Introduction to Galois Cohomology with Applications to Local Fields

A. Hayward

Spring 2001

Contents

Introduction

We consider the problem of investigating the Galois group of a field extension. In general, this is a very difficult problem. There are, however, certain fields, related very closely to the fields we really want to study (number fields and function fields), for which there is a theory which helps us in this task. This "Local Class Field Theory" is the subject of this report and tells us very explicitly about the *abelianisation* (maximal abelian quotient) of the Galois group. More precisely, our aim is to establish a homomorphism, called the Artin reciprocity map,

$$\psi : K^* \longrightarrow \mathrm{Gal}_K^{ab}.$$

Here K^* is the multiplicative group of a local field and Gal_K^{ab} the maximal abelian quotient of the absolute Galois group of K. This map ψ is "almost" an isomorphism, in that it is bijective on finite quotients of the groups.

The definition of this function is far from trivial. We need a very powerful tool to compare these apparently dissimilar objects. That tool will be the cohomology of groups, and most of the text will be taken up with explaining it. Group cohomology plays an increasingly important role in Number Theory, although a number of Number Theory texts try to exclude it entirely because its exposition is necessarily a lengthy diversion. This approach is less than satisfactory, because it is not so clear and more technical. I hope that the present text gives a reasonable presentation of this deserving theory.

The structure of the presentation roughly follows that of the second half of the book [1] by Serre, which is the main reference for much of the material here. The presentation of cohomology theory comes from the expositions by Serre in [1] and Atiyah and Wall [3]. Other references may be found in the text and the bibliography.

This report contains nothing original, but I hope that I have managed in parts to give a clearer explanation than can be found in the standard literature.

My supervisor for this project was Dr. Mohamed Saidi, to whom I extend my thanks.

0.1 Preliminaries

0.1.1 Rings and Modules

I assume the reader is familiar with rings and fields. If G is a group, the *integral group ring* $\mathbb{Z}[G]$ is the set of formal finite $\mathbb{Z}$-linear combinations of elements of G, $\sum_{g\in G} n_g g$. Multiplication is defined linearly by the multiplication in G. For $\sum_{g\in G} n_g g \in \mathbb{Z}[G]$, $\sum_{g\in G} n_g \in \mathbb{Z}$ is called its *augmentation*. Augmentation is a homomorphism $\mathbb{Z}[G] \longrightarrow \mathbb{Z}$.

If R is a ring (with a multiplicative identity $1 \in R$), a (left-) R-module M is an abelian group (usually written additively) and a map

$$\begin{array}{rcl} R \times M & \longrightarrow & M \\ (r, m) & \longmapsto & rm \end{array}$$

called scalar multiplication, satisfying

1. $(rs)m = r(sm)$
2. $r(m+n) = rm + rn$
3. $1m = m$ for all $r, s \in R, m, n \in M$.

A *right R-module* is defined similarly except we require $(rs)m = s(rm)$ instead of the first property above. Then we usually write $(r, m) \longmapsto mr$. If R is a field, a left R-module is called an R-vector space. If $R = \mathbb{Z}$, a left R-module is an abelian group.

If M, N are R-modules, an *R-homomorphism* $\theta : M \longrightarrow N$ is a group homomorphism such that $\theta(rm) = r\theta(m)$ for all $r \in R, m \in M$. We write $\mathrm{Hom}_R(M, N)$ for the additive group of R-homomorphisms $M \longrightarrow N$.

We define submodules and quotient modules in the obvious way. We have that $\ker\theta$ is a submodule of M and $\mathrm{im}\,\theta$ is a submodule of N. As for abelian groups, $\mathrm{im}\,\theta \cong M/\ker\theta$ as R-modules. We define $\mathrm{coker}\,\theta = N/\mathrm{im}\,\theta$, the *cokernel*.

As usual, a bijective R-homomorphism $M \longrightarrow M$ is called an *R-automorphism* of M. The group of all such maps under composition is written $\mathrm{Aut}_R(M)$.

An R-module M is called *free* if there is a subset $B \subseteq M$, called a basis, such that for any R-module N and any function $f : B \longrightarrow N$ there is an R-homomorphism from M to N which restricts to f.

0.1.2 Category Theory

Category theory provides a useful language for discussing cohomology. A category $\mathcal{C}$ consists of a *class* of "objects" $\mathrm{Obj}\,\mathcal{C}$ and, for each pair $A, B \in \mathrm{Obj}\,\mathcal{C}$, a *set* $\mathrm{Mor}(A, B)$ called the *morphisms* $A \longrightarrow B$.

In addition, for $\phi \in \mathrm{Mor}(A, B)$, $\theta \in \mathrm{Mor}(B, C)$ there is defined a *composite* $\theta \circ \phi \in \mathrm{Mor}(A, C)$. This law must satisfy

1. For each A, $\mathrm{Mor}(A,A) \ni \mathrm{id}_A$ which is an element such that for all $\phi \in \mathrm{Mor}(A,B), \psi \in \mathrm{Mor}(B,A)$, we have $\phi \circ \mathrm{id}_A = \phi$ and $\mathrm{id}_A \circ \psi = \psi$.

2. $\circ$ must be associative.

If in addition to this each $\mathrm{Mor}(A,B)$ is an additive group, and composition distributes over addition, then $\mathcal{C}$ is called a *pre-additive* category.

If $\phi \in \mathrm{Mor}(A,B)$ is such that there exists $\psi \in \mathrm{Mor}(B,A)$ with $\phi \circ \psi = \mathrm{id}_B$ and $\psi \circ \phi = \mathrm{id}_A$ then ϕ is called an *isomorphism.* An isomorphism in $\mathrm{Mor}(A,A)$ is called an automorphism of A.

If $\mathcal{C}, \mathcal{D}$ are categories, then a *(covariant) functor* $F : \mathcal{C} \longrightarrow \mathcal{D}$ is a function $F : \mathrm{Obj}\,\mathcal{C} \longrightarrow \mathrm{Obj}\,\mathcal{D}$ and, for each pair $A, B \in \mathrm{Obj}\,\mathcal{C}$, a function $F : \mathrm{Mor}(A,B) \longrightarrow \mathrm{Mor}(FA, FB)$, such that $F(\phi \circ \psi) = F\phi \circ F\psi$. A *contravariant functor* is defined similarly except we have $F : \mathrm{Mor}(A,B) \longrightarrow \mathrm{Mor}(FB, FA)$ such that $F(\phi \circ \psi) = F\psi \circ F\phi$.

If $F, G : \mathcal{C} \longrightarrow \mathcal{D}$ are functors then they are called *naturally equivalent* if in each $\mathrm{Mor}(FA, GA)$ in $\mathcal{D}$ there is an isomorphism ι_A such that for any $\phi : A \longrightarrow B$ in $\mathcal{C}$, $\iota_B \circ F\phi = G\phi \circ \iota_A$.

0.1.3 The Category of R-modules

If R is a ring, the class of all R-modules and the R-homomorphisms between them form a pre-additive category.

If $f : M \longrightarrow N$, $g : N \longrightarrow P$ are R-homomorphisms between R-modules, we call the diagram

$$M \xrightarrow{f} N \xrightarrow{g} P \tag{1}$$

a *sequence* of R-modules. Longer "sequences" may be made up from parts like this. When $\ker g = \mathrm{im}\, f$, (1) is called an *exact sequence.* A longer sequence is called exact if each subsequence (1) is exact. A *short exact sequence* is a sequence of the form

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0 \tag{2}$$

where 0 denotes the trivial R-module. Then A is (isomorphic to) a submodule of B and $C \cong B/A$.

(2) is called *split* if there is a morphism $j : C \longrightarrow B$ such that $p \circ j = \mathrm{id}_C$. This is the case if and only if there is a morphism $q : B \longrightarrow A$ such that $q \circ i = \mathrm{id}_A$. Equivalently, $B \cong A \times C$ as R-modules, and then i, j are the inclusions of A and C into B, q, p the projections on the components. Note that for any subring S of R, A, B, C are S-modules, and (2) may be S-split but not R-split.

If $F : \mathcal{C} \longrightarrow \mathcal{D}$ is a covariant functor, F is called *left-exact* if exactness of $0 \to A \to B \to C$ implies exactness of $0 \to FA \to FB \to FC$. It is called *right-exact* if exactness of $A \to B \to C \to 0$ implies exactness of $FA \to FB \to FC \to 0$. If F is both left- and right-exact it is called *exact.* Then F takes any exact sequence to a corresponding exact sequence.

If $F : \mathcal{C} \longrightarrow \mathcal{D}$ is contravariant, F is called *left-exact* if exactness of $A \to B \to C \to 0$ implies exactness of $0 \to FC \to FB \to FA$. Given this, the definition of *right-exact* and *exact* contravariant functors is obvious.

Note that any functor preserves exactness of split short exact sequences.

Theorem 0.1.1 *For any R-module M, $\mathrm{Hom}_R(?, M)$ is a contravariant left-exact functor*[1] *and $\mathrm{Hom}_R(M, ?)$ is a covariant left-exact functor.*

For the proof, see [7].

If for an R-module M, $\mathrm{Hom}_R(?, M)$ is exact, M is called (R-)injective. If $\mathrm{Hom}_R(M, ?)$ is exact, M is called (R-)projective. Free modules are both projective and injective.

If A is a right R-module and B is a left R-module, we define the *tensor product over* R of A and B, written $A \otimes_R B$, to be the quotient of the group of formal finite $\mathbb{Z}$-linear combinations of elements of $A \times B$ by the subgroup generated by all elements of the form

$$\begin{array}{ll} (a + a', b) - (a, b) - (a', b) & \\ (a, b + b') - (a, b) - (a, b') & \\ \quad (ar, b) - (a, rb) & \text{for all } a, a' \in A, b, b' \in B, r \in R \end{array}$$

The class of (a, b) is written $a \otimes b$ and these generate the abelian group $A \otimes_R B$.

Theorem 0.1.2 (Universal Mapping Property of Tensor Products) *If X is an abelian group and $f : A \times B \longrightarrow X$ any group homomorphism such that $f(ar, b) = f(a, rb)$ for all $a \in A, b \in B, r \in R$, then there is a unique map $\bar{f} : A \otimes_R B \longrightarrow X$ such that $\bar{f}(a \otimes b) = f(a, b)$ for all $(a, b) \in A \times B$.*

If R is commutative, $A \otimes_R B$ is an R-module. When R is a field, $A \otimes_R B$ is an R-vector space, and if U_A is a basis of A, U_B a basis of B, then $\{u \otimes v : u \in U_A, v \in U_b\}$ is a basis of $A \otimes_R B$.

For any left R-module M, $? \otimes_R M$ is a covariant right-exact functor. For any right R-module M, $M \otimes_R ?$ is again a covariant right-exact functor.

For more details on tensor products, see Bourbaki's *Algèbre* or [7].

A *diagram* is a system of objects of a category placed in Euclidean space and morphisms between them. A diagram is said to *commute* if any chain of morphisms from one point to another composes to give the same morphism. For example the diagram

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \downarrow\psi & & \downarrow\tau \\ C & \xrightarrow{\theta} & D \end{array}$$

commutes if and only if $\theta \circ \psi = \tau \circ \phi$. Then we may draw a $\Box$ in the middle.

[1] from the category of R-modules to the category of abelian groups

Proposition 0.1.3 (Snake Lemma) *A commutative diagram with exact rows*

$$\begin{array}{ccccccccc} & & A & \longrightarrow & B & \xrightarrow{f} & C & \longrightarrow & 0 \\ & & \downarrow_\alpha & \square & \downarrow_\beta & \square & \downarrow_\gamma & & \\ 0 & \longrightarrow & D & \xrightarrow{g} & E & \longrightarrow & F & & \end{array}$$

defines an exact sequence

$$\ker\alpha \longrightarrow \ker\beta \longrightarrow \ker\gamma \xrightarrow{\delta} \operatorname{coker}\alpha \longrightarrow \operatorname{coker}\beta \longrightarrow \operatorname{coker}\gamma,$$

where $\delta := g^{-1} \circ \beta \circ f^{-1}$.

The proof is basic diagram-chasing.

0.1.4 Abelianisation of Groups

If G is a group, its *derived subgroup* G' is the subgroup generated by the *commutators* $[g, h]$ for $g, h \in G$. By definition, $[g, h] = ghg^{-1}h^{-1}$.

G' is a normal subgroup of G. G/G' is the maximal abelian quotient of G. It is also called the *abelianisation* G^{ab} of G.

If H is any subgroup of G such that G/H is abelian, then $G' \subseteq H$, for

$$gg'H = g'gH \Rightarrow g^{-1}g'^{-1}gg' \in H'.$$

One final definition used in the text: *almost all* means all but a finite number.

Chapter 1

Cohomology of Groups

[The reader who is not familiar with homological algebra is referred to Appendix A for the "general nonsense" underlying this material.]

1.1 Basic Definitions and Results

1.1.1 G-modules

Let G be a group, either finite or infinite (although we will only use the finite case here). Let A be an abelian group, and suppose we have a homomorphism

$$G \longrightarrow \mathrm{Aut}(A).$$

Then we say that A is an *abelian (left-)G-module*. What this means is that for each $g \in G$ there is an automorphism $a \longmapsto ga$ in such a way that $(gh)a = g(ha)$ for all $g, h \in G, a \in A$ and $g(a + a') = ga + ga'$ for all $g \in G, a, a' \in A$. In this section we will write simple "G-module".

Consider the integral group ring $\mathbb{Z}[G]$. If A is a G-module, putting

$$\begin{array}{ccc} \mathbb{Z}[G] \times A & \longrightarrow & A \\ (\sum_{g \in G} n_g g, a) & \longmapsto & \sum_{g \in G} n_g ga \end{array}$$

defines a $\mathbb{Z}[G]$-module structure on A, extending the G-module structure linearly. On the other hand, a $\mathbb{Z}[G]$-module structure on A is necessarily a G-module structure on A, the action of G on A being given by $g : a \longmapsto ga$. Thus an abelian G-module is the same as a $\mathbb{Z}[G]$-module. $\mathbb{Z}[G]$-homomorphisms will also be called G-homomorphisms. If the homomorphism $G \longrightarrow \mathrm{Aut}(A)$ is trivial, G is said to act trivially on A.

1.1.2 The Fixed-Point Functor

Write A^G for the set of elements of A fixed by every $g \in G$; it is a $\mathbb{Z}[G]$-submodule of A. $A \longmapsto A^G$ is a covariant functor on the category of G-modules and G-homomorphisms.

Proposition 1.1.1 *$A \longmapsto A^G$ is naturally equivalent to the functor $A \longmapsto \mathrm{Hom}_G(\mathbb{Z}, A)$ where G acts trivially on $\mathbb{Z}$.*

PROOF - An element $a \in A^G$ can be made to correspond to a map

$$\begin{array}{rccc} \phi_a : & \mathbb{Z} & \longrightarrow & A \\ & 1 & \longmapsto & a \end{array}$$

because for such a map $ga = g\phi_a(1) = \phi_a(g1) = \phi_a(1) = a$. Then a homomorphism $A^G \longrightarrow B^G$ induces a homomorphism $\mathrm{Hom}_G(\mathbb{Z}, A) \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, B)$. Natural equivalence is easy.

□

We know $\mathrm{Hom}_G(\mathbb{Z}, ?)$ is left-exact, so ^{G} is left-exact. That is, given an exact sequence, say

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

of G-modules, the sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \tag{1.1}$$

is exact. We are going to use the cohomology theory developed in Appendix A to continue this sequence to the right.

1.1.3 Some G-module Structures

In this section A, B will denote G-modules (for the same G, of course). X will denote an additive abelian group. X can be given the structure of a G-module by making G act trivially on X (ie. $gx = x$ for all $g \in G, x \in X$).

Consider first the group $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ of group homomorphisms $A \longrightarrow B$.

Definition 1.1.2 *The standard G-module structure on $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ is given by*

$$(g\phi)(a) = g(\phi(g^{-1}a)) \qquad \textit{for all } g \in G, \phi \in \mathrm{Hom}_{\mathbb{Z}}(A, B), a \in A$$

This can be checked to define a G-module structure. Notice that with this structure, $\mathrm{Hom}_{\mathbb{Z}}(A, B)^G = \mathrm{Hom}_G(A, B)$.

We must always be careful about the G-module structure of the arguments A, B. For example, when we talk about co-induced modules, we show how to embed any G-module A in $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A_+)$. Here A_+ denotes A considered as a trivial G-module (abelian group).

Now consider the tensor product $A \otimes_{\mathbb{Z}} B$.

Definition 1.1.3 *The standard G-module structure on $A \otimes_{\mathbb{Z}} B$ is given by*

$$g(a \otimes b) = ga \otimes gb \qquad \textit{for all } g \in G, a \in A, b \in b$$

Again we must be careful when factors are to be considered with trivial G-action.

If A is a left G-module then A is a right $\mathbb{Z}[G]$-module under the action $as := s^{-1}a$ for each $a \in A, s \in G$. This allows us to define for each pair of G-modules A, B the *tensor product over G*

$$A \otimes_G B := A \otimes_{\mathbb{Z}[G]} B.$$

1.1.4 The Cohomology Groups of a G-module

The first step is to choose a G-free resolution of $\mathbb{Z}$. By this we mean an acyclic complex

$$\mathbf{P}: \qquad \ldots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0.$$

So the d_i are G-homomorphisms and the sequence is exact. We will exhibit two such resolutions in the next section, so the reader may trust that they exist.

Now let A be a G-module we want to study, and apply the contravariant functor $\mathrm{Hom}_G(?, A)$ to the "deleted complex" $\mathbf{P}_{\mathbb{Z}}$

$$\ldots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \to 0$$

to obtain a cochain complex $\mathrm{Hom}_G(\mathbf{P}_{\mathbb{Z}}, A) =: \mathbf{K}(A)$ of abelian groups

$$0 \to \mathrm{Hom}_G(P_0, A) \xrightarrow{d_0} \mathrm{Hom}_G(P_1, A) \xrightarrow{d_1} \mathrm{Hom}_G(P_2, A) \xrightarrow{d_2} \ldots$$

so $K^q(A) = \mathrm{Hom}_G(P_q, A)$ for $q \geq 0$, $K^q(A) = 0$ for $q < 0$, and d_q acts on a cochain $f \in \mathrm{Hom}_G(P_q, A)$ by $(d_q f)(x) := f(d_q(x))$.

The *cohomology groups of G with coefficients in A* are now defined as the cohomology groups of this complex

$$H^q(G, A) := H^q(\mathbf{K}(A))$$

Thus an element of the q-th cohomology group $H^q(G, A)$ is an equivalence class of G-homomorphisms $P_q \longrightarrow A$. When we want to show a property of one of these elements, we will usually work with a representative G-homomorphism, and then show that our conclusion does not depend on which representative we choose. The groups $H^q(G, A)$ for $q > 0$ are called the *higher* cohomology groups of G with coefficients in A.

The lowest cohomology group $H^0(G, A)$ has a special meaning: it is (naturally equivalent to) A^G. This is because the sequence

$$P_1 \xrightarrow{d_0} P_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

is exact, so applying the contravariant left-exact functor $\mathrm{Hom}_G(?, A)$ gives an exact sequence of abelian groups

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \longrightarrow \mathrm{Hom}_G(P_0, A) \xrightarrow{d_0} \mathrm{Hom}_G(P_1, A)$$

so that $\ker d_0$ is naturally equivalent to $\mathrm{Hom}_G(\mathbb{Z}, A)$, which in turn is naturally equivalent to A^G (by Proposition 1.1.1). So $H^0(\mathbf{K}(A)) = \ker d_0/\mathrm{im}\, d_{-1} = \ker d_0/0 = A^G$.

Suppose now we are given a short exact sequence of G-modules

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0. \tag{1.2}$$

We apply for each $q \in \mathbb{Z}$ the covariant functor $\mathrm{Hom}_G(P_q, ?)$, which is exact because P_q is G-free and hence G-projective. We obtain the commutative diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_G(P_0, A) & \xrightarrow{i^*} & \mathrm{Hom}_G(P_0, B) & \xrightarrow{p^*} & \mathrm{Hom}_G(P_0, C) & \longrightarrow 0 \\
 & & d_0\downarrow & \square & d_0\downarrow & \square & d_0\downarrow & & \\
0 & \longrightarrow & \mathrm{Hom}_G(P_1, A) & \xrightarrow{i^*} & \mathrm{Hom}_G(P_1, B) & \xrightarrow{p^*} & \mathrm{Hom}_G(P_1, C) & \longrightarrow 0 \\
 & & d_1\downarrow & \square & d_1\downarrow & \square & d_1\downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

with exact rows and columns, in other words an exact sequence of complexes

$$0 \longrightarrow \mathbf{K}(A) \longrightarrow \mathbf{K}(B) \longrightarrow \mathbf{K}(C) \longrightarrow 0.$$

We know from Appendix A that this gives rise to the long exact cohomology sequence, which in our new notation is

$$\begin{aligned}
0 \longrightarrow H^0(G, A) &\xrightarrow{i^*} H^0(G, B) \xrightarrow{p^*} H^0(G, C) \\
\xrightarrow{\delta} H^1(G, A) &\xrightarrow{i^*} H^1(G, B) \xrightarrow{p^*} \dots
\end{aligned} \tag{1.3}$$

We have obtained the promised continuation of (1.1). This continuation is in a sense unique, as will soon be shown.

1.1.5 Uniqueness of the Cohomology Groups

Proposition 1.1.4 *If A is G-injective then $H^q(G, A) = 0$ for $q \geq 1$.*

PROOF - recall that the condition means that $\mathrm{Hom}_G(?, A)$ is an exact functor. This means that it takes the exact sequence

$$\dots \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

to an exact sequence

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \xrightarrow{\epsilon} \mathrm{Hom}_G(P_0, A) \xrightarrow{d_0} \mathrm{Hom}_G(P_1, A) \xrightarrow{d_1} \dots$$

so that $\ker d_q = \mathrm{im}\, d_{q-1}$ for $q \geq 1$.

$\square$

We need:

Theorem 1.1.5 *For any ring R, every R-module is a submodule of an injective R-module.*

For the proof, see [7], §3, theorem 3.26.

We can now establish

Proposition 1.1.6 *The cohomological functor $\{H, \delta\}$ is characterised by the properties*

- $H^0(G, A) = A^G$
- $H^q(G, ?)$ *is a covariant functor for each q*
- δ *gives a long exact sequence for each short exact sequence* $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$
- *If A is an injective G-module, $H^q(G, A) = 0$ for $q > 0$.*

PROOF - We have seen that the functor $\{H, \delta\}$ defined as above has these properties. On the other hand, suppose $\{H, \delta\}$ is a functor with these properties, then by the theorem above there is, for a given A, an exact sequence

$$0 \longrightarrow A \xrightarrow{i} A^* \xrightarrow{p} A^*/A \longrightarrow 0$$

with A^* injective; the long exact cohomology sequence then gives an exact sequence

$$0 \to H^0(G, A) \xrightarrow{i^*} H^0(G, A^*) \xrightarrow{p^*} H^0(G, A^*/A) \xrightarrow{\delta} H^1(G, A) \xrightarrow{i^*} H^1(G, A^*)$$

But $H^1(G, A^*) = 0$ so δ induces an isomorphism

$$\frac{H^0(G, A^*/A)}{\operatorname{im} p^*} \longrightarrow H^1(G, A)$$

Which defines $H^1(G, A)$ in terms of H^0. Similarly for $q > 1$, the long exact cohomology sequence gives an exact sequence

$$0 \longrightarrow H^{q-1}(G, A^*/A) \xrightarrow{\delta} H^q(G, A) \longrightarrow 0$$

so that $H^{q-1}(G, A^*/A) \cong H^q(G, A)$. In this way H^q is always determined by H^{q-1} up to natural equivalence, and as we know H^0, the functor $\{H, \delta\}$ must be naturally equivalent to the one defined above.

$\square$

Thus we see in particular that the cohomology groups and connecting homomorphisms as defined above do not depend on which free G-resolution of $\mathbb{Z}$ is chosen.

The trick used in the proof is called "dimension-shifting": we use a short exact sequence with a module in the middle which has zero cohomology groups to relate a q-dimensional cohomology group to a $(q-1)$-dimensional one.

1.1.6 Cohomology of Co-induced Modules

The condition of injectivity is excessively strong. We will show that a weaker condition suffices for the higher cohomology groups to be zero.

Definition 1.1.7 *A G-module is* co-induced *if it is isomorphic to a module* $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)$, *where X is an abelian group (see Definition 1.1.2). A G-module is called* relatively injective *if it is a direct factor of a co-induced module.*

Proposition 1.1.8 *A G-module A embeds in the co-induced G-module* $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A_+)$, *where A_+ indicates the additive group of A. (cf. Theorem 1.1.5)*

PROOF - The required monomorphism is

$$\begin{array}{ccl} A & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A_+) \\ a & \longmapsto & \qquad\qquad \phi_a : \begin{array}{ccc} \mathbb{Z}[G] & \longrightarrow & A_+ \\ g & \longmapsto & g^{-1}a \end{array} \end{array}$$

the inverse $\phi \longmapsto \phi(1_G)$ showing injectivity.

□

It can be shown that injective modules are relatively injective.

Lemma 1.1.9 (Additivity of Cohomology Functors) *Let $A \oplus B$ denote the direct sum of two G-modules A and B. Then $H^q(G, A \oplus B) = H^q(G, A) \oplus H^q(G, B)$.*

PROOF - Take cohomology of the split short exact sequence

$$0 \longrightarrow A \underset{\longleftarrow}{\overset{\longrightarrow}{}} A \oplus B \underset{\longleftarrow}{\overset{\longrightarrow}{}} B \longrightarrow 0$$

noting that then the connecting homomorphisms are all the zero map.

□

We can now show the weaker condition, with the help of the following lemma.

Lemma 1.1.10 *A free G-resolution of $\mathbb{Z}$ admits $\mathbb{Z}$-homomorphisms*

$$\begin{array}{l} h_0 : \mathbb{Z} \longrightarrow P_0 \\ h_1 : P_0 \longrightarrow P_1 \quad \text{etc.} \end{array}$$

so that $h_n \circ d_{n-1} + d_n \circ h_{n+1}$ is the identity map.

$$\begin{tikzcd} \cdots \arrow[r, "d_2"] & P_2 \arrow[r, "d_1"] \arrow[l, bend left, "h_3"] & P_1 \arrow[r, "d_0"] \arrow[l, bend left, "h_2"] & P_0 \arrow[r, "\epsilon"] \arrow[l, bend left, "h_1"] & \mathbb{Z} \arrow[r] \arrow[l, bend left, "h_0"] & 0 \end{tikzcd}$$

This is proved by defining the maps inductively, using the fact that each P_q is a free $\mathbb{Z}$-module.

The maps h_n form a "contracting homotopy" of $\mathbb{Z}$-homomorphisms on the resolution.

Proposition 1.1.11 *If A is relatively injective, $H^q(G, A) = 0$ for $q > 0$.*

PROOF - By the lemma on additivity, if we show that co-induced modules have zero cohomology, their direct factors must also. So let $A = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)$.

Then the functors on the category of G-modules, $\mathrm{Hom}_G(?, A)$ and $\mathrm{Hom}_{\mathbb{Z}}(?, X)$ are naturally equivalent, the isomorphism for any G-module M being

$$\begin{array}{ccc} \mathrm{Hom}_G(M, A) & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}}(M, X) \\ \phi & \longmapsto & (m \mapsto \phi(m)(1_G)) \end{array}$$

Applying $\mathrm{Hom}_G(?, A)$ to the free resolution of $\mathbb{Z}$ now yields a sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, X) \xrightarrow{\epsilon} \mathrm{Hom}_{\mathbb{Z}}(P_0, X) \xrightarrow{d_0} \mathrm{Hom}_{\mathbb{Z}}(P_1, X) \xrightarrow{d_1} \dots$$

We use the last lemma to show that this sequence is exact, and so the cohomology of A is zero. We have $d_{q+1} \circ d_q$, so $\mathrm{im}\, d_q \subseteq \ker d_{q+1}$. If $\phi : P_{q+1} \longrightarrow X$ is in $\ker d_{q+1}$, so that $\phi \circ d_{q+1} = 0$, put $\psi = \phi \circ h_{q+1} : P_q \longrightarrow X$. Then

$$\begin{aligned} \psi(d_q(y)) &= \phi(h_{q+1} \circ d_q(y)) \\ &= \phi((h_{q+1} \circ d_q + d_{q+1} \circ h_{q+2})(y)) \\ &= \phi(y) \end{aligned}$$

so that $\phi \in \mathrm{im}\, d_q$.

□

All this works because $\mathbb{Z}$ is a free $\mathbb{Z}$-module - note that it is not a free $\mathbb{Z}[G]$-module, for nontrivial G.

1.2 The Standard Resolution

Recall (§1.1, Proposition 1.1.6) that any free G-resolution of $\mathbb{Z}$ will do to obtain the cohomology groups of G with coefficients in A. In practice, there is one which is particularly useful.

Define Q_q for $q \geq 0$ to be the free $\mathbb{Z}$-module on G^{q+1}, made into a G-module via the diagonal action

$$s(g_0, \dots, g_q) := (sg_0, \dots, sg_q)$$

this is a free G-module with basis eg. $\{(1, g_1, \dots, g_q) : g_j \in G\}$. The boundary formula is given, for each $\mathbb{Z}$-generator of Q_q, by

$$d_{q-1}(g_0, \dots, g_q) = \sum_{i=0}^{q} (-1)^i (g_0, \dots, g_{i-1}, g_{i+1}, \dots, g_q)$$

which defines a G-homomorphism $Q_q \longrightarrow Q_{q-1}$. Note that $d_{-q} : Q_0 \longrightarrow \mathbb{Z}$ is just the "augmentation map"

$$\begin{array}{ccc} \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} \\ \sum_{g \in G} n_g g & \longmapsto & \sum_{g \in G} n_g \end{array}$$

Proposition 1.2.1 *The sequence of G-modules*

$$\dots \xrightarrow{d_2} Q_2 \xrightarrow{d_1} Q_1 \xrightarrow{d_0} Q_0 \xrightarrow{d_{-1}} \mathbb{Z} \longrightarrow 0$$

is exact.

PROOF - It is easy to check that $d_{q-1} \circ d_q = 0$, and so $\operatorname{im} d_q \subseteq \ker d_{q-1}$. To show the reverse inclusion, we construct a contracting homotopy on the complex. Define

$$\begin{array}{cccc} h_i : & P_{i-1} & \longrightarrow & P_i \\ & (g_0, \dots, g_{i-1}) & \longmapsto & (1, g_0, \dots, g_{i-1}) \end{array}$$

Then it is easy to check that $h_q \circ d_{q-1} + d_q \circ h_{q+1} = \mathrm{id}_{Q_q}$, so if $x \in \ker d_{q-1}$ then

$$x = (h_q \circ d_{q-1} + d_q \circ h_{q+1})(x) = d_q(h_{q+1}(x)) \in \operatorname{im} d_q$$

□

Thus this resolution of $\mathbb{Z}$ gives the cochain complex

$$0 \longrightarrow \mathrm{Hom}_G(Q_0, A) \xrightarrow{d_0} \mathrm{Hom}_G(Q_1, A) \xrightarrow{d_1} \mathrm{Hom}_G(Q_2, A) \xrightarrow{d_2} \dots$$

called the *homogeneous cochain complex.* A q-dimensional homogeneous cochain is then a G-homomorphism

$$\mathbb{Z}[G^{q+1}] \longrightarrow A$$

As such a function is clearly defined by its values on the $\mathbb{Z}$-basis G^{q+1}, we may say that a q-dimensional homogeneous cochain is a function

$$f : G^{q+1} \longrightarrow A$$

such that $s(f(g_0, \dots, g_q)) = f(sg_0, \dots, sg_q)$

1.2.1 The Inhomogeneous Cochain Complex

This is not a particularly efficient definition because one of the g_i is superfluous, by the G-homomorphism definition; for example, $f(g_0, \dots, g_q) = g_0 f(1, g_0^{-1} g_1, \dots, g_0^{-1} g_q)$ This leads us to rewrite the definition as follows. Let P_q be the free $\mathbb{Z}[G]$-module on the basis G^q, so that P_q is the set of formal sums of products of an element s of G and a q-tuple[1] $[g_1, \dots, g_q] \in G^q$.

Define G-homomorphisms

$$\begin{array}{rcl} Q_q & \longrightarrow & P_q \\ (g_0, \dots, g_q) & \longmapsto & g_0[g_0^{-1} g_1, g_1^{-1} g_2, \dots, g_{q-1}^{-1} g_q] \end{array}$$

$$\begin{array}{rcl} P_q & \longrightarrow & Q_q \\ [g_1, \dots, g_q] & \longmapsto & (1, g_1, g_1 g_2, \dots, g_1 g_2 \dots g_q) \end{array}$$

[1]We will always write square brackets when dealing with the P_q.

It is easy to check that these are mutually inverse.

These G-isomorphisms, along with the boundary formula for homogeneous cochains, yield a boundary homomorphism

$$P_{q+1} \longrightarrow Q_{q+1} \xrightarrow{d_q} Q_q \longrightarrow P_q$$

given by the formula

$$\begin{aligned} d_q[g_1, \ldots, g_{q+1}] &= g_1[g_2, \ldots, g_{q+1}] \\ &+\sum_{j=1}^{q}(-1)^j[g_1, \ldots, g_j g_{j+1}, \ldots, g_{q+1}] \\ &+(-1)^{q+1}[g_1, \ldots, g_q] \end{aligned} \tag{1.4}$$

So now we have a *free G-resolution* of $\mathbb{Z}$

$$\ldots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \longrightarrow \mathbb{Z}$$

and the cochain complex obtained is

$$0 \longrightarrow \mathrm{Hom}_G(P_0, A) \xrightarrow{d_0} \mathrm{Hom}_G(P_1, A) \xrightarrow{d_1} \mathrm{Hom}_G(P_2, A) \xrightarrow{d_2} \ldots$$

called the *inhomogeneous cochain complex.* A q-dimensional inhomogeneous cochain is then a G-homomorphism $P_q \longrightarrow A$ or, what amounts to the same, any function

$$f : G^q \longrightarrow A$$

The coboundary of f is $df : G^{q+1} \longrightarrow A$ given by

$$\begin{aligned} df[g_1, \ldots, g_{q+1}] &= g_1 f[g_2, \ldots, g_{q+1}] \\ &+\sum_{j=1}^{q}(-1)^j f[g_1, \ldots, g_j g_{j+1}, \ldots, g_{q+1}] \\ &+(-1)^{q+1} f[g_1, \ldots, g_q] \end{aligned} \tag{1.5}$$

This is the "bare hands" definition of cohomology which is most useful in practice. Although we always know the cohomology of a G-module exists and is unique, actually calculating the groups is in general very difficult. That is why it is useful to have this more concrete representation.

1.2.2 Explicit Descriptions of the Cochain Complex

Let's examine more closely the inhomogeneous cochain complex. A q-cocycle is a function $f : G^q \longrightarrow A$ satisfying $df = 0$, ie.

$$\begin{aligned} g_1 f[g_2, \ldots, g_{q+1}] + \sum_{j=1}^{q}(-1)^j f[g_1, \ldots, g_j g_{j+1}, \ldots, g_{q+1}] & \\ +(-1)^{q+1} f[g_1, \ldots, g_q] &= 0 \end{aligned}$$

for all $[g_1, \ldots, g_{q+1}] \in G^{q+1}$. A q-coboundary is $dh : G^q \longrightarrow A$ for some $(q-1)$-cochain h. If

$$0 \longrightarrow A \xrightarrow{i} B \xrightarrow{p} C \longrightarrow 0$$

is a short exact sequence of G-modules, then the connecting homomorphism may be evaluated as follows. Given a q-cocycle f in C representing a cohomology class, there is a q-cochain $h : G^q \longrightarrow B$ with $p \circ h = f$, because p is surjective.

$$\begin{array}{ccccccc} & & & & \mathrm{Hom}_G(P_q, B) & \xrightarrow{p^*} & \mathrm{Hom}_G(P_q, C) & \longrightarrow & 0 \\ & & & & \downarrow d & & & & \\ 0 & \longrightarrow & \mathrm{Hom}_G(P_{q+1}, A) & \xrightarrow{i^*} & \mathrm{Hom}_G(P_{q+1}, B) & & & & \end{array}$$

Applying d gives dh, a $(q+1)$-coboundary in B and hence a $(q+1)$-cocycle in B. But $p^* \circ d = d \circ p^*$, since p^* is a morphism of complexes, so $p \circ dh = 0$ and so dh takes values in $\ker p = \mathrm{im}\, i = i(A)$. Thus $i^{-1} \circ dh$ is a $(q+1)$-cocycle in A, whose cohomology class is by definition $\delta_q f$.

Let us now look at some low-dimensional examples.

$q = 0$**:** We know $H^0(G, A) \cong A^G$. Let us see how this fits with the inhomogeneous cochains. A 0-cocycle is a function

$$f : G^0 = \{1\} \longrightarrow A$$

ie. an element of A, with $df = 0$. Since

$$df[g_1] = g_1 f - f$$

This condition says that $f \in A$ satisfies $f = g_1 f$ for all $g_1 \in G$, so that f is an element of A^G.

$q = 1$**:** Now the coboundary formula takes a 1-cochain $f : G \longrightarrow A$ to

$$\begin{array}{cccc} df : & G^2 & \longrightarrow & A \\ & [g_1, g_2] & \longmapsto & g_1 f[g_2] - f[g_1 g_2] + f[g_1] \end{array}$$

so that a 1-cocycle is a function $f : G \longrightarrow A$ with

$$f[g_1 g_2] = f[g_1] + g_1 f[g_2].$$

Such a function is called a *crossed homomorphism.* f is a 1-coboundary if there is $a \in A$ such that

$$f[g_1] = g_1 a - a.$$

From this we see that when G acts trivially on A, $H^1(G, A) = \mathrm{Hom}_{\mathbb{Z}}(G, A)$.

$q = 2$: This time a 2-cocycle is a function $f : G^2 \longrightarrow A$ satisfying

$$g_1 f[g_2, g_3] - f[g_1 g_2, g_3] + f[g_1, g_2 g_3] - f[g_1, g_2] = 0$$

Such a function is called a *factor set*. Factor sets arise in the problem of *group extensions* (see [7] §5). f is a 2-coboundary if there is a function $h : G \longrightarrow A$ with

$$f[g_1, g_2] = g_1 h[g_2] - h[g_1 g_2] + h[g_1]$$

1.3 Homology of Groups

There is a dual theory to the cohomology theory introduced above. Starting with a free G-resolution of $\mathbb{Z}$,

$$\ldots \xrightarrow{d_2} P_2 \xrightarrow{d_1} P_1 \xrightarrow{d_0} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

remove $\mathbb{Z}$ and apply the covariant functor $? \otimes_{\mathbb{Z}[G]} A$, which is, in a sense, the "dual" to $\mathrm{Hom}_G(?, A)$. We obtain a chain complex

$$\ldots \xrightarrow{d_2 \otimes 1_A} P_2 \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_1 \otimes 1_A} P_1 \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_0 \otimes 1_A} P_0 \otimes_{\mathbb{Z}[G]} A \longrightarrow 0$$

where $1_A = \mathrm{id}_A$, the identity function on A. The *q-th homology group of G with coefficients in A* is now

$$H_q(G, A) := \frac{\ker(d_{q-1} \otimes 1)}{\mathrm{im}\,(d_q \otimes 1)}$$

a quotient of a subgroup of the additive group $P_q \otimes_{\mathbb{Z}[G]} A$. Similarly to before, H_0 has a special meaning. Applying the right-exact functor $? \otimes_{\mathbb{Z}[G]} A$ to the exact sequence

$$P_1 \xrightarrow{d_0} P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

gives an exact sequence

$$P_1 \otimes_{\mathbb{Z}[G]} A \xrightarrow{d_0 \otimes 1_A} P_0 \otimes_{\mathbb{Z}[G]} A \longrightarrow \mathbb{Z} \otimes_{\mathbb{Z}[G]} A \longrightarrow 0$$

so that

$$\frac{P_0 \otimes_{\mathbb{Z}[G]} A}{\mathrm{im}\,(d_0 \otimes 1)} \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A$$

and we have only to identify $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A$. Let I_G be the "augmentation ideal" of $\mathbb{Z}[G]$, that is, the additive subgroup generated by all $\sum_{g \in G} n_g g$ in $\mathbb{Z}[G]$ with augmentation $\sum_{g \in G} n_g = 0$. If we project an element of $I_G A$ onto $\mathbb{Z} \otimes_{\mathbb{Z}[G]} A$ then it maps to an element of $\mathbb{Z} I_G \otimes_{\mathbb{Z}[G]} A$. But the action of G on $\mathbb{Z}$ is trivial, so $\mathbb{Z} I_G = 0$. Thus I_G projects to zero. In fact:

Proposition 1.3.1 *We have the isomorphism of abelian groups*

$$\mathbb{Z} \otimes_{\mathbb{Z}[G]} A \cong \frac{A}{I_G A}$$

PROOF - The correspondence

$$\begin{array}{ccc} \mathbb{Z} \otimes_{\mathbb{Z}[G]} A & \longleftrightarrow & \dfrac{A}{I_G A} \\ n \otimes a & \longleftrightarrow & na + I_G A \end{array}$$

gives well-defined inverse homomorphisms.

□

$A/I_G A$ is written A_G, and is the largest quotient group of A on which G acts trivially[2]. $H_q(G, A)$ is the unique homological extension of the functor $A \longmapsto A_G$, and is characterised by

- $H_0(G, A) = A_G$
- $H_q(G, ?)$ is a covariant functor for each q
- δ (see Appendix A) gives a long exact sequence

$$\begin{aligned} \ldots \longrightarrow H_1(G, C) \xrightarrow{\delta} H_0(G, A) \longrightarrow H_0(G, B) \\ \longrightarrow H_0(G, C) \longrightarrow 0 \end{aligned} \tag{1.6}$$

  for each short exact sequence $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$

- If A is a projective G-module, $H_q(G, A) = 0$ for $q > 0$.

The proof is similar to that of the corresponding result in cohomology. Again, the last condition can be weakened.

A G-module A is called *induced* if it has the form $\mathbb{Z}[G] \otimes_{\mathbb{Z}} X$, where X can be any additive group, the G-action being as defined in §1.1.3. A is called *relatively projective* if it is a direct factor of such a module. Relatively projective modules also have all their higher homology groups zero. The proofs are similar to those for the corresponding results in cohomology.

We know that every module is a quotient of a free, and hence projective, module. Moreover, the surjective G-homomorphism

$$\begin{array}{ccc} \mathbb{Z}[G] \otimes_{\mathbb{Z}} A_+ & \longrightarrow & A \\ s \otimes a & \longmapsto & sa \end{array}$$

shows that every module is canonically a quotient of an induced module. Thus for any A there is always an exact sequence

$$0 \longrightarrow A' \longrightarrow A_* \longrightarrow A \longrightarrow 0$$

with A_* induced, which allows dimension-shifting.

[2]Compare A^G, which was the largest subgroup on which G acts trivially.

1.3.1 The Standard Resolution

We can use our standard resolution to give a description of these groups as groups of homology classes of inhomogeneous chains. Recall that P_q is the free $\mathbb{Z}[G]$-module on G^q. The properties of tensor products show that any $(q+1)$-dimensional chain can be uniquely written

$$x = \sum [g_1, \ldots, g_{q+1}] \otimes a_{[g_1,\ldots,g_{q+1}]}$$

where the summation is over all $(q+1)$-tuples $[g_1, \ldots, g_{q+1}] \in G^{q+1}$, and only finitely many of the a are nonzero. So x is effectively a function

$$\begin{array}{cccc} f: & G^{q+1} & \longrightarrow & A \\ & [g_1, \ldots, g_{q+1}] & \longmapsto & a_{[g_1,\ldots,g_{q+1}]} \end{array}$$

with almost all its values zero (meaning all but a finite number).

We can use the boundary formula $d : P_{q+1} \longrightarrow P_q$ (1.4) to give a formula for the boundary

$$\begin{array}{cccc} d: & P_{q+1} \otimes_{\mathbb{Z}[G]} A & \longrightarrow & P_q \otimes_{\mathbb{Z}[G]} A \\ & [g_1, \ldots, g_{q+1}] \otimes a_{[g_1,\ldots,g_{q+1}]} & \longmapsto & (d[g_1, \ldots, g_{q+1}]) \otimes a_{[g_1,\ldots,g_{q+1}]} \end{array}$$

and the result is

$$\begin{aligned} df[g_1, \ldots, g_q] &= \sum_{g \in G} g^{-1} f[g, g_1, \ldots, g_q] \\ &\quad + \sum_{j=1}^{q} (-1)^j \sum_{g \in G} f[g_1, \ldots, g_{j-1}, g_j g, g^{-1}, g_{j+1}, \ldots g_q] \\ &\quad + (-1)^{q+1} \sum_{g \in G} f[g_1, \ldots, g_q, g] \end{aligned}$$

Note that a G-homomorphism $\phi : A \longrightarrow B$ induces $\phi : H_q(G, A) \longrightarrow H_q(G, B)$ by $\phi(f) = \phi \circ f$.

1.3.2 The Group $H_1(G, \mathbb{Z})$

Our final task in this section is to identify the group $H_1(G, \mathbb{Z})$, where G acts trivially on $\mathbb{Z}$. This group will be of central importance later.

Consider the exact sequence

$$0 \longrightarrow I_G \xrightarrow{i} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

where

$$\begin{array}{cccc} \epsilon: & \mathbb{Z}[G] & \longrightarrow & \mathbb{Z} \\ & \sum_{g \in G} n_g g & \longmapsto & \sum_{g \in g} n_g \end{array}$$

is the augmentation map and I_G its kernel. The exact homology sequence gives an exact sequence

$$H_1(G, \mathbb{Z}[G]) \xrightarrow{\epsilon_*} H_1(G, \mathbb{Z}) \xrightarrow{\delta} H_0(G, I_G) \xrightarrow{i_*} H_0(G, \mathbb{Z}[G])$$

As $\mathbb{Z}[G] \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}$ is induced, $H_1(G, \mathbb{Z}[G])$ is zero. On the other hand,

$$\frac{I_G}{I_G I_G} \xrightarrow{i_*} \frac{\mathbb{Z}[G]}{I_G \mathbb{Z}[G]}$$

is the zero map, so $\ker i_* = \operatorname{im} \delta = H_0(G, I_G) = I_G/I_G^2$. Thus δ is an isomorphism

$$H_1(G, \mathbb{Z}) \longrightarrow I_G/I_G^2$$

We can further identify I_G/I_G^2. It is not hard to see that I_G is an abelian group generated by the set $\{g - 1 : g \in G\}$. Define a function ϕ from the multiplicative group G to the additive group I_G/I_G^2 by $\phi(g) = (g-1) + I_G^2$. Then because

$$\begin{aligned} gh - 1 &\equiv (g-1)(h-1) + (g-1) + (h-1) \\ &\equiv (g-1) + (h-1) \qquad \pmod{I_G^2} \end{aligned}$$

ϕ is a homomorphism. ϕ is clearly surjective. If we can identify $\ker \phi$, we have found I_G/I_G^2 as a quotient of G.

The key here is to note that $G/\ker \phi$ is abelian. Hence $G' \subseteq \ker \phi$, where G' is the derived subgroup of G. In fact, $G' = \ker \phi$; to see the reverse inclusion, define

$$\begin{array}{rccc} \psi : & I_G/I_G^2 & \longrightarrow & G/G' \\ & \sum n_g(g-1) + I_G^2 & \longmapsto & (\prod g^{n_g})G' \end{array}$$

Let's check ψ is well-defined: suppose $x, x' \in I_G$ represent the same class in I_G/I_G^2. Then

$$\begin{aligned} x' &= x + \sum_i (h_i - 1)(l_i - 1) \qquad \text{(for some } h_i, l_i \in G) \\ &= x + \sum_i \big[(h_i l_i - 1) - (h_i - 1) - (l_i - 1)\big] \end{aligned}$$

and so

$$\psi(x' + I_G^2) = \Big(\prod_i h_i l_i h_i^{-1} l_i^{-1}\Big)\psi(x + I_G^2) = \psi(x + I_G^2)$$

since G/G' is abelian. Clearly ψ is surjective.

Since $G' \subseteq \ker \phi$, ϕ defines a homomorphism

$$\bar{\phi} : G/G' \longrightarrow I_G/I_G^2$$

and clearly $\bar{\phi} \circ \psi = \mathrm{id}_{I_G/I_G^2}$. The surjectivity of ψ then shows $\bar{\phi}$ is injective, so $\ker \phi \subseteq G'$.

So we obtain that $H_1(G, \mathbb{Z}) \cong G/G'$, so that we have a homology group equal to the abelianization of G.

1.4 Change of Group

Let G' and G be groups, and

$$\phi : G' \longrightarrow G$$

a homomorphism. Denote the standard resolutions of $\mathbb{Z}$ by free G'- and G-modules (see §1.2) by

$$\mathbf{P}(G') \text{ and } \mathbf{P}(G)$$

respectively. Then ϕ induces a morphism of complexes

$$\begin{array}{ccccccccc}
\ldots \rightarrow & P_2(G') & \rightarrow & P_1(G') & \rightarrow & P_0(G') & \rightarrow & \mathbb{Z} & \rightarrow 0 \\
 & \downarrow\phi_2 & \square & \downarrow\phi_1 & \square & \downarrow\phi_0 & \square & \| & \\
\ldots \rightarrow & P_2(G) & \rightarrow & P_1(G) & \rightarrow & P_0(G) & \rightarrow & \mathbb{Z} & \rightarrow 0
\end{array}$$

by taking a typical $\mathbb{Z}$-generator $g'_0[g'_1, \ldots, g'_q]$ of $P_q(G')$ to $\phi(g'_0)[\phi(g'_1), \ldots, \phi(g'_q)]$.

Now suppose A is a G-module. Then A is also a G' module via $g'a := \phi(g')a$ for $g' \in G', a \in A$. Thus we can apply the contravariant functor $\mathrm{Hom}_G(?, A)$ to the induced maps ϕ_q:

$$\mathrm{Hom}_G(P_q(G), A) \longrightarrow \mathrm{Hom}_G(P_q(G'), A) \subseteq \mathrm{Hom}_{G'}(P_q(G'), A)$$

where the last inclusion is a consequence of $\mathrm{im}\,\phi \subseteq G$. These together define a morphism of complexes[3]

$$\mathrm{Hom}_G(\mathbf{P}_{\mathbb{Z}}(G), A) \longrightarrow \mathrm{Hom}_{G'}(\mathbf{P}_{\mathbb{Z}}(G'), A)$$

Hence it gives a morphism of cohomological functors

$$H^q(G, A) \longrightarrow H^q(G', A)$$

A similar process can be done for homology, using the covariant functor $\otimes_{\mathbb{Z}[G]}A$ in place of $\mathrm{Hom}_G(?, A)$, giving morphisms $H_q(G', A) \longrightarrow H_q(G, A)$.

For the moment, we wish to define two morphisms:

Restriction: If H is a subgroup of G, and $\phi : H \hookrightarrow G$ is inclusion, then ϕ induces

$$\mathrm{Res}_{G/H} : H^q(G, A) \longrightarrow H^q(H, A)$$

For a cochain $f : G^q \longrightarrow A$, Res f is simply the restriction

$$f\Big|_{H^q} \longrightarrow A$$

In dimension 0, Res is the inclusion $A^G \hookrightarrow A^H$.

Inflation: If H is a normal subgroup of G, then A^H has the structure of a G/H module. Let $\phi : G \longrightarrow G/H$ be the quotient map, then ϕ induces a morphism

$$H^q(G/H, A^H) \longrightarrow H^q(G, A^H)$$

[3] $\mathbf{P}_{\mathbb{Z}}$ denoting the corresponding "deleted complex", ie. with $\mathbb{Z}$ removed.

We know that the inclusion $A^H \hookrightarrow A$ induces a morphism

$$H^q(G, A^H) \longrightarrow H^q(G, A)$$

So compose these to get

$$\mathrm{Inf} : H^q(G/H, A^H) \longrightarrow H^q(G, A)$$

For a q-cocycle $f : (G/H)^q \longrightarrow A^H$, Inf f is the map $G^q \longrightarrow A$ which takes $[g_1, \ldots, g_q]$ to $f[g_1H, \ldots, g_qH]$.

1.4.1 The Restriction-Inflation Sequence

Proposition 1.4.1 *Let H be a normal subgroup of G, A a G-module. Then the sequence*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G, A) \xrightarrow{\mathrm{Res}} H^1(H, A)$$

is exact.

Proposition 1.4.2 *If $H^i(H, A) = 0$ for $1 \leq i \leq q-1$ then the sequence*

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^q(G, A) \xrightarrow{\mathrm{Res}} H^q(H, A)$$

is exact

The first proposition is proved by direct verification on the inhomogeneous cochains. The second proposition follows from the first by dimension-shifting. For the proofs, see [1], Chapter 7, §6.

1.5 Cohomology of Finite Groups

1.5.1 The Tate Groups

If G is a group, then for an exact sequence of G-modules $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$, we have defined the long exact homology and cohomology sequences:

$$\begin{array}{cccccccc} \ldots \to H_1(G, C) & \xrightarrow{\delta} H_0(G, A) & \to H_0(G, B) & \to H_0(G, C) & \to & 0 & & \\ 0 & \to H^0(G, A) & \to H^0(G, B) & \to H^0(G, C) & \xrightarrow{\delta} & H^1(G, A) & \to \ldots \end{array}$$

When G is finite, these two sequences can be spliced together to form a doubly-infinite exact cohomology sequence. The tool for doing this is the element

$$N = \sum_{g \in G} g \in \mathbb{Z}[G]$$

called the *norm*. Multiplication by N defines a G-homomorphism $N : A \longrightarrow A^G$ because

$$Ng = gN = N \qquad \text{for all } g \in G$$

If I_G is the augmentation ideal of $\mathbb{Z}[G]$ (see §1.3), then $NI_G = 0$ because $N(g-1) = N - N = 0$ for each generator $g - 1$ of I_G. Hence $NI_GA = 0$, and N defines a G-homomorphism

$$N^* : A/I_GA \longrightarrow A^G$$

ie. $N^* : H_0(G, A) \longrightarrow H^0(G, A)$.

Definition 1.5.1 *Define*[4] $\hat{H}^{-1}(G, A) = \ker N^*$ *and* $\hat{H}^0(G, A) = \operatorname{coker} N^*$, *in other words*

$$\begin{array}{rclcl} \hat{H}^{-1}(G,A) & = & \ker N/I_GA & \subseteq & H_0(G,A) \\ \hat{H}^0(G,A) & = & A^G/NA & = & H^0(G,A)/NA \end{array}$$

The next definition brings in the rest of the homology and cohomology groups:

$$\begin{array}{rcll} \hat{H}^{-q}(G,A) & := & H_{q-1}(G,A) & \text{for } q > 2 \\ \hat{H}^{q}(G,A) & := & H^{q}(G,A) & \text{for } q > 1 \end{array}$$

These groups $\hat{H}^q(G, A), q \in \mathbb{Z}$ are called the *Tate cohomology groups of G with coefficients in A.*

Suppose now that

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

is an exact sequence of G-modules. Then the diagram

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

is commutative and has exact rows. Thus the *snake lemma* (0.1.3) shows that it defines a homomorphism

$$\delta : \ker N_C^* \longrightarrow \operatorname{coker} N_A^*$$

such that the sequence

$$\begin{array}{c} \ker N_A^* \longrightarrow \ker N_B^* \longrightarrow \ker N_C^* \xrightarrow{\delta} \operatorname{coker} N_A^* \\ \longrightarrow \operatorname{coker} N_B^* \longrightarrow \operatorname{coker} N_C^* \end{array} \tag{1.7}$$

is exact, ie.

$$\begin{array}{c} \hat{H}^{-1}(G,A) \longrightarrow \hat{H}^{-1}(G,B) \longrightarrow \hat{H}^{-1}(G,C) \xrightarrow{\delta} \hat{H}^0(G,A) \\ \longrightarrow \hat{H}^0(G,B) \longrightarrow \hat{H}^0(G,C) \end{array}$$

is exact.

[4] $\hat{H}^{-1}$ is also written $\hat{H}_0$, and $\ker N$ is also written ${}_NA$

Theorem 1.5.2 *Let G be a finite group and*

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

an exact sequence of G-modules. Then the definitions of $\delta : \hat{H}^{q-1}(G,C) \longrightarrow \hat{H}^q(G,A)$ from the exact cohomology and homology sequences, and from (1.7) above, give a doubly-infinite exact sequence

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

PROOF - In view of the exactness of the homology and cohomology sequences (1.6 and 1.3) we need only check that they fit together properly in the middle.

1. We need that the connecting homomorphism $\delta : H_1(G,C) \longrightarrow A/I_G A$ (in the notation of §1.3) is in fact a map into $\ker N_A/I_G A$, ie. $N_A \circ \delta = 0$.

   We represent an element of $H_1(G,C)$ as a one-dimensional chain $f : G \longrightarrow C$ (see §1.3). Calculate δf by lifting f to $h : G \longrightarrow B$ and applying the boundary formula:
   $$dh = \sum_{g \in G} g^{-1} f[g] - \sum_{g \in G} f[g] = \sum_{g \in G} (g^{-1} - 1) f[g]$$
   Applying $N \in \mathbb{Z}[G]$ to this gives $\sum_{g \in G} (N - N) f[g] = 0$ so $\delta f \in \ker N_A^*$. This was what we needed to show, and now the exactness of

   $$H_1(G,B) \longrightarrow H_1(G,C) \xrightarrow{\delta} H_0(G,A) \longrightarrow H_0(G,B)$$

   implies exactness of

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

2. We need exactness of

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

   which follows as above if we can show that the connecting homomorphism in

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

   is constant on the cosets of $\operatorname{im} N_C^*$ in $H^0(G,C)$, so that we may pass to the quotient. If $c \in H^0(G,C) = C^G$ is in $\operatorname{im} N_C^*$, lift c to $Nb \in B^G$, then $dc[g] = gNh - Nh = Nh - Nh = 0$, which is what we needed.

□

Proposition 1.5.3 *If G is finite, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X) \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ for any abelian group X. Hence a G-module A is co-induced if and only if it is induced.*

PROOF - The map

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X) & \longrightarrow & \mathbb{Z}[G] \otimes_{\mathbb{Z}} X \\ f & \longmapsto & \sum_g g \otimes f(g^{-1}) \end{array}$$

sends $sf, s \in G$ to

$$\sum_{g\in G} g \otimes f(s^{-1}g^{-1}) = \sum_{g'\in G} sg' \otimes f(g'^{-1}) = s(\sum_{g'\in G} g' \otimes f(g'^{-1}))$$

and so is a G-homomorphism. The inverse map takes a general element $\sum_g g \otimes x_g$ to the map $\mathbb{Z}[G] \longrightarrow X$, $g \longmapsto x_{g^{-1}}$.

□

Corollary 1.5.4 *A is relatively injective if and only if it is relatively projective.*

Remark 1.5.5 *Note that if A is G-induced, then A is H-induced for any subgroup H of G. This is easy to see by considering $\mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ as a direct sum*

$$\bigoplus_{g\in G} g \cdot X = \bigoplus_{h\in H} h \cdot Y$$

where $Y = \bigoplus_{t\in T} t \cdot X$ for T a system of representatives of the cosets tH in G.

Definition 1.5.6 *If G is a finite group, a G-module A is called* cohomologically trivial *if $\hat{H}^q(H, A) = 0$ for every $q \in \mathbb{Z}$ and every subgroup H of G.*

Proposition 1.5.7 *If A is an induced G-module then A is cohomologically trivial.*

PROOF - By Remark 1.5.5, it is sufficient to check that $H^q(G, A) = 0$ for all $q \in \mathbb{Z}$. We know (§1.3) that $\hat{H}^{-2}(G, A), \hat{H}^{-3}(G, A), \ldots$ are all zero. By Proposition 1.5.3, A is co-induced, so §1.1 shows $\hat{H}^1(G, A), \hat{H}^2(G, A), \ldots$ are all zero. So we just have to show $\hat{H}^0(G, A)$ and $\hat{H}^{-1}(G, A)$ are zero.

Now $A = \mathbb{Z}[G] \otimes_{\mathbb{Z}} X$ for some abelian group X, so every element can be written uniquely in the form $\sum_{g\in G} g \otimes x_g$ for some $x_g \in X$. $\hat{H}^{-1}(G, A) = \ker N/I_G A$ so suppose $a = \sum g \otimes x_g \in \ker N$. So

$$\begin{aligned} 0 &= \textstyle\sum_{s\in G} s \sum_{g\in G} g \otimes x_g = \sum_{g\in G} \sum_{s\in G} sg \otimes x_g \\ &= \textstyle\sum_{g\in G} \sum_{s\in G} g \otimes x_{s^{-1}g} = \sum_{g\in G} g \otimes (\sum_{t\in G} x_t) \end{aligned}$$

Hence $\sum_{t\in G} x_t = 0$ and so

$$a = \sum_{g\in G} (g-1) \otimes x_g \in I_G A$$

as required.

For the next group, $\hat{H}^0(G, A) = A^G/NA$, take a general element $a = \sum g \otimes x_g \in A^G$. Then $sa = \sum sg \otimes x_g = \sum g \otimes x_g$ for all $s \in G$ so that $x_1 = x_s$ for all $s \in G$ and consequently $a \in NA$.

□

1.5.2 Dimension Shifting of Tate Cohomology Groups

Let $A^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$ be the canonical co-induced module associated to A (see Proposition 1.1.8), and $A_* = \mathbb{Z}[G] \otimes_{\mathbb{Z}} A_+$ the canonical induced module associated to A (see §1.3). If G is finite, $A^* = A_*$ by Proposition 1.5.3. The dimension-shifting sequences

$$0 \longrightarrow A \longrightarrow A^* \longrightarrow A' \longrightarrow 0$$

$$0 \longrightarrow A' \longrightarrow A_* \longrightarrow A \longrightarrow 0$$

express A as a submodule or as a quotient module of a cohomologically trivial G-module, and so allow dimension-shifting up and down.

Let us now look at some results which show how dimension-shifting is a "nice" process, by which we mean that the forming of the two dimension-shift sequences above constitute functors from the category of G-modules to the category of short exact sequences of G-modules. These four results are needed for the proof of Tate's Theorem (1.6.4).

Lemma 1.5.8 *Let $f : B \longrightarrow C$ be a G-homomorphism. Then there exists a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B' & \longrightarrow & B_* & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow_{f'} & \Box & \downarrow_{f''} & \Box & \downarrow_{f} & & \\ 0 & \longrightarrow & C' & \longrightarrow & C_* & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

PROOF - Recall $B_* \longrightarrow B$ is given by $g \otimes b \longmapsto gb$. Define $f''(g \otimes b) = g \otimes f(b)$. It is easy to check that f'' is a G-homomorphism, the second square is commutative, and it follows from this that the restriction of f'' to $B' \subseteq B_*$ is a function into C'.

$\Box$

Lemma 1.5.9 *Let $\phi : A \otimes_{\mathbb{Z}} B \longrightarrow C$ be a G-homomorphism. Then there exists a commutative diagram with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \otimes_{\mathbb{Z}} B' & \longrightarrow & A \otimes_{\mathbb{Z}} B_* & \longrightarrow & A \otimes_{\mathbb{Z}} B & \longrightarrow & 0 \\ & & \downarrow_{\phi'} & \Box & \downarrow_{\phi''} & \Box & \downarrow_{\phi} & & \\ 0 & \longrightarrow & C' & \longrightarrow & C_* & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

PROOF - The top row is exact because

$$0 \longrightarrow B' \longrightarrow B_* \longrightarrow B \longrightarrow 0$$

is a $\mathbb{Z}$-split exact sequence, as is shown by the $\mathbb{Z}$-homomorphism $B \longrightarrow B_*, b \longmapsto 1 \otimes b$.

Define

$$\begin{array}{rccc} \phi'' : & A \otimes_{\mathbb{Z}} B_* & \longrightarrow & C_* \\ & a \otimes g \otimes b & \longmapsto & g \otimes \phi(g^{-1}a \otimes b). \end{array}$$

Then $\phi''(s(a \otimes g \otimes b)) = \phi''(sa \otimes sg \otimes b) = sg \otimes \phi(g^{-1}ss^{-1}a \otimes b) = s\phi''(a \otimes g \otimes b)$, so ϕ'' is a G-homomorphism. Commutativity of the second square can easily be checked, and the rest follows.

$\square$

Similar results apply for dimension-shifting in the other direction, when B is expressed as a submodule of a co-induced module.

Lemma 1.5.10 *Let $f : B \longrightarrow C$ be a G-homomorphism. Then there exists a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & B^* & \longrightarrow & B' & \longrightarrow & 0 \\ & & \downarrow f & \square & \downarrow f'' & \square & \downarrow f' & & \\ 0 & \longrightarrow & C & \longrightarrow & C^* & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

PROOF - If $\beta \in B^*$, let

$$\begin{array}{rccc} f''(\beta) : & \mathbb{Z}[G] & \longrightarrow & C \\ & g & \longmapsto & f(\beta(g)) \end{array}$$

This is a G-homomorphism and the first square commutes. General properties of diagrams then show that f'' defines f' making the second square commute, since the composition

$$\begin{array}{ccc} B^* & & \\ \downarrow f'' & & \\ C^* & \longrightarrow & C' \end{array}$$

carries the submodule B to zero.

$\square$

Lemma 1.5.11 *Let $\phi : A \otimes_{\mathbb{Z}} B \longrightarrow C$ be a G-homomorphism. Then there exists a commutative diagram with exact rows*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A \otimes_{\mathbb{Z}} B & \longrightarrow & A \otimes_{\mathbb{Z}} B^* & \longrightarrow & A \otimes_{\mathbb{Z}} B' & \longrightarrow & 0 \\ & & \downarrow \phi & \square & \downarrow \phi'' & \square & \downarrow \phi' & & \\ 0 & \longrightarrow & C & \longrightarrow & C^* & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

PROOF - The top row is exact because

$$0 \longrightarrow B \longrightarrow B^* \longrightarrow B' \longrightarrow 0$$

is a $\mathbb{Z}$-split exact sequence, as is shown by the $\mathbb{Z}$-homomorphism $B^* \longrightarrow B, \beta \longmapsto \beta(1)$.

Define for $\beta \in B^*$

$$\begin{array}{rccc} \phi''(a \otimes \beta) : & \mathbb{Z}[G] & \longrightarrow & C \\ & g & \longmapsto & \phi(g^{-1}a \otimes \beta(g)). \end{array}$$

This map carries $s(a \otimes \beta) = sa \otimes (g \mapsto \beta(s^{-1}g))$ to

$$\big(g \mapsto \phi(g^{-1}sa \otimes \beta(s^{-1}g))\big) = \big(g \mapsto \phi((s^{-1}g)^{-1}a \otimes \beta(s^{-1}g))\big)$$

which is $s\phi''(a \otimes \beta)$. So ϕ'' is a G-homomorphism. It is easy to check the commutativity of the first square, and then the properties of ϕ' follow.

$\square$

1.5.3 Complete Resolutions

In §1.5.1 we defined the doubly-infinite sequence of Tate cohomology groups, by piecing together the cohomology and homology groups. There is another way to define this sequence, which is more elegant but less explicit. We start with a resolution of the G-module $\mathbb{Z}$ (with trivial G-action) by finitely-generated free G-modules:

$$\ldots \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0 \tag{1.8}$$

and apply the contravariant functor $\mathrm{Hom}_{\mathbb{Z}}(?, \mathbb{Z})$ to obtain the *dual* sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\epsilon^*} P_0^* \longrightarrow P_1^* \longrightarrow \ldots$$

so $P_i^* = \mathrm{Hom}_{\mathbb{Z}}(P_i, \mathbb{Z})$, the sequence being exact because the P_i are $\mathbb{Z}$-free (see Lemma 1.1.10 and the proof of the result which follows it).

Putting these together gives an exact sequence

$$\ldots \longrightarrow P_1 \longrightarrow P_0 \xrightarrow{\epsilon^* \circ \epsilon} P_0^* \longrightarrow P_1^* \longrightarrow \ldots$$

and we apply the functor $\mathrm{Hom}_G(?, A)$ to obtain the complex

$$\mathbf{K}: \qquad \ldots \longrightarrow \mathrm{Hom}_G(P_1^*, A) \longrightarrow \mathrm{Hom}_G(P_0^*, A) \longrightarrow \mathrm{Hom}_G(P_0, A) \longrightarrow \ldots$$

The Tate groups are now the cohomology groups of this complex, namely $\hat{H}^q(G, A) = H^q(\mathbf{K})$. For more details and proof, see [3].

1.5.4 The Cup Product

Theorem 1.5.12 *Let G be a finite group. Then there exists a unique family of homomorphisms*

$$\hat{H}^p(G, A) \otimes_{\mathbb{Z}} \hat{H}^q(G, B) \longrightarrow \hat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} B)$$

(denoted $a \otimes b \longmapsto a \cdot b$) defined for all integers p, q and all G-modules A, B, such that

1. *The homomorphisms are functorial in A and B (considering each side as a covariant bifunctor in (A,B)). Namely, if $f : A \longrightarrow A'$ and $g : B \longrightarrow B'$ are G-homomorphisms, the diagram*

$$\begin{array}{ccc} \hat{H}^p(G, A) \otimes_{\mathbb{Z}} \hat{H}^q(G, B) & \longrightarrow & \hat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} B) \\ \downarrow f^* \otimes g^* & & \downarrow (f \otimes g)^* \\ \hat{H}^p(G, A') \otimes_{\mathbb{Z}} \hat{H}^q(G, B') & \longrightarrow & \hat{H}^{p+q}(G, A' \otimes_{\mathbb{Z}} B') \end{array}$$

   is commutative.

2. *For $p = q = 0$ they are induced by the inclusion*

$$A^G \otimes_{\mathbb{Z}} B^G \hookrightarrow (A \otimes_{\mathbb{Z}} B)^G$$

3. *If $0 \to A \to A'' \to A' \to 0$ is an exact sequence of G-modules, and if $0 \to A \otimes_{\mathbb{Z}} B \to A'' \otimes_{\mathbb{Z}} B \to A' \otimes_{\mathbb{Z}} B \to 0$ is exact, then for $a' \in \hat{H}^p(G, A')$ and $b \in \hat{H}^q(G, B)$ we have*

$$(\delta a') \cdot b = \delta(a' \cdot b) \qquad \text{(in } \hat{H}^{p+q+1}(G, A \otimes_{\mathbb{Z}} B)\text{)}$$

4. *If $0 \to B \to B'' \to B' \to 0$ is an exact sequence of G-modules, and if $0 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B'' \to A \otimes_{\mathbb{Z}} B' \to 0$ is exact, then for $a \in \hat{H}^p(G, A)$ and $b' \in \hat{H}^q(G, B)$ we have*

$$a \cdot (\delta b') = (-1)^p \delta(a \cdot b') \qquad \text{(in } \hat{H}^{p+q+1}(G, A \otimes_{\mathbb{Z}} B)\text{)}$$

The proof of this can be found in [3], p106. I will sketch it here.

Let P_q be a complete resolution of $\mathbb{Z}$ as described in the last section. We need to map a pair of cochains $f \in \mathrm{Hom}_G(P_p, A)$ and $g \in \mathrm{Hom}_G(P_q, B)$ to a cochain $f \cdot g \in \mathrm{Hom}_G(P_{p+q}, A \otimes_{\mathbb{Z}} B)$. The tensor product

$$\begin{array}{rccc} f \otimes g: & P_p \otimes_{\mathbb{Z}} P_q & \longrightarrow & A \otimes_{\mathbb{Z}} B \\ & a \otimes b & \longmapsto & f(a) \otimes g(b) \end{array}$$

is the starting point, and we consider composing it with a G-homomorphism

$$\phi_{p,q} : P_{p+q} \longrightarrow P_p \otimes_{\mathbb{Z}} P_q$$

to obtain a G-homomorphism from P_{p+q} to $A \otimes_{\mathbb{Z}} B$. Suppose we can find such a ϕ with the following two properties:

- a $\phi_{p,q} \circ d = (d \otimes 1) \circ \phi_{p+1,q} + (-1)^p (1 \otimes d) \circ \phi_{p,q+1}$, where d is the coboundary map in the resolution;
- b $(\epsilon \otimes \epsilon) \circ \phi_{0,0} = \epsilon$, where ϵ is as in (1.8).

Then we find that the cochain $f \cdot g$ has all the properties required for the cup product. Property (a) shows that a pair of cocycles maps to a cocycle, whose cohomology class depends only on their ones. Thus we do have a homomorphism $\hat{H}^p(G, A) \otimes_{\mathbb{Z}} \hat{H}(G, B) \longrightarrow \hat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} B)$. That this satisfies the first condition of the theorem can be seen by looking at how maps are induced between the $\hat{H}^q$.

Let us demonstrate the second requirement. Recall that the exact sequence

$$P_1 \xrightarrow{d_0} P_0 \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

gives an exact sequence

$$0 \longrightarrow \mathrm{Hom}_G(\mathbb{Z}, A) \xrightarrow{\epsilon} \mathrm{Hom}_G(P_0, A) \xrightarrow{d_0} \mathrm{Hom}_G(P_1, A),$$

and similarly for B and $A \otimes_{\mathbb{Z}} B$. So if $\alpha \in \mathrm{Hom}_G(P_0, A)$ is a cocycle, then $\alpha \in \mathrm{im}\,\epsilon$ so that $\alpha = a \circ \epsilon$ for some $a : \mathbb{Z} \longrightarrow A$. Similarly if $\beta \in \mathrm{Hom}_G(P_0, B)$ is a cocycle, $\beta = b \circ \epsilon$ for $b : \mathbb{Z} \longrightarrow B$. Thus

$$\begin{aligned} \alpha \cdot \beta &= (a \circ \epsilon \otimes b \circ \epsilon) \circ \phi_{0,0} \\ &= (a \otimes b) \circ (\epsilon \otimes \epsilon) \circ \phi_{0,0} \\ &= (a \otimes b) \circ \epsilon \; = \; \alpha \otimes \beta : P_0 \longrightarrow A \otimes_{\mathbb{Z}} B, \end{aligned}$$

which shows that $\cdot$ is induced by the inclusion $(A^G \otimes_{\mathbb{Z}} B^G) \hookrightarrow (A \otimes_{\mathbb{Z}} B)^G$, remembering that $a \in A^G$ is identified with a G-homomorphism $\mathbb{Z} \longrightarrow A, 1 \longmapsto a$.

Properties (3) and (4) are checked by verifying that the various stages in the evaluation of the connecting homomorphism in question are represented by the appropriate cup-products of cochains of A and B, using property (b).

Now we define ϕ, after Atiyah and Wall in [3]. We use the complete resolution by *homogeneous cochains* (see §1.2). So

$$Q_q = \mathbb{Z}[G^{q+1}] \qquad \text{for } q \geq 0$$

$$Q_{-q} = Q^*_{q-1} = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G^q], \mathbb{Z}) \qquad \text{for } q \geq 1$$

and a basis for Q_{-q} is given by homomorphisms of the form $(g_1^*, \ldots, g_q^*)$, which means the map which takes $(g_1, \ldots, g_q) \in G^q$ to 1 and all other basis elements to zero. The G-action is then $s(g_1^*, \ldots, g_q^*) = ((sg_1)^*, \ldots, (sg_q)^*)$, and the coboundary

$$\begin{array}{rccc} d: & Q_{-q} & \longrightarrow & Q_{-q-1} \\ & (g_1^*, \ldots, g_q^*) & \longmapsto & \sum_{s \in G} \sum_{i=0}^{q} (-1)^i (g_1^*, \ldots, g_i^*, s^*, g_{i+1}^*, \ldots g_q^*) \end{array}$$

for $q \geq 1$, and

$$\begin{array}{rccc} d: & Q_0 & \longrightarrow & Q_{-1} \\ & (g_0) & \longmapsto & \sum_{s \in G} (s^*). \end{array}$$

Then $\phi_{p,q} : Q_{p+q} \longrightarrow Q_p \otimes_{\mathbb{Z}} Q_q$ is defined by

- If $p \geq 0$ and $q \geq 0$,

$$\phi_{p,q}(g_0, \ldots, g_{p+q}) = (g_0, \ldots, g_p) \otimes (g_p, \ldots, g_{p+q})$$

- If $p \geq 1$ and $q \geq 1$,

$$\phi_{-p,-q}(g_1^*, \ldots, g_{p+q}^*) = (g_1^*, \ldots, g_p^*) \otimes (g_{p+1}^*, \ldots, g_{p+q}^*)$$

- If $p \geq 0$ and $q \geq 1$,

$$\begin{aligned} \phi_{p,-p-q}(g_1^*, \ldots, g_q^*) &= \sum (g_1, s_1, \ldots, s_p) \otimes (s_p^*, \ldots, s_1^*, g_1^*, \ldots, g_q^*) \\ \phi_{-p-q,p}(g_1^*, \ldots, g_q^*) &= \sum (g_1^*, \ldots, g_q^*, s_1^*, \ldots, s_p^*) \otimes (s_p, \ldots, s_1, g_q) \\ \phi_{p+q,-q}(g_0, \ldots, g_p) &= \sum (g_0, \ldots, g_p, s_1, \ldots, s_q) \otimes (s_q^*, \ldots, s_1^*) \\ \phi_{-q,p+q}(g_0, \ldots, g_p) &= \sum (s_1^*, \ldots, s_q^*) \otimes (s_q, \ldots, s_1, g_0, \ldots, g_p) \end{aligned}$$

In the sums on the right-hand side, the s_i run independently through G.

1.5.5 Restriction and Corestriction

Recall from §1.4 that the *restriction homomorphism* was defined for the cohomology groups

$$\mathrm{Res} : H^q(G, A) \longrightarrow H^q(H, A)$$

for any subgroup H of G. The dimension-shifting of §1.5.2 shows it can be extended to all the Tate groups $\hat{H}^q$. Res is the unique morphism of Tate cohomology functors which is induced in dimension 0 by the inclusion $A^G \subseteq A^H$.

The *corestriction* is a morphism in the other direction

$$\mathrm{Cor} : \hat{H}^q(H, A) \longrightarrow \hat{H}^q(G, A)$$

induced in dimension zero by the norm map

$$\begin{array}{rccc} N_{G/H} : & A^H & \longrightarrow & A^G \\ & a & \longmapsto & \sum_i s_i a \end{array}$$

where $G/H = \{s_1 H, \ldots, s_{(G:H)} H\}$. This extends by dimension shifting to all the Tate groups.

Proposition 1.5.13 Cor $\circ$ Res *is multiplication by* $(G : H)$.

PROOF - This is clear in dimension zero. So if f denotes multiplication by $(G : H)$, then Cor$\circ$Res$-f$ is a morphism of cohomological functors which is zero in dimension zero for all G-modules. By dimension-shifting, it is zero in all dimensions.

□

Corollary 1.5.14 *If* $|G| = n$ *then* $n\hat{H}^q(G, A) = 0$ *for all* G*-modules* A *and all* $q \in \mathbb{Z}$.

PROOF - Set $H = \{1\}$, then $\hat{H}^q(G, A) = 0$ because H-module means the same as $\mathbb{Z}$-module, and so all H-modules are induced, and so cohomologically trivial. Now Res is the zero map, and so Cor $\circ$ Res is the zero map, and is equal to multiplication by n.

□

Corollary 1.5.15 *If* A *is a finitely-generated* G*-module then the* $\hat{H}^q(G, A)$ *are finite groups.*

PROOF - The definition in terms of the standard resolution shows they are finitely-generated groups. By the previous corollary, the generators have order at most n, so that the groups are actually finite.

□

1.6 Tate's Theorem

Tate's Theorem is the central result of finite group cohomology which we want to apply to Number Theory. To prove this theorem, a lengthy and technical diversion into the cohomology of p-groups is necessary, and was carried out by Tate and Nakayama. Good accounts of this can be found in [1], Chapter 9, and [3]. Space considerations prevent us from presenting the discussion here, so we state only the conclusion.

By Sylow's Theorem ([1], Chapter 9), a group of order $\prod p^{m_p}$ contains subgroups of order p^{m_p} for each p, called *Sylow p-subgroups of G*. For a given p, any two such subgroups are conjugate in G. We choose a system of Sylow subgroups $\{G_p : p \text{ prime}\}$ in G.

Theorem 1.6.1 *Let A be a G-module, where G is a finite group. Suppose that for each p there is $q_p \in \mathbb{Z}$ such that*

$$\hat{H}^{q_p}(G_p, A) = \hat{H}^{q_p+1}(G_p, A) = 0.$$

Then A is cohomologically trivial.

We use this result to prove an isomorphism criterion:

Theorem 1.6.2 *Let G be a finite group, B and C two G-modules, and $f : B \longrightarrow C$ a G-homomorphism. For each prime p, suppose there exists an integer n_p such that*

$$f_n^* : \hat{H}^n(G_p, B) \longrightarrow \hat{H}^n(G_p, C)$$

is surjective for $n = n_p$, bijective for $n = n_p + 1$ and injective for $n = n_p + 2$. Then for any subgroup H of G and any integer n,

$$f_n^* : \hat{H}^n(H, B) \longrightarrow \hat{H}^n(H, C)$$

is an isomorphism.

PROOF - Let $B^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], B_+)$ and $i : B \longrightarrow B^*$ the injection of Proposition 1.1.8. Then $f \times i : B \longrightarrow C \oplus B^*$ is injective, giving an exact sequence

$$0 \longrightarrow B \longrightarrow C \oplus B^* \longrightarrow D \longrightarrow 0.$$

B^* is cohomologically trivial so the cohomology of $C \oplus B^*$ is the same as that of C (see Lemma 1.1.9).

Then one may check that the exact cohomology sequence for G_p shows $\hat{H}^{n_p}(G_p, D) = \hat{H}^{n_p+1}(G_p, D) = 0$. Hence by the previous theorem, D is a cohomologically trivial G-module, so the exact cohomology sequence for $H < G$ gives the result.

□

Tate's Theorem will follow from the next general result.

Theorem 1.6.3 *Let A,B and C be three G-modules and*

$$\phi : A \otimes_{\mathbb{Z}} B \longrightarrow C$$

a G-homomorphism. Fix an integer q and an element $a \in \hat{H}^q(G, A)$. Write $\cdot$ for the cup-product *(see §1.5.4).*

Suppose that for all p there is an integer n_p such that the function

$$\begin{array}{ccc} \hat{H}^n(G_p, B) & \longrightarrow & \hat{H}^{n+q}(G_p, C) \\ x & \longmapsto & \phi^*(\mathrm{Res}_{G/G_p}(a) \cdot x) \end{array}$$

is surjective for $n = n_p$, bijective for $n = n_p + 1$ and injective for $n = n_p + 2$.

Then for all subgroups H of G and all $n \in \mathbb{Z}$,

$$\begin{array}{ccc} \hat{H}^n(H, B) & \longrightarrow & \hat{H}^{n+q}(H, C) \\ x & \longmapsto & \phi^*(\mathrm{Res}_{G/H}(a) \cdot x) \end{array}$$

is an isomorphism.

PROOF - As the first step, we deal with the case $q = 0$. We choose $\alpha \in A^G$ representing a (so α also represents $\mathrm{Res}_{G/H}(a)$ for all subgroups H of G). Define

$$\begin{array}{cccc} f_\phi : & B & \longrightarrow & C \\ & b & \longmapsto & \phi(\alpha \otimes b). \end{array}$$

f_ϕ is a G-homomorphism, since α is G-invariant.

We claim that for all $b \in \hat{H}^n(H, B)$, and any ϕ,

$$\phi^*(\mathrm{Res}_{G/H}(a) \cdot b) = f_\phi^*(b).$$

The claim is clearly true for $n = 0$. It is proved for the other n by dimension-shifting. For example, suppose it is true for $n - 1$, for all modules and ϕ's. From Lemma 1.5.10 we obtain a commutative diagram

$$\begin{array}{ccc} \hat{H}^{n-1}(H, B') & \xrightarrow[\sim]{\delta} & \hat{H}^n(H, B) \\ \downarrow f'^* & \Box & \downarrow f_\phi^* \\ \hat{H}^{n-1}(H, C') & \xrightarrow[\sim]{\delta} & \hat{H}^{n-1}(H, C) \end{array}$$

and from Lemma 1.5.11 we obtain a map $\phi' : A \otimes_{\mathbb{Z}} B' \longrightarrow C'$. It is easy to check from the definitions that $f' = f_{\phi'}$. So the inductive hypothesis shows

$$\phi'^*(\mathrm{Res}_{G/H}(a) \cdot b) = f'^*(b).$$

Then for each b' in B',

$$\begin{aligned} f^*(\delta b') &= \delta(f'(b')) \\ &= \delta\phi'^*(\mathrm{Res}_{G/H}(a)\cdot b') \\ &= \phi^*(\delta(\mathrm{Res}_{G/H}(a)\cdot b')) \qquad \text{by Lemma 1.5.11} \\ &= \phi^*(\mathrm{Res}_{G/H}(a)\cdot \delta b'). \end{aligned}$$

Since every $b \in B$ is of the form $\delta b'$, this proves the claim.

One may carry out the dimension-shifting from $n+1$ to n in an entirely similar way, using Lemmas 1.5.8 and 1.5.9.

Having proved the claim, we need only to apply the previous theorem to obtain the stated result for $q = 0$.

Step 2: We vary q. Suppose the statement is true for $q+1$. Let

$$0 \longrightarrow A' \longrightarrow A_* \longrightarrow A \longrightarrow 0$$

be an exact sequence with $A_* = \mathbb{Z}[G]\otimes_{\mathbb{Z}} A_+$. Then $\hat{H}^q(G,A) \xrightarrow[\sim]{\delta} \hat{H}^{q+1}(G,A')$ is an isomorphism. Put $a' = \delta a$, and note that $\mathrm{Res}_{G/H}(a') = \delta\mathrm{Res}_{G/H}(a)$ since Res is a morphism of cohomological functors.

From Lemma 1.5.9 we obtain a map

$$\phi'^* : \hat{H}^{n+q+1}(G_p, A'\otimes_{\mathbb{Z}} B) \longrightarrow \hat{H}^{n+q+1}(G_p, C').$$

We have the commutative diagram

$$\begin{array}{ccc} \hat{H}^n(G_p,B) & = & \hat{H}^n(G_p,B) \\ \downarrow\otimes\mathrm{Res}(a) & \square & \downarrow\otimes\mathrm{Res}(a') \\ \hat{H}^n(G_p,B)\otimes_{\mathbb{Z}}\hat{H}^q(G_p,A) & \xrightarrow{1\otimes\delta} & \hat{H}^n(G_p,B)\otimes_{\mathbb{Z}}\hat{H}^{q+1}(G_p,A') \\ \downarrow\cdot & \square & \downarrow\cdot \\ \hat{H}^{n+q}(G_p,A\otimes_{\mathbb{Z}} B) & \xrightarrow{\delta} & \hat{H}^{n+q+1}(G_p,A'\otimes_{\mathbb{Z}} B) \\ \downarrow\phi^* & \square & \downarrow\phi'^* \\ \hat{H}^{n+q}(G,C) & \xrightarrow{\delta} & \hat{H}^{n+q+1}(G,C) \end{array}$$

In this diagram, the first square commutes because Res is a morphism of cohomological functors, the second by the properties of the cup product, and the third by Lemma 1.5.9.

This diagram shows that when the map $\hat{H}^n(G_p,B) \longrightarrow \hat{H}^{n+q+1}(G,C')$ given by the second column is surjective or injective, then so is the corresponding map given by the first column. This allows for the induction in the downwards direction. Lemma 1.5.11 works just the same to show induction in the other direction.

$\square$

We want the following special case of this.

Theorem 1.6.4 (Tate) *Let G be a finite group, A a G-module, and a an element of $H^2(G, A)$. For each prime p let G_p be a Sylow subgroup of G, and assume*

1. $H^1(G_p, A) = 0$,
2. $H^2(G_p, A)$ *is generated by* $\mathrm{Res}_{G/G_p}(a)$ *and has order equal to that of* G_p.

Then for all subgroups H of G and all $n \in \mathbb{Z}$, the map[5]

$$\begin{array}{ccc} \hat{H}^n(H, \mathbb{Z}) & \longrightarrow & \hat{H}^{n+2}(H, A) \\ x & \longmapsto & x \cdot \mathrm{Res}_{G/H}(a) \end{array}$$

is an isomorphism.

PROOF - Set $B = \mathbb{Z}, C = A, q = 2, n_p = -1$ in Theorem 1.6.3. For $n = -1$, $\hat{H}^{-1}(G_p, \mathbb{Z}) \longrightarrow \hat{H}^1(G_p, A)$ is surjective by (1). For $n = 0$, we have a map defined on $\hat{H}^0(G_p, \mathbb{Z}) = \mathbb{Z}/|G_p|\mathbb{Z}$ (see Definition 1.5.1). We claim that $1 \cdot \mathrm{Res}_{G/G_p}(a) = \mathrm{Res}_{G/G_p}(a)$, so that the generator 1 maps to a generator of $H^2(G_p, A)$, and then the equipotence condition shows the map is bijective. To see the claim, we use the cup-product formulae of §1.5.4. In the notation of that section, we have the G-homomorphism

$$\begin{array}{cccc} \phi_{0,2}: & Q_2 & \longrightarrow & Q_0 \otimes_{\mathbb{Z}} Q_2 \\ & (g_0, g_1, g_2) & \longmapsto & (g_0) \otimes (g_0, g_1, g_2) \end{array}$$

Represent $x \in \hat{H}^0(G_p, \mathbb{Z})$ by a homogeneous cochain $x \in \mathrm{Hom}_G(Q_0, \mathbb{Z})$ and $\mathrm{Res}_{G/G_p})(a)$ by $\alpha \in \mathrm{Hom}_G(Q_2, A)$. Then the cup-product is represented by the cochain

$$\begin{aligned} (x \cdot \alpha)(g_0, g_1, g_2) &= x(g_0) \otimes \alpha(g_0, g_1, g_2) \\ &= x(1) \otimes \alpha(g_0, g_1, g_2) \in \mathrm{Hom}_G(Q_2, \mathbb{Z} \otimes_{\mathbb{Z}} A). \end{aligned}$$

So if $x = 1$, $x \cdot \alpha = \alpha$, as required.

Finally, consider $n = 1$. We have $\hat{H}^1(G_p, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G_p, \mathbb{Z}) = 0$ and so the map is injective for $n = 1$.

Hence we have satisfied all the conditions of Theorem 1.6.3 and so Tate's Theorem is proved.

□

[5] identifying A with $A \otimes_{\mathbb{Z}} \mathbb{Z}$

Chapter 2

Galois Cohomology

2.1 Finite Galois Cohomology

[We refer to Appendix C for basic ideas and results of Galois Theory.]

Now we apply the cohomology of groups to studying fields. If L/K is a finite Galois extension, then the Galois group $G := \mathrm{Gal}(L/K)$ makes the additive and multiplicative groups of L into abelian G-modules. Thus we have two cohomology sequences, $\hat{H}^q(G, L)$ and $\hat{H}^q(G, L^*)$.

Theorem 2.1.1 *For every $q \in \mathbb{Z}$, $\hat{H}^q(G, L) = 0$.*

PROOF - By the normal basis theorem (C.2.6)

$$L = \bigoplus_{s \in G} s \cdot K = \mathbb{Z}[G] \otimes_{\mathbb{Z}} K$$

is an induced G-module, hence cohomologically trivial (noting G is finite, so induced is the same as co-induced by Proposition 1.5.3).

□

Next we investigate the multiplicative group L^*. Its cohomology groups are not all trivial. However, we have the very important result:

Theorem 2.1.2 *$H^1(G, L^*) = 0$, for any finite group G of automorphisms of L.*

PROOF - Let $f : G \longrightarrow L^*$ be a 1-cocycle. For $c \in L$, form the "Poincaré series"

$$b = \sum_{s \in G} f[s] \cdot sc$$

By Dedekind's lemma (C.1.9), the map $\sum_{s \in G} f[s] \cdot s$ is not identically zero, so c can be chosen so that $b \neq 0$. But $sb = \sum_{t \in G} sf[t] \cdot stc$, which using the 1-cocycle condition $f[st] = f[s] \cdot sf[t]$ is the same as

$$\sum_{t \in G} f[s]^{-1} \cdot f[st] \cdot stc = f[s]^{-1} \cdot b$$

since st runs through G as t does. Thus $f[s] = (sb)^{-1} \cdot b$ is a coboundary.

□

Corollary 2.1.3 (Hilbert's Theorem 90) *If $G = \mathrm{Gal}(L/K) =< s >$ is finite cyclic, and $x \in L^*$ has $N_{L/K}x = 1$, then $x = y/sy$ for some $y \in L^*$.*

PROOF - Define $f : G \longrightarrow L^*$ by $f[1] = 1$, $f[s] = x, \ldots, f[s^n] = x \cdot sx \cdot s^2x \cdot \ldots \cdot s^{n-1}x$. Then $f[s^n]$ depends only on s^n and not n because the norm of x is 1. Furthermore, $f[s^n s^m] = f[s^n] \cdot s^n f[s^m]$, so that f is a 1-cocycle. Hence f is a 1-coboundary, so $x = f[s] = y/sy$.

□

Note that Theorem 2.1.2 is also sometimes called Hilbert's Theorem 90.

It can be shown by extending this argument that:

Proposition 2.1.4 $H^1(G, \mathbf{GL}(n, L)) = 0$

See [1], Chapter 10, §1, Proposition 3 for more details. This result will be used when we study the Brauer group later on.

The remainder of this chapter will be spent showing how to extend the ideas of Galois correspondence and cohomology to infinite extensions.

2.2 Infinite Galois Theory

2.2.1 The Krull Topology

Let L/K be a Galois[1] extension, and $G = \mathrm{Gal}(L/K)$ the group of K-automorphisms of L. If L/K is finite, the Fundamental Theorem of Galois Theory (C.1.8) says that the intermediate subfields are in bijective correspondence with the subgroups of G. In the more general case, this is not always true - there may be more subgroups than subfields.

The solution is to turn G into a *topological group*. The reader is referred to Appendix D for the facts about topological groups that we need.

For $G = \mathrm{Gal}(L/K)$ we define a canonical topology, called the *Krull topology*, as follows. The nonempty open sets are defined to be all unions of the cosets

$$\sigma \mathrm{Gal}(L/E) : \sigma \in G, E/K \text{ is a finite Galois extension.}$$

We claim that the subset

$$\{\mathrm{Gal}(L/E) : E/K \text{ is a finite Galois extension}\}$$

forms a fundamental system of neighbourhoods of the identity in the sense of Definition D.0.7. The required properties follow easily from finite Galois theory. For example:

[1] meaning normal and separable.

Proposition 2.2.1 *If L/K is Galois, $\bigcap_E \mathrm{Gal}(L/E) = \{1\}$.*

PROOF - Let $\sigma \in \mathrm{Gal}(L/E) - \{1\}$. We want to show there is a finite Galois extension E' of K contained in L such that $\sigma \notin \mathrm{Gal}(L/E')$, ie. σ does not fix E' pointwise. But $\sigma \neq 1$ so there is $y \in L$ with $\sigma y \neq y$. By finite Galois theory, there is a finite Galois extension E' of K contained in L with $y \in E'$.

□

Definition 2.2.2 *A topological group which is compact, and has a fundamental system of open neighbourhoods of the identity consisting of normal subgroups is called a* profinite group.

We will see later that a Galois group with the Krull topology is compact, so that Galois groups are profinite.

2.2.2 Open and Closed Subgroups

Proposition 2.2.3 *For any topological group G, every open subgroup is also closed.*

PROOF - Let H be an open subgroup. Then the cosets $sH, s \in G$ partition G, and are open. Then

$$H = G - \bigcup_{s \notin H} sH$$

is the complement of an open set and so is closed.

□

Hence the open subgroups are special cases of the closed subgroups. Not all closed subgroups are necessarily open. If H is a closed subgroup of G with *finite index* in G, ie.

$$(G : H) = |G/H| < \infty$$

then H must be open in G. This is because, if $\{e, g_2, \ldots, g_n\}$ is a finite system of representatives of the set G/H of left-cosets, then

$$H = G - (g_2H \cup \ldots \cup g_nH) = (G - g_2H) \cap \ldots \cap (G - g_nH)$$

is a finite intersection of open sets and so is open. When G is *compact* this condition is also necessary:

Proposition 2.2.4 *Let G be a compact topological group and H a closed subgroup of G. Then H is open if and only if it has finite index in G.*

PROOF - One implication has been shown. So suppose H is open, then decompose G as

$$G = \bigcup_{s \in G} sH$$

This is an open covering of G, so there is a finite set $s_1, \ldots, s_n \in G$ such that $G = s_1H \cup \ldots \cup s_nH$. This shows that $(G : H)$ is finite.

□

2.2.3 Projective Limits

To characterise the profinite groups differently, we make use of the concept of projective limit.

Definition 2.2.5 *1. A* directed set *I is a set with a relation $\leq$ which is reflexive*[2] *and transitive*[3] *and has the property that, given $x, y \in I$, we can always find $z \in I$ with $x \leq z$ and $y \leq z$.*

2. An inverse system *of topological groups over a directed set I consists of an indexed collection of topological groups $G^i, i \in I$ and continuous homomorphisms $\pi_i^j : G^j \longrightarrow G^i$ for each pair $i \leq j$. We require that $\pi_i^i = \mathrm{id}_{G^i}$ and, if $i \leq j \leq k$, $\pi_i^j \circ \pi_j^k = \pi_i^k$.*

To an inverse system $\{G^i, \pi_i^j\}$ is associated a topological group called the *projective limit* (or sometimes the *inverse limit*) of the G^i, written $\varprojlim_i G^i$.

To define it, start with the product group $\prod_{i \in I} G^i$. This is a topological group as described in Appendix D. We define $\Lambda = \varprojlim_i G^i$ to be the subset of $\prod G^i$ consisting of those (x_i) such that $\pi_i^j(x_j) = x_i$ whenever $i \leq j$. Think of the π as projections and an element of the projective limit as a system of group elements compatible with these projections. Λ is a subgroup of $\prod G^i$ and inherits the *induced topology* from this group.

We assume from now on that the G^i are *finite* groups, since this will be our only application.

Proposition 2.2.6 *Λ is closed in $\prod G^i$.*

PROOF - Suppose $x = (x_i) \notin \Lambda$, then there are $i \leq j$ such that $\pi_i^j x_j \neq x_i$. The set of all elements in $\prod G^i$ with i-th term x_i and j-th term x_j is open in $\prod G^i$ (see Appendix D) and disjoint from Λ. Λ is the complement of the union of all such open sets.

$\square$

Now each of the groups G^i is compact, being finite. Tychonoff's Theorem (D.0.9) shows that $\prod G^i$ is compact. We know that a closed subset of a compact space is always itself a compact space. Hence we see:

Proposition 2.2.7 *$\varprojlim G^i$ is a compact group.*

[2]This means $x \leq x \, \forall x \in I$.

[3]This means that whenever $x \leq y$ and $y \leq z$ then $x \leq z$.

2.2.4 The Galois Group as a Projective Limit

We now apply this construction to the Galois case. Let L/K be any Galois extension. Our directed set I will be the set of all finite Galois extensions E of K contained in L. The groups in the inverse system will be the Galois groups $\mathrm{Gal}(E/K)$ of these extensions, considered as topological groups with the discrete topology.

In the directed set, we say $E' \leq E$ when $E' \subseteq E$. When this is the case, a homomorphism

$$\mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(E'/K)$$

is given by restricting[4] an automorphism to the subset E'. This satisfies all the conditions of an inverse system. Hence we obtain the inverse limit Λ. We now identify this with the Galois group. In fact there is the general result

Proposition 2.2.8 *A topological group G is profinite if and only if it is isomorphic to a projective limit of finite groups. These groups are then the finite quotients of G.*[5]

The proof can be found in [4]. I will demonstrate it here for the special case of a Galois group.

Proposition 2.2.9 *If we ignore the topology, there is a group isomorphism $\mathrm{Gal}(L/K) \cong \Lambda$.*

PROOF - As above, restriction gives a homomorphism $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K)$ for each $E \in I$. These combine to give a homomorphism

$$\theta : \mathrm{Gal}(L/K) \longrightarrow \prod_{E \in I} \mathrm{Gal}(E/K).$$

It is clear that $\operatorname{im}\theta \subseteq \Lambda$ (θ and the $\pi^E_{E'}$ are defined by restricting field automorphisms). So we need to show that θ is bijective.

If $s \in G - \{1\}$ then there is $y \in L$ with $sy \neq y$. Then there exists E containing y. So $s\Big|_E \in \mathrm{Gal}(E/K)$ is not the identity. Hence $\theta(y) \neq 1$, so θ is injective.

Now let $(s_E) \in \Lambda$. Define

$$s : L \longrightarrow L$$

by $s(x) := s_E(x)$ for any E such that $x \in E$. The conditions on Λ mean that s is well-defined. Using the restrictions s_E, it is easy to show that s is a K-automorphism of L. Hence $s \in \mathrm{Gal}(L/K)$ and $(s_E) = \theta(s)$. So θ is surjective.

□

[4]because E'/K is normal, we can be sure that the images of these restricted automorphisms will be contained in E'

[5]Yet another characterisation of a profinite group is that it is compact and totally disconnected.

Proposition 2.2.10 *The group isomorphism defined above is a homeomorphism*

PROOF - We have to show that θ and θ^{-1} are continuous.

First θ^{-1}. Let H be an open subset of $\mathrm{Gal}(L/K)$; by the existence of the fundamental system of neighbourhoods of the identity, it is enough to assume that H is an open, normal subgroup of G. We have to show that the preimage of H under θ^{-1}, ie. $\theta(H)$, is open in Λ.

We know that $H = \mathrm{Gal}(L/E)$ for some finite Galois extension E/K. So if $\sigma \in \mathrm{Gal}(L/E)$, then $\sigma : L \longrightarrow L$ is a field automorphism with $\sigma\Big|_E = \mathrm{id}_E$. This shows that the image of σ under θ is an element $(\sigma_{E'})_{E' \in I}$ with

$$\sigma\Big|_{E\cap E'} = \mathrm{id}_{E\cap E'}$$

for each $E' \in I$. On the other hand, the proof of the previous proposition shows that every such element comes from an element of H. So $\theta(H)$ is equal to this subgroup. But this subgroup is precisely $\ker \pi_E \cap \Lambda$, where

$$\pi_E : \prod_{E' \in I} \mathrm{Gal}(E'/K) \longrightarrow \mathrm{Gal}(E/K)$$

is projection on the E-th component. So $\theta(H)$ is open. We have thus established that θ^{-1} is continuous.

To see θ is continuous, let X be a closed subset of Λ. We have to show the pre-image $\theta^{-1}(X)$ is closed. All that is needed here is elementary topology. X is a closed subset of the compact space Λ, so is a compact space. $\theta^{-1}(X)$ is the continuous image of a compact space so is also compact. Then $\theta^{-1}(X)$ is a compact subspace of a Hausdorff space and so is closed.

$\square$

Corollary 2.2.11 *If L/K is a Galois extension, then* $\mathrm{Gal}(L/K)$ *(with the Krull topology) is a compact group*

PROOF - $\mathrm{Gal}(L/K)$ is homeomorphic to $\varprojlim \mathrm{Gal}(E/K)$ as E runs through all finite Galois subextensions of L/K. By the comments at the end of §2.2.3, this group is compact.

$\square$

2.2.5 The Fundamental Theorem

We can use the topology on the Galois group to extend Galois theory to infinite extensions.

Theorem 2.2.12 (Fundamental Theorem of Galois Theory) *Let L/K be a Galois extension with group G, $\mathcal{C}$ the set of all closed subgroups of G and $\mathcal{F}$ the set of all fields between K and L. Then*

$$E \longmapsto \mathrm{Gal}(L/E)$$

is a bijection $\mathcal{F} \longrightarrow \mathcal{C}$. Then inverse is $H \longmapsto E^H$, the fixed-field function.

For the proof, see [4]

2.3 Infinite Galois Cohomology

2.3.1 Direct Limits

In order to proceed with the definition of infinite-dimensional Galois cohomology, we need the notion of direct limit. This is a dual to the definition of projective limit given in §2.2.3. The reader is asked to recall from that section the notion of a directed set. Note that in contrast to that section, we are not going to be interested in the topology on a direct limit, as all the ones we deal with will be given the discrete topology - so this has been omitted from the definition.

Definition 2.3.1 *A direct system of groups over a directed set I is an indexed set of groups $(G^i)_{i\in I}$ and homomorphisms $\iota_i^j : G^i \longrightarrow G^j$ for $i \leq j$. We require that $\iota_i^i = \mathrm{id}_{G^i}$ and, if $i \leq j \leq k$, $\iota_j^k \circ \iota_i^j = \iota_i^k$.*

To define the *direct limit*[6] $\varinjlim_i G^i$ of a direct system, we begin with the *disjoint union* of the G^i. This is the set-theoretic union of the G^i with no $x_i \in G^i$ identified with any $x_j \in G^j$ for $i \neq j$. We define an equivalence relation on the disjoint union by saying that

- $x_i \in G^i$ and $x_j \in G^j$ are equivalent when $i \leq j$ and $\iota_i^j(x_i) = x_j$

Let $+$ denote the group law in each G^i. The set of equivalence classes is made into a group by defining the composition of the class of $x_i \in G^i$ and $x_j \in G^j$ to be the class of $\iota_i^k(x_i) + \iota_j^k(x_j)$ for any $k \geq i, j$. This is well-defined, and the resulting group is by definition the direct limit $\varinjlim_i G^i$.

Remark 2.3.2
1. *There are obvious injections $\iota_i : G^i \longrightarrow \varinjlim G^i$ which are compatible with the ι_i^j.*
2. *When the G^i are all subgroups of some group G, with $G^i \subseteq G^j \iff i \leq j$, and $\iota_i^j : G^i \longrightarrow G^j$ defined by inclusion, then the direct limit $\varinjlim G^i$ is the same as the union $\bigcup G^i$.*

[6] Also called the *injective limit*

3. *We can just as easily define the direct limit of a direct system of R-modules, by replacing "group" by "R-module" and "homomorphism" by "R-homomorphism" throughout.*

2.3.2 Properties of Direct Limits

Let (G^i, ι) be a direct system.

Proposition 2.3.3 (Universal Mapping Property of Direct Limits) *Given a system of homomorphisms $f_i : G^i \longrightarrow X$ for some group X such that $f_i = f_j \circ \iota_i^j : G^i \longrightarrow G^j \longrightarrow X$ for each $i \leq j$, there exists a unique homomorphism $f : \varinjlim G^i \longrightarrow X$ such that $f \circ \iota_j = f_j$ for all j. The picture is:*

$$\begin{tikzcd}
X & & \varinjlim G^i \arrow[ll, dashed, "\exists! f"'] \\
& G^j \arrow[ul, "f_j"'] \arrow[ur, "\iota_j"] & \\
& G^i \arrow[u, "\iota_i^j"'] \arrow[uul, "f_i"] \arrow[uur, "\iota_i"'] &
\end{tikzcd}$$

The proof is a simple matter of applying the definition.

From this property we deduce the functoriality of direct limits, as follows. We make all direct systems of groups over a given directed set into a category by defining morphisms between them in the obvious way (collections of homomorphisms that commute appropriately with the ι_i^j). The proposition then shows that a morphism $(G^i) \longrightarrow (H^i)$ induces a morphism of the direct limits $\varinjlim G^i \longrightarrow \varinjlim G^j$ in an obvious way. Hence $\varinjlim$ is a functor. In fact, it is much more:

Proposition 2.3.4 $\varinjlim$ *is an exact functor. That is, if*

$$(G^i) \longrightarrow (H^i) \longrightarrow (M^i)$$

is an exact sequence of direct systems over I (in an obvious sense) then the sequence

$$\varinjlim G^i \longrightarrow \varinjlim H^i \longrightarrow \varinjlim M^i$$

is exact.

For the proof, see [7].

2.3.3 Cohomology of Profinite Groups

Let A be a G-module where G is a profinite group. Suppose $A = \bigcup_H A^H$ where H runs through all the open normal subgroups of G. The H form a directed set with respect to the ordering $H_1 \leq H_2 \iff H_2$ is a subgroup of H_1. As a first observation, this shows that $A = \varinjlim_H A^H$.

Note next that if $H_1 \leq H_2$ then H_1/H_2 must be a *normal* subgroup of G/H_2. So the quotient map

$$G/H_2 \longrightarrow G/H_1 \Big(\cong (G/H_2)/(H_1/H_2) \Big)$$

gives, by the results of §1.4, an inflation homomorphism

$$\mathrm{Inf}_q : H^q(G/H_1, A^{H_1}) \longrightarrow H^q(G/H_2, A^{H_2})$$

for each q. The cohomology groups and inflation homomorphisms now form a direct system of groups, in the sense of §2.3.1. Hence we may define

$$H^q(G, A) := \varinjlim_H H^q(G/H, A^H)$$

which is a direct limit of finite groups.

We can use this definition to deduce certain properties of $H^q(G, A)$ from the finite case. For example, if all the $H^q(G/H, A^H)$ are trivial then the definition shows $H^q(G, A)$ must also be.

Furthermore Proposition 2.3.4 shows that the same exact cohomology sequences we have for finite groups hold also for this new definition for infinite groups.

Note that we could simply apply our original definitions of cohomology from §1.1 to the G-module A. The groups $H^q(G, A)$ thus obtained are *not* the same as the ones we have defined here. The reason is that it is important to consider the topology on the group, which was not done in that definition. However, our new definition exactly comes from considering the topology on the group, as will be demonstrated soon.

2.3.4 Continuous Cochains

Definition 2.3.5 *Let G be a profinite group and A a G-module, given the discrete topology. A will be called a* discrete G-module *if the action*

$$\begin{array}{ccc} G \times A & \longrightarrow & A \\ (g, a) & \longmapsto & ga \end{array}$$

is continuous.

If A is a discrete G-module, a q-dimensional continuous cochain *is a continuous map*

$$G^q \longrightarrow A$$

Proposition 2.3.6 *If G is a profinite group and A a discrete G-module, and $f : G \longrightarrow A$ is a function, then the following are equivalent.*

1. *f is continuous;*

2. *For each $g \in G$, there is a neighbourhood of g on which f is constant ("f is locally constant");*

3. *f can be filtered through a finite quotient of G, ie. there exists an open normal subgroup H of G such that f is equal to the composition*

$$G \xrightarrow{proj.} G/H \xrightarrow{\bar{f}} A$$

PROOF - (1) $\Rightarrow$ (2): Let $g \in G$, then $f^{-1}(\{f(g)\})$ is open in G (since A has the discrete topology) and so there is a neighbourhood of g on which f takes only the value $f(g)$.

(2) $\Rightarrow$ (3): Take for each g an open neighbourhood gM_g of g on which f is constant. These form an open cover of the compact group G and so there is a finite subcover $\{gM_g : g \in S\}$, where $S \subseteq G$ is a finite subset. The intersection $\bigcap_{g\in S} M_g$ is an open subgroup M of G such that g is constant on gM for each $g \in G$. M contains an open normal subgroup H of G by the definition of profinite group. Then f is constant on each gH, ie. the diagram

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr] & & A \\ & G/H \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

commutes.

(3) $\Rightarrow$ (1): If $a \in A$ and $f(g) = a$ then $f^{-1}(\{a\})$ contains gH where H is an open normal subgroup of G, and so is open in G. Then for any open set $U \in A$ (ie. any subset) we have $f^{-1}(U) = \bigcup_{u\in U} f^{-1}(\{u\})$ is open, and so f is continuous.

□

Corollary 2.3.7 *A function $G^q \longrightarrow A$ is continuous if and only if it is locally constant.*

PROOF - The above discussion extends easily to a finite product of copies of G.

□

Note that a continuous map on G has finite image.

Let $C^n(G,A)$ denote the group of continuous cochains $G^n \longrightarrow A$. Define a coboundary map

$$d : C^n(G,A) \longrightarrow C^{n+1}(G,A)$$

by the usual formula for inhomogeneous cochains (1.5):

$$\begin{aligned} df[g_1,\ldots,g_{q+1}] &= g_1 f[g_2,\ldots,g_{q+1}] \\ &\quad + \sum_{j=1}^{q}(-1)^j f[g_1,\ldots,g_j g_{j+1},\ldots,g_{q+1}] \\ &\quad + (-1)^{q+1} f[g_1,\ldots,g_q]. \end{aligned}$$

It is clear that if f is continuous then so is df, using the previous proposition. We check as in §1.2.1 that

$$\mathbf{C}(G,A): \qquad 0 \longrightarrow C^0(G,A) \xrightarrow{d_0} C^1(G,A) \xrightarrow{d_1} C^2(G,A) \longrightarrow \dots$$

is a cochain complex. Hence we may define the cohomology groups

$$H^q(\mathbf{C}(G,A)) := \ker d_q / \operatorname{im} d_{q-1}$$

Proposition 2.3.8 *$H^q(\mathbf{C}(G,A))$ is naturally equivalent to the $H^q(G,A)$ defined in §2.3.3.*

SKETCH PROOF - First we want an isomorphism of groups

$$\theta : C^q(G,A) \longrightarrow \varinjlim_{H} C^q(G/H, A^H)$$

Where H runs through the open normal subgroups of G. We note that, using the usual definition of inhomogeneous cochains in terms of the standard free G/H resolution of $\mathbb{Z}$, $C^q(G/H, A^H) = \operatorname{Hom}_G(P_q(G/H), A^H)$ because G/H is finite (and so continuity of maps on G/H is automatic). Given a map $f \in C^q(G,A)$, we know f can be filtered through G^q/H'^q for some open normal subgroup H' of G. Furthermore $\operatorname{im} f$ is finite, so there is H'' with $\operatorname{im} f \subseteq A^{H''}$ by Definition 2.3.5. Set $H = H' \cap H''$, and map f to the class of $\bar{f} : G^q/H^q \longrightarrow A^H$ in $\varinjlim C^q(G/H, A^H)$. This gives a well-defined homomorphism θ.

On the other hand we use Proposition 2.3.3 to define an inverse. For $h \in C^q(G/H_1, A^{H_1})$ map h by inflation to a map in $C^q(G,A)$. This commutes with the inflations $C^q(G/H_1, A^{H_1}) \longrightarrow C^q(G/H_2, A^{H_2})$ for $H_2 \subseteq H_1$ and so defines a map

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

which, checking on the $C^q(G/H, A^H)$, is inverse to θ. Hence we have the isomorphism.

Now the functoriality of direct limits (§2.3.2) defines another coboundary map d', so that we have a diagram

$$\begin{array}{ccc} C^q(G,A) & \xrightarrow{d} & C^{q+1}(G,A) \\ \downarrow\wr & & \downarrow\wr \\ \varinjlim C^q(G/H, A^H) & \xrightarrow{d'} & \varinjlim C^{q+1}(G/H, A^H) \end{array}$$

which is easily seen to be commutative since continuous maps can be filtered through finite quotients.

Finally we have to show that taking cohomology commutes with taking direct limits. For each $q \geq 0$, the exact sequences

$$0 \longrightarrow \ker f_q \longrightarrow C^q(G/H, A^H) \xrightarrow{d_q} \operatorname{im} d_q \longrightarrow 0$$

make up an exact sequence of direct systems, and so

$$0 \longrightarrow \varinjlim_H \ker d_q \longrightarrow \varinjlim_H C^q(G/H, A^H) \xrightarrow{d'_q} \varinjlim_H \operatorname{im} d_q \longrightarrow 0$$

is exact, giving natural equivalence

$$\frac{\ker d'_q}{\operatorname{im} d'_{q-1}} = \frac{\varinjlim_H \ker d_q}{\varinjlim_H \operatorname{im} d_{q-1}} = \varinjlim_H \frac{\ker d_q}{\operatorname{im} d_{q-1}}.$$

2.3.5 The Restriction-Inflation Sequence

Recall the Restriction-Inflation sequence of §1.4.1. We show an analogous result for profinite groups. First we need some technical results about profinite groups. The quotient of a profinite group by a closed subgroup is again a profinite group, under the identification topology.

Let G be a profinite group, $G = \varprojlim_U G/U$, where U runs through the open normal subgroups of G.

Proposition 2.3.9 *1. If H is a closed subgroup of G, $H \cong \varprojlim_U H/H \cap U$.*

2. If H is a closed, normal subgroup of G, $G/H \cong \varprojlim_U G/UH$.

For the proof, see [4].

Proposition 2.3.10 *Suppose $H^n(H/H \cap U, A^U) = 0$ for all U and all n with $1 \leq n < q$. Then the sequence*

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A)$$

is exact.

PROOF - In the finite restriction-inflation sequence (Proposition 1.4.2), take G/U as the main group "G" and $HU/U \cong H/H \cap U$ as the subgroup "H". The isomorphism is by the second isomorphism theorem. The quotient of these is G/HU by the third isomorphism theorem. Take A^U as the module "A". We obtain an exact sequence

$$0 \longrightarrow H^q(G/HU, A^{HU}) \xrightarrow{\text{Inf}} H^q(G/U, A^U) \xrightarrow{\text{Res}} H^q(H/H \cap U, A^U)$$

This forms an exact sequence of direct systems, and we pass to the direct limit over U to obtain exact

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} \varinjlim_U H^q(H/H \cap U, A^U).$$

Let us see that

$$\varinjlim_U H^q(H/H\cap U, A^U) = H^2(H,A) = \varinjlim_U H^q(H/H\cap U, A^{H\cap U}).$$

The exact sequence of $H/H\cap U$-modules

$$0 \longrightarrow A^U \longrightarrow A^{H\cap U} \longrightarrow A^{H\cap U}/A^U \longrightarrow 0$$

gives exact

$$H^{q-1}\Big(\frac{H}{H\cap U}, \frac{A^{H\cap U}}{A^U}\Big) \longrightarrow H^q\Big(\frac{H}{H\cap U}, A^U\Big) \longrightarrow H^q\Big(\frac{H}{H\cap U}, A^{H\cap U}\Big). \qquad (2.1)$$

This is another exact sequence of direct systems. So we may pass to the direct limit over U to obtain an exact sequence of groups.

Let us show that $\varinjlim_U H^n(H/H\cap U, A^{H\cap U}/A^U) = 0$. Let f be a cocycle. Choose U' so that $A^{U'} \supseteq \operatorname{im} f$ (a finite set because the domain of f is finite). Then

$$\operatorname{Inf} f : (H/H\cap U')^n \longrightarrow A^{H\cap U'}/A^{U'}$$

is the zero map. So the class of f is zero. This shows the vanishing of the direct limits and then (2.1) gives us the identification we wanted.

□

2.4 Infinite Galois Cohomology

We apply this theory to the cohomology of infinite Galois extensions. Recall that the Galois group $\mathrm{Gal}(L/K)$ of a Galois field extension L/K acts on the multiplicative group L^* and the additive group L, making them abelian G-modules. This action is continuous if L, L^* are given the discrete topology, and G has the canonical (Krull) topology (see §2.2.1). To see this, suppose $a \in L$, then a is contained in a finite Galois extension $M \subseteq L$ of K. Let (g,b) be an element of the preimage of a under the map

$$G \times L \longrightarrow L$$

so that $gb = a$. Then $b \in M$ because M is a normal extension. Hence the open set $g\mathrm{Gal}(L/M) \times \{b\}$ is also contained in the preimage of a, and so this preimage is open. Hence the action is continuous.

Therefore L and L^* are discrete G-modules in the sense of Definition 2.3.5.

We see

$$H^q(\mathrm{Gal}(L/K), L^*) = \varinjlim_H (\mathrm{Gal}(L/K)/H, L^{*H}) = \varinjlim_E (\mathrm{Gal}(E/K), E^*)$$

where H runs through all open normal subgroups, or, equivalently[7], E runs through all finite Galois subextensions of L/K, ordered by $E \le E' \iff E \subseteq E'$. Exactly the same result holds for the additive group.

[7] By the Fundamental Theorem of Galois Theory, 2.2.12!

Theorem 2.4.1 $H^q(\mathrm{Gal}(L/K), L) = 0$ *for all* $q \geq 1$.

PROOF - Pass to the limit on L in Theorem 2.1.1.

□

We write again $H^q(L/K)$ for $H^q(\mathrm{Gal}(L/K), L^*)$.

Theorem 2.4.2 $H^1(L/K) = 0$.

PROOF - Pass to the limit on L in Theorem 2.1.2.

□

2.5 Functoriality of Galois Cohomology Groups

We conclude this section by looking at the object $H^q(L/K)$ more closely. It depends functorially on the pair $(L, K) =: L/K$. Take the class of Galois field extensions L/K and make it into a category $\mathcal{C}$ by defining morphisms

$$L/K \longrightarrow L'/K'$$

whenever there is a field homomorphism $\iota : L \hookrightarrow L'$ with $\iota(K) \supseteq K'$. If $G := \mathrm{Gal}(L/K), G' := \mathrm{Gal}(L'/K')$ then there is a corresponding morphism $G' \longrightarrow G$, where $\sigma \in \mathrm{Gal}(L'/K')$ acts on L/K by

$$\sigma(\lambda) = \iota^{-1} \circ \sigma \circ \iota(\lambda),$$

(note $\sigma(\iota(\lambda)) \in \iota(L)$ by normality). The restriction morphism then gives

$$\mathrm{Res} : H^q(G, L^*) \longrightarrow H^q(G', \iota(L^*)) \longrightarrow H^q(G', L'^*)$$

ie. $\mathrm{Res} : H^q(L/K) \longrightarrow H^q(L'/K')$. We see that $H^q(L/K)$ is a covariant functor in the argument L/K from $\mathcal{C}$ to the category of abelian groups.

Chapter 3

The Brauer Group

3.1 Definitions

If K is a field, let K_s denote the separable closure of K, which is the union of all finite Galois extensions of K. The usual Zorn's lemma arguments shows that this field is well-defined and unique up to isomorphism. In the last chapter we saw how to define $H^2(K_s/K)$ as a direct limit of $H^2(L/K)$ over all finite Galois extensions L/K. This group[1] $H^2(K_s/K)$ is called the *Brauer Group* of K, and will also be written $\mathrm{Br}(K)$. It occupies a central place in Local Class Field Theory by dint of Tate's Theorem (1.6.4). It also has a very interesting arithmetic interpretation, and the purpose of this chapter is to explore this.

It turns out that each element of $\mathrm{Br}(K)$ corresponds to a class of *central simple K-algebras.* A central simple K-algebra is a ring A with centre K and which is finite-dimensional over K, and furthermore is a simple ring. We refer to Appendix E for basic facts about central simple algebras.

3.2 Characterization of Central Simple Algebras

Proposition 3.2.1 *Let A be a finite-dimensional algebra over a field K. Then the following properties are equivalent:*

(a) *A is central simple over K;*

(b) *$A \otimes_K \bar{K} \cong M_n(\bar{K})$ as $\bar{K}$-algebras, for some n, where $\bar{K}$ is an algebraic closure of K;*

(b') *There exists a finite Galois extension L of K such that $A \otimes_K L \cong M_n(L)$ as L-algebras, for some n;*

(c) *$A \cong M_n(D)$ as K-algebras, for some n, where D is a finite-dimensional central division algebra over K.*

[1]This group is well-defined, ie. independent of our choice of separable closure. See [4].

PROOF - "(a) $\Rightarrow$ (c)" is Wedderburn's Theorem, proved in §E.2.
"(b') $\Rightarrow$ (b)": Given (b'),

$$A \otimes_K \bar{K} \cong A \otimes_K (L \otimes_L \bar{K}) \cong (A \otimes_K L) \otimes_L \bar{K} \cong M_n(L) \otimes_L \bar{K} \cong M_n(\bar{K})$$

"(b) $\iff$ (a)" is shown in §E.5.
Then "(c) $\Rightarrow$ (b')" follows from Proposition E.6.1 and the results of §E.3.

□

3.3 Structure of the Classical Brauer Group

Consider the class of central simple of algebras over K, and the equivalence relation on this class given by isomorphism of K-algebras. Any such algebra is isomorphic as a K-algebra to the K-vector space K^n supplied with a ring multiplication, which is a function $\mu : K^n \times K^n \longrightarrow K^n$. This shows that the isomorphism relation has a *set* of representatives, consisting of the set[2] of such pairs (K^n, μ).

Two central simple K-algebras will be called *similar* or *equivalent* if the division algebras associated to them by Proposition 3.2.1 are isomorphic (as K-algebras).

By the uniqueness up to isomorphism of the D (§E.2) this is an equivalence relation on the set of isomorphism classes of central simple K-algebras.

Write $[A]$ for the class of A, and $\mathrm{Br}(K)$ for the set of equivalence classes. $\mathrm{Br}(K)$ is given the structure of an abelian group, and so becomes the classical *Brauer Group* of K, as follows. Define the product of $[A]$ and $[B]$ by

$$[A] \cdot [B] := [A \otimes_K B]$$

We have to check this is well-defined. Well,

$$\begin{aligned} M_n(D) \otimes_K M_{n'}(D') &\cong \big(M_n(K) \otimes_K M_{n'}(K)\big) \otimes_K \big(D \otimes_K D'\big) \\ &\cong M_{nn'}(K) \otimes_K M_m(D'') \\ &\cong M_{nn'm}(D'') \end{aligned}$$

and then it follows from Proposition E.2.3 of §E.2 that D'' is determined up to isomorphism by the isomorphism classes of D and D', so that the class $[A \otimes_K B]$ depends only on the similarity classes of A and B, and multiplication is well-defined.

The commutativity and associativity of $\otimes_K$ give the same properties for the group law.

Since

$$[K] \cdot [B] = [K \otimes_K B] = [B] = [B \otimes_K K] = [B] \cdot [K]$$

$[K]$ is an identity element for the group.

Now §E.5 shows $A \otimes_K A^\circ \cong \mathrm{End}_K(A) \cong M_n(K)$, so that $[A] \cdot [A^\circ] = [K]$, ie. $[A^\circ]$ is an inverse for $[A]$. Thus $\mathrm{Br}(K)$ is an abelian group.

[2]Recall that a class is a set if it has a cardinal number, that is, it is equipotent with a set which can be built up from the axioms of set theory, like this $\{(K^n, \mu)\}$

3.4 Relating the Brauer Group to a One-Dimensional Cohomology Set

Let $L \supseteq K$ be a field extension, and write $A_n(L)$ for the set of elements $[A]$ of the Brauer group such that $A \otimes_K L \cong M_n(L)$.[3]

The strategy is to relate $A_n(L)$ to the cohomology set H^1 of a particular non-abelian G-module[4]. Let A be a central simple K-algebra with $A \otimes_K L \cong M_n(L)$; let $F : M_n(L) \longrightarrow A \otimes_K L$ be the isomorphism. For $s \in \mathrm{Gal}(L/K) =: G$, let sF be defined by

$$\begin{array}{rccc} sF: & M_n(L) & \longrightarrow & A \otimes_K L \\ & (\lambda_{ij})_{i,j} & \longmapsto & s(F((s^{-1}\lambda_{ij})_{i,j})) \end{array}$$

ie. $sF = s \circ F \circ s^{-1}$. Put $\theta(A)[s] := F^{-1} \circ sF \in \mathrm{Aut}(M_n(L))$, ie. $\theta(A)[s] = F^{-1} \circ s \circ F \circ s^{-1}$. Here $\mathrm{Aut}(M_n(L)) =: C$ is the group of L-linear ring automorphisms of $M_n(L)$ under composition, made into a non-abelian G-module by $sc := s \circ c \circ s^{-1}$ for $s \in G, c \in C$.

Proposition 3.4.1 *$\theta(A)$ is a 1-cocycle of G with values in C, which depends only on the similarity class $[A]$ of A. Choosing a different F changes $\theta(A)$ to a cohomologous cocycle. Thus θ determines a function $A_n(K) \longrightarrow H^1(G, C)$.*

PROOF - Recall from Appendix B that $H^1(G, C)$ consists of 1-cocycles $f : G \longrightarrow C$, ie. $f[st] = f[s] \circ sf[t]$, and two such cocycles $f, f'$are cohomologous if there is $c \in C$ such that $f[s] = c^{-1} \circ f'[s] \circ sc$ for all $s \in G$. Let us check the 1-cocycle condition on $\theta(A)$:

$$\begin{aligned} \theta(A)[st] &= F^{-1} \circ st \circ F \circ t^{-1}s^{-1} \\ &= F^{-1} \circ (s \circ F \circ s^{-1} \circ s \circ F^{-1} \circ s^{-1}) \circ st \circ F \circ t^{-1}s^{-1} \\ &= \theta(A)[s] \circ s \circ F^{-1} \circ t \circ F \circ t^{-1} \circ s^{-1} \\ &= \theta(A)[s] \circ s\theta(A)[t] \end{aligned}$$

Next we check the independence of F. If $F, F' : M_n(L) \longrightarrow A \otimes_K L$ are isomorphisms defining $\theta(A)$ and $\theta'(A)$ then

$$\begin{aligned} \theta(A)[s] &= F^{-1} \circ s \circ F \circ s^{-1} \\ &= (F^{-1} \circ F') \circ F'^{-1} \circ s \circ F' \circ s^{-1} \circ (s \circ F'^{-1} \circ F \circ s^{-1}) \\ &= c^{-1} \circ \theta'(A)[s] \circ sc \end{aligned}$$

[3] We might choose $L = \bar{K}$ to be an algebraic closure of K, then $\mathrm{Br}(K) = \cup_{n=1}^{\infty} A_n(L)$, since L neutralises all central simple K-algebras. Then we would relate it to the group $H^2(K_s/K)$ by using the definition of this group in terms of continuous cochains. This is the approach taken by Weil in *Basic Number Theory*. Alternatively, we can take L/K to be a finite extension and pass to the limit later. The second approach is shown here.

[4] This is a special case of the general method of "Galois descent"; A_n is a set of K-vector spaces with a particular type of additional structure, which all become isomorphic to each other when the functor $\otimes_K L$ is applied (isomorphic in the sense that a morphism must also preserve the additional structure). Such systems can be systematically related to cohomology sets H^1. See [1], Chapter 10 for more details.

where $c = F^{-1} \circ F'$, so that $\theta(A)$ is cohomologous to $\theta'(A)$.

Now suppose A' is a similar algebra to A, then $A \cong M_m(D)$ and $A' \cong M_{m'}(D)$ for some m, m'. But comparing K-dimensions (since both A, A are in $A_n(L)$) shows that $m = m'$, so that in fact $A \cong A'$. This induces an isomorphism $\mu : A \otimes_K L \longrightarrow A' \otimes_K L$ which commutes with the action of $\mathrm{Gal}(L/K)$, $s(a \otimes \lambda) = a \otimes s\lambda$. Thus if $F' : M_n(L) \longrightarrow A' \otimes_K L$ is an isomorphism then $F' = \mu \circ F$ for some isomorphism $F : M_n(L) \longrightarrow A \otimes_K L$, and so

$$\begin{aligned}
\theta(A') &= F^{-1} \circ \mu^{-1} \circ s \circ \mu \circ F \circ s^{-1} \\
&= F^{-1} \circ (\mu^{-1} \circ \mu) \circ s \circ F \circ s^{-1} \\
&= \theta(A)
\end{aligned}$$

Also, $\theta(M_n(K)) = 1$ because G acts trivially on K, which verifies that θ is a morphism of pointed sets.

□

Proposition 3.4.2 *θ is injective.*

PROOF - Suppose $\theta(A) = \theta(B)$, ie. we have

$$\begin{array}{rccc}
F : & M_n(L) & \longrightarrow & A \otimes_K L \\
F' : & M_n(L) & \longrightarrow & B \otimes_K L
\end{array}$$

with $F^{-1} \circ s \circ F \circ s^{-1} = F'^{-1} \circ s \circ F' \circ s^{-1}$ for all $s \in G$. We want to show that $A \cong B$. We have

$$F' \circ F^{-1} \circ s = s \circ F' \circ F^{-1} \qquad \text{for all } s \in G$$

so that $f := F' \circ F^{-1} : A \otimes_K L \longrightarrow B \otimes_K L$ is an isomorphism that commutes with the action of the Galois group.

Take $a \otimes \kappa \in A \otimes_K K$; we show that $f(a \otimes \kappa) \in B \otimes_K K$. Any element $x \in B \otimes_K L$ can be uniquely written as:

$$x = \sum_{i=1}^{\dim_K B} b_i \otimes \lambda_i$$

where $\{b_i\}$ is a K-basis for B, and the $\lambda_i \in L$. Recall $s \in G$ takes x to $sx = \sum b_i \otimes s\lambda_i$. If G acts trivially x, then it follows that $s\lambda_i = \lambda_i$ for each λ_i, which shows that $\lambda_i \in K$ and so $x \in B \otimes_K K$. Applying this to the G-invariant element $f(a \otimes \kappa)$ shows that f restricts to an injective morphism of K-algebras

$$A \otimes_K K \longrightarrow B \otimes_K K$$

Comparing K-dimension shows this is an isomorphism, and then identifying $A \otimes_K K \cong A$ shows $A \cong B$, so $[A] = [B]$.

Proposition 3.4.3 *θ is surjective*

PROOF - Let $f : G \longrightarrow C$ be a 1-cocycle. We want to show that there is a central simple K-algebra A such that $A \otimes_K L \cong M_n(L)$ and there is such an isomorphism $F : M_n(L) \longrightarrow A \otimes_K L$ with $f[s] = F^{-1} \circ s \circ F \circ s^{-1}$.

We build the required K-algebra from $M_n(L)$. Let F be an L-automorphism of $M_n(L)$, then choosing a basis of $M_n(L)$ identifies F with a matrix $X = (x_{ij})_{i,j}$ in $\mathbf{GL}(n^2, L)$. Recall sF is the L-automorphism of $M_n(L)$ defined by $s \circ F \circ s^{-1}$. This L-automorphism has matrix $sX = (sx_{ij})_{i,j}$, for we can choose the basis $(v_i)_{i=1}^{n^2}$ of $M_n(L)$ to be G-invariant, for example, the standard basis. Then

$$(sF)v_i = s(Fv_i) = s(\sum_j x_{ji}v_j) = \sum_j (sx_{ji})v_j$$

Applying this to the L-automorphisms $f[st]$, $f[s]$ and $sf[t]$ shows that, if $X[st]$ etc. are the associated matrices,

$$f[st] = f[s] \cdot sf[t] \Rightarrow X[st] = X[s] \cdot sX[t]$$

So this $X : G \longrightarrow \mathbf{GL}_(n^2, L)$ is a 1-cocycle. Now we can apply the result about the Galois cohomology of such a group (Proposition 2.1.4):

$$H^1(G, \mathbf{GL}(n^2, L)) = 0$$

so that X is in fact a 1-coboundary, ie. there is $Y \in \mathbf{GL}(n^2, L)$ with

$$X[s] = Y^{-1} \cdot sY \qquad \text{for all } s \in G.$$

Y determines an L-linear map

$$F : M_n(L) \longrightarrow M_n(L)$$

such that $f[s] = F^{-1} \cdot (sF) = F^{-1} \cdot s \cdot F \cdot s^{-1}$.

We can use this to define a composition law on $M_n(L)$

$$(A, B) \longmapsto A \odot B := F(F^{-1}(A) \cdot F^{-1}(B))$$

where $\cdot$ is usual matrix multiplication.

$\odot$ is associative because $\cdot$ is associative, and distributive because F is L-linear. $F(1)$ is the identity for multiplication. So we have defined a new ring structure on $M_n(L)$. In fact, this ring structure restricts to the subspace $M_n(K)$. For:

$$\begin{aligned}
s(A \odot B) &= s\Big(F(F^{-1}(A) \cdot F^{-1}(B)\Big) \\
&= (sF)\Big(s(F^{-1}(A)) \cdot s(F^{-1}(B))\Big) \\
&= (sF)\Big((sF^{-1})(sA) \cdot (sF^{-1})(sB)\Big) \\
&= (F \circ f[s])\Big((f[s]^{-1} \circ F^{-1})(sA) \cdot (f[s]^{-1} \circ F^{-1})(sB)\Big) \\
&= (F \circ f[s])f[s]^{-1}(F^{-1}(sA) \cdot F^{-1}(sB)) \\
& \text{(since } f[s] \text{ is a ring homomorphism)} \\
&= (sA) \odot (sB)
\end{aligned}$$

So if $A, B \in M_n(K)$ and so are fixed by G, then $A \odot B$ is fixed by G and so is in $M_n(K)$.

By looking at the standard basis under the identification $M_n(K) \otimes_K L \cong M_n(L)$, we see that our ring multiplication $\odot$ in $M_n(L)$ is the same as the ring multiplication in $M_n(K) \otimes_K L$ defined by

$$(A \otimes \lambda, B \otimes \lambda') \longmapsto (A \odot B) \otimes \lambda\lambda'$$

so that, if we put A for $M_n(K)$ with multiplication defined by $\odot$,

$$F : M_n(L) \longrightarrow A \otimes_K L$$

gives $f[s] = F^{-1} \circ sF$

□

3.5 Brauer Groups as Two-Dimensional Cohomology Groups

So far we have an isomorphism of pointed sets

$$\theta : A_n(L) \longrightarrow H^1(G, C)$$

where C is the G-module of L-linear ring automorphisms of $M_n(L)$. The next task is to identify C and fit it in a short exact sequence, so we can use the cohomology sequence of Appendix B. We use the following result, a special case of the Theorem of Skolem-Noether:

Proposition 3.5.1 *Let B be a central-simple L-algebra. Then every L-linear ring automorphism of B is of the form $x \longmapsto b^{-1}xb$ for some invertible $b \in B$, ie. is an inner automorphism.*

For the proof, see [10], Chapter 9, §1, Prop. 4.

Applying this to $M_n(L)$ shows that an element of C is an inner automorphism

$$X \longmapsto Q^{-1}XQ$$

for some $Q \in \mathbf{GL}(n, L)$. Multiplying Q by an element of L^* does not change the automorphism; on the other hand, if

$$Q^{-1}XQ = Q'^{-1}XQ'$$

for some invertible Q and Q' in $\mathbf{GL}(n, L)$ and all $X \in M_n(L)$ then $Q'Q^{-1}$ is in the centre L of $\mathbf{GL}(n, L)$. Hence the exact sequence of non-abelian G-modules

$$1 \longrightarrow L^* \longrightarrow \mathbf{GL}(n, L) \longrightarrow C \longrightarrow 1$$

which shows that C is isomorphic as a G-module and L-algebra to $\mathbf{PGL}(n, L) = \mathbf{GL}(n, L)/L^*$, a projective general linear group of L.

We now apply again the Proposition 2.1.4 that $H^1(G, \mathbf{GL}(n, L))$ is trivial. The exact cohomology sequence of Appendix B gives an exact sequence

$$1 \longrightarrow H^1(G, C) \xrightarrow{\delta} H^2(G, L^*)$$

That is, a morphism of pointed sets $\delta : H^1(G, C) \longrightarrow H^1(G, L^*)$ with trivial "kernel" (preimage of the identity element). Thus we have a morphism of pointed sets

$$\alpha_n = \delta \circ \theta : A_n(L) \longrightarrow H^2(G, L^*)$$

which we now study.

Proposition 3.5.2 $\alpha_{nm}([A][B]) = \alpha_n([A]) \cdot \alpha_m([B])$, *where $\cdot$ denotes composition in the abelian group $H^2(G, L^*)$ and A and B are central-simple K-algebras such that $A \otimes_K L \cong M_n(L)$ and $B \otimes_K L \cong M_m(L)$.*

PROOF - Isomorphisms

$$\begin{array}{ccc} M_n(L) & \xrightarrow{F} & A \otimes_K L \\ M_m(L) & \xrightarrow{F'} & B \otimes_K L \end{array}$$

induce an isomorphism

$$M_{nm}(L) = M_n(L) \otimes_L M_m(L) \xrightarrow{F \otimes F'} (A \otimes_K L) \otimes_L (B \otimes_K L) = (A \otimes_K B) \otimes_K L$$

Then $\theta([A])$ is defined by $\theta([A])[s] = F^{-1} \circ s \circ F \circ s^{-1}$, $\theta([B])$ similarly in terms of F', and $\theta([A][B])$ similarly in terms of $F \otimes F'$. Lift these automorphisms of matrix algebras to matrices giving them by conjugation, so

$$\begin{array}{rcll} \theta([A])[s] & \rightsquigarrow & M[s] & \quad \text{such that } \theta([A])[s](X) = M[s]XM[s]^{-1} \\ \theta([B])[s] & \rightsquigarrow & M'[s] & \\ \theta([A][B])[s] & \rightsquigarrow & M[s] \otimes M'[s] & \end{array}$$

Applying d gives $d(M \otimes M')[s, t] = (dM)[s, t] \otimes (dM')[s, t]$, and we know these matrices are now of the form $\lambda 1_M$ for some $\lambda \in L^*$ and for $1_M \in M_{nm}(L)$. So comparing the top-left entry (under the correspondences defined in §E.3) shows that

$$\begin{array}{rcl} \alpha_{mn}([A \otimes_K B])[s, t]1_M & = & d(M \otimes M')[s, t] \\ & = & dM[s, t] \otimes dM'[s, t] \\ & = & \alpha_n([A])[s, t]1_M \otimes \alpha_m([B])[s, t]1_M \end{array}$$

so $\alpha_{mn}([A \otimes_K B]) = \alpha_n([A])\alpha_m([B])$ in $H^2(G, L^*)$.

$\square$

Now the group $A(L/K) := \bigcup_{n=1}^{\infty} A_n(L)$ is a subgroup of the Brauer group $\mathrm{Br}(K)$. All the α_n together define a *homomorphism*

$$\alpha : A(L/K) \longrightarrow H^2(G, L^*)$$

Proposition 3.5.3 *α is injective*

PROOF - If $\alpha([A]) = \alpha([B])$ then $\alpha_n([A][B]^{-1}) = 1$ for some n. So $[A][B]^{-1} \in \theta^{-1}(\delta^{-1}(\{1\})) = \{1\}$, ie. $[A] = [B]$, so α is injective.

$\square$

Lemma 3.5.4 (See [1], Chapter 10, §5) *if $n = [L : K]$, then*

$$\delta_n : H^1(G, \mathbf{PGL}(n, L)) \longrightarrow H^2(G, L^*)$$

is surjective.

PROOF - We need to show that given a 2-cocycle

$$h : G^2 \longrightarrow L^*$$

there is a 1-cochain $f : G \longrightarrow \mathbf{GL}(n, L)$ such that $h[s,t] = f[s] \cdot sf[t] \cdot f[st]^{-1}$. Let V be the L-vector space with basis $(e_s)_{s \in G}$, so $\dim_L V = n$. Let $f[s] \in \mathrm{Hom}_K(V, V)$ be given by

$$\begin{array}{rccc} f[s]: & V & \longrightarrow & V \\ & e_t & \longmapsto & h[s,t]e_{st} \end{array}$$

Then

$$\begin{array}{rcl} f[s] \circ sf[t](e_u) & = & h[s,tu] \cdot sh[t,u]e_{stu} \\ h[s,t]f[st](e_u) & = & h[s,t] \cdot h[st,u]e_{stu} \end{array}$$

and because h is a 2-cocycle, this gives $h[s,t] = f[s] \cdot sf[t] \cdot f[st]^{-1}$, as required.

$\square$

Thus we have a group isomorphism

$$\alpha : A(L/K) \longrightarrow H^2(L/K)$$

Now

$$\mathrm{Br}(K) = \cup A(L/K) = \varinjlim A(L/K)$$

as L runs through all finite Galois extensions of K, and similarly

$$H^2(K_s/K) = \varinjlim H^2(L/K)$$

One checks that the maps in the direct systems commute with the α, so that the α define a group isomorphism

$$\mathrm{Br}(K) \cong H^2(K_s/K)$$

Chapter 4

Local Class Field Theory

4.1 The Restriction-Inflation Sequence

Proposition 4.1.1 *Let $L \supseteq M \supseteq K$ be a tower of fields with L/M and M/K Galois extensions. Then there is an exact sequence*

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

PROOF - Let $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/M)$ the subgroup corresponding to M. Note that $\mathrm{Gal}(M/K) = G/H$ by the Fundamental Theorem of Galois Theory. The result then follows from Theorem 2.4.2 and Proposition 2.3.10.

□

Corollary 4.1.2 *With the hypotheses of the proposition, there is an exact sequence*

$$0 \longrightarrow H^2(M/K) \longrightarrow \mathrm{Br}(K) \longrightarrow \mathrm{Br}(M)$$

PROOF - Set $L = K_s$.

4.2 Local Fields

There is a very special class of fields for which we can say enough about the Brauer group to use it to obtain the reciprocity isomorphism, our ultimate aim. In this section we describe these "local fields". They are systematically studied in the first part of [1], and are also described in Anne Esslemont's part of this project. We recall the basic definitions here.

Definition 4.2.1 *Let K be a field and $v : K \longrightarrow \mathbb{R} \cup \{+\infty\}$ be a map satisfying*

1. $v\big|_{K^*} : K^* \longrightarrow \mathbb{R}$ *is a nonzero homomorphism*
2. $v(0) = +\infty$

3. *$v(x+y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$*

4. *The image $v(K^*)$ is a discrete subgroup of $\mathbb{R}$.*

Then v is called a discrete valuation *on K.*

$v(K^*)$ is an infinite cyclic group; if $v(K^*) = \mathbb{Z}$ then v is called *normalised.*

The set $\{x \in K : v(x) \geq 0\}$ is a subring of K called the *valuation ring* of v and written $\mathcal{O}_K$. The subset $\mathfrak{m}_K := \{x \in K : v(x) > 0\}$ is the unique prime ideal of $\mathcal{O}_K$. It is a principal ideal generated by any element π with minimal positive valuation ($v(\pi) = 1$ for a normalised valuation). The π are called *uniformisers* of K. All ideals of $\mathcal{O}_K$ are of the form $\pi^n \mathcal{O}_K = \mathfrak{m}_K^n$ for some $n \geq 0$.

The set $\mathcal{O}_K - \mathfrak{m}_K$ comprises the elements of valuation zero; these are all the *units*, ie. the *invertible elements* of $\mathcal{O}_K$. We write $U_K = \mathcal{O}_K - \mathfrak{m}_K$.

Any principal ideal domain with a unique prime ideal is called a *discrete valuation ring*, and its field of fractions then has a discrete valuation defined on it by a uniformiser. Namely, every element is of the form $\pi^n u$ for some unit u and integer n, which we take to be the valuation of the element.

Finally, we define the *residue field* of K to be

$$k := \mathcal{O}_K / \mathfrak{m}_K,$$

which is a field because $\mathfrak{m}_K$ is a maximal ideal[1].

The discrete valuation v defines an *absolute value* of K as follows. Pick any real number a with $0 < a < 1$. Define for $x \in K$,

$$\|x\|_v := a^{v(x)}.$$

Then $\| \ \|_v$ satisfies

1. $\|xy\|_v = \|x\|_v \|y\|_v$,

2. $\|0\|_v = 0$,

3. $\|x + y\|_v \leq \max\{\|x\|_v, \|y\|_v\}$.

The third property is called the *non-Archimedean triangle inequality*; an absolute value which has it is called *ultrametric* or *non-Archimedean.* $\| \ \|_v$ defines a metric on K in the usual way,

$$\mathrm{d}(x, y) = \|x - y\|_v,$$

and hence a topology on K , called the *topology defined by v*. This topology does not depend on the choice of the number a.

Definition 4.2.2 *If K is a field and v a discrete valuation of K such that K is* complete *with respect to the topology defined by v, and the residue field k is* finite[2]*, then K will be called a* local field.

[1] for there certainly exists a maximal ideal of $\mathcal{O}_K$, which must be prime and so is $\mathfrak{m}_K$

[2] More generally, for the purposes of local class field theory, it is sufficient to take k to be *quasi-finite*. For a treatment of the quasi-finite residue field case, see [1], chapter 8, §2.

4.3 Extensions of Local Fields

If L/K is a finite extension and K is complete under a discrete valuation v, then v extends uniquely to L. That is to say, there is a unique discrete valuation w of L with $w\Big|_K = v$. L is again *complete* with respect to the topology defined by w. This is shown in [1] to follow from the structure of L as a *topological vector space* over K, using results about such spaces in [9].

It is clear that a finite extension of a local field is again a local field.

We classify these extensions according to their "ramification properties". If π_L, π_K are uniformisers of L and K respectively then the ratio of valuations

$$\frac{w(\pi_K)}{w(\pi_L)} =: e_{L/K}$$

is called the *ramification index* of L/K. Note that if w' is a normalised multiple of w then $e_{L/K} = w(\pi_K)$. If $e = 1$ then π_K is also a uniformiser of L.

Note that $\mathfrak{m}_K = \mathfrak{m}_L \cap \mathcal{O}_K$ - just look at the valuations under w. Hence there is a natural injective homomorphism

$$\mathcal{O}_K/\mathfrak{m}_K \longrightarrow \mathcal{O}_L/\mathfrak{m}_L$$

on the residue fields; ie. $l = \mathcal{O}_L/\mathfrak{m}_L$ is an *extension* of k. It can be shown that $\mathcal{O}_L$ is always a finitely-generated module over $\mathcal{O}_K$ ([1], Chapter 2, §2, Proposition 3), hence l/k is a finite extension. Define

$$f_{L/K} := [l : k];$$

it is called the *residue degree* of L/K. $e_{L/K}$ and $f_{L/K}$ are connected by the *fundamental identity*

$$[L : K] = e_{L/K} f_{L/K}.$$

See [1], Chapter 1, §5, Proposition 10.

Definition 4.3.1 *Let L/K be a finite extension of a field K which is complete with respect to a discrete valuation. If $e_{L/K} = 1$ and the residue extension l/k is* separable[3] *then we say L/K is an* unramified *extension.*

This is the simplest case, and it turns out to be the most important when discussing the Brauer groups. It is particularly easy to work with because any uniformiser π_L of L is actually an element of K, and so fixed by K-linear maps such as those in $\mathrm{Gal}(L/K)$. We will make extensive use of the following fundamental results about unramified extensions, for which we refer to [1], Chapter 3, §6, Theorem 3.

[3] If K is a local field then this is always the case, since then k is a finite field and so is perfect, namely won't admit inseparable extensions.

Theorem 4.3.2 *Let L/K be a finite unramified extension, where K is a field complete with respect to a discrete valuation. Let l/k be the corresponding residue extension. Let L'/K be any finite extension, with residue extension l'/k. Then there is an isomorphism from the group of K-linear ring homomorphisms $L \longrightarrow L'$ to the group of k-linear ring homomorphisms $l \longrightarrow l'$. The isomorphism is defined by restricting a map $L \longrightarrow L'$ to a map $\mathcal{O}_L \longrightarrow \mathcal{O}_{L'}$ and then reducing modulo the respective maximal ideals.*

Corollary 4.3.3 *With the hypotheses of the theorem,* $\mathrm{Gal}(L/K)$ *is canonically isomorphic to* $\mathrm{Gal}(l/k)$*.*

Corollary 4.3.4 *If M/K is a finite extension where K is as in the theorem, and m/k the corresponding residue extension, then the subextensions L/K of M/K which are unramified are in 1-1 correspondence with the separable subextensions l/k of m/k.*

The union of all the unramified extensions of K within an algebraic closure of K is called the *maximal unramified extension of* K and written K_{nr}. The unique extension of discrete valuations on the finite level shows that K_{nr} has a discrete valuation, and is unramified in the sense that it has π_K as a uniformiser. K_{nr} is also a Galois extension. Its residue field is the *separable closure* k_s of k (see §3.1). Since this is infinite, we note that K_{nr} is not a local field in our sense.

4.4 Unramified Extensions and Brauer Groups

We return to the question of determining the Brauer Group of a local field K. In Corollary 4.1.2, set $M = K_{nr}$. We get an exact sequence

$$0 \longrightarrow H^2(K_{nr}/K) \longrightarrow \mathrm{Br}(K) \longrightarrow \mathrm{Br}(K_{nr})$$

We will prove soon:

Theorem 4.4.1 $\mathrm{Br}(K_{nr}) = 0$.

It follows then that

Theorem 4.4.2 $\mathrm{Br}(K) = H^2(K_{nr}/K)$.

Hence the unramified extensions of K are sufficient to determine its Brauer group $H^2(K_s/K)$.

There are a number of possible approaches to proving this theorem. In [1], Chapter 12, §1, Theorem 1, Serre uses results about the norm map in finite, "totally ramified" extensions to show that only unramified extensions are needed to determine $\mathrm{Br}(K)$. Alternatively, in [5], §§1.4, 1.5 he takes a different approach by looking at subgroups of the unit group in a finite extension L/K, and applying a technical result.

The third method is to use the interpretation of the Brauer group in terms of central simple algebras. This is the method we use here.

Let K be a field complete under a (normalised) discrete valuation v and D a central division algebra of rank n^2 over K. We wish to extend the discrete valuation on K to a "discrete valuation" on D.

For this we use the absolute norm map $N_{D/K} : D \longrightarrow K$ (see Appendix E, §E.7). One can also use the reduced norm Nrd. For $x \in D^*$, set

$$w(x) = \frac{1}{n^2} v(N_{D/K}(x))$$

and let $w(0) = +\infty$. Then $w : D^* \longrightarrow \frac{1}{n^2}\mathbb{Z}$ is a homomorphism and $w\Big|_K = v$ since $N_{D/K}(y) = y^{n^2}$ for $y \in K$.

Now consider the restriction of w to a commutative subfield L of D containing K. We know (Proposition E.7.2) that $N_{D/K}(\lambda) = N_{L/K}(\lambda)^{[D:L]}$ for all $\lambda \in L$, so that $w(\lambda) = \frac{[D:L]}{n^2} v(N_{L/K}(\lambda))$.

Now it follows from unique extension of the valuation of K to a valuation of L (see §4.3 and [1], Chapter 2, §2, Proposition 3) that $v \circ N_{L/K}$ is a multiple of the valuation of L; in particular, w restricts to a discrete valuation of L. Apply this to the field $K(x^{-1}y)$ for $x, y \in D^*$; it shows that

$$w(1 + x^{-1}y) \geq \min\{w(1), w(x^{-1}y)\}.$$

Add $w(x)$ to each side to see that $w(x + y) \geq \min\{w(x), w(y)\}$.

Hence w satisfies all the axioms (Definition 4.2.1) of a usual discrete valuation on a commutative field.

In particular, the ring of integers of a commutative subfield L of D containing K is $\{x \in L : w(x) \geq 0\}$ and the maximal ideal is $\{x \in L : w(x) > 0\}$. L is complete in the topology defined by w, since w extends v.

Theorem 4.4.3 *Let K be a field complete under a discrete valuation and having perfect residue field. Then every nontrivial finite dimensional central division algebra D over K contains a proper unramified extension of K.*

PROOF - Let D have rank n^2 over K. Suppose $n^2 > 1$ but K does not have a proper unramified extension in D. Then for each field L with $D \supseteq L \supseteq K$, the residue field $l = k$; otherwise by Corollary 4.3.4 there is an unramified extension of K in L, not equal to K.

Let $b \in D$ have $w(b) \geq 0$. Then b reduces modulo the maximal ideal of $\mathcal{O}_{K(b)}$ to an element $\bar{a}$ of k, and lifting to $a \in \mathcal{O}_K$ shows that $w(b - a) > 0$. Choose $\pi \in D$ with minimal positive valuation (a *uniformiser* of D), then $b = a + \pi b_1$ with $w(b_1) \geq 0$. Repeating this procedure for b_1 gives a series for b:

$$b = a + \pi a_1 + \pi^2 a_2 + \dots \qquad a, a_i \in \mathcal{O}_K.$$

$K(\pi)$ is complete with respect to the topology defined by w. Hence $b \in K(\pi)$. Now any $x \in D$ has $w(\pi^\nu x) \geq 0$ for some positive integer ν and so is equal to $\pi^{-\nu} b$ for some such b. Hence $D \subseteq K(\pi)$ and so is commutative - contradicting the assumption that D has centre K and $n^2 > 1$.

□

Corollary 4.4.4 *When K is as in the proposition,* $\mathrm{Br}(K_{nr}) = 0$

PROOF - If D is a finite dimensional central division algebra over K_{nr} of rank > 1, then D contains a proper finite unramified extension L of K_{nr}. Hence by Corollary 4.3.4 the residue extension l/k_s (where k_s is the separable closure of k - see §4.3) is nontrivial and separable, which is impossible by the maximality of k_s.

□

This proves Theorem 4.4.1.

Soon we will calculate $H^2(K_{nr}/K) = \mathrm{Br}(K)$ for a local field K. This turns out to be related to the Brauer group of the residue field k, by Witt's theorem (4.8.2). We therefore turn now to determining the Brauer group of a finite field. We show a general criterion for vanishing of the Brauer group, and show that finite fields have this property.

4.5 Quasi-Algebraically Closed Fields

Definition 4.5.1 *A field K is called* quasi-algebraically closed, *or C_1, or a* Chevalley field, *if it has the following property.*

- *Every nonzero homogeneous polynomial $f \in K[X_1, \ldots, X_n]$ of degree $< n$ has a nontrivial zero $0 \neq \mathbf{x} \in K^n$.*

Proposition 4.5.2 *if K is C_1 then* $\mathrm{Br}(K) = 0$.

PROOF - Let D be a finite dimensional central division algebra over K of rank n^2. Fix a K-basis $(u_1, \ldots, u_{n^2})$ of D; then the *reduced norm* (Appendix E §E.7)

$$\mathrm{Nrd}(x_1 u_1 + \ldots + x_{n^2} u_{n^2}) = f(x_1, \ldots, x_{n^2}) \qquad x_i \in K$$

for f homogeneous of degree n in $K[X_1, \ldots, X_{n^2}]$, by Proposition E.7.4. The same proposition shows that the only zero of Nrd in D is 0. Hence the only zero of f is K^{n^2} is 0. So by the C_1 property, $\deg f = n \geq n^2$. Thus $n = 1$ and $D = K$.

So all central division algebras over K are trivial and $\mathrm{Br}(K) = 0$.

□

Remark 4.5.3 *In fact the fields K_{nr} are C_1. This was proved by S. Lang in "On Quasi-Algebraic Closure", Annals of Mathematics 55 (1952), pp. 373-390.*

4.6 Finite Fields are Quasi-Algebraically Closed

This proof may be found in [12], Chapters 2 and 3. Let $F = \mathbb{F}_q$, the finite field of q elements.

Proposition 4.6.1 *Define the d-th power sum for a finite field F by*

$$S_d = \sum_{x \in F} x^d \qquad d = 1, 2, \ldots$$

Then $S_d = -1$ if $q-1|d$ and 0 otherwise.

PROOF - Since $x^q = x$ for all $x \in F$, S_d depends only on the congruence class of d mod. $q-1$.

$$S_{q-1} = \sum_{x \in F - \{0\}} 1 = q - 1 = -1.$$

So assume $1 \leq d \leq q-1$, and choose $b \in F^*$ with $b^d \neq 1$, ie. not one of the d roots of $X^d - 1 = 0$. Then since multiplication by b permutes F, we have $S_d = b^d S_d$, so that S_d must be zero.

□

Proposition 4.6.2 *Let $f \in F[X_1, \ldots, X_n]$ have degree $d < n(q-1)$. Then*

$$\sum_{\mathbf{x} \in F^n} f(\mathbf{x}) = 0$$

PROOF - It suffices to prove this for each monomial $g(X_1, \ldots, X_n) = X_1^{a_1} X_2^{a_2} \ldots X_n^{a_n}$ with $\sum a_i = d < n(q-1)$. If, say, $a_1 = 0$ then each value $g(*, x_2, \ldots, x_n)$ appears q times in the sum and so the sum is zero. So assume no $a_i = 0$. Then

$$\begin{aligned}
\sum_{\mathbf{x} \in F^n} g(\mathbf{x}) &= \sum_{(x_1, \ldots, x_n)} x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} \\
&= \Big(\sum_{x \in F} x^{a_1}\Big)\Big(\sum_{x \in F} x^{a_2}\Big) \ldots \Big(\sum_{x \in F} x^{a_n}\Big) \\
&= S_{a_1} S_{a_2} \ldots S_{a_n}
\end{aligned}$$

But $a_1 + \ldots + a_n < n(q-1)$ so $0 < a_i < q-1$ for at least one index i. Then the factor $S_{a_i} = 0$.

□

Theorem 4.6.3 *Let $f \in F[X_1, \ldots, X_n]$ have degree $d < n$. Then the number of zeros of f in F^n is divisible by $p = \mathrm{char}\, F$.*

PROOF - Let $V = f^{-1}(\{0\}) \subseteq F^n$. Put $\bar{f} = 1 - f^{q-1}$, then $\bar{f}$ is the characteristic function[4] of V, and

$$\sum_{\mathbf{x} \in F^n} \bar{f}(\mathbf{x}) = \mathrm{Card}(V) \cdot 1_F$$

But $\deg \bar{f} = d(q-1) < n(q-1)$ and so by Proposition 4.6.2 this sum is $0 \in F$. Hence $p|\mathrm{Card}(V)$.

□

Corollary 4.6.4 *F is C_1.*

Remark 4.6.5 *The fact that $\mathrm{Br}(\mathbb{F}_q) = 0$ is a famous result called Wedderburn's Theorem (but not to be confused with the other result (Theorem E.2.2) also called Wedderburn's Theorem). It states that any finite division ring is commutative. We might compare it with the result that any finite integral domain is a field. The proof of that extends easily to the non-commutative case, and together these results show that any finite ring either has zero-divisors or is a field.*

There are many proofs of Wedderburn's theorem; an elementary one can be found in [10], Chapter 1, Theorem 1.

4.7 Unit Group of an Unramified Extension

Let K be a field complete under a discrete valuation and having perfect[5] residue field. We continue in the calculation of $\mathrm{Br}(K) = H^2(K_{nr}/K)$. To this end, let L be a finite unramified extension of K. Let $G = \mathrm{Gal}(L/K)$, then also $G = \mathrm{Gal}(l/k)$, the Galois group of the residue extension, by Theorem 4.3.2. Consider the exact sequence

$$0 \longrightarrow U_L \longrightarrow L^* \xrightarrow{v} \mathbb{Z} \longrightarrow 0. \tag{4.1}$$

We claim this is an exact sequence of G-modules, where G acts trivially on $\mathbb{Z}$. This is because any element of L^* is of the form $\pi_K^n u$, where π_K is a uniformiser of K (on which G acts trivially) and $u \in U_L$. Moreover, this sequence *splits*: the choice of π_K establishes a G-isomorphism $L^* \cong \mathbb{Z} \times U_L$ by $\pi_K^n u \longleftrightarrow (n, u)$.

Applying the covariant functor $H^q(G, ?)$ for $q \geq 0$ gives a split exact sequence

$$0 \longrightarrow H^q(G, U_L) \overset{\longleftarrow}{\longrightarrow} H^q(G, L^*) \overset{\longleftarrow}{\longrightarrow} H^q(G, \mathbb{Z}) \longrightarrow 0.$$

We want to show that $H^q(G, U_L) = H^q(G, l^*) = H^q(l/k)$, then this sequence will relate the cohomology of L to that of its residue field.

To do this, we define a *filtration* of the unit group. For integer $n \geq 0$, we define

$$U_L^{(n)} := \{x \in U_L : v(1-x) \geq n\}$$

[4]Meaning it takes the value $1 \in F$ on V and 0 elsewhere. This follows from $x^{q-1} = 1$ for $x \neq 0$.
[5]Note that we are most interested in the case where the residue field is finite, and then it is automatically perfect

Since

$$\begin{aligned} v\big((1-x)(1-y)\big) &= v\big((1-x)+(1-y)-(1-xy)\big) \\ &\geq \min\{v(1-x), v(1-y), v(1-xy)\}, \end{aligned}$$

each $U_L^{(n)}$ is a subgroup of $U_L = U_L^{(0)}$. Let us look at the quotients of successive groups.

Proposition 4.7.1 *If $n \geq 1, U_L^{(n)}/U_L^{(n+1)} \cong l$, the additive group of the residue field. If L/K is a finite unramified extension, this is as* $\mathrm{Gal}(L/K)$*-modules.*

PROOF - A general element of $U_L^{(n)}$ is $1+\pi_L^n y$ for $y \in \mathcal{O}_L$; map this to $\bar{y}$, the class of y in l. Then $(1+\pi_L^n y)(1+\pi_L^n y')$ maps to $\bar{y}+\bar{y'}$ so this is a homomorphism. It is clearly onto, and its kernel is $U_L^{(n+1)}$. If L/K is unramified, it is a $\mathrm{Gal}(L/K)$-homomorphism because for each s in the Galois group, $s(1+\pi_L^n y) = 1+\pi_L^n s(y)$ maps to $s(\bar{y})$.

□

Corollary 4.7.2 *If L/K is a finite unramified Galois extension with Galois group G, $H^q(G, U_L^{(n)}/U_L^{(n+1)}) = 0$ for each $n \geq 1, q \geq 1$.*

PROOF - This follows from the above isomorphism and Theorem 2.4.1.

□

Proposition 4.7.3 $H^q(G, U_L^{(1)}) = 0$*, for each $q \geq 1$.*

PROOF - This follows from a general result on the cohomology of filtered modules - see [1], Chapter 12, §3, Lemma 3. I will demonstrate the method. Let $f : G^q \longrightarrow U_L^{(1)}$ be a q-cocycle. Since $H^q(G, U_L^{(n)}/U_L^{(n+1)}) = 0$, there exists a $(q-1)$-cocycle $h_1 : G^{q-1} \longrightarrow U_L^{(1)}$ such that

$$f = \delta h_1 + f_1,$$

where $f_1 : G^q \longrightarrow U_L^{(2)}$ is a q-cochain with values in $U_L^{(2)}$. Applying this procedure to f_1 and iterating gives a sequence

$$\begin{aligned} f &= \delta h_1 + f_1 \\ f &= \delta h_1 + \delta h_2 + f_2 \\ &\vdots \\ f &= \delta h_1 + \delta h_2 + \ldots + \delta h_n + f_n. \end{aligned}$$

The valuation topology on L shows that the sequence h_1, $h_2, \ldots$ converges to a $(q-1)$-cochain $h : G^{q-1} \longrightarrow U_L^{(1)}$. Then the previous equations show that $f = \delta h$, so that $H^q(G, U_L^{(1)}) = 0$

$\square$

It remains to calculate $H^q(G, U_L)$. Let L/K be a finite unramified Galois extension with group G, and consider the exact sequence of G-modules[6]

$$0 \longrightarrow U_L^{(1)} \longrightarrow U_L \xrightarrow{p} l^* \longrightarrow 0$$

where p is reduction modulo the prime ideal of $\mathcal{O}_L$. Then the exact cohomology sequence and Proposition 4.7.3 give an isomorphism

$$H^q(G, U_L) \cong H^q(G, l^*) = H^q(l/k). \tag{4.2}$$

4.8 Witt's Theorem

The split short exact sequence 4.1 becomes, in view of 4.2,

$$0 \longrightarrow H^q(G, l^*) \longrightarrow H^q(G, L^*) \longrightarrow H^q(G, \mathbb{Z}) \longrightarrow 0.$$

Take the direct limit over the finite unramified Galois extensions L to obtain a split exact sequence

$$0 \longrightarrow H^q(k_s/k) \longrightarrow H^q(K_{nr}/K) \longrightarrow H^q(G, \mathbb{Z}) \longrightarrow 0,$$

with $G = \mathrm{Gal}(K_{nr}/K)$. So for $q = 2$, using Theorem 4.4.2, we have a split exact sequence

$$0 \longrightarrow \mathrm{Br}(k) \longrightarrow \mathrm{Br}(K) \longrightarrow H^2(G, \mathbb{Z}) \longrightarrow 0.$$

Of course, we now wish to identify $H^2(G, \mathbb{Z})$. For this, we use the exact sequence of G-modules (with trivial G-action):

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0 \tag{4.3}$$

Proposition 4.8.1 *For finite G, the G-module $\mathbb{Q}$ (with trivial G-action) is relatively injective (see Definition 1.1.7).*

PROOF - Consider the G-module $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q})$ (see §1.1.3). Let Q be the subset of maps which are constant on elements of G. It is an additive subgroup and a G-submodule, on which G acts trivially. Let Q' be the G-submodule of maps f such that $\sum_{g \in G} f(g) = 0$. Any element ϕ can be written as

$$\phi(s) = \frac{1}{|G|} \sum_{g \in G} \phi(g) + \big(\phi(s) - \frac{1}{|G|} \sum_{g \in G} \phi(g)\big) \in Q + Q',$$

and since $Q \cap Q' = 0$, have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], \mathbb{Q}) = Q \oplus Q'$ as G-modules. Since $\mathbb{Q}$ is clearly G-isomorphic to Q, we conclude that $\mathbb{Q}$ is relatively injective.

[6] Again, this is G-exact because G fixes the uniformisers of L

$\square$

Hence $H^q(G,\mathbb{Q}) = 0$ for all $q \geq 1$ and finite G. Indeed if G is *profinite* (see Chapter 2), then passing to the direct limit of these cohomology groups shows again that[7] $H^q(G,\mathbb{Q}) = 0$.

Thus the connecting homomorphism of the long exact cohomology sequence gives an isomorphism

$$H^1(G,\mathbb{Q}/\mathbb{Z}) \xrightarrow[\sim]{\delta} H^2(G,\mathbb{Z}),$$

and we recall (§1.2.2) that the trivial G-action means that $H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G,\mathbb{Q}/\mathbb{Z})$, the group of continuous group homomorphisms. Hence we have an isomorphism

$$H^2(G,\mathbb{Z}) \xrightarrow[\sim]{\delta^{-1}} \mathrm{Hom}_Z(G,\mathbb{Q}/\mathbb{Z}).$$

$\mathrm{Hom}_Z(G,\mathbb{Q}/\mathbb{Z})$ is called the (1-dimensional) *character group* of G.[8] We write it as $X(G)$.

To summarise, we have proved the following theorem.

Theorem 4.8.2 (Witt) *(reference: E. Witt, "Schiefkörper über diskret bewerteten Körpern",* J. reine ang. Math. *176, 1936, pp. 153-156)*

Let K be a field complete under a discrete valuation and having perfect residue field k. Let $G = \mathrm{Gal}(k_s/k) = \mathrm{Gal}(K_{nr}/K)$ and let $X(G)$ be its character group. Then there is a split exact sequence

$$0 \longrightarrow \mathrm{Br}(k) \longrightarrow \mathrm{Br}(K) \longrightarrow X(G) \longrightarrow 0.$$

By the results of §4.6, we know that if k is finite, $\mathrm{Br}(k) = 0$ and so then $\mathrm{Br}(K) = X(G)$.

4.9 The Group $\hat{\mathbb{Z}}$

We will need to use a "completion" of $\mathbb{Z}$. Recall the definition of an inverse system (Definition 2.2.5). Consider the projective system of finite cyclic groups

$$\mathbb{Z}/n\mathbb{Z},$$

over the directed set of positive integers ordered by division, where the morphism $\mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ for $m|n$ is given by the natural projection. We define

$$\hat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

$\hat{\mathbb{Z}}$ is thus a profinite group, called the *profinite completion of* $\mathbb{Z}$.

$\mathbb{Z}$ is included in $\hat{\mathbb{Z}}$ in an obvious way, so an integer M maps to $(M \mod n)_n \in \hat{\mathbb{Z}}$. In fact:

[7]We have to be careful about G here. For example, recall (§1.2.2) that $H^1(G,\mathbb{Q}) = \mathrm{Hom}_{\mathbb{Z}}(G,\mathbb{Q})$ because of the trivial G-action. If, say, $G = \mathbb{Z}$, this group is not zero.

[8]It is the *Pontrjagin Dual* of G/G', ie. $\mathrm{Hom}_Z(G/G',\mathbb{Q}/\mathbb{Z})$

Proposition 4.9.1 *$\hat{\mathbb{Z}}$ contains $\mathbb{Z}$ as a dense*[9] *subset.*

PROOF - Take an open set containing an element $(m_n)_n \in \hat{\mathbb{Z}}$. So (§2.2.3) this is a finite intersection of sets of the form

$$S_j = \Big((m_n)_n + 1 \times \prod_{k \neq j} \mathbb{Z}/k\mathbb{Z}\Big) \cap \hat{\mathbb{Z}}.$$

Take J to be a common multiple of all the j, and consider the integer $M = m_J$. We see that under the projection $\mathbb{Z}/J\mathbb{Z} \longrightarrow \mathbb{Z}/j\mathbb{Z}$, M maps to m_j, for each j. Hence the inclusion of M into $\hat{\mathbb{Z}}$ is in $\bigcap_j S_j$.

Thus every nonempty open set of $\hat{\mathbb{Z}}$ contains an integer, as required.

□

The group $\hat{\mathbb{Z}}$ is important to us because it arises as the absolute Galois group of a finite field. We recall from Appendix C the Galois Theory of finite fields. Let k be a finite field, then for each $n \geq 1$ there is a unique extension l of k of degree n. The extension is Galois, and $\mathrm{Gal}(l/k)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, where the Frobenius automorphism corresponds to the generator 1. We note that if m/k is another extension containing l, we have

$$[m : k] = [m : l][l : k]$$

and the Frobenius of l/k is the restriction of the Frobenius of m/k. Hence the natural projection $\mathrm{Gal}(m/k) \longrightarrow \mathrm{Gal}(l/k)$ corresponds under the isomorphism to the natural projection

$$\mathbb{Z}/[m : k]\mathbb{Z} \longrightarrow \mathbb{Z}/[l : k]\mathbb{Z}.$$

So we have an isomorphism of inverse systems[10].

The union of all the l is the *separable closure* of k. The results of Chapter 2 §2.2.4 give us

$$\mathrm{Gal}(k_s/k) = \varprojlim_l \mathrm{Gal}(l/k) = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Now let K be a local field and K_{nr} its maximal unramified extension (see §§4.2, 4.3). It follows from Corollary 4.3.3 that also $\mathrm{Gal}(K_{nr}/K) = \hat{\mathbb{Z}}$.

We are now ready to identify the character group $X(G)$ in Theorem 4.8.2, where $G = \mathrm{Gal}(k_s/k) = \hat{\mathbb{Z}}$. Recall this is the group of continuous homomorphisms from $\hat{\mathbb{Z}}$ into $\mathbb{Q}/\mathbb{Z}$. But because of Proposition 4.9.1, we see that a continuous homomorphism

$$\phi : \hat{\mathbb{Z}} \longrightarrow \mathbb{Q}/\mathbb{Z}$$

is defined completely by the value $\phi(1)$; ie.

[9] Meaning that the closure of $\mathbb{Z}$ in $\hat{\mathbb{Z}}$ is all of $\hat{\mathbb{Z}}$; every element of $\hat{\mathbb{Z}}$ can be "approximated arbitrarily closely" by an integer

[10] This means a system of isomorphisms between each element of the inverse systems which is compatible with the projections in each system.

Proposition 4.9.2 *The map*

$$\begin{array}{rccl} \gamma: & \mathrm{Hom}^{cont}_{\mathbb{Z}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & \phi & \longmapsto & \phi(1) \end{array}$$

is an isomorphism.

4.10 The Invariant Map

We have proved:

Theorem 4.10.1 *Let K be a local field. Then*

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

PROOF - This follows from

- Theorem 4.4.2;
- Witt's Theorem (4.8.2);
- Wedderburn's Theorem (§4.6) applied to the residue field k;
- Proposition 4.9.2.

□

We write

$$\mathrm{inv}_K : \mathrm{Br}(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}.$$

Let us retrace our steps to see how inv_K is calculated. For each finite unramified Galois extension L/K, the sequence (4.1) and Witt's Theorem (4.8.2) show that the valuation induces an isomorphism

$$H^2(L/K) \longrightarrow H^2(\mathrm{Gal}(L/K), \mathbb{Z}).$$

If $M \supseteq L$ is another unramified extension of K, then the valuation of M restricts to the valuation of L, by the unramified condition. Hence we passed to the direct limit over L to obtain an isomorphism

$$H^2(K_{nr}/K) \longrightarrow H^2(\hat{\mathbb{Z}}, \mathbb{Z}).$$

Now the connecting homomorphism which comes from the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

gives

$$H^2(\hat{\mathbb{Z}}, \mathbb{Z}) \xrightarrow[\sim]{\delta^{-1}} H^1(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}).$$

Finally, we let γ represent the evaluation map at 1. We may describe inv_K by $\mathrm{inv}_K = \gamma \circ \delta^{-1} \circ v$:

$$\mathrm{Br}(K) = H^2(K_{nr}/K) \xrightarrow{v} H^2(\hat{\mathbb{Z}}, \mathbb{Z}) \xrightarrow{\delta^{-1}} \mathrm{Hom}_{\mathbb{Z}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\gamma} \mathbb{Q}/\mathbb{Z}.$$

4.11 Properties of the Invariant Map

Proposition 4.11.1 *Let K be a local field, L/K a finite extension of degree n. Then $K_{nr} \subseteq L_{nr}$. The diagram*

$$\begin{array}{ccc} H^2(K_{nr}/K) & \xrightarrow{\text{Res}} & H^2(L_{nr}/L) \\ \downarrow\text{inv}_K & \square & \downarrow\text{inv}_L \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes.

PROOF - Let $G_K = \text{Gal}(K_{nr}/K)$, $F_K \in G_K$ the Frobenius automorphism[11], G_L and F_L similarly for L. If $f := [l : k]$ denotes the residue degree, then $F_L = (F_K)^f$. Let e be the ramification index of L/K. Consider the diagram

$$\begin{array}{ccccccc} H^2(G_K, K_{nr}^*) & \xrightarrow{v_K} & H^2(G_K, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & \text{Hom}_{\mathbb{Z}}^{cont}(G_K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow\text{Res} & \square & \downarrow e\text{Res} & \square & \downarrow e\text{Res} & \square & \downarrow n \\ H^2(G_L, L_{nr}^*) & \xrightarrow{v_L} & H^2(G_L, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & \text{Hom}_{\mathbb{Z}}^{cont}(G_L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\gamma_L} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

In this diagram $\gamma_{K,L}$ are evaluation at the Frobenius. The diagram commutes by the basic results about ramification in §4.2 and the fundamental identity $ef = n$.

Because $\text{inv} = \gamma \circ \delta^{-1} \circ v$ (§4.10), we have the desired result.

$\square$

Corollary 4.11.2 *For any Galois extension L/K of degree n, $H^2(L/K)$ is cyclic of degree n, and generated by the unique element $u_{L/K} \in \text{Br}(K)$ such that $\text{inv}_K(u_{L/K}) = 1/n$.*

Note that we are not assuming the extension to be unramified any more.
PROOF - Recall that the inclusion $H^2(L/K) \hookrightarrow \text{Br}(K)$ is given by inflation. Then the restriction-inflation sequence (Corollary 4.1.2)

$$0 \longrightarrow H^2(L/K) \xrightarrow{\text{Inf}} \text{Br}(K) \xrightarrow{\text{Res}} \text{Br}(L)$$

shows $H^2(L/K)$ is the kernel of Res. By $\text{inv}_L \circ \text{Res} = n\text{inv}_K$, and injectivity of inv, we have that $\text{inv}_K(\ker \text{Res})$ consists of all those $a \in \mathbb{Q}/\mathbb{Z}$ such that $na = 0$; ie. it is the subgroup $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Hence $\ker \text{Res}$ is also cyclic of order n, generated by $\text{inv}_K^{-1}(1/n)$.

$\square$

Corollary 4.11.3 *1.* $\text{Res} : H^2(K_{nr}/K) \longrightarrow H^2(L_{nr}/L)$ *is surjective.*

[11] This is the element of the Galois group which corresponds to the q-th power map in the residue extension k_s/k, where $\text{Card}(k) = q$. The correspondence is via Theorem 4.3.2. It is identified with the topological generator $1 \in \hat{\mathbb{Z}}$.

2. Cor : $H^2(L_{nr/L}) \longrightarrow H^2(K_{nr}/K)$ *is injective.*

3. $\mathrm{inv}_K \circ \mathrm{Cor} = \mathrm{inv}_L$.

PROOF - (1) follows because $\mathrm{Res} = \mathrm{inv}_L^{-1} \circ n \circ \mathrm{inv}_K$, a composition of surjective maps. Then (3) is a consequence of Proposition 1.5.13, because

$$\mathrm{inv}_L \circ \mathrm{Res} = n\mathrm{inv}_K = \mathrm{inv}_K \circ \mathrm{Cor} \circ \mathrm{Res},$$

and Res is surjective. Finally, (3) implies (2) by the injectivity of inv_L.

□

We summarise the position of Inf relative to inv in the following proposition.

Proposition 4.11.4 *Let $L \supseteq M \supseteq K$ be a tower of finite extensions of local fields with L/K and M/K Galois. Let $a = [L : M]$, $b = [M : K]$. Then the following diagram commutes.*

$$\begin{tikzcd}
0 \arrow[r] & H^2(M/K) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{inv}_K"] \arrow[dr, phantom, "\square"] & H^2(L/K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] \arrow[dr, phantom, "\square"] & H^2(L/M) \arrow[d, "\mathrm{inv}_M"] \\
0 \arrow[r] & \frac{1}{b}\mathbb{Z}/\mathbb{Z} \arrow[r, hook] & \frac{1}{ab}\mathbb{Z}/\mathbb{Z} \arrow[r, "b"] & \frac{1}{a}\mathbb{Z}/\mathbb{Z}.
\end{tikzcd}$$

PROOF - The first square commutes because inflations are the homomorphisms in the direct limit, and so we have the commutative diagram:

$$\begin{tikzcd}
 & \varinjlim_E H^2(E/K) \arrow[r, "\mathrm{inv}_K"] & \mathbb{Q}/\mathbb{Z} \\
H^2(L/K) \arrow[ur, "\mathrm{Inf}"] & & \\
H^2(M/K) \arrow[u, "\mathrm{Inf}"] \arrow[uur, "\mathrm{Inf}"'] & &
\end{tikzcd}$$

The images of $H^2(M/K)$, $H^2(L/K)$ are $\frac{1}{b}\mathbb{Z}/\mathbb{Z}$, $\frac{1}{ab}\mathbb{Z}/\mathbb{Z}$ by Corollary 4.11.2. The second square commutes by Proposition 4.11.1.

□

We shift our attention now to the canonical generators of the cohomology groups. If L/K is a finite extension of local fields of degree n, we write $u_{L/K} := \mathrm{inv}_K^{-1}(1/n) \in H^2(L/K)$.

Proposition 4.11.5 *Let K be a local field and $L \supseteq M \supseteq K$ be a tower of finite extensions with L/K Galois.*

1. If M/K is also Galois then $\mathrm{Inf}(u_{M/K}) = [L : M]u_{L/K}$.

2. $\mathrm{Res}(u_{L/K}) = u_{L/M}$.

3. $\mathrm{Cor}(u_{L/M}) = [M : K]u_{L/K}$.

All this follows easily from the results of this section.

4.12 The Reciprocity Map

Recall Tate's Theorem (1.6.4). We have now established enough facts about $\mathrm{Br}(K)$, when K is a local field, to apply this theorem. If L/K is a finite Galois extension, we know that for each Galois subextension M, $H^2(\mathrm{Gal}(L/M), L^*)$ is cyclic of order $[L:M] = |\mathrm{Gal}(L/M)|$ and generated by $u_{L/M}$. Furthermore, $u_{L/M} = \mathrm{Res}(u_{L/K})$. We conclude by Tate's Theorem:

Theorem 4.12.1 *Let L/K be a finite Galois extension of local fields with group G. Then for all $n \in \mathbb{Z}$, the map*

$$\begin{array}{rccc} \theta_n : & \hat{H}^n(G,\mathbb{Z}) & \longrightarrow & \hat{H}^{n+2}(G,L^*) \\ & x & \longmapsto & x \cdot u_{L/K}, \end{array}$$

where $\cdot$ denotes cup product, is an isomorphism.

We are particularly interested in the case $n = -2$. Then

$$\theta_{-2} : G/G' \longrightarrow K^*/NL^*$$

is an isomorphism relating the abelianisation of the Galois group to the multiplicative group of the field. The inverse of this isomorphism will be called the *norm residue symbol* and denoted

$$\begin{array}{ccccc} K^* & \longrightarrow & K^*/NL^* & \longrightarrow & G/G' \\ a & \longmapsto & & & (a, L/K) \end{array}$$

It is so called because $(a, L/K) = 1$ if and only if a is the norm of an element of L.

The next proposition lists some of the functorial properties of the norm residue symbol, which is denoted in the proposition by the vertical arrows.

Proposition 4.12.2 *Let K be a local field, $L \supseteq M \supseteq K$ a tower of finite extensions with L/K Galois. Then:*

1. *The morphism* Cor *gives a commutative diagram*

$$\begin{array}{ccc} M^* & \stackrel{norm}{\longrightarrow} & K^* \\ \downarrow & \square & \downarrow \\ \mathrm{Gal}(L/M)^{ab} & \stackrel{can.}{\longrightarrow} & \mathrm{Gal}(L/K)^{ab}. \end{array}$$

   Here "can." denotes the canonical map induced by inclusion of Galois groups.

2. *The morphism* Res[12] *gives a commutative diagram*

$$\begin{array}{ccc} K^* & \hookrightarrow & M^* \\ \downarrow & \square & \downarrow \\ \mathrm{Gal}(L/K)^{ab} & \stackrel{\mathrm{Res}}{\longrightarrow} & \mathrm{Gal}(L/M)^{ab}. \end{array}$$

[12]The map $G/G' \longrightarrow H/H'$, where H is a subgroup of G, defined by $\mathrm{Res} : \hat{H}^{-2}(G,\mathbb{Z}) \longrightarrow \hat{H}^{-2}(H,\mathbb{Z})$, is classically called the *transfer*, written "Ver".

3. If M/K is Galois, we have a commutative diagram

$$\begin{array}{ccc} K^* & = & K^* \\ \downarrow & \square & \downarrow \\ \mathrm{Gal}(L/K)^{ab} & \xrightarrow{proj.} & \mathrm{Gal}(M/K)^{ab}. \end{array}$$

The proof of this can be found in [1], Chapter 11. For (1) and (2) it follows from Proposition 4.11.5 and properties of Cor and Res relative to the cup product. For (3) it requires some more detailed cup-product calculations.

The property (3) shows that the norm residue symbols define together a homomorphism

$$\psi : K^* \longrightarrow \varprojlim_E \mathrm{Gal}(E/K)^{ab},$$

where E runs through all finite Galois extensions, since the norm residue symbols form a consistent system with respect to the projections in the projective limit.

It can be shown that this projective limit is equal to the abelianisation of the absolute Galois group of K, $\mathrm{Gal}(K_s/K)^{ab}$. This is the Galois group of the maximal abelian extension of K.

The map ψ is called the *Artin Reciprocity Map.* It is *almost* an isomorphism, in the sense that for any finite Galois extension L of K, we have the diagram

$$\begin{array}{ccc} K^* & \xrightarrow{\psi} & \mathrm{Gal}_K^{ab} \\ \downarrow & \square & \downarrow \\ K^*/NL^* & \underset{\sim}{\xrightarrow{(?,L/K)}} & \mathrm{Gal}(L/K)^{ab}, \end{array}$$

and the bottom row is an isomorphism.

This shows that Gal_K^{ab} is isomorphic to $\varprojlim_E K^*/NE^*$, the *completion of K^* with respect to the norm topology.* We see that for a local field, the Galois group of its maximal abelian extension is precisely related to its multiplicative structure.

It will not be possible to study the norm topology here. The main result is:

Theorem 4.12.3 (The Existence Theorem) *Let H be a subgroup of K^*. Then $H = NE^*$ for some finite Galois extension E/K if and only if H is closed and of finite index in K^*.*

E is called a *class field* for H. For more details, see [1], Chapters 11 and 14.

Conclusion

The general group cohomology theory of Chapter 1 allows us to build a bridge between field arithmetic and the Galois group, via the appearance as Tate cohomology groups of

$$\begin{aligned}\hat{H}^0(\mathrm{Gal}(L/K), L^*) &= K^*/NL^* \\ \hat{H}^{-2}(G, \mathbb{Z}) &= G/G'.\end{aligned}$$

We saw in Tate's Theorem (1.6.4) that to do this we need certain properties of groups $H^2(L/K)$. In Chapter 3 we investigated the arithmetical significance of these groups. Then in Chapter 4 we studied local fields and showed that they give a context in which Tate's Theorem applies. As a result, the Artin reciprocity law could be established.

This is only the starting point of class field theory. I will discuss some of the possibilities for application of the theory, and for further investigation of problems suggested by this text.

The Brauer groups and central-simple algebras of Chapter 3 arise in problems of number-theory and algebraic geometry, and investigation of their properties is a subject of research. They are relevant to function fields of algebraic curves.

On the theme of investigating Galois groups, we note that we have only looked at the abelianised group. This is equivalent to the determination of all the one-dimensional representations of G, ie. all homomorphisms

$$G \longrightarrow \mathbf{GL}(n, \mathbb{C}),$$

where $n = 1$. For larger n, this is the problem of higher-dimensional Galois representation and is also the subject of research.

Artin's reciprocity map itself is worthy of much more attention than it was possible to give it here. The definition is not very helpful when it comes to actually trying to evaluate this function, and the difficulty of doing this turns out to depend greatly on the properties of a given extension of local fields L/K. The discussion is phrased in terms of "local symbols", which prove relatively easy to calculate in the case of a "tamely ramified" extension and much more complicated otherwise.

We find that Artin's map is helpful in studying the *ramification groups* of an extension of local fields (see [1], Chapter 4, and Anne Esslemont's part of this project). Under the reciprocity map, these correspond precisely to the filtration of the unit group in §4.7.

Local class field theory as introduced here is taken as the basis for *global class field theory*. Consider for example a Galois number field K (ie. $K/\mathbb{Q}$ is a finite Galois extension). All the absolute values on K are either Archimedean, and so related to the usual norms on $\mathbb{R}$ and $\mathbb{C}$, or come from discrete valuations (a theorem of Ostrowski). The completions of K for each of these valuations may be studied via local class-field theory, with applications to studying the Galois group and investigating factorisation in the field.

Appendix A

Homology of Complexes

A.1 Complexes

Definition A.1.1 *Let R be a ring. A* complex $\mathbf{A}$ *of R-modules is a doubly-infinite sequence of modules and homomorphisms*

$$\dots \xrightarrow{d_3} A_2 \xrightarrow{d_2} A_1 \xrightarrow{d_1} A_0 \xrightarrow{d_0} A_{-1} \xrightarrow{d_{-1}} \dots \tag{A.1}$$

such that $d_q \circ d_{q+1} = 0$ for each $q \in \mathbb{Z}$

For each $q \in \mathbb{Z}$, $\operatorname{im} d_{q+1}$ is a submodule of $\ker d_q$, because $d_q \circ d_{q+1} = 0$. We define the q-th *homology group* of $\mathbf{A}$ to be the quotient:

$$H_q(\mathbf{A}) := \frac{\ker d_q}{\operatorname{im} d_{q+1}}$$

Remember that if $\operatorname{im} d_{q+1} = \ker d_q$ then (A.1) is an *exact sequence*, in which case it will also be called an *acyclic complex*, and we see that it has zero homology. So in a sense, the homology groups measure the "inexactness" of the sequence (A.1). Note that for each $q \in \mathbb{Z}$, $H_q(\mathbf{A})$ is a quotient group of a subgroup of A_q. We will be particularly concerned with the case $R = \mathbb{Z}$, so that "R-module" means abelian group.

There is now a large amount of arcane jargon to introduce, which comes from the origination of homology in the study of topological surfaces.

Definition A.1.2
1. *A complex of $\mathbb{Z}$-modules (A.1) will also be called a* chain complex. *An element of A_q is a* q-dimensional chain *or* q-chain.
2. *The q-dimensional chains in* $\ker d_q$ *are called* q-dimensional cycles *or* q-cycles. *Those q-chains which are in* $\operatorname{im} d_{q+1}$ *are called* q-boundaries; *they are necessarily q-chains because $d_q \circ d_{q+1} = 0$. d_q is called the q-dimensional boundary operator.*

3. *Two q-cycles are called* homologous *if their difference is a q-boundary, ie. they give the same coset in* $H_q(\mathbf{A})$. *An element of* $H_q(\mathbf{A})$ *is called a* homology class. *A q-cycle is* homologous to zero *if it is homologous to the zero chain, ie. it is a q-boundary.*

A.2 Cohomology

Now let us write the sequence (A.1) differently, putting $A^q := A_{-q}$ and d_{-q} instead of d_q:

$$\ldots \xrightarrow{d_{-3}} A^{-2} \xrightarrow{d_{-2}} A^{-1} \xrightarrow{d_{-1}} A^0 \xrightarrow{d_0} A^1 \xrightarrow{d_1} \ldots \tag{A.2}$$

so $d_q \circ d_{q-1} = 0$. The $(-q)$-th homology group of this complex will now be written

$$H^q(\mathbf{A}) = \frac{\ker d_q}{\operatorname{im} d_{q-1}}$$

and called the *q-th cohomology group of* $\mathbf{A}$. A *q-dimensional cochain* will be a $(-q)$-dimensional chain; (A.2) will now be called a *cochain complex.* similarly we define "cocycles", "coboundaries", "cohomologous cocycles", etc.

This distinction at this stage seems artificial and confusing, since a cochain complex is just a chain complex differently written down. However, we will see later that the different numberings tend to arise in different ways, so that the distinction is useful in practice.

From now on we discuss only "cohomology", since this is the notation that will be used the most later on. There are obvious corresponding results for "homology", by renumbering.

A.3 Morphisms of Complexes

Definition A.3.1 *A morphism of complexes* $\mathbf{A} \longrightarrow \mathbf{B}$ *where*

$$\begin{aligned} \mathbf{A} &= \ldots \xrightarrow{d_{-1}} A^0 \xrightarrow{d_0} A^1 \xrightarrow{d_1} \ldots \\ \mathbf{B} &= \ldots \xrightarrow{d_{-1}} B^0 \xrightarrow{d_0} B^1 \xrightarrow{d_1} \ldots \end{aligned}$$

is a sequence of homomorphisms

$$\phi_q : A^q \longrightarrow B^q \qquad q \in \mathbb{Z}$$

such that for each $q \in \mathbb{Z}$, *the diagram*

$$\begin{array}{ccc} A^q & \xrightarrow{d_q} & A^{q+1} \\ \downarrow\phi_q & & \downarrow\phi_{q+1} \\ B^q & \xrightarrow{d_q} & B^{q+1} \end{array}$$

commutes (ie. ϕ *commutes with the coboundary operators).*

Morphisms of complexes are also called *chain maps.*

This definition of morphism makes the complexes into a pre-additive category. For any $q \in \mathbb{Z}$, the procedure $\mathbf{A} \longmapsto H^q(\mathbf{A})$ is then a *covariant functor* from the category of complexes to the category of abelian groups. For if $f : \mathbf{A} \longrightarrow \mathbf{B}$ is a morphism of complexes then for each $q \in \mathbb{Z}$ the homomorphism

$$f_q : A^q \longrightarrow B^q$$

carries $\ker d_q \subseteq A^q$ into $\ker d_q \subseteq B^q$ because $d_q \circ f_q = f_{q+1} \circ d_q$, and carries $\operatorname{im} d_{q-1} \subseteq A^q$ into $\operatorname{im} d_{q-1} \subseteq B^q$ because $d_{q-1} \circ f_{q-1} = f_q \circ d_{q-1}$.

Thus f_q defines a homomorphism

$$\begin{array}{rlcc} f_q^* : & \ker d_q/\operatorname{im} d_{q-1} & \longrightarrow & \ker d_q/\operatorname{im} d_{q-1} \\ \text{ie.} \quad f_q^* : & H^q(\mathbf{A}) & \longrightarrow & H^q(\mathbf{B}), \end{array}$$

called the *homomorphism induced by f in dimension q.* Since

$$(f_q \circ g_q)^* = f_q^* \circ g_q^* \qquad \text{and} \qquad (id_{A^q})^* = id_{H^q(\mathbf{A})}$$

H^q is a covariant functor. Since $(f_q + g_q)^* = f_q^* + g_q^*$ it is pre-additive. H^q is called the *q-dimensional cohomology functor.*

Definition A.3.2 *Let $f : \mathbf{A} \longrightarrow \mathbf{B}$ be a morphism of complexes. Then* $\ker f$ *and* $\operatorname{im} f$ *are the subcomplexes*

$$\ldots \xrightarrow{d_{-2}} \ker f_{-1} \xrightarrow{d_{-1}} \ker f_0 \xrightarrow{d_0} \ker f_1 \xrightarrow{d_1} \ldots$$
$$\ldots \xrightarrow{d_{-2}} \operatorname{im} f_{-1} \xrightarrow{d_{-1}} \operatorname{im} f_0 \xrightarrow{d_0} \operatorname{im} f_1 \xrightarrow{d_1} \ldots$$

Note that the relation $f_{q+1} \circ d_q = d_q \circ f_q$ shows that the coboundary maps restrict as required.

Thus a sequence of complexes

$$\ldots \mathbf{A} \xrightarrow{\alpha} \mathbf{B} \xrightarrow{\beta} \mathbf{C} \longrightarrow \ldots$$

is *exact at* $\mathbf{B}$ if $\operatorname{im} \alpha = \ker \beta$, ie. $\operatorname{im} \alpha_q = \ker \beta_q$ for all $q \in \mathbb{Z}$, and an *exact sequence* if it is exact at every place.

A.4 The Connecting Homomorphism

Consider now the "short exact sequence of complexes"

$$0 \longrightarrow \mathbf{A} \xrightarrow{i} \mathbf{B} \xrightarrow{p} \mathbf{C} \longrightarrow 0 \tag{A.3}$$

where 0 denotes the zero complex, so that i is injective, p surjective and $\ker p = \operatorname{im} i$. In this situation there is a "canonical homomorphism"

$$\delta_q : H^q(\mathbf{C}) \longrightarrow H^{q+1}(\mathbf{A})$$

which will now be defined.

What we want to do is get from the top-right to the bottom-left in the following diagram

$$\begin{array}{ccccc} A^q & \xrightarrow{i_q} & B^q & \xrightarrow{p_q} & C^q \\ \downarrow d_q & \Box & \downarrow d_q & \Box & \downarrow d_q \\ A^{q+1} & \xrightarrow{i_{q+1}} & B^{q+1} & \xrightarrow{p_{q+1}} & C^{q+1} \end{array}$$

Since $p \circ i = 0$, we will not have much luck trying to go too far horizontally. So omit some of the diagram to get

$$\begin{array}{ccccc} & & B^q & \xrightarrow{p_q} & C^q \\ & & \downarrow d_q & & \\ A^{q+1} & \xrightarrow{i_{q+1}} & B^{q+1} & & \end{array}$$

The necessary path is now clear. So starting with a cocycle $c \in C^q$, representing a cohomology class in $H^q(\mathbf{C})$, choose $b \in B^q$ with $p_q(b) = c$. This is possible because p_q is surjective. Now b is a cochain but not necessarily a cocycle. Applying now d_q to b gives a $(q+1)$-coboundary $d_q b$ in B^{q+1}; in particular, $d_q b$ is a $(q+1)$-cocycle. Now if we were to apply p_{q+1} to $d_q b$:

$$\begin{array}{ccc} B^q & \xrightarrow{p_q} & C^q \\ \downarrow d_q & \Box & \downarrow d_q \\ B^{q+1} & \xrightarrow{p_{q+1}} & C^{q+1} \end{array}$$

We would get $(p_{q+1} \circ d_q)b = (d_q \circ p_q)b = d_q c = 0$ because c is a cocycle. So in fact $d_q b \in \ker p_{q+1} = \operatorname{im} i_{q+1}$.

Now i_{q+1} is injective so there is a unique $(q+1)$-cochain $a = i_{q+1}^{-1}(d_q b)$ in A^{q+1}. a is a cocycle because $(i_{q+2} \circ d_{q+1})a = (d_{q+1} \circ i_{q+1})a = (d_{q+1} \circ d_q)b = 0$, and then the injectivity of i_{q+2} shows that $d_{q+1}a = 0$. Thus a defines a cohomology class in $H^{q+1}(\mathbf{A})$, which we propose to write $\delta_q c$.

What do we need to check to be sure that δ_q is a well-defined function $H^q(\mathbf{C}) \longrightarrow H^{q+1}(\mathbf{A})$? We have to show that $\delta_q c$ does not depend on the arbitrary choices we made in defining it. These were two: we chose the representative $c \in C^q$ of the cohomology class in $H^1(\mathbf{C})$, and we chose $b \in p_q^{-1}(\{c\})$.

Independence of b: If $b, b' \in p_q^{-1}(\{c\})$ then $p_q(b - b') = c - c = 0$ so $b - b' \in \ker p_q = \operatorname{im} i_q$, so that $b - b' = i_q(a)$ for some $a \in A^q$. Then

$$\begin{aligned} d_q b &= d_q(b' + i(a)) \\ &= d_q b' + (d_q \circ i_q)a \\ &= d_q b' + (i_{q+1} \circ d_q)a \end{aligned}$$

so that $(i_{q+1}^{-1} \circ d_q)b = (i_{q+1}^{-1} \circ d_q)b' + d_q a$ is cohomologous to $(i_{q+1}^{-1} \circ d_q)b'$.

Independence of c: Let c' be a q-cocycle cohomologous to c, so $c' = c + d_{q-1}c''$ for some $(q-1)$-cochain c''. Let $b \in B^q$ be such that $p_q b = c$ and $b'' \in B^{q-1}$ be such that $p_{q-1}b'' = c''$, then $p_q(b + d_{q-1}b'') = c + d_{q-1}c'' = c'$ so that we choose (as we now know we may) $b' = b + d_{q-1}b'' \in p_q^{-1}(\{c'\})$. Then, going to the next step in the evaluation of $\delta_q c$, $d_q b' = d_q b + (d_q \circ d_{q-1})b'' = d_q b$ so that we lose any dependence on c'', as required.

This shows that δ_q is a well-defined function. Lifting a sum of cocycles $c+c' \in C^q$ to $b + b' \in B^q$ shows $\delta_q(c + c') = i_{q+1}^{-1}(d_q b) + i_{q+1}^{-1}(d_q b) = \delta_q c + \delta_q c'$ so that δ_q is a group homomorphism. We write $\delta = i^{-1} \circ d \circ p^{-1}$ to mean "δ_q associates to the cohomology class of a cocycle $c \in C^q$ the cohomology class of $i_{q+1}^{-1}(d_q b)$ where $b \in p_q^{-1}(\{c\})$ may be chosen arbitrarily". δ_q is called the *connecting homomorphism in dimension q*.

A.5 The Exact Triangle

We can now show the central result of cohomology:

Theorem A.5.1 (Exact Triangle) *Let*

$$0 \longrightarrow \mathbf{A} \xrightarrow{i} \mathbf{B} \xrightarrow{p} \mathbf{C} \longrightarrow 0 \tag{A.4}$$

be an exact sequence of complexes. Define for each $q \in \mathbb{Z}$ the connecting homomorphism

$$\delta_q : H^q(\mathbf{C}) \longrightarrow H^{q+1}(\mathbf{A})$$

as above. Then the doubly infinite sequence of abelian groups

$$\ldots \overset{p^*_{q-1}}{\to} H^{q-1}(\mathbf{C}) \overset{\delta_{q-1}}{\to} H^q(\mathbf{A}) \overset{i^*_q}{\to} H^q(\mathbf{B}) \overset{p^*_q}{\to} H^q(\mathbf{C}) \overset{\delta_q}{\to} H^{q+1}(\mathbf{A}) \overset{i^*_{q+1}}{\to} \ldots \tag{A.5}$$

is exact.

PROOF - For $q \in \mathbb{Z}$ there are three places of exactness to check. We work with cocycle representatives of the cohomology classes for brevity.

1. $H^q(\mathbf{A})$: $\operatorname{im} \delta_{q-1} = \ker i^*_q$: $a \in A^{q-1}$ represents a cohomology class in $\ker i^*_q$ $\iff$ $i_q a$ is cohomologous to zero in B^{q-1} $\iff$ $i_q a = d_{q-1} b$ for some $b \in B^{q-1}$ $\iff$ $a = (i_q^{-1} \circ d_{q-1})b = \delta_{q-1}(p_{q-1}b)$ $\iff$ a represents a cohomology class in $\operatorname{im} \delta_{q-1}$.

2. $H^q(\mathbf{B})$: $\operatorname{im} i^*_q \subseteq \ker p^*_q$: $p_q \circ i_q = 0$ by exactness of (A.4). $\operatorname{im} i^*_q \supseteq \ker p^*_q$: Suppose a q-cocycle b has $p_q b$ cohomologous to zero in C^q, ie. $p_q b = d_{q-1} c$. Let $b' \in p_{q-1}^{-1}(\{c\})$ so that $p_q(b - d_{q-1}b') = 0$, so $b - d_{q-1}b' \in \ker p_q = \operatorname{im} i_q$, ie. $b - d_{q-1}b' = i_q a$ for some $a \in A^q$. Now

$$(i_{q+1} \circ d_q)a = (d_q \circ i_q)a = d_q b - (d_q \circ d_{q-1}b' = d_q b = 0$$

   This shows $d_q a = 0$ because i_{q+1} is injective. Thus b is cohomologous to $i_q(a)$.

3. $H^q(\mathbf{C})$: $\operatorname{im} p_q^* \subseteq \ker \delta_q$: If a q-cocycle $c = p_q b$ for some q-cocycle b then $\delta_q c$ is represented by $(i_{q+1}^{-1} \circ d_q)b = i^{-1}(0) = 0$. $\operatorname{im} p_q^* \supseteq \ker \delta_q$: if a q-cocycle c can be lifted to $b \in p_q^{-1}(\{c\})$ such that $(i_{q+1} \circ d_q)b$ is cohomologous to zero in A^{q+1} then $(i_{q+1} \circ d_q)b = d_q a$ for some $a \in A^q$. So

$$d_q b = (i_{q+1} \circ d_q)a = (d_q \circ i_q)a$$

Thus $c = p_q(b - i_q a)$ and $d_q(b - i_q a) = 0$ so that $b - i_q a$ is a q-cocycle.

$\square$

This result is called the exact triangle because of the diagram

$$\begin{array}{ccc} H(\mathbf{A}) & \xrightarrow{i^*} & H(\mathbf{B}) \\ \nwarrow^{\delta} & \triangledown & \swarrow_{p^*} \\ & H(\mathbf{C}) & \end{array}$$

The pair $\{H^q, \delta\}$ is said to form a *cohomological functor*. By this we mean that whenever we have two short exact sequences of complexes $0 \to \mathbf{A}' \to \mathbf{A} \to \mathbf{A}'' \to 0$ and $0 \to \mathbf{B}' \to \mathbf{B} \to \mathbf{B}'' \to 0$ and a morphism between them, ie. a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{A}' & \longrightarrow & \mathbf{A} & \longrightarrow & \mathbf{A}'' & \longrightarrow & 0 \\ & & \downarrow f' & \square & \downarrow f & \square & \downarrow f'' & & \\ 0 & \longrightarrow & \mathbf{B}' & \longrightarrow & \mathbf{B} & \longrightarrow & \mathbf{B}'' & \longrightarrow & 0 \end{array}$$

then the morphisms f', f, f'' induce a commutative diagram

$$\begin{array}{ccccccccc} \ldots \to & H^{q-1}(\mathbf{A}'') & \xrightarrow{\delta} & H^q(\mathbf{A}') & \to & H^q(\mathbf{A}) & \to & H^q(\mathbf{A}'') & \xrightarrow{\delta} \ldots \\ & \downarrow f''^*_{q-1} & \square & \downarrow f'^*_q & \square & \downarrow f^*_q & \square & \downarrow f''^*_q & \\ \ldots \to & H^{q-1}(\mathbf{B}'') & \xrightarrow{\delta} & H^q(\mathbf{B}') & \to & H^q(\mathbf{B}) & \to & H^q(\mathbf{B}'') & \xrightarrow{\delta} \ldots \end{array}$$

called a morphism of cohomology functors. This property is called "naturality of δ"; its verification is routine.

Appendix B

Non-Abelian Cohomology of Groups

[This appendix follows [1], Chapter 7, appendix]

B.1 Definitions

We consider the case of a *non-abelian G-module A*. This means that A is a group and we have a homomorphism

$$G \longrightarrow \mathrm{Aut}(A)$$

so that G acts on A. It turns out that it is still reasonable to define objects $H^0(G, A)$ and $H^1(G, A)$ and obtain an "exact sequence", shorter than the one we had before. The definition is a "hands-dirty" job, using the inhomogeneous cochains directly.

Throughout this section, we will denote composition in A by $(a, b) \mapsto a \cdot b$ and the G-action by $(g, a) \mapsto ga$.

Everything that we will say also makes sense in the context of the continuous cochains of §2.3.4.

Definition B.1.1 *Let A be a non-abelian G-module.*

1. $H^0(G, A) := A^G$

2. *A* 1-cochain of G with values in A *is a map*

$$f : G \longrightarrow A$$

3. *A* 1-cocycle of G with values in A *is a 1-cochain with $f[st] = f[s] \cdot sf[t]$.*

4. *Two 1-cochains f, g are* cohomologous *if there is $a \in A$ such that*

$$g[s] = a^{-1} \cdot f[s] \cdot sa$$

for all $s \in G$. f is called cohomologous to zero *if $f[s] = a^{-1} \cdot sa$, ie. f is cohomologous to the trivial cochain $s \mapsto 1$.*

Proposition B.1.2 *(3) defines an equivalence relation on the set of 1-cocycles.*

PROOF - Since $s1 = s(1 \cdot 1) = s1 \cdot s1$, $s1 = 1$, and so $f[s] = 1^{-1} \cdot f[s] \cdot s1$ for all $s \in G$, ie. f is cohomologous to itself. If $g[s] = a^{-1} \cdot f[s] \cdot sa$ then $f[s] = (a^{-1})^{-1} \cdot g[s] \cdot s(a^{-1})$ so the relation is commutative. If $g[s] = a^{-1} \cdot f[s] \cdot sa$ and $h[s] = a'^{-1} \cdot g[s] \cdot sa'$ then $h[s] = (a \cdot a')^{-1} \cdot f[s] \cdot s(a \cdot a')$ showing transitivity.

□

Definition B.1.3 *The* 1-dimensional cohomology set of G with values in A *is the set of equivalence classes of 1-cocycles, and is written* $H^1(G, A)$.

$H^1(G, A)$ has the structure of a *pointed set* – it is not necessarily a group, but a set with one element singled out, called the unit element. In this case the unit is the class of the trivial cocycle $s \mapsto 1$.

Note that the definitions coincide with the earlier ones if A is abelian, except then $H^1(G, A)$ also has a group law.

$H^0(G, A)$ and $H^1(G, A)$ are functors in A: If $f : A \longrightarrow B$ is a G-homomorphism, ie. $f(sa) = sf(a) \forall s \in G$, then f induces morphisms

$$f^{*0} = f\Big|_{A^G} : H^0(G, A) \longrightarrow H^0(G, B)$$

$$\begin{array}{rccccccc} f^{*1}: & H^1(G, A) & \longrightarrow & H^1(G, B) & & & & \\ & g & \longmapsto & f \circ g : & G & \longrightarrow & B \\ & & & & s & \longmapsto & f(g[s]) \end{array}$$

satisfying $(f \circ f')^* = f^* \circ f'^*$ and $\mathrm{id}_A^* = \mathrm{id}_{H(G,A)}$. The map f^{*0} is a group homomorphism while f^{*1} is a *morphism of pointed sets*, which means a function which maps the unit element to the unit element. By the *kernel* of a morphism of pointed sets is meant the preimage of the unit element. Thus we can talk about an *exact sequence* of pointed sets.

B.2 The Zero-Dimensional Connecting Morphism

Let

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

be a short exact sequence of non-abelian G-modules. Then $\operatorname{im} i = \ker p$ is a normal subgroup of B. Recall the definition of the *connecting homomorphism* $\delta_q : H^q(G, C) \longrightarrow H^{q+1}(G, A)$ in the abelian case; if $K^q(A)$ denotes the cochain complex underlying the cohomology groups, we have the situation

$$\begin{array}{ccccc} & & K^q(B) & \xrightarrow{p} & K^q(C) \\ & & \downarrow d & & \\ K^{q+1}(A) & \xrightarrow{i} & K^{q+1}(B) & & \end{array}$$

and $\delta_q(f) := i^{-1} \circ d \circ p^{-1}(f)$; that is, given a q-dimensional inhomogeneous cocycle $f : G^q \longrightarrow C$, choose a cochain $g : G^q \longrightarrow B$ such that $p(g[s_1, \ldots s_q]) = f[s_1, \ldots s_q]$. Then apply the coboundary map d to g to obtain $dg : G^{q+1} \longrightarrow B$ We show that dg is a $(q+1)$-cocycle taking values in $i(A)$, and that its cohomology class depends only on the class of f in $H^q(C)$.

This construction is adapted to the non-abelian case as follows. In (B.1) assume for simplicity that A is a subgroup of B, so that i is inclusion of sets.

Let $c \in H^0(G, C) = C^G$ and choose $b \in B$ so that $p(b) = c$. Now the coboundary db is defined as

$$\begin{array}{rccc} db: & G & \longrightarrow & B \\ & s & \longmapsto & b^{-1} \cdot sb \end{array}$$

Note that

$$p(b^{-1} \cdot sb) = p(b^{-1}) \cdot p(b) = c^{-1} \cdot sc = c^{-1} \cdot c = 1$$

so that $b^{-1} \cdot sb \in \ker p = \operatorname{im} i = A$ for each $s \in G$. So put

$$\begin{array}{rccc} \delta_0 c: & G & \longrightarrow & A \\ & s & \longmapsto & b^{-1} \cdot sb \end{array}$$

We have to show:

- $\delta_0 c$ is a 1-cocycle:

$$\delta_0 c[st] = b^{-1} \cdot st(b) = b^{-1} \cdot sb \cdot sb^{-1} \cdot st(b) = \delta_0 c[s] \cdot s(\delta_0 c[t])$$

- The cohomology class of $\delta_0 c$ depends only on the cohomology class of c, not on the choice of $b \in p^{-1}(\{c\})$: Choose $b' \in p^{-1}(\{c\})$, then $b'^{-1} \cdot b \in \ker p = \operatorname{im} i = A$ so $b = b'a$ for some $a \in A$. Then $b^{-1} \cdot sb = a^{-1} \cdot b'^{-1} \cdot sb' \cdot sa$ which is cohomologous to $b'^{-1} \cdot sb'$.

So δ_0 gives a well-defined function $H^0(G, C) \longrightarrow H^1(G, A)$. Since $\delta_0 1 = 1$, δ_0 is a morphism of pointed sets. δ_0 is called the connecting morphism in dimension 0.

B.3 The One-Dimensional Connecting Morphism

Now suppose A is in the *centre* $Z(B)$ of B. Then A is particular is an abelian G-module and so we have already defined the 2-dimensional homology group of G with values in A, $H^2(G, A)$.

Remembering the long exact cohomology sequence, we would like a morphism

$$\delta_1 : H^1(G, C) \longrightarrow H^2(G, A)$$

We can define this similarly to δ_0, as follows.

Let $f : G \longrightarrow C$ be a 1-dimensional cocycle with values in C and choose a 1-cochain $g : G \longrightarrow B$ such that $p(g[s]) = f[s]$ for each $s \in G$. Now remembering[1] the 1-dimensional coboundary formula

$$d[s,t] = [s] + s[t] - [st]$$

define

$$\begin{array}{rccc} dg: & G^2 & \longrightarrow & B \\ & [s,t] & \longmapsto & g[s] \cdot sg[t] \cdot g[st]^{-1} \end{array}$$

Then $p(dg[s,t]) = f[s] \cdot sf[t] \cdot f[st]^{-1} = 1$ because f is a 1-cocycle. Thus for each $[s,t]$, $dg[s,t] \in \ker p = \operatorname{im} i = A$. So dg gives a function $G^2 \to A$. There are three checks to be done to complete the definition of δ_1:

Proposition B.3.1 *dg is a 2-cocycle, ie. a factor set. That is,*

$$sdg[t,u] \cdot dg[s,tu] = dg[st,u] \cdot dg[s,t]$$

for all $s,t,u \in G$

Note that dg measures how far the lifting g differs from a 1-cocycle, in that

$$dg[s,t] \cdot g[st] = g[s] \cdot sg[t]$$

The associative law in A shows

$$g[s] \cdot (sg[t] \cdot stg[u]) \quad = \quad (g[s] \cdot sg[t]) \cdot stg[u]$$

ie.

$$g[s] \cdot (sdg[t,u] \cdot sg[tu]) \quad = \quad (dg[s,t] \cdot g[st]) \cdot stg[u]$$

so, remembering $\operatorname{im} dg \subseteq Z(B)$,

$$\begin{aligned} sdg[t,u] \cdot (g[s] \cdot sg[tu]) &= dg[s,t] \cdot (g[st] \cdot stg[u]) \\ sdg[t,u] \cdot dg[s,tu] \cdot g[stu] &= dg[s,t] \cdot dg[st,u] \cdot g[stu] \end{aligned}$$

and cancelling $g[stu]$ gives

$$sdg[t,u] \cdot dg[s,tu] \quad = \quad dg[st,u] \cdot dg[s,t]$$

as required.

Proposition B.3.2 *The cohomology class of dg does not depend of the choice of g given f.*

[1] remembering it and choosing a certain order in which to write its terms down. This order is chosen because it makes the rest of the construction work; not all orderings do.

Choose a cochain $g' : G \longrightarrow B$ with $p \circ g' = f$. Then $p(g'[s]g[s]^{-1}) = 1$ so $g'[s]g[s]^{-1} \in \ker p = \operatorname{im} i = A$ for all $s \in G$ and $g'[s] = g[s] \cdot a[s]$ for some cochain $a : G \longrightarrow A$.

Thus

$$\begin{aligned} dg'[s,t] &= g'[s] \cdot sg'[t] \cdot g'[st]^{-1} \\ &= g[s] \cdot a[s] \cdot sg[t] \cdot sa[t] \cdot a[st]^{-1} \cdot g[st]^{-1} \\ &= a[s] \cdot sa[t] \cdot a[st]^{-1} \cdot dg[s,t] \end{aligned}$$

since A is in the centre of B, which shows that dg' is cohomologous to dg in the abelian group $H^2(G, A)$.

Proposition B.3.3 *dg depends only on the cohomology class of f.*

Let f' be cohomologous to f, so $f'[s] = c^{-1} \cdot f[s] \cdot sc$ for some $c \in C$. Let $g : G \longrightarrow B$ be a lifting of f, then choosing $b \in p^{-1}(\{c\})$ gives a lifting $g'[s] = b^{-1} \cdot g[s] \cdot sb$ of f'.

Then

$$\begin{aligned} dg'[s,t] &= g'[s] \cdot sg'[t] \cdot g'[st]^{-1} \\ &= b^{-1} \cdot g[s] \cdot (sb \cdot sb^{-1}) \cdot sg[t] \cdot (stb \cdot stb^{-1}) \cdot g[st]^{-1} \cdot b \\ &= b^{-1} \cdot dg[s,t] \cdot b \\ &= dg[s,t] \cdot b^{-1} \cdot b \qquad \text{since } \operatorname{im} dg \subseteq A \subseteq Z(B) \\ &= dg[s,t] \end{aligned}$$

□

Thus the function which assigns to the cohomology class of f in $H^1(G, C)$ the cohomology class of dg in $H^2(G, A)$ is well-defined, and will be written δ_1 and called the *1-dimensional connecting morphism.* It is easy to check that it is a morphism of pointed sets.

B.4 The Exact Cohomology Sequence

It is now routine to check the exactness of the following "cohomology sequences".

Proposition B.4.1 *Let*

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

be an exact sequence of non-abelian G-modules. Then the sequence of pointed sets

$$\begin{aligned} 1 \to H^0(G,A) &\xrightarrow{i^*} H^0(G,B) \xrightarrow{p^*} H^0(G,C) \\ &\xrightarrow{\delta_0} H^1(G,A) \xrightarrow{i^*} H^1(G,B) \xrightarrow{p^*} H^1(G,C) \end{aligned}$$

is exact. If in addition $i(A)$ is in the centre of B, the sequence of pointed sets

$$\begin{array}{c} 1 \to H^0(G,A) \xrightarrow{i^*} H^0(G,B) \xrightarrow{p^*} H^0(G,C) \\ \xrightarrow{\delta_0} H^1(G,A) \xrightarrow{i^*} H^1(G,B) \xrightarrow{p^*} H^1(G,C) \xrightarrow{\delta_1} H^2(G,A) \end{array}$$

is exact.

PROOF - There are six places of exactness to check. Again we assume A is a subgroup of B, and i is inclusion, for simplicity of writing.

1. $H^0(G,A)$: $A^G \overset{i^*}{\hookrightarrow} B^G$.

2. $H^0(G,B)$: $\operatorname{im} i^* \subseteq \ker p^*$ because $p \circ i = 0$ so $p^* \circ i^* = 0$. $\ker p^* \subseteq \operatorname{im} i^*$: if $b \in \ker p^* \subseteq B^G$ then $b \in \ker p = \operatorname{im} i = A$ and $sb = b$ so $b \in B^G \cap A = A^G = \operatorname{im} i^*$.

3. $H^0(G,C)$: $\operatorname{im} p^* \subseteq \ker \delta_0$: If $c = p(b)$ then $\delta_0 c = db$ which is cohomologous to zero. $\ker \delta_0 \subseteq \operatorname{im} p^*$: if $c \in H^0(G,C) = C^G$ is in $\ker \delta_0$ then there is a lifting $b \in B$ of c such that db is cohomologous to zero in $H^1(G,A)$, ie. there is $a \in A$ with $b^{-1} \cdot sb = a^{-1} \cdot sa$ f or all $s \in G$. Then $b \cdot a^{-1} = s(b \cdot a^{-1})$ so $b \cdot a^{-1} \in A^G \subseteq B^G$. But $p(b \cdot a^{-1}) = c \cdot 1 = c$ so $c \in \operatorname{im} p^* : B^G \longrightarrow C^G$.

4. $H^1(G,A)$: $\operatorname{im} \delta_0 \subseteq \ker i^*$: Let $b \in p^{-1}(\{c\})$, then

$$\begin{array}{ccccc} G & \overset{\delta_0 c = db}{\longrightarrow} & A & \overset{i}{\longrightarrow} & B \\ s & \longmapsto & b^{-1} \cdot sb & \longmapsto & b^{-1} \cdot sb \end{array}$$

   is cohomologous to zero in $H^1(G,B)$. $\ker i^* \subseteq \operatorname{im} \delta_0$: if $f \in \ker i^*$ then there is $b \in B$ such that $f[s] = b^{-1} \cdot sb$ for all $s \in G$. So $f = db$ and so $f \in \operatorname{im} \delta_0$

5. $H^1(G,B)$: $\operatorname{im} i^* \subseteq \ker p^*$ because $p \circ i = 0$ so $p^* \circ i^* = 0$. $\ker p^* \subseteq \operatorname{im} i^*$: if $f \in \ker p^*$ then $p(f[s]) = c^{-1} \cdot sc$ for some $c \in C$ and all $s \in G$. Choose $b \in p^{-1}(\{c\})$, then $p(b \cdot f[s] \cdot sb^{-1}) = 1$ for all s, so $b \cdot f[s] \cdot sb^{-1} = a[s]$ for some cochain $a : G \longrightarrow A$.

$$\begin{aligned} a[st] &= b \cdot f[s] \cdot (sb^{-1} \cdot sb) \cdot sf[t] \cdot stb^{-1} \\ &= a[s] \cdot sa[t] \end{aligned}$$

   so a is a 1-cocycle and so $f[s] = b^{-1} \cdot a[s] \cdot s[b]$ is cohomologous to $a \in \operatorname{im} i^*$.

6. $H^1(G,C)$, assuming $A \subseteq Z(B)$. $\operatorname{im} p^* \subseteq \ker \delta_1$: if $f[s] = p(g[s])$ for a 1-cocycle $g : G \longrightarrow B$ then $\delta_1 f = dg$ which is cohomologous to zero in $H^2(G,A)$. $\ker \delta_1 \subseteq \operatorname{im} p^*$: Let $f \in \ker \delta_1, f : G \longrightarrow C$. So there is a lifting $g : G \longrightarrow B$ such that $dg[s,t] = a[s] \cdot sa[t] \cdot a[st]^{-1}$ for some cochain $a : G \longrightarrow A$, ie.

$$g[s] \cdot sg[t] \cdot g[st]^{-1} = a[s] \cdot sa[t] \cdot a[st]^{-1}$$

Which rearranges, because A is in the centre of B, to give

$$(a[s]^{-1} \cdot g[s]) \cdot s(a[t]^{-1} \cdot g[t]) \quad = \quad a[st]^{-1} \cdot g[st]$$

so that $g'[s] := a[s]^{-1} \cdot g[s] : G \longrightarrow B$ is a 1-cocycle with $p^*g' = p^*(a^{-1} \cdot g) = p^*g = f$, and so $f \in \operatorname{im} p^*$.

$\square$

Appendix C

Galois Theory

In this section I list the ideas and results of Galois Theory needed for the discussion of Galois Cohomology in Chapter 2. Most of the results are fundamental and are stated without proof; for more details, see any introductory text on Galois Theory, for example Stewart, [8]. Two particularly relevant results (the Normal Basis Theorem, linear independence of automorphisms) are proved here.

C.1 Basic Results

If L is a field and K a subfield of L, then L is called an *extension* of K. In this situation we write L/K to denote the pair (L, K). The group of K-automorphisms of L, ie. field automorphisms of L which leave every element of K fixed, under composition of functions, is called the *Galois Group* of L over K, written in this text as $\mathrm{Gal}(L/K)$. Elsewhere it is variously written as $G(L/K)$, $G_{L/K}$, $\Gamma(L/K)$, $\Gamma_{L/K}$ or $\mathrm{Aut}_K(L)$.

Definition C.1.1 *L/K is called a* normal *extension if every polynomial in $K[X]$ with one root in L factorises into linear factors in L.*

Proposition C.1.2 *L/K is a normal extension if and only if it has the following property: every K-homomorphism from L into an extension M of L has its image contained in L.*

Definition C.1.3 *L/K is called a* separable *extension if, for every $\lambda \in L$, the polynomial of least degree in $K[X]$ having λ as a root is not divisible by $(X-\lambda)^2$ in $\bar{K}[X]$. If L/K is not separable it is called* inseparable.

Some fields do not have any inseparable extensions; such fields are called *perfect*.

Proposition C.1.4 *A field K is perfect if and only if one of the following conditions holds.*

1. *K has characteristic zero*

2. K has characteristic $p > 0$, and the field homomorphism

$$\begin{array}{ccc} K & \longrightarrow & K \\ a & \longmapsto & a^p \end{array}$$

is bijective; ie. every element has a unique p^{th} root.

If L/K is a field extension, then L is naturally a K-vector space. Write $[L : K] := \dim_K L$. If $[L : K]$ is finite, L/K is called a *finite extension*.

Definition C.1.5 *L/K is called a* Galois Extension *if the fixed field of its Galois group (ie. $\{a \in L : \sigma a = a \, \forall \sigma \in \mathrm{Gal}(L/K)\}$) is equal to K.*

Proposition C.1.6 *A finite extension is a Galois extension if and only if it is normal and separable.*

The next proposition makes no assumptions of finiteness. In the finite case it forms a component of the usual Fundamental Theorem of Galois Theory.

Proposition C.1.7 *If L/K is any extension and $L \supseteq E \subseteq K$ such that E/K is normal, then $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$.*

PROOF - If $s \in \mathrm{Gal}(L/K)$ then normality of E/K implies $sE = E$. Let $t \in \mathrm{Gal}(L/E)$ and $x \in E$. Then $(s^{-1}ts)x = s^{-1}t(sx) = s^{-1}(sx)$ since $sx \in E$, and this is again x. So $s^{-1}ts \in \mathrm{Gal}(L/E)$, as required.

$\square$

Theorem C.1.8 (Fundamental Theorem of Galois Theory) *Let L/K be a finite Galois extension with group $G = \mathrm{Gal}(L/K)$. Then $\mathrm{Card}(G) = [L : K]$. Let $\mathcal{C}$ be the set of subgroups of G and $\mathcal{F}$ the set of subextensions M (ie. $L \supseteq M \supseteq K$). The map*

$$\begin{array}{ccc} \mathcal{F} & \longrightarrow & \mathcal{C} \\ M & \longmapsto & \mathrm{Gal}(L/M) \end{array}$$

is bijective. Then inverse is given by taking a subgroup H of G to its fixed field inside L. M/K is a normal extension if and only if $\mathrm{Gal}(L/M)$ is a normal subgroup of G, in which case $\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$.

One stage in the proof of this is the following lemma of Dedekind.

Lemma C.1.9 (Linear Independence of Monomorphisms) *Let L and M be fields. Then any set of distinct injective homomorphisms ("monomorphisms") $L \longrightarrow M$ is linearly independent over M.*

PROOF - Let $\{\psi_i\}_{i \in I}$ be a set of distinct monomorphisms and suppose

$$a_1\psi_1 + \ldots + a_n\psi_n = 0 \qquad a_i \in M \tag{C.1}$$

is an equation of linear dependence between some of the ψ_i, with all $a_i \neq 0$ and n smallest possible. Then $n > 1$ because each ψ_i is a monomorphism.

Now let $y \in L$ be such that $\psi_1(y) \neq \psi_n(y)$. Evaluate (C.1) at yx to get

$$a_1\psi_1(y)\psi_1(x) + \ldots + a_n\psi_n(y)\psi_n(x) = 0$$

for all $x \in L$. Now multiply (C.1) by $\psi_n(y)$ and evaluate at x:

$$a_1\psi_n(y)\psi_1(x) + \ldots + a_n\psi_n(y)\psi_n(x) = 0$$

for all $x \in L$. Subtracting these equations gives a nonzero relation of linear dependence with less nonzero terms than (C.1), a contradiction.

□

The Galois theory of finite fields is particularly simple. If L/K is a finite extension of finite fields, let p be the characteristic of K (and hence also of L). Then elementary linear algebra shows that K has $q = p^m$ elements and L has q^n elements, where $m = [K : \mathbb{F}_p]$ is the degree of K over the base field $\mathbb{F}_p = \mathbb{Z}/p$ and $n = [L : K]$. L/K is always a Galois extension - K is perfect, so that L/K is separable, and one can show that L is a splitting field for the polynomial $X^{q^n} - X$ over K, so that it is normal.

In fact, there is a unique field of cardinality p^m for each prime p and positive integer m.

The map $\sigma : L \longrightarrow L$ which maps $x \in L$ to x^q is a K-automorphism of L, called the *Frobenius automorphism.* In fact, any K-automorphism of L is a power of the Frobenius. Thus $\mathrm{Gal}(L/K)$ is cyclic of order n.

C.2 The Normal Basis Theorem

It is Theorem C.2.6. This proof is taken from David J. Winter, *The Structure of Fields* (Springer), page 51.

Lemma C.2.1 *Let L/K be a cyclic extension. Then L has a K-basis of the form $\{\sigma(y) : \sigma \in G = \mathrm{Gal}(L/K)\}$ for some $y \in L$.*

PROOF - Dedekind's lemma shows that

$$e, \tau, \tau^2, \ldots, \tau^{n-1}$$

are L-linearly independent. Hence the minimum polynomial for $\tau \in \mathrm{End}_K(L)$ is $X^n - 1$. If we make L into a $K[X]$-module via τ in the usual way ($f(X)\lambda := f(\tau)(\lambda)$), then the structure theorem for modules over principle ideal domains shows that L decomposes as a direct sum of cyclic $K[X]$-modules, one of which is then $K[X]/(X^n - 1)$. Counting K-dimension shows this is the only one, so that L is a cyclic $K[G]$-module, which is what we wanted to show.

□

Corollary C.2.2 *if L/K is a finite extension of a finite field then L has a normal K-basis.*

PROOF - in this case L/K is a Galois extension and $\mathrm{Gal}(L/K)$ is cyclic.

□

That disposes of the case L finite.

Theorem C.2.3 *Let K be an infinite field, let L_1 and L_2 be two extensions of K and let $\sigma_1, \ldots, \sigma_n$ be distinct elements of $\mathrm{Hom}_K(L_1, L_2)$. Then there is $a \in L_1$ such that $\sigma_1(a), \ldots, \sigma_n(a)$ are pairwise distinct.*

PROOF - Choose some elements $a_0, \ldots, a_m \in L_1$ such that

$$(\sigma_i a_0, \sigma_i a_1, \ldots, \sigma_i a_m) = (\sigma_j a_0, \sigma_j a_1, \ldots, \sigma_j a_m) \iff i = j$$

Let $h(X) = \sum_{r=0}^{m} a_r X^r$ and note that

$$\sigma_i(h(X)) = \sigma_j(h(X)) \text{ in } L_2[X] \iff i = j$$

Thus

$$\prod_{i \neq j} \big((\sigma_i h)(X) - (\sigma_j h)(X)\big)$$

is a nonzero polynomial in $L_2[X]$. Since K is infinite, there is $t \in L$ such that

$$\prod_{i \neq j} \big((\sigma_i h)(t) - (\sigma_j h)(t)\big) \neq 0$$

Put $a = h(t)$, then $\sigma_1(a), \ldots, \sigma_n(a)$ are distinct.

□

Proposition C.2.4 *Let L/K be a finite extension with Galois group $G = \{1 = \sigma_1, \ldots, \sigma_n\}$. Assume K is infinite. Then there is $y \in L$ such that $\det(\sigma_i^{-1}\sigma_j(y)) \neq 0$.*

PROOF - By the theorem, we can choose $z \in L$ such that $\sigma_1(z), \ldots, \sigma_n(z)$ are distinct. Define a polynomial $f \in L[X]$ such that $f(z) = 1, f(\sigma_i(z)) = 0$ for $i \neq 1$, by

$$f(X) = \prod_{i \neq 1} \frac{X - \sigma_i(z)}{z - \sigma_i(z)}$$

Then $f(\sigma_j^{-1}\sigma_i(z)) = \delta_{ij}$ (Kronecker delta). Apply $\sigma_i^{-1}\sigma_j$ to this equation:

$$\big(\sigma_j^{-1}\sigma_i(f)\big)(z) = \delta_{ij}$$

where $\left(\sigma_j^{-1}\sigma_i(f)\right)$ means the polynomial obtained from f by applying $\sigma_j^{-1}\sigma_i(f)$ to each coefficient. Hence

$$\det\left(\left(\sigma_j^{-1}\sigma_i(f)\right)(z)\right)_{i,j} = 1$$

so the polynomial in $L[X]$

$$\det\left(\left(\sigma_j^{-1}\sigma_i(f)\right)(X)\right)_{i,j}$$

is not identically zero. Now because K is infinite, there is $x \in K$ such that the value of this polynomial at x is not zero. But because x is fixed by G, this means that

$$\det\left(\sigma_j^{-1}\sigma_i(f(x))\right)_{i,j} \neq 0.$$

Setting $y = f(x)$ gives the desired result.

□

Corollary C.2.5 *Let L/K be as in the proposition, and assume furthermore that it is a Galois extension. Then there is $y \in L$ such that $\sigma_1(y), \ldots, \sigma_n(y)$ are K-linearly independent (and hence a K-basis for L).*

PROOF - Take y as given by the proposition. If a K-linear dependence of $\sigma_1(y), \ldots, \sigma_n(y)$ existed, it would give a K-linear dependence of the columns of the $n \times n$ matrix $(\sigma_i^{-1}\sigma_j(y))_{i,j}$.

□

Theorem C.2.6 (Normal Basis Theorem) *Let L/K be a finite Galois extension with group G. Then there exists $y \in L$ such that $\{\sigma(y) : \sigma \in G\}$ is a K-basis for L, ie. L is a cyclic $K[G]$-module.*

PROOF - This is corollaries C.2.5 and C.2.2

□

Appendix D

Topological Groups

The purpose of this appendix is to outline the basic ideas of topological groups needed in Chapter 2. The reader is assumed to have knowledge of the ideas of topologies, open and closed sets, compactness, induced topology on subspaces, the discrete topology and complete metric spaces. Our reference for these ideas is M. A. Armstrong, *Basic Topology* (Springer). For the properties of topological groups we refer to [6].

A *topological group* G is a group and a Hausdorff topological space, and these two structures must be compatible in that the multiplication and inversion maps

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & xy \end{array} \qquad \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array}$$

are continuous.

The topology on a group is essentially the same at each point, because a set $X \subseteq G$ is open if and only if its translation sX is open for each $s \in G$. Therefore we may restrict our attention to the neighbourhoods of the identity element e. We will study topological groups via the following definition:

Definition D.0.7 *A set S of subsets of a group G is said to form a* fundamental system of open neighbourhoods of the identity *if the following conditions hold.*

1. $\bigcap S = \{e\}$*;*
2. *S is closed under finite intersection, ie. if $U, V \in S$ then $U \cap V \in S$;*
3. *For $U \in S$, there is $V \in S$ with $VV^{-1} \subseteq U$;*
4. *If $U \in S$ and $a \in U$ there is $V \in S$ with $Va \subseteq U$;*
5. *If $U \in S$ and $a \in G$ then there is $V \in S$ with $aVa^{-1} \subseteq U$.*

For such an S we have the result

Theorem D.0.8 *The set S defines a topology on G consisting of unions of sets of the form $\{Va : V \in S, a \in G\}$ making G into a topological group.*

For the proof see [6], page 26.

We will also need to use the topology on a product of topological groups. Let $\{G^i\}_{i \in I}$ be a possibly infinite collection of topological groups. Then the Cartesian product $\prod G^i$ is a group. The product topology on $\prod G^i$ is by definition the smallest[1] topology on the set such that for each $j \in I$, the projection on the j-th component map

$$\pi_j : \prod G^i \longrightarrow G^j$$

is continuous. The open sets are then of the form

$$\{(x_i) : x^j \in U_j \text{ for } j \in J, x_i \in G^i \text{ for } i \in I - J\}$$

for some finite subset $J \subseteq I$ and open sets $U_j \subseteq G^j$ chosen for each $j \in J$. Now in the case where we will use this, each G^i will be a *finite* group, with the *discrete* topology. In this case the open sets in the product can be built up in a very natural way from the sets

$$\ker \pi_j = \prod_{i \neq j} G^i \times \{e\} = \{(x_i) : x_j = e\}$$

by taking a finite intersection of them, translating by an element of $\prod G^i$, and then taking a union of such sets.

We will also need:

Theorem D.0.9 (Tychonoff's Theorem) *The product of a collection of compact topological spaces is compact.*

The proof, which relies on the Axiom of Choice, can be found in [6]

[1] "smallest topology" with a certain property means that it is a subset of every other topology with this property.

Appendix E

Central Simple Algebras

Let K be a field. We discuss here K-algebras, simple rings and their structures.

Definition E.0.10 *A K-*algebra *A is a ring which is also a K-vector space, and whose ring-multiplication is K-bilinear in the sense that*

$$(\kappa a) \cdot b = a \cdot (\kappa b) = \kappa(a \cdot b)$$

for all $a, b \in A, \kappa \in K$.

There is a natural inclusion

$$\begin{array}{ccc} K & \hookrightarrow & A \\ \kappa & \mapsto & \kappa 1_A \end{array}$$

so that K may be regarded as a subfield of the ring A. Since $(\kappa 1) \cdot a = \kappa(1 \cdot a) = \kappa(a \cdot 1) = a \cdot (\kappa 1)$, K is then in the *centre* $Z(A)$ of A, the set of all the elements of A which commute with all the other elements of A. Conversely, a ring containing K in its centre is necessarily a K-algebra.

A morphism of K-algebras is simply a K-linear ring homomorphism.

The K-algebras that we can study with the Brauer group have to satisfy three conditions, which will now be described.

A K-algebra A is called *finite-dimensional* if it is finite-dimensional as a K-vector space. It is called *central* if its centre is K.

We will study K-algebras which satisfy these two conditions, and are also *simple* rings.

E.1 Simple Rings

Definition E.1.1 *Let R be a ring.*

1. *A left-R-module is called* simple *if it has no R-submodules other than itself and 0.*

2. *A left-R-module is called* semisimple *if it decomposes as a direct sum of simple submodules.*

3. *R is called* semisimple *if it is semisimple as a left-R-module.*

4. *a left-ideal of R is called* simple *if it is simple as a left-R-module*

5. *R is called* simple *if it is semisimple and all its simple left-ideals are isomorphic as R-modules.*

Proposition E.1.2 *A simple ring has no proper nonzero double-sided ideals.*

PROOF - Write $R = \sum_{i\in I} \mathfrak{a}_i$ where $\mathfrak{a}_i$ are simple left-R-modules, and let $\mathfrak{b}$ be a proper nonzero double-sided ideal of R.

So $\mathfrak{b} = \mathfrak{b}R$ (because $1 \in R$) $= \sum_{i\in I} \mathfrak{b}\mathfrak{a}_i$, so $\mathfrak{b}\mathfrak{a}_i \neq 0$ for some $i \in I$, say $\mathfrak{b}\mathfrak{a}_1 \neq 0$. Thus $\mathfrak{b}\mathfrak{a}_1 = \mathfrak{a}_1$, being a nonzero submodule of $\mathfrak{a}_1$.

R being simple, there are R-module isomorphisms $\sigma_i : \mathfrak{a}_1 \to \mathfrak{a}_i$. So $\mathfrak{a}_i = \sigma_i(\mathfrak{a}_1) = \sigma_i(\mathfrak{b}\mathfrak{a}_1) = \mathfrak{b}\sigma_i(\mathfrak{a}_1) = \mathfrak{b}\mathfrak{a}_i$. Thus

$$\mathfrak{b} = \sum_{i\in I} \mathfrak{b}\mathfrak{a}_i = \sum_{i\in I} \mathfrak{a}_i = R$$

□

There is a converse of this result, using the following lemma:

Lemma E.1.3 *Let R be a ring, $\mathfrak{a}$ a simple left-ideal of R and M a simple left-R-module. If $\mathfrak{a} \not\cong M$ then $\mathfrak{a}M = 0$.*

PROOF - Suppose $\mathfrak{a}M \neq 0$, so there are $a \in \mathfrak{a}, m \in M$ with $am \neq 0$. Define

$$\begin{array}{rccc} \phi : & \mathfrak{a} & \longrightarrow & M \\ & x & \longmapsto & xm \end{array}$$

for this m. Then ϕ is an R-module homomorphism. $\operatorname{im}\phi$ is an R-submodule of M and is not 0, so it is all of M. $\ker\phi$ is an R-submodule of $\mathfrak{a}$ which is not all of $\mathfrak{a}$, so $\ker\phi = 0$. Hence ϕ is an isomorphism. So $\mathfrak{a}M \neq 0 \Rightarrow \mathfrak{a} \cong M$, as required.

□

Proposition E.1.4 *If R is a semisimple ring with no proper nonzero double-sided ideals then R is simple.*

PROOF - Suppose R is not simple, then either R is not semisimple or $R = \bigoplus_{i\in I} \mathfrak{a}_i$, a direct sum of simple left-ideals. Let $I' := \{i \in I : \mathfrak{a}_i \cong \mathfrak{a}_1\}$, a proper subset of I, and $\mathfrak{b} := \sum_{i\in I'} \mathfrak{a}_i$, which is a nonzero left-ideal of R because R is not simple. If we had $\mathfrak{b} = R$ then for any simple left ideal $\mathfrak{a}$ of R, $\mathfrak{a} \cap \mathfrak{a}_i$ would be nonzero for some $i \in I'$, giving $\mathfrak{a} = \mathfrak{a}_i$ because $\mathfrak{a} \cap \mathfrak{a}_i$ is a nonzero submodule of each, and contradicting $I \neq I'$.

So $\mathfrak{b}$ is a proper nonzero left-ideal of R. Now

$$\mathfrak{b}R = (\sum_{i \in I'} \mathfrak{a}_i)(\sum_{j \in I} \mathfrak{a}_j) = \sum_{i \in I'} \mathfrak{a}_i(\sum_{j \in I'} \mathfrak{a}_j + \sum_{j \in I - I'} \mathfrak{a}_j) = \mathfrak{b}^2 + 0 = \mathfrak{b}^2 \subseteq \mathfrak{b}$$

so $\mathfrak{b}$ is a proper nonzero double-sided ideal of R.

□

Proposition E.1.5 *If a Noetherian ring R has a simple left-ideal, and R has no proper nonzero double-sided ideals, then R is simple.*

PROOF - Consider the set of direct sums of simple left-ideals of R ordered by containment ($\mathfrak{a} \leq \mathfrak{b} \iff \mathfrak{a} \subseteq \mathfrak{b}$). By the ascending chain condition, this set has a maximal element, ie. a direct sum $\mathfrak{b} = \bigoplus_{i \in I} \mathfrak{a}_i$ which is not contained properly in any other such direct sum. (*a priori* the set I may be empty, in which case $\mathfrak{b} = 0$).

Now for any $j \in I$, $\mathfrak{a}_j t$ is either simple or zero. This is because the map

$$\begin{array}{ccc} \mathfrak{a}_j & \longrightarrow & \mathfrak{a}_j t \\ m & \longmapsto & mt \end{array}$$

is clearly a surjective R-module homomorphism, and its kernel, being an R-submodule of $\mathfrak{a}_j$, is either all of $\mathfrak{a}_j$ or 0. Therefore it is either an isomorphism or the zero map, and so $\mathfrak{a}_j t$ is either simple or zero.

If $\mathfrak{a}_j t = 0$ for given j and t, then $\mathfrak{a}_j t \subseteq \mathfrak{b}$. If on the other hand $\mathfrak{a}_j t \neq 0$, the sum

$$\sum_{i \in I} \mathfrak{a}_i + \mathfrak{a}_j t$$

is not direct, so $\mathfrak{a}_j t \cap \mathfrak{a}_i \neq 0$ for some $i \in I$. But then $\mathfrak{a}_j t = \mathfrak{a}_j t \cap \mathfrak{a}_i = \mathfrak{a}_i$, the intersection being a nonzero submodule of both of the simple modules.

This shows $\mathfrak{b}t \subseteq \mathfrak{b}$ for all $t \in R$, so $\mathfrak{b}$ is a double-sided ideal of R. Since R has a simple left-ideal, $\mathfrak{b} \neq 0$, so $\mathfrak{b} = R$ and $R = \bigoplus_{i \in I} \mathfrak{a}_i$ is semisimple.

Now the previous proposition shows R is simple.

□

Proposition E.1.6 *A finite-dimensional K-algebra A is a simple ring if and only if it has no proper nonzero double-sided ideals.*

PROOF - "$\Rightarrow$" was shown above.

"$\Leftarrow$": Because A is a finite-dimensional K-vector space, and a left-ideal of A a vector subspace, A must satisfy both the ascending and descending chain conditions on left-ideals, ie. A is both Noetherian and Artinian. This is because an ascending or descending sequence of ideals gives a monotonic and bounded sequence of integers under the map $\dim_K$. Such a sequence must be constant and so linear algebra shows the original sequence of ideals is constant (ie. $V \subseteq W \text{and} \dim_K V = \dim_K W \Rightarrow V = W$).

By the descending chain condition it is possible to choose a nonzero left-ideal of A which is minimal in the set of all such, ie. which has no proper nonzero submodules, ie. is simple.

Thus A is a Noetherian ring with a simple left-ideal and no proper nonzero double-sided ideals, so by proposition E.1.5, A is simple.

$\square$

It can be shown[1] that if A is a simple algebra like this, so $A = \bigoplus_{i=1}^{n} \mathfrak{a}$, then all finite-dimensional left-A-modules are also A-module-isomorphic to a direct sum $\bigoplus_{i=1}^{N} \mathfrak{a}$; in particular, all simple left-A-modules are isomorphic.

Definition E.1.7 *A finite-dimensional K-algebra is called* central simple *if it is simple and has centre K.*

These algebras will be described by the elements of the Brauer Group. There is a general structure theorem for simple rings which will be necessary, and which is described next.

E.2 Structure of Simple Algebras

[This part follows Weil, "Basic Number Theory", Chapter IX, §1]

We will be interested in comparing our central simple algebras to matrix algebras.

Definition E.2.1 *If R is a ring, write*

$$\begin{array}{rccc} \mu: & R \times R & \longrightarrow & R \\ & (x,y) & \longmapsto & x \cdot y \end{array}$$

for the multiplication table of R. Then the additive group $(R,+)$ combined with the multiplication

$$\begin{array}{rccc} \mu^\circ: & R \times R & \longrightarrow & R \\ & (x,y) & \longmapsto & \mu(y,x) \end{array}$$

is a ring, called the opposite ring *or* inverse ring *of R and written R°.*

Theorem E.2.2 (Wedderburn's Theorem) *If R is a simple ring then R is isomorphic to a matrix ring $M_n(D)$ where D is a division ring.*

[1] Weil, *Basic Number Theory*, ch. 9, §1, Prop. 1

PROOF - Let $\mathfrak{a}$ be a simple left-ideal of R and put $D := \mathrm{End}_R(\mathfrak{a})$, the ring of R-endomorphisms of the R-module $\mathfrak{a}$ under pointwise addition, and composition of endomorphisms. If $\delta \in D$ then $\ker\delta$ and $\operatorname{im}\delta$ are R-submodules of $\mathfrak{a}$; if $\ker\delta \neq 0$ then $\ker\delta = \mathfrak{a}$ so that $\delta = 0$; otherwise $\operatorname{im}\delta \neq 0$ so $\operatorname{im}\delta = \mathfrak{a}$, so that δ is an R-automorphism of $\mathfrak{a}$ and so is invertible in D.

Thus every nonzero element of D is invertible, so D is a division ring.

Now consider $\mathrm{End}_R(R)$; if $\psi \in \mathrm{End}_R(R)$ then $\psi(x) = x\psi(1)\ \forall x \in R$ so that ψ is a right-homothety. Define the homothety map

$$\begin{array}{rcccccc} h: & R & \longrightarrow & \mathrm{End}_R(R) & & & \\ & x & \longmapsto & h(x): & R & \longrightarrow & R \\ & & & & y & \longmapsto & yx \end{array}$$

h satisfies $h(x + x') = h(x) + h(x')$ and $h(xx') = h(x')h(x)$ so that h is a ring anti-homomorphism. h is surjective by the comment above, and, since $h(x)(1) = x$, injective. Thus h is a ring anti-isomorphism.

But $\mathrm{End}_R(R) = \mathrm{End}_R(\bigoplus_{i=1}^n \mathfrak{a}) \cong M_n(End_R(\mathfrak{a}))$ as follows.

If $\psi \in \mathrm{End}_R(\bigoplus_{i=1}^n \mathfrak{a})$ then, writing $\mathfrak{a}_i$ for the i-th summand,

$$\pi_i \circ \psi\Big|_{\mathfrak{a}_j} : \mathfrak{a}_j \longrightarrow \bigoplus_{i=1}^n \mathfrak{a} \xrightarrow{\pi_i} \mathfrak{a}_i$$

is an R-endomorphism of $\mathfrak{a}$, ie. an element of D. Putting

$$\begin{array}{rccc} \mu: & \mathrm{End}_R(R) & \longrightarrow & M_n(D) \\ & \psi & \longmapsto & \left(\pi_i \circ \psi\Big|_{\mathfrak{a}_j}\right)_{i,j} \end{array}$$

we have

$$\begin{aligned} \mu(\psi \circ \phi) &= \left(\pi_i \circ (\psi \circ \phi)\Big|_{\mathfrak{a}_j}\right)_{i,j} \\ &= \left(\pi_i \circ \Big(\sum_k (\psi\Big|_{\mathfrak{a}_k} \circ \pi_k) \circ \phi\Big|_{\mathfrak{a}_j}\right)_{i,j} \\ &= \Big(\sum_k (\pi_i \circ \psi\Big|_{\mathfrak{a}_k}) \circ (\pi_k \circ \phi\Big|_{\mathfrak{a}_j})\Big)_{i,j} \\ &= \left(\pi_i \circ \psi\Big|_{\mathfrak{a}_j}\right)_{i,j} \left(\pi_i \circ \phi\Big|_{\mathfrak{a}_j}\right)_{i,j} = \mu(\psi)\mu(\phi) \end{aligned}$$

and it is easy to check that μ is additive and bijective, so that μ is an isomorphism of rings. Thus R is anti-isomorphic to $M_n(D)$.

Define

$$\begin{array}{rccc} \tau: & M_n(D) & \longrightarrow & M_n(D^\circ) \\ & (d_{ij})_{i,j} & \longmapsto & (d_{ji})_{i,j} \end{array}$$

so that τ is given by transposition of matrices. τ is clearly an isomorphism of additive groups, and (writing all products in the ring D),

$$\tau\big((d_{ij})_{i,j}(d'_{ij})_{i,j}\big) = \tau\big((\sum_k d_{ik}d'_{kj})_{i,j}\big) = (\sum_k d_{jk}d'_{ki})_{i,j}$$

while

$$\tau\big((d'_{ij})_{i,j}\big)\tau\big((d_{ij})_{i,j}\big) = (d'_{ji})_{i,j}(d_{ji})_{i,j} = (\sum_k d_{jk}d'_{ki})_{i,j}$$

so that τ is an anti-isomorphism of rings. Then $\tau \circ \mu \circ h : R \longrightarrow M_n(D^\circ)$ is an isomorphism of rings. Since D° is a division ring, the theorem is proved.

□

Remark - one may avoid the use of anti-homomorphisms by considering $\mathrm{End}_R(R)$ as operating on the right, so that $(x)\phi \circ \psi = ((x)\phi)\psi$ is the product $\phi \circ \psi \in \mathrm{End}_R(R)$. The effect of this is to replace $\mathrm{End}_R(R)$ by its opposite ring, to which it is anti-isomorphic.

If A is a central simple K-algebra, then $D = \mathrm{End}_A(\mathfrak{a})$ is also a central-simple algebra over K, and the isomorphism given by Wedderburn's Theorem is an isomorphism of K-algebras (it is easy to check that each of h, μ, τ is K-linear). Let us check the assertions about D:

- Finite-dimensional: $\mathrm{End}_A(\mathfrak{a}) \subseteq \mathrm{End}_K(\mathfrak{a}) \cong M_m(K)$.
- Central: since $A \cong M_n(D)$ as K-algebras, $K \subseteq Z(M_n(D)) \cong Z(A) = K$ which is a 1-dimensional K-vector space over $K \subseteq A$, so $Z(D) = K$.
- Simple: D is simple just like a field is simple - any nonzero ideal contains an invertible element, and so is all of D.

Proposition E.2.3 *A determines n uniquely, and D up to isomorphism.*

PROOF - It is sufficient to show that the K-algebra $M_n(D)$ determines D up to isomorphism. For then if $A \cong M_n(D) \cong M_{n'}(D')$ we have $D \cong D'$ and, considering the dimension of the free modules $M_n(D)$ and $M_{n'}(D')$ over the principal ideal domain D, $n^2 = n'^2$ so n is also uniquely determined.

Let $E_{kl} := (\delta_{ik}\delta_{jl})_{i,j}$ be the standard D-basis for $M_n(D)$, where δ denotes the Kronecker δ-symbol. Then

$$M := M_n(D)E_{11}$$

is the left-$M_n(D)$-submodule of matrices with 0 outside the first column. If $X = (x_{ij})_{i,j} \in M$ is nonzero then $x_{k1} \neq 0$ for some k and $x_{ij} = 0$ for $j > 1$. So

$$x_{k1}^{-1}E_{mk}X = x_{k1}^{-1}(\sum_p \delta_{im}\delta pk x_{pj})_{i,j} = x_{k1}^{-1}(\delta_{im}x_{kj})_{i,j} = E_{m1} \in M$$

So $M_n(D)X = M$, ie. M is a simple-left-$M_n(D)$-module.

Now consider $\mathrm{End}_{M_n(D)}(M)$. If $f \in End_{M_n(D)}(M)$ then put

$$X = (x_{ij})_{i,j} := f(E_{11})$$

X has zeros outside the first column because $X \in M$; in fact $M_n(D)$-linearity implies that X also has zeros outside the first row, for

$$\begin{aligned} 0 = f(0) = f(E_{1k}E_{11}) \qquad (\text{for} k \neq 1) \\ = E_{1k}f(E_{11}) = (\textstyle\sum_p \delta_{i1}\delta_{jk}x_{pj})_{i,j} = (\delta_{i1}x_{kj})_{i,j} \end{aligned}$$

Considering the $(1,1)$-th element of this matrix gives $x_{k1} = 0$ for $k > 1$. So $X = (\delta_{1i}\delta_{1j}d)$ for some $d \in D$, and $f((y_{ij})_{i,j}) = (y_{ij}d)_{i,j}$. $f \longmapsto d$ defines a K-linear anti-isomorphism $\mathrm{End}_{M_n(D)} \longrightarrow D$, and so shows that $M_n(D)$ determines D up to isomorphism.

□

Proposition E.2.4 *If K is algebraically closed and A is a central simple K-algebra then*

$$A \cong M_n(K)$$

as K-algebras for some n.

PROOF - Wedderburn's Theorem shows that $A \cong M_n(D)$ for a finite-dimensional division algebra over K. But K admits no such algebras other than itself. For if $D \neq K$ is such an algebra, let $d \in D - K$, then $K(d)$ is an algebraic extension of K, other than K, which is impossible. So in fact,

$$A \cong M_n(K)$$

E.3 Matrix Rings and Tensor Products

It will be useful to have the following two observations on the interplay of the functor M_n and the bifunctor $\otimes_K$.

Proposition E.3.1 *If B is a K-algebra then*

$$M_n(B) \cong M_n(K) \otimes_K B$$

as K-algebras.

PROOF - Define

$$\begin{array}{rccc} \phi: & M_n(K) \times B & \longrightarrow & M_n(B) \\ & ((\kappa_{ij})_{i,j}, b) & \longmapsto & (\kappa_{ij}b)_{i,j} \end{array}$$

ϕ is K-bilinear so defines

$$\begin{array}{rccc} \tilde{\phi}: & M_n(K)\otimes_K B & \longrightarrow & M_n(B) \\ & (\kappa_{ij})_{i,j}\otimes b & \longmapsto & (\kappa_{ij}b)_{i,j} \end{array}$$

a K-linear map.

$$\begin{aligned} \tilde{\phi}\big(((\kappa_{ij})_{i,j}\otimes b)((\kappa'_{ij})_{i,j}\otimes b')\big) &= \tilde{\phi}((\sum_p \kappa_{ip}\kappa'_{pj})_{i,j}\otimes bb') \\ &= (\sum_p \kappa_{ip}\kappa'_{pj}bb')_{i,j} = (\kappa_{ip}b\kappa'_{pj}b')_{i,j} \\ &= \tilde{\phi}((\kappa_{ij})_{i,j}\otimes b)\tilde{\phi}((\kappa'_{ij})_{i,j}\otimes b') \end{aligned}$$

so $\tilde{\phi}$ is a ring homomorphism. $\tilde{\phi}$ is surjective for, given $(b_{ij})_{i,j}\in M_n(B)$, $(b_{ij})_{i,j} = \tilde{\phi}(\sum_{i,j}[(\delta_{ki}\delta_{lj})_{k,l}\otimes b_{ij}])$. Now compare the K-dimensions:

$$\dim_K M_n(B) = n^2\dim_K B = \dim_K(M_n(K)\otimes_K B)$$

Thus $\tilde{\phi}$ is an isomorphism.

$\square$

Proposition E.3.2 *$M_n(M_{n'}(K)) \cong M_{nn'}(K)$ as K-algebras.*

PROOF - Define

$$\begin{array}{rccc} \phi: & M_n(M_{n'}(K)) & \longrightarrow & M_{nn'}(K) \\ & \big((\kappa^{i\,j}_{i'j'})_{i',j'}\big)_{i,j} & \longmapsto & \big(\kappa^{i\,j}_{i'j'}\big)_{s,t} \end{array}$$

where we write $s,t\in\{1,\dots,nn'\}$ in the unique expression as $s=n'i+i', t=n'j+j'$ to obtain i,j,i',j'. ϕ is a K-linear map. Define typical matrices in $M_n(M_{n'}(K))$ by:

$$A := \big((a^{i\,j}_{i'j'})_{i',j'}\big)_{i,j}, \qquad B := \big((b^{i\,j}_{i'j'})_{i',j'}\big)_{i,j}$$

Then

$$AB = \big(\sum_p (a^{i\,p}_{i'j'})_{i',j'}(b^{p\,j}_{i'j'})_{i',j'}\big)_{i,j} = \big(\sum_p\big(\sum_{p'} a^{i\,p}_{i'p'}b^{p\,j}_{p'j'}\big)_{i',j'}\big)_{i,j}$$

so

$$\phi(AB) = \big(\sum_{p,p'} a^{i\,p}_{i'p'}b^{p\,j}_{p'j'}\big)_{s,t} = \big(a^{i\,j}_{i'j'}\big)_{s,t}\big(b^{i\,j}_{i'j'}\big)_{s,t} = \phi(A)\phi(B)$$

So ϕ is a ring homomorphism. Since ϕ is obviously bijective, the proposition is proved.

$\square$

Corollary E.3.3 $M_n(K)\otimes_K M_{n'}(K)\cong M_{nn'}(K)$.

E.4 Extension of Scalars

We look at how, given a field extension $L \supseteq K$, we can obtain L-algebras from K-algebras.

If V is a K-vector space and $L \supseteq K$ a field extension, then $V \otimes_K L$ is made into an L-vector space by

$$\lambda(v \otimes \lambda') := v \otimes \lambda\lambda' \qquad \forall \lambda, \lambda' \in L, v \in V.$$

Proposition E.4.1 *If V is finite-dimensional with K-basis $(u_i)_{i=1}^n$ then $V \otimes_K L$ is a finite-dimensional L-vector space with L-basis $(u_i \otimes 1)_{i=1}^n$.*

PROOF - $(u_i \otimes 1)_{i=1}^n$ spans $V \otimes_K L$, for every $\mathbb{Z}$-generator $v \otimes \lambda$ of $V \otimes_K L$ may be written

$$v \otimes \lambda = (\sum_{i=1}^n \kappa_i u_i) \otimes \lambda = \sum_{i=1}^n u_i \otimes \kappa_i \lambda = \sum_{i=1}^n \kappa_i \lambda (u_i \otimes 1)$$

for some $\kappa_i \in K$. To see L-linear independence, consider the function

$$\begin{array}{cccc} \psi : & V \times L & \longrightarrow & L^n \\ & (\sum \kappa_i v_i, \lambda) & \longmapsto & (\kappa_i \lambda)_{i=1}^n. \end{array}$$

This is clearly K-bilinear so defines a function $\tilde{\psi} : V \otimes_K L \to L^n$ with $\tilde{\psi}(v \otimes \lambda) = \psi(v, \lambda)$ by the universal property of tensor products. But then if $\sum_{i=1}^n \lambda_i (u_i \otimes 1) = 0$ for some $(\lambda_i)_{i=1}^n \in L^n$ then

$$0 = \tilde{\psi}(\sum_{i=1}^n \lambda_i (u_i \otimes 1)) = \tilde{\psi}(\sum_{i=1}^n u_i \otimes \lambda_i) = (\lambda_i)_{i=1}^n,$$

so that $(\lambda_i)_{i=1}^n = 0$

□

If A is a K-algebra, then $A \otimes_K L$ is an L-algebra, with the product of two $\mathbb{Z}$-generators defined by

$$(a \otimes \lambda)(a' \otimes \lambda') := aa' \otimes \lambda\lambda'$$

If A is finite-dimensional over K, the proposition above shows that $A \otimes_K L$ is finite-dimensional over L. The next result shows that $A \otimes_K L$ is central over L if and only if A is central over K.

Proposition E.4.2 *Let $Z(R)$ denote the centre of a ring R. Then*

$$Z(A \otimes_K L) = Z(A) \otimes_K L$$

PROOF - "$\supseteq$": Let $z = \sum_{i=1}^n a_i\lambda_i \in Z(A) \otimes_K L, a_i \in Z(A)$ be a typical element of the RHS. Then for any $\mathbb{Z}$-generator $a \otimes \lambda$ of $A \otimes_K L$,

$$(a \otimes \lambda)z = (a \otimes \lambda)(\sum_{i=1}^n a_i \otimes \lambda_i) = \sum_{i=1}^n aa_i \otimes \lambda\lambda_i$$
$$= \sum_{i=1}^n a_i a \otimes \lambda_i\lambda = (\sum_{i=1}^n a_i \otimes \lambda_i)(a \otimes \lambda) = z(a \otimes \lambda)$$

so $z \in Z(A \otimes_K L)$.

"$\subseteq$": Let $z = \sum_{i=1}^n a_i \otimes \lambda_i \in Z(A \otimes_K L)$. Using the relations in tensor products, this may be written with the λ_i K-linearly independent.

Then for any $a \in A$, $z(a \otimes 1) = (a \otimes 1)z$, that is $\sum_{i=1}^n a_i a \otimes \lambda_i = \sum_{i=1}^n aa_i \otimes \lambda_i$ or

$$\sum_{i=1}^n (a_i a - aa_i) \otimes \lambda_i = 0 \tag{E.1}$$

Consider now the sub-K-vector space of $A \otimes_K L$ with basis $(u_j \otimes \lambda_i)_{i=1,j=1}^{n \quad m}$, where $(u_j)_{j=1}^m$ is a K-basis for A. The element (E.1) belongs to this subspace, which shows that $a_i a - aa_i = 0$ in A for all i and hence $a_i \in Z(A)$ for all i. Thus $z \in Z(A) \otimes_K L$.

$\square$

Corollary E.4.3 *$A \otimes_K L$ is central over L if and only if A is central over K.*

PROOF - This follows from the fact that $K \otimes_K L$ is equal to $\{1 \otimes \lambda : \lambda \in L\}$, the inclusion of L into $A \otimes_K L$.

$\square$

We let $\mathrm{Gal}(L/K)$ act on $A \otimes_K L$ on the second factor.

E.5 Simple Algebras and Opposite Rings

Proposition E.5.1 *Let A be a finite-dimensional central K-algebra, and $C = A \otimes_K A^\circ$. Define a K-linear map*

$$\begin{array}{rccccccc} F: & C & \longrightarrow & \mathrm{End}_K(A) & & & \\ & a \otimes b & \longmapsto & F(a \otimes b): & A & \longrightarrow & A \\ & & & & x & \longmapsto & axb \end{array}$$

by the universal property of tensor products.

Then A is simple if and only if F is surjective. When this is the case, F is a K-vector space isomorphism.

For the proof, see [10], Chapter 9.

Corollary E.5.2 *If $L \supseteq K$ is a field extension then A is simple if and only if $A \otimes_K L$ is simple.*

PROOF - The proposition says that $A \otimes_K L$ is simple if and only if

$$F_L : (A \otimes_K L) \otimes_L (A^\circ \otimes_K L) \longrightarrow \mathrm{End}_L(A \otimes_K L)$$

is surjective. But the properties of tensor products give canonical isomorphisms

$$(A \otimes_K L) \otimes_L (A^\circ \otimes_K L) \cong A \otimes_K A^\circ \otimes_K (L \otimes_L L) \cong (A \otimes_K A^\circ) \otimes_K L$$

so that the map becomes $F_L : (A \otimes_K A^\circ) \otimes_K L \longrightarrow \mathrm{End}_L(A \otimes_K L)$ given by $F_L(a \otimes b \otimes \lambda)(x) = axb \otimes \lambda$. But if $n = \dim_K A = \dim_L A \otimes_K L$ then

$$\mathrm{End}_L(A \otimes_K L) \cong M_n(L) \cong M_n(K) \otimes_K L \cong \mathrm{End}_K(A) \otimes_K L$$

where the correspondence is

$$\begin{array}{ccc} \mathrm{End}_K(A) \otimes_K L & \cong & \mathrm{End}_L(A \otimes_K L) \\ \phi \otimes \lambda & \mapsto & \phi \otimes \lambda \end{array}$$

Thus F_L is surjective if and only if F is, ie. A is simple if and only if $A \otimes_K L$ is.

□

Corollary E.5.3 *If $L = \bar{K}$ is an algebraic closure of K, then A is simple if and only if $A \otimes_K L \cong M_n(L)$ for some n.*

PROOF - A is simple if and only if $A \otimes_K L$ is simple, and this is the case if and only if $A \otimes_K L \cong M_n(L)$ (see §E.2).

□

Thus there is always a field which, when tensored with A, gives a matrix algebra. Such a field is called a *neutralising field* for A. We will see soon that there is always a neutralising field which is a finite extension of K. But first there is one more corollary to the proposition

Corollary E.5.4 *If A and B are central simple K-algebras then so is $A \otimes_K B$.*

PROOF - Let $L = \bar{K}$ be an algebraic closure of K. Then $A \otimes_K L$ is simple with centre L so $A \otimes_K L \cong M_n(L)$. Similarly $B \otimes_K L \cong M_{n'}(L)$. Using this and the properties of tensor products,

$$
\begin{aligned}
(A \otimes_K B) \otimes_K L &\cong A \otimes_K (L \otimes_K B) \\
&\cong A \otimes_K ((L \otimes_L L) \otimes_K B) \\
&\cong (A \otimes_K L) \otimes_L (B \otimes_K L) \\
&\cong M_n(L) \otimes_L M_{n'}(L) \\
&\cong M_{nn'}(L)
\end{aligned}
$$

This shows that $(A \otimes_K B) \otimes_K L$ is central over L, so by §E.4 $A \otimes_K B$ is central over K, and then by the previous corollary $A \otimes_K B$ is simple.

□

E.6 Finite Dimensional Neutralising Fields

Proposition E.6.1 *Let D be a finite-dimensional central division algebra over a field K. Then there exists a finite Galois extension L of K such that $D \otimes_K L \cong M_n(L)$ as L-algebras, for some n.*

PROOF - We know that D is central simple over K, so by §E.5 we have $D \otimes_K \bar{K} \cong M_n(\bar{K})$, so $\dim_K D = \dim_{\bar{K}} D \otimes_K \bar{K} = n^2$ is a square. The desired field L will be constructed from a subfield L' of D, whose existence follows from the following result, proved in [11], §10, no.3.

- Any maximal commutative subring of D is a field L' with $\dim_K L' = n$; L' can be chosen so that L'/K is a separable extension.

We show that L' is a neutralising field for D, ie. $D \otimes_K L'$ is isomorphic to a matrix algebra over L'. To see this, define in the usual way, using the universal property of tensor products,

$$
\begin{array}{rclcrcl}
\phi: & D \otimes_K L' & \longrightarrow & \mathrm{End}_{L'}(D) & & & \\
 & d \otimes \lambda & \longmapsto & \phi(d \otimes \lambda): & D & \longrightarrow & D \\
 & & & & x & \longmapsto & \lambda x d
\end{array}
$$

ϕ is clearly L'-linear, given the L'-vector space structure on $D \otimes_K L'$. Now

$$
\begin{gathered}
\phi((d \otimes \lambda)(d' \otimes \lambda'))(x) = \phi(dd' \otimes \lambda\lambda')(x) \\
= \lambda\lambda' x d d' = \phi(d' \otimes \lambda')(\lambda x d) = \phi(d' \otimes \lambda') \circ \phi(d \otimes \lambda)(x)
\end{gathered}
$$

so ϕ is a ring anti-homomorphism. We know (§E.5) that $D \otimes_K L'$ is simple, and since ϕ is not the zero map and $\ker \phi$ is a double-sided ideal of $D \otimes_K L'$, $\ker \phi = 0$, so ϕ is injective.

Now consider the L'-dimension of each side to show that ϕ is also surjective. For the left-hand side, $\dim_{L'}(D \otimes_K L') = \dim_K D = n^2$. For the right-hand side,

$$\begin{array}{rcll} \dim_K D & = & (\dim_{L'} D)(\dim_K L') & \quad \text{by considering bases, so} \\ n^2 & = & (\dim_{L'} D)n & \end{array}$$

so $\dim_{L'} D = n$ and hence $\dim_{L'} \mathrm{End}_{L'}(D) = n^2$

Thus the L'-dimensions are equal, and linear algebra shows that the L'-linear map ϕ is injective if and only if it is surjective, hence it is surjective.

But $\mathrm{End}_{L'}(D) \cong M_n(L')$ is anti-isomorphic to itself under the transposition map, so $D \otimes_K L' \cong M_n(L')$ as L'-algebras.

Recall that it is possible to choose L' so that L'/K is a separable extension. With this L', its normal closure in a chosen $\bar{K}$ is a finite Galois extension of K, and

$$D \otimes_K L \cong (D \otimes_K L') \otimes_{L'} L \cong M_n(L') \otimes_{L'} L \cong M_n(L).$$

$\square$

E.7 Norms on Finite Dimensional Algebras

These results are needed for our study of Brauer groups of local fields in Chapter 4.

E.7.1 The Absolute Norm

Definition E.7.1 *Let K be a field, A a finite dimensional K-algebra. For $a \in A$, define θ_a to be the left-homothety by a in A, ie.*

$$\begin{array}{rccc} \theta_a : & A & \longrightarrow & A \\ & x & \longmapsto & ax, \end{array}$$

which is a K-linear map. Define the norm map of A/K by

$$N_{A/K}(a) := \det \theta_a.$$

The norm map has the following properties.

Proposition E.7.2 *1. $N_{A/K}(a) \in K$;*

2. $N_{A/K}(ab) = N_{A/K}(a) N_{A/K}(b)$;

3. If a is invertible, $N_{A/K}(a) \neq 0$;

4. If one fixes a K-basis of A, then $N_{A/K}(a)$ is a homogeneous polynomial of degree $[A : K]$ in the $[A : K]$ coordinates of a, with coefficients in K;

5. *If L is a commutative subfield of A containing K, and $\lambda \in L$, then*

$$N_{A/K}(\lambda) = N_{L/K}(\lambda)^{[A:L]}.$$

PROOF -

1. Obvious.

2. $\theta_{ab} = \theta_a \circ \theta_b$ so that $\det \theta_{ab} = (\det \theta_a)(\det \theta_b)$.

3. $\mathrm{id}_A = \theta_{a^{-1}a} = \theta_a \circ \theta_{a^{-1}}$ so $1 = (\det \theta_a)(\det \theta_{a^{-1}})$.

4. Obvious.

5. Write $m = [A : L]$. A is an L-vector space by scalar multiplication on the left. Choose an L-basis $u_1, \ldots, u_m$ of A so

$$A = Lu_1 \oplus \ldots \oplus Lu_m.$$

Now $\lambda \in L$ takes an element $\sum c_i u_i \in A$ to $\sum (\lambda c_i) u_i$, so if Θ_λ is the matrix for multiplication by λ in the K-vector space L, then the matrix for multiplication by λ in the K-vector space A is the block-diagonal matrix

$$\begin{pmatrix} \Theta_\lambda & & & \\ & \Theta_\lambda & & \\ & & \ddots & \\ & & & \Theta_\lambda \end{pmatrix}$$

with determinant $(\det \Theta_\lambda)^m = N_{L/K}(\lambda)^{[A:L]}$.

□

E.7.2 The Reduced Norm

Let A be a central simple K-algebra of dimension n^2. Let L be a neutralising field for A (see §E.5) and $h : A \otimes_K L \longrightarrow M_n(L)$ an isomorphism.

Definition E.7.3 *The* reduced norm *of A is*

$$\begin{array}{rccc} \mathrm{Nrd}: & A & \longrightarrow & L \\ & x & \longmapsto & \det h(x \otimes 1). \end{array}$$

Proposition E.7.4 *1.* Nrd *does not depend on the choice of L or h.*

2. $\mathrm{Nrd}(xy) = \mathrm{Nrd}(x)\mathrm{Nrd}(y)$ *for all $x, y \in A$.*

3. $\mathrm{Nrd}(x) \in K$.

4. If $x \in A$ is invertible, $\mathrm{Nrd}(x) \neq 0$.

5. *If one fixes a K-basis of A then* $\mathrm{Nrd}(x)$ *is a homogeneous polynomial of degree n in the n^2 coordinates of x, with coefficients in K.*

6. $N_{A/K}(x) = \mathrm{Nrd}(x)^n$.

PROOF -

1. Independence of h: Suppose $h' : A \otimes_K L \longrightarrow M_n(L)$ is another isomorphism. Then $h' \circ h^{-1} : M_n(L) \longrightarrow M_n(L)$ is an L-algebra automorphism. By the Skolem-Noether Theorem (Proposition 3.5.1) this is an inner automorphism, ie. there is $B \in M_n(L)^*$ such that $h' \circ h^{-1}(X) = B^{-1}XB$ for all $X \in M_n(L)$. So if $X = h(x \otimes 1)$,
$$h'(x \otimes 1) = B^{-1}h(x \otimes 1)B,$$
and so $\det h'(x \otimes 1) = \det h(x \otimes 1)$.

   Independence of L: Take two neutralising fields L, L' and embed them into a common field L''. Let
$$\begin{array}{rccc} h: & A \otimes_K L & \longrightarrow & M_n(L) \\ h': & A \otimes_K L' & \longrightarrow & M_n(L') \end{array}$$
be isomorphisms. Consider the diagram
$$\begin{array}{ccccccccc} A \otimes_K L & \xrightarrow[\sim]{h} & M_n(L) & & M_n(L') & \xleftarrow{h'} & A \otimes_K L' \\ \downarrow \mathrm{id}\otimes 1 & \square & \downarrow \mathrm{inc.} & & \downarrow \mathrm{inc.} & \square & \downarrow \mathrm{id}\otimes 1 \\ A \otimes_K L \otimes_L L'' & \xrightarrow{h\otimes\mathrm{id}} & M_n(L'') & = & M_n(L'') & \xleftarrow{h'\otimes 1} & A \otimes_K L' \otimes_{L'} L''. \end{array}$$
We have $\det h(x \otimes 1) = \det 1 \otimes h(x \otimes 1)$ and by independence of the isomorphism, this is $\det(h'(x \otimes 1) \otimes 1) = \det h'(x \otimes 1)$.

2. Obvious.

3. Recall (Proposition 3.2.1) there exists a Galois neutralising field for A. If
$$h : D \otimes_K L \longrightarrow M_n(L)$$
is an isomorphism, so is $s \circ h$ for any $s \in \mathrm{Gal}(L/K)$, and $\det(s \circ h(x \otimes 1)) = s \det h(x \otimes 1)$ because s is a ring homomorphism. Hence by (1) above, $s \det h(x \otimes 1) = \det h(x \otimes 1)$ for all such s and so $\mathrm{Nrd}(x) \in K$ (see Definition C.1.5).

4. Follows from (2) as in Proposition E.7.2.

5. If $(u_1, \ldots, u_{n^2})$ is a K-basis for A then a general element of A comes from an n^2-tuple of coordinates $(x_1, \ldots, x_{n^2}) \in K^{n^2}$, and the Nrd map is then given by the homogeneous polynomial form
$$\mathrm{Nrd}(x) = \det(\sum_i x_i h(u_i \otimes 1)) \in L[x_1, \ldots, x_{n^2}].$$

As in (3), take L to be a Galois neutralising field for A. We apply the Skolem-Noether Theorem (Proposition 3.5.1) again to see that for each $s \in \mathrm{Gal}(L/K)$ there is a matrix $B \in M_n(L)$ such that

$$sh(x \otimes 1) = B^{-1}h(x \otimes 1)B \qquad \text{for all } x \in A.$$

Hence

$$\begin{aligned} s\mathrm{Nrd}(x) &= \det(\sum(x_i)sh(u_i \otimes 1)) \\ &= \det(\sum(x_i)B^{-1}h(u_i \otimes 1)B) \\ &= \det(\sum(x_i)h(u_i \otimes 1)) = \mathrm{Nrd}(x) \end{aligned}$$

as polynomials in $L[x_1, \ldots, x_{n^2}]$. So each coefficient is $\mathrm{Gal}(L/K)$-invariant, and so belongs to K.

6. Write $B = h(x \otimes 1)$, so $\mathrm{Nrd}(x) = \det B$ and $N_{A/K}(x) = \det \theta_x$ where θ_x is left-homothety by x in the K-vector space A. We note that in the extension of scalars (Chapter 3 §E.4) a K-basis of A becomes an L-basis of $A \otimes_K L$, so that the matrix of θ_x is also the matrix for left-homothety by $x \otimes 1$ in the L-vector space $A \otimes_K L$.

   Applying h to this is equivalent to a basis change, so $N_{A/K}(x) = \det \theta_B$ where θ_B is left-homothety by B in the L-vector space $M_n(L)$.

   $M_n(L)$ is the direct sum of n copies of the column space L^n as an $M_n(L)$-module. Left-multiplication by B induces an L-endomorphism of this column space with determinant $\det B$. Hence

$$\det \theta_B = (\det B)^n$$

   ie. $N_{A/K}(x) = (\mathrm{Nrd}(x))^n$.

$\square$

Bibliography

[1] J-P. Serre, *Local Fields* (Graduate Texts in Mathematics ♯ 67), Springer Verlag, New York, 1979.

[2] J-P. Serre, *Galois Cohomology*, Springer Verlag, New York, 1997.

[3] M. F. Atiyah and C. T. C. Wall, "Cohomology of Groups", in Cassels and Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, 1967.

[4] K. Gruenberg, "Profinite Groups", in Cassels and Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, 1967.

[5] J-P. Serre, "Local Class Field Theory", in Cassels and Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, 1967.

[6] D. Montgomery and L. Zippin, *Topological Transformation Groups*, Interscience, New York and London, 1955.

[7] J. J. Rotman, *Notes on Homological Algebra*, Van Nostrand Reinhold, New York, 1970.

[8] I. Stewart, *Galois Theory*, Chapman and Hall, London, 1989.

[9] N. Bourbaki, *Elements de Mathematique, Livre 5: Espaces Vectoriels Topologiques*, 1955

[10] A. Weil, *Basic Number Theory*, Springer Verlag, Berlin / New York, 1967.

[11] N. Bourbaki, *Elements de Mathematique, Livre 2: Algèbre, Chapitre 8: Modules et Anneaux Semi-Simples*, 1958.

[12] C. Small, *Arithmetic of Finite Fields*, M. Dekker, New York, 1991.

Typeset in LaTeX.