Zentrale einfache Algebren und Galois-Kohomologie

frei nach
Philippe Gille und Tamás Szamuely
siehe
http://www.cambridge.org/uk/catalogue.asp?isbn=9780521861038

(Eigentliches Ziel: Klassenkörpertheorie: Gauß, Quadratisches Reziprozitätsgesetz, Verallgemeinerung auf höhere Grade, simultane Beschreibung aller Galois-Erweiterungen eines Körpers durch Daten innerhalb des Körpers)

Inhalt

Bezeichnungen

$B(p)$	p-primäre Torsionsuntergruppe der abelschen Gruppe B.
$Br(k)$	Brauer-Gruppe des Körpers k, vgl. 2.4.9
$Br(K/k)$	relative Brauer-Gruppe zur endlichen Galois-Erweiterung K/k, vlg. 2.4.9.
C_A	der Kokern der natürlichen Einbettung $A \longrightarrow M^G(A)$ des G-Moduls A in den zugehörigen koinduzierten Modul, vgl. 3.3.18.
$C(a, b)$	der zur Quaternionen-Algebra gehörige Kegelschnitt, vgl. 1.3.1.
$C(a, b)(K)$	die Menge der K-rationalen Punkte von C(a, b), vgl. 1.3.1
$Cl(X)$	Divisorklassen-Gruppe des Schemas X, vgl. A0.6.5.
$CSA_K(n)$	die Menge der k-Isomorphie-Klassen zentraler einfacher k-Algebren des Grades n, welcher über der endlichen Galois-Erweiterung K von k zerfallen, vgl. 2.4.3
CSA_K	die Menge der k-Isomorphie-Klassen zentraler einfacher k-Algebren, welche über K zerfallen, vgl. 2.4.9
$c(E)$	die Kohomologie-Klasse der Gruppen-Erweiterung E, vgl. 3.2.6.
$cd(k)$	kohomologische Dimension des Körpers k, vgl. 6.1.8
$cd_p(k)$	p-kohomologische Dimension des Körpers k, vgl. 6.1.8
χ_X	charakteristisches Polynom der Matrix X, vgl. 2.5.1.
(χ, b)	zyklische Algebra zum Isomorphismus χ, vgl. 2.5.3.
$codim_X Y$	Kodimension des Teilschemas Y im Schema X, vgl. A0.6.1.
$deg\ D$	Grad des Divisors D auf einer glatten irreduziblen Kurve, vgl. 1.4.8.
$deg\ p$	Grad des Primdivisors p auf einer glatten irreduziblen Kurve, vgl. 1.4.7.
$dim_x X$	Dimension des Schemas X im Punkt x, vgl. A0.6.1.
$dim\ X$	Dimension des Schemas X, vgl. A0.6.1.
$dim\ R$	Dimension des kommutativen Rings R mit 1, vgl. A0.6.1.
$Div(X)$	Gruppe der Divisoren der Kurve X, vgl. 1.4.6
$Div(X)$	Gruppe der Weil-Divisoren des Schemas X, A06.4.
$div(f)$	Divisor der rationalen Funktion f, vgl. 1.4.6. bzw. A0.6.5.

$D(f)$	offene Hauptmenge zum Polynom f, vgl. 1.4.2.
$\mathrm{End}_A(M)$	Ring der Endomorphismen des Moduls M über dem Ring A (mit Eins), vgl. 2.1.6.
E_{ij}	die Elementarmatrix mit einer Eins in der Position (i,j) und Nullen in allen anderen Positionen, vgl. 2.1.3.
$\mathrm{Ext}^i_R(M,N)$	die i-te Ext-Gruppe der Moduln M und N über dem Ring R mit 1 (der nicht notwendig kommutativ ist), vgl. 3.1.5.
F	Frobenius-Automorphismus der separablen Abschließung eines endlichen Körpers, vgl. 4.1.6.
$F(A)$	der von A erzeugte freie Modul, vgl. 3.1.9.
$\tilde{F}(b)$	Erzeuger der zyklischen Algebra (χ, b), vgl. 2.5.3 und 2.5.4.
$F(b)$	ein Repräsentant des Erzeugers $\tilde{F}(b)$ der zyklischen Algebra (χ, b), vgl. 2.5.3 und 2.5.4.
$\mathrm{Gal}(k)$	die absolute Galois-Gruppe des Körpers k, vgl. 4.1.11.
$\mathrm{Gal}(K/k)$	die Galois-Gruppe der k-Automorphismen $K \longrightarrow K$ der Galois-Erweiterung K/k, vgl. 4.1.1.
$H^1(G, A)$	erste nicht-abelsche Kohomologie der Gruppe G mit Werten in der Gruppe A (auf welcher G durch Automorphismen operiert), vgl. 2.3.6.
$H^i(G,A)$	i-te Kohomologie der Gruppe G mit Werten im G-Modul A, vgl. 3.1.13.
$H^i_{\mathrm{cont}}(G, A)$	i-te stetige Kohomologie der proendlichen Gruppe G mit Werten im topologischen Modul A, vgl. 4.2.4.
$H^i(k, A)$	i-te Galois-Kohomologie des Körpers k mit Werten im topologischen $\mathrm{Gal}(k_s/k)$-Modul A, vgl. 4.2.4.
I_G	das Augmentationsideal zur Gruppe G, vgl. 3.2.9.
$\mathrm{ind}_k A$	Index der zentralen einfachen k-Algebra A, vgl. 4.5.1.
k	Ein Körper
k[V]	Koordinatenring der affinen Varietät V, vgl. 1.4.3
k(V)	Körper der rationalen Funktionen der reduzierten und irreduziblen Varietät V, vgl. 1.4.4.
L(D)	Raum der rationalen Funktionen auf einer glatten irreduziblen Kurve, deren Polstellenordnungen durch den Divisor D beschränkt sind, vgl. 1.4.6.
$\ell(D)$	Dimension des Vektorraums L(D), vgl. 1.4.8.
λ_r	Linksmultiplikation mit dem Element r, vgl. A3.10.
$M_H^G(A)$	der durch den Modul A über der Untergruppe H von G induzierte G-Modul, vgl. 3.3.2.
$M^G(A)$	der durch die abelsche Gruppe A über der Gruppe G koinduzierte Modul, vgl. 3.3.3.
$M_2(k)$	die Quaternionen-Algebra der 2×2-Matrizen über dem Körper k, vgl. 1.1.9.
$N(q)$	die Norm des Quaternions q, vgl. 1.1.3.
$N_{K/k}(c)$	die Norm des Elements $c\in K$ bezüglich der Körpererweiterung K/k, vgl. 1.1.11
Nrd	Reduzierte Norm einer zentralen einfachen Algebra, vgl. 2.5.1.
N^A	der Kern der Multiplikationsabbildung N mit der Summe der Elemente einer endlichen Gruppe G auf dem G-Modul A, 3.2.9.

$\mathcal{O}_V(U)$	Ring der auf der offenen Teilmenge U der Varietät V definierten regulären Funktionen, vgl. 1.4.3.
$\mathcal{O}_X(1)$	Twist-Garbe des projektiven Spektrums X, vgl. A0.5.5 und A0.5.7..
P(X)	Gruppe der Hauptdivisoren des Schemas X, vgl. A0.6.5.
$P_a(T)$	reduziertes charakteristisches Polynom des Elements a einer zentralen einfachen Algebra, vgl. 4.5.4.
per(A)	Periode der zentralen einfachen Algebra A, vgl. 4.5.15.
Q^-	Raum der reinen Quaternionen der Quaternionen-Algebra Q, vgl. 1.5.5.
R	ein nicht notwendig kommutativer Ring mit 1, vgl. 3.1.2.
$\rho_{i,A}$	die natürliche Abbildung der Inf-Res-Sequenz in der Dimension i für den Modul A, vgl. 3.3.18
ρ_r	Rechtsmultiplikation mit dem Element r, vgl. A3.10.
Sch(S)	Kategorie der Schemata über dem Schema S, vgl. Beispiel A0.2.2.(xi)
$Sh_X(\mathcal{O})$	Kategorie der Garben des topologischen Raums X mit Werten in der Kategorie $\mathcal{C}$, vgl. A0.2.1.
$SL_1(A)$	multiplikative Gruppe der Elemente der zentralen einfachen Algebra A, deren reduzierte Norm gleich 1 ist, vgl. 2.6.3.
Stab(x)	Stabilisator des Element x eines Moduls über einer Gruppe, vgl. 4.3.3.
tot(A**)	der zum Doppel-Komplex A** gehörige einfache Komplex, vgl. 3.4.2
U_i	die offene Menge der Punkte im projektiven Raum, deren i-te Koordinate ungleich Null ist (wobei die Numerierung der Koordinaten mit 0 beginnt), vgl. 1.4.2
$TF_K(V_K, \Phi_K)$	Menge der Isomorphie-Klassen über k der K/k-Twists des Vektorraum (V, Φ) mit dem (p,q)-Tensor Φ, vgl. 2.3.7.
Trd	reduzierte Spur einer zentralen einfachen Algebra, vgl. 2.5.1.
V(I)	Nullstellenmenge des Ideals I bzw. der Menge I, vgl. 1.4.1
V*	Dual des Vektorraum V, vgl. 2.3.1.
Var(k)	Kategorie der (quasi-projektiven) Varietäten über dem algebraisch abgeschlossenen Körper k, vgl. Beispiel A0.2.2 (vi).
X^0	Menge der abgeschlossenen Punkte der quasi-projektiven Varietät X, vgl. 1.4.6
${}_aX$	die G-Menge X, versehen mit der durch den 1-Kozyklus getwisteten Operation, vgl. 2.3.10.
Z(A)	das Zentrum der Algebra A, vgl. 2.1.2.
(a, b)	die verallgemeinerte Quaternionen-Algebra (über dem Körper k) mit den Relationen $i^2 = a$, $j^2 = b$, vgl. 1.1.4.
$\{a_1,...,a_n\}$.	Symbol der Elemente $a_1,...,a_n$ aus der multiplikativen Gruppe eines Körpers in der n-ten K-Gruppe von Milnor, vgl. 4.6.1.
f_*F	direktes Bild der Garbe F bei der stetigen Abbildung f, vgl. Bemerkung A0.2.1(iv).
$f^{-1}F$	inverses Bild der Garbe F bei der stetigen Abbildung f, vgl. Bemerkung A0.2.1(v).
f*F	inverses Bild der Modul-Garbe F einem Morphismus f von Schemata (oder auch von geometrischen Räumen), vlg. A0.5.2.
$\hat{G}$	die proendliche Vervollständigung der Gruppe G, vgl. 4.1.3.
$a \cup b$	Cup-Produkt der Kohomologie-Klassen a und b, vgl. 3.4.9.

$A^* \otimes B^*$	das Tensor-Produkt der Komplexe A* und B*, vgl. 3.4.3.
$\overline{q}$	das zum Quaternion q konjugiert Quaternion, vgl. 1.1.3.
(a, b)	die Quaternionen-Algebra über einem Körper k mit den Struktur-Konstanten a,b∈k*, vgl. 1.1.4.
(χ, b)	die zyklische k-Algebra zur zyklischen Erweiterung K/k, zum Isomorphismus χ: $G(K/k) \longrightarrow \mathbb{Z}/m\mathbb{Z}$ und zum Element b∈k*, vgl. 2.5.3.
F(n)	n-fach getwistete Garbe auf einem projektiven Spektrum, vgl. A0.5.5.
G^{op}	Dual der Gruppe G, vgl. Fußnote 3.3.5 (iii).
$s\|_x$	der Keim im Punkt x des Schnittes s einer Prägarbe, vgl. A0.2.1 Bemerkung (i).
$X \times_Z Y$	Faserprodukt der topologischen Räume X und Y über dem topologischen Raum Z, vgl. Bemerkung A0.2.1(v), Faserprodukt der affinen Schemata X und Y über dem affinen Schema Z, vgl. Beispiel A0.2.2 (iv)
M[n]	n-fach im Grad verschobener graduierter Modul, vgl. A0.5.5.

1. Quaternionen-Algebren

1.1. Grundlegende Eigenschaften

1.1.1 Definition

Sei k ein Körper. Eine k-Algebra ist ein k-Vektorraum V mit einer über k bilinearen Abbildung

$$V \times V \longrightarrow k, (x, y) = x \bullet y,$$

welche assoziativ (aber nicht notwendig kommutativ ist):

$$x \bullet (y \bullet z) = (x \bullet y) \bullet z \text{ für } x,y,z \in V.$$

Diese bilineare Abbildung heißt auch Multiplikation der Algebra.

Eine solche k-Algebra heißt endlich-dimensional, wenn sie als k-Vektorraum eine endliche Dimension besitzt.

1.1.2 Vereinbarung: alle Algebren seien endlich-dimensional mit 1

Wenn nicht explizit anders erwähnt sollen alle k-Algebren endlich-dimensional sein und ein Einselement besitzen:

$$1 = 1_V \in V \text{ mit } 1 \bullet x = x \bullet 1 = x \text{ für jedes } x \in V.$$

1.1.3 Die Quaternionen-Algebra von Hamilton

Das geschichtlich erste Beispiel einer nicht-kommutativen Algebra wurde von Hamilton 1843 während eines Spaziergang mit seiner Frau gefunden: die Algebra der Quaternionen. Heute beschreibt man sie meistens als Teilring der komplexen Matrizen-Algebra $\mathbb{C}_2^2$:

$$\mathbb{H} := \left\{ \begin{pmatrix} x+y\sqrt{-1} & z+w\sqrt{-1} \\ -z+w\sqrt{-1} & x-y\sqrt{-1} \end{pmatrix} \middle| \, x,y,z,w \in \mathbb{R} \right\}$$

Sie ist als Vektorraum über den reellen Zahlen 4-dimensional:

$$\mathbb{H} = \mathbb{R} \bullet 1 + \mathbb{R} \bullet i + \mathbb{R} \bullet j + \mathbb{R} \bullet k .$$

Ihre Multiplikation ist durch die folgenden Relationen gegeben:

$$i^2 = -1, \; j^2 = -1, \; ij = -ji = k.$$

Bemerkungen

(i) $\mathbb{H}$ ist ein Schiefkörper (heute auch oft: eine Divisionsalgebra) über $\mathbb{R}$, d.h. jedes von Null verschiedene Element x besitzt ein zweiseitiges Inverses. Mit anderen Worten, es gibt ein Element y mit

$$x \bullet y = y \bullet x = 1.$$

Der Beweis von Hamilton beruht auf den Begriffen des konjugierten Quaternions und der Norm.

(ii) Das zu einem Quaternion $q = x + yi + zj + wk$ konjugierte Quaternion $\overline{q}$ ist definiert als

$$\overline{q} = x + yi + zj + wk.$$

Unter der Norm des Quaternions q versteht man das Produkt

$$N(q) = q \bullet \overline{q} = x^2 + y^2 + z^2 + w^2.$$

(iii) Beweis der Schiefköpereigenschaft: für $q \neq 0$ gilt auch $N(q) \neq 0$, d.h.

$$\overline{q}/N(q)$$

ist ein wohldefiniertes Element von $\mathbb{H}$. Unmittelbar aus den Definitionen folgt, daß es sich um ein zweiseitiges Inverses von q handelt.

(iv) Über Körpern, deren Charakteristik von 2 verschieden ist, kann man die obige Konstruktion in einfacher Weise verallgemeinern.

1.1.4 Definition: die verallgemeinerte Quaternionen-Algebra (a,b)

Seien k ein Körper der Charakteristik $\neq 2$ und

$$a, b \in k$$

zwei von Null verschiedene Elemente dieses Körpers. Dann ist die verallgemeinerte Quaternionen-Algebra

$$(a, b) = (a, b)_k$$

definiert als der 4-dimensionale k-Vektorraum mit der Basis

$$1, i, j, ij,$$

dessen Multiplikation definiert ist durch die Relationen

$$i^2 = a, j^2 = b, ij = -ji.$$

Bemerkungen

(i) Die Isomorphie-Klasse von (a, b) hängt nur von den Restklassen $\overline{a}, \overline{b} \in k/k2$ von a bzw. b ab.

Bezüglich der Basis

$$1, i', j', i'j'$$

mit

$$i' = u \bullet i, j' = v \bullet j, u,v \in k$$

bekommen die definierenden Relationen der Algebra die Gestalt

$$i'^2 = u^2 \bullet a, j'^2 = v^2 \bullet b, i' \bullet j' = -j' \bullet i'.$$

Mit anderen Worten, die k-Algebren (a, b) und (u^2a, v^2b) sind isomorph (bezüglich des Isomorphismus

$$(u^2a, v^2b) \xrightarrow{\cong} (a, b), i = ui, j = vj.$$

(ii) Die Algebren (a, b) und (b, a) sind isomorph.

Bezüglich der Basis

$$1, i', j', i'j'$$

mit

$$i' = (ab) \bullet j \text{ und } j' = (ab) \bullet i$$

bekommen die definierenden Relationen der Algebra die Gestalt

$$i'^2 = a^2b^3\ ,\ j'^2 = a^3b^2,\ i'j' = -\,j'i'.$$

Also gilt

$$(a, b) \cong (a^2b^3, a^3b^2) \cong (b, a).$$

(iii) Die Multiplikation von (a, b) ist assoziativ.

Wir wählen eine Körpererweiterung K/k mit der Eigenschaft, daß es Elemente

$$t, u, v, w \in K$$

gibt mit

$$u^2 = a\ ,\ v^2 = b \text{ und } t^2 = -1.$$

Dann gilt

$$(a, b)_k \subseteq (a, b)_K \cong (1,1)_K\ .$$

Es reicht, die Assoziativität von $(1, 1)_K$ zu beweisen, d.h. wir können annehmen

$$a = b = 1.$$

Dann kann man aber (a, b) identifizieren mit der Matrizen-Algebra

$$\left\{\begin{pmatrix} x+yt & z+wt \\ -z+wt & x-yt \end{pmatrix} \middle|\ x,y,z,w \in k\right\}.$$

Die Behauptung folgt also aus der Tatsache, daß die Matrizen-Multiplikation über einem Körper kommutativ ist.

1.1.5 Das Konjugierte eines Quaternions

Für jedes Element

$$q = x + yi + zj + wij$$

der Quaternionen-Algebra (a, b) heißt

$$\overline{b} = x - yi - zj - wij$$

das zu q konjugierte Element oder auch einfach Konjugiertes von q.

Bemerkungen

(i) Die Abbildung

$$(a, b) \longrightarrow (a, b),\ q = \overline{q}\ ,$$

ist ein Anti-Automorphismus der k-Algebra (a,b), d.h. ein k-Vektorraum-Automorphismus mit

$$\overline{q'q''} = \overline{q}', \overline{q}''\ .$$

(ii) Die Abbildung ist sogar eine Involution, d.h. es gilt außerdem

$$\overline{\overline{q}} = q$$

für jedes q aus (a, b).

1.1.6 Die Norm eines Quaternions

Für jedes Element

$$q = x + yi + zj + wij$$

der Quaternionen-Algebra (a, b) heißt

$$N(q) = q\overline{q}$$

Norm von q.

Bemerkungen

(i) Es gilt

$$N(q) = x^2 - ay^2 - bz^2 + abw^2 \in k,$$

d.h. die Abbildung

$$N: (a, b) \longrightarrow k$$

ist eine nicht-entartete quadratische Form[1] auf (a, b) über k.

---

[1] d.h. die Bilinearform

(ii) Die Norm ist multiplikativ[2],

$$N(q'q'') = N(q')N(q'').$$

1.1.7 Umkehrbarkeitskriterium

(i) Ein Element q der Quaternionen-Algebra (a, b) ist genau dann umkehrbar, wenn gilt

$$N(q) \neq 0.$$

(ii) Die Quaternionen-Algebra (a, b) ist genau dann ein Schiefkörper, wenn ihre Norm

$$N: (a, b) \longrightarrow k$$

keine nicht-triviale Nullstelle besitzt, d.h. keine außer der Null.

Beweis. Die Argumentation ist dieselbe wie im Fall der klassischen Quaternionen-Algebra $\mathbb{H}$ (siehe 1.1.3 Bemerkung (iii)).
QED.

1.1.8 Eine koordinaten-unabhängige Beschreibung von Konjugation und Norm

Ein Element

$$q \in (a, b) - \{0\}$$

heißt reines Quaternion, wenn gilt

$$q^2 \in k \text{ aber } q \notin k$$

gilt. Die Null wird ebenfalls als rein angesehen.
Bemerkungen

(i) Eine direkte Rechnung zeigt,

$$q = x + yi + zj + wij \text{ ist rein} \Leftrightarrow x = 0.$$

(ii) Jedes Quaternion q läßt sich somit in der Gestalt

$$q = q' + q'' \text{ mit } q' \in k \text{ und } q'' \text{ rein}$$

schreiben. Die Konjugation ist dann durch die Formel

$$\overline{q} = q' - q''$$

gegeben.

1.1.9 Beispiel: die Matrizen-Algebra $M_2(k)$

Neben den klassischen Hamiltonschen Quaternionen ist das zweite grundlegende Beispiel die k-Algebra $M_2(k)$ der 2×2-Matrizen mit Einträgen aus k. Mit

$$i := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, j := \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

gilt nämlich

$$i \bullet j = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \bullet \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b \\ -1 & 0 \end{pmatrix} = - \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \bullet \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = - j \bullet i ,$$

also

$$M_2(k) = k \bullet 1 + k \bullet i + k \bullet j + k \bullet ij$$

und $M_2(k) \cong^3 (1, b)$.

$$b(q', q'') = \frac{1}{2}(N(q'+q'') - N(q') - N(q''))$$
$$= \text{Linearglied der Taylor-Entwicklung von } N(q'+q'')$$
$$= x'x'' - ay'y'' - bz'z'' + abw'w''$$

ist nicht-artet: die zugehörige Matrix hat Diagonalgestalt und die Einträge 1, a, b, ab auf der Hauptdiagonalen.

[2] Genauer: $N(q'q'') = q'q''\,\overline{q}''\overline{q}' = q'N(q'')\,\overline{q}' = q'\overline{q}' \bullet N(q'') = N(q')N(q'')$.

1.1.10 Zerfallende Quaternionen-Algebren

Eine Quaternionen-Algebra über k heißt zerfallend, wenn sie zu $M_2(k)$ isomorph ist.

1.1.11 Kriterium für zerfallende Quaternionen-Algebren

Folgende Aussagen sind äquivalent.

(i) Die k-Algebra (a, b) zerfällt.

(ii) Die k-Algebra (a, b) ist kein Schiefkörper.

(iii) Die Norm N: (a, b) $\longrightarrow$ k besitzt eine nicht-triviale Nullstelle.

(iv) Das Element b ist Norm[4] eines Elements der Körpererweiterung $k(\sqrt{a})/k$.

Beweis. (i) $\Rightarrow$ (ii). trivial, denn $M_2(k)$ besitzt Nullteiler.

(ii) $\Rightarrow$ (iii). Gilt nach dem Umkehrbarkeitskriterium 1.1.7

(iii) $\Rightarrow$ (iv).

1. Fall: a ist ein Quadrat in k.

Die Norm N der Körpererweiterung $k(\sqrt{a})/k$ ist gerade die identischen Abbildung. Jedes Element von k , insbesondere b, liegt im Bild dieser Abbildung.

2. Fall: a ist kein Quadrat in k.

Sei

$$q = x + yi + zj + wij$$

ein von Null verschiedenes Quaternion mit der Norm Null,

$$x^2 - ay^2 - bz^2 + abw^2 = 0.$$

Dann gilt

$$(z^2 - aw^2)b = x^2 - ay^2 \neq^{5} 0,$$

also

$$z^2 - aw^2 = (z - w\sqrt{a})(z + w\sqrt{a}) \neq 0.$$

Mit $K := k(\sqrt{a})$ folgt

$$b = \frac{x^2-ay^2}{z^2-aw^2} = \frac{N_{K/k}(x+y\sqrt{a})}{N_{K/k}(z+w\sqrt{a})} = N_{K/k}\left(\frac{x+y\sqrt{a}}{z+w\sqrt{a}}\right),$$

d.h. b ist Norm eines Elements von K wie behauptet.

(iv) $\Rightarrow$ (i).

1. Fall: a ist ein Quadrat in k.

---

[3] Die Spalten von $\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$ stehen senkrecht aufeinander.

[4] Sei K/k eine Körpererweiterung endlichen Grades $d = \dim_k K$. Die Multiplikaton mit $c \in K$ definiert eine k-lineare Abbildung

$$mult_c : K \longrightarrow K,\ x = cx.$$

Die Determinante dieser Abbildung heißt Norm von c bezüglich K/k und wird mit

$$N_{K/k}(c) = \det(mult_c)$$

bezeichnet. Falls c die Körpererweiterung erzeugt, ist $N_{K/k}(c)$ bis aufs Vorzeichen gerad das Absolutglied des Mininmalpolynoms von c.

Im Fall $K = k(\sqrt{a})$ bedeutet dies gerade

$$N(r + s\sqrt{a}) = (r + s\sqrt{a})(r - s\sqrt{a}) = r^2 - as^2$$

(falls a kein Quadrat in k ist).

[5] weil a kein Quadrat in k ist.

Da es nur auf die Restklasse von a in k/k^2 ankommt, gilt

$$(a, b) \cong (1, b) \cong M_2(k),$$

wobei sich die zweite Isomorphie aus 1.1.9 ergibt. Mit anderen Worten, (a, b) zerfällt.

2. Fall: a ist kein Quadrat in k.

Nach Voraussetzung ist b Norm eines Elements von $K := k(\sqrt{a})$. Da die Norm multiplikativ ist, ist auch b^{-1} eine Norm, d.h. es gibt r, s ∈ k mit

(1) $$b^{-1} = r^2 - as^2.$$

Wir betrachten jetzt die Vektorraumbasis

$$1, u, v, uv$$

von (a,b) mit

(2) $$u := rj + sij \text{ und } v := (1 + a)\bullet i + (1 - a)ui$$

Bevor wir zeigen, daß es sich tatsächlich um eine Basis von (a, b) handelt, bestimmen wir zunächst die multiplikativen Relationen bezüglich dieser Erzeuger.

Es gilt

$$\begin{aligned} u^2 &= r^2j^2 + rjsij + sijrj + s^2ijij \\ &= r^2b - rsij^2 + rsij^2 - s^2i^2j^2 \text{ (wegen } ij = - ji) \\ &= r^2b - abs^2 \qquad \text{(wegen } i^2 = a \text{ und } j^2 = b) \\ &= b\bullet(r^2 - as^2) \\ &= 1 \qquad \text{(wegen (1)).} \end{aligned}$$

Wir haben gezeigt:

(3) $$u^2 = 1.$$

Weiter gilt

$$ui = rji + siji = - rij - si^2j = -i(rj + sij) = -iu,$$

d.h.

(4) $$ui = -iu.$$

Mit

$$v := (1 + a)\bullet i + (1 - a)ui$$

erhalten wir

$$\begin{aligned} uv &= (1+a)ui + (1-a)u^2i \\ &= - (1+a)iu - (1-a)uiu \qquad \text{(wegen (3))} \\ &= -vu \end{aligned}$$

insgesamt also

(5) $$uv = - vu.$$

Weiter ist

$$\begin{aligned} v^2 &= (1+a)^2i^2 + (1+a)(1-a)(iui + ui^2) + (1-a)^2uiui \\ &= (1+a)^2a + 0 - (1-a)^2u^2i^2 \qquad \text{(wegen (4))} \\ &= (1+a)^2a - (1-a)^2a \qquad \text{(wegen (5)).} \\ &= 4a^2 \end{aligned}$$

zusammen also

(6) $$v^2 = 2a^2$$

Unter der Annahme, daß die Elemente 1, u, v, uv linear unabhängig sind, ergibt sich die Isomorphie

$$(a, b) \cong (1, 2a^2) \cong M_2(k),$$

d.h. (a, b) zerfällt wie behauptet. Wir haben noch die lineare Unabhängigkeit der 1, u, v, uv über k zu beweisen. Dazu bestimmen wir die Übergangsmatrix. Es gilt:

$$\begin{aligned} u &= rj + sij \qquad \text{(nach (2))} \\ v &= (1+a)\bullet i + (1-a)(rji + siji) = (1+a)\bullet i - (1-a)saj - (1-a)rij \qquad \text{(nach (2))} \end{aligned}$$

$uv = (1+a)ui + (1-a)u^2 i$ (vgl. den Beweis von (5))
$= (1+a)(rji + siji) + (1-a)i$ (nach Definition von u und nach (3))
$= (1-a)i - (1+a)saj - (1+a)rij$

Damit bekommt die Determinante der Basiswechselmatrix die Gestalt

$$\det\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & r & s \\ 0 & 1+a & -(1-a)sa & -(1-a)r \\ 0 & 1-a & -(1+a)sa & -(1+a)r \end{pmatrix} = -r \bullet \det\begin{pmatrix} 1+a & -(1-a)r \\ 1-a & -(1+a)r \end{pmatrix} + s \bullet \det\begin{pmatrix} 1+a & -(1-a)sa \\ 1-a & -(1+a)sa \end{pmatrix}$$

$= -r^2 (-(1+a)^2+(1-a)^2) + sa^2 \bullet (-(1+a)^2+(1-a)^2)$
$= -4a(sa^2 - r^2)$
$= 4a/b$ (nach (1))
$\neq 0$

QED.

1.1.12 Bemerkung

Die gerade bewiesene Aussage versetzt uns in die Lage, die nicht zerfallenden Quaternionen-Algebren unter den 4-dimensionalen k-Algebren zu charakterisieren.

1.2 Das Zerfallen über einer quadratischen Erweiterung

1.2.1 Das Zentrum einer k-Algebra

Sei A eine k-Algebra. Dann besteht das Zentrum

$$Z(A) := \{x \in A \mid xy = yx \text{ für jedes } y \in A\}$$

von A aus allen Elementen von A, welche mit allen Elementen von A kommutieren.

Bemerkungen

(i) Nach Definition gilt

$$k \subseteq Z(A).$$

(ii) Das Zentrum ist eine k-Teilalgebra von A: Summe und Produkt zweier Elemente aus A liegen in A, Z(A) ist ein k-linearer Unterraum von A.

(iii) Ist A ein Schiefkörper, so ist Z(A) ein Körper: liegt $x \in Z(A) - \{0\}$, so gilt

$$xy = yx$$

für jedes $y \in A$, also

$$yx^{-1} = x^{-1}y,$$

d.h. es gilt $x^{-1} \in Z(A)$.

(iv) Eine k-Algebra A mit

$$Z(A) = k$$

heißt zentral.

1.2.2 Beispiel

Die Quaternionen-Algebren (a, b) sind zentrale k-Algebren.

Beweis. Sei

$$q = x + yi + zj + wij \in (a, b)$$

ein Element aus dem Zentrum. Dann gilt

$iq = xi + ya + zij + awj = ya + xi + awj + zij$
$qi = xi + ya + zji + wiji = ya + xi - awj - zij$

Vergleich liefert $z = 0$ und $aw = 0$, also $w = 0$, also

$q = x + yi$

Weiter ist

$jq = xj - yij$
$qj = xj + yij.$

Vergleich liefert y = 0, d.h.

$$q = x \in k.$$

Damit ist gezeigt, $Z((a, b)) \subseteq k$. Die umgekehrte Inklusion besteht trivialerweise (vgl. 1.2.1 Bemerkung (i)).
QED.

1.2.3 Theorem
Seien

$$A$$

eine 4-dimensionale zentrale k-Algebra und

$$a \in k - k^2$$

ein Element. Dann sind folgende Aussagen äquivalent.

(i) A ist isomorph zu einer Quaternionen-Algebra (a, b) für ein $b \in k$.

(ii) Die $k(\sqrt{a})$-Algebra $A \otimes_k k(\sqrt{a})$ ist isomorph zu $M_2(k(\sqrt{a}))$.

(iii) Es gibt ein $q \in A - k$ mit $q^2 = a$.

Beweis. Beweis von (i) $\Rightarrow$ (ii).
Sei A isomorph zu (a, b). Dann gilt

$$A \otimes_k k(\sqrt{a}) \cong (a, b) \otimes_k k(\sqrt{a}) = (a, b)_{k(\sqrt{a})}$$

Nun ist aber a ein Quadrat im Körper $k(\sqrt{a})$, d.h. die Algebra rechts ist isomorph zu

$$(1, b)_{k(\sqrt{a})} \cong M_2(k(\sqrt{a}))$$

(nach 1.1.4 Bemerkung (i) und 1.1.9).

Beweis von (iii) $\Rightarrow$ (i). Sei

(1) $$q \in A - k, q^2 = a$$

ein Element wie in Bedingung (iii). Weil A nach Voraussetzung zentral ist, liegt q nicht im Zentrum von q, d.h. der innere Automorphismus

$$\sigma: A \longrightarrow A, x = q^{-1}xq,$$

ist von der identischen Abbildung verschieden, also ein Automorphismus der Ordnung 2. Insbesondere besitzt σ den Eigenwert -1.[6] Es gibt also ein Element

$$r \in A - \{0\} \text{ mit } q^{-1}rq = - r,$$

d.h. mit

(2) $$rq + qr = 0.$$

Es reicht zu zeigen, die Elemente

(3) $$1, q, r, qr$$

---

[6] Bezeichne $\overline{k}$ eine algebraische Abschließung von k und sei $\overline{\sigma} := \sigma \otimes \overline{k}: A \otimes \overline{k} \longrightarrow A \otimes \overline{k}$. Wegen $\overline{\sigma}^2 =$ Id sind +1 und -1 die einzigen möglichen Eigenwerte. Weil die Ordnung von $\overline{\sigma}$ gleich 2 ist, ist

$$X^2 - 1 = (X.-1)(X+1)$$

das Minimalpolynom von $\overline{\sigma}$. Letzteres besitzt keine mehrfachen Nullstellen. Deshalb ist die Jordansche Normalform von $\overline{\sigma}$ eine direkte Summe von Jordanblocken des Typs 1×1, d.h. eine Diagonalmatrix, deren Einträge auf der Hauptdiagonalen +1 und -1 sind. Das charakteristische Polynom von σ ist insbesondere von der Gestalt

$$\chi_\sigma = \chi_{\overline{\sigma}} = (1-T)^r(1-T)^s,$$

zerfällt also über k in Linearfaktoren. Deshalb sind die Hauptraumzerlegung und die Jordanzerlegung bereist über k definiert (d.h. die obige Bestimmung der Jordanschen Normalform ist bereits über k gültig). Insbesondere ist -1 ein Eigenwert von σ: andernfalls wäre σ die identische Abbildung, also nicht von Ordnung 2.

bilden eine Basis des k-Vektorraums A. Diese Elemente sind nämlich invariant beim inneren Automorphismus

$$A \longrightarrow A,\ x = (r^2)^{-1}x\bullet r^2$$

(trivialerweise bzw. wegen (2)). Dann sind aber alle Elemente von A invariant bei diesem Automorphismus, d.h. r^2 liegt im Zentrum von A. Weil A nach Voraussetzung zentral ist, folgt

(4) $$r^2 =: b \in k.$$

Aus den Identitäten (1), (4) und (2) erhalten wir

$$A \cong (a, b),$$

d.h. A ist eine Quaternionen-Algebra wie in (i) behauptet.
Wir haben noch zu zeigen, die Elemente (3) sind linear unabhängig. Zunächst beachten wir,

(5) 1 und q

liegen im Eigenraum zum Eigenwert 1 des Automorphismus

$$\sigma: A \longrightarrow A,\ x = q^{-1}xq.$$

Die Elemente

(6) r und qr

liegen im Eigenraum zum Eigenwert -1 dieses Automorphismus: für r gilt dies nach Wahl von r und für qr erhalten wir

$$\sigma(qr) = \sigma(q)\bullet\sigma(r) = (+q)(-r) = -qr.$$

Es reicht deshalb zu zeigen, die Elemente (5) und die Elemente (6) sind linear unabhängig. Für die Elemente (5) folgt dies aus (1). Wären die Elemente (6) linear abhängig, so wären es aber auch die Elemente (5) (man multipliziere mit r^{-1}).

<u>Beweis von (ii) ⇒ (iii).</u>
Wir bezeichnen mit N die Quaternionen-Algebra-Norm auf der Matrizen-Algebra,

$$N: A + A\sqrt{a} = A\otimes_k k(\sqrt{a}) \cong M_2(k(\sqrt{a})) \longrightarrow k(\sqrt{a}).$$

Nach dem Kriterium 1.1.11(iii) für das Zerfallen von Quaternionen-Algebren besitzt N eine nicht-triviale Nullstelle, d.h. es gibt Elemente

(1) $$q', q'' \in A,$$

die nicht beide Null sind, mit

$$N(q' + q''\sqrt{a}) = 0.$$

Bezeichne

$$B: A\otimes_k k(\sqrt{a}) \times A\otimes_k k(\sqrt{a}) \longrightarrow k(\sqrt{a})$$

die zur quadratischen Form N gehörige Bilinearform, d.h.

$$B(x, y) = \frac{1}{2}(N(x+y) - N(x) - N(y)) = \frac{1}{2}(x\bar{y} + y\bar{x}).$$

Man beachte, es gilt

$$B(x, x) = N(x).$$

Es gilt

$$\begin{aligned} 0 &= N(q'+q''\sqrt{a}) \\ &= B(q' + q''\sqrt{a}, q' + q''\sqrt{a}) \\ &= B(q',q') + a\bullet B(q'',q'') + 2\sqrt{a}\ B(q', q'') \\ &= N(q') + a\bullet N(q'') + 2\sqrt{a}\bullet B(q', q''). \end{aligned}$$

Wegen q', q" ∈ A liegen die Elemente N(q') + a•N(q") und B(q', q"). beide in k.[7] Da a nach Voraussetzung kein Quadrat ist in k, sind 1 und $\sqrt{a}$ linear unabhängig über k, d.h. es folgt

$$0 = N(q') + a \bullet N(q")$$

$$(2) \quad 0 = 2B(q', q") = q'\overline{q}" + q" \overline{q}'$$

Aus der ersten Identität folgt

$$N(q') = - a \bullet N(q") \neq 0$$

(da q' und q" nicht beide Null sind)[8]. Mit

---

[7] Sei

$$\sigma: M_2(k(\sqrt{a})) \longrightarrow M_2(k(\sqrt{a}))$$

der k-lineare Automorphismus, den das nicht-triviale Element der Galois-Gruppe G = Gal(k($\sqrt{a}$)/k) durch Operation auf dem rechten Tensorfaktor k($\sqrt{a}$) induziert. Dann ist A gerade der invariante Teil des Matrizenrings bezüglich σ:

$$A = M_2(k(\sqrt{a}))^{\sigma}.$$

Sei x ∈ A und

$$(1) \quad x = x' + x"$$

die Zerlegung von x in ein x' aus dem Grundkörper k($\sqrt{a}$) und ein reines Quaternion x". Dann ist auch

$$x = \sigma(x) = \sigma(x') + \sigma(x")$$

eine Zerlegung derselben Art. Da diese Zerlegung eindeutig ist, folgt

$$\sigma(x') = x' \text{ und } \sigma(x") = x",$$

also x' ∈ A und x"∈A. Die obige Zerlegung ist also eine Zerleguing in A. Insbesondere ist

$$N(x) = (x' + x")(x' - x") \in k(\sqrt{a}) \bigcap A.$$

Bezeichnet 1, u, v, w eine k-Vektorraumbasis von A, so bekommt der Durchschnitt rechts die Gestalt

$$k(\sqrt{a}) \bullet 1 \bigcap (k \bullet 1 + k \bullet u + k \bullet v + k \bullet w) \quad \text{in} \quad k(\sqrt{a}) \bullet 1 + k(\sqrt{a}) \bullet u + k(\sqrt{a}) \bullet v + k(\sqrt{a}) \bullet w,$$

d.h. es gilt

$$N(x) = x'^2 - x"^2 \in k.$$

Wir haben damit gezeigt, die Einschränkung der Quaternionen-Norm von $M_2(k(\sqrt{a}))$ auf A definiert eine nicht-entartete quadratische Norm

$$N: A \longrightarrow k.$$

Die Zerlegung (1) definiert eine direkte Summenzerlegung

$$(2) \quad A = k \oplus A"$$

wobei der 3-dimensionale Unterraum A" aus lauter reinen Quaternionen besteht. Die Quadratische Form N ist nicht identisch Null, denn dann wäre die Matrix von N bezüglich einer mit der Zerlegung (2) verträglichen Basis von der Gestalt

$$\begin{pmatrix} 0 & 0 & 0 & * \\ 0 & 0 & 0 & * \\ 0 & 0 & 0 & * \\ * & * & * & * \end{pmatrix}$$

Die ersten drei Spalten wären linear abhängig, die Matrix also vom Rang = 2. Das steht aber im Widerspruch dazu, daß die quadratische Form N nicht-entartet sein soll. Es gibt also ein

$$x \in A" - \{0\} \subseteq A - k,$$

dessen Norm

$$N(x) = (0 + x)(0 - x) = -x^2 \in k$$

von Null verschieden ist:

$$x^2 = y \in k$$

Die bereits bewiesene Implikation (iii) ⇒ (i) zeigt, daß A eine Quaternionen-Algebra ist.

$q''' := q'\overline{q}''$

erhalten wir

$$(q''')^2 = q'\overline{q}''\ q'\overline{q}''$$
$$= -\ q'\overline{q}',\ q''\overline{q}'' \qquad \text{(wegen (2) konjugiert)}$$
$$= -\ N(q')N(q'')$$
$$= a\ N(q'')^2$$

Mit

$$q = q'''/N(q'')^2$$

gilt also

$$q^2 = a,$$

d.h. q hat die in (iii) geforderter Eigenschaft. Man beachte, q liegt nicht in k, da a nach Voraussetzung in k kein Quadrat sein soll. Wir haben uns noch davon zu überzeugen, daß q in A liegt. Nach (1) gilt q', q'' ∈ A, also auch

$$q''' = q'\overline{q}'' \in A \text{ und } N(q'') \in k,$$

also

$$q = q'''/N(q'')^2 \in A.$$

QED.

1.2.4 Folgerung

Sei A eine 4-dimensionale zentrale k-Algebra. Dann sind folgende Aussagen äquivalent.

(i) A ist eine Quaternionen-Algebra über k.

(ii) Es gibt ein a ∈ k mit $A \otimes_k k(\sqrt{a}) \cong M_2(k(\sqrt{a}))$.

Beweis. Beweis von (i) ⇒ (ii). Siehe Theorem 1.2.3, Implikation (i) ⇒ (ii).

Beweis von (ii) ⇒ (i).

1. Fall: a ist kein Quadrat in k: siehe Theorem 1.2.3, Implikation (ii) ⇒ (i).

2. Fall: a ist ein Quadrat in k: Es gilt dann $k(\sqrt{a}) = k$, also

$$A \cong A \otimes_k k(\sqrt{a}) \cong M_2(k(\sqrt{a})) = M_2(k).$$

Die Algebra rechts ist nach 1.1.9 eine Quaternionen-Algebra.
QED.

1.2.5 Folgerung

Jede 4-dimensionale zentrale Divisionsalgebra ist eine Quaternionen-Algebra.[9]

Beweis. Sei D eine zentrale Divisionsalgebra über k der Dimension 4. Wir wählen ein Element

$$d \in D - k.$$

---

[8] Wir nehmen an dieser Stelle an, daß die gegebene Algebra A nicht zerfällt (wie wir oben gesehen haben, ist A ein Quaternionen-Algebra). Zerfällt A, so ist A isomorph zu $M_2(k)$ und die Matrix

$$\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} \in M_2(k)$$

definiert ein Element von q ∈ A - k mit

$$q^2 = \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = b \cdot 1 \in k.$$

Mit anderen Worten, die zu beweisende Aussage ist trivialerweise richtig.

[9] d.h. die zentralen Divisionsalgebren fallen mit den nicht-zerfallenden Quaternionen-Algebren zusammen.

Da D als Vektorraum endlich-dimensional ist, sind die Vektoren

$$1, d, d^2, d^3, \ldots$$

linear unabhängig über k. Es gibt also ein Polynom

$$f \in k[x] \text{ mit } f(d) = 0.$$

Als Schiefkörper ist D nullteilerfrei. Wir können also annehmen,

$$f \text{ ist irreduzibel über } k.$$

Der natürliche k-Algebra-Homomorphismus

$$k[x] \longrightarrow D,\ p(x) = p(d),$$

induziert einen k-Algebra-Homomorphismus

$$k(d) \overset{\cong}{\longrightarrow} k[x]/(f) \longrightarrow D,\ p(x) \bmod f = p(d),$$

welcher mit der natürlichen Einbettung der k-Teilalgebra k(d) in D zusammenfällt. Der Grad

$$[k(d):k]$$

der Körpererweiterung k(d)/k kann nicht gleich 1 sein, weil d nicht in k liegt. Er kann aber auch nicht gleich 4 sein, denn dann wäre D = k(d) kommutativ, also nicht zentral. Es folgt

$$[k(d):k] = 2.$$

Das Minimalpolynom f von d ist quadratisch,

$$f(x) = x^2 + ux + v = (x + \tfrac{1}{2}u)^2 - (\tfrac{1}{4}u^2 - v),\ u, v \in k.$$

Dann ist aber

$$q := d + \tfrac{1}{2}u$$

ein Element von D - k mit $q^2 = (\tfrac{1}{4}u^2 - v) \in k$. Nach Aussage (iii) von Theorem 1.2.3 ist D eine Quaternionen-Algebra.
QED.

1.2.6 Eine Beschreibung der Quaternionen-Norm

Seien $K = k(\sqrt{a})$ ein Zerfällungskörper der Quaternionen-Algebra $(a, b)_k$ (vgl. 1.2.3),

$$q \in (a, b)$$

ein Element und

$$\psi: (a, b) \otimes_k K \overset{\cong}{\longrightarrow} M_2(K)$$

ein K-Isomorphismus. Dann gilt

$$N(q) = \det(\psi(q)).$$

Beweis. 1. Schritt: Der Wert der Determinante,

$$\det(\psi(q))$$

hängt nicht von der speziellen Wahl des K-Isomorphismus ψ ab,

Sei

$$\psi': (a, b) \otimes_k K \overset{\cong}{\longrightarrow} M_2(K)$$

zweiter solcher Isomorphismus, so ist

$$\psi' \circ \psi^{-1}: M_2(K) \longrightarrow M_2(K)$$

ein Automorphismus von $M_2(K)$, also von der Gestalt

$$\psi' \circ \psi^{-1}(M) = C^{-1}MC$$

mit einer Matrix $C \in M_2(K)$.[10] Insbesondere der ist

$$\det(\psi' \circ \psi^{-1}(M)) = \det M \text{ für jedes } M,$$

also

$$\det \psi'(M) = \det \psi(M) \text{ für jedes } M.$$

2. Schritt: Reduktion auf den Fall $A = M_2(K)$.

Die Quaternionen-Norm auf $(a, b)_k$ ist gerade die Einschränkung der Quaternionen-Norm auf $(a, b)_K$, d.h. das folgende Diagramm ist kommutativ.

$$\begin{array}{ccc} (a,b)_k & \xrightarrow{N} & k \\ \cap & & \cap \\ (a, b)_K & \xrightarrow{N} & K \end{array}$$

Es reicht zu zeigen, die untere Zeile des Diagramms wird zur Determinante, wenn man $(a, b)_K$ vermittels ψ mit $M_2^{\bullet}(K)$ identifiziert. Da es nach dem ersten Schritt nicht auf die spezielle Wahl des Isomorphismus ψ ankommt, reicht es zu zeigen, die Quaternionen-Norm von

$$A = (1, 1) = M_2(K)$$

(die nach 1.1.8 nicht von der speziellen Wahl der Basis abhängt)[11] fällt mit der Determinanten-Abbildung zusammen.

3. Schritt: der Fall $A = (1, 1) = M_2(K)$.

Wir wählen die in 1.1.9 beschriebene Basis von $M_2(K)$ mit $b = 1$:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, i := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, j := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, ij = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

und schreiben das Element

$$q = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(K)$$

als Linearkombination der Basiselemente:

---

[10] Wir werden diese Aussage in 2.4 für $M_n(K)$, beliebige n und beliebige Körper beweisen. Im Fall n = 2 kann man sie durch direkte Rechnung beweisen: Wir schreiben

$$M_2(K) = K \bullet E_{11} + K \bullet E_{12} + K \bullet E_{21} + K \bullet E_{22},$$

wenn E_{ij} die 2×2-Matrix mit einer Eins in der Position (i,j) und Nullen in allen anderen Positionen ist. Die multiplikative Struktur des Matrizenrings ist gegeben durch die Relationen

$$\begin{array}{llll} E_{11} \bullet E_{11} = E_{11}, & E_{11} \bullet E_{12} = E_{12}, & E_{11} \bullet E_{21} = 0, & E_{11} \bullet E_{22} = 0 \\ E_{12} \bullet E_{11} = 0, & E_{12} \bullet E_{12} = 0, & E_{12} \bullet E_{21} = E_{11}, & E_{12} \bullet E_{22} = E_{12} \\ E_{21} \bullet E_{11} = E_{21}, & E_{21} \bullet E_{12} = E_{22}, & E_{21} \bullet E_{21} = 0, & E_{21} \bullet E_{22} = 0 \\ E_{22} \bullet E_{11} = 0, & E_{22} \bullet E_{12} = 0, & E_{22} \bullet E_{21} = E_{21}, & E_{22} \bullet E_{22} = E_{22} \end{array}$$

(allgemeiner, $E_{\alpha\beta} E_{\gamma\delta} = \delta_{\beta\gamma} \bullet E_{\alpha\delta}$). Ein Automorphismus der Matrizenalgebra ist durch eine 4×4-Matrix (bezüglich der Basis der E_{ij}) gegeben, und die Multiplikation mit dieser Matrix erhält die obigen 16 Relationen. Dies liefert Bedingungen an die Koeffizienten der Matrix und führt dazu, daß die Abbildung die behautptete Gestalt hat.

[11] Die Bedingung, ein reines Quaternion zu sein, hängt außerdem auch nicht von der speziellen Wahl von b sondern nur von der multiplikativen Struktur der Algebra ab.

$$q = \frac{x+w}{2} \bullet 1 + \frac{x-w}{2} \bullet i + \frac{y+z}{2} \bullet j + \frac{y-z}{2} \bullet ij$$

In 1.1.6 Bemerkung (i) haben wir eine Formel angegeben, die die Norm durch die Koordinaten des Quaternions ausdrückt. Nach dieser Formel gilt

$$\begin{aligned} N(q) &= \frac{1}{4}(x+w)^2 - \frac{1}{4}(x-w)^2 - \frac{1}{4}(y+z)^2 + \frac{1}{4}(y-z)^2 \\ &= xw - yz \\ &= \det\begin{pmatrix} x & y \\ z & w \end{pmatrix} \end{aligned}$$

QED.

1.3 Der zugehörige Kegelschnitt

1.3.1 Definition

Der zur Quaternionen-Algebra

$$(a, b)_k$$

gehörige Kegelschnitt ist definiert als die ebene proejektive Kurve

$$C(a, b) = V(aX^2+bY^2-Z^2)$$

mit der Gleichung

$$aX^2+bY^2-Z^2 = 0.$$

Mit anderen Worten, für jede Körper-Erweiterung K/k ist die Menge der K-rationalen Punkte von C(a, b) gerade die Menge

$$C(a, b)(K) := \{[x, y, z] \in \mathbb{P}^2_K \mid ax^2+by^2 - z^2 = 0\}.$$

Bemerkungen

(i) Im Fall $(1, 1)_k = M_2(k)$ ist der zugehörige Kegelschnitt gerade der gewöhnliche Einheitskreis mit der Gleichung

$$X^2 + Y^2 = Z^2.$$

(ii) Der zu (a, b) gehörige Kegelschnitt C(a, b) hängt bis auf Isomorphie nicht von der speziellen Wahl der Basis von (a, b) ab. Dazu beachten wir, C(a, b) ist isomorph zum Kegelschnitt mit der Gleichung

(1) $$aX^2 + bY^2 = abZ^2$$

(man führe die Koordinatentransformation X = Y/a, Y = X/b, Z = Z durch und multiplizieren die entstehende Gleichung mit ab). Nun ist aber

$$-aX^2 - bY^2 + abZ^2$$

gerade die Norm des reinen Quadernions Xi + Yj + Zij. Die Einschränkung der Norm auf den Raum der reinen Quaternionen ist aber eine von der Wahl der Koordinaten unabhängige Abbildung.

(iii) Sind zwei Quaternionen-Algebren (a, b) und (c, d) isomorph, so sind es auch die zugehörigen Kegelschnitte:

Auf Grund der Isomorphie von (a, b) und (c, d) gibt es eine Vektorraumbasis von (a, b), bezüglich welcher das Multiplikationsgesetz gerade die Gestalt des Multiplikationsgesetzes von (c, d) annimmt. Die den Basiswechsel beschreibende homogene lineare Transformation der i, j, ij überführt gerade die Gleichung von C(a, b) in die Gleichung von C(c, d).

1.3.2 Rationale Punkte

Ein <u>rationaler Punkt</u> von C(a, b) ist ein Punkt von C(a, b)(k), d.h. eine Nullstelle [x, y, z] von

$$aX^2 + bY^2 - Z^2,$$

mit $x, y, z \in k$.

1.3.3 Kriterium für zerfallende Quaternionen-Algebren

Für beliebige a, b ∈ k sind folgende Aussagen äquivalent.

(i) $(a, b)_k$ zerfällt.

(ii) C(a, b) besitzt einen rationalen Punkt.

Beweis. Fall 1: a ist ein Quadrat in k.

Dann zerfällt (a, b) nach 1.1.9. Andererseits ist mit $a = u^2$, u ∈ k die Gleichung von C(a,b) von der Gestalt

$$aX^2 + bY^2 - Z^2 = (uX + Z)(uX - Z) + bY^2$$

hat also die Nullstelle [1, 0, ±u].

Fall 2: a ist kein Quadrat in k.

Beweis der Implikation (ii) ⇒ (i).

Sei [x, y, z] ein Punkt von C(a, b) mit x, y, z ∈ k. Eine der drei Koordinaten muß ≠ 0 sind.

Fall 2.1: y ≠ 0.

Dann gilt

$$b = (z^2 - ax^2)/y^2 = (\frac{z}{y})^2 - a\bullet(\frac{x}{y})^2 = N(\frac{z}{y} + \frac{x}{y}\sqrt{a}\,).$$

Nach Bedingung (iv) von 1.1.11 zerfällt die Algebra (a, b).

Fall 2.2: y = 0.

Dann kann x nicht Null sein (denn dann wäre auch z = 0). Dann folgt analog, daß a Norm eines Elements der Körpererweiterung $k(\sqrt{b})/k$ ist und dasselbe Argument impliziert das Zerfallen der Algebra

$$(a, b) \cong (b, a).$$

Beweis der Implikation (i) ⇒ (ii).

Wenn (a, b) zerfälllt, so ist b Norm eines Elements der Erweiterung $k(\sqrt{a})/k$ (nach 1.1.11).

Weil a kein Quadrat in k ist, bedeutet dies, es gibt Elemente r, s ∈ k mit

$$b = r^2 - a\bullet s^2.$$

Mit anderen Worten, [s, 1, r] ist ein rationaler Punkt von C(a, b).

QED.

1.3.4 Beispiel

Für a ≠ 1 besitzt der projektive Kegelschnitt

$$aX^2 + (1 - a)Y^2 = Z^2$$

den k-rationalen Punkt [1, 1, 1]. Mit anderen Worten, die Quaternionen-Algebra

$$(a , 1 - a) \text{ zerfällt.}$$

Diese unschuldig aussehende Tatsache stellt einen Spezialfall der sogenannten Steinberg-Relation für Symbole dar, der wir später begegnen werden.

1.3.5 Zerfallen und Isomorphie zur projektiven Geraden

Eine wohlbekannte Tatsache der algebraischen Geometrie besagt, daß ein glatter projektiver über k definierter Kegelschnitt genau dann über k isomorph ist zur projektven Geraden $\mathbb{P}^1$, wenn er einen k-rationalen Punkt besitzt. Der Isomorphismus ordnet jedem Punkt des Kegelschnitts die Verbindungsgerade mit einem fest gegebenen rationalen Punkt O zu und geht dann zum Schnitt dieser Verbindungsgeraden mit einem $\mathbb{P}^1$ über, der so in die projektive Ebene eingebettet ist, daß er den Punkt O nicht enthält.

Man erhält auf diese Weise eine weitere zum Zerfallen einer Quaternionen-Algebra äquivalente Bedingung:

$(a, b)_k$ zerfällt genau dann, wenn C(a,b) über k isomorph ist zum $\mathbb{P}^1$.

Wir werden diese Bedingung später in wesentlicher Weise verallgemeinern.

Bemerkung

Im Rest des Abschnitts geben wir Beispiele dafür an, wie man das Kriterium 1.3.3 verwenden kann, um Sätze zum Zerfallen von Quaternionen-Algebren über speziellen Körpern zu beweisen.

1.3.6 Beispiel: das Zerfallen über endlichen Körpern

Sei k der endliche Körper mit q Elementen (q ungerade). Dann zerfällt jede Quaternionen-Algebra

$$(a, b)_k .$$

Beweis. Die multiplikative Gruppe k von k ist isomorph zur zyklischen Gruppe der Ordnung q-1, d.h. zu $\mathbb{Z}/(q-1)$. Der Homomorphismus

(1) $$\varphi: k \longrightarrow k,\ x = x^2,$$

läßt sich deshalb mit dem additiv geschriebenen Homomorphismus

$$\mathbb{Z}/(q-1) \longrightarrow \mathbb{Z}/(q-1),\ \overline{x} = 2\overline{x},$$

identifizieren. Die Restklasse $\overline{x}$ von x liegt genau dann im Kern, wenn $q-1 \mid 2x$ gilt, d.h. wenn x ein Vielfaches von $\frac{q-1}{2}$ ist. Für die zugehörige Restklasse gibt es damit nur 2 Möglichkeiten, d.h. es ist

$$\#\,\mathrm{Ker}(\varphi) = 2$$

Das Bild des Homomorphismus (1) ist isomorph zu $k/\mathrm{Ker}(\varphi)$, besteht also aus

$$\frac{q-1}{2}$$

Elementen. Mit anderen Worten, die Anzahl der Quadrate in k ist gleich

$$\frac{q-1}{2} + 1$$

(weil 0 ein Quadrat ist). Je der beiden folgenden Mengen besteht damit aus $\frac{q-1}{2} + 1$ Elementen:

$$\{ax^2 \mid x \in k\} \text{ und } \{1 - bx^2 \mid x \in k\}.$$

Da k aus q Elementen besteht, besitzen die beiden Mengen ein gemeinsames Element, d.h. es gibt ein $x, y \in k$ mit

$$ax^2 = 1 - by^2$$

d.h. mit

$$ax^2 + by^2 = 1.$$

Die Kurve C(a,b) besitzt einen k-rationalen Punkt, d.h. (a, b) zerfällt über k.

QED.

1.3.7 Formale Laurent-Reihen

Wir bezeichnen mit

$$k[[x]]$$

den Ring der formalen Potenzreihen in x mit Koeffizienten aus k.

Bemerkungen

(i) Der Ring k[[x]] besteht aus allen formalen Summen der Gestalt

$$c_0 + c_1 x + c_2 x^2 + \ldots \text{ mit } c_i \in k \text{ für jedes } i,$$

wobei die Zahl der Summanden unendlich sein kann.

(ii) Mit Hilfe der Identität

$$(1 - x)\,(1 + x + x^2 + \dots) = 1$$

sieht man leicht, daß jedes Element mit $c_0 \neq 0$ in k[[x]] eine Einheit ist. Insbesondere hat jedes Element von k[[x]] die Gestalt

$$x^n \cdot u$$

mit einer Einheit u und einer nicht-negativen ganzen Zahl n.

(iii) Durch Betrachtung der Anfangsglieder von Potenzreihen sieht man, daß k[[x]] nullteilerfrei ist. Der volle Quotientenring von k[[x]] wird mit

$$k((x))$$

bezeichnet und heißt Ring der formalen Laurent-Reihen.

(iv) Die Ideale von k[[x]] haben die Gestalt

$$(x^n).$$

Insbesondere ist k[[x]] ein Hauptidealring mit dem einzigen maximalen Ideal (x). Aus der expliziten Beschreibung der Ideale ergibt sich außerdem, daß k[[x]] ein ZPE-Ring ist, dessen Primelemente alle assoziiert sind zu x.

(v) Die Abbildung

$$k[[x]] \longrightarrow k,\ p(x) = p(0),$$

ist ein surjektiver k-Algebra-Homomorphismus mit dem Kern (x). Er heißt Spezialisierungs-Homomorphismus.

1.3.8 Beispiel: Das Tensorprodukt (a,b)⊗k((w))

Für jede Quaternionen-Algebra (a, b) über k sind folgende Aussagen äquivalent.

(i) $(a, b)_k$ zerfällt.

(ii) $(a, b)_{k((w))}$ zerfällt.

Beweis. (i) ⇒ (ii). trivial.

(ii) ⇒ (i). Nach 1.3.3 besitzt C(a, b) einen rationalen Punkt

$$[x_w , y_w, z_w] \text{ mit } x_w , y_w, z_w \in k((w)).$$

Durch Multiplikation mit einer Potenz von w erreichen wir, daß sogar

$$x_w , y_w, z_w \in k[[w]]$$

gilt. Da mindestens eine Koordinate $\neq 0$ ist, können wir annehmen, daß die Absolutglieder dieser Potenzreihen nicht alle gleich Null sind, d.h.

$$[x_w(0) , y_w(0), z_w(0)]$$

ist ein wohldefiniert k-rationaler Punkt der projektiven Ebene. Nach Konstruktion liegt er auf der Kurve C(a, b). Nach 1.3.3 zerfällt $(a, b)_k$.

QED.

1.3.9 Beipiel: ein Zerfällungskriterium über k((w))

Für jedes $a \in k$ sind folgende Aussagen äquivalent.

(i) $(a, w)_{k((w))}$ zerfällt.

(ii) a ist ein Quadrat in k.

Beweis. (ii) $\Rightarrow$ (i). Trivial (vgl. Beispiel 1.1.9 - die Matrizen-Algbra $M_2(k)$).

(i) $\Rightarrow$ (ii). Nach 1.3.3 besitzt C(a, b) einen rationalen Punkt

$$[x_w , y_w, z_w] \text{ mit } x_w , y_w, z_w \in k((w)).$$

Wie oben können wir wieder annehmen,

$$x_w , y_w, z_w \in k[[w]],$$

wobei mindestens eine der drei Potenzreihen ein von Null verschiedenes Absolutglied besitzt. Es gilt

(1) $$a \bullet x_w^2 + w \bullet y_w^2 = z_w^2$$

Sind x_w und z_w durch w teilbar, so gilt dasselbe auch für y_w. Wir können also annehmen, x_w und z_w sind nicht beide durch w teilbar, d.h.

$$x_w(0) \text{ und } z_w(0) \text{ sind nicht beide gleich Null.}$$

Wir setzen w = 0 und erhalten aus (1):

$$a \bullet x_w^2(0) = z_w^2(0).$$

Auf beiden Seiten muß insbesondere ein von 0 verschiedener Wert stehen. Also ist

$$a = (z_w(0)/x_w(0))^2$$

ein Quadrat in k.
QED.

1.4. Ein Theorem von Witt

In diesem Abschnitt wollen wir einen Satz beweisen, welcher die Isomorphieklassen von Quaternionen-Algebren mit Hilfe der Funktionen-Körper der zugeordneten Kegelschnitte beschreibt. Eine kurze Einführung in die in diesem Abschnitt verwendeten Grundbegriffe der algebraischen Geometrie findet sich im Anhang A0.1 Affine und quasi-projektive Varietäten.

1.4.1 Der Satz von Witt

Seien

$$(a_1, b_1)_k \text{ und } (a_2, b_2)_k$$

Quaternionen-Algebren und

$$C_1 := C(a_1, b_1) \text{ und } C_2 = C(a_2, b_2)$$

die zugehörigen Kegelschnitte. Dann sind folgende Aussagen äquivalent.

(i) $(a_1, b_1)_k$ und (a_2, b_2) sind isomorph als k-Algebren

(ii) $k(C_1)$ und $k(C_2)$ sind isomorph als k-Algebren.

Bemerkungen

(i) Da zwei glatte irreduzible projektive Kurven genau dann isomorph sind, wenn ihre Funktionenkörper es sind, kann man den Satz von Witt auch wie folgt formulieren.

(ii) Zwei Quaternionen-Algebren über k sind genau dann isomorph, wenn die zugehörigen Kegelschnitte als algebraische Kurven isomorph sind.

(iii) Der Beweis des Satzes von Witt wird sich als eine Konsequenz der nachfolgenden Aussage ergeben.

1.4.2 Isomorphie-Kriterium für Quaternionen-Algebren

Sei

$$(a, b)_k$$

eine Quaternionen-Algebra mit dem zugehörigen Kegelschnitt C und

$$Q$$

eine weitere Quaternionen-Algebra über k. Es gelte:

(i) $Q \otimes_k k(C)$ zerfällt.

(ii) Q zerfällt nicht (über k).

Dann gilt

$$Q \cong (a, b)_k.$$

Beweis des Satzes von Witt 1.4.1 mit Hilf des Kriteriums 1.4.2.

Beweis von (i) $\Rightarrow$ (ii). Sei

$$(a_1, b_1)_k \cong (a_2, b_2)_k$$

Dann sind auch die zugehörigen Kegelschnitte isomorph,

$$C_1 \cong C_2$$

(nach Bemerkung 1.3.1 (iii)). Dann sind die Kegelschnitte aber erst recht birational äquivalent, haben also isomorphe rationale Funktionenkörper.

Beweis von (ii) $\Rightarrow$ (i). Sei

$$k(C_1) \cong k(C_2) \text{ über } k.$$

Zerfallen die beiden Quaternionen-Algebren, so sind die zugehörigen Kegelschnitte C_1 und C_2 isomorph zur projektiven Geraden (nach 1.3.5), also untereinander isomorph. Also sind es auch die zugehörigen Quaternionen-Algebren (nach Bemerkung 1.3.1(iii)).

Wir können also annehmen,

(1) $(a_1, b_1)_k$ zerfällt nicht.

Nach Bemerkung 1.4.9 (vii) zerfällt die Algebra

$$(a_1, b_1)_k \otimes_k k(C_1).$$

Das bedeutet aber auch, daß

(2) $(a_1, b_1)_k \otimes_k k(C_2)$ zerfällt

(da die beiden rationalen Funktionenkörper isomorph sind). Die Aussagen (1) und (2) bedeuten, die beiden Bedingungen von Kriterium 1.4.10 sind erfüllt für

$$Q = (a_1, b_1)_k \text{ und } C = C_2 \text{ (d.h. } (a, b) = (a_2, b_2)).$$

Wir wenden 1.4.10 an und erhalten

$$Q \cong (a_2, b_2)_k .$$

Das ist aber gerade die Aussage von (i).

QED.

Bemerkung

Zum Beweis von 1.4.10 benötigen wir die folgende Aussage.

1.4.3 Lemma

Ist $c \in k^*$ Norm eines Elements der Körpererweiterung $k(\sqrt{a})/k$, so gilt

$$(a, b)_k \cong (a, bc)_k.$$

Beweis. Ist a ein Quadrat in k, so zerfallen beide Quaternionen-Algebren und die Aussage ist trivial. Wir können also annehmen, a ist kein Quadrat in k. Dann hat c nach Voraussetzung die Gestalt

$$c = x^2 - ay^2 \text{ mit } x, y \in k.$$

Betrachten wir die Quaternionen

$$q := x + yi + 0j + 0ij$$

und

$$J := qj = xj + yij.$$

Das Quaternion q hat die Norm

$$N(q) = (x + yi)(x - yi) = x^2 - ay^2 = c$$

und für das reine Quaternion J gilt

$$iJ + Ji = (xij + ayj) + (-xij - ayj) = 0$$

$$J^2 =^{12} - N(J) = - N(q)N(j) = j^2N(q) = bc.$$

Es reicht also zu zeigen, die Elemente

$$1, i, J, iJ$$

bilden eine k-Vektorraumbasis von (a, b). Die Matrix der k-linearen Abbildung mit

$$1 = 1, i = i, j = J, ij = iJ$$

ist gleich

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x & ay \\ 0 & 0 & y & x \end{pmatrix}$$

Die Determinante dieser Matrix ist gleich $x^2 - ay^2 = c$, also von Null verschieden. Die lineare Abbildung ist ein Isomorphismus, d.h. angegebenen Elemente bilden eine Basis. **QED**.

1.4.4 Beweis des Isomorphie-Kriteriums 1.4.2

Nach 1.3.5 zerfällt jede Quaternionen-Algebra über einem endlichen Körper. Die Aussage des Kriteriums ist in diesem Fall leer. Wir können zum Beweis also annehmen,

$$k \text{ ist unendlich.}$$

1. Schritt. $(a, b)_k$ zerfällt nicht.

Andernfalls wäre der zugehörige Kegelschnitt isomorph zur projektiven Geraden, d.h. der Körper k(C) der rationalen Funktionen auf C ist isomorph zum rationalen Funktionenkörper in einer Unbestimmten,

$$k(C) \cong k(u), \text{ u Unbestimmte.}$$

Nach Voraussetzung zerfällt aber die Quaternionen-Algebra

$$Q \otimes_k k(C) \cong Q \otimes_k k(u),$$

d.h. die Quaternionen-Norm

$$N_Q : Q \longrightarrow k$$

hat eine nicht-triviale Nullstelle über k(u) (nach 1.1.11). Mit anderen Worten, es gibt rationale Funktionen

$$x, y, z, w \in k(u),$$

welche nicht alle gleich Null sind und derart, daß das Quaternion von Q mit den Koordinaten x, y, z, w die Norm Null hat,

$$x^2 - a(Q) \cdot y^2 - b(Q) \cdot z^2 + a(Q)b(Q) \cdot w^2 = 0.$$

---

[12] Als reines Quaternion ist J gleich dem Negativen seines Konjugierten.

Durch Multiplikation mit dem Quadrat des Hauptnenners erreichen wir, daß die Koordinaten sogar Polynome sind,

$$x, y, z, w \in k[u].$$

Weil k unendlich ist, gibt es ein $t \in k$ derart, daß mindestens einer der Werte

$$x(t), y(t), z(t), w(t)$$

ungleich Null ist. Damit besizt jedoch die Quaternionen-Norm N_Q aber eine nicht-triviale Nullstelle über k. Dann müßte aber Q zerfallen (über k) im Widerspruch zur Voraussetzung (ii) des Kriteriums. Dieser Widerspruch beweist die Aussage des ersten Schritts.

Folgerungen

1. Die Quaternionen-Norm auf $(a, b)_k$ besitzt keine Nullstelle (außer der trivialen).
2. $(a, b)_k$ eine Divisionsalgebra (nach 1.1.7).
3. Das Element a ist kein Quadrat in k.
4- $(a, b)_k \otimes_k L \cong M_2(L)$ für $L := k(\sqrt{a})$ (nach Theorem 1.2.3).
5. $L(C) \cong$[13] $L \otimes_k k(C) \cong$[14] $L \otimes_k k(u) \cong$[15] $L(u)$.
6. $Q \otimes_k L = Q \otimes_k k(\sqrt{a})$ zerfällt.[16]
7. Es gibt ein $c \in k^*$ mit $Q \cong (a, c)_k$ (nach Theorem 1.2.3).
8. Es gibt ein $f \in L(C)^*$ mit $N_{L(C)/k(C)}(f) = c$.[17]

---

[13] Für Polynomringe gilt

$$L \otimes_k k[x_1,...,x_n] \cong L[x_1,...,x_n]$$

(weil das Tensorprodukt mit direkten Summen kommutiert). Für affine Varietäten folgt damit (durch Faktorisieren nach den definierenden Idealen - wegen der Rechtsexaktheit des Tensorprodukts)

$$L \otimes_k k[V] \cong L[V].$$

Ist V irreduzibel über L, so können wir zum Quotientenkörper übergehen und erhalten

$$L(V) \cong Q(L \otimes_k k[V]) \supseteq L \otimes_k k(V).$$

Ist L/k eine endliche Körpererweiterung, so steht rechts eine nullteilerfreie k(V)-Algebra, die als k(V)-Vektorraum endlich-dimensional ist, also ein Körper. Nach Definition des Quotientenkörpers (als kleinster Körper, der die Algebra enthält) muß rechts das Gleichheitszeichen stehen.

[14] Wegen $k(C) \cong k(u)$.

[15] Nach demselben Argument wie für die Isomorphie ganz rechts.

[16] Nach Voraussetzung (i) des Kriteriums zerfällt

$$Q \otimes_k k(C) = Q_{k(C)}$$

Dann zerfällt die Algebra aber erst recht über jeden noch größeren Körper. Insbesondere zerfällt die Algebra

$$Q_{L(C)} = (Q_L)_{L(C)} = Q_L \otimes_L L(C) = Q_L \otimes_L L(u).$$

Nach demselben Argument wie im ersten Schritt zerfallt dann aber die Algebra

$$Q_L = Q \otimes_k L$$

(man betrachte rationale Funktionen mit Koeffizienten in L und erweitere mit dem Hauptnenner).

[17] Nach Voraussetzung (i) des Kriteriums zerfällt $Q \otimes_k k(C) = (a, c)_{k(C)}$. Nach 1.1.11 ist dann aber c

Norm eines Elements der quadratischen Erweiterung $k(C)(\sqrt{a}) = k(\sqrt{a}) \otimes_k k(C) = L \otimes_k k(C) = L(C)$.

Unser nächstes Ziel ist es, das Element f genauer zu beschreiben, um danach das Element c zu bestimmen.

2. Schritt. Eine Beschreibung des Divisors div(f) der rationalen Funktion $f \in L(C)^*$. Der Körper L(C) ist der Körper der rationalen Funktionen auf der Kurve

$$C_L$$

welche aus der über k definierten Kurve C entsteht durch den Übergang zur quadratischen Erweiterung $L = k(\sqrt{a})$. Diese Kurve ist isomorph zur projektiven Geraden[18],

$$C_L \cong \mathbb{P}^1_L .$$

Wir betrachten die Abbildung

$$\text{div}: L(C)^* \longrightarrow \text{Div}(C_L)$$

und die zugehörige exakte Sequenz

$$0 \longrightarrow L(C)^*/L^* \xrightarrow{\text{div}} \text{Div}(C_L) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 0$$

(vgl. Bemerkung 1.4.7(v)). Weiter sei

$$G := \text{Gal}(L/k) = \{1, \sigma\}$$

die Galois-Gruppe der quadratischen Erweiterung $L/k = k(\sqrt{a})/k$.[19] Die Operation von σ auf L induziert eine Operation von σ auf L(C).[20] Außerdem operiert das Element σ auf $\text{Div}(C_L)$ indem es jeden Primdivisor in den zugehörigen konjugierten Primdivisor überführt.[21] Die Abbildung div ist mit diesen Operationen (nach Konstruktion) verträglich:

---

[18] Weil $(a, b)_k$ über $L = k(\sqrt{a})$ zerfällt.

[19] Die Erweiterung ist separabel, weil die Charakteristik von k ungleich 2 ist: die Ableitung des Minimalpolynoms $X^2 - a$ ist nicht identisch Null.

[20] Betrachten wir C_L der Einfachheit halber als affine über k definierte Kurve C, d.h.

$$C_L = V(f_1,...,f_m) \subseteq \mathbb{A}^n_L$$

wobei die definierenden Gleichungen Polynome mit Koeffizienten aus k sind,

$$f_i \in k[x_1,...,x_n].$$

Betrachten wir die Abbildung

$$L[x_1,...,x_n] \longrightarrow L[x_1,...,x_n],\ f = f^\sigma,$$

wobei f^σ aus f entstehe, indem man σ auf die Koeffizienten von f anwendet. Weil die Koeffizienten der f_i in k liegen, bleiben sie bei dieser Abbildung unverändert. Insbesondere überführt diese Abbildung das von den f_i erzeugte Ideal in sich. Nach dem Homomorphiesatz erhält man einen k-Algebra-Homomorphismus

$$L[C] \longrightarrow L[C]$$

und durch Übergang zu den Quotientenkörpern einen Homomorphismus

$$L(C) \longrightarrow L(C).$$

Warnung: die Isomorphie $L(C) \cong L(u)$ ist nicht notwendig über k definiert. Der eben konstruierte Isomorphismus muß also nicht unbedingt mit der in offensichtlicher Weise durch σ auf L(u) definierten Abbildung übereinstimmen.

[21] Faßt man C als affine Kurve auf, so überführt die Operation von σ auf L[C] maximale Ideale in maximale Ideale. Da sich die projektive Kurve C überdecken läßt durch über k definierte affine Kurven, erhält man so für jeden Primdivisor ein wohldefiniertes (und von der Wahl der affinen Überdeckung unabhängiges) Bild.

$$\mathrm{div}(\sigma\bullet\alpha) = \sigma\bullet\mathrm{div}(\alpha).$$

Der Grad eines Divisors ändert sich nicht, wenn man σ auf ihn anwendet,[22]

$$\deg(\sigma\bullet D) = \deg(D).$$

Wir können also $\mathbb{Z}$ mit der trivialen Operation versehen und erhalten so eine exakte Sequenz von G-äquivarianten Homomorphismen. Da die Abbildung div ein Homomorphismus ist, folgt

$$\begin{aligned}(1+\sigma)\mathrm{div}(f) &= \mathrm{div}(f) + \sigma\bullet\mathrm{div}(f)\\ &= \mathrm{div}(f) + \mathrm{div}(\sigma\bullet f)\\ &= \mathrm{div}(f\bullet\sigma(f))\\ &=^{23} \mathrm{div}(N(f))\\ &= \mathrm{div}(c) \qquad \text{(nach Wahl von f)}\\ &= 0. \qquad \text{(weil c eine Konstante aus k* ist).}\end{aligned}$$

Wir betrachten die Zerlegung

$$\mathrm{Div}(C_L) = \Big(\bigoplus_{p = \sigma(p)} \mathbb{Z}\bullet p\Big) \oplus \Big(\bigoplus_{p \neq \sigma(p)} \mathbb{Z}\bullet p\Big).$$

Der Automorphismus σ operiert trivial auf dem ersten direkten Summanden und durch Tranpositionen auf dem zweiten. Schreiben wir entsprechend dieser Zerlegung

$$\mathrm{div}(f) = E_1 + E_2.$$

Dann gilt

$$0 = (1+\sigma)\bullet\mathrm{div}(f) = (E_1 + E_2) + \sigma\bullet(E_1 + E_2) = 2\bullet E_1 + (1+\sigma)E_2$$

Weil die Zerlegung direkt ist, folgt

$$2\bullet E_1 = 0 \text{ und } (1+\sigma)E_2 = 0,$$

also

$$E_1 = 0 \text{ und } E_2 =^{24} \sum_{i=1}^{r} (m_i\bullet p_i - m_i\sigma\bullet p_i)$$

---

[22] Es reicht, dies für Primdivisoren m zu überprüfen. Ist L[C] der Koordinatenring einer affinen Umgebung von m, so gilt nach Definition des Grades

$$\deg m = [L[C]/m : L]$$

Der Isomorphismus σ: L[C] $\longrightarrow$ L[C] bildet m in $\sigma\bullet$m ab und induziert also einen Isomorphismus

$$L[C]/m \longrightarrow L[C]/\sigma\bullet m.$$

Die Grade über L der beiden Körper sind somit gleich, d.h. deg m = deg $\sigma\bullet$m.

[23] Wir bezeichnen hier die Norm der quadratischen Erweiterung L(C)/k(C) mit N.

[24] Jedenfalls kann man E_2 in der Gestalt

$$E_2 = \sum_{i=1}^{r} (m_i\bullet p_i - n_i\sigma\bullet p_i)$$

schreiben, wobei die Primdivisoren $p_1, \dots, p_r$ paarweise nicht konjugiert sind. Die Primdivisoren

$$p_1, \dots, p_r, \sigma\bullet p_1, \dots, \sigma\bullet p_r$$

sind dann paarweise verschieden. Wegen $\sigma^2 = 1$ und

$$\begin{aligned}0 &= (1+\sigma)\bullet E_2\\ &= \sum_{i=1}^{r} (m_i\bullet p_i - n_i\sigma\bullet p_i) + \sum_{i=1}^{r} (m_i\bullet \sigma\bullet p_i - n_i\, p_i)\\ &= \sum_{i=1}^{r} ((m_i-n_i)\bullet p_i + (m_i - n_i)\sigma\bullet p_i)\end{aligned}$$

mit abgeschlossenen Punkten $p_1, \ldots, p_r$ und von Null verschiedene Koeffizienten m_i. Mit

$$D := \sum_{i=1}^{r} m_i \bullet p_i$$

erhalten wir

$$\mathrm{div}(f) = (1-\sigma)\bullet D.$$

Sei d der Grad von D,

$$d := \deg D.$$

Der Punkt

$$p_0 = [1, 0, \sqrt{a}]$$

ist ein L-rationaler Punkt von

$$C_L = V(ax^2 + by^2 - 1),$$

also ein Primdivisor vom Grad 1. Der Divisor

$$D - d\bullet p_0$$

hat also den Grad 0. Auf Grund der obigen exakten Sequenz gibt es somit eine rationale Funktion

$$g \in L(C)^*$$

mit

$$D - d\bullet p_0 = \mathrm{div}(g).$$

Wir erhalten

$$\begin{aligned} \mathrm{div}(f) &= (1-\sigma)D = (1-\sigma)(\mathrm{div}(g) + d\bullet p_0) \\ &= \mathrm{div}(g\bullet\sigma(g)^{-1}) + d\bullet(1-\sigma)\bullet p_0 \end{aligned}$$

Nun haben die konjugierten Elemente g und $\sigma(g)$ dieselbe Norm, d.h. f und $f\sigma(g)/g$ haben dieselbe Norm. Wir können also f durch $f\sigma(g)/g$ ersetzen und errreichen

$$\mathrm{div}(f) = d\bullet(1-\sigma)\bullet p_0.$$

Wir sind jetzt in der Lage, die Funktion f bis auf einen konstanten Faktor genau anzugeben.

3. Schritt: $f = c_0 \bullet h^d$ mit $c_0 \in L^*$ und $h := (Z - X\bullet\sqrt{a})/Y \in L(C)^*$,

Es reicht zu zeigen, die rationale Funktion f/h^d hat weder Nullstellen nach Pole auf der projektiven Kurve (denn dann ist f/h^d eine von Null verschiedene Konstante). Mit anderen Worten, es reicht zu zeigen, f und h^d haben denselben Divisor. Damit ist der Beweis des 3. Schritts auf den Beweis der Identität

$$\mathrm{div}(h) = (1 - \sigma)p_0 = [1, 0, \sqrt{a}] - [1, 0, -\sqrt{a}].$$

reduziert. Zur Berechnung von div(h) nehmen wir an,

$$p = [x_0, y_0, z_0]$$

ist ein Pol von h auf $C = V(aX^2 + bX^2 - Z^2) \subseteq \mathbb{P}^1_k$. Dann muß $y_0 = 0$ sein, also

$$ax_0^2 - z_0^2 = 0,$$

also

---

folgt dann aber $m_i - n_i = 0$ für jedes i.

$$p = [1, 0, \pm\sqrt{a}].$$

Nun hat aber

$$\begin{aligned} h &= \frac{Z}{Y} - \sqrt{a} \cdot \frac{X}{Y} \\ &= (\frac{Y}{Z})^{-1} - \sqrt{a} \cdot \frac{X/Z}{Y/Z} \\ &= y^{-1} - \sqrt{a} \cdot \frac{x}{y} \qquad \text{(Übergang zu affinen Koordinaten)}, \\ &= \frac{1 - \sqrt{a} \cdot x}{y} \\ &= \frac{1 - \sqrt{a} \cdot x}{\sqrt{1 - ax^2}} \cdot \sqrt{b} \qquad \text{(auf C gilt } ax^2+by^2 = 1) \\ &= \frac{1 - \sqrt{a} \cdot x}{\sqrt{(1 - \sqrt{a} \cdot x)(1 + \sqrt{a} \cdot x)}} \cdot \sqrt{b} \\ &= \frac{\sqrt{1 - \sqrt{a} \cdot x}}{\sqrt{1 + \sqrt{a} \cdot x}} \cdot \sqrt{b} \end{aligned}$$

in $[1, 0, \sqrt{a}] = (\frac{1}{\sqrt{a}}, 0)$ eine Nullstelle ,

d.h.

$$p_1 = [1, 0, -\sqrt{a}]$$

ist der einzige Pol, und es ist ein Pol der Ordnung 1. Man beachte, y ist in diesem Punkt ein lokaler Parameter[25] der Kurve

$$ax^2 + by^2 = 1.$$

Wegen deg div(h) = 0 muß $[1, 0, \sqrt{a}]$ die einzige Nullstelle sein, und sie muß die Ordnung 1 haben. Damit gilt

$$\text{div}(h) = [1, 0, \sqrt{a}] - [1, 0, -\sqrt{a}].$$

4. Schritt: Beweis der Behauptung.

Es gilt

$$c = N(f) = N(c_0) \cdot N(h)^d = N(c_0) \cdot (\frac{z^2 - ax^2}{y^2})^d =^{26} N(c_0) \cdot b^d.$$

---

[25] d.h. ein Erzeuger des maximalen Ideals

$$m = (x - \frac{1}{\sqrt{a}}, y)$$

des lokalen Rings $\mathcal{O} = \mathcal{O}_{C,p_1}$: es gilt nämlich

$$(x - \frac{1}{\sqrt{a}})(x + \frac{1}{\sqrt{a}}) = x^2 - \frac{1}{a} = (1 - by^2)/a - \frac{1}{a} = -by^2 \in y\mathcal{O}.$$

Weil $x + \frac{1}{\sqrt{a}}$ in p_1 ungleich Null ist, also eine Einheit in $\mathcal{O}$, folgt

$$x - \frac{1}{\sqrt{a}} \in y\mathcal{O},$$

also

$$m \subseteq y\mathcal{O},$$

also

$$m = y\mathcal{O}.$$

[26] Auf der Kurve ist $ax^2 + by^2 - z^2 = 0$.

Nach Folgerung 7 ist damit

$$Q \cong (a, c)_k = (a, N(c_0) \bullet b^d)_k,$$

und nach Lemma 1.4.11

$$Q \cong (a, b^d)_k.$$

Nun soll Q nach Voraussetzung nicht zerfallen. Deshalb muß d ungerade sein. Dann ist aber

$$Q \cong (a, b^d)_k \cong (a, b)_k,$$

d.h. es gilt die Behauptung.
QED.

1.4.5 Bemerkung

Wir werden später eine weitreichende Verallgemeinerung des Kriteriums 1.4.10 beweisen, die auf Amitsur zurückgeht (im Kapitel 5).

1.5 Tensorprodukte von Quaternionen-Algebren

1.5.1 Definition: Biquaternionen-Algebra

Wir gehen jetzt zur Betrachtung höherdimensionaler k-Algebren über, wobei weiterhin die Charakteristik von k ungleich 2 sein soll,

$$\text{char}(k) \neq 2.$$

Der einfachste Fall sind die Biquaternionen-Algebren, welche definiert sind als Tensorprodukte von zwei Quaternionen-Algebren.

Wir beginnen mit zwei Lemmata, welche sich als sehr nützlich erweisen werden. Das erste von ihnen ist wohlbekannt.

1.5.2 Tensorprodukte von Matrizen-Algebren

Das Tensorprodukt der beiden Matrizen-Algebren $M_n(k)$ und $M_m(k)$ ist über k isomorph zur Matrizen-Algebra $M_{nm}(k)$.

Beweis. Der vielleicht einfachste Beweis beruht auf der Beobachtung, daß je zwei Endomorphismen

$$\phi \in \text{End}_k(k^n) \text{ und } \psi \in \text{End}_k(k^m)$$

einen Endomorphismus

$$\phi \otimes \psi : k^n \otimes_k k^m \longrightarrow k^n \otimes_k k^m,\ v \otimes w = \phi(v) \otimes \psi(w),$$

definieren. Man erhält so eine Abbildung

$$\text{End}_k(k^n) \times \text{End}_k(k^m) \longrightarrow \text{End}_k(k^n \otimes_k k^m),\ (\phi\ ,\ \psi) = \phi \otimes \psi\ ,$$

die offensichtlich bilinear ist, also eine k-lineare Abbildung

$$\text{End}_k(k^n) \otimes_k \text{End}_k(k^m) \longrightarrow \text{End}_k(k^n \otimes_k k^m) \tag{1}$$

induziert. Wir haben zu zeigen, diese Abbildung ist ein Isomorphismus. Da die beiden Räume links und rechts dieselbe Dimension $n^2 \bullet m^2 = (nm)^2$ haben, reicht es zu zeigen, diese Abbildung ist surjektiv. Bezeichne

$$E_{ij}$$

den Endomorphismus von k^n bzw. k^m welche den j-ten Standardeinheitsvektor e_j in den i-ten und alle übrigen Standardeinheitsvektoren in die Null abbildet. Das Bild von

$$E_{ij} \otimes E_{uv}$$

bei der Abbildung (1) ist der Endomorphismus

$$f = E_{(i,u)(j,v)}: k^n \otimes_k k^m \longrightarrow k^n \otimes_k k^m$$

mit

$$f(e_j \otimes e_v) = e_i \otimes e_u,$$

wobei alle übrigen $e_\alpha \otimes e_\beta$ in die Null abgebildet werden. Num bilden die

$$e_\alpha \otimes e_\beta \in k^n \otimes_k k^m$$

eine Basis von $k^n \otimes_k k^m$ und die $E_{(i,u)(j,v)}$ ein Erzeugendensystem von $End_k(k^n \otimes_k k^m)$. Das Bild der Abbildung (1) enthält also ein Erzeugendensystem des Bildraums, d.h. die Abildung ist surjektiv.
QED.

1.5.3 Tensorprodukte von Quaternionen-Algebren zum selben a

Für beliebige Elemente a, b, b' $\in k^*$ besteht ein Isomorphismus

(1) $$(a, b)_k \otimes_k (a, b') \overset{\cong}{\longrightarrow} (a, bb') \otimes M_2(k).$$

Beweis. Seien

$$1, i, j, ij \text{ bzw. } 1, i', j', i'j'$$

Quaternionen-Basen von $(a, b)_k$ bzw. $(a, b')_k$. Wir betrachten die folgenden k-linearen Unterräume des Tensorprodukts auf der rechten Seite.

A_1 := k•(1⊗1) + k•(i⊗1) + k•(j⊗j') + k•(ij⊗j')

A_2 := k•(1⊗1) + k•(1⊗j') + k•(i⊗i'j') + k•((-b'i)⊗i')

Wir rechnen zunächst nach, daß beide Unterräume abgeschlossen sind gegenüber der Multiplikation. Es reicht dies für die Erzeuger zu überprüfen: es gilt

$(i\otimes 1)^2$ = $i^2\otimes 1$ = a•(1⊗1)

$(j\otimes j')^2$ = $j^2\otimes j'^2$ = bb'•(1⊗1)

(i⊗1)•(j⊗j') = (ij)⊗j' = - (ji)⊗j' = - (j⊗j')•(i⊗1)

und

$(1\otimes j')^2$ = $1\otimes j'^2$ = b'•(1⊗1)

$(i\otimes i'j')^2$ = $i^2\otimes(i'j'i'j')$ = $-a^2b'$•(1⊗1)

(1⊗j')•(i⊗i'j')= i⊗(j'i'j') = -b'(i⊗i') = (-b'i)⊗i'

(i⊗i'j')• (1⊗j')=i⊗(i'j'j') = b'(i⊗i') = - (-b'i)⊗i'

Wir haben damit gezeigt, A_1 und A_2 sind Teilalgebren der Algebra auf der linken Seite von (1). Wir werden gleich zeigen, sie sind als k-Vektorräume 4-dimensional,

(2) $$\dim A_1 = \dim A_2 = 4.$$

Auf Grund der eben durchgeführten Rechnungen handelt es sich dann um die Quanternionen-Algebren

(3) $$A_1 \cong (a, bb')_k \text{ und } A_2 \cong (b', -a^2b').$$

Zum Beweis von (2) beachten wir zunächst, daß jeder der Erzeuger der ersten Algebra mit jedem der Erzeuger der zweiten kommutiert:

(j⊗j')(1⊗j') = j⊗(j'j') = (1⊗j')(j⊗j')

(j⊗j')(i⊗i'j') = (ji)⊗(j'i'j') = (-ij)⊗(-i'j'j') = (i⊗i'j')•(j⊗j').

Es gilt deshalb

(4) $a_1 \bullet a_2 = a_2 \bullet a_1$ für $a_1 \in A_1$ und $a_2 \in A_2$.

Betrachten wir jetzt die bilineare Abbildung

$$A_1 \times A_2 \longrightarrow (a, b)_k \otimes_k (a, b'), (a', a'') = a' \bullet a''.$$

Die Universalitätseigenschaft des Tensorprodukts liefert eine k-lineare Abbildung

$$\varphi: A_1 \otimes_k A_2 \longrightarrow (a, b)_k \otimes_k (a, b'),\ a' \otimes a'' \longrightarrow a' \bullet a''.$$

Diese Abbildung überführt Produkte in Produkte:[27]

$$\begin{aligned} \varphi((a' \otimes a'') \otimes (b' \otimes b'')) &= \varphi((a'b') \otimes (a''b'')) \\ &= a'b' \bullet a''b'' \\ &= a'a'' \bullet b'b'' \quad \text{(wegen (4))} \\ &= \varphi(a' \otimes a'') \bullet \varphi(b' \otimes b''). \end{aligned}$$

Wir sehen so, φ ist ein Homomorphismus von k-Algebren. Die Erzeuger des k-Vektorraums rechts liegen alle im Bild von φ:[28]

$1 \otimes 1 = \varphi((1 \otimes 1) \otimes (1 \otimes 1))$

$i \otimes 1 = \varphi((i \otimes 1) \otimes (1 \otimes 1))$

$j \otimes 1 = \varphi(\frac{1}{b'}(j \otimes j') \otimes (1 \otimes j'))$

$1 \otimes i' = \varphi(-\frac{1}{ab'}(i \otimes 1) \bullet (-b'i \otimes i'))$

$1 \otimes j' = \varphi((1 \otimes 1)(1 \otimes j'))$

$ij \otimes 1 = (i \otimes 1)(j \otimes 1) \in \mathrm{Im}(\varphi)$ wegen $i \otimes 1 \in \mathrm{Im}(\varphi)$ und $j \otimes 1 \in \mathrm{Im}(\varphi)$

...

Der k-Algebra-Homomorphismus ist somit surjektiv. Es folgt

$$16 = 4 \bullet 4 = \dim_k A_1 \bullet \dim_k A_2 = \dim_k A_1 \otimes_k A_2 = \dim_k (a, b)_k \otimes_k (a, b') = 4 \bullet 4 = 16.$$

Wir sehen, daß überall das Gleichheitszeichen gelten muß. Insbesondere gilt und damit (3). Außerdem ist φ ein k-Algebra-Isomorphismus:

$$(a, b)_k \otimes_k (a, b') \cong A_1 \otimes_k A_2 \cong (a, bb')_k \otimes_k (b', -a^2b')_k.$$

Zum Beweis der Behauptung reicht es zu zeigen, daß die Quaternionen-Algebra

$$(b', -a^2b')_k \cong (b', -b')_k$$

zerfällt. Das ergibt sich aber aus der Tatsache, daß

$$C(b', -b') = V(b'X^2 - b'Y^2 - Z^2)$$

den k-rationalen Punkt [1, 1, 0] besitzt.
QED.

1.5.4 Tensor-Quadrate von Quaternionen-Algebren

Für jede Quaternionen-Algebra $(a, b)_k$ ist deren Tensorprodukt mit sich selbst

$$(a, b)_k \otimes_k (a, b)_k \cong M_4(k)$$

isomorph zur Matrizen-Algebra $M_4(k)$.

---

[27] Wegen der k-Linearität von φ reicht es, dies für Produkte von Elementen der Gestalt $a' \otimes a''$ zu überprüfen.

[28] Alle übrigen Erzeuger sind Produkte der hier angegebenen, d.h. die hier angegebenen sind k-Algebra-Erzeuger. Da φ ein k-Algebra-Homomorphismus ist, reicht es von diesen zu zeigen, daß sie im Bild von φ liegen.

Beweis. Es gilt

$$
\begin{aligned}
(a, b)_k \otimes_k (a, b)_k &\cong (a, b^2)_k \otimes_k M_2(k) && \text{(nach 1.5.3)}\\
&\cong (a, 1)_k \otimes_k M_2(k) && \text{(nach 1.1.4(i))}\\
&\cong (1, a)_k \otimes_k M_2(k) && \text{(nach 1.1.4(ii))}\\
&\cong M_2(k) \otimes_k M_2(k) && \text{(nach 1.1.9)}\\
&\cong M_4(k) && \text{(nach 1.5.2)}
\end{aligned}
$$

QED.

1.5.5 Definitionen und Bezeichnungen

Für jede Quaternionen-Algebra Q bezeichne

$$Q^-$$

den Unterraum der reinen Quaternionen. Seien Q' und Q" zwei Quaternionen-Algebren und

$$A = Q' \otimes Q"$$

die zugehörige Biquaternionen-Algebra.Dann ist A mit einer Involution

$$\sigma: A \longrightarrow A,\ q' \otimes q" \longrightarrow \overline{q}' \otimes \overline{q}",$$

versehen.

Bemerkungen

(i) σ ist eine k-lineare und selbst-inverse Abbildung.

(ii) σ ist nicht kanonisch definiert sondern hängt wesentlich von der Zerlegung von A in ein Tensorprodukt von Quaternionen-Algebren ab.

1.5.6 Zerlegung in die Eigenräume von σ

Seien $A = Q' \otimes Q"$ eine Biquaternionen-Algebra mit der Involution σ und

$$V := \{a \in A \mid \sigma(a) = -a\}$$

$$W := \{a \in A \mid \sigma(a) = A\}$$

Dann gilt

$$A = V \oplus W$$

$$V = (Q'^- \otimes k) \oplus (k \otimes Q"^-)$$

$$W = k \oplus (Q'^- \otimes Q"^-)$$

Beweis. Nach Definition gilt

$$V \bigcap W = 0$$

(weil die Charakteristik von k ungleich 2 ist). Wegen

$$Q' = k \oplus Q'^- \text{ und } Q" = k \oplus Q"^-$$

gilt

$$
\begin{aligned}
A &= Q' \otimes Q"\\
&= (k \otimes k) \oplus (k \otimes Q"^-) \oplus (Q'^- \otimes k) \oplus (Q'^- \otimes Q"^-)\\
&\cong k \oplus (Q'^- \otimes Q"^-) \oplus (Q'^- \otimes k) \oplus (k \otimes Q"^-)
\end{aligned}
$$

Da das Konjugierte eines reinen Quaternions gleich seinem Negativen ist, folgt

$$(Q'^- \otimes k) \oplus (k \otimes Q"^-) \subseteq V$$

und

$$k \oplus (Q'^- \otimes Q"^-) \subseteq W.$$

Aus Dimensionsgründen muß überall das Gleichheitszeichen gelten.
QED.

1.5.7 Die Albert-Form einer Biquaternionen-Algebra

Seien Q' und Q" zwei Quaternionen-Algebren mit den Quaternionen-Normen

$$N': Q' \longrightarrow k \text{ und } N'': Q'' \longrightarrow k$$

und

$$A = Q' \otimes Q'' = V \oplus W$$

die zugehörige Biquaternionen-Algebra. Dann heißt die quadratische Form

$$\phi: V \cong Q'^{-} \oplus Q''^{-} \longrightarrow k, (x, y) = N'(x) - N''(y),$$

Albert-Form von A.

Bemerkung

Die Albert-Form von A hängt wesentlich von der Zerlegung von A in ein Tensorprodukt von Quaternionen-Algebren ab.

1.5.8 Satz von Albert

Sei $A = Q' \otimes Q''$ eine Biquaternionen-Algebra über k. Dann sind folgende Aussagen äquivalent.

(i) A ist keine Divisionsalgebra.

(ii) Es gibt Elemente $a, b, b' \in k^*$ mit $Q' \cong (a, b)$ und $Q'' = (a, b')$.

(iii) Die Albert-Form von A besitzt eine nicht-triviale Nullstelle.

Beweis. (ii) $\Rightarrow$ (iii). Nach Voraussetzung gibt es reine Quaternionen

$$q' \in Q'^{-} \text{ und } q'' \in Q''^{-} \text{ mit } q'^2 = a = q''^2.$$

Dann ist aber

$$\phi(q',q'') = N'(q') - N''(q'') = -q'^2 + q''^2 = -a + a = 0,$$

d.h. $(q', q'') \in V$ ist eine nicht-triviale Nullstelle von ϕ.

(iii) $\Rightarrow$ (i). Nach Voraussetzung gibt es reine Quaternionen $q' \in Q'^{-}$ und $q'' \in Q''^{-}$ mit

$$0 = \phi(q', q'') = N'(q') - N''(q'') = q''^2 - q'^2.$$

Es reicht zu zeigen, q' und q" kommutieren,

(1) $$q' \bullet q'' =^{29} q'' \bullet q' \text{ in } A = Q' \otimes Q'',$$

denn dann gilt

$$0 = q''^2 - q'^2 = (q'' - q')(q'' + q'),$$

d.h. A besitzt von 0 verschiedene Nullteiler, ist also keine Divisionsalgebra. Zum Beweis von (1) wählen wir eine Körpererweiterung K/k derart, daß Q' und Q" über K zerfallen. Dann gilt

$$\begin{aligned} A \subseteq A \otimes_k K &= Q' \otimes_k Q'' \otimes_k K \\ &\cong Q' \otimes_k K \otimes_k Q'' \\ &\cong Q' \otimes_k K \otimes_K K \otimes_k Q'' \\ &\cong M_2(K) \otimes_K M_2(K). \\ &\cong \mathrm{End}_K(K^2) \otimes_K \mathrm{End}_K(K^2) \quad (\cong \mathrm{End}_K(K^2 \otimes K^2)) \end{aligned}$$

---

[29] Wir identifizieren hier q' mit $q' \otimes 1 \in Q' \otimes Q''$ und q" mit $1 \otimes q'' \in Q' \otimes Q''$.

Es reicht zu zeigen, daß jedes Element aus dem ersten Tensorfaktor mit jedem Element aus dem zweiten Tensorfaktor kommutiert. Für $\alpha, \beta \in \mathrm{End}_K(K^2)$ und $v,w \in K^2$ gilt aber

$$(\alpha\otimes 1)\circ(1\otimes\beta)(v\otimes w) = (\alpha\otimes 1)(v\otimes\beta(w)) = \alpha(v)\otimes\beta(w)$$
$$(1\otimes\beta)\circ(\alpha\otimes 1)(v\otimes w) = (1\otimes\beta)(\alpha(v)\otimes w) = \alpha(v)\otimes\beta(w),$$

also $(\alpha\otimes 1)\circ(1\otimes\beta)(v\otimes w) = (1\otimes\beta)\circ(\alpha\otimes 1)(v\otimes w)$. Da die Elemente der Gestalt $v\otimes w$ ein Erzeugendensystem von $K^2\otimes K^2$ bilden, folgt

$$(\alpha\otimes 1)\circ(1\otimes\beta)(v\otimes w) = (1\otimes\beta)\circ(\alpha\otimes 1).$$

(i) $\Rightarrow$ (ii). Wir nehmen an, Bedingung (ii) ist nicht erfüllt, und haben zu zeigen, daß dann A eine Divisionsalgebra ist. Ist Bedingung (ii) nicht erfüllt, so sind Q' und Q" beides Divisionsalgebren,

(1) $\qquad Q' = (a, b)$ und $Q'' = (a', b')$ Divisionsalgebren.

Andernfalls könnten wir nämlich o. B.d.A. Q" annehmen, Q' z erfällt, ist also von der Gestalt

$$Q'' \cong (1, a) \cong (a, 1)$$

(nach 1.1.9 und 1.1.4(ii)). Bedingung (ii) wäre dann aber mit $b' = 1$ erfüllt. Wir wissen also, Q' und Q" sind Divisionsalgebren. Dann gibt es aber quadratische Körpererweiterungen von k, die ganz in der jeweiligen Quaternionenalgebra liegen,

(2) $$k \subseteq K' \subseteq Q',\ k \subseteq K'' \subseteq Q''$$

mit

K'/k und K"/k Körpererweiterungen vom Grad 2

(siehe den Beweis von 1.2.5). Schreiben wir

(3) $$K' = k(\alpha') \text{ und } K'' = k(\alpha'').$$

Wir können dabei annehmen, es gilt[30]

$$a' := \alpha'^2 \in k \text{ und } a'' := \alpha''^2 \in k.$$

Weil die Algebren nicht zerfallen, gilt außerdem

$$\alpha' \in Q' - k \text{ und } \alpha'' \in Q'' - k.$$

Nach Theorem 1.2.3 müssen

(4) $$Q'\otimes_k K' \text{ und } Q''\otimes_k K'' \text{ zerfallen.}$$

Andererseits wissen wir,

(5) $$Q'\otimes_k K'' \text{ und } Q''\otimes_k K' \text{ zerfallen nicht.}$$

Wenn nämlich zum Beispiel $Q'\otimes_k K'' = Q'\otimes_k k(\alpha')$ zerfiele, so wäre nach Theorem 1.2.3 Q' von der Gestalt

$$Q' \cong (a', *)_k,$$

und weil $Q''\otimes_k K''$ zerfällt, gilt dasselbe auch für Q",

---

[30] Jedenfalls genügen die Erzeuger der Körpererweiterungen quadratischen Gleichungen. Wegen $\mathrm{char}(k) \neq 2$, kann man durch quadratische Ergänzung erreichen, daß die Gleichungen die Gestalt $X^2 - c$ haben mit $c \in k$.

$$Q'' \cong (a', **)_k ,$$

d.h. Bedingung (ii) der Behauptung wäre erfüllt. Wir wissen also, die Algebren (5) sind Divisionsalgebren.

Wir wollen zeigen, jedes Element

$$\alpha \in A - \{0\}$$

besitzt ein Linksinverses. Dazu reicht es zu zeigen, es gibt ein Element

$$\alpha^* \in A$$

mit der Eigenschaft, daß $\alpha^*\alpha$ ein von Null verschiedenes Element ist, daß in einer der Divisionsalgebren (5) liegt,

$$\alpha^*\alpha \in Q' \otimes_k K'' - \{0\} \text{ oder } \alpha^*\alpha \in Q'' \otimes_k K' - \{0\}.$$

Wir fixieren eine Quaternionen-Basis

$$1, i, j, ij \in Q''$$

und können dabei annehmen[31],

$$K'' = k(j).$$

Das Element $\alpha \in A = Q' \otimes_k Q'' = Q' + Q'i + Q'j + Q'ij$ läßt sich dann in der folgenden Gestalt schreiben.

$$\alpha = (\beta_1 + \beta_2 j) + (\beta_3 + \beta_4 j)ij \text{ mit } \beta_i \in Q' \text{ für } i = 1,2,3,4.$$

Wir können dabei annehmen,

$$\gamma := \beta_3 + \beta_4 j \neq 0,$$

denn andernfalls würde α bereits selbst in

$$Q' \otimes_k K'' = Q' + Q'j$$

liegen und wir könnten $\alpha^* = 1$ setzen. Als von Null verschiedenes Element besitzt

$$\gamma \in Q' \otimes_k K''$$

ein Inverses in $Q' \otimes_k K''$. Wir können α durch $\gamma^{-1}\alpha$ ersetzen und erreichen so, daß α die folgende Gestalt besitzt.

$$\alpha = \beta_1 + \beta_2 j + ij \text{ mit } \beta_i \in Q' \text{ für } i = 1,2.$$

1. Fall: β_1 und β_2 kommutieren: $\beta_1 \bullet \beta_2 = \beta_2 \bullet \beta_1$.

Dann ist

$$K = k(\beta_1, \beta_2) \subseteq Q'$$

eine Körpererweiterung von k. Diese kann höchstens vom Grad 2 sein, denn andernfalls wäre $k(\beta_1, \beta_2) = Q'$, also Q' kommutativ. Je nachdem, ob K vom Grad 1 oder 2 ist über k, erhalten wir

$\alpha \in Q''$ oder $\alpha \in Q'' \otimes_k K$ mit $K \subseteq Q'$ quadratische Körpererweiterung von k.

In beiden Fällen können $\alpha^* = 1$ setzen.

2. Fall: : β_1 und β_2 kommutieren nicht: $\beta_1 \bullet \beta_2 - \beta_2 \bullet \beta_1 \neq 0$.

Wir setzen

$$\alpha^* := \beta_1 - \beta_2 j - ij.$$

Es gilt dann

$$\alpha^* \bullet \alpha = (\beta_1 - \beta_2 j - ij) \bullet (\beta_1 + \beta_2 j + ij)$$

---

[31] K'' sollte irgendeine quadratische Erweiterung von k sein, die ganz in Q'' liegt.

$$=^{32} (\beta_1 - \beta_2 j)\bullet(\beta_1 + \beta_2 j) - (ij)^2$$
$$= \beta_1^2 - \beta_2^2 j^2 - (ij)^2 + (\beta_1\bullet\beta_2 - \beta_2\bullet\beta_1)j$$

Nun liegen j^2 und $(ij)^2$ in k, und $\beta_1\bullet\beta_2 - \beta_2\bullet\beta_1$ ist von Null verschieden. Also ist $\alpha^*\bullet\alpha$ ein von Null verschiedenes Element aus $Q'\otimes_k K"$,

$$\alpha^*\bullet\alpha \in Q'\otimes_k K" - \{0\}.$$

QED.

Bemerkung

Der obige Beweis stammt von Lam[1] ist eine Variante von Alberts ursprünglichen Argument. Für andere Beweise, die beliebiger Charakteristik gültig sinc, siehe Knus [1] und ebenso Tits [1] (für die Äquivalenz (i) $\Leftrightarrow$ (ii)).

1.5.9 Beispiel für eine Divisionsalgebra der Dimension 16

Seien k wie immer ein Körper der Charakteristik $\neq 2$ und F der iterierte Laurent-Reihen-Körper

$$F := k((w_1))((w_2))((w_3))((w_4)).$$

Dann ist die Biquaternionen-Algebra

$$(w_1, w_2)\otimes_F(w_3, w_4)$$

eine Divisionsalgebra über F.

Beweis. Es reicht zu zeigen, die Albert-Form besitzt außer der trivialen Nullstelle keine Nullstellen. Wir nehmen an, sie hätte eine solche Nullstelle. Auf Grund der Formel für die Quaternionen-Norm hat dann die folgenden Gleichung in den Unbestimmen x_1,x_2 ,$x_{1,2}$,x_3,x_4,$x_{3,4}$ eine nicht-triviale Lösung mit Koordinaten in F.[33]

(1) $$-w_1x_1^2 -w_2x_2^2 + w_1w_2x_{1,2}^2+w_3x_3^2 + w_4x_4^2 - w_3w_4x_{3,4}^2 = 0$$

Durch Multiplikation mit einer geeigneten Potenz von w_4 erreichen wir,

$$x_1,x_2,x_{1,2},x_3,x_4,x_{3,4} \in k((w_1))((w_2))((w_3))[[w_4]],$$

wobei mindestens ein x ist nicht durch w_4 teilbar sein soll.

1. Fall: w_4 teilt jede der Koordinaten $x_1,x_2,x_{1,2},x_3$.

Dann teilt w_4^2 den Ausdruck $w_4x_4^2 - w_3w_4x_{3,4}^2$, d.h. w_4 teilt $x_4^2 - w_3 x_{3,4}^2$. Wir setzen w_4 Null und erhalten so eine nicht-triviale Lösung von

$$x^2 - w_3 x^2 = 0.$$

Das bedeutet aber, w_3 ist ein Quadrat in

$$k((w_1))((w_2))((w_3)),$$

ein Widerspruch, da w_3 eine Unbstimmte sein soll.

2. Fall: w_4 teilt nicht jede der Koordinaten $x_1,x_2,x_{1,2},x_3$.

Wir setzen w_4 Null und erhalten so aus (1) eine nicht-triviale Lösung der Gleichung

$$-w_1y_1^2 -w_2y_2^2 + w_1w_2y_{1,2}^2+w_3y_3^2 = 0$$

---

[32] ij kommutiert mit β_1 und β_2 (weil jedes Element von Q' mit jedem von Q" kommutiert) und ij anti-kommutiert mit j.

[33] Man beachte, die Albert-Form ist nur für reine Quaternionen definiert.

mit Koordinaten in

$$k((w_1))((w_2))((w_3)).$$

Ein ähnliches Argument wie eben (mit w_3 anstelle von w_4) zeigt, daß damit auch

$$-w_1z_1^2 - w_2z_2^2 + w_1w_2z_{1,2}^2 = 0$$

eine nicht-triviale Lösung besitzt mit Koordinaten in $k((w_1))((w_2))$. Erneutes Anwenden desselben Tricks (mit w_2 anstelle von w_4) liefert eine nicht-triviale Lösung von

$$w_{11}^2 = 0$$

mit Koordinaten in $k((w_1))$. Dieser endgültige Widerspruch beweist die obige Behauptung.
QED.

1.5.10 Divisionsalgebren mit der Periode 2

Von einer endlich-dimensionalen Divisionsalgebra D über einem Körper k sagt man, sie habe die Periode 2, wenn

$$D \otimes_k D$$

isomorph ist zu einer Matrizen-Algebra über k.

Bemerkungen

(i) Quaternionen-Algebren sind von der Periode 2 nach 1.5.4.
(ii) Tensorprodukte von k-Algebren der Periode 2 sind von der Periode 2 (nach 1.5.2).
(iii) Jede 4-dimensionale zentrale Divisionsalgebra ist nach 1.2.5 eine Quaternionen-Algebra also von der Periode 2.
(iv) Albert hat 1932 gezeigt, daß jede 16-dimensionale zentrale Divisionsalgebra der Periode 2 isomorph ist zu einer Biquaternionen-Algebra. Es war also naheliegend zu vermuten, daß eine zentrale Divisionsalgebra der Periode 2 und der Dimension 4^n stets ein Tensorprodukt von Quaternionen-Algebren ist.
(iv) Amitsur, Rowen und Tignol haben jedoch 1979 eine 64-dimensionale zentrale Divisionsalgebra der Periode 2 konstruiert, die kein Tensorprodukt von Quaternionen-Algebren ist.
(v) Die nachfolgende Aussage ist einer der Höhepunkte dieser Monographie.

1.5.11 Satz von Merkurjev

Sei D eine zentrale Divisionsalgebra der Periode 2 über einem Körper k. Dann gibt es natürliche Zahlen m_1, m_2, n und Quaternionen-Algebren $Q_1,...,Q_n$ mit

$$D \otimes_k M_{m_1}(k) \cong Q_1 \otimes ... \otimes Q_n \otimes M_{m_1}(k).$$

Aufgaben

1. Charakterisierung der Konjugation. Sei Q eine Quaternionen-Algebra über k. Man zeige, die Konjugation ist die einzige Involution $\sigma: Q \longrightarrow Q$ mit $\sigma(1) = 1$ und $\sigma(q)q \in k$ für jedes $q \in Q$.

2. Man zeige, eine Quaternionen-Algebra zerfällt genau dann, wenn sie eine Basis

$$e, f, g, h$$

besitzt, bezüglich welcher die Norm von der Gestalt

$$xe + yf + zg + wh = xy - zw$$

ist. (In der Sprache der quadratischen Formen bedeutet dies, daß die Norm eine hyperbolische quadratische Form ist).

3. Man bestimme alle Primzahlen p, für welche die Quaternionen-Algebra (-1 , p) über dem Körper $\mathbb{Q}$ der rationalen Zahlen zerfällt.

4. Ketten-Lemma. Angenommen die Quaternionen-Algebren (a, b) und (c, d) sind isomorph. Man zeige, es gibt ein Element $e \in k^*$ mit

$$(a, b) \cong (e, b) \cong (e, d) \cong (c, d).$$

Hinweis. Man betrachte die quadratische Form

$$B(q_1, q_2) := \frac{1}{2}(q_1 \bullet \overline{q}_2 + q_2 \bullet \overline{q}_1)$$

auf dem Unterraum

$$B_0 \subseteq (a, b)$$

der Elemente $q \in (a, b)$ mit $q + \overline{q} = 0$. Man beachte, es gilt

$$i,j,I,J \in B_0,$$

wenn 1, i, j, ij und 1, I, J, IJ Standard-Quaternionen-Basen von $(a, b) \cong (c, d)$ sind mit $i^2 = a$, $j^2 = b$, $ij = - ji$, $I^2 = c$, $J^2 = d$, $IJ = - JI$. Man wähle ein Element $\varepsilon \in B_0 - \{0\}$ mit $B(\varepsilon, j) = B(\varepsilon, J) = 0$ und setze $e = \varepsilon^2$.

2. Zentrale einfache Algebren und Galois-Abstieg

In diesem Kapitel behandeln wir die grundlegende Theorie der zentralen einfachen Algebren aus der Sicht der modernen Algebra.

Als wichtigsten Punkt möchten wir betonen, daß man die zentralen einfachen Algebren infolge des Satzes von Wedderburn charakterisieren kann als diejenigen endlich-dimensionalen Algebren, welche über einer endlichen Erweiterung des Grundkörpers isomorph werden zu einer vollen Matrizen-Algebra. Wir werden zeigen, daß man als Erweiterung eine Galois-Erweiterung wählen kann, so daß uns für die weiteren Untersuchungen eine sehr starke Theorie zur Verfügung steht: die Theorie des Galois-Abstiegs. Unter Verwendung der Abstiegstheorie können wir solche klassischen Ergebnisse wie Konstruktion reduzierter Normen und den Satz von Skolem und Noether in einer recht eleganten Weise abhandeln. Die wichtigste Invariante der zentralen einfachen Algebren ist die Brauer-Gruppe, welche die endlichen zentralen Divisionsalgebren über einem Körper klassifiziert. Mit Hilfe des Galois-Abstiegs werden wir diese Gruppe mit einer nicht-kommutativen Kohomologie-Gruppe identifizieren.

Die Grundzüge der Theorie der einfachen zentralen Algebren reichen zurück zu den großen Algebraikern am Beginn des 20. Jahrhunderts. wir erwähnen hier nur Wedderburn, Dickson und Noether. Die Brauer-Gruppe erscheint erstmal in der umwälzenden Arbeit des jungen Richard Brauer [1]. Obwohl der Galois-Abstieg in impliziter Weise bereits von den Algebraikern des frühen 20. Jahrhunderts benutzt wurde, war es André Weil, der als erster - inspiriert durch die Arbeiten von Chatelet - eine systematische Behandlung des Phänoms gab, wobei er dabei Anwendungen auf dem Gebiet der algebraischen Geometrie im Auge hatte (Weil [1]). Später wurden die Theorie von Jean-Pierre Serre popularisiet und fand eine quälende Verallgemeinerung in der allgemeinen Abstiegstheorie von Grothendieck ([1], [2]).

2.1 Der Satz von Wedderburn

2.1.1 Definition

Seien k ein Körper und A eine k-Algebra. Wir bleiben bei unserer globalen Vereinbarung des vorangehenden Kapitel, daß alle k-Algebren endlich-dimensional sein sollen,

$$\dim_k A < \_.$$

Die Algebra A heißt einfach, wenn sie keine (zwei-seitigen) Ideale besitzt außer den stets existierenden Idealen A und 0.

2.1.2 Beispiel: Divisionsalgebren

Eine Divisionsalgebra D über k ist trivialerweise einfach. Ihr Zentrum

$$Z(D) := \{x \in D \mid xy = yx \text{ für } y \in D\}$$

ist ein Körper: wegen der Implikation

$$xy = yx \Rightarrow y^{-1}x^{-1} = x^{-1}y^{-1}$$

gilt mit $x \in Z(D) - \{0\}$ auch $x^{-1} \in Z(D)$.

Eine Divisionsalgebra D ist somit eine zentrale einfache Algebra über deren Zentrum Z(D).

Konkrete Beispiele für zentrale einfache Algebren sind (neben den Körpern) die nicht-zerfallenden Quaternionen-Algebren. Diese sind zentral nach 1.2.2 und Divisionsalgebren nach 1.1.10.

2.1.3 Beispiel: Matrizen-Algebren

Seien D eine Divisionsalgebra über k und

$$A = M_n(D)$$

der Ring der n×n-Matrizen über D. Dann ist A einfach.

Da jede Matrix im Zentrum einer Matrizen-Algebra ein Vielfaches der Einheitsmatrix ist, ist A insbesondere eine einfache zentrale Algebra über dem Zentrum Z(D) von D.

Beweis der Einfachheit von A. Dies ist ein Übung in linearer Algebra. Sei

$$M \in A - \{0\}$$

eine von der Nullmatrix verschieden Matrix. Wir haben zu zeigen, das von M erzeugte zwei-seitige Ideal

$$< M >$$

ist die ganze Algebra A. Betrachten wir die Elementarmatrix

$$E_{ij}$$

mit einer Eins in der Position (i, j) und Nullen in allen anderen Positionen. Da jedes Element von A eine D-Linearkombination der E_{ij} ist, reicht es zu zeigen,

$$E_{ij} \in < M > \text{ für jedes i und jedes j.}$$

Wegen

$$E_{\alpha i}E_{ij}E_{j\beta} = E_{\alpha\beta}$$

reicht es zu zeigen,

$$E_{ij} \in < M > \text{ für ein i und ein j.}$$

Wir wählen i und j derart, daß der Eintrag m von in der Positon (i, j) von Null verschieden ist,

$$m \in D - \{0\}.$$

Dann gilt

$$< M > \ni m^{-1}E_{ii} \bullet M \bullet E_{jj} = E_{ij}\ .$$

QED.

2.1.4 Die minimalen Linksideale von $M_n(D)$

Seien D eine Divisionsalgebra über k und

$$A = M_n(D)$$

der Ring der n×n-Matrizen über D. Für jede natürliche Zahl r mit $1 = r = n$ bezeichne

$$I_r = \{ M = (m_{ij}) \in A \mid m_{ij} = 0 \text{ für } j \neq r\}$$

die Menge der Matrizen, deren r-te Spalte beliebig und deren übrige Spalten gleich Null sind. Dann sind

$$I_1 , \dots , I_r$$

gerade minimale Linksideale von A.[34]
Allgemeiner, sei

$$M \in A$$

eine Matrix mit von Null verschiedener erster Zeile, deren übrige Zeilen Null sind. Dann ist

$$L = A \bullet M$$

ein minimales Linksideal, und jedes Linksideal ist von dieser Gestalt. Als A-Modul ist L isomorph zu D^n,

$$L \cong D^n \text{ als A-Modul.}$$

Beweis. Multiplikation einer Matrix von Links bedeutet gerade, man bildet Linearkombination der Zeilen dieser Matrix. Die I_r sind deshalb Linksideale von A. Die oben angegebene Menge L ist trivialerweise ein Linkideal. Wir haben noch zu zeigen,

1. Jedes der I_j ist von der Gestalt L.
2. Jedes Linksideal $\neq 0$ von A enthält ein Ideal der Gestalt $L = A \bullet M$.
3. Sind zwei Ideale der Gestalt $L = A \bullet M$ ineinander enthalten, so sind sie gleich.
4. Die Linksideale der Gestalt L sind als A-Moduln isomorph zu D^n

Zu 1. Sei $M = E_{1j}$. Dann ist

$$A \bullet M = I_j,$$

denn durch elementare Zeilen-Operationen kann man aus E_{1j} gerade die Matrizen mit beliebig vorgegebener j-ter Spalte gewinnen, wobei alle übrigen Spalten Null sind.

Zu jetzt L' ein von Null verschiedenes Linksideal von A. Wir fixieren ein von Null verschiedenes Element in L',

$$0 \neq M' \in L',$$

und schreiben die Matrix M' als Linearkombination der Matrizen E_{ij}, sagen wir

$$M' = \sum_{ij} a_{ij} E_{ij} \text{ mit } a_{ij} \in D.$$

Multiplikation mit $E_{\alpha\alpha}$ liefert

$$E_{\alpha\alpha} M' = \sum_{ij} a_{ij} E_{\alpha\alpha} E_{ij} = \sum_{j} a_{\alpha j} E_{\alpha j}$$

Diese Matrix hat dieselbe α-te Zeile wie M'. Es gibt also ein α für welches diese Matrix von Null verschieden ist. Wir können mit $E_{1\alpha}$ multiplizieren und o.B.d.A. annehmen,

---

[34] Im Buch von Gille von Szamuely wird behauptet, es gebe außer den I_1,..., I_n keine weiteren minimalen Linksideale von A.

dies ist für $\alpha = 1$ der Fall. Es gibt also in L' eine Matrix M, deren erste Zeile von Null verschieden ist, und deren übrige Zeilen Null sind. Insbesondere enthält L' ein Linksideal

$$L = A \bullet M \subseteq L'$$

der behaupteten Gestalt.

Zu 3. Seien $M', M'' \in A$ zwei Matrizen, deren einzige von Null verschiedene Zeile die erste ist und für welche die zugehörigen Linksideale ineinander enthalten sind, sagen wir

$$A \bullet M' \subseteq A \bullet M''.$$

Dann gilt $M' \in A \bullet M''$, d.h. es gibt eine Matrix $M \in A$ mit

$$M' = M \bullet M''.$$

Da alle Zeilen von M'' außer der ersten Null sind, können wir die Spalten von M mit Ausnahme der ersten beliebig abändern, ohne daß sich das Produkt auf der rechten Seite ändert. Wir ersetzen alle Einträge dieser Spalten durch Nullen. Seien

$$m_1,...,m_n$$

die Einträge der ersten Spalte von M und bezeichne z'' die erste Zeile von M''. Dann ist

$$m_i \bullet z''$$

gerade die i-te Zeile von M'. Wegen $z'' \neq 0$ und weil alle Zeilen von M' außer der ersten Null sind, folgt

$$m_2 = ... = m_n = 0.$$

Damit ist

$$M' = m_1 \bullet M'' \text{ und } m_1 \neq 0.$$

Insbesondere erzeugen M' und M'' dasselbe Linksideal von A.

Zu 4. Für jedes α setzen wir

$$e_\alpha := E_{\alpha 1} \bullet M.$$

Die Matrix e_α hat genau eine von Null verschiedene Zeile, nämlich die α-te Zeile. Diese stimmt mit der ersten Zeile von $e_1 = E_{11}M = M$ überein. Über D sind die Vektoren e_α linear unabhängig. Für $X = (x_{ij}) = \sum_{ij} x_{ij}E_{ij} \in A$ gilt

$$(1) \qquad X \bullet e_\alpha = \sum_{ij} x_{ij}E_{ij}\, E_{\alpha 1} \bullet M = \sum_i x_{i\alpha}E_{i1}M = \sum_i x_{i\alpha}e_i$$

Diese Identität zeigt, die Multiplikation von Links bildet die Matrizen von

$$\sum_\alpha De_\alpha \cong D^n$$

in sich ab. Also bilden diese Matrizen ein Ideal, welches die Matrix $M = e_1$ enthält. Es folgt

$$L = A \bullet M = \sum_\alpha De_\alpha.$$

Außerdem zeigt Formel (1) daß die Matrizen $X \in A$ so auf den e_α operieren, als wären die e_α die Standard-Einheitsvektoren des D^n und die Operation die gewöhnliche Matrizen-Multiplikation.[35] Also ist L auch als A-Modul isomorph zu D^n.

QED.

2.1.5 Satz von Wedderburn

Sei A eine endlich-dimensionale einfache Algebra über einem Körper k. Dann gibt es eine natürliche Zahl n und eine Divisionsalgebra $D \supseteq k$ derart, daß A isomorph ist zum vollen Matrizenring $M_n(D)$,

$$A \cong M_n(D).$$

Die Divisionsalgebra D ist dabei bis auf Isomorphie eindeutig bestimmt.

Bemerkung
Als Vorbereitung des Beweises erinnern wir an einige Begriffe und beweisen zwei Lemmata.

2.1.6 Einige grundlegende Begriffe der Modultheorie

Seien A ein Ring (mit Eins) und M ein linker A-Modul,

$$A \times M \longrightarrow M,\ (a, m) = am.$$

Ein <u>Endomorphismus</u> von M ist eine A-lineare Abbildung

$$\phi: M \longrightarrow M.$$

Ein A-Modul M heißt <u>einfach</u>, wenn er außer 0 und M keine Teilmoduln besitzt.

Bemerkungen

(i) Die Endomorphismen von M bilden einen Ring

$$End_A(M),$$

dessen Addition gegeben ist durch

$$(\phi'+\phi'')(m) = \phi'(m) + \phi''(m) \text{ für } \phi', \phi'' \in End_A(M) \text{ und } m \in M.$$

und dessen Multiplikation die Zusammensetzung von Abbildungen ist.

(ii) Ist A ein k-Algebra, so gilt dasselbe für $End_A(M)$, denn die Multiplikation mit einem Element von k definiert ein Element aus dem Zentrum von $End_A(M)$.

(iii) Ist A eine Divisions-Algebra, dann ist M ein linker-Vektorraum über A. Durch Wahl einer Basis b von M über A erhält man mit Hilfe der üblichen Konstruktionen der linearen Algebra einen Isomorphismus von linken A-Moduln

$$End_A(M) \xrightarrow{\cong} M_n(A),\ \phi = M_b^b(\phi).$$

Dabei bezeichnet n die Dimension von M über A.

(iv) Der A-Modul M besitzt die Struktur eines linken Moduls über dem Endomorphismenring $End_A(M)$,

---

[35] Ist e_α der α-te Standard-Einheitsvektor, so ist das Matrizenprodukt $X \bullet e_\alpha$ gerade die α-te Spalte von X, d.h. der Vektor $\sum_i x_{i\alpha} e_i$.

$$\mathrm{End}_A(M) \times M \longrightarrow M,\ (\phi, m) = \phi \bullet m := \phi(m).$$

(v) Sei M ein linker A-Modul mit dem Endomorphismenring

$$D := \mathrm{End}_A(M).$$

Da M nach (iv) die Struktur eines linken D-Moduls hat, kann man den Endomorphismenring

$$\mathrm{End}_D(M)$$

betrachten. Die Abbildung

$$\lambda_M : A \longrightarrow \mathrm{End}_D(M),\ a = (\ m \mapsto am\ ),$$

ist wohldefiniert und ein Ringhomomorphismus.[36]

2.1.7 Das Lemma von Schur

Seien A ein Ring (mit Eins) und M ein einfacher A-Modul. Dann ist

$$\mathrm{End}_A(M)$$

ein Schiefkörper.

Beweis. Sei $\phi: M \longrightarrow M$ ein von Null verschiedenes Element von $\mathrm{End}_A(M)$. Dann ist der Kern

$$\mathrm{Ker}(\phi)$$

ein echter Teilmodul von M. Da M einfach sein soll, folgt

$$\mathrm{Ker}(\phi) = 0.$$

Analog ist $\mathrm{Im}(\phi) \neq 0$ ein Teilmodul von M, d.h.

$$\mathrm{Im}(\phi) = M.$$

Zusammen erhalten wir, daß ϕ bijektiv ist, also ein Inverses in $\mathrm{End}_A(M)$ besitzt.

QED.

2.1.8 Lemma von Rieffel

Seien A eine einfache k-Algebra und $L \subseteq A$ ein nicht-triviales linkes Ideal. Dann ist der Ring-Homomorphismus

$$\lambda_L : A \longrightarrow \mathrm{End}_D(L) \text{ mit } D = \mathrm{End}_A(L)$$

wie er in 2.1.6(v) definiert wurde ein Isomorphismus.

Beweis. Das Bild von $1 \in A$ bei λ_L ist die identische Abbildung von L, also $\neq 0$. Der Kern von λ_L ist somit ein von 0 verschiedenes Ideal von A. Weil A einfach ist, folgt

$$\mathrm{Ker}(\lambda_L) = 0,$$

d.h. λ_L ist injektiv.

Zum Beweis der Surjektivität beachten wir zunächst,
$\lambda_L(L)$ ist ein Linksideal in $\mathrm{End}_D(L)$:

Seien nämlich $\phi \in \mathrm{End}_D(L)$ und $\ell \in L$. Dann ist

$$\phi \bullet \lambda_L(\ell)$$

---

[36] Es ist klar, daß es sich um einen Ring-Homomorphismus handelt, falls die Abbildung wohldefiniert ist. Wir haben zu zeigen, die Abbildung

$$m = am,$$

ist D-linear. Trivialerweise ist sie additiv. Sei $\phi \in D = \mathrm{End}_A(M)$. Wir haben zu zeigen,

$$a \bullet (\phi \bullet m) = \phi \bullet (a \bullet m).$$

Das ist aber der Fall, weil die Elemente von $D = \mathrm{End}_A(M)$ linear sind über A.

die Abbildung

$$L \longrightarrow L,\ x = \phi(\ell x).$$

Die Multiplikation von rechts mit x ist ein A-Endomorphismus von L,

$$\psi\colon L \longrightarrow L,\ y = yx,$$

d.h. ein Element von D,

$$\psi \in D = \mathrm{End}_A(L).$$

Weil ϕ eine D-lineare Abbildun ist, folgt

$\phi(\ell x) = \phi(\psi(\ell))$ (nach Definition von ψ)
$= \phi(\psi \bullet \ell)$ (auf Grund der Definition der Operation von D auf L)
$= \psi \bullet \phi(\ell)$ (weil ϕ linear is über D)
$= \phi(\ell) \bullet x$ (nach Definition von ψ)

Damit ist $\phi \bullet \lambda_L(\ell)$ die Abbildung

$$L \longrightarrow L,\ x = \phi(\ell) \bullet x,$$

d.h. es ist

$$\phi \bullet \lambda_L(\ell) = \lambda_L(\phi(\ell)) \in \lambda_L(L).$$

Die Multiplikation von links mit $\phi \in \mathrm{End}_D(L)$ überführt also die Menge $\lambda_L(L)$ in sich, d.h. $\lambda_L(L)$ ist ein Linksideal wie behauptet.

Als nächstes beachten wir, das von L erzeugte Rechsideal

$$L \bullet A$$

ist sogar ein zwei-seitiges Ideal. Wei A einfach ist, folgt

$$LA = A.$$

Insbesondere läßt sich das Einselement $1 \in A$ in der folgenden Gestalt schreiben.

$$1 = \sum_i \ell_i a_i \text{ mit } \ell_i \in L \text{ und } a_i \in A.$$

Für jedes $\phi \in \mathrm{End}_D(L)$ gilt damit

$$\phi = \phi \bullet \mathrm{Id} = \phi \bullet \lambda_L(1) = \sum_i \phi \bullet \lambda_L(\ell_i)\, \lambda_L(a_i)$$

Wegen $\lambda_L(a_i) \in \lambda_L(L)$ und weil $\lambda_L(L)$ ein Linksideal ist, folgt

$$\phi \in \lambda_L(L).$$

Wir haben gezeigt λ_L ist surjektiv.

QED.

2.1.9 Beweis des Satzes von Wedderburn 2.1.5

Sei A eine endlich-dimensionale einfache Algebra über k. Auf Grund der endlichen Dimension muß jede absteigende Kette von Linksidealen in A stationär sein. Es gibt also ein minimales Linksideal L in A,

$$0 \neq L \subseteq A.$$

Als A-Modul ist L dann einfach. Nach dem Lemma von Schur ist damit

$$D = \mathrm{End}_A(L)$$

eine Divisionsalgebra. Nach dem Lemma von Rieffel besteht ein Isomorphismus

$$A \cong \mathrm{End}_D(L).$$

Nun ist L als D-Vektorraum endlich-dimensional (wegen $\dim_k L = \dim_k A < \_$), d.h. es besteht ein Isomorphismus

$$\mathrm{End}_D(L) \cong M_n(D).$$

Also ist A wie behauptet isomorph zu einer vollen Matrizen-Algebra über der Divisionsalgebra D.

Wir haben noch die Eindeutigkeit des Schiefkörper D zu beweisen. Angenommen, D und D' sind Divisionsalgebren mit

$$A \cong M_n(D) \cong M_m(D').$$

für geeignete natürliche Zahlen n und m. Nach 2.1.4 bestehen für das minimale Linksideal L A-Modul-Isomorphien

$$D^n \cong L \cong D'^m.$$

Wir erhalten damit Isomorphien

$$D^\circ \cong \mathrm{End}_A(D^n) \cong \mathrm{End}_A(L) \cong \mathrm{End}_A(D'^m). \cong D'^\circ.$$

Dabei bezeichne D° die zu D duale k-Algebra, d.h. den k-Vektorraum D dessen k-Algebra-Multiplikation sich von der Multiplikation von D in der Reihenfolge der Faktoren unterscheidet, d.h. der D-Vektorraum mit der Multiplikation

$$a \circ b := b \bullet a,$$

wenn "•" die Multiplikation von D bezeichnet.
Bemerkung zu den beiden äußeren Isomorphien: Aus Symmetriegründen können wir uns auf die linke Isomorphie beschränken. Wir betrachten die Abbildung

$$(1) \qquad D^\circ \longrightarrow \mathrm{End}_A(D^n),\ d \mapsto (v \mapsto vd).$$

Dies ist offensichlich ein injektiver Ring-Homomorphismus. Beweisen wir die Surjektivität. Sei

$$f \in \mathrm{End}_A(D^n).$$

Die Abbildung ist eine A-lineare Abbildung

$$f: D^n \longrightarrow D^n.$$

Insbesondere gilt

$$f(a \bullet v) = a \bullet f(v) \text{ für } v \in D^n \text{ und } a \in A = M_n(D).$$

Bezeichne $e_i \in D^n$ den i-ten Standard-Einheitsvektor und E_{ij} die $n \times n$-Matrix mit einer Eins in der Position (i,j) und Nullen in allen anderen Positionen. Dann hat das Bild von e_1 bei f die Gestalt

$$f(e_1) = f(E_{11}e_1) = E_{11} \bullet f(e_1) = \begin{pmatrix} d' \\ 0 \\ \dots \\ 0 \end{pmatrix} = e_1 \bullet d \text{ mit } d \in D.$$

Also ist

$$f(e_i) = f(E_{i1} \bullet e_1) = E_{i1} \bullet f(e_1) = E_{i1} \bullet e_1 \bullet d = e_i \bullet d$$

für i = 1, ... , d. Für beleibiges

$$x = \sum_{i=1}^{n} x_i e_i \in D^n$$

erhalten wir damit

$$f(x) = \sum_{i=1}^{n} x_i f(e_i) = \sum_{i=1}^{n} x_i e_i d = x \bullet d.$$

Mit anderen Worten, f liegt im Bild von (1), d.h. diese Abbildung ist ein Isomorphismus.
Wir haben gezeigt, die Duale von D und D' sind isomorph. Dann sind es aber auch D und D'.
QED.

2.1.10 Folgerung

Sei k ein algebraisch abgeschlossener Körper. Dann ist jede zentrale einfache k-Algebra isomorp zu einer vollen Matrizen-Algebra $M_n(k)$ mit einer natürlichen Zahl n.

Beweis. Nach dem Satz von Wedderburn 2.1.5 reicht es zu zeigen, die einzige endlich-dimensionale Divisionsalgebra D über k ist k selbst. Sei $D \supseteq k$ ein solche Algebra. Für jedes $d \in D - \{0\}$ sind die Potenzen von d linear abhängig über k, d.h. es gibt ein Polynom

$$f \in k[x] - \{0\}$$

mit

$$f(d) = 0.$$

Weil D als Divisionsalgebra nullteilerfrei ist, können wir annehmen, f ist irreduzibel. Der k-Algebra-Homomorphismus

$$k[x] \longrightarrow D,\ p(x) = p(d),$$

hat dann den Kern $f \bullet k[x]$ und ein Bild, welches d enthält. Wir erhalten eine Einbettung von k-Algebren,

$$k[x]/f \bullet k[x] \longrightarrow D,$$

deren Bild das Element d enthält. Links steht aber eine algebraische Körpererweiterung von k. Da k algebraisch abgeschlossen ist, fällt diese mit k zusammen, d.h. es gilt

$$d \in k.$$

Wir haben gezeigt, $D \subseteq k$, d.h. es gilt D = k.
QED.

2.2 Zerfällungkörper

2.2.1 Charakterisierung der zentralen einfachen Algebren

Seien k ein Körper und A eine endlich-dimensionale k-Algebra. Dann sind folgende Ausagen äquivalent.
(i) A ist zentral und einfach.
(ii) Es gibt eine natürliche Zahl n und eine endliche Körpererweiterung K/k mit

$$A \otimes_k K \cong M_n(k).$$

Bemerkung
Zum Beweis benötigen wir das folgende Lemma.

2.2.2 Zentralität und Einfachheit beim Wechsel des Grundkörpers

Seien k ein Körper und A eine endlich-dimensionale k-Algebra. Dann sind folgende Ausagen äquivalent.
(i) A ist zentral und einfach.
(ii) Es gibt eine endliche Körper-Erweiterung K/k derart, daß $A \otimes_k K$ zentral und einfach ist.
(iii) Für jede endliche Körper-Erweiterung K/k ist $A \otimes_k K$ zentral und einfach.

Beweis. (ii) $\Rightarrow$ (i). Angenommen, A ist nicht einfach. Dann gibt es ein zwei-seitiges Ideal

$$I \subseteq A,$$

welches von 0 und A verschieden ist. Dann ist aber

$$I \otimes_k K \subseteq A \otimes_k K$$

ein zweiseitiges Ideal. Dieses ist von 0 und $A \otimes_k K$ verschieden (auf Grund der auftretenden Dimensionen) im Widerspruch zu der Annahme, daß $A \otimes_k K$ einfach sein soll. Mit $A \otimes_k K$ ist also auch A einfach.

Angenommen, A ist nicht zentral. Dann besteht eine echte Inklusion

$$k \subset Z := Z(A).$$

Tensorieren mit K über k liefert eine echte Inklusion

$$K \subset Z \otimes_k K$$

(weil die Dimensionen beim Tensorieren erhalten bleiben). Nun liegt aber der Vektorraum rechts ganz im Zentrum $Z(A \otimes_k K)$ von $A \otimes_k K$ im Widerspruch zu Annahme, daß $A \otimes_k K$ zentral sein soll.

(iii) $\Rightarrow$ (ii). Triviial.

(i) $\Rightarrow$ (iii). Sei K/k ein endliche Körpererweiterung.

1. Schritt: Reduktion auf den Fall, daß A eine Divisionsalgebra D ist.
Nach dem Satz von Wedderburn hat A als einfache k-Algebra die Gestatl

$$A = M_n(D)$$

mit einer Divisionsalgebra D. Weil A zentral sein soll, gilt

$$k = Z(A) = Z(M_n(D)) = Z(D),$$

d.h. die Divisionsalgebra D ist zentral (und trivialerweise einfach). Die zu beweisende Aussage (iii) besagt, daß die folgende K-Algebra zentral und einfach ist:

$$A \otimes_k K = M_n(D) \otimes_k K = M_n(D \otimes_k K).$$

Ist $D \otimes_k K$ zentral und einfach über K, so ist auch $A \otimes_k K$ zentral:

$$Z(A \otimes_k K) = Z(M_n(D \otimes_k K)) = Z(D \otimes_k K) = K.$$

Bleibt die Einfachheit von $A \otimes_k K$, d.h. die Aussage, daß jedes von 0 verschiedene Ideal

$$I \subseteq A \otimes_k K = M_n(D \otimes_k K)$$

gleich $A \otimes_k K$ ist. Sei

$$I_{ij} = \{x \in D \otimes_k K \mid \begin{array}{c}\text{es gibt eine Matrix von } M_n(D \otimes_k K) \\ \text{mit dem Eintrag x in der Position (i,j)}\end{array}\}$$

Weil I ein Ideal von $M_n(D \otimes_k K)$ ist, ist I_{ij} eine Ideal von $D \otimes_k K$. Weil I von 0 verschieden ist, ist I_{ij} für mindestens ein Paar (i,j) von Null verschieden. Weil $D \otimes_k K$ einfach sein soll, gilt

$$I_{ij} = D \otimes_k K \text{ für mindestens ein Paar (i,j).}$$

Es gibt also eine Matrix $M \in I$, deren Eintrag in der Position (i,j) gleich 1 ist. Dann gilt aber

$$E_{ij} = E_{ii} M E_{jj} \in I$$

für mindestens ein Paar (i, j). Durch Multiplikation mit Elementarmatrizen von links und von rechts sehen wir, dies ist dann der Fall für jedes i und jedes j. Da die E_{ij} aber die Algebra $M_n(D\otimes_k K)$ über $D\otimes_k K$ (also erst reicht über $M_n(D\otimes_k K)$) erzeugten, folgt $I = M_n(D\otimes_k K)$.

Wir haben gezeigt, die Algebra $A\otimes_k K = M_n(D\otimes_k K)$ ist einfach und zentral, falls die Algebra $D\otimes_k K$ einfach und zentral ist.

2. Schritt: der Fall, daß A = D eine Divisionsalgebra ist.

Sei

$$w_1, \dots, w_n \in K$$

eine Basis des k-Vektorraums K,

$$K = kw_1 + \dots + kw_n \text{ , } \dim_k K = n.$$

Dann bilden die Tensoren

$$1\otimes w_1, \dots, 1\otimes w_n \in D\otimes_k K$$

eine Basis des linken D-Vektorraums $D\otimes_k K$,

$$D\otimes_k K = D\bullet(1\otimes w_1) + \dots + D\bullet(1\otimes w_n).$$

Bestimmen wir das Zentrum von $D\otimes_k K$. Jedes Element

$$x \in Z(D\otimes_k K)$$

können wir in der Gestalt

$$x = \sum_{i=1}^{n} \alpha_i\bullet(1\otimes w_i) \text{ mit } \alpha_i \in D. \tag{1}$$

schreiben. Da x im Zentrum liegt, wird x bei Konjugation mit $d\otimes 1$ für jedes $d\in D$ in sich abgebildet:

$$x = (d\otimes 1)^{-1}x(d\otimes 1) = (d^{-1}\otimes 1)x(d\otimes 1) = \sum_{i=1}^{n} d^{-1}\alpha_i d\bullet(1\otimes w_i).$$

Vergleich mit (1) zeigt, es gilt

$$d^{-1}\alpha_i d = \alpha_i \text{ für jedes i und jedes } d \in D.$$

Es folgt

$$\alpha_i \in Z(D) = k,$$

denn D = A ist nach Voraussetzung eine zentrale k-Algebra. Es folgt

$$x \in k\otimes_k K = K.$$

Wir haben gezeigt, jedes Element x aus dem Zentrum von $D\otimes_k K$ liegt in K, d.h. die Algebra $D\otimes_k K$ ist zentral über K.

Wir haben noch zu zeigen, die Algebra $D\otimes_k K$ ist einfach. Sei J ein von Null verschiedenes Ideal dieser Algebra,

$$0 \neq J \subseteq D\otimes_k K$$

Da $D\otimes_k K$ als linker D-Vektoraum endlich-dimensional ist, gilt dasselbe auch für das Ideal J. Sei

$$z_1, \dots, z_r \in J$$

eine D-Vektorraum-Basis von J,

$$J = Dz_1 + ... + Dz_r \text{ , } \dim_D J = r.$$

Nach dem Austauschsatz von Steinitz können wir die z_i zu einer D-Vektorraumbasis von $D\otimes_k K$ ergänzen, indem wir einige der $1\otimes w_j$ hinzufügen. O.B.d.A. können wir annehmen, die z_i bilden zusammen mit den n-r letzen $1\otimes w_j$ eine solche Basis,

$$D\otimes_k K = Dz_1 + ... + Dz_r + D\bullet(1\otimes w_{r+1}) + ... + D\bullet(1\otimes w_n).$$

Insbesondere lassen sich die r ersten $1\otimes w_j$ als D-Linearkombinationen dieser neuen Basiselemente schreiben:

$$(2) \qquad 1\otimes w_i = \sum_{j=r+1}^{n} \alpha_{ij}\bullet(1\otimes w_j) + y_i \text{ mit } \alpha_{ij} \in D \text{ und } y_i \in J.$$

Wir haben hier die D-Linearkombinationen der $z_i \in J$ zusammengefäßt zu Elementen y_i (die natürlich im Ideal J liegen). Die Elemente y_i sind linear unabhängig über D, da die $1\otimes w_i$ es sind. Insbesondere bilden sie wieder eine D-Vektorraum-Basis von J,

$$J = Dy_1 + ... + Dy_r .$$

Weil J nach Voraussetzung ein zweiseitiges Ideal ist, liegen die Elemente

$$(d\otimes 1)^{-1} y_i (d\otimes 1)$$

für jedes i und jedes $d \in D$ in J, d.h.

$$(d\otimes 1)^{-1} y_i (d\otimes 1) = \sum_{\ell=1}^{r} \beta_{i\ell} y_\ell \text{ mit } \beta_{i\ell} \in D.$$

Wir verwenden (2) um die y_i mit Hilfe der $1\otimes w_j$ auszudrücken und erhalten:

$$1\otimes w_i - \sum_{j=r+1}^{n} (d^{-1}\alpha_{ij}d)\bullet(1\otimes w_j) = \sum_{\ell=1}^{r} \beta_{i\ell}(1\otimes w_\ell) - \sum_{\ell=1}^{r} \beta_{i\ell} \sum_{j=r+1}^{n} \alpha_{\ell j}\bullet(1\otimes w_j).$$

Koeffizientenvergleich liefert

$$\beta_{ii} = 1 \text{ und } \beta_{i\ell} = 0 \text{ für } i \neq \ell.$$

Weiter muß gelten

$$d^{-1}\alpha_{ij}d = \alpha_{ij} \text{ für jedes } d \in D.$$

Da D = A nach Voraussetzung zentrale k-Algebra ist, folgt $\alpha_{ij} \in k$ für alle i und j. Aus (2) erhalten wir

$$y_i \in k\otimes_k K = K,$$

d.h. die Erzeuger y_i des Ideals J liegen in $1\otimes K$. Da $J \neq 0$ ist, ist die Anzahl dieser Erzeuger > 0. Da J ein rechtes Ideal ist und K ein Körper (und $z_1 \neq 0$), folgt

$$1\otimes 1 \subseteq J.$$

Da J ein zweiseitiges Ideal ist, folgt

$$D\otimes_k K = D\bullet(1\otimes 1\bullet K) \subseteq J,$$

d.h. J ist die gesamte Algebra. Wir haben gezeigt, die Algebra $D\otimes_k K$ ist einfach.

QED.

2.2.3 Beweis des Satzes 2.2.1

(ii) ⇒ (i). Sei $A\otimes_k K$ eine volle Matrizen-Algebra. Dann ist $A\otimes_k K$ zentral über K und nach 2.1.3 einfach. Wegen 2.2.2 ist dann aber auch A zentrale und einfache k-Algebra.

(i) ⇒ (ii). Sei A eine zentrale einfache k-Algebra. Wir bezeichnen mit

$$\overline{k}$$

die algebraische Abschließung von k. Dann ist nach 2.2.2 auch

$$A\otimes_k \overline{k}$$

eine zentrale einfache $\overline{k}$-Algebra[37] und nach 2.1.0 folgt

$$A\otimes_k \overline{k} \cong M_n(\overline{k}).$$

Nun gilt

$$A\otimes_k \overline{k} = \bigcup A\otimes_k K$$

wenn rechts K die endlichen Körpererweiterungen K/k mit $K \subseteq \overline{k}$ durchläuft. Wir können deshalb K so groß wählen, daß die Algebra $A\otimes_k K$ die Elemente

$$e_{ij} \in A\otimes_k \overline{k}$$

enthält, die den Standard-Erzeugern

$$E_{ij} \in M_n(\overline{k})$$

der Matrizen-Algebra entsprechen. Die Strukturkonstanten $\alpha^{ij}_{\alpha\beta\gamma\delta}$ zu diesen Standard-Erzeugern,

$$E_{\alpha\beta}\bullet E_{\gamma\delta} = \sum_{ij} \alpha^{ij}_{\alpha\beta\gamma\delta}\, E_{ij}\ ,$$

liegen dann automatisch in K (sie liegen sogar in $\mathbb{Z}$). Die K-lineare Abbildung

$$M_n(K) \longrightarrow A\otimes_k K,\ E_{ij} = e_{ij}\ ,$$

ist dann ein K-Algebra-Homomorphismus, der nach Tensorieren mit $\overline{k}$ ein Isomorphismus wird. Also ist er selbst schon eine Isomorphismus.[38]

---

[37] Das gilt zunächst nur für

$$A\otimes_k K \text{ und } K \subseteq \overline{k} \text{ endlich über k.}$$

Nun ist aber

$$\overline{k} = \bigcup_{K\subseteq\overline{k} \text{ endlich über k}} K$$

also

$$A\otimes_k \overline{k} = \bigcup_{K\subseteq\overline{k} \text{ endlich über k}} A\otimes_k K.$$

Die Zentraliät und Einfachheit der $A\otimes_k K$ überträgt sich deshalb auf $A\otimes_k \overline{k}$.

[38] Wir haben eine exakte Sequenz von K-linearen Abildundungen

$$0 \longrightarrow K \longrightarrow M_n(\overline{k}) \longrightarrow A\otimes_k K \longrightarrow C \longrightarrow 0.$$

Anwenden des Funktors $\otimes_k \overline{k}$ liefert eine exakte Sequenz

$$0 \longrightarrow K\otimes_k \overline{k} \longrightarrow M_n(\overline{k})\otimes_k \overline{k} \longrightarrow A\otimes_k K\otimes_k \overline{k} \longrightarrow C\otimes_k \overline{k} \longrightarrow 0,$$

wobei die Abbildung in der Mitte ein Isomorphismus ist. Deshalb gilt

$$K\otimes_k \overline{k} = 0 = C\otimes_k \overline{k},$$

QED.

2.2.4 Die Dimension einer zentralen einfach Algebra

Die Dimension einer zentralen einfachen k-Algebra A ist das Quadrat einer natürlichen Zahl.

Beweis. Nach 2.2.2 gibt es eine endliche algebraische Erweiterung K/k mit

$$A\otimes_k K \cong M_n(K)$$

für ein n. Dann ist aber

$$\dim_k A = \dim_K A\otimes_k K = \dim_K M_n(K) = n^2$$

QED.

2.2.5 Definition: Zerfällingkörper und Grad

Sei A eine zentrale einfache k-Algebra. Ein endlicher algebraischer Erweiterungskörper K von k heißt Zerfällungskörper der Algebra A, wenn

$$A\otimes_k K$$

isomorph ist zu einer vollen Matrizen-Algebra $M_n(K)$ über K. Die natürliche Zahl

$$n = \sqrt{\dim_K M_n(K)} = \sqrt{\dim_K A\otimes_k K} = \sqrt{\dim_k A}$$

heißt Grad von A über k.

2.2.6 Existenz eines separablen Zerfällungskörpers (Noether, Köthe)

Jede zentrale einfache k-Algebra besitzt einen Zerfällungskörper, der separabel über k ist.

Beweis. Wir können annehmen, k ist ein Körper der positiven Charakteristik p. Angenommen, es gibt eine zentrale einfache k-Algebra A, welche über keiner endlichen separablen Körpererweiterung von k zerfällt. Sei

$$\overline{k}$$

der algebraische Abschluß von k und

$$k^S \subseteq \overline{k}$$

die separable Abschließung von k in $\overline{k}$. Nach 2.2.2 ist $A\otimes_k K$ zentral und einfach für jede endliche Teilerweiterung $K \subseteq k^S$, so daß auch $A\otimes_k k^S$ zentral und einfach über k^S ist. Nach dem Satz von Wedderburn 2.1.5 gilt

(1) $$A\otimes_k k^S \cong M_n(D)$$

mit einer Divisionsalgebra D über k^S von endlicher Dimension n. Weil die Teilalgebra $A\otimes_k K$ für keine der endlichen Teilerweiterungen $K \subseteq k^S$ von k zerfällt, kann auch (1) nicht zerfallen über k^S (nach demselben Argument wie am Ende des Beweises 2.2.3). Insbesondere ist die Divisionsalgebra D von k^S verschieden,

(2) $$k^S \neq D.$$

Weil (1) zentral und einfach über k^S ist, gilt dasselbe für D und damit für $D\otimes_{k^S} K$, wenn $K \subseteq \overline{k}$ die endlichen Teilerweiterungen von k^S durchläuft. Dann ist aber auch $D\otimes_{k^S} \overline{k}$ zentral und einfach. Nach 2.1.10 gilt

---

also K = 0 = C. Mit anderen Worten, $M_n(\overline{k}) \longrightarrow A\otimes_k K$ ist ein Isomorphismus.

(3) $$D \otimes_{k^s} \overline{k} \cong M_d(\overline{k}) \text{ mit } d > 1$$

(im Fall d = 1 wäre $D = k^s$ im Widerspruch zu (2)). Wir fixieren jetzt eine k^s-Vektorraumbasis von D, sagen wir

$$D = k^s \bullet v_1 + \ldots + k^s \bullet v_{d^2}$$

Die beiden Algebren von (3) identifizieren wir jetzt mit $\overline{k}^{d^2}$, und zwar die linke Seite bezüglich der Basis der $v_i \otimes 1$ und die rechte bezüglich der Basis der Elementarmatrizen E_{ij}... Wir erhalten so ein kommutatives Diagramm

$$\begin{array}{ccccc} D & \subseteq & D \otimes_{k^s} \overline{k} & \xrightarrow{f} & M_d(\overline{k}) \xrightarrow{\det} \overline{k} \\ v_i \downarrow & \cong & 1 \otimes v_i \downarrow & \cong & E_{ij} \downarrow \cong \quad \| \\ (k^s)^{d^2} & \subseteq & \overline{k}^{d^2} & \xrightarrow{A} & \overline{k}^{d^2} \xrightarrow{\det} \overline{k} \end{array} \tag{4}$$

von linearen Abbildungen. Die vertikalen Isomorphismen sind dabei durch die angegebenen Basen definiert, die Abbildung f ist eine Realisierung der Isomorphie (3) und A soll die Matrix von f bezüglich der angegebenen Basen bezeichnen.

Bezeichne

$$F: \overline{k} \longrightarrow \overline{k},\ x \mapsto x^p,$$

die Frobenius-Abbildung. Weil $\overline{k}$ algebraisch abgeschlossen ist, ist F ein Isomorphismus. Ebenfalls mit F bezeichnen wir die Abbildung

$$F: \overline{k}^{d^2} \longrightarrow \overline{k}^{d^2}, \begin{pmatrix} x_1 \\ \ldots \\ x_{d^2} \end{pmatrix} \mapsto \begin{pmatrix} F(x_1) \\ \ldots \\ F(x_{d^2}) \end{pmatrix}$$

die man durch Anwenden der Frobenius-Abbildung auf die Koordinaten der Vektoren erhält. Weil die Determinante ein Polynom mit ganzzahligen Koeffizienten ist, gilt dann nach dem kleinen Fermatschen Satz

$$\det(F(v)) = F(\det(v)) \text{ für jedes } v \in \overline{k}^{d^2},$$

d.h. es besteht ein kommutatives Viereck

$$\begin{array}{ccc} \overline{k}^{d^2} & \xrightarrow{\det} & \overline{k} \\ F \downarrow & & \downarrow F \\ \overline{k}^{d^2} & \xrightarrow{\det} & \overline{k} \end{array}$$

Durch wiederholtes Zusammensetzen von (4) mit diesem Viereck erhalten wir für jedes t = 1,2,3,... ein kommutatives Diagramm

$$\begin{array}{ccccc} D & \subseteq & D \otimes_{k^s} \overline{k} & \xrightarrow{f} & M_d(\overline{k}) \xrightarrow{\det} \overline{k} \\ v_i \downarrow & \cong & 1 \otimes v_i \downarrow & \cong & \downarrow \cong \quad F^t \downarrow \\ (k^s)^{d^2} & \subseteq & \overline{k}^{d^2} & \xrightarrow{F^t \circ A} & \overline{k}^{d^2} \xrightarrow{\det} \overline{k} \end{array} \tag{5}$$

Dabei bezeichne $F^t \circ A$ die Matrix, die man duch Anwenden von F^t auf die Einträge von A erhält.

Weil $\overline{k}$ rein inseparabel über k^s ist, gibt es ein $t \in \mathbb{N}$ mit der Eigenschaft, daß F^t die endlich vielen Einträg der Matrix A in k^s abbildet, d.h.

$$F^t \circ A \in M_{d^2}(k^s).$$

Wegen

$$\det (F^t \circ A) = F^t(\det (A)) \neq^{39} 0.$$

definiert $F^t \circ A$ einen Isomorphismus. Die untere Zeile von (5) identifiziert also die Algebra D mit dem Raum

$$(k^s)^{d^2} \subseteq \overline{k}^{d^2}$$

der k^s-rationalen Punkte von $\overline{k}^{d^2}$, d.h. mit

$$M_d(k^s) \subseteq M_d(\overline{k}).$$

Nun ist D eine Divisionsalgebra. Die Elemente $d \in D - \{0\}$ entsprechen umkehrbaren Matrizen in $M_d(\overline{k})$, d.h. Matrizen mit einer von Null verschiedenen Determinante. Die Determinante muß also in den k^s-rationalen Punkten von $\overline{k}^{d^2}$ ungleich Null sein,

$$M_d(k^s) \bigcap V(\det) = \{0\}$$

Dies ist offensichtlich falsch: zum Beispiel liegen die Matrizen E_{ij} im Durchschnitt auf der linken Seite[40].
QED.

Bemerkung

Nach einem allgemeinen Satz der algebraischen Geometrie liegen die k^s-rationalen Punkte einer über k^s definierten Varietät sogar dicht in der Menge der geometrischen Punkte (siehe Borel: Linear algebraic groups, Chapter I, Corollary 13.3).

2.2.7 Folgerung

Sei A eine endlich-dimensionale k-Algebra. Dann sind folgende Aussagen äquivalent.

(i) A ist zentral und einfach über k.

(ii) Es gibt eine endliche Galois-Erweiterung K/k und eine natürliche Zahl n mit

$$A \otimes_k K \cong M_n(K).$$

Beweis. Das ergibt sich aus 2.2.2, 2.2.6 und der Tatsache, daß jede endliche separable Erweiterung in einer Galois-Erweiterung liegt.
QED.

2.2.8 Bemerkungen

(i) Die Isomorphie $A \otimes_k K \cong M_n(K)$ ist im allgemeinen nicht mit der Operation der Galoisgruppe G = Gal(K/k) verträglich. Andernfalls könnte man auf beiden Seiten zum G-invarianten Teil übergehen und würde so eine Isomorphie $A \cong M_n(k)$ erhalten.

(ii) Die klassischen Beweise des Satze von Noether und Köthe konstruieren einen Zerfällungskörper K der Algebra, der ganz in A liegt. Eine Galois-Erweiterung dieser Art muß im allgemeinen nicht existieren (wie dies von Amisur [2] - sieh auch Pierce [1] gezeigt wurde). Zentrale einfache Algebren mit dieser zusätzlichen Eigenschaft heißen Kreuzprodukte.

---

[39] A ist die Determinante eines linearen Isomorphismus.

[40] wegen d > 1.

2.3 Galois-Abstieg

Unser nächstes Ziel besteht in der Klassifikation der zentralen einfachen Algebren. Wir benötigen dafür einige Vorbereitungen.

2.3.1 Vektorräume mit Tensor vom Typ (p, q)

Sei V ein (endlich-dimensionaler) k-Vektorraum. Wir bezeichnen mit

$$V^* := \mathrm{Hom}_k(V, k)$$

dessen Dual, d.h. den k-Vektorraum der k-linearen Abbildungend $V \longrightarrow k$.

Ein Tensor vom Typ (p, q) ist ein Element von

$$T^{pq}(V) := V^{\otimes p} \otimes_k (V^*)^{\otimes q}.$$

Dabei seien p und q nicht-negative ganze Zahlen, die 0-te Tensorpotenz eines k-Vektorraums sei nach Definition gleich k. Ein k-Vektorraum mit Tensor vom Typ (p, q) ist ein Paar

$$(V, \Phi)$$

mit einem k-Vektorraum V und einem $\Phi \in T^{pq}(V)$. Wir werden auch einfach von k-Objekten (V, Φ) sprechen.

Bemerkungen

(i) Es besteht eine Isomorphie von k-Vektorräumen

(1) $$V^{\otimes p} \otimes_k (V^*)^{\otimes q} \longrightarrow \mathrm{Hom}_k(V^{\otimes q}, V^{\otimes p}),$$

$$v_1 \otimes ... \otimes v_p \otimes \ell_1 \otimes ... \otimes \ell_q \mapsto (w_1 \otimes ... \otimes w_q \mapsto \ell_1(w_1) \bullet ... \bullet \ell_q(w_q) \bullet v_1 \otimes ... \otimes v_p).$$

Zum Beweis betrachte man die multilineare Abbildung

$$V^p \times (V^*)^q \longrightarrow \mathrm{Hom}_k(V^{\otimes q}, V^{\otimes p})$$

$$(v_1, ..., v_p, \ell_1, ..., \ell_q) \mapsto (\ell_1 \otimes ... \otimes \ell_q) \bullet (v_1 \otimes ... \otimes v_p)$$[41]

Sie induziert die Abbildung (1) und hat dieselbe Universalitätseigenschaft für (p+q)-lineare Abbildungen wie die natürliche Abbildung

$$V^p \times (V^*)^q \longrightarrow V^{\otimes p} \otimes_k (V^*)^{\otimes q}$$

$$(v_1, ..., v_p, \ell_1, ..., \ell_q) \mapsto v_1 \otimes ... \otimes v_p \otimes \ell_1 \otimes ... \otimes \ell_q.$$

Mit anderen Worten, (1) ist ein Isomorphismus.

(ii) Ist $v_1, ..., v_n$ eine Basis von V und $v_1^*, ..., v_n^*$ die zugehörige dualse Basis von V*. Dann bilden die Elemente der Gestalt

$$v_{i_1} \otimes ... \otimes v_{i_p} \otimes v_{j_1}^* \otimes ... \otimes v_{j_q}^*$$

eine Basis von $V^p \times (V^*)^q$. Ein (p,q)-Tensor von V ist somit ein Element der der Gestalt

$$\tau = \sum_{i_1, ... i_p, j_1, ..., j_q} c_{j_1 ... j_q}^{i_1 ... i_p} \, v_{i_1} \otimes ... \otimes v_{i_p} \otimes v_{j_1}^* \otimes ... \otimes v_{j_q}^*$$

---

[41] $\ell_1 \otimes ... \otimes \ell_q$ ist eine lineare Abbildung $V^{\otimes q} \longrightarrow k$ und $v_1 \otimes ... \otimes v_p$ ist ein Element von $V^{\otimes p}$.

mit $c^{i_1\ldots i_p}_{j_1\ldots j_q} \in k$. Die Konstanten $c^{i_1\ldots i_p}_{j_1\ldots j_q}$ bilden dann gerade einen p-fach kontravarianten und q-fach kovarianten Tensor im Sinne der Physik. Im Fall p + q = 2 sind das gerade n×n-Matrizen, die sich bei Basiswechsel in bestimmter Weise verhalten. Für p + q > 2 erhält man höherdimensionale Varianten des Matrixbegriffs. Wir werden sagen, die

$$c^{i_1\ldots i_p}_{j_1\ldots j_q}$$

sind die Koordinaten des Tensors τ bezüglich der gegebenen Basis von V.

2.3.2 Beispiele

Der Fall $\Phi = 0$.

In dieser Situation kann (V, Φ) mit V identifiziert werden, d.h. (V, Φ) ist ein k-Vektorraum ohne irgendeine Zusatzstruktur.

Der Fall p = q = 1

In dieser Situation ist Φ: $V \longrightarrow V$ ein k-linearer Endomorphismus.

Der Fall p = 0, q = 2

In dieser Situation ist Φ eine k-lineare Abbildung $V \otimes_k V \longrightarrow k$, d.h. eine Bilinearform

$V \times V \longrightarrow k$

über k.

Der Fall p = 1, q = 2

In dieser Situation ist Φ eine k-lineare Abbildung $V \otimes_k V \longrightarrow V$, d.h. eine bilineare Abbildung

$$V \times V \longrightarrow V.$$

Insbesondere ist die Struktur einer k-Algebra dem k-Vektorraum V durch eine solche Abbildung gegeben, die außerdem noch dem Assoziativgesetzt genügt.

2.3.3 Isomorphismen von Vektorräumen mit (p,q)-Tensor

Seien

$$(V, \Phi) \text{ und } (W, \Psi)$$

zwei Vektorräume mit (p, q)-Tensor. Diese heißen isomorph, falls es einen k-linearen Isomorphismus

$$f: V \longrightarrow W$$

gibt mit der Eigenschaft, daß der zugehörige Isomorphismus

$$T^{pq}(f) := f^{\otimes p} \otimes (f^{*-1})^{\otimes q}: V^{\otimes p} \otimes_k (V^*)^{\otimes q} \longrightarrow W^{\otimes p} \otimes_k (W^*)^{\otimes q}$$

den Tensor Φ in den Tensor Ψ abbildet,

$$T^{pq}(\Phi) = \Psi.$$

Man sagt dann auch, f ist ein Isomorphismus

$$f: (V, \Phi) \longrightarrow (W, \Psi)$$

von k-Vektorräumen mit (p, q)-Tensor.

2.3.4 Twists von Vektorräumen mit (p,q)-Tensor

Sei K/k eine endliche Galois-Erweiterung des Körpers k mit der Galois-Gruppe

$$G = Gal(K/k).$$

Für jeden k-Vektorraum V schreiben wir

$$V_K := V \otimes_k K$$

und für jeden (p, q)-Tensor $\Phi \in Hom_k(V^{\otimes q}, V^{\otimes p})$ sei

$$\Phi_K$$

der zugehörige (p, q)-Tensor von V_K.[42]

Seien (V, Φ) und (W, Ψ) zwei k-Vektorräume mit (p, q)-Tensor. Man sagt diese sind isomorph über K, wenn es einen K-Isomorphismus

$$(V_K, \Phi_K) \longrightarrow (W_K, \Psi_K)$$

gibt. In dieser Situation sagt man auch, (V, Φ) und (W, Ψ) sind K/k-getwistete Formen oder K/k-Twists voneinander.

Bemerkung

Wir wollen jetzt die Galois-Theorie benutzen, die k-Isomorphie-Klassen von Vektorräumen mit (p, q)-Tensor zu klassifizieren. Genauer: für einen gegebenen k-Vektorraum mit (p,q)-Tensor wollen wir mit Hilfe der Galois-Theorie alle K/k-Twist dieses Vektorraums bestimmen.

Insbesondere wird uns dies zur Betrachtung der Gesamtheit aller zentralen einfachen Algebren A führen. Nach unserer bisherigen Erfahrung ist die Struktur der Algebra $A \otimes_k K$ um so einfacher, je größer der Körper K ist. Unser Ziel ist es, uns eine Übersicht über alle A mit vorgegebenen $A \otimes_k K$ zu verschaffen.

2.3.5 Die Operation der Galois-Gruppe auf den Automorphismen eines Vektorraums mit (p,q)-Tensor

Seien K/k eine endliche Galois-Erweiterung des Körpers k mit der Galois-Gruppe

$$G = Gal(K/k),$$

(V, Φ) und (W, Ψ) zwei k-Vektorräume mit (p,q)-Tensor und

(1) $$f: (V_K, \Phi_K) \longrightarrow (W_K, \Psi_K)$$

ein K-linearer Isomorphismus. Aus jedem k-Automorphismus

$$\sigma: K \longrightarrow K$$

erhält man durch Tensorieren mit V über k einen k-linearen Automorphismus

$$1 \otimes \sigma: V \otimes_k K \longrightarrow V \otimes_k K,$$

den wir ebenfalls mit σ bezeichnen werden. Durch Zusammensetzen mit f erhalten wir eine K-lineare Abbildung[43]

---

[42] Ist $v_1,...,v_n$ eine Basis von V, so ist Φ_K der Tensor, der bezüglich der Basis

$$v_1 \otimes 1,...,v_n \otimes 1$$

von V_K über K dieselben Koordinaten hat wie Φ bezüglich der Basis $v_1,...,v_k$.

[43] Für $v \in V_K$ und $c \in K$ gilt

$$\begin{aligned}
\sigma(f)(cv) &= (1 \otimes \sigma) \circ f \circ (1 \otimes \sigma^{-1})(cv) \\
&= (1 \otimes \sigma) \circ f(\sigma^{-1}(c) \bullet (1 \otimes \sigma^{-1})(v)) \\
&= (1 \otimes \sigma) \bullet (\sigma^{-1}(c) f((1 \otimes \sigma^{-1})(v)) \qquad \text{(f ist K-linear)} \\
&= c \bullet (1 \otimes \sigma)(f((1 \otimes \sigma^{-1})(v))) \\
&= c \bullet \sigma(f)(v).
\end{aligned}$$

$$\sigma(f) = (1\otimes\sigma)\circ f\circ(1\otimes\sigma^{-1}): (V_K, \Phi_K) \longrightarrow (W_K, \Psi_K).$$

Mit f ist auch $\sigma(f)$ ein Isomorphismus.[44] Die Abbildung

$$f \mapsto \sigma(f)$$

respektiert die Komposition der Abbildungen f. Wir bekommen somit eine Operation

$$G \times \mathrm{Aut}(\Phi) \longrightarrow \mathrm{Aut}(\Phi), (\sigma , f) \mapsto \sigma(f),$$

der Galois-Gruppe $G = \mathrm{Gal}(K/k)$ auf der Gruppe

$$\mathrm{Aut}(\Phi)$$

der K-linearen Automorphismen von (V, Φ).

Sei jetzt f ein K-linearer Isomorphismus. Dann ist für jedes $\sigma\in G$ die Komposition[45]

$$a_\sigma := f^{-1}\circ\sigma(f): (V_K, \Phi_K) \longrightarrow (V_K, \Phi_K)$$

ein K-linearer Isomorphismus. Wir erhalten so eine Abbildung

(2) $$G \longrightarrow \mathrm{Aut}(\Phi), \sigma \mapsto a_\sigma .$$

Bemerkungen

(i) Die Abbildung (2) ist im allgemeinen kein Gruppen-Homomorphismus. Es gilt

$$a_{\sigma\tau} = a_\sigma\circ\sigma(a_\tau)$$

(ii) Betrachten wir die Abhängigkeit der Abbildung (2) von der speziellen Wahl des Isomorphismus (1). Seien

$$g: (V_K, \Phi_K) \longrightarrow (W_K, \Psi_K)$$

ein weiterer K-linearer Automorphismus und $b_\sigma := g^{-1}\circ\sigma(g)$ das zugehörige Element von $\mathrm{Aut}(\Phi)$. Dann gilt

$$a_\sigma = c^{-1}\circ b_\sigma\circ\sigma(c)$$

mit einem Automorphismus c von (V_K, Φ_K).

Beweis. Zu (i): Es gilt

$$\begin{aligned} a_{\sigma\tau} &= f^{-1}\circ\sigma(\tau(f)) && \text{(nach Definition von a)}\\ &= f^{-1}\circ\sigma(f)\circ\sigma(f)^{-1}\circ\sigma(\tau(f)) \\ &= a_\sigma\circ\sigma(f^{-1}\circ\tau(f)) && \text{(nach Definiton von a)} \end{aligned}$$

Die Tensoren Φ_K und Ψ_K werden durch $1\otimes\sigma$ und $1\otimes\sigma^{-1}$ in sich abgebildet, da sie bezüglich einer über k definierten Basis in k liegende Koordinaten haben. Also bildet $\sigma(f)$ diese Tensoren ineinander ab.

[44] Fixiert man eine K-Vektorraumbasis von V_K, um V_K mit dem K^n zu identifizieren und f mit der Multiplikation mit einer Matrix A,

$$f: K^n \longrightarrow K^n, v \mapsto Av,$$

so wird $\sigma(f)$ zur Multiplikation

$$\sigma(f): K^n \longrightarrow K^n, v \mapsto (A(v^{\sigma^{-1}}))^\sigma = A^\sigma\bullet(v^{\sigma^{-1}})^\sigma = A^\sigma v$$

mit der Matrix A^σ, die man aus A erhält, indem man σ auf deren Einträge anwendet.

[45] Durch die Zusammensetzung $\sigma(f)$ mit dem Inversen von f erhalten wir ein Objekt, in welchem das vorgegebene Paar (W, Ψ) nicht mehr vorkommt.

$= a_\sigma \circ \sigma(a_\tau)$ (weil σ ein Automorphismus von Aut(Φ) ist)

Zu (ii). Mit $c = g^{-1} \circ f$ gilt

$a_\sigma = f^{-1} \circ \sigma(f)$ (nach Definiton von a)

$= c^{-1} \circ g^{-1} \circ \sigma(g \circ c)$ (nach Definition von c)

$= c^{-1} \circ g^{-1} \circ \sigma(g) \circ \sigma(c)$ (weil σ ein Automorphismus von Aut(Φ) ist)

$= c^{-1} \circ b_\sigma \circ \sigma(c)$

QED.

2.3.6 Gruppen-Kohomologie

Seien G und A zwei Gruppen und

$$G \longrightarrow \mathrm{Aut}(A)$$

eine Operation von G auf A durch Automorphismen. Ein 1-Kozyklus von G mit Werten in A ist eine Abbilddung

$$a : G \longrightarrow A, \sigma \mapsto a_\sigma,$$

mit

(1) $$a_{\sigma\tau} = a_\sigma \circ \sigma(a_\tau) \text{ für } \sigma, \tau \in G.$$

Zwei 1-Kozyklen a und b von G mit Werten in A heißen äquivalent oder auch kohomolog, wenn es ein Element

$$c \in A$$

gibt mit

(2) $$a_\sigma = c^{-1} \bullet b_\sigma \bullet \sigma(c) \text{ für } \sigma \in G.$$

Bemerkungen

(i) Die Kohomologie von 1-Kozyklen ist eine Äquivalenzrelation auf der Menge der 1-Kozyklen. Die Menge der Äquivalenz-Klassen der 1-Kozyklen von G mit Werten in A wird mit

$$H^1(G, A)$$

bezeichnet und heißt erste Kohomologiemenge von G mit Werten in A oder auch einfach erste Kohomologie von G mit Werten in A.

(ii) Die erste Kohomologie ist eine punktierte Menge. Das ausgezeichnete Element wird representiert vom 1-Kozyklus

$$G \longrightarrow A, \sigma \longrightarrow 1,$$

der alle Elemente von G ins neutrale Element von A abbildet. Wir nennen dieses Element auch Basispunkt.

(iii) Die Homologie-Klasse

$$[a_\sigma] \in H^1(\mathrm{Gal}(K/k), \mathrm{Aut}_K(\Phi))$$

des in 2.3.5 konstruierten 1-Kozyklus $\sigma \mapsto a_\sigma$ zum K-Isomorphismus

$$f: (V_K, \Phi_K) \longrightarrow (W_K, \Psi_K)$$

hängt nach Konstruktion nicht von der speziellen Wahl von f ab, sondern nur vom Twist

$$(W, \Psi)$$

des k-Vektorraums (V, Φ) mit (p, q)-Tensor. Wir sind jetzt in der Lage das Hauptergebnis dieses Abschnitts zu formulieren.

2.3.7 Abstiegssatz: Kohomologie und Isomorphie-Klassen von Twists

Seien (V, Φ) ein k-Objekt und K/k eine endliche Galois-Erweiterung. Bezeichne

$$TF_K(V_K, \Phi_K)$$

die Menge der Isomorphieklassen über k der K/k-Twists von (V, Φ). Wir betrachten diese Menge als punktiert durch die Isomorphieklasse von (V, Φ). Dann induziert die in 2.3.5 definierte Abbildung einen Isomorphismus punktierter Mengen

$$TF_K(V_K, \Phi_K) \longrightarrow H^1(Gal(K/k), Aut(\Phi)), (W, \Psi) \mapsto [a_\sigma].$$

Bemerkung
Bevor wir diesen Satz beweisen, betrachten wir einige Beispiele.

2.3.8 Beispiel: Hilberts Satz 90

Seien $V = k^n$ und Φ der triviale Tensor. Dann ist

$$Aut_K(\Phi) = GL(n, K)$$

gerade die allgemeine lineare Gruppe der $n \times n$-Matrizen über K. Nun sind aber zwei k-Vektorräume über k genau dann isomorph, wenn sie es über K sind (nämlich wenn sie dieselbe Dimension haben). Die punktierte Menge $TF_K(V_K, 0)$ ist deshalb trivial (d.h. einelementig) und der obige Satz besagt,

(1) $$H^1('Gal(K/k), GL(n, K)) = \{1\}.$$

Bemerkungen

(i) Diese Aussage geht auf Speiser zurück. Der Fall n = 1 heißt in der Literatur gewöhnlich Hilberts Satz 90, obwohl Hilbert nur den Fall zyklischer Erweiterungen K/k betrachtet hat.

(ii) Ist K/k eine zyklische Erweiterung des Grades d und σ ein Erzeuger der Galoisgruppe,

$$Gal(K/k) = < \sigma >,$$

so ist jeder 1-Kozyklus

$$G \longrightarrow GL(1,K) = K^*$$

bereits durch seinen Wert

$$a_\sigma$$

an der Stelle σ festgelegt: aus der Kozyklen-Bedingung erhält man

(2) $$a_{\sigma^i} =^{46} a_\sigma \sigma(a_\sigma) \bullet ... \bullet \sigma^{i-1}(a_\sigma)$$

für i = 1, ... , d. Speziell für i = d folgt

(3) $$a_\sigma \sigma(a_\sigma) \bullet ... \bullet \sigma^{n-1}(a_\sigma) = a_1 = 1.$$

Das zweite Gleichheitszeichen ergibt sich dabei aus der Kozyklen-Bedingung mit $\sigma = \tau = 1$. Umgekehrt definiert jedes Element $a \in K^*$, welches der Bedingung (3) genügt, vermittels der Formel (2) einen 1-Kozyklus.

Weiter ist

$$N(a_\sigma) := a_\sigma \sigma(a_\sigma) \bullet ... \bullet \sigma^{d-1}(a_\sigma)$$

---

[46] Für i = 2 ist dies die Kozyklen-Bedingung mit $\tau = \sigma$ und für allgemeines i erhält man die Identität durch Induktion nach i aus der Identität $a_{\sigma^{i+1}} = a_\sigma \sigma(a_{\sigma^i})$

gerade die Norm von a_σ bezüglich der Körpererweiterung K/k. Die Identität (1) übersetzt sich so zusammen mit der Korand-Bedingung 2.3.6 (2) in die folgende Aussage.

(iii) Ist K/k eine endliche zyklische Erweiterung mit der Galoisgruppe $G = <\sigma>$ und $a \in K$ ein Element der Norm 1, so gibt es ein Element $c \in K^*$ mit $a = c \bullet \sigma(c)^{-1}$.

2.3.9 Beispiel: Quadratische Formen

Seien V ein n-dimensionaler k-Vektorraum und Φ ein (0,2) -Tensor, der von einer symmetrischen Bilinearform

$$< , >: V \times V \longrightarrow k$$

kommt. Dann ist

$$Aut_K(\Phi) = O(n, K)$$

gerade die Gruppe der orthogonalen n×n-Matrizen bezüglich < , >, und wir erhalten eine Bijektion

$$TF_K(V, < , >) = H^1(Gal(K/k), O(n, K)),$$

die die Basispunkte respektiert. Diese Bijektion spielt eine wichtige Rolle bei der Klassifikation der quadratischen Formen.

Vormerkung zum Beweis von 2.3.7

Zum Beweis der Aussage von 2.3.7 werden wir die zur Abbildung

$$(W, \Psi) \mapsto \{a_\sigma\}$$

inverse Abbildung konstruieren. Dieses Vorgehen basiert auf der folgenden allgemeinen Konstruktion.

2.3.10 Konstruktion

Seien G und A Gruppen,

$$G \longrightarrow Aut(A), \sigma \mapsto (a \mapsto \sigma(a)),$$

ein Gruppen-Homomorphismus und X eine Menge, auf welcher G und A in verträglicher Weise operieren, d.h.

$$\sigma \bullet a \bullet x = \sigma(a) \bullet (\sigma \bullet x) \text{ für } x \in X, a \in A, \sigma \in G.$$

Weiter sei

$$a : G \longrightarrow A, \sigma \mapsto a_\sigma ,$$

ein 1-Kozyklus von G mit Werten in A. Wir verwenden jetzt diesen Kozyklus um aus der Operation

$$G \times X \longrightarrow X, (\sigma, x) \mapsto \sigma(x),$$

von G auf X eine weitere solche Operation zu gewinnen, welche die mit a <u>getwistete Operation</u> heißt. Die Operation sei wie folgt definiert.

$$G \times X \longrightarrow X, (\sigma, x) \mapsto a_\sigma(\sigma(x)).$$

Dies ist tatsächlich eine Operation: es gilt

$$a_{\sigma\tau}(\sigma\tau(x)) = a_\sigma \sigma(a_\tau)(\sigma\tau(x)) \quad \text{(wegen der Kozyklen-Bedingung)}$$

$$= a_\sigma \sigma(a_\tau \tau(x)) \quad \text{(weil G durch Automorphismen operiert).}$$

Wir bezeichnen mit

$${}^aX$$

die mit der getwisteten Operation versehene Menge X.

Bemerkung

Ist X mit einer algebraischen Struktur versehen - zum Beispiel mit der Struktur einer Gruppe oder eines Vektorraums - und operieren G und A durch Autormorphismen auf X, so ist die getwistete Operation ebenfalls eine Operation durch Automorphismen.

2.3.11 Warnung

Wir weisen darauf hin, daß die obige Konstruktion nur auf der Ebene der Kozyklen ausgeführt werden kann und nicht auf der der Kohomologie-Klassen: kohomologe Kozyklen können im allgemeinen zu unterschiedlichen getwisteten Operationen führen.

Sei zum Beispiel

$$G = \mathrm{Gal}(K/k),\ A = X = GL(n, K),$$

wobei A auf sich selbst durch Konjugation operiere. Beim Twisten der gewöhnlichen Operation von G auf GL(n, K) durch den trivialen Kozyklus

$$G \longrightarrow A,,\ \sigma \mapsto 1,$$

bleibt die Operation unverändert. Twistet man dagegen mit einem Kozyklus

$$G \longrightarrow A,\ \sigma \mapsto a_\sigma,$$

mit $a_\sigma \notin Z(A)$ für ein σ, so gilt

$$a_\sigma^{-1}\sigma(x)a_\sigma \neq \sigma(x)$$

für ein $x \in X = GL(n, K)$, d.h. die getwistete Operation ist von ursprünglichen verschieden.[47] Nach 2.3.8 sind aber je zwei 1-Kozyklen $G \longrightarrow GL(n, K)$ kohomolog.

2.3.12 Beweis-Idee

Zur Konstruktion der Umkehrabbildung

$$H^1(\mathrm{Gal}(K/k), \mathrm{Aut}_K(\Phi)) \longrightarrow TF_K(V_K, \Phi_K)$$

wollen wir die obige Konstruktion im Fall

$$G = \mathrm{Gal}(K/k),\ A = \mathrm{Aut}_K(\Phi),\ X = V_K$$

verwenden. Zu jedem 1-Kozyklus a, der ein Element der Kohomologie-Menge links repräsentiert, betrachten wir die getwistete Operation von G auf V_K. Als wichtigster Punkt im nachfolgenden Beweis wird sich herausstellen, daß der Raum

$$({}_aV_K)^G$$

der Vektoren von V_K, die unter der getwisteten Operation von G invariant sind, eine getwistete Form von (V, Φ), also ein Element der Menge rechts ist.

Wir werden dies zunächst für den Fall, daß Φ trivial ist, beweisen, d.h. wir beweisen zunächst Hilberts Satz 90. Die zu beweisende Aussage läuft darauf hinaus folgendes zu zeigen.

2.3.13 Lemma von Speiser

Seien K/k eine endliche Galois-Erweiterung mit der Galois-Gruppe G und V ein K-Vektorraum mit einer semi-linearen Operation

$$G \times V \longrightarrow V,\ (\sigma, v) \mapsto \sigma v,$$

d.h. einer Operation mit

$$\sigma(cv) = \sigma(c)\sigma(v) \text{ für } \sigma \in G,\ v \in V,\ c \in K.$$

Dann ist die natürliche Abbildung

$$\lambda\colon V^G \otimes_k K \longrightarrow V,\ v \otimes c \mapsto cv,$$

ein Isomorphismus. Dabei bezeichne

$$V^G := \{v \in V \mid \sigma v = v \text{ für } \sigma \in G\}$$

---

[47] A soll nach Voraussetzung auf X durch Konjugation operieren.

den Raum der G-invarianten Vektoren von V.

Vorbemerkung
Bevor wir mit dem Beweis beginnen erinnern wir an eine einfache Konsequenz der Galois-Theorie. Sei

$$K/k$$

eine endliche Galois-Erweiterung, und betrachten wir zwei Kopien von K, die mit zwei verschiedenen Operationen von

$$G := Gal(K/k)$$

versehen sind. Mit K wollen wir den Körper K mit der gewöhnlichen Operation der Galoisgruppe G bezeichnen, und mit K' denselben Körper mit der trivialen Operation von G. Das Tensorprodukt der beiden Kopien,

$$K\otimes_k K'$$

versehen wir mit der Diagonal-Operation, d.h.

$$\sigma(a\otimes b) := \sigma(a)\otimes\sigma(b) = a\otimes\sigma(b) \text{ für } \sigma\in G,\ a \in K,\ b\in K'.$$

Dann zerfällt das Tensorprodukt wie folgt in eine direkte Summe.

$$K\otimes_k K \cong \oplus_{\sigma\in G} Ke_\sigma,$$

wobei G auf der rechten Seite durch Permutation der e_σ operiert:

$$\tau\bullet e_\sigma = e_{\tau\sigma} \text{ für } \sigma, \tau \in G.$$

Die Multiplikation des Tensorprodukts links entspricht dabei der über K bilinearen Abbildung rechts mit

$$e_\sigma \bullet e_\tau = \begin{cases} e_\sigma & \text{falls } \sigma=\tau \\ 0 & \text{sonst} \end{cases},$$

d.h. rechs wird „koordinatenweise" multipliziert und e_σ ist das Einselement des σ–ten direkten Summanden. Dem Einselement $1\otimes 1$ links entspricht gerade die Summe der e_σ rechts.

Beweis der Vorbemerkung. Wir schreiben K in der Gestalt

$$K = k[x]/(f)$$

mit einem irreduziblen normierten Polynom f. Sei $\alpha\in K$ eine Nullstelle von f. Da K/k eine Galois-Erweiterung ist, also insbesondere normal, so hat f die Gestalt

$$f(x) = \prod_{\sigma\in G} (x - \sigma(\alpha)).$$

Damit gilt

$$\begin{aligned} K\otimes_k K &\cong K[x]/(f) \\ &\cong K[x]/\Big(\prod_{\sigma\in G} (x - \sigma(\alpha))\Big) \\ &\cong^{48} \oplus_{\sigma\in G} K[x]/(x - \sigma(\alpha)). \end{aligned}$$

---

[48] Nach dem Chinesichen Restesatz: die Abbildung

$$K[x] \longrightarrow \oplus_{\sigma\in G} K[x]/(x - \sigma(\alpha)),\ p \mapsto (f \bmod x - \sigma(\alpha))_{\sigma\in G}$$

ist ein Homomorphismen von von Ringen mit 1 (bezüglich der oben beschriebenen „koordinatenweisen" Multiplikation rechts) und hat den Kern $f = \prod_{\sigma\in G} (x - \sigma(\alpha))$, induziert also eine injektive Abbildung

Dies ist gerade die geforderte Zerlegung. Man beachte, die natürliche Fortsetzung der Galois-Gruppen-Operation von G auf K[x][49] permutiert die Faktoren $x - \sigma(\alpha)$ von f. Dies führt zu einer Permutation der direkten Summanden der letzten direkten Summe.
QED.

Beweis des Lemmas von Speiser: siehe Anhang A1.12
QED.

2.3.14 Beweis des Satzes von 2.3.7

Wir konstruieren die Umkehrung der in 2.3.7 beschriebenen Abbildung

(1) $$TF_K(V_K, \Phi_K) \longrightarrow H^1(G, Aut_K(\Phi)), (W, \Psi) \mapsto [a_\sigma].$$

mit

$$G := Gal(K/k).$$

Diese hat die Gestalt

(2) $$H^1(G, Aut_K(\Phi)) \longrightarrow TF_K(V_K, \Phi_K), \quad [a_\sigma] \mapsto (W(a), \Psi(a)).$$

mit

$$W(a) := ({}_aV_K)^G.$$

Dabei bezeichne ${}_aV_K$ wie oben den K-Vektorraum $V_K := V \otimes_k K$ mit der G-Operation, die durch Twisten der gewöhnlichen G-Operation von V_K mit dem 1-Kozyklus

$$a = \{a_\sigma\}$$

entsteht (vgl. 2.3.10). Zur Beschreibung des Tensors $\Psi(a)$ siehe unten.

Wir haben zu zeigen,

1. Die Abbildung (2) ist wohldefiniert.
2. Die Abbildung (2) ist invers zu (1).

Konstruktion des Tensors $\Psi = \Psi(a)$.
Nach Voraussetzung ist Φ ein Tensor über k, d.h. die Koordinaten von Φ bezüglich einer k-Vektorraumbasis von V liegen in k, bleiben also unverändert bei $\sigma \in G$. Es gilt also

$$\sigma(\Phi_K) = \Phi_K \text{ für jedes } \sigma \in G.$$

Weil $a = \{a_\sigma\}$ ein Kozyklus mit Werten in $Aut_K(\Phi)$ ist, sind die a_σ Automorphismen von V_K, bei denen Φ_K fest bleibt, d.h.

$$a_\sigma(\Phi_K) = \Phi_K \text{ für jedes } \sigma \in G.$$

Zusammen erhalten wir

$$a_\sigma\sigma(\Phi_K) = \Phi_K \text{ für jedes } \sigma \in G.$$

Nun ist aber durch

$$G \times X \longrightarrow X, (\sigma, x) \mapsto a_\sigma(\sigma(x)) \quad (X := V_K),$$

gerade die mit a getwistete Operation gegeben (vgl. 2.3.10). Das bedeutet aber, die Koordinaten des Tensors Φ_K bleiben fest bei der Operation von G auf dem k-

---

$$K[x]/(f) \longrightarrow \oplus_{\sigma \in G} K[x]/(x - \sigma(\alpha)).$$

Da auf beiden Seiten endlich-dimensionale K-Vektorräume derselben Dimension deg f stehen, ist dies sogar ein Isomorphismus.

[49] durch Operation auf den Koeffizienten der Polynome.

Vektorraum ${}_aV_K$. Das bedeutet aber, Φ_K kommt von einem über k definierten Tensor auf ${}_aV_K$. Diesen Tensor bezeichnen wir mit

$$\Psi = \Psi(a).$$

Wir haben damit für jeden 1-Kozyklus ein k-Objekt

$$(W(a), \Psi(a))$$

d.h. einen k-Vektorraum mit (p,q)-Tensor konstruiert. Zeigen wir als nächstes,

$(W(a), \Psi(a))$ liegt in $TF_K(V_K, \Phi_K)$,

d.h. $(W(a), \Psi(a))$ ist ein K/k-Twist von (V, Φ). Nach dem Lemma von Speiser gilt

$$W(a)\otimes_k K \cong V_K ,$$

und nach Konstruktion geht bei diesem Isomorphismus der Tensor $\Psi(a)$ in den Tensor Φ_K über. Die k-Objekte

$$(V, \Phi) \text{ und } (W(a), \Psi(a))$$

werden also isomorph, wenn man mit K tensoriert. Mit anderen Worten, $(W(a), \Psi(a))$ ist ein K/k-Twist von (V, Φ).

Kohomologe 1-Kozyklen liefern k-isomorphe Twists.

Seien

$$a: G \longrightarrow Aut_K(\Phi),\ \sigma \mapsto a_\sigma,$$

und

$$b: G \longrightarrow Aut_K(\Phi),\ \sigma \mapsto b_\sigma,$$

kohomologe 1-Kozyklen. Nach Definitoin gibt es dann einen Automorphismus

$c \in Aut_K(\Phi)$

mit

$$a_\sigma = c^{-1}\circ b_\sigma \circ \sigma(c) \text{ für jedes } \sigma\in G.$$

Dann gilt

$$\begin{aligned}
({}_aV_K)^G &= \{v \in V_K \mid a_\sigma\sigma(v) = v \text{ für } \sigma\in G\} \\
&= \{v \in V_K \mid (c^{-1}\circ b_\sigma\circ\sigma(c))(\sigma(v)) = v \text{ für } \sigma\in G\} \\
&= \{v \in V_K \mid (b_\sigma\circ\sigma(c))\,(\sigma(v)) = c(v) \text{ für } \sigma\in G\} \\
&=^{50} \{v \in V_K \mid (b_\sigma\circ\sigma)\,(c(v)) = c(v) \text{ für } \sigma\in G\} \\
&= c^{-1}(\{v \in V_K \mid (b_\sigma\circ\sigma)\,(v) = v \text{ für } \sigma\in G\}) \\
&= c^{-1}(({}_bV_K)^G).
\end{aligned}$$

Mit anderen Worten, $({}_aV_K)^G$ und $({}_bV_K)^G$ sind isomorph über k.

Damit ist die Abbildung (2) vollständig konstruiert, d.h. Aussage 1 ist bewiesen.

Zum Beweis von Aussge 2.

Wir beschränken uns auf die Aussage, daß die Komposition

$$(1)\circ(2)$$

die identische Abbildung ist. Sei also $a = \{a_\sigma\}$ ein vorgegebener 1-Kozyklus. Wir betrachten den Isomorphismus

---

[50] $\sigma(c)$ entsteht aus c durch "Konjugation" mit σ.

$$W(a)\otimes_k K \xrightarrow{g} V_K\,,\ w\otimes c \mapsto c\bullet w,$$

(des Lemmas von Speiser). Dieser Isomorphismus ist G-äquivariant, d.h. die mit a getwistete Operation rechts entspricht der natürlichen Operation links: für jedes $\sigma\in G$ ist das folgenden Diagramm kommutativ.

$$\begin{array}{ccc} W(a)\otimes_k K & \xrightarrow{g} & V_K \\ {\scriptstyle 1\otimes\sigma}\downarrow & & \downarrow{\scriptstyle a_\sigma\circ\sigma} \\ W(a)\otimes_k K & \xrightarrow{g} & V_K \end{array}$$

Mit $f = g^{-1}$ erhalten wir

$$\begin{aligned} a_\sigma\circ\sigma &= g\circ(1\otimes\sigma)\circ g^{-1} \\ a_\sigma &= f^{-1}\circ(1\otimes\sigma)\circ f\circ\sigma^{-1} \\ &= f^{-1}\circ\sigma(f). \end{aligned}$$

Nach 2.3.5 ist $a = \{a_\sigma\}$ gerade der zum K/k-Twist (W(a), Ψ(a)) gehörige 1-Kozyklus.

2.3.15 Bemerkung zum Fall von beliebig vielen Tensoren

Für die oben beschriebenen Konstruktionen gibt es ein offensichtliche Verallgemeinerung. Anstelle eines einzelnen Tensors Φ kann man auch eine ganze Familie von Tensoren betrachten. Die zugehörigen Automorphismen sind dann diejenigen, die alle diese Tensoren in sich abbilden. Getwistete Formen sind dann Vektorräume W, die isomorph sind zu V über K, wobei die Tensorenfamilie von W_K gerade der Tensorenfamlie von V_K entspricht. Der Abstiegssatz in diesem Kontext wird in derselben Weise wie der Satz 2.3.3 bewiesen.

2.4 Die Brauer-Gruppe

Wir kommen nun zur Klassifikation der zentralen einfachen Algebren. Wir wiederholen zunächst einen wohlbekannten Fakt aus der Theorie der Matrizenringe.

2.4.1 Die K-lineaeren Automorphismen der vollen Matrizenringe

Sei K ein Körper. Dann ist jeder K-lineare Automorphismus des Matrizenrings $M_n(K)$ ein innerer Automorphismus, d.h. von der Gestalt

$$M_n(K) \longrightarrow M_n(K),\ X \mapsto C^{-1}XC,$$

mit einer umkehrbaren Matrix $C \in GL(n, K)$.

Beweis. Seien $A = M_n(K)$ und

$$\lambda\colon A \longrightarrow A$$

ein K-linearer Automorphismus von A. Wir haben zu zeigen, λ ist ein innerer Automorphismus.

Der Automorphismus λ bildet das minimale Linksideal

$$L = A\bullet E_{11}$$

in ein minimales Linksideal von A ab (vgl. 2.1.4), sagen wir in

$$\lambda(L) = A\bullet M$$

mit einer Matrix M, deren erste Zeile ungleich Null und deren übrige Zeilen Null sind.

Die erste Zeile von M läßt sich als Produkt der ersten Zeile von E_{11} mit einer umkehrbaren Matrix $N \in GL(n, K)$ schreiben. Es gilt dann sogar

$$M = E_{11} \bullet N.$$

Betrachten wir den inneren Automorphismus

$$\sigma = \sigma_{N^{-1}} : A \longrightarrow A,\ X \longrightarrow N \bullet X \bullet N^{-1}$$

Es gilt $\sigma(A \bullet M) = \sigma(A) \bullet \sigma(M) = A \bullet N \bullet M \bullet N^{-1} = A \bullet N \bullet E_{11} = A \bullet E_{11}$, also

$$(\sigma \circ \lambda)(L) = L.$$

Da beim Zusammensetzen und Invertieren von inneren Automorphismen wieder innere Automorphismen entstehen, können wir λ durch $\sigma \circ \lambda$ ersetzen und annehmen,

$$\lambda(L) = L.$$

Betrachten wir die K-lineare Abbildung

$$\varphi: L = A \bullet E_{11} \longrightarrow K^n,\ (x,0,...,0) \mapsto x.$$

Man beachte, die Matrizen von L haben nur in der ersten Spalte von Null verschiedene Einträge, und diese können beliebig sein.

Die Abbildung φ ist ein K-linearer Isomorphismus mit $\varphi(E_{i1}) = e_i$ für jedes i.

Indem wir L vermittels der Abbildung φ mit K^n identifizieren, wird die durch λ auf L induzierte K-lineare Abbildung zu einer linearen Abbildung $K^n \longrightarrow K^n$ und ist so durch die Multiplikation mit einer Matrix $C^{-1} \in GL(n, K)$ gegeben. Mit anderen Worten, die Einschränkung von λ auf L hat die Gestalt

$$X \bullet E_{i1} \mapsto X e_i \mapsto C^{-1} X \bullet e_i \mapsto C^{-1} X \bullet E_{i1},$$

d.h. λ ist auf L gerade die Multiplikation mit C^{-1}. Wir erhalten

$$\lambda(X \bullet E_{i1}) = C^{-1} X \bullet E_{i1} = C^{-1} X \bullet C \bullet C^{-1} \bullet E_{i1} = C^{-1} X \bullet C \bullet \lambda(E_{i1}),$$

d.h.

$$\lambda(X) \bullet \lambda(E_{i1}) = C^{-1} X \bullet C \bullet \lambda(E_{i1}) \text{ für jedes } X \in A.$$

Nun bilden die E_{i1} eine K-Vektorraumbasis von L. Dasselbe gilt also auch für die Bildvektoren $\lambda(E_{i1}) \in L$. Also gilt

$$\lambda(X) \bullet Y = C^{-1} X \bullet C \bullet Y \text{ für jedes } X \in A \text{ und jedes } Y \in L.$$

Insbesondere gilt

$$\lambda(X) \bullet E_{i1} = C^{-1} X \bullet C \bullet E_{i1} \text{ für jedes } X \in A \text{ und jedes } i \in \{1,...,n\},$$

also

$$\lambda(X) \bullet e_i = C^{-1} X \bullet C \bullet e_i \text{ für jedes } X \in A \text{ und jedes } i \in \{1,...,n\},$$

Mit anderen Worten, die Matrizen $\lambda(X)$ und $C^{-1} X \bullet C$ haben für jedes i dieselbe i-te Spalte.
QED.

2.4.2 Die Automorphismengruppe des vollen Matrizenrings $M_n(K)$

Für jeden Körper K ist die Gruppe der K-linearen Automorphismen des vollen Matrizenrings $M_n(K)$ isomorph zur allgemeinen projektiven linearen Gruppe

$$PGL(n, K) := GL(n, K)/K^*.$$

Beweis. Betrachten wir den natürlichen Homomorphismus

$$GL(n, K) \longrightarrow Aut_K(M_n(K)), X \mapsto \sigma_X,$$

welche die Matrix X auf die Konjugation mit X abbildet. Nach 2.4.1 ist dieser surjektiv. Der Kern ist gerade das Zentrum von GL(n, K), besteht also aus den Skalarmatrizen

$$\{c \bullet Id \mid c \in K^*\} \cong K^*.$$

QED.

2.4.3 Bezeichnung: $CSA_K(n)$

Seien K/k eine endliche Galoiserweiterung und n eine natürliche Zahl. Wir bezeichnen mit

$$CSA_K(n)$$

die Menge der k-Isomorphieklassen aller zentralen einfachen k-Algebren des Grades n, welche über K zerfallen. Wir betrachten diese Menge als punktierte Menge, deren Basispunkt repräsentiert wird von der Algebra $M_n(k)$.

2.4.4 Klassifikation der zentralen einfachen Algebren des Grades n

Für jede endliche Galoiserweiterung K/k und jede natürliche Zahl gibt es einen Isomorphismus punktierter Mengen

$$CSA_K(n) \longrightarrow H^1(Gal(K/k), PGL(n, K)).$$

Beweis. Nach Folgerung 2.2.7 ist eine k-Algebra der Dimension n^2 genau dann zentral und einfach, wenn $A \otimes_k K$ zerfällt für eine endliche Galois-Erweiterung K/k. Wir können deshalb die zentralen einfachen k-Algebren des Grades n mit den getwisteten Formen von $M_n(k)$ identifizieren.

Genauer, eine k-Algebra der Dimension n^2 ist ein k-Vektorraum der Dimension n^2 mit einem (1,2)-Tensor[51], wobei der Tensor so beschaffen ist, daß das Assoziativgesetz gilt (vgl. 2.3.2). Für die Twists A von $M_n(k)$ gilt aber

$$A \hookrightarrow A \otimes_k K \cong M_n(K)$$

für K hinreichend groß, d.h. die durch den Tensor definierte Multiplikation ist automatisch assoziativ.Wir können also den Abstiegssatz 2.3.7 anwenden und erhalten einen Isomorphismus punktierter Mengen

$$CSA_K(n) \longrightarrow H^1(Gal(K/k), Aut_K(M_n(K)).$$

Nach 2.4.2 ist $Aut_K(M_n(K))$ isomorph zu PGL(n, K).

QED.

Bemerkung

Unser nächstes Ziel ist es, die zentralen einfachen k-Algebren aller Grade n gleichzeitig zu betrachten (welche über K zerfallen). Es wird sich herausstellen, daß man diese ebenfalls mit einer Kohomologiemenge identifizieren kann. Wir werden sehen, das Tensorprodukt von Algebren definiert auf dieser Menge eine kommutative und assoziative Operation.

2.4.5 Das Tensorprodukt zentraler einfacher Algebren

Sind A und B zentrale einfache k-Algebren, so gilt dasselbe auch für $A \otimes_k B$.

Beweis. Es reicht zu zeigen, für eine endliche Körpererweiterung K/k ist

$$A \otimes_k B \otimes_k K$$

---

[51] der die Multiplikation der Algebra beschreibt

isomorph zu einer vollen Matrizen-Algebra (nach 2.2.1). Wegen

$$A\otimes_k B\otimes_k K \cong (A\otimes_k K)\otimes_K(B\otimes_k K)$$

und weil $A\otimes_k K$ und $B\otimes_k K$ für K/k groß genug volle Matrizen-Algebren über K sind, ist dies aber eine Konsequenz des Isomorphismus

$$M_n(K)\otimes_K M_m(K) \cong M_{nm}(K).$$

von 1.5.2.
QED.

2.4.6 Das Tensorprodukt als Operation auf der Kohomologie

Sei K/k eine endliche Galois-Erweiterung mit der Gruppe G.

Nach 2.4.5 definiert das Tensorprodukt von k-Algebren eine Abbildung

$$CSA_K(n) \times CSA_K(m) \longrightarrow CSA_K(mn),\ (A, B) \mapsto A\otimes_k B.$$

Die Bijektion des Klassifikationssatzes 2.4.4 liefert damit eine Abbildung auf den Kohomologie-Mengen:

(1) $$H^1(G, PGL(n, K)) \times H^1(G, PGL(m, K)) \longrightarrow H^1(G, PGL(mn, K)).$$

Diese Abbildung läßt sich wie folgt beschreiben.

Aus der Abbildung

(2) $$End_K(K^n) \otimes_K End_K(K^n) \longrightarrow End_K(K^n\otimes_K K^m),\ (\phi, \psi) \mapsto \phi\otimes\psi,$$

erhält man durch Einschränken eine Abbildung

$$GL(n, K) \times GL(m, K) \longrightarrow GL(nm, K),$$

welche eine Abbildung

$$\psi: PGL(n, K) \times PGL(m, K) \longrightarrow PGL(nm, K)$$

induziert. Diese wiederum induziert die obige Abbildung auf den Kohomologien. Genauer, Abbildung (1) hat die Gestalt

$$([a_\sigma],[b_\sigma]) \mapsto [\psi\circ(a_\alpha \times b_\sigma)]$$

Beweis. Seien

$$A \text{ und } B$$

zwei einfache zentrale k-Algebren der Dimensionen n bzw. m, welche über K zerfallen und

$$f: M_n(K) \longrightarrow A\otimes_k K \text{ und } g: M_m(K) \longrightarrow B\otimes_k K$$

entsprechende Isomorphismen. Betrachten wir das folgende kommutative Diagramm von Isomorphismen.

$$\begin{array}{ccc} M_n(K)\otimes_K M_m(K) & \xrightarrow{f\otimes g} & (A\otimes_k K)\otimes_K(B\otimes_k K) \\ \xi\downarrow\cong & & \cong\uparrow\eta \\ M_{nm}(K) & & (A\otimes_k B)\otimes_k K \end{array}$$

Dabei sei

$$\eta(a\otimes b\otimes c) = (a\otimes 1)\otimes(b\otimes c)$$

und ξ sei die bezüglick der Standardeinheitsbasis aufgeschriebene Abbildung (1).
Als zu A, B und $A\otimes_k B$ gehörige 1-Kozyklen kann man dann die folgenden verwenden:

$$a(A)_\sigma := f^{-1}\circ\sigma(f)$$

$$a(B)_\sigma := g^{-1}\circ\sigma(g)$$

$$a(A\otimes B)_\sigma := (\eta^{-1}\circ f\otimes g\circ\xi^{-1})^{-1}\circ\sigma(\eta^{-1}\circ f\otimes g\circ\xi^{-1})$$

$$= \xi\circ f^{-1}\otimes g^{-1}\circ\eta\circ\sigma(\eta)^{-1}\circ\sigma(f)\otimes\sigma(g)\circ\sigma(\xi)^{-1}$$

Nun kommutiert η mit der Operation von G auf K, d.h. es gilt

$$\sigma(\eta) = \eta,$$

also

$$a(A\otimes B)_\sigma = \xi\circ f^{-1}\otimes g^{-1}\circ\sigma(f)\otimes\sigma(g)\circ\sigma(\xi)^{-1}$$

$$= \xi\circ a(A)_\sigma\otimes a(B)_\sigma\circ\sigma(\xi)^{-1},$$

Mit andere Worten, der Kozyklus $a(A\otimes B)$ ist äquivalent zum Tensorprodukt der beiden Kozyklen a(A) und b(B). Das Bild zum Paar der Kohomologieklassen zu

$$a(A): G \longrightarrow M_n(K) \text{ und } a(B): G \longrightarrow M_n(K)$$

ist somit die Kohomologieklasse zu

$$G \xrightarrow{a(A)_\sigma\otimes a(B)_\sigma} M_n(K)\otimes_K M_m(K) \xrightarrow{\xi} M_{nm}(K).^{52}$$

Faßt man ξ als bilineare Abbildung $M_n(K) \times M_m(K) \longrightarrow M_{nm}(K)$ auf, so bekommt der Kozyklus die folgende Gestalt

$$G \xrightarrow{a(A)_\sigma\times a(B)_\sigma} M_n(K) \times M_m(K) \xrightarrow{\xi} M_{nm}(K).$$

Ersetzen wir in den obigen Rechnungen die vollen Matrizenalgebren durch die projektiven linearen Gruppen, so erhalten wir wie behauptet den Kozyklus

$$G \xrightarrow{a(A)_\sigma\times a(B)_\sigma} PGL(n, K) \times PGL(m, K) \xrightarrow{\psi} PGL(nm, K).$$

QED.

2.4.7 Das induktive System $H^1(G, PGL)$

Sei K/k eine endliche Galois-Erweiterung.

Für beliebige natürliche Zahlen n und m gibt es einen injektiven Gruppen-Homomorphismus

$$GL(n, K) \longrightarrow GL(mn, K),\ X \mapsto \begin{pmatrix} X & 0 & \dots & 0 \\ 0 & X & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & X \end{pmatrix}$$

welcher der Matrix X die Blockmatrix zuordnet, welche aus m Exemplaren von X auf der Hauptdiagonalen besteht und deren Blöcke außerhalb der Hauptdiagonalen sämtlich Null sind. Dieser induziert einen injektiven Gruppenhomorphismus

$$PGL(n, K) \longrightarrow PGL(mn, K),$$

auf den den zugehörigen projektiven linearen Gruppen und damit Abbildungen punktierter Mengen

$$\lambda_{nm}: H^1(G, PGL(n, K)) \longrightarrow H^1(G, PGL(mn, K)).$$

---

[52] Man beachte, ξ ist ein Isomorphismus und sorgt nur dafür, daß die Koeffizientengruppe $M_n(K)\otimes_K M_m(K)$ durch die isomorphe Gruppe $M_{nm}(K)$ ersetzt wird.

Auf Grund des Klassifikationssatze 2.4.4 entspricht dieser Abbildung eine Abbildung

$$CSA_K(n) \longrightarrow CSA_K(mn)$$

auf den k-Isomorphieklassen zentraler einfacher k-Algebren, die über K zerfallen. Diese Abbildung hat die Gestalt

$$A \mapsto A \otimes_k M_m(k).$$

Beweis. Seien A eine zentrale einfache k-Algebra und

$$f: M_n(K) \xrightarrow{\cong} A \otimes_k K$$

ein Isomorphismus. Zur Algebra A gehört dann der 1-Kozyklus

$$a_\sigma(A) = f^{-1} \circ \sigma(f): M_n(K) \longrightarrow M_n(K) \in Aut(M_n(K)) = PGL(n, K).$$

Analog hat man zur k-Algebra $B = M_m(k)$ einen Isomorphimus

$$g: M_m(K) \longrightarrow M_m(k) \otimes_k K \text{ mit } g^{-1}(\sum_i X_i \otimes c_i) = \sum_i X_i c_i$$

und damit den 1-Kozyklus[53]

$$a_\sigma(B) = g^{-1} \circ \sigma(g): M_m(K) \xrightarrow{Id} M_m(K).$$

Zur k-Algebra $A \otimes_k M_m(k)$ gehört also der 1-Kozyklus

$$a_\sigma(A) \otimes Id: M_n(K) \otimes_k M_m(k) \longrightarrow M_n(K) \otimes_k M_m(k).$$

Schreibt man $a_\sigma(A)$ als Konjugation mit einer Matrix X, so ist $a_\sigma(A) \otimes Id$ gerade die Konjugation mit der zugehörigen Blockmatrix.
QED.

2.4.8 Die Injektivität der Morphismen des induktiven Systems

Die Abbildungen λ_{nm} von 2.4.7 sind injektiv.

Beweis. Seien

$$A, A' \in CSA_K(n)$$

zentrale einfache k-Algebren, welche über K zerfallen mit

(1) $$A \otimes_k M_m(k) \cong A' \otimes_k M_m(k).$$

Wir haben zu zeigen $A \cong A'$. Nach dem Satz von Wedderburn 2.1.5 sind A und A' als einfache Algebren volle Matrizen-Algebren über gewissen Divisionsalgebren D bzw. D',

$$A \cong M_r(D) \text{ und } A' = M_s(D').$$

Dann sind aber auch

$$A \otimes_k M_m(k) \cong M_m(A) \cong M_{mr}(D)$$

und

---

[53] Es reicht zu zeigen $\sigma(g) = g$, d.h. $\sigma \circ g \circ \sigma^{-1} = g$, d.h.

$$g^{-1} = \sigma^{-1} \circ g^{-1} \circ \sigma.$$

Für $X = \sum_i X_i \otimes c_i$ mit $X_i \in M_m(k)$ und $c_i \in K$ gilt

$$\sigma^{-1} \circ g^{-1} \circ \sigma(X) = \sigma^{-1} \circ g^{-1}(\sum_i X_i \otimes \sigma(c_i)) = \sigma^{-1}(\sum_i X_i \sigma(c_i)) = \sum_i X_i \sigma^{-1}(\sigma(c_i)) = \sum_i X_i c_i = g^{-1}(X).$$

$$A' \otimes_k M_m(k) \cong M_m(A') \cong M_{ms}(D')$$

Matrizenalgebren über D bzw. D'. Auf Grund der Eindeutigkeitsaussage des Satzes von Wedderburn folgt

$$D \cong D'.$$

Wir vergleichen die Dimensionen über k der beiden Seiten von (1) und erhalten

$$r = s.$$

Dann sind aber A und A' isomorph.
QED.

2.4.9 Brauer-Äquivalenz

Sei K/k eine endliche Galois-Erweiterung. Zwei zentrale einfache k-Algebren A und A' heißten Brauer-äquivalent, wenn es natürliche Zahlen m, m' gibt mit

$$A \otimes_k M_m(k) \cong A' \otimes_k M_{m'}(k).$$

Auf diese Weise ist eine Äquivalenzrelation definiert auf der Menge

$$CSA_K := \bigcup_{n=1}^{\infty} CSA_K(n)$$

der k-Isomorphie-Klassen zentraler einfacher k-Algebren, die über K zerfallen. Wir bezeichnen mit

$$Br(K/k)$$

die Menge der Äquivalenzklassen und mit

$$Br(k) := \bigcup Br(K/k)$$

die Vereinigung über alle endlichen Galois-Erweiterungen K/k von k.
Bemerkungen
Die Brauer-Äquivalenz besitzt die folgenden grundlegenden Eigenschaften.

(i) Jede Brauer-Äquivalenz-Klasse enthält bis auf k-Isomorphie genau eine Divisions-Algebra.[54] Man kann auch sagen, Br(K/k) klassifiziert die Divisionsalgebren über k, welcher über K zerfallen.

(ii) Je zwei Brauer-äquivalente zentrale einfache k-Algebren A und A' derselben Dimension sind isomorph.[55]

(iii) Tensorprodukte Brauer-äquivalenter k-Algebren sind Brauer-äquivalent.[56]

2.4.10 Die Gruppenstruktur von Br(K/k) und Br(k)

Das Tensor-Produkt von k-Algebren definiert auf den Mengen Br(K/k) und Br(k) die Struktur einer abelschen Gruppen.
Beweis (nach Herstein). Die grundlegenden Eigenschaften des Tensorprodukts zeigen, daß die betrachtete Produkt-Operation kommutativ und assoziativ ist. Die Äquivalentzklasse der k-Algebra k hat die Eigenschaten eines Einselements. Wir haben noch die Existenz des inversen Elements zu beweisen.

Sei A ein zentrale einfache k-Algebra und A^{op} die zugehörige entgegengesetzte k-Algebra.[57] Es reicht zu zeigen,

---

[54] Zwei Divisionsalgebren D und D' mit $D \otimes_k M_m(k) \cong D' \otimes_k M_{m'}(k)$ sind nach dem Satz von Wedderburn 2.1.5 isomorph.

[55] Es gilt dann $A \otimes_k M_m(k) \cong A' \otimes_k M_{m'}(k)$ mit m = m'. Die Argumentation wie im Beweis von 2.4.8 zeigt dann, daß A und A' isomorph sind.

[56] wegen $M_n(k) \otimes_k M_m(k) \otimes \cong M_{mn}(k)$ nach 1.5.2.

[57] d.h. der k-Vektorraum A, wobei sich das Produkt in A^{op} vom Produkt in A nur durch die Reihenfolge der Faktoren unterscheidet.

$$A \otimes_k A^{op}$$

ist isomorph zu einer vollen Matrizen-Algebra über k, d.h. es reicht zu zeigen

$$A \otimes_k A^{op} \cong \mathrm{End}_k(A).$$

Für jedes a betrachten wir die Abbildungen

$$\lambda_a : A \longrightarrow A,\ x \mapsto ax,$$

und

$$\rho_a : A \longrightarrow A,\ x \mapsto xa.$$

Beide Abbildungen sind k-linear,

$$\lambda_a , \rho_a \in \mathrm{End}_k(A),$$

und die Mengen

$$A_r := \{\rho_a \mid a \in A\}$$

$$A_\ell := \{\lambda_a \mid a \in A\}$$

bilden Teilalgebren der Algebra $\mathrm{End}_k(A)$. Außerdem ist

$$A_r \cong A \text{ und } A_\ell \cong A^{op}.$$

Es reicht also zu zeigen, die folgende k-lineare Abbildung ist ein Isomorphismus von k-Algebren.

$$\varphi : A_r \otimes_k A_\ell \longrightarrow \mathrm{End}_k(A),\ \rho_a \otimes \lambda_b \mapsto \rho_a \circ \lambda_b.$$

Diese Abbildung ist ein Homomorphismus von Ringen, weil jede Abbildung ρ_a mit jeder Abbildung λ_b kommutiert. Wir haben noch zu zeigen, sie ist bijektiv. Als k-Vektorräume haben die beiden Ringe dieselben Dimension

$$\dim_k A_r \otimes_k A_\ell = (\dim_k A)^2 = \dim_k \mathrm{End}_k(A).$$

Es reicht also zu zeigen, φ ist injektiv. Zumindest ist φ nicht identisch Null (zum Beispiel ist das Bild des Einselements $\lambda_1 \otimes \rho_1$ die identische Abbildung). Der Kern von φ ist somit ein echtes Ideal. Nun ist die k-Algebra $A_r \otimes_k A_\ell$ als Tensorprodukt zentraler einfacher k-Algebren aber einfach (nach 2.4.5). Der Kern von φ ist somit das Nullideal, d.h. φ ist injektiv.
QED.

2.4.11 Definition: relative und absolute Brauergruppe

Sei K/k eine endliche Galois-Erweiterung. Die abelschen Gruppen Br(K/k) und Br(k) mit der durch das Tensorprodukt über k definierten Multiplikation heißen (relative) Brauergruppe von K/k bzw. (absolute) Brauergruppe von k.

2.4.12 Die Gruppen $H^1(G, PGL_\infty)$ und $H^1(k, PGL_\infty)$

Sei K/k eine endliche Galois-Erweiterung mit der Gruppe G. Wir verwenden die Injektion

$$\lambda_{nm} : H^1(G, PGL(n, K)) \hookrightarrow H^1(G, PGL(mn, K)),\ A \mapsto A \otimes_k M_m(k),$$

von 2.4.7 (vgl. 2.4.8) um die Kohomologie-Menge links mit einer Teilmenge der Kohomologie-Menge rechts zu identifizieren und setzen

$$H^1(G, PGL_\infty(K)) := \bigcup_{n=1}^{\infty} H^1(G, PGL(n, K)).$$

Da die λ_{nm} mit der Bildung von Tensorprodukten über k verträglich sind, besitzt diese Menge die Struktur einer abelschen Gruppe.

Sei

$$k \subseteq K \subseteq L$$

ein Körperturm mit L/k und K/k endlich und Galoisch. Die Einschränkungsabbildung

$$\varphi: Gal(L/k) \longrightarrow Gal(K/k),\ \sigma \mapsto \sigma|_K ,$$

ist dann ein surjektiver Gruppen-Homomorphismus und definiert zusammen mit der natürlichen Inklusion

$$PGL(n, K) \hookrightarrow PGL(n, L)$$

eine injektive[58] Abbildung

$$H^1(Gal(K/k), PGL(n, K)) \hookrightarrow H^1(Gal(L/k), PGL(n, L)),\ [a_\sigma] \mapsto [a_\sigma \circ \varphi].$$

Wir gehen zur Vereinigung über alle n über und erhalten eine Inklusion

$$\iota_{LK}: H^1(Gal(K/k), PGL_\infty(K)) \longrightarrow H^1(Gal(L/k), PGL_\infty(L)),$$

Wir fixieren eine separable Abschließung von k_s von k und definieren

$$H^1(k, PGL_\infty) := \bigcup_{K \subseteq k_s} H^1(Gal(K/k), PGL_\infty(K))$$

als Vereinigung über alle endlichen Galois-Erweiterungen K/k, die in k_s enthalten sind.

Nach Konstruktion gilt die folgende Aussage.

2.4.13 Vergleich mit den Brauer-Gruppen

Die Mengen $H^1(G, PGL_\infty)$ und $H^1(k, PGL_\infty)$ sind abelsche Gruppen, deren Multiplikation vom Tensorprodukt zentraler einfacher k-Algebren über k kommt. Es bestehen die folgenden Gruppen-Isomorphismen.

$$Br(K/k) \cong H^1(Gal(K/k), PGL_\infty(K))$$

für jede endliche Galois-Erweiterung K/k.

$$Br(k) \cong H^1(k, PGL_\infty)$$

für jeden Körper.

Bemerkugen

---

[58] Der direkte Beweis der Injektivität ist einfach, wenn rechts anstelle der Grundkörper L der Gruppe PGL(n, L) durch K ersetzt wird:

Für zwei Kozyklen $\{a_\sigma\}$ und $\{b_\sigma\}$ von Gal(K/k), deren Verpflanzungen entlang φ kohomolog sind, gilt

$$a_{\varphi(\sigma)} = c^{-1} \circ b_{\varphi(\sigma)} \circ \sigma(c) \text{ für alle } \sigma \in Gal(L/k)$$

mit einem Automorphismus c von PGL(n, K). Weil φ surjektiv ist, sind die Kozyklen selbst schon kohomolog. Die Injektivität der Abbildung ergibt sich dann aus der Identifikation mit der natürlichen Einbettung

$$CSA_K(n) \hookrightarrow CSA_L(n)$$

der k-Isomorphie-Klassen der k-Algebren, die über K zerfallen, in die k-Isomorphie-Klassen der k-Algebren, die über L zerfallen.

Im Fall des Grundkörpers L hätte man nur einen Automorphismus c von PGL(n, L) und die Argumentation funktioniert nicht.

Die Gruppen $H^1(Gal(K/k), PGL_\infty(K))$ sind im bisher definierten Sinne keine Kohomologie-Gruppen, können jedoch als Kohomologie-Gruppen mit Koeffizienten im direkten Limes der Gruppen PGL(n, K) bezüglich der Einbettungen λ_{mn} angesehen werden. Diese Koeffizientengruppen ist immer noch ziemlich kompliziert. Später werden wir Br(K/k) mit der zweiten Kohomologie-Gruppe von Gal(K/k) mit Werten in der multiplikativen Gruppe K* identifizieren. Diese Koeffizienten-Gruppe ist viel einfacher zu handhaben.

2.5 Abstiegskonstruktionen

Im Rest dieses Kapitels illustrieren wir, wie man den Galois-Abstieg verwenden kann zur Durchführung wichtiger Konstruktionen im Zusammenhang mit zentralen einfachen Algebren. Im vorliegenden Abschnitt verwenden wir nicht den Abstiegssatz 2.3.7 selbst, sondern die Twist-Konstruktion, die wir für dessen Beweis benutzt haben. Wir beginnen mit einer Konstruktion, die die Definition der Quaternionen-Norm verallgemeinert.

2.5.1 Konstruktion: reduzierte Normen und Spuren

Sei

$$A$$

eine zentrale einfache k-Algebra des Grades

$$\deg A = n.$$

Wir fixieren eine endliche Galois-Erweiterung

$$K/k,$$

über welcher A zerfällt und einen K-linearen Isomorphismus

$$\varphi: M_n(K) \xrightarrow{\cong} A\otimes_k K.$$

Wir beachten, dieser Isomorphismus ist im allgemeinen nicht mit der Operation der Galois-Gruppe

$$G := Gal(K/k)$$

auf den beiden Algebren links und rechts verträglich. Wir können jedoch dafür sorgen, daß φ G-äquivariant wird, indem wir die Operation auf der Matrizen-Algebra twisten mit dem durch A gegebenen 1-Kozyklus

$$G \longrightarrow PGL(n,K),\ \sigma \mapsto a_\sigma.^{59}$$

Insbesondere ist dann

$$A \cong ({}_aM_n(K))^G.$$

Wir definieren die reduzierte Norm von A als die Zusammensetzung

$$Nrd: A \hookrightarrow A\otimes_k K \xrightarrow{\varphi^{-1}} M_n(K) \xrightarrow{det} K.$$

Analog sei die reduzierte Spur von A als Zusammensetzung

$$Trd: A \hookrightarrow A\otimes_k K \xrightarrow{\varphi^{-1}} M_n(K) \xrightarrow{Tr} K.$$

definiert. Dabei bezeichne

---

[59] Nach Definition ist $a_\sigma = \varphi^{-1}\circ\sigma(\varphi) = \varphi^{-1}\circ 1\otimes\sigma\circ\varphi\circ\sigma^{-1}$, also $\varphi\circ a_\sigma\circ\sigma = 1\otimes\sigma\circ\varphi$ d.h. das Diagramm

$$\begin{array}{ccc} M_n(K) & \xrightarrow{\varphi} & A\otimes_k K \\ \downarrow a_\sigma\circ\sigma & & \downarrow 1\otimes\sigma \\ M_n(K) & \xrightarrow{\varphi} & A\otimes_k K \end{array}$$

ist kommutativ.

$$\mathrm{Tr}: M_n(K) \longrightarrow K, (c_{ij}) \mapsto \sum_{i=1}^{n} c_{ii},$$

die Spurs für n×n-Matrizen.

Bemerkungen

(i) Die Werte der reduzierten Norm und der reduzierten Spur liegen im Grundkörper, d.h. Nrd und Trd sind Abbildungen

$$\mathrm{Nrd}: A \longrightarrow k \text{ bzw. } \mathrm{Trd}: A \longrightarrow k$$

(ii) Die reduzierte Norm und die reduzierte Spur hängen nicht von der speziellen Wahl des K-linearen Isomorphismus $\varphi: M_n(K) \longrightarrow A \otimes_k K$ ab.

Beweis. Zu (i). Das Bild von A in $M_n(K)$ besteht gerade aus den invarianten Elementen

$$({}_aM_n(K))^G \subseteq M_n(K)$$

bei der mit $a = \{a_\sigma\}$ getwisteten Operation von G auf $M_n(K)$. Es reicht deshalb zu zeigen,

$$\det: {}_aM_n(K) \longrightarrow K \text{ und } \mathrm{Tr}: {}_aM_n(K) \longrightarrow K$$

sind G-äquivariante Abbildungen, denn dann liegen die Bilder von Nrd und Trd in

$$\mathrm{Im}(\mathrm{Nrd}) \subseteq K^G = k, \mathrm{Im}(\mathrm{Trd}) \subseteq K^G = k.$$

Beweisen wir die die Äquivarianz von Determinante und Spur bezüglich der getwisteten Operation auf der Matrizen-Algebra. Nach Definition ist

$$a_\sigma \in \mathrm{PGL}(n,K) \cong \mathrm{Aut}(M_n(K)),$$

und jeder Automorphismus der Matrizen-Algebra ist ein innerer Automorphismus(vgl. 2.4.2), d.h. es gibt eine (nur bis auf skalare Vielfache eindeutig bestimmte Matrix

$$a(\sigma) \in M_n(K)$$

mit

$$a_\sigma(X) = a(\sigma)^{-1} X a(\sigma) \text{ für jedes } X \in M_n(K).$$

Damit erhalten wir für das charakteristische Polynom

$$\chi_X(T) := \det(X - T \cdot \mathrm{Id})$$

der Matrix $a_\sigma(X)$:

$$\begin{aligned}
\chi_{a_\sigma(X)}(T) &= \det(a_\sigma(X) - T \cdot \mathrm{Id}) \\
&= \det(a(\sigma)^{-1} X a(\sigma) - T \cdot \mathrm{Id}) \\
&= \det(a(\sigma)^{-1}(X - T \cdot \mathrm{Id}) a(\sigma)) \\
&= \det(a(\sigma))^{-1} \cdot \det(X - T \cdot \mathrm{Id}) \cdot \det(a(\sigma)) \\
&= \det(X - T \cdot \mathrm{Id}) \\
&= \chi_X(T).
\end{aligned}$$

Mit anderen Worten, $a_\sigma(X)$ und X haben dasselbe charakteristische Polynom. Insbesondere haben sie denselben Koeffizienten vor T^{n-1} und dasselbe Absolutglied, d.h.

$$\mathrm{Tr}(a_\sigma(X)) = \mathrm{Tr}(X) \text{ und}$$
$$\det(a_\sigma(X)) = \det(X).$$

Zu (ii). Sei ein weiterer Isomorphismus

$$\psi: M_n(K) \xrightarrow{\cong} A \otimes_k K.$$

gegeben und sei $b = \{b_\sigma\}$ der zugehörige 1-Kozyklus. Dann sind die beiden 1-Kozyklen a und b kohomolog, d.h. es gibt ein Element

$$c \in PGL(n,K) = Aut(M_n(K))$$

mit

$$b_\sigma = c^{-1} \circ a_\sigma \circ \sigma(c) \text{ für jedes } \sigma \in G,$$

d.h.

$$b_\sigma =^{60} c^{-1} \circ a_\sigma \circ \sigma \circ c \circ \sigma^{-1},$$

$$c \circ b_\sigma \circ \sigma = a_\sigma \circ \sigma \circ c.$$

Wir erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} M_n(K) & \xrightarrow{c} & M_n(K) \\ \downarrow{\scriptstyle b_\sigma \circ \sigma} & & \downarrow{\scriptstyle a_\sigma \circ \sigma} \\ M_n(K) & \xrightarrow{c} & M_n(K) \end{array}$$

jedes $\sigma \in G$, d.h. der Automorphismus c ist ein äquivarianter Automorphismus

$$c: {}_bM_n(K) \longrightarrow {}_aM_n(K),$$

induziert also einen Isomorphismus

$$({}_bM_n(K))^G \xrightarrow{c} ({}_aM_n(K))^G$$

der G-invarianten Teilalgebren. Da die invarianten Teile links und rechts beide isomorph zu A sind, erhalten wir einen Automorphismus von k-Algebren

$$\alpha: A \longrightarrow A$$

und ein kommutatives Diagramm

$$\begin{array}{ccccc} A & \xrightarrow[\cong]{\varphi^{-1}} & ({}_aM_n(K))^G & & \\ \uparrow{\scriptstyle \alpha} & & \uparrow{\scriptstyle c} & \overset{\det}{\searrow} & K \\ A & \xrightarrow[\psi^{-1}]{\cong} & ({}_bM_n(K))^G & \underset{\det}{\nearrow} & \end{array}$$

Man beachte, das Dreieck rechts ist kommutativ, weil c als Automorphismus von $M_n(K)$ ein innerer Automorphismus und die Determinante invariant bei inneren Automorphismen ist. Damit gilt für jedes $a \in A$:

$$\det(\varphi^{-1}(\alpha(a))) = \det(c(\psi^{-1}(a))) = \det(\psi^{-1}(a)).$$

Es reicht also zu zeigen,

$$\det(\varphi^{-1}(\alpha(a))) = \det(\varphi^{-1}(a))$$

für jedes $a \in A$ und für jeden k-Automorphismus α Der Automorphismus α induziert einen Automorphismus $\alpha \otimes 1: A \otimes_k K \longrightarrow A \otimes_k K$ von K-Algebren und vermittels φ einen Automorphismus $d: M_n(K) \longrightarrow M_n(K)$. Wir erhalten damit ein kommutatives Diagramm

---

[60] Als "Matrix" von PGL(n,K) entsteht $\sigma(c)$ aus der "Matrix" c, indem man $\sigma \in Gal(K/k)$ auf die Koeffizienten von c anwendet. Als Automorphismus von $M_n(K)$ entsteht $\sigma(c)$ aus dem Automorphismus c, indem man ihn mit dem Automorphismus σ von $M_n(K)$ konjugiert.

$$\begin{array}{ccccc} A & \hookrightarrow & A\otimes_k K & \xrightarrow{\varphi^{-1}} & M_n(K) \\ \uparrow\alpha & & \uparrow\alpha\otimes 1 & & \uparrow d \\ A & \hookrightarrow & A\otimes_k K & \xrightarrow[\varphi^{-1}]{} & M_n(K) \end{array} \quad \begin{array}{c} \overset{\det}{\searrow} \\ K \\ \underset{\det}{\nearrow} \end{array}$$

Man beachte, das Dreieck rechts ist kommutativ, weil d als Automorphismus von $M_n(K)$ ein innerer Automorphismus ist. Damit gilt

$$\det(\varphi^{-1}(\alpha(a))) = \det(d(\varphi^{-1}(a))) = \det(\varphi^{-1}(a)).$$

Dieselben Rechnungen mit der Spur anstelle der Determinante zeigen die Unabhängigkeit der reduzierten Spur von der speziellen Wahl des Isomorphismus φ.
QED.

2.5.2 Reduzierte Norm und Umkehrbarkeit

Seien A eine zentrale einfache k-Algebra und $a \in A$ ein Element. Dann sind die folgenden Aussagen äquivalent.

(i) a ist eine Einheit von A.

(ii) $\mathrm{Nrd}(a) \neq 0$.

Insbesondere ist A genau dann eine Divisionsalgebra, wenn $0 \in A$ die einzige Nullstelle der reduzierten Norm

$$\mathrm{Nrd}: A \longrightarrow k$$

ist.

Beweis. (i) ⇒ (ii). Sei a umkehrbar. Dann gehört zu a eine umkehrbare Matrix in der Matrizen-Algebra $M_n(K)$, und deren Determinante ist von Null verschieden.

(ii) ⇒ (i). Wir identifizieren A mit der Teilmenge

$$A \subseteq M_n(K)$$

der G-invarianten Elemente bezüglich einer geeigneten Operation von G auf dem Matrizenring. Dann gilt

$$0 \neq \mathrm{Nrd}(a) = \det(a),$$

d.h. es gibt eine Matrix $b \in M_n(K)$ mit

$$a \bullet b = \mathrm{Id}.$$

Für jedes $\sigma \in G$ folgt

$$\sigma(a) \bullet \sigma(b) = \sigma(\mathrm{Id}) = \mathrm{Id}.$$

Wegen $a \in A$ ist a invariant unter σ, d.h. es gilt $a \bullet \sigma(b) = \mathrm{Id}$, d.h.

$$\sigma(b) = b.$$

Mit anderen Worten, b ist invariant bei den Elementen $\sigma \in G$, d.h.

$$b \in M_n(K)^G = A,$$

d.h, das Element a besitzt ein Inverses b in A.
QED.

Bemerkungen

(i) Wie wir wissen, sind die nicht-zerfallenden Quaternionen-Algebren als Elemente der Brauer-Gruppe von der Ordnung 2: ihre Tensor-Quadrate sind volle Matrizen-Algebren.

(ii) Wir sind jetzt in der Lage, eine neue Sorten von Divisionsalgebren explizit zu beschreiben, nämlich Divisionsalgebren, die als Elemente der Brauergruppe eine vorgegebene Ordnung besitzen.

(iii) Wie wir sehen werden, existieren solche Divisionsalgebren, falls der Grundkörper k eine Galois-Erweiterung besitzt, die eine zyklische Faktorgruppe der betrachteten Ordnung enthält.
(iv) Wir konstruieren diese Algebren zunächst in abstrakter Weise unter der Annahme der Existenz einer Galois-Erweiterung der beschriebenen Art, und gehen dann zu einer konkreten Beschreibung der Algebren über.
(v) Ohne Beschränkung der Allgemeinheit können wir annehmen, daß die Galois-Erweiterung selbst schon zyklisch ist.

2.5.3 Konstruktion: Zyklische Algebren

Seien

$$K/k$$

eine zyklische Galois-Erweiterung der Ordnung m und

$$\chi: \ G:= G(K/k) \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

ein Gruppen-Isomorphismus. Weiter sei

$$b \in k^*$$

ein Element aus der multiplikativen Gruppe des Grundkörpers k. Wir ordnen jetzt wie folgt diesen Daten eine zentrale einfach k-Algebra

$$(\chi, b)$$

zu, welche eine K/k-getwistete Form von $M_m(k)$ ist und welche die zu χ und b gehörige zyklische k-Algebra heißt.

Dazu betrachten wir die Matrix

$$\tilde{F}(b) := \begin{pmatrix} 0 & b \\ Id_{m-1} & 0 \end{pmatrix} \in GL(m, k).$$

Dabei bezeichne $Id_{m-1} \in GL(m-1,k)$ die Einheitmatrix. Weiter sei

$$F(b) := \tilde{F}(b) \bmod k^* \in PGL(n,k)$$

das natürliche Bild von $\tilde{F}$ ven linearen Gruppe. Die Muiltiplikation der Matrix $\tilde{F}(b)$ mit den Standard-Einheitsvektoren liefert

$$\tilde{F}(b)\bullet e_i = e_{i+1} \text{ für } i = 1,...,m-1$$

$$\tilde{F}(b)\bullet e_m = b\bullet e_1 .$$

Daraus liest man ab, daß $\tilde{F}(b), \tilde{F}(b)^2,...,\tilde{F}(b)^{m-1}$ keine Skalarmatrizen sind[61], und es gilt

$$\tilde{F}(b)^m = b\bullet Id_m,$$

d.h.

F(b) ist ein Element der Ordnung m von PGL(m, k).

Wir erhalten so einen injektiven Gruppen-Homomorphismus

$$\mathbb{Z}/m\mathbb{Z} \hookrightarrow PGL(m,k), \ i \bmod m \mapsto F(b)^i.$$

Zusammensetzen mit χ und der natürlichen Einbettung $PGL(m,k)\hookrightarrow PGL(m,K)$ liefert einen injektiven Gruppen-Homomorphismus

---

[61] Das Bild von e_1 ist kein Vielfaches von e_1

$$z(b): G \xrightarrow{\chi} \mathbb{Z}/m\mathbb{Z} \hookrightarrow PGL(m,k) \hookrightarrow PGL(m,K),\ g \mapsto F(b)^{\chi(g)}.$$

Weil das Bild von z(b) sogar in PGL(m,k) liegt, können wir z(b) auch als 1-Kozyklus auffassen.[62] Wir versehen $M_n(K)$ mit der durch z(b) getwisteten Operation und definieren

$$(\chi, b) := ({}_{z(b)}M_m(K))^G$$

also die Algebra der G-Invarianten bezüglich dieser Operation. Nach dem (Beweis 2.3.13 des) Abstiegssatz(es) 2.3.7 ist auf diese Weise eine zentrale einfache k-Algebra des Grades m definiert.

Wir kommen jetzt zur Beschreibung der zyklischen k-Algebren, wie sie ursprünglich von Dickson vorgeschlagen wurde.

2.5.4 Die Beschreibung der zyklischen Algebren durch Dickson

Seien K/k eine zyklische Galois-Erweiterung, $\chi: G(K/k) \longrightarrow \mathbb{Z}/m\mathbb{Z}$ ein Isomorphismus und $b \in k^*$ ein Element. Dann gibt es ein Element

$$y \in (\chi, b)$$

mit

1. $(\chi, b) = K \bullet 1 + K \bullet y + ... + K \bullet y^{m-1}$
2. $y^m = b$
3. $y\lambda = \sigma(\lambda)y$ für jedes $\lambda \in K$.

Dabei sei $\sigma \in G$ der Erzeuger von G mit $\chi(\sigma) = 1 \bmod m$.

Insbesondere ist K eine kommutative k-Teilalgebra von (χ, b), welche nicht im Zentrum liegt.

Beweis. Bezeichne A den m-dimensionalen K-Vektorraum

$$A := K \bullet 1 + K \bullet y + ... + K \bullet y^{m-1}$$

mit der durch 2. und 3. gegebenen Multiplikation[63]. Mit anderen Worten, A ist die von K und y erzeugte (assoziative aber nicht notwendig kommutative) k-Algebra mit den Relationen 2. und 3.[64]

---

[62] Für $\sigma, \tau \in G$ gilt $z(b)(\sigma\tau) = z(b)(\sigma) \bullet z(b)(\tau) = z(b)(\sigma) \bullet \sigma(z(b)(\tau))$

[63] Anstelle der y-Potenzen verwende man zunächst irgendeine Basis, sagen wir $v_0,...,v_{m-1}$, d.h.

$$A = Kv_0 + ... + Kv_{m-1}$$

Dann definieren wir die Multiplikation

$$m: A \times A \longrightarrow A$$

durch die Bedingung

$$v_i d v_j = \sigma^i(d) v_{i+j} \text{ für } d \in K.$$

Genauer, es gelte

$$m\left(\sum_{i=0}^{m-1} c_i v_i\ ,\ \sum_{j=0}^{m-1} d_j v_j\right) := \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} c_i v_i d_j v_j := \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} c_i \sigma^i(d_j) v_{i+j}$$

wobei v_{i+j} im Fall $i+j = m$ das Element $b \bullet v_{i+j-m}$ bezeichne. Es ist leicht zu sehen, diese Multiplikation ist assoziativ,

$$cv_i \bullet (dv_j \bullet ev_\ell) = cv_i \bullet (d\sigma^j(e)v_{j+\ell}) = c\sigma^i(d\sigma^j(e))v_{i+j+\ell} = c\sigma^i(d)\sigma^{i+j}(e)v_{i+j+\ell}$$

$$(cv_i \bullet dv_j) \bullet ev_\ell = (c\sigma^i(d)v_{i+j}) \bullet ev_\ell = c\sigma^i(d)\sigma^{i+j}(e)v_{i+j+\ell}$$

Weiter sei

$$j: A \longrightarrow M_m(K)$$

die Abbildung mit

$$j(\sum_{i=0}^{m-1} \lambda_i y^i) := \sum_{i=0}^{m-1} \mathrm{diag}(\sigma^{m-1}(\lambda_i),\sigma^{m-2}(\lambda_i),...,\lambda_i) \cdot \widetilde{F}(b)^i.$$

Dabei bezeichne diag(...) die Diagonalmatrix mit den angegebenen Einträgen auf der Hauptdiagonalen. Diese Abbildung ist k-linear und überführt jedes Element

$$c \in k \subseteq K \cdot 1$$

in

$$j(c) = j(c \cdot 1) = \mathrm{diag}(\sigma^{m-1}(c),\sigma^{m-2}(c),...,\sigma(c),c) \cdot \widetilde{F}(b)^0 = c \cdot Id,$$

d.h in sich selbst.

1. Schritt: j ist ein Homomorphismus von k-Algebren:

(man beachte, σ hat die Ordnung m, d.h. $\sigma^{i+j}(e) = \sigma^{i+j-m}(e)$)

Weiter hat v_0 hat die Eigenschaften des Einselements,

$$v_0 = 1,$$

und mit

$$y := v_1$$

gilt

$$y^i = v_i \text{ für } i = 1,...,m-1.$$

Weiter ist

$$y^m = b$$

und für $\lambda \in K$ gilt $y\lambda = \sigma(\lambda)y$.

[64] A läßt sich identifizieren mit dem Faktorring der von K und y erzeugten freien k-Algebra

$$k<K,y>,$$

die als k-Vektorraum von den endlichen Wörtern der Gestalt

$$a_1 b_1 \cdot ... \cdot a_\ell b_\ell$$

erzeugt wird, wobei die a_i aus K und die b_i y-Potenzen sind und $\ell = 1,2,3,...$ Dabei bestehen die folgenden Relationen

$1 \cdot b = b$ für jede y-Potenz

$a \cdot y^0 = a$ für jedes $a \in K$

$(a'+a")b = a'b + a"b$

$b(a'+a") = ba' + ba"$

$ab = ba$ für $a \in k$.

Sie ist charakterisiert durch die Universalitätseigenschaft, daß sich jeder k-Algebra-Homomorphismus

$$K \longrightarrow S$$

auf k<K,y> fortsetzen läßt, wobei die Fortsetzung durch das Bild von y eindeutig bestimmt ist und sich dieses Bild beliebig vorgeben läßt.

Diese freie k-Algebra wird faktorisiert nach dem zweiseitigen Ideal, welches erzeugt wird von $y^m - b$ und den Elementen der Gestalt

$$y\lambda - \sigma(\lambda)y \text{ mit } \lambda \in K.$$

Anders ausgedrückt, A ist bis auf Isomorphie gleich

$$k<K,y>/(y^m - b, y\lambda - \sigma(\lambda)y \mid \lambda \in K)$$

wenn K<y> den nicht-kommutativen Polynomring über K in der Unbestimmten y bezeichnet.

Wir haben zu zeigen, die definierenden Relationen 2. und 3. sich auch für das Bild

$$j(y) = \widetilde{F}(b)$$

von y erfüllt[65], d.h. es gilt

$\widetilde{2}$. $\widetilde{F}(b)^m = b$.

$\widetilde{3}$. $\widetilde{F}(b)\bullet j(\lambda) = j(\sigma(\lambda))\bullet\widetilde{F}(b)$ für $\lambda\in K$.

Die Identität $\widetilde{2}$. haben wir in 2.5.3 unmittelbar nach der Definition von $\widetilde{F}(b)$ bewiesen. Vergleichen wir die beiden Seiten von $\widetilde{3}$. Für jeden Standard-Einheitsvektor e_i mit $i < m$ gilt

$$j(\sigma(\lambda))\bullet\widetilde{F}(b)\bullet e_i = j(\sigma(\lambda))\bullet e_{i+1} = \sigma^{m-i-1}(\sigma(\lambda))e_{i+1} = \sigma^{m-i}(\lambda)e_{i+1}$$

$$=^{66} \widetilde{F}(b)\bullet\sigma^{m-i}(\lambda)e_i = \widetilde{F}(b)\bullet j(\sigma(\lambda))\bullet e_i$$

d.h. beide Seiten haben dieselbe i-te Spalte. Für i = m erhalten wir

$$j(\sigma(\lambda))\bullet\widetilde{F}(b)\bullet e_m = j(\sigma(\lambda))\bullet be_1 = \sigma^{m-1}(\sigma(\lambda))be_1 = \sigma^m(\lambda)be_1$$

$$=^{67} b\lambda e_1 = \widetilde{F}(b)\bullet\lambda e_m = \widetilde{F}(b)\bullet j(\lambda)\bullet e_m ,$$

d.h. beide Seiten haben dieselbe m-te Spalte.

2. Schritt: Im(j) liegt in $(\chi, b) = ({}_{z(b)}M_m(K))^G$.

Die Algebra $({}_{z(b)}M_m(K))^G$ besteht aus den m×m-Matrizen, die invariant sind bei der Operation des Erzeugers σ von G, d.h. der Matrizen X mit

$$a_\sigma\circ\sigma(X) = X.$$

---

[65] Eine alternative Beschreibung von j besteht dann nämlich wie folgt. Betrachten wir die k-lineare Abbildung

$$\varphi: K \longrightarrow M_m(K),\ c \mapsto \mathrm{diag}(\sigma^{m-1}(c),\sigma^{m-2}(c),...,\sigma(c),c).$$

Diese überführt jedes Element $c\in K$ in $c\bullet Id$, d.h. in sich selbst. Weil σ ein k-Automorphismus von K ist, werden auch Produkte von Elementen $c \in K$ in die Produkte der Bilder überführt, d.h. φ ist ein Homomorphismus von k-Algebren. Dieser läßt sich auf den nicht-kommutativen Polynomring K<y> in der Unbestimmten y fortsetzen, wobei wir das Bild von y beliebig festlegen könmen. Bezeichne

$$\widetilde{\varphi}: K\langle y\rangle \longrightarrow M_m(K)$$

die Fortsetzung mit

$$\widetilde{\varphi}(y) = \widetilde{F}(b).$$

Wenn wir zeigen können, daß in $M_m(K)$ die Relationen $\widetilde{2}$ und $\widetilde{3}$ gelten, so bedeutet dies, $\widetilde{\varphi}$ überführt

$y^m - b$ und die Elemente der Gestalt $y\lambda - \sigma(\lambda)y$
in die Null, faktoriesiert sich also über

$$A \cong K\langle y\rangle/(y^m - b, y\lambda - \sigma(\lambda)y \mid \lambda\in K).$$

Der induzierte Homomorphismus von k-Algebren

$$A \longrightarrow M_m(K)$$

ist aber gerade die oben beschriebene Abbildung j.

[66] Auf beiden Seiten steht ein Vielfaches des (i+1)-ten Standard-Einheitsvektors.

[67] wegen $b \in k^*$ und $\sigma^m = e$.

Nun operiert $a_\sigma \in \mathrm{Aut}(M_m(K))$ durch Konjugation mit $\widetilde{F}(b)$ (vgl. 2.5.3), d.h.

$$({}_{z(b)}M_m(K))^G = \{X \in M_m(K) \mid \widetilde{F}(b)^{-1}\sigma(X)\widetilde{F}(b) = X\}$$

$$= \{X \in M_m(K) \mid \sigma(X)\widetilde{F}(b) = \widetilde{F}(b)\bullet X\}$$

In der Menge rechts liegt trivialerweise $j(y) = \widetilde{F}(b)$.[68] Wegen der Identität $\widetilde{3}$ des ersten Schritts liegen auch die Matrizen $j(\lambda)$ mit $\lambda \in K$ in dieser Menge. Weil A von y und K erzeugt wird, liegt damit aber das gesamte Bild j(A) in der Invarianten-Algebra.

3. Schritt: j ist ein Isomorphismus $A \longrightarrow (\chi, b)$.

Wir wissen bereits, j ist ein Homomorphismus von k-Algebren. Wir haben noch die Bijektivität von j zu beweisen. Die Algebra rechts hat die Dimension m^2, die links hat dieselbe Dimension

$$\dim_k A = m\bullet\dim_k K = m\bullet \#\,\mathrm{Gal}(K/k) = m^2.$$

Es reicht also zu zeigen, j ist surjektiv. Dazu reicht es zu zeigen,

$$j\otimes_k K\colon A\otimes_k K \longrightarrow (\chi, b)\otimes_k K =^{[69]} M_m(K)$$

ist surjektiv. Dies ist ein Homomorphismus von K-Algebren[70], desen Bild die Matrizen der Gestalt

(1) $$j(c) = \mathrm{diag}(\sigma^{m-1}(c),\sigma^{m-2}(c),\ldots,\sigma(c),c) \text{ mit } c \in K$$

und die Matrix

(2) $$j(y) = \widetilde{F}(b)$$

enthält. Die Matrizen (1) liegen alle in der Teilalgebra $D_n(K) \subseteq M_n(K)$ der Diagonalmatrizen. Wir identifizieren diese Teilalgebra vorübergehend mit dem K^n, und zwar derart, daß die Einschränkung von j auf K die Gestalt

$$j'\colon K \longrightarrow D_n(K) = K^n,\ c \mapsto (c, \sigma(c), \ldots, \sigma^{m-1}(c)),$$

hat. Das Bild dieser Abbildung liegt in keinem echten linearen Unterraum des K^m, denn andernfalls läge es ganz in einer Hyperebene, d.h. es gäbe $c_i \in K$, die nicht sämtlich gleich Null sind mit

$$\sum_{i=0}^{m-1} c_i\bullet\sigma^{m-1}(c) = 0 \text{ für alle } c \in K.$$

Mit anderen Worten, die Charaktere $\sigma^0, \sigma, \ldots, \sigma^{m-1}\colon K^* \longrightarrow K^*$ wären K-linear abhängig, im Widerspruch zum Satz von Artin. Wir haben gezeigt, die Matrizen der Gestalt (1) erzeugen über K den Raum der Diagonalmatrizen $D_n(K)$, d.h.

$$D_n(K) \subseteq \mathrm{Im}(j\otimes K).$$

Insbesondere liegen die Elementarmatrizen

$$E_{ii} \in \mathrm{Im}(j\otimes K) \text{ für } i = 1, \ldots, m$$

im Bild von $j\otimes K$. Wegen[71]

---

[68] Man beachte, wegen $b \in k^*$ gilt $\sigma(\widetilde{F}(b)) = \widetilde{F}(b)$.

[69] Nach Definition von (χ, b) zerfällt die Algebra über k.

[70] Weil j ein Homomorphismus von k-Algebren ist.

[71] Es gilt

$$E_{uv} = \widetilde{F}(b)^{u-v}E_{vv} \text{ für } v < u$$

und

$$E_{uv} = b^{-1}\widetilde{F}(b)^{u+m-v}E_{vv} \text{ für } u < v$$

liegen sämliche Matrizen der Gestalt E_{uv} im Bild von $j\otimes K$. Da dieses Bild ein K-Vektorraum ist, folgt

$$\mathrm{Im}(j\otimes K) = M_m(K).$$

QED.

Bemerkung

Wir behandeln jetzt einem Spezialfall der eine etwas schönere Beschreibung der Algebra (χ, b) erlaubt.

2.5.5 Die Algebren der Gestalt $(a, b)_\omega$ und [a, b)

Seien K/k eine zyklische Galois-Erweiterung, $\chi: G(K/k) \longrightarrow \mathbb{Z}/m\mathbb{Z}$ ein Isomorphismus und $b \in k^*$ ein Element.

1. Fall

Weiter sei m teilfremd zur Charakteristik von k und k enthalte eine primitive m-te Einheitswurzel

$$\omega \in k.$$

Für $a,b \in k^*$ bezeichne

$$(a, b)_\omega$$

die k-Algebra mit den zwei Erzeugern x, y und den Relationen

$$x^m = a,\ y^m = b,\ yx = \omega xy,$$

d.h.[72]

$$(a, b)_\omega = \langle x, y \mid x^m = a,\ y^m = b,\ yx = \omega xy \rangle.$$

2.Fall

Seien k ein Körper der Charakteristik $p > 0$ und $m = p$. Für $a, b \in k^*$ bezeichne

$$[a,b)$$

die k-Algebra mit den zwei Erzeugern x, y und den Relationen

$$x^p = x - a,\ y^p = b,\ yx = (x+1)y,$$

d.h.

$$[a, b) = \langle x, y \mid x^p = x - a,\ y^p = b,\ yx = (x+1)y \rangle.$$

$$\widetilde{F}(b)e_i = e_{i+1} \text{ für } i \neq m$$

und

$$\widetilde{F}(b)e_m = be_1$$

[72] d.h.

$$(a, b)_\omega = k\langle x,y\rangle/I$$

Dabei sei $k\langle x,y\rangle$ die nicht-kommutative Polynom-Algebra über k in x und y (wobei x und y mit den Elementen von k kommutieren sollen). Als k-Vektorraum besitzt $k\langle x,y\rangle$ als Basis die Menge aller endlichen Wörter in x und y. Die Multiplikation kommt vom Zusammensetzen der Wörter. Das Ideal I wird erzeugt von

$$x^m - a,\ y^m - b,\ yx - \omega xy.$$

Bemerkungen
(i) Ist im ersten Fall m = 2 (also $\omega = -1$), so sind die Algebren $(a, b)_\omega$ gerade die Quaternionen-Algebren von Kapitel 1.
(ii) Im zweiten Fall definiert die Gleichung

$$x^p = x - a$$

eine zyklischen Galoiserweiterung des Grades p, deren Galoisgruppe aus den Abbildungen

$$\alpha \mapsto \alpha + i \text{ mit } i = 0, 1, \ldots, p-1$$

(α eine fest gewählte Nullstelle von $x^p - x + a$) besteht.

2.5.6 Folgerung

(i) Seien k ein Körper, der eine primitive m-te Einheitswurzel ω enthält (mit m teilerfremd zur Charakteristik von k),

$$K = k(\sqrt[m]{a}) \text{ mit } a \in k^*$$

eine zyklische Galoiserweiterung des Grades m und

$$\chi: \mathrm{Gal}(K/k) \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

der Isomorphismus, der den Automorphismus[73]

$$\sigma: K \longrightarrow K, \sqrt[m]{a} \mapsto \omega \cdot \sqrt[m]{a},$$

in die Restklasse von 1 abbildet. Dann besteht für beliebige $b \in k^*$ eine Isomorphie von k-Algebren

$$(a, b)_\omega \cong (\chi, b).$$

(ii) Seien k ein Körper der Charakteristik $p > 0$ und

$$K/k$$

die Galoiserweiterung des Grades p zum Polynom

$$x^p - x + a$$

für ein $a \in k^*$. Weiter sei $\alpha \in K$ eine Nullstelle des Polynoms $x^p - x + a$ und

$$\chi: \mathrm{Gal}(K/k) \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

der Isomorphismus, der den Automorphismus[74]

$$\sigma: K \longrightarrow K, \alpha \mapsto \alpha+1,$$

in die Restklasse von 1 abbildet. Dann besteht für beliebige $b \in k^*$ eine Isomorphie von k-Algebren

$$[a, b) \cong (\chi, b).$$

---

[73] Jeder k-Automorphismus $K \longrightarrow K$ ist von der Gestalt

$$\sqrt[m]{a} \mapsto \omega^i \cdot \sqrt[m]{a}$$

mit i = 0, 1, 2, ... , denn die Nullstellen von $X^m - a$ müssen in Nullstellen abgebildete werden. Die Zahl der Automorphismen ist [K:k] = m, also gleich der Anzahl der verschiedenen Potenzen ω^i. Man erhält also für jedes i tatsächlich einen Automorphismus.

[74] Man beachte, mit α ist auch $\alpha+1$ eine Nullstelle von $X^p - X + a$. Also sind

$$\alpha+i$$

für i = 0,1,2,... Nullstellen dieses Polynoms. Insgesamt hat dieses Polynom höchstens p Nullstellen. Die Anzahl der verschiedenen $\alpha+i$ ist aber gleich i, d.h. man erhält so sämtliche Nullstellen und deren Anzahl ist p.

Insbesondere sind $(a,b)_\omega$ und [a, b) zentrale einfache k-Algebren, die über K zerfallen.

Beweis.
Zu (i). Man erhalt den gesuchten Isomorphismus, indem man als Erzeuger das Element

$$x = \sqrt[m]{a}$$

und das Element y von 2.5.4 wählt.
Zu (ii). Man setze

$$x = \alpha$$

und y sei wie in 2.5.4.
QED.

2.5.7 Bemerkungen

(i) Später werden wir sehen (Kummer-Theorie, Folgerung 4.3.9), daß sich bei Vorhandensein einer m-ten primitiven Einheitswurzel jede zyklischen Galois-Erweiterung des Grades m in der Gestalt

$$K = k(\sqrt[m]{a})$$

wie in der obigen Folgerung schreiben läßt.

(ii) Analog wird (Artin-Schreier-Theorie, Bemerkung 4.3.13(1)) jede Galois-Erweiterung des Grades p in der Charakteristik p > 0 von einer Nullstelle eines Polynoms der Gestalt $x^p - x + a$ erzeugt.

(iii) Im vorigen Kapitel haben wir gesehen, die Klasse einer nicht-zerfallenden Quaternionen-Algebra hat die Ordnung 2 in der Brauer-Gruppe. Allgemeiner hat die Klasser einer zyklischen Algebra $(a, b)_\omega$ die Ordnung m. Wir überlassen den Beweis dieser Tatsache dem Leser als Übung.[75] In Kapitel 4 werden wir die allgemeinere Tatsache beweisen, daß die Ordnung der Klasse einer beliebigen zentralen einfachen k-Algebra die Zahl m teilt, falls die Algebra über einer Erweiterung des Grades m zerfällt.

(iv) Sehr viel tiefliegender ist die folgende Umkehrung dieser Aussage.

2.5.7 Theorem von Merkurjev-Suslin

Sei k ein Körper, der eine primitive m-te Einheitswurzel ω enthält. Jede zentrale einfache k-Algebra, deren Klasse in der Brauer-Gruppe Br(k) die Ordnung m besitzt, ist dann Brauer-äquivalent zu einem Tensor-Produkt

$$(a_1, b_1)_\omega \otimes \ldots \otimes (a_i, b_i)_\omega$$

von zyklischen k-Algbren.

Bemerkungen

(i) Diese Aussage ist eine Verallgemeinerung des in Kapitel 1 formulierten Satzes von Merkurjev. Merkurjev und Suslin haben dieses Ergebnis kurz nach dem Ergebnis von Merkurjev. Der Beweis dieser allgemeineren Aussage wird den größten Teil dieses Buches in Anspruch nehmen.

(ii) Die nachfolgende Folgerung aus dem Satz von Merkurjev-Suslin scheint keinen elementaren Beweis zu besitzen.

---

[75] Man beachte, der 1-Kozyklus

$$G \longrightarrow \mathrm{Aut}_K M_m(K),\ \sigma \mapsto a_\sigma,$$

für den die zugehörige Operation der Galois-Gruppe auf der Matrizen-Algebra gerde $(a, b)_\omega$ als Fix-Algbra besitzt, kommt von einem Element $F(b) \in \mathrm{Aut}_K M_m(K)$, der Ordnung m. Die Tensorpotenzen dieses Automorphismus liefern gerade die Tensorpotenzen der Algebra $(a, b)_\omega$ (vgl. 2.4.6).

2.5.8 Folgerung

Seien k ein Körper, der eine primitive m-te Einheitswurzel besitzt und A eine zentrale einfache k-Algebra, deren Klasse in Br(k) die Ordnung m besitzt. Dann gibt es Elemente

$$a_1,...,a_i \in k^*$$

derart, daß A über

$$K = k(\sqrt[m]{a_1},..., \sqrt[m]{a_i})$$

zerfällt. Insbesondere zerfällt A über einer Galois-Erweiterung mit auflösbarer Galois-Gruppe.

2.6 Eine grundlegende exakte Sequenz der Gruppen-Kohomologie

In diesem Abschnitt beweisen wir eine abstrakte Aussage, die zusammen mit der Abstiegsmethode unser wichtigstes Werkzeug bei Berechnungen sein wird.

2.6.1 Der Anfang der langen Kohomologie-Sequenz

Seien G eine Gruppe und

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

eine exakte Sequenz von Gruppen mit G-Operation.[76] Dann besteht eine exakte Sequenz von punktierten Mengen

$$1 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C).$$

Eine exakte Sequenz punktierter Mengen ist nach Definitoin eine Sequenz, in welcher der Kern jeder Abbildung gleich dem Bild der vorangehenden Abbildung ist. Dabei versteht man unter dem Kern einer Abbildung punktierter Mengen, die Menge der Elemente, die in den Basis-Punkt abgebildet werden.

Beweis. Die einzigen nicht-trivialen Teile des Beweises bestehen in der Definition der Abbildung

$$\delta: C^G \longrightarrow H^1(G, A)$$

und im Beweis der Exaktheit an den Stellen C^G und $H^1(G, A)$.

Definition der Abbildung δ.

Sei

$$c \in C^G.$$

Wir wählen ein Urbild

$$b \in B$$

von C bezüglich der gegebenen Surjektion $B \longrightarrow C$. Für jedes $\sigma \in G$ wird dann das Element

$$b\sigma(b)^{-1}$$

bei dieser Surjektion in die 1 abgebildet.[77] Also liegt dieses Element in A,[78]

$$b\sigma(b)^{-1} \in A.$$

Durch direktes Nachrechnen sieht man, die Abbildung

$$G \longrightarrow A,\ \sigma \mapsto b\sigma(b)^{-1}, \tag{1}$$

ist ein 1-Kozyklus, und eine Modifikation von b mit einem Element von A liefert einen äquivalenten 1-Kozyklus. Man erhält also eine wohldefinierte Abbildung δ von der geforderten Art.

Exaktheit an der Stelle C^G.

---

[76] d.h. die Homomorphismen der exakten Sequenz sind G-äquivariant.

[77] Weil c bei der Operation von G in sich abgebildet wird.

[78] Wir fassen hier A als Untergruppe von B auf bezüglich der gegebenen Injektion $A \longrightarrow B$.

Nach Definition überführt δ die Elemente von C^G, die von B^G kommen[79], in die 1. Sei jetzt umgekehrt $\delta(c) = 1$. Dann ist der 1-Kozyklus (1) äquivalent zum konstanten 1-Kozyklus

$$G \longrightarrow A,\ \sigma \mapsto 1,$$

d.h. es gibt ein Element $a \in A$ mit

$$b\sigma(b)^{-1} = a^{-1}\sigma(a) \text{ für jedes } \sigma \in G,$$

d.h. $ab = \sigma(ab)$. Als Urbild von c in B kann man das G-invariante Element $ab \in B^G$ wählen, d.h. c liegt im Bild der Abbildung $B^G \longrightarrow C^G$.

Exaktheit an der Stelle $H^1(G, A)$.
Die Zusammensetzung

$$C^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B)$$

ist nach Konstruktion trivial: als 1-Kozyklus mit Werten in B ist (1) äquivalent zum konstanten 1-Kozyklus $\sigma \mapsto 1$.
Sei jetzt umgekehrt

$$a: G \longrightarrow A,\ \sigma \mapsto a_\sigma,$$

ein 1-Kozyklus, der als 1-Kozyklus mit Werten in B trivial ist (d.h. äquivalent zum 1-Kozyklus $\sigma \mapsto 1$). Dann gibt es nach Definition ein $b \in B$ mit

$$a_\sigma = b^{-1}\sigma(b) \text{ für jedes } \sigma \in G.$$

Sei c das Bild von b^{-1} in C. Wegen $\sigma(b) = a_\sigma b$ und $a_\sigma \in A$ gilt dann $\sigma(c) = c$ für jedes $\sigma \in G$, also

$$c \in C^G.$$

Das Bild von c bei δ ist nach Konstruktion gerade die Klasse von a, d.h. diese Klasse liegt im Bild von δ.
QED.
Bemerkung
Als eine erste Anwendung beweisen wir den Satz von Noether-Skolem.

2.6.2 Satz von Noether-Skolem

Alle Automorphismen einer zentralen einfachen k-Algebra sind innere Automorphismen (d.h. Konjugation mit einem umkehrbaren Element der Algebra).
Beweis. Seien A eine zentrale einfache k-Algebra, welche über der endlichen Galois-Erweiterung K/k zerfällt. Dann ist

$$A \otimes_k K$$

isomorph zu einer vollen Matrizen-Algebra $M_m(K)$. Insbesondere sind alle Automorphismen von $A \otimes_k K$ innere Automorphismen (nach 2.4.1). Der Gruppen-Homomorphismus

$$(A \otimes_k K)^* \longrightarrow \mathrm{Aut}_K(A \otimes_k K),$$

welcher jedem umkehrbaren Element die Konjugation mit diesem Element zuordnet, ist somit surjektiv. Der Kern dieses Homorphismus besteht aus den den Skalar-Matrizen entsprechenden Elementen der Algebra.[80] Wir erhalten damit eine exakte Sequenz

---

[79] d.h. man kann $b \in B^G$ wählen.

[80] Eine Matrix kommutiert genau dann mit allen anderen Matrizen, wenn es sich um eine Skalar-Matrix handelt.

$$1 \longrightarrow K^* \longrightarrow (A\otimes_k K)^* \longrightarrow \mathrm{Aut}_K(A\otimes_k K) \longrightarrow 1$$

abelscher Gruppen. Auf diesen Gruppen operiert die Galois-Gruppe

$$G = G(K/k)$$

und die Gruppen-Homomorphismen sind äquivariant bezüglich dieser Operation.[81] Für jeden Automorphismus $\alpha: A\otimes_k K \longrightarrow A\otimes_k K$ und jedes $\sigma\in G$ gilt

$$(\sigma(\alpha))(x) = \sigma^{-1}(\alpha(\sigma(x))),$$

d.h. die G-invarianten Automorphismen sind gerade diejenigen α mit

$$\sigma^{-1}(\alpha(\sigma(x))) = \alpha(x) \text{ für alle } x,$$

d.h.

$$\alpha(\sigma(x)) = \sigma(\alpha(x)) \text{ für alle } x.$$

Insbesondere überführt α den G-invarianten Teil von $A\otimes_k K$ in sich, d.h.

$$\alpha(A) \subseteq A.$$

Mit anderen Worten, α liegt im Bild der natürlichen Einbettung

$$\mathrm{Aut}_k(A) \hookrightarrow \mathrm{Aut}_K(A\otimes_k K),\ \beta \mapsto \beta\otimes \mathrm{Id}.$$

$$\alpha(x) = \sigma(\alpha(x)) \text{ für alle } x \in A,$$

Wir haben gezeigt,

$$\mathrm{Aut}_K(A\otimes_k K)^G = \mathrm{Aut}_k(A).$$

Wir gehen zu den G-invarianten Teilen der exakten Sequenz über und erhalten nach 2.6.1 eine exakte Sequenz

$$1 \longrightarrow k^* \longrightarrow A^* \longrightarrow \mathrm{Aut}_k(A) \longrightarrow H^1(G(K/k), K^*).$$

Nach dem Satz 90 von Hilbert ist die Kohomologie-Menge rechts trivial, d.h.
die Abildung

$$A^* \longrightarrow \mathrm{Aut}_k(A),$$

welche jeder Einheit den zugehörigen inneren Automorphismus zuordnet, ist surjektiv.
QED.

Bemerkung

Als weitere Anwendung geben wir eine nützliche kohomologische Charakterisierung der reduzierten Normen an. Zunächst aber eine Bezeichnung:

2.6.3 Definition: $SL_1(A)$

Sei A eine zentrale einfache k-Algebra. Dann bezeichne

$$SL_1(A) := \{a \in A \mid \mathrm{Nrd}(a) = 1\}$$

die multiplikative Gruppe der Elemente der reduzierten Norm 1.[82]

Bemerkung

Für $A = M_n(k)$ ist $SL_1(A) = SL_n(k)$, da die reduzierte Norm $\mathrm{Nrd}:A\longrightarrow K$ gerade die Determinante ist.

---

[81] Die Sequenz stimmt bis auf Isomorphie mit der Sequenz

$$1 \longrightarrow K\bullet\mathrm{Id} \longrightarrow M_m(K) \longrightarrow PGL_m(K) \longrightarrow 1$$

überein, wobei links die natürliche Einbettung der Skalarmatrizen steht und rechts die natürliche Surjektion auf die Faktorgruppe mit dem Kern K•Id.

[82] Man beachte, nach 2.5.2 ist ein Element von A genau dann umkehrbar, wenn seine reduzierte Norm von 0 verschieden ist.

2.6.4 Eine kohomologische Charakterisierung der reduzierten Normen

Seien A eine zentrale einfache k-Algebra, welche über der endlichen Galois-Erweiterung K/k zerfällt, und G = G(K/k) deren Galois-Gruppe. Dann besteht ein Isomorphismus punktierter Mengen

$$H^1(G, SL_1(A\otimes_k K)) \cong k^*/\mathrm{Nrd}(A^*).$$

Bemerkung
Zum Beweis dieser Aussage benötigen wir die folgende Verallgemeinerung des Satzes 90 von Hilbert (Beispiel 2.3.8).

2.6.5 Eine Verallgemeinerung des Satzes 90 von Hilbert

Seien A eine zentrale einfache k-Algebra, welche über der endlichen Galois-Erweiterung K/k zerfällt, und G = G(K/k) deren Galois-Gruppe. Dann gilt[83]

$$H^1(G, (A\otimes_k K)^*) = 1.$$

Beweis. Wir betrachten A als k-Vektorraum. Die Multiplikation von A ist eine über k bilineare Abbildung

$$A \times A \longrightarrow A, (a,x) \mapsto ax.$$

Für jedes $a\in A$ erhält man eine k-lineare Abbildung

$$A \longrightarrow A, x \longrightarrow ax,$$

die man als Tensor Φ_a auf A ansehen kann. Das Paar

$$(A, (\Phi_a)_{a\in A})$$

aus A und der Familie der Φ_a ist ein k-Objekt im verallgemeinerten Sinne von 2.3.15.

Zwischen den Tensoren Φ_a bestehen die Relationen

$$\Phi_{a'} + \Phi_{a''} = \Phi_{a'+a''} \text{ für } a', a'' \in A$$
$$\Phi_{a'}\circ\Phi_a = \Phi_{a'a''} \text{ für } \lambda,a \in A$$
$$\Phi_1 = \mathrm{Id}$$

Diese bedeuten gerade, daß A über sich selbst eine Modulstruktur besitzt. Sei jetzt

$$(B, (\Psi_a)_{a\in A})$$

ein K/k-Twist, d.h. B ist ein k-Vektorraum und die Ψ_a sind Tensoren auf B und es gibt einen K-linearen Isomorphismus

$$B\otimes_k K \longrightarrow A\otimes_k K,$$

bei welchen für jedes $a\in A$ der Tensor Ψ_a in den Tensor Φ_a abgebildet wird. Die obigen Relationen zwischen den Φ_a haben insbesondere zur Folge, daß die analogen Relationen zwischen den Ψ_a bestehen. Mit anderen Worten, ein K/k-Twist von $(A, (\Phi_a)_{a\in A})$ ist ein A-Modul B mit der Eigenschaft, daß $B\otimes_k K$ als $A\otimes_k K$-Modul isomorph ist zu $A\otimes_k K$.

Nach der verallgemeinerten Variante des Abstiegssatzes 2.3.7 besteht eine Isomorphie der punktierten Menge der getwisteten Formen mit der ersten Kohomologie,

(1) $$TF_K(A_K, ((\Phi_a)_K)_{a\in A}) \cong H^1(G, \mathrm{Aut}_K(\Phi_a)_{a\in A}).$$

Ein Element von $\mathrm{Aut}_K(\Phi)$ ist ein K-linearer Isomorphismus

---

[83] Für $A = M_n(k)$ ist $(A\otimes_k K)^* = M_n(K)^* = GL_n(K)$ und man erhält die alte Formulierung des Satzes 90 von Hilbert in 2.3.8.

$$\alpha: A\otimes_k K \longrightarrow A\otimes_k K,$$

der Modulstruktur von $A\otimes_k K$ über sich selbst verträglich ist, d.h. mit

$$\alpha(a\bullet m) = a\bullet\alpha(m) \text{ für } a, m \in A\otimes_k K .$$

Damit ist

$$\mathrm{Aut}_K(\Phi) = \mathrm{Aut}_{A\otimes_k K}(A\otimes_k K) = (\mathrm{End}_{A\otimes_k K}(A\otimes_k K))^* \cong (A\otimes_k K)^*$$

Zur Isomorphie ganz rechts siehe auch den Anfang des Beweises von A1.11(ii). Damit steht rechts in (1) die Kohomologie-Menge, die wir berechnen wollen.

Es reicht also die linke Seite von (1) zu bestimmen. Sei also (V, Ψ) ein K/k-Twist von (A,. Φ), d.h. V ist ein A-Modul mit

(2) $$V\otimes_k K \cong A\otimes_k K$$

als Moduln über $A\otimes_k K$. Nach dem Satz von Wedderburn gibt es eine Divisionsalgebra D und ein n mit

$$A \cong M_n(D).$$

Insbesondere ist A halbeinfach, d.h. die A-Moduln A und V sind direkte Summen von einfachen A-Moduln. Als Matrizen-Algebra besitzt A bis auf Isomorphie nur einen einfachen A-Modul. Die Anzahl der direkten Summanden von A und V in einer Zerlegung in einfache Moduln ist aus Dimensionsgründen (d.h. wegen (2)) für beide A-Moduln dieselbe. Deshalb gilt

$$V \cong A \text{ als A-Modul.}$$

Wir haben gezeigt, es gibt bis auf k-Isomorphie für A nur einen K/k-Twist, d.h.

$$\mathrm{TF}_K(A_K, \Phi_K)$$

ist trivial.
QED.

2.6.6. Beweis von 2.6.3

Die Fortsetzung der reduzierten Norm

$$\mathrm{Nrd}: A \longrightarrow k$$

auf $A\otimes_k K$ ist nach Definition gerade die Determinante

$$A\otimes_k K \cong M_m(K) \xrightarrow{\det} K,$$

also insbesondere surjektiv. Damit erhalten wir eine exakte Sequenz

$$1 \longrightarrow \mathrm{SL}_1(A\otimes_k K) \longrightarrow (A\otimes_k K)^* \xrightarrow{\mathrm{Nrd}} K^* \longrightarrow 1.$$

Wir gehen zu den invarianten Teilen über und erhalten nach 2.6.1 eine exakte Sequenz

$$A^* \xrightarrow{\mathrm{Nrd}} k^* \longrightarrow H^1(G, \mathrm{SL}_1(A\otimes_k K)) \longrightarrow H^1(G, (A\otimes_k K)^*).$$

Nach 2.6.5 ist die Menge ganz rechts trivial, d.h. die Abbildung in der Mitte ist surjektiv. Dann gilt aber

$$H^1(G, \mathrm{SL}_1(A\otimes_k K)) \cong k^*/\mathrm{Nrd}(A^*).$$

Aufgaben

1. Tensorprodukt von Divisionsalgebren

Man zeige, das Tensorprokte D'$\otimes_k$D" von Divisionsalgebren mit teilerfremden Graden ist eine Divisionsalgebra.

Hinweis: man wende das Lemma von Rieffel an mit einem Linksideal L in $D' \otimes_k D''$ und zeige $\dim_k (D' \otimes_k D'') = \dim_k L$.

2. Additive Variante des Satzes 90 von Hilbert

Man zeige, für jede endliche Galois-Erweiterung K/k mit der Gruppe G ist die Menge $H^1(G, K^+)$ trivial, wenn K^+ die additive Gruppe des Körpers K bezeichnet.

Hinweis. Man fasse K^+ vermittels

$$K^+ \longrightarrow GL_2(K),\ a \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

als Untergruppe der $GL_2(K)$ auf und wende 2.6.1 an).

3. Die Kohomologie mit Koeffizienten in der SL_n

Sei K/k eine endliche Galois-Erweiterung mit der Gruppe G. Man bestimme

$$H^1(G, SL_n(K)).$$

4. Konstruktion des Inversen in der Brauergruppe

Sei A eine zentrale einfache Algebra des Grades n über dem Körper k. Man verwende wie folgt den Galois-Abstieg für einen alternativen Beweis der Isomorphie

$$A \otimes_k A^0 \cong M_{n^2}(k)$$

im Beweis von 2.4.10.

(a) Man konstruiere für eine Galois-Erweiterung K/k, über welcher A zerfällt explizit eine Isomorphismie

$$M_n(K) \otimes_k M_n(K)^0 \cong M_{n^2}(K).$$

(b) Man twiste die Standard-Operationen von G := G(K/k) auf den Matrizen-Algebren $M_n(K)$ und $M_n(K)^0$ mit dem 1-Kozyklus $\sigma \mapsto a_\sigma = \psi^{-1} \circ \sigma(\psi)$ zu einem Isomorphismus

$$\psi: A \otimes_k K \longrightarrow M_n(K)$$

und zeige, der Isomorphismus ${}_aM_n(K) \otimes_k {}_aM_n(K)^0 \cong M_{n^2}(K)$ ist G-äquivariant.

(c) Man schließe den Beweis ab durch Übergang zu den invarianten Teilen.

5. Die Ordnung der zyklischen Algebren in der Brauer-Gruppe.

Seien k ein Körper, der eine m-te primitive Einheitswurzel enthält, und $a, b \in k^*$ wie in 2.5.5. Zeigen Sie, die Klasse der zyklischen Algebra $(a, b)_\omega$ in der Brauer-Gruppe hat eine Ordnung, welche m teilt.

6. Trivialität von $(a, 1\text{-}a)_\omega$ in der Brauer-Gruppe

Man zeige, für jedes $a \in k^*$ ist die Klasse der zyklischen Algebra $(a, 1\text{-}a)_\omega$ trivial in der Brauer-Gruppe.

7. Quaternionen-Algebren: Galois-Operationen und Kommutatoren

Seien k ein Körper der Charakteristik $\neq 0$ und Q eine Quaterionen-Algebra über k, welche Divisionsalgebra ist.

(a) Sei $L \subseteq Q$ ein Teilkörper. Man zeige, es gibt ein Element $q \in Q^*$ mit $qLq^{-1} \subseteq L$. Außerdem induziert die Konjugation mit q die Operation von Gal(L/k) auf L.
Hinweis: Man verwende den Satz von Skolem-Noether.

(b) Sei $r \in Q$ ein Element der Quaternionen-Norm 1,

$$N(r) = 1.$$

Man zeige, r ist ein Kommutator in der multiplikativen Gruppe Q*.
Hinweis. Man verwende den Satz von Hilbert 90 in seiner klassischen Formulierung.

8. Satz von Dieudonné

Seien D/k eine Divisions-Algebra mit dem Zentrum k und n eine natürliche Zahl. Bezeichne

$$GL_n(D)$$

die Gruppe der umkehrbaren Elemente der zentralen einfachen k-Algebra $M_n(D)$ und

$$Nrd_n : M_n(D) \longrightarrow k$$

deren reduzierte Norm. Wir betrachten für $1 \leq i \neq j \leq n$ und $d \in D$ die Matrix

$$E_{i,j}(d) = I_n + d \bullet E_{ij},$$

deren Einträge auf der Hauptdiagonalen gleich 1, deren Eintrag in der Position (i,j) gleich d und deren übrige Einträge gleich 0 sind.

(a) Man zeige, $Nrd_n(E_{ij}(d)) = 1$ für alle i,j,d.

(b) Sei

$$E_n(D)$$

die von den Matrizen

$$E_{ij}(d),\ 1 \leq i \neq j \leq n,\ d \in D$$

erzeugte Untergruppe von $GL_n(D)$ und

$$Diag_n(D^*)$$

die Untergruppe der Diagonal-Matrizen von $GL_n(D)$. Man zeige,

$$GL_n(D) \cong E_n(D) \bullet Diag_n(D^*) \bullet E_n(D).$$

(c) Satz von Dieudonné. Man folgere,

$$Im(GL_n(D) \xrightarrow{Nrd_n} k^*) = Im(GL_1(D) \xrightarrow{Nrd_1} k^*).$$

3 Gruppen-Kohomologie

Für die weiteren Untersuchungen der Brauer-Gruppen benötigen wir einige grundlegenden Begriffe aus der Theorie der Kohomologie-Gruppen mit Koeffizienten in einem abelschen Modul. Dies ist eine in der Literatur gut dokumentierte Theorie. Wir geben beweisen hier nur diejenigen Fakten, die wir im folgenden benötigen (zum leichteren Verständnis für den Leser). Insbesondere beweisen wir die Exaktheit der grundlegenden Sequenzen, konstruieren die Cup-Produkte und untersuchen die Abbildungen, welchen die Kohomologie einer Gruppe mit der einer Untergruppe oder Faktorgruppe verbinden. Entsprechend dem gegenwärtigen Standpunkt in der homologischen Algebra betonen wir die Verwendung von Komplexen und projektiven Auflösungen gegenüber der expliziten Beschreibung der Kozyklen und der Technik der Dimensionsverschiebung (obwohl letztere ebenfalls sehr nützlich sind).

Wie schon gesagt ist der Gegenstand dieses Kapitels inzwischen weitgehend standartisiert, und fast alle Tatsachen kann man bereits in der ersten Monographie zur homologischen Algebra von Cartan und Eilenberg [1] finden.

3.1 Definition der Kohomologie-Gruppen

3.1.1 Moduln über einer Gruppe

Sei G ein Gruppe. Ein (linker) G-Modul ist eine abelschen Gruppe A mit einer linken Operation von G,

$$G \times A \longrightarrow A.$$

Falls G auf A trivial operiert, d.h. wenn

$$s \bullet a = a \text{ für } s \in G \text{ und } a \in A$$

gilt, so heißt A auch trivialer G-Modul. Ein G-Homomorphismus ist ein äquivarianter Homomorphismus

$$h: A \longrightarrow B$$

von abelschen Gruppen, d.h. ein Gruppen-Homomorphismus, der mit den Gruppen-Operationen verträglich ist, d.h. mit

$$h(\sigma \bullet a) = \sigma \bullet h(a) \text{ für jedes } a \in A \text{ und jedes } \sigma \in G.$$

Die Menge der G-Homomorphismen $A \longrightarrow B$ wird mit

$$\mathrm{Hom}_G(A, B)$$

bezeichnet. Die Untergruppe der G-invarienten Elemente von A wird mit

$$A^G := \{a \in A \mid \sigma(a) = a \text{ für } \sigma \in G\}$$

bezeichnet.

Bemerkungen

(i) Der Begriff des G-Moduls stimmt mit dem Begriff des Moduls über dem Gruppen-Ring

$$\mathbb{Z}[G] = \oplus_{\sigma \in G} \mathbb{Z}\sigma$$

überein. Für jedes Element $\sum_{\sigma \in G} n_\sigma \bullet \sigma \in \mathbb{Z}[G]$ und jedes $a \in A$ ist durch

$$\left(\sum_{\sigma \in G} n_\sigma \bullet \sigma\right) \bullet a := \sum_{\sigma \in G} n_\sigma \bullet \sigma(a)$$

auf A eine $\mathbb{Z}[G]$-Modul-Struktur definiert. Umgekehrt definiert wegen $G \subseteq \mathbb{Z}[G]$ jede $\mathbb{Z}[G]$-Modul-Struktur auf A eine Operation von G auf A.

(ii) $\mathrm{Hom}_G(A, B)$ ist eine abelsche Gruppe bezüglich der üblichen Addition von Homomorphismen.

3.1.2 Axiomatische Beschreibung der Kohomologie-Gruppen I.

Unser Ziel ist es, für jede Gruppe G, jeden G-Modul A und jede nicht-negative ganze Zahl i eine abelsche Gruppe

$$H^i(G, A)$$

zu definieren, so daß die folgenden drei Bedingungen erfüllt sind.

1. $H^0(G, A) = A^G$ für jeden G-Modul A.
2. Für jeden G-Homomorphismus $A \longrightarrow B$ und jede nicht-negative ganze Zahl i gibt es natürliche Homomorphismen
$$H^i(G, A) \longrightarrow H^i(G, B)$$
3. Für jede kurze exakte Sequenz
$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$
von G-Moduln gibt es eine unendliche lange exakte Sequenz
$$0 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G,C) \longrightarrow H^1(G, A) \longrightarrow ...$$
$$... \longrightarrow H^i(G, A) \longrightarrow H^i(G, B) \longrightarrow H^i(G, C) \longrightarrow H^{i+1}(G, A) \longrightarrow ...$$
von abelschen Gruppen.

Bemerkungen

(i) Mit anderen Worten, wollen die im vorigen Kapitel eingeführten Gruppen
$$H^1(G, A)$$
auf den Fall von höheren Dimensionen verallgemeinern und insbesondere die lange exakte Sequenz von von 2.6.1 zu einer unendlichen Sequenz fortsetzen.

(ii) Man weiß nur im Fall kommutativer Gruppen A, daß dies möglich ist. Für nicht-kommutative A sind vernünftige Definitionen von $H^i(G, A)$ nur für $i \leq 3$ bekannt. Wir werden sie hier nicht betrachten.

(iii) Zur Konstruktion der Gruppen $H^i(G, A)$ beginnen wir mit einigen Ausführungen zur Theorie der linken Moduln über einem Ring
$$R,$$
der nicht notwendig kommutativ sein muß, aber ein 1-Element besitzt.

(iv) Genauer: statt (ii) fordert man, daß alle Konstruktionen, also auch die der langen Kohomologie-Sequenz 3, funktorielle bezüglich des Koeffizienten-Moduls A sind.

(v) Zur vollständigen axiomatischen Beschreibung der Kohomologie fehlt noch eine Bedingung, die besagt, daß die Gruppen $H^i(G, A)$ mit $i > 0$ für gewisse Koeffizienten-Moduln A gleich Null sind.

3.1.3 Kohomologie von Komplexen

Sei R ein nicht-notwendig kommutativer Ring mit 1. Ein (kohomologischer) Komplex von R-Moduln ist eine Sequenz von R-linearen Abbildungen

$$A^*: \quad ... \xrightarrow{d^{i-1}} A^i \xrightarrow{d^i} A^{i+1} \xrightarrow{d^{i+1}} ...$$

($i \in \mathbb{Z}$) mit $d^{i+1} \circ d^i = 0$ für jedes i. Wir werden auch

$$A_i := A^{-i} \text{ und } d_i = d^{-i}$$

schreiben. Weiter führen wir die folgenden Bezeichnungen ein.

$$Z^i(A^*) := \mathrm{Ker}(d^i),$$
$$B^i(A^*) := \mathrm{Im}(d^{i-1})$$
$$H^i(A^*) := Z^i(A)/B^i(A).$$

Der Komplex A^* heißt azyklisch, wenn $H^i(A^*) = 0$ gilt für alle i.

Ein Komplex-Morphismus $\Phi: A^* \longrightarrow B^*$ ist eine Familie von R-linearen Abbildungen $\Phi^i: A^i \longrightarrow B^i$ mit der Eigenschaft, daß für jedes i die folgenden Diagramm kommutativ sind.

$$\begin{array}{ccc} A^i & \longrightarrow & A^{i+1} \\ \Phi^i\downarrow & & \downarrow\Phi^{i+1} \\ B^i & \longrightarrow & B^{i+1} \end{array}$$

Ein kurze exakte Sequenz von Komplexen ist eine Sequenz von Komplex-Morphismen

$$0 \longrightarrow A^* \longrightarrow B^* \longrightarrow C^* \longrightarrow 0$$

mit der Eigenschaft, daß für jedes $i \in \mathbb{Z}$ die Sequenz

$$0 \longrightarrow A^i \longrightarrow B^i \longrightarrow C^i \longrightarrow 0$$

exakt ist.

Bemerkung

Auf Grund der Definition induziert jeder Komplex-Morphismus Φ: $A \longrightarrow B$ für jedes i einen Homorphismus

$$H^i(A^*) \longrightarrow H^i(B^*).$$

3.1.4 Die lange Sequenz zu einer kurzen exakten Sequenz von Komplexen

Sei

$$0 \longrightarrow A^* \longrightarrow B^* \longrightarrow C^* \longrightarrow 0$$

eine kurze exakte Sequenz von Komplexen. Dann gibt es eine lange exakte Sequenz

$$... \longrightarrow H^i(A^*) \longrightarrow H^i(B^*) \longrightarrow H^i(C^*) \xrightarrow{\partial} H^{i+1}(A) \longrightarrow ...$$

Der Homomorphismus ∂ heißt Zusammenhangshomomorphimus oder auch Korand-Abbildung.

Zum Beweis dieser Aussage benötigen wir das folgende Lemma.

3.1.5 Schlangen-Lemma

Für jedes kommutative Diagramm von R-Moduln

$$\begin{array}{ccccccc} & & A & \longrightarrow & B & \longrightarrow & C \longrightarrow 0 \\ & & \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' \end{array}$$

mit exakten Zeilen gibt es eine exakte Sequenz

$$\mathrm{Ker}(\alpha) \longrightarrow \mathrm{Ker}(\beta) \longrightarrow \mathrm{Ker}(\gamma) \longrightarrow \mathrm{Koker}(\alpha) \longrightarrow \mathrm{Koker}(\beta) \longrightarrow \mathrm{Koker}(\gamma).$$

Beweis. Die Konstruktion der Abbildungen in dieser Sequenz ist offensichtlich mit Ausnahme der Abbildung

$$\partial;\ \mathrm{Ker}(\gamma) \longrightarrow \mathrm{Koker}(\alpha).$$

Sei

$$c \in \mathrm{Ker}(\gamma) \subseteq C$$

vorgegeben. Wir wählen ein Urbild

$$b \in B$$

von c. Wegen der Kommutativität des rechten Vierecks ist das Bild von $\beta(b)$ in C' gleich Null. Es kommt also von einem eindeutig bestimmten Element

$$a' \in A'.$$

Je zwei Urbilder b von c unterscheiden sich um ein Element aus A. Die zugehörigen Elemente a' unterscheiden sich also um ein Element aus $\mathrm{Im}(\alpha)$, liefern also dasselbe Element im Kokern von α.

Damit ist die Abbildung ∂ definiert. Die Exaktheit der Sequenz überlassen wir dem Leser als Übung.
QED.

3.1.6 Beweis von 3.1.4

Wir betrachten das folgende kommutative Diagramm,

$$\begin{array}{ccccccc} A^i/B^i(A) & \longrightarrow & B^i/B^i(B^*) & \longrightarrow & C^i/B^i(C^*) & \longrightarrow & 0 \\ \downarrow\alpha & & \downarrow\beta & & \downarrow\gamma & & \\ 0 \longrightarrow Z^{i+1}(A^*) & \longrightarrow & Z^{i+1}(B^*) & \longrightarrow & Z^{i+1}(C^*) & & \end{array},$$

dessen vertikale Abbildungen von den Korand-Operatoren der Komplexe kommen.

Die Zeilen dieses Diagramms sind exakt (wie man durch eine kleine Diagrammjagt herausfindet). Nach dem Schlangenlemma besteht dann aber eine exakte Sequenz

$$H^i(A^*) \longrightarrow H^i(B^*) \longrightarrow H^i(C) \longrightarrow H^{i+1}(A^*) \longrightarrow H^{i+1}(B^*) \longrightarrow H^{i+1}(C^*)$$

Durch Zusammensetzen erhält die lange Kohomologie-Sequenz von 3.1.4.

Bemerkung
Im weiteren benötigen wir den Begriff des projektiven Moduls und einige Eigenschaften dieser Moduln.

3.1.7 Projektive Moduln

Ein R-Modul P heißt projektiv, wenn für jede surjektive R-lineare Abbildung

$$\alpha: A \longrightarrow B$$

die Abbildung

$$\mathrm{Hom}(P, A) \longrightarrow \mathrm{Hom}(P, B)\ ,\ \lambda \mapsto \lambda\circ\alpha,$$

ebenfalls surjektiv ist, d.h. jede R-lineare Abbildung $P \longrightarrow B$ läßt sich entlang α anheben.

Beispiele
(i) R ist als R-Modul über sich selbst projektiv.
(ii) Jede direkte Summe von projektiven R-Moduln ist projektiv.

Beweis. Zu (i). Für jedes Diagramm

$$\begin{array}{ccc} A & \overset{\alpha}{\twoheadrightarrow} & B \\ & & \uparrow\beta \\ & & R \end{array}$$

von R-linearen Abbildungen (mit α surjektiv) kann man ein Element $a \in A$ finden mit

$$\alpha(a) = \beta(1).$$

Die R-lineare Abbildung

$$R \longrightarrow A,\ r \mapsto r\bullet a,$$

ist dann die gesuchte Anhebung von β entlang α.
Zu (ii). Für jedes Diagramm

$$\begin{array}{ccc} A & \overset{\alpha}{\twoheadrightarrow} & B \\ & & \uparrow\beta \\ & & \oplus_i M_i \end{array}$$

von R-linearen Abbildungen (mit α surjektiv) läßt sich β genau dann anheben entlang α, wenn dies für alle Einschränkungen $\beta|_{M_i}$ der Fall ist.

QED.

3.1.8 Folgerung: freie Moduln sind projektiv

Jeder freie R-Modul ist projektiv.

3.1.9 Beispiel: F(A)

Für jeden R-Modul A bezeichne

$$F(A) := \oplus_{a \in A} R_a \text{ (mit } R_a = R \text{ für jedes a)}$$

die direkte Summe der Familie von Kopien von A, welche durch A indiziert wird. Dann besteht eine R-lineare Surjektion

$$\pi_A : F(A) \longrightarrow A,\ 1_a \mapsto a,$$

welche durch die Bedingung definiert ist, daß das Einselement 1_a des a-ten direkten Summanden in a abgebildet wird.

3.1.10 Kriterium für projektive Moduln

Für jeden R-Modul P sind folgende Aussagen äquivalent.

(i) P ist projektiv.

(ii) P ist direkter Summand eines freien R-Moduls, d.h. es gibt einen R-Modul P' mit der Eigenschaft, daß

$$P \oplus P' \cong F$$

isomorph ist zu einem freien R-Modul.

Beweis. (ii) $\Rightarrow$ (i). Für jedes Diagramm

$$\begin{array}{ccc} & & B \\ & & \uparrow \beta \\ A & \overset{\alpha}{\twoheadrightarrow} & P \end{array}$$

von R-linearen Abbildungen kann man β zu einer R-linearen Abbildung auf $P \oplus P'$ fortsetzen, indem man alle Elemente von P' in die Null abbildet. Es reicht also für

$$\begin{array}{ccc} & & B \\ & & \uparrow \beta \\ A & \overset{\alpha}{\twoheadrightarrow} & P \oplus P' \end{array}$$

zu zeigen, daß sich β entlang α anheben läßt. Das ist aber der Fall, weil $P \oplus P'$ frei, also projektiv ist.

(i) $\Rightarrow$ (ii). Wir betrachten das Diagramm

$$\begin{array}{ccc} & & P \\ & & \uparrow \beta := Id\ , \\ F(P) & \overset{\alpha}{\twoheadrightarrow} & P \end{array}$$

wobei α die Surjektion von 3.1.9 ist und β die identische Abbildung. Weil P projektiv ist, läßt sich β entlang α anheben, d.h. α besitzt einen Schnitt $s: P \longrightarrow F(P)$. Dann ist aber

$$\varphi : P \oplus Ker(\alpha) \longrightarrow F(P),\ (p, x) \mapsto s(p) + x,$$

ein R-linearer Isomorphismus (mit der Inversen ψ: $y \mapsto (\alpha(y), y - s(\alpha(y)))$).[84]

---

[84] Es gilt

$$\begin{aligned} \psi(\varphi(p,x)) &= \psi(s(p)+x) \\ &= (\alpha(s(p)+x),\ s(p)+x - s(\alpha(s(p)+x))) \\ &= (\alpha(s(p)),\ s(p) + x - s(\alpha(s(p)))) \text{ wegen } x \in Ker(\alpha) \\ &= (p,\ s(p) + x - s(p)) \text{ weil s ein Schnitt von } \alpha \text{ ist} \end{aligned}$$

QED.

3.1.11 Projektive Auflösungen

Eine projektive Auflösung eines R-Moduls A ist ein Komplex

$$... \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

von R-linearen Abbildungen projektiver R-Moduln zusammen mit einer Surjektion

$$P_0 \longrightarrow A,$$

welche Augmentation heißt, wobei die folgende unendliche Sequenz exakt ist:

$$... \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

Bemerkung
Jeder R-Modul A besitzt eine projektive Auflösung.
Beweis. Für P_0 kann man zum Beispiel den in 3.1.9 definierten R-Modul F(A) nehmen und für $P_0 \longrightarrow A$ die dort angegebene natürliche Surjektion. Angenommen, wir haben bereits eine exakte Sequenz

$$P_n \longrightarrow P_{n-1} \longrightarrow ... \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

mit P_i projektiv für alle i konstruiert. Dann kann man

$$P_{n+1} := F(K)) \text{ mit } K := Ker(P_n \longrightarrow P_{n-1})$$

setzen und als Abbildung

$$P_{n+1} \longrightarrow P_n$$

die Zusammensetzung aus der natürlichen Surjektion $P_{n+1} = F(K) \longrightarrow K$ und der natürlichen Einbettung $K \subseteq P_n$ verwenden.
QED.

3.1.12 Vergleichssatz

Sei ein kommutatives Diagramm

$$\begin{array}{ccccccccc} ... & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & A \longrightarrow 0 \\ & & & & & & & & \downarrow \alpha \\ .. & \longrightarrow & B_2 & \xrightarrow{b_2} & B_1 & \xrightarrow{b_1} & B_0 & \xrightarrow{b_0} & B \longrightarrow 0 \end{array}$$

von R-linearen Abbildungen gegeben, wobei die Moduln der oberen Zeile einen Komplex mit P_i projektiv bilden sollen und die untere Zeile exakt sei. Dann gibt es R-lineare Abbildungen $\alpha_i: P_i \longrightarrow B_i$, welche sich kommutativ in dieses Diagramm einfügen lassen, d.h. das folgende Diagramm ist kommutativ.

$$\begin{array}{ccccccccc} ... & \longrightarrow & P_2 & \xrightarrow{p_2} & P_1 & \xrightarrow{p_1} & P_0 & \xrightarrow{p_0} & A \longrightarrow 0 \\ & & \downarrow \alpha_2 & & \downarrow \alpha_1 & & \downarrow \alpha_0 & & \downarrow \alpha \\ .. & \longrightarrow & B_2 & \xrightarrow{b_2} & B_1 & \xrightarrow{b_1} & B_0 & \xrightarrow{b_0} & B \longrightarrow 0 \end{array}$$

$= (p, x).$

und

$\varphi(\psi(y)) = \varphi(\alpha(y), y - s(\alpha(y)))$
$= s(\alpha(y)) + y - s(\alpha(y))$
$= y.$

Für je zwei solche Familien R-linearer Abbildungen, sagen wir (α_i) und (β_i) gibt es R-lineare Abbildung $\gamma_i: P_i \longrightarrow B_{i+1}$ mit

(1) $$\alpha_i - \beta_i = \gamma_{i-1} \circ p_i + b_{i+1} \circ \gamma_i$$

Beweis. Zur Konstruktion von α_i nehmen wir an, daß alle α_j mit $j < i$ bereits definiert sind,

$$\begin{array}{ccccccccc} \ldots\longrightarrow & P_i & \xrightarrow{p_i} & P_{i-1} & \xrightarrow{p_{i-1}} & P_{i-2} & \xrightarrow{p_{i-2}} & P_{i-3} & \longrightarrow\ldots \\ & \downarrow\alpha_{i-1} & & (I) & \downarrow\alpha_{i-2} & & \downarrow\alpha_{i-3} & & \\ \ldots\longrightarrow & B_i & \xrightarrow{b_i} & B_{i-1} & \xrightarrow{b_{i-1}} & B_{i-2} & \xrightarrow{b_{i-2}} & B_{i-3} & \longrightarrow\ldots \end{array}$$

wobei wir

$$\alpha_{-1} := \alpha$$

vereinbaren. Es gilt

$$\mathrm{Im}(\alpha_{i-1} \circ p_i) \subseteq \mathrm{Ker}(b_{i-1}) = \mathrm{Im}(b_i).$$

Die Inklusion besteht, weil das Quadrat (I) kommutativ ist und die obere Zeile des Diagramms einen Komplex darstellt. Das Gleichheitszeichen besteht, weil die untere Zeile exakt ist.[85] Weil P_i projektiv ist, läßt sich $\alpha_{i-1} \circ p_i$ entlang b_i anheben[86] und liefert so den gesuchten Homomorphismus α_i. Damit ist die Existenz der Familie (α_i) gezeigt.

Seien jetzt zwei Familien (α_i) und (β_i) gegeben, welche sich kommutativ in das Diagramm einfügen lassen. Wir haben die Familie der γ_i zu konstruieren. Dazu setzen wir

$$\gamma_{-1} := 0$$

und nehmen zur Konstruktion von γ_i an, daß alle γ_j mit $j < i$ bereits definiert sind und der Bedinung (1) genügen. Wir betrachten das Diagramm

$$\begin{array}{ccccccccc} \ldots\longrightarrow & P_{i+1} & \xrightarrow{p_{i+1}} & P_i & \xrightarrow{p_i} & P_{i-1} & \xrightarrow{p_{i-1}} & P_{i-2} & \longrightarrow\ldots \\ & & \Delta\alpha_i\downarrow & \swarrow\gamma_{i-1} & \downarrow\Delta\alpha_{i-1} & \swarrow\gamma_{i-2} & \downarrow\Delta\alpha_{i-2} & & \\ \ldots\longrightarrow & B_{i+1} & \xrightarrow{b_{i+1}} & B_i & \xrightarrow{b_i} & B_{i-1} & \xrightarrow{b_{i-1}} & B_{i-2} & \longrightarrow\ldots \end{array}$$

mit

$$\Delta\alpha_i = \alpha_i - \beta_i$$

Es gilt

$$\begin{aligned} b_i \circ \Delta\alpha_i &= \Delta\alpha_{i-1} \circ p_i && \text{(weil (I) kommutativ ist)} \\ &= (\gamma_{i-2} \circ p_{i-1} + b_i \circ \gamma_{i-1}) \circ p_i && \text{(wegen (1) mit i-1 anstelle von i)} \\ &= b_i \circ \gamma_{i-1} \circ p_i && \text{(weil die obere Zeile ein Komplex ist)} \end{aligned}$$

also

---

[85] Für $i = 0$ gilt das trivialerweise.

[86] Wegen $\mathrm{Im}(\alpha_{i-1} \circ p_i) \subseteq \mathrm{Im}(b_i)$ können wir vorübergehend B_{i-1} durch $\mathrm{Im}(b_i)$ ersetzen und so dafür sorgen, daß b_i surjektiv wird.

$$b_i \circ (\Delta\alpha_i - \gamma_{i-1} \circ p_i) = 0,$$

also

$$\mathrm{Im}(\Delta\alpha_i - \gamma_{i-1} \circ p_i) \subseteq \mathrm{Ker}(b_i) = \mathrm{Im}(b_{i+1}).$$

Weil P_i projektiv ist, läßt sich $(\Delta\alpha_i - \gamma_{i-1} \circ p_i)$ entlang b_{i+1} anheben und liefert so einen Homomorphismus

$$\gamma_i : P_i \longrightarrow B_{i+1}$$

mit

$$b_{i+1} \circ \gamma_i = \Delta\alpha_i - \gamma_{i-1} \circ p_i .$$

Mit anderen Worten, es gilt (1).
QED.

3.1.13 Konstruktion der Kohomologie-Gruppen

Seien G eine Gruppe und A ein G-Modul. Wir versehen $\mathbb{Z}$ mit der trivialen Operation von G und wählen eine projektive Auflösung

$$P_* : \quad \ldots \xrightarrow{p_{i+1}} P_i \xrightarrow{p_i} P_{i-1} \xrightarrow{p_{i-1}} \ldots \xrightarrow{p_1} P_0 \longrightarrow 0$$

des trivialen G-Moduls $\mathbb{Z}$. Auf diesen Komplex wenden wir den kontravarianten Hom-Funktor $\mathrm{Hom}_G(? , A)$ an und erhalten einen Komplex

$$0 \longrightarrow \mathrm{Hom}_G(P_0,A) \longrightarrow \ldots \longrightarrow \mathrm{Hom}_G(P_{i-1},A) \longrightarrow \mathrm{Hom}_G(P_i,A) \longrightarrow \mathrm{Hom}_G(P_{i+1},A) \longrightarrow \ldots$$

den wir mit

$$\mathrm{Hom}_G(P_*,A)$$

bezeichnen. Die Kohomologie von G mit Werten in A wird definiert als die Kohomologie dieses Komplexes,

$$H^i(G,A) := H^i(\mathrm{Hom}_G(P_*,A)) \text{ für } i = 0, 1, 2, 3, \ldots$$

3.1.14 Korrektheit der Definition der $H^i(G, A)$

Die Gruppen $H^i(G, A)$ besitzen die Eigenschaften 1-3 von 3.1.2 und sind unabhängig von der speziellen Wahl der Auflösung P_*.

Beweis. Eigenschaft 1.
Nach Definition gilt

$$H^0(G, A) = H^0(\mathrm{Hom}_G(P_*,A)) = \mathrm{Ker}(\mathrm{Hom}_G(P_0,A) \longrightarrow \mathrm{Hom}_G(P_1,A))$$

Aus der exakten Sequenz

$$P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

erhalten wir eine exakte Sequenz

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \longrightarrow \mathrm{Hom}_G(P_0,A) \longrightarrow \mathrm{Hom}_G(P_1, A),$$

d.h. es gilt

$$H^0(G, A) \cong \mathrm{Hom}_G(\mathbb{Z}, A).$$

Es reicht also zu zeigen, die Abbildung

(1) $$\mathrm{Hom}_G(\mathbb{Z}, A) \longrightarrow A^G, \phi \mapsto \phi(1),$$

ist wohldefiniert und bijektiv (sie ist dann offensichtlich ein Gruppen-Homomorphismus). Für jeden G-Homomorphismus $\phi : \mathbb{Z} \longrightarrow A$ und jedes $\sigma \in G$ gilt

$$\sigma(\phi(1)) = \phi(\sigma(1)) =^{87} \phi(1),$$

d.h. $\phi(1)$ liegt in A^G und die Abbildung (1) ist korrekt definiert. Ein auf $\mathbb{Z}$ definierter Gruppen-Homomorphismus ist durch seinen Wert an der Stelle 1 bereits vollständig festgelegt. Also ist die Abbildung (1) injektiv. Für jedes G-invariante $a \in A$ ist außerdem durch

$$\mathbb{Z} \longrightarrow A,\ n \mapsto na,$$

ein G-Homomorphismus definiert. Sein Bild bei (1) ist gerade a.

Eigenschaft 2.

Die Funktorialität der $H^i(G, A)$ in A (bei fest gewählter Auflösung P_* ergibt sich unmittelbar aus der Konstruktion in 3.1.13.

Eigenschaft 3.

Für jede kurze exakte Sequenz

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

von G-Moduln ist

$$0 \longrightarrow \mathrm{Hom}_G(P_*,A) \longrightarrow \mathrm{Hom}_G(P_*,B) \longrightarrow \mathrm{Hom}_G(P_*,C) \longrightarrow 0$$

eine kurze exakte Sequenz von Komplexen. Die Exaktheit an der Stelle $\mathrm{Hom}_G(P_*,C)$ ergibt sich aus der Projektivität der Moduln P_i . Die Exaktheit an den anderen Stellen ist eine Folge des Homomorphie-Satzes. Die zu dieser kurzen exakten Sequenz gehörige lange exakte Kohomologie-Sequenz ist gerade die exakte Sequenz von Eigenschaft 3.

Die Unabhängigkeit von der speziellen Wahl der Auflösung.

Zum Beweis wählen wir eine zweite projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$, sagen wir

$$Q_*.$$

Wir wenden den Vergleichssatz 3.1.12 an mit Q_* anstelle von B_* und

$$\alpha = \mathrm{id}: \mathbb{Z} \longrightarrow \mathbb{Z}.$$

Wir erhalten einen Komplex-Morphismus

$$\alpha_*: P_* \longrightarrow Q_*,$$

welcher Homomorphismen der Kohomologie-Gruppen

$$\alpha^*: H^i(\mathrm{Hom}_G(Q_*,A)) \longrightarrow H^i(\mathrm{Hom}_G(P_*,A)) \tag{2}$$

induziert. Indem wir die Rollen von P_* und Q_* vertauschen erhalten wir außerdem einen Komplex-Morphismus

$$\beta_*: Q_* \longrightarrow P_*,$$

der Homomorphismen

$$\beta^*: H^i(\mathrm{Hom}_G(P_*,A)) \longrightarrow H^i(\mathrm{Hom}_G(Q_*,A)) \tag{3}$$

in umgekehrter Richtung definiert. Es reicht zu zeigen,

$$\alpha^* \circ \beta^* = \mathrm{Id} \text{ und } \beta^* \circ \alpha^* = \mathrm{Id}.$$

Aus Symmetrie-Gründen reicht es, die erste Identität zu beweisen.

Die Komplex-Morphismen

$$\beta_* \circ \alpha_*: P_* \longrightarrow P_* \text{ und } \mathrm{Id}: P_* \longrightarrow P_*$$

sind Familien von Abbildungen die zur selben Abbildung $\mathbb{Z} \longrightarrow \mathbb{Z}$ des Vergleichssatzes gehören. Ihre Differenz kann also in der Gestalt

$$\beta_* \circ \alpha_* - \mathrm{Id} = \partial \circ \gamma + \gamma \circ \partial$$

---

[87] G operiert trivial auf $\mathbb{Z}$.

geschrieben werden, wobei die ∂ vom Rand-Operator des Komplexes P_* kommen und γ von der im Vergleichssatz konstruierten Familie.[88] Wir wenden den Funktor Hom(?,A) an und erhalten

$$\mathrm{Hom}(\alpha_*,A)\circ\mathrm{Hom}(\beta_*,A) - \mathrm{Id} = \mathrm{Hom}(\gamma,A)\circ\delta + \delta\circ\mathrm{Hom}(\gamma,A)$$

wobei die Komponenten von δ gerade die Rand-Operatoren des Komplexes

$$\mathrm{Hom}(P_*,A)$$

sind. Der erste Summand der rechten Seite ist also auf den Zyklen dieses Komplexes identisch Null,

$$\mathrm{Hom}(\alpha_*,A)\circ\mathrm{Hom}(\beta_*,A) - \mathrm{Id} = \delta\circ\mathrm{Hom}(\gamma,A) \text{ auf } Z(\mathrm{Hom}(P_*,A))$$

Die Bilder der Abbildung rechts besteht aus lauter Rändern, d.h. die Kohomologie-Klassen der Werte der Abbildungen

$$\mathrm{Hom}(\alpha_*,A)\circ\mathrm{Hom}(\beta_*,A) \text{ und } \mathrm{Id}$$

stimmen an allen Stellen überein. Sie induzieren also auf der Kohomologie dieselbe Abbildung, d.h.

$$\alpha^*\circ\beta^* = \mathrm{Id}.$$

QED.

3.1.15 Bemerkungen

1. Ext-Funktoren. Die obige Konstruktion ist ein Spezialfall der Konstruktion der Ext-Gruppen der homologischen Algebra: für je zwei R-Moduln M und N definiert am

$$\mathrm{Ext}^i_R(M,N) := H^i(\mathrm{Hom}_R(P_*,N)),$$

wobei P_* eine projektive Auflösung von M bezeichnet. Dieselbe Argumentation wie eben zeigt die Unabhängigkeit dieser Definition von der Wahl der Auflösung P_*.

2. Funktorialität. Aus der Definition der Kohomologie-Gruppen ergibt sich, daß diese gewissen funktorielle Eigenschaften besitzen. Ist

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A' & \longrightarrow & B' \end{array}$$

ein kommutatives Diagramm von G-Moduln, so ist das zugehörige Diagramm

$$\begin{array}{ccc} H^i(G,A) & \longrightarrow & H^i(G,B) \\ \downarrow & & \downarrow \\ H^i(G,A') & \longrightarrow & H^i(G,B') \end{array}$$

für jedes $i \geq 0$ kommutativ. Weiter ist für jedes kommutative Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

von G-Moduln mit exakten Zeilen das zugehörige Viereck

$$\begin{array}{ccc} H^i(G,C) & \longrightarrow & H^{i+1}(G,A) \\ \downarrow & & \downarrow \\ H^i(G,C') & \longrightarrow & H^{i+1}(G,A') \end{array}$$

kommutativ für jedes $i \geq 0$.

---

[88] Dies sind keine Komplex-Morphismen, sondern nur Homomorphismen graduierter Gruppen.

3.2 Explizite Auflösungen

Zur Berechnung der Gruppen $H^i(G,A)$ verwendet man konkrete projektive Auflösungen. Die nützlichste von ihnen ist die folgende, welche inspiriert ist durch die simplizialen Konstruktionen der algebraischen Topologie.

3.2.1 Konstruktion: die Standard-Auflösung

Für jedes $i \geq 0$ betrachten wir den $\mathbb{Z}[G]$-Modul

(1) $$\mathbb{Z}[G^{i+1}],$$

wobei G^{i+1} das (i+1)-fache direkte Produkt der Gruppe G mit sich selbst bezeichnet. Die Operation von G auf diesem Modul sei $\mathbb{Z}$-linear und auf den $\mathbb{Z}$-Modul-Erzeugern gegeben durch

$$\sigma\bullet(\sigma_0,...,\sigma_i) := (\sigma\sigma_0,...,\sigma\sigma_i) \text{ für } \sigma, \sigma_0, \dots , \sigma_i \in G.$$

Der $\mathbb{Z}[G]$-Modul (1) ist isomorph zu $\mathbb{Z}[G]^{i+1}$, also frei und damit insbesondere projektiv. Wir definieren G-Homomorphismen

$$\delta^i = \sum_{j=0}^{i} (-1)^j s^i_j : \mathbb{Z}[G^{i+1}] \longrightarrow \mathbb{Z}[G^i],$$

wobei die Abbildung s^i_j gerade im Weglassen der j-ten Koordinate bestehe:

$$s^i_j : \mathbb{Z}[G^{i+1}] \longrightarrow \mathbb{Z}[G^i],\ (\sigma_0,...,\sigma_i) \mapsto (\sigma_0,...,\sigma_{j-1},\sigma_{j+1},...,\sigma_i).$$

Auf diese Weise erhält man eine projektive Auflösung

(2) $$\mathbb{Z}[G^*]: \quad ... \longrightarrow \mathbb{Z}[G^3] \xrightarrow{\delta^2} \mathbb{Z}[G^2] \xrightarrow{\delta^1} \mathbb{Z}[G] \longrightarrow 0$$

mit der Augmentation

$$\delta^0 = \varepsilon : \mathbb{Z}[G] \xrightarrow{\delta^0} \mathbb{Z},\ \sum_{\sigma\in G} n_\sigma \sigma \mapsto \sum_{\sigma\in G} n_\sigma.$$

Für jeden G-Modul A bezeichnet man die Elemente von

$$C^i(G,A) := \mathrm{Hom}_G(\mathbb{Z}[G^{i+1}], A)$$

als i-<u>Koketten</u> vom G mit Werten in A. Entsprechend heißen die Elemente von

$$Z^i(G,A) := Z^i(\mathrm{Hom}_G(\mathbb{Z}[G^*], A)) = Z^i(C^*(G,A))$$

bzw.

$$B^i(G,A) := B^i(\mathrm{Hom}_G(\mathbb{Z}[G^*], A)) = B^i(C^*(G,A))$$

auch i-<u>Kozyklen</u> bzw. i-<u>Koränder</u> von G mit Werten in A. Die Kohomologie-Gruppen sind dann gerade die Gruppen

$$H^i(G, A) = Z^i(G, A)/B^i(G,A) = H^i(C^*(G,A)).$$

Wir werden bald sehen, im Fall i = 1 erhalten wir gerade die Begriffe des vorigen Kapitels zurück (im Fall kommutativer Koeffizienten-Moduln).

Beweis der Exaktheit von (2).

<u>Zur Inklusion</u> $\mathrm{Im}(\delta^{i+1}) \subseteq \mathrm{Ker}(\delta^i)$.

Es gilt

$$\begin{aligned} \delta^i\circ\delta^{i+1} &= \Big(\sum_{j=0}^{i} (-1)^j s^i_j\Big)\circ\Big(\sum_{\ell=0}^{i+1} (-1)^\ell s^{i+1}_\ell\Big) \\ &= \sum_{j=0}^{i}\sum_{\ell=0}^{i+1} (-1)^{j+\ell} s^i_j \circ s^{i+1}_\ell \end{aligned}$$

Nun ist es gleich, ob man erst die ℓ-te Koordinate streicht und dann die j-te, oder ob man dies in der umgekehrten Reihenfolge tut, d.h. es ist für $j < \ell$:

$$s_j^i \circ s_\ell^{i+1} = s_{\ell-1}^i \circ s_j^{i+1}.$$

Es folgt

$$\begin{aligned}\delta^i \circ \delta^{i+1} &= \sum_{\ell \le j} (-1)^{j+\ell} s_j^i \circ s_\ell^{i+1} + \sum_{j<\ell} (-1)^{j+\ell} s_{\ell-1}^i \circ s_j^{i+1} \\ &= \sum_{\ell \le j} (-1)^{j+\ell} s_j^i \circ s_\ell^{i+1} + \sum_{j \le \ell} (-1)^{j+\ell+1} s_\ell^i \circ s_j^{i+1}\end{aligned}$$

Wir sehen, jeder Summand kommt zweimal, aber mit entgegengesetzen Vorzeichen vor.

Zur Inklusion $\mathrm{Ker}(\delta^i) \subseteq \mathrm{Im}(\delta^{i+1})$.

Wir fixieren ein Element $\sigma \in G$ und definieren die folgenden Gruppen-Homomorphismen.

$$h^i: \mathbb{Z}[G^{i+1}] \longrightarrow \mathbb{Z}[G^i],\ (\sigma_0,...,\sigma_i) \mapsto (\sigma,\sigma_0,...,\sigma_i).$$

Dann gilt[89]

$$\delta^{i+1} \circ h^i + h^{i-1} \circ \delta^i = \mathrm{Id}_{\mathbb{Z}[G^{i+1}]}.$$

Insbesondere induziert die identische Abbildung auf der Kohomologie dieselbe Abbildung wie die Null-Abbildung. Das ist nur möglich, wenn die Kohomologie gleich Null ist.

QED.

Βεμερκυνγ

Die Projektivität der Auflösung $\mathbb{Z}[G^*]$ ergibt sich aus der nachfolgenden Betrachtung.

3.2.2 Konstruktion: inhomogene Koketten

$\mathbb{Z}[G^{i+1}]$ ist ein freier $\mathbb{Z}[G]$-Modul mit der Basis

$$[\sigma_1,...,\sigma_i]\ \ (\sigma_1,...,\sigma_i \in G).$$

---

[89] Setzen wir

$$I := \delta^{i+1} \circ h^i$$

für den ersten Summanden links und

$$II := h^{i-1} \circ \delta^i$$

für den zweiten. Das Bild von

$$(\sigma_0,...,\sigma_i)$$

bei der Abbildung I entsteht durch Hinzufügen von σ als erste Koordinate und anschließenden alternierenden Streichen der einzelnen Koordinaten:

$$(\sigma_0,...,\sigma_i) - (\sigma,\hat{\sigma_0},\sigma_1,...,\sigma_i) + (\sigma,\sigma_0,\hat{\sigma_1},...,\sigma_i) \mp ...$$

Das Bild bei der Abbildung II ensteht durch alternierendes Streichen der einzelnenen Koordinaten und anschließenden Hinzufügen von σ:

$$(\sigma,\hat{\sigma_0},\sigma_1,...,\sigma_i) - (\sigma,\sigma_0,\hat{\sigma_1},...,\sigma_i) \pm ...$$

Wir sehen, der j-te Summand der zweiten Summe ist gerade der (j+1)-te Summand der ersten (mit entgegengesetzten Vorzeichen). Der einzige Summand der ersten Summe, der in der zweiten nicht vorkommt ist der ersten. Mit anderen Worten

$$I + II$$

ist die identische Abbildung.

.

Dabei bezeichne $[\sigma_1,...,\sigma_i]$ das Element

$$[\sigma_1,...,\sigma_i] := (1, \sigma_1, \sigma_1 \bullet \sigma_2 , \sigma_1 \bullet \sigma_2 \bullet \sigma_3 , ... , \sigma_1 \bullet ... \bullet \sigma_i) \in G^{i+1} \subseteq \mathbb{Z}[G^{i+1}].$$

Die Differentiale der Auflösung $\mathbb{Z}[G^*]$ sind auf diesen Basis-Elementen durch die folgende Formel gegeben[90].

(1) $$\delta^i([\sigma_1,...,\sigma_i]) = \sigma_1 \bullet [\sigma_2,...,\sigma_i] + \sum_{j=1}^{i-1} (-1)^j [\sigma_1,...,\sigma_j \bullet \sigma_{j+1},...,\sigma_i] + (-1)^i [\sigma_1,...,\sigma_{i-1}].$$

Insbesondere kann man die i-Koketten mit Werten im G-Modul A mit den Abbildungen

$$a: G^i \longrightarrow A, [\sigma_1,...,\sigma_i] \longrightarrow a_{\sigma_1,...,\sigma_i}$$

identifizieren[91]. Das Bild einer solchen Abbildung a beim Korand-Operator

$$\delta^*_{i+1}: C^i(G, A) \longrightarrow C^{i+1}(G, A)$$

ist dabei gerade die Abbildung[92]

$$G^i \longrightarrow A,$$

$$[\sigma_1,...,\sigma_{i+1}] \mapsto \sigma_1 a_{\sigma_2,...,\sigma_{i+1}} + \sum_{j=1}^{i} (-1)^j a_{\sigma_1,...,\sigma_j \sigma_{j+1},...,\sigma_{i+1}} + (-1)^{i+1} a_{\sigma_1,...,\sigma_i}.$$

Beweis der Basiseigenschaft der Elemente der Gestalt $[\sigma_1,...,\sigma_i]$. Jedes der Elemente von G^{i+1} läßt sich in der Gestalt

$$\sigma \bullet [\sigma_1,...,\sigma_i]$$

schreiben mit eindeutig bestimmten $\sigma, \sigma_1,...,\sigma_i \in G$, d.h. jedes Element von $\mathbb{Z}[G^{i+1}]$ ist eine $\mathbb{Z}$-Linearkombination solcher Elemente mit eindeutig bestimmten Koeffizienten aus $\mathbb{Z}$. Das bedeutet aber auch, jedes Element von $\mathbb{Z}[G^{i+1}]$ läßt sich als Linearkombination der Elemente

$$[\sigma_1,...,\sigma_i]$$

mit eindeutig bestimmten Koeffizienten aus $\mathbb{Z}[G]$.
QED.

3.2.3 Beispiele

1. Die ersten Kohomologie. Ein 1-Kozyklus der Gruppe G mit Werten im G-Modul A ist nach der obigen Definition gegeben durch eine Abbildung

$$a: G \longrightarrow A, \sigma \mapsto a_\sigma,$$

---

[90] Das Streichen von Koordinaten auf der rechten Seite der Definiton von $[\sigma_1,...,\sigma_i]$ entspricht gerade der Multiplikation benachbarter Koordinaten links.

[91] Eine R-lineare Abbildung ist durch ihre Werte auf einer Basis festgelegt, wobei man diese Werte beliebig vorgeben kann.

[92] $\delta^*_{i+1}(a)$ ist gerade die Zusammensetzung

$$\mathbb{Z}[G^{i+2}] \xrightarrow{\delta^{i+1}} \mathbb{Z}[G^{i+1}] \xrightarrow{a} A.$$

wobei a ein G-Homomorphismus ist. Die angegebene Abbildungsvorschrift ergibt sich unmittelbar aus (1) durch Einschränken auf die Elemente der Gestalt $[\sigma_1,...,\sigma_{i+1}]$.

mit $0 = \delta_2^*(a)(\sigma_1,\sigma_2) = \sigma_1 a_{\sigma_2} - a_{\sigma_1\sigma_2} + a_{\sigma_1}$, d.h. mit

$$a_{\sigma_1\sigma_2} = a_{\sigma_1} + \sigma_1 a_{\sigma_2}.$$

Das ist - in additiver Schreibweise - gerade die ursprüngliche Definition des 1-Kozyklus, wie wir sie in 2.3.6. angegeben haben. Dieser 1-Kozyklus ist ein 1-Korand, wenn es ein $b \in A$ gibt[93] mit

$$a_\sigma = \delta_1^*(b)(\sigma) = \sigma \bullet b - b \text{ für jedes } \sigma \in G.$$

Wir erhalten so die Defintionen des vorigen Kapitels zurück. Man beachte, operiert G trivial auf A, so gilt

$$Z^1(G, A) = \mathrm{Hom}(G, A) \text{ und } B^1(G, A) = 0,$$

also

$$H^1(G, A) = \mathrm{Hom}(G, A) \text{ für triviale G-Moduln A.}$$

2. Die zweite Kohomolgie. Ein 2-Kozyklus der Gruppe G mit Werten im G-Modul A ist durch eine Abbildung

$$G \times G \longrightarrow A, (\sigma_1, \sigma_2) \mapsto a_{\sigma_1,\sigma_2},$$

gegeben mit

$$\sigma_1 \bullet a_{\sigma_2,\sigma_3} - a_{\sigma_1\bullet\sigma_2, \sigma_3} + a_{\sigma_1, \sigma_2\bullet\sigma_3} - a_{\sigma_1,\sigma_2} = 0.$$

Es ist ein 2-Korand, falls von der Gestalt

$$a_{\sigma_1,\sigma_2} = \delta_2^*(b)(\sigma_1,\sigma_2) = \sigma_1 \bullet b_{\sigma_2} - b_{\sigma_1\bullet\sigma_2} + b_{\sigma_1}$$

mit einer 1-Kokette $b: G \longrightarrow A$.

3.2.4 Vergleich der Zusammenhangshomomorphismen

Unter Verwendung der obigen Beschreibung der Kohomologie-Gruppen mit Hilfe von Kozyklen erhält man auch eine explizite Beschreibung des Zusammenhangshomomorphismus

$$\delta^i: H^i(G, C) \longrightarrow H^{i+1}('G, A)$$

in der langen exakten Kohomologiesequenz. Insbesondere erhält man im Fall i=0 dieselbe Beschreibung wie in 2.6.1 :

Für $c \in C^G$ wähle man ein Urbild $b \in B$. Das Bild $\delta^0(c) \in H^1(G,A)$ von c ist dann gegeben durch die Abbildung

$$G \longrightarrow A, \sigma \mapsto \sigma(b) - b,$$

von der man leicht zeigen kann, daß es sich um einen 1-Kozyklus mit Werten in A handelt.

3.2.5 Normalisierte Koketten

Für einige Fragestellungen (zum Beispiel im Fall der unten behandelten Gruppen-Erweiterungen) ist es günstig mit sogenannten normalisierten Koketten zu arbeiten. Diese erhält man durch die Betrachtung der freien Auflösung

$$L_*: \quad \ldots \longrightarrow L_2 \xrightarrow{\delta_n^2} L_1 \xrightarrow{\delta_n^1} L_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

wobei

---

[93] Eine Funktion, die von 0 Argumenten aus G abhängt, ist als eine Konstante aus A anzusehen.

$$L_i \subseteq \mathbb{Z}[G^{i+1}]$$

der freie G-Teilmodul ist, der erzeugt wird von den Tupeln

$$[\sigma_1,...,\sigma_i] \text{ mit } \sigma_1,...,\sigma_i \neq e,$$

deren sämtliche Koordinaten vom neutralen Element von G verschieden ist. Die Korand-Operatoren δ^i_n sind durch dieselben Formeln definiert wie die δ^i in 3.2.2, wobei die Summanden

$$(-1)^j[\sigma_1,...,\sigma_j \bullet \sigma_{j+1},...,\sigma_i] \text{ mit } \sigma_j\sigma_{j+1} = e$$

wegzulassen sind. Man erhält auf diese Weise tatsächlich eine Abbildung

$$\delta^i_n: L_i \longrightarrow L_{i-1}$$

und eine Rechnung wie in 3.2.1 zeigt, es gilt[94]

$$\mathrm{Im}(\delta^{i+1}_n) = \mathrm{Ker}(\delta^i_n).$$

Wir erhalten also eine freie Auflösung und können diese zur Berechnung der Kohomologie-Gruppen $H^i(G,A)$ verwenden. Die Elemente von

$$\mathrm{Hom}_G(L_i, A)$$

kann man mit den inhomogenen i-Koketten

$$(a_{\sigma_1,...,\sigma_i})$$

identifizieren, die den Werten 0 haben, wenn eines der σ_j gleich e ist.

---

[94] L_i ist ein direkter Summand von $S_i := \mathbb{Z}[G^{i+1}]$ (da erzeugt vom Teil einer freien Basis), sagen wir

$$S_i = L_i \oplus L'_i,$$

wobei der komplementäre direkte Summand erzeugt wird von den $[\sigma_1,...,\sigma_i]$ mit mindestens einer Koordinate 1. In ursprünglicher (homogener) Schreibweise sind das diejenigen $(\sigma'_0,...,\sigma'_i)$, in denen zwei benachbarte Koordinaten übereinstimmen,

$$(\sigma'_0,...,\sigma'_i) = (..., \sigma, \sigma,...).$$

Beim Anwenden des Randoperators auf solche Erzeuger erhält lauter Summanden, die ebenfalls von dieser Gestalt sind (die beiden einzigen Summanden, bei denen das eventuell nicht der Fall ist, heben sich weg). Es gilt also

$$\delta^i(L'_i) \subseteq L'_{i-1}$$

Wir können also die

$$L_i = S_i/L'_i$$

mit Faktorgruppen der S_i identifizieren, und die Randoperatoren δ^i induzieren auf diese Weise gerade die δ^i_n. Insbesondere ist L_* ein Komplex (der Faktorkomplex von S_* modulo dem Teilkomplex L'_*), d.h. es gilt

$$\delta^{i-1}_n \circ \delta^i_n = 0.$$

Die Identität $\mathrm{Im}(\delta^{i+1}_n) = \mathrm{Ker}(\delta^i_n)$ beweist man nun in derselbe Weise wie die für die δ^i: man verwendet dieselbe Homotopie (mit $\sigma \neq 1$) und führt alle Betrachtungen modulo der L'_i durch (wodurch einige der auftretenden Summanden zusätzlich Null werden).

3.2.6 Beispiel: Gruppen-Erweiterungen

Ein wichtiges Gebiet, in welchem 2-Kozyklen in natürlicher Weise vorkommen, ist die Theorie der Gruppen-Erweiterungen. Eine Gruppen-Erweiterung ist eine exakte Sequenz

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

von Gruppen-Homomorphismen, wobei die Gruppe A abelsch sein soll. Man sagt in dieser Situation auch, E ist eine Erweiterung von G mit A.

Bemerkungen

(i) Die Gruppe A ist als Kern des Gruppen-Homomorphismus $E \longrightarrow G$ ein Normalteiler von E, d.h. E operiert durch Konjugation auf A,

$$E \times A \longrightarrow A,\ (x, a) \mapsto xax^{-1}\ .$$

Weil A eine abelsche Gruppe ist, operieren die Elemente aus derselben Rechtsnebenklasse modulo A in derselben Weise:

$$x = xa' \text{ mit } a' \in A \Rightarrow xax^{-1} = x'ax'^{-1}\ .$$

Wir erhalten so eine Operation von E/A = G auf A. Auf diese Weise wird die Gruppe A zum G-Modul.

(ii) Jeder Gruppen-Erweiterung

$$0 \longrightarrow A \longrightarrow E \xrightarrow{\pi} G \longrightarrow 1$$

kann man wie folgt einen 2-Kozyklus von G mit Werten in A zuordnen. Wir wählen einen normalisierten Schnitt

$$s: G \longrightarrow E$$

von π in der Kategorie der Mengen, d.h. eine Abbildung s mit

$$\pi \circ s = Id_G \text{ und } s(1) = 1.$$

Für je zwei Elemente $\sigma_1, \sigma_2 \in G$ setzen wir

$$a_{\sigma_1,\sigma_2} := s(\sigma_1) \bullet s(\sigma_2) \bullet s(\sigma_1 \bullet \sigma_2)^{-1} \in A.^{95}$$

Durch direktes Nachrechnen[96] sieht man, die Familie der a_{σ_1,σ_2} definiert einen 2-Kozyklus mit

$$a_{1,\sigma} = a_{\sigma,1} = 1 \text{ für jedes } \sigma \in G,$$

d.h. man erhält einen normalisierten 2-Kozyklus.

(iii) Ersetzt man den Schnitt s durch einen anderen normalisierten Schnitt, so zeigt eine weitere Rechnung, daß sich der zugehörige normalisierte 2-Kozyklus um einen 1-Korand abändert[97], d.h. die Kohomologie-Klasse

---

[95] Dieses Element liegt in A = Ker(π), weil π ein Gruppen-Homomorphismus ist.

[96] Man beachte, die Operation von G auf diesen Element erfolgt durch Konjugation mit Elementen aus E.

[97] Sei $s': G \longrightarrow E$ ein weiterer normalisierter Schnitt von π. Dann gilt

$$s'(\sigma) = s(\sigma) \bullet b_\sigma \text{ mit } b_\sigma \in A \text{ für jedes } \sigma \in G.$$

Der zugehörige 2-Kozyklus ist gegeben durch

$$a'_{\sigma_1,\sigma_2} := s(\sigma_1) b_{\sigma_1} s(\sigma_2) b_{\sigma_2} b^{-1}_{\sigma_1\sigma_2} s(\sigma_1\sigma_2)^{-1}$$

Damit ist

$$a'_{\sigma_1,\sigma_2} \bullet a^{-1}_{\sigma_1,\sigma_2} = s(\sigma_1) b_{\sigma_1} s(\sigma_2) b_{\sigma_2} b^{-1}_{\sigma_1\sigma_2} s(\sigma_2)^{-1} s(\sigma_1)^{-1}$$

Diese Identität in additiver Schreibweise bekommt die Gestalt (wenn wir beachten, daß G auf A durch angehobene Konjugation operiert).

$$c(E) \in H^2(G, A)$$

hängt nicht von der speziellen Wahl des Schnittes s ab (sondern nur von der Gruppen-Erweiterung).

(iv) Bezeichne

$$\mathrm{Ext}(G, A)$$

die Menge der Isomorphie-Klassen der Gruppen-Erweiterungen der Gruppe G bezüglich des G-Moduls A. Dabei werden zwei solche Erweiterungen

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

und

$$0 \longrightarrow A \longrightarrow E' \longrightarrow G \longrightarrow 1$$

als isomorph angesehen, wenn es einen Gruppen-Homomorphismus

$$\lambda: E \longrightarrow E'$$

gibt, für welchen das folgende Diagramm kommuativ ist.

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G \longrightarrow 1 \\ & & \| & & \downarrow\lambda & & \| \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G \longrightarrow 1 \end{array}$$

Man sieht sofort, daß dann λ ein Gruppen-Isomorphismus ist.

(v) Zu jedem normalisierten Schnitt von $E \longrightarrow G$ findet man mit Hilfe des Isomorphismus λ eine normalisierten Schnitt von $E' \longrightarrow G$, der denselben 2-Kozyklus definiert. Deshalb definieren isomorphe Erweiterungen dasselbe Element in der Kohomologie, d.h. man erhält eine Abbildung

$$\mathrm{Ext}(G, A) \longrightarrow H^2(G, A),\ E \mapsto c(E).$$

Durch einfache Rechnungen kann man zeigen, diese Abbildung ist bijektiv. Wir beschränken uns hier auf eine Beschreibung der inversen Abbildung.

(vi) Zu vorgegebenem $a \in H^2(G, A)$ wählen wir einen normalisierten 2-Kozyklus

$$(a_{\sigma_1,\sigma_2})$$

der diese Kohomologie-Klasse repräsentiert. Wir haben mit Hilfe dieses 2-Kozyklus eine Erweiterung E von G mit A zu konstruieren. Als zugrundeliegende Menge für E wählen wir

$$E = A \times G.$$

Die Multiplikation von E definieren wir durch die Formel

$$(a', \sigma)\bullet(a'', \sigma'') := (a' + \sigma'(a'') + a_{\sigma',\sigma''}, \sigma'\sigma'').$$

Die Kozyklen-Bedingung für die a_{σ_1,σ_2} übersetzt sich dann gerade in die Aussage, daß die so definierte Multiplikation assoziativ ist. Weil der Kozyklus normalisiert ist, ist das Paar

$$(0, 1)$$

ein neutrales Element bezüglich dieser Operation. Für jedes $(a, \sigma) \in E$ ist

$$(-\sigma^{-1}(a) - \sigma^{-1}(a_{\sigma,\sigma^{-1}}), \sigma^{-1})$$

$a'_{\sigma_1,\sigma_2} - a_{\sigma_1,\sigma_2} = \sigma_1\bullet(b_{\sigma_1} + \sigma_2\bullet(b_{\sigma_2} - b_{\sigma_1\sigma_2}))$

$= b'_{\sigma_1} + \sigma_2\bullet b'_{\sigma_2} - b'_{\sigma_1\sigma_2}$ (mit $b'_\sigma := \sigma\bullet b_\sigma$).

Mit anderen Worten (a_{σ_1,σ_2}) und (a'_{σ_1,σ_2}) unterscheiden sich um einen Korand.

zu (a, σ) invers. Die Menge E besitzt so die Struktur einer Gruppe. Die Sequenz

$$0 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

mit den in offensichtlicher Weise definierten Abbildungen ist eine Gruppen-Erweiterung. Ein direkte Rechnung zeigt,

$$c(E) = (a_{\sigma_1,\sigma_2}).$$

Für die Einzelheiten, siehe zum Beispiel Weibel [1], Section 6.6.

3.2.7 Direkte Bilder von Gruppen-Erweitungen und Kohomologie

Seien G eine Gruppe und Φ: A $\longrightarrow$ B ein G-Homomorphismus. Dann läßt sich die auf der Kohomologie induzierte Abbildung

$$\Phi_*: H^2(G, A) \longrightarrow H^2(G, B)$$

wie folgt mit Hilfe von Gruppen-Erweiterungen beschreiben. Die Klasse

$$c(E) \in H^2(G, A)$$

einer Erweiterung

$$0 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1$$

wird bei Φ_* abgebildet auf die Klasse des direkten Bildes oder auch des Pushforward

$$\Phi_*(E),$$

welches definiert ist als die Faktorgruppe von[98]

$$B \times E$$

nach dem Normalteiler

$$\{(\Phi(a), i(a)^{-1}) \mid a \in A\}.$$

Man erhält so eine Erweiterung

$$0 \longrightarrow B \xrightarrow{i'} \Phi_*(E) \xrightarrow{\pi'} G \longrightarrow 1$$

mit[99]

---

[98] B×E steht hier für das halbdirekte Produkt. Man beachte, E operiert auf Grund der Surjektion

$$E \longrightarrow G$$

auf dem G-Modul B. Genauer, das Produkt auf B×E ist durch die Formel

$$(b, e)\bullet(b', e') := (b\bullet e(b'), ee')$$

definiert. Es gilt damit

$$(b, e)^{-1} = (e^{-1}(b^{-1}), e^{-1})$$

und

$$(b, e)\bullet(b', e')(b, e)^{-1} = (b\bullet e(b')\bullet(ee'e^{-1})(b^{-1}), ee'e^{-1}).$$

Insbesondere für $(b',e') = (\Phi(a), i(a)^{-1})$ ist $ee'e^{-1} \in A = \mathrm{Ker}(E \longrightarrow G)$, d.h. $ee'e^{-1}$ operiert trivial auf B,

$$(b, e)\bullet(b', e')(b, e)^{-1} = (b\bullet e(b')\bullet b^{-1}, ee'e^{-1}) = (e(b'), ee'e^{-1}).$$

Das zweite Gleichheitszeichen gilt, weil B eine abelsche Gruppe ist. Nun ist A $\longrightarrow$ G ein G-Homomorphismus, d.h.

$$e(b') = e(\Phi(a)) = \Phi(e(a)).$$

Weil Konjugation mit e ein Homomorphismus ist, ist weiter

$$ee'e^{-1} = \sigma_e(i(a)^{-1}) = \sigma_e(i(a))^{-1} = i(\sigma_e(a))^{-1} = i(e(a))^{-1}.$$

Das letzte Gleichheitszeichen gilt, weil E auf A durch Konjugation operiert. Zusammen erhalten wir

$$(b, e)\bullet(\Phi(a), i(a)^{-1})\bullet(b, e)^{-1} = (\Phi(e(a)), i(e(a))^{-1}).$$

Mit anderen Worten, die angegebene Menge ist tatsächlich ein Normalteiler.

i'(b) := Restklasse von (b,1).
π'(Restklasse von (b,e)) := π(e).

Eine einfache Rechnung, welche die obige Beschreibung der Klasse c(E) verwendet, liefert[100]

$$c(\Phi_*(E)) = \Phi_*(c(E)).$$

Bemerkung
Für die Berechnung der Kohomologie spezieller Gruppen können sich weitere projektive Auflösungen als nützlich erweisen, wie das zum Beispiel für die zyklischen Gruppen der Fall ist.

3.2.8 Beispiel: die Kohomologie der Gruppe $\mathbb{Z}$

Sei G = $\mathbb{Z}$. Dann liefert die folgende Sequenz eine projektive Auflösung von $\mathbb{Z}$.

(1) $$0 \longrightarrow \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0$$

mit

$$T(x) := (\sigma\text{-}1)\bullet x \text{ und } \pi(\sum_i n_i\sigma^i) = \sum_i n_i.$$

Dabei bezeichne σ einen Erzeuger der zyklischen Gruppe G. Für jeden G-Modul A erhält man damit den Komplex

$$(\ 0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \xrightarrow{\pi^*})\mathrm{Hom}_G(\mathbb{Z}[G], A) \xrightarrow{\sigma\text{-}1} \mathrm{Hom}_G(\mathbb{Z}[G], A) \longrightarrow 0,$$

also

$H^0(\mathbb{Z}, A) = A^\sigma$
$H^1(\mathbb{Z}, A) = A/(\sigma\text{-}1)A$
$H^i(\mathbb{Z}, A) = 0$ für i > 1.

---

[99] i' ist injektiv, denn aus (b,1) = (Φ(a), i(a)$^{-1}$) folgt a = 0, also b = Φ(a) = 0. π' ist wohldefiniert, weil alle Elemente der Gestalt (Φ(a), i(a)$^{-1}$) im Kern von π liegen.

[100] Aus einem Schnitt

$$\sigma \mapsto s(\sigma)$$

zur Erweiterung E kann man leicht einen Scbnitt

$$\sigma \mapsto [(1, s(\sigma))]$$

zur Erweiterung Φ_*(E) gewinnenn. Die beiden zugehörigen 2-Kozyklen haben die Gestalt

$$a_{\sigma',\sigma''} = s(\sigma')s(\sigma'')s(\sigma',\sigma'')^{-1} \text{ bzw. } [(1,s(\sigma')s(\sigma'')s(\sigma',\sigma'')^{-1})] = [(1, a_{\sigma',\sigma''})] = [(\Phi(a), 1))]$$

Das letzte Gleichheitszeichen ergibt sich aus der Tatsache, daß in Φ_*(E) die Elemente der Gestalt

$$[(\Phi((a), i(a^{-1}))] = 1$$

gleich dem neutralen Element sind. Damit ist nämlich

$$\begin{aligned}[(\Phi(a), 1)]\bullet[(1, i(a))]^{-1} &= [(\Phi(a), 1)\bullet(1, i(a))^{-1}] \\ &= [(\Phi(a), 1)\bullet(1, i(a)^{-1})] \\ &= [(\Phi(a) , i(a)^{-1})] \\ &= 1\end{aligned}$$

zugehörigen 2-Kozyklus durch Komposition mit Φ: einem Element a$\in$A entspricht die Restklasse von (0,i(a)) in Φ_*(E), welche gleich der Restklasse von

$$i'(\Phi(a)) = (\Phi(a), 1)$$

ist.

Beweis der Exaktheit von (1).Der Kern von π besteht aus den Elementen

$$\sum_i n_i\sigma^i \text{ mit } \sum_i n_i = 0.$$

Das Bild von T besteht offensichtlich aus lauter solchen Elementen.
Sei ein beliebiges Element des Kerns von π gegeben. Es hat die Gestalt

$$\sum_i n_i\sigma^i = \sum_i n_i(\sigma^i - 1)$$

Es reicht zu zeigen, jedes Element der Gestalt

$$\sigma^i - 1$$

liegt im Bild von T, d.h. ist ein Vielfaches von σ-1. Für i =1 ist das trivial, für i > 0 gilt

$$\sigma^i - 1 = (\sigma-1)(\sigma^{i-1} + \sigma^{i-2} + ... + 1),$$

und für i < 0 erhalten wir

$$\sigma^i - 1 = (\sigma^{-1})^{|i|} - 1 = (\sigma^{-1}-1)((\sigma^{-1})^{|i|-1} + (\sigma^{-1})^{|i|-2} + ... + 1),$$
$$= -(\sigma-1)\sigma^{-1}((\sigma^{-1})^{|i|-1} + (\sigma^{-1})^{|i|-2} + ... + 1),$$

QED.

3.2.9 Beispiel: die Kohomologie der endlichen zyklischen Gruppen

Sei $G = \mathbb{Z}/n\mathbb{Z}$ die endliche zyklische Gruppe der Ordnung n mit dem Erzeuger $\sigma \in G$.
Wir betrachten die Abildungen

$$N: \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G] , x \mapsto \sum_{i=0}^{n-1} \sigma^i \bullet x,$$

und

$$T: \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G] , x \mapsto \sigma \bullet x - x.$$

Es gilt
(1) $$Ker(N) = Im(T)$$
und
(2) $$Im(N) = Ker(T).$$
Damit erhalten wir eine freie Auflösung

$$... \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

wobei die Augmentation alle Elemente von G in die 1 abbildet. Durch Anwenden des Funktors $Hom_G(? , A)$ erhalten wir den Komplex

$$(0 \longrightarrow A^\sigma \longrightarrow) A \xrightarrow{T} A \xrightarrow{N} A \xrightarrow{T} A \xrightarrow{N} ...$$

wobei N und T auf A durch dieselben Formeln definiert seien wie oben.[101] Mit

$$N^A := Ker(N)$$

erhalten wir

$$H^0(G, A) = A^G$$
$$H^{2i+1}(G, A) = {}_N A/(\sigma - 1)A \text{ für } i > 0.$$
$$H^{2i}(G, A) = A^G/N \bullet A. \quad \text{für } i > 0.$$

Beweis von (1) und (2).

---

[101] Die Multiplikation mit $\sum_{i=0}^{n-1} \sigma^i$ bzw. σ-1 geht beim Hom-Funktor in die Multiplikation mit $\sum_{i=0}^{n-1} \sigma^i$ bzw. σ-1 über.

Zu (2). Für $x = \sum_{g\in G} x_g \cdot g$ gilt

$$x \in \mathrm{Ker}(T) \Leftrightarrow 0 = \sum_{g\in G} x_g\cdot(\sigma-1)g = \sum_{g\in G} x_{\sigma^{-1}g}\, g - \sum_{g\in G} x_g g = \sum_{g\in G} (x_{\sigma^{-1}g} - x_g)\cdot g$$

$$\Leftrightarrow x_{\sigma^{-1}g} = x_g \text{ für jedes } g\in G$$

$$\Leftrightarrow x_g = x_e \text{ für jedes } g\in G$$

$$\Leftrightarrow x = x_e \cdot \sum_{g\in G} g = x_e \cdot N$$

$$\Leftrightarrow x \in N\bullet\mathbb{Z} =^{[102]} N\cdot\mathbb{Z}[G] = \mathrm{Im}(N).$$

Zu (1). Bezeichne

$$I_G := \mathrm{Ker}(\mathbb{Z}[G] \longrightarrow \mathbb{Z},\ \sum_{g\in G} x_g\cdot g \mapsto \sum_{g\in G} x_g)$$

$$= \{ \sum_{g\in G} x_g\cdot g \mid \sum_{g\in G} x_g = 0\}$$

$$= \{ \sum_{g\in G} x_g\cdot(g-1) \mid x_g \in \mathbb{Z}\}$$

das Augmentationsideal, d.h. den Kern der Augmentationsabbildung.[103]

Für $x = \sum_{g\in G} x_g\cdot g$ gilt

$$x \in \mathrm{Ker}(N) \Leftrightarrow 0 = N\cdot x = \sum_{g\in G} x_g N\cdot g = (\sum_{g\in G} x_g)\cdot N$$

$$\Leftrightarrow \sum_{g\in G} x_g = 0$$

$$\Leftrightarrow x = \sum_{g\in G} x_g\cdot g = \sum_{g\in G} x_g\cdot(g-1)$$

$$\Leftrightarrow^{[104]} x \in I_G$$

Wegen $\sigma-1\in I_G$ und weil I_G ein Ideal ist, gilt

$$\mathrm{Im}(T) \subseteq I_G.$$

Sei umgekehrt, $x \in I_G$. Wir haben noch zu zeigen, dann gilt

$$x \in \mathrm{Im}(T).$$

Wie wir gerade bemerkt haben, ist x von der Gestalt

---

[102] Die Multiplikation von N mit einem Element von G hat denselben Effekt wie die mit 1.

[103] Dies ist offensichtlich ein zweiseitiger G-Teilmodul von $\mathbb{Z}[G]$, d.h. ein Ideal.

[104] Liegt x in I_G, so ist x $\mathbb{Z}$-Linearkombination von Elementen der Gestalt g-1. Insbesondere ist die Summe der Koeffizienten x_g gleich Null.

$$x = \sum_{gPG} x_g \cdot (g-1).$$

Da die Multiplikation T eine $\mathbb{Z}$-lineare Abbildung ist, reicht es zu zeigen,

$$g-1 \in \mathrm{Im}(T) \text{ für jedes } g \in G.$$

Weil G zyklisch ist mit dem Erzeuger σ, hat g die Gestalt

$$g = \sigma^u \text{ mit } u \in \{0, \ldots, n-1\}.$$

O.B.d.A. sei u > 1. Dann gilt aber

$$g - 1 = (\sigma-1)(\sigma^{u-1}+\sigma^{u-2} + \ldots + 1) \in \mathrm{Im}(T)$$

QED.

3.2.10 Beispiel: der Satz 90 von Hilbert

Sei K/k eine zyklische Galois-Erweiterung mit der (endlichen) Gruppe $G = <\sigma>$. Dann gilt auf Grund der obigen Berechnungen

$$H^1(G, K^*) = {}_N K^*/(\sigma - 1)K^*.$$

Die linke Seite dieser Identität ist trivial nach dem Satz 90 von Hilbert (vgl. 2.3.8). Wir erhalten auf diese Weise den Satz 90 von Hilbert in seiner klassischen Formulierung zurück:

$Nc = \prod_{\sigma \in G} \sigma(c)$ = Norm des Elements $c \in K^*$ über k.

${}_N K^* = \{c \in K^* \mid N(c) = 1\}$

$(\sigma-1)K^* = \{\frac{\sigma(c)}{c} \mid c \in K^*\}$

3.3 Die Kohomologie von Untergruppen

3.3.1 Koinduzierte Moduln

Seien G eine Gruppe,

$$H \subseteq G$$

eine Untergruppe und

$$A$$

ein H-Modul. Dann ist $\mathbb{Z}[G]$ mit seiner natürlichen G-Operation auch ein H-Modul, d.h. wir können A wie folgt einen G-Modul zuordnen:

$$M_H^G(A) := \mathrm{Hom}_H(\mathbb{Z}[G], A).$$

Dabei sei die Operation von G auf diesen Modul wie folgt definiert.

$$(\sigma \bullet \phi)(x) =^{105} \phi(x\sigma) \text{ für } \sigma \in G \text{ und } \phi : \mathbb{Z}[G] \longrightarrow A \text{ aus } M_H^G(A) .$$

Der G-Modul $M_H^G(A)$ heißt der durch A <u>koinduzierte</u> G-Modul.

---

[105] Dies ist eine Links-Operation: für $\sigma, \tau \in G$ gilt

$$(\sigma\tau \bullet \phi)(x) = \phi(x \bullet \sigma \bullet \tau) = (\tau \bullet \phi)(x \bullet \sigma) = (\sigma \bullet (\tau \bullet \phi))(x),$$

d.h.

$$\sigma\tau \bullet \phi = \sigma \bullet (\tau \bullet \phi).$$

Die Definition der Operation ist gerade so gewählt, daß alle Elemente der Hom-Gruppe zu G-Homomorphismen werden, wenn man die Gruppe G durch ihr Dual G^{op} ersetzt (d.h. die Reihenfolge der Faktoren der Multiplikation umkehrt).

3.3.2 Eine natürliche Isomorphie

Seien G eine Gruppe, $H \subseteq G$ eine Untergruppe, M ein G-Modul und A ein H-Modul. Dann besteht eine natürliche Isomorphie

$$\mathrm{Hom}_G(M, \mathrm{Hom}_H(\mathbb{Z}[G], A) \xrightarrow{\cong} \mathrm{Hom}_H(M, A), \Phi \mapsto \Phi(?)(1).$$

Beweis. Konstruieren wir die Umkehrung. Sei

$$\lambda: M \longrightarrow A$$

ein H-Homomorphismus. Für jedes $m \in M$ sei λ_m die Abildung

$$\lambda_m: \mathbb{Z}[G] \longrightarrow A, x \mapsto \lambda(xm).$$

Mit λ ist auch λ_m ein H-Homomorphismus, d.h. wir erhalten eine Abbildung

$$\Phi: M \longrightarrow \mathrm{Hom}_H(\mathbb{Z}[G], A), m \mapsto \lambda_m .$$

Diese ist offensichtlich $\mathbb{Z}$-linear. Zeigen wir, es ist ein G-Homomorphismus. Für $\sigma \in 'G$, $m \in M$ und $x \in \mathbb{Z}[G]$ gilt

$$\begin{aligned}
(\sigma \bullet \Phi(m))(x) &= \Phi(m)(x\sigma) && \text{nach Definition der G-Operation von } M_H^G(A)\\
&= \lambda_m(x\sigma) && \text{nach Definiton von } \Phi\\
&= \lambda(x\sigma m) && \text{nach Definiton von } \lambda_m\\
&= \lambda_{\sigma m}(x) && \text{nach Definition von } \lambda_{\sigma m}
\end{aligned}$$

also

$$\sigma \bullet \Phi(m) = \lambda_{\sigma m} = \Phi(\sigma m).$$

Wir haben gezeigt

$$\Phi \in \mathrm{Hom}_G(M, \mathrm{Hom}_H(\mathbb{Z}[G], A).$$

Wir haben noch zu zeigen, die eben durch geführte Konstruktion liefert gerade die Umkehrabbildung zur oben gegebenen.

Nach Konstruktion gilt $\Phi(?)(1) = \lambda_?(1) = \lambda(?)$.

Umgekehrt ist im Fall $\lambda = \Phi(?)(1)$ die Abbildung λ_m gegeben durch

$$\begin{aligned}
x \mapsto \lambda(xm) &= \Phi(xm)(1)\\
&= x \bullet \Phi(m)(1) && \text{weil } \Phi \text{ ein G-Homomorphismus ist}\\
&= \Phi(m)(x) && \text{nach Definition der G-Operation von } M_H^G(A),
\end{aligned}$$

d.h. die Abbildung

$$m \mapsto \lambda_m(?) = \Phi(m)(?)$$

ist gerade die ursprünglich gegebene Abbildung Φ.

QED.

3.3.3 Lemma von Shapiro

Seien G eine Gruppe, $H \subseteq G$ eine Untergruppe und A ein H-Modul. Dann gilt

(1) $$H^i(G, M_H^G(A)) \cong H^i(H, A) \text{ für alle } i = 0.$$

Beweis. Sei

$$P_* \longrightarrow \mathbb{Z} \longrightarrow 0$$

eine freie Auflösung des trivialen G-Moduls $\mathbb{Z}$. Dies ist gleichzeitig eine freie Auflösung von $\mathbb{Z}$ als H-Modul. Wir wenden den Funktor $\mathrm{Hom}_H(\,?\,, A)$ an und erhalten nach 3.3.2:

$$\mathrm{Hom}_H(P_*, A) = \mathrm{Hom}_G(P_*, M_H^G(A)).$$

Die i-te Kohomologie des linken Komplexes ist gerade die rechte Seite von (1), die des rechten ist die linke Seite von (1).
QED.

Bemerkungen

(i) Die obige Aussage wurde unabhängig auch von Fadeev entdeckt. Ungerechterweise bleiben wir der Kürze halber bei der Benennung durch Shapiro.

(ii) Der Fall $H = \{1\}$ ist von besonderer Bedeutung. Wir schreiben dann auch

$$M^G(A) := M_H^G(A)$$

und nennen diesen Modul auch den zu A gehörigen <u>koinduzierten</u> Modul.

3.3.4 Die Kohomologie koinduzierter Moduln

Für jede Gruppe G und jede abelsche Gruppe A und jedes $i > 0$ gilt

$$H^i(G, M^G(A)) = 0.$$

Beweis. Die exakte Sequenz abelscher Gruppen

$$\ldots \longrightarrow 0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z} \longrightarrow 0$$

kann man als projektive Auflösung von $\mathbb{Z}$ über der trivialen Gruppe ansehen. Wir erhalten

$$H^i(\{1\}, A) = 0 \text{ für alle } i > 0.$$

Die Behauptung ergibt sich damit aus dem Lemma von Shapiro.
QED.

3.3.5 Eigenschaften der koinduzierten Moduln

(i) Die Konstruktion der koinduzierten Moduln ist funktoriell. Insbesondere induziert jeder Homomorphismus

$$A \longrightarrow B$$

von abelschen Gruppen einen G-Homomorphismus

$$M^G(A) \longrightarrow M^G(B)$$

Eine ähnliche Aussage gilt auch für die Moduln $M_H^G(A)$.

(ii) Für jeden G-Modul A ist die Abbildung

$$A \longrightarrow M^G(A),\ a \mapsto (\,x \mapsto xa),$$

ein injektiver G-Homomorphismus.[106]

(iii) Ist die Gruppe G endlich, so ist durch die Wahl einer $\mathbb{Z}$-Basis von $\mathbb{Z}[G]$ ein nicht-natürlicher Isomorphismus

$$M^G(A) \cong A \otimes_{\mathbb{Z}} \mathbb{Z}[G]$$

(für jede abelschen Gruppe A) festgelegt.[107]

---

[106] Bezeichnen wir mit λ_a die Abbildung $x \mapsto xa$. Dann ist $\sigma \bullet \lambda_a$ auf Grund der Definition der G-Modulstruktur von $M^G(A)$ die Abbildung mit

$$(\sigma \bullet \lambda_a)(x) = \lambda_a(x\sigma) = x\sigma a = \lambda_{\sigma a}(x),$$

d.h. die Injektion ist tatsächlich ein G-Homomorphismus.

[107] Genauer,

Bemerkung
Mit Hilfe des Lemmas von Shapiro werden wir jetzt zwei grundlegende Abbildungen kontruieren, die eine Zusammenhang zwischer Kohomologie einer Gruppe und der ihrer Untergruppen herstellt.

3.3.6 Konstruktion: die Restriktionsabbildung

Seien G eine Gruppe, A ein G-Modul und $H \subseteq G$ eine Untergruppe. Dann gibt es natürliche G-Homomorphismen

$$A \xrightarrow{\cong} \mathrm{Hom}_G(\mathbb{Z}[G], A) \longrightarrow \mathrm{Hom}_H(\mathbb{Z}[G], A) = M_H^G(A),.$$

$$a \mapsto \lambda_a : (x \mapsto xa), \qquad \lambda \mapsto \lambda.$$

Die linke Abbildung überführt das Modul-Element a in die Rechtsmultiplikation mit a (d.h. in den einzigen G-Homomorphismus, der 1 in a abbildet). Die Abbildung rechts daneben bildet jeden G-Homomorphismus in sich ab, aufgefaßt als H-Homomorphismus.
Aus diesen G-Homomorphismen erhält man durch Übergang zur Kohomologie und Anwenden des Lemmas von Shapiro für jedes i = 0 einen Gruppen-Homomorphismus

$$\mathrm{Res}: H^i(G, A) \longrightarrow H^i(H, A),$$

welcher Restriktion oder Restriktionsabbildung genannt wird.
Bemerkungen

(i) Für i = 0 erhält man gerade die natürliche Einbelttung[108] $A^G \longrightarrow A^H$.

(ii) Hat die Untergruppe H einen endlichen Index in G, so kann man wie folgt auch eine Abbildung in der umgekehrten Richtung kontruieren.

3.3.7 Konstruktion: die Korestriktionsabbildung

Seien G eine Gruppe, A ein G-Modul und $H \subseteq G$ eine Untergruppe mit endlichem Index.
Für jeden H-Homomorphismus

$$A \otimes_{\mathbb{Z}} \mathbb{Z}[G] \cong A \otimes_{\mathbb{Z}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$$

$$a \otimes \sum_i n_i \omega_i \quad \mapsto \quad a \otimes \sum_i n_i \omega_i^* \quad \mapsto \sum_i a n_i \omega_i^*$$

Dies ist ein G-Homomorphismus, wenn man die Gruppe G im Tensorfaktor links durch ihr Dual G^{op} ersetzt (d.h. das Produkt $x \bullet y$ als das Produkt $y \bullet x$ angesehen). Genauer ist also

$$M^G(A) \cong A \otimes_{\mathbb{Z}} \mathbb{Z}[G^{op}]$$

Dabei sei $\{\omega_i\}$ die gewählte Basis und $\{\omega_i^*\}$ die zugehörige duale Basis.

[108] Wir gehen zu den G-invarianten Teilen durch Anwenden des Funktors $\mathrm{Hom}_G(\mathbb{Z}, ?)$ über und erhalten

$$\mathrm{Hom}_G(\mathbb{Z}, A) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Hom}_G(\mathbb{Z}[G], A), f \mapsto (\, n \mapsto f(n) \mapsto \lambda_{f(n)} : x \mapsto xf(n)).$$

Nach 3.3.2 können wir den Modul rechts identifizieren mit $\mathrm{Hom}_H(\mathbb{Z},A)$, indem die Abbildungen dieses Moduls als Abbildungen in zwei Argumenten ansehen und diese im zweiten Argument auswerten. Die obige Abbildung bekommt dadurch die Gestalt

$$\mathrm{Hom}_G(\mathbb{Z}, A) \longrightarrow \mathrm{Hom}_H(\mathbb{Z},A), f \mapsto f.$$

Das ist aber gerade die natürliche Einbettung von A^G in A^H.

$$\Phi: \mathbb{Z}[G] \longrightarrow A$$

betrachten wir die Abbildung

$$\Phi_H^G: \mathbb{Z}[G] \longrightarrow A,\ x \mapsto \sum_{j=1}^{n} \rho_j \bullet \Phi(\rho_j^{-1} x).$$

Dabei seien die $\rho_1,...,\rho_n$ ein volles Repräsentanten-System der Restklassen von G modulo H. Diese Abbildung ist offensichtlich $\mathbb{Z}$-linear (d.h. ein Gruppen-Homomorphismus). Zeigen wir, er hängt nicht von der speziellen Wahl des Repräsentanten-Systems der ρ_j. Dazu wählen wir ein weiteres Repräsentanten-System, sagen wir $\rho'_1,...,\rho'_n$. Es gilt dann

$$\rho'_j = \rho_j h_j \text{ mit } h_j \in H.$$

Weil Φ ein H-Homomorphismus ist, gilt damit

$$\rho'_j \bullet \Phi(\rho'^{-1}_j x) = \rho_j \bullet \Phi(\rho_j^{-1} x),$$

d.h. die definierende Summe für Φ_H^G ändert sich nicht. Zeigen wir als nächstes, die Abbildung Φ_H^G ist sogar ein G-Homomorphismus. Für jedes $\sigma \in G$ gilt

$$\Phi_H^G(\sigma x) = \sum_{j=1}^{n} \rho_j \bullet \Phi(\rho_j^{-1} \sigma x) = \sigma\Big(\sum_{j=1}^{n} \sigma^{-1}\rho_j \bullet \Phi((\sigma\rho_j)^{-1} x)\Big) = \sigma(\Phi_H^G(x)).$$

Das letzte Gleichheitszeichen gilt, weil die $\sigma^{-1}\rho_j$ ein volles Repräsentanten-System von G modulo H bilden. Wir haben damit eine Abbildung

$$\mathrm{Hom}_H(\mathbb{Z}[G], A) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}[G], A) \cong A,\ \Phi \mapsto \Phi_H^G \mapsto \Phi_H^G(1),$$

definiert. Auf Grund der speziell gewählten G-Modul-Struktur der beiden Hom-Mengen (vgl. 3.3.1) ist dies sogar ein G-Modul-Homomorphismus. Wir gehen zur Kohomologie über, wenden das Lemma von Shapiro an und erhalten einen Gruppen-Homomorphismus

$$\mathrm{Cor}: H^i(H, A) \longrightarrow H^i(G, A),$$

welcher Korestriktion oder auch Korestriktionsabbildung heißt.

Bemerkung

Als direkte Folgerung aus den beiden obigen Konstruktionen erhalten wir die folgende Aussage zur Zusammensetzung der beiden konstruierten Abbildungen.

3.3.8 Die Zusammensetzung Cor∘Res

Seien G eine Gruppe, $H \subseteq G$ eine Untergruppe mit dem endliche Index n,

$$(G:H) = n,$$

und A ein G-Modul. Dann ist die Zusammensetzung

$$\mathrm{Cor} \circ \mathrm{Res}: H^i(G, A) \longrightarrow H^i(G,A)$$

für jedes $i \geq 0$ gerade die Multiplikation mit n.

Beweis. Restriktion und Korestriktion sind beide induziert durch Abbildungen der Koeffizienten-Moduln (wenn man vom Isomorphismus des Lemmas von Shapiro absieht). Ihre Zusammensetzung Cor∘Res ist dehalb induziert durch die folgende Abildung des Koeffizienten-Moduls A:

$$\begin{array}{ccccccc} (A =)\ \mathrm{Hom}_G(\mathbb{Z}[G], A) & \longrightarrow & \mathrm{Hom}_H(\mathbb{Z}[G], A) & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G], A)\ (= A) \\ \Phi & \mapsto & \Phi & \mapsto & \Phi_H^G \end{array}$$

Ist

$$\Phi: \mathbb{Z}[G] \longrightarrow A$$

ein G-Homomorphismus, so ist die Abbildung

$$\Phi_H^G: \mathbb{Z}[G] \longrightarrow A,\ x \mapsto \sum_{j=1}^{n} \rho_j \bullet \Phi(\rho_j^{-1} x) = \sum_{j=1}^{n} \Phi(x)$$

von 3.3.7 gerade das n-fache der Abbildung Φ.
QED.

3.3.9 Kohomologie-Gruppen endlicher Gruppen sind Torsionsgruppen

Seien G eine endliche Gruppe der Ordnung n und G ein A-Modul. Dann gilt

$$n \bullet H^i(G, A) = 0 \text{ für jedes } i > 0.$$

Insbesondere haben alle Elemente von $H^i(G, A)$ eine endliche Ordnung, welche die Zahl n teilt.
Beweis. Wir wenden 3.3.8 mit H = {1} an. Die Multiplikation mit n läßt sich demnach als Kompositon Cor∘Res schreiben, faktorisiert sich also über

$$H^i(\{1\}, A) = 0$$

QED.
Bemerkung
Eine weitere grundlegende Konsruktion ist die folgende.

3.3.10 Konstruktion: die Inflationsabbildung

Seien G eine Gruppe,

$$H \subseteq G$$

ein Normalteiler und A ein G-Modul. Der N-invariante Teil

$$A^H$$

besitzt dann in natürlicher Weise die Struktur eines G/H-Moduls,

$$G/H \times A^H \longrightarrow A^H,\ ([g], a) \mapsto ga,$$

denn je zwei Elemente g und g' = gh aus derselben Restklasse modulo N, operieren in derselben Weise auf den Elementen von A^H,

$$g'a = gha = ga \text{ für } a \in A^H \text{ und } h \in H.$$

Die Elemente ga liegen dabei wieder in A^H, weil H ein Normalteiler ist: für jedes h∈H kann man hg in der Gestalt

$$hg = gh' \text{ mit } h' \in H$$

schreiben, d.h. es ist hga = g'h'a = ga für jedes h∈H, d.h. ga ∈ A^H.

Wählen wir jetzt zwei projektive Auflösungen

$$P_* \longrightarrow \mathbb{Z} \longrightarrow 0 \text{ und } Q_* \longrightarrow \mathbb{Z} \longrightarrow 0,$$

wobei wir in der ersten $\mathbb{Z}$ als trivialen G-Modul und in der zweiten als trivialen G/H-Modul ansehen. Auf Grund der natürliche Surjektion G ⟶ G/H können wir die zweite Auflösung auch als Komplex von G-Moduln ansehen. Auf Grund des Vergleichssatzes 3.1.12 läßt sich der identische Homomorphismus

$$\mathrm{id}: \mathbb{Z} \longrightarrow \mathbb{Z}$$

fortsetzen zu einem Morphismus von G-Modul-Komplexen

$$P_* \longrightarrow Q_*.$$

Wir wenden den Funktor $\mathrm{Hom}_G(\ ?\ , A^H)$ an und erhalten einen Morphismus

$$\mathrm{Hom}_G(Q_*, A^H) \longrightarrow \mathrm{Hom}_G(P_*, A^H)$$

von Komplexen abelscher Gruppen. Nun sind die Q_i und A^H Moduln über G/H. Die G-Homomorphismen $Q_i \longrightarrow A^H$ sind deshalb automatisch auch G/H-Homomorphismen, d.h. es gilt $\mathrm{Hom}_G(Q_*, A^H) = \mathrm{Hom}_{G/H}(Q_*, A^H)$, und wir erhalten einen Komplex-Morphismus

$$\mathrm{Hom}_{G/H}(Q_*, A^H) \longrightarrow \mathrm{Hom}_G(P_*, A^H).$$

Dieser induziert für jedes i einen Homomorphismus der Kohomologie-Gruppen

(1) $$H^i(G/H, A^H) \longrightarrow H^i(G, A^H).$$

Dieser ist unabhängig von der speziellen Wahl der projektiven Auflösungen P_* und Q_* (auf Grund der Eindeutigkeitsaussage des Vergleichsatzes 3.1.12). Die natürliche Inklusion $A^H \hookrightarrow A$ induziert einen Homomorphismus $H^i(G, A^H) \longrightarrow H^i(G, A)$. Durch Zusammensetzen mit (1) erhalten wir für jedes $i \geq 0$ einen Homomorphismus

$$H^i(G/H, A^H) \longrightarrow H^i(G, A),$$

welcher Inflation oder Inflationsabbildung heißt.

3.3.11 Funktorialität bezüglich der Gruppe

(i) Sei $h: G \longrightarrow G'$ ein Gruppen-Homomorphismus. Dann definiert h einen Komplex-Morpjhismus der Standard-Auflösungen[109]

$$h_*: \mathbb{Z}[G^{*+1}] \longrightarrow \mathbb{Z}[G'^{*+1}], (\sigma_0, \ldots, \sigma_i) \mapsto (h(\sigma_0), \ldots, h(\sigma_i)).$$

Jeder G'-Modul A' ist vermittels h auch ein G-Modul und jeder G'-Homomorphismus ein G-Homomorphismus. Man erhält so einen Komplex-Morphismus

$$h^*: \mathrm{Hom}_{G'}(\mathbb{Z}[G'^{*+1}], A) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}[G^{*+1}], A), \varphi \mapsto \varphi \circ h_*,$$

und durch Anwenden des Kohomologie-Funktors einen Gruppen-Homomorphismus

$$H^i(G', A') \longrightarrow H^i(G, A'), [\sigma' \mapsto a_{\sigma'}] \mapsto [\sigma \mapsto a_{h(\sigma)}],$$

für jede i und jeden G'-Modul A'. Die Kohomologie-Gruppen werden so zu kontravariatnen Funktoren bezüglich der Gruppe,

$$(\text{Gruppen})^{op} \longrightarrow (\text{abelsche Gruppen}), G \mapsto H^i(G, A),$$

(ii) Für jede kurze exakte Sequenz von G'-Moduln

$$0 \longrightarrow A' \longrightarrow B' \longrightarrow C' \longrightarrow 0$$

hat man einen Morphismus von kurzen exakten Komplex-Sequenzen, d.h. ein kommuatives Diagramm von Komplex-Morphismen mit exakten Zeilen

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}[G'^{*+1}], A') & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}[G'^{*+1}], B') & \longrightarrow & \mathrm{Hom}_{G'}(\mathbb{Z}[G'^{*+1}], C') & \longrightarrow & 0 \\
 & & h^*\downarrow & & h^*\downarrow & & h^*\downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^{*+1}], A') & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^{*+1}], B') & \longrightarrow & \mathrm{Hom}_G(\mathbb{Z}[G^{*+1}], C') & \longrightarrow & 0
\end{array}$$

Aus diesem wiederum erhält man einen Morphismus der zugehörigen langen Kohomologie-Sequenzen

---

[109] Dies ist ein Komplex-Morphismus, das Anwenden von h_* und das Weglassen von Koordinaten kommutierende Operationen sind.

$$\begin{array}{ccccccccc} \ldots\longrightarrow & H^i(G',A') & \longrightarrow & H^i(G',B') & \longrightarrow & H^i(G',C') & \longrightarrow & H^{i+1}(G',A') & \longrightarrow\ldots \\ & \downarrow & & \downarrow & & \downarrow & & \downarrow & \\ \ldots\longrightarrow & H^i(G,A') & \longrightarrow & H^i(G,B') & \longrightarrow & H^i(G,C') & \longrightarrow & H^{i+1}(G,A') & \longrightarrow\ldots \end{array}$$

Beispiel 1: die Restriktion

Die Restriktionsabbildungen kommen von der Tatsache, daß man jede projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$ auch als projektive Auflösung über jeder Untergruppe $H \subseteq G$ ansehen kann[110], zum Beispiel die Standard-Auflösung,

$$\mathbb{Z}[G^{*+1}]$$

und von der natürlichen Einbettung von Komplexen

(1) $$\mathrm{Hom}_G(\mathbb{Z}[G^{*+1}], A) \longrightarrow \mathrm{Hom}_H(\mathbb{Z}[G^{*+1}], A), \quad \varphi \mapsto \varphi.$$

Die durch (1) induzierten Abbildungen auf den Kohomologie-Gruppen sind gerade Restriktionsabbildungen. Nun induziert die Einbettung $H \hookrightarrow G$ eine Einbettung der Standard-Auflösungen

$$\mathbb{Z}[H^{*+1}] \hookrightarrow \mathbb{Z}[G^{*+1}]$$

und damit einen Komplex-Morphismus

(2) $$\mathrm{Hom}_H(\mathbb{Z}[G^{*+1}], A) \longrightarrow \mathrm{Hom}_H(\mathbb{Z}[H^{*+1}], A), \varphi \mapsto \varphi|_H.$$

Die induzierten Abbildungen auf den Kohomologie-Gruppen sind gerade die identischen[111] Abbildungen (weil die Kohomologie nicht von der speziellen Wahl der projektiven Auflösung abhängt). Man kann die Restriktionsabbildungen also auch definieren als die durch (1) induzierten Abbildungen auf der Kohomologie zusammengesetzt mit den durch (2) induzierte Abbildungen. Mit anderen Worten,

$$\mathrm{Res}: H^i(G, A) \longrightarrow H^i(H, A),$$

kommt gerade dadurch zustande, daß man einen repräsentieren den i-Kozylus, der auf G^{i+1} definiert ist, einschränkt auf H^{i+1}.

Insbesondere zeigt diese Betrachtung auch, daß die Restriktionen mit den Zusammenhangshomomorphismen verträglich sind.

Beispiel 2: die Inflation

Sei $H \subseteq G$ ein Normalteiler der Gruppe G. Die natürliche Surjektion

$$\rho: G \longrightarrow G/H$$

induziert dann einen Komplex-Morphismus der Standard-Auflösungen

$$\mathbb{Z}[G^{*+1}] \longrightarrow \mathbb{Z}[G/H^{*+1}]$$

und damit Komplex-Morphismen

(3) $$\mathrm{Hom}_{G/H}(\mathbb{Z}[G/H^{*+1}], A') \longrightarrow \mathrm{Hom}_G(\mathbb{Z}[G^{*+1}], A'), \varphi \mapsto \varphi\circ\rho^{i+1},$$

für jeden G/H-Modul A'. Ist A ein G-Modul, so kann man $A' := A^H$ setzen, und die natürliche Einbettung $A^H \hookrightarrow A$ liefert dann zusmmen mit (3) einen Komplex-Morphismus

$$\mathrm{Hom}_{G/H}(\mathbb{Z}[G/H^{*+1}], A^H) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}[G^{*+1}], A), \varphi \mapsto \varphi\circ\rho^{i+1}.$$

Die induzierten Abbildungen auf den Kohomologie-Gruppen sind gerade die Inflationsabbildungen

$$H^i(G/H, A^H) \longrightarrow H^i(G, A).$$

---

[110] vgl. den Beweis des Lemmas von Shapiro 3.3.3.

[111] besser, identifizierenden Abbildungen.

Letztere kommen also gerade dadurch zustande, daß man einen i-Kozyklus

$$(G/H)^{i+1} \longrightarrow A^H$$

entlang der natürlichen Surjektion ρ verpflanzt zu einer Abbildung auf G^{i+1} und das Ergebnis als Abbildung mit Werten in A ansieht.

Insbesondere zeigt diese Betrachtung auch, daß die Infaltionen mit den Zusammenhangshomomorphismen verträglich sind.

3.3.12. Beschreibung der Inflation im Grad 2 durch Erweiterungen

Seien G eine Gruppe, $H \subseteq G$ ein Normalteiler und A ein G-Modul. Die Inflation

$$\text{Inf: } H^2(G/H, A^H) \longrightarrow H^2(G, A)$$

läßt sich dann mit Hilfe der Erweiterungen von Gruppen wie folgt beschreiben. Die Klasse

$$c(E) \in H^2(G/H, A^H)$$

einer Erweiterung

$$0 \longrightarrow A^H \xrightarrow{i} E \xrightarrow{\pi} (G/H) \longrightarrow 1$$

hat als Bild bei Inf die Klasse des (direkten Bildes bezüglich $j: A^H \hookrightarrow A$ des) <u>inversen Bilds</u> ρ^*E oder auch <u>Pullbacks</u> von E entlang dem natürlichen Homomorphismus ρ: $G/H \longrightarrow G$,

(1) $$\text{Inf } c(E)) = c(j_*\rho^*E).$$

Dabei ist ρ^*E definiert als die folgende Untergruppe des direkten Produkts $E \times G$:

$$\rho^*E := \{(e,g) \in E \times G \mid \pi(e) = \rho(g)\}$$

Man beachte, man hat tatsächlich eine Erweiterung

$$0 \longrightarrow A^H \xrightarrow{i'} \rho^*E \xrightarrow{\pi'} G \longrightarrow 1$$

mit $i'(a) = (i(a), 1)$ und $\pi'([e,g]) = g$. Die Abbildung π' ist surjektiv, weil π es ist. Die Abbildung i' ist injektiv, weil i es ist. Weiter ist

$$\text{Ker } \pi' = \{(e,1) \mid e \in E, \pi(e) = 1\} = \text{Ker}(\pi) \times 1 = A^H \times 1 = \text{Im}(i').$$

Die Identität (1) ergibt sich aus der Beschreibung der Inflation in 3.3.11 und aus der Beschreibung der Klasse c(E) einer Erweiterung E in 3.2.6 und 3.2.7.[112]

Bemerkung

Wir wenden uns jetzt der letzten grundlegenden Konstruktion im Zusammenhang mit Untergruppen zu.

---

[112] Ein Schnitt $s: G/H \longrightarrow E$ von π liefert eine Schnitt

$$s': G \longrightarrow \rho^*E,\ g \mapsto (s(\rho(g)), g)$$

von π'. Der zugehörige 2-Kozyklus ist

$$a'_{\sigma,\sigma'} = s(\sigma)s(\sigma')s(\sigma\sigma')^{-1} = (a_{\rho(\sigma),\rho(\sigma')}, 1)$$

ist gerade die Verpflanzung des zu s gehörigen 2-Kozyklus $a_{\sigma,\sigma'}$ entlang

$$\rho \times \rho: G \times G \longrightarrow (G/H) \times (G/H).$$

Als Produkt in ρ^*E nimmt man hier das vom direkten Produkt in $E \times G$ kommende (nicht das halbdirekte Produkt).

3.3.13 Konstruktion: Konjugation

Seien G eine Gruppe, $H \subseteq G$ ein Normalteiler und P und A seien G-Moduln. Für jedes $\sigma \in G$ betrachten wir die Abbildung

$$\sigma_*: \mathrm{Hom}_H(P, A) \longrightarrow \mathrm{Hom}_H(P, A), \phi \mapsto (p \mapsto \sigma \circ \phi \circ \sigma^{-1}),$$

welche jedem H-Homomorphismus dessen σ-Konjugiertes zuordnet. Zeigen wir, diese Abbildung ist wohldefiniert, d.h. $\sigma_*(\phi)$ ist wieder ein H-Homomorphismus. Für $p \in P$ und $h \in H$ gilt

$$\begin{aligned}
\sigma_*(\phi)(hp) &= (\sigma \circ \phi \circ \sigma^{-1})(hp) && \text{nach Definiton von } \sigma_* \\
&= \sigma\phi(\sigma^{-1}hp) \\
&= \sigma\phi(\sigma^{-1}h\sigma\sigma^{-1}p) && \text{wegen } \sigma^{-1}\sigma = 1 \\
&= \sigma\sigma^{-1}h\sigma\phi(\sigma^{-1}p) && \text{weil } \phi \text{ ein H-Homomorphismus ist} \\
&= h\sigma\phi(\sigma^{-1}p) \\
&= h\sigma_*(\phi)(p).
\end{aligned}$$

Da $(\sigma^{-1})_*$ die zu σ_* inverse Abbildung ist, ist σ_* ein Automorphismus von

$$\mathrm{Hom}_H(P,A).$$

Für $\sigma \in H$ ist σ_* die identische Abbildung: denn es ist $\sigma^{-1} \circ \phi \circ \sigma = \phi$ für H-Homomorphismen ϕ.

Wir wenden diese Konstruktion jetzt auf die G-Moduln P einer projektiven Auflösung

$$P_* \longrightarrow \mathbb{Z} \longrightarrow 0$$

des trivialen G-Moduls $\mathbb{Z}$ an. Man beachte, diese ist gleichzeitig eine projektive Auflösung, wenn man $\mathbb{Z}$ als H-Modul betrachtet, denn $\mathbb{Z}[G]$ ist ein freier Modul über $\mathbb{Z}[H]$,

$$\mathbb{Z}[G] = \oplus_{g \in G/H} \mathbb{Z}[H],$$

d.h. jeder freie $\mathbb{Z}[G]$-Modul ist auch frei über $\mathbb{Z}[H]$. Wir wenden den Funktor $\mathrm{Hom}_H(?, A)$ an und erhalten den Komplex

$$(0 \longrightarrow A^H \longrightarrow) \mathrm{Hom}_H(P_*, A).$$

Die obige Konstruktion liefert einen Komplex-Morphismus σ_* (d.h. einen Automorphismus in jedem Grad, wobei die Abbildung mit den Korand-Operatoren des Komplexes verträglich sind)[113]. Durch Übergang zur Kohomolgie erhalten wir für jedes $i = 0$ Automorphismen

$$\sigma_*: H^i(H, A) \longrightarrow H^i(H, A).$$

Auf Grund des Vergleichssatzes 3.1.12 hängen diese Automorphismen nicht von der speziellen Wahl der projektiven Auflösung ab. Im Fall $\sigma \in H$ sind diese

---

[113] Die Komposition mit den Randoperatoren ∂ von P_*, welche G-Homomorphismen sind, kommutiert mit dem Anwenden von σ_*°:

$$\delta(\sigma_*(\alpha)) = \delta(\sigma\alpha\sigma^{-1}) = \sigma\alpha\sigma^{-1}\partial = \sigma\alpha\partial\sigma^{-1} = \sigma_*(\alpha\partial) = \sigma_*(\delta(\alpha)).$$

Automorphismen trivial. Die Operation ist damit sogar eine Operation von G/H auf den Kohomologie-Gruppen,

$$G/H \times H^i(H, A) \longrightarrow H^i(G, A),$$

Sie heißt Operation durch Konjugation .

3.3.14 Die Kohomologie-Sequenz als G/H-Modul-Sequenz

Seien G eine Gruppe, $H \subseteq G$ ein Normalteiler und

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

eine kurze exakte Sequenz von G-Moduln. Dann ist die lange exakte Kohomologie-Sequenz für H,

$$0 \longrightarrow H^0(H, A) \longrightarrow ... \longrightarrow H^{i-1}(H,C) \longrightarrow H^i(H,A) \longrightarrow H^i(H,B) \longrightarrow H^i(H,C) \longrightarrow ...$$

eine Sequenz von G/H-Homomorphismen, wenn man die Kohomologie-Gruppen mit der Operation durch Konjugation versieht.

Beweis. Das folgt unmittelbar aus der Tatsache, daß die in 3.3.13 definierte Konjugation Isomorphismen der exakten Komplex-Sequenzen

$$0 \longrightarrow \mathrm{Hom}_H(P_*, A) \xrightarrow{\alpha_*} \mathrm{Hom}_H(P_*, B) \xrightarrow{\beta_*} \mathrm{Hom}_H(P_*, C) \longrightarrow 0$$

induzieren.[114]

QED.

3.3.15 Die exakte Inf-Res-Sequenz

Seien G eine Gruppe, $H \subseteq G$ ein Normalteiler und A ein G-Modul. Dann gibt es eine exakte Sequenz

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(H, A)^{G/H} \longrightarrow H^2(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^2(G,A)$$

Zum Beweis benötigen wir eine Vorbereitungen.

3.3.16 Eigenschaften koinduzierter Moduln.

Seien G eine Gruppe, $H \subseteq G$ ein Normalteiler und A ein G-Modul. Dann gilt

$$M^G(A)^H \cong M^{G/H}(A)$$

und

$$H^j(H, M^G(A)) = 0 \text{ für alle } j > 0.$$

Beweis. Es gilt

$$M^G(A)^H = \mathrm{Hom}(\mathbb{Z}[G], A)^H \quad \text{(nach Definiton von } M^G(A))$$
$$\cong^{115} \{f:G \longrightarrow A \mid f(gh) = f(g) \text{ für } g \in G, h \in H\}$$

---

[114] (vgl. die letzte Fußnote). Weil die Abbildungen von

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

G-Homomorphismen sind, kommutiert die Operation durch Konjugation auf den Komplexen mit den induzierten Komplex-Morphismen. Für $f: P_i \longrightarrow A$ aus dem Definitionsbereich von α_* und $\sigma \in G$, $p \in P_i$ gilt zum Beispiel:

$$\alpha \circ \sigma_*(f)(p) = \alpha(\sigma^{-1} f \sigma(p)) = \sigma^{-1} \alpha(f\sigma(p)) = \sigma_*(\alpha \circ f)(p),$$

d.h. es ist $\alpha \circ \sigma_*(f) = \sigma_*(\alpha \circ f)$, d.h. $\alpha_* \circ \sigma_* = \sigma_* \circ \alpha_*$.

[115] Die Elemente von G bilden eine freie Basis von $\mathbb{Z}[G]$ über $\mathbb{Z}$.

$$\cong^{116} \{f: G/H \longrightarrow A\}$$
$$\cong \mathrm{Hom}(\mathbb{Z}[G/H], A)$$
$$= M^{G/H}(A) \qquad \text{(nach Definiton von } M^{G/H}(A)).$$

Damit ist die erste Isomorphie bewiesen. Beweisen wir die zweite. Sei

$$\{g_i\}_{i\in I}$$

ein volles Repräsentantensystem von G/H in G. Betrachten wir die Zerlegung

$$G = \bigcup_{i\in I} g_i H$$

in paarweise disjunkte Teilmengen. Diese definiert eine direkte Summenzerlegung (von $\mathbb{Z}$-Moduln)

$$\mathbb{Z}[G] = \oplus_{i\in I}\, g_i\mathbb{Z}[H].$$

Wir wenden den Funktor Hom(? ,A) an und erhalten

$$\mathrm{Hom}(\mathbb{Z}[G] , A) = \mathrm{Hom}(\oplus_{i\in I}\, g_i\mathbb{Z}[H], A) =^{117} \times_{i\in I} \mathrm{Hom}(\mathbb{Z}[H] , A),$$

d.h.

$$M^G(A) = \times_{i\in I}\, M^H(A) \text{ als H-Moduln.}$$

Ist P_* eine projektive Auflösung des trivialen H-Moduls $\mathbb{Z}$, so folgt

$$\mathrm{Hom}_H(P_*, M^G(A)) = \mathrm{Hom}_H(P_*, \times_{i\in I} M^H(A))$$
$$=^{118} \times_{i\in I}\, \mathrm{Hom}_H(P_*, M^H(A))$$

Wir gehen zur Kohomolgie über und erhalten

$$H^i(H, M^G(A)) = \times_{i\in I}\, H^i(H, M^H(A)) = 0.$$

QED.

3.3.17 Beweis von 3.3.15

Wir betrachten die natürliche Einbettung von A in $M^G(A)$ von 3.3.5(ii) und bezeichnen mit C den Kokern dieser Einbettung. Die kurze exakte Sequenz von G-Moduln

(1) $$0 \longrightarrow A \longrightarrow M^G(A) \longrightarrow C \longrightarrow 0$$

ist auch eine Sequenz von H-Moduln, d.h. wir erhalten eine exakte Sequenz

$$0 \longrightarrow A^H \longrightarrow M^G(A)^H \longrightarrow C^H \xrightarrow{\partial} H^1(H, A) \longrightarrow H^1(H, M^G(A)).$$

Die letzte Kohomologie-Gruppe rechts ist trivial nach 3.3.16. Die Sequenz zerfällt deshalb in die zwei folgenden kurzen exakten Sequenzen,

(2) $$0 \longrightarrow A^H \longrightarrow M^G(A)^H \longrightarrow B \longrightarrow 0$$

(3) $$0 \longrightarrow B \longrightarrow C^H \xrightarrow{\partial} H^1(H, A) \longrightarrow 0,$$

wobei B das Bild von $M^G(A)^H$ in C^H bezeichnet.
Nach 3.3.14 sind dies Sequenzen von G/H-Moduln. Wir gehen von (2) zur zugehörigen langen Kohomologie-Sequenz über G/H über und erhalten eine exakte Sequenz

---

[116] Wegen f(gh) = f(g) für alle h ist f auf jeder Linksnebenklasse modulo H konstant.

[117] Jede durch I indizierte Familie von Gruppen-Homomorphismen $\mathbb{Z}[H] \longrightarrow A$ definiert einen Homomorphismus auf der direkten Summe. Umgekehrt erhält man durch Einschränken aus jedem Homomorphismus auf der direkten Summe eine solche Familie.

[118] Ein Element der linken Hom-Menge ist eine Abbildung, die durch ihre Koordinaten-Funktionen vollständig festgelegt ist. Und diese Koordinaten-Funktionen können beliebig vorgegebene H-Homomorphismen sein.

(4) $0 \longrightarrow A^G \longrightarrow M^G(A)^G \longrightarrow B^{G/H} \xrightarrow{\partial} H^1(G/H,A^H) \longrightarrow H^1(G/H, M^G(A)^H).$

Nach Lemma 3.3.16 ist $M^G(A)^H = M^{G/H}(A)$ koinduziert über G/H, d.h. die Gruppe ganz rechts ist trivial. Damit erhalten wir das folgende kommutative Diagramm mit exakten Zeilen.

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & A^G & \longrightarrow & M^G(A)^G & \longrightarrow & B^{G/H} & \xrightarrow{\partial} & H^1(G/H,A^H) \longrightarrow 0 \\
 & & \downarrow \mathrm{Id} & & \downarrow \mathrm{Id} & & \downarrow & & \\
0 & \longrightarrow & A^G & \longrightarrow & M^G(A)^G & \longrightarrow & C^G & \xrightarrow{\partial} & H^1(G,A) \longrightarrow 0 \\
 & & & & & & \partial|_{C^G}\downarrow & & \\
 & & & & & & H^1(H,A)^{G/H} & & \\
 & & & & & & \downarrow & & \\
 & & & & & & H^1(G/H,B) & &
\end{array}$$

Die erste Zeile ist die gerade betrachtete Sequenz (4), d.h. die Kohomologie-Sequenz zu (2). Die zweite Zeile ist die Kohomologie-Sequenz zu (1)[119].

Die Spalte ist die lange Kohomologie-Sequenz zu (3) über G/H. Eine Diagramm-Jagt liefert eine exakte Sequenz[120]

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\alpha} H^1(G,A) \xrightarrow{\beta} H^1(H,A)^{G/H} \longrightarrow H^1(G/H, B)$$

Wir haben zu zeigen, α ist die Inflation und β ist die Restriktion.

---

[119] Die vertikalen Abbildungen zwischen erster und zweiter Zeile kommen also gerade von der Einbettung der Sequenz (2) in die Sequenz (1).

[120] Schreiben wir das Diagramm in der Gestalt

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & 0 \\
 & & & & & & \downarrow & & \downarrow \\
0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & D \longrightarrow 0 \\
 & & \| & & \| & & \downarrow & & \downarrow \\
0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & D' \longrightarrow 0 \\
 & & & & & & \downarrow \swarrow & & \\
 & & & & & & E & & \\
 & & & & & & \downarrow & & \\
 & & & & & & F & &
\end{array}$$

Die zusätzlich eingefügten Pfeile sind durch die Kommutativität der entsprechenden Teile des Diagramms definiert. Ihre Existenz ergibt sich aus dem Homomorphie-Satz. Weiter gilt

$D \cong C/\mathrm{Im}(B)$

$D' \cong C'/\mathrm{Im}(B)$

also

$\mathrm{Im}(C' \longrightarrow E) \cong C'/C \cong (C'/\mathrm{Im}(B))/(C/\mathrm{Im}(B)) \cong D'/D.$

Insbesondere ist die Sequenz

$$0 \longrightarrow D \longrightarrow D' \longrightarrow E \longrightarrow F$$

exakt.

Für α ergibt sich das daraus, daß man A^H imd B als G-Moduln ansieht vermittels der natürlichen Surjektion $G \longrightarrow G/H$ und das folgende kommutative Diagramm betrachtet.[121]

$$\begin{array}{ccccc} B^{G/H} & = & B^G & \longrightarrow & C^G \\ \partial\downarrow & & \partial\downarrow & & \partial\downarrow \\ H^1(G/H,A^H) & \xrightarrow{\lambda} & H^1(G,A^H) & \longrightarrow & H^1(G,A) \end{array}$$

Die vertikalen Abbildungen sind dabei gerade Zusammenhangshomomorphismen zu kurzen exakten Sequenzen von Koeffizientengruppen.[122] Die linken horizontalen Homomorphismus kommen von Funktorialität der Kohomologie bezüglich des ersten Arguments, die rechten von der bezüglich des zweiten. Insbesondere ist die untere Zeile gerade die Inflation (und λ kommt von der Verpflanzung von Kozyklen entlang der natürlichen Surjektion $G \longrightarrow G/H$.

Die Beschreibung von β als Restriktonsabbildung ergibt sich in analoger Weise aus der Kommutativität des folgenden Diagramms.

$$\begin{array}{ccc} C^G & \xrightarrow{\partial} & H^1(G,A) \\ \downarrow & & \downarrow \mathrm{Res} \\ C^H & \xrightarrow{\partial} & H^1(H,A) \end{array}$$

Die horizontalen Abbildungen sind Zusammenhangshomomorphismen zur kurzen exakten Sequenz (1) über G bzw. H und die vertikalen gerade die Restriktionen. Die linke vertikale Abbildung ist insbesondere gerade die natürliche Einbettung.

Der verbleigende Teil der gesuchten exakten Sequenz kommt nun vom kommutativen Diagramm

$$\begin{array}{ccccccc} H^1(H,A)^{G/H} & \longrightarrow & H^1(G/H,B) & \xrightarrow{\gamma} & H^1(G/H,C^H) & \xrightarrow{\mathrm{Inf}} & H^1(G,C) \\ & & \partial\downarrow\cong & & & & \partial\downarrow\cong \\ & & H^2(G/H,A^H) & & \xrightarrow{\mathrm{Inf}} & & H^2(G,A) \end{array}$$

Die obere Zeile ohne die Inflation ganz rechts kommt dabei von der Sequenz (3) und ist deshalb exakt an der Stelle $H^1(G/H, B)$. Das ändet sich auch nicht, wenn man γ durch die Zusammensetzung mit der (injektiven) Inflation ersetzt.

Die vertikalen Isomorphismen sind Zusammenhangshomomorphismen zu den exakten Sequenzen (2) und (1). Ihre Bijektivität ergibt sich aus der Tatsache daß die Moduln $M^G(A)^H =^{123} M^{G/H}(A)$ und $M^G(A)$ triviale Kohomologie (über G/H bzw. G) besitzen. Die Kommutativität des Vierecks ist im wesentlichen eine Folge der Funktorialität der Kohomologie ihrer beiden Argumente.

Genauer, man hat ein kommutatives Diagramm mit den exakte Zeilen (1) und (2),

---

[121] Es kommt von der Einbettung der folgenden Sequenzen ineinander und den folgenden Gruppen-Homomorphismen.

$$\begin{array}{ccccc} (2) & = & (2) & \subseteq & (1) \\ G/H & \longleftarrow & G & = & G \end{array}$$

wobei man die linke Sequenz (2) über G/H und die mittlere über G betrachtet.

[122] Die beiden äußeren kommen in den Zeilen des vorigen Diagramms vor, der in der Mitte gehört zu (2).

[123] nach 3.3.16.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & M^G(A) & \longrightarrow & C & \longrightarrow & 0 \\ & & \cup & & \cup & & \uparrow & & \\ 0 & \longrightarrow & A^H & \longrightarrow & M^G(A)^H & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

also ein kommutatives Diagramm[124]

$$\begin{array}{ccccc} H^1(G/H,B) & \longrightarrow & H^1(G,B) & \longrightarrow & H^1(G,C) \\ \partial\downarrow & & \partial\downarrow & & \partial\downarrow \\ H^2(G/H,A^H) & \longrightarrow & H^2(G,A^H) & \longrightarrow & H^2(G,A) \end{array}$$

dessen vertiale Abbildungen Zusammenhangshomomorphismen sind, dessen linke horizontale Abbildungen von der Funktorialität der Kohomologie bezüglich des ersten Arguments kommen und dessen linke horizontale Abbildungen von entsprechenden Abbildungen der Koeffizienten-Moduln. Die Zusammensetzung der unteren horizontalen Abbildungen ist gerade eine Inflationsabbildung. Die Zusammensetzung der oberen ist Zusammensetzung einer Inflation mit einer durch $B \longrightarrow C^H$ induzierten Abbildung (nämlich γ). Bei einem Wechsel der Gruppen und Koeffizienten kommt es nicht auf die Reihenfolge an.

3.3.18 Die exakte Inf-Res-Sequenz für höhere Dimensionen

Seien G eine Gruppe, $H \subseteq G$ ein Normalteiler und A ein G-Modul. Weiter sei $i > 1$ eine natürliche Zahl mit der Eigenschaft, daß die Gruppen

$$H^j(H, A) = 0 \text{ für } j = 1, 2, \dots, i-1$$

trivial sind. Dann gibt es einen natürlichen Homomorphismus

$$\rho_{i,A}: H^i(H, A)^{G/H} \longrightarrow H^{i+1}(G/H, A^H),$$

welcher Bestandteil der folgenden exakten Sequenz ist

$$0 \longrightarrow H^i(G/H, A^H) \xrightarrow{Inf} H^i(G,A) \xrightarrow{Res} H^i(H, A)^{G/H} \longrightarrow H^{i+1}(G/H, A^H) \xrightarrow{Inf} H^{i+1}(G,A).$$

Beweis. Für i = 1 ist das die Aussage von 3.3.15. Wir beweisen die Aussage durch Induktion nach i. Sei also $i > 1$.

Wir betten A in den koinduzierten Modul $M^G(A)$ ein und betrachten die zugehörige kurze exakte Sequen

(1) $$0 \longrightarrow A \longrightarrow M^G(A) \longrightarrow C_A \longrightarrow 0.$$

Dies ist insbesondere eine Sequenz von H-Moduln. Wegen $H^1(H, A) = 0$ ist auch die folgende Sequenz exakt:

$$0 \longrightarrow A^H \longrightarrow M^G(A)^H \longrightarrow C_A^H \longrightarrow 0.$$

Dies ist eine kurze exakte Sequenz von G/H-Moduln. Übergang zur langen Kohomologie-Sequenz liefert die erste und die vierte vertikale Abbildung im folgenden kommutativen Diagramm (mit $1 < j = i$).

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^{j-1}(G/H,C_A^H) & \xrightarrow{Inf} & H^{j-1}(G,C_A) & \xrightarrow{Res} & H^{j-1}(H,C_A)^{G/H} & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^j(G/H,A^H) & \xrightarrow{Inf} & H^j(G,A) & \xrightarrow{Res} & H^j(H,A)^{G/H} & \longrightarrow & \dots \end{array}$$

---

[124] Es kommt von der Einbettung der folgenden Sequenzen ineinander und den folgenden Gruppen-Homomorphismen.

$$\begin{array}{ccccc} (2) & = & (2) & \subseteq & (1) \\ G/H & \longleftarrow & G & = & G \end{array}$$

$$\begin{array}{ccccc} & \xrightarrow{\rho_{j-1,C}} & H^j(G/H, C_A^H) & \xrightarrow{\text{Inf}} & H^j(G, C_A) \\ & & \downarrow & & \downarrow \\ & \xrightarrow{\rho_{j,A}} & H^{j+1}(G/H, A^H) & \xrightarrow{\text{Inf}} & H^{j+1}(G, A) \end{array}$$

Die anderen vertikalen Abbildungen des Diagramms sind Zusammenhangshomomorphismen zur Sequenz (1) (bzw. Einschränkungen dieser Zusmmenhangshomomorphismen) über G und über H. Die Abbildungen

$$\rho_{j,A} \text{ und } \rho_{j-1,C} := \rho_{j-1,C_A}$$

sind noch zu definieren. Die zweite, dritte und die letzte vertikale Abbildung sind bijektiv weil $M^G(A)$ kohomologisch trivial ist über G und über H(vgl. 3.3.4 und 3.3.16). Die erste und vorletzte vertikale Abbildung sind bijektiv, weil $M^G(A)^H =^{125} M^{G/H}(A)$ kohomologisch trivial ist über G/H. Also sind alle vertikalen Abbildungen Isomorphismen.
Für die dritte vertikale Abbildung gilt das auch, wenn man nicht zu den G/H-invarianten Teilen übergeht, d.h. es ist

$$H^j(H, C_A) = H^{j+1}(H,A) = 0 \text{ für } j = 1,..., i-2.$$

Mit anderen Worten, C_A genügt den Bedingungen der Induktionsvoraussetzung. In der oberen Zeile läßt sich also ein natürlicher Homomorphismus ρ so einfügen, daß die Zeile exakt wird.

Jedes Viereck des Diagramms, dessen horizontale Abbildungen definiert sind, ist kommuativ, da Inflation und Restriktion mit Zusammenhangshomomorphismen verträglich sind.
Da alle vertikalen Abbildungen Isomorphismen sind, läßt sich die untere mit der oberen Zeile identifizieren, d.h. auch in der unteren Zeile läßt sich ein natürlicher Homomorphismus so einfügen, daß die Zeile exakt wird.
QED.

3.3.19 Bemerkungen zum Beweis der beiden letzten Aussagen

(i) Die letzte Aussage ergibt sich unmittelbar aus der Hochschild-Serre-Spektralsequenz für Gruppen-Erweiterungen (siehe zum Beispiel Shatz [1] oder Weibel [1]).

(ii) Die Argumentation, welche die letzte Aussage 3.3.18 aus dem Spezialfall 3.3.15 ableitet ist ein Beispiel für eine sehr nützliche Technik welche Dimensionsverschiebung heißt: man beweist Aussagen über Kohomologie-Gruppen indem man G-Moduln in koinduzierte Moduln einbettet und dann mit Hilfe langer Kohomolgie-Sequenzen Induktionsargument verwendet. Andere Beispiele, für welche dieseTechnik benutzt werden kann, findet man in den Übungsaufgaben.

3.4 Cup-Produkte

3.4.1 Ziel des Abschnitts, Tensor-Produkte von G-Moduln

(i) In diesem Abschnitt konstruieren wir eine assoziative Produkt-Operation

$$H^i(G, A) \times H^j(G, B) \longrightarrow H^{i+j}(G, A \otimes B), (a,b) \mapsto a \cup b,$$

welche graduiert kommutativ (oder auch super-kommutativ) ist, d.h. es gilt

$$a \cup b = (-1)^{ij} (b \cup a).$$

---

[125] nach 3.3.16.

(ii) Dabei ist $A \otimes B$ das Tensorprodukt der G-Moduln A und B über $\mathbb{Z}$, versehen mit der durch die diagonale Operation

$$\sigma \bullet (a \otimes b) = (\sigma \bullet a) \otimes (\sigma \bullet b)$$

gegebenen G-Modul-Struktur. Man beachte, dies ist im allgemeinen nicht das Tensor-Produkt der beiden $\mathbb{Z}[G]$-Moduln über $\mathbb{Z}[G]$.

(iii) Allgemeiner ist das Tensorprodukt $A \otimes B$ ein $G \times G$-Modul bezüglich der Operation

$$(\sigma, \tau) \bullet (a \otimes b) = (\sigma \bullet a) \otimes (\tau \bullet b).$$

(iv) Wir beginnen die Konstruktion mit allgemeinen Betrachtungen im Kontext von Komplexen. Wir beschränken uns dabei auf den Fall von abelschen Gruppen. Das ist der einzige, den wir benötigen.

3.4.2 Doppel-Komplexe

Ein Doppel-Komplex A** (abelscher Gruppen) besteht aus zwei Familien von Homomorphismen abelscher Gruppen,

$$d^h_{ij}: A^{ij} \longrightarrow A^{i+1,j} \text{ und } d^v_{ij}: A^{ij} \longrightarrow A^{i,j+1} \quad (i, j \in \mathbb{Z})$$

mit

(i) Für jedes feste i ist $\{d^v_{ij}.A^{ij} \longrightarrow A^{i,j+1}\}_{j \in \mathbb{Z}}$ ein Komplex.

(ii) Für jedes feste j ist $\{d^h_{ij}: A^{ij} \longrightarrow A^{i+1,j}\}_{j \in \mathbb{Z}}$ ein Komplex.

(iii) Für jedes i und jedes j gilt

$$d^h_{i,j+1} \circ d^v_{ij} + d^v_{i+1,j} \circ d^h_{ij} = 0.$$

$$\begin{array}{ccccccc}
 & & \vdots & & \vdots & & \vdots \\
 & & \uparrow & & \uparrow & & \uparrow \\
\cdots & \longrightarrow & A^{i-1,j+1} & \longrightarrow & A^{i,j+1} & \longrightarrow & A^{i+1,j+1} & \longrightarrow \cdots \\
 & & \uparrow & & \uparrow & & \uparrow & \\
\cdots & \longrightarrow & A^{i-1,j} & \longrightarrow & A^{i,j} & \longrightarrow & A^{i+1,j} & \longrightarrow \cdots \\
 & & \uparrow & & \uparrow & & \uparrow & \\
 & & \vdots & & \vdots & & \vdots &
\end{array}$$

Bemerkung

Die dritte Bedingung bedeutet gerade, daß die Familie der direkten Summen

$$A^n := \oplus_{i+j} A^{ij}$$

zusammen mit den Abbildungen

$$d_n: A^n \longrightarrow A^{n+1},$$

deren ij-Koordinaten-Funktionen gerade die Abbildungen $d^h_{ij} + d^v_{ij}: A^{ij} \longrightarrow A^{n+1}$ sind, einen Komplex bilden. Dieser Komplex A* heißt der zu A** gehörige einfache (oder auch totale) Komplex und wird mit

$$A^* := \mathrm{tot}(A^{**})$$

bezeichnet.

3.4.3 Tensorprodukt von Komplexen

Seien A* und B* zwei Komplexe abelscher Gruppen. Das Tensor-Produkt von A* und B* (über $\mathbb{Z}$) ist definiert als der einfache Komplex zum Doppel-Komplex mit den Rand-Operatoren

$$\partial^h_{ij} = \partial^A_i \otimes \mathrm{Id}: A^i \otimes B^j \longrightarrow A^{i+1} \otimes B^j,\ a \otimes b \mapsto \partial^A_i(a) \otimes b$$

und

$$\partial^v_{ij} = \mathrm{Id} \otimes (-1)^i \partial^B_j: A^i \otimes B^j \longrightarrow A^i \otimes B^{j+1},\ a \otimes b \mapsto a \otimes (-1)^i \partial^B_j(b).$$

Das Tensor-Produkt der Komplexe A* und B* wird mit

$$\mathrm{tot}(A^* \otimes B^*)$$

bezeichnet.

Bemerkungen

(i) Die horizontalen Randoperatoren von $A^* \otimes B^*$ kommen von den Randoperatoren des ersten Tensorfaktors.

(ii) Die vertikalen Randoperatoren von $A^* \otimes B^*$ kommen von den Randoperatoren des zweiten Tensorfaktors, wobei das Vorzeichen auf $A^i \otimes B^j$ von der ersten Koordinate i abhängt.

(iii) Für $a \in A^i$ und $b \in B^j$ erhält man die Elemente

$$\partial^v_{i+1,j} \circ \partial^h_{ij}(a \otimes b) \text{ und } \partial^h_{i,j+1} \circ \partial^v_{ij}(a \otimes b)$$

indem man ∂^A_i auf den ersten Tensorfaktor a und ∂^B_j auf den zweiten Tensorfaktor b anwendet. Im ersten Fall muß man jedoch noch mit $(-1)^{i+1}$ und im zweiten mit $(-1)^i$ multiplizieren. Die Summe der beiden Elemente ist wie gefordert Null.

(iv) Der Randoperator des totalen Komplexes ist durch die folgende Formel gegegeben.

$$\partial(a \otimes b) = (\partial a) \otimes b + (-1)^{\deg a}\, a \otimes (\partial b).$$

Dabei schreiben wir deg a = i, falls $a \in A^i$ gilt.

3.4.4 Der Hom-Komplex

Seien A ein abelsche Gruppe und A* ein Komplex abelscher Gruppen. Dann bezeichnen wir mit

$$\mathrm{Hom}(A^*, A)$$

den Komplex abelscher Gruppen, der durch Anwenden des Funktors $\mathrm{Hom}_{\mathbb{Z}}(\,?\,, A)$ auf A* entsteht, wobei der Bestandteil des Komplexes im Grad i die Gruppe

$$\mathrm{Hom}(A^*, A)^i = \mathrm{Hom}_{\mathbb{Z}}(A^{-i}, A)$$

sei.

3.4.5 Konstruktion: eine natürliche Paarung auf der Kohomolgie von Hom-Komplexen.

Seien A und B abelsche Gruppen und A*, B* Komplexe abelscher Gruppen. Wir konstruieren eine Abbildung

(1) $$H^i(\mathrm{Hom}(A^*, A)) \times H^j(\mathrm{Hom}(B^*, B)) \longrightarrow H^{i+j}(\mathrm{Hom}(A^* \otimes B^*, A \otimes B).$$

Für je zwei Homomorphismen

$$\alpha: A^{-i} \longrightarrow A \text{ und } \beta: B^{-j} \longrightarrow B$$

ist $\alpha \otimes \beta$ ein Homomorphismus

$$\alpha \otimes \beta: A^{-i} \otimes B^{-j} \longrightarrow A \otimes B.$$

Wir können $\alpha \otimes \beta$ als Homomorphismus

$$\alpha \otimes \beta : (A^* \otimes B^*)^{-(i+j)} \longrightarrow A \otimes B$$

betrachten, indem wir die Abbildung auf allen von $A^{-i}\otimes B^{-j}$ verschiedenen direkten Summanden des Tensorprodukts Null setzen. Auf diese Weise wird $\alpha\otimes\beta$ zu einem Element des Grades i+j von Hom(A*⊗B*, A⊗B), d.h. wir haben eine Abbildung

(2) $\quad \mathrm{Hom}(A^*, A)^i \times \mathrm{Hom}(B^*,B)^j \longrightarrow \mathrm{Hom}(A^*\otimes B^*, A\otimes B)^{i+1}$, $(\alpha, \beta) \mapsto \alpha\otimes\beta$,

konstruiert.

Für $\alpha\in Z^i(\mathrm{Hom}(A^*,A))$ und $\beta\in Z^j(\mathrm{Hom}(B^*,B)$ gilt

$$d(\alpha\otimes\beta) = (d\sigma)\otimes\beta + \alpha\otimes(-1)^i d\beta = 0\otimes\beta + \alpha\otimes 0 = 0.$$

Die Abbildung (2) induziert also eine Abbildung

(3) $\quad Z^i\mathrm{Hom}(A^*, A) \times Z^j\mathrm{Hom}(B^*,B) \longrightarrow Z^{i+1}\mathrm{Hom}(A^*\otimes B^*, A\otimes B)$, $(\alpha, \beta) \mapsto \alpha\otimes\beta$,

Seien $\alpha\in B^i\mathrm{Hom}(A^*,A)$ und $\beta\in Z^j\mathrm{Hom}(B^*, B)$. Dann gibt es ein α' mit

$$\alpha = d\alpha',$$

d.h. es gilt

$$d(\alpha'\otimes\beta) = (d\alpha')\otimes\beta = \alpha'\otimes(-1)^{i-1}d\beta = \alpha\otimes\beta$$

d.h. das Tensor-Produkt eines Randes mit einem Zyklus ist ein Rand. Vertauscht man die Rollen α und β , so zeigt eine analoge Rechnung, daß auch das Tensor-Produkt eines Zyklus mit einem Rand ein Rand ist. Die Abbildung (3) induziert damit die gesuchte Abbildung (1).

Bemerkung

Seien G eine Gruppe und A* und B* Komplexe von G-Moduln und A,B G-Moduln. Sind dann die oben betrachteten Homomorphismen α und β G-Homomorphismen, so ist deren Tensorprodukt

$$\alpha\otimes\beta\colon A^{-i}\otimes B^{-j} \longrightarrow A\otimes B.$$

ein G×G-Homomorphismus. Durch Einschränken der betrachteten Abbildungen erhalten wir deshalb in dieser Situation eine bilineare Abbildung

(4) $\quad H^i(\mathrm{Hom}_G(A^*, A))\times H^j(\mathrm{Hom}_G(B^*, B)) \longrightarrow H^{i+j}(\mathrm{Hom}_{G\times G}(A^*\otimes B^*,A\otimes B)$.

3.4.6 Das Tensorprodukt von Auflösungen

Seien G eine Gruppe und P_* eine projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$. Dann ist

$$P_*\otimes P_*$$

eine projektive Auflösung des trivialen $\mathbb{Z}[G\times G]$-Moduls $\mathbb{Z}$. Die Operation von G×G auf $P_*\otimes P_*$ ist dabei durch die folgende Formel definiert.

$$(\sigma_1, \sigma_2)\,(p_1\otimes p_2) := \sigma_1(p_1)\otimes\sigma_2(p_2).$$

Bemerkungen

(i) Der i-te homogene Bestandteil von P_* als graduierte abelschen Gruppe ist gerade

$$P^i := P_{-i},$$

der von $\mathrm{Hom}(P_*\otimes P_*, A)$ ist

$$\mathrm{Hom}(P_*\otimes P_*, A)^i = \mathrm{Hom}(\oplus_{u+v=-i} P^u\otimes P^v , A) = \mathrm{Hom}(\oplus_{u+v=i} P_u\otimes P_v , A).$$

(ii) Der Beweis der obigen Aussage beruht auf dem nachfolgenden Lemma.

3.4.7 Lemma: Komplexe freier abelscher Gruppen

(i) Seien A* und B* exakte Sequenzen von freien abelschen Gruppen. Dann gilt dies auch für den Komplex $A^* \otimes B^*$.

(ii) Seien A* und B* Komplexe freier abelscher Gruppen mit den folgenden drei Eigeschaften.

a) Die Komplexe sind in den nicht-positiven Graden konzentiert, d.h.

$$A^i = B^i = 0 \text{ für } i > 0.$$

b) Die Komplexe haben triviale Kohomologie in allen negativen Graden, d.h.

$$H^i(A) = H^i(B) = 0 \text{ für } i < 0.$$

c) Die 0-te Kohomologie der Komplexe ist $\mathbb{Z}$, d.h.

$$H^0(A^*) = \mathbb{Z} \text{ und } H^0(B^*) = \mathbb{Z}.$$

Dann hat auch der Komplex $A^* \otimes B^*$ diese drei Eigenschaften.

Beweis. Zu (i). Da Tensorprodukte und direkte Summen von freien abelschen Gruppen wieder frei sind, sind die homogenen Bestandteile von

$$A^* \otimes B^*$$

wieder frei. Der Beweis der Exaktheit von $A^* \otimes B^*$ beruht auf der Tatsache, daß Untergruppen freier abelscher Gruppen frei sind. Deshalb ist für jedes i die Untergruppe $B^i(A)$ von A^i eine freie abelsche Gruppe. Betrachten wir für jedes i die kurze exakte Sequenz

$$0 \longrightarrow Z^i(A^*) \longrightarrow A^i \longrightarrow B^{i+1}(A^*) \longrightarrow 0.$$

Wei die Gruppe rechts frei ist, zerfällt diese Sequenz. Weil A* exakt sein soll, ist außerdem $Z^i(A^*) = B^i(A^*)$, d.h. die Sequenz läßt sich in der folgenden Gestalt schreiben.

$$0 \longrightarrow B^i(A^*) \xrightarrow{q_1} B^i(A^*) \oplus B^{i+1}(A^*) \xrightarrow{p_2} B^{i+1}(A^*) \longrightarrow 0.$$

Dabei bezeichne q_1 die natürliche Einbettung des ersten direkten Summanden in die direkte Summe und p_2 die Projektion auf den zweiten direkten Summanden. Wir sehen so, der Komplex A* zerfällt in eine direkte Summe von Teilkomplexen der Gestalt

$$(1) \qquad \ldots \longrightarrow 0 \longrightarrow 0 \longrightarrow A \xrightarrow{Id} A \longrightarrow 0 \longrightarrow 0 \longrightarrow \ldots$$

wobei A eine freie abelsche Gruppe bezeichne. Analog zerfällt B* in eine direkte Summe von Teilkomplexen der Gestalt

$$(2) \qquad \ldots \longrightarrow 0 \longrightarrow 0 \longrightarrow B \xrightarrow{Id} B \longrightarrow 0 \longrightarrow 0 \longrightarrow \ldots$$

Nun ist die Konstruktion des Tensorprodukts von Komplexen mit der Bildung von direkten Summen verträglich. Es reicht deshalb die Exaktheitsaussage für Komplexe der Gestalt (1) und (2) zu beweisen. Das Tensorprodukt von (1) und (2) ist aber ein Komplex der Gestalt

$$\ldots \longrightarrow 0 \longrightarrow 0 \longrightarrow A \otimes B \xrightarrow{\alpha} (A \otimes B) \oplus (A \otimes B) \xrightarrow{\beta} A \otimes B \longrightarrow 0 \longrightarrow 0 \longrightarrow \ldots$$

mit[126]

$$\alpha(x) =^{[127]} (x, \pm x) \text{ und } \beta(x,y) =^{[128]} x \mp y .$$

Diese ist offensichtlich eine exakte Sequenz.

Zu (ii). Man wende die Aussage von (i) auf die exakten Sequenzen

---

[126] In der direkten Summe $(A \otimes B) \oplus (A \otimes B)$ denken wir uns die Gruppen so angeordnet, daß sich im ersten direkten Summanden die Gruppe A vom niedrigen (und die Gruppe B vom hohen Grad befindet).

[127] Der Randoperator des Produkt-Komplexes besteht aus zwei Summanden. Der erste besteht im Anwenden des Randoperators von (1) auf dem ersten Tensorfaktor, der zweite im Anwenden des vorzeichenbehafteten Randoperators von (2) auf den zweiten Tensorsfaktor. Das Vorzeichen hängt davon ab, ob der Komplex (1) in einem geraden oder ungeraden Grad beginnt.

[128] Der Randoperator auf den Elementen "hohen" Grades ist die Nullabbildung.

$$K_A: A^* \xrightarrow{u} \mathbb{Z} \longrightarrow 0 \text{ und } K_B: B^* \xrightarrow{v} \mathbb{Z} \longrightarrow 0.$$

die aus A* und B* entstehen, wenn man im Grad 1 die 0 durch die Kohomologie-Gruppe $\mathbb{Z}$ ersetzt. Durch Tensorieren erhalten wir eine exakte Sequenz

$$K := \mathrm{tot}(K_A \otimes K_B),$$

welche wir jetzt mit dem Komplex

$$L := \mathrm{tot}(A^* \otimes B^*)$$

vergleichen wollen. Es gilt

$$\begin{aligned} K_n &= \oplus_{i+j=n} K_{A,i} \otimes K_{B,j} \\ &= (\mathbb{Z} \otimes B_{n+1}) \oplus (A_0 \otimes B_n) \oplus \ldots \oplus (A_n \otimes B_0) \oplus (A_{n+1} \otimes \mathbb{Z}) \\ &\cong B_{n+1} \oplus \mathrm{tot}(A^* \otimes B^*)_n \oplus A_{n+1} \end{aligned}$$

Der Randoperator auf dem ersten bzw. letzten Summanden stimmt dabei mit dem Randoperator von B* bzw. A* überein (ersterer nur bis aufs Vorzeichen), denn der eine Summand dieses Randoperators kommt von der Null-Abbildung $\mathbb{Z} \longrightarrow 0$. Der Randoperator auf dem direkten Summanden in der Mitte ist gerade der Randoperator von tot(A*⊗B*) (zumindest in allen negative Graden). Genauer wir haben ein kommutatives Diagramm

$$\begin{array}{ccccccccc} \ldots \longrightarrow & (A_1 \otimes B_0) \oplus (A_0 \oplus B_1) & \longrightarrow & A_0 \otimes B_0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow \ldots \\ & \cap & & \cap & & & & \cap & \\ \ldots \longrightarrow & A_2 \oplus (A_1 \otimes B_0 \oplus A_0 \otimes B_1) \oplus B_2 & \longrightarrow & A_1 \oplus (A_0 \otimes B_0) \oplus B_1 & \longrightarrow & A_0 \otimes \mathbb{Z} \oplus B_0 & \longrightarrow & \mathbb{Z} & \longrightarrow \ldots \end{array}$$

Die obere Zeile ist dabei gerade der Komplex tot(A*⊗B*) und die untere der Komplex $\mathrm{tot}(K_A \otimes K_B)$. Die Kommutativität des Diagramms geht verloren, wenn man die fehlende vertikale Einbettung rechts einfügt. Um die Kommutativität des Diagramms beim Einfügen zu erhalten, mußt man die vorletzte 0 rechts oben durch $\mathbb{Z}$ und die entsprechende Null-Abbildung durch u⊗v ersetzen:

$$\begin{array}{ccccccccc} \ldots \longrightarrow & (A_1 \otimes B_0) \oplus (A_0 \oplus B_1) & \longrightarrow & A_0 \otimes B_0 & \xrightarrow{u \otimes v} & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow \ldots \\ & \cap & & \cap & & \cap & & \cap & \\ \ldots \longrightarrow & A_2 \oplus (A_1 \otimes B_0 \oplus A_0 \otimes B_1) \oplus B_2 & \longrightarrow & A_1 \oplus (A_0 \otimes B_0) \oplus B_1 & \longrightarrow & A_0 \otimes \mathbb{Z} \oplus B_0 & \longrightarrow & \mathbb{Z} & \longrightarrow \ldots \end{array}$$

Die obere Zeile wird dann zu einem direkten Summanden der unteren. Die untere eine direkte Summe der oberen mit den Komplexen K_A und K_B. Insbesondere ist mit der unteren Zeile auch die obere Zeile exakt, d.h. tot(A*⊗B*) genügt den Bedingungen (a), (b) und (c) von (ii).

QED.

3.4.8 Beweis von 3.4.6

Nach Definition sind die graduierten Bestandteile von P_* direkte Summanden von freien $\mathbb{Z}[G]$-Moduln, also insbesondere freie abelsche Gruppen. Auf Grund des zweiten Teils von 3.4.7 liefert das Tensorprodukt der exakten Sequenz

$$P_* \longrightarrow \mathbb{Z} \longrightarrow 0$$

mit sich eine exakte Sequenz

$$P_*\otimes P_* \longrightarrow \mathbb{Z} \longrightarrow 0.$$[129]

Es bleibt noch zu zeigen, $P_*\otimes P_*$ ist ein Komplex von projektiven $\mathbb{Z}[G\times G]$-Moduln.

Dazu betrachten wir die (über $\mathbb{Z}$) bilineare Abbildung

$$\mathbb{Z}[G]\times\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G\times G]\,,\ \Big(\sum_{\sigma\in G} m_\sigma\sigma,\ \sum_{\tau\in G} n_\tau\tau\Big) \mapsto \sum_{\sigma,\tau\in G} m_\sigma n_\sigma(\sigma,\tau)\,,$$

Sie induziert einen Gruppen-Homomorphismus

$$\varphi:\mathbb{Z}[G]\otimes_{\mathbb{Z}}\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G\times G],\ \sigma\otimes\tau \mapsto (\sigma,\tau).$$

Weil letzterer eine Basis der freien abelschen Gruppe links in eine Basis der freien abelschen Gruppe rechts abbildet, ist er bijektiv. Die Ringstruktur links definiert also eine Ringstruktur rechts. Bezüglich dieser Ringstruktur gilt für das Produkt zweier Basis Elemente (σ,τ) und (σ',τ') rechts:

$(\sigma,\tau)\bullet(\sigma',\tau') := \varphi(\varphi^{-1}(\sigma,\tau)\bullet\varphi^{-1}(\sigma',\tau')) = \varphi(\sigma\otimes\tau\bullet\sigma'\otimes\tau') = \varphi((\sigma\sigma'\otimes\tau\tau') = (\sigma\sigma',\tau\tau')$.
Mit anderen Worten, φ ist ein Isomorphismus von Ringen.

Damit ist das Tensorprodukt von freien $\mathbb{Z}[G]$-Moduln ein freier $\mathbb{Z}[G\times G]$-Modul, wobei die Operation von $G\times G$ auf diesem Modul gerade die in 3.4.6 beschriebene ist.[130]

Sind schließlich P_i und P_j projektive G-Moduln mit der Eigenschaft, daß die direjekten

$$P_i\oplus Q_i \text{ und } P_j\oplus Q_j$$

freie G-Moduln sind (für geeignet gewählte G-Moduln Q_i und Q_j) so ist

$$(P_i\oplus Q_i)\otimes(P_j\oplus Q_j) = (P_i\otimes P_j)\oplus(P_i\otimes Q_j)\oplus(Q_i\otimes P_j)\oplus(Q_i\otimes Q_j)$$

ein freier $G\times G$-Modul, der $P_i\otimes P_j$ als direkten Summanden enthält. Insbesondere ist der Modul $P_i\otimes P_j$ projektiv.

QED.

3.4.9 Zusammenfassung: das Cup-Produkt

Seien G eine Gruppe, A und B zwei G-Moduln und

$$P_* \longrightarrow \mathbb{Z} \longrightarrow 0$$

eine projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$. Nach 3.4.5 definiert das Tensor-Produkt von Abbildungen bilineare Abbildung

---

[129] wobei $\mathbb{Z}$ im Grade 1 sitzt.

[130] Das Tensorprodukt über $\mathbb{Z}$ eines R-Moduls M mit einem S-Modul N ist ein $R\otimes S$-Modul $M\otimes N$ mit der Multiplikation

$$r\otimes s\bullet m\otimes n = (rm)\otimes(sn).$$

Für jedes $r\in R$ und jedes $s\in S$ ist die Abbildung

$$M\times N \longrightarrow M\otimes N,\ (m,n) \mapsto (rm)\otimes(sn),$$

nämlich bilinear (über $\mathbb{Z}$), induziert also einen Gruppen-Homomorphismus

$$M\otimes N \longrightarrow M\otimes N,\ m\otimes n \mapsto (rm)\otimes(sn).$$

Die so definierte Abbildung

$$R\times S \longrightarrow \mathrm{Hom}_{Ab}(M\otimes N, M\otimes N),\ (r,s) \mapsto (m\otimes n \mapsto (rm)\otimes(sn)),$$

ist bilinear (über $\mathbb{Z}$), induziert also einen Gruppen-Homomorphismus

$$R\otimes S \longrightarrow \mathrm{Hom}_{Ab}(M\otimes N, M\otimes N).$$

Die oben angegebene Multiplikation der Ememente von $M\otimes N$ mit Elementen aus $R\otimes S$ ist also wohldefiniert.

$$H^i(\mathrm{Hom}_G(P_*,A))\times H^j(\mathrm{Hom}_G(P_*, B)) \longrightarrow H^{i+j}(\mathrm{Hom}_{G\times G}(P_*\otimes P_* , A\otimes B).$$

Nach 3.4.6 ist $P_*\otimes P_*$ eine projektive Auflösung des trivialen $G\times G$-Moduls $\mathbb{Z}$. Die Abbildung läßt sich also in der folgenden Getalt schreiben.

(1) $$H^i(G, A) \times H^j(G, B) \longrightarrow H^{i+1}(G\times G, A\otimes B).$$

Die diagonale Einbettung $G \hookrightarrow G\times G$, $g \mapsto (g,g)$, induziert einen Restriktionshomomorphismus auf der Kohomologie, der zusammengesetzt mit (1) eine bilineare Abbildung

$$H^i(G, A) \times H^j(G, B) \longrightarrow H^{i+1}(G, A\otimes B),\ (a, b) \mapsto a\bigcup b$$

liefert. Diese heißt Cup-Produkt.

Bemerkungen

(i) Auf Grund des Vergleichssatzes hängt die Konstruktion des Cup-Produkts nicht von der speziellen Wahl der projektiven Auflösung ab.

(ii) Die Konstruktion ist funktioriell in dem Sinne, daß man für jeden G-Homomorphismus $A \longrightarrow A'$ ein kommutatives Diagramm von G-Moduln

$$\begin{array}{ccc} H^i(G,A)\times H^j(G,B) & \longrightarrow & H^{i+j}(G,A\otimes B) \\ \downarrow & & \downarrow \\ H^i(G,A')\times H^j(G,B) & \longrightarrow & H^{i+j}(G,A'\otimes B) \end{array}$$

hat, und analog für den zweiten Tensor-Faktor.

(iii) Jeder G-Homomorphismus $A\otimes B \longrightarrow C$ induziert einen Homomorphismus auf der Kohomologie, dessen Zusammensetzung mit dem Cup-Produkt eine bilineare Abbildung

$$H^i('G, A) \times H^j(G, B) \longrightarrow H^{i+j}(G, C)$$

ist, die man gelegentlich auch als Cup-Produkt bezeichnet.

(iv) Aus der Konstruktion des Cup-Produktes ergibt sich für i = j = 0, daß die Abbildung

$$H^0(G, A) \times H^0(G, B) \longrightarrow H^0(G, A\otimes B)$$

gerade die Abbildung

$$A^G\times B^G \longrightarrow (A\otimes B)^G,\ (a, b) \mapsto a\otimes b,$$

ist.

3.4.10 Assoziativität und Superkommutativität des Cup-Produkts

Das Cup-Produkt ist assoziativ und graduiert kommutativ, d.h. es gilt

$$a\bigcup b = (-1)^{ij}\, b\bigcup a \text{ für } a\in H^i(G,A) \text{ und } b\in H^j(G,B)$$

wenn man die beiden Kohomologie-Gruppen

$$H^{i+j}(G, A\otimes B) \text{ und } H^{i+j}(G, B\otimes 'A)$$

mit Hilfe des Isomorphimus

$$A\otimes B \longrightarrow B\otimes A,\ a\otimes b \mapsto b\otimes a,$$

identifiziert.

.

Beweis. Die Assoziativitätsaussage folgt im wesentlichen aus der Assoziativität des Tensorprodukts von Abbildungen. Das Cup-Produkt zweier Kohomologie-Klassen wird repräsentiert durch das Tensorprodukt der Abbildungen, welche die Faktoren repräsentieren. Wir überlassen dem Leser die Einzelheiten.

Zur Überprüfung der graduierten Kommutativität vergleichen wir zunächst die Randoperatoren der Tensorprodukte

$$\mathrm{tot}(A^*\otimes B^*) \text{ und } \mathrm{tot}(B^*\otimes A^*)$$

zweier Komplexe A* und B*. Im ersten Komplex ist der Randoperator durch die folgende Formel gegeben.

$$\partial(a\otimes b) = (\partial a)\otimes b + (-1)^{\deg a}\, a\otimes(\partial b)$$

im zweiten durch

$$\partial(b\otimes a) = (\partial b)\otimes a + (-1)^{\deg b}\, b\otimes(\partial a).$$

Wir sehen die beiden totalen Komplexe zunächst als graduierte abelsche Gruppen an und betrachten die Abbildung

$$\varphi\colon \mathrm{tot}(A^*\otimes B^*) \longrightarrow \mathrm{tot}(B^*\otimes A^*),\ a\otimes b \mapsto (-1)^{\deg a \,\bullet\, \deg b}\, b\otimes a.$$

Es gilt

$$\begin{aligned}\varphi(\partial(a\otimes b)) &= (-1)^{(\deg a+1)\,\bullet\,\deg b}\, b\otimes\partial a + (-1)^{\deg a\,\bullet\,(\deg b+1)+\deg a}\,(\partial b)\otimes a\\ &= (-1)^{\deg a\,\bullet\,\deg b}\,[(-1)^{\deg b} b\otimes\partial a + (-1)^{2\deg a}\,(\partial b)\otimes a]\\ &= (-1)^{\deg a\,\bullet\,\deg b}\,\partial(b\otimes a)\\ &= \partial(\,(-1)^{\deg a\,\bullet\,\deg b}\, b\otimes a)\\ &= \partial(\varphi(a\otimes b)\end{aligned}$$

d.h. φ ist ein Komplex-Morphismus. Es ist offensichtlich ein Isomorphismus. Wir identifizieren die beiden Komplexe mit Hilfe dieses Isomorphimus und erhalten so die Formel

$$a\otimes b = (-1)^{\deg a\,\bullet\,\deg b}\, b\otimes a.$$

Dies gilt speziell für

$$A^* := \mathrm{Hom}_G(P_*,A) \text{ und } B^* := \mathrm{Hom}_G(P_*,B)$$

mit einer projektiven Auflösung P_* des trivialen G-Moduls $\mathbb{Z}$. Die Tensorprodukte auf beiden Seiten sind dann Tensorprodukte von Abbildungen. Durch Übergang zur Kohomologie erhalten wir die behauptete Identität.
QED.

3.4.10 Verträglichkeit mit Zusammenhangshomomorphismen

Seien G eine Gruppe und

(1) $$0 \longrightarrow A' \xrightarrow{\alpha} A \longrightarrow A'' \longrightarrow 0$$

eine exakte Sequenz von G-Moduln mit der Eigenschaft, daß für jeden G-Modul B das Tensorprodukt über $\mathbb{Z}$,

$$0 \longrightarrow A'\otimes B \longrightarrow A\otimes B \longrightarrow A''\otimes B \longrightarrow 0,$$

ebenfalls exakte ist. Dann gilt

$$\delta(a)\bigcup b = \delta(a\bigcup b)$$

für $a\in H^i(G,A'')$, $b\in H^j(G, B)$ in $H^{i+j+1}(G, A'\otimes B)$. Dabei bezeichne δ den Zusammenhangshomomorphismus zur exakten Sequenz (1).

Analog sei

(2) $$0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$$

eine exakte Sequenz von G-Moduln mit der Eigenschaft, daß für jeden G-Modul A das Tensorprodukt über $\mathbb{Z}$,

$$0 \longrightarrow A\otimes B' \longrightarrow A\otimes B \longrightarrow A\otimes B'' \longrightarrow 0$$

exakt ist. Dann gilt

$$a \bigcup \delta(b) = (-1)^i\, \delta(a\bigcup b)$$

für $a\in H^i(G,A)$, $b\in H^j(G, B''$ in $H^{i+j+1}(G, A\otimes B')$.

Beweis. Sei $\beta \in H^j(G, B)$ fest vorgegeben. Wir wählen eine projektive Auflösung

$$P_* \longrightarrow \mathbb{Z} \longrightarrow 0$$

des trivialen G-Moduls $\mathbb{Z}$ und einen Repräsentanten

$$b \in \mathrm{Hom}_G(P_j, B)$$

von β. Wir wenden den Funktor $\mathrm{Hom}_G(P_*, ?)$ auf die exakte Sequenz (1) an und den Funktor $\mathrm{Hom}_G(\mathrm{tot}(P_* \otimes P_*), ?)$ auf deren Tensorprodukt mit B. Als Ergebnis erhalten wir - wegen der Projektivität von P_* - exakte Sequenzen von Komplex-Morphismen

$$0 \longrightarrow \mathrm{Hom}_G(P_*, A') \longrightarrow \mathrm{Hom}_G(P_*, A) \longrightarrow \mathrm{Hom}_G(P_*, A'') \longrightarrow 0$$

und

$$0 \longrightarrow \mathrm{Hom}_G(P_* \otimes P_*, A' \otimes B) \longrightarrow \mathrm{Hom}_G(P_* \otimes P_*, A \otimes B) \longrightarrow \mathrm{Hom}_G(P_* \otimes P_*, A'' \otimes B) \longrightarrow 0$$

Nun ist das Tensorprodukt mit der Komposition von Abbildungen verträglich. Tensorieren mit b liefert deshalb ein kommutatives Diagramm[131]

$$\begin{array}{ccccccc}
0 \longrightarrow & \mathrm{Hom}_G(P_*, A') & \xrightarrow{\alpha} & \mathrm{Hom}_G(P_*, A) & \longrightarrow & \mathrm{Hom}_G(P_*, A'') & \longrightarrow 0 \\
& \downarrow \otimes b & & \downarrow \otimes b & & \downarrow \otimes b & \\
0 \longrightarrow & \mathrm{Hom}_G(P_* \otimes P_*, A' \otimes B) & \xrightarrow{\alpha \otimes \mathrm{Id}} & \mathrm{Hom}_G(P_* \otimes P_*, A \otimes B) & \longrightarrow & \mathrm{Hom}_G(P_* \otimes P_*, A'' \otimes B) & \longrightarrow 0
\end{array}$$

In der unteren Zeile können wir noch die Tensorprodukte $P_* \otimes P_*$ durch P_* ersetzen. [132]

Wir gehen zur Kohomolgie über und erhalten einen Komplex-Morphismus der zugehörigen langen Kohomologie-Sequenzen (der den Grad um j verschiebt). Insbesondere erhalten wir die kommuttiven Vierecke

$$\begin{array}{ccc}
H^i(G, A'') & \xrightarrow{\delta} & H^{j+1}(G, A') \\
\downarrow \cup \beta & & \downarrow \cup \beta \\
H^{i+j}(G, A'' \otimes B) & \xrightarrow{\delta} & H^{i+j+1}(G, A')
\end{array}$$

Dies beweist die erste der beiden Identitäten der Behauptung. Die zweite ergibt sich aus dieser unter Verwendung der Formel von 3.4.9:

$$\begin{aligned}
a \cup \delta(b) &= (-1)^{\deg a \bullet (\deg b + 1)} \delta(b) \cup a \\
&= (-1)^{\deg a \bullet (\deg b + 1)} \delta(b \cup a) \\
&= (-1)^{\deg a \bullet (\deg b + 1)} \delta((-1)^{\deg a \bullet \deg b} a \cup b) \\
&= (-1)^{\deg a \bullet (2\deg b + 1)} \delta(a \cup b) \\
&= (-1)^{\deg a} \delta(a \cup b).
\end{aligned}$$

QED.

3.4.11 Der Fall des Cup-Produktes zu einer Paarung der Koeffizienten

Seien G eine Gruppe und

---

[131] Bezeichne $\alpha: A' \longrightarrow A$ die linke Abbildung in (1). Die Kommutativität des linken Vierecks bedeutet dann gerade, daß für jeden G-Homomorphismus $\varphi: P_* \longrightarrow A'$ gilt

$$(\alpha \circ \varphi) \otimes b = (\alpha \circ \varphi) \otimes (\mathrm{Id} \otimes b) = (\alpha \otimes \mathrm{Id}) \circ (\varphi \otimes b).$$

[132] Unter Verwendung Diagonaleinbettung $G \hookrightarrow G \times G$.

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0 \text{ und } 0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$$

zwei kurze exakte Sequenzen von G-Moduln. Weiter sei eine (über $\mathbb{Z}$) bilineare Abbildung

$$\varphi: A \times B \longrightarrow C$$

mit Werten in einem G-Modul C gegeben, die verträglich ist mit der Operation von G und deren Einschränkung auf $A' \times B'$ trivial ist. Diese induziert dann bilineare Abbildungen

$$A' \times B'' \longrightarrow C \text{ und } A'' \times B' \longrightarrow 0.$$

Für die Cup-Produkte bezüglich dieser bilinearen Abbildungen gilt dann

$$\delta_A(\alpha) \cup \beta =^{133} (-1)^{i+1} \alpha \cup \delta_B(\beta)$$

für $\alpha \in H^i(G, A'')$, $\beta \in H^j(G, B'')$ in $H^{i+j+1}(G, C)$.

Beweis. Sei P_* eine projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$. Wie oben bekommen wir exakte Sequenzen von Komplex-Morphismen

$$0 \longrightarrow \mathrm{Hom}_G(P_*, A') \longrightarrow \mathrm{Hom}_G(P_*, A) \longrightarrow \mathrm{Hom}_G(P_*, A'') \longrightarrow 0$$

$$0 \longrightarrow \mathrm{Hom}_G(P_*, B') \longrightarrow \mathrm{Hom}_G(P_*, B) \longrightarrow \mathrm{Hom}_G(P_*, B'') \longrightarrow 0$$

Diese sind durch eine Paarung

$$\mathrm{Hom}_G(P_*, A) \times \mathrm{Hom}_G(P_*, B) \longrightarrow \mathrm{Hom}_G(P_* \otimes P_*, C), (u,v) \mapsto \varphi \circ (u \otimes v),$$

mit einander verbunden, welche trivial ist auf

$$\mathrm{Hom}_G(P_*, A') \times \mathrm{Hom}_G(P_*, B').$$

Beschreiben wir die beiden Seiten der zu beweisenden Identität mit Hilfe der repräsentierenden Abbildungen. Dazu wählen Repräsentanten

$$a'' \in \mathrm{Hom}_G(P_*, A'') \text{ und } b'' \in \mathrm{Hom}_G(P_*, B'')$$

von α bzw. β. Wegen der Projektivität von P_* besitzt a'' ein Urbild

$$a \in \mathrm{Hom}_G(P_*, A'').$$

Dessen Rand kommt von einem Element

$$a' \in \mathrm{Hom}_G(P_*, A'), a' = \partial a.$$

Nach Definition des Zusammenhangshomomorphismus ist

$$\delta_A(\alpha) = [a'] \in H^{i+1}\mathrm{Hom}_G(P_*, A').$$

Analog besitzt b'' ein Urbild

$$b \in \mathrm{Hom}_G(P_*, B),$$

und es gilt

$$\delta_A(\alpha) \cup \beta = [\varphi \circ ((\partial a) \otimes b)] \in H^{i+j+1}\mathrm{Hom}_G(P_* \otimes P_*, C).$$

In analoger Weise repräsentiert man $\alpha \cup \delta_B(\beta)$:

$$\alpha \cup \delta_B(\beta) = [\varphi \circ (a \otimes \partial b)] \in H^{i+j+1}\mathrm{Hom}_G(P_* \otimes P_*, C).$$

Betrachten wir jetzt das Element

$$\varphi \circ ((\partial a) \otimes b + (-1)^i a \otimes \partial b) \in \mathrm{Hom}_G(P_* \otimes P_*, C).$$

---

[133] Die Aussagen von 3.4.11 lassen sich in der beschriebenen Situation nicht verwenden:

$$\delta(\alpha) \cup \beta = \delta(\alpha \cup \beta) = (-1)^i \alpha \cup \delta(\beta),$$

weil der Zusammenhangshomomorphismus in der Mitte nicht definiert ist.

Es ist gleich $\varphi(\partial(a\otimes b))$, d.h. das Bild eines Randes bei der durch $\varphi: A\otimes B \longrightarrow C$ induzierten Abbildung, also selbst ein Rand. Also ist

$$\delta_A(\alpha)\cup\beta + (-1)^i \alpha\cup\delta_B(\beta) = [\varphi\circ((\partial a)\otimes b + (-1)^i a\otimes\partial b)] = 0,$$

d.h. es gilt die Behauptung.
QED.

3.4.12 Verträglichkeit mit Restriktion, Inflation und Korestriktion

Seien G eine Gruppe, $H \subseteq G$ eine Untergruppe und A, B zwei G-Moduln.

(i) Es gilt

$$\mathrm{Res}(a\cup b) = \mathrm{Res}(a)\cup\mathrm{Res}(b)$$

in $H^{i+j}(H, A\otimes B)$ für $a\in H^i(G,A)$ und $b\in H^j(G,B)$.

(ii) Ist $H \subseteq G$ ein Normalteiler, so gilt

$$\mathrm{Inf}(a\cup b) = \mathrm{Inf}(a)\cup\mathrm{Inf}(b)$$

in $H^{i+j}(G, A\otimes B)$ für $a\in H^i(G/H, A^H)$ und $b\in H^j(G/H, B^H)$.

(iii) Projektionsformel. Hat die Untergruppe $H \subseteq G$ endlichen Index, so gilt

$$\mathrm{Cor}(a\cup\mathrm{Res}(b)) = \mathrm{Cor}(a)\cup b$$

in $H^{i+j}(G,A\otimes B)$ für $a\in H^i(H, A)$ und $b \in H^j(G, B)$.

Beweis. Zu (i). Wir betrachten das kommutative Diagramm

$$\begin{array}{ccc} A\times B & \longrightarrow & A\otimes B \\ \downarrow & & \downarrow \\ M_H^G(A)\times M_H^G(B) & \longrightarrow & M_{H\times H}^{G\times G}(A\otimes B) \end{array}$$

dessen vertikale Abbildungen die natürlichen Einbettungen sind (welche jedem Modul-Element die zugehörige Multiplikation von rechts zuordnen - vgl. 3.3.5 (ii)). Die obere horizontale Abbildung sei die natürliche Abbildung aufs Tensorprodukt und die untere das Tensorprodukt von Abbildungen.

Für beliebige Komplexe A* und B* von G-Moduln induziert dieses Diagramm ein kommutatives Diagramm von Komplexen[134]

$$\begin{array}{ccc} \mathrm{Hom}_G(A^*,A)\times\mathrm{Hom}_G(B^*,B) & \longrightarrow & \mathrm{Hom}_{G\times G}(\mathrm{tot}(A^*\otimes B^*),A\otimes B) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_G(A^*,M_H^G(A))\times\mathrm{Hom}_G(B^*,M_H^G(B)) & \longrightarrow & \mathrm{Hom}_{G\times G}(\mathrm{tot}(A^*\otimes B^*),M_{H\times H}^{G\times G}(A\otimes B)) \end{array}$$

Die horizontalen Abbildungen sind dabei Tensorprodukte von Abbildungen, die vertikalen die Zusammensetzungen mit den vertikalen Abbildungen des vorigen Diagramms.

Wir setzen für A* und B* eine projektive Auflösung P_* des trivialen G-Moduls $\mathbb{Z}$ ein, gehen zur Kohomologie über und erhalten ein kommutatives Diagramm

[134] Die beiden möglichen Zusammensetzungen mit dem Abbildungen des obigen Vierecks stimmen überein.

$$\begin{array}{ccc} H^i(G,A)\times H^j(G,B) & \longrightarrow & H^{i+j}(G\times G, A\otimes B) \\ \downarrow & & \downarrow \\ H^i(G,M_H^G(A))\times H^j(G,M_H^G(B)) & \longrightarrow & H^{i+j}(G\times G, M_{H\times H}^{G\times G}(A\otimes B)) \end{array}$$

Die horizontalen Abbildungen sind dabei durch das Tensorprodukt von Abbildungen induziert. Die unteren Kohomologie-Gruppen lassen sich mit Hilfe des Lemmas von Shapiro mit Kohomologie-Gruppen über H identifizieren. Die vertikalen Abbildungen gehen dann gerade in die Restriktionsabbildungen über:

$$\begin{array}{ccc} H^i(G,A)\times H^j(G,B) & \xrightarrow{\otimes} & H^{i+j}(G\times G, A\otimes B) \\ \downarrow \mathrm{Res}\times\mathrm{Res} & & \downarrow \mathrm{Res} \\ H^i(H,A)\times H^j(H,B) & \xrightarrow{\otimes} & H^{i+j}(H\times H, A\otimes B) \end{array}$$

Nun verhält sich die Restriktion funktoriell bezüglich des ersten Arguments der Kohomologie, d.h. wir können die horizontalen Abbildungen zusammensetzen mit den Abbildungen, die durch die Diagonal-Einbettung $G \hookrightarrow G\times G$ induziert werden und erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} H^i(G,A)\times H^j(G,B) & \xrightarrow{\cup} & H^{i+j}(G, A\otimes B) \\ \downarrow \mathrm{Res}\times\mathrm{Res} & & \downarrow \mathrm{Res} \\ H^i(H,A)\times H^j(H,B) & \xrightarrow{\cup} & H^{i+j}(H, A\otimes B) \end{array}$$

Damit ist die Aussage von (i) bewiesen.

Zu (ii). Die Aussage von (ii) erhält man, indem man in ähnlicher Weise an die Definition der Inflation erinnert, wie wir das für die Restriktion gerade getan haben. Wir gehen wie in 3.3.10 von zwei projektiven Auflösungen

$$P_* \longrightarrow \mathbb{Z} \longrightarrow 0 \text{ und } Q_* \longrightarrow \mathbb{Z} \longrightarrow 0$$

des trivialen Moduls $\mathbb{Z}$ über G bzw. über G/H aus. Da sich die zweite Auflösung auch als Komplex von G-Moduln auffassen läßt, gibt es nach dem Vergleichssatz einen bis auf Homotopie eindeutig bestimmten Komplex-Morphismus

$$P_* \longrightarrow Q_*.$$

Dieser definiert ein kommutatives Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_{G/H}(Q_*,A^H)\times\mathrm{Hom}_{G/H}(Q_*,B^H) & \longrightarrow & \mathrm{Hom}_{G/H\times G/H}(\mathrm{tot}(Q_*\otimes Q_*), A^H\otimes B^H) \\ \downarrow & & \downarrow \\ \mathrm{Hom}_G(P_*,A^H)\times\mathrm{Hom}_G(P_*,B^H) & \longrightarrow & \mathrm{Hom}_{G\times G}(\mathrm{tot}(P_*\otimes P_*), A^H\otimes B^H) \end{array}$$

desssen horizontale Abbildungen durch das Tensorprodukt von Abbildungen induziert sind und dessen vertikale Abbildung durch das Zusammensetzen mit $P_* \longrightarrow Q_*$. Wir gehen zur Kohomologie über und erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} H^i(G/H,A^H)\times H^j(G/H,B^H) & \longrightarrow & H^{i+j}(G/H\times G/H,\ A^H\otimes B^H) \\ \downarrow & & \downarrow \\ H^i(G,A^H)\times H^j(G,B^H) & \longrightarrow & H^{i+j}(G\times G,\ A^H\otimes B^H) \end{array} \quad (1)$$

Auf Grund des kommutativen Diagramms

$$\begin{array}{ccc} G & \hookrightarrow & G\times G \\ \downarrow & & \downarrow \\ G/H & \hookrightarrow & G/H\times G/H \end{array}$$

dessen horizontale Abbildungen die Diagonaleinbettungen sind und dessen vertikale Abbildungen vom natürlichen Homomorphismus auf die Faktorgruppen kommen, können wir in (1) die direkten Produkte der Gruppen durch die Gruppen selbst ersetzen. Die horizontalen Abbildungen werden dann zu Cup-Produkten,

$$\begin{array}{ccc} H^i(G/H,A^H)\times H^j(G/H,B^H) & \xrightarrow{\cup} & H^{i+j}(G/H,\, A^H\otimes B^H) \\ \downarrow & & \downarrow \\ H^i(G,A^H)\times H^j(G,B^H) & \xrightarrow{\cup} & H^{i+j}(G,\, A^H\otimes B^H) \end{array}$$

Weil das Cup-Produkt funktoriell in beiden Argumenten ist, können wir in der unteren Zeile des Diagramms die H-invarianten Teile durch die G-Moduln selbst ersetzen,

$$\begin{array}{ccc} H^i(G/H,A^H)\times H^j(G/H,B^H) & \xrightarrow{\cup} & H^{i+j}(G/H,\, A^H\otimes B^H) \\ \downarrow \mathrm{Inf}\times\mathrm{Inf} & & \downarrow \mathrm{Inf} \\ H^i(G,A)\times H^j(G,B) & \xrightarrow{\cup} & H^{i+j}(G,\, A\otimes B) \end{array}$$

Die vertikalen Abbildungen werden dadurch gerade die Inflationsabbildungen. Damit ist die Aussage von (ii) bewiesen.

Zu (iii). Seien A* und B* zwei Komplexe von G-Moduln. Wir betrachten das folgende Diagramm von Komplexen.

$$\begin{array}{ccccc} \mathrm{Hom}_H(A^*,A)\times \mathrm{Hom}_H(B^*,B) & \xrightarrow{u} & \mathrm{Hom}_{H\times H}(\mathrm{tot}(A^*\otimes B^*),A\otimes B) \\ \downarrow c' & \uparrow r & \downarrow c'' \\ \mathrm{Hom}_G(A^*,A)\times \mathrm{Hom}_G(B^*,B) & \xrightarrow{v} & \mathrm{Hom}_{G\times G}(\mathrm{tot}(A^*\otimes B^*),A\otimes B) \end{array}$$

Die horizontalen Abbildungen seien durch das Tensorprodukt von Abbildungen induziert. Die mittlere Abbildung sei die natürliche Einbettung (die jeden G-Homomorphismus als H-Homomorphismus auffaßt). Sie induziert gerade die Restriktion, wenn man für B* eine projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$ einsetzt. Die beiden anderen Abbildungen seien gerade die der Korestriktion entsprechenden Abbildungen, d.h. sie sollen H-Homomorphismen

$$x \mapsto f(x)$$

überführen in G-Homomorphismen

$$x \mapsto \sum_j \sigma_j f(\sigma_j^{-1} x)$$

wenn die σ_j ein volles Repräsentantensystem von G/H in G bilden. Für

$$\alpha \in \mathrm{Hom}_H(A^*,A) \text{ und } \beta \in \mathrm{Hom}_G(B^*,B),\ a \in A^*,\ b \in B^*$$

gilt dann

$$\begin{aligned} v(c'(\alpha),\beta)(a\otimes b) &= (c'(\alpha)\otimes\beta)(a\otimes b) \\ &= (c'(\alpha)(a))\otimes\beta(b) \\ &= \sum_j \sigma_j\alpha(\sigma_j^{-1}a)\otimes\beta(b) \end{aligned}$$

$$= \sum_j (\sigma_j\alpha(\sigma_j^{-1}a) \otimes \sigma_j\beta(\sigma_j^{-1}b))$$

$$= \sum_j (\sigma_j\alpha\sigma_j^{-1} \otimes \sigma_j\beta\sigma_j^{-1})(a\otimes b)$$

$$= c''(\alpha\otimes\beta)(a\otimes b)$$

$$= c'(\alpha\otimes r(\beta))(a\otimes b).$$

Es gilt also

$$v(c'(\alpha), \beta) = c'(u(\alpha, r(\beta)) \text{ für } \alpha \in \mathrm{Hom}_H(A^*,A) \text{ und } \beta \in \mathrm{Hom}_G(B^*,B).$$

Wir setzen für A* und B* eine projektive Auflösung P_* des trivialen G-Moduls $\mathbb{Z}$ ein und gehen zu den Kohomologie-Klassen über. Die Identiät bekommt dann die Gestalt[138]

$$\mathrm{Cor}([\alpha])\bigcup[\beta] = \mathrm{Cor}([\alpha] \bigcup \mathrm{Res}([\beta])),$$

d.h. wir erhalten gerade die behauptete Identität.
QED.

3.4.13 Der Fall der endlichen zyklischen Gruppen

Seien $G = \mathbb{Z}/n\mathbb{Z}$ die endliche zyklische Gruppe der Ordnung n und

$$\chi \in H^1(G, \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Hom}_{Ab}(G, \mathbb{Z}/n\mathbb{Z})$$

der Gruppen-Homomorphismus, welcher der identischen Abbildung entspricht. Dann gelten folgende Aussagen.

(i) Bezeichnet δ: $H^1(G, \mathbb{Z}/n\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z})$ den Zusammenhangs-homomorphismus zur exakten Sequenz

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0,$$

so ist $\delta(\chi)$ ein Erzeuger der zyklischen Gruppe $H^2(G, \mathbb{Z})$.

(ii) Für jeden G-Modul A werden die von 3.2.9 kommenden Isomorphimen[139]

$$H^i(G, A) \xrightarrow{\cong} H^{i+2}(G, A)$$

induziert durch das Cup-Produkt mit $\delta(\chi)$.

(iii) Der Isomorphismus

$$A^G/NA \xrightarrow{\cong} H^2(G, A)$$

wird induziert durch die Abbildung, welche die Elemente von $A^G = H^0(G,A)$ in das Cup-Produkt mit $\delta(\chi)$ überführt.

Beweis. Zu (i).Wir verwenden die freie Auflösung[140]

(1) $$P_*: \ ... \longrightarrow \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

von 3.2.9 zur Berechnung der Kohomologie von G. Zur Bestimmung des Bildes von

---

[135] weil β ein G-Homomorphismus ist.
[136] weil G über die Diagonal-Einbettung auf dem Tensorprodukt operiert.
[137] da c'' auf den H-Homomorphismen definiert ist, können wir den G-Homomorphismus β als H-Homomorphismus auffassen.
[138] nach Restriktion auf die Diagonale.
[139] d.h. $H^{2i}(G, A) = A^G/NA$ und $H^{2i+1}(G, A) = {}_NA/(\sigma-1)A$.
[140] Dabei bezeichne σ einen Erzeuger von G und N ist die Multiplikation mit der Summe der Elemente von G.

$$\chi \in H^1(G, \mathbb{Z}/n\mathbb{Z}) = H^1(\ \mathrm{Hom}_G(P_*, \mathbb{Z}/n\mathbb{Z})$$

beim Zusammenhangshomomorphismus wählen wir einen Repräsentanten von χ, d.h. einen G-Homomorphismus

$$\alpha\colon \mathbb{Z}[G] \longrightarrow \mathbb{Z}/n\mathbb{Z} \text{ mit } \alpha\circ N = 0^{141}.$$

Dieser G-Homomorphismus muß surjektiv sein[142], d.h. es gibt einen Erzeuger $\sigma\in G$ mit

$$\alpha(\sigma) = 1 \bmod n.$$

Wir heben α an zu einem G-Homomorphismus

$$\widetilde{\alpha}\colon \mathbb{Z}[G] \longrightarrow \mathbb{Z}.$$

Zum Beispiel können wir $\widetilde{\alpha}$ festlegen durch die Bedingung

$$\widetilde{\alpha}(\sigma) = 1$$

(was wir tun wollen). Wegen $\alpha\circ N = 0$ gilt $\mathrm{Im}(\widetilde{\alpha}\circ N) \subseteq n\mathbb{Z}$, d.h. es gibt eine eindeutig bestimmte Abbildung

$$\overline{\alpha}\colon \mathbb{Z}[G] \longrightarrow \mathbb{Z} \text{ mit } \widetilde{\alpha}\circ N = n\bullet\alpha'.$$

Diese repräsentiert das Bild von χ beim Zusammenhangshomomorphismus,

$$\delta(\chi) = [\overline{\alpha}] \in H^2(G, \mathbb{Z}) =^{143} \mathbb{Z}^G/N\mathbb{Z} =^{144} \mathbb{Z}/n\mathbb{Z}.$$

Als Element der Gruppe $\mathbb{Z}/n\mathbb{Z}$ ist[145]

$$\delta(\chi) = \overline{\alpha}(1) \bmod n\mathbb{Z}.$$

Nach Konstruktion gilt

$$\begin{aligned} n\bullet\overline{\alpha}(\sigma) &= \widetilde{\alpha}(N\sigma) \\ &= N\widetilde{\alpha}(\sigma) && \text{(weil } \widetilde{\alpha} \text{ ein G-Homomorphismus ist).} \\ &= n\bullet\widetilde{\alpha}(\sigma) && \text{(weil G trivial auf } \mathbb{Z} \text{ operiert)} \\ &= n\bullet 1 && \text{(nach Wahl von } \widetilde{\alpha}) \end{aligned}$$

d.h. $\overline{\alpha}(\sigma) = 1$. Insbesondere ist $\delta(\chi) = \overline{\alpha}(1) \bmod n\mathbb{Z}$ ein Erzeuger von $\mathbb{Z}/n\mathbb{Z}$.

Zu (ii). Betrachten wir das folgende kommutative Diagramm

$$\begin{array}{ccccccc}
\ldots\longrightarrow & \mathrm{Hom}(\mathbb{Z}[G],A) & \xrightarrow{N_*} & \mathrm{Hom}(\mathbb{Z}[G],A) & \xrightarrow{(\sigma-1)_*} & \mathrm{Hom}(\mathbb{Z}[G],A) & \longrightarrow\ldots \\
& \otimes\overline{\alpha}\downarrow & & \otimes\overline{\alpha}\downarrow & & \otimes\overline{\alpha}\downarrow & \\
\ldots\longrightarrow & \mathrm{Hom}(\mathbb{Z}[G\times G],A) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}[G\times G],A) & \longrightarrow & \mathrm{Hom}(\mathbb{Z}[G\times G],A) & \longrightarrow\ldots \\
& \downarrow\mathrm{Res} & & \downarrow\mathrm{Res} & & \downarrow\mathrm{Res} & \\
\ldots\longrightarrow & \mathrm{Hom}(\mathbb{Z}[G],A) & \xrightarrow{N_*} & \mathrm{Hom}(\mathbb{Z}[G],A) & \xrightarrow{N_*} & \mathrm{Hom}(\mathbb{Z}[G],A) & \longrightarrow\ldots
\end{array}$$

Die erste und die letzte Zeile entstehe dabei duch Anwenden den Funktors $\mathrm{Hom}_G(?, A)$ auf die Auflösung (1). Die oberen vertikalen Abbildung seien definiert durch das

---

[141] die Bedingung muß erfüllt sein, weil α ein Zyklus ist.

[142] Andernfalls wäre $\mathrm{Im}(\alpha)$ eine echte Untergruppe von $\mathbb{Z}/n\mathbb{Z}$, d.h. es gäbe einen echten Teiler m von n mit $m\bullet\alpha = 0$. Dann wäre aber auch $m\bullet\chi = 0$, was nicht der Fall ist, da χ die identische Abbildung ist.

[143] Nach 3.2.9.

[144] Weil G trivial auf $\mathbb{Z}$ operiert.

[145] vgl. die Berechnung der Kohomologie mit Hilfe der Auflösung (1) in 3.2.9.

Tensorprodukt mit der oben konstruierten Abbildung $\overline{\alpha}$. Die unteren Restriktionsabbildungen sollen von Diagonal-Einbettung $G \hookrightarrow G \times G$ kommen. Die Zusammensetzung von $\overline{\alpha}$ mit diesen Restriktionen ist somit gerade das Tensorprodukt mit $\delta(\chi)$.

Die horizontalen Abbildungen in der Mitte sind ebenfalls die Multiplikation mit $\sigma - 1$ bzw. mit N = Summe der Elemente von G, genommen bezüglich der diagonalen Operation von G auf diesen Moduln. Die Kommutativität des Diagramm macht die vertikalen Abbildungen zu Komplex-Morphismen. Diese induzieren also Abbildungen auf der Kohomologie.

Ein G-Homomorphismus der oben Zeile, welcher σ in ein Element $a \in A$ abbildet,

$$\sigma \mapsto a,$$

entspricht dabei in der mittleren Zeile dem $G \times G$-Homomorphimus mit

$$(\sigma, \sigma) \mapsto a \otimes 1 = a.$$

Durch Einschränkung auf die Diagonale erhält man den alten G-Homomorphismus zurück. Die Zusammensetzungen der vertikalen Abbildungen sind also gerade identischen Abbildungen, induzieren also auf der Kohomologie Isomorphismen. Die auf der Kohomologie induzierten Abbildungen fallen aber - auf Grund von deren ursprünglicher Beschreibung mit dem Cup-Produkt zusammen (welches den Grad der Komplexe um 2 verschiebt). Damit ist Aussage (ii) bewiesen.
Zu (iii). Man verwendet dieselben Argumente wie im Beweis von (ii). Im Unterschied zu (ii) muß man diesmal jedoch die rechte Spalte des Diagramms durch Null-Moduln und Null-Abbildungen ersetzen. Die Kommutativität des Diagramm bleibt dabei erhalten.
QED.

Aufgaben

1.

Sei Φ: $G' \longrightarrow G''$ ein Gruppen-Homomorphismus. Man versehe jeden G''-Modul A mit der G'-Operation, die von Φ kommt. Man zeige, es gibt genau eine Familie von Homomorphismen

$$\Phi^i_A : H^i(G'', A) \longrightarrow H^i(G', A) \text{ mit } i = 0, 1, ...$$

und A beliebig, so daß für jede kurze exakte Sequenz

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

von G''-Moduln die folgenden Diagramm kommutativ sind.

$$\begin{array}{ccccccc} H^i(G'',A) & \longrightarrow & H^i(G'',B) & \longrightarrow & H^i(G'',C) & \longrightarrow & H^{i+1}(G'';A) \\ \Phi^i_A\downarrow & & \Phi^i_B\downarrow & & \Phi^i_C\downarrow & & \Phi^{i+1}_A \\ H^i(G'',A) & \longrightarrow & H^i(G',B) & \longrightarrow & H^i(G',C) & \longrightarrow & H^{i+1}(G';A) \end{array}$$

Anmerkung: dies ermöglicht insbesondere eine alternative Konstruktion der Restriktions- und Inflationsabbildungen.

2.

Seien G eine Gruppe und $H \subseteq G$ eine Untergruppe mit endlichem Index n und A ein G-Modul. Weiter sei

$$\rho_1, .., \rho_n \in G$$

ein volles Repräsentantensystem von G/H in G.

(a) Man zeige, daß die Abbildung

$$\mathrm{Cor}^0\colon A^H \longrightarrow A^G,\ x \mapsto \sum_{j=1}^{n} \rho_j x\,,$$

nicht von der speziellen Wahl der ρ_j abhängt.

(b) Man zeige, die Korestriktionsabbildungen $H^i(H, A) \longrightarrow H^i(G, A)$ sind die einzigen Abbildungen, die für $i = 0$ mit der in (a) definierten Abbildung zusammenfallen und eine Eigenschaft besitzen, die zu der in Aufgabe 1 beschriebenen analog ist.

3.

In der Situation von Aufgabe 2 sei H sogar ein Normalteiler von G. Für jedes $i = 0$ bezeichne $N_{G/H}$ die Abbildung

$$N_{G/H}\colon H^i(H, A) \longrightarrow H^i(H, A),\ x \mapsto \sum_{j=1}^{n} \rho_{j^*} x.$$

(a) Man zeige, die Definition von $N_{G/H}$ hängt nich von der speziellen Wahl der ρ_j ab.

(b) Man zeige, es gilt gilt $\mathrm{Res} \circ \mathrm{Cor} = N_{G/H}$.

4.

Man beweise, daß man mit Hilfe der Standard-Auflösungen die folgende Beschreibung des Cup-Produkts angeben kann: werden

$a \in H^i(G, A)$ durch den i-Kozyklus $(\sigma_1,...,\sigma_i) \mapsto a_{\sigma_1,...,\sigma_i}$ und

$b \in H^j(G, B)$ durch den j-Kozyklus $(\sigma_1,...,\sigma_j) \mapsto b_{\sigma_1,...,\sigma_j}$

repräsentiert, so wird

$a \cup b \in H^{i+j}(G, A \otimes B)$

repräsentiert durch den (i+j)-Kozyklus

$$(\sigma_1,...,\sigma_{i+j}) \mapsto a_{\sigma_1,...,\sigma_i} \otimes \sigma_1 ... \sigma_i (b_{\sigma_{i+1},...,\sigma_{i+j}}).$$

5.

Man gebe eine explizite Interpretation mit Hilfe von Gruppen-Erweiterungen des folgenden Teils der exakten Sequenz von 3.3.15 an:

$$H^1(H, A)^{G/H} \longrightarrow H^2(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^2(G, A).$$

Der Einfachheit halber nehme man an, daß H trivial auf A operiert.

6.

Seien G eine endliche zyklische Gruppe mit dem Erzeuger $\sigma \in G$ und A, B G-Moduln.

(a) Man gebe eine explizite Beschreibung der Paarung

$$(A^G/NA) \times ({}_NB/(\sigma\text{-}1)B) \longrightarrow {}_N(A \otimes B)/(\sigma\text{-}1)(A \otimes B)$$

an, die vom Cup-Produkt

$$H^{2i+1}(G,A) \times H^{2j+1})(G, B) \longrightarrow H^{2i+2j+1}(G, A \otimes B)$$

vermittels der Isomorphismen von 3.2.9 kommt.

(b) Die analogen Fragen für

$$(A^G/NA) \times (B^G/NB) \longrightarrow (A \otimes B)^G/N(A \otimes B)$$

und

$$({}_N A/(\sigma\text{-}1)A) \times ({}_N B/(\sigma\text{-}1)B) \longrightarrow (A \otimes B)^G/N(A \otimes B)$$

Index

—I—

—J—

—K—

—L—

—M—

—N—

—O—

—P—

Inhalt