Galois Cohomology and the Brauer Group

Ludvig Modin

Abstract

We introduce basic concepts and results in group cohomology, central simple algebras and Galois cohomology. The Braur group of a field is defined, first in a cohomological way and then as equivalence classes of central simple algebras over the field, equivalently as isomorphism classes of division algebras over the field. An isomorphism between the cohomological and the classical Brauer groups is given. We use these results to prove that every finite division ring is commutative, and that the only division ring central over the real numbers is the Hamiltonian quaternions.

Aknowledgements

I want to thank Wushi Goldring for all the enlightening discussions on my thesis and on mathematics in general which has been very helpful and fun. And also for supporting me in my choice of topic.

Contents

1 Introduction

In this thesis we study one way to apply homological algebra to a problem in the intersection of non-commutative algebra and number theory. Namely the classification of central simple algebras over a given field.

The basic idea of homological algebra, originating from algebraic topology, can be summed up as investigating characteristic properties of some complicated mathematical objects which are invariant under an apropriate notion of equivalence. The idea we try to present in this thesis is to apply, both the formal tools of homological algebra and its philosophy on the study of which structures are definable over a given field. In particular, we study what central simle algebras can be defined over a field or equivalently, as will be shown, which division rings that are central over the field. The classical example of this kind of structure is the Hamiltonian quaternions, the as we shall see unique non-commutative division algebra defined over the real numbers.

After giving basic definitions and results in group cohomology and central simple algebras, we introduce Galois cohomology with a digression on profinite groups. It is in this setting that we define the Brauer group in two seemingly very different ways and then prove that they are equal. The tools this proof hinges on are those of Galois descent and profinite cohomology.

The thesis finnishes with three examples, the Brauer groups of $\mathbb{F}_p$, $\mathbb{R}$ and $\mathbb{Q}_p$. That is of any finite field, the real numbers and of the p-adic numbers, for any prime p.

The main sources used for writing this thesis have been [1], [2] and [3].

2 Group Cohomology

In this section we introduce the basic concepts in group cohomology and prove some results on them. We begin by defining the basic category that we will work from, the category of $G-$modules. Then we define the cohomology and homology of G-modules. We investigate the (co)homological properties of some classes of G-modules, and on ways that the cohomology of G- and H-modules are related when there are maps between them and between G and H.

2.1 G-modules

Definition 2.1.1. *Let G be any group, the operation of which we write multiplicatively, and A an Abelian group, with its operation written additivly. We define a left action of G on A by a group homomorphism $G \to Aut(A)$, that is we map G to the group of automorphisms of A, which is equivalent to having a map $G \times A \to A$ defined by $(g, a) \mapsto g \cdot a$ such that*

1. $1 \cdot a = a$
2. $g \cdot (a + a') = g \cdot a + g \cdot a'$
3. $(gg') \cdot a = g \cdot (g' \cdot a)$.

In this case we say that A is a (left) G-module.

We may in the following from time to time adopt the slight abuse of notation and write ga or $g.a$ in place of $g \cdot a$ for the action of $g \in G$ on $a \in A$.

As each Abelian group is a $\mathbb{Z}$-module, an equivalent viewpoint to the one above is to, given a action defined above, see A as a $\mathbb{Z}G$-module, with the action

$$(\sum_{g \in G} n_g g) \cdot a = \sum_{g \in G} n_g (g \cdot a)$$

where $n_g \in \mathbb{Z}$ and $n_g = 0$ for all but a finite number of $g \in G$. Conversly if A is a $\mathbb{Z}G$-module we get a well defined left action of G on A by considering $g \cdot a$ i.e. all n_s are 0 except for $n_g = 1$.

Let the morphisms in the category of G-modules be the $\mathbb{Z}G$-module homomorphisms, thus the category of G-modules is the categoty of $\mathbb{Z}G$-modules. Hence the category of G-modules is an Abelian category, see [4] or [2].

2.2 Cohomology

Suppose A is a G-module, we denote the set of elements in A invariant under the action of G by A^G, i.e.

$$A^G = \{a \in A : \forall g \in G,\ ga = a\}.$$

Clearly $0 \in A^G$, suppose $a, a' \in A^G$, then $g(a - a') = ga - ga' = a - a'$ i.e. A^G is a subgroup of A. If A, B are G-modules and f a homomorhism from A to B we have

$$f(ga) = gf(a)$$

hence if $a \in A^G$,

$$gf(a) = f(a) \Leftrightarrow f(a) \in B^G$$

that is $(-)^G$ (the notation for taking the invariant elements under G for an arbitrary G-module) preserves arrows between objects and also their direction, which means exactly that it is a covariant functor from the category of G-modules to the category of Abelian groups.

Proposition 2.2.1. *The functor $(-)^G$ is left exact.*

Proof. Suppose we have an exact sequence of G-modules

$$0 \to A \to B \to C$$

apply $(-)^G$ to it and get

$$0 \to A^G \to B^G \to C^G$$

which is exact at A^G since the restirction of an injective map is still injective. If $b \in B^G$ is maped to 0, by the exactness of the original sequence, there is a (unique)$a \in A$ that maps to b. Suppose $a \notin A^G$, then there is a $g \in G$ such that $ga \neq a$. As b is invariant under the action of G on B, if we denote the map in the sequence from A to B by f, $f(a) = b$ but by injectivity, $gf(a) = f(ga) \neq b$, a contradiction. Hence the new sequence is exact at B as well, and we have showed that $(-)^G$ is a left exact functor. □

Proposition 2.2.2. *$A^G \cong Hom_{\mathbb{Z}G}(\mathbb{Z}, A)$ as Abelian groups, where we consider $\mathbb{Z}$ as a $G-$ module with $\mathbb{Z}^G = \mathbb{Z}$.*

Proof. This can be seen from the fact that any $\varphi \in \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ will also be a homomorphism of Abelian groups, and as such it is completely determined by where it maps 1, since 1 generate $\mathbb{Z}$ as a group, as G acts trivialy on $\mathbb{Z}$ we must have that for all $g \in G$, $g\varphi(1) = \varphi(1)$. These facts taken together shows that there is a bijective correspondence between A^G and $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$ and as both are Abelian groups we have that, denoting the morphism sending 1 to a by φ_a, that the map $a \mapsto \varphi_a$ is an isomorphism, as $a + a' \mapsto \varphi_{a+a'} = \varphi_a + \varphi'_a$. From the above we conclude that $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z},)$ and $(-)^G$ can be identified as functors. □

As $(-)^G$ is left exact, we can consider it's right derived functors (see [2]), the cohomology groups of G with coefficients in the $G-$module we chose as input. We denote these $H^q(G, \_)$, where q is any integer greater than or equal to 0. As $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \cong (A)^G$ we can also identify the cohomology groups by

$$H^q(G, A) \cong \mathrm{Ext}^q_{\mathbb{Z}G}(\mathbb{Z}, A)$$

for any $G-$module A, since $\mathrm{Ext}^q_{\mathbb{Z}G}(\mathbb{Z}, \_)$ are the right derived functors of $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, \_)$, see [2] for an extensive discussion on derived functors and their uniqueness.

From these identifications we get a concrete way to compute the group cohomology of the groups we are interested in. As any module is a quotient of a free module, and every free module is projective, there is a projective resolution of

any $\mathbb{Z}G$-module, hence to compute the cohomology of G, all we have to do is to pick a projective resolution of $\mathbb{Z}$ viewed as a $G-$module in the way described above, say

$$\ldots \longrightarrow P_n \longrightarrow P_{n-1} \longrightarrow \ldots \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

and apply $\mathrm{Hom}_{\mathbb{Z}G}(\_, A)$, with A the $G-$module we want coefficients in. Then compute the cohomology of the resulting cochain complex

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(P_0, A) \longrightarrow \ldots \longrightarrow \mathrm{Hom}_{\mathbb{Z}G}(P_n, A) \longrightarrow \ldots$$

i.e. the usual way to compute Ext-groups.

By the long exact sequence in cohomology of chain complexes [2], given an short exact sequence of $G-$modules

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

we get a long exact sequence in cohomology, i.e.

$$\ldots \longrightarrow H^q(G, B) \longrightarrow H^q(G, C) \xrightarrow{\delta} H^{q+1}(G, A) \longrightarrow \ldots$$

where δ is called the connecting homomorphism.

2.2.1 The standard resolution

We introduce here what we will call the standard resolution of the trivial G-module $\mathbb{Z}$. Let P_n for $n \in \mathbb{Z}_{\geq 0}$ denote the free Abelian group on $\prod_{i=0}^{n} G$ and define a left action of G on P_n by for any $s \in G$ and $(g_0, \ldots, g_n)$ in the standard basis for P_n letting

$$s.(g_0, \ldots, g_n) = (sg_0, \ldots, sg_n)$$

and extending linearily to all of P_n.

Now suppose we have a G-module map $f : P_n \to N$ and a surjective G-module map $g : M \to N$, then in particular all the maps are homomorphisms of Abelian groups. Whence there is a $\mathbb{Z}$-homomorphism $h : P_n \to M$ such that $f = g \circ h$, as P_n is a free and hence projective Abelian group. By f being a G-map, for any $s \in G$ and $p \in P_n$ we have $f(s.p) = sf(p)$ and by $f = g \circ h$, $g \circ h(s.p) = s.g \circ h(p)$ and as g also is a G-map, $g(s.h(p)) = s.g \circ h(p) = g \circ h(s.p)$, whence $h(s.p) - s.h(p) \in \ker g$. Hence we can define h so that $h(s.p) = s.h(p)$, i.e. as a G-map and still have $f = g \circ h$. This shows that P_n is projective for all $n \geq 0$.

We define the differential/coboundary map $d : P_n \to P_{n-1}$, $n \geq 1$ by

$$d(g_0, \ldots, g_n) = \sum_{i=0}^{n} (-1)^i (g_0, \ldots, \hat{g_i}, \ldots, g_n)$$

where $\hat{x}$ means that this entry is to be omitted. We define what will be called the augumentation map $\epsilon : P_0 \to \mathbb{Z}$ by $g \mapsto 1$, all of these maps are then extended linearily to the rest of their domain (which is permited as we defined them on

the basis). A somewhat lenghty calculation shows that the resulting complex indeed is an exact sequence, and hence a projective G-module resolution of $\mathbb{Z}$.

We apply $\mathrm{Hom}_{\mathbb{Z}G}(-, A)$ to the standard resolution of $\mathbb{Z}$.

By the definition of P_n, any element of $\mathrm{Hom}_{\mathbb{Z}G}(P_n, A)$ can be identified with a map $f : G^{n+1} \to A$ such that

$$f(s.g_0, \ldots, s.g_n) = s.f(g_0, \ldots, g_n).$$

By the definition of the $G-$action on P_n, we have that one basis for P_n as a G-module is all elements of the form $(1, g_1, g_1g_2, \ldots, g_1g_2 \ldots g_n)$. Hence by linear extension we can interpret $f \in \mathrm{Hom}_{\mathbb{Z}G}(P_n, A)$ as functions of only n arguments in G. Using the coboundary map induced by the differential defined in the standard resolution we get

$$d : \mathrm{Hom}_{\mathbb{Z}G}(P_n, A) \to \mathrm{Hom}_{\mathbb{Z}G}(P_{n+1}, A)$$

defined by

$$df(g_1, \ldots, g_{n+1}) = g_1.f(g_2, \ldots, g_n) + \sum_{i=1}^{n} (-1)^i f(g_0, \ldots, g_ig_{i+1}, \ldots, g_{n+1})$$

$$+(-1)^{n+1} f(g_1, \ldots, g_n).$$

We call $f \in \mathrm{Hom}_{\mathbb{Z}G}(P_n, A)$ a n-cocycle if $df = 0$ and a n-coboundary if there is a $g \in \mathrm{Hom}_{\mathbb{Z}G}(P_{n-1}, A)$ with $dg = f$.

Two special cases of this that we will use a lot is that 1-cocycles are maps $f : G \to A$ such that

$$f(gg') = gf(g') + f(g)$$

and 2-cocycles maps $f : G \times G \to A$ such that

$$g.f(g', g'') - f(gg', g'') + f(g, g'g'') - f(g, g') = 0.$$

2.3 Homology

We will here introduce the basics of group homology.

If A is a G-module, let DA be the submodule generated by $\{s.a - a | s \in G, a \in A\}$. Define $A_G := A/DA$. As $s.(a + DA) = s.a - s.a + a + DA = a + DA$, A_G is invariant under the action of G, and it can be shown that this is the largest quotient of A that is invariant under G (if a is invariant $s.a - a = 0$).

$-_G$ is in fact a additive and right exact functor, whence it comes with a left derived functor $H_n(G, -)$. Consider $\mathbb{Z}$ as a right trivial G-module, and consider the map

$$A \to \mathbb{Z} \otimes_{\mathbb{Z}G} A$$

defined by

$$a \mapsto 1 \otimes a.$$

By the definition of the tensor product, $1 \otimes s.a = 1 \otimes a$ for all $s \in G$, hence D is in the kernel of the map. If $a - b$ (any element of A can be represented like this, for example by setting $b = 0$) is mapped to 0, then $1 \otimes (a - b) = 0$ equivalently $b \in \mathbb{Z}Ga$ whence $a - b \in D$. By the tensor product being taken over $\mathbb{Z}G$, the map is clearly surjective. Hence $H_0(G, A) = A_G = \mathbb{Z} \otimes_{\mathbb{Z}G} A$.

Using the standard resolution again we get that $H_n(G, A) = \mathrm{Tor}_n^{\mathbb{Z}G}$ with the inherited connecting homomorphism from Tor. We identify an element $x \in P_n \otimes A$ with functions $x(g_1, \ldots, g_n)$ with values in A zero except for finitely many $(g_1, \ldots, g_n)$ by $x(g_1, \ldots, g_n) = x(\overline{g}) = \sum_{a \in A} n_{\overline{g} \otimes a} g_1 g_2 \ldots g_n.a$ where $x = \sum_{\overline{g} \otimes a \in P_n \otimes A} n_{\overline{g} \otimes a} \overline{g} \otimes a$. From this identification we get that the boundaries are defined by

$$dx(g_1, \ldots, g_{n-1}) = \sum_{g \in G} g^{-1} x(g, g_1, \ldots, g_{n-1})$$

$$+ \sum_{j=1}^{n-1} (-1)^j \sum_{g \in G} x(g_1, \ldots, g_j g, g^{-1}, g_{j+1}, \ldots, g_{n-1}) + (-1)^n \sum_{g \in G} x(g_1, \ldots, g_{n-1}, g^{-1}).$$

A nice analogy to algebraic topology can be noted here, namely that $H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$, just like the 1-dimensional singular homology of a path connected space is isomorphic to the abelianization of the same space's fundamental group. For an outline of a proof that $H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$, see [1].

2.4 Compatible maps and their cohomology

Suppose $f : H \to G$ is a group homomorphism, A a G-module. We introduce a H-action on A by $s.a = f(s)a$ for $a \in A$ and $s \in H$. We denote the H-module obtained from this action by f^*A. As H acts on A through elements of G, we get that A^G is a subgroup of f^*A^H, i.e. we have an inclusion $H^0(G, A) \hookrightarrow H^0(H, f^*A)$. Hence we can, by the universal property of derived functors (Theorem 2.4.7 [2]), extend this morphism to a morphism from $H^q(G, A) \to H^q(H, f^*A)$ for all $g \geq 0$. In other words we have a morphism of δ-functors $\{H^q(G, -), \delta\} \to \{H^q(H, f^*-), \delta\}$.

Given an additive map $g : A \to B$ where A is a G-module and B an H-module, then we say that f, g are compatible if for all $a \in A$ and $s \in H$, we have

$$g(f(s).a) = s.g(a)$$

i.e. g is a H-homomorphism from f^*A into B. And just as above, we get a map

$$H^q(H, f^*A) \to H^q(H, B)$$

and composing with the morphism above, we get a morphism

$$(f, g)^q : H^q(G, A) \to H^q(H, B),$$

we call this the morphism associated to the pair (f, g). In terms of cochains we get, given $\psi : G^q \to A$

$$(f, g)^q(\psi) = g \circ \psi \circ f^q$$

where f^q denotes the map $(g_i)_i \mapsto (f(g_i))_i)$, from H^q to G^q.

We introduce here a few compatible maps of special importance and consider the morphisms associated to the pairs:

2.4.1 Restriction

Suppose H is a subgroup of G with f the inclusion homomorphism, and A an G-module with i the identity mapping from to A as a H-module. These maps are clearly compatible and we call the associated morphism in cohomology restriction

$$\mathrm{res}^G_H : H^q(G, A) \to H^q(H, A).$$

2.4.2 Inflation

If H is a normal subgroup of G, and A a $G-$module, we get that A^H is a G/H-module (as invariance under choice of coset representative is nessecary and sufficient to define a G/H-action), and we get compatible morphisms $\pi : G \to G/H$ and $i : A^H \to A$, where π is the natural projection and i inclusion. From these we get the morphism associated to the pair

$$\inf : H^q(G/H, A^H) \to H^q(G, A)$$

called inflation.

2.4.3 Inner automorphisms

We give a result about the maps in cohomology that are induced by inner automorphisms on G. This is one of the results that will help us in the chapter on Galois cohomology, specifically when defining the cohomological Brauer group. Suppose $\sigma_t \in \mathrm{Inn}(G)$ is defined by $s \mapsto \sigma_t(s) = tst^{-1}$. Let A be a G-module and $f_t : A \to A$ be definined by $a \mapsto t^{-1}.a$.

Proposition 2.4.1. *σ_t and f_t are compatible and the induced map in cohomology is the identity.*

Proof. $f_t(\sigma_t(s).a) = f_t(tst^{-1}.a) = t^{-1}tst^{-1}.a = st^{-1}.a = s.g_t(a)$, so the maps are compatible.

As $H^0(G, A) = A^G$, the induced map is just $a \mapsto t^{-1}.a = a$ for $q = 0$, that is in the zeroeth level it is the identity.

To prove this for $q \geq 1$, let A^* be a co-induced G-module (i.e. $A^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, X)$ for some Abelian group X) that A embedds into (for example $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$ as we can let $a \mapsto g_a$ where $g_a(1) = a$) and let $B = A^*/A$, also a $G-$module. We get an exact sequence

$$0 \to A \to A^* \to B \to 0$$

as A^* is coinduced, $H^q(G, A^*) = 0$ for all $q \geq 1$, whence, applying $H^q(G, -)$ we get from the long exact sequence in cohomology, for each $q \geq 0$ a commutative

diagram

$$\begin{array}{ccccc} H^q(G,B) & \xrightarrow{\delta} & H^{q+1}(G,A) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \sigma_t} & & \downarrow{\scriptstyle \sigma_t} & & \\ H^q(G,B) & \xrightarrow{\delta} & H^{q+1}(G,A) & \longrightarrow & 0 \end{array} .$$

As σ_t induces the identity for $q = 0$, the case when $q = 1$ follows from the diagram, and similarily for all other $q \geq 0$ by induction, proving our claim. □

2.5 Induced and coinduced modules & Shapiro's Lemma

2.5.1 Induced modules

We say that a G-module A is induced if there is an Abelian group X such that $A \cong \mathbb{Z}G \otimes_{\mathbb{Z}} X$ as G-modules, where $\mathbb{Z}G \otimes_{\mathbb{Z}} X$ has the G-action $s(g \otimes x) = sg \otimes x$, extended linearily. By the definition of tensor products, this is equivalent to

$$A \cong \bigoplus_{s \in G} sX$$

for an Abelian group X, where G acts on the mudule by what could be interpreted as permuting the coordinates.

Lemma 2.5.1. *Given a G-module A, there is a induced G-module A^* and a G-module surjection $\pi : A^* \to A$.*

Proof. Let A_0 be the underlying Abelian group of A, and define $A^* := \mathbb{Z}G \otimes_{\mathbb{Z}} A_0$. Let $\pi(s \otimes a) = s.a$. Given $a \in A$, by definition $\pi(1 \otimes a) = a$, thus proving that the map is surjective and $s.\pi(h \otimes a) = s.(h.a) = sh.a = \pi(sh \otimes a)$, which proves that π is a G-module map. □

We define $\phi : A \to A^*$ by $\phi(a) = 1 \otimes a$, and we clearly have $\pi \otimes \phi = \mathrm{Id}_A$, that is there are always (set theoretic) sections of this projectjion map. In general these sections won't be G-module morphisms.

We say that a G-module A is relatively projective if π maps a direct summand of A^* $G-$isomorphically onto A, that is there is a injective homomorphism $\nu : A \to A^*$ such that $\nu = \pi\big|^{-1}_{\nu(A)}$. By the module isomorphism theorems this is equivalent to $\ker \pi$ being a direct summand of A^*.

Given any two G-modules A and B, we can make $A \otimes B$ into a G-module by introducing the action

$$s.(a \otimes b) = s.a \otimes s.b.$$

In particular this gives an alternative G-module structure on $A^* = \mathbb{Z}G \otimes A_0$.

Lemma 2.5.2. *The two $G-$module structures we have introduced on $\mathbb{Z}G \otimes A$ are isomorphic.*

Proof. Let the module obtained by the action $s(h \otimes a) = sh \otimes a$ be denoted by A^* and the one obtained by $s(h \otimes a) = sh \otimes sa$ be denoted by A'. We define $\varphi : A^* \to A'$ by $s \otimes a \mapsto s \otimes sa$. If $\varphi(s \otimes a) = 0$, then either $s = 0$ or $s.a = 0$. If $s = 0$, $s \otimes a = 0 \otimes a = 0$ and if $s.a = 0$, then $a = s^{-1}s.a = s^{-1}(s.a) = s^{-1}(0) = 0$, and again $s \otimes a = 0$, proving that φ is injective (on basic tensors and hence on all of the product). Given any basic tensor $s \otimes a \in A'$, we have $\varphi(s \otimes s^{-1}a) = s \otimes a$, whence the map is surjective. Finally,to prove that it is a G-map, note that

$$s.\varphi(h \otimes a) = sh \otimes sh.a = \varphi(s(h \otimes a))$$

which proves $A^* \cong A'$. □

We can by this lemma define another surjection $\tau := \pi \circ \varphi^{-1}$, this time from A' to A.

Lemma 2.5.3. *If A is a relatively projective G-module, then there is a $\rho \in \mathrm{End}_{\mathbb{Z}}(A)$ such that*

- *for every $a \in A$, $\rho(s^{-1}.a) = 0$ for all but finitely many $s \in G$.*
- *$\forall a \in A$, $a = \sum_{s \in G} s.\rho(s^{-1}.a)$.*

Proof. Fix the same notation as in the proof of the preceding lemma.

Let A be a relatively projective G-module. Then we have a G-module section ν of τ (proposition 8.4 of chapter X in [5]), that is we have the following commutative diagram in the category of G-modules

$$\begin{array}{ccc} A & \xhookrightarrow{\nu} & A' \\ & \searrow^{\mathrm{Id}_A} & \downarrow \tau \\ & & A \end{array}.$$

G is a $\mathbb{Z}$-module basis for $\mathbb{Z}G$, whence for all $a \in A$

$$\nu(a) = \sum_{s \in G} s \otimes g(s, a)$$

for some $\mathbb{Z}$-module map $g : G \times A \to A$ such that for each $a \in A$, $g(x, a) = 0$ for all but finitely many $x \in G$.

Let $h \in G$, we have

$$\nu(h.a) = \sum_{s \in G} s \otimes g(s, h.a)$$

and

$$h.\nu(a) = \sum_{s \in G} hs \otimes h.g(s, a) = \sum_{s \in G} s \otimes h.g(h^{-1}s, a).$$

We claim no that the condition

$$h.\nu(a) = \nu(h.a)$$

is equivalent to

$$h.g(h^{-1}s, a) = g(s, h.a)$$

for all $s, h \in G$. Indeed, suppose for some $s \in G$ that $s \otimes h.g(h^{-1}s, a) - g(s, h.a) \neq 0$, then the linear independence of G as a subset of $\mathbb{Z}G$ yields that $h.\nu(a) - \nu(h.a) \neq 0$. The other direction is trivial.

It follows that

$$g(s, a) = s.g(1, s^{-1}a)$$

by considering $h = s$ and replacing a with $s^{-1}.a$ in the formula above.

Define $\rho : A \to A$ by $\rho(a) = g(1, a)$, which gives us

$$g(s, a) = s.\rho(s^{-1}.a)$$

As for every $a \in A$, $g(s, a) = 0$ for all but finitely many $s \in G$, the same holds for $\rho(s^{-1}a) = s^{-1}g(s, a)$, proving the first part of the lemma.

As ν is a section of τ, we have for all $a \in A$

$$a = \tau(\nu(a)) = \tau\left(\sum_{s\in G} s \otimes g(s, a)\right) = \sum_{s\in G} g(s, a) = \sum_{s\in G} s.\rho(s^{-1}.a)$$

which proves the last part of the lemma. □

The converse of the above lemma can also be proven, see [5].

2.5.2 Coinduced modules

Dually to induced G-modules, we say that a G-module A is co-induced if $A \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, X)$ for some Abelian group X, where the action is defined by $s.\varphi(h) = \varphi(hs)$.

Proposition 2.5.1. *Every G-module embeds into a coinduced G-module.*

Proof. If we again denote by A_0 the underlying Abelian group of some G-module A, we define $i : A \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A_0)$ by $a \mapsto (s \mapsto s.a)$ and extend linearily. If $i(a) = 0$, then $s.a = 0$ for all $s \in G$ including 1, whence $a = 0$, proving that every G-module embeds in a coinduced G-module. □

A module is defined to be relatively injective if it is a direct factor of a co-induced module.

2.5.3 Shapiro's lemma and some consequences

We now look at coresponding relative notions (relative in a sense that will be obvious). Suppose H is a subgroup of G and A is a H-module. We define

$$\mathrm{Ind}_H^G(A) := \mathbb{Z}G \otimes_{\mathbb{Z}H} A$$

with the G-action $s.(g \otimes a) = sg \otimes a$ and

$$\mathrm{Coind}_H^G(A) = \mathrm{Hom}_H(\mathbb{Z}G, A)$$

with the G-action $s.\varphi(g) = \varphi(gs)$.

Theorem 2.5.1 (Shapiro's Lemma)**.** *If H is a subgroup of G and A is an H-module, then for all $n \geq 0$*

$$H_n(G, \mathrm{Ind}_H^G(A)) \cong H_n(H, A)$$

and

$$H^n(G, \mathrm{Coind}_H^G(A)) \cong H^n(H, A).$$

Proof. We first note that $\mathbb{Z}G$ is a free $\mathbb{Z}H$-module, with any set of coset representatives (of the cosets of H) as a basis. It follows that any projective $\mathbb{Z}G$-module resolution $P \to \mathbb{Z}$ also is a projective $\mathbb{Z}H$-module resolution. We conclude, as any two projective resolutions of a module yields the same (co)homology, that the homology of the complex

$$P \otimes_{\mathbb{Z}G} (\mathbb{Z}G \otimes_{\mathbb{Z}H} A) \cong P \otimes A$$

is isomorphic both to

$$\mathrm{Tor}_n^{\mathbb{Z}G}(\mathbb{Z}, \mathbb{Z}G \otimes_{\mathbb{Z}H} A) \cong H_n(G, \mathrm{Ind}_H^G(A))$$

and

$$\mathrm{Tor}_n^{\mathbb{Z}H}(\mathbb{Z}, A) \cong H_n(H, A)$$

proving the first part of the theorem.

We again assume that $P \to \mathbb{Z}$ is a projective $\mathbb{Z}G$-module resolution of $\mathbb{Z}$, hence also a projective $\mathbb{Z}H$-resolution. Define

$$\Phi : \mathrm{Hom}_{\mathbb{Z}G}(P_n, \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)) \to \mathrm{Hom}_{\mathbb{Z}H}(P_n, A)$$

by for any $f \in \mathrm{Hom}_{\mathbb{Z}G}(P_n, \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A))$ and $p \in P_n$ letting $\Phi(f)(p) = f(p)(1)$, equivalently $\Phi(f) = \mathrm{ev}_1 \circ f$, where $\mathrm{ev}_1(\phi) = \phi(1)$ is the evaluation map. Define

$$\Psi : \mathrm{Hom}_{\mathbb{Z}H}(P_n, A) \to \mathrm{Hom}_{\mathbb{Z}G}(P_n, \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A))$$

by for any $f \in \mathrm{Hom}_{\mathbb{Z}H}(P_n, H)$, any $p \in P_n$ and any $s \in G$ letting $\Psi(f(p))(s) = f(sp)$. As $f : P_n \to A$ is a H-module map and P_n is a G-module, $\Psi(f(p))$ is a well defined G-module map from P_n to $\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)$.

By the definition of our maps,

$$\Phi \circ \Psi(f)(p) = \Psi(f(p))(1) = f(p)$$

similarily, if $f \in \mathrm{Hom}_{\mathbb{Z}G}(P_n, \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A))$, $p \in P_n$ and $g \in G$

$$\Psi \circ \Phi(f)(p)(g) = \Psi(\mathrm{ev}_1 \circ f)(p)(g) = \mathrm{ev}_1 \circ f(gp) = f(gp)(1) = g.f(p)(1) = f(p)(g)$$

by the definitions of the the maps and the G-action on $\mathrm{Hom}_H(\mathbb{Z}G, A)$ and f being a G-map, proving that the maps are isomorphisms. It follows that, just as in the homology case, the cohomology of the complex

$$\mathrm{Hom}_{\mathbb{Z}G}(P, \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, A)) \cong \mathrm{Hom}_{\mathbb{Z}H}(P, A)$$

are both

$$\mathrm{Ext}^*_{\mathbb{Z}G}(\mathbb{Z}, \mathrm{Hom}_H(\mathbb{Z}G, A)) \cong H^*(G, \mathrm{Coind}^G_H(A))$$

and

$$\mathrm{Ext}^*_{\mathbb{Z}H}(\mathbb{Z}, A) \cong H^*(H, A)$$

proving the theorem. □

Corollary 2.5.1. *Every induced module has trivial homology and every co-induced module has trivial cohomology.*

Proof. $\{e\}$, the trivial group, is a subgroup of every group. A $\{e\}$-module is just an Abelian group. By definition, A is induced is equivalent to

$$A \cong \mathrm{Ind}^G_{\{e\}}(X)$$

for some Abelian group X, and similarily for co-induced modules. By Shapiros Lemma, for $n \geq 1$, if $A \cong \mathrm{Ind}^G_{\{e\}}(X)$ is an induced module

$$H_n(G, A) \cong H_n(\{e\}, X) = \mathrm{Tor}^{\mathbb{Z}}_n(\mathbb{Z}, X)$$

and if $A \cong \mathrm{Coind}^G_{\{e\}}(X)$ is co-induced

$$H^n(G, A) \cong H^n(\{e\}, X) = \mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}, X).$$

We we notice that as $\mathbb{Z}$ is a free $\mathbb{Z}$-module

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mathrm{Id}} \mathbb{Z} \longrightarrow 0$$

is a free and hence projective resolution of $\mathbb{Z}$. By the definiton of Tor and Ext respectively as derived functors of $\_ \otimes_{\mathbb{Z}} \mathbb{Z}$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \_)$ it is now clear that if A is induced then $H_n(G, A) = 0$ for all $n \geq 1$ and if A is coinduced $H^n(G, A) = 0$ for all $n \geq 1$. □

The power of this corollary will become apparent in the coming sections.

Lemma 2.5.4. *If H is a subgroup of G with finite index, then $\mathrm{Ind}^G_H(A) \cong \mathrm{Coind}^G_H(A)$ for any H-module A.*

Proof. Suppose A is a H-module. Let X be a set of left coset representatives of G/H (one member per co-set). X is a basis for $\mathbb{Z}G$ as a right H-module. By definition,

$$\mathrm{Ind}^G_H(A) \cong \mathbb{Z}G \otimes_{\mathbb{Z}H} A \cong \bigoplus_{x \in X} x \otimes A$$

with G-action $g(x \otimes a) = y \otimes ha$, where $gx = yh$ for some $h \in H$ and $y \in G$, as X is a right H-module basis of $\mathbb{Z}G$, this is always well defined.

Let $X^{-1} := \{x^{-1} | x \in X\}$, as $\forall s \in G$ there are $x \in X$ and $h \in H$ such that $s = xh \Leftrightarrow s^{-1} = h^{-1}x^{-1}$, X^{-1} is basis for $\mathbb{Z}G$ as a left H-module. Define

$$\pi_x a : \mathbb{Z}G \to A$$

defining it for $s \in X^{-1}$ by

$$\pi_x a(s) = \begin{cases} a \text{ , if } s = x^{-1} \\ 0, \text{ , if } s \neq x^{-1} \end{cases}$$

and extending $\mathbb{Z}H$-linearily to . We claim that

$$\text{Coind}_H^G = \text{Hom}_H(\mathbb{Z}G, A) \cong \prod_{x \in X} \pi_x A$$

where $\pi_x A := \{\pi_x a | a \in A\}$.

As X^{-1} is a left H-module basis for $\mathbb{Z}G$, $\varphi \in \text{Hom}_H(\mathbb{Z}G, A)$ is uniquely determined by $(\varphi(x^{-1}))_{x \in X} = (\pi_x(\varphi(x^{-1})))_{x \in X}$. That is φ is uniquely represented by some $\pi \in \prod_{x^{-1}} \pi_x A$. Conversely, if $(\tau_x)_{x \in X} \in \prod_{x \in X} \pi_x A$, the map $x^{-1} \mapsto \tau_x(x^{-1})$, defines by $\mathbb{Z}H$-linear extension a unique element in $\text{Hom}_H(\mathbb{Z}G, A)$, proving that there is a biective correspondence.

If $gx = yh \Leftrightarrow y^{-1}g = hx^{-1}$ where $h \in H$, $x, y \in X$ and $g \in G$, by all maps being $\mathbb{Z}H$-linear

$$g(\pi_x a(y^{-1})) = \pi_x a(y^{-1}g) = \pi_x a(hx^{-1}) = h.\pi_x a(x^{-1})) = ha.$$

If $z \neq y$, $z^{-1}g \neq hx^{-1}$ for any $h \in H$, whence$g(\pi_x a(z^{-1})) = 0$. Hence $g(\pi_x a) = \pi_y(ha)$.

We define the map $\Psi : \text{Ind}_H^G \to \text{Coind}_H^G$ by for all $x \in X$ and all $a \in A$

$$x \otimes a \mapsto \pi_x a$$

as usual, extending $\mathbb{Z}H$-linearily. $\Psi(x \otimes a) = \Psi(y \otimes b) \Leftrightarrow x = y$ and $a = b$, whence the map is injective on the basis elements, and as this is a injecitive linear map between Hmodules of finite rank, $[G : H]$, it is an isomorphism, which is what we wanted to show. □

Corollary 2.5.2. *If G is a finite group, a G-module is induced if, and only if it is coinduced.*

2.6 An exact sequence relating restriction and inflation

Let H be a normal subgroup of the group G and A a G-module

Theorem 2.6.1. *The following is a exact sequence*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{inf} H^1(G, A) \xrightarrow{res} H^1(H, A) \ .$$

Proof. We first show that $\text{res} \circ \inf = 0$, suppose $f \in \inf([g])$ is cochain representative in $H^1(G, A)$, then f is a map from G to $A^H \subset A$ that factors through G/H, i.e. if $\pi : G \to G/H$ is the natural projection, $f = g \circ \pi$. $\text{res}(f) = f\big|_H$, and as $\pi\big|_H = 0$. Hence $\text{res} \circ \inf([g]) = 0$, proving that the diagram is a chain complex.

Now, suppose f is a cocycle representative of some class in $H^1(G/H, A)$ such that $\inf([f]) = f \circ \pi = 0$. As $f(sH) = sH.f(1H) - f(1H)$ by the cocycle condition, we can, for all $s \in G$, express $\inf(f)(s) =: f'(s) = s.a - a$ for $a = f(1H)$. Hence, as $f'(h) = 0$ for all $h \in H$, $f'(s) = s.a - a = f'(ts) = st.a - a =$ for all $t \in H$ i.e. $t.a = a$ for all $t \in H$ proving that $a \in A^H$ and $f = 0$ in $H^1(G/H)$ ($f(s) = s.a - a$ is equivalent to f being a one-dimensional coboundary) proving exactness at $H^1(G/H, A^H)$.

Let f be a cocycle representing a cohomology class in $\ker \text{res}$, i.e. it is a cocycle of $H^1(G, A)$ such that $f\big|_H(t) = t.a - a$ for all $t \in H$. Define $f'(s) := f(s) - s.a + a$ to reduce to the case $f\big|H' = 0$ as $f \sim f'$ (they are cohomologous). By f' being a cocycle in $H^1(G, A)$, $f'(st) = s.f'(t) + f'(s) = f'(s)$ for all $t \in H$, i.e. f' is constant on cosets of H. With $s \in H$ and $t \in G$ we get $f'(st) = s.f'(t) + f'(s) = s.f'(t)$, now as H is a normal subgroup of G, $tH = Ht$ whence $f'(t) = f'(tH) = f'(Ht) = H.f'(t)$ and f' is invariant under H, and hence factors through a cocycle on G/H, i.e. $[f] = [f'] \in \text{im}(\inf)$, proving exactness at $H^1(G, A)$, and the sequence is exact as claimed.

□

We give a usefull generalisation of the above result

Proposition 2.6.1. *If $H^i(H, A) = 0$ for $1 \leq i \leq q-1$ ($q, i \in \mathbb{Z}$), we get directly from the long exact sequence in cohomology that $H^i(G/H, A^H) \cong H^i(G, A)$ for $1 \leq i \leq q-1$ and we have that the following sequence is exact*

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{inf} H^q(G, A) \xrightarrow{res} H^q(H, A) \ .$$

Proof. To prove this, we argue by induction on q, which is convinient as the base case $q = 1$ is a special case of the theorem we proved above. So, suppose $q \geq 2$ and the claim is true for positive integers $< q$. Let $B = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$ be the canonical choice of co-induced G-module that A embeds into (see propsosition 2.5.1. above). By a similar identification we use to get $H^q(G, A) = \text{Ext}^q_{\mathbb{Z}G}(\mathbb{Z}, A)$, we can identify any element in B with a function $f : G \to A$ such that $f(ts) = sf(t)$ for all $s, t \in G$, letting $f_a(t) = t.a$ for $a \in A$ and $t \in G$ defines our embedding of A into B. Let $C = B/A$ to get the short exact secquence of G-modules

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

As $\mathbb{Z}G$ is free as a $\mathbb{Z}H$-module (picking a representative from each coset of H defines a basis), we get that $\mathbb{Z}G = \mathbb{Z}H \otimes M$ for some Abelian group M (the free one on the basis elements described in the last parenthesis for example) and by Adjoint Associativity ([3], chapter 10 theorem 43), $B \cong \text{Hom}_{\mathbb{Z}}(\mathbb{Z}H, \text{Hom}_{\mathbb{Z}}(M, A))$ whence it is co-induced as a H-module as well. By our hypothesis $H^1(H, A) = 0$,

whence we have the exact sequence

$$0 \longrightarrow A^H \longrightarrow B^H \longrightarrow C^H \longrightarrow 0$$

and by definition of B^H it is invariant under H, whence $B^H \cong \mathrm{Hom}(\mathbb{Z}G/H, A)$, and hence co-induced as a $G/H-$module. Now let us analyse the commutative diagram

$$\begin{array}{ccccccc}
 & & H^{q-1}(G/H, B^H) = 0 & & H^{q-1}(G, B) = 0 & & H^{q-1}(H, B) = 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^{q-1}(G/H, C^H) & \xrightarrow{\inf} & H^{q-1}(G, C) & \xrightarrow{\mathrm{res}} & H^{q-1}(H, C) \\
 & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\
0 & \longrightarrow & H^q(G/H, A) & \xrightarrow{\inf} & H^q(G, A) & \xrightarrow{\mathrm{res}} & H^q(H, A) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & H^q(G/H, B^H) = 0 & & H^q(G, B) = 0 & & H^q(H, B) = 0
\end{array}$$

where the columns come from the long exact sequences in cohomology, as B is G- and H-coinduced and B^H is G/H-coinduced we get that the conecting homomorphisms are all isomorphisms whence we have an isomorphism of sequences. If we replace q by $q-1$ in the diagram, our hypothesis on A gives us that C satisfies the hypothesis (as the sequences are isomorphic and $H^{q-1}(H, A) = 0$). Hence by induction the top row is exact, whence the isomorphism of sequences imply that the bottom row is exact as well, proving the proposition. □

3 Non-Abelian Cohomology

We will develop a theory of low dimensional non-Abelian cohomology here. With this we will prove that there is a partial version of the classical long exact sequence for cohomology with coefficients in a non-Abelian G-module.

This is of special interest to us as the short exact sequence

$$1 \longrightarrow k^\times \longrightarrow \mathrm{GL}_n(k) \longrightarrow \mathrm{PGL}_n(k) \longrightarrow 1$$

where k is any field will be leveraged when we consider the Brauer groups of fields (which will be identified with the second dimensional cohomology of the (absolute) Galois group of k with coefficients in $k^\times$), and for the nontrivial cases when $n \geq 2$, we will indeed need some non-Abelian theory. It turns out that the theory developed below covers just enough for our further purpose.

3.1 Basic definitions

Let G be a group acting from the left on the group A (not necessarily Abelian), the action written $(s, a) \mapsto s(a)$, we say that A is a G-module if this action

commutes with the group operation in A. Throughout this section we will use the term $G-$module in the wider sense just defined, i.e. we don't assume the underlying group is Abelian.

3.1.1 $H^0(G,-)$ and $H^1(G,-)$

As in the Abelian case, we define $A^G := \{a \in A | s.a = a \forall g \in G\}$. We will write A multiplicatively to give emphasis that it need not be Abelian. We define $H^0(G,A) = A^G$ as in the Abelian case. We say that a map $f : G \to A$ is a cocycle if $f(s) := a_s$ and $a_{st} = s.a_t$ for all $s,t \in G$, if there is a $a \in A$ such that $b_s = a^{-1}.a_s.s(a)$ for all $s \in G$, we say that b_s is cohomologuos to a_s and write $b_s \sim a_s$. Obviously $a_s \sim a_s$ and $b_s \sim a_s \Rightarrow a_s \sim b_s$, suppose $a_s \sim b_s$ and $b_s \sim c_s$, then there are $a,b \in A$ such that $b_s = a^{-1}a_s s(a)$ and $c_s = b^{-1}b_s s(b)$ for all $s \in G$, but then

$$c_s = b^{-1}b_s s(b) = b^{-1}a^{-1}a_s s(a)s(b) = (ab)^{-1}a_s s(ab)$$

whence a_s is cohomologuos to c_s, proving that $\sim$ is a equivalence relation.

We shall call the set of cocycles from G to A quotiened by $\sim$ and having the class containing the unit cocycle $a_s = 1$ as a distinguished element, the cohomology set of G with values in A. If A is Abelian this is the underlying set of the usual $H^1(G,A)$ but without the structure of an Abelian group, keeping only the unit cocycle as a distinguished element, i.e. it is the image of $H^1(G,A)$ under the forgetfull functor from Abelian groups to pointed sets.

As $H^0(G,-)$ maps any G-module to a subset, it clearly maps morphisms between modules to their restriction, and just as in the Abelian case, the image of an invariant element must again be invariant, whence $H^0(G,-)$ is a functor. We make $H^1(G,-)$ into a functor as well by given a map $f : A \to B$ of G-modules, defining $H^1(G,f) = f \circ (-)$, i.e. we compose the cocycles of A with f to get a cocycle of b, as f is a G-module map, this composition is compatible with the equivalence relation $\sim$ whence it is well defined on cohomology classes.

Given a map of pointed sets $f : A \to B$ (with distinguished points denoted 1), we say that the kernel of f is the preimage of the distinguished point, that is $\ker f = f^{-1}(1)$. As we have the notion of a kernel of maps, we can now talk about exact sequences of pointed sets in the same sense as in any Abelian category, namely $A \xrightarrow{i} B \xrightarrow{p} C$ is exact at B if $\mathrm{im} i = \ker p$.

Let $1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$ be an exact sequence of G-modules with $i(A)$ normal in B. We will now in a few steps define $\delta : C^G \to H^1(G,A)$, the coboundary operator.

Suppose $c \in C^G$ and pick $b \in p^{-1}(c)$, which is possible by the exactness of the sequence. For the same reason and by $i(A)$ normal in B, we get that $C \cong B/i(A)$ whence $s.b \equiv b \bmod i(A)$ for all $s \in G$, since otherwise we contradict that $c \in C^G$. Now, define $a_s := i^{-1}(b^{-1}s(b))$. To show that this is a cocycle whose cohomology class is independent of which fiber of c we pick, we first compute

$$a_{st} = i^{-1}(b^{-1}st(b)) = i^{-1}(b^{-1}s(bb^{-1}t(b))) = i^{-1}(b^{-1}s(b)s(b^{-1}t(b))) = a_s.s(a_t)$$

proving that we hit at least one cocycle. Secondly, suppose $b, b' \in p^{-1}(c)$, then since $B/i(A) \cong C$ there is a $a \in A$ such that $b' = bi(a)$, and if we let a'_s be the cocycle associated to b' we get that

$$a'_s = b'^{-1}s(b') = i(a)^{-1}b^{-1}s(b)s(i(a)) = i(a)^{-1}a_s s(i(a))$$

and $a'_s \sim a_s$, proving that the cohomology class of the cocycles are independent of the choice of fibers of c, hence $\delta(c) = [a_s]$ (the cohomology class of a_s) is a well defined coboundary operator from $H^0(G, C)$ into $H^1(G, A)$. We note that this coboundary operator coincides with the classical one in the Abelian case.

3.1.2 $H^2(G, -)$ for central submodules

Consider the case when A is contained in the center of B in the exact sequence $1 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$. As A is contained in the center of B it is in particular Abelian, whence $H^2(G, A)$ is well defined in the usuall way, we will however forget the Abelian stucture of this set and only consider it as a pointed set for the most part. We shall define a second coboundary operator, $\Delta : H^1(G, C) \to H^2(G, A)$. Given a cocycle c_s of C, for each $s \in G$, pick a $b_s \in B$ such that $p(b_s) = c_s$, by definition we get that $p(b_{st}) = c_{st} = c_s s(c_t) = p(b_s)p(s(c_t))$ whence by the original sequence $b_{st} \equiv b_s s(b_t) \mod i(A)$ for all $s, t \in G$ and we will define $a_{s,t} := b_s.s(b_t)b_{st}^{-1}$. We will now show that this defines a cocycle independent of the representative of $[c_s]$ (the cohomology class of c_s) and of the choice of $b_s \in p^{-1}(c_s)$, and we then define $\Delta(c_s)$ as the cohomology class of $a_{s,t}$. Recalling that a 2-cocycle in the Abelian case is a map $f : G \times G \to A$ such that for all $a, t, u \in G$

$$s.f(t, u) - f(st, u) + f(s, tu) - f(s, t) = 0$$

which in our multiplicative notation becomes

$$s.f(t, u)f(s, tu) = f(st, u)f(s, t)$$

and as A is Abelian we only need to verify that for all $s, t, u \in G$

$$a_{s,t}^{-1}a_{s,tu}a_{st,u}^{-1}s(a_{t,u}) = 1.$$

We do this by a explicit computation

$$a_{s,t}^{-1}a_{s,tu}a_{st,u}^{-1}s(a_{t,u}) = (b_s.s(b_t)b_{st}^{-1})^{-1}(b_s.s(b_{tu})b_{stu}^{-1})(b_{st}.st(b_u)b_{stu}^{-1})^{-1}s(a_{t,u})$$

using that by definition $a_{s,t} = b_s.s(b_t)b_{st}^{-1}$, we get

$$a_{s,t}^{-1}a_{s,tu}a_{st,u}^{-1}s(a_{t,u}) = b_{st}s(b_t)^{-1}b_s^{-1}b_s s(b_{tu})b_{stu}^{-1}b_{stu}st(b_u)^{-1}b_{st}^{-1}s(a_{t,u})$$

by expanding the parentheses,

$$a_{s,t}^{-1}a_{s,tu}a_{st,u}^{-1}s(a_{t,u}) = b_{st}s(b_t)^{-1}s(b_{tu})st(b_u)^{-1}b_{st}^{-1}s(a_{t,u})$$

$$= b_{st}s(b_t)^{-1}s(a_{t,u})s(b_{tu})st(b_u)^{-1}b_{st}^{-1}$$

using that A is contained in the center of B, then by expanding $s(a_{t,u}) = s(b_t)st(b_u)s(b_{tu})^{-1}$,

$$a_{s,t}^{-1}a_{s,tu}a_{st,u}^{-1}s(a_{t,u}) = b_{st}s(b_t)^{-1}s(b_t)st(b_u)^{-1}s(b_{tu})^{-1}s(b_{tu})st(b_u)b_{st}^{-1}$$

$$= b_{st}st(b_u)^{-1}st(b_u)b_{st}^{-1} = 1$$

which is what we wanted.

Suppose $c'_s = c^{-1}c_s s(s)$ for some $c \in C$, that is c'_s is cohomologuos to c_s. We lift c'_s to the B-cocycle $b'_s = b^{-1}b_s s(b)$ for some $b \in p^{-1}(c)$ and let $a'_{s,t}$ be the associated 2-cocycle of A. We compute

$$a'_{s,t} = b'_s s(b'_t)b'^{-1}_{st} = b^{-1}b_s s(b)s(b^{-1}b_t t(b))(b^{-1}b_{st}st(b))^{-1} =$$

$$= b^{-1}b_s s(b)s(b^{-1})s(b_t)st(b))st(b)^{-1}b_{st}^{-1}b = b^{-1}b_s s(b_t)b_{st}^{-1}b = b^{-1}a_{s,t}b = a_{s,t}$$

proving the independence of cocycle representative.

Lastly, suppose $b_s, b'_s \in p^{-1}(c_s)$, then there is a cocycle a_s of A such that $b'_s = b_s a_s = a_s b_s$. It follows that the 2-cocycle associated to b'_s is

$$a'_{s,t} = a_s b_s s(a_t b_t)b_{st}^{-1}a_{st}^{-1}$$

which, as A is contained in the center of B can be rewritten as

$$a'_{s,t} = a_s s(a_t)a_{st}^{-1}b_s s(b_t)b_{st}^{-1} = a_{st}a_{s,t}$$

for some $1-$cocycle a_{st} whence $a'_{s,t} \sim a_{s,t}$ finally proving that Δ is a well defined coboundary operator.

3.2 The long exact sequence

This following theorem is what we will use in our study of the Brauer group.

Theorem 3.2.1 ("Long exact sequence"). *Given an exact sequence of not necessarily Abelian G-modules*

$$1 \xrightarrow{i} A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 1$$

we have an exact sequence in cohomology

$$1 \longrightarrow H^0(G,A) \xrightarrow{i_0} H^0(G,B) \xrightarrow{p_0} H^0(G,C)$$

$$\xrightarrow{\delta} H^1(G,A) \xrightarrow{i_1} H^1(G,B) \xrightarrow{p_1} H^1(G,C)$$

and if A is contained in the center of B

$$1 \longrightarrow H^0(G,A) \longrightarrow H^0(G,B) \longrightarrow H^0(G,C) \xrightarrow{\delta} H^1(G,A)$$

$$\longrightarrow H^1(G,B) \longrightarrow H^1(G,C) \xrightarrow{\Delta} H^2(G,A).$$

Proof. As $H^0(G,A) = A^G$ and $H^0(G,B) = B^G$, the exactness of the original sequence gives exactness at $H^0(G,A)$ as A injects into B and the image of an invarian element must be invariant (proven in the same way as for the Abelian case above).

By the exactness of the original sequence, $p_0 \circ i_0 = 1$, this also follows by functoriality (the initial/terminal object maps to initial/terminal object if they exist in the image of the functor). Suppose $b \in B^G$ is in the kernel of p_0, then by the exactness of the starting sequence, $b \in B^G \cap i(A) = i(A)^G = i(A^G)$, proving exactness at $H^0(G,B)$.

If $c \in p_0(B^G)$, then there is a $b \in B^G$ such that $p(b) = c$, and if $\delta(c) = 1$, we have by definition that the cocycle class associated to c contains $a_s = b^{-1}s(b) = 1$ for some $b \in p^{-1}(c)$ and all $s \in G$, but this b is obviously invariant under G and hence $\ker\delta = p_0(B^G)$, proving exactness at $H^0(G,C)$.

If a_s is a cocycle of A whoose class is contained in the kernel of i_1, there is by the definition of the definition of $H^1(G,B)$, a $b \in B$ such that $i(a_s) = b^{-1}s(b)$ for all $s \in G$, which by the definition of δ holds if the class is in the image of δ. On the other hand, if $[a_s] \in \delta(C^G)$, there is a $b \in p^{-1}(c)$, where $\delta(c) = [a_s]$, such that $a_s = b^{-1}s(b)$ whence $i(a_s) = b^{-1}s(b)$ is a 1-coboundary of B and cohomologuous to 1, i.e. a_s is contained in the kernel of i_1, proving exactness at $H^1(G,A)$.

By functoriality, $p_1 \circ i_1 = 1$, (see parethesis in proof of exactness at $H^0(G,B)$). If $p_1([b_s]) = [1]$, then there is a $c \in C$ such that $p(b_s) = c^{-1}s(c)$ for all $s \in G$ as it is cohomologuous to 1, but as $\mathrm{im}i_1 \subset \ker p_1$, 1 is cohomologuous to a cocycle of the form $p(i(a_s))$ where a_s is a cocycle of A. Hence, as p is surjective and by $s(b) \equiv b \bmod i(A)$ for all $b \in B$ and all $s \in G$, there is a $b \in B$ such that for all $s \in G$, $b_s = b^{-1}i(a_s)s(b)$, that is $[b_s] \in \mathrm{im}i_1$, proving exactness at $H^1(G,B)$.

Suppose now that A is contained in the center of B. By the definition of Δ, we have that b_s is a cocycle of B, then we have the $2-$cocycle $a_{s,t} = b_s s(b_t) b_{st}^{-1}$ associated to $p(b_s)$. As b_s is a cocycle, $a_{s,t} = b_s s(b_t) b_{st}^{-1} = b_s s(b_t)(b_s s(b_t))^{-1} = 1$, and $\Delta \circ p_1 = 1$. Conversely, if c_s is a cocycle whoose class is contained in the kernel of Δ, we have that there is a $b_s \in B$ such that $p(b_s) = c_s$ and the associated $2-$cocycle $a_{s,t} = b_s s(b_t) b_{st}^{-1}$ is cohomologuous to zero (A being thought of as additive as it is Abelian) and of the form $a_s s(a_t) a_{st}^{-1}$ where a_s is a 1-cocycle of A. As we showed above that the associated cocycle is independent of the choice of coset representative of $b_s \bmod i(A)$, whence we can replace b_s with $a_s^{-1}b_s$. This gives us

$$a_{s,t} = a_s^{-1} b_s s(a_t^{-1}) s(b_t) b_{st}^{-1} a_{st} = a_s^{-1} a_{st} s(a_t^{-1}) b_s s(b_t) b_{st}^{-1} =$$

$$= a_s^{-1} a_{st} s(a_t^{-1}) a_s s(a_t) a_{st}^{-1} = 1$$

by A contained in the center of B. But from this we get $b_{st}^{-1} = (b_s s(b_t))^{-1} \Leftrightarrow b_{st} = b_s s(b_t)$ and b_s is a cocycle of B with $p(b_s) = c_s$, proving that if c_s is contained in a class contained in the kernel of Δ, then this class is in the image of p_1, proving exactness at $H^1(G,C)$. $\square$

4 Tate cohomology and cohomology of finite cyclic groups

In this section we will introduce Tate cohomology, a way to connect the long exact sequence in homology to the long exact sequence in cohomology of G-modules when G is finite. Then we consider an even more narrow case, when G is finite and cyclic. It will turn out that in this case, the Tate cohomology of a G-module is cyclic, whit a period 2, a fact that substantially reducess the amount of calculations needed to get any cohomological and homological information about any such G-module.

4.1 Tate cohomology

Assume G is a finite group and A a G-module. The map

$$N : A \to A$$

defined by

$$a \mapsto Na = \sum_{s \in G} s.a$$

is well defined and called the norm map, and the element $N = \sum_{s \in G} s$ is called the norm of G.

Let as above I_G denote the augumentation ideal of $\mathbb{Z}G$, i.e. the set of linear combinations of $s - 1$, $s \in G$. We have that $N(s-1) = \sum_{g \in G} g(s-1) = 0$ as G is finite and $Ns = N$, hence $I_G A \subset \ker N$. And, again by G being finite $sN = N$ for all $s \in G$, whence im $N \subset A^G$.

By definition $H_0(G, A) = A/I_G A$ and $H^0(G, A) = A^G$, hence what we just showed imply that there is a uniquely determined homomorphism

$$N* : H_0(G, A) \to H^0(G, A)$$

such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{N} & A \\ \downarrow & & \uparrow{\scriptstyle i} \\ H_0(G, A) & \xrightarrow{N^*} & H^0(G, A) \end{array}$$

commutes. We define

$$\hat{H}_0(G, A) := \ker N^* = \ker N / I_G A$$

and

$$\hat{H}^0(G, A) := \text{coker} N^* = A^G / NA.$$

Theorem 4.1.1. *If A is a relatively projective, or equivalently as G is finite, a relatively injective G-module. Then*

$$\hat{H}_0(G, A) = 0 = \hat{H}^0(G, A).$$

Proof. Suppose A is relatively projective, then by lemma 2.6.1.3, there is a $\rho \in \mathrm{End}_{\mathbb{Z}}(A)$ such that for all $a \in A$, $a = \sum_{s\in G} s.\rho(s^{-1}.a)$. Suppose that $a \in \ker N$, then as ρ is a additive map, $\sum_{s\in G} \rho(s^{-1.a}) = \rho(\sum_{s\in G} s^{-1}.a) = \rho(N.a) = 0$. Hence

$$a = \sum_{s\in G} s.\rho(s^{-1}.a) - \sum_{s\in G} \rho(s^{-1}.a) = \sum_{s\in G} (s-1).\rho(s^{-1}.a).$$

That is $a \in I_G A$, hence by definition, $\hat{H}_0(G, A) = 0$.

If A is induced (and therefore coinduced), then $A \cong \bigoplus_{s\in G} s.X$ for some subgroup X of A. Hence for all $a \in A$, $a = \sum_{s\in G} s.x_s$. Suppose $a \in A^G$, then for all $g \in G$

$$a = g.a = g.\sum_{s\in G} s.x_s = \sum_{s\in G} gs.x_s$$

that is $x_s = x_{gs}$ for all $s \in G$, but as this is true for all $g \in G$, $x_s = x_t =: x$ for all $s, t \in G$, that is $a = \sum_{s\in G} s.x = N.x$ and $A^G = \mathrm{im}N$ whence $H^0(G, A) = 0$. As every relatively projective module is a direct factor of a (co)induced module, this proves the theorem. □

Let

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

be an exact sequence of G-modules.

Lemma 4.1.1. *There is a homomrphism*

$$\delta : \hat{H}_0(G, C) \to \hat{H}^0(G, A)$$

such that

$$\hat{H}_0(G, B) \longrightarrow \hat{H}_0(G, C) \xrightarrow{\delta} \hat{H}^0(G, A) \longrightarrow \hat{H}^0(G, B)$$

is an exact sequence.

Proof. Consider the diagram

$$\begin{array}{ccccccccc}
H_1(G,C) & \longrightarrow & H_0(G,A) & \longrightarrow & H_0(G,B) & \longrightarrow & H_0(G,C) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle N_A^*} & & \downarrow{\scriptstyle N_B^*} & & \downarrow{\scriptstyle N_C^*} & & \\
0 & \longrightarrow & H^0(G,A) & \longrightarrow & H^0(G,B) & \longrightarrow & H^0(G,C) & \longrightarrow & H^1(G,C)
\end{array}$$

where N_X^* is the map induced by the the norm and passing to the quotient on the module X defined above. As $N(I_G) = 0$, all of the vertical arrows are independent of the coset representative of $a \in A/I_G A$ (similarily for B and C). If φ is the G-module map from A to B in the original sequence, we get

$$N_B^*(\varphi(a + I_G A) = N_B^*(\varphi(a) + I_G A) = N(\varphi(a)) = \sum_{s\in G} s.\varphi(a)$$

and

$$\varphi(N_A^*(a)) = \varphi(\sum_{s\in G} s.a) = \sum_{s\in G} s.\varphi(a).$$

proving that the first square commutes. The commutativity of the second one is proven by an analogous argument. It follows from the Snake Lemma [2](lemma 1.3.2), that δ is well defined.

Explicitly; if $c \in \ker N_C^*$, lift using exactness of the rows which comes from the long exact sequence of homology and cohomology, c to $b \in H_0(G, B)$. Then as $c \in \ker N_C^*$, the commutativity of the diagram gives that there is a $a \in H^0(G, A)$ such that $\varphi(a) = N_B^*(b)$. As the map from $H^0(G, A)$ to $H^0(G, B)$ is injective, this is unique element. We define $\delta(c) = a$. Suppose b, b' are both in the fiber of c, then there are unique a, a' such that $\varphi(a) = N_B^*(b)$ and $\varphi(a') = N_B^*(b')$. As both b and b' maps to c under the morphism from $H_0(G, B)$ to $H_0(G, C)$, $b - b'$ is in the kernel of this morphism. Hence there is, by exactness, a $a + I_G A \in H_0(G, A)$ such that $\varphi(a + I_G A) = b - b'$. We get $\varphi(N_A^*(a + I_G A)) = \varphi(Na) = N\varphi(a) \equiv 0 \bmod \mathrm{im} N_A^*$, that is the image of c under δ is independent of the choice of b in the preimage of c, and hence δ is a well defined map.

By the definition of $\hat{H}_0(G, -)$ and $\hat{H}^0(G, -)$ and the Snake Lemma, together with the long exact sequences in cohomology and homology the lemma follows. □

We are now ready to define the Tate cohomology groups $\hat{H}^q(G, \_)$ for $q \in \mathbb{Z}$.

Definition 4.1.1. *Given a $G-$module A, where G is a finite group, define*

$$\hat{H}^q(G, A) := \begin{cases} H^q(G, A) \text{ , if } q \geq 1 \\ A^G/NA \text{ , if } q = 0 \\ \ker N/I_G A \text{ , if } q = -1 \\ H_{g+1}(G, A) \text{ , if } q \leq -2. \end{cases}$$

The lemma we showed above proves that a short exact sequecnce of G-modules gives rise to a long exact sequence of Tate cohomology groups. We have also seen that a consequence of Shapiros lemma is that if A is a relatively projective/injective then $\hat{H}^q(G, A) = 0$ for $q \in \mathbb{Z} \setminus \{0, -1\}$ and we proved above that $\hat{H}^{-1}(G, A) = 0 = \hat{H}^0(G, A)$. With this together with the long exact sequence in Tate-cohomology, we get the following:

Theorem 4.1.2 (Dimension shifting of Tate cohomology)**.**

- *Every G-module A embedds into a induced G-module A^**
- *Every G-module A is the quotient of an induced G-module A_* by a submodule A'*

and the following identities hold for all $q \in \mathbb{Z}$

$$\hat{H}^q(G, A) = \hat{H}^{q+1}(G, A^*/A)$$

and

$$\hat{H}^q(G, A) = \hat{H}^{q-1}(G, A').$$

We can furthermore choose A^* and A_* so that A is a direct $\mathbb{Z}$-module factor of A^* and A' of A_*.

4.2 Cohomology of finite cyclic groups

Let G be a finite cyclic group of order n generated by $s \in G$. Define

$$N := \sum_{t \in G} t = \sum_{k=0}^{n-1} s^k$$

and

$$D = s - 1.$$

We define the cochain complex K by letting $K^i = \mathbb{Z}[G]$ for all $i \in \mathbb{Z}$, and $d : K^i \to K^{i+1}$ by multiplication by D if i is even and by multiplication by N if i is odd. For any G-module A let $K(A) := K \otimes_{\mathbb{Z}G} A$ so that for all $i \in \mathbb{Z}$, $K^i(A) = A$. It follows that $d : K^i \to K^{i+1}(A)$ is defined by multiplication by D if i is even and by N if i is odd. If we apply $K(-)$ to a short exact sequence of G-modules

$$0 \to A \to B \to C \to 0$$

we get a short exact sequence of complexes

$$0 \to K(A) \to K(B) \to K(C) \to 0.$$

Taking cohomology, we get a long exact sequence of cohomology groups with a connecting homomrphism $\delta : H^q(K(C)) \to H^{q+1}(K(A))$. It is worth noting that by definition, the cohomology groups of $K(A)$ depends only on the parity of their index, i.e. $H^q(K(A)) = H^l(K(A))$ if and only if $k \equiv l \bmod 2$.

Theorem 4.2.1. *The cohomological functors $\{H^q(K(\_)), \delta\}$ and $\{\hat{H}^q(G, \_), \delta\}$ are isomorphic.*

Proof. As G is cyclic, it follows that

$$H^{-1}(K(A)) = \ker N / \mathrm{im} D \cong \ker N / I_G A = \hat{H}^{-1}(G, A)$$

and

$$H^0(K(A)) = \ker D / \mathrm{im} N = A^G / \mathrm{im} N = \hat{H}^0(G, A).$$

Also, as the connecting homomorphism from degree -1 to 0 of both functors arises by the snake lemma applied to the same diagram;

$$\begin{array}{ccccccc} & & \ker N_A / I_G A & \longrightarrow & N_B / I_G B & \longrightarrow & N_C / I_G C \longrightarrow 0 \\ & & \downarrow{\scriptstyle N_A^*} & & \downarrow{\scriptstyle N_B^*} & & \downarrow{\scriptstyle N_C^*} \\ 0 & \longrightarrow & A^G / \mathrm{im} N_A & \longrightarrow & B^G / \mathrm{im} N_B & \longrightarrow & C^G / \mathrm{im} N_C \end{array}$$

whence they coincide. It follows that $H^q(K(A)) = 0$ for $q = 0, -1$ and hence by periodicity for all q if A is relatively projective. The full theorem now follows by induction and dimension shifting of Tate cohomology. □

Corollary 4.2.1.

$$\hat{H}^q(G, A) = \begin{cases} A^G / NA \text{ , if } q \text{ is even} \\ \ker N / I_G A \text{ , if } q \text{ is odd.} \end{cases}$$

If $\hat{H}^0(G,A)$ and $\hat{H}^1(G,A)$ are both finite, let $h_0(A)$ and $h_1(A)$ denote their order respective. We define the Herbrand quotient of A to be

$$h(A) := \frac{h_0(A)}{h_1(A)}.$$

Theorem 4.2.2. *Consider an exact sequence $0 \to A \to B \to C \to 0$ of G-modules. If at least two of the Herbrand quotients $h(A), h(B), h(C)$ are defined, then so is the third, and*

$$h(B) = h(A)h(C).$$

Proof. Without loss of genereality (as the other cases follows by considering groups in the long exact sequence in different orders), we assume that $h(A)$ and $h(C)$ are defined. From the long exact sequence of Tate cohomology,

$$h_i(B) = h_i(A)h_i(C)$$

for $i \in \{0,1\}$. As the Herbrand quotients for A and C are defined, this shows that $h_i(B)$ is always finite, and $h(B) = h(A)h(C)$, which is what we wanted. □

Theorem 4.2.3. *If A is a finite G-module, then $h(A) = 1$.*

Proof. Consider the sequence

$$0 \longrightarrow A^G \longrightarrow A \xrightarrow{D} A \longrightarrow A_G \longrightarrow 0.$$

As A^G is a submodule of A, it is exact at A^G. $Da = 0$ if and only if $sa = a$ i.e. if $a \in A^G$, hence it is exact at the leftmost A. If $I_G A \ni a = \sum_{k=0}^{n-1}(s^k - 1)x_k = \sum_{k=0}^{n-1}(s-1)(s^{k-1} + \ldots + 1)x_k$, $a \in DA$, whence the sequence is exact in the rightmost A. It is exact at A_G by definition.

From the exactness of the sequence, it follows that $\frac{\mathrm{Card}(A)}{\mathrm{Card}(A^G)} = \mathrm{Card}(DA)$, and $\frac{\mathrm{Card}(A)}{\mathrm{Card}(DA)} = \mathrm{Card}(A_G)$ whence $\mathrm{Card}(A^G) = \mathrm{Card}(A_G)$. Next, consider the sequence

$$0 \longrightarrow \hat{H}^1(G,A) \longrightarrow A_G \xrightarrow{N} A^G \longrightarrow \hat{H}^0(G,A) \longrightarrow 0.$$

As $\hat{H}^1(G,A) \cong \ker N/DA = \ker N/I_G A \subset A_G$, the sequence is exact at $\hat{H}^1(G,a)$ and by the same isomorphism, it is exact at A_G. $\hat{H}^0(G.A) = A^G/NA$, whence the sequence is exact in the two leftmost entries as well, hence the sequence is exact. It follows from exactness and $\mathrm{Card}(A_G) = \mathrm{Card}(A^G)$ that $h_0(A) = \mathrm{Card}(\hat{H}^0(G,A)) = \mathrm{Card}(\hat{H}^1(G,A)) = h_1(A)$, whence $h(A) = 1$. □

5 Central Simple Algebras.

In this section we introduce basic definitions and results on simple algebras, in particular simple algebras central over a field. We give a proof of Wedderburn's theorem, and four equivalent definitions of a simple algebra central over a field k.

5.1 Some results

We recall that a ring R is said to be simple if the only two sided ideals of it is $0, R$, as all $k-$algebras are rings the same definition is used for them (for any unital ring k). Similarily an R-module is simple if the only proper submodule it has is the zero module. Throughout this chapter A will denote a k-algebra, where k is a field.

Definition 5.1.1. *A k-algebra D is called division algebra if all non zero elements are invertible, i.e. $D^\times = D \setminus 0$.*
Lemma 5.1.1. *If D is a division k-algebra, then for any integer $n \geq 1$, the ring of n by n matrices, $M_n(D)$, is a simple algebra.*

Proof. We need to prove that any non-zero (two sided) ideal of $M_n(D)$ is the whole ring. Suppose $A \in M_n(D)\backslash\{0\}$, then there is a element $(i,j) \in \{1,\dots,n\}^2$ such that $a_{ij} \neq 0$, and as D is a division ring, it is invertible. Let E_{kl} denote the matrix in $M_n(D)$ with all entries equal to zero except the $ij-$th entry which is 1. We get by the laws of matrix multiplication that $a_{ij}^{-1}E_{ii}AE_{jj} = E_{ij}$ and as $E_{ki}E_{ij}E_{jl} = E_{kl}$, we have that $E_{kl} \in (A)$ (the two-sided ideal generated by A), and as $\{E_{kl}\}_{k,l\in\{1,\dots,n\}}$ is a basis for $M_n(D)$ as a left(and right) $M_n(D)-$module, $(A) = M_n(D)$, proving the lemma. □

As the center of $M_n(D)$ is scalar multiples of the identity matrix with elements in the center of D, it is a central simple algebra over the field that is the center of D.

Proposition 5.1.1. *If D is a division ring and N a simple $M_n(D)-$module for some postive integer n, then $N \cong D^n$.*

Proof. First, let $I_r \subset M_n(D)$ be the left submodule of matrices with entries $a_{ij} = 0$ for all $j \neq r$, i.e. the set of matrices whose only non-zero entries lay in the $r-$th column. Given $(a_{ij}) = A \in I_r \setminus \{0\}$, there is a $i \in \{1,\dots,n\}$ such that the entry $a_{ir} \neq 0$. As $a_{ir}^{-1}E_{ji}A = E_{jr}$ we get that a basis for I_r is contained in the submodule generated by A, whence I_r is a simple $M_n(D)-$module. It is now rather clear that $M_n(D) \cong \bigoplus_{r=1}^n I_r$ as a $M_n(D)$-module.

Suppose now that N is a simple left $M_n(D)$-module, as I_rN is a submodule of N we must have that $I_rN \in \{0, N\}$. Suppose $I_rN = N$ and let $a \in N \setminus 0$, as $N = I_rN$ is simple, $I_ra = N$ and we get a module isomorphism $I_r \to N$ by $x \mapsto xa$, with the obvious inverse. Hence all simple $M_n(D)-$modules are isomorphic to I_r for some r and as the map induced by $a_{ir} \mapsto a_{il}$ is an isomorphism between

I_r and I_l we can pick any $r \in \{1, \ldots, n\}$, say 1, so any simple $M_n(D)-$module is isomorphic to I_1.

That N is isomorphic to D^n follows from mapping $(a_{ij})_{i,j} \in I_r$ defined above to $(a_{ir})_i \in D$ as all other entries are zero in any element of I_r, this map is injective and clearly a left $D-$module homomorphism, it is also surjective whence it is an isomorphism. □

Consider the endomorphism ring of a left A-module, where A is a k-algebra. The operations in $\mathrm{End}_A(M)$ are given by pointwise addition and function compostion. Given $\phi, \psi \in \mathrm{End}_A(M)$ and $a, b \in M$, by linearity

$$\psi(\phi(a) + b) = \psi \circ \phi(a) + \psi(b)$$

and the ring structure is indeed well definied. Given $a \in k$, we define $m_a(x) = ax$ for $x \in M$, which clearly is a A-endomorphism as $k \in A$, and as $m_a = 0$ if and only if $a = 0$, and $m_{ab+c} = m_a \circ m_b + m_c$ this defines a ring embedding, whence k embedds into the center of $\mathrm{End}_A(M)$, i.e. $\mathrm{End}_A(M)$ is a k-algebra.

Any A-module M is also a $\mathrm{End}_A(M)$-module by the action

$$\psi.a = \psi(a)$$

for any $\psi \in \mathrm{End}_A(M)$ and any $a \in M$.

Definition 5.1.2. *If D is a division ring, we call left D-modules left vector spaces over D and similarily for right vector spaces.*

Definition 5.1.3. *If R is a ring, we define the opposite ring of R, R^o to be the same Abelian group but with multiplication given by $a * b = ba$, where xy denotes the usuall product in R.*

Lemma 5.1.2. *If A is a division algebra, and M is a left vector space over A, and if $\dim_A M = n < \infty$, choosing a basis for M yields an isomorphism between $End_A(M)$ and a matrix algebra. More precisely, $End_A(M) \cong M_n(A^o)$, where n, as above is the dimension of M over A.*

Proof. To prove this let $\psi, \phi \in \mathrm{End}_A(M)$ and $\{m_i\}_{i=1}^n$ be a A-basis for M. Then ψ, ϕ are completely determined by where they map $\{m_i\}_i$. Let

$$\phi(m_i) = \sum_j a_{ji} m_j$$

and

$$\psi(m_i) = \sum_j b_{ji} m_j.$$

We get that

$$\psi \circ \phi(m_i) = \sum_j a_{ji} \psi(m_j) = \sum_j a_{ji} \sum_k b_{kj} m_k = \sum_{j,k} a_{ji} b_{kj} m_k$$

which gives us that $\psi \circ \phi$, relative to the choosen basis, is represented by the matrix

$$\left(\sum_j a_{ji} b_{kj}\right)_{i,k} = \left(\sum_j b_{kj} * a_{ji}\right)_{i,k} = (b_{kj})_{k,j} (a_{ji})_{j,i}$$

where the last product is taken in the matrix ring $M_n(A^o)$. This shows that any A-basis of M comes with a natural ring homomorphism α from $\mathrm{End}_A(M)$ to $M_n(A^o)$. If for some endomorphism ϕ, $\alpha(\phi) = 0$, this directly by the definition of α means that $\phi(m_i) = 0$ for any element in the choosen basis, thus $\phi = 0$, proving that α is injective. Given any $\{v_i\}_{i=1}^n \subset M$, which expressed in coordinate form in the given basis is the columns of an matrix in $M_n(^o)$, defining a map sending m_i to v_i and then extending linearily (possible by the universal property of free modules for example), defines a endomorphism ψ_v. $\alpha(\psi_v)$ will be the matrix with the v_is as columns, proving surjectivity, hence we have $\mathrm{End}_A(M) \cong M_{\dim_A M}(A^o)$ for any finite dimensional left module M over the division ring A.

□

Lemma 5.1.3 (Schur's Lemma)**.** *If M is a simple A-module where A is a k-algebra, then $End_A(M)$ is a division algebra.*

Proof. The kernel of any endomorphism of M is a submodule. As M is simple, any endomorphism is either injective or trivial. As the quotient of M by the zero module is isomorphic to M, it follows from the isomorphism theorems for modules that $f(M) \cong M/\ker f \cong M$ for any nontrivial endomorphism f. This shows that any nontrivial endomorphism is an automorphism, i.e. every non-zero element in $\mathrm{End}_A(M)$ has a multiplicative inverse (recall that the product is function composition), and we have proved that $\mathrm{End}_A(M)$ is a division algebra. □

Let M be an A-module with endomorphism ring $E = \mathrm{End}_A(M)$, by the action defined above M is also an E-module. Consider the endomorphism ring $\mathrm{End}_E(M)$. We define the map

$$\lambda_M : A \to \mathrm{End}_E(M)$$

by

$$a \mapsto (m \mapsto am)\,.$$

As M is a A-module, given $\phi \in E$,

$$\phi(am) = a\phi(m).$$

This gives that $\lambda_M(a)(\phi) = \phi.\lambda_M(a)$ i.e. $\lambda_M(a)$ is a E-module endomorphism. Hence the map is well defined and clearly a ring homomorphism.

Lemma 5.1.4 (Rieffel's Lemma)**.** *If A is a simple k-algebra, L a non zero left ideal of A and $E = End_A(L)$. Then $\lambda_L : A \to End_E(L)$ is an isomorphism.*

Proof. As λ_L is a ring homomorphism, its kernel will be a two sided ideal of A whence simplicity of A yields that $\ker \lambda_L \in \{0, A\}$.As L is a non-zero ideal $\lambda_L \neq 0$ and it is hence injective.

Let $\phi \in \mathrm{End}_E(L)$ and $l \in L$, we get $\phi\lambda_L(l)(x) = \phi(lx)$. We have that for all $x \in L$, the map $y \mapsto \psi_x(y) = yx$, where $y \in L$, is an A-endomorphism of L, that is $\psi_x \in E$. As ϕ is an E-endomorphism, we get

$$\phi\lambda_L(l)(x) = \phi(lx) = \phi(\psi_x(l)) = \psi_x(\phi(l)) = \phi(l)x$$

and as $\phi(l) \in L$, $\phi\lambda_L(l) \in \lambda_L(L)$, i.e. $\lambda_L(L)$ is a left ideal in $\mathrm{End}_E(L)$.

Note that, as A is simple and L is a left ideal, the right ideal LA generated by L is the whole algebra. Hence

$$1_A = \sum l_i a_i$$

for some $l_i \in L$ and $a_i \in A$. As λ_L is injcetive,

$$1_{\mathrm{End}_E(L)} = \lambda_L(1_A) = \sum \lambda_L(l_i)\lambda_L(a_i).$$

For any $\phi \in \mathrm{End}_E(L)$

$$\phi = \phi 1_{\mathrm{End}_E(L)} = \phi \sum \lambda_L(l_i)\lambda_L(a_i) = \sum \phi\lambda_L(l_i)\lambda_L(a_i) = \sum \lambda_L(\phi(l_i))\lambda_L(a_i)$$

$$= \lambda_L\left(\sum \phi(l_i)a_i\right).$$

Hence $\phi \in \lambda_L A$, that is λ_L is surjective, proving the lemma. □

Theorem 5.1.1 (Wedderburn's Theorem)**.** *Let A be a finite dimensional simple algebra over a field k. Then there is a division algebra D over k and an integer $n \geq 1$ such that $A \cong M_n(D)$. Moreover, this division ring D is uniquely determined up to isomorphism. We say that this division ring is the associated division ring of A.*

Proof. Let $L \subset A$ be any left ideal. For all $a \in k$ and all $x, y \in L$, $ax + y \in L$, that is L is a vector subspace of A. As A is a finite dimensional vector space, A is left Artinian, that is we can choose L to be minimal. Do so. By minimality, L is a simple left A-module. By Schur's lemma, $E := \mathrm{End}_A(L)$ is a division algebra over k. By Rieffel's lemma $A \cong \mathrm{End}_E(L)$. From the discussion and lemma preceding Schur's lemma, it follows that $A \cong \mathrm{End}_E(L) \cong M_n(E^o)$, where $n = \dim_E L$. As E is a $k-$algebra and L is a subspace of a finite dimensional k-vectorspace, $n < \infty$. The opposite ring of a division ring is clearly a division ring. Hence $D := E^o$ gives $A \cong M_n(D)$ where D is a division algebra over k, prvoving the first part of the theorem.

For uniqueness, assume $M_n(D) \cong A \cong M_m(E)$ where D and E are division algebras over k. By the structure of matrix rings discussed above, there is a minimal left ideal $L \subset A$ such that $D^n \cong L \cong E^m$. This isomorphism is in the category of A-modules, whence

$$\mathrm{End}_{M_n(D)}(D^n) \cong \mathrm{End}_A(D^n) \cong \mathrm{End}_A(L) \cong \mathrm{End}_A(E^m) \cong \mathrm{End}_A(E^m).$$

As the category of R-modules is Morita equivalent to the category of $M_n(R)$-modules for any ring R and any integer $n \geq 1$ by the functor mapping a R-module M to the $M_n(R)$-module M^n, we have that $\mathrm{End}_D(D) \cong \mathrm{End}_{M_n(D)}(D^n)$ and $\mathrm{End}_E(E) \cong \mathrm{End}_{M_m(D)}(E^m)$, see [2] (Proposition 9.5.2). But any D-linear endomorphism on D is completely determined by where it maps 1_D, whence $D \cong \mathrm{End}_D(D)$ and similarily for E. The chain of isomorphisms can now be completed to

$$D \cong \mathrm{End}_{M_n(D)}(D^n) \cong \mathrm{End}_A(D^n) \cong \mathrm{End}_A(L) \cong \mathrm{End}_A(E^m) \cong \mathrm{End}_A(E^m) \cong E.$$

This finnishes the proof of Wedderburn's theorem (as a isomorphic to b is a transative property). □

Corollary 5.1.1. *Let k be an algebraically closed field. Then every finite dimensional central simple algebra over k is isomorphic to $M_n(k)$ for some integer $n \geq 1$.*

Proof. By Wedderburn's theorem it is enough to show that any finite dimensional division ring over k is isomorphic to k. For this, assume $D \supseteq k$ is a finite dimensional division algebra central over k. Let $d \in D$ and consider the minimal algebra over k containing d, i.e. $k(d)$. As k contained in the center of D, $ad = da$ for all $a \in k$ and clearly $d^k d^l = d^l d^k$ for all integers k, l. As {1,d} can be extended to a finite dimensional basis for D (by it being finite dimensional over k), there is a maximal integer $l \geq 0$ such that $\{1, d, d^2, \ldots, d^l\}$ is linearily independent. Clearly $k(d)$ is a subspace of D and there is a $r \leq l$ such that $\{1, d, d^2, \ldots, d^r\}$ forms a basis for $k(d)$, but as this subalgebra of D has commutative multiplication i.e. is a field, and is finite dimensional, it is an algebraic extension of k. Hence $k(d) = k$, as k is algebraically closed, as this holds true for any $d \in D$, $D = k$. This finishes the proof. □

We summarise the results of this section together with a stronger version of the last corollary that we won't give the proof of (it is the middle two that we won't give a proof of here). You can find proofs of these statements in [6].

Theorem 5.1.2 (Characterization of Central simple algebras over k.)**.** *Let k be a field and A a finite dimensional k-algebra. The following are equivalent*

- *A is central over k and has no non trivial two sided ideals.*
- *If K is an algebraic closure of k, then $A \otimes_k K$ is isomorphic to a matrix algebra over K*
- *There is a finite Galois extension L of k such that $A \otimes_k L$ is isomorphic to a matrix algebra over L.*
- *There is a unique (up to isomorphism) division algebra D over k and an integer $n \geq 1$ such that $A \cong M_n(D)$.*

Any of the above can be used as a definition of central simple algebras over k.

6 Galois Cohomology

In this section we put together the results obtained above. We study group cohomology where the group is the Galois group of some field extension, Galois cohomology. The culmination of the theory in this section, as well as in this thesis, is the result that we can classify all central simple algebras over a field, and therefore all division algebras, by computing a cohomology group. This is the Brauer group of the field.

6.1 Basics and usefull examples

Throughout this section we suppose that K/k is a finite Galois extension with Galois group G. G acts naturally on K and K^* (the additive and multiplicative groups of K respectively) which gives us two examples of G-modules to study.

Proposition 6.1.1. *For all $n \in \mathbb{Z}_{\geq 1}$, $H^n(G, K) = 0$.*

Proof. By the normal basis theorem, see [7], there is a $\alpha \in K$ such that $\{s.\alpha\}_{s\in G}$ is a basis for K as a k vector space, whence $K \cong \mathbb{Z}G \otimes_k \alpha k$. That is K is an induced module (and as G is finite also coinduced), and hence cohomologicaly trivial. □

Proposition 6.1.2. $H^1(G, K^*) = 0$.

Proof. Suppose $s \mapsto a_s$ is a 1-cocycle of G taking values in K^*. Given $c \in K$, define

$$b(c) = \sum_{s\in G} a_s.s(c).$$

As the automorphisms are linearily independant over K (see [7] page 35), we can chose $c \in K^*$ such that $b := b(c) \neq 0$. Now we get that for any $h \in G$

$$h(b) = \sum_{s\in G} h(a_s).hs(c) = \sum_{s\in G} a_h^{-1}a_{hs}.hs(c)$$

$$= a_h^{-1} \sum_{s\in G} a_{hs}.hs(c) = a_h^{-1} \sum_{s\in G} a_s.s(c) = a_h^{-1}b$$

where we in the last equality used that hG just is a permutation of its elements, whence the sums are equal. From this we get that for all $h \in G$ $a_h = b.h(b)^{-1}$, that is, a_h is a coboundary and as a_h was an arbitrary cocycle, we get that $H^1(G, K^*) \cong \{0\}$, which we wanted to show. □

Proposition 6.1.3. $H^1(G, GL(n, K)) = \{1\}$.

Proof. Let $s \mapsto a_s$ be a 1-cocycle of G taking values in $\mathrm{GL}(n, K)$. For $x \in K^n \setminus \{0\}$, define

$$b(x) = \sum_{s\in G} a_s.s(x).$$

Now, suppose $u \in (K^n)^*$, the dual space of K^n, such that $u(b(x)) = 0$ for all $x \in K^n$. Then, for all $\gamma \in K$,

$$0 = u(b(\gamma x)) = u(\sum_{s\in G} a_s.s(\gamma x)) = \sum_{s\in G} u(a_s.s(\gamma)s(x)) = \sum_{s\in G} s(\gamma)u(a_s.s(x)).$$

If $u(a_s.s(x)) \neq 0$ for some $s \in G$ and some $x \in K^n$, this sets up a linear dependence of the automorphisms in G, hence by the linear independence of automorphisms of K/k over K, we get that $u(a_s.s(x)) = 0$ for all $s \in G$ and $x \in K^n$. As $a_s \in GL(n, K)$ and $s \in G$ they are both invertible, whence for all $x \in K^n$ $u(x) = 0$, proving $u = 0$. This shows that $\text{span}_K(b(K^n)) = K^n$, since every proper subspace is determined as the zero locus of one or more non zero linear forms and we just showed that there is no non zero linear form which has a zero locus containing $b(K^n)$.

Pick $x_1, \ldots, x_n \in K^n$ such that $y_i := b(x_i)$ forms a basis for K^n. Let c be the K-linear map taking the canonical basis elements e_i to x_i. We have by construction that $b \circ c(e_i) = y_i$ and in matrix representation (over standard basis where c acts by multiplication on the left) $c = \begin{pmatrix} x_1 & \ldots & x_n \end{pmatrix}$ and hence $b \circ c = \begin{pmatrix} y_1 & \ldots & y_n \end{pmatrix}$, that is, as the y_i forms a basis, $b \circ c$ is a invertible K-linear transformation.

For any $h \in G$

$$h(b(c)) = \sum_{s\in G} h(a_s).hs(c) = \sum_{s\in G} a_h^{-1}a_{hs}.hs(c) = a_h^{-1}\sum_{s\in G} a_{hs}.hs(c)$$
$$= a_h^{-1}\sum_{s\in G} a_s.s(c) = a_h^{-1}b(c),$$

by re-indexing, and as a_h and $b(c)$ are both invertible matrices, $a_s = b(c)s(b(c))^{-1}$ for all $s \in G$, and a_s is a coboundary, proving that $H^1(G, GL(n, K)) \cong \{1\}$. □

Corollary 6.1.1. $H^1(G, SL_n(K)) = \{1\}$

Proof. We have a short exact sequence

$$1 \longrightarrow \text{SL}_n(K) \longrightarrow \text{GL}_n(K) \xrightarrow{\det} K^* \longrightarrow 1$$

which after application of the functor $H^*(G, -)$ gives rise to the exact sequence (the long exact sequence, see non-Abelian cohomology above, together with the proposition we just proved)

$$1 \longrightarrow \text{SL}_n(K)^G \longrightarrow \text{GL}_n(K)^G \xrightarrow{\det} (K^*)^G \longrightarrow H^1(G, \text{SL}_n(K)) \longrightarrow 1$$

equivalently

$$1 \longrightarrow \text{SL}_n(k) \longrightarrow \text{GL}_n(k) \xrightarrow{\det} k^* \longrightarrow H^1(G, \text{SL}_n(K)) \longrightarrow 1$$

and as the determinant mapping from $\text{GL}_n(k)$ to k^* is surjective, exactness yields that $H^1(G, \text{SL}_n(K)) = \{1\}$. □

6.2 Descent

We will in this section introduce the concept of Galois descent, which informally can be described as an investigation into wheter two objects over k, not isomorphic, becomes isomorphic over K, where K is some Galois extension of k. It also encompasses the study of the isomorphism classes of some type of objects over k_s, the separable closure of k, but this part of the study will be dealt with in a later section, specifically in the study of the Brauer group of some field k, which is the set of classes of central simple algebras over k modulo isomorphism over some Galois extension of k. The goal of this section will be to introduce a cohomological interpretetation of descent.

Let V be k-vector space and $x \in \bigotimes^p V \otimes_k \bigotimes^q V^*$, i.e. a tensor of type (p, q). We say that two such pairs (V, x) and V', x' are k-isomorphic if there is a k-linear isomorphism $f : V \to V'$ such that $f(x) = x'$ (whence a necessary condition for two pairs to be k-isomorphic is that their tensors are of the same type).

Furthermore, let K/k be a finite Galois extension of k, define $V_K := V \otimes_k K$, i.e. V with scalars extended to K, $x_K := i(x)$ where i is the embedding $i : V \to V_K$ (or rather the induced map on the $(p, q)-$tensors over V). We say that (V, x) and V', x' are $K-$isomorphic if (V_K, x_K) and (V'_K, x'_K) are $K-$isomorphic (in the sense described for $k-$isomorphisms above).

Let $E_{(V,x)}(K/k)$ denote the set of k-isomorphism classes that are K-isomorphic to (V, x), we denote it just by $E(K/k)$ if the space-tensor pair is clear from context.

Let A_K be the group of K-automorphisms of (V_K, x_K). We define a action of $G(=$ Gal(K/k)) on A_K by first introducing an action on V_K, namely for any $s \in G$ and $x \otimes \lambda$ a basic tensor in V_K, let $s.(x \otimes \lambda) := x \otimes s(\lambda)$ and extend by linearity. Then if $f \in \mathrm{End}_K(V_K)$ define $s(f) := s \circ f \circ s^{-1}$.

Now, given a class $[(V', x')] \in E(K/k)$ and $f : V_K \to V'_K$ a K-isomorphism with $f(i(x)) = i(x')$, define for any $s \in G$

$$p_s := f^{-1} \circ s(f) = f^{-1} \circ s \circ f \circ s^{-1}.$$

Clearly this defines an automorphism of V_K and as $p_s(x \otimes 1) = x \otimes 1$, its extension to the tensor algebra on V_K maps x_K to x_K as this is a k-rational tensor and $f(x_K) = x'_K$ whence $p_s \in A_K$. Now given $s, h \in G$,

$$p_s \circ s(p_h) = f^{-1} \circ s \circ f \circ s^{-1} \circ s \circ p_h \circ s^{-1} = f^{-1} \circ s \circ f \circ s^{-1} \circ s \circ f^{-1} \circ h \circ f \circ h^{-1} \circ s^{-1} =$$

$$= f^{-1} \circ s \circ h \circ f \circ h^{-1} \circ s^{-1} = p_{sh}$$

proving that p_s is a 1-cocycle of G with values in A_K. To show that p_s is independent up to cohomology of which isomorphism from V_K to V'_K we choose, assume $f, g : V_K \to V'_K$ are two $K-$linear isomorphisms, we want to find $a \in A_K$ such that, denoting by p_s^f the cocycle induced by choosing f as isomorphism, $p_s^g = a^{-1} \circ p_s^f \circ s(s)$.

$$a^{-1} \circ p_s^f \circ s(a) = a^{-1} \circ p_s^f \circ s \circ a \circ s^{-1}$$

$$= a^{-1} \circ f^{-1} \circ s \circ f \circ s^{-1} \circ s \circ a \circ s^{-1} = a^{-1} \circ f^{-1} \circ s \circ f \circ a \circ s^{-1}$$

hence if we let $a = f^{-1} \circ g$, we get $p_s^g = a^{-1} \circ p_s^f \circ s(s)$, and as a is given by compostion of isomorphisms from V_K to V'_K back to V_K, $a \in A_K$, proving that, up to cohomology, the cocycle asigned to a class is independent on choice of isomorphism. Thus, passing to the quotient identifying cohomologous elements we get a well defined map

$$\theta : E(K/k) \to H^1(G, A_K).$$

Proposition 6.2.1. *The map θ defined above is a bijection.*

Proof. Suppose (V_1, x_1) and V_2, x_2 are $K-$isomorphic to (V, x) via f_1 and f_2 respectively, such that they correspond to cohomologous cocycles $p_s = f_1^{-1} s(f_1)$ and $q_s = f_2^{-1} s(f_2)$. Then there is a $a \in A_K$ such that

$$f_1^{-1} s(f_1) = a^{-1} f_2^{-1} s(f_2) s(a) = (f_2 \circ a)^{-1} s(f_2 \circ a)$$

whence $s(f_2 \circ a \circ f_1^{-1}) = f_2 \circ a \circ f_1^{-1}$, that is, the map $f := f_2 \circ a \circ f_1^{-1}$ is $G-$invariant and restricts to a $k-$isomorphism of (V_1, x_1) onto (V_2, x_2), proving that if two pairs map to the same cohomology class, then they are contained in the same $k-$isomorphism class, which proves that θ is injective.

Now, let p_s be a $1-$cocycle of G with values in A_K. As any $K-$automorphism of (V_K, x_K) in particular is a $K-$linear automorphism of V_K, we get that $A_K \subset \mathrm{GL}(V_K)$. Hence as $H^1(G, \mathrm{GL}(V_K)) \cong \{e\}$, p_s is a coboudary when we consider coefficients in $GL(V_K)$. Hence there is a $f \in GL(V_K)$ such that

$$p_s = f^{-1} \circ s(f)$$

for all $s \in G$. We extend f to the tensor algebra over V_K, and consider the action of G on the element $x' = f(x)$. We compute, given $s \in G$, keeping in mind that x is $k-$rational and hence invariant under our action and that $f \circ p_s = s \circ f \circ s^{-1} = s(x)$,

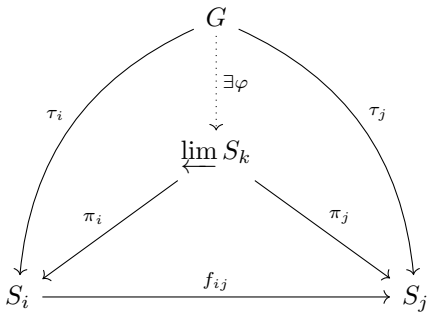
$$s(x') = s(f)(s(x)) = s(f)(x) = f \circ p_s(x) = f(x) = x'$$

which proves that x' is invariant under the action of G and hence $k-$rational. It follows that (V, x') defines a class of $E(K/k)$, and this class will under θ be mapped to the cohomology class containing $f^{-1} s(f) = p_s$, proving that θ is surjective. □

6.3 Infinite Galois extensions & profinite groups

We recall briefly that a inverse system is a set of objects in a category indexed by some partially ordered set with morphisms from an object to another whenever the first objects index is greater than or equal to the second ones, with the identity from object i to object i. Given an inverse system $\{S_i, f_{ij}\}_{i,j \in I}$ we denote by $\varprojlim S_i$ the (up to isomorphism) unique object (given it exists in the category) together with morphisms $\pi_i : \varprojlim S_k \to S_i$ with the universal property

that the following diagram commutes for all G such that there are $\tau_i : G \to S_i$ commuting with the maps from the inverse system:



For a more detailed survey on inverse/projective limits, see [8], [9] or [2].

The notion of direct limits is the dual of projective limits, i.e. its universal property is obtained by reversing the arrows in the above diagram.

We denote by k_s the separable closure of the field k, this is the subfield of the algebraic closure of k containing all elements separable over k, so when k is a perfect field, which it is in all the cases we will consider, k_s is the algebraic closure of k. As such $k_s = \bigcup L_i/k$ where L_i/k is a finite Galois extension, furthermore the L_is are partially ordered by inclusions of subextensions into bigger extensions. From the Galois correspondence (see [7] or [3]) we get that $\{\mathrm{Gal}(L_i, k)\}_{k \subset L_i, [L_i,k] < \infty}$ forms an inverse system with every morphism surjective (every automorphism of a subfield has at least one extension to the bigger field) and we can consider $\varprojlim \mathrm{Gal}(L_i/k)$. We have the following result due to Krull

Theorem 6.3.1 (Krull's Theorem)**.** *The Galois group $Gal(k_s/k)$ of all field automorphisms of k_s fixing k is isomorphic to $\varprojlim Gal(L_i/k)$, where the limit is taken over all finite Galois extensions of k.*

Proof. As every L_i is a splitting field over k, we have that any automorphism α of K_s restricts to a unique automorphism α_i of L_i, furthermore, the restriction mapings $\mathrm{Gal}(k_s/k) \to \mathrm{Gal}(L_i/k)$ are compatible with the maps between the L_is, as these are just further restrictions. Hence we get, by the universal property of $\varprojlim \mathrm{Gal}(L_i/k)$, a group homomorphism

$$\phi : \mathrm{Gal}(k_s/k) \to \varprojlim \mathrm{Gal}(L_i/k) \subset \prod \mathrm{Gal}(L_i/k).$$

Suppose α isn't the identity automorphism of k_s, then there is a $x \in k_s$ such that $\alpha(x) \neq x$, and we have an L_i being the splitting field of x on which α isn't the identity either, hence $\phi(\alpha) \neq 1$, showing that ϕ is injective.

Given $(\alpha_i)_I \in \varprojlim \mathrm{Gal}(L_i/k)$, we define $\alpha \in \mathrm{Gal}(k_s/k)$ by, for any $x \in k_s$, pick any finite Galois extension $L_i \ni x$ and let $\alpha(x) = \alpha_i(x)$. As $(\alpha_i)_i \in \varprojlim \mathrm{Gal}(L_i/k)$, it is compatible with the maps between finite extensions and $\alpha(x)$ is independent of the choice of L_i and as any $x, y \in k_s$ lie in some L_i, this is indeed an automorphism of k_s, which fixes k and by construction $\phi(\alpha) = (\alpha_i)_i$, proving surjectivity and the proof is complete. □

We say that a set is profinite if it is the projective limit of a familly of finite sets, and profinite objects in other concrete categories are the objects that are limits of objects whose underlying sets are finite. We can endow $\mathrm{Gal}(k_s/k)$ with a natural topology, namely by giving each finite group the discrete topology, viewing $\mathrm{Gal}(k_s/k)$ as a subspace of the product topology, which is closed, and as the product is over compact Hausdorff spaces, Tychonoffs theorem yields that $\mathrm{Gal}(k_s/k)$ is a compact Hausdorff space as well. It is also totally disconnected, as any profinite topological space is, and homeomorphic to a subspace of the Cantor set. We will not pursue this line of investigation further, but the interested reader may look into [8] and/or [2] for more details. It can be shown that the profinite topology on a profinite group coincides with the topology generated by taking as a basis the family of finite index normal subgroups of the profinite group G.

We will now give a few statements without proof, some of which can be found in exercises of [2], and others as propositions in the same book.

Lemma 6.3.1. *If G is a profinite group, let $\mathcal{U}$ be the partially ordered set of open normal subgroups U of G. Then $\mathcal{U}$ forms a fundamental system of neighbourhoods of e, the identity of G, each G/U is a finite group and $G \cong \varprojlim G/U$.*

Proof. See [2] lemma 6.11.7, page 209. □

Definition 6.3.1. *We say that a G-module A is a discrete G-module if it is endowed with the discrete topology and the G-action on A is continuous as a function from $G \times A$ with the product topology to A.*

Proposition 6.3.1. *The following are equivalent;*

- *A is a discrete G-module*
- *for every $a \in A$ the set $\{s \in G : s(a) = a\}$ is an open subgroup of G*
- *$A = \bigcup A^U$, where U runs through open normal subgroups of G.*

Proposition 6.3.2. *The category C_G of discrete G-modules is an Abelian category with an exact inclusion into G-mod. Furthermore, for all discrete G-modules A and G-modules B,*

$$Hom_G(A, B) = Hom_G(A, \bigcup B^U)$$

where U runs through open normal subgroups of G. That is $C_G \subset G-mod$ has $\bigcup(-)^U$ as a right adjoint.

Definition 6.3.2. *We say that a category has enough injectives if there is a monomorphism into an injective object from every object in the category.*

This is a usefull concept as for any object in a Abelian category with enough injectives, there is a injective resolution. This allow means that the right derived

functor of the Hom functor is well defined for all objects in the category.

Lemma 6.3.2. *The Abelian category C_G has enough injectives.*

Proof. As the category of $\mathbb{Z}G$-modules has enough injectives, we may embed any discrete G-module A in an injective G-module I. By the proposition above, $A \subseteq \bigcup I^U \subseteq I$. As $\bigcup(-)^U$ is rightadjoint to the exact functor $C_G \subset G$-mod, it preserves injectives (proposition 2.3.10 [2]). Hence $\bigcup I^U$ is injective in the category of discrete $G-$modules, proving that this category has enough injectives. □

Definition 6.3.3. *If A is a discrete G-module, let $C^n(G, A)$ be the set of continuous maps from $G^n \to A$.*

These sets are made into Abelian groups by pointwise addition. They are in fact, subgroups of the groups of cochains defined in ordinary group cohomology above. We define d to be the boundary map we defined above in i $G-$mod restricted to continuous cochains, and as the action of g and addition in A are continuous, this restriction maps continuous cochains to continuous cochains, as can be seen by looking at its explicit formula which indeed uses only $G-$action and addition.

Lemma 6.3.3. *Any map from a topological space into a discrete space is continuous if, and only if it is locally constant.*

Proof. Suppose $f : X \to Y$ is a map between topological spaces where Y is equiped with the discrete topology. If f is locally constant, for all $x \in X$ there is a open subset U_x such that $f(U_x) = \{f(x)\}$. We clearly have that $f^{-1}(y) = \bigcup_{x \in f^{-1}(y)} U_x$, where U_x is as above. Hence the preimage of any point in Y is the union of open sets and thence open. As Y is discrete, its singeltons form a basis, proving that f is continuous.

Conversely, suppose f is continuous, then in particular, as Y is discrete, $f^{-1}(f(x))$ is open for all $x \in X$. This is a open neighbourhood of x on which f is constant, proving the lemma. □

Lemma 6.3.4. *If G is profinite, then the functor $C^n(G, -)$ is exact.*

Proof. Let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

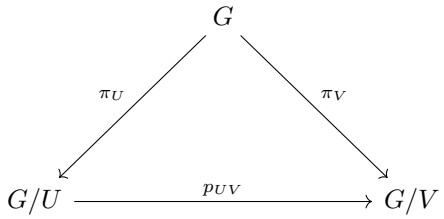
be a short exact sequence of discrete G-modules. Suppose $\phi : G^n \to A$ is a continuous map such that $f \circ \phi = 0$. As f is injective, this means that $\phi = 0$, proving exactness at A. Suppose $\psi : G^n \to B$ is a continuous map such that $g \circ \psi = 0$. We get that $\psi(G^n) \subset \ker g = \mathrm{im} f$, and as A, B, C are discrete, the map $\psi' : G^n \to A$ defined by $\psi'(g) = f^{-1}(\psi(G))$ is continuous and $f \circ \psi' = \psi$, proving exactness at B. Finally, suppose $\alpha : G^n \to C$ is a continuous map, and θ some section of g. As B and C are discrete, θ is continuous, and as continuity is preserved by composition, $\theta \circ \alpha : G^n \to B$ is a continuous map with $g \circ \theta \circ \alpha = \alpha$, proving exactness at C. □

Lemma 6.3.5. *If G is a profinite group and A a discrete G-module, then*

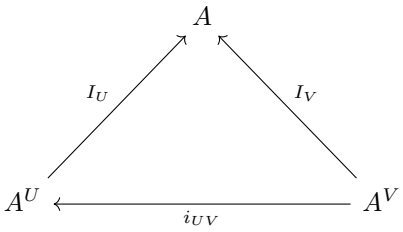
$$C^n(G,U) = \varinjlim C^n(G/U, A^U)$$

where U runs through open normal subgroups.

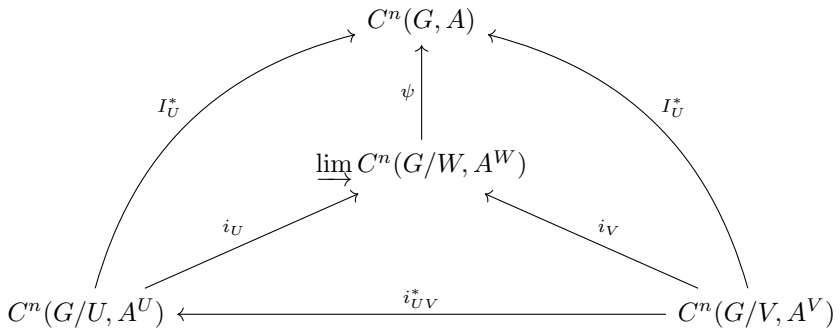
Proof. Fix an integer $n \geq 0$. If G is finite, then it has the discrete topology and $\{e\}$ is a open normal subgroup whence the identity is obvious, assume therefore that G is infinite. Let U, V be two normal open subgroups of G with U contained in V. We get that $A^V \hookrightarrow A^U$. By Lemma 6.11.7 [2], $G \cong \varprojlim G/W$ where W runs through the open normal subgroups of G. Hence we get the following diagrams



and



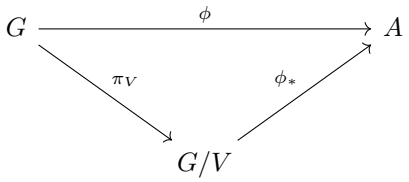
where all maps are continuous as the modules are discrete and the maps between G and its quotients are continuous by the definition of the profinite topolgy. For breivety, we will denote the projections from G^n to G/U^n and G/U^n to G/V^n simply by π_U instead of π_U^n and p_{UV} instead of p_{UV}^n. Suppose we have $\phi \in C^n(G/V, A^V)$, then as the composition of linear maps is continuous,$i_{UV} \circ \phi \circ p_{UV} \in C^n$ and $I_U \circ \phi \circ \pi_U \in C^n(G,A)$. Hence we have natural homomorphisms $i_{UV}^* : C^n(G/V, A^V) \to C^n(G/U, A^U)$ for all open normal subgroups $U \subset V$ and $I_V^* : C^n(G/V, A^V) \to C^n(G,A)$ for all open normal subgroups V. Hence, by the universal property of the direct limit, there is homomorphism $\psi : \varinjlim C^n(G/W, A^W) \to C^n(G,A)$ such that the diagram



commutes.

Suppose $f \in \varinjlim C^n(G/W, A^W)$ such that $\psi(f) = 0$, then by the commutativity of diargram above, if $i_U(\overline{f}) = f$, $0 = I_U^*(\overline{f})) = I_U \circ \overline{f} \circ \pi_U$. As I_U is injective, $\overline{f} \circ \pi_U = 0$, and as π_U is surjective $\overline{f} = 0$. This shows that $f = 0$ as i_U is a homomorphism, and if f wasn't in the image of any i_U, it wouldn't be an element in the direct limit by minimality.

Suppose $\phi \in C^n(G, A)$, as G is a profinite group, it is compact and as A is a discrete space, $\phi(G)$ is finite by continuity. As ϕ is continuous, $\phi^{-1}(a)$ is open for all $a \in A$, hence all points in it are inner. By lemma 6.11.7 [2], the normal open subgroups of G is a fundamental system of neighbourhoods of the identity e. Hence, for all $s \in \phi^{-1}(a)$, if $a \in \phi(G)$, there is a open normal subgroup U_s such that $sU_s \subset \phi^{-1}(a)$. Pick one such neighbourhood for every $s \in G$, i.e. $sU_s \subset \phi^{-1}(\phi(s))$, these sets form an open cover of G. As G is compact, there is a finite subcover $\{s_j U_{s_j}\}_{j=1}^n$. The intersection $\bigcap_j^n U_{s_j}$ is nonempty as it contains e and open as finite intersections of open sets are open. Using again that the open normal subgroups forms a fundamental system of neighbourhoods of e, we can pick a subset $V \subset \bigcap_j^n U_{s_j}$, that is a open normal subgroup. Now, for any $g \in G$, $g \in s_j U_{s_j}$ for some $j \in \{1, \dots, n\}$, and $V \subset U_{s_j}$ by construction. Also, as V is open and normal, it is one of the subgroups that our limit runs through. Hence $gV \subset s_j U_{s_j} \subset \phi^{-1}(\phi(g))$, that is ϕ is constant on the cosets of V and therefore the diagram



commutes, or equivalently ϕ is completely determined by ϕ_*. Now, $I_V^*(\phi_*) = I_V \circ \phi_* \circ \pi_V = \phi$, hence by the construction of ψ, $\psi(i_V(\phi_*)) = \phi$, proving that ψ is also surjective, finnishing the proof of the lemma. □

Theorem 6.3.2. *Let G be a profinite group and A a discrete G-module. Then*

$$H^q(G, A) \cong H^q(C(G, A)) \cong \varinjlim H^q(G/U, A^U)$$

where U runs through the open normal subgroups of G.

Proof. Let us, following Weibel, use the notation $T^n(A) := H^q(C(G, A))$. First, we calculate

$$T^0(A) = \ker(d : A \to C^1(G, A)) = \{a \in A | (\forall s \in G)\ 0 = (da)(g) = ga - a\} = A^G.$$

We showed above that $C^q(G, A) = \varinjlim C^q(G/U, A^U)$, and by theorem 2.6.15 [2], direct limits of Abelian groups is an exact functor from direct systems of Abelian groups to Abelian groups, hence the exact sequence, considered for all U open and normal subgroups in G

$$0 \longrightarrow C^n(G/U) \xrightarrow{d_n} \ker d_{n+1} \longrightarrow H^n(C^n(G/U, A^U)) \longrightarrow 0$$

is preserved, whence direct limits commutes with cohomology. Hence $T^n(A) \cong \varinjlim H^n(G/U, A)$.

As we showed above, if $0 \to A \to B \to C \to 0$ is an exact sequence of discrete $G-$modules, then the sequence

$$0 \longrightarrow C^n(G, A) \longrightarrow C^n(G, B) \longrightarrow C^n(G, C) \longrightarrow 0$$

is exact. Hence, by proposition 1.3.4 [2], we get a long exact sequence in cohomology with connecting homomorphism $\delta^n : T^n(C) \to T^{n+1}(A)$, whence T^n is a cohomological delta functor from discrete G-modules to Abelian groups. Suppose $I \in C_G$ is a injective discrete G-module. If U is an open normal subgroup of G, then I^U is an injective object in the category of G/U-modules, as $-^U$ is right adjoint to the forgetfull functor from G/U-modules to G-modules, lemma 6.8.1 in [2] and right adjoints preserves injectivity, proposition 2.3.10 [2]. Hence, as injective G/U-modules in particular are relatively injective,

$$T^n(I) = \varinjlim H^n(G/U, A^U) = 0.$$

As $T^0(A) = H^0(G, A) = A^G$, and C_G has enough injectives, we conclude by induction through dimension shifting that $H^q(G, A) \cong H^q(C(G, A))$, which is what we wanted to show. □

6.4 The cohomological Brauer group

Let us for shorthand use the notation $H^q(K/k) := H^q(\mathrm{Gal}(K/k), K^*)$ where K is a Galois extension of the field k, as this will be our main object of study from now on. We will show that these groups depend functorially on the pair (K, k). We recall that any ring homomorphism of fields by necessity is a injective or a triviall one, this is because the kernel of any ring homomorphism will be an ideal, and any field only has the field itself and 0 as ideals. Hence the only morphisms we need to consider is injective ones (cohomology with coefficients in 0 is necessarily trivial as there is only one map from S to 0, even in the category of sets). Suppose K/k is a Galois extension with group G, k'/k an extension and K'/k' a Galois extension with group G'. Let $f : K \to K'$ be a $k$linear injection, we define $\overline{f} : G' \to G$ by $s' \mapsto s$ where s is the unique element in G such that $s' \circ f = f \circ s$. Uniqueness follows from $f \circ s = f \circ g$ implying $f(x) = f(gs^{-1}.x)$ for all $x \in K$, and as f is an injection $x = gs^{-1}.x$, whence $gs^{-1} = 1_G$ and $s = g$. Given $a \in K$, we get $f(\overline{(f)}(s').a) = f(s(a)) = f \circ s(a) = s' \circ f(a) = s'.f(a)$, and the maps are compattible in the sense of section 2.5. Hence we get an induced map in cohomology

$$f_q : H^q(K/k) \to H^q(K'/k').$$

Proposition 6.4.1. *The map f_q is independent of the choice of injection from K to K'.*

Proof. We first recall that any Galois extension is a splitting field of some polynomial, and as splitting fields contained in a bigger field are unique, given $f, g : K \to K'$ two k-embeddings, they have the same image, that is $f(K) = g(K)$.

It follows that $h = g|^{-1}_{f(K)} \circ f$ defines an element in G, and clearly $g \circ h = f$. Hence $f \circ h^{-1} \circ \overline{g}(s) \circ h = g \circ \overline{g}(s) \circ h = s \circ g \circ h = s \circ f$ and by the definition, $\overline{f}(s) = h^{-1} \circ \overline{g}(s) \circ h$.

Applying this on the map induced by $f, \overline{f}$ on cocycles, say ψ an q-cocycle, we get (denoting by f_q also the map between cocycles before passing to the quotient, a slight but practical abuse of notation), letting $c^q_h((s_i)_i) = (h^{-1})^q \circ (s_i)_i \circ (h)^q$

$$f_q(\psi) = f \circ \psi \circ \overline{f}^q = g \circ h \circ \psi \circ c^q_h \circ \overline{g}^q.$$

But $c_h : G \to G$ defined by $s \mapsto h^{-1}sh$ is compatible with the map $K \to K$ defined by $a \mapsto ha$ and this pair extends in cocycles to

$$\sigma : H^q(K/k) \to H^q(K/k)$$

defined by

$$\psi \mapsto \sigma(\psi) = h \circ \psi \circ c^q_h.$$

Hence we get the following commutative diagram:

$$\begin{array}{ccc} H^q(K/k) & \xrightarrow{\sigma} & H^q(K/k) \\ & \searrow^{f_q} & \downarrow{\scriptstyle g_q} \\ & & H^q(K'/k') \end{array}$$

that is $f_q = g_q \circ \sigma_h$ and using that after taking quotints to get the actuall maps in cohomology, σ_h is the identity (as inner automorphisms induces identity in cohomology, see proposition 2.4.1), whence $f_q = g_q$ in cohomology, proving the desired independence of choice of embedding. □

The above propostion in particular yields that if $k \cong k'$ and $K \cong K'$, then $H^q(K/k) \cong H^q(K'/k')$, where the isomorphism is canonical, namely the one constructed above with the obvious inverse.

The proposition also applies for k_s/k, that is the cohomology is independent of what particular realisation (as a set) we choose for the separable closure of k, whence we are justified in denoting $H^q(\ /k) := H^q(k_s/k)$.

The propostion above also yields that these groups depend functorially on k, as $f : k \hookrightarrow k'$ gives a map $f_q : H^q(\ /k) \to H^q(\ /k')$, and all non trivial field maps are embeddings as mentioned above.

As $H^q(\ /k) \cong \varinjlim H^q(K/k)$ where K runs through all finite Galois extensions of k, proposition 6.1.2 yields that $H^1(\ /k) = \{e\}$. We will call $B_k := H^2(\ /k)$ the (cohomological) Brauer group of k.

Proposition 6.4.2. *Let L/k be a finite Galois extension containing the Galois extension K/k. Then there is an exact sequence*

$$0 \longrightarrow H^2(K/k) \longrightarrow H^2(L/k) \longrightarrow H^2(L/K)\ .$$

Proof. To prove this, let $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$, whence by the Galois correspondence (of finite extensions), $G/H \cong \mathrm{Gal}(K/k)$. As $H^1(H, L^*) = 0$, it follows from the exact sequence relating restriction to inflation that the following sequence is exact

$$0 \longrightarrow H^2(G/H, K^*) \xrightarrow{\inf} H^2(G, L^*) \xrightarrow{\mathrm{res}} H^2(H, L^*)$$

which is the same sequence as in the proposition by the Galois correspondence, proving the proposition. □

By passing to the limit over L, we get the following

Corollary 6.4.1. *There is an exact sequence*

$$0 \longrightarrow H^2(K/k) \longrightarrow B_k \longrightarrow B_K.$$

By passing to the limit over K (and $L \supseteq K$) the proposition and corollary above still holds for infinite Galois extensions.

We say that an element $a \in B_k$ is split by K if $a \in \ker(B_k \to B_K)$, which, if K/k is Galois amounts to $a \in H^2(K/k) \leq B_k$ by the corollary above.

6.5 The classical Brauer group

We say that two central simple algebras are equivalent if their associated division rings are isomorphic. When the two algebras have the same dimension this amounts to saying that they are k-isomorphic in the sense of the section on Galois descent.

Denote by A_k the set of equivalence classes of central simple algebras over k under the relation just described. We define a binary operation on A_k

$$\otimes : A_k \times A_k \to A_k$$

by

$$[A] \otimes [B] = [A \otimes B].$$

To see that this is a well defined operation, we first show

Lemma 6.5.1. *If k is a field, then $M_n(k) \otimes_k M_m(k) \cong M_{nm}(k)$.*

Proof. As $M_l(k) \cong \mathrm{End}_k(k^l)$, we work on endomorphism rings. Let $\phi \in \mathrm{End}_k(k^n)$ and $\psi \in \mathrm{End}_k(k^m)$. We note that $k^n \otimes_k k^m \cong k^{nm}$, composing with this isomorhism $\phi \otimes \psi$ defines an element in $\mathrm{End}_k(k^{nm})$. This defines an injective algebra homomorphism $\mathrm{End}_k(k^n) \otimes \mathrm{End}_k(k^m) \to \mathrm{End}_k(k^{nm})$, and as the spaces are finite dimensional over k it also surjective. In conclusion

$$M_n(k) \otimes_k M_m(k) \cong \mathrm{End}_k(k^n) \otimes \mathrm{End}_k(k^m) \cong \mathrm{End}_k(k^{nm}) \cong M_{nm}(k).$$

□

Now considering the isomorphism $(A \otimes_k K) \otimes_K (B \otimes_k K) \cong (A \otimes_k B) \otimes_k K$, the third equivalent characterization of a central simple algebra over k gives that $A \otimes_k B$ is a central simple algebra, and by passage to the quotient we get our operation on A_k. In conclusion, the above defined opereation on A_k is well defined, and we also get that it is commutative. Hence A_k is an Abelian group, this is the classical Brauer group of k.

A_k is in fact a covariant functor of k. We see this by noting that if K is an extension of k, extension of scalars to K defines a homomorphism

$$A_k \to A_K$$

by $[B] \mapsto [B \otimes_k K]$.

Denote by $A(K/k)$ the kernel of this homomorphism, which by definition consits of all the classes of algebras whose extension by scalars are isomorphic to a matrix algebra over K. If K is a algebraic closure of k, $A_k = A(K/k)$. Hence A_k is the union of $A(K/k)$ where K runs through all finite (Galois by the characterization) extensions of k. Let $A(n, K/k) \subset A_k$ denote the subset of classes containing a algebra A such that $A \otimes_k K \cong M_n(k)$. By the characterization, $A(K/k) \cong \bigcup_{n=1}^{\infty} A(n, K/k)$.

We can describe an element in $A(n, K/k)$ as a pair V, x where V is a n^2-dimensional vector space over k and x is a $(1,2)-$tensor describing the multiplication in A, where (V, x) is K-isomorphic to the standard pair describing $M_n(k)$. That multiplication in a $k-$algebra can be viewed as a $(1,2)-$tensor can be seen for example in the classical matrix multiplication by the formula

$$(a_{ij})(b_{jl}) = \sum_{i,l} E_{il} \sum a_{ij} b_{jl}$$

which is described by the $(1,2)$-tensor over $M_n(k)$ (vieved as a vectorspace)

$$\sum_{i,j,k} E_{ij} \otimes E_{ij}^* \otimes E_{jl}^*.$$

In general this comes from the isomorphism $V^* \otimes_k V^* \otimes_k V \to \mathrm{Hom}_k(V \times V, V)$ defined by $v^* \otimes w^* \otimes x \mapsto ((v_1, v_2) \mapsto v^*(v_1) w^*(v_2) x)$. If $v^*(v_1) w^*(v_2) x = 0$ for all $(v_1, v_2) \in V \times V$, then either v^*, w^* or x is 0 and hence $v^* \otimes w^* \otimes x = 0$, by linearity this proves injectivity. As the spaces are finite dimensional, of the same dimension, the map is also surjective. As every algebra product is given by a bilinear map $A \times A \to A$, the multiplication is indeed described by a $(1,2)$ tensor.

Let C_K^n denote the group of K-automorphisms of $M_n(K)$ and $G := \mathrm{Gal}(K/k)$. Using descent as described on the section with the same title, we get that the map

$$\theta : A(n, K/k) \to H^1(G, C_K^n)$$

is a bijection.

Lemma 6.5.2. $C_K^n \cong PGL_n(K)$.

This proof is due to Peter Semrl [10].

Proof. Let $\psi \in C_K^n$ and $u, y \in K^n \setminus \{0\}$. As ψ is injective, there is a $z \in K^n$ such that $\psi(uy^t)z \neq 0$ (matrix multiplication). Define the map $T : K^n \to K^n$ by $T(x) = \psi(xy^t)z$, as ψ is linear, so is T. As $Tu \neq 0$, T isn't the zero map. Now, pick any $A \in M_n(K)$ and $x \in K^n$. We compute

$$T(Ax) = \psi(Axy^t)z = \psi(A \cdot xy^t)z$$

where $\cdot$ denotes the product in $M_n(K)$. As $\psi \in C_K^n$,

$$\psi(A \cdot xy^t)z = \psi(A)\psi(xy^t)z = \psi(A)T(x).$$

Hence

$$TA = \psi(A)T.$$

Let $w \in K^n$. As $Tu \neq 0$, and because ψ is surjective, there is a $B \in M_n(K)$ such that $TBu = \psi(B)Tu = w$. As $Bu \in K^n$, this shows that T is surjective, and as K^n finite dimensional, all surjective endomorphisms are injective. Hence T is invertible. It follows that

$$\psi(A) = TAT^{-1}$$

that is every automorphism in C_K^n is inner. As $\lambda TA(\lambda T)^{-1} = TAT^{-1}$ for all $\lambda \in K^\times$, $C_K^n \cong GL_n(K)/K^\times \cong PSL_n(K)$, proving the lemma. □

We summarize:

Proposition 6.5.1. *There is a canonical bijection*

$$\theta : A(n, K/k) \to H^1(G, PGL_n(K)).$$

From the exact sequence

$$1 \longrightarrow K^\times \longrightarrow \mathrm{GL}_n(K) \longrightarrow \mathrm{PGL}_n(K) \longrightarrow 1$$

we get the coboundary map (see non-Abelian cohomology)

$$\Delta_n : H^1(G, PGL_n(K)) \to H^2(G, K) = H^2(K/k).$$

Define

$$\delta_n : A(n, K/k) \to H^2(K/k)$$

by

$$\delta_n = \Delta_n \circ \theta.$$

Define $\delta : A(K/k) \to H^2(K/k)$ by for $[C] \in A(K/k)$ choosing a representative C with $C \otimes_k K \cong M_n(K)$ and let $\delta([C]) = \delta_n([C])$.

Lemma 6.5.3. *δ is a injective well defined group homomorphism.*

Proof. Suppose C is a representative of $[C] \in A(n, K/k)$ with $f : C \otimes_k K \to M_n(K)$ an K-isomorphism and C' is a representative of $[C'] \in A(m, K/k)$ with $g : C' \otimes_k K \to M_m(K)$ a $K-$isomorphism. We get that

$$f \otimes g : (C \otimes_k C') \otimes_k K \cong (C \otimes_k K) \otimes_K (C' \otimes_k K) \to M_n(K) \otimes_K M_m(K)$$

is a K-isomorphism. And as the map $(a_{ij})_{ij} \otimes (b_{kl})_{kl} \mapsto (a_{ij}(b_{kl})_{kl})_{ij}$ (block matrix) is injective (if image zero, one of the matrices in the tensor product is zero, hence also the tensor), $M_n(K) \otimes_K M_m(K) \cong M_{nm}(K)$, by both spaces having the same finite dimension. So $f \otimes g$ defines (under last identification) a K-isomorphism from $C_K \otimes_K C'_K$ to $M_{nm}(K)$.

By the definition of θ (see Descent), we have (using brackets to denote the cohomology class of an element, when enclosing a cocycle)

$$[p_s] = \theta([C]) = [f^{-1} \circ s \circ f \circ s^{-1}],$$

$$[p'_s] = \theta([C']) = [g^{-1} \circ s \circ g \circ s^{-1}]$$

and

$$\theta([C \otimes_k C']) = [f^{-1} \otimes g^{-1} \circ s \circ f \otimes g \circ s^{-1}] = [p_s \otimes p'_s].$$

The sequence

$$1 \longrightarrow K^\times \xrightarrow{i} \mathrm{GL}_n(K) \xrightarrow{p} \mathrm{PGL}_n(K) \longrightarrow 1$$

is exact. We can hence pick b_s and b'_s such that $pb_s = p_s$ and $pb'_s = p'_s$ whence $p(b_s \otimes b'_s) = [p_s \otimes p'_s]$. By the definition of the coboundary map $\Delta_l : H^1(G, \mathrm{PGL}_n(K)) \to H^2(K/k)$ (see non-Abelian cohomology),

$$\delta_n([C]) = [a_{s,t}] := [i^{-1}(b_s.s(b_t).b_{st}^{-1})],$$

and

$$\delta_m([C']) = [a'_{s,t}] := [i^{-1}(b'_s.s(b'_t).b'^{-1}_{st})],$$

whence

$$\delta_{nm}([C \otimes C']) = [i^{-1}\left(i(a_{s,t}) \otimes i(a'_{s,t})\right)]\,.$$

As $i(a_{s,t})$ and $i(a'_{s,t})$ are central in $GL_n(K)$ and $GL_m(K)$ respectively they are of the form $a_{s,t}\mathrm{Id}$ and $a'_{s,t}\mathrm{Id}$ where Id are the respective identity matrices. It follows that $i(a_{s,t}) \otimes i(a'_{s,t}) = a_{s,t}a'_{s,t}\mathrm{Id}_{\mathrm{GL}_{nm}(K)}$, whence

$$\delta_{nm}([C \otimes C']) = [a_{s,t}a'_{s,t}] = \delta_n([C])\delta_m([C']),$$

that is, assuming δ is well defined, δ is a group homomorphism.

For any given n, $\delta_n([C]) = 1$ if, and only if $C \cong M_n(k)$, this follows from the exact sequence

$$1 \longrightarrow K^\times \xrightarrow{i} \mathrm{GL}_n(K) \xrightarrow{p} \mathrm{PGL}_n(K) \longrightarrow 1$$

and the associated long excact cohomology sequence, as $H^1(G, \mathrm{GL}_n(K)) = \{1\}$, whence δ_n is injective.

To prove that δ is well defined, suppose $C, C' \in [C]$ such that $C \cong M_n(D)$ and $C' \cong M_m(D)$, where D is the division algebra of $[C]$. Now, as $A(K/k)$ is a group, there is a A with $A_K \cong M_l(K)$ such that $C \otimes_k A, C' \otimes_k A \in [k]$, $[A] \otimes [C] = [k]$ if one of the containments are true. As we proved that δ_n is injective for all $n \in \mathbb{Z}_{\geq 1}$ and as $\delta_n(x)\delta_m(y) = \delta_{nm}(xy)$ we have

$$\delta_n([C])\delta_l([A]) = \delta([C \otimes A]) = 1$$

and

$$\delta_m([C'])\delta_l([A]) = \delta([C \otimes A]) = 1$$

whence, by multiplying with the inverse of $\delta_m(C')\delta_l([A])$, we have

$$1 = \delta_n(C)\delta_m(C')^{-1} = \delta_{nm}([C][C']^{-1})$$

proving that $\delta([C])$ is independent of our choice of representatve and $\delta : A(K/k) \to H^2(K/k)$ is indeed a well defined injective homomorphism. □

Lemma 6.5.4. *If $n = [K : k]$, the map $\delta_n : A(n, K/k) \to H^2(K/k)$ is surjective.*

Proof. As θ is bijective, we only need to show that $\Delta_n : H^1(G, \mathrm{PGL}_n(K)) \to H^2(K/k)$ is surjective. by the definition of Δ_n, this is equivalent to showing that any 2-cocycle $a_{s,t}$ of G with values in K^* can be realized as

$$a_{s,t} = p_s s(p_t) p_{st}^{-1}, \text{ where } p_s \in \mathrm{GL}_n(K).$$

Let $V = \mathrm{span}_K(e_s)_{s \in G}$ (the free K-module with basis indexed by G, which of course is a vector space as K is a field). Let $p_s \in \mathrm{End}_K(V)$ be defined by $e_t \mapsto p_s(e_t) = a_{s,t}e_{st}$. As p_s maps the basis to a basis, it is an automorphism, hence in $\mathrm{GL}_n(K)$ as $n = [K : k] = |G|$ (by the extension being Galois). Then we have, by a computation using the definitions of the maps, cocycles and the group action

$$p_s s(p_t)(e_u) = a_{s,tu} s(a_{t,u}) e_{stu}$$

and

$$a_{s,t} p_{st}(e_u) = a_{s,t} a_{st,u} e_{stu}.$$

This togheter with the cocycle condition

$$s(a_{t,u}) a_{s,tu} = a_{st,u} a_{s,t}$$

and $K^\times$ being Abelian, gives us

$$a_{s,t} a_{st,u} = a_{s,tu} s(a_{t,u})$$

which means that

$$p_s s(p_t) = a_{s,t} p_{st}$$

equivalently

$$a_{s,t} = p_s s(p_t) p_{st}^{-1}$$

which is what we wanted to show. We conclude that $H^2(K/k) \subset \delta(A(K/k))$ for all finite Galois extensions of k.

□

These two lemmas togehter proves that

Proposition 6.5.2.

$$A(K/k) \cong H^2(K/k).$$

Proposition 6.5.3. *If K/k and K'/K are finite Galois extensions with $G = Gal(K/k)$ and $G' = Gal(K'/k)$, the following diagram commute*

$$\begin{array}{ccc} A(K/k) & \xrightarrow{\delta} & H^2(K/k) \\ \downarrow{\scriptstyle I} & & \downarrow{\scriptstyle inf} \\ A(K'/k) & \xrightarrow{\delta} & H^2(K'/k) \end{array}$$

where the vertical arrows are regular inclusion (on the left) and the inflation homomorphism (on the right).

Proof. We use the following commutative diagram with exact rows (exactness proven above)

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times & \xrightarrow{i} & \mathrm{GL}_n(K) & \xrightarrow{p} & \mathrm{PGL}_n(K) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle -\otimes 1} & & \downarrow{\scriptstyle -\otimes 1} & & \\ 1 & \longrightarrow & K'^\times & \xrightarrow{i\otimes 1} & \mathrm{GL}_n(K') & \xrightarrow{p\otimes 1} & \mathrm{PGL}_n(K') & \longrightarrow & 1 \end{array}$$

where the vertical arrows are given by the fact that the lower sequence is isomorphic to the higher one with scalars extended to K'.

Let $[C] \in A(K/k)$ with $f : C \otimes K \to M_n(K)$ an K-isomorphism. By the construction of δ, we have that

$$\delta([C]) = [a_{s,t}]$$

where $a_{s,t} = b_s s(b_t) b_{st}^{-1}$, $b_s \in \mathrm{GL}_n(K)$ such that $p(b_s) = f^{-1} \circ s \circ f \circ s^{-1}$. And by the definition of the inflation morphism, $\inf \circ \delta([C]) = [a_{s|_G,t|_G}]$, where we use that $K \subset K'$. The inclusion $A(K/k) \hookrightarrow A(K'/k)$ maps $[C]$ to itself. Hence the map $f \otimes 1 : C_{K'} \to M_n(K')$ is a K'-isomorphism, (extension of scalars preserves isomorphisms). Let $b'_s \in \mathrm{GL}_n(K')$ such that $p\otimes 1(b'_s) = (f\otimes 1)^{-1} s \circ (f\otimes 1) \circ s^{-1} = \left(f^{-1} \circ s \circ f \circ s^{-1}\right) \otimes 1 = p(b_s) \otimes 1$ and we can assume $b'_s = b_s \otimes 1$. Now by the definition of δ

$$\delta \circ I([C]) = [a'_{s,t}]$$

where $a_{s,t} = b'_s s(b'_t) b'^{-1}_{st} = a_{s,t} \otimes 1 = a_{s,t}$ when we consider K as a subfield of K'. This proves that $\delta \circ I = \inf \circ \delta$, i.e. the diagram commutes. □

We conclude this section by noting that by the definition of directed limits and threorem 6.3.2, the we get

Theorem 6.5.1.

$$A_k \cong \varinjlim A(K/k) \cong \varinjlim H^2(K/k) \cong B_k.$$

That is the classical and cohomological Brauer group of a field are isomorphic.

7 Applications of the theory

We will here give three applications of the theory developed above. Although there are more elementary ways to prove, at least the first two, what we will show below, the simplicity of the proofs using Galois cohomology gives us a hint to the power of these methods.

7.1 Computation of the Brauer group of $\mathbb{F}_p$

We recall that any finite field extension of $\mathbb{F}_p$ is Galois with cyclic Galois group genereated by the Frobenius automorphism $x \mapsto x^p$ we can hence apply the results we showed in the section on the cohomology of finite cyclic groups. Let $K/\mathbb{F}_p$ be a finite extension with Galois group G, then K^* is a finite G-module where G acts by automorphism. Hence the Herbrand quotient of K^*, $h(K^*) = 1$.

We saw above that $H^1(G, K^*) = 0$ for all field extensions K/k with $G = \mathrm{Gal(K/k)}$, so this is in particular true for $K/\mathbb{F}_p$. Combinig this with the fact that $h(K^*) = 1$, we get that the order of all of the Tate-cohomology groups of K^* is 1, that is all the cohomology must be trivial. In particular $\hat{H}^2(G, K^*) = H^2(K/k) = 0$.

By the theorem 6.3.2 and Krulls theorem, we have that, if $K/\mathbb{F}_p$ is the (separable) algebraic closure of $\mathbb{F}_p$ with absoloute Galois group G. Then

$$Br(\mathbb{F}_p) = H^2(G, K/k) = \varinjlim H^2(\mathrm{Gal}(L/\mathbb{F}_p), L^*) = \varinjlim \{e\} = \{e\}.$$

That is, the Brauer group of any finite field is trivial. As we saw in the chapter on central simple algebras, this means that there is only one isomorphism class of division algebras over $\mathbb{F}_p$, for any finite field $\mathbb{F}_p$. As a field is a division algebra, and every division ring contains a nontrivial prime field (can be seen by taking the field of fractions of the subring of elements being a n-fold sum of the multiplicative identity of the division ring), this proves that every finite division ring is commutative.

For a very nice more elementary proof of this fact due to Ernst Witt, see [11]. We give here a more condensed version of this proof:

7.1.1 Witt's proof

For brievety of notation, we use the convention $A^* = A \setminus \{0\}$ for any subset A of a division ring.

Suppose R is a finite division ring, and for contradiction assume it is not commutative. Let Z denote the center of R and C_s the centralizer of s (with respect to multiplication). As $Z \subset C_s \subset R$ for all $s \in R$ and all of them are closed under addition and multiplication by elements in Z, they are all vector spaces over the finite field Z. Let the cardinality of Z be q, we get $\mathrm{Card}(C_s) = q^{n_s}$ and $\mathrm{Card}(R) = q^n$ with $n \geq n_s$.

Let A_s denote the orbit of s under the action $a \mapsto xax^{-1}$ for all $x \in R^\times = R\setminus\{0\}$, i.e. A_s is the conjugacy class of s under the natural conjugation action of R^*

on R. Define

$$f_s : R^* \to A_s$$

by

$$x \mapsto x^{-1}sx.$$

We get that $f_s(x) = f_s(y) \Leftrightarrow yx^{-1} \in C_s^* \Leftrightarrow y \in C_s^* x$. As all cosets of a subgroup have the same cardinality, $\mathrm{Card}(C_s^* x) = \mathrm{Card}(C_s^*) = q^{n_s}$. Hence

$$\mathrm{Card}(A_s) = \frac{\mathrm{Card}(R^*)}{\mathrm{Card}(C_s^*)} = \frac{q^n - 1}{q^{n_s} - 1}.$$

Hence $\frac{q^n-1}{q^{n_s}-1}$ is an integer, whence n_s divides n, whence $\mathrm{Card}(A_s) > 1$ for all $s \notin Z$. Let $A_{s_1}, \ldots, A_{s_k}$ be the non-central conjugacy classes of R. By the class equation, see section 4.3 in [3],

$$\mathrm{Card}(R^*) = \mathrm{Card}(Z^*) + \sum_{i=1}^{k} \mathrm{Card}(A_i)$$

$$\Leftrightarrow q^n - 1 = q - 1 + \sum_{i=1}^{k} \frac{q^n - 1}{q^{n_{s_i}} - 1}.$$

$x^n - 1 = \prod_{d|n} \Phi_d(x)$, where $\Phi_d \in \mathbb{Z}[x]$ is the d'th cyclotomic polynomial, see [3] or [11]. Consider n_{s_i} for some $i \in \{1, \ldots, k\}$, we have seen that $n_{s_i} | n$, whence

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = (x^{n_{s_i}} - 1) \prod_{d|n, d \not| n_{s_i}} \Phi_d(x)$$

. We get

$$\Phi_n(q) \big| q^n - 1 \text{ and } \Phi_n(q) \big| \frac{q^n - 1}{q^{n_{s_i}} - 1}$$

for all $i \in \{1, \ldots, k\}$. And from the class formula,

$$\Phi_n(q) \big| q - 1.$$

By assumption, $n > 1$, whence $\Phi_n(1) \neq 0$. Let $a + bi$ be a complex root of $\Phi_n(x)$. As $a + bi$ is a root of 1, $|a + bi|^2 = a^2 + b^2 = 1$. Hence

$$|q - a - bi|^2 = (q-a)^2 + b^2 = q^2 - 2aq + a^2 + b^2 = q^2 - 2aq + 1 > q^2 - 2q + 1 = (q-1)^2$$

whence $|q - a - bi| > q - 1$ for all roots of $\Phi_n(x)$. But

$$|\Phi_n(q)| = \prod_{\lambda} |q - \lambda| > q - 1$$

where λ runs through the roots of $\Phi_n(x)$. But then $\Phi_n(q)$ cannot divide $q - 1$, a contradiction.

7.2 Computation of the Brauer group of $\mathbb{R}$

The extension $\mathbb{C}/\mathbb{R}$ is Galois of degree 2, with Galois group G generated by complex conjugation. As $\mathbb{C}$ is algebraically closed, see the appendix of chapter 2 in [12] or any standard textbook on complex analysis for a proof, $\mathbb{C}$ is (up to isomorphism) the algebraic closure of $\mathbb{R}$ and G the absolute Galois group of $\mathbb{R}$. It follows that the Brauer group of $\mathbb{R}$ is $H^2(G, \mathbb{C}^*)$.

As G is a cyclic group of order 2, we can again use the results we obtained in the chapter on finite cyclic cohomology. In particular, that

$$Br(\mathbb{R}) = H^2(G, \mathbb{C}^*) = \hat{H}^2(G, \mathbb{C}^*) = \hat{H}^0(G, \mathbb{C}^*) = (\mathbb{C}^*)^G / N\mathbb{C}^* = \mathbb{R}^*/N\mathbb{C}^*$$

where N is the norm homomorphism $x \mapsto \prod_{s\in G} s.x = x\overline{x}$ (as $\mathbb{C}^*$ is written as a multiplicative group by convention). In this case we see that the norm homomorphism N simply is the map $x \mapsto |x|^2$, whence $N\mathbb{C}* = \mathbb{R}_{>0}$ and $\mathbb{R}^*/N\mathbb{C}^* \cong \mathbb{Z}/(2)$ as for any $x \in \mathbb{R}^*$, $x\mathbb{R}_0 = x\frac{1}{|x|}\mathbb{R}_{>0} = \text{sign}(x)\mathbb{R}_{>0}$. We conclude that $Br(\mathbb{R}) \cong \mathbb{Z}/(2)$, and hence that there are precisely two distinct classes of division algebras over $\mathbb{R}$. The one corresponding to the identity of the Brauer groups is of course $\mathbb{R}$ itself, and the other one is the Hamiltonian quaternions

$$\mathbb{H} = \{x_1 + x_2 i + x_3 j + x_4 ij | x_i \in \mathbb{R}\}$$

with multiplication defined by the relations $i^2 = j^2 = (ij)^2 = -1$, $ji = -ij$ and the multiplication of two general elements are determined by demanding multiplication to distribute over the standard vector space addition.

7.3 The Brauer group of $\mathbb{Q}_p$

Indeed, these methods can be applied to prove more complicated results, for example that $Br(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$, which in particular shows that there are infinitly many distinct division algebras defined over the p-adic rationals. The idea of the proof is to first show that $Br(\mathbb{Q}_p) = H^2(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \cong H^2((\mathbb{Q}_p)_{nr}/\mathbb{Q}_p)$, where $(\mathbb{Q}_p)_{nr}$ is the maximal unramified extension of $\mathbb{Q}_p$. Then one shows that the residue field of $\mathbb{Q}_p$ is isomorphic to $\mathbb{F}_p$ and that there is a split exact sequence

$$0 \longrightarrow Br(k) \longrightarrow Br(K) \longrightarrow X(\text{Gal}(K_{nr}/K))$$

for any field K complete under a discrete valuation, where $X(G) = \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$, the character group of G and where k denotes the residue field of K. As we saw above, the residue field of $\mathbb{Q}_p$ is finite, hence its Brauer group is trivial and $Br(\mathbb{Q}_p) \to \text{Hom}(\mathbb{Q}_p)_{nr}/\mathbb{Q}_p, \mathbb{Q}/\mathbb{Z})$ is injective, one proves that also surjectivity holds and lastly one shows that $\text{Hom}(\mathbb{Q}_p)_{nr}/\mathbb{Q}_p, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Q}/\mathbb{Z}$. For a full proof, see [1] (section XIII, 3).

References

[1] J.-P. Serre and translated by M.J. Greenberg, *Local Fields*, 1st ed., S. Axler, F. Gehring, and K. Ribet, Eds. New York, US: Springer Science+Business Media New York, 1979.

[2] C. A. Weibel, *An introduction to homological algebra*. Cambridge, UK: Cambridge University Press, 1994.

[3] D. S. Dummit and R. M. Foote, *Abstract Algebra*. US: John Wiley and Sons, Inc, 2003.

[4] P. Freyd, *Abelian Categories*. New York, US: Harper & Row, 1966.

[5] H. Cartan and S. Eilenberg, *Homological Algebra*. Princeton, US: Prinston University Press, 1956.

[6] P. Gille and T. Szamuely, *Central Simple Algebras and Galois Cohomomlogy*, 2nd ed. Cambridge, UK: Cambridge University Press, 2006.

[7] E. Artin and A. N. Milgram, *Galois Theory*. New York, US: Dover Publications, Inc., 1998.

[8] S. S. Shatz, *Profinite Groups, Arithmetic and Geometry*. Princeton, US: Prinston University Press, 1972.

[9] M. Atiyah and I. MacDonald, *Introduction To Commutative Algebra*. Addison-Wesley, 1969.

[10] P. Semrl, "Maps on matrix spaces," Ljubliana, 2005.

[11] M. Aigner and G. M. Ziegler, *Proofs from THE BOOK*. Berlin Heidelberg New York: Springer Verlag, 1998.

[12] A. J. Samuel, Pierre translated by Silberger, *Algebraic Theory of Numbers*. New York, US: Dover Publications, Inc., 1970.