# Group Cohomology in Number Theory: A Brief Exploration of Galois Cohomology

Geoff Vooys

December 18, 2014

## 1 Introduction

When I took my first course in number theory we began with the motto 'number theory is the study of the integers and their inherent properties by any means necessary.' We heard this and promptly began to use some basic algebra and analysis to introduce (and understand) Dirichlet Characters and prove quadratic reciprocity. While this seemed to be a reasonable use of algebraic and analytic tools in order to give some number-theoretic results, nothing felt like we were really justifying the 'by any means necessary' part of our motto. However, we will discuss tools and machinery here that will be used in the study of $\mathbb{Q}$, $\mathbb{F}_q$, $\mathbb{Q}_p$ (and their algebraic extensions) and use some fairly exotic methods which will hopefully add a certain amount of justification to the 'any means necessary' part of the statement. In particular, we shall describe how by looking at the cohomological and topological behavior of the Galois group of an algebraic field extension $L/K$ through group cohomological methods, we may classify exactly how exotic the structure of central simple algebras on $K$ may act, and as such better understand the behavior and nature of $\mathbb{Q}, \mathbb{Q}_p$, and $\mathbb{F}_p$, and consequently of $\mathbb{Z}$. Now let us dive directly in to this exploration of the theory of numbers through group cohomology by beginning with some homological algebra.

## 2 Homological Algebra and Group Modules

Homological algebra is a truly gorgeous branch of mathematics, both in the strength and power of the theorems and results as well as the inherent generality of the techniques that characterize the subject. For instance, through homological algebra it is possible to approach both the subjects of homotopy and homology from a completely algebraic standpoint; here the notion of homology allows us to study exactly how exact a sequence of objects in an Abelian category, is while homotopy allows us to see when two maps of Abelian sequences $\varphi, \psi : A_\bullet \to B_\bullet$ induce the same homomorphism between the homology groups $H_*(A_\bullet) \xrightarrow{\alpha} H_*(B_\bullet)$. This provides us with an interesting contrast between the classiscal topological perspective of both homology and homotopy. The fact that both these perspectives are valid allows us to cast some difficult topological questions in an algebraic light and approach them from a different, and perhaps easier, direction. It is with this idea and insight that brings us to define and use homological-algebraic methods in our study of number theory. It is worth keeping in mind, however, that we will use cohomological methods more than homological methods in this paper (despite homology being the dual of cohomology), as many of the spaces that we shall deal with have more natural cohomological presentations and behavior than homological behavior.

It is now pertinent to introduce some of the notations and technical details of the mathematics we will be using. We assume at least a passing familiarity with the basic homological algebra and category theory (namely so that we may talk about derived functors, Abelian categories, inductive systems, and projective systems freely). Furthermore, it is useful to set the convention that we assume all rings $R$ to be, perhaps perversely, rings of unity, although noncommutative in general. While it may seem unnecessarily restrictive to assume our rings to be unital, and it is certainly possible to talk about the homology groups of $R$-modules when $R$ is a ring without identity, it is much more difficult and some things lose all semblance of kindness.

For instance, the extremely useful and canonical isomorphisms $R \otimes_R A \cong A$ and $B \otimes_R R \cong B$ do not necessarily hold for left $R$-modules $A$ and right $R$-modules $B$ when $R$ is not unital. Furthermore, the notion of what it means for a module $F$ to be a free $R$-module is not at all nicely behaved; in fact, in order for a module $F$ to be free when $R$ is not unital, one must first pass into the category of $\overline{\mathbf{R}} - \mathbf{Mod}$, where $\overline{R}$ is the standard adjunction of $R$ with an identity element, check that the image of $F$ is free in $\overline{\mathbf{R}} - \mathbf{Mod}$, and then pass back to the category $\mathbf{R} - \mathbf{Mod}$ (an exercise detailing this process is given as Exercise IV.2.2 of [Hungerford], albeit in slightly different terminology). With these assumptions in mind, we move now to begin our study of group cohomology by defining what it means for an Abelian group to have a $G$-module structure.

**Definition 2.1** (Burde, p. 21)**.** *Let $G$ be a group and $A$ an Abelian group. We then say that $A$ is a* left $G$-module *if and only if, for all $g, h \in G$ and all $a, b \in A$ the following hold*

1. $g(a + b) = ga + gb$.
2. $(gh)a = g(ha)$.
3. $1_G a = a$, *where $1_G$ is the identity element in $G$.*

Note that we could state an equivalent form of the above definition by stating that there is an $A$-linear group homomophism $\varphi : G \to \mathrm{Aut}_{\mathbf{Grp}}(A)$ such that the actiong of $G$ on $A$ is given by the correspondence $\varphi(g)(m) := gm$. There is one issue with the definition that is somewhat unsettling: how can we justify calling $A$ a $G$-module when $G$ is not even a ring in any obvious or non-trivial way? Well, to a reader familiar with representation theory the process in which we justify such a name should look very natural and familiar, as it begins with considering the group ring.

**Definition 2.2** (Hungerford, p. 117)**.** *Let $R$ be a ring and let $G$ be a group. Then define the set of formal sums*

$$R[G] := \left\{ \sum_{g \in G} r_g g \mid r_g \in R, g \in G \right\}$$

*with the natural linear addition and define multiplication of elements by the pointwise rule*

$$(r_g g)(r_h h) = r_g r_h (gh)$$

*where $g, h \in G$ and $r_g, r_h \in R$. Then $R[G]$ is the* group ring *of $G$ in $R$. Moreover, $R[G]$ is Abelian if and only if $R$ is commutative and $G$ is Abelian, and $R[G]$ is unitary if and only if $R$ is unitary.*

Now, when $\mathbb{Z} = R$ we call $R[G] = \mathbb{Z}[G]$ the integral group ring of $G$. We can then, through the action $G \to A$ and through linearity, give any $G$-module $A$ a $\mathbb{Z}[G]$ action by defining the action, for each $\sum_{g \in G} n_g g \in \mathbb{Z}[G]$ and $a \in A$,

$$\left( \sum_{g \in G} n_g g \right) \circ a = \sum_{g \in G} n_g (ga)$$

where the proximity operation $(ga)$ is given through the $G$-action on $A$. This extension through linearity transforms every $G$-module into a $\mathbb{Z}[G]$-module; similarly, we can make any $\mathbb{Z}[G]$-module into a $G$-module through a restriction given by $(n_g g)a \mapsto 1_{\mathbb{Z}}(ga) = ga$. Thusly we may write the terminology $G$-module without fear of doing anything heinous, as any $G$-module may treated as a $\mathbb{Z}[G]$-module freely (if the terminology $G$-module is still bothersome, think of a $G$-module as a $\mathbb{Z}[G]$-module). Furthermore, the class $\mathscr{G}$ of all left $G$-modules, when equipped with $G$-linear maps, forms a category: the category of (left) $G$-modules, written $\mathbf{G} - \mathbf{Mod}$. The category $\mathbf{Mod} - \mathbf{G}$ denotes the category of right $G$-modules, as is convention, and the category $\mathbf{G} - \mathbf{Mod} - \mathbf{G}$ denotes the category of $G$-bimodules. All these categories are all Abelian categories, and as such we can apply the methods of homological algebra to them.

Before we move forward in more general homological branches, we provide two important facts and definitions about group rings that will prove useful to us later on: the definition of a $G$-norm on $G$-modules $A$ and the definition of the augmentation ideal $I[G]$ of $\mathbb{Z}[G]$.

**Definition 2.3** (Burde, 69)**.** *Let $A$ be a $G$-module and let $G$ be a finite group. Then the map* $\mathrm{Norm}_G : A \to A$ *given by*

$$a \mapsto \sum_{g \in G} ga$$

*is the* $G$-norm *map on* $A$*.*

**Definition 2.4** (Brown, p. 12)**.** *Let $G$ be any group and consider $R = \mathbb{Z}[G]$. Then there is a unique homomorphism of rings*

$$\varepsilon : \mathbb{Z}[G] \to \mathbb{Z}$$

*such that $\varepsilon(g) = 1_{\mathbb{Z}}$ for all $g \in G$. We call $\varepsilon$ the* augmentation map *of $G$. Then we call the ideal* $\ker \varepsilon =: I[G]$ *the* augmentation ideal *of $G$.*

Now that we have the Abelian categories $\mathbf{G-Mod}$ and $\mathbf{Mod-G}$, we must now define the cochain cycles on a $G$-module $A$ so that we have an appropriate setting in which to define group cohomology. After we do this it is then simply a matter of using well known theory of homological algebra to give the cohomology of $G$ and $A$ through the cohains on $G$ and $A$. From here on out we restrict ourselves to left $G$-modules $A$ and remark that the definitions we give are symmetric and may be given verbatim for right $G$-modules $B$ with the word 'left' simply replaces with the word 'right.'

**Definition 2.5** (Burde, 22)**.** *Let $C^n(G, A)$ denote the Abelian group of functions*

$$f : G^n \to A.$$

*We define, for $n = 0$, $C^0(G, A) := \mathrm{Hom}_{\mathbf{G-Mod}}(1_G, A) \cong A$. Then the groups $C^n(G, A)$ are the $n$-cochain groups.*

It then follows from the fact that $A$ is an Abelian group that when we define addition by $(f+g)(x_1, \cdots, x_n) = f(x_1, \cdots, x_n) + g(x_1, \cdots, x_n)$ that $C^n(G, A)$ becomes an Abelian group with the zero function as the identity in $C^n(G, A)$, justifying that $C^n(G, A)$ is actually a group. From here it simply remains to define a chain of maps $\delta_n : C^n(G, A) \to C^{n+1}(G, A)$ so that $\delta_{n+1}\delta_n = 0$ in order that we have a (co)complex $C^\bullet(G, A)$ and can then talk about the cohomology of this complex.

**Definition 2.6** (Burde, p. 23)**.** *Define the map*

$$\delta_n : C^n(G, A) \to C^{n+1}(G, A)$$

*given by, for all $f \in C^n(G, A)$*

$$\begin{aligned}\delta_n(f(x_1, \cdots, x_n)) &= (\delta_n f)(x_1, \cdots, x_{n+1}) \\ &= x_1 f(x_2, \cdots, x_{n+1}) + (-1)^{n+1} f(x_1, \cdots, x_n) + \sum_{i=1}^{n} (-1)^k f(x_1, \cdots, x_{i-1}, x_i x_{i+1}, \cdots, x_{n+1}).\end{aligned}$$

Note that an alternative, and perhaps more elegant, formation of the above definition is given on page 57 of [Brown]. We provide the formultation above because it has a more explicit form which consequently makes proving that $\delta_{n+1}\delta_n = 0$ a little easier. We provide, without proof (the proof is lengthy, and we do not have the space nor time to provide it, but follows from a direct calculation of the composition $\delta_{n+1}\delta_n$), this fact as a lemma in order to show that $C^\bullet(G, A)$ is, in fact, a cochain complex. The proof of the lemma is given on pages 23 and 24 of [Burde], although we give a statement below.

**Lemma 2.1** (Burde, p. 23–24)**.** *For the groups $C^n(G, A)$ with maps $\delta_n : C^n(G, A) \to C^{n+1}(G, A)$ we have that $\delta_{n+1}\delta_n = \delta_{n+1} \circ \delta_n = 0$.*

From this lemma we have the following theorem:

**Theorem 2.1.** *The set* $C^\bullet(G,A) := \{C^n(G,A), \delta_n \mid n \in \mathbb{N}\}$ *is a cochain complex in the Abelian category* $\mathbf{G-Mod}$.

Now that we know $C^\bullet(G,A)$ forms a cochain complex in $\mathbf{G-Mod}$ we may define the cohomology groups of $C^\bullet$ in a natural way. In fact, we can do this in two ways: we can either follow the method, perhaps more classical and illuminating to the categorical nature of $H^*(C^\bullet(G,A))$, given through derived functors that is in [Hilton] or through the method described in [Burde], perhaps more illuminating to the relationship of $H^{ast}$ to $H_*$ as some sort of a measure to how exact the maps in the complex $C^\bullet(G,A)$ are. We give both, but it will often be more convenient to use the description given in [Burde].

**Definition 2.7** (Hilton, p. 189)**.** *Let* $G$ *be a group and* $A$ *a left* $G$*-module. Then we define the* $n$*-th cohomology group of* $G$ *with coefficients in* $A$ *by*

$$H^n(G,A) = \mathrm{Ext}^n_G(\mathbb{Z}, A)$$

*where* $\mathbb{Z}$ *is regarded as a trivial* $G$*-module*

This definition is compatable with the definition we give below, although more general and technically more cumbersome. What is useful about this defintion is that we only need to know of a group $G$ and a $G$-module $A$; however, having to use the functor $\mathrm{Ext}^n_G(-)$ is than quite difficult in general. The use of the definition we give below is that it is much easier to compute and use technically, although it does require that we have a cochain complex $C^\bullet(G,A)$ as above. This is the form we will primarily use in this paper, as it is used by Serre in the ubiquitous *Cohomologie Galoisenne*, and as such has influenced and guided the progress and constructions of Galois cohomology.

**Definition 2.8** (Burde, p. 24)**.** *Let* $C^\bullet(G,A)$ *be a cochain complex as in Theorem 2.1. Then we define the* $n$-th cohomology group *of* $C^\bullet(G,A)$*, denoted* $H^n(C^\bullet(G,A))$*, as*

$$H^n(C^\bullet(G,A)) = \ker \delta_n / \operatorname{im} \delta_{n-1}$$

Another benefit of the above definition is that it passes readily into the use for profinite groups, which we shall describe in the next section. We now provide some preliminary results on the above compleces that are pleasing as group cohomological and homological algebraic results before moving on to define and use the techniques involved in profinite groups to understand better the cohomological structure of fields $K$.

**Theorem 2.2** (Hilton, p. 189)**.** *Let* $H^n(G,A)$ *be the* $n$*-th cohomology group in the sense of Definition 2.7. Then for any short exact sequence of* $G$*-modules* $A_1, A_2$*, and* $A_3$*,*

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow A_3 \longrightarrow 0$$

*there is a long exact sequence of cohomology groups*

$$0 \longrightarrow H^0(G,A_1) \longrightarrow H^0(G,A_2) \longrightarrow H^0(G,A_3) \longrightarrow H^1(G,A_1) \longrightarrow \cdots \longrightarrow H^n(G,A_1) \longrightarrow \cdots$$

The proof of this theorem follows directly from the definition of $H^n(G,A_i)$ as $\mathrm{Ext}^n_G(\mathbb{Z},A_i)$ and some standard results on right derived functors. We now compute $H^0(G,A)$ in order to provide some insight through a toy example into the nature of the calculations that are necessary in the study of group cohomology.

**Proposition 2.1.** *Let* $A$ *be a left* $G$*-module and define*

$$A^G := \{a \in A \mid ga = a \text{ for all } g \in G\}.$$

*Then* $H^0(G,A) = A^G$.

*Proof.* Note that by definition we have that $H^0(G,A) = \mathrm{Hom}_{\mathbf{G-Mod}}(G,A)$. Then we may completely determine a morphism $\varphi : \mathbb{Z} \to A$ with $\varphi \in \mathrm{Hom}_{\mathbf{G-Mod}}(G,A)$ entirely by tracing the image of $1_{\mathbb{Z}}$ with $\varphi(1) = a \in A$. Now, since $\varphi$ is $G$-linear, we have that for all $g \in G$,

$$ga = g\varphi(1) = \varphi(1) = a$$

and so $\varphi$ is $G$-linear if and only if $\varphi(1) = a$ remains fixed under the action of $G$ on $A$. Thusly, with $A^G$ given as above we find that since $\mathbb{Z}$ is a trivial $G$-module it follows that

$$H^0(G,A) = \mathrm{Hom}_{\mathbf{G-Mod}}(G,A) = A^G,$$

as was to be shown. □

We now provide two theorems below that calculate both $H^1(G,A)$ and $H^2(G,A)$. While the proofs of both are quite reasonable, we do not have the time nor space to be able to go into them in the detail that they require (it is infeasible given the scope of this paper to formally define and prove theorems on both derivations and group extensions; see [Hilton], sections VI.5 and VI.10 for proofs and discussions on both topics and see Chapter IV of [Brown] for a discussion on group extensions given in an alternative fashion). These theorems are extremely useful, and shall be reffered to when we introduce cohomological dimension in Section 4. We provide the general results here out of interest and in order to provide contrast between the general case and when we begin to look at a continuous structural constraint on our group and group action, ie when $G$ is a topological group with continuous action on its (left, right) modules.

**Theorem 2.3** (Hilton, p. 195)**.**

$$H^1(G,A) \cong Der(G,A)/Ider(G,A)$$

*where $Der(G,A)$ denotes the group of derivations $d : G \to A$ and $Ider(G,A)$ denotes the group of inner derivations $i : G \to A$; $H^1(G,A)$ is frequently referred to as the group of crossed-homomorphisms from $G$ to $A$.*

**Theorem 2.4** (Hilton, p. 209)**.** *Let $M(G,A)$ be the group of equivalence classes of extensions of $G$ by $A$. Then there is a bijection between the sets $H^2(G,A)$ and $M(G,A)$;*

The above theorems and proposition all show calculations and facts that are typical in group cohomology. It is now pertinent to leave the realm of general group cohomology and move forward to the realm of Galois cohomology, as this will be our most fruitful area of study. In order to proper introduction to Galois cohomolgy, we move forward to the realm of profinite groups, the realm of the Krull topology, and slowly towards understanding how cohomological methods are powerful ways to study fields.

# 3 Profinite Groups

We move now to introduce profinite groups and provide a basic study of some of their properties. Before we give a technical definition, we provide a brief motivation of profinite groups. Strictly speaking, profinite groups are topological groups that are projective limits of a projective system of finite groups, eqch equipped with the discrete topology; this means that they are totally disconnected topological groups that behave in a remarkable way when the topology on $G$ is compact Hausdorff (note that this projective limit intuition also holds when $(A_i, \pi_{ij})$ is a projective system of finite rings equipped with the discrete topology). In particular, we find that there are some classical examples of interesting complete spaces that correspond to profinite groups (rings): for example, consider the projective system $(\mathbb{Z}/p^n\mathbb{Z}, \pi_n)$ where the map $\pi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is the canonical projection of additive groups. Then it follows that

$$\varprojlim \frac{\mathbb{Z}}{p^n\mathbb{Z}} \cong \mathbb{Z}_p$$

where $\mathbb{Z}_p$ denotes the group (ring) of $p$-adic integers. This is a slightly different, more homological, way of constructing the $p$-adics than the more traditional method described in [Zariski] as a completion of the $p$-adic topology on the ring $\mathbb{Z}$ (this is described on page 256 of [Zariski] and requires only basic topological algebra). What is nice about our more homological construction is that it makes it somewhat more immediate that $\mathbb{Z}_p$ is a local ring with unique maximal ideal $p\,\mathbb{Z}_p$ than from some other definitions (cf. Exercise 2.40 of [Farb]). These profinte groups then, as topological groups, contain some topological data about the space on which they act, and by studying them we may learn not only about the nature and structure of the topology and 'shape,' as it were, about the space on which they act, but also about the group and how it is forced to act (note that this is a direct result of the fact that the action of $G$ on a topological space $D$ is continuous and the nature of the topology on $D$ influences how $G$ itself must act). We now give a formal definition of profinite groups, a basic proposition, and some toy examples of profinite groups.

**Definition 3.1** (Serre, p.3)**.** *Let $(G_i, \pi_{ij})$ be a projective system of finite groups, each given the discrete topology. Then let $G$ be a topological group such that*

$$G = \varprojlim G_i.$$

*Then $G$ is a profinite group. Furthermore, $G$ is totally disconnected and compact.*

As an aside, we now introduce some notation that we will use extensively throughout our discussion on groups. Let $\mathscr{G}$ denote the class of all groups. We then define the partial ordering $(\mathscr{G}, \leq)$ by saying that $H \leq G$ if and noly if $H$ is a subgroup of $G$. Furthermore, we define a second partial ordering $(\mathscr{G}, \trianglelefteq)$ by $H \trianglelefteq G$ if and only if $H$ is a normal subgroup of $G$.

**Proposition 3.1** (Serre, p.3)**.** *Let $G$ be a totally disconnected, compact topological group. Then $G$ is profinite.*

*Proof.* Let $G$ be a totally disconnected, compact topological group. Then, since $G$ is locally compact and $G$ is totally disconnected, the open subgroups $H \leq G$ form a basis of open neighborhoods of $1_G$. Then, since $G$ is compact, we have that the index of $H$ in $G$ is finite; write $[G : H] = n \in \mathbb{N}$ for some non-zero $n$. Since $[G : H] = n$, we have that there are finitely many conjugates $gHg^{-1}$. Moreover, we have that the subgroup

$$N_H := \bigcap_{g \in G} gHg^{-1}$$

is an open normal subgroup in $G$. We then have that the collection

$$\mathscr{B} := \{N_H \trianglelefteq G \mid H \leq G\}$$

forms a basis of open neighborhoods of $1_G$. This tells us that the canonical map

$$G \xrightarrow{\varphi} \varprojlim G/N_H$$

is a continuous monomorphism of groups with $\varphi(G)$ dense in $\varprojlim G/N_H$. From here it follows by the compactness of both $G$ and $\varprojlim G/N_H$ that $\varphi$ is, in fact an epimorphism of groups as well. Thus, since $\varphi$ is both epimorphic and monomorphic in **Grp**, we find that $\varphi$ is an isomorphism and hence $G$ is a profinite group. □

**Definition 3.2** (Serre, 3)**.** *Let $G$ be a discrete topological group and let $\hat{G}$ be given as, for all subgroups $N \trianglelefteq G$ with $[G : N] = n \in \mathbb{N}$,*

$$\hat{G} := \varprojlim G/N.$$

*Then the group $\hat{G}$ is the profinite group associated to $G$ and is the separated completion of $G$ for the topology defined by all subgroups of finite index in $G$.*

A well known example of a profinite group associated to a group $G$ provides us with a construction of certain ring very important to algebraic number theory (in particular to class field theory): the ring of adeles. We provide a brief construction of this group, but defer the reader to chapter VII of [Lang] for more details. We construct the ring of adeles by beginning with observing that $\mathbb{Z}$ is a discrete topological group. Then we have that the normal subgroups of $\mathbb{Z}$ of finite index are exactly the ideals $n\,\mathbb{Z}$ for some $n \in \mathbb{Z}$. Then, by the definition above

$$\hat{\mathbb{Z}} = \varprojlim \frac{\mathbb{Z}}{n\,\mathbb{Z}}$$

which, after an application of the Chinese Remainder Theorem gives

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p\,.$$

Then we define the ring of integer adeles, denoted $\mathbb{A}_{\mathbb{Z}}$, as

$$\mathbb{A}_{\mathbb{Z}} := \mathbb{R} \times \hat{\mathbb{Z}} \cong \mathbb{R} \times \left( \prod_{p \text{ prime}} \mathbb{Z}_p \right).$$

Moreover, the ring of rational adeles, denoted $\mathbb{A}_{\mathbb{Q}}$, is defined as

$$\mathbb{A}_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{A}_{\mathbb{Z}}.$$

Note that $\mathbb{A}_{\mathbb{Z}}$ corresponds to a ring in which each algebraic component is a completion of $\mathbb{Z}$ with respect to a valuation; $\mathbb{R}$ corresponds to the Euclidean valuation $|\cdot|$ and each $\mathbb{Z}_p$ corresponds to the completion of $\mathbb{Z}$ with respect to the valuation $||\cdot|_p$. In an analogous fashion, $\mathbb{A}_{\mathbb{Q}}$ corresponds to a ring in which each algebraic component is a completion of $\mathbb{Q}$ with respect to a different valuation. We may also generalize this notion by letting $K$ be an algebraic number field and defining $\mathbb{A}_K := K \otimes_{\mathbb{Z}} \mathbb{A}_{\mathbb{Z}}$ and giving it the topology of $\deg_{\mathbb{Q}}(K)$ copies of $\mathbb{A}_{\mathbb{Q}}$. This ring is obviously important within the study of valuation theory; an introduction to valuations may be found generally in [Zariski] with general valuation theory found in the first section of the book and the topic of completions of $\mathfrak{m}$-adic valuations found at the beginning of the section of local algebra (here $\mathfrak{m}$ denotes an ideal of a commutative ring $R$; the notation is given out of respect to Zariski and Samuel), or within the context of $\mathbb{Q}$ and the valuations on $\mathbb{Q}$ in [Lang].

This example provides us with an instance of where the study of profinite groups is quite useful; it is fundamental in the construction of $\mathbb{A}_{\mathbb{Z}}$ that $\hat{\mathbb{Z}}$ is profinite. While this is an interesting example, it is not representative of the methods in which we will generally persue and study profinite groups, as it is not (co)homological in nature, but more of a strict algebro-topological flavor and lacks truly homological-algebraic methods. We instead move in a more categorical direction by observing that the class $\mathscr{P}$ of all profinite groups creates a category with morphisms continuous homomorphisms of groups; in particular, $\mathscr{P}$ forms the object class of a category both in which infinite products and projective limits exist. We now provide a motivating example that will be useful to us; in fact, it will provide us with a nice characterisation of Galois groups, but will also yield an important fact that we will use later when we tie everything together.

**Proposition 3.2** (Serre, 3)**.** *Let $K$ be a field and let $L/K$ be a Galois extension of $K$. Then* $\mathrm{Gal}(L/K)$ *is profinite.*

*Proof.* Note that for all finite Galois extensions $L_n/K$ with $L_n$ contained in $L$ we have that when $L_k \subseteq L_n$, there are canonical restriction maps $\pi_{nk} : \mathrm{Gal}(L_n/K) \to \mathrm{Gal}(L_k/K)$. Thus we find that $(\mathrm{Gal}(L_n/K), \pi_{nk})$ forms a projective system, and by construction we have that $\mathrm{Gal}(L/K)$ is given by

$$\mathrm{Gal}(L/K) \cong \varprojlim \mathrm{Gal}(L_n/K).$$

Thus $\mathrm{Gal}(L/K)$ is a profinite group. □

We now introduce a topology on Galois groups that is extremely important in the study of Galois cohomology: the Krull topology. It allows us to give a topology on a Galois group $\mathrm{Gal}(L/K)$ in which there is an open basis of 1 given exactly by the normal subgroups of $\mathrm{Gal}(L/K)$. The reason why this works is as follows: by assumption $L/K$ is a Galois extension, implying that $L$ is an algebraic, normal, and separable extension of $K$. Then when $L \supseteq F \supseteq K$ is a finite extension of $K$ we may form a subgroup of $\mathrm{Gal}(L/K)$ that takes the form $\mathrm{Gal}(L/F) \leq \mathrm{Gal}(L/K)$. Then the Galois closure $A$ of $F$ is a finite Galois extension of $K$ and hence we find that $\mathrm{Gal}(L/A) \trianglelefteq \mathrm{Gal}(L/K)$. We will then we get that the set $\mathscr{B} = \{\mathrm{Gal}(L/F) \mid F \text{ is a finite Galois extension of } K\}$ determines an open basis of 1 for $\mathrm{Gal}(L/K)$ under the Krull topology. For each $\varphi \in \mathrm{Gal}(L/K)$ we define an open basis of $\varphi$, denoted $\varphi\mathscr{B}$, to be the set $\varphi\mathscr{B} = \{\varphi N \mid N \in \mathscr{B}\}$. This will then define a topology $\mathfrak{T}$ on $\mathrm{Gal}(L/K)$ induced by $\mathscr{B}$ which is called Krull topology.

**Theorem 3.1** (Burde, p.43)**.** *The collection $\mathscr{B}$ defined above induces a topology $\mathfrak{T}$ on $\mathrm{Gal}(L/K)$ in such a way that $(\mathrm{Gal}(L/K), \mathfrak{T})$ is a topological group.*

*Proof.* We begin by showing that $\mathfrak{T}$ is indeed a topology on $\mathrm{Gal}(L/K)$. First, since $K$ is a finite extension of itself, we find that $\mathrm{Gal}(L/K) \in \mathscr{B}$. Furthermore, because $\varnothing$ is initial in the category **Set** and because $\mathscr{B}$ is an object in **Set**, we find that $\varnothing \in \mathscr{B}$ as well.
Now take $N_i = \mathrm{Gal}(L/F_i)$ for some finite Galois extension $F_i/K$ and some index $i \in I$ for index set $I$. Then we find that for $i, j \in I$

$$N_i \cap N_j = \mathrm{Gal}(L/F_iF_j).$$

Since the composite $F_iF_j$ of two finite Galois extensions is again a finite Galois extension of $K$ we find that $N_i \cap N_j \in \mathscr{B}$. A routine induction then says that $\bigcap_{i=1}^{n} N_i \in \mathscr{B}$ for finite intersections (note that we cannot extend this argument to the infinite case), showing that $\mathscr{B}$ is closed under finite intersections.
Now let $\mathscr{F} = \{N_i\}_{i\in I}$ be a collection with $N_i \in \mathscr{B}$ for every $i \in I$. Then we find that

$$\bigcup_{i\in I} N_i = \mathrm{Gal}\left(L/\left(\bigcap_{i\in I} F_i\right)\right).$$

Because the arbitrary intersection of finite Galois extensions of $K$ is again a finite Galois extention of $K$, it then follows that $\bigcup_{i\in I} N_i \in \mathscr{B}$, showing that $\mathscr{B}$ induces a topology on $\mathrm{Gal}(L/K)$; furthermore, it is clear that $\mathscr{B}$ must form a basis because of the structure of normal subgroups. Thus, when we take $\mathfrak{T}$ to be the topology on $\mathrm{Gal}(L/K)$ with basis $\mathscr{B}$, we find that $\mathfrak{T}$ is indeed a topology.
It now remains to be shown that $\mathrm{Gal}(L/K)$ is, in fact, a topological group. We may see this by showing first that the map $\alpha : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/K)$ given by $x \mapsto x^{-1}$ is continuous with respect to $\mathfrak{T}$. Well, since $\mathrm{Gal}(L/K)$ is a group, $\alpha^{-1}(\mathrm{Gal}(L/K)) = \mathrm{Gal}(L/K)$ and so the preimage of every open $N \in \mathscr{B}$ has that $\alpha^{-1}(N) = N$, yielding that the inverse map on $\mathrm{Gal}(L/K)$ is continuous with respect to $\mathfrak{T}$.
We now show that the group operation is continuous with respect to $\mathfrak{T}$. To see this, let $\varphi, \psi \in \mathrm{Gal}(L/K)$ and consider $\varphi\psi N$, $\varphi N$ and $\psi N$, for some fixed $N \in \mathscr{B}$, as open neighborhoods of $\varphi\psi$, $\varphi$, and $\psi$, respectively. Then we find that

$$(\varphi N)(\psi N) = (\varphi\psi N)(N) = \varphi\psi N,$$

and hence the group operation is continuous and we see that $(\mathrm{Gal}(L/K), \mathfrak{T})$ is a topological group. □

**Proposition 3.3** (Burde, p.43)**.** $\mathrm{Gal}(L/K)$*, under the Krull topology, is Hausdorff topological group.*

*Proof.* We begin by taking $\varphi, \psi \in \mathrm{Gal}(L/K)$ such that $\varphi \neq \psi$. Then choose some $a \in L$ such that $\varphi(a) \neq \psi(a)$; such an $a$ exists because the maps $\varphi$ and $\psi$ are not equivalent. Now let $F$ be the normal closure of $K(a)$, which is clearly a finite Galois extension of $F$. Thus, we set $N := \mathrm{Gal}(L/F) \in \mathscr{B}$.
Now, for the purpose of deriving a contradiction, assume that $\varphi N \cap \psi N \neq \varnothing$. Then, since this intersection is nonempty, we have that $\varphi \in \psi N$. However, this then implies that $\varphi(a) = \psi(a)$ because $a \in F$ and $N$ fixes $F$ elementwise, providing us with a contradiction. Therefore it follows that $\varphi N \cap \psi N = \varnothing$ and so $(\mathrm{Gal}(L/K), \mathfrak{T})$ is Hausdorff. □

We now show that the Krull topology is equivalent to the profinite topology on any Galois group $\mathrm{Gal}(L/K)$. We do this by providing two lemmas without proof: both lemmas are given as a single proposition in [Burde] with the first one is given in its entirety and the second only sketched and the reader deferred to Emil Artin's book *Algebraic Numbers and Algebraic Functions*. We use these two statements as lemmas because, after one accepts them, Proposition 3.1 shows that $(\mathrm{Gal}(L/K), \mathfrak{T})$ is profinite.

**Lemma 3.1** (Burde, p.43)**.** $(\mathrm{Gal}(L/K), \mathfrak{T})$ *is completely disconnected.*

**Lemma 3.2** (Burde, p.43–44)**.** $(\mathrm{Gal}(L/K), \mathfrak{T})$ *is compact.*

**Theorem 3.2.** *The profinite topology on* $\mathrm{Gal}(L/K)$ *corresponds with the topology* $\mathfrak{T}$*.*

*Proof.* Apply the results of the above two lemmas to Proposition 3.1. This completes the proof. □

We have now completed quite a bit of work dealing with both profinite groups and the Krull topology, but we have not dealt with the question as to why we would bother with all this work. There are two main reasons behind these approaches: the first is that the Krull topology allows us to 'fix' where the Fundamental Theorem of Galois Theory fails over infinite field extensions; the second reason is that profinite groups allow us to cast certain problems involving Galois groups as (continuous) group cohomological problems. We are primarily interested in the second reason for dealing with profinite groups and the Krull topology, as this will let us translate certain number theoretic problems more easily into group cohomological problems, which we may then attack with the results and properties developed in Section 2 and some methods that we will develop in Section 4. We will, however, explain now what is meant when we say that the Fundamental Theorem of Galois Theory fails over infinite field extensions. To do this we first recall the Fundamental Theorem.

**Theorem 3.3** (E. Galois; Fundamental Theorem of Galois Theory)**.** *Let* $K \subseteq L \subseteq M$ *be a tower of finite field extensions with* $M/K$ *a Galois extension. Then when* $L/K$ *is algebraic there is a one-to-one correspondence between the sets*

$$E := \{L \mid K \subseteq L \subseteq M\}$$

*and*

$$S := \{H \mid H \leq \mathrm{Gal}(M/K)\}$$

*given by* $H \mapsto M^H$*, where* $M^H$ *is the largest subfield of* $M$ *that is fixed by* $H$*. Furthermore, two intermediate fields* $L_1, L_2$ *satisfy* $L_1 \subseteq L_2$ *if and only if* $\mathrm{Gal}(M/L_2) \subseteq \mathrm{Gal}(M/L_1)$ *and* $\mathrm{Gal}(M/L_1L_2) = \mathrm{Gal}(M/L_1) \cap \mathrm{Gal}(M/L_2)$*. Moreover,* $L$ *is a Galois extension of* $K$ *if and only if* $\mathrm{Gal}(M/L) \trianglelefteq \mathrm{Gal}(M/K)$*; in this case, the isomorphism*

$$\frac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(M/L)} \cong \mathrm{Gal}(L/K)$$

*induced by* $\varphi \mapsto \varphi\big|_L$ *holds in the category* **Grp**.

Note that this provides us with an anti-equivalence between the subextensions of a Galois extension $M/K$ and the subgroups of $\mathrm{Gal}(M/K)$. However, it was known by Dedekind that the Fundamental Theorem fails for infinite Galois extensions $M/K$, which is illustrated in the following example.

**Proposition 3.4** (Burde, 44)**.** *Let* $\mathbb{F}_p$ *be the field with* $p$ *elements (*$p \in \mathbb{Z}$ *an integer prime) and let* $\overline{\mathbb{F}} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}$ *be its algebraic closure. Then, when* $\varphi(x) = x^p$ *denotes the Frobenius automorphism, we find that* $\varphi \in \mathrm{Gal}(\overline{\mathbb{F}}, \mathbb{F}_p)$ *and so* $\langle \varphi \rangle \leq \mathrm{Gal}(\overline{\mathbb{F}}, \mathbb{F}_p)$*, but*

$$\mathbb{F}^G = \mathbb{F}_p = \mathbb{F}^H$$

*while* $H \neq G$*.*

A proof for this proposition is outlined on pages 44-45 of [Burde], and we defer the reader to this proof. We instead describe how to fix this problem in order to translate the Fundamental Theorem of Galois Theory to the setting of infinite field extensions, a problem originally solved by Krull (and so explains the name of the Krull topology). To do this, equip $\mathrm{Gal}(M/K)$ with the Krull topology. This will then lead to an anti-equivalence of intermediate field extensions $M/L/K$ and closed subgroups $H \leq \mathrm{Gal}(M/L)$.

**Theorem 3.4** (Burde, 45)**.** *Let $M/K$ be a Galois extension of fields. Then there is a canonical bijection between the sets*

$$E := \{L \mid K \subseteq L \subseteq M\}$$

*and*

$$S := \{H \mid H \leq \mathrm{Gal}(M/K), H \text{ closed}\}$$

*given by $H \mapsto M^H$, where $M^H$ is the largest subfield of $M$ that is fixed by $H$. Every open subgroup of $\mathrm{Gal}(M/K)$ is closed and open subgroups correspond to finite extensions $M^H/K$. Furthermore, two intermediate fields $L_1, L_2$ satisfy $L_1 \subseteq L_2$ if and only if $\mathrm{Gal}(M/L_2) \subseteq \mathrm{Gal}(M/L_1)$ and $\mathrm{Gal}(M/L_1L_2) = \mathrm{Gal}(M/L_1) \cap \mathrm{Gal}(M/L_2)$. Moreover, $L$ is a Galois extension of $K$ if and only if $\mathrm{Gal}(M/L) \trianglelefteq \mathrm{Gal}(M/K)$; in this case, the isomorphism*

$$\frac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(M/L)} \cong \mathrm{Gal}(L/K)$$

*with the factor group equipped with the quotient topology induced by $\varphi \mapsto \varphi\big|_L$ holds in the category* **TopGrp** *of topological groups and continuous group homomorphisms.*

We now move from aspects of the Krull topology towards more cohomological methods, which require the profinite topology in fundamental ways. Since the Krull topology on Galois groups is equivalent to the profinite topology, the statements we will make about profinite groups all certainly apply to Galois groups, but because not all profinite groups are Galois groups, what we will move on to state is more general than what we strictly require. In spite of this, we will hold Galois groups as our motivating examples and much of what we actually do with profinite groups will be applied to Galois groups of Galois extensions $L/K$ and their cohomological behavior. Sadly, before we may appropriately study the cohomological behavior of $\mathrm{Gal}(L, K)$, we need to talk about two things: cohomological dimension and the Brauer group. We move to first talk about cohomological dimension, as it is a natural extension of both our introduction to profinite groups and of group cohomology.

# 4 Cohomological Dimension

We begin this section by making an observation: since $G$ is profinite, it is a topological group, and as such there will be $G$-modules $A$ on which $G$ acts continuously. This observation raises a natural question: what can we say as to the structure of these modules and how do they differ from general $G$-modules? A key difference in structure may be seen in the following assertion, which will guide our approach in studying Galois groups and Galois cohomology.

**Proposition 4.1** (Serre, p.10)**.** *Let $G$ be a profinite group. Then the class of discrete Abelian groups on which $G$ acts continuously form an Abelian category* $\mathbf{G-DiscMod}$ *(or, as it is denoted in* [Serre] *and* [Burde]*, $C_G$). Furthermore,* $\mathbf{G-DiscMod}$ *is a full subcategory of* $\mathbf{G-Mod}$*.*

We omit the proof of the above proposition. Instead, we will observe that if a $G$-module $A$ is an object in $\mathbf{G-DiscMod}$ we have that the stabilizer of each $a \in A$ is again open in $G$, or, equivalently, that for all open subgroups $H \leq G$, we have that

$$A = \bigcup_{\substack{H \leq G \\ H \text{ open}}} A^H.$$

Such modules $A$ are called *discrete $G$-modules*. We will only be interested in discrete $G$-modules, as it is here that we may use cohomology as a tool to exploit both the topological structure of $G$ and the algebraic

structure of the Abelian category $\mathbf{G-DiscMod}$. With this in mind, from here on out when we write that $A$ is a $G$-module, we imply only that $A$ is in fact a discrete $G$-module. When there is any room for any amount of confusion, we shall make very clear distinction between general $G$-modules and discrete $G$-modules.

The cohomology of discrete $G$-modules looks, at a first glance, formally exactly like the cohomology of general $G$-modules. In fact, whenever $A$ is a discrete $G$-module, we have the same cochain compleces $C^\bullet(G,A)$, save for one important difference: each group $C^n(G,A)$ is the set of all *continuous* maps $f: G^n \to A$ with the coboundary maps $\delta_n : C^n(G,A) \to C^{n+1}(G,A)$ given exactly as in Definition 2.6. When $G$ is finite, the results given in Section 2 carry over explicitly, although with some work it is possible to reduce the general case of an infinite group to the case of finite groups. An example of this is seen in the following theorem.

**Theorem 4.1** (Serre, p.11)**.** *Let $(G_i, \pi_{ij})$ be a projective system of profinite groups and let $(A_i, \varphi_{ij})$ be a directed (inductive) system of discrete $G_i$-modules so that the maps $A_i \xrightarrow{\varphi_{ij}} A_j$ are compatable with the maps $G_i \xrightarrow{\pi_{ij}} G_j$. Let $G = \varprojlim G_i$ and $A = \varinjlim A_i$. Then we have that for all $n \in \mathbb{N}$ (note that we make the natural assumption and take $0 \in \mathbb{N}$)*

$$H^n(G,A) = \varinjlim H^n(G_i, A_i).$$

*Proof.* We begin by considering the canonical map

$$\varinjlim C^\bullet(G_i, A_i) \xrightarrow{\psi_\bullet} C^\bullet(G,A).$$

Now, since $G$ is the projective limit of the $G_i$ and since $A$ is the direct limit of the $A_i$, we find that the only way we have

$$\psi\left(\varinjlim C^n(G_i, A_i)\right) = 0$$

is if $\varinjlim C^n(G_i, A_i) = 0$. Similarly, we find that $\psi$ is surjective at every section, ie the diagram

$$\begin{array}{ccccccc}
\cdots \longrightarrow & \varinjlim C^{n-1}(G_i,A_i) & \xrightarrow{\partial_{n-1}} & \varinjlim C^n(G_i,A_i) & \longrightarrow \cdots \\
& \downarrow{\scriptstyle \psi_{n-1}} & & \downarrow{\scriptstyle \psi_n} & \\
\cdots \longrightarrow & C^{n-1}(G,A) & \xrightarrow{\delta_{n-1}} & C^n(G,A) & \longrightarrow \cdots
\end{array}$$

commutes with $\psi_i$ a surjection for every $i$. Thus, since both sequences $\varinjlim C^\bullet(G_i, A_i)$ and $C^\bullet(G,A)$ are sequences in an Abelian category, we find that $\psi_\bullet$ is, in fact, an isomorphism of compleces. Now, by passing to (co)homology we find that

$$H^n(G,A) = \varinjlim H^n(G_i, A_i),$$

whence the theorem. □

The above theorem allows us to see both that when $A$ is an injective object in $\mathbf{G-DiscMod}$ we have $H^n(G,A) = 0$ for all $n \in \mathbb{N}$ and that even when $A$ is not injective, the functors given by $A \mapsto H^n(G,A)$ are the derived functors of $A \mapsto A^G$, as our discussion in Definition 2.5 would suggest they should be. Now, since the functor $A \mapsto H^n(G,A)$ is given by $\mathrm{Ext}^n_G(\mathbb{Z}, A)$, we may mirror the computation of Proposition 2.1 to derive again that $H^0(G,A) = A^G$. We now provide two theorems that give calculations of $H^1(G,A)$ and $H^2(G,A)$, which, when compared to the results given at the end of Section 2, give results that are analogous; the big difference, however, is that now we insist upon continuity in our extensions and our maps, which makes the groups $H^1(G,A)$ and $H^2(G,A)$ slightly different in flavor.

**Theorem 4.2** (Serre, p.11)**.** *Let $G$ be a profinite group and let $A$ be a discrete $G$-module. Then $H^1(G,A)$ is the group of classes of continuous crossed-homomorphisms $d: G \to A$ and $H^2(G,A)$ is the group of classes of continuous factor systems from $G$ to $A$ (cf. Theorems 2.3 and 2.4).*

We now have the tools at hand to give the main definition for this section: the definition of cohomological dimension. Before we do this, however, we clear up some notation that will be used later. When $G$ is a group and $p \in \mathbb{Z}$ is a prime, we define $G(p)$ to be the $p$-primary component of $G$; ie,
$G(p) := \{g \in G \mid g^{p^n} = 1, n \in \mathbb{N}\}$. We see easily the reason for this notation in the following definition:

**Definition 4.1** (Serre, p.17)**.** *Let $G$ be a profinite group and let $p \in \mathbb{Z}$ be a prime number. Then the $p$-cohomological dimension of $G$, denoted $\mathrm{cd}_p(G)$ , is the lower bound of all integers $n$ such that for every torsion module $A \in \mathrm{Ob}(\mathbf{G-DiscMod})$ and for every $m > n$, we have that $H^m(G, A)(p) = 0$ (if no such integer $n$ exists we write $\mathrm{cd}_p(G) = \infty$).*

**Definition 4.2.** *Let $G$ be a profinite group. Then we define the cohomological dimension of $G$ to be given by, for $p \in \mathbb{Z}$ prime*

$$\mathrm{cd}(G) = \sup_p \mathrm{cd}_p(G).$$

This above definition allows us to characterise how the $p$-primary components of torsion $G$-modules behave cohomologically; in fact, $\mathrm{cd}_p(G)$ tells us exactly which parts of the long exact sequence $H^\bullet(G, A)(p)$, if any, are non-trivial. We now give a theorem that allows us some different, perhaps more preferable, perspectives on cohomological dimension.

**Theorem 4.3** (Serre, 17)**.** *Let $G$ be a profinite group and $n, p \in \mathbb{Z}$ with $p$ a prime. Then the following are equivalent:*

1. $\mathrm{cd}_p(G) \leq n$.
2. $H^m(G, A) = 0$ *for all $m > n$ and every discete $G$-module $A$ such that $A$ is a $p$-primary torsion group.*
3. $H^{n+1}(G, A) = 0$ *when $A$ is a simple discrete $G$-module such that $g^{p^k} = 1$ for all $g \in G$ and some $k \in \mathbb{Z}$.*

We do not prove this theorem, although a proof may be found on page 17 of [Serre]. We may use this characterization, however, to provide a powerful description and understanding of Theorem 6.1 and to prove results necessary for the proof of said theorem. Now, however, before we may proceed we must define the Brauer group in order to truly understand and characterize the power of cohomological extensions. What is fascinating about this is that a study of cohomology and cohomological dimension of $\mathrm{Gal}(K_s/K)$ (when $K_s$ is the separable closure of $K$) will tell us, up to a certain equivalence class, about the structure of all central simple $K$-algebras; in fact, cohomology tells us how exotic these structures are allowed to be. As such, we move forward in order to define and best understand these structures and to have a notion as to what the Brauer group is.

# 5 A Brief Digression into Brauer Groups

We now briefly venture outside the explicit borders of group cohomology and profinite groups to give a reasonable explanation and definition of Brauer groups. It is important for us to do this not only because the theorem to which we build contains a statement about Brauer groups, but also because Brauer groups are a powerful tool for investigating structural properties of fields and the cohomology of $\mathrm{Gal}(K_s, K)$. In fact, it is possible (once one has the Skolem-Noether theorem) to give a short proof of Wedderburn's Little Theorem (all finite division rings are fields). With these remarks in mind, it should be hardly surprising to say many things about Brauer groups from many different perspectives; we will introduce it from the perspective of noncommutative algebra. As such, we begin by making taking two reasonable constraints: firstly, we assume that all algebras $R$ are defined over fields $K$; secondly, we assume that all algebras $R$ are unitary (we unfortunately do not have time to consider the subtlties and beauty of non-unitary rings); thirdly, all algebras are assumed to be associative. Now, having set these conditions, it is pertinent to give some key definitions.

**Definition 5.1** (Page 86 of [Farb]). *Let $R$ be a $K$-algebra. Then we say that $R$ is* central *if $Z(R) = K$, where $Z(R)$ denotes the center of $R$. Furthermore, if $R$ is central and $R$ is simple as a ring, then $R$ we say that $R$ is a* central simple *$K$-algebra.*

This is useful structural constraint on $K$-algebras, as it allows us to look at the 'nicest' algebraic extensions of $K$ without insisting upon any potentially restrictive conditions such as commutativity. It is now natural to ask what the central simple algebras $R$ of finite dimension (ie, $R$ is finite dimensional as a $K$ vector space) look like, for these will be the easiest central simple algebras to understand. It turns out that this question is answered by the well known Wedderburn Structure Theorem for Simple Rings (which is closely related to the Artin-Wedderburn Theorem), which holds for any Artinian simple ring of unity $R$:

**Theorem 5.1** (Wedderburn Structure Theorem for Simple Rings; Page 44 of [Farb]). *The following are equivalent for a ring of unity $R$:*

1. *$R$ is a simple Artinian ring.*
2. *$R$ is isomorphic to a matrix ring over a division ring.*
3. *$R$ is semisimple and all simple $R$-modules are isomorphic.*
4. *$R$ is homogeneous and semisimple as an $R$-module.*
5. *$R$ is Artinian and has a faithful simple module $A$.*

The proof of this theorem is classical in ring theory, but omitted due to space. Because we are not interested primarily in the structure of noncommutative rings, it is not worht the time and space it takes to write the proof. We instead defer the reader to chapter I of [Farb] for a proof.

We now need only one more technical fact in order to give a definition of the Brauer group. This fact is both an interesting structural property of central simple algebras and the technical reason behind why the Brauer group is, in fact, closed under its operation. We do not prove the theorem here, but instead refer the reader to [Farb] for a proof, given on pages 87-88.

**Theorem 5.2** (Page 86 of [Farb]). *Let $K$ be a field, $R$ an arbitrary $K$-algebra, and $S$ a central simple $K$-algebra. Then we have that every two-sided ideal of $R \otimes S$ has the form $I \otimes S$, with $I \trianglelefteq R$ a two-sided ideal of of $R$. In particular, if $R$ is simple then $R \otimes S$ is simple.*

It is a direct corollary of this theorem that if $R$ and $S$ are central simple $K$-algebras, then so is $R \otimes S$. With this theorem and the Artin-Wedderburn Theorem at our hands, all that remains now is to actually define the Brauer group; however, we explain the intuition and idea behind what the Brauer group is doing before we give a technical definition. The main idea is that we may describe how a field $K$ may be algebraically extended by looking at equivalence classes of finite dimensional central simple $K$-algebras $R$. Then, since these algebras are finite dimensional, they are certainly Artinian, and so $R \cong \mathrm{Mat}_n(D)$ for some division ring $D$. We then say that two central simple $K$-algebras $R$ and $S$ are similar and write $R \sim S$ if and only if when $R \cong \mathrm{Mat}_n(D_1)$ and $S \cong \mathrm{Mat}_m(D_2)$ then $D_1 \cong D_2$. This forms an equivalence class on all central simple $K$-algebras. Because these algebras may be extended through the tensor product to form new central simple algebras, it is natural to ask when the tensor product $R \otimes S$ is actually different from $R$ or $S$. It turns out that when we define the tensor product to be our binary operation, the set of all similar central simple $K$-algebras under $\otimes$ forms a group. Furthermore, this group tells us about the nature of central simple algebras through its structure; in fact, when $\mathrm{Br}(K) = 0$, the only finite dimensional central simple algebras over $K$ take the form $\mathrm{Mat}_n(K)$ for some positive integer $n$.

**Definition 5.2** (Farb, p.110). *Let $K$ be a field. Then the* Brauer Group*, denoted $\mathrm{Br}(K)$, is the set of equivalence classes of finite dimensional $K$-algebras under the equivalence class $\sim$ with the tensor product $\otimes$ acting as the group operation and the equivalence class $[K]$ acting as the identity element.*

It now remains to show that $\mathrm{Br}(K)$ is actually a group. To do this we introduce two lemmas and one proposition.

**Proposition 5.1.** *Let $S$ be a central simple $K$-algebra and let $S^{op}$ denote the opposite ring (opposite algebra) of $S$. Then $S \otimes_K S^{op} \cong \mathrm{Mat}_n(K)$ where $n = [S : K]$.*

*Proof.* To begin let $s \in S$ be arbitrary and define the maps $L_s, R_s \in \mathrm{End}_{\mathbf{K-Alg}}(S)$ given by

$$L_s(a) = sa$$

and

$$R_s(a) = as$$

for every $a \in S$. Now take $A := \{R_s \in \mathrm{End}_{\mathbf{K-Alg}}(S) \mid s \in S\}$ and $B := \{R_s \in \mathrm{End}_{\mathbf{K-Alg}}(S) \mid s \in S\}$. Then $A \cong S$ and $B \cong S^{op}$. Furthermore, the maps $L_s$ and $R_s$ commute through the associativity law (as surprising as that is), which is seen in the calculation

$$L_s R_s(a) = L_s(as) = s(as) = (sa)s = R_s(sa) = R_s L_s(a).$$

Through this we define a map

$$\varphi : R \otimes_K R^{op} \to \mathrm{End}_{\mathbf{K-Alg}}(S)$$

given by

$$(a \otimes b) \mapsto L_a R_b.$$

Now, since both $S$ (and $S^{op}$) are central simple as $K$-algebras by assumption, which gives us through Theorem 5.2 that $S \otimes_K S^{op}$ is central simple as well, implying that $\varphi$ is injective. Now, because

$$\dim_{\mathbf{K-Alg}}(S \otimes S^{op}) = \dim_{\mathbf{K-Alg}}(S) \dim_{\mathbf{K-Alg}}(S^{op}) = \dim_{\mathbf{K-Alg}}(S)^2 = \dim_{\mathbf{K-Alg}}(\mathrm{End}_{\mathbf{K-Alg}}(S))$$

we find that $\varphi$ is surjective. Since $\varphi$ is a morphism of rings of unity (unital $K$-algebras) it then follows that $\varphi$ is an isomorphism of $K$-algebras exactly because of the identity element in $S$. Now, because it is well known that $\mathrm{End}_{\mathbf{K-Alg}}(S) \cong \mathrm{Mat}_n(K)$, where $n = [S : K]$, we have then that

$$S \otimes_K S^{op} \cong \mathrm{End}_{\mathbf{K-Alg}}(S) \cong \mathrm{Mat}_n(K),$$

and so the proposition is proved. □

**Lemma 5.1.** *Let $R$ be any $K$-algebra $R$. Then the following hold:*

1. $\mathrm{Mat}_n(R) \cong R \otimes_K \mathrm{Mat}_n(K)$.
2. $\mathrm{Mat}_n(K) \otimes \mathrm{Mat}_m(K) \cong \mathrm{Mat}_{mn}(K)$.

*Proof.* Let everything be given as above. Then there is a natural inclusion $\iota_R : R \hookrightarrow \mathrm{Mat}_n(R)$ given by $r \mapsto rI$ (where $I$ is the $n \times n$ identity map) and a natural inclusion $\iota_K : \mathrm{Mat}_n(K) \hookrightarrow \mathrm{Mat}_n(R)$. Then, for each matrix $(a_{ij}) \in \mathrm{Mat}_n(K)$ we have that

$$(rI)(a_{ij}) = r(I(a_{ij})) = r(a_{ij}) = (a_{ij})r = (a_{ij})(rI).$$

Now, because the images of $\iota_R$ and $\iota_K$ commute, we have that there is a map $\varphi$ in the category **Ring** with $\varphi \in \mathrm{Hom}_{\mathbf{Ring}}(R \otimes_K \mathrm{Mat}_n(K), \mathrm{Mat}_n(R))$ given by, for $E_{i,j}$ the elementary matrix with a 1 in the $(i,j)$th position, $1 \otimes E_{i,j} \mapsto E_{i,j}$. Then, since $\varphi$ takes an $R$-basis to an $R$-basis it is clear that $\varphi$ is in fact an isomorphism, proving part (1).
To prove the second part of the lemma, observe that as a $K$-vector space $\dim_{\mathbf{K\text{-}Vect}}(\mathrm{Mat}_n(K)) = n^2$ and $\dim_{\mathbf{K\text{-}Vect}}(\mathrm{Mat}_m(K)) = m^2$. Then, since the tensor product is multiplicative with respect to $K$-dimension, we have that

$$\dim_{\mathbf{K\text{-}Vect}}(\mathrm{Mat}_n(K) \otimes_K \mathrm{Mat}_m(K)) = (nm)^2 = \dim_{\mathbf{K\text{-}Vect}}(\mathrm{Mat}_{nm}(K)).$$

Since the implied map above agrees on $K$-dimension, we have that this implied map sends a basis of $\mathrm{Mat}_n(K) \otimes_K \mathrm{Mat}_m(K)$ surjectively and injectively to a basis of $\mathrm{Mat}_{nm}(K)$, we have that
$\mathrm{Mat}_n(K) \otimes_K \mathrm{Mat}_m(K) \cong \mathrm{Mat}_{nm}(K)$, as was to be shown. □

**Lemma 5.2.** *Let $R_1 \sim S_1$ and $R_2 \sim S_2$ for central simple $K$-algebras $R_1, R_2, S_1$, and $S_2$. Then $[R_1 \otimes R_2] \sim [S_1 \otimes S_2]$.*

*Proof.* Since $R_1 \cong S_1$, $R_1$ and $S_1$ have the same division algebra; call it $D_1$. Similarly, call $D_2$ the division algebra for $R_2$ and $S_2$. Then we may write, for positive integers $m_1, m_2, n_1, n_2$,

$$R_1 \cong \mathrm{Mat}_{m_1}(D_1), S_1 \cong \mathrm{Mat}_{n_1}(D_1), R_2 \cong \mathrm{Mat}_{m_2}(D_2), S_2 \cong \mathrm{Mat}_{n_2}(D_2).$$

Now, we compute through the aid of Lemma 5.1

$$R_1 \otimes R_2 \cong \mathrm{Mat}_{m_1}(D_1) \otimes \mathrm{Mat}_{m_2}(D_2) \cong D_1 \otimes \mathrm{Mat}_{m_1}(K) \otimes D_2 \otimes \mathrm{Mat}_{m_2}(K)$$

which is isomorphic to

$$D_1 \otimes D_2 \otimes \mathrm{Mat}_{m_1 n_1}(K) \cong \mathrm{Mat}_{m_1 n_1}(D_1 \otimes D_2).$$

Similarly we have that $S_1 \otimes S_2 \cong \mathrm{Mat}_{m_2 n_2}(D_1 \otimes D_2)$ and the lemma is proved. □

We now have the tools at hand to prove that $\mathrm{Br}(K)$ is, in fact, a group. As a preliminary for notation, we once again let $R^{op}$ denote the opposite ring (algebra) of $R$, as the class $[R^{op}]$ will turn out to be the inverse of $[R]$ in $\mathrm{Br}(K)$.

**Theorem 5.3** (Frab, p.112)**.** *The set* $\mathrm{Br}(K)$ *under the operation* $\otimes$ *is an Abelian group.*

*Proof.* Let $R$ and $S$ be two finite-dimensional central simple $K$-algebras. Clearly $[K]$ acts as the identity in $\mathrm{Br}(K)$ by construction and because

$$R \otimes_K \mathrm{Mat}_n(K) \cong \mathrm{Mat}_m(D) \otimes_K \mathrm{Mat}_n(K) \cong \mathrm{Mat}_{mn}(D \otimes_K K) \cong \mathrm{Mat}_{mn}(D).$$

Then $R \otimes S$ is finite-dimesional as well and by Theorem 5.2 is also central simple, showing the closure of $\mathrm{Br}(K)$. The associativity of $\mathrm{Br}(K)$ follows from the fact that the tensor product is associative. Now since $R \otimes R^{op} \cong \mathrm{Mat}_n(K)$ for some finite-dimensional central simple algebra $R$, we have that $[R] \otimes [R^{op}] = [K]$ and so $[R^{op}]$ is the inverse of $[R]$ in $\mathrm{Br}(K)$. It then follows that $\mathrm{Br}(K)$ is Abelian because both central simple algebras $R$ and $S$ have two-sided $K$ actions and satisfy the canonical isomorphism $R \otimes_K S \cong S \otimes_K R$. □

As has been previously stated, the Brauer group is a powerful tool that has many applications in number theory. In order to illustrate this, we will provide a short proof of Wedderburn's Little Theorem and a short exact sequence of Abelian groups important in valuation theory. With this in mind, we state the Skolem-Noether Theorem.

**Theorem 5.4** (Skolem-Noether; Page 93 of [Farb])**.** *Let $R$ be a finite-dimensional central simple $K$-algebra. Then if $\varphi, \psi : R \to S$ are $K$-algebra homomorphisms (necessarily injective), then there is an inner autormorphism $f \in \mathrm{Aut}_{\mathbf{K-Alg}}(S)$ such that $f\varphi = \psi$. Equivalently, if $R_1$ and $R_2$ are isomorphic simple subalgebras of $S$, then for any map $\varphi \in \mathrm{Hom}_{\mathbf{K-Alg}}(R_1, R_2)$ there exists an inner automorphism $f$ of $S$ so that $f\big|_{R_1} = \varphi$. In particular, any automorphism of $S$ is inner.*

The proof of this theorem is short, but shall be omitted. While the proof is somewhat classical and while it contains a certain beauty and elegance, it is not particularly relevent to our proof of Wedderburn's Theorem or our discussion of Galois cohomology.

**Theorem 5.5** (Wedderburn's Little Theorem)**.** *Let $D$ be a finite division ring. Then $D$ is a field.*

*Proof.* Let $D$ be a finite division algebra of its maximal subfield $K$. Then by the Skolem-Noether Theorem, the group $U(D)$ of multiplicative units of $D$ is a union of conjugates of $L$. Then, since $U(D)$ is a finite group, we find that $U(D) = \cup_{d \in D} dU(L)d^{-1}$ is impossible unless $D = L$, proving the theorem. □

Now, because this it is important in local class field theory, we shall provide an example of a short exact sequence of Abelian groups involving $\mathrm{Br}(\mathbb{Q})$. As a preliminary define $V$ to be the set of all valuations on $\mathbb{Q}$ (note that this discussion could be improved by introducing the notion of the places $\mathscr{P}$ of a commutative ring $R$, but we do not have time enough to introduce such a topic; we instead refer the reader to the first section of [Zariski] for further details). Then the following diagram is a short exact sequence of Abelian groups

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \bigoplus_{v \in V} \mathrm{Br}(\mathbb{Q}_v) \to \mathbb{Q} \,/\, \mathbb{Z} \to 0$$

with the direct sum appearing above in place of the direct product because each of the injections into the middle term exist upon finite support, ie for any $a \in \mathrm{Br}(\mathbb{Q})$, the inclusion $\mathrm{Br}(\mathbb{Q}) \to \oplus_{v \in V} \mathrm{Br}(\mathbb{Q}_v)$ is trivial for all but finitely many $v$.

The only thing that remains now is to tie the Brauer group to Galois cohomology. It is not immediately obvious, but it turns out that $\mathrm{Br}(K)$ corresponds to an equivalence class of group extensions of $\mathrm{Gal}(K_s, K)$ by $U(K_s)$, and so corresponds to $H^2(\mathrm{Gal}(K_s, K), U(K_s)$. This is seen in the next two definitions and in Theorem 5.7.

**Definition 5.3** (Brown, p.86)**.** *Let $G$ and $N$ be groups. We then say that an* extension *of $G$ by $N$ is a short exact sequence of groups*

$$1 \longrightarrow N \longrightarrow E \longrightarrow G \longrightarrow 1.$$

**Definition 5.4** (Brown, p.86)**.** *Let $G$ and $N$ be groups with extensions $1 \to N \to E \to G$ and $1 \to N \to F \to G \to 1$. We then say that the two extensions of $G$ by $N$ are* equivalent extensions *if and only if there exists a map $\varphi \in \mathrm{Hom}_{\mathbf{Grp}}(E, F)$ such that the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \Big\downarrow{\scriptstyle =} & & \Big\downarrow{\scriptstyle \varphi} & & \Big\downarrow{\scriptstyle =} & & \\ 1 & \longrightarrow & N & \longrightarrow & F & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

*commutes in* **Grp**. *Note that by the Five Lemma (in particular, the Short Five Lemma) the map $\varphi$ is necessarily an isomorphism.*

**Theorem 5.6** (Brown, p.93)**.** *Let $G$ be a group and $A$ a $G$-module with the set $\mathscr{E}(G, A)$ defined to be the set of equivalence classes of extensions of $G$ by $A$ inducing the action of $G$ on $A$. Then there is a bijection of sets*

$$\mathscr{E}(G, A) \cong H^2(G, A).$$

These definitions and the above theorem then give us the basic language in which to understand how $\mathrm{Br}(K)$ is related to equivalence classes on the set of extensions of $\mathrm{Gal}(K_s, K)$ by $U(K_s)$. In particular, this will tie the group $\mathrm{Br}(K)$ to Galois cohomology and allow us to move forward after stating the following theorem. Note that Theorem 5.7 is proved in [Farb], and as such the proof is omitted.

**Theorem 5.7.** *Let $K$ be a field with separable closure $K_s$. Then there is an isomorphism of Abelian groups*

$$\mathrm{Br}(K) \cong H^2(\mathrm{Gal}(K_s, K), U(K_s)).$$

# 6 Galois Cohomology and Tying Everything Together

We now make a triumphant return to the realm of Galois cohomology and begin the last leg of our journey. We have but a few short tasks to complete prior to proving Theorem 6.1: first, we shall define Tate (co)homology groups in order to give a definition of what it means for a $G$-module $A$ to be cohomologically trivial; secondly, we must provide some results that give us criteria for cohmological dimension, which will provide us with some of the technical tools that we require to prove Theorem 6.1.

We now consider and define the Tate cohomology groups on finite groups $G$ and their modules $A$. These groups are named for the mathematician John Tate, a man who played a key role in introducing Galois cohomology into algebraic number theory. The reason that we are interested in the Tate groups is because they allow us to create a long exact sequence of $G$-modules (both on a fixed module $A$ and induced from a short exact sequence $0 \to A \to B \to C \to 0$) that extends infinitely in both directions. In order to do this, recall that through a process dual to the one we took in Section 2, we may transfer many of the theorems and propositions from cohomology to homology; this is primarily done by taking the *left* derived functors of a module in place of the right derived functors; in particular, we take the dual notion, for any $G$-module $A$

$$H_n(G, A) := \mathrm{Tor}_n^G(A)$$

as the definition of the homology group $H_n(G, A)$. This allows us to give a concrete and elegant definition of the Tate cohomology groups.

**Definition 6.1** (Burde, 69; Brown, 134)**.** *Let $G$ be a finite group and let $A$ be a $G$-module. Then let $H_T^k(G, A) = \hat{H}^k(G, A)$ denote the $k$-*th Tate cohomology group *and define $\hat{H}^k(G, A)$ as*

$$\hat{H}^k(G, A) := \begin{cases} H^k(G, A) & k \geq 1 \\ A^G / \mathrm{Norm}_G(A) & k = 0 \\ \ker(\mathrm{Norm}_G(A))/I[G] & k = -1 \\ H_{-(k+1)}(G, A) & k \leq -2 \end{cases}$$

From the definition of the Tate groups, it follows that if $G$ is a finite group and the sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is a short exact sequence of $G$-modules, then there is a long exact sequence extending infinitely in both directions of the form, for all $k \in \mathbb{Z}$,

$$\cdots \longrightarrow \hat{H}^k(G, A) \longrightarrow \hat{H}^k(G, B) \longrightarrow \hat{H}^k(G, C) \xrightarrow{\delta} \hat{H}^{k+1}(G, A) \longrightarrow \hat{H}^{k+1}(G, B) \longrightarrow \hat{H}^{k+1}(G, C) \xrightarrow{\delta} \hat{H}^{k+2}(G, A) \longrightarrow \cdots$$

where the maps $\delta$ are connecting homomorphisms given by the Snake Lemma. Now we observe, as is observed in [Brown] on page 135, that by the structure and construction of the Tate group, we could give it the alternative definition as taken from the long exact sequence (while suppressing arguments)

$$\begin{array}{ccccccccccccc} \cdots & \longrightarrow & \hat{H}^{-3} & \longrightarrow & \hat{H}^{-2} & \longrightarrow & \hat{H}^{-1} & \longrightarrow & \hat{H}^0 & \longrightarrow & \hat{H}^1 & \longrightarrow & \hat{H}^2 & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle =} & & \downarrow & & \downarrow & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle =} & & \\ \cdots & \longrightarrow & H_2 & \longrightarrow & H_1 & \longrightarrow & H_0 & \xrightarrow[\mathrm{Norm}_G]{} & H^0 & \longrightarrow & H^1 & \longrightarrow & H^2 & \longrightarrow & \cdots \end{array}$$

which may be dualized to give a definition of the Tate *homology* groups in a natural way; see sections VI.4 and VI.7 of [Brown] for more details.

The condition in which the sequence $\hat{H}^\bullet(G, A) = 0$ is of particular interest to us. In particular, this says that the cohomology groups and homology groups on $C^\bullet(G, A)$ and $C_\bullet(G, A)$ are trivial for $k \geq 1$ and satisfy $\ker(\mathrm{Norm}_G(A)) = I[G]$ and $\mathrm{Norm}_G(A) = A^G$. The next defintion will capture this and be of particular use to us.

**Definition 6.2** (Mathew, 8)**.** *Let $G$ be a finite group. Then we say that a $G$-module $A$ is cohomologically trivial if $\hat{H}^k(G, A) = 0$ for all integers $k$.*

We now provide some preliminary results that will be used in the proof of Theorem 6.1. These results are important as to the structure of fields, the cohomological dimensions of their Galois groups $\mathrm{Gal}(K_s, K)$ (for separable closure $K_s/K$), and some behaviors of their algebraic extensions.

**Proposition 6.1** (Serre, p.74)**.** *Let $G$ be a profinite group and let $G(p) = G/N$ be the largest quotient of $G$ that such that $G/N$ is the projective limit of $p$-groups. Then, assuming that $\mathrm{cd}_p(N) \leq 1$, we find that the canonical maps*

$$H^n(G(p), \mathbb{Z}/p\mathbb{Z}) \to H^n(G, \mathbb{Z}/p\mathbb{Z})$$

*are isomorphisms. In particularl, $\mathrm{cd}(G(p)) \leq \mathrm{cd}_p(G)$.*

**Proposition 6.2** (Serre, p.75)**.** *Let $K$ be a field of characteristic $p \in \mathbb{Z}$ prime. Then $\mathrm{cd}_p(\mathrm{Gal}(K_s/K)) \leq 1$ and $\mathrm{cd}(\mathrm{Gal}(K_s, K)(p)) \leq 1$.*

*Proof.* Let $f : K \to K$ be the additive function $f(x) = x^p - x$. Then, writing $K_a = (K, +)$ (the additive group of $K$), we have that there is a short exact sequence

$$0 \longrightarrow \tfrac{\mathbb{Z}}{p\mathbb{Z}} \longrightarrow K_a \xrightarrow{f} K_a \longrightarrow 0,$$

which implies the commutative diagram of Abelian groups

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{\mathbb{Z}}{p\mathbb{Z}} & \longrightarrow & K_s & \xrightarrow{\overline{f}} & K_s & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \frac{\mathbb{Z}}{p\mathbb{Z}} & \longrightarrow & K_a & \xrightarrow{f} & K_a & \longrightarrow & 0 \end{array}$$

whence the top row is exact. Passing to cohomology yields the exact sequence

$$H^1(K, K_a) \longrightarrow H^2\left(K, \tfrac{\mathbb{Z}}{p\mathbb{Z}}\right) \longrightarrow H^2(K, K_a).$$

Now, since $\mathrm{Char}(K) = p$ we find that $H^2(\mathrm{Gal}(K_s, K), \mathbb{Z}/p\mathbb{Z}) = 0$. Then, since $\mathrm{Gal}(K_s, K)$ carries a topology, we may apply the triviality of $H^2$ to the closed subgroups of $\mathrm{Gal}(K_s, K)$. Becuase the closed subgroups $H$ of $\mathrm{Gal}(K_s, K)$ are again Galois, we may then apply the triviality of $H^2$ to the Sylow $p$-groups of $H$. Then we find that $\mathrm{cd}(H) \leq 1$ by Proposition I.21 of [Serre] (see page 27), implying that $\mathrm{cd}_p(K) \leq 1$. Now let $\varphi : \mathrm{Gal}(K_s, K) \to \mathrm{Gal}(K_s, K)(p)$ be the canonoical map. Then $\ker\varphi$ is a closed subgroup of $\mathrm{Gal}(K_s, K)$ and the previous argument applies to $\ker\varphi$; as such, we get that $\mathrm{cd}_p(\ker\varphi) \leq 1$. It then follows through the prior proposition that

$$\mathrm{cd}(\mathrm{Gal}(K_s, K)(p)) \leq \mathrm{cd}_p(\mathrm{Gal}(K_s, K)) \leq 1$$

and we are done. □

**Proposition 6.3** (Albert-Hochschild; Serre, p.75)**.** *Let $L$ be a purely inseparable extension of $K$. Then the canonical map $\varphi : \mathrm{Br}(K) \to \mathrm{Br}(L)$ is epimorphic in* **Ab**.

*Proof.* Let $L_s$ be a separable closure of $L$ containing $K_s$. Then, since $L/K$ is purely inseparable, we can identify $\mathrm{Gal}(K_s, K) = \mathrm{Gal}(L_s, L)$. Thusly, it follows that

$$\mathrm{Br}(K) = H^2(\mathrm{Gal}(K_s, K), U(K_s))$$

and

$$\mathrm{Br}(L) = H^2(\mathrm{Gal}(K_s, K), U(L_s)).$$

Then, for each $x \in L_s$ we get that there is an integer $q = p^k$ such that $x^q \in K_s$, showing that the group $U(L_s)/U(K_s)$ is a $p$-primary torsion group. Since, by the above proposition, we have that $\mathrm{cd}_p(\mathrm{Gal}(K_s, K)) \leq 1$ it then follows that $H^2(\mathrm{Gal}(K_s, K), U(L_s)/U(K_s)) = 0$. From here, it follows through the cohomology exact sequence that the map $H^2(\mathrm{Gal}(K_s, K), U(K_s)) \xrightarrow{\varphi} H^2(\mathrm{Gal}(K_s, K), U(L_s))$ is epic. □

**Proposition 6.4** (Serre, p.76)**.** *Let $K$ be a field and let $p \in \mathbb{Z}$ be a fixed prime with char$(K) \neq p$. Moreover, assume that $n \in \mathbb{N}$ with $n \geq 1$. Then the following are equivalent:*

1. $\mathrm{cd}_p(\mathrm{Gal}(K_s, K)) \leq n$.
2. *For any algebraic extension $L/K$, we have $H^{n+1}(L, U(K))(p) = 0$ and the group $H^n(L, U(K))$ is $p$-divisible.*
3. *For any separable, finite, extension with $[L : K] = m$ with $\gcd(m, p) = 1$, we have $H^{n+1}(L, U(K))(p) = 0$ and $H^n(L, U(K))$ is $p$-divisible.*

*Proof.* Let $\mu_p$ be the group of $p$-th roots of unity. Then we have that $\mu_p \subseteq K_s$ and as such the diagram of Abelian groups, written multiplicatively,

$$1 \longrightarrow \mu_p \longrightarrow U(K) \xrightarrow{p} U(K) \longrightarrow 1$$

is short exact with the map $p$ given by multiplication by $p$ in $K$. From here, the cohomology exact sequence shows us that condition (2) implies that $H^{n+1}(L, U(K)) = 0$ fo all $L$; condition (3) may be translated analogously for finite, separable extensions $L$ with $\gcd([L : K], p) = 1$. We now provide a cyclic proof of the proposition.
(1) $\implies$ (2) : Assume that $\mathrm{cd}_p(\mathrm{Gal}(K_s, K)) \leq n$. Since $\mathrm{Gal}(K_s, L) \cong N \trianglelefteq \mathrm{Gal}(K_s, K)$ and $N$ is closed, we find that $\mathrm{cd}_p(\mathrm{Gal}(K_s, L)) \leq n$. Then, by the definition of cohomological dimension, we find that $H^{n+1}(L, \mu_p) = 0$ and the assertion has been shown.
(2) $\implies$ (3) : Trivial.
(3) $\implies$ (1) : Assume that condition (3) holds and let $H$ be a Sylow $p$-subgroup in $\mathrm{Gal}(K_s, K)$ and let $L$ be the extension $L/K$ corresponding to $H$. Then we have the charcterization

$$L = \varinjlim L_i$$

where the $L_i/K$ are all finite, separable with $\gcd([L_i : K], p) = 1$. Then, by condition (3) we have

$$H^{n+1}(L_k, \mu_p) = 0$$

and hence

$$H^{n+1}(L, \mu_p) = 0.$$

Now, since $H$ is a pro-$p$-group, we have that $H$ acts trivially on $\mathbb{Z}/p\mathbb{Z}$ and so we find that again by Proposition I.21 of [Serre], we get that $\mathrm{cd}_p(H) \leq n$ and consequently $\mathrm{cd}_p(\mathrm{Gal}(K_s, K)) \leq n$. □

**Theorem 6.1** (Serre, p.78)**.** *Let $K$ be a field, let $L/K$ be an algebraic extension, and let $K_s$ be the separable closure of $K$. Then the follwing are equivalent:*

1. $\mathrm{cd}(\mathrm{Gal}(K_s, K)) \leq 1$. *If, moreover, char$(K) = p \neq 0$, then* $\mathrm{Br}(L)(p) = 0$ *for every algebraic extension $L/K$.*
2. $\mathrm{Br}(L) = 0$ *for every algebraic extension $L/K$.*
3. *Let $M/L$ be a finite Galois extension with $L$ an algebraic extension of $K$. Then the* $\mathrm{Gal}(M/L)$*-module $U(M)$ is cohomologically trivial.*
4. *Let $M/L$ be a finite Galois extension with $L$ an algebraic extension of $K$. Then the norm*
$$\mathrm{Norm}_{M/L} : U(M) \to U(K)$$
*is an epimorphism of groups.*
5. $\mathrm{cd}(\mathrm{Gal}(K_s, K)) \leq 1$. *If, moreover, char$(K) = p \neq 0$, then* $\mathrm{Br}(L)(p) = 0$ *for every finite, separable algebraic extension $M/K$.*
6. $\mathrm{Br}(L) = 0$ *for every finite, separable algebraic extension $L/K$.*
7. *Let $M/L$ be a finite Galois extension with $L$ a finite separable algebraic extension of $K$. Then the* $\mathrm{Gal}(M/L)$*-module $U(M)$ is cohomologically trivial.*
8. *Let $M/L$ be a finite Galois extension with $L$ a finite separable algebraic extension of $K$. Then the norm*
$$\mathrm{Norm}_{M/L} : U(M) \to U(K)$$
*is an epimorphism of groups.*

Note that we use the term epimorphism of groups in place of surjection of groups. While in the category **Grp** the terms are equivalent (a sketch of the proof of this fact is given in Exercise I.5.5 of [Mac Lane]), we use the term epimorphism to more readily bring our categorical intuition into play, as opposed to the more set-theoretic (and classical) term 'surjective.' With this explaining our use of the term 'surjective,' we now proceed to prove Theorem 6.1.

*Proof.* We begin the proof of the theorem by observing that through Propositions 6.3 and 6.4 we get that (1) $\iff$ (5) and (2) $\iff$ (6). Moreover, (1) $\iff$ (2) follows from Propositions 6.2 and 6.4.
We now show (6) $\iff$ (7) $\iff$ (8). Begin with (7) $\implies$ (6). Since $\mathrm{Br}(L) \cong H^2(\mathrm{Gal}(L_s, L), U(L_s))$, we find that since the $\mathrm{Gal}(M, L)$-module $U(M)$ is cohomologically trivial for all finite separable algebraic extensions $L/K$ with $M/L$ Galois, $\hat{H}^2(\mathrm{Gal}(M, L), U(M)) = H^2(\mathrm{Gal}(M, L), U(M)) = 0$. Thus, we have that
$$\mathrm{Br}(L) = H^2(\mathrm{Gal}(L_s, L), U(L_s)) = \varinjlim H^2(\mathrm{Gal}(M, L), U(M)) = \varinjlim 0 = 0,$$
proving that $\mathrm{Br}(L) = 0$.
We now show that (7) $\implies$ (8). Because $U(M)$ is cohomologically trivial, $\hat{H}^k(\mathrm{Gal}(M, L), U(M)) = 0$ for all integers $k$. Thus we have that
$$\hat{H}^0(\mathrm{Gal}(M, L), U(M)) = \frac{U(M)^{\mathrm{Gal}(M,L)}}{\mathrm{Norm}_{\mathrm{Gal}(M,L)}(U(M))} = 0$$
implying that $U(M)^{\mathrm{Gal}(M,L)} = \mathrm{Norm}_{\mathrm{Gal}(M,L)}$. Now, since for any $\ell \in L$ and $m \in M$ we have that the map
$$\mathrm{Norm}_{M/L} : U(M) \to U(L)$$

is given by

$$m \mapsto \prod_{\sigma \in \mathrm{Gal}(M,L)} \sigma(m),$$

showing us that the map $\mathrm{Norm}_{\mathrm{Gal}(M,L)}(U(M))$ is, in fact the field norm $\mathrm{Norm}_{M/L}$. Moreover, because $U(M)^{\mathrm{Gal}(M,L)} = \mathrm{Norm}_{M/L}(U(M))$ it then follows that the sequence

$$1 \longrightarrow U(M)^{\mathrm{Gal}(M,L)} \longrightarrow U(M) \xrightarrow{\mathrm{N}_{M/L}} U(L) \longrightarrow 1$$

is exact in **Grp**, proving that $\mathrm{Norm}_{M/L}$ is in fact epimorphic.
We defer the reader to part three of Serre's book *Local Fields* for the cases (6) $\implies$ (7) and (8) $\implies$ (7).
Moving onwards, we observe that if $K$ satisfies condition (2) we have that every algebraic extension $L/K$ satisfies (2) and hence also satisfies (6) and (7), implying that $K$ satisfies (3) as well.
Observe now that condition (3) $\implies$ (7) and condition (4) $\implies$ (8) in the same trivial way; as such, if we can show that (2) $\implies$ (3) and (2) $\implies$ (4) we will have completed the proof of the theorem. However, since if $L/K$ algebraic satisfies (2) we have that $L$ satisfies conditions $(5), (6), (7)$, and (8) as well, we find that $K$ also satisfies (3) by taking the inductive limit.
Similarly as above, we see that (4) $\implies$ (8) trivially. Then taking the same argument as above, we have that (2) $\implies$ (4) and so the theorem is proved. □

This theorem proves for us that we may describe the cohomological behavior and structure of a field, and as such describe some of the structure of certain numbers or number fields, by simply describing any of the above criteria. Moreover, we see that there is a relationship between the cohomological dimension of a field $L$ and whether or not the norm map $\mathrm{Norm} : U(M) \to U(L)$ with $M/L$ Galois is epimorphic or not in **Grp**. This allows us to study in a new frame properties of number fields $K$, and from there glean some knowledge about $\mathbb{Q}$, its algebraic extensions, and consequently about $\mathbb{Z}$.

# 7 Conclusion

It should now be apparent that our motto of 'we shall study the integers by any means necessary' really does mean by any means necessary; even if it means appealing to methods of noncommutative algebra, homological algebra, topology, and group cohomology, we shall study the properties of $\mathbb{Z}$. What is interesting about this, however, is that the study of numbers and their properties gives us connections and relationships between areas of mathematics which may not be obvious; in particular, the notion of the Brauer group, being related to the second cohomology group of the $\mathrm{Gal}(K_s, K)$-module $U(K_s)$ is not at all obvious when thinking only of central simple algebras, but is rather illuminating to the structure of fields $K$ and how these fields act under $K_s$-automorphisms, and the structure these automorphisms force upon equivalence classes of central simple algebras over these fields $K$. By studying numbers through these homological-algebraic and topological methods, we gain strong structural insight into the nature of finite fields, number fields, and $p$-adic fields. While we may have taken some truly exotic paths to arrive at the results we have aquired, the strength of these results is well worth the struggle and is certainly characteristic to the mentality to which we approach number theory.

# References


[Brown] Brown, Kenneth S.. *Cohomology of Groups*. 1st Ed. New York NY: Springer-Verlag. 1982. Print. GTM 87.

[Burde] Burde, Dietrich. *Cohomology of groups with applications to number theory: Lecture Notes 2009*. Updated 2009. Web. Accessed October 15, 2014.

[Farb] Farb, Benson, and R. Keith Dennis. *Noncommutative Algebra*. 1st Ed. New York NY: Springer-Verlag. 1993. Print. GTM 144.

[Hilton] Hilton, P.J., and U. Stammbach. *A Course in Homological Algebra*. 2nd Ed. New York NY: Springer-Verlag. 1997. Print. GTM 4.

[Hungerford] Hungerford, Thomas W. *Algebra*. 2nd Ed. New York NY: Springer-Verlag. 1973. Print. GTM 73.

[Lang] Lang, Serge. *Algebraic Number Theory*. 2nd Ed. New York NY: Springer-Verlag. 1994. Print. GT 110.

[Mac Lane] Mac Lane, Saunders. *Categories for the Working Mathematician*. 2nd Ed. New York NY: Springer-Verlag. 1997. Print. GTM 5.

[Mathew] Mathew, Akil. *Group Cohomology*. January 23, 2009. Web. Accessed November 18, 2014.

[Serre] Serre, Jean-Pierre. *Galois Cohomology*. 2nd Ed. Trans. Patrick Ion. New York NY: Springer-Verlag. 2002. Print. SMM.

[Zariski] Zariski, Oscar, Pierre Samuel. *Commutative Algebra*. 2nd Ed. Vol. 2. New York, NY: Springer-Verlag. 1960. Print. GTM 29.