GROUP COHOMOLOGY AND KUMMER THEORY

KRIS HARPER

Abstract. We develop group cohomology by means of derived functors and the Ext groups. This leads to a direct application in the subject of field extensions known as Kummer theory in which we take particular fields and classify their finite abelian extensions as subgroups of a particular group.

Contents

1. Introduction

The main idea behind *Kummer theory* is to classify certain abelian extensions of a field K that contains the n^{th} roots of unity. In order to arrive at these results, we first must introduce the idea of group cohomology, which will be defined in §4. We'll develop this concept using some basic results from homological algebra, including derived functors and the Ext groups, which are discussed in §2 and §3 respectively.

Historically, this subject began by focusing on the case when L/K is an extension with cyclic Galois group. In this specific case it can be shown that $L = K(\sqrt[n]{\alpha})$ for some element $\alpha \in K$. The following theorem gets its name from the fact that it was the 90^{th} theorem in Hilbert's seminal work *Zahlbericht* of 1897.

Theorem 1.1 (Hilbert's Theorem 90)**.** *Let L/K be a Galois extension. Suppose $G = Gal(L/K)$ is cyclic of order n, and σ is a generator. Then $N_{L/K}(a) = 1$ if and only if $a = \sigma(b)/b$ for some b in L.*

Proof. First suppose $a = \sigma(b)/b$. Then since $\sigma^n = 1$ we have

$$N_{L/K}(a) = \prod_{i=0}^{n-1} \sigma^i\left(\frac{\sigma(b)}{b}\right) = \prod_{i=0}^{n-1} \frac{\sigma^{i+1}(b)}{\sigma^i(b)} = \frac{\sigma(b)\sigma^2(b)\ldots\sigma^n(b)}{b\sigma(b)\ldots\sigma^{n-1}(b)} = \frac{\sigma^n(b)}{b} = 1.$$

Date: August 13, 2010.

Conversely, suppose $N_{L/K}(a) = \prod_{i=0}^{n-1} \sigma^i(a) = 1$. Consider

$$\lambda(c) = \sum_{i=0}^{n-1} \left(\prod_{j=0}^{i} \sigma^j(a) \right) \sigma^i(c).$$

Note that the term with $i = n-1$ reduces to $\sigma^{n-1}(c)$ by assumption. Lemma 5.1 will show there exists $c \in L$ such that $\lambda(c) \neq 0$. Let $b = \lambda(c)$. Now note that

$$\begin{aligned} \sigma(b) = \sigma(\lambda(c)) &= \sum_{i=0}^{n-1} \left(\prod_{j=0}^{i} \sigma^{j+1}(a) \right) \sigma^{i+1}(c) \\ &= a^{-1}(b - ac) + \sigma^n(c) \\ &= a^{-1}(b - ac) + c \\ &= ba^{-1}. \end{aligned}$$

Thus $a = b/\sigma(b)$. But $N_{L/K}(a) = 1 = N_{L/K}(a^{-1})$ so we could have just as well started with a^{-1} and shown $a = \sigma(b)/b$. □

We will eventually prove a stronger statement of this theorem in §5. Our overall goal and the goal of Kummer theory in general is to generalize beyond the case where the Galois group is cyclic.

Within this paper we will chiefly be dealing with modules over rings. To that end, whenever a category is mentioned, it should be assumed that it is a category of modules. Among other things, this ensures us that for each object A there is projective object P and an epimorphism $P \to A$ as well as an injective object I and a monomorphism $I \to A$.

Additionally, we will often be dealing with fields K which contain the n^{th} roots of unity. In all of these cases, if the characteristic of K is nonzero then it should be assumed that the characteristic does not divide n.

2. Derived Functors

We recall the notion of a chain complex and the homology groups of such. Chain and cochain complexes will be denoted by boldface type as $\mathbf{C}$. The homology and cohomology groups of these complexes will be denoted as $H_i(\mathbf{C})$ and $H^i(\mathbf{C})$ respectively.

For the purposes of background information we will state an important theorem of homological algebra which will be used in the proof of Lemma 2.2. A proof can be found in [4] pp. 35-36.

Theorem 2.1. *Let $\mathbf{P}$ be a projective resolution of an object A in a category $\mathcal{A}$ and let $f' : A \to B$ be a morphism of objects in $\mathcal{A}$. Then for each resolution $\mathbf{Q}$ of B there is a chain map $f : \mathbf{P} \to \mathbf{Q}$ lifting f'. The chain map f is unique up to homotopy.*

Lemma 2.2. *Let $\mathbf{P}$ and $\mathbf{Q}$ be projective resolutions of some object A in a category $\mathcal{A}$. Then there is a canonical isomorphism $H_i(F(\mathbf{P})) \to H_i(F(\mathbf{Q}))$.*

Proof. Since $\mathbf{P}$ and $\mathbf{Q}$ are projective resolutions, Theorem 2.1 gives a chain map f which lifts the identity map on A. This gives the induced map $f_* : H_i(F(\mathbf{P})) \to H_i(F(\mathbf{Q}))$. Furthermore, any other such map must be chain homotopic to f and thus have the same induced map f_*. This shows that f_* is indeed canonical. Note also we have a map $g : \mathbf{Q} \to \mathbf{P}$ so that $g_* : H_i(F(\mathbf{Q})) \to H_i(F(\mathbf{P}))$. We know the identity map on $\mathbf{P}$ and gf are both chain maps that lift the identity on A and are therefore homotopic as chain maps. Using the fact that $g_*f_* = (gf)_*$ we see g_*f_* is the identity on $H_i(F(\mathbf{P}))$. A similar argument shows f_*g_* is the identity on $H_i(F(\mathbf{Q}))$ so that f_* is an isomorphism. □

Definition 2.3. Let $F : \mathcal{A} \to \mathcal{B}$ be a right exact functor. Let A be an object of $\mathcal{A}$ and let $\mathbf{P}$ be a projective resolution of A. Then for each $i \geq 0$ we define

$$L_iF(A) = H_i(F(\mathbf{P})).$$

The functors L_iF are called the *left derived functors of* F and their collection will be known as a *left derived series for* F.

Note that since we've required F to be a right exact functor in the previous definition, the sequence $F(P_1) \to F(P_0) \to F(A) \to 0$ is exact. This means we always have $L_0F(A) \cong F(A)$. Furthermore, in light of Lemma 2.2 we know the functors L_iF are independent of the choice of projective resolution for A.

One of the most fundamental results of homology theory is the long exact sequence of homology groups: given a short exact sequence of chain complexes, we get a long exact sequence of homology groups with well-defined connecting homomorphisms. Since left derived functors give chain complexes, we may expect a similar result given a short exact sequence. The following theorem will construct a long exact sequence of the left derived functors.

Theorem 2.4. *Let $F : \mathcal{A} \to \mathcal{B}$ be an additive functor and let*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\varphi"] & B \arrow[r, "\psi"] & C \arrow[r] & 0 \end{tikzcd}$$

be a short exact sequence. Then for each i there exists a connecting homomorphism $\delta_i : L_iF(C) \to L_{i-1}F(A)$ so that

$$\begin{tikzcd} \cdots \arrow[r] & L_iF(A) \arrow[r, "\varphi_*"] & L_iF(B) \arrow[r, "\psi_*"] & L_iF(C) \arrow[r, "\delta_i"] & L_{i-1}F(A) \arrow[r] & \cdots \end{tikzcd}$$

$$\begin{tikzcd} \cdots \arrow[r] & L_1F(C) \arrow[r, "\delta_1"] & L_0F(A) \arrow[r, "\varphi_*"] & L_0F(B) \arrow[r, "\psi_*"] & L_0F(C) \arrow[r] & 0 \end{tikzcd}$$

is a long exact sequence.

Proof. Let P_0 and R_0 be projective modules with surjective maps $f_0 : P_0 \to A$ and $h_0 : R_0 \to C$. We then have the diagram

$$\begin{tikzcd} & R_0 \arrow[dl, dashed, "\eta"'] \arrow[d, "h_0"] & \\ B \arrow[r, "\psi"] & C \arrow[r] & 0 \end{tikzcd}$$

where we know the map $\eta : R_0 \to B$ exists since R_0 is projective. We can form the projective module $Q_0 = P_0 \oplus R_0$ and a map $g_0 : Q_0 \to B$ defined component-wise. The first component of g_0 is $\varphi f_0 : P_0 \to B$ and the second component is given by

η. This gives the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & P_0 \arrow[r] \arrow[d, "f_0"] & Q_0 \arrow[r] \arrow[d, "g_0"] & R_0 \arrow[r] \arrow[d, "h_0"] & 0 \\
0 \arrow[r] & A \arrow[r, "\varphi"] & B \arrow[r, "\psi"] & C \arrow[r] & 0
\end{tikzcd}$$

which has exact rows.

Let P_1 be a projective module with a surjection $P_1 \to \ker f_0$. Note that we have an inclusion $\ker f_0 \to P_0$, so we can define the map f_1 as the composite $P_1 \to \ker f_0 \to P_0$. Inductively, given $\ker f_n$, let P_{n+1} be a projective module surjecting onto it and let f_{n+1} be the composite $P_{n+1} \to \ker f_n \to P_n$. Hence, we have the diagram

$$\begin{tikzcd}
0 \arrow[dr] & & 0 & & 0 \arrow[dr] & & 0 & & & & \\
& \ker f_3 \arrow[ur] \arrow[dr] & & & & \ker f_1 \arrow[ur] \arrow[dr] & & & & & \\
\cdots \arrow[ur] \arrow[rr] & & P_3 \arrow[rr, "f_3"] \arrow[dr] & & P_2 \arrow[ur] \arrow[rr, "f_2"] & & P_1 \arrow[rr, "f_1"] \arrow[dr] & & P_0 \arrow[r, "f_0"] & A \arrow[r] & 0 \\
& & & \ker f_2 \arrow[ur] \arrow[dr] & & & & \ker f_0 \arrow[ur] \arrow[dr] & & & \\
& & 0 \arrow[ur] & & 0 & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

giving a projective resolution $\mathbf{P}$ of A. We can use the same process to construct a projective resolution $\mathbf{R}$ for C. Then form $Q_i = P_i \oplus R_i$ for each i and define g_i component-wise in the same way we defined g_0. This gives a projective resolution $\mathbf{Q}$ for B. All this gives a short exact sequence of chain complexes

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{P} \arrow[r] & \mathbf{Q} \arrow[r] & \mathbf{R} \arrow[r] & 0.
\end{tikzcd}$$

Since F is an additive functor and $Q_i = P_i \oplus R_i$ for each i, we also know

$$\begin{tikzcd}
0 \arrow[r] & F(\mathbf{P}) \arrow[r] & F(\mathbf{Q}) \arrow[r] & F(\mathbf{R}) \arrow[r] & 0.
\end{tikzcd}$$

is a short exact sequence. Now we can use the connecting homomorphism of homology to get a map $\delta_i : H_i(F(\mathbf{R})) \to H_{i-1}(F(\mathbf{P}))$. We also use the long exact sequence of homology to get the desired long exact sequence. Note that by Lemma 2.2 the maps δ_i do not depend on the projective resolutions and only depend on the original short exact sequence. □

It should be noted that Theorem 2.4 shows that L_i is a functor from the category of short exact sequences to the category of long exact sequences.

There is an obvious complement to left derived functors. Namely, if we take an object, make an injective resolution and apply a functor, this results in a cochain complex instead of a chain complex. We can then begin to discuss cohomology groups. Definition 2.5 will make this comparison formal.

Definition 2.5. Let $F : \mathcal{A} \to \mathcal{B}$ be a left exact functor between abelian categories. Let A be an object of $\mathcal{A}$ and let $\mathbf{I}$ be an injective resolution of A. Then for each $i \geq 0$ we define

$$R^i F(A) = H^i(F(\mathbf{I})).$$

The functors $R^i F$ are called the *right derived functors of* F and their collection will be known as a *right derived series for* F.

In an analog to the functors L_iF, note that since we've required F to be left exact, we get the exact sequence $0 \to F(A) \to F(I^0) \to F(I^1)$. We then have $R^0F(A) \cong F(A)$ for each object A.

Consider the opposite categories $\mathcal{A}^{op}$ and $\mathcal{B}^{op}$ with each morphism reversed. It is immediate that if F is a left exact functor then $F^{op} : \mathcal{A}^{op} \to \mathcal{B}^{op}$ is a right exact functor. Then using Definition 2.3 we have a left derived series L_iF^{op}. Furthermore, an injective resolution $\mathbf{I}$ in $\mathcal{A}$ is a projective resolution in $\mathcal{A}^{op}$ so that $R^iF(A) = (L_iF^{op})^{op}(A)$. In particular, we have corresponding results to Lemma 2.2 and Theorem 2.4 for the functors R^iF.

3. The Hom Functors

Now we are in a position to begin using derived functors in specific contexts. We'll start with the Hom functors. Let R be a ring and A an R-module. Recall that $\mathrm{Hom}_R(A, -)(B)$ is the group of all R-module homomorphisms from A to B. Thus $\mathrm{Hom}_R(A, -)$ is a covariant functor from the category of R-modules to itself. Furthermore, this functor is left exact, and is exact if and only if A is a projective module.

Definition 3.1. Let R be a ring and A an R-module. We define the *Ext groups* as the right derived series for $\mathrm{Hom}_R(A, -)$. Namely,

$$\mathrm{Ext}^i_R(A, B) = R^i\mathrm{Hom}_R(A, -)(B).$$

Note that we have $\mathrm{Ext}^0_R(A, B) = \mathrm{Hom}_R(A, B)$.

Recall now that, given a ring R and an R-module B, we also have the contravariant functor $\mathrm{Hom}_R(-, B)$ and that this is a left exact functor as well. In this case the functor is exact if and only if B is an injective module. Note that we obviously have $R^i\mathrm{Hom}_R(A, -)(B) = R^i\mathrm{Hom}_R(-, B)(A)$ when $i = 0$. We may then wish for some correspondence between the two groups for higher values of i. The next theorem will show that there is indeed a natural equivalence between them for each i.

Theorem 3.2. *Let A and B be R-modules. Define $F^i(A, B) = R^i\mathrm{Hom}_R(A, -)(B)$ and $G^i(A, B) = R^i\mathrm{Hom}_R(-, B)(A)$. Then there is a natural isomorphism between $F^i(-, -)$ and $G^i(-, -)$.*

Proof. We will use induction to define natural equivalences $\Psi^i : F^i(-, -) \to G^i(-, -)$. In the case $i = 0$ we may take Ψ to be the identity map since by definition $F^0(A, B) = \mathrm{Hom}_R(A, B) = G^0(A, B)$. Now let $0 \longrightarrow B \xrightarrow{\varphi} I \xrightarrow{\psi} C \longrightarrow 0$ be a short exact sequence of R-modules with I injective. Recall that $\mathrm{Hom}_R(-, I)$ is an exact functor so we have $F^i(A, I) = 0 = G^i(A, I)$ for $i \geq 1$ and each R-module A.

Now by Theorem 2.4 we have long exact sequences corresponding to $F^i(A, -)$ and $G^i(A, -)$. Since $F^i(A, I) = 0 = G^i(A, I)$ for each $i \geq 1$, we know the connecting homomorphisms δ_i and δ_i' are all surjective. This gives the following diagram

$$\begin{tikzcd}
\mathrm{Hom}_R(A, I) \arrow[r, "\psi_*"] \arrow[d, equal] & \mathrm{Hom}_R(A, C) \arrow[r, "\delta_1"] \arrow[d, equal] & F^1(A, B) \arrow[r] \arrow[d, dashed, "\Psi^1_{A,B}"] & 0 \\
\mathrm{Hom}_R(A, I) \arrow[r, "\psi'_*"] & \mathrm{Hom}_R(A, C) \arrow[r, "\delta'_1"] & G^1(A, B) \arrow[r] & 0
\end{tikzcd}$$

where we define $\Psi^1_{A,B}$ as follows. Take $a \in F^1(A,B)$ and since δ_1 is surjective, there is some $b \in \mathrm{Hom}_R(A,C)$ with $\delta_1(b) = a$. Then set $\Psi^1_{A,B}(a) = \delta_1'(b)$. To show this is well defined, suppose we also have $b' \in \mathrm{Hom}_R(A,C)$ with $\delta_1(b') = a$. Then $\delta_1(b - b') = 0$ so $b - b' \in \ker \delta_1$. But these sequences are exact, so $\ker \delta_1 = \mathrm{im}\, \psi_* = \mathrm{im}\, \psi'_* = \ker \delta_1'$. Thus $b - b' \in \ker \delta_1'$ as well and $\delta_1'(b) = \delta_1'(b') = \Psi^1_{A,B}(a)$. Note that the definition of $\Psi^1_{A,B}$ makes the above diagram commute.

Similarly, if Ψ^i is defined, we can define $\Psi^{i+1}_{A,B}(a) = \delta_i' \Psi^i_{A,C}(b)$ where $\delta_i(b) = a$. To show this is well defined, suppose we have some $b' \in F^{i+1}(A,B)$ with $\delta_i(b') = a$. Then $b - b' \in \ker \delta_i$ so there is some $c \in F^i(A,I)$ with $\psi_*(c) = b - b'$. By commutativity of the following diagram

$$\begin{tikzcd}
\cdots \arrow[r] & F^i(A,I) \arrow[r, "\psi_*"] \arrow[d, "\Psi^i_{A,I}"] & F^i(A,C) \arrow[r, "\delta_i"] \arrow[d, "\Psi^i_{A,C}"] & F^{i+1}(A,B) \arrow[r] \arrow[d, dashed, "\Psi^{i+1}_{A,B}"] & 0 \arrow[r] & \cdots \\
\cdots \arrow[r] & G^i(A,I) \arrow[r, "\psi_*"] & G^i(A,C) \arrow[r, "\delta_i'"] & G^{i+1}(A,B) \arrow[r] & 0 \arrow[r] & \cdots
\end{tikzcd}$$

we know $\Psi^i_{A,C}(b - b') = \psi'_* \Psi^i_{A,I}(a)$. But then $b - b' \in \mathrm{im}\, \psi'_*$ and by exactness $b - b' \in \ker \delta_i'$. Thus $\delta_i'(b) = \delta_i'(b') = \Psi^{i+1}_{A,B}$. As in the base case, note that by definition $\Psi^{i+1}_{A,B}$ makes the above diagram commute.

We must show $\Psi^{i+1}_{A,B}$ is independent of the short exact sequence presenting B. Suppose we have the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r] \arrow[d, "\alpha"] & I \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & B' \arrow[r] & I' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

where I and I' are both injective. Now consider the following diagram

$$\begin{tikzcd}
& F^i(A,C') \arrow[rr, "\delta_i"] \arrow[dd, "\Psi^i"] & & F^{i+1}(A,B') \arrow[dd, "\Psi^{i+1}"] \\
F^i(A,C) \arrow[ur, "\gamma_*"] \arrow[rr, "\delta_i"] \arrow[dd, "\Psi^i"] & & F^{i+1}(A,B) \arrow[ur, "\alpha_*"] \arrow[dd, "\Psi^{n+1}"] & \\
& G^i(A,C') \arrow[rr, "\delta_i"] & & G^{i+1}(A,B') \\
G^i(A,C) \arrow[ur, "\gamma_*"] \arrow[rr, "\delta_i"] & & G^{i+1}(A,B). \arrow[ur, "\alpha_*"] &
\end{tikzcd}$$

The top square is commutative by the naturality of the long exact sequence in homology, which translates to the long exact sequence in Theorem 2.4. The same argument holds for the bottom square. The front and back squares are commutative due to the definition of $\Psi^{i+1}_{A,B}$ and the left square is commutative by our inductive hypothesis that $\Psi^i_{A,S}$ is a natural transformation. Since δ_i is a surjection, we must have that the right square commutes as well. Now we just let $\alpha : B \to B$ be the identity to see that the two versions of Ψ^i are the same.

Note that the commutativity of the right square also shows that Ψ^{i+1} is natural in B. We can use a similar argument to show that it's natural in A, giving a natural equivalence between $F^i(-,-)$ and $G^i(-,-)$. □

Corollary 3.3. *We have* $\mathrm{Ext}^i_R(A,B) \cong R^i\mathrm{Hom}_R(-,B)(A)$.

4. Group Cohomology

We now begin to introduce *group cohomology.* If R is a ring and G a group, recall the definition of the group ring RG. This is the set of formal sums

$$\textstyle\sum_{i=1}^n a_i g_i \quad a_i \in R \text{ and } g_i \in G$$

where addition and multiplication are defined in the obvious way.

Definition 4.1. Let G be a group. A *G-module* is an abelian group A with a $\mathbb{Z}G$ action, that is, a module over the group ring $\mathbb{Z}G$.

Note that we can always form a $\mathbb{Z}G$ module from any abelian group A by giving it the trivial action under $\mathbb{Z}G$, that is, $ga = a$ for all $g \in G$ and $a \in A$. These are known as *trivial* $\mathbb{Z}G$ modules. For our purposes we will usually consider $\mathbb{Z}$ as a trivial $\mathbb{Z}G$-module.

Definition 4.2. Let G be a group and let A be a G-module. We have the *invariant subgroup*

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

Let M be the G-module generated by elements of the from $ga - a$ for $g \in G$ and $a \in A$. Then we also have the *coinvariant quotient group*

$$A_G = A/M.$$

We note that $-^G$ and $-_G$ are functors form the category of G modules to the category of abelian groups. The following lemma will relate the invariant functor $-^G$ to our previous discussion of the Hom groups.

Lemma 4.3. *Let G be a group and A a G-module. Then* $A^G \cong \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$.

Proof. Let $\varphi_a \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)$ be the grop homomorphism such that $\varphi_a(1) = a$. Note that this completely determines φ_a. Consider the map $\Psi : a \mapsto \varphi_a$. Note then that Ψ is surjective by definition. Clearly if $a \neq b$ in A then $\varphi_a \neq \varphi_b$ since they differ at 1, so Ψ is injective as well. Finally note $\varphi_{a+b}(1) = a + b = \varphi_a(1) + \varphi_b(1)$ and since φ_a and φ_b are determined by where 1 is sent, this shows $\Psi : A \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)$ is an isomorphism.

Now let Ψ' be the restriction of Ψ to A^G. Let $\varphi_a \in \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$. Then since $\mathbb{Z}G$ has trivial action on $\mathbb{Z}$, for $g \in G$ we have $\Psi'(a) = \varphi_a(1) = \varphi_a(g \cdot 1) = g\varphi_a(1) = g \cdot a$. Thus $a \in A^G$ so Ψ' surjects onto $\mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A)$. Since Ψ' is the restriction of the isomorphism Ψ, this gives $A^G \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A)$. □

At this point we are able to define group cohomology. Our definition arises from the theory of derived functors, which may seem strange when compared with the often explicit construction of the cohomology of topological spaces. However, it should be noted that there is an equivalent definition of group cohomology which makes no use of derived functors and instead relies on the familiar coboundary and cocycle constructions. We will soon use some of these ideas to give explicit descriptions of the first cohomology group.

Definition 4.4. Let G be a group and let A be a G-module. The *homology groups of G with coefficients in A* are defined to be the left derived functors $L_i(-_G)(A)$ and are written $H_i(G, A)$. Likewise, the *cohomology groups of G with coefficients in A* are defined to be the right derived functors $R^i(-^G)(A)$ and are written $H^i(G, A)$. By definition $H_0(G, A) = A_G$ and $H^0(G, A) = A^G$.

Corollary 4.5. *Let G be a group and A a G-module. Then*

$$H^i(G, A) \cong \operatorname{Ext}^i_{\mathbb{Z}G}(\mathbb{Z}, A).$$

Proof. From Lemma 4.3 we know that the functor $-^G$ is equivalent to $\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}, -)$. In light of Definition 4.4 we know $H^i(G, A)$ is then isomorphic to $R^i\operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}, -)(A)$, which is $\operatorname{Ext}^i_{\mathbb{Z}G}(\mathbb{Z}, A)$ by definition. □

At this point we should also recall Theorem 3.2 and the remarks following it. Namely, we also know that $H^i(G, A) \cong R^i\operatorname{Hom}_R(-, A)(\mathbb{Z})$. Of course, this discussion is still lacking in explicit descriptions of the cohomology groups. The following definition will begin to address that.

Definition 4.6. Let G be a group and A a left G-module. A *crossed homomorphism* or 1-*cocyle* is a map $d : G \to A$ which satisfies $d(gh) = gd(h) + d(g)$. The collection of 1-cocyles will be denoted $Z(G, A)$.

For each $a \in A$ we define the *principle crossed homomorphism* or 0-*coboundary* $d_a : G \to A$ such that $d_a(g) = ga - a$. The set of 0-coboundaries will be denoted $B(G, A)$.

It should be noted that for $a \in A$ we have

$$d_a(gh) = gha - a = gha - ga + ga - a = gd_a(h) + d_a(g)$$

so that d_a is a 1-cocycle for each a. It's easy to show $Z(G, A)$ is a group with the operation $(d + d')(g) = d(g) + d'(g)$. Furthermore $d_{a+b}(g) = g(a + b) - a + b = ga - a + gb - b = d_a(g) + d_b(g)$ so that $B(G, A)$ is a subgroup of $Z(G, A)$. Since A is abelian we know that $B(G, A)$ is normal in $Z(G, A)$.

Definition 4.7. In the group ring $\mathbb{Z}G$ we have the *augmentation map* $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ given by

$$\varepsilon\left(\sum_i n_i g_i\right) = \sum_i n_i.$$

This gives the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{I} \arrow[r, "\iota"] & \mathbb{Z}G \arrow[r, "\varepsilon"] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

where the kernel $\mathcal{I}$ is the *augmentation ideal of* $\mathbb{Z}G$.

Note that $\mathcal{I}$ is clearly generated by elements of the form $g - g_i$ with $g \neq g_i$. Multiplying by g_i^{-1} shows that it's equivalently generated by elements of the form $g - 1$ with $g \neq 1$.

For each $\varphi \in \operatorname{Hom}_{\mathbb{Z}G}(\mathcal{I}, A)$ we have an associated map $d_\varphi : G \to A$ where $d_\varphi(g) = \varphi(g - 1)$. Note that

$$\begin{aligned} d_\varphi(gh) = \varphi(gh - 1) &= \varphi(gh - g + g - 1) \\ &= \varphi(gh - g) + \varphi(g - 1) \\ &= g\varphi(h - 1) + \varphi(g - 1) \\ &= gd_\varphi(h) + d_\varphi(g) \end{aligned}$$

so that $d_\varphi \in Z(G, A)$.

We now give an important lemma which demonstrates the importance of the augmentation ideal.

Lemma 4.8. *Let $\Psi : \mathrm{Hom}_{\mathbb{Z}G}(\mathcal{I}, A) \to Z(G, A)$ be given by $\Psi(\varphi) = d_\varphi$. Then Ψ is an isomorphism.*

Proof. Let $\varphi, \psi \in \mathrm{Hom}_{\mathbb{Z}G}(\mathcal{I}, A)$. Then

$$\begin{aligned}\Psi(\varphi + \psi)(g) &= d_{\varphi+\psi}(g)\\ &= (\varphi + \psi)(g - 1)\\ &= \varphi(g - 1) + \psi(g - 1)\\ &= d_\varphi(g) + d_\psi(g)\\ &= \Psi(\varphi)(g) + \Psi(\psi)(g)\end{aligned}$$

so Ψ is a homomorphism. If $\Psi(\varphi)(g) = 0$ for all g, we must have $\varphi = 0$ since $\mathcal{I}$ is generated by elements $g - 1$ with $g \neq 1$. Thus Ψ is injective. Now suppose $d \in Z(G, A)$ and defined a function $\varphi(g-1) = d(g)$. We've shown that the elements $g - 1$ generate $\mathcal{I}$ so φ is now defined on $\mathcal{I}$. We need to check that φ is a $\mathbb{Z}G$-map so let $h \in G$. Then

$$\begin{aligned}\varphi(h(g - 1)) = \varphi(hg - h + 1 - 1) &= \varphi(hg - 1) - \varphi(h - 1)\\ &= d(gh) - d(h) = hd(g) = h\varphi(g - 1).\end{aligned}$$

Therefore $\varphi \in \mathrm{Hom}_{\mathbb{Z}G}(\mathcal{I}, A)$ and $\Psi(\varphi) = d$ so Ψ is surjective and thus an isomorphism. □

The next result gives an explicit description of $H^1(G, A)$, as was promised earlier. Incidentally, this theorem shows that the group cohomology can be described in terms of cocycles and coboundaries in a similar fashion to the singular cohomology of topological spaces. While this result only gives a description of $H^1(G, A)$, it's possible to give similar descriptions of $H^i(G, A)$ so that this theorem is only a special case.

Theorem 4.9. *We have $H^1(G, A) \cong Z(G, A)/B(G, A)$.*

Proof. We start with the short exact augmentation sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{I} \arrow[r, "\iota"] & \mathbb{Z}G \arrow[r, "\varepsilon"] & \mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

and note that by Theorems 2.4 and 3.2 we have a long exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, A) \arrow[r] & \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \arrow[r, "\Phi"] & \mathrm{Hom}_{\mathbb{Z}G}(\mathcal{I}, A) \arrow[r] & \mathrm{Ext}^1_{\mathbb{Z}G}(\mathbb{Z}, A) \arrow[r] & 0. \end{tikzcd}$$

Using Lemma 4.3, Lemma 4.8 and Corollary 4.5 this sequence reduces to

$$\begin{tikzcd} 0 \arrow[r] & A^G \arrow[r] & \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A) \arrow[r, "\Phi"] & Z(G, A) \arrow[r] & H^1(G, A) \arrow[r] & 0. \end{tikzcd}$$

Let $\varphi \in \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}G, A)$ and note that $\Phi(\varphi) = \varphi\iota$. Thus, using the correspondence from Lemma 4.8, $\Phi(\varphi)(g-1) = \varphi(g-1) = d_\varphi(g)$ and $\Phi(\varphi) = d_\varphi$. Hence the image of Φ in $Z(G, A)$ is simply $B(G, A)$ and it follows from exactness that $H^1(G, A) \cong Z(G, A)/B(G, A)$. □

We will often be concerned with the case that G acts trivially on a G-module. In this case Theorem 4.9 reduces to a convenient and familiar form.

Corollary 4.10. *If G acts trivially on A then*

$$H^1(G,A) \cong Z(G,A) = \mathrm{Hom}_{\mathbf{Grp}}(G,A).$$

Proof. If G acts trivially on A then for for each $a \in A$ we have $ga = a$. Thus $d_a(g) = ga - a = 0$ so all 0-coboundaries are trivial and $H^1(G,A) \cong Z(G,A)/B(G,A) = Z(G,A)$. For the second equality note that under a trivial action a 1-cocycle is simply a map $d : G \to A$ such that $d(gh) = d(g) + d(h)$. Thus these maps are simply the group homomorphisms from G to A. □

5. Kummer Theory

At this point we've developed the necessary background to begin discussing Kummer theory. We will concern ourselves with a field K and finite, abelian extensions L/K with Galois groups $G = \mathrm{Gal}(L/K)$. The field K will be required to contain the n^{th} roots of unity. Our goal is to use group cohomology to classify the possibilities for L given these conditions on K.

Lemma 5.1. *Let L/K be a finite Galois extension. Let $\overline{L}$ be an algebraic closure of L and let $G = \mathrm{Hom}(L, \overline{L})$ be the vector space over L of field homomorphisms $L \to \overline{L}$. Then distinct elements of G are linearly independent over L.*

Proof. Let $S = \{\sigma_1, \ldots, \sigma_n\}$ be a set of distinct elements of G. Suppose that S is linearly dependent over L. Considering the set of all linear dependence relations choose one with the minimal number m of nonzero coefficients a_i so that we have

$$\sum_{i=1}^{m} a_i \sigma_i = 0. \tag{1}$$

Note this holds for any element $x \in L$. We know (perhaps after reordering) that there is some $x_0 \in L$ with $\sigma_1(x_0) \neq \sigma_m(x_0)$ since the σ_i are distinct. Now, by (1) we have

$$\sum_{i=1}^{m} a_i \sigma_i(x x_0) = \sum_{i=1}^{m} a_i \sigma_i(x)\sigma_i(x_0) = 0. \tag{2}$$

If we put x into (1), multiply through by $\sigma_m(x_0)$ and subtract from (2) we obtain

$$\sum_{i=1}^{m-1} (\sigma_m(x_0) - \sigma_i(x_0)) a_i \sigma_i(x) = 0$$

which holds for all $x \in L$. Since the first coefficient is nonzero, we've obtained a dependence relation with fewer than m nonzero coefficients, a contradiction. Thus S must be linearly independent over L. □

The following theorem is known in literature as Hilbert's Theorem 90. The statement given in the introduction can be seen as a special case of this theorem by comparing the two proofs, which are very similar. The more general result that is Theorem 5.2 can be attributed to Emmy Noether while the result in §1 was originally due to Kummer.

Theorem 5.2 (Hilbert's Theorem 90)**.** *Let L/K be a finite Galois extension with Galois group G. Then $H^1(G, L^\times) = 0$.*

Proof. Let $\varphi : G \to L^\times$ be a 1-cocyle. Note that since $L^\times$ is multiplicative this means $\varphi(\sigma\tau) = \sigma(\varphi(\tau)) \cdot \varphi(\sigma)$ for each $\sigma, \tau \in G$, where we've used $\cdot$ to denote multiplication in $L^\times$. Given $\sigma \in G$ we wish to find $c \in L^\times$ so that $\varphi(\sigma) = \sigma(c)/c$. In this way, φ is a 0-coboundary so that $Z(G, L^\times) = B(G, L^\times)$.

Note $\{\varphi(\sigma)\cdot\sigma \mid \sigma \in G\}$ is a subset of distinct elements of G. Thus by Lemma 5.1 there exists $a \in L^\times$ such that

$$b = \sum_{\sigma \in G} \varphi(\sigma) \cdot \sigma(a)$$

is nonzero. Recall that left multiplication by a fixed element permutes the elements of G. Then given arbitrary $\tau \in G$ and using the fact that φ is a 1-cocyle we have

$$\begin{aligned} \tau(b) = \sum_{\sigma \in G} \tau(\varphi(\sigma)) \cdot \tau\sigma(a) &= \sum_{\sigma \in G} \tau(\tau^{-1}(\varphi(\tau\sigma) \cdot \varphi(\tau)^{-1})) \cdot \tau\sigma(a) \\ &= \sum_{\sigma \in G} \varphi(\tau)^{-1} \cdot \varphi(\tau\sigma) \cdot \tau\sigma(a) = \varphi(\tau)^{-1} b. \end{aligned}$$

This gives $\varphi(\tau) = b/\tau(b) = \tau(b^{-1})/b^{-1}$. We can then take b^{-1} to be our desired c so that φ is a 0-coboundary. Thus $Z(G, L^\times) = B(G, L^\times)$ and $H^1(G, L^\times) = 0$ using Theorem 4.9. □

Suppose now that L/K is an extension with infinite Galois group G and A is a G-module. In this case, G is a topological group whose basic open sets are those subgroups $H \leq G$ which have finite index in G. We can define the cohomology groups of G with coefficients in A as

$$H^i(G, A) = \varinjlim H^i(G/H, A^H)$$

Where H runs through all open normal subgroups of G. This leads to the following corollary.

Corollary 5.3. *Let L/K be an infinite extension with Galois group G. Then $H^1(G, L^\times) = 0$.*

Proof. Let H be an open normal subgroup of G. Then note that G/H is the Galois group of some finite extension L_H/K. Furthermore, L^H is the fixed field for the subgroup H, so $L^H = L_H$ by the Fundamental Theorem of Galois Theory. But by Theorem 5.2 we have $H^1(G/H, L_H^\times) = 0$. Since this is trivial for each open normal subgroup H, the direct limit must also be trivial and we have $H^1(G, L^\times) = 0$. □

We now arrive at a fundamental result in Kummer theory. Let μ_n denote the multiplicative group of n^{th} roots of unity in a field K. Recall that μ_n is cyclic of order n. Let $(K^\times)^n$ denote the n^{th} powers of $K^\times$.

Theorem 5.4. *Let L/K be a finite Galois extension with Galois group G and suppose $\mu_n \subseteq K$. Then $(K^\times \cap (L^\times)^n)/(K^\times)^n \cong \operatorname{Hom}(G, \mu_n)$.*

Proof. We have the following short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mu_n \arrow[r] & L^\times \arrow[r, "n"] & (L^\times)^n \arrow[r] & 0 \end{tikzcd}$$

where the map $L^\times \xrightarrow{n} (L^\times)^n$ is the n^{th} power map. This gives the long exact group cohomology sequence

$$\begin{tikzcd} 0 \arrow[r] & \mu_n^G \arrow[r] & (L^\times)^G \arrow[r, "n"] & ((L^\times)^n)^G \arrow[r] & H^1(G, \mu_n) \arrow[r] & H^1(G, L^\times) \arrow[r] & \cdots . \end{tikzcd}$$

Now K is the fixed field of L under G so $\mu_n^G = \mu_n$, $(L^\times)^G = K^\times$ and $((L^\times)^n)^G = K^\times \cap (L^\times)^n$. Since μ_n is contained in the fixed field of G, G has trivial action on these elements. Hence $H^1(G, \mu_n) \cong \mathrm{Hom}(G, \mu_n)$ by Corollary 4.10. Finally, $H^1(G, L^\times) = 0$ by Theorem 5.2. Thus the above sequence reduces to

$$\begin{tikzcd}0 \arrow[r] & \mu_n \arrow[r] & K^\times \arrow[r, "n"] & K^\times \cap (L^\times)^n \arrow[r] & \mathrm{Hom}(G, \mu_n) \arrow[r] & 0.\end{tikzcd}$$

This gives the isomorphism $(K^\times \cap (L^\times)^n)/(K^\times)^n \cong \mathrm{Hom}(G, \mu_n)$. □

Corollary 5.5. *If $\overline{K}$ is an algebraic closure of K and $G = \mathrm{Gal}(\overline{K}/K)$ then $K^\times/(K^\times)^n \cong \mathrm{Hom}(G, \mu_n)$.*

Proof. Since $\overline{K}$ is algebraically closed, the n^{th} power map is surjective. Thus

$$K^\times \cap (\overline{K}^\times)^n = K^\times.$$

Making this substitution in Theorem 5.4 gives the desired result. □

Fix an algebraic closure $\overline{K}$ and set $G = \mathrm{Gal}(\overline{K}/K)$. Suppose that $\varphi \in \mathrm{Hom}(G, \mu_n)$ is a homomorphism from the Galois group G to μ_n. Then $\ker \varphi$ is an open normal subgroup of G, so by Galois theory it corresponds to a Galois extension L_φ/K. Furthermore $\mathrm{Gal}(L_\varphi/K) \cong \mathrm{im}\,\varphi \subseteq \mu_n$ so L_φ must be a cyclic extension of K with degree d where $d \mid n$ and d is the order of φ in G. If m is relatively prime to d then φ^m has the same kernel as φ, so these two homomorphisms define the same extension L_φ.

Conversely, given a cyclic extension L/K of degree d with $d \mid n$, we get a set of such elements in $\mathrm{Hom}(G, \mu_n)$. Namely, these are the set of elements which are trivial on $\mathrm{Gal}(\overline{K}/L)$ which also map a generator of $\mathrm{Gal}(L/K)$ to an element of order d in μ_n. In this way we have a bijection between the cyclic subgroups of order dividing n of $\mathrm{Hom}(G, \mu_n) \cong K^\times/(K^\times)^n$ and the cyclic extensions of K of degree dividing n. We summarize this correspondence in the following theorem.

Theorem 5.6. *There is a bijective correspondence between the cyclic subgroups of $K^\times/(K^\times)^n$ and cyclic extensions L/K.*

This correspondence can be taken one step further. Recall that a group G has *exponent* n if for each $\sigma \in G$ we have $\sigma^n = 1$. We say that a field extension has exponent n if its Galois group has exponent n. Suppose that L/K is a finite abelian extension with exponent d where $d \mid n$. Then from the Fundamental Theorem of Finitely Generated Abelian Groups we know $\mathrm{Gal}(L/K) = G_1 \times \cdots \times G_m$ where each G_i is cyclic with order d_i and $d_i \mid n$. Let L_i be the fixed field for $G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_m$ so that $\mathrm{Gal}(L_i/K) = G_i$. So now we have m cyclic extensions, which by the proof of Theorem 5.6 correspond to m elements $\varphi_1, \ldots \varphi_m \in \mathrm{Hom}(G, \mu_n)$ each of which has kernel $\mathrm{Gal}(\overline{K}/L_i)$. Each φ_i corresponds to a cyclic subgroup of $K^\times/(K^\times)^n$ of order d_i. Let $\varphi = \varphi_1 \times \cdots \times \varphi_m$ and note that $\varphi \in \mathrm{Hom}(G, \mu_n)$ with kernel $\mathrm{Gal}(\overline{K}/L)$. Then φ corresponds to a subgroup of $K^\times/(K^\times)^n$ with exponent n.

Conversely, given any finitely generated subgroup $H \subseteq K^\times/(K^\times)^n$ of exponent n we can write $H = H_1 \times \cdots \times H_m$ with each H_i cyclic of order d_i. Then each of these cyclic subgroups corresponds to some $\varphi_i \in \mathrm{Hom}(G, \mu_n)$ with order d_i. Now, as above, each φ_i corresponds to a cyclic Galois extension L_i with cyclic Galois group $G_i \cong \mathrm{im}\,\varphi_i$ of order d_i. Taking the product $G_1 \times \cdots \times G_m$ gives a Galois group for the composite extension $L = L_1L_2 \dots L_m$. Note that $\mathrm{Gal}(L/K)$ is a finite abelian group of exponent n. This proves the following stronger correspondence.

Corollary 5.7. *There is a bijective correspondence between finite abelian subgroups of $K^\times/(K^\times)^n$ of exponent n and finite abelian extensions L/K of exponent n.*

Finally, the isomorphism in Theorem 5.4 can be made explicit using the connecting homomorphism from Theorem 2.4, which traces itself back to the Snake Lemma. In particular, given $\alpha \in K^\times$ and $\sigma \in G$ there is $\beta \in L^\times$ such that $\beta^n = \alpha$. Then the homomorphism

$$\varphi : \sigma \mapsto \frac{\sigma(\beta)}{\beta}$$

is the element of $H^1(G, \mu_n) \cong \mathrm{Hom}(G, \mu_n)$ which is the image of α under the connecting homomorphism.

Since $\sigma(\beta)/\beta \in \mu_n$, the map φ depends only on the smallest positive integer d such that $\beta^d \in K$. Suppose that we choose two different values β and β' with $\beta^n = \beta'^n = \alpha$ and $\beta^d, \beta'^{d'} \in K$. Without loss of generality, take $d \leq d'$. Then $(\beta/\beta')^n = \alpha/\alpha = 1$ so that $\beta/\beta' \in \mu_n$ and is thus an element of K. Then $(\beta/\beta')^d = \beta^d/\beta'^d$ is in K as well, which means $\beta'^d \in K$. Because of the minimality of d', this shows that we must have $d = d'$. Therefore, if we choose different preimages of α, the resulting map φ still has the same image in μ_n.

Note that if we write β as $\sqrt[n]{\alpha}$ then $\ker \varphi$ is a subgroup of G which has fixed field $K(\sqrt[n]{\alpha})$. By the remarks above and the proofs of Theorem 5.6 and Corollary 5.7 we are able to conclude that when K contains the n^{th} roots of unity, an extension L/K is Galois with a cyclic Galois group of order $d \mid n$ if and only if $L = K(\sqrt[n]{\alpha})$ for some $\alpha \in K^\times$ and is Galois with exponent $d \mid n$ if and only if $L = K(\sqrt[n]{\alpha_1}, \dots, \sqrt[n]{\alpha_n})$ for some $\alpha_1, \dots, \alpha_n \in K^\times$.

6. Conclusion

The first ideas involving group cohomology were developed in other forms over a century ago. Hilbert's Theorem 90 from 1897 is generally considered to be the first result in the subject. The notation we use today, which mimics cohomology in topology, was developed in the 1940s. Group cohomology is a far reaching subject which has many applications in topology, algebraic number theory and class field theory. In particular, there are many connections between group cohomology and the cohomology of topological spaces, especially in the idea that cohomology also measures "how far" a sequence is from being exact.

Ernst Kummer originally developed the foundations of Kummer theory in his work on Fermat's Last Theorem. This was done in the 1840s, long before the concept of cohomology and when Galois theory was in its infancy. The subject is related to Fermat's Last Theorem through algebraic number theory through consideration of specific fields and their ideal class groups. Kummer's work is important because the results essentially don't depend on the nature of the field in question. Instead, we get general, far-reaching theorems describing abelian extensions of a field with few initial conditions.

Kummer theory provides a good classification for extensions of fields which contain the n^{th} roots of unity. In the case that a field doesn't contain the n^{th} roots of unity, the problem is much more difficult, and is a question answered by class field theory. In some ways Kummer theory is a first step into this subject, which attempts to classify abelian extensions of arbitrary fields.

Acknowledgements. I'd like to thank my mentor, Preston Wake, for helping me immensely on this paper. He did a great job of taking what I already knew and showing me how I could expand upon that knowledge.

References

[1] D. Dummit, R. Foote, *Abstract Algebra, 3rd Edition,* (Hoboken, New Jersey: John Wiley and Sons, Inc., 2004).

[2] P. Hilton, J. Stammbach, *A Course in Homological Algebra,* (New York, New York: Springer-Verlag, 1971).

[3] J.S. Milne, *Class Field Theory Notes,* (2008).

[4] C. Weibel, *An Introduction to Homological Algebra,* (New York, New York: Cambridge University Press, 1994).