Einführung in die algebraische K-Theorie

Sommersemester 2001

Di 9.15-10.45 Seminargebäude 4-10
Fr 13.15-14.45 Seminargebäude 4-10

frei nach:

Gille & Szamuely: Central simple algebras
Cassels & Fröhlich: Algebraic number theory.

1. Einführung

1.1 Zu den Ursprüngen der K-Theorie:

1.1.1 Topologische K-Theorie

- Vektorraumbündel[1]
- die K-Gruppe von Grothendieck[2]
- Ähnlichkeiten mit der Kohomologie-Theorie[3]
- Problem: die höheren K-Gruppen

---

[1] Der Satz vom Igel, oder allgemeiner die Frage nach der Existenz gewisser Vektorraumfelder zum Beispiel auf den Sphären.
Siehe auch

Husemoller, D.: Fibre bundles, McGraw-Hill Book Company, New York 1966.

In engem Zusammenhang dazu steht die Frage nach der Berechnung von Homotopie-Gruppen.

Spanier, E.: Algebraic topology, McGraw-Hill Book Company, New York 1966 (Chapter 9)
Toda, H.: Composition methods in the homotopy groups of spheres, Ann. Math. Studies 49, Princeton 1962

(Darstellungen der Lorentz-Gruppe auf Vektorraumbündeln und Elementarteilchen).

[2] Sei X ein topologischer Raum (eventuell mit irgendeiner Zusatzstruktur). Man betrachtet die von allen Vektorraum-Bündeln (mit Zusatzstruktur) erzeugte freie abelsche Gruppe

$$F(X)$$

und faktorisiert nach der Untergruppe

$$R(X)$$

die erzeugt wird von allen Elementen der Gestallt

$$V - V' - V''$$

für jede kurze exakte Sequenz von Vektorraum-Bündeln über X,

(1) $$0 \longrightarrow V' \longrightarrow V \longrightarrow V'' \longrightarrow 0.$$

Mit anderen Worten, man macht die Vektorraum-Bündel über X zu einer Gruppe, wobei für jede kurze exakte Sequenz gilt

$$V = V' + V''.$$

Die entstehende Gruppe

$$K(X) = F(X)/R(X)$$

heißt K-Gruppe von X. Ihre Element lassen sich repräsentieren durch Differenzen

$$V_1 - V_2$$

von Vektorraum-Bündeln.

[3] Siehe zum Beispiel

Karoubi, M.: K-Theory, An Introduction, Springer Berlin 1978

oder auch Kapitel 11 in

Switzer, R.M.: Algebraic topology - homotopy and homology, Springer Berlin 1975

1.1.2 Algebraische K-Theorie

- Viele Versuche, eine algebraische Verallgemeinerung zu konstruieren[4].
  Ein früher Versuch führt zur

  Milnor-K-Theorie.[5]

- Die finale Konstruktion liefert ein K-Theorie für fast jede additive Kategorie:

  Quillen-K-Theorie[6].

---

[4] Beispiel: Sei der betrachtete topologische Raum durch ein polynomailes Gleichungssystem

$$f_1(x_1,...,x_n) = ... = f_m(x_1, ... , x_n) = 0$$

mit Polynomen, deren Koeffizienten in einem Körper K liegen,

$$f_1, ... , f_m \in K[x_1, ... , x_n],$$

so kann man den Raum X mit der Menge

$$\text{Spec } R$$

identifizieren. Anstelle von topologischen Räumen kann man also kommutative Ringe R mit Eins betrachten. Die Vektorraum-Bündel entsprechen dabei gerade den projektiven R-Moduln (bei Bündeln, deren Übergangsfunktionen algebraische Funktionen sind). Man erhält so eine K-Gruppe

$$K(R) = F(R)/I((R),$$

wobie F(R) die freie abelschen Gruppe ist, die von den endlich erzeugten projektiven R-Moduln erzeugt wird und I(R) die Untergruppe der Elemente der Gestalt

$$M - M' - M'',$$

mit projektiven R-Moduln M, M', M'', die sich in eine kurze exakte Sequenz

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

einfügen lassen.
der Primideal des Rings

$$R := K[x_1, ... , x_n]/(f_1, ... , f_m)$$

[5] Siehe

Milnor, J.: Algebraic K-theory and quadratic forms, Invent. Math. 9 (1970), 318-344

oder

Milnor, J.: Introduction to algebraic K-theory, Princeton University Press & University of Tokyo Press, Princeton, New Jersey, 1974

Bei der Definition der K-Gruppen von Milnor beschränken wir uns hier auf den Fall der K-Gruppen eines Körper.
Seien k ein Körper und n eine nicht-negative ganze Zahl. Im Fall n > 1 ist die n-te K-Gruppe von Milnor,

$$K_n^M(k) := (k^*)^{\otimes n} / < a_1 \otimes ... \otimes a_n \mid \text{es gibt i, j mit } a_i + a_j = 1 >,$$

definiert als Faktorgruppe der n-ten Tensorpotenz

$$(k^*)^{\otimes n} = k^* \otimes_{\mathbb{Z}} ... \otimes_{\mathbb{Z}} k^* \text{ (n-mal)}$$

der multiplikativen Gruppe k* von k modulo der Untergruppe, die erzeugt wird von allen Tensorprodukten

$$a_1 \otimes ... \otimes a_n \text{ mit } a_1, ... , a_n \in k^* ,$$

in denen es zwei Faktoren gibt, deren Summe gleich 1 ist,

$$a_i + a_j = 1.$$

[6] Siehe:

Quillen, D.: Higher K-theory I, Lecture Notes in Math. 342 (1973), 77-139.

Sei

$$\mathcal{M} \subset \mathcal{A}$$

eine additive Kategorie, die als volle Teilkategorie in eine abelsche Kategorie $\mathcal{A}$ eingebettet ist. Wir nehmen weiter an, $\mathcal{M}$ ist abgeschlossen gegenüber Erweiterungen, d.h. für jede kurze exakte Sequenz

$$0 \longrightarrow M' \longrightarrow A \longrightarrow M'' \longrightarrow 0$$

in $\mathcal{A}$ mit $M', M'' \in \mathcal{M}$ ist A isomorph zu einem Objekt von $\mathcal{M}$. Dann kann man eine neue Kategorie

$$Q(\mathcal{M})$$

konstruieren, die dieselben Objekte hat wie $\mathcal{M}$, in welcher ein Morphismus

$$M' \longrightarrow M$$

definiert ist als ein Isomorphismus

$$M' \xrightarrow{\cong} M_1/M_0$$

von M' mit einem Subquotienten von M mit Teilobjekten $M_0 \subseteq M_1 \subseteq M$, welche M_0 umd M/M_1 isomorph sind zu Objekten von $\mathcal{M}$. Äquivalent, Morphismen von $Q(\mathcal{M})$ sind Isomorphie-Klassen von Diagrammen der Gestalt

$$M' \twoheadleftarrow N \rightarrowtail M$$

(wobei die Isomorphismen Identitäten auf M' und M induzieren sollen), wobei jeder der beiden Morphismen zulässen sein soll, d.h. er definiert eine Sequenz in $\mathcal{M}$, die kurz-exakt in $\mathcal{A}$ ist. Diese Kategorie $Q(\mathcal{M})$ definiert einen sogenannten klassifizierenden Raum

$$BQ(\mathcal{M}).$$

Die i-te Quillen-K-Gruppe ist dann definiert als (i+1)-te Homotopie-Gruppe dieses Raums,

$$K_i(M) := \pi_{i+1}(BQ(\mathcal{M}), 0).$$

Zur Definition des klassifizierenden Raums einer Kategorie: sei $\mathcal{C}$ eine (kleine) Kategorie. Der Nerv

$$N(\mathcal{C})$$

dieser Kategorie ist dann definiert als die (semi-) simpliziale Menge, derem p-simplexe gerade die die Diagramme von $\mathcal{C}$ der Gestalt

(1) $$S: X_0 \longrightarrow X_1 \longrightarrow ... \longrightarrow X_p \ .$$

Die Seiten eines solchen Simplexes erhält man, indem man Objekte X_i wegläßt (und die ensprechenden Morphismen durch deren Zusammensetzung ersetzt). Die Entartungen eines solchen Simplexes erhält man, indem man Objekte X_i durch identische Morphismen $X_i \xrightarrow{id} X_i$ ersetzt. Der klassifizierende Raum der Kategorie $\mathcal{C}$ ist dann definiert als die geometrische Realisierung

$$B(\mathcal{C})$$

von $N(\mathcal{C})$, d.h. für jedes p-Simplex (1) wählt man ein Exemplar Δ (S) des p-dimensionenalen Standard-Simplex

$$\Delta_p := \{ x = (x_0,...,x_p) \in \mathbb{R}^{p+1} \mid \sum_{i=0}^{p} x_i = 1, 0 \le x_i \}$$

wobei man die i-te Ecke von Δ_p mit X_i identifiziert. Ist S' ein Teildiagramm von S, so identifiziert man $\Delta(S')$ in natürlicher Weise mit einem Teilsimplex von $\Delta(S)$, indem man die Ecken identifiziert. Die geometrische Realisierung erhält man, indem man die Simplexe $\Delta(S)$ entlang gemeinsamer Teilsimplexe verklebt.

- Es gibt Verallgemeinerungen durch Axiomatisierung gewisser Eigenschaften der Faserbündel der algebraischen Topologie: Homotopische Algebra.[7]

1.2 Zur Einordnung dieser Vorlesung

- Die Kenntnis der Quillen-K-Gruppen ist extrem interessant aber gleichzeitig sehr schwierig.
- Quillen-K-Theorie ist in erster Linie eine Ansammlung von Problemen.
- Selbst die einfachsten K-Gruppen lassen sich nur in Ausnahme-Fällen berechnen.
- Für die Berechnung der K-Gruppen einpunktiger Räume (des Spektrums eines Körpers) gibt es eine Vermutung: die

  Bloch-Kato-Vermutung

  Sie besagt im wesentlichen, daß im Körper-Fall die Quillen-K-Gruppen mit den Milnor-K-Gruppen übereinstimmen.
- Die Quillen-K-Gruppen spielen hier die Rolle des interessierenden qualitativen Objekts und die Milnor-K-Gruppen die des Kochrezepts, mit dessen Hilfe man dieses Objekt ausrechnen kann.

1.3 Gegenstand der Vorlesung

Ziel der Vorlesung ist es nicht, eine systematische Darstellung der algebraischen K-Theorie zu geben. Statt dessen soll an einem möglichst einfachen Beispiel demonstriert werden, wozu die algebraische K-Theorie gut ist (es gibt viele andere Beispiele). Unser Programm besteht im wesentlichen aus den folgenden Punkten.

- Beschreibung der Bloch-Kato-Vermutung
  (unter Vermeidung der explizen Definition der Quillen-K-Funktoren)
- Beweis eines Spezialfalls der Bloch-Kato-Vermutung
- Anwendung dieses Spezialfalls auf die Klassifikation der zentralen einfachen Algebren. Genauer, wir wollen den Satz von Merkurjev beweisen. Beschreiben wir diesen Satz.

1.4 Zentrale einfache Algebren und der Satz von Merkurjev

1.4.1 Definition, Beispiele und erste Eigenschaften zentraler einfacher Algebren

Erinnern wir an die Definition des Begriffs der zentralen einfachen Algebra.
Eine Algebra über einem Körper k ist nach Defintion ein endlich-dimensionaler k-Vektorraum A zusammen mit einer k-bilinearen Abbildung

$$A \times A \longrightarrow A,$$

durch welche A die Struktur eines (nicht-notwendig kommutativen) Rings mit 1 bekommt. Dabei soll die Abbildung

$$k \longrightarrow A, c \mapsto c \cdot 1,$$

ein Homomorphismus von Ringen mit 1 sein, dessen Bild im Zentrum

$$Z(A) := \{ a \in A \mid ax = xa \text{ für jedes } x \in A\}$$

von A liegt.

Bemerkung
Diese Abbildung ist injektiv (weil k ein Körper ist), und wir werden im allgemeinen k mit seinem Bild in A identifizieren.

---

[7] Siehe auch:
Quillen, D.: Homotopical Algebra, Lecture Notes in Math. 43 (1967).
Hirschhorn, P.S.: Model categories and their localizations, Mathematicl Surveys and Monographs 99, Amer. Math. Soc. 2003.
Mazza, C., Voevodsky, V., Weibel, C.: Notes on motivic cohomology (publiziert in Internet).

Eine solche k-Algebra A heißt zentral, wenn ihr Zentrum gleich k ist,

$$Z(A) = k.$$

Eine solche k-Algebra A heißt einfach, wenn sie außer 0 und A selbst keine weiteren zweiseitigen Ideale besitzt.

Bemerkungen

(i) Beispiele von einfachen Algebren sind die Erweiterungskörper von k und die Schiefkörper, deren Zentrum k enthält.

(ii) Die volle Matrizen-Algebra

$$M_n(k) = k^{n \times n}$$

d.h. die Algebra der $n \times n$-Matrizen mit Einträgen aus k, ist eine einfache k-Algebra.

(iii) Für jede einfache k-Algebra A ist das Zentrum

$$Z(A) \ (\supseteq k)$$

ein Körper, d.h. A ist eine zentrale einfache Algebra über dem Körper Z(A).). Die Bedingung, zentral zu sein läßt sich für einfache Algebren also stets dadurch realisiern, daß man den Grundkörper geeignet vergrößert.

Um einzusehen, daß Z(A) tatsächlich ein Körper ist, benötigt man den Satz von Wedderburn, der im folgenden auch anderweitig eine wichtige Rolle spielen wird.

Satz von Wedderburn.
Sei A eine (endlich-dimensionale) einfache Algbra über einem Körper k. Dann gibt es eine natürliche Zahl n und eine Divisionsalgebra[8] $D \supseteq k$ derart, daß A isomorph ist zur Matrizen-Algebra $M_n(D)$,

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

Die Divisionsagebra D ist dabei bis auf Isomorphie durch A eindeutig bestimmt.[9]

Wenden wir den Satz von Wedderburn an: das Zentrum von A, d.h. der Matrizen-Algebra $M_n(D)$ ist gerade das Zentrum von D, d.h. es ist

$$k \subseteq Z(A) \subseteq D \subseteq M_n(D) \cong A.$$

Insbesondere ist Z(A) nullteilerfrei und damit als endlich-dimensionaler k-Vektorraum selbst ein Körper.

(iv) Man kann zeigen, das Tensorprodukt

$$A' \otimes_k A''$$

zweier zentraler einfacher k-Algebren A' und A'' ist eine zentrale einfache k-Algebra.

(v) Man kann zeigen, für jede zentrale einfache k-Algebra und jede Körper-Erweiterung k'/k ist

$$A \otimes_k k'$$

eine zentrale einfache k'-Algebra. Dabei kann man k' so wählen, daß dieses Tensorprodukt isomorph wird zu einer vollen Matrizen-Algebra über k' (es gibt ein solches k', welches endlich und separabel über k ist). Man sagt dann, A zerfällt über k' und k' ist eine Zerfällungskörper von A.

(vi) Umgekehrt ist eine k-Algebra A genau dann zentral und einfach, wenn es eine Körper-Erweiterung k'/k gibt, für welche $A \otimes_k k'$ isomorph ist zu einer vollen

---

[8] d.h. einen Schiefkörper, den den Körper k in seinem Zentrum enthält.

[9] G & S, 2.1.5

Matrizen-Algebra über k' (Man kann dabei stets k'/k endlich und separabel wählen).

(vii) Das einfachste Beispiel einer (nicht-trivialen) zentralen einfachen k-Algebra ist die Quaternionen-Algeba

$$(a, b) \text{ mit } a, b \in k^*.$$

Sie ist definiert als der 4-dimensionale k-Vektorraum mit der Basis 1, i, j, ij, wobei die Multiplikation der Algebra durch die folgende Relationen gegeben ist

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

(die Charakteristik von k sei dabei $\neq 2$).

Im Fall $k = \mathbb{C}$ und a = b = -1 erhät man gerade die klassische Quaternionen-Algebra von Hamilton.

Die Quaternionen-Algebren (a,b) sind im allgemeinen nicht isomorph zur vollen Matrizen-Algebra $M_2(k)$. Genauer gilt (vgl. [G & S], 1.1.11):

(viii) Seien k ein Körper der Charakteristik $\neq 2$ und $a,b \in k^*$. Dann sind äquivalent:

1. Die k-Algbra (a,b) zerfällt.
2. Die k-Algebra (a, b) ist kein Schiefkörper.
3. Die Norm $N: (a, b) \longrightarrow k, q \mapsto q \bullet \overline{q}$, besitzt eine nicht-triviale Nullstelle.
4. Das Element b ist Norm eines Element der Körper-Erweiterung $k(\sqrt{a})/k$.

(ix) Die Quaternionen-Algebren besitzen eine weitere bemerkenswerte Eigenschaft: Das Tensor-Quadrat einer jeden Quaternionen-Algebra zerfällt.

Bevor wir weitere Beispiele für zentrale einfache Algebren angeben, wollen wir für diese letzte Eigenschaft der Quaternionen-Algebren eine alternative Beschreibung angeben.

1.4.2 Die Brauer-Gruppe eines Körpers

Sei k ein Körper. Zwei zentrale einfache k-Algebren A und A' heißen Brauer-äquivalent, wenn es natürliche Zahlen m und m' gibt mit

$$A \otimes_k M_m(k) \cong A' \otimes_k M_{m'}(k)$$

Die Brauer-Äquivalenz ist eine Äquivalenz-Relation auf der Menge der zentralen einfachen k-Algebren (und auch auf der Menge der zentralen einfachen k-Algebren, die über einer gegeben Körper-Erweiterung k'/k zerfallen). Wir bezeichnen mit

$$Br(k)$$

die Menge der Brauer-Äquivalenzklassen aller zentraler einfacher Algebren über k und mit

$$Br(k'/k) \subseteq Br(k)$$

die Menger der Brauer-Äquivalenzklassen der über k' zerfallenden zentralen einfachen k-Algbren. Wie oben bemerkt gilt

$$Br(k) = \bigcup_{k \subseteq k'} Br(k'/k).$$

Nach Wedderburn hat jede zentralen einfache k-Algebra A die Gestalt

$$A \cong M_n(D)$$

mit einer Divisionsalgebra D, die durch A eindeutig festgelegt ist und deren Zentrum gleich k ist. Nach Definition sind A und D Brauer-Äquivalent. Jedes Element von

$$Br(k)$$

wird somit durch eine Divisionsalgebra repräsentiert. Sind D und D' zwei Divisonsalgebren, die dasselbe Element von Br(k) repräsentieren, so gilt nach Definition

$$M_m(D) \cong M_{m'}(D')$$

für geeignet gewählte natürliche Zahlen m und m'. Nach dem Satz von Wedderburn sind dann aber D und D' isomorph über k. Wir haben damit gezeigt:

$$\mathrm{Br}(k) = \left\{ \begin{array}{c} \text{Menge der Isomorphieklassen der zenralen} \\ \text{einfachen Divisionsalgebren über k} \end{array} \right\}$$

$$\mathrm{Br}(k'/k) = \left\{ \begin{array}{c} \text{Menge der Isomorphieklassen der zenralen} \\ \text{einfachen Divisionsalgebren über k} \\ \text{welche über k' zerfallen} \end{array} \right\}$$

Wie oben bemerkt, ist das Tensorprodukt von zwei zentralen einfachen k-Algebren eine zentralen einfache k-Algebra. Die beiden Mengen Br(k) und Br(k'/k) sind deshalb mit einer assoziativen Multiplikation versehen. Wegen

$$A \otimes_k k \cong A$$

besitzt diese Multiplikation ein neutrales Element (die Äquivalenzklasse von der k-Algebra k). Für jede zentrale einfache k-Algebra A ist die duale k-Algebra

$$A^{op},$$

die aus denselben Elementen wie A besteht und deren Multiplikation sich von der Multiplikation von A in der Reihenfolge der Faktoren unterscheidet,

$$a \bullet_{op} b = b \bullet a,$$

wieder eine zentrale einfache k-Algebra. Man kann zeigen, es gilt

$$A \otimes_k A^{op} = \mathrm{End}_k(A)$$

(vgl. [G & S] 2.4.10). Die k-Algbra auf der rechten Seite ist aber isomorph zu einer vollen Matrizen-Algebra über k. In Br(k) ist somit das Produkt von A und A^{op} gerade das neutrale Element der Multiplikation, d.h. A und A^{op} sind zueinander inverse Element. Wir haben damit gezeigt, Br(k) und Br(k'/k) sind Gruppen.

Br(k) heißt Brauer-Gruppe des Körpers k.
Br(k'/k) heißt relative Brauer-Gruppe des Körpers k.

Bemerkungen

(i) Die oben erwähnte Eigenschaft 1.4.1 (ix) der Quaternionen-Algebren übersetzt sich jetzt in die Aussage, daß die (nicht-zerfallenden) Quaternionen-Algebren Elemente der Ordnung 2 in der Brauer-Gruppe repräsentieren.

(ii) Dies legt die Frage nahe, ob es auch Algebren gibt, die Elemente mit einer von 2 verschiedenen Ordung repräsentieren. Es wird sich herausstellen, daß die Suche nach solchen Elementen der Brauer-Gruppe uns letztlich zu allen zentralen einfachen Algebren führen wird.
Der zentrale Punkt bei dieser Suche ist eine alternative Beschreibung der Brauer-Gruppe, nämlich als Galois-Kohomologie-Gruppe.

(iii) Aus den oben angegebenen Eigenschaften zentraler einfacher Algebren ergibt sich,

$$\mathrm{Br}(k) = 0$$

falls k algebraisch abgeschlossen ist. Mit anderen Worten, über algebraisch abgeschlossenen Körpern gibt es nur eine Divisionsalgebra, nämlich k selbst.

(iv) Die Beschreibung der Brauer-Gruppe als Kohomologie-Gruppe gestattet es, die Brauer-Gruppen in besonders einfachen Fällen zu berechnen. Insbesondere kann man zeigen,[10]

---

[10] Es gilt (nach Cassels & Fröhlich, Algebraic number theory, V, 2.8)

$$\mathrm{Br}(\mathbb{R}) = H^2(G(\mathbb{C}/\mathbb{R}), \mathbb{C}^*)$$

Dabei bezeichne G die Galois-Gruppe der separablen Abschließung $\mathbb{C}$ von $\mathbb{R}$. Weil $G = \mathbb{Z}/2\mathbb{Z}$ zyklisch ist, folgt (Cassels & Fröhlich, Algebraic number theory, V, §8)

$$\mathrm{Br}(\mathbb{R}) = (\mathbb{C}^*)^G/N(\mathbb{C}^*).$$

$$\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}.$$

Mit anderen Worten, über $\mathbb{R}$ gibt es nur zwei Divisionsalgebren: $\mathbb{R}$ selbst und Hamiltonschen Quaternionen $\mathbb{H}$.

(v) Die Galois-Kohomologie steht in Beziehung zur Quillen-K-Theorie. In unserer Formulierung der Bloch-Kato-Vermutung wird die Galois-Kohomologie die Stelle der Quillen-K-Theorie einnehmen (vgl. [G & S], 4.6.7).

(v) Unser nächstes Ziel ist die Einführung der Galois-Kohomologie. Zu diesem Zwecke müssen wir mehrere Kohomologie-Theorien einführen:

Gruppen-Kohomologie
Gruppen-Homologie
Tate-Kohomologie
Galois-Kohomogie

1.4.3 G-Moduln

Sei G ein Gruppe. Ein G-Modul is eine abelsche Gruppe A mit G-Operation, d.h. eine abelsche Gruppe zusammen mit einer Abbildung

$$G \times A \longrightarrow A, (g, a) \mapsto ga,$$

mit

(i) $1 \bullet a = a$ für jedes $a \in A$.

(ii) $g \bullet (g' \bullet a) = (g \bullet g') \bullet a$ für beliebige $g, g' \in G$ und beliebige $a \in A$.

Bezeichne

$$\mathbb{Z}[G] = \oplus_{g \in G} \mathbb{Z} \bullet g$$

den Gruppen-Ring der Gruppe G, d.h.

$$\left(\sum_{g \in G} m_g \bullet g \right) + \left(\sum_{g \in G} n_g \bullet g \right) = \left(\sum_{g \in G} (m_g + n_g) \bullet g \right)$$

$$\left(\sum_{g \in G} m_g \bullet g \right) \bullet \left(\sum_{g \in G} n_g \bullet g \right) = \left(\sum_{g \in G} \sum_{g' \bullet g'' = g} (m_{g'} \bullet n_{g''}) \bullet g \right)$$

Beispiel: $(5 \bullet g_1 + g_2) \bullet (7 g_3 + 2 g_4) = 35 g_1 g_3 + 10 g_1 g_4 + 7 g_2 g_3 + 2 g_2 g_4$

Mit dieser Definion ist ein G-Modul nichts anderes als ein Modul über dem Ring $\mathbb{Z}[G]$.

Sei X eine beliebige abelsch Gruppe (d.h. ein $\mathbb{Z}$-Modul). Dann hat die Gruppe

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}} X$$

in natürlicher Weise die Struktur eines G-Moduls mit der G-Operation

---

Dabei ist N: $\mathbb{C}^* \longrightarrow \mathbb{R}^*$ die Norm-Abbildung und das nicht-triale Element von G operiert durch komplexe Konjugation auf $\mathbb{C}^*$, d.h. es ist

$$(\mathbb{C}^*)^G = \mathbb{R}^*$$

$$N(\mathbb{C}^*) = \{z \bullet \bar{z} \mid z \in \mathbb{C}^*\} = \{|z|^2 \mid z \in \mathbb{C}^*\} = \{r \in \mathbb{R}^* \mid r > 0\} = \mathbb{R}^*_{>0}$$

Damit ist

$$\mathrm{Br}(\mathbb{R}) = \mathbb{R}^*/\mathbb{R}^*_{>0} = \{+1, -1\} = \mathbb{Z}/2\mathbb{Z}.$$

$$g\bullet(\sigma\otimes x) = (g\sigma)\otimes x \text{ für } g\in G,\ \sigma\in\mathbb{Z}[G],\ x\in X.$$[11]

Ein G-Modul, welcher isomorph ist zu einem G-Modul dieser Gestalt, heißt induziert.

Analog hat die Gruppe

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]\ ,\ X)$$

der $\mathbb{Z}$-linearen Abbildungen $\mathbb{Z}[G] \longrightarrow X$ die Struktur eines G-Moduls mit der Operation

$$G \times \mathrm{Hom}(\mathbb{Z}[G]\ ,\ X) \longrightarrow \mathrm{Hom}(\mathbb{Z}[G]\ ,\ X),\ (\ g,\ f)\ \mapsto\ g\bullet f,$$

wobei[12]

---

[11] Sind A und B zwei G-Moduln, so besitzt deren Tensorprodukt über $\mathbb{Z}$,

$$A\otimes_{\mathbb{Z}}B,$$

in natürlcher Weise die Struktur eines G-Moduls mit

$$g\bullet(a\otimes b) = (ga)\otimes(gb) \text{ für } g\in G,\ a\in A,\ b\in B.$$

Die obige G-Modul-Struktur auf $\mathbb{Z}[G]\otimes_{\mathbb{Z}}X$ erhält man als Spezialfall, wenn man die abelsche Gruppe X als G-Modul ansieht bezüglich der trivialen Operation

$$g\bullet x = x \text{ für } g\in G \text{ und } x\in X.$$

[12] Für je zwei G-Moduln A und B besitzt die Menge

$$\mathrm{Hom}_{\mathbb{Z}}(A\ ,\ B)$$

der $\mathbb{Z}$-linearen Abbildungen $f\colon A \longrightarrow B$ die Struktur eines G-Moduls mit

$$(g\bullet f)(a) := g\bullet f(g^{-1}\bullet a) \text{ für } a \in A \text{ und } g \in G.$$

Die G-Modul-Struktur eines koinduzierten Moduls entspricht gerade dem Spezialfall

$$A = \mathbb{Z}[G] \text{ und } B = X,$$

wobei man X als G-Modul mit der trivialen G-Operation ansieht.

Der Anti-Isomorphismus

$$G \longrightarrow G,\ g \mapsto g^{-1}\ ,$$

induziert eine $\mathbb{Z}$-lineare Bijektion

$$\psi\colon\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]$$

und damit einen Isomorphismus

$$\psi* :\mathrm{Hom}(\mathbb{Z}[G]\ ,\ X) \longrightarrow \mathrm{Hom}(\mathbb{Z}[G]\ ,\ X),$$

Mit

$$(g*f)(\sigma) := f(\sigma\bullet g) \text{ sei für } g\in G,\ \sigma\in\mathbb{Z}[G],\ f \in \mathrm{Hom}(\mathbb{Z}[G]\ ,\ X).$$

gilt

$$\psi^*(g*f) = g\bullet\psi^*(f), \qquad (*)$$

d.h. die Multplikation "$\bullet$" des koinduzierten Moduls (die von der rechten G-Modul-Struktur des Gruppen-Rings $\mathbb{Z}[G]$ kommt) entspricht bei diesem Isomorphismus ψ^* gerade die Multiplikation "$*$" (die von der zur linken G-Modul-Struktur von $\mathbb{Z}[G]$ gehörigen rechten G-Modul-Struktur kommt).

Die Identität (*) beweist man durch direktes Nachrechnen: für $g'\in G$ gilt

$$\begin{aligned}(\psi^*(g*f))(g') &= (g*f)(\psi(g'))\\ &= f(\psi(g')\bullet g)\\ &= f(g'^{-1}g) = f((g^{-1}g')^{-1})\end{aligned}$$

$$(g\bullet f)(\sigma) := f(g^{-1}\bullet\sigma) \text{ sei für } g\in G,\ \sigma\in\mathbb{Z}[G],\ f\in \mathrm{Hom}(\mathbb{Z}[G]\ , X).$$

Ein G-Modul, der isomorph ist zu einem Modul dieser Gestalt heißt koinduziert.

Bemerkungen

(i) Für jedes Element $a\in A$ eines G-Moduls A und jedes Element $\sigma = \sum_{g\in G} n_g \bullet G \in$ $\mathbb{Z}[G]$ ist das Produkt

$$\sigma\bullet a = \sum_{g\in G} n_g a \in A$$

ein wohldefiniertes Element von A, d.h. jeder G-Modul A ist ein $\mathbb{Z}[G]$-Modul. Die natürliche Abbildung

$$\mathbb{Z}[G]\otimes_{\mathbb{Z}} A \longrightarrow A,\ \sigma\otimes a \mapsto \sigma\bullet a, \qquad (1)$$

ist dabei ein Homomorphismus von $\mathbb{Z}[G]$-Moduln, welcher offensichtlich surjektive ist (man setze $\sigma = 1$). Insbesondere ist jeder G-Modul ein Faktormodul eines induzierten Moduls. Wiederholt man diese Konstruktion mit dem Kern der Abbildung (1) so erhält man für jeden G-Modul A eine exakte Sequenz

$$\ldots \longrightarrow I_2 \longrightarrow I_1 \longrightarrow I_0 \longrightarrow A \longrightarrow 0$$

von G-Moduln, wobei die I_j induziert sind, d.h. wir erhalten eine Auflösung von A durch induzierte G-Moduln.

(ii) Für jedes Element $a \in A$ eines G-Moduls A definiert die Rechtsmultiplikation mit a eine $\mathbb{Z}$-lineare Abbildung[13]

$$\lambda_a : \mathbb{Z}[G] \longrightarrow A,\ \sigma \mapsto a\sigma,$$

$$= f(\psi(g^{-1}g'))$$
$$= \psi^*(f)(g^{-1}g')$$
$$= (g\bullet\psi^*(f))(g').$$

Also ist $\psi^*(g*f) = (g\bullet\psi^*(f))$.

[13] Wir verwenden hier die zur gegebenen linken G-Modul-Struktur von A gehörige rechte G-Modul-Struktur

$$a\bullet g := g^{-1}a \text{ für } a\in A \text{ und } g\in G.$$

Verwendet man die $*$-Multiplikation des koinduzierten Moduls, so muß man stattdessen die Rechtsmultiplikation

$$\rho_a : \mathbb{Z}[G] \longrightarrow A,\ \sigma \mapsto \sigma a$$

und die Einbettung

$$A \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]\ , X),\ a \mapsto \rho_a,$$

benutzen.

d.h. ein Element des koinduzierten Moduls $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]\ , X)$. Die so definierte Abbilung

$$A \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]\ , X),\ a \mapsto \lambda_a, \qquad (2)$$

ist ein Homomorphismus von G-Moduln, denn es gilt

$$\begin{aligned}
(g\bullet\lambda_a)(g') &= \lambda_a(g^{-1}g') \\
&= a\,(g^{-1}g') \\
&= (g^{-1}g')^{-1}a \quad \text{(rechte G-Modul-Struktur von A)} \\
&= g'^{-1}ga \\
&= (ga)g' \quad \text{(rechte G-Modul-Struktur von A)} \\
&= \lambda_{ga}(g'),
\end{aligned}$$

d.h.

$$g\bullet\lambda_a = \lambda_{ga}$$

für $g, g' \in G, a \in A$.[14]

Dieser Homomorphismus ist injektiv, denn aus $\lambda_a = 0$ folgt $0 = \lambda_a(1) = a$. Wir sehen so, daß jeder G-Modul Teilmodul eines koinduzierten G-Moduls ist. Wendet man dies auf den Kokern von (2) an, so erhalten wir für jeden G-Modul A eine exakte Sequenz

$$0 \longrightarrow A \longrightarrow C^0 \longrightarrow C^1 \longrightarrow C^2 \longrightarrow \ldots$$

von G-Moduln, wobei die C^j koinduziert sind, d.h. wir erhalten eine Auflösung von A durch koinduzierte G-Moduln.

(iii) Für jeden G-Modul A ist dessen invarianter Teil

$$A^G := \{a \in A \mid ga = a \text{ für jedes } g \in G\} \cong^{15} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}\ , A)$$

eine abelsche Gruppe. Auf diese Weise ist ein (additiver und linksexakter) Funktor[16]

$$G\text{-Mod} \longrightarrow Ab,\ A \mapsto A^G,$$

definiert. Dabei bezeichne

$$G\text{-Mod}$$

die Kategorie der G-Moduln und

$$Ab$$

---

[14] Für die $*$-Multiplikation des koinduzierten Moduls erhält man

$$(g\bullet\rho_a)(\sigma) = \rho_a(\sigma\bullet g) = \sigma ga = \rho_{ga}(\sigma) \text{ für } g \in G, a \in A, \sigma \in \mathbb{Z}[G].$$

[15] Die Abbildung

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}\ , A) \longrightarrow A,\ f \mapsto f(1), \qquad (*)$$

ist $\mathbb{Z}$-linear. Als $\mathbb{Z}$-lineare Abbildung ist f durch den Wert an der Stelle 1 bereits vollständig festgelegt, d.h. (*) ist injektiv. Weil G auf $\mathbb{Z}$ trivial operiert, liegt das Bild von (*) ganz in A^G. Für jedes $a \in A^G$ ist durch $f(n) = g\bullet a$ eine $\mathbb{Z}[G]$-lineare Abbildung definiert deren Bild bei (*) gleich a ist. Das Bild der Abbildung ist somit gleich A^G

[16] $A^G = \mathrm{Hom}_{Ab}(Z, A)^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.

die Kategorie der abelschen Gruppen.

(iv) Seien $A = \mathbb{Z}$ der G-Modul mit der trivialen Operation von G und $a = 1 \in \mathbb{Z}$. Dann wird die natürliche Surjektion von (i) auch mit

$$\varepsilon: \mathbb{Z}[G] \longrightarrow \mathbb{Z}, \sigma = \sum_{g\in G} n_g \bullet g \mapsto \sigma\bullet 1 = \sum_{g\in G} n_g.$$

bezeichnet und heißt Augmentation von G. Dies ist ein Homomorphismus von linken und rechten G-Moduln.[17] Der Kern der Augmentation

$$I_G := \mathrm{Ker}(\varepsilon)$$

ist somit ein zweiseitiges Ideal von $\mathbb{Z}[G]$. Es besteht aus den $\mathbb{Z}$-Linearkombinationen der Elementen der Gestalt g - e mit $g\in G$,

$$I_G =^{18} \sum_{g\in G} \mathbb{Z}\bullet(g-e)$$

und heißt Augmentationsideal.
Für jeden G-Modul A heißt die Faktorgruppe

$$A_G := A/I_G A \cong \mathbb{Z}\otimes_{\mathbb{Z}[G]} A$$

der Gruppe A auch Gruppe der Koinvarianten von A bezüglich G. Auf diese Weise ist ein (additiver und rechtsexakter) Funktor

$$\text{G-Mod} \longrightarrow \text{Ab}, A \mapsto A_G,$$

definiert.

1.4.4 Gruppen-Kohomologie

Unter der Kohomolgie einer Gruppe G versteht man eine Familie von Funktoren

$$H^i(G, ?): \text{G-Mod} \longrightarrow \text{Ab}, A \mapsto H^i(G, A),$$

mit folgende Eigenschaften

(i) $H^0(G, ?)$ ist gerade der Funktor $A \mapsto A^G$.

(ii) $H^i(G, A) = 0$ für $i > 0$ und A koinduziert.

(iii) Für jede kurze exakte Sequenz von G-Moduln

$$E: 0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$$

gibt es ein Gruppen-Homomorphismen

$$\delta_E: H^i(G, A'') \longrightarrow H^{i+1}(G, A'),$$

---

[17] Multiplikation von

$$\sum_{g\in G} n_g \bullet g \qquad (*)$$

mit einem Element aus G (von links oder rechts) permutiert nur die Koeffizienten von (*), läßt die Summe der Koeffizienten also unverändert.

[18] Für $\sigma = \sum_{g\in G} n_g \bullet g \in I_G$ gilt $\sum_{g\in G} n_g = 0$, also

$$\sum_{g\in G} n_g \bullet(g - e) = \sum_{g\in G} n_g \bullet g - \sum_{g\in G} n_g \bullet e = \sum_{g\in G} n_g \bullet g = \sigma.$$

die in funktorieller Weise von E abhängen und für welche die folgende Sequenz exakt ist.

$$0 \longrightarrow H^0(G, A') \longrightarrow H^0(G,A) \longrightarrow H^0(G,A'') \longrightarrow H^1(G, A') \longrightarrow \ ....$$

$$... \longrightarrow H^i(G,A') \longrightarrow H^i(G,A) \longrightarrow H^i(G,A'') \xrightarrow{\delta_E} H^{i+1}(G,A') \longrightarrow ...$$

Bemerkungen

(i) Durch die angegebenen Eigenschaften sind die Funktoren H^i bis auf natürliche Isomorphie eindeutig festgelegt. Die Gruppe $H^i(G, A)$ heißt i-te Kohomologie der Gruppe G mit Koeffizienten in A.

(ii) Anstelle von Bedingung (ii) kann man auch fordern, $H^i(G, A) = 0$ für $i > 0$ und A injektiv.[19]

(iii) Aus den obigen Axiomen kann man ableiten[20], daß sich die Gruppe

$$H^i(G, A)$$

wie folgt berechnen läßt: man wähle eine Auflösung von A durch koinduzierte G-Moduln, sagen wir

$$0 \longrightarrow A \longrightarrow C^0 \longrightarrow C^1 \longrightarrow C^2 \longrightarrow ...$$

Dann wende man auf die Sequenz

$$C^*: 0 \longrightarrow C^0 \longrightarrow C^1 \longrightarrow C^2 \longrightarrow ...$$

Den Funktor $H^0(G, ?) = ?^G$ an. Die i-te Kohomologie des entstehenden Komplexes

$$(C^*)^G: 0 \longrightarrow (C^0)^G \longrightarrow (C^1)^G \longrightarrow (C^2)^G \longrightarrow ...$$

ist gerade die gesuchte Kohomologie-Gruppe

$$H^i(G, A) = H^i((C^*)^G) = \mathrm{Ker}((C^i)^G \longrightarrow (C^{i+1})^G)/\ \mathrm{Im}((C^{i-1})^G \longrightarrow (C^i)^G)$$

(iv) In der Sprache der homologischen Algebra[21] besagt die obige Beschreibung der Gruppen $H^i(G,A)$ gerade, daß es sich um die abgeleiteten Funktoren des linksexakten Funktors

$$H^0(G,A) = A^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

handelt, d.h.

$$H^i(G,A) = \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

---

[19] d.h. der Funktor $\mathrm{Hom}_{\mathbb{Z}[G]}(? , A)$: G-$\mathrm{Mod}^0 \longrightarrow$ Ab ist exakt.

[20] Im Fall i = 0 verwende man die Linksexaktheit des Funktors $A \mapsto A^G$ und den Fall $i > 0$ beweise man durch Induktion nach i.

[21] Das klassische Lehrbuch der homologischen Algebra in der Sprache der Ringe und Moduln ist das Buch von Carten und Eilenberg:

Cartan, H., Eilenberg, S.: Homological Algebra, Princeton University Press.

Für allgemeine abelsche Kategorien findet man die entsprechenden Sätze (mit einer viel besseren Darlegung der Theorie der Spektralsequenzen) im folgenden Artikel von Grothendieck:

Grothendieck, A.: Sur quelques points d' algèbra homologique, Tohoku Mathematical Journal 9 (1957). 119-221.

Eine schnelle (in sich geschlossene) Beschreibung der Theorie der abgesleiteten Funktoren (mit allen wesentlichen Eigenschaften) findet man auch auf den ersten sechs Seiten im dritten Kapitel des Buches von Hartshorne:

R. Hartshorne: Algebraic geometry, Springer, Berlin 1977.

Dabei wird $\mathbb{Z}$ als $\mathbb{Z}[G]$-Modul mit der trivialen Operation von G angesehen, d.h.

$$g \bullet n = n \text{ für } g \in G \text{ und } n \in \mathbb{Z}.$$

Aus der allgemeinen Theorie der abgeleiteten Funktors ergibt sich daher, daß man in (iii) anstelle der koinduzierten Moduln auch die injektiven Moduln verwenden kann. Außerdem ergibt sich aus der Theorie der Ext-Funktoren die folgende Berechnungmethode für die Gruppen $H^i(G, A)$.

(v) Man wähle eine Auflösung des trivialen $\mathbb{Z}[G]$-Moduls $\mathbb{Z}$, sagen wir

$$\ldots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

durch projektive $\mathbb{Z}[G]$-Moduln P_i. Auf den zugehörigen Komplex

$$P_*: \ldots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

wende man den kontravarianten Funktor $\mathrm{Hom}_{\mathbb{Z}[G]}(?\ , A) = \mathrm{Ext}^0_{\mathbb{Z}[G]}(?, A)$. Die i-te Kohomologie des entstehenden Komplexes

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P_*, A): 0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A) \longrightarrow \ldots$$

ist gerade die gesuchte Kohomologie-Gruppe

$$H^i(G, A) = H^i(\mathrm{Hom}_{\mathbb{Z}[G]}(P_*, A))$$

(vi) Ein Beispiel für eine projektive Auflösung P_* von $\mathbb{Z}$ ist die folgende Standard-Auflösung. Es sei

$$P_n := \mathbb{Z}[G^{n+1}] = \mathbb{Z}[G \times \ldots \times G]$$

mit der G-Modul-Struktur $g \bullet (g_0, \ldots, g_n) = (g\ g_0, \ldots, gg_n)$. Die Rand-Homomorphismen seien die $\mathbb{Z}$-linearen Abbildungen

$$\partial: \mathbb{Z}[G^{n+1}] \longrightarrow \mathbb{Z}[G^n]$$

mit

$$\partial(g_0, \ldots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n)$$

Es sind offensichtlich G-Modul-Homomorphismen mit $\partial \circ \partial = 0$[22]. Man erhält also einen Komplex. von freien also projektiven Moduln. Weiter verwendet man die folgende Augmentation,

$$P_0 = \mathbb{Z}[G] \longrightarrow \mathbb{Z}, \quad \sum_{g \in G} n_g \bullet g \mapsto \sum_{g \in G} .$$

Die Exaktheit des so definierten Komplexes beweist man durch die Konstruktion einer Homotopie.[23]

---

[22] Man erhält die Summanden von $\partial(\partial(g_0, \ldots, g_n))$ indem man in $(g_0, \ldots, g_n)$ auf alle möglichen Weisen zwei Koordinaten weg läßt. Man kann diese Operation des Weglassens von zwei gegebenen Koordinaten in unterschiedlicher Reihenfolge durchführen. In beiden Fällen erhält man dasselbe (n-1)-Tupel aber mit unterschiedlichem Vorzeichen.

[23] Man fixiere ein $s \in G$ und betrachte die Abbildungen

$$h: \mathbb{Z}[G^{n+1}] \longrightarrow \mathbb{Z}[G^{n+2}], (g_0, \ldots, g_n) \mapsto (s, g_0, \ldots, g_n).$$

Durch direktes Nachrechnen sieht man $\partial h + h\partial = \mathrm{Id}$. Durch Übergang zur Homologie des Komplexes sieht man, daß die identische Abbildung auf den Homologie-Gruppen mit der Null-Abbildung übereinstimmt. Deshalb müssen die Homologie-Gruppen trivial sein.

(vii) Aus der Konstruktion der Standard-Auflösung ergibt sich eine Beschreibung der Elemente von

$$H^i(G, A)$$

als Äquivalenzklassen von Abbildungen $G^i = G\times...\times G \longrightarrow A$, die gewissen Relationen genügen.[24] Man schreibt

$$H^i(G, A) = \{ \text{i-Kozyklen } G^i \longrightarrow A\}/\{ \text{i-Koränder } G^i \longrightarrow A\}.$$

Ein 1-Kozyklus ist dabei eine Abbildung der Gestalt

$$\varphi: G \longrightarrow A \text{ mit } \varphi(g'g'') = g'\bullet\varphi(g'') + \varphi(g').$$

Falls G auf A trivial operiert, ist dies gerade ein Gruppen-Homomorphismus.
Ein 1-Korand ist eine Abbildung der Gestalt

$$\varphi: G \longrightarrow A, g \mapsto ga - a,$$

mit $a\in A$. Man beachte, 1-Koränder sind insbesondere 1-Kozyklen.

(viii) Die $H^i(G, A)$ sind auch kontravariante Funktoren bezüglich G.[25] Insbesondere hat man für jede Untergruppe $H \subseteq G$ einen Gruppen-Homomorphismus

$$\text{Res: } H^i(G, A) \longrightarrow H^i(H, A)$$

welcher <u>Restriktion</u> hei0t. Auf dem Niveau der Kozyklen von (vii) entspricht die Restriktion gerade der Einschränkung der auf Abbildungen $G^i \longrightarrow A$ auf H^i. Für i = 0 ist die Restriktion gerade die natürliche Einbettung

$$A^G \subseteq A^H.$$

(ix) Analog induziert für jeden Normalteiler $N \subseteq G$ der natürliche Homomorphismus

$$G \longrightarrow G/N$$

einen Gruppen-Homorphismus

$$\text{Inf: } H^i(G/N, A^N) \longrightarrow H^i(G, A^N) \longrightarrow H^i(G, A),$$

wobei der zweite Homomorphismus durch die natürliche Einbettung $A^N \longrightarrow A$ induziert wird. Dieser Homomorphismus heißt <u>Inflation</u>.

Man beachte, der G-Modul A ist im allgemeinen kein G/N-Modul. Deshalb muß man auf der linken Seite den Modul A^N der N-invarianten Elemente verwenden.

(x) Inflation und Restriktion sind durch eine exakte Sequenz miteinander verbunden. Genauer, für jeden Normalteiler $N \subseteq G$ und jeden G-Modul A ist die folgende Sequenz exakt.

$$0 \longrightarrow H^1(G/N, A^N) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(N, A).$$

Außerdem hat man exakte Sequenzen

---

vgl. Kapitel IV, §2 in
Cassels, J.W.S, Fröhlich, A.: Algebraic number theory, Academic Press, London 1967.

[24] Zunächst sind es Äquivalenzklassen von $\mathbb{Z}[G]$-Modul-Homomorphismen

$$\mathbb{Z}[G^{i+1}] \longrightarrow A.$$

Da diese Abildung insbesondere $\mathbb{Z}$-linear sind, sind sie bereits durch ihre Einschränkungen auf G^{i+1} vollständig festgelegt. Weil es G-Modul-Homomorphismen sind, können wir sie sogar auf

$$\{e\}\times G^i \ (\cong G^i)$$

einschränken, ohne irgendwelche Informationen zu verlieren.

[25] Wie sich aus der Beschreibung mit Hilfe der Standard-Auflösung ergibt.

$$0 \longrightarrow H^i(G/N, A^N) \xrightarrow{\text{Inf}} H^i(G, A) \xrightarrow{\text{Res}} H^i(N, A)$$

falls gilt

$$0 = H^1(N, A) = H^2(N, A) = \ldots = H^{i-1}(N, A).$$

(xi) Lemma von Schapiro. Seien G eine Gruppe, $H \subseteq G$ eine Untergruppe und B ein H-Modul. Dann ist $A := \mathrm{Hom}(\mathbb{Z}[G], B)$ ein G-Modul mit

$$H^i(G, A) = H^i(H, B).$$

(xii) Hilbert's Satz 90. Sei K/k eine endliche Galois-Erweiterung mit der Galois-Gruppe G = G(K/k). Dann ist K* ein G-Modul mit

$$H^1(G, K^*) = 0.$$

1.4.5 Gruppen-Homologie

Unter der Homolgie einer Gruppe G versteht man eine Familie von Funktoren

$$H_i(G, ?): \text{G-Mod} \longrightarrow \text{Ab}, A \mapsto H_i(G, A),$$

mit folgende Eigenschaften

(i) $H_0(G, ?)$ ist gerade der Funktor $A \mapsto A_G$.

(ii) $H_i(G, A) = 0$ für $i > 0$ und A induziert.

(iii) Für jede kurze exakte Sequenz von G-Moduln

$$E: 0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$$

gibt es Gruppen-Homomorphismen

$$\delta_E: H_{i+1}(G,A'') \xrightarrow{\delta_E} H_i(G,A'),$$

die in funktorieller Weise von E abhängen und für welche die folgende Sequenz exakt ist.

$$0 \longrightarrow H^0(G, A') \longrightarrow H^0(G,A) \longrightarrow H^0(G,A'') \longrightarrow H^1(G, A') \longrightarrow \ldots.$$

$$\ldots \longrightarrow H_{i+1}(G,A'') \xrightarrow{\delta_E} H_i(G,A') \longrightarrow H_i(G,A) \longrightarrow H_i(G,A'') \longrightarrow \ldots$$

$$\ldots \longrightarrow H_0(G, A') \longrightarrow H_0(G,A) \longrightarrow H_0(G,A'') \longrightarrow 0$$

Bemerkungen

(i) Durch die angegebenen Eigenschaften sind die Funktoren H_i bis auf natürliche Isomorphie eindeutig festgelegt. Die Gruppe $H_i(G, A)$ heißt i-te Homologie der Gruppe G mit Koeffizienten in A.

(ii) Anstelle von Bedingung (ii) kann man auch fordern, $H_i(G, A) = 0$ für $i > 0$ und A projektiv.[26]

(iii) Aus den obigen Axiomen kann man ableiten[27], daß sich die Gruppe

$$H_i(G, A)$$

wie folgt berechnen läßt: man wähle eine Auflösung von A durch induzierte G-Moduln, sagen wir

---

[26] d.h. der Funktor $\mathrm{Hom}_{\mathbb{Z}[G]}(A, ?)$: G-Mod $\longrightarrow$ Ab ist exakt.

[27] Im Fall i = 0 verwende man die Rechtsexaktheit des Funktors $A \mapsto A_G$ und den Fall $i > 0$ beweise man durch Induktion nach i.

$$... \longrightarrow I_2 \longrightarrow I_1 \longrightarrow I_0 \longrightarrow A \longrightarrow 0.$$

Dann wende man auf die Sequenz

$$I^*: ... \longrightarrow I_2 \longrightarrow I_1 \longrightarrow I_0 \longrightarrow 0$$

Den Funktor $H_0(G, ?) = ?_G$ an. Die i-te Homologie des entstehenden Komplexes

$$(I^*)_G: *: ... \longrightarrow (I_2)_G \longrightarrow (I_1)_G \longrightarrow (I_0)_G \longrightarrow 0$$

ist gerade die gesuchte Homologie-Gruppe

$$H_i(G, A) = H_i((I^*)_G) = \mathrm{Ker}((I_i)_G \longrightarrow (I_{i-1})_G)/\ \mathrm{Im}((I_{i+1})_G \longrightarrow (I_i)_G)$$

(iv) In der Sprache der homologischen Algebra besagt die obige Beschreibung der Gruppen $H_i(G,A)$ gerade, daß es sich um die abgeleiteten Funktoren des rechtsexakten Funktors

$$H_0(G,A) = A_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$$

handelt, d.h.

$$H_i(G,A) = \mathrm{Tor}_i^{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

Dabei wird $\mathbb{Z}$ wie bisher als $\mathbb{Z}[G]$-Modul mit der trivialen Operation von G angesehen.
Aus der allgemeinen Theorie des Tor-Funktors ergibt sich daher die folgende Berechnungmethode für die Gruppen $H_i(G, A)$.

(v) Man wähle eine Auflösung des trivialen $\mathbb{Z}[G]$-Moduls $\mathbb{Z}$, sagen wir

$$... \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0$$

durch projektive $\mathbb{Z}[G]$-Moduln P_i. Auf den zugehörigen Komplex

$$P_*: ... \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow 0$$

wende man den Funktor $?\otimes_{\mathbb{Z}[G]}A = \mathrm{Tor}_0^{\mathbb{Z}[G]}(?, A)$. Die i-te Homologie des entstehenden Komplexes

$$P_* \otimes_{\mathbb{Z}[G]} A: ... \longrightarrow P_1 \otimes_{\mathbb{Z}[G]} A \longrightarrow P_0 \otimes_{\mathbb{Z}[G]}, A \longrightarrow 0$$

ist gerade die gesuchte Homologie-Gruppe

$$H_i(G, A) = H_i(P_* \otimes_{\mathbb{Z}[G]} A)$$

(vi) Als projektive Auflösung P_* kann man insbesodere die Standard-Auflösung von 1.4.4 (vi) verwenden.

(vii) Die $H_i(G, A)$ sind auch kovariante Funktoren bezüglich G.[28] Insbesondere hat man für jede Untergruppe $H \subseteq G$ einen Gruppen-Homomorphismus

$$\mathrm{Cor}: H^i(H, A) \longrightarrow H^i(G, A)$$

welcher Coestriktion heißt.. Für i = 0 ist die Corestriktion gerade die natürliche Surjektion

$$A_H = A/I_H A \twoheadrightarrow A_G = A/I_G A,$$

[28] Wie sich aus der Beschreibung mit Hilfe der Standard-Auflösung ergibt.

welche sich aus der Enthaltenseinsrelationn $I_H \subseteq I_G$ ergibt.

(viii) Wir haben jetzt alle Hilfmittel zusammengestellt, die man zur Konstruktion der Tate-Kohomologie benötigt. Etwas vereinfachend gesagt, ensteht die Tate-Kohomologie durch Zusammenkleben von Gruppen-Homologie und Kohomologie zu einer einzigen (Ko-) Homologie-Theorie (im Fall, daß die Gruppe G endlich ist).

1.4.6 Tate-Kohomologie

Sei G eine endliche Gruppe. Wir setzen

$$N := \sum_{g \in G} g \in \mathbb{Z}[G]$$

und bezeichnen für jeden G-Modul A die Multiplikation mit N ebenfalls mit N,

$$N: A \longrightarrow A,\ a \mapsto N \bullet a.$$

Man beachte, dies ist ein G-Modul-Homomorphismus.[29] Direkt aus der Definition ergibt sich[30]

$$I_G A \subseteq \mathrm{Ker}(N) \text{ und } \mathrm{Im}(N) \subseteq A^G.$$

Wir können also N als Abbildung $N: A \longrightarrow A^G$ auffassen, und nach dem Homomorphie-Satz induziert letztere Abbildung einen Gruppen-Homomorphismus

$$H_0(G, A) = A_G \xrightarrow{N^*} A^G = H^0(G, A).$$

Betrachten wir die exakte Sequenz

$$0 \longrightarrow \mathrm{Ker}(N^*) \hookrightarrow A_G \xrightarrow{N^*} A^G \longrightarrow A^G/\mathrm{Im}(N^*) \longrightarrow 0$$

und schreiben diese in der Gestalt

$$0 \longrightarrow \hat{H}^{-1}(G,A) \longrightarrow H_0(G, A) \xrightarrow{N^*} H^0(G, A) \longrightarrow \hat{H}^0(G,A) \longrightarrow 0$$

mit

$$\hat{H}^{-1}(G,A) := \mathrm{Ker}(N^*)$$

$$\hat{H}^0(G,A) := \mathrm{Koker}(N^*)$$

Weiter setzen wir

$$\hat{H}^{-n}(G, A) := H_{n-1}(G, A) \text{ für } n = 2, 3, 4, \ldots$$

$$\hat{H}^n(G, A) := H^n(G, A) \quad \text{für } n = 1, 2, 3, \ldots$$

Die Gruppe

$$\hat{H}^n(G, A) \text{ mit } n \in \mathbb{Z}$$

heißt n-te Tate-Kohomologie von G mit Koeffizienten aus A.

Bemerkungen

---

[29] Für jedes $g \in G$ gilt $g \bullet N = N = N \bullet g$. Für $a \in A$ ist damit

$$N(g \bullet a) = N \bullet g \bullet a = g \bullet N \bullet a = g \bullet N(a).$$

[30] Die erste Inklusion folgt aus der Tatsache, daß I_G von den Elementen der Gestalt g - e erzeugt wird und

$$N((g - e)\, a) = N \bullet g \bullet a - N \bullet e \bullet a = N \bullet a - N \bullet a = 0$$

gilt. Die zweite Inklusion besteht wegen

$$g \bullet N(a) = g \bullet N \bullet a = N \bullet a = N(a).$$

(i) $\hat{H}^n(G, A) = 0$ für jedes $n \in \mathbb{Z}$, falls A (ko-) induziert ist.[31]

---

[31] Sei X eine beliebige abelsche Gruppe. Betrachten wir die Abbildung

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X) \longrightarrow \mathbb{Z}[G]\otimes_{\mathbb{Z}} X,\ \varphi \mapsto \sum_{g\in G} g\otimes \varphi(g). \qquad (*)$$

Die Gruppe rechts kann man mit einer direkten Summe von Exemplaren von X identifizieren,

$$\mathbb{Z}[G]\otimes_{\mathbb{Z}} X = (\oplus_{g\in G}\mathbb{Z})\otimes_{\mathbb{Z}} X \cong \oplus_{g\in G} X.$$

Die Abbildung (*) bekommt dadurch die Gestalt

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X) \longrightarrow \oplus_{g\in G} X,\ \varphi \mapsto (\varphi(g))_{g\in G}. \qquad (**)$$

Weil $\mathbb{Z}[G]$ als $\mathbb{Z}$-Modul frei ist, ist eine Abbildung der Hom-Menge links durch ihre Werte auf den Erzeugern $g\in G$ bestimmt, wobei man diese Werte beliebig vorgeben kann. Mit anderen Worten, die Abbildung (**) ist bijektiv. Also ist auch (*) bijektiv.

Außerdem ist (*) ein G-Modul-Homomorphismus: das Bild von $g\bullet\varphi$ bei (*) ist

$$\sum_{g'\in G} g'\otimes g\varphi(g') = \sum_{g'\in G} g'\otimes \varphi(g^{-1}g')$$

$$= \sum_{g'\in G} gg'\otimes \varphi(g') \qquad \text{(Reparametrisierung } g' \mapsto gg')$$

$$= g\bullet \sum_{g'\in G} g'^{-1}\otimes \varphi(g')$$

Wir haben gezeigt, für endliche Gruppen fallen die Begriffe “induziert” und “koinduziert” zusammen. Insbesondere gilt die Behauptung für

$$n < -1 \text{ oder } 0 < n.$$

Wir haben noch die Fälle $n = -1$ und $n = 0$ zu behandeln, d.h. wir haben zu zeigen,

1. $\mathrm{Ker}(N^*: A_G \longrightarrow A^G) = 0$ für A induziert.
2. $\mathrm{Koker}(N^*: A_G \longrightarrow A^G) = 0$ für A induziert.

Sei also A induziert, d.h.

$$A = \mathbb{Z}[G]\otimes X$$

mit einer abelschen Gruppe X. Jedes Element von A hat dann die Gestalt

$$x = \sum_{g\in G} g\otimes x_g$$

mit eindeutig bestimmten Elementen $x_g \in X$.

Zu 2: Liegt $x = \sum_{g\in G} g\otimes x_g$ in A^G, so gilt $g'x = x$ für jedes $g'\in G$, d.h.

$$\sum_{g\in G} g\otimes x_g = \sum_{g\in G} g'g\otimes x_g = \sum_{g\in G} g\otimes x_{g',-1g}$$

d.h. $x_g = x_{g',-1g}$ für beliebige $g, g' \in G$, d.h. alle x_g sind gleich,

$$x = N\bullet x_e = N(x_e) \in \mathrm{Im}(N^*).$$

(ii) Für jede kurze exakte Sequenz

$$E : 0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$$

von G-Moduln gibt es Gruppen-Homomorphismen

$$\delta_E : \hat{H}^i(G, A'') \longrightarrow \hat{H}^{i+1}(G, A'),$$

die funktoriell von E abhängen und für welche die folgende Sequenz exakt ist.[32]

$$\ldots \longrightarrow \hat{H}^i(G,A') \longrightarrow \hat{H}^i(G,A) \longrightarrow \hat{H}^i(G,A'') \longrightarrow \hat{H}^{i+1}(G,A') \longrightarrow \ldots$$

Zu 1: Repräsentiere $x = \sum_{g\in G} g\otimes x_g \in A$ ein Element aus dem Kern von N*, d.h.

$$0 = N(\sum_{g\in G} g\otimes x_g) = \sum_{g\in G} (Ng)\otimes x_g = \sum_{g\in G} N\otimes x_g = N\otimes \sum_{g\in G} x_g$$

Identifizienen wir $A = \mathbb{Z}[G]\otimes X$ mit der direkten Summe $\oplus_{g\in G} X$, so wird das Element rechts ein Tupel, dessen sämtliche Koordinaten gleich $\sum_{g\in G} x_g$ sind. Da dieses Element Null sein soll, folgt $\sum_{g\in G} x_g = 0$, also $x = \sum_{g\in G} g\otimes x_g = \sum_{g\in G} (g - e)\otimes x_g \in I_G\otimes X = I_G A$. Das Element x repräsentiert somit das Null-Element von $A_G = A/I_G A$.

Anmerkung:
Denkt man sich die Hom-Menge rechts mit der $*$-Multiplikation versehen, so muß man anstelle von (*) die Abbildung $\varphi \mapsto \sum_{g\in G} g^{-1}\otimes \varphi(g)$. verwenden.

[32] Weil N*: $A_G \longrightarrow A^G$ ein funktorieller Morphismus ist, besteht das folgende kommutative Diagramm mit exakten Zeilen.

$$\begin{array}{ccccccccc}
\ldots\longrightarrow H_1(G,A'') & \xrightarrow{\alpha} & H_0(G,A') & \longrightarrow & H_0(G,A) & \xrightarrow{\beta'} & H_0(G,A'') & \longrightarrow & 0 \\
\downarrow & & \downarrow N' & & \downarrow N & & \downarrow N'' & & \downarrow \\
0 \longrightarrow & & H^0(G,A') & \xrightarrow{\alpha'} & H^0(G,A) & \longrightarrow & H^0(G,A'') & \xrightarrow{\beta} & H^1(G,A') \longrightarrow \ldots
\end{array}$$

Man beachte, das linke äußere Viereck ist kommuativ, d.h.

$$N'\circ\alpha = 0,$$

weil das linke innere es ist, d.h. $\alpha'\circ N'\circ\alpha = 0$ (und α' injektiv ist).
Analog, das rechte äußere Viereck ist kommuativ, d.h.

$$\beta\circ N'' = 0,$$

weil das rechte innere es ist, d.h. $\beta\circ N''\circ\beta'' = 0$ (und β' surjektiv ist).
Aus der Kommutativität des linken äußeren Vierecks folgt, daß das Bild von α im Kern von N' liegt.
Aus der Kommuativität des rechten äußeren Vierecks folgt, daß sich β über den Kokern von N'' faktorisiert. Die gesuchte exakte Sequenz ergibt sich jetzt aus dem Schlangen-Lemma.

(iii) Wie im Fall der Gruppen-Kohomologie bzw. Homologie kann man die Tate-Gruppen als Kohomologie-Gruppen einer sogenannten vollen Auflösung beschreiben. Diese läßt sich wie folgt konstruieren. Sei

$$P_*: \ldots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

eine Auflösung von A durch freie endlich erzeugte G-Moduln P_i (zum Beispiel die Standard-Auflösung). Wir wenden den Funktor $\mathrm{Hom}_{\mathbb{Z}}(? , \mathbb{Z})$ an und erhalten einen Komplex

$$P^*: 0 \longrightarrow \mathbb{Z} \xrightarrow{\varepsilon^*} P^0 \longrightarrow P^1 \longrightarrow P^2 \longrightarrow$$

mit $P^i = \mathrm{Hom}_{\mathbb{Z}}(P_i , \mathbb{Z})$. Diese Sequenz ist wieder exakt.[33] Die exakten Sequenzen P_* und P^* setzen sich zusammen zu einer exakten Sequenz

$$L^*: \ldots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\varepsilon^* \circ \varepsilon} P^0 \longrightarrow P^1 \longrightarrow P^2 \longrightarrow \ldots$$

mit

$$L^i = \begin{cases} P^i & \text{für } 0 \le i \\ P_{-i-1} & \text{für } i < 0 \end{cases}$$

Die Exaktheit dieser Sequenz ist klar außer an den Stellen P_0 und P^0. An der Stelle P_0 ergibt sich diese Exaktheit aus der von P_* und aus

$$\mathrm{Ker}(\varepsilon^* \circ \varepsilon) = \mathrm{Ker}(\varepsilon)$$

denn ε^* ist injektiv. An der Stelle P^0 ergibt sich diese Exaktheit aus der von P^* und aus

$$\mathrm{Im}(\varepsilon^* \circ \varepsilon) = \mathrm{Im}(\varepsilon^*),$$

denn ε ist surjektiv. Mit Hilfe von L^* kann man die Tate-Gruppen wie folgt berechnen.

$$\hat{H}^i(G, A) := H^i(\mathrm{Hom}_{\mathbb{Z}[G]}(L^*, A)).$$

---

[33] Dies folgt sofort aus der Theorie des Ext-Funktors:

$$H^i(P^*) = \mathrm{Ext}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) = 0 \text{ für } i > 0.$$

Elementar kann man wie folgt argumentieren. Man zerlege den Ausgangskomplex P_* in kurze exakte Sequenzen

$$0 \longrightarrow C_{i+1} \longrightarrow P_i \longrightarrow C_i \longrightarrow 0 \text{ mit } C_0 = \mathbb{Z} \text{ und}$$

beachte,

1. C_0 ist projektiv.
2. Ist C_i projektiv, so zerfällt die i-te exakte Sequenz, $P_i \cong C_i \oplus C_{i+1}$, und insbesondere ist auch C_{i+1} projektiv.

Wir sehen so, alle diese kurzen exakten Sequenzen zerfallen (und alle C_i sind projektiv). Durch Anwenden des Dualisierungsfunktors $\mathrm{Hom}_{\mathbb{Z}}(? , \mathbb{Z})$ entstehen aus diesen zerfallenden exakten Sequenzen wieder zerfallende exakte Sequenzen. Letztere setzen sich zu einer exakten Sequenz zusammen, nämlich zu P^*. Insbesonder ist P^* also exakt.

(iv) Sei G eine endliche zyklische Gruppe. Dann gilt für jeden G-Modul A und jede ganze Zahl i,

$$\hat{H}^{2i}(G, A) = \hat{H}^{0}(G, A) = A^G/N\bullet A$$

und

$$\hat{H}^{2i+1}(G, A) = \hat{H}^{-1}(G, A) = {}_NA/I_GA.$$

Dabei bezeichne ${}_NA$ den Kern der Abbildung $N: A \longrightarrow A$.

Beweis von Bemerkung (iii).

Im Fall $0 < i$ folgt die Aussage aus unserer Beschreibung der Gruppen-Kohomologie (Bemerkung 1.4.4 (v)).

Im Fall $i < -1$ folgt sie aus unserer Beschreibung der Gruppen-Homologie (Bemerkung 1.4.5 (v)). Dazu beachten wir (siehe unten), es bestehen Isomorphismen abelscher Gruppen

$$P_n \otimes_{\mathbb{Z}[G]} A \xrightarrow{\alpha} (P_n \otimes_{\mathbb{Z}} A)_G \xrightarrow{N^*} (P_n \otimes_{\mathbb{Z}} A)^G \xrightarrow{\beta} \mathrm{Hom}_{\mathbb{Z}}(P_n, A)^G = \mathrm{Hom}_{\mathbb{Z}[G]}(P_n, A) \qquad (1)$$

Für $n \geq 0$ ist die Hom-Gruppe rechts gerade

$$\mathrm{Hom}_{\mathbb{Z}[G]}(L^{-(n+1)}, A),$$

also gilt

$$H^{-(n+1)}(\mathrm{Hom}_{\mathbb{Z}[G]}(L^*, A)) = H_n(P_* \otimes_{\mathbb{Z}[G]} A) = H_n(G, A) = \hat{H}^{-(n+1)}(G,A)$$

für alle $n > 0$.

Die Isomorphismen (1) ergeben sich wie folgt.

<u>Das letzte Gleichheitszeichen</u>:

G operiert auf $\mathrm{Hom}_{\mathbb{Z}}(P_n, A)$ durch

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

Der invariante Teil von $\mathrm{Hom}_{\mathbb{Z}}(P_n, A)$ fällt deshalb mit den G-Modul-Homomorphismen zusammen.

<u>Der Isomorphismus β</u>.

Wir betrachten die bijektive[34] Abbildung

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \longrightarrow \mathbb{Z}[G]\otimes_{\mathbb{Z}} A, \varphi \mapsto \sum_{g\in G} g\otimes\varphi(g).$$

Versieht man das Tensorprodukt $\mathbb{Z}[G]\otimes_{\mathbb{Z}}A$ mit der "diagolnalen" G-Modul-Struktur[35]

---

[34] Vgl. die Aussage, daß im Fall endlicher Gruppen die induzierten mit den koinduziertem G-Moduln zusmmenfallen.

[35] Für je zwei G-Moduln A, B und jedes $g\in G$ ist durch

$$g\bullet(\sigma\otimes a) = (g\sigma)\otimes(ga),$$

so ist dies sogar ein G-Modul-Homomorphismus:

$$g\bullet\varphi \mapsto \sum_{g'\in G} g'\otimes(g\varphi)(g') = \sum_{g'\in G} g'\otimes g\varphi(g^{-1}g') = \sum_{g'\in G} (gg')\otimes g\varphi(g') = g\bullet \sum_{g'\in G} g'\otimes\varphi(g'),$$

also ein Isomorphismus von G-Moduln. Da der Hom-Funktor und das Tensorprodukt mit endlichen direkten Summen kommutieren (und P_n eine solche endliche direkte Summe ist) liefert dieser Isomorphismus auch einen Isomorphismus

$$P_n\otimes_{\mathbb{Z}}A \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(P_n, A)$$

Durch Übergang zu den invarianten Teilen erhält man den Isomorphismus β.

Die Bijektivität von N*. In der exakten Sequenz

$$0 \longrightarrow \hat{H}^{-1}(G,A) \longrightarrow A_G \xrightarrow{N^*} A^G \longrightarrow \hat{H}^0(G,A) \longrightarrow 0$$

ersetzen wir den G-Modul A durch den induzierten G-Modul $P_n\otimes_{\mathbb{Z}}A$ und verwenden die Aussage von Bemerkung (i).

Der Isomorphismus α.
Es reicht zu zeigen, daß für je zwei G-Moduln A und B eine natürliche Isomorphie

$$A\otimes_{\mathbb{Z}[G]}B \cong (A\otimes_{\mathbb{Z}}B)_G \qquad (2)$$

besteht. Man beachte, zur Bildung des Tensorprodukts auf der linken Seite muß man A mit der Struktur eines rechten G-Moduls versehen,

$$a\bullet g := g^{-1}a.$$

Zum Beweis von (2) charakterisieren wir beide Seiten durch eine Universalitätseigenschaft.

Für jeden G-Modul A ist $A_G = A/I_GA$ ein G-Modul mit trivialer G-Operation: für $g\in G$ und $a \in A$ gilt

$$g\bullet a = e\bullet a + (g-e)a = a + (g-e)\bullet a \equiv a \bmod I_GA$$

(wegen $g-e \in I_G$).
Umgekehrt gilt für jeden Faktor-Modul A/A' von A mit trivialer G-Operation,

$$g\bullet a \equiv a \bmod A',$$

$$A\times B \longrightarrow A\otimes_{\mathbb{Z}}B, (a,b) \mapsto (ga)\otimes(gb),$$

eine biadditive Abbildung definiert. Diese faktorisiert sich somit über

$$A\times B \longrightarrow A\otimes_{\mathbb{Z}}B, (a,b) \mapsto a\otimes b.$$

Es gibt also einen wohldefinierten Gruppen-Homomorphismus

$$A\otimes_{\mathbb{Z}}B \longrightarrow A\otimes_{\mathbb{Z}}B, a\otimes b \mapsto (ga)\otimes(gb).$$

Das Bild von $a\otimes b$ bei diesem Homomorphismus wird mit

$$g\bullet(a\otimes b) = (ga)\otimes(gb).$$

bezeichnet. Auf diese Weise bekommt $A\otimes_{\mathbb{Z}}B$ die Struktur eines G-Moduls.

d.h. $(g - e)\, a = ga - a \in A'$, d.h. $I_G A \subseteq A'$, d.h. die natürliche Abbildung $A \longrightarrow A/A'$ faktorisiert sich (eindeutig) über die natürliche Abbildung $A \longrightarrow A_G = A/I_G$. Mit anderen Worten, A_G ist der größte Faktor-Modul von A, auf welchem G trivial operiert. Ensprechend ist der Modul auf der rechten Seite von (2) der größte Faktor-Modul von $A \otimes_{\mathbb{Z}} B$, auf welchem G trivial operiert. Betrachten wir die linke Seite von (2).

Weil die natürliche Abbildung

$$A \times B \longrightarrow A \otimes_{\mathbb{Z}[G]} B$$

biadditiv ist, faktorisiert sie sich über $A \times B \longrightarrow A \otimes_{\mathbb{Z}} B$, d.h. wir haben eine lineare Abbildung

$$A \otimes_{\mathbb{Z}} B \longrightarrow A \otimes_{\mathbb{Z}[G]} B\ ,\ a \otimes b \mapsto a \otimes b. \qquad (3)$$

Diese ist offensichtlich surjektiv, d.h. $A \otimes_{\mathbb{Z}[G]} B$ ist ein Faktormodul von $A \otimes_{\mathbb{Z}} B$. Die Surjektion ist ein G-Modul-Homomorphismus,, wenn man beide Tensorprodukte mit diagonalen Operation von G versieht. Außerdem gilt im rechten Tensorprodukt

$$\begin{aligned} g \bullet (a \otimes b) &= (ga) \otimes (gb) \\ &= (ag^{-1}) \otimes (gb) \text{ (rechte G-Modul-Struktur von A)} \\ &= a \otimes (g^{-1} gb) \quad \text{(Bilinearität von } \otimes) \\ &= a \otimes b. \end{aligned}$$

Mit anderen Worten, G operiert trivial auf $A \otimes_{\mathbb{Z}[G]} B$. Wir haben noch zu zeigen, die Abildung (3) ist universell bezüglich dieser Eigenschaft. Sei also

$$f: A \otimes_{\mathbb{Z}} B \longrightarrow C$$

ein surjektiver G-Modul-Homomorphismus[36], wobei G auf C trivial operiere. Wir haben zu zeigen, f faktorisiert sich eindeutig über (3). Die Eindeutigkeitsaussage ist trivial wegen der Surjektivität von (3). Beweisen wir die Existenz einer Faktorisierung. Dazu betrachten wir die Abbildung

$$\tilde{f}: A \times B \longrightarrow C,\ (a, b) \mapsto f(a \otimes b).$$

Für $g \in G$ gilt

$$\begin{aligned} \tilde{f}(ag, b) &= f((ag) \otimes b) \\ &= f((g^{-1} a) \otimes b) && \text{(Definition der rechten G-Modul-Struktur)} \\ &= f(g^{-1} \bullet (a \otimes (gb)) && \text{(G-Modul-Struktur von } A \otimes_{\mathbb{Z}} B) \\ &= g^{-1} f(a \otimes (gb)) && (\mathbb{Z}[G]\text{-Linearität von f}) \\ &= f(a \otimes (gb)) && \text{(Trivialität der G-Operation auf C)} \\ &= \tilde{f}(a, gb). \end{aligned}$$

Wir haben gezeigt, die Abbildung $\tilde{f}$ ist bilinear über $\mathbb{Z}[G]$. Sie faktorisiert sich also über $A \otimes_{\mathbb{Z}[G]} B$. Wir erhalten eine Abbildung

$$A \otimes_{\mathbb{Z}[G]} B \longrightarrow C,\ a \otimes b \mapsto \tilde{f}(a, b) = f(a \otimes b).$$

---

[36] d.h. eine $\mathbb{Z}[G]$-lineare Abbildung.

Die Zusammensetzung mit (3) ist gerade die vorgegebene Abbildung f. Damit ist die gesuchte Faktorisierung konstruiert.

Damit ist die Aussage von (iii) mit Ausnahme der Fälle i = 0 und i = -1 bewiesen. Für das weitere benötigen wir eine funktorielle Variante des obigen Isomorphismus β. Für jeden G-Modul A bezeichne

$$A^* := \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z})$$

den dualen G-Modul mit der Multiplikation

$$(g \bullet \varphi)(a) = \varphi(g^{-1}a) \text{ für } \varphi \in A^*, g \in G, a \in A.$$

Für je zwei G-Moduln A, B betrachten wir die Abbildung

$$B \otimes_{\mathbb{Z}} A \xrightarrow{\alpha} \mathrm{Hom}_{\mathbb{Z}}(B^*, A), b \otimes a \mapsto (f \mapsto f(b) \bullet a). \qquad (4)$$

Dies ist ein G-Modul-Homomorphismus der funktoriell von A und B abhängt und ein Isomorphismus für den Fall, daß B ein endlich erzeugter freier G-Modul ist.[37]

---

[37] Funktorialität bezüglich A. Sei $h: A \longrightarrow A'$ ein G-Modul-Homomorphismus. Dann gilt

$$\begin{aligned} h(\alpha(b \otimes a)(f)) &= h(f(b)a) \\ &= f(b)h(a) \qquad \text{(wegen } f \in B^*, \text{ d.h. } f(b) \in \mathbb{Z}) \\ &= \alpha(b \otimes h(a))(f) \end{aligned}$$

also $h(\alpha(b \otimes a)) = \alpha(b \otimes h(a))$, also

$$h \circ \alpha = \alpha \circ (\mathrm{id} \otimes h).$$

Mit anderen Worten, das Diagramm

$$\begin{array}{ccc} B \otimes A & \xrightarrow{\alpha} & \mathrm{Hom}(B^*, A) \\ {\scriptstyle \mathrm{id} \otimes h}\downarrow & & \downarrow{\scriptstyle h\circ} \\ B \otimes A' & \xrightarrow{\alpha} & \mathrm{Hom}(B^*; A') \end{array}$$

ist kommutativ.

Funktorialität bezüglich B. Sei jetzt $h: B \longrightarrow B'$ ein G-Modul-Homomorphismus. Wie üblich bezeichne

$$h^*: B'^* \longrightarrow B^*$$

die auf den dualen Moduln induzierte Abbildung.

$$\begin{array}{ccc} B \otimes A & \xrightarrow{\alpha} & \mathrm{Hom}(B^*, A) \\ {\scriptstyle h \otimes \mathrm{id}}\downarrow & & \downarrow{\scriptstyle \circ h^* = h^{**}} \\ B' \otimes A & \xrightarrow{\alpha} & \mathrm{Hom}(B'^*; A) \end{array}$$

Es gilt für $f' \in B'^*$:

$$\begin{aligned} \alpha(h(b) \otimes a)(f') &= f'(h(b)) \bullet a \\ &= (f' \circ h)(b) \bullet a \\ &= \alpha(b \otimes a)(f' \circ h) \\ &= \alpha(b \otimes a)(h^*(f')) \end{aligned}$$

also

$$\alpha(h(b) \otimes a) = \alpha(b \otimes a) \circ h^*$$

also

$$(\alpha \circ (h \otimes \mathrm{id}))(b \otimes a) = ((\circ h^*) \circ \alpha)(b \otimes a)$$

also

$$\alpha \circ (h \otimes \mathrm{id}) = (\circ h^*) \circ \alpha.$$

Mit anderen Worten, das obige Diagramm ist kommutativ:

G-Linearität von α. Für $a \in A$, $b \in B$, $g \in G$, $f \in B^*$ gilt

$$\begin{aligned} \alpha(g \bullet (b \otimes a))(f) &= \alpha((gb) \otimes (ga))(f) \\ &= f(gb) \bullet ga && \text{(Definition von } \alpha) \\ &= g \bullet (f(gb) \bullet a) && \text{(Wegen } f \in B^*, \text{ d.h. } f(gb) \in \mathbb{Z}) \\ &= g \bullet ((g^{-1}f)(b) \bullet a) && \text{(G-Modul-Struktur von } B^*) \end{aligned}$$

Zur Berechnung der beiden verbleibenden Kohomologie-Gruppen betrachten wir die Augmentation der gegebenen Auflösung von $\mathbb{Z}$,

$$\varepsilon: P_0 \longrightarrow \mathbb{Z}$$

deren Dual

$$\varepsilon^*: \mathbb{Z} = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(P_0, \mathbb{Z}) = P_0^*, 1 \mapsto \varepsilon,$$

und die Bilder von ε^* und ε beim Funktor $F(A) := \mathrm{Hom}_{\mathbb{Z}[G]}(\,?\,, A)$,

$$\mathrm{Hom}_{\mathbb{Z}[G]}(P_0^*, A) \xrightarrow{F(\varepsilon^*)} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \xrightarrow{F(\varepsilon)} \mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A).$$

Die Komposition dieser beiden Abbildungen ist gerade der Homomorphismus in der "Mitter" der Sequenz $\mathrm{Hom}_{\mathbb{Z}[G]}(L^*, A)$, deren Kohomologie wir berechnen wollen (d.h. an der Stelle, an welcher der homologische Teil endet und der kohomologische beginnt). Weil ε surjektiv ist, ist

---

$= g\bullet(\alpha(b\otimes a)(g^{-1}f))$ (Definition von α)
$= (g\bullet\alpha(b\otimes a))(f)$ (G-Modul-Struktur von Hom(B*,A))

also

$\alpha(g\bullet(b\otimes a)) = g\bullet\alpha(b\otimes a)$.

Bijektivität von α im Fall freier $\mathbb{Z}[G]$-Moduln B.

Da das Tensor-Produkt und der Hom-Funktor mit endlichen direkten Summen kommutieren, können wir annehmen,

$$B = \mathbb{Z}[G].$$

Wir haben die Bijektivität der Abbildung

$$\mathbb{Z}[G]\otimes_{\mathbb{Z}} A \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^*, A), \sigma\otimes a \mapsto (f \mapsto f(\sigma)\bullet a), \qquad (***)$$

zu beweisen. Für jedes $g\in G$ bezeichne

$$\overset{\vee}{g}: \mathbb{Z}[G] \longrightarrow \mathbb{Z}$$

die $\mathbb{Z}$-lineare Abbildung, die in g den Wert 1 und in allen anderen Gruppen-Elementen den Wert 0 hat (duale Basis). Dann ist $\mathbb{Z}[G]^*$ die von den $\overset{\vee}{g}$ mit $g\in G$ erzeugte freie abelsche Gruppe. Die $\mathbb{Z}$-lineare Abbildung

$$\mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]^*, g \mapsto \overset{\vee}{g},$$

ist ein Isomorphismus von abelschen Gruppen und induziert einen Isomorphismus abelscher Gruppen $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G]^*, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$. Durch Zusammensetzen mit (***) erhalten wir die Abbildung

$$\mathbb{Z}[G]\otimes_{\mathbb{Z}} A \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A), \sigma\otimes a \mapsto (g \mapsto \overset{\vee}{g}(\sigma)\bullet a), \qquad (\#)$$

Es reicht zu zeigen, diese Abbildung ist bijektiv. Aus dem Beweis von Bemerkung (i) kennen wir die Bijektion

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) \longrightarrow \mathbb{Z}[G]\otimes_{\mathbb{Z}} A, \varphi \mapsto \sum_{g\in G} g\otimes\varphi(g). \qquad (\#\#)$$

Es reicht zu zeigen, (#) ist einseitige Inverse dieser Bijektion. Es gilt

$$g'\otimes a \overset{(\#)}{\mapsto} (g \mapsto \overset{\vee}{g}(g')\bullet a) \overset{(\#\#)}{\mapsto} \sum_{g\in G} g\otimes \overset{\vee}{g}(g')\bullet a = g'\otimes a,$$

d.h. (#) ist rechtsinvers zu (##).

F(ε) injektiv.

Die Abbildung F(ε*) läßt sich auch schreiben als

$$\mathrm{Hom}_{\mathbb{Z}}(P_0^*, A)^G \xrightarrow{F(\varepsilon^*)} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)^G$$

Der natürliche Homomorphismus (4) liefert ein kommuatives Diagramm

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(P_0^*,A)^G & \xrightarrow{F(\varepsilon^*)} & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z};A)^G \\ \cong\uparrow & & \uparrow \\ (P_0\otimes_{\mathbb{Z}}A)^G & \xrightarrow{\varepsilon\otimes id} & (\mathbb{Z}\otimes_{\mathbb{Z}}A)^G \end{array}$$

Die linke vertikale Abbildung ist bijekiv, weil P_0 ein freier und endlich erzeugter $\mathbb{Z}[G]$-Modul ist. Der oben definierte Homomorphismus N*: $A_G \longrightarrow A^G$ is funktoriell bezüglich A und liefert daher ein kommutatives Diagramm

$$\begin{array}{ccc} (P_0\otimes_{\mathbb{Z}}A)^G & \xrightarrow{\varepsilon\otimes id} & (\mathbb{Z}\otimes_{\mathbb{Z}}A)^G \\ N^*\uparrow\cong & & N^*\uparrow \\ (P_0\otimes_{\mathbb{Z}}A)_G & \xrightarrow{(\varepsilon\otimes id)_G} & (\mathbb{Z}\otimes_{\mathbb{Z}}A)_G \\ \| & & \| \\ P_0\otimes_{\mathbb{Z}[G]}A & & \mathbb{Z}\otimes_{\mathbb{Z}[G]}A \end{array}$$

Der linke vertikale Morphismus ist ein Isomorphismus, weil $P_0\otimes_{\mathbb{Z}}A$ ein induzierter Modul ist. Damit können wir F(ε*) mit der folgenden Komposition identifizieren.

$$F(\varepsilon^*): P_0\otimes_{\mathbb{Z}[G]} A \xrightarrow{\varepsilon\otimes id} A_G \xrightarrow{N^*} A^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \qquad (5)$$

Damit ist

$$\begin{aligned} H^0(\mathrm{Hom}_{\mathbb{Z}[G]}(L^*, A)) &= \mathrm{Ker}(\mathrm{Hom}_{\mathbb{Z}[G]}(P_0, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}[G]}(P_1, A))/\mathrm{Im}(F(\varepsilon)\circ F(\varepsilon^*)) \\ &= H^0(G, A)/\mathrm{Im}(F(\varepsilon)\circ F(\varepsilon^*)) && \text{(Bemerkung 1.4.4(v))} \\ &= A^G/\mathrm{Im}(F(\varepsilon^*)) && \text{(Injektivität von F(ε))} \\ &= A^G/\mathrm{Im}(N^*) && \text{(ε⊗id surjektiv)} \\ &= \mathrm{Koker}(N^*) \\ &= \hat{H}^0(G, A) && \text{(Definition von } \hat{H}^0\text{)} \end{aligned}$$

Weiter gilt

$$\begin{aligned} H^{-1}(\mathrm{Hom}_{\mathbb{Z}[G]}(L^*, A)) &= \mathrm{Ker}(F(\varepsilon)\circ F(\varepsilon^*))/\mathrm{Im}(P_1\otimes_{\mathbb{Z}[G]} A \longrightarrow P_0\otimes_{\mathbb{Z}[G]} A) \\ &= \mathrm{Ker}(F(\varepsilon^*))/\mathrm{Im}(P_1\otimes_{\mathbb{Z}[G]} A \longrightarrow P_0\otimes_{\mathbb{Z}[G]} A) && \text{(Injektivität von F(ε))} \\ &= \mathrm{Ker}(N^*\circ(\varepsilon\otimes id))/\mathrm{Im}(P_1\otimes_{\mathbb{Z}[G]} A \longrightarrow P_0\otimes_{\mathbb{Z}[G]} A) \end{aligned}$$

Mit der Sequenz

$$P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

ist auch die folgende exakt.

$$P_1 \otimes_{\mathbb{Z}[G]} A \longrightarrow P_0 \otimes_{\mathbb{Z}[G]} A \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \longrightarrow 0,$$

d.h.

$$\mathrm{Im}(P_1 \otimes_{\mathbb{Z}[G]} A \longrightarrow P_0 \otimes_{\mathbb{Z}[G]} A) = \mathrm{Ker}(P_0 \otimes_{\mathbb{Z}[G]} A \xrightarrow{\varepsilon\otimes id} \mathbb{Z} \otimes_{\mathbb{Z}[G]} A).$$

Damit ist

$$\begin{aligned} H^{-1}(\mathrm{Hom}_{\mathbb{Z}[G]}(L^*, A)) &= \mathrm{Ker}(N^* \circ (\varepsilon\otimes id))/\mathrm{Ker}(\varepsilon\otimes id) \\ &= \mathrm{Ker}(N^*) \qquad\qquad \text{(vgl. (5))} \\ &= \hat{H}^{-1}(G, A) \end{aligned}$$

QED.

Beweis von Bemerkung (vi). Seien $s \in G$ ein Erzeuger von G,

$$G = < s >,$$

und

$$n := \# G$$

die Ordnung von G.
Wir setzen

$$T := s - e \in \mathbb{Z}[G]$$

und bezeichen die Multiplikation mit s - e , zum Beispiel auf dem G-Modul A, ebenfalls mit T,

$$T: A \longrightarrow A,\ a \mapsto (s-e)\bullet a.$$

Es gilt

$$\begin{aligned} \mathrm{Ker}(T: A \longrightarrow A) &= \{ a \in A \mid (s-e)a = 0\} \\ &= \{ a \in A \mid sa = a\} \\ &= A^G \end{aligned}$$

Speziell für $A = \mathbb{Z}[G]$ erhalten wir

$$\begin{aligned} \mathrm{Ker}(T: \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]) &= \{ \sum_{g\in G} n_g \bullet g \mid n_g \in \mathbb{Z}\}^G \\ &= \{ \sum_{g\in G} n_g \bullet g \mid n_g \in \mathbb{Z} \text{ unabhängig von } g\} \\ &= \{ n \bullet N \mid n \in \mathbb{Z}\} \\ &=^{38} \{N \bullet \sigma \mid \sigma \in \mathbb{Z}[G]\} \\ &= \mathrm{Im}(N: \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]). \end{aligned}$$

Weiter gilt

$$\begin{aligned} \mathrm{Ker}(N: \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]) &= \{ \sum_{g\in G} n_g \bullet g \mid n_g \in \mathbb{Z},\ \sum_{g\in G} n_g = 0\} \\ &= \{ \sum_{g\in G} n_g \bullet (g-e) \mid n_g \in \mathbb{Z} \} \\ &= I_G \end{aligned}$$

---

[38] $N \bullet \sigma = n \bullet N$ mit n = Summe der Koeffizienten von σ.

Wegen $G = < s >$ hat jedes $g \in G$ die Gestalt $g = s^m$, d.h. es ist

$$g - e = s^m - e = (s-e)(s^{m-1} + s^{m-2} + ... + s + e) \in \text{Im}\,(T : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]),$$

also

$$\text{Ker}(N: \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]) \subseteq \text{Im}(T : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G])$$

Die umgekehrte Inklusion besteht ebenfalls:

$$N(T(\sigma)) = N \bullet (s-e) \bullet \sigma = (N \bullet s - N) \bullet \sigma = (N-N) \bullet \sigma = 0.$$

Für $A = \mathbb{Z}[G]$ gilt damit

$$\text{Ker}(T) = \text{Im}(N) = \mathbb{Z} \bullet N$$
$$\text{Ker}(N) = \text{Im}(T) = I_G$$

Wir haben damit exakte Sequenzen

$$P_*: ... \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \longrightarrow \mathbb{Z}[G]/I_G \longrightarrow 0$$

$$P^*: 0 \longrightarrow \mathbb{Z} \bullet N \longrightarrow \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} ...$$

Weil der G-Modul

$$\mathbb{Z}[G] = \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}$$

induziert (also auch koinduziert) ist, sind dies induzierte bzw. koinduzierte Auflösungen von

$$\mathbb{Z} \cong \mathbb{Z}[G]/I_G \cong \mathbb{Z} \bullet N.$$

Nun gehen beim Dualisieren (d.h. dem Anwenden des Funktors $\text{Hom}_{\mathbb{Z}}(? , \mathbb{Z})$) die Multiplikationen mit T bzw. N in sich über, d.h. beim Dualisieren von P_* erhält man gerade P^*. Die beiden Auflösungen setzen sich also zu einer vollen Auflösung

$$L^*: ... \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \longrightarrow (\mathbb{Z} \longrightarrow) \mathbb{Z}[G] \xrightarrow{T} \mathbb{Z}[G] \xrightarrow{N} ...$$

zusammen. Durch Anwenden von $\text{Hom}_{\mathbb{Z}[G]}(? , A)$ erhalten wir einen Komplex

$$\text{Hom}_{\mathbb{Z}[G]}(L^* , A): ... \xrightarrow{N} A \xrightarrow{T} A \,(\longrightarrow A^G) \longrightarrow A \xrightarrow{T} A \xrightarrow{N} ...,$$

dessen Kohomologie gerade die Tate-Gruppen sind:

$$\hat{H}^{2i}(G, A) = \hat{H}^0(G, A) = \text{Ker}(T)/\text{Im}(N) = A^G/N \bullet A$$
$$\hat{H}^{2i+1}(G,A) = \hat{H}^{-1}(G,A) = \text{Ker}(N)/\text{Im}(T) = {}_N A/I_G A.$$

QED.

1.4.7 Tate-Kohomologie und Dimensionsverschiebung

Sei G eine endliche Gruppe. Wie wir wissen, ist dann jeder G-Modul sowohl Teilmodul als auch Faktor-Modul eines (ko-) induzierten Moduls, d.h. äußerer Modul einer exakten Sequenz

$$0 \longrightarrow M' \longrightarrow C \longrightarrow M'' \longrightarrow 0$$

mit C (ko-)induziert. Die zugehörige lang Kohomomologie-Sequenz zerfällt in exakte Sequenzen

$$\begin{array}{ccccccc} \hat{H}^i(G,C) & \longrightarrow & \hat{H}^i(G,M'') & \longrightarrow & \hat{H}^{i+1}(G,M') & \longrightarrow & \hat{H}^{i+1}(G,C) \\ || & & & & & & || \\ 0 & & & & & & 0 \end{array}$$

d.h. es gilt

$$\hat{H}^i(G,M'') \cong \hat{H}^{i+1}(G,M')$$

für alle $i \in \mathbb{Z}$.

Bemerkungen

(i) Jede i-te Kohomologie-Gruppe ist auch (i+1)-te und (i-1)-te Kohomologie-Gruppe.

(ii) Was für festes i und alle i-ten Kohomolgie-Gruppen gilt, gilt für alle Kohomologie-Gruppen überhaupt.

(iii) Diese Tatsache wird es uns erlauben, Konstruktionen, Definitionen und Sätze für ein festes i anzugeben und dann auf alle ganzzahligen i auszudehnen. Diese Vorgehensweise wird auch Dimensionsverschiebung genannt.

(iv) Seien G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Dann sind die Restriktionsabbildungen

$$\text{Res: } H^i(G, M) \longrightarrow H^i(H, M) \text{ für jedes } i \geq 1$$

definiert (und mit den Zusammenhangshomomorphismen verträglich). Auf Grund der Dimensionsverschiebung, sind sie für alle Tate-Gruppen definiert.

$$\text{Res: } \hat{H}^i(G, M) \longrightarrow \hat{H}^i(H, M) \text{ für jedes } i \in \mathbb{Z}$$

definiert.[39] Man kann zeigen, für i = -1 werden sie gerade durch die Abbldung

$$N_{G/H}: M_G \longrightarrow M^G, m \mapsto \sum_i s_i^{-1} m,$$

induziert, wenn die $s_i \in G$ ein vollständiges Repräsentanten-System für die Restklassen von G/H bilden. Das folgende Diagramm ist kommutativ.[40]

$$\begin{array}{ccc} \hat{H}^{-1}(G,M) & \xrightarrow{\text{Res}} & \hat{H}^{-1}(H,M) \\ \cap & & \cap \\ M_G & \xrightarrow{N_{G/H}} & M_H \end{array}$$

(v) Analog sind die Korestriktionsabbildungen

$$\text{Cor: } H_i(H, M) \longrightarrow H_i(G, M) \text{ für jedes } i \geq 1$$

definiert (und mit den Zusammenhangshomomorphismen verträglich). Auf Grund der Dimensionsverschiebung sind sie für alle Tate-Gruppen definiert.

$$\text{Cor: } \hat{H}^i(H, M) \longrightarrow \hat{H}^i(G, M) \text{ für jedes } i \in \mathbb{Z}.$$

Man kann zeigen, für i = 0 sind sie gerade durch die Abbildung

$$N^{G/H}: M^H \longrightarrow M^G, m \mapsto \sum_i s_i m,$$

induziert, wobei wie oben die $s_i \in G$ ein vollständiges Respräsentantensystem für G/H bilden sollen. Das folgende Diagramm ist kommutativ.[41]

---

[39] Man verwendet die langen Kohomologie-Sequenzen für G und H und die Tatsache, daß der obige bezüglich G induzierte Modul C auch bezüglich H induziert ist.

[40] Die Inklusionen kommen von der Tatsache, daß die (-1)-te Tate-Kohomologie definiert ist als Kern der Abbildung

$$N: M_G \longrightarrow M^G \text{ bzw. } M_H \longrightarrow M^H,$$

also ein Teilmodul von M_G bzw. M_H ist.

$$\begin{array}{ccc} \hat{H}^0(H,M) & \xrightarrow{\text{Cor}} & \hat{H}^0(G,M) \\ \uparrow\uparrow & & \uparrow\uparrow \\ M^H & \xrightarrow{N^{G/H}} & M^G \end{array}$$

(vi) Die Zusammensetzeung von Restriktion und Korestriktion.

Für jede endliche Gruppe G und jede Untergruppe $H \subseteq G$ ist die Zusammensetzung

$$\hat{H}^i(G, M) \xrightarrow{\text{Res}} \hat{H}^i(H, M) \xrightarrow{\text{Cor}} \hat{H}^i(G, M)\ (i \in \mathbb{Z}),\ x \mapsto n \bullet x,$$

gerade die Multiplikation mit dem Index $n := (G:H)$.[42]

(vii) Jedes Element von $\hat{H}^i(G, M)$ wird durch die Gruppen-Ordnung $n := \# G$ annulliert,[43]

$$n \bullet \hat{H}^i(G, M) = 0.$$

Die Tate-Gruppen sind also Torsionsgruppen.[44]

(viii) Für jede endliche Gruppe G und jeden endlich erzeugten G-Modul M sind die Tate-Gruppen[45]

$$\hat{H}^i(G, M) \text{ endlich.}$$

(ix) Sei $S \subseteq G$ eine p-Sylow-Untergruppe der endlichen Gruppe G. Dann ist die Restriktion

$$\text{Res: } \hat{H}^i(G, M) \longrightarrow \hat{H}^i(S, M)$$

injektiv auf der p-primären Komponente ihres Definitionsbereichs (d.h. der Untergruppe aller Elemente, die von einer p-Potenz annulliert werden).[46]

(x) Seien G eine endliche Gruppe und

$$x \in \hat{H}^i(G, M)$$

ein Element, welches im Kern der Restriktion

$$\text{Res: } \hat{H}^i(G, M) \longrightarrow \hat{H}^i(S, M)$$

liegt für jede p-Sylow-Untergruppe $S \subseteq G$. Dann gilt $x = 0$.[47]

---

[41] Die Surjektionen kommen von der Tatsache, daß die 0-te Tate-Kohomologie definiert ist als Kokern der Abbildung

$$N: M_G \longrightarrow M^G \text{ bzw. } M_H \longrightarrow M^H,$$

also ein Faktor-Modul von M^G bzw. M^H ist.

[42] Dies folgt as den Bemerkungen 1.4.7 (iv) und (v).

[43] Man wende (vi) auf die triviale Untergruppe $H = \{e\}$ an.

[44] d.h. jedes Element hat eine endliche Ordnung.

[45] Mit M sind auch die Tate-Gruppen endlich erzeugt (und nach (vii) sind alle Elemente von endlicher Ordnung).

[46] Es reicht zu zeigen, die Zusammensetzung mit der zugehörigen Korestriktion ist injektiv, d.h. die Multiplikation mit (G:S) ist injektiv. Weil S eine p-Sylow-Untergruppe ist, ist aber (G:S) eine zu p teilerfremde Zahl. Ein Element, welches von einer p-Potenz und der zu p teilerfremden Zahl (G:S) annulliert wird, muß aber selbst schon Null sein.

[47] Die p-primären Komponenten zu je zwei verschiedenen p haben den Durchscbnitt 0. Es ist nicht sehr schwer, zu zeigen, jede abelsche Gruppe aus Elementen endlicher Ordnung ist gleich der direkten Summe ihrer p-primären Kompoenten.

Bevor wir zur Kohomologie der proendlichen Gruppen und der Galois-Kohomologie übergehen können, müssen wir noch eine Konstruktion beschreiben, die es für die meisten Kohomolgie-Theorien gibt: das Cup-Produkt. Es definiert eine multiplikative Struktur auf den Kohomologie-Gruppen, durch welche zum Beispiel die direkte Summe der Kohomologie-Gruppen mit Koeffizienten in $\mathbb{Z}$ ein Ring wird.

1.4.8 Cup-Produkte

Sei G eine endliche Gruppe. Dann gibt es genau eine eine Familie von Gruppen-Homomorphismen

$$\hat{H}^i(G, A)\otimes_{\mathbb{Z}}\hat{H}^j(G, B) \longrightarrow \hat{H}^{i+j}(G, A\otimes_{\mathbb{Z}}B),\ a,\otimes b \mapsto a\bullet b,$$

wobei i und j die ganzen Zahlen und A und B die G-Moduln durchlaufen, sodaß die folgenden Bedingungen erfüllt sind.

(i) Die Homomorphismen hängen funktoriell von A und B ab.

(ii) Für i = j = 0 wird der Homomorphismus durch die natürliche Abbildung

$$A^G\otimes_{\mathbb{Z}}B^G \longrightarrow (A\otimes_{\mathbb{Z}}B)^G$$

induziert.

(iii) Verträglichkeit mit den Zusammenhangshomomorphismen I. Für jede exake Sequenz von G-Moduln

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0$$

und jeden G-Modul B, für welchen die Sequenz

$$0 \longrightarrow A'\otimes_{\mathbb{Z}}B \longrightarrow A\otimes_{\mathbb{Z}}B \longrightarrow A''\otimes_{\mathbb{Z}}B \longrightarrow 0$$

exakt ist, gilt

$$(\delta a'')\bullet b = \delta(a''\bullet b) \in \hat{H}^{i+j+1}(G, A'\otimes_{\mathbb{Z}}B)$$

für beliebige $a''\in \hat{H}^i(G,A'')$ und $b\in \hat{H}^j(G, B)$. Dabei soll δ die Zusammenhangshomo-morphismen

$$\hat{H}^i(G,A'') \longrightarrow \hat{H}^{i+1}(G,A') \text{ bzw. } \hat{H}^{i+j}(G,A''\otimes_{\mathbb{Z}}B) \longrightarrow \hat{H}^{i+j+1}(G,A'\otimes_{\mathbb{Z}}B)$$

zu den beiden kurzen exakten Sequenzen bezeichnen.

(iv) Verträglichkeit mit den Zusammenhangshomomorphismen II Für jede kurze exakte Sequenz von G-Moduln

$$0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$$

und jeden G-Modul A, für welchen die Sequenz

$$0 \longrightarrow A\otimes_{\mathbb{Z}}B' \longrightarrow A\otimes_{\mathbb{Z}}B \longrightarrow A\otimes_{\mathbb{Z}}B'' \longrightarrow 0$$

exakt ist, gilt

$$a\bullet(\delta b'') = (-1)^i\delta(a\bullet b'') \in \hat{H}^{i+j+1}(G, A\otimes_{\mathbb{Z}}B')$$

für beliebige $a \in \hat{H}^i(G,A)$ und $b''\in \hat{H}^j(G, B'')$. Dabei soll δ die Zusammenhangshomo-morphismen

$$\hat{H}^j(G,B'') \longrightarrow \hat{H}^{j+1}(G,B') \text{ bzw. } \hat{H}^{i+j}(G,A\otimes_{\mathbb{Z}}B'') \longrightarrow \hat{H}^{i+j+1}(G,A\otimes_{\mathbb{Z}}B')$$

Das Element $a\bullet b \in \hat{H}^{i+j}(G, A\otimes_{\mathbb{Z}}B)$ mit $a \in \hat{H}^i(G, A)$ und $b\in\hat{H}^j(G, B)$ heißt Cup-Produkt von a und b.

Bemerkungen

(i) Der natürliche Isomorphismus

$$(A\otimes_{\mathbb{Z}}B)\otimes_{\mathbb{Z}}C \cong A\otimes_{\mathbb{Z}}(B\otimes_{\mathbb{Z}}C)$$

führt zur Identifikation

$$(a\bullet b)\bullet c = a\bullet(b\bullet c).$$

(ii) Der natürliche Isomorphismus

$$A\otimes B \cong B\otimes A$$

führt zu Idenfikation

$$a\bullet b = (-1)^{\dim a \,\bullet\, \dim b}\, b\bullet a.$$

(iii)

$$\mathrm{Res}(a\bullet b) = \mathrm{Res}(a)\bullet\mathrm{Res}(b).$$

(iv) Projektionsformel.

$$\mathrm{Cor}(a\bullet\mathrm{Res}(b) = \mathrm{Cor}(a)\bullet b.$$

(v) Periodizität. Seien G eine zyklische Gruppe der Ordnung n und ξ ein Erzeuger der Gruppe

$$\hat{H}^2(G, \mathbb{Z}) = \mathbb{Z}^G/N\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}.$$

Dann definiert für jeden G-Modul A das Cup-Produkt mit ξ Isomorphismen

$$\hat{H}^i(G, A) \longrightarrow \hat{H}^{i+2}(G, A),\ a \mapsto \xi\bullet a.$$

(vi) Kohomologische Trivialität I.
Seien G eine endliche Gruppe und A ein G-Modul. Dann sind folgende Aussagen äquivalent.

1. A ist kohomologisch trivial: $\hat{H}^i(G, A) = 0$ für jedes $i\in\mathbb{Z}$.
2. Für jede Primzahl p gibt ein $i \in \mathbb{Z}$ derart, daß für die p-Sylow-Untergruppe G_p von G gilt
$$\hat{H}^i(G_p, A) = \hat{H}^{i+1}(G_p, A) = 0.$$
3. Für jede Primzahl p ist A kohomologisch trivial über G_p.
4. A besitzt eine projektive Auflösung der Länge ≤ 1,
$$0 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow A \longrightarrow 0.$$

(vii) Kohomologische Trivialität II.
Seien G eine endliche Gruppe und A ein $\mathbb{Z}$-freier G-Modul. Dann sind folgende Aussagen äquivalent.

1. A ist kohomologisch trivial.
2. Für jedes p ist A/pA ein freier $\mathbb{F}_p[G]$-Modul.
3. A ist ein projektiver G-Modul.

(Die Aussagen sind auch äquivalent - für fest vorgegebenes p in Aussage 2 - falls G eine p-Gruppe ist und A keine p-Torsion besitzt).

(viii) Kohomologische Trivialität III.
Seien G eine p-Gruppe und A ein G-Modul mit pA = 0. Dann sind folgende Aussagen äquivalent.

1. A ist kohomologisch trivial.
2. A ist ein induzierter G-Modul.
3. A ist ein freier $\mathbb{F}_p[G]$-Modul.

4. $\hat{H}^i(G, A) = 0$ für ein $i \in \mathbb{Z}$.

Unser nächstes Ziel ist die Einführung der Kohomologie der proendlichen Gruppen und der Galois-Kohomologie. Das wichtigste Beispiel einer proendlichen Gruppe ist die Galois-Gruppe einer unendlichen Körper-Erweiterung. Wir beginnen deshalb mit einer Beschreibung dieser Galois-Gruppe.

1.4.9 Galois-Theorie und projektive Systeme

Sei K/k eine (nicht notwendig endliche) Galois-Erweiterung, d.h. eine separable und normale algebraische Körper-Erweiterung. Wir bezeichnen mit

$$G(K/k)$$

die Galois-Gruppe dieser Erweiterung, d.h. die Gruppe der Automorphismen von K, welche k elementweise fest lassen.

Bemerkungen

(i) Weil K/k algebraisch ist, liegt jedes Element von K bereits in einer endlichen Galoisschen Teilerweiterung von K, d.h.

$$K = \bigcup \{ K' \mid k \subseteq K' \subseteq K, K'/k \text{ endliche Galois-Erweiterung} \}$$

Für jeden k-Automorphismus $\sigma: K \longrightarrow K$ ist die Einschränkung $\sigma|_{K'}: K' \longrightarrow K'$ auf eine endliche Galoissche Teilerweiterung ein k-Automorphismus von K'. Durch Einschsränken erhalten wir einen Gruppen-Homomorphismus

$$\Phi_{KK'}: G(K/k) \longrightarrow G(K'/k),\ \sigma \mapsto \sigma|_{K'}.$$

Umgekehrt läßt sich jeder k-Automorphismus von K' zu einem k-Automorphismus von K fortsetzen (weil K/k algebraisch und normal ist). Dieser Homomorphismus ist somit surjektiv. Sein Kern ist die Galois-Gruppe G(K/K'). Wir erhalten somit eine exakte Sequenz

$$0 \longrightarrow G(K/K') \longrightarrow G(K/k) \xrightarrow{\Phi_{KK'}} G(K'/k) \longrightarrow 0$$

für jede Galois-Erweiterung K/k und jede (nicht notwendig endliche) Teilerweiterung K'/k.

(ii) Für je zwei endliche Galoissche Teilerweiterungen K'/k und K"/k mit

$$k \subseteq K' \subseteq K" \subseteq K$$

definiert die Einschränkdung von k-Automorphismen auf Teilkörper ein kommutatives Diagramm

$$\begin{array}{ccc} G(K/k) & \xrightarrow{\Phi_{KK'}} & G(K'/k) \\ {\scriptstyle F_{KK"}}\downarrow & \nearrow{\scriptstyle \Phi_{K"K'}} & \\ G(K"/k) & & \end{array}$$

Eine Familie von Morphismen $\phi_{\alpha\beta}: G_\beta \longrightarrow G_\alpha$ einer Kategorie $\mathcal{C}$, wobei die Indizes α, β in einer halbgeordneten Menge I liegen und der Bedingung $\alpha \leq \beta$ genügen, heißt projektives System, wenn für je drei Indizes α, β, γ mit $\alpha \leq \beta \leq \gamma$ das Diagramm

$$\begin{array}{ccc} G_\gamma & \xrightarrow{\phi_{\gamma\alpha}} & G_\alpha \\ {\scriptstyle \phi_{\gamma\beta}}\downarrow & \nearrow{\scriptstyle \phi_{\beta\alpha}} & \\ G_\beta & & \end{array}$$

kommutativ ist.[48]

Die Galois-Gruppen der endlichen Galoisschen Teilerweiterungen von K/k bilden also ein projektives System.[49]

Faßt man die Index-Menge I als Kategorie auf, deren Objekte die Indizes und deren Morphismen die Kleiner-Gleich-Beziehungen $\alpha \leq \beta$ sind, so ist das projektive System nichts anderes als ein kontravarianter Funktor[50]

$$\underline{G}: I^{op} \longrightarrow \mathcal{C}, \alpha \mapsto G_\alpha, \alpha \leq \beta \mapsto \phi_{\beta\alpha}: G_\beta \longrightarrow G_\alpha.$$

(iii) Morphismen projektiver Systeme. Ist ein weiteres solches projektives System

$$\underline{G'}: I^{op} \longrightarrow \mathcal{C}, \alpha \mapsto G'_\alpha, \alpha \leq \beta \mapsto \phi'_{\beta\alpha}: G'_\beta \longrightarrow G'_\alpha.$$

(zur selben Index-Menge) gegeben, so ist ein funktorieller Morphismus

$$\underline{G'} \longrightarrow \underline{G}$$

nichts anderes als eine Familie von Morphismen in $\mathcal{C}$,

$$G'_\alpha \xrightarrow{\phi_\alpha} G_\alpha, \alpha \in I,$$

mit der Eigenschaft, daß für je zwei Indizes $\alpha, \beta \in I$ mit $\alpha \leq \beta$ das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} G'_\beta & \xrightarrow{\phi_\beta} & G_\beta \\ {\scriptstyle \phi_{\beta\alpha}}\downarrow & & \downarrow{\scriptstyle \phi'_{\beta\alpha}} \\ G'_\alpha & \xrightarrow{\phi_\alpha} & G_\beta \end{array}$$

Ein solcher funktorieller Morphismus heißt auch Morphismus von projektiven Systemen,

$$\{\phi'_{\beta\alpha}: G'_\beta \longrightarrow G'_\alpha\}_{\alpha \in I,\, \beta \leq \alpha} \longrightarrow \{\phi_{\beta\alpha}: G_\beta \longrightarrow G_\alpha\}_{\alpha \in I,\, \beta \leq \alpha}$$

Betrachtet man zum Beispiel neben dem projektiven System der Gruppen-Homomorphismen

$$\Phi_{K''K'}: G(K''/k) \longrightarrow G(K'/k) \text{ mit } k \subseteq K' \subseteq K'' \subseteq K$$

noch das projektive System der identischen Morphismus

$$\mathrm{Id}: G(K/k) \longrightarrow G(K/k) \text{ mit } k \subseteq K' \subseteq K'' \subseteq K,$$

so definieren die Einschränkungshomomorphismen

$$\Phi_{KK'}: G(K/k) \longrightarrow G(K'/k),$$

einen Morphismus von projektiven Systemen[51]

$$\{\mathrm{Id}: G(K/k) \longrightarrow G(K/k)\}_{K' \subseteq K''} \longrightarrow \{\Phi_{K''K'}: G(K''/k) \longrightarrow G(K'/k)\}_{K' \subseteq K''}$$

(iv) Limites. Ein projektives System

$$\mathcal{G} := \{\phi_{\beta\alpha}: G_\beta \longrightarrow G_\alpha\}_{\alpha \in I,\, \beta \leq \alpha} \qquad (1)$$

---

[48] Ein induktives System ist ein System, welches projektiv in der dualen Kategorie ist.

[49] Die Halbordnung der Index-Menge {K'} ist die Inklusion '$\subseteq$' von Teilkörpern.

[50] Analog ist ein induktives System ein kovarianter Funktor

$$I^{op} \longrightarrow \mathcal{C}, \alpha \mapsto G_\alpha, \alpha \leq \beta \mapsto \phi_{\alpha\beta}: G_\alpha \longrightarrow G_\beta.$$

[51] Wegen der Kommutativität der Diagramme von Bemerkung (ii).

dessen sämtliche Objekte gleich sind und dessen sämtliche Morphismen gleich dem identischen Morphismus sind,

$$G_\alpha = G \text{ und } \phi_{\beta\alpha} = Id,$$

heißt konstantes projektives System zum Objekt $G \in \mathcal{C}$ und wird mit

$$const_G$$

Sei jetzt (1) irgend ein projektives System von $\mathcal{C}$, G ein Objekt von $\mathcal{C}$ und

$$\phi = \{\phi_\alpha\}:const_G \longrightarrow \mathcal{G} \qquad (2)$$

ein Morphismus projektiver Systeme. Man sagt dann, G ist projektiver Limes[52] oder auch Limes oder auch inverser Limes von $\mathcal{G}$ und schreibt

$$G = \varprojlim \mathcal{G} = \varprojlim_{\alpha \in I} G_\alpha$$

falls der Morphismus universell im folgenden Sinne ist: für jedes Objekt G' von $\mathcal{C}$ und jedem Morphismus

$$\phi' = \{\phi'_\alpha\}:const_{G'} \longrightarrow \mathcal{G}$$

von projektiven Systemen gibt es genau einen Morphismus

$$f:G' \longrightarrow G$$

in $\mathcal{C}$ derart, daß das folgende Diagramm kommutativ ist,

$$\begin{array}{ccc} const_{G'} & \xrightarrow{\phi'} & \mathcal{G} \\ {\scriptstyle f_*}\downarrow & \nearrow{\scriptstyle \phi} & \\ const_G & & \end{array}$$

d.h. für jedes $\alpha \in I$ ist das Diagramm

$$\begin{array}{ccc} G' & \xrightarrow{\phi'_\alpha} & G_\alpha \\ {\scriptstyle f}\downarrow & \nearrow{\scriptstyle \phi_\alpha} & \\ G & & \end{array}$$

kommutativ.
Man kann zeigen, alle diese projektiven Limites existieren in (additiven) Kategorien genau dann, wenn die Kategorie Produkte und Kerne besitzt.[53] In der Kategorie der Gruppen sowie in Ens, Top, Ab, R-Mod, Mod-R, Cat kann man die projektiven Limites wie folgt beschreiben[54]

---

[52] Ein induktiver oder auch direkter Limes oder auch Kolimes ist ein projektiver Limes in der dualten Kategorie.

[53] Läßt man "additiv" weg, so muß man "Kerne" durch "Differenzkerne" ersetzen. Ersetzt man "Produkte" durch "endliche Produkte" so muß man "projektive Limites" durch "endliche projektive Limites" ersetzen (d.h. solche mit endlichen Index-Mengen).

[54] Analog kann man die direkten Limites in der folgenden Gestalt schreiben.

$$\varinjlim \mathcal{G} = \oplus_{\alpha \in I} G_\alpha /\sim$$

wobei $\sim$ die kleinste Äquivalenz-Relation bezeichnet, für welche die beiden Elemente $x_\alpha \in G_\alpha$ und $x_\beta \in G_\beta$ genau dann äquivalent sind, wenn es ein $\gamma \in I$ gibt, für welches $\phi_{\alpha\gamma}$ und $\phi_{\beta\gamma}$ existieren und

$$\phi_{\alpha\gamma}(x_\alpha) = \phi_{\beta\gamma}(x_\beta)$$

gilt.

$$\varprojlim \mathcal{G} = \{(g_\alpha) \in \prod_{\alpha \in I} G_\alpha \mid \phi_{\beta\alpha}(g_\beta) = g_\alpha\}$$

Man beachte die natürlichen Projektionen des direkten Produkts induzieren natürliche Morphismen

$$\varprojlim \mathcal{G} \longrightarrow G_\alpha$$

Es ist nicht schwer zu zeigen, der zugehörige Morphismes des constanten projektiven Systems in das projektive System der G_α besitzt die Universalitätseingenschaft eines Limes.

(v) Ersetzt man jedes G_α durch das natürliche Bild von $\varprojlim \mathcal{G}$ in G_α, so erhält man ein neues projektives System mit demselben Limes. Die Morphismen $\phi_{\alpha\beta}$ dieses neuen Systems sind dann surjektiv (!).

(vi) Verallgemeinerung. In den oben angegebenen Konstruktionen kann man die halbgeordnete Menge I durch eine beliebige Kategorie ersetzen, d.h. einen beliebigen Funktor

$$F: I^{0p} \longrightarrow \mathcal{C}$$

betrachten. Für jedes Objekt $G \in \mathcal{C}$ hat man dann den konstanten Funktor

$$\text{const}_G: I^{0p} \longrightarrow \mathcal{C},$$

der jedem Objekt von I das Objekt G und jedem Morphismus von I den identischen Morphismus von $\mathcal{C}$ zuordnet. Ein Limes oder auch inverser Limes oder auch projektiver Limes des Funktors F ist dann ein Objekt

$$G = \varprojlim_{\alpha \in I} F(\alpha)$$

zusammen mit einer natürlichen Transformation

$$\xi: \text{const}_G \longrightarrow F$$

derart daß sich jede natürliche Transformation der Gestatl $\text{const}_{G'} \longrightarrow F$ (mit $G' \in \mathcal{C}$) eindeutig über ξ faktorisiert. Ersetzt man die Kategorie I (oder die Kategorie $\mathcal{C}$) durch deren Dual, so erhält man den Begriff des Kolimes oder direkten Limes oder induktiven Limes eines Funktors.

(vii) Beispiel G(K7k). Ein Beispiel für einen solchen projektiven Limes ist die Galois-Gruppe einer nicht-notwendig endlichen Galois-Erweiterung K/k. Genauer, wir wollen jetzt zeigen

$$G(K/k) = \varprojlim_{\substack{k \subseteq K' \subseteq K \\ K'/k \text{ endl.,Galoisch}}} G(K'/k)$$

Zum Beweis geben wir eine Familie von "verträglichen" Gruppen-Homomorphismen

$$\phi_{K'}: G \longrightarrow G(K'/k),\ k \subseteq K' \subseteq K,\ K'/k \text{ endliche Galois-Erweiterung}$$

vor, wobei G irgendeine Gruppe ist. "Verträglich" bedeutet dabei, für je zwei endliche algebraische Galois-Erweiterungen K', K" zwischen k und K mit

$$K' \subseteq K"$$

ist das folgende Diagramm kommutativ.

$$\begin{array}{ccc} G & \xrightarrow{\phi_{K'}} & G(K'/k) \\ {\scriptstyle \phi_{K''}}\downarrow & \nearrow_{\Phi_{K''K'}} & \\ G(K''/k) & & \end{array}$$

(vergleiche das erste Diagramm von (ii)). Mit anderen Worten, für jedes $g \in G$ gilt

$$\phi_{K'}(g) = \Phi_{K''K'}(\phi_{K''}(g)) = \phi_{K''}(g)|_{K'}, \quad (3)$$

Der Automorphismus $\phi_{K''}(g)\colon K'' \longrightarrow K''$ ist somit eine Fortsetzung des Automorphismus $\phi_{K'}(g)\colon K' \longrightarrow K'$. Für vorgegebenes $x \in K$ können wir eine endliche Galois-Erweiterung K'/k mit $K' \subseteq K$ und $x \in K'$ wählen und setzen

$$\phi(g) = \phi_{K'}(g)(x).$$

Wegen (3) ist diese Definition von der speziellen Wahl von K' unabhängig. Nach Definition gilt

$$\phi|_{K'} = \phi_{K'} \text{ für jedes } K'. \quad (4)$$

Insbesondere induziert ϕ auf jedem K' einen k-Automorphismus und ist damit ein k-Automorphismus von K. Wir haben eine Abbildung

$$\phi\colon G \longrightarrow G(K/k)$$

konstruiert. Da die $\phi_{K'}$, Gruppen-Homomorphismen sind, gilt dasselbe auch auch für ϕ. Nach (4) ist das folgende Diagramm kommutativ für jedes K'.

$$\begin{array}{ccc} G & \xrightarrow{\phi_{K'}} & G(K'/k) \\ {\scriptstyle \phi}\downarrow & \nearrow_{\phi_{KK'}} & \\ G(K/k) & & \end{array}$$

Außerdem ist ϕ durch die Kommutativität dieser Diagramme eindeutig festgelegt.[55] Wir haben gezeigt, die Galois-Gruppe G(K/k) ist projektiver Limes der Galois-Gruppen der endlichen Teilerweiterungen K'/k.

(viii) ogie. Die Galois-Gruppen G(K'/k) zu den endlichen Galoisschen Teilerweiterungen K' sind endlich. Wir versehen sie mit der diskreten Topologie. Unter den Topologien der Gruppe G(K/k), für welche die Homomorphismen[56]

$$\Phi_{KK'}\colon G(K/k) \longrightarrow G(K'/K)$$

stetig sind, gibt es dann eine schwächste.[57] Es ist klar, daß in dieser Topologie die Mengen der Gestalt[58]

$$\sigma \bullet \mathrm{Ker}(\Phi_{KK'}) = \Phi_{KK'}^{-1}(\Phi_{KK'}(\sigma))$$

offen sein müssen. Man überprüft leicht, daß die Mengen dieser Gestalt die Basis einer Topologie bilden (und daß die Mengen dieser Gestalt mit festem σ dann eine Umgebungsbasis von σ bilden)[59]. Sie definieren also gerade diese schwächste Topologie. Wir wollen im folgenden G(K/k) mit dieser Topologie versehen.

---

[55] Die Einschränkungen von ϕ auf alle endlichen Galoisschen Teilerweiterungen K' sind dadurch festgelegt.

[56] mit K'/k endliche Galoissche Teilerweiterung von K/k

[57] Eine mit möglichst wenigen offenen Mengen.

[58] mit $\sigma \in G(K/k)$ und K'/k endliche Galoissche Teilerweiterung von K/k.

[59] Man hat zu zeigen, für jedes Element aus dem Durchschnitt zweier Mengen dieser Gestalt gibt es eine Menge dieser Gestalt, die ganz in diesem Durchschnitt liegt und das gegebene Element enthält.

(ix) Hauptsatz der Galois-Theorie. Sei K/k eine Galois-Erweiterung. Dann ist die Abbildung

$$\{\text{Teilerweiterungen von } K/k\} \longrightarrow \{\text{abgeschlossene Untergruppen von } G(K/k)\},$$

$$K' \qquad \mapsto \qquad G(K/K'),$$

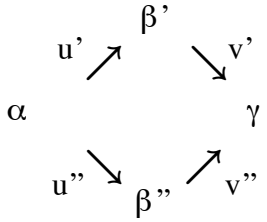
wohldefiniert und bijektiv, wobei die Umkehrabbildung die folgende Gestalt hat.

$$H \mapsto K^H := \{x \in K \mid hx = x \text{ für jedes } h \in H\}.$$

Die offenen Untergruppen entsprechen bei dieser Bijektion gerade den endlichen Teilerweiterungen.[60]

(x) Filtrierende Limites.
Eine nicht-leere Kategorie heißt filtrierend, wenn die folgenden Bedingungen erfüllt sind.

1. Für je zwei Morphismen $u'\colon \alpha \longrightarrow \beta'$ und $u''\colon \alpha \longrightarrow \beta''$ von I mit derselben Quelle α gibt es zwei Morphismen $v'\colon \beta' \longrightarrow \gamma$ und $v''\colon \beta'' \longrightarrow \gamma$ von I mit demselben Ziel γ derart, daß das Diagramm



kommutativ ist.
2. Gilt $\beta' = \beta''$ in der Situation von (i), so kann man die Morphismen v', v'' sogar so wählen, daß $v' = v''$ gilt.
3. Für je zwei Objekte β', β'' von I gibt es zwei Morphismen $v'\colon \beta' \longrightarrow \gamma$ und $v''\colon \beta'' \longrightarrow \gamma$ von I mit demselben Ziel.

Projektive Systeme über filtrierenden Index-Mengen heißen filtrierend.

Projektive Limites von filtrierenden projektiven Systemen heißen auch filtrierende Limites.[61]

Für Kategorien I zu halb geordneten Mengen folgen die Bedingungen 1 und 2 aus Bedingung 3.

---

[60] Alle offenen Untergruppen sind abgeschlossen.

[61] Eine Kategorie heißt kofiltrierend, wenn die duale Kategorie filtrierend ist. Induktive Limites

$$G = \varinjlim G = \varinjlim_{\alpha \in I} G_\alpha$$

von induktiven Systemen über kofiltrierenden heißen kofiltrierende Kolimites. Für die obige mengentheoreitsche Beschreibung der induktiven Limites bedeutet dies:

1) Für jedes Element $x \in G$ gibt es ein $\alpha \in I$ derart, daß x Bild eines Elements $x_\alpha \in G_\alpha$ ist beim natürlichen Morphismus

$$G_\alpha \longrightarrow G.$$

2) Zwei Elemente $x_\alpha \in G_\alpha$ und $x_\beta \in G_\beta$ haben genau dann dasselbe Bild in G, wenn es eine obere Schranke $\gamma \in I$ von α und β derart gibt, daß die Bilder von x_α und x_β in G_γ übereinstimmen.

Letztere Bedingung ist im Fall der Familie der endlichen Galois-Teilerweiterungen der Erweiterung K/k erfüllt: für je zwei endliche Galois-Teilerweiterungen K'/k und K"/k von K/k gibt es eine weitere endliche Galois-Teilerweiterung L/k mit

$$K' \subseteq L \text{ und } K'' \subseteq L.$$

1.4.10 Proendliche Gruppen

Eine proendliche Gruppe ist eine Gruppe, welche Limes eines filtrierenden[62] projektiven Systems von endlichen Gruppen ist.

$$G = \varprojlim_{\alpha \in I} G_\alpha$$

Analog ist eine Pro-p-Gruppe, wobei p eine Primzahl bezeichne, definiert als Limes eines filtrierenden projektiven Systems von p-Gruppen, d.h. von Gruppen deren Ordnung eine Potenz von p ist.

Beispiele

(i) Die Galois-Gruppe jeder nicht-notwending endlichen Galois-Gruppe ist eine proendliche Gruppe.

(ii) Für jede Gruppe G bilden die endlichen Faktor-Gruppen G/N ein (filtrierendes)[63] projektives System. Dessen Limes

$$\hat{G} := \varprojlim_{N \subseteq G \text{ Normalteiler mit endl. Index}} G/N \; \left(\subseteq \prod_{N \subseteq G} G/N \right)$$

ist eine proendliche Gruppe, welche proendliche Vervollständigung heißt. Die natürlichen Projektionen $G \longrightarrow G/N$ definieren einen natürlichen Homomorphismus

$$G \longrightarrow \hat{G}\,,\; g \mapsto (g \bmod N)_{N \subseteq G}.$$

(iii) Für jede Gruppe G und jede Primzahl p bilden die Faktor-Gruppen G/N von p-Potenz-Index ein projektives System. Dessen Limes

$$\hat{G}_p := \varprojlim_{(G:N)=\text{p-Potenz}} G/N$$

heißt p-adische Vervollständigung von G. Es ist ein Beispiel für eine Pro-p-Gruppe. Ist $G = \mathbb{Z}$ die additive Gruppe der ganzen Zahlen, so ist

---

[62] Durch die Forderung, filtrierend zu sein, wird sichergestellt, daß die Kerne der natürlichen Abbildungen

$$G \longrightarrow G_\alpha$$

eine Umgebungsbasis des neutralen Elements bilden: im Durchschnitt von je zwei solchen Kernen ist ein solcher Kern ganz enthalten. Ohne die Forderung an das projektive System, filtrierend zu sein, wäre die Topologie der Gruppe G komplizierter.

Außerden erhält man durch Anwenden von kontravarianten Funktoren auf solche System kofiltrierende induktive Systeme, deren Kolimites wie oben angebenen eine einfachere Beschreibung als im allgemeinen Fall besitzen.

[63] Für je zwei solche endlichen Faktorgrujppen G/N' und G/N" hat man eine exakte Sequenz

$$0 \longrightarrow N'/N' \bigcap N'' \longrightarrow G/N' \bigcap N'' \longrightarrow G/N' \longrightarrow 0,$$

wobei die beiden äußeren Gruppen G/N' und

$$N'/N' \bigcap N'' \cong N'N''/N'' \subseteq G/N''$$

endlicb sind. Also ist auch $G/N' \bigcap N''$ endlich.

$$\hat{\mathbb{Z}}_p = \{ \sum_{n=0}^{\infty} a_n \cdot p^n \mid 0 \leq a_n < p \}$$

gerade die additve Gruppe der p-adischen Zahlen (d.h. die additive Gruppe des Rings, welchen man erhält, wenn man den Ring der ganzen Zahlen bezüglich der p-adischen Topologie vervollständigt)[64].

(iv) (See Serre [1], I, §1, Section 1.5).Seien p eine Primzahl, I eine beliebige Menge und

$$L(I)$$

die von I erzeugte freie Gruppe[65] Bezeichne X die Familie der Normalteiler $N \subseteq L(I)$ mit

1. L(I)/N ist eine endliche p-Gruppe.
2. N enthält fast alle $\alpha \in I$ (d.h. alle bis auf endliche viele).

Dann bilden die Faktorgruppen L(I)/N ein projektives System über X, und wir setzen

$$F(I) := \varprojlim_{N \in X} L(I)/N.$$

Die Pro-p-Gruppe F(I) heißt die von I erzeugte freie Pro-p-Gruppe. Diese Bezeichnung ist auf Grund der folgende Universalitätseigenschaft der natürlichen Abbildung

$$I \longrightarrow F(I)$$

gerechtfertigt.

Für jede Abbildung $f: I \longrightarrow G$ mit Werten in einer Pro-p-Gruppe G mit der Eigenschaft, daß für jeden offenen Normalteiler $N \subseteq G$ fast alle Elemente von f(I) in N liegen, gibt es genau einen stetigen Homomorphismus $F(I) \longrightarrow G$, dessen Einschränkung auf I gleich f ist.

Läßt man in der Definition von F(I) die zweite Bedingung weg, so erhält man gerade die p-adische Vervollständigung $F_s(I)$ von L(I). Diese hat die analoge Universalitätseigenschaft, bei der man an die Abbildungen $f: I \longrightarrow G$ mit Werten in der Pro-p-Gruppe G keinerlei Bedingung stellt. Man kann zeigen, daß $F_s(I)$ eine freie Pro-p-Gruppe ist (mit einem anderen I, siehe Serre [1]).

---

[64] Für zwei ganze Zahlen $a, b \in \mathbb{Z}$ setzt man

$$d(a, b) = p^{-n},$$

wenn ihre Differenz durch p^n aber nicht durch p^{n+1} teilbar ist. Im Fall a = b setzt man d(a, b) = 0. Auf diese Weise ist auf $\mathbb{Z}$ eine Metrik definiert, die p-adische Metrik. $\hat{\mathbb{Z}}_p$ ist die Vervollständigung von $\mathbb{Z}$ bezüglich dieser Metrik.

[65] Für jedes Element $\alpha \in I$ führen wir ein Symbol α^{-1} ein. Bezeichne I^{-1} die Menge der α^{-1}.
Die Elemente von L(I) sind dann die Wörter über dem Alphabet $I \cup I^{-1}$ und die Multiplikation besteht aus dem Zusammenfügen dieser Wörter. Dabei besteht die Relation $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$ (:= leeres Wort).

Bemerkungen

(i) Sei die proendliche Gruppe G der Limes des projektiven Systems

$$\mathcal{G} = \{\phi_{\beta\alpha}: G_\beta \longrightarrow G_\alpha\}_{\alpha,\beta\in I,\ \alpha\le\beta}$$

der endlichen Gruppen G_α. Nach Bemerkung 1.4.9 (iv) gilt dann

$$G = \{(g_\alpha) \in \prod_{\alpha\in I} G_\alpha \mid \phi_{\beta\alpha}(g_\beta) = g_\alpha\}$$

Als endliche Gruppen sind die G_α kompakt. Dasselbe gilt dann aber auch für deren direktes Produkt und damit auch für die abgeschlossene Untergruppe G dieses direkten Produkt. Proendliche Gruppen sind kompakt.

(ii) Sei $C \subseteq G$ eine zusammenhängende Teilmenge der proendlichen Gruppe G. In den Bezeichnungen von (iii) sind dann die Bilder von C bei den natürlichen Homomorphismen

$$\phi_\alpha: G \longrightarrow G_\alpha\ ,\ (g_\alpha,)_{\alpha'\in I} \mapsto g_\alpha\ ,$$

ebenfalls zusammenhängend (da die Homomorphismen stetig sind). Weil die G_α diskrete Gruppen sind, ist $\phi_\alpha(C)$ für jedes α eine einpunktige Menge, d.h. für die α-te Koordinate gibt es nur eine Möglichkeit. Da dies für alle α gilt, muß C selbst eine einpunktige Menge sein. Topologische Räume, in welchen jede Zusammenhangskomponente aus nur einem Punkt besteht, heißen total unzusammenhängend. Wir haben gezeigt: Proendliche Gruppen sind total unzusammenhängend. [66]

(iii) Eine topologische Gruppe G ist genau dann proendlich, wenn sie kompakt und total unzusammenhängend ist[67].

Zum Beweis verwendet man die folgende Aussagen.[68]

---

[66] Die Topologie der proendlichen Gruppen ist im allgemeinen von der diskreten Topologie verschieden. Wäre die Topologie von G diskret, so wäre die Menge {e} welche nur aus den neutralen Element besteht offen in G. Da die Kerne der Homomorphismen $\phi_\alpha: G \longrightarrow G_\alpha$ eine Umgebungsbassi von e bilden, würde es also ein α geben mit

$$\operatorname{Ker} \phi_\alpha = \{e\},$$

d.h. G wäre eine Untergruppe der endlichen Gruppe G_α, also selbst schon endlich. Wir haben gezeigt:

für proendliche Gruppen sind die folgenden Aussagen äquivalent:

(i) G ist endlich.

(ii) Die Topologie von G ist diskret.

[67] vgl. Grünberg [1] oder Cassels & Fröhlich [1] oder 5.1.4.7 der Notizen zur Vorlesung "Algebraische Zahlentheorie" nach Cassels & Fröhling.

[68] Sei G eine kompakte und total unzusammenhängende topologische Gruppe. Wir haben zu zeigen, G ist proendlich. Bezeichne

$$\{U_i\}_{i\in I}$$

die Familie der offenen Normalteiler von G. Dann sind die Faktorgruppen G/U_i diskret und kompakt, also endlich. Außerdem bilden die Faktoren G/U_i ein filtrierendes projektives System (weil der Durchschnitt zweier U_i wieder ein U_i ist). Es reicht zu zeigen, G ist isomorph zu

$$L := \varprojlim_{i\in I} G/U_i$$

1. Eine kompakte Gruppe ist genau dann total unzusammenhängend, wenn der Durchschnitt aller kompakten offenen Umgebungen des neutralen Elements $e \in G$ gleich $\{e\}$ ist.[69]

2. In einer kompakten total unzusammenhängenden topologischen Gruppe enthält jede Umgebung des neutralen Elements einen offenen Normalteiler (d.h. die offenen Normalteiler bilden eine Umgebungsbasis des neutralen Elements).[70]

(iv) Aus Bemerkung 1.4.9 (v)[71] und der Beschreibung der Topologie in Bemerkung 1.4.9 (viii)[72] ergibt sich für jede proendliche Gruppe G,

---

Betrachten wir den Gruppen-Homomorphismus

$$h: G \longrightarrow L,\ g \mapsto (gU_i)_{i \in I}\ .$$

Die Zusammensetzungen von h mit den natürlichen Projektionen $L \longrightarrow G/U_i$ sind gerade die natürlichen Homomophismen $G \longrightarrow G/U_i$, also stetig. Auf Grund der Definition der Topologie von L ist dann aber auch h stetig. Es reicht zu zeigen, G ist bijektiv (denn jede stetige Bijektion eines kompakten Raums in einen Hausdorff-Raum ist ein Homöomorphismus).
Injektivität von h. Der Kern von h ist gerade der Durchschnitt aller U_i. Nach der obigen ersten Aussage ist dieser Durchschnitt aber gleich $\{e\}$.
Surjektivität von h. Sei $(\overline{g}_N)_N$ ein Element des Limes auf der rechten Seite. Bezeichne $g_N \in G$ einen Repräsentanten von $\overline{g}_N \in G/N$. Zeigen wir zunächst, der Durchschnitt

$$\bigcap g_N N \qquad (1)$$

ist nicht leer. Andernfalls wäre schon der Durchschnitt von endlich vielen der $g_N N$ leer (weil G kompakt und N abgeschlossen ist), sagen wir

$$g_1 N_1 \bigcap ... \bigcap g_n N_n = \varnothing.$$

Nun ist aber $D := N_1 \bigcap ... \bigcap N_n$ ein offener Normalteiler. Weil die Familie der $g_N N = \overline{g}_N$ im inversen Limes liegt, gilt $g_N N_i = g_i N_i$ für jedes $N \subseteq D$, d.h. $g_N \in g_i N_i$ für jedes i, d.h. der Durchschnitt der $g_i N_i$ kann nicht leer sein. Wir haben gezeigt, der Durchschnitt (1) ist nicht leer. Sei

$$g \in \bigcap g_N N$$

ein Elemen dieses Durchschnitts. Dann gilt

$$gN = g_N N = \overline{g}_N \text{ für jedes N,}$$

d.h. das Bild von $g \in G$ bei der Abbildung h ist die vorgegebene Familie der $\overline{g}_N$.

[69] Siehe 5.1.4.4 der Notizen zur Vorlesung "Algebraische Zahlentheorie" nach Cassels & Fröhlich.
[70] Siehe 5.1.4.6 der Notizen zur Vorlesung "Algebraische Zahlentheorie" nach Cassels & Fröhlich.
[71] Man kann sich auf projektive Systeme $\{G_\alpha\}$ beschränken, deren Morphismen surjektiv sind.

$$G \cong \varprojlim_{N} G/N,$$

wobei N die offenen Normalteiler von G durchlaufe (d.h. die abgeschlossenen Normalteiler mit endlichem Index).[73]

(v) Für jede abgeschlossene Untergruppe $H \subseteq G$ einer proendlichen Gruppe gilt

$$H \cong \varprojlim_{N} H/H\bigcap N$$

mit N wie in (vii).[74]

(vi) Für jeden abgeschlossenen Normalteiler $H \subseteq G$ einer proendlichen Gruppe gilt

$$G/H \cong \varprojlim_{N} G/NH$$

mit N wie in (vii).[75]

---

[72] Die Kerne der natürlichen Morphismen $G \longrightarrow G_\alpha$ definieren die Topologie von G.

[73] Weil G kompakt und N offen ist, ist G/N ist kompakt und diskret, also endlich. Also ist G endliche und disjunkte Vereinigumg der offenen Nebenklassen modulo N. Also sind alle diese Nebenklassen abgeschlossen. Eine analoge Argumentation zeigt, daß abgeschlossene Normalteiler mit endlichem Index offen sind.

Die behauptete Isomorphie ergibt sich aus dem Beweis der vorangehenden Bemerkung (iv).

[74] Die Untergruppe H ist mit G ebenfalls kompakt und total unzusammenhängend, also proendlich. Nach Bemerkung (iv) gilt

$$G \cong \varprojlim_{N'} G/N'$$

wobei N' alle offenen Normalteiler von H durchläuft. Jeder solche Normalteiler hat die Gestalt

$$N' = H\cap U$$

mit einer offenen Menge $U\subseteq G$. Da G proendlich ist, enthält U einen offenen Normalteiler N von G (nach Bemerkung (iii)). Insbesondere gilt $H\cap N\subseteq N'$, d.h. jeder offene Normalteiler von H enthält einen offenen Normalteiler der Gestalt $H\cap N$. Die Gruppen der Gestalt $H/H\cap N$ bilden ein kofinales Teilsystem des Systems aller G/N'. Ein solches Teilsystem hat denselben projektiven Limes.

[75] Schreibt man

$$G/NH = (G/H)/(NH/H)$$

so sieht man, daß in der zu beweisenden Isomorphie rechts der Limes über alle offenen Normalteiler von G/H steht. Nach Bemerkung (vi) genügt es deshalb zu zeigen, daß G/H proendlich ist. Dazu benutzen wir die topologische Charakterisierung der proendlichen Gruppen von Bemerkung (iii). Mit G ist natürlich auch G/N kompakt. Es reicht also zu zeigen, G/N ist total unzusammenhängend.

Sei $x\notin N$ ein beliebiger Punkt. Da G ein Hausdorff-Raum ist, gibt es zu jedem $y\in N$ disjunkte offene Umgebungen $U_y(x)$ von x und V_y von y. Da G total unzusammenhängend ist, können wir nach Bemerkung (iii) sogar annehmen, $U_y(x)$ hat die Gestalt

$$U_y(x) = N'(y)x$$

mit einem offenen kompakten Normalteiler N'(y) (mit endlichem Index). Nun ist N als abgeschlossene Untergruppe von G kompakt, wird also von endlich vielen der Mengen V_y überdeckt. Der Durchschnitt von endlich vielen der Mengen $U_y(x)$ ist deshalb disjunkt zum Normalteiler N. Mit anderen Worten, es gibt einen offenen kompakten Normalteiler N' von G mit

$$N'x\cap N = \varnothing.$$

Dann gilt aber $x\notin N'N$, also $xN\cap N'N = \varnothing$. Das bedeutet, es gibt eine kompakte offene Umgebung N'N/N des neutralen Elements von G/N, welche ein vorgegebenes Element xN nicht enthält. Die

(vii) Beispiel. Sei K die algebraische Abschließung des endlichen Körpers

$$k = \mathbb{F}_p.$$

Dann ist die Galois-Gruppe

$$G(K/\mathbb{F}_p) \cong \hat{\mathbb{Z}} \; (= \prod_{p \text{ Primzahl}} \hat{\mathbb{Z}}_p)$$

isomorph zur proendlichen Vervollständingung der additiven Gruppe $\mathbb{Z}$ der ganzen Zahlen.[76]

(viii) Bei der nachfolgenden Einführung der Kohomologie für proendliche Gruppen, werden die Koeffizienten sogenannte diskrete G-Moduln sein. Wir führen deshalb an diesen Begriff an diese Stelle ein. Sei G eine proendliche Gruppe,

$$G = \varprojlim_N G/N,$$

wobei G wie bisher die offenen Normalteiler durchlaufe. Für jeden G-Modul A bezeichne A^N wie bisher die Menge der Elemente von A, die bei der Operation von N fest bleiben:

$$A^N := \{a \in A \mid ua = a \text{ für } u \in N\}.$$

Ein G-Modul heißt diskrete, wenn gilt

$$A = \bigcup \{ A^N \mid N \subseteq G \text{ offener Normalteiler } \}.$$

Folgende Aussage sind äquivalent:

1. A ist ein diskreter G-Modul.
2. Der Stabilisator

$$G_a := \{g \in G \mid ga = a \}$$

jedes Elements $a \in A$ ist eine offene Untergruppe von G.

3. Die Abbildung

$$G \times A \longrightarrow A, (g, a) \longrightarrow ga,$$

ist stetig, wenn man A mit der diskreten Topologie und G mit der proendlichen Topologie versieht.[77]

Zusammenhangskomponente des neutralen Elements von G/N besteht nur aus einem Element, d.h. G/N ist total unzusammenhängend.

[76] Sei K'/k endlich vom Grad n. Dann ist

$$K' = \mathbb{F}_{p^n}$$

und

$$G(K'/k) \cong \mathbb{Z}/n\mathbb{Z}$$

ist zyklisch von der Ordnung n (und wird von der Frobenius-Abbildung erzeugt). Es folgt

$$G(K/k) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Man beachte jede Untergruppe von $\mathbb{Z}$ ist von der Gestalt $n\mathbb{Z}$.

[77] 1. $\Rightarrow$ 2. Nach Voraussetzung gibt es für jedes $a \in A$ einen offenen Normalteiler $U \subseteq G$ mit $a \in A^U$, d.h. mit $Ua = \{a\}$. Mit anderen Worten, es gilt $U \subseteq G_a$. Dann ist aber G_a Vereinigung von Nebenklassen modulo U und als solche offen.

2 $\Rightarrow$ 3. Da die Topologie von A diskret sein soll, genügt es zu zeigen, für jedes $a \in A$ ist die Faser $\mu^{-1}(a)$ der Multiplikationsabbildung

$$\mu: G \times A \to A, (g,a) \mapsto ga,$$

eine offene Teilmenge von $G \times A$. Der Stabilisator G_a von a operiert auf der Faser

$$\mu^{-1}(a) = \{(g,b) \in G \times A \mid gb = a\}$$

1.4.11 Die Kohomologie der proendlichen Gruppen

Seien G eine proendliche Gruppe, A ein diskreter G-Modul und

$$\{U_\alpha\}_{\alpha\in I}$$

die Familie der offenen Normalteiler[78] von G. Dann gilt

$$G \cong \varprojlim_{\alpha\in I} G/U_\alpha$$

und

$$A \cong \varinjlim_{\alpha\in I} A^{U_\alpha}$$

Für je zwei Indizes $\alpha, \beta \in I$ mit $\alpha \le \beta$ bezeichne[79]

$$\lambda_\alpha^\beta : H^i(G/U_\alpha, A^{U_\alpha}) \longrightarrow H^i(G/U_\beta, A^{U_\beta})$$

die Inflation. Die Inflationsabbildungen bilden ein projektives System, Dessen induktiver Limes wird mit

$$H^i(G, A) := \varinjlim_{\alpha\in I} H^i(G/U_\alpha, A^{U_\alpha})$$

bezeichnet und heißt i-te Kohomologie der proendlichen Gruppe G mit Koeffizienten in A.

Bemerkung

Die Kohomologie der proendlichen Gruppen besitzt eine Beschreibung, die analog ist zur Beschreibung der Gruppen-Kohomologie mit Hilfe von Kozyklen und Koränder. Bezeichne

$$C^i = C^i(G, A)$$

---

vermittels der Vorschrift

$$G_a \times \mu^{-1}(a) \to \mu^{-1}(a), (h, (g,b)) \mapsto (hg,b),$$

d.h. die Menge $\mu^{-1}(a)$ zerfällt in die Vereinigung von G_a-Orbits. Diese sind Mengen der Gestalt G_a g×{b}, also nach Voraussetzung 2 offene Teilmengen von G×A. Dann ist aber auch die Menge $\mu^{-1}(a)$ offen in G×A.

3 ⇒ 1. Da die Mulitiplikation $\mu: G\times A \to A$, $(g,a) \mapsto ga$, stetig ist, ist

$$\mu^{-1}(a)$$

für jedes $a\in A$ eine offene Menge. Nach Bemerkung (iii) gibt es deshalb einen offenen Normalteiler $U \subseteq \mu^{-1}(a)$, d.h. es ist $a\in A^U$. Da a beliebig war, sehen wir A ist ein diskreter G-Modul.

[78] Die Index-Mange sei halbgeordnet mit

$$\alpha \le \beta \Leftrightarrow U_\beta \subseteq U_\alpha$$

[79] Zur Erinnerung, G" := G/U_α ist eine Faktorgruppe von G' := G/U_β und der G"-Modul A" := A^{U_α} ist gleichzeitig ein G'-Modul. Der natürliche Homomorphismus G' ⟶ G" induziert also einen Gruppen-Homomorphismus

$$H^i(G", A") \longrightarrow H^i(G', A") \qquad (1)$$

(weil die Gruppen-Kohomologie ein kontravarianter Funktor bzgl. des ersten Arguments ist). Weiter induziert die Einbettung A" ↪ A' := A^{U_β} einen Gruppen-Homomorphismus

$$H^i(G', A") \longrightarrow H^i(G', A'). \qquad (2)$$

Die Zusammensetzung von (1) und (2) ist gerade die Inflation.

die additive Gruppe der stetigen Abbildungen $G^i \longrightarrow A$. Wir definieren einen Korand-Operator

$$d: C^i \longrightarrow C^{i+1}$$

durch die Formel

$$(df)(g_1, \dots, g_{i+1}) = g_1 \bullet f(g_2, \dots, g_{i+1}) + \sum_{\alpha=1}^{i} (-1)^\alpha f(g_1, \dots, g_\alpha g_{\alpha+1}, \dots, g_{i+1}) + (-1)^{i+1} f(g_1, \dots, g_i).$$

Auf diese Weise ist ein Komplex C*(G, A) definiert. Dessen Kohomologie-Gruppen sind isomorph zu den oben definierten,

$$H^i(G, A) \cong H^i(C^*(G, A)).$$

Der Beweis dieser Aussage ist nicht sehr schwierig, aber vergleichsweise lang und etwas langweilig. Die Grundidee für die Konstruktion des Isomorphismus besteht in folgenden. Eine Abbildung

$$\phi: H \longrightarrow B$$

einer proendlichen Gruppe H mit Werten in einem diskreten H-Modul ist genau dann stetig, wenn es einen offenen Normalteiler $K \subseteq H$ derart gibt, daß sich ϕ über die endliche Gruppe H/K faktorisiert,

$$\phi: H \longrightarrow H/K \longrightarrow B.$$[80]

Speziell für $\phi \in C^i(G, A)$ bedeutet dies, es gibt einen offenen Normalteiler $U' \subseteq G$ derart, daß sich ϕ über $(G/U')^i$ faktorisiert,

$$\phi: G^i \longrightarrow (G/U')^i \longrightarrow A.$$

Da die Funktion ϕ nur endlich viele Wert annimmt, gibt es einen offenen Normalteiler U" derart, daß das Bild von ϕ in $A^{U"}$ liegt. Mit $U = U' \bigcap U"$ erhalten wir eine Faktorisierung

$$\phi: G^i \longrightarrow (G/U)^i \longrightarrow A^U.$$

Die Abbildung rechts ist dabei ein Element von $C^i(G/U; A^U)$. Wir erhalten auf diese Weise, daß

$$C^i(G, A) = \varinjlim_{i \in I} C^i(G/U_i, A^{U_i})$$

gilt.

Beispiel

Seien G eine Pro-p-Gruppe und $\mathbb{F}_p$ der Körper mit p Elementen. Wir betrachten die additive Gruppe von $\mathbb{F}_p$ als G-Modul bezüglich der trivialen Operation von G. Aus der obigen Beschreibung der proendlichen Kohomologie mit Hilfe von Kozyklen und Korändern erhalten wir[81]

---

[80] H wird von Nebenklassen offener Normalteiler überdeckt, auf denen ϕ konstant ist. Da H kompakt ist, ist diese Überdeckung endlich. Man kann für K den Durchschnitt der beteiligten Normalteiler nehman.

[81] Für einen 1-Kozyklus $f: G \longrightarrow A$ gilt

$$0 = (df)(g,h) = g \bullet f(h) - f(gh) + f(g),$$

d.h.

$$f(gh) = f(g) + f(h).$$

$$H^1(G, \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{Groups}}(G, \mathbb{F}_p).$$

Weil die additive Gruppe von $\mathbb{F}_p$ kommutativ ist, faktorisiert sich jeder Homomorphismus $G \longrightarrow \mathbb{F}_p$ über G/[G, G]. Weil die Mutiplikation mit p auf $\mathbb{F}_p$ identisch Null ist, faktorisiert sich jeder Homomorphismus $G/[G, G] \longrightarrow \mathbb{F}_p$ über[82]

$$G/G^* \text{ mit } G^* = G^p[G, G].$$

Wir erhalten somit

$$H^1(G, \mathbb{F}_p) = \mathrm{Hom}_{\mathrm{Ab}}(G/G^*, \mathbb{F}_p) =^{83} \mathrm{Hom}_{\mathbb{F}_p}(G/G^*, \mathbb{F}_p).$$

Nehmen wir jetzt an, G ist als topologische Gruppe endlich erzeugt[84]. Dann ist die Gruppe G/G* endlich[85] ,[86] also auch endlich erzeugt.

Die 1-Kozyklen sind also gerade die Gruppen-Homomorphismen. Wir haben noch nach den 1-Korändern zu faktorisieren, d.h. nach den Abbildungen der Gestalt df mit einem 0-Kozyklus f,

$$df(g) = g \bullet f - f, f \in \mathbb{F}_p.$$

Da G auf $\mathbb{F}_p$ trivial operiert, sind die 0-Kozyklen aber alle identisch Null.

[82] Das natürliche Bild U von G^p in G/[G, G] ist ein Normalteiler, weil G/[G, G] kommutativ ist. Die Menge G* ist gerade der Kern der natürlichen Surjektion $G \longrightarrow G/[G, G] \longrightarrow (G/[G, G])/U$, also ebenfalls ein Normalteiler.

[83] G/G* ist eine abelsche Gruppe, also ein $\mathbb{Z}$-Modul. Da die Multiplikation mit p jedes Element von G/G* annulliert, ist G/G* sogar ein $\mathbb{Z}/p\mathbb{Z}$-Modul, d.h. ein $\mathbb{F}_p$-Vektorraum.

[84] d.h. es gebe endlich viele Elemente in G mit der Eigenschaft, daß jede abgeschlossene Untergruppe, die diese Elemente enthält, gleich G ist.

[8585] Nach Voraussetzung gibt es einen surjektiven stetigen Homomorphismus

$$F(I) \longrightarrow G$$

mit einer endlichen Menge I, sagen wir

$$\# I = n.$$

Dieser induziert eine Surjektion

$$F(I)/F(I)^* \longrightarrow G/G^*.$$

Es reicht deshalb zu zeigen, daß F(I)/F(I)* endlich ist. Nach Definition von F(I) ist

$$F(I)/[F(I), F(I)]$$

isomorph zum inversen Limes der Faktoren von $L(I)/[L(I), L(I)] \cong \mathbb{Z}^n$ von p-Potenz-Ordnung, d.h.

$$F(I)/[F(I), F(I)] \cong \hat{\mathbb{Z}}_p^n$$

(siehe nachfolgende Fußnote).Damit gilt aber

$$F(I)/F(I)^* \cong \hat{\mathbb{Z}}_p^n/p\hat{\mathbb{Z}}_p^n \cong (\hat{\mathbb{Z}}_p/p\hat{\mathbb{Z}}_p)^n \cong (\mathbb{Z}/p\mathbb{Z})^n.$$

Die Ordnung von F(I)/F(I)* ist somit endlich. Man beachte, die Isomorphie rechts ergibt sich aus

$$\hat{\mathbb{Z}}_p/p\hat{\mathbb{Z}}_p \cong \mathbb{Z}/p\mathbb{Z}.$$

Letzteres gilt weil der Homomorphismus

$$\hat{\mathbb{Z}}_p \longrightarrow \mathbb{Z}/p\mathbb{Z}, \sum_{n=0}^{\infty} a_n p^n \mapsto a_0 \bmod p\mathbb{Z},$$

Seien $x_1, \dots, x_d \in G$ Elemente, die eine Basis des Vektorraums G/G* bilden. Nach dem Satz von Bernside[87] bilden dann die $x_1, \dots, x_d$ ein System von topologischen Erzeugern von G. Damit ist

$$\begin{aligned}\dim_{\mathbb{F}_p} H^1(G, \mathbb{F}_p) &= \dim_{\mathbb{F}_p} \mathrm{Hom}_{\mathbb{F}_p}(G/G^*, \mathbb{F}_p) \\ &= \dim_{\mathbb{F}_p} G/G^*\end{aligned}$$

gerade die minimale Anzahl von Elementen aus G, welche G topologisch erzeugen können.

1.4.12 Verschwindungssätze für die Kohomologie der proendlichen Gruppen

(i) Für jede Galois-Erweiterung K/k und jedes $i > 0$ gilt[88]

$$H^i(G(K/k), E) = 0.$$

(ii) Satz 90 von Hilbert. Für jede Galois-Erweiterung gilt[89]

---

der jede Potenzreihe in p auf ihr Absolutglied modulo p abbildet, surjektiv ist und den Kern $p\hat{\mathbb{Z}}_p$ besitzt.

[86] Die Isomorphie $F(I)/[F(I), F(I)] \cong \hat{\mathbb{Z}}_p^n$ der vorangehenden Fußnote ergibt sich wie folgt. Für jede Gruppe G bezeichnen wir mit

$$G' := G/[G,G]$$

deren Faktorkommutatorgruppe. Weiter bezeichne $\underline{M} = \{M\}$ die Familie der Normalteiler von L(I), deren Index eine p-Potenz ist, d.h.

$$F(I) = \varprojlim_{M \in \underline{M}} L(I)/M.$$

Dann hat man ein kommutatives Diagramm

$$\begin{array}{ccc} F(I) & = & \varprojlim_{M} L(I)/M \\ \downarrow & & \downarrow \\ F(I)' & \longrightarrow & \varprojlim_{M} (L(I)/M)' \end{array}$$

wobei der rechte untere Limes als Limes in der Kategorie der abelschen Gruppen angesehen werden kann und der untere Morphismus von der Tatsache kommt, daß letzterer Limes eine abelsche Gruppe ist. Wir haben zu zeigen, der untere Pfeil bezeichnet einen Isomorphismus. Wir zeigen dies, indem wir beweisen, daß F(I)' die Universalitätseigenschaft des Limes rechts unten besitzt (in der Kategorie der abelschen Gruppen): Jede Abbildung $I \longrightarrow A$ der endlichen Menge I mit Werten in einer abelschen Pro-p-Gruppe läßt sich eindeutig zu einen stetigen Homomorphismue $F(I)' \longrightarrow A$ fortsetzen. Zumintest hat man eine eindeutige Fortsetzung zu einem stetigen Homomorphismus $F(I) \longrightarrow A$. Weil A abelsch ist, faktorisiert sich dieser über F(I)'. Die Eindeutigkeitsaussage ergibt sich aus der Surjektivität des natürlichen Homomorphismus $F(I) \longrightarrow F(I)'$.

[87] Ein stetiger Homomorphismus $f: G' \longrightarrow G$ von Pro-p-Gruppen ist genau dann surjektiv, wenn er eine Surjektion $G'/G'^* \longrightarrow G/G^*$ induziert, vgl. 5.2.5.2 der Notizen zur Vorlesung "Algebraische Zahlentheorie" nach Cassels & Fröhling.

[88] Die additive Gruppe von K mit der natürlichen Operation von G = G(K/k) auf K ist ein diskreter G-Modul (nach dem Hauptsatz der Galois-Theorie).

$$H^1(G(K/k), K^*) = 0.$$

Beweis. Zu(i). Bezeichne $\{K_i\}_{i\in I}$ die Familie der endlichen Galoisschen Teilerweiterungen von K/k und sei

$$U_i := G(K/K_i) \ (= \mathrm{Ker}(G(K/k) \longrightarrow G(K_i/k))$$

die zugehörige Falmilie der offenen Normalteiler von G(K/k). Dann gilt

$$G = \varprojlim_{i\in I} G/U_i$$

und

$$H^n(G, K) = \varinjlim_{i\in I} H^n\,(G/U_i\,, K^{U_i}).$$

Wegen $G/U_i = G(K_i/k)$ und $K^{U_i} = K_i$ reicht es zu zeigen, die Behauptung gilt für endliche Galois-Erweiterungen,

$$H^i(G(K/k), K) = 0 \text{ für } i > 0 \text{ und } K/k \text{ endlich.}$$

Im endlichen Fall folgt die Behauptung aus dem Satz über die Normalbasis: es gibt eine Vektorraumbasis von K/k, die bei der Operation der Galois-Gruppe G = G(K/k) permutiert wird, d.h.

$$k[G] \longrightarrow K,\ g \mapsto g(\eta),$$

ist ein Isomorphismus von G-Moduln, wenn η ein Element der Normalbasis bezeichnet. Das bedeutet nämlich

$$K \cong k[G] = k\otimes_{\mathbb{Z}}\mathbb{Z}[G]$$

ist ein induzierter G-Modul.

Zu (ii). Es gilt

$$H^1(G, K^*) = \varinjlim_{i\in I} H^1\,(G/U_i\,, K^{*\,U_i}) = \varinjlim_{i\in I} H^1\,(G/U_i\,, K_i^*)$$

Es reicht deshalb, zu zeigen, die Behauptung ist richtig für endliche Galois-Erweiterungen. Nehmen wir also an,

$$K/k \text{ endlich.}$$

Sei

$$f: G \longrightarrow K^*$$

ein 1-Kozyklus, d.h.

$$f(g'g'') = f(g')\bullet g'f(g'') \text{ für } g', g'' \in G. \qquad (1)$$

Es reicht zu zeigen, f is ein 1-Korand, d.h. von der Gestalt

$$f(g) = x(gx)^{-1} \text{ für ein } x \in K^*.$$

Nach dem Satz von Artin über die K-lineare Unabhängigkeit der Elemente von G = G(K/k) ist die Abbildung

---

[89] Die multiplikative Gruppe von K mit der natürlichen Operatione von G = G(K/k) auf K* ist ein

$$\sum_{g\in G} f(g)\bullet g : K \longrightarrow K$$

nicht identisch Null, d.h. es gibt ein $c \in K$ mit

$$x := \sum_{g\in G} f(g)\bullet g(c) \neq 0.$$

Für $g' \in G$ gilt

$$g'(x) = \sum_{g\in G} g'(f(g))\bullet g'(g(c))$$

$$= \sum_{g\in G} f(g')^{-1} f(g'g)\bullet(g'g)(c) \qquad \text{(vgl (1))}$$

$$= f(g')^{-1} \sum_{g\in G} f(g'g)\bullet(g'g)(c)$$

$$= f(g')^{-1} x$$

also

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

Also ist f tatsächlich ein Kozyklus.
QED.
Bemerkung
Der Satz 90 von Hilbert der Grundvorlesung Algebra ist ein Spezialfall des hier bewiesenen Satzes:

Seien K/k eine endliche Galois-Erweiterung mit G(K/k) zyklisch,

$$G(K/k) = <\sigma>$$

und $a \in K^*$ ein Element der Norm 1,

$$N_{K/k}(a) = 1.$$

Dann gibt es ein Element $b \in K'$ mit

$$a = \frac{b}{\sigma(b)}.$$

Beweis. Weil G eine zyklische Gruppe ist, gilt für jeden G-Modul A:

$$H^1(G, A) = \hat{H}^1(G, A) = {}_N A /(1-\sigma)A$$

(vgl. Bemerkung 1.4.6 (iv)). Im Fall

$$A = K^*$$

ist

---

diskreter G-Modul.

$$ {}_{N}A = \mathrm{Ker}\,(N\colon A \longrightarrow A) = \{x \in K^* \mid N_{K/k}(x) = 1\} $$

Insbesondere gilt

$$ a \in {}_{N}A. $$

Auf Grund des Satzes 90 von Hilbert gilt $H^1(G, A) = 0$, d.h.

$$ a \in {}_{N}A = (1-\sigma)A = \{ (1-\sigma)x \mid x \in K^*\} = \{\frac{x}{\sigma(x)} \mid x \in K^*\} $$

QED.

1.4.13 Galois-Kohomologie

Seien k ein Körper und k^s/k eine separable Abschließung von k. Dann heißt

$$ H^i(k) := H^i(G(k^s/k), (k^s)^*) $$

i-te Galois-Kohomolgie des Körpers k. Die Gruppe

$$ H^2(k) $$

heißt auch kohomologische Brauer-Gruppe von k.

Beispiel

$$ H^2(\mathbb{R}) = H^2(G(\mathbb{C}/\mathbb{R}), \mathbb{C}^*) $$

Weil $G = G(\mathbb{C}/\mathbb{Z})$ zyklisch von der Ordnung 2 ist, folgt

$$ \begin{aligned} H^2(\mathbb{R}) &= \hat{H}^{2i}(G, \mathbb{C}^*) \\ &= (\mathbb{C}^*)^G/N\bullet\mathbb{C}^* \qquad \text{(Bemerkung 1.4.6 (iv))} \\ &= \mathbb{R}^*/\{ x^2+y^2 \mid x, y \in \mathbb{R}\} \\ &= \mathbb{Z}/2\mathbb{Z} \end{aligned} $$

Die kohomologische Brauer-Gruppe von $\mathbb{R}$ besteht also aus 2 Elementen.

Bemerkungen

(i) Je zwei separable Abschließungen von k sind isomorph. Die Galois-Kohomologie $H^i(k)$ ist somit bis auf Isomorphie eindeutig bestimmt. Genauer, sind k^s und $k^{s'}$ zwei separable Abschließungen von k, so gibt es einen k-Isomorphismus

$$ k^s \longrightarrow k^{s'}, \qquad (1) $$

welcher seinerseits einen Isomorphismus

$$ H^i(G(k^s/k), (k^s)^*) \longrightarrow H^i(G(k^{s'}/k), (k^{s's})^*). $$

induziert. Wie sich herausstellt, hängt dieser nicht von der speziellen Wahl des k-Isomorphismus (1) ab, sodaß die Galois-Kohomologie sogar bis auf natürliche Isomorphie eindeutig bestimmt ist. Um das einzusehen, betrachten wir eine etwas allgemeinere Situation.

(ii) Seien K'/k und K"/k zwei Galois-Erweiterungen mit den Galois-Gruppen

$$ G' := G(K'/k) \text{ und } G'' := G(K''/k) $$

und

$$ j\colon K' \longrightarrow K'' $$

ein k-Homomorphismus. Dann ist j(K') eine Galoissche Teilerweiterung von K " und die Einschränkungsabbildung

$$ \Phi_{K''j(K')}\colon G'' = G(K''/k) \longrightarrow G(j(K')/k) \cong G' $$

definiert einen (surjektiven) Gruppen-Homomorphismus[90]

---

[90] Weil j(K') eine normale Erweiterung von k ist, bildet g diese Teilerweiterung in sich ab, d.h. es gilt

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

$$\overline{j}: G'' \longrightarrow G',\ g \mapsto j^{-1} \circ g \circ j.$$

mit dem Kern U" := G(K"/j(K')). Die Inflationsabbildung

$$\text{Inf: } H^i(G''/U'', (K''^*)^{U''}) \longrightarrow H^i(G'', K''^*)$$

setzt sich mit dem durch $\overline{j}$ induzierten Isomorphismus

$$H^i(G', K'^*) \xrightarrow{\cong} H^i(G''/U'', (K''^*)^{U''})$$

zusammen zu einem Gruppen-Homomorphismus

$$j^*: H^i(G', K'^*) \longrightarrow H^i(G'', K''^*).$$

Dieser hängt nicht von der speziellen Wahl von j ab.

Sei

$$j': K' \longrightarrow K''$$

ein weiterer k-Homomorphismus. Dann sind j(K') und j'(K') zwei k-isomorphe Teilerweiterungen von K". Der k-Isomorphismus $j' \circ j^{-1}: j(K') \longrightarrow j'(K')$ läßt sich zu einem k-Automorphismus g: K" $\longrightarrow$ K" fortsetzen.[91] Insbesondere gilt

$$g \circ j = j'$$

also ist

$$\overline{j}'(x) = j'^{-1} \circ x \circ j' = j^{-1} g^{-1} x g j = \overline{j}(\overline{g}(x)),$$

d.h.

$$\overline{j}' = \overline{j} \circ \overline{g}$$

wenn $\overline{g}$ den inneren Automorphismus

$$\overline{g}: G'' \longrightarrow G'',\ x \longrightarrow g^{-1} x g\ ,$$

bezeichnet. Es reicht also zu zeigen, dieser innere Automorphismus induziert auf der Kohomologie die identische Abbildung. Wir zeigen dies in einer allgemeineren Situation.

(iii) Seien G eine Gruppe, A ein G-Modul, $g \in G$ ein Element,

$$\sigma: G \longrightarrow G,\ x \mapsto g^{-1} x g\ ,$$

der durch g definierte innere Automorphismus von G. Der Automorphismus σ definiert auf A eine zweite G-Modul-Struktur,

$$G \times A \longrightarrow A,\ (x, a) \mapsto \sigma(x) \bullet a = g^{-1} x g a.$$

Wir bezeichnen mit A^σ den Modul A, der mit dieser neuen G-Modul-Struktur versehen ist.

Weil die Gruppen-Kohomologie kontravariant von der Gruppe abhängt induziert σ einen Gruppen-Isomorphismus

$$\sigma^*: H^i(G, A) \longrightarrow H^i(G, A^\sigma) \qquad (2)$$

Die Abbildung

$$A^\sigma \longrightarrow A,\ a \mapsto g a\ ,$$

ist ein Isomorphismus von G-Moduln und induziert damit einen Gruppen-Isomorphismus

$$g_*: H^i(G, A^\sigma) \longrightarrow H^i(G, A) \qquad (3).$$

Insbesondere ist $j^{-1} \circ g \circ j$ wohldefiniert.

[91] Weil K" normal über k ist.

Wir haben zu zeigen, die Zusammensetzung von (1) und (2) ist die identische Abbildung. Das ergibt sich aber durch Induktion nach i.[92]

(iv) Seien K/k und L/k Galois-Erweiterungen mit $K \subseteq L$. Dann besteht eine exakte Sequenz der Gestalt

$$0 \longrightarrow H^2(G(K/k), K^*) \longrightarrow H^2(G(L/k), L^*) \longrightarrow H^2(G(L/K), L^*).$$

(v) Für jede Galois-Erweiterung K/k besteht eine exakte Sequenz[93]

$$0 \longrightarrow H^2(G(K/k), K^*) \longrightarrow H^2(k) \longrightarrow H^2(K).$$

(vi) Seien K/k eine Galois-Erweiterung und $(K_i)_{i\in I}$ die Familie der endlichen Galoisschen Teilerweiterungen von K. Dann gilt[94]

---

[92] Für i = 0 identifizieren wir $H^0(G, A)$ mit der Menge der 0-Kozyklen f: $G \longrightarrow A$ d.h. der G-linearen Abbildungen f mit $(df)(g', g'') = f(g')-f(g'') = 0$, d.h. der Menge der konstanten Abbildungen $G \longrightarrow A^G$. Wir haben dann die Bijektion

$$H^0(G, A) \longrightarrow A^G\ ,\ G \xrightarrow{f} A \mapsto f(e).$$

Wir erhalten ein kommutatives Diagramm

$$\begin{array}{ccccc} H^0(G,A) & \xrightarrow{\sigma^*} & H^0(G,A^\sigma) & f & \mapsto & f\circ\sigma \\ \downarrow\cong & & \cong\downarrow & \downarrow & & \downarrow \\ A^G & & (A^\sigma)^G & f(e) & & f(\sigma(e)) \end{array}$$

welches zeigt, daß die Abbildung (2) für i = 0 gerade die identische Abbildung

$$\sigma^* = \mathrm{id}: A^G \longrightarrow A^G$$

ist. Abbildung (3) ist durch die Multiplikation mit g induziert, also gerade die Abbildung

$$g_*: A^G \longrightarrow A^G,\ a \mapsto ga,$$

welche ebenfalls die identische Abbildung ist. Im Fall i = 0 ist also die Zusammensetzung von (2) und (3) tatsächlich die Identität.

Im Fall i > 1 betrachten wir eine kurze exakte Sequenz von G-Moduln

$$0 \longrightarrow A \longrightarrow I \longrightarrow A' \longrightarrow 0$$

mit I induziert. Dies läßt sich auch als kurze exakte Sequenz

$$0 \longrightarrow A^\sigma \longrightarrow I^\sigma \longrightarrow A'^\sigma \longrightarrow 0$$

auffassen, wobei I^σ ebenfalls induziert ist. Wegen der Funktorialität der Gruppen-Kohomologie in beiden Argumenten erhalten wir ein kommutatives Diagramm mit exakten Zeilen

$$\begin{array}{ccccc} H^{i-1}(G,A') & \xrightarrow{\delta} & H^i(G,A) & \longrightarrow & 0 \\ \downarrow\sigma^* & & \downarrow\sigma^* & & \\ H^{i-1}(G,A'^\sigma) & \xrightarrow{\delta^\sigma} & H^i(G,A^\sigma) & \longrightarrow & 0 \\ \downarrow g_* & & \downarrow g_* & & \\ H^{i-1}(G,A') & \xrightarrow{\delta} & H^i(G,A) & \longrightarrow & 0 \end{array}$$

Nach Induktionsvoraussetzung können wir annehmen, die Zusammensetzung der linken vertikalen Abbildungen ist gleich der Identität. Auf Grund der Surjektivität der horizontalen Abbildungen gilt dann aber dasselbe auch für die Zusammensetzung der rechten vertikalen Abbildungen.

[93] Man wähle in (iv) für L eine separable Abschließung von K.

[94] Sei L eine separable Abschließung von K. Dann gilt mit G = G(L/k)

$$H^2(k) = H^2(G, L^*) = \varinjlim_{i\in I} H^2(G/U_i, (L^*)^{U_i}) = \varinjlim_{i\in I} H^2(G(K_i/k), K_i^*)$$

$$H^2(k) = \bigcup_{i\in I} H^2(G(K_i/k), K_i^*).$$

Beweisskitze für Aussage (iv). Zum Beweis formulieren wir die Aussage mit Hilfe abstrakter proendlicher Gruppen. Seien

$$G := G(L/k), H := G(L/K), A := L^*.$$

Dann ist H eine abgeschlossene Untergruppe und es gilt

$$G/H \cong G(K/k) \text{ und } A^H =^{95} K^*.$$

Es reicht zu zeigen, die Sequenz

$$0 \longrightarrow H^2(G/H, A^H) \xrightarrow{Inf} H^2(G, A) \xrightarrow{Res} H^2(H, A) \qquad (4)$$

ist exakt für jede proendliche Gruppe G, jede diskreten G-Modul A und jede abgeschlossene Untergruppe $H \subseteq G$ mit

$$H^1(H, A) = 0. \qquad (5)$$

(vgl. 1.4.4 (xii)).

Bedingung (5) ist äquivalent zu der Aussage, daß

$$H^1(HU_i/U_i, A^{U_i}) = 0$$

gilt für jeden offenen Normalteiler U_i von G. Nach 1.4.4 (xii) ist dann aber die folgende Sequenz exakt.

$$0 \longrightarrow H^2(G/HU_i, A^{HU_i}) \longrightarrow H^2(G/U_i, A^{U_i}) \longrightarrow H^2(HU_i/U_i, A^{U_i}).$$

Für $i \le j$ betrachten wir zusätzlich die exakte Sequenz mit j anstelle von i. Die beiden exakten Sequenzen sind durch Inflationsabbildungen verbunden, die zu einem kommutativen Diagramm führen. Die Behauptung erhält man jetzt durch Übergang zum induktiven Limes bei Beachtung der folgenden Fakten:

1. $\varinjlim_I$ ist ein exakter Funktor auf den induktiven Systemen über einer fest gewählten Index-Menge.
2. $\varprojlim_i H/H\bigcap U_i \cong H$ und $\varprojlim_i G/HU_i \cong G/N$.

Die Exaktheit von (4) im proendlichen Fall kann man auch direkt beweisen nach derselben Methode wie für den Fall abstrakter Gruppen.
QED.

1.4.14 Gruppen-Kohomologie mit nicht-notwendig abelschen Koeffizienten[96]

Seien G und A zwei Gruppen und

$$G \times A \longrightarrow A, (\sigma, a) \mapsto \sigma(a),$$

eine Operation von G auf A durch Gruppen-Automorphismen. Ein 1-Kozyklus von G mit Werten in A ist eine Abbildung

$$a: G \longrightarrow A, \sigma \mapsto a_\sigma,$$

mit[97]

Da die Gruppen rechts alles Untergruppen von $H^2(k)$ sind, wird der direkte Limes zur Vereinigung.

[95] Nach dem Hauptsatz der Galois-Theorie.

[96] vgl. [G & S], 2.3.6

[97] Additiv geschrieben ist dies gerade die 1-Kozyklen-Bedingung im (kommuativen) Fall eines G-Moduls A:

$$0 = (da)(\sigma, \tau) = \sigma\bullet a_\tau - a_{\sigma\tau} + a_\sigma$$

$$a_{\sigma\tau} = a_\sigma \bullet \sigma(a_\tau) \text{ für } \sigma, \tau \in G.$$

Zwei 1-Kozyklen

$$a: G \longrightarrow A, \sigma \mapsto a_\sigma ,$$

$$b: G \longrightarrow A, \sigma \mapsto b_\sigma ,$$

heißen äquivalent, wenn es ein Element

$$c \in A$$

gibt mit[98]

$$a_\sigma = c^{-1} \bullet b_\sigma \bullet \sigma(c) \text{ für } \sigma \in G.$$

Die Menge der Äquivalenzklassen von 1-Kozyklen wird mit

$$H^1(G, A)$$

bezeichnet und heißt erste Kohomologie von G mit Koeffizienten in A.

Bemerkungen

(i) Ist die Gruppe A abelsch, so ist $H^1(G, A)$ eine Gruppe und fällt mit der üblichen ersten Gruppen-Kohomologie von G zusammen.

(ii) Im allgemeinen Fall ist $H^1(G, A)$ nur eine punktierte Menge, wobei der ausgezeichnete Punkt durch den 1-Kozyklus

$$G \longrightarrow A, \sigma \mapsto 1,$$

repräsentiert wird.

(iii) Seien G eine Gruppe und

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$$

eine exakte Sequenz von Gruppen mit G-Operation (d.h. die Homomorphismen seien G-äquivariant). Dann gibt es eine exakte Sequenz von punktierten Mengen[99]

$$1 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C).$$

(iv) Satz 90 von Hilbert. Für jede endiche Galois-Erweiterung K/k gilt

$$H^1(G(K/k), GL(n, K)) = \{1\}.$$

Dabei operiere G(K/k) koordinatenweise auf den Einträgen der n×n-Matrizen. Der Beweis ist derselbe wie der obige Beweis im Fall n = 1.

(v) Seien G eine Gruppe, A eine Gruppe mit G-Operation und X eine Menge, auf welcher G und A in verträglicher Weise operieren,

$$G \times X \longrightarrow X, (\sigma, x) \mapsto \sigma(x),$$

$$A \times X \longrightarrow X, (\sigma, x) \mapsto \sigma \bullet a,$$

d.h. es gelte

$$\sigma(a \bullet x) = \sigma(a) \bullet \sigma(x)$$

für $\sigma \in G$, $a \in A$ und $x \in X$. Weiter sei ein 1-Kozyklus von G mit Koeffizienten in A gegeben,

$$a: G \longrightarrow A, \sigma \mapsto a_\sigma .$$

Dann läßt sich die Operation von G auf X mit Hilfe des Kozyklus abändern, d.h. es läßt sich eine neue Operation von G auf X wie folgt konstruieren.

---

[98] Additiv geschrieben bedeutet dies im kommuativen Fall:

$a_\sigma - b_\sigma = \sigma \bullet c - c = (dc)(\sigma)$,

d.h. die beiden 1-Kozyklen unterscheiden sich um einen 1-Korand.

[99] sieh [G & S], 2.6.1.

$$G \times X \longrightarrow X, (\sigma, x) \mapsto a_\sigma \bullet (\sigma(x)).$$

Man erhält auf diese Weise tatsächlich eine Operation von G auf X, denn für $\sigma, \tau \in G$ und $x \in X$ gilt:

$a_{\sigma\tau} \bullet (\sigma\tau(x)) = a_\sigma \sigma(a_\tau) \bullet (\sigma\tau(x))$ (Kozyklen-Bedingung)

$= a_\sigma \sigma(a_\tau \tau(x))$ (Verträglichkeit der Operationen von G und A)

Die neue Operation von G auf X heißt auch die mit a getwistete Operation. Die mit der getwisteten G-Operation versehene Menge wird mit

$${}_aX$$

bezeichnet.

1.4.15 Beispiel: die natürliche Operation einer Galoisgruppe auf einem Vektorraum

Seien K/k eine Galois-Erweiterung,

$G := G(K/k)$ Galois-Gruppe

$X := K^n$

$A := \mathrm{Aut}_K(X)$ Gruppe der K-linearen Automorphismen.

Die Operation von G auf X sei die koordinatenweise Fortsetzung der natürlichen Operation von G auf K,

$$G \times X \longrightarrow X, (\sigma, x) \mapsto x^\sigma \text{ mit } \begin{pmatrix} c_1 \\ \dots \\ c_n \end{pmatrix}^\sigma := \begin{pmatrix} \sigma(c_1) \\ \dots \\ \sigma(c_n) \end{pmatrix}$$

Die Operation von A auf X sei die natürliche[100]:

$$A \times X \longrightarrow X, (a, x) \mapsto a(x),$$

und die Operation von G auf A sei die übliche Operation[101]:

$$G \times A \longrightarrow A, (\sigma, a) \mapsto (x \mapsto (a(x^{\sigma^{-1}}))^\sigma)$$

Die Operationen von G und A auf X sind verträglich:

$$\sigma(a) \bullet \sigma(x) = \sigma(a)(x^\sigma) = (a(x^{\sigma\sigma^{-1}}))^\sigma = a(x)^\sigma = \sigma(a \bullet x)$$

Da G und A auf X durch k-lineare Automorphismen operieren, ist auch die getwistete Operation

$$G \times {}_aX \longrightarrow {}_aX, (\sigma, x) \mapsto a_\sigma \bullet (\sigma(x)),$$

eine Operation durch k-lineare Automorphismen.

Bemerkungen

(i) Identifiziert man $\mathrm{Aut}_K(X)$ mit den $n \times n$-Matrizen,

$$M_n(K) \overset{\cong}{\longrightarrow} \mathrm{Aut}(X) = A, M \mapsto f_M \text{ mit } f_M(x) = Mx,$$

so wird die oben definierte Operation von G auf A zur koordinatenweisen Operation

$$M \mapsto M^\sigma$$

---

[100] d.h. die Matrizen-Multiplikation, wenn man A mit den $n \times n$-Matrizen über K identifiziert.

[101] d.h. die Einschränkung auf A der G-Modul-Operation auf $\mathrm{Hom}_K(K^n, K^n)$.

von G auf den Einträgen der Matrizen:

$$(f_M(x^{\sigma^{-1}}))^\sigma = (M \bullet x^{\sigma^{-1}})^\sigma$$
$$= M^\sigma \bullet x^{\sigma^{-1}\sigma}$$
$$= M^\sigma \bullet x$$

(ii) Bekanntermaßen[102] ist jeder Automorphismus der Matrizen-Algebra $M_n(K)$ ein innerer Automorphismus, d.h. von der Gestalt

$$M_n(K) \longrightarrow M_n(K), X \mapsto C^{-1}XC,$$

mit einer umkehrbaren Matrix $C \in GL(n, K)$. Ersetzt man C durch ein skalaren Vielfaches erhält man eine Matrix, die in derselben Weise (durch Konjugation) auf der Matrizen-Algebra operiert. Dies definiert eine Operation der projektiven Gruppe

$$PGL(n, K) := GL(n, K)/K^*$$

auf $M_n(K)$,

$$PGL(n, K) \times M_n(K) \longrightarrow M_n(K), (C, M) \mapsto CMC^{-1}.$$

Auf diese Weise wird PGL(n , K) gerade zur Automorphismen-Gruppe der Matrizenalgebra $M_n(K)$.

1.4.16 Der Abstiegssatz für zentrale einfache Algebren[103]

Sei K/k eine endliche Galois-Erweiterung. Wir bezeichnen mit

$$CSA_K(n) = CSA_{K/k}(n)$$

die Menge der Isomorphieklassen zentraler einfacher k-Algebren des Grades n, welche über K zerfallen. Die Elemente

$$A \in CSA_K(n)$$

sind also zentrale einfache k-Algebren mit

$$A \otimes_k K \cong M_n(K).$$

Die Menge $CSA_K(n)$ ist eine punktierte Menge mit dem Basispunkt

$$M_n(k).$$

Satz[104]

Es besteht ein natürlicher Isomorphismus punktierter Mengen

$$CSA_K(n) \longrightarrow H^1(G(K/k), PGL(n, K)).$$

Beweisskitze. Wir beschränken uns darauf den Isomorphismus und dessen Umkehrung zu beschreiben. Die Einzelheiten siehe [G & S], 2.3.7 - 2.4.4.

Beschreibung der Abbildung des Satzes. Sei $A \in CSA_K(n)$ eine zentrale einfache k-Algebra, welche über K zerfällt. Wir fixieren einen K-linearen Isomorphismus

$$f: M_n(K) \xrightarrow{\cong} A \otimes_k K,$$

d.h.

---

[102] vgl [G & S], 2.4.1.

[103] vgl. [G & S], 2.4.3 und 2.3.7.

[104] Wir sind hier zunächst in der Situation endlicher Galois-Erweiterungen K/k. Um alle zentralen einfachen Algebren zu bekommen, müssen wir jedoch alle endlichen Körper-Erweiterungen K/k betrachten. Dadurch kommt die proendliche Kohomologie ins Spiel.

$$f(c\bullet M) = (1\otimes c)\bullet f(M) =: c\bullet f(M)$$

für $M \in M_n(K)$ und $c \in K$.

Jedes Element der Galois-Gruppe $G = G(K/k)$ definiert einen k-linearen Isomorphismus

$$1\otimes\sigma\colon A\otimes_k K \longrightarrow A\otimes_k K.$$

Durch Zusammensetzen mit f erhalten wir einen K-linearen Isomorphismus

$$\sigma(f) := (1\otimes\sigma)\circ f\circ\sigma^{-1}.$$

wobei der rechte Faktor σ^{-1} auf der rechten Seite die koordinatenweise Operation von G auf der Matrizen-Algebra bezeichne. Dieser Isomorphismus ist wieder K-linear: für $A\in M_n(K)$ und $c \in K$ gilt

$$\begin{aligned}
\sigma(f)(c\bullet A) &= (1\otimes\sigma)\circ f\circ\sigma^{-1}(c\bullet A) && \text{(Definition von } \sigma(f)) \\
&= (1\otimes\sigma)\circ f(c^{\sigma^{-1}} A^{\sigma^{-1}}) && (\ \sigma\in G(K/k)) \\
&= (1\otimes\sigma)\circ((1\otimes c^{\sigma^{-1}})\bullet f(A^{\sigma^{-1}})) && \text{(f ist K-linear)} \\
&= c\bullet (1\otimes\sigma)(\ f(A^{\sigma^{-1}})) && \text{(Definition der Multiplikation)} \\
&= c\bullet\sigma(f)(A). && \text{(Definition von } \sigma(f))
\end{aligned}$$

Wir setzen

$$a_\sigma := f^{-1}\circ\sigma(f) \in \mathrm{Aut}_K(M_n(K)).$$

Zeigen wir, die Abbildung

$$G \longrightarrow \mathrm{Aut}_K(M_n(K)) = PGL(n, K),\ \sigma \mapsto a_\sigma\ ,$$

ist ein 1-Kozyklus. Es gilt

$$\begin{aligned}
a_{\sigma\tau} &= f^{-1}\circ\sigma\tau(f) \\
&= f^{-1}\circ(1\otimes\sigma\tau)\circ f\circ(\tau^{-1}\sigma^{-1}) && \text{(Definitionb von } \sigma\tau(f)) \\
&= f^{-1}\circ(1\otimes\sigma)\circ(1\otimes\tau)\circ f\circ\tau^{-1})\circ\sigma^{-1} && \text{(Funktorialität von } \otimes) \\
&= f^{-1}\circ(1\otimes\sigma)\circ\tau(f)\circ\sigma^{-1} && \text{(Definition von } \tau(f)) \\
&= (a_\sigma\circ\sigma(f)^{-1})\circ(1\otimes\sigma)\circ\tau(f)\circ\sigma^{-1} && \text{(Definition von } a_\sigma) \\
&= a_\sigma\circ(\sigma\circ f^{-1}\circ(1\otimes\sigma)^{-1})\circ(1\otimes\sigma)\circ\tau(f)\circ\sigma^{-1} && \text{(Definition von } \sigma(f)) \\
&= a_\sigma\circ\sigma\circ f^{-1}\circ\tau(f)\circ\sigma^{-1} \\
&= a_\sigma\circ\sigma\circ a_\tau\circ\sigma^{-1} && \text{(Definition von } a_\tau) \\
&= a_\sigma\circ\sigma\bullet a_\tau. && \text{(Definition der Operation von G auf } \mathrm{Aut}(M_n(K))).
\end{aligned}$$

Wir haben gezeigt,

$$G \longrightarrow \mathrm{Aut}(M_n(K)) = PGL(n, K),\ \sigma \mapsto a_\sigma$$

ist ein 1-Kozyklus. Ersetzt man den Isomorphismus f durch einen anderen, so sieht man durch direktes Nachrechnen, daß der 1-Kozyklus durch einen äquivalenten 1-Kozyklus ersetzt wird. Wir erhalten so eine Abbildung der gesuchten Art.

Beschreibung der Umkehrabbildung. Sei ein Element der Kohomologie-Gruppe auf der rechten Seite gegeben. Wir wählen einen repräsentierenden 1-Kozyklus

$$G \longrightarrow \mathrm{Aut}(M_n(K)) = \mathrm{PGL}(n, K), \sigma \mapsto a_\sigma.$$

Mit Hilfe dieses 1-Kozyklus können wir die koordinatenweise Operation von G auf der Matrizen-Algebra abändern und erhalten eine Operation

$$G \times M_n(K) \longrightarrow M_n(K), (\sigma, M) \mapsto a_\sigma(M^\sigma).$$

Wir versehen die Matrizen-Algebra mit dieser getwisteten Operation und betrachten deren invarianten Teil,

$$A := ({}_aM_n(K))^G.$$

Dies ist eine k-Teilalgebra von $M_n(K)$,

$$A \subseteq M_n(K).$$

Nach dem Lemma von Speiser[105] gilt

$$A \otimes_k K \cong M_n(K).$$

Insbesondere ist A eine zentrale einfache k-Algebra des Grades n, welche über K zerfällt,

$$A \in \mathrm{CSA}_K(n).$$

A ist das gesuchte Urbild bei der oben beschriebenen Abbildung des Satzes.
QED.

Bemerkungen

(i) Das Tensorprodukt zentraler einfacher k-Algebren definiert für beliebige natürliche Zahlen m und n eine Abbildung

$$\mathrm{CSA}_K(n) \times \mathrm{CSA}_K(m) \longrightarrow \mathrm{CSA}_K(mn), (A, A') \mapsto A \otimes_k A'.$$

Auf Grund der obigen Bijektion ist damit auch eine Abbildung

$$H^1(G, \mathrm{PGL}(n, K)) \times H^1(G, \mathrm{PGL}(m, K)) \longrightarrow H^1(G, \mathrm{PGL}(mn, K)) \quad (1)$$

definiert. Diese läßt sich wie folgt beschreiben.

Das Tensorprodukt von linearen Abbildungen,

$$\mathrm{End}_K(K^n) \otimes_K \mathrm{End}_K(K^m) \longrightarrow \mathrm{End}_K(K^n \otimes_K K^m), (\phi, \psi) \mapsto \phi \otimes \psi,$$

läßt sich als Abbildung

$$\mathrm{GL}(n, K) \times \mathrm{GL}(m, K) \longrightarrow \mathrm{GL}(nm, K), ((a_{ij}), (b_{k\ell})) \mapsto (a_{ij} b_{k\ell}),$$

---

[105] 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

$$\sigma(cv) = \sigma(c) \bullet \sigma(v) \text{ für } \sigma \in G, v \in V, c \in K.$$

Dann ist die natürliche Abbildung

$$\lambda: V^G \otimes_k K \longrightarrow V, v \otimes c \mapsto cv,$$

ein Isomorphismus von K-Vektorräumen. Dabei bezeichne

$$V^G := \{v \in V \mid \sigma v = v \text{ für } \sigma \in G\}$$

den Raum der G-invarianten Vektoren von V.

(vgl. [G & S] 2.3.13). Der Beweis des Lemmas von Speiser verwendet die Theorie der halbeinfachen Ringe und Moduln, wie man sie zum Beispiel im Buch von Scheja und Storch dargelegt findet,

G. Scheja und U. Storch: Lehrbuch der Algebra, Teubner-Verlag Stuttgart 1994,

oder im Anhang meiner Vorlesungsnotizen [G & S] zur Monografie

Gille und Szamuely: Central simple algebras (vgl. A1.12).

auffassen und induziert eine Abbildung

$$\psi: PGL(n, K) \times PGL(m, K) \longrightarrow PGL(nm, K).$$

Diese wiederum induziert die obige Abbildung auf den Kohomologien. Genauer, Abbildung (1) hat die Gestalt[106]

$$([a_\alpha],[b_\beta]) \mapsto [\psi\circ(a_\alpha \times b_\beta)\circ\Delta],$$

wenn $\Delta: G \longrightarrow G\times G$, $x \mapsto (x,x)$, die Diagonal-Einbettung bezeichnet.
(zum Beiweis siehe [G & S], 2.4.6).

(ii) Für beliebige natürliche Zahlen m und n induzieren die Abbildungen

$$GL(n, K) \longrightarrow GL(mn, K), X \mapsto \begin{pmatrix} X & 0 & \dots & 0 \\ 0 & X & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & X \end{pmatrix},$$

Gruppen-Homomorphismuen

$$PGL(n, K) \longrightarrow PGL(mn, K),$$

welche ein induktives System bilden. Durch Übergang zur Gruppen-Kohomologie erhält man ein induktives System

$$\lambda_{nm}: H^1(G, PGL(n, K)) \longrightarrow H^1(G, PGL(mn, K)).$$

Das zugehörige induktive System für die zentralen einfachen Algebren hat die Gestalt

$$CSA_K(n) \longrightarrow CSA_K(mn), A \mapsto A\otimes_k M_m(k).$$

Die Abbildungen λ_{nm} sind injektiv. (zum Beiweis siehe [G & S], 2.4.7 und 2.4.8).

(iii) Durch Übergang zum direkten Limes erhält man aus (i) und (ii) die folgende Abbildung

$$\begin{array}{ccc} \varinjlim_n CSA_K(n) & \xrightarrow{\lambda} & \varinjlim_n H^1(G, PGL(n, K)) \\ \| & & \| \\ \bigcup_{n=1}^{\infty} CSA_K(n) & & \bigcup_{n=1}^{\infty} H^1(G, PGL(n, K)) \end{array}$$

Wir schreiben

$$CSA_K / \sim := \bigcup_{n=1}^{\infty} CSA_K(n)$$

für die Menge der Isomorphieklassen zentraler einfacher k-Algebren, welche über K zerfallen, modulo der Identifikationen $A \mapsto A\otimes_k M_m(k)$.[107] Weiter schreiben wir

$$H^1(G, PGL(\infty, K)) = \bigcup_{n=1}^{\infty} H^1(G, PGL(n, K))$$

---

[106] Die repräsentierenden Kozyklen sind Abbildungen

$$a: G \longrightarrow PGL(n, K) \text{ bzw. } b: G \longrightarrow PGL(m, K).$$

Durch Komposition erhält man eine Abbildung

$$G \xrightarrow{\Delta} G\times G \xrightarrow{a\times b} PGL(n, K) \times PGL(m, K) \xrightarrow{\psi} PGL(mn, K).$$

[107] d.h. zwei zentrale einfache Algebren sind als gleich anzusehen, wenn sie als Elemente einer der Mengen $CSA_K(n)$ gleich sind.

für die Menge auf der rechten Seite. Die Abbildung bekommt so die Gestalt

$$\lambda_K: CSA_K/\sim \longrightarrow H^1(G, PGL(\infty, K))$$

Sie ist nach Konstruktion bijektiv und respektiert die in (i) beschriebenen multiplikativen Strukturen:

$$\lambda(A\otimes_k A') = \lambda(A)\bullet\lambda(A').$$

Die Relation $\sim$ ist gerade die Brauer-Äquivalenz:

$$A \sim A' \Leftrightarrow A\otimes_k M_m(k) \cong A'\otimes_k M_{m'},(k) \text{ für geeignete m und m'}$$

$$\Leftrightarrow A \text{ und } A' \text{ sind Brauer-äquivalent,}$$

d.h. es ist

$$CSA_K/\sim \cong Br(K/k)$$

gerade die relative Brauer-Gruppe. Die Abbildung λ definiert damit eine Gruppen-Isomorphie

$$Br(K/k) \cong H^1(G, PGL(\infty, K)).$$

Durch Übergang zum direkten Limes über die endlichen Galois-Erweiterungen von k erhält man eine Gruppen-Isomorphie

$$Br(k) \cong \varinjlim_{K/k} H^1(G, PGL(\infty, K)) =: H^1(k, PGL_\infty)$$

1.4.17 Konstruktion: Vergleich von $H^1(k, PGL(\infty, K))$ und $H^2(G(K/k), K^*)$.

(i) Für jede endliche Galois-Erweiterung K/k hat man eine exakte Sequenz

$$1 \longrightarrow K^\times \longrightarrow GL(m, K) \longrightarrow PGL(m, K) \longrightarrow 1$$

und damit eine exakte Kohomologie-Sequenz (punktierter Mengen)

$$H^1(G, GL(m, K)) \longrightarrow H^1(G, PGL(m, K)) \xrightarrow{\delta_m} H^2(G, K^\times),$$

wobei G = G(K/k) die Galois-Gruppe bezeichne.

Für je zwei natürliche Zahlen m und n ist dabei das folgende Diagramm kommutativ.

$$\begin{array}{ccc} H^1(G, PGL(m,K)) & \xrightarrow{\delta_m} & H^2(G,K^\times) \\ \lambda_{m,n}\downarrow & & \downarrow Id \\ H^1(G,PGL(mn,K)) & \xrightarrow{\delta_{mn}} & H^2(G,K^\times) \end{array}$$

(ii) Die Abbildungen δ_m von (i) definieren also einen Morphismus induktiver Systeme und induzieren somit Abbildungen (punktierter Mengen) auf den induktiven Limites (bezüglich n und K),

$$\delta_K: H^1(G, PGL(\infty, K)) \longrightarrow H^2(G, K^\times), G = G(K/k),$$

$$\delta: H^1(k, PGL_\infty) \longrightarrow H^2(k,)$$

(wobei rechts unten die Galois-Kohomologie des Körpers k steht). Dies sind Gruppen-Homomorphismen.

(iii) Die Gruppen-Homomorphismen δ_K und δ von (ii) sind Isomorphismen.

Beweis Zu (i). Seien $[c]\in H^1(G, PGL(m,K))$ ein Element und

(1) $$c: G \longrightarrow PGL(m,K), \sigma \mapsto c_\sigma,$$

ein repräsentierender 1-Kozyklus. Das Bild von [c] bei δ_m wird dann repräsentiert durch den 2-Kozyklus

$$a: G\times G \longrightarrow K^\times, (\sigma,\tau) \mapsto a_{\sigma,\tau} \text{ mit } a_{\sigma,\tau}\bullet Id_m :=^{108} b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1}.$$

Dabei bezeichne $b_\sigma \in GL(m,K)$ einen Repräsentanten von c_σ und Id_m die $m\times m$-Einheitsmatrix. Einen Repräsentanten für das Bild

$$\lambda_{m,n}([c])$$

erhält man, indem man in (1) Repräsentanten b_σ von c_σ durch die Block-Matrix

$$b'_\sigma = \begin{pmatrix} b_\sigma & 0 & 0 \\ \dots & \dots & \dots \\ 0 & 0 & b_\sigma \end{pmatrix}$$

ersetzt, die aus n Exemplaren der Matrix b_σ auf der Hauptdiagonalen und sonst lauter Null-Matrizen besteht. Das Element

$$\delta_{m,n}(\lambda_{m,n}([c]))$$

wird also repräsentiert durch den 2-Kozyklus

$$a': G\times G \longrightarrow K^\times, (\sigma,\tau) \mapsto a'_{\sigma,\tau},$$

wobei $a'_{\sigma,\tau}$ den Eintrag auf der Hauptdiagonalen der folgenden Skalarmatrix bezeichnet.

$$b'_\sigma \sigma(b'_\tau) b'^{-1}_{\sigma\tau} = \begin{pmatrix} b_\sigma & 0 & 0 \\ \dots & \dots & \dots \\ 0 & 0 & b_\sigma \end{pmatrix} \begin{pmatrix} \sigma(b_\tau) & 0 & 0 \\ \dots & \dots & \dots \\ 0 & 0 & \sigma(b_\tau) \end{pmatrix} \begin{pmatrix} b_{\sigma\tau} & 0 & 0 \\ \dots & \dots & \dots \\ 0 & 0 & b_{\sigma\tau} \end{pmatrix}^{-1}$$

$$= \begin{pmatrix} b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1} & 0 & 0 \\ \dots & \dots & \dots \\ 0 & 0 & b_\sigma \sigma(b_\tau) b_{\sigma\tau}^{-1} \end{pmatrix}$$

$$= \begin{pmatrix} a_{\sigma,\tau}\bullet Id_m & 0 & 0 \\ \dots & \dots & \dots \\ 0 & 0 & a_{\sigma,\tau}\bullet Id_m \end{pmatrix}$$

$$= a_{\sigma,\tau}\bullet Id_{nm}$$

Es gilt also $a'_{\sigma,\tau} = a_{\sigma,\tau}$ wie behauptet.

---

[108] Die rechte Seite dieser Identität ist dabei die nicht-abelsche Variante des abelschen Korandes von b,

$$(db)_{\sigma,\tau} = \sigma\bullet b_\tau - b_{\sigma\tau} + b_\sigma$$

Zu (ii). Nach Bemerkung 1.4.14 (i) wird die Gruppen-Struktur von $H^1(G, PGL(\infty, K))$ durch die Abbildungen

$$H^1(G, PGL(n, K)) \times H^1(G, PGL(m, K)) \longrightarrow H^1(G, PGL(mn, K)).$$

definiert, die induziert werden durch Abbildungen

$$PGL(n, K) \times PGL(m, K) \longrightarrow PGL(nm, K), ([\varphi], [\psi]) \mapsto [\varphi\otimes\psi],$$

der Koeffizienten-Gruppen, die ihrerseits vom Tensorprodukt

$$GL(n, K) \times GL(m, K) \longrightarrow GL(nm, K), (\varphi, \psi) \mapsto \varphi\otimes\psi,$$

linearer Endomorphismen kommen.
Seien jetzt

$$[c] \in H^1(G, PGL(n, K)) \ , [d] \in H^1(G, PGL(m, K))$$

vorgegebene Elemente. Wir haben zu zeigen,

$$\delta_{mn}([c]\bullet[d]) = \delta_n([c])\bullet\delta_m([d])$$

Wir wählen repräsentierende 1-Kozyklen

$$G \longrightarrow PGL(n, K), \sigma\mapsto [c_\sigma], \text{ und } G \longrightarrow PGL(m, K), \sigma\mapsto [d_\sigma],$$

für [c] bzw. [d]. Für jedes $\sigma\in G$ seien $c_\sigma\in GL(n,K)$ und $d_\sigma\in GL(m,K)$ geeignete lineare Automorphismen, die die entsprechenden Elemente der projektiven linearen Gruppen repräsentieren. Dann wird

$$[c]\bullet[d] \in H^1(G, PGL(mn, K))$$

repräsentiert durch den 1-Kozyklus

$$\sigma \mapsto [c_\sigma\otimes d_\sigma] \in Aut(K^n\otimes K^m)/K^* = Aut(K^{nm})/K^* = PGL(mn, K).$$

Nach Defnition (vgl. den Beweis von (i)) werden die Elemente

$$\delta_n([c]) = [a], \delta_m([d]) = [b] \text{ und } \delta_{mn}([c]\bullet[d]) = [x]$$

repräsentiert durch die 2-Kozyklen

$$a, b, x: G\times G \longrightarrow K^\times, (\sigma, \tau) \mapsto a_{\sigma,\tau} , (\sigma, \tau) \mapsto b_{\sigma,\tau} , (\sigma, \tau) \mapsto x_{\sigma,\tau} ,$$

mit

$$a_{\sigma,\tau} = c_\sigma\sigma(c_\tau)c_{\sigma\tau}^{-1} \in K^\times\bullet Id_n \cong K^\times,$$

$$b_{\sigma,\tau} = d_\sigma\sigma(d_\tau)d_{\sigma\tau}^{-1} \in K^\times\bullet Id_m \cong K^\times,$$

$$x_{\sigma,\tau} = (c_\sigma\otimes d_\sigma)\sigma(c_\tau\otimes d_\tau)(c_{\sigma\tau}\otimes d_{\sigma\tau})^{-1} \in K^\times\bullet Id_{mn} \cong K^\times.$$

(wenn wir die Gruppe $K^\times$ mit deren natürlichen Bildern in GL(n,K), GL(m,K) und GL(mn,K) identifizieren, d.h. die Elemente von $K^\times$ mit den zugehörigen Skalarmatrizen). Die Endomorphismen c_σ und d_τ operieren auf unterschiedlichen Tensor-Faktoren, d.h. diese Operationen kommutieren.[109] Deshalb gilt

$$\begin{aligned} x_{\sigma,\tau} &= (c_\sigma\otimes d_\sigma)\sigma(c_\tau\otimes d_\tau)(c_{\sigma\tau}\otimes d_{\sigma\tau})^{-1} \\ &= c_\sigma\sigma(c_\tau)c_{\sigma\tau}^{-1}\otimes d_\sigma\sigma(d_\tau)d_{\sigma\tau}^{-1}. \\ &= a_{\sigma,\tau}\otimes b_{\sigma,\tau} \qquad \text{in } GL(mn,K) \end{aligned}$$

---

[109] d.h. $(c_\sigma\otimes 1)\bullet(1\otimes d_\tau) = c_\sigma\otimes d_\tau = (1\otimes d_\tau)\bullet(c_\sigma\otimes 1)$.

Für die zugehörigen 2-Kozyklen erhalten wir

$$[x] = [a]\bullet[b] \text{ in } H^1(G, K^\times),$$

d.h.

$$\delta_{mn}([c]\bullet[d]) = \delta_n([c]) \bullet \delta_m([d]).$$

Zu (iii). Es reicht, die Bijektivität von δ_K zu beweisen. Die von δ ergibt sich dann durch Übergang zum induktiven Limes. Zum Beweis der Injektivität von

$$\delta_K: H^1(G, PGL(\infty, K)) \longrightarrow H^2(G, K^\times)$$

reicht es zu zeigen, die Einschränkungen δ_m von δ_K auf die Teilmengen

$$H^1(G, PGL(m, K))$$

haben einen trivialen Kern (als Morphismus punktierter Mengen). Wegen der exakten Sequenz

$$H^1(G, GL(m, K)) \longrightarrow H^1(G, PGL(m, K)) \xrightarrow{\delta_m} H^2(G, K^\times)$$

von (i) reicht es zu zeigen, $H^1(G, GL(m, K)) = 0$. Das ist aber der Fall nach dem Satz 90 von Hilbert (vgl. 1.4.14(iv))

Wir haben noch die Surjektivität von δ_K zu beweisen, d.h. wir haben zu zeigen, jedes Element von $H^2(G, K^\times)$ liegt im Bild von mindestens einer der Abbildungen δ_m. Wir werden hier sogar zeigen, die Abbildung

$$\delta_m: H^1(G, PGL(m,K)) \longrightarrow H^2(G, K^\times)$$

ist surjektiv, falls

$$m = \# G$$

die Ordnung von G ist.

Zum Beweis betrachten wir den K-Vektorraum

$$K\otimes_k K$$

mit der G-Modul-Struktur,[110] die durch die Operation von G auf dem zweiten Faktor gegeben ist,

$$\sigma\bullet(c'\otimes c'') := c'\otimes\sigma(c'').$$

Durch Wahl einer k-Vektorraum-Basis für den ersten Tensor-Faktor (d.h. eines Isomorphismus des letzteren mit k^m) wird das Tensor-Produkt isomorph zu K^m,

$$K\otimes_k K \cong k^m\otimes_k K \cong K^m.$$

Die Multiplikation mit einem umkehrbaren Element von $K\otimes_k K$ definiert einen K-linearen Automorphismus $K\otimes_k K \longrightarrow K\otimes_k K$ und man erhält so einen Gruppen-Homomorphismus

$$(K\otimes_k K)^\times \longrightarrow GL(m, K), x \mapsto \text{Multiplikation mit } x.$$

Dieser ist ein Homomorphismus von Gruppen mit mit G-Operation, G = G(K/k).[111] Er läßt sich wie folgt in ein kommutatives Diagramm mit exakten Zeilen einfügen.

---

[110] Die K-Vektorraum-Struktur komme von der K-Vektorraum-Struktur des zweiten Tensor-Faktors.

[111] Ist $\omega_1,...,\omega_m$ die betrachtete k-Vektorraumbasis von K über k, also $\omega_1\otimes 1,...,\omega_m\otimes 1$ die von $K\otimes_k$ K über K, so sind die Eintrge c_{ij} der Matrix zur Einheit $\alpha\in K\otimes_k K$ durch die Bedingung

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \longrightarrow & (K\otimes_k K)^\times & \longrightarrow & (K\otimes_k K)^\times/K^\times & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & GL(m,K) & \longrightarrow & PGL(m,K) & \longrightarrow & 1 \end{array}$$

Dabei soll Abbildung links oben von der Einbettung in den zweiten Tensor-Faktor kommen,

$$K^\times \longrightarrow (K\otimes_k K)^\times, c \mapsto 1\otimes c.$$

Alle Abbildungen des Diagramms sind dann verträglich mit der Operation der Galois-Gruppe G. Wir gehen zur Kohomologie über und erhalten ein kommutatives Diagramm mit exakter oberer Zeile:

$$\alpha\bullet(\omega_i\otimes 1) = \sum_{j=1}^{m} c_{ji}\bullet\omega_j\otimes 1$$

gegeben. Ersetzen wir α durch $\sigma(\alpha)$, so läuft dies darauf hinaus, c_{ij} durch $\sigma(c_{ij})$ zu ersetzen: Mit

$$\alpha = \sum_\ell \alpha_\ell\otimes\alpha'_\ell$$

gilt, weil G nur auf den zweiten Tensorfaktor wirkt,

$$\begin{aligned} \sigma(\alpha)\bullet(\omega_i\otimes 1) &= \sigma(\sum_\ell \alpha_\ell\otimes\alpha'_\ell)\bullet(\omega_i\otimes 1) \\ &= (\sum_\ell \alpha_\ell\otimes\sigma(\alpha'_\ell))\bullet(\omega_i\otimes 1) \quad \text{(Definition der Operation von } \sigma) \\ &= (\sum_\ell \alpha_\ell\,\omega_i\otimes\sigma(\alpha'_\ell)) \quad \text{(Definition der Multiplikation in } K\otimes K) \\ &= \sigma(\sum_\ell \alpha_\ell\,\omega_i\otimes\alpha'_\ell) \quad \text{(Definition der Operation von } \sigma) \\ &= \sigma((\sum_\ell \alpha_\ell\otimes\alpha'_\ell)\bullet(\omega_i\otimes 1)) \quad \text{(Definition der Multiplikation von } K\otimes K)) \\ &= \sigma(\alpha\bullet(\omega_i\otimes 1)) \quad \text{(Definition von } \alpha_\ell \text{ und } \alpha'_\ell) \\ &= \sigma(\sum_{j=1}^{m} c_{ji}\bullet\omega_j\otimes 1) \quad \text{(Definition der } c_{ji}) \\ &= \sigma(\sum_{j=1}^{m} \omega_j\otimes c_{ji}) \quad \text{(Defintion der K-Algebra-Struktur von } K\otimes K). \\ &= \sum_{j=1}^{m} \omega_j\otimes\sigma(c_{ji}) \quad \text{(Definition der Operation von } \sigma) \\ &= \sum_{j=1}^{m} \sigma(c_{ji})\bullet\omega_j\otimes 1 \quad \text{(Defintion der K-Algebra-Struktur von } K\otimes K). \end{aligned}$$

$$\begin{array}{ccccc} H^1(G,(K\otimes_k K)^\times/K^\times) & \xrightarrow{\alpha} & H^2(G,K^\times) & \longrightarrow & H^2(G,(K\otimes_k K)^\times) \\ \downarrow & & || & & \\ H^1(G,PGL(m,K)) & \xrightarrow{\delta_m} & H^2(G,K^\times) & & \end{array}$$

Zum Beweis der Surjektivität von δ_m reicht es, die von α zu beweisen. Wegen der Exaktheit der oberen Zeile wiederum reicht es zu zeigen,

$$H^2(G, (K\otimes_k K)^\times) = 0.$$

Dazu wiederum reicht es zu zeigen, daß $(K\otimes_k K)^\times$ ein koinduzierter G-Modul ist.

Zum Beweis schreiben wir die endliche Galois-Erweiterung K/k als einfache Erweiterung

$$K = k[x]/(f)$$

mit einem irreduziblen Polynom $f\in k[x]$. Ist $\alpha\in K$ eine Nullstelle von f, so gilt

$$f(x) = \prod_{\sigma\in G} (x - \sigma(\alpha)).$$

wobei die $\sigma(\alpha)$ paarweise verschieden sind (denn K/k ist separabel). Wir schreiben jetzt den ersten Tensor-Faktor (d.h. den mit der trivialen Operation) von $K\otimes_k K$ in der Gestalt k[x]/(f) und erhalten

$$\begin{aligned} K\otimes_k K &\cong k[x]/(f)\otimes_k K \\ &\cong K[x]/(f) \\ &\cong K[x]/(\prod_{\sigma\in G} (x - \sigma(\alpha))) \\ &\cong \oplus_{\sigma\in G} K[x]/(x - \sigma(\alpha)) \\ &\cong \oplus_{\sigma\in G} K\sigma \end{aligned}$$

wobei die vorletzte Isomorphie nach dem Chinesischen Restesatz besteht. Die Operation von G auf dem Tensorprodukt entspricht dabei der folgenden Operation auf der direkten Summe[112]

$$G \times (\oplus_{\sigma\in G} K\sigma) \longrightarrow \oplus_{\sigma\in G} K\sigma, (\sigma, \sum_{\tau\in G} c_\tau\tau) \mapsto \sum_{\tau\in G} \sigma(c_\tau)\sigma\tau .$$

Die Multiplikation der Tensor-Algebra entspricht nach dem Chinesischen Restesatz gerade der "koordinatenweisen" Multiplikation[113]:

---

[112] Die Operation von G auf K[x]/(f) kommt von der Operation

$$G \times K[x] \longrightarrow K[x], (\sigma , g) \mapsto g^\sigma,$$

wobei das Polynom g^σ entstehe durch Anwenden von σ auf alle Koeffizienten des Polynoms g. Diese letztere Operation permutiert die Linearfaktoren $x - \tau(\alpha)$ des Polynoms f.

[113] Die Projektionen auf die einzelnen direkten Summanden sind Ring-Homomorphismen, d.h. der τ-te direkte Summand wird in den $\sigma\tau$-ten direkten Summanden abgebildet.

$$(\sum_{\tau\in G} c_\tau\tau)\bullet(\sum_{\tau\in G} d_\tau\tau) = \sum_{\tau\in G} c_\tau d_\tau\tau .$$

Insbesondere bestehen für die multiplikativen Gruppen die Isomorphien

$$(K\otimes_k K)^\times \cong \oplus_{\sigma\in G} K^\times\bullet\sigma = K^\times\otimes_{\mathbb{Z}}\mathbb{Z}[G] \cong^{114} \mathrm{Hom}_{Ab}(\mathbb{Z}[G], K^\times)$$

welche mit den G-Operationen verträglich sind. Mit anderen Worten, $(K\otimes_k K)^\times$ ist ein koinduzierter G-Modul.
.**QED**.

1.4.18 Die kohomologische Brauer-Gruppe

Seien k ein Körper, k^s eine separable Abschließung von k und K/k eine endliche Galois-Erweiterung mit der Gruppe G. Dann bestehen folgende natürliche Isomorphien von abelschen Gruppen.

$$Br(K/k) \cong H^2(G, K^\times) \text{ und } Br(k) \cong H^2(k, k_s^\times).$$

Außerdem sind die Abbildungen

$$\delta_m : H^1(G, PGL(m, K)) \longrightarrow H^2(G, K^\times)$$

injektiv für jedes m und bijektiv, falls

$$m = [K:k] \text{ ist.}$$

Im letzteren Fall gilt weiter:

1. Die Abbildungen
$$\lambda_{m,n} : H^1(G, PGL(m, K)) \longrightarrow H^1(G, PGL(mn, K))$$
bijektiv für jedes n.[115]
2. Die punktierte Menge
$$H^1(G, PGL(m, K))$$
besitzt eine Gruppen-Struktur mit der Multiplikation
$$H^1(G, PGL(m, K)) \times H^1(G, PGL(m, K)) \longrightarrow H^1(G, PGL(m^2, K)) \cong H^1(G, PGL(m, K)).$$
3. Die Abbildung
$$\delta_n : H^1(G, PGL(m, K)) \longrightarrow H^2(G, K^\times)$$
ist ein Isomorphismus abelscher Gruppen.

Für die Einzelheiten, vgl. [G & S] 4.4.8.

Bemerkungen

(i) Die Brauer-Gruppen Br(K/k) und Br(k) sind Torsionsgruppen (d.h. jedes Element hat eine endliche Ordnung).

(ii) Sei m eine zur Charakteristik von k teilerfremde natürliche Zahl. Dann ist die m-Torsions-Untergruppe der Brauergruppe isomorph zu
$${}_mBr(k) \cong H^2(k, \mu_m).$$
Dabei bezeichnet wie bisher $\mu_m \subseteq k^s$ die Gruppe der m-ten Einheitswurzeln mit der natürlichen Operation der Galois-Gruppe $G := G(k_s/k)$.

---

[114] G = G(K/k) ist endlich, d.h. die Begriffe "induziert" und "koinduziert" fallen zusammen.

[115] Beide Mengen sind "Teilmengen" von Br(K/k) und die linke Menge ist bereits die ganze Menge Br(K/k).

(iii) Sei K/k eine zyklische Galois-Erweiterung (endlicher Ordnung). Dann ist die relative Brauer-Gruppe isomorph zu

$$Br(K/k) \cong k^\times / N_{K/k}(K^\times),$$

d.h. wir haben einen surjektiven Gruppen-Homomorphismus

$$k^\times \longrightarrow Br(K/k)$$

mit dem Kern $N_{K/k}(K^\times)$. Dieser heißt auch Norm-Reste-Abbildung.

(iv) Für jede endliche Galois-Erweiterung K/k besteht eine exakte Sequenz

$$0 \longrightarrow Br(K/k) \xrightarrow{Inf} Br(k) \xrightarrow{Res} Br(K).$$

Diese reflektiert gerade die Beschreibung von Br(K/k) als die Menger der Klassen zentraler einfacher k-Algebren, die über K zerfallen.

Beweis. Zu (i). Wegen

$$Br(k) = H^2(k, k^{s\times}) = \varinjlim_{K/k} H^2(G(K/k), K^\times)$$

liegt jedes Element von Br(k) im Bild eines natürlichen Homomorphismus

$$Br(K/k) = H^2(G(K/k), K^\times) \longrightarrow H^2(k, k^{s\times})$$

mit einer geeigneten endlichen Galois-Erweiterung K/k. Die Kohomologie-Gruppe links wird aber von der Gruppen-Ordnung von G(K/k) annulliert, d.h. jedes Element dieser Gruppe hat eine endliche Ordnung. Dasselbe gilt dann aber auch für das homomorphe Bild dieses Elements in $H^2(k, k^{s\times})$.
Zu (ii). Wir verwenden die exakte G-Modul-Sequenz von Kummer

$$1 \longrightarrow \mu_m \longrightarrow k_s^\times \xrightarrow{m} k^{s\times} \longrightarrow 1,$$

wobei die Abbildung m hier den Übergang zur m-ten Potzen bezeichne. Dies ist offensichtlich ein Homomorphismus der multiplikativen Gruppen (und kommutiert mit der Operation der Galois-Gruppe). Um zu sehen, daß diese Abbildung surjektiv ist, beachte man, das Polynom

$$T^m - c \text{ mit } c \in k^{s\times}$$

ist separabel (weil m teilerfremd zur Charakteristik von k ist). Seine Nullstellen liegen also sämtlich in $k^{s\times}$.

Wir gehen zu Kohomologie über und erhalten die exakte Sequenz

$$H^1(k, k^{s\times}) \longrightarrow H^2(k, \mu_m) \longrightarrow H^2(k, k^{s\times}) \xrightarrow{m} H^2(k, k^{s\times}) .$$

Die Gruppe links ist trivial nach dem Satz 90 von Hilbert (1.4.12 (ii)). Die Abbildung rechts kommt vom Erheben der Elemente von $k_s^\times$ in die m-te Potenz. Dies entspricht dem Übergang zur m-ten Tensor-Potenz der zugehörigen k-linearen Automorphismen von k_s und damit der Multiplikation mit m auf der additiv geschriebenen Gruppe

$$H^2(k, k_s^\times) = Br(k).$$

Zu (iii). Weil G = G(K/k) nach Voraussetzung zyklisch ist, gilt nach Bemerkung 1.4.6 (iv)

$$H^2(G, K^\times) \cong (K^\times)^G / N \bullet K^\times = k^\times / N_{K/k}(K^\times).$$

Dabei bezeichne N in der Mitte gerade die Summe der Elemente von G im Gruppenring $\mathbb{Z}[G]$.
Zu (iv). Dies ist gerade die exakte Sequenz von Bemerkung 1.4.13.(v).
QED.

Als nächstes wollen wir den Abstiegssatz zur Konstruktion neuer zentraler einfacher Algebren verwenden.

1.4.19 Zyklische Algebren (vgl. G & S 2.5.4)

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, d.h. eine zentrale einfache k-Algebra A mit

$$A\otimes_k K \cong M_m(k)\otimes_k K,$$

und welche die zu χ und b gehörige zyklische k-Algebra heißt.

Dazu betrachten wir die Matrix

$$\widetilde{F}(b) := \begin{pmatrix} 0 & b \\ Id_{m-1} & 0 \end{pmatrix} \in GL(m, k).$$

wobei $Id_{m-1} \in GL(m-1,k)$ die Einheitmatrix bezeichne. Weiter sei

$$F(b) := \widetilde{F}(b) \bmod k^* \in PGL(n,k)$$

das natürliche Bild von $\widetilde{F}$ ven linearen Gruppe. Die Muiltiplikation der Matrix $\widetilde{F}(b)$ mit den Standard-Einheitsvektoren liefert

$$\widetilde{F}(b)\bullet e_i = e_{i+1} \text{ für } i = 1,...,m-1$$

$$\widetilde{F}(b)\bullet e_m = b\bullet e_1 .$$

Daraus liest man ab, daß $\widetilde{F}(b)$, $\widetilde{F}(b)^2$,...,$\widetilde{F}(b)^{m-1}$ keine Skalarmatrizen sind[116], und es gilt

$$\widetilde{F}(b)^m = b\bullet Id_m,$$

d.h.

F(b) ist ein Element der Ordnung m von PGL(m, k).

Wir erhalten so einen injektiven Gruppen-Homomorphismus

---

[116] Das Bild von e_1 ist kein Vielfaches von e_1

$$\mathbb{Z}/m\mathbb{Z} \hookrightarrow PGL(m,k),\ i \bmod m \mapsto F(b)^i.$$

Zusammensetzen mit χ und der natürlichen Einbettung $PGL(m,k) \hookrightarrow PGL(m,K)$ liefert einen injektiven Gruppen-Homomorphismus

$$z(b): G \xrightarrow{\chi} \mathbb{Z}/m\mathbb{Z} \hookrightarrow PGL(m,k) \hookrightarrow PGL(m,K),\ g \mapsto F(b)^{\chi(g)}.$$

Weil das Bild von z(b) sogar in PGL(m,k) liegt, können wir z(b) auch als 1-Kozyklus auffassen.[117] Wir versehen $M_n(K)$ mit der durch z(b) getwisteten Operation und definieren

$$(\chi, b) := ({}_{z(b)}M_m(K))^G$$

d.h. (χ, b) ist die Algebra der G-Invarianten bezüglich dieser Operation. Nach dem Abstiegssatz 1.4.16 ist auf diese Weise eine zentrale einfache k-Algebra des Grades m definiert, die über K zerfällt.

Bemerkung

Die zyklische k-Algebren (χ, b) läßt sich wie folgt beschreiben:[118] es gibt 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 von (i). 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[119]. Mit anderen Worten, A ist die von K und y erzeugte (assoziative aber nicht notwendig kommutative) k-Algebra mit den Relationen 2. und 3.[120]

---

[117] Für $\sigma,\tau \in G$ gilt $z(b)(\sigma\tau) = z(b)(\sigma) \bullet z(b)(\tau) = z(b)(\sigma) \bullet \sigma(z(b)(\tau))$

[118] Diese Beschreigung wurde ursprünglich von Dickson vorgeschlagen.

[119] Anstelle der y-Potenzen verwenden wir 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

$$j(\sum_{i=0}^{m-1} \lambda_i y^i) := \sum_{i=0}^{m-1} \mathrm{diag}(\sigma^{m-1}(\lambda_i),\sigma^{m-2}(\lambda_i),...,\lambda_i)\bullet\widetilde{F}(b)^i.$$

Dabei bezeichne diag(...) die Diagonalmatrix mit den angegebenen Einträgen auf der Hauptdiagonalen. Diese Abbildung ist k-linear und überführt jedes Element

$$c \in k \subseteq K\bullet 1$$

in

$$j(c) = j(c\bullet 1) = \mathrm{diag}(\sigma^{m-1}(c),\sigma^{m-2}(c),...,\sigma(c),c)\bullet\widetilde{F}(b)^0 = c\bullet Id,$$

d.h in sich selbst.

(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 $y\lambda = \sigma(\lambda)y$.

[120] 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

$$a_1 b_1 \bullet ... \bullet a_\ell b_\ell$$

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

$1\bullet b = b$ für jede y-Potenz

$a\bullet y^0 = a$ 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.

1. Schritt: j ist ein Homomorphismus von k-Algebren:
Wir haben zu zeigen, die definierenden Relationen 2. und 3. sich auch für das Bild

$$j(y) = \widetilde{F}(b)$$

von y erfüllt[121], 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 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

$$j(\sigma(\lambda))\bullet\widetilde{F}(b)\bullet e_i = j(\sigma(\lambda))\bullet e_{i+1} = \sigma^{m-i-1}(\sigma(\lambda))e_{i+1} = \sigma^{m-i}(\lambda)e_{i+1}$$

$$=^{122} \widetilde{F}(b)\bullet\sigma^{m-i}(\lambda)e_i = \widetilde{F}(b)\bullet j(\lambda)\bullet e_i$$

d.h. beide Seiten haben dieselbe i-te Spalte. Für i = m erhalten wir

$$j(\sigma(\lambda))\bullet\widetilde{F}(b)\bullet e_m = j(\sigma(\lambda))\bullet be_1 = \sigma^{m-1}(\sigma(\lambda))be_1 = \sigma^m(\lambda)be_1$$

$$=^{123} b\lambda e_1 = \widetilde{F}(b)\bullet\lambda e_m = \widetilde{F}(b)\bullet j(\lambda)\bullet e_m ,$$

d.h. beide Seiten haben dieselbe m-te Spalte.
2. Schritt: Im(j) liegt in $(\chi, b) = ({}_{z(b)}M_m(K))^G$.

---

[121] 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 $K\langle y\rangle$ 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.

[122] Auf beiden Seiten steht ein Vielfaches des (i+1)-ten Standard-Einheitsvektors.

[123] wegen $b \in k^*$ und $\sigma^m = e$.

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

$$a_\sigma \circ \sigma(X) = X.$$

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 $j(y) = \widetilde{F}(b)$.[124] 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,

$$j\otimes_k K\colon A\otimes_k K \longrightarrow (\chi, b)\otimes_k K =^{125} M_m(K)$$

ist surjektiv. Dies ist ein Homomorphismus von K-Algebren[126], 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.

---

[124] Man beachte, wegen $b \in k^*$ gilt $\sigma(\widetilde{F}(b)) = \widetilde{F}(b)$.

[125] Nach Definition von (χ, b) zerfällt die Algebra über K.

[126] Weil j ein Homomorphismus von k-Algebren ist.

$$D_n(K) \subseteq \mathrm{Im}(j\otimes K).$$

Insbesondere liegen die Elementarmatrizen

$$E_{ii} \in \mathrm{Im}(j\otimes K) \text{ für } i = 1, \dots, m$$

im Bild von $j\otimes K$. Wegen[127]

$$E_{uv} = \widetilde{F}(b)^{u-v}E_{vv} \text{ für } v < u$$

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.

1.4.20 Spezialfälle

(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[128]

$$\sigma: K \longrightarrow K, \ \sqrt[m]{a} \mapsto \omega\bullet\sqrt[m]{a},$$

in die Restklasse von 1 abbildet. Dann ist für jedes $b\in k^*$ die zyklische k-Algebra

$$(\chi, b)$$

(über k) isomorph zur k-Algebra

$$(a, b)_\omega = \langle x, y \rangle$$

mit den Erzeugern x und y und den Relationen

$$x^m = a, \ y^m = b, \ yx = \omega xy.$$

(ii) Seien k ein Körper der Charakteristik $p > 0$ und

$$K/k$$

---

[127] Es gilt

$$\widetilde{F}(b)e_i = e_{i+1} \text{ für } i \neq m$$

und

$$\widetilde{F}(b)e_m = be_1$$

[128] Jeder k-Automorphismus $K \longrightarrow K$ ist von der Gestalt

$$\sqrt[m]{a} \mapsto \omega^i\bullet\sqrt[m]{a}$$

mit $i = 0, 1, 2, \dots,$ denn die Nullstellen von X^m- en abgebildet 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.

die Galoiserweiterung des Grades p zum irreduziblen 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[129]

$$\sigma: K \longrightarrow K, \alpha \mapsto \alpha+1,$$

in die Restklasse von 1 abbildet. Dann ist für jedes $b \in k^*$ die zyklische k-Algebra

$$(\chi, b)$$

(über k) isomorph zur k-Algebra

$$[a, b) = < x, y >$$

mit den Erzeugern x und y und den Relationen

$$x^p = x - a, y^p = b, yx = (x+1)y,$$

Insbesondere sind $(a,b)_\omega$ und [a, b) zentrale einfache k-Algebren, die über K zerfallen. (vgl. [G & S], 2.5.5 unf 2.5.6).

Bemerkungen

(i) Im Fall m = 2 (also $\omega = -1$) erhält man gerade die Quaternionen-Algebren.

(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.

(iii) Bei Vorhandensein einer m-ten primitiven Einheitswurzel läßt sich jede zyklische Galois-Erweiterung des Grades m in der Gestalt

$$K = k(\sqrt[m]{a})$$

schreiben (Kummer-Theorie, vgl. [G & S] 4.3.9).

(iv) Analog wird (Artin-Schreier-Theorie, [G & S], 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.

1.4.21 Der Index einer zentralen einfachen Algebra[130]

Sei A eine zentrale einfache k-Algebra. Nach dem Satz von Wedderburn ist dann A isomorph zu einer Matrizen-Algebra über einer zentralen Divisionsalgebra D,

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

Dabei ist m eindeutig und D bis auf k-Isomorphie eindeutig bestimmt. Dann heißt die natürlichen Zahl

---

[129] 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 p, d.h. man erhält so sämtliche Nullstellen und deren Anzahl ist gleich p.

[130] Wir nehmen hier an, der Gruundkörper k ist unendlich. Später werden wir sehen, für endliche Körper k ist die Brauergruppe Br(k) trivial, so daß die hier beschriebenen Ergebnisse in diesem Fall trivialerweise gelten.

$$\mathrm{ind}_k(A) = \deg_k(D)\ (= \sqrt{\dim_k D}\ )$$

Index von A über k.

Bemerkungen

(i) A ist Divisionsalgebra $\Leftrightarrow \mathrm{ind}_k(A) = \deg_k(A)$.

(ii) $\mathrm{ind}_k A$ hängt nur von $[A] \in \mathrm{Br}(k)$.[131]

(iii) A zerfällt über k $\Leftrightarrow \mathrm{ind}_k A = 1$.

(iv) Zerfällungskriteriums für zentrale Divisionsalgebren.
Sei D eine zentrale Divisionsalgebra über k. Es gebe einen Zwischenkörper

$$k \subseteq K \subseteq D$$

mit

$$\mathrm{ind}(D) = [K: k].$$

Dann zerfällt D über K,

$$D \otimes_k K \cong M_m(K)$$

(mit $m = \deg_k(D)$).

(v) Jede zentrale einfache k-Algebra A zerfällt über einer separablen Körper-Erweiterung K/k des Grades $\mathrm{ind}_k A$ mit $K \subseteq A$.

Zum Beweis benötigen wir die Begriffe der reduzierten Norm und des reduzierten charakteristischen Polynoms (oder das nachfolgende klassische Ergebnis, welches wir hier ohne Beweis anführen).

Man beachte, ist A eine Divisionsalgebra, so ergibt sich aus der Wahl von K[132]

$$[K:k] = \mathrm{ind}_k A = \deg_k A = \dim_K A.$$

(vi) Sei D eine Divisionsalgebra über dem Körper k. Dann gibt es einen maximalen Teilkörper K von D,

---

[131] Nach dem Satz von Wedderburn sind Brauer-äquivalente Divisionsalgebren isomorph.

[132] Das erste Gleichheitszeichen gilt nach Wahl von K, das zweite, weil A eine Divisionsalgebra ist. Zum Beweis des dritten setzen wir

$$d := \deg_k A\ (= [K:k]).$$

Weil A über K zerfallen soll, können wir

$$A \otimes_k K = M_d(K)$$

schreiben. Es folgt

$$\dim_k A = \dim_K A \otimes_k K = \dim_K M_d(K) = d^2$$

also

$$\dim_K A = \dim_k A / [K:k] = d^2/d = d$$

$$k \subseteq K \subseteq D,$$

welcher separabel über k ist mit

$$[K:k] = \dim_K D = \deg_k D.$$

Beweise. Zu (iv). Sei D^{op} die zu D entgegengesetzte k-Algebra und analog sei

$$\mathrm{End}_k(D)^{op}$$

entgegengesetzt zu $\mathrm{End}_k(D)$. Dann besteht ein Isomorphismus[133]

$$\varphi: D \otimes_k D^{op} \xrightarrow{\cong} \mathrm{End}_k(D)^{op},\ d \otimes d' \mapsto \rho_d \circ \lambda_{d'},: x \mapsto d'xd, \qquad (1)$$

Wegen $K \subseteq D$ und K kommutativ, besteht auch eine Inklusion $K \subseteq D^{op}$. Durch Einschränken von (1) erhalten wir eine Inklusion

$$\iota: D \otimes_k K \longrightarrow \mathrm{End}_k(D)^{op}.$$

Aus der Abbildungsvorschrift (1) liest man ab, es gilt[134]

---

[133] φ ist wohldefiniert und k-linear, weil die Abbildung

$$D \times D^{op} \longrightarrow \mathrm{End}_k(D)^{op},\ (d, d') \mapsto \rho_d \circ \lambda_{d'}$$

bilinear über k ist. Es ist ein Homomorphismus von k-Algebren, weil für $d, d', \tilde{d}, \tilde{d}' \in D$ gilt

$$\begin{aligned}
&\varphi(d \otimes d' \bullet \tilde{d} \otimes \tilde{d}') \\
&\quad = \varphi((d \bullet \tilde{d}) \otimes (\tilde{d}' \bullet d')) \quad (\text{“}\bullet\text{” sei die Multiplikation in D}) \\
&\quad = \rho_{d\tilde{d}} \circ \lambda_{\tilde{d}', d'}, \quad (\text{Definition von } \lambda) \\
&\quad = \rho_{\tilde{d}} \circ \rho_d \circ \lambda_{\tilde{d}'} \circ \lambda_{d'}, \\
&\quad = \rho_{\tilde{d}} \circ \lambda_{\tilde{d}'} \circ \rho_d \circ \lambda_{d'}, \quad (\text{Links- und Rechtsmultiplikationen kommutieren}) \\
&\quad = \varphi(\tilde{d} \otimes \tilde{d}') \circ \varphi(d \otimes d') \\
&\quad = \varphi(d \otimes d') \bullet \varphi(\tilde{d} \otimes \tilde{d}') \quad (\text{“}\bullet\text{” sei die Multiplikation in } \mathrm{End}_k D)^{op})
\end{aligned}$$

Die Abbildung φ ist nicht identisch Null, ihr Kern ist somit ein echtes zweiseitiges Ideal von $D \otimes_k D^{op}$. Weil $D \otimes_k D^{op}$ eine zentrale einfache Algebra ist, ist dieses Ideal das Null-Ideal, d.h. φ ist injektiv. Weil Definitionsbereich und Wertevorrat von φ dieselbe Dimension

$$(\dim_k D)^2$$

über k haben, ist φ bijektiv.

[134] Für $d \in D, c, \lambda \in K, x \in D$ gilt

$$\begin{aligned}
\iota(d \otimes c)(\lambda x) &= c \bullet (\lambda x) \bullet d \\
&= (c\lambda) \bullet x \bullet d \\
&= (\lambda c) \bullet x \bullet d \quad (\text{K kommutativ}) \\
&= \lambda \bullet \iota(d \otimes c)(x)
\end{aligned}$$

$$\mathrm{Im}(\iota) \subseteq \mathrm{End}_K(D)^{op}.$$

Zum Beweis der Behauptung reicht es zu zeigen, es gilt sogar das Gleichheitszeichen, denn dann ist

$$\iota: D \otimes_k K \xrightarrow{\cong} \mathrm{End}_K(D)^{op} = M_n(K)^{op} \cong^{135} M_n(K)$$

Zum Beweis des Gleichheitszeichens reicht es zu beweisen, beide Algebren haben als Vektorräume über K dieselbe Dimension.
Zum Beweis idendifizieren wir den Ring der K-linearen Endomorphismen von D mit einem Matrizenring,

$$\mathrm{End}_K(D) = M_n(K).$$

Dabei ist

$$\begin{aligned} n &= \dim_K D && (2)\\ &= (\dim_k D)/[K:k] && \text{(Lagrange)}\\ &= (\deg_k D)^2/[K:k] && \text{(Definition von } \deg_k D)\\ &= (\mathrm{ind}_k D)^2/[K:k] && \text{(Bemerkung (i))}\\ &= \mathrm{ind}_k D && \text{(wegen } [K:k] = \mathrm{ind}_k D \text{ nach Voraussetzung)} \end{aligned}$$

Es folgt

$$\dim_K \mathrm{End}_K(D) = \dim_K M_n(K) = n^2$$

und

$$\begin{aligned} \dim_K D \otimes_k K &= \dim_k D\\ &= \dim_K D \bullet [K:k] && \text{(Lagrange)}\\ &= n \bullet [K:k] && \text{(nach (2))}\\ &= n \bullet \mathrm{ind}_k D && \text{(wegen } [K:k] = \mathrm{ind}_k D \text{ nach Voraussetzung)}\\ &= n^2 && \text{(siehe die Rechnung (2)).} \end{aligned}$$

Die beiden Dimensionen sind also tatsächlich gleich.

Zu (v). Die Behauptung ergibt sich wie folgt aus der nachfolgenden Bemerkung. Wir können annehmen, A ist eine Divisionsalgebra. Nach (vi) gibt es einen maximalen Teilkörper

$$k \subseteq K \subseteq A,$$

welcher separabel über k ist mit

$$\dim_k K = \dim_K A = \deg_k A = \mathrm{ind}_k A$$

---

[135] Ein Isomorphismus ist der Übergang zur transponierten Matrix.

Der Körper K genügt also den Bedingungen von (iv). Also zerfällt A über k.

Da wir die nachfolgende Bemerkung hier nicht beweisen werden, geben wir nachfolgend einen alternativen Beweis an (mit Hilfe des Begriffe der reduzierten Spur und des reduzierten charakteristischen Polynoms).

Zu (vi). Siehe [G & S], Anhang A3.12 und A3.7.

QED.

1.4.22 Reduzierte Norm und reduziertes Spur auf einer zentralen einfachen Algebra

Sei A eine zentrale einfache k-Algebra. Dann gibt es eine endliche Galois-Erweiterung K/k, über welcher A zerfällt, d.h. es gibt einen Isomorphismus von K-Algebren

$$\varphi\colon A\otimes_k K \xrightarrow{\cong} M_d(K).$$

Dieser Isomorphismus ist im allgemeinen nicht mit der Operation der Galois-Gruppe G := G(K/k) auf den beiden K-Algebren verträglich. Wir können jedoch die Operation von G auf der Matrizen-Algebra mit Hilfe des zu A gehörigen 1-Kozyklus

$$a\colon G \longrightarrow PGL(n,K)\ (= Aut_K(M_d(K)), \sigma \mapsto a_\sigma\ ,$$

so abändern, daß φ mit diesen Operationen verträglich wird. Genauer, sei ${}_aM_d(K)$ die Matrizen-Algebra $M_n(K)$ mit der Operation

$$G \times {}_aM_d(K) \longrightarrow {}_aM_d(K), (\sigma, M) \mapsto a_\sigma(M^\sigma),$$

dann ist φ ein Isomorphismus von K-Algebren mit G-Operation,

$$\varphi\colon A\otimes_k K \xrightarrow{\cong} {}_aM_d(K)$$

und induziert einen k-Isomorphismus der invarianten Teile,

$$A \cong ({}_aM_d(K))^G.$$

Die reduzierte Norm von A ist definiert als die Zusammensetzung

$$\mathrm{Nrd}\colon A \hookrightarrow A\otimes_k K \xrightarrow{\varphi^{-1}} {}_aM_d(K) \xrightarrow{\det} K.$$

$$a \mapsto a\otimes 1$$

der Inversen von φ mit der Determinate auf der Matrizen-Algebra. Analog ist die reduzierte Spur von A definiert als die Zusammensetzung

$$\mathrm{Trd}\colon A \hookrightarrow A\otimes_k K \xrightarrow{\varphi^{-1}} {}_aM_d(K) \xrightarrow{Tr} K.$$

mit der Spur auf der Matrizen-Algebra,

$$Tr((c_{ij})) := \sum_i c_{ii}\ .$$

Bemerkungen

(i) Die Werte der reduzierten Norm und reduzierten Spur liegen bereits im Grundkörper, d.h. diese sind Abbildungen

$$\mathrm{Nrd}\colon A \longrightarrow k \text{ bzw. } \mathrm{Trd}\colon A \longrightarrow k.$$

(ii) Reduzierte Norm und die reduzierte Spur hängen nicht von der speziellen Wahl des K-linearen Isomorphismus $\varphi\colon M_d(K) \longrightarrow A\otimes_k K$ ab.

(iii) Sei k ein unendlicher Körper. Fixiert man eine k-Vektorraum-Basis von A, d.h. eine k-lineare Bijektion,

$$\psi: k^{d^2} \xrightarrow{\cong} A,$$

so ist die reduzierte Norm durch ein Polynom des Grades d mit Koeffizienten aus k gegeben, d.h. es gibt ein Polynom

$$p \in k[x_1,\ldots,x_{d^2}]$$

des Grades d mit

$$p(v) = Nrd(\varphi(v))$$

für jedes $v \in k^{n^2}$.

(iv) Für jedes Element $a \in A$ der zentralen einfachen k-Algebra A sind äquivalent:

1. a ist Einheit von A.

2. $Nrd(a) \neq 0$.

Insbesondere ist A genau dann eine Divisions-Algebra, wenn Nrd außer der trivialen Nullstelle 0 keine weiteren Nullstellen besitzt.

Beweis. Wir beschränken uns auf die Aussagen bezüglich der reduzierten Norm. Die Aussagen zur reduzierten Spur werden analog bewiesen.

Zu (i). Wir betrachten die Abbildung

$$Nrd: A \hookrightarrow A\otimes_k K \xrightarrow{\psi} {}_aM_d(K) \xrightarrow{det} K.$$

Wie oben bemerkt ist der Isomorphismus $\psi := \varphi^{-1}$ eine G-äquivariante Abbildung (mit $G = G(K/k)$). Es reicht zu zeigen, daß dies auch für die Determinanten gilt, denn dann können wir zu den G-invarianten Teilen übergehen und erhalten eine Beschreibung von Nrd als Zusammensetzung

$$Nrd: A = (A\otimes_K K)^G \xrightarrow{\psi'} ({}_aM_d(K))^G \xrightarrow{det'} K^G = k.$$

Dabei bezeichne ψ' und det' die Einschränkung von ψ bzw. det auf die invarianten Teile. Beweisen wir also die G-Äquivarianz der Determinante, d.h.

$$det(a_\sigma(M^\sigma)) = \sigma(det(M)) \text{ für } \sigma\in G.$$

Dazu wählen wir einen Repräsentanten $b_\sigma \in GL(n, K)$ für den Automorphismus a_σ von $M_n(K)$, d.h.

$$a_\sigma(M) = b_\sigma M b_\sigma^{-1} \quad \text{(Matrizen-Multiplikation)}$$

für jedes $\sigma\in G$ und jede Matrix $M \in M_d(K)$. Es folgt

$$\begin{aligned} det(a_\sigma(M^\sigma)) &= det(b_\sigma M^\sigma b_\sigma^{-1}) \\ &= det(b_\sigma)\bullet det(M^\sigma)\bullet det(b_\sigma^{-1}) \\ &= det(M^\sigma) \\ &= \sigma(det(M)) \end{aligned}$$

wie behauptet.

Zu (ii). Sei ein weiterer Isomorphismus

$$\psi: M_d(K) \xrightarrow{\cong} A\otimes_k K.$$

gegeben und sei $b = \{b_\sigma\}$ der zugehörige 1-Kozyklus. Dann sind die beiden 1-Kozyklen a und b äquivalent, d.h. es gibt ein Element

$$c \in PGL(d,K) = Aut(M_d(K))$$

mit

$$b_\sigma = c^{-1}\circ a_\sigma\circ\sigma(c) \text{ für jedes } \sigma\in G,$$

d.h.

$$b_\sigma =^{136} c^{-1}\circ a_\sigma\circ\sigma\circ c\circ\sigma^{-1},$$

$$c\circ b_\sigma\circ\sigma = a_\sigma\circ\sigma\circ c.$$

Wir erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} M_d(K) & \xrightarrow{c} & M_d(K) \\ \downarrow{\scriptstyle b_\sigma\circ\sigma} & & \downarrow{\scriptstyle a_\sigma\circ\sigma} \\ M_d(K) & \xrightarrow{c} & M_d(K) \end{array}$$

für jedes $\sigma\in G$, d.h. der Automorphismus c ist ein äquivarianter Automorphismus

$$c: {}_bM_d(K) \longrightarrow {}_aM_d(K),$$

induziert also einen Isomorphismus

$$({}_bM_d(K))^G \xrightarrow{c} ({}_aM_d(K))^G$$

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

$$\begin{array}{ccccc} A & \overset{\varphi^{-1}}{\underset{\cong}{\rightrightarrows}} & ({}_aM_d(K))^G & & \\ \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle c} & \overset{\det}{\searrow} & K \\ A & \underset{\psi^{-1}}{\overset{\cong}{\rightarrow}} & ({}_bM_d(K))^G & \underset{\det}{\nearrow} & \end{array}$$

Man beachte, das Dreieck rechts ist kommutativ, weil c als Automorphismus von $M_d(K)$ ein innerer Automorphismus und die Determinante invariant bei inneren Automorphismen ist. Damit gilt für jedes $a \in A$:

$$\det(\varphi^{-1}(\alpha(a))) = \det(\psi^{-1}(a)).$$

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 $d: M_d(K) \longrightarrow M_d(K)$. Wir erhalten damit ein kommutatives Diagramm

$$\begin{array}{ccccc} A & \hookrightarrow & A\otimes_k K & \xrightarrow{\varphi^{-1}} & M_d(K) \\ \uparrow{\scriptstyle\alpha} & & \uparrow{\scriptstyle\alpha\otimes 1} & & \uparrow{\scriptstyle d} \\ A & \hookrightarrow & A\otimes_k K & \underset{\varphi^{-1}}{\longrightarrow} & M_d(K) \end{array} \qquad \begin{array}{c} \overset{\det}{\searrow} \\ K \\ \underset{\det}{\nearrow} \end{array}$$

[136] G operiert auf der Automorphismen-Gruppe durch “Konjugation”.

Man beachte, das Dreieck rechts ist kommutativ, weil d als Automorphismus von $M_n(K)$ ein innerer Automorphismus ist. Damit gilt

$$\det(\varphi^{-1}(\alpha(a))) = \det(\varphi^{-1}(a)).$$

Zu (iii). Sei $\varphi: M_d(K) \longrightarrow A \otimes_k K$ wie bisher ein K-linearer Isomorphismus und sei

$$\widetilde{\psi}: K^{d^2} \xrightarrow{\cong} A \otimes_k K$$

die K-lineare Fortsetzung von ψ. Dann ist die Zusammensetzung

$$K^{d^2} \xrightarrow{\widetilde{\psi}} A \otimes_k K \xrightarrow{\varphi^{-1}} M_d(K) \xrightarrow{\det} K$$

durch ein Polynom des Grades n mit Koeffizienten aus K gegeben[137]:

$$\mathrm{Nrd}(\widetilde{\psi}(v)) = p(v) \text{ für jedes } v \in K^{d^2}$$

mit einem Polynom

$$p \in K[x_1,...,x_{d^2}].$$

des Grades d. Wie wir gesehen haben, ist $\det \circ \varphi^{-1}$ eine G-äquivariante Abbildung. Dasselbe gilt für $\widetilde{\psi}$ (weil die Elemente von A invariant sind bei der Operation von G). Also gilt

$$p(\sigma \bullet v) = \sigma \bullet p(v) \text{ für jedes } v \in K^{d^2} \text{ und jedes } \sigma \in G,$$

d.h.

$$\begin{aligned} p(v) &= \sigma \bullet p(\sigma^{-1} v) \\ &= p^{\sigma}(\sigma \bullet \sigma^{-1} v) \\ &= p^{\sigma}(v). \end{aligned}$$

Dabei bezeichne p^{σ} das Polynom, welches man aus p durch Anwenden von σ auf alle Koeffizienten erhält. Da letztere Identität für alle v gilt und der Körper k unendlich ist, folgt

$$p = p^{\sigma},$$

d.h. die Koeffizienten von p sind invariant gegenüber der Operation der Gruppe G. Die Koeffizienten von p liegen somit in k,

$$p \in k[x_1,...,x_{d^2}].$$

Zu (iv). Wir identifizieren A mit der Teilmenge

$$A \subseteq M_d(K)$$

der G-invarianten Elemente bezüglich einer geeigneten Operation von G auf dem Matrizenring.

1. $\Rightarrow$ 2.. Sei a umkehrbar als Element von A. Dann ist a umkehrbar als Element der Matrizen-Algebra, also eine umkehrbare Matrix. Letztere hat eine von Null verschiedene Determinante,

$$\mathrm{Nrd}(a) = \det(a) \neq 0.$$

2. $\Rightarrow$ 1. Nach Voraussetzung gilt

---

[137] Die Determinate ist ein ganzzahliges Polynom des Grades n in den Einträgen der Matrix. Man erhält p durch Zusammensetzen mit der K-linearen Abbildung $\varphi^{-1} \circ \widetilde{\psi}$.

$$0 \neq \mathrm{Nrd}(a) = \det(a),$$

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.

$$b \in M_d(K)^G = A,$$

d.h, das Element a besitzt ein Inverses b in A.
QED.

1.4.23 Separabilität eines charakteristischen Polynoms

Seien k ein unendlicher Körper und A eine zentrale einfache k-Algebra. Dann gibt es ein Element

$$a \in A$$

derart, daß das charakteristische Polynom

$$P_a(T) = \mathrm{Nrd}(T \bullet 1 - a)$$

von a keine mehrfachen Nullstellen besitzt.
Beweis. Bezeichne

$$\overline{k}$$

eine algebraische Abschließung von k und

$$k^s \subseteq \overline{k}$$

die zugehörige separable Abschließung. Wir fixieren einen Isomorphismus von $\overline{k}$-Algebren

$$\varphi: M_d(\overline{k}) \longrightarrow A \otimes_k \overline{k} \ (\hookleftarrow A)$$

und betrachten $\varphi^{-1}(A)$ als k-linearen Unterraum des $\overline{k}$-Vektorraums $M_d(\overline{k})$,

$$\begin{array}{ccc} \varphi^{-1}(A) & \subseteq & M_d(\overline{k}) \\ || & & || \\ k^{d^2} & & \overline{k}^{d^2} \end{array}$$

der eine Basis des $\overline{k}$-Vektorraums enthält. Das charakteristische Polynom $P_a(T)$ entsteht dann durch Verpflanzen entlang φ und Einschränken auf A aus dem Polynom

$$\widetilde{P}_a(T) := \det(T \bullet 1 - a),\ a \in M_d(\overline{k}).$$

Betrachten wir die Diskriminante[138] von $\widetilde{P}_a$,

$$\widetilde{D}(a) = \mathrm{Res}(\widetilde{P}_a, \widetilde{P}'_a)$$

---

[138] d.h. die Resultante des Polynoms und dessen Ableitung.

Weil $\widetilde{P}_a$ ein ganzzahliges Polynom in T und den Einträgen der Matrix a ist, ist $\widetilde{D}(a)$ ein ganzzahliges Polynom in den Einträgen der Matrix a. Dabei gilt

$$\widetilde{D}(a) = 0 \Leftrightarrow \widetilde{P}_a \text{ hat mehrfache Nullstellen} \Leftrightarrow a \text{ hat mehrfache Eigenwerte.}$$

Setzt man also für a eine Matrix mit paarweise verschiedenen Eigenwerten ein, so erhät man einen von Null verschiedenen Wert,

$$\widetilde{D}(a) \neq 0 \text{ für ein } a \in M_d(\overline{k}).$$

Das Polynom $\widetilde{D}$ ist somit nicht das Nullpolynom. Dasselbe gilt für die Verpflanzung von $\widetilde{D}$ entlang des Isomorphismus φ.

$$D(a) := \widetilde{D}(\varphi^{-1}(a))$$

ist ein vom Nullpolynom verschiedenes Polynom mit Koeffizienten aus $\overline{k}$ bezüglich einer beliebigen Basis des $\overline{k}$-Vektorraums $A \otimes_k \overline{k} = \overline{k}^{d^2}$. Auf Grund von Bemerkung 1.4.22 (iii) wissen wir sogar, daß wir ein Polynom mit Koeffizienten aus k erhalten, wenn wir die Basiselemente so wählen, daß sie im Unterraum $A = k^{d^2}$ liegen. Weil k ein unendlicher Körper ist, gibt es ein

$$a \in A$$

derart, daß

$$D(a) := \widetilde{D}(\varphi^{-1}(a)) \neq 0$$

ungleich Null ist[139]. Dann hat aber das Polynom

$$P_a(T) = \widetilde{P}_{\varphi^{-1}(a)}(T) = \det(T \bullet 1 - \varphi^{-1}(a))$$

keine mehrfachen Nullstellen.
QED.

1.4.24 Existenz eines separablen Zerfällungskörpers dessen Grad gleich dem Index ist

Seien k ein unendlicher Körper und A eine zentrale einfache k-Algebra. Dann gibt es einen Teilkörper K von A,

$$k \subseteq K \subseteq A$$

mit

1. A zerfällt über K, d.h. $A \otimes_k K \cong M_d(K)$ für eine natürliche Zahl d.
2. $[K:k] = \text{ind}_k A$.

Beweis. Nach dem Satz von Wedderburn ist A eine Matrizen-Algebra über einer Divisionsalgebra D,

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

---

[139] Für Polynome in einer Unbestimmten ist das klar, weil sie nur endlich viele Nullstellen besitzen. Polynome in zwei Unbestimmten betrachtet man als Polynome in einer Unbestimmten, deren Koeffizienten Polynome sind, und wählt zunächst ein Element aus k, für welches ein Koeffizent ungleich Null ist, usw.

Es reicht zu zeigen, D zerfällt über einem Teilkörper $K \subseteq D$ des Grades

$$\mathrm{ind}_k A = \deg_k D.$$

Wir können also annehmen,

$$A = D$$

ist eine zentrale Divisionsalgebra über k. Weil k unendlich ist, gibt es nach 1.4.23 ein Element

$$a \in A = D$$

derart, daß

$$P_a(T) = \mathrm{Nrd}(T \bullet 1 - a) \in [140]\ k[T]$$

keine mehrfache Nullstellen besitzt.

Bezeichne $\overline{k}$ eine algebraische Abschließung von k. Unter Verwendung eines Isomorphismus von $\overline{k}$-Algebren

$$\varphi: M_d(\overline{k}) \longrightarrow A \otimes_k \overline{k}\ (\hookleftarrow A)\ , d = \deg A$$

können wir A mit einer k-Teilalgebra der Matrizen-Algebra identifizieren,

$$A \hookrightarrow M_d(\overline{k}).$$

Das Polynom

$$P_a(T) \in k[T]$$

wird dann gerade das characteristische Polynom der Matrix a. Nach dem Satz von Hamilton-Cayley ist a Nullstelle von P_a. Weil nach Konstruktion P_a keine mehrfachen Nullstellen besitzt (in $\overline{k}$) ist P_a gerade das Minimalpolynom von $a \in M_d(\overline{k})$, d.h. jedes Polynom mit Koeffizienten aus $\overline{k}$ und der Nullstelle $a \in M_d(\overline{k})$ ist in $\overline{k}[T]$ ein Vielfaches von P_a.[141] Man beachte, das bedeutet nicht, daß P_a irreduzibel ist (denn die Matrizen-Algebra kann Nullteiler besitzen).Wegen $a \in D$ gilt

---

[140] Man schreibe die Elemente 1 und a von A als k-Linearkombination einer Basis des k-Vektorraums A und wende Bemerkung 1.4.22(iii) an.

[141] Bezeichne $f(T) \in \overline{k}[T]$ ein Polynom mit der Nullstelle $a \in M_n(\overline{k})$. Ist λ ein Eigenwert von a und $v \in \overline{k}^n$ ein Eigenvektor zum Eigenwert λ, so ist der Unterraum

$$\overline{k} \bullet v$$

$$k[a] \subseteq D,$$

und P_a ist auch das Minimal-Polynom von $a \in k[a]$ über k. Nun ist

$$K = k[a] \subseteq D$$

eine nullteilerfreie k-Algebra die als k-Vektorraum endlich-dimensional ist, also ein Körper.[142] Sein Grad über k ist gleich

$$[K:k] = \deg P_a = d = \deg_k A =^{143} \operatorname{ind}_k D$$

Die Erweiterung ist separabel, weil P_a keine mehrfachen Nullstellen besitzt. Nach dem Zerfällungskriterium von Bemerkung 1.4.21 (iv) zerfällt A = D über dem Körper K. **QED**.

1.4.25 Alternative Beschreibungen des Index

Seien k ein Körper und A eine zentrale einfache k-Algebra. Dann gilt

(i)
$$\operatorname{ind}_k(A) = \text{ggT}\{ [K:k] \mid K/k \text{ endlich separabel, A zerfällt über K}\}$$

d.h. der Index ist der größte gemeinsame Teiler der Grade endlicher separabler Körpererweiterungen K/k, für welche A zerfällt über K.

(ii)
$$\operatorname{ind}(A) = \min \{[K:k] \mid K/k \text{ endliche separabel, A zerfällt über K}\}$$

d.h. der Index ist der kleinste Grad einer endlichen separablen Körpererweiterung von k , über welcher A zerfällt.

Beweis. siehe [G & S], 4.5.10 und 4.5.11.

1.4.26 Der Index von Algebren die in Br(k) dieselbe Untergruppe erzeugen

Seien A und B zentrale einfache Algebren über dem Körper k, welche in Br(k) dieselbe Untergruppe erzeugen. Dann gilt

$$\operatorname{ind}_k A = \operatorname{ind}_k B.$$

Beweis. Bezeichnen wir mi "$\sim$" die Brauer-Äquivalenz. Nach Voraussetzung gibt es eine natürliche Zahlen m mit

$$A^{\otimes m} \sim B,$$

d.h. die beiden Algebren besitzen isomorphe Matrizen-Algebren,

(1) $$M_a(A^{\otimes m}) \cong M_b(B)$$

für geeignet gewählte natürliche Zahlen a und b.

---

invariant bezüglich der "Multiplikation" mit a. Wegen f(a) = 0 ist die Einschränkung von f(a) auf diesen Unterraum die Nullabbildung, d.h.

$$0 = f(a)v = f(\lambda \bullet \mathrm{Id})v = f(\lambda)v,$$

d.h. $f(\lambda) = 0$. Jeder Eigenwert ist eine Nullstelle von f. Weil P_a keine mehrfachen Nullstellen besitzt folgt $P_a \mid f$.

[142] Als Minimalpolynom eines Erzeugers einer endlichen Körper-Erweiterung ist P_a damit irreduzibel.

[143] A = D ist eine Divisionsalgebra über k.

Nach 1.4.21 (v) gibt es eine separable Körper-Erweiterung K/k derart, daß

$$[K:k] = \mathrm{ind}_k A$$

ist und A über K zerfällt, d.h. A ist isomorph zu einer Matrizen-Algebra über K. Dann gilt aber letzteres auch für $A^{\otimes m}$ und wegen (1) auch für $M_b(B)$. Nach Bemerkung 1.4.21(iii) ist damit

$$\begin{aligned} 1 &= \mathrm{ind}_K M_b(B\otimes_k K) \\ &= \mathrm{ind}_K B\otimes_k K, \qquad \text{(vgl. 1.4.21 (i))} \end{aligned}$$

d.h. B zerfällt über K Auf Grund der Beschreibung des Index als ggT in 1.4.25 folgt $\mathrm{ind}_k B \le [K:k] = \mathrm{ind}_k A$.

Aus Symmetrie-Gründen besteht auch die umgekehrte Ungleichung.
QED.

1.4.27 Teilbarkeitsrelationen

Seien k ein unendlicher Körper, K/k eine endliche separable Körper-Erweiterung und A eine zentrale einfache k-Algebra. Dann gilt

$$\mathrm{ind}_K A\otimes_k K \mid \mathrm{ind}_k(A) \mid [K:k]\bullet\mathrm{ind}_K(A\otimes_k K).$$

Beweis. Die linke Teilbarkeit folgt aus der Charakterisierung des Index als größten gemeinsamen Teiler in 1.4.25.[144] Zum Beweis der rechten wählen wir eine endliche separable Körper-Erweiterung K'/K mit

$$[K':K] = \mathrm{ind}_K A\otimes_k K,$$

über welcher $A\otimes_k K$ zerfällt. Eine solche existiert nach Bemerkung 1.4.21 (v). Dann ist aber K' auch ein Zerfällungskörper für A. Die Charakterisierung des Index als größten gemeinsamen Teiler in 1.4.25 liefert

$$\mathrm{ind}_k A \mid [K':k] = [K:k]\bullet[K':K] = [K:k]\bullet\mathrm{ind}_K A\otimes_k K$$

QED.

1.4.28 Erweiterungen mit einem zum Index teilerfremden Grad

Seien k ein unendlicher Körpr, K/k eine endliche separable Körper-Erweiterung und A eine zentrale einfache k-Algebra mit

$$\mathrm{ind}_k A \text{ teilerfremd zu } [K:k].$$

Dann gilt

$$\mathrm{ind}_k A = \mathrm{ind}_K(A\otimes_k K).$$

Insbesondere ist $A\otimes_k K$ eine Divisionsalgebra, falls A eine ist.

Beweis. In der zweiten Teilbarkeitsbeziehung von 1.4.27 kann man den Faktor [K:k] auf der rechten Seite weglassen (wegen der Teilerfremdheit). Es gilt also

$$\mathrm{ind}_k A = \mathrm{ind}_K(A\otimes_k K).$$

Ist A eine Divisionsalgebra, so gilt damit

$$\begin{aligned} \mathrm{ind}_K(A\otimes_k K) &= \mathrm{ind}_k A \\ &= \deg A \qquad \text{(weil A Divisionsalgebra ist)} \\ &= \deg_K (A\otimes_k K). \end{aligned}$$

Also ist auch $A\otimes_k K$ eine Divisionsalgebra (über K).

---

[144] Jeder Körper-Erweiterung, über welcher A zerfällt, ist auch eine Erweiterung, über welcher $A\otimes_k K$ zerfällt.

QED.

1.4.29 Die Periode einer zentralen einfachen Algebra

Die Periode oder auch der Exponent einer zentralen einfachen Algebra A über dem Körper k ist definiert als die Ordnung der zugehörigen Brauer-Klasse

$$[A] \in Br(k).$$

Sie wird mit

$$per(A) := ord\ [A]$$

bezeichnet.

1.4.30 Die Teiler von Index und Periode

Seien k ein (unendlicher) Körper und A eine zentrale einfache k-Algebra. Dann gilt:

(i) $per(A) \mid ind_k(A)$.

(ii) In den Primfaktorzerlegungen von per(A) und $ind_k(A)$ kommen dieselben Primzahlen vor.

Zum Beweis von (ii) benötigen wir die folgende Aussage.

Lemma

Seien A eine zentrale einfache k-Algebra und p eine Primzahl welche die Periode von A nicht teilt. Dann zerfällt A über einer endlichen separablen Körper-Erweiterung K/k mit einem zu p teilerfremden Grad.

Beweis des Lemmas. Sei L/k eine endliche Galois-Erweiterung mit der Eigenschaft, daß Br(L/k) die Klasse der Algebra A enthält[145],

$$[A] \in Br(L/k).$$

Bezeichne weiter

$$P \subseteq G(L/k)$$

eine p-Sylow-Untergruppe und

$$K := L^P,$$

deren Fixkörper. Nach dem Hauptsatz der Galois-Theorie ist dann

$$G(L/K) = P,$$

und wir erhalten

$$Br(L/K) \cong H^2(G(L/K), L^\times) = H^2(P, L^\times).$$

Weil die Ordnung von P nach Konstruktion eine Potenz von p ist, ist diese Brauer-Gruppe eine p-Torsions-Gruppe. Die Ordnung des Bildes von [A] bei der Restriktionsabbildung

$$Res: Br(L/k) \longrightarrow Br(L/K),\ A \mapsto A \otimes_k K,$$

muß also eine p-Potenz sein. Nach Voraussetzung soll aber per(A) teilerfremd zu p sein. Das Bild von [A] bei der Restriktion ist also trivial. Mit anderen Worten, A zerfällt über K. Nach Konstruktion ist der Grad

$$[K:k] = [L:k]/[L:K] = \#Gal(L/k)/\#Gal(L/K) = \#Gal(L/k)/\#P$$

teilerfremd zu p.

QED (Lemma).

Beweis des Satzes.

Zu (i). Nach 1.4.21(v) gibt es eine separable Körper-Erweiterung K/k des Grades

$$[K:k] = ind_k\ A,$$

---

[145] z.B. kann man für L einen Zerfällungskörper von A wählen.

sodaß A über K zerfällt, d.h. [A]∈Br(k) liegt im Kern der Restriktionsabbildung

$$\text{Res: } Br(k) \longrightarrow Br(K);\ A \mapsto A \otimes_k K$$

Wir setzen diese Abbildung mit der Korestriktion Cor: Br(K) ⟶ Br(k) zusammen und sehen so, daß [A] annulliert wird bei der Multiplikation mit dem Index

$$n = (G(k_s/k):G(k_s/K)) =^{146} [K:k] =^{147} \text{ind}_k A$$

d.h.

$$n \bullet [A] = 0.$$

Die Ordnung von [A] ist also ein Teiler von n, d.h. es gilt die Aussage von (i).
Zu (ii). Sei p eine Primzahl, welche teilerfremd zu per(A) ist. Nach dem Lemma gibt es einen separablen Zerfällungskörper K von A (über k) mit

$$[K:k] \text{ teilerfremd zu } p.$$

Auf Grund der Charakterisierung von $\text{ind}_k A$ als größten gemeinsamen Teiler (vgl. 4.5.10) ist damit

$$\text{ind}_k A \text{ teilerfremd zu } p.$$

Zusammen mit der Aussage von (i), per(A) | $\text{ind}_k A$, liefert dies die Behauptung von (ii).

QED.

1.4.31 Dekompositionssatz von Brauer

Seien k ein Körper und D eine zentrale Divisionsalgebra über k, deren Index die Primfaktorzerlegung

$$\text{ind}_k(D) = p_1^{m_1} \bullet \ldots \bullet p_r^{m_r}$$

besitzt. Dann gibt es bis auf Isomorphie eindeutig bestimmte zentrale Divisionsalgebren $D_1,\ldots,D_r$ über k mit

$$\text{ind}_k D_i = p_i^{m_i} \text{ für } i = 1, \ldots, r$$

und

$$D = D_1 \otimes_k \ldots \otimes_k D_r.$$

Beweis. Die Brauer-Gruppe ist eine Torsionsgruppe. Sie zerfällt deshalb in eine direkte Summe ihrer p-primären Torsionsuntergruppen,[148]

---

[146] Sei L/k eine Galois-Erweiterung, welche den Körper K enthält. Dann gilt

$$G(k_s/L)) = \text{Ker}(G(k_s/k) \longrightarrow G(L/k), \sigma \mapsto \sigma|_L)$$

$$G(k_s/L)) = \text{Ker}(G(k_s/K) \longrightarrow G(L/K), \sigma \mapsto \sigma|_L)$$

also

$$[L:k] = \#\, G(L/k) = \#\, G(k_s/k)/G(k_s/L))$$

$$[L:K] = \#\, G(L/K) = \#\, G(k_s/K)/G(k_s/L))$$

und damit

$$[K:k] = [L:k]/[L:K] = \#(G(k_s/k)/G(k_s/K)) = n$$

[147] nach Wahl von K.

[148] Sei $x \in Br(k)$ ein Element der Ordung $n = p_1^{m_1} \bullet \ldots \bullet p_r^{m_r}$. Wir definieren

$$a_i$$

$$Br(k) = \oplus_{p \text{ Primzahl}} Br(k)(p).$$

Die Klasse von D läßt sich entsprechend als Summe

(1) $$[D] = [D_1]+...+[D_r] \ (= [D_1 \otimes_k ... \otimes_k D_r])$$

schreiben mit Divisionsalgebren D_i , deren Klassen $[D_i] \in Br(k)(p_i)$ eine Ordnung besitzen, welche gleich einer Potenz einer Primzahl p_i ist. Das Tensorprodukt

$$A := D_1 \otimes_k ... \otimes_k D_r$$

hat den Grad

$$\deg_k A = \prod_{i=1}^{r} \text{ind}_k(D_i)$$

und den Index

(2) $$\text{ind}_k(A) = \deg_k(D)$$

(da letzterer für Brauer-äquivalente Algebren derselbe ist)[149]. Insbesondere ist der Index von D,

(3) $$\text{ind}_k(D) \mid \prod_{i=1}^{r} \text{ind}_k(D_i)$$

ein Teiler des Produkts der Indizes der D_i.

Nach 1.4.5.22(v) zerfällt jede zentrale einfache k-Algebra über einer separablen Erweiterung, deren Grad gleich dem Index der Algebra ist. Durch wiederholtes Anwenden dieser Tatsache finden wir für jedes i eine endliche separable Erweiterung

---

als das Produkt aller $p_j^{m_j}$ mit $j \neq i$. Dann ist $a_i x$ ein Element der Ordnung $p_i^{m_i}$,

$$\text{ord}(a_i x) = p_i^{m_i}.$$

Weiter sind die a_i teilerfremd, d.h. es gilt

$$1 = \sum_{i=1}^{r} a'_i a_i \text{ für geeignete } a'_i \in \mathbb{Z},$$

d.h.

$$x = \sum_{i=1}^{r} a'_i a_i x$$

und der i-te Summand hat als Ordnung eine Potenz von p_i. Wir haben noch die Eindeutigkeit der Zerlegung zu beweisen. Angenommen die Zerlegung wäre nicht eindeutig. Dann gäbe es eine nicht-triviale Zerlegung der Null,

(*) $$0 = x_1+...+x_r \text{ mit } \text{ord}(x_i) = p_i^{m_i}.$$

Weil a_i teilerfremd zu p_i ist, ist die Multiplikation mit a_i auf den Elementen von p_i-Potenzordnung injektiv. Es reicht also zu zeigen,

$$a_i x_i = 0 \text{ für jedes i.}$$

Bei Multiplikation von (*) mit a_i werden aber alle Summanden der rechten Seite von (*) annulliert (mit eventueller Ausnahme des i-ten Summanden).

[149] beide sind Brauer-äquivalent zum Tensorprodukt der D_i.

$$K_i/k \text{ mit } [K_i:k] \text{ teilerfremd zu } p_i$$

über welcher alle D_j mit $j \neq i$ zerfallen.[150] Wegen (1) haben dann aber

$$D \otimes_k K_i \text{ und } D_i \otimes K_i$$

dieselbe Klasse in $Br(K_i)$. Insbesondere gilt

$$ind_{K_i}(D_i \otimes K_i) = ind_{K_i}(D \otimes_k K_i) \mid ind_k(D).$$

(nach 1.4.27). Die Algebren $D_i \otimes K_i$ sind nach wie vor Divisionsalgebren über K_i vom Index $ind_k D_i = p_i$-Potenz (weil der Grad von $[K_i:k]$ teilerfremd zu diesem Index ist, vgl. 1.4.28), d.h.

$$ind_k(D_i) \mid ind_k(D).$$

Zusammen mit (3) erhalten wir damit

$$(4) \qquad ind_k(D) = \prod_{i=1}^{r} ind_k(D_i) =^{151} ind_k A.$$

Die Algebren D und A haben dieselbe Brauer-Klasse (nach (1)). Außerdem gilt

$$\begin{aligned} ind_k A &= \prod_{i=1}^{r} ind_k(D_i) && \text{(nach (4))} \\ &= \prod_{i=1}^{r} deg_k(D_i) && \text{(die } D_i \text{ sind Divisionsalgebren)} \\ &= deg_k A && \text{(nach Definition von A)} \end{aligned}$$

Insbesondere ist auch A eine Divisionsalgebra. Als Brauer-äquivalente Divisisonsalgebren sind D und A aber isomorph,

$$D \cong A,$$

d.h. es existiert die behauptete Zerlegung.

Umgekehrt erhält man aus einer Zerlegung der behaupteten Art eine Summen-Zerlegung (1). Aus deren Eindeutigkeit folgt dann aber die Eindeutigkeit der D_i bis auf Isomorphie (weil es nach Wedderburn in jeder Brauerklasse genau eine Divisionsalgbra gibt bis auf Isomorphie).
QED.

Bemerkung

Der Gegenstand dieser Vorlesung ist eine Präzisierung des Satzes von Brauer, nämlich der folgende Satz von Merkurjev-Suslin.

1.4.32 Satz 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.

Bemerkung

---

[150] Nach Wahl von D_j hat D_j als Periode eine Potenz von p_j. Dasselbe gilt dann aber auch für den Index (nach 1.4.30).

[151] Wegen (2) ist ind A = deg D = ind D.

Die nachfolgende Konsequenz des Satzes von Merkurjev-Suslin scheint keinen elementaren Beweis zu besitzen.

1.4.33 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.

Unser nächstes Ziel ist die Definition und die Untersuchung des Galois-Symbols. Das Galois-Symbol ist eine Abbildung den Milnor-K-Gruppen mit Werten in einer Galois-Kohomologie-Gruppen. Wir erinnern zunächst an die Milnor-K-Gruppen.

1.4.34 Die K-Gruppe von Milnor des Körpers k

Seien k ein Körper und n > 1 eine natürliche Zahl. Die n-te K-Gruppe von Milnor des Körpers k,

$$K_n^M(k),$$

ist definiert als die Faktorgruppe des n-fachen Tensorprodukts

$$k^\times \otimes_{\mathbb{Z}} ... \otimes_{\mathbb{Z}} k^\times$$

nach der Untergruppe, die von allen Elementen

$$a_1 \otimes ... \otimes a_n$$

erzeugt wird, für welche es Indizes i und j gibt mit

$$a_i + a_j = 1.$$

Für $a_1,...,a_n \in k^\times$ bezeichnen wir die Restklasse des Elements $a_1 \otimes ... \otimes a_n$ in der n-ten K-Gruppe mit

$$\{a_1,...,a_n\} \ (\in K_n^M(k)\ ).$$

Die Elemente dieser Gestalt werden wir Symbole nennen.
Wir setzen außerdem

$$K_0^M(k) = \mathbb{Z} \text{ und } K_1^M(k) = k^\times$$

und nennen diese Gruppen auch 0-te bzw. 1-te Milnor-K-Gruppe.

1.4.35 Konstruktion: die Kummer-Abbildung

Seien k ein Körper und m eine natürliche Zahl welche teilerfremd zur Charakteristik von k ist,

$$ggT(m, char(k)) = 1.$$

Das Cup-Produkt definiert dann eine Abbildung

$$H^1(k, \mu_m)) \otimes ... \otimes H^1(k, \mu_m)) \longrightarrow H^n(k, \mu_m^{\otimes n}),\ c_1 \otimes ... \otimes c_n \mapsto c_1 \cup ... \cup c_n$$

des n-fachen Tensorprodukts von $H^1(k, \mu_m))$ über $\mathbb{Z}$ mit Werten in der n-ten Galois-Kohomologie von k. Die Gruppe $G(k^s/k)$ operiert dabei auf $\mu_m^{\otimes n}$ vermittels

$$\sigma(x_1 \otimes ... \otimes x_n) = \sigma(x_1) \otimes ... \otimes \sigma(x_n) \text{ für } \sigma \in G(k_s/k) \text{ und } x_i \in \mu_m.$$

Aus der exakten Kummer-Sequenz

$$1 \longrightarrow \mu_m \longrightarrow k^{s\times} \xrightarrow{m} k^{s\times} \longrightarrow 1$$

erhalten wir durch Übergang zur Kohomologie bezüglich $G(k^s/k)$ und auf Grund des Satzes 90 von Hilbert

$$H^1(k, \mu_m)) \cong k^\times/(k^\times)^m,$$

d.h. es besteht eine Surjektion

$$\partial: k^\times \twoheadrightarrow H^1(k, \mu_m))$$

mit dem Kern $(k^\times)^m$, welche wir im folgenden Kummer-Abbildung nennen wollen. Durch Zusammensetzen dieser Surjektion mit dem Cup-Produkt erhalten wir eine Abbildung

$$\partial^n: k^\times \otimes_{\mathbb{Z}} ... \otimes_{\mathbb{Z}} k^\times \longrightarrow H^n(k, \mu_m^{\otimes n}),\ c_1 \otimes ... \otimes c_n \mapsto \partial(c_1) \cup ... \cup \partial(c_n).$$

Bemerkung
Unser nächstes Ziel ist es zu zeigen, diese Abbildung faktorisiert sich über die n-te K-Gruppe von Milnor. Die auf der Milnor-Gruppe induzierte Abbildung wird dann das zu konstruierende Galois-Symbol sein.

1.4.36 Einige Elemente aus dem Kern von ∂^n

Seien k ein Körper, m eine zur Charakteristik von k teilerfremde natürliche Zahl und

$$a_1, ..., a_n \in k^\times$$

Elemente mit der Eigenschaft, daß es Indizes i,j,

$$1 \le i \le j \le n$$

gibt für welche

$$a_i + a_j = 1$$

ist. Dann gilt

$$\partial^n(a_1 \otimes ... \otimes a_n) = 0,$$

wenn ∂^n die in 1.4.30 konstruierte Abbildung bezeichnet.

Zum Beweis benötigen wir die folgende Aussage.

Lemma (Zwei kommutative Diagramme)
Sei K/k eine endliche separable Körper-Erweiterung. Dann sind die folgenden beiden Diagramme kommutativ.

$$\begin{array}{ccc} k^\times & \xrightarrow{\partial_k} & H^1(k,\mu_m) \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle Res} \\ K^\times & \xrightarrow{\partial_K} & H^1(K,\mu_m) \end{array} \qquad \begin{array}{ccc} K^\times & \xrightarrow{\partial_K} & H^1(K,\mu_m) \\ {\scriptstyle N_{K/k}}\downarrow & & \downarrow{\scriptstyle Cor} \\ k^\times & \xrightarrow{\partial_k} & H^1(k,\mu_m) \end{array}$$

Dabei bezeichne i: $k^\times \longrightarrow K^\times$ die natürliche Einbettung.

Beweis des Lemmas. Im Kontext der Definitonen von Restriktion und Korestriktion haben wir gesehen, daß diese Abbildungen mit den Zusammenhangshomomorphismen zu exakten Sequenzen der Koeffizienten-Gruppen kommutieren. Das gilt insbesondere für die kurze exakte (Kummer-) Sequenz

$$1 \longrightarrow \mu_m \longrightarrow k_s^\times \xrightarrow{m} k_s^\times \longrightarrow 1.$$

Mit anderen Worten, man erhält kommutative Diagramme, wenn man die linken vertikalen Abbildungen i bzw. $N_{K/k}$ durch die Abbildungen

$$\begin{array}{ccc} H^0(k, k_s^\times) & \xrightarrow{Res} & H^0(K, k_s^\times) \\ \| & & \| \\ k^\times & & K^\times \end{array} \quad \text{und} \quad \begin{array}{ccc} H^0(K, k_s^\times) & \xrightarrow{Cor} & H^0(k, k_s^\times) \\ \| & & \| \\ K^\times & & k^\times \end{array} .$$

ersetzt. Nun ist aber Res fur die 0-te Kohomologie gerade die natürliche Einbettung i, d.h. das linke Diagramm ist tatsächlich kommutativ. Die Korestriktion wird mit Hilfe eines Repräsentantensystems

$$\sigma_1,\ldots,\sigma_n \in G(k_s/k)$$

der Restklassen modulo $G(k_s/K)$ definiert. Für die 0-te Kohomologie ist sie gerade durch die Abbildungsvorschrift

$$\Phi \mapsto \sum_{j=1}^{n} \sigma_j \bullet \Phi(\sigma_j^{-1} 1) = \sum_{j=1}^{n} \sigma_j \bullet \Phi$$

gegeben (wenn der Koeffizienten-Modul A eine additive Gruppe ist). Speziell für die multiplikative Gruppe $A = K^\times$ erhält man gerade die Norm-Abbildung.
QED (Lemma).

Beweis des Satzes. Auf Grund der Superkommutativität des Cup-Produkts können wir annehmen, es gilt

$$i = 1 \text{ und } j = 2.$$

Auf Grund der Assoziativität des Cup-Produkts können wir annehmen

$$n = 2,$$

d.h. es reicht zu zeigen, für jedes $a \in k^\times$ ist

$$\partial^2(a \otimes (1-a)) = \partial(a) \bigcup \partial(1-a)$$

die triviale Kohomologie-Klasse.
Zum Beweis betrachten wir die Zerlegung

$$x^m - a = \prod_{\ell=1}^{s} f_\ell \in k[x]$$

des Polynoms x^m-a in irreduzible Faktoren $f_\ell \in k[x]$. Für jedes ℓ fixieren wir eine Nullstelle α_ℓ in k^s ,

$$f_\ell(\alpha_\ell) = 0, \alpha_\ell \in k^s ,$$

und setzen

$$K_\ell := k(\alpha_\ell).$$

Wir erhalten

$$1 - a = \prod_{\ell=1}^{s} f_\ell(1) =^{152} \prod_{\ell=1}^{s} N_{K_\ell/k}(1-\alpha_\ell).$$

Weil die Kummer-Abbildung ∂ ein Gruppen-Homomorphismus ist, folgt

$$\partial^2(a\otimes(1-a)) = \partial(a)\bigcup \sum_{\ell=1}^{s} \partial(N_{K_\ell/k}(1-\alpha_\ell)).$$

Auf Grund des zweiten kommutativen Diagramms des Lemmas können wir den Ausdruck rechts auch schreiben als

$$\partial^2(a\otimes(1-a)) = \partial(a)\bigcup \sum_{\ell=1}^{s} \mathrm{Cor}_k^{K_\ell}\partial(1-\alpha_\ell) = \sum_{\ell=1}^{s} \mathrm{Cor}_k^{K_\ell}(\mathrm{Res}_k^{K_\ell}\, \partial(a) \bigcup \partial(1-\alpha_\ell)).$$

Das Gleichheitszeichen rechts kommt von der Projektionsformel für das Cup-Produkt. Zum Beweis der Behauptung reicht es zu zeigen, das Bild von a beim Zusammenhangshomomorphismus

$$\partial: K_\ell^\times \longrightarrow H^1(K_\ell, \mu_m)$$

zur Kummer-Sequenz ist Null. Der Kern dieses Zusammenhangshomomorphismus besteht gerade aus dem m-ten Potenzen $(K_\ell^\times)^m$. Wegen

$a = \alpha_\ell^m$ und $\alpha_\ell \in K_\ell$ liegt a tatsächlich im Kern dieser Abbildung.

QED.

1.4.37 Das Galois-Symbol

Seien k ein Körper und m eine natürliche Zahl welche teilerfremd zur Charakteristik von k ist,

$$ggT(m, char(k)) = 1.$$

Die in 1.4.33 konstruierte Abbildung

$$\partial^n: k^\times\otimes_{\mathbb{Z}}...\otimes_{\mathbb{Z}}k^\times \longrightarrow H^n(k, \mu_m^{\otimes n}), c_1\otimes...\otimes c_n \mapsto \partial(c_1)\bigcup...\bigcup \partial(c_n).$$

faktorisiert sich nach 1.4.34 über die n-te Milnorsche K-Gruppe des Körpers k. Die induzierte Abbildung

$$h_{k,m}^n: K_n^M(k) \longrightarrow H^n(k, \mu_m^{\otimes n})$$

heißt n-tes Galois-Symbol von k.

1.4.38 Bloch-Kato-Vermutung

Seien k ein Körper und m eine natürliche Zahl welche teilerfremd zur Charakteristik von k ist,

$$ggT(m, char(k)) = 1.$$

Dann induziert das Galois-Symbol einen Isomorphismus

$$K_n^M(k)\otimes\mathbb{Z}/m\mathbb{Z} \longrightarrow H^n(k, \mu_m^{\otimes n}).$$

Bemerkungen

---

[152] Man denke sich $f_\ell(x)$ in Linearfaktoren zerlegt. Einer dieser Linearfaktoren ist $x - \alpha_\ell$. Die übrigen erhält man, indem man α_ℓ durch seine Konjugierten ersetzt, d.h. $f_\ell(1)$ ist das Produkt der Konjugierten von $1-\alpha_\ell$.

(i) Der Fall, daß m eine Potenz von 2 ist, wird auch als Milnor-Vermutung bezeichnet. Die Verknüpfung der Vermutung mit den Namen von Bloch und Kato ist nicht sicher aber allgemein akzeptiert.

(ii) Für n = 0 ist die Behauptung trivial.[153]

(iii) Für n = 1 ist das gerade der Satz von Kummer $H^1(k, \mu_m)) \cong k^\times/(k^\times)^m$, vgl. 1.4.35.

(iv) Der Fall n = 2 ist Gegenstand dieser Vorlesung.

(v) Der Fall n beliebig und m eine Potenz von 2 wurde von Voevodsky [1] bewiesen.

(vi) Ein Beweis des allgemeinen Falls ist von Voevodsky und Rost angekündigt, die Einzelheiten sind jedoch nur teilweise zugänglich.

1.4.39 Satz von Merkurjev-Suslin II

Die Bloch-Kato Vermutung ist richtig für n = 2.

1.4.40 Vereinbarung

Unser nächstes Ziel ist es, den Zusammenhang zwischen der Bloch-Kato-Vermutung (im Fall n = 2) und der Theorie der zentralen einfachen Algebren zu beschreiben.

Wir nehmen fürs erste an, daß der Grundkörper k eine zu m teilerfremde Charakteristik besitzt und eine m-te primitive Einheitswurzel enthält,

m teilerfremd zu char(k)

$\omega \in k$, ω primitive m-te Einheitswurzel.

Das Symbol $h^2_{k,m}$ nimmt Werte in $H^2(k, \mu_m^{\otimes 2})$ an. Wir fixieren einen Isomorphismus

$$\mu_m \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}, \omega \mapsto 1,$$

und identifizieren auf diese Weise den Wertevorrat dieses Symbols,

(1) $$H^2(k, \mu_m^{\otimes 2}) \cong H^2(k, \mathbb{Z}/m\mathbb{Z}) \cong H^2(k, \mu_m) \cong {}_m\mathrm{Br}(k),$$

mit den m-Teilungspunkten der Brauergruppe Br(k), vgl. Bemerkung 1.4.18 (ii). Wir weisen darauf hin, diese Folge von Isomorphismen hängt von der Wahl der Einheitswurzel ω ab.

1.4.41 Symbole von $K_2^M(k)$ und zyklishen k-Algebren

Seien $a, b \in k^\times$. Dann entspricht bei den Isomorphismen von 1.4.40(1) das Element

$$h^2_{k,m}(\{a,b\}) \in H^2(k, \mu_m^{\otimes 2})$$

gerade die Brauer-Äquivalenz-Klasse

$$[\,(a,b)_\omega^{-1}\,] \in {}_m\mathrm{Br}(k)$$

der zur zyklischen Algebra $(a,b)_\omega$ von 1.4.20[154] entgegengesetzten k-Algebra.

Mit anderen Worten, das Galois-Symbol hat im Grad 2 die Gestalt

---

[153] Auf beiden Seiten steht $\mathbb{Z}/m\mathbb{Z}$.

[154] Zur Erinnerung: $(a,b)_\omega = \langle x, y\rangle$ mit $x^m = a$, $y^m = b$, $yx = \omega xy$.

$$h^2_{k,m}: K_2^M(k) \longrightarrow H^2(k, \mu_m^{\otimes 2}) \cong H^2(k, \mu_m) \cong {}_mBr(k), \{a,b\} \mapsto [(a,b)_\omega^{-1}]$$

(falls k eine zu m teilerfremde Charakteristik besitzt und eine primitive m-te Einheitswurzel enthält, vgl. 1.4.40).

Bemerkungen

(i) Wie wir in 1.4.20 und 1.4.19 gesehen haben, zerfällt die Algebra $(a,b)_\omega$ über einer Galois-Erweiterung K/k des Grades m, d.h. des gilt (nach 1.4.25 und 1.4.30)

$$per((a,b)_\omega \mid ind\,(a,b)_\omega \mid m,$$

d.h diese Algebra repräsentiert tatsächlich ein Element von ${}_mBr(k)$.

(ii) Aus unserer Aussage ergibt sich, daß der Satz von Merkurjev-Suslin, wie wir ihn in 1.4.32 formuliert haben aus der Surjektivität von $h^2_{k,m}$ folgt (unter der Annahme, $\omega \in k$)[155]. Im folgenden wollen wir deshalb unter dem Satz von Merkurjev-Suslin die allgemeinere Aussage von 1.4.39 verstehen.

(iii) Bevor wir uns dem Beweis von 1.4.41 zuwenden, erinnern wir an einige Konstruktionen im Zusammenhang mit der Kummer-Sequenz 1.4.35.

1.4.42 Satz von Kummer

Seien k ein Körper und m eine zur Charakteristik von k teilerfremde natürliche Zahl.

$$m \text{ teilerfrem zu } char(k).$$

Wir nehmen weiter an, k enthält eine primitive m-te Einheitswurzel

$$\omega \in k.$$

Dann hat jede endliche Galois-Erweiterung von k mit einer zu $\mathbb{Z}/m\mathbb{Z}$ isomorphen Galois-Gruppe die Gestalt

$$k(\alpha)/k \text{ und } \alpha^m \in k^\times$$

mit $\alpha \in k$.

Beweis. Eine Galois-Erweiterung K/k der angegebenen Art entspricht einer Faktorgruppe von

$$G = G(k^s/k),$$

die isomorph ist zu $\mathbb{Z}/m\mathbb{Z}$. Betrachten wir die zugehörige Surjektion

$$\lambda: G \longrightarrow G(K/k) = \mathbb{Z}/m\mathbb{Z}, \sigma \mapsto \sigma|_K$$

Nach Voraussetzung gilt $\mu_m \subseteq k^\times$, also

$$\begin{aligned} Hom(G, \mathbb{Z}/m\mathbb{Z}) &= H^1(G, \mathbb{Z}/m\mathbb{Z}) \text{ (weil G trivial operiert auf } \mathbb{Z}/m\mathbb{Z}) \\ &= H^1(k, \mu_m). \end{aligned}$$

Die zweite Isomorphie hängt von der Wahl von ω ab. Wegen

$$k^\times/k^{\times m} \cong H^1(k, \mu_m)$$

---

[155] Weil $K_2^M(k)$ von den Symbolen {a, b} erzeugt wird (nach Definition der Milnor-Gruppe), folgt aus der Surjektivität von $h^2_{k,m}$, daß ${}_mBr(k)$ von den Klassen der Algebren $(a,b)_\omega$ erzeugt wird, d.h. jede zentrale einfache Algebra der Periode m ist Brauer-äquivalent zu einem Tensorprodukt von Algebren der Gestalt $(a,b)_\omega$.

(vgl. 1.4.35) entspricht λ gerade der Restklasse eines $a \in k^\times$ modulo $k^{\times m}$. Wir wählen für α eine m-te Wurzel aus a. Nach Definition von a ist dann λ das Bild von a beim Zusammenhangshomomorphismus

$$k^\times \longrightarrow H^1(k, \mu_m),\ a \mapsto \alpha \mapsto (\sigma \mapsto \sigma(\alpha)/\alpha)$$

der Kummer-Sequenz, d.h. λ ist die Abbildung $G \longrightarrow \mathbb{Z}/m\mathbb{Z} = \mu_m$, $\sigma \mapsto \alpha/\sigma(\alpha)$. Für den Kern von λ erhalten wir damit

$$G(k^s/K) = \mathrm{Ker}(\lambda) = \{\sigma \in G \mid \sigma(\alpha)/\alpha = 1\} = \{\sigma \in G \mid \sigma|_{k(\alpha)} = \mathrm{Id}\} = G(k_s/k(\alpha)),$$

Nach dem Hauptsatz der Galois.-Theorie ist

$$K = k(\alpha).$$

QED.

1.4.43 Eine Beschreibung der Kummer-Abbildung $\partial: k^\times \longrightarrow H^1(k, \mu_m)$

Sei k ein Körper, welcher eine primitive m-te Einheitswurzel

$$\omega \in k$$

enthält. Identifiziert man

$$H^1(k, \mu_m) \cong^{156} H^1(k, \mathbb{Z}/m\mathbb{Z}) =^{157} \mathrm{Hom}(G(k_s/k), \mathbb{Z}/m\mathbb{Z}),$$

so entspricht das Bild $\partial(a)$ von $a \in k^\times$ bei der Kummer-Abbildung gerade einem Charakter

$$\lambda: G(k_s/k) \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

mit $\lambda(\sigma) = 1$,[158] wobei σ den k-Automorphismus

$$\sigma: k_s \longrightarrow k_s,\ \sqrt[m]{a} \mapsto \omega \bullet \sqrt[m]{a},$$

bezeichnet, der eine m-te Wurzel $\sqrt[m]{a}$ aus a in $\omega \bullet \sqrt[m]{a}$ abbildet. Den Kern dieses Charakters haben im Beweis von 1.4.42 berechnet:

$$\mathrm{Ker}(\lambda) = G(k_s/k(\alpha)),$$

d.h. λ induziert einen Isomorphismus

$$\tilde{\lambda}: G(k(\alpha)/k) = G(k_s/k)/G(k_s/k(\alpha)) \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}.$$

Nach 1.4.20 ist dann die k-Algebra $(a,b)_\omega$ isomorph[159] zur zyklischen k-Algebra $(\tilde{\lambda}, b)$,

---

[156] Wir identifizieren μ_m mit $\mathbb{Z}/m\mathbb{Z}$ indem wir ω in die Restklasse der 1 abbilden.

[157] Weil $G = G(k_s/k)$ auf $\mathbb{Z}/m\mathbb{Z}$ trivial operiert, sind die 1-Kozyklen von G gerade die Homomorphismen und die 1-Koränder sind alle identisch Null.

[158] Der zu a gehörige Charakter ist nach dem Beweis von 1.4.42 die Abbildung

$$G(k_s/k) \longrightarrow \mu_m,\ \sigma \mapsto \sigma(\alpha)/\alpha,$$

Speziell für den angegebenen Automorphis erhalten wir als Bild die Einheitwurzel ω, die gerade dem Erzeuger 1 von $\mathbb{Z}/m\mathbb{Z}$ entspricht.

[159] Weil λ den Automorphismus $\sigma: k(\sqrt[m]{a}) \longrightarrow k(\sqrt[m]{a})$, $\sqrt[m]{a} \mapsto \omega \bullet \sqrt[m]{a}$, in die Restklasse von 1 abbildet.

$$(a,b)_\omega = (\widetilde{\lambda}, b) \text{ mit } \lambda = \partial(a).$$

1.4.44 Die zyklische Algebra (χ, b) als Cup-Produkt

Seien k ein Körper, $m > 0$ eine natürliche Zahl und

$$K/k$$

eine zyklische Galois-Erweiterung des Grades m mit der Gruppe G. Weiter seien

$$\widetilde{\lambda}: G \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$$

ein Isomorphismus und

$$\lambda: G(k_s/k) \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

eine Anhebung von $\widetilde{\lambda}$ zu einem Charakter auf der absoluten Galois-Gruppe von k. Schließlich sei

$$\delta: H^1(k, \mathbb{Z}/m\mathbb{Z}) \longrightarrow H^2(k, \mathbb{Z})$$

der Zusammenhangshomomorphismus zur kurzen exakten Sequenz

$$0 \longrightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0.$$

Dann ist für jedes $b \in k^\times$ das Bild von $(\delta(\lambda), b)$ beim Cup-Produkt

$$H^2(k, \mathbb{Z}) \times H^0(k, k_s^\times) \longrightarrow H^2(k, k_s^\times) \cong Br(k)$$

gerade die Brauer-Klasse der zyklischen k-Algebra $(\widetilde{\lambda}, b)$,

$$\delta(\lambda) \bigcup b = [(\widetilde{\lambda}, b)].$$

Beweis. Wir erinnern an die Konstruktion der k-Algebra (χ, b) in 1.4.19 mit Hilfe des Galois-Abstiegssatzes 1.4.16.

Der Isomorphismus $\widetilde{\lambda}$ definiert einen injektiven Homomorphismus

$$z(b): G \xrightarrow{\widetilde{\lambda}} \mathbb{Z}/m\mathbb{Z} \longrightarrow PGL(m, K),$$

wobei die zweite Abbildung die Restklasse von 1 auf die Klasse F(b) der umkehrbaren $m \times m$-Matrix

$$\widetilde{F}(b) := \begin{pmatrix} 0 & 0 & \dots & 0 & b \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

abbildet. Weil die Einträge der Matrix $\widetilde{F}(b)$ im Grundkörper k liegen, bleibt F(b) invariant unter der Operation von G auf PGL(m,K), d.h. z(b) läßt sich als 1-Kozyklus ansehen und definiert ein Element von

$$H^1(G, PGL(m,K))$$

und damit eine zentrale einfache k-Algebra $(\widetilde{\lambda}, b)$ des Grades m. Genauer,

$$(\widetilde{\lambda}, b) := ({}_{z(b)}M_m(K))^G,$$

wenn ${}_{z(b)}M_m(K)$ die Matrizen-Algebra über K mit der durch z(b) getwisteten Operation bezeichnet. Wie wir in 1.4.19 gesehen haben, gilt

$$\widetilde{F}(b)^m = b \bullet Id_m. \qquad (1)$$

Wir betrachten das folgende kommutative Diagramm mit exakten Zeilen.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{Z} & \xrightarrow{m} & \mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} & \longrightarrow & 1 \\ & & b\downarrow & & \widetilde{F}(b)\downarrow & & F(b)\downarrow & & \\ 1 & \longrightarrow & K^\times & \longrightarrow & GL(m,K) & \longrightarrow & PGL(m,K) & \longrightarrow & 1 \end{array}$$

Dabei sollen die mit b, $\widetilde{F}(b)$ und F(b) bezeichneten Abbildungen die Gruppen-Homomorphismen bezeichnen, welche den Erzeuger 1 bzw. 1 mod m in das entsprechende Element abbilden.[160] Die Kommutativität des linken Quadrats folgt aus der Identität (1), die des rechten Quadrats aus der Definiton von F(b). Wir gehen zu den langen exakten Kohomologie-Sequenzen über und erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} H^1(G,\mathbb{Z}/m\mathbb{Z}) & \xrightarrow{\delta} & H^2(G,\mathbb{Z}) \\ F(b)_*\downarrow & & b_*\downarrow \\ H^1(G,PGL(m,K)) & \xrightarrow{\delta_m} & H^2(G,K^\times) \end{array},$$

dessen horizontale Abbildungen Zusammenhangshomomorphismen sind. Der Isomorphismus $\widetilde{\lambda}$ läßt sich als Element

$$\widetilde{\lambda} \in \mathrm{Hom}(G,\mathbb{Z}/m\mathbb{Z}) =^{161} H^1(G, \mathbb{Z}/m\mathbb{Z})$$

der linken oberen Kohomologie-Gruppe auffassen und wird bei $F(b)_*$ in die Klasse des Kozyklus z(b) abgebildet[162],

$$F(b)_*(\widetilde{\lambda}) = [z(b)].$$

Deshalb ist

$$\delta_m(F(b)_*(\widetilde{\lambda})) = \delta_n[z(/b)] = [(\widetilde{\lambda},b)]$$

gerade die Klasse der durch z(b) definierten zentralen einfachen k-Algebra $(\widetilde{\lambda},b)$. Auf Grund der Kommutativität des Vierecks folgt

$$[(\widetilde{\lambda},b)] = b_*(\delta(\widetilde{\lambda})). \qquad (2)$$

Wir haben jetzt die rechte Seite dieser Identität als Cup-Produkt zu interpretieren. Dazu erinnern wir an die Definiton des Cup-Produkts

$$H^2(G,\mathbb{Z}) \times H^0(G,K^\times) \longrightarrow H^2(G,K^\times), ([x],[y]) \mapsto [x] \bigcup [y]$$

(vgl. G & S 3.4.9): man wähle Repräsentanten

$$x\colon \mathbb{Z}[G\times G] \longrightarrow \mathbb{Z},\ y\colon \mathbb{Z} \longrightarrow K^\times$$

der Klassen [x], [y], bilde das zugehörige Tensorprodukt der Abbildungen,

$$x \otimes y\colon \mathbb{Z}[G\times G] \longrightarrow K^\times$$

---

[160] Die rechte vertikale Abbildung ist wohldefiniert wegen (1).

[161] G operiert trivial auf $\mathbb{Z}/m\mathbb{Z}$.

[162] nach Definition von z(b) (und der durch F(b) induzierten Abbildung $F(b)_*$).

und gehe zur zugehörige Kohomologie-Klasse über. Im Fall y = b ist x⊗y gerade das Produkt der Abbildung x mit b, d.h. $[x]\bigcup[b] = b_*([x])$. Die Identität (2) erhält damit die Gestalt

$$[(\widetilde{\lambda},b)] = \delta(\widetilde{\lambda})\bigcup b$$

in $H^2(G, K^\times) = Br(K/k)$. Wir wenden auf diese Identität die Inflationsabbildung zur natürlichen Surjektion

$$\rho:G' := G(k_s/k) \longrightarrow G = G(K/k), \sigma \mapsto \sigma|_K.$$

mit dem Kern $H' := Ker(\rho) = G(k_s/K)$ an,

$$\begin{array}{ccc} \text{Inf: } H^2(G'/H', (k_s^\times)^H) & \longrightarrow & H^2(G',k_s^\times) \\ \| & & \| \\ H^2(G, K^\times) & & Br(k) \\ \| & & \\ Br(K/k) & & \end{array}$$

welche die relative in die absolute Brauer-Gruppe einbettet und erhalten in Br(k):

$$[(\widetilde{\lambda},b)] = Inf(\delta(\widetilde{\lambda})\bigcup b)$$

$$=^{163} Inf(\delta(\widetilde{\lambda}))\bigcup Inf(b)$$

$$=^{164} \delta(Inf(\widetilde{\lambda}))\bigcup Inf(b)$$

Die beiden Inflationsabbildungen[165] der letzten Zeile lassen sich explizit beschreiben.

$$\text{Inf: } H^2(G,\mathbb{Z}/m\mathbb{Z}) \longrightarrow H^2(G',\mathbb{Z}/m\mathbb{Z})$$

$$\begin{array}{ccc} \text{Inf: } H^0(G,K^\times) & \longrightarrow & H^0(G',k_s^\times) \\ \| & & \| \\ (K^\times)^G & & (k_s^\times)^{G'} \\ \| & & \| \\ k^\times & & k^\times \end{array}$$

Die zweite ist die identische Abbildung,

$$[(\widetilde{\lambda},b)] = \delta(Inf(\widetilde{\lambda}))\bigcup b,$$

die erste wird induziert durch die Abbildung, welche jedem Homomorphismus

$$G \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

auf dessen Zusammensetzung mit ρ abbildet. Wegen $\widetilde{\lambda}\circ\rho = \lambda$, erhalten wir

$$[(\widetilde{\lambda},b)] = \delta(\lambda)\bigcup b$$

wie behauptet.
QED.

1.4.45 Beschreibung der Norm-Reste-Abbildung

Seien k ein Körper, m > 0 eine natürliche Zahl,

$$K/k$$

---

[163] Verträglichkeit der Inflation mit dem Cup-Produkt, vgl. [G&S] 3.4.12(ii).
[164] Verträglichkeit der Inflation mit Zusammenhangshomomorphismen, vgl. [G&S] 3.3.11 Beispiel 2
[165] Sämtlich hier auftretenden Inflationsabbildung gehören zur Surjektion ρ: G'⟶G.

eine zyklische Galois-Erweiterung des Grades m mit der Gruppe G und

$$\widetilde{\lambda}: G \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$$

ein Isomorphismus. Dann wird der Isomorphismus

$$H^2(G, K^\times) \cong k^\times/N_{K/k}(K^\times)$$

von Bemerkung 1.4.18 (iii) induziert durch die Norm-Reste-Abbildung, welche die Gestalt

$$k^\times \longrightarrow H^2(G, K^\times)\ , b \mapsto [(\widetilde{\lambda}, b)].$$

besitzt.

Beweis. Nach Voraussetzung ist $G = G\ /\ $ eine zyklische Gruppe. Die Norm-Reste-Abbildung 1.4.18(iii) kommt nach Definition vom Tate-Kohomologie-Isomorphismus (vgl. Bemerkung "Periodizität", 1.4.6 (iv))

$$H^2\ (G, K^\times) \cong (K^\times)^G/N\bullet K^\times = k^\times/N_{K/k}(K^\times).^{166}$$

Nach Bemerkung 1.4.8 (v) läßt sich dieser als Cup-Produkt mit einem Erzeuger

$$\xi \in \hat{H}^2(G, \mathbb{Z}) = \mathbb{Z}^G/N\mathbb{Z} = \mathbb{Z}/m\mathbb{Z},$$

interpretieren:

$$\begin{array}{ccc} \hat{H}^0(G, K^\times) & \longrightarrow & \hat{H}^2\ (G, K^\times),\ a \mapsto \xi \bigcup a. \\ \| & & \| \\ \mathrm{Koker}(K^\times{}_G \xrightarrow{N^*} K^{\times G}) & & H^2\ (G, K^\times), \\ \| & & \\ k^\times/N_{K/k}(K^\times) & & \end{array}$$

Die Norm-Reste-Abbildung ist somit die Abbildung

$$\varphi: k^\times \longrightarrow H^2(G, K^\times)\ , b \mapsto \xi \bigcup b.$$

Zum Beweis der Behauptung reicht es zu zeigen, für ξ kann man das Bild von

$$\widetilde{\lambda} \in \mathrm{Hom}(G, \mathbb{Z}/m\mathbb{Z}) = H^1(G, \mathbb{Z}/m\mathbb{Z})$$

beim Zusammenhangshomomorphismus

$$\delta: H^1(G, \mathbb{Z}/m\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z})$$

zur exakten Sequenz

$$0 \longrightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0.$$

verwenden, denn dann gilt (nach auf Grund des Beweises von 1.4.44):

$$\varphi(b) = \delta(\widetilde{\lambda}) \bigcup b = [(\widetilde{\lambda}, b)].$$

Zum Beweis reicht es zu zeigen,

1. $\widetilde{\lambda}$ ist ein Erzeuger von $\mathrm{Hom}(G, \mathbb{Z}/m\mathbb{Z})$.
2. $\delta: H^1(G, \mathbb{Z}/m\mathbb{Z}) \longrightarrow H^2(G, \mathbb{Z})$ ist ein Isomorphismus.

Zu 1. Nach Voraussetzung ist $\widetilde{\lambda}$ ein Isomorphismus, und damit ein Erzeuger von

$$\mathrm{Hom}(G, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z},\ f \mapsto f(e),$$

---

[166] N ist die Summe der Elemente von G im Gruppen-Ring $\mathbb{Z}[G]$.

Zu 2. Aus der obigen kurzen exakten Sequenz erhalten wir eine exakte Sequenz

$$\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow H^1(G, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{\delta} H^1(G, \mathbb{Z}) \xrightarrow{m} H^1(G, \mathbb{Z}).$$

Weil G die Ordnung m besitzt ist die Multiplikation ganz rechts die Null-Abbildung. Die Abbildung ganz links ist surjektiv, die rechts daneber also identisch Null. Damit erhalten wir eine exakte Sequenz

$$0 \xrightarrow{0} H^1(G, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{\delta} H^1(G, \mathbb{Z}) \xrightarrow{m} 0.$$

Mit anderen Worten, δ ist ein Isomorphismus.
QED.

1.4.46 Kriterium für das Zerfallen der zyklischen Algebra (χ,b)

Die Brauer-Äquivalenz-Klasse der zyklischen k-Algebra (χ,b) zur Galois-Erweitrung K/k ist genau dann trivial, wenn b im Bild der Norm-Abbildung $N_{K/k}: K^\times \longrightarrow k^\times$ liegt.
Beweis. Die Aussage folgt unmittelbar aus 1.4.45.
QED.

1.4.47 Folgerung

Seien k ein Körper, m > 0 eine natürliche Zahl,
K/k
eine zyklische Galois-Erweiterung des Grades m mit der Gruppe G und
A
eine zentrale einfache k-Algebra, die über K zerfällt. Dann gilt:
(i) Es gibt einen Isomorphismus

$$\chi: G \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z}$$

und ein Element $b \in k^\times$ mit der Eigenschaft, daß A Brauer-Äquivalent zu (χ,b) ist,

$$[A] = [(\chi,b)].$$

(ii) Hat A außerdem den Grad m, so gilt sogar $A \cong (\chi,b)$.
Beweis. Zu (i). Weil A über K zerfällt, liegt die Brauer-Äquivalenz-Klasse von A in der relativen Brauer-Gruppe,

$$[A] \in Br(K/k) = H^2(G, K^\times).$$

Die Behauptung folgt damit aus der Surjektivität der Abbildung

$$k^\times \longrightarrow H^2(G, K^\times) \ , \ b \mapsto [(\chi,b)].$$

von 1.4.45 (wobei der Isomorphismus beliebig vorgegeben werden kann).

Zu (ii). Die zu A nach (i) gehörige zyklischen k-Algebra (χ, b) hat dann denselben Grad wie A. Brauer-Äquivalente k-Algebren desselben Grades sind aber isomorph.[167]

QED.

Zum Beweis der Aussage von 1.4.41 fehlen uns noch eine leichte Verallgemeinerung des Cup-Produkts, nämlich das Cup-Produkt bezüglich einer Paarung, und die folgende Eigenschaft des Cup-Produkts (vgl. [G&S] 3.4.1).

---

[167] Beide k-Algebren sind nach Wedderburn (bis auf Isomorphie) Matrizen-Algebren über der einzigen Divisionsalgebra D in ihrer Brauer-Klasse, sagen wir $M_a(D)$ bzw. $M_b(D)$. Da sie denselben Grad, also dieselbe Dimension, über k besitzen, muß a = b gelten, d.h. sie sind isomorph.

1.4.48 Das Cup-Produktes zu einer Paarung der Koeffizienten

Seien G eine Gruppe und

$$0 \longrightarrow A' \longrightarrow A \longrightarrow A'' \longrightarrow 0 \text{ und } 0 \longrightarrow B' \longrightarrow B \longrightarrow B'' \longrightarrow 0$$

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

$$A' \times B'' \longrightarrow C \text{ und } A'' \times B' \longrightarrow C.$$

Für die Cup-Produkte bezüglich dieser bilinearen Abbildungen gilt dann

$$\delta_A(\alpha) \cup \beta =^{168} (-1)^{i+1} \alpha \cup \delta_B(\beta)$$

für $\alpha \in H^i(G, A'')$, $\beta \in H^j(G, B'')$ in $H^{i+j+1}(G, C)$.[169]

Beweis. Sei P_* eine projektive Auflösung des trivialen G-Moduls $\mathbb{Z}$. Wir erhalten 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

---

[168] 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.

[169] Nach unserer bisherigen Definition liegen die Werte des Cup-Produkts eigentlich in

$$H^{i+j+1}(G, A \otimes B)$$

Die Paarung $A \times B \longrightarrow C$, bzw. der zugehörige G-Modul-Homomorphismus $A \otimes B \longrightarrow C$ induziert aber einen Gruppen-Homomorphismus

$$H^{i+j+1}(G, A \otimes B) \longrightarrow H^{i+j+1}(G, C)$$

Das Bild des Cup-Produkts bei diesem Homomorphismus bezeichnen wir ebenfalls mit $\cup$ bzw. $\bullet$ und sprechen vom Cup-Produkt bezüglich der gegebenen Paarung.

$$\delta_A(\alpha) = [a'] \in H^{i+1}\mathrm{Hom}_G(P_*,A').$$

Analog besitzt b" ein Urbild

$$b \in \mathrm{Hom}_G(P_*, B),$$

und es gilt

$$\delta_A(\alpha)\bigcup\beta = [\varphi\circ((\partial a)\otimes b)] \in H^{i+j+1}\mathrm{Hom}_G(P_*\otimes P_*, C).$$

In analoger Weise repräsentiert man $\alpha\bigcup\delta_B(\beta)$:

$$\alpha\bigcup\delta_B(\beta) = [\varphi\circ(a\otimes\partial b)] \in H^{i+j+1}\mathrm{Hom}_G(P_*\otimes P_*, C).$$

Betrachten wir jetzt das Element

$$\varphi\circ((\partial a)\otimes b + (-1)^i a\otimes\partial b) \in \mathrm{Hom}_G(P_*\otimes P_*, C).$$

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

$$\delta_A(\alpha)\bigcup\beta + (-1)^i\,\alpha\bigcup\delta_B(\beta) = [\varphi\circ((\partial a)\otimes b + (-1)^i a\otimes\partial b)] = 0,$$

d.h. es gilt die Behauptung.
QED.

1.4.49 Beweis von 1.4.41

Wir verwenden die Bezeichnungen von 1.4.44. Auf Grund der dortigen Beschreibung der Brauer-Klasse der zyklischen Algebra $(\widetilde{\lambda}, b)$,

$$\delta(\lambda)\bigcup b = [(\widetilde{\lambda}, b)] \text{ in } \mathrm{Br}(k) = H^2(k, k_s^\times),$$

reicht es zu zeigen,

$$-\delta(\lambda)\bigcup b = \lambda\bigcup\partial(b) \qquad (1)$$

wobei das Cup-Produkt rechts gerade die Abbildung

$$H^1(k, \mathbb{Z}/m\mathbb{Z}) \times H^1(k, \mu_m) \longrightarrow H^1(k, \mu_m^{\otimes 2}) =^{170}\ {}_m\mathrm{Br}(k).$$

sei und $\partial: k^\times \longrightarrow H^1(k, \mu_m)$ die Kummer-Abbildung.

Der Isomorphismus

$$\widetilde{\lambda}: G \longrightarrow \mathbb{Z}/m\mathbb{Z},$$

der in 1.4.44 beliebig gewählt werden kann, sei dabei gerade der Isomorphismus $\widetilde{\lambda}$ von 1.4.43, d.h.

$$\partial(a) = \lambda \text{ und } (a,b)_\omega = (\widetilde{\lambda}, b).^{171}$$

Die zu beweisende Identität ist aber ein Spezialfall der allgemeinen Identität 1.4.48 (mit i = bzw. die proendliche Variante davon. Wir verwenden hier, daß δ bzw. ∂ Zusammenhangshomomorphismen zu den exakten Sequenzen

$$0 \longrightarrow \mathbb{Z} \xrightarrow{m} \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \longrightarrow 0$$

---

[170] vgl. 4.7.1(1).

[171] d.h. die rechte Seite von (1) ist gerade das Bild des Symbols {a,b} bei der Bloch-Kata-Abbildung $h^2_{k,m}$.

$$1 \longrightarrow \mu_m \longrightarrow k_s^\times \xrightarrow{m} k_s^\times \longrightarrow 1$$

sind und die Paarung

$$\mathbb{Z} \otimes_{\mathbb{Z}} k_s^\times \longrightarrow k_s^\times, x \otimes c \mapsto c^x,$$

trivial ist $m\mathbb{Z} \otimes \mu_m$.

1.4.50 Folgerung

Seien k ein Körper, der eine primitive m-te Einheitswurzel ω enthält und $a,b \in k^\times$. Dann sind die folgende Aussagen äquivalent.

(i) Das Bild $h^2_{k,m}(\{a,b\})$ des Symbols {a,b} ist trivial.

(ii) Die zyklische k-Algebra $(a,b)_\omega$ zerfällt.

(iii) Das Element b liegt im Bild der Normabbildung $N_{K/k}: K := k(\sqrt[m]{a}) \longrightarrow k$.

Bemerkungen

(i) Da die ersten beiden Aussagen symmetrisch in a und b sind, ist b genau dann Norm eines Elements von $k(\sqrt[m]{a})$, wenn a Norm eines Elements von $k(\sqrt[m]{b})$. Aussagen dieses Typs heißt gewöhnlich Reziprozitätsgesetz.

Beweis. (i) ⇔ (ii). Ergibt sich aus der Beschreibung von $h^2_{k,m}$ in 14.41.

(ii) ⇔ (iii). Ergibt sich aus der Beschreibung der Norm-Reste-Abbildung in 1.4.45.
QED.

Anhänge

A0.1 Affine und quasi-projektive Varietäten

A0.1.1 Klassische affine und projektive Varietäten

Sei k ein Körper. Eine (über k definierte affine) Varietät V im affinen Raum $\mathbb{A}^n_k$ ist definiert als Nullstellenmenge einer Menge

$$M \subseteq A := k[x_1,...,x_n]$$

von Polynomen: für jede Körpererweiterung K/k ist die Menge der K-rationalen Punkte dieser Varietät definiert als

$$V(K) := \{(c_1, ... , c_n) \in K^n \mid f(c_1, ... , c_n) = 0 \text{ für jedes } f \in M \}$$

Die zu M gehörige Varietät wird mit V(M) bezeichnet. Die Menge ihrer K-rationalen Punkte also mit V(M)(K).

Eine (projektive) Varietät V im projektiven Raum $\mathbb{P}^n_k$ ist definiert als Nullstellenmenge einer Menge

$$M \subseteq A := k[x_0,..., x_n]$$

von _____nen Polynomen: für jede Körpererwerweiterung K/k ist die Menge der K-rationalen Punkte dieser Varietät definiert als

$$V(K) := \{(c_0, \dots, c_n) \in \mathbb{P}^n_K \mid f(c_0, \dots, c_n) = 0 \text{ für jedes } f \in M\}.$$

Die zu M gehörige Varietät wird mit V(M) bezeichnet. Die Menge ihrer K-rationalen Punkte also mit V(M)(K). Die Varietät V = V(M) selbst werden wir mit der Abbildung

$$K = V(K)$$

auf der Menge der Körpererweiterungen K/k identitizieren.

Bemerkungen

(i) Ist

$$K := \overline{k}$$

die algebraische Abschließung von k, so nennt man

$$V(K)$$

auch die Menge der <u>geometrischen Punkte</u> der Varietät V. Oft kann man eine Varietät V einfach mit der Menge ihrer geometrischen Punkte identifizieren. Wenn in den nachfolgenden Bemerkungen Varietäten wie Mengen behandelt werden - zum Beispiel, wenn von Vereinigungen und Durchschnitten die Rede ist - so beziehen sich diese Aussagen zunächst nur auf die Mengen der geometrischen Punkte.

Bei dieser Betrachtungsweise geht jedoch Information verloren (nämlich die bezüglich des Teilkörpers k). Wir werden deshalb den Begriff des Punktes soweit verallgemeinern, das solche Aussagen auch für K = k gelten.

(ii) Ersetzt man die Menge M durch das von M erzeugte Ideal

$$<M> := \{a_1 m_1 + \dots + a_r m_r \mid m_1, \dots, m_r \in M, a_1, \dots, a_r \in A\},$$

so gilt

$$V(M) = V(<M>),$$

d.h. man kann von der Menge der definierenden Gleichungen immer annehmen, daß sie ein Ideal bilden.

(iii) der Polynomring A noethersch ist, hat jedes Ideal ein endliches Erzeugendensystem und man kann das Ideal <M> durch ein Erzeugendensystem des Ideals ersetzen, zum Beispiel also durch eine endliche Teilmenge. Für jedes M gibt es also endlich viele Polynome $f_1, \dots f_r \in A$ mit

$$V(M) = V(f_1, \dots f_r).$$

(iv) Es ist leicht zu zeigen, daß der Durchschnitt einer beliebigen Familie von Varietäten eine Varietät ist und daß die Vereinigung endlich vieler Varietäten eine Varietät ist:

$$\bigcap V(I_\alpha) = V(\sum_\alpha I_\alpha) \text{ und } V(I_1) \bigcup V(I_2) = V(^{172}I_1 \bullet I_2) = V(I_1 \bigcap I_2) \text{ für Ideale } I_j.$$

(v) Eine Varietät V heißt (geometrisch)[173] <u>irreduzibel</u>, wenn sie nicht Vereinigung von zwei echten abgeschlossenen Teilmengen ist.

Zum Beispiel ist die Hyperfläche

$$V(f)$$

genau dann irreduzibel, wenn f ein irreduzibles Polynom ist. Ein Kreis ist irreduzibel. Die Vereinigung zweier unterschiedlicher Kreise ist es nicht. Ellipsen, Hyperbeln und Parabeln sind irreduzibel. Die Vereinigung zweier Geraden ist es nicht.

(vi) Jede Varietät ist Vereinigung von endlich vielen irreduziblen.

(vii) Im Fall

---

[172] $I_1 \bullet I_2$ bezeichnet das <u>Produkt-Ideal</u>, d.h. das von den Produkten

$$a_1 \bullet a_2 \text{ mit } a_1 \in I_1 \text{ und } a_2 \in I_2$$

erzeugte Ideal.

[173] Der Zusatz ‘geometrisch’ soll darauf hinweisen, daß wir uns auf die Menge der geometrischen Punkte der Varietät beziehen. Ohne diesen Zusatz sind die ‘verallgemeinerten Punkte’ der Varietät gemeint.

$$K := \overline{k}$$

können wir für jede affine[174] Varietät

$$V = V(I)$$

ein Ideal definieren:

$$I(V) := \{f \in := K[x_1,...,x_n] \mid f(p) = 0 \text{ für jeden Punkt } p \in V\}.$$

Es gilt dann

$$I(V) = \sqrt{I} := \{f \in k[x_1,...,x_n] \mid f^m \in I \text{ für eine natürliche Zahl } m\}.$$

Diese Aussage ist eine Variante des sogenannten Hilbertschen Nullstellensatzes. Man beachte, trivialerweise gilt für jedes Ideal

$$V(I) = V(\sqrt{I}).$$

Wir bekommen auf diese Weise eine bijektive Abbildung

$$\{ \text{afffine Varitäten im } \mathbb{A}^n_K \} \longrightarrow \{ \text{Ideale } I \subseteq K[x_1,...,x_n] \text{ mit } I = \sqrt{I} \}, V \mapsto I(V),$$

mit der Umkehrabbildung $I \mapsto V(I)$.

(viii) Eine Varietät $V = V(I)$ ist genau dann irreduzibel, wenn das Radikal des definierenden Ideals I ein Primideal ist:

$$V \text{ irreduzibel} \Leftrightarrow \sqrt{I} \text{ ist Primideal.}$$

(ix) Eine affine Varietät V(I) heißt reduziert, wenn wenn das definierende Ideal I mit seinem Radikal übereinstimmt. Eine projektive Varietät heiß reduziert, wenn sie Vereinigung affiner reduzierter Varietäten ist (die mit offenen Teilmengen identifiziert werden können - siehe unten).

(x) Für jedes irreduzible Polynom f ist

$$V(f)$$

reduziert und irreduzibel. Für jedes Primideal I ist V(I) irreduzibel.

A0.1.2 Die Zariski-Topologie

Sei V eine affine (bzw. projektive) Varietät. Die Menge der in V enthaltenen affinen (bzw. projektiven) Varietäten bilden die abgeschlossenen Mengen einer Topologie, welche Zariski-Topologie heißt. Die offenen Mengen von V sind von der Gestalt

$$V - W$$

mit einer affinen (bzw. projektiven) Varietät. Eine Menge dieser Gestalt, wobei W durch ein einziges Polynom f definiert ist, heißt offene Hauptmenge und wird mit

$$D(f) = D_V(f)$$

bezeichnet. Eine offene Teilmenge einer projektiven Varietät heißt auch quasi-projektive Varietät.

Bemerkungen

(i) Die offenen Hauptmengen bilden eine Topologie-Basis der Zariski-Topologie, d.h. jede offene Menge ist Vereinigung endlich vieler offener Hauptmengen. Zum Beispiel ist

$$\mathbb{A}^n_k - V(f_1,..., f_m) = D(f_1) \cup ... \cup D(f_m)$$

(ii) Die Mengen

---

[174] Eine analoge Konstruktion ist auch im projektiven Fall möglich: I(V) ist dann das Ideal, das von allen homogenen Polynomen erzeugt wird, die auf V identisch Null sind. Allerdings gilt dann für das definierende Ideal I von V im allgemeinen nicht mehr

$$I(V) = \sqrt{I}.$$

Beispiel: die Ideale (1) und $(x_0,...,x_n)$ haben dieselbe Nullstellenmenge (nämlich die leere Menge) aber verschiedene Radikale: das zweite Ideal ist ein Primideal, stimmt also mit seinem Radikal überein. Letzteres ist somit vom gesamten Ring, d.h. von (1) verschieden.

$$U_i := \mathbb{P}^n_k - V(x_i) = \{[x_0,...,x_n] \in \mathbb{P}^n_k \mid x_i \neq 0\}$$

sind offene Hauptmengen im projektiven Raum. Jede von ihnen läßt sich mit dem affinen Raum identifizieren vermittels

$$\mathbb{A}^n_k \longrightarrow U_i, (x_1,...,x_n) = [x_1,...,x_{i-1}, 1, x_{i+1},...,x_n].$$

Da jeder Punkt im projektiven Raum eine von Null verschiedene projektive Koordinate besitzt, gilt

$$\mathbb{P}^n_k = U_0 \bigcup ... \bigcup U_n .$$

Der projektive Raum wird also vom afinen Räumen überdeckt. Analog sieht man, daß jede projektive Varietät überdeckt wird durch affine Varietäten. Insbesondere sind affine Varietäten quasi-projektiv.

(ii) Die affinen und die projektiven Varietäten sind (quasi-)kompakt bezüglich der Zariski-Topologie.

A0.1.3 Affine Spektren

Sei A ein kommutativer Ring mit 1. Dann wird die Menge der Primideal von A mit

$$\text{Spec } A$$

bezeichnet und heißt Spektrum von A.

Wir werden die Elemente dieser Menge auch als Punkte bezeichnen. Für jeden Punkt

$$p \in \text{Spec } A$$

bezeichen wir den Quotienten-Körper des Restklassen-Körpers von p mit

$$\kappa(p) := Q(A/p)$$

und nennen diesen Restklassenkörper von p. Für jeden Punkt $p \in \text{Spec } A$ und jedes Element $f \in A$ bezeichne

$$f(p) \in \kappa(p)$$

das Bild von $f \in A$ bei der natürlichen Abbildung

$$A \longrightarrow A/p \hookrightarrow Q(A/p) = \kappa(p), f \mapsto f \bmod p.$$

Wir sagen auch, f(p) ist der Wert von f im Punkt p. Auf diese Weise ist jedem Element von A eine auf Spec definierte Funktion zugeordnet.

Ist K/k eine Körpererweiterung, A eine (kommutative) K-Algebra, so sagt man A ist über k definiert, falls es eine k-Algebra A_k gibt mit

$$A_k \otimes_k K \cong A.$$

Die k-Algebra A_k heißt in dieser Situation auch k-Struktur von A. Man sagt dann auch vom zugehörigen Spektrum Spec A, es sei über k definiert.

Beispiel

Seien k ein Körper und

$$I \subseteq k[x_1, ... , x_n]$$

ein Ideal eines Polynomringe über k. Weiter sei

$$X := V(I)$$

die durch I definierte affine Varietät. Für jede Körpererweiterung

K/k

und jeden K-rationalen Punkt $p \in X(K)$ ist ein Auswertungshomomorphismus

$$k[x_1, \dots, x_n] \longrightarrow K, f \mapsto f(p),$$

definiert, dessen Kern das Ideal I enthält und somit einen Homomorphismus

$$e_p: k[X] := k[x_1, \dots, x_n]/I \longrightarrow k.$$

induziert. Der Faktor-Ring k[X] heißt Koodinatenring der affinen Varietät. Weil K nullteilerfrei ist, ist der Kern dieses Homomorphismus ein Primideal Ideal. Wir erhalten so eine Abbildung

$$X(K) \longrightarrow \operatorname{Spec} k[X], p \mapsto \operatorname{Ker}(e_p) \qquad (1)$$

für jede Körpererweiterung K/k.

Umgekehrt definiert jeder Punkt $p \in \operatorname{Spec} k[X]$ eine Körpererweiterung

$$K := \kappa(p) = Q(k[X]/p)$$

von k. Im folgenden bezeichne

$$\overline{\ }: k[x_1, \dots, x_n] \longrightarrow k[X], f \mapsto \overline{f} = f \bmod I,$$

den natülichen Homomorphismus. Für jedes $f \in I$ gilt dann

$$\begin{aligned}
0 &=^{175} \overline{0}(p) \\
&= \overline{f}(p) && (\overline{0} = \overline{f} \bmod I) \\
&= e_p(\overline{f}(x_1, \dots, x_n)) && (\text{Definition von } \overline{f}(p)) \\
&= e_p(f(\overline{x}_1, \dots, \overline{x}_n)) && (\overline{\ } \text{ ist k-Algebra-Homomorphismus}) \\
&= f(e_p(\overline{x}_1), \dots, e_p(\overline{x}_n)) && (e_p \text{ ist k-Algebra-Homomorphismus}) \\
&= f(\overline{x}_1(p), \dots, \overline{x}_n(p)) && (\text{Definition von } \overline{x}_i(p)) \\
&= f(c_1, \dots, c_n)
\end{aligned}$$

mit

$$c_i := \overline{x}_i(p) \in K.$$

Wir haben gezeigt,

$$c := (c_1, \dots, c_n) \in X(K)$$

ist ein K-rationaler Punkt von X.

Weil die $c_i = \overline{x}_i(p) = x_i \bmod p$ den Faktorring k[X]/p erzeugen[176], gilt

$$k(c_1, \dots, c_n) = Q(k[X]/p) = K = \kappa(p).$$

Wegen

$$c_i = x_i \bmod p = e_p(\overline{x}_i)$$

für jedes i ist die durch c definierte Auswertungsabbildung gleich e_p,

$$e_c = e_p$$

---

[175] Jeder Ring-Homomorphismus bildet die Null in die Null ab.

[176] denn k[X] ist ein Faktorring des Polynomrings $k[x_1, \dots, x_n]$

und das durch c definierte Primideal gleich $\mathrm{Ker}(e_p) = p$. Wir haben gezeigt, jedes Primideal des Koordinatenrings liegt im Bild einer der Abbildungen (1).

Es ist nicht schwer zu zeigen, zwei Punkte p', p" von X über irgendeinem Körper haben genau dann dasselbe Bild in Spec k[X] wenn es einen k-Isomorphismus

$$\kappa(p') \longrightarrow \kappa(p")$$

gibt, bei welchem ihre Koordinaten ineinander abgebildet werden. Eine Möglichkeit, zwei Punkte, die dasselbe Element von Spec k[X] repräsentieren, als verschieden zu betrachten, besteht darin, die Auswertungsabbildungen

$$k[X] \longrightarrow K$$

anstelle von deren Kernen zu betrachten.

Literatur

G & S

Zentrale einfache Algebren und Galois-Kohomologie,
frei nach der Monographie von Gille und Szamuely (s.u)
Notizen zu den Vorlesungen
Zahlentheorie 2 (2008-2009)
Zahlentheorie 3 (2009-2010)

Borel, Armand

[1] Linear algebraic groups, Notes by Hyman Bass, Columbia University, W. A. Benjamin, New York - Amsterdam 1969.

Cassels, J.W.S., Fröhlich, A.

[1] Algebraisc number theory, Proceedings of an instructional conference organized by the London Mathematical Society, Academic Press, London and New York 1967.

Gille, Ph., Szamuely, T.

[1] Central simple algebras and Galois cohomolgy, Cambridge University Press, 2006.

Gruenberg, Karl, W.

[1] Profinite groups, in Algebraic Number Theory (J.W.S. Cassels and A.Fröhlich, eds), Academic Press, London 1967, 116-127.

Serre, Jean-Pierre

[1] Cohomologie Galoisienne, Springer, Berlin 1964

Voevodsky, Vladimir

[1] Motivic cohomology with $\mathbb{Z}/2$-coefficients, Publ. Math. Inst. Hautes Études Sci 98 (2003), 59-104.

Inhalt

Index

—G—

—H—

—I—

—K—

—L—

—M—

—N—

—O—

—P—

—Q—

—R—

—S—

—T—

—V—

—W—

—Z—