Galois Cohomology and Kummer Theory

Bryce Goldman, Austin Lei, and Chris Randall

May 2021

1 Introduction

If K is a field with characteristic not dividing n and $K(\sqrt[n]{a})/K$ is a Galois extension of degree n, then we can show that the Galois group $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ as follows. Note that a K-automorphism of $K(\sqrt[n]{a})$ is uniquely determined by where it sends $\sqrt[n]{a}$, and that the Galois conjugates of $\sqrt[n]{a}$ are the roots $\sqrt[n]{a}, \zeta\sqrt[n]{a}, \ldots, \zeta^{n-1}\sqrt[n]{a}$ of $x^n - a$, where ζ is a primitive n^{th} root of unity. Since each of the maps $\sqrt[n]{a} \mapsto \zeta^k\sqrt[n]{a}$ is a K-automorphism, the Galois group consists of exactly these maps, and so is isomorphic to the group of n^{th} roots of unity, which is itself isomorphic to $\mathbb{Z}/n\mathbb{Z}$, as it is generated by ζ.

A natural question is whether the converse of this is also true; if L/K is a Galois extension with Galois group $\mathbb{Z}/n\mathbb{Z}$, does there exist some $a \in K$ such that $L = K(\sqrt[n]{a})$? In general the answer is no, as demonstrated by the following counterexample:

Let $K = \mathbb{Q}$ and L be the splitting field of $p(x) = x^3 - 7x + 7$. This polynomial is irreducible by Eisenstein's criterion and visibly has three distinct real roots. Thus, since any splitting field of an irreducible polynomial over a characteristic 0 field is a Galois extension of that field, L/K is Galois. Moreover, by simple computation the discriminant of $p(x)$ is 49, a rational square, so the Galois group is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Now, since all the roots of $p(x)$ are real, $L \subseteq \mathbb{R}$. Suppose that $L = \mathbb{Q}(\sqrt[3]{a})$ for some $a \in \mathbb{Q}$. Then we must take $\sqrt[3]{a}$ to be the real cube root of a, whose Galois conjugates are $\sqrt[3]{a}, \zeta\sqrt[3]{a}, \zeta^2\sqrt[3]{a}$, where ζ is a primitive cube root of unity. In particular, ζ is not real, and hence neither are the conjugates of $\sqrt[3]{a}$. But L is Galois (i.e. normal), so it must contain each root of the minimal polynomial of $\sqrt[3]{a}$, which implies that $L \not\subseteq \mathbb{R}$, a contradiction.

Generalizing this example, we can find two explicit obstructions to our extension having this form. First, if K has characteristic dividing n, then $x^n - a$ has at most one root in any extension of K, so $K(\sqrt[n]{a})/K$ cannot be separable. The other obstruction is more subtle: if K does not contain a primitive n^{th} root of unity then $K(\sqrt[n]{a})/K$ need not be a Galois extension of order n. However, we will be able to show that these are the only obstructions, by proving the following theorem:

Theorem 1.1. *Let L/K be a Galois extension with Galois group isomorphic to $\mathbb{Z}/n\mathbb{Z}$, and suppose K has characteristic not dividing n and contains a primitive n^{th} root of unity, then $L = K(\sqrt[n]{a})$ for some $a \in K$.*

2 Group Cohomology

We will need to build the tool of group cohomology in order to prove the main result. Given a group G, a G-module is an abelian group A, equipped with a linear action by G. Similarly, a G-equivariant map between G-modules A and B is a $\mathbb{Z}[G]$-linear map, or equivalently a $\mathbb{Z}$-linear map φ such that for any $g \in G$,

$$g \cdot \varphi(x) = \varphi(g \cdot x)$$

The category G-**mod** whose objects are G-modules and morphisms are given by G-equivariant maps is then canonically isomorphic to $\mathbb{Z}$[G]-**mod**, the category of (ring-theoretic) $\mathbb{Z}[G]$-modules, and thus is an abelian category with enough injectives (by exercise 2.3.5 of [1]). In light of this isomorphism, we will refer to $\mathbb{Z}[G]$-modules simply as G-modules.

Definition 2.1. *If A is a G-module, then we can define a submodule*

$$A^G = \{a \in A : g \cdot a = a \text{ for all } g \in G\}$$

called the G-invariance of A.

In fact the map sending $A \mapsto A^G$ extends to a functor $F : G\text{-}\mathbf{mod} \to \mathbf{Ab}$, by sending a morphism $\lambda : A \to B$ to its restriction $\lambda|_{A^G}$. Note that for $a \in A^G$ we have

$$g \cdot \lambda(a) = \lambda(g \cdot a) = \lambda(a)$$

so $\lambda|_{A^G}$ is a morphism $A^G \to B^G$. Furthermore, as we will see shortly this functor is left exact, allowing us to define its right derived functors, which give us a notion of *group cohomology*:

Proposition 2.2. *The functor F is naturally isomorphic to the functor* $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -) : G\text{-}\mathbf{mod} \to \mathbf{Ab}$*, where $\mathbb{Z}$ is equipped with the trivial G-action.*

Proof. For each $\mathbb{Z}[G]$-module A, define

$$\varphi_A : \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) \to A^G$$

by

$$\varphi_A(f) = f(1)$$

First, we must check that φ_A is an isomorphism of abelian groups. It is well-defined, for if $g \in G$ and $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ then we have

$$g \cdot \varphi_A(f) = g \cdot f(1) = f(g \cdot 1) = f(1) = \varphi_A(f)$$

as $\mathbb{Z}$ is G-invariant by hypothesis, so $\varphi_A(f) \in A^G$. Moreover, φ_A is certainly a homomorphism, for by definition we have $(f + h)(n) = f(n) + h(n)$ for all $h \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ and all $n \in \mathbb{Z}$. Moreover, if $\varphi_A(f) = \varphi_A(g)$ then

$$f(n) = nf(1) = ng(1) = g(n)$$

so $f = g$, and hence φ_A is injective. Lastly, given $a \in A^G$ we can define $f_a : \mathbb{Z} \to A$ by

$$f_a(n) = na$$

Clearly f_a is a homomorphism of abelian groups, and furthermore if $g \in G$ then

$$f_a(g \cdot n) = f_a(n) = na = g \cdot (na) = g \cdot f_a(n)$$

since $a \in A^G$, and thus $na \in A^G$ as well. Hence f_a is G-equivariant, that is, $f_a \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$, and moreover

$$\varphi_A(f_a) = f_a(1) = a$$

so we conclude that φ_A is surjective. Therefore φ_A is an isomorphism, as desired.

It remains to be shown that the maps φ_A, taken over all $\mathbb{Z}[G]$-modules A, assemble into a natural transformation $\varphi : \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -) \Rightarrow F$. Fix $\mathbb{Z}[G]$-modules A and B, and suppose $\lambda : A \to B$ is a G-equivariant homomorphism. We must verify that the following diagram commutes:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A) & \xrightarrow{\lambda_*} & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, B) \\ \downarrow{\scriptstyle \varphi_A} & & \downarrow{\scriptstyle \varphi_B} \\ A^G & \xrightarrow[F\lambda]{} & B^G \end{array}$$

Let $f \in \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$. Then

$$F\lambda\varphi_A(f) = F\lambda(f(1)) = \lambda f(1) = (\lambda^*(f))(1) = \varphi_B\lambda^*(f)$$

so the diagram commutes. Therefore φ is a natural transformation, and since each of its components φ_A is an isomorphism we conclude that F and $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ are naturally isomorphic. □

We obtain the following as an immediate corollary of proposition 2.2:

Corollary 2.3. *F is left exact.*

Proof. F is naturally isomorphic to $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, which is left exact. □

Thus F has right derived functors, which we will denote by $\mathrm{H}^\bullet(G, -)$. Moreover, these derived functors have the following concrete interpretation:

Corollary 2.4. *For each G-module A we have*

$$A^G \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

and

$$\mathrm{H}^i(G, A) \cong \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

Proof. By definition $F(A) = A^G$, and F is naturally isomorphic to $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ by proposition 2.2, so the first claim is automatic. Moreover, $\mathrm{Ext}^\bullet_{\mathbb{Z}[G]}(\mathbb{Z}, -)$ are the right derived functors of $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, -)$, so for each nonnegative i we see that there is a natural isomorphism

$$\mathrm{H}^i(G, -) \cong \mathrm{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, -)$$

In particular, evaluating each functor on a given G-module A proves the second claim. □

3 The Bar Resolution

Throughout this section, we fix a group G and a G-module A. In order to assist in the computation of group cohomology, we will construct a cochain complex $C^\bullet(G, A)$ of $\mathbb{Z}[G]$-modules whose cohomology agrees with the group cohomology $H^\bullet(G, A)$, defined in section 2.

3.1 Construction of the Bar Resolution

First, we define G-modules F_n for each nonnegative integer n by

$$F_n = \bigotimes_{i=0}^{n} \mathbb{Z}[G] = \underbrace{\mathbb{Z}[G] \otimes \cdots \otimes \mathbb{Z}[G]}_{n+1 \text{ times}}$$

where each tensor product is taken over $\mathbb{Z}$. We further define an action of G on the simple tensors of F_n by

$$g \cdot (g_0 \otimes g_1 \otimes \cdots \otimes g_n) = (gg_0) \otimes g_1 \otimes \cdots \otimes g_n$$

for all $g, g_0, \ldots, g_n \in G$. Extending this map linearly to all of F_n turns it into a $\mathbb{Z}[G]$-module.

Proposition 3.1. *Each F_n is a free G-module, with a basis consisting of all simple tensors of the form*

$$1 \otimes g_1 \otimes \cdots \otimes g_n$$

where each $g_i \in G$.

Proof. For each nonnegative n, let M_n be the free G-module

$$M_n = \bigoplus_{v \in G^n} \mathbb{Z}[G]$$

and let e_v be the basis element of M_n whose $(g_1, \ldots, g_n)^{\text{th}}$ coordinate is 1 if $v = (g_1, \ldots, g_n)$ and 0 otherwise.

We proceed by induction on n. If $n = 0$ then by definition

$$F_0 = \mathbb{Z}[G]$$

which trivially has the element 1 as a basis over $\mathbb{Z}[G]$, and we are done. Now, let k be a nonnegative integer and suppose by induction that we have shown that F_k is free over $\mathbb{Z}[G]$ with basis

$$\{1 \otimes g_1 \otimes \cdots \otimes g_k : g_i \in G\}$$

Suppose further that $n = k + 1$. On the one hand, we can define $\psi : M_{k+1} \to F_k \otimes \mathbb{Z}[G]$ by extending

$$\psi(e_{(g_1,\ldots,g_{k+1})}) = (1 \otimes g_1 \otimes \cdots \otimes g_k) \otimes g_{k+1}$$

linearly to all of M_{k+1}. Conversely, for each $r = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$ (with each $a_g \in \mathbb{Z}$ and all but finitely many equal to zero) we define $\phi_r : F_k \to M_{k+1}$ by extending

$$\phi_r(1 \otimes g_1 \otimes \cdots \otimes g_k) = \sum_{g \in G} a_g e_{(g_1,\ldots,g_k,g)}$$

linearly to all of F_k. Each ϕ_r is well-defined, for $1 \otimes g_1 \otimes \cdots \otimes g_k$ form a basis.

Next, we define $\Phi : F_k \times \mathbb{Z}[G] \to M_{k+1}$ by

$$\Phi(x, r) = \phi_r(x)$$

for each $x \in F_k$ and $r \in \mathbb{Z}[G]$. This map is $\mathbb{Z}$-linear in the first coordinate by construction, as each ϕ_r is $\mathbb{Z}[G]$-linear. On the other hand, if $g, g', g_i \in G$ for $i = 1, \ldots, k$, then

$$\begin{aligned}\phi_{g+g'}(1 \otimes g_1 \otimes \cdots \otimes g_k) &= e_{(g_1,\ldots,g_k,g)} + e_{(g_1,\ldots,g_k,g')} \\ &= \phi_g(1 \otimes g_1 \otimes \cdots \otimes g_k) + \phi_{g'}(1 \otimes g_1 \otimes \cdots \otimes g_k)\end{aligned}$$

so Φ is $\mathbb{Z}$-linear in the second coordinate as well, as the elements of G form a basis for $\mathbb{Z}[G]$ as a free abelian group. Hence Φ induces an abelian group homomorphism

$$\varphi : F_k \otimes \mathbb{Z}[G] \to M_{k+1}$$

We claim that ψ and φ are inverses. If $v = (g_1, \ldots, g_{k+1}) \in G^{k+1}$ then we have

$$\varphi\psi(e_v) = \varphi((1 \otimes g_1 \otimes \cdots \otimes g_k) \otimes g_{k+1}) = e_v$$

so $\varphi\psi$ is the identity on a basis for M_{k+1}, and is thus the identity. On the other hand, by the $\mathbb{Z}[G]$-linearity of ψ we have

$$\psi\varphi((g_0 \otimes g_1 \otimes \cdots \otimes g_k) \otimes g_{k+1}) = \psi(g_0 e_v) = g_0((1 \otimes g_1 \otimes \cdots \otimes g_k) \otimes g_{k+1})$$

which is precisely

$$(g_0 \otimes g_1 \otimes \cdots \otimes g_k) \otimes g_{k+1}$$

so $\psi\varphi$ is the identity on all elements of this form. But these generate $F_k \otimes \mathbb{Z}[G]$ as an abelian group, so we conclude that by the $\mathbb{Z}$-bilinearity of the tensor product that $\psi\varphi$ is the identity on $F_k \otimes \mathbb{Z}[G]$. Therefore $F_k \otimes \mathbb{Z}[G]$ and M_{k+1} are isomorphic as G-modules, since ψ is a G-module homomorphism. Additionally, since F_{k+1} is naturally isomorphic to $F_k \otimes \mathbb{Z}[G]$ by associativity, we conclude that F_{k+1} is free over $\mathbb{Z}[G]$. Finally, we note that

$$\{1 \otimes g_1 \otimes \cdots \otimes g_{k+1} : g_i \in G\}$$

is a basis for F_{k+1}, since each such tensor is mapped to a basis element e_v of M_{k+1} by the natural isomorphism followed by ψ. □

Next, we wish to assemble the F_n into a free resolution $\mathcal{F}$ for $\mathbb{Z}$ (as before, equipped with the trivial action by G). To do this, we first define the *augmentation map* $\text{aug} : F_0 = \mathbb{Z}[G] \to \mathbb{Z}$ by

$$\text{aug}\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} a_g$$

Clearly this is an abelian group homomorphism, as addition in $\mathbb{Z}[G]$ is defined coordinate-wise, so

$$\text{aug}\left(\sum_{g\in G} a_g g + \sum_{g\in G} b_g g\right) = \text{aug}\left(\sum_{g\in G}(a_g+b_g)g\right) = \sum_{g\in G}(a_g+b_g)$$

and

$$\sum_{g\in G}(a_g+b_g) = \sum_{g\in G} a_g + \sum_{g\in G} b_g = \text{aug}\left(\sum_{g\in G} a_g g\right) + \text{aug}\left(\sum_{g\in G} b_g g\right)$$

Moreover, aug is G-equivariant: if $g_1, g_2 \in G$ then

$$g_1 \cdot \text{aug}(g_2) = g_1 \cdot 1 = 1 = \text{aug}(g_1 g_2)$$

since the action of G on $\mathbb{Z}$ is trivial, and aug is an abelian group homomorphism (so it suffices to show G-equivariance for each g_2, as we have just done). Finally, aug is clearly a surjection, for if $n \in \mathbb{Z}$ then $n \in \mathbb{Z}[G]$ as well, and thus $\text{aug}(n) = n$.

Taking aug to be our augmentation map $\mathcal{F} \to \mathbb{Z}$, we must now establish the maps within the complex. For each positive integer n we define the differentials $d_n : F_n \to F_{n-1}$ on the basis elements of F_n by

$$d_n(1 \otimes g_1 \otimes \cdots \otimes g_n) = g_1 \otimes \cdots \otimes g_n + \sum_{i=1}^{n-1}(-1)^i \otimes g_1 \otimes \cdots \otimes g_i g_{i+1} \otimes \cdots \otimes g_n + (-1)^n \otimes g_1 \otimes \cdots \otimes g_{n-1}$$

for $n \geq 2$, and define $d_1(1 \otimes g) = g - 1$. Extending these maps linearly to all of F_n yields G-equivariant homomorphisms, which we will subsequently show form a chain map on the F_n. While it is possible to show this is a chain map by direct computation, it is easier to instead demonstrate an isomorphism with a simpler complex.

For each n, define P_n to be the free $\mathbb{Z}$-module with basis $\{(g_0, \ldots, g_n) : g_i \in G\}$ and coordinatewise G-action

$$g \cdot (g_0, \ldots, g_n) = (gg_0, \ldots, gg_n)$$

Then we claim that the P_n form a chain complex $\mathcal{P}$, whose n^{th} differential is given by $\tilde{d}_n : P_n \to P_{n-1}$ by

$$(g_0, \ldots, g_n) \mapsto \sum_{i=0}^{n}(-1)^i(g_0, \ldots, \hat{g}_i, \ldots, g_n)$$

where $\hat{g}_i$ denotes deleting the i^{th} term. This map is G-equivariant, since

$$\begin{aligned}
\tilde{d}_n(g \cdot (g_0, \ldots, g_n)) &= \sum_{i=0}^{n}(-1)^i(gg_0, \ldots, \widehat{gg}_i, \ldots, gg_n) \\
&= g \cdot \sum_{i=0}^{n}(-1)^i(g_0, \ldots, \hat{g}_i, \ldots, g_n) \\
&= g \cdot \tilde{d}_n((g_0, \ldots, g_n))
\end{aligned}$$

Then we see that it is in fact a chain map, since

$$\begin{aligned}
\tilde{d}_{n-1}\tilde{d}_n((g_0, \ldots, g_n)) &= \sum_{i=0}^{n}(-1)^i \tilde{d}_{n-1}((g_0, \ldots, \hat{g}_i, \ldots, g_n)) \\
&= \sum_{i=1}^{n}\sum_{j=0}^{i-1}(-1)^{i+j}(g_0, \ldots, \hat{g}_j, \ldots, \hat{g}_i, \ldots, g_n) + \sum_{i=0}^{n-1}\sum_{j=i+1}^{n}(-1)^{i+j+1}(g_0, \ldots, \hat{g}_i, \ldots, \hat{g}_j, \ldots, g_n) \\
&= 0
\end{aligned}$$

Now we construct an isomorphism $\psi : F_n \to P_n$ defined by

$$g_0 \otimes \cdots \otimes g_n \mapsto (g_0, g_0g_1, \ldots, g_0 \cdots g_n)$$

which is G-equivariant since

$$\begin{aligned}\psi(g \cdot (g_0 \otimes \cdots \otimes g_n)) &= \psi((gg_0 \otimes \cdots \otimes g_n)) \\ &= (gg_0, gg_0g_1, \ldots, gg_0 \cdots g_n) \\ &= g \cdot (g_0, g_0g_1, \ldots, g_0 \cdots g_n) \\ &= g \cdot \psi((g_0 \otimes \cdots \otimes g_n))\end{aligned}$$

To see that this is an isomorphism, we construct its inverse $\varphi : P_n \to F_n$ defined by

$$(g_0, \ldots, g_n) \mapsto g_0 \otimes (g_0^{-1}g_1) \otimes \cdots \otimes (g_{n-1}^{-1}g_n)$$

then we verify

$$\begin{aligned}\psi\varphi((g_0, \ldots, g_n)) &= \psi(g_0 \otimes (g_0^{-1}g_1) \otimes \cdots \otimes (g_{n-1}^{-1}g_n)) \\ &= (g_0, g_0g_0^{-1}g_1, g_0g_0^{-1}g_1g_1^{-1}g_2, \ldots, g_0g_0^{-1} \cdots g_{n-1}g_{n-1}^{-1}g_n) \\ &= (g_0, \ldots, g_n)\end{aligned}$$

and

$$\begin{aligned}\varphi\psi(g_0 \otimes \cdots \otimes g_n) &= \varphi((g_0, g_0g_1, \ldots, g_0 \cdots g_n)) \\ &= g_0 \otimes (g_0^{-1}g_0g_1) \otimes \cdots \otimes ((g_0 \cdots g_{n-1})^{-1}g_0 \cdots g_n) \\ &= g_0 \otimes \cdots \otimes g_n\end{aligned}$$

Finally, we show that this isomorphism takes our proposed differential for F_n to the differential of P_n.

$$\begin{aligned}\psi d_n(g_0 \otimes \cdots \otimes g_n) &= g_0 \cdot (\psi(g_1 \otimes \cdots \otimes g_n) + \sum_{i=1}^{n-1}(-1)^i\psi(1 \otimes \cdots \otimes g_ig_{i+1} \otimes \cdots \otimes g_n) + (-1)^n\psi(1 \otimes \cdots \otimes g_{n-1})) \\ &= \sum_{i=0}^{n-1}(-1)^i\psi(g_0 \otimes \cdots \otimes g_ig_{i+1} \otimes \cdots \otimes g_n) + (-1)^n\psi(g_0 \otimes \cdots \otimes g_{n-1}) \\ &= \sum_{i=0}^{n-1}(-1)^i(g_0, g_0g_1, \ldots, g_0 \cdots g_{i-1}, g_0 \cdots g_{i+1}, \ldots, g_0 \cdots g_n) + (-1)^n(g_0, g_0g_1, \ldots, g_0 \cdots g_{n-1}) \\ &= \sum_{i=0}^{n}(-1)^i(g_0, g_0g_1, \ldots, \widehat{g_0 \cdots g_i}, \ldots, g_0 \cdots g_n) \\ &= \tilde{d}_n((g_0, g_0g_1, \ldots, g_0 \cdots g_n)) \\ &= \tilde{d}_n\psi(g_0 \otimes \cdots \otimes g_n)\end{aligned}$$

Thus the d_n form a chain map, and ψ is a chain isomorphism $\mathcal{F} \to \mathcal{P}$.

In fact, the isomorphism above tells us more; it will allow us to show that the $\mathcal{F}$ is indeed a resolution for $\mathbb{Z}$. Let $\mathcal{F}^*$ denote the augmented complex $\mathcal{F} \xrightarrow{\text{aug}} \mathbb{Z}$. Then since $F_0 = \mathbb{Z}[G] = P_0$ and ψ_0 is visibly the identity on $\mathbb{Z}[G]$, taking $\mathcal{P}^*$ to be the augmented complex $\mathcal{P} \xrightarrow{\text{aug}} \mathbb{Z}$ shows that ψ extends to an isomorphism $\mathcal{F}^* \to \mathcal{P}^*$. We will leverage the structure of $\mathcal{P}^*$ to show that it, and hence also $\mathcal{F}^*$, is exact.

For each positive integer n, define $s_n : P_{n-1} \to P_n$ by extending

$$s_n(g_0, \ldots, g_{n-1}) = (1, g_0, \ldots, g_{n-1})$$

linearly to all of P_{n-1}, and define $s_0 : \mathbb{Z} \to P_0$ by $s_0(m) = m$. We claim that the s_n form a chain contraction of the identity map on $\mathcal{P}$. Let $(g_0, \ldots, g_n) \in P_n$. Then

$$\begin{aligned} s_n \tilde{d}_n(g_0, \ldots, g_n) &= s_n \left(\sum_{i=0}^{n} (-1)^i (g_0, \ldots, \hat{g_i}, \ldots, g_n) \right) \\ &= \sum_{i=0}^{n} (-1)^i (1, g_0, \ldots, \hat{g_i}, \ldots, g_n) \end{aligned}$$

and on the other hand

$$\begin{aligned} \tilde{d}_{n+1} s_{n+1}(g_0, \ldots, g_n) &= \tilde{d}_{n+1}(1, g_0, \ldots, g_n) \\ &= \sum_{j=0}^{n+1} (-1)^j (1, g_0, \ldots, \hat{g_j}, \ldots, g_n) \end{aligned}$$

But each term of the second sum appears in the first one, except with the opposite sign, so we conclude that

$$(s_n \tilde{d}_n + \tilde{d}_{n+1} s_{n+1})(g_0, \ldots, g_n) = (-1)^0 (\hat{1}, g_0, \ldots, g_n) = (g_0, \ldots, g_n)$$

Therefore $s_n \tilde{d}_n + \tilde{d}_{n+1} s_{n+1}$ is the identity on P_n for each positive n. Similarly, if $n = 0$ then we have

$$s_0 \operatorname{aug}(g_0) + \tilde{d}_1 s_1(g_0) = s_0(1) + \tilde{d}_1(1, g_0) = 1 + g_0 - 1 = g_0$$

and if $n = -1$ then

$$\operatorname{aug} s_0(m) = \operatorname{aug}(m) = m$$

so the s_n form a chain contraction, as claimed. That is, the identity map on $\mathcal{P}^*$ is null homotopic, which implies that $\mathcal{P}^*$ is split exact (see [1], exercise 1.4.3). Thus by the chain isomorphism $\psi : \mathcal{P}^* \to \mathcal{F}^*$ we conclude that $\mathcal{F}^*$ is exact. Hence $\mathcal{F}$ is a free resolution for $\mathbb{Z}$. (Note: we will subsequently omit indices when there is no risk of ambiguity.)

Finally, we are ready to define the *Bar resolution*. Given the free resolution $\mathcal{F}$ for $\mathbb{Z}$ described above, we can tensor with the contravariant functor $\operatorname{Hom}_{\mathbb{Z}[G]}(-, A)$. This yields a cochain complex

$$\cdots \xleftarrow{d^*} \operatorname{Hom}_{\mathbb{Z}[G]}(F_2, A) \xleftarrow{d^*} \operatorname{Hom}_{\mathbb{Z}[G]}(F_1, A) \xleftarrow{d^*} \operatorname{Hom}_{\mathbb{Z}[G]}(F_0, A) \leftarrow 0$$

which, as suggested at the beginning of this section, we will denote by $C^\bullet(G, A)$. Since $\mathcal{F}$ is a free (i.e. projective) resolution for $\mathbb{Z}$, taking the i^{th} cohomology of $C^\bullet$ gives us

$$\mathrm{H}^i(C^\bullet(G, A)) = \operatorname{Ext}^i_{\mathbb{Z}[G]}(\mathbb{Z}, A) \cong \mathrm{H}^i(G, A)$$

by the definition of Ext and corollary 2.4. Thus the cohomology of $C^\bullet(G, A)$ is the same as the group cohomology $\mathrm{H}^\bullet(G, A)$, as desired.

3.2 Homology of the Bar Resolution

Why do we care specifically about the Bar resolution, as opposed to any other resolution for $\mathbb{Z}$? The following lemma will make explicit the potency of this particular complex.

Lemma 3.2. *For each nonnegative integer n, there is an isomorphism $\Lambda : C^n(G, A) \to \mathcal{W}_n$, where $\mathcal{W}_n$ denotes the G-module of functions $G^n \to A$, equipped with the G-module structure induced by that of A; that is,*

$$(g \cdot t)(x) = g \cdot t(x)$$

and

$$(t + l)(x) = t(x) + l(x)$$

for all $t, l \in \mathcal{W}_n$, $g \in G$, and $x \in G^n$.

Proof. Fix n, and let $f \in C^n(G, A) = \mathrm{Hom}_{\mathbb{Z}[G]}(F_n, A)$; that is, f is a homomorphism of G-modules $F_n \to A$. Then we define

$$\begin{aligned} \Lambda(f) : G^n &\to A \\ (g_1, \ldots, g_n) &\mapsto f(1 \otimes g_1 \otimes \cdots \otimes g_n) \end{aligned}$$

Then Λ is an abelian group homomorphism, for if $h \in C^n(G, A)$ then

$$\Lambda(f+h)(g_1, \ldots, g_n) = (f+h)(x) = f(x) + h(x) = \Lambda(f)(g_1, \ldots, g_n) + \Lambda(h)(g_1, \ldots, g_n)$$

where $x = 1 \otimes g_1 \otimes \cdots \otimes g_n$, and if $g \in G$ then

$$(g \cdot \Lambda(f))(g_1, \ldots, g_n) = g \cdot f(x) = (g \cdot f)(x) = \Lambda(g \cdot f)(g_1, \ldots, g_n)$$

so Λ is $\mathbb{Z}[G]$-linear.

To see that Λ is injective, we note that if

$$\Lambda(f) = \Lambda(h)$$

then by proposition 3.1 f and h agree on a basis for the free G-module F_n, and thus are equal. On the other hand, if $t : G^n \to A$ is a function then we can define $f_t \in C^n(G, A)$ by extending

$$f_t(1 \otimes g_1 \otimes \cdots \otimes g_n) = t(g_1, \ldots, g_n)$$

linearly (which is well-defined, since we have defined f_t on a basis for F_n by proposition 3.1). By construction we have

$$\Lambda(f_t)(g_1, \ldots, g_n) = t(g_1, \ldots, g_n)$$

so $\Lambda(f_t) = t$, and hence Λ is surjective. Therefore Λ is an isomorphism of G-modules, as claimed. □

Using lemma 3.2, we can turn the $\mathcal{W}_n$ into a cochain complex $\mathcal{W}$ isomorphic to $C^\bullet(G, A)$, by simply taking the n^{th} differential $d' : \mathcal{W}_n \to \mathcal{W}_{n+1}$ to be

$$d' = \Lambda d^* \Lambda^{-1}$$

where d^* is the n^{th} differential of $C^\bullet(G, A)$. This will prove particularly useful for understanding the first group cohomology $\mathrm{H}^1(G, A)$, as we will see shortly. First, we make the following definitions:

Definition 3.3. *A function $t : G \to A$ is a* crossed homomorphism *if*

$$t(g_1 g_2) = g_1 \cdot t(g_2) + t(g_1)$$

for each $g_1, g_2 \in G$. Moreover, a crossed homomorphism t is generated by $a \in A$ *if*

$$t(g) = g \cdot a - a$$

Such a function is clearly a crossed homomorphism, for

$$t(g_1 g_2) = (g_1 g_2) \cdot a - a = g_1 \cdot (g_2 \cdot a) - g_1 \cdot a + g_1 \cdot a - a = g_1 \cdot t(g_2) + t(g_1)$$

If such an a exists then t is said to be a principal crossed homomorphism.

We then have the following theorem, which gives us a concrete perspective on the degree one cohomology of $\mathcal{W}$, and hence of the first group cohomology $\mathrm{H}^1(G, A)$:

Theorem 3.4. *The cocycles of $\mathcal{W}$ in degree one are precisely the crossed homomorphisms $G \to A$, and the coboundaries are precisely the principal crossed homomorphisms.*

Proof. Let $t : G \to A$ be some element of $\mathcal{W}_1$, and let $f_t = \Lambda^{-1}(t) : F_1 \to A$. Then we have

$$d'(t) = (\Lambda d^*)(f_t) = \Lambda(f_t d)$$

so that

$$d'(t)(g_1, g_2) = \Lambda(f_t d)(g_1, g_2) = f_t d(1 \otimes g_1 \otimes g_2)$$

But

$$d(1 \otimes g_1 \otimes g_2) = g_1 \otimes g_2 - 1 \otimes g_1 g_2 + 1 \otimes g_1) = g_1 \cdot (1 \otimes g_2) - 1 \otimes g_1 g_2 + 1 \otimes g_1)$$

so we have

$$d'(t)(g_1, g_2) = g_1 \cdot f_t(1 \otimes g_2) - f_t(1 \otimes g_1 g_2) + f_t(1 \otimes g_1) = g_1 \cdot t(g_2) - t(g_1 g_2) + t(g_1)$$

Now, t is a cocycle if and only if $d'(t) = 0$, that is, if and only if

$$g_1 \cdot t(g_2) - t(g_1 g_2) + t(g_1) = d'(t)(g_1, g_2) = 0$$

for all $g_1, g_2 \in G$. Rearranging terms yields

$$t(g_1 g_2) = g_1 \cdot t(g_2) + t(g_1)$$

so we conclude that t is a cocycle if and only if t is a crossed homomorphism.

Now, suppose $l : 1 \to A$ is an element of $\mathcal{W}_0$, and let $h_l = \lambda^{-1}(l) : \mathbb{Z}[G] \to A$. Then we have

$$d'(l) = (\Lambda d^*)(h_l) = \Lambda(h_l d)$$

so that

$$d'(l)(g) = \Lambda(h_l d)(g) = h_l d(1 \otimes g) = h_l(g - 1) = g \cdot h_l(1) - h_l(1)$$

for each $g \in G$. Thus, $d'(l)$ is generated by $h_l(1) \in A$, so each coboundary is a principal crossed homomorphism. On the other hand, given a principal crossed homomorphism $k : G \to A$ generated by some $a_0 \in A$, define $k_0 : 1 \to A$ by $k_0(1) = a_0$. Then we have

$$\Lambda^{-1}(k_0)(1) = k_0(1) = a_0$$

so by the computation above

$$d'(k_0)(g) = g \cdot a_0 - a_0 = k(g)$$

for all $g \in G$, and thus k is a coboundary, completing the proof. □

Corollary 3.5. *The first group cohomology* $\mathrm{H}^1(G, A)$ *is isomorphic to the quotient of the crossed homomorphisms* $G \to A$ *by the principal crossed homomorphisms.*

Proof. Immediate from theorem 3.4, together with the isomorphism of cochain complexes $\mathcal{W} \cong C^\bullet(G, A)$ and the proof above that

$$\mathrm{H}^i(C^\bullet(G, A)) \cong \mathrm{H}^i(G, A)$$

□

As we will see in section 4, this interpretation of the first group cohomology is a powerful tool, which will help us prove the main result. Finally, we have the following:

Corollary 3.6. *If* A *is invariant under* G *(i.e.* $A^G = A$*) then* Λ *is an isomorphism between* $\mathrm{H}^1(G, A)$ *and the group of homomorphisms* $G \to A$*.*

Proof. Let $t : G \to A$ be a crossed homomorphism, and let $g_1, g_2 \in G$. Then we have

$$t(g_1 g_2) = g_1 \cdot t(g_2) + t(g_1) = t(g_1) + t(g_2)$$

as $t(g_2)$ is invariant under g_1, and thus t is a group homomorphism. The converse follows from an identical argument, so we conclude that the group of crossed homomorphisms $G \to A$ is the same as $\mathcal{W}_1$, the group of homomorphisms $G \to A$.

Similarly, if $l : G \to A$ is a principal crossed homomorphism generated by $a \in A$, then for each $g \in G$ we have

$$l(g) = g \cdot a - a = a - a = 0$$

as a is invariant under g, and thus the only principal crossed homomorphism $G \to A$ is the zero map. Hence, by corollary 3.5 we conclude that $\mathrm{H}^1(G, A) = \mathcal{W}_1$ is isomorphic to the group of homomorphisms $G \to A$ via Λ. □

3.3 Profinite Group Cohomology

It turns out that this definition of group cohomology is not well behaved for infinite groups. In general, this deficiency is quite hard to fix, but in the case of profinite groups we can take motivation from infinite Galois theory. If L/K is an algebraic Galois extension, then we can write its Galois group $G = \mathrm{Gal}(L/K)$ as an inverse limit

$$G = \varprojlim_{M} \mathrm{Gal}(M/K)$$

over all its finite Galois subextensions M/K. This makes G into a profinite group, and so it can then be given the *Krull topology*: the coarsest topology making each of the maps $G \to \mathrm{Gal}(M/K)$ continuous, where $\mathrm{Gal}(M/K)$ is given the discrete topology. This topology then allows us to extend the Galois correspondence to infinite extensions. Namely, if L/K is an algebraic Galois extension, then the usual bijection of the Galois correspondence gives us a bijection between the subextensions of L/K and the closed subgroups of G. The details of this can be found in the Infinite Galois Theory section of the Stacks Project [2]. We then want to be able to define Galois cohomology—the cohomology of G-modules where G is the Galois group of an algebraic extension—to reflect this profinite structure. The failure of standard group cohomology to respect the profinite structure of G can be reduced to the fact that

$$\mathrm{H}^n(G, A) = \varinjlim_{N} \mathrm{H}^n(G/N, A^N)$$

does not hold in general, where N ranges over all open normal subgroups of G. Motivated by this, we define a modified group cohomology for profinite groups:

Definition 3.7. *If G is a profinite group and A is a discrete G-module, then the continuous group cohomology is given by*

$$\hat{\mathrm{H}}^n(G, A) = \mathrm{H}^n(\hat{C}^\bullet(G, A))$$

where $\hat{C}^i(G, A)$ denotes the continuous homomorphisms $F_n \to A$, with F_n as in section 3.1.

Note that this turns out to be the right derived functor of our invariance functor $F : A \mapsto A^G$, viewed as a functor from a certain modified module category (see [3] for details). In particular, since this is a derived functor we get the usual long exact sequence. More to the point, we get the property that motivated our definition:

$$\hat{\mathrm{H}}^n(G, A) = \varinjlim_{N} \hat{\mathrm{H}}^n(G/N, A^N)$$

where N ranges over all open normal subgroups of G. In the next section, as is customary in Galois theory, we will refer to the continuous group cohomology simply as group cohomology and in the finite case ignore topological details, as in that case the continuous cohomology coincides with the standard group cohomology (i.e. finite groups are given the discrete topology).

4 The Kummer Sequence

Finally, we can apply the machinery of group cohomology to prove the main theorem. If L/K is a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, then we have some natural examples of G-modules. Namely,

the additive group L and multiplicative group $L^\times$ are both G-modules via the action $\sigma \cdot x = \sigma(x)$ for $\sigma \in G$. Then K and $K^\times$ have trivial G-action and so in particular are G-modules. Finally, we can define a submodule of $L^\times$ given by

$$\mu_n(L) = \{x \in L^\times : x^n = 1\}$$

We note that $\mu_n(L)$ is closed under the action of G, since for any $\sigma \in G$ and any $x \in \mu_n(L)$,

$$\sigma(x)^n = \sigma(x^n) = \sigma(1) = 1$$

so $\sigma(x) \in \mu_n(L)$, and thus $\mu_n(L)$ is a G-module.

We can now compute the invariance of each of these modules. Since our extension is not necessarily finite, we need to use the infinite Galois correspondence (see [2], theorem 9.22.4) for this, viewing G with the Krull topology. In particular, since G is closed in itself, $L^G = K$, and since G acts on $L^\times$ in the same way, $(L^\times)^G = K^\times$. Then, since the invariance of a submodule is just its intersection with the invariance of the full module,

$$\mu_n(L)^G = \mu_n(L) \cap K = \mu_n(K)$$

Let K be a field containing a primitive root of unity, and n be an integer relatively prime to the characteristic of K. If $\overline{K}$ is the separable closure of K (the largest separable subextension of an algebraic closure), then $\overline{K}/K$ is Galois and we denote its Galois group by Γ_K. Then, the Γ_K modules discussed above fit into an exact sequence called the Kummer sequence

$$1 \to \mu_n(\overline{K}) \to \overline{K}^\times \xrightarrow{x \mapsto x^n} \overline{K}^\times \to 1$$

To see that this sequence is exact, first note that $\mu_n(\overline{K})$ is the kernel of the map $x \mapsto x^n$ by definition, so all that remains to show is that this map is surjective. Consider any $a \in \overline{K}^\times$. We wish to show that the polynomial $x^n - a$ has roots in $\overline{K}^\times$. Note that the formal derivative of the polynomial $x^n - a$ is nx^{n-1}, which is nonzero since the characteristic of K is relatively prime to n. Thus, the only root of nx^{n-1} is 0, which is not a root of $x^n - a$ as a is nonzero, and hence $x^n - a$ is separable. Since $\overline{K}$ is the separable closure of K, all of the roots of $x^n - a$ lie in $\overline{K}$, as desired. Then, the long exact sequence on homology gives us

$$1 \to \mu_n(\overline{K})^{\Gamma_K} \to (\overline{K}^\times)^{\Gamma_K} \to (\overline{K}^\times)^{\Gamma_K} \to \hat{\mathrm{H}}^1(\Gamma_K, \mu_n(\overline{K})) \to \hat{\mathrm{H}}^1(\Gamma_K, \overline{K}^\times)$$

We know all of the terms on the left

$$1 \to \mu_n(K) \to K^\times \xrightarrow{x \mapsto x^n} K^\times \xrightarrow{\delta} \hat{\mathrm{H}}^1(\Gamma_K, \mu_n(\overline{K})) \to \hat{\mathrm{H}}^1(\Gamma_K, \overline{K}^\times) \tag{1}$$

Next we will show that the rightmost term is 1, a result which is commonly referred to as Hilbert's theorem 90. First, we show that this is the case when when L/K is any finite Galois extension.

Theorem 4.1. *Let L/K be a finite Galois extension with Galois group G. Then*

$$\hat{\mathrm{H}}^1(G, L^\times) = 1$$

Proof. By corollary 3.5, together with the fact that $\hat{\mathrm{H}}^\bullet(G, -) = \mathrm{H}^\bullet(G, -)$ when G is finite (see section 3.3), it will suffice to show that every crossed homomorphism $t : G \to L^\times$ is principal. To do this, we first set

$$a_t = \prod_{\tau \in G} t(\tau)$$

Since G is finite by hypothesis this is a well-defined element of L, and since each $t(\tau)$ is nonzero so is a_t. We aim to show that t is generated by a_t^{-1}. Let $\sigma \in G$. Then we have

$$t(\sigma) \cdot \sigma(a_t) = t(\sigma) \cdot \sigma\left(\prod_{\tau \in G} t(\tau)\right) = t(\sigma) \cdot \prod_{\tau \in G} \sigma(t(\tau)) \tag{2}$$

Moreover, since t is a crossed homomorphism, we have

$$t(\sigma\tau) = \sigma(t(\tau))t(\sigma)$$

for each $\tau \in G$, so rearranging terms gives us

$$\sigma(t(\tau)) = \frac{t(\sigma\tau)}{t(\sigma)}$$

Combining this with (2) yields

$$t(\sigma) \cdot \sigma(a_t) = t(\sigma) \cdot \prod_{\tau \in G} \frac{t(\sigma\tau)}{t(\sigma)} = \prod_{\tau \in G} t(\sigma\tau) = a_t$$

where the last equality holds because $\sigma G = G$. Finally, since σ is an automorphism we have $\sigma(a_t)^{-1} = \sigma(a_t^{-1})$, so we have

$$t(\sigma) = \sigma(a_t)^{-1} a_t = \sigma(a_t^{-1})(a_t^{-1})^{-1}$$

completing the proof that t is a principal crossed homomorphism generated by a_t^{-1}, and therefore that

$$\hat{\mathrm{H}}^1(G, L^\times) = \mathrm{H}^1(G, L^\times) = 1$$

□

Miraculously, this, along with the following lemma, is all we need to prove Hilbert's theorem 90, even when $\overline{K}/K$ is infinite:

Lemma 4.2. *Let G be a topological group, and let $N \trianglelefteq G$ be an open normal subgroup. Then G/N is a discrete group.*

Proof. Since N is open, by the definition of the quotient topology the subset $\{N\}$ of G/N is open. Moreover, G/N is a topological group, so $\{gN\}$ is open for all $g \in G$ as translation by g is a homeomorphism. Thus each singleton subset of G/N is open, so G/N is discrete. □

Corollary 4.3. *The first group cohomology of $\overline{K}^\times$ over Γ_K vanishes:*

$$\hat{\mathrm{H}}^1(\Gamma_K, \overline{K}^\times) = 1$$

Proof. As observed in section 3.3, we have

$$\hat{\mathrm{H}}^1(\Gamma_K, \overline{K}^\times) = \varinjlim_N \hat{\mathrm{H}}^1(\Gamma_K/N, (\overline{K}^\times)^N) \tag{3}$$

where N ranges over all open normal subgroups of Γ_K. Moreover, Γ_K is compact since it is profinite. This follows from the fact that it the limit of the Galois groups of its finite subextensions, that is, Γ_K is a closed subgroup of the product of discrete (and hence compact) groups. Thus each quotient Γ_K/N by an open normal subgroup N of Γ_K is compact, and since it is discrete by lemma 4.2 we conclude that it is finite.

Now, if $N \trianglelefteq \Gamma_K$ is an open normal subgroup then it is also closed by lemma 4.2, since it is the preimage of the closed subset $\{N\} \subseteq G/N$. It follows from the infinite Galois correspondence that the fixed field L_N of N in $\overline{K}$ is a Galois extension of K with

$$\mathrm{Gal}(L_N/K) = \frac{\Gamma_K}{N}$$

Therefore we see from (3) that $\hat{\mathrm{H}}^1(\Gamma_K, \overline{K}^\times)$ is the direct limit of the group cohomologies of finite Galois subextensions, which are each trivial by theorem 4.1. That is, we have

$$\hat{\mathrm{H}}^1(\Gamma_K, \overline{K}^\times) = \varinjlim 1 = 1$$

completing the proof of Hilbert's theorem 90. □

Next, we turn our attention to the homology $\hat{\mathrm{H}}^1(\Gamma_K, \mu_n(\overline{K})$ in the special case when $\mu_n(\overline{K})$ is contained in K. As noted above, the invariance $\mu_n(\overline{K})^{\Gamma_K}$ is precisely the subgroup of roots of unity in the base field K, so since $\mu_n(\overline{K}) \subseteq K$ we know that $\mu_n(\overline{K})$ is Γ_K-invariant. Furthermore, since the polynomial $x^n - 1$ is separable $\overline{K}$ contains each of its roots, or in other words, $\mu_n(\overline{K})$ is a cyclic group of order n (generated by any primitive n^{th} root of unity). These two facts give us the following theorem:

Theorem 4.4. *There is a surjection $\Omega : \hat{\mathrm{H}}^1(\Gamma_K, \mu_n(\overline{K})) \to \mathcal{V}$, where $\mathcal{V}$ is the collection of Galois subextensions L/K lying in $\overline{K}$ such that*

$$\mathrm{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z}$$

for some positive integer m dividing n.

Proof. Let $\mathcal{U}$ be the group of continuous homomorphisms $\Gamma_K \to \mu_n(\overline{K})$. Since $\mu_n(\overline{K})$ is invariant under the action of Γ_K, by corollary 3.6 we see that $\hat{\mathrm{H}}^1(\Gamma_K, \mu_n(\overline{K}))$ is isomorphic to $\mathcal{U}$ — we note that this corollary still holds in the continuous case, simply by making each (resp. crossed, principal crossed) homomorphism continuous. Thus, it will suffice to define a surjection $\Omega' : \mathcal{U} \to \mathcal{V}$, then take Ω to be the precomposition of Ω' with the isomorphism $\Lambda : \hat{\mathrm{H}}^1(\Gamma_K, \mu_n(\overline{K})) \to \mathcal{U}$ from corollary 3.6 (again, making all appropriate maps continuous).

Let $f : \Gamma_K \to \mu_n(\overline{K})$ be a continuous group homomorphism in $\mathcal{U}$, and let $K_f = K^{\ker f}$ be the fixed field of $\ker f$. We must first verify that $K_f \in \mathcal{V}$. To see this, we observe that $\Gamma_K/\ker f$ is isomorphic to the subgroup $\operatorname{im} f$ of $\mu_n(\overline{K})$, so in particular is finite (i.e. equipped with the discrete topology). But f is continuous and $\{0\} \subseteq \operatorname{im} f$ is closed, so $\ker f = f^{-1}(\{0\})$ is closed in Γ_K, and since it is also normal we conclude by the infinite Galois correspondence (as well as lemma 9.22.5 of [2]) that K_f/K is Galois and

$$\mathrm{Gal}(K_f/K) \cong \frac{\mathrm{Gal}(\overline{K}/K)}{\mathrm{Gal}(\overline{K}/K_f)} = \frac{\Gamma_K}{\ker f} \cong \operatorname{im} f$$

Moreover, $\operatorname{im} f$ is a subgroup of $\mu_n(\overline{K})$, a cyclic group of order n, so $\mathrm{Gal}(K_f/K) \cong \operatorname{im} f$ is a cyclic group whose order divides n. Therefore $K_f \in \mathcal{V}$, so Ω' is well-defined.

It remains to be shown that Ω' is a surjection. Let $L \in \mathcal{V}$, so that $\mathrm{Gal}(L/K) \cong \mathbb{Z}/m\mathbb{Z}$ for some positive integer m dividing n. Additionally, let $f_L : \Gamma_K \to \mu_n(\overline{K})$ be the composition

$$\Gamma_K \xrightarrow{\pi} \frac{\Gamma_K}{N} \xrightarrow{\iota} \mu_n(\overline{K})$$

where $N = \mathrm{Gal}(\overline{K}/L)$, π is the quotient map, and ι is the inclusion map which sends a generator of $\mathrm{Gal}(L/K)$ to an element of order m in $\mu_n(\overline{K})$. We note that this N is indeed normal in Γ_K, as L/K is a Galois subextension of $\overline{K}$ (so π exists), and $\mu_n(\overline{K})$ contains an element of order m since m divides n (so some embedding ι exists). Moreover, ι is injective and $\ker \pi = N$, so we conclude that $\ker f = N$. Therefore, by the infinite Galois correspondence we have

$$\Omega'(f) = K^N = L$$

so Ω' is surjective, and thus so is $\Omega = \Omega'\Lambda$. □

Theorem 4.4 relates our cohomological framework to cyclic extensions of K, which will be essential when proving the main theorem. To complete the proof of theorem 1.1 we require one final result, which, in light of corollary 3.6, allows us to unwind the connecting morphism δ of the Kummer sequence in (1) as a map into the group of homomorphisms $\Gamma_K \to \mu_n(\overline{K})$.

Theorem 4.5. *Suppose $\mu_n(\overline{K}) \subseteq K$. Then for each $a \in K^\times$ the homomorphism $\Lambda^*(\delta(a)) : \Gamma_K \to \mu_n(\overline{K})$ is given by*

$$\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

where Λ^* is the map on cohomology induced by the chain isomorphism $\Lambda : C^1(\Gamma_K, \mu_n(\overline{K})) \to \mathcal{W}_1$ given in lemma 3.2.

Proof. Let $a \in K^\times$. By the snake lemma, in order to compute $\delta(a)$ we must first pull a back along the map $x \mapsto x^n$ to obtain an n^{th} root $\sqrt[n]{a}$ of a in $\overline{K}^\times$. Under the natural isomorphism

$$\overline{K}^\times \cong \mathrm{Hom}_{\mathbb{Z}[\Gamma_K]}(\mathbb{Z}[\Gamma_K], \overline{K}^\times) = C^0(\Gamma_K, \overline{K}^\times)$$

the element $\sqrt[n]{a}$ is carried to the G-module homomorphism $f : \mathbb{Z}[\Gamma_K] \to \overline{K}^\times$ given by $1 \mapsto \sqrt[n]{a}$. Next we apply the differential d^* to f, to obtain an element $d^*(f) = fd \in C^1(\Gamma_K, \overline{K}^\times)$ with

$$fd(1 \otimes \sigma) = f(\sigma - 1) = \sigma(f(1))f(1)^{-1} = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

for all $\sigma \in \Gamma_K$. But by the snake lemma we have $\delta(a) = d^*(f)$, so

$$\Lambda(\delta(a))(\sigma) = fd(1 \otimes \sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

proving the desired result. □

Finally, we are equipped with the necessary tools to complete the proof of the main theorem:

Proof of Theorem 1.1. Let L/K be a Galois extension with Galois group isomorphic to $\mathbb{Z}/n\mathbb{Z}$, and suppose K contains a primitive n^{th} root of unity. Letting $\overline{K}$, Γ_K, and $\mu_n(\overline{K})$ be as above, we have an exact sequence

$$1 \to \mu_n(K) \to K^\times \xrightarrow{x \mapsto x^n} K^\times \xrightarrow{\delta} \hat{\mathrm{H}}^1(\Gamma_K, \mu_n(\overline{K})) \to 1 \tag{4}$$

by Hilbert's theorem 90 (corollary 4.3), together with the Kummer sequence (1). Moreover, taking $\Omega : \mathcal{U} \to \mathcal{V}$ to be the surjection defined in theorem 4.4, noting that $L \in \mathcal{V}$ by hypothesis, we see that there exists some $h \in \hat{\mathrm{H}}^1(\Gamma_K, \mu(\overline{K}))$ such that

$$\Omega(h) = K^{\ker \Lambda(h)} = L$$

But it follows from the exactness of (4) that δ is surjective, and hence that there is some $a \in K^\times$ satisfying $\delta(a) = h$, so that L is the fixed field of $N = \ker \Lambda(\delta(a))$. Finally, by theorem 4.5 we see that $\Lambda(\delta(a))$ is given by

$$\Lambda(\delta(a))(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$$

so $\sigma \in N$ if and only if

$$\sigma(\sqrt[n]{a}) = \sqrt[n]{a}$$

that is, if and only if σ fixes the extension $K(\sqrt[n]{a})$. In other words, the fixed field K^N is given precisely by adjoining an n^{th} root of a to K, so we conclude that

$$L = K^N = K(\sqrt[n]{a})$$

completing the proof. □

References

[1] C. A. Weibel, *An Introduction to Homological Algebra*. Cambridge University Press, 1994.

[2] T. Stacks project authors, "The stacks project." `https://stacks.math.columbia.edu/tag/0BMI`, 2021.

[3] B. Conrad, "Profinite group cohomology class notes." `http://math.stanford.edu/~conrad/210BPage/handouts/profcohom.pdf`, 2021.

[4] R. M. F. David S. Dummit, *Abstract Algebra*. Englewood Cliffs, 1991.