Distribution Agreement

Signature:

______________________________________ ______________

Adheep Joseph Date

On the Brauer group of a local field

By

Adheep Joseph
Master of Science

Department of Mathematics

Parimala Raman, Ph.D.
Advisor

Suresh Venapally, Ph.D.
Committee Member

David Zureick-Brown, Ph.D.
Committee Member

Accepted:

Kimberly Jacob Arriola, Ph.D., MPH
Dean of the James T. Laney School of Graduate Studies

Date

On the Brauer group of a local field

By

Adheep Joseph
B.S., University of Maryland, College Park, 2019

Advisor: Parimala Raman, Ph.D.

An abstract of
A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of Science
in Department of Mathematics
2022

Abstract

On the Brauer group of a local field
By Adheep Joseph

This thesis focuses on the study of Brauer groups via Galois Cohomology. In particular, it will cover Wedderburn theory of central simple algebras over general fields, group cohomology and Galois Cohomology, generic splitting, and a description of the Brauer group as a Galois Cohomology group. With a blend of arithmetic results from class field theory, the main aim of the thesis will be the determination of the Brauer group of a local field and establishing the reciprocity sequence for the Brauer group of a number field.

On the Brauer group of a local field

By

Adheep Joseph
B.S., University of Maryland, College Park, 2019

Advisor: Parimala Raman, Ph.D.

A dissertation submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of Science
in Department of Mathematics
2022

Acknowledgments

First and foremost, I would like to thank my advisor, Dr. Parimala Raman, for making this moment possible. She has been a great source of inspiration and support for me and being able to work under her wonderful guidance is undoubtedly the best highlight of my career as a graduate student. I could not have asked for a better advisor, and I certainly cannot thank her enough for her continued support and assistance throughout my time here at Emory. I would also like to thank Dr. Suresh Venapally and Dr. David Zureick-Brown for agreeing to be a part of my thesis committee and for making time in their busy schedules to answer my questions regarding research and grad school. Last but not least, I want to thank my family for their unconditional love and support that carried me through my toughest times.

Contents

Chapter 1

Central Simple Algebras and The Brauer Group

This chapter focuses on the basic theory of central simple algebras. We provide a proof of the classical Wedderburn's theorem and use it to characterize central simple algebras as those finite-dimensional algebras which become isomorphic to some some full matrix algebra over a finite extension of the base field. In addition, we show that this extension can be chosen to be a Galois extension and give an elegant treatment of the Skolem-Noether theorem. We then define the Brauer group, the main invariant concerning central simple algebras, which classifies all finite-dimensional central division algebras over a field. This chapter is based on Gille & Szamuely [1] supplemented by relevant materials from Balwant Singh's notes [2].

1.1 Wedderburn's Theorem

Let k be a field. We assume throughout this chapter that all k-algebras under consideration are finite dimensional over k and the dimension of a k-algebra A over k will be denoted by $[A : k]$.

Definition 1.1.1. A k-algebra A is called *simple* if it has no two-sided ideals other that 0 and A and is *central* if its center $Z(A)$ equals k. In particular, a k-algebra A is *central simple* if it is both central and simple

We provide a basic example of central simple algebras.

Lemma 1. *Let A be a simple k-algebra. Then the ring $M_n(A)$ of $n \times n$ matrices over A is simple for all $n \geq 1$.*

Proof. Suppose I is a nonzero two-sided ideal of $M_n(A)$ and let $I^{'}$ be the subset of A consisting of all entries of elements of I. We claim that $I^{'}$ is a two-sided ideal of A. To see this, let $\sum a_{ij}E_{ij}$ be an element of I, where $a_{ij} \in A$ and E_{ij} denotes the $n \times n$ matrix whose ij-th entry is 1 and all other entries are zero. Observe that for $1 \leq k, k^{'}, l, l^{'} \leq n$ and $b, c \in A$, we have $ba_{k^{'}l^{'}}cE_{kl} = (bE_{kk^{'}})(\sum b_{ij}E_{ij})(cE_{l^{'}l})$ is in I. In particular, this shows that $I^{'}$ is stable under multiplication on the left and right by elements of A. Also note that for $b = c = 1$, we see that if $a \in I^{'}$, then $aE_{kl} \in I$, so that $(a_1 + a_2)E_{kl} \in I$ and thus $a_1 + a_2 \in I^{'}$. Therefore it follows that $I^{'}$ is a two-sided ideal of A. Since A is simple, $A = I^{'}$, so $1 \in I^{'}$. Then we have $E_{kl} \in I$ for all k, l. This shows that $I = M_n(A)$, so $M_n(A)$ is simple.

□

Remark 1. Observe that a division algebra D over k is simple. In addition, its center over k is a field. This can be easily seen by inverting the relation $xy = yx$, which gives us $y^{-1}x^{-1} = x^{-1}y^{-1}$, for all $y \in D, x \in Z(D)$. Hence D is a central simple algebra over k, so by **Lemma 1**, we see that the matrix ring $M_n(D)$ is simple for all $n \geq 0$. Also, observe that the center $M_n(D)$ can only contain scalar multiples of the identity matrix. Hence it follows that $M_n(D)$ is central simple over k for all $n \geq 1$.

We recall some basic facts from module theory.

Definition 1.1.2. A nonzero A-module M is called *simple* if it has no A-submodules other than 0 and M.

Before we proceed, let us make the following useful remark.

Remark 2. Consider the matrix ring $M_n(D)$, where D is a division k-algebra. For $1 \leq r \leq n$, let I_r be the left ideal of $M_n(D)$ formed by matrices $M = [m_{ij}]$ with $m_{ij} = 0$ for $j \neq r$. A similar argument as in **Lemma 1** with the matrices E_{ij} shows that I_r are minimal left ideals with respect to inclusion, i.e. simple $M_n(D)$-modules. Moreover, $M_n(D) = \bigoplus I_r$ and the I_r are all isomorphic as $M_n(D)$-modules. In addition, if M is a simple $M_n(D)$-module, it must be a quotient of $M_n(D)$, so the induced map $\bigoplus I_r \to M$ must induce an isomorphism with some I_r. Thus all simple $M_n(D)$-modules are isomorphic to I_1 (say).

Definition 1.1.3. An *endomorphism* of a left A-module M over a ring A is an A-homomorphism from M to M.

Remark 3. Observe that the set of endomorphisms of a left A-module M form a ring, denoted by $\text{End}_A(M)$, where addition is defined by $(\phi + \psi)(x) = \phi(x) + \psi(x)$, for all $\phi, \psi \in \text{End}_A(M), x \in M$ and multiplication is defined by function composition. Also note that if A is a k-algebra, then $\text{End}_A(M)$ is a k-algebra as well since multiplication by an element of k defines an element in the center of $\text{End}_A(M)$. When A is a division algebra, M is a left vector space over A. Then, by the usual argument from linear algebra, we see that choosing a basis of M induces an isomorphism of $\text{End}_A(M)$ with a matrix algebra. Now we define the *opposite algebra* A° of A as the k-algebra with the same underlying k-vector space as A, but in which the product of two elements x, y is given by $x \cdot_{opp} y = yx$ with respect to the product in A. Then $\text{End}_A(M) \cong M_n(A^\circ)$, where n is the dimension of M over A.

Also note that the module M is equipped with a left module structure over $\text{End}_A(M)$ with the action given by $\phi \cdot x := \phi(x)$, for $x \in M, \phi \in \text{End}_A(M)$.

We will prove the following crucial lemmas from which the Wedderburn's theorem follows.

Lemma 2 (**Schur**)**.** *Let M be a simple module over a k-algebra A. Then* $\mathrm{End}_A(M)$ *is a division algebra.*

Proof. Observe that the kernel of a nonzero endomorphism ϕ of M is an A-submodule of M that is different from M, so it must be 0. Similarly, its image must be the whole of M, so it is an isomorphism. Hence ϕ has an inverse in $\mathrm{End}_A(M)$, so it follows that $\mathrm{End}_A(M)$ is a division algebra. □

Let M be a left A-module with the endomorphism ring $E = \mathrm{End}_A(M)$. Since M is naturally a left E-module, we can consider the endomorphism ring $\mathrm{End}_E(M)$. In particular, we define a ring homomorphism $\lambda_M \colon A \to \mathrm{End}_E(M)$ by sending $a \in A$ to the endomorphism $x \mapsto ax$ of M. It is straightforward to check that λ_M is an E-endomorphism by simply observing that if $\psi \colon M \to M$ is an element of E, then we have $\psi \cdot ax = \psi(ax) = a\psi(x) = a\psi \cdot x$, for all $x \in M$.

Lemma 3 (**Rieffel**)**.** *Let L be a nonzero left ideal in a simple k-algebra A and* $E = \mathrm{End}_A(L)$*. Then the map $\lambda_L \colon A \to$* $\mathrm{End}_E(L)$ *defined above is an isomorphism.*

Proof. Observe that in a ring A, a left ideal is a submodule of the left A-module A. Since $\lambda_L \neq 0$, its kernel is a proper two-sided ideal of A. However A is simple, so λ_L is injective. To show that λ_L is surjective, we first show that $\lambda_L(L)$ is a left ideal in $\mathrm{End}_E(L)$. So consider $\phi \in \mathrm{End}_E(L)$ and $l \in L$. Then $\phi \cdot \lambda_L(l)$ is the map $x \mapsto \phi(lx)$. But observe that for all $x \in L$, the map $y \mapsto yx$ is an A-endomorphism of L, i.e. an element of E. Since ϕ is an E-endomorphism, we have $\phi(lx) = \phi(l)x$, so $\phi \cdot \lambda_L(l) = \lambda_L(\phi(l))$.

Observe that the right ideal LA generated by L is a two-sided ideal, so $LA = A$. In particular, we have $1 = \sum l_i a_i$ with $l_i \in L, a_i \in A$. Hence, for $\phi \in \mathrm{End}_E(L)$, we have $\phi = \phi \cdot 1 = \phi\lambda_L(1) = \sum \phi\lambda_L(l_i)_L(a_i)$. Since $\lambda_L(L)$ is a left ideal, we have $\phi\lambda_L(l_i) \in \lambda_L(L)$ for all i, so $\phi \in_L (A)$. Thus λ_L is surjective and therefore an isomorphism. □

We will now formally state and prove the Wedderburn's Theorem.

Theorem 1.1.1 (**Wedderburn**). *Let A be a finite dimensional simple algebra over a field k. Then there exist an integer $n \geq 1$ and a division algebra $k \subset D$ such that A is isomorphic to the matrix ring $M_n(D)$. Moreover, the division algebra D is uniquely determined up to isomorphism.*

Proof. Observe that since A is finite-dimensional, a descending chain of left ideals must stabilize. Let L be a minimal left ideal, so it is a simple A-module. By *Schur's lemma*, $E = \mathrm{End}_A(L)$ is a division algebra and by *Rieffel's lemma*, we have an isomorphism $A \cong \mathrm{End}_E(L)$. Observe that $\mathrm{End}_E(L) \cong M_n(E^\circ)$, where n is the dimension of L over E (note that it is finite as L is already finite dimensional over k). Setting $D \coloneqq E^\circ$, we see that $A \cong M_n(D)$.

For uniqueness, assume that D and $D^{'}$ are division algebras such that $A \cong M_n(D) \cong M_m(D^{'})$ with suitable integers m, n. Then, by **Remark 2**, the minimal left ideal L then satisfies $D^n \cong L \cong D^{'^m}$, so we get a chain of isomorphisms $D \cong \mathrm{End}_A(D^n) \cong \mathrm{End}_A(L) \cong \mathrm{End}_A(D^{'^m}) \cong D^{'}$.

□

Corollary 1.1.1.1. *Let k be an algebraically closed field. Then every central simple k-algebra is isomorphic to $M_n(k)$ for some $n \geq 1$.*

Proof. Note that, by the Wedderburn's theorem, it suffices to show that there is no finite-dimensional division algebra D containing k. Let $d \in D \setminus k$. Then we have an irreducible polynomial $f \in k[X]$ and a k-algebra homomorphism $k[X]/(f) \to D$ whose image contains d. Since k is algebraically closed, it follows that $k[X]/(f) \cong k$, so $d \in k$, a contradiciton. Thus the result follows. □

1.2 Central Simple Algebras (Some Results)

In this section, we discuss some important results involving central simple algebras.

Theorem 1.2.1. *Let A be a central simple k-algebra. If B is a k-algebra which is simple, then $A \otimes B$ is simple.*

Proof. Since A is simple, by Wedderburn's theorem, there exists a division ring D such that $A \cong M_n(D)$. Observe that D is a central division algebra over k. Also, we have $A \otimes B \cong M_n(D) \otimes B \cong M_n(D \otimes B)$. If $D \otimes B$ is simple, then by **Lemma 1**, it follows that $A \otimes B$ is simple as well. Thus it is enough to prove the theorem for the case when A is a central division algebra.

Let D be a central division algebra and let I be any nonzero two-sided ideal of $D \otimes B$. Let $\{e_\alpha\}_{\alpha \in J}$ be a basis of B over k. Observe that any element $a \in I$ can be written uniquely in the form $a = \sum_{\alpha \in J} a_\alpha \otimes e_\alpha$, where $a_\alpha \in D, a_\alpha = 0$, for almost all α. Let $I(a) \coloneqq \{\alpha \in I : a_\alpha \neq 0\}$. Then for each $a \in I, I(a)$ is a finite subset of I. Let $c = \sum c_\alpha \otimes e_\alpha$ be a nonzero element of I such that $I(c)$ is minimal in the set $\{I(a) : a \in I, a \neq 0\}$. Multiplying c by an element of D, we can clearly assume that at least one c_α, say c_β, is equal to 1. Since I is a two-sided ideal, for any $d \in D$, we have

$$c^{'} = (d \otimes 1)c - c(d \otimes 1) = \sum (dc_\alpha - c_\alpha d) \otimes e_\alpha \in I.$$

Note that since $c_\beta = 1, dc_\beta = c_\beta d$, so we have $I(c^{'}) \subsetneq J(c)$. Then, by the minimality of $I(c)$, it follows then that $c^{'} = 0$. That is, $dc_\alpha = c_\alpha d$ for all α. Since d was arbitrarily chosen and D is central, it follows that $c_\alpha \in k$. In other words, $c \in I \cap (1 \otimes B)$. Thus $I \cap (1 \otimes B)$ is a nonzero two-sided ideal of $1 \otimes B$. In particular, $1 \otimes 1 \in I$, so $I = A \otimes B$, and the result follows. □

Definition 1.2.1. If A is any ring and E a nonempty subset of A, the *commutant* of E, denoted by $E^{'}$, is defined to be the set $\{a \in A : ae = ea, \forall e \in E\}$.

It is straightforward to check that $E^{'}$ is a subring of A. Also, observe that if A and B are k-algebras and $C \subset A$ and $D \subset B$ are k-subalgebras, then the induced k-algebra homomorphism $C \otimes D \to A \times B$ is a monomorphism. We will identify $C \otimes D$ under this mapping with a k-subalgebra of $A \otimes B$.

Proposition 1. *Let A and B be k-algebras. If $C \subset A, D \subset B$ are k-subalgebras and $C^{'}, D^{'}, (C \otimes D)^{'}$ are the commutants of $C, D,$ and $C \otimes D$ in $A, B,$ and $A \otimes B$ respectively, then we have*

$$(C \otimes D)^{'} = C^{'} \otimes D^{'}.$$

Proof. It is easy to see that $C^{'} \otimes D^{'} \subset (C \otimes D)^{'}$. Let $\{e_\alpha\}$ be a k-basis of B and let $\lambda = \sum a_\alpha \otimes e_\alpha \in (C \otimes D)^{'}$, where $a_\alpha \in A$. For any $c \in C$, we have $(c \otimes 1)\lambda = \lambda(c \otimes 1)$. That is, $\sum ca_\alpha \otimes e_\alpha = \sum a_\alpha c \otimes e_\alpha$, which implies that $ca_\alpha = a_\alpha c$, for all α. Since c was arbitrarily chosen, it follows then that $a_\alpha \in C^{'}$. In other words, $\lambda \in C^{'} \otimes B$. Similarly, it follows that $\lambda \in A \otimes D^{'}$, so $\lambda \in (C^{'} \otimes B) \cap (A \otimes D^{'})$. Thus $(C \otimes D)^{'} \subset C^{'} \otimes D^{'}$ and the result follows. □

Corollary 1.1. *If A and B are k-algebras, we have*

$$Z(A \otimes B) = Z(A) \otimes Z(B).$$

Proof. Follows with $A^{'} = Z(A), B^{'} = Z(B)$, and $(A \otimes B)^{'} = Z(A \otimes B)$. □

Corollary 1.2. *If A and B are central simple algebras over k, then $A \otimes B$ is central simple over k.*

Proof. Observe that by **Theorem 1.2.1**, $A \otimes B$ is simple. By **Corollary 1.2**, we have $Z(A \otimes B) = Z(A) \otimes Z(B) = k \otimes k = k$, so $A \otimes B$ is central simple over k. □

Corollary 1.3. *If A is a central simple k-algebra and L any field extension of K, then $L \otimes_K A$ is a central simple algebra over L.*

Proof. It follows from **Theorem 1.2.1** that $L \otimes A$ is a simple L-algebra. By **Corollary 1.1**, we have $Z(L \otimes A) = L \otimes k = L$, so the result follows. □

Corollary 1.4. *If A is a central simple k-algebra, then $[A : k]$ is a perfect square.*

Proof. Let $\bar{k}$ be the algebraic closure of k. By **Corollary 1.3**, $\bar{k} \otimes A$ is central simple over $\bar{k}$, so by **Corollary 1.1.1.1**, $\bar{k} \otimes A \cong M_n(\bar{k})$. Thus, $[A : k] = [\bar{k} \otimes A : \bar{k}] = n^2$. □

Suppose A is a central simple k-algebra and let A° be the opposite ring. It is easy to see that A° is again a central simple k-algebra. For any $a \in A$, let L_a denote the k-linear endomorphism of A given by left multiplication by a. Similarly, let R_a denote the right multiplication by a. The mappings $\phi \colon A \to \mathrm{End}_k(A)$ and $\psi \colon A^\circ \to \mathrm{End}_k(A)$ defined by $\phi(a) = L_a$ and $\psi(a^\circ) = R_a$ are k-algebra homomorphisms. Since every element of $\phi(A)$ commutes with every element of $\psi(A^\circ)$, we have an induced k-algebra homomorphism

$$\theta \colon A \otimes A^\circ \to \mathrm{End}_k(A)$$

defined by $\theta(a \otimes b^\circ) = \phi(a)\psi(b^\circ) = L_a R_b$.

Theorem 1.2.2. *The map $\theta \colon A \otimes A^\circ \to \mathrm{End}_k(A)$ is an isomorphism of k-algebras.*

Proof. Since A is central simple, it follows from **Corollary 1.2** that $A \otimes A^\circ$ is central simple. Since $\ker(\theta)$ is a two-sided ideal of $A \otimes A^\circ$ and $\ker(\theta) \neq A \otimes A^\circ$, it follows that $\ker(\theta) = (0)$, so θ is a monomorphism. Also, since $\dim(A \otimes A^\circ) = (\dim(A))^2 = \dim(\mathrm{End}_k(A))$, it follows that θ is surjective, so θ is a k-algebra isomorphism. □

Corollary 1.2.2.1. *If A is a central simple k-algebra with $[A : k] = n^2$, then $A \otimes A^\circ \cong M_{n^2}(k)$.*

Proof. The result follows by simply observing that $\mathrm{End}_K(A) \cong M_{n^2}(k)$. □

1.3 Skolem-Noether Theorem

Theorem 1.3.1 (Skolem-Noether). *Let A be a central simple algebra over k and let B be a simple k-algebra. If $f, g\colon B \to A$ are k-algebra monomorphisms, then there exists an invertible element $u \in A$ such that for any $b \in B$, we have $g(b) = uf(b)u^{-1}$.*

Proof. Suppose first that A is a matrix algebra $M_n(k)$. Then, to say that we are given two monomorphisms $f, g\colon B \to M_n(k)$ simply means that we are given two B-module structures on k^n. Then, it follows that these modules are isomorphic since the dimensions are the same. This means that there exists an invertible element $u \in M_n(k)$ such that for any $b \in B$, the diagram

$$\begin{tikzcd}
K^n \arrow[r, "u"] \arrow[d, "f(b)"'] & K^n \arrow[d, "g(b)"] \\
K^n \arrow[r, "u"] & K^n
\end{tikzcd}$$

is commutative and therefore implies the statement of the theorem.

Let A be any central simple algebra and let A° be its opposite algebra. Observe that we have k-algebra monomorphisms $f \otimes 1^\circ, g \otimes 1^\circ\colon B \otimes A^\circ \to A \otimes A^\circ$, where 1° denotes the identity map of A°. Since $A \otimes A^\circ \cong M_n(k)$, for some n, we get an invertible element $u \in A \otimes A^\circ$ such that

$$(g \otimes 1^\circ)(b \otimes a^\circ) = u(f \otimes 1)(b \otimes a^\circ)u^{-1} \tag{1.1}$$

for every $b \in B, a^\circ \in A^\circ$. Letting $b = 1$, we see that

$$(g \otimes 1^\circ)(1 \otimes a^\circ) = u(1 \otimes a^\circ)u^{-1}.$$

In other words, u commutes with $1 \otimes a^\circ$. Since $a^\circ \in A^\circ$ was arbitrarily chosen, it follows that $u \in (1 \otimes A^{\circ})^{'}$. By **Proposition 1**, we have $(1 \otimes A^{\circ})^{'} = A \otimes 1$. Thus $u = u_1 \otimes 1 \in A \otimes 1$, where u_1 is an invertible element of A. It is easy to see then that by setting $a^{\circ} = 1$ in (1.1) that u_1 satisfies the required property and the result follows. □

Corollary 1.3.1.1. *Every k-algebra automorphism of a central simple k-algebra is an inner automorphism.*

Proof. This is immediate from the Skolem-Noether theorem by taking $B = A, F = \mathrm{id}$, and g to be the given automorphism. □

Proposition 2. *Let A be a central simple k-algebra, B a simple k-subalgebra and $B^{'}$ the commutant of B in A. Then $B^{'}$ is simple, the commutant $B^{''}$ of $B^{'}$ is B and we have $[B : k][B^{'} : k] = [A : k]$.*

Proof. Let $\mathrm{End}_k(B)$ be the k-algebra endomorphisms of the k-vector space B. Since $\mathrm{End}_k(B)$ is a k-matrix algebra, it is a central simple algebra over k. Since A is central simple, it follows then that $A \otimes \mathrm{End}_k(B)$ is also central simple. The inclusion of B in A induces a k-algebra monomorphism $f \colon B \to A \otimes \mathrm{End}_k(B)$. On the other hand, B can be embedded in $\mathrm{End}_k(B)$ under the map $b \mapsto L_b$ where L_b is the left multiplication by b. This induces a k-algebra monomorphism $g \colon B \to A \otimes \mathrm{End}_k(B)$ such that $g = (\mathrm{Int\ u}) \circ f$, where Int u is the inner automorphism of $A \otimes \mathrm{End}_k(B)$ given by u. Thus Int u maps $f(B)$ isomorphically onto $g(B)$ and hence the commutant $f(B)^{'}$ onto $g(B)^{'}$. By **Proposition 1**, it is easy to see then that $f(B)^{'} = B^{'} \otimes \mathrm{End}_k(B)$ and $g(B)^{'} = A \otimes B^{\circ}$. Thus $B^{'} \otimes \mathrm{End}_k(B) \cong A \otimes B^{\circ}$. Since B° is also simple, it follows that $A \otimes B^{\circ}$ is simple and hence $B^{'} \otimes \mathrm{End}_k(B)$ is simple as well, which implies that $B^{'}$ is simple. Equating the dimensions of $B^{'} \otimes \mathrm{End}_k(B)$ and $A \otimes B^{\circ}$, we have

$$[B^{'} : k][B : k]^2 = [A : k][B : k]$$

which gives $[B^{'} : k][B : k] = [A : k]$. Applying this formula to the simple k-subalgebra $B^{'}$, we have

$$[B^{''} : K][B^{'} : k] = [A : k]$$

so we get $[B^{''} : k] = [B : k]$. Since $B \subset B^{''}$, $B = B^{''}$ and the result follows. □

Corollary 2.1. *If B is a central simple k-subalgebra of a central simple k-algebra A, then $B^{'}$ is also central simple and the inclusions $B \hookrightarrow A, B^{'} \hookrightarrow A$ induce an isomorphism $B \otimes B^{'} \xrightarrow{\sim} A$.*

Proof. Observe that the inclusions $B \hookrightarrow A, B^{'} \hookrightarrow A$ induce a k-algebra homomorphism $\phi \colon B \otimes B^{'} \to A$. Since B is central simple, it follows that $B \otimes B^{'}$ is simple, so ϕ is a monomorphism. Also, by **Proposition 2**, we have

$$[B \otimes B^{'} : k] = [B : k][B^{'} : k] = [A : k].$$

Thus ϕ is surjective. It is also clear that the center of $B^{'}$ is k, so the result follows.

□

Corollary 2.2. *Let A be a central simple k-algebra and let L be a commutative subring of A containing k. Then the following are equivalent:*

1. *L is a maximal commutative ring of A.*

2. *L conincides with its commutant.*

3. *$[A : k] = [L : k]^2$.*

Proof. $(1 \implies 2)$ Let $L^{'}$ be the commutant of L. Since L is commutative, it follows that $L \subset L^{'}$. Let $x \in L^{'}$, Then the subring of A generated by L and x is commutative. By the maximality of L, it follows that $x \in L$, so $L^{'} \subset L$. Hence $L = L^{'}$.

$(2 \implies 1)$ Let $L \subset L_1$ be a commutative subring of A. Since L_1 is commutative, it follows that $L_1 \subset L^{'} = L$. Thus $L_1 = L$ and L is a maximal commutative subring of A.

$(3 \implies 2)$ Suppose $L^{'}$ is the commutant of L. Observe that $L \subset L^{'}$. On the other hand, $[L : k]^2 = [A : k] = [L : k][L^{'} : k]$ which implies that $[L : k] = [L^{'} : k]$. Thus $L^{'} = L$. □

Corollary 2.3. *Let D be a central division algebra over k. If L is a maximal commutative subfield of D containing k, then*

$$[D : k] = [L : k]^2$$

.

Proof. Observe that any commutative subring of D containing k is a subfield. So applying **Corollary 2.2**, the result follows immediately. □

1.4 The Brauer Group

We now have developed most of the background tools to define the Brauer group

Definition 1.4.1. Given two central simple k-algebras A and B, we say that A and B are *equivalent* or *Brauer equivalent*, denoted by $A \sim B$, if there exist matrix algebras $M_m(k)$ and $M_n(k)$ such that $A \otimes M_m(k) \cong B \otimes M_n(k)$. That is, $M_m(A) \cong M_n(B)$.

Proposition 3. *Let A, B be central simple k-algebras and let D_A, D_B denote the division algebras of A and B respectively. Then $A \sim B$ if and only if $D_A \cong D_B$.*

Proof. Let $A \cong M_p(D_A)$ and $B \cong M_l(D_B)$. If $A \sim B$, the for some m, n, $M_m(A) \cong M_n(B)$. That is, $M_{mp}(D_A) \cong M_{nl}(D_B)$. By *Wedderburn's theorem*, this implies that $D_A \cong D_B$.

Conversely, assume $D_A \cong D_B$. Then

$$M_l(A) \cong M_l(M_p(D_A)) \cong M_{lp}(D_A) \cong M_{lp}(D_B) \cong M_p(M_l(D_B)) \cong M_p(B).$$

Thus the result follows. □

The set of equivalence classes of central simple k-algebras is denoted by $\mathrm{Br}(k)$. For any central simple k-algebra, we denote its equivalence class by $[A]$. If A and B are central simple k-algebras, by **Corollary 1.2** that $A \otimes B$ is central simple as well. We define a binary composition on $\mathrm{Br}(k)$ by $[A] \cdot [B] := [A \otimes B]$. It is straightforward to check that this operation is well-defined.

Proposition 4. *With the above composition* $\mathrm{Br}(k)$ *is an abelian group. The identity of this group is* $[k]$, *the class of* k *and consists of all matrix algebras over* k. *The inverse of* $[A]$ *is* $[A^\circ]$.

Proof. It is straightforward to check that $\mathrm{Br}(k)$ is an abelian group. Since $A \otimes k \cong A$, it is clear that $[k]$ is the identity. By **Corollary 1.2.2.1**, it follows that for any central simple algebra A, $[A \otimes A^\circ] = [k]$, so $[A]$ is invertible and has $[A^\circ]$ as its inverse. □

Definition 1.4.2. The group $\mathrm{Br}(k)$ defined above is called the *Brauer group* of k.

1.5 Relative Brauer Group

We now define the relative Brauer group of an extension $K|k$.

Lemma 4. *Let* $K|k$ *be a field extension and let* A, B *be* k*-algebras. Then there is an isomorphism of* K*-algebras*

$$(A \otimes_k B) \otimes_k K \cong (A \otimes_k K) \otimes_K (B \otimes_k K)$$

Thus

$$\mathrm{Br}(k) \to \mathrm{Br}(K) \text{ defined by } [A] \mapsto [A \otimes_k K]$$

is a group homomorphism.

Proof. The isomorphism is straightforward to write down in terms of elements. The homomorphism property follows immediately. □

Definition 1.5.1. Let $K|k$ be a field extension. The *relative Brauer group* $\mathrm{Br}(K|k)$ is defined to be the kernel of the homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(K) \text{ defined by } [A] \mapsto [A \otimes_k K]$$

We sometimes refer to $\mathrm{Br}(k)$ as the *absolute Brauer group.*

Let $K|k$ be a field extension of k.

Definition 1.5.2. Let A be a central simple k-algebra and let $K|k$ be an extension of fields. We say that K is a *splitting field* of A or that K *splits* A if $K \otimes A$ is K-isomorphic to $M_n(K)$, for some n.

This simply means that $[A]$ is in the kernel of the homomorphism $\mathrm{Br}(k) \to \mathrm{Br}(K)$. In particular, if $k \subset K$ is an algebraically closed field, then K splits any central simple k-algebra A.

Theorem 1.5.1. *Let $K|k$ be a finite field extension. For any central simple k-algebra A, the following are equivalent:*

1. *K is a splitting field for A.*

2. *K is a maximal commutative subring of some central simple k-algebra equivalent to A.*

Proof. ($1 \implies 2$) Let $\phi \colon K \otimes A \xrightarrow{\cong} \mathrm{End}_K(V)$ be a K-isomorphism, where V is a finite-dimensional K-vector space. Since K is finite-dimensional over k, V is finite-dimensional over k and $\mathrm{End}_k(V)$ is a central simple k-algebra containing $\mathrm{End}_K(V)$. Let C be the commutant of $\phi(1 \otimes A)$ in $\mathrm{End}_k(V)$. Since the commutant $\phi(K \otimes A)$ in $\mathrm{End}_k(V)$ is K and $1 \otimes A \subset K \otimes A$, it follows that $K \subset C$. Since C is central simple, it follows from **Corollary 2.1** that $A \otimes C \cong \mathrm{End}_k(V)$. That is $A \sim C^\circ$. So if we set $B = C^\circ$, then $K \subset B$ and we will be done provided we show that K is a maximal commutative subring of B. Observe that by **Corollary 2.2**, it suffices to show that $[B : k] = [K : k]^2$. Note that we have $[B : k] = [C : k]$ and $[A : k][C : k] = [\mathrm{End}_k(V) : k] = [\mathrm{End}_K(V) : k][K : k] = [K \otimes_k A : k][K : k] = [K : k]^2[A : k]$, which shows that $[C : k] = [K : k]^2$.

($2 \implies 1$) It suffices to show that if K is a maximal commutative subring of A, then K splits A. Observe that by **Theorem 1.2.2**, we have an isomorphism $A \otimes A^\circ \xrightarrow{\cong} \mathrm{End}_k(A)$. Since $K \subset A$ and K is commutative, it follows that $K \subset A^\circ$. By **Proposition 1**, the commutant of $1 \otimes K$ in $A \otimes A^\circ$ is, $A \otimes K$. On the other hand, the commutant of K in $\mathrm{End}_k(A)$ is $\mathrm{End}_K(A)$. Thus $A \otimes K \cong \mathrm{End}_K(A) \cong M_n(K)$ with $n = [A : K]$, so the result follows. □

Corollary 1.5.1.1. *Any maximal commutative subfield of a central division algebra D is a splitting field for D.*

We now prove the existence of Galois splitting fields.

Lemma 5. *Let $D \neq k$ be a central division algebra over k. Then D contains a separable algebraic extension of k containing k properly.*

Proof. Assume, for a contradiciton, that the statement is false. Observe that if there exists some element $\alpha \in D$ which is not purely inseparable over k, then $k(\alpha)$ contains a separable subextension of k other than k and this would prove the lemma. Therefore, assume that every element of D is purely inseparable over k. Thus every element

$x \in D$ satisfies $x^{p^e} \in k$ for some positive integer e depending on x, where p is the characteristic of k. Since D is finite-dimensional over k, there exists an integer e such that $x^{p^e} \in k$ for all $x \in D$. Let $1 = e_1, \ldots, e_n$ be a k-basis of D and let $x = \sum_i x_i e_i \in D$, where $x_i \in k$. Then $x^{p^e} = \sum_j P_j(x_1, \ldots, x_n)e_j$, where P_j re polynomials in x_i whose coefficients can be expressed in the terms of the structure constants of D. Observe that, by the hypothesis, $P_j(x_1, \ldots, x_n) = 0$ for $j \neq 1$ and for all systems of values of x_i in k. Since we can assume that k is infinite (if k is finite, then every finite extension of k is separable) we see that $P_j (j \neq 1)$ vanish identically. This implies that the same condition $x^{p^e} \in k$ also holds if we extend the base field. In particular, this must be true if we extend k to its algebraic closure K. But then $K \otimes D$ is a matrix algebra and there are idempotents of $K \otimes D$ which fail to satisfy the condition. Thus we arrive at a contradiction and the lemma follows. □

Theorem 1.5.2. *Every central division algebra D over a field k contains a maximal commutative subfield which is separable over k*

Proof. Suppose K be a subfield of D which is a maximal separable extension of k. We claim that K is a maximal commutative subfield of D. If not, let $K^{'} \neq K$ be the commutant of K. Then $K^{'}$ is a division algebra of center K. By **Lemma 4**, there exists a proper separable extension of K contained in $K^{'}$, which contradicts our assumption on K. Therefore it follows that K is a maximal commutative subfield and the result follows. □

Corollary 1.5.2.1. *Let k be a field and $k \subset K$ be a separably algebraically closed field (a field which has no proper separable algebraic extensions). Then K splits any central simple k-algebra.*

Proof. Let A be a central simple algebra over k. Then $K \otimes A \cong M_n(D)$, where D is a finite-dimensional division algebra over K. If $D \neq K$, then by **Theorem 1.5.2**, D

must contain a proper finite separable extension of K. But this is impossible since K is separably algebraically closed, by assumption. Thus $D = K$ and K splits A. □

Corollary 1.5.2.2. *Every central simple k-algebra A admits a splitting field which is a finite Galois extension of k.*

Proof. Let D be the division algebra of A. Then, by **Theorem 1.5.2**, D contains a maximal commutative subfield K which is separable over k. By **Corollary 1.5.1.1**, the field K splits D, and hence splits A as well. Let $K^{'}$ be the normal closure of K. Then $K^{'}$ is clearly finite and Galois extension of K which splits A. □

We can now relate the absolute Brauer group $\mathrm{Br}(k)$ with the relative Brauer group $\mathrm{Br}(K|k)$.

Proposition 5.

$$\mathrm{Br}(k) = \bigcup_{K} \mathrm{Br}(K|k)$$

where the union is taken over all finite Galois extensions of k.

Proof. The inclusion $\supset$ follows immediately from the definitions. To show the containment in the other direction, let A be a central simple k-algebra. By *Wedderburn's Theorem*, $A \cong M_d(D)$, for some division algebra D. Then, by **Theorem 1.5.2**, we can find a maximal subfield F of D which is a separable extension of k. Then we have $D \otimes_k F \cong M_l(F)$, where $\dim_k(D) = l^2$. Then clearly F splits A. Since F is separable over k, its normal closure L is a finite Galois extension of k, splits A. Thus $[A] \in \mathrm{Br}(K|k)$ and the result follows. □

Corollary 5.1. *Let k be a field with separable closure k^{sep}. Then*

$$\mathrm{Br}(k) = \mathrm{Br}(k^{\mathrm{sep}}|k).$$

Proof. The inclusion $\supset$ follows immediately from the definitions. To show the containment in the other direction, let A be a central simple k-algebra. By *Wedderburn's Theorem*, $A \cong M_d(D)$, for some division algebra D. Then, by **Theorem 1.5.2**, we can find a maximal subfield F of D which is a separable extension of k, so $F \subset k^{\text{sep}}$. Then we have $D \otimes_k F \cong M_l(F)$, where $\dim_k(D) = l^2$.

Then we have

$$A \otimes_k F \cong M_n(F)$$

where $n = dl$. Since $F \subset k^{\text{sep}}$, we have

$$A \otimes_k k^{\text{sep}} \cong (A \otimes_k F) \otimes_F k^{\text{sep}} \cong M_n(F) \otimes_F k^{\text{sep}} \cong M_n(k^{\text{sep}})$$

so $[A] \in \text{Br}(k^{\text{sep}}|k)$. □

Chapter 2

The Cohomological Brauer Group

This chapter focuses on applying techniques from the cohomology theory of groups to the study of Brauer groups. In particular, we describe the Brauer group of a field using factor sets and crossed products, which enables us to identify it with a certain second cohomology group. We conclude our discussion by computing the Brauer groups of some well-known fields. This chapter closely follows Gille & Szamuely [1], Guillot [6], and Rapinchuk's notes [7] with occasional results from Sharifi's notes [8] from algebraic number theory.

2.1 Profinite Groups

In this section, we develop some background on direct and inverse limits, since they play a crucial role in determining the Galois group of an infinite field extension.

Definition 2.1.1. A *filtered inverse system* of groups (G_i, ϕ_{ij}) consists of:

- a partially ordered set $(\Gamma, \leq)$ which is directed in the sense that for all $(i, j) \in \Gamma$, there exists some $k \in \Gamma$ such that $i \leq k, j \leq k$;
- for each $i \in \Gamma$ a group G_i;

- for each $i \leq j$, a homomorphism $\phi_{ij}\colon G_j \to G_i$ such that we have equalities $\phi_{ik} = \phi_{ij} \circ \phi_{jk}$, for all $i \leq j \leq k$.

The *inverse limit* of the system is defined as the subgroup of the direct product $\prod_{i\in\Gamma} G_i$ consisting of the sequences (g_i) such that $\phi_{ij}(g_j) = g_i$ for all $i \leq j$. It is denoted by $\varprojlim G_i$.

A *filtered direct system* of groups (B_i, ϕ_{ij}) consists of:

- a partially ordered set $(\Gamma, \leq)$ which is directed in the sense that for all $(i, j) \in \Gamma$, there exists some $k \in \Gamma$ such that $i \leq k, j \leq k$;
- for each $i \in \Gamma$ an abelian group B_i;
- for each $i \leq j$, a homomorphism $\psi_{ij}\colon B_i \to B_j$ such that we have equalities $\psi_{ik} = \psi_{jk} \circ \psi_{ij}$, for all $i \leq j \leq k$.

The *direct limit* of the system is defined as the quotient of the direct sum $\bigoplus_{i\in\Gamma} B_i$ by the subgroup generated by elements of the form $b_j - \psi_{ij}(b_i)$. It is denoted by $\varinjlim B_i$. Also, given a direct systems (B_i, ψ_{ij}) and (C_i, ρ_{ij}) indexed by the same directed set Γ together with maps $\lambda_i\colon B_i \to C_i$ satisfying $\lambda_j \circ \psi_{ij} = \rho_{ij} \circ \lambda_i$, for all $i \leq j$, we have an induced map $\lambda\colon \varinjlim B_i \to \varinjlim C_i$ called the *direct limit of the maps* λ_i.

We now have all the necessary tools to define a profinite group.

Definition 2.1.2. A *profinite* group is an inverse limit of a system of finite groups. For a prime number p, a *pro-p group* is an inverse limit of finite p-groups.

We will also need some general facts about topological groups.

Definition 2.1.3. A *topological group* is a group G which is also endowed with a topology for which the multiplication map

$$G \times G \to G,\ (x, y) \mapsto xy$$

as well as the inverse map

$$G \to G, \ x \mapsto x^{-1}$$

are continuous.

Proposition 6. *Let G be a topological group.*

1. *An open subgroup of G is also closed.*

2. *A closed subgroup of finite index is open.*

3. *If G is compact, then every open subgroup has finite index.*

Proof. (1) and (2) are immediate using the facts that cosets of a subgroup partition the group and each coset is homeomorphic to the original subgroup. For (3) the cosets partition the group and are also open, so there can only be finitely many of them. □

Remark 4. Consider a profinite group $G = \varprojlim G_i$. Equipping G_i with discrete topology, topology on the inverse limit is the subspace topology for the product topology on $\prod_{i \in \Gamma} G_i$. A profinite group is endowed with the inverse limit topology.

We now state a very important topological fact as a lemma to obtain a crucial result concerning profinite groups.

Lemma 6. *A compact Hausdorff space is totally disconnected (that is, if every point is a connected component) if and only if it has a basis of open neighborhoods that are also closed.*

We now give a topological characterization of profinite groups.

Proposition 7. *A profinite topological group G is compact, Hausdorff, and totally disconnected.*

Proof. Suppose G is profinite, equal to an inverse limit of a system (G_i, ϕ_{ij}) of finite groups over a directed indexing set I. The direct product $\prod_{i \in I} G_i$ of finite (discrete) groups G_i is compact Hausdorff (compactness follows from the well-known

Tychonoff's theorem). As a subset of the direct product, G is Hausdorff. To see that it is compact, we show that G is closed. Suppose that

$$(g_i) \in \prod_{i \in I} G_i$$

with $(g_i)_i \notin G_i$ and choose $i, j \in I$ with $i > j$ and $\phi_{ij}(g_i) \neq g_j$. The open subset

$$\left\{ (h_k) \in \prod_{k \in I} G_k : h_i = g_i, h_j = g_j \right\}$$

of the direct product contains (g_i) and has trivial intersection with G. Thus the complement of G is open and G itself is closed. We observe that any open set $\prod_{i \in I} U_i$ with each U_i open in G_i and $U_i = G_i$ for all but finitely many i is also closed. That is, its complement is the intersection

$$\bigcap \left((G_j \setminus U_j) \times \prod_{i \in I \setminus \{j\}} U_i \right)$$

of open sets, which is equal to the finite intersection over $j \in I$ with $U_i \neq G_i$. Therefore it follows that it is open and, by **Lemma 6** , it follows that the group G is totally disconnected. □

Lemma 7. *Let G be a profinite group and (U_i) the system of open normal subgroups in G.*

1. *Given a closed subgroup $H \subset G$, there is a canonical isomorphism*

$$H \cong \varprojlim H/(H \cap U_i)$$

of topological groups. Consequently, the group H is profinite and its profinite topology is the same as its subgroup topology.

2. If moreover H is normal, the natural map

$$\varprojlim G/HU_i \to G/H$$

is an isomorphism of topological groups as well, and therefore G/H is a profinite group.

Proof. We only prove the first statement since the proof of the second one is very similar. Observe that the quotients $H/(H \cap U_i)$ form an inverse system of finite groups as subgroups of the quotients G/U_i, so their inverse limit identifies with a subgroup of G. Thus the inclusion map $H \hookrightarrow G$ factors as a composite $H \to \varprojlim H/(H \cap U_i) \hookrightarrow G$. Each element g of the open complement of H in G has an open neighborhood of the form gU_i not meeting H and thus its class in G/U_i does not come from $\varprojlim H/(H \cap U_i)$. Hence each element of $\varprojlim H/(H \cap U_i)$ comes from H and the homomorphism $H \to \varprojlim H/(H \cap U_i)$ is a continuous bijection. Since its domain and codomain are are both compact, it follows then that it is an isomorphism of topological groups. □

Let $K|k$ be a Galois extension and let $\mathcal{E}$ denote the set of intermediate subfields $k \subset E \subset K$ such that $E|k$ is finite Galois. Then

$$K = \bigcup_{E \in \mathcal{E}} E.$$

In addition, observe that $\mathcal{E}$ is partially ordered by inclusion since the compositum $EE^{'}|k$ is a finite Galois extension containing E and $E^{'}$. If $E \subset E^{'}$, then we have a restriction map $\mathrm{Gal}(E^{'}|k) \to \mathrm{Gal}(E|k)$ by restricting the automorphisms of $E^{'}$ to E. This makes the Galois groups $\mathrm{Gal}(K|k)$ into a directed inverse system.

Proposition 8. *Let $K|k$ be a Galois extension. Then*

$$\mathrm{Gal}(K|k) \to \varprojlim \mathrm{Gal}(E|k),\ \sigma \mapsto \sigma|_E$$

where E ranges over intermediate subfields $k \subset E \subset K$ such that $E|k$ is finite Galois is an isomorphism.

Proof. It is straightforward to check that this actually maps into the direct limit and is a group homomorphism. Now let $\sigma \in \mathrm{Gal}(K|k)$. If $\sigma|_E = 1$ for all $E \in \mathcal{E}$, then since

$$L = \bigcup_{E \in \mathcal{E}} E$$

we have that $\sigma = 1$. On the other hand, if elements $\sigma_E \in \mathrm{Gal}(E|k)$ for each $E \in \mathcal{E}$ are compatible under restriction, then define $\sigma \in \mathrm{Gal}(K|k)$ by $\sigma(\alpha) = \sigma_E(\alpha)$ if $\alpha \in E$. Then if $\alpha \in E^{'}$ for some $E^{'} \in \mathcal{E}$, then

$$\sigma_{E'}(\alpha) = \sigma_{E \cap E'}(\alpha) = \sigma_E(\alpha)$$

by noting that $E \cap E^{'} \in \mathcal{E}$. Therefore σ is well-defined and so the above map is bijective. □

The above isomorphism makes $\mathrm{Gal}(K|k)$ a profinite group.

Definition 2.1.4. Let $K|k$ be a Galois extension of fields. The *Krull topology* on $\mathrm{Gal}(K|k)$ is the unique topology under which the set of $\mathrm{Gal}(K|E)$ for $E|k$ finite Galois with $E \subset K$ forms a basis of open neighborhoods of 1.

Remark 5. The Krull topology agrees with the inverse limit topology induced by the isomorphism in **Proposition 8** since

$$1 \to \mathrm{Gal}(K|E) \to \mathrm{Gal}(K|k) \to \mathrm{Gal}(E|k) \to 1$$

is exact. Thus if $K|k$ is Galois, then $\mathrm{Gal}(K|k)$ is a topological group under the Krull topology.

2.2 Cohomology of Profinite Groups

Let $G = \varprojlim G_i$ be a profinite group. By a *discrete continuous G-module*, we mean a G-module A such that the stabilizer of each $a \in A$ is open in G. Throughout this section, we assume that A is equipped with the discrete topology, so continuous G-modules are precisely the ones for which the action of G (equipped with its profinite topology) is continuous.

If $G_i = G/U_i$ is one of the standard quotients of G, then the submodule A^{U_i} is a G_i-module. The canonical surjection $\phi_{ij} \colon G_j \to G_i$ between the standard quotients induces inflation maps $\mathrm{Inf}_i^j \colon H^n(G_i, A^{U_i}) \to H^n(G_j, A^{U_j})$ for all $n \geq 0$. In addition, the compatibility condition $\phi_{ik} = \phi_{ij} \circ \phi_{jk}$ implies that the groups $H^n(G_i, A)$ together with the maps Inf_i^j form a directed system.

Definition 2.2.1. The *absolute Galois group* of a field k is the Galois group $\mathrm{Gal}(k^{\mathrm{sep}}|k)$, where k^{sep} is a separable closure of k. Let $G = \varprojlim G_i$ be a profinite group and A a continuous G-module. For all integers $n \geq 0$, we define the *n-th continuous cohomology group* $H^n_{\mathrm{cont}}(G, A)$ as the direct limit of the direct system $(H^n(G_i, A^{U_i}), \mathrm{Inf}_i^j)$ as constructed above. In the case when $G = \mathrm{Gal}(k^{\mathrm{sep}}|k)$, we also denote $(H^n(G_i, A^{U_i}), \mathrm{Inf}_i^j)$ by $H^n(k, A)$ and call it the *n-th Galois cohomology group of k with values in A.*

From now on, all cohomology groups of a profinite group in this section will be assumed to be continuous, so we drop the subscript cont from the notation. Now let us recall some results from the theory of group cohomology.

Proposition 9. *Let G be a group, H a subgroup of finite index n in G and A a G-module. Then the composite maps*

$$\mathrm{Cor} \circ \mathrm{Res} \colon H^i(G, A) \to H^i(G, A)$$

are given by multiplication by n for all $i \geq 0$.

Proof. See Gille & Szamuely [1], *Proposition 3.3.7.* □

Corollary 9.1. *Let G be a finite group of order n. Then the elements of $H^i(G, A)$ have finite order dividing n for all G-modules A and integers $i > 0$.*

Proof. Follows immediately from **Proposition 9** when $H = \{1\}$. □

We now consider some basic properties of the cohomology of profinite groups.

Proposition 10. *Fro a profinite group G and a continuous G-module A the groups $H^i(G, A)$ are torsion abelian groups for all $i > 0$. Moreover, if G is a pro-p-group, then they are p-primary torsion groups.*

Proof. This follows from the definition together with **Corollary 9.1**. □

Corollary 10.1. *Let V be a $\mathbb{Q}$-vector space equipped with a continuous action by a profinite group G. Then $H^i(G, V) = 0$, for all $i > 0$.*

Proof. It follows from the construction of cohomology that in this case the groups $H^i(G, V)$ are $\mathbb{Q}$-vector spaces. However, since they are also torsion groups for $i > 0$, they must be zero and the result follows. □

Remark 6. Let G be a profinite group, H a closed subgroup, and A a continuous G-module. We define continuous restriction maps

$$\mathrm{Res}\colon H^n(G, A) \to H^n(H, A)$$

as the direct limit of the system of composite maps

$$H^n(G/U_i, A^{U_i}) \xrightarrow{\mathrm{Res}} H^n(H/(H \cap U_i), A^{U_i}) \to H^n(H/H \cap U_i, A^{H \cap U_i})$$

where U_i are the open normal subgroups of G. Then, by **Lemma 7 (1)**, it is easy to see that the target of Res is the group $H^n(H, A)$.

In the case when H is open in G, we can define continuous corestriction maps

$$\mathrm{Cor}\colon H^n(H, A) \to H^n(G, A)$$

in a similar fashion. When H is a closed normal subgroup in G, we define the inflation maps

$$\mathrm{Inf}\colon H^n(G/H, A^H) \to H^n(G, A)$$

as the direct limit of the system of inflation maps

$$H^n(G/HU_i, A^{HU_i}) \to H^n(G/U_i, A^{U_i})$$

by observing that the groups G/HU_i have inverse limit G/H by **Lemma 7 (2).**

The construction of the maps above implies the following basic property of the cohomology of profinite groups

Proposition 11. *Let G be a profinite group, H an open subgroup of index n and A a continuous G-module. Then the composite maps*

$$\mathrm{Cor} \circ \mathrm{Res}\colon H^i(G, A) \to H^i(G, A)$$

are given by multiplication by n for all $i > 0$ Consequently, the restriction $H^i(G, A) \to H^i(H, A)$ is injective on the prime-to-n torsion part of $H^i(G, A)$.

Proof. Observe that each element of $H^i(G, A)$ comes from some $H^i(G/U_i, A^{U_i})$, so **Proposition 9** applies. For the second statement, note that the multiplication-by-n map is injective on the subgroup of elements of prime-to-n. □

We can further refine the last statement in the above proposition as follows.

Corollary 11.1. *Let G be a profinite group, p a prime number, and H a closed subgroup such that the image of H in each finite quotient of G has order prime to p.*

Then for each continuous G-module A, the restriction map $H^n(H, A) \to H^n(H, A)$ is injective on the p-primary torsion part of $H^i(G, A)$.

Proof. Assume that an element of $H^n(G, A)$ of p-power order maps to 0 in $H^n(H, A)$. It comes from an element of some $H^n(G_i, A^{U_i})$ of which we may assume, up to replacing U_i by a smaller subgroup, that it maps to 0 in $H^n(H/(H \cap U_i), A^{U_i})$. Then, by applying **Proposition 11** to the finite group G/U_i, it must be 0 and the result follows. □

2.3 Hilbert's Theorem 90

This section focuses on motivating and developing the necessary background that enables us to state and prove the famous *Hilbert's Theorem 90*, a result that plays a pivotal role in the discussion of cohomological Brauer groups.

Definition 2.3.1. A k-vector space V is called *a vector space equipped with a tensor* Φ *of type* (p, q) if Φ is an element of the tensor product $V^{\otimes p} \otimes_k (V^*)^{\otimes q}$, where $p, q \geq 0$ are integers and V^* is the dual space $\mathrm{Hom}_k(V, k)$.

Observe that there is a natural isomorphism

$$V^{\otimes p} \otimes_k (V^*)^{\otimes q} \cong \mathrm{Hom}_k(V^{\otimes q}, V^{\otimes p})$$

based on the isomorphism $\mathrm{Hom}_k(V, k) \otimes_k W \cong \mathrm{Hom}_k(V, W)$.

Example. The following cases will be the most important to us:

- The trivial case $\Phi = 0$ (with any p, q). This is just V with no additional structure.

- $p = 1, q = 1$. In this case Φ is given by a k-linear endomorphism of V.

- $p = 0, q = 2$. Then Φ is a sum of tensor products of k-linear functions. That is, a k-bilinear form $V \otimes_k V \to k$.
- $p = 1, q = 2$. This case corresponds to a k-bilinear map $V \otimes_k V \to V$.

Remark 7. Consider pairs (V, Φ) of k-vector spaces equipped with a tensor of fixed type (p, q) as above. A k-isomorphism between two such objects (V, Ψ) and (W, Ψ) is given by a k-isomorphism $f \colon V \to W$ of k-vector spaces such that

$$f^{\otimes p} \otimes (f^{*-1})^{\otimes q} \colon V^{\otimes p} \otimes_k (V^*)^{\otimes q} \to W^{\otimes p} \otimes_k (W^*)^{\otimes q}$$

maps Φ to Ψ. Note that $f^* \colon W^* \to V^*$ is the transpose isomorphism induced by f.

Now fix a Galois extension $K|k$ with Galois group $G = \mathrm{Gal}(K|k)$. Let V_K denote the K-vector space $V \otimes_k K$ and let Φ_K denote the tensor induced on V_K by Φ. This gives us a way to associate a K-object (V_K, Φ_K) with (V, Φ). We say that (V, Φ) and (W, Ψ) *become isomorphic over* K if there exists a K-isomorphism between (V_K, Φ_K) and (W_K, Ψ_K). In this case, (W, Ψ) is also called a $(K|k)$-*twisted form* of (V, Φ).

We can now make use of Galois cohomology to classify k-isomorphism classes of twisted forms. Given a k-automorphism $\sigma \colon K \to K$, tensoring by V gives a k-automorphism $V_K \to V_K$, which we again denote by σ. Each K-linear map $f \colon V_K \to W_K$ induces a map $\sigma(f) \colon V_K \to W_K$ defined by $\sigma(f) = \sigma \circ f \circ \sigma^{-1}$. Now if f is a K-isomorphism from (V_K, Φ_K) to (W_K, Ψ_K), then so is $\sigma(f)$. The map $f \to \sigma(f)$ preserves composition of automorphisms, so we get a *left action* of $G = \mathrm{Gal}(K|k)$ on the group $\mathrm{Aut}_K(\Phi)$ of K-automorphisms of (V_K, Φ_K). In addition, given two objects (V, Φ) and (W, Ψ) as well as a K-isomorphism $g \colon (V_K, \Phi_K) \to (W_K, \Psi_K)$, we get a map $G \to \mathrm{Aut}_K(\Phi)$ associating $a_\sigma := g^{-1} \circ \sigma(g)$ to $\sigma \in G$. The map a_σ satisfies the relation

$$a_{\sigma\tau} = a_\sigma \cdot \sigma(a_\tau) \tag{2.1}$$

for all $\sigma, \tau \in G$. Also, if $h\colon (V_K, \Phi_K) \to (W_K, \Psi_K)$ is another K-isomorphism, then defining $b_\sigma := h^{-1} \circ \sigma(h)$ for $\sigma \in G$ gives us the relation

$$a_\sigma = c^{-1} b_\sigma \sigma(c) \tag{2.2}$$

where c is the K-automorphism $h^{-1} \circ g$.

Definition 2.3.2. Let G be a group and A be another group on which G acts on the left. Then a 1-*cocycle* of G with values in A is a map $\sigma \mapsto a_\sigma$ from G to A satisfying the relation (2.1) as above. Two 1-cocycles a_σ and b_σ are called *equivalent* if there exists $c \in A$ such that the relation (2.2) holds.

We define the *first cohomology set* $H^1(G, A)$ of G with values in A as the quotient of the set of 1-cocycles by the equivalence relation (2.2). It is a *pointed set.* That is, a set equipped with a distinguished element coming from the trivial cocycle $\sigma \mapsto 1$, where 1 is the identity element of A. We call this element the *base point.*

Remark 8. Let A be a group equipped with a left action by another group G. Assume that X is a set on which both G and A act in a compatible way. That is, we have $\sigma(a(x)) = (\sigma(a))(\sigma(x))$ for all $x \in X, a \in A$ a,d $\sigma \in G$. Suppose that we have a 1-cocycle $\sigma \mapsto a_\sigma$ of G with values in A. Then we define the *twisted action of* G *on* X *by the cocycle* a_σ by

$$(\sigma, x) \mapsto a_\sigma(\sigma(x)).$$

It is straightforward to check that this is a G-action. The notation ${}_aX$ will mean that X is equipped with the twisted G-action by the cocycle a_σ.

Now we state a lemma that leads us to the main result of this section.

Lemma 8 (**Speiser**). *Let $K|k$ be a finite Galois extension with group G and V a*

K-vector space equipped with a semi-linear G-action. That is, a G-action satisfying

$$\sigma(\lambda v) = \sigma(\lambda)\sigma(v)$$

for all $\sigma \in G, v \in V, \lambda \in K$. Then the natural map

$$\lambda\colon V^G \otimes_k K \to V$$

is an isomorphism, where V^G denotes the invariants under G.

Proof. See Gille & Szmauely [1], *Lemma 2.3.8.* □

Note that in our situation, the class $[a_\sigma]$ in $H^1(G, \mathrm{Aut}_K(\Phi))$ of the 1-cocycle a_σ associated with the K-isomorphism $g\colon (V_K, \Phi_K) \to (W_K, \Psi_K)$ depends only on (W, Ψ) but not on the map g. This enables us to state the following crucial result.

Theorem 2.3.1. *For a k-object (V, Φ), consider the pointed set $TF_K(V, \Phi)$ of twisted $(K|k)$-forms of (V, Φ), the base point being given by (V, Φ). Then the map $(W, \Psi) \to [a_\sigma]$ defined as above yields a base point preserving bijection*

$$TF_K(V, \Phi) \longleftrightarrow H^1(G, \mathrm{Aut}_K(\Phi)).$$

Proof. Our main goal is to show that taking the invariant space $({}_aV_K)^G$ under the twisted action yields a twisted form of (V, Φ). So let a_σ be a 1-cocycle representing some cohomology class in $H^1(G, \mathrm{Aut}(\Phi))$ and consider the invariant subspace $W := ({}_aV_K)^G$. Note that $\sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$ since Φ_K comes from the k-tensor Φ. Also, observe that $a_\sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$ as $a_\sigma \in \mathrm{Aut}_K(\Phi)$. Thus $a_\sigma\sigma(\Phi_K) = \Phi_K$ for all $\sigma \in G$, which implies that Φ_K comes from a k-tensor on W. Denoting this tensor by Ψ, we have defined a k-object (W, Ψ). Then **Speiser's Lemma** gives us an isomorphism $W \otimes_k K \cong V_K$ and by construction this isomorphism identifies

Ψ_K with Φ_K. Thus (W, Ψ_K) is indeed a twisted form of (V, Φ). If $a_\sigma = c^{-1} b_\sigma \sigma(c)$ with some 1-cocycle $\sigma \mapsto b_\sigma$ and $c \in \mathrm{Aut}_K(\Phi)$, we see from the definitions that $({}_bV_K)^G = c(W)$, which is a k-vector space isomorphic to W. Thus, we have a well-defined map $H^1(G, \mathrm{Aut}_K(\Phi)) \to TF_K(V, \Phi)$. It is straightforward to check that this map is the inverse of the map $(W, \Psi) \mapsto [a_\sigma]$ of the theorem. □

Remark 9. Let $K|k$ is a finite Galois extension and suppose V is an n-dimensional vector space over k and Φ is the trivial tensor. Then $\mathrm{Aut}_K(\Phi)$ is just the group of $\mathrm{GL}_n(K)$ of invertible $n \times n$ matrices. On the other hand since any two n-dimensional k-vector spaces are already isomorphic over k, by **Theorem 2.3.1**, we see that

$$H^1(G, \mathrm{GL}_n(K)) = \{1\}.$$

In particular when $n = 1$, we see that $H^1(G, K^\times)$ is trivial. The case $n = 1$ is called *Hilbert's Theorem 90* which we will state formally as follows.

Theorem 2.3.2 (**Hilbert's Theorem 90**). *If $K|k$ is a finite Galois extension with Galois group $G = \mathrm{Gal}(K|k)$, then*

$$H^1(G, K^\times) = \{1\}.$$

That is, the first cohomology group of G with values in $K^\times$ is trivial.

2.4 Brauer Group as Galois Cohomology Group

The main goal of this section is to identify the Brauer group of a field k with a certain profinite cohomology group. In particular,

$$\mathrm{Br}(k) \cong H^2(\mathrm{Gal}(k^{\mathrm{sep}}|k), (k^{\mathrm{sep}})^\times).$$

In general, if $K|k$ is a Galois extension, then we have

$$\mathrm{Br}(K|k) \cong H^2(\mathrm{Gal}(K|k), K^\times).$$

We establish this result by first considering the case when $K|k$ is finite Galois and then extending the result in the infinite case *via* direct limits.

Let $K|k$ be a finite Galois extension of degree n and let $G = \mathrm{Gal}(K|k)$. Note that every element of $\mathrm{Br}(K|k)$ can be represented by a central simple k-algebra A of dimension n^2 which contains K. By **Theorem 1.3.1 (Skolem-Noether)**, for every $\sigma \in G$, there exists $x_\sigma \in A^\times$ such that

$$x_\sigma a x_\sigma^{-1} = \sigma(a)$$

for all $a \in K$.

Lemma 9. *The set $\{x_\sigma : \sigma \in G\}$ is a basis of A over K.*

Proof. Note that since $\dim_K A = n = |G|$, it suffices to show that these elements are linearly independent over K. Assume, for a contradiction, that they are linearly dependent and let

$$a_1 x_{\sigma_1} + \cdots + a_r x_{\sigma_r} = 0$$

be the shortest possible relation of linear dependence, so $a_i \neq 0$. Clearly, $r > 1$. Now choose $\alpha \in K$ such that $K = k(\alpha)$, so $\sigma_i(\alpha) \neq \sigma_j(\alpha)$, for $i \neq j$. Then we have

$$0 = \sigma_r(\alpha)(a_1 x_{\sigma_1} + \cdots + a_r x_{\sigma_r}) - (a_1 x_{\sigma_1} + \cdots + a_r x_{\sigma_r})\alpha$$

$$= a_1(\sigma_r(\alpha) - \sigma_1(\alpha))x_{\sigma_1} + \cdots + a_{r-1}(\sigma_r(\alpha) - \sigma_{r-1}(\alpha))x_{\sigma_{r-1}}$$

which is a shorter relation of linear dependence in which all the coefficients are nonzero, a contradiciton. Therefore

$$A = \bigoplus_{\sigma \in G} K x_\sigma.$$

□

Note that for $a_\sigma, a_\tau \in K$, we have

$$(a_\sigma x_\sigma)(a_\tau x_\tau) = (a_\sigma \sigma(a_\tau)) x_\sigma x_\tau.$$

Thus to understand multiplication in A, it is enough to describe the products $x_\sigma x_\tau$ for all $\sigma, \tau \in G$. For this we simply compute the action of these products on K. For any $a \in K$, we have

$$(x_\sigma x_\tau) a (x_\sigma x_\tau)^{-1} = x_\sigma (x_\tau a x_\tau^{-1}) x_\sigma^{-1} = \sigma(\tau(a)) = (\sigma\tau)(a) = x_{\sigma\tau} a x_{\sigma\tau}^{-1}.$$

It follows then that $c_{\sigma,\tau} := x_{\sigma\tau}^{-1} x_\sigma x_\tau$ centralizes K and thus $c_{\sigma,\tau} \in K^\times$. Then we can write

$$x_\sigma x_\tau = x_{\sigma\tau} c_{\sigma,\tau} = a_{\sigma,\tau} x_{\sigma\tau}$$

where $a_{\sigma,\tau} := x_{\sigma\tau} c_{\sigma,\tau} x_{\sigma\tau}^{-1} = (\sigma\tau)(c_{\sigma,\tau}) \in K^\times$. Hence multiplication in A is completely determined by simply specifying the elements $a_{\sigma,\tau} \in K^\times$, for all $\sigma, \tau \in G$.

Definition 2.4.1. The collection $\{a_{\sigma,\tau}\}$ is called a *factor set* of A relative to K.

Definition 2.4.2. Let G be a group and A an abelian group equipped with a left G-action. A 2-*cocycle of* G *with values in* A is a map $(\sigma, \tau) \mapsto a_{\sigma,\tau}$ from $G \times G \to A$ satisfying the relation

$$\sigma(a_{\tau,\nu}) a_{\sigma\tau,\nu}^{-1} a_{\sigma,\tau\nu} a_{\sigma,\tau}^{-1} = 1$$

for all $\sigma, \tau, \nu \in G$. These form an abelian group $Z^2(G, A)$ for the multiplication induced from that of A. Two 2-cocycles $a_{\sigma,\tau}$ and $a'_{\sigma,\tau}$ are *cohomologous* if $a_{\sigma,\tau} {a'_{\sigma,\tau}}^{-1}$

is a 2-*coboundary*. That is, it is of the form $(\sigma, \tau) \mapsto a_\sigma \sigma(a_\tau) a_{\sigma\tau}^{-1}$ with some map $\sigma \mapsto a_\sigma$ from G to A. It is straightforward to check that 2-coboundaries are 2-cocycles and form a subgroup in $Z^2(G, A)$ denoted by $B^2(G, A)$. Thus the set $H^2(G, A)$ of cohomology classes of 2-cocycles is an abelian group called the *second cohomology group of G with values in A.*

Remark 10. Now we state some facts regarding factor sets that are easy to verify.

1. Factor sets can be viewed as functions

$$G \times G \to K^\times,\ (\sigma, \tau) \mapsto a_{\sigma,\tau}.$$

2. The functions $a_{\sigma,\tau}$ are in fact 2-cocycles and therefore can be viewed as elements of $Z^2(G, K^\times)$ since they satisfy the relations

$$\rho(a_{\sigma,\tau}) a_{\rho,\sigma\tau} = a_{\rho,\sigma} a_{\rho\sigma,\tau}$$

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

3. Note that if we replace A with another Brauer equivalent central simple $A^{'}$ and repeat the construction as above to obtain a factor set $\{a^{'}_{\sigma,\tau}\}$ for $A^{'}$, then there exists elements $b_\sigma \in K^\times$ such that

$$a^{'}{}_{\sigma,\tau} = \left(\frac{b_\sigma \sigma(b_\tau)}{b_{\sigma\tau}}\right) a_{\sigma,\tau}.$$

Observe that $\left(\frac{b_\sigma \sigma(b_\tau)}{b_{\sigma\tau}}\right)$ are elements of the group of 2-coboundaries $B^2(G, K^\times)$. Thus we can associate a well-defined element of $H^2(G, K^\times)$ to every isomorphism class of central simple k-algebras A having dimension n^2 and containing K. Now combining this with the fact that every element of $\mathrm{Br}(K|k)$ can be represented uniquely upto isomorphism such algebra, we get a well defined map

$$\phi\colon \mathrm{Br}(K|k) \to H^2(G, K^\times),\ [A] \mapsto \{a_{\sigma,\tau}\} \pmod{B^2(G, K^\times)}.$$

Lemma 10. *The map* $\phi\colon \mathrm{Br}(K|k) \to H^2(G, K^\times)$ *(as defined above) is injective.*

Proof. Let A and $A^{'}$ be two central simple k-algebras having dimension n^2 and containing K. Assume that

$$A = \bigoplus_{\sigma\in G} Lx_\sigma \text{ and } A^{'} = \bigoplus_{\sigma\in G} Lx^{'}_\sigma$$

where the elements $x_\sigma, x^{'}_\sigma$ satisfy the relations

$$x_\sigma a x_\sigma^{-1} = \sigma(a) \text{ and } x^{'}_\sigma a x^{'-1}_\sigma = \sigma(a)$$

for all $a \in K$. The corresponding factor sets are defined by

$$x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau} \text{ and } x^{'}_\sigma x^{'}_\tau = a^{'}_{\sigma,\tau} x^{'}_{\sigma\tau}.$$

Observe that if $\phi([A]) = \phi([A^{'}])$, then there exists elements $b_\sigma \in K^\times$ such that the relation in **Remark 10** holds. We need to show that $A \cong A^{'}$. To do so, we define a map $f\colon A \to A^{'}$ as

$$f\left(\sum_\sigma a_\sigma x_\sigma\right) = \sum_\sigma a_\sigma b_\sigma^{-1} x^{'}_\sigma.$$

It is straightforward to check that f is an isomorphism of K-vector spaces and that it is multiplicative by simply checking that f is multiplicative on elements of the form $a_\sigma x_\sigma$ because of the distributive law. Hence it follows that $A \cong A^{'}$, so ϕ is injective. □

Lemma 11. *The map* $\phi\colon \mathrm{Br}(K|k) \to H^2(G, K^\times)$ *(as defined above) is surjective.*

Proof. Let $\{a_{\sigma,\tau}\}$ be an arbitrary element of $Z^2(G, K^\times)$. Consider an n-dimensional vector space over K with a basis $\{x_\sigma : \sigma \in G\}$

$$A = \bigoplus_{\sigma \in G} L x_\sigma.$$

Now we define multiplication on A by the formula

$$\left(\sum_\sigma a_\sigma x_\sigma\right)\left(\sum_\sigma a_\sigma x_\sigma\right) := \sum_{\sigma,\tau} a_\sigma \sigma(b_\tau) a_{\sigma,\tau} x_{\sigma\tau}.$$

It is straightforward to see that this multiplication is k-bilinear and satisfies the associative and distributive laws, so A is a k-algebra. Also note that $u := a^{'}_{1,1} x_1$ is an identity element for A and $x_\sigma^{'-1} = (a_{\sigma^{-1},\sigma} a^{'}_{1,1})^{-1} x_{\sigma^{-1}}$ is an inverse for x_σ, so x_σ is invertible. Now suppose $z = \sum a_\sigma x_\sigma \in Z(A)$. Then for any $a \in K$

$$a\left(\sum a_\sigma x_\sigma\right) = \sum a a_\sigma x_\sigma = \left(\sum a_\sigma x_\sigma\right) a = \sum a_\sigma \sigma(a) x_\sigma$$

so it follows that $a_\sigma(a - \sigma(a)) = 0$, for all $\sigma \in G$. Now choose a such that $K = k(a)$. Then for any $\sigma \neq 1$, we have $\sigma(a) \neq a$, so the above relation gives $a_\sigma = 0$. Thus $z \in K$. Then $x_\sigma z x_\sigma^{-1} = \sigma(z) = z$, for any $\sigma \in G$, so $z \in k$. Thus A is a central k-algebra.

Let $I \subset A$ be a nonzero two-sided ideal. Choose a nonzero element $a \in I$ that has the shortest presentation of the form

$$a = a_{\sigma_1} x_{\sigma_1} + \cdots + a_{\sigma_r} x_{\sigma_r}$$

Then all the coefficients are nonzero. Now, assume that $r > 1$. Then a similar argument as in **Lemma 9** shows that this leads to a contradiction, so $r = 1$. Then $a = a_{\sigma_1} x_{\sigma_1}$. Since any nonzero element of this form is invertible, we see that $A = I$, so A is a central simple k-algebra. By construction, we have $\phi([A]) = \{a_{\sigma,\tau}\}$, so ϕ is surjective.

□

Definition 2.4.3. The algebra A as constructed in the proof of **Lemma 11** is called the *crossed product of* K *and* G *relative to the factor set* $\{a_{\sigma,\tau}\}$ and is denoted by $(L, G, \{a_{\sigma,\tau}\})$.

Now we have all the necessary ingredients to prove the following crucial result.

Theorem 2.4.1. *The map* $\phi\colon \mathrm{Br}(K|k) \to H^2(G, K^\times)$ *(as defined above) is a group isomorphism.*

Proof. It is easy to see that, by **Lemma 10** and **Lemma 11**, ϕ is bijective. It only remains to show that ϕ is a group homomorphism. Let $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ be two factor sets and consider the factor set $c_{\sigma,\tau} \coloneqq a_{\sigma,\tau}b_{\sigma,\tau}$. Let

$$A = \bigoplus_{\sigma} Lx_\sigma,\ B = \bigoplus_{\sigma} Ly_\sigma,\ C = \bigoplus_{\sigma} Lz_\sigma$$

where

$$x_\sigma a x_\sigma^{-1} = y_\sigma a y_\sigma^{-1} = z_\sigma a z_\sigma^{-1} = \sigma(a)$$

for all $a \in K$ and

$$x_\sigma x_\tau = a_{\sigma,\tau}x_{\sigma\tau},\ y_\sigma y_\tau = b_{\sigma,\tau}y_{\sigma\tau},\ z_\sigma z_\tau = c_{\sigma,\tau}z_{\sigma\tau}$$

be the corresponding crossed products. We will show that $[C] = [A][B] = [A \otimes_k B]$ by proving that $A \otimes_k B \cong M_n(C)$. In order to do so, consider $M \coloneqq A \otimes_K B$, where both A and B are treated as left K-modules. Note that $\dim_K A = \dim_K B = n$, so $\dim_K M = n^2$. Then we can give M a right $(A \otimes_k B)$-module structure such that

$$(x \otimes_K y)(a \otimes_k b) = xa \otimes_K yb.$$

Now we claim that there is a left C-module structure on M such that

$$(c_\sigma z_\sigma)(a \otimes_K b) = (c_\sigma x_\sigma a) \otimes_K y_\sigma b.$$

Observe that the left multiplications by $c_\sigma x_\sigma$ and y_σ are k-linear maps of A and B respectively, so there exists a k-linear map $\theta\colon A \otimes_k B \to A \otimes_k B$ such that $(a \otimes_k b) \mapsto (c_\sigma x_\sigma a) \otimes_k y_\sigma b$. But M can be written as $(A \otimes_k B)/R$, where R is the k-vector subspace of $A \otimes_k B$ spanned by elements of the form $\theta(la \otimes b - a \otimes lb)$, for all $a \in A, b \in B$ and $l \in L$. Note that

$$\theta(la \otimes b - a \otimes lb) = \sigma(l) c_\sigma x_\sigma a \otimes y_\sigma b - c_\sigma x_\sigma a \otimes \sigma(l) y_\sigma b \in R$$

so $\theta(R) \subset R$. Thus θ induces a k-linear map on M such that $\theta(a \otimes b) = c_\sigma x_\sigma a \otimes y_\sigma b$ and this is precisely the multiplication map by $c_\sigma z_\sigma$. It is straightforward to check that this multiplication extends to a map $C \times M \to M$ such that $(c_1 + c_2)m = c_1 m + c_2 m$ and $(c_1 c_2)m = c_1(c_2 m)$. It is also easy to see that

$$(cm)(a \otimes_k b) = c(m(a \otimes_k b)).$$

It follows then that the right multiplication by $A \otimes_k B$ gives rise to a k-algebra homomorphism

$$\gamma\colon (A \otimes_k B)^\circ \to \mathrm{End}_C(M).$$

Since $A \otimes_k B$ is simple, $(A \otimes_k B)^\circ$ is also simple, so ϕ is injective. Note that we have

$$\dim_k M = n^3 = dim_k C^n$$

so since C is simple, it follows then that $M \cong C^n$ as C-modules. Then

$$\mathrm{End}_C(M) \cong M_n(C)^\circ \cong M_n(C^\circ).$$

Thus $\dim_k \mathrm{End}_C(M) = n^2 \cdot \dim_k C = n^4 = \dim_k A \otimes_k B$, so γ is surjective. Thus γ is an isomorphism, so we have

$$A \otimes_k B \cong (\mathrm{End}_C(M))^\circ \cong M_n(C).$$

Thus ϕ is a group homomorphism and hence an isomorphism. □

We have thus shown that for a finite Galois extension $K|k$

$$\mathrm{Br}(K|k) \cong H^2(G, K^\times)$$

where $G = \mathrm{Gal}(K|k)$.

We now extend this isomorphism to infinite Galois extensions. Suppose $K|k$ is an infinite Galois extension with $G = \mathrm{Gal}(K|k)$. Let $\{P_i\}_{i\in I}$ be a family of finite Galois extensions of k contained in K such that $K = \bigcup_{i\in I} P_i$ and for any $i, j \in I$, there exists $k \in I$ such that $P_i, P_j \subset P_k$. Then we have $G = \varprojlim G_i$, where $G_i = \mathrm{Gal}(P_i|k) = \mathrm{Gal}(K|k)/\mathrm{Gal}(K|P_i)$. It is straightforward to check that $\mathrm{Br}(K|k) = \bigcup_{i\in I} \mathrm{Br}(P_i|k)$.

Remark 11. We can interpret $\mathrm{Br}(K|k) = \bigcup_{i\in I} \mathrm{Br}(P_i|k)$ as follows: For $P_i \subset P_j$, consider the inclusion map $\iota_j^i \colon \mathrm{Br}(P_i|k) \to \mathrm{Br}(P_j|k)$. Then $\left\{\mathrm{Br}(P_i|k), \iota_j^i\right\}$ is a direct system and

$$\mathrm{Br}(K|k) = \varinjlim \left\{\mathrm{Br}(P_i|k), \iota_j^i\right\}.$$

On the other hand, note that for $P_i \subset P_j$, we have the natural surjective map

$\rho_i^j\colon \mathrm{Gal}(P_j|k) \to \mathrm{Gal}(P_i|k)$ which gives us the inflation map

$$\theta_j^i\colon H^2(\mathrm{Gal}(P_i|k), P_i^\times) \to H^2(\mathrm{Gal}(P_j|k), P_j^\times)$$

defined by sending the class of a cocycle $\{a_{\sigma,\tau}\} \in Z^2(\mathrm{Gal}(P_i|k), P_i^\times)$ to the class of the cocylce $\hat{a}_{\hat{\sigma},\hat{\tau}} \in Z^2(\mathrm{Gal}(P_j|k), P_j^\times)$ given by $\hat{a}_{\hat{\sigma},\hat{\tau}} = a_{\rho_i^j(\hat{\sigma}),\rho_i^j(\hat{\tau})}$. Then, by the definition of the cohomology of profinite groups, we have

$$H^2(G, K^\times) = \varinjlim \left\{H^2(\mathrm{Gal}(P_i|k), P_i^\times), \theta_j^i\right\}$$

Now for each i, by **Theorem 2.4.1**, we have an isomorphism $\phi_{P_i|k}\colon \mathrm{Br}(P_i|k) \to H^2(G_i, P_i^\times)$. So, in order to construct an isomorphism $\phi_{K|k}\colon \mathrm{Br}(K|k) \to H^2(G, K^\times)$, it suffices to show that the system $\{\phi_{P_i|k}\}$ defines an isomorphism between the direct systems $\{\mathrm{Br}(P_i|k), \iota_j^i\}$ and $\{H^2(\mathrm{Gal}(P_i|k), P_i^\times), \theta_j^i\}$. Then we can set $\phi_{K|k} = \varinjlim \phi_{P_i|k}$

Proposition 12. *Let $E \subset F$ be finite Galois extensions of k. Let $\iota\colon \mathrm{Br}(E|k) \to \mathrm{Br}(F|k)$ be the natural embedding and let $\theta\colon H^2(\mathrm{Gal}(E|k), E^\times) \to H^2(\mathrm{Gal}(F|k), F^\times)$ be the inflation map. Then the diagram*

$$\begin{tikzcd}
\mathrm{Br}(P_i|k) \arrow[r, "\iota"] \arrow[d, "\phi_{E|k}"'] & \mathrm{Br}(P_j|k) \arrow[d, "\phi_{F|k}"] \\
H^2(G_i, P_i^\times) \arrow[r, "\theta"] & H^2(G_j, P_j^\times)
\end{tikzcd}$$

is commutative.

Proof. Let $[E : k] = m, [F : k] = n, r = n/m$, and let $\rho\colon \mathrm{Gal}(F|k) \to \mathrm{Gal}(E|k)$ be the canonical map. Observe that any element of $\mathrm{Br}(E|k)$ can be represented by an algebra A which is a crossed product $(E, \mathrm{Gal}(E|k), \{a_{\sigma,\tau}\})$ for some factor set $\{a_{\sigma,\tau}\}$.

Then

$$A = \bigoplus_{\sigma \in \mathrm{Gal}(E|k)} E x_\sigma$$

where $x_\sigma a x_\sigma^{-1} = \sigma(a)$, for all $a \in E$ and $x_\sigma x_\tau = a_{\sigma,\tau} x_{\sigma\tau}$.

Then $\theta(\phi_{E|k}([A]))$ is represented by the cocycle $\hat{a}_{\hat{\sigma},\hat{\tau}}$ such that $\hat{a}_{\hat{\sigma},\hat{\tau}} = a_{\rho(\hat{\sigma}),\rho(\hat{\tau})}$. On the other hand, $\iota([A]) = [B]$, where $B = M_r(A)$. Thus in order to prove the claim, it suffices to show that

$$B = \bigoplus_{\hat{\sigma} \in \mathrm{Gal}(F|k)} F y_{\hat{\sigma}}$$

where $y_{\hat{\sigma}} b y_{\hat{\sigma}}^{-1} = \hat{\sigma}(b)$, for all $b \in F$ and $y_{\hat{\sigma}} y_{\hat{\tau}} = a_{\hat{\sigma},\hat{\tau}} y_{\hat{\sigma}\hat{\tau}}$.

To do so, we pick a basis $e_1, \ldots, e_r$ if F over E and embed F into $M_r(E) \subset B$ using the left regular representation λ given by

$$\lambda(b) = (s_{ij}) \text{ where } b e_j = \sum_{i=1}^{r} s_{ij} e_i.$$

In addition, for $\hat{\sigma} \in \mathrm{Gal}(F|k)$, we set

$$\mu(\hat{\sigma}) = (t_{ij}) \text{ where } \hat{\sigma}(e_j) = \sum_{i=1}^{r} t_{ij} e_i.$$

Now define an action of $\mathrm{Gal}(F|k)$ on $M_r(E)$ by

$$\hat{\sigma}((u_{ij})) = (\rho(\hat{\sigma})(u_{ij})).$$

Then we have the relations $\mu(\hat{\sigma}\hat{\tau}) = \mu(\hat{\sigma})\hat{\sigma}(\mu(\hat{\tau}))$ and $\lambda(\hat{\sigma}(b))\mu(\hat{\sigma}) = \mu(\hat{\sigma})\hat{\sigma}(\lambda(b))$. A straightforward computation shows that $y_{\hat{\sigma}} := \mu(\hat{\sigma})\tilde{x}_{\hat{\sigma}}$ where $\tilde{x} = \mathrm{diag}(x_{\rho(\hat{\sigma})}, \ldots, x_{\rho(\hat{\sigma})})$ satisfies the equations $y_\sigma b y_{\hat{\sigma}}^{-1} = \hat{\sigma}(b)$ for all $b \in F$ and $y_{\hat{\sigma}} y_{\hat{\tau}} = \hat{a}_{\hat{\sigma},\hat{\tau}} y_{\hat{\sigma}\hat{\tau}}$, so the result follows. □

Note that, by **Corollary 5.1**, $\mathrm{Br}(k) = \mathrm{Br}(k^{\mathrm{sep}}|k)$, where k^{sep} is a separable closure of k. This gives us the following theorem.

Theorem 2.4.2. *For any Galois extension $K|k$, there is an isomorphism*

$$\phi_{K|k}\colon \mathrm{Br}(K|k) \to H^2(\mathrm{Gal}(K|k), K^\times).$$

In particular, $\mathrm{Br}(k) \cong H^2(\mathrm{Gal}(k^{\mathrm{sep}}|k), (k^{\mathrm{sep}})^\times)$.

Corollary 2.4.2.1. *Let $K|k$ be a Galois extension of degree n. Then each element of the relative Brauer group $\mathrm{Br}(K|k)$ has order dividing n.*

Proof. This follows from the above theorem together with **Corollary 9.1**. □

Corollary 2.4.2.2. *Let ${}_n\mathrm{Br}(k)$ denote the n-torsion part of the Brauer group. For each positive integer m prime to the characteristic of k, we have a canonical isomorphism*

$${}_m\mathrm{Br}(k) \cong H^2(k, \mu_m)$$

where μ_m denotes the group of m-th roots of unity in k^{sep} equipped with its canonical Galois action.

Proof. Consider the exact sequence of $\mathrm{Gal}(k^{\mathrm{sep}}|k)$-modules

$$1 \to \mu_m \to (k^{\mathrm{sep}})^\times \xrightarrow{m} (k^{\mathrm{sep}})^\times \to 1$$

where the third map is given by raising elements to the m-th power. This map is surjective because the polynomial $x^m - a$ is separable for all $a \in k^{\mathrm{sep}}$, in view of the assumption on m. A piece of the associated long exact sequence is

$$H^1(k, (k^{\mathrm{sep}})^\times) \to H^2(k, \mu_m) \to H^2(k, (k^{\mathrm{sep}})^\times) \to H^2(k, (k^{\mathrm{sep}})^\times)$$

where the first group is trivial by **Hilbert's Theorem 90**. The corollary follows by noting that the last map is multiplication by m. □

Remark 12. Let G be a finite cyclic group of order n generated by an element σ. Consider the maps $\mathbb{Z}[G] \to \mathbb{Z}[G]$ defined by

$$N\colon a \mapsto \sum_{i=0}^{n-1} \sigma^i a \quad \text{and} \quad \sigma - 1\colon a \mapsto \sigma a - a.$$

It is straightforward to check that $\ker(N) = \mathrm{Im}(\sigma - 1)$ and $\mathrm{Im}(N) = \mathrm{Ker}(\sigma - 1)$. Hence we have a free resolution

$$\cdots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

where the last map is induced by $\sigma \mapsto 1$.

For a G module A, define maps $N\colon A \to A$ and $\sigma - 1\colon A \to A$ by the same formulae as above and set ${}_NA \coloneqq \mathrm{Ker}(N)$. Then using the above resolution, it follows easily that

$$H^0(G, A) = A^G, \quad H^{2i+1}(G, A) =_N A/(\sigma - 1)A, \quad H^{2i+2}(G, A) = A^G/NA$$

for all $i > 0$.

Corollary 2.4.2.3. *For a cyclic Galois extension $K|k$, there is an isomorphism*

$$\mathrm{Br}(K|k) \cong k^\times/N_{K|k}(K^\times).$$

Proof. The result follows easily from **Theorem 2.4.2** in view of the calculation of the cohomology of cyclic groups above. □

2.5 Some Computations

We conclude this chapter by computing the Brauer groups of some special fields. Let us start with algebraically closed fields.

Proposition 13. *Let k be an algebraically closed field. Then*

1. *The only finite-dimensional division algebra over k is k itself.*

2. *If A is a finite dimensional simple k-algebra, then $A \cong M_n(k)$, for some n*

3. $\mathrm{Br}(k)$ *is trivial.*

Proof. (1) This follows as an easy consequence of **Corollary 1.1.1.1**.

(2) Observe that, by **Wedderburn's Theorem**, $A \cong M_n(D)$ for some division algebra D over k, so by (1) it follows that $D = k$. Hence $A \cong M_n(k)$.

(3) Note that $M_n(k)$ represents the identity element of $\mathrm{Br}(k)$, so from (2) it follows that every element in the Brauer group is equivalent to the identity. Thus $\mathrm{Br}(k)$ is trivial. □

We now compute the Brauer group of the field of real numbers.

Proposition 14. $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. Note that $\mathrm{Br}(\mathbb{R}) = \mathrm{Br}(\mathbb{C}|\mathbb{R})$. Then, by **Corollary 2.4.2.3**, we have

$$\mathrm{Br}(\mathbb{C}|\mathbb{R}) \cong \mathbb{R}^\times / N_{\mathbb{C}|\mathbb{R}}(\mathbb{C}^\times).$$

The image of the norm map $\mathbb{C}^\times \to \mathbb{R}^\times$ is $\mathbb{R}_{>0}$, so we have

$$\mathrm{Br}(\mathbb{R}) \cong \mathrm{Br}(\mathbb{C}|\mathbb{R}) \cong \mathbb{R}^\times / \mathbb{R}_{>0} \cong \mathbb{Z}/2\mathbb{Z}.$$

Thus it follows that $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. □

Finally we compute the Brauer group of a finite field.

Proposition 15. *Let $k = \mathbb{F}_q$ be a finite field with q elements. Then* $\mathrm{Br}(k)$ *is trivial.*

Proof. Let $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$, so $K|k$ is cyclic and its Galois group is generated by the corresponding Frobenius automorphism. Then, by **Corollary 2.4.2.3**, we have

$$\mathrm{Br}(K|k) \cong k^\times / N_{K|k}(L^\times).$$

However it is a well-known fact that the norm map over finite fields is surjective, so $\mathrm{Br}(K|k)$ is trivial for any finite extension $K|k$ and therefore $\mathrm{Br}(k)$ is trivial. □

2.6 Central Simple Algebras Over Complete Discrete Valued Fields

Let K denote a field complete with respect to a discrete valuation with perfect residue field κ.

Lemma 12. *Suppose D is a central division K-algebra of degree $d > 1$. The discrete valuation ν of K extends to a unique discrete valuation on D given by the formula*

$$w = \frac{1}{d} v \circ \mathrm{Nrd}_D$$

where Nrd_D *is the reduced norm map. In addition, D is complete with respect to w.*

Proof. See Gille & Szamuely [1], *Proposition 2.9.2.* □

Proposition 16. *Every central division algebra D of degree $d > 0$ over K contains a K-subalgebra L that is an unramified field extension of K of degree > 1.*

Proof. The key tool in this proof is the extension of the valuation K to D. A discrete valuation on a division algebra D, by definition, is a map $w \colon D \to \mathbb{Z} \cup \{\infty\}$ satisfying the same properties as in the commutative case. The elements satisfying $w(x) \geq 0$ form a subring $A_w \subset D$ in which the set M_w of elements with $w(x) > 0$ is a two-sided ideal. Fixing an element $\pi \in D$ such that $w(\pi)$ is the positive generator of the group $w(D \setminus \{0\}) \subset \mathbb{Z}$, we can write each $m \in M_w$ as $m = b\pi$, wehre $b \in A_w$. Thus we start by extending the valuation ν of K to a discrete valuation w of D as in **Lemma 12**. If the statement of the proposition is false, then for each finite field extension $L|K$ contained in D, the valuation $w|_L$ has residue field equal to that of ν. In particular, this is true for any $b \in A_w$. Fixing b, we thus find a_0 in the ring of integers A_v of K with $b - a_0 \in M_w$. Fixing a generator π as mentioned before, we have

$$b = a_0 + b_1\pi$$

with some $b_1 \in A_w$. Repeating this procedure with b_1 in place of b and continuing in the same fashion, we construct inductively for each $N > 0$ elements $a_N \in A_v$ and $b_N \in A_w$ such that

$$b = \sum_{i=0}^{N-1} a_i\pi^i + b_N\pi^N.$$

Then we infer that b is in the closure of the subfield $K(\pi) \in D$ for the w-adic topology on D. But $K(\pi)$is closed in D (this is true for any linear subspace in a finite-dimensional normed vector space over a complete valued field), so $b \in K(\pi)$. Since b was arbitrarily here and for every $x \in D$, we have $x\pi^m \in A_w$, for m large enough. we conclude that $D \subset K(\pi)$, which is a contradiction since the center of D is K. Thus the result follows. □

Definition 2.6.1. Let A be a central simple algebra over a field k. The *index* of A over k, denoted by $\mathrm{ind}_k(A)$ is defined to be the degree of D over k, where D is the division algebra for which $A \cong M_n(D)$.

Theorem 2.6.1. *Every central simple algebra A over K is split by a finite unramified extension of K*

Proof. We use induction on the index d of A. The case $d = 1$ is obvious. Using **Wedderburn's Theorem**, we may assume that A is a division algebra of degree d. Then, by **Proposition 16**, we find a non-trivial unramified extension $L|K$ that embeds in A over K. The L-algebra $A \otimes_K L$ is not a division algebra since it contains $L \otimes_K L$ which is a product of copies of L. Thus $\mathrm{ind}(A \otimes_K L) < \mathrm{ind}(A) = d$, and so $A \otimes_K L$ splits over an unramified extension and the result follows. □

Corollary 2.6.1.1. *The Brauer group* $\mathrm{Br}(K_{nr}) = 0$*, where* K_{nr} *denotes the maximal unramified extension of* K*.*

Proof. Every central simple algebra A over K_{nr} is defined over a finite extension $L|K$ which is contained in K_{nr}. The field L is again a complete discrete valued field with perfect residue field. and $L_{nr} = K_{nr}$. Then, by **Theorem 2.6.1**, A is split by a finite unramified extension which is still contained in K_{nr}, and hence A is split over K_{nr} and the result follows. □

Chapter 3

Applications to Class Field Theory

This chapter focuses on applying techniques developed in the previous sections to prove some major results in local class field theory. Our main goal is to establish a canonical isomorphism between the Brauer group of a local field K and $\mathbb{Q}/\mathbb{Z}$ *via* a special map known as the *Hasse invariant map.* We start by verifying some crucial results that lead us to the verification of the above claim. The material is based on Gille & Szamuely [1], Serre [3], and Nëukirch [4] with some results taken from Sharifi [8].

3.1 Cohomological Dimension

In this section, we discuss the relevant cohomological background. Note that for an abelian group B and a prime number p, the notation $B\{p\}$ denotes the p-primary torsion subgroup of B, i.e., the subgroup of elements of p-power order.

Definition 3.1.1. Let G be a profinite group, p a prime number. We say that G has *p-cohomological dimension* $\leq n$ if $H^i(G, A)\{p\} = 0$ for all $i > n$ and all continuous torsion G-modules A. We define the *p-cohomological dimension* $\mathrm{cd}_p(G)$ to be the smallest positive integer n for which G has cohomological dimension $\leq n$ if such an

n exists and set $\mathrm{cd}_p(G) = \infty$ otherwise.

Proposition 17. *Assume that* $\mathrm{cd}_p(G) \leq n$. *Then,* $H^i(G, A)\{p\} = 0$ *for all* $i > n + 1$ *and all continuous* G*-modules* A.

Proof. Let A be a continuous G-module and consider the multiplication-by-p map $p\colon A \to A$. Observe that its kernel ${}_pA$ and cokernel A/pA are torsion G-modules that fit into the exact sequence

$$0 \to {}_pA \to A \xrightarrow{p} A \to A/pA \to 0$$

which may be split into two short exact sequences

$$0 \to {}_pA \to A \xrightarrow{p} C \to 0 \text{ and } 0 \to C \to A \to A/pA \to 0$$

where $C \coloneqq \mathrm{Im}(p)$. Note that, by assumption, the groups $H^i(G, {}_pA)$ and $H^i(G, A/pA)$ vanish for $i > n$, so the associated long exact sequences induce isomorphisms

$$H^i(G, A) \cong H^i(G, C) \text{ and } H^{i+1}(G, C) \cong H^{i+1}(G, A)$$

for $i > n$. Thus for $i > n + 1$ the induced map $p_*\colon H^i(G, A) \to H^{i+1}(G, A)$ is an isomorphism. But by the construction of cohomology, the map p_* is also given by multiplication by p, so if it is an isomorphism, then the group $H^i(G, A)$ cannot have p-primary torsion. Thus the result follows.

□

Let us recall some relevant results from group cohomology.

Lemma 13 (**Shapiro's Lemma**). *Given a subgroup* H *of* G *and an* H*-module* A, *there are canonical isomorphisms*

$$H^i(G, M_H^G(A)) \cong H^i(H, A)$$

for all $i \geq 0$ where $M_H^G(A) \coloneqq \mathrm{Hom}_H(\mathbb{Z}[G], A)$ is the G-module with the action of G on a H-homomorphism $\phi\colon \mathbb{Z}[G] \to A$ is given by $(\sigma\phi)(g) \coloneqq \phi(g\sigma)$ for a basis element $g \in G$.

Proof. See Gille & Szamuely [1], *Corollary 3.3.2.* □

Lemma 14. *The group $H^i(G, M^G(A))$ is zero for all $i > 0$.*

Proof. In this situation, the right hand side in **Shapiro's Lemma** is zero (for instance, $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$ gives a projective resolution of $\mathbb{Z}$). □

Now we state the following fundamental exact sequence involving inflation and restriction maps for cohomology groups.

Proposition 18. *Let G be a group, H a normal subgroup, and A a G-module. Let $i > j$ be an integer and assume that the groups $H^j(H, A)$ are trivial for $1 \leq j \leq i-1$. Then there is a natural map*

$$\tau_{i,A}\colon H^i(H, A)^{G/H} \to H^{i+1}(G/H, A^H)$$

fitting into an exact sequence

$$0 \to H^i(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^i(G, A) \xrightarrow{\mathrm{Res}} H^i(H, A)^{G/H} \xrightarrow{\tau_{i,A}} H^{i+1}(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^{i+1}(G, A).$$

Proof. See Gille & Szamuely [1], *Proposition 3.3.19.* □

Note: Observe that the above result also holds true if G is a profinite group and H is a normal closed subgroup. (See Gille & Szamuely [1], *Corollary 4.3.5*).

Now we prove a general lemma about cohomological dimension.

Lemma 15. *Let G and p be as above and let H be a closed subgroup of G. Then, $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$. Here equality holds in the case when the image of H in all finite* *quotients of G has index prime to p. In particular,* $\mathrm{cd}_p(G) = \mathrm{cd}_p(G_p)$ *for a pro-p-Sylow group G_p of G.*

Proof. Let B be a continuous torsion H-module. Then it is easy to see that the continuous G-module $M_H^G(B)$ is also torsion and satisfies $H^i(H, B) = H^i(G, M_H^G(B))$ for all $i \geq 0$ by **Shapiro's Lemma**. Thus we have $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$. The converse inequality in the case when H satisfies the prime-to-p condition of the lemma follows immediately from **Corollary 11.1**. □

Note that in the case of pro-p-groups, there is a very useful criterion to determine the p-cohomological dimension.

Proposition 19. *Let G be a pro-p-group for some prime p. Then* $\mathrm{cd}_p(G) \leq n$ *if and only if* $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.

Proof. See Gille & Szamuely [1], *Proposition 6.1.5.* □

Now we define the cohomological dimension of fields.

Definition 3.1.2. The *p-cohomological dimension* $\mathrm{cd}_p(k)$ of a field k is the p-cohomological dimension of the absolute Galois group $\mathrm{Gal}(k_s|k)$ for some separable closure k_s of k. Its *cohomological dimension* $\mathrm{cd}(k)$ is defined as the supremum of the $\mathrm{cd}_p(k)$ for all primes p.

We now have all the necessary tools to prove the following result.

Theorem 3.1.1. *Let k be a field and p a prime number different from the characteristic of k. Then the following statements are equivalent:*

1. *The p-cohomological dimension of k is ≤ 1.*

2. *For all separable algebraic extensions $K|k$, we have* $\mathrm{Br}(K)\{p\} = 0$.

3. *The norm map $N_{L|K} \colon L^\times \to K^\times$ is surjective for all separable algebraic extensions $K|k$ and all Galois extensions $L|K$ with* $\mathrm{Gal}(L|K) \cong \mathbb{Z}/p\mathbb{Z}$.

Proof. (1) $\Longrightarrow$ (2) Choose a separable closure k_s of k containing K. Then $\mathrm{Gal}(k_s|K)$ identifies with a closed subgroup of $\mathrm{Gal}(k_s|k)$, so by **Lemma 15** , we have $\mathrm{cd}_p(K) \leq \mathrm{cd}_p(k) \leq 1$. In particular, the group $H^2(K, \mu_{p^i})$ is zero for all $i > 0$, But, by **Corollary 2.4.2.2**, this group is the p^i-torsion part of $\mathrm{Br}(K)$.

(2) $\Longrightarrow$ (3) Observe that, by **Corollary 2.4.2.3**, for $L|K$ as in (3), we have $\mathrm{Br}(L|K) \cong K^\times/N_{L|K}(L^\times)$. But $\mathrm{Gal}(L|K) \cong \mathbb{Z}/p\mathbb{Z}$ also implies that $\mathrm{Br}(L|K)$ is annihilated by p, so $\mathrm{Br}(L|K) \subset \mathrm{Br}(K)\{p\} = 0$ and the claim follows.

(3) $\Longrightarrow$ (1) Let G_p be a pro-p-Sylow subgroup of $\mathrm{Gal}(k_s|k)$. Then, by **Lemma 15**, it suffices to show that $\mathrm{cd}_p(G_p) \leq 1$. In particular, by **Proposition 19**, it is enough to show that $H^2(G_p, \mathbb{Z}/p\mathbb{Z}) = 0$. Since the extension $k(\mu_p)|k$ has degree $p-1$, the fixed field k_p of G_p contains the p-th roots of unity, so we have a chain of isomorphisms $H^2(G_p, \mathbb{Z}/p\mathbb{Z}) \cong H^2(k_p, \mu_p) \cong {}_p\mathrm{Br}(k_p)$. Let $K_p|k_p$ be a finite extension contained i k_s and denote P by the Galois group $\mathrm{Gal}(K_p|k_p)$. As $\mathrm{Br}(K_p|k_p)$ injects into $\mathrm{Br}(k_p)$, we are reduced to showing that ${}_p\mathrm{Br}(K_p|k_p) = 0$. Observe that since P is a finite p-group, it is solvable, so we have a finite chain

$$P = P_0 \supset P_1 \supset \cdots \supset P_n = \{1\}$$

of normal subgroups such that $\mathrm{Gal}(K_i|k_p) \cong P/P_i$. We now show that ${}_p\mathrm{Br}(K_i|k) = 0$ by induction on i. The case $i = 0$ is trivial. Assuming the statement for $i-1$, consider the exact sequence

$$0 \to H^2(P/P_{i-1}, K_{i-1}^\times) \to H^2(P/P_i, K_i^\times) \to H^2(P_{i-1}/P_i, K_i^\times)$$

coming from **Proposition 18** with $G = P/P_i, H = P_{i-1}/P_i$ and $A = K_i^\times$, noting that $H^1(P_i/P_{i-1}, K_i^\times) = 0$, by **Hilbert's Theorem 90**. Restricting to the p-torsion subgroups, we have

$$0 \to {}_p\mathrm{Br}(K_{i-1}|k_p) \to {}_p\mathrm{Br}(K_i|k_p) \to {}_p\mathrm{Br}(K_i|K_{i-1}).$$

Observe that the right-hand side group is zero by (3) applied with $K = K_{i-1}$ and $L = K_i$ (and noting **Corollary 2.4.2.3** again) and the left-hand side group is zero by induction, so the middle one is zero as well. Thus the result follows. □

We now aim to establish a complement to the above theorem. To do so, we first verify the following results.

Lemma 16. *For an arbitrary field k, the groups $H^i(k, k_s)$ are zero for all $i > 0$.*

Proof. We prove the triviality of $H^i(G, K)$ for all finite Galois extensions $K|k$ with group G and all $i > 0$. Observe that by the normal basis theorem of Galois theory, there exists an element $x \in K$ such that $\sigma_1(x), \dots, \sigma_n(x)$ form a basis of the k-vector space K, where $1 = \sigma_1, \dots, \sigma_n$ are the elements of G. This means that K is isomorphic to $k \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ as a G-module. But this is a co-induced G-module, so by **Lemma 14**, it follows that its cohomology is trivial. □

Proposition 20. *Let k be a field of characteristic $p > 0$. Denote $\mathcal{P}\colon k \to k$ the endomorphism mapping $x \in k$ to $x^p - x$. Then there exists a canonical isomorphism*

$$k/\mathcal{P}(k) \cong H^1(k, \mathbb{Z}/p\mathbb{Z})$$

induced by mapping $a \in k$ to the cocycle $\sigma \mapsto \sigma(\alpha) - \alpha$, where α is a root of the equation $x^p - x = a$.

Proof. Observe that the endomorphism $\mathcal{P}$ extends to the separable closure k_s of k with the same definition. Its kernel is the prime field $\mathbb{F}_p$, which is isomorphic to the trivial $\mathrm{Gal}(k_s|k)$-module $\mathbb{Z}/p\mathbb{Z}$ as a $\mathrm{Gal}(k_s|k)$-module. Moreover the map $\mathcal{P}\colon k_s \to k_s$

is surjective since for each $a \in k_s$, the polynomial $x^p - x - a$ is separable. Thus we have an exact sequence of $\mathrm{Gal}(k_s|k)$-modules

$$0 \to \mathbb{Z}/p\mathbb{Z} \to k_s \xrightarrow{\mathcal{P}} k_s \to 0.$$

A part of the associated long exact sequence reads

$$H^0(k, k_s) \to H^0(k, k_s) \to H^1(k, \mathbb{Z}/p\mathbb{Z}) \to H^1(k, k_s)$$

where the last group is trivial, by **Lemma 16**. Noting that $H^0(k, k_s) = k$, by construction of cohomology, we get the required isomorphism. □

We now prove the complement to **Theorem 3.3.1**

Proposition 21. *Let k be a field of characteristic $p > 0$. Then* $\mathrm{cd}_p(k) \leq 1$.

Proof. By **Lemma 15**, we may replace k by the fixed field of some pro-p-Sylow group of $\mathrm{Gal}(k_s|k)$, so we may assume that k is a field of characteristic p whose absolute Galois group is a pro-p-group. Then, by **Proposition 19**, it is enough to establish the vanishing of $H^2(k, \mathbb{Z}/p\mathbb{Z})$. In order to do so, we use the exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to k_s \xrightarrow{\mathcal{P}} k_s \to 0$$

as in the proof of **Proposition 20**, where $\mathcal{P}\colon k_s \to k_s$ is given by $\mathcal{P}(x) = x^p - x$. Then part of the associated sequence reads

$$H^1(k, k_s) \to H^2(k, \mathbb{Z}/p\mathbb{Z}) \to H^2(k, k_s).$$

Observe that, by **Lemma 16**, the two extremal terms are zero, so we get the required vanishing. □

3.2 Brauer Group of a Local Field

The main goal of this section is to compute the Brauer group of a local field. We will start our discussion by recalling some basic facts from algebraic number theory.

Let K be a field complete with respect to a discrete valuation ν with residue field κ. Fix a separable closure K_s of K and let K_{nr} be the maximal unramified field extension of K. The valuation ν extends uniquely to a discrete valuation of K_{nr} with residue field κ_s, a separable closure of κ. The extension $K_{nr}|K$ is Galois and the Galois group $G \coloneqq \mathrm{Gal}(K_{nr}|K)$ is canonically isomorphic to $\mathrm{Gal}(\kappa_s|\kappa)$.

Let U_{nr} denote the multiplicative group of units in K_{nr}, so we get an exact sequence of G-modules

$$1 \to U_{nr} \to K_{nr}^{\times} \xrightarrow{\nu} \mathbb{Z} \to 0 \tag{3.1}$$

which is split by the map $\mathbb{Z} \to K_{nr}^{\times}$ sending 1 to a local parameter π of ν, which belongs to K and hence G fixed. Thus for each $i \geq 0$, we have a split exact sequence of cohomology groups

$$0 \to H^i(G, U_{nr}) \to H^i(G, K_{nr}^{\times}) \to H^i(G, \mathbb{Z}) \to 0.$$

Observe that for $i = 0$, this is just the analogue of (3.1) for K instead of K_{nr} and for $i = 1$, there is nothing interesting going on because of **Hilbert's Theorem 90**. For $i \geq 2$, we can use the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0 \tag{3.2}$$

to obtain isomorphisms $H^i(G, \mathbb{Z}) \cong H^{i-1}(G, \mathbb{Q}/\mathbb{Z})$ as $H^i(G, \mathbb{Q}) = 0$ for $i > 0$, by **Corollary 10.1**. Thus we can rewrite the exact sequence as

$$0 \to H^i(G, U_{nr}) \to H^i(G, K_{nr}^{\times}) \xrightarrow{r_{\nu}^{i}} H^{i-1}(G, \mathbb{Q}/\mathbb{Z}) \to 0.$$

The map r^i_ν is called the *residue map* associated to ν.

We now state a lemma that leads us to the proof of a very crucial result.

Lemma 17. *Let Γ be a finite group and (A_j, ϕ_{jk}) an inverse system of Γ-modules indexed by the set $\mathbb{Z}_+$ with surjective transition maps ϕ_{jk}. If $i > 0$ is an integer such that $H^i(\Gamma, A_1) = 0$ and $H^i(\Gamma, \ker(\phi_{jk})) = 0$ for all j, then $H^i(\Gamma, \varprojlim A_j) = 0$.*

Proof. See Gille & Szamuely, *Lemma 6.3.2.* □

Proposition 22. *The natural reduction map $U_{nr} \to \kappa_s^\times$ induces isomorphisms*

$$H^i(G, U_{nr}) \cong H^i(G, \kappa_s^\times)$$

for all $i > 0$. Therefore we have split exact sequences

$$0 \to H^i(G, \kappa^\times) \to H^i(G, K_{nr}^\times) \xrightarrow{r^i_\nu} H^{i-1}(G, \mathbb{Q}/\mathbb{Z}) \to 0$$

for $i \geq 2$.

Proof. Note that in view of the discussions preceding the proposition, we only need to show the first statement. In order to do so, it suffices to consider a finite unramified Galois extension $L|K$ with Galois group Γ and residual extension $\lambda|\kappa$ and establish isomorphisms $H^i(\Gamma, U_L) \cong H^i(\Gamma, \lambda^\times)$, where U_L is the group of units in L. Consider, for all $j > 0$, the multiplicative subgroups

$$U_L^j := \{x \in L : \nu(x-1) \geq j\}$$

in the group of units U_L of L. Observe that the groups U_L^j form a decreasing filtration of U_L^1 such that the natural map $U_L^1 \to \varprojlim U_L^1/U_L^j$ is an isomorphism. In addition, the reduction map $U_L \to \lambda^\times$ gives us the exact sequence

$$1 \to U_L^1 \to U_L \to \lambda^\times \to 1$$

whose associated long exact sequence shows that the proposition follows if we prove that $H^i(\Gamma, U_L^1) = 0$ for all $i > 0$. To do this, fix a local parameter π generating the maximal ideal of the valuation ring $A_\nu \subset L$ of ν and consider the maps $U_L^j \to \lambda$ sending $1 + a\pi^j$ to the image of $a \in A_\nu$ in λ. Note that these maps are surjective group homomorphisms giving rise to exact sequences of Γ-modules

$$1 \to U_L^{j+1} \to U_L^j \to \lambda \to 0$$

for all j. Observe that, by **Lemma 16**, $H^i(\Gamma, \lambda) = 0$ for all $i > 0$, so we have $H^i(\Gamma, U_L^j/U_L^{j+1}) = 0$ for $i, j > 0$. Now by induction on j using the exact sequences

$$1 \to U_L^j/U_L^{j+1} \to U_L^1/U_L^{j+1} \to U_L^1/U_L^j \to 1$$

we see that $H^i(\Gamma, U_L^1/U_L^j) = 0$ for all $i > 0$ and $j > 0$. Then the result follows by applying **Lemma 17** to the inverse system of Γ-modules formed by the quotients U_L^1/U_L^j. □

Now we state some important facts from algebraic number theory which leads us to our main goal.

Proposition 23. *Let K be complete with respect to a discrete valuation ν and $L|K$ a finite extension.*

1. *There is a unique discrete valuation w of L extending ν, L complete with respect to w, and its valuation ring A_w is the integral closure of A_ν in L.*

2. *With the notation $f := [\kappa(w) : \kappa(\nu)]$, we have $w = (1/f)(\nu \circ N_{L|K})$.*

3. *If the extension $\kappa(w)|\kappa(\nu)$ is separable, there is a unique unramified extension $N|K$ contained in L such that $[N : K] = f$.*

Proof. See Nëukirch [4], *Chapter II, Theorem 7.7.* □

Proposition 24. *Let K be a field compete under a discrete valuation, with perfect residue field $\bar{K}$. Let K_{nr} be the maximal unramified extension of K and let $K_{nr} \subset E \subset F$ be two finite extensions of K_{nr} with $F|E$ separable. Then $N_{F|E}(F^{\times}) = E^{\times}$.*

Proof. See Serre [3], *Chapter V.4, Proposition 7.* □

We now show that $\mathrm{Gal}(K_{nr}|K)$ can be identified with $\hat{\mathbb{Z}}$.

Lemma 18. *The set of roots of unity of order prime to p, where p is the characteristic of the residue field of K, in a local field K has order $q-1$, where q is the order of the residue field of K*

Proof. Note that the polynomial $x^p - x$ splits completely over the residue field of κ of K, so *Hensel's Lemma* tells us that $\mu_{q-1}(K)$ has order q and maps isomorphically onto $\kappa(K)^{\times}$. □

Lemma 19. *Let K be a local field. For each positive integer n, there exists a unique unramified extension of K of degree n, equal to $K(\mu_{q^n-1})$, where q is the order of the residue field K.*

Proof. Let L/K be an unramified extension of degree n. Then $\kappa(L)$ is a degree n extension of $\kappa(K)$, by the degree formula. The fact that L contains $K(\mu_{q^n-1})$ follows from **Lemma 18**. In addition, $K(\mu_{q^n-1})$ is by definition of degree n over K, so equals L. □

Proposition 25. *The maximal unramified extension K_{nr} of a local field K is given by adjoining all prime-to-p roots of unity in a separable closure of K. Its Galois group* $\mathrm{Gal}(K_{nr}|K)$ *is isomorphic to $\hat{\mathbb{Z}}$ via the map that takes the Frobenius automorphism to* 1.

Proof. Observe that, by definition, K_{nr} is the union of the finite unramified extensions of K in K_s, which is to say the fields $K_n = K(\mu_{q^n-1})$ as evident from **Lemma 19.**

Since any prime-to-p integer m divides $q^n - 1$ for some n, we see that K_{nr} is given by adjoining all prime-to-p roots of 1. Note that $\mathrm{Gal}(K_n|K) \cong \mathbb{Z}/n\mathbb{Z}$ *via* the map that takes the Frobenius automorphism to 1. Thus the given isomorphism is simply the composite of the canonical maps

$$\mathrm{Gal}(K_{nr}|K) \cong \varprojlim \mathrm{Gal}(K_n|K) \cong \varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}.$$

□

We will now assume κ to be a perfect field to obtain the following result.

Proposition 26. *Assume that κ is perfect. Then the inflation maps*

$$\mathrm{Inf}\colon H^i(G, K_{nr}^\times) \to H^i(K, K_s^\times)$$

are isomorphisms for all $i > 0$.

Proof. Observe that since κ is perfect, by **Proposition 24** and **Theorem 3.1.1**, it follows that the cohomological dimension of K_{nr} is ≤ 1. In addition, the Brauer group of K_{nr} is trivial. This implies, by **Proposition 17**, the vanishing of the groups $H^i(K_{nr}, K_s^\times)$ for $i > 1$. It also holds for $i = 1$ by **Hilbert's Theorem 90**. Thus the condition for the exactness of the inflation-restriction sequence in **Proposition 18** is satisfied, so we have an exact sequence

$$0 \to H^i(G, K_{nr}^\times) \xrightarrow{\mathrm{Inf}} H^i(K, K_s^\times) \xrightarrow{\mathrm{Res}} H^i(K_{nr}, K_s^\times)$$

for all $i > 0$. Observe that the last group vanishes for all $i > 0$, so the result follows. □

Corollary 26.1 (Witt). *For a completely discrete valued field K with perfect residue* *field κ, there is a split exact sequence*

$$0 \to \mathrm{Br}(\kappa) \to \mathrm{Br}(K) \to \mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{Q}/\mathbb{Z}) \to 0$$

where $G = \mathrm{Gal}(\kappa_s|\kappa)$.

Proof. The result follows immediately from **Proposition 22** when $i = 2$ together with the identification with Brauer groups as in **Theorem 2.4.2** and the isomorphism $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{Q}/\mathbb{Z})$. □

We have now developed all the necessary background to verify the main result in this section.

Theorem 3.2.1 (**Hasse**). *For a complete discretely valued field K with finite residue field κ (that is, a local field), we have a canonical isomorphism*

$$\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}.$$

The map inducing the above isomorphism is classically called the *Hasse invariant map* and is denoted by inv_K.

Proof. Observe that, by **Proposition 13**, the Brauer group of a finite field is zero. Then the result is immediate from **Corollary 25.1** together with the isomorphism $\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\kappa_s|\kappa), \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(K_{nr}|K), \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}_{\mathrm{cont}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$. □

Remark 13. We will now give an explicit description of the Hasse invariant map inv_K. Based on the discussion at the very beginning of this section and **Proposition 22**, we have an isomorphism

$$\nu\colon H^i(G, K_{nr}^{\times}) \to H^i(G, \mathbb{Z}).$$

Also, note that in the associated long exact sequence of (3.2), the groups $H^i(G, \mathbb{Q})$ vanish for $i > 0$, so the connecting homomorphism

$$\delta\colon H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$$

is an isomorphism. Since G has a special element σ (*Frobenius element*) which restricts to the Frobenius automorphism in any unramified subextension, We also have an isomorphism

$$\gamma\colon \mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{Q}/\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z}$$

defined by $f \mapsto f(\sigma)$. In addition, again by **Proposition 22**, we also have the isomorphism

$$\alpha\colon \mathrm{Br}(K) \to H^2(G, K_{nr}^{\times}).$$

Then it is easy to see that $\mathrm{inv}_K\colon \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$ is the composition of the maps

$$\mathrm{Br}(K) \xrightarrow{\alpha} H^2(G, K_{nr}^{\times}) \xrightarrow{\nu} H^2(G, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z}.$$

We now prove an interesting result concerning any finite separable extension of a local field K.

Theorem 3.2.2. *Suppose K is a complete discretely valued field with finite residue field κ and let $L|K$ is a finite separable extension such that $[L : K] = n$, Then the diagram*

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\mathrm{inv}_K"] \arrow[d, "\mathrm{Res}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\
\mathrm{Br}(L) \arrow[r, "\mathrm{inv}_L"'] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

commutes. Here the right vertical map is multiplication by the degree $[L : K]$.

Proof. We begin our proof with two special cases.

(a) $L|K$ is unramified

In this case, we have $K_{nr} = L_{nr}$. Let $G_n \coloneqq \mathrm{Gal}(K_{nr}|L) = \mathrm{Gal}(\kappa_s|\lambda)$ where λ is the residue field of L.

Consider the diagram

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\alpha"] \arrow[d, "\mathrm{Res}"'] & H^2(G, K_{nr}^{\times}) \arrow[r, "\nu"] \arrow[d, "\mathrm{Res}"'] & H^2(G, \mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "\mathrm{Res}"'] & H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\gamma"] \arrow[d, "\mathrm{Res}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\
\mathrm{Br}(L) \arrow[r, "\alpha^{'}"'] & H^2(G_n, K_{nr}^{\times}) \arrow[r, "\nu^{'}"'] & H^2(G_n, \mathbb{Z}) \arrow[r, "\delta^{'-1}"'] & H^1(G_n, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\gamma^{'}"'] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

where all the vertical homomorphisms are restrictions except the on the far right, which is multiplication by n. We need to verify the commutativity of this diagram. Note that for the squares involving Res, the commutativity is obvious, so we only need to check the commutativity of the last square

$$\begin{tikzcd}
H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\gamma"] \arrow[d, "\mathrm{Res}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\
H^1(G_n, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\gamma^{'}"'] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Suppose $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$. Then, based on the definition of γ, we have $\gamma(\chi) = \chi(\sigma)$, where σ is the distinguished Frobenius element of G. On the other hand, note that $\mathrm{Res}(\chi)$ is simply the restriction of χ to the subgroup G_n of G and the distinguished Frobenius generator of G_n is σ^n. Thus we have

$$\gamma^{'}(\mathrm{Res}(\chi)) = \chi(\sigma^n) = n \cdot \chi(\sigma) = n \cdot \gamma(\chi)$$

which gives us the desired commutativity.

(b) $L|K$ is totally ramified (i.e., $\kappa = \lambda$)

In this case, the extension $K_{nr}|K$ is linearly disjoint from $L|K$ and $L_{nr} = K_{nr}L$. Also, observe that the Galois group G is the same for L as for K.

Consider the diagram

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\alpha"] \arrow[d, "\mathrm{Res}"'] & H^2(G, K_{nr}^{\times}) \arrow[r, "\nu"] \arrow[d, "\iota"'] & H^2(G, \mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "{[L:K]}"'] & H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\gamma"] \arrow[d, "{[L:K]}"'] & \mathbb{Q}/\mathbb{Z} \arrow[d, "{[L:K]}"] \\
\mathrm{Br}(L) \arrow[r, "\alpha^{'}"'] & H^2(G, L_{nr}^{\times}) \arrow[r, "\nu^{'}"'] & H^2(G, \mathbb{Z}) \arrow[r, "\delta^{'-1}"'] & H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[r, "\gamma^{'}"'] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

where ι is induced by the inclusion of $K_{nr}^{\times}$ into $L_{nr}^{\times}$. Commutativity of the first square is obvious and that of the second one follows from the fact that the valuation w of L_{nr} prolongs the valuation ν of K_{nr} with ramification index $e = n$. The commutativity of the other squares is trivial.

Thus the result follows in either of the special cases. Then, by **Proposition 23**, it must hold true for the general case based on the fact that L is a totally unramified extension of an intermediate field $K^{'}$ that is unramified over K.

□

3.3 Some Concluding Remarks

We will end our discussion by introducing the *Albert-Brauer-Hasse-Noether theorem*, which is about local-global property of central simple algebras over number fields.

Theorem 3.3.1 (**Albert-Brauer-Hasse-Noether**)**.** *Let A be a central simple algebra over a number field K and assume that A splits over a local field K_P for any prime P in K. That is,*

$$A \otimes_K K_P \cong M_d(K_P)$$

for some fixed $d > 0$. Then $A \cong M_d(K)$. In other words, A splits over K.

This theorem can also be stated as follows: *for each prime P of K, we have a homomorphism* $\mathrm{Br}(K) \to \mathrm{Br}(K_P)$ *defined by* $[A] \mapsto [A \otimes_K K_P]$*.* One can show that for any $[A] \in \mathrm{Br}(K)$, its image in $\mathrm{Br}(K_P)$ is zero for all but finitely many P. Thus we have a well-defined map

$$\mathrm{Br}(K) \xrightarrow{\sum} \bigoplus_P \mathrm{Br}(K_P)$$

and the *Albert-Brauer-Hasse-Noether* theorem says that this map is injective. Hasse proved a stronger result

Theorem 3.3.2 (**Hasse**)**.** *We have an exact sequence*

$$1 \to \mathrm{Br}(K) \xrightarrow{\sum} \bigoplus_P \mathrm{Br}(K_P) \xrightarrow{\mathrm{inv}} \mathbb{Q}/\mathbb{Z} \to 0$$

where inv *is called the Hasse invariant map.*

Note that $\mathrm{Br}(K_P) \cong \mathbb{Q}/\mathbb{Z}$ via the invariant map $\mathrm{inv_P}$ (See Gille & Szamuely [1], *Theorem 6.5.1*) so that, $\mathrm{Br}(K_P) = \mathbb{Z}/2\mathbb{Z} \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z} \hookrightarrow \mathbb{Q}/\mathbb{Z}$, if P is a real place, and $\mathrm{Br}(K_P) = 0$, if P is a complex place. Furthermore the map

$$\mathrm{inv}\colon \bigoplus_P \mathrm{Br}(K_P) \to \mathbb{Q}/\mathbb{Z}$$

is simply addition on $\bigoplus \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$. Thus we have a description of the Brauer group $\mathrm{Br}(K)$ in terms of a subgroup of countable direct sum of $\mathbb{Q}/\mathbb{Z}$. For instance, if $K = \mathbb{Q}$, then we have $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$ and $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$. Therefore *Hasse's theorem* gives us

$$1 \to \mathrm{Br}(\mathbb{Q}) \to \frac{1}{2}\mathbb{Z}/\mathbb{Z} \oplus \left(\bigoplus_{p<\infty} \mathbb{Q}/\mathbb{Z} \right) \xrightarrow{\text{inv}} \mathbb{Q}/\mathbb{Z} \to 0$$

Therefore we have

$$\mathrm{Br}(\mathbb{Q}) \cong \left\{ (a, x) : a \in \{0, 1/2\}, x = (x_p)_p \in \bigoplus_{p<\infty} \mathbb{Q}/\mathbb{Z}, a + \sum_{p<\infty} x_p = 0 \right\}.$$

Other number fields can also be described in a similar fashion.

Bibliography

[1] P. Gille and T. Szamuely (2017) *Central Simple Algebras and Galois Cohomology*, Cambridge studies in advanced mathematics, 2nd ed.

[2] Balwant Singh (1960) *Semi-simple Rings*, Tata Institute of Fundamental Research, Bombay.

[3] Jean-Pierre Serre (1979) *Local Fields*, Springer-Verlag, NY, 1979. ISBN 0-387-90424-7.

[4] Jürgen Neukirch. *Algebraic Number Theory.* Grundlehren der Mathematischen Wissenschaften 322. Springer Berlin Heidelberg, 1999. ISBN 3-540-65399-6.

[5] D.S. Dummit and R.M. Foote *Abstract Algebra.* John Wiley & Sons, Inc, Third edition. ISBN 978-0-471-43334-7.

[6] Pierre Guillot (2018) *A Gentle Course In Local Class Field Theory*, Cambridge University Press. ISBN 978-1-108-43224-5.

[7] Igor Rapinchuk *The Brauer Group Of A Field*, Notes on Brauer group of a field.

[8] Romyar Sharifi *Algebraic Number Theory*, Notes on Algebraic Number Theory.