mathbb{Z}$-Algebra $\mathbb{Q}^{2\times 2}$ zwar ganz, ihre Produkte aber nicht:

$$\begin{pmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Das Minimalpolynom des Produkts ist ja $X(X - \frac{1}{2})$, und es gibt kein normiertes ganzzahliges Vielfaches davon.

2.5 Darstellungstheorie endlicher Gruppen

Bemerkung 2.5.1 Erinnerung

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 (2.1.11) sowie das Lemma von Schur (2.1.13).

Es seien G eine Gruppe und K ein Körper. Eine K-lineare Darstellung von G ist eine Operation $\bullet : G \times V \to V$ auf einem K-Vektorraum V, sodass für alle $g \in G$ die Abbildung $V \ni v \mapsto g \bullet v =: gv \in V$ ein K-linearer Automorphismus ist.

Alternativ kann man das auffassen als einen Gruppenhomomorphismus

$$\rho : G \to \mathrm{Aut}_K(V),\ \rho(g) := [V \ni v \mapsto gv \in V].$$

Dies wiederum ist nichts anderes als ein K-Algebrenhomomorphismus

$$\tilde{\rho} : K[G] \to \mathrm{End}_K(V),\ \sum c_g \delta_g \mapsto \sum c_g \rho(g).$$

Dabei ist $\{\delta_g \mid g \in G\}$ die nun schon legendäre K-Basis des Gruppenrings.

Eine besonders wichtige Darstellung von G ist die *reguläre* Darstellung. Es ist die Darstellung, die dem $K[G]$-Modul $K[G]$ entspricht, also die Aktion von G auf dem Vektorraum $V = \mathrm{Abb}(G, K)_0$ vermöge linearer Fortsetzung von $g \bullet \delta_h := \delta_{gh}$. In koordinatenfreier Schreibweise ist das

$$g \bullet f(x) = f(g^{-1}x).$$

Das Invertieren ist manchmal störend, lässt sich aber nicht umgehen.

Eine Darstellung heißt *irreduzibel*, wenn sie keine nichttriviale echte Unterdarstellung hat und selbst nichttrivial ist.

Jede irreduzible Darstellung ist ein Quotient der regulären Darstellung (vgl. 2.1.7), und wenn die Charakteristik von K kein Teiler der Ordnung von G ist (das jetzt als endlich vorausgesetzt sei), so ist jede endlichdimensionale Darstellung nach Maschke eine direkte Summe von irreduziblen.

Definition/Bemerkung 2.5.2 Ein Halbring

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.

Wenn die Charakteristik von K kein Teiler der Ordnung $|G|$ ist, dann ist jede endlich dimensionale K-lineare Darstellung von G eine direkte Summe von irreduziblen Darstellungen, das sagt uns der Satz von Maschke. Außerdem ist jede irreduzible Darstellung von G enthalten als Teilmodul im Gruppenring selbst, es gibt also nur endlich viele Typen irreduzibler Darstellungen.

Diese nennen wir jetzt $M_1, \ldots, M_h$.

Es sei

$$\Phi : M_1^{e_1} \oplus \cdots \oplus M_h^{e_h} \to M_1^{f_1} \oplus \cdots \oplus M_h^{f_h},$$

ein Isomorphismus von $K[G]$-Moduln.

Eingeschränkt auf $M_i^{e_i}$ liefert er eine Einbettung in die rechte Seite. Jeder irreduzible Teilmodul in $M_j^{f_j}$ ist – wegen der Halbeinfachheit – zu M_j isomorph. Daher muss das Bild von $M_i^{e_i}$ im Teilraum $M_i^{f_i}$ landen. Da die Dimension endlich ist, folgt $f_i \geq e_i$ für alle i. Analog folgt $f_i \leq e_i$ für alle i, und daher stimmen die Exponenten e_i und f_i jeweils überein.

Daher gehört zu jedem Isomorphietyp V einer Darstellung von G genau ein Modul der Gestalt $M_1^{e_1} \oplus \cdots \oplus M_h^{e_h}$, und V legt auf eindeutige Art die Exponenten $e_1, \ldots, e_h \in \mathbb{N}_0$ fest. Man nennt e_i die *Multiplizität* oder *Vielfachheit* von M_i in V.

Die additive Halbgruppe von $\mathcal{H}_K(G)$ ist also isomorph zu

$$\mathbb{N}_0 M_1 + \mathbb{N}_0 M_2 + \cdots + \mathbb{N}_0 M_h \cong \mathbb{N}_0^h.$$

Insbesondere gilt in $\mathcal{H}_K(G)$ unter der Voraussetzung, dass $\mathrm{char}(K)$ kein Teiler von $|G|$ ist, eine Kürzungsregel:

$$V_1 \oplus V_2 \cong V_1 \oplus V_3 \Rightarrow V_2 \cong V_3.$$

Definition/Bemerkung 2.5.3 Der Darstellungsring

Durch Einführung von formalen inversen (wie von $\mathbb{N}_0$ nach $\mathbb{Z}$) bezüglich der Addition macht man aus $\mathcal{H}_K(G)$ einen Ring:

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

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

Wir schreiben dann auch $\rho_1 - \rho_2$ für die Äquivalenzklasse von (ρ_1, ρ_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 ρ_1 und ρ_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 braucht man eine Kürzungsregel in $\mathcal{H}_K(G)$, wie wir sie oben unter der Voraussetzung sahen, dass die Charakteristik von K kein Teiler der Gruppenordnung ist. *Das setzen wir nun voraus.*

In diesem Fall ist in der Notation von 2.5.2

$$\mathcal{R}_K(G) = \bigoplus_{i=1}^{h} \mathbb{Z} M_i$$

ein freier, endlich erzeugter $\mathbb{Z}$-Modul.

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

Die Darstellungstheorie hat das Ziel, diesen kommutativen Ring zu verstehen und aus diesem Verständnis auch für individuelle Darstellungen Informationen zu gewinnen. Dazu betrachtet man den leichter verständlichen Ring der Klassenfunktionen, der in Kürze eingeführt wird. Vorher machen wir ein erstes Beispiel.

Beispiel 2.5.4 Endliche abelsche Gruppen

Es sei G eine endliche abelsche Gruppe und K ein algebraisch abgeschlossener Körper.

Weiter sei ρ eine irreduzible Darstellung von G.

Für festes g ist dann wegen der Kommutativität von G der Automorphismus $\rho(g)$ des K-Vektorraums auch ein Verkettungsoperator. Daher ist er nach dem Lemma von Schur die Multiplikation mit einem Skalar aus K. Da dies für jedes g gilt, ist jeder Vektor $v \neq 0$ ein gemeinsamer Eigenvektor der $\rho(g)$, und damit ist Kv ein nichttrivialer Untermodul der Darstellung. Diese ist aber irreduzibel und folglich gleich Kv. Die irreduziblen Darstellungen von G sind also alle eindimensional. Sie entsprechen der Gruppe $\hat{G} := \mathrm{Hom}(G, K^\times)$ (mit punktweiser Multiplikation als Verknüpfung).

Wenn nun zwei irreduzible Darstellungen $\rho : G \to \mathrm{Aut}_K(Kb)$ und $\sigma : G \to \mathrm{Aut}_K(Kc)$ (mit jeweils einem fest gewählten Basisvektor) sind und $\rho(g)(b) =$

$\chi_1(g) \cdot b, \quad \sigma(g)(c) = \chi_2(g) \cdot c,$ dann folgt

$$(\rho \otimes \sigma)(g)(b \otimes c) = (\chi_1 \cdot \chi_2)(g) \cdot b \otimes c.$$

Die Multiplikation in $\mathcal{R}_K(G)$ von zwei irreduziblen entspricht also der Multiplikation der zugehörigen Homomorphismen in $\hat{G}$.

Nun müssen wir noch sehen, ob wir noch mehr über $\hat{G}$ herausbekommen. Dies geht am besten im Fall, dass $\mathrm{char}(K)$ kein Teiler von $|G|$ ist.

Wir verwenden dann die Zerlegung

$$K[G] = \bigoplus_{\chi \in \hat{G}} \chi^{e_\chi},$$

die es laut Maschke gibt. Für eine Funktion in $f \in \chi^{e_\chi}$ gilt dann, dass

$$\forall h \in G : f(h) = f(he_G) = (h^{-1} \bullet f)(e_G) = \chi(h^{-1}) \cdot f(e_G),$$

und f ist eindeutig durch seinen Wert bei e_G festgelegt. Daher ist der Vektorraum χ^{e_χ} eindimensional, und die Anzahl der Summanden ist gleich der Ordnung $|G|$. Es folgt

$$|\hat{G}| = |G|.$$

Nutzt man nun den Hauptsatz für endliche abelsche Gruppen aus, so sieht man sogar einen Isomorphismus zwischen G und $\hat{G}$.

Insgesamt folgt für den Darstellungsring unter unseren speziellen Bedingungen:

$$\mathcal{R}_K(G) \cong \mathbb{Z}[\hat{G}] \cong \mathbb{Z}[G].$$

Definition 2.5.5 Charaktere, Klassenfunktionen, κ_G

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

Dann definieren wir die Abbildung

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

Sie heißt der *Charakter von* ρ.

Dann gilt für alle $g, h \in G$:

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

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 χ_ρ auf den Konjugationsklassen von G konstant. Eine Funktion $f : G \longrightarrow K$ heißt eine *Klassenfunktion*, wenn sie auf den Konjugationsklassen von G konstant ist, also für 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 κ_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 κ_G Isomorphieklassen irreduzibler Darstellungen über $\mathbb{C}$.

Dazu brauchen wir zunächst einmal eine Aussage über Charaktere.

Hilfssatz 2.5.6 ein Ringhomomorphismus

Die Abbildung

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

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 TEXen. Es seien also $\rho : G \longrightarrow \mathrm{Aut}_K(V)$ und $\sigma : G \longrightarrow \mathrm{Aut}_K(W)$ 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 $\left(\begin{smallmatrix} A & 0 \\ 0 & \tilde{A} \end{smallmatrix}\right)$ die Abbildung $\rho(g) \oplus \sigma(g)$ auf $V \oplus W$ bezüglich einer geeignet gewählten Basis, und offensichtlich ist damit

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

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

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

ist. ◯

Bemerkung 2.5.7 positive Charakteristik

In Charakteristik $p > 0$ ist die Abbildung χ 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 eindeutig bestimmt. Wir werden das aber nur in der Situation des Gruppenrings weiterverfolgen.

Definition/Bemerkung 2.5.8 eine Bilinearform

Es seien K ein Körper und G eine endliche Gruppe. Dann führen wir auf dem Raum $\mathrm{Abb}(G, K)$ 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 $\rho(g)$ konjugert 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 sich für Charaktere im zweiten Argument von β nur um den Faktor $\frac{1}{|G|}$ unterscheidet.

Analog 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 β eingeführt?

Hilfssatz 2.5.9 Schur und die Spur

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

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

die Nullabbildung, wenn ρ und σ nicht isomorph sind.

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

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

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

Daher ist $\widetilde{\Phi} = 0$, wenn ρ und σ 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 $\widetilde{\Phi}$ die Multiplikation mit einem Skalar $\lambda \in K$ ist. Es gilt wegen der Ähnlichkeitsinvarianz der Spur

$$\dim_K(V) \cdot \lambda = \mathrm{Spur}(\widetilde{\Phi}) = \sum_{g \in G} \mathrm{Spur}(\Phi) = |G| \cdot \mathrm{Spur}(\Phi),$$

woraus sich der angegebene Wert von λ berechnet. ◯

Bemerkung 2.5.10 Kuriosität am Rande

Es sei K ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$ und G ein endliche Gruppe, deren Ordnung kein Vielfaches von p ist. Dann ist die Dimension einer irreduziblen Darstellung niemals ein Vielfaches von p. Schließlich gibt es auf jedem nichttrivialen Vektorraum einen Endomorphismus mit Spur 1, und dann hätten wir immer noch die Gleichung $\dim_K(V) \cdot \lambda = |G|$, und rechts steht etwas von 0 verschiedenes.

Die Dimension einer irreduziblen K-linearen Darstellung einer p-Gruppe ist sogar immer 1: Nur die triviale Darstellung ist eine irreduzible Darstellung einer p-Gruppe in Charakteristik p.

Das sieht man per vollständiger Induktion nach der Gruppenordnung. Der Induktionsanfang für $|G| = 1$ ist klar. Ist $|G| = p^n > 1$, so sei $\rho : G \to \mathrm{Aut}(V)$

eine Darstellung in Charakteristik p. Das Zentrum von G ist nichttrivial und operiert nach dem Lemma von Schur über die Multiplikation mit einem Homomorphismus $\alpha : Z(G) \to K^\times$. Da K Charakteristik p hat, ist die einzige p-Potenz-EInheitswurzel in K die Eins, also ist α konstant gleich 1, und daher operiert die Faktorgruppe $G/Z(G)$ auf V. Auch diese Aktion ist irreduzibel, und nach Induktionsvoraussetzung daher trivial. Das zeigt die Behauptung.

Anwendung 2.5.11 „Matrixkoeffizienten“

Wir wählen nun in der Situation des vorangegangenen Hilfssatzes Basen der Vektorräume und erhalten daraus Abbildungsmatrizen $A(g) := (a_{ij}(g))_{1\le i,j\le d}$ für ρ und $B(g) := (b_{ij}(g))_{1\le i,j\le e}$ für σ, wobei $d := \dim_K(V)$, $e := \dim_K(W)$ gelte. Wenn Φ durch die Elementarmatrix $(E_{j,k})$ beschrieben wird, dann wird $\widetilde{\Phi}$ 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 λ wie in 2.5.9 durch $\lambda = \#G/\dim_K(V)$ gegeben, der Fall $j = k$ entspricht ja einer Elementarmatrix mit Spur 1.

Folgerung 2.5.12 Schursche Orthogonalitätsrelation

Es seien ρ, σ irreduzible Darstellungen der endlichen Gruppe G über einem algebraisch abgeschlossenen Körper K der Charakterstik 0. (Dasselbe geht auch für $\mathrm{char}(K) \not| \#G$ *.)*

Dann gilt für die Charaktere χ_ρ und χ_σ:

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

Beweis: Wir wählen ein Matrizenmodell von ρ wie zuvor und erhalten mit obiger Rechenregel

$$\beta_G(\chi_\rho, \chi_\rho) = \sum_g \sum_i a_{ii}(g) \sum_j a_{jj}(g^{-1}) = \sum_{i=1}^{\dim \rho} \sum_g a_{ii}(g) a_{ii}(g^{-1}) = |G|.$$

Für verschiedene irreduzible sieht die Rechnung ähnlich aus, nur dass eben am Ende 0 herauskommt. ◯

Folgerung 2.5.13 Injektivität von χ, Kriterium der Irreduzibiltät

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 ρ 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 zerlegen $\rho = \bigoplus_{i=1}^k \rho_i^{m_i}$ in irreduzible Summanden. 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 wir nur einen Summanden haben, wenn also ρ irreduzibel ist. ◯

Bemerkung 2.5.14 Algebraisch offen

a) Wenn K nicht algebraisch abgeschlossen ist, aber immer noch Charakteristik 0 hat, dann ist χ 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[6] Inklusionen stehen. Da χ in der unteren Zeile injektiv ist, gilt dies also auch in der oberen.

[6]Der Nachweis, dass links wirklich eine Inklusion steht, ist allerdings noch eine Überlegung wert.

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 dies 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 kein Teiler von $\#G$ ist, dann gilt 2.5.13 immerhin fast: χ ist zwar nicht mehr injektiv, aber der Kern von χ ist so klein, wie er nur sein kann: $\mathrm{Kern}(\chi) = p \cdot \mathcal{R}_K(G)$. Der Beweis ist analog zu dem in Charakteristik 0, die Charaktere der irreduziblen Darstellungen sind immer noch linear unabhängig über $K,$ da sie bezüglich β orthogonal und anisotrop sind.

d) Insbesondere gilt im Falle eines Körpers K, dessen Charakteristik nicht die Gruppenordnung teilt, dass die Anzahl der irreduziblen Darstellung nicht größer ist als die Anzahl $\kappa(G)$ der Konjugationsklassen in G.

Denn für algebraisch abgeschlossene Körper stimmt das, und ansonsten liegt der Darstellungsring $\mathcal{R}_K(G)$ ja immer noch in dem Darstellungsring von G über dem algebraischen Abschluss von K. Diese Inklusion werde ich später noch einmal thematisieren.

Folgerung 2.5.15 Zerlegung einer gegebenen Darstellung

Es sei ρ eine endlichdimensionale Darstellung der endlichen Gruppe G über dem algebraisch abgeschlossenen Körper K der Charakteristik 0. Weiter seien $\rho_1, \ldots, \rho_k$ 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 / Bemerkung. Klar / In positiver Charakteristik p erhält man auf diesem Weg nur die Multiplizitäten modulo p, daher muss man hier wirklich Charakteristik 0 voraussetzen. ◯

Folgerung 2.5.16 Zerlegung der regulären Darstellung

Wenn K algebraisch abgeschlossen von Charakteristik 0 ist und $\rho_1, \ldots, \rho_k$ die irreduziblen Darstellungen sind, dann ist die Multiplizität der irreduziblen Darstellung ρ_i in der regulären Darstellung gleich $\dim(\rho_i)$. Es ist ja der Charakter $\chi_{\rho_{\text{reg}}}$ der regulären Darstellung gegeben durch

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

Nach der oben geklärten Formel ist die Multiplizität von ρ_i in der regulären Darstellung ρ_{reg} also

$$\begin{aligned} \tfrac{1}{|G|}\beta_G(\chi_{\rho_{\text{reg}}}, \chi_{\rho_i}) &= \tfrac{1}{|G|}\textstyle\sum_g \chi_{\rho_{\text{reg}}}(g)\chi_{\rho_i}(g^{-1}) \\ &= \tfrac{1}{|G|}\chi_{\rho_{\text{reg}}}(e_G)\chi_{\rho_i}(e_G) + \tfrac{1}{|G|}\textstyle\sum_{g\neq e_G} 0 \cdot \chi_{\rho_i}(g^{-1}) \\ &= \chi_{\rho_i}(e_G) = \dim(\rho_i). \end{aligned}$$

Konkret heißt das: Wenn $\rho_1, \ldots, \rho_k$ die irreduziblen Darstellungen von G sind und d_i die Dimension von ρ_i, dann gilt

$$K[G] \cong \bigoplus_{i=1}^{k} d_i \cdot \rho_i, \quad |G| = \sum_{i=1}^{k} d_i^2.$$

Nun sollten wir noch sehen, wie viele irreduzible Darstellungen es gibt. Es können höchstens κ_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.

Satz 2.5.17 Eine Basis des Raums der Klassenfunktionen

Es sei K ein algebraisch abgeschlossener Körper, dessen Charakteristik kein Teiler der Ordnung der endlichen Gruppe G ist.

Dann bilden die Charaktere χ_i, $1 \leq i \leq k$, der irreduziblen Darstellungen von G eine Basis des Raums $\mathcal{C}_K(G)$ der Klassenfunktionen.

Insbesondere gilt $k = \kappa(G)$.

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

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

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

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 ρ_i isomorph. Da Φ nicht irgendein Endomorphismus der regulären Darstellung ist, sondern eine Linearkombination der Wirkungen der Gruppenelemente, lässt Φ tatsächlich jeden G-invarianten Teilraum invariant, insbesondere also auch die irreduziblen Bestandteile.

Wegen des Lemmas von Schur ist die Einschränkung von Φ auf solch einen irreduziblen Teilraum die Multiplikation mit einem Skalar λ_i; dieser berechnet sich wegen

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

als

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

Wegen 2.5.10 ist diese Division in K immer möglich.

Für die Funktion

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

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

Da f sich vermöge

$$\Phi(\delta_{e_G}) = \sum_{g \in G} f(g)\delta_{g^{-1}}$$

aus Φ zurückgewinnen lässt, folgt

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

Damit erzeugen die χ_i den Raum der Klassenfunktionen als K-Vektorraum. ◯

Definition/Bemerkung 2.5.18 Eine Projektion

Es seien G, K wie im letzten Satz und ρ eine beliebige, endlichdimensionale und K-lineare Darstellung von G.

Weiter sei $\rho = \sum_j \sigma_j$ eine Zerlegung von ρ in irreduzible Teildarstellungen.

Weiter sei ρ_i eine irreduzible Darstellung von G

Das Bild des Endomorphismus

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

von ρ hat folgende Eigenschaft: Auf jedem zu ρ_i isomorphen σ_j ist Φ die Multiplikation mit dem Skalar $|G|/\dim(\rho_i)$, und auf jedem anderen σ_j ist es die Nullabbildung.

Da dies für jede Zerlegung von ρ in irreduzible stimmt, ist jedenfalls die Summe der zu ρ_i isomorphen σ_j wohldefiniert. Er heißt die *isotypische Komponente von* ρ_i *in* ρ.

Die beste Projektion auf diese Komponente haben wir gerade scho fast hingeschrieben: Der Endomorphismus $\frac{\dim(\rho_i)}{|G|} \sum_{g \in G} \chi(g)\rho(g^{-1})$ ist eine G-äquivariante Projektion auf die Isotypische Komponente.

Beispiel 2.5.19 zyklische Gruppe

Es sei $G = \langle \sigma \rangle$ eine zyklische Gruppe der Ordnung n und $K = \mathbb{C}$. Die irreduziblen Darstellungen von G entsprechen den Homomorphismen von G nach $\mathbb{C}^\times$, eine d-dimensionale Darstellung ρ ist durch eine Matrix $A = \rho(\sigma)$ gegeben, für die $A^n = I_d$ die Einheitsmatrix ist. Nach geeigneter Basiswahl können wir uns A als Diagonalmatrix wünschen:

$$\rho(\sigma) := A = \mathrm{diag}(\zeta_1, \zeta_1 \ldots, \zeta_1, \zeta_2, \ldots \zeta_2, \ldots, \zeta_l, \ldots, \zeta_l),$$

wobei $\zeta_1, \ldots \zeta_l$ die l Eigenwerte von A sind und damit auch die Gleichung $\zeta_i^n = 1$ erfüllen.

Für den Charakter

$$\chi_j : G \to \mathbb{C}^\times, \chi_j(\sigma^k) = \zeta_j^k,$$

ist dann

$$\Phi_j := \sum_{g \in G} \chi_j(g)\rho(g^{-1}) = \sum_{k=0}^{n-1} \zeta_j^k A^{-k}$$

eine Diagonalmatrix mit den Einträgen

$$\sum_{k=0}^{n-1} \zeta_j^k \zeta_i^{-k} = \sum_{k=0}^{n-1} (\zeta_j/\zeta_i)^k = \begin{cases} 0, & j \neq i, \\ n, & j = i. \end{cases}$$

Daher ist Φ_j das n-fache der Projektion auf den Eigenraum von A zum Eigenwert ζ_j längs der Summe der anderen Eigenräume.

Die isotypische Komponente von χ_j in ρ **ist** dieser Eigenraum.

Beispiel 2.5.20 Jetzt muss die Theorie sich bewähren

a) Wir wissen jetzt, dass es (im algebraisch abgeschlossenen Fall in Charakterstik 0) genau κ_G Isomorphietypen von irreduziblen Darstellungen einer endlichen Gruppe G mit κ_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. Hilfreich ist hierbei auch immer ein Stück linearalgebraischer Intuition.

b) Als Beispiel nehmen wir $K = \mathbb{C}$ und $G = S_4$. Die Gruppe G hat 24 Elemente und 5 Konjugationsklassen. Diese entsprechen bijektiv den (aufsteigenden) Partitionen von 4, wobei einer Partition eben ein Typ von Zykelzerlegung zugeordnet wird. Wir wählen Repräsentanten der Konjugationsklassen:

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

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

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 (bis auf Permutation) 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 der zugehörigen Darstellungen zu bestimmen. Da es nur eine zweidimensionale irreduzible Darstellung gibt und diese nach Tensorieren mit dem Signum wieder eine zweidimensionale irreduzible Darstellung gibt, muss die Spur von ρ_3 auf den ungeraden Permutationen verschwinden. $\chi_2(e_G) = 2$ gilt aus Dimensionsgründen.

Eine 2×2-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 χ_3 mit dem trivialen Charakter sagt

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

Die Vorfaktoren $1, 3, 8, 6, 6$ geben hier jeweils die Kardinalitäten der Konjugationsklassen wieder.

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 χ_3.

Nun brauchen wir noch χ_4 und χ_5. Dies sind Charaktere von dreidimensionalen Darstellungen. Bei den Transpositionen und Vierzykeln dürfen die nicht alle verschwinden, denn sonst nähme jeder Charakter bei Transpositionen und Vierzykeln denselben Wert an (denn χ_1, χ_2, χ_3 tun das auch schon). Wäre $\rho_{4/5}((1\ 2))$ trivial, so wäre $(1\ 2)$ im Kern von $\rho_{4/5}$, und damit $\rho_{4/5}$ trivial, weil die einzige normale Untergruppe der S_4, die $(1\ 2)$ enthält, eben S_4 selbst ist.

Die Darstellung zu χ_4 muss also $(1\ 2)$ auf eine Matrix der Ordnung 2 abbilden, die in Dimension 3 Spur 1 oder -1 hat: $\chi_4((1\ 2)) = \pm 1$. Da das Tensorieren mit dem Signum ρ_4 und ρ_5 vertauscht, darf man sich das Vorzeichen aussuchen: ohne Einschränkung gilt $\chi_4((1\ 2)) = 1$.

Da χ_4 sowohl auf χ_1 als auch auf χ_2 senkrecht steht, sieht man, dass $\chi_4((1\,2\,3\,4)) = -1$ gelten muss. Es folgt mit ähnlichen Rechnungen wie für χ_3 die folgende Charaktertafel für S_4:

Klasse	χ_1	χ_2	χ_3	χ_4	χ_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 ρ_3 bekommt man so: weil $\chi_3((1\ 2)(3\ 4)) = 2$ gilt, ist die zugehörige 2×2-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 Permutationen bilden zusammen mit der Identität die Kleinsche Vierergruppe V_4, und $S_4/V_4 \cong S_3$. Wir erhalten ρ_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 ρ_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 dreidimensionaler invarianter Unterraum.

Der Charakter der vierdimensionalen Darstellung σ ist

$$\chi_\sigma(e_G) = 4, \chi_\sigma((1\ 2)) = 2,\ \chi_\sigma((1\ 2)(3\ 4)) = 0, \chi_\sigma((1\ 2\ 3)) = 1,\ \chi_\sigma((1\ 2\ 3\ 4)) = 0.$$

Es ergibt sich $\chi_\sigma = \chi_1 + \chi_4$, und dem dreidimsionalen Teilraum bleibt nichts anderes übrig, als die Darstellung zu χ_4 zu sein.

Schließlich setzen wir $\rho_5(g) := \mathrm{sgn}(g)\rho_4(g)$ und erhalten die zweite irreduzible Darstellung von S_4 in Dimension 3.

Da wir ja eigentlich den Darstellungsring kennen lernen wollten, sollten wir noch überlegen, wie sich jeweils die Produkte der Charaktere als Linearkombinationen der Charaktere schreiben lassen.

Das Ergebnis ist folgende Tabelle:

$\cdot$	χ_1	χ_2	χ_3	χ_4	χ_5
χ_1	χ_1	χ_2	χ_3	χ_4	χ_5
χ_2	χ_2	χ_1	χ_3	χ_5	χ_4
χ_3	χ_3	χ_3	$\chi_1+\chi_2+\chi_3$	$\chi_4+\chi_5$	$\chi_4+\chi_5$
χ_4	χ_4	χ_5	$\chi_4+\chi_5$	$\chi_1+\chi_3+\chi_4+\chi_5$	$\chi_2+\chi_3+\chi_4+\chi_5$
χ_5	χ_5	χ_4	$\chi_4+\chi_5$	$\chi_2+\chi_3+\chi_4+\chi_5$	$\chi_1+\chi_3+\chi_4+\chi_5$

Das kann man entweder durch Gauß-Verfahren feststellen, oder man rechnet etwas systematischer die Vielfachheiten von χ_k in $\chi_i \cdot \chi_j$ mit $\frac{1}{24}\beta_G(\chi_i \cdot \chi_j, \chi_k)$.

Außerdem ist es manchmal bequem, zum Beispiel $\chi_2 \cdot \chi_4 = \chi_5$ zu benutzen, um $\chi_4^2 = \chi_5^2$ einzusehen (da $\chi_2^2 = \chi_1$) oder $\chi_3\chi_5$ auf $\chi_3\chi_4$ zurückzuführen.

Bemerkung 2.5.21 Terminologie

Der enge Zusammenhang zwischen Charakteren und Darstellungen führt dazu, dass man in Charakteristik 0 auch von der Dimension eines Charakters spricht, und damit natürlich die Dimension der bis auf Isomorphie eindeutigen zugehörigen Darstellung meint.

Die eindimensionalen Charaktere sind insbesondere die Charaktere der Homomorphismen von G nach $K^\times$, die aber blöder Weise sogar mit diesen Homomorphismen übereinstimmen. Dies führt bisweilen zur Verwirrung, insbesondere, wenn manche Leute dazu neigen, die eindimensionalen Charaktere einfach nur Charaktere zu nennen. Das kommt häufiger vor als man meint.

Bemerkung 2.5.22 Untergruppen

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

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

b) Es sei $\rho : G \to \mathrm{Aut}_K(V)$ gegeben. Wir wählen in V einen Untervektorraum W, der unter der H-Aktion irreduzibel ist.

Für $g \in G,\ h \in H$ gilt dann

$$\rho(g)W = \rho(gh)W.$$

Wenn H normal ist und wir Nebenklassenvetreter $g_1, \ldots, g_d$ von H in G gewählt haben, dann ist insbesondere

$$\sum_{i=1}^{d} g_i W \subseteq V$$

eine Unterdarstellung von ρ, denn für jedes $g \in G$ und jedes i gibt es ein j und ein $h \in H$, sodass $gg_i = g_j h$. Die Wirkung von g permutiert also die Summanden.

Wenn nun ρ irreduzibel war, dann ist dieser Modul zwangsläufig alles:

$$V = \sum_{i=1}^{d} g_i W.$$

Insbesondere gilt $\dim(V) \leq [G : H] \dim(W)$.

Das zeigt, dass die irreduziblen Darstellungen einer Gruppe, die einen abelschen Normalteiler von Index d besitzt, höchstens Dimension d haben, zumindest über Körpern, in denen es eine primitive $|H|$-te Einheitswurzel gibt.

c) Wenn die Summe in Teil b) eine direkte Summe und gleich V ist, dann heißt ρ die *von der Darstellung von H auf W induzierte Darstellung.*

Dies wollen wir jetzt noch systematischer behandeln und uns überlegen, dass es für jede Darstellung von H eine induzierte gibt.

Definition/Bemerkung 2.5.23 Die induzierte Darstellung

a) Es seien $H \subseteq G$ zwei endliche Gruppen. Wir wollen einen Funktor einführen, der aus einer Darstellung von H immer eine von G produziert. Alles soll für den Körper K klappen.

Wir nehmen also einen $K[H]$-Modul W und wollen diesem einen $K[G]$-Modul zuordnen. Dazu nehmen wir hilfsweise den Vektorraum

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

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 $\hat{W}$, 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 $\hat{W}$. Wir nennen ihn $\mathrm{Ind}_H^G W$.

Ein schönes konkretes Modell erhalten wir wie folgt:

Es ist

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

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

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

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

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

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

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

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!

b) 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 $g_1, \ldots, g_r \in G$, sodass

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

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

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

Wir erhalten somit eine Bijektion von $\mathrm{Ind}_H^G W$ 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 $1 \leq \pi(i) \leq r$ und $h \in H$, sodass $g^{-1}g_i = g_{\pi(i)}h_i$ gilt. Dann macht die Operation von g aus dem r-Tupel $(w_1, \ldots, w_r)$ das Tupel

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

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

c) Beispiel: Wenn $W = K$ die triviale eindimensionale Darstellung von H ist, dann ist die induzierte Darstellung isomorph zur Darstellung von G auf $\mathrm{Abb}(G/H, K)$, die durch $(g \bullet f)(xH) := f(g^{-1}xH)$ gegeben wird, also eine sogenannte *Permutationsdarstellung*.

Bemerkung 2.5.24 Der Charakter eines induzierten Moduls

Es seien W ein endlichdimensionaler $K[H]$-Modul (Darstellung $\sigma : H \longrightarrow \mathrm{Aut}_K(W)$), H eine Untergruppe der endlichen Gruppe G, und $V := \mathrm{Ind}_H^G(W)$ 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:

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

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 σ ja eine Darstellung von H ist, und nicht von G!

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

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

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

Nun betrachten wir uns die K-linearen Abbildungen

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

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, für alle $\eta \in \mathcal{C}_K(H),\ \gamma \in \mathcal{C}_K(G)$:

$$\frac{1}{\#G}\beta_G(\mathrm{Ind}_H^G\eta, \gamma) = \frac{1}{\#H}\beta_H(\eta, \mathrm{Res}_H^G\gamma).$$

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

Man sollte sich hier für Charaktere χ_1, χ_2 von Darstellungen ρ_1, ρ_2 einer Gruppe G überlegen, dass in Charakteristik 0 folgendes gilt:

$$\frac{1}{|G|}\beta_G(\chi_1, \chi_2) = \dim_K(\mathrm{Hom}_{K[G]}(\rho_1, \rho_2)).$$

Das passt wunderbar zur Adjungiertheit der beiden Abbildungen, denn es gilt der folgende Satz:

Satz 2.5.25 Frobenius[7]reziprozität

Wenn $H \subseteq G$ endliche Gruppen sind und K ein Körper ist, dann ist der Funktor Ind_H^G zum Funktor Res_H^G linksadjungiert.

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

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

[7]Georg Ferdinand Frobenius, 1849-1917

Diese müssen durch ein geeignetes universelles Element für den richtigen Funktor zustande kommen, z.B. für den Funktor $V \rightsquigarrow \mathrm{Hom}_{K[H]}(W, \mathrm{Res}^G_H V)$. Die gewünschte Adjungiertheit legt nahe, dass wir einen H-Morphismus von W nach $\mathrm{Res}^G_H \mathrm{Ind}^G_H W$ 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 $F : W \longrightarrow \mathrm{Ind}^G_H W$, 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

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

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

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

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:

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

Wir sind ja im induzierten Modul!

Nun definieren wir die Abbildung

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

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

Dabei ist es hilfreich wich das Folgende zuerst zu überlegen:

$$\forall f \in \mathrm{Ind}^G_H W : \ f = \sum_{i=1}^{r} g_i * F(f(g_i)).$$

Dies gilt, denn die Abbildung rechter Hand nimmt bei $x \in G$ den Wert

$$\sum_{i=1}^{r} g_i * F(f(g_i))(x) = \sum_{i=1}^{r} F(f(g_i))(g_i^{-1}x)$$

an, und dieser sieht nur den Summanden mit $g_i^{-1}x \in H$, wo der Wert von $F(f(g_i))$ gerade

$$x^{-1}g_i f(g_i) = f(g_i(x^{-1}g_i)^{-1}) = f(x)$$

ist.

Da Φ ein $K[G]$-Modulhomomorphismus mit, folgt

$$\Phi(f) = \Phi(\sum_{i=1}^{r} g_i * F(f(g_i)) = \sum_{i=1}^{r} g_i(\Phi \circ F)(f(g_i)) = M \circ \mathrm{Ind}_H^G(\Phi \circ F)(f)$$

denn $\mathrm{Ind}_H^G(\Phi \circ F)$ ist ja nur die Anwendung von $\Phi \circ F$ auf die Funktionswerte von f. Folglich ist

$$M \circ \mathrm{Ind}_H^G(\Phi \circ F) = \Phi.$$

Dass auch $M \circ \mathrm{Ind}_H^G(\Psi) \circ F = \Psi$ für alle $\Psi \in \mathrm{Hom}_{K[H]}(W, \mathrm{Res}_H^G(V))$ gilt, sieht man ähnlich ein. ◯

Bemerkung 2.5.26 Tellerrand

Der Prozess der Induktion führt manchmals 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 zahlentheoretischen Hilfssatz über Einheitswurzeln in $\mathbb{C}$.

Hilfssatz 2.5.27 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 α Betrag ≤ 1 haben. Dann ist $\alpha = 0$ oder α ist eine Einheitswurzel.

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

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

Wenn α algebraisch ganz ist, dann ist es 0 oder eine Einheitswurzel.

Beweis.

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

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

Die Koeffizienten von f sind die Ausdrücke

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

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

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

Die Potenzen α^k, $k \in \mathbb{N}_0$, erfüllen alle dieselbe Voraussetzung wie α selbst: sie sind ganz (denn die ganzen Zahlen bilden einen Ring) und alle Nullstellen ihrer Minimalplynome haben Betrag ≤ 1 (denn diese sind $\{\alpha_i^k | 1 \le i \le n\}$). Außerdem ist der Grad ihrer Minimalpolynome nicht größer als n. Demnach liegt das Minimalpolynom von α^k also in P, und es gibt nur endlich viele Möglichkeiten für die Werte von α^k. Speziell gibt es natürliche Zahlen $k < l$, sodass $\alpha^k = \alpha^l$ gilt, und die Behauptung folgt.

b) Wenn α ganz ist, dann erfüllt es alles, was in a) verlangt wird. ◯

Hilfssatz 2.5.28 Anwendung für Spuren

Es sei $\rho : G \longrightarrow \mathrm{GL}_n(\mathbb{C})$ eine irreduzible Darstellung der endlichen Gruppe G mit Charakter χ. Weiter sei $g \in G$ ein Element, C seine Konjugationsklasse in G und $\eta = \#C$. Wenn hierbei η 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 2.5.27, 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 ρ 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 λI_n, deren Spur $n\lambda$ gleich $\sum_{x \in C} \mathrm{Spur}(\rho(x)) = \eta \cdot \chi(g)$ ist. Da s als Element einer Ordnung in $\mathbb{Q}[G]$ ganz ist, muss auch $\lambda = \eta\chi(g)/n$ ganz sein. ◯

Satz 2.5.29 Ein 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 $p \not| \chi(1) = \dim(\chi)$. Anderenfalls wäre ja p^{-1} ganz algebraisch, was aber nicht stimmt.

Es sei χ so ein Charakter und ρ die zugehörige irreduzible Darstellung. Dann gilt $\chi(e_G) = \dim(\rho)$, und nach 2.5.28 folgt $\chi(g)/\chi(e_G) =: \lambda$ 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. ◯

Folgerung 2.5.30 Burnside's p^aq^b-Satz

Es seien p und q Primzahlen und G eine Gruppe, deren Ordnung gleich p^aq^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 auflösbar (sogar nilpotent) sind (siehe Algebra I; Sylowsätze und Folgerungen), dürfen wir $a, b > 0$ annehmen. Dann wählen wir im Zentrum einer q-Sylowgruppe S ein Element $s \neq e_G$. Das geht wiederum, weil S nilpotent ist.

Wenn dann s im Zentrum von G liegt, sind wir fertig (s erzeugt einen nichttrivialen Normalteiler), und ansonsten ist die Mächtigkeit der Konjugationsklasse von s eine p-Potenz > 1 und mit Satz 2.5.29 sind wir wieder fertig. ◯

2.6 Anfänge der Gruppenkohomologie

Im letzten Abschnitt dieser Vorlesung will ich ein paar Aussagen aus der Kohomologietheorie von Gruppen erläutern. Dies kann man zum Einen verstehen als

einen konkreten Anlass, um homologische Algebra zu machen, die in vielen Bereichen der modernen Mathematik eine große Rolle spielt. Zum Anderen gibt es einige Situationen, wo gerade die Kohomologiemengen oder -gruppen niedrigen Grades einer konkreten Interpretation zugänglich sind, sodass hier kohomologische Argumente auch an sich schon interessant werden.

Bemerkung 2.6.1 Soviel vorweg – H^0

a) Es sei G eine Gruppe, die auf einer anderen Gruppe Γ durch Automorphismen operiert: $\bullet : G \times \Gamma \to \Gamma$, $\forall g \in G : \Gamma \ni \gamma \mapsto g \bullet \gamma \in \Gamma$ ist ein Automorphismus von Γ.

Dann interessiert man sich natürlich für die Fixpunkte dieser Operation:

$$H^0(G, \Gamma) := \Gamma^G := \{\gamma \in \Gamma \mid \forall g \in G : g \bullet \gamma = \gamma\}.$$

H^0 ist ein Funktor von der Kategorie aller Gruppen mit G-Aktion in die Kategorie der Gruppen. Hier kann es manchmal hilfreich sein, Untergruppen und Quotienten von Γ anzusehen, auf denen G auch operiert. Konkreter:

Es sei $\Delta \subseteq \Gamma$ ein Normalteiler, der unter allen Automorphismen aus G invariant ist. Dann operiert G auch auf Γ/Δ, und wir erhalten eine kurze exakte Sequenz von Gruppen mit G-Aktion:

$$1 \to \Delta \to \Gamma \to \Gamma/\Delta \to 1.$$

Hierbei steht 1 für die triviale Gruppe.

Der Funktor H^0 ist linksexakt, die Fixpunkte von Δ bilden immer noch einen Normalteiler in den Fixpunkten von Γ und sind er Kern der Abbildung von $H^0(G, \Gamma)$ nach $H^0(G, \Gamma/\Delta)$, aber diese letzte Abbildung wird im Allgemeinen nicht mehr surjektiv sein.

b) Wir werden gleich beschreiben, wie man die mangelnde Surjektivität auffangen kann. In der allgemeinen Situation muss man aber die Kategorie der Grupen verlassen und sie durch die Kategorie der punktierten Mengen ersetzen. Das ist die Kategorie, deren Objekte Paare (M, m_0) sind, wobei M eine Menge und $m_0 \in M$ ein festes Element ist, und deren Morphismen von (M, m_0) nach (N, n_0) die Abbildungen von M nach N sind, die m_0 auf n_0 abbilden.

Eine Folge

$$(M, m_0) \to (N, n_0) \to (P, p_0)$$

heißt exakt, wenn das Urbild von p_0 unter der rechten Abbildung das Bild der linken Abbildung ist.

Es gibt einen offensichtlichen Funktor von der Kategorie der Gruppen in die Kategorie der punktierten Mengen, die eine Gruppe G auf das Paar (G, e_G) abbildet, und einen Gruppenhomomorphismus auf „sich selbst“.

In diesem Sinne fassen wir jetzt H^0 als Funktor von der Kategorie der Gruppen mit G-Aktion in die Kategorie der punktierten Mengen auf, und wollen versuchen, ihn exakt fortzusetzen.

Definition/Bemerkung 2.6.2 H^1

a) Wir gehen in die Situation von eben zurück und betrachten die Sequenz

$$1 \to H^0(G,\Delta) \to H^0(G,\Gamma) \to H^0(G,\Gamma/\Delta)$$

Was hindert den letzten Pfeil daran, surjektiv zu sein?

Es sei $\gamma\Delta$ eine G-invariante Nebenklasse, das heißt:

$$\forall g \in G : \gamma^{-1}(g \bullet \gamma) \in \Delta.$$

Dies liefert eine Abbildung

$$\kappa : G \to \Delta, \kappa(g) := \gamma^{-1}(g \bullet \gamma).$$

Diese Abbildung misst, wie weit γ davon entfernt ist, G-invariant zu sein. G-Invarianz bedeutet einfach, dass κ konstant den Wert e annimmt.

b) Die Abbildung κ hat eine interessante Funktionalgleichung:

$$\forall g,h \in G : \kappa(gh) = \gamma^{-1}((gh) \bullet \gamma) = \kappa(g)(g \bullet \kappa(h)).$$

Wir definieren die Menge der 1-Kozykel von G mit Werten in Δ als

$$Z^1(G,\Delta) := \{k : G \to \Delta \mid \ \forall g,h \in G : f(gh) = f(g)(g \bullet f(h))\}.$$

Diese Definition nimmt keinen Bezug mehr auf unsere exakte Sequenz und ist für jede Gruppe Δ mit G-Aktion sinnvoll. Für $g = h = e_G$ folgt übrigen $f(e_G) = f(e_G)f(e_G)$, also $f(e_G) = e_\Delta$.

c) Allerdings gibt es keine naheliegende Abbildung von $H^0(G,\Gamma/\Delta)$ nach $Z^1(G,\Delta)$, denn wir haben schließlich den 1-Kozykel κ durch die Wahl eines Vertreters γ der invarianten Klasse gewonnen.

Was passiert bei Wahl eines anderen Vertreters? Dann wird γ durch ein Element $\gamma\delta$ ersetzt mit $\delta \in \Delta$. Der Kozykel ändert sich dabei ab zu

$$\tilde{\kappa}(g) := (\gamma\delta)^{-1}(g \bullet (\gamma\delta)) = \delta^{-1}\kappa(g)(g \bullet \delta).$$

Dies führt uns zur Definition einer Äquivalenzrelation auf $Z^1(G,\Delta)$. Wir nennen zwei 1-Kozykel $\kappa, \tilde{\kappa}$ äquivalent, wenn ein $\delta \in \Delta$ existiert mit

$$\forall g \in G : \tilde{\kappa}(g) = \delta^{-1}\kappa(g)(g \bullet \delta).$$

Die Menge all dieser Äquivalenzklassen nennen wir die *erste Kohomologiemenge* von G mit Koeffizienten in Δ. Sie wird punktiert durch Wahl der Klasse des trivialen (d.h. konstanten) Kozykels als ausgezeichneten Punkt.

d) Nun erhalten wir eine wohldefinierte Abbildung von $H^0(G, \Gamma/\Delta)$ nach $H^1(G, \Delta)$ durch $\gamma\Delta \mapsto [\kappa]$, wobei κ der oben konstruierte 1-Kozykel ist. Wir nennen diese Abbidung δ. Sie heißt die *Randabbildung*. Sie bildet das Einselement in Γ/Δ auf die Klasse des trivialen Kozykels ab, ist also eine Abbildung in der Kategorie der punktierten Mengen.

Die Sequenz $H^0(G, \Gamma) \to H^0(G, \Gamma/\Delta) \to H^1(G, \Delta)$ ist exakt. Denn: Der Kozykel κ, der zu $\gamma\Delta \in H^0(G, \Gamma/\Delta)$ gehört, ist genau dann äquivalent zum trivialen Kozykel, wenn ein $\delta \in \Delta$ existiert, für das $\gamma\delta$ unter G-invariant ist.

e) Wir können nun noch einen Schritt weitergehen, denn $H^1(G, -)$ ist ein Funktor von der Kategorie der Gruppen mit G-Aktion in die Kategorie der punktierten Mengen. Ist nämlich

$$\Phi : \Gamma \to \tilde{\Gamma}$$

ein G-äquivarianter Gruppenhomomorphismus, so definiert

$$[\kappa] \mapsto [\Phi \circ \kappa]$$

einen Morphismus von $H^1(G, \Gamma)$ nach $H^1(G, \tilde{\Gamma})$ (jeweils mit der Klasse des trivialen Kozykels punktiert).

Man kann leicht verifizieren, dass die Sequenz

$$\begin{aligned} 1 \quad &\to H^0(G, \Delta) \to H^0(G, \Gamma) \to H^0(G, \Gamma/\Delta) \\ &\to H^1(G, \Delta) \to H^1(G, \Gamma) \to H^1(G, \Gamma/\Delta) \end{aligned}$$

an jeder Stelle exakt ist. (Für die Pfeile zwischen den H^1en haben wir das noch nicht verifiziert – tun Sie das!)

Beispiel 2.6.3 und eine Rechenregel

a) Für jeden 1-Kozykel κ auf G mit Werten in Γ und jedes $g \in G$ gilt $\kappa(g^2) = \kappa(g)(g \bullet \kappa(g))$, und induktiv sieht man

$$\kappa(g^r) = \kappa(g)(g \bullet \kappa(g))(g^2 \bullet \kappa(g)) \dots g^{r-1} \bullet \kappa(g)).$$

Wenn insbesondere g Ordnung r hat, muss dieses Element – wie oben gesehen – e_Γ sein.

Ähnlich sieht man auch ein, dass wegen

$$\kappa(e) = \kappa(gg^{-1}) = \kappa(g)(g \bullet \kappa(g^{-1}))$$

die Gleichung

$$\kappa(g^{-1}) = (g^{-1} \bullet \kappa(g))^{-1}$$

gilt.

b) Wenn speziell die Operation von G auf Γ trivial ist, dann ist $Z^1(G,\Gamma) = \mathrm{Hom}_{\mathrm{Grupen}}(G,\Gamma)$, und $H^1(G,\Gamma)$ besteht aus den Γ-Konjugationsklassen aller Homomorphismen von G nach Γ.

c) Nun sei $\Gamma = \mathrm{GL}_n(K)$ für einen Körper K und $G = \{1,\sigma\}$ die Gruppe mit 2 Elementen. G operiert auf Γ durch

$$\sigma(A) := (A^\top)^{-1}.$$

Die G-invarianten in Γ sind gerade die Matrizen A mit $AA^\top = I_n$, also $H^0(G,\Gamma) = \mathrm{O}_n(K)$, die orthogonale Gruppe.

In Γ liegt die normale Gruppe $\Delta := \mathrm{SL}_n(K)$, die unter der G-Aktion invariant ist. Die Faktorgruppe ist $\Gamma/\Delta = K^\times$, wobei die Identifikation über die Determinante passiert. Die Aktion von G auf $K^\times$ besteht darin, dass $\sigma \bullet x = x^{-1}$.

Leider ist die zugehörige Sequenz auf den G-invarianten schon exakt:

$$1 \to \mathrm{SO}_n(K) \to \mathrm{O}_n(K) \to \{\pm 1\} \to 1,$$

aber trotzdem kann man ja einmal Kozykel ausrechenen, nicht wahr?

$Z^1(G,\Gamma) \ni \kappa \mapsto \kappa(\sigma) \in \Gamma$ ist eine injektive Abbildung, deren Bild gerade die Matrizen $A \in \Gamma$ sind, für die $A \cdot \sigma \bullet A = 1$ gilt, also

$$A = A^\top.$$

Das Bild besteht also aus den regulären symmetrischen Matrizen.

Die Äquivalenzrelation, der Klassen dann die Kohomologiemenge ist, wird hier gegeben durch

$$A \sim \tilde{A} \iff \exists B \in \Gamma : \ \tilde{A} = BAB^\top,$$

und das beschreibt gerade Basiswechsel für symmetrische Bilinearformen.

Auf $K^\times$ ist die Kohomologiemenge wegen der Kommutativität einfach die Gruppe der Quadrateklassen

$$K^\times/\{x^2 \mid x \in K^\times\}.$$

Genau die symmetrischen Matrizen, deren Determinante ein Quadrat ist, lassen sich hier durch symmetrische Matrizen mit Determinante 1 ersetzen. Es ist also hier auch die Sequenz der H^1-Mengen exakt:

$$1 \to H^1(G,\Delta) \to H^1(G,\Gamma) \to H^1(G,K^\times) \to 1.$$

Dass dies nicht der Normalfall ist, werden wir noch sehen.

Beispiel 2.6.4 $G = \mathbb{Z}$ **und eine geometrische Bemerkung**

a) Es ist klar, dass ein 1-Kozykel auf G durch seine Werte bei den Erzeugern gegeben wird.

Auf einer Gruppe Γ wird eine $\mathbb{Z}$-Aktion durch Vorgabe eines Automorphismus σ vorgeschrieben und dann $k \bullet \gamma := \sigma^k(\gamma)$ gesetzt. Die Abbildung

$$Z^1(\mathbb{Z}, \Gamma) \to \Gamma, \ \kappa \mapsto \kappa(1)$$

ist injektiv und – wie man sich leicht überlegt – auch surjektiv. Zwei Elemente $\gamma, \tilde{\gamma}$ liefern als Funktionswerte beim Erzeuger 1 denselben Kozykel genau dann, wenn ein $\beta \in \Gamma$ existiert, sodass

$$\tilde{\gamma} = \beta^{-1}\gamma\sigma(\beta).$$

Nun sei speziell $\Gamma = \mathbb{Z}^2$ und $\sigma(\binom{a}{b}) := \binom{a+b}{b}$. Die Abbildungsmatrix dieses Automorphismus ist also ein Jordankästchen der Länge 2 zum Eigenwert 1.

In Γ liegt die σ-invariante Untergruppe $\Delta := \mathbb{Z}\binom{1}{0}$, das ist der Eigenraum zum Eigenwert 1, und damit ist das gleich $H^0(\mathbb{Z}, \Gamma)$. Die Faktorgruppe ist ebenfalls freiabelsch vom Rang eins mit trivialer $\mathbb{Z}$-Aktion. Folglich ist die letzte Abbildung der exakten Sequenz

$$0 \to H^0(\mathbb{Z}, \Delta) \to H^0(\mathbb{Z}, \Gamma) \to H^0(\mathbb{Z}, \Gamma/\Delta)$$

in diesem Beispiel nicht surjektiv, und wir erhalten eine nichttriviale Randabbildung δ nach $H^1(\mathbb{Z}, \Delta)$.

Da andererseits ein Kozykel beim Erzeuger 1 der freien Gruppe $\mathbb{Z}$ jeden Wert annehmen darf und hierdurch eindeutig festgelegt ist, ist zwangsläufig die Abbildung $H^1(\mathbb{Z}, \Gamma) \to H^1(\mathbb{Z}, \Gamma/\Delta)$ surjektiv, und zwar sogar für alle Paare Δ, Γ.

b) Wir werden im Fall von abelschen Koeffizientengruppen Γ in Kürze auch noch höhere Kohomologiegruppen einführen und eine lange exakte Kohomologiesequenz angeben.

Da $\mathbb{Z}$ auf einem wunderschönen topologischen Raum (nämlich $\mathbb{R}$) wunderbar (nämlich eigentlich diskontinuierlich und fixpunktfrei) operiert (nämlich durch Translationen), sagt ein wunderschöner Satz von Grothendieck, dass sich die Kohomologie von $\mathbb{Z}$ mit Werten in einem $\mathbb{Z}[\mathbb{Z}]$-Modul Γ immer identifizieren lässt mit der Kohomologie einer Garbe auf $\mathbb{R}/\mathbb{Z}$, die sich aus Γ konstruieren lässt. Da aber $\mathbb{R}$ Dimension eins hat, sagen weitere Sätze aus der (topologischen) Kohomologietheorie der Garben, dass die höheren Kohomologiegruppen trivial sind. Das entspricht in gewisser Weise der Tatsache, dass man sie nicht braucht, um die obige Sequenz exakt fortzusetzen.

Manachmal ist es tatsächlich hilfreich zu wissen, dass eine Kohomologiemenge trivial ist. Wir werden gleich arithmetische Konsequenzen aus dem folgenden Faktum ziehen:

Proposition 2.6.5 Galoiserweiterungen

Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G. Dann operiert G natürlich auf den abelschen Gruppen $(L,+)$ und $(L^\times,\cdot)$.

In beiden Fällen ist die erste Kohomologiemenge trivial.

Beweis. Wenn wir die Automorphismen von L auf $L^\times$ einschränken, so erhalten wir eindimensionale Charaktere von $L^\times$, und die sind linear unabhängig über L (das war Hilfssatz 4.4.18 in der letzten Algebra I). Wir werden dieses Lemma jetzt für den Beweis beider Aussagen benutzen.

Es sei $\kappa : G \to L$ ein additiver 1-Kozykel, d.h.

$$\forall g,h \in G : \kappa(gh) = \kappa(g) + g(\kappa(h)).$$

Da die Automorphismen über L linear unabhängig sind, ist $\sum_{g\in G} g$ nicht die Nullabbildung, es gibt also ein $\ell \in L$, sodass

$$\mathrm{Tr}(\ell) = \sum_{g\in G} g(\ell) \neq 0.$$

(Dass das die Spur von ℓ ist, sei hier nur am Rande erähnt.)

Wir setzen dann

$$b := \mathrm{Tr}(\ell)^{-1} \sum_{g\in G} \kappa(g)g(\ell).$$

Das ergibt für $h \in G$ die Gleichung

$$h(b) = \mathrm{Tr}(\ell)^{-1} \sum_g h(\kappa(g))\cdot(hg)(\ell) = \mathrm{Tr}(\ell)^{-1} \sum_g [\kappa(hg)-\kappa(h)]\cdot(hg)(\ell) = b-\kappa(h),$$

also

$$-b + \kappa(h) + h(b) = 0.$$

Damit ist κ äquivalent zum konstanten Kozykel, was $H^1(G,L) = \{[0]\}$ zeigt.

Nun betrachten wir die multiplikative Situation. Also sei jetzt $\kappa : G \to L^\times$ ein multiplikativer 1-Kozykel, d.h.

$$\forall g,h \in G : \kappa(gh) = \kappa(g) \cdot g(\kappa(h)).$$

Wieder wegen der linearen Unabhängigkeit der $g \in G$ gibt es ein $\ell \in L$, sodass

$$B := \sum_{g\in G} \kappa(g)g(\ell) \neq 0.$$

Wieder rechnen wir nach, dass für $h \in G$ wegen der Kozykelrelation

$$h(B) = \sum_g \kappa(g)^{-1}\kappa(hg)hg(\ell) = \kappa(h)^{-1}B,$$

also

$$B^{-1}\kappa(h)h(B) = 1.$$

Damit ist auch dieser multiplikative Kozykel trivial und $H^1(G, L^\times) = \{[1]\}$. ◯

Bemerkung 2.6.6 Hilberts Satz 90

a) Der folgende Spezialfall der letzten Proposition ist das, was man oft Hilberts Satz 90 nennt. Das war die Numerierung in Hilberts Zahlbericht, der Ende des 19. Jhdts. den damaligen Stand der Zahlentheorie dokumentierte.

Dazu sei $G = \mathrm{Gal}(L|K)$ zyklisch. Wir benutzen jetzt doch die obige Erwähnung am Rande, um die Werte von 1-Kozykeln $\kappa \in Z^1(G, L)$ beim Erzeuger σ von G zu spezifizieren. Die Ordnung von σ sei d. Dann folgt aus $\kappa(\sigma) = x \in L$, dass $(1 + \sigma + \sigma^2 + \cdots + \sigma^{d-1})(x) = 0$. Da hier über alle Elemente von G summiert wird, sind die Werte von Kozykeln bei σ genau die Elemente aus L mit Spur 0. Da die Kohomologie trivial ist, sind das genau die Elemente aus L von der Gestalt $z - \sigma(z),\ z \in L$.

Die multiplikative Version sagt analog, dass die Einheiten in L mit Norm 1 genau die Elemente der Gestalt $z/\sigma(z)$ sind.

b) Die Aussage aus der letzten Proposition gilt hier immer noch, wenn man $L^\times$ durch $\mathrm{GL}_n(L)$ ersetzt. Auch der Beweis bleibt im Wesentlichen derselbe, wobei man etwas mehr aufpassen muss, da man nicht nur eine Matrix $B := \sum_{g\in G} \kappa(g)g(A) \neq 0$ konstruieren muss, die nicht 0 ist, sondern B muss invertierbar sein. Das geht aber auch, und zwar mit folgendem Argument:

Es sei $\kappa \in Z^1(G, \mathrm{GL}_n(L))$ ein 1-Kozykel. Dann ist für jedes $v \in L^n$ auch

$$s(v) := \sum_{g\in G} \kappa(g) \cdot g(v) \in L^n.$$

Wenn nun $\lambda : L^n \to L$ eine Linearform ist, die auf allen $s(v)$ den Wert 0 annimmt, so folgt für alle $l \in L, v \in L^n$:

$$0 = \lambda(s(lv)) = \sum_{g\in G} \lambda(\kappa(g)g(v)) \cdot \lambda(l),$$

aber hier sind die Faktoren $\lambda(\kappa(g)g(v))$ von l unabhängig, und aus der linearen Unabhängigkeit der $g \in G$ folgt, dass all diese Faktoren 0 sind. Da aber $\kappa(g)$ immer invertierbar ist, ist λ gleich 0, und daher ist

$$L^n = \{s(v) \mid v \in \mathbb{L}^n\}.$$

Insbesondere gibt es $v_1, \ldots, v_n$, sodass $s(v_1), \ldots, s(v_n)$ linear unabhängig sind, und daher tut die Matrix $A = (v_1 \ \ldots \ v_n)$ das, was wir uns eben gewünscht haben.

Folgerung 2.6.7 Darstellungstheorie

Es sei K ein perfekter Körper und L ein endlicher Erweiterungskörper. Weiter seien

$$\pi_i : H \to \mathrm{GL}_n(K),\ i = 1, 2,$$

zwei K-lineare Darstellungen einer endlichen Gruppe H, deren Ordnung in K invertierbar ist.

Wenn dann eine Matrix $S \in \mathrm{GL}_n(L)$ existiert, für die

$$\forall h \in H : \pi_2(h) = S\pi_1(h)S^{-1}$$

gilt, dann gibt es so eine Matrix auch schon mit Einträgen in K.

Beweis. Wir zerlegen über dem algebraischen Abschluss $\overline{L}$ von L die Darstellung π_1 als direkte Summe von irreduziblen Darstellungen:

$$\pi_1 = \rho_1^{m_1} \oplus \cdots \oplus \rho_k^{m_k},$$

wobei $\rho_1, \ldots, \rho_k$ paarweise verschiedene irreduzible Darstellungen sind und ρ_j mit Vielfachheit m_j in π_1 auftritt.

Der Endomorphismenring von $\pi_1 \otimes_K \mathrm{Id}_{\overline{L}}$ (als $\overline{L}$-lineare Darstellung von G) ist dann wegen des Lemmas von Schur isomorph zu

$$\bigoplus_{j=1}^{k} \overline{L}^{m_j \times m_j}.$$

Wir wählen so einen Isomorphismus Φ.

Wenn $b_1, \ldots, b_N$ eine Basis von $\mathrm{End}_{K[H]}(\pi_1)$ ist, dann wird $\oplus_{j=1}^{k} \overline{L}^{m_j \times m_j}$ über $\overline{L}$ von $\Phi(b_1), \ldots, \Phi(b_N)$ erzeugt.

Es sei $M \subseteq \overline{L}$ die kleinste Galoiserweiterung von K, die L und alle Einträge dieser Matrizen umfasst. Da es nur endlich viele Matrizen sind, ist das eine endliche Galoiserweiterung von K.

Es sei $G = \mathrm{Gal}(M \mid K)$. Dann gilt für alle $g \in G$ und alle $h \in H$

$$g(S\pi_1(h)S^{-1}) = g(\pi_2(h)) = \pi_2(h) = S\pi_1(h)S^{-1},$$

also ist für alle $g \in G$ die Multiplikation mit

$$S^{-1}g(S)$$

ein Automorphismus von π_1 über M, da $\pi_1(h)$ ja unter g fix ist.

Es ist nun klar, dass die Abbildung

$$G \ni g \mapsto S^{-1}g(S) \in \mathrm{Aut}_{M[H]}(\pi_1 \otimes_K \mathrm{Id}_M) = \prod_{j=1}^{k} \mathrm{GL}_{m_j}(M)$$

ein 1-Kozykel ist.

Da dieser 1-Kozykel trivial ist, gibt es ein $T \in \mathrm{Aut}_{M[H]}(\pi_1 \otimes_K \mathrm{Id}_M)$, sodass

$$\forall g \in G : S^{-1}g(S) = T^{-1}g(T),$$

oder auch

$$\forall g \in G : TS^{-1} = g(TS^{-1}).$$

Andererseits ist TS^{-1} ein über M definierter Verkettungsoperator von π_2 nach π_1 und damit durch eine Matrix in $\mathrm{GL}_n(M)$ darstellbar. Diese ist dann zwangsläufig invariant unter G und hat damit alle Einträge im Fixkörper von G, also in K. Ihr inverses ist „die“ gesuchte Matrix. ◯

Bemerkung 2.6.8 Ein Nachtrag

In 2.5.14 hatten wir von der natürlichen Abbildung zwischen Darstellungsringen einer Gruppe über zwei Körpern gesprochen, und können jetzt einen Nachtrag zur Injektivität dort machen. Tatsächlich leistet unsere Folgerung eben genau das: Wenn zwei Darstellungen über dem algebraischen Abschluss isomorph werden, waren sie das vorher schon, zumindest wenn der Ausgangskörper perfekt ist (also keine inseparable Erweiterung hat) und die Ordnung der Gruppe kein Vielfaches der Charakteristik. In Charakteristik 0 sind wir also auf der sicheren Seite.

Definition/Bemerkung 2.6.9 abelsche Koeffizienten und H^2

a) Ab jetzt seien die Gruppen $\Gamma, \Delta, \ldots$ abelsch, also $\mathbb{Z}$-Moduln. Wir gehen sogar einen kleinen Schritt weiter und betrachten Moduln über einem Ring R, auf denen die Gruppe G über R-lineare Automorphismen operiert, also $R[G]$-Moduln. Es sei M so ein Modul.

Dann ist $H^0(G, M)$ ein R-Untermodul von M, und auch $Z^1(G, M)$ ist ein R-Modul, nämlich ein R-Untermodul von $\mathrm{Abb}(G, M)$.

Die Abbildung

$$M \ni m \mapsto [g \mapsto m - gm] \in \mathrm{Abb}(G, M)$$

ist R-linear, und ihr Bild ist gerade $B^1(G, M)$, das damit zu einem Untermodul von $Z^1(G, M)$ wird.

Das liefert auf $H^1(G, M) = Z^1(G, M)/B^1(G, M)$ eine R-Modulstruktur.

Alle natürlichen Abbildungen einschließlich der Randabbildung d in der exakten Kohomologiesequenz sind R-linear, wie man leicht nachrechnet.

b) Nun seien $N \subseteq M$ zwei $R[G]$-Moduln und

$$0 \to N \to M \to M/N \to 0$$

die zugehörige kurze exakte Sequenz.

Dann gibt es eine Kohomologiesequenz dazu, die nach unserem Kenntnisstand bei

$$\to H^1(G, M) \to H^1(G, M/N)$$

aufhört. Wenn $\pi : M \to M/N$ die natürliche Projektion ist, dann ist diese letzte Abbildung $H^1(G, \pi)$ und wird auf der Klasse $[\kappa]$ des Kozykels $\kappa \in Z^1(G, M)$ durch

$$H^1(G, \pi)([\kappa]) = [\pi \circ \kappa]$$

gegeben.

Wieso ist diese Abbildung nicht surjektiv?

Wir machen unseren alten Trick einfach ein zweites Mal:

Es sei also $\kappa \in Z^1(G, M/N)$ ein Kozykel. Dann gibt es eine Abbildung $f : G \to M$, sodass für alle $g \in G$:

$$\kappa(g) = f(g) + N.$$

Wir müssen wieder danach fragen, was f davon abhält, ein Kozykel mit Werte in M zu sein. Dazu müsste ja für alle $g, h \in G$ die Gleichung

$$f(gh) - f(g) - g \bullet f(h) = 0$$

gelten. Als Kongruenz modulo N gilt diese auf jeden Fall, denn modulo N **ist** f ja ein Kozykel. Wir erhalten daher eine Abbildung

$$\varphi : G \times G \to N, \quad \varphi(g, h) := f(gh) - f(g) - g \bullet f(h).$$

Diese Abbildung hat die interessante Eigenschaft, dass für alle $g, h, k \in G$ die folgende Bedingung gilt:

$$\varphi(g, h) + \varphi(gh, k) = g \bullet \varphi(h, k) + \varphi(g, hk).$$

Dies ist wieder eine Bedingung, die man an Abbildungen von $G \times G$ nach N stellen kann, ohne die Herkunft unseres φ vorauszusetzen. Wir nennen den R-Modul

$$\begin{aligned} Z^2(G, N) := \{ \quad & \psi : G \times G \to N \mid \forall g, h, k \in G : \\ & \psi(g, h) + \psi(gh, k) = g \bullet \psi(h, k) + \psi(g, hk)\} \end{aligned}$$

die Menge der *2-Kozykel* von G mit Koeffizienten in N. Ein 2-Kozykel wird gelegentlich auch eine *Faktormenge* (siehe 2.6.11) genannt.

Wenn wir oben anstelle unsere Abbildung f andere Abbidung $\tilde{f}$ wählen, dann gibt es eine Abbildung $r : G \to N$, sodass

$$\tilde{f} = f + r.$$

Das heißt für die zu f und $\tilde{f}$ gehörigen Kozykel, dass

$$(\tilde{\varphi} - \varphi)(g, h) = r(gh) - r(g) - g \bullet r(h).$$

Dies motiviert die Einführung von

$$B^2(G, N) := \{\beta : G \times G \to N \mid \exists r : G \to N : \ \beta(g, h) = r(gh) - r(g) - g \bullet r(h)\}.$$

Dies ist der R-Modul der *2-Koränder* von G mit Koeffizienten in N. Er ist immer ein Untermodul von $Z^2(G, N)$.

Nun sollte es nicht mehr überraschen, dass der R-Modul

$$H^2(G, N) := Z^2(G, N)/B^2(G, N)$$

die *zweite Kohomologie von G mit Werten in N* heißt.

Bemerkung 2.6.10 Verlängerung

Wir gehen in unsere alte Ausgangssituation zurück, zur kurzen exakten Sequenz

$$0 \to N \to M \to M/N \to 0$$

von $R[G]$-Moduln.

Wir waren bei

$$\to H^1(G, M) \to H^1(G, M/N)$$

stehengeblieben und haben jetzt aber ein Möglichkeit gefunden, dies durch eine Abbildung

$$d^1 : H^1(G, M/N) \to H^2(N)$$

fortzusetzen. Diese ist durch

$$d^1(\kappa + B^1(G, M/N))) := \varphi + B^2(G, N)$$

gegeben, was nach Konstruktion von φ und $B^2(G, N)$ wohldefiniert ist.

κ liegt genau dann im Kern von d^1, wenn es Bild eines $1-Kozykels$ mit Werten in M ist.

Außerdem ist $H^2(G, -)$ ein Funktor von der Kategorie der $R[G]$-Moduln in die Kategorie der R-Moduln, indem wir einem Morphismus $\Phi : M_1 \to M_2$ die Abbildung

$$H^2(G, \Phi) : H^2(G, M_1) \to H^2(G, M_2), \ \varphi + B^2(G, M_1) \mapsto \Phi \circ \varphi + B^2(G, M_2)$$

zuordnen.

Dann wird die Sequenz

$$\begin{aligned} 0 \quad &\to H^0(G,N) \to H^0(G,M) \to H^0(G,M/N) \\ &\to H^1(G,N) \to H^1(G,M) \to H^1(G,M/N) \\ &\to H^2(G,N) \to H^2(G,M) \to H^2(G,M/N) \end{aligned}$$

eine noch längere exakte Sequenz von R-Moduln, wie man nachprüfen kann.

Beispiel 2.6.11 Sitz im Leben I: Quaternionenalgebren

a) Es sei F ein Körper, dessen Charakteristik nicht 2 ist, und $a, b \in F^\times$ fest gewählte Elemente. Spätestens in 2.3.9 haben wir dazu die Quaternionenalgebra $\left(\frac{a,b}{F}\right)$ kennen gelernt. Sie ist eine vierdimensionale F-Algebra A mit Basis $1, I, J, K,$ und die Multiplikation ist so gemacht, dass

$$I^2 = a, J^2 = b, IJ = -JI = K.$$

Es sei a kein Quadrat in $F^\times$. Dann ist $E := F(\sqrt{a})$ eine quadratische Erweiterung von F, die wir als Teilalgebra von A denken dürfen: $E \cong F + FI \subseteq A$. Die Konjugation mit der Einheit J lässt E invariant und liefert hier den nichttrivialen Automorphismus von E über F, denn $JIJ^{-1} = -I$.

Es sei $G = \mathrm{Gal}(E \mid F)$ und $\sigma \in G$ der Erzeuger. Weiter sei

$$F : \mathrm{Abb}(G, E) \to A$$

die Abbildung

$$x\delta_1 + y\delta_\sigma \mapsto x + yJ.$$

Dann ist die Abbildung

$$\varphi : G \times G \to E^\times, \varphi(g,h) := F(\delta_g)(F(\delta_h))F(\delta_{gh})^{-1},$$

ein 2-Kozykel von G mit Werten in $E^\times$.

Er diktiert letztlich die Multiplikation in A, wenn man sie zur linken Seite zurücktransportiert und diese damit zu einer neuen F-Algebra macht.

Genau dann, wenn er ein Korand ist, ist A isomorph zum Matrizenring $F^{2\times 2}$.

b) Allgemeiner sei $F \subseteq E$ eine endliche Galoiserweiterung mit Gruppe G und $\varphi \in Z^2(G, E^\times)$. Dann wird $A := \mathrm{Abb}(G, E)$ zu einer F-Algebra, wenn wir zwei Elemente $\sum x_g\delta_g, \sum y_g\delta_g$ durch die Formel

$$(\sum x_g\delta_g) \cdot (\sum y_h\delta_h) := \sum_{g,h} x_g g(y_h)\varphi(g,h)\delta_{gh}$$

multiplizieren. Wohlgemerkt ist E nicht im Zentrum dieses Rings, das Zentrum ist F. Die 2-Kozykelbedingung ist hierbei für die Assoziativität verantwortlich.

Zwei Kozykel liefern genau dann isomorphe F-Algebren, wenn sie sich um einen Korand unterscheiden. Es steht also $H^2(G, E^\times)$ in Bijektion zu einer Menge von F-Algebren. Diese kann man übrigens auch anders charakterisieren: es sind zentral einfache F-Algebren (d.h. das Zentrum ist F und es gibt keine interessanten zweiseitigen Ideale), die nach Tensorieren mit E zum Matrizenring $M_n(E)$ isomorph sind. Dabei ist $n = [E : F]$.

Dieser Sachverhalt, der von Emmy Noether und ihren Mitarbeitern systematisch untersucht wurde, ist für die Namensgebung *Faktormengen* verantwortlich.

Ein Stichwort im näheren Umkreis ist die *Brauergruppe.*

c) Das Ganze passt übrigens wunderbar zu 2.6.7 oder jedenfalls zu Argumenten in diesem Umkreis. Wenn $F \subseteq E$ eine Galoiserweiterung mit Gruppe G ist und A_0 eine endlichdimensionale Algebra über F, dann möchte man manchmal wissen, welche nicht zu A isomorphen Algebren es gibt, die nach Tensorieren mit E isomorphe E-Algebren liefern.

Wenn B eine weitere Algebra ist und $A_0 \otimes_F E \cong A \otimes_F E$ gilt, dann wählt man einen Isomorphismus $\Phi : A_0 \otimes_F E \to A \otimes_F E$ und erhält durch

$$\kappa : G \ni g \; mapsto \Phi^{-1} g(\Phi) \in \mathrm{Aut}_{E-\mathrm{Alg}}(A_0 \otimes_F E)$$

einen 1-Kozykel. Die Kohomologieklasse diese 1-Kozykels charakterisiert A in Relation zu A_0.

Im Beispiel der Quaternionenalgebra A sei $A_0 = M_2(F)$ der Matrizenring. Nach einem Satz von Skolem und Noether ist jeder Automorphismus von $A_0 \otimes_F E = M_2(E)$ ein innerer Automorphismus, also die Konjugation mit einem Element aus $\mathrm{GL}_2(E)$. Da hierbei das Zentrum $E^\times$ trivial operiert, ist die Automorphismengruppe präziser $\mathrm{PGL}_2(E) = \mathrm{GL}_2(E)/E^\times$.

Diese Gruppen sitzen in einer kurzen exakten Sequenz

$$1 \to E^\times \to \mathrm{GL}_2(E) \to \mathrm{PGL}_2(E) \to 1$$

von Gruppen mit G-Aktion und die zugehörige etwas längere Sequenz in der Kohomologie enthält einen exakten Teil

$$H^1(G, \mathrm{GL}_2(E)) \to H^1(G, \mathrm{PGL}_2(E)) \to H^2(G, E^\times)$$

Da jedoch nach Hilberts Satz 90 der erste Term hier trivial ist, erhalten wir eine Einbettung von $H^1(G, \mathrm{PGL}_2(E))$ nach $H^2(G, E^\times)$. Das erste ist unser Auffangbecken für die Kohomologieklassen, die von Kandidaten für A herkommen, das zweite ist unser System von Faktormengen aus a) bzw. b). Die Inklusion erweist sich als Bijektion, die noch dazu mit den zwei Konstruktionsverfahren von Algebren harmoniert.

Beispiel 2.6.12 Sitz im Leben II: Gruppenerweiterungen

a) Eine weitere Herkunft von 2-Kozykeln kommt von folgender Situation her:

Es seien G, N zwei Gruppen. Eine Erweiterung von N um G ist eine kurze exakte Sequenz

$$1 \to N \xrightarrow{\alpha} E \xrightarrow{\pi} G \to 1$$

von Gruppen, also eine Gruppe E, die G als Normalteiler enthält sodass der $E/N \cong G$.

Zwei solche Erweiterungen $E, \tilde{E}$ heißen äquivalent, wenn es einen Isomorphismus von E nach $\tilde{E}$ gibt, der auf N und G die Identität induziert.

Man kann 2-Kozykel zur Klassifikation der Erweiterungsklassen benutzen, wenn N abelsch ist. Dann ist es ja so, dass N im Kern der Operation von E auf N durch Konjugation liegt, dass also jede Erweiterungsklasse eine wohldefinierte Operation von G auf N liefert.

Es sei weiter $s : G \to E$ eine Abbildung, sodass $\pi \circ s = \mathrm{Id}_G$. Die Aktion von G auf N ist dann gegeben durch

$$g \bullet n := s(g) n s(g)^{-1}.$$

Weiter gilt

$$G = \{\alpha(n)s(g) \mid n \in N,\ g \in G\},$$

und die Zerlegung der Elemente von G in solche Faktoren ist eindeutig. Allerdings ist s in aller Regel kein Gruppenhomomorphismus. Was hindert s daran, einer zu werden?

Für $n_1, n_2 \in N$ und $g_1, g_2 \in G$ gilt

$$\alpha(n_1)s(g_1)\alpha(n_2)s(g_2) = \alpha(n_1)s(g_1)\alpha(n_2)s(g_1)^{-1}s(g_1)s(g_2),$$

und das wird von π auf $g_1 g_2$ projiziert. Daher liegt

$$\phi(g_1, g_2) := s(g_1 g_2)^{-1} s(g_1) s(g_2)$$

in N (oder präziser in $\alpha(N)$). Man rechnet nach, dass ϕ ein 2-Kozykel von G mit Werten in N ist (bezüglich der gegebenen Aktion!). Die Assoziativität der Multiplikation in E entspricht wieder der 2-Kozykelrelation.

Übergang zu anderen Wahlen von s oder zu äquivalenten Erweiterungen liefert dieselbe Kohomologieklasse, und es zeigt sich, dass man sogar eine Bijektion erhält zwischen der Menge der Äquivalenzklassen der Erweiterungen von N um G bei fest vorgegebener Aktion un der Menge $H^2(G, N)$. Der Spezialfall des trivialen Kozykels entspricht dem semidirekten Produkt oder eben der Situation, dass s als Homomorphismus gewählt werden kann.

Wenn man alle Erweiterungen von N um G kennen will, muss man das für alle möglichen Operationen von G auf der abelschen Gruppe N durchführen.

b) Ein konkretes Beispiel. Wenn $N = G = C_p := \mathbb{Z}/pZ$ ist, dann gibt es nur einen Homomorphismus von G nach $\mathrm{Aut}(N) = \mathbb{F}_p^\times$, denn diese Gruppen haben teilerfremde Ordnung. Wir müssen also nur Kozykel bezüglich der trivialen Aktion betrachten, um alle Gruppen der Ordnung p^2 zu finden, oder präziser: alle Erweiterungsklassen von N um G.

Man sieht sehr schnell, dass es mindestens 2 Erweiterungsklassen gibt, nämlich $E = C_p \times C_p$ und $E = C_{p^2} := \mathbb{Z}/p^2\mathbb{Z}$. Aber Vorsicht: Zu einer Erweiterungsklasse gehören ja auch noch die Einbettung von N und die Projektion nach G als Daten dazu.

Im Fall $E = C_p \times C_p$ sind je zwei Erweiterungsklassen äquivalent, was letztlich die lineare Algebra sagt.

Im anderen Fall gibt es $p - 1$ inäquivalente Erweiterungsklassen, sodass man insgesamt p Klassen erhält, die wunderbar in einen $\mathbb{F}_p$-Vektorraum passen, was $H^2(C_p, C_p)$ ja sein muss.

Ein Beispiel für einen 2-Korand kommt von der Sequenz

$$0 \to C_p \xrightarrow{\alpha} C_{p^2} \xrightarrow{\beta} C_p \to 0$$

her, wobei

$$\alpha(a + p\mathbb{Z}) := pa + p^2\mathbb{Z},\ \beta(b + p^2\mathbb{Z}) := b + p\mathbb{Z}.$$

Als s können wir hier

$$s(b + p\mathbb{Z}) := b + p^2\mathbb{Z}\ \ (0 \le b \le p - 1)$$

wählen, wobei wir uns auf Repräsentanten festlegen müssen – es gibt nun einmal keine natürliche Abbildung von C_p nach C_{p2}, die die kanonische Projektion spaltet.

Mit dieser Wahl von s berechnet sich κ zu

$$\kappa(b, c) := (b + c - r)/p + p\mathbb{Z},$$

wobei $0 \le r \le p-1$ der kleinste nichtnegative Vertreter der Restklasse von $b+c$ in C_p ist. Für $p = 3$ etwa erhalten wir die Wertetabelle für den Kozykel

	0	1	2
0	0	0	0
1	0	0	1
2	0	1	1

Definition/Bemerkung 2.6.13 Höher und höher

Für jeden $R[G]$-Modul M gibt es Kohomologiegruppen $H^i(G,M)$ für alle $i \in \mathbb{N}_0$. Diese lassen sich ad-hoc einführen als Faktormodul

$$H^i(G,M) = Z^i(G,M)/B^i(G,M).$$

Um hierbei die Z^i- und B^i-Terme zu definieren, betrachtet man für $i \in \mathbb{N}^0$ den R-Modul $C^i(G,M) := \mathrm{Abb}(G^i, M)$ und definiert eine Abbildung (manchmal das *Differential* genannt)

$$d^i : C^i(G,M) \to C^{i+1}(G,M)$$

durch

$$\begin{aligned}(d^i f)(g_1,\ldots,g_{i+1}) &:= g_1 \cdot f(g_2,\ldots,g_{i+1}) + \textstyle\sum_{j=1}^{i} f(g_1,\ldots,g_{j-1},g_jg_{j+1},\ldots g_i)\\ &\quad + (-1)^{i+1} f(g_1,\ldots,g_i).\end{aligned}$$

Hier sollte man nachrechnen, dass $d^i \circ d^{i-1} = 0$ gilt, und daher

$$B^i(G,M) := \mathrm{Bild}(d^{i-1}) \subseteq Z^i(G,M) := \mathrm{Kern}(d^i).$$

Für alle Zweifler sei noch mitgeteilt, dass $d^{-1} : 0 \to C^0(G,M) = M$ die Nullabbildung ist.

Das beendet die Definition.

Beispiel 2.6.14 Vergleich

a) Für $i = 0$ ist $B^0(G,M) = 0$ und

$$Z^0(G,M) = \{m \in M \mid \forall g : g \cdot m - m = 0\} = M^G,$$

also stimmt unser neues H^0 mit dem alten überein.

Für $i = 1$ ist

$$B^1(G,M) = \{f \in C^1(G,M) \mid \exists m \in M : \forall g : f(g) = gm - m\},$$

was mit unserer alten Definition übereinstimmt. Weiter ist

$$Z^1(G,M) = \{f \in C^1(G,M) \mid \forall g,h \in G : (d^1 f)(g,h) = gf(h) - f(gh) + f(g) = 0\},$$

auch im Einklang mit unserem alten Bild.

Auch für $i = 2$ passt die neue Definition mit der alten überein.

b) Wenn $0 \to N \xrightarrow{\alpha} M \xrightarrow{\pi} M/N \to 0$ eine kurze exakte Sequenz von $R[G]$-Moduln ist, dann erhalten wir aus der offensichtlichen Funktorialität von H^i eine lange Sequenz

$$\begin{aligned}0 \to H^0(G,n) \overset{H^0(G,\alpha)}{\to} H^0(G,M) \overset{H^0(G,\pi)}{\to} H^0(G,M/N) &\xrightarrow{\partial} H^1(G,N) \to\\ \cdots \to H^i(G,M/N) &\xrightarrow{\partial} H^{i+1}(G,N) \to \ldots\end{aligned}$$

wobei der ominöse Pfeil $\partial : H^i(G, M/N) \to H^{i+1}(G, N)$ immer durch

$$\partial([\kappa]) := d^i(f)$$

mit $f \in C^i(G, M)$, $\pi \circ f = \kappa$ gegeben wird, denn $d^i(f)$ ist immer ein $i+1$-Korand mit Werten in M, er nimmt aber sogar Werte in N an, da κ ein Kozykel ist.

Man rechnet nach, dass diese lange Sequenz immer exakt ist.

Definition/Bemerkung 2.6.15 Kohomologische Induktion

a) Ein $R[G]$-Modul heißt *azyklisch*, wenn

$$\forall i \geq 1 : H^i(G, M) = \{0\}.$$

b) Wenn $0 \to N \to M \to M/N \to 0$ eine kurze exakte Sequenz von $R[G]$-Moduln ist, so liefert die lange exakte Sequenz aus 2.6.14b) insbeondere auch exakte Teilstücke der Gestalt

$$H^i(G, M) \to H^i(G, M/N) \to H^{i+1}(G, N) \to H^i(G, M)$$

Wenn M azyklisch ist, so ist die Randabbildung $\partial : H^i(G, M/N) \to H^{i+1}(G, N)$ ein Isomorphismus, und man kann bisweilen Aussagen über $(i+1)$-te Kohomologie auf solche über i-te zurückführen. Das nennt man dann *kohomologische Induktion*.

c) Als Beispiel hierfür sei die folgende Situation ins Feld geführt: Es sei G eine endliche Gruppe und R ein Ring, in dem die Gruppenordnung von G invertierbar ist. Weiter sei M ein $R[G]$-Modul. Dann ist jeder 1-Kozykel $\kappa : G \to M$ ein Korand.

Denn: Es sei $m := -\sum_{g \in G} \kappa(g)$. Dann gibt es genau ein Element $n \in M$ mit $|G| \cdot n = m$, denn die Multiplikation mit der Gruppenordnung ist invertierbar. Für dieses n und jedes $g \in G$ aber gilt dann

$$|G| \cdot (n - gn) = \sum_{h \in G} (\kappa(h) - g\kappa(h)) = [\sum_{h \in G} \kappa(h) - \kappa(gh) + \kappa(g)] = |G|\kappa(g),$$

und da man hier kürzen darf, folgt

$$\kappa(g) = n - gn,$$

also ist κ ein Korand.

Nun benötigen wir noch das Faktum, dass jeder Modul sich in einen azyklischen einbetten lässt. Darauf werde ich in 2.6.17 noch zu sprechen kommen.

Es sei nun N ein beliebiger $R[G]$-Modul und $N \subseteq M$ eine Einbettung in einen azyklischen Modul. Dann gibt es nach dem oben gesagten einen Isomorphismus $H^1(G, M/N) \to H^2(G, N)$, aber $H^1(G, M/N)$ ist trivial, denn jeder 1-Kozykel ist ein Korand. Also ist auch $H^2(G, N)$ für jeden Modul trivial, insbesondere auch für M/N. Der Isomorphismus $H^2(G, M/N) \to H^3(G, N)$ sagt dann, dass auch alle $H^3(G, N)$ trivial sind, und jetzt sehen Sie wie die kohomologische Induktion ins Rollen kommt.

Fazit. Für jeden $R[G]$-Modul M verschwinden alle $H^i(G, M), i \geq 1$.

Das hängt eng damit zusammen, dass in dieser Situation der Funktor $H^0(G, -)$ exakt ist.

Er ist exakt, da es zu jedem Untermodul $N \subseteq M$ einen komplementären Untermodul U gibt und damit $M \cong N \oplus U$ gilt. Hier induziert die natürliche Projektion $M \to M/N$ einen $K[G]$-Isomorphismus von U nach M/N, und daher lässt sich insbesondere jedes G-invariante Element aus M/N zu einem G-invarianten Element in $U \subseteq M$ liften.

Die Motivation für die Definition von H^1 versagt hier also: Wir brauchen H^1 nicht. Interessant, dass H^1 dann tatsächlich trivial ist! Und mit ihm auch alle höhere Kohomologie.

Definition 2.6.16 zwei Typen von Moduln

Es sei R ein Ring.

a) Ein R-Modul P heißt *projektiv*, wenn für jeden surjektiven Homomorphismus $\pi : M \to N$ von R-Moduln und für jden Homorphismus $\alpha : P \to N$ ein Homomorphismus $\varphi : P \to M$ existiert, sodass $\alpha = \pi \circ \varphi$ gilt. Im Diagramm:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow & \downarrow & & \\ M & \to & N & \to & 0 \end{array}$$

Jeder freie Modul P ist projektiv, denn wenn $B \subseteq P$ eine Basis ist, so sucht man zuerst für $b \in B$ Urbilder $\varphi(b)$ von $\alpha(b)$ unter π und setzt diese Vorschrift linear zu einem Modulhomomorphismus fort.

Jeder projektive Modul ist ein direkter Summand in einem freien Modul. Ist nämlich P projektiv und F ein freier Modul, von dem aus es einen surjektiven Homomorphismus π nach P gibt (z.B. F frei mit Basis P), so nutze die Projektivität von P mit $\alpha = \mathrm{Id}_P$, um eine Abbildung $\varphi : P \to F$ zu finden, sodass $\pi \circ \varphi = \mathrm{Id}_P$ gilt. Dann ist φ injektiv, und das Bild von φ ist komplementär zum Kern von π, also $F \cong \mathrm{Ker}(\pi) \oplus P$.

Jeder direkte Summand in einem freien Modul ist projektiv. Wenn nämlich $F = P \oplus \tilde{P}$ frei ist und $M \to N$ surjektiv, so lässt sich $\alpha : P \to N$ nach

F fortsetzen mithilfe der Projektion von F auf P, anschließend nutzen wir aus, dass F projektiv ist, und dann schränken wir die Abbildung von F nach M, die wir dadurch bekamen, auf P ein.

Außerdem ist jeder R-Modul ein Faktormodul von einem projektiven Modul, das geht ja sogar mit freien Moduln.

Aber eigentlich ist der Begriff des projektiven Moduls gar nicht der für uns relevante...

b) Ein R-Modul Q heißt *injektiv*, wenn es für jeden injektiven R-Modulhomomorphismus $\iota : N \to M$ und jeden R-Modulhomomorphismus $\beta : N \to Q$ eine Fortsetzung von ι nach M gibt. Im Diagramm:

$$\begin{array}{ccccc} 0 & \to & N & \to & M \\ & & \downarrow & \swarrow & \\ & & Q & & \end{array}$$

Hier wurden im Diagramm aus a) alle Pfeile umgedreht („dualisiert“).

Leider ist es nicht so einfach, injektive Moduln anders zu charakterisieren (außer für Hauptidealringe). Es lässt sich aber zeigen, dass jeder Modul ein Untermodul eines injektiven Moduls ist.

Ich zeige das für $R = \mathbb{Z}$. Hier ist jeder divisible Modul M injektiv, wobei divisibel bedeutet, dass die Multiplikation mit jeder natürlichen Zahl surjektiv ist. Zum Beispiel $\mathbb{Q}$ oder $\mathbb{Q}/\mathbb{Z}$ sind injektive Moduln. Diese Charakterisierung der Injektivität ist zum Beispiel in Jacobson, Basic Algebra II, bewiesen.

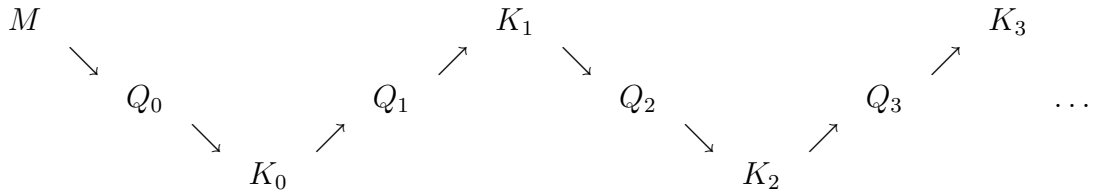
Ist nun M irgendein $\mathbb{Z}$-Modul, so ist er von der Gestalt F/U, wobei F ein freier $\mathbb{Z}$-Modul ist. Dann ist aber $(F \otimes_{\mathbb{Z}} \mathbb{Q})/U$ als Quotient eines Vektorraums divisibel, und damit injektiv, und enthält $F/U \cong M$.

Dies kann man letztlich als Hebel benutzen, um die Behauptung oben für alle Ringe R zu zeigen.

Bemerkung 2.6.17 Alternative Definition der Kohomologie

a) Wir wollen hier glauben, dass jeder injektive $R[G]$-Modul azyklisch ist. Letztlich sagt Injektivität von Q, dass jede kurze exakte Sequenz $0 \to Q \to M \to N \to 0$ spaltet, also $M \cong Q \oplus N$ gilt, und dann braucht man keine höhere Kohomologie von G mit Koeffizienten in Q.

b) Nun sei M ein $R[G]$-Modul. Dieser liegt in einem injektiven Modul Q_0, der Kokern der Inklusion heiße K_0. Dann liegt auch K_0 in einem injektiven Modul Q_1 mit Kokern K_1, welcher in einem injektiven Modul Q_2 mit Kokern K_2 liegt u.s.w. Das gibt ein paar kurze exakte Sequenzen, die wir auf folgende Art kreuz und quer schreiben:



Darin sieht man in der Mitte jeweils eine Abbildung von $d^i : Q_i \to Q_{i+1}$, die sich aus der Projektion nach K_i und dessen Einbettung in Q_{i+1} zusammensetzt. Aus dieser Konstruktion ist auch klar, dass die Sequenz

$$Q_0 \xrightarrow{d^0} Q_1 \xrightarrow{d^1} Q_2 \xrightarrow{d^2} Q_3 \dots$$

exakt ist. Der Kern von d^0 ist genau M.

Nun wenden wir auf diese Sequenz den Funktor $H^0(G, -)$ an und erhalten die Sequenz

$$Q_0^G \xrightarrow{d^0} Q_1^G \xrightarrow{d^1} Q_2^G \xrightarrow{d^2} Q_3^G \dots$$

Wegen der Funktorialität von $H^0(G, -)$ gilt hier immer noch $d^i \circ d^{i-1} = 0$, und nun kann man tatsächlich kohomologische Induktion benutzen, um zu zeigen, dass

$$H^i(G, M) = \mathrm{Kern}(d^i | Q_i^G) / \mathrm{Bild}(d^{i-1} | Q_{i-1}^G).$$

Das nennt man die *Kohomologie des Kettenkomplexes* $(Q_i^G, d^i)_{i \in \mathbb{N}_0}$.

c) Die hier vorgestellte alternative Konstruktion der Kohomologie kann man in größerer Allgemeinheit benutzen, um linksexakte Funktoren „abzuleiten“. Dies ist der Gegenstand der homologischen Algebra.

Bemerkung 2.6.18 Blickwinkel

Die höheren Kohomologiegruppen, die zuerst als Vehikel erscheinen, um eine mangelnde Exaktheit aufzufangen, sind in vielen Situationen an sich schon interessant, gerade auch wenn es um Beziehungen zu topologisch gewonnenen Kohomologiegruppen geht. Dass es so etwas gibt und dass dies auch in der Zahlentheorie wichtig ist, ist eine der Einsichten aus dem Gebiet der Modulformen, die im letzten Jahrhundert zum Beispiel den Weg zum Beweis der Fermatschen Vermutung geebnet haben.