Brauergruppen
– Arbeitsversion –

Prof. Dr. Ina Kersten

3. März 2005

Inhaltsverzeichnis

Sei K ein Körper.

0 Worum geht es?

In der Algebra-Vorlesung haben wir endliche Körpererweiterungen von K studiert.

Beispiel. $K = \mathbb{R}$. Es ist $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$ eine Körpererweiterung von $\mathbb{R}$ vom Grad 2, wobei $\{1, i\}$ mit $i^2 = -1$ eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum ist. Bis auf Isomorphie ist $\mathbb{C}$ die einzige endliche Körpererweiterung von $\mathbb{R}$.

Probleme.

1) Wie sehen die endlichen nicht-kommutativen Körpererweiterungen von K aus?

2) Eine Übersicht über alle solche zu bekommen.
Die Brauergruppe $\mathrm{Br}(K)$ gibt Auskunft.

Der Quaternionenschiefkörper

Dieser wurde von Hamilton 1843 entdeckt. Sei

$$\mathbb{H} := \left\{ \begin{pmatrix} z & u \\ -\overline{u} & \overline{z} \end{pmatrix} \mid z, u \in \mathbb{C} \right\} \subset \mathrm{M}_{2\times 2}(\mathbb{C}),$$

wobei $\overline{z} = a - bi$ mit $a, b \in \mathbb{R}$ die zu $z = a + bi$ konjugiert komplexe Zahl ist. Dann gelten:

(1) $\mathbb{H}$ ist ein Ring bezüglich Matrizenaddition und -multiplikation mit Einselement $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

(2) $\mathbb{H}$ ist nicht kommutativ, denn z.B.

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

(3) Jedes Element $h \neq \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ ist invertierbar in $\mathbb{H}$.
Sei dazu $h = \begin{pmatrix} z & u \\ -\overline{u} & \overline{z} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ in $\mathbb{H}$. Dann ist $\det(h) = z\overline{z} + u\overline{u} \neq 0$ und $h^{-1} = \frac{1}{\det h}\begin{pmatrix} \overline{z} & -u \\ \overline{u} & z \end{pmatrix}$.
Der Ring $\mathbb{H}$ ist also ein „Schiefkörper“.

(4) Es ist $\mathbb{R}$ das *Zentrum* von $\mathbb{H}$, d.h. es ist

$$\mathbb{R} = \{r \in \mathbb{H} \mid hr = rh \; \forall \, h \in \mathbb{H}\}.$$

Hierbei ist $\mathbb{R}$ durch $\mathbb{R} \hookrightarrow \mathbb{H}$, $r \longmapsto \left(\begin{smallmatrix} r & 0 \\ 0 & r \end{smallmatrix}\right)$, in $\mathbb{H}$ eingebettet. Man sagt, $\mathbb{H}$ sei eine zentrale $\mathbb{R}$-Algebra.

(5) $\mathbb{H}$ ist als $\mathbb{R}$-Vektorraum vierdimensional mit Basis

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

(6) Man kann den Körper $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ wie folgt in $\mathbb{H}$ einbetten:

$$\mathbb{C} \hookrightarrow \mathbb{H}, \; a + bi \longmapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Dann ist $\mathbb{C}$ ein maximaler (kommutativer) Teilkörper von $\mathbb{H}$. Die maximalen Teilkörper spielen bei Problem 1) eine wesentliche Rolle.

(7) Wir werden zeigen: $\mathbb{H}$ ist bis auf Isomorphie die einzige endliche nichtkommutative Körpererweiterung von $\mathbb{R}$. Daher besteht die Brauergruppe $\mathrm{Br}(\mathbb{R})$ aus zwei Elementen $[\mathbb{R}]$ und $[\mathbb{H}]$, also $\mathrm{Br}(\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$. Dabei besteht $[\mathbb{R}]$ aus allen Matrizenringen $\mathrm{M}_{n\times n}(\mathbb{R})$, $n \geq 1$ und $[\mathbb{H}]$ aus allen Matrizenringen $\mathrm{M}_{n\times n}(\mathbb{H})$, $n \geq 1$.

Problem.

3) $\mathrm{Br}(K) = {?}$ Dies ist im allgemeinen noch ungelöst.
$\mathrm{Br}(K)$ ist z.B. für $K = \mathbb{Q}$ oder allgemeiner für einen Zahlkörper K bekannt. $\mathrm{Br}(\mathbb{R})$ ist wie in 0.1 (7) gegeben. Es sind $\mathrm{Br}(\mathbb{C}) = \{[\mathbb{C}]\}$ und $\mathrm{Br}(\mathbb{F}_q) = \{[\mathbb{F}_q]\}$ trivial.

Um die genannten Probleme zu lösen, studiert man zentrale einfache K-Algebren A. Dabei bedeutet zentral, daß

$$\mathcal{Z}(A) := \{a \in A \mid ab = ba \; \forall \, b \in A\} = K$$

gilt, und einfach, daß A keine zweiseitigen Ideale außer (0) und (1) enthält. Wir werden zeigen:

Satz (Struktursatz von Wedderburn (1907)). *Sei A eine zentrale einfache K-Algebra mit $\dim_K A < \infty$.*
Dann gilt $A \simeq \mathrm{M}_{n\times n}(D)$ mit einem geeigneten Schiefkörper D. Dabei sind n und bis auf Isomorphie auch D durch A eindeutig bestimmt.

Richard Brauer führte eine Äquivalenzrelation

$$\boxed{\mathrm{M}_{n\times n}(D) \sim \mathrm{M}_{m\times m}(D')} \quad :\Longleftrightarrow \quad \boxed{D \simeq D'}$$

ein und zeigte, daß die Äquivalenzklassen von endlich dimensionalen zentralen einfachen K-Algebren eine abelsche Gruppe bilden.

Bemerkung. Dies inspirierte Witt, seinen Ring der Äquivalenzklassen von quadratischen Formen einzuführen.
Für eine quadratische Form $q = \sum\limits_{i=1}^{n} a_i X_i^2 =: \langle a_1, \dots, a_n \rangle$ mit $a_i \in K^*$ gilt im Fall $\operatorname{char} K \neq 2$:

$$q \simeq \underbrace{\langle 1, -1 \rangle \perp \dots \perp \langle 1, -1 \rangle}_{i \text{ Summanden}} \perp q_{\mathrm{an}} \,,$$

wobei der Wittindex i und bis auf Isometrie die anisotrope Form q_{an} durch q eindeutig bestimmt sind (In der Analogie entsprechen sich der Schiefkörper D und die Form q_{an}). Witt fand die Analogie merkwürdig. Mit Hilfe der neueren Theorie der einfachen algebraischen Gruppen wird sie einleuchtend.

Unter anderem werden wir in der Vorlesung zeigen:

- Die Brauergruppe $\mathrm{Br}(K)$ kann als eine zweite „Kohomologiegruppe“ bezüglich der sogenannten Galoiskohomologie interpretiert werden.
- Die Brauergruppe ist eine abelsche „Torsionsgruppe“. Die Gruppenoperation wird dabei vom Tensorprodukt induziert.
- Jede zentrale einfache K-Algebra A mit $\dim_K A < \infty$ besitzt einen galoisschen „Zerfällungskörper“ L über K, d.h. es gilt $A \otimes_K L \simeq \mathrm{M}_{n\times n}(L)$ mit $n^2 = \dim_K A$.
- Die Lösung der Probleme 1), 2), 3) soll für einen „lokalen Körper“ vorgeführt werden.

Vereinbarung.

- In einem Ring ist stets $1 \neq 0$.
- Für jeden Ring R bezeichnet R^* die multiplikative Gruppe der invertierbaren Elemente.
- Ein *Schiefkörper* ist ein Ring, in dem jedes Element $\neq 0$ invertierbar ist.
- Ein *Körper* ist ein kommutativer Schiefkörper.

Teil I
Einfache Algebren

Sei K ein Körper.

1 Struktursatz von Wedderburn

1.1 Algebren

Definition.

(i) Ein Ring A heißt *K-Algebra*, falls auf A eine K-Vektorraumstruktur gegeben ist, die

$$(\lambda a)b = a(\lambda b) = \lambda(ab) \;\forall\, \lambda \in K\,,\; a, b \in A$$

erfüllt und deren Addition die des Ringes A ist. Die Dimension $\dim_K A$ einer K-Algebra A ist die Dimension von A als K-Vektorraum.

(ii) Ein *Schiefkörper A über K* ist eine K-Algebra, in der jedes Element $\neq 0$ invertierbar ist. Man spricht dann auch von einer *Divisionsalgebra*, und bezeichnet diese mit dem Buchstaben D.

Bemerkung. Ist A eine K-Algebra, so ist $K \longrightarrow A\,,\; \lambda \longmapsto \lambda \cdot 1$, injektiv, und deswegen fassen wir diese Abbildung oft als Inklusion auf.

Beispiel. Der Ring $\mathrm{M}_{n\times n}(K)$ aller $n \times n$-Matrizen mit Einträgen in K ist eine n^2-dimensionale K-Algebra mit Basis e_{ij}, $1 \le i, j \le n$, wobei die Matrix e_{ij} aus Nullen besteht, abgesehen von einer 1 an der Stelle (i, j). Ist $n \ge 2$, so ist $\mathrm{M}_{n\times n}(K)$ nicht-kommutativ und kein Schiefkörper (z.B. $e_{11}e_{22} =$ Nullmatrix).

1.2 Oppositioneller Ring

Sei A ein Ring. Der *oppositionelle Ring* A^{op} von A ist wie folgt definiert:
Es ist $A^{\mathrm{op}} = A$ als additive Gruppe, und für die Multiplikation in A^{op} gilt:

$$A^{\mathrm{op}} \times A^{\mathrm{op}} \longrightarrow A^{\mathrm{op}},\; (a, b) \longmapsto b \cdot a \text{ (Multiplikation in } A)$$

(Dem Produkt ab in A entspricht das Produkt ba in A^{op}).

1.3 Der Endomorphismenring über einem Schiefkörper

Sei D ein Schiefkörper, und sei V ein D-Linksvektorraum. Dann ist

$$\operatorname{End}_D V := \{\varphi\colon V \longrightarrow V \mid \varphi \text{ ist } D\text{-linear}\}$$

ein Ring mit Addition $(\varphi+\psi)(v) = \varphi(v)+\psi(v)\ \forall\, v \in V$ und Multiplikation $\varphi\psi = \varphi \circ \psi$ (Hintereinanderausführung).
Sei $\dim_D V < \infty$ und $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V über D.
Jedem $\varphi \in \operatorname{End}_D V$ mit $\varphi(v_j) = \sum\limits_{i=1}^{n} a_{ij} v_i$ und $a_{ij} \in D$ ordnen wir die Matrix $\mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\varphi) = (a_{ij})_{1 \le i,j \le n}$ zu. Dann ist

$$\operatorname{End}_D V \longrightarrow \mathrm{M}_{n\times n}(D^{\mathrm{op}})\,,\ \varphi \longmapsto \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\varphi)\,,$$

ein Ringisomorphismus, denn mit $\psi(v_k) = \sum\limits_{j=1}^{n} b_{jk} v_j$ gilt

$$\begin{aligned}(\varphi\circ\psi)(v_k) &= \sum_{j=1}^{n} b_{jk}\varphi(v_j) = \sum_{j=1}^{n} b_{jk}\left(\sum_{i=1}^{n} a_{ij}v_i\right)\\ &= \sum_{i=1}^{n}\left(\sum_{j=1}^{n} a_{ij}b_{jk}\right) v_i\,,\end{aligned}$$

wobei $a_{ij},\ b_{jk} \in D^{\mathrm{op}}$.

1.4 Minimale Linksideale

Sei A ein Ring, und sei I eine additive Untergruppe von A. Dann heißt I ein *Linksideal* (bzw. *Rechtsideal*), falls $ax \in I$ (bzw. $xa \in I$) $\ \forall\, x \in I,\ a \in A$, und I heißt *zweiseitiges Ideal*, falls I sowohl Links- als auch Rechtsideal ist. Ein Linksideal I in A heißt *minimal*, falls I außer (0) und I keine Linksideale enthält.

Bemerkung. In jeder endlich-dimensionalen K-Algebra A gibt es minimale Linksideale $\neq 0$. (Ist $A \supsetneqq I_1 \supsetneqq \cdots \supsetneqq I_n$ eine Kette von Linksidealen, so gilt $\dim_K A \ge n$).

Satz. *Sei $A = \mathrm{M}_{n\times n}(D)$ mit einem Schiefkörper D. Dann ist das Linksideal*

$$L_i := \left\{ \begin{pmatrix} 0 & \dots & 0 & * & 0 & \dots & 0\\ \vdots & & \vdots & \vdots & \vdots & & \vdots\\ 0 & \dots & 0 & * & 0 & \dots & 0 \end{pmatrix} \in A \right\}$$

mit Einträgen $\neq 0$ höchstens in der i-ten Spalte minimal für jedes $i = 1, \dots, n$.

Beweis. Sei $x \in L_i$ nicht die Nullmatrix. Dann ist $x = \sum_{j=1}^{n} e_{ji} d_j$ mit $d_j \in D$, wobei e_{ji} die Matrix mit lauter Nullen außer einer Eins an der Stelle (j,i) ist, und es gibt ein k mit $d_k \neq 0$. Es folgt

$$\underbrace{\left(d_k^{-1} e_{kk}\right)}_{\in L_i} x = e_{ki} \in L_i \,.$$

Da e_{ki} das Linksideal L_i erzeugt, erzeugt auch x das Linksideal L_i. □

1.5 Einfache Ringe

Sei A ein Ring. Dann ist A *einfach,* falls A außer (0) und (1) keine zweiseitigen Ideale enthält. Eine K-Algebra heißt einfach, falls sie einfach als Ring ist.

Beispiel. Jeder Schiefkörper D ist ein einfacher Ring, denn ist I ein zweiseitiges Ideal in D und $0 \neq x \in I$, so ist $x^{-1}x = xx^{-1} = 1$ in I, also $I = D$.

Allgemeiner gilt folgender

Satz. *Ist D ein Schiefkörper, so ist der Ring $\mathrm{M}_{n\times n}(D)$ einfach für jedes $n \geq 1$.*

Beweis. Sei e_{ij} wieder die Matrix mit lauter Nullen außer einer Eins an der Stelle (i,j). Sei $x = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{M}_{n\times n}(D)$. Dann gilt

$$\boxed{a_{ij} e_{rr} = e_{ri} x e_{jr}} \qquad \text{für } 1 \leq i,j \leq n \,.$$

Ist x in einem zweiseitigen Ideal I enthalten und x nicht die Nullmatrix, so gibt es ein Paar (i,j) mit $a_{ij} \neq 0$, und es ist

$$e_{rr} = a_{ij}^{-1} e_{ri} x e_{jr} \text{ in } I \qquad \forall\, r = 1,\ldots,n \,.$$

Es folgt $E_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = \sum_{r=1}^{n} e_{rr} \in I$, und also $I = \mathrm{M}_{n\times n}(D)$. □

1.6 Einfache Moduln

Sei A ein Ring. Falls nichts anderes gesagt ist, verstehen wir unter einem A-Modul einen A-Linksmodul wie in Algebra 10.1 definiert.
Ein A-Modul M heißt *einfach*, falls M keine Untermoduln außer (0) und M enthält.

Beispiel. Jedes minimale Linksideal ist ein einfacher A-Modul.

Lemma (Schur). *Ist M ein einfacher A-Modul, so ist der Endomorphismenring* $\operatorname{End}_A M$ *ein Schiefkörper.*

Beweis. Sei $f\colon M \longrightarrow M$ ein Endomorphismus, der nicht die Nullabbildung ist. Dann ist $\operatorname{kern} f \neq M$ und $\operatorname{bild} f \neq (0)$. Da M einfach ist, folgt $\operatorname{kern} f = (0)$ und $\operatorname{bild} f = M$. Also existiert f^{-1} in $\operatorname{End}_A M$. □

Satz. *Sei $A = \mathrm{M}_{n\times n}(D)$ mit einem Schiefkörper D. Dann sind alle einfachen A-Moduln $\neq (0)$ und insbesondere alle minimalen Linksideale $\neq (0)$ in A isomorph.*

Beweis. Es ist $A = \sum\limits_{i=1}^{n} L_i$, wobei die Linksideale L_i nach Satz 1.4 minimal sind. Sei $\mathcal{N}$ ein einfacher A-Modul $\neq (0)$. Dann ist ist $(0) \neq \mathcal{N} = A\mathcal{N} = \left(\sum\limits_{i=1}^{n} L_i\right)\mathcal{N}$. Also gibt es ein i mit $L_i\mathcal{N} \neq (0)$. Es gibt dann auch ein $x \in \mathcal{N}$, so daß die Rechtsmultiplikation

$$r_x\colon L_i \longrightarrow \mathcal{N}\,,\ \alpha \longmapsto \alpha x\,,$$

nicht die Nullabbildung ist. Da $\mathcal{N}$ und L_i einfache Moduln sind, ist r_x ein A-Modulisomorphismus (analog wie beim Beweis des Lemmas von Schur). □

1.7 Existenzsatz

Satz. *Sei A eine endlich-dimensionale einfache K-Algebra. Dann gibt es eine K-Algebraisomorphie*

$$A \simeq \mathrm{M}_{n\times n}(D)$$

mit einem Schiefkörper D über K und einem $n \in \mathbb{N}$.

Beweis. Nach Bemerkung 1.4 besitzt A ein minimales Linksideal $I \neq (0)$, und nach 1.6 ist

$$\boxed{D := \operatorname{End}_A I}$$

ein Schiefkörper (über K). Betrachte I als D-Linksvektorraum vermöge

$$\boxed{f \cdot x := f(x) \quad \forall\, f \in D,\ x \in I}\,.$$

Dann gelten:

(1) $\dim_D I < \infty$, da $\dim_K I < \infty$ nach Voraussetzung.

(2) Die Linksmultiplikation $\ell_a\colon I \longrightarrow I\,,\ x \longmapsto ax$, ist D-linear für jedes $a \in A$, denn es gilt $\ell_a(f\cdot x) = af(x) = f(ax) = f \cdot \ell_a(x)$.

(3) Die Abbildung $\ell\colon A \longrightarrow \operatorname{End}_D I\,,\ a \longmapsto \ell_a\,$, ist ein K-Algebrahomomorphismus. Dieser ist injektiv, denn $\ker \ell$ ist ein zweiseitiges Ideal $\neq (1)$ in A, und A ist ein einfacher Ring.
Es ist nur noch zu zeigen, daß ℓ surjektiv ist, denn dann folgt

$$A \underset{(3)}{\simeq} \operatorname{End}_D I \underset{1.3}{\simeq} \mathrm{M}_{n\times n}(D^{\mathrm{op}}) \qquad \text{mit } n = \dim_D I$$

und mit dem Schiefkörper D^{op}.
Um die Surjektivität von ℓ zu zeigen, genügt es zu zeigen, daß $\ell(A)$ ein Linksideal in $\operatorname{End}_D I$ ist (denn $\ell(A)$ enthält $\ell(1) = \ell_1 = 1_{\operatorname{End}_D I}$, und also folgt dann $\ell(A) = \operatorname{End}_D I$). Wir zeigen zunächst

(4) **Behauptung:** $\ell(I)$ ist ein Linksideal in $\operatorname{End}_D I$.

Beweis. Es ist $\ell(I) = \{\ell_a\colon I \longrightarrow I \mid a \in I\}$.
Zu zeigen: $\psi \circ \ell_a \in \ell(I)\ \forall\, \psi \in \operatorname{End}_D I,\ a \in I$.
Für alle $x \in I$ gilt

$$\begin{aligned}
(\psi \circ \ell_a)(x) &= \psi(ax) && \text{nach Definition von } \ell_a\\
&= \psi(r_x \cdot a)\,, && \text{wobei } r_x\colon I \longrightarrow I\,,\ a \longmapsto ax\,,\\
& && \text{die Rechtsmultiplikation mit } x \text{ ist}\\
&= r_x \cdot \psi(a)\,, && \text{da } r_x \in D \text{ und } \psi\ D\text{-linear}\\
&= \psi(a)x && \text{nach Definition von } r_x\\
&= \ell_{\psi(a)}(x)\,,
\end{aligned}$$

also $\psi \circ \ell_a = \ell_{\psi(a)} \in \ell(I)$. □

(5) **Behauptung:** $\ell(A) = \ell(I)\ell(A)$.

Beweis. Es ist IA ein zweiseitiges Ideal $\neq (0)$ in A, und also $IA = A$, da A einfach ist. Da ℓ multiplikativ ist, folgt (5). □

Es folgt nun

$$\begin{aligned}
(\operatorname{End}_D I)\ell(A) &= (\operatorname{End}_D I)\ell(I)\ell(A) && \text{nach}(5)\\
&= \ell(I)\ell(A) && \text{nach}(4)\\
&= \ell(A) && \text{nach}(5),
\end{aligned}$$

und also ist $\ell(A)$ ein Linksideal in $\operatorname{End}_D I$. □

1.8 Ein Hilfssatz

Lemma. *Sei* $A = \mathrm{M}_{n\times n}(D)$ *mit einem Schiefkörper* D *und einem* $n \in \mathbb{N}$. *Dann ist*

$$D^n := \left\{ \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} \mid d_1, \dots, d_n \in D \right\}$$

ein einfacher A*-Modul, und es gibt eine Ringisomorphie*

$$D^{\mathrm{op}} \simeq \mathrm{End}_A(D^n)$$

(Dabei gilt bezüglich Matrizenmultiplikation $xv \in D^n \; \forall \, x \in A$ *und* $v \in D^n$*).*

Beweis. D^n ist einfach, da D^n zu den in Satz 1.4 eingeführten einfachen A-Moduln L_i isomorph ist. Da D^n ein D-Rechtsvektorraum ist, gibt es einen Ringhomomorphismus

$$\boxed{\varphi\colon D^{\mathrm{op}} \longrightarrow \mathrm{End}_A D^n, \; d \longmapsto r_d},$$

wobei r_d die Rechtsmultiplikation mit d ist. Da D^{op} ein Schiefkörper ist, ist φ injektiv.
Zu zeigen: φ ist surjektiv. Sei $f \in \mathrm{End}_A D^n$, und sei $(e_1, \dots, e_n)$ die Standardbasis von D^n. Dann ist $f(e_1) = e_1 d_1 + \dots + e_n d_n$ mit $d_1, \dots, d_n \in D$.
Wir zeigen: $\boxed{f = r_{d_1}}$, also $\varphi(d_1) = f$. Sei wieder e_{ij} die $n \times n$-Matrix mit lauter Nullen außer einer 1 an der Stelle (i, j). Dann gilt:

$$\begin{aligned}
f(e_1) &= f(e_{11}e_1), && \text{da } e_{11}e_1 = e_1 \\
&= e_{11}f(e_1), && \text{da } f \; A\text{-linear} \\
&= e_1 d_1, && \text{da } e_{11}e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \text{ für } j > 1\,, \\
\text{und } f(e_j) &= f(e_{j1}e_1), && \text{da } e_j = e_{j1}e_1 \\
&= e_{j1}f(e_1), && \text{da } f \; A\text{-linear} \\
&= e_{j1}e_1 d_1\,, && \text{wie eben gezeigt} \\
&= e_j d_1, && \text{da } e_{j1}e_1 = e_j \text{ für } j = 2, \dots, n\,.
\end{aligned}$$

Da f durch die Werte $f(e_1), \dots, f(e_n)$ eindeutig bestimmt ist,
folgt $f = r_{d_1}$. □

1.9 Eindeutigkeitssatz

Satz. *Sind D und E Schiefkörper und gilt*

$$\mathrm{M}_{n\times n}(D) \simeq \mathrm{M}_{m\times m}(E)\,,$$

so ist $D \simeq E$ und $m = n$.

Beweis. Seien $A := \mathrm{M}_{n\times n}(D)$ und $B := \mathrm{M}_{m\times m}(E)$, sowie $\varphi\colon A \xrightarrow{\sim} B$ ein Ringisomorphismus. Dann ist E^m ein A-Modul vermöge

$$aw := \varphi(a)w \quad \forall\, a \in A,\ w \in E^m\,.$$

Da E^m nach 1.8 ein einfacher B-Modul ist, ist E^m auch einfach als A-Modul. Nach Satz 1.6 sind alle einfachen A-Moduln $\neq (0)$ isomorph, und es folgt

$$\begin{aligned} E^{\mathrm{op}} &\simeq \mathrm{End}_B\, E^m && \text{nach 1.8} \\ &\simeq \mathrm{End}_A\, E^m && \text{vermöge } \varphi\colon A \xrightarrow{\sim} B \\ &\simeq \mathrm{End}_A\, D^n && \text{nach Satz 1.6} \\ &\simeq D^{\mathrm{op}} && \text{nach 1.8}\,. \end{aligned}$$

Es folgt $E \simeq D$ und $m^2 = \dim_E B = \dim_D A = n^2$, also $m = n$. □

1.10 Struktursatz von Wedderburn (1907)

Satz. *Sei A eine endlich-dimensionale einfache K-Algebra. Dann gibt es genau ein $n \in \mathbb{N}$ und bis auf Isomorphie genau einen Schiefkörper D über K so, daß $A \simeq \mathrm{M}_{n\times n}(D)$ gilt.*

Beweis. folgt direkt aus 1.7 und 1.9. □

2 Zentrum und Zentralisator

2.1 Zentrale Algebren

Für einen Ring A ist das *Zentrum* $\mathcal{Z}(A)$ definiert als

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

Dann ist $\mathcal{Z}(A)$ ein kommutativer Unterring von A. Ist A eine K-Algebra, so gilt $K \subset \mathcal{Z}(A)$ nach Definition 1.1. Eine K-Algebra A heißt *zentral*, falls $K = \mathcal{Z}(A)$ gilt.

2.2 Das Zentrum eines Matrizenringes

Satz. *Sei D ein Schiefkörper. Dann ist das Zentrum $\mathcal{Z}(D)$ ein Körper, und die Inklusion*

$$\mathcal{Z}(D) \hookrightarrow \mathcal{Z}(\mathrm{M}_{n\times n}(D)),\; x \longmapsto xE_n\,,$$

ist surjektiv für alle $n \in \mathbb{N}$. Also gilt $\mathcal{Z}(\mathrm{M}_{n\times n}(D)) = \mathcal{Z}(D)$.

Beweis. Sei $x \neq 0$ in $\mathcal{Z}(D)$. Für $d \neq 0$ in D ist dann

$$\begin{aligned} dx^{-1} &= (xd^{-1})^{-1}, && \text{denn } (xd^{-1})(dx^{-1}) = 1 \text{ in } D \\ &= (d^{-1}x)^{-1}, && \text{denn } x \in \mathcal{Z}(D) \\ &= x^{-1}d, && \text{denn } (d^{-1}x)(x^{-1}d) = 1 \text{ in } D, \end{aligned}$$

also $x^{-1} \in \mathcal{Z}(D)$. Daher ist $\mathcal{Z}(D)$ ein Körper.
Sei $A = \mathrm{M}_{n\times n}(D)$, und sei $a = (a_{ij})_{1\le i,j\le n} \in \mathcal{Z}(A)$. Wir zeigen, daß a_{11} Urbild von a ist.
Sei e_{ij} die Matrix mit lauter Nullen außer einer Eins an der Stelle (i,j). Für $1 \le i,j \le n$ gilt dann $e_{ij}a = ae_{ij}$, da $a \in \mathcal{Z}(A)$.
Es folgt $a_{ii} = a_{jj}\;\forall\, i,j$ und $a_{ij} = 0$ für $i \neq j$, also

$$a = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{11} \end{pmatrix} = a_{11} \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

Es ist $a_{11} \in \mathcal{Z}(D)$, da $a \in \mathcal{Z}(A)$. □

2.3 Das Zentrum einer einfachen Algebra

Satz. *Sei A eine endlich-dimensionale einfache K-Algebra. Dann ist das Zentrum $\mathcal{Z}(A)$ ein Körper, der K enthält.*

Beweis. Nach 1.7 ist $A \simeq \mathrm{M}_{n\times n}(D)$ mit einem Schiefkörper D und einem $n \in \mathbb{N}$. Aus 2.2 folgt, daß $\mathcal{Z}(A)$ ein Körper ist. Mit Hilfe von Bemerkung 1.1 erhalten wir $K \hookrightarrow \mathcal{Z}(A)$. □

2.4 Definition des Zentralisators

Sei A ein Ring, und sei A' ein Unterring von A. Dann ist der *Zentralisator von A' in A* definiert durch

$$\boxed{\mathcal{Z}_A(A') := \{a \in A \mid a'a = aa' \; \forall\, a' \in A'\}}\,.$$

Es ist $\mathcal{Z}_A(A) = \mathcal{Z}(A)$ gerade das Zentrum von A.

2.5 Der Zentralisator eines Tensorproduktes

Satz. *Gegeben seien K-Algebren A, A', B, B' mit $A' \subset A$ und $B' \subset B$. Dann ist*

$$\boxed{\mathcal{Z}_{A\otimes_K B}(A' \otimes_K B') = \mathcal{Z}_A(A') \otimes_K \mathcal{Z}_B(B')}\,.$$

Insbesondere gilt:

$$\mathcal{Z}(A \otimes_K B) = \mathcal{Z}(A) \otimes_K \mathcal{Z}(B)\,.$$

Beweis. „$\supset$“: Sei $x \in \mathcal{Z}_A(A') \otimes_K \mathcal{Z}_B(B')$, also $x = \sum\limits_i^{\text{endl.}} a_i \otimes b_i$ mit $a_i \in \mathcal{Z}_A(A')$ und $b_i \in \mathcal{Z}_B(B')$.

Zu zeigen: $yx = xy \;\forall\, y \in A' \otimes_K B'$. Für $y = \sum\limits_j^{\text{endl.}} a'_j \otimes b'_j$ mit $a'_j \in A'$ und $b'_j \in B'$ folgt

$$yx = \sum_{i,j} a'_j a_i \otimes b'_j b_i = \sum_{i,j} a_i a'_j \otimes b_i b'_j = xy\,.$$

Also gilt $x \in \mathcal{Z}_{A\otimes_K B}(A' \otimes_K B')$.

„$\subset$“: Sei $x \in \mathcal{Z}_{A\otimes_K B}(A' \otimes_K B')$. Zu zeigen: $x = \sum\limits_i^{\text{endl.}} c_i \otimes b_i$ mit $c_i \in \mathcal{Z}_A(A')$ und $b_i \in \mathcal{Z}_B(B')$.

Sei $(e_j)_{j\in J}$, wobei J eine Indexmenge sei, eine Basis von B über K. Nach Algebra 10.11 gilt dann $A \otimes_K B \ni x = \sum_{j\in J} a_j \otimes e_j$ mit eindeutig bestimmten $a_j \in A$, die Null sind bis auf endlich viele. Für alle $a \in A'$ folgt

$$\begin{aligned}\sum_j aa_j \otimes e_j &= (a \otimes 1)x = x(a \otimes 1)\,, \qquad \text{da } x \in \mathcal{Z}_{A\otimes_K B}(A' \otimes_K B')\\ &= \sum_j a_j a \otimes e_j\,.\end{aligned}$$

Wegen der Eindeutigkeit der Darstellung folgt $aa_j = a_j a \; \forall \, j$, und also $a_j \in \mathcal{Z}_A(A') \; \forall \, j$.
Wähle eine Basis $(c_i)_{i \in I}$ von $\mathcal{Z}_A(A')$ über K und schreibe jedes a_j als K-Linearkombination der c_i. Dann folgt $c_i \in \mathcal{Z}_A(A')$ und $x = \sum\limits_i c_i \otimes b_i$ mit eindeutig bestimmten $b_i \in B$ (vgl. Algebra 10.11).
Für jedes $b \in B'$ folgt analog wie oben

$$\sum c_i \otimes bb_i = (1 \otimes b)x = x(1 \otimes b) = \sum c_i \otimes b_i b \,,$$

und also $b_i \in \mathcal{Z}_B(B') \; \forall \, i$.

□

2.6 Tensorprodukt von einfachen Algebren

Das Tensorprodukt zweier einfacher K-Algebren ist nicht notwendig eine einfache K-Algebra. Z.B. ist $\mathbb{C}$ eine einfache $\mathbb{R}$-Algebra, aber $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ ist nicht einfach, (denn $z = i \otimes 1 + 1 \otimes i$ mit $i^2 = -1$ erzeugt ein echtes Ideal $\neq (0)$ in $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$, da $\underbrace{z}_{\neq 0}(\underbrace{i \otimes 1 - 1 \otimes i}_{\neq 0}) = 0$ gilt).
Es gilt aber der

Satz. *Sind A, B einfache K-Algebren, und ist wenigstens eine der beiden zentral, so ist $A \otimes_K B$ eine einfache K-Algebra.*

Beweis. Da $A \otimes_K B \simeq B \otimes_K A$ gilt, können wir ohne Einschränkung annehmen, daß A zentral ist. Sei $I \neq (0)$ ein zweiseitiges Ideal in $A \otimes_K B$.
Zu zeigen: $I = A \otimes_K B$. Jedes $x \neq 0$ in I läßt sich schreiben als

$$\boxed{x = \sum_{i=1}^{m} a_i \otimes b_i}$$

mit eindeutig bestimmten $a_i \in A$ und linear unabhängigen $b_1, \ldots, b_m \in B$, vgl. Algebra 10.11.
Wähle ein $x \neq 0$ in I mit kleinstmöglichem $m \in \mathbb{N}$. Ohne Einschränkung können wir annehmen, daß $a_1 = 1$ gilt, denn Aa_1A ist ein zweiseitiges Ideal $\neq (0)$ in A, also $Aa_1A = A$, da A einfach ist, und daher gibt es $c_j, c_j' \in A$ mit $1 = \sum\limits_j^{\text{endl.}} c_j a_1 c_j'$, und mit x ist auch

$$0 \neq x' := \sum_i^{\text{endl.}} (c_j \otimes 1) x (c_j' \otimes 1) = \sum_{i=1}^{m} \Bigg(\sum_j c_j a_i c_j' \Bigg) \otimes b_i \in I \,.$$

Behauptung. $m = 1$.

Beweis. Angenommen, $m > 1$. Dann ist $a_2 \in A \setminus K$, denn andernfalls wäre

$$a_1 \otimes b_1 + a_2 \otimes b_2 = 1 \otimes b_1 + 1 \otimes a_2 b_2 = 1 \otimes (b_1 + a_2 b_2)\,,$$

und man hätte eine Darstellung von x mit weniger als m Summanden im Widerspruch zur Minimalität von m. Da A zentral ist, gibt es also ein $z \in A$ mit $a_2 z \neq z a_2$. Da I ein zweiseitiges Ideal in $A \otimes_K B$ ist, enthält I das Element

$$\begin{aligned}(z \otimes 1)x - x(z \otimes 1) &= \sum_{i=1}^{m} z a_i \otimes b_i - \sum_{i=1}^{m} a_i z \otimes b_i \\ &\underset{a_1=1}{=} (\underbrace{z \cdot 1 - 1 \cdot z}_{=0}) \otimes b_1 + (\underbrace{z a_2 - a_2 z}_{\neq 0}) \otimes b_2 \\ &\quad + \sum_{i=3}^{m} (z a_i - a_i z) \otimes b_i\,.\end{aligned}$$

Dies ist ungleich 0, da $b_1, \ldots, b_m$ linear unabhängig sind, und es hat eine kürzere Länge als x im Widerspruch zur Minimalität von m. □

Es ist also $x = 1 \otimes b_1 \neq 0$ in I. Da B einfach ist, ist $B b_1 B = B$ und also $1 = \sum_{j}^{\text{endl.}} d_j b_1 d'_j$ mit $d_j, d'_j \in B$.
Dann ist mit $x = 1 \otimes b_1$ auch

$$\sum_j (1 \otimes d_j)(1 \otimes b_1)(1 \otimes d'_j) = 1 \otimes 1 \in I\,,$$

und es folgt $I = A \otimes_K B$. □

2.7 Tensorprodukt von zentralen einfachen Algebren

Satz. *(a) Das Tensorprodukt endlich vieler zentraler K-Algebren ist eine zentrale K-Algebra.*

(b) Das Tensorprodukt endlich vieler zentraler einfacher K-Algebren ist eine zentrale einfache K-Algebra.

Beweis. Seien A, B zentrale K-Algebren. Dann ist

$$\mathcal{Z}(A \otimes_K B) \underset{2.5}{=} \mathcal{Z}(A) \otimes_K \mathcal{Z}(B) = K \otimes_K K = K \text{(vgl. 2.1 und Algebra 10.9)}\,.$$

Sind A, B zusätzlich einfach, so ist $A \otimes_K B$ eine einfache K-Algebra nach 2.6. Mit einer Induktion erhält man nun den Satz. □

2.8 Beispiele für zentrale einfache K-Algebren

1) $\mathrm{M}_{n\times n}(K)$ für jedes $n \in \mathbb{N}$ (insbesondere auch K selbst).

2) $\mathrm{M}_{n\times n}(D)$ für jeden zentralen Schiefkörper D über K und jedes $n \in \mathbb{N}$ nach Satz 1.5 und 2.2.

3 Definition der Brauergruppe

Sei weiterhin K ein Körper.

3.1 Nützlicher Hilfssatz

Lemma. *Sei A ein einfacher Ring, und sei B ein beliebiger Ring. Dann ist jeder Ringhomomorphismus $f\colon A \longrightarrow B$ injektiv.*

Beweis. $\ker f$ ist ein zweiseitiges Ideal in A. Da $f(1) = 1 \neq 0$ ist, ist $\ker f \neq A$. Also folgt $\ker f = (0)$, da A einfach ist, vgl. Definition 1.5. □

Wir werden das Lemma meist auf K-Algebren anwenden.

3.2 Definition einer Azumaya-Algebra

Wir nennen eine endlich-dimensionale, zentrale, einfache K-Algebra eine *Azumaya-Algebra über K*. Dieser Begriff wird in der neueren Literatur häufig benutzt – einmal wegen der kürzeren Sprechweise und zum anderen, weil G. Azumaya mit seiner Arbeit „On maximally central algebras" Nagoya Math. J.2 (1951) den Grundstein für die Definition der Brauergruppe eines kommutativen Ringes legte.

3.3 Das Tensorprodukt von A und A^{op}

Sei A eine K-Algebra. Mit Hilfe der universellen Eigenschaft des Tensorprodukts (vgl.Algebra 10.8) zeigt man, daß es eine K-lineare Abbildung

$$\begin{aligned} \varrho\colon A \otimes_K A^{\mathrm{op}} &\longrightarrow \mathrm{End}_K A \\ a \otimes b &\longmapsto \begin{cases} A \longrightarrow A, \\ x \longmapsto axb \end{cases} \end{aligned}$$

gibt, die $\forall\, a \in A,\ b \in A^{\mathrm{op}}$ erfüllt. Es ist $\varrho(1 \otimes 1) = \mathrm{id}$, und ϱ ist multiplikativ, denn für alle $a, a', x \in A$ und $b, b' \in A^{\mathrm{op}}$ gilt

$$\varrho((a \otimes b)(a' \otimes b'))(x) = (\varrho(aa' \otimes b'b))(x) = aa'xb'b\,,$$
$$\varrho(a \otimes b)(\varrho(a' \otimes b')(x)) = \varrho(a \otimes b)(a'xb') = aa'xb'b\,.$$

Satz. *Für eine Azumaya-Algebra A über K ist der K-Algebrahomomorphismus*

$$\varrho\colon A \otimes_K A^{\mathrm{op}} \longrightarrow \mathrm{End}_K A\,,\ a \otimes b \longmapsto (x \longmapsto axb)\,,$$

bijektiv. Insbesondere gilt

$$\boxed{A \otimes_K A^{\mathrm{op}} \simeq \mathrm{M}_{m \times m}(K)} \quad \textit{mit } m = \dim_K A\,.$$

Beweis. Nach Satz 2.6 ist $A \otimes_K A^{\mathrm{op}}$ eine einfache K-Algebra, und daher ist ϱ nach 3.1 injektiv. Nach AGLA 4.4 und AGLA 4.7 gibt es eine K-Algebraisomorphie $\mathrm{End}_K A \simeq \mathrm{M}_{m\times m}(K)$ mit $m = \dim_K A$.
Es folgt $\dim_K(\mathrm{End}_K A) = m^2 = (\dim_K A)(\dim_K A^{\mathrm{op}}) = \dim_K(A \otimes_K A^{\mathrm{op}})$ nach Algebra 10.11(3). Also ist ϱ surjektiv nach AGLA 3.23. □

3.4 Ähnlichkeit (oder Brauer-Äquivalenz)

Seien A, B Azumaya-Algebren über K. Dann heißen A und B *ähnlich* (in Zeichen: $A \sim B$), wenn es $n, m \in \mathbb{N}$ so gibt, daß gilt:

$$\boxed{A \otimes_K \mathrm{M}_{n\times n}(K) \simeq B \otimes_K \mathrm{M}_{m\times m}(K)}\,.$$

Es ist $\sim$ eine Äquivalenzrelation auf der Menge der Isomorphieklassen, denn

$$\begin{aligned} &A \sim A \quad \text{(dabei ist } n = m = 1) \\ &A \sim B \Longrightarrow B \sim A \quad \text{klar} \\ &A \sim B,\ B \sim C \Longrightarrow A \sim C \end{aligned}$$

Beweis der Transitivität. Es gelte $A \otimes_K \mathrm{M}_{n\times n}(K) \simeq B \otimes_K \mathrm{M}_{m\times m}(K)$ und $B \otimes_K \mathrm{M}_{k\times k}(K) \simeq C \otimes_K \mathrm{M}_{\ell\times\ell}(K)$. Dann ist

$$\begin{aligned} A \otimes_K \mathrm{M}_{nk\times nk}(K) &\underset{\text{Aufgabe 10(b)}}{\simeq} A \otimes_K \mathrm{M}_{n\times n}(K) \otimes_K \mathrm{M}_{k\times k}(K) \\ &\simeq B \otimes_K \mathrm{M}_{m\times m}(K) \otimes_K \mathrm{M}_{k\times k}(K) \\ &\simeq B \otimes_K \mathrm{M}_{k\times k}(K) \otimes_K \mathrm{M}_{m\times m}(K) \\ &\simeq C \otimes_K \mathrm{M}_{\ell m\times \ell m}(K) \quad \text{nach Voraussetzung und Aufgabe 10(b)} \end{aligned}$$

□

Bemerkung. Nach 1.10 und 2.2 gibt es eindeutige Darstellungen

$$\boxed{A \simeq \mathrm{M}_{r\times r}(D)} \quad \text{und} \quad \boxed{B \simeq \mathrm{M}_{s\times s}(D')}$$

mit $r, s \in \mathbb{N}$ und zentralen Schiefkörpern D, D' über K. Es gilt

$$\boxed{A \sim B \Longleftrightarrow D \simeq D'}\,.$$

Beweis. „$\Longrightarrow$“: $A \sim B \Longrightarrow A \otimes_K \mathrm{M}_{n\times n}(K) \simeq B \otimes_K \mathrm{M}_{m\times m}(K)$
$\Longrightarrow \mathrm{M}_{nr\times nr}(D) \simeq \mathrm{M}_{sm\times sm}(D') \underset{1.9}{\Longrightarrow} D \simeq D'$. ✓

„$\Longleftarrow$“: $D \simeq D' \Longrightarrow D \otimes_K \mathrm{M}_{rs\times rs}(K) \simeq D' \otimes_K \mathrm{M}_{rs\times rs}(K)$
$\Longrightarrow A \otimes_K \mathrm{M}_{s\times s}(K) \simeq B \otimes_K \mathrm{M}_{r\times r}(K) \Longrightarrow B \sim A$.

□

Bis auf K-Algebraisomorphie gibt es also in jeder Äquivalenzklasse genau einen Schiefkörper D.

Folgerung.

$$\boxed{A \sim B} \quad \textit{und} \quad \boxed{\dim_K A = \dim_K B} \quad \Longrightarrow \quad \boxed{A \simeq B}.$$

Beweis. Ist $A \sim B$, so impliziert die Bemerkung $A \simeq \mathrm{M}_{r\times r}(D)$ und $B \simeq \mathrm{M}_{s\times s}(D)$ mit demselben Schiefkörper D, und wegen $\dim_K A = \dim_K B$ folgt $r = s$. □

3.5 Die Brauergruppe $\mathrm{Br}(K)$

Sei $[A] := \{B \mid B \sim A\}$ die Äquivalenzklasse einer Azumaya-Algebra A über K. Dann ist die Multiplikation

$$[A] \cdot [B] := [A \otimes_K B]$$

wohldefiniert, denn

$$(A \otimes_K \mathrm{M}_{n\times n}(K)) \otimes_K (B \otimes_K \mathrm{M}_{m\times m}(K)) \underset{\text{Aufgabe 10(b)}}{\simeq} A \otimes_K B \otimes_K \mathrm{M}_{nm\times nm}(K).$$

Die Multiplikation ist assoziativ, kommutativ und hat $[K]$ als Einselement. Zu jeder Klasse $[A]$ gehört nach Satz 3.3 die inverse Klasse $[A^{\mathrm{op}}] = [A]^{-1}$. Die Ähnlichkeitsklassen von Azumaya-Algebren über K bilden also eine kommutative Gruppe, genannt *Brauergruppe von* K. Wir schreiben $\mathrm{Br}(K)$.

3.6 Die Brauergruppe eines algebraisch abgeschlossenen Körpers

Satz. *Sei K algebraisch abgeschlossen, und sei D ein Schiefkörper über K mit $\dim_K D =: n < \infty$. Dann ist $D = K$. Insbesondere ist $\mathrm{Br}(K) = \{1\}$.*

Beweis. Sei $x \in D$. Dann erzeugt x nach 5.3 unten einen Körper $K(x) \subset D$. Die Körpererweiterung $K(x)$ ist algebraisch über K nach Algebra 12.2. Da K algebraisch abgeschlossen ist, folgt $K(x) = K$ für jedes $x \in D$. Also gilt $D = K$. □

3.7 Funktorielles Verhalten

Satz. *Sei L eine Körpererweiterung von K. Ist A eine Azumaya-Algebra über K, so ist $A \otimes_K L$ eine Azumaya-Algebra über L, und es gibt einen Gruppenhomomorphismus*

$$\boxed{r_{L/K}\colon\ \mathrm{Br}(K) \longrightarrow \mathrm{Br}(L)\,,\ [A] \longmapsto [A \otimes_K L]}.$$

Dabei gilt

$$\boxed{r_{L/K} = r_{L/M} \circ r_{M/K}}$$

für Körpererweiterungen $K \subset M \subset L$.

Beweis. Bette L in $A \otimes_K L$ vermöge $L \hookrightarrow A \otimes_K L$, $\lambda \longmapsto 1 \otimes \lambda$, ein. Es ist $\mathcal{Z}(A \otimes_K L) \underset{2.5}{=} \mathcal{Z}(A) \otimes_K \mathcal{Z}(L) \underset{A \text{ zentral}}{=} K \otimes_K L = L$ und also $A \otimes_K L$ eine zentrale L-Algebra. Nach Satz 2.6 ist $A \otimes_K L$ eine einfache K-Algebra und also auch eine einfache L-Algebra. Es ist $\dim_L(A \otimes_K L) \underset{\text{Aufgabe 9}}{=} \dim_K A < \infty$.
Es folgt $[A \otimes_K L] \in \mathrm{Br}(L)$.
Die Abbildung ist multiplikativ, denn es gilt

$$(A \otimes_K B) \otimes_K L \simeq (A \otimes_K L) \otimes_L (B \otimes_K L), \quad \text{vgl. Algebra 10.9}\,.$$

Setzt man hierin $B = \mathrm{M}_{n \times n}(K)$ ein, so sieht man, daß $r_{L/K}$ auch wohldefiniert ist, da $\mathrm{M}_{n \times n}(K) \otimes_K L \simeq \mathrm{M}_{n \times n}(L)$ gilt, vgl. Aufgabe 10.
Da $A \otimes_K L \simeq (A \otimes_K M) \otimes_M L$ gilt, folgt die letzte Behauptung. □

Bemerkung. Der Homomorphismus

$$r_{L/K} \colon \mathrm{Br}(K) \longrightarrow \mathrm{Br}(L)\,,\; [A] \longmapsto [A \otimes_K L]\,,$$

ist i.a. weder injektiv noch surjektiv.

Beispiel. Ist $\mathrm{Br}(K) \neq \{1\}$ und $\overline{K}$ ein algebraischer Abschluß von K , so ist $r_{\overline{K}/K} \colon \mathrm{Br}(K) \longrightarrow \mathrm{Br}(\overline{K})$ nicht injektiv nach 3.6.
Insbesondere ist $r_{\mathbb{C}/\mathbb{R}} \colon \mathrm{Br}(\mathbb{R}) \longrightarrow \mathrm{Br}(\mathbb{C})$ nicht injektiv.

Bezeichnung. $r_{L/K}$ wird *Restriktion* genannt. Ist $[A] \in \mathrm{kern}(r_{L/K})$, so heißt L *Zerfällungskörper von* A .
Es ist dann $A \otimes_K L \in [L]$ und also $A \otimes_K L \simeq \mathrm{M}_{n \times n}(L)$ mit einem $n \in \mathbb{N}$.

3.8 Charakterisierung von Azumaya-Algebren

Satz. *Sei A eine endlich-dimensionale K-Algebra. Dann sind folgende Aussagen äquivalent:*

(i) A ist eine zentrale, einfache K-Algebra.

(ii) Es gibt eine K-Algebraisomorphie $A \simeq \mathrm{M}_{m \times m}(D)$ mit einem zentralen Schiefkörper D über K und einem $m \in \mathbb{N}$.

(iii) Es gibt eine K-Algebraisomorphie

$$A \otimes_K A^{\mathrm{op}} \xrightarrow{\sim} \mathrm{End}_K A\,, \; a \otimes b \longmapsto (x \longmapsto axb)\,.$$

(iv) Es gibt eine $\overline{K}$-Algebraisomorphie $A \otimes_K \overline{K} \simeq \mathrm{M}_{n\times n}(\overline{K})$ für ein $n \in \mathbb{N}$, wobei $\overline{K}$ ein algebraischer Abschluß von K ist.

(v) Es gibt einen Körper $L \supset K$ und eine L-Algebraisomorphie $A \otimes_K L \simeq \mathrm{M}_{n\times n}(L)$ für ein $n \in \mathbb{N}$.

Beweis. (i)$\Longleftrightarrow$(ii): nach 1.7, 2.2 und Satz 1.5.

(i)$\Longrightarrow$(iii): nach Satz 3.3.

(iii)$\Longrightarrow$(i): Nach (iii) gibt es nach Wahl einer Basis von A über K einen Isomorphismus

$$\varphi\colon A \otimes_K A^{\mathrm{op}} \xrightarrow{\sim} \mathrm{M}_{r\times r}(K)$$

so, daß $\varphi(a \otimes 1) = \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}$ $\forall\, a \in A$ gilt. Da $\mathrm{M}_{r\times r}(K)$ einfach ist, ist also auch A einfach, vgl. Aufgabe 11. Für jedes $a \in \mathcal{Z}(A)$ gilt

$$\begin{aligned} a \otimes 1 \in \mathcal{Z}(A) \otimes_K \mathcal{Z}(A^{\mathrm{op}}) &\underset{2.5}{=} \mathcal{Z}(A \otimes_K A^{\mathrm{op}}) \\ &\underset{\varphi}{\simeq} \mathcal{Z}(\mathrm{M}_{r\times r}(K)) \underset{2.2}{=} K \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}. \end{aligned}$$

Es folgt $a \in K$ wegen $\varphi(a\otimes 1) = \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} \in \mathrm{M}_{r\times r}(K)$. Also ist A eine zentrale K-Algebra.

(i)$\Longrightarrow$(iv): Nach (i) und 3.7 ist $A \otimes_K \overline{K}$ eine zentrale, einfache $\overline{K}$-Algebra, und also gilt $A \otimes_K \overline{K} \simeq \mathrm{M}_{n\times n}(\overline{D})$ mit einem (endlich-dimensionalen) Schiefkörper $\overline{D}$ über $\overline{K}$, vgl. 1.7. Nach 3.6 ist $\overline{D} = \overline{K}$.

(iv)$\Longrightarrow$(v): trivial (nimm $L = \overline{K}$).

(v)$\Longrightarrow$(i): Es ist $\mathcal{Z}(A)\otimes_K L = \mathcal{Z}(A)\otimes_K \mathcal{Z}(L) \underset{2.5}{=} \mathcal{Z}(A\otimes_K L) = \mathcal{Z}(\mathrm{M}_{n\times n}(L)) \underset{2.2}{=} L$. Es folgt $1 = \dim_L(\mathcal{Z}(A) \otimes_K L) \underset{\text{Aufgabe 9}}{=} \dim_K \mathcal{Z}(A)$ und also $K = \mathcal{Z}(A)$.
Nach (v) und Satz 1.5 ist $A\otimes_K L \simeq \mathrm{M}_{n\times n}(L)$ ein einfacher Ring und also eine einfache K-Algebra. Daher ist auch A einfach nach Aufgabe 11. $\square$

3.9 Die Dimension einer Azumaya-Algebra

Aus 3.8 ergibt sich sofort die folgende Erkenntnis

Satz. *Die Dimension einer Azumaya-Algebra A über K ist eine Quadratzahl, d.h. $\exists\, n \in \mathbb{N}$ mit $\dim_K A = n^2$.*
Insbesondere ist die Dimension eines Schiefkörpers über seinem Zentrum eine Quadratzahl oder ∞ .

Beweis. Nach 3.8 (i)$\Longrightarrow$(v) gibt es eine Körpererweiterung L von K , so daß $A \otimes_K L \simeq \mathrm{M}_{n\times n}(L)$ für ein $n \in \mathbb{N}$ gilt.
Es folgt $\dim_K A \underset{\text{Aufgabe 9}}{=} \dim_L(A \otimes_K L) = \dim_L \mathrm{M}_{n\times n}(L) = n^2$. □

3.10 Der Index teilt den Grad

Die Zahl n aus Satz 3.9 heißt der *Grad von A* . Es ist

$$\boxed{\operatorname{grad}_K A := \sqrt{\dim_K A}}\,.$$

Hierbei ist A eine Azumaya-Algebra über K und also $A \simeq \mathrm{M}_{m\times m}(D)$ mit einem zentralen Schiefkörper D über K , vgl. 3.8 (i)$\Longrightarrow$(ii). Nach 1.9 ist D bis auf K-Algebraisomorphie eindeutig bestimmt. Der *Index* $\operatorname{ind}_K A$ ist definiert als

$$\boxed{\operatorname{ind}_K A := \sqrt{\dim_K D}}\,.$$

Es gilt $\operatorname{grad}_K A = \sqrt{\dim_K \mathrm{M}_{m\times m}(D)} = m \cdot \operatorname{ind}_K A$ und also

$$\boxed{\operatorname{ind}_K A \mid \operatorname{grad}_K A}\,.$$

Beispiel. $\operatorname{ind}_{\overline{K}}(A \otimes_K \overline{K}) = 1$ nach 3.8 (i)$\Longrightarrow$(iv).
Allgemeiner gilt: Der Index wird bei Körpererweiterungen kleiner oder bleibt gleich.

4 Der Satz von Skolem-Noether und der Zentralisatorsatz

Sei K ein Körper.

4.1 Lemma

Sei C eine endlich-dimensionale einfache K-Algebra. Sind M und M' zwei C-Moduln mit $\dim_K M = \dim_K M' < \infty$, so sind M und M' isomorph.

Beweis. Wähle ein minimales Linksideal $I \neq (0)$ in C, vgl. 1.4.

Behauptung. $\exists\, n \in \mathbb{N}$ mit $M \simeq I^n = \underbrace{I \oplus \cdots \oplus I}_{n \text{ Summanden}}$

Beweis. Es ist $IC = \{\sum\limits_{i}^{\text{endl.}} x_i c_i \mid x_i \in I,\, c_i \in C\}$ ein zweiseitiges Ideal $\neq (0)$ in C, da I Linksideal $\neq (0)$ in C. Da C eine einfache K-Algebra ist, ist also $IC = C$. Es folgt

$$
\begin{aligned}
M &= CM, && \text{da } M \text{ ein } C\text{-Linksmodul}\\
&= ICM, && \text{da } IC = C\\
&= IM, && \text{da } CM = M\,.
\end{aligned}
$$

Für jede K-Basis $\{v_1, \dots, v_m\}$ von M gilt also $M = Iv_1 + \cdots + Iv_m$. Wähle n minimal, so daß $M = Iw_1 + \cdots + Iw_n$ mit $w_1, \dots, w_n \in M$. Dann ist

$$\boxed{\varphi\colon I^n \longrightarrow M\,,\ (x_1, \dots, x_n) \longmapsto \sum_{i=1}^{n} x_i w_i}$$

surjektiv. Sei $\varphi(x_1, \dots, x_n) = \sum\limits_{i=1}^{n} x_i w_i = 0$.
Zeige $x_i = 0\ \forall\, i = 1, \dots, n$.
Angenommen, es ist $x_i \neq 0$ für ein i, etwa für $i = 1$. Dann ist $Cx_1 = I$, da I minimales Linksideal ist und also $Iw_1 = Cx_1w_1 \subset Cx_2w_2 + \cdots + Cx_nw_n$, da $x_1w_1 = -x_2w_2 - \cdots - x_nw_n$.
Es folgt $Iw_1 \subset Iw_2 + \cdots + Iw_n$ im Widerspruch zur Minimalität von n. Also ist φ injektiv, und die Behauptung folgt. □

Analog ist $M' \simeq I^r$ mit einem $r \in \mathbb{N}$. Wegen $\dim_K M = \dim_K M'$ folgt $r = n$ und also $M \simeq M'$. □

4.2 Der Satz von Skolem-Noether

Satz. *Sei A eine Azumaya-Algebra über K, und sei B eine endlich-dimensionale, einfache K-Algebra. Sind $f, g\colon B \longrightarrow A$ zwei K-Algebrahomomorphismen, so gibt es eine Einheit $u \in A^*$ so, daß gilt:*

$$\boxed{g(b) = uf(b)u^{-1} \;\forall\, b \in B}.$$

Beweis. Sei $C = B \otimes_K A^{\text{op}}$. Dann ist auf A eine C-Modulstruktur durch

(1) $\qquad (b \otimes a') \cdot a := f(b)aa' \qquad \forall\, a, a' \in A,\ b \in B$

gegeben. Schreibe für diesen C-Modul A_f. Entsprechend ist A ein C-Modul A_g mit

(2) $\qquad (b \otimes a') \cdot a := g(b)aa' \qquad \forall\, a, a' \in A,\ b \in B$.

Nach Voraussetzung und Satz 2.6 ist C eine endlich-dimensionale einfache K-Algebra. Nach 4.1 gibt es einen C-Modulisomorphismus $h\colon A_f \longrightarrow A_g$. Setze $u := h(1)$. Dann gilt:

$$\begin{aligned} h(a) &= h(\underbrace{f(1)}_{1}\,1a) = h((1 \otimes a) \cdot 1) \\ &= (1 \otimes a) \cdot h(1)\,, && \text{da } h \ C\text{-linear} \\ &= g(1)h(1)a && \text{nach (2)} \\ &= ua \;\forall\, a \in A\,. \end{aligned}$$

Speziell für $a = f(b)$ folgt

$$uf(b) = h(f(b)) = h((b \otimes 1) \cdot 1) = (b \otimes 1) \cdot h(1) = g(b)u\,.$$

Es ist nur noch zu zeigen, daß u invertierbar ist. Wie oben gezeigt, gilt

(3) $\qquad h(a) = ua \;\forall\, a \in A\,.$

Da h bijektiv ist, gibt es ein $v \in A$ mit $h(v) = 1$. Es folgt $1 = h(v) = uv$ und also $h(vu) = u(vu) = (uv)u = u = h(1)$. Da h injektiv ist, folgt $vu = 1$. Also ist $v = u^{-1}$. □

4.3 Satz über innere Automorphismen

Sei A eine K-Algebra. Dann heißt ein K-Algebraautomorphismus $g\colon A \longrightarrow A$ ein *innerer Automorphismus*, falls es ein $u \in A^*$ so gibt, daß für alle $a \in A$ gilt:

$$\boxed{g(a) = uau^{-1}}.$$

Satz. *Ist A eine Azumaya-Algebra über K, so ist jeder K-Algebrahomomorphismus $g\colon A \longrightarrow A$ ein innerer Automorphismus.*

Beweis. Nach 3.1 ist g injektiv und daher aus Dimensionsgründen surjektiv. Wende nun 4.2 mit $B = A$ und $f = \mathrm{id}$ an. □

4.4 Einfachheit des Zentralisators

Für eine Unteralgebra B einer K-Algebra A ist durch

$$\mathcal{Z}_A(B) := \{a \in A \mid ba = ab \;\forall\, b \in B\}$$

der *Zentralisator von B in A* definiert. Es ist $\mathcal{Z}_A(B)$ eine K-Algebra, und es gilt $\mathcal{Z}_A(K) = A$ nach Definition 1.1. Ist A eine Azumaya-Algebra über K, so gibt es nach Satz 3.3 eine K-Algebraisomorphie

$$\boxed{A \otimes_K A^{\mathrm{op}} \simeq \mathrm{M}_{m\times m}(K) \quad \text{mit } m = \dim_K A}\,.$$

Wir folgern nun aus dem Satz von Skolem-Noether 4.3, daß allgemeiner folgendes gilt:

Lemma. *Sei B eine einfache Unteralgebra einer Azumaya-Algebra A über K. Dann gibt es einen K-Algebraisomorphismus*

$$\boxed{\varphi\colon A \otimes_K B^{\mathrm{op}} \xrightarrow{\;\sim\;} \mathcal{Z}_A(B) \otimes_K \mathrm{M}_{n\times n}(K) \quad \textit{mit } n = \dim_K B}\,.$$

Insbesondere ist $\mathcal{Z}_A(B)$ eine einfache K-Algebra mit Zentrum $\mathcal{Z}(\mathcal{Z}_A(B)) = \mathcal{Z}(B)$. Ferner gilt: Ist B kommutativ, also $B \subset \mathcal{Z}_A(B)$, so ist $\varphi(1 \otimes b) = b \otimes 1 \;\forall\, b \in B$.

Beweis. Sei $E =: \mathrm{End}_K B$. Es ist dann K vermöge $K \hookrightarrow E$, $\lambda \longmapsto \lambda 1_E$, in E eingebettet. Da B einfach ist, sind die K-Algebrahomomorphismen

$$\ell\colon B \longrightarrow E,\; b \longmapsto \begin{cases} B \xrightarrow{\ell_b} B, \\ x \longmapsto bx \end{cases} \text{und } r\colon B^{\mathrm{op}} \longrightarrow E,\; b \longmapsto \begin{cases} B \xrightarrow{r_b} B, \\ x \longmapsto xb \end{cases}$$

nach 3.1 injektiv, und es folgt

$$\begin{aligned}
A \otimes_K B^{\mathrm{op}} &\simeq A \otimes_K r(B^{\mathrm{op}}) \\
&= A \otimes_K \mathcal{Z}_E(\ell(B)) && \text{nach Aufgabe 7} \\
&= \mathcal{Z}_A(K) \otimes_K \mathcal{Z}_E(\ell(B)), && \text{da } A = \mathcal{Z}_A(K) \\
&= \mathcal{Z}_{A\otimes_K E}(K \otimes_K \ell(B)) && \text{nach 2.5} \\
&\simeq \mathcal{Z}_{A\otimes_K E}(B \otimes_K K) && \text{nach der Behauptung unten} \\
&= \mathcal{Z}_A(B) \otimes_K \mathcal{Z}_E(K) && \text{nach 2.5} \\
&= \mathcal{Z}_A(B) \otimes_K E, && \text{da } \mathcal{Z}_E(K) = E \\
&\simeq \mathcal{Z}_A(B) \otimes_K \mathrm{M}_{n\times n}(K) && \text{mit } n = \dim_K B\,,\ \text{da } E = \mathrm{End}_K B
\end{aligned}$$

Insbesondere ist $\mathcal{Z}_A(B) \otimes_K \mathrm{M}_{n\times n}(K)$ einfach, da $A \otimes_K B^{\mathrm{op}}$ nach Satz 2.6 einfach ist. Daher folgt aus Aufgabe 11, daß $\mathcal{Z}_A(B)$ einfach ist. Außerdem folgt

$$\begin{aligned}
\mathcal{Z}(\mathcal{Z}_A(B)) &\simeq \mathcal{Z}(\mathcal{Z}_A(B)) \otimes_K \mathcal{Z}(\mathrm{M}_{n\times n}(K))\,, && \text{da } \mathcal{Z}(\mathrm{M}_{n\times n}(K)) = K \text{ nach 2.2} \\
&= \mathcal{Z}(\mathcal{Z}_A(B) \otimes_K \mathrm{M}_{n\times n}(K)) && \text{nach 2.5} \\
&\simeq \mathcal{Z}(A \otimes_K B^{\mathrm{op}})\,, && \text{wie oben gezeigt} \\
&= \mathcal{Z}(A) \otimes_K \mathcal{Z}(B^{\mathrm{op}}) && \text{nach 2.5} \\
&= K \otimes_K \mathcal{Z}(B^{\mathrm{op}})\,, && \text{da } A \text{ zentral} \\
&\simeq \mathcal{Z}(B)\,.
\end{aligned}$$

Da $\mathcal{Z}(B) \subset \mathcal{Z}(\mathcal{Z}_A(B))$ ist, folgt $\mathcal{Z}(B) = \mathcal{Z}(\mathcal{Z}_A(B))$. Zeige nun, wie oben angekündigt:

Behauptung. $\mathcal{Z}_{A\otimes_K E}(K \otimes_K \ell(B)) \simeq \mathcal{Z}_{A\otimes_K E}(B \otimes_K K)$.

Beweis. Definiere $f, g\colon B \longrightarrow A \otimes_K E$ durch $f(b) = b \otimes 1_E$ und $g(b) = 1 \otimes \ell_b \;\forall\, b \in B$. Dann gilt

$$\begin{aligned}
\mathcal{Z}_{A\otimes_K E}(K \otimes_K \ell(B)) &= \mathcal{Z}_{A\otimes_K E}(g(B))\,, && \text{da } K \otimes_K \ell(B) = g(B) \text{ nach Definition von } g \\
&= \mathcal{Z}_{A\otimes_K E}(uf(B)u^{-1}) && \text{mit einem } u \in (A \otimes_K E)^* \text{ nach 4.2} \\
&= u\mathcal{Z}_{A\otimes_K E}(f(B))u^{-1} && \text{nach Aufgabe 15} \\
&\simeq \mathcal{Z}_{A\otimes_K E}(f(B)) && \text{durch Konjugation mit } u^{-1} \\
&= \mathcal{Z}_{A\otimes_K E}(B \otimes_K K)\,, && \text{da } f(B) = B \otimes_K K \text{ nach Definition von } f\,.
\end{aligned}$$

□

Sei nun B kommutativ. Dann ist $1 \otimes \ell_b \in \mathcal{Z}_{A\otimes_K E}(K \otimes_K \ell(B))$ und $b \otimes 1 \in \mathcal{Z}_{A\otimes_K E}(B \otimes_K K) \;\forall\, b \in B$, und der Beweis der Behauptung ergibt

$$1 \otimes \ell_b = g(b) = uf(b)u^{-1} \xmapsto{\;\sim\;} f(b) = b \otimes 1_E\,.$$

□

4.5 Der Zentralisatorsatz

Satz. *Sei A eine Azumaya-Algebra über K, und sei B eine einfache Unteralgebra von A. Dann ist*

$$\boxed{\mathcal{Z}_A(\mathcal{Z}_A(B)) = B}\,.$$

Ferner gilt: Ist B zentral, so ist $\mathcal{Z}_A(B)$ eine Azumaya-Algebra über K, und es gibt einen K-Algebraisomorphismus

$$\varphi\colon \mathcal{Z}_A(B) \otimes_K B \xrightarrow{\;\sim\;} A \;\text{ mit } \varphi(x \otimes b) = xb \;\forall\, x \in \mathcal{Z}_A(B), b \in B\,.$$

Beweis. Nach Lemma 4.4 gilt für jede einfache Unteralgebra B von A die Formel

$$(\dim_K A)(\dim_K B) = (\dim_K \mathcal{Z}_A(B))(\dim_K B)^2$$

und also

$$(*) \qquad \boxed{\dim_K A = (\dim_K \mathcal{Z}_A(B))(\dim_K B)}$$

Nach 4.4 ist $\mathcal{Z}_A(B)$ eine einfache Unteralgebra von A. Anwendung von $(*)$ auf $\mathcal{Z}_A(B)$ anstelle von B ergibt

$$\dim_K A = \dim_K(\mathcal{Z}_A(\mathcal{Z}_A(B)))(\dim_K \mathcal{Z}_A(B)) .$$

Ein Vergleich mit $(*)$ ergibt, daß

$$\dim_K B = \dim_K \mathcal{Z}_A(\mathcal{Z}_A(B))$$

gilt. Da $B \subset \mathcal{Z}_A(\mathcal{Z}_A(B))$ gilt, folgt Gleichheit.
Ist B zentral, so ist $K = \mathcal{Z}(B) \underset{4.4}{=} \mathcal{Z}(\mathcal{Z}_A(B))$, und also ist dann $\mathcal{Z}_A(B)$ eine Azumaya-Algebra über K . Es folgt aus Satz 2.6, daß $\mathcal{Z}_A(B) \otimes_K B$ einfach ist. Nach 3.1 ist also φ injektiv, und aus $(*)$ folgt dann, daß φ auch surjektiv ist. □

4.6 Anwendung von 4.5 auf Körpererweiterungen

Wir wenden den Zentralisatorsatz 4.5 auf den Fall an, daß die einfache Unteralgebra B von A ein Körper ist.

Satz. *Sei L eine Körpererweiterung von K , und sei A eine Azumaya-Algebra über K , die L als Ungeralgebra enthalte. Dann gibt es eine L-Algebraisomorphie*

$$\boxed{A \otimes_K L \simeq \mathcal{Z}_A(L) \otimes_L \mathrm{M}_{n\times n}(L) \quad \textit{mit } n = \dim_K L}.$$

Insbesondere ist der Zentralisator $\mathcal{Z}_A(L)$ eine Azumaya-Algebra über L , und es gilt

$$\boxed{[A \otimes_K L] = [\mathcal{Z}_A(L)] \textit{ in } \mathrm{Br}(L)}.$$

Beweis. Es gibt K-Algebraisomorphismen

$$\begin{aligned} A \otimes_K L &\simeq \mathcal{Z}_A(L) \otimes_K \mathrm{M}_{n\times n}(L) \text{ mit } n = \dim_K L && \text{nach Lemma 4.4} \\ &\simeq \mathcal{Z}_A(L) \otimes_L (L \otimes_K \mathrm{M}_{n\times n}(K)) && \text{nach Algebra 10.9} \\ &\simeq \mathcal{Z}_A(L) \otimes_L \mathrm{M}_{n\times n}(L) && \text{nach Aufgabe 10.} \end{aligned}$$

Da L kommutativ ist, gilt nach Lemma 4.4 hierbei

$$1 \otimes \lambda \underset{4.4}{\overset{\sim}{\longmapsto}} \lambda \otimes 1 \overset{\sim}{\longmapsto} \lambda \otimes 1_L \otimes 1 \overset{\sim}{\longmapsto} \lambda \otimes 1 \qquad \forall \lambda \in L\,.$$

Es gibt also einen K-Algbraisomorphismus

$$\psi\colon A \otimes_K L \longrightarrow \mathcal{Z}_A(L) \otimes_L \mathrm{M}_{n\times n}(L) \text{ mit } \psi(1 \otimes \lambda) = \lambda \otimes 1 \qquad \forall \lambda \in L\,.$$

Für alle $\lambda \in L$ und $x \in A \otimes_K L$ folgt daher

$$\begin{aligned} \psi(\lambda \cdot x) &= \psi((1 \otimes \lambda)x) && \text{kanonische Struktur} \\ &= \psi(1 \otimes \lambda)\psi(x), && \text{da } \psi \text{ multiplikativ} \\ &= (\lambda \otimes 1)\psi(x) \\ &= \lambda \cdot \psi(x) && \text{kanonische Struktur.} \end{aligned}$$

Nach 3.7 ist $A \otimes_K L$ eine Azumaya-Algebra über L, daher ist auch $\mathcal{Z}_A(L) \otimes_L \mathrm{M}_{n\times n}(L)$ eine solche. Nach Aufgabe 11 ist $\mathcal{Z}_A(L)$ einfach, und es gilt

$$\mathcal{Z}(\mathcal{Z}_A(L)) \underset{4.4}{=} \mathcal{Z}(L) = L\,, \qquad\qquad \text{da } L \text{ kommutativ.}$$

Also ist $\mathcal{Z}_A(L)$ eine Azumaya-Algebra über L, und aus 3.4 folgt die letzte Behauptung. □

4.7 Eine Dimensionsbeziehung

Satz. *Sei L eine Körpererweiterung von K, und sei A eine Azumaya-Algebra über K, die L als K-Unteralgebra enthalte. Dann gelten:*

1) $\boxed{\mathcal{Z}_A(L) = L} \iff \boxed{\dim_K A = (\dim_K L)^2}\,.$

2) Ist eine der beiden Bedingungen in (1) erfüllt, so ist $[A \otimes_K L] = [L]$ in $\mathrm{Br}(L)$ und also L ein Zerfällungskörper von A.

Beweis. 1) Da L kommutativ ist, gilt $L \subset \mathcal{Z}_A(L)$. Es folgt 1), weil $\dim_K A \underset{\text{Aufgabe 9}}{=} \dim_L(A \otimes_K L) \underset{4.6}{=} (\dim_L \mathcal{Z}_A(L))(\dim_K L)^2$ gilt.

2) Nach Satz 4.6 ist $[A \otimes_K L] = [\mathcal{Z}_A(L)]$ in $\mathrm{Br}(L)$. Hieraus folgt 2). □

Beispiel. Seien $K = \mathbb{R}$ und $A = \mathbb{H}$ wie in 0.1 definiert. Dann ist $\dim_{\mathbb{R}} \mathbb{H} = 4 = (\dim_{\mathbb{R}} \mathbb{C})^2$, also gilt nach dem Satz $\mathcal{Z}_{\mathbb{H}}(\mathbb{C}) = \mathbb{C}$, und $\mathbb{C}$ ist Zerfällungskörper von $\mathbb{H}$, also $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \simeq \mathrm{M}_{2\times 2}(\mathbb{C})$.

Bemerkung. Sind A und L wie im Satz gegeben, so gilt:
$\mathcal{Z}_A(L) = L \Longrightarrow L$ ist ein maximaler Teilkörper von A
nach Aufgabe 7. Die Umkehrung gilt i.a. nicht, vgl. Aufgabe 16.

5 Zerfällungskörper und maximale Teilkörper

Sei K ein Körper.

5.1 Der Begriff des Zerfällungskörpers

Sei L eine Körpererweiterung von K, und sei A eine Azumaya-Algebra über K.

Definition. 1) L heißt *Zerfällungskörper von* A, falls $[A] \in \operatorname{kern}(r_{L/K}\colon \operatorname{Br}(K) \longrightarrow \operatorname{Br}(L)\,,\ [B] \longmapsto [B \otimes_K L])$ gilt.

2) Die *relative Brauergruppe* $\operatorname{Br}(L/K)$ ist definiert als $\operatorname{Br}(L/K) := \operatorname{kern}(r_{L/K})$.

Bemerkung. Offenbar gilt:

(a) Ist L Zerfällungskörper von A, so ist L Zerfällungskörper von jeder zu A ähnlichen Azumaya-Algebra über K.

(b) Ist L Zerfällungskörper von A, so ist jede Körpererweiterung L' von L auch Zerfällungskörper von A, denn

$$A \otimes_K L' \simeq (\underbrace{A \otimes_K L}_{\mathrm{M}_{n\times n}(L)}) \otimes_L L' \simeq \mathrm{M}_{n\times n}(L')\,.$$

(c) Die relative Brauergruppe $\operatorname{Br}(L/K)$ ist eine Untergruppe der Brauergruppe von K. Es ist

$$\operatorname{Br}(L/K) = \{[A] \in \operatorname{Br}(K) \mid [A \otimes_K L] = [L]\}\,.$$

(d) Wir werden in 5.7 zeigen, daß A stets einen über K galoisschen Zerfällungskörper L (mit $\dim_K L < \infty$) besitzt.

5.2 Maximal kommutative Unterringe eines Schiefkörpers

Nach Aufgabe 7 ist ein Unterring B eines Ringes A genau dann maximal kommutativ, wenn $\mathcal{Z}_A(B) = B$ gilt.
Dabei ist $\mathcal{Z}_A(B) := \{a \in A \mid ab = ba\ \forall\, b \in B\}$.

Satz. *Sei S ein Unterring eines Schiefkörpers D. Dann ist $\mathcal{Z}_D(S)$ ein Schiefkörper. Insbesondere ist jeder maximal kommutative Unterring von D ein Körper.*

Beweis. Sei $x \in \mathcal{Z}_D(S)$ mit $x \neq 0$. Dann besitzt x ein Inverses $x^{-1} \in D$, da D ein Schiefkörper ist. Zu zeigen: $x^{-1} \in \mathcal{Z}_D(S)$.
Es ist $xs = sx \ \forall\, s \in S$, da $x \in \mathcal{Z}_D(S)$. Multipliziere diese Gleichung von links und von rechts mit x^{-1}. Dann folgt $sx^{-1} = x^{-1}s \ \forall\, s \in S$, und also $x^{-1} \in \mathcal{Z}_D(S)$. Daher ist $\mathcal{Z}_D(S)$ ein Schiefkörper. Ist S maximal kommutativer Unterring von D, so ist $S = \mathcal{Z}_D(S)$ und also S ein Körper. □

5.3 Lemma über einfach erzeugte Teilkörper

Lemma. *Sei D ein endlich-dimensionaler Schiefkörper über K, und sei L ein Zwischenkörper, also $K \subset L \subset D$. Dann erzeugt jedes $x \in \mathcal{Z}_D(L)$ einen Körper $L(x)$. Insbesondere erzeugt jedes $x \in D$ einen Körper $K(x)$.*

Beweis. Sei $x \in \mathcal{Z}_D(L)$. Dann ist die von x erzeugte L-Unteralgebra $L[x]$ von $\mathcal{Z}_D(L)$ kommutativ (sie besteht aus allen endlichen Linearkombinationen $\sum \lambda_i x^i$ mit $\lambda_i \in L$).
Für jedes $z \in L[x]$ mit $z \neq 0$ ist die Abbildung $\ell_z\colon L[x] \longrightarrow L[x]$, $y \longmapsto zy$, L-linear. Sie ist injektiv, da $L[x]$ als Unterring eines Schiefkörpers keine nichttrivialen Nullteiler besitzt. Aus Dimensionsgründen ist ℓ_z daher auch surjektiv. Es gibt also ein $y \in L[x]$ mit $1 = \ell_z(y) = zy$. Also ist $L[x]$ ein Körper (für den wir $L(x)$ schreiben). Da $\mathcal{Z}_D(K) = D$ ist, folgt die zweite Behauptung. □

Folgerung. *Seien L und D wie im Lemma gegeben. Dann gilt:*

$$\boxed{L = \mathcal{Z}_D(L)} \quad \Longleftrightarrow \quad \boxed{L \textit{ ist maximaler Teilkörper von } D}.$$

Beweis. „$\Longrightarrow$“: folgt aus Aufgabe 7.

„$\Longleftarrow$“: Da L kommutativ ist, gilt $L \subset \mathcal{Z}_D(L)$. Jedes $x \in \mathcal{Z}_D(L) \setminus L$ würde nach dem Lemma einen Teilkörper $L(x)$ von D mit $L \subsetneqq L(x)$ erzeugen im Widerspruch zur Maximalität von L.

□

5.4 Maximale Teilkörper eines zentralen Schiefkörpers

Satz. *Sei D ein endlich-dimensionaler zentraler Schiefkörper über K. Dann besitzt D maximale Teilkörper, und jeder maximale Teilkörper L von D ist Zerfällungskörper von D. Genauer gilt:*

$$\boxed{D \otimes_K L \simeq \mathrm{M}_{n\times n}(L) \textit{ mit } n = \dim_K L \textit{ und } n^2 = \dim_K D}.$$

Beweis. Mit Hilfe des Zornschen Lemmas (vgl. Algebra 7.5, 7.6) zeigt man, daß D maximale Teilkörper enthält. Sei L ein solcher. Nach Folgerung 5.3 ist $L = \mathcal{Z}_D(L)$, und also folgt
$K = \mathcal{Z}(D) \subset \mathcal{Z}_D(L) = L$. Ferner folgt aus Satz 4.7, daß $\dim_K D = n^2$ mit $n = \dim_K L$ und L Zerfällungskörper von D ist.
Dies ergibt $n^2 = \dim_L(D \otimes_K L)$, also $D \otimes_K L \simeq \mathrm{M}_{n\times n}(L)$, da L Zerfällungskörper von D ist. □

Korollar. *Jede Azumaya-Algebra A über K besitzt einen Zerfällungskörper L mit* $\dim_K L = \mathrm{ind}_K A$.

Beweis. Es ist $A \sim D$ mit einem zentralen Schiefkörper D über K (vgl. 3.8). Sei L ein maximaler Teilkörper von D. Dann ist L Zerfällungskörper von A (vgl. 5.1(a)), und es gilt $\dim_K L = \sqrt{\dim_K D} \underset{3.10}{=}: \mathrm{ind}_K A$. □

5.5 Separable Elemente in D

Satz. *Sei D ein endlich-dimensionaler zentraler Schiefkörper über K mit $D \neq K$. Dann besitzt D einen Teilkörper $\neq K$, der separabel über K ist.*

Beweis. Ist $\mathrm{char}\, K = 0$, so ist jedes Element $x \in D$ separabel über K nach Algebra 16.8(1). Da $D \neq K$ ist, folgt die Behauptung aus Lemma 5.3.
Sei $\mathrm{char}\, K =: p > 0$. Dann gibt es zu jedem $x \in D$ ein $n \geq 0$ so, daß x^{p^n} separabel über K ist. (S. Lang, Algebra VII, 4, Prop. 9)
Angenommen: Jedes über K separable Element aus D liegt in K. Dann gibt es ein $d \in D \setminus K$ mit $d^p \in K$ nach Annahme. Wir zeigen unten folgende
Behauptung. Zu $\sigma\colon D \longrightarrow D$, $y \longmapsto dyd^{-1}$ gibt es ein Element $c \in D$ mit $\sigma(c) = c + 1$.
Hieraus folgt der Satz, denn es ist c^{p^m} separabel über K für ein $m \in \mathbb{N}$, und also $c^{p^m} \in K$ nach Annahme. Dies ergibt

$$c^{p^m} = \sigma(c)^{p^m} = (1 + c)^{p^m} = 1 + c^{p^m},$$

woraus der Widerspruch $0 = 1$ folgt. □

Beweis der Behauptung. Sei $\tau\colon D \longrightarrow D$, $y \longmapsto \sigma(y) - y$. Dann ist $\tau^p(y) = 0 \;\forall\, y \in D$, da $d^p \in K$ und da $\mathrm{char}\, K = p$. Es ist aber $\tau(y) \neq 0$ für ein $y \in D$, da $d \in D \setminus K$ und $K = \mathcal{Z}(D)$.
Hieraus folgt: $\exists\, r \in \mathbb{N}$ und $z \in D$ mit $\tau^{r+1}(z) = 0$ und $\tau^r(z) \neq 0$. Setze

$$\boxed{c = \tau^{r-1}(z)\,\tau^r(z)^{-1}}\,.$$

Dann folgt

$$\begin{aligned}\sigma(c) &= \sigma(\tau^{r-1}(z))\sigma(\tau^r(z)^{-1}) \\ &= (\tau^r(z) + \tau^{r-1}(z))(\underbrace{\tau^{r+1}(z)}_{=0} + \tau^r(z))^{-1}, \qquad \text{da } \sigma(y) = \tau(y) + y \\ &= 1 + \tau^{r-1}(z)\,\tau^r(z)^{-1} \\ &= 1 + c\,.\end{aligned}$$

□

5.6 Existenz eines separablen Zerfällungskörpers

Satz. *Sei D ein endlich-dimensionaler zentraler Schiefkörper über K. Dann besitzt D einen maximalen Teilkörper L, der separabel über K ist. Dabei gilt*

$$\dim_K D = (\dim_K L)^2\,,$$

und L ist Zerfällungskörper von D.

Beweis. Falls $D = K$, nimm $L = K$. Sei $D \neq K$. Dann besitzt D nach 5.5 einen Teilkörper $\neq K$, der separabel über K ist. Wähle einen Teilkörper L von D, der K enthält und maximal ist bezüglich der Eigenschaft: L ist separabel über K.
Nach Satz 5.2 ist $\mathcal{Z}_D(L)$ ein Schiefkörper über L, und nach 4.6 ist $\mathcal{Z}_D(L)$ zentral über L. Wäre $L \subsetneqq \mathcal{Z}_D(L)$, so würde $\mathcal{Z}_D(L)$ nach 5.5 einen Teilkörper $\neq L$ enthalten, der separabel über L wäre im Widerspruch zur Wahl von L. Also ist $\mathcal{Z}_D(L) = L$ und daher L ein maximaler Teilkörper von D. Der Rest folgt nun aus Satz 4.7. □

5.7 Existenz eines galoisschen Zerfällungskörpers

Satz. *Sei A eine Azumaya-Algebra über K. Dann besitzt A einen über K galoisschen Zerfällungskörper L mit $\dim_K L < \infty$.*

Beweis. Es ist $[A] = [D]$ mit einem zentralen Schiefkörper D über K, (vgl. 3.5, 3.8). Nach 5.6 und 5.1(a) besitzt A einen separablen Zerfällungskörper L' mit $\dim_K L' < \infty$. Bette L' in eine (endliche) Galoiserweiterung L von K ein (vgl. Algebra 15.9). Dann ist L Zerfällungskörper von A nach 5.1(b). □

5.8 Folgerung für die Brauergruppe

In 5.1 hatten wir die relative Brauergruppe

$$\mathrm{Br}(L/K) = \{[A] \in \mathrm{Br}(K) \mid A \otimes_K L \sim L\}$$

eingeführt. Aus 5.7 folgt, daß sich die Bestimmung der Brauergruppe $\mathrm{Br}(K)$ auf die Bestimmung aller Untergruppen $\mathrm{Br}(L/K)$ zurückführen läßt, wobei L (endlich) galoissch über K ist. Sei $\overline{K}$ ein algebraischer Abschluß von K. Dann ist $\mathrm{Br}(K) = \bigcup\limits_{L} \mathrm{Br}(L/K)$, wobei L alle (endlich) galoisschen Körpererweiterungen von K in $\overline{K}$ durchläuft.

5.9 Satz über endlich-dimensionale Zerfällungskörper

Nach 5.7 besitzt jede Azumaya-Algebra A einen über K (endlich) galoisschen Zerfällungskörper L. Dieser läßt sich i.a. nicht als Unterring von A realisieren. Es gibt aber immer eine zu A ähnliche Azumaya-Algebra B über K, die L als maximal kommutativen Unterring enthält.

Satz. *Sei A eine Azumaya-Algebra über K, und sei L eine endliche Körpererweiterung von K. Dann sind äquivalent:*

(i) *L ist Zerfällungskörper von A.*

(ii) *L ist Unteralgebra einer Azumaya-Algebra B über K mit den Eigenschaften:*
$$B \sim A \quad \textit{und} \quad \mathcal{Z}_B(L) = L\,.$$

(iii) *L ist Unteralgebra einer Azumaya-Algebra B über K mit $B \sim A$ und $\dim_K B = (\dim_K L)^2$.*

Beweis. „(i)$\Longrightarrow$(ii)“: Es ist $A \sim \mathrm{M}_{r\times r}(D)$ mit einem zentralen Schiefkörper D über K, vgl. 3.8. Sei I ein minimales Linksideal $\neq (0)$ in $D^{\mathrm{op}} \otimes_K L$ (vgl. Bemerkung 1.4). Setze
$$\boxed{B := \mathrm{End}_{D^{\mathrm{op}}\otimes_K K}(I)}\,.$$
Es ist $D^{\mathrm{op}} \otimes_K K \simeq D^{\mathrm{op}}$ und also $B \simeq \mathrm{M}_{m\times m}(D)$ mit $m = \dim_D I$ (vgl. 1.3). Hieraus folgt, daß B eine zu A ähnliche Azumaya-Algebra über K ist, vgl. Bemerkung 3.4 und 3.8.
Noch zu zeigen: $L = \mathcal{Z}_B(L)$. Bette L vermöge
$$L \hookrightarrow B\,,\ \lambda \longmapsto \begin{cases} I & \longrightarrow I\,, \\ x & \longmapsto (1\otimes\lambda)x \end{cases}$$
in B ein. Wie leicht nachzurechnen ist (vgl. Aufgabe 17), gilt
$$\boxed{\mathcal{Z}_B(L) = \mathrm{End}_{D^{\mathrm{op}}\otimes_K L}(I)}\,,$$

und also ist $\mathcal{Z}_B(L)$ ein Schiefkörper nach dem Lemma von Schur 1.6 (da $I \neq (0)$ minimal). In $\mathrm{Br}(L)$ gilt:

$$\begin{aligned} [L] &= [B \otimes_K L]\,, && \text{da } L \text{ Zerfällungskörper von } A \sim B \\ &= [\mathcal{Z}_B(L)] && \text{nach 4.6.} \end{aligned}$$

Da $\mathcal{Z}_B(L)$ ein Schiefkörper ist, folgt $L \simeq \mathcal{Z}_B(L)$ nach Bemerkung 3.4. Da $L \subset \mathcal{Z}_B(L)$ ist, folgt nun $L = \mathcal{Z}_B(L)$.

„(ii)$\Longrightarrow$(iii)“: folgt aus 4.7.1).

„(iii)$\Longrightarrow$(i)“: folgt aus 4.7.2).

□

6 Beispiele

6.1 Lemma aus der Gruppentheorie

Lemma. *Sei G eine endliche Gruppe, und sei H eine Untergruppe von G. Dann gilt:*

$$\boxed{G = \bigcup_{g \in G} gHg^{-1}} \quad \Longrightarrow \quad \boxed{H = G}.$$

Beweis. Seien $g_1 H, \ldots, g_n H$ die verschiedenen Linksnebenklassen von H in G.

Behauptung. $G = \bigcup\limits_{i=1}^{n} g_i H g_i^{-1}$.

Beweis der Behauptung. „$\supset$": klar.

„$\subset$": Sei $x \in G \Longrightarrow x = ghg^{-1}$ mit $g \in G,\ h \in H$, da $G = \bigcup_g gHg^{-1}$ nach Voraussetzung, und also

$$\begin{aligned} x &= g_j h' h (g_j h')^{-1}, && \text{da } G = \bigcup_{i=1}^{n} g_i H \text{ nach AGLA 10.10 und 10.9} \\ &= g_j \underbrace{h' h h'^{-1}}_{\in H} g_j^{-1} \in \bigcup_{i=1}^{n} g_i H g_i^{-1}. \end{aligned}$$

□

Sei $|X|$ die Anzahl der Elemente einer endlichen Menge X. Es folgt

$$\begin{aligned} |H| n &= |G| && \text{nach der Abzählformel in AGLA 10.10} \\ &\leq (|H| - 1) n + 1 && \text{nach der Behauptung, da } |g_i H g_i^{-1}| = |H| \ \forall\, i \\ & && \text{ und } 1 \in g_i H g_i^{-1} \\ &= |H| n - n + 1 \end{aligned}$$

Dies ergibt $n = 1$ und $|H| = |G|$. Da $H \subset G$ gilt, folgt $H = G$. □

6.2 Satz von Wedderburn (1905)

Satz. *Jeder endliche Schiefkörper ist kommutativ.*

Beweis. Sei D ein Schiefkörper mit endlich vielen Elementen, und sei $K = \mathcal{Z}(D)$ das Zentrum von D. Nach 5.4 gilt $\dim_K L = \sqrt{\dim_K D}$ für jeden maximalen Teilkörper L von D. Da D endlich ist, haben alle maximalen

Teilkörper von D dieselbe Anzahl von Elementen und sind daher alle isomorph (vgl. Algebra 14.3 und 14.4).
Wähle einen maximalen Teilkörper L von D aus. Dann ist

$$\boxed{D = \bigcup_{u \in D^*} uLu^{-1}},$$

denn: Ist $d \in D$, so ist $K(d) \subset L'$ mit einem maximalen Teilkörper L' von D, vgl. Lemma 5.3, 5.4. Sei $\varphi\colon L' \longrightarrow L \subset D$ ein Isomorphismus. Anwendung des Satzes von Skolem-Noether 4.2 mit $g = \mathrm{id}$ und $f = \varphi$ ergibt $d = u\varphi(d)u^{-1}$ mit einem $u \in D^*$.
Wende nun Lemma 6.1 auf die multiplikativen Gruppen $H = L^*$ und $G = D^*$ an. Dann folgt $L = D$, und also ist D kommutativ. □

6.3 Die Brauergruppe eines endlichen Körpers

Aus dem Satz von Wedderburn 6.2 ergibt sich als

Korollar. *Ist K ein endlicher Körper, so ist*

$$\mathrm{Br}(K) = \{1_{\mathrm{Br}(K)}\} = \{[K]\}\,.$$

Beweis. Nach 6.2 ist K bis auf Isomorphie der einzige zentrale endlichdimensionale Schiefkörper über K. □

6.4 Eine Anwendung von 6.3

Sei $K(X)$ der rationale Funktionenkörper in einer Unbestimmten X über K, also der Quotientenkörper des Polynomrings $K[X]$ (vgl. Algebra 6.11). Es ist

$$K(X) = \left\{ \frac{f}{g} \mid f, g \in K[X],\, g \neq 0 \right\}.$$

Satz. *Für jeden Körper K ist der Homomorphismus*

$$r_{K(X)/K}\colon\ \mathrm{Br}(K) \longrightarrow \mathrm{Br}(K(X))\,,\ [A] \longmapsto [A \otimes_K K(X)]\,,$$

injektiv.

Beweis. Ist K endlich, so ist $r_{K(X)/K}$ injektiv nach 6.3. Sei nun K ein Körper mit unendlich vielen Elementen. Ist $[A] \in \mathrm{kern}(r_{K(X)/K})$, so gib es einen $K(X)$-Algebraisomorphismus

$$\boxed{\varphi\colon A \otimes_K K(X) \xrightarrow{\ \sim\ } \mathrm{M}_{n\times n}(K(X))},$$

wobei $n^2 = \dim_K A$ (nach Aufgabe 9) gilt.
Zu zeigen: $A \simeq \mathrm{M}_{n\times n}(K)$.
Sei $a_1, \ldots, a_{n^2}$ eine K-Basis von A , und sei $\{e_{ij} \mid 1 \leq i,j \leq n\}$ die Standardbasis von $\mathrm{M}_{n\times n}(K(X))$ über $K(X)$ (wie in Beispiel 1.1). Dann ist

$$\varphi(a_i \otimes 1) = \sum_{j,k=1}^{n} \lambda_{ijk} e_{jk} \text{ mit } \lambda_{ijk} \in K(X)\,.$$

Es ist $g\lambda_{ijk} \in K[X]\ \forall\, i,j,k$, wobei $g \in K[X]$ das Produkt der Nenner von allen $\lambda_{ijk} \neq 0$ bezeichnet.
Also induziert φ einen $K\left[X, \frac{1}{g}\right]$-Algebrahomomorphismus

$$\widetilde{\varphi}\colon A \otimes_K K\left[X, \tfrac{1}{g}\right] \longrightarrow \mathrm{M}_{n\times n}\left(K\left[X, \tfrac{1}{g}\right]\right)\,.$$

Da K unendlich ist, gibt es ein $\alpha \in K$ mit $g(\alpha) \neq 0$ (nach Algebra, Satz 8.2).
Die „Spezialisierung“ $K[X] \longrightarrow K\,,\ f \longmapsto f(\alpha)$, induziert also einen K-Algebrahomomorphismus

$$s\colon K\left[X, \tfrac{1}{g}\right] \longrightarrow K \quad \text{mit} \quad s\left(\tfrac{f}{g^m}\right) = \tfrac{f(\alpha)}{g(\alpha)^m}$$

und daher einen K-Algebrahomomorphismus

$$\widetilde{s}\colon \mathrm{M}_{n\times n}\left(K\left[X, \tfrac{1}{g}\right]\right) \longrightarrow \mathrm{M}_{n\times n}(K)\,,\ (a_{ij}) \longmapsto (s(a_{ij}))\,.$$

Man erhält nun einen K-Algebrahomomorphismus

$$\psi\colon A \longrightarrow \mathrm{M}_{n\times n}(K)\,,\ a \longmapsto (\widetilde{s} \circ \widetilde{\varphi})(a \otimes 1)\,.$$

Nach 3.1 ist ψ injektiv und daher aus Dimensionsgründen surjektiv. $\square$

6.5 Satz von Frobenius (1878)

Sei $\mathbb{H}$ der in 0.1 eingeführte Quaternionenschiefkörper über $\mathbb{R}$.

Satz. *Sei D ein endlich-dimensionaler nicht-kommutativer Schiefkörper über $\mathbb{R}$. Dann gibt es einen $\mathbb{R}$-Algebraisomorphismus $\mathbb{H} \xrightarrow{\sim} D$.*

Beweis. Bis auf Isomorphie ist $\mathbb{C}$ die einzige endliche Körpererweiterung von $\mathbb{R}$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, und D nicht kommutativ ist, ist D kein Schiefkörper über $\mathbb{C}$ (vgl. 3.6). Es folgt $\mathbb{R} = \mathcal{Z}(D)$.
Nach Satz 5.4 besitzt D einen maximalen Teilkörper $\mathbb{C}'$ mit $(\dim_{\mathbb{R}} \mathbb{C}')^2 = \dim_{\mathbb{R}} D$. Da $\dim_{\mathbb{R}} D > 1$ gilt nach Voraussetzung, folgt $\mathbb{R} \subsetneqq \mathbb{C}'$, also $\mathbb{C}' \simeq \mathbb{C}$.
Es folgt $\dim_{\mathbb{R}} D = 4$.
Nun ist nur noch ein $\mathbb{R}$-Algebrahomomorphismus $\varphi\colon \mathbb{H} \longrightarrow D$ anzugeben.
Dieser ist dann nach 3.1 injektiv und daher aus Dimensionsgründen auch

surjektiv.
Es ist $\mathbb{C}' = \mathbb{R} \bigoplus j\mathbb{R}$ mit $j^2 = -1$, und $\mathbb{C}'$ ist galoissch über $\mathbb{R}$ mit Gruppe $\{\mathrm{id}, \sigma\}$, wobei $\sigma\colon \mathbb{C}' \longrightarrow \mathbb{C}'$, $a + bj \longmapsto a - bj \; \forall\, a, b \in \mathbb{R}$ gilt. Nach dem Satz von Skolem-Noether 4.2 gibt es ein $u \in D \setminus \{0\}$ mit

$$\boxed{\sigma(x) = uxu^{-1} \;\forall\, x \in \mathbb{C}'}\,.$$

Behauptung 1. $u^2 \in \mathbb{R}$.

Beweis. Es ist $u^2 j u^{-2} = \sigma^2(j) = j$, da $\sigma^2 = \mathrm{id}$, und also ist $u^2 j = j u^2$. Hieraus folgt $u^2 \in \mathcal{Z}_D(\mathbb{C}') \underset{4.7}{=} \mathbb{C}'$ und daher $\sigma(u^2) = u u^2 u^{-1} = u^2$.
Es folgt $u^2 \in \mathbb{R}$, da $\mathbb{C}'$ galoissch über $\mathbb{R}$ mit Gruppe $\langle \sigma \mid \sigma^2 = \mathrm{id} \rangle$. □

Behauptung 2. $u^2 < 0$.

Beweis. Angenommen, $u^2 > 0$. Dann ist $u \in \mathbb{R}$, da man aus jeder positiven reellen Zahl die Quadratwurzel ziehen kann und u^2 in $\mathbb{R}(u)$ die beiden Wurzeln u und $-u$ besitzt.
Da $\mathbb{R} = \mathcal{Z}(D)$ gilt, folgt der Widerspruch $-j = \sigma(j) = uju^{-1} \underset{u \in \mathcal{Z}(D)}{=} j$. □

Aus Behauptung 2 folgt $u^2 = -r^2$ mit $r \in \mathbb{R}$ und $r > 0$. Nach 0.1 besitzt $\mathbb{H} \subset \mathrm{M}_{2\times 2}(\mathbb{C})$ eine $\mathbb{R}$-Basis

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

wobei $i \in \mathbb{C}$ mit $i^2 = -1$.
Man rechnet nun nach, daß die Zuordnung

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longmapsto 1, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \longmapsto j, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \longmapsto ur^{-1}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \longmapsto ur^{-1}j,$$

den gesuchten $\mathbb{R}$-Algebrahomomorphismus $\varphi\colon \mathbb{H} \longrightarrow D$ induziert. Man beachte dabei, daß $-j = \sigma(j) = uju^{-1}$ und also $uj = -ju$ gilt. Eine Nebenrechnung folgt. □

Multiplikationstabellen:

1	j	ur^{-1}	$ur^{-1}j$
j	-1	$-ur^{-1}j$	ur^{-1}
ur^{-1}	$ur^{-1}j$	-1	$-j$
$ur^{-1}j$	$-ur^{-1}$	j	-1

$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$	$\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}$	$\begin{pmatrix}i & 0\\0 & -i\end{pmatrix}$	$\begin{pmatrix}0 & i\\i & 0\end{pmatrix}$
$\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}$	$\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$	$\begin{pmatrix}0 & -i\\-i & 0\end{pmatrix}$	$\begin{pmatrix}i & 0\\0 & -i\end{pmatrix}$
$\begin{pmatrix}i & 0\\0 & -i\end{pmatrix}$	$\begin{pmatrix}0 & i\\i & 0\end{pmatrix}$	$\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$	$\begin{pmatrix}0 & -1\\1 & 0\end{pmatrix}$
$\begin{pmatrix}0 & i\\i & 0\end{pmatrix}$	$\begin{pmatrix}-i & 0\\0 & i\end{pmatrix}$	$\begin{pmatrix}0 & 1\\-1 & 0\end{pmatrix}$	$\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$

6.6 Die Brauergruppe von $\mathbb{R}$

Satz. $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \simeq \mathbb{Z}/2\mathbb{Z}$.

Beweis. Der Satz folgt aus 6.5 und der Definition der Brauergruppe, vgl. 3.4 und 3.5. □

6.7 Der Satz von Tsen

Satz (Tsen 1933). *Sei K ein algebraisch abgeschlossener Körper, und sei F eine algebraische Körpererweiterung von $K(X)$. Dann ist* $\mathrm{Br}(F) = \{1\}$.

Beweis. steht z.B. in R.S. Pierce, Associative Algebras, Springer-Verlag 1982 (19.4a). □

Teil II
Kohomologische Beschreibung der Brauergruppe

Sei K ein Körper. Nach 5.8 ist

$$\boxed{\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)}\,,$$

wobei L alle (endlich) galoisschen Körpererweiterungen von K in $\overline{K}$ durchläuft (Dabei ist $\overline{K}$ ein algebraischer Abschluß von K). Die relative Brauergruppe

$$\mathrm{Br}(L/K) := \{[A] \in \mathrm{Br}(K) \mid [A \otimes_K L] = [L]\}$$

ist in 5.1 eingeführt worden. Wir werden u.a. zeigen

$$\boxed{\mathrm{Br}(L/K) \simeq H^2(G, L^*)}\,,$$

wobei L eine (endlich) galoissche Körpererweiterung von K mit Galoisgruppe G ist, und die zweite Kohomologiegruppe noch zu definieren ist.

7 Verschränkte Produkte

7.1 Definition

Eine Azumaya-Algebra A über K heißt *verschränktes Produkt*, falls A einen über K galoisschen Körper L enthält mit

$$\boxed{\dim_L A = \dim_K L}\,.$$

7.2 Ähnlichkeit mit einem verschränkten Produkt

Satz. *Jede Azumaya-Algebra A über K ist ähnlich einem verschränkten Produkt.*

Beweis. Nach 5.7 besitzt A einen (endlich) galoisschen Zerfällungskörper L über K, und nach 5.9 gibt es eine zu A ähnliche Azumaya-Algebra B über K, die L enthält, und für die gilt: $\dim_K B = (\dim_K L)^2$. Es folgt

$$(\dim_K L)(\dim_L B) \underset{\text{Aufgabe 8}}{=} \dim_K B = (\dim_K L)(\dim_K L)\,.$$

□

Bemerkung. S. A. Amitsur (Israel J. Math. 1972) gelang als erstem die Konstruktion eines über seinem Zentrum endlich-dimensionalen Schiefkörpers, der nicht isomorph zu einem verschränkten Produkt ist.

Fazit.
- Im Satz 5.6 kann also „separabel“ nicht durch „galoissch“ verschärft werden.
- Im Satz 7.2 kann also „ähnlich“ nicht durch „isomorph“ verschärft werden.

7.3 Strukturanalyse für verschränkte Produkte

Sei A ein verschränktes Produkt über K. Nach Definition 7.1 gibt es dann eine Galoiserweiterung L von K mit Gruppe G, so daß

$$\boxed{L \hookrightarrow A} \quad \text{und} \quad \boxed{\dim_L A = \dim_K L = |G|}$$

gilt, wobei $\dim_K L = |G|$ aus Algebra 15.7 folgt.
Nach dem Satz von Skolem-Noether 4.2 gibt es zu jedem $\sigma \in G$ ein $u_\sigma \in A^*$ mit $\sigma(x) = u_\sigma x u_\sigma^{-1}\ \forall x \in L$. Es folgt die Vertauschungsregel

(1) $$\boxed{u_\sigma x = \sigma(x) u_\sigma \qquad \forall x \in L,\ \sigma \in G}.$$

Wir benutzen (1) auch in den folgenden Formen. Ersetze x durch $\sigma^{-1}(x)$ in (1). Dann folgt

(1’) $$\boxed{u_\sigma \sigma^{-1}(x) = x u_\sigma \qquad \forall x \in L,\ \sigma \in G}.$$

Multipliziere (1’) von links und rechts mit u_σ^{-1}. Dann folgt

(1”) $$\boxed{\sigma^{-1}(x) u_\sigma^{-1} = u_\sigma^{-1} x \qquad \forall x \in L,\ \sigma \in G}.$$

Lemma 1. Die Elemente $u_\sigma, \sigma \in G$, sind L-linear unabhängig in A und bilden also eine Basis von A als L-Vektorraum.

Beweis. Nach dem Satz vom primitiven Element (Algebra 13.9) ist $L = K(x)$ mit einem $x \in L$. Hieraus folgt

(∗) $$\boxed{\sigma(x) \neq \tau(x) \qquad \forall \sigma, \tau \in G \text{ mit } \sigma \neq \tau},$$

denn nach Algebra 11.10 gibt es eine K-Basis von L, die aus Potenzen von x besteht. Die Rechtsmultiplikation $r_x \colon A \longrightarrow A$, $a \longmapsto ax$, ist L-linkslinear. Nach (1) ist $r_x(u_\sigma) = \sigma(x) u_\sigma\ \forall \sigma \in G$, und also ist $\sigma(x)$ Eigenwert von r_x zum Eigenvektor u_σ für jedes $\sigma \in G$. Es ist $u_\sigma \neq 0$, da $u_\sigma \in A^*$. Aus (∗) folgt nun, daß die $u_\sigma, \sigma \in G$, linear unabhängig über L sind, vgl. AGLA 9.6. Da $\dim_L A = |G|$ gilt, bilden sie sogar eine Basis. □

Lemma 2. Zu jedem $(\sigma,\tau) \in G \times G$ gibt es ein Element $f(\sigma,\tau) \in L^*$, so daß gelten:

$$\boxed{u_\sigma u_\tau = f(\sigma,\tau)u_{\sigma\tau} \qquad \forall\, \sigma,\tau \in G}\,, \tag{2}$$

$$\boxed{f(\sigma,\tau)f(\sigma\tau,\varrho) = \sigma(f(\tau,\varrho))f(\sigma,\tau\varrho) \qquad \forall\, \sigma,\tau,\varrho \in G}\,. \tag{3}$$

Beweis. Setze $f(\sigma,\tau) := u_\sigma u_\tau u_{\sigma\tau}^{-1}$. Dann ist (2) erfüllt, und es gilt $f(\sigma,\tau) \in A^*$. Für jedes $x \in L$ gilt

$$\begin{aligned}
f(\sigma,\tau)x &= u_\sigma u_\tau u_{\sigma\tau}^{-1}x && \text{nach Definition von } f(\sigma,\tau)\\
&= u_\sigma u_\tau(\sigma\tau)^{-1}(x)u_{\sigma\tau}^{-1} && \text{nach (1”)}\\
&= u_\sigma \tau((\sigma\tau)^{-1}(x))u_\tau u_{\sigma\tau}^{-1} && \text{nach (1)}\\
&= u_\sigma \sigma^{-1}(x)u_\tau u_{\sigma\tau}^{-1} && \text{da } \tau(\sigma\tau)^{-1} = \sigma^{-1}\\
&= xu_\sigma u_\tau u_{\sigma\tau}^{-1} && \text{nach (1')}\\
&= xf(\sigma,\tau)\,.
\end{aligned}$$

Es folgt $f(\sigma,\tau) \in \mathcal{Z}_A(L) \underset{4.7}{=} L$. Es ist nun noch (3) zu zeigen.

$$\begin{aligned}
(u_\sigma u_\tau)u_\varrho &= f(\sigma,\tau)u_{\sigma\tau}u_\varrho && \text{nach (2)}\\
&= f(\sigma,\tau)f(\sigma\tau,\varrho)u_{\sigma\tau\varrho}
\end{aligned}$$

nach (2)

$$\begin{aligned}
u_\sigma(u_\tau u_\varrho) &= u_\sigma f(\tau,\varrho)u_{\tau\varrho} && \text{nach (2)}\\
&= \sigma(f(\tau,\varrho))u_\sigma u_{\tau\varrho} && \text{nach (1)}\\
&= \sigma(f(\tau,\varrho))f(\sigma,\tau\varrho)u_{\sigma\tau\varrho} && \text{nach (2)}\,.
\end{aligned}$$

Da A assoziativ ist und $u_{\sigma\tau\varrho} \in A^*$ gilt, folgt (3). □

Lemma 3. Es ist $u_{\mathrm{id}} = f(\mathrm{id},\mathrm{id})$, also $u_{\mathrm{id}} \in L$.

Beweis. Wende (2) mit $\sigma = \mathrm{id} = \tau$ an. □

Fazit. Aus Lemma 1 folgt, daß die Multiplikation in A durch die Gleichungen (1) und (2) festgelegt ist. Die Gleichung (3) garantiert die Assoziativität, und aus Lemma 3 folgt $f(\mathrm{id},\mathrm{id})^{-1}u_{\mathrm{id}} = 1$.

Bemerkung. Die Ergebnisse dieses Abschnitts sind von Emmy Noether. Die Elemente $f(\sigma,\tau)$ in Lemma 2 heißen *Noethersches Faktorensystem*. Heutzutage spricht man von „Kozyklen“.

Wir fassen die Ergebnisse dieses Abschnitts in einem Satz zusammen.

Satz. *Sei L eine Galoiserweiterung von K mit Gruppe G, und sei A eine Azumaya-Algebra über K, die L enthalte und für die $\dim_L A = \dim_K L$ gelte. Dann gibt es zu jedem $\sigma \in G$ ein $u_\sigma \in A^*$ derart, daß $\{u_\sigma \mid \sigma \in G\}$ eine Basis von A als L-Vektorraum bildet, und die folgenden Gleichungen erfüllt sind:*

(1) $u_\sigma x = \sigma(x) u_\sigma \; \forall\, x \in L\,,\ \sigma \in G\,,$

(2) $u_\sigma u_\tau = f(\sigma,\tau) u_{\sigma\tau} \; \forall\, \sigma,\tau \in G\,.$

Dabei ist $f\colon G \times G \longrightarrow L^*$ *ein „2-Kozyklus", d.h. es gilt:*

(3) $f(\sigma,\tau) f(\sigma\tau,\varrho) = \sigma(f(\tau,\varrho)) f(\sigma,\tau\varrho) \; \forall\, \sigma,\tau,\varrho \in G\,.$

Beweis. folgt leicht aus obiger Strukturanalyse. □

7.4 Über 2-Zyklen

Sei L eine (endliche) Galoiserweiterung von K mit Gruppe G. Eine Abbildung $f\colon G \times G \longrightarrow L^*$ heißt 2-*Zyklus*, falls

(3) $$f(\sigma,\tau) f(\sigma\tau,\varrho) = \sigma(f(\tau,\varrho)) f(\sigma,\tau\varrho) \qquad \forall\, \sigma,\tau,\varrho \in G$$

gilt.

Bemerkung. Mit der Schreibweise $1 = 1_G$, also $1 = \mathrm{id}$ gelten:

(3a) $$f(\sigma,1) = \sigma(f(1,1)) \qquad \forall\, \sigma \in G$$
(3b) $$f(1,1) = f(1,\varrho) \qquad \forall\, \varrho \in G$$

Beweis. (3a): Wende (3) mit $\tau = 1 = \varrho$ an.
Dann folgt $f(\sigma,1) f(\sigma,1) = \sigma(f(1,1)) f(\sigma,1)$, und also (3a).

(3b): Wende (3) mit $\sigma = 1 = \tau$ an.
Dann folgt $f(1,1) f(1,\varrho) = f(1,\varrho) f(1,\varrho)$, und also (3b).

□

7.5 Konstruktion von verschränkten Produkten

Aus der Strukturanalyse 7.3 ergibt sich eine Konstruktionsmethode für Azumaya-Algebren.
Vorgegeben:

- L/K galoissch mit Gruppe G (endlich)

- Ein 2-Kozyklus $f\colon G \times G \longrightarrow L^*$. Es gelte also

$$(3) \qquad f(\sigma,\tau)f(\sigma\tau,\varrho) = \sigma(f(\tau,\varrho))f(\sigma,\tau\varrho) \qquad \forall\, \sigma,\tau,\varrho \in G$$

Ansatz: $A := \bigoplus_{\sigma\in G} Lu_\sigma$ mit formalen Symbolen u_σ.
Dann ist A ein $|G|$-dimensionaler L-Linksvektorraum.
Aufgabe: Eine Multiplikation in A so zu definieren, daß

$$(1) \qquad u_\sigma x = \sigma(x)u_\sigma \qquad \forall\, x \in L\,,\ \sigma \in G$$

$$(2) \qquad u_\sigma u_\tau = f(\sigma,\tau)u_{\sigma\tau} \qquad \forall\, \sigma,\tau \in G$$

gelten und A einfach und zentral über K ist.

Bemerkung. Die u_σ können als Abbildungen

$$u_\sigma\colon G \longrightarrow L\,,\ \tau \longmapsto \begin{cases} 1 & \sigma = \tau \\ 0 & \sigma \neq \tau \end{cases}$$

realisiert werden. Diese erzeugen einen $|G|$-dimensionalen L-Linksvektorraum.
(Sei $\sum_{\sigma\in G} x_\sigma u_\sigma = 0$ mit $x_\sigma \in L \Longrightarrow 0 = \sum_{\sigma\in G} x_\sigma u_\sigma(\tau) = x_\tau\ \forall\, \tau \in G$.)

Satz (E. Noether). *Sei L eine n-dimensionale Galoiserweiterung von K mit Gruppe G, und sei $f\colon G \times G \longrightarrow L^*$ ein 2-Kozyklus. Dann ist der n^2-dimensionale K-Vektorraum*

$$A := (L,G,f) := \bigoplus_{\sigma\in G} Lu_\sigma \qquad (u_\sigma \text{ formale Symbole})$$

mit der durch

$$\boxed{xu_\sigma \cdot yu_\tau = x\sigma(y)f(\sigma,\tau)u_{\sigma\tau} \text{ für } x,y \in L \text{ und } \sigma,\tau \in G}$$

definierten Multiplikation eine Azumaya-Algebra über K mit Einselement $1_A = f(\mathrm{id},\mathrm{id})^{-1}u_{\mathrm{id}}$. Ferner gelten:

(i) Durch $x \longmapsto x1_A$ wird L in A eingebettet.

(ii) Es ist $u_\sigma \in A^*\ \forall\, \sigma \in G$.

(iii) Es gilt $\mathcal{Z}_A(L) = L$.

Insbesondere ist L Zerfällungskörper von A, und A ist ein verschränktes Produkt.

Beweis in sieben Schritten.

Behauptung 1. Die Multiplikation ist assoziativ.

Beweis. Für $x, y, z \in L$ und $\sigma, \tau, \varrho \in G$ gelten nach Definition der Multiplikation:

$$\begin{aligned}(xu_\sigma \cdot yu_\tau) \cdot zu_\varrho &= x\sigma(y)f(\sigma,\tau)u_{\sigma\tau} \cdot zu_\varrho \\ &= x\sigma(y)f(\sigma,\tau)(\sigma\tau)(z)f(\sigma\tau,\varrho)u_{\sigma\tau\varrho} \\ &= x\sigma(y)(\sigma\tau)(z)f(\sigma,\tau)f(\sigma\tau,\varrho)u_{\sigma\tau\varrho}\,,\end{aligned}$$

da L kommutativ ist und

$$\begin{aligned}xu_\sigma \cdot (yu_\tau \cdot zu_\varrho) &= xu_\sigma \cdot y\tau(z)f(\tau,\varrho)u_{\tau\varrho} \\ &= x\sigma(y)\sigma(\tau(z))\sigma(f(\tau,\varrho))f(\sigma,\tau\varrho)u_{\sigma\tau\varrho}\,.\end{aligned}$$

Die Gleichheit folgt nun aus (3). □

Behauptung 2. Es ist $1_A = f(1,1)^{-1}u_1$, wobei $1 = 1_G = \mathrm{id}$ gilt, und durch $x \longmapsto x1_A$ wird L in A eingebettet.

Beweis. Es ist

$$\begin{aligned}xu_\sigma \cdot f(1,1)^{-1}u_1 &= x\sigma(f(1,1)^{-1})f(\sigma,1)u_\sigma \\ &= x1_Lu_\sigma && \text{nach (3a) in 7.4} \\ &= xu_\sigma\end{aligned}$$

und

$$\begin{aligned}f(1,1)^{-1}u_1 \cdot xu_\sigma &= f(1,1)^{-1}xf(1,\sigma)u_\sigma \\ &= 1_Lxu_\sigma && \text{da } L \text{ kommutativ und wegen (3b) in 7.4} \\ &= xu_\sigma\end{aligned}$$

Also ist $f(1,1)^{-1}u_1$ Einselement in A.
Die Abbildung $\varphi\colon L \longrightarrow A\,,\ x \longmapsto x1_A$, ist additiv. Ferner gilt:

$$\varphi(1_L) = \underbrace{1_Lf(1,1)^{-1}}_{\in L}u_1 = 1_A$$

und

$$\begin{aligned}\varphi(x)\cdot\varphi(y) &= xf(1,1)^{-1}u_1 \cdot yf(1,1)^{-1}u_1 \\ &= xf(1,1)^{-1}yf(1,1)^{-1}f(1,1)u_1 \\ &= xyf(1,1)^{-1}u_1 \\ &= \varphi(xy) && \forall x,y \in L\,.\end{aligned}$$

Nach 3.1 ist φ injektiv. □

Behauptung 3. Es gilt in A die Vertauschungsregel

$$(1) \qquad u_\sigma x = \sigma(x)u_\sigma \qquad \forall\, x \in L\,,\ \sigma \in G\,.$$

Beweis. Es ist

$$\begin{aligned} u_\sigma \cdot x1_A &= u_\sigma \cdot xf(1,1)^{-1}u_1 && \text{nach Behauptung 2} \\ &= \sigma(x)\sigma(f(1,1)^{-1})f(\sigma,1)u_\sigma \\ &= \sigma(x)u_\sigma && \text{nach (3a) in 7.4.} \end{aligned}$$

□

Behauptung 4. Es ist $u_\sigma \in A^*$ mit

$$u_\sigma^{-1} = f(\sigma^{-1},\sigma)^{-1}f(1,1)^{-1}u_{\sigma^{-1}} \qquad \forall\, \sigma \in G\,.$$

Beweis. Es ist

$$\begin{aligned} f(\sigma^{-1},\sigma)^{-1}f(1,1)^{-1}u_{\sigma^{-1}} \cdot u_\sigma &= f(\sigma^{-1},\sigma)^{-1}f(1,1)^{-1}f(\sigma^{-1},\sigma)u_1 \\ &= 1_A \quad \text{nach Behauptung 2} \end{aligned}$$

und

$$\begin{aligned} u_\sigma \cdot f(\sigma^{-1},\sigma)^{-1}f(1,1)^{-1}u_{\sigma^{-1}} &= \sigma(f(\sigma^{-1},\sigma))^{-1}\sigma(f(1,1))^{-1}f(\sigma,\sigma^{-1})u_1 \\ &= f(1,1)^{-1}u_1 \quad \text{nach Aufgabe 21} \\ &= 1_A\,. \end{aligned}$$

□

Behauptung 5. A ist einfach.

Beweis. Sei I ein zweiseitiges Ideal $\neq (0)$ in A, und sei

$$a = x_{\sigma_1}u_{\sigma_1} + \cdots + x_{\sigma_r}u_{\sigma_r} \text{ in } I\,,\ a \neq 0\,,\ x_{\sigma_i} \in L^*$$

mit minimalem $r \geq 1$. Angenommen, $r > 1$. Wähle $y \in L$ mit $\sigma_1(y) \neq \sigma_2(y)$. Nach (1) in Behauptung 3 ist dann

$$\sigma_1(y)^{-1}ay = \sigma_1(y)^{-1}x_{\sigma_1}\sigma_1(y)u_{\sigma_1} + \underbrace{\sigma_1(y)^{-1}x_{\sigma_2}\sigma_2(y)u_{\sigma_2}}_{\neq x_{\sigma_2}} + \cdots$$

und also ist $a - \sigma_1(y)^{-1}ay \neq 0$ ein Element in I, dessen Basisdarstellung kürzere Länge als r hat. Also enthält I ein Element $a = xu_\sigma$ mit $x \in L^*$, wobei $\sigma \in G$. Nach Behauptung 4 ist also $a \in A^*$, und es folgt

$$\underbrace{a^{-1}}_{\in A^*}\underbrace{a}_{\in I} = 1_A \in I\,.$$

□

Behauptung 6. A ist zentral über K, d.h. es gilt $\mathcal{Z}(A) = K$.

Beweis. „$\supset$“: nach (1) in Behauptung 3 gilt $u_\sigma\lambda = \lambda u_\sigma\ \forall\,\lambda \in K$, also $K \subset \mathcal{Z}(A)$.

„$\subset$“: Sei $a = \sum\limits_{\sigma\in G} x_\sigma u_\sigma \in \mathcal{Z}(A)$ mit $x_\sigma \in L$. Für jedes $y \in L$ ist dann

$$0 = ya - ay \underset{(1)}{=} \sum_{\sigma\in G} x_\sigma(y - \sigma(y))u_\sigma\,.$$

Wähle y so, daß $\sigma(y) \neq y\ \forall\,\sigma \in G\backslash\{1\}$ gilt. Dann folgt $x_\sigma = 0\ \forall\,\sigma \neq 1$, da u_σ linear unabhängig über L sind, und also gilt $a = x_1u_1 \in L$ (da $u_1 = f(1,1)^{-1}1_A \in L$ nach Behauptung 2). Es folgt

$$\begin{aligned} 0 &= u_\sigma a - au_\sigma\,, && \text{da } a \in \mathcal{Z}(A) \\ &= \sigma(a)u_\sigma - au_\sigma && \text{nach (1) in Behauptung 3} \\ &= (\sigma(a) - a)u_\sigma && \forall\,\sigma \in G\,, \end{aligned}$$

und also $\sigma(a) = a\ \forall\,\sigma \in G$. Daher gilt $a \in L^G = K$.

□

Behauptung 7. $L = \mathcal{Z}_A(L)$ ist Zerfällungskörper von A, und A ist ein verschränktes Produkt.

Beweis. Dies folgt aus 4.7 und 5.1. □

□

7.6 Über 2-Koränder

Definition. Seien L und G wie in 7.5. Eine Abbildung $f\colon G \times G \longrightarrow L^*$ heißt 2-*Korand*, falls es eine Abbildung $\lambda\colon G \longrightarrow L^*$ gibt, so daß

$$f(\sigma,\tau) = \lambda(\sigma)\,\sigma(\lambda(\tau)) \cdot \lambda(\sigma\tau)^{-1} \qquad\qquad \forall\,\sigma,\tau \in G$$

gilt.

Bemerkung. Jeder 2-Korand ist ein 2-Kozyklus, wie man durch Einsetzen in (3) nachprüft.

7.7 Kriterium für Isomorphie von verschränkten Produkten

Gegeben sei eine (endliche) Galoiserweiterung L von K mit Gruppe G.

Satz (E. Noether). *Seien $f, g\colon G \times G \longrightarrow L^*$ zwei 2-Kozyklen, $A := (L, G, f) = \bigoplus_{\sigma \in G} Lu_\sigma$ und $B := (L, G, g) = \bigoplus_{\sigma \in G} Lv_\sigma$ die gemäß 7.5 zugehörigen verschränkten Produkte. Dann sind äquivalent:*

(a) Es gibt eine K-Algebraisomorphie $(L, G, f) \simeq (L, G, g)$.

(b) Es gibt eine Abbildung $\lambda\colon G \longrightarrow L^*$, so daß gilt:

$$\boxed{f(\sigma, \tau) = \lambda(\sigma\tau)^{-1}\lambda(\sigma)\,\sigma(\lambda(\tau))\,g(\sigma, \tau) \qquad \forall\, \sigma, \tau \in G}.$$

Beweis. „(a) $\Longrightarrow$ (b)“: Es gibt einen Isomorphismus $\varphi\colon A \xrightarrow{\sim} B$ mit

(I) $$\boxed{\varphi(x1_A) = x1_B \qquad \forall\, x \in L},$$

denn: Sei $\phi\colon A \xrightarrow{\sim} B$ irgendein (nach (a) existierender) Isomorphismus. Wende den Satz von Skolem-Noether 4.2 auf das Kompositum $L \hookrightarrow A \xrightarrow{\phi} B$, $x \longmapsto \phi(x1_A)$, und die Einbettung $L \hookrightarrow B$, $x \longmapsto x1_B$, an.
Dann gibt es ein $v \in B^*$ so, daß $x1_B = v\phi(x1_A)v^{-1}$ $\forall\, x \in L$ gilt. Der Automorphismus $\psi\colon B \longrightarrow B$, $b \longmapsto vbv^{-1}$, erfüllt dann

$$\psi(\phi(x1_A)) = v\phi(x1_A)v^{-1} = x1_B \;\forall\, x \in L.$$

Setze $\varphi = \psi \circ \phi$. Dann gilt (I). Setze

$$\boxed{\lambda(\sigma) := \varphi(u_\sigma)v_\sigma^{-1} \text{ für } \sigma \in G}.$$

Dann ist $\lambda(\sigma) \in B^*$, und für alle $x \in L$, $\sigma \in G$ gilt:

$$\begin{aligned}
\lambda(\sigma)x1_B &= \varphi(u_\sigma)v_\sigma^{-1}x1_B \\
&= \varphi(u_\sigma)\sigma^{-1}(x)1_B v_\sigma^{-1} && \text{vgl. (1”) in 7.3} \\
&= \varphi(u_\sigma)\varphi(\sigma^{-1}(x)1_A)v_\sigma^{-1} && \text{nach (I)} \\
&= \varphi(u_\sigma\sigma^{-1}(x)1_A)v_\sigma^{-1}, && \text{da } \varphi \text{ multiplikativ} \\
&= \varphi(x1_A u_\sigma)v_\sigma^{-1} && \text{nach Behauptung 3 in 7.5} \\
&= x1_B\varphi(u_\sigma)v_\sigma^{-1} && \text{nach (I), da } \varphi \text{ multiplikativ} \\
&= x1_B\lambda(\sigma) && \text{nach Definition von } \lambda.
\end{aligned}$$

Also ist $\lambda(\sigma) \in \mathcal{Z}_B(L) \underset{7.5}{=} L$. Es gilt

$$\begin{aligned}
\varphi(u_\sigma u_\tau) &= \varphi(f(\sigma,\tau)\, u_{\sigma\tau}) && \text{nach 7.5} \\
&= f(\sigma,\tau)\, \varphi(u_{\sigma\tau}) && \text{nach (I), da } \varphi \text{ multiplikativ} \\
&= f(\sigma,\tau)\, \lambda(\sigma\tau)\, v_{\sigma\tau} && \text{nach Definition von } \lambda\,.
\end{aligned}$$

Andererseits gilt

$$\begin{aligned}
\varphi(u_\sigma u_\tau) &= \varphi(u_\sigma)\cdot\varphi(u_\tau)\,, && \text{da } \varphi \text{ multiplikativ} \\
&= \lambda(\sigma) v_\sigma \cdot \lambda(\tau) v_\tau && \text{nach Definition von } \lambda \\
&= \lambda(\sigma)\, \sigma(\lambda(\tau))\, g(\sigma,\tau)\, v_{\sigma\tau} && \text{nach 7.5}\,.
\end{aligned}$$

Es folgt (b).

„(b) $\Longrightarrow$ (a)“: Definiere $\varphi\colon A \longrightarrow B$ durch

$$\boxed{\varphi(xu_\sigma) = x\lambda(\sigma)\, v_\sigma \qquad \forall\, x \in L\,,\ \sigma \in G}\,.$$

Dann ist

$$\begin{aligned}
\varphi(1_A) &= \varphi(f(1,1)^{-1} u_1) && \text{nach 7.5 (mit } 1 = \mathrm{id} = 1_G) \\
&= f(1,1)^{-1} \lambda(1)\, v_1 && \text{nach Definition von } \varphi \\
&= g(1,1)^{-1} v_1 && \text{nach (b) für } \sigma = 1 = \tau \\
&= 1_B && \text{nach 7.5.}
\end{aligned}$$

Ferner gelten

$$\begin{aligned}
\varphi(xu_\sigma \cdot yv_\tau) &\underset{7.5}{=} \varphi(x\sigma(y)\, f(\sigma,\tau)\, u_{\sigma\tau}) \\
&= x\sigma(y)\, f(\sigma,\tau)\, \lambda(\sigma\tau)\, v_{\sigma\tau} \\
&= x\sigma(y)\, \lambda(\sigma)\, \sigma(\lambda(\tau))\, g(\sigma,\tau)\, v_{\sigma\tau} && \text{nach (b)} \\
&= x\lambda(\sigma)\, \sigma(y\lambda(\tau))\, g(\sigma,\tau)\, v_{\sigma\tau}
\end{aligned}$$

und

$$\begin{aligned}
\varphi(xu_\sigma)\cdot\varphi(yu_\tau) &= x\lambda(\sigma)\, v_\sigma \cdot y\lambda(\tau)\, v_\tau && \text{nach Definition von } \varphi \\
&= x\lambda(\sigma)\, \sigma(y\lambda(\tau))\, g(\sigma,\tau)\, v_{\sigma\tau} && \text{nach 7.5.}
\end{aligned}$$

Nach 3.1 ist φ injektiv und daher aus Dimensionsgründen auch surjektiv.

□

7.8 Die zweite Kohomologiegruppe

Sei L (endlich) galoissch über K mit Gruppe G. In 7.4 haben wir einen 2-Kozyklus als Abbildung $f\colon G\times G \longrightarrow L^*$ definiert, so daß

$$(3) \qquad f(\sigma,\tau)f(\sigma\tau,\varrho)=\sigma(f(\tau,\varrho))f(\sigma,\tau\varrho) \qquad \forall\,\sigma,\tau,\varrho\in G$$

gilt. Die 2-Kozyklen bilden eine abelsche Gruppe, wobei die Verknüpfung durch

$$(fg)(\sigma,\tau)=f(\sigma,\tau)\,g(\sigma,\tau)\ \forall\,\sigma,\tau\in G$$

gegeben ist. Das Einselement ist der 2-Kozyklus $G\times G\longrightarrow L^*$, $(\sigma,\tau)\longmapsto 1$, und $f^{-1}\colon G\times G\longrightarrow L^*$, $(\sigma,\tau)\longmapsto f(\sigma,\tau)^{-1}$, ist invers zu f. Die Gruppe der 2-Kozyklen bezeichnen wir mit $\mathcal{Z}^2(G,L^*)$.
Nach 7.6 heißt ein 2-Kozyklus ein 2-Korand, falls ein $\lambda\colon G\longrightarrow L^*$ so existiert, daß $f(\sigma,\tau)=\lambda(\sigma\tau)^{-1}\lambda(\sigma)\,\sigma(\lambda(\tau))\ \forall\,\sigma,\tau\in G$. Die 2-Koränder bilden eine Untergruppe von $\mathcal{Z}^2(G,L^*)$. Diese bezeichnen wir mit $\mathcal{B}^2(G,L^*)$. Die Faktorgruppe $\mathcal{H}^2(G,L^*):=\mathcal{Z}^2(G,L^*)/\mathcal{B}^2(G,L^*)$ heißt *zweite Kohomologiegruppe von G mit Werten in L^**. Für $f\in\mathcal{Z}^2(G,L^*)$ bezeichne $[f]$ die zugehörige Nebenklasse in $\mathcal{H}^2(G,L^*)$.

Bemerkung. Seien $f,g\in\mathcal{Z}^2(G,L^*)$ und seien (L,G,f) und (L,G,g) die gemäß 7.5 zugehörigen verschränkten Produkte. Dann gilt:

$$\begin{aligned}\boxed{(L,G,f)\sim(L,G,g)} &\iff \boxed{(L,G,f)\simeq(L,G,g)} && \text{nach Folgerung 3.4}\\ &\iff [f]=[g] && \text{nach 7.7.}\end{aligned}$$

Sei $n=|G|$, dann folgt spezieller

$$\begin{aligned}(L,G,f)\sim K &\iff (L,G,f)\simeq \mathrm{M}_{n\times n}(K) && \text{nach 3.4}\\ &\iff (L,G,f)\simeq(L,G,1) && \text{nach Aufgabe 24}\\ &\iff f \text{ ist ein 2-Korand.}\end{aligned}$$

7.9 Die erste Kohomologiegruppe

Sei L (endlich) galoissch mit Gruppe G über K. Ein 1-*Kozyklus* ist eine Abbildung $f\colon G\longrightarrow L^*$ mit

$$\boxed{f(\sigma\tau)=f(\sigma)\sigma(f(\tau)) \quad \forall\,\sigma,\tau\in G}\,.$$

Ein 1-Kozyklus heißt 1-*Korand*, falls es ein $x\in L^*$ gibt, so daß gilt:

$$\boxed{f(\sigma)=\sigma(x)x^{-1} \quad \forall\,\sigma\in G}\,.$$

Sei $\mathcal{Z}^1(G, L^*)$ die Gruppe der 1-Kozyklen $G \longrightarrow L^*$ und $\mathcal{B}^1(G, L^*)$ die Untergruppe der 1-Koränder. Setze $\mathcal{H}^1(G, L^*) := \mathcal{Z}^1(G, L^*)/\mathcal{B}^1(G, L^*)$. Dann heißt $\mathcal{H}^1(G, L^*)$ *erste Kohomologiegruppe von G mit Werten in L^*.*

Noethersche Gleichung. Es ist $\mathcal{H}^1(G, L^*) = \{1\}$.

Beweis. Sei $f\colon G \longrightarrow L^*$ ein 1-Kozyklus. Da die Automorphismen aus G linear unabhängig über L sind (Algebra 18.4), gibt es ein $c \in L$, so daß

$$b := \sum_{\tau \in G} f(\tau)\,\tau(c) \neq 0$$

ist. Es ist dann

$$\begin{aligned} \sigma(b) &= \sum_{\tau \in G} \sigma(f(\tau))\,\sigma(\tau(c)) \\ &= \sum_{\tau \in G} f(\sigma\tau) f(\sigma)^{-1} \sigma(\tau(c))\,, \qquad && \text{da } f \text{ ein Kozyklus ist} \\ &= b f(\sigma)^{-1}\,. \end{aligned}$$

Setze $x := b^{-1}$. Dann folgt $f(\sigma) = \sigma(x)x^{-1}\ \forall\, \sigma \in G$. $\square$

8 Die Isomorphie $H^2(G, L^*) \simeq \mathrm{Br}(L/K)$

Sei L eine (endliche) Galoiserweiterung von K mit Gruppe G.

8.1 Normierung von 2-Kozykeln

Ein 2-Kozyklus f heißt *normiert*, falls

$$\boxed{f(1,\sigma) = f(\sigma,1) = 1 \qquad \forall\, \sigma \in G}$$

gilt.

Lemma. *Zu jedem 2-Kozyklus $g\colon G \times G \longrightarrow L^*$ gibt es einen normierten 2-Kozyklus $f\colon G \times G \longrightarrow L^*$, so daß $[f] = [g]$ in $\mathcal{H}^2(G, L^*)$ gilt.*

Beweis. Definiere $\lambda\colon G \longrightarrow L^*$, $\sigma \longmapsto g(1,1)^{-1}$ und $f\colon G \times G \longrightarrow L^*$, $(\sigma,\tau) \longmapsto \lambda(\sigma\tau)^{-1}\lambda(\sigma)\,\sigma(\lambda(\tau))\,g(\sigma,\tau)$. Dann ist $f \in \mathcal{Z}^2(G, L^*)$, und es ist $[f] = [g]$, vgl. 7.8. Es ist

$$\begin{aligned}
f(\sigma,1) &= \lambda(\sigma)^{-1}\lambda(\sigma)\,\sigma(\lambda(1))\,g(\sigma,1) && \text{nach Definition von } f\\
&= \sigma(g(1,1))^{-1}g(\sigma,1) && \text{nach Definition von } \lambda\\
&= g(\sigma,1)^{-1}g(\sigma,1) && \text{nach (3a) in 7.4}\\
&= 1\,, \\
f(1,\sigma) &= \lambda(\sigma)^{-1}\lambda(1)\,\lambda(\sigma)\,g(1,\sigma) && \text{nach Definition von } f\\
&= g(1,1)^{-1}g(1,\sigma) && \text{nach Definition von } \lambda\\
&= 1 && \text{nach (3b) in 7.4.}
\end{aligned}$$

□

Folgerung. *Ist $f \in \mathcal{Z}^2(G, L^*)$ normiert, so ist u_1 das Einselement des in 7.5 konstruierten verschränkten Produkts (L, G, f), wobei $1 = 1_G = \mathrm{id}$ sei.*

8.2 Multiplikativitätssatz

Satz. *Seien $f, g\colon G \times G \longrightarrow L^*$ normierte 2-Kozyklen. Dann gilt:*

$$\boxed{(L,G,f) \otimes_K (L,G,g) \sim (L,G,fg)}\,.$$

nach S. Chase, *Communications in Algebra, 12, 1984.* Zu f, g und fg gehören nach 7.5 die Azumaya-Algebren $A := (L,G,f) = \bigoplus_{\sigma \in G} Lu_\sigma$, $B := (L,G,g) = \bigoplus_{\sigma \in G} Lv_\sigma$ und $C := (L,G,fg) = \bigoplus_{\sigma \in G} Lw_\sigma$ über K mit der dort definierten

Multiplikation.
Zu zeigen: $A \otimes_K B \sim C$. Sei $\boxed{M := A\dot{\otimes}_L B}$ das Tensorprodukt der L-Linksvektorräume A und B, es gilt also

(i) $$\boxed{xa\dot{\otimes}b = a\dot{\otimes}xb \qquad \forall\, x \in L\,,\ a \in A\,,\ b \in B}\,.$$

Zwischenbemerkung: In der Definition von $A \otimes_L B$ (ohne Punkt) ist A ein L-Rechtsvektorraum und B ein L-Linksvektorraum (vgl. Algebra 10.7), und es gilt im Kontrast zu (i) zum Beispiel

$$\begin{aligned} u_\sigma \otimes xb &= u_\sigma x \otimes b && \text{wegen der } L\text{-Rechtsstruktur von } A\\ &= \sigma(x)\, u_\sigma \otimes b && \text{nach Behauptung 3 in 7.5.} \end{aligned}$$

Behauptung 1. M ist ein C-Linksmodul.

Beweis. Aus (i) und der universellen Eigenschaft des Tensorprodukts ersieht man, daß die C-Linksstruktur von M durch

(ii) $$\boxed{xw_\sigma(a\dot{\otimes}b) = xu_\sigma a\dot{\otimes}v_\sigma b}$$

für alle $x \in L$, $\sigma \in G$, $a \in A$, $b \in B$ wohldefiniert ist, vgl. Aufgabe 28. Es ist

$$\begin{aligned} 1_C(a\dot{\otimes}b) &= w_1(a\dot{\otimes}b) && \text{nach Folgerung 8.1}\\ &= u_1a\dot{\otimes}v_1b && \text{nach (ii)}\\ &= a\dot{\otimes}b\,, && \text{da } u_1 = 1_A \text{ und } v_1 = 1_B \text{ nach Folgerung 8.1.} \end{aligned}$$

Prüfe nun nach, daß $(cc')m = c(c'm)$ für $c = xw_\sigma$, $c' = x'w_\tau$ und $m = a\dot{\otimes}b$ gilt. Nach Definition von C und 7.5 gilt

(iii) $$\boxed{w_\sigma w_\tau = f(\sigma,\tau)\, g(\sigma,\tau) w_{\sigma\tau} \qquad \forall\, \sigma,\tau \in G}\,.$$

Es folgt

$$\begin{aligned} (xw_\sigma \cdot x'w_\tau)(a\dot{\otimes}b) &= x\sigma(x')\, f(\sigma,\tau)\, g(\sigma,\tau)\, w_{\sigma\tau}(a\dot{\otimes}b)\\ &= x\sigma(x')\, f(\sigma,\tau) u_{\sigma\tau} a\dot{\otimes} g(\sigma,\tau)\, v_{\sigma\tau} b && \text{nach (ii) und (i)}\\ &= xu_\sigma \cdot x'u_\tau a\dot{\otimes}v_\sigma v_\tau b && \text{nach 7.5}\\ &= xw_\sigma(x'u_\tau a\dot{\otimes}v_\tau b) && \text{nach (ii)}\\ &= xw_\sigma(x'w_\tau(a\dot{\otimes}b)) && \text{nach (ii).} \end{aligned}$$

Die übrigen Modul-Postulate sind leichter nachzurechnen. □

Aufgrund von Behauptung 1 gibt es die K-Unteralgebra $\operatorname{End}_C M$ von $\operatorname{End}_K M$.

Behauptung 2. Es gibt K-Algebraisomorphien

$$\operatorname{End}_C M \simeq \mathrm{M}_{n\times n}(C^{\mathrm{op}}) \simeq C^{\mathrm{op}} \otimes_K \mathrm{M}_{n\times n}(K)$$

mit $n = |G|$.

Beweis. Es ist

$$\begin{aligned} \dim_L M &= (\dim_L A)(\dim_L B) && \text{nach Definition von } M \\ &= n^2 = \dim_K C && \text{nach 7.5.} \end{aligned}$$

Es folgt

$$\begin{aligned} \dim_K M &= (\dim_K L)(\dim_L M) && \text{nach Aufgabe 8} \\ &= n \dim_K C = \dim_K(C^n)\,. \end{aligned}$$

Nach 4.1 gibt es daher eine C-Modulisomorphie $M \simeq C^n$. Da C^n ein freier C-Modul ist, folgt

$$\operatorname{End}_C(C^n) \simeq \mathrm{M}_{n\times n}(C^{\mathrm{op}}) \qquad \simeq C^{\mathrm{op}} \otimes_K \mathrm{M}_{n\times n}(K) \qquad \text{nach Aufgabe 10.}$$

□

Die Rechtsmultiplikation $r_y \colon M \longrightarrow M\,,\ m \longmapsto my$, mit $y \in A \otimes_K B$ ist C-linkslinear. Sie ist gegeben durch

$$(a'\dot{\otimes}b')(a \otimes b) = a'a\dot{\otimes}b'b \qquad\qquad \forall\, a, a' \in A\,,\ b, b' \in B\,.$$

Behauptung 3. Die K-lineare Abbildung

$$\psi \colon (A \otimes_K B)^{\mathrm{op}} \longrightarrow \operatorname{End}_C M\,,\ y \longmapsto r_y\,,$$

ist ein Isomorphismus von K-Algebren.

Beweis. Es ist $\psi(1) = \mathrm{id}_M$ und

$$\begin{aligned} (\psi(y) \circ \psi(z))(m) &= \psi(y)(mz) = mzy \\ &= my * z\,, && \text{wobei } * \text{ das Produkt in } (A \otimes_K B)^{\mathrm{op}} \text{ ist} \\ &= \psi(y * z)(m) && \forall\, y, z \in (A \otimes_K B)^{\mathrm{op}} \text{ und } m \in M\,. \end{aligned}$$

Nach 3.1 ist ψ injektiv, und es gilt

$$\dim_K(\operatorname{End}_C M) = n^2 \cdot n^2 = \dim_K (A \otimes_K B)^{\mathrm{op}}\,.$$

Also ist ψ auch surjektiv. □

$\square$

Fazit. Nach Behauptung 2 und 3 gilt

$$(A \otimes_K B)^{\mathrm{op}} \simeq C^{\mathrm{op}} \otimes_K \mathrm{M}_{n \times n}(K) \simeq C^{\mathrm{op}} \qquad \text{nach 3.4.}$$

Es folgt $A \otimes_K B \simeq C$.

8.3 Hauptsatz

Theorem. *Sei L eine (endliche) Galoiserweiterung von K mit Gruppe G . Dann gibt es einen Gruppenisomorphismus*

$$\alpha_{L/K} \colon \mathcal{H}^2(G, L^*) \xrightarrow{\sim} \mathrm{Br}(L/K)\,,$$

so daß $\alpha_{L/K}([f]) = [(L, G, f)]$ für jedes $f \in \mathcal{Z}^2(G, L^*)$ gilt.

Beweis. Nach Bemerkung 7.8 ist $\alpha_{L/K}$ wohldefiniert und injektiv. Aus 8.1 und 8.2 folgt, daß $\alpha_{L/K}$ ein Gruppenhomomorphismus ist. Aus 7.2 und 7.3 folgt, daß $\alpha_{L/K}$ surjektiv ist. $\square$

8.4 Die Isomorphie $\mathcal{H}^2(K) \simeq \mathrm{Br}(K)$

Nach 5.8 ist $\mathrm{Br}(K) = \bigcup \mathrm{Br}(L/K)$, wobei L alle über K (endlich) galoisschen Körper in einem algebraischen Abschluß $\overline{K}$ von K durchläuft. Sei $G_{L/K}$ die Galoisgruppe von L über K , und sei $\mathcal{H}^2_L := \mathcal{H}^2(G_{L/K}, L^*)$. In 8.6 werden wir im Fall $L \subset L'$ die sogenannte „Inflationsabbildung“ $\inf_{L \subset L'} \colon \mathcal{H}^2_L \longrightarrow \mathcal{H}^2_{L'}$ einführen. Diese ist injektiv, und man erhält ein induktives (oder direktes) System, d.h. es gilt $\inf_{L \subset L} = \mathrm{id}$ und $\inf_{L \subset L''} = \inf_{L' \subset L''} \circ \inf_{L \subset L'}$. Ferner ist die Menge $\{L \subset \overline{K} \mid L/K \text{ endlich galoissch }\}$ „gerichtet“, d.h. zu L, L' existiert ein L'' mit $L \subset L''$ und $L' \subset L''$. Hieraus folgt dann die Existenz des „induktiven Limes“ $\mathcal{H}^2(K) := \varinjlim_{L} \mathcal{H}^2_L$. Aus 8.3, dem Inflationssatz 8.6, 8.7 unten folgt dann

$$\mathcal{H}^2(K) \simeq \mathrm{Br}(K)\,.$$

8.5 Ein Darstellungslemma

Sei L eine (endlich) galoissche Erweiterung von K mit Gruppe G . Ferner sei F ein über K galoisscher Zwischenkörper, es gelte also

$$K \hookrightarrow F \hookrightarrow L$$

und $\sigma(x) \in F \; \forall x \in F$, $\sigma \in G$, vgl. Algebra, Satz 16.3. Sei $r := \dim_F L$, und $\sigma \in G$ wirke auf Matrizen über F koeffizientenweise.

Lemma. *Es gibt einen injektiven F-Algebrahomomorphismus*

$$\boxed{\ell\colon L \longrightarrow \mathrm{M}_{r\times r}(F)\,,\ x \longmapsto \ell_x}\,,$$

und zu jedem $\sigma \in G$ eine Matrix $U_\sigma \in \mathrm{M}_{r\times r}(F)$, so daß gelten:

(a) $U_\sigma\sigma(\ell_x) = \ell_{\sigma(x)}U_\sigma \;\forall\, \sigma \in G\,,\ x \in L\,,$

(b) $U_{\sigma\tau} = U_\sigma\sigma(U_\tau) \;\forall\, \sigma, \tau \in G\,.$

Ferner ist $U_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

Beweis. Wähle eine Basis $\{a_1, \ldots, a_r\}$ von L als F-Rechtsvektorraum und stelle die Linksmultiplikation mit $x \in L$ in $\mathrm{M}_{r\times r}(F)$ dar. Für jedes $x \in L$ und $j = 1, \ldots, r$ ist dann

$$xa_j = a_1x_{1j} + \cdots + a_rx_{rj} \qquad\qquad \text{mit } x_{1j}, \ldots, x_{rj} \in F\,.$$

Setze $\ell_x := \begin{pmatrix} x_{11} & \cdots & x_{1r} \\ \vdots & \ddots & \vdots \\ x_{r1} & \cdots & x_{rr} \end{pmatrix}$. Jedes $\sigma \in G$ wird dargestellt vermöge

$$\boxed{\sigma(a_j) = \sum_{i=1}^{r} a_iu_{ij}^{(\sigma)} \quad \text{mit } u_{ij}^{(\sigma)} \in F}\,,$$

also durch $U_\sigma := \begin{pmatrix} u_{11}^{(\sigma)} & \cdots & u_{1r}^{(\sigma)} \\ \vdots & \ddots & \vdots \\ u_{r1}^{(\sigma)} & \cdots & u_{rr}^{(\sigma)} \end{pmatrix}$. Sei L^r der L-Vektorraum der Zeilen $(x_1, \ldots, x_r)$ mit $x_1, \ldots, x_r \in L$. Mit $\vec{a} = (a_1, \ldots, a_r)$ gilt dann in Matrizenschreibweise

(i) $$\boxed{x\vec{a} = \vec{a}\ell_x \quad \forall\, x \in L}\,,$$

(ii) $$\boxed{\sigma(\vec{a}) = \vec{a}U_\sigma \quad \forall\, \sigma \in G}\,.$$

Zeige nun (a): Es ist

$$\begin{aligned} \vec{a}U_\sigma(\ell_x) &\underset{\text{(ii)}}{=} \sigma(\vec{a})\sigma(\ell_x) = \sigma(\vec{a}\ell_x) \\ &\underset{\text{(i)}}{=} \sigma(x\vec{a}) = \sigma(x)\sigma(\vec{a}) \\ &\underset{\text{(ii)}}{=} \sigma(x)\vec{a}U_\sigma \underset{\text{(i)}}{=} \vec{a}\ell_{\sigma(x)}U_\sigma\,. \end{aligned}$$

Hieraus folgt (a), da $a_1, \ldots, a_r$ linear unabhängig über F sind.
Zeige (b): Es ist

$$\begin{aligned} \vec{a}U_{\sigma\tau} &\underset{\text{(ii)}}{=} \sigma\tau(\vec{a}) = \sigma(\tau(\vec{a})) \\ &\underset{\text{(ii)}}{=} \sigma(\vec{a}U_\tau) = \sigma(\vec{a})\sigma(U_\tau) \\ &\underset{\text{(ii)}}{=} \vec{a}U_\sigma\sigma(U_\tau)\,. \end{aligned}$$

Hieraus folgt (b), da $a_1,\dots,a_r$ linear unabhängig über F sind.
Die Abbildung $\ell\colon L \longrightarrow \mathrm{M}_{r\times r}(F)$, $x \longmapsto \ell_x$, ist ersichtlich additiv und injektiv. Es ist $\ell_x = \begin{pmatrix} x & & 0 \\ & \ddots & \\ 0 & & x \end{pmatrix}$ $\forall x \in F$, da $xa_j = a_j x$ Basisdarstellung bezüglich der Basis $\{a_1,\dots,a_r\}$ $\forall x \in F$ ist. Sei $\ell_{xy} = \begin{pmatrix} z_{11} & \cdots & z_{1r} \\ \vdots & \ddots & \vdots \\ z_{r1} & \cdots & z_{rr} \end{pmatrix}$. Für $j = 1,\dots,r$ gilt also

$$\begin{aligned}\sum_{k=1}^{r} a_k z_{kj} = (xy)a_j \underset{\text{L assoziativ}}{=} x(ya_j) &= \sum_{i=1}^{r} x a_i y_{ij} \\ = \sum_{i=1}^{r}\left(\sum_{k=1}^{r} a_k x_{ki}\right) y_{ij} &= \sum_{k=1}^{r} a_k \left(\sum_{i=1}^{r} x_{ki} y_{ij}\right),\end{aligned}$$

und es folgt $\ell_{xy} = \ell_x \circ \ell_y$. □

Ziel: kommutatives Diagramm

$$\begin{tikzcd} \mathcal{H}^2(G(F/K),F^*) \arrow[r, "\sim", "\alpha_{F/K}"'] \arrow[d, dashed, "\text{„Inflationssatz“}"] & \mathrm{Br}(F/K) \arrow[d, hook] \\ \mathcal{H}^2(G(L/K),L^*) \arrow[r, "\sim", "\alpha_{L/K}"'] & \mathrm{Br}(L/K) \end{tikzcd}$$

8.6 Inflationssatz

Sei L eine (endliche) Galoiserweiterung von K mit Gruppe $G = G(L/K)$, und sei F ein über K galoisscher Zwischenkörper. Es gelte also $K \subset F \subset L$ und $G(F/K) = G/H$, wobei $H = G(L/F)$ ist. Es gibt dann einen wohldefinierten Gruppenhomomorphismus

$$\inf_{F\subset L}\colon \mathcal{H}^2(G/H,F^*) \longrightarrow \mathcal{H}^2(G,L^*),\ [\overline{f}] \longmapsto [f],$$

wobei f das Kompositum

$$G\times G \xrightarrow{\text{kan}} G/H \times G/H \xrightarrow{\overline{f}} F^* \hookrightarrow L^*$$

sei (und $\overline{f} \in \mathcal{Z}^2(G/H,F^*)$ vorgegeben). Es gilt also $f(\sigma,\tau) = \overline{f}(\overline{\sigma},\overline{\tau})\ \forall \sigma,\tau \in G$. Dabei ist $\overline{\varrho} = \varrho H\ \forall \varrho \in G$. Der 2-Kozyklus f heißt *Inflation von* $\overline{f}$ und wird mit $\inf \overline{f}$ bezeichnet.

Satz (H. Hasse 1933, Math. Annalen 107). *Sei $f = \inf \overline{f}$. Dann gilt*

$$\boxed{(L,G,f) \sim (F,G/H,\overline{f})}\,.$$

Beweis. Nach 8.1 können wir o.E. annehmen, daß f und $\overline{f}$ normiert sind. Sei $B := (F, G/H, \overline{f}) = \bigcup_{\overline{\sigma}\in G/H} Fv_{\overline{\sigma}}$ wie in 7.5 und sei $r := \dim_F L$. Dann ist

$$\begin{aligned}\dim_K \mathrm{M}_{r\times r}(B) = r^2 \dim_K B \underset{7.5}{=} r^2(\dim_K F)^2 = (\dim_F L)^2(\dim_K F)^2 \\ \underset{\text{Aufgabe 8}}{=} (\dim_K L)^2 \underset{7.5}{=} \dim_K(L, G, f)\,.\end{aligned}$$

Da $\mathrm{M}_{r\times r}(B) \simeq B \otimes_K \mathrm{M}_{r\times r}(K)$ nach Aufgabe 10 gilt, folgt $B \sim \mathrm{M}_{r\times r}(B)$ nach 3.4, und es ist nur noch die Existenz eines K-Algebrahomomorphismus $\varphi\colon (L, G, f) \longrightarrow \mathrm{M}_{r\times r}(B)$ zu zeigen. Dieser ist dann injektiv, und daher aus Dimensionsgründen surjektiv.
Es sei B vermöge $B \hookrightarrow \mathrm{M}_{r\times r}(B)\,,\ b \longmapsto b\begin{pmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{pmatrix}$ in $\mathrm{M}_{r\times r}(B)$ eingebettet. Es gilt dann

$$(*)\qquad \begin{cases} v_{\overline{\sigma}}a = \overline{\sigma}(a)v_{\overline{\sigma}} & \forall\, a \in \mathrm{M}_{r\times r}(F)\\ v_{\overline{\sigma}}v_{\overline{\tau}} = \overline{f}(\overline{\sigma},\overline{\tau})v_{\overline{\sigma\tau}} = \underbrace{f(\sigma,\tau)}_{\in F^*}\,v_{\overline{\sigma\tau}}\,. & \end{cases}$$

Sei $(L, G, f) = \bigcup_{\sigma\in G} Lu_\sigma$ wie in 7.5. Definiere

$$\boxed{\varphi\colon (L, G, f) \longmapsto \mathrm{M}_{r\times r}(B)\,,\ xu_\sigma \longmapsto \ell_x U_\sigma v_{\overline{\sigma}}}\,,$$

wobei ℓ_x für $x \in L$ und U_σ für $\sigma \in G$ wie in Lemma 8.5 gegeben seien. Es ist $\varphi(u_1) = v_1$ (vgl. Folgerung 8.1), und

$$\begin{aligned}
\varphi(xu_\sigma \cdot yu_\tau) &= \varphi(\underbrace{x\sigma(y)f(\sigma,\tau)}_{\in L}\,u_{\sigma\tau}) && \text{nach } 7.5\\
&= \ell_x\ell_{\sigma(y)}U_{\sigma\tau}f(\sigma,\tau)v_{\overline{\sigma\tau}} && \text{nach Definition von } \varphi\\
& && \text{und da } \ell\ F\text{-linear ist}\\
& && \text{und } f(\sigma,\tau)\in F\\
&= \ell_x\ell_{\sigma(y)}U_\sigma\sigma(U_\tau)f(\sigma,\tau)v_{\overline{\sigma\tau}} && \text{nach 8.5 b)}\\
&= \ell_x U_\sigma\sigma(\ell_y)\sigma(U_\tau)v_{\overline{\sigma}}v_{\overline{\tau}} && \text{nach 8.5 a) und } (*)\\
&= \ell_x U_\sigma\sigma(\ell_y)v_{\overline{\sigma}}U_\tau v_{\overline{\tau}} && \text{nach } (*)\\
&= \ell_x U_\sigma v_{\overline{\sigma}}\ell_y U_\tau v_{\overline{\tau}} && \text{nach } (*)\\
&= \varphi(xu_\sigma)\cdot\varphi(yu_\tau)\,.
\end{aligned}$$

□

8.7 Folgerung für die Brauergruppe

Sei L (endlich) galoissch über K, und sei F ein über K galoisscher Zwischenkörper. Es gilt $K \subset F \subset L$, und man hat eine Inklusion
$\mathrm{Br}(F/K) \hookrightarrow \mathrm{Br}(L/K)$, da mit F stets auch L Zerfällungskörper ist, vgl. 5.1 (b).

Satz. *Das Diagramm*

$$\begin{array}{ccc}
[\overline{f}] & \longmapsto & [(F, G(F/K), \overline{f})] \\
\mathcal{H}^2(G(F/K), F^*) & \xrightarrow[\alpha_{F/K}]{\sim} & \mathrm{Br}(F/K) \\
\downarrow \mathrm{inf} & & \downarrow \cap \\
\mathcal{H}^2(G(L/K), L^*) & \xrightarrow[\alpha_{L/K}]{\sim} & \mathrm{Br}(L/K) \\
[f] & \longmapsto & [(L, G, f)]
\end{array}$$

ist kommutativ. Insbesondere ist die Inflation injektiv, und es ist

$$\mathcal{H}^2(K) \simeq \mathrm{Br}(K)\,.$$

Beweis. Die Isomorphismen $\alpha_{F/K}$ und $\alpha_{L/K}$ sind durch 8.3 gegeben. Nach dem Inflationssatz 8.6 ist das Diagramm kommutativ. Da drei der Abbildungen injektiv sind, ist dies dann auch die vierte, nämlich inf . Mit Hilfe von 8.4 folgt die letzte Behauptung. $\square$

9 Exponent und Index

Sei K ein Körper, und sei $A \simeq \mathrm{M}_{n\times n}(D)$ mit einem zentralen Schiefkörper D über K. Der Index von A ist durch $\mathrm{ind}_K A := \sqrt{\dim_K D}$ gegeben, vgl. 3.10.

9.1 Ein weiteres Darstellungslemma

Lemma.
Sei $A := (L, G, f) = \bigoplus_{\sigma\in G} Lu_\sigma$ *ein verschränktes Produkt über* K, *wie in* 7.5 *eingeführt, und sei* $m := \mathrm{ind}_K A$. *Dann gibt es zu jedem* $\sigma \in G$ *eine Matrix* $U_\sigma \in \mathrm{GL}_m(L)$, *so daß*

$$\boxed{f(\sigma,\tau)U_{\sigma\tau} = \sigma(U_\tau)U_\sigma \quad \forall\, \sigma,\tau \in G}$$

gilt. Hierbei wirkt σ *koeffizientenweise auf Matrizen über* L.

Beweis. Es ist $A \simeq \mathrm{M}_{r\times r}(D)$ mit einem $r \in \mathbb{N}$ und einem zentralen Schiefkörper D über K nach 3.8, also $\dim_K A = r^2 \dim_K D = r^2m^2$ und daher $\boxed{\dim_K L = rm}$ nach 7.5.

Sei D^r der Linksvektorraum der Spalten $\begin{pmatrix} d_1\\ \vdots \\ d_r\end{pmatrix}$ mit $d_i \in D$.

Da $L \hookrightarrow A \simeq \mathrm{M}_{r\times r}(D)$ gilt, kann man den $\mathrm{M}_{r\times r}(D)$-Linksmodul D^r auch als A-Linksmodul und als L-Linksvektorraum auffassen. Berechne nun $\dim_L D^r$. Es ist

$$\begin{aligned} rm^2 = (\dim_D D^r)(\dim_K D) &\underset{\text{Aufgabe 8}}{=} \dim_K D^r \\ &\underset{\text{Aufgabe 8}}{=} (\dim_L D^r)(\dim_K L) = (\dim_L D^r)rm\,. \end{aligned}$$

Es folgt

$$\boxed{\dim_L D^r = m}\,.$$

Sei $\{v_1,\dots,v_m\}$ eine Basis von D^r über L. Für $i = 1,\dots,m$ und $\sigma \in G$ gilt dann

$$\boxed{u_\sigma v_i = x_{i1}^{(\sigma)}v_1 + \cdots + x_{im}^{(\sigma)}v_m}$$

mit $x_{ij}^{(\sigma)} \in L$ für $j = 1,\dots,m$. Setze

$$U_\sigma = \begin{pmatrix} x_{11}^{(\sigma)} & \dots & x_{1m}^{(\sigma)} \\ \vdots & \ddots & \vdots \\ x_{m1}^{(\sigma)} & \dots & x_{mm}^{(\sigma)} \end{pmatrix}$$

mit $\vec{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}$ erhält man in Matrizenschreibweise

$$(*) \qquad \boxed{u_\sigma \vec{v} = U_\sigma \vec{v} \qquad \forall\, \sigma \in G}$$

denn $\begin{pmatrix} u_\sigma v_1 \\ \vdots \\ u_\sigma v_m \end{pmatrix} = \begin{pmatrix} x_{11}^{(\sigma)} v_1 + \ldots + x_{1m}^{(\sigma)} v_m \\ \vdots \qquad\qquad \vdots \\ x_{m1}^{(\sigma)} v_1 + \ldots + x_{mm}^{(\sigma)} v_m \end{pmatrix} = U_\sigma \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix}$. Es folgt

$$(**) \qquad u_\sigma u_\tau \vec{v} \underset{7.5}{=} f(\sigma,\tau) u_{\sigma\tau} \vec{v} \underset{(*)}{=} f(\sigma,\tau) U_{\sigma\tau} \vec{v}\,.$$

Andererseits gilt

$$\begin{aligned} u_\sigma u_\tau v_i = u_\sigma \left(\sum_{j=1}^m x_{ij}^{(\tau)} v_j \right) &\underset{7.5}{=} \sum_{j=1}^m \sigma(x_{ij}^{(\tau)}) u_\sigma v_j \\ &= \sum_{j=1}^n \sigma(x_{ij}^{(\tau)}) \sum_{k=1}^m x_{jk}^{(\sigma)} v_k \\ &= \sum_{k=1}^m \left(\sum_{j=1}^m \sigma(x_{ij}^{(\tau)}) x_{jk}^{(\sigma)} \right) v_k \end{aligned}$$

und also $u_\sigma u_\tau \vec{v} = \sigma(U_\tau) U_\sigma \vec{v}$. Aus $(**)$ folgt nun

$$f(\sigma,\tau) U_{\sigma\tau} = \sigma(U_\tau) U_\sigma\,,$$

da $v_1, \ldots, v_m$ linear unabhängig über L sind. Es ist $u_1 \in L^*$ (vgl. Lemma 3 in 7.3). Nach Konstruktion folgt $U_1 \in \mathrm{GL}_m(L)$, und da

$$\underbrace{f(\sigma, \sigma^{-1})}_{\in L^*} U_1 = \sigma(U_{\sigma^{-1}}) U_\sigma$$

gilt, ist $U_\sigma \in \mathrm{GL}_m(L)\ \forall\, \sigma \in G$. □

9.2 Torsion in der Brauergruppe

Satz. *Für jede Azumaya-Algebra A über K gilt $[A]^m = 1$ in $\mathrm{Br}(K)$ mit $m = \mathrm{ind}_K A$.*

Beweis. Da A nach 7.2 ähnlich zu einem verschränkten Produkt ist, können wir ohne Einschränkung annehmen, daß $A = (L, G, f) = \bigoplus_{\sigma \in G} L u_\sigma$ wie in 9.1 gilt. Setze $\lambda(\sigma) = \det(U_\sigma)$. Dann folgt aus 9.1 die Gleichung

$$f(\sigma,\tau)^m \cdot \lambda(\sigma\tau) = \sigma(\lambda(\tau)) \cdot \lambda(\sigma) \qquad\qquad \forall\, \sigma, \tau \in G\,.$$

Hieraus folgt, daß f^m ein 2-Korand ist, und 8.3 ergibt die Behauptung. □

9.3 Der Exponent teilt den Index

Aus 9.2 folgt, daß jedes Element aus $\mathrm{Br}(K)$ endliche Ordnung hat. Die kleinste Zahl $e \in \mathbb{N}$ mit $[A]^e = 1_{\mathrm{Br}(K)}$ heißt der *Exponent* einer Azumaya-Algebra A über K. Wir schreiben $e = \exp_K A$.

Satz. $\mathrm{Br}(K)$ *ist eine Torsionsgruppe, und es gilt:* $\exp_K A$ *teilt* $\operatorname{ind}_K A$ *für jedes* $[A] \in \mathrm{Br}(K)$.

Beweis. Sei $m = \operatorname{ind}_K A$ und $e = \exp_K A > 1$. Nach 9.2 gilt $e \leq m$. Also existiert ein $n \in \mathbb{N}$, so daß $m = ne + r$ mit $0 \leq r < e$ gilt.
Angenommen, $r > 0$. Dann folgt

$$1 \underset{9.2}{=} [A]^m = [A]^{ne+r} = [A]^{en}[A]^r = [A]^r$$

im Widerspruch zur Definition des Exponenten als kleinster Zahl e mit $[A]^e = 1$. □

Bemerkung. Es gilt $\exp_K A \mid \operatorname{ind}_K A$. Gleichheit gilt im allgemeinen nicht. Ist jedoch K ein lokaler oder globaler Körper, so gilt $\exp_K A = \operatorname{ind}_K A$. Es gilt stets: Exponent und Index haben dieselben Primteiler.

Sei A eine Azumaya-Algebra über K.

Satz. *Für jede Primzahl* p *mit* $p \mid \operatorname{ind}_K A$ *gilt* $p \mid \exp_K A$.

Beweis. Nach 5.7 besitzt A einen über K galoisschen Zerfällungskörper L mit Gruppe G der Ordnung $n < \infty$. Es folgt

$$p \mid \operatorname{ind}_K A \mid \dim_K L \qquad \text{nach Aufgabe 18}.$$

Sei H eine p-Sylowuntergruppe von G, und sei P der zugehörige Zwischenkörper. Es gilt also $H = G(L/P)$, und $\dim_K P = (G : H)$ ist teilerfremd zu p. Also ist P kein Zerfällungskörper von A (denn andernfalls würde $p \mid \operatorname{ind}_K A \mid \dim_K P$ gelten). Es folgt

$$1 < \exp_P(A \otimes_K P) \underset{9.3}{\mid} \operatorname{ind}_P(A \otimes_K P) \underset{\text{Aufgabe 18}}{\mid} \dim_P L = |H| = p^\ell$$

und daher $\exp_P(A \otimes_K P) = p^k$ mit einem $k \in \mathbb{N}$. Aufgabe 29 ergibt daher $p^k \mid \exp_K A$. □

9.4 Primfaktorzerlegung eines Schiefkörpers

Satz. *Sei D ein zentraler Schiefkörper über K vom Index d und Exponenten $e > 1$. Sind $d := p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r}$ und $e := p_1^{\varepsilon_1} \cdot \ldots \cdot p_r^{\varepsilon_r}$ die Primfaktorzerlegungen von d und e (gemäß 9.3), so gilt $D \simeq D_1 \otimes_K \cdots \otimes_K D_r$ mit zentralen Schiefkörpern D_i vom Index $p_i^{\delta_i}$ und Exponenten $p_i^{\varepsilon_i}$ für $i = 1, \ldots, r$.*

Beweis. Setze $e_i = \frac{e}{p_i^{\varepsilon_i}}$ für $i = 1, \ldots, r$. Dann ist $\mathrm{ggT}(e_1, \ldots, e_r) = 1$, und also gibt es $n_1, \ldots, n_r \in \mathbb{Z}$ mit $\boxed{\sum_{i=1}^{r} n_i e_i = 1}$ nach Algebra, Satz 8.4.

Sei D_i der zur Klasse $[D]^{n_i e_i}$ gehörige Schiefkörper. Dann gelten:

$$(*) \qquad [D_1 \otimes_K \cdots \otimes_K D_r] = [D]^{\sum_{i=1}^{r} n_i e_i} = [D]$$

und

$$(1) \qquad [D_i]^{p_i^{\varepsilon_i}} = [D]^{n_i e_i p_i^{\varepsilon_i}} = [D]^{e n_i} = 1\,.$$

Es folgt $\exp_K D_i \mid p_i^{\varepsilon_i}\ \forall\, i = 1, \ldots, r$, und daher sind $\exp_K D_1, \ldots, \exp_K D_r$ paarweise teilerfremd. Dies ergibt

$$\begin{aligned} p_1^{\varepsilon_1} \cdot \ldots \cdot p_r^{\varepsilon_r} &= \exp_K D \\ &= \exp_K (D_1 \otimes_K \cdots \otimes_K D_r) && \text{nach } (*) \\ &= \exp_K D_1 \cdot \ldots \cdot \exp_K D_r && \text{nach Algebra, Lemma 14.1 (2)} \end{aligned}$$

und $\exp_K D_i = p_i^{\varepsilon_i}\ \forall\, i = 1, \ldots, r$. Es folgt $\mathrm{ind}_K D_i = p_i^{x_i}$ mit $x_i \in \mathbb{N}$, denn $p_i^{\varepsilon_i} \underset{9.3}{\mid} \mathrm{ind}_K D_i$ und $\mathrm{ind}_K D_i$ hat nach 9.3 dieselben Primteiler wie $\exp_K D_i$. Nun gilt

$$\begin{aligned} p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r} &= \mathrm{ind}_K D \\ &= \mathrm{ind}_K (D_1 \otimes_K \cdots \otimes_K D_r) && \text{nach } (*) \\ &= \mathrm{ind}_K D_1 \cdot \ldots \cdot \mathrm{ind}_K D_r && \text{nach Aufgabe 32.} \end{aligned}$$

Es folgt $x_i = \delta_i\ \forall\, i = 1, \ldots, r$ und

$$\dim_K D = \dim_K (D_1 \otimes_K \cdots \otimes_K D_r)\,.$$

Aus $(*)$ und Folgerung 3.4 folgt nun

$$D \simeq D_1 \otimes_K \cdots \otimes_K D_r\,.$$

□

9.5 Eindeutigkeit der Primfaktorzerlegung

Satz. *Seien $A_1, \ldots, A_r, B_1, \ldots, B_r$ Azumaya-Algebren über K .*
Es gelte $\exp_K A_i = p_i^{x_i}$ und $\exp_K B_i = p_i^{y_i}$ mit paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$ und $x_i, y_i \in \mathbb{N}$ für $i = 1, \ldots, r$. Dann gilt

$$\boxed{A_1 \otimes_K \cdots \otimes_K A_r \sim B_1 \otimes_K \cdots \otimes_K B_r} \quad \Longrightarrow \quad \boxed{A_i \sim B_i \quad \forall\, i = 1, \ldots, r}.$$

Beweis. Es ist $\exp_K(A_i \otimes_K {B_i}^{\mathrm{op}})$ eine p_i-Potenz. Es folgt

$$\begin{aligned} 1 &= \exp_K(A_1 \otimes_K {B_1}^{\mathrm{op}} \otimes_K \cdots \otimes_K A_r \otimes_K {B_r}^{\mathrm{op}}) \\ &= \exp_K(A_1 \otimes_K {B_1}^{\mathrm{op}}) \cdot \ldots \cdot \exp_K(A_r \otimes_K {B_r}^{\mathrm{op}}) \quad \text{nach Algebra 14.1 (2)} \end{aligned}$$

und $\exp_K(A_i \otimes_K {B_i}^{\mathrm{op}}) = 1\ \forall\, i = 1, \ldots, r$. □

Korollar. *In der Primfaktorzerlegung $D \simeq D_1 \otimes_K \cdots \otimes_K D_r$ aus 9.4 sind die Schiefkörper D_i bis auf Isomorphie eindeutig bestimmt.*

Beweis. Gilt $D_1 \otimes_K \cdots \otimes_K D_r \simeq D \simeq D_1' \otimes_K \cdots \otimes_K D_r'$, so folgt $D_i \sim D_i'\ \forall\, i = 1, \ldots, r$ nach dem Satz. Da D_i, D_i' Schiefkörper sind, folgt $D_i \simeq D_i'\ \forall\, i = 1, \ldots, r$ nach Bemerkung 3.4. □

10 Zyklische Algebren

Sei L galoissch über K mit Gruppe G der Ordnung $n < \infty$. Die Beschreibung der relativen Brauergruppe $\mathrm{Br}(L/K)$ als zweiter Kohomologiegruppe $H^2(G, L^*)$ ist für viele Anwendungen noch nicht so gut brauchbar, da man die relativ komplizierte Kozykelgleichung

$$f(\sigma,\tau)f(\sigma\tau,\varrho) = \sigma(f(\tau,\varrho))f(\sigma,\tau\varrho) \qquad \forall\,\sigma,\tau,\varrho \in G$$

zu erfüllen hat. Wenn aber G zyklisch ist, so ist dies mit Aufgabe 33 erledigt, und man bekommt eine sehr schöne, einfache Beschreibung von verschränkten Produkten und von $\mathrm{Br}(L/K)$.

10.1 Definition

Eine Azumaya-Algebra A über K heißt *zyklisch* oder *zyklisch verschränktes Produkt*, falls A einen über K galoisschen Körper L mit zyklischer Gruppe enthält und $\dim_L A = \dim_K L$ gilt.

Bemerkung. Eine zyklische Algebra ist also stets ein verschränktes Produkt, vgl. 7.1.

10.2 Struktursatz

Für zyklische K-Algebren vereinfacht sich die Strukturanalyse 7.3 wie folgt:

Satz. *Sei A eine n^2-dimensionale zyklische K-Algebra. Definitionsgemäß enthalte A eine Galoiserweiterung L von K mit Gruppe $G = \{1, \sigma, \dots, \sigma^{n-1}\}$ der Ordnung n. Dann gibt es ein $u \in A^*$, so daß $1, \dots, u^{n-1}$ eine Basis von A als L-Vektorraum bilden und folgendes gilt:*

(1_Z) *Es ist $ux = \sigma(x)u \;\forall\, x \in L$*

(2_Z) *Es ist $u^n =: a \in K^*$*

Beweis. Nach (1) und Lemma 1 in 7.3 ist $A = \bigoplus_{i=0}^{n} Lu_{\sigma^i}$, wobei insbesondere $u_\sigma x = \sigma(x)u_\sigma \;\forall\, x \in L$ gilt. Setze $u := v_\sigma$. Dann ist (1_Z) erfüllt. Aus Lemma 2 (2) und Lemma 3 in 7.3 folgt $u^i = x_i u_{\sigma^i}$ mit gewissen $x_i \in L^*$ für $i = 0, \dots, n-1$. Also bilden $1, u, \dots, u^{n-1}$ eine L-Basis von A, da $\{u_{\sigma^i} \mid i = 0, \dots, n-1\}$ eine solche nach 7.3 bildet. Es gilt

$$u^n x = \sigma^n(x)u^n = xu^n \;\forall\, x \in L\,.$$

Daher folgt $u^n \in \mathcal{Z}_A(L) \underset{4.7}{=} L$ und $\sigma(u^n) = uu^nu^{-1} = u^n$.
Da σ erzeugendes Element von G ist, folgt $u^n =: a \in K^*$. □

10.3 Existenzsatz

Satz. *Sei L eine Galoiserweiterung von K mit Gruppe $G = \{1, \sigma, \dots, \sigma^{-1}\}$ der Ordnung n. Dann gibt es zu jedem $a \in K^*$ eine zyklische K-Algebra*

$$\boxed{(L, \sigma, a) := \bigoplus_{i=0}^{n-1} Lu^i},$$

so daß

$$\boxed{ux = \sigma(x)u \quad \forall\, x \in L} \quad \text{und} \quad \boxed{u^n = a}$$

gelten. Es ist $(L, \sigma, a) = (L, G, f_a)$ mit dem normierten 2-Kozyklus

$$f_a \colon G \times G \longrightarrow L^*,\ (\sigma^i, \sigma^j) \longmapsto \begin{cases} 1 & \text{falls } i + j < n \\ a & \text{falls } i + j \geq n \end{cases}$$

für $i, j = 0, \dots, n-1$. Ferner gelten

(I) Jede K-Algebra $B = \bigoplus_{i=0}^{n-1} Lv^i$, die $\boxed{vx = \sigma(x)v \quad \forall\, x \in L}$ und $\boxed{v^n = a}$ erfüllt, ist isomorph zu (L, σ, a).

(II) Für jedes zu n teilerfermde $k \in \mathbb{Z}$ gilt $(L, \sigma^k, a^k) \simeq (L, \sigma, a)$.

Beweis. Nach Aufgabe 33 ist f_a ein normierter 2-Kozyklus. Nach 7.5 und Definition von f_a ist $(L, G, f_a) = \bigoplus_{i=0}^{n-1} Lu_{\sigma^i}$ mit $u_{\sigma^i} = u_\sigma^i\ \forall\, i = 0, \dots, n-1$ und es gilt $u_\sigma x = \sigma(x) u_\sigma$ nach 7.5. Es folgt

$$u_\sigma^n = u_{\sigma^{n-1}} u_\sigma \underset{7.5}{=} f_a(\sigma^{n-1}, \sigma) u_{\sigma^n} = a u_1 = a,$$

da f_a normiert. Setze $u := u_\sigma$ und $(L, \sigma, a) := (L, G, f_a)$. Dann ist (L, σ, a) eine zyklische K-Algebra nach 7.5.

Zu (I) Durch $(L, \sigma, a) \longrightarrow B$, $xu^i \longmapsto xv^i$ für $x \in L$ und $i = 0, \dots, n-1$ ist ein L-linearer K-Algebrahomomorphismus festgelegt. Dieser ist nach 3.1 injektiv, und daher sind $1, v, \dots, v^{n-1}$ linear unabhängig über L, vgl. AGLA, Aufgabe 18. Es folgt $\dim_L B = n = \dim_L(L, \sigma, a)$ und $B \simeq (L, \sigma, a)$.

Zu (II) Nach obigem ist $(L,\sigma,a) = \bigoplus_{i=0}^{n-1} Lu^i$ mit $ux = \sigma(x)u \ \forall\, x \in L$ und $u^n = a$. Es folgt $u^k x = \sigma^k(x)u^k \ \forall\, x \in L$ und $(u^k)^n = a^k$. Da σ erzeugendes Element von G ist, ist die K-Unteralgebra $B = \bigoplus_{i=0}^{n-1} L(u^k)^i$ von (L,σ,a) nach (I) isomorph zu (L,σ^k,a^k). Es folgt $\dim_K B = \dim_K(L,\sigma^k,a^k) = n^2 = \dim_K(L,\sigma,a)$ und daher $B = (L,\sigma,a)$.

□

10.4 Multiplikativität

Satz. *Sei L galoissch über K mit Gruppe $G = \{1,\sigma,\ldots,\sigma^{n-1}\}$. Dann gilt*

$$\boxed{(L,\sigma,a)\otimes_K (L,\sigma,b) \sim (L,\sigma,ab) \qquad \forall\, a,b \in K^*}\,.$$

Beweis. Ersichtlich gilt $f_a f_b = f_{ab}$, und daher folgt die Behauptung aus 10.3 und 8.2. □

10.5 Das Isomorphiekriterium

Sei L galoissch über K mit Gruppe $G = \{1,\sigma,\ldots,\sigma^{n-1}\}$. Für $x \in L$ ist dann die Norm von x gegeben durch

$$\boxed{N_{L/K}(x) = x\sigma(x)\cdot\ldots\cdot\sigma^{n-1}(x)}\,,$$

und es gilt $N_{L/K}(x) \in K^* \ \forall\, x \in L^*$.

Satz. *Für $a,b \in K^*$ gilt*

$$\boxed{(L,\sigma,a) \simeq (L,\sigma,b)} \quad \Longleftrightarrow \quad \boxed{\exists\, x \in L^* \text{ mit } a = N_{L/K}(x)b}\,.$$

Beweis. „$\Longrightarrow$“: Nach Voraussetzung und 10.3 gilt $(L,G,f_a) \simeq (L,G,f_b)$ und $f_a(\sigma^i,\sigma^j) = 1 = f_b(\sigma^i,\sigma^j) \ \forall\, i,j = 0,\ldots,n-1$ mit $i+j<n$. Nach 7.7 gibt es daher eine Abbildung $G \longrightarrow L^*$, $\sigma^i \longmapsto \lambda_i$ für $i = 0,\ldots,n-1$, so daß

$$(*) \qquad \boxed{\lambda_{i+1} = \lambda_i\sigma^i(\lambda_1) \qquad \forall\, i = 0,\ldots,n-2}$$

und $a \underset{\text{Def.}}{=} f_a(\sigma^{n-1},\sigma) \underset{7.7}{=} \lambda_0^{-1}\lambda_{n-1}\sigma^{n-1}(\lambda_1)\underbrace{f_b(\sigma^{n-1},\sigma)}_{b}$ gelten.

Es ist $\lambda_1 = \lambda_{0+1} \underset{(*)}{=} \lambda_0\sigma^0(\lambda_1) = \lambda_0\lambda_1$, und also $\lambda_0 = 1$. Daher folgt

$$(**) \qquad \boxed{a = \lambda_{n-1}\sigma^{n-1}(\lambda_1)b}\,.$$

Nach $(*)$ ist $\lambda_2 = \lambda_1\sigma(\lambda_1)$, also $\lambda_3 = \lambda_{2+1} \underset{(*)}{=} \lambda_2\sigma^2(\lambda_1) = \lambda_1\sigma(\lambda_1)\sigma^2(\lambda_1)$ und induktiv

$$\begin{aligned}\lambda_{n-1} = \lambda_{(n-2)+1} &\underset{(*)}{=} \lambda_{n-2}\sigma^{n-2}(\lambda_1)\\ &= \lambda_1\sigma(\lambda_1)\cdot\ldots\cdot\sigma^{n-3}(\lambda_1)\sigma^{n-2}(\lambda_1)\,.\end{aligned}$$

Aus $(**)$ folgt nun $a = N_{L/K}(\lambda_1)b$.

„$\Longleftarrow$“: Sei $(L,\sigma,a) = \bigoplus_{i=0}^{n-1} Lu_i$ wie in 10.3 gegeben. Setze $v = x^{-1}u$, wobei $N_{L/K}(x)b = a$ gelte. Dann ist $vy = x^{-1}uy = x^{-1}\sigma(y)u = \sigma(y)v \;\forall\, y \in L$ und $v^n = x^{-1}ux^{-1}u\cdot\ldots\cdot x^{-1}u = N_{L/K}(x^{-1})u^n \underset{10.3}{=} N_{L/K}(x)^{-1}a = b$. Mit 10.3 (II) folgt die Behauptung. Also ist die K-Unteralgebra $\bigoplus_{i=0}^{n-1} Lv^i$ von (L,σ,a) isomorph zu (L,σ,b) nach 10.3 (I). Aus Dimensionsgründen folgt $(L,\sigma,a) \simeq (L,\sigma,b)$.

□

10.6 Die relative Brauergruppe im zyklischen Fall

Sei $N_{L/K}(L^*) = \{N_{L/K}(x) \mid x \in L^*\}$. Dann ist $N_{L/K}(L^*)$ eine Untergruppe von K^*.

Satz. *Sei L (endlich) galoissch mit zyklischer Gruppe G, und sei σ ein erzeugendes Element von G. Dann induziert die Zuordnung $a \longmapsto (L,\sigma,a)$ einen surjektiven Homomorphismus $\beta\colon K^* \twoheadrightarrow \mathrm{Br}(L/K)$ und einen Isomorphismus*

$$\overline{\beta}\colon K^*/N_{L/K}(L^*) \xrightarrow{\sim} \mathrm{Br}(L/K)\,.$$

Beweis. Nach 10.2 und 10.3 ist β surjektiv, und nach 10.5 ist $\overline{\beta}$ wohldefiniert und injektiv. Schließlich ergibt 10.4 die Homomorphieaussage. □

Bemerkung. Ist L (endlich) galoissch mit zyklischer Gruppe G, so gilt $\mathcal{H}^2(G,L^*) \simeq K^*/N_{L/K}(L^*)$ nach 8.2 und obigem Satz.

10.7 Anwendungsbeispiele

Nach 5.8 ist $\mathrm{Br}(K) = \bigcup_L \mathrm{Br}(L/K)$, wobei L alle (endlich) galoisschen Erweiterungen von K in $\overline{K}$ durchläuft und $\overline{K}$ ein algebraischer Abschluß von K ist.

1) $\mathrm{Br}(\mathbb{R}) \underset{5.8}{=} \mathrm{Br}(\mathbb{C}/\mathbb{R}) \underset{10.6}{\simeq} \mathbb{R}^*/N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^*)$

$$= \mathbb{R}^*/\mathbb{R}_{>0}\,, \qquad \text{da } N_{\mathbb{C}/\mathbb{R}}(z) = z\overline{z} = |z|^2 \;\forall\, z \in \mathbb{C}^* \text{ gilt}$$
$$\simeq \mathbb{Z}/2\mathbb{Z}\,.$$

Also folgt $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$ (wie schon in 6.5 gezeigt).

2) Ist L eine endliche Körpererweiterung eines endlichen Körpers K, so ist die Normabbildung $N_{L/K}\colon L^* \longrightarrow K^*$, $x \longmapsto N_{L/K}(x)$, surjektiv.

Beweis. Nach 6.3 ist $\mathrm{Br}(K) = \{1\}$. Da die Galoisgruppe $G(L/K)$ nach Algebra 16.7 zyklisch ist, folgt die Behauptung aus 10.6. □

3) Sei K ein endlicher Körper. Nach Algebra 16.7 und 5.8 ist dann $\mathrm{Br}(K) = \bigcup\limits_{L\subset\overline{K}} \mathrm{Br}(L/K)$, wobei die Gruppe $G(L/K)$ zyklisch ist. Zeigt man direkt, ohne 6.3 zu benutzen, daß $N_{L/K}\colon L^* \longrightarrow K^*$ surjektiv ist, so ergibt 10.6, daß $\mathrm{Br}(K) = \{1\}$ ist.
Dies ergibt einen neuen Beweis von 6.2, daß jeder endliche Schiefkörper kommutativ ist.

4) Sei $\mathrm{char}\, K \neq 2$, und sei A eine Quaternionenalgebra über K, d.h. eine vier-dimensionale Azumaya-Algebra über K. Nach den Aufgaben 22 und 26 gibt es Elemente $u, v \in A^*$, so daß $A = K \oplus Ku \oplus Kv \oplus Kuv$ sowie $u^2 =: a \in K^*$, $v^2 =: b \in K^*$ und $uv = -vu$ gilt.

Lemma. *Äquivalent sind:*

(i) $A \simeq \mathrm{M}_{2\times 2}(K)$,

(ii) $a \in N_{K(v)/K}(K(v)^*)$,

(iii) $b \in N_{K(u)/K}(K(u)^*)$,

(iv) Die quadratische Form $q = X_1^2 - aX_2^2 - bX_3^2 =: \langle 1, -a-, b\rangle$ *ist isotrop.*

Beweis. (i) $\Longleftrightarrow$ (ii): Sei $L = K(v)$.

1. Fall: $\dim_K L = 1$. Dann ist $v^2 = b = c^2$ mit einem $c \in K^*$ und $v \neq \pm c$ (da sonst $v \in \mathcal{Z}(K)$ im Widerspruch zur Gleichung $uv = -vu$). Es folgt $\underbrace{(v+c)}_{\neq 0}\underbrace{(v-c)}_{\neq 0} = v^2 - c^2 = 0$. Also ist A kein Schiefkörper. Es folgt $A \simeq \mathrm{M}_{2\times 2}(K)$. Ferner $a = N_{L/K}(a)$, da $\dim_K L = 1$.

2. Fall: $\dim_K L = 2$. Dann ist L galoissch mit Gruppe $\{1, \sigma\}$, wobei $\sigma(v) = -v$ gilt, und es folgt $A \simeq (L, \sigma, a)$ nach 10.3 (I). Aus 10.6 folgt nun die Äquivalenz (i) $\Longleftrightarrow$ (ii).

(i) $\Longleftrightarrow$ (iii): Der Beweis verläuft analog.

(ii) $\Longrightarrow$ (iv): Sei $L = K(v)$.

1. Fall: $\dim_K L = 1$. Dann ist $a = N_{L/K}(a)$. Ferner ist $v^2 = b = c^2$ mit $c \in K^*$ und also $q(c, 0, 1) = c^2 - b^2 = 0$.

2. Fall: $\dim_K L = 2$. Aus (ii) folgt: $\exists\, x_1, x_2 \in K$, so daß $a = N_{L/K}(x_1 + x_2 v) = (x_1 + x_2 v)(x_1 - x_2 v) = x_1^2 - x_2^2 v^2 = x_1^2 - x_2^2 b$ gilt. Es folgt $q(x_1, 1, x_2) = x_1^2 - a - b x_2^2 = 0$.

(iv) $\Longrightarrow$ (ii): Es gebe $x_1, x_2, x_3 \in K$, die nicht alle Null sind, mit $x_1^2 - a x_2^2 - b x_3^2 = 0$. Dann ist $x_2 \neq 0$, da sonst $b = \left(\frac{x_1}{x_3}\right)^2$ gelten würde im Widerspruch zu $\dim_K L = 2$. Es folgt $a = N_{L/K}\left(\frac{x_1}{x_2} + \frac{x_3}{x_2} v\right)$.

$\square$

Bemerkung. Sei $K = \mathbb{Q}$. Dann gibt es zu jeder Primzahl p einen Körper $L_p = \mathbb{Q}(\sqrt{p})$ mit Galoisgruppe $\{1, \sigma\}$ der Ordnung 2, vgl. Algebra 9.9. Mit Hilfsmitteln der elementaren Zahlentheorie läßt sich folgendes zeigen:

(1) Es gibt unendlich viele Primzahlen $p \equiv 3 \bmod 4$.

(2) Die Gleichung $X_1^2 + X_2^2 - p X_3^2 = 0$ besitzt in $\mathbb{Z}$ nur die triviale Lösung $(0, 0, 0)$ für alle Primzahlen $p \equiv 3 \bmod 4$. Nach dem Lemma ist also die Quaternionenalgebra $A_p = (L_p, \sigma_p, -1)$ ein Schiefkörper für alle Primzahlen $p \equiv 3 \bmod 4$.

(3) $A_p \not\sim A_q$ für alle Primzahlen p, q mit $p \neq q$ und $p, q \equiv 3 \bmod 4$ (vgl. Lorenz, Algebra II, §30).

10.8 Inflationssatz im zyklischen Fall

Sei M galoissch über K mit Gruppe $\{1, \tau, \ldots, \tau^{m-1}\}$, und sei L galoissch über K mit Gruppe $\{1, \sigma, \ldots, \sigma^{n-1}\}$. Es gelte $K \subset M \subset L$.

Satz. *Es sei σ so gewählt, daß $\sigma|_M = \tau$ gelte. Für jedes $a \in K^*$ gilt dann*

$$\boxed{(M, \tau, a) \sim (L, \sigma, a^r) \quad \textit{mit} \quad r = \dim_M L = \frac{n}{m}}.$$

Beweis. Seien $G = G(L/K)$ und $H = G(L/M)$. Dann gibt es einen surjektiven Homomorphismus

$$G \longrightarrow G(M/K)\,,\ \sigma \longmapsto \sigma|_M$$

mit dem Kern H, vgl. Algebra 16.3. Setze $\overline{\sigma} = \sigma H$. Nach Wahl von σ gilt dann

$$(M, \tau, a) = (M, \overline{\sigma}, a) \underset{10.3}{=} (M, G/H, \overline{f_a}) \underset{8.6}{\sim} (L, G, f)\,,$$

wobei $f = \inf(\overline{f_a})$ gilt und also

$$f(\sigma^i, \sigma^j) = \overline{f_a}(\overline{\sigma}^i, \overline{\sigma}^j) = \begin{cases} 1 & \text{für } i + j < m \\ a & \text{für } m \le i + j < 2m\,. \end{cases}$$

Es folgt $(L, G, f) \underset{7.5}{=} \bigoplus_{i=0}^{m-1} L u_{\sigma^i}$ mit $u_\sigma x = \sigma(x) u_\sigma \ \forall\, x \in L$ und $u_\sigma^m = u_\sigma^{m-1} u_\sigma = u_{\sigma^{m-1}} u_\sigma = \overline{f_a}(\overline{\sigma}^{m-1}, \overline{\sigma}) u_{\sigma^m} = a u_1 = a$. Es folgt $u_\sigma^n = u_\sigma^{mr} = a^r$ und also $(L, G, f) \simeq (L, \sigma, a^2)$. □

10.9 Weiterer Beweis des Satzes von Wedderburn

Satz. *Jeder endliche Schiefkörper ist kommutativ.*

Beweis. Sei D ein endlicher Schiefkörper mit Zentrum $K = \mathcal{Z}(D)$. Es genügt zu zeigen, daß jede zyklische Algebra (M, τ, a) über K zerfällt (vgl. 5.8 und Algebra 16.7).
Sei $r = |K| - 1$. Dann ist $a^r = 1$ (vgl. Algebra 14.2). Sei L eine Körpererweiterung von M mit $\dim_M L = r$ (vgl. Aufgabe 36). Dann ist L galoissch mit zyklischer Gruppe (nach Algebra 16.7), und es folgt

$$(M, \tau, a) \underset{10.8}{\sim} (L, \sigma, a^r) \sim (L, \sigma, 1)\,.$$

□

10.10 Zyklizitätsprobleme

Im zyklischen Fall gilt

$$\boxed{\mathrm{Br}(L/K) \simeq K^*/N_{L/K}(L^*)}$$

nach 10.6. (Definition einer zyklischen Algebra in 10.1.)

Problem 1. Ist jede Azumaya-Algebra über K zyklisch? (Gegenbeispiel Dickson 1932)
Problem 2. Ist jede Azumaya-Algebra A über K ähnlich einer zyklischen Algebra? (Gegenbeispiel Amitsur 1972)
(vgl. R. S. Pierce: Associative Algebras, Springer 1982)

Theorem (Merkurjev-Suslin 1982).
Enthält K die n-ten Einheitswurzeln und ist $[A]^n = 1$, so ist A ähnlich einem Tensorprodukt von zyklischen Algebren.

Beweis. tiefliegend und sehr schwierig. □

Hilfsmittel: Hilbert 90 für die K-Gruppe $K_2(K)$ offen bis heute. Gilt dies Theorem auch im Fall $\operatorname{char} K \nmid n$ ohne die Einheitswurzelbedingung?

Teil III

Die Brauergruppe eines lokalen Körpers

11 Diskrete Bewertungen

Für $\mathbb{Z}$ aufgefaßt als additive Gruppe schreiben wir häufig auch $\mathbb{Z}^+$.

11.1 Definition

Eine *diskrete Bewertung v von K* ist ein surjektiver Gruppenhomomorphismus $v\colon K^* \longrightarrow \mathbb{Z}^+$ derart, daß

$$(1_d) \qquad \boxed{v(x+y) \geq \operatorname{Min}(v(x), v(y)) \;\forall\, x, y \in K \text{ mit } x \neq -y}$$

gilt. Wie üblich sei $v(0) := +\infty$ gesetzt. Eine solche diskrete Bewertung wird häufig auch *normierte Exponentenbewertung* genannt.

11.2 Elementare Eigenschaften

Lemma. *Eine diskrete Bewertung $v\colon K^* \longrightarrow \mathbb{Z}^+$ hat die folgenden Eigenschaften:*

(i) $v(xy) = v(x) + v(y) \;\forall\, x, y \in K^*$

(ii) $v(1) = 0$

(iii) $v(-x) = v(x) \;\forall\, x \in K^*$

(iv) $v(x^{-1}) = -v(x) \;\forall\, x \in K^*$

(v) Für $x, y \in K^*$ gilt

$$\boxed{v(x) \neq v(y)} \quad \Longrightarrow \quad \boxed{v(x+y) = \operatorname{Min}(v(x), v(y))}$$

Beweis.

(i) und (ii) gelten, weil v ein Gruppenhomomorphismus ist.

(iii) Es ist $0 \underset{\text{(ii)}}{=} v(1) = v((-1)(-1)) \underset{\text{(i)}}{=} v(-1) + v(-1)$,
also $v(-1) = -v(-1)$. Es folgt $v(-1) = 0$ und daher

$$v(-x) = v((-1)x) \underset{\text{(ii)}}{=} \underbrace{v(-1)}_{=0} + v(x) = v(x)$$

(iv) Es gilt $0 \underset{\text{(ii)}}{=} v(xx^{-1}) \underset{\text{(i)}}{=} v(x) + v(x^{-1})$.

(v) Angenommen, es gibt x, y mit $v(x) < v(y)$
und $v(x+y) > \mathrm{Min}(v(x), v(y)) = v(x)$. Dann folgt

$$\begin{aligned} v(x) = v((x+y) + (-y)) &\geq \mathrm{Min}(v(x+y), v(y)) && \text{nach } (1_d) \text{ und (iii)} \\ &> v(x) && \text{Widerspruch.} \end{aligned}$$

□

11.3 Fundamentales Lemma

Lemma. *Sei $v\colon K^* \longrightarrow \mathbb{Z}^+$ eine diskrete Bewertung. Dann ist die Menge*

$$\boxed{\Lambda := \{x \in K^* \mid v(x) \geq 0\}}$$

ein Hauptidealring mit genau einem Primideal

$$\boxed{\mathfrak{m}_v := \{x \in K \mid v(x) > 0\} \neq (0)}$$

und mit der Einheitengruppe

$$\boxed{\Lambda^* = \{x \in K^* \mid v(x) = 0\}}\,.$$

Bei fester Wahl eines Elementes $\pi \in \Lambda$ mit $v(\pi) = 1$ läßt sich jedes Element $x \in K^*$ schreiben als

$$\boxed{x = \pi^{v(x)}u \quad \textit{mit einem von } x \textit{ abhängigen } u \in \Lambda^*}\,.$$

Ferner ist jedes Ideal $\neq (0)$ in Λ von der Form $\pi^n\Lambda$ mit einem $n \geq 0$.

Beweis. Aus 11.1 und 11.2 folgt, daß Λ ein Unterring von K und $\mathfrak{m}_v$ ein Ideal in Λ ist. Es ist $\Lambda^* = \{x \in K^* \mid v(x) = 0\}$, denn $x \in \Lambda^* \Longrightarrow x^{-1} \in \Lambda \Longrightarrow v(x^{-1}) \geq 0 \underset{\text{(iv)}}{\Longrightarrow} v(x) \leq 0 \Longrightarrow v(x) = 0$, da $x \in \Lambda$.
Ist umgekehrt $x \in K^*$ und $v(x) = 0$, so ist $x \in \Lambda$ und $v(x^{-1}) \underset{\text{(iv)}}{=} -v(x) = 0$

und also $x^{-1} \in \Lambda$.
Wähle $\pi \in \Lambda$ mit $v(\pi) = 1$. Für $x \in K^*$ setze

$$\boxed{u := x\pi^{-v(x)}}.$$

Dann folgt $x = \pi^{v(x)}u$ und

$$v(u) \underset{\text{(i)}}{=} v(x) + v\left(\pi^{-v(x)}\right) \underset{\text{(i)}}{=} v(x) + -v(x)\underbrace{v(\pi)}_{=1} = 0$$

und also $u \in \Lambda^*$.
Sei I ein Ideal in Λ mit $I \neq (0)$ und $I \neq (1)$. Wähle ein $n \in \mathbb{N}$, so daß $v(x) \geq n\ \forall x \in I$ und $v(x) = n$ für mindestens ein $x \in I$ gilt. Dann folgt $I \subset \pi^n\Lambda$, denn für $x \neq 0$ in I ist

$$x = \pi^{v(x)}u = \pi^n \underbrace{\pi^{v(x)-n}}_{\in\Lambda,\text{ da } v(x)\geq n} u \in \pi^n\Lambda\,.$$

Umgekehrt ist $\pi^n \in I$ und also $\pi^n\Lambda \subset I$, denn wähle ein $x \in I$ mit $v(x) = n$ und also mit $v(\pi^n x^{-1}) \underset{\text{(i)}}{=} n + v(x^{-1}) \underset{\text{(iv)}}{=} n - n = 0$.
Dann ist $\pi^n = \underbrace{\pi^n x^{-1}}_{\in\Lambda}\underbrace{x}_{\in I} \in I$. Es folgt $I = \pi^n\Lambda$.
Gezeigt ist, daß jedes Ideal in Λ ein Hauptideal ist, und daß jedes Ideal $\neq (0)$ in der Kette

$$\cdots \subset \pi^n\Lambda \subset \pi^{n-1}\Lambda \subset \cdots \subset \pi^2\Lambda \subset \pi\Lambda \subsetneqq \Lambda$$

vorkommt. Also ist $\pi\Lambda$ das einzige maximale Ideal in Λ. Es ist $\pi{+}\Lambda$ Nullteiler in $\Lambda/\pi^n\Lambda$ für jedes $n > 1$. Also ist $\pi^n\Lambda$ kein Primideal für $n > 1$, vgl. Algebra 7.4. □

11.4 Bewertungsring und Restklassenkörper

Definition. Ist $v\colon K^* \longrightarrow \mathbb{Z}^+$ eine diskrete Bewertung, so heißt der Ring Λ in 11.3 *Bewertungsring von K bezüglich v*, und der Körper $k_v = \Lambda/\mathfrak{m}_v$ heißt *Restklassenkörper von K bezüglich v*. Jedes Element $\pi \in \Lambda$ mit $v(\pi) = 1$ heißt *Primelement bezüglich v*.

11.5 Beispiele

1) Diskrete Bewertungen von $K(X)$:
   Seien $K[X]$ der Polynomring in einer Unbestimmten X und $K(X)$ der

Quotientenkörper von $K[X]$, genannt „rationaler Funktionenkörper in der Unbestimmten X“ . Es ist

$$K(X) = \left\{ \frac{f}{g} \mid f, g \in K[X],\ g \neq 0 \right\} .$$

Ist p ein normiertes irreduzibles Polynom in $K[X]$, so läßt sich jedes Polynom $f \neq 0$ aus $K[X]$ eindeutig schreiben als $f = p^{v(f)}u$, wobei $v(f) \in \mathbb{N}_0$ und $u \in K[X]$ nicht durch p teilbar ist (denn $K[X]$ ist faktoriell, vgl. Algebra 8.10).
Dann ist $v\colon K(X)^* \longrightarrow \mathbb{Z}^+$, $\frac{f}{g} \longmapsto v(f) - v(g)$, eine diskrete Bewertung von $K(X)$ mit Bewertungsring

$$\Lambda = \left\{ \frac{f}{g} \in K(X) \mid p \nmid g \right\}$$

und Restklassenkörper

$$\boxed{k_v = \Lambda/p\Lambda}\,.$$

Behauptung. Es gibt eine kanonische Isomorphie

$$\boxed{k_v \simeq K[X]/pK[X]}\,.$$

Beweis. Die Inklusion $K[X] \hookrightarrow \Lambda$ induziert einen Homomorphismus

$$\varphi\colon K[X]/pK[X] \longrightarrow \Lambda/p\Lambda\,.$$

Dieser ist injektiv, da $K[X]/pK[X]$ ein Körper ist, vgl. Algebra 8.13(b).
Für $f \in K[X]$ sei $\overline{f} := f + pK[X]$. Sei $h \in \Lambda$, also $h = \frac{f}{g}$ mit $f, g \in K[X]$ und $p \nmid g$. Da $\overline{g} \neq \overline{0}$ gilt, hat die Gleichung $\overline{g}X = \overline{f}$ eine Lösung $\overline{x}$ im Körper $K[X]/pK[X]$, und es folgt $\varphi(\overline{x}) = h + p\Lambda$. □

Beobachtung.
Es ist $\Lambda = S^{-1}(K[X])$ mit der multiplikativen Menge $S = K[X] \setminus pK[X]$. Also ist Λ die *Lokalisierung* von $K[X]$ nach dem Primideal $pK[X]$.

2) Gradbewertung von $K(X)$:
Sei $f \in K[X]$ und $f \neq 0$. Setze $v_\infty(f) = -\operatorname{grad} f$. Dann ist

$$v_\infty\colon K(X)^* \longrightarrow \mathbb{Z}^+,\ \frac{f}{g} \longmapsto v_\infty(f) - v_\infty(g)\,,$$

eine weitere diskrete Bewertung von $K(X)$. Es ist X^{-1} Primelement, und

$$\Lambda = \left\{ \frac{f}{g} \in K(X)^* \mid \operatorname{grad} f \leq \operatorname{grad} g \right\} \cup \{0\}$$

ist der Bewertungsring von $K[X]$ bezüglich v_∞. Es ist Λ isomorph zur Lokalisierung von $K[X^{-1}]$ nach dem Primideal $X^{-1}K[X^{-1}]$, und der Restklassenkörper k_{v_∞} ist isomorph zu K.

3) Diskrete Bewertungen von $\mathbb{Q}$:
Sei p eine Primzahl. Analog zu Beispiel 1 gilt dann: Jedes $x \in \mathbb{Z} \setminus \{0\}$ läßt sich als $x = p^{v(x)}u$ schreiben, wobei $v(x) \geq 0$ und $p \nmid u$ gilt. Dann ist

$$v =: v_p \colon \mathbb{Q}^* \longrightarrow \mathbb{Z}^+ \,, \quad \frac{x}{y} \longmapsto v(x) - v(y) \,,$$

eine diskrete Bewertung von $\mathbb{Q}$ mit Bewertungsring

$$\Lambda = \left\{ \frac{x}{y} \in \mathbb{Q} \mid p \nmid y \right\}$$

und Restklassenkörper

$$\Lambda/\mathfrak{m}_v \underset{11.3}{=} \Lambda/p\Lambda \simeq \mathbb{Z}/p\mathbb{Z} \,.$$

4) Diskrete Bewertungen eines Zahlkörpers:
Sei K ein Zahlkörper, also K eine endliche Körpererweiterung von $\mathbb{Q}$. Situation:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, hook] \arrow[d, hook] & \mathbb{Q} = \operatorname{quot}(\mathbb{Z}) \arrow[d, hook] \\ \mathfrak{o}_K \arrow[r, hook] & K = \operatorname{quot}(\mathfrak{o}_K) \end{tikzcd}$$

Hierbei ist $\mathfrak{o}_K$ der *Ganzheitsring von* K, also

$$\mathfrak{o}_K = \{ x \in K \mid f_x \in \mathbb{Z}[X] \} \,,$$

wobei f_x das Minimalpolynom von $x \in K$ bezeichne. Jedes Ideal $I \neq (0)$ in $\mathfrak{o}_K$ läßt eine eindeutige Zerlegung der Form $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ zu, wobei $\mathfrak{p}$ alle Primideale $\neq (0)$ in $\mathfrak{o}_K$ durchläuft, und $n(\mathfrak{p})$ nicht-negative ganze Zahlen sind, die bis auf endlich viele Null sind, vgl. Bücher über Algebraische Zahlentheorie oder auch N. Bourbaki, Commutative Algebra, Chap. VII, §2, no. 3, Hermann 1972.

Die Zerlegung gilt in jedem „Dedekindring" und allgemeiner sogar für „Fraktionsideale" , wobei dann zusätzliche Exponenten auftauchen können. Für jedes $x \neq 0$ in $\mathfrak{o}_K$ setzen wir $v_\mathfrak{p}(x) = n(\mathfrak{p})$ gemäß der Zerlegung $x\mathfrak{o}_K = \prod_\mathfrak{p} \mathfrak{p}^{n(\mathfrak{p})}$ des von x in $\mathfrak{o}_K$ erzeugten Hauptideals. Wir erhalten also für jedes Primideal $\mathfrak{p} \neq (0)$ in $\mathfrak{o}_K$ eine diskrete Bewertung

$$v_\mathfrak{p} \colon K^* \longrightarrow \mathbb{Z}^+ \quad \text{mit} \quad v_\mathfrak{p}\left(\frac{x}{y}\right) = v_\mathfrak{p}(x) - v_\mathfrak{p}(y)$$

für $x, y \in \mathfrak{o}_K \backslash \{0\}$. Der Bewertungsring Λ von K bezüglich $v_\mathfrak{p}$ ist die Lokalisierung von $\mathfrak{o}_K$ nach dem Primideal $\mathfrak{p}$, also $\Lambda = S^{-1}(\mathfrak{o}_K)$ mit $S = \mathfrak{o}_K \backslash \mathfrak{p}$. Gemeint ist damit die Lokalisierung im Sinne der kommutativen Algebra. In der Algebraischen Zahlentheorie beinhaltet dieser Begriff meist zusätzlich noch „Vervollständigung" .

11.6 Absolutbeträge

Ein *Absolutbetrag* (oder kurz *Betrag*) von K ist eine Abbildung $| \; | : K \longrightarrow \mathbb{R}$, $x \longmapsto |x|$, mit den Eigenschaften

1) $|x| \geq 0$,

2) $x = 0 \Longleftrightarrow |x| = 0$,

3) $|xy| = |x| \; |y|$,

4) $|x + y| \leq |x| + |y| \;\; \forall\, x, y \in K$.

Zwei Absolutbeträge ${}_1| \; |$ und ${}_2| \; |$ heißen *äquivalent*, wenn es ein $c > 0$ aus $\mathbb{R}$ gibt, so daß

$${}_2|x| = {}_1|x|^c \;\; \forall\, x \in K \text{ gilt.}$$

Setzt man $d(x, y) := |x - y|$ für $x, y \in K$, so gelten $d(x, y) = 0 \Longleftrightarrow x = y$ und $d(x, y) \leq d(x, y) + d(y, z)$.
Damit ist K dann ein metrischer Raum, wie er in der Analysis betrachtet wird, und man kann mit Begriffen wie „offen" , „Konvergenz von Folgen" , „Nullfolgen" und „Cauchyfolgen" arbeiten.
Zwei Beträge ${}_1| \; |$ und ${}_2| \; |$ sind genau dann äquivalent, wenn jede Nullfolge bezüglich ${}_1| \; |$ auch eine Nullfolge bezüglich ${}_2| \; |$ ist und umgekehrt.

Beispiele.

(i) Der triviale Betrag, definiert durch $|0| = 0$ und $|x| = 1 \; \forall\, x \in K^*$.

(ii) Sei $r \in \mathbb{R}$ mit $0 < r < 1$ fest gewählt. Dann ist für jede Primzahl p durch

$$|x| := r^{v_p(x)}, \quad v_p \text{ wie in } 11.4(3)$$

ein Betrag von $\mathbb{Q}$ definiert. Dieser ist nicht-archimedisch, d.h. es gilt

$$|x+y| \leq \text{Max}(|x|, |y|) \; \forall \, x, y \in \mathbb{Q} \,.$$

Üblicherweise wählt man $r = p^{-1}$ und erhält einen äquivalenten Betrag

$$|\;|_p : \mathbb{Q} \longrightarrow \mathbb{R}\,, \; x \longmapsto p^{-v_p(x)}\,,$$

wobei $|0|_p = 0$ sei. Dieser Betrag heißt *p-adischer Absolutbetrag.*

(iii) Man kann zeigen, daß jeder Absolutbetrag von $\mathbb{Q}$ entweder zum gewöhnlichen Absolutbetrag oder zu einem p-adischen Absolutbetrag äquivalent ist (Beweis z.B. Lorenz, Algebra II).

11.7 Übergang vom Betrag zur Bewertung

Sei $|\;| : K \longrightarrow \mathbb{R}_{\geq 0}$ ein Absolutbetrag, der nicht-archimedisch sei, d.h. es gelte die verschärfte Dreiecksungleichung

$$|x+y| \leq \text{Max}(|y|, |y|) \; \forall \, x, y \in K \,.$$

Für ein $c \in \mathbb{R}$ mit $0 < c < 1$ betrachte man die Abbildung

$$v \colon K \longrightarrow \mathbb{R} \cup \{\infty\}\,,$$

die $|x| = c^{v(x)} \; \forall \, x \in K$ erfüllt, wobei $v(0) := \infty$ gesetzt wird. Dann gelten

$$\begin{aligned} v(xy) &= v(x) + v(y) \\ v(x+y) &\geq \text{Min}(v(x), v(y)) \\ v(x) = \infty &\iff x = 0 \end{aligned}$$

Man nennt v dann eine *Exponentenbewertung* von K. Diese heißt *diskret*, falls es einen kleinsten Wert $v(a) > 0$, $a \in K$ gibt, so daß alle anderen vorkommenden Werte ein ganzzahliges Vielfaches von $v(a)$ sind. Man kann dann v so normieren, daß $v(K^*) = \mathbb{Z}$ gilt.

11.8 Vervollständigung

Sei $|\ |: K \longrightarrow \mathbb{R}_{\geq 0}$ ein Absolutbetrag wie in 11.6 definiert.
Eine Folge $(a_n)_{n\in\mathbb{N}} \subset K$ heißt *Cauchyfolge*, falls es zu jedem $\varepsilon \in \mathbb{R}_{>0}$ ein $n_0 \in \mathbb{N}$ gibt mit $|a_n - a_m| < \varepsilon \;\forall\, n, m \geq n_0$. Wie in der Analysis zeigt man:

(a) Die Menge $\mathcal{C}$ aller Cauchyfolgen in K bildet einen kommutativen Ring, und die Menge $\mathcal{N}$ der Nullfolgen ist ein Ideal in $\mathcal{C}$.

(b) Der Ring $\widehat{K} := \mathcal{C}/\mathcal{N}$ ist ein Körper.

(c) Durch $\iota\colon K \hookrightarrow \widehat{K}$, $a \longmapsto (a, a, \dots)$ (konstante Folge) wird K als Ring in $\widehat{K}$ eingebettet.

(d) Der vorgegebene Absolutbetrag $|\ |: K \longrightarrow \mathbb{R}_{\geq 0}$ setzt sich in einem Absolutbetrag $\widehat{|\ |}: \widehat{K} \longrightarrow \mathbb{R}_{\geq 0}$ fort:
Für eine Cauchyfolge $(a_n \in K)_{n\in\mathbb{N}}$ sei $\alpha = ((a_n)_{n\in\mathbb{N}} + \mathcal{N}) \in \widehat{K}$. Dann ist die Folge $(|a_n|)_{n\in\mathbb{N}}$ eine Cauchyfolge in $\mathbb{R}$ nach Aufgabe 41. Also gibt es $\widehat{|\alpha|} := \lim\limits_{n\to\infty} |a_n|$ in $\mathbb{R}$, da $\mathbb{R}$ vollständig (bezüglich des gewöhnlichen Absolutbetrags) ist. Der Betrag $\widehat{|\ |}$ ist wohldefiniert, und es ist $\widehat{|\iota(a)|} = |a| \;\forall\, a \in K$.

(e) Es ist K dicht in $\widehat{K}$, d.h. jedes Element aus $\widehat{K}$ ist Grenzwert einer Folge aus K.

(f) Es ist $\widehat{K}$ vollständig bezüglich $\widehat{|\ |}$, d.h. jede Cauchyfolge aus $\widehat{K}$ konvergiert.

Definition. Jedes Paar $(\widetilde{K}, \widetilde{|\ |})$, wobei $\widetilde{K}$ eine Körpererweiterung von K und $\widetilde{|\ |}: \widetilde{K} \longrightarrow \mathbb{R}$ ein Absolutbetrag ist, heißt *Vervollständigung* (oder *Komplettierung* oder *vollständige Hülle*) von $(K, |\ |)$, falls $\widetilde{K}$ vollständig bezüglich $\widetilde{|\ |}$, $\widetilde{|\ |}$ eine Fortsetzung von $|\ |$ und K dicht in $\widetilde{K}$ ist.

(g) Sind $(\widehat{K}, \widehat{|\ |})$ und $(\widetilde{K}, \widetilde{|\ |})$ zwei Komplettierungen von $(K, |\ |)$, so gibt es genau einen K-Algebraisomorphismus $\varphi\colon \widehat{K} \longrightarrow \widetilde{K}$ mit $\widetilde{|\varphi(x)|} = \widehat{|x|} \;\forall\, x \in \widehat{K}$.

(h) Sei $|\ |: K \longrightarrow \mathbb{R}_{\geq 0}$ nicht-archimedisch, d.h. es gelte die *verschärfte Dreiecksungleichung*

$$|x + y| \leq \operatorname{Max}(|x|, |y|) \;\forall\, x, y \in K.$$

Dann ist die Menge $R := \{x \in K \mid |x| \leq 1\}$ ein lokaler Ring mit maximalem Ideal $\mathfrak{o} := \{x \in K \mid |x| < 1\}$ (vgl. Aufgabe 42). Analog seien $\widehat{R}$ und $\widehat{\mathfrak{o}}$ für die Komplettierung $(\widehat{K}, \widehat{|\;|})$ gegeben.

Behauptung. Es gilt $\widehat{\left|\widehat{K}\right|} = |K|$, und die Inklusion $R \hookrightarrow \widehat{R}$ induziert einen Isomorphismus

$$R/\mathfrak{o} \xrightarrow{\sim} \widehat{R}/\widehat{\mathfrak{o}}\,.$$

Beweis. Sei $a \in \widehat{K}$. Da K dicht in $\widehat{K}$ ist, gibt es eine Folge $(a_n \in K)_{n\in\mathbb{N}}$ mit $\lim\limits_{n\to\infty} a_n = \alpha$. Sei $\alpha \neq 0$. Dann gibt es ein $n_0 \in \mathbb{N}$, so daß $\widehat{|a_n - \alpha|} < \widehat{|\alpha|}$ $\forall\, n \geq n_0$ gilt. Setze $a = a_{n_0+1}$. Dann ist $a \in K^*$, und es folgt

$$\begin{aligned}
\widehat{|\alpha|} &= \widehat{|(a-\alpha)+\alpha|} && \text{nach Aufgabe 39}\\
&= |a| && \text{nach (d)}\\
\Longrightarrow \widehat{\left|\widehat{K}\right|} &= |K|\,.
\end{aligned}$$

Für $\alpha \in \widehat{R} \setminus \{0\}$ folgt $\widehat{|a-\alpha|} < \widehat{|\alpha|} \leq 1$, also $a - \alpha \in \widehat{\mathfrak{o}}$ und $|a| = \widehat{|a|}$, und daher $\alpha \in R$. Dies ergibt $\alpha + \widehat{\mathfrak{o}} = a + \widehat{\mathfrak{o}}$ mit $a \in R$. Der Homomorphismus $R/\mathfrak{o} \longrightarrow \widehat{R}/\widehat{\mathfrak{o}}$ ist also surjektiv. Er ist injektiv, da $R/\mathfrak{o}$ ein Körper ist. $\square$

Bemerkung. Sei $|\;| : K \longrightarrow \mathbb{R}_{\geq 0}$ nicht-archimedisch. Geht man dann zu einer Exponentenbewertung ν über, wie in 11.7 beschrieben, so lassen sich die Aussagen bezüglich $|\;|$ in Aussagen bezüglich ν übersetzen und umgekehrt.

12 Diskret bewertete vollständige Körper

Struktur- und Klassifikationsaussagen sind im blauen Zahlentheoriebuch von Hasse nachzulesen. Wir stellen hier einige Hilfsmittel bereit, die im weiteren benötigt werden.

12.1 Henselsches Lemma

Sei K vollständig bezüglich einer vorgegebenen diskreten Bewertung von K. Gemäß 11.3, 11.4 bezeichne Λ den zugehörigen Bewertungsring, $\pi \in \Lambda$ ein Primelement und $k := \Lambda/\Lambda\pi$ den Restklassenkörper.
Für $\lambda \in \Lambda$ sei $\overline{\lambda} := \lambda + \Lambda\pi$ die zugehörige Restklassen in k, und für ein Polynom $f = \sum_{i=0}^{m} \lambda_i X^i \in \Lambda[X]$ sei $\overline{f} = \sum_{i=0}^{m} \overline{\lambda_i} X^i$ das zugehörige Polynom in $k[X]$. Die Schreibweise

$$\boxed{f_1 \equiv f_2 \bmod \pi^n} \quad \text{bedeute} \quad \boxed{f_1 - f_2 \in \Lambda[X]\,\pi^n}$$

für $f_1, f_2 \in \Lambda[X]$ und $n \in \mathbb{N}$.

Lemma (K. Hensel). *Sei $f \in \Lambda[X]$ mit $\overline{f} \neq \overline{0}$. Ist $\overline{f} = \varphi\psi$ mit teilerfremden Polynomen*
$\varphi, \psi \in k[X]$, so gibt es Polynome $g, h \in \Lambda[X]$ mit den Eigenschaften

$$f = gh\,, \qquad \overline{g} = \varphi\,, \qquad \overline{h} = \psi \qquad \textit{und} \qquad \operatorname{grad} g = \operatorname{grad} \varphi\,.$$

Beweis. Sei $m := \operatorname{grad} f$. Wähle $g_0 \in \Lambda[X]$ mit $\overline{g_0} = \varphi$ und $r := \operatorname{grad} g_0 = \operatorname{grad} \varphi$. Nach Voraussetzung gibt es dann ein $h_0 \in \Lambda[X]$ mit $\overline{h_0} = \psi$ und

$$\boxed{f \equiv g_0 h_0 \bmod \pi}\,.$$

Es kann also h_0 mit $\operatorname{grad} h_0 \leq m - r$ gewählt werden.

Behauptung 1. Sei $d \in \Lambda[X]$ mit $\operatorname{grad} d \leq m$. Dann gibt es Polynome $a, b \in \Lambda[X]$ mit $\operatorname{grad} a < r$ und $\operatorname{grad} b \leq m - r$, so daß

$$\boxed{a h_0 + b g_0 \equiv d \bmod \pi}$$

gilt.

Beweis. Da $\overline{g_0}$ und $\overline{h_0}$ teilerfremd in $k[X]$ sind, gibt es Polynome $\alpha, \beta \in \Lambda[X]$ mit $\alpha h_0 + \beta g_0 \equiv 1 \bmod \pi$ nach Algebra 8.4. Es folgt

$$(*) \qquad \alpha d h_0 + \beta d g_0 \equiv d \bmod \pi\,.$$

Ist $\operatorname{grad} \alpha d < r$, so setze $a = \alpha d$ und $b = \beta d$. Ist $\operatorname{grad} \alpha d \geq r$, so ist $\alpha d = b' g_0 + a$ mit $\operatorname{grad} a < r$ nach Algebra 8.1.
Aus ($*$) folgt dann $ah_0 + bg_0 \equiv d \bmod \pi$ mit $b = b' + \beta d$.
Man kann nun b gegebenenfalls so abändern, daß der Leitkoeffizient von b nicht durch π teilbar ist. Dann folgt

$$\begin{aligned} m &\geq \operatorname{grad} bg_0\,, && \text{da } \operatorname{grad} d \leq m \text{ und } \operatorname{grad} ah_0 \leq m \\ &= \operatorname{grad} b + \underbrace{\operatorname{grad} g_0}_{r} && \text{nach Algebra 6.13 (c)}\,. \end{aligned}$$

□

Behauptung 2. Die Polynome g_0 und h_0 sind Startelemente von $(g_n)_{n\geq 0}$ und $(h_n)_{n\geq 0}$ in $\Lambda[X]$ mit den Eigenschaften

(I) $\qquad g_n \equiv g_0 \bmod \pi \quad$ und $\quad \operatorname{grad} g_n = r \quad \forall\, n$.

(II) $\qquad h_n \equiv h_0 \bmod \pi \quad$ und $\quad \operatorname{grad} h_n \leq m - r \quad \forall\, n$.

(III) $\qquad f \equiv g_n h_n \bmod \pi^{n+1}\ \forall\, n$.

Beweis. Es gelte (I), (II), (III) für festes $n \geq 0$. Dann gibt es ein $d \in \Lambda[X]$ mit $\operatorname{grad} d \leq m$, so daß gilt

(III') $$f - g_n h_n = d\pi^{n+1}\,.$$

Wähle $a, b \in \Lambda[X]$ wie in Behauptung 1. Nach (I), (II) und Behauptung 1 folgt dann $ah_n + bg_n \equiv d \bmod \pi$ und also

(IV) $$ah_n + bg_n = d + c\pi \quad \text{mit einem } c \in \Lambda[X]\,.$$

Setze

(V) $$\boxed{g_{n+1} = g_n + a\pi^{n+1}} \quad \text{und} \quad \boxed{h_{n+1} = h_n + b\pi^{n+1}}\,.$$

Dann sind (I) und (II) auch für g_{n+1} und h_{n+1} erfüllt. Ferner gilt:

$$\begin{aligned} g_{n+1}h_{n+1} &= g_n h_n + (ah_n + bg_n)\pi^{n+1} + ab\pi^n\pi^{n+2} \\ &\equiv g_n h_n + d\pi^{n+1} \bmod \pi^{n+2} \\ &= g_n h_n + f - g_n h_n \bmod \pi^{n+2} \\ &= f \bmod \pi^{n+2}\,. \end{aligned}$$

□

Nach (V) sind die r Koeffizienten von $g_{n+1} - g_n$ alle durch π^{n+1} teilbar, haben also jeweils für $n \to \infty$ den Grenzwert 0. Da K vollständig ist, konvergiert also die Folge $(g_n)_{n\geq 0}$ gegen ein Polynom $g \in \Lambda[X]$ mit dem Grad r.
Analog konvergiert $(h_n)_{n\geq 0}$ gegen ein $h \in \Lambda[X]$ vom Grad $\leq m - r$. Aus Behauptung 2 folgt nun Hensels Lemma. □

12.2 Wichtige Funktionen

Sei K vollständig bezüglich einer diskreten Bewertung $v\colon K^* \longrightarrow \mathbb{Z}^+$. Es sei $v(0) = +\infty$ gesetzt, und wie in 11.3, 11.4 seien

$$\begin{array}{rll} & \Lambda = \{x \in K \mid v(x) \geq 0\} & \text{der Bewertungsring,} \\ & \Lambda\pi = \{x \in K \mid v(x) > 0\} & \text{das maximale Ideal in } \Lambda\,, \\ \text{und} & k = \Lambda/\Lambda\pi & \text{der Restklassenkörper bezüglich } v\,. \end{array}$$

Satz. *Sei $f = a_0 + a_1X + \cdots + a_{d-1}X^{d-1} + X^d \in K[X]$ ein irreduzibles Polynom vom Grad d. Ist $v(a_0) \geq 0$, so ist $v(a_i) \geq 0\ \forall\, i = 1, \ldots, d-1$. Anders gesagt:*

$$\boxed{a_0 \in \Lambda} \quad \Longrightarrow \quad \boxed{a_i \in \Lambda\ \forall\, i}\,.$$

Beweis. Für $d = 1$ ist nichts zu zeigen. Sei $d > 1$.
Angenommen: $\exists\, n$ mit $v(a_n) < 0$.
Dann ist $n > 0$, da $v(a_0) \geq 0$.
Setze n so, daß $v(a_n) = \operatorname{Min}(v(a_0), \ldots, v(a_{d-1}))$ gilt. Setze

$$\boxed{b_i := \frac{a_i}{a_n} \quad \text{für} \quad i = 0, \ldots, d-1} \quad \text{und} \quad \boxed{b_d = \frac{1}{a_n}}\,.$$

Dann folgt $v(b_i) \underset{11.2}{=} v(a_i) - v(a_n) \geq 0$, $v(b_n) = 0$ und $v(b_d) \underset{11.2}{=} -v(a_n) > 0$.
Fazit:

$$\frac{1}{a_n} f = \sum_{i=0}^{d} b_i X^i \in \Lambda[X]\,, \text{ wobei } \overline{\frac{1}{a_n} f} \neq \bar{0} \in k\,,$$
$$\exists\, r \text{ mit } 0 < n \leq r < d\,, \text{ so daß}$$
$$v(b_r) = 0 \text{ und } v(b_i) > 0\ \forall\, i = r+1, \ldots, d\,.$$

Es folgt: $\overline{\frac{1}{a_n} f} = (\overline{b_0} + \overline{b_1}X + \cdots + \overline{b_r}X) \cdot \bar{1}$. Nach dem Hensellemma 12.1 gibt es $g, h \in \Lambda[X]$ mit $\frac{1}{a_n} f = gh$ und $0 < \operatorname{grad}(g) = r < d$. Also sind g und h beide nicht konstant im Widerspruch zur Irreduzibilität von f. $\square$

12.3 Die Norm für Schiefkörpererweiterungen

Sei K ein Körper, und sei A eine endlich-dimensionale K-Algebra. Für jedes $x \in A$ sei $\ell_x\colon A \longrightarrow A$, $a \longmapsto xa$, die Linksmultiplikation mit x. Die *Norm* $N_{A/K}(x) \in K$ ist durch

$$\boxed{N_{A/K}(x) := \det(\ell_x)}$$

definiert. Sei $A = D$ ein Schiefkörper. Dann erzeugt jedes $x \in D$ einen Körper $K(x)$ nach 5.3.

Lemma. *Sei* $f = a_0 + a_1X + \cdots + a_{r-1}X^{r-1} + X^r \in K[X]$ *das Minimalpolynom von* $x \in D^*$. *Dann gelten:*

(a) $N(x) := N_{K(x)/K}(x) = (-1)^r a_0$,

(b) $N_{D/K(x)} = N(x)^s$ *mit* $s = \dim_{K(x)} D$,

(c) $N_{D/K}(a) = a^n$ *mit* $n = \dim_K D \; \forall \, a \in K^*$,

(d) Ist $L = D$ *eine Galoiserweiterung von* K *mit Gruppe* G , *so ist* $N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x)$.

Beweis. (a) Die Menge $\mathcal{B} = \{1, x, \ldots, x^{r-1}\}$ bildet eine Basis von $K(x)$ über K nach Algebra 11.10. Es ist $x^r = -a_0 - a_1x - \cdots - a_{r-1}x^{r-1}$, und daher gehört nach AGLA 4.4 zu $\ell_x \colon K(x) \longrightarrow K(x)$ bezüglich $\mathcal{B}$ die Matrix

$$M := \mathrm{M}_{\mathcal{B}}^{\mathcal{B}}(\ell_x) = \begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & \ddots & \ddots & 0 & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -a_{r-1} \end{pmatrix}$$

Entwicklung nach der ersten Zeile (AGLA 6.8) ergibt
$N(x) = \det(M) = (-1)^{r+1}a_0 = (-1)^{r-1}(-a_0) = (-1)^r a_0$.

(b) Sei $\{v_1, \ldots, v_s\}$ eine Basis von D über $K(x)$. Dann ist

$$\begin{aligned} \mathcal{C} := \{&1v_1, xv_1, \ldots, x^{r-1}v_1, \\ &1v_2, xv_2, \ldots, x^{r-1}v_2, \\ &\ldots \\ &1v_s, xv_s, \ldots, x^{r-1}v_s\} \end{aligned}$$

eine Basis von D über K . Nach AGLA 4.4 gehört zu $\ell_x \colon D \longrightarrow D$ bezüglich $\mathcal{C}$ die Matrix

$$\mathrm{M}_{\mathcal{C}}^{\mathcal{C}}(\ell_x) = \begin{pmatrix} M & & 0 \\ & \ddots & \\ 0 & & M \end{pmatrix}$$

mit s Blöcken in der Diagonalen. Es folgt $N_{D/K}(x) = \det(M)^s = N(x)^s$.

(c) Da $X - a$ das Minimalpolynom von $a \in K^*$ ist, folgt $N(a) = a$, und nach (b) folgt $N_{D/K}(a) = a^n$.

(d) Sei $H := G(L/K(x))$. Dann gilt $\#H = s$, und es gibt $\sigma_1, \ldots, \sigma_r \in G$, so daß

$$G = \bigcup_{i=1}^{r} \sigma_i H \quad \text{(disjunkte Vereinigung)}$$

und $\#\sigma_i H = \#H$ gilt. Insbesonere $\sigma_i(x) \neq \sigma_j(x)\ \forall\, i \neq j$ in $\{1, \ldots, r\}$. Es folgt $f = \prod_{i=1}^{r}(X - \sigma_i(x))$ in $L[X]$ (vgl. AGLA 10.10 und Algebra 15.7, 15.8 „(1) $\Longrightarrow$ (3)“ , Satz 11.4).
Vergleich der Absolutglieder ergibt

$$(*) \qquad a_0 = (-1)^r \prod_{i=1}^{r} \sigma_i(x)\,.$$

Insgesamt folgt

$$\begin{aligned}
\prod_{\sigma \in G} \sigma(x) &= \prod_{\tau \in H} (\sigma_1\tau)(x) \cdot \cdots \cdot \prod_{\tau \in H} (\sigma_r\tau)(x) \\
&= \sigma_1(x)^s \cdot \cdots \cdot \sigma_r(x)^s, && \text{da } \tau(x) = x\ \forall\, \tau \in H \\
&= ((-1)^r a_0)^s && \text{nach } (*) \\
&= N(x)^s && \text{nach (a)} \\
&= N_{L/K}(x) && \text{nach (b)}\,.
\end{aligned}$$

□

12.4 Fortsetzungssatz

Sei D ein Schiefkörper über K mit $\dim_K D =: n < \infty$. Eine *Exponentenbewertung von* D ist eine Abbildung $w\colon D^* \longrightarrow \mathbb{R}$ mit

$$(1_D) \qquad w(xy) = w(x) + w(y)$$

$$(2_D) \qquad w(x+y) \geq \operatorname{Min}(w(x), w(y))$$

für alle $x, y \in D^*$. Dabei sei $w(0) := +\infty$ gesetzt. Analog zu 11.2 gelten

$$\begin{aligned}
w(1) &= 0\,, \\
w(-x) &= w(x) \text{ und} \\
w(x^{-1}) &= -w(x)\,.
\end{aligned}$$

Satz. *Sei K bezüglich einer diskreten Bewertung $v\colon K^* \longrightarrow \mathbb{Z}^+$ vollständig. Dann gibt es genau eine Exponentenbewertung $w\colon D^* \longrightarrow \mathbb{R}$, die v fortsetzt. Diese ist durch die Formel*

$$(1) \qquad w(x) = \frac{1}{n} v\left(N_{D/K}(x)\right)\ \forall\, x \in D^*$$

gegeben. Ferner ist D vollständig bezüglich w.

Beweis. **Existenz:** Definiere w durch die Formel (1). Dann ist w eine Fortsetzung von v, da $N_{D/K}(a) = a^n$ nach 12.3(c) und also $w(a) = \frac{1}{n}(nv(a)) = v(a)$ für alle $a \in K^*$ gilt. Da die Determinante und damit die Norm multiplikativ ist, folgt

$$w(xy) = w(x) + w(y)\ \forall\, x, y \in D^* \quad \text{nach 11.2 und (1)}\,.$$

Also gilt (1_D). Sei $f = a_0 + a_1X + \cdots + a_{r-1}X^{r-1} + X^r \in K[X]$ das Minimalpolynom von $x \in D^*$. Dann gilt

$$\text{(1')} \qquad w(x) = \frac{1}{r}v(a_0)\,, \ \text{denn}$$

$$\begin{aligned}
w(x) &= \frac{1}{n}v\left(N(x)^{n/r}\right) && \text{nach 12.3 (b)}\\
&= \frac{1}{r}v\left(N(x)\right) && \text{nach 11.2}\\
&= \frac{1}{r}v\left((-1)^r a_0\right) && \text{nach 12.3 (a)}\\
&= \frac{1}{r}v(a_0) && \text{nach 11.2}\,.
\end{aligned}$$

Ist $w(x) \geq 0$, so ist $w(a_0) \geq 0$ nach (1') und also $w(a_i) \geq 0\ \forall\, i = 1, \ldots, r-1$ nach 12.2. Da das Minimalpolynom von $1 + X$ das Absolutglied $a_0 - a_1 + a_2 - \cdots + (-1)^{r-1}a_{r-1} + (-1)^r$ hat, folgt dann auch $w(1 + x) \geq 0$. Sind nun $z, y \in D^*$ mit $w(z) \leq w(y)$ gegeben, so gilt $w(x) \geq 0$ für $x = z^{-1}y$ und daher

$$\begin{aligned}
w(z + y) &= w(z + zx) = w(z(1 + x))\\
&= w(z) + \underbrace{w(1 + x)}_{\geq 0} \geq w(z) = \mathrm{Min}(w(z), w(y))\,.
\end{aligned}$$

Damit ist (2_D) gezeigt.

Eindeutigkeit: Sei $w' \colon D^* \longrightarrow \mathbb{R}$ eine beliebige Exponentenbewertung, die v fortsetzt, und sei $w \colon D^* \longrightarrow \mathbb{R}$ durch die Formel (1') gegeben. Wir zeigen $w' = w$. Wähle $\pi \in K^*$ mit $v(\pi) = 1$.
Dann gilt

$$\boxed{w(\pi) = 1 = w'(\pi)}\,.$$

Sei $y \in D^*$. Dann gibt es nach (1) ein $m \in \mathbb{Z}$ mit

$$\boxed{nw(y) = m}\,.$$

Für $x := y^n \pi^{-m}$ folgt also $w(x) \underset{(1_D)}{=} nw(y) - mw(\pi) = nw(y) - m = 0$. Wie die Behauptung unten zeigt, gilt $w'(x) = 0$. Es folgt $w'(x) = nw'(y) - m = 0$ und also $w(y) = w'(y)$.

Behauptung. Für jedes $x \in D^*$ mit $w(x) = 0$ gilt $w'(x) = 0$.

Beweis. Angenommen: $w'(x) < 0$.
Sei $f = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in K[X]$ das Minimalpolynom von x. Dann gilt $w'(a_0) = v(a_0) \underset{(1')}{=} 0$, da $w(x) = 0$ ist, und also $w'(a_i) = v(a_i) \geq 0 \ \forall\, i = 1, \ldots, r-1$ nach 12.2. Multipliziere die Gleichung $f(x) = 0$ mit x^{1-r}. Dann folgt

$$-x = a_{r-1} + a_{r-2}x^{-1} + \cdots + a_0 x^{1-r}$$

und also

$$w'(-x) \geq \operatorname{Min}(w'(a_{r-1}), w'(a_{r-2}) - w'(x), \ldots, w'(a_0) + (1-r)w'(x))$$

nach (1_D) und (2_D). Es folgt $w'(x) = w'(-x) \geq 0$ im Widerspruch zur Annahme. Damit ist $w'(x) \geq 0$ gezeigt. Es folgt $w'(x^{-1}) = -w'(x) \leq 0$. Man führt nun analog die Annahme $w'(x^{-1}) < 0$ zum Widerspruch und erhält $w'(x^{-1}) = -w'(x) \geq 0$. Es folgt $w'(x) = 0$. □

Den Vollständigkeitsnachweis führen wir allgemeiner in 12.5 bezüglich eines Absolutbetrages $|\ | : D^* \longrightarrow \mathbb{R}_{\geq 0}$ durch. Setzt man $|x| = e^{-w(x)}$ und $w(x) = -\log|x|$ für $x \in D^*$, so folgt der Fortsetzungssatz.

□

12.5 Vollständigkeitsnachweis in 12.4

Sei D ein Schiefkörper über K mit $\dim_K D = m < \infty$. Sei K vollständig bezüglich eines Absolutbetrages $|\ | : K^* \longrightarrow \mathbb{R}_{\geq 0}$, und sei $|\ | : D^* \longrightarrow \mathbb{R}_{\geq 0}$ eine Fortsetzung, d.h. es gelte $|xy| = |x|\ |y|$ und $|x+y| \leq |x|+|y| \ \forall\, x, y \in D^*$ sowie $|0| = 0$.
Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge in D, und sei $\{e_1, \ldots, e_m\}$ eine Basis von D über K. Dann gilt:

$$x_n = a_1^{(n)}e_1 + \cdots + a_m^{(n)}e_m \quad \text{mit} \quad a_i^{(n)} \in K \ \forall\, n \in \mathbb{N}, i = 1, \ldots, m.$$

Lemma. *Ist* $\left(a_i^{(n)}\right)_{n\in\mathbb{N}}$ *eine Cauchyfolge für jedes* $i = 1, \ldots, m$, *so existiert* $x := \lim\limits_{x\to\infty} x_n$ *in* D. *Es ist* $x = a_1e_1 + \cdots + a_me_m$ *mit* $a_i = \lim\limits_{n\to\infty} a_i^{(n)} \ \forall\, i = 1, \ldots, m$.

Beweis. Da K vollständig ist, $\exists\, a_i = \lim\limits_{n\to\infty} a_i^{(n)}\ \forall\, i = 1, \dots, m$. Wähle $M > 0$ in $\mathbb{R}$, so daß $|e_i| \le M\ \forall\, i = 1, \dots, m$ gilt. Zu jedem $0 < \varepsilon \in \mathbb{R}$ gibt es dann ein $n_0 \in \mathbb{N}$, so daß

$$\left|a_i^{(n)} - a_i\right| < \frac{\varepsilon}{mM} \qquad \forall\, n \ge n_0 \text{ und } i = 1, \dots, m \text{ gilt.}$$

Setze

$$\boxed{x = a_1 e_1 + \cdots + a_m e_m}\,.$$

Dann folgt

$$\begin{aligned} |x_n - x| &= \left|\left(a_1^{(n)} - a_1\right) e_1 + \cdots + \left(a_m^{(n)} - a_m\right) e_m\right| \\ &\le \left(\left|a_1^{(n)} - a_1\right| + \cdots + \left|a_m^{(n)} - a_m\right|\right) M \\ &< \left(m \frac{\varepsilon}{mM}\right) M = \varepsilon\ \forall\, n \ge n_0\,. \end{aligned}$$

□

Satz. *Ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge in D, so ist $\left(a_i^{(n)}\right)_{n\in\mathbb{N}}$ eine Cauchyfolge in K für jedes $i = 1, \dots, m$.*

Beweis. Zeige durch Induktion nach $r \le m$:
Ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge in D mit $x_n = \sum\limits_{i=1}^{r} a_i^{(n)} e_i$, so ist $\left(a_i^{(n)}\right)_{n\in\mathbb{N}}$ eine Cauchyfolge $\forall\, i = 1, \dots, r$.

$r = 1$: Dann ist $x_n = a_1^{(n)} e_1$ und $\left(a_i^{(n)}\right)_{n\in\mathbb{N}}$ eine Cauchyfolge, da $(x_n)_{n\in\mathbb{N}}$ eine solche ist.

$r > 1$: Sei $x_n = \sum\limits_{i=1}^{r} a_i^{(n)} e_i$ für jedes $n \in \mathbb{N}$.

1. Fall: Die Folge $\left(a_r^{(n)}\right)_{n\in\mathbb{N}}$ ist eine Cauchyfolge. Dann ist $\left(x_n - a_r^{(n)} e_r\right)_{n\in\mathbb{N}}$ eine Cauchyfolge, und daher sind nach Induktionsvoraussetzung auch die Folgen $\left(a_i^{(n)}\right)_{n\in\mathbb{N}}$ für $i = 1, \dots, r-1$ Cauchyfolgen.

2. Fall: Die Folge $\left(a_r^{(n)}\right)_{n\in\mathbb{N}}$ ist keine Cauchyfolge. Dann gibt es eine Zahlenfolge $(m_1, m_2, m_3, \dots) \subset \mathbb{N}$ und $\varepsilon > 0$ in $\mathbb{R}$, so daß $\left|a_r^{(n)} - a_r^{(n+m_n)}\right| > \varepsilon\ \forall\, n \in \mathbb{N}$ gilt. Die Folge $(z_n)_{n\in\mathbb{N}}$ mit

$$z_n = \frac{x_n - x_{n+m_n}}{a_r^{(n)} - a_r^{(n+m_n)}} = \left(\sum_{i=1}^{r-1} \frac{a_i^{(n)} - a_i^{(n+m_n)}}{a_r^{(n)} - a_r^{(n+m_n)}} e_i\right) + e_r =: \left(\sum_{i=1}^{r-1} b_i^{(n)} e_i\right) + e_r$$

ist daher eine Nullfolge, denn da $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge ist, geht der Zähler $x_n - x_{n+m_n}$ für $n \to \infty$ nach 0. Es ist

$$z_n - e_r = \sum_{i=1}^{r-1} b_i^{(n)} e_i$$

und also $\left(b_i^{(n)}\right)_{n\in\mathbb{N}}$ eine Cauchyfolge für alle $i = 1, \ldots, r-1$ nach Induktionsvoraussetzung. Da K vollständig ist, existiert $b_i := \lim\limits_{n\to\infty} b_i^{(n)}$. Nach dem Lemma folgt

$$-e_r = \sum_{i=1}^{r-1} b_i e_i$$

im Widerspruch zur linearen Unabhängigkeit von $e_1, \ldots, e_r$. Der 2. Fall kann also gar nicht auftreten. Aus dem 1. Fall folgt nun der Satz.

□

Korollar. *D ist vollständig.*

Beweis. folgt aus dem Satz und dem Lemma. □

Bemerkung. Die obigen Betrachtungen verallgemeinern den bekannten Satz, daß eine Folge $(z_n)_{n\in\mathbb{N}}$ komplexer Zahlen (bezogen auf den gewöhnlichen Absolutbetrag) genau dann konvergiert, wenn die Folgen $(\Re(z_n))_{n\in\mathbb{N}}$ und $(\Im(z_n))_{n\in\mathbb{N}}$ in $\mathbb{R}$ konvergieren.
Im Fall der Konvergenz gilt

$$\lim_{n\to\infty} z_n = \lim_{n\to\infty} \Re(z_n) + \lim_{n\to\infty} \Im(z_n)\sqrt{-1}\,.$$

Hiermit zeigt man, daß $\mathbb{C}$ vollständig ist, vgl. Forster, Analysis 1, § 13, Sätze 2,3,4.

12.6 Verzweigungsindex

Sei K vollständig bezüglich einer diskreten Bewertung $v\colon K^* \longrightarrow \mathbb{Z}^+$, und sei D ein Schiefkörper über K mit $\dim_K D = n < \infty$. Dann besitzt v nach 12.4 genau eine Fortsetzung $w\colon D^* \longrightarrow \mathbb{R}$, und für diese gilt

$$\boxed{nw(x) \in \mathbb{Z}\ \forall\, x \in D^*}$$

nach (1) in 12.4.

Lemma. *(a) Es gibt einen positiven Teiler e von n, so daß $w(D^*) = \frac{1}{e}\mathbb{Z}$ gilt.*

(b) Es gibt genau eine diskrete Bewertung $v_D\colon D^* \twoheadrightarrow \mathbb{Z}^+$ mit

$$\boxed{v_D(a) = ev(a)\ \forall\, a \in K^*}\,.$$

Diese ist durch $v_D = ew$ gegeben und hat die folgenden Eigenschaften, wobei $v_D(0) := +\infty$ gesetzt sei:

(1) Es gibt einen Bewertungsring

$$\Lambda_D := \{x \in D \mid v_D(x) \geq 0\}$$

mit Einheitengruppe

$$\Lambda_D^* = \{x \in D \mid v_D(x) = 0\}\,.$$

(2) Es gibt ein Primelement, *das ist ein Element $\pi_D \in \Lambda_D$ mit $v_D(\pi_D) = 1$. Für jedes $x \in D^*$ gilt*

$$\boxed{x = u_x \pi_D^{v_D(x)} \ \textit{mit}\ u_x \in \Lambda_D^*}\,.$$

(3) Das zu v_D gehörige Bewertungsideal *wird von π_D erzeugt. Es gilt*

$$\Lambda_D \pi_D = \{x \in D \mid v_D(x) > 0\}\,.$$

(4) Es sei $\pi \in K^*$ ein Primelement bezüglich v, es gelte also $v(\pi) = 1$. Dann ist

$$\boxed{\pi = u\pi_D^e \quad \textit{mit einem}\ u \in \Lambda_D^*}\,.$$

(5) Es ist D vollständig bezüglich v_D.

Beweis. (a) Es ist $nw(D^*)$ eine Untergruppe von $\mathbb{Z}^+$, denn es gilt $0 = nw(1)$ und $nw(x) - nw(y) = nw(xy^{-1})\ \forall\, x, y \in D^*$.
Nach AGLA 10.5.5 gibt es daher ein $m \in \mathbb{Z}$ mit

$$\boxed{nw(D^*) = m\mathbb{Z}}\,.$$

Wir können hierbei $m > 0$ annehmen. Es ist $n = nw(\pi) \in nw(D^*)$ und also $n = me$ mit einem $e \in \mathbb{Z}$. Es folgt $e > 0$ und $w(D^*) = \frac{m}{n}\mathbb{Z} = \frac{1}{e}\mathbb{Z}$.

(b) Die Existenz- und Eindeutigkeitsaussage folgt aus 12.4 und (a). Die Eigenschaften 1,2,3 folgen analog wie in 11.2 und 11.3.

4. Da $v_D(\pi) = ev(\pi) = e$ gilt, folgt $\pi = u_\pi \pi_D^e$ mit $u_\pi \in \Lambda_D^*$ nach 2.
5. folgt, weil D bezüglich $w = \frac{1}{e} v_D$ nach 12.4 vollständig ist.

□

Definition. Die Zahl e aus dem Lemma heißt *Verzweigungsindex* von D über K.

Bemerkung. (i) Es ist e der Index von $w(K^*)$ in $w(D^*)$, also $e = (w(D) : w(K^*))$ im Sinne der Gruppentheorie, denn nach (b) ist $ew(D^*) = \mathbb{Z}$ und $ew(K^*) = e\mathbb{Z}$.

(ii) Aus dem Lemma folgt

$$\boxed{\pi \text{ Primelement bezüglich } v_D} \quad \Longleftrightarrow \quad \boxed{e = 1}.$$

Ist D kommutativ, so folgt aus 4. und 11.3

$$\boxed{\Lambda_D \pi \text{ ist Primideal}} \quad \Longleftrightarrow \quad \boxed{e = 1}.$$

12.7 Restklassengrad

Sei K vollständig bezüglich einer diskreten Bewertung $v\colon K^* \longrightarrow \mathbb{Z}^+$. Wir beschränken uns hier aus den Fall, daß der Schiefkörper D in 12.6 eine Körpererweiterung $D = L$ vom Grad n über K ist, und betrachten die Restklassenkörper

$$\boxed{k := \Lambda/\Lambda\pi} \quad \text{und} \quad \boxed{\ell := \Lambda_L/\Lambda_L \pi_L}.$$

Aus 11.3 und 12.6 folgt $\Lambda \subset \Lambda_L$. Hierdurch wird ein Homomorphismus $k \longrightarrow \ell$ induziert, denn $\Lambda\pi \subset \Lambda_L \pi \underset{4.}{=} \Lambda_L \pi_L^e \subset \Lambda_L \pi_L$. Da k ein Körper ist, können wir also ℓ als Körpererweiterung von k auffassen.

Definition. Der Körpergrad $f := \dim_k \ell$ heißt *Restklassengrad* von L über K.

Lemma. *Es gilt* $f \leq n := \dim_K L$.

Beweis. Angenommen, es existiert ein $r > n$ und r linear unabhängige Elemente $\overline{x_1}, \dots, \overline{x_r} \in \ell^*$. Wähle $x_1, \dots, x_r \in \Lambda_L$ mit $x_i + \Lambda_L \pi_L = \overline{x_i}$ für $i = 1, \dots, r$. Dann sind $x_1, \dots, x_r$ linear abhängig. Es gibt also eine nicht-triviale Linearkombination $\sum\limits_{i=1}^{r} a_i x_i = 0$ mit $a_i \in K$. Durch Multiplikation mit $\frac{1}{a_j}$, wobei $v(a_j)$ ein minimaler Wert ist, kann man erreichen, daß alle Koeffizienten in Λ liegen und mindestens einer in Λ^* liegt (wie im Beweis von 12.2). Reduktion nach $\Lambda_L \pi_L$ ergibt eine nicht-triviale Linearkombination $\sum\limits_{i=1}^{r} \overline{a_i x_i} = \overline{0}$ in ℓ im Widerspruch zur Annahme. □

12.8 Reihenentwicklung

Sei K vollständig bezüglich einer diskreten Bewertung $v\colon K^* \longrightarrow \mathbb{Z}^+$, wobei $v(0) := +\infty$ gesetzt sei. Es seien Λ der Bewertungsring, π ein Primelement und $k = \Lambda/\Lambda\pi$ der Restklassenkörper. Wähle zu jedem $\overline{x} \in k$ einen Vertreter $x \in \Lambda$ aus und erhalte so ein Vertretersystem $\mathcal{R} \subset \Lambda$ für die Elemente von k. Es sei $0 \in \mathcal{R}$.

Satz. *Jedes $a \in K$ hat eine eindeutige Darstellung als*

$$a = \sum_{n=v(a)}^{\infty} a_n \pi^n \quad \textit{mit} \quad a_n \in \mathcal{R}\,.$$

Umgekehrt konvergiert jede Reihe der Form $\sum\limits_{-\infty \ll n}^{\infty} b_n \pi^n$ mit $b_n \in \mathcal{R}$ gegen ein $b \in K$ mit $v(b) = \mathrm{Min}(n \mid b_n \neq 0)$.

Beweis mit rekursiver Argumentation:. Sei zunächst $a \in \Lambda^*$, also $v(a) = 0$. Nach Wahl von $\mathcal{R}$ gibt es ein $a_0 \in \mathcal{R}$ mit $a \equiv a_0 \bmod \Lambda\pi$.
Es gebe $a_0, \dots, a_{n-1} \in \mathcal{R}$ mit

$$a \equiv a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} \bmod \Lambda\pi^n\,.$$

Dann ist $a = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + b\pi^n$ mit einem $b \in \Lambda$. Zu b gibt es genau ein $a_n \in \mathcal{R}$ mit $b \equiv a_n \bmod \Lambda\pi$. Es folgt

$$a \equiv a_0 + a_1\pi + \cdots + a_n\pi^n \bmod \Lambda\pi^{n+1}\,,$$

und daher gilt $a = \sum\limits_{n=0}^{\infty} a_n\pi^n$.
Sei $\sum\limits_{n=0}^{\infty} a_n\pi^n = a = \sum\limits_{n=0}^{\infty} b_n\pi^n$ mit $a_n, b_n \in \mathcal{R}$.
Reduktion mod $\Lambda\pi$ ergibt $a_0 \equiv b_0 \bmod \Lambda\pi$, und daher $a_0 = b_0$ nach Wahl von $\mathcal{R}$.
Es gelte $a_n = b_n$ für $n = 0, \dots, r-1$. Dann folgt

$$\sum_{n=r}^{\infty} a_n\pi^n = \sum_{n=r}^{\infty} b_n\pi^n\,.$$

Multiplikation mit mit π^{-r} und Reduktion mod $\Lambda\pi$ ergibt dann $a_r \equiv b_r \bmod \Lambda\pi$ und also $a_r = b_r$. Die Darstellung von a ist daher eindeutig.
Für $a = 0$ ist der Satz richtig, da $0 \in \mathcal{R}$ ist. Sei $a \neq 0$ in K. Dann ist $a = u\pi^{v(a)}$ mit einem $u \in \Lambda^*$ nach 11.3. Wie schon gezeigt, ist $u = \sum\limits_{i=0}^{\infty} c_i\pi^i$ mit eindeutig bestimmten $c_i \in \mathcal{R}$.

Es folgt $a = \sum\limits_{i=0}^{\infty} c_i \pi^{i+v(a)} = \sum\limits_{n=v(a)}^{\infty} a_n \pi^n$ mit $a_n = c_{n-v(a)}$.

Umgekehrt: Da K vollständig ist, existiert $b := \sum\limits_{-\infty \ll n}^{\infty} b_n \pi^n$. Da $0 \in \mathcal{R}$ ist, wird die Restklasse $\overline{0}$ durch 0 vertreten. Ist also $b_n \neq 0$, so ist $b_n \in \Lambda \setminus \Lambda\pi$ und also $v(b_n) = 0$. Es folgt $v(b_n \pi^n) = v(b_n) + n = n$ und daher $v(b) = \mathrm{Min}\{n \mid b_n \neq 0\}$. □

12.9 Die p-adischen Zahlen

Sei p eine Primzahl. Die Vervollständigung von $\mathbb{Q}$ bezüglich des (in 11.6 (ii) definierten) p-adischen Absolutbetrags heißt *p-adischer Zahlkörper* und wird mit $\mathbb{Q}_p$ bezeichnet. Man kann $\mathbb{Q}_p$ auch als Vervollständigung von $\mathbb{Q}$ bezüglich der diskreten Bewertung v_p ansehen, wobei $v_p(x)$ der Exponent von p in der Primfaktorzerlegung von $x \in \mathbb{Q}^*$ ist, vgl. 11.5.3.
Nach 12.8 lassen sich daher die Elemente von $\mathbb{Q}_p$ eindeutig darstellen als

$$a = \sum_{-\infty \ll n}^{\infty} a_n \pi^n \text{ mit } a_n \in \{0, 1, \ldots, p-1\}.$$

In dieser Form wurden die p-adischen Zahlen zuerst entdeckt, und zwar von K. Hensel. Die Theorie bewerteter Körper wurde durch Steinitz, Ostrowski u.a. entwickelt.

12.10 Funktionenkörper

Sei $K(X)$ der rationale Funktionenkörper in einer Unbestimmten X. Wie in 11.5.1 beschrieben, definiert jedes normierte irreduzible Polynom $p \in K[X]$ eine diskrete Bewertung von $K(X)$, und der Restklassenköper ist isomorph zu $K[X]/pK[X]$, also $k = K(x)$ mit einer Nullstelle x von p.
Sei $K(X)_p$ die zugehörige Vervollständigung von $K(X)$. In der gemäß 12.8 eindeutigen Darstellung

$$\alpha = \sum_{-\infty \ll n} \alpha_n p^n \text{ mit } \alpha_n \in \mathcal{R}.$$

Für die Elemente von $K(X)_p$ kann als Vertretersystem das kleinste Restsystem mod p gewählt werden. Das sind dann die Polynome vom Grad $< \operatorname{grad} p$. Ist $p = X - a$ mit $a \in K$, so ist $k = K$ und $\mathcal{R} = K$ wählbar. Speziell für $p = X$ ist $K(X)_p =: K((X))$ der *Körper der formalen Laurent-Reihen in einer Unbestimmten X mit endlichem Hauptteil.*
Ist $K(X)$ mit der Gradbewertung aus 11.5.2 versehen und $K(X)_\infty$ die Vervollständigung, so ist $K(X)_\infty = K((X^{-1}))$.

12.11 Verallgemeinerte Reihendarstellung

Seien L ein Körper, der bezüglich einer diskreten Bewertung $v_L \colon L^* \longrightarrow \mathbb{Z}^+$ vollständig sei, Λ_L der Bewertungsring, ℓ der Restklassenkörper und $\mathcal{R}_L \subset \Lambda_L$ ein Vertretersystem für die Elemente aus ℓ, das 0 enthalte.

Lemma. *Für jedes $i \in \mathbb{Z}$ sei ein Element $\pi_i \in L^*$ mit $v_L(\pi_i) = i$ vorgegeben. Dann besitzt jedes $\alpha \in L$ eine eindeutige Darstellung*

$$\boxed{\alpha = \sum_{-\infty \ll i} \alpha_i \pi_i \quad \textit{mit} \quad \alpha_i \in \mathcal{R}_L}\,.$$

Beweis. Analog wie in 12.8, vgl. Aufgabe 49. □

12.12 Die Formel $ef = n$

Sei K ein diskret bewerteter vollständiger Körper mit Bewertungsring Λ und Restklassenkörper k. Sei L eine Körpererweiterung von K mit $\dim_K L = n < \infty$ und $v_L \colon L^* \longrightarrow \mathbb{Z}^+$ die diskrete Bewertung von L gemäß 12.6. Ferner sei $f = \dim_k \ell$ der Restklassengrad und e der Verzweigungsindex von L über K.

Satz. *Es gilt $ef = n$.*

Beweis. Nach 12.7 ist $f \leq n$. Wähle $x_1, \ldots, x_f \in \Lambda_L$, so daß die Restklassen $\overline{x_1}, \ldots, \overline{x_f}$ eine Basis von ℓ über k bilden, und wähle ein Primelement π_L bezüglich v_L. Wir zeigen, daß die Elemente

$$x_i \pi_L^j \text{ für } i = 1, \ldots, f \text{ und } j = 0, \ldots, e-1$$

eine Basis von L über K bilden. Hieraus folgt $ef = n$.
Sei $\mathcal{R}$ ein Vertretersytem für die Elemente aus k, das 0 enthalte. Dann ist

$$\mathcal{R}_L = \{a_1 x_1 + \cdots + a_f x_f \mid a_1, \ldots, a_f \in \mathcal{R}\}$$

ein Vertretersystem in Λ_L für die Elemente von ℓ mit $0 \in \mathcal{R}_L$. Wähle ein Primelement $\pi \in K$. Für $0 \leq j < e$ und $m \in \mathbb{Z}$ gilt dann

$$v_L(\pi_L^j \pi^m) \underset{11.2}{=} j \underbrace{v_L(\pi_L)}_{1} + m \underbrace{v_L(\pi)}_{e} \underset{12.6}{=} j + me\,.$$

Nach 12.11 und Wahl von $\mathcal{R}_L$ ist also jedes $\alpha \in L$ eindeutig darstellbar als

$$\alpha = \sum_{-\infty \ll m} \sum_{j=0}^{e-1} \alpha_{j+me} \pi_L^j \pi^m\,,$$

wobei

$$\alpha_{j+me} = \sum_{i=1}^{f} a_{ijm} x_i \text{ mit eindeutig bestimmten } a_{ijm} \in \mathcal{R}\,.$$

Es folgt $\sum\limits_{-\infty \ll m} \sum\limits_{j=0}^{e-1} \sum\limits_{i=1}^{f} a_{ijm} x_i \pi_L^j \pi^m$. Durch Umordnung ergibt sich

$$\alpha = \sum_{j=0}^{e-1} \sum_{i=1}^{f} a_{ij} x_i \pi_L^j \text{ mit } a_{ij} = \sum_{-\infty \ll m} a_{ijm} \pi^m$$

aus K nach 12.8.
Also bilden die Elemente $x_i \pi_L^j$ ein Erzeugendensystem von L über K . Noch zu zeigen ist, daß die Koeffizienten a_{ij} durch α eindeutig bestimmt sind. Sei $\alpha = \sum\limits_{j=0}^{e-1} \sum\limits_{i=1}^{f} b_{ij} x_i \pi_L^j$ mit $b_{ij} \in K$. Dann ist $b_{ij} = \sum\limits_{-\infty \ll m} b_{ijm} \pi^m$ mit $b_{ijk} \in \mathcal{R}$ nach 12.8. Durch rückwärtige Ausführung der Umordnung folgt

$$\alpha = \sum_{-\infty \ll m} \sum_{j=0}^{e-1} \underbrace{\sum_{i=1}^{f} b_{ijm} x_i \pi_L^j}_{\in \mathcal{R}_L} \pi^m\,.$$

Nach 12.11 ist diese Darstellung eindeutig. Es folgt $\sum\limits_{i=1}^{f} b_{ijm} x_i = \sum\limits_{i=1}^{f} \alpha_{ijm} x_i$ und hieraus $b_{ijm} = a_{ijm}$ nach Wahl von $\mathcal{R}_L$. Hieraus wiederum folgt $b_{ij} = a_{ij}$. $\square$

12.13 Unverzweigte Erweiterungen

Seien K und L wie in 12.12 gegeben. Dann heißt L *unverzweigt* über K , falls der Verzweigungsindex $e = 1$ ist, und falls der Restklassenkörper ℓ separabel über k ist.
Ist $e = 1$, so gilt $f = \dim_k \ell = \dim_K L$ nach 12.12. Ist der Restklassenkörper k vollkommen, so ist jede endliche Körpererweiterung von k separabel, und es genügt, $e = 1$ zu fordern. Insbesondere genügt dies, falls k endlich ist (vgl. Algebra 16.8).

13 Lokale Körper

Ein *lokaler Körper* ist ein diskret bewerteter, vollständiger Körper mit endlichem Restklassenkörper.

13.1 Beispiele für lokale Körper

1) Die p-adischen Körper $\mathbb{Q}_p$ (vgl. 12.9).

2) Jede endliche Körpererweiterung eines Körpers $\mathbb{Q}_p$ (folgt aus 12.6 und 12.7).

3) Die Körper $\mathbb{F}_q((X))$, wobei $\mathbb{F}_q$ ein endlicher Körper ist (vgl. 12.10).

Man kann zeigen, daß hierdurch alle lokalen Körper erfaßt sind, und daß in 2) genau die Komplettierungen der endlichen Körpererweiterungen von $\mathbb{Q}$ auftreten (bezüglich diskreter Bewertungen, vgl. Lorenz, Algebra II).

13.2 Hilfssatz über Einheitswurzeln

Sei K ein Körper, der bezüglich einer diskreten Bewertung $v_K\colon K^* \twoheadrightarrow \mathbb{Z}^+$ vollständig sei, und sei $m \in \mathbb{N}$ mit $\operatorname{char} K \nmid m$. Bezeichnet Λ_K den Bewertungsring bezüglich v_K, so gelten:

(1) Ist ξ eine m-te Einheitswurzel über K, und ist $L = K(\xi)$, so ist $\xi \in \Lambda_L^*$.

(2) Ist p ein normierter, irreduzibler Faktor des Polynoms $X^m - 1 \in K[X]$, so ist $p \in \Lambda_K[X]$.

Beweis. (1) Es ist $0 \underset{11.2}{=} v_L(1) = v_L(\xi^m) \underset{11.2}{=} m v_L(\xi)$, und also ist $\xi \in \Lambda_L^*$ nach 11.3.

(2) Sei $p = X^r + a_{r-1}X^{r-1} + \cdots + a_0 \in K[X]$, und sei ξ eine Nullstelle von p im m-ten Einheitswurzelkörper und $L = K(\xi)$.
Dann gilt $0 \underset{(1)}{=} v_L(\xi) = \frac{e}{r} v_K(a_0)$ nach 12.6 und (1') in 12.4. Also ist $a_0 \in \Lambda_K^*$, und nach 12.2 folgt $a_i \in \Lambda_K \;\forall\, i = 1, \ldots, r-1$.

□

13.3 Charakterisierung unverzweigter Erweiterungen

Die Anzahl der Elemente eines endlichen Körpers ist stets eine Primzahlpotenz. Umgekehrt gibt es zu jeder Primzahlpotenz q bis auf Isomorphie genau einen Körper $\mathbb{F}_q$ mit q Elementen (vgl. Algebra 14.3, 14.4).

Satz. *Seien F ein lokaler Körper, L eine endliche Körpererweiterung von F und $\mathbb{F}_q$ bzw. ℓ die Restklassenkörper von F bzw. L. Dann sind äquivalent:*

(i) L ist unverzweigt über F.

(ii) L ist Zerfällungskörper des Polynoms $X^{q^n-1}-1 \in F[X]$ für ein $n \in \mathbb{N}$.

(iii) L ist galoissch über F, und die Galoisgruppe $G(L/F)$ ist kanonisch isomorph zur Galoisgruppe $G(\ell/\mathbb{F}_q)$.

Beweis. Da $\operatorname{char} F = 0$ oder $\operatorname{char} F = \operatorname{char} \mathbb{F}_q$ gilt, ist $q^n - 1$ teilerfremd zu $\operatorname{char} F$ und $\operatorname{char} \mathbb{F}_q$ $\forall\, n \in \mathbb{N}$. Nach 12.6, 12.7 ist L ein lokaler Körper.

„(ii) $\Longrightarrow$ (iii)“: Sei $n \in \mathbb{N}$, und sei L Zerfällungskörper von $X^m - 1 \in F[X]$ mit $m = q^n - 1$. Dann ist $L = F(\zeta)$ mit einer primitiven m-ten Einheitswurzel ζ über F, und insbesondere ist L galoissch über F (vgl. Algebra 17.1–17.4). Aus (ii) und 13.2 folgt

$$(*) \qquad X^m - 1 = \prod_{i=0}^{m-1} (X - \zeta^i) \text{ in } \Lambda_L[X]$$

und also

$$X^m - 1 = \prod_{i=0}^{m-1} (X - \overline{\zeta}^i) \text{ in } \ell[X],$$

wobei $\overline{\zeta}$ die Restklasse von ζ in ℓ ist. Hieraus folgt

$$\boxed{\mathbb{F}_{q^m} \hookrightarrow \ell} \quad \text{und} \quad \operatorname{ord}(\overline{\zeta}) = m,$$

denn $\mathbb{F}_{q^m}^*$ besteht genau aus allen Nullstellen des Polynoms $X^m - 1$ nach Algebra 14.4. Für $\sigma \in G(L/F)$ und jedes $x \in L^*$ gilt

$$N_{L/F}(x) = N_{L/F}(\sigma(x)) \text{ nach } 12.3$$

und also $v_L(x) = v_L(\sigma(x))$ nach (1) in 12.4 und 12.6 (b). Hieraus folgt, daß σ einen Automorphismus $\overline{\sigma} \in G(\ell/\mathbb{F}_q)$ induziert. Bezeichnet $\overline{x}$ die Restklasse von $x \in \Lambda_L$ in ℓ, so gilt $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$. Es ist $\boxed{\sigma(\zeta) = \zeta^{m_\sigma}}$ mit einem $m_\sigma \in \{1, \ldots, m\}$, vgl. $(*)$ und Algebra, Satz 11.4.
Ist $\overline{\sigma} = \mathrm{id}$, so folgt $\overline{\zeta} = \overline{\sigma}(\overline{\zeta}) = \overline{\sigma(\zeta)} = \overline{\zeta}^{m_\sigma}$ und also $m_\sigma = 1$, denn andernfalls wäre $\overline{\zeta}^{m_\sigma - 1} = 1$ im Widerspruch dazu, daß m die Ordnung von $\overline{\zeta}$ ist. Es folgt $\sigma(\zeta) = \zeta$ und also $\sigma = \mathrm{id}$, da $L = F(\zeta)$ gilt. Der Homomorphismus

$$G(L/F) \longrightarrow G(\ell/\mathbb{F}_q), \; \sigma \longmapsto \overline{\sigma},$$

ist also injektiv. Da zusätzlich

$$|G(\ell/\mathbb{F}_q)| = \dim_{\mathbb{F}_q} \ell \underset{12.7}{\leq} \dim_F L = |G(L/F)|$$

gilt, ist er auch surjektiv. Es folgt (iii). ✓

„(iii) $\Longrightarrow$ (i)“: Es ist

$$ef \underset{12.12}{=} \dim_F L \underset{L \text{ gal.}}{=} |G(L/F)| \underset{(iii)}{=} |G(\ell/\mathbb{F}_q)| = f$$

und also $e = 1$.

„(i) $\Longrightarrow$ (ii)“: Ist L unverzweigt über F, so gilt

$$f = \dim_{\mathbb{F}_q} \ell \underset{12.12}{=} \dim_F L =: n\,.$$

Es folgt $|\ell| = q^n$. Sei $m := q^n - 1$. Dann zerfällt das Polynom $X^m - 1$ in $\ell[X]$ in paarweise verschiedene Linearfaktoren, vgl. Algebra 14.4, und also auch in $L[X]$ nach dem Hensellemma 12.1. Es folgt $L' \subset L$, wobei L' Zerfällungskörper von $X^m - 1 \in F[X]$ ist. Wie in (ii) $\Longrightarrow$ (iii) gilt $\mathbb{F}_{q^n} \hookrightarrow \ell'$ für den Restklassenkörper ℓ' von L' und also

$$\dim_F L = n = \dim_{\mathbb{F}_q} \mathbb{F}_{q^n} \leq \dim_{\mathbb{F}_q} \ell' \underset{12.7}{\leq} \dim_F L'\,.$$

Es folgt $L = L'$.

□

13.4 Der Frobeniusautomorphismus

Sei F ein lokaler Körper mit Restklassenkörper $\mathbb{F}_q$.

Korollar. *Zu jedem $n \in \mathbb{N}$ gibt es bis auf Isomorphie genau einen unverzweigten Körper F_n vom Grad n über F. Es ist dies der Körper $F_n := F(\zeta)$ mit einer primitiven $(q^n - 1)$-ten Einheitswurzel ζ. Insbesondere ist F_n ein lokaler Körper, der galoissch mit zyklischer Galoisgruppe über F ist.*

Beweis. Ist $p \in F[X]$ das Minimalpolynom von ζ, so folgt $p \in \Lambda_F[X]$ nach 13.2 und also

$$\dim_F F_n = \operatorname{grad} p = \operatorname{grad} \overline{p} = \dim_{\mathbb{F}_q} \mathbb{F}_q(\zeta) = n\,.$$

Da der Zerfällungskörper von $X^{q^n-1} - 1$ bis auf Isomorphie eindeutig ist (Algebra 13.4) und die Galoisgruppe $G(\mathbb{F}_{q^n}/\mathbb{F}_q)$ zyklisch ist (Algebra 16.7), folgt das Korollar aus 13.3 und 12.6.5, 12.7. □

Definition. Der F-Automorphismus $\varphi_n \colon F_n \longrightarrow F_n$, der den $\mathbb{F}_q$-Automorphismus $\ell \longrightarrow \ell$, $x \longmapsto x^q$, induziert, heißt *Frobeniusautomorphismus von* F_n .

Bemerkung. Die Galoisgruppe $G(F_n/F)$ wird von φ_n erzeugt, vgl. 13.3 und Algebra 16.7.

13.5 Normensatz

Satz. *Sei F ein lokaler Körper, und sei L eine unverzweigte Körpererweiterung von F vom Grad $n < \infty$. Dann ist jede Einheit $u \in \Lambda_F^*$ die Norm einer Einheit $z \in \Lambda_L^*$.*

Beweis. Wie zuvor ist Λ_L bzw. Λ_F der Bewertungsring von L bzw. F und ℓ bzw. $\mathbb{F}_q$ der Restklassenkörper von L bzw. F.
Wähle ein Primelement $\pi \in F^*$. Da L unverzweigt über F ist, ist π auch Primelement über L^*, und die diskrete Bewertung $v_F \colon F^* \twoheadrightarrow \mathbb{Z}^+$ setzt sich zu einer diskreten Bewertung $v_L \colon L^* \twoheadrightarrow \mathbb{Z}^+$ fort, vgl. 12.6. Es folgt $\mathbb{F}_q = \Lambda_F/\Lambda_F\pi$ und $\ell = \Lambda_L/\Lambda_L\pi$ nach 11.3.
Für $x \in L$ sei $\overline{x}$ die Restklasse von x in ℓ. Die Norm $N_{\ell/\mathbb{F}_q} \colon \ell \longrightarrow \mathbb{F}_q$ ist nach 10.7.2 surjektiv. Es gibt also ein $z_1 \in \Lambda_L^*$ mit $\overline{N_{L/F}(z_1)} \underset{13.3}{=} N_{\ell/\mathbb{F}_q}(\overline{z_1}) = \overline{u}$. Hieraus folgt

$$\text{(I)} \qquad uN_{L/F}(z_1)^{-1} = 1 + a_1\pi \text{ mit einem } a_1 \in \Lambda_F\,.$$

Nach 13.3 gibt es ein $\varphi \in G(L/F)$ mit $G(L/F) = \langle \varphi \mid \varphi^n = \mathrm{id} \rangle$ und $G(\ell/\mathbb{F}_q) = \langle \overline{\varphi} \mid \overline{\varphi}^{\,n} = \mathrm{id} \rangle$. Da die Spur

$$S_{\ell/\mathbb{F}_q} \colon \ell \longrightarrow \mathbb{F}_q\,,\ y \longmapsto \sum_{i=0}^{n-1} \overline{\varphi}^{\,i}(y)\,,$$

surjektiv ist (vgl. Algebra 19.8), gibt es ein $\alpha_1 \in \Lambda_L$ mit

$$\overline{S_{L/F}(\alpha_1)} \underset{13.3}{=} S_{\ell/\mathbb{F}_q}(\overline{\alpha_1}) = \overline{a_1}\,,$$

also mit

$$\text{(I')} \qquad S_{L/F}(\alpha_1) \equiv a_1 \bmod \Lambda_F\pi\,.$$

Es folgt

$$\begin{aligned} N_{L/F}(1+\alpha_1\pi) &= \prod_{i=0}^{n-1} \varphi^i(1+\alpha_1\pi) \\ &= \prod_{i=0}^{n-1}(1+\varphi^i(\alpha_1)\pi)\,, && \text{da } \pi \in F \\ &\equiv 1 + S_{L/F}(\alpha_1)\pi \bmod \Lambda_F\pi^2 \\ &= 1 + a_1\pi \bmod \Lambda_F\pi^2 \\ &= uN_{L/F}(z_1)^{-1} \bmod \Lambda_F\pi^2 && \text{nach (I).} \end{aligned}$$

Für $z_2 := z_1(1+\alpha_1\pi)$ folgt

$$N_{L/F}(z_2) \equiv u \bmod \Lambda_F\pi^2 \quad \text{und} \quad z_2 \equiv z_1 \bmod \Lambda_L\pi\,.$$

Daraus folgt

(II) $$uN_{L/F}(z_2)^{-1} = 1 + a_2\pi^2 \text{ mit einem } a_2 \in \Lambda_F\,.$$

Es ist $z_2 \in \Lambda_L^*$, denn $z_1 \in \Lambda_L^*$ und $v_L(1+\alpha_1\pi) = \mathrm{Min}(0, \underbrace{v_L(\alpha_1\pi)}_{>0}) = 0$ nach 11.2 (v). Wähle $\alpha_2 \in \Lambda_L^*$ mit

(II') $$S_{L/F}(\alpha_2) \equiv a_2 \bmod \Lambda_F\pi\,.$$

Dann folgt analog

$$\begin{aligned} N_{L/F}(1+\alpha_2\pi^2) &\equiv 1 + a_2\pi^2 \bmod \Lambda_F\pi^3 && \text{nach (II')} \\ &= uN_{L/F}(z_2)^{-1} \bmod \Lambda_F\pi^3 && \text{nach (II)} \end{aligned}$$

Für $z_3 := z_2(1+\alpha_2\pi^2)$ folgt

$$N_{L/F}(z_3) \equiv u \bmod \Lambda_F\pi^3 \quad \text{und} \quad z_3 \equiv z_2 \bmod \Lambda_L\pi^2\,,$$

und es ist $z_3 \in \Lambda_L^*$, da $z_2 \in \Lambda_L^*$.
So fortfahrend erhält man eine Folge $(z_m \in \Lambda_L^*)_{m\in\mathbb{N}}$ mit $N_{L/F}(z_m) \equiv u \bmod \Lambda_F\pi^m$ und $z_{m+1} \equiv z_m \bmod \Lambda_L\pi^m$. Da L nach 13.4 vollständig ist, existiert $z := \lim\limits_{m\to\infty} z_m$ in Λ_L^*, und es folgt $N_{L/F}(z) = u$, da die Norm stetig ist, vgl. Aufgabe 51. □

13.6 Relative Brauergruppen

Korollar. *Seien F ein lokaler Körper, π ein Primelement bezüglich der diskreten Bewertung $v_F\colon F^* \twoheadrightarrow \mathbb{Z}^+$ und φ_n der Frobeniusautomorphismus des unverzweigten Körpers F_n aus 13.4 für $n \in \mathbb{N}$. Dann hat man einen surjektiven Homomorphismus*

$$\theta\colon \mathbb{Z}^+ \longrightarrow \mathrm{Br}(F_n/F)\,,\ m \longmapsto [(F_n, \varphi_n, \pi^m)]\,,$$

und dieser induziert einen Isomorphismus

$$\theta_n\colon \mathbb{Z}/n\mathbb{Z} \xrightarrow{\ \sim\ } \mathrm{Br}(F_n/F)\,.$$

Beweis. Nach 10.4 ist θ ein Homomorphismus. Sei A eine Azumaya-Algebra über F, die von F_n zerfällt wird. Dann gilt $A \sim (F_n, \varphi_n, a)$ mit einem $a \in F^*$ nach 10.6. Nach 11.3 ist $\boxed{a = u\pi^m}$ mit einem $u \in \Lambda_F^*$ und $m = v_F(a) \in \mathbb{Z}$. Es folgt $A \underset{10.4}{\sim} (F_n, \varphi_n, u) \otimes_F (F_n, \varphi_n, \pi^m) \underset{10.5}{\sim} (F_n, \varphi_n, \pi^m)$, da $u \in N_{F_n/F}(F_n^*)$ nach 13.5. Also ist θ surjektiv.
θ_n ist wohldefiniert, da $n \underset{13.4}{=} \dim_F F_n \underset{10.3}{=} \mathrm{grad}(F_n, \varphi_n, \pi^m)\ \forall m \in \mathbb{N}$ und $\exp \underset{9.3}{\mid} \mathrm{ind} \underset{3.10}{\mid} \mathrm{grad}$ gelten.
Sei $(F_n, \varphi_n, \pi^m) \simeq (F_n, \varphi_n, 1)$. Dann ist $\pi^m = N_{F_n/F}(y)$ mit einem $y \in F_n^*$ nach 10.5. Da F_n unverzweigt ist, folgt

$$\begin{aligned} n v_{F_n}(y) &= v_F(N_{F_n/F}(y)) && \text{nach 12.4, 12.6} \\ &= v_F(\pi^m) = m\,, \end{aligned}$$

und also $m \equiv 0 \bmod n\mathbb{Z}$. Also ist θ_n injektiv. □

13.7 Existenz eines unverzweigten Zerfällungskörpers

Seien F ein lokaler Körper mit Restklassenkörper $\mathbb{F}_q$ und D ein endlichdimensionaler Schiefkörper über F. Jedes $x \in D^*$ erzeugt dann einen Körper $F(x)$ nach 5.3.

Lemma. *Es gebe einen Teilkörper $F(x)$ von D mit Restklassengrad $f_x > 1$. Dann besitzt D einen über F unverzweigten Teilkörper $\neq F$.*

Beweis. Sei $L := F(x)$, und sei ζ eine primitive m-te Einheitswurzel über F mit $m := q^{f_x} - 1$. Dann ist der Körper $F(\zeta)$ unverzweigt über F, und es gilt $\dim_F F(\zeta) \underset{13.4}{=} f_x > 1$.
Zeige nun, daß $\zeta \in L$ gilt. Dann folgt $F \neq F(\zeta) \subset L \subset D$ und damit das Lemma.

Sei $p \in L[X]$ das Minimalpolynom von ζ über L. Dann ist p ein normierter, irreduzibler Faktor von $X^m - 1 \in L[X]$ und also $p \in \Lambda_L[X]$ nach 13.2. Nach Voraussetzung gilt $\dim_{\mathbb{F}_q} \ell = f_x$ für den Restklassenkörper ℓ von L.
Also zerfällt $X^m - 1$ und damit $\overline{p}$ in $\ell[X]$ in paarweise verschiedene Linearfaktoren. Nach dem Hensellemma 12.1 folgt $p = X - \zeta \in L[X]$ und damit $\zeta \in L$. □

Satz. *Sei D zentral über F. Dann besitzt D einen maximalen Teilkörper L, der unverzweigt über F ist, und es gilt*

$$\dim_F D = (\dim_F L)^2 .$$

Beweis. Ist $F = D$, so erfüllt $F = L$ die Behauptung. Sei $F \neq D$.
Annahme: D enthält keinen über F unverzweigten Körper M mit $M \neq F$. Nach dem Lemma hat dann die Körpererweiterung $F(x)$ für jedes $x \in D^*$ den Restklassengrad $f_x = 1$. Sei Λ_D der Bewertungsring von D, und sei π_D ein Primelement von D, wie in 12.6 definiert. Wir zeigen durch Induktion, daß es zu jedem $x \in \Lambda_D$ passende Elemente $c_0, \ldots, c_{n-1} \in \Lambda_F$ mit

$$(*) \qquad x \equiv c_0 + c_1\pi_D + \cdots + c_{n-1}\pi_D^{n-1} \bmod \Lambda_D \pi_D^n$$

gibt. Für $n = 1$ folgt $(*)$, da $f_x = 1$ gilt. Es gelte $(*)$ für n. Dann ist

$$x = c_0 + c_1\pi_D + \cdots + c_{n-1}\pi_D^{n-1} + y\pi_D^n \text{ mit } y \in \Lambda_D .$$

Da $f_y = 1$ ist, folgt $y \equiv c_n \bmod \Lambda_D\pi_D$ für $c_n \in \Lambda_F$ und also

$$x \equiv c_0 + \cdots + c_n\pi^n \bmod \Lambda_D\pi_D^{n+1} .$$

Da $F(\pi_D)$ nach 12.4 vollständig ist, folgt $\Lambda_D \subset F(\pi_D)$. Da $x = u_x\pi_D^{n_x}$ mit $n_x \in \mathbb{Z}$ und $u_x \in \Lambda_D^*$ gilt (vgl. 12.6), folgt $D \subset F(\pi_D)$. Also ist D kommutativ im Widerspruch zu $D \neq F = \mathcal{Z}(D)$.
Es sei nun L ein Teilkörper von D, der F enthält und der maximal ist bezüglich der Eigenschaft: L ist unverzweigt über F.
Der Zentralisator $\mathcal{Z}_D(L)$ ist ein zentraler Schiefkörper über L nach 5.2 und 4.6. Wäre $L \neq \mathcal{Z}_D(L)$, so gäbe es nach dem oben gezeigten einen in $\mathcal{Z}_D(L) \subset D$ enthaltenen, über L unverzweigten Körper $M \neq L$, im Widerspruch zur Maximalität von L. Es folgt $L = \mathcal{Z}_D(L)$ und also $\dim_F D = (\dim_F L)^2$ nach Satz 4.7. □

Folgerung. *Jede Azumaya-Algebra A über F besitzt einen unverzweigten Zerfällungskörper L mit $\dim_F L = \mathrm{ind}_F A$.*
Ferner gilt $\mathrm{Br}(F) = \bigcup_{n\in\mathbb{N}} (F_n/F)$, wobei F_n durch 13.4 gegeben ist.

Beweis. Es ist $A \underset{3.8}{\sim} D$ mit einem zentralen Schiefkörper D über F. Nach dem Satz enthält D einen unverzweigten Körper L mit $\operatorname{ind}_F A = \sqrt{\dim_F D} = \dim_F L$. Es ist L Zerfällungskörper von D nach 5.9, und es gilt $L \simeq F_n$ mit $n = \dim_F L$ nach 13.4. □

13.8 Zyklizitätssatz

Satz. *Jede Azumaya-Algebra A über einem lokalen Körper F ist zyklisch.*

Beweis. Nach Folgerung 13.7 besitzt A einen unverzweigten Zerfällungskörper F_n mit $n = \dim_F F_n = \operatorname{ind}_F A$. Für $r := \operatorname{grad}_F A$ gilt $n \mid r$ nach 3.10, und daher $F_n \underset{13.4}{\subset} F_r$.
Also ist auch F_r Zerfällungskörper von A, und es folgt $A \sim (F_r, \varphi_r, a)$ mit einem $a \in F^*$ nach 13.6. Da r so gewählt ist, daß beide Algebren dieselbe Dimension über F haben, folgt $A \simeq (F_r, \varphi_r, a)$ nach Folgerung 3.4. □

13.9 Die Gruppe $\mathbb{Q}/\mathbb{Z}$

Mit $\mathbb{Q}/\mathbb{Z}$ ist die additive Gruppe $\mathbb{Q}^+/\mathbb{Z}^+$ gemeint. Es ist $\mathbb{Q}/\mathbb{Z}$ isomorph zur Gruppe μ aller Einheitswurzeln in $\mathbb{C}$, denn die komplexe Exponentialfunktion

$$\mathbb{C}^+ \longrightarrow \mathbb{C}^+, \; z \longmapsto e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!},$$

hat als Kern die Untergruppe $\{2\pi i m \mid m \in \mathbb{Z}\} \subset \mathbb{C}^+$, und also hat man einen surjektiven Homomorphismus

$$\mathbb{Q}^+ \longrightarrow \mu, \; a \longmapsto e^{2\pi i a},$$

mit $\mathbb{Z}^+$ als Kern.

Lemma. *(a) Die Multiplikation mit n induziert einen Gruppenisomorphismus*
$\frac{1}{n}\mathbb{Z}/\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$ *für jedes $n \in \mathbb{N}$.*

(b) Es ist $\mathbb{Q}/\mathbb{Z} = \bigcup_{n \in \mathbb{N}} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Beweis. klar. □

13.10 Die Brauergruppe eines lokalen Körpers

Seien F ein lokaler Körper, φ_n der Frobeniusautomorphismus des unverzweigten Körpers F_n aus 13.4 und π ein Primelement von F.

Satz. *Es gibt eine Gruppenisomorphie*

$$\psi\colon \mathbb{Q}/\mathbb{Z} \xrightarrow{\sim} \mathrm{Br}(F) \text{ mit } \psi\left(\frac{m}{n}+\mathbb{Z}\right) = [(F_n, \varphi_n, \pi^m)]$$

für $n \in \mathbb{N}$ *und* $m \in \mathbb{Z}$ *mit* $0 \le m < n$ *.*

Beweis. Jedes $a \in \mathbb{Q}^*$ läßt sich als gekürzter Bruch $a = \frac{s}{n}$ mit einem $n \in \mathbb{N}$ und einem $s \in \mathbb{Z}$ schreiben. Es ist $s = jn+m$ mit $j \in \mathbb{Z}$ und $0 \le m < n$ und also $a = \frac{jn+m}{n} = \frac{m}{n} + j$. Daher gilt $a + \mathbb{Z} = \frac{m}{n} + \mathbb{Z}$ mit $0 \le m < n$. Nach dem Inflationssatz 10.8 gilt

$$(F_n, \varphi_n, \pi^m) \sim (F_{nr}, \varphi_{nr}, \pi^{mr}) \qquad \forall\, n, r \in \mathbb{N}\,.$$

Also ist ψ wohldefiniert, und man hat ein kommutatives Diagramm

$$\begin{tikzcd}
\frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r, "\sim", "\cdot n"'] \arrow[d, hook] & \mathbb{Z}/n\mathbb{Z} \arrow[r, "\sim", "\theta_n"'] \arrow[d, hook, "\cdot r"] & \mathrm{Br}(F_n/F) \arrow[d, hook] \\
\frac{1}{nr}\mathbb{Z}/\mathbb{Z} \arrow[r, "\sim", "\cdot nr"'] & \mathbb{Z}/nr\mathbb{Z} \arrow[r, "\sim", "\theta_{nr}"'] & \mathrm{Br}(F_{nr}/F)\,,
\end{tikzcd}$$

wobei $\theta_n\colon (m + n\mathbb{Z}) \longmapsto (F_n, \varphi, \pi^m)$ der Isomorphismus aus 13.6 ist. Da $\mathbb{Q}/\mathbb{Z} = \bigcup\limits_{n\in\mathbb{N}} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ und $\mathrm{Br}(F) = \bigcup\limits_{n\in\mathbb{N}} \mathrm{Br}(F_n/F)$ nach 13.9 und Korollar 13.7 gilt, folgt die Behauptung. □

13.11 $\exp A = \operatorname{ind} A$

Korollar. *Für jede Azumaya-Algebra A über einem lokalen Körper F gilt*

$$\boxed{\exp_F A = \operatorname{ind}_F A}\,.$$

Beweis. Nach 13.10 können wir $\psi^{-1}([A])$ als $\frac{m}{n} + \mathbb{Z}$ mit $0 \le m < n$ und $\mathrm{ggT}(m,n) = 1$ schreiben, und es ist $[A] = [(F_n, \varphi_n, \pi^m)]$.
Da m teilerfremd zu n ist, folgt

$$\exp_F(F_n, \varphi_n, \pi^m) \underset{13.6}{=} n \underset{10.3}{=} \mathrm{grad}_F(F_n, \varphi_n, \pi^m)\,,$$

und da $\exp \underset{9.3}{\le} \operatorname{ind} \underset{3.10}{\le} \mathrm{grad}$ gilt, folgt $\exp_F A = \operatorname{ind}_F A$. □

13.12 Bemerkung zur Brauergruppe eines Zahlkörpers

Sei K ein Zahlkörper, das ist eine endliche Körpererweiterung von $\mathbb{Q}$. Dann gibt es genau $\dim_{\mathbb{Q}} K$ verschiedene Einbettungen $\sigma\colon K \hookrightarrow \mathbb{C}$ nach Algebra 13.1 und Satz 11.4. Zu jedem σ erhält man einen (archimedischen) Absolutbetrag $\nu_\sigma\colon K \longrightarrow \mathbb{R}_{\geq 0}$, $a \longmapsto |\sigma(a)|$. Man nennt ν_σ *reell*, falls $\sigma(K) \subset \mathbb{R}$ gilt und andernfalls *komplex*. Ferner besitzt K noch die diskreten Bewertungen $\nu_{\mathfrak{p}}$ für jedes Primideal $\mathfrak{p}$ aus dem Ganzheitsring $\mathfrak{o}_K$, vgl. 11.5.4. Schreibe einheitlich ν für ν_σ oder $\nu_{\mathfrak{p}}$. Sei K_ν die Vervollständigung von K bezüglich ν (vgl. 11.8). Es gelten dann:

- Ist ν diskret, so ist $\psi^{-1}\colon \operatorname{Br}(K_\nu) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$ ein Isomorphismus nach 13.10. Man nennt das Element $\psi^{-1}([A]) \in \mathbb{Q}/\mathbb{Z}$ die *Hasse-Invariante* einer Azumaya-Algebra A über K_ν und schreibt $\operatorname{inv}_{K_\nu} A$.
- Ist ν reell, so ist $K_\nu = \mathbb{R}$ und also $\operatorname{Br}(K_\nu) \underset{6.6}{\simeq} \mathbb{Z}/2\mathbb{Z} \underset{13.10}{\simeq} \frac{1}{2}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$.
- Ist ν komplex, so ist $K_\nu = \mathbb{C}$ und also $\operatorname{Br}(K_\nu) \underset{3.6}{=} \{0\} \subset \mathbb{Q}/\mathbb{Z}$.

Die Einbettungen $K \hookrightarrow K_\nu$ induzieren einen Gruppenhomomorphismus $\operatorname{Br}(K) \longrightarrow \bigoplus_\nu \operatorname{Br}(K_\nu)$, und man hat eine exakte Gruppensequenz

$$0 \longrightarrow \operatorname{Br}(K) \longrightarrow \bigoplus_\nu \operatorname{Br}(K_\nu) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$
$$([A_\nu]_\nu) \longmapsto \sum_\nu a_\nu\,,$$

wobei a_ν das Bild von $[A_\nu]$ unter dem Monomorphismus $\operatorname{Br}(K_\nu) \hookrightarrow \mathbb{Q}/\mathbb{Z}$ ist. Für einen Beweis vgl. z.B. Lorenz, Algebraische Zahlentheorie.

Teil IV
Normresthomomorphismen

14 Normrestalgebren

Sei $n \in \mathbb{N}$, und sei K ein Körper, der eine primitive n-te Einheitswurzel ζ enthalte. Insbesondere gelte $\operatorname{char} K \nmid n$.

14.1 Erzeugende und Relationen

Für $a, b \in K^*$ ist die *Normrestalgebra* (a, b, ζ) definiert als eine K-Algebra mit zwei Erzeugenden u, v, welche die Relationen

$$u^n = a\,,\ v^n = b \text{ und } vu = \zeta uv \tag{2}$$

erfüllen. Es gilt dann $u, v \in (a, b, \zeta)^*$ und also

$$\boxed{vuv^{-1} = \zeta u} \quad \text{sowie} \quad \boxed{uvu^{-1} = \zeta^{-1} v}\,. \tag{3}$$

14.2 Basis und Dimension

Satz. *Die Elemente $u^i v^j$ mit $0 \le i, j \le n-1$ bilden eine Basis der Normrestalgebra $A := (a, b, \zeta)$ über K. Insbesondere gilt $\dim_K A = n^2$, und A ist bis auf Isomorphie durch die Relationen (2) eindeutig bestimmt.*

Beweis. Die Elemente $u^i v^j$ bilden offenbar ein Erzeugendensystem von A als K-Vektorraum. Um zu zeigen, daß sie linear unabhängig sind, definieren wir K-Algebraautomorphismen

$$g_u\,, g_v \colon A \longrightarrow A \quad \text{durch} \quad g_u(x) = uxu^{-1} \text{ und } g_v(x) = vxv^{-1}\ \forall\, x \in A\,.$$

Sei $\sum\limits_{i,j=0}^{n-1} a_{ij} u^i v^j = 0$ mit $a_{ij} \in K$. Für $w_i := \sum\limits_{j=0}^{n-1} a_{ij} u^i v^j$ folgt dann

$$\begin{aligned} g_v(w_i) &= \sum_{j=0}^{n-1} a_{ij} (vuv^{-1})^i v v^j v^{-1} \\ &\underset{(2)}{=} \sum_{j=0}^{n-1} a_{ij} \zeta^i u^i v^j = \zeta^i w_i\,. \end{aligned}$$

Also sind diejenigen w_i , die ungleich Null sind, linear unabhängig, da sie zu verschiedenen Eigenwerten von g_v gehören (AGLA 9.6).
Da $\sum_{i=0}^{n-1} w_i = 0$ gilt, folgt $w_i = 0\;\forall\, i = 0, \ldots, n-1$. Es ist

$$\begin{aligned} g_u(u^i v^j) &= u u^i u^{-1} (u v u^{-1})^j \\ &= u^i \zeta^{-j} v^j = \zeta^{-j} u^i v^j \,. \end{aligned}$$

Da $u^i v^j \neq 0\;\forall\, i, j$ gilt, sind die Vektoren $u^i, u^i v, \ldots, u^i v^{n-1}$ für festes $i \in \{0, \ldots, n-1\}$ nach AGLA 9.6 linear unabhängig. Da $\sum\limits_{j=0}^{n-1} a_{ij} u^i v^j = w_i = 0$ gilt, folgt $a_{ij} = 0\;\;\forall\, i, j \in \{0, 1 \ldots, n-1\}$.
Es folgt $\dim_K A = n^2$ und damit auch die Eindeutigkeitsaussage. □

14.3 Realisierung durch Matrizen

Die Normrestalgebra (a, b, ζ) existiert tatsächlich, denn man kann sie als Unterring von $\mathrm{M}_{n\times n}(K(\sqrt[n]{b}))$ realisieren. Sei $L = K(y)$ mit $y^n = b$. Setze

$$u = \begin{pmatrix} 0 & \ldots & 0 & a \\ 1 & \ddots & & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} y & & & \\ & \zeta y & & \\ & & \ddots & \\ & & & \zeta^{n-1} y \end{pmatrix} = v \text{ in } \mathrm{M}_{n\times n}(L)\,.$$

Dann folgt $u^n = a$, $v^n = b$ und $vu = \zeta uv$.

Bemerkung. Ist $b = c^n$ mit einem $c \in K^*$, so gilt $(a, b, \zeta) \simeq \mathrm{M}_{n\times n}(K)$.

Beweis. In der obigen Realisierung kann man $y = c$ nehmen. Aus 14.2 folgt dann, daß (a, b, ζ) isomorph zu einer n^2-dimensionalen Unteralgebra von $\mathrm{M}_{n\times n}(K)$ ist. □

14.4 Abhängigkeit von der Einheitswurzel

Lemma. *(i)* $\boxed{\mathrm{ggT}(r, n) = 1} \implies \boxed{(a, b, \zeta) \simeq (a^r, b, \zeta^r)}$

(ii) $\boxed{d \mid n} \implies \boxed{(a, b^d, \zeta) \sim (a, b, \zeta^d)}$

Beweis. (i) Ist (a, b, ζ) durch die Regeln $u^n = a$, $v^n = b$ und $uv = \zeta vu$ gegeben, so folgt $u^{rn} = a^r$, $v^n = b$ und $vu^r = \zeta^r u^r v$.
Da $\mathrm{ggT}(r, n) = 1$ gilt, ist ζ^r eine primitive n-te Einheitswurzel (vgl. Algebra 17.3), und 14.2 ergibt, daß (a^r, b, ζ^r) eine n^2-dimensionale K-Unteralgebra von (a, b, ζ) ist. ✓

(ii) Es ist $n = dm$ mit einem $m \in \mathbb{N}$. Sei $A := (a, b, \zeta^d)$. Dann ist A durch die Regeln $u^m = a$, $v^m = b$ und $vu = \zeta^d uv$ gegeben, und es gilt $\dim_K A = n^2$ nach 14.2.
Definiere $U, V \in \mathrm{M}_{d\times d}(A)$ durch

$$U = \begin{pmatrix} 0 & & & u \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix} \quad \text{und} \quad V = \begin{pmatrix} v & & & 0 \\ & \zeta v & & \\ & & \ddots & \\ 0 & & & \zeta^{d-1} v \end{pmatrix}.$$

Dann gelten $U^n = (U^d)^m = u^m = a$ und $V^n = v^n = v^{md} = b^d$ sowie $VU = \zeta UV$. Die von U und V erzeugte K-Unteralgebra von $\mathrm{M}_{d\times d}(A)$ ist also isomorph zu (a, b^d, ζ). Da $\dim_K(a, b^d, \zeta) = n^2 = d^2m^2 = \dim_K \mathrm{M}_{d\times d}(A)$ gilt, folgt

$$(a, b^s, \zeta) \simeq A \otimes_K \mathrm{M}_{d\times d}(K).$$

□

14.5 Weitere Eigenschaften

Satz. *Sei ζ eine primitive n-te Einheitswurzel, und seien $a, b \in K^*$. Für die Normrestalgebra (a, b, ζ) gelten*

(i) (a, b, ζ) *ist eine Azumaya-Algebra über* K.

(ii) (a, b, ζ) *ist ähnlich zu der zyklischen K-Algebra* $(K(\sqrt[n]{b}), \sigma, a)$ *mit passendem* $\sigma \in G(K(\sqrt[n]{b})/K)$.

(iii) $(a, b, \zeta) \otimes_K (a', b, \zeta) \sim (aa', b, \zeta)\ \forall\, a' \in K^*$ *und*
$(a, b, \zeta) \otimes_K (a, b', \zeta) \sim (a, bb', \zeta)\ \forall\, b' \in K^*$ *(„Bilinearität“)*

(iv) $(a, b, \zeta) \sim K \iff a \in N_{L/K}(L^*)$ *mit* $L = K(\sqrt[n]{b}) \iff b \in N_{M/K}(M^*)$ *mit* $M = K(\sqrt[n]{a})$.

(v) Ist $a + b = 1$, *so ist* $(a, b, \zeta) \sim K$. *(„Steinberg-Relation“)*

(vi) $(a, -a, \zeta) \sim K$.

(vii) $(a, b, \zeta) \simeq (-\frac{a}{b}, a + b, \zeta)$ *(„Witt-Relation“)*

(viii) $(a, b, \zeta) \simeq (b, a, \zeta)^{\mathrm{op}}$ *(„Schiefsymmetrie“)*

Beweis. Sei $A := (a, b, \zeta)$. Dann ist $\dim_K A = n^2$.

(i) Es gilt $K \subset \mathcal{Z}(A)$. Sei $x \in \mathcal{Z}(A)$. Zu zeigen: $x \in K$. Es ist

$$\begin{aligned} x &= \sum_{i,j=0}^{n-1} a_{ij} u^i v^j && \text{mit eindeutig bestimmten } a_{ij} \in K \text{ nach 14.2.} \\ &= v x v^{-1}, && \text{da } x \in \mathcal{Z}(A) \\ &= \sum_{i,j=0}^{n-1} a_{ij} \zeta^i u^i v^j && \text{nach (2).} \end{aligned}$$

Koeffizientenvergleich ergibt $a_{ij} = 0 \;\forall\, i = 1, \ldots, n{-}1$ und $j = 0, \ldots, n-1$. Es folgt

$$\sum_{j=0}^{n-1} a_{0j} v^j = x \underset{x \,\in\, \mathcal{Z}(A)}{=} u x u^{-1} \underset{(2)}{=} \sum_{j=0}^{n-1} a_{0j} \zeta^{-j} v^j \,.$$

Koeffizientenvergleich ergibt $a_{0j} = 0 \;\forall\, j = 1, \ldots, n-1$ und daher $x = a_{00} \in K$. Also ist A zentral.
Sei $I \neq (1)$ ein zweiseitiges Ideal in A. Dann ist A/I ebenfalls eine n^2-dimensionale K-Algebra nach 14.2. Es folgt $I = (0)$. Also ist A einfach.

(ii) Sei $L = K(y)$ mit $y^n = b$ und $\dim_K L =: m$. Dann ist

$$\boxed{y^m =: c \in K^*} \quad \text{und} \quad \boxed{b = c^d \text{ mit } d := \frac{n}{m}}\,.$$

Es folgt $K[X]/(X^m{-}c) \simeq K(\sqrt[n]{c}) = L$, und L ist ein galoisscher Körper über K mit zyklischer Galoisgruppe $\langle \sigma \mid \sigma^m = \mathrm{id} \rangle$ nach Algebra 18.3(i). Wähle das erzeugende Element σ so, daß $\sigma(y) = \zeta^{-d} y$ gilt. Die zyklische Algebra (L, σ, a) ist durch die Regeln

$$\boxed{u^m = a} \quad \text{und} \quad \boxed{ux = \sigma(x) u \;\forall\, x \in L}$$

festgelegt, vgl. 10.3. Insbesondere folgt $uy = \zeta^{-d} yu$ $(\sigma(y) = \zeta^{-d} y)$ und also $yu = \zeta^d uy$. Die Normrestalgebra (a, c, ζ^d) ist durch die Regeln

$$\boxed{w^m = a\,, \quad v^m = c \quad \text{und} \quad vw = \zeta^d wv}$$

festgelegt, vgl. 14.2. Man erhält also eine K-Algebraisomorphie

$$\boxed{(L, \sigma, a) \xrightarrow{\;\sim\;} (a, c, \zeta^d)}$$

durch die Zuordnung $u \longmapsto w$, $y \longmapsto v$. Da $(a, c, \zeta^d) \sim (a, c^d, \zeta)$ nach 14.4 (ii) gilt, folgt (ii).

(iii) Da sich die zyklische Algebra (L, σ, a) in a multiplikativ verhält (vgl. 10.4), folgt die erste Beziehung aus (ii). Offenbar gilt $(a, b, \zeta) \simeq (b, a, \zeta^{-1})$ nach 14.2. Daher folgt analog die Multiplikativität in b.

(iv) Läßt sich analog wie (iii) auf die entsprechenden Beziehungen 10.5 oder 10.6 für zyklische Algebren zurückführen.

(v) Sei $L = K(y)$ mit $y^n = b$ und $\dim_K L =: m$. Sei $\sigma\colon L \longrightarrow L$ das durch $\sigma(y) = \zeta^d y$ mit $d = \frac{n}{m}$ definierte erzeugende Element von $G(L/K)$. Es ist

$$X^n - b = \prod_{i=0}^{n-1} (X - \zeta^i y) \text{ in } L[X]\,. \tag{4}$$

Setze in diese Gleichung $X = 1$ ein. Dann folgt

$$\begin{aligned} a \underset{\text{Vor.}}{=} 1 - b &= \prod_{i=0}^{n-1} (1 - \zeta^i y) \\ &= \prod_{j=0}^{m-1} \prod_{r=0}^{d-1} (1 - \zeta^{jd+r} y) = \prod_{j=0}^{m-1} \sigma^j(x) \\ &= N_{L/K}(x) \text{ mit } x = \prod_{r=0}^{d-1} (1 - \zeta^r y)\,. \end{aligned}$$

Also folgt $(a, b, \zeta) \sim K$ nach (iv).

(vi) Setze in (4) $X = 0$ ein. Dann folgt analog

$$a \underset{\text{Vor.}}{=} -b = N_{L/K}(z) \text{ mit } z = \prod_{r=0}^{d-1} -\zeta^r y\,.$$

und also $(a, -a, \zeta) \sim K$ nach (iv).

(vii) +(viii) Übung.

□

14.6 Die multiplikative Gruppe

Sei K ein Körper. Die Gruppe K^* ist ein $\mathbb{Z}$-Modul vermöge

$$m \cdot a = a^m \text{ für } m \in \mathbb{Z}\,,\ a \in K^*\,,$$

und für den $\mathbb{Z}$-Modul $K^* \otimes_{\mathbb{Z}} K^*$ gelten:

$$\begin{aligned} 0 = 0 \cdot (a \otimes b) = 1 \otimes b = a \otimes 1 \text{ und} \\ -(a \otimes b) = a^{-1} \otimes b = a \otimes b^{-1}\ \forall\, a, b \in K^*\,. \end{aligned}$$

14.7 Die 2. Milnorsche K-Gruppe

Es ist $K_2(K) := (K^* \otimes_{\mathbb{Z}} K^*)/\langle a \otimes (1-a) \mid a \neq 1 \rangle$, wobei $\langle a \otimes (1-a) \mid a \neq 1 \rangle$ die von allen Elementen $a \otimes (1-a)$ mit $(1-a) \neq 0$ erzeugte Untergruppe von $K^* \otimes_{\mathbb{Z}} K^*$ sei. Mit $\{a, b\}$ sei die Restklasse von $a \otimes b$ in $K_2(K)$ bezeichnet.

Lemma. *Für $a, a', b, b' \in K^*$ gelten:*

(i) $\{a, 1-a\} = 0$ *(„Steinberg-Relation")*

(ii) $\{aa', b\} = \{a, b\} + \{a', b\}$ *und*
$\{a, bb'\} = \{a, b\} + \{a, b'\}$ *(„Bilinearität")*

(iii) $\{a, -a\} = 0$ *und* $\{a, a\} = \{a, -1\}$

(iv) $\{a, b\} = -\{b, a\}$ *(„Schiefsymmetrie")*

(v) $\{a, b\} = \left\{-\frac{a}{b}, a+b\right\}$

Beweis. (i) und (ii) folgen aus der Definition von $K_2(K)$ und des Tensorprodukts.

(iii) Da $1 - a = -a(1 - a^{-1})$ ist folgt

$$\begin{aligned} 0 &\underset{(i)}{=} \{a, 1-a\} = \{a, -a(1-a^{-1})\} \\ &\underset{(ii)}{=} \{a, -a\} + \{a, 1-a^{-1}\} \underset{14.6}{=} \{a, -a\} - \{a^{-1}, 1-a^{-1}\} \\ &\underset{(i)}{=} \{a, -a\}\,. \end{aligned}$$

Hieraus folgt

$$\begin{aligned} \{a, a\} &= \{a, (-1)(-a)\} \\ &\underset{(ii)}{=} \{a, -1\} + \{a, -a\} = \{a, -1\}\,. \end{aligned}$$

(iv) Es ist

$$\begin{aligned} 0 &\underset{(iii)}{=} \{ab, -ab\} \\ &\underset{(ii)}{=} \{a, -a\} + \{a, b\} + \{b, a\} + \{b, -b\} \\ &= \{a, b\} + \{b, a\}\,. \end{aligned}$$

□

14.8 Der Homomorphismus $R_{K,n}$

Sei K ein Körper, der eine primitive n-te Einheitswurzel ζ enthalte. Nach 14.5(iii) gibt es eine $\mathbb{Z}$-bilineare Abbildung

$$K^* \times K^* \longrightarrow \mathrm{Br}(K)\,,\ (a,b) \longmapsto [(a,b,\zeta)]\,.$$

Diese induziert einen Gruppenhomomorphismus

$$\boxed{R_{K,n}\colon k_2(K) \longrightarrow {}_n\mathrm{Br}(K)}\,,$$

wobei $k_2(K) := K_2(K)/nK_2(K)$ und

$${}_n\,\mathrm{Br}(K) := \{[A] \in \mathrm{Br}(K) \mid [A]^n = 1\}\,.$$

Dies folgt aus Bemerkung 14.3, 14.5 und der universellen Eigenschaft des Tensorprodukts.

Lemma. *Ist μ_n die Gruppe der n-ten Einheitswurzeln in K, so ist der durch $(a,b) \longmapsto (a,b,\zeta) \otimes \zeta$ induzierte Gruppenhomomorphismus*

$$k_2 \longrightarrow {}_n\mathrm{Br}(K) \otimes_{\mathbb{Z}} \mu_n$$

unabhängig von der Auswahl der primitiven n-ten Einheitswurzel ζ.

Beweis. Für $r \in \mathbb{Z}$ mit $\mathrm{ggT}(r,n) = 1$ gilt

$$\begin{aligned}
[(a,b,\zeta^r)] \otimes \zeta^r &= [(a,b,\zeta^r)]^r \otimes \zeta\,, && \text{da } \otimes = \otimes_{\mathbb{Z}} \text{ vgl. 14.6}\\
&= [(a^r,b,\zeta^r)] \otimes \zeta && \text{nach 14.5}\\
&= [(a,b,\zeta)] \otimes \zeta && \text{nach 14.4}\,.
\end{aligned}$$

□

Theorem (Merkurjev-Suslin). *$R_{K,n}$ ist bijektiv.*

15 Galoiskohomologie

Sei L eine Galoiserweiterung eines Körpers K mit endlicher Gruppe G. Dann gelten $H^1(G, L^*) = \{1\}$ nach 7.9 und $H^2(G, L^*) \simeq \mathrm{Br}(L/K)$ nach 8.3.

15.1 Hilberts Satz 90

Satz. *Ist $G = \langle\sigma\rangle$ zyklisch, so hat jedes Element $x \in L^*$ mit $N_{L/K}(x) = 1$ die Gestalt $x = \sigma(y)y^{-1}$ mit passendem $y \in L^*$.*

Beweis. Ist $N_{L/K}(x) = 1$, so ist $f\colon G \longrightarrow L^*$ mit $f(\mathrm{id}) = 1$ und $f(\sigma^i) = x\sigma(x) \cdot \ldots \cdot \sigma^{i-1}(x)$ für $i = 1, \ldots, |G| - 1$ ein 1-Kozyklus und daher nach 7.9 ein 1-Korand. Da $x = f(\sigma)$ ist, folgt die Behauptung. □

Bemerkung. Für die zweite K-Gruppe gibt es einen der Norm entsprechenden Gruppenhomomorphismus

$$c_{L/K}\colon K_2(L) \longrightarrow K_2(K)$$

für jede endliche Körpererweiterung L von K. Es gilt hierbei die sogenannte *Projektionsformel*

$$c_{L/K}(\{\alpha, b\}) = \{N_{L/K}(\alpha), b\} \qquad\qquad \forall\, \alpha \in L^*, b \in K^*.$$

Die Abbildung $c_{L/K}$ heißt *Korestriktion* oder *Transfer*. Ihre Definition ist aufwendig.

Satz (Hilbert 90 für K_2). *Sei L galoissch über K mit Gruppe $G = \langle\sigma\rangle$ der Primzahlordnung p mit $p \neq \mathrm{char}\, K$. Ist $x \in K_2(L)$ und $c_{L/K}(x) = 0$, so gibt es ein $y \in K_2(L)$ mit $x = \sigma(y) - y$.*

Beweis. Der Beweis ist sehr schwierig und tiefliegend. Hilberts Satz 90 für K_2 ist ein wesentliches Hilfsmittel beim Beweis des Theorems von Merkurjev-Suslin, daß der Normresthomomorphismus $R_{K,p}\colon k_2(K) \longrightarrow {}_p\mathrm{Br}(K)$ bijektiv ist. □

15.2 Krulltopologie

Sei K ein Körper, und sei Ω eine algebraische Körpererweiterung von K. Dann heißt Ω galoissch über K, falls $\Omega^{G_{\Omega/K}} = K$ gilt, wobei $G_{\Omega/K} := \mathrm{Aut}_K\, \Omega$ die Gruppe der K-Algebraautomorphismen von Ω und

$$\Omega^{G_{\Omega/K}} = \{x \in \Omega \mid \sigma(x) = x\ \forall\, \sigma \in G_{\Omega/K}\}$$

ist. Sei nun Ω galoissch über K. Dann versieht man die Gruppe $G_{\Omega/K}$ mit der sogenannten *Krulltopologie.*
Für jedes $\sigma \in G_{\Omega/K}$ nimmt man die Nebenklasse $\sigma G_{\Omega/L}$ als Umgebungsbasis von σ, wobei L alle endlich galoisschen Körpererweiterungen von K in Ω durchläuft.
Bezüglich der Krulltopologie von $G_{\Omega/K}$ gelten:

(i) $G_{\Omega/K}$ ist eine topologische Gruppe.

(ii) $G_{\Omega/K}$ ist kompakt und haussdorffsch.

(iii) Es gibt eine Bijektion

$$\begin{aligned} \{\text{Zwischenkörper } K \subset L \subset \Omega\} &\longrightarrow \{\text{abg. Untergruppen von } G_{\Omega/K}\} \\ L &\longmapsto G_{\Omega/L}\,. \end{aligned}$$

Die über K endlichen Zwischenkörper L entsprechen dabei genau den offenen Untergruppen von $G_{\Omega/K}$. Beachte, daß jede offene Untergruppe auch abgeschlossen ist.

Beweis. s. Algebra-Seminar. □

15.3 Proendliche Gruppen

Eine *proendliche Gruppe* G ist eine topologische Gruppe mit den Eigenschaften

(1) G ist kompakt und hausdorffsch.

(2) $1 \in G$ besitzt eine offene Umgebungsbasis, die aus Normalteilern von G besteht.

Die Bedingung (2) ist äquivalent dazu, daß G total unzusammenhängend ist.

Sei G eine proendliche Gruppe, und sei $\{N_i \mid i \in I\}$ ein System von offenen Normalteilern in G, wobei I durch $i \leq j :\Longleftrightarrow N_j \subset N_i$ gerichtet ist, d.h. I ist eine halbgeordnete Menge, und zu $i, j \in I$ gibt es stets ein $k \in I$, so daß $i \leq k$ und $j \leq k$ gelten. Da G kompakt ist, hat jedes N_i endlichen Index in G. Also ist $G_i := G/N_i$ eine endliche Gruppe für jedes $i \in I$, und die G_i bilden mit den Projektionen $f_{ij}\colon G_j \longrightarrow G_i$ für $i, j \in I$ mit $i \leq j$ ein *projektives System*, d.h. es gilt $f_{ik} = f_{ij} \circ f_{jk}$, wann immer $i \leq j \leq k$.

$$\begin{tikzcd} G_k \arrow[rr, "f_{ik}"] \arrow[dr, "f_{jk}"'] & & G_i \\ & G_j \arrow[ur, "f_{ij}"'] & \end{tikzcd}$$

Sei

$$\varprojlim G_i := \{(\sigma_i)_i \in \prod_{i \in I} G_i \mid f_{ij}(\sigma_j) = \sigma_i \text{ für } i \leq j\}$$

der *projektive Limes der* G_i . Dann gilt $G = \varprojlim G_i$. Umgekehrt gilt: Ist $\{G_i, f_{ij}\}$ ein projektives System von endlichen Gruppen, so ist $\varprojlim G_i$ eine projektive Gruppe, wie z.B. $\varprojlim \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p = \{\text{ganze Zahlen in } \mathbb{Q}_p\}$.

Beispiel. Die Galoisgruppe $G_{\Omega/K}$ einer Galoiserweiterung Ω von K ist eine proendliche Gruppe. $G_{\Omega/K}$ ist kompakt und hausdorffsch. Die Gruppen $G_{L/K}$, wobei L alle endlich-galoisschen Erweiterungen von K in Ω durchläuft, bilden eine offene Umgebungsbasis der $1 \in G_{\Omega/K}$, und es gilt

$$G_{\Omega/K} \simeq \varprojlim G_{L/K} \,.$$

Benutzt werden, daß sich jedes L innerhalb von Ω in eine endliche Galoiserweiterung von K einbetten läßt, und der Hauptsatz der Galoistheorie 15.2 (iii) sowie Algebra 16.1, 16.3.

15.4 G-Moduln

Sei G eine Gruppe. Ein *G-Modul* U ist eine abelsche Gruppe, auf der G als eine Automorphismengruppe vermöge

$$G \times U \longrightarrow U \,, \quad (\sigma, x) \longmapsto \sigma(x) \,,$$

operiert. Es gilt dann

$$1x = x \,, \quad \sigma(xy) = \sigma(x)\sigma(y) \quad \text{und} \quad (\sigma\tau)(x) = \sigma(\tau(x)) \quad \forall\, x, y \in U \,,\ \sigma, \tau \in G \,.$$

Der *Fixmodul* eines G-Moduls U ist die Untergruppe

$$U^G := \{x \in U \mid \sigma(x) = x \; \forall \, \sigma \in G\} ,$$

und U heißt *trivialer G-Modul*, falls $U = U^G$.

- Ist G eine proendliche Gruppe, so fordern wir zusätzlich, daß die Abbildung

  $$G \times U \longrightarrow U \, , \; (\sigma, x) \longmapsto \sigma(x) \, ,$$

  stetig ist, wenn U mit der diskreten Topologie versehen wird.

- Ein *G-Homomorphismus* von G-Moduln U, V ist ein Gruppenhomomorphismus $\varphi \colon U \longrightarrow V$ mit

  $$\varphi(\sigma(x)) = \sigma(\varphi(x)) \qquad\qquad \forall \, x \in U \, , \; \sigma \in G \, .$$

15.5 Kohomologie proendlicher Gruppen

Sei G eine proendliche Gruppe, und sei U ein diskreter G-Modul. Dann definiert man die *Kokettengruppen*

$$\mathcal{C}^0(G,U) := U \quad \text{und} \quad \mathcal{C}^q(G,U) := \{f \colon G^q \longrightarrow U \mid f \text{ stetig}\} \quad \text{für } q \in \mathbb{N} \, ,$$

wobei $G^q := G \times \cdots \times G$ mit q Faktoren sei. Es ist $\mathcal{C}^q(G,U)$ eine abelsche Gruppe vermöge

$$(fg)(z) := f(z)g(z) \qquad\qquad \forall \, z \in G^q \, , \; f, g \in \mathcal{C}^q(G,U) \, .$$

Zu jedem $q > 0$ gibt es Abbildungen

$$\partial_q \colon \mathcal{C}^q(G,U) \longrightarrow \mathcal{C}^{q+1}(G,U) \, ,$$

definiert durch $\partial_0(x)(\sigma) = x^{-1}\sigma(x)$, wobei $x \in U$, $\sigma \in G$, und für $q \in \mathbb{N}$ durch

$$\partial_q(f)(\sigma_1, \ldots, \sigma_{q+1}) = \sigma_1(f(\sigma_2, \ldots, \sigma_{q+1})) \cdot \prod_{i=1}^{q} f(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{q+1})^{(-1)^i} \cdot \\ \cdot f(\sigma_1, \ldots, \sigma_q)^{(-1)^i} \, ,$$

wobei $f \in \mathcal{C}^q(G,U)$ und $\sigma_1, \ldots, \sigma_{q+1} \in G$ sind.
Es gilt dann $\partial_{q+1} \circ \partial_q = 1 \; \forall \, q \geq 0$. Die Gruppe

$$\boxed{H^q(G,U) := \operatorname{kern} \partial_q / \operatorname{bild} \partial_{q-1}}$$

heißt *q-te Kohomologiegruppe von G mit Werten in G* für $q \in \mathbb{N}$. Setze $H^0(G,U) := U^G$. Es ist $H^1(G,U)$ die Gruppe der Kohomologieklassen von stetigen Abbildungen $f\colon G \longrightarrow U$ mit $f(\sigma\tau) = f(\sigma)\sigma(f(\tau))\ \forall\,\sigma,\tau \in G$ und $H^2(G,U)$ die Gruppe der Klassen von stetigen Abbildungen $f\colon G\times G \longrightarrow U$ mit $f(\sigma,\tau)\cdot f(\sigma\tau,\varrho) = \sigma(f(\tau,\varrho))f(\sigma,\tau\varrho)\ \forall\,\sigma,\tau,\varrho \in G$, vgl. 7.4 und 7.8.

Bemerkung. Sei G eine proendliche Gruppe, und sei U ein diskreter G-Modul. Dann ist

$$H^q(G,U) = \varinjlim H^q(G/N, U^N)\,,$$

wobei N die offenen Normalteiler von G durchläuft $\forall\, q \geq 0$. Insbesondere ist $H^q(G,U)$ eine abelsche Torsionsgruppe.

Beweis. s. 15.3 und Algebra-Seminar. □

Beispiel. Ein separabler Abschluß K_s von K ist galoissch über K. In 8.4 und 8.7 haben wir gezeigt, daß $\mathrm{Br}(K) = \varinjlim H^2(G_{L/K}, L^*)$ gilt, wobei L alle endlich galoisschen Körpererweiterungen von K in K_s durchläuft. Aus der Bemerkung folgt also:

$$\boxed{\mathrm{Br}(K) \simeq H^2(G_{K_s/K}, K_s^*)}\,.$$

15.6 Die lange exakte Kohomologiesequenz

Sei G eine proendliche Gruppe, und sei U ein diskreter G-Modul.
Mit $\mathcal{Z}^q(G,U) := \ker \partial_q$ sei die Gruppe der *q-Kozyklen von G in U* bezeichnet, wobei ∂_q wie in 15.5 definiert ist. Ist $\varphi\colon U \longrightarrow V$ ein G-Homomorphismus, so induziert die Zuordnung $f \longmapsto \varphi\circ f$ für $f \in \mathcal{Z}^q(G,U)$ einen Gruppenhomomorphismus $H^q(G,U) \longrightarrow H^q(G,V)\ \forall\, q \geq 0$.

Satz. *Sei $1 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 1$ eine exakte G-Modulsequenz. Dann hat man für jedes q einen* Verbindungshomomorphismus

$$\delta_q\colon H^q(G,W) \longrightarrow H^{q+1}(G,U)$$

so, daß folgende Gruppensequenz exakt ist:

$$\begin{aligned} \ldots \longrightarrow H^q(G,U) \longrightarrow H^q(G,V) \longrightarrow H^q(G,W) \xrightarrow{\delta_q} \\ \xrightarrow{\delta_q} H^{q+1}(G,U) \longrightarrow H^{q+1}(G,V) \longrightarrow \cdots\,. \end{aligned}$$

Beweis. s. Algebra-Seminar WS 2001/02. □

15.7 Artin-Schreier-Theorie

Sei K ein Körper mit $\operatorname{char} K = p > 0$. Dann ist das Polynom $X^p - X - a$ für jedes $a \in K$ separabel, denn ist v eine Nullstelle, so sind $v+1, \dots, v+(p-1)$ die anderen Nullstellen. Die Abbildung

$$\wp\colon K_s \longrightarrow K_s\,,\ x \longmapsto x^p - x\,,$$

ist also ein surjektiver G-Homomorphismus, wobei $G = G_{K_s/K}$ sei. Betrachtet man $\mathbb{Z}/p\mathbb{Z}$ als trivialen G-Modul, so induziert die exakte Sequenz

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow K_s \xrightarrow{\wp} K_s \longrightarrow 0$$

nach 15.6 eine exakte Sequenz

$$\longrightarrow K \xrightarrow{\wp} K \xrightarrow{\delta_0} H^1(G, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^1(G, K_s) = \{0\}\,,$$

da $H^0(G, K_s) = K_s^G = K$ gilt. Es folgt

$$K/\wp K \simeq H^1(G, \mathbb{Z}/p\mathbb{Z}) = \operatorname{Hom}_{\text{stet}}(G, \mathbb{Z}/p\mathbb{Z})\,.$$

15.8 Kummer-Theorie und der Fall $q = 2$

Es gelte $\operatorname{char} K \nmid n$, und K enthalte die Gruppe μ_n der n-ten Einheitswurzeln. Dann hat man eine exakte G-Modulsequenz

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_n & \longrightarrow & K_s^* & \longrightarrow & K_s^* & \longrightarrow & 1\,, \\ & & & & x & \longmapsto & x^n\,, & & \end{array}$$

wobei $G := G_{K_s/K}$ trivial auf μ_n operiert. Analog wie in 15.7 folgt

$$\boxed{K^*/K^{*n} \simeq H^1(G, \mu_n) = \operatorname{Hom}_{st}(G, \mu_n)}\,.$$

Nach 15.6 induziert die exakte Sequenz

$$1 \longrightarrow \mu_n \longrightarrow K_s^* \longrightarrow K_s^* \longrightarrow 1$$

eine kommutatives Diagramm mit exakter Zeile

$$\begin{tikzcd} 1 \underset{7.9}{=} H^1(G, K_s^*) \arrow[r] & H^2(G, \mu_n) \arrow[r] & H^2(G, K_s^*) \arrow[r] \arrow[d, "15.5"', "\simeq"] & H^2(G, K_s^*) \arrow[d, "15.5"', "\simeq"] \\ & & \operatorname{Br}(K) \arrow[r] & \operatorname{Br}(K) \\ & & {[A]} \arrow[r, mapsto] & {[A]^n}\,. \end{tikzcd}$$

Es folgt $H^2(G, \mu_n) \simeq {}_n\operatorname{Br}(K) = \{[A] \in \operatorname{Br}(K) \mid [A^n] = 1\}$. Da $\mu_n \subset K$ gilt, operiert G trivial auf μ_n, und man erhält Isomorphien

$$H^2(G, \mu_n \otimes_{\mathbb{Z}} \mu_n) \simeq H^2(G, \mu_n) \otimes_{\mathbb{Z}} \mu_n \simeq {}_n\operatorname{Br}(K) \otimes_{\mathbb{Z}} \mu_n\,.$$

15.9 Kohomologische Fassung des Theorems von Merkurjev-Suslin

Es gelte char $K \nmid n$, und μ_n sei die Gruppe der n-ten Einheitswurzeln in K_s^*. Für die in 15.5 eingeführten Kohomologiegruppen $H^q(G,U)$ schreibt man im Fall $G = G_{K_s/K}$ meist $H^q(K,U)$. Mit dieser Schreibweise gilt das

Theorem. *Das Cupprodukt*

$$\cup\colon H^1(K,\mu_n) \times H^1(K,\mu_n) \longrightarrow H^2(K,\mu_n \otimes_{\mathbb{Z}} \mu_n)$$

induziert einen Gruppenisomorphismus

$$h^{(2)}_{K,n}\colon K_2(K)/nK_2(K) \longrightarrow H^2(K,\mu_n \otimes_{\mathbb{Z}} \mu_n)\,.$$

Der Beweis geschieht in Reduktionsschritten:

1) Es genügt, $n = p^m$ mit einer Primzahl $p \neq \operatorname{char} K$ anzunehmen.

2) Man kann $m = 1$ nehmen.

3) Es genügt zu zeigen: Ist $\mu_p \subset K$, so ist

$$R_{K,p}\colon K_2(K)/pK_2(K) \longrightarrow {}_p\mathrm{Br}(K)$$

bijektiv, vgl. 14.8 für die Definition von $R_{K,p}$ und 10.10 für eine Anwendung des Theorems auf Azumaya-Algebren. Für die Definition des Cupprodukts s. Algebra-Seminar.

15.10 Bloch-Kato-Vermutungen

Sei K ein Körper. Die *Milnorschen K-Gruppen* sind durch $K_0(K) = \mathbb{Z}$ und für $q \in \mathbb{N}$ durch

$$K_q(K) := (K^* \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} K^*)/\langle a_1 \otimes \cdots \otimes a \otimes \cdots \otimes 1-a \otimes \cdots \otimes a_q \mid a \neq 1\rangle$$

definiert. Mit $\{a_1,\ldots,a_q\}$ sei die Restklasse von $a_1 \otimes \cdots \otimes a_q$ bezeichnet. Dann ist $K_1(K) = \{\{a\} \mid a \in K^*\}$ mit der Addition $\{a\}+\{b\} := \{ab\}$.

Vermutung. Für jede Primzahl $p \neq \operatorname{char} K$ und jedes $q \in \mathbb{N}$ ist der durch das Cupprodukt induzierte Homomorphismus

$$h^{(q)}_{K,p}\colon K_q(K)/pK_q(K) \longrightarrow H^q(K,\underbrace{\mu_p \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mu_p}_{q\text{-mal}})$$

bijektiv. Bezeichne die Vermutung mit BKV(q,p). Dann ist folgendes schon bewiesen:

BKV$(2,2)$	Merkurjev 1982
BKV$(2,p)$	Merkurjev-Suslin 1983
BKV$(3,2)$	Merkurjev-Suslin, Rost 1986
BKV$(q,2)$	Voevodsky 1996–2001
$\left.\begin{array}{r}\text{BKV}(3,3)\\ \text{BKV}(4.3)\end{array}\right\}$	Voevodsky – Rost 1996/97
BKV(q,p) ?	Voevodsky – Rost 1996/97 (char $K = 0$)

vgl. u.a. K-Theorie-Preprint-Server.

Die *Milnor-Vermutungen* beziehen sich auf ein kommutatives Diagramm

$$\begin{tikzcd}
K_q(K)/2K_q(K) \arrow[rr, "h_{K,2}^{(q)}"] \arrow[dr, "s_q"'] & & H^q(K,\mathbb{Z}/2\mathbb{Z}) \\
& I^q(K)/I^{q+1}(K) \arrow[ur, dashed, "e_q"'] &
\end{tikzcd}$$

Hierbei ist $I(K)$ das Ideal der Klassen gerade-dimensionaler quadratischer Formen im Wittring $\mathcal{W}(K)$ und $I^q(K)$ dessen q-te Potenz. $I^q(K)$ wird von q-fachen Pfisterformen

$$\ll a_1, \ldots, a_q \gg := \langle 1, -a_1\rangle \otimes \cdots \otimes \langle 1, -a_q\rangle$$

erzeugt und daher wird s_q durch

$$\{a_1, \ldots, a_q\} \longmapsto \ \ll a_1, \ldots, a_q \gg$$

induziert.

16 Index