MSc Mathematics

Track: Algebra and Geometry

Master thesis

Brauer groups of local fields and algebraic number fields

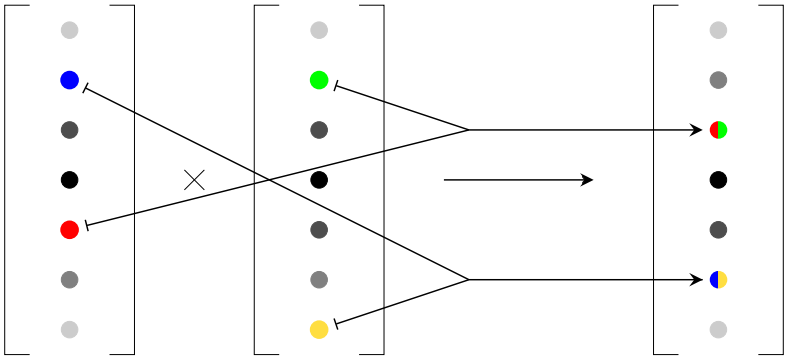
by

David Koetsier

July 20, 2018

Supervisor: prof.dr. Rob de Jeu

Second examiner: dr. Sander Dahmen



Department of Mathematics

Faculty of Sciences

VU UNIVERSITY AMSTERDAM

Abstract

We start by defining and studying modules over rings, algebras over commutative rings, and tensor products of modules and algebras. We define Morita equivalence on the class $\mathbf{CSA}(F)$ of finite-dimensional central simple algebras over a field F, and define the Brauer group $\mathbf{B}(F)$ of F as the group of Morita equivalence classes of $A \in \mathbf{CSA}(F)$ with the product of the classes of A and B in $\mathbf{CSA}(F)$ equal to the class of the tensor product of A and B. Galois cohomology is introduced, and it is used to prove that Brauer groups are torsion groups. We then consider valuations of division rings, and use them and Galois cohomology to prove that Brauer groups of infinite local fields are isomorphic to $\mathbb{Q}/\mathbb{Z}$. Finally, most of these tools are combined to prove a structure theorem for Brauer groups of algebraic number fields.

Title: Brauer groups of local fields and algebraic number fields
Author: David Koetsier, d.f.koetsier@student.vu.nl, 2521126
Supervisor: prof.dr. Rob de Jeu
Second examiner: dr. Sander Dahmen
Date: July 20, 2018

Department of Mathematics
VU University Amsterdam
de Boelelaan 1081, 1081 HV Amsterdam
http://www.math.vu.nl/

Contents

Popular Summary

In this thesis, we define and study the Brauer group $\mathbf{B}(F)$ of a field F. The Brauer group is a group that functions as an invariant of fields, meaning that isomorphic fields have isomorphic Brauer groups. Furthermore, there is a connection between certain properties of a field and certain properties of its Brauer group. We will study some of these connections by, for instance, determining the structure of $\mathbf{B}(F)$ when F is a local field or an algebraic number field, but we will also prove more general properties of Brauer groups, such as the fact that all elements of $\mathbf{B}(F)$ have finite order.

The definition of the group product in the Brauer group $\mathbf{B}(F)$ of a field F is based on the tensor product of F-algebras. An object A is an F-algebra when it is an F-vector space and a ring with unit element 1_A such that the ring multiplication is bilinear. The tensor product $A \otimes B$ of two F-algebras A and B is an F-algebra with some special properties. Some of these special properties somewhat resemble the defining properties of a commutative group product. For instance, if A, B and C are F-algebras, then

$$\begin{aligned} &(A \otimes B) \otimes C \cong A \otimes (B \otimes C), \\ &A \otimes B \cong B \otimes A \qquad \text{and} \\ &A \otimes F \cong F \otimes A \cong A, \end{aligned} \tag{0.1}$$

where all isomorphisms are isomorphisms of F-algebras. Inverses are a problem, however, since for most F-algebras A no F-algebra B exists with $A \otimes B \cong F$.

In order to get around this problem, we restrict ourselves to the class $\mathbf{CSA}(F)$ of finite-dimensional central simple F-algebras. An F-algebra A is finite-dimensional when it is finite-dimensional as an F-vector space, and it is simple when it is simple as a ring. If we define the center $\mathbf{Z}(A)$ as $\mathbf{Z}(A) = \{x \in A |\ xy = yx \text{ for all } y \in A\}$, then A is central precisely when $\mathbf{Z}(A) = 1_A F$. It turns out that the tensor product of A and B in $\mathbf{CSA}(F)$ is again an element of $\mathbf{CSA}(F)$.

We define an equivalence relation on $\mathbf{CSA}(F)$ called Morita equivalence, and use the equivalence classes of this equivalence relation as the objects of the Brauer group $\mathbf{B}(F)$. We then define a product map on $\mathbf{B}(F)$ as $[A][B] = [A \otimes B]$. The definition of Morita equivalence implies that this product map is well-defined and that for each $A \in \mathbf{CSA}(F)$ there exists $B \in \mathbf{CSA}(F)$ with $A \otimes B \in [F]$. Isomorphic F-algebras are Morita equivalent, so (0.1) yields that the product map is associative, commutative and has a unit element $[F]$. We conclude that $[A][B] = [A \otimes B]$ defines a group product on $\mathbf{B}(F)$, so the Brauer group is an abelian group.

As is clear from its definition, the study of $\mathbf{B}(F)$ is closely related to the study of finite-dimensional central simple F-algebras. Because of this, the process of studying the Brauer group will also involve proving a number of theorems on the structure of such algebras.

Introduction

The Brauer group is a piece of abstract algebra with a somewhat involved construction and few, if any, real-world applications. This construction does, however, lead to some interesting mathematics, and it gives useful results of a more theoretical nature. The Brauer group lies at the intersection of various basic algebraical concepts, such as groups, fields, algebras and tensor products, with connections to Galois theory and cohomology. We will thoroughly explore these concepts, connections and the Brauer group itself, with special focus on Brauer groups of local fields and of algebraic number fields.

The reader of this thesis is expected to have a thorough understanding of group theory, ring theory, topology, and Galois theory. The reader is also expected to be familiar with short exact sequences of groups and the Snake Lemma of abelian groups. A basic understanding of cohomology is helpful, but not required.

Both the abstract and popular summary give short descriptions of the definition of the Brauer group $\mathbf{B}(F)$ of a field F, and Section 2.3 of this thesis contains the actual definition, so we will not define it again here.

In Chapter 1 we define modules over rings, algebras over commutative rings and tensor products of each of these structures, and consider some examples. In preparation of the rest of the thesis, we prove a number of basic properties of modules and algebras, with special focus on the tensor products of algebras.

Chapter 2 introduces the notion of central simple algebras. We consider examples, and prove some theorems on their structure. Finally, we define Morita equivalence and the Brauer group , and find some basic properties of the Brauer group. We also determine the structure of $\mathbf{B}(F)$ for F a finite field, $F = \mathbb{R}$ and $F = \mathbb{C}$.

Chapter 3 develops machinery for studying the structure of $\mathbf{B}(F)$ for general fields F. We consider subfields of algebras $A \in \mathbf{CSA}(F)$, and define crossed products, which are algebras with a subfield with special properties. We define a cohomology theory with the name Galois cohomology, and use crossed products to describe a connection between subgroups of $\mathbf{B}(F)$ and a second order Galois cohomology group. This connection is also used to prove that Brauer groups are torsion groups.

In Chapter 4 we define and study valuations of division rings and local fields. We slowly work our way towards a proof that the Brauer group $\mathbf{B}(F)$ of an infinite local field F is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

Chapter 5 studies the Brauer group of algebraic number fields, which are fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ such that the degree $[F : \mathbb{Q}]$ is finite. A full proof of the structure theorem for these Brauer groups is beyond the scope of this text, so we will use without proof three general, powerful theorems from algebra. However, the proof of the structure theorem will still take up most of this chapter and it will use almost all of the tools that we develop in this thesis.

1 Modules and Algebras

In this chapter we lay the groundwork for the other chapters of this thesis. We first define and study modules over rings and tensor products of modules in Sections 1.1 and 1.2, respectively. Next, we define algebras over commutative rings and consider some examples of these algebras in Section 1.3. Section 1.4 contains a number of basic properties of algebras and definitions related to algebras that will be used in later chapters. In Section 1.5 we consider another example of algebras in the form of endomorphism algebras. Finally, in Section 1.6 we define and study the tensor product of algebras. This last section contains three subsections that each describe an application of the Universal Property of the tensor product of algebras.

1.1 Modules over Rings

In this thesis, all rings R are defined to have a unit element 1_R with $x1_R = 1_R x = x$ for all $x \in R$. The identity element under addition is denoted by 0_R. Let R° denote the *unit group* of R, which is the multiplicative group $\{x \in R |\ xy = yx = 1_R \text{ for some } y \in R\}$.

In this section R denotes a ring. The letter F will always denote a field in this thesis.

Definition 1.1. A *right R-module* M consists of an abelian group $(M, +)$ with a *scalar multiplication* $M \times R \to M$, notation $(u, a) \mapsto ua$, such that for all $u, v \in M$ and $a, b \in R$:

i) $(u + v)a = ua + va$;

ii) $u(a + b) = ua + ub$;

iii) $u(ab) = (ua)b$;

iv) $u1_R = u$.

Left R-modules are defined similarly, except that R acts on the left of M in the scalar multiplication. This means that the scalar multiplication is defined as a map from $R \times M$ to M, and that the four axioms are changed accordingly. When appropriate, M_R will denote a right R-module M and ${}_R M$ will denote a left R-module M.

We will drop the words left and right, and simply talk about modules when it is clear from context which is meant, or when the statement applies to both kinds of modules.

Note that when F is a field, F-modules are simply F-vector spaces. This also means that we can define the *dimension* of an F-module M, notation $\dim_F M$, to be its dimension as an F-vector space.

For two right R-modules M and N, a map $\phi : M \to N$ is called a *right R-module homomorphism* when for all $u, v \in M$ and $a \in R$

$$\phi(u+v) = \phi(u) + \phi(v) \quad \text{and}$$
$$\phi(ua) = \phi(u)a.$$

The analogous definition holds for *left R-module homomorphisms*. The term *R-module homomorphism* will be used to refer to either left or right R-module homomorphisms, depending on context. *Module isomorphisms*, *endomorphisms* and *automorphisms* are defined as expected. For M and N two R-modules, the map $M \to N$ defined as $u \mapsto 0_N$ for all $u \in M$ is called the *trivial homomorphism*, where 0_N denotes the identity element for addition in N.

A *submodule* of an R-module M is an R-module N such that N is a subset of M for which the inclusion map is an R-module homomorphism. For any R-module M, $\{0_M\}$ is a submodule consisting of a single element. A module consisting of a single element is called a *trivial module*. If N is a submodule of the R-module M, then the *quotient module* M/N is the R-module that is the quotient of the abelian groups $(M, +)$ and $(N, +)$ with the scalar multiplication $(u + N)a = ua + N$ for all $u \in M$ and $a \in R$.

The *direct product* $\prod_{i \in I} M_i$ of a collection of R-modules M_i with $i \in I$ is the R-module that consists of the Cartesian product of these R-modules M_i with addition and scalar multiplication defined to be componentwise. The *direct sum* $\bigoplus_{i \in I} M_i$ of a collection of R-modules M_i with $i \in I$ is the submodule of $\prod_{i \in I} M_i$ defined as

$$\{(u_i)_{i \in I} |\ u_i = 0_{M_i} \text{ for all but finitely many } i \in I\}.$$

If I is a finite set $\{1, \ldots, n\}$, then the direct sum and direct product are equal, and we sometimes use the notation $M_1 \times M_2 \times \cdots \times M_n$ for $\prod_{i \in I} M_i$ and $M_1 \oplus M_2 \oplus \cdots \oplus M_n$ for $\bigoplus_{i \in I} M_i$. If there are no non-zero elements of the R-modules M_i that are an element of more than one of the modules M_i, then we will often denote elements of $\bigoplus_{i \in I} M_i$ by finite sums of the entries in the various M_i. For instance, an element $(u_i)_{i \in I}$ would be denoted as $\sum_{i \in I} u_i$.

1.2 Tensor Products of Modules

In this section, R denotes a ring.

Definition 1.2. Let M and N be two right R-modules. The *tensor product* of M and N is a right R-module $M \otimes N$ together with a bilinear map $M \times N \to M \otimes N$, notation $(u, v) \mapsto u \otimes v$, such that the following two conditions hold.

i) $M \otimes N$ is generated by $\{u \otimes v |\ u \in M, v \in N\}$ as a right R-module.

ii) (Universal Property) For any right R-module P and bilinear map $\Phi : M \times N \to P$ there exists a unique homomorphism $\phi : M \otimes N \to P$ such that $\phi(u \otimes v) = \Phi(u, v)$ for all $u \in M$ and $v \in N$.

We will prove existence and uniqueness of such an R-module $M \otimes N$ in Theorem 1.6. The elements $u \otimes v$ of $M \otimes N$ with $u \in M$ and $v \in N$ are called *rank one tensors*.

If M and N are both right R-modules and right S-modules for some ring S, then we can apply either the tensor product of R-modules or the tensor product of S-modules, and the resulting modules need not be similar. We will write the tensor product of R-modules M and N as $M \otimes_R N$ whenever we wish to specify the ring R.

If M and N are right R-modules, then the bilinearity of the map $(u, v) \mapsto u \otimes v$ implies that the following equalities hold for all $u, u_1, u_2 \in M$, $v, v_1, v_2 \in N$ and $a, b \in R$:

$$u \otimes (v_1 a + v_2 b) = (u \otimes v_1)a + (u \otimes v_2)b; \tag{1.1}$$

$$(u_1 a + u_2 b) \otimes v = (u_1 \otimes v)a + (u_2 \otimes v)b; \tag{1.2}$$

$$u \otimes 0_N = 0_M \otimes v = 0_{M \otimes N}; \tag{1.3}$$

$$(ua) \otimes v = (u \otimes v)a = u \otimes (va). \tag{1.4}$$

Equation (1.4) and the fact that $M \otimes N$ is generated by the rank one tensors together imply the following lemma.

Lemma 1.3. *Let M and N be right R-modules. All elements of $M \otimes N$ are equal to*

$$u_1 \otimes v_1 + \cdots + u_n \otimes v_n$$

for some $u_1, \ldots, u_n \in M$ and $v_1, \ldots, v_n \in N$.

This lemma will allow us to prove statements for all elements of $M \otimes N$ by first proving them for the rank one tensors and then extending them to finite sums of rank one tensors. However, one has to be careful with this approach, since this representation as a finite sum of rank one tensor is far from unique, and there is not necessarily a canonical way to choose a unique representation of each element of $M \otimes N$. If M and N are right F-modules, then bases can be used to canonically choose unique representations of all elements of $M \otimes N$.

Theorem 1.4. *If M and N are right F-modules with bases $\{u_i |\ i \in I\}$ and $\{v_j |\ j \in J\}$, respectively, then $\{u_i \otimes v_j |\ i \in I, j \in J\}$ is a basis of $M \otimes N$. In particular, if M and N are finite-dimensional over F, then $\dim_F(M \otimes N) = (\dim_F M)(\dim_F N)$.*

Proof. This proof is mostly calculation without interesting insights, so we refer to the proof of Corollary 2.4 of Chapter 16 from [Lang, 2002]. □

The following isomorphisms of tensor products will be important in later sections.

Theorem 1.5. *Let M, N and P be right R-modules.*

i) $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$ by an isomorphism ϕ_1 that maps $(u \otimes v) \otimes w$ to $u \otimes (v \otimes w)$.

ii) $M \otimes N \cong N \otimes M$ by an isomorphism ϕ_2 that maps $u \otimes v$ to $v \otimes u$.

iii) $M \otimes R \cong M$ *by an isomorphism* ϕ_3 *that maps* $u \otimes a$ *to* ua.

iv) $R \otimes M \cong M$ *by an isomorphism* ϕ_4 *that maps* $a \otimes u$ *to* ua.

Proof. The existence of these module homomorphisms can be proven by applying the Universal Property of the tensor product to the right choice of bilinear maps, where the correct choice of bilinear maps should be fairly obvious. In the case of ϕ_1 the Universal Property needs to be applied twice.

In a similar way, we can construct homomorphisms $\psi_1 : M \otimes (N \otimes P) \to (M \otimes N) \otimes P$ such that $u \otimes (v \otimes w) \mapsto (u \otimes v) \otimes w$, and $\psi_2 : N \otimes M \to M \otimes N$ such that $v \otimes u \mapsto u \otimes v$. Furthermore, we can define the homomorphisms $\psi_3 : M \to M \otimes R$ $\psi_4 : M \to R \otimes M$ as $u \mapsto u \otimes 1_R$ and $u \mapsto 1_R \otimes u$, respectively.

The fact that tensor products are generated as R-modules by their rank one tensors implies that ψ_i is an inverse of ϕ_i for each $i = 1, \ldots, 4$. This proves that each ϕ_i is indeed an isomorphism. □

Finally, we need to fulfill our promise of proving the existence and uniqueness of the tensor product of right R-modules.

Theorem 1.6. *For any right* R*-modules* M *and* N*, the tensor product* $M \otimes N$ *exists and is unique up to module isomorphism.*

Proof. Let $\mathbf{F}(M \times N)$ be the free right R-module with the basis $M \times N$. This means that $\mathbf{F}(M \times N)$ is the right R-module consisting of all elements of the form $\sum_{(u,v) \in M \times N} (u, v) c_{u,v}$ with all $c_{u,v} \in R$, $c_{u,v} = 0_R$ for all but finitely many $(u, v) \in M \times N$ and such that $M \times N$ is linearly independent in $\mathbf{F}(M \times N)$. Addition and scalar multiplication in $\mathbf{F}(M \times N)$ are defined as expected.

The R-module $M \otimes N$ is defined as a quotient $\mathbf{F}(M \times N)/G(M, N)$, with $G(M, N)$ the submodule of $\mathbf{F}(M \times N)$ generated by all elements of the form

$$(u_1 a + u_2 b, v) - (u_1, v)a - (u_2, v)b \quad \text{or}$$
$$(u, v_1 a + v_2 b) - (u, v_1)a - (u, v_2)b$$

with $u, u_1, u_2 \in M$, $v, v_1, v_2 \in N$ and $a, b \in R$. The rank one tensor $u \otimes v$ is defined to be the residue class $(u, v) + G(M, N)$ for all $u \in M$ and $v \in N$. Note that the definition of $G(M, N)$ ensures that the map $M \times N \to M \otimes N$ defined as $(u, v) \mapsto u \otimes v$ is bilinear.

Since $\mathbf{F}(M \times N)$ is generated by the set $M \times N$, $M \otimes N$ is generated by the rank one tensors $u \otimes v = (u, v) + G(M, N)$ with $(u, v) \in M \times N$, so condition i) of the definition of the tensor product is satisfied. For condition ii), suppose that P is a right R-module and that $\Phi : M \times N \to P$ is a bilinear map. Since $\mathbf{F}(M \times N)$ is free over $M \times N$, Φ can be extended to a right R-module homomorphism $\psi : \mathbf{F}(M \times N) \to P$. The bilinearity of Φ implies that $G(M, N)$ is a subset of $\operatorname{Ker} \psi$, so ψ factors through the projection $\mathbf{F}(M \times N) \to M \otimes N$. This implies the existence of an R-module homomorphism $\phi : M \otimes N \to P$ such that $\phi(u \otimes v) = \psi(u, v) = \Phi(u, v)$ for all $(u, v) \in M \times N$. This homomorphism is unique, since Lemma 1.3 implies that any homomorphism $M \otimes N \to P$ is fully determined by its value on the rank one tensors of $M \otimes N$.

The tensor product $M \otimes N$ is unique up to module isomorphism since Lemma 1.3 and equations (1.1) up to (1.4) fully determine the right R-module structure of $M \otimes N$. □

1.3 Algebras over Commutative Rings

From this point forward, the letter R will always denote a commutative ring.

Definition 1.7. An *R-algebra* (or *algebra over R*) is a right R-module A with an associative, bilinear *multiplication* map $A \times A \to A$, denoted by $(x, y) \mapsto xy$, for which a unit element $1_A \in A$ exists with the property that $1_A x = x 1_A = x$ for all $x \in A$. The multiplication map is also called the *product* of A.

Note that any R-algebra A is a ring with unit element 1_A, though A is not necessarily commutative. This also means that the unit group A° is well-defined.

We will now consider some examples of R-algebras.

Example 1.8 (Ring algebras)**.**
Any ring R is an R-algebra with both multiplication and scalar multiplication the same as the ring multiplication. If S is a ring containing R, then S is also an R-algebra with these standard operations. As an R-algebra, the zero ring is called the *trivial algebra*. Any R-algebra that is not trivial is called *non-trivial*.

Example 1.9 (Matrix algebras)**.**
If A is an R-algebra, let $M_n(A)$ be the set of $n \times n$ matrices with entries in A. This set is an R-algebra with the standard addition, multiplication and scalar multiplication. This algebra is called the *$n \times n$ matrix algebra over A*. The unit element $1_{M_n(A)}$ of this algebra is the $n \times n$ identity matrix over A, and it is denoted by ι_n^A or ι_n.

For $\alpha \in M_n(A)$ and $i, j \in \{1, 2, \ldots, n\}$, $\alpha_{i,j}$ denotes the entry in α in row i and column j. Let ϵ_{ij} and ϵ_{ij}^A denote the matrix with a 1_A as the entry in row i and column j and 0_A everywhere else. The identity

$$\alpha = \sum_{i,j} \epsilon_{ij} \alpha_{i,j} \tag{1.5}$$

clearly holds for all $\alpha \in M_n(A)$. Note that $\{\epsilon_{ij} |\ 1 \leq i, j \leq n\} \subseteq M_n(A)$ is linearly independent over A. If A is an F-algebra, then this and (1.5) together imply that $\dim_F M_n(A)$ is equal to $n^2 \dim_F A$.

Example 1.10 (Quaternion algebras)**.**
Let F be a field, and suppose that A is the four dimensional vector space over F with basis $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$. We identify the space $\mathbf{1}F$ with F, and, therefore, write elements of A as $c_0 + \mathbf{i}c_1 + \mathbf{j}c_2 + \mathbf{k}c_3$ with $c_0, c_1, c_2, c_3 \in F$.

Theorem 1.11. *Suppose that $a, b \in F^\circ$. There exists a multiplication map on A with unit element 1_F that satisfies*

$$\mathbf{i}^2 = a,\ \mathbf{j}^2 = b \text{ and } \mathbf{ij} = -\mathbf{ji} = \mathbf{k}, \tag{1.6}$$

and A is an F-algebra with this multiplication.

Proof. Let S be the ring $F[\mathbf{x}]/(\mathbf{x}^2 - a)$. All elements of S can be represented as $[c + d\mathbf{x}]$ for some unique $c, d \in F$. Consider $M_2(S)$ as an F-algebra. Define $\phi : A \to M_2(S)$ as

$$\phi(c_0 + \mathbf{i}c_1 + \mathbf{j}c_2 + \mathbf{k}c_3) = \begin{pmatrix} [c_0 + c_1\mathbf{x}] & [c_2 + c_3\mathbf{x}] \\ [c_2 b - c_3 b\mathbf{x}] & [c_0 - c_1\mathbf{x}] \end{pmatrix}.$$

Note that ϕ is an injective homomorphism of vector spaces over F, that $\phi(1_F)$ is the identity element of $M_2(S)$, and that the image of ϕ is closed under matrix multiplication. Since ϕ is injective, we can lift this product to A by defining the product of $y, z \in A$ to be equal to $\phi^{-1}(\phi(y)\phi(z))$. This product imposes an F-algebra structure on A that satisfies (1.6) and such that 1_A is equal to 1_F. □

With the product in this theorem A is called a *(generalized) quaternion algebra over* F, notation $A = \left(\frac{a,b}{F}\right)$. The classical Hamilton quaternions are equal to $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ in this notation.

Note that the product in Theorem 1.11 also satisfies

$$\mathbf{k}^2 = -ab,\ \mathbf{ik} = -\mathbf{ki} = \mathbf{j}a \text{ and } \mathbf{jk} = -\mathbf{kj} = -\mathbf{i}b. \tag{1.7}$$

Any product of two elements of $\left(\frac{a,b}{F}\right)$ can be calculated by combining the multiplication rules in (1.6) and (1.7) with the fact that the product is bilinear.

Example 1.12 (Opposite algebras)**.**
For any R-algebra A there exists an *opposite algebra to* A, notation A^{op}. This opposite algebra has the same elements and R-module structure as A, but the product is defined in the opposite order. If $\circ$ is the product in A^{op}, then for all x and y in A^{op}, we define $x \circ y$ to be equal to yx, when yx is calculated with the product in A.

1.4 Properties of Algebras

Now that we have defined algebras, we discuss some of their properties. We also give many definitions related to algebras that we will use in the remainder of this thesis.

Let A and B be R-algebras and let $\phi : A \to B$ be a map. The map ϕ is an *R-algebra homomorphism* if it is both an R-module homomorphism and a ring homomorphism that preserves the unit element. As expected, ϕ is called an *R-algebra isomorphism* if it is a bijective R-algebra homomorphism. A *subalgebra* of A is an R-algebra B such that B is a subset of A for which the inclusion map is a homomorphism of algebras.

Let A be an R-algebra. The map $R \to A$ defined as $a \mapsto 1_A a$ is a homomorphism of R-algebras. If this map is injective, then we can identify R with the subalgebra $1_A R$ of A. Note that $1_A = 1_R$ and $0_A = 0_R$ under this identification. If A is an F-algebra, then the map $a \mapsto 1_A a$ is always injective, so we will always identify F with $1_A F$ in this case.

The bilinearity of the multiplication map implies that $(1_A a)x = (1_A x)a = xa$ for all $x \in A$ and $a \in R$. Since R is commutative, we can use this equation to define a left R-module structure on A as $ax = (1_A a)x = xa$ for all $x \in A$ and $a \in R$, and this left R-module structure is essentially the same as the right R-module structure on A.

A set $I \subseteq A$ is a *two-sided ideal* of A if it is a two-sided ring ideal of the ring A. *Left* and *right ideals* are defined analogously. Unless specified otherwise, the word *ideal* will refer to two-sided ideals. The *trivial ideal* is the ideal $\{0_A\}$, and any other ideal is called *non-trivial*. Note that any two-sided ideal or right ideal I of A is also an R-submodule, since for any $x \in I$ and $a \in R$, $xa = x(1_A a)$ is again an element of I. If I is an ideal of the R-algebra A, then the *quotient algebra* A/I is the quotient module A/I together with the multiplication defined by $(x + I)(y + I) = xy + I$ for $x, y \in A$.

For a subset X of an R-algebra A, the *centralizer* $\mathbf{C}_A(X)$ of X in A is defined as

$$\mathbf{C}_A(X) = \{y \in A |\ xy = yx \text{ for all } x \in X\}.$$

The centralizer is a subalgebra of A. The centralizer $\mathbf{C}_A(A)$ is also called the *center* of A, notation $\mathbf{Z}(A)$. The center of A is the set of all elements of A that commute with all other elements of A. The subalgebra $1_A R$ is a subset of the center $\mathbf{Z}(A)$, since the bilinearity of the multiplication map implies that $(1_A a)x = (1_A x)a = (x1_A)a = x(1_A a)$ for all $x \in A$ and $a \in R$.

A non-trivial R-algebra A is a *division algebra* if as a ring A is a division ring. This means that A is a division algebra if and only if A is non-trivial and the unit group A° is equal to $A \setminus \{0_A\}$. All subalgebras of a division algebras are also division algebras, but we will delay the proof of this fact until Corollary 3.2.

The direct product $\prod_{i \in I} A_i$ of a set of R-algebras A_i with $i \in I$ is the R-algebra defined as the direct product of the R-modules A_i with multiplication defined to be componentwise, and the unit element of this direct product is $(1_{A_i})_{i \in I}$. If infinitely many of the A_i are non-trivial, then the direct sum

$$\bigoplus_{i \in I} A_i = \left\{ (x_i)_{i \in I} \in \prod_{i \in I} A_i \,\middle|\, x_i = 0_{A_i} \text{ for almost all } i \in I \right\}$$

does not define an R-algebra, since it does not contain a unit element. However, if I is finite then $\bigoplus_{i \in I} A_i$ is exactly equal to $\prod_{i \in I} A_i$. In this situation we will usually use the notation $\bigoplus_{i \in I} A_i$ so that we can use the sum notation $\sum_{i \in I} x_i$ for the elements of $\bigoplus_{i \in I} A_i$ when appropriate.

Let A be an R-algebra. Then N is a *right module over the algebra* A if it is a right module over the ring A. Note that N inherits a right R-module structure from A, via $ua = u(1_A a)$ for $u \in N$ and $a \in R$. For two right A-modules M and N, $\phi : M \to N$ is a *right A-module homomorphism* when it is a module homomorphism when considering A as a ring. *Left A-modules* and *left A-module homomorphisms* are defined analogously, and left A-modules inherit a left R-module structure from A.

If A and B are R-algebras, then M is an A-B *bimodule* if it is both a left A-module and a right B-module, with the property that for all $u \in M$, $x \in A$, $y \in B$ and $a \in R$

$$\begin{aligned} (xu)y &= x(uy) \quad \text{and} \\ au &= ua. \end{aligned}$$

Any A-A bimodules will be called *A-bimodules* instead. For two A-B bimodules M and N, $\phi : M \to N$ is called an A-B *bimodule homomorphism* if it is a homomorphism of

both left A-modules and right B-modules. When appropriate, ${}_AM_B$ will be used to denote that M is an A-B bimodule.

Note that an R-algebra A is bimodule over itself. When viewing A as an A-bimodule, the subbimodules of A are exactly the ideals of the algebra A.

1.5 Endomorphism Algebras

If A be an R-algebra and M is a right A-module, then let $\mathbf{E}_A(M)$ be the right A-module consisting of right A-module endomorphisms from M to M, with addition and scalar multiplication defined pointwise. With the right R-module structure inherited from this right A-module structure, $\mathbf{E}_A(M)$ is an R-algebra with function composition as the multiplication map and the identity map id_M as the unit element. This algebra $\mathbf{E}_A(M)$ is called the *endomorphism algebra* of M.

Matrix algebras over fields are closely related to certain endomorphism algebras. If A is an n-dimensional F-algebra, then $\mathbf{E}_F(A_F)$ is isomorphic to $M_n(F)$ as F-algebras. To see this, suppose that $u_1, \ldots, u_n$ is an F-basis of A, which means that A is isomorphic to $\bigoplus_{i=1}^n u_i F$ as F-vector spaces. For each endomorphism ϕ in $\mathbf{E}_F(A_F)$ we can define a matrix $\alpha_\phi \in M_n(F)$ by choosing $(\alpha_\phi)_{i,j} \in F$ for $1 \leq i, j \leq n$ in such a way that $\phi(u_j) = \sum_{i=1}^n u_i(\alpha_\phi)_{i,j}$ for all $1 \leq j \leq n$. The map from $\mathbf{E}_F(A_F)$ to $M_n(F)$ defined by $\phi \mapsto \alpha_\phi$ is an isomorphism of F-algebras.

Let A and B be R-algebras, and let M be an A-B bimodule. We will now define a canonical injective algebra homomorphism $\lambda : A \to \mathbf{E}_B(M_B)$. The map $\lambda_x : M \to M$ defined by $u \mapsto xu$ for all $u \in M$ is a right B-module homomorphism for all $x \in A$, so $\lambda : A \to \mathbf{E}_B(M_B)$ defined as $\lambda(x) = \lambda_x$ is a well-defined map. The equation $\lambda_x(1_M) = x$ proves that λ is injective. Furthermore, λ is an R-algebra homomorphism since for all $x, y \in A$ and $a \in R$:

i) $\lambda(x + y) = \lambda_{x+y} = \lambda_x + \lambda_y = \lambda(x) + \lambda(y)$.

ii) $\lambda(xy) = \lambda_{xy} = \lambda_x \circ \lambda_y = \lambda(x) \circ \lambda(y)$.

iii) $\lambda(xa) = \lambda(x)a$.

iv) $\lambda(1_A) = \lambda_{1_A} = id_M = 1_{\mathbf{E}_B(M_B)}$.

The third equation requires a more detailed explanation. For any $x \in A$, $a \in R$ and $u \in M$, $\lambda(xa)(u)$ is by definition equal to $(xa)u$. The definition of the left scalar multiplication by R in A and M, the fact that M is a left A-module and the second bimodule condition together imply that

$$(xa)u = (ax)u = ((1_A a)x)u = (1_A a)(xu) = a(xu) = (xu)a.$$

This means that $\lambda(xa)(u)$ is equal to $(\lambda(x)(u))a$, which is equal to $(\lambda(x)a)(u)$ by definition of scalar multiplication in $\mathbf{E}_B(M_B)$. Since $\lambda(xa)(u)$ is equal to $(\lambda(x)a)(u)$ for all $u \in M$, we conclude that $\lambda(xa)$ is equal to $\lambda(x)a$ for all $x \in A$ and $a \in R$.

We have proven that for any A-B bimodule M, λ is an injective algebra homomorphism from A to $\mathbf{E}_B(M_B)$. Note that A can be viewed as an A-bimodule. In this case, $\lambda : A \to \mathbf{E}_A(A_A)$ is called the *left regular representation of* A.

Theorem 1.13. *The left regular representation $\lambda : A \to \mathbf{E}_A(A_A)$ of an F-algebra A is an isomorphism of R-algebras.*

Proof. We only still need to prove that λ is surjective. If ϕ is an element of $\mathbf{E}_A(A_A)$, then ϕ is a right A-module endomorphism, so for all $x \in A$

$$\phi(x) = \phi(1_A x) = \phi(1_A)x = \lambda(\phi(1_A))(x).$$

We conclude that ϕ is equal to $\lambda(\phi(1_A))$, so λ is surjective. □

Corollary 1.14. *Any n-dimensional F-algebra A is isomorphic to a subalgebra of $M_n(F)$.*

Proof. Theorem 1.13 yields the isomorphism $A \cong \mathbf{E}_A(A_A)$, and $\mathbf{E}_A(A_A)$ is by definition a subalgebra of $\mathbf{E}_F(A_F)$. By choosing an F-basis of A, we see that $\mathbf{E}_F(A_F)$ is isomorphic to $M_n(F)$ as F-algebras. □

1.6 Tensor Products of Algebras

If we let A and B be two R-algebras, then they are also both right R-modules. This means that the right R-module $A \otimes B$ is well-defined. To turn $A \otimes B$ into an R-algebra, we need to define a multiplication on it.

Theorem 1.15. *Let A and B be R-algebras. There exists a multiplication on $A \otimes B$ that satisfies $(x_1 \otimes y_1)(x_2 \otimes y_2) = x_1x_2 \otimes y_1y_2$ for all $x_1, x_2 \in A$ and $y_1, y_2 \in B$, and this multiplication turns $A \otimes B$ into an R-algebra with unit element $1_{A\otimes B} = 1_A \otimes 1_B$.*

Proof. For all $x \in A$ and $y \in B$, the Universal Property of the tensor product of modules yields the existence of a right R-module endomorphism $\phi_{x,y} : A \otimes B \to A \otimes B$ with $\phi_{x,y}(p \otimes q) = (xp) \otimes (yq)$ for all $p \in A$ and $q \in B$. The map $\phi : A \times B \to \mathbf{E}_R(A \otimes B)$ defined by $(x, y) \mapsto \phi_{x,y}$ is bilinear, so another application of the Universal Property proves the existence of an R-module homomorphism $\psi : A \otimes B \to \mathbf{E}_R(A \otimes B)$ such that $\psi(x \otimes y) = \phi_{x,y}$ for all $x \in A$ and $y \in B$. We can now define multiplication on $A \otimes B$ as $z \otimes w = \psi(z)(w)$, and this multiplication satisfies all of the required properties. □

Equations (1.1) up to (1.4) still hold, as does the following equivalent of Theorem 1.5.

Theorem 1.16. *Let A, B and C be R-algebras.*

i) $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$ *by an isomorphism ϕ_1 that maps $(x \otimes y) \otimes z$ to $x \otimes (y \otimes z)$.*

ii) $A \otimes B \cong B \otimes A$ *by an isomorphism ϕ_2 that maps $x \otimes y$ to $y \otimes x$.*

iii) $A \otimes R \cong A$ *by an isomorphism ϕ_3 that maps $x \otimes a$ to xa.*

iv) $R \otimes A \cong A$ *by an isomorphism ϕ_4 that maps $a \otimes x$ to xa.*

Proof. We will only prove claim i), since the proofs of the other claims are similar.

The R-algebras A, B and C are also right R-modules, so Theorem 1.5 provides us with a right R-module isomorphism $\phi : (A \otimes B) \otimes C \to A \otimes (B \otimes C)$ that satisfies $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$ for all $x \in A$, $y \in B$ and $z \in C$. It is clear that $\phi(pq)$ is equal to $\phi(p)\phi(q)$ for all p and q that are equal to $(x \otimes y) \otimes z$ for some $x \in A$, $y \in B$ and $z \in C$. Lemma 1.3 and the fact that ϕ is an R-module isomorphism then imply that $\phi(pq) = \phi(p)\phi(q)$ is true for all $p, q \in (A \otimes B) \otimes C$. The isomorphism ϕ is bijective and ϕ maps $1_{(A\otimes B)\otimes C} = (1_A \otimes 1_B) \otimes 1_C$ to $1_A \otimes (1_B \otimes 1_C) = 1_{A\otimes(B\otimes C)}$, so we conclude that ϕ is an R-algebra isomorphism. □

An important application of tensor products is in the form of scalar extensions. Scalar extensions are a method of extending the domain of scalars R of an R-algebra A to a larger commutative ring S containing R.

Theorem 1.17. *If A is an R-algebra and S is a commutative ring containing R, then $A \otimes_R S$ can be viewed as an S-algebra with the scalar product defined as*

$$zc = z(1_A \otimes c) \tag{1.8}$$

for all $z \in A \otimes S$ and $c \in S$.

Proof. The tensor product $A \otimes_R S$ exists by Theorem 1.15, since S has an R-algebra structure. The proof that the scalar product in (1.8) imposes an S-algebra structure on $A \otimes_R S$ is trivial. □

We will often use the notation A^S for $A \otimes_R S$ when we wish to view it as an S-algebra. Scalar extensions will most often be used to extend an F-algebra A to an E-algebra A^E, where E/F is a field extension.

Theorem 1.18. *Let A be an F-algebra and E/F be a field extension. If $\{x_i |\ i \in I\}$ is an F-basis of A, then $\{x_i \otimes 1_E |\ i \in I\}$ is an E-basis of A^E. If A is finite-dimensional over F, then $\dim_E A^E = \dim_F A$.*

Proof. If $\{c_j |\ j \in J\}$ is an F-basis of E, then $\{x_i \otimes c_j |\ i \in I, j \in J\}$ is an F-basis of A^E by Theorem 1.4. The definition of the scalar multiplication by E in A^E implies that $x_i \otimes c_j$ is equal to $(x_i \otimes 1_E)c_j$, so the set $\{x_i \otimes 1_E |\ i \in I\}$ spans A^E over E, and the linear independence over E of this set follows directly from the linear independence over F of $\{x_i \otimes c_j |\ i \in I, j \in J\}$. If $\dim_F A$ is finite, then the described bases imply that $\dim_E A^E = |I| = \dim_F A$. □

Similar to the tensor product of modules, the tensor product of R-algebras also has a universal property.

Theorem 1.19 (Universal Property)**.** *Let A, B and C be R-algebras. If $\phi : B \to A$ and $\psi : C \to A$ are algebra homomorphisms such that $\phi(B) \subseteq \mathbf{C}_A(\psi(C))$, then there exists a unique algebra homomorphism $\theta : B \otimes C \to A$ such that for all $x \in B$ and $y \in C$*

$$\theta(x \otimes y) = \phi(x)\psi(y).$$

Proof. If A, B, C, ϕ and ψ are defined as in the theorem, then $(x, y) \mapsto \phi(x)\psi(y)$ is a bilinear map from $B \times C$ to A. Since A, B and C are also R-modules, the Universal Property of the tensor product of R-modules implies the existence of a unique R-module homomorphism $\theta : B \otimes C \to A$ satisfying $\theta(x \otimes y) = \phi(x)\psi(y)$. A short calculation using the fact that $\phi(B)$ is a subset of $\mathbf{C}_A(\psi(C))$ shows that $\theta\big((x_1 \otimes y_1)(x_2 \otimes y_2)\big)$ is equal to $\theta(x_1 \otimes y_1)\theta(x_2 \otimes y_2)$ for all $x_1, x_2 \in B$ and $y_1, y_2 \in C$. Since $B \otimes C$ is generated as an R-module by rank one tensors and since θ is an R-module homomorphism, these equations imply that θ is an R-algebra homomorphism.

The uniqueness of θ follows from the fact that θ is fully determined by its value on rank one tensors, and that $\theta(x \otimes y)$ is equal to $\phi(x)\psi(y)$ for all $x \in B$ and $y \in C$. □

The following three subsections discuss three applications of this universal property.

1.6.1 Inner Tensor Products

If A is an R-algebra with two subalgebras B and C such that $B \subseteq \mathbf{C}_A(C)$, then the Universal Property implies that the inclusion homomorphisms $B \to A$ and $C \to A$ induce a unique algebra homomorphism $\theta : B \otimes C \to A$ such that $\theta(x \otimes y) = xy$ for all $x \in B$ and $y \in C$. When this homomorphism is an R-algebra isomorphism, we write $A = B \otimes C$ and call A the *inner tensor product* of B and C.

Suppose that the F-algebra A is an inner tensor product of two subalgebras B and C. The homomorphism $B \mapsto B \otimes C$ defined by $x \mapsto x \otimes 1_C$ for $x \in B$ isomorphically maps B to $B \otimes F$. Similarly, the homomorphism $C \mapsto B \otimes C$ defined by $y \mapsto 1_B \otimes y$ for $y \in C$ isomorphically maps C to $F \otimes C$. We will therefore often identify B with $B \otimes F$ and C with $F \otimes C$ when working with inner tensor products of an algebra over a field.

Inner tensor products can be characterized in the following way.

Theorem 1.20. *Let A be an F-algebra with two subalgebras B and C. Then $A = B \otimes C$ if and only if the following two conditions hold:*

i) $B \subseteq \mathbf{C}_A(C)$.

ii) *There exists bases $\{x_i |\ i \in I\}$ of B and $\{y_j |\ j \in J\}$ of C such that $\{x_i y_j |\ i \in I, j \in J\}$ is a basis of A.*

If A is finite-dimensional, then condition ii) can be replaced by

iii) *$B \cup C$ generates A as an F-algebra and $\dim_F A = (\dim_F B)(\dim_F C)$.*

Proof. Suppose that A is the inner tensor product of B and C. Property i) follows from the fact that $B \otimes F \subseteq \mathbf{C}_{B \otimes C}(F \otimes C)$ in $B \otimes C$, and property ii) is a consequence of Theorem 1.4. If A is finite-dimensional, then ii) clearly implies iii).

Now assume that B and C satisfy property i). Let $\theta : B \otimes C \to A$ be the algebra homomorphism induced by the inclusion homomorphisms of B and C into A and the Universal Property of the tensor product of algebras.

If B and C satisfy property $ii)$ as well, then $\{x_i \otimes y_j |\ i \in I, j \in J\}$ is a basis of $B \otimes C$ by Theorem 1.4. The homomorphism θ maps this basis of $B \otimes C$ to the basis $\{x_i y_j |\ i \in I, j \in J\}$ of A, so $\theta : B \otimes C \to A$ is an algebra isomorphism in this case.

If A is finite-dimensional and B and C satisfy property $iii)$ instead of property $ii)$, then θ is surjective, since $B \cup C$ is clearly a subset of the image of θ and θ is an F-algebra homomorphism. The fact that $\theta : B \otimes C \to A$ is a surjective algebra homomorphism with $\dim_F(B \otimes C) = (\dim_F B)(\dim_F C) = \dim_F A$ implies that θ is an isomorphism in this case as well. $\square$

1.6.2 Tensor Product of Matrix Algebras

Tensor products of matrix algebras will be important when defining the Brauer group, so we study them in more detail in the following theorem.

Theorem 1.21. *For all finite-dimensional F-algebras A and B and all $m, n \in \mathbb{N}$, $M_m(A) \otimes M_n(B) \cong M_{mn}(A \otimes B)$ as F-algebras.*

Proof. For all $x \in A$ and $\beta = \sum_{i,j} \epsilon_{ij} \beta_{i,j} \in M_m(B)$, define

$$x \otimes \beta = \begin{pmatrix} x \otimes \beta_{1,1} & x \otimes \beta_{1,2} & \cdots & x \otimes \beta_{1,m} \\ x \otimes \beta_{2,1} & x \otimes \beta_{2,2} & \cdots & x \otimes \beta_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ x \otimes \beta_{m,1} & x \otimes \beta_{m,2} & \cdots & x \otimes \beta_{m,m} \end{pmatrix}.$$

Let $\phi : M_n(A) \to M_{mn}(A \otimes B)$ be defined such that $\phi(\alpha)$ is equal to the block matrix

$$\begin{pmatrix} \alpha_{1,1} \otimes \iota_m^B & \alpha_{1,2} \otimes \iota_m^B & \cdots & \alpha_{1,n} \otimes \iota_m^B \\ \alpha_{2,1} \otimes \iota_m^B & \alpha_{2,2} \otimes \iota_m^B & \cdots & \alpha_{2,n} \otimes \iota_m^B \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n,1} \otimes \iota_m^B & \alpha_{n,2} \otimes \iota_m^B & \cdots & \alpha_{n,n} \otimes \iota_m^B \end{pmatrix},$$

for all $\alpha \in M_n(A)$. The map ϕ is clearly an F-algebra homomorphism. We can also define an F-algebra homomorphism $\psi : M_n(B) \to M_{mn}(A \otimes B)$ such that $\psi(\beta)$ is equal to the block matrix

$$\begin{pmatrix} 1_A \otimes \beta & 0_A \otimes \beta & \cdots & 0_A \otimes \beta \\ 0_A \otimes \beta & 1_A \otimes \beta & \cdots & 0_A \otimes \beta \\ \vdots & \vdots & \ddots & \vdots \\ 0_A \otimes \beta & 0_A \otimes \beta & \cdots & 1_A \otimes \beta \end{pmatrix}$$

with $1_A \otimes \beta$ on the diagonal and $0_A \otimes \beta$ everywhere else.

Since $\phi(M_n(A)) \subseteq \psi(M_m(B))$, the Universal Property implies the existence of a unique F-algebra homomorphism $\theta : M_n(A) \otimes M_m(B) \to M_{mn}(A \otimes B)$ such that $\theta(\alpha \otimes \beta) = \phi(\alpha)\psi(\beta)$ for all $\alpha \in M_n(A)$ and $\beta \in M_m(B)$. In particular, careful consideration shows that for all $1 \leq i, j \leq n$ and $1 \leq k, l \leq m$

$$\theta\left((\epsilon_{ij}^A x) \otimes (\epsilon_{kl}^B y)\right) = \phi(\epsilon_{ij}^A x)\psi(\epsilon_{kl}^B y) = \epsilon^{A \otimes B}_{m(i-1)+k, m(j-1)+l}(x \otimes y). \tag{1.9}$$

The map θ is an F-algebra homomorphism and $M_{mn}(A \otimes B)$ is generated as an F-vector space by the set $\{\epsilon_{pq}^{A\otimes B}(x \otimes y) |\ x \in A, y \in B, 0 \leq p, q \leq mn\}$, so (1.9) implies that θ is surjective. If we compare the dimensions, then

$$\begin{aligned}\dim_F(M_n(A) \otimes M_m(B)) &= (\dim_F M_n(A))(\dim_F M_m(B)) = (n^2 \dim_F A)(m^2 \dim_F B) \\ &= (mn)^2(\dim_F A)(\dim_F B) \qquad = \dim_F M_{mn}(A \otimes B)\end{aligned}$$

gives that θ is in fact an F-algebra isomorphism. □

Corollary 1.22. *For any finite field extension E/F and $n \in \mathbb{N}$, $M_n(F)^E$ is isomorphic to $M_n(E)$ as E-algebras.*

Proof. Theorem 1.16 yields that $F \otimes_F E \cong E$ as F-algebras, so Theorem 1.21 implies that $M_n(F)^E \cong M_n(E)$ as F-algebras. By comparing the definitions of the scalar product by E in $M_n(F)^E$ and $M_n(E)$, we find that this isomorphism is also an isomorphism of E-algebras. □

1.6.3 Bimodules and the Enveloping Algebra

We will now study the equivalence between A-bimodules and right $A^{op} \otimes A$-modules. The tensor product $A^{op} \otimes A$ is called the *enveloping algebra* of the R-algebra A.

Theorem 1.23. *Let A be an R-algebra. If M is an A-bimodule, then M is also a right $A^{op} \otimes A$-module with scalar multiplication satisfying*

$$u(x \otimes y) = xuy \tag{1.10}$$

for all $x, y \in A$ and $u \in M$. If N is a right $A^{op} \otimes A$-module, then N is also an A-bimodule with scalar multiplications $xv = v(x \otimes 1_A)$ and $vy = v(1_{A^{op}} \otimes y)$ for all $x, y \in A$ and $v \in N$.

Proof. If M is an A-bimodule, then we can define the right $A^{op} \otimes A$ multiplication on M by using a construction similar to the one in the proof of Theorem 1.15. If N is a right $A^{op} \otimes A$-module, then we only need to check that the described left and right A-module structures are compatible. The equation $(xv)y = x(vy)$ holds for all $x, y \in A$ and $v \in N$ since $x \otimes 1_A$ and $1_{A^{op}} \otimes y$ commute in $A^{op} \otimes A$, and $av = va$ is true for all $a \in R$ and $v \in N$ since $a \otimes 1_A$ is equal to $1_{A^{op}} \otimes a$ for all $a \in R$. □

The theorem implies that there is no real difference between A-bimodules and right $A^{op} \otimes A$-modules. Furthermore, equation (1.10) implies that $\phi : {}_AM_A \to {}_AN_A$ is a bimodule homomorphism if and only if ϕ acts as a right $A^{op} \otimes A$-module homomorphism from $M_{A^{op}\otimes A}$ to $N_{A^{op}\otimes A}$.

2 Central Simple Algebras and Brauer Groups

In this chapter we introduce and study central simple algebras, Morita equivalence and Brauer groups. Section 2.1 defines simple modules and algebras, and this section also contains a proof that all finite-dimensional simple algebras over a field F are isomorphic to a matrix algebra $M_n(D)$ for a unique $n \in \mathbb{N}$ and a finite-dimensional division algebra D over F unique up to isomorphism. In Section 2.2 we define central simple algebras over fields and consider some examples of these algebras. The three subsections of this section prove four important theorems related to central simple algebras. Section 2.3 starts by defining Morita equivalence and the Brauer group, and concludes with some basic properties of Brauer groups. In Section 2.4 we calculate our first Brauer groups. In particular, we determine $\mathbf{B}(F)$ for F a finite field, $F = \mathbb{R}$ and $F = \mathbb{C}$.

In this chapter R always denotes a commutative ring, and F always denotes a field.

2.1 Simple Modules and Algebras

Let A be an R-algebra. A right A-module M is called *simple* when it is non-trivial and the only submodules of M are $\{0_M\}$ and M itself. Schur's Lemma describes a classical result for simple A-modules.

Theorem 2.1 (Schur's Lemma)**.** *Let M and N be right A-modules and let $\phi : M \to N$ be a non-trivial homomorphism.*

i) If M is simple, then ϕ is injective.

ii) If N is simple, then ϕ is surjective.

Proof. It is clear that $\operatorname{Ker}\phi$ and $\operatorname{Im}\phi$ are submodules of M and N, respectively. Since ϕ is a non-trivial homomorphism, the kernel $\operatorname{Ker}\phi$ is not equal to M and the image $\operatorname{Im}\phi$ is not equal to $\{0_N\}$. If M is simple, then $\operatorname{Ker}\phi = \{0_M\}$, which means that ϕ is injective. If N is simple, then $\operatorname{Im}\phi = N$, which proves that ϕ is surjective. □

An R-algebra is *simple* when it is non-trivial and its only ideals are $\{0_A\}$ and A itself. Note that this means that A is a simple algebra if and only if it is simple as a ring. In particular, all division algebras are simple, since all division rings are simple. The concept of simple algebras is closely related to simple modules.

Theorem 2.2. *Let A be an R-algebra. Then A is a simple algebra if and only if it is a simple right $A^{op} \otimes A$-module.*

Proof. Note that the ideals of A are exactly the A-subbimodules of A. By Theorem 1.23 any A-bimodule is a right $A^{op} \otimes A$-module and vice versa, so the ideals of A are exactly the right submodules of A as a right $A^{op} \otimes A$-module. A comparison of the definitions of simple modules and simple algebras completes the proof. □

In particular, this theorem implies that Schur's Lemma can be applied to R-algebras.

We would of course like to find a nice characterization of the simple algebras A over a ring R. We succeed in the case where A is a finite-dimensional F-algebra. To prove this characterization theorem, we first discuss a technical lemma on minimal right ideals.

A non-trivial right ideal I of an R-algebra A is called *minimal* if all right ideals J of A with $\{0_A\} \subseteq J \subseteq I$ are equal to $\{0_A\}$ or I. Note that I is a minimal right ideal of A precisely when it is a simple right A-submodule of A_A.

Lemma 2.3. *Suppose that A is a finite-dimensional, simple F-algebra.*

i) There exists a minimal right ideal of A.

ii) All minimal right ideals of A are isomorphic as right A-modules.

iii) If M is a right A-module that is finite-dimensional over F, and I is a minimal right ideal of A, then as right A-modules

$$M \cong \bigoplus_{k=1}^{n} I_A \tag{2.1}$$

for some $n \in \mathbb{N}$. This n satisfies $\dim_F M = n \dim_F I_F$, and n is independent of the choice of I.

Proof. Note that A is itself a non-trivial right ideal of A. Since right ideals of A are also right F-submodules and A is finite-dimensional over F, a non-trivial right subideal of A of minimal dimension over F is a minimal right ideal of A.

Claim *ii*) and most of claim *iii*) are consequences of Proposition 3.3a, Proposition 3.3b and Corollary 3.3 from [Pierce, 1982]. Note that $\dim_F M = n \dim_F I_F$ follows directly from (2.1) and the definition of the direct sum of modules. □

We will now work our way up to the characterization theorem by proving two lemmas.

Lemma 2.4. *The algebra $M_n(D)$ is a simple F-algebra for all $n \in \mathbb{N}$ and division algebras D over F.*

Proof. Let D be a division algebra over F, and let n be a natural number. Suppose that J is a non-trivial ideal of $M_n(D)$. Since J is non-trivial, it contains a non-zero element β. Since β is non-zero, $\beta_{i,j}$ is non-zero for some $1 \leq i, j \leq n$. The matrix $\epsilon_{kl} = \epsilon_{ki}\beta\epsilon_{jl}\beta_{i,j}^{-1}$ is an element of J for all k and l, so $\alpha = \sum_{i,j} \epsilon_{ij}\alpha_{i,j}$ is an element of J for any $\alpha \in M_n(D)$. We conclude that $J = M_n(D)$, so $M_n(D)$ is indeed simple. □

Lemma 2.5. *Suppose that A is a finite-dimensional, simple F-algebra. If I is a minimal right ideal of A, then $A \cong M_n(D)$ for the division algebra $D = \mathbf{E}_A(I_A)$ and the $n \in \mathbb{N}$ that satisfies $\dim_F A = n \dim_F I_F$.*

Proof. Part *iii*) of Lemma 2.3 implies that A_A is isomorphic to $\bigoplus_{k=1}^n I_A$ for $n \in \mathbb{N}$ with $\dim_F A = n \dim_F I_F$, so $A \cong \mathbf{E}_A(A_A) \cong \mathbf{E}_A\left(\bigoplus_{k=1}^n I_A\right)$ holds by Theorem 1.13.

Define the right A-module homomorphism $\kappa_j : I_A \to \bigoplus_{k=1}^n I_A$ as the identity map to the j'th summand of $\bigoplus_{k=1}^n I_A$, and $\pi_i : \bigoplus_{k=1}^n I_A \to I_A$ as the projection homomorphism of the i'th summand I_A. We can define the map $\phi : \mathbf{E}_A(\bigoplus_{k=1}^n I_A) \to M_n(\mathbf{E}_A(I_A))$ as $\psi \mapsto \alpha_\psi$ with $(\alpha_\psi)_{i,j} = \pi_i \psi \kappa_j$ for all $1 \leq i, j \leq n$, and this map ϕ is a homomorphism of F-algebras. We can define an inverse homomorphism $\phi^{-1} : M_n(\mathbf{E}_A(I_A)) \to \mathbf{E}_A(\bigoplus_{k=1}^n I_A)$ as $\alpha \mapsto \psi_\alpha$, where $\psi_\alpha : \bigoplus_{k=1}^n I_A \to \bigoplus_{k=1}^n I_A$ is defined such that $\pi_i \psi_\alpha = \sum_{j=1}^n \alpha_{i,j} \pi_j$ for all $1 \leq i \leq n$. We conclude that $A \cong \mathbf{E}_A\left(\bigoplus_{k=1}^n I_A\right) \cong M_n(\mathbf{E}_A(I_A))$ as F-algebras.

Since I is a minimal right ideal of A, it is a simple right A-submodule of A_A, so Schur's Lemma implies that all non-trivial elements of $\mathbf{E}_A(I_A)$ are invertible. We conclude that A is isomorphic to $M_n(D)$ with $D = \mathbf{E}_A(I_A)$ a division algebra. □

Theorem 2.6. *A finite-dimensional F-algebra A is simple if and only if $A \cong M_n(D)$ for some natural number n and some finite-dimensional division algebra D over F. In this case, A determines n uniquely and D up to isomorphism.*

Proof. Lemmas 2.4 and 2.5 together imply the first half of the theorem, so we only need to still prove the uniqueness part of this theorem.

Let n be a natural number and let D be a division algebra over F such that $A = M_n(D)$ is finite-dimensional over F. Since A is simple, part *ii*) of Lemma 2.3 implies that all minimal right ideals of A are isomorphic as right A-modules. If we can prove that D is isomorphic to $\mathbf{E}_A(I_A)$ for some minimal right ideal I of A, then this proves that D is unique up to isomorphism, and the equation $\dim_F A = \dim_F M_n(D) = n^2 \dim_F D$ then yields that n is unique as well.

Consider $I = \epsilon_{11} M_n(D)$, consisting of exactly those $\alpha \in M_n(D)$ for which $\alpha_{i,j} = 0$ for all $i > 1$. This is a right ideal of $A = M_n(D)$. To prove that I is minimal, suppose that J is a non-trivial subideal of I. If β is one of the non-zero elements of J, then there exists some $j \in \{1, \ldots, n\}$ such that $\beta_{1,j} \neq 0$. The matrix $\epsilon_{11} = \beta \epsilon_{j1} \beta_{1,j}^{-1}$ is an element of J, so J contains $\epsilon_{11} M_n(D) = I$. We conclude that $J = I$, so I is indeed minimal.

The ideal I has the structure of a D-A bimodule, so $\lambda : D \to \mathbf{E}_A(I_A)$ defined by $x \mapsto \lambda_x$ is an injective F-algebra homomorphism. We only need to check surjectivity. The equality $\epsilon_{11}^2 = \epsilon_{11}$ gives that $\epsilon_{11} \alpha = \alpha$ for all $\alpha \in I$. For any $\phi \in \mathbf{E}_A(I_A)$

$$\phi(\alpha) = \phi(\epsilon_{11} \alpha) = \phi(\epsilon_{11}) \alpha = \lambda(\phi(\epsilon_{11}))(\alpha)$$

holds for all $\alpha \in I$, so ϕ is equal to $\lambda(\phi(\epsilon_{11}))$. This proves that λ is surjective, completing the proof. □

2.2 Central Simple Algebras

Definition 2.7. An F-algebra A is called *central simple over* F when A is simple and $\mathbf{Z}(A)$ is equal to F.

This definition is less restrictive than it might seem at first glance. For starters, the requirement for $\mathbf{Z}(A)$ to be a field is easily fulfilled.

Theorem 2.8. *If A is a simple R-algebra, then $\mathbf{Z}(A)$ is a field.*

Proof. The set $\mathbf{Z}(A)$ is by definition commutative, so we only need to show that all non-zero elements of $\mathbf{Z}(A)$ are invertible.

Suppose that $x \in \mathbf{Z}(A)$ with $x \neq 0_A$. The set $xA = \{xy |\ y \in A\}$ is clearly an ideal of A, and it contains the nonzero element $x = x1_A$, so the fact that A is simple implies that $xA = A$. In particular, there exists an $y \in A$ such that $xy = 1_A$. From the definition of the center we find that $yx = xy = 1_A$, so y is the inverse of x. This inverse y is also an element of $\mathbf{Z}(A)$, since $yz = yz1_A = yzxy = yxzy = 1_Azy = zy$ holds for all $z \in A$. □

If A is a simple R-algebra, then A can also be considered to be an algebra over the field $\mathbf{Z}(A)$ with the scalar multiplication induced by the multiplication in A. Furthermore, A is still simple as an algebra over $\mathbf{Z}(A)$. This means that all simple R-algebras A are central simple over their center $\mathbf{Z}(A)$.

Most of our time will be spent on finite-dimensional central simple algebras, so we introduce the following notation.

Definition 2.9. Denote the class of all finite-dimensional central simple algebras over F by $\mathbf{CSA}(F)$.

We will now consider a few examples of finite-dimensional central simple algebras.

Example 2.10 (Field algebra)**.**
For all fields F, it is clear that $F \in \mathbf{CSA}(F)$.

Example 2.11 (Opposite algebras)**.**
If $A \in \mathbf{CSA}(F)$, then the opposite algebra A^{op} is also an element of $\mathbf{CSA}(F)$. To see this, note that $\mathbf{Z}(A^{op}) = \mathbf{Z}(A)$ as sets, that the ideals of A^{op} are precisely the same sets as the ideals of A, and that $\dim_F A^{op}$ is equal to $\dim_F A$.

Example 2.12 (Matrix algebras)**.**
Lemma 2.4 states that $M_n(D)$ is a simple F-algebra for all $n \in \mathbb{N}$ and division algebras D over F. A quick calculation proves that $\mathbf{Z}(M_n(D))$ is equal to $\iota_n^D\mathbf{Z}(D) = 1_{M_n(D)}\mathbf{Z}(D)$ for all F-algebras D. Finally, the dimension of $M_n(D)$ over F is equal to $n^2 \dim_F D$. Together, these statements prove the following theorem.

Theorem 2.13. *The class $\mathbf{CSA}(F)$ contains $M_n(D)$ for all $n \in \mathbb{N}$ and $D \in \mathbf{CSA}(F)$.*

Corollary 2.14. *The algebra $M_n(F)$ is in $\mathbf{CSA}(F)$ for all $n \in \mathbb{N}$.*

Theorem 2.6 actually implies that all elements of $\mathbf{CSA}(F)$ are of the form $M_n(D)$ for some division algebra D.

Theorem 2.15. *If $A \in \mathbf{CSA}(F)$, then $A \cong M_n(D)$ for some unique $n \in \mathbb{N}$ and $D \in \mathbf{CSA}(F)$ unique up to isomorphism.*

Proof. Since A is simple, Theorem 2.6 implies that $A \cong M_n(D)$ for some unique $n \in \mathbb{N}$ and division algebra D over F unique up to isomorphism. The fact that D is a division algebra implies that D is simple, and the equation $F = \mathbf{Z}(A) \cong \mathbf{Z}(M_n(D) = \iota_n^D \mathbf{Z}(D)$ implies that D is central over F. The fact that $\dim_F A = n^2 \dim_F D$ is finite implies that D is finite-dimensional over F. □

Corollary 2.16. *The algebra $M_n(A)$ is in $\mathbf{CSA}(F)$ for all $n \in \mathbb{N}$ and $A \in \mathbf{CSA}(F)$.*

Proof. Theorem 2.15 implies that there exist $m \in \mathbb{N}$ and $D \in \mathbf{CSA}(F)$ such that $A \cong M_m(D)$. We conclude that $M_n(A)$ is isomorphic to $M_n(M_m(D)) \cong M_{mn}(D)$, which is an element of $\mathbf{CSA}(F)$ by Theorem 2.13. □

Example 2.17 (Quaternion algebras)**.**
Let $\operatorname{char} F$ denote the characteristic of the field F.

Theorem 2.18. *Suppose that F is a field with $\operatorname{char} F \neq 2$. For $a, b \in F^\circ$, $A = \left(\frac{a,b}{F}\right)$ is an element of $\mathbf{CSA}(F)$.*

Proof. For convenience, define the Lie bracket operation $[x, y] = xy - yx$ for $x, y \in \left(\frac{a,b}{F}\right)$. Let $x = c_0 + \mathbf{i}c_1 + \mathbf{j}c_2 + \mathbf{k}c_3$ be an element of $\mathbf{Z}\left(\left(\frac{a,b}{F}\right)\right)$. By definition of the center

$$\begin{aligned} [\mathbf{i}, x] &= \mathbf{j}(2ac_3) + \mathbf{k}(2c_2) &&= 0_A, \\ [\mathbf{j}, x] &= \mathbf{i}(-2bc_3) + \mathbf{k}(-2c_1) = 0_A \quad \text{and} \\ [\mathbf{k}, x] &= \mathbf{i}(2bc_2) + \mathbf{j}(-2ac_1) &&= 0_A. \end{aligned}$$

This implies that $c_1 = c_2 = c_3 = 0_F$, so $\mathbf{Z}\left(\left(\frac{a,b}{F}\right)\right)$ is a subset of F. The opposite inclusion is true by definition, so $\mathbf{Z}\left(\left(\frac{a,b}{F}\right)\right) = F$.

Let I be a non-trivial ideal of $\left(\frac{a,b}{F}\right)$. If $x = c_0 + \mathbf{i}c_1 + \mathbf{j}c_2 + \mathbf{k}c_3$ is a non-zero element of I, then I also contains

$$\begin{aligned} [\mathbf{j}, [\mathbf{i}, x]] &= \mathbf{i}(-4bc_2), \\ [\mathbf{k}, [\mathbf{j}, x]] &= \mathbf{j}(4abc_3) \qquad \text{and} \\ [\mathbf{i}, [\mathbf{k}, x]] &= \mathbf{k}(-4ac_1), \end{aligned}$$

which means that I also contains the elements

$$\begin{aligned} [\mathbf{j}, [\mathbf{i}, x]]\mathbf{i} &= (-4abc_2), \\ [\mathbf{k}, [\mathbf{j}, x]]\mathbf{j} &= (4ab^2c_3) \qquad \text{and} \\ [\mathbf{i}, [\mathbf{k}, x]]\mathbf{k} &= (4a^2bc_1). \end{aligned}$$

If c_1, c_2 or c_3 is non-zero, then one of these three elements is a non-zero element of F that is contained in I. If $c_1 = c_2 = c_3 = 0_F$, then x is itself a non-zero element of F such that $x \in I$. From the fact that I contains a non-zero element of F we conclude that $I = A$, so A is indeed simple.

Since A is by definition four-dimensional over F, this proves that $A \in \mathbf{CSA}(F)$. □

Corollary 2.19. *Suppose that F is a field with* $\operatorname{char} F \neq 2$. *For $a, b \in F^\circ$, $A = \left(\frac{a,b}{F}\right)$ is either a division algebra, or isomorphic to $M_2(F)$ as F-algebras.*

Proof. By Theorem 2.6 A is isomorphic to $M_n(D)$ for some natural number n and some division algebra D that is finite-dimensional over F. The dimension equation $n^2 \dim_F D = \dim_F A = 4$ implies that either $n = 1$ and $\dim_F D = 4$, in which case A is isomorphic to D, or $n = 2$ and $\dim_F D = 1$, in which case $D = F$ and A is isomorphic to $M_2(F)$. □

We can distinguish between these two cases by using the following theorem.

Theorem 2.20. *Suppose that F is a field with* $\operatorname{char} F \neq 2$. *Let a and b be non-zero elements of some field F, and define $A = \left(\frac{a,b}{F}\right)$. The following conditions are equivalent:*

i) A is a division algebra.

ii) If $(c_0, c_1, c_2) \in F^3$ satisfies $c_0^2 = ac_1^2 + bc_2^2$, then $c_0 = c_1 = c_2 = 0_F$.

Proof. We will only describe the proof of one half of this theorem. See for instance the proof of Proposition 1.6 from [Pierce, 1982] for a proof of the other implication.

If $(c_0, c_1, c_2) \in F^3$ is a non-trivial solution to $c_0^2 = ac_1^2 + bc_2^2$, then $c_0 + \mathbf{i}c_1 + \mathbf{j}c_2$ and $c_0 - \mathbf{i}c_1 - \mathbf{j}c_2$ are two non-trivial elements of A with

$$(c_0 + \mathbf{i}c_1 + \mathbf{j}c_2)(c_0 - \mathbf{i}c_1 - \mathbf{j}c_2) = c_0^2 - ac_1^2 - bc_2^2 = 0_F = 0_A.$$

This implies that A is not a division algebra. □

One consequence of this theorem and Corollary 2.19 is that $\left(\frac{1_F,1_F}{F}\right)$ is isomorphic to $M_2(F)$, since $c_0^2 = c_1^2 + c_2^2$ has $c_0 = c_1 = 1_F$, $c_2 = 0_F$ as a non-trivial solution. The quaternion algebras $\left(\frac{-1_F,1_F}{F}\right)$ and $\left(\frac{1_F,-1_F}{F}\right)$ are isomorphic to $M_2(F)$ for similar reasons.

The following three subsections contain four important theorems on central simple algebras that will be used in later sections and chapters of this thesis.

2.2.1 Tensor Products of Central Simple Algebras

We first introduce a lemma discussing some basic properties of the centers and simpleness of the tensor product of F-algebras. We then consider some properties of tensor products involving central simple algebras. Finally, we characterize the inner tensor products where one of the subalgebras is central simple.

Lemma 2.21. *Let B and C be F-algebras. Denote $B \otimes C$ by A.*

i) $\mathbf{C}_A(B \otimes F) = \mathbf{Z}(B) \otimes C$.

ii) $\mathbf{Z}(A) = \mathbf{Z}(B) \otimes \mathbf{Z}(C)$.

iii) If B is central simple and C is simple, then A is simple.

Proof. The proof of this lemma is not particularly interesting, so it is omitted. See for instance the proofs of Lemmas 12.4b and 12.4c from [Pierce, 1982] for more details. □

Theorem 2.22. *Let B and C be central simple F-algebras.*

i) $B \otimes C$ is a central simple F-algebra.

ii) If E/F is a field extension, then B^E is a central simple E-algebra.

iii) If $n = \dim_F B$ is finite, then $B^{op} \otimes B \cong M_n(F)$ as F-algebras.

Proof. Statements *i)* and *ii)* follow directly from parts *ii)* and *iii)* of Lemma 2.21. The proof of statement *iii)* is a bit more involved.

Suppose that $n = \dim_F B < \infty$. We have already seen that $B^{op} \in \mathbf{CSA}(F)$, so statement *i)* implies that $B^{op} \otimes B \in \mathbf{CSA}(F)$. Define $\lambda : B^{op} \to \mathbf{E}_F(B)^{op}$ as $x \mapsto \lambda_x$, with $\lambda_x(z) = xz$ for all $z \in B$, and define $\rho : B \to \mathbf{E}_F(B)^{op}$ as $x \mapsto \rho_x$, with $\rho_x(z) = zx$ for all $z \in B$. The maps λ and ρ are well-defined, they are both algebra homomorphisms and $\lambda(B^{op})$ is a subset of $\mathbf{C}_{\mathbf{E}_F(B)^{op}}(\rho(B))$, so the Universal Property of the tensor product of algebras implies the existence of an algebra homomorphism $\phi : B^{op} \otimes B \to \mathbf{E}_F(B)^{op}$ such that $\phi(x \otimes y) = \lambda(x)\rho(y)$ for all $x, y \in B$.

By choosing an F-basis for B, we find an isomorphism $\mathbf{E}_F(B)^{op} \cong M_n(F)^{op}$, and the transposition map implies that $M_n(F)^{op} \cong M_n(F)$. In particular, $\mathbf{E}_F(B)^{op}$ is an element of $\mathbf{CSA}(F)$. Both $B^{op} \otimes B$ and $\mathbf{E}_F(B)^{op}$ are simple F-algebras and ϕ is non-trivial, so Schur's Lemma implies that $\phi : B^{op} \otimes B \to \mathbf{E}_F(B)^{op}$ is an isomorphism. We conclude that $B^{op} \otimes B \cong M_n(F)$ as F-algebras. □

Before we can characterize the inner tensor products where one of the subalgebras is central simple, we need one more technical lemma.

Lemma 2.23. *Let B and C be subalgebras of the F-algebra A such that $C \subseteq \mathbf{C}_A(B)$ and B is central simple over F. For $x_1, \ldots, x_n \in B$ linearly independent and $y_1, \ldots, y_n \in C$, $x_1y_1 + \cdots + x_ny_n = 0_A$ implies that $y_1 = \cdots = y_n = 0_A$.*

Proof. See for instance the proof of Lemma 12.4a from [Pierce, 1982]. □

Theorem 2.24. *Let B and C be subalgebras of the finite-dimensional F-algebra A such that $C \subseteq \mathbf{C}_A(B)$ and B is central simple over F. The following conditions are equivalent:*

i) $A = BC$.

ii) $\dim_F A = (\dim_F B)(\dim_F C)$.

iii) *A is the inner tensor product of B and C, so $A = B \otimes C$.*

Proof. Suppose that $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_m\}$ are bases of B and C, respectively. The set $\{x_i y_j | 1 \leq i \leq n, 1 \leq j \leq m\} \subseteq A$ is linearly independent over F, since if $\sum_{i=1}^n \sum_{j=1}^m x_i y_j a_{ij} = 0_A$ for all $a_{ij} \in F$, then Lemma 2.23 implies that $\sum_{j=1}^m y_j a_{ij} = 0_A$ for all $1 \leq i \leq n$, which means that $a_{ij} = 0_F$ for all $1 \leq i \leq n$ and $1 \leq j \leq m$.

If condition *i)* or *ii)* holds, then $\{x_i y_j | 1 \leq i \leq n, 1 \leq j \leq m\} \subseteq A$ is an F-basis of A, so Theorem 1.20 implies that $A = B \otimes C$. On the other hand, if condition *iii)* holds, then Theorem 1.20 implies conditions *i)* and *ii)*. □

2.2.2 Double Centralizer Theorem

In this subsection we will study some properties of the centralizer $\mathbf{C}_A(B)$, where B is a subalgebra of an F-algebra A. In particular, the Double Centralizer Theorem will describe some useful properties of $\mathbf{C}_A(B)$ when B is a simple subalgebra of $A \in \mathbf{CSA}(F)$.

Lemma 2.25. *Let B be a subalgebra of some F-algebra A. The inclusion homomorphism $B^{op} \otimes A \to A^{op} \otimes A$ induces a right $B^{op} \otimes A$-module structure on A. The left regular representation $\lambda : A \to \mathbf{E}_A(A_A)$ induces an isomorphism $\mathbf{C}_A(B) \cong \mathbf{E}_{B^{op} \otimes A}(A_{B^{op} \otimes A})$.*

Proof. We know that A is a right $A^{op} \otimes A$-module from Theorem 1.23, since A is clearly an A-bimodule. Theorem 1.13 states that the left regular representation $\lambda : A \to \mathbf{E}_A(A_A)$, $x \mapsto \lambda_x$ is an isomorphism of F-algebras. Note that $\mathbf{C}_A(B)$ and $\mathbf{E}_{B^{op} \otimes A}(A_{B^{op} \otimes A})$ are subalgebras of A and $\mathbf{E}_A(A_A)$, respectively.

If x is an element of A, then the endomorphism $\lambda_x \in \mathbf{E}_A(A_A)$ is an element of $\mathbf{E}_{B^{op} \otimes A}(A_{B^{op} \otimes A})$ precisely when $\lambda_x(yz) = y\lambda_x(z)$ for all $y \in B$ and $z \in A$. Simple calculation shows that this holds if and only if $xy = yx$ for all $y \in B$, so precisely when x is an element of $\mathbf{C}_A(B)$. This completes the proof of this lemma. □

Theorem 2.26 (Double Centralizer Theorem)**.** *Let $A \in \mathbf{CSA}(F)$ and suppose that B is a simple subalgebra of A.*

i) $\mathbf{C}_A(B)$ *is simple.*

ii) $(\dim_F B)(\dim_F \mathbf{C}_A(B)) = \dim_F A$.

iii) $\mathbf{C}_A(\mathbf{C}_A(B)) = B$.

iv) *If B is central simple, then $\mathbf{C}_A(B)$ is central simple and $A = B \otimes \mathbf{C}_A(B)$.*

Proof. Part *iii*) of Lemma 2.21 implies that $B^{op} \otimes A \cong A \otimes B^{op}$ is a simple F-algebra, and $B^{op} \otimes A$ is clearly finite-dimensional over F. Let I be a minimal right ideal of $B^{op} \otimes A$, and define D as the division algebra $D = \mathbf{E}_{B^{op} \otimes A}(I_{B^{op} \otimes A})$. If n is the natural number that satisfies the equation $\dim_F(B^{op} \otimes A) = n \dim_F I_F$, then part *iii*) of Lemma 2.3 and Lemma 2.5 describe isomorphisms $B^{op} \otimes A \cong \bigoplus_{i=1}^{n} I_{B^{op} \otimes A}$ as right $B^{op} \otimes A$-modules and $B^{op} \otimes A \cong M_n(D)$ as F-algebras, respectively.

Since A is a right $B^{op} \otimes A$-module with $\dim_F A$ finite, part *iii*) of Lemma 2.3 implies that $A_{B^{op} \otimes A} \cong \bigoplus_{i=1}^{k} I_{B^{op} \otimes A}$ for some $k \in \mathbb{N}$. Lemma 2.25 yields that

$$\mathbf{C}_A(B) \cong \mathbf{E}_{B^{op} \otimes A}(A_{B^{op} \otimes A}) \cong \mathbf{E}_{B^{op} \otimes A}\left(\bigoplus_{i=1}^{k} I_{B^{op} \otimes A} \right) \cong M_k\big(\mathbf{E}_{B^{op} \otimes A}(I_{B^{op} \otimes A})\big) \cong M_k(D),$$

so Theorem 2.6 yields that $\mathbf{C}_A(B)$ is simple.

If we compare the dimensions over F of our various F-algebras and $B^{op} \otimes A$-modules, then we find the equations

$$\begin{aligned} (\dim_F A)(\dim_F B) = \dim_F(B^{op} \otimes A) = n \dim_F I_F = n^2 \dim_F D, \\ \dim_F A = k \dim_F I_F \qquad \text{and} \\ \dim_F \mathbf{C}_A(B) = k^2 \dim_F D. \end{aligned}$$

These equations together imply that $(\dim_F B)(\dim_F \mathbf{C}_A(B)) = \dim_F A$ for all simple subalgebras B of A. We have just proven that $\mathbf{C}_A(B)$ is simple, so

$$(\dim_F \mathbf{C}_A(B))(\dim_F \mathbf{C}_A(\mathbf{C}_A(B))) = \dim_F A = (\dim_F B)(\dim_F \mathbf{C}_A(B)).$$

We conclude that $\dim_F \mathbf{C}_A(\mathbf{C}_A(B)) = \dim_F B$. The inclusion $B \subseteq \mathbf{C}_A(\mathbf{C}_A(B))$ holds by definition of the centralizer, so $\mathbf{C}_A(\mathbf{C}_A(B)) = B$.

If B is central simple, then Theorem 2.24 and the fact that $\dim_F A$ is equal to $(\dim_F B)(\dim_F \mathbf{C}_A(B))$ together imply that $A = B \otimes \mathbf{C}_A(B)$. By comparing centers, we find that

$$F = \mathbf{Z}(A) = \mathbf{Z}(B \otimes \mathbf{C}_A(B)) = \mathbf{Z}(B) \otimes \mathbf{Z}(\mathbf{C}_A(B)) = F \otimes \mathbf{Z}(\mathbf{C}_A(B)),$$

so $\mathbf{Z}(\mathbf{C}_A(B)) = F$ and $\mathbf{C}_A(B)$ is central simple. □

2.2.3 Noether-Skolem Theorem

The Noether-Skolem Theorem describes the algebra homomorphisms from B to A when A is a simple subalgebra of an algebra $A \in \mathbf{CSA}(F)$. We first prove a related lemma.

Lemma 2.27. *Suppose that B is a finite-dimensional, simple F-algebra and that M is a finite-dimensional right F-module. If ϕ and ψ are two F-algebra homomorphisms from B to $\mathbf{E}_F(M)$, then there exists $\theta \in \mathbf{E}_F(M)^\circ$ such that $\phi(x) = \theta^{-1}\psi(x)\theta$ for all $x \in B$.*

Proof. The homomorphisms ϕ and ψ both induce right B^{op}-module structures on M. Let M_ϕ be the B^{op}-module with scalar multiplication $ux = \phi(x)(u)$ for $u \in M$ and $x \in B^{op}$, and define M_ψ as the B^{op}-module with $ux = \psi(x)(u)$ for $u \in M$ and $x \in B^{op}$. Note that $\dim_F M_\phi = \dim_F M = \dim_F M_\psi$ follows from the fact that ϕ and ψ are F-algebra homomorphisms.

Suppose that I is a minimal right ideal of B^{op}. Since B^{op} is finite-dimensional and simple, Lemma 2.3 implies that there exist $m, n \in \mathbb{N}$ such that $M_\phi \cong \bigoplus_{i=1}^m I_{B^{op}}$ and $M_\psi \cong \bigoplus_{i=1}^n I_{B^{op}}$. The equation $\dim_F M_\phi = \dim_F M = \dim_F M_\psi$ now yields that $m = n$ and $M_\phi \cong M_\psi$. If we let $\theta : M_\phi \to M_\psi$ be a right B^{op}-module isomorphism, then $\theta \in \mathbf{E}_F(M)^\circ$ and

$$\theta(\phi(x)(u)) = \theta(ux) = \theta(u)x = \psi(x)(\theta(u))$$

for all $u \in M$ and $x \in B^{op}$. We conclude that $\phi(x) = \theta^{-1}\psi(x)\theta$ for all $x \in B$. □

Theorem 2.28 (Noether-Skolem Theorem)**.** *Let $A \in \mathbf{CSA}(F)$ and let B be a simple subalgebra of A. For any algebra homomorphism $\chi : B \to A$, there exists $u \in A^\circ$ such that $\chi(y) = u^{-1}yu$ for all $y \in B$.*

Proof. We will prove this theorem in a fairly indirect manner.

Part *iii*) of Theorem 2.22 yields that $A^{op} \otimes A$ is isomorphic to $M_n(F)$ with $n = \dim_F A$, and the isomorphism $\mathbf{E}_F(A) \cong M_n(F)$ follows from choosing an F-basis of A. We can combine these isomorphisms into an F-algebra isomorphism $\rho : A^{op} \otimes A \to \mathbf{E}_F(A)$. The Universal Property of the tensor product of algebras implies the existence of algebra homomorphisms $\phi_1 : A^{op} \otimes B \to A^{op} \otimes A$ and $\phi_2 : A^{op} \otimes B \to A^{op} \otimes A$ such that $\phi_1(x \otimes y) = x \otimes \chi(y)$ and $\phi_2(x \otimes y) = x \otimes y$ for all $x \in A^{op}$ and $y \in B$. Define the algebra homomorphisms $\psi_1 : A^{op} \otimes B \to \mathbf{E}_F(A)$ and $\psi_2 : A^{op} \otimes B \to \mathbf{E}_F(A)$ as $\psi_1 = \rho \circ \phi_1$ and $\psi_2 = \rho \circ \phi_2$.

Since A^{op} is central simple and B is simple, part *iii*) of Lemma 2.21 implies that $A^{op} \otimes B$ is simple as well. We can therefore apply Lemma 2.27 to find $\theta \in \mathbf{E}_F(A)^\circ$ such that $\psi_1(x \otimes y) = \theta^{-1}\psi_2(x \otimes y)\theta$ for all $x \in A^{op}$ and $y \in B$. Define $z = \rho^{-1}(\theta) \in (A^{op} \otimes A)^\circ$ and note that for all $x \in A^{op}$ and $y \in B$,

$$\begin{aligned} \rho(z(x \otimes \chi(y))) &= \rho(z)\rho(x \otimes \chi(y)) = \theta\psi_1(x \otimes y) \\ &= \psi_2(x \otimes y)\theta \qquad = \rho(x \otimes y)\rho(z) = \rho((x \otimes y)z). \end{aligned}$$

Since ρ is injective, this implies that $z(x \otimes \chi(y)) = (x \otimes y)z$ for all $x \in A^{op}$ and $y \in B$. In particular, for $y = 1_B$, we find that $z(x \otimes 1_B) = (x \otimes 1_B)z$ for all $x \in A^{op}$, which means that z is an element of $\mathbf{C}_{A^{op} \otimes A}(A^{op} \otimes F)$, and $\mathbf{C}_{A^{op} \otimes A}(A^{op} \otimes F)$ is equal to $F \otimes A$ by part *i*) of Lemma 2.21. An analogous proof shows that $z^{-1} \in F \otimes A$, so there exist $u, v \in A$ such that $z = 1_{A^{op}} \otimes u$ and $z^{-1} = 1_{A^{op}} \otimes v$. Clearly $u \in A^\circ$ with $v = u^{-1}$, so

$$x \otimes \chi(y) = z^{-1}(x \otimes y)z = x \otimes (u^{-1}yu)$$

holds for all $x \in A^{op}$. We conclude that $\chi(y) = u^{-1}yu$ for all $y \in B$. □

2.3 The Brauer Group

In order to define Brauer groups, we first define Morita equivalence on $\mathbf{CSA}(F)$.

Lemma 2.29. *For all $A \in \mathbf{CSA}(F)$ and $n \in \mathbb{N}$, $M_n(A)$ is isomorphic to $A \otimes M_n(F)$ as F-algebras.*

Proof. The isomorphisms $A \otimes M_n(F) \cong M_1(A) \otimes M_n(F) \cong M_n(A \otimes F) \cong M_n(A)$ follow from Theorems 1.16 and 1.21. □

Theorem 2.30. *Let A and B be elements of $\mathbf{CSA}(F)$. The following statements are equivalent:*

i) There exist $m, n \in \mathbb{N}$ such that $A \otimes M_m(F) \cong B \otimes M_n(F)$ as F-algebras.

ii) There exist $m, n \in \mathbb{N}$ such that $M_m(A) \cong M_n(B)$ as F-algebras.

iii) There exist a division algebra $D \in \mathbf{CSA}(F)$ and $m, n \in \mathbb{N}$ such that $A \cong M_m(D)$ and $B \cong M_n(D)$ as F-algebras.

If these statements hold, then A and B are called Morita equivalent*, notation $A \sim B$, and the division algebra $D \in \mathbf{CSA}(F)$ and $m, n \in \mathbb{N}$ from statement iii) are unique up to isomorphism and unique, respectively.*

Proof. The equivalence of *i)* and *ii)* follows from Lemma 2.29.

Suppose that m and n are natural numbers such that $M_m(A) \cong M_n(B)$ as F-algebras. Theorem 2.15 implies that there exist unique $k, l \in \mathbb{N}$ and $D_1, D_2 \in \mathbf{CSA}(F)$ unique up to isomorphism such that $A \cong M_k(D_1)$ and $B \cong M_l(D_2)$. We conclude that

$$M_{km}(D_1) \cong M_m(M_k(D_1)) \cong M_m(A) \cong M_n(B) \cong M_n(M_l(D_2)) \cong M_{ln}(D_2).$$

The uniqueness statement in Theorem 2.15 now implies that $D_1 \cong D_2$. This means that $A \cong M_k(D_1)$ and $B \cong M_l(D_1)$ with $k, l \in \mathbb{N}$ unique and D_1 unique up to isomorphism.

Finally, it is clear that $M_n(M_m(D)) \cong M_{mn}(D) \cong M_m(M_n(D))$ as F-algebras, and this yields that *iii)* implies *ii)*. □

Theorem 2.31. *Morita equivalence is an equivalence relation on $\mathbf{CSA}(F)$.*

Proof. Morita equivalence is clearly reflexive and symmetric, and transitivity follows from the third equivalent definition of Morita equivalence and the fact that for each $A \in \mathbf{CSA}(F)$ the division algebra $D \in \mathbf{CSA}(F)$ with $A \cong M_n(D)$ for some $n \in \mathbb{N}$ is unique up to isomorphism by Theorem 2.15. □

We will call two algebras $A, B \in \mathbf{CSA}(F)$ *equivalent* when they are Morita equivalent. The equivalence class of $A \in \mathbf{CSA}(F)$ with respect to the Morita equivalence relation will be denoted by $[A]$. Note that for all $A, B \in \mathbf{CSA}(F)$, $A \cong B$ implies that $A \sim B$.

The interplay between Morita equivalence and the tensor product is at the foundation of the idea behind Brauer groups. The following lemma describes their compatibility.

Lemma 2.32. *If A, B, A' and B' are elements of $\mathbf{CSA}(F)$ such that $A \sim A'$ and $B \sim B'$, then $A \otimes B$ is Morita equivalent to $A' \otimes B'$.*

Proof. The equivalences $A \sim A'$ and $B \sim B'$ imply that there exist $m, n, k, l \in \mathbb{N}$ such that $M_m(A) \cong M_n(A')$ and $M_k(B) \cong M_l(B')$. Theorem 1.21 yields that

$$M_{mk}(A \otimes B) \cong M_m(A) \otimes M_k(B) \cong M_n(A') \otimes M_l(B') \cong M_{nl}(A' \otimes B'),$$

so $A \otimes B$ and $A' \otimes B'$ are Morita equivalent. □

We are now ready to define the Brauer group.

Definition 2.33. The *Brauer group* $\mathbf{B}(F)$ of a field F is defined to be the set[1] of Morita equivalence classes $\{[A] |\ A \in \mathbf{CSA}(F)\}$ with the group product $[A][B] = [A \otimes B]$.

Theorem 2.34. *For any field F, $\mathbf{B}(F)$ is an abelian group with unit element $[F]$ and inverse operation $[A]^{-1} = [A^{op}]$.*

Proof. We first prove that the group product $[A][B] = [A \otimes B]$ is well-defined. Let F be a field and let A and B be elements of $\mathbf{CSA}(F)$. Part *i)* of Theorem 2.22 implies that $A \otimes B$ is central simple over F and it is clearly finite-dimensional over F, so $A \otimes B$ is an element of $\mathbf{CSA}(F)$. Lemma 2.32 implies that the equivalence class $[A \otimes B]$ is independent of the choice of representatives of $[A]$ and $[B]$ in $\mathbf{CSA}(F)$, so the product is well-defined.

The commutativity and associativity of the product on $\mathbf{B}(F)$ follows from the first two isomorphisms in Theorem 1.16. Furthermore, part *iii)* of Theorem 1.16 implies that $[A] = [A \otimes F] = [A][F]$ for all $A \in \mathbf{CSA}(F)$, so $[F]$ is the unit element. We know that $A^{op} \in \mathbf{CSA}(F)$ if and only if $A \in \mathbf{CSA}(F)$, and $[A^{op}][A] = [M_n(F)] = [F]$ for all $[A] \in \mathbf{CSA}(F)$ by Theorem 2.22, so $[A^{op}]$ is the inverse of $[A] \in \mathbf{CSA}(F)$. □

The following theorem describes two useful properties of the Brauer group.

Theorem 2.35. *Let $A, B \in \mathbf{CSA}(F)$.*

i) $A \cong B$ if and only if $[A] = [B]$ and $\dim_F A = \dim_F B$.

ii) Every class $[A] \in \mathbf{B}(F)$ can be represented by a division algebra $D \in \mathbf{CSA}(F)$, and this division algebra is unique up to isomorphism.

Proof. It is clear that $A \cong B$ implies that $[A] = [B]$ and $\dim_F A = \dim_F B$. Conversely, suppose that $[A] = [B]$ and $\dim_F A = \dim_F B$. The equation $[A] = [B]$ is by definition equivalent to the existence of $D \in \mathbf{CSA}(F)$ and $m, n \in \mathbb{N}$ such that $A \cong M_n(D)$ and $B \cong M_m(D)$. The equality $\dim_F A = \dim_F B$ implies that $m = n$, so $A \cong B$.

Part *ii)* is a consequence of the third equivalent definition of Morita equivalence. □

Finally, we will describe a canonical group homomorphism $\mathbf{B}(F) \to \mathbf{B}(E)$ when E/F is a field extension, but we first need two lemmas for the proof of its existence.

[1] See Proposition 12.5a from [Pierce, 1982] for a proof that this is a set.

Lemma 2.36. *If A is an F-algebra and B and C are E-algebras for some field extension E/F, then $(A \otimes_F B) \otimes_E C \cong A \otimes_F (B \otimes_E C)$ as F-algebras by an isomorphism that maps $(x \otimes_F y) \otimes_E z$ to $x \otimes_F (y \otimes_E z)$.*

Proof. We will omit this proof, because it is almost identical to the proof of part i) of Theorem 1.16. □

Lemma 2.37. *If E/F is a field extension and A and B are F-algebras, then $(A \otimes_F B)^E$ is isomorphic to $A^E \otimes_E B^E$ as E-algebras.*

Proof. Theorem 1.16 and Lemma 2.36 together imply that

$$\begin{aligned}(A \otimes_F B) \otimes_F E &\cong A \otimes_F (E \otimes_F B) \\ &\cong A \otimes_F ((E \otimes_E E) \otimes_F B) \\ &\cong (A \otimes_F E) \otimes_E (B \otimes_F E)\end{aligned} \tag{2.2}$$

as F-algebras by isomorphisms that together map elements of the form $(x \otimes_F y) \otimes_F c$ in $(A \otimes_F B) \otimes_F E$ to $(x \otimes_F 1_E) \otimes_E (y \otimes_F c)$ in $(A \otimes_F E) \otimes_E (B \otimes_F E)$. By definition of the scalar product with elements of E in these E-algebras, we see that this F-algebra isomorphism $(A \otimes_F B) \otimes_F E \to (A \otimes_F E) \otimes_E (B \otimes_F E)$ is also an E-algebra isomorphism. □

Theorem 2.38. *Suppose that E/F is a field extension. If $\kappa : F \to E$ is the inclusion homomorphism, then κ induces a group homomorphism $\kappa_* : \mathbf{B}(F) \to \mathbf{B}(E)$ defined as $\kappa_*([A]) = [A^E]$. Furthermore, if E/K and K/F are field extensions with inclusion homomorphisms $\kappa_1 : K \to E$ and $\kappa_2 : F \to K$, then $(\kappa_1 \circ \kappa_2)_* = \kappa_{1*} \circ \kappa_{2*}$.*

Proof. Theorem 1.18 and Theorem 2.22 together imply that $A^E = A \otimes_F E$ is an element of $\mathbf{CSA}(E)$ for all $A \in \mathbf{CSA}(F)$, so $[A^E] \in \mathbf{B}(E)$ for all $A \in \mathbf{CSA}(F)$. Lemma 2.37 yields that the equality $[(A \otimes_F B)^E] = [A^E][B^E]$ holds in $\mathbf{B}(E)$ for all $A, B \in \mathbf{CSA}(F)$, so κ_* is a homomorphism if it is well-defined. In order to conclude that κ_* is a well-defined map, we still need to prove that $[A^E] = [(A')^E]$ in $\mathbf{B}(E)$ if $[A] = [A']$ in $\mathbf{B}(F)$.

If $A, A' \in \mathbf{CSA}(F)$ are Morita equivalent, then there exist $m, n \in \mathbb{N}$ such that $A \otimes_F M_m(F) \cong A' \otimes_F M_n(F)$. Corollary 1.22 and Lemma 2.37 together imply that

$$\begin{aligned}A^E \otimes_E M_m(E) &\cong A^E \otimes_E M_m(F)^E \cong (A \otimes_F M_m(F))^E \\ &\cong (A' \otimes_F M_n(F))^E \cong A'^E \otimes_E M_n(F)^E \cong (A')^E \otimes_E M_n(E),\end{aligned}$$

We conclude that A^E and $(A')^E$ are Morita equivalent as central simple E-algebras, so κ_* is a well-defined homomorphism.

Now suppose that $\kappa_1 : K \to E$ and $\kappa_2 : F \to K$ are inclusion homomorphisms of fields. It is clear that $\kappa_1 \circ \kappa_2$ is an inclusion homomorphism of F into E, so $(\kappa_1 \circ \kappa_2)_*$ is well-defined. The homomorphisms $(\kappa_1 \circ \kappa_2)_*$ and $\kappa_{1*} \circ \kappa_{2*}$ are equal precisely when $[(A^K)^E] = [A^E]$ holds for all $A \in \mathbf{CSA}(F)$. Fortunately, for any $A \in \mathbf{CSA}(F)$

$$(A^K)^E = (A \otimes_F K) \otimes_K E \cong A \otimes_F (K \otimes_K E) \cong A \otimes_F E = A^E$$

follows directly from Theorem 1.16 and Lemma 2.36. □

2.4 Examples of Brauer Groups

In this section, we calculate the Brauer group $\mathbf{B}(F)$ for F a finite field, $F = \mathbb{R}$, and $F = \mathbb{C}$. Our method is based on the fact that Theorem 2.35 yields that each element of the Brauer group $\mathbf{B}(F)$ is represented by a division algebra $D \in \mathbf{CSA}(F)$, and that this division algebra is unique up to isomorphism. Since all division algebras are simple, the division algebra D over F is an element of $\mathbf{CSA}(F)$ if and only if it is finite-dimensional and central over F.

Let F be a finite field and suppose that D is a division algebra in $\mathbf{CSA}(F)$. Since F is finite and D is finite-dimensional over F, D is also finite. All finite division rings are fields, so multiplication in D is commutative. In particular, D is equal to its own center $\mathbf{Z}(D) = F$. We conclude that the only division algebra in $\mathbf{CSA}(F)$ is F itself.

Theorem 2.39. *For any finite field F, the Brauer group $\mathbf{B}(F) = \{[F]\}$ is trivial.*

If we wish to determine $\mathbf{B}(\mathbb{R})$ in a similar way, then we need to know what division algebras are elements of $\mathbf{CSA}(\mathbb{R})$. Fortunately, there is a famous theorem by Frobenius that describes the finite-dimensional division algebras over the real numbers.

Theorem 2.40 (Frobenius Theorem)**.** *If D is a finite-dimensional division $\mathbb{R}$-algebra, then D is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.*

Proof. See for instance the proof of Theorem 18.12 from [Roman, 2008] for an elementary proof of this theorem using only techniques from linear algebra. □

Remember that $\mathbb{H}$ is the quaternion algebra $\left(\frac{-1,-1}{\mathbb{R}}\right)$. If we calculate the center of each of these division algebras, then we find that $\mathbf{Z}(\mathbb{R}) = \mathbb{R}$, $\mathbf{Z}(\mathbb{C}) = \mathbb{C}$ and $\mathbf{Z}(\mathbb{H}) = \mathbb{R}$.

Corollary 2.41. *The Brauer group of $\mathbb{R}$ satisfies $\mathbf{B}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\} \cong \mathbb{Z}/2\mathbb{Z}$.*

Proof. The only finite-dimensional, central division algebras over $\mathbb{R}$ are $\mathbb{H}$ and $\mathbb{R}$ itself. These algebras are not isomorphic, so the group $\mathbf{B}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$ has two elements. □

Since $\mathbb{R}$ is a subfield of $\mathbb{C}$ of finite degree $[\mathbb{C} : \mathbb{R}] = 2$, any finite-dimensional division algebra over $\mathbb{C}$ is also a finite-dimensional $\mathbb{R}$-algebra. The Frobenius Theorem therefore implies that the only finite-dimensional, central division algebra over $\mathbb{C}$ is $\mathbb{C}$ itself.

Corollary 2.42. *The Brauer group $\mathbf{B}(\mathbb{C}) = \{[\mathbb{C}]\}$ is the trivial group.*

The next obvious step would be to determine the Brauer group $\mathbf{B}(\mathbb{Q})$. However, this Brauer group is much more complicated than the examples we have seen so far. We will spend most of the remainder of this thesis developing machinery so that we can determine the structure of the Brauer groups of $\mathbb{Q}$ and other algebraic number fields, which are fields F with $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ and $[F : \mathbb{Q}] < \infty$.

3 Subfields and Galois Cohomology

Chapter 3 develops machinery for studying the structure of $\mathbf{B}(F)$ for general fields F. Section 3.1 defines subfields of algebras $A \in \mathbf{CSA}(F)$, and looks at some consequences of their existence. Section 3.2 defines splitting fields of algebras and uses them to find a way to write the Brauer group $\mathbf{B}(F)$ as a union of subgroups $\mathbf{B}(E/F)$ with E/F ranging over the finite Galois extensions of F. In Section 3.3 we define crossed products, which are algebras with a subfield with special properties, and find that each class $[A] \in \mathbf{B}(E/F)$ contains a crossed product that is unique up to isomorphism. Section 3.4 develops a cohomology theory named Galois cohomology, and we also use crossed products to prove that $\mathbf{B}(E/F)$ is isomorphic to a certain second order Galois cohomology group. Section 3.5 defines two new numerical invariants of algebras and uses one of them and the isomorphism between $\mathbf{B}(E/F)$ and the second order Galois cohomology group to prove that all Brauer groups are torsion groups. Finally, Section 3.6 focuses on cyclic algebras, which are a special kind of crossed product.

In this chapter F always denotes a field.

3.1 Maximal Subfields

A *subfield* of an F-algebra A is a subalgebra E of A that is also a field. Note that F is a subfield of any F-algebra A. If E is a subfield of an F-algebra A, then E is a field extension of F, since all subalgebras of A contain F. If A is also finite-dimensional, then $[E : F] \leq \dim_F A$ yields that the extension is finite.

We first consider some subfields of division algebras.

Lemma 3.1. *Let D be a finite-dimensional division algebra over F. If $x \in D$, then $F[x] = \{\Phi(x) |\ \Phi \in F[\mathbf{x}]\}$ is a subfield of D containing x.*

Proof. This follows immediately from the fact that $F \subseteq \mathbf{Z}(D)$. □

Corollary 3.2. *If B is a subalgebra of a finite-dimensional division algebra D over F, then B is also a division algebra.*

We already promised this result when defining division algebras. It follows from the lemma, since for any non-zero element $x \in B$, x^{-1} is an element of $F[x] \subseteq B$.

A subfield $E \subseteq A$ is called a *maximal* subfield if all subfields K of A with $E \subseteq K$ are equal to E.

All finite-dimensional F-algebras A contain maximal subfields. To see this, assume that A is a finite-dimensional F-algebra with no maximal subfields. If K is a subfield of A, then the fact that K is not maximal implies the existence of a subfield E of A

that contains K with $[E:F] > [K:F]$. Starting from the subfield F of A, we find an infinite sequence of subfields of A with ever increasing field degrees, which contradicts the fact that these field degrees are bounded from above by $\dim_F A < \infty$.

The centralizer of a subfield of an F-algebra has some interesting properties.

Theorem 3.3. *Let $A \in \mathbf{CSA}(F)$. If E is a subfield of A, then $\mathbf{C}_A(E)$ is an element of $\mathbf{CSA}(E)$, and $\mathbf{C}_A(E)$ and A^E are Morita equivalent as elements of $\mathbf{CSA}(E)$.*

Proof. Note that $\mathbf{C}_A(E)$ can be viewed as an E-algebra, since E is a subset of $\mathbf{Z}(\mathbf{C}_A(E))$.

Lemma 2.25 implies that $\mathbf{C}_A(E) \cong \mathbf{E}_{E^{op}\otimes A}(A_{E^{op}\otimes A}) \cong \mathbf{E}_{A^E}(A_{A^E})$ as F-algebras, but the described map is also an isomorphism of E-algebras. If I is a minimal right ideal of A^E, then Lemma 2.3 implies that $A_{A^E} \cong \bigoplus_{i=1}^k I_{A^E}$ as right A^E-modules for some $k \in \mathbb{N}$. Analogous to the proof of Lemma 2.5 we find that $\mathbf{C}_A(E) \cong \mathbf{E}_{A^E}(\bigoplus_{i=1}^k I_{A^E}) \cong M_k(D)$, where D is the division algebra $\mathbf{E}_{A^E}(I_{A^E})$. Lemma 2.5 also implies that $A^E \cong M_n(D)$ for some $n \in \mathbb{N}$. The equation $E = \mathbf{Z}(A^E) \cong \mathbf{Z}(M_n(D)) = \iota_n^D \mathbf{Z}(D)$ implies that D is central over E, so $D \in \mathbf{CSA}(E)$. Theorem 2.13 and the third definition of Morita equivalence now imply that $\mathbf{C}_A(E) \in \mathbf{CSA}(E)$ and $\mathbf{C}_A(E) \sim A^E$. □

Theorem 3.4. *Let $A \in \mathbf{CSA}(F)$, and suppose that E is a maximal subfield of A with $k = [E:F]$. There exists $n \in \mathbb{N}$ such that $\mathbf{C}_A(E) \cong M_n(E)$ and $\dim_F A = (kn)^2$.*

Proof. Theorem 3.3 states that $\mathbf{C}_A(E) \in \mathbf{CSA}(E)$, so by Theorem 2.15 there exist $n \in \mathbb{N}$ and a division algebra $D \in \mathbf{CSA}(E)$ such that $\mathbf{C}_A(E) \cong M_n(D)$. Since E is maximal in A and $E \subseteq \mathbf{C}_A(E)$, E is also maximal in $\mathbf{C}_A(E) \cong M_n(D)$. This implies that E is also maximal as a subfield of D, since else a larger subfield $K \subseteq D$ containing E would induce a larger subfield $\iota_n K \subseteq M_n(D)$ containing $\iota_n E = E$. Using the same construction as in Lemma 3.1 we find that $D = E$, because else $E[x]$ with $x \in D \setminus E$ would be a strictly larger subfield of D. The Double Centralizer Theorem yields that

$$\dim_F A = (\dim_F \mathbf{C}_A(E))\,(\dim_F E) = (\dim_F M_n(E))\,(\dim_F E) = n^2[E:F]^2 = (kn)^2.$$

□

Corollary 3.5. *Let $A \in \mathbf{CSA}(F)$. For some $m \in \mathbb{N}$, $\dim_F A = m^2$. For any subfield $E \subseteq A$, $[E:F]$ divides m.*

This corollary follows from the fact that any subfield of A can be extended to a maximal subfield. The number m will be called the *degree* of A, notation $\operatorname{Deg} A$. Note that the inequality $[E:F] \leq \operatorname{Deg} A$ in the corollary is a notable improvement over the bound $[E:F] \leq \dim_F A = (\operatorname{Deg} A)^2$ that we found earlier.

The bound $[E:F] \leq \operatorname{Deg} A$ implies that any subfield E of A with $[E:F] = \operatorname{Deg} A$ is maximal, though the converse is not necessarily true. A maximal subfield E of $A \in \mathbf{CSA}(F)$ with $[E:F] = \operatorname{Deg} A$ will be called a *strictly maximal* subfield. Note that for any strictly maximal subfield E of $A \in \mathbf{CSA}(F)$,

$$(\dim_E A_E)[E:F] = \dim_F A = (\operatorname{Deg} A)^2 = [E:F]^2$$

implies that $\dim_E A_E = [E:F]$.

Theorem 3.6. *A field $E \subseteq A \in \mathbf{CSA}(F)$ is strictly maximal if and only if $\mathbf{C}_A(E) = E$.*

Proof. The Double Centralizer Theorem implies that

$$(\operatorname{Deg} A)^2 = \dim_F A = (\dim_F \mathbf{C}_A(E))(\dim_F E) = (\dim_F \mathbf{C}_A(E))[E : F],$$

and clearly $E \subseteq \mathbf{C}_A(E)$, so $[E : F]$ is equal to $\operatorname{Deg} A$ if and only if $\mathbf{C}_A(E) = E$. □

3.2 Splitting Fields

Definition 3.7. If A is an element of $\mathbf{CSA}(F)$, then an extension E of F is called a *splitting field* of A when $A^E \sim E$ as E-algebras. If E is a splitting field of A, then E is said to *split* A.

If E/F is a field extension with canonical inclusion homomorphism $\kappa : F \to E$, then Theorem 2.38 states that κ induces a homomorphism $\kappa_* : \mathbf{B}(F) \to \mathbf{B}(E)$ defined by $[A] \mapsto [A^E]$. The kernel of κ_* will be called the *relative Brauer group of* E/F, notation $\mathbf{B}(E/F)$. The following theorem holds by definition.

Theorem 3.8. *If $A \in \mathbf{CSA}(F)$ and E/F is a field extension, then E splits A if and only if $[A] \in \mathbf{B}(E/F)$.*

This reformulation of the definition of splitting fields immediately leads to a useful corollary. If we let E/K and K/F be two field extension with inclusions κ_1 and κ_2, respectively, then Theorem 2.38 states that $(\kappa_1 \circ \kappa_2)_* = \kappa_{1*} \circ \kappa_{2*}$, so $\mathbf{B}(K/F) = \operatorname{Ker} \kappa_{2*}$ is a subset of $\operatorname{Ker}(\kappa_1 \circ \kappa_2)_* = \mathbf{B}(E/F)$.

Corollary 3.9. *If E is a splitting field of $A \in \mathbf{CSA}(F)$, then all extension fields of E also split A.*

The following lemma describes some characterizing properties of splitting fields of $A \in \mathbf{CSA}(F)$ that are also subfields of A.

Lemma 3.10. *Let $A \in \mathbf{CSA}(F)$. Let E be a subfield of A, and let $k \in \mathbb{N}$ such that $k[E : F] = \operatorname{Deg} A$. The following conditions are equivalent.*

i) E is a splitting field of A.

ii) $\mathbf{C}_A(E) \cong M_k(E)$ as E-algebras.

iii) $A = B \otimes C$, where $B \in \mathbf{CSA}(F)$, $C \cong M_k(F)$, and E is a strictly maximal subfield of B.

Proof. If E is a splitting field of A, then Theorem 3.3 implies that $\mathbf{C}_A(E) \cong M_m(E)$ for some $m \in \mathbb{N}$. The Double Centralizer Theorem implies that $\dim_F A$ is equal to $(\dim_F \mathbf{C}_A(E))(\dim_F E) = m^2[E : F]^2$, so m is equal to k.

Now suppose that $\mathbf{C}_A(E) \cong M_k(E)$ as E-algebras. This means that $\mathbf{C}_A(E) \cong M_k(E)$ as F-algebras, so Corollary 1.22 and Theorem 2.24 imply that $\mathbf{C}_A(E) = E \otimes_F C$ for some

$C \subseteq \mathbf{C}_A(E)$ isomorphic to $M_k(F)$. If we define $B = \mathbf{C}_A(C)$, then the Double Centralizer Theorem and the definition of the centralizer together give that $E = \mathbf{C}_A(\mathbf{C}_A(E))$ is a subfield of $\mathbf{C}_A(C) = B$. Since C is an element of $\mathbf{CSA}(F)$, the Double Centralizer Theorem also implies that $B \in \mathbf{CSA}(F)$, that $A = B \otimes \mathbf{C}_A(B) = B \otimes C$, and that $\operatorname{Deg} B = \operatorname{Deg} A / \operatorname{Deg} C = (\operatorname{Deg} A)/k = [E : F]$.

Finally, suppose that condition *iii*) holds. Since E is a strictly maximal subfield of B, Theorem 3.6 implies that $\mathbf{C}_B(E) = E$. Theorem 3.3 states that B^E is Morita equivalent to $\mathbf{C}_B(E)$, so $[A] = [B]$ is an element of $\mathbf{B}(E/F)$. In other words, E splits A. □

Theorem 3.4 and Lemma 3.10 together imply that any maximal subfield of an algebra $A \in \mathbf{CSA}(F)$ splits A. The converse is not true, but it is true up to Morita equivalence.

Theorem 3.11. *Let $A \in \mathbf{CSA}(F)$ and let E/F be a finite field extension. The following three conditions are equivalent.*

i) E is a splitting field of A.

ii) There exists $B \in \mathbf{CSA}(F)$ such that $A \sim B$ and $E \subseteq B$ is strictly maximal.

iii) There exists $B \in \mathbf{CSA}(F)$ such that $A \sim B$ and $E \subseteq B$ is maximal.

Proof. It is immediately clear that *ii*) implies *iii*). As mentioned before, if we assume condition *iii*), then Theorem 3.4 and Lemma 3.10 imply that E splits B. Since A is Morita equivalent to B, Theorem 3.8 implies that E splits A as well.

Now suppose that E is a splitting field of A. Corollary 1.14 implies that we may as well assume that E is a subfield of the matrix algebra $M_n(F)$ with $n = [E : F]$. In this case, E is a subfield of the tensor product $A \otimes M_n(F)$, and E splits $A \otimes M_n(F)$, since $A \otimes M_n(F)$ is equivalent to A. Lemma 3.10 now implies the existence of $B \in \mathbf{CSA}(F)$, $k \in \mathbb{N}$ and $C \cong M_k(F)$ such that E is a strictly maximal subfield of B and $A \otimes M_n(F) = B \otimes C$, which implies that

$$A \sim A \otimes M_n(F) = B \otimes C \cong B \otimes M_k(F) \sim B.$$

□

Corollary 3.12. *Let $A \in \mathbf{CSA}(F)$. If E is a finite field extension of F such that $[E : F] = \operatorname{Deg} A$, then E splits A if and only if E is isomorphic as an F-algebra to a strictly maximal subfield of A.*

Proof. This follows directly from Theorem 3.11 and the fact that A and B in $\mathbf{CSA}(F)$ are isomorphic precisely when $A \sim B$ and $\dim_F A = \dim_F B$. □

The final theorem and corollary of this section explain the main reason why we are so interested in strictly maximal subfields and splitting fields.

Lemma 3.13. *Let $D \in \mathbf{CSA}(F)$ be a division algebra. If all subfields of D are purely inseparable over F, then $D = F$.*

Proof. See for instance the proof of Proposition 13.5 of [Pierce, 1982, p. 244-245] for a proof of this lemma. □

Lemma 3.14. *Let $D \in \mathbf{CSA}(F)$ be a division algebra. If K is a subfield of D that is maximal with the property that K/F is separable, then $K \subseteq D$ is strictly maximal.*

Proof. Consider the centralizer $\mathbf{C}_D(K)$. It is a subalgebra of the division algebra D, so Corollary 3.2 implies that $\mathbf{C}_D(K)$ is a division algebra, and $\mathbf{C}_D(K) \in \mathbf{CSA}(K)$ by Theorem 3.3. Since K is maximal with the property that K/F is separable, all subfields of $\mathbf{C}_D(K)$ have to be purely inseparable over K. Lemma 3.13 gives that $\mathbf{C}_D(K) = K$, so Theorem 3.6 yields that K is strictly maximal in D. □

Theorem 3.15. *For any $A \in \mathbf{CSA}(F)$, there exist $B \in \mathbf{CSA}(F)$ and a strictly maximal subfield E of B such that $A \sim B$ and E/F is a Galois extension.*

Proof. Let $D \in \mathbf{CSA}(F)$ be a division algebra such that $D \sim A$. We obtain from Lemma 3.14 that D contains a strictly maximal subfield K such that K/F is separable, and K splits A by Theorem 3.11. Since K/F is separable, it is well-known from Galois theory that there exists a field E containing K such that E/F is Galois, and Corollary 3.9 implies that this field E also splits A. The theorem now follows from Theorem 3.11. □

Corollary 3.16. *The Brauer group $\mathbf{B}(F)$ is equal to the union of relative Brauer groups $\mathbf{B}(E/F)$ with E/F ranging over all finite Galois extensions. Each element of $\mathbf{B}(E/F)$ has a representative $A \in \mathbf{CSA}(F)$ such that E is a strictly maximal subfield of A, and this representative is unique up to isomorphism.*

The uniqueness part of this corollary follows from the fact that A and B in $\mathbf{CSA}(F)$ are isomorphic precisely when $[A] = [B]$ and $\dim_F A = \dim_F B$, since the strict maximality of E implies that $\dim_F A$ is equal to $[E : F]^2$.

This corollary allows us to study the Brauer group $\mathbf{B}(F)$ by studying its relative Brauer groups $\mathbf{B}(E/F)$ with E/F a finite Galois extension.

3.3 Crossed Products

Corollary 3.16 implies the importance of algebras $A \in \mathbf{CSA}(F)$ with a strictly maximal subfield E of A such that E/F is finite and Galois. This section describes a construction of these algebras A.

If E/F is a Galois extension with Galois group $G = \mathbf{G}(E/F)$, then exponential notation $c \mapsto c^\sigma$ will be used to denote the action of G on E with $\sigma \in G$ and $c \in E$. We define the product in the Galois group to be the opposite of function composition, which ensures that $c^{\sigma\tau}$ is equal to $(c^\sigma)^\tau$ for all $c \in E$ and $\sigma, \tau \in \mathbf{G}(E/F)$.

The following lemma describes some properties of the algebra A we are trying to construct.

Lemma 3.17. *Let $A \in \mathbf{CSA}(F)$ such that A contains E as a strictly maximal subfield, where E/F is Galois with Galois group $G = \mathbf{G}(E/F)$.*

i) There exists a set $\{u_\sigma |\ \sigma \in G\} \subseteq A^\circ$ such that for all $\sigma \in G$ and $c \in E$

$$c^\sigma = u_\sigma^{-1} c u_\sigma. \tag{3.1}$$

ii) If $\{u_\sigma |\ \sigma \in G\} \subseteq A^\circ$ *satisfies i), then it is an* E*-vector space basis of* A_E*, and* $\Phi(\sigma,\tau) = u_{\sigma\tau}^{-1} u_\sigma u_\tau$ *defines a map* $\Phi : G \times G \to E^\circ$ *with the property that*

$$\Phi(\sigma,\tau)\Phi(\rho\sigma,\tau)^{-1}\Phi(\rho,\sigma\tau)(\Phi(\rho,\sigma)^\tau)^{-1} = 1_A \tag{3.2}$$

for all $\rho,\sigma,\tau \in G$*.*

iii) If $u_{1_G} = 1_A$*, then* $\Phi(\sigma,1_G) = \Phi(1_G,\sigma) = 1_A$ *for all* $\sigma \in G$*.*

Proof. Part *i*) is a direct consequence of the Noether-Skolem Theorem, and part *iii*) follows directly from the definition of Φ.

For part *ii*), assume that $\{u_\sigma |\ \sigma \in G\} \subseteq A^\circ$ satisfies *i*). The fact that E is strictly maximal in A yields that $\dim_E A_E = [E:F] = |G|$. Therefore, if $\{u_\sigma |\ \sigma \in G\}$ is linearly independent, then it is an E-basis of A_E.

If $\{u_\sigma |\ \sigma \in G\}$ is linearly dependent, then there exists a minimal non-empty set $X \subseteq G$ and $c_\sigma \in E^\circ$ for $\sigma \in X$ such that $\sum_{\sigma\in X} u_\sigma c_\sigma = 0_A$. All of the u_σ are non-zero, so $|X|$ is at least equal to 2. Note that $\sum_{\sigma\in X} u_\sigma c_\sigma d^\sigma$ is equal to $d\left(\sum_{\sigma\in X} u_\sigma c_\sigma\right) = 0_A$ for all $d \in E^\circ$. Since X was chosen to be minimal, the sequences $(c_\sigma d^\sigma)_{\sigma\in X}$ and $(c_\sigma)_{\sigma\in X}$ have to be proportional. This implies that $d^\sigma = d^\tau$ for all $d \in E^\circ$ and $\sigma,\tau \in X$, which is only possible if $|X| \leq 1$. This contradiction yields that $\{u_\sigma |\ \sigma \in G\}$ is indeed an E-basis for A_E. Note that the fact that $\{u_\sigma |\ \sigma \in G\}$ satisfies part *i*) of the theorem was enough to prove that this set is linearly independent. No other information was needed.

Repeated applications of (3.1) show that $u_{\sigma\tau}^{-1} u_\sigma u_\tau c = c u_{\sigma\tau}^{-1} u_\sigma u_\tau$ for all $c \in E^\circ$, so $u_{\sigma\tau}^{-1} u_\sigma u_\tau$ is an element of $\mathbf{C}_A(E) = E$, where $\mathbf{C}_A(E) = E$ follows from Theorem 3.6 and the fact that E is strictly maximal. Furthermore, $\{u_\sigma | \sigma \in G\} \subseteq A^\circ$ gives that $\Phi(\sigma,\tau) = u_{\sigma\tau}^{-1} u_\sigma u_\tau \neq 0_A$, and

$$\begin{aligned}\Phi(\rho\sigma,\tau)^{-1}\Phi(\rho,\sigma\tau)\Phi(\sigma,\tau) =& u_\tau^{-1} u_{\rho\sigma}^{-1} u_{\rho\sigma\tau} u_{\rho\sigma\tau}^{-1} u_\rho u_{\sigma\tau} u_{\sigma\tau}^{-1} u_\sigma u_\tau \\ =& u_\tau^{-1}\left(u_{\rho\sigma}^{-1} u_\rho u_\sigma\right) u_\tau = \Phi(\rho,\sigma)^\tau\end{aligned}$$

clearly holds for all $\rho,\sigma,\tau \in G$. The commutativity of E now yields (3.2). □

The definition of Φ may seem a bit arbitrary, but Φ was defined such that (3.2) is the *cocycle condition* for certain Galois cohomology groups. The construction and study of this Galois cohomology will be the focus of most of the remainder of this chapter.

Lemma 3.18. *If* G *is a group,* E *is a field, and* $\Phi : G^2 \to E^\circ$ *is a map that satisfies the cocycle condition in (3.2), then* $\Phi(\sigma,1_G) = \Phi(1_G,1_G)$ *and* $\Phi(1_G,\sigma) = \Phi(1_G,1_G)^\sigma$ *hold for all* $\sigma \in G$*.*

Proof. These two equations follow from applying the cocycle condition to the cases where $\sigma = \tau = 1_G$ and $\rho = \sigma = 1_G$. □

Theorem 3.19. *Let* E/F *be a finite Galois extension with Galois group* $G = \mathbf{G}(E/F)$*, and suppose that* $\Phi : G^2 \to E^\circ$ *satisfies the cocycle condition in (3.2). Let* $\{u_\sigma |\ \sigma \in G\}$ *be a basis for the* E*-space* $A = \bigoplus_{\sigma\in G} u_\sigma E$*, and define* $\mu : A \times A \to A$ *as*

$$\mu\left(\sum_{\sigma\in G} u_\sigma c_\sigma, \sum_{\tau\in G} u_\tau d_\tau\right) = \sum_{\sigma,\tau\in G} u_{\sigma\tau}\Phi(\sigma,\tau) c_\sigma^\tau d_\tau.$$

The map μ is F-bilinear and associative, and it defines a product on A with unit element $1_A = u_{1_G}\Phi(1_G, 1_G)^{-1}$. With this product A is a central simple F-algebra, $1_A E$ is a strictly maximal subfield of A, $\{u_\sigma |\ \sigma \in G\}$ satisfies part i) of Lemma 3.17, and $u_{\sigma\tau}^{-1} u_\sigma u_\tau$ is equal to $1_A\Phi(\sigma, \tau)$ for all $\sigma, \tau \in G$.

Proof. The definition of the product map μ makes most of the calculations in this proof annoyingly complicated. We often need the cocycle condition and Lemma 3.18 for even the simplest properties of A. However, with these tools and the tools derived from the fact that E/F is a finite Galois extension, most of the calculations and checks are actually quite straightforward. We therefore omit this proof, and refer to the proof of Proposition 14.1 from [Pierce, 1982] for more details. □

This algebra A is called the *crossed product of E and G relative to* Φ, notation (E, G, Φ), and we will often identify E with $1_A E \subseteq A$. We will simply write xy for the product $\mu(x, y)$ of $x, y \in (E, G, \Phi)$. A basis $\{u_\sigma |\ \sigma \in G\}$ of (E, G, Φ) that satisfies the conditions in this theorem will be called a *characterizing basis* of (E, G, Φ).

Corollary 3.16 implies the following corollary.

Corollary 3.20. *If E/F is finite Galois, then $\Phi \mapsto [(E, G, \Phi)]$ is surjective from the maps $\Phi : G^2 \to E^\circ$ that satisfy the cocycle condition to the relative Brauer group $\mathbf{B}(E/F)$.*

It would of course have been ideal if the map $\Phi \mapsto [(E, G, \Phi)]$ had been injective as well, but this is sadly not the case.

Theorem 3.21. *Let E/F be a finite Galois extension with Galois group $G = \mathbf{G}(E/F)$. If Φ and Ψ both satisfy the cocycle condition, then $(E, G, \Phi) \cong (E, G, \Psi)$ if and only if a map $\Theta : G \to E^\circ$ exists such that*

$$\Phi(\sigma, \tau)\Psi(\sigma, \tau)^{-1} = \Theta(\tau)\Theta(\sigma\tau)^{-1}\Theta(\sigma)^\tau. \tag{3.3}$$

for all $\sigma, \tau \in G$.

Proof. We will only sketch the proof of this theorem. See for instance the proof of Lemma 14.2 from [Pierce, 1982] for more details.

Suppose that $A = (E, G, \Phi)$ and $B = (E, G, \Psi)$ have characterizing bases $\{u_\sigma |\ \sigma \in G\}$ and $\{v_\sigma |\ \sigma \in G\}$, respectively.

If $\phi : A \to B$ is an F-algebra isomorphism, then the Noether-Skolem implies that the homomorphism $1_B c \mapsto \phi(1_A c)$ with $c \in E$ extends to an automorphism α on B. In this case, the map $\psi = \alpha^{-1}\phi : A \to B$ is an isomorphism that satisfies $\psi(1_A c) = 1_B c$ for all $c \in E$. If we define $\Theta : G \to E^\circ$ as $\Theta(\sigma) = \psi(u_\sigma)v_\sigma^{-1}$, then

$$\begin{aligned} 1_B\Phi(\sigma, \tau) = \psi(1_A\Phi(\sigma, \tau)) = \psi(u_{\sigma\tau}^{-1} u_\sigma u_\tau) &= \left(v_{\sigma\tau}\Theta(\sigma\tau)\right)^{-1} v_\sigma\Theta(\sigma)v_\tau\Theta(\tau) \\ &= \Theta(\sigma\tau)^{-1} v_{\sigma\tau}^{-1} v_\sigma v_\tau\Theta(\sigma)^\tau\Theta(\tau) = 1_B\Theta(\sigma\tau)^{-1}\Psi(\sigma, \tau)\Theta(\sigma)^\tau\Theta(\tau) \end{aligned}$$

implies that Θ satisfies (3.3).

For the proof in the other direction, suppose that $\Theta : G \to E^\circ$ satisfies (3.3). The map $\psi : A \to B$ defined as $\psi(u_\sigma) = v_\sigma\Theta(\sigma)$ is an F-algebra isomorphism. □

3.4 Galois Cohomology

In this section we will define Galois cohomology. Prior knowledge of cohomology is helpful, but not required.

Let E/F be a finite Galois extension with Galois group $G = \mathbf{G}(E/F)$. For $n \geq 0$, define $C^n(G, E^\circ)$ to be the abelian group of maps from G^n to E°, where the group multiplication is defined as pointwise multiplication. The elements of $C^n(G, E^\circ)$ are called *n-cochains on G with values in E°*. Note that $C^0(G, E^\circ)$ is canonically isomorphic to E°. We will often identify these two groups by using this isomorphism.

For $n \geq 0$, define the *n'th coboundary homomorphism* $\delta^{(n)} : C^n(G, E^\circ) \to C^{n+1}(G, E^\circ)$ as follows. For $n = 0$, define $\left(\delta^{(0)}(c)\right)(\sigma) = c(c^\sigma)^{-1} = c^{1-\sigma}$ for all $c \in E^\circ = C^0(G, E^\circ)$ and $\sigma \in G$. For $n \geq 1$, define

$$\left(\delta^{(n)}(\Omega)\right)(\sigma_1, \ldots, \sigma_{n+1}) = \\ \Omega(\sigma_2, \ldots, \sigma_{n+1}) \left(\prod_{i=1}^{n} \Omega(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{n+1})^{(-1)^i} \right) (\Omega(\sigma_1, \ldots, \sigma_n)^{\sigma_{n+1}})^{(-1)^{n+1}}$$

for all $\Omega \in C^n(G, E^\circ)$ and $\sigma_i \in G$.

Lemma 3.22. *For all $n \geq 0$, $\delta^{(n)}$ is a group homomorphism and $\delta^{(n)}\delta^{(n+1)} = 0$.*

Proof. See for instance Lemma 11.1 from [Pierce, 1982]. □

Define $Z^n(G, E^\circ) = \operatorname{Ker} \delta^{(n)}$, $B^n(G, E^\circ) = \operatorname{Im} \delta^{(n-1)}$ for $n \geq 1$ and $B^0(G, E^\circ) = \{1_E\}$. The elements of $Z^n(G, E^\circ)$ and $B^n(G, E^\circ)$ are called *n-cocycles* and *n-coboundaries*, respectively. For each $n \geq 0$, $B^n(G, E^\circ)$ is a subgroup of $Z^n(G, E^\circ)$ by Lemma 3.22.

Definition 3.23. For $n \geq 0$, define the *n'th Galois cohomology group* $H^n(G, E^\circ)$ as

$$H^n(G, E^\circ) = \frac{Z^n(G, E^\circ)}{B^n(G, E^\circ)}.$$

The elements of $H^n(G, E^\circ)$ are called *n-cohomology classes*.

We are mainly interested in the second Galois cohomology group $H^2(G, E^\circ)$. The definition of the coboundary homomorphisms implies that

$$\left(\delta^{(1)}(\Theta)\right)(\sigma, \tau) = \Theta(\tau)\Theta(\sigma\tau)^{-1}\Theta(\sigma)^\tau \qquad \text{and}$$
$$\left(\delta^{(2)}(\Phi)\right)(\rho, \sigma, \tau) = \Phi(\sigma, \tau)\Phi(\rho\sigma, \tau)^{-1}\Phi(\rho, \sigma\tau)(\Phi(\rho, \sigma)^\tau)^{-1}$$

for $\Theta \in C^1(G, E^\circ)$, $\Phi \in C^2(G, E^\circ)$ and $\rho, \sigma, \tau \in G$. The definition of $\delta^{(2)}$ implies that $\Phi \in C^2(G, E^\circ)$ satisfies the cocycle condition if and only if Φ is a cocycle. The definition of $\delta^{(1)}$ and Theorem 3.21 together imply that two cocycles $\Phi, \Psi \in Z^2(G, E^\circ)$ satisfy $(E, G, \Phi) \cong (E, G, \Psi)$ if and only if $[\Phi] = [\Psi]$ in $H^2(G, E^\circ)$. The definition of the crossed product and Corollary 3.16 now imply that the map $[\Phi] \mapsto [(E, G, \Phi)]$ is a bijection from $H^2(G, E^\circ)$ to $\mathbf{B}(E/F)$. The following theorem follows from the fact that this map is also a group homomorphism.

Theorem 3.24. *The map* $[\Phi] \mapsto [(E, G, \Phi)]$ *is an isomorphism of groups from* $H^2(G, E^\circ)$ *to* $\mathbf{B}(E/F)$.

The fact that $[\Phi] \mapsto [(E, G, \Phi)]$ is a homomorphism of groups is equivalent to the following lemma.

Lemma 3.25. *If* E/F *is a finite Galois extension with* $G = \mathbf{G}(E/F)$, *then*

$$(E, G, \Phi) \otimes (E, G, \Psi) \sim (E, G, \Phi\Psi)$$

for all $\Phi, \Psi \in Z^2(G, E^\circ)$.

Proof. Since the proof of this lemma is quite technical and of little interest to us, we refer to [Pierce, 1982, p. 256-259]. □

For the remainder of this section, we will focus on three theorems and a corollary that describe Morita equivalences between crossed products in different relative Brauer groups $\mathbf{B}(E/F)$. We only sketch the proofs of these theorems and refer to [Pierce, 1982] for the full proofs.

Theorem 3.26. *Let* E/F *and* K/F *be finite Galois extensions with* $K \subseteq E$ *and define* $G = \mathbf{G}(E/F)$, $H = \mathbf{G}(K/F)$ *and* $r = [E : K]$. *The homomorphism* $\sigma \mapsto \sigma|_K$ *from* G *to* H *induces an adjoint homomorphism* $C^n(H, K^\circ) \to C^n(G, E^\circ)$ *denoted by* $\Phi \mapsto \Phi^*$, *with* Φ^* *defined as* $\Phi^*(\sigma_1, \sigma_2, \ldots, \sigma_n) = \Phi(\sigma_1|_K, \sigma_2|_K, \ldots, \sigma_n|_K)$. *The crossed products* (K, H, Φ) *and* (E, G, Φ^*) *are equivalent for all* $\Phi \in Z^2(H, K^\circ)$.

Proof. Define $A = (E, G, \Phi^*)$ and $B = (K, H, \Phi)$. This proof revolves around the construction of a characterizing basis $\{u_\sigma |\ \sigma \in G\}$ of A in $M_r(B)$, which induces an isomorphism $A \cong M_r(B) \cong M_r(F) \otimes B$ that proves the theorem. See for instance the proof of Proposition 14.5 from [Pierce, 1982]. □

Theorem 3.27. *Let* E/F *be a finite Galois extension with Galois group* $G = \mathbf{G}(E/F)$. *Suppose that* K *is a field with* $F \subseteq K \subseteq E$, *and define* $H = \mathbf{G}(E/K) \subseteq G$. *If* Φ *is an element of* $Z^2(G, E^\circ)$, *then* $\Phi|_{H^2}$ *is an element of* $Z^2(H, E^\circ)$, *and* $(E, H, \Phi|_{H^2})$ *is Morita equivalent to* $(E, G.\Phi)^K$.

Proof. If $\{u_\sigma |\ \sigma \in G\}$ is a characterizing basis of $A = (E, G, \Phi)$, then $B = \bigoplus_{\tau \in H} u_\tau E$ is a subalgebra of A that is isomorphic to $(E, H, \Phi|_{H^2})$. This B is exactly equal to $\mathbf{C}_A(K)$ and Theorem 3.3 states that $\mathbf{C}_A(K) \sim A^K$, so $(E, H, \Psi) \sim (E, G, \Phi)^K$. See the proof of Lemma 14.7a from [Pierce, 1982] for more details. □

If E and K are subfields of some field L, then define the field EK as

$$EK = \left\{ \sum_{i=1}^{n} a_i b_i \,\middle|\, n \in \mathbb{N} \text{ and } a_i \in E, b_i \in K \text{ for all } 1 \leq i \leq n \right\}.$$

Theorem 3.28. *Let* E *and* K *be subfields of a field* L *such that* $E/E \cap K$ *is finite and Galois. The extension* EK/K *is finite and Galois, and we can identify* $\mathbf{G}(EK/K)$ *with the group* $H = \mathbf{G}(E/E \cap K)$ *through the restriction map* $\sigma \mapsto \sigma|_E$. *The isomorphism* $(EK, H, \Phi) \cong (E, H, \Phi)^K$ *holds for all* $\Phi \in Z^2(H, E^\circ) \subseteq Z^2(H, EK^\circ)$.

Proof. If $\{u_\sigma |\ \sigma \in G\}$ is a characterizing basis of (E, G, Φ), then it is clear that $(E, G, \Phi)^K$ and $\bigoplus_{\sigma \in G} u_\sigma EK$ are isomorphic as K-spaces. In fact, $\{u_\sigma |\ \sigma \in G\}$ turns out to be a characterizing basis for (EK, G, Φ) as well, proving the theorem. See the proof of Lemma 14.7c from [Pierce, 1982] for more details. □

Corollary 3.29. *Let F, E, and K be subfields of a field L such that $F \subseteq E \cap K$ and E/F is a finite Galois extension, and define $G = \mathbf{G}(E/F)$ and $H = \mathbf{G}(EK/K)$. If we identify H with the subgroup $\mathbf{G}(E/E \cap K)$ of G through the restriction map $\sigma \mapsto \sigma|_E$, then $(E, G, \Phi)^K \sim (EK, H, \Phi|_{H^2})$ holds for all $\Phi \in Z^2(G, E^\circ)$.*

Proof. Since K is equal to $(E \cap K)K$, $(E, G, \Phi)^K = (E, G, \Phi)^{(E\cap K)K}$ is isomorphic to $((E, G, \Phi)^{E\cap K})^K$. Theorem 3.27 implies that $(E, G, \Phi)^{E\cap K} \sim (E, H, \Phi|_{H^2})$, so we conclude that $(E, G, \Phi)^K \sim (E, H, \Phi|_{H^2})^K \cong (EK, H, \Phi|_{H^2})$, where the last isomorphism is a consequence of Theorem 3.28. □

3.5 The Schur Index and the Exponent

The degree map is not invariant under Morita equivalence. We therefore define two other numerical functions on central simple algebras, and we use them to prove that all Brauer groups are torsion groups.

Definition 3.30. The *Schur index* of $A \in \mathbf{CSA}(F)$ is defined as $\operatorname{Ind} A = \operatorname{Deg} D$, with $D \in \mathbf{CSA}(F)$ a division algebra such that $A \sim D$.

The Schur index is well-defined, since part *ii*) of Lemma 2.35 implies that the division algebra $D \in [A]$ is unique up to isomorphism. We usually simply call $\operatorname{Ind} A$ the index of A. The following theorem describes some properties of the index.

Theorem 3.31. *Let $A, B \in \mathbf{CSA}(F)$ and let E/F be a finite field extension.*

i) If $A \sim B$, then $\operatorname{Ind} A = \operatorname{Ind} B$.

ii) $\operatorname{Ind} A$ *divides* $\operatorname{Deg} A$.

iii) $\operatorname{Ind} A = \operatorname{Deg} A$ *if and only if A is a division algebra.*

iv) If E splits A, then $\operatorname{Ind} A$ *divides* $[E : F]$.

Proof. Part *i*) follows directly from the definition. Theorem 2.15 implies that there exist a unique $n \in \mathbb{N}$ and a division algebra $D \in \mathbf{CSA}(F)$ such that $A \cong M_n(D)$, hence part *ii*) and *iii*) follow from the equation $\operatorname{Deg} A = n \operatorname{Deg} D = n \operatorname{Ind} A$. Suppose that E splits A. Theorem 3.11 implies that there exists $C \in \mathbf{CSA}(F)$ such that $C \sim A$ and E is a strictly maximal subfield of C. Since $C \sim A$, there exists $m \in \mathbb{N}$ such that $C \cong M_m(D)$. We conclude that $[E : F] = \operatorname{Deg} C = m \operatorname{Deg} D = m \operatorname{Ind} A$. □

We can use crossed products and the index to prove the following theorem.

Theorem 3.32. *If $A \in \mathbf{CSA}(F)$ has index n, then $[A]^n = [F]$ in $\mathbf{B}(F)$. In particular, $\mathbf{B}(F)$ is a torsion group.*

Proof. Since Ind is constant on equivalence classes in $\mathbf{B}(F)$, Theorem 3.15, Lemma 3.17 and Theorem 3.19 together imply that we may as well assume that there exist a finite Galois extension E/F with Galois group $G = \mathbf{G}(E/F)$ and $\Phi \in Z^2(G, E^\circ)$ such that A is equal to (E, G, Φ). By Theorem 3.24, the claim $[A]^n = [F]$ is equivalent to the claim that $[\Phi]^n$ is trivial in $H^2(G, E^\circ)$, which is true if and only if $\Phi^n = \delta^{(1)}\Theta$ for some map $\Theta : G \to E^\circ$. We will now construct such a map Θ.

Part *ii*) of Theorem 3.31 states that $n = \operatorname{Ind} A$ divides $\operatorname{Deg} A$, so $[E : F] = \operatorname{Deg} A$ is equal to mn for some $m \in \mathbb{N}$. By definition of Deg and Ind, this implies that $A \cong M_m(D)$ for some division algebra $D \in \mathbf{CSA}(F)$ of degree n. Let M be the left D-module $\bigoplus_{i=1}^m D$. We can define a right scalar multiplication by A on M that is based on the vector-matrix product of column vectors of height m over D with matrices in $M_m(D)$, and this turns M into a D-A bimodule.

Since E is a subfield of A, M can also be viewed as a right E-module M_E. We would like to determine $\dim_E M_E$. The bimodule condition $au = ua$ for all $a \in F$ and $u \in M$ implies that $\dim {}_F M = \dim M_F$, which means that

$$(\dim M_E)mn = (\dim M_E)[E : F] = \dim M_F = \dim {}_F M = m(\dim {}_F D) = mn^2.$$

We conclude that $\dim M_E = n$.

Let $w_1, \ldots w_n$ be a basis of M_E and suppose that $\{u_\sigma |\ \sigma \in G\}$ is a characteristic basis of A. Let $\mu(\sigma) \in M_n(E)$ be the matrix that describes right multiplication by u_σ in M_E with respect to the basis $w_1, \ldots, w_n$, so $w_j u_\sigma = \sum_{i=1}^n w_i(\mu(\sigma)_{i,j})$ for all $1 \leq j \leq n$. The fact that u_σ is an element of A° implies that $\mu(\sigma)$ is invertible. Furthermore,

$$\begin{aligned}\sum_{i=1}^n w_i(\mu(\sigma\tau)_{i,j})\Phi(\sigma,\tau) = w_j u_{\sigma\tau}\Phi(\sigma,\tau) = w_j u_\sigma u_\tau &= \sum_{k=1}^n w_k(\mu(\sigma)_{k,j})u_\tau \\ &= \sum_{k=1}^n w_k u_\tau(\mu(\sigma)_{k,j})^\tau = \sum_{k=1}^n \sum_{i=1}^n w_i(\mu(\tau)_{i,k})(\mu(\sigma)_{k,j})^\tau \\ &= \sum_{i=1}^n w_i \left(\sum_{k=1}^n (\mu(\tau)_{i,k})(\mu(\sigma)_{k,j})^\tau \right),\end{aligned}$$

implies that $\mu(\sigma\tau)\Phi(\sigma,\tau) = \mu(\tau)\mu(\sigma)^\tau$ for all $\sigma, \tau \in G$, where $\mu(\sigma)^\tau$ is the matrix in $M_n(E)$ defined by $(\mu(\sigma)^\tau)_{i,j} = (\mu(\sigma)_{i,j})^\tau$ for all $1 \leq i, j \leq n$. If we define $\Theta : G \to E^\circ$ as $\Theta(\sigma) = \det \mu(\sigma)$, then clearly $\Theta(\sigma\tau)\Phi(\sigma,\tau)^n = \Theta(\tau)\Theta(\sigma)^\tau$ for all $\sigma, \tau \in G$, which means that $\Phi^n = \delta^{(1)}\Theta$. □

Definition 3.33. Let $A \in \mathbf{CSA}(F)$. The order of $[A]$ in $\mathbf{B}(F)$ is called the *exponent of* A, notation $\operatorname{Exp} A$.

Theorem 3.32 clearly implies that $\operatorname{Exp} A$ is finite for all $A \in \mathbf{CSA}(F)$. The following theorems lists some properties of the exponent.

Theorem 3.34. *Let $A, B \in \mathbf{CSA}(F)$ and let E/F be a finite field extension.*

i) If $A \sim B$, then $\operatorname{Exp} A = \operatorname{Exp} B$.

ii) $\operatorname{Exp} A$ divides $\operatorname{Ind} A$.

iii) $\operatorname{Exp} A^E$ divides $\operatorname{Exp} A$.

Proof. Property *i)* follows directly from the definition of the exponent, and property *ii)* is a direct consequence of Theorem 3.32. Property *iii)* follows from the fact that $[A] \mapsto [A^E]$ defines a homomorphism from $\mathbf{B}(F)$ to $\mathbf{B}(E)$. □

Theorem 3.35. *If F is finite, $F = \mathbb{R}$ or $F = \mathbb{C}$, then $\operatorname{Exp} A$ is equal to $\operatorname{Ind} A$ for all algebras $A \in \mathbf{CSA}(F)$.*

Proof. If F is finite or $F = \mathbb{C}$, then $\mathbf{B}(F)$ is trivial by Theorem 2.39 and Corollary 2.42, so $\operatorname{Exp} A = \operatorname{Ind} A = 1$ for all $A \in \mathbf{CSA}(F)$. For the field $\mathbb{R}$ Corollary 2.41 states that $\mathbf{B}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$. Since Exp and Ind are constant on Morita equivalence classes, it is sufficient to note that $\operatorname{Exp} \mathbb{R} = 1 = \operatorname{Ind} \mathbb{R}$ and $\operatorname{Exp} \mathbb{H} = 2 = \operatorname{Ind} \mathbb{H}$. □

It will turn out that $\operatorname{Exp} A$ is also equal to $\operatorname{Ind} A$ for all $A \in \mathbf{CSA}(F)$ when F is a local field and when F is an algebraic number field, but it will take some work to prove this fact.

3.6 Cyclic Algebras

Definition 3.36. A field extension E/F is *cyclic* when E/F is Galois and $\mathbf{G}(E/F)$ is a finite cyclic group. An algebra $A \in \mathbf{CSA}(F)$ is *cyclic* when A contains a strictly maximal subfield E such that E/F is cyclic.

By definition, any cyclic algebra is a crossed product. We will encounter cyclic algebras when determining the structure of Brauer groups of local fields and algebraic number fields, so we study them in some detail here.

Theorem 3.37. *Let E/F be a cyclic extension such that $G = \mathbf{G}(E/F)$ is cyclic of order n with generator σ. If $A \in \mathbf{CSA}(F)$ contains E as a strictly maximal subfield, then there exists $u \in A^\circ$ such that the following statements hold.*

i) $A = \bigoplus_{0=1}^{n-1} u^i E$.

ii) $u^{-1} d u = d^\sigma$ for all $d \in E$.

iii) $u^n = a \in F^\circ$.

Conversely, if A is the F-algebra defined by i), ii) and iii), then $A \cong (E, G, \Phi_a)$ with

$$\Phi_a(\sigma^i, \sigma^j) = \begin{cases} 1_F & \text{if } 0 \leq i, j < n \text{ and } i + j < n, \\ a & \text{if } 0 \leq i, j < n \text{ and } i + j \geq n. \end{cases}$$

Proof. Assume that $A \in \mathbf{CSA}(F)$ contains E as a strictly maximal subfield. The Noether-Skolem Theorem implies that there exists $u \in A^\circ$ such that $u^{-1}du = d^\sigma$ for all $d \in E$, so induction yields $u^{-j}du^j = d^{\sigma^j}$ for all $j \in \mathbb{N}$. Part *ii)* of Lemma 3.17 implies that $A = \bigoplus_{i=0}^{n-1} u^i E$. Furthermore, $u^{-n}du^n = d$ implies that u^n is an element of $\mathbf{C}_A(E) = E$, where $\mathbf{C}_A(E) = E$ follows from Theorem 3.6 since E is strictly maximal. Clearly, u^n is also an element of $\mathbf{C}_A(\bigoplus_{i=0}^{n-1} u^i E) = \mathbf{C}_A(A) = \mathbf{Z}(A) = F$, so $u^n \in A^\circ \cap F = F^\circ$.

For the second half of the proof, assume that A is an F-algebra that satisfies *i)*, *ii)* and *iii)*. Note that these conditions together fully determine the algebraic structure of A, so the algebra that satisfies the conditions is unique up to isomorphism. To complete the proof, we will now show that $B = (E, G, \Phi_a)$ satisfies condition *i)*, *ii)* and *iii)*.

A straightforward computation shows that Φ_a satisfies the cocycle condition, so the algebra $B = (E, G, \Phi_a) = \bigoplus_{0 \le j < n} u_{\sigma^j} E$ is well-defined. Define $u = u_\sigma$, and note that 1_B satisfies $1_B = u_{1_G}\Phi_a(1_G, 1_G)^{-1} = u_{1_G}$. If j is an integer with $1 < j < n$, then $u_\sigma u_{\sigma^{j-1}} = u_{\sigma^j}\Phi_a(\sigma, \sigma^j) = u_{\sigma^j}$ implies that $u_{\sigma^j} = u^j$ for all $0 \le j < n$. Furthermore,

$$u^n = uu^{n-1} = u_\sigma u_{\sigma^{n-1}} = u_{\sigma^n}\Phi_a(\sigma, \sigma^{n-1}) = u_{1_G}a = 1_B a = a,$$

so all three conditions hold for $u = u_\sigma$ in B. □

It makes sense to simplify the crossed product notation when the algebra is cyclic. We will write (E, σ, a) instead of $(E, \mathbf{G}(E/F), \Phi_a)$ when $\mathbf{G}(E/F)$ is a cyclic group generated by σ. A *characterizing element* u or u_σ of (E, σ, a) is an element of $(E, \sigma, a)^\circ$ that satisfies $u^n = a$ for $n = [E : F]$ and $u^{-1}du = d^\sigma$ for all $d \in E$.

We will now translate some of our results on crossed products to this new notation, and we will add some new results as well.

Let $N_{E/F} : E \to F$ denote the field norm of a field extension E/F. Note that the field norm satisfies $N_{E/F}(c) = \prod_{\sigma \in \mathbf{G}(E/F)} c^\sigma$ for all $c \in E$ when E/F is a finite Galois extension.

Theorem 3.38. *Let E/F be a cyclic extension of degree n with $\mathbf{G}(E/F) = \langle\sigma\rangle$, and suppose that $a, b \in F^\circ$.*

i) $(E, \sigma, a) \otimes (E, \sigma, b) \sim (E, \sigma, ab)$.

ii) $(E, \sigma, 1_F) \sim F$.

iii) $(E, \sigma^k, a^k) \cong (E, \sigma, a)$ *for $k \in \mathbb{Z}$ relatively prime to n.*

iv) $(E, \sigma, a) \cong (E, \sigma, b)$ *if and only if $b/a \in N_{E/F}(E^\circ)$.*

v) $(E, \sigma, a) \sim F$ *if and only if $a \in N_{E/F}(E^\circ)$.*

Proof. Part *i)* follows from Lemma 3.25 and the fact that $\Phi_a\Phi_b = \Phi_{ab}$ for all $a, b \in F^\circ$. Part *ii)* follows directly from part *i)* and the isomorphism $\mathbf{B}(E/F) \cong H^2(\mathbf{G}(E/F), E^\circ)$ in Theorem 3.24. Part *ii)* and *iv)* together imply part *v)*.

For the proof of part *iii)*, suppose that u is a characterizing element of $A = (E, \sigma, a)$. If $k \in \mathbb{Z}$ is relatively prime to n, then we find that $A = \bigoplus_{i=1}^{n} (u^k)^i E$, $\mathbf{G}(E/F) = \langle\sigma^k\rangle$,

$u^{-k}du^k = d^{\sigma^k}$, and $(u^k)^n = a^k$, so the algebras (E, σ^k, a^k) and (E, σ, a) are isomorphic by Theorem 3.37.

For part *iv*), let $u \in (E, \sigma, a)^\circ$ be a characterizing element. If v is equal to uc for some $c \in E^\circ$, then $v^{-1}dv = c^{-1}u^{-1}duc = c^{-1}d^\sigma c = d^\sigma$ for all $d \in E$ and

$$\begin{aligned} v^2 =& u(cu)c = u(uc^\sigma)c = u^2c^{1+\sigma}, \\ v^3 =& ucu^2c^{1+\sigma} = u^3c^{\sigma^2}c^{1+\sigma} = u^3c^{1+\sigma+\sigma^2}, \\ & \vdots \\ v^n =& ucu^{n-1}c^{1+\sigma+\ldots+\sigma^{n-2}} = u^nc^{1+\sigma+\ldots+\sigma^{n-1}} = aN_{E/F}(c). \end{aligned}$$

We find that $(E, \sigma, a) = \bigoplus_{i=1}^n v^iE$, so Theorem 3.37 implies that (E, σ, a) is isomorphic to $(E, \sigma, aN_{E/F}(c))$ for all $c \in E^\circ$. In particular, we conclude that $(E, \sigma, a) \cong (E, \sigma, b)$ if $b/a \in N_{E/F}(E^\circ)$.

Conversely, let $\phi : (E, \sigma, b) \to (E, \sigma, a)$ be an F-algebra isomorphism, and suppose that $u \in (E, \sigma, a)$ and $v \in (E, \sigma, b)$ are characterizing elements. As in the proof of Theorem 3.21, we can construct an automorphism α on (E, σ, a) such that the map $\psi = \alpha^{-1}\phi : (E, \sigma, b) \to (E, \sigma, a)$ is an F-algebra isomorphism with the property that $\psi(d) = d$ for all $d \in E$.

Apply ψ to the equation $u^{-1}du = d^\sigma$ and note that $(\psi(u))^{-1}d(\psi(u)) = d^\sigma = v^{-1}dv$ for all $d \in E$. We find that $\psi(u)v^{-1}$ is equal to some $c \in \mathbf{C}_{(E,\sigma,a)}(E) = E$, where $\mathbf{C}_{(E,\sigma,a)}(E) = E$ follows from Theorem 3.6 and the fact that E is strictly maximal. The fact that b/a is an element of $N_{E/F}(E^\circ)$ now follows from the equation

$$b = \psi(b) = \psi(v^n) = (uc)^n = aN_{E/F}(c).$$

□

Corollary 3.39. *If E/F is a cyclic extension, then the relative Brauer group $\mathbf{B}(E/F)$ is isomorphic to the multiplicative group $F^\circ/N_{E/F}(E^\circ)$. In particular, if σ is a generator of $\mathbf{G}(E/F)$, then the map $F^\circ/N_{E/F}(E^\circ) \to \mathbf{B}(E/F)$ defined by $aN_{E/F}(E^\circ) \mapsto [(E, \sigma, a)]$ is a group isomorphism.*

Proof. The map $\phi : F^\circ \to \mathbf{B}(E/F)$ defined by $a \mapsto [(E, \sigma, a)]$ is well-defined and surjective by Theorem 3.37. Parts *i*) and *v*) of Theorem 3.38 imply that ϕ is a group homomorphism with kernel $N_{E/F}(E^\circ)$, so the theorem follows from the first isomorphism theorem for groups. □

In the next chapter, we will use this corollary in combination with Corollary 3.16 to find the structure of $\mathbf{B}(F)$ when F is a local field.

We consider two more theorems on Morita equivalence of cyclic algebras.

Theorem 3.40. *Let E/F be a cyclic extension of degree n with $\mathbf{G}(E/F) = \langle\sigma\rangle$. If K is a field with $F \subseteq K \subseteq E$ and $[K : F] = m$, then K/F is cyclic with $\mathbf{G}(K/F) = \langle\sigma|_K\rangle$, and $(K, \sigma|_K, a)$ is equivalent to $(E, \sigma, a^{n/m})$ for all $a \in F^\circ$.*

Proof. Since $\mathbf{G}(E/F)$ is cyclic, all subgroups of $\mathbf{G}(E/F)$ are normal. This implies that $\mathbf{G}(E/K)$ is a normal subgroup of $\mathbf{G}(E/F)$, so K/F is Galois with $\mathbf{G}(K/F)$ equal to $\{\tau|_K|\ \tau \in \mathbf{G}(E/F)\} = \langle \sigma|_K \rangle$, which is a cyclic group of order m.

If we use the notation $(K, \sigma|_K, a) = (K, H, \Psi_a)$ and $(E, \sigma, a^{n/m}) = (E, G, \Phi_{a^{n/m}})$, then Theorem 3.26 yields that $(K, H, \Psi_a) \sim (E, G, \Psi_a^*)$. A straightforward calculation shows that $\Phi_{a^{n/m}}$ is equal to $\Psi_a^*(\delta^{(1)}\Theta)$ for $\Theta : G \to E^\circ$ defined as $\Theta(\sigma^i) = a^r$ if $0 \leq i < n$ can be written as $i = rm + k$ with $0 \leq k, l < m$. Theorem 3.21 now implies that $(E, G, \Psi_a^*) \cong (E, G, \Phi_{a^{n/m}})$, which completes the proof. $\square$

Theorem 3.41. *If F, E and K are subfields of a field L such that $F \subseteq E \cap K$ and E/F is cyclic of degree n with $\mathbf{G}(E/F) = \langle \sigma \rangle$, then EK/K is cyclic and $\mathbf{G}(EK/K) \cong \langle \sigma^r \rangle$, where $r = [E \cap K : F] = [E : F]/[EK : K]$. Moreover, for all $a \in F^\circ$, $(E, \sigma, a)^K$ is cyclic and $(E, \sigma, a)^K \sim (EK, \sigma^r, a)$.*

Proof. This corollary follows directly from Corollary 3.29, where we use the described restriction of automorphisms to identify $\mathbf{G}(EK/K)$ with $\mathbf{G}(E/(E \cap K)) \cong \langle \sigma^r \rangle$. Note that $[EK : K] = [E : E \cap K]$ implies that $[E \cap K : F]$ is equal to $[E : F]/[EK : K]$. $\square$

4 Local Fields

In this chapter we define valuations of division rings, and we use these valuations to define and study local fields, culminating in an isomorphism between $\mathbf{B}(F)$ and $\mathbb{Q}/\mathbb{Z}$ when F is a local field with infinitely many elements.

Section 4.1 contains the definition of valuations of division rings and basic properties of these valuations. The metric topology induced by these valuations is studied in Section 4.2, and this section also includes a definition and characterization of local fields. Section 4.3 discusses the completions of division rings with respect to their valuation topologies. In Section 4.4 we find sufficient conditions under which valuations of a field can be uniquely extended to finite-dimensional division algebras over that field. The ramification index and relative degree of a field extension are defined in Section 4.5, and we use them to prove that the Brauer group $\mathbf{B}(F)$ of an infinite local field F is equal to the union of the relative Brauer groups $\mathbf{B}(K/F)$ with K/F ranging over the finite extensions of F with ramification index 1. In Section 4.6 we study these finite extensions of infinite local fields with ramification index 1, and prove that the relative Brauer groups of these extensions are finite cyclic groups. Finally, Section 4.7 contains the proof that the Brauer group of an infinite local field is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

In this chapter F will always denote a field.

4.1 Valuations of Division Rings

Definition 4.1. A *valuation* of a division ring D is a map $v : D \to \mathbb{R}$ such that

i) $v(x) \geq 0$ for all $x \in D$.

ii) $v(x) = 0$ if and only if $x = 0_D$.

iii) $v(xy) = v(x)v(y)$ for all $x, y \in D$.

iv) there exists $a \in \mathbb{R}_{>0}$ with $v(x + y) \leq a \max\{v(x), v(y)\}$ for all $x, y \in D$.

Note that for any valuation v of D, $v|_{D^\circ}$ is a group homomorphism from D° to the multiplicative group $\mathbb{R}_{>0}$, and note that any group homomorphism $w : D^\circ \to \mathbb{R}_{>0}$ that satisfies property iv) can be extended to a valuation by defining $w(0_D) = 0$. For instance, the trivial homomorphism from $D^\circ \to \mathbb{R}_{>0}$ extends to the *trivial valuation* defined as $v(x) = 1$ for $x \in D^\circ$ and $v(0_D) = 0$. Other valuations of D are called *non-trivial*.

If v is a valuation of the division ring D, then v^e is also a valuation of D for any $e \in \mathbb{R}_{>0}$, where v^e is defined as $v^e(x) = v(x)^e$ for all $x \in D$. Two valuations v and w

of D are called *equivalent* if $v = w^e$ for some $e \in \mathbb{R}_{>0}$. Equivalence of valuations is an equivalence relation on the set of valuations of D.

Suppose that D_1 and D_2 are division rings such that $D_1 \subseteq D_2$, and suppose that v and w are valuations of D_1 and D_2, respectively. The valuation w is said to *extend* v, notation $v \subseteq w$, if the restriction $w|_{D_1}$ of w to D_1 is equal to v. The valuation w is said to *divide* v, notation $w|v$, if $w|_{D_1}$ is merely equivalent to v.

Properties $i)$ and $iv)$ of Definition 4.1 imply that $\{v(1_D + x)|\ x \in D, v(x) \leq 1\}$ is a bounded subset of $\mathbb{R}$, so we can define the *valuation constant* $a(v)$ as

$$a(v) = \sup\{v(1_D + x)|\ x \in D, v(x) \leq 1\}.$$

Note that $a(v) \geq 1$ and that $a(v)$ is the smallest value of $a \in \mathbb{R}_{>0}$ such that property $iv)$ is satisfied. The following lemma extends this usage of $a(v)$ to larger sums.

Lemma 4.2. *Let v be a valuation of a division ring D and let $x_1, \ldots, x_n \in D$ for some $n \in \mathbb{N}$. Then*

$$v(x_1 + \ldots + x_n) \leq a(v)^m \max\{v(x_i)|\ i = 1, \ldots, n\},$$

where m is the integer such that $\log_2(n) \leq m < \log_2(n) + 1$.

Proof. This lemma can be proven for n of the form 2^m by induction on m. For other values of n we can simply add $2^m - n$ terms 0_D to the sum $x_1 + \ldots + x_n$ and then apply the result for n a power of 2. □

We list some simple properties of valuations without proof

Lemma 4.3. *Let D be a division ring, $x, y \in D$, $n \in \mathbb{N}$, $e \in \mathbb{R}_{>0}$, and let v be a valuation of D.*

i) *If $v(x^n) = v(y^n)$, then $v(x) = v(y)$.*

ii) $v(-x) = v(x)$.

iii) $a(v) \geq 1$.

iv) $a(v^e) = a(v)^e$.

v) *If $a(v) = 1$, then $a(w) = 1$ for all valuations w that are equivalent to v.*

vi) *If $a(v) > 1$ and $a \in \mathbb{R}$ with $a > 1$, then there exists a unique valuation w equivalent to v with $a(w) = a$.*

Proof. These properties follow directly from the definitions of valuations and valuation constants. □

A valuation v of a division ring D is called *non-archimedean* when $a(v) = 1$ and *archimedean* when $a(v) > 1$. Part $v)$ of Lemma 4.3 implies that for equivalent valuations v and w, v is non-archimedean if and only if w is non-archimedean.

We now consider some examples of valuations and check whether these examples are archimedean or non-archimedean. The trivial valuation is clearly non-archimedean. For any subfield F of $\mathbb{C}$, the *absolute value* $v_\infty(x) = |x|$ defines a valuation v_∞ or v_∞^F of F with $a(v_\infty) = 2$. For any prime number p, we can define the *p-adic valuation* valuation v_p of $\mathbb{Q}$ as $v_p(0) = 0$ and $v_p(x) = (1/p)^k$ for $x \in \mathbb{Q}^\circ$, where k is the unique integer such that $x = p^k a/b$ for some $a, b \in \mathbb{Z} \setminus p\mathbb{Z}$. A quick calculation shows that $a(v_p) = 1$ for all p-adic valuations v_p. At the end of this section we will see that all non-trivial valuations of $\mathbb{Q}$ are equivalent to either a p-adic valuation v_p or to the absolute value v_∞.

Note that all of the valuations we just mentioned satisfy the triangle inequality. The valuations that satisfy the triangle inequality can be characterized as follows.

Theorem 4.4. *Let v be a valuation of the division ring D. Then v satisfies the triangle inequality $v(x+y) \leq v(x) + v(y)$ for all $x, y \in D$ if and only if $a(v) \leq 2$.*

Proof. If v satisfies the triangle inequality, then $v(1_D + x) \leq v(1_D) + v(x) \leq 2$ is true for all $x \in D$ with $v(x) \leq 1$, so $a(v) \leq 2$ by definition. See for instance Proposition 17.1 from [Pierce, 1982] for a proof of the opposite implication. □

Corollary 4.5. *All valuations of a division ring are equivalent to a valuation that satisfies the triangle inequality.*

Proof. This corollary follows directly from Theorem 4.4 and part *vi)* of Lemma 4.3. □

The following theorem characterizes the non-archimedean valuations.

Theorem 4.6. *For any valuation v of a division ring D, the following are equivalent.*

i) v is non-archimedean.

ii) $v(m1_D) \leq 1$ for all $m \in \mathbb{Z}$.

iii) $\{v(m1_D) |\ m \in \mathbb{N}\}$ is bounded.

Proof. If v is non-archimedean, then $v(m1_D) = v(-m1_D) \leq 1$ for all $m \in \mathbb{N}$ and $v(0_D) = 0$, so *ii)* holds. It is clear that *ii)* implies *iii)*.

Assume that there exists $c \in \mathbb{R}_{>0}$ such that $v(m1_D) \leq c$ for all $m \in \mathbb{N}$. If $x \in D$ satisfies $v(x) \leq 1$, then for all $k \in \mathbb{N}$ and $l \in \mathbb{Z}$ such that $\log_2(k) \leq l < \log_2(k) + 1$

$$v(1_D + x)^k = v\left(\sum_{i=0}^{k} \binom{k}{i} x^i\right) \leq a(v)^l \max\left\{v\left(\binom{k}{i}\right) v(x)^i |\ 0 \leq i \leq k\right\} \leq a(v)^l c$$

by Lemma 4.2. We find that $v(1_D + x) \leq \lim_{k\to\infty} a(v)^{l/k} c^{1/k}$, and $\lim_{k\to\infty} \log_2(k)/k = 0$ implies that $\lim_{k\to\infty} a(v)^{l/k} c^{1/k}$ is equal to 1. We conclude that $a(v)$ is equal to 1. □

The following theorem describes to what extend some properties of valuations are inherited through extensions.

Theorem 4.7. *Let D_1 and D_2 be division rings with $D_1 \subseteq D_2$ and suppose that the valuation w of D_2 extends the valuation v of D_1.*

i) w is non-archimedean if and only if v is non-archimedean.

ii) If w is trivial, then v is trivial.

iii) If v is trivial and D_1 is a field with $\dim_{D_1} D_2 < \infty$, then w is trivial.

Proof. Part *i*) is an immediate consequence of Theorem 4.6, and part *ii*) is trivial. Now assume that the conditions in part *iii*) hold, and let X be a D_1-basis of D_2. The fact that $\dim_{D_1} D_2$ is finite implies that $\sup w(D_2) = \sup w(X)$ is finite, so w is trivial. □

If v is a non-archimedean valuation of a division ring D, then

$$v(x_1 + \ldots + x_n) \leq \max\{v(x_i)|\ i = 1, \ldots, n\}$$

holds for all $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in D$ by Lemma 4.2. The Domination Principle makes an even stronger statement about $v(x_1 + \ldots + x_n)$.

Theorem 4.8 (Domination Principle)**.** *Let v be a non-archimedean valuation of the division ring D. If $x_1, \ldots, x_n$ are elements of D such that $v(x_1) > v(x_i)$ for all $2 \leq i \leq n$, then $v(x_1 + \ldots + x_n) = v(x_1)$.*

Proof. Denote $z = x_2 + \ldots + x_n$ and note that $v(z) \leq \max\{v(x_i)|\ i = 2, \ldots, n\} < v(x_1)$. Two applications of the inequality $v(x + y) \leq \max\{v(x), v(y)\}$ with $x, y \in D$ show that

$$\begin{aligned} v(x_1 + z) &\leq \max\{v(x_1), v(z)\} = v(x_1) = v((x_1 + z) + (-z)) \\ &\leq \max\{v(x_1 + z), v(-z)\} = \max\{v(x_1 + z), v(z)\} = v(x_1 + z), \end{aligned}$$

where the last equality follows from the fact that $v(z) < v(x_1)$. We conclude that $v(x_1 + z)$ is equal to $v(x_1)$. □

For a valuation v of a division ring D, define the sets $O(D, v) = \{x \in D|\ v(x) \leq 1\}$ and $P(D, v) = \{x \in D|\ v(x) < 1\}$. If v is a non-archimedean valuation, then $O(D, v)$ is called the *valuation ring of* v, $P(D, v)$ is called the *valuation ideal of* v, and the quotient $E(D, v) = O(D, v)/P(D, v)$ is called the *residue class field of* D. The following lemma mostly justifies the choice of names.

Lemma 4.9. *If v is a non-archimedean valuation of a division ring D, then $O(D, v)$ is a subring of D, $P(D, v)$ is a prime ideal of $O(D, v)$ and $E(D, v)$ is a division ring.*

Proof. Since v is non-archimedean, $v(x - y) \leq \max\{v(x), v(y)\}$ for all $x, y \in D$. This implies that $O(D, v)$ and $P(D, v)$ are subgroups of D with respect to addition. The equation $v(xy) = v(x)v(y)$ then implies that $O(D, v)$ is a subring of D and that $P(D, v)$ is a prime ideal of $O(D, v)$. The fact that $v(x^{-1}) = v(x)^{-1}$ for all $x \in D^\circ$ implies that $O(D, v)^\circ = \{x \in D^\circ|\ v(x) = 1\} = O(D, v) \setminus P(D, v)$. We conclude that the quotient $E(D, v) = O(D, v)/P(D, v)$ is a division ring. □

The residue class field $E(D,v)$ is called a field because $E(D,v)$ is commutative in most situations where we will encounter it.

The sets $O(D,v)$ and $P(D,v)$ turn out to be an excellent way to check for equivalence of valuations.

Lemma 4.10. *Let v and w be non-trivial valuations of a division ring D. The following statements are equivalent.*

i) v *and* w *are equivalent.*

ii) $O(D,v) = O(D,w)$ *and* $P(D,v) = P(D,w)$.

iii) $O(D,v) = O(D,w)$.

iv) $O(D,v) \subseteq O(D,w)$.

v) $P(D,v) \subseteq P(D,w)$.

Proof. It is clear from the definitions that *i)* implies *ii)*, and it is obvious that *ii)* implies *iii)*, *iv)*, and *v)*. An element x of D is contained in $P(D,v)$ if and only if either $x = 0_D$ or $x^{-1} \notin O(D,v)$, so $O(D,v) = O(D,w)$ implies that $P(D,v) = P(D,w)$. In other words, *iii)* implies *ii)*. If we prove that *ii)* implies *i)*, and that both *iv)* and *v)* imply *iii)*, then that would complete this proof.

Suppose that $O(D,v) = O(D,w)$ and $P(D,v) = P(D,w)$. All $x, y \in D$ with $w(x) > 1$ and $w(y) > 1$ satisfy $v(x) > 1$ and $v(y) > 1$. For such x and y and all $m, n \in \mathbb{N}$, $\log(w(x))/\log(w(y)) \leq m/n$ is equivalent to $x^m y^{-n} \in O(D,w) = O(D,v)$, so

$$\left\{ \frac{m}{n} \middle| \, m,n \in \mathbb{N}, \frac{\log(w(x))}{\log(w(y))} \leq \frac{m}{n} \right\} = \left\{ \frac{m}{n} \middle| \, m,n \in \mathbb{N}, \frac{\log(v(x))}{\log(v(y))} \leq \frac{m}{n} \right\}.$$

We conclude that $\log(w(x))/\log(w(y))$ is equal to $\log(v(x))/\log(v(y))$, so the fraction $\log(w(x))/\log(v(x))$ is equal to some constant $e \in \mathbb{R}_{>0}$ for all $x \in D$ with $w(x) > 1$. We conclude that $w(x) = v(x)^e$ for all $x \in D$ with $w(x) > 1$, and taking inverses shows that it is also true for all $x \in D$ with $w(x) < 1$. The equation $w(x) = v(x)^e$ trivially holds for all remaining elements of D, so v and w are equivalent.

If $O(D,v) \subseteq O(D,w)$, let x be a non-zero element of $O(D,w)$. It is clear that $w(x^{-n}) \geq 1$ for all $n \in \mathbb{N}$. Since w is non-trivial, there exists $y \in D$ with $w(y) > 1$. We find that $w(x^{-n}y) > 1$ for all $n \in \mathbb{N}$, so $v(x^{-n}y) > 1$ for all $n \in \mathbb{N}$. This is only possible if $v(x) \leq 1$, so $x \in O(D,v)$. We conclude that $O(D,w) \subseteq O(D,v)$, so $O(D,v) = O(D,w)$.

If $P(D,v) \subseteq P(D,w)$, then

$$O(D,w)\backslash\{0_D\} = \{x \in D^\circ | \, x^{-1} \notin P(D,w)\} \subseteq \{x \in D^\circ | \, x^{-1} \notin P(D,v)\} = O(D,v)\backslash\{0_D\}$$

implies that $O(D,w)$ is a subset of $O(D,v)$, and we have just seen that this implies that $O(D,w)$ is equal to $O(D,v)$. □

We will now fulfill the promise that we would classify the valuations of $\mathbb{Q}$. We first prove a technical lemma and then move on to the classification theorem itself.

Lemma 4.11. *Let $m, n \in \mathbb{N}$ with $m > n$. Each $k \in \mathbb{N}$ can be written as $\sum_{i=0}^{r} a_i(m/n)^i$ with $r \geq 0$ and $a_i \in \{0, 1, \ldots, m-1\}$ for all i.*

Proof. Define $k_0 = k$ and use long division by m to write $k_0 = l_0 m + a_0$. For each $i \geq 1$, define $k_i = l_{i-1} n$ and use long division by m to write $k_i = l_i m + a_i$. Note that k_i and l_i are non-negative integers during this entire process and that each a_i is an element of $\{0, 1, \ldots, m-1\}$. Furthermore, $k_i > 0$ implies that $k_i = l_i m + a_i > l_i n = k_{i+1}$, and $k_i = 0$ implies that $k_{i+1} = 0$, so there exists $r \geq 0$ such that a_r is the last non-zero a_i. Unwrapping our definitions, we find that $k = \sum_{i=0}^{r} a_i(m/n)^i$. □

Theorem 4.12. *Let v be a non-trivial valuation of $\mathbb{Q}$.*

i) If v is non-archimedean, then v is equivalent to the p-adic valuation v_p for a unique prime number p. In this case $E(\mathbb{Q}, v) \cong \mathbb{Z}/p\mathbb{Z}$.

ii) If v is archimedean, then v is equivalent to the absolute value v_∞.

Proof. Suppose that v is non-archimedean. Theorem 4.6 implies that $v(m) \leq 1$ for all $m \in \mathbb{Z}$, so $\mathbb{Z}$ is a subset of $O(\mathbb{Q}, v)$. The set $\mathbb{Z} \cap P(\mathbb{Q}, v)$ is a prime ideal of $\mathbb{Z}$ by Lemma 4.9, so $\mathbb{Z} \cap P(\mathbb{Q}, v) = p\mathbb{Z}$ for some prime number p. If x is an element of $O(\mathbb{Q}, v_p)$, then x is equal to a/b for some integers $a \in \mathbb{Z} \subseteq O(\mathbb{Q}, v)$ and $b \in \mathbb{Z} \setminus p\mathbb{Z} = \mathbb{Z} \setminus P(\mathbb{Q}, v)$. In particular, we find $v(x) \leq 1$. This means that $O(\mathbb{Q}, v_p)$ is a subset of $O(\mathbb{Q}, v)$, so v is equivalent to v_p.

Since v_p is non-archimedean, it is clear that $\mathbb{Z} + P(\mathbb{Q}, v_p)$ is a subset of $O(\mathbb{Q}, v_p)$. For the proof of the opposite inclusion, note that $\gcd(b, p) = 1$ implies that there exist $c, d \in \mathbb{Z}$ such that $cb + dp = 1$. This implies that $x = a/b = ac + adp/b$ is an element of $\mathbb{Z} + P(\mathbb{Q}, v_p)$, so $O(\mathbb{Q}, v_p) = \mathbb{Z} + P(\mathbb{Q}, v_p)$. We conclude from Lemma 4.10 that

$$E(\mathbb{Q}, v) \cong E(\mathbb{Q}, v_p) = \frac{O(\mathbb{Q}, v_p)}{P(\mathbb{Q}, v_p)} = \frac{\mathbb{Z} + P(\mathbb{Q}, v_p)}{P(\mathbb{Q}, v_p)} \cong \frac{\mathbb{Z}}{\mathbb{Z} \cap P(\mathbb{Q}, v_p)} = \frac{\mathbb{Z}}{p\mathbb{Z}} = \mathbb{Z}/p\mathbb{Z}.$$

This also proves that the prime p is unique.

Suppose that v is archimedean. Corollary 4.5 implies that we may as well assume that v satisfies the triangle inequality. Lemma 4.10 implies that it is sufficient to prove that all $x \in \mathbb{Q}$ with $v(x) < 1$ satisfy $|x| < 1$. Since $v(-x) = v(x)$ and $|-x| = |x|$, we may as well assume that $x > 0$.

Suppose that $v(x) < 1$ and $x \geq 1$. It is impossible for x to be equal to 1, since $v(1) = 1$ follows from the fact that 1 is the unit element of $\mathbb{Q}$. This means that x is larger than 1, so We can uniquely write x as m/n with $m, n \in \mathbb{N}$ relatively prime and $m > n$. Lemma 4.11 implies that each $k \in \mathbb{N}$ can be written as $\sum_{i=0}^{r} a_i(m/n)^i$ with each a_i in $\{0, 1, \ldots, m-1\}$. Then

$$v(k) \leq \sum_{i=0}^{r} a_i v(m/n)^i \leq (m-1) \sum_{i=0}^{\infty} v(x)^i = \frac{m-1}{1 - v(x)}$$

implies that $v(\mathbb{N})$ is bounded, so v is non-archimedean by Theorem 4.6. This is a contradiction, so all $x \in \mathbb{Q}_{>0}$ with $v(x) < 1$ satisfy $|x| = x < 1$. □

4.2 Valuation Topology and Local Fields

In this section, we will see that a valuation v of a division ring D induces a topology on D. We will study this topology and use it to define local fields. Finally we describe some properties of local fields.

A valuation v of D that satisfies the triangle inequality defines a metric δ_v on D by $\delta_v(x, y) = v(x - y)$ for all $x, y \in D$, so v also defines a metric topology on D with a basis consisting of the neighborhoods $N(x, e, v) = \{y \in D |\ v(x - y) < e\}$ with $x \in D$ and $e \in \mathbb{R}_{>0}$. Note that for all $f \in \mathbb{R}_{>0}$, $N(x, e, v) = N(x, e^f, v^f)$, so equivalent valuations induce identical neighborhoods. In particular, the sets $N(x, e, v)$ form a basis of a metric topology even when v does not satisfy the triangle inequality, since all valuations are equivalent to a valuation that does satisfy the triangle inequality. The topology with the set $\{N(x, e, v) |\ x \in D, e \in \mathbb{R}_{>0}\}$ as basis is called the *v-topology*.

Lemma 4.13. *If v and w are valuations of a division ring D, then the v-topology and w-topology on D coincide if and only if v and w are equivalent.*

Proof. We have already noted that equivalent valuations induce the same topology. If v and w induce the same topologies, then there exists $e \in \mathbb{R}_{>0}$ such that $N(0_D, e, w)$ is a subset of $N(0_D, 1, v)$. If $x \in P(D, w)$, then there exists $n \in \mathbb{N}$ such that $w(x)^n < e$, which implies that $v(x^n) < 1$. We conclude that $x \in P(D, v)$, so $P(D, w)$ is a subset of $P(D, v)$. Lemma 4.10 implies that v and w are equivalent. □

Lemma 4.14. *Let v be a valuation of a division ring D, and let the v-topology be the topology on D. The valuation v is continuous on D. Addition and subtraction are uniformly continuous on D. Multiplication is uniformly continuous on bounded subsets of D. The inverse operation is uniformly continuous on sets that are bounded away from 0_D.*

Proof. The valuation v is continuous by definition of the v-topology. See for instance Lemma 17.4b from [Pierce, 1982, p. 322] for a proof of the other statements. □

We are now ready to define local fields. Local fields will be used extensively in the remainder of this thesis.

Definition 4.15. A field F is a *local field* if there exists a non-archimedean valuation v on F such that $O(F, v)$ is compact in the v-topology.

Note that a field F is a local field with respect to the trivial valuation if and only if F is finite.

In order to be able to characterize local fields in a more practical manner, we first introduce a related concept. A valuation v on a division ring D is called *discrete* when $v(D^\circ)$ is a cyclic subgroup of $\mathbb{R}_{>0}$. This means that v is discrete if and only if for some $z \in D^\circ$, $v(D^\circ) = \{v(z)^n |\ n \in \mathbb{Z}\}$. If this z is chosen in such a way that $v(z) < 1$, then z is called a *uniformizer* at v. An element $x \in D^\circ$ is said to have *exponential value l at v* when for a uniformizer z at v, $v(x) = v(z)^l$. Note that all valuations equivalent to a discrete valuation are discrete themselves.

We discuss a few immediate consequences of these definitions in the following lemma.

Lemma 4.16. *If v is a discrete valuation of the division ring D, then this valuation v is non-archimedean and $P(D,v) = zO(D,v) = O(D,v)z$ for all uniformizers z at v.*

Proof. Suppose that v is archimedean. Theorem 4.6 implies that all valuations of a division ring with characteristic non-zero are non-archimedean, so $\operatorname{char} D = 0$ and D contains a subfield that is isomorphic to $\mathbb{Q}$. We therefore may as well assume that $\mathbb{Q} \subseteq D$. Theorem 4.7 yields that $v|_{\mathbb{Q}}$ is also archimedean, so $v|_{\mathbb{Q}}$ is equivalent to the absolute value on $\mathbb{Q}$ by Theorem 4.12. In particular, $v(\mathbb{Q}^\circ) \subseteq v(D^\circ)$ and $v(\mathbb{Q}^\circ)$ is dense in $\mathbb{R}_{>0}$, so v is not discrete. We have proven that archimedean valuations of D are not discrete, so all discrete valuations of D are non-archimedean.

Let z be a uniformizer of the discrete valuation v of D. We will only prove that $P(D,v) = zO(D,v)$, the other equality can be proven similarly. It is immediately clear that $zO(D,v) \subseteq P(D,v)$. For the other inclusion, let x be an element of $P(D,v)$. By definition of z, $v(x) = v(z)^n$ for some $n \in \mathbb{N}$. This implies that $z^{-n}x$ is an element of $O(D,v)$, so $x = z^n(z^{-n}x)$ is an element of $z^nO(D,v) \subseteq zO(D,v)$. □

We would like to characterize the non-archimedean valuations v and division rings D such that $O(D,v)$ is compact. We are most interested in the case where D is a field, but the extra generality will be useful in later proofs. We first prove two technical lemmas.

Lemma 4.17. *If D is a division ring with a valuation v such that $O(D,v)$ is compact, then D is complete in the v-topology.*

Proof. Let $\{x_n\}_{n\in\mathbb{N}} \subseteq D$ be a Cauchy sequence. Choose $N \in \mathbb{N}$ such that $v(x_m - x_n) < 1$ for all $m, n \geq N$. The Cauchy sequence $\{x_n - x_N\}_{n\geq N}$ is a subset of the compact set $O(D,v)$, so it has a limit $y \in O(D,v)$. In this case $y + x_N \in D$ is the limit of $\{x_n\}_{n\in\mathbb{N}}$, so D is complete. □

Lemma 4.18. *Let v be a non-trivial discrete valuation of a division ring D. If z is a uniformizer at v, then $z^nO(D,v)/z^{n+1}O(D,v) \cong E(D,v)$ as abelian groups by addition for all $n \in \mathbb{N}$. In particular, if $E(D,v)$ is finite, then $|O(D,v)/z^nO(D,v)| = |E(D,v)|^n$ for all $n \in \mathbb{N}$.*

Proof. For each integer $n \in \mathbb{N}$, the map $\phi_n : z^{n-1}O(D,v) \to z^nO(D,v)$ defined by $x \mapsto zx$ is a surjective group homomorphism with $\phi_n^{-1}(z^{n+1}O(D,v)) = z^nO(D,v)$, so

$$\frac{z^nO(D,v)}{z^{n+1}O(D,v)} \cong \frac{z^{n-1}O(D,v)}{z^nO(D,v)} \cong \ldots \cong \frac{zO(D,v)}{z^2O(D,v)} \cong \frac{O(D,v)}{zO(D,v)} = E(D,v).$$

□

Theorem 4.19. *Let v be a non-archimedean valuation of a division ring D and let the v-topology be the topology on D. The set $O(D,v)$ is compact if and only if v is discrete, D is complete and $E(D,v)$ is finite.*

Proof. If v is trivial, then v is discrete and D is complete. Furthermore, $D = O(D,v)$ is compact if and only if $E(D,v) \cong D$ is finite, so the theorem holds. For the remainder of the proof, we will assume that v is non-trivial.

First assume that $O(D,v)$ is compact. Lemma 4.17 implies that D is complete. Let X be a set of representatives of the equivalence classes in $E(D,v)$. It is clear that $O(D,v) = \bigcup_{x\in X}(x + P(D,v))$, that $(x + P(D,v)) \cap (y + P(D,v)) = \emptyset$ for all $x, y \in X$ with $x \neq y$, and that each set $x + P(D,v)$ is open in the v-topology. The compactness of $O(D,v)$ implies that X is finite, so $E(D,v)$ is finite as well. Since the sets $x + P(D,v)$ are open in D, $P(D,v) = O(D,v) \setminus \bigcup_{x\in X\setminus P(D,v)}(x + P(D,v))$ is closed in $O(D,v)$. In particular, $P(D,v)$ is compact. This implies that the supremum $\sup\{v(x)|\ x \in P(D,v)\}$ is attained in some $z \in P(D,v)$, and this z satisfies $0 \leq v(x) \leq v(z) < 1$ for all $x \in P(D,v)$. We will prove that $v(D^\circ)$ is equal to $\{v(z)^n|\ n \in \mathbb{Z}\}$, which would imply that v is discrete.

For all non-zero $x \in P(D,v)$ there exists $n \in \mathbb{N}$ such that $v(z)^{n+1} < v(x) \leq v(z)^n$. We conclude that $v(z) < v(xz^{-n}) \leq 1$, and $xz^{-n} \in P(D,v)$ would contradict the definition of z, so $v(xz^{-n})$ is equal to 1. We conclude that $v(x) = v(z)^n$, which means that $v(P(D,v) \setminus \{0_D\})$ is a subset of $\{v(z)^n|\ n \in \mathbb{N}\}$. For all $y \in D^\circ$ there exists $m \in \mathbb{N}$ such that $v(yz^m) < 1$, so $v(yz^m) = v(z)^n$ for some $n \in \mathbb{N}$. This implies that $v(y)$ is an element of $\{v(z)^n|\ n \in \mathbb{Z}\}$ for all $y \in D^\circ$, so $v(D^\circ) \subseteq \{v(z)^n|\ n \in \mathbb{Z}\}$. The opposite inclusion is obvious, so v is discrete with uniformizer z.

Now assume that v is discrete, D is complete and $E(D,v)$ is finite. Since $O(D,v)$ is a closed subset of D, $O(D,v)$ is complete as well. If we can prove that $O(D,v)$ is totally bounded, then we can conclude that $O(D,v)$ is compact, since it is well-known from topology that all complete, totally bounded metric spaces are compact. By definition, the set $O(D,v)$ is *totally bounded* when for all $e \in \mathbb{R}_{>0}$, $O(D,v)$ is a finite union of sets with diameter less than e.

Let $e \in \mathbb{R}_{>0}$, and suppose that z is a uniformizer at v. Let n be a natural number such that $v(z)^n < e$, and consider the sets $x + z^n O(D,v)$ with $x \in O(D,v)$. For $p, q \in O(D,v)$ the inequality $v(x + z^n p - (x + z^n q)) = v(z)^n v(p - q) < e$ follows from the fact that $p - q \in O(D,v)$ by Lemma 4.9. This implies that the set $x + z^n O(D,v)$ has diameter less than e for all $x \in O(D,v)$. Lemma 4.18 implies that $O(D,v)/z^n O(D,v)$ is finite if v is non-trivial, so $O(D,v)$ is covered by finitely many sets of the form $x + z^n O(D,v)$ with $x \in O(D,v)$. In other words, $O(D,v)$ is totally bounded. □

Corollary 4.20. *Let v be a non-archimedean valuation of a division ring D. Any two of the following three properties imply the third:*

i) $O(D,v)$ is compact in the v-topology.

ii) D is finite.

iii) v is trivial.

Proof. If v is trivial, then $D = O(D,v)$ implies that $O(D,v)$ is compact if and only if D is finite. If D is finite and $O(D,v)$ is compact, then Theorem 4.19 implies that v is discrete. Since D is finite, this is only possible if v is trivial. □

One consequence of this corollary is that if F is a local field with respect to a valuation v, then F is finite if and only if v is trivial. We will use the term *infinite local field* to refer to local fields that contain infinitely many elements.

Corollary 4.21. *If F is an infinite local field with respect to the valuation v and z is a uniformizer at v, then every proper, non-trivial ideal of $O(F,v)$ is equal to $z^nO(F,v)$ for some $n \in \mathbb{N}$. In particular, $O(F,v)$ is a principal ideal domain.*

Proof. Suppose that I is a non-trivial ideal of $O(F,v)$. The supremum $\sup\{v(a)|\ a \in I\}$ is attained in some $b \in F$, since $v(I)$ is a subset of $\{v(z)^n|\ n \geq 0\}$. If $n \geq 0$ satisfies $v(b) = v(z)^n$, then $I \subseteq z^nO(F,v)$. For any $c \in z^nO(F,v)$, $v(c) \leq v(z)^n = v(b)$, so $b^{-1}c$ is an element of $O(F,v)$. We conclude that $c = b(b^{-1}c)$ is an element of I, so $I = z^nO(F,v)$. The ideal $z^nO(F,v)$ contains 1_F precisely when $n = 0$, so all proper, non-trivial ideals of $O(F,v)$ are equal to $z^nO(F,v)$ for some $n \in \mathbb{N}$. □

We would also like to describe the close relation between the compactness of $O(D,v)$ and local compactness of D. A topological space is *locally compact* when every point in that space has a compact neighborhood. In particular, D is locally compact in the v-topology if for every $x \in D$, there exists $e \in \mathbb{R}_{>0}$ such that the closed ball $\overline{N}(x,e,v) = \{y \in D|\ v(x-y) \leq e\}$ is compact.

Theorem 4.22. *Let v be a valuation of a division ring D, and let the v-topology be the topology on D.*

i) If $O(D,v)$ is compact, then D is locally compact.

ii) If D is locally compact, then v is trivial or $O(D,v)$ is compact.

iii) If v is trivial, then D is locally compact.

Proof. If $O(D,v)$ is compact, then the continuity of addition implies that $x + O(D,v)$ is compact for all $x \in D$. The equality $x + O(D,v) = \overline{N}(x,1,v)$ then yields that D is locally compact.

If D is locally compact and v is non-trivial, then there exists $e \in \mathbb{R}_{>0}$ such that $\overline{N}(0_D,e,v)$ is compact. Since v is non-trivial, there exists $y \in D^\circ$ such that $v(y) < 1$. For $n \in \mathbb{N}$ with $v(y)^n < e$, $y^nO(D,v) = \overline{N}(0_D,v(y)^n,v)$ is a closed subset of $\overline{N}(0_D,e,v)$, so it is compact. Since multiplication in D is continuous, $O(D,v) = y^{-n}(y^nO(D,v))$ is compact as well.

If v is trivial, then $\overline{N}(x,1/2,v) = \{x\}$ is a compact neighborhood of $x \in D$. □

4.3 Completions of Division Rings

If v is a valuation of a division ring D, then D is not necessarily complete in the v-topology. However, we can construct a larger division ring $\hat{D}_v$ and an extension $\hat{v}$ of v to $\hat{D}_v$ such that D is dense in $\hat{D}_v$ and $\hat{D}_v$ is complete in the $\hat{v}$-topology.

Theorem 4.23. *Let v be a valuation of the division ring D. There exists a division ring $\hat{D}_v$ that contains D as a subring, and a valuation $\hat{v}$ of $\hat{D}_v$ such that:*

i) $\hat{D}_v$ is complete in the $\hat{v}$-topology;

ii) D is dense in $\hat{D}_v$;

iii) $\hat{v}|_D = v$;

iv) $a(\hat{v}) = a(v)$;

v) if v is non-archimedean, then $\hat{v}(\hat{D}_v^\circ) = v(D^\circ)$;

vi) if D is a field, then so is $\hat{D}_v$.

The division ring $\hat{D}_v$ that satisfies properties i), ii) and iii) is unique up to an isometric isomorphism that is the identity on D.

Proof. First assume that v satisfies the triangle inequality. We will later generalize our results to v that do not satisfy this inequality. Let $\hat{D}_v$ be the metric space completion of D with respect to the metric δ_v. We first prove that $\hat{D}_v$ is a division ring that contains D. We then define $\hat{v}$ and derive the six statements of the theorem.

The uniform continuity of the ring operations implies that these operations uniquely extend to $\hat{D}_v$. For instance, for $\hat{x}, \hat{y} \in \hat{D}_v$, there exist Cauchy sequences $\{x_n\}_{n\in\mathbb{N}}$ and $\{y_n\}_{n\in\mathbb{N}}$ in D such that $\lim_{n\to\infty} x_n = \hat{x}$ and $\lim_{n\to\infty} y_n = \hat{y}$ in $\hat{D}_v$. These sequences are bounded, so $\{x_n y_n\}_{n\in\mathbb{N}}$ is a Cauchy sequence with some limit in $\hat{D}_v$. This limit does not depend on the choice of Cauchy sequences $\{x_n\}_{n\in\mathbb{N}}$ and $\{y_n\}_{n\in\mathbb{N}}$, so we can define $\hat{x}\hat{y} = \lim_{n\to\infty} x_n y_n$. Addition, subtraction and the inverse operation can be extended to $\hat{D}_v$ in a similar way, and the fact that they satisfy the identities that identify $\hat{D}_v$ as a division ring can be derived from the corresponding identities in D. If D is a field, then $\hat{D}_v$ is a field as well for analogous reasons. The fact that $x \in D$ is the limit of the Cauchy sequence $\{x\}_{n\in\mathbb{N}}$ proves that D is a dense subring of $\hat{D}_v$.

If $\hat{\delta}$ is the induced metric on $\hat{D}_v$, then define $\hat{v} : \hat{D}_v \to \mathbb{R}$ as $\hat{v}(\hat{x}) = \hat{\delta}(\hat{x}, 0_D)$ for all $\hat{x} \in \hat{D}_v$. It is clear that $\hat{v}$ is a valuation of $\hat{D}_v$ with $\hat{v}|_D = v$, and that $\hat{\delta}$ is the distance function induced by $\hat{v}$. In particular, $\hat{v}$ is continuous and $\hat{D}_v$ is complete in the $\hat{v}$-topology. Since D is dense in $\hat{D}_v$, $a(\hat{v}) = a(v)$ follows directly from the continuity of $\hat{v}$. If v is non-archimedean, then $a(\hat{v}) = a(v) = 1$ and for all $\hat{x} \in \hat{D}_v^\circ$ there exists $x \in D^\circ$ such that $\hat{v}(\hat{x} - x) < \hat{v}(\hat{x})$, since D is dense in $\hat{D}_v$. The Domination Principle then implies that $\hat{v}(\hat{x}) = \hat{v}(\hat{x} - (\hat{x} - x)) = \hat{v}(x) = v(x)$, so $\hat{v}(\hat{D}_v^\circ) = v(D^\circ)$.

If v does not satisfy the triangle inequality, then $w = v^e$ satisfies the triangle inequality for some $e \in \mathbb{R}_{>0}$. We can simply define $\hat{D}_v = \hat{D}_w$ and $\hat{v} = \hat{w}^{1/e}$, and properties *i)* to *vi)* for the valuation v follow from their equivalents for w.

We note that, when two division rings D_1 and D_2 are equipped with valuations v and w, respectively, then a homomorphism $\phi : D_1 \to D_2$ is isometric with respect to the respective valuation topologies precisely when $w(\phi(x))$ is equal to $v(x)$ for all $x \in D_1$. The uniqueness of the division ring $\hat{D}_v$ with properties *i)*, *ii)* and *iii)* therefore follows directly from the continuity statements in Lemma 4.14 and assumption *ii)* □

The division ring $\hat{D}_v$ is called the *completion of D in the v-topology*. The valuation that extends v to $\hat{D}_v$ will usually be denoted by v as well.

Corollary 4.24. *Let D be a division ring with a valuation v such that D is complete in the v-topology. If C is a subring of D, then the closure of C in D is isometrically isomorphic to $\hat{C}_v$.*

Proof. The closure of C in D is a division ring that is complete in the v-topology and it contains C as a dense subring, so this corollary follows from the uniqueness statement in Theorem 4.23. □

Corollary 4.25. *If v is a non-archimedean valuation of the division ring D, then $O(\hat{D}_v, v) = O(D, v) + P(\hat{D}_v, v)$ and $P(D, v) = O(D, v) \cap P(\hat{D}_v, v)$. Thus, the inclusion map $O(D, v) \to O(\hat{D}_v, v)$ induces an isomorphism from $E(D, v)$ to $E(\hat{D}_v, v)$.*

Proof. The only part of this proof that is not straightforward is the proof that $O(\hat{D}_v, v)$ is a subset of $O(D, v) + P(\hat{D}_v, v)$, so that is the only part that we discuss here. See for instance the proof of Corollary 17.4b from [Pierce, 1982] for more details.

Suppose that $\hat{x} \in O(\hat{D}_v, v)$ is non-zero. Since D is dense in $\hat{D}_v$, there exists $x \in D$ such that $v(\hat{x} - x) < v(\hat{x}) \leq 1$. The Domination Principle yields that $v(x) = v(\hat{x}) \leq 1$, so $\hat{x} = x + (\hat{x} - x)$ is an element of the set $O(D, v) + P(\hat{D}_v, v)$. □

As an example, consider the various completions of the field $\mathbb{Q}$. For the absolute value v_∞ of $\mathbb{Q}$, the completion of $\mathbb{Q}$ in the v_∞-topology is $\mathbb{R}$. Indeed, $\mathbb{Q}$ is dense in $\mathbb{R}$, $v_\infty^{\mathbb{Q}}$ is equal to $v_\infty^{\mathbb{R}}|_{\mathbb{Q}}$ and $\mathbb{R}$ is complete in the $v_\infty^{\mathbb{R}}$-topology. For any prime number p, the completion of $\mathbb{Q}$ in the v_p-topology is called the *field of p-adic numbers*, notation $\hat{\mathbb{Q}}_p$.

Corollary 4.26. *For any prime number p, $\hat{\mathbb{Q}}_p$ is a local field.*

Proof. If we can prove that v_p is discrete on $\hat{\mathbb{Q}}_p$, $\hat{\mathbb{Q}}_p$ is complete in the v_p-topology and $E(\hat{\mathbb{Q}}_p, v_p)$ is finite, then Theorem 4.19 implies that $\hat{\mathbb{Q}}_p$ is a local field. Since $v_p|_{\mathbb{Q}}$ is a non-archimedean valuation, Theorem 4.23 implies that v_p is discrete, and that $\hat{\mathbb{Q}}_p$ is complete in the v_p-topology. Theorem 4.12 and Corollary 4.25 together imply that $E(\hat{\mathbb{Q}}_p, v_p) \cong \mathbb{Z}/p\mathbb{Z}$, so $E(\hat{\mathbb{Q}}_p, v_p)$ is finite. □

The following theorem gives a useful description of the elements of $\hat{\mathbb{Q}}_p$.

Theorem 4.27. *Every $x \in \hat{\mathbb{Q}}_p^\circ$ has a unique* p-adic expansion $x = \sum_{i=m}^{\infty} a_i p^i$ *with $m \in \mathbb{Z}$, $a_i \in \{0, 1, \ldots, p-1\}$ for all $i \geq m$ and $a_m \neq 0$.*

Proof. See for instance Proposition F9 from Chapter 23 of [Lorenz, 2008]. □

Note that if $x \in \hat{\mathbb{Q}}_p^\circ$ has the p-adic expansion $\sum_{k=m}^{\infty} a_k p^k$, then $v_p(x)$ is equal to p^{-m}.

One might wonder why we are so interested in complete division rings in the first place. Part of the reason is that we will need them to determine the Brauer group of algebraic number fields. Another part is that complete division algebras have some interesting properties. One of these properties is described in Hensel's Lemma.

Theorem 4.28 (Hensel's Lemma)**.** *Let D be a division algebra over a field F, and suppose that D is complete in the v-topology for some non-archimedean valuation v of D. If $\Phi \in O(F, v)[\mathbf{x}]$ is such that $\overline{\Phi}$ and $\overline{\Phi}'$ are relatively prime in $E(F, v)[\mathbf{x}]$, then for any root $\overline{x} \in E(D, v)$ of $\overline{\Phi}$, there exists $y \in O(D, v)$ such that y is a root of Φ and $\overline{y} = \overline{x}$.*

Proof. See for instance [Pierce, 1982, p. 324] for a proof of this theorem. □

This is only one specific form of Hensel's Lemma. See for instance Subsection 4.1.7 of [Cohen, 2008] for more general forms of this famous lemma.

4.4 Division Algebras over Locally Compact Fields

In this section, we discuss extensions of a valuation v of F such that F is locally compact in the v-topology to a division algebra D that is finite-dimensional over F. To do this, we first briefly discuss the concept of the uniform topology and the concept of the reduced norm. We then use these concepts to sketch a proof of the main theorem of this section.

Lemma 4.29. *Suppose that v is a valuation of F that satisfies the triangle inequality, and suppose that M is a finite-dimensional F-space with the basis $x_1, \ldots, x_n$. If the map $x \mapsto ||x||_v$ from M to $\mathbb{R}$ is defined as $||x_1a_1 + \ldots x_na_n||_v = \max\{v(a_i)|\ i = 1, \ldots, n\}$ for all $a_1, \ldots, a_n \in F$, then*

i) $||x||_v \geq 0$ *for all* $x \in M$.

ii) $||x||_v = 0$ *if and only if* $x = 0_M$.

iii) $||x + y||_v \leq ||x||_v + ||y||_v$ *for all* $x, y \in M$.

iv) $||xa||_v = ||x||_v v(a)$ *for all* $x \in M$ *and* $a \in F$.

Proof. This lemma follows directly from the known properties of valuations. □

The mapping $x \mapsto ||x||_v$ is called the *uniform v-norm* on M relative to the basis $x_1, \ldots, x_n$. The metric $(x, y) \mapsto ||x - y||_v$ induces a topology on M that is called the *uniform v-topology* on M.

Lemma 4.30. *Suppose that D is a finite-dimensional division algebra over F, where F is a local field with respect to a valuation v of F that satisfies the triangle inequality.*

i) The uniform v-topology on D is independent of the choice of F-basis of D.

ii) If w extends v to D, then the w-topology is equal to the uniform v-topology on D.

Proof. This is a consequence of Lemma 17.6b and part of the proof of Proposition 17.6 from [Pierce, 1982]. □

In particular, part *ii*) of this lemma implies that all extensions w of v induce the same topology on D. Lemma 4.13 now implies that all extensions of v to D are equivalent. If v is non-trivial, then this means that there exists at most one extension of v to D. Does such an extension always exist? Yes, but in order to construct it we will need to make use of the reduced norm.

Lemma 4.31. *For any $A \in \mathbf{CSA}(F)$, there exists a function $\boldsymbol{\nu}_{A/F} : A \to F$ called the* reduced norm. *We list two of its properties:*

i) $\boldsymbol{\nu}_{A/F}(xy) = \boldsymbol{\nu}_{A/F}(x)\boldsymbol{\nu}_{A/F}(y)$ *for all* $x, y \in A$;

ii) $\boldsymbol{\nu}_{A/F}(a) = a^{\deg A}$ *for all* $a \in F$.

Proof. This lemma is a consequence of Definition 16.1, Proposition 16.1 and Lemma 16.3a from [Pierce, 1982]. □

We are now ready for the main theorem of this section.

Theorem 4.32. *Let D be a finite-dimensional division algebra over the field F, where F is locally compact with respect to the non-trivial valuation v.*

i) v extends uniquely to a valuation w on D.

ii) $O(D, w)$ is compact in the w-topology.

iii) If v is discrete, then so is w and $[w(D^\circ) : v(F^\circ)]$ divides $[\mathbf{Z}(D) : F](\operatorname{Deg} D)$, where $\operatorname{Deg} D$ is the degree of D as an element of $\mathbf{CSA}(\mathbf{Z}(D))$.

Proof. We will merely sketch the proof of this theorem, and will refer to the proof of Proposition 17.6 in [Pierce, 1982] for the remaining details.

We can assume without loss of generality that v satisfies the triangle inequality, since all valuations are equivalent to such a valuation and the properties in the theorem are invariant under equivalence of valuations.

For convenience, we define $K = \mathbf{Z}(D)$. Since all division algebras are simple, D is an element of $\mathbf{CSA}(K)$, so the degree $\operatorname{Deg} D$ and the reduced norm $\boldsymbol{\nu}_{D/K}$ are well-defined. Denote $m = [K : F](\operatorname{Deg} D)$, and define $w : D \to \mathbb{R}$ by

$$w(x) = v\left(N_{K/F}\left(\boldsymbol{\nu}_{D/K}(x)\right)\right)^{1/m}$$

for all $x \in D$. It is clear that $w(xy) = w(x)w(y)$ for all $x, y \in D$, and for $a \in F$ we find

$$w(a) = v\left(N_{K/F}\left(\boldsymbol{\nu}_{D/K}(a)\right)\right)^{1/m} = v\left(N_{K/F}\left(a^{\operatorname{Deg} D}\right)\right)^{1/m} = v(a^{[K:F](\operatorname{Deg} D)})^{1/m} = v(a),$$

so if w is a valuation, then w extends v. We refer to the proof of Proposition 17.6 in [Pierce, 1982] for the proof that w satisfies the other properties of a valuation.

Note that F is by assumption locally compact in the v-topology. By definition of the uniform v-topology, D is homeomorphic to a finite product of copies of F with the v-topology, so D is locally compact in the uniform v-topology. This means that D is locally compact in the w-topology, so $O(D, w)$ is compact by Theorems 4.7 and 4.22.

Suppose that v is discrete. By definition of w, $w(x) \mapsto w(x)^m$ is an injective group homomorphism from $w(D^\circ)$ to $v(F^\circ)$. We conclude that w is discrete and that the degree $[w(D^\circ) : v(F^\circ)]$ divides $m = [\mathbf{Z}(D) : F] \operatorname{Deg} D$. □

Since the extension of v to D is unique, we will use v to refer to both the original valuation and the extension to D.

Corollary 4.33. *If K/F is a finite Galois extension of local fields with respect to the valuation v of K and $\sigma \in \mathbf{G}(K/F)$, then $v(y^\sigma) = v(y)$ for all $y \in K$.*

Proof. If v is trivial, then this is obvious. If v is non-trivial, then the map $w : K \to \mathbb{R}$ defined as $w(y) = v(y^\sigma)$ for all $y \in K$ is a valuation of K such that $w|_F = v|_F$, so part $i)$ of Theorem 4.32 implies that $v^\sigma = v$. □

The following corollary is trivial in the finite case and a direct consequence of parts *i)* and *ii)* of Theorem 4.32 in the infinite case.

Corollary 4.34. *If F is a local field and K/F is a finite field extension, then K is a local field.*

4.5 Ramification Index and Relative Degree

Let v be a discrete valuation of a division ring D, and suppose that K is a subfield of D. In this section we define the ramification index $e(D/K)$(or $e_v(D/K)$) of K in D and the relative degree $f(D/K)$(or $f_v(D/K)$) of D/K. We then study some of the properties of $e(D/F)$ and $f(D/F)$ when F is a local field and D is a finite-dimensional division algebra over F.

Let v, D and K have the properties described in the previous paragraph. If $v|_K$ is non-trivial, then $v(K^\circ)$ is a subgroup of $v(D^\circ)$ of finite index. The order of the group $v(D^\circ)/v(K^\circ)$ is called the *ramificiation index of K in D at v*, and is denoted by either $e(D/K)$ or $e_v(D/K)$. A field extension K/F is called *unramified* with respect to a discrete valuation v of K when $e_v(K/F)$ is equal to 1.

Let $\pi : O(D,v) \to E(D,v)$ be the natural projection map. The restriction $\pi|_{O(K,v)}$ has the property that $\operatorname{Ker}\pi|_{O(K,v)} = K \cap P(D,v) = P(K,v)$. This implies that the inclusion homomorphism $O(K,v) \to O(D,v)$ induces an injective ring homomorphism $E(K,v) \to E(D,v)$. This allows us to identify $E(K,v)$ with a subfield of $E(D,v)$, and we will often do so. Furthermore, $E(D,v)$ can be viewed as a vector space over $E(K,v)$. The dimension of $E(D,v)$ over $E(K,v)$ is called the *relative degree of D/K at v*, denoted by $f(D/K)$ or $f_v(D/K)$.

Lemma 4.35. *Let D be a division ring with subfields K and F such that $F \subseteq K \subseteq D$. Suppose that w is a discrete valuation of D and $v = w|_K$.*

i) $e_w(D/F) = e_w(D/K)e_v(K/F)$.

ii) $f_w(D/F) = f_w(D/K)f_v(K/F)$.

Proof. These formulas follow directly from the definitions. □

We first study some properties of $e_v(D/F)$ and $f_v(D/F)$ when D is a finite-dimensional division algebra over F and v is a non-trivial discrete valuation of D.

Theorem 4.36. *If v is a non-trivial discrete valuation of a finite-dimensional division algebra D over F, then $e_v(D/F)f_v(D/F) \leq \dim_F D$.*

Proof. Define $e = e_v(D/F)$. If $z \in P(D,v)$ and $c \in P(F,v)$ are uniformizers at v and $v|_F$, respectively, then $v(z)^e = v(c)$, $P(D,v) = zO(D,v)$ by Lemma 4.16, and $P(F,v) = cO(F,v) = z^eO(D,v) \cap O(F,v)$ by the definition of the ramification index and Lemma 4.16. If $\pi : O(D,v) \to O(D,v)/z^eO(D,v)$ is the projection map, then

$$\pi\left(O(F,v)\right) = \frac{O(F,v)}{z^eO(D,v)} \cong \frac{O(F,v)}{z^eO(D,v) \cap O(F,v)} = \frac{O(F,v)}{P(F,v)} = E(F,v),$$

and therefore $O(D,v)/z^eO(D,v)$ is a $\pi\left(O(F,v)\right)$-space. We find that

$$e_v(D/F)f_v(D/F) = e\dim_{E(F,v)} E(D,v) = \dim_{\pi(O(F,v))} \frac{O(D,v)}{z^eO(D,v)} \leq \dim_F D,$$

where the second equality follows from Lemma 4.18, and the inequality follows from the fact that any elements $x_1,\ldots,x_r$ of $O(D,v)$ with $\pi(x_1),\ldots,\pi(x_r)$ linearly independent over $\pi(O(F,v))$ are also linearly independent over F. □

If the field F is also a local field with respect to v, then the ramification index and relative degree are even more well-behaved.

Lemma 4.37. *Let v be a discrete valuation of the division algebra D over F. Suppose that K is a subfield of D such that $v|_K$ is non-trivial and $f(D/K) = 1$. If $z \in P(D,v)$ is a uniformizer at v and $e = e_v(D/K)$, then as a K-space $D_K = K + zK + \ldots + z^{e-1}K$. In particular,* $\dim_F D \leq e_v(D/K)[K:F]$.

Proof. This lemma follows from a combination of Lemma 17.7b and part of the proof of Proposition 17.7 from [Pierce, 1982]. The dimension inequality follows from the fact that $\dim_F D = (\dim_K D_K)(\dim_F K) \leq e(D/K)[K:F]$. □

Theorem 4.38. *Let D be a finite-dimensional division algebra over F, and suppose that v is a non-trivial discrete valuation of D such that F is a local field with respect to $v|_F$.*

i) D contains a subfield K such that K/F is unramified and $f_v(D/K) = 1$.

ii) $e_v(D/F)f_v(D/F) = \dim_F D$.

iii) If $F = \mathbf{Z}(D)$, then $e_v(D/F) = f_v(D/F)$ and K is a strictly maximal subfield of D.

Proof. Theorem 4.32 states that $O(D,v)$ is compact in the v-topology, so Theorem 4.19 yields that D is complete in the v-topology and that $E(D,v)$ and $E(F,v)$ are both finite fields. Since the multiplicative groups of finite fields are cyclic, the fact that $E(F,v)$ is a subfield of $E(D,v)$ implies that there exists $\overline{x} \in E(D,v)$ and a monic polynomial $\Phi \in O(F,v)[\mathbf{x}]$ of degree $f_v(D/F) = \dim_{E(F,v)} E(D,v)$ such that $E(D,v)$ is equal to $E(F,v)(\overline{x})$ and $\overline{\Phi} \in E(F,v)[\mathbf{x}]$ is the minimal polynomial of $\overline{x}$.

Note that $O(F,v)$ is a principal ideal domain by Corollary 4.21. The polynomial Φ is irreducible over F, since else we could apply Gauss's Lemma to the principal ideal domain $O(F,v)$ to find non-constant monic $\Theta, \Psi \in O(F,v)[\mathbf{x}]$ such that $\Phi = \Theta\Psi$. This would however imply that $\overline{\Phi} = \overline{\Theta\Psi}$ with $\overline{\Theta}$ and $\overline{\Psi}$ non-constant polynomials in $E(F,v)[\mathbf{x}]$, contradicting the fact that $\overline{\Phi}$ is irreducible.

The fact that $\overline{\Phi}$ is an irreducible polynomial over the finite field $E(F,v)$ implies that $\overline{\Phi}$ is a separable polynomial, so $\overline{\Phi}$ and $\overline{\Phi}'$ are relatively prime. Since D is complete in the v-topology, Hensel's Lemma implies the existence of some $y \in O(D,v)$ such that $\Phi(y) = 0_F$ and $\overline{y} = \overline{x}$. If we define $K = F(y)$, then K is a subfield of D with $[K:F] = \deg\Phi = f_v(D/F)$ and $E(K,v) = E(F,v)(\overline{y}) = E(D,v)$, so $f_v(D/K) = 1$. Theorem 4.36 and Lemma 4.37 now imply that

$$\dim_F D \leq e_v(D/K)[K:F] = e_v(D/K)f_v(D/F) \leq e_v(D/F)f_v(D/F) \leq \dim_F D.$$

We conclude that $e_v(D/F)f_v(D/F) = \dim_F D$ and $e_v(D/K) = e_v(D/F)$. The equality $e_v(D/K) = e_v(D/F)$ implies that $e_v(K/F) = 1$, so K/F is unramified.

If $F = \mathbf{Z}(D)$, then part *iii*) of Theorem 4.32 implies that $e_v(D/F) \leq \operatorname{Deg} D$, and $f_v(D/F) = [K : F] \leq \operatorname{Deg} D$ by Corollary 3.5, since K is a subfield of D. The equality $e_v(D/F)f_v(D/F) = \dim_F D = (\operatorname{Deg} D)^2$ then implies that

$$e_v(D/F) = f_v(D/F) = [K : F] = \operatorname{Deg} D,$$

so $e_v(D/F) = f_v(D/F)$ and K is a strictly maximal subfield of D. □

The following corollary connects the results of this theorem to the central simple algebras over a local field.

Corollary 4.39. *Let F be an infinite local field. Any division algebra $D \in \mathbf{CSA}(F)$ contains a maximal subfield K such that K is unramified.*

Corollary 3.16 states that $\mathbf{B}(F)$ is equal to the union of all relative Brauer groups $\mathbf{B}(E/F)$, with E ranging over all finite Galois extensions of F. When F is an infinite local field, we now find a similar statement for unramified extensions.

Corollary 4.40. *Let F be an infinite local field. The Brauer group $\mathbf{B}(F)$ is equal to the union of relative Brauer groups $\mathbf{B}(K/F)$ with K/F ranging over the finite, unramified extensions of F.*

Proof. The union of the relative Brauer groups $\mathbf{B}(K/F)$ is by definition a subset of $\mathbf{B}(F)$. For the proof in the opposite direction, let $[A]$ be an element of $\mathbf{B}(F)$. Theorem 2.35 implies that there exists a division algebra $D \in \mathbf{CSA}(F)$ with $D \sim A$. Corollary 4.39 states that D contains a maximal subfield K such that K/F is unramified, and this field K splits D by Theorem 3.11, so $[A] = [D]$ is an element of $\mathbf{B}(K/F)$ with K/F unramified and $[K : F] \leq \operatorname{Deg} D < \infty$. □

4.6 Unramified Extensions of Infinite Local Fields

In light of Corollary 4.40, we will take some time to study the unramified extension of infinite local fields in more detail. We find a characterization of these extensions and prove that they are cyclic. We then use this new knowledge to prove that the relative Brauer groups of these extensions are finite cyclic groups.

It is convenient to introduce some shortened notation for the next few sections. If K/F is a finite field extension of degree n with K and F local fields relative to the non-trivial valuation v, then let $\overline{K}$ and $\overline{F}$ be alternate notation for $E(K, v)$ and $E(F, v)$, respectively. The fields $\overline{K}$ and $\overline{F}$ are finite, since K and F are local fields. Let q denote the order of the field $\overline{F}$. Note that $q > 1$, since v is non-trivial and discrete.

We first prove a small lemma and then move on to a theorem that characterizes unramified extensions of local fields in several useful ways.

Lemma 4.41. *Suppose that K/F is a finite Galois extension such that K and F are local fields with respect to a non-trivial valuation v. There exists a group homomorphism $\phi : \mathbf{G}(K/F) \to \mathbf{G}(\overline{K}/\overline{F})$ such that $\overline{y^\sigma} = \overline{y}^{\phi(\sigma)}$ for all $y \in O(K,v)$ and $\sigma \in \mathbf{G}(K/F)$.*

Proof. For $\sigma \in \mathbf{G}(K/F)$, Corollary 4.33 implies that $\sigma(O(K,v)) = O(K,v)$ and that $\sigma(P(K,v)) = P(K,v)$, so σ induces an automorphism $\phi(\sigma)$ on $\overline{K} = O(K,v)/P(K,v)$ with $\overline{y}^{\phi(\sigma)} = \overline{y^\sigma}$ for all $y \in O(K,v)$. It is clear that $\overline{b}^{\phi(\sigma)} = \overline{b^\sigma} = \overline{b}$ and $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$ for all $b \in O(F,v)$ and $\sigma, \tau \in \mathbf{G}(K/F)$, so ϕ defines a group homomorphism from $\mathbf{G}(K/F)$ to $\mathbf{G}(\overline{K}/\overline{F})$. □

Note that the *splitting field of a polynomial* $\Phi \in F[\mathbf{x}]$ is the smallest field extension K of F such that Φ splits into linear factors over K. An finite extension E/F is Galois if and only if E is the splitting field of a separable polynomial in $F[\mathbf{x}]$.

Theorem 4.42. *Suppose that K/F is a field extension of degree n such that K and F are local fields with respect to the non-trivial valuation v. The following properties of K/F are equivalent.*

i) K is the splitting field over F of the polynomial $\mathbf{x}^{q^n-1} - 1_F$.

ii) K/F is finite and Galois, and the homomorphism $\phi : \mathbf{G}(K/F) \to \mathbf{G}(\overline{K}/\overline{F})$ in Lemma 4.41 is an isomorphism.

iii) K/F is unramified.

Proof. The proof of this theorem is quite technical and of little interest to us, so we refer to the proof of Proposition 17.8 from [Pierce, 1982]. □

The following corollary fully describes the unramified field extensions of a local field.

Corollary 4.43. *Let F be an infinite local field and suppose that F^{alg} is an algebraic closure of F. For each $n \in \mathbb{N}$ there exists a unique field K between F and F^{alg} with $[K : F] = n$ such that K/F is unramified and separable.*

This corollary follows directly from Theorem 4.42. Note that a local field is infinite precisely when it is local with respect to a non-trivial valuation. For any infinite local field F and $n \in \mathbb{N}$, let $K_n(F)$ denote the unique field between F and F^{alg} such that $K_n(F)$ is an unramified, separable extension of degree n. Determining whether $K_n(F)$ is a subfield of $K_m(F)$ for natural numbers n and m is quite easy.

Corollary 4.44. *For any infinite local field F, $\mathbf{B}(F) = \bigcup_{n\in\mathbb{N}} \mathbf{B}(K_n(F)/F)$.*

Proof. Let F be an infinite local field. Corollary 4.40 states that $\mathbf{B}(F)$ is equal to the union of the relative Brauer groups $\mathbf{B}(K/F)$ with K/F ranging over the finite, unramified field extensions of F. Theorem 4.42 implies that all finite, unramified field extensions of F are Galois, so they are separable as well. Corollary 4.43 then yields that the extensions $K_n(F)/F$ with $n \in \mathbb{N}$ are precisely the finite, unramified extensions of F. We conclude that $\mathbf{B}(F)$ is equal to the union $\bigcup_{n\in\mathbb{N}} \mathbf{B}(K_n(F)/F)$. □

This subdivision of $\mathbf{B}(F)$ will be used to describe the Brauer group of an infinite local field in Theorem 4.51.

Corollary 4.45. *If $m, n \in \mathbb{N}$, then $K_n(F)$ is a subfield of $K_m(F)$ if and only if $n|m$, and $[K_m(F) : K_n(F)]$ is equal to m/n in this case.*

Proof. Part *i)* of Theorem 4.42 implies that $K_n(F)$ and $K_m(F)$ are splitting fields over F of $\mathbf{x}^{q^n-1} - 1$ and $\mathbf{x}^{q^m-1} - 1$, respectively. If $n|m$, then $q^n - 1$ clearly divides $q^m - 1$, so $\mathbf{x}^{q^n-1} - 1$ divides $\mathbf{x}^{q^m-1} - 1$. In particular, $K_n(F)$ is a subfield of $K_m(F)$. On the other hand, if $K_n(F)$ is a subfield of $K_m(F)$, then

$$[K_m(F) : K_n(F)] = [K_m(F) : F]/[K_n(F) : F] = m/n$$

proves that n divides m. □

Theorem 4.42 implies that $K_n(F)/F$ is Galois and that its Galois group $\mathbf{G}(K_n(F)/F)$ is isomorphic to $\mathbf{G}(\overline{K_n(F)}/\overline{F})$.

Lemma 4.46. *The Galois group $\mathbf{G}(\overline{K_n(F)}/\overline{F})$ is cyclic of order n, with $\overline{\sigma} : \overline{x} \mapsto \overline{x}^q$ as a canonical generator, where $q = |\overline{F}|$.*

Proof. This lemma simply describes the Galois group of a finite field extension of finite groups, which is a well-known result in Galois theory. See for instance Theorem 9.4 from [Lorenz, 2006]. □

The isomorphism between $\mathbf{G}(K_n(F)/F)$ and $\mathbf{G}(\overline{K_n(F)}/\overline{F})$ implies that $\mathbf{G}(K_n(F)/F)$ is also cyclic with a corresponding canonical generator σ. This generator is called the *Frobenius automorphism of $K_n(F)/F$*, and it can be characterized as the F-algebra automorphism on $K_n(F)$ that satisfies $v(x^\sigma - x^q) < 1$ for all $x \in O(K_n(F))$. The following theorem summarizes some of these results.

Theorem 4.47. *For any infinite local field F and natural number n, $K_n(F)/F$ is cyclic, and the Frobenius automorphism σ generates $\mathbf{G}(K_n(F)/F)$.*

We will now prove that $\mathbf{B}(K_n(F)/F)$ is a cyclic group of order n for all infinite local fields F and $n \in \mathbb{N}$. Corollary 3.39 describes a group isomorphism between $\mathbf{B}(K_n(F)/F)$ and $F^\circ/N_{K_n(F)/F}(K_n(F)^\circ)$, so we can prove the described structure of $\mathbf{B}(K_n(F)/F$ by proving that the group $F^\circ/N_{K_n(F)/F}(K_n(F)^\circ)$ is cyclic of order n when F is an infinite local field.

Let F be an infinite local field and suppose that v is a non-trivial valuation of $K = K_n(F)$ relative to which F and $K_n(F)$ are local fields. Note that for all $y \in K^\circ$, $v(N_{K/F}(y)) = \prod_{j<n} v(y^{\sigma^j}) = v(y)^n$ by Corollary 4.33 and Theorem 4.47.

Lemma 4.48. *If F is an infinite local field, n is a natural number and v is valuation of $K = K_n(F)$ relative to which F and K are local fields, then $N_{K/F}(O(K, v)^\circ) = O(F, v)^\circ$.*

Proof. Note that $O(K, v)^\circ = \{y \in K |\ v(y) = 1\}$ and $O(F, v)^\circ = \{a \in F |\ v(a) = 1\}$. The fact that $v(N_{K/F}(y)) = v(y)^n$ for all $y \in K^\circ$ yields that $N_{K/F}(O(K, v)^\circ)$ is a subset of $O(F, v)^\circ$. For a proof of the other inclusion, see for instance the proof of Lemma 17.9b from [Pierce, 1982]. □

Theorem 4.49. *Suppose that F is an infinite local field and n is a natural number. Write K for $K_n(F)$, and suppose that v is a valuation of K relative to which F and K are local fields. If $a \in F^\circ$ is a uniformizer at v for F, then $F^\circ/N_{K/F}(K^\circ)$ is a cyclic group with generator $aN_{K/F}(K^\circ)$.*

Proof. Let 1 denote the trivial group and define $\eta_n : \langle v(a)\rangle \to \langle v(a)\rangle$ as the exponentiation map $t \mapsto t^n$. The diagram of maps

$$\begin{array}{ccccccccc} 1 & \to & O(K,v)^\circ & \to & K^\circ & \overset{v}{\to} & \langle v(a)\rangle & \to & 1 \\ & & \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle \eta_n} & & \\ 1 & \to & O(F,v)^\circ & \to & F^\circ & \underset{v}{\to} & \langle v(a)\rangle & \to & 1 \end{array}$$

commutes and has exact rows, so the Snake Lemma implies that the commuting diagram

$$\begin{array}{ccccccccc} 1 & \to & O(K,v)^\circ & \to & K^\circ & \overset{v}{\to} & \langle v(a)\rangle & \to & 1 \\ & & \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle N_{K/F}} & & \downarrow{\scriptstyle \eta_n} & & \\ 1 & \to & O(F,v)^\circ & \to & F^\circ & \overset{v}{\to} & \langle v(a)\rangle & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ O(F,v)^\circ/N_{K/F}(O(K,v)^\circ) & & \to & & F^\circ/N_{K/F}(K^\circ) & \overset{v_*}{\to} & \langle v(a)\rangle/\langle v(a)^n\rangle & \to & 1 \end{array}$$

has exact rows and columns. In particular, since Lemma 4.48 implies that the quotient group $O(F,v)^\circ/N_{K/F}(O(K,v)^\circ)$ is trivial, v_* is an isomorphism from $F^\circ/N_{K/F}(K^\circ)$ to $\langle v(a)\rangle/\langle v(a)^n\rangle$. Since $\langle v(a)\rangle/\langle v(a)^n\rangle$ is cyclic of order n with generator $v(a)\langle v(a)^n\rangle$, $F^\circ/N_{K/F}(K^\circ)$ is cyclic of order n with generator $aN_{K/F}(K^\circ)$. □

Corollary 4.50. *If F is an infinite local field, then $\mathbf{B}(K_n(F)/F)$ is a cyclic group of order n generated by $[(K_n(F),\sigma,a)]$, where σ is the Frobenius automorphism and $a \in F^\circ$ is a uniformizer of F.*

Proof. This corollary follows directly from Corollary 3.39 and Theorem 4.49. □

4.7 Brauer Groups of Infinite Local Fields

We have already seen in Theorem 2.39 that the Brauer group of a finite local field is trivial. The following theorem describes the structure of $\mathbf{B}(F)$ when F is an infinite local field.

Theorem 4.51. *If F is an infinite local field, then $\mathbf{B}(F)$ satisfies $\mathbf{B}(F) \cong \mathbb{Q}/\mathbb{Z}$ by an isomorphism $\theta_F : \mathbb{Q}/\mathbb{Z} \to \mathbf{B}(F)$ defined as*

$$k/n + \mathbb{Z} \mapsto [(K_n(F),\sigma,a^k)],$$

for $n \in \mathbb{N}$, $0 \le k < n$, σ the Frobenius automorphism of F and $a \in F^\circ$ a uniformizer.

This theorem is a combination of three claims.

i) For fixed $n \in \mathbb{N}$ the map $\theta_n : n^{-1}\mathbb{Z}/\mathbb{Z} \to \mathbf{B}(K_n(F)/F)$ defined as

$$k/n + \mathbb{Z} \mapsto [(K_n(F),\sigma,a^k)]$$

for $0 \le k < n$ is a well-defined isomorphism.

ii) Let m and n be natural numbers. The diagram

$$\begin{array}{ccc} n^{-1}\mathbb{Z}/\mathbb{Z} & \to & (mn)^{-1}\mathbb{Z}/\mathbb{Z} \\ {\scriptstyle\theta_n}\downarrow & & {\scriptstyle\theta_{mn}}\downarrow \\ \mathbf{B}(K_n(F)/F) & \to & \mathbf{B}(K_{mn}(F)/F) \end{array}$$

commutes, where the horizontal maps are inclusions.

iii) $\mathbb{Q}/\mathbb{Z} = \bigcup_{n\in\mathbb{N}} n^{-1}\mathbb{Z}/\mathbb{Z}$ and $\mathbf{B}(F) = \bigcup_{n\in\mathbb{N}} \mathbf{B}(K_n(F)/F)$.

Proof. For fixed $n \in \mathbb{N}$, the map $k \mapsto (K_n(F), \sigma, a^k)$ is a group homomorphism from $\mathbb{Z}$ to $\mathbf{B}(K_n(F)/F)$ by part *i)* of Theorem 3.38. Corollary 4.50 implies that this homomorphism is surjective and has kernel $n\mathbb{Z}$, so the isomorphism $n^{-1}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ proves *i)*.

Claim *ii)* is equivalent to the statement that $(K_n(F), \sigma, a^k) \sim (K_{mn}(F), \sigma, a^{km})$ for all $k \in \mathbb{N}$, which follows from Theorem 3.40 and Corollary 4.45.

The first part of *iii)* is trivial, and the second part is equal to Corollary 4.44. □

The isomorphism θ_F can be used to define an invariant INV_F of algebras $A \in \mathbf{CSA}(F)$ when F is an infinite local field. Define $\mathrm{INV}_F : \mathbf{CSA}(F) \to \mathbb{Q}/\mathbb{Z}$ as

$$\mathrm{INV}_F\, A = \theta_F^{-1}([A]).$$

We also use INV_F to denote the map $\theta_F^{-1} : \mathbf{B}(F) \to \mathbb{Q}/\mathbb{Z}$ itself. The difference will always be clear from context.

This invariant map INV_F will be important in determining the structure of Brauer groups of algebraic number fields, so we will now study it in some detail. Before we start, we first need to introduce some new notation. If A is an F-algebra and $m \in \mathbb{N}$, then let $A^{\otimes m}$ denote the tensor product $A \otimes \cdots \otimes A$ with m copies of A.

Corollary 4.52. *Let F be an infinite local field, $A, B \in \mathbf{CSA}(F)$ and $m \in \mathbb{N}$.*

i) $A \sim B$ *if and only if* $\mathrm{INV}_F\, A = \mathrm{INV}_F\, B$.

ii) $A \sim F$ *if and only if* $\mathrm{INV}_F\, A = 0 + \mathbb{Z}$.

iii) $\mathrm{INV}_F(A \otimes B) = \mathrm{INV}_F\, A + \mathrm{INV}_F\, B$.

iv) $\mathrm{INV}_F\, A^{\otimes m} = m\,\mathrm{INV}_F\, A$.

v) $\mathrm{Ind}\, A$ *is the order of* $\mathrm{INV}_F\, A$ *in* $\mathbb{Q}/\mathbb{Z}$.

Proof. Parts *i)* to *iv)* follow directly from Theorem 4.51. For part *v)*, suppose that $\mathrm{INV}_F\, A = k/n + \mathbb{Z}$, with $n \in \mathbb{N}$, $0 \leq k < n$ and k and n relatively prime. It is clear that the order of $\mathrm{INV}_F\, A = k/n + \mathbb{Z}$ is equal to n, so we need to prove that $\mathrm{Ind}\, A = n$. Part *i)* of this corollary and Theorem 4.51 together yield that $A \sim (K_n(F), \sigma, a^k)$, so $\mathrm{Ind}\, A$ is equal to $\mathrm{Ind}(K_n(F), \sigma, a^k)$. The order of a^k modulo $N_{K_n(F)/F}(K_n(F)^\circ)$ is n by Theorem 4.49, so Corollary 3.39, Theorem 3.31 and Theorem 3.34 together imply that

$$n = \mathrm{Exp}(K_n(F), \sigma, a^k) \leq \mathrm{Ind}(K_n(F), \sigma, a^k) \leq \mathrm{Deg}(K_n(F), \sigma, a^k) = n.$$

We conclude that $\mathrm{Ind}\, A = \mathrm{Ind}(K_n(F), \sigma, a^k) = n$. □

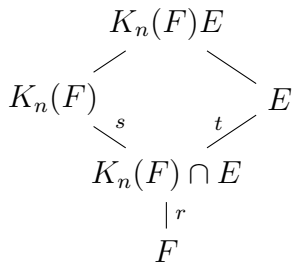
Parts *ii*), *iv*) and *v*) together imply one of the fundamental properties of central simple algebras over a local field.

Corollary 4.53. *Let F be an infinite local field. For all $A \in \mathbf{CSA}(F)$, $\operatorname{Ind} A = \operatorname{Exp} A$.*

This fulfills our promise in Section 3.5 that $\operatorname{Ind} A$ and $\operatorname{Exp} A$ would be equal for all $A \in \mathbf{CSA}(F)$ when F is a local field, since we have already seen that it is true for finite fields F.

Our next theorem describes a useful relation between $\operatorname{INV}_E A^E$ and $\operatorname{INV}_F A$ when E/F is a finite field extension of infinite local fields and $A \in \mathbf{CSA}(F)$. We first introduce a technical lemma.

Lemma 4.54. *Let E/F be a finite extension of infinite local fields. Define $m = [E : F]$, $r = [K_n(F) \cap E : F]$, $s = [K_n(F) : K_n(F) \cap E]$ and $t = [E : K_n(F) \cap E]$. This can be visualized as the following diagram:*



Also define $l = f(E/K_n(F) \cap E)$. The following statements hold true:

i) $n = rs$ *and* $m = rt$.

ii) $K_n(F)E = K_s(E)$ *and* $K_n(F) \cap E = K_r(F)$.

iii) $f(E/F) = lr$ *and* $t = le(E/F)$.

iv) $\gcd(l, s) = 1$.

Proof. See for instance the proof of Proposition 17.10 in [Pierce, 1982]. □

Theorem 4.55. *If E/F is a finite extension of infinite local fields and A is an element of $\mathbf{CSA}(F)$, then $\operatorname{INV}_E A^E = [E : F] \operatorname{INV}_F A$.*

Proof. The statement of the theorem is equivalent to stating that the diagram

$$\begin{array}{ccc} \mathbb{Q}/\mathbb{Z} & \overset{[E:F]}{\to} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \theta_F}\downarrow & & {\scriptstyle \theta_E}\downarrow \\ \mathbf{B}(F) & \overset{\kappa_*}{\to} & \mathbf{B}(E) \end{array}$$

commutes, where the top map is multiplication by $[E:F]$, and κ_* is the homomorphism induced by the inclusion of F in E. We therefore only need to prove that the equation $\kappa_*(\theta_F(k/n+\mathbb{Z})) = \theta_E([E:F]k/n+\mathbb{Z})$ holds for all $n \in \mathbb{N}$ and $0 \leq k < n$.

We first describe the connections between uniformizers of E and uniformizers of F, and between the Frobenius automorphisms σ_E of E and σ_F of F. Let w be a valuation of E such that E and F are local fields with respect to w, let v be the restriction of w to F and let a be a uniformizer of w. By definition, the ramification index $e_w(E/F)$ is equal to the order of the group $w(E^\circ)/v(F^\circ)$. In particular, $b = a^{e_w(E/F)}$ is a uniformizer of v. Under the isomorphisms $\mathbf{G}(K_s(E)/E) \cong \mathbf{G}(\overline{K_s(E)}/\overline{E})$ and $\mathbf{G}(K_n(F)/F) \cong \mathbf{G}(\overline{K_n(F)}/\overline{F})$, σ_E corresponds to the map $\overline{x} \mapsto \overline{x}^{|\overline{E}|}$ and σ_F corresponds to $\overline{x} \mapsto \overline{x}^{|\overline{F}|}$. The definition of $f_w(E/F)$ implies that $|\overline{E}|$ is equal to $f_w(E/F)|\overline{F}|$, so $\sigma_E|_{K_n(F)}$ is equal to $\sigma_F^{f_w(E/F)}$.

Let m, r, s, t and l be defined as in Lemma 4.54. For $n \in \mathbb{N}$ and $0 \leq k < n$, $\kappa_*(\theta_F(k/n+\mathbb{Z})) = \kappa_*([(K_n(F), \sigma_F, b^k)]) = [(K_n(F), \sigma_F, b^k)^E]$ by definition of θ_F and κ_*. After applying Theorem 3.41 and Lemma 4.54 we find that

$$\begin{aligned}[(K_n(F), \sigma_F, b^k)^E] &= [(K_n(F)E, \sigma_F^r, b^k)] = [(K_s(E), \sigma_F^r, a^{ke(E/F)})] \\ &= [(K_s(E), \sigma_F^{lr}, a^{kle(E.F)})] = [(K_s(E), \sigma_E, a^{kt})],\end{aligned}$$

where we could apply part *iii)* of Theorem 3.38 since $\gcd(l,s) = 1$. Theorem 3.40, Corollary 4.45 and Lemma 4.54 together imply that

$$[(K_s(E), \sigma_E, a^{kt})] = [(K_n(E), \sigma_E, a^{krt})] = [(K_n(E), \sigma_E, a^{km})] = \theta_E([E:F]k/n+\mathbb{Z}).$$

We conclude that $\kappa_*(\theta_F(k/n+\mathbb{Z})) = \theta_E([E:F]k/n+\mathbb{Z})$ for all $n \in \mathbb{N}$ and $0 \leq k < n$. $\square$

We have now proven some properties of INV_F, but we have not yet determined the actual value of $\mathrm{INV}_F A$ for a local field F and an algebra $A \in \mathbf{CSA}(F)$ that is not already in the form $(K_n(F), \sigma, a^k)$ with $n \in \mathbb{N}$ and $0 \leq k < n$. This is quite difficult to do in general, so we will only tackle a relatively simple example.

Suppose that A is the quaternion algebra $\left(\frac{a,b}{F}\right)$ with $a, b \in F^\circ$ and $\operatorname{char} F \neq 2$. The dimension $\dim_F A$ is by definition equal to 4, so the degree $\operatorname{Deg} A$ is equal to 2. Theorem 3.31 and Corollary 4.53 imply that $\operatorname{Exp} A = \operatorname{Ind} A$ divides $\operatorname{Deg} A$, so $\operatorname{Exp} A$ is equal to either 1 or 2. This corresponds to the elements $0+\mathbb{Z}$ and $1/2+\mathbb{Z}$ of $\mathbb{Q}/\mathbb{Z}$, where $\mathrm{INV}_F A$ is equal to $1/2+\mathbb{Z}$ precisely when $\operatorname{Ind} A = 2 = \operatorname{Deg} A$, so precisely when $A = \left(\frac{a,b}{F}\right)$ is a division algebra. Theorem 2.20 states that $\left(\frac{a,b}{F}\right)$ is a division algebra precisely when the only solution to $c_0^2 = ac_1^2 + bc_2^2$ with $c_0, c_1, c_2 \in F$ is $c_0 = c_1 = c_2 = 0_F$. This means that we have converted the problem of determining $\mathrm{INV}^{(F)} A$ to the problem of solving equations of the form $c_0^2 = ac_1^2 + bc_2^2$ where c_0, c_1 and c_2 are elements of F that are not all zero.

However, even over the p-adic numbers it can be quite difficult to determine whether $c_0^2 = ac_1^2 + bc_2^2$ has solutions with c_0, c_1 and c_2 not all trivial. Fortunately, this problem has already been studied extensively. For p a prime number and $a, b \in \mathbb{Q}^\circ$, the *Hilbert symbol* $(a,b)_p$ is defined as 1 when $c_0^2 = ac_1^2 + bc_2^2$ has a non-trivial solution over $\hat{\mathbb{Q}}_p$ and as -1 when it does not have such a solution. We can therefore summarize some of our

results up to this point as

$$\mathrm{INV}_{\hat{\mathbb{Q}}_p}\left(\frac{a,b}{\hat{\mathbb{Q}}_p}\right) = \begin{cases} 0+\mathbb{Z} & \text{if } (a,b)_p = 1 \\ \frac{1}{2}+\mathbb{Z} & \text{if } (a,b)_p = -1. \end{cases}$$

See for instance Section 5.2 of [Cohen, 2008] for a thorough discussion of the Hilbert symbol. This section also describes a formula for the Hilbert symbol. It uses the *Legendre symbol*, which we define as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square modulo } p, \\ -1 & \text{if } a \text{ is not a square modulo } p. \end{cases}$$

for p an odd prime and $a \in \mathbb{Z}$ with $\gcd(a,p) = 1$. An integer a is a square modulo p when $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ is equal to $\overline{x}^2$ for some $\overline{x} \in \mathbb{Z}/p\mathbb{Z}$. We also define

$$\left(\frac{a}{2}\right) = (-1)^{\frac{a^2-1}{8}} = \begin{cases} 1 & \text{if } a \equiv \pm 1 \mod 8, \\ -1 & \text{if } a \equiv \pm 3 \mod 8. \end{cases}$$

for odd integers a. This is a specific case of the Kronecker symbol $\left(\frac{a}{n}\right)$, which is one of the possible extensions of the Legendre symbol to all integers n. See for instance Section 2.2 of [Cohen, 2008] for a discussion on this subject.

Let p be a prime number and suppose that a and b are elements of $\mathbb{Q}^\circ$. Write $a = p^k a'$ and $b = p^l b'$ with $k, l \in \mathbb{Z}$ and $a', b' \in \mathbb{Q}^\circ$ with $\gcd(a', p) = \gcd(b', p) = 1$. If p is an odd prime, then the formula for the Hilbert symbol is

$$(a,b)_p = (-1)^{\frac{kl(p-1)}{2}} \left(\frac{a'}{p}\right)^l \left(\frac{b'}{p}\right)^k,$$

and for $p = 2$ the formula is

$$(a,b)_2 = (-1)^{\frac{(a'-1)(b'-1)}{4}} \left(\frac{a'}{2}\right)^l \left(\frac{b'}{2}\right)^k.$$

As an example, we consider the case where $a = b = -1$. It is clear that $k = l = 0$ and $a' = b' = -1$ in this case, so for p an odd prime the Hilbert symbol is equal to

$$(-1,-1)_p = (-1)^0 \left(\frac{-1}{p}\right)^0 \left(\frac{-1}{p}\right)^0 = 1,$$

and the Hilbert symbol $(-1,-1)_2$ can be calculated as

$$(-1,-1)_2 = (-1)^{\frac{(-2)(-2)}{4}} \left(\frac{-1}{2}\right)^0 \left(\frac{-1}{2}\right)^0 = -1.$$

We conclude that for a prime number p

$$\mathrm{INV}_{\hat{\mathbb{Q}}_p}\left(\frac{-1,-1}{\hat{\mathbb{Q}}_p}\right) = \begin{cases} 0+\mathbb{Z} & \text{if } p \neq 2 \\ \frac{1}{2}+\mathbb{Z} & \text{if } p = 2. \end{cases}$$

As a second example, consider $\left(\frac{3,5}{\hat{\mathbb{Q}}_p}\right)$. For all odd primes unequal to 3 and 5, $k = l = 0$ implies that

$$(3,5)_p = (-1)^0 \left(\frac{3}{p}\right)^0 \left(\frac{5}{p}\right)^0 = 1.$$

If p is equal to 3, then $k = 1$, $l = 0$, $a' = 1$ and $b' = 5$ give that

$$(3,5)_3 = (-1)^0 \left(\frac{1}{3}\right)^0 \left(\frac{5}{3}\right)^1 = \left(\frac{5}{3}\right) = -1,$$

and for $p = 5$ we find that $e = 0$, $f = 1$, $a' = 3$ and $b' = 1$, so

$$(3,5)_5 = (-1)^0 \left(\frac{3}{5}\right)^1 \left(\frac{1}{5}\right)^0 = \left(\frac{3}{5}\right) = -1.$$

The Legendre symbols $\left(\frac{5}{3}\right)$ and $\left(\frac{3}{5}\right)$ are both equal to -1 since in $\mathbb{Z}/5\mathbb{Z}$ the class $\overline{3}$ is not a square and in $\mathbb{Z}/3\mathbb{Z}$ the class $\overline{5} = \overline{2}$ is not a square. Finally, the Hilbert symbol $(3,5)_2$ is equal to

$$(3,5)_2 = (-1)^{\frac{(3-1)(5-1)}{4}} \left(\frac{3}{2}\right)^0 \left(\frac{5}{2}\right)^0 = 1.$$

Now that we have determined all Hilbert symbols $(3,5)_p$, we find that for a prime p

$$\mathrm{INV}_{\hat{\mathbb{Q}}_p} \left(\frac{3,5}{\hat{\mathbb{Q}}_p}\right) = \begin{cases} 0 + \mathbb{Z} & \text{if } p \neq 3 \text{ and } p \neq 5 \\ \frac{1}{2} + \mathbb{Z} & \text{if } p = 3 \text{ or } p = 5. \end{cases}$$

We have now found the value of $\mathrm{INV}_{\hat{\mathbb{Q}}_p} A$ for some algebras $A \in \mathbf{CSA}(\hat{\mathbb{Q}}_p)$. One problem with this approach is that it cannot be generalized to algebras in $\mathbf{CSA}(\hat{\mathbb{Q}}_p)$ of higher dimension over $\hat{\mathbb{Q}}_p$. We used the fact that any quaternion algebra $A \in \mathbf{CSA}(\hat{\mathbb{Q}}_p)$ is 4-dimensional over F to conclude that its equivalence class has order 1 or 2 in $\mathbf{B}(\hat{\mathbb{Q}}_p)$. This order fully determines $\mathrm{INV}_{\hat{\mathbb{Q}}_p} A$, since $\mathbb{Q}/\mathbb{Z}$ has unique elements of order 1 and 2. This is not true for larger orders, so a different approach would be needed to determine $\mathrm{INV}_{\hat{\mathbb{Q}}_p} A$ when $\dim_{\hat{\mathbb{Q}}_p} A > 4$.

5 Brauer Groups of Algebraic Number Fields

In this chapter we study the Brauer groups of algebraic number fields. An *algebraic number field* is a subfield F of $\mathbb{C}$ with $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$ such that the degree $[F : \mathbb{Q}]$ is finite. Brauer groups of algebraic number fields are more complex than the Brauer groups we have encountered so far, and many of the proofs in this chapter match this complexity.

Section 5.1 is spent on the study of valuations of algebraic number fields. In Section 5.2 we define the global invariant, which is an injective map from the Brauer group $\mathbf{B}(F)$ of an algebraic number field F to a direct product of countably many subgroups of $\mathbb{Q}/\mathbb{Z}$. We calculate the global invariant of two quaternion algebras over $\mathbb{Q}$ in Section 5.3, and use them to determine what quadratic fields split these two quaternion algebras. Section 5.4 contains the main theorem of this chapter. It describes the structure of Brauer groups $\mathbf{B}(F)$ of algebraic number fields F by constructing a short exact sequence with $\mathbf{B}(F)$ as the first non-trivial term, and the proof of this theorem is spread out over this sections three subsections. Section 5.5 studies some concrete consequences of this main theorem, and Section 5.6 applies much of what we have learned in this thesis to prove that all algebras over algebraic number fields are cyclic and have identical index and exponent.

In this chapter F will always denote a field.

5.1 Valuations of Algebraic Number Fields

Our study of Brauer groups of algebraic number fields requires some knowledge of the valuations of algebraic number fields. The following lemma will be useful in that regard.

Lemma 5.1. *Let v be a non-trivial valuation of F such that $\hat{F}_v$ is locally compact in the v-topology, and assume that K/F is a finite, separable field extension.*

i) For some integer r with $1 \leq r \leq [K : F]$, there are r distinct extensions $w_1, \ldots, w_r$ of v to K, and they satisfy $\sum_{i=1}^{r} [\hat{K}_{w_i} : \hat{F}_v] = [K : F]$.

ii) If v is discrete, then all w_i are discrete. Furthermore, $e_{w_i}(K/F) = e_{w_i}(\hat{K}_{w_i}/\hat{F}_v)$ and $f_{w_i}(K/F) = f_{w_i}(\hat{K}_{w_i}/\hat{F}_v)$ hold for all $i = 1, \ldots, r$.

iii) Suppose that K/F is Galois and that w extends v to K. If $w^\sigma : K \to \mathbb{R}$ with $\sigma \in \mathbf{G}(K/F)$ is defined as $w^\sigma(x) = w(x^{\sigma^{-1}})$ for all $x \in K$, then w^σ is a valuation that also extends v. Every extension of v to K is equal to w^σ for some $\sigma \in \mathbf{G}(K/F)$.

Proof. This lemma is a combination of parts of Proposition 18.2, Corollary 18.2a and Corollary 18.2b from [Pierce, 1982]. □

If F is an algebraic number field, then $F/\mathbb{Q}$ is by definition finite and $\operatorname{char}\mathbb{Q} = 0$ yields that it is also separable. All non-trivial valuations of $\mathbb{Q}$ are equivalent to v_∞ or v_p for some prime p by Theorem 4.12, we know that $\hat{\mathbb{Q}}_{v_\infty} = \mathbb{R}$ is locally compact in the v_∞-topology, and Theorem 4.22 and Corollary 4.26 yield that $\hat{\mathbb{Q}}_{v_p} = \hat{\mathbb{Q}}_p$ with p prime is locally compact in the v_p-topology. By applying Lemma 5.1 in this way, we find the following theorem.

Theorem 5.2. *Let v be a non-trivial valuation of an algebraic number field F.*

i) If v is non-archimedean, then v divides a p-adic valuation v_p of $\mathbb{Q}$ for a unique prime p, v is discrete, $E(F, v)$ is a finite field, and $\hat{F}_v$ is an infinite local field. For each prime p, there are at most $[F : \mathbb{Q}]$ distinct extensions of v_p to F.

ii) If v is archimedean, then v divides the absolute value $v_\infty^{\mathbb{Q}}$ of $\mathbb{Q}$. There exists an isometric isomorphism from $\hat{F}_v$ to either $\mathbb{R}$ and $\mathbb{C}$ equipped with the absolute values $v_\infty^{\mathbb{R}}$ or $v_\infty^{\mathbb{C}}$, respectively. There are at most $[F : \mathbb{Q}]$ distinct extensions of $v_\infty^{\mathbb{Q}}$ to F.

Proof. If v is non-archimedean, then Theorem 4.7 yields that $v|_{\mathbb{Q}}$ is non-archimedean and non-trivial, so Theorem 4.12 implies that $v|_{\mathbb{Q}}$ is equivalent to v_p for a unique prime p and that $E(\mathbb{Q}, v|_{\mathbb{Q}})$ is finite. Lemma 5.1 yields that $[\hat{F}_v : \hat{\mathbb{Q}}_p]$ is finite and that v is discrete. This means that $\hat{F}_v$ is an infinite local field by Corollary 4.34 and that $f_v(F/\mathbb{Q}) = f_v(\hat{F}_v/\hat{\mathbb{Q}}_{v|_{\mathbb{Q}}})$ is finite by Theorem 4.36. The fact that $f_v(F/\mathbb{Q})$ and $E(\mathbb{Q}, v|_{\mathbb{Q}})$ are finite implies that $E(F, v)$ is also a finite field.

If v is archimedean, then Theorem 4.12 implies that v divides the absolute value $v_\infty^{\mathbb{Q}}$ of $\mathbb{Q}$. Note that $\hat{\mathbb{Q}}_{v_\infty}$ is equal to $\mathbb{R}$, that $\hat{F}_v/\hat{\mathbb{Q}}_{v_\infty}$ is finite by Lemma 5.1, and that F is a subfield of $\mathbb{C}$ with $\mathbb{C}$ complete in the $v_\infty^{\mathbb{C}}$-topology. The only fields E with $\mathbb{R} \subseteq E \subseteq \mathbb{C}$ are $E = \mathbb{R}$ and $E = \mathbb{C}$, so we conclude from Corollary 4.24 that $\hat{F}_v$ is isometrically isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ with the standard absolute value $v_\infty^{\mathbb{R}}$ or $v_\infty^{\mathbb{C}}$.

Finally, note that in both cases $\hat{F}_v$ is locally compact in the v-topology and $F/\mathbb{Q}$ is separable, so part i) of Lemma 5.1 implies that for each non-trivial valuation v' of $\mathbb{Q}$ there are at most $[F : \mathbb{Q}]$ distinct extensions of v' to F. □

This theorem implies that $\hat{F}_v$ is locally compact in the v-topology for all non-trivial valuations v of an algebraic number field F. If K/F is an extension of algebraic number fields, then K/F is both finite and separable, so we can apply Lemma 5.1 to K/F whenever K is equipped with a non-trivial valuation.

We are especially interested in the completions of algebraic number fields. If K/F is an extension of algebraic number fields and w is a valuation of K that restricts to v on F, then Corollary 4.24 implies that $\hat{F}_v$ can be identified with a subfield of $\hat{K}_w$, which implies that $\hat{K}_w$ has the structure of an $\hat{F}_v$-algebra. The following lemma describes some properties of the completions $\hat{K}_w$ and $\hat{F}_v$ when K/F is Galois.

Lemma 5.3. *Assume that K/F is a finite Galois extension, v is a non-trivial valuation of F such that $\hat{F}_v$ is locally compact in the v-topology, and that w is an extension of v to K.*

i) As an $\hat{F}_v$-algebra, $\hat{K}_w$ is independent of the choice of w.

ii) $\hat{K}_w/\hat{F}_v$ is finite and Galois.

iii) The subfields K and $\hat{F}_v$ of $\hat{K}_w$ satisfy $\hat{K}_w = K\hat{F}_v$.

Proof. This lemma is a summary of parts of Proposition 18.2 and Corollary 18.2c from [Pierce, 1982]. □

If K/F is an extension of algebraic number fields and w is a valuation of K that divides some non-trivial valuation v of F, then $\hat{K}_w/\hat{F}_v$ is a finite field extension by part i) of Lemma 5.1. The degree $[\hat{K}_w : \hat{F}_v]$ is called the *local degree of K/F at w*. When K/F is Galois, Lemma 5.3 states that $\hat{K}_w$ has the same $\hat{F}_v$-algebra structure for all extensions w of v. In this case, we write $\hat{K}_v$ for $\hat{K}_w$ and call $[\hat{K}_v : \hat{F}_v]$ the *local degree of K/F at v*. Note that the Galois group $\mathbf{G}(\hat{K}_v/\hat{F}_v)$ is also well-defined in this case.

Let K/F be a Galois extension of algebraic number fields, and suppose that v is a non-trivial valuation of F. We note that $\hat{K}_v$ inherits a canonical $\hat{F}_v$-algebra structure from the completions $\hat{K}_w$ with w an extension of v to K, since this $\hat{F}_v$-algebra structure is independent of the choice of w. The canonical inclusions $\kappa_w : K \to \hat{K}_w$ also induce a K-algebra structure on each completion $\hat{K}_w$, but this does not necessarily induce a canonical K-algebra structure on $\hat{K}_v$, since these K-algebra structure are not necessarily independent of the choice of w. The following theorem does prove a weaker result.

Theorem 5.4. *Suppose that K/F is a Galois extension of algebraic number fields, and let v be a non-trivial valuation of F. All injective F-algebra homomorphisms $K \to \hat{K}_v$ have the same image.*

Proof. The fact that K/F is Galois implies that K is the splitting field of some separable $\Phi \in F[\mathbf{x}]$. Let n be the degree of the polynomial Φ. Since Φ splits in K, Φ splits in $\hat{K}_w \supseteq K$ as well. Let $y_1, \ldots, y_n$ be the roots of Φ in $\hat{K}_w$.

If $\psi : K \to \hat{K}_w$ is an injective F-algebra homomorphism, then ψ acts as the identity on F, so ψ maps the roots of $\Phi \in F[\mathbf{x}]$ in K to the roots $y_1, \ldots, y_n \in \hat{K}_w$. In particular, the image of ψ is equal to $F(y_1, \ldots, y_n) \subseteq \hat{K}_w$.

The $\hat{F}_v$-algebra structure of $\hat{K}_w$ is independent of the choice of w, so the embedding of both F and the roots of $\Phi \in F[\mathbf{x}]$ into $\hat{K}_w$ is also independent of this choice. We conclude that all injective F-algebra homomorphisms from K to $\hat{K}_v$ have the same image. □

In particular, this theorem implies that the inclusions $\kappa_w : K \to \hat{K}_w$ all have essentially the same image for extensions w of the same valuation v of F. Since each κ_w is isometric, we can identify K with a subfield of $\hat{K}_v$ by choosing an extension w of v to K and then identifying K with $\kappa_w(K)$. The precise embedding depends on the choice of w, but we find that $\hat{K}_v = K\hat{F}_v$ is true for any such choice. In later sections, we will often use this method to identify K with a subfield of $\hat{K}_v$ such that $\hat{K}_v = K\hat{F}_v$.

We will now study the Galois groups of completions of algebraic number fields.

Lemma 5.5. *Let v be a non-trivial valuation of F and suppose that $\hat{F}_v$ is locally compact in the v-topology, K/F is a finite Galois extension, and w is a valuation of K that extends v. Let $\kappa_w : K \to \hat{K}_w$ denote the canonical inclusion of K into $\hat{K}_w$.*

i) The map $\phi_w : \mathbf{G}(\hat{K}_w/\hat{F}_v) \to \mathbf{G}(K/F)$ defined by $\sigma \mapsto \kappa_w^{-1}\sigma\kappa_w$ for all $\sigma \in \mathbf{G}(\hat{K}_w/\hat{F}_v)$ is an injective group homomorphism. Denote the image of ϕ_w by G_w.

ii) If σ and τ are elements of $\mathbf{G}(K/F)$, then $w^\sigma = w^\tau$ if and only if $\sigma\tau^{-1} \in G_w$.

iii) If $\mathbf{G}(K/F)$ is abelian, then G_w independent of the choice of w.

Proof. This lemma is a consequence of Corollary 18.2c from [Pierce, 1982]. □

The group G_w is called the *decomposition group of w*. When $\mathbf{G}(K/F)$ is abelian, write G_v for G_w and note that we can identify G_v with $\mathbf{G}(\hat{K}_w/\hat{F}_v)$ by using the injective homomorphism ϕ_w. Note that this lemma also implies that $[\hat{K}_v : \hat{F}_v] = |\mathbf{G}(\hat{K}_v/\hat{F}_v)|$ divides $|\mathbf{G}(K/F)| = [K : F]$ whenever K/F is finite and Galois.

The following theorem follows from the fact that ϕ_w acts as an isomorphism from $\mathbf{G}(\hat{K}_w/\hat{F}_v)$ to G_w.

Theorem 5.6. *Let K/F be a Galois extension of algebraic number fields and suppose that w is a non-trivial discrete valuation of K with $e_w(K/F) = 1$ that extends the valuation v of F. The decomposition group G_w is cyclic, and there exists a unique generator σ_w of G_w such that $w(x^{\sigma_w} - x^q) < 1$ for all $x \in O(K, w)$, where $q = |E(F, v)|$. For all $\tau \in \mathbf{G}(K/F)$, σ_{w^τ} is equal to $\tau^{-1}\sigma_w\tau$.*

Proof. Part *ii*) of Lemma 5.1 implies that $e_w(\hat{K}_w/\hat{F}_v) = e_w(K/F) = 1$. Since $\hat{K}_w/\hat{F}_v$ is a finite unramified Galois extension of infinite local fields, $\hat{K}_w$ is isomorphic as a $\hat{F}_v$-algebra to $K_n(\hat{F}_v)$ with $n = [\hat{K}_w : \hat{F}_v]$. Theorem 4.47 then implies that $\mathbf{G}(\hat{K}_w/\hat{F}_v)$ is cyclic and generated by the Frobenius automorphism σ uniquely characterized by $w(x^\sigma - x^q) < 1$ for all $x \in O(\hat{K}_w, w)$. The isomorphism between G_w and $\mathbf{G}(\hat{K}_w/\hat{F}_v)$ proves the existence and uniqueness of the generator σ_w.

If $\tau \in \mathbf{G}(K/F)$ and $x \in O(K, w^\tau)$, then $x^{\tau^{-1}}$ is an element of $O(K, w)$ such that

$$w^\tau(x^{\tau^{-1}\sigma_w\tau} - x^q) = w((x^{\tau^{-1}})^{\sigma_w} - (x^{\tau^{-1}})^q) < 1.$$

By the unique characterization of σ_{w^τ}, σ_{w^τ} is equal to $\tau^{-1}\sigma_w\tau$. □

The element σ_w of $\mathbf{G}(K/F)$ is called the *Frobenius automorphism of K/F at w*. When K/F is Galois, σ_w is only defined for the discrete valuations w of K such that $e_w(K/F) = 1$, but we will later see that many valuations w of K satisfy these conditions. Note that σ_w is equal to $\sigma_{w'}$ when w and w' are equivalent valuations of K. When $\mathbf{G}(K/F)$ is abelian, part *iii*) of Lemma 5.1 and $\sigma_{w^\tau} = \tau^{-1}\sigma_w\tau$ together imply that $\sigma_w = \sigma_{w'}$ for all valuations w and w' of K that divide the same valuation v of F. In this case, we will write σ_v for $\sigma_w = \sigma_{w'}$.

Many of the definitions and properties related to valuations are only dependent on the equivalence class of a valuation. One of the ways of dealing with this is by choosing a

representative for each of these classes. For algebraic number fields, we can for instance use the normalized valuations as representatives.

Let v be a non-trivial valuation of an algebraic number field F. Theorem 5.2 implies that v divides v_p for either p prime or $p = \infty$. If v satisfies $v|_{\mathbb{Q}} = v_p^{n(v)}$ with $n(v)$ defined as $n(v) = [\hat{F}_v : \hat{\mathbb{Q}}_p]$ for p prime and $n(v) = [\hat{F}_v : \mathbb{R}]$ for $p = \infty$, then v is called a *normalized valuation of* F. Clearly, every non-trivial valuation of F is equivalent to a unique normalized valuation. Also, if p is prime or ∞, then only finitely many normalized valuations divide v_p. Let $\mathbf{V}(F)$ be the set of non-trivial, normalized valuations of F. If p is prime or ∞, let $\mathbf{V}_p(F)$ be the set of $v \in \mathbf{V}(F)$ that divide v_p.

The following theorem describes two useful properties of normalized valuations.

Theorem 5.7. *Suppose that K/F is an extension of algebraic number fields.*

i) If $v \in \mathbf{V}(F)$, $w \in \mathbf{V}(K)$ and $w|v$, then $w|_F$ is equal to v^k with $k = [\hat{K}_w : \hat{F}_v]$.

ii) If $x \in F^\circ$, then $v(x) = 1$ for almost all $v \in \mathbf{V}(F)$.

Proof. Suppose that v is an element of $\mathbf{V}_p(F)$ for p prime or ∞. If $w \in \mathbf{V}(K)$ satisfies $w|v$, then $w|_F = v^k$ for some $k \in \mathbb{R}_{>0}$, and $w|v_p$ implies that w is an element of $\mathbf{V}_p(K)$. If we define $n(w) = [\hat{K}_w : \hat{\mathbb{Q}}_p]$ and $m(v) = [\hat{F}_v : \hat{\mathbb{Q}}_p]$, then $v_p^{n(w)} = w|_{\hat{\mathbb{Q}}_p} = v^k|_{\hat{\mathbb{Q}}_p} = v_p^{m(v)k}$ implies that k satisfies $k = n(w)/m(v) = [\hat{K}_w : \hat{F}_v]$.

All elements of F° are algebraic over $\mathbb{Q}$, since $[F : \mathbb{Q}] < \infty$. Suppose that $x \in F^\circ$ satisfies $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ with $a_i \in \mathbb{Q}$, $a_n \neq 0$ and $n \geq 1$. Let X be the set of all prime factors present in the numerators and denominators of the non-zero a_i. Note that X is finite, and that $v_p(a_i) = 1$ for all primes $p \notin X$ and $1 \leq i \leq n$ such that $a_i \neq 0$.

If p is prime, $p \notin X$ and $v \in \mathbf{V}_p(F)$, then $v(a_i x^{n-i}) = v(x)^{n-i}$ for all i with $a_i \neq 0$. The Domination Principle implies that $v(x) = 1$ in the following way. If $v(x) > 1$, then $v(x^n) = v(x)^n > v(a_i x^{n-i})$ for all $1 \leq i \leq n$ implies that

$$0 = v(0) = v(x^n + a_1 x^{n-1} + \ldots + a_n) = v(x^n) > 1.$$

If $v(x) < 1$, then $v(a_n) = 1 > v(a_i x^{n-i})$ for all $0 \leq i < n$ implies that

$$0 = v(0) = v(x^n + a_1 x^{n-1} + \ldots + a_n) = v(a_n) = 1.$$

We conclude that $v(x) = 1$ for all $v \in \mathbf{V}(F)$ that are not an element of the finite set $\mathbf{V}_\infty(F) \cup \bigcup_{p \in X} \mathbf{V}_p(F)$. □

5.2 The Global Invariant

In this section, we first discuss and derive the Albert-Hasse-Brauer-Noether Theorem. We then rephrase this important theorem into a form that will be more directly useful for our study of the Brauer groups of algebraic number fields in the next few sections.

Theorem 5.8 (Albert-Hasse-Brauer-Noether Theorem)**.** *Let F be an algebraic number field. If $A \in \mathbf{CSA}(F)$ satisfies $A \otimes \hat{F}_v \sim \hat{F}_v$ for all $v \in \mathbf{V}(F)$, then $A \sim F$.*

For convenience, we will refer to this theorem as the AHBN-Theorem. A full proof of the AHBN-Theorem is beyond the scope of this thesis, so instead we will derive the AHBN-Theorem from the Hasse Norm Theorem, which is a fairly deep result from class field theory.

Theorem 5.9 (Hasse Norm Theorem)**.** *Let K/F be a cyclic extension of algebraic number fields. An element $a \in F^\circ$ is the norm of some element in K° if and only if $a \in N_{\hat{K}_v/\hat{F}_v}(\hat{K}_v^\circ)$ for all $v \in \mathbf{V}(F)$.*

Proof. See for instance the proofs leading up to Remark 8.6 in [Cassels and Fröhlich, 1986, p. 180]. □

Since K/F is Galois, part i) of Lemma 5.3 states that $\hat{K}_w$ has the same $\hat{F}_v$-algebra structure regardless of the choice of extension w of v. This implies that $N_{\hat{K}_w/\hat{F}_v}(\hat{K}_w)$ is also independent of this choice, so the notation $N_{\hat{K}_v/\hat{F}_v}(\hat{K}_v)$ instead of $N_{\hat{K}_w/\hat{F}_v}(\hat{K}_w)$ is justified. As discussed in the previous section, we will identify K and $\hat{F}_v$ with subfields of $\hat{K}_v$ such that $\hat{K}_v = K\hat{F}_v$.

We need one more technical lemma to prove the AHBN-Theorem.

Lemma 5.10. *Suppose $A \in \mathbf{CSA}(F)$ satisfies $\operatorname{Ind} A > 1$. If p is a prime divisor of $\operatorname{Ind} A$, then for some separable extension E/F, A^E is Morita equivalent to some cyclic division algebra $D \in \mathbf{CSA}(E)$ of degree p.*

Proof. This lemma is a direct consequence of Proposition 15.2 from [Pierce, 1982]. □

Proof of Theorem 5.8. We first consider the case where A is a cyclic algebra. We then derive the general result from this specific case.

Suppose that $A = (K, \sigma, a)$ satisfies $A \otimes \hat{F}_v \sim \hat{F}_v$ for all $v \in \mathbf{V}(F)$, where K/F is a cyclic extension of algebraic number fields, $\mathbf{G}(K/F) = \langle\sigma\rangle$ and $a \in F^\circ$. Theorem 3.41 yields that

$$\hat{F}_v \sim (K, \sigma, a) \otimes \hat{F}_v \sim (K\hat{F}_v, \sigma^r, a) = (\hat{K}_v, \sigma^r, a)$$

with $r = [K : F]/[\hat{K}_v : \hat{F}_v]$. Part v) of Theorem 3.38 gives that $a \in N_{\hat{K}_v/\hat{F}_v}(\hat{K}_v^\circ)$ for all $v \in \mathbf{V}(F)$, so the Hasse Norm Theorem implies that a is an element of $N_{K/F}(K^\circ)$. Another application of part v) of Theorem 3.38 then shows that $A = (K, \sigma, a) \sim F$.

We prove the general case by contradiction. Suppose that $A \in \mathbf{CSA}(F)$ satisfies $\operatorname{Ind} A > 1$ and $A \otimes \hat{F}_v \sim \hat{F}_v$ for all $v \in \mathbf{V}(F)$. If p is a prime divisor of $\operatorname{Ind} A$, then let E be the algebraic number field and $D \in \mathbf{CSA}(E)$ the division algebra described in Lemma 5.10. In particular, D is cyclic and $D \not\sim E$. If $w \in \mathbf{V}(E)$ divides $v \in \mathbf{V}(F)$, then we identify $\hat{F}_v$ with a subfield of $\hat{E}_w$ and find that

$$D \otimes_E \hat{E}_w \sim A^E \otimes_E \hat{E}_w \cong (A \otimes \hat{F}_v) \otimes_{\hat{F}_v} \hat{E}_w \sim \hat{F}_v \otimes_{\hat{F}_v} \hat{E}_w \cong \hat{E}_w$$

yields that $D \in \mathbf{CSA}(E)$ is a cyclic algebra such that $D \otimes_E \hat{E}_w \sim \hat{E}_w$ for all $w \in \mathbf{CSA}(E)$. The first part of the proof now implies that $D \sim E$, but this is in contradiction to our choice of D. □

The maps INV_F as defined in Section 4.7 can be used to put the AHBN-Theorem in a more convenient form, but in order to do so we first need to extend the definition of INV_F to the cases $F = \mathbb{R}$ and $F = \mathbb{C}$.

We would like INV_F to be a group isomorphism from $\mathbf{B}(F)$ to a subgroup of $\mathbb{Q}/\mathbb{Z}$. Corollaries 2.41 and 2.42 state that $\mathbf{B}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$ with $[\mathbb{R}] \neq [\mathbb{H}]$ and $\mathbf{B}(\mathbb{C}) = \{[\mathbb{C}]\}$, so we define the maps $\mathrm{INV}_{\mathbb{R}} : \mathbf{B}(\mathbb{R}) \to (1/2)\mathbb{Z}/\mathbb{Z}$ and $\mathrm{INV}_{\mathbb{C}} : \mathbf{B}(\mathbb{C}) \to \{0 + \mathbb{Z}\}$ as

$$\mathrm{INV}_{\mathbb{R}}([A]) = \begin{cases} 0 + \mathbb{Z} & \text{if } [A] = [\mathbb{R}] \\ 1/2 + \mathbb{Z} & \text{if } [A] = [\mathbb{H}] \end{cases} \qquad \text{and}$$
$$\mathrm{INV}_{\mathbb{C}}([A]) = 0 + \mathbb{Z}.$$

Similar to what we did for infinite local fields F, we will also use the notations $\mathrm{INV}_{\mathbb{R}}$ and $\mathrm{INV}_{\mathbb{C}}$ for the corresponding maps $\mathbf{CSA}(\mathbb{R}) \to (1/2)\mathbb{Z}/\mathbb{Z}$ and $\mathbf{CSA}(\mathbb{C}) \to \{0 + \mathbb{Z}\}$, respectively.

Let F be an algebraic number field. Theorem 5.2 implies that $\hat{F}_v$ is an infinite local field for discrete $v \in \mathbf{V}(F)$, and it also implies that $\hat{F}_v$ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ for archimedean $v \in \mathbf{V}(F)$. An archimedean valuation v of F is called *real* when $\hat{F}_v \cong \mathbb{R}$ and *complex* when $\hat{F}_v \cong \mathbb{C}$. We conclude that all valuations of F are either discrete, real or complex. This distinction is called the *type* of a valuation v of F.

Define the subgroup $I_v(F)$ of $\mathbb{Q}/\mathbb{Z}$ for F an algebraic number field and $v \in \mathbf{V}(F)$ as

$$I_v(F) = \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } v \text{ is discrete,} \\ (1/2)\mathbb{Z}/\mathbb{Z} & \text{if } v \text{ is real,} \\ \{0 + \mathbb{Z}\} & \text{if } v \text{ is complex.} \end{cases}$$

If v is real or complex, then we define $\mathrm{INV}_{\hat{F}_v} : \mathbf{CSA}(\hat{F}_v) \to I_v(F)$ as the map analogous to $\mathrm{INV}_{\mathbb{R}}$ or $\mathrm{INV}_{\mathbb{C}}$, respectively. We have now defined $\mathrm{INV}_{\hat{F}_v} : \mathbf{CSA}(\hat{F}_v) \to I_v(F)$ for all valuations $v \in \mathbf{V}(F)$. To simplify notation, we will write INV_v for both $\mathrm{INV}_{\hat{F}_v}$ and the corresponding homomorphism from $\mathbf{B}(\hat{F}_v)$ to $I_v(F)$.

For $A \in \mathbf{CSA}(F)$ and $v \in \mathbf{V}(F)$, $\mathrm{INV}_v(A \otimes \hat{F}_v)$ is called the *local invariant of A at v*. The map $\mathrm{INV}^{(F)} : \mathbf{CSA}(F) \to \prod_{v \in \mathbf{V}(F)} I_v(F)$ defined as

$$\mathrm{INV}^{(F)} A = \Big(\mathrm{INV}_v(A \otimes \hat{F}_v)\Big)_{v \in \mathbf{V}(F)}$$

is called the *global invariant of A*. Since $\mathrm{INV}^{(F)} A$ is equal to $\mathrm{INV}^{(F)} B$ when $A \sim B$, $\mathrm{INV}^{(F)}$ can also be viewed as a map from $\mathbf{B}(F)$ to $\prod_{v \in \mathbf{V}(F)} I_v(F)$. In this context, $\mathrm{INV}^{(F)}$ is a group homomorphism, since each coordinate map $[A] \mapsto \mathrm{INV}_v(A \otimes \hat{F}_v)$ is a composition of the homomorphisms $\mathrm{INV}_v : \mathbf{B}(\hat{F}_v) \to I_v(F)$ and $\kappa_* : \mathbf{B}(F) \to \mathbf{B}(\hat{F}_v)$ defined by $[A] \mapsto [A \otimes \hat{F}_v]$. We will use the same notation $\mathrm{INV}^{(F)}$ in both contexts.

We can now finally rephrase the AHBN-Theorem in the following form.

Theorem 5.11 (Rephrased AHBN-Theorem)**.** *If F is an algebraic number field, then $\mathrm{INV}^{(F)} : \mathbf{B}(F) \to \prod_{v \in \mathbf{V}(F)} I_v(F)$ is an injective group homomorphism.*

The AHBN-Theorem is equivalent to the claim that $\mathrm{INV}^{(F)}$ is injective.

The following corollary is a direct consequence of the Rephrased AHBN-Theorem and Theorem 2.35.

Corollary 5.12. *Let F be an algebraic number field and $A, B \in \mathbf{CSA}(F)$.*

i) $A \sim B$ if and only if $\mathrm{INV}^{(F)} A = \mathrm{INV}^{(F)} B$.

ii) $A \cong B$ if and only if $\mathrm{INV}^{(F)} A = \mathrm{INV}^{(F)} B$ and $\mathrm{Deg}\, A = \mathrm{Deg}\, B$.

5.3 Examples of the Global Invariant

We would like to determine the value of $\mathrm{INV}^{(F)} A$ for some algebraic number field F and $A \in \mathbf{CSA}(F)$. We already know that $A \sim F$ implies that $\left(\mathrm{INV}^{(F)} A\right)_v = 0 + \mathbb{Z}$ for all $v \in \mathbf{V}(F)$, but a non-trivial example should be more interesting. Determining $\mathrm{INV}^{(F)} A$ is quite difficult to do in general, so we will start with quaternion algebras over $\mathbb{Q}$.

Suppose that a and b are elements of $\mathbb{Q}^\circ$. In order to determine $\mathrm{INV}^{(\mathbb{Q})}\left(\frac{a,b}{\mathbb{Q}}\right)$, we need to determine $\mathrm{INV}_v\left(\left(\frac{a,b}{\mathbb{Q}}\right) \otimes_{\mathbb{Q}} \hat{\mathbb{Q}}_v\right)$ for all $v \in \mathbf{V}(\mathbb{Q})$. First, we note that $\left(\frac{a,b}{\mathbb{Q}}\right) \otimes_{\mathbb{Q}} \hat{\mathbb{Q}}_v$ is isomorphic to $\left(\frac{a,b}{\hat{\mathbb{Q}}_v}\right)$ by definition of the quaternion algebra. This implies that we need to determine $\mathrm{INV}_{v_\infty}\left(\frac{a,b}{\mathbb{R}}\right)$ and $\mathrm{INV}_{v_p}\left(\frac{a,b}{\hat{\mathbb{Q}}_p}\right)$ for all primes p. Section 4.7 describes a way to calculate $\mathrm{INV}_{v_p}\left(\frac{a,b}{\hat{\mathbb{Q}}_p}\right)$, so we will focus on $\mathrm{INV}_{v_\infty}\left(\frac{a,b}{\mathbb{R}}\right)$ for now.

The map INV_{v_∞} was defined as

$$\mathrm{INV}_{v_\infty}\left(\frac{a,b}{\mathbb{R}}\right) = \begin{cases} 0+\mathbb{Z} & \text{if } \left(\frac{a,b}{\mathbb{R}}\right) \sim \mathbb{R}, \\ \frac{1}{2}+\mathbb{Z} & \text{if } \left(\frac{a,b}{\mathbb{R}}\right) \sim \mathbb{H}. \end{cases}$$

Note that $\left(\frac{a,b}{\mathbb{R}}\right) \sim \mathbb{H}$ is equivalent to the equality $\mathrm{Ind}\left(\frac{a,b}{\mathbb{R}}\right) = \mathrm{Deg}\left(\frac{a,b}{\mathbb{R}}\right) = 2$, which is equivalent to the claim that $\left(\frac{a,b}{\mathbb{R}}\right)$ is a division algebra. Theorem 2.20 states that $\left(\frac{a,b}{\mathbb{R}}\right)$ is a division algebra precisely when $c_0^2 = ac_1^2 + bc_2^2$ has no non-trivial solution with $c_0, c_1, c_2 \in \mathbb{R}$. We conclude that

$$\mathrm{INV}_{v_\infty}\left(\frac{a,b}{\mathbb{R}}\right) = \begin{cases} 0+\mathbb{Z} & \text{if } a > 0 \text{ or } b > 0 \\ \frac{1}{2}+\mathbb{Z} & \text{if } a < 0 \text{ and } b < 0. \end{cases}$$

Consider the quaternion algebras $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\left(\frac{3,5}{\mathbb{Q}}\right)$. From our previous calculations in Section 4.7 and our newfound knowledge on INV_{v_∞} we conclude that

$$\left(\mathrm{INV}^{(\mathbb{Q})}\left(\frac{-1,-1}{\mathbb{Q}}\right)\right)_v = \begin{cases} 0+\mathbb{Z} & \text{if } v \neq v_2 \text{ and } v \neq v_\infty, \\ \frac{1}{2}+\mathbb{Z} & \text{if } v = v_2 \text{ or } \quad v = v_\infty, \end{cases} \tag{5.1}$$

$$\left(\mathrm{INV}^{(\mathbb{Q})}\left(\frac{3,5}{\mathbb{Q}}\right)\right)_v = \begin{cases} 0+\mathbb{Z} & \text{if } v \neq v_3 \text{ and } \quad v \neq v_5, \\ \frac{1}{2}+\mathbb{Z} & \text{if } v = v_3 \text{ or } v = v_5 \end{cases} \tag{5.2}$$

holds for all $v \in \mathbf{V}(\mathbb{Q})$.

We will use the following theorem to further study these examples.

Theorem 5.13. *Let K/F be an extension of algebraic number fields and suppose that A is an element of $\mathbf{CSA}(F)$.*

i) For all $v \in \mathbf{V}(F)$ and $w \in \mathbf{V}(K)$ such that $w|v$,

$$\mathrm{INV}_w(A^K \otimes_K \hat{K}_w) = [\hat{K}_w : \hat{F}_v]\,\mathrm{INV}_v(A \otimes_F \hat{F}_v).$$

ii) K splits A if and only if $[\hat{K}_w : \hat{F}_v]\,\mathrm{INV}_v(A \otimes_F \hat{F}_v) = 0 + \mathbb{Z}$ for all $v \in \mathbf{V}(F)$ and $w \in \mathbf{V}(K)$ such that $w|v$.

Proof. For discrete v, part i) follows from Theorem 4.55. The cases where v is an archimedean valuation are fairly straightforward, see for instance the proof of Lemma 18.4 of [Pierce, 1982]. Part ii) follows from part i) and the Rephrased AHBN-Theorem. □

This theorem implies that in order to determine $\mathrm{INV}^{(F)}\left(\frac{a,b}{F}\right)$ for an algebraic number field F and $a, b \in \mathbb{Q}^\circ$, it suffices to know $\mathrm{INV}^{(\mathbb{Q})}\left(\frac{a,b}{\mathbb{Q}}\right)$, the $w \in \mathbf{V}(F)$ that divide each $v_p \in \mathbf{V}(\mathbb{Q})$, and the local degree $[\hat{F}_w : \hat{\mathbb{Q}}_{v_p}]$ for each $w \in \mathbf{V}(F)$ that divides $v_p \in \mathbf{V}(\mathbb{Q})$. The second part of this theorem describes a way to check which algebraic number fields F split $\left(\frac{a,b}{\mathbb{Q}}\right)$. We will give an example of this method by finding some splitting fields of quaternion algebras over $\mathbb{Q}$.

To keep things simple, we only consider fields F with $[F : \mathbb{Q}] = 2$. The fields F with $[F : \mathbb{Q}]$ equal to 2 are called *quadratic fields*, and it is trivial to see that they are all of the form $\mathbb{Q}(\sqrt{d})$ for some square-free integer d unequal to 0 and 1.

Let d be a square-free integer unequal to 0 and 1, and suppose that $a, b \in \mathbb{Q}^\circ$. Since by definition of quaternion algebras $\left(\frac{a,b}{E}\right)$ is isomorphic to $\left(\frac{a,b}{\mathbb{Q}}\right)^E$ for any field extension $E/\mathbb{Q}$, Theorem 5.13 implies that

$$\mathrm{INV}_w\left(\left(\frac{a,b}{\mathbb{Q}(\sqrt{d})}\right) \otimes_{\mathbb{Q}(\sqrt{d})} \widehat{\mathbb{Q}(\sqrt{d})}_w\right) = [\widehat{\mathbb{Q}(\sqrt{d})}_w : \hat{\mathbb{Q}}_{v_p}]\,\mathrm{INV}_{v_p}\left(\left(\frac{a,b}{\hat{\mathbb{Q}}_{v_p}}\right)\right)$$

for all p prime or $p = \infty$ and $w \in \mathbf{V}(\mathbb{Q}(\sqrt{d}))$ that divide v_p. We need to determine the degree $[\widehat{\mathbb{Q}(\sqrt{d})}_w : \hat{\mathbb{Q}}_{v_p}]$ and the number of $w \in \mathbf{V}(\mathbb{Q}(\sqrt{d}))$ that divide each $v_p \in \mathbf{V}(\mathbb{Q})$. Fortunately, these two problems are closely related. The degree $[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}]$ is equal to 2, so Lemma 5.1 yields that each v_p has either one or two distinct extensions to $\mathbb{Q}(\sqrt{d})$, and the sum of their local degrees $[\widehat{\mathbb{Q}(\sqrt{d})}_w : \hat{\mathbb{Q}}_{v_p}]$ is equal to 2. This means that either there exists one $w \in \mathbf{V}(\mathbb{Q}(\sqrt{d}))$ that divides v_p and $[\widehat{\mathbb{Q}(\sqrt{d})}_w : \hat{\mathbb{Q}}_{v_p}] = 2$, or there exist two distinct $w_1, w_2 \in \mathbf{V}(\mathbb{Q}(\sqrt{d}))$ that divide v_p and $[\widehat{\mathbb{Q}(\sqrt{d})}_{w_1} : \hat{\mathbb{Q}}_{v_p}] = [\widehat{\mathbb{Q}(\sqrt{d})}_{w_2} : \hat{\mathbb{Q}}_{v_p}] = 1$.

How do we determine the degree $[\widehat{\mathbb{Q}(\sqrt{d})}_w : \hat{\mathbb{Q}}_{v_p}]$ when $w \in \mathbf{V}(\mathbb{Q}(\sqrt{d}))$ divides the valuation $v_p \in \mathbf{V}(\mathbb{Q})$? Note that $[\widehat{\mathbb{Q}(\sqrt{d})}_w : \hat{\mathbb{Q}}_{v_p}]$ is equal to 1 precisely when $\widehat{\mathbb{Q}(\sqrt{d})}_w$ is

equal to $\hat{\mathbb{Q}}_{v_p}$, which is true precisely when the minimal polynomial $\Phi_{\sqrt{d}} \in \mathbb{Q}[\mathbf{x}]$, defined as $\Phi_{\sqrt{d}}(\mathbf{x}) = \mathbf{x}^2 - d$, has a root in $\hat{\mathbb{Q}}_{v_p}$. We therefore need to determine for which p prime or $p = \infty$ the integer d is the square of some $c \in \hat{\mathbb{Q}}_{v_p}$.

Theorem 5.14. *Let p be a prime number or ∞. A square-free integer $d \neq 0, 1$ is a square in $\hat{\mathbb{Q}}_{v_p}$ precisely when one of the following holds:*

i) $p = 2$ and $\overline{d} = \overline{1}$ in $\mathbb{Z}/8\mathbb{Z}$.

ii) p is an odd prime that does not divide d and $\overline{d}$ is a square in $\mathbb{Z}/p\mathbb{Z}$.

iii) $p = \infty$ and $d > 0$.

Proof. In each of the following cases, let $w \in \mathbf{V}(\mathbb{Q}(\sqrt{d})$ be a valuation that divides v_p.

The case $p = \infty$ is trivial, since it is clear that d is the square of some $c \in \hat{\mathbb{Q}}_{v_p} = \mathbb{R}$ if and only if d is positive.

We now consider the case where p divides d. The fact that d is square-free implies that p^2 does not divide d, so $w(\sqrt{d})^2 = v_p(d) = p^{-1}$ gives that $w(\sqrt{d})$ is equal to $p^{-1/2}$. This means that $w(\widehat{\mathbb{Q}(\sqrt{d})_w})$ is strictly larger than $v_p(\hat{\mathbb{Q}}_p) = v_p(\mathbb{Q}) = \{p^m |\ m \in \mathbb{Z}\}$, so the ramification index $e_w(\widehat{\mathbb{Q}(\sqrt{d})_w}/\hat{\mathbb{Q}}_p)$ is by definition larger than 1. Theorem 4.36 implies that

$$e_w(\widehat{\mathbb{Q}(\sqrt{d})_w}/\hat{\mathbb{Q}}_p) \leq [\widehat{\mathbb{Q}(\sqrt{d})_w} : \hat{\mathbb{Q}}_p],$$

so $[\widehat{\mathbb{Q}(\sqrt{d})_w} : \hat{\mathbb{Q}}_p]$ and $e_w(\widehat{\mathbb{Q}(\sqrt{d})_w}/\hat{\mathbb{Q}}_p)$ are both equal to 2. We conclude that d is not a square in $\hat{\mathbb{Q}}_p$ in this case.

The third case that we consider is the case where p is an odd prime that does not divide d. Note that any $c \in \hat{\mathbb{Q}}_p$ with $c^2 = d$ satisfies $v_p(c) = \sqrt{v_p(d)} = 1$. We would like to apply Hensel's Lemma. The minimal polynomial $\Phi_{\sqrt{d}}$ is clearly an element of $O(\hat{\mathbb{Q}}_p, v_p)[\mathbf{x}]$ and $E(\hat{\mathbb{Q}}_p, v_p)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ by Theorem 4.12 and Corollary 4.25. Note that $\overline{\Phi_{\sqrt{d}}}(\mathbf{x}) = \mathbf{x}^2 - \overline{d}$ and $\overline{\Phi'_{\sqrt{d}}}(\mathbf{x}) = \overline{2}\mathbf{x}$ imply that $\overline{\Phi_{\sqrt{d}}}$ and $\overline{\Phi'_{\sqrt{d}}}$ are relatively prime in $E(\hat{\mathbb{Q}}_p, v_p)[\mathbf{x}]$. Hensel's Lemma then implies that $\Phi_{\sqrt{d}}$ has a root $c \in \hat{\mathbb{Q}}_p$ precisely when $\overline{\Phi_{\sqrt{d}}}$ has a root in $E(\hat{\mathbb{Q}}_p, v_p) \cong \mathbb{Z}/p\mathbb{Z}$, so if and only if $\overline{d}$ is a square in $\mathbb{Z}/p\mathbb{Z}$.

The fourth and final case is the one where $p = 2$ and d is odd. Suppose that c is an element of $\hat{\mathbb{Q}}_2$ with $c^2 = d$. It is clear that $v_2(c) = \sqrt{v_2(d)} = 1$, so c has a 2-adic expansion $\sum_{k=0}^{\infty} a_k 2^k$ by Theorem 4.27. If we define $c_2 = a_0 + a_1 2 + a_2 2^2 \in \mathbb{Z}$, then $c^2 = d$ implies that c_2^2 is equivalent to d modulo 8. The only squares in $\mathbb{Z}/8\mathbb{Z}$ are $\overline{0}$, $\overline{1}$ and $\overline{4}$, so the fact that d is square-free implies that d is equivalent to 1 modulo 8.

Now suppose that d satisfies $d \equiv 1 \mod 8$. Then d is equal to $8k + 1$ for some $k \in \mathbb{Z}$, and if there exists $a \in O(\hat{\mathbb{Q}}_2, v_2)$ such that $(2a + 1)^2$ is equal to $d = 8k + 1$, then d is a square in $\hat{\mathbb{Q}}_2$. After simplifying, this means that it would suffice to find a solution $a \in O(\hat{\mathbb{Q}}_2, v_2)$ to the equation $\mathbf{x}^2 + \mathbf{x} - 2k = 0$. Let $\Psi_k \in O(\hat{\mathbb{Q}}_2, v_2)[\mathbf{x}]$ be defined as $\Psi_k(\mathbf{x}) = \mathbf{x}^2 + \mathbf{x} - 2k$. The residue class field $E(\hat{\mathbb{Q}}_2, v_2)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ by Theorem 4.12 and Corollary 4.25, and $\overline{\Psi_k}$ and $\overline{\Psi'_k}$ are relatively prime, since

$\overline{\Psi_k}(\mathbf{x}) = \mathbf{x}^2 + \mathbf{x}$ and $\overline{\Psi_k'}(\mathbf{x}) = 1$. Hensel's Lemma now implies that the root $\overline{1}$ of $\overline{\Psi_k}$ can be lifted to a root $a \in O(\hat{\mathbb{Q}}_2, v_2)$ of Ψ_k with $\overline{a} = \overline{1}$. In other words, d is equal to $(2a+1)^2$ in $\hat{\mathbb{Q}}_2$. $\square$

We can now determine the quadratic fields $\mathbb{Q}(\sqrt{d})$ that split $\left(\frac{a,b}{\mathbb{Q}}\right)$ with $a, b \in \mathbb{Q}^\circ$ in the following way. We first determine the set $X_{a,b}$ of $v_p \in \mathbf{V}(\mathbb{Q})$ such that $\left(\mathrm{INV}^{(\mathbb{Q})}\left(\frac{a,b}{\mathbb{Q}}\right)\right)_{v_p}$ is equal to $1/2 + \mathbb{Z}$. If d is a square-free integer unequal to 0 and 1, then Theorem 5.13 implies that $\mathbb{Q}(\sqrt{d})$ splits $\left(\frac{a,b}{\mathbb{Q}}\right)$ precisely when $[\widehat{\mathbb{Q}(\sqrt{d})}_w : \hat{\mathbb{Q}}_{v_p}] = 2$ for all $w \in \mathbf{V}(\mathbb{Q}(\sqrt{d})$ that divide some $v_p \in X$. The local degree $[\widehat{\mathbb{Q}(\sqrt{d})}_w : \hat{\mathbb{Q}}_{v_p}]$ is equal to 2 precisely when d is not a square in $\hat{\mathbb{Q}}_{v_p}$, and Theorem 5.14 precisely describes when this occurs.

If we consider the quaternion algebras $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\left(\frac{3,5}{\mathbb{Q}}\right)$, then (5.1) and (5.2) imply that $X_{-1,-1} = \{v_2, v_\infty\}$ and $X_{3,5} = \{v_3, v_5\}$. Suppose that d is a square-free integer with $d \neq 0, 1$. We conclude from our procedure that $\mathbb{Q}(\sqrt{d})$ splits $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ if and only if $d < 0$ and $d \not\equiv 1 \mod 8$, and that $\mathbb{Q}(\sqrt{d})$ splits $\left(\frac{3,5}{\mathbb{Q}}\right)$ if and only if $\overline{d}$ is either $\overline{0}$ or not a square in $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}$. The squares in $\mathbb{Z}/3\mathbb{Z}$ are precisely $\overline{0}$ and $\overline{1}$, and the squares in $\mathbb{Z}/5\mathbb{Z}$ are $\overline{0}$, $\overline{1}$ and $\overline{4}$, so the Chinese Remainder Theorem implies that $\mathbb{Q}(\sqrt{d})$ splits $\left(\frac{3,5}{\mathbb{Q}}\right)$ precisely when d is equivalent to 0, 2, 3, 5, 8 or 12 modulo 15.

5.4 Brauer Groups of Algebraic Number Fields

The Rephrased AHBN-Theorem states that the Brauer group of an algebraic number field can be embedded in an infinite product of additive groups $I_v(F)$. The following theorem describes this embedding in more detail.

Theorem 5.15. *Let F be an algebraic number field. Define $\mathbf{I}(F) = \bigoplus_{v \in \mathbf{V}(F)} I_v(F)$ and $\gamma : \mathbf{I}(F) \to \mathbb{Q}/\mathbb{Z}$ as $\gamma\left((t_v)_{v \in \mathbf{V}(F)}\right) = \sum_{v \in \mathbf{V}(F)} t_v$. The sequence*

$$1 \to \mathbf{B}(F) \overset{\mathrm{INV}^{(F)}}{\to} \mathbf{I}(F) \overset{\gamma}{\to} \mathbb{Q}/\mathbb{Z} \to 1$$

is a short exact sequence of groups.

We will later show that the map $\mathrm{INV}^{(F)}$ is still well-defined with $\mathbf{I}(F)$ instead of $\prod_{v \in \mathbf{V}(F)} I_v(F)$ as the codomain. The injectivity of $\mathrm{INV}^{(F)}$ follows from the Rephrased AHBN-Theorem. Surjectivity of γ is obvious, since if we let $v \in \mathbf{V}(F)$ be discrete, then $I_v(F) = \mathbb{Q}/\mathbb{Z}$ implies that $\gamma(\mathbf{I}(F))$ contains $\gamma(I_v(F)) = \mathbb{Q}/\mathbb{Z}$. To complete the proof of Theorem 5.15, we also still need to prove that $\operatorname{Im} \mathrm{INV}^{(F)} = \operatorname{Ker} \gamma$.

The remainder of the proof of this theorem is split into three separate theorems. The first theorem states that $\operatorname{Im} \mathrm{INV}^{(F)}$ is actually a subset of $\mathbf{I}(F)$. The second theorem states that $\operatorname{Im} \mathrm{INV}^{(F)}$ is a subset of $\operatorname{Ker} \gamma$, and the third theorem states that $\operatorname{Ker} \gamma$ is a subset of $\operatorname{Im} \mathrm{INV}^{(F)}$. Each of these theorems will be proven in a separate subsection.

Proving Theorem 5.15 from scratch is beyond the scope of this thesis, so we will use three classical theorems from algebraic number theory: the Grunwald-Wang Theorem, Artin's Reciprocity Law, and Chebotarev's Density Theorem. We will refer to other texts for the proofs of these three theorems.

5.4.1 The Image of the Global Invariant

In this section we will prove the following theorem as part of the proof of Theorem 5.15.

Theorem 5.16. *Let F be an algebraic number field. For all algebras $A \in \mathbf{CSA}(F)$ $\mathrm{INV}_v(A \otimes \hat{F}_v) = 0 + \mathbb{Z}$ for almost all $v \in \mathbf{V}(F)$.*

It was already clear that each $\mathrm{INV}_v(A \otimes \hat{F}_v)$ is an element of $I_v(F)$ for each $v \in \mathbf{V}(F)$, so this theorem implies that the image of the global invariant $\mathrm{INV}^{(F)}$ is a subset of $\mathbf{I}(F)$. We need the following lemma to prove this theorem.

Lemma 5.17. *If K/F is a Galois extension of algebraic number fields, then $e_w(K/F)$ is equal to 1 for almost all $w \in \mathbf{V}(K)$.*

Proof. The proof of this lemma is quite technical and of little interest to us, so we refer to the proof of Lemma 18.5 from [Pierce, 1982] for the details. □

Proof of Theorem 5.16. Since $\mathrm{INV}^{(F)}$ is constant on equivalence classes in $\mathbf{B}(F)$, we may as well assume that A is a crossed product (K, G, Φ) with K/F a Galois extension, $G = \mathbf{G}(K/F)$ and $\Phi \in Z^2(G, K^\circ)$. Theorems 5.2 and 5.7 and Lemma 5.17 together imply the existence of some finite set $X \subseteq \mathbf{V}(F)$ such that for all $v \in \mathbf{V}(F) \setminus X$ and $w \in \mathbf{V}(K)$ dividing v, v is discrete, $\hat{K}_w/\hat{F}_v$ is unramified and $w(\Phi(\rho, \tau)) = 1$ for all $\rho, \tau \in G$. We will prove that $\mathrm{INV}_v(A \otimes \hat{F}_v) = 0 + \mathbb{Z}$ for all $v \in \mathbf{V}(F) \setminus X$.

Let $v \in \mathbf{V}(F) \setminus X$ and suppose that $w \in \mathbf{V}(K)$ divides v. We can identify K with a subfield of $\hat{K}_w$ such that $\hat{K}_w = K\hat{F}_v$. Since $\hat{F}_v$ is an infinite local field and the extension $\hat{K}_w/\hat{F}_v$ is unramified, Theorem 4.47 implies that $\hat{K}_w/\hat{F}_v$ is cyclic with the Frobenius automorphism σ generating $H = \mathbf{G}(\hat{K}_w/\hat{F}_v)$. Let k be the degree of $\hat{K}_w/\hat{F}_v$.

By definition of the crossed product, there exists a K-basis $\{u_\tau | \tau \in G\}$ of A such that $A = \bigoplus_{\tau \in G} u_\tau K$, $u_\tau^{-1} d u_\tau = d^\tau$ for all $d \in K$ and $\tau \in G$, and $u_\rho u_\tau = u_{\rho\tau}\Phi(\rho, \tau)$ for all $\rho, \tau \in G$. Corollary 3.29 implies that $A \otimes \hat{F}_v \sim (\hat{K}_w, H, \Phi|_{H^2}) = \bigoplus_{i=0}^{k-1} u_{\sigma^i} \hat{K}_w$.

From the definition of the product in A we find that

$$
\begin{aligned}
u_\sigma^0 &= 1_A = u_{1_G}\Phi(1_G, 1_G)^{-1} = u_{\sigma^0}\Phi(1_G, 1_G)^{-1};\\
u_\sigma^1 &= u_\sigma;\\
u_\sigma^2 &= u_{\sigma^2}\Phi(\sigma, \sigma);\\
u_\sigma^3 &= u_\sigma u_\sigma^2 = u_\sigma\left(u_{\sigma^2}\Phi(\sigma, \sigma)\right) = u_{\sigma^3}\Phi(\sigma, \sigma^2)\Phi(\sigma, \sigma);\\
u_\sigma^4 &= u_\sigma u_\sigma^3 = u_\sigma u_{\sigma^3}\Phi(\sigma, \sigma^2)\Phi(\sigma, \sigma) = u_{\sigma^4}\Phi(\sigma, \sigma^3)\Phi(\sigma, \sigma^2)\Phi(\sigma, \sigma);\\
&\vdots\\
u_\sigma^{k-1} &= u_\sigma u_\sigma^{k-2} = u_{\sigma^{k-1}}\Phi(\sigma, \sigma^{k-2})\Phi(\sigma, \sigma^{k-3})\cdots\Phi(\sigma, \sigma).
\end{aligned}
$$

Since $\Phi(\rho,\tau)$ is by definition an element of K° for all $\rho,\tau \in G$, these equations imply that $\bigoplus_{i=0}^{k-1} u_{\sigma^i}\hat{K}_w = \bigoplus_{i=0}^{k-1}(u_\sigma)^i\hat{K}_w$.

If we continue this sequence of equations, we can use Lemma 3.18 to find that

$$\begin{aligned} u_\sigma^k &= u_{\sigma^k}\Phi(\sigma,\sigma^{k-1})\Phi(\sigma,\sigma^{k-2})\cdots\Phi(\sigma,\sigma) \\ &= u_{1_G}\Phi(\sigma,\sigma^{k-1})\Phi(\sigma,\sigma^{k-2})\cdots\Phi(\sigma,\sigma) \\ &= \Phi(1_G,1_G)\Phi(\sigma,\sigma^{k-1})\Phi(\sigma,\sigma^{k-2})\cdots\Phi(\sigma,\sigma), \end{aligned}$$

so u_σ^k is an element of K°. Since u_σ^k clearly commutes with u_σ^i for all $0 \leq i < k$, u_σ^k is an element of the center of $(\hat{K}_w, H, \Phi|_{H^2}) \in \mathbf{CSA}(\hat{F}_v)$. Define $a \in \hat{F}_v \cap K^\circ$ as $a = u_\sigma^k$. Theorem 3.37 implies that $(\hat{K}_w, H, \Phi|_{H^2}) \cong (\hat{K}_w, \sigma, a)$. Since $w(\Phi(\rho,\tau))$ is equal to 1 for all $\rho,\tau \in G$, $v(a) = w(a)$ is equal to 1, so $a \in N_{\hat{K}_w/\hat{F}_v}(\hat{K}_w^\circ)$ by Lemma 4.48. Thus, part v) of Theorem 3.38 yields that $A \otimes \hat{F}_v \sim (\hat{K}_w, \sigma, a) \sim \hat{F}_v$, so $\mathrm{INV}_v(A \otimes \hat{F}_v) = 0 + \mathbb{Z}$ for all $v \in \mathbf{V}(F) \setminus X$. □

Theorem 5.16 has some interesting implications for splitting fields of algebraic number fields. Theorem 5.13 states that for an extension of algebraic number fields K/F and an algebra $A \in \mathbf{CSA}(F)$, K splits A if and only if $[\hat{K}_w : \hat{F}_v]\,\mathrm{INV}_v(A \otimes \hat{F}_v) = 0 + \mathbb{Z}$ for all $w \in \mathbf{V}(K)$ and $v \in \mathbf{V}(F)$ such that $w|v$. Theorem 5.16 implies that this condition is automatically fulfilled for almost all $v \in \mathbf{V}(F)$. Since for each $v \in \mathbf{V}(F)$ there exist only finitely many $w \in \mathbf{V}(K)$ that divide v, this means that we only need to consider a finite amount of local degrees $[\hat{K}_w : \hat{F}_v]$ to determine whether the field K splits A or not. Furthermore, if K/F is Galois, then the local degree $[\hat{K}_w : \hat{F}_v] = [\hat{K}_v : \hat{F}_v]$ is independent of the choice of $w \in \mathbf{V}(K)$ that divides v, further reducing the amount of conditions to check.

We can combine this realization with the Grunwald-Wang Theorem.

Theorem 5.18 (Grunwald-Wang Theorem)**.** *Let F be an algebraic number field, and let $\{(v_1,n_1),\ldots,(v_r,n_r)\}$ be a finite set of pairs such that $v_i \in \mathbf{V}(F)$, $n_i \in \mathbb{N}$, $n_i \leq 2$ when v_i is real, and $n_i = 1$ when v_i is complex. Let m be the least common multiple of $\{n_1,\ldots,n_r\}$. If $n \in \mathbb{N}$ is a multiple of m, then there is a cyclic extension K/F of degree n such that n_i divides $[\hat{K}_{v_i} : \hat{F}_{v_i}]$ for $1 \leq i \leq r$. If n is a multiple of $2m$, then K can be chosen such that $\hat{K}_{v_i}/\hat{F}_{v_i}$ is unramified for all v_i that are discrete.*

Proof. See for instance Chapter 10 of [Artin and Tate, 1952] for a full discussion of the Grunwald-Wang Theorem and its proof. □

In particular, for any algebraic number field F and algebra $A \in \mathbf{CSA}(F)$, this theorem implies the existence of a cyclic extension K/F of relatively small degree $[K : F]$ such that K splits A. Furthermore, with a slight increase in degree K can even be chosen such that $\hat{K}_v/\hat{F}_v$ is unramified for all discrete $v \in \mathbf{V}(F)$ with $\mathrm{INV}_v(A \otimes \hat{F}_v) \neq 0 + \mathbb{Z}$. We will make use of this fact in the following two subsections.

5.4.2 Artin Reciprocity

In this section, we prove the following theorem as part of the proof of Theorem 5.15.

Theorem 5.19. *If F is an algebraic number field, then $\sum_{v\in\mathbf{V}(F)} \mathrm{INV}_v(A\otimes\hat{F}_v) = 0+\mathbb{Z}$ for all $A\in\mathbf{CSA}(F)$.*

To proof this theorem, we will make use of Artin's Reciprocity Law. We start by discussing this law.

Let F be an algebraic number field. The *idele group of* F is the subgroup J_F of $\prod_{v\in\mathbf{V}(F)}\hat{F}_v^\circ$ consisting of those elements $(y_v)_{v\in\mathbf{V}(F)}$ such that $v(y_v)=1$ for almost all $v\in\mathbf{V}(F)$. If x is an element of F°, then $v(x)=1$ for almost all $v\in\mathbf{V}(F)$ by Theorem 5.7. This implies that the diagonal map $x\mapsto(x)_{v\in\mathbf{V}(F)}$ embeds F° into the idele group J_F. We identify F° with the image of this embedding.

Let K/F be a Galois extension of algebraic number fields with valuations $v\in\mathbf{V}(F)$ and $w\in\mathbf{V}(K)$ such that $w|v$. For convenience, we write N_w for the field norm $N_{\hat{K}_w/\hat{F}_v}$. The maps N_w can be used to define a homomorphism $N: J_K\to J_F$ as

$$(z_w)_{w\in\mathbf{V}(K)}\mapsto\left(\prod_{w|v}N_w(z_w)\right)_{v\in\mathbf{V}(F)}.$$

Indeed, if $w\in\mathbf{V}(K)$ satisfies $w(z_w)=1$, then $w(N_w(z_w))=\prod_{\sigma\in\mathbf{G}(\hat{K}_w/\hat{F}_v)}w(z_w^\sigma)=1$ by Corollary 4.33 and the definition of N_w. If $v\in\mathbf{V}(F)$ has the property that $w(z_w)=1$ for all $w\in\mathbf{V}(K)$ that divide v, then $v\left(\prod_{w|v}N_w(z_w)\right)=\prod_{w|v}w(N_w(z_w))=1$ as well. Since there exist only finitely many $w\in\mathbf{V}(K)$ with $w(z_w)\neq 1$, there are only finitely many $v\in\mathbf{V}(F)$ with $v\left(\prod_{w|v}N_w(z_w)\right)\neq 1$.

By Lemma 5.3, the structure of $\hat{K}_w$ as a $\hat{F}_v$-algebra is independent of the choice of w that divides $v\in\mathbf{V}(F)$, which implies that $N_w(\hat{K}_w^\circ)$ is also independent of this choice. We will therefore often write $\hat{K}_v$ for $\hat{K}_w$ and $N_v(\hat{K}_v^\circ)$ for $N_w(\hat{K}_w^\circ)$.

We are now ready to state Artin's Reciprocity Law.

Theorem 5.20 (Artin's Reciprocity Law)**.** *Suppose that K/F is a Galois extension of algebraic number fields such that $\mathbf{G}(K/F)$ is abelian. There exists a group homomorphism $\alpha: J_F\to\mathbf{G}(K/F)$ such that*

$$1\to N(J_K)F^\circ\to J_F\xrightarrow{\alpha}\mathbf{G}(K/F)\to 1$$

is a short exact sequence.

Proof. This theorem is for instance proven as part of Main Theorem 5.1 on page 172 of [Cassels and Fröhlich, 1986]. □

The map α is called the *Artin mapping*. For $v\in\mathbf{V}(F)$, denote the restriction of α to the component $\hat{F}_v^\circ$ of J_F as α_v. Such a map $\alpha_v:\hat{F}_v^\circ\to\mathbf{G}(K/F)$ is called a *local Artin mapping*. Note that $\alpha_v(x_v)=1_{\mathbf{G}(K/F)}$ for all $x_v\in N_v(\hat{K}_v^\circ)$. If $\hat{K}_v/\hat{F}_v$ is unramified,

then Lemma 4.48 implies that all $x_v \in \hat{F}_v$ with $v(x_v) = 1$ are elements of $N_v(\hat{K}_v^\circ)$. Since $\mathbf{G}(K/F)$ is abelian, this implies that $\prod_{v \in \mathbf{V}(F)} \alpha_v$ is a homomorphism from J_F to $\mathbf{G}(K/F)$. As seen in result 6.3 from [Cassels and Fröhlich, 1986, p. 175], this product of local Artin mappings $\prod_{v \in \mathbf{V}(F)} \alpha_v$ is actually equal to the global Artin mapping α.

For the proof of the main theorem of this section, we will need a description of α_v in two cases: when v is discrete and K/F is unramified at v, as well as when v is archimedean, K/F is cyclic and $[\hat{K}_v : \hat{F}_v] = 2$. The descriptions of these local Artin mappings were paraphrased from [Pierce, 1982, p. 362].

Assume that v is discrete and $e_v(K/F) = 1$. If a_v is a uniformizer at v in $\hat{F}_v$, then the exponential value of $x_v \in \hat{F}_v^\circ$ was defined as the unique $l \in \mathbb{Z}$ such that $v(x_v) = v(a_v)^l$. If $x_v \in \hat{F}_v^\circ$ has exponential value l, then the local Artin mapping α_v is defined as $\alpha_v(x_v) = \sigma_v^l$, where σ_v is the Frobenius automorphism of K/F at v.

Now assume that K/F is cyclic of degree n, $\mathbf{G}(K/F) = \langle \tau \rangle$, v is archimedean and $[\hat{K}_v : \hat{F}_v]$ is equal to 2. The fact that $[\hat{K}_v : \hat{F}_v]$ divides $[K : F] = n$ implies that n is even. Since v is archimedean, $[\hat{K}_v : \hat{F}_v] = 2$ is only possible if $\hat{K}_v \cong \mathbb{C}$ and $\hat{F}_v \cong \mathbb{R}$. Corollary 4.24 implies that we may as well identify $\hat{F}_v$ with $\mathbb{R} = \hat{\mathbb{Q}}_{v_\infty}$. In this situation, $\alpha_v : \hat{F}_v \to \mathbf{G}(K/F)$ is the homomorphism defined as $\alpha_v(x_v) = 1_{\mathbf{G}(K/F)}$ for $x_v > 0$ and $\alpha_v(x_v) = \tau^{n/2}$ for $x_v < 0$.

We can now connect these descriptions of α_v to the local invariants $\mathrm{INV}_v(A \otimes \hat{F}_v)$ in the following way.

Lemma 5.21. *Let K/F be a cyclic extension of algebraic number fields of degree n and suppose that τ generates $\mathbf{G}(K/F)$. The elements of $(1/n)\mathbb{Z}/\mathbb{Z}$ act as endomorphisms on $\mathbf{G}(K/F)$ by the rule $\sigma^{(k/n+\mathbb{Z})} = \sigma^k$ for all $\sigma \in \mathbf{G}(K/F)$. If $v \in \mathbf{V}(F)$ and $A = (K, \tau, a)$ for some $a \in F^\circ$, then $\mathrm{INV}_v(A \otimes \hat{F}_v)$ is an element of $(1/n)\mathbb{Z}/\mathbb{Z}$, and*

$$\alpha_v(a) = \tau^{\mathrm{INV}_v(A \otimes \hat{F}_v)}$$

in the following three partially overlapping cases: $\mathrm{INV}_v(A \otimes \hat{F}_v) = 0 + \mathbb{Z}$; v is archimedean; v is discrete and $e_v(K/F) = 1$.

Proof. As seen before, K and $\hat{F}_v$ can be identified with subfields of $\hat{K}_v$ such that $\hat{K}_v = K\hat{F}_v$. Define $n(v) = [\hat{K}_v : \hat{F}_v]$. By Theorem 3.41, $A \otimes \hat{F}_v = (K, \tau, a)^{\hat{F}_v}$ is equivalent to $(K\hat{F}_v, \tau^{k(v)}, a) = (\hat{K}_v, \tau^{k(v)}, a)$, where $k(v) = n/n(v)$.

We start with the case where $\mathrm{INV}_v(A \otimes \hat{F}_v) = 0 + \mathbb{Z}$. Part v) of Theorem 3.38 and the equivalences $(\hat{K}_v, \tau^{k(v)}, a) \sim A \otimes \hat{F}_v \sim \hat{F}_v$ together yield that a is an element of $N_v(\hat{K}_v^\circ)$, so $\alpha_v(a)$ is equal to $1_{\mathbf{G}(K/F)} = \tau^{\mathrm{INV}_v(A \otimes \hat{F}_v)}$ in this case.

Now assume that v is archimedean. If $\hat{K}_v = \hat{F}_v$, then N_v is by definition equal to the identity map, so $a \in N_v(\hat{K}_v)$. By part v) of Theorem 3.38 and the definition of INV_v, $\mathrm{INV}_v(A \otimes \hat{F}_v) = \mathrm{INV}_v(\hat{K}_v, \tau^{k(v)}, a) = 0 + \mathbb{Z}$, and we have already discussed this case. If $\hat{K}_v \neq \hat{F}_v$, then $\hat{K}_v \cong \mathbb{C}$ and $\hat{F}_v \cong \mathbb{R}$. If we make these identifications, then part v) of Theorem 3.38 implies that

$$\mathrm{INV}_v(A \otimes \hat{F}_v) = \begin{cases} 0 + \mathbb{Z} & \text{if } a \in N_{\mathbb{C}/\mathbb{R}}(\mathbb{C}^\circ) = \mathbb{R}_{>0}, \\ 1/2 + \mathbb{Z} & \text{if } a \notin \mathbb{R}_{>0}. \end{cases}$$

From our previous description of α_v in this case, we see that $\alpha_v(a)$ is equal to $\tau^{\mathrm{INV}_v(A\otimes\hat{F}_v)}$.

Finally, we discuss the case where v is discrete and $e_v(K/F) = 1$. Suppose that a_v is a uniformizer at v in $\hat{F}_v$. Note that the definition of $(\hat{K}_v, \tau^{k(v)}, a) \in \mathbf{CSA}(\hat{F}_v)$ implies that $\tau^{k(v)}$ is a generator of $\mathbf{G}(\hat{K}_v/\hat{F}_v)$. If we use the isomorphism $G_v \cong \mathbf{G}(\hat{K}_v/\hat{F}_v)$ to identify these two groups, then the Frobenius automorphism σ_v also generates $\mathbf{G}(\hat{K}_v/\hat{F}_v)$, so $\sigma_v = \tau^{k(v)m(v)}$ for some $m(v)$ that is relatively prime to $n(v)$. If a has exponential value l, then a/a_v^l is an element of $O(\hat{F}_v, v)^\circ = \{b \in \hat{F}_v |\ v(b) = 1\}$, which is a subset of $N_{\hat{K}_v/\hat{F}_v}(\hat{K}_v^\circ)$ by Lemma 4.48. Parts *iii)* and *iv)* of Theorem 3.38 together imply that

$$A \otimes \hat{F}_v \sim (\hat{K}_v, \tau^{k(v)}, a) \sim (\hat{K}_v, \tau^{k(v)}, a_v^l) \sim (\hat{K}_v, \tau^{k(v)m(v)}, a_v^{lm(v)}) = (\hat{K}_v, \sigma_v, a_v^{lm(v)}).$$

From the definition of INV_v for discrete v we now find that $\mathrm{INV}_v(A \otimes \hat{F}_v)$ is equal to $lm(v)/n(v)+\mathbb{Z} = lk(v)m(v)/n+\mathbb{Z}$. The description of α_v for discrete v with $e_v(K/F) = 1$ gives that

$$\alpha_v(a) = \sigma_v^l = \tau^{lk(v)m(v)} = \tau^{\mathrm{INV}_v(A\otimes\hat{F}_v)}.$$

This concludes the proof of this lemma. □

We can use this more thorough description of the local Artin mappings α_v to prove the main theorem of this section.

Proof of Theorem 5.19. Theorem 5.16 states that there are only finitely many valuations $v \in \mathbf{V}(F)$ such that $\mathrm{INV}_v(A \otimes \hat{F}_v) \neq 0 + \mathbb{Z}$. If $v_1, \ldots, v_r$ are the valuations such that $\mathrm{INV}_{v_i}(A \otimes \hat{F}_{v_i}) \neq 0 + \mathbb{Z}$, then let n_i be the order of $\mathrm{INV}_{v_i}(A \otimes \hat{F}_{v_i})$ for $1 \leq i \leq r$. The Grunwald-Wang Theorem and Theorem 5.13 together prove the existence of a cyclic extension K/F of finite degree such that K splits A and $e_v(K/F) = 1$ for all discrete $v \in \mathbf{V}(F)$ with $\mathrm{INV}_v(A \otimes \hat{F}_v) \neq 0 + \mathbb{Z}$. Since the global invariant of A is independent of the choice of representative A of $[A] \in \mathbf{B}(F)$, Theorems 3.11 and 3.37 together imply that we may as well assume that $A = (K, \tau, a)$, where $\mathbf{G}(K/F) = \langle\tau\rangle$ and $a \in F^\circ$.

All $v \in \mathbf{V}(F)$ satisfy at least one of the three cases in Lemma 5.21, so

$$\tau^{\sum_{v\in\mathbf{V}(F)}\mathrm{INV}_v(A\otimes\hat{F}_v)} = \prod_{v\in\mathbf{V}(F)} \tau^{\mathrm{INV}_v(A\otimes\hat{F}_v)} = \prod_{v\in\mathbf{V}(F)} \alpha_v(a) = \alpha(a) = 1_{\mathbf{G}(K/F)},$$

where the last equality is a consequence of Artin's Reciprocity Law. In particular, these equations imply that $\sum_{v\in\mathbf{V}(F)} \mathrm{INV}_v(A \otimes \hat{F}_v)$ is equal to $0 + \mathbb{Z}$. □

5.4.3 Surjectivity to Kernel

In this section, we complete the proof of Theorem 5.15 by proving the following theorem.

Theorem 5.22. *Let F be an algebraic number field. If $\xi = (t_v)_{v\in\mathbf{V}(F)} \in \mathbf{I}(F)$ satisfies $\sum_{v\in\mathbf{V}(F)} t_v = 0 + \mathbb{Z}$, then $\xi = \mathrm{INV}^{(F)} A$ for some $A \in \mathbf{CSA}(F)$.*

For this proof, we will need a weaker version of Chebotarev's Density Theorem, which we will not prove. Chebotarev's Density Theorem is a generalization of Dirichlet's Theorem on arithmetic progressions.

Theorem 5.23 (Chebotarev's Density Theorem)**.** *Let K/F be a Galois extension of algebraic number fields such that $\mathbf{G}(K/F)$ is abelian. For any $\rho \in \mathbf{G}(K/F)$, there are infinitely many discrete valuations v of F with $e_v(K/F) = 1$ such that $\sigma_v = \rho$.*

Proof. See for instance the appendix of [Stevenhagen and Lenstra Jr., 1996] for a proof of this theorem. □

We will use both the Grunwald-Wang Theorem and Chebotarev's Density Theorem in the proof of the main theorem of this subsection.

Proof of Theorem 5.22. We will construct a cyclic algebra $A = (K, \tau, a) \in \mathbf{CSA}(F)$ such that $\mathrm{INV}^{(F)} A = \xi$. If v is a normalized valuation of F, then Theorem 3.41 implies that $(K, \tau, a) \otimes \hat{F}_v$ is equivalent $(\hat{K}_v, \tau^{k(v)}, a)$ with $k(v) = [K : F]/[\hat{K}_v : \hat{F}_v]$. This means that we need to construct K, τ and a in such a way that $\mathrm{INV}_v(\hat{K}_v, \tau^{k(v)}, a)$ equals t_v for all $v \in \mathbf{V}(F)$.

Let the finite set X be defined as $\{v \in \mathbf{V}(F) |\, t_v \neq 0 + \mathbb{Z}\}$. For $v \in X$, we can uniquely write $t_v = k_v/n_v + \mathbb{Z}$, with $k_v, n_v \in \mathbb{N}$, $k_v < n_v$, and $\gcd(k_v, n_v) = 1$. Note that if $v \in X$ is archimedean, then v is real and $t_v = 1/2 + \mathbb{Z}$. The Grunwald-Wang Theorem implies the existence of a cyclic extension of algebraic number fields K/F such that n_v divides $n(v) = [\hat{K}_v : \hat{F}_v]$ for all $v \in X$ and $e_v(K/F) = 1$ for all discrete $v \in X$. Define n as $n = [K : F]$ and let τ be a generator of $\mathbf{G}(K/F)$.

If $v \in X$ is discrete, then Theorem 4.51 implies that $\mathrm{INV}_v(\hat{K}_v, \sigma_v, z_v) = t_v$ for some $z_v \in \hat{F}_v^\circ$. As in the proof of Lemma 5.21, if we define $k(v) = n/n(v)$, then there exists $m(v) \in \mathbb{N}$ with $\sigma_v = \tau^{k(v)m(v)}$ and $\gcd(m(v), n(v)) = 1$. Since $m(v)$ and $n(v)$ are coprime, there exists $y_v \in \hat{F}_v^\circ$ such that $z_v / y_v^{m(v)}$ is an element of $(\hat{F}_v^\circ)^{n(v)} \subseteq N_v(\hat{K}_v^\circ)$. We can now apply parts *iii)* and *iv)* of Theorem 3.38 to conclude that

$$\mathrm{INV}_v(\hat{K}_v, \tau^{k(v)}, y_v) = \mathrm{INV}_v(\hat{K}_v, \tau^{k(v)m(v)}, y_v^{m(v)}) = \mathrm{INV}_v(\hat{K}_v, \sigma_v, z_v) = t_v.$$

If $v \in X$ is archimedean, then $n(v)$ is equal to either 1 or 2 and $n_v = 2$ divides $n(v)$, so $n(v) = 2$. We conclude that $k(v) = n/n(v)$ is equal to $n/2$. Since $\mathbf{G}(\hat{K}_v/\hat{F}_v)$ has order 2, $\mathbf{G}(\hat{K}_v/\hat{F}_v)$ is generated by $\tau^{n/2} = \tau^{k(v)}$. If we define $y_v = -1$, then

$$\mathrm{INV}_v(\hat{K}_v, \tau^{k(v)}, y_v) = 1/2 + \mathbb{Z} = t_v$$

by the definition of INV_v for real v.

By Chebotarev's Density Theorem, there exists a discrete valuation $v_0 \in \mathbf{V}(F) \setminus X$ with $e_{v_0}(K/F) = 1$ such that $\sigma_{v_0} = (\prod_{v \in X} \alpha_v(y_v))^{-1}$. Suppose that $y_{v_0} \in \hat{F}_{v_0}^\circ$ is a uniformizer at v_0. By the initial definition of α_v for discrete v with $e_v(K/F) = 1$, $\alpha_{v_0}(y_{v_0}) = \sigma_{v_0} = (\prod_{v \in X} \alpha_v(y_v))^{-1}$.

Define $\zeta = (x_v)_{v \in \mathbf{V}(F)} \in J_F$ as $x_v = y_v$ for $v \in X \cup \{v_0\}$ and $x_v = 1_{\hat{F}_v}$ for other v. This ζ is by definition an element of $\operatorname{Ker} \alpha = N(J_K)F^\circ$, which implies that there exists $a \in F^\circ$ such that $x_v a^{-1} \in N_v(\hat{K}_v^\circ)$ for all $v \in \mathbf{V}(F)$.

If we define $A \in \mathbf{CSA}(F)$ as $A = (K, \tau, a)$, then for all $v \in \mathbf{V}(F)$,

$$A \otimes \hat{F}_v \sim (\hat{K}_v, \tau^{k(v)}, a) \cong (\hat{K}_v, \tau^{k(v)}, x_v).$$

In particular, this implies that $\mathrm{INV}_v(A \otimes \hat{F}_v) = t_v$ holds for all $v \in X$. If v is an element of $\mathbf{V}(F) \setminus (X \cup \{v_0\})$, then $A \otimes \hat{F}_v \sim (\hat{K}_v, \tau^{k(v)}, 1_{\hat{F}_v}) \sim \hat{F}_v$ yields that $\mathrm{INV}_v(A \otimes \hat{F}_v)$ equals $0 + \mathbb{Z} = t_v$. Finally, we conclude from Theorem 5.19 and $\sum_{v \in \mathbf{V}(F)} t_v = 0 + \mathbb{Z}$ that

$$\mathrm{INV}_{v_0}(A \otimes \hat{F}_{v_0}) = -\sum_{v \in \mathbf{V}(F) \setminus \{v_0\}} \mathrm{INV}_v(A \otimes \hat{F}_v) = -\sum_{v \in \mathbf{V}(F) \setminus \{v_0\}} t_v = t_{v_0}.$$

This completes the proof that $\mathrm{INV}^{(F)} A$ is equal to ξ for $A = (K, \tau, a) \in \mathbf{CSA}(F)$. $\square$

5.5 Structure of Brauer Groups of Algebraic Number Fields

Now that we have proven Theorem 5.15, we can use it to find that, for any algebraic number field F, $\mathrm{INV}^{(F)}$ defines an isomorphism from $\mathbf{B}(F)$ to the subgroup

$$\left\{ (t_v)_{v \in \mathbf{V}(F)} \in \mathbf{I}(F) \middle| \sum_{v \in \mathbf{V}(F)} t_v = 0 + \mathbb{Z} \right\}.$$

of $\mathbf{I}(F) = \bigoplus_{v \in \mathbf{V}(F)} I_v(F)$, where $I_v(F)$ with $v \in \mathbf{V}(F)$ was defined as

$$I_v(F) = \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } v \text{ is discrete,} \\ (1/2)\mathbb{Z}/\mathbb{Z} & \text{if } v \text{ is real,} \\ \{0 + \mathbb{Z}\} & \text{if } v \text{ is complex.} \end{cases}$$

It is clear by the definition of normalized valuations that $\mathbf{V}(\mathbb{Q}) = \{v_\infty^{\mathbb{Q}}\} \cup \{v_p | \ p \text{ prime}\}$. Since $v_\infty^{\mathbb{Q}}$ is real and v_p is discrete for all primes p, we find that

$$\mathbf{B}(\mathbb{Q}) \cong \left\{ (a, x) \middle| \ a \in (1/2)\mathbb{Z}/\mathbb{Z}, x \in \bigoplus_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z} \text{ and } a + \sum_{i=1}^{n} x_i = 0 + \mathbb{Z} \right\}.$$

Now consider a general algebraic number field F. To determine the structure of $\mathbf{B}(F)$, we need to determine the amount of valuations w in $\mathbf{V}(F)$ of each type. Since this is preserved by equivalence of valuations, we only need to know in how many inequivalent ways the valuations in $\mathbf{V}(\mathbb{Q})$ can be extended to F, and whether these extensions are discrete, real or complex.

Since $F/\mathbb{Q}$ is finite and separable and since $\hat{\mathbb{Q}}_v$ is locally compact in the v-topology for all $v \in \mathbf{V}(\mathbb{Q})$, part i) of Lemma 5.1 states that each $v \in \mathbf{V}(\mathbb{Q})$ has at least one and at most $[F : \mathbb{Q}]$ inequivalent extensions to F. In particular, the set $\mathbf{V}(F)$ contains a countably infinite number of discrete valuations. Since for a complex valuation $v \in \mathbf{V}(F)$, $I_v(F) = \{0 + \mathbb{Z}\}$ does not provide a meaningful contribution to the structure of $\mathbf{I}(F) = \bigoplus_{v \in \mathbf{V}(F)} I_v(F)$, we only need to know how many extensions of $v_\infty^{\mathbb{Q}}$ to F are real to determine the structure of $\mathbf{B}(F)$. We conclude that

$$\mathbf{B}(F) \cong \left\{ (a, x) \middle| \ a \in \bigoplus_{\substack{v \in \mathbf{V}(F) \\ v \text{ real}}} (1/2)\mathbb{Z}/\mathbb{Z}, x \in \bigoplus_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z} \text{ and } \sum_{\substack{v \in \mathbf{V}(F) \\ v \text{ real}}} a_v + \sum_{i=1}^{n} x_i = 0 + \mathbb{Z} \right\}.$$

The following theorem helps to determine the number of real extensions of v_∞ to F.

Lemma 5.24. *All archimedean valuations of $\mathbb{R}$ and $\mathbb{C}$ are equivalent to the standard absolute value v_∞.*

Proof. This lemma is a consequence of the uniqueness statements in Theorems 4.23 and 4.32, where $\mathbb{R}$ is to be taken as the locally compact field in Theorem 4.32. □

Theorem 5.25 (Ostrowski's Theorem)**.** *Let F be an algebraic number field. Every archimedean valuation v of F is equivalent to $w = v_\infty \circ \phi$ for some field homomorphism $\phi : F \to \mathbb{C}$, and v is real precisely when $\operatorname{Im}\phi$ is a subfield of $\mathbb{R}$.*

Proof. Note that $w(x) = |\phi(x)|$ defines an archimedean valuation of F for any field homomorphism $\phi : F \to \mathbb{C}$.

If v is archimedean, then $\hat{F}_v$ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$. In any case, there exists a non-zero, injective field homomorphism $\psi : \hat{F}_v \to \mathbb{C}$. The valuation v' of $\operatorname{Im}\psi$ defined as $v'(\psi(x)) = v(x)$ is archimedean, so it is equivalent to v_∞ by Lemma 5.24. Since v' is equivalent to v_∞, $v = v' \circ \psi$ is equivalent to $w' = v_\infty \circ \psi$ on $\hat{F}_v$. By restricting to F, we find that $\phi : F \to \mathbb{C}$ defined as $\phi = \psi|_F$ is a field homomorphism and that v is equivalent to $w'|_F = v_\infty \circ \psi|_F = w$.

If $\phi : F \to \mathbb{C}$ is a field homomorphism such that v is equivalent to $w = v_\infty \circ \phi$, then v is real precisely when w is real. Note that $\widehat{\phi(F)}_{v_\infty} \subseteq \mathbb{C}$ is a field that contains $\widehat{\phi(\mathbb{Q})}_{v_\infty} = \mathbb{R}$, and that $\widehat{\phi(F)}_{v_\infty} = \mathbb{R}$ occurs precisely when $\operatorname{Im}\phi \subseteq \mathbb{R}$. Since ϕ is by definition isometric, $\widehat{\phi(F)}_{v_\infty} = \mathbb{R}$ is true if and only if $\hat{F}_w \cong \mathbb{R}$, so if and only if w is real. □

Ostrowski's Theorem is especially useful in the following special case.

Theorem 5.26. *If F is an algebraic number field such that $F/\mathbb{Q}$ is Galois, then F is of the form $\mathbb{Q}(y)$ for some $y \in \mathbb{C}$, and the number of distinct real valuations of $\mathbb{Q}(y)$ is equal to the number of real roots of the minimal polynomial $\Phi_y \in \mathbb{Q}[\mathbf{x}]$ of y.*

Proof. The extension $F/\mathbb{Q}$ is finite and separable, so the Primitive Element Theorem implies that F is of the form $\mathbb{Q}(y)$ for some $y \in \mathbb{C}$.

Any field homomorphism $\phi : \mathbb{Q}(y) \to \mathbb{C}$ restricts to the identity on $\mathbb{Q}$, so ϕ is fully determined by $\phi(y)$. The equation $\Phi_y(\phi(y)) = \phi(\Phi_y(y)) = 0$ implies that $\phi(y)$ is equal to one of the roots of Φ_y. On the other hand, for any root z of Φ_y, $\psi_z(y) = z$ induces a field homomorphism $\psi_z : \mathbb{Q}(y) \to \mathbb{C}$, so the field homomorphisms from $\mathbb{Q}(y)$ to $\mathbb{C}$ are precisely the maps ψ_z with z ranging over the roots of Φ_y. Finally, note that $\operatorname{Im}\psi_z$ is a subfield of $\mathbb{R}$ precisely when z is a real root of Φ_y. □

5.6 Central Simple Algebras over Algebraic Number Fields

In the final section of this thesis, we apply some of the theorems we have directly or indirectly used in the proof of Theorem 5.15 to prove that all central simple algebras over algebraic number fields are cyclic. We also fulfill our promise from Section 3.5 that $\operatorname{Ind} A$ is equal to $\operatorname{Exp} A$ for all $A \in \mathbf{CSA}(F)$ when F is an algebraic number field.

Theorem 5.27. *Let F be an algebraic number field. If $A \in \mathbf{CSA}(F)$, then A is cyclic and $\operatorname{Ind} A = \operatorname{Exp} A$.*

Proof. Theorem 5.16 implies that there are only finitely many $v \in \mathbf{V}(F)$ such that $\mathrm{INV}_v(A \otimes \hat{F}_v) \neq 0 + \mathbb{Z}$. Label these valuations as $v_1, \ldots, v_r$, and define $n_i = \operatorname{Ind}(A \otimes \hat{F}_{v_i})$. Let m denote the least common multiple of the n_i, and define n to be the degree of A. Part *ii*) of Theorem 2.22 and part *ii*) of Theorem 3.31 together imply that n_i divides $\operatorname{Deg}(A \otimes \hat{F}_{v_i}) = n$ for each $1 \leq i \leq r$. Thus, m divides n as well.

From the definition of the maps INV_v, we conclude that none of the v_i are complex, and that if v_i is real, then $A \otimes \hat{F}_{v_i} \sim \mathbb{H}$ and $n_i = 2$. We can therefore apply the Grunwald-Wang Theorem to prove the existence of cyclic extensions K/F of degree n and L/F of degree m such that n_i divides both $[\hat{K}_{v_i} : \hat{F}_{v_i}]$ and $[\hat{L}_{v_i} : \hat{F}_{v_i}]$ for all $1 \leq i \leq r$. Part *v*) of Corollary 4.52 states that n_i is the order of $\mathrm{INV}_{v_i}(A \otimes \hat{F}_{v_i})$ when v_i is discrete. The same is clearly true for real v_i, so K and L split A by Theorem 5.13. By Corollary 3.12 the equation $[K : F] = n = \operatorname{Deg} A$ implies that K is isomorphic to a strictly maximal subfield of A, so the fact that K is cyclic implies that A is cyclic.

Let k be equal to $\operatorname{Exp} A$. The fact that $k\,\mathrm{INV}^{(F)}[A] = \mathrm{INV}^{(F)}[A]^k = 0_{\mathbf{I}(F)}$ implies that $k\,\mathrm{INV}_{v_i}(A \otimes \hat{F}_{v_i}) = 0 + \mathbb{Z}$ for all $i = 1, \ldots, r$. Thus, n_i divides k for all i, so m divides k. Since L splits A, part *iv*) of Theorem 3.31 implies that $\operatorname{Ind} A$ divides $[L : F] = m$. Combining these statements, we conclude that $\operatorname{Ind} A$ divides $\operatorname{Exp} A$. Part *ii*) of Theorem 3.34 states that $\operatorname{Exp} A$ divides $\operatorname{Ind} A$ for central simple algebras in general, so $\operatorname{Ind} A = \operatorname{Exp} A$. □

Conclusion

Over the course of this thesis, we have found a number of useful results on Brauer groups and central simple algebras over various fields F. We will now summarize our main results. Let F be a field.

Starting with our general results, we found that for any field F each class in $\mathbf{B}(F)$ contains a finite-dimensional central division algebra D over F that is unique up to isomorphism, and all elements of the class $[D] \in \mathbf{B}(F)$ are isomorphic to a matrix algebra $M_n(D)$ for some unique $n \in \mathbb{N}$. We then used this fact to find $\mathbf{B}(F)$ in three simple cases. Namely, we found that $\mathbf{B}(F) = \{[F]\}$ is trivial when F is finite, $\mathbf{B}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$ is a group of order 2, and $\mathbf{B}(\mathbb{C}) = \{[\mathbb{C}]\}$ is a trivial group.

In the third chapter, we found that $\mathbf{B}(F)$ is equal to the union of relative Brauer groups $\mathbf{B}(E/F)$, that each class in $\mathbf{B}(E/F)$ has a crossed product $(E, \mathbf{G}(E/F), \Phi)$ as representative for some $\Phi \in Z^2(G, E^\circ)$, and that this crossed product is unique up to isomorphism. We then defined Galois cohomology and found an isomorphism between $H^2(G, E^\circ)$ and $\mathbf{B}(E/F)$ based on these crossed products. We then used this isomorphism to prove that $\mathbf{B}(F)$ is a torsion group for all fields F. Finally, we introduced a new notation (E, σ, a) with $\mathbf{G}(E/F) = \langle\sigma\rangle$ and $a \in F^\circ$ for crossed products where E/F is cyclic, and for cyclic extensions E/F we found that $\mathbf{B}(E/F)$ is isomorphic to the quotient group $F^\circ/N_{E/F}(E^\circ)$ with an isomorphism defined by $[(E, \sigma, a)] \mapsto aN_{E/F}(E^\circ)$.

The fourth chapter was focused on local fields. We had already determined that the Brauer group of a finite field is trivial, so we worked our way towards determining the structure of $\mathbf{B}(F)$ for local fields F that are infinitely large. If F is an infinite local field, then we found that for each $n \in \mathbb{N}$ there exists a unique field $K_n(F)$ in F^{alg} such that $K_n(F)/F$ is an unramified cyclic extension of degree n, that $\mathbf{B}(F)$ is equal to the union of the relative Brauer groups $\mathbf{B}(K_n(F)/F)$ with n ranging over $\mathbb{N}$, and that each $\mathbf{B}(K_n(F)/F)$ is a cyclic group of order n generated by the class $[(K_n(F), \sigma, a)]$ with σ the Frobenius automorphism and $a \in F^\circ$ a uniformizer of F. We combined these facts to prove that the map $\mathrm{INV}_F : \mathbf{B}(F) \to \mathbb{Q}/\mathbb{Z}$ defined by $[(K_n(F), \sigma, a^k)] \mapsto k/n + \mathbb{Z}$ is an isomorphism of groups when F is an infinite local field.

We spent the last chapter looking at algebraic number fields. We found that for all algebraic number fields F and non-trivial valuations v of F the completion $\hat{F}_v$ is an infinite local field when v is non-archimedean, and that $\hat{F}_v$ is isometrically isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ with the standard absolute value v_∞ when v is archimedean. For each case we defined group isomorphism $\mathrm{INV}_v = \mathrm{INV}_{\hat{F}_v} : \mathbf{B}(\hat{F}_v) \to I_v(F)$ with

$$I_v(F) = \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } \hat{F}_v \text{ is an infinite local field,} \\ (1/2)\mathbb{Z}/\mathbb{Z} & \text{if } \hat{F}_v \text{ is isometrically isomorphic to } \mathbb{R} \text{ with valuation } v_\infty^{\mathbb{R}}, \\ \{0 + \mathbb{Z}\} & \text{if } \hat{F}_v \text{ is isometrically isomorphic to } \mathbb{C} \text{ with valuation } v_\infty^{\mathbb{C}}, \end{cases}$$

and we proved that the global invariant map $\mathrm{INV}^{(F)} : \mathbf{B}(F) \to \prod_{v \in \mathbf{V}(F)} \mathbb{Q}/\mathbb{Z}$ is an injective homomorphism if $\mathrm{INV}^{(F)}$ is defined as $\left(\mathrm{INV}^{(F)}[A]\right)_v = \mathrm{INV}_v([A \otimes \hat{F}_v])$ for $[A] \in \mathbf{B}(F)$ and $v \in \mathbf{V}(F)$, where $\mathbf{V}(F)$ is the set of normalized valuation of F. Finally, we used the Grunwald-Wang-Theorem, Artin's Reciprocity Law and a weaker version of Chebotarev's Density Theorem to prove that the Brauer group $\mathbf{B}(F)$ of an algebraic number field F satisfies the short exact sequence

$$1 \to \mathbf{B}(F) \overset{\mathrm{INV}^{(F)}}{\to} \mathbf{I}(F) \overset{\gamma}{\to} \mathbb{Q}/\mathbb{Z} \to 1,$$

where $\mathbf{I}(F)$ is the direct sum $\mathbf{I}(F) = \bigoplus_{v \in \mathbf{V}(F)} I_v(F)$ and $\gamma : \mathbf{I}(F) \to \mathbb{Q}/\mathbb{Z}$ is defined as $\gamma\left((t_v)_{v \in \mathbf{V}(F)}\right) = \sum_{v \in \mathbf{V}(F)} t_v$.

Acknowledgements

Writing this thesis was a long journey whose destination has now finally been reached. I could not have completed this journey alone. First of all, I would like to thank my supervisor prof.dr. Rob de Jeu for all of his assistance and support. I thoroughly enjoyed our talks and through them I have learned much about math, writing and many other things. I would also like to thank dr. Sander Dahmen for agreeing to be the second examiner of my thesis, though I regret that you have to complete this task in the middle of summer vacation. Finally, I would like to thank my friends and family for their endless support and begrudging willingness to listen to me talk about math. Your sacrifice has not gone unnoticed.

Bibliography

E. Artin and J.T. Tate. *Class field theory*, volume 366. American Mathematical Soc., 1952.

J.W.S. Cassels and A. Fröhlich. *Algebraic number theory*. Academic Press Inc., reprint of the 1967 original edition, 1986.

H. Cohen. *Number Theory: Volume I: Tools and Diophantine Equations*, volume 239. Springer Science & Business Media, 2008.

S. Lang. *Algebra*. Springer, revised third edition, 2002.

F. Lorenz. *Algebra: Volume I: Field and Galois Theory*. Springer Science & Business Media, 2006.

F. Lorenz. *Algebra: Volume II: Fields with Structure, Algebras and Advanced Topics*. Springer Science & Business Media, 2008.

R.S. Pierce. *Associative Algebras*. Springer, first edition, 1982.

S. Roman. *Advanced Linear Algebra*, volume 135. Springer Science & Business Media, 2008.

P. Stevenhagen and H.W. Lenstra Jr. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18, NO. 2, 1996.