# Brauergruppen

Benjamin Sambale*

21. Dezember 2020

## 1 Einfache Algebren

**Definition 1.1.** Sei $K$ ein Körper. Eine *($K$-)Algebra* $A$ ist ein Ring mit 1 und zugleich ein endlichdimensionaler $K$-Vektorraum, sodass die Multiplikation mit der Skalarmultiplikation verträglich ist, d. h. es gilt

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

Mit $A$ ist auch das *Zentrum* $\mathrm{Z}(A) := \{a \in A : ab = ba \forall b \in A\}$ eine $K$-Algebra. Ebenso hat man die *entgegengesetzte* Algebra $A^o$, bei der die Multiplikation durch $a * b := ba$ für $a, b \in A$ ersetzt wird. Man nennt $A$

- *zentral*, falls $\mathrm{Z}(A) = K1 \cong K$,
- *einfach*, falls 0 und $A$ die einzigen Ideale in $A$ sind,
- *Divisionsalgebra*, falls $A^\times = A \setminus \{0\}$.

**Satz 1.2.** *Für $n \in \mathbb{N}$ und jede zentrale Divisionsalgebra $D$ ist $D^{n\times n}$ eine zentral einfache Algebra. Insbesondere ist $K^{n\times n}$ zentral einfach.*

*Beweis.* Sei $0 \neq I \trianglelefteq D^{n\times n}$ und $A = (a_{ij}) \in I$ mit $a_{st} \neq 0$. Sei $E_{ij} \in D^{n\times n}$ die Matrix mit einer 1 an Position $(i, j)$ und sonst nur Nullen. Für jedes $B = (b_{ij}) \in D^{n\times n}$ gilt

$$B = \sum_{i,j=1}^{n} b_{ij} a_{st}^{-1} E_{is} A E_{tj} \in I.$$

Also ist $D^{n\times n}$ einfach. Für $A = (a_{ij}) \in \mathrm{Z}(D^{n\times n})$ gilt

$$(\delta_{is} a_{tj})_{i,j} = E_{st}A = AE_{st} = (\delta_{jt} a_{is})_{i,j}.$$

Dies zeigt $a_{ij} = 0$ für $i \neq j$ und $a_{11} = \ldots = a_{nn}$. Daher ist $\mathrm{Z}(D^{n\times n}) = \mathrm{Z}(D)1_n = K1_n$. □

*Institut für Mathematik, Friedrich-Schiller-Universität Jena, 07737 Jena, Germany, benjamin.sambale@uni-jena.de

**Beispiel 1.3.** Jede endliche Körpererweiterung von $K$ ist eine Divisionsalgebra. Umgekehrt ist jede kommutative Divisionsalgebra ein Körper. Jede Divisionsalgebra $D$ ist zentral über dem Körper $\mathrm{Z}(D)$. Für $n \geq 2$ ist $K^{n\times n}$ keine Divisionsalgebra. Der Faktorring $K[X]/(X^2)$ ist eine nicht-einfache Algebra. Schließlich bilden die *Hamiltonschen Quaternionen*

$$\mathbb{H} := \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\} \subseteq \mathbb{C}^{2\times 2}$$

eine nicht-kommutative $\mathbb{R}$-Divisionsalgebra.

**Bemerkung 1.4.** Jeder Modul $M$ einer Algebra $A$ wird durch $\lambda m := (\lambda 1_A)m$ $(\lambda \in K, m \in M)$ zu einem $K$-Vektorraum. Ist $M$ als $A$-Modul endlich erzeugt, so ist $M$ als Vektorraum endlich-dimensional. Homomorphismen zwischen $A$-Moduln sind auch $K$-linear. Ist $M$ einfach und $0 \neq m \in M$, so ist $f : A \to M$, $a \mapsto am$ ein Epimorphismus und es folgt $M \simeq A/\mathrm{Ker}(f)$. Daher tritt jeder einfache Modul als Kompositionsfaktor des regulären Moduls auf. Nach Jordan-Hölder gibt es nur endlich viele einfache Moduln bis auf Isomorphie.

**Satz 1.5** (Schurs Lemma)**.** *Sei $A$ eine Algebra und $M$ ein einfacher $A$-Modul. Dann ist die Endomorphismenalgebra $\mathrm{End}_A(M)$ eine Divisionsalgebra.*

*Beweis.* Mit komponentenweiser Addition und Skalarmultiplikation sowie mit der Komposition als Multiplikation wird $E := \mathrm{End}_A(M)$ eine Algebra. Für $f \in E \setminus \{0\}$ sind $\mathrm{Ker}(f) \neq M$ und $f(M) \neq 0$ Untermoduln des einfachen Moduls $M$. Daher gilt $\mathrm{Ker}(f) = 0$ und $f(M) = M$. Also ist $f$ ein Isomorphismus und daher invertierbar in $E$. □

**Bemerkung 1.6.** Jeder $A$-Modul $M$ wird durch $fm := f(m)$ $(f \in \mathrm{End}_A(M),\ m \in M)$ zu einem $\mathrm{End}_A(M)$-Modul. Nach Algebra 2 besitzt jeder Modul über einer Divisionsalgebra eine Basis und jede zwei Basen sind gleichmächtig. Man spricht dann auch von Vektorräumen und deren Dimension.

**Satz 1.7** (Wedderburn)**.** *Jede einfache Algebra $A$ besitzt nur einen einfachen Modul $S$ bis auf Isomorphie. Für die Divisionsalgebra $D := \mathrm{End}_A(S)$ gilt $A \cong (D^o)^{n\times n}$, wobei $n$ die Dimension von $S$ über $D$ ist ($n$ ist auch die Vielfachheit von $S$ als Kompositionsfaktor des regulären $A$-Moduls). Insbesondere sind $n$ und $D$ (bis auf Isomorphie) eindeutig durch $A$ bestimmt.*

*Beweis.* Wegen $\dim A < \infty$ existiert ein einfacher Untermodul $S$ des regulären $A$-Moduls (also ein minimales Linksideal). Für $a \in A$ ist die Abbildung $S \to A$, $x \mapsto xa$ ein Homomorphismus. Insbesondere ist $Sa$ ein Untermodul von $A$. Außerdem ist $\sum_{a\in A} Sa$ ein Ideal und die Einfachheit von $A$ zeigt $A = \sum_{a\in A} Sa$. Wir wählen $a_1, \ldots, a_n \in A$ minimal mit $A = Sa_1 + \ldots Sa_n$. Dann ist $Sa_1 \cap (Sa_2 + \ldots + Sa_n)$ ein echter Untermodul des einfachen Moduls $Sa_1$. Dies zeigt $Sa_1 \cap (Sa_2 + \ldots + Sa_n) = 0$ und $A = Sa_1 \oplus \ldots \oplus Sa_n$. Dabei ist $S \simeq Sa_1 \simeq \ldots \simeq Sa_n$ einfach. Nach Jordan-Hölder ist $S$ der einzige einfache $A$-Modul bis auf Isomorphie. Außerdem existieren kanonische Isomorphismen

$$A \cong \mathrm{End}_A(A)^o \cong \mathrm{End}_A(S^n)^o \cong (D^{n\times n})^o \cong (D^o)^{n\times n}$$

(benutze Projektion, Injektion und Transposition). Wegen $n \dim_D(S) = \dim_D(A) = n^2 \dim(D)$ ist $n = \dim_D(S)$ und $n$ ist die Vielfachheit von $S$ als Kompositionsfaktor von $A$. □

**Satz 1.8.** *Jede Divisionsalgebra über einem algebraisch abgeschlossenen Körper $K$ ist zu $K$ isomorph.*

*Beweis.* Sei $D$ eine Divisionsalgebra und $x \in D$. Dann sind die Potenzen $1, x, x^2, \ldots$ linear abhängig über $K$. Daher existiert $\alpha \in K[X]$ mit $\alpha(x) = 0$. Da $K$ algebraisch abgeschlossen ist, zerfällt $\alpha$ in Linearfaktoren, etwa $\alpha = (X - a_1) \ldots (X - a_n)$ mit $a_1, \ldots, a_n \in K$. Da $D$ eine Divisionsalgebra ist, existiert ein $i$ mit $x - a_i 1_A = 0$, d. h. $x = a_i 1_A \in K1$. Dies zeigt $D = K1 \cong K$. □

**Lemma 1.9.** *Sei $S$ ein einfacher Modul einer Algebra $A$ und $D := \mathrm{End}_A(S)$. Sei $T \subseteq S$ eine endliche Teilmenge und $I := \{a \in A : aT = 0\}$. Für $s \in S$ mit $Is = 0$ gilt dann $s \in \mathrm{Span}_D T$.*

*Beweis.* Induktion nach $|T|$. Im Fall $T = \varnothing$ ist $I = A$ und $s = 0 \in \mathrm{Span}_K T$. Sei also $t \in T$ und die Behauptung für $T' := T \setminus \{t\}$ bereits gezeigt. Sei $I' := \{a \in A : aT' = 0\}$. Im Fall $I't = 0$ ist $I' = I$ und $s \in \mathrm{Span}_K T' \subseteq \mathrm{Span}_K T$ nach Induktion. Sei also $I't \neq 0$. Offenbar ist $I't$ ein $A$-Untermodul von $S$ und die Einfachheit von $S$ liefert $I't = S$. Die Abbildung $f : S \to S$, $it \mapsto is$ mit $i \in I'$ ist wohldefiniert und $A$-linear, d. h. $f \in D$. Für $i \in I'$ folgt $i(s - f(t)) = is - if(t) = is - f(it) = 0$. Also ist $I'(s - f(t)) = 0$ und $s - f(t) \in \mathrm{Span}_D T'$ nach Induktion. Dies zeigt $s \in \mathrm{Span}_D T$. □

**Satz 1.10** (Jacobsons Dichtigkeitssatz)**.** *Sei $S$ ein einfacher Modul einer Algebra $A$ und $D := \mathrm{End}_A(S)$. Sei $T \subseteq S$ eine endliche $D$-linear unabhängige Teilmenge. Für jedes $\varphi \in \mathrm{End}_D(S)$ existiert dann ein $a \in A$ mit $\varphi(t) = at$ für alle $t \in T$.*

*Beweis.* Durch Induktion nach $|T|$ können wir $T \neq \varnothing$ annehmen. Sei $s \in T$ und $T' := T \setminus \{s\}$. Nach Induktion existiert $b \in A$ mit $\varphi(t) = bt$ für alle $t \in T'$. Sei $I := \{a \in A : aT' = 0\}$. Da $T$ linear unabhängig ist, gilt $s \notin \mathrm{Span}_D T'$. Nach Lemma 1.9 ist daher $Is \neq 0$. Wie üblich ist dann $Is = S$ und es existiert $i \in I$ mit $is = \varphi(s) - bs$. Für $a := b + i \in A$ gilt nun

$$\varphi(t) = \begin{cases} bt = at & \text{falls } t \neq s, \\ at & \text{falls } t = s. \end{cases}$$

□

## 2 Tensorprodukte

**Definition 2.1.** Seien $A$ und $B$ Algebren mit Basen $a_1, \ldots, a_n$ bzw. $b_1, \ldots, b_m$. Sei $A \otimes B = A \otimes_K B$ der $K$-Vektorraum mit Basis $a_i \otimes b_j$ $(1 \leq i \leq n,\ 1 \leq j \leq m)$. Die Vorschrift $(a_i, b_j) \mapsto a_i \otimes b_j$ definiert eine bilineare Abbildung $\otimes : A \times B \to A \otimes B$. Wir setzen $a \otimes b := \otimes(a, b)$ für $a \in A$ und $b \in B$. Durch

$$(a_i \otimes b_j)(a_r \otimes b_s) := a_i a_r \otimes b_j b_s$$

wird $A \otimes B$ zu einer $K$-Algebra. Man nennt $A \otimes B$ das *Tensorprodukt* von $A$ und $B$.

**Satz 2.2** (Universelle Eigenschaft)**.** *Für Algebren $A, B, C$ und jede bilineare Abbildung $\beta : A \times B \to C$ existiert genau ein $K$-Homomorphismus $F : A \otimes B \to C$ mit $F(a \otimes b) = \beta(a, b)$.*

*Beweis.* Wie oben seien $a_1, \ldots, a_n$ und $b_1, \ldots, b_m$ Basen von $A$ bzw. $B$. Durch $F(a_i \otimes b_j) := \beta(a_i, b_j)$ erhält man die gewünschte Abbildung. □

**Lemma 2.3.** *Für Algebren $A, B, C$ gilt $A \otimes B \cong B \otimes A$, $A \otimes K \cong A$ und $A \otimes (B \otimes C) \cong (A \otimes B) \otimes C$.*

*Beweis.* Die bilineare Abbildung $A \times B \to B \otimes A$, $(a, b) \mapsto b \otimes a$ liefert eine lineare Abbildung $F : A \otimes B \to B \otimes A$. Offenbar ist $F$ auch ein Isomorphismus von Algebren. Die anderen Behauptungen sind analog. □

**Bemerkung 2.4.**

(i) Für $x_1 = \sum_{j=1}^n x_{1j}a_j, x_2 = \sum_{i=1}^n x_{2i}a_i \in A$ und $y_1 = \sum_{i=1}^n y_{1i}b_i, y_2 = \sum_{i=1}^n y_{2i}b_i \in B$ gilt

$$\begin{aligned}(x_1 \otimes y_1)(x_2 \otimes y_2) &= \Big(\sum_{i,j} x_{1i}y_{1j}(a_i \otimes b_j)\Big)\Big(\sum_{r,s} x_{2r}y_{2s}(a_r \otimes b_s)\Big) \\ &= \sum_{i,j,r,s} x_{1i}y_{1j}x_{2r}y_{2s}(a_ia_r \otimes b_jb_s) = x_1y_1 \otimes x_2y_2.\end{aligned}$$

(ii) Sei $A = A_1 \oplus A_2$ eine Zerlegung in Untervektorräume. Wir wählen eine Basis $a_1, \ldots, a_n$ von $A$, sodass $a_1, \ldots, a_k$ (bzw. $a_{k+1}, \ldots, a_n$) eine Basis von $A_1$ (bzw. $A_2$) ist. Jedes Element von $A \times B$ lässt sich eindeutig in der Form $\sum_{i=1}^n a_i \otimes b_i$ mit $b_i \in B$ schreiben. Dies zeigt $A \otimes B = (A_1 \otimes B) \oplus (A_2 \otimes B)$. Man zeigt auch leicht $A \otimes B \cong B \otimes A$ sowie $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$.

**Lemma 2.5.** *Es gilt* $\mathrm{Z}(A \otimes B) = \mathrm{Z}(A) \otimes \mathrm{Z}(B)$.

*Beweis.* Sicher ist $\mathrm{Z}(A) \otimes \mathrm{Z}(B) \subseteq \mathrm{Z}(A \otimes B)$. Sei $A = \mathrm{Z}(A) \oplus A_1$ eine Zerlegung in Untervektorräume und $z \in \mathrm{Z}(A \otimes B)$. Wir schreiben $z = x + y$ mit $x \in \mathrm{Z}(A) \otimes B$ und $y \in A_1 \otimes B$. Da $a \otimes 1$ sowohl mit $z$ als auch mit $x$ vertauschbar ist, ist $a \otimes 1$ auch mit $y$ vertauschbar für alle $a \in A$. Sei $b_1, \ldots, b_m$ eine Basis von $B$ und $y = \sum_{i=1}^m a_i \otimes b_i$ mit $a_i \in A$. Wegen

$$\sum_{i=1}^m a_ia \otimes b_i = y(a \otimes 1) = (a \otimes 1)y = \sum_{i=1}^m a_ia \otimes b_i$$

gilt $a_ia = aa_i$ für $i = 1, \ldots, m$. Da $a \in A$ beliebig war, gilt $a_i \in \mathrm{Z}(A)$ für $i = 1, \ldots, m$. Dies zeigt $y \in A_1 \cap \mathrm{Z}(A) = 0$ und $\mathrm{Z}(A \otimes B) \subseteq \mathrm{Z}(A) \otimes B$. Wir können nun analog $B = \mathrm{Z}(B) \oplus B_1$ zerlegen und schreiben $z = x + y$ mit $x \in \mathrm{Z}(A) \otimes \mathrm{Z}(B)$ sowie $y \in \mathrm{Z}(A) \otimes B_1$. Dann ist $y$ mit $1 \otimes b$ ($b \in B$) vertauschbar und man erhält leicht $y = 0$. Insgesamt ist $\mathrm{Z}(A \otimes B) \subseteq \mathrm{Z}(A) \otimes \mathrm{Z}(B)$. □

**Lemma 2.6.** *Seien $A$ und $B$ Algebren und $n, m \in \mathbb{N}$. Dann ist $(A^{n\times n})^{m\times m} \cong A^{nm\times nm}$ und $A^{n\times n} \otimes B^{m\times m} \cong (A \otimes B)^{nm\times nm}$.*

*Beweis.* Die erste Aussage ergibt sich, indem man jede Matrix in $A^{nm\times nm}$ als Blockmatrix mit Blöcken von Format $n \times n$ auffasst.

Das Kroneckerprodukt von Matrizen liefert eine bilineare Abbildung $A^{n\times n} \times B^{m\times m} \to (A \otimes B)^{nm\times nm}$. Diese liefert eine Homomorphismus von $K$-Algebren $A^{n\times n} \otimes B^{m\times m} \to (A \otimes B)^{nm\times nm}$. Wählt man Basen $a_1, \ldots, a_r$ von $A$ und $b_1, \ldots, b_s$ von $B$, so bilden die Matrizen $a_iE_{kl}$ bzw. $b_iE_{kl}$ Basen von $A^{n\times n}$ bzw. $B^{m\times m}$. Dann bilden

$$F(a_iE_{kl} \otimes b_jE_{pq}) = (a_i \otimes b_j)E_{(k-1)m+p,(l-1)m+p}$$

eine $K$-Basis von $(A \otimes B)^{nm\times nm}$. Also ist $F$ surjektiv und aus Dimensionsgründen auch injektiv. □

**Lemma 2.7.** *Sei $A$ eine einfache Algebra und $B$ eine zentral einfache Algebra. Dann ist $A \otimes B$ einfach.*

*Beweis.* Nach Wedderburn existieren Divisionsalgebren $D_A$ und $D_B$ und $n, m \in \mathbb{N}$ mit $A \cong D_A^{n\times n}$ sowie $B \cong D_B^{m\times m}$. Dabei ist $\mathrm{Z}(D_B) \cong \mathrm{Z}(D_B^{m\times m}) \cong \mathrm{Z}(B) \cong K$. Mit Lemma 2.6 folgt

$$A \otimes B \cong (D_A \otimes D_B)^{nm\times nm}.$$

Wir werden zeigen, dass $D_A \times D_B$ einfach ist, denn dann existiert eine Divisionsalgebra $D$ und $k \in \mathbb{N}$ mit $D_A \otimes D_B \cong D^{k\times k}$ und

$$A \otimes B \cong D^{knm\times knm}$$

nach Lemma 2.6. Wir können nun also $A = D_A$ und $B = D_B$ annehmen.

Sei $a_1, \ldots, a_n$ eine $K$-Basis von $A$ und $0 \neq I \trianglelefteq A \otimes B$. Wähle $x \in I \setminus \{0\}$, sodass in der eindeutigen Darstellung $x = \sum_{i=1}^n a_i \otimes b_i$ möglichst viele der $b_i$ verschwinden. O. B. d. A. sei $b_1 \neq 0$. Nach Multiplikation mit $1 \otimes b_1^{-1}$ können wir $b_1 = 1$ annehmen (beachte: $B = D_B$ ist eine Divisionsalgebra). Für alle $b \in B$ gilt dann

$$I \ni (1 \otimes b)x - x(1 \otimes b) = \sum_{i=2}^n a_i \otimes (bb_i - b_i b).$$

Die Wahl von $x$ zeigt $bb_i = b_i b$, d. h. $b_i \in \mathrm{Z}(B) = K1_B$. Daher ist $x = \left(\sum_{i=1}^n b_i a_i\right) \otimes 1$. Insbesondere ist $J := \{a \in A : a \otimes 1 \in I\}$ ein nicht-triviales Ideal in $A$. Da $A$ einfach ist, gilt $1 \in J$ und daher $1 = 1 \otimes 1 \in I$. □

**Beispiel 2.8.** Das Tensorprodukt von beliebigen einfachen Algebren muss nicht einfach sein: Sei $K = \mathbb{R}$, $x := \mathrm{i} \otimes 1 \in \mathbb{C} \otimes \mathbb{C}$ und $y := 1 \otimes \mathrm{i} \in \mathbb{C} \otimes \mathbb{C}$. Wir definieren eine lineare Abbildung $f : \mathbb{C} \otimes \mathbb{C} \to \mathbb{C} \oplus \mathbb{C}$ durch $f(1 \otimes 1) := (1, 1)$, $f(x) = (\mathrm{i}, \mathrm{i})$, $f(y) = (\mathrm{i}, -\mathrm{i})$ und $f(xy) = f(x)f(y) = (-1, 1)$. Wegen $f(x^2) = f(-1) = (-1, -1) = f(x)^2$ und $f(y^2) = f(y)^2$ ist $f$ ein Isomorphismus von Algebren, d. h. $\mathbb{C} \otimes \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$.

# 3 Zentral einfache Algebren

**Satz 3.1.** *Sind $A$ und $B$ zentral einfache Algebren, so auch $A \otimes B$.*

*Beweis.* Folgt aus Lemma 2.5 und Lemma 2.7. □

**Satz 3.2.** *Eine Algebra $A$ ist genau dann zentral einfach, wenn die Abbildung $F : A \otimes A^o \to \mathrm{End}_K(A)$ mit $F(a \otimes b)(x) := axb$ ein Isomorphismus von Algebren ist.*

*Beweis.* Für $a, b \in A$ ist offenbar $f_{a,b} : A \to A$, $x \mapsto axb$ ein $K$-Homomorphismus. Man den Axiomen für Algebren ist die Abbildung $A \times A^o \to \mathrm{End}_K(A)$, $(a, b) \mapsto f_{a,b}$ bilinear. Mit der universellen Eigenschaft erhält man, dass $F$ $K$-linear ist. Für $a, b, c, d \in A$ ist außerdem

$$F((a \otimes b)(c \otimes d))(x) = F(ac \otimes db)(x) = acxdb = F(a \otimes b)(F(c \otimes d)(x)).$$

Daher ist $F$ ein Homomorphismus von Algebren.

Sei nun $A$ zentral einfach. Nach Satz 3.1 ist $A \otimes A^o$ einfach und daher $\mathrm{Ker}(F) = 0$. Wegen $\dim A \otimes A^o = \dim^2 A = \dim \mathrm{End}_K(A)$ ist $F$ ein Isomorphismus. Sei umgekehrt $F$ ein Isomorphismus. Dann ist $A \otimes A^o \cong \mathrm{End}_K(A) \cong K^{n\times n}$ zentral einfach. Wegen $\mathrm{Z}(A) \otimes \mathrm{Z}(A) \cong \mathrm{Z}(A \otimes A^o) \cong \mathrm{Z}(K)$ ist auch $\mathrm{Z}(A) \cong K$. Für $0 \neq I \trianglelefteq A$ ist auch $0 \neq I \otimes A^o \trianglelefteq A \otimes A^o$. Da $A \otimes A^o$ einfach ist, folgt $\dim(I) \dim(A) = \dim(I \otimes A^o) = \dim(A \otimes A^o) = \dim^2(A)$ und $I = A$. Also ist $A$ einfach. □

**Definition 3.3.** Zentral einfache Algebren $A$ und $B$ heißen *äquivalent*, falls eine Divisionsalgebra $D$ und $n, m \in \mathbb{N}$ mit $A \cong D^{n\times n}$ sowie $B \cong D^{m\times m}$ existiert. Offenbar definiert dies eine Äquivalenzrelation. Die Äquivalenzklasse von $A$ bezeichnen wir mit $[A]$. Schließlich sei $\mathrm{Br}(K) := \{[A] : A \text{ zentral einfach}\}$.

**Bemerkung 3.4.** Nach Wedderburn enthält jede Äquivalenzklasse von zentral einfachen Algebren genau eine Divisionsalgebra.

**Satz 3.5.** *Durch*

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

*wird* $\mathrm{Br}(K)$ *zu einer abelschen Gruppe. Man nennt* $\mathrm{Br}(K)$ *die* Brauergruppe *von* $K$*.*

*Beweis.* Seien $D, D_A, D_B$ Divisionsalgebren mit $A \cong D_A^{n\times n}$, $B \cong D_B^{m\times m}$ und $D_A \times D_B \cong D^{k\times k}$. Wie in Lemma 2.7 ist $A \otimes B \cong D^{nmk\times nmk}$. Daraus folgt leicht, dass $[A] \cdot [B]$ nicht von der Wahl der Repräsentanten $A$ und $B$ abhängt. Nach Lemma 2.3 ist $\cdot$ assoziativ, kommutativ und $[K]$ ist ein neutrales Element. Nach Satz 3.2 ist $[A] \cdot [A^o] = [\mathrm{End}_K(A)] = [K^{n\times n}] = [K]$. Also ist $[A^o]$ das Inverse zu $[A]$. □

**Beispiel 3.6.** Für jeden algebraisch abgeschlossenen Körper $K$ ist $\mathrm{Br}(K) = 1$ nach Satz 1.8.

**Satz 3.7** (Skolem-Noether)**.** *Sei $A$ zentral einfach und $B$ einfach. Für Homomorphismen $f, g : B \to A$ existiert ein $a \in A^\times$ mit $f(x) = ag(x)a^{-1}$ für alle $x \in A$.*

*Beweis.* Wir betrachten $M_f := A$ als $A \otimes B^o$-Modul via

$$(a \otimes b)m := amf(b) \qquad (a \in A, b \in B, m \in M).$$

Nach Lemma 2.7 ist $A \otimes B^o$ einfach. Insbesondere besitzt $A \otimes B^o$ nur einen einfachen Modul $S$ bis auf Isomorphie. Daher ist $M_f \simeq S^k$ für ein $k \in \mathbb{N}$. Analog ist auch $M_g$ ein $A \otimes B^o$-Modul der gleichen Dimension. Daher ist $M_f \simeq S^k \simeq M_g$. Sei $\varphi : M_f \to M_g$ ein Isomorphismus. Für $a := \varphi(1)$ und $x \in A$ gilt dann

$$ag(x) = (1 \otimes x)\varphi(1) = \varphi((1 \otimes x)1) = \varphi(f(x)) = \varphi((f(x) \otimes 1)1) = (f(x) \otimes 1)\varphi(1) = f(x)a.$$

Für $b := \varphi^{-1}(1)$ gilt $ba = (b \otimes 1)\varphi(1) = \varphi((b \otimes 1)1) = \varphi(b) = 1 = ab$. Daher ist $a \in A^\times$. □

**Beispiel 3.8.** Aus Skolem-Noether folgt, dass $K^{n\times n}$ nur innere Automorphismen besitzt (setze $A = B$ und $g = 1$).

**Satz 3.9** (Doppel-Zentralisator-Satz)**.** *Sei $A$ eine zentral einfache $K$-Algebra und $B \subseteq A$ eine einfache Unteralgebra. Dann gilt*

*(i)* $C := \mathrm{C}_A(B)$ *ist einfach,*

*(ii) Ist $D$ eine Divisionsalgebra mit $C \cong D^{k\times k}$, so gilt $A \otimes B^o \cong D^{n\times n}$ mit $k \mid n$.*

*(iii)* $\dim A = \dim(B)\dim(C)$*,*

*(iv)* $\mathrm{C}_A(C) = B$*.*

*Beweis.*

(i) Sei $f : B \to A$ die Inklusionsabbildung. Wie im Satz von Skolem-Noether betrachten wir $M_f := A$ als Modul der einfachen Algebra $A \otimes B^o$. Sei $S$ der einfache $A \otimes B^o$-Modul und $D := \mathrm{End}_{A\otimes B^o}(S)$ eine Divisionsalgebra (Schurs Lemma). Dann ist $(A \otimes B^o)^o \cong D^{n\times n}$, wobei $S \cong D^{n\times 1}$. Sei $M_f \cong S^k$. Nach Schurs Lemma ist $E := \mathrm{End}_{A\otimes B^o}(M_f) \cong D^{k\times k}$ einfach. Sei $\varphi \in E$ und $a := \varphi(1)$. Für $b \in B$ gilt dann

$$ab = (1 \otimes b)\varphi(1) = \varphi((1 \otimes b)1) = \varphi((b \otimes 1)1) = (b \otimes 1)\varphi(1) = ba,$$

d. h. $a \in C$. Für jedes $c \in C$ ist umgekehrt die Abbildung $\varphi : M \to M$, $m \mapsto cm$ ein Element von $E$. Daher ist die Abbildung $E \to C^o$, $\varphi \mapsto \varphi(1)$ ein Isomorphismus von Algebren. Folglich ist $C \cong E^o$ einfach.

(ii) Es gilt $C \cong E^o \cong (D^o)^{k\times k}$ und $A \otimes B^o \cong (D^o)^{n\times n}$. Wegen $k \dim(A) \dim(B) = kn^2 \dim(D) = nk \dim(S) = n \dim(M_f) = n \dim(A)$ ist $k \mid n$.

(iii) Nun gilt

$$\begin{aligned}\dim(A) \dim(B) \dim(C) &= \dim(A \otimes B^o) \dim(E) = (nk \dim(D))^2 \\ &= \dim(k \dim(S))^2 = \dim(M_f)^2 = \dim(A)^2.\end{aligned}$$

(iv) Da $C$ einfach ist, können wir $B$ durch $C$ ersetzen und erhalten

$$\dim(C) \dim(\mathrm{C}_A(C)) = \dim(A) = \dim(C) \dim(B).$$

Wegen $B \subseteq \mathrm{C}_A(C)$ folgt $\mathrm{C}_A(C) = B$. □

**Lemma 3.10.** *Ein Teilkörper $L$ einer Divisionsalgebra $D$ ist genau dann maximal, wenn $\mathrm{C}_D(L) = L$ gilt.*

*Beweis.* Im Fall $\mathrm{C}_D(L) = L$ ist $L$ sicher maximal. Sei nun umgekehrt $L$ maximal und $c \in \mathrm{C}_D(L)$. Dann ist auch $L(c)$ ein Teilkörper von $D$ und es folgt $c \in L$. □

**Satz 3.11.** *Sei $L$ ein maximaler Teilkörper einer zentralen Divisionsalgebra $D$. Dann ist $\dim D = \dim(L)^2$ und $L \otimes D \cong L^{n\times n}$ mit $n := \dim L$.*

*Beweis.* Nach Lemma 3.10 und dem Doppel-Zentralisator-Satz gilt $\dim D = \dim(L) \dim(\mathrm{C}_D(L)) = \dim(L)^2$ und $D \otimes L \cong D \otimes L^o \cong L^{n\times n}$. Dimensionsvergleich zeigt $n = \dim L$. □

**Satz 3.12** (Wedderburn)**.** *Jeder endliche Schiefkörper ist ein Körper.*

*Beweis.* Sei $R$ ein endlicher Schiefkörper. Offenbar ist $K := \mathrm{Z}(R)$ ein Körper und $R$ wird zu einer zentralen Divisionsalgebra. Sei $L \subseteq R$ ein maximaler Teilkörper. Nach Satz 3.11 ist $\dim R = \dim(L)^2$. Insbesondere ist $|L|$ eindeutig bestimmt. Jeder weitere maximale Teilkörper $L'$ von $R$ ist als endlicher Körper dazu zu $L$ isomorph (Algebra 1). Sei $f : L \to L' \subseteq R$ ein Isomorphismus und $g : L \to R$ die Inklusionsabbildung. Nach Skolem-Noether gilt $f(x) = axa^{-1}$ für ein $x \in R^\times$, d. h. $L$ und $L'$ sind konjugiert. Jedes Element $x \in R$ erzeugt einen Teilkörper $K(x) \subseteq R$ und liegt daher in einem maximalen Teilkörper. Man hat daher eine Vereinigung von Gruppen

$$R^\times = \bigcup_{x\in R^\times} xL^\times x^{-1}.$$

Wegen $1 \in L^\times$ sind die Konjugierten nicht disjunkt. Die Anzahl der Konjugierten ist bekanntlich $|R^\times : \mathrm{N}_{R^\times}(L^\times)| \leq |R : L^\times|$. Im Fall $L \neq R$ hätte man den Widerspruch

$$|R^\times| < |L^\times||R^\times : L^\times| = |R^\times|.$$

Daher ist $R = L$ ein Körper. □

**Bemerkung 3.13.** Für jeden endlichen Körper $K$ gilt daher $\mathrm{Br}(K) = 1$.

**Satz 3.14** (Frobenius)**.** *Jede endlich-dimensionale Divisionsalgebra über* $\mathbb{R}$ *ist zu* $\mathbb{R}$*,* $\mathbb{C}$ *oder* $\mathbb{H}$ *isomorph. Insbesondere ist* $\mathrm{Br}(\mathbb{R}) = \langle[\mathbb{H}]\rangle \cong C_2$.

*Beweis.* Sei $D$ eine $\mathbb{R}$-Divisionsalgebra. Wir identifizieren $\mathbb{R}$ mit $\mathbb{R}1_D \subseteq D$ und nehmen $\mathbb{R} \neq D$ an. Sei $L \subseteq D$ ein maximaler Teilkörper und $x \in L$ ein primitives Element der separablen Körpererweiterung $\mathbb{R} \subseteq L$. Für das irreduzible Minimalpolynom $\mu \in \mathbb{R}[X]$ von $x$ gilt bekanntlich $|L : \mathbb{R}| = |\mathbb{R}(x) : \mathbb{R}| = \deg \mu = 2$ nach dem Fundamentalsatz der Algebra. Sei $\mu = X^2 + aX + b$ mit $a, b \in \mathbb{R}$. Da $\mu$ irreduzibel ist, gilt $y := D_\mu = a^2 - 4b < 0$ und

$$L = \mathbb{R}(x) = \mathbb{R}(\sqrt{y}) = \mathbb{R}\Big(\frac{\sqrt{y}}{\sqrt{-y}}\Big) = \mathbb{R}(\sqrt{-1}) \cong \mathbb{C}.$$

Wir können daher $x^2 = -1$ annehmen. Im Fall $\mathrm{Z}(D) = L$ ist $D \cong \mathbb{C}$ nach Satz 3.11. Anderenfalls ist $D$ zentral mit $\dim D = \dim(L)^2 = 4$. Nach Skolem-Noether sind $x$ und $-x$ in $D$ konjugiert. Sei also $y \in D$ mit $yx = -xy$. Dann ist $y^2 \in \mathrm{C}_D(L) \cap \mathbb{R}(y) = L \cap \mathbb{R}(y) = \mathbb{R}$. Im Fall $y^2 > 0$ wäre $y \in \mathbb{R} \subseteq L$, denn das Polynom $X^2 - y^2$ besitzt höchstens zwei Nullstellen in $\mathbb{R}(y)$. Nach Normierung können wir also $y^2 = -1$ annehmen. Wegen $y \notin L$ ist $1, x, y, xy$ eine $\mathbb{R}$-Basis von $D$ und die Multiplikationstabelle ist eindeutig bestimmt. Dies zeigt $D \cong \mathbb{H}$. □

# 4 Zerfällungskörper

**Definition 4.1.** Für eine endliche Körpererweiterung $K \subseteq L$ und eine Algebra $A$ sei $A_L := L \otimes A$. Durch

$$\lambda(x \otimes a) := (\lambda \otimes 1)(x \otimes a) = (\lambda x) \otimes a \qquad (\lambda, x \in L, a \in A)$$

wird $A_L$ zu einer $L$-Algebra. Man sagt, $A_L$ entsteht durch *Skalarerweiterung* aus $A$. Existiert ein $n \in \mathbb{N}$ mit $A_L \cong_L L^{n\times n}$, so nennt man $L$ *Zerfällungsköper* von $A$.

**Bemerkung 4.2.**

(i) Ist $a_1, \ldots, a_n$ eine Basis von $A$, so ist $1 \otimes a_1, \ldots, 1 \otimes a_n$ eine $L$-Basis von $A_L$. Insbesondere ist $\dim A = \dim_L(A_L)$.

(ii) Sei $f : A_L \to L^{n\times n}$ ein Ringisomorphismus. Einschränken von $f$ liefert einen Ringisomorphismus $L \otimes \mathrm{Z}(A) \cong \mathrm{Z}(A_L) \to \mathrm{Z}(L^{n\times n}) \cong L$. Insbesondere ist $A_L$ zentral einfach. Nach Skolem-Noether kann man $f(\lambda \otimes 1) = \lambda 1_n$ für $\lambda \in L$ annehmen. Dann ist $f$ auch ein Isomorphismus von $L$-Algebren. Für die Konstruktion von Zerfällungskörpern genügt es also Ringisomorphismen zu betrachten.

(iii) Nach Satz 3.11 besitzt jede zentrale Divisionsalgebra $D$ einen Zerfällungskörper $L$, sagen wir $D_L \cong L^{n\times n}$. Wegen $L \otimes D^{k\times k} \cong D_L^{k\times k} \cong L^{nk\times nk}$ besitzt auch jede zentral einfache Algebra einen Zerfällungskörper.

(iv) Mit $L$ ist auch jede endliche Erweiterung $M$ von $L$ ein Zerfällungskörper von $A$, denn

$$A_M = M \otimes A \cong M \otimes_L L \otimes A \cong M \otimes_L A_L \cong M \otimes_L L^{n\times n} \cong (M \otimes_L L)^{n\times n} \cong M^{n\times n}$$

(betrachte $x \otimes a \mapsto x \otimes (1 \otimes a)$ für $x \in M$ und $a \in A$).

**Satz 4.3.** *Für jede endliche Körpererweiterung $K \subseteq L$ ist die Abbildung*

$$\mathrm{Br}(K) \to \mathrm{Br}(L), \qquad [A] \mapsto [A_L]$$

*ein wohldefiniert Homomorphismus. Sein Kern bezeichnet man mit* $\mathrm{Br}(L|K)$.

*Beweis.* Sei $A$ eine zentral einfache $K$-Algebra. Nach Lemma 2.7 ist $A_L$ einfach und nach Lemma 2.5 ist $\mathrm{Z}(A_L) \cong \mathrm{Z}(A) \otimes L \cong K \otimes L \cong L$. Also ist $[A_L] \in \mathrm{Br}(L)$. Sei $[A] = [B]$ mit $A \cong D^{n\times n}$ und $B \cong D^{m\times m}$ für eine Divisionsalgebra $D$. Dann ist $A_L = L \otimes D^{n\times n} \cong D_L^{n\times n}$ nach Lemma 2.6. Wie bereits gezeigt, ist $D_L$ eine einfache $L$-Algebra. Also existiert eine Divisionsalgebra $E$ mit $D_L \cong E^{k\times k}$ und es folgt $A_L \cong E^{nk\times nk}$ sowie $B_L \cong E^{mk\times mk}$. Daher ist $[A_L] = [B_L]$. Für $[A], [B] \in \mathrm{Br}(K)$ gilt schließlich

$$(A \otimes B)_L = L \otimes A \otimes B \cong A \otimes (L \otimes_L L) \otimes B \cong (A \otimes L) \otimes_L (L \otimes B) \cong A_L \otimes_L B_L$$

(betrachte $x \otimes a \otimes b \to (x \otimes a) \otimes (1 \otimes b)$ für $x \in L$, $a \in A$, $b \in B$). Dies zeigt $[A_L][B_L] = [(A \otimes B)_L]$. □

**Bemerkung 4.4.** Nach Bemerkung 4.2 gilt

$$\mathrm{Br}(K) = \bigcup_{\substack{L \supseteq K,\\ |L:K|<\infty}} \mathrm{Br}(L|K).$$

**Satz 4.5** (Noether)**.** *Jede zentrale Divisionsalgebra $D$ besitzt einen maximalen Teilkörper $L$, sodass $K \subseteq L$ separabel ist.*

*Beweis.* Wir argumentieren durch Induktion nach $\dim(D)$. Dabei können wir $D \neq K$ und $\operatorname{char} K = p > 0$ annehmen. Ist jedes Element aus $D$ separabel über $K$, so folgt die Behauptung aus Satz 3.11. Sei nun $x \in D \setminus K$ inseparabel mit Minimalpolynom $\mu$. Wegen $\mu' = 0$ existiert ein irreduzibles Polynom $\nu \in K[X]$ mit $\mu(X) = \nu(X^p)$. Dann ist $\nu$ das Minimalpolynom von $x^p$. Ist auch $x^p$ inseparabel, so können wir $x^{p^2}$ betrachten usw. Am Ende erhalten wir ein inseparables Element $x \in D$, sodass $x^p$ separabel ist. Nehmen wir $x^p \in K$ an und betrachten die Abbildung $\delta : D \to D$, $d \mapsto dx - xd$. Wegen $x \notin K = \mathrm{Z}(D)$, existiert ein $y \in D$ mit $\delta(y) \neq 0$. Mit Induktion nach $k \geq 0$ erhält man

$$\delta^k(y) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} x^i y x^{k-i}.$$

Insbesondere ist

$$\delta^p(y) = yx^p - x^p y = 0$$

wegen $x^p \in K$. Sei $m \in \mathbb{N}$ minimal mit $\delta^m(y) \neq 0$ und sei $z := \delta^{m-1}(y)$ sowie $w := \delta^{m-2}(y)$. Dann ist $z = \delta(w) = wx - xw$. Setze $u := x^{-1}z$. Wegen $\delta(z) = 0$ ist $ux = xu$. Es folgt

$$x = zu^{-1} = (wx - xw)u^{-1} = wxu^{-1} - xwu^{-1} = (wu^{-1})x - x(wu^{-1}).$$

Für $a := wu^{-1}$ gilt also $x = ax - xa$ und $a = 1 + xax^{-1}$. Wie zu Beginn des Beweises existiert eine Potenz $p^n = q$, sodass $a^q$ separabel ist. Nun ist aber $a^q = 1 + xa^q x^{-1}$. Insbesondere sind $x$ und $a^q$ nicht vertauschbar und es folgt $a^q \notin K$. Damit haben wir ein separables Element $a \in D \setminus K$ gefunden.

Sei $M := K(a)$ und $C := \mathrm{C}_D(M)$. Offenbar ist $C$ eine Divisionsalgebra und nach Satz 3.9 ist $M \subseteq \mathrm{Z}(C) \subseteq \mathrm{C}_D(C) = M$. Also ist $C$ zentral über $M$ mit $\dim_M(C) < \dim_K(D)$. Nach Induktion besitzt $C$ einen maximalen Teilkörper $L$, der separabel über $M$ ist. Bekanntlich ist $L$ dann auch separabel über $K$. Außerdem ist $\dim_M(C) = \dim_M(L)^2$. Nach Satz 3.9 ist

$$\dim(D) = \dim(M)\dim(C) = \dim_M(C)\dim(M)^2 = \dim_M(L)^2\dim(M)^2 = \dim(L)^2.$$

Nach Satz 3.11 ist $L$ also auch ein maximaler Teilkörper von $D$. □

**Folgerung 4.6.** *Jede zentral einfache Algebra besitzt einen Zerfällungskörper $L$, sodass $K \subseteq L$ eine Galoiserweiterung ist.*

*Beweis.* Es genügt die Behauptung für zentrale Divisionsalgebren $D$ zu beweisen. Nach Satz 4.5 existiert ein maximaler Teilkörper $L \subseteq D$, sodass $K \subseteq L$ separabel ist. Bekanntlich liegt jede separable Erweiterung in einer Galois-Erweiterung $K \subseteq M$. Nun ist auch $M$ ein Zerfällungskörper von $D$. □

**Definition 4.7.** In der Situation von Satz 4.5 heißt $L$ ein *Galois-Zerfällungskörper* von $A$.

**Lemma 4.8.** *Sei $L$ ein Zerfällungskörper einer zentralen Divisionsalgebra $D$. Dann ist $L$ zu einer Unteralgebra von $D^{n\times n}$ isomorph, wobei $\dim(L)^2 = n^2\dim(D)$ ist.*

*Beweis.* Sei $D_L \cong L^{k\times k}$ und sei $S \simeq L^{k\times 1}$ der einfache $D_L$-Modul. Wie üblich ist dann $S$ ein $L$- und ein $D$-Vektorraum. Die Skalarmultiplikation von $L$ bewirkt einen Algebrenhomomorphismus $f : L \to \mathrm{End}_D(S)$, der injektiv ist, da $L$ einfach ist. Da $S$ über $D$ eine Basis besitzt, gilt $\mathrm{End}_D(S) \cong D^{n\times n}$ mit $n := \dim_D(S)$. Nun ist $\dim(D)\dim(L) = \dim(D_L) = k^2\dim(L)$ und $k\dim(L) = \dim(S) = \dim_D(S)\dim(D) = nk^2$. Es folgt $\dim(L)^2 = n^2k^2 = n^2\dim(D)$. □

# 5 Faktorensysteme

**Definition 5.1.** Sei $K \subseteq L$ eine Galois-Erweiterung und $G := \mathrm{Gal}(L|K)$. Sei $C^n(G, L^\times)$ Gruppe aller Abbildung $G^n \to L^\times$ bzgl. komponentenweiser Verknüpfung. Ein $\gamma \in C^2(G, L^\times)$ heißt *Faktorensystem* (oder 2-*Kozyklus*), falls

$$\gamma(g,h)\gamma(gh,k) = g(\gamma(h,k))\gamma(g,hk) \qquad \forall g,h,k \in G. \tag{5.1}$$

Die Menge aller Faktorensysteme bildet eine Untergruppe $Z^2(G, L^\times) \leq C^2(G, L^\times)$.

**Lemma 5.2.** *Die Abbildung $\partial : C^1(G, L^\times) \to Z^2(G, L^\times)$ mit $\partial\lambda(g,h) = \lambda(g)g(\lambda(h))\lambda(gh)^{-1}$ für $\lambda \in C^1(G, L^\times)$ und $g, h \in G$ ist ein Homomorphismus.*

*Beweis.* Für $g, h, k \in G$ gilt

$$\begin{aligned}\partial\lambda(g,h)\partial\lambda(gh,k) &= \lambda(g)g(\lambda(h))\lambda(gh)^{-1}\lambda(gh)(gh)(\lambda(k))\lambda(ghk)^{-1}\\ &= g(\lambda(h)h(\lambda(k))\lambda(hk)^{-1})\lambda(g)g(\lambda(hk))\lambda(ghk)^{-1} = g(\partial\lambda(h,k))\partial\lambda(g,hk).\end{aligned}$$

Daher bildet $\partial$ nach $Z^2(G, L^\times)$ ab. Die Homomorphie ist offensichtlich. □

**Definition 5.3.** Man setzt $B^2(G, L^\times) := \partial(C^1(G, L^\times))$ und nennt $\mathrm{H}^2(G, L^\times) := Z^2(G, L^\times)/B^2(G, L^\times)$ die *zweite Kohomologiegruppe* von $G$ mit Werten in $L^\times$.

**Lemma 5.4.** *Für $\gamma \in Z^2(G, L^\times)$ und $g \in G$ gilt $\gamma(1, g) = \gamma(1, 1)$ und $g(\gamma(1, 1)) = \gamma(g, 1)$. Jedes Element von $\mathrm{H}^2(G, L^\times)$ enthält ein* normalisiertes *Faktorensystem $\gamma$ mit $\gamma(1, g) = \gamma(g, 1) = 1$ für alle $g \in G$.*

*Beweis.* Setzt man $g = h = 1$ in (5.1), so folgt $\gamma(1, 1)\gamma(1, k) = \gamma(1, k)\gamma(1, k)$. Setzt man $h = k = 1$, so ergibt sich $\gamma(g, 1)\gamma(g, 1) = g(\gamma(1, 1))\gamma(g, 1)$. Für die zweite Behauptung ersetzt man $\gamma$ durch $\gamma\partial\lambda$ mit $\lambda(g) := \gamma(1, 1)^{-1}$. □

**Definition 5.5.** Sei $D$ eine zentrale Divisionsalgebra mit Galois-Zerfällungskörper $L$. Nach Lemma 4.8 lässt sich $L$ in die zentral einfache Algebra $A := D^{n\times n}$ einbetten. Dabei gilt $\dim(A) = \dim(L)^2$. Nach dem Doppel-Zentralisator-Satz ist $L$ ein maximaler Teilkörper von $A$. Insbesondere ist $\mathrm{C}_A(L) = L$. Sei $G := \mathrm{Gal}(L|K)$ und $g \in G$. Nach Skolem-Noether lässt sich $g$ zu einem inneren Automorphismus von $A$ fortsetzen. Sei $a_g \in A^\times$ mit $g(x) = a_g x a_g^{-1}$ für alle $x \in L$. Wegen $\mathrm{C}_A(L) = L$ ist $a_g$ bis auf $L$-Multiplikation eindeutig bestimmt. Ist auch $h \in G$, so gilt

$$a_{gh} x a_{gh}^{-1} = (gh)(x) = g(h(x)) = a_g a_h x a_h^{-1} a_g^{-1}.$$

Daher ist $a_g a_h = \gamma(g, h) a_{gh}$ mit $\gamma(g, h) \in L^\times$.

**Lemma 5.6.** *Die Abbildung $\gamma : G \times G \to L^\times$ ist ein Faktorensystem. Die induzierte Nebenklasse $\overline{\gamma} \in \mathrm{H}^2(G, L^\times)$ hängt nicht von der Wahl der $a_g$ ab.*

*Beweis.* Seien $g, h, k \in G$ und $x \in A$. Dann ist

$$\begin{aligned}\gamma(g, h)\gamma(gh, k)a_{ghk} &= \gamma(g, h)a_{gh}a_k = (a_g a_h)a_k = a_g(a_h a_k) = a_g\gamma(h, k)a_{hk}\\ &= g(\gamma(h, k))a_g a_{hk} = g(\gamma(h, k))\gamma(g, hk)a_{ghk}.\end{aligned}$$

Dies zeigt $\gamma \in \mathrm{Z}^2(G, L^\times)$. Sei nun $\lambda : G \to L^\times$ mit $a'_g = \lambda(g)a_g$ und $a'_g a'_h = \gamma'(g, h)a'_{gh}$. Dann folgt

$$\gamma'(g, h)\lambda(gh)a_{gh} = \gamma'(g, h)a'_{gh} = a'_g a'_h = \lambda(g)a_g\lambda(h)a_h = \lambda(g)g(\lambda(h))\gamma(g, h)a_{gh}$$

und $\gamma'(g, h) = \gamma(g, h)\lambda(g)g(\lambda(h))\lambda(gh)^{-1}$. Dies zeigt $\gamma' = \gamma\partial_\lambda$. □

**Definition 5.7.** Sei $K \subseteq L$ eine Galois-Erweiterung, $G := \mathrm{Gal}(L|K)$ und $\gamma \in \mathrm{Z}^2(G, L^\times)$. Wir definieren die *verschränkte Gruppenalgebra* $L_\gamma G$ als $K$-Vektorraum $LG$ mit der Multiplikation

$$\lambda_g g \cdot \lambda_h h := \lambda_g g(\lambda_h)\gamma(g, h)gh \qquad (g, h \in G, \lambda_g, \lambda_h \in L).$$

**Satz 5.8.** *Mit den Bezeichnungen aus Definition 5.7 ist $L_\gamma G$ eine zentral einfache $K$-Algebra mit Zerfällungskörper $L$.*

*Beweis.* Für $g, h, k \in G$ gilt

$$\begin{aligned}(\lambda_g g \cdot \lambda_h h) \cdot \lambda_k k &= \lambda_g g(\lambda_h)\gamma(g, h)gh \cdot \lambda_k k = \lambda_g g(\lambda_h)\gamma(g, h)(gh)(\lambda_k)\gamma(gh, k)ghk\\ &= \lambda_g g(\lambda_h h(\lambda_k))g(\gamma(h, k))\gamma(g, hk)ghk = \lambda_g g \cdot \lambda_h h(\lambda_k)\gamma(h, k)hk\\ &= \lambda_g g \cdot (\lambda_h h \cdot \lambda_k k)\end{aligned}$$

Dies zeigt die Assoziativität der Multiplikation in $A := L_\gamma G$. Das Einselement ist $e := \gamma(1,1)^{-1}1$, denn nach Lemma 5.4 gilt $eg = \gamma(1,1)^{-1}\gamma(1,g)g = g$ sowie $ge = g(\gamma(1,1))^{-1}\gamma(g,1)g = g$ für alle $g \in G$. Somit wird $A$ eine $K$-Algebra. Sei $x := \sum_{g\in G} \lambda_g g \in \mathrm{Z}(A)$. Für $\mu \in L$ ist

$$\sum_{g\in G} \mu\lambda_g g = \mu x = x\mu = \sum_{g\in G} \lambda_g g(\mu) g.$$

Im Fall $\lambda_g \neq 0$ ist daher $g(\mu) = \mu$ für alle $\mu \in L$. Dies zeigt $x = \lambda_1$ und $\mathrm{C}_A(L) = L$. Außerdem ist

$$g(\lambda_1)g = gx = xg = \lambda_1 g$$

für alle $g \in G$. Daher ist $\lambda_1 \in L^G = K$ und $\mathrm{Z}(A) = K$.

Sei nun $0 \neq I \trianglelefteq A$. Wir wählen $x = \sum_{g\in G} \lambda_g g \in I \setminus \{0\}$, sodass möglichst viele $\lambda_g$ verschwinden. Nach Multiplikation mit einem $g \in G$ können wir $\lambda_1 \neq 0$ annehmen. Sei $\mu \in L$ beliebig. Dann gilt

$$I \ni x\mu - \mu x = \sum_{g\in G\setminus\{1\}} (\lambda_g g(\mu) - \mu\lambda_g)g$$

und es folgt $x\mu = \mu x$. Daher ist $x \in \mathrm{C}_A(L) = L$. Insbesondere ist $x$ invertierbar und man erhält $I = A$. Also ist $A$ einfach.

Nach dem Doppel-Zentralisator-Satz ist $L \otimes A \cong A \otimes \mathrm{C}_A(L)^o \cong L^{n\times n}$. Somit ist $L$ ein Zerfällungskörper von $A$. □

**Lemma 5.9.** *Für $\gamma, \delta, \in \mathrm{Z}^2(G, L^\times)$ gilt $L_\gamma G \cong L_\delta G$ genau dann, wenn $\gamma \equiv \delta \pmod{B^2(G, L^\times)}$.*

*Beweis.* Sei $A := L_\gamma G$, $B := L_\delta G$ und $f : A \cong B$. Offenbar ist $L \to A$, $\lambda \mapsto \gamma(1,1)^{-1}\lambda 1$ ein Monomorphismus. Wir können daher $L$ als Teilkörper von $A$ und $B$ auffassen. Nach Skolem-Noether können wir dann $f(\lambda) = \lambda$ für alle $\lambda \in L$ annehmen. Für $g \in G$ gilt

$$f(g)\lambda = f(g\lambda) = f(g(\lambda)g) = g(\lambda)f(g).$$

Dies zeigt $f(g) = \mu(g)g$ für $\mu(g) \in \mathrm{C}_B(L) = L$. Nun ist

$$\begin{aligned}\gamma(g,h)\mu(gh)gh = \gamma(g,h)f(gh) = f(\gamma(g,h)gh) = f(g\cdot h) = f(g)\cdot f(h)\\ = \mu(g)g\cdot\mu(h)h = \mu(g)g(\mu(h))\delta(g,h)gh,\end{aligned}$$

also $\gamma = \delta\partial\mu$.

Sei umgekehrt $\gamma = \delta\partial\mu$ mit $\mu \in C^1(G, L^\times)$. Wir betrachten die lineare Abbildung $f : A \to B$, $\lambda g \mapsto \lambda\mu(g)g$ für $g \in G$ und $\lambda \in L$. Wegen $\gamma(1,1) = \delta(1,1)\mu(1)1(\mu(1))\mu(1)^{-1} = \delta(1,1)\mu(1)$ gilt $f(1_A) = f(\gamma(1,1)^{-1}1) = \gamma(1,1)^{-1}\mu(1) = \delta(1,1)^{-1}1 = 1_B$. Für $g, h \in G$ und $\lambda_g, \lambda_h \in L$ ist

$$\begin{aligned}f(\lambda_g g\cdot\lambda_h h) &= f(\lambda_g g(\lambda_h)\gamma(g,h)gh) = \lambda_g g(\lambda_h)\gamma(g,h)\mu(gh)gh\\ &= \lambda_g g(\lambda_h)\delta(g,h)\mu(g)g(\mu(h))gh = \lambda_g\mu(g)g\cdot\lambda_h\mu(h)h = f(\lambda_g g)\cdot f(\lambda_h h).\end{aligned}$$

Also ist $f$ ein Homomorphismus. Da $A$ einfach ist, ist $f$ injektiv. Wegen $\dim A = \dim B$ ist $f$ auch surjektiv. □

**Satz 5.10.** *Für jede Galois-Erweiterung $K \subseteq L$ mit $G := \mathrm{Gal}(L|K)$ ist*

$$\begin{aligned}\Gamma : \mathrm{H}^2(G, L^\times) &\to \mathrm{Br}(L|K),\\ \gamma &\mapsto [L_\gamma G]\end{aligned}$$

*ist ein Isomorphismus.*

*Beweis.* Nach Satz 5.8 und Lemma 5.9 ist $\Gamma$ wohldefiniert. Sei $D$ eine zentrale Divisionsalgebra mit Zerfällungskörper $L$. Wie in Definition 5.5 ist $L$ zu einer Unteralgebra von $A := D^{n\times n}$ isomorph und man erhält $a_g \in A^\times$ und $\gamma \in Z^2(G, L^\times)$ mit $g(x) = a_g x a_g^{-1}$ und $a_g a_h = \gamma(g,h)a_{gh}$ für $g, h \in G$ und $x \in L$. Daher ist $f : L_\gamma G \to A$, $\lambda g \mapsto \lambda a_g$ ein Homomorphismus von Algebra. Da $L_\gamma G$ einfach ist, ist $f$ surjektiv. Nach Lemma 4.8 ist

$$\dim(L_\gamma G) = \dim(L)|G| = \dim(L)|L : K| = \dim(L)^2 = n^2 \dim(D) = \dim(A).$$

Also ist $f$ ein Isomorphismus und $\Gamma$ ist surjektiv.

Seien nun $\gamma, \delta \in \mathrm{Z}^2(G, L^\times)$, $A := L_\gamma G$, $B := L_\delta G$ und $C := L_{\gamma\delta} G$. Nach Lemma 5.4 können wir $\gamma(1,1) = \delta(1,1) = 1$ annehmen. Das neutrale Element von $G$ ist dann das Einselement in $A$, $B$ und $C$. Wir dürfen also $L$ als Unteralgebra von $A$, $B$ und $C$ auffassen. Wir betrachten die $K$-Vektorräume $U := \langle \lambda a \otimes b - a \otimes \lambda b : a \in A, b \in B, \lambda \in L\rangle$ und

$$V := (A \otimes B)/U$$

(es gilt $V \cong A \otimes_L B$). Offenbar ist $U$ ein Untermodul des regulären $A \otimes B$-Rechtsmoduls. Daher ist $V$ ein $(A \otimes B)^o$-Linksmodul. Sei $n := \dim L = |G|$. Seien $a_1, \dots, a_{n^2} \in A$ und $b_1, \dots, b_{n^2} \in B$ $K$-Basen von $A$ bzw. $B$. Für $\lambda_g g \in C$ mit $\lambda_g \in L$, $g \in G$ definieren wir

$$(\lambda_g g)(a_i \otimes b_j) := \lambda_g g a_i \otimes g b_j.$$

Für $\mu \in L$ ist

$$(\lambda_g g)(\mu a_i \otimes b_j - a_i \otimes \mu b_j) = \lambda_g g(\mu) g a_i \otimes g b_j - \lambda_g g a_i \otimes g(\mu) g b_j = g(\mu)(\lambda_g g a_i) \otimes g b_j - \lambda_g g a_i \otimes g(\mu) g b_j \in U.$$

Für $\lambda_h h \in C$ gilt

$$\begin{aligned}(\lambda_g g \cdot \lambda_h h)(a_i \otimes b_j) &= (\lambda_g g(\lambda_h)\gamma(g,h)\delta(g,h)gh)(a_i \otimes b_j) = \lambda_g g(\lambda_h)\gamma(g,h)\delta(g,h)gha_i \otimes ghb_j \\ &\equiv \lambda_g g(\lambda_h)\gamma(g,h)gha_i \otimes \delta(g,h)ghb_j \equiv (\lambda_g g)(\lambda_h h a_i \otimes hb_j) \\ &\equiv (\lambda_g g)((\lambda_h h)(a_i \otimes b_j)) \pmod U.\end{aligned}$$

Durch lineare Fortsetzung wird wird $V$ zu einem $C$-Modul. Da die beiden Operationen kommutieren, erhält man einen Homomorphismus $f : (A \otimes B)^o \to \mathrm{End}_C(V)$. Da $A \otimes B$ einfach ist, ist $f$ injektiv.

Offenbar bilden die Elemente der Form $a_i \otimes g$ mit $1 \le i \le n^2$ und $g \in G$ eine $K$-Basis von $V$. Dies zeigt $\dim V = n^3$. Sei $C \simeq S^r$ die Zerlegung des regulären $C$-Moduls mit den einfachen Modul $S$ der einfachen Algebra $C$. Wegen $n^2 = \dim C = r \dim S$ folgt $V \simeq S^{nr}$. Nach Wedderburn ist $\mathrm{End}_C(V) \cong D^{nr\times nr}$ mit der Divisionsalgebra $D := \mathrm{End}_C(S)$. Außerdem ist $n^2 = \dim C^o = \dim \mathrm{End}_C(C) = r^2 \dim D$. Dies zeigt

$$\dim(A \otimes B)^o = n^4 = n^2 r^2 \dim D = \dim \mathrm{End}_C(V).$$

Daher ist $f$ ein Isomorphismus. Insbesondere ist $A \otimes B \cong (D^o)^{nr\times nr}$ sowie $C \cong (D^o)^{r\times r}$. Dies liefert $[A] \cdot [B] = [C]$, d. h. $\Gamma$ ist ein Epimorphismus.

Für die Injektivität betrachten wir das triviale Faktorensystem $\gamma =: 1$ mit $\gamma(g,h) = 1$ für alle $g, h \in G$. Dann besitzt $A := L_1 G$ den einfachen Untermodul $S := Le$ mit $e := \sum_{g\in G} g$. Daher ist $A \cong \mathrm{End}_A(S^n)^o \cong (\mathrm{End}_A(S)^o)^{n\times n}$ und $\mathrm{End}_A(S)^o \cong K$ aus Dimensionsgründen. Also ist $\Gamma(1) = 1$. Sei nun $\gamma \in Z^2(G, L^\times)$ mit $\Gamma(\gamma) = 1$. Dann ist $L_\gamma G \cong K^{n\times n} \cong L_1 G$ und Lemma 5.9 zeigt $\gamma \equiv 1 \pmod{B^2(G, L^\times)}$. □

**Satz 5.11.** *Für $\overline{\gamma} \in \mathrm{H}^2(G, L^\times)$ ist $\overline{\gamma}^{|G|} = 1$. Insbesondere ist $\mathrm{Br}(K)$ eine Torsionsgruppe.*

*Beweis.* Sei $\delta(g) := \prod_{x\in G} \gamma(g,x)$ für $g \in G$. Nach (5.1) ist

$$\gamma(g,h)^{|G|}\delta(gh) = \prod_{x\in G} \gamma(g,h)\gamma(gh,x) = \prod_{x\in G} g(\gamma(h,x))\gamma(g,hx) = g(\delta(h))\delta(g).$$

Dies zeigt $\gamma^{|G|} = \partial\delta \in B^2(G, L^\times)$. Die zweite Behauptung folgt aus Satz 5.10. □

**Definition 5.12.** Aus Satz 3.11 folgt, dass die Dimension einer zentral einfachen Algebra $A$ stets ein Quadrat ist. Man nennt $\deg A := \sqrt{\dim A}$ den *Grad* von $A$. Ist $D$ eine Divisionsalgebra mit $A \cong D^{n\times n}$, so nennt man $e(A) := \deg(D)$ den *Index* von $A$ (nach Wedderburn ist dies wohldefiniert).

**Bemerkung 5.13.** Für eine zentrale Divisionsalgebra $D$ mit Zerfällungskörper $L$ gilt $\deg D \mid \dim L$ nach Lemma 4.8. Der folgende Satz verbessert daher Satz 5.11.

**Satz 5.14.** *Für* $[A] \in \mathrm{Br}(K)$ *gilt* $[A]^{e(A)} = 1$.

*Beweis.* Wir können annehmen, dass $A = D$ eine Divisionsalgebra mit $e := e(A) = \deg(D)$ ist. Sei $L$ ein Galois-Zerfällungskörper von $D$. Wie in Definition 5.5 können wir $L$ in $A := D^{n\times n}$ einbetten. Dabei gilt $(ne)^2 = n^2 \dim D = \dim A = \dim(L)^2$ und $\dim L = ne$. Sei $G := \mathrm{Gal}(L|K)$. Dann existieren $a_g \in A^\times$ mit $g(\lambda) = a_g \lambda a_g^{-1}$ und $a_g a_h = \gamma(g,h)gh$ für $g,h \in G$, $\lambda \in L$ und $\gamma \in C^2(G, L^\times)$. Sei $S = D^{n\times 1}$ der einfache $A$-Modul. Durch Einschränkung wird $S$ ein $L$-Vektorraum. Dabei gilt

$$\dim_L(S) = \frac{\dim S}{\dim L} = \frac{n \dim D}{ne} = e.$$

Sei $v_1, \ldots, v_e$ eine $L$-Basis von $S$. Für $g \in G$ sei $\alpha(g) = (\alpha_{ij}(g)) \in L^{e\times e}$ mit

$$a_g v_i = \sum_{j=1}^{e} \alpha_{ij}(g) v_j.$$

Für $g,h \in G$ gilt dann

$$\begin{aligned}\gamma(g,h)\sum_{j=1}^{e} \alpha_{ij}(gh)v_j = \gamma(g,h)a_{gh}v_i = a_g a_h v_i = a_g\Big(\sum_{k=1}^{e} \alpha_{ik}(h)v_k\Big)\\ = \sum_{k=1}^{e} g(\alpha_{ik}(h))a_g v_k = \sum_{k,j=1}^{e} g(\alpha_{ik}(h))\alpha_{kj}(g)v_j.\end{aligned}$$

Dies zeigt $\gamma(g,h)\alpha(gh) = g(\alpha(h))\alpha(g)$ für alle $g,h \in G$. Sei schließlich $\lambda(g) := \det(\alpha(g))$. Dann folgt

$$\gamma(g,h)^e\lambda(g) = \det(\gamma(g,h)\alpha(gh)) = \det(g(\alpha(h)))\det(\alpha(g)) = g(\lambda(h))\lambda(g).$$

Also ist $\gamma^e = \partial\lambda \in B^2(G, L^\times)$ und die Behauptung folgt aus Satz 5.10. □