The Brauer group of a field

Javan Peykar, A.

Abtien Javanpeykar

The Brauer group of a field

Bachelor's thesis, September 6, 2011

Thesis advisor: prof.dr. H.W. Lenstra

Mathematisch Instituut, Universiteit Leiden

Contents

Introduction

In this thesis we study a group, defined in 1929 by Richard Brauer (1901–1977), that classifies central simple algebras (see Definition 1.38) over a given field. Examples of central simple algebras over a field k are division rings for which a ring isomorphism between the center and k is given and the underlying k-vector space is finite-dimensional, as are the $n \times n$-matrix rings over these division rings for $n \in \mathbb{Z}_{>0}$. The ring of quaternions $\mathbb{H}$, introduced by William Hamilton (1805–1865), is a central simple algebra over $\mathbb{R}$, but $\mathbb{C}$ is not, since its center is not $\mathbb{R}$.

Let k be a field. Define $\mathrm{CSA}(k)$ as the class of all central simple algebras over k, and observe that $\mathrm{CSA}(k)$ is not empty, since k and the matrix rings $\mathrm{M}_n(k)$, for $n \in \mathbb{Z}_{>0}$, are central simple over k. We say that two central simple algebras A and B over k are *similar* if there exist positive integers m and n such that $\mathrm{M}_m(A)$ is isomorphic as a k-algebra to $\mathrm{M}_n(B)$. This defines an equivalence relation on $\mathrm{CSA}(k)$, which reduces to k-algebra isomorphism when the two central simple algebras have the same k-dimension.

Theorem 1. *Let k be a field. Then there exists a pair (G, s) consisting of a group G and a surjective map $s\colon \mathrm{CSA}(k) \to G$ that for every two central simple k-algebras A and B satisfies:* (i) *the equality $s(A \otimes_k B) = s(A) \cdot s(B)$ holds;* (ii) *the equality $s(A) = s(B)$ holds if and only if A and B are similar. Moreover, the pair (G, s) is uniquely determined up to isomorphism, that is, if (G', s') is another pair satisfying the above, then there is a unique group isomorphism $\sigma\colon G \to G'$ such that we have $s' = \sigma \circ s$.*

The group of the uniquely determined pair (G, s), written multiplicatively, is called the Brauer group of k, denoted by $\mathrm{Br}(k)$. Moreover, for a central simple algebra A over k we denote $s(A)$ by $[A]$. For the proof of Theorem 1 see section 1 of Chapter 2.

The Brauer group of a finite field is trivial, as shown by Joseph Wedderburn (1882–1948). The Brauer group of an algebraically closed field is also trivial. Moreover, a theorem of Ferdinand Frobenius (1849–1917) showed that $\mathbb{R}$ and $\mathbb{H}$ are the only central simple algebras over $\mathbb{R}$ that are division rings. Consequently, the Brauer group of $\mathbb{R}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

For an algebra A over k we define the opposite algebra A° as the opposite ring of A (see Definition 1.4) with the same k-structure map as A. If A is a central simple algebra over k, then the opposite algebra A° of A is also central simple over k.

Theorem 2. *Let k be a field. Then the following statements hold.*

(i) *The unit element of* $\mathrm{Br}(k)$ *is* $[k]$.

(ii) *For every A in* $\mathrm{CSA}(k)$ *the equality* $[A^{\circ}] = [A]^{-1}$ *holds in* $\mathrm{Br}(k)$.

(iii) *The group* $\mathrm{Br}(k)$ *is abelian.*

(iv) *All elements of* $\mathrm{Br}(k)$ *have finite order.*

(v) *If k is perfect of characteristic p with p a prime number, then every element of* $\mathrm{Br}(k)$ *has order not divisible by p.*

For a proof of (i), (ii) and (iii) see section 1 of Chapter 2, and for a proof of (iv) see section

Chapter 3. A proof of (v) can be found in section 1 of Chapter 3.

Let $f\colon k \to l$ be a field homomorphism, and let A be a central simple algebra over k. Then the extended algebra $A \otimes_k l$ is the l-algebra obtained by extension of scalars via f, usually denoted by A_f, or by A_l when the map f is understood. If k is of characteristic p, with p a prime number, an important example is the k-algebra $A \otimes_k k$ obtained via the Frobenius endomorphism $\mathrm{Frob}_k\colon k \to k$ given by $x \mapsto x^p$, denoted by A_{Frob_k}.

Furthermore, we let **Fld** denote the category of fields with the morphisms given by field homomorphisms, and let **Ab** denote the category of abelian groups with morphisms given by group homomorphisms. Then the following theorem shows that the Brauer group is covariantly functorial.

Theorem 3. *The following statements hold.*

(i) *For each field homomorphism $f\colon k \to l$ there is a unique group homomorphism $\mathrm{Br}(f)\colon \mathrm{Br}(k) \to \mathrm{Br}(l)$ that satisfies $[A] \mapsto [A_f]$.*

(ii) *The Brauer group defines a covariant functor $\mathrm{Br}\colon \mathbf{Fld} \to \mathbf{Ab}$ that maps a field k to $\mathrm{Br}(k)$ and maps a field homomorphism f to $\mathrm{Br}(f)$.*

(iii) *Let k be a field of characteristic p, with p a prime number. Then the group homomorphism $\mathrm{Br}(\mathrm{Frob}_k)\colon \mathrm{Br}(k) \to \mathrm{Br}(k)$ is given by $b \mapsto b^p$.*

For a proof of (i) and (ii) see section 3 of Chapter 2, and for a proof of (iii) see section 1 of Chapter 3.

The proof of Theorem 2(iv) uses a cohomological description of the Brauer group. This description is obtained via so-called relative Brauer groups.
Let $f\colon k \to l$ be a field extension. The kernel of $\mathrm{Br}(f)$ is called the *relative Brauer group* of the field extension $l \supset k$, denoted by $\mathrm{Br}(l/k)$. If A is a central simple algebra over k such that $[A]$ is contained in $\mathrm{Br}(l/k)$, then we say that l *splits* the central simple k-algebra A or that l is a *splitting field* for A. In the case that $l \supset k$ is a Galois field extension, then $\mathrm{Br}(l/k)$ is isomorphic as a group to the second Galois cohomology group $\mathrm{H}^2(\mathrm{Gal}(l/k), l^*)$ of the field extension $l \supset k$ with coefficients in l^*. In particular, a separable closure k_{sep} of k splits all central simple algebras over k. Hence, $\mathrm{Br}(k)$ is isomorphic as a group to $\mathrm{H}^2(\mathrm{Gal}(k_{\mathrm{sep}}/k), k_{\mathrm{sep}}^*)$. This will be shown in section 4 of Chapter 2.

We define the degree of an arbitrary field homomorphism $f\colon k \to l$ as the dimension of l as a vector space over $\mathrm{im}(f)$, denoted by $\deg(f)$. Furthermore, we let $\mathbf{Fld}_{\mathrm{f}}$ denote the category of fields with the morphisms given by the field homomorphisms of finite degree.

Theorem 4. *There exists a contravariant functor $\mathrm{Br}^{\mathrm{o}}\colon \mathbf{Fld}_{\mathrm{f}} \to \mathbf{Ab}$ that maps a field k to $\mathrm{Br}(k)$ such that for every morphism $f\colon k \to l$ in $\mathbf{Fld}_{\mathrm{f}}$ and every $b \in \mathrm{Br}(k)$ the equality $(\mathrm{Cor}(f) \circ \mathrm{Br}(f))(b) = b^{\deg(f)}$ holds.*

An outline of the proof of this theorem will be given in Chapter 3.

This thesis is organized as follows.

In Chapter 1 our focus is the theory of central simple algebras over a field. We begin by introducing algebras over arbitrary commutative rings and some examples of algebras, namely endomorphism algebras and matrix algebras, and study tensor products of algebras. Moreover, a brief explanation of the theory of semisimple rings and modules, and its connection with central simple algebras is given. The technique of changing the base ring of an algebra is introduced, and more properties of central simple algebras are proven. Then splitting fields are studied, including strictly maximal subfields of a central simple algebra. We will conclude the chapter with the Skolem-Noether theorem.

In Chapter 2 we will construct the Brauer group in the classical way. Furthermore, examples of Brauer groups are given, including the Brauer group of a quasi-algebraically closed field (Definition 2.6). The functorial property of the Brauer group is treated briefly, which is followed by the study of relative Brauer groups. Then crossed product algebras are studied, and we conclude the chapter by giving the cohomological description of the Brauer group.

In Chapter 3 our goal is to prove that the Brauer group is torsion. We study the corestriction map for finite separable field extensions, and extend it to arbitrary finite field extensions. This will include the study of the p-power of elements of the Brauer group, for p a prime number. We use this map to prove that the Brauer group is torsion. We will conclude the chapter by a brief study of the exponent and index of an element of the Brauer group, and give a decomposition theorem for central division algebras.

The assumed knowledge in this thesis includes a firm understanding of the tensor product theory of modules and the basics of category theory. For the first we refer to [Lan02, Chapter 6] or [AM69, Chapter 2], as for the second we refer to [Mac98, Chapter 1 and Chapter 2] or [Lan02, Chapter 1, section 11]. For section 5 of Chapter 2 the reader is required to have a basic understanding of group cohomology, for which we refer to Chapter 2 of [Mil11] or Chapter 4 of [CF67].

Chapter 1

Algebras

Let R be a commutative ring. An *algebra over R*, or *R-algebra*, is a pair (A, φ) consisting of a ring A and a ring homomorphism $\varphi\colon R \to \mathrm{Z}(A)$ called the *structure map* of A over R, where $\mathrm{Z}(A) = \{x \in A : xa = ax \text{ for all } a \in A\}$ is called the *center* of A, which is a subring of A. One usually refers to A as the R-algebra, and keeps the structure map in mind. If A is an R-algebra that is a division ring, we say that A is a *division algebra.* Furthermore, a *simple ring* is a ring with exactly two two-sided ideals. An R-algebra is called *simple* if it is simple as a ring.

An *algebra homomorphism* $f\colon A \to A'$ between two R-algebras is a ring homomorphism such that the diagram

$$\begin{tikzcd}
A \arrow[rr, "f"] & & A' \\
& R \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

commutes. This defines the category $\mathbf{Alg}_R$ of R-algebras, in which we denote the set of R-algebra homomorphisms by $\mathrm{Alg}_R(-,-)$.

1. Endomorphism and matrix algebras

If A is any ring, then by an A-module we mean a left A-module, leaving the right A-modules disregarded. However, the theory about left modules can easily be obtained for right modules by replacing the base ring with its opposite ring (see Definition 1.4). Furthermore, if A and B are two rings such that the additive group B^+ of B is given an A-module structure, then we often write ${}_AB$ to denote the A-module B^+.

Let R be a commutative ring, and observe that the additive group A^+ of an R-algebra (A, φ) is an R-module by restriction of scalars, i.e., by the composed map

$$R \xrightarrow{\varphi} \mathrm{Z}(A) \xrightarrow{i} A \xrightarrow{f} \mathrm{End}(A^+)\ ,$$

where i is the inclusion map, and f defines the usual A-module structure on A^+.

Now let A be any ring, and let M be a A-module. Then the *endomorphism ring* $\mathrm{End}_A(M)$ is the ring consisting of A-linear endomorphisms of M, where multiplication and addition are given by composition and pointwise addition, respectively. For $a \in A$, let λ_a denote the A-linear endomorphism of M given by left-multiplication by a, and note that λ_a is clearly in the center of $\mathrm{End}_A(M)$ if $a \in \mathrm{Z}(A)$. Observe that the map $g\colon \mathrm{Z}(A) \to \mathrm{Z}\left(\mathrm{End}_A(M)\right)$ given by $a \mapsto \lambda_a$ is a ring homomorphism, which in particular gives $\mathrm{End}_A(M)^+$ the usual $\mathrm{Z}(A)$-module structure. Let R be a commutative ring, and suppose a ring homomorphism $h\colon R \to \mathrm{Z}(A)$ is given. Then the composed map

$$R \xrightarrow{h} \mathrm{Z}(A) \xrightarrow{g} \mathrm{Z}\left(\mathrm{End}_A(M)\right)$$

defines an R-algebra structure on $\mathrm{End}_A(M)$. An algebra of this form is often referred to as an *endomorphism algebra.*

Definition 1.1. Let R be a commutative ring, and let A be an R-algebra. Then $\mathrm{End}_R(A)$ is defined as the R-algebra $\mathrm{End}_R({}_RA)$.

Let A be any ring, and let $n \in \mathbb{Z}_{>0}$. Then the *$n \times n$-matrix ring* $\mathrm{M}_n(A)$ is the ring consisting of the $n \times n$-matrices with coefficients in A, where multiplication and addition are given by the usual matrix multiplication and addition. An elementary linear algebra computation shows that the ring homomorphism $\mathrm{Z}(A) \to \mathrm{Z}(\mathrm{M}_n(A))$ given by $a \mapsto aI_n$, where I_n is the $n \times n$-identity matrix, is an isomorphism. This implies that if R is a commutative ring and a ring homomorphism $R \to \mathrm{Z}(A)$ is given, then the ring $\mathrm{M}_n(A)$ is an R-algebra. An algebra of this form is often referred to as a *matrix algebra*.

Proposition 1.2. *Let A be a ring, and let $n \in \mathbb{Z}_{>0}$. Then there is a bijection between the set of two-sided ideals of A and the set of two-sided ideals of $\mathrm{M}_n(A)$ that sends an two-sided ideal I of A to the two-sided ideal $\mathrm{M}_n(I)$ of $\mathrm{M}_n(A)$.*

Proof. See [Row88, Proposition 1.1.5]. □

Corollary 1.3. *Let A be a simple ring, and let $n \in \mathbb{Z}_{>0}$. Then $\mathrm{M}_n(A)$ is a simple ring.* □

Definition 1.4. Let R be a ring. The *opposite ring* R^{o} of R is the additive group R^+ endowed with a multiplication operation '$\star$' defined for $x, y \in R^+$ by $x \star y = y \cdot x$, where '$\cdot$' is the multiplication operation of R.

Definition 1.5. Let R be a commutative ring, and let (A, φ) be an algebra over R. A k-algebra (B, ψ) is called the *opposite algebra* of A if B is A^{o} as a ring, and φ is equal to ψ.

Proposition 1.6. *Let R be a commutative ring, and let A be an R-algebra. Then there is an R-algebra isomorphism between A^{o} and $\mathrm{End}_A({}_AA)$ that maps an element x in A^{o} to the A-linear endomorphism of A given by right-multiplication with x.*

Proof. For an element a in A, we let ρ_a denote the A-linear endomorphism of A given by right-multiplication with a. Define the map $f\colon A^{\mathrm{o}} \to \mathrm{End}_A({}_AA)$ by $x \mapsto \rho_x$, and observe that f is a ring homomorphism.

Let $r \in R$ and $a \in A^{\mathrm{o}}$, then the equality $f(r \star a) = \rho_r \circ \rho_a$ holds. Since r commutes with any element of A, the equality $\lambda_r = \rho_r$ holds, where λ_r is the A-linear endomorphism of A given by left-multiplication with r. As the action of R on $\mathrm{End}_A({}_AA)$ is given by left-multiplication, we have the equalities $f(r \star a) = r\rho_a = rf(a)$, that is, f is an R-algebra homomorphism.

Observe that ${}_AA$ is a faithful A-module, since $1 \in A$ is only annihilated by $0 \in A$; hence, f is injective. Moreover, since elements of $\mathrm{End}_A({}_AA)$ are A-linear, it is easy to see that these elements are given by right-multiplication with an element of A. It follows that f is surjective. Thus, f is an R-algebra isomorphism. □

Let R be a commutative ring, and let A be an R-algebra. Let M be a A-module, and let $n \in \mathbb{Z}_{>0}$. Then it is easy to check that we have the R-algebra isomorphism $\mathrm{End}_A(M^n) \cong \mathrm{M}_n(\mathrm{End}_A(M))$. In particular, if M is a free A-module of rank n, that is, if M is isomorphic to A^n as an A-module, then there is an R-algebra isomorphism $\mathrm{End}_A(M) \cong \mathrm{M}_n(A^{\mathrm{o}})$ by the above proposition.

2. Algebras and tensor products

Theorem 1.7. *Let R be a commutative ring, and let A and B be two R-algebras. Then there is a unique R-algebra structure on $A \otimes_R B$ that for any $a, c \in A$ and $b, d \in B$ satisfies*

$$(a \otimes b) \cdot (c \otimes d) = ac \otimes bd.$$

Proof. Given $(a, b) \in A \times B$ we have an R-bilinear map $M_{a,b} \colon A \times B \to A \otimes_R B$ defined by $(x, y) \mapsto xa \otimes yb$. Hence, $M_{a,b}$ induces a unique R-linear homomorphism $m_{a,b} \colon A \otimes_R B \to A \otimes_R B$ satisfying $x \otimes y \mapsto xa \otimes yb$. Thus, for any pair $(c, d) \in A \times B$ we have a unique R-linear homomorphism $m_{c,d} \colon A \otimes_R B \to A \otimes_R B$, i.e., there is a bilinear map $F \colon A \times B \to \operatorname{End}_R(A \otimes_R B)$ defined by $(x, y) \mapsto m_{x,y}$. It is easy to check that F is R-bilinear, since R maps in the center of A and in the center of B, and the universal tensor product map $A \times B \to A \otimes_R B$ is R-bilinear. This gives an R-linear homomorphism $f \colon A \otimes_R B \to \operatorname{End}_R(A \otimes_R B)$ satisfying $a \otimes b \mapsto m_{a,b}$. Now, define the multiplication map $\varphi \colon A \otimes_R B \times A \otimes_R B \to A \otimes_R B$ by $(x, y) \mapsto f(x)(y)$, and observe that φ satisfies $(a \otimes b, c \otimes d) \mapsto ac \otimes bd$. It is easy to check that φ is R-bilinear, since f and the elements of $\operatorname{End}_R(A \otimes_R B)$ are R-linear.

The bilinearity of φ implies that the multiplication on $A \otimes_R B$ is distributive over the addition. By this distributivity and the bilinearity of the universal tensor product map it suffices to show the remaining R-algebra properties for the pure tensors. This makes it easy to check that $1 \otimes 1$ is the identity element and that the multiplication is associative. Furthermore, we have a commutative diagram

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "g"'] & \mathrm{Z}(A) \arrow[d, "\alpha"] \\
\mathrm{Z}(B) \arrow[r, "\beta"'] & \mathrm{Z}\left(A \otimes_R B\right)
\end{tikzcd}$$

where f and g are the structure maps for A and B, and α and β are the natural homomorphisms given by $\alpha(a) = a \otimes 1$ and $\beta(b) = 1 \otimes b$, respectively. It follows that $A \otimes_R B$ has a unique R-algebra structure such that $(a \otimes b)(c \otimes d) = ac \otimes bd$ holds for all $a, c \in A$ and $b, d \in B$. □

As the tensor product of algebras inherits the universal mapping property of modules, it also obtains a universal mapping property of algebras. This mapping property, to be stated in the proposition below, is often used to construct algebra homomorphisms from the tensor product to another algebra.

Proposition 1.8. *Let R be a commutative ring, and let A and B be two R-algebras. Then for every R-algebra C there is a bijection f between*

$$\operatorname{Alg}_R(A \otimes_R B, C)$$

and the set

$$\{(\varphi, \psi) \in \operatorname{Alg}_R(A, C) \times \operatorname{Alg}_R(B, C) : \varphi \textit{ and } \psi \textit{ have centralizing images in } C\}$$

given by

$$f(m) = (m \circ \alpha, m \circ \beta) \text{ for } m \in \mathrm{Alg}_R(A \otimes_R B, C),$$

where $\alpha \colon A \to A \otimes_R B$ and $\beta \colon B \to A \otimes_R B$ are the natural R-algebra homomorphisms given by $\alpha(a) = a \otimes 1$ for $a \in A$ and $\beta(b) = 1 \otimes b$ for $b \in B$.

Proof. First, observe that the images of α and β clearly centralize each other in $A \otimes_R B$. Hence, the multiplicativity of m implies that the images of $m \circ \alpha$ and $m \circ \beta$ centralize each other in C. Thus, the map f is well-defined.

Let $m, n \in \mathrm{Alg}_R(A \otimes_R B, C)$ and suppose $f(m) = f(n)$ holds. Let i and j be the structure maps of A and B over R, respectively. Then we have the following commutative diagram

$$\begin{tikzcd}
R \arrow[r, "i"] \arrow[d, "j"'] & A \arrow[d, "\alpha"] \arrow[ddr, bend left, "\varphi"] & \\
B \arrow[r, "\beta"'] \arrow[drr, bend right, "\psi"'] & A \otimes_R B \arrow[dr, shift left, "n"] \arrow[dr, shift right, "m"'] & \\
 & & C
\end{tikzcd}$$

from which it follows that m and n are equal when restricted to the pure tensors $\{a \otimes b : a \in A, b \in B\}$. As the pure tensors generate $A \otimes_R B$, it follows that m and n are equal on their whole domain. Thus, the map f is injective.

For the surjectivity of f, suppose we have a pair $(\varphi, \psi) \in \mathrm{Alg}_R(A, C) \times \mathrm{Alg}_R(B, C)$ such that the images of φ and ψ in C centralize each other. Observe that the map $M \colon A \times B \to C$ given by $(a, b) \mapsto \varphi(a)\psi(b)$ is R-bilinear. Hence, M induces a unique R-linear homomorphism $m \colon A \otimes_R B \to C$ satisfying $a \otimes b \mapsto \varphi(a)\psi(b)$ for all $a \in A$ and $b \in B$. Observe that m is also multiplicative, since the images of φ and ψ centralize each other in C. Moreover, it holds that $m(1 \otimes 1) = 1$. Hence, m is an R-algebra homomorphism. Furthermore, it is clear that $m \circ \alpha = \varphi$ and $m \circ \beta = \psi$ hold; hence, f is surjective. □

Notation. Let R be a commutative ring, and let A and B be two R-algebras. Let $A \otimes_R 1$ denote the subalgebra $\{a \otimes 1 : a \in A\}$ of $A \otimes_R B$, and let $1 \otimes_R B$ denote the subalgebra $\{1 \otimes b : b \in B\}$ of $A \otimes_R B$. Often we will reduce notation to A_1 for $A \otimes_R 1$ and ${}_1B$ for $1 \otimes_R B$.

Definition 1.9. Let A be a ring, and let X be a subset of A. Then $\mathrm{C}_A(X) = \{a \in A : xa = ax \text{ for all } x \in X\}$ is called the *centralizer* of X in A.

It is easy to check that the centralizer of a subset of a ring A, is a subring of A as well.

Theorem 1.10. *Let k be a field, and let A and B be two k-algebras. Then $\mathrm{Z}(A \otimes_k B)$ and $\mathrm{Z}(A) \otimes_k \mathrm{Z}(B)$ are isomorphic as k-algebras.*

Proof. First, observe that if $A = \{0\}$ or $B = \{0\}$ hold, the statement clearly holds. Thus, assume A and B are unequal to $\{0\}$. Consider the sequence

$$0 \longrightarrow \mathrm{Z}(A) \xrightarrow{i} A \xrightarrow{f} \mathrm{End}_k(A)$$

of k-algebras, where i is the natural inclusion and f is given by $x \mapsto [a \mapsto ax - xa]$, and observe that it is clearly exact. Since k-modules are flat, the sequence

$$0 \longrightarrow \mathrm{Z}(A) \otimes_k B \xrightarrow{i \otimes \mathrm{id}_B} A \otimes_k B \xrightarrow{f \otimes \mathrm{id}_B} \mathrm{End}_k(A) \otimes_k B$$

is exact too, where id_B is the identity on B. Let $g \colon \mathrm{End}_k(A) \otimes_k B \to \mathrm{Hom}_k(A, A \otimes_k B)$ be given by $f \otimes b \mapsto [a \mapsto f(a) \otimes b]$, and observe that g is clearly a well-defined k-linear homomorphism. It is easy to check that g maps $\mathrm{im}(f \otimes \mathrm{id}_B)$ injectively to $\mathrm{Hom}_k(A, A \otimes_k B)$. Hence, the composed map $(g \circ f) \otimes \mathrm{id}_B$ has the same kernel as $f \otimes \mathrm{id}_B$. Seeing that $\ker((g \circ f) \otimes \mathrm{id}_B)$ is obviously $\mathrm{C}_{A \otimes_k B}(A_1)$, we have the equality $\mathrm{C}_{A \otimes_k B}(A_1) = \mathrm{Z}(A) \otimes_k B$. In the same manner we can show that $\mathrm{C}_{A \otimes_k B}({}_1B) = A \otimes_k \mathrm{Z}(B)$ holds.

Now, clearly the inclusions $\mathrm{Z}(A \otimes_k B) \subset \mathrm{C}_{A \otimes_k B}(A_1)$ and $\mathrm{Z}(A \otimes_k B) \subset \mathrm{C}_{A \otimes_k B}({}_1B)$ hold. Hence, $\mathrm{Z}(A \otimes_k B) \subset \mathrm{C}_{A \otimes_k B}(A_1) \cap \mathrm{C}_{A \otimes_k B}({}_1B)$ holds. Moreover, we have that $(\mathrm{Z}(A) \otimes_k B) \cap (A \otimes_k \mathrm{Z}(B)) = \mathrm{Z}(A) \otimes_k \mathrm{Z}(B)$ holds by elementary linear algebra arguments. Thus $\mathrm{Z}(A \otimes_k B) \subset \mathrm{Z}(A) \otimes_k \mathrm{Z}(B)$ holds.

At last, observe that the flatness of A and B as k-modules showed that the inclusions $\mathrm{Z}(A) \otimes_k B \subset A \otimes_k B$ and $A \otimes_k \mathrm{Z}(B) \subset A \otimes_k B$ hold. In particular, their intersection $\mathrm{Z}(A) \otimes_k \mathrm{Z}(B)$ is also contained in $A \otimes_k B$. Moreover, it is easy to check that $\mathrm{Z}(A) \otimes_k \mathrm{Z}(B)$ is contained in $\mathrm{Z}(A \otimes_k B)$. □

Below we prove the commutativity of the tensor product of two algebras with the help of the Yoneda lemma.

Definition 1.11. Let $\mathcal{C}$ be a category. Then $\mathcal{C}^\wedge$ is the opposite category of the category $\mathrm{Funct}(\mathcal{C}, \mathbf{Set})$ of functors from $\mathcal{C}$ to $\mathbf{Set}$.

Lemma 1.12. *Let $\mathcal{C}$ be a category. Then $h^\wedge \colon \mathcal{C} \to \mathcal{C}^\wedge$ given by $X \mapsto \mathrm{Hom}_\mathcal{C}(X, -)$ for every object $X \in \mathcal{C}$ is a contravariant functor.*

Proof. See [Dor08, §2.4.2]. □

Theorem 1.13 (Yoneda)**.** *Let $\mathcal{C}$ be a category. The functor $h^\wedge$ is fully faithful, i.e., for every $X, Y \in \mathcal{C}$ the natural homomorphism $\mathrm{Hom}_\mathcal{C}(X, Y) \to \mathrm{Hom}_{\mathcal{C}^\wedge}(h^\wedge(X), h^\wedge(Y))$ is a bijection.*

Proof. See [Dor08, Proposition 2.4.9]. □

Proposition 1.14. *Let R be a commutative ring, and let A and B be R-algebras. Then there is a unique R-algebra isomorphism $A \otimes_R B \to B \otimes_R A$ that satisfies $a \otimes b \mapsto b \otimes a$.*

Proof. First, observe that the symmetric property of Proposition 1.8 implies that the functors $\mathrm{Alg}_R(A \otimes_R B, -)$ and $\mathrm{Alg}_R(B \otimes_R A, -)$ are naturally isomorphic. Consequently, Theorem 1.13 implies that there is a unique isomorphism between $A \otimes_R B$ and $B \otimes_R A$ that satisfies $a \otimes b \mapsto b \otimes a$. □

Proposition 1.15. *Let R and S be commutative rings. Let A be an R-algebra, B be an R-algebra and an S-algebra and C be an S-algebra. Then there is a unique $R \otimes_\mathbb{Z} S$-algebra isomorphism $(A \otimes_R B) \otimes_S C \to A \otimes_R (B \otimes_S C)$ satisfying $(a \otimes b) \otimes c \mapsto a \otimes (b \otimes c)$.*

Proof. See [Bou73, Chapter 3, §4, section 1]. □

Lemma 1.16. *Let R be a commutative ring, and let A be an R-algebra. Let $m, n \in \mathbb{Z}_{>0}$. Then the R-algebra isomorphism $\mathrm{M}_m(\mathrm{M}_n(A)) \cong \mathrm{M}_{mn}(A)$ holds.*

Proof. Write $A^{\mathrm{opp}} = B$. By the isomorphism below Proposition 1.6, we have the following R-algebra isomorphisms

$$\begin{aligned} \mathrm{M}_{mn}(A) &\cong \mathrm{End}_B(B^{mn}) \\ &\cong \mathrm{End}_B((B^n)^m) \\ &\cong \mathrm{M}_m(\mathrm{End}_B(B^n)) \\ &\cong \mathrm{M}_m(\mathrm{M}_n(\mathrm{End}_B(B))) \\ &\cong \mathrm{M}_m(\mathrm{M}_n(A)) \end{aligned}$$

that prove the lemma. □

Proposition 1.17. *Let R be a commutative ring, and let A be an R-algebra. Then the R-algebra isomorphism $A \otimes_R \mathrm{M}_n(R) \cong \mathrm{M}_n(A)$ holds for any $n \in \mathbb{Z}_{>0}$.*

Proof. First, observe that $f\colon A \to \mathrm{M}_n(A)$ given by $a \mapsto aI$, where I is the identity matrix in $\mathrm{M}_n(A)$, is an R-algebra homomorphism. Furthermore, the map $g\colon \mathrm{M}_n(R) \to \mathrm{M}_n(A)$ given by $(a_{ij})_{i,j=1}^n \mapsto (\varphi(a_{ij}))_{i,j=1}^n$ is an R-algebra homomorphism. Clearly the images of f and g centralize each other in $\mathrm{M}_n(A)$. Hence, by Proposition 1.8 there is a unique R-algebra homomorphism $h\colon A \otimes_R \mathrm{M}_n(R) \to \mathrm{M}_n(A)$ satisfying $a \otimes M \mapsto ag(M)$.

Let $S = \{e_{ij} \in \mathrm{M}_n(R) : i, j \in \{1, \dots, n\}\}$, where e_{ij} is defined in the proof of the previous lemma. Observe that $A \otimes_R \mathrm{M}_n(R)$ has an R-basis $\{a \otimes e : a \in A, e \in S\}$, which is mapped under f to the R-basis $\{ag(e) : a \in A, e \in S\}$ of $\mathrm{M}_n(A)$. It follows that f is an R-algebra isomorphism. □

Corollary 1.18. *Let R be a commutative ring, and let A and B be two R-algebras. Then for any $m, n \in \mathbb{Z}_{>0}$ the R-algebra isomorphisms $\mathrm{M}_m(A) \otimes_R \mathrm{M}_n(B) \cong \mathrm{M}_{mn}(A \otimes_R B)$ hold.*

Proof. Let $m, n \in \mathbb{Z}_{>0}$ and observe that the R-algebra isomorphisms $\mathrm{M}_m(R) \otimes_R \mathrm{M}_n(R) \cong \mathrm{M}_n(\mathrm{M}_m(R)) \cong \mathrm{M}_{mn}(R)$ hold by the previous proposition and Proposition 1.16. Furthermore, we have the R-algebra isomorphisms $\mathrm{M}_m(A) \cong A \otimes_R \mathrm{M}_m(R)$ and $\mathrm{M}_n(B) \cong B \otimes_R \mathrm{M}_n(R)$. Hence, the commutativity of the tensor product implies that the R-algebra isomorphisms $\mathrm{M}_m(A) \otimes_R \mathrm{M}_n(B) \cong (A \otimes_R B) \otimes_R (\mathrm{M}_m(R) \otimes_R \mathrm{M}_n(R)) \cong (A \otimes_R B) \otimes_R \mathrm{M}_{mn}(R)$ hold. Thus, the previous proposition implies that the R-algebra isomorphisms $\mathrm{M}_m(A) \otimes_R \mathrm{M}_n(B) \cong \mathrm{M}_{mn}(A \otimes_R B)$ hold. □

3. Semisimplicity

In this subsection we will briefly explain the theory of semisimple rings and modules. This theory provides information about the underlying module structure of certain simple algebras, which enables us to prove many theorems. Unfortunately it is not in the range of this text to fully cover this abundant theory; hence, we shall only race our way through parts of the theory that are of our interest. For a more extensive and complete treatment of this theory see [Bou73, Chapter 8], [FD93, Chapter 1] or [CR62, Chapter 4].

Definition 1.19. Let R be a ring, and let M be an R-module. If M has exactly two R-submodules, then M is called *simple*.

Proposition 1.20. *Let R be a ring, and let M be an R-module. Then the following statements are equivalent:*

(i) *M is a simple R-module;*
(ii) *M is non-zero and is generated by any non-zero element of M;*
(iii) *there is a maximal left ideal I of R such that $M \cong_R R/I$ holds.*

Proof. See [Bou73, Chapter 8, §3, Proposition 1 and 2]. □

Example 1.21. A maximal ideal of $\mathbb{Z}$ is of the form (p) for some prime number p, and conversely every ideal in $\mathbb{Z}$ generated by a prime number is a maximal ideal. Hence, the simple $\mathbb{Z}$-modules are the cyclic groups of prime order.

The following lemma is due to Issai Schur (1875–1941) and shows a way to construct a division ring.

Lemma 1.22 (Schur's Lemma). *Let R be a ring, and let M be a simple R-module. Then the endomorphism ring $\operatorname{End}_R(M)$ is a division ring.*

Proof. See [Bou73, Chapter 8, §4, Proposition 2]. □

Definition 1.23. Let R be a ring, and let M be an R-module. If any exact sequence of R-modules

$$0 \longrightarrow K \longrightarrow M \longrightarrow L \longrightarrow 0$$

splits, then M is called *semisimple*.

Proposition 1.24. *Let R be a ring, and let M be an R-module. Then the following statements are equivalent:*

(i) *M is a semisimple R-module;*
(ii) *M is a direct sum of a family of simple R-submodules;*
(iii) *M is a sum of a family of simple R-submodules;*
(iv) *every R-submodule of M has a complement.*

Proof. See [Bou73, Chapter 8, §3, Proposition 7]. □

Corollary 1.25. *Let R be a ring, and let M be an R-module. Then every submodule of M and every quotient module of M is semisimple.*

Proof. See [Bou73, Chapter 8, §3, Corollary 1]. □

Example 1.26. A $\mathbb{Z}$-module is semisimple if and only if it is a direct sum of cyclic groups of prime order. Equivalently, a $\mathbb{Z}$-module is semisimple if and only if each element has finite square-free order.

Example 1.27. It is easy to see that all modules over a division ring are free. Corresponding to the case of fields, modules over a division ring are usually called vector spaces. Now, since every exact sequence of free modules splits, any module over a division ring is semisimple.

Definition 1.28. A ring R is called *semisimple* if it is semisimple as a module over itself.

In fact, a semisimple ring as in the definition above is a left semisimple ring. There is also a notion of a right semisimple ring, which is a ring that is semisimple as a right module over itself. We will soon see that a ring is left semisimple if and only if it is right semisimple; hence, a ring R is semisimple if and only if R^{o} is semisimple, meaning that the use of 'left' and 'right' is superfluous.

Proposition 1.29. *A ring R is semisimple if and only if every R-module is semisimple.*

Proof. See [Bou73, Chapter 8, §5, Proposition 1]. □

Proposition 1.30. *Let R be a semisimple ring. Then there are only finitely many simple R-modules in the unique decomposition of ${}_RR$ in simple R-modules. Moreover, every simple R-module is isomorphic to a direct summand of this decomposition.*

Proof. See [FD93, Theorem 1.9]. □

Example 1.31. From Example 1.27 it follows that any division ring is semisimple.

Example 1.32. Clearly $\mathbb{Z}^+$ is not a finite direct sum of cyclic groups of prime order; hence, $\mathbb{Z}$ is not a semisimple ring.

The following theorem, due to Emil Artin (1898–1962) and Joseph Wedderburn (1882–1948), classifies semisimple rings. In 1907 Wedderburn first proved a structure theorem for simple algebras over a division ring, and in 1927 Artin generalized this structure theory to semisimple rings. Nowadays this generalized structure theorem is called the Artin-Wedderburn theorem and is stated as follows.

Theorem 1.33 (Artin-Wedderburn). *Let R be a ring. Then R is semisimple if and only if there is $t \in \mathbb{Z}_{>0}$ such that there are division rings $D_1, \ldots, D_t$ and $n_1, \ldots, n_t \in \mathbb{Z}_{>0}$ such that R is isomorphic to $\prod_{i=1}^{t} \mathrm{M}_{n_i}(D_i)$ as a ring. The number t is uniquely determined, as are the division algebras $D_1, \ldots, D_t$ up to isomorphism. There are exactly t mutually nonisomorphic simple modules over R.*

Proof. See [FD93, Proposition 1.10, Theorem 1.11 and Theorem 1.13]. □

Corollary 1.34. *A ring is left semisimple if and only if it is right semisimple.* □

Definition 1.35. A ring R is called *left* (respectively *right*) *artinian* if there is no strictly descending infinite chain $I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \ldots$ of left (respectively right) ideals of R. A ring is called *artinian* if it is both left and right artinian.

The following theorem classifies simple semisimple rings, and is in fact the original result of Wedderburn formulated in a more modern way.

Theorem 1.36. *Let R be a ring. Then the following statements are equivalent:*

(i) *R is a simple artinian ring;*

(ii) *R is semisimple, and all simple R-modules are isomorphic;*

(iii) *there exist $n \in \mathbb{Z}_{>0}$ and a division ring D such that R is isomorphic to $\mathrm{M}_n(D)$ as a ring.*

Proof. See [FD93, Theorem 1.15]. □

Corollary 1.37. *Let R be a simple artinian ring. Then there is a unique $n \in \mathbb{Z}_{>0}$ and a division ring D that is unique up to isomorphism such that R is isomorphic to $\mathrm{M}_n(D)$ as a ring.*

Proof. See [CR62, Theorem 26.4]. □

4. Central simple algebras

If R is a commutative ring, we say that an R-algebra A is *central* if the structure map $R \to \mathrm{Z}(A)$ is an isomorphism. Observe that any ring is a central algebra over its center.

Let k be a field, and observe that the additive group A^+ of a k-algebra A is a k-vector space. The k-dimension that A^+ hereby gets is called the *rank* of the algebra A, denoted $[A : k]$. If $[A : k]$ is finite, we say that A has *finite rank* over k or that A is of *finite rank* over k.

Definition 1.38. Let k be a field. A *central simple k-algebra* is a central and simple k-algebra of finite rank over k.

Example 1.39. Every field is a central simple algebra over itself.

Example 1.40. The quaternion ring $\mathbb{H}$ is a central simple algebra of rank 4 over $\mathbb{R}$.

Proposition 1.41. *The center of a simple ring is a field.*

Proof. Let A be a simple ring and let $x \in \mathrm{Z}(A)$ be non-zero. Then the two-sided ideal (x) generated by x is equal to A; hence, there is $y \in A$ such that $xy = 1$ holds. It follows that y is the inverse of x. Now, let $z \in A$ and observe that $yz = yzxy = yxzy = zy$ holds, that is, we have $y \in \mathrm{Z}(A)$. □

Example 1.42. Let A be a simple ring. Then A is a central and simple algebra over its center $\mathrm{Z}(A)$. In particular, for any $n \in \mathbb{Z}_{>0}$ the matrix algebra $\mathrm{M}_n(A)$ is central and simple over $\mathrm{Z}(A)$. Additionally, if A is of finite rank over $\mathrm{Z}(A)$, then for any $n \in \mathbb{Z}_{>0}$ the matrix algebra $\mathrm{M}_n(A)$ is central simple over $\mathrm{Z}(A)$.

By Theorem 1.10 the tensor product of two central algebras over a field remains central over the same field. The following theorem shows that the tensor product also preserves simplicity in a certain case.

Theorem 1.43. *Let k be a field. Let A be a central and simple k-algebra and B a simple k-algebra. Then $A \otimes_k B$ is a simple k-algebra.*

Proof. See [Ker07, 2.6]. □

Remark 1.44. The condition that A is central over k cannot be omitted from Theorem 1.43. Indeed, suppose $l \supsetneq k$ is a field strictly containing k, and observe that the map $\mathrm{id}_l \otimes \mathrm{id}_l \colon l \otimes_k l \to l$ satisfying $x \otimes y \mapsto xy$ is a surjective ring homomorphism. Let $x \in l \setminus k$, and observe that $x \otimes 1 - 1 \otimes x$ is a non-zero element of $l \otimes_k l$. Since $(\mathrm{id}_l \otimes \mathrm{id}_l)(x \otimes 1 - 1 \otimes x) = 0$ holds, the kernel of $\mathrm{id}_l \otimes \mathrm{id}_l$ is a non-zero two-sided ideal of $l \otimes_k l$. It follows that $l \otimes_k l$ is not simple.

Corollary 1.45. *Let k be a field, and let A and B be two central simple k-algebras. Then $A \otimes_k B$ is a central simple k-algebra.*

Proof. Since A and B are of finite rank over k, their tensor product is too. Hence, Theorem 1.10 and Theorem 1.43 prove the statement. □

Proposition 1.46. *Any algebra of finite rank over a field is an artinian ring.*

Proof. Let A be an algebra of finite rank over a field k, and suppose $I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \dots$ is a strictly descending chain of left ideals of A. Each ideal I_i in this chain is obviously a k-vector subspace of A; hence, $\dim_k(I_i) < \infty$ for every ideal I_i in the descending chain. As the chain is strictly descending, it follows that $\dim_k(I_1) > \dim_k(I_2) > \dots$ holds. Since $\dim_k(I_1)$ is finite and the standard ordering on $\mathbb{Z}_{\geq 0}$ is a well-ordering, it follows that the chain is not strictly descending. This contradiction implies that A is left artinian. Analogously we can show that A is right artinian. Thus A is artinian. □

Definition 1.47. Let k be a field, and let D be an algebra over k. If D is a central algebra of finite rank over k that is also a division ring, then D is called a *central division algebra* over k.

Proposition 1.48. *Let k be a field, and let A be a k-algebra. Then A is a simple algebra of finite rank over k if and only if there exist $n \in \mathbb{Z}_{>0}$ and a division algebra D of finite rank over k such that A is isomorphic to $\mathrm{M}_n(D)$ as a k-algebra. The integer n is uniquely determined, as is the division algebra D up to isomorphism.*

Proof. By Theorem 1.36 there exist $n \in \mathbb{Z}_{>0}$ and a division ring D such that A is isomorphic to $\mathrm{M}_n(D)$ as a ring. Observe that D is a division k-algebra via the k-algebra structure of A given by the ring isomorphisms $\mathrm{Z}(A) \cong \mathrm{Z}(\mathrm{M}_n(D)) \cong \mathrm{Z}(D)$. Clearly we now have the k-algebra isomorphism $A \cong \mathrm{M}_n(D)$. Moreover, we have the equalities $[A : k] = [\mathrm{M}_n(D) : k] = n^2[D : k]$, where $[A : k]$ is finite; hence, $[D : k]$ is finite too. It follows that D is a division algebra of finite rank over k.

Conversely, suppose there exist $n \in \mathbb{Z}_{>0}$ and a division algebra D of finite rank over k such that A is isomorphic to $\mathrm{M}_n(D)$ as a k-algebra. Then Corollary 1.3 implies that A is a simple algebra over k. Furthermore, the rank of D over k is finite; hence, A is also of finite rank over k. It follows that A is a simple algebra of finite rank over k.

For the last statement see [Ker07, §1.11]. □

Corollary 1.49. *Let k be a field, and let A be a k-algebra. Then A is a central simple algebra of finite rank over k if and only if there exist $n \in \mathbb{Z}_{>0}$ and a division algebra D of finite rank over k such that A is isomorphic to $\mathrm{M}_n(D)$ as a k-algebra. The integer n is uniquely determined, as is the division algebra D up to isomorphism.*

Proof. This follows from the previous proposition and the obvious k-algebra isomorphisms $k \cong \mathrm{Z}(A) \cong \mathrm{Z}(D)$. □

With this structure theorem at hand, we first prove that any central simple algebra over an algebraically closed field k is isomorphic as a k-algebra to a matrix algebra with coefficients in k.

Lemma 1.50. *Let k be an algebraically closed field. Then any division algebras of finite rank over k is isomorphic to k as an algebra.*

Proof. Suppose D is a noncommutative division algebra of finite rank over k, and let x be an element of D. Then x generates the commutative extension $k(x)$ of k, which is finite for D is of finite rank over k. As finite field extensions are algebraic and k is algebraically closed, it follows that $k(x) = k$ holds. Consequently, x is an element of k, that is, we have that $D = k$ holds.

□

Corollary 1.51. *Let k be an algebraically closed field. Then every central simple k-algebra is isomorphic to $\mathrm{M}_n(k)$ as a k-algebra for some $n \in \mathbb{Z}_{>0}$.*

Proof. By Corollary 1.49 and Lemma 1.16 it suffices to prove the statement for central division algebras over k. Since central division k-algebras have finite rank over k, the previous lemma proves this corollary. □

A technique that will prove to be very helpful in understanding the structure of central simple algebras is the extension of the base field of an algebra, also called extension of scalars or base change of an algebra.

Let $f : k \to l$ be a field homomorphism. Then the ring homomorphism $\varphi : l \to \mathrm{Z}(A) \otimes_k l$ defined by $x \mapsto 1 \otimes x$ gives $A \otimes_k l$ an l-algebra structure, since the k-algebra isomorphism $\mathrm{Z}(A) \otimes_k l \cong \mathrm{Z}(A \otimes_k l)$ holds by Theorem 1.10. The l-algebra $A \otimes_k l$ is called the *extended algebra* of A via f, and we say that this algebra is obtained by *extension of scalars* via f or by *base change* via f. We often denote this algebra by A_f, or by A_l when the map f is understood. For example, in the case of field extensions $l \supset k$, we write A_l for the extended algebra $A \otimes_k l$.

Proposition 1.52. *Let k be a field, and let A be an algebra over k. Let $L \supset k$ be a field extension of k. Then A is a central simple algebra over k if and only if $A \otimes_k l$ is a central simple algebra over l.*

Proof. Suppose A is central simple over k, then Theorem 1.10 and Theorem 1.43 imply that A_l is central and simple over l. As $[A_l : l] = [A : k]$ holds, we see that A_l is a central simple l-algebra.

Conversely, suppose $A \otimes_k l$ is central simple over l. Then Theorem 1.10 implies that the k-algebra isomorphism $\mathrm{Z}(A) \otimes_k l \cong l$ holds; hence, we have the k-algebra isomorphism $\mathrm{Z}(A) \cong k$. Now, suppose A is not simple, and let I be a two-sided ideal of A. Then $I \otimes_k 1$ is a two-sided ideal of A_l, which is simple. This contradiction implies that A is simple as a ring. As $[A_l : l] = [A : k]$ holds, it follows that A is central simple over k. □

It is no coincidence that the rank of $\mathbb{H}$ over $\mathbb{R}$ is a square, and in fact this is a property all simple algebras of finite rank over a field enjoy. Together with the above technique we prove this statement below.

Proposition 1.53. *Let k be a field, and let A be a central simple algebra over k. Then the rank of A over k is a square.*

Proof. Let $\overline{k}$ be an algebraic closure of k, then there is $n \in \mathbb{Z}_{>0}$ such that $A_{\overline{k}}$ and $\mathrm{M}_n(\overline{k})$ are isomorphic as $\overline{k}$-algebras. Then we have the equalities

$$[A : k] = [A_{\overline{k}} : \overline{k}] = [\mathrm{M}_n(\overline{k}) : \overline{k}] = n^2,$$

which prove the statement. □

Definition 1.54. Let k be a field, and let A be a central simple k-algebra. The integer $\sqrt{[A : k]}$ is called the *degree* of A over k.

We conclude this section with a lemma that is essential in the construction of the Brauer group in the next chapter.

Lemma 1.55. *Let k be a field, and let A be a central simple algebra over k. Let n be the degree of A. Then $A \otimes_k A^{\mathrm{o}}$ is isomorphic to $\mathrm{M}_n(k)$ as a k-algebra.*

Proof. Let $\varphi\colon A \to \mathrm{End}_k(A)$ be the k-algebra homomorphism given by $A \mapsto [x \mapsto ax]$. Furthermore, define the k-algebra homomorphism $\psi\colon A^{\mathrm{o}} \to \mathrm{End}_k(A)$ by $a \mapsto [x \mapsto xa]$ and observe that ψ and φ have centralizing images in $\mathrm{End}_k(A)$. By Proposition 1.8 there is a unique k-algebra homomorphism $f\colon A \otimes_k A^{\mathrm{o}} \to \mathrm{End}_k(A)$ satisfying $a \otimes b \mapsto \varphi(a)\psi(b)$. Since $A \otimes_k A^{\mathrm{o}}$ is simple, f is injective. Moreover, we have the equalities $[A \otimes_k A^{\mathrm{o}} : k] = n^2$ and $[\mathrm{End}_k(A) : k] = n^2$; hence, f is surjective. It clearly holds that $\mathrm{End}_k(A)$ is isomorphic to $\mathrm{M}_n(k)$ as a k-algebra, which finishes the proof. □

5. Splitting fields

We have seen that every central simple algebra over an algebraically closed field is isomorphic as an algebra to a matrix algebra over the same field, see Proposition 1.51. In particular, for a central simple algebra A over a field k with algebraic closure $\bar{k}$, this means that there is $n \in \mathbb{Z}_{>0}$ such that the $\bar{k}$-algebra isomorphism $A_{\bar{k}} \cong \mathrm{M}_n(\bar{k})$ holds. Moreover, for an arbitrary field extension l of a field k and every $m \in \mathbb{Z}_{>0}$, it holds that $\mathrm{M}_m(k) \otimes_k l$ is isomorphic to $\mathrm{M}_m(l)$ as an algebra by Proposition 1.17.

In general, if A is a central simple algebra over k and there is $n \in \mathbb{Z}_{>0}$ such that A_l is isomorphic to $\mathrm{M}_n(l)$ as an l-algebra, then we say that A *splits* over l or that l is a *splitting field* for A.

Proposition 1.56. *Let k be a field, and let A be a central simple k-algebra. Let n be the degree of A, and let l be a field over k that splits A. Then the l-algebra isomorphism $A_l \cong M_n(l)$ holds.*

Proof. By definition of splitting we have that A_l is isomorphic to $\mathrm{M}_i(l)$ as an l-algebra for some $i \in \mathbb{Z}_{>0}$; hence, it rests to show that $i = n$ holds. Observe that $[A_l : l] = [A : k]$ holds, where $[A : k] = n^2$ and $[A_l : l] = i^2$ hold. As i and n are positive integers, the equality $i = n$ follows.

□

Splitting fields make it possible in the next chapter to divide the collection of all central division algebras over a field into more convenient parts, which are in turn provided with a transparent description through homological algebra. We will shortly introduce our very first type of splitting field for a central simple algebra A, but first we are required to look at the centralizers in A of subalgebras of A, done by the following proposition.

Proposition 1.57. *Let k be a field. Let A be a central simple algebra over k, and let B be a simple k-subalgebra of A. Then*

(i) $\mathrm{C}_A(B)$ *is simple;*

(ii) $[A : k] = [B : k][\mathrm{C}_A(B) : k]$.

Proof. See [Bou73, Chapter 8, §10, Theorem 2]. □

Corollary 1.58. *Let k be a field. Let A be a central simple algebra over k, and let B be a simple k-subalgebra of A. Then $C_A(C_A(B)) = B$ holds.*

Proof. As the first statement of the previous proposition asserts that $C_A(B)$ is simple, we can also apply the second statement of the same proposition to $C_A(B)$. This gives $[A : k] = [C_A(B) : k][C_A(C_A(B)) : k]$; hence, $[C_A(C_A(B)) : k] = [B : k]$ holds. Since $B \subset C_A(C_A(B))$ clearly holds, we have that $B = C_A(C_A(B))$ holds for their dimensions over k are equal. □

Let k be a field, and let A be a central simple algebra over k. Let l be a subfield of A that is equal to its centralizer in A and suppose m is a field extension of l inside A. Then $m \subset \mathrm{C}_A(l) = l$ holds. Consequently, $l = m$ holds, that is, l is a maximal subfield of A. These subfields of A that equal their centralizer in A will henceforth be called *strictly maximal subfields* of A.

Proposition 1.59. *Let k be a field, and let A be a central simple algebra over k. Let n be the degree of A, and let l be a subfield of A containing k. Then the following statements are equivalent:*

(i) *l is a strictly maximal subfield of A;*

(ii) *l is of degree n over k;*

(iii) *l is a maximal commutative k-subalgebra of A.*

Proof. First, we prove that (i) and (ii) are equivalent. By the previous proposition we have that $n^2 = [A : k] = [l : k][\mathrm{C}_A(l) : k]$ holds. Hence, if $l = \mathrm{C}_A(l)$ holds, it clearly follows that $[l : k] = n$ holds. On the other hand, if $[l : k] = n$ holds, then we have that $[\mathrm{C}_A(l) : k] = n$ holds. As we always have $l \subset \mathrm{C}_A(l)$, it follows that $l = \mathrm{C}_A(l)$ holds for they have equal rank over k. This shows that (i) and (ii) are equivalent.

Now we prove that (i) and (iii) are equivalent. Assume $l = \mathrm{C}_A(l)$ holds and suppose that there is a commutative k-subalgebra m of A such that $l \subset m$ holds. Then clearly $m \subset \mathrm{C}_A(l)$ holds, that is, we have that $l = m$ holds. On the other hand, assume l is a maximal commutative k-subalgebra of A and let $x \in \mathrm{C}_A(l)$. Then $l[x]$ is a commutative k-subalgebra of A; hence, by maximality of l we have that $l[x] = l$ holds. It follows that (i) is equivalent with (iii). □

The above proposition shows, specifically, that a strictly maximal subfield of A is a maximal commutative k-subalgebra of A of degree n over k. In particular, if D is a division algebra, then any commutative k-subalgebra of D is a field. Therefore, any maximal subfield of a division algebra is strictly maximal. However, this does not hold in general for central simple algebras, and in fact strictly maximal subfields do not always exist for central simple algebras.

For example, consider the real matrix algebra $A = \mathrm{M}_m(\mathbb{H})$ for some $m \in \mathbb{Z}_{>0}$, and observe that this algebra has rank $4m^2$ over $\mathbb{R}$. By Proposition 1.59 a strictly maximal subfield of A is of degree $2m$ over $\mathbb{R}$. But $\mathbb{R}$ and $\mathbb{C}$ are the only finite field extensions of $\mathbb{R}$. Therefore $\mathrm{M}_m(\mathbb{H})$ has no strictly maximal subfields for any $m \in \mathbb{Z}_{>1}$.

Theorem 1.60. *Let k be a field, and let A be a central simple k-algebra. Then any strictly maximal subfield of A is a splitting field for A.*

Proof. Let l be a strictly maximal subfield of A, and observe that the injection $i\colon l \to A$ gives A an l-module structure by restriction of scalars. Define the maps $\varphi\colon A \to \mathrm{End}_l(B)$ and $\psi\colon l \to \mathrm{End}_l(B)$ by $a \mapsto [x \mapsto ax]$ and $l \mapsto [y \mapsto yl]$, respectively, where B denotes the right l-module A. It is easy to check that these maps are k-algebra homomorphisms, and that φ and ψ have centralizing images in $\mathrm{End}_l(B)$. Now Proposition 1.8 implies that there is a unique k-algebra homomorphism $f\colon A \otimes_k l \to \mathrm{End}_l(B)$ satisfying $a \otimes b \mapsto \varphi(a)\psi(b)$, and it is easy to check that f is in fact an l-algebra homomorphism.

Since $A \otimes_k l$ is simple by Theorem 1.43 and f is non-zero, the map f is injective. Moreover, let n be the degree of A over k, and observe that the rank of $A \otimes_k l$ over l is n^2 and the rank of $\mathrm{End}_l({}_lA)$ over l is also n^2. Consequently, f is an l-algebra isomorphism. As ${}_lA$ is isomorphic to l^n as an l-module, we have the l-algebra isomorphism $\mathrm{End}_l({}_lA) \cong \mathrm{M}_n(l)$. □

6. The Skolem-Noether theorem

It is known that any k-linear automorphism of the matrix ring $\mathrm{M}_n(k)$ is an inner automorphism (see [GS06, Lemma 2.4.1]), meaning there is an invertible matrix C such that the k-linear automorphism is given by $M \mapsto CMC^{-1}$. To conclude this chapter, we give the generalization of this statement to arbitrary central simple algebras, formulated by the Skolem-Noether Theorem.

Definition 1.61. Let R be a commutative ring, and let A be an R-algebra. Then an R-algebra automorphism f of A is called *inner* if there is an invertible element $b \in A$ such that for all $a \in A$ the identity $f(a) = bab^{-1}$ holds.

Theorem 1.62 (Skolem-Noether)**.** *Let k be a field. Let A be a simple algebra over k, and let B be a central simple algebra over k. Suppose $f, g\colon A \to B$ are k-algebra homomorphisms. Then f and g differ by an inner k-algebra automorphism of B, i.e., there exists an invertible element $b \in B$ such that for all $a \in A$ the identity $f(a) = b \cdot g(a) \cdot b^{-1}$ holds.*

Proof. See [Bou73, Chapter 8, §10, Theorem 1]. □

Corollary 1.63. *Let k be a field, and let A be a central simple algebra over k. Let B and C be two simple k-subalgebras of A. Then any k-algebra isomorphism $f\colon B \to C$ is induced by an inner k-algebra automorphism of A.*

Proof. Let $i\colon B \to A$ and $j\colon C \to A$ be the k-algebra inclusion maps of B and C in A. Consider the k-algebra homomorphisms $j \circ f$ and $i \circ \mathrm{id}_B$, where id_B is the identity map on B, and apply the previous theorem to these maps. Then there exists $a \in A^*$ such that for all $b \in B$ we have the identity $f(b) = aba^{-1}$, implying that f is induced by an inner k-algebra automorphism of A. □

Corollary 1.64. *Let k be a field, and let A be a central simple k-algebra. Then any k-algebra automorphism of A is inner.*

Proof. Let $f\colon A \to A$ be a k-algebra automorphism and observe that A is a simple k-subalgebra of itself. Applying the previous corollary to f, we see that f is in fact an inner k-algebra automorphism of A. □

Chapter 2

The Brauer group

In this chapter we construct the Brauer group of a field without any deep set theoretic detail. A set theorist is referred to [Bou73, Chapter 8, §10.4] for a more detailed construction of the Brauer group of a field.

1. Construction

Let k be a field, and let $\mathrm{CSA}(k)$ be the class of all central simple algebras over k. We say that two central simple k-algebras A and B are *similar*, denoted by $A \sim B$, if there are positive integers m and n such that $\mathrm{M}_m(A)$ is isomorphic to $\mathrm{M}_n(B)$ as a k-algebra. In the next lemma we prove that this defines an equivalence relation on $\mathrm{CSA}(k)$, which reduces to k-algebra isomorphism when the two central simple algebras have the same rank over k.

Lemma 2.1. *Let k be a field. Then $\sim$ is an equivalence relation on* $\mathrm{CSA}(k)$*, which reduces to k-algebra isomorphism when two central simple algebras have the same rank over k.*

Proof. Observe that $\sim$ is clearly reflexive and symmetric on $\mathrm{CSA}(k)$. Let A, B and C be elements of $\mathrm{CSA}(k)$ such that $A \sim B$ and $B \sim C$. Then there are $m, n, s, t \in \mathbb{Z}_{>0}$ such that the k-algebra isomorphisms $\mathrm{M}_m(A) \cong \mathrm{M}_n(B)$ and $\mathrm{M}_s(B) \cong \mathrm{M}_t(C)$ hold. It follows that the k-algebra isomorphisms

$$\mathrm{M}_{sm}(A) \cong \mathrm{M}_s(\mathrm{M}_m(A)) \cong \mathrm{M}_s(\mathrm{M}_n(B)) \cong \mathrm{M}_n(\mathrm{M}_s(B)) \cong \mathrm{M}_n(\mathrm{M}_t(C)) \cong \mathrm{M}_{nt}(C)$$

hold; hence, $A \sim C$ holds. Consequently, $\sim$ is also a transitive relation on $\mathrm{CSA}(k)$, and therefore an equivalence relation on $\mathrm{CSA}(k)$.

Suppose A and B are two elements of $\mathrm{CSA}(k)$ of the same rank that are similar. Then there are $m, n \in \mathbb{Z}_{>0}$ such that the k-algebra isomorphism $\mathrm{M}_m(A) \cong \mathrm{M}_n(B)$ holds. Observe that we have that $[\mathrm{M}_m(A) : k] = m^2 \cdot [A : k] = [\mathrm{M}_n(B) : k] = n^2 \cdot [B : k]$ holds, from which the equality $[A : k] = [B : k]$ implies that $m^2 = n^2$ holds. Now, it is clear that the k-algebra isomorphism $\mathrm{M}_m(A) \cong \mathrm{M}_m(B)$ holds if and only if the k-algebra isomorphism $A \cong B$ holds. □

The next lemma shows that the tensor product is a class invariant under similarity.

Lemma 2.2. *Let k be a field, and let A, B, A' and B' be central simple k-algebras such that $A \sim A'$ and $B \sim B'$. Then $A \otimes_k B \sim A' \otimes_k B'$.*

Proof. There exist $m, n, s, t \in \mathbb{Z}_{>0}$ such that the k-algebra isomorphisms $\mathrm{M}_m(A) \cong \mathrm{M}_n(A')$ and $\mathrm{M}_s(B) \cong \mathrm{M}_t(B')$ hold. Observe that we have the k-algebra isomorphism

$$\mathrm{M}_m(A) \otimes_k \mathrm{M}_s(B) \cong \mathrm{M}_n(A') \otimes_k \mathrm{M}_t(B'),$$

and that Proposition 1.18 implies that we have the k-algebra isomorphism

$$\mathrm{M}_{ms}(A \otimes_k B) \cong \mathrm{M}_{nt}(A' \otimes_k B').$$

Hence, $A \otimes_k B$ and $A' \otimes_k B'$ are similar. □

Observe that for a field k the class $\mathrm{CSA}(k)$ is not empty, since for every $n \in \mathbb{Z}_{>0}$ the matrix algebra $\mathrm{M}_n(k)$ is an element of $\mathrm{CSA}(k)$. We are now ready to prove the main theorem of this section.

Theorem 2.3. *Let k be a field. Then there exists a pair (G, s) consisting of a group G and a surjective map $s\colon \mathrm{CSA}(k) \to G$ that for every two central simple k-algebras A and B satisfies:* (i) *the equality $s(A \otimes_k B) = s(A) \cdot s(B)$ holds;* (ii) *the equality $s(A) = s(B)$ holds if and only if A and B are similar. Moreover, the pair (G, s) is uniquely determined up to a unique isomorphism, that is, if (G', s') is another pair satisfying the above, then there is a unique group isomorphism $\sigma\colon G \to G'$ such that we have the equality $s' = \sigma \circ s$.*

Proof. Let H be a subclass of $\mathrm{CSA}(k)$ that is a set such that every element of $\mathrm{CSA}(k)$ is isomorphic as a k-algebra to at least one element of H, and let G be the quotient set of H by $\sim$. For those who are interested, it is easy to show that such a set does exist. For an element A of $\mathrm{CSA}(k)$ we let $[A]$ denote the element of G that contains the elements of H that are similar to A, which gives a surjective map $s\colon \mathrm{CSA}(k) \to G$ defined by $B \mapsto [B]$.

We will now show that G is an abelian group under the tensor product over k. To this end, observe that the map $\cdot : G \times G \to G$ given by $([A], [B]) \mapsto [A \otimes_k B]$ is well-defined by Lemma 2.2; hence, it remains to prove that G satisfies the group axioms and commutativity with respect to the tensor product. Observe that for any central simple k-algebra A it clearly holds that $A \otimes_k k$ is isomorphic to A as a k-algebra; hence, $[k]$ functions as the identity element of G under the tensor product over k. Associativity follows from Proposition 1.15, and commutativity follows from Proposition 1.14. At last, the existence of inverse elements in G is proven by Lemma 1.55, which states that the inverse of an element $[A]$ of G is given by the element containing the opposite algebra of A. Thus, we have showed that G is an abelian group under the tensor product over k.

Furthermore, it is clear that for every $A, B \in \mathrm{CSA}(k)$ the map s satisfies the equality $s(A \otimes_k B) = s(A) \cdot s(B)$; hence, we have a pair (G, s) that satisfies the theorem. Now, suppose (G', s') is another pair that satisfies the theorem, and define $\sigma\colon G \to G'$ by $[A] \mapsto s'(A)$. It is easily checked that σ is a unique group isomorphism; hence, we have the equality $s = \sigma \circ s'$. It follows that (G, s) is uniquely determined up to isomorphism. □

Definition 2.4. Let k be a field. The group of the uniquely determined pair (G, s) is called the Brauer group of k, denoted by $\mathrm{Br}(k)$, and is written multiplicatively. For a central simple algebra A over k we denote $s(A)$ by $[A]$. Moreover, an element b of $\mathrm{Br}(k)$ is often denoted by $[A]$, where A is an element of $\mathrm{CSA}(k)$ that is similar to an element of b.

Proposition 2.5. *Let k be a field. Then every element of $\mathrm{Br}(k)$ contains a unique central division k-algebra up to isomorphism.*

Proof. Let $[A]$ be an element of $\mathrm{Br}(k)$. By Corollary 1.49 there exist a unique $n \in \mathbb{Z}_{>0}$ and a unique central division k-algebra D up to isomorphism such that A is isomorphic to $\mathrm{M}_n(D)$ as a k-algebra. It follows that D and A are similar; hence, D is an element of $[A]$. Suppose D' is another central division algebra over k that is similar to A. Then there are $m, n \in \mathbb{Z}_{>0}$ such that the k-algebra isomorphism $\mathrm{M}_m(D) \cong \mathrm{M}_n(D')$ holds. Applying Corollary 1.49 to $\mathrm{M}_m(D)$ and $\mathrm{M}_n(D')$, it immediately follows that $m = n$ holds and that D is isomorphic to D' as a k-algebra . □

2. Examples of Brauer groups

We have already seen in Corollary 1.51 of Chapter 1 that there are no non-trivial central division algebras over an algebraically closed field. Hence, the Brauer group of an algebraically closed field is trivial. Furthermore, Wedderburn proved in 1905 that any finite division ring is a field (see [Bou73, Chapter 8, §11.1, Theorem 1]), implying that the Brauer group of a finite field is also trivial. There is actually a more general family of fields to which finite fields and algebraically closed fields belong, and for which the Brauer group is trivial, the so-called *quasi-algebraically closed fields*.

Definition 2.6. Let $i \in \mathbb{Z}_{>0}$. We say that a field k is C_i if for every $n \in \mathbb{Z}_{>0}$ every non-constant homogeneous polynomial $f \in k[X_1, \ldots, X_n]$ with $(\deg f)^i < n$ has a non-trivial zero. In particular, we say that k is *quasi-algebraically closed* if k is C_1.

Remark 2.7. It is clear that if a field is C_i for some $i \in \mathbb{Z}_{>0}$, then it is also C_j for all $j \in \mathbb{Z}_{\geq i}$.

The statement that a finite field is C_1 is a direct corollary of the Chevalley-Warning Theorem due to Claude Chevalley (1909-1984) and Ewald Warning (1910–1999).

Theorem 2.8 (Chevalley-Warning)**.** *Let k be a finite field, and let $n, m \in \mathbb{Z}_{>0}$. Let $f_1, \ldots, f_m \in k[X_1, \ldots, X_n]$ be non-constant polynomials with $\sum_{i=1}^{m} \deg(f_i) < n$. Then the zero-locus $\mathrm{Z}(f_1, \ldots, f_m) \subset k^n$ has cardinality divisible by p.*

Proof. See [Ax64]. □

Corollary 2.9. *A finite field is C_1.* □

Proposition 2.10. *An algebraically closed field is C_0.*

Proof. See [Lan52, Part I, Theorem 1]. □

Theorem 2.11. *The Brauer group of a C_1 field is trivial.*

Proof. See [Sta08, Proposition 3.2]. □

In 1877 Ferdinand Frobenius (1849–1917) showed that a real division algebra is either isomorphic to $\mathbb{R}$, $\mathbb{H}$ or $\mathbb{C}$, see [FD93, Theorem 3.20] for a proof. Since $\mathbb{C}$ is not central over $\mathbb{R}$, it follows that $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z}$ holds.

3. The Brauer group as a functor

Proposition 2.12. *For each field homomorphism $f\colon k \to l$ there is a unique group homomorphism $\mathrm{Br}(f)\colon \mathrm{Br}(k) \to \mathrm{Br}(l)$ that satisfies $[A] \mapsto [A_f]$.*

Proof. Let $f\colon k \to l$ be a field homomorphism, and let A be a central simple algebra over k. By Proposition 1.52 it holds that A_f is central simple over l. Define the map $\mathrm{Br}(f)\colon \mathrm{Br}(k) \to \mathrm{Br}(l)$ by $[A] \mapsto [A_f]$, and observe that this is a well-defined function by Lemma 2.2. Moreover, by associativity and commutativity of the tensor product we have that

$$\begin{aligned}
\mathrm{Br}(f)\left([A] \cdot_k [B]\right) = [A \otimes_k l] \cdot_l [B \otimes_k l] &= [(A \otimes_k l) \otimes_l (l \otimes_k B)] \\
&= [(A \otimes_k (l \otimes_l (l \otimes_k B))] \\
&= [A \otimes_k (l \otimes_k B)] \\
&= [(A \otimes_k B) \otimes_k l] = \mathrm{Br}(f)\left([A \otimes_k B]\right),
\end{aligned}$$

holds, that is, $\mathrm{Br}(f)$ is a group homomorphism. It is clear that $\mathrm{Br}(f)$ is uniquely determined. □

Let **Fld** denote the category of fields with the morphisms given by field homomorphisms, and let **Ab** denote the category of abelian groups with morphisms given by group homomorphisms.

Theorem 2.13. *The Brauer group defines a covariant functor* $\mathrm{Br}\colon$ **Fld** $\to$ **Ab** *that maps a field k to* $\mathrm{Br}(k)$ *and maps a field homomorphism f to* $\mathrm{Br}(f)$.

Proof. Observe that $\mathrm{Br}(\mathrm{id}_k) = \mathrm{id}_{Br(k)}$ clearly holds for every field k. Furthermore, let $f\colon k \to l$ and $g\colon l \to m$ be two field homomorphisms, and let $[A]$ be an element of $\mathrm{Br}(k)$. Then we have that $\mathrm{Br}(g \circ f)([A]) = [A \otimes_k m]$ and $(\mathrm{Br}(g) \circ \mathrm{Br}(f))\left([A]\right) = [(A \otimes_k l) \otimes_l m] = [A \otimes_k m]$ hold by associativity of the tensor product. It follows that Br is a covariant functor from **Fld** to **Ab**. □

Passing to the next section, we first give a name to the kernel of the map $\mathrm{Br}(f)$ for every field homomorphism $f\colon k \to l$, which is only non-trivial if $f\colon k \to l$ is a non-trivial field extension. This kernel, containing all classes of central simple k-algebras that are split by l, will prove to be very useful in studying the Brauer group and is called *the relative Brauer group* of the field extension $l \supset k$, denoted $\mathrm{Br}(l/k)$.

Lemma 2.14. *Let k be a field, and let A be a central simple algebra over k. Let n be the degree of A, and let $l \supset k$ be a field extension. Then l is a splitting field for A if and only if $[A]$ is an element of* $\mathrm{Br}(l/k)$.

Proof. Suppose l splits A, and let B be a central simple k-algebra similar to A. Then there are $i, j \in \mathbb{Z}_{>0}$ such that $\mathrm{M}_i(A)$ is isomorphic to $\mathrm{M}_j(B)$ as a k-algebra. As l splits A, we have the l-algebra isomorphisms $\mathrm{M}_i(A) \otimes_k l \cong \mathrm{M}_i(A_l) \cong \mathrm{M}_{in}(l)$ by Corollary 1.18 and Lemma 1.16. Hence, the l-algebra isomorphism $\mathrm{M}_j(B_l) \cong \mathrm{M}_{in}(l)$ holds, implying B_l and l are similar central simple l-algebras. It follows that B is also split by l.

The converse holds by definition of the relative Brauer group. □

4. Relative Brauer groups

In this section we show that for every central simple algebra A over a field k there exists a finite Galois extension of k that splits A. This enables us to write the Brauer group of k as a union of relative Brauer groups of finite Galois extensions of k.

Theorem 2.15. *Let k be a field, and let $l \supset k$ be a finite field extension of degree n. If x is an element of $\mathrm{Br}(l/k)$, then x has a representative A of degree n over k that is unique up to isomorphism and contains l as a strictly maximal subfield.*

Proof. See [Mil11, Chapter 4, Corollary 3.6]. □

The above theorem together with Theorem 1.60 imply the following important theorem.

Theorem 2.16. *Let k be a field, and let $l \supset k$ be a finite field extension of degree n. Then an element x of $\mathrm{Br}(k)$ is an element of $\mathrm{Br}(l/k)$ if and only if x has a representative A of degree n over k that is unique up to isomorphism and contains l as a strictly maximal subfield.*

Proof. This follows from the above theorem and Theorem 1.60. □

Theorem 2.17 (Jacobson-Noether). *Let k be a field, and let D be a noncommutative central division algebra over k. Then there is an element $x \in D \setminus \mathrm{Z}(D)$ that is separable over k.*

Proof. See [Ker07, §5.5]. □

Theorem 2.18. *Let k be a field, and let x be an element of $\mathrm{Br}(k)$. Then there is a separable field extension $l \supset k$ such that x is an element of $\mathrm{Br}(l/k)$.*

Proof. If $x = [k]$ holds, then the statement is trivial. Assume $x \neq [k]$ holds, and let D be a central division algebra in x. By the previous theorem there are separable subfields of D containing k. Let l be a subfield of D containing k that is maximal with respect to the property that $l \supset k$ is separable. Observe that the k-subalgebra $C_A(l)$ is a division k-algebra containing l. Moreover, Corollary 1.58 states that $l = C_A(C_A(l))$ holds, that is, l is the center of $C_A(l)$. Hence, $C_A(l)$ is a central division l-algebra. Assume that $l \neq C_A(l)$. By Theorem 2.17 there is $x \in C_A(l) \setminus l$ such that $l(x) \supset l$ is a non-trivial separable extension. Then $l(x)$ is a subfield of D strictly larger than l and separable over k, which contradicts the maximality of l with respect to separability. It follows that $l = C_A(l)$ holds; hence, Theorem 2.16 asserts that l is a splitting field for x. □

Corollary 2.19. *Let k be a field, and let x be an element of $\mathrm{Br}(k)$. Then there is a finite Galois field extension $l \supset k$ such that x is an element of $\mathrm{Br}(l/k)$.*

Proof. Let D be a central division algebra in x. By the previous theorem there is a separable field extension $l \supset k$ that splits D. Consider the normal closure of $l \supset k$, say m, and observe that $m \supset k$ is Galois. Let f be the inclusion of k in l, and let g be the inclusion of l in m. Since $f_*(x) = [l]$ holds, the functoriality of the Brauer group asserts that $(g_* \circ f_*)(x) = [m]$ holds. □

Corollary 2.20. *Let k be a field. Then the equality $\mathrm{Br}(k) = \bigcup_{l \supset k \text{ finite Galois}} \mathrm{Br}(l/k)$ holds.*

Proof. Let x be an element of $\mathrm{Br}(k)$, and let D be a central division algebra over k in x.

Then by Corollary 2.19 there exists a finite Galois extension $l \supset k$ such that x is an element of $\mathrm{Br}(l/k)$. This implies that $\mathrm{Br}(k)$ is contained in $\bigcup_{l/k \text{ finite Galois}} \mathrm{Br}(l/k)$. On the other hand, the relative Brauer group of any field extension $l \supset k$ is by definition a subgroup of $\mathrm{Br}(k)$; hence, the opposite inclusion clearly holds. □

5. Crossed product algebras

In this section we will construct central simple algebras over a field k via a finite Galois field extension of k. With these central simple algebras at hand we then give the cohomological description of the Brauer group. From this point forward we will assume the reader is familiar with the basics of group cohomology, for which we refer to Chapter 2 of [Mil11] or Chapter 4 of [CF67].

Theorem 2.21. *Let k be a field, and let $l \supset k$ be a finite Galois extension. Let a be a 2-cocycle of G with values in l^*, and let A be the left vector space over L with basis $\{e_\sigma\}_{\sigma \in G}$ for which multiplication is defined by*

$$\left(\sum_{\sigma \in G} x_\sigma e_\sigma\right) \cdot \left(\sum_{\tau \in G} y_\tau e_\tau\right) = \sum_{\sigma \in G} \sum_{\tau \in G} x_\sigma \sigma(y_\tau) a(\sigma, \tau) e_{\sigma\tau},$$

where $x_\sigma, y_\tau \in L$ for $\sigma, \tau \in G$. Then A is a central simple algebra over k that contains l as a strictly maximal subfield.

Proof. See [Ker07, 7.5]. □

Definition 2.22. The central simple algebra A over k defined in Theorem 2.21 is called the *crossed product algebra* over k of l and G with respect to a, denoted by (l, G, a).

Proposition 2.23. *Let k be a field, and let $l \supset k$ be a finite Galois extension with Galois group G. Then two 2-cocycles a and b of G with values in l^* are cohomologous if and only if (l, G, a) and (l, G, b) are isomorphic as k-algebras.*

Proof. See [Ker07, 7.7]. □

Theorem 2.24. *Let k be a field, and let x be an element of* $\mathrm{Br}(k)$*. Then for each finite Galois extension $l \supset k$ that splits x, there exists a 2-cocycle a of* $\mathrm{Gal}(l/k)$ *with values in l^* that is unique up to cohomology such that the crossed product algebra $(l, \mathrm{Gal}(l/k), a)$ over k is a representative of x.*

Proof. Let k be a field, and let x be an element of $\mathrm{Br}(k)$. Let $l \supset k$ be a finite Galois extension that splits x, which exists by Corollary 2.20. By Theorem 2.16 there is a representative A of x that is unique up to isomorphism and contains l as a maximal subfield. Let G be the Galois group of $l \supset k$. By Corollary 1.63 any element $\sigma \in G$ is induced by an inner k-algebra automorphism of A, that is, for any $\sigma \in G$ there exists an invertible element $e_\sigma \in A$ such that

$$\text{for all } c \in l \text{ the identity } \sigma(c) = e_\sigma c e_\sigma^{-1} \text{ holds.} \tag{2.1}$$

This gives a map $e\colon G \to A^*$ defined by $\sigma \mapsto e_\sigma$ that for each $\sigma \in G$ satisfies , which we will call a *basis-map* for A. For any basis-map e and any $\sigma \in G$ we usually denote $e(\sigma)$ by e_σ.

Let e and f be two basis-maps for A, and let $\sigma \in G$. Then for every $c \in l$ the identity $e_\sigma c e_\sigma^{-1} = f_\sigma c f_\sigma^{-1}$ holds, implying that $f_\sigma^{-1} e_\sigma$ centralizes l. As l is a strictly maximal subfield of A, it is equal to its centralizer in A. Hence, the identity $e_\sigma = d f_\sigma$ holds for some $d \in l^*$, that is, a basis-map for A is unique up to multiplication by elements of l^*.

Observe that for $\sigma, \tau \in G$ the product $e_\sigma e_\tau$ and the element $e_{\sigma\tau}$ both satisfy () for $\sigma\tau$. Hence, there exists an $a(\sigma, \tau) \in l^*$ such that $e_\sigma e_\tau = a(\sigma, \tau) e_{\sigma\tau}$ holds. This gives a map $a\colon G \times G \to l^*$ defined by $(\sigma, \tau) \mapsto a(\sigma, \tau)$ that for each $\sigma, \tau \in G$ satisfies the equality $e_\sigma e_\tau = a(\sigma, \tau) e_{\sigma\tau}$. Observe that for every $\rho, \sigma, \tau \in G$ the map a satisfies the equality $e_\rho a(\sigma, \tau) = \rho(a(\sigma, \tau)) e_\rho$. Moreover, for every $\rho, \sigma, \tau \in G$ the associativity law on A implies that the identities

$$(e_\rho e_\sigma) e_\tau = a(\rho, \sigma) e_{\rho\sigma} e_\tau = a(\rho, \sigma) a(\rho\sigma, \tau) e_{\rho\sigma\tau}$$

and

$$e_\rho (e_\sigma e_\tau) = e_\rho a(\sigma, \tau) e_{\sigma\tau} = \rho(a(\sigma, \tau)) e_\rho e_{\sigma\tau} = \rho(a(\sigma, \tau)) a(\rho, \sigma\tau) e_{\rho\sigma\tau}$$

are equal. It follows that for every $\rho, \sigma, \tau \in G$ the map a satisfies the equality

$$a(\rho, \sigma) a(\rho\sigma, \tau) = \rho(a(\sigma, \tau)) a(\rho, \sigma\tau),$$

hence the map a is a 2-cocycle of G with values in l^*.

Let e be a basis-map for A, then Lemma 1 in section 7.3 of [Ker07] implies that the image of e defines a basis for A as left vector space over l. For $\alpha, \beta \in A$ write $\alpha = \sum_{\sigma \in G} x_\sigma e_\sigma$ and $\beta = \sum_{\tau \in G} y_\tau e_\tau$, where $x_\sigma, y_\tau \in l$ for $\sigma, \tau \in G$. Recall that for each $\sigma, \tau \in G$ and $a \in l$ we have the identities $e_\sigma a = \sigma(a) e_\sigma$ and $e_\sigma e_\tau = a(\sigma, \tau) e_{\sigma\tau}$. This gives the equality

$$\left(\sum_{\sigma \in G} x_\sigma e_\sigma\right) \cdot \left(\sum_{\tau \in G} y_\tau e_\tau\right) = \sum_{\sigma \in G} \sum_{\tau \in G} x_\sigma \sigma(y_\tau) a(\sigma, \tau) e_{\sigma\tau},$$

hence A is a crossed product algebra over k of l and G with respect to a.

It now rests to show that different basis-maps for A give isomorphic crossed product algebras over k. To this end, let e and f be two basis-maps for A, and let a and b be the corresponding 2-cocycles of G with values in l^*, respectively. Then for $\sigma \in G$ we have that $e_\sigma = \varphi(\sigma) f_\sigma$ holds for some $\varphi(\sigma) \in l^*$. This gives a map $\varphi\colon G \to l^*$ defined by $\sigma \mapsto \varphi(\sigma)$ that for each $\sigma \in G$ satisfies the equality $e_\sigma = \varphi(\sigma) f_\sigma$. It is easy to check that for every $\sigma, \tau \in G$ the equality

$$b(\sigma, \tau) = \frac{\varphi(\sigma)\sigma(\varphi(\tau))}{\varphi(\sigma\tau)} a(\sigma, \tau)$$

holds; hence, a and b are cohomologous 2-cocycles. It follows by Proposition 2.23 that (l, G, a) and (l, G, b) are isomorphic as k-algebras. This finishes the proof of Theorem 2.24. □

Theorem 2.25. *Let k be a field, and let $l \supset k$ be a finite Galois extension. Then the map $f\colon \mathrm{H}^2(\mathrm{Gal}(l/k), l^*) \to \mathrm{Br}(l/k)$ given by $[a] \mapsto [(l, \mathrm{Gal}(l/k), a)]$ is a bijection.*

Proof. Let $G = \mathrm{Gal}(l/k)$. Observe that for a 2-cocycle a of G with values in l^* we have that (l, G, a) is a central simple k-algebra that contains l as a strictly maximal subfield by Theorem 2.21. Hence, $[(l, G, a)]$ is contained in $\mathrm{Br}(l/k)$ by Theorem 2.16. Furthermore, by

Proposition 2.23 cohomologous 2-cocycles a and b of G with values in l^* define isomorphic as k-algebras crossed product algebras (l, G, a) and (l, G, b). It follows that the map f is well-defined.

Moreover, Proposition 2.23 also implies that two 2-cocycles a and b of G with values in l^* with equal images under f are cohomologous; hence, f is injective. By Theorem 2.24 we know that for any element x of $\mathrm{Br}(l/k)$ there exists a 2-cocycle a of G with values in l^* such that $x = [(l, G, a)]$ holds, which proves that f is surjective. It follows that f is a bijection. □

The next lemma shows that the bijection f in the theorem above is multiplicative, which implies that f is a group isomorphism.

Lemma 2.26. *Let k be a field, and let $l \supset k$ be a finite Galois extension. Let a and b be two 2-cocycles of $\mathrm{Gal}(l/k)$ with values in l^*. Then the equality $[(l, \mathrm{Gal}(l/k), a)] \cdot [(l, \mathrm{Gal}(l/k), b)] = [(l, \mathrm{Gal}(l/k), ab)]$ holds in $\mathrm{Br}(k)$.*

Proof. See [Ker07, 8.2]. □

Theorem 2.27. *Let k be a field, and let $l \supset k$ be a finite Galois extension. Then the map $f\colon \mathrm{H}^2(\mathrm{Gal}(l/k), l^*) \to \mathrm{Br}(l/k)$ given by $[a] \mapsto [(l, \mathrm{Gal}(l/k), a)]$ is a group isomorphism.* □

Theorem 2.28. *Let k be a field, and let k_{sep} be a separable closure of k. Then $\mathrm{Br}(k)$ and $\mathrm{H}^2(\mathrm{Gal}(k_{\mathrm{sep}}/k), k_{\mathrm{sep}}^*)$ are isomorphic as groups.*

Proof. See [Ker07, 8.4]. □

Chapter 3

The Brauer group is torsion

Let k be a field. Given a finite field extension $l \supset k$ and a central simple algebra A over l, we wish to construct a central simple algebra over k from A. In the case that $l \supset k$ is a finite separable field extension, this is done by the corestriction functor in group cohomology, see [Bro82, Chapter 3, §9] or [Mil11, Chapter 2, Example 1.29]. We will briefly study this case, and study the case that $l \supset k$ is a finite purely inseparable field extension. Combining these two cases we define a group homomorphism from $\mathrm{Br}(l)$ to $\mathrm{Br}(k)$ for any finite field extension $l \supset k$, which we will use to define a contravariant functor from the category of fields with morphisms given by finite field extensions to the category **Ab**. By means of this functor we will show that the Brauer group is torsion.

1. The corestriction of central simple algebras

Definition 3.1. Let $f\colon k \to l$ be a field homomorphism. Then the *degree* of f is the dimension of l as vector space over $\mathrm{im}(f)$, denoted by $\deg(f)$, or by $[l : k]$ when the map f is understood.

The following definition defines the algebra-theoretic analogue of the corestriction map Cor on the second cohomology groups, where the latter is defined in [Bro82, Chapter 3, §9] or [Mil11, Chapter 2, Example 1.29].

Definition 3.2. Let k be a field, and let $f\colon k \to l$ be a separable field homomorphism of finite degree. Let k_{sep} be a separable closure of k and l. The *corestriction map* $\mathrm{Cor}(f)$ of f is the group homomorphism that makes the following diagram

$$\begin{tikzcd}
\mathrm{Br}(l) \arrow[r, "\mathrm{Cor}(f)"] \arrow[d] & \mathrm{Br}(k) \arrow[d] \\
\mathrm{H}^2(\mathrm{Gal}(k_{\mathrm{sep}}/l), k_{\mathrm{sep}}^*) \arrow[r, "\mathrm{Cor}"'] & \mathrm{H}^2(\mathrm{Gal}(k_{\mathrm{sep}}/k), k_{\mathrm{sep}}^*)
\end{tikzcd}$$

commute, where the vertical maps are the group isomorphisms associated by Theorem 2.28.

Let k be a field, and let $f\colon k \to l$ be a separable field homomorphism of finite degree. We will now briefly give a explicit description of the corestriction map of f, and refer to [Dra83, Chapter 1, §8] or [Ker90, §18] for a more detailed study of this explicit description.

Let k_{sep} be a separable closure of k, and let A be a central simple algebra over l. Let $\mathrm{T}(A)$ denote the tensor product $\bigotimes_{\varphi \in \mathrm{Hom}_k(l, k_{\mathrm{sep}})} A_\varphi$ over l of all extended algebras of A via k-embeddings of l into k_{sep}, and observe that $\mathrm{T}(A)$ is central simple over l. For every σ in the absolute Galois group $\mathrm{Gal}(k_{\mathrm{sep}}/k)$ we have the k-algebra isomorphism $A_{\sigma^{-1}\varphi} \to A_\varphi$ induced by σ. This gives an action of $\mathrm{Gal}(k_{\mathrm{sep}}/k)$ on $\mathrm{T}(A)$, viewed as an algebra over k, given for each $\sigma \in \mathrm{Gal}(k_{\mathrm{sep}}/k)$ by

$$\sigma\left(\otimes_\varphi a_\varphi\right) = \otimes_\varphi b_\varphi, \text{ where } b_\varphi = \sigma(a_{\sigma^{-1}\varphi}).$$

By [Ker90, §18] the invariant ring $\mathrm{T}(A)^{\mathrm{Gal}(k_{\mathrm{sep}}/k)}$ is a central simple algebra over k.

Proposition 3.3. *Let k be a field, and let $f\colon k \to l$ be a finite separable field extension. Then the map from $\mathrm{Br}(l)$ to $\mathrm{Br}(k)$ defined by $[A] \mapsto \left[\mathrm{T}(A)^{\mathrm{Gal}(k_{\mathrm{sep}}/k)}\right]$ is the corestriction map of f.*

Proof. See [Rie70, Theorem 11]. ■

Proposition 3.4. *Let k be a field, and let $f\colon k \to l$ be a finite separable field extension. Then for every x in $\mathrm{Br}(k)$ we have the equality $(\mathrm{Cor}(f) \circ \mathrm{Br}(f))(x) = x^{\deg(f)}$.*

Proof. See [Ker90, §18]. □

Remark 3.5. As $\mathrm{Br}(f)$ is clearly the analogue of the restriction map in group cohomology (see [Mil11, Chapter 2, Example 1.27]), the above proposition follows directly from [Mil11, Chapter 2, Proposition 1.30].

Now, we study the case of central simple algebras over a finite purely inseparable field extension of a given field. To this end, let k be a field of characteristic p, with p a prime number. We let Frob_k denote the Frobenius endomorphism of k, given by $x \mapsto x^p$. The following theorem shows that the group homomorphism $\mathrm{Br}(\mathrm{Frob}_k)$ is equal to the homomorphism $\mathrm{Br}(k) \to \mathrm{Br}(k)$ given by $x \mapsto x^p$.

Theorem 3.6. *Let k be a field of characteristic p, with p a prime number. Then for any element $[A]$ of $\mathrm{Br}(k)$ the identity $[A]^p = [A_{\mathrm{Frob}_k}]$ holds.*

Proof. See [Jac10, Theorem 4.1.2]. □

A direct corollary of this theorem is that the p-torsion subgroup of the Brauer group of a perfect field of characteristic p, with p a prime number, is trivial.

Corollary 3.7. *Let k be a perfect field of characteristic p, with p a prime number. Then every element x of finite order in $\mathrm{Br}(k)$ has order not divisible by p.*

Proof. Write $x = [A]$. Observe that the equality $\left[(A_{\mathrm{Frob}_k})_{\mathrm{Frob}_k^{-1}}\right] = [A]$ holds. This means that $[A_{\mathrm{Frob}_k}]$ is not equal to $[k]$ if x is non-trivial, since the extended algebra $A_{\mathrm{Frob}_k^{-1}}$ is unequal to A if x is non-trivial. Hence, for every non-trivial element $[A]$ in $\mathrm{Br}(k)$ we have that $[A_{\mathrm{Frob}_k}] = [A]^p$ is unequal to $[k]$ in $\mathrm{Br}(k)$. □

Definition 3.8. Let k be a field of characteristic p, with p a prime number. Let $f\colon k \to l$ be a finite purely inseparable field extension, and let p^n be the degree of f. Then n is called the *exponent* of f, denoted by $\exp(f)$, or by $\exp[l : k]$ when the map f is understood.

Let $f\colon k \to l$ be a finite purely inseparable field extension. Observe that the image of $\mathrm{Frob}_l^{\exp(f)}$ is contained in k, since $l \supset k$ is purely inseparable. Hence, there exists a field homomorphism $\alpha(f)$ such that we have the equality $\mathrm{Frob}_l^{\exp(f)} = f \circ \alpha(f)$. We define the map $\mathrm{Br}^{\mathrm{o}}(f)\colon \mathrm{Br}(l) \to \mathrm{Br}(k)$ by $x \mapsto \mathrm{Br}(\alpha(f))(x)$, which is a group homomorphism by definition.

Proposition 3.9. *Let k be a field of characteristic p, with p a prime number. Let $f\colon k \to l$ be a finite purely inseparable field extension. Then for each x in $\mathrm{Br}(k)$ we have the equality $(\mathrm{Br}^{\mathrm{o}}(f) \circ \mathrm{Br}(f))(x) = x^{\deg(f)}$.*

Proof. We have the equalities $\mathrm{Br}^{\mathrm{o}}(f) \circ \mathrm{Br}(f) = \mathrm{Br}(\alpha(f)) \circ \mathrm{Br}(f) = \mathrm{Br}(\alpha(f) \circ f)$ by functoriality of the Brauer group. It is easy to check that $\alpha(f) \circ f$ is equal to the homomorphism $\mathrm{Frob}_k^{\exp(f)}$. Now, by Theorem 3.6 we have for each x in $\mathrm{Br}(k)$ the equality $\mathrm{Br}(\mathrm{Frob}_k^{\exp(f)})(x) = x^{\deg(f)}$. □

For each finite field homomorphism $f\colon k \to l$ we will now construct a group homomorphism $\mathrm{Br}^{\mathrm{o}}(f)\colon \mathrm{Br}(l) \to \mathrm{Br}(k)$ by combining the corestriction map and the map defined above.

Definition 3.10. Let k be a field, and let $f\colon k \to l$ be a field extension. Then l_{s} is the *separable closure* of k in l. Moreover, the inclusion map of l_{s} in l is denoted by f_{pi}, and the inclusion map of k in l_{s} is denoted by f_{s}.

Definition 3.11. Let k be a field, and let $f\colon k \to l$ be a finite field extension. Then we define $\mathrm{Br}^{\mathrm{o}}(f)\colon \mathrm{Br}(l) \to \mathrm{Br}(k)$ as the composed map $\mathrm{Cor}(f_{\mathrm{s}}) \circ \mathrm{Br}^{\mathrm{o}}(f_{\mathrm{pi}})$.

Proposition 3.12. *Let k be a field, and let $f\colon k \to l$ be a finite field extension. Then $\mathrm{Br}^{\mathrm{o}}(f)\colon \mathrm{Br}(l) \to \mathrm{Br}(k)$ is a group homomorphism that for every x in $\mathrm{Br}(k)$ satisfies $(\mathrm{Br}^{\mathrm{o}}(f) \circ \mathrm{Br}(f))(x) = x^{\deg(f)}$.*

Proof. First, observe that $\mathrm{Br}^{\mathrm{o}}(f)$ is a group homomorphism by definition. Now, write $\mathrm{Br}(f) = \mathrm{Br}(f_{\mathrm{pi}} \circ f_{\mathrm{s}})$, and observe that $\mathrm{Br}^{\mathrm{o}}(f) \circ \mathrm{Br}(f) = \mathrm{Cor}(f_{\mathrm{s}}) \circ \mathrm{Br}(\alpha(f_{\mathrm{pi}}) \circ f_{\mathrm{pi}}) \circ \mathrm{Br}(f_{\mathrm{s}})$ holds. It follows that $\mathrm{Br}^{\mathrm{o}}(f) \circ \mathrm{Br}(f)$ is equal to $\mathrm{Cor}(f_{\mathrm{s}}) \circ \mathrm{Br}(\mathrm{Frob}_l^{\exp(f_{\mathrm{pi}})}) \circ \mathrm{Br}(f_{\mathrm{s}})$. Hence, we have that $(\mathrm{Br}^{\mathrm{o}}(f) \circ \mathrm{Br}(f))(x) = x^{\deg(f_{\mathrm{pi}})\deg(f_{\mathrm{s}})} = x^{\deg(f)}$ holds. □

We are now able to state the main result of this section. We let $\mathbf{Fld}_{\mathrm{f}}$ denote the category of fields with the morphisms given by field homomorphisms of finite degree.

Theorem 3.13. *There exists a contravariant functor $\mathrm{Br}^{\mathrm{o}}\colon \mathbf{Fld}_{\mathrm{f}} \to \mathbf{Ab}$ that maps a field k to $\mathrm{Br}(k)$ and a morphism f to $\mathrm{Br}^{\mathrm{o}}(f)$.*

An outline of a proof. Observe that for every field k, we clearly have the equality $\mathrm{Br}^{\mathrm{o}}(\mathrm{id}_k) = \mathrm{id}_{\mathrm{Br}(k)}$.

Now let $f\colon k \to l$ and $g\colon l \to m$ be two field homomorphisms of finite degree. As the corestriction in group cohomology is functorial, it suffices to show that the following diagram

$$\begin{tikzcd}
\mathrm{Br}(l \cdot m) \arrow[r] \arrow[d] & \mathrm{Br}(m) \arrow[d] \\
\mathrm{Br}(l) \arrow[r] & \mathrm{Br}(k)
\end{tikzcd}$$

commutes. ■

2. Index and exponent

We will now prove that the Brauer group is torsion by means of the corestriction functor, and briefly study the index and exponent of an element of the Brauer group. We conclude this chapter by giving a decomposition theorem for central division algebras over a field.

Theorem 3.14. *Let k be a field. Then $\mathrm{Br}(k)$ is a torsion group, and for any field homomorphism $f\colon k \to l$ of finite degree, the relative Brauer group $\mathrm{Br}(l/k)$ is annihilated by $\deg(f)$.*

Proof. Let $f\colon k \to l$ be a field homomorphism of finite degree, and let x be an element of $\mathrm{Br}(l/k)$. By Proposition 3.9 the equality $(\mathrm{Br}^{\mathrm{o}}(f) \circ \mathrm{Br}(f))(x) = x^{\deg(f)}$ holds. Let $1_{\mathrm{Br}(k)}$ and $1_{\mathrm{Br}(l)}$ denote the identity elements of $\mathrm{Br}(k)$ and $\mathrm{Br}(l)$, respectively. As the equality $\mathrm{Br}(f)(x) = 1_{\mathrm{Br}(l)}$ holds, we have that $x^{\deg(f)} = 1_{\mathrm{Br}(k)}$ holds. This means that every element of $\mathrm{Br}(l/k)$ has order dividing $\deg(f)$, and in particular that x has finite order. Now Corollary 2.20 implies that the Brauer group is torsion. □

Definition 3.15. Let k be a field, and let A be a central simple algebra over k. Then the *index* of A is the degree of the central division algebra associated to A by Corollary 1.49, denoted by $\mathrm{ind}(A)$.

Definition 3.16. Let k be a field, and let A be a central simple algebra over k. Then the *exponent* of A is the order of $[A]$ in $\mathrm{Br}(k)$.

Observe that the index and exponent are class invariants under similarity; hence, we may speak of the index and exponent of an element of the Brauer group, which we will simply denote by $\mathrm{ind}(x)$ and $\exp(x)$ for an element x of the Brauer group of some field.

Proposition 3.17. *Let k be a field. Then for every element x of $\mathrm{Br}(k)$ the exponent of x divides the index of x.*

Proof. Let x be an element of $\mathrm{Br}(k)$, and let D be a central division algebra over k representing x. Then a strictly maximal subfield l of D has degree $\mathrm{ind}(D)$ over k, and is in particular a finite field extension of k. As x is an element of $\mathrm{Br}(l/k)$ by Theorem 2.16, the statement follows from Theorem 3.14. □

Proposition 3.18. *Let k be a field, and let x be an element of $\mathrm{Br}(k)$. Then every prime divisor of $\mathrm{ind}(x)$ is a prime divisor of $\exp(x)$.*

Proof. See [Ker07, 9.4]. □

Theorem 3.19. *Let k be a field, and let D be a central division algebra over k. Let $\prod_{i=1}^r p_i^{d_i}$ and $\prod_{i=1}^r p_i^{e_i}$ be the prime factorization of $\mathrm{ind}(D)$ and $\exp(D)$, respectively. Then D is k-algebra isomorphic to ${}_k\bigotimes_{i=1}^r D_i$, where D_i is a unique central division k-algebra up to isomorphism with $\mathrm{ind}(D_i) = p_i^{d_i}$ and $\exp(D_i) = p_i^{e_i}$ for $i = 1, \ldots, r$.*

Proof. See [Ker07, 9.5, 9.6]. □

Bibliography

[AM69] M. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Company, 1969.

[Ax64] J. Ax, *Zeroes of polynomials over finite fields*, American Journal of Mathematics **86** (1964), no. 2, 255–261.

[Bou73] N. Bourbaki, *Elements of mathematics - Algebra*, Springer-Verlag, 1973.

[Bro82] K. S. Brown, *Cohomology of groups*, Springer-Verlag, 1982.

[CF67] J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, 1967.

[CR62] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, John Wiley & Sons, 1962.

[Dor08] F. Doray, *Homological algebra*, Lecture notes, 2008, `http://www.math.leidenuniv.nl/~doray/HomAlg/index.html`.

[Dra83] P. K. Draxl, *Skew fields*, Cambridge University Press, 1983.

[FD93] B. Farb and K. R. Dennis, *Noncommutative algebra*, Springer-Verlag, 1993.

[GS06] P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*, Cambridge University Press, 2006.

[Jac10] N. Jacobson, *Finite-dimensional division algebras over fields*, corr. 2nd printing ed., Springer-Verlag, 2010.

[Ker90] I. Kersten, *Brauergruppen von Körpern*, Friedr. Vieweg & Sohn, 1990.

[Ker07] ———, *Brauergruppen*, Universitätsverlag Göttingen, 2007.

[Lan52] S. Lang, *On quasi algebraic closure*, The Annals of Mathematics **55** (1952), no. 2, 373–390.

[Lan02] ———, *Algebra*, revised third ed., Springer-Verlag, 2002.

[Mac98] S. Maclane, *Categories for the working mathematician*, second ed., Springer-Verlag, 1998.

[Mil11] J. Milne, *Class field theory*, Course notes, 2011, `http://www.jmilne.org/math/CourseNotes/CFT.pdf`.

[Rie70] C. Riehm, *The corestriction of algebraic structures*, Inventiones Mathematicae **11** (1970), no. 1, 73–98.

[Row88] L. Rowen, *Ring theory volume 1*, Academic Press, 1988.

[Sta08] J. M. Starr, *Brauer groups and Galois cohomology of function fields of varieties*, Lecture notes, 2008, `http://www.math.sunysb.edu/~jstarr/papers/Escola_07_08d_nocomments.pdf`.