GALOIS COHOMOLOGY

MARK CURRAN

Galois cohomology in its current form took shape during the 1950s as a way of formulating class field theory in a more topological way. This viewpoint was developed by the likes of John Tate, Emil Artin and Gerhard Hochschild. At the 1962 International Congress of Mathematics, (the conference where the Field's medals are awarded) Tate announced several duality theorems about the group cohomology of finite modules and abelian varieties over local and global fields. The famous duality theorem for finite modules (known as local Tate-duality) relies heavily on the work of Nakayama ([11]) while several other results are jointly attributed to Poitou ([10] pg.v). Surprisingly, many of these results were never formally published. Indeed James Milne said the motivation for the writing [10] was to record proofs of these results, while other proofs were given in [6] as reproductions of personal correspondence between Serge Lang and Tate.

Despite its modern formalism, results best described using Galois cohomology were already being employed as early as the l890s. Two famous examples include the 90th theorem of Hilbert's famous *Zahlbericht* which relies heavily on the first cohomology group being trivial. Another such example occurs when k is a field of characteristic p, where p is a nonzero prime, and K is a Galois extension of k. Kummer described the homomorphisms from $Gal(\frac{K}{k})$ to $\frac{\mathbb{Z}}{p\mathbb{Z}}$ in terms of the arithmetic of k, a result which can be easily be proved using Galois cohomology. It was also known prior to the second world war that the second cohomology group of the separable closure of a number field is isomorphic to the Brauer group of the field.

Suppose G is a group and A is some abelian group with a left G-action. For $q \geq 1$, one can think of the cocycles as maps $\phi : G^q \to A$ satisfying some algebraic property (also one can think of the coboundaries as cocycles that satisfy a more restrictive algebraic property). We let $H^q(G, A)$ be the group of cocycles modulo the group of coboundaries. If k is a field and K is a Galois extension of k then a common choice of A is $K^\times$ with multiplication. If G is the Galois group of K over k, we have an action of G on the abelian group A. In general the descriptions of the $H^q(G, A)$ become increasingly complicated as q increases. In most cases of interest, the cohomology groups are trivial for $q \geq 3$ ([15], Chapter II, §5.3).

If G is an infinite Galois extension then one can write $H^q(G, A)$ as the direct limit of the groups $H^q(G_i, A_i)$ where the $G_i \subset G$ are finite Galois extensions and the $A_i \subset A$ are intermediate fields. This process requires a topology on the group G that makes G into Hausdorff, compact and totally disconnected space. Such groups are called profinite groups and play a central role in understanding the cohomology of a Galois extension.

This thesis aims to give an overview of Galois cohomology. We will start by reviewing some graduate level topics in Galois theory. In this section we will assume many analagous results from the case of a finite extension. We will then proceed to define group cohomology using a standard construction. One can use the machinery of the Ext-functor to define cohomology groups, though we will avoid using category theory as much as possible. We will also discuss the inflation map, restriction map and the cup product. Once group cohomology is defined we will use Galois cohomology to treat the classical problems of Hilbert and Kummer. These problems require no more knowledge then what has been developed in sections 1 and 2.

Sections 4 and 5 develop some important tools for studying Galois cohomology, namely the method by which one can reduce problems to the case of a finite Galois extension. In section 4 we investigate the properties of profinite groups. A profinite group is a projective limit of finite groups and if each constituent finite group has the discrete topology then the limit will be compact, Hausdorff and totally disconnected. In fact there is a canonical way to write any group with these topoligcal properties as a limit of finite groups. The motivating examples of profinite groups occur in Galois theory; an infinite Galois extension can be thought of as a limit of its intermediate finite extensions. In section 5 we develop a cohomology theory for profinite groups. We also discuss why the cohomology theory of section 5 is equivalent to the theory developed in section 2.

Section 6 explores some more applications of Galois cohomology. Of particular importance is Tate's duality result via the cup product. We assume a result due to Nakayama ([11]) to give a proof of Tate local duality on finite modules. We also outline three duality theorems in number theory that are expressed in the language of Galois cohomology. Section 7 is a series of short appendices on some of the important concepts required in the thesis body.

The author would like to thank Daniel Delbourgo and Antonio Lei for their advice and expertise.

1. TOPICS IN GALOIS THEORY

For the remainder of this section let k be field and K an algebraic extension of k. For $\alpha \in K$ let $m_\alpha(X) \in k[X]$ be the minimal polynomial of α. The goal of this section will be to establish some of the fundamental results of Galois theory when K is not necessarily a finite extension of k. We will assume many results from the finite case (see [19],[7],[1])

1.1. INFINITE GALOIS EXTENSIONS.

Lemma 1.1. *Let K be a normal extension of k with B and B' intermediate fields between K and k. Let $\sigma : B \to B'$ be any isomorphism with $\sigma|k = id_k$. Then σ extends to an automorphism of K i.e. to an element of $Gal(\frac{K}{k})$.*

Proof. Consider the set

$$S = \{(D, \tau) |\, B \subset D\, \tau : D \to D \,\text{such that}\, \tau|B = \sigma\}$$

Order S by defining $(D_1, \tau_1) \leq (D_2, \tau_2)$ iff $D_1 \subset D_2$ and $\tau_2|D_1 = \tau_1$. It's easy to see that S is partially ordered and that any chain $\{D_i, \tau_i\}_{i\in\Lambda}$ is bounded above by $D = \bigcup D_i$ and $\tau(d_i) = \tau_i(d_i)$. Zorn's lemma implies there is a maximal extension of σ; let's denote it (K_0, τ_0). We obviously want to show that $K_0 = K$.

Assume for contradiction there exists some $\alpha \in K$ such that $\alpha \notin K_0$. Let K_1 be the splitting field of $m_\alpha(X)$ over K_0. Then K_1 is a finite extension of K_0 and as such τ_0 extends to an automorphism on K_1, contradicting the maximality of K_0 (see [1]§6.4, Lemma 6.4.4). □

Theorem 1.1. *Let $G = Gal(\frac{K}{k})$. The following are equivalent.*

1. *K is a Galois extension of k i.e. the field fixed by G (denoted K^G) is equal to k.*
2. *K is normal and separable.*
3. *For every intermediate finite extensions B (i.e. $k \subset B \subset K$) there exists a finite, normal and separable extension D such that $k \subset B \subset D \subset K$.*

Proof. 1. $\Rightarrow$ 2. Let $\alpha \in K$. Suppose $\sigma \in G$. Then $m_\alpha(\sigma(\alpha)) = \sigma(m_\alpha(\alpha)) = 0$. So σ permutes the roots $\{\alpha_1, \cdots, \alpha_n\}$ of $m_\alpha(X)$. Consider $f(X) = \prod_{i=1}^n (X - \alpha_i)$. We just established that this polynomial is invariant under $\sigma \in G$ and since K is Galois by assumption we have $f(X) \in k[X]$. If $g(X) \in k[X]$ is a polynomial such that $g(\alpha) = 0$ then by a similar calculation to that done for $m_\alpha(X)$ we know that $g(\alpha_i) = 0$ for $1 \leq i \leq n$. Then $f(X)|g(X)$ so $f(X)$ is irreducible. Thus $f(X) = m_\alpha(X)$ which means $m_\alpha(X)$ is a separable polynomial that splits in K.

2. $\Rightarrow$ 3. Let $B = k(\alpha_i, \cdots, \alpha_n)$ be a finite extension of k. Let D be the splitting field of $\prod_{i=1}^{n} m_{\alpha_i}(X)$. Then $D \subset K$ and D is a finite extension of k. Since each $m_{\alpha_i}(X)$ is separable by assumption we deduce that D is a separable extension.

3. $\Rightarrow$ 1. Choose $\alpha \in K$ with $\alpha \notin k$. Let $B = k(\alpha)$. By assumption we can say $B \subset D$ where D is a finite extension and is the splitting field of a separable polynomial in $k[X]$. We may assume that finite, normal and separable extensions are Galois ([19]§2.7, Theorem 2.7.14). Then there exists $\sigma \in Gal(\frac{D}{k})$ such that $\sigma(\alpha) \neq \alpha$. By lemma 1.1 there exists some $\tau \in G$ that extends σ. In particular $\tau(\alpha) \neq \alpha$ so α is not fixed by some element of G. Since α was chosen arbitrarily $K^G = k$. □

Corollary 1.1. *The following are equivalent*

(1) *K is Galois over k*
(2) *K is the splitting field of a set of separable polynomials in $k[X]$.*

Proof. 1. $\Rightarrow$ 2. We know that K is normal and separable by theorem 1.1. Thus for every $\alpha \in K$, there exists some $m_\alpha(X) \in k[X]$ such that m_α is a separable, irreducible polynomial that splits in K. Thus K is the splitting field of the set $\{m_\alpha(X)\}_{\alpha \in K}$.

2. $\Rightarrow$ 1. Let K be the splitting field of some set of separable, irreducible polynomials in $k[X]$, say $\{f_i(X)\}_{i \in \Lambda}$ (henceforth Λ will always denote an indexing set). For any $\alpha \in K$, α is contained in the splitting field of finitely many of the $f_i(X)$'s say $\{f_{j_\alpha}(X)\}_{j=1}^{J(\alpha)}$ where $J(\alpha)$ is a positive integer depending on α. If $B = k(\alpha_1, \cdots, \alpha_n)$ is any finite extension of k then this observation implies B is contained in the splitting field of $\bigcup_{i=1}^{n} \bigcup_{j=1}^{J(\alpha_i)} \{f_{j_{\alpha_i}}(X)\}$. By theorem 1.1, this is equivalent to K being a Galois extension of k. □

Corollary 1.2. *If K is a Galois extension of k and B is any intermediate extension (i.e. $k \subset B \subset K$) then K is a Galois extension of B.*

Proof. Let $A = B(\alpha_1, \cdots, \alpha_n)$ be a finite extension of B. Let $A' = k(\alpha_1, \cdots, \alpha_n)$. We first claim that A' is a finite extension of k. A' can be written as the composite of elements from $k(\alpha_i)$ i.e. $A' = (\sum_{i=1}^{n} a_i)(\sum_{i=1}^{n} a_i')^{-1}$ where each $a_i, a_i' \in k(\alpha_i)$ (see [19]§2.3, Remark 2.3.3). Hence it will suffice to show that $k(\alpha_i)$ is finite for a fixed i. Let $m_i'(X) \in B[X]$ be the minimal polynomial of α_i. Let B_i be the extension of k given by adjoing all the coefficients of $m_i'(X)$ to k. Then $B_i(\alpha_i)$ is a finite extension of B_i which is in turn a finite extension of k. So $B_i(\alpha_i)$ is a finite extension of k and since $k(\alpha_i) \subset B_i(\alpha_i)$ we have the claim.

By theorem 1.1 there exists an intermediate extension D' (in this case $A' \subset D' \subset K$) such that D' is a finite Galois extension of k. In particular we can write D' as the splitting field of a separable polynomial $f(X) \in k[X]$ (if D' is the splitting field of several polynomials take their product). But $A \subset BA' \subset BD'$

and BD' is a finite extension of B that is the splitting field of the separable polynomial $f(X) \in B[X]$. The result follows from part 3. of theorem 1.1. □

1.2. **KRULL TOPOLOGY.**

Proposition 1.1. *Consider $G = Gal(\frac{K}{k})$. Define a basis of open sets around $1 \in G$ by*

$$\{U_B = Gal(\frac{K}{B}) \mid B \textit{is a finite extension of } k\} \tag{1.1}$$

Then these sets form the basis for a topology on G called the Krull topology on G.

Before proceeding we make some simple oberservations. Firstly that $\tau \in U_B$ iff $\tau|_B = id_B$ and similarly $\tau \in \sigma U_B$ iff $\tau|_B = \sigma|_B$. Moreover if G is finite then the Krull topology makes G into a topological group with the discrete topology.

Proof. Let $U_i = U_{B_i}$ with $i = 1, 2$. Let $U_3 = U_1 \bigcap U_2$ and $B_3 = B_1 B_2$ i.e. the composite of the fields B_1 and B_2. Then B_3 is a finite extension of k and $B_3 = K^{U_1 \bigcap U_2}$ ([19] §2.8, Proposition 2.8.14).

We claim that $U_3 = Gal(\frac{K}{B_3})$ which will imply that U_3 is open and therefore establishes the sets in 1.1 are a neighborhood basis at $e \in G$. Translation about G will give a neighborhood basis at every point in G thus defining a topology on G. First it's clear that $U_3 \subset Gal(\frac{K}{B_3})$. If $\sigma \notin U_3$ then WLOG we may assume $\sigma \notin U_1$. Then $\sigma|_{B_1} \neq id_{B_1}$ and therefore σ acting on an element of the form $B_1 e \in B_3$ is not the identity. In particular $\sigma \notin Gal(\frac{K}{U_3})$ which establishes $U_3 = Gal(\frac{K}{U_3}) = U_{B_3}$. □

Lemma 1.2. *The sets U_B are subgroups and*

$$\{\sigma U_B | \, \sigma \in G, \, B \textit{is a finite extension of } k\} = \{U_B \sigma | \, \sigma \in G, \, B \textit{is a finite extension of } k\}$$

Proof. That the sets U_B are subgroups is clear. If $\sigma \in G$ then $U_B \sigma^{-1}$ takes $\sigma(B)$ to B and hence $\sigma U_B \sigma^{-1} = U_{\sigma(B)}$. In particular

$$U_B \sigma = \sigma(\sigma^{-1} U_B \sigma) = \sigma U_{\sigma^{-1}(B)}$$

The result follows from the fact that each $\sigma(B)$ is a finite extension. □

Proposition 1.2. *G with the Krull topology is a topological group.*

Proof. Consider the multiplication map $m : G \times G \to G$ and let $\sigma\tau U$ be a neighborhood of $\sigma\tau$. Let $g, h \in G$ be elements such that $m(g, h) \in \sigma\tau U$ then $g(hUh^{-1}) \times hU \subset \sigma\tau U$. If σU is a neighborhood of σ we have $(\sigma U)^{-1} = U^{-1}\sigma^{-1} = U\sigma^{-1}$. □

Theorem 1.2. *(Fundamental Theorem of Galois Theory): Let K be a Galois extension of k where$G = Gal(\frac{K}{k})$ is equipped with the Krull topology.*

(1) *There is a 1-1 correspondence between intermediate fields $k \subset B \subset K$ and closed subgroups of G given by*
$$G_B = Gal(\frac{K}{B}) \text{ and } B = K^{G_B}$$
(2) *The following are equivalent:*
- *B is a normal extension of k*
- *B is a Galois extension of k*
- *G_B is a normal subgroup*

(3) *If G_B is normal we have an isomorphism of topological groups*
$$Gal(\frac{B}{k}) \simeq \frac{G}{G_B}$$

Proof. 1. Let B be an intermediate field $k \subset B \subset K$. Let $G_B = Gal(\frac{K}{B})$. We first verify that G_B is closed. Let $\sigma \in \overline{G_B}$ and let $\beta \in B$. Then $k(\beta)$ is a finite extension of k and therefore $U = Gal(\frac{K}{k(\beta)})$ is an open neighborhood of the identity. In particular, there exists a $\tau \in G_B$ such that $\tau \in \sigma U \bigcap G_B$. Let $\tau = \sigma\nu$ with $\nu \in U$, then $\tau(\beta) = \beta$ and $\nu(\beta) = \beta$. Therefore $\sigma(\beta) = \sigma(\nu(\beta)) = \sigma\nu(\beta) = \tau(\beta) = \beta$. So $\sigma \in G_B$ and since $\sigma \in \overline{G_B}$ was arbitrary we have $G_B = \overline{G_B}$.

To see that the association is injective suppose B_1 and B_2 are intermediate fields. Then by corollary 1.2 we know that K is a Galois extension of both B_1 and B_2. If $G_{B_1} = G_{B_2}$ we have $Gal(\frac{K}{B_1}) = Gal(\frac{K}{B_2})$ and thus
$$B_1 = K^{G_{B_1}} = K^{G_{B_2}} = B_2$$

Surjectivity is not trivial. Let $H \subset G$ be a closed subgroup and let $B = K^H$. Then $H \subset Gal(\frac{K}{B})$ is clear. For the reverse inequality let $U_A = Gal(\frac{K}{A})$ where A is some finite extension of k. By corollary 1.2 K is a Galois extension of B. We know that AB (the composite of A and B) is a finite extension of B so by theorem 1.1 there exists an intermediate extension $B \subset AB \subset D \subset K$ such that D is the splitting field of some polynomial $f(X) \in B[X]$.

Every element of $Gal(\frac{K}{B})$ permutes the roots of $f(X)$ and will therefore restrict to an element of $Gal(\frac{D}{B})$. Conversely lemma 1.1 indicates that every element of $Gal(\frac{D}{B})$ extends (not necessarily uniquely) to an element of $Gal(\frac{K}{B})$. Hence we can define a surjective restriction map $R : Gal(\frac{K}{B}) \to Gal(\frac{D}{B})$.

Let $\sigma \in Gal(\frac{K}{B})$, $\sigma_0 = R(\sigma) \in Gal(\frac{D}{B})$ and $H_0 = R(H)$. Since D is a Galois extension of B
$$K^{H_0} = K^H = B$$

Assuming the fundamental theorem of Galois theory for finite extensions we have $H_0 = Gal(\frac{D}{B})$. Then since R is surjective there exists a $\tau \in H$ with $R(\tau) = \sigma_0 = R(\sigma)$ i.e. $\tau|_D = \sigma|_D$ so $\tau \in \sigma U_D$. Because $A \subset D$ we have $\sigma U_A \bigcap H \neq \emptyset$.

Since U_A was arbitrary $\sigma \in \overline{H}$ and because H was closed, $\sigma \in H$.

2. We will show that an intermediate extension $k \subset B \subset K$ is a normal extension iff G_B is normal. Let $\sigma \in G$. We have remarked in lemma 1.2 that $\sigma(B) = K^{\sigma G_B \sigma^{-1}}$. So G_B is normal iff $\sigma(B) = B$ for all $\sigma \in G$. First suppose B is normal so for any $\beta \in B$, $m_\beta(X)$ splits over B. Since any $\sigma \in G$ permutes roots of $m_\beta(X)$ we see that $\sigma(\beta) \in B$. Thus $\sigma(B) \subset B$ while $\sigma^{-1}(B) \subset B$ gives equality. Conversely suppose that B is not a normal extension. Choose $\beta \in B$ such that there exists a second root β' of $m_\beta(X)$ with $\beta' \notin B$. Since $k(\beta) \simeq k(\beta')$ we can apply lemma 1.1 to establish the existence of some $\sigma \in G$ such that $\sigma(\beta) = \beta'$. In particular $\sigma(B) \neq B$.

The statement that B is a normal and separable extension of k iff B is a Galois extension of k is the content of theorem 1.1. We claim that in the current context B is a Galois extension iff B is a normal extension. Indeed K is Galois so by corollary 1.1 K is the splitting field of a set of separable polynomials. $B \subset K$ is a normal extension of k so it is the splitting field of a subset of these polynomials. In particular B is automatically separable, so if $B \subset K$ is normal then B is a Galois extension of k. The converse is just theorem 1.1 again.

3. It remains to establish $Gal(\frac{B}{k}) \simeq \frac{G}{G_B}$. As in part 1. (with k in place of B and B in place of D) the restriction map is a surjective group homomorphism

$$R : Gal(\frac{K}{k}) \to Gal(\frac{B}{k})$$

given by $R(\sigma) = \sigma|_B$. The kernel of this map is obviously $Gal(\frac{K}{B})$ so it remains to show that the quotient topology on $Gal(\frac{B}{k})$ is the Krull topology. If $U_0 = \{\sigma \in Gal(\frac{B}{k}) | \, \sigma|_A = id\}$ where $A \subset B$ is a finite extension of k then U_0 is the image of the set $U_A \subset Gal(\frac{K}{k})$. On the other hand any $U_A \subset Gal(\frac{K}{k})$ where A is a finite extension of k with $k \subset A \subset K$ will restrict to $U_0 = \{\sigma \in Gal(\frac{K}{k}) | \, \sigma|_{B \bigcap A} = id\}$. But this is open since $A \bigcap B \subset A$ and hence must also be a finite extension of k. □

1.3. FURTHER PROPERTIES OF THE KRULL TOPOLOGY.

Lemma 1.3. *Each set σU_B in the Krull topology is closed.*

Proof. Suppose $\tau \notin \sigma U_B$. Then since U_B is a group $\tau U_B \bigcap \sigma U_B = \emptyset$. □

Lemma 1.4. *Let $\sigma : K \to K$ be a field homorphism such that $\sigma|_K = id$. Then σ is an isomorphism*

Proof. Any field homorphism is either the zero homorphism or is injective. Since $\sigma(1) = 1$ we are obviously in the later case. Let $\sigma \in K$ and consider

$$S = \{\beta \in K | \, m_\alpha(\beta) = 0\}$$

Since $\sigma|_k = id$, σ permutes the elements of S. So σ restricts to an injective map on S. But since S is finite σ must restrict to a bijective map on S i.e. there exists a $\beta_0 \in S$ such that $\sigma(\beta_0) = \alpha$. □

Theorem 1.3. *Let K be a Galois extension of k. Then $G = Gal(\frac{K}{k})$ with the Krull topology is Hausdorff, compact and totally disconnected.*

Proof. G is a topological group so to establish the Hausdorff property it suffices to show that G is T_0. To this end it suffices to separate any point from the indentity which is equivalent to showing

$$\bigcap U_B = \{id\} \text{ where } B\text{is a finite extension.}$$

Let $\sigma \in G$ with $\sigma \neq id$. Then for some $\alpha \in K$, $\sigma(\alpha) \neq \alpha$. Let $B = k(\alpha)$. Then $\sigma \notin U_B$ and so $\sigma \notin \bigcap U_B$.

To see that G is totally disconnected let $\sigma, \tau \in G$ with $\sigma \neq \tau$. We will construct disjoint clopen sets containing σ and τ which will imply they cannot be in the same connected component. Because$\sigma \neq \tau$ and G is Hausdorff so there exists an open set U_B with $\tau \notin \sigma U_B$. We can write $G = \sigma U_B \bigcup (G - \sigma U_B)$ where $G - \sigma U_B$ is open by lemma 1.3.

It remains to establish compactness. For each $\alpha \in K$ define the set $R_\alpha = \{\beta \in K | \, m_\alpha(\beta) = 0\}$. Let $\Delta = \prod_{\alpha \in K} R_\alpha$. Identify each $(\beta_\alpha)_{\alpha \in K}$ as a function from K to K. These functions fix k (for $\alpha \in k$, $m_\alpha(X) = X - \alpha$) so we can identify $G \subset \Delta$. If we give each R_α the discrete topology then since each R_α is finite, the R_α are compact. Moreover Δ is compact by Tchonoff's theorem. Hence to prove G is compact it will suffice to to prove two claims; first that the Krull topology on G is the subspace topology from Δ and second that G is a closed subset of Δ.

For the first claim suppose σU_B is open in G. Let $\{\beta_1, \cdots, \beta_n\}$ be a basis for B over k. Then for $\tau \in G$ we know that $\tau \in \sigma U_B$ iff $\tau|_B = \sigma|_B$. Since τ and σ are linear maps over k this is equivalent to $\tau(\beta_i) = \sigma(\beta_i)$ for $1 \leq i \leq n$. If we let $V = \prod S_\alpha$ with $S_\alpha = R_\alpha$ when $\alpha \neq \beta_i$ and $S_{\beta_i} = \{\sigma(\beta_i)\}$. Then V is open in Δ and $G \bigcap V = \sigma U_B$.

Conversely let $V \subset \Delta$ be open where $V = \prod S_\alpha$ with $S_\alpha = R_\alpha$ for almost all $\alpha \in K$. For the coordinates α_i (say $1 \leq i \leq n$) where $S_{\alpha_i} \neq R_{\alpha_i}$ we can take S_{α_i} to be a finite union of singletons so WLOG we may assume $S_{\alpha_i} = \{\alpha_i'\}$. Let $B = k(\alpha_1', \cdots, \alpha_n')$. If $\sigma \in G$ satisfies $\sigma(\alpha_i) = \alpha_i'$ then $G \bigcap B = \sigma U_B$. If not then $G \bigcap V = \emptyset$ which is of course open. This finishes the proof of the claim that the Krull topology is equivalent to the subspace topology from Δ.

For the second claim we make some important observations. We know that any field homorphism from $K \to K$ that fixes k is is automatically an automorphism by lemma 1.4. In particular for any $f \in \Delta$, f fixes k so f is a field homorphism iff $f \in G$. Let $f \in \Delta$ with $f \notin G$. Since f cannot be a field homorphism we know that at least one of the following hold

(1) $f(\alpha_1 + \alpha_2) \neq f(\alpha_1) + f(\alpha_2)$
(2) $f(\alpha_1)f(\alpha_2) \neq f(\alpha_1)f(\alpha_2)$

We only deal with the first case with the second being almost identical. Let $V = \prod S_\alpha$ with $S_\alpha = R_\alpha$ except for $S_{\alpha_1} = \{f(\alpha_1)\}$, $S_{\alpha_2} = \{f(\alpha_2)\}$ and $S_{\alpha_1+\alpha_2} = \{f(\alpha_1 + \alpha_2)\}$. Then V is open, $f \in V$ and $G \bigcap V = \emptyset$. Hence G is closed. □

1.4. **ALGEBRAIC AND SEPARABLE CLOSURE.** We are interested in finding algebraic extensions of k that are algebraically closed. To this end we effectively take the union of all such extensions. However given any two extensions of k we have no concept of taking their union. In this subsection we establish one way of finding algebraic extensions of k that are maximal in some sense.

Proposition 1.3. *Let k be a field, $f(X) \in k[X]$ a polynomial of degree ≥ 1. Then there exists an extension K with $k \subset K$ and such that f has a root in K.*

Proof. The theorem is trivial if f is not irreducible. In the later we know there exists a field B and an injective homorphism $\sigma : k \to B$ such that f (as an element of $\sigma(k)[X]$) has a root in B, say $\alpha \in B$. Let S be a set with cardinality equal to $B \backslash \sigma(k)$ that is disjoint from k. Define $K = k \bigcup S$. Extend σ to a bijective map $\sigma : K \to B$. Give K a field structure by

$$x + y = \sigma^{-1}(\sigma(x) + \sigma(y))$$

$$xy = \sigma^{-1}(\sigma(x))$$

Then f has a root in K given by $\sigma^{-1}(\alpha)$. □

Corollary 1.3. *Let k be a field and let $f_1, \cdots, f_n$ be polynomials in $k[X]$ of degree ≥ 1. Then there exists a field K with $k \subset K$ such that each f_i $(1 \leq i \leq n)$ has a root in K.*

Proof. Let K_1 be a field with $k \subset K$ and such that f_1 has a root in K_1. Likewise let K_2 be a field with $K_1 \subset K_2$ and such that $f_2 \in k[X] \subset K_1[X]$ has a root in K_2. Repeat this procedure n times. □

Theorem 1.4. *Let k be a field. Then there exists an algebraically closed field containing k as a subfield.*

Proof. First we will construct a field, denoted K_1, satisfying two important properties

- $k \subset K_1$
- Each polynomial of degree ≥ 1 in $k[X]$ has a root in K_1

We can then repeat the procedure to construct K_2 with $K_1 \subset K_2$ and such that every polynomial in $K_1[X]$ has a root in K_2. This gives a chain of fields

$$k \subset K_1 \subset K_2 \subset \cdots$$

Let $K = \bigcup_{n=1}^{\infty} K_n$. It's easy to see that K is a field. For any polynomial $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ we know there exists integers $\lambda(i) \geq 1$ such that $a_i \in K_{\lambda(i)}$. In particular $f(X) \in K_{max\{\lambda(i)\}}[X]$ which has a root $K_{max\{\lambda(i)\}+1} \subset K$. Hence every polynomial has a root in K and so K is algebraically closed. It remains to construct K_1.

For every polynomial in $k[X]$ of degree ≥ 1 associate a symbol X_f. Let S be the set $S = \bigcup\{X_f\}$ and consider $k[S]$, the polynomial ring in several variables. We claim the ideal generated by the $f(X_f)$ is not the unit ideal. Assume for contradiction one has

$$g_1 f_1(X_{f_1}) + \cdots g_n f_n(X_{f_n}) = 1 \tag{1.2}$$

where the $g_i \in k[S]$ for $1 \leq i \leq n$. For notational convenience write $X_{f_i} = X_i$. Each g_i has finitely many variables so we can write 1.2 as

$$\sum_{i=1}^{n} g_i(X_1, \cdots, X_N) f_i(X_i) = 1 \tag{1.3}$$

for some $N \geq n$. Let $k \subset F$ where F is a finite extension in which each f_i has a root say α_i. For $i > n$ set $\alpha_i = 0$. Evaluating 1.3 at $\{\alpha_1, \cdots, \alpha_N\}$ gives $0 = 1$; a contradiction. Let m be the maximal ideal containing the ideal generated by $\{f(X_f)\}_{f \in k[X]}$. Then $\frac{k[S]}{m}$ is a field and one has a ring homorphism $\sigma : k[S] \to \frac{k[S]}{m}$. Any polynomial $f \in k[X]$ of degree ≥ 1 can be identified with some $f \in m \subset f[S]$. So f has a root in $\frac{k[S]}{m}$. $\frac{k[S]}{m}$ is an extension of $\sigma(k)$ and we have embeddings $k \to k[S] \to \frac{k[S]}{m}$. Using a similar argument to that in proposition 1.3 we can write $k \subset \frac{k[S]}{m}$. Then $K_1 = \frac{k[S]}{m}$ has the desired properties. $\square$

Given a field k we can embed k is some algebraically closed field denoted $\overline{k}$. The union of all intermediate algebraic extensions $k \subset B \subset \overline{k}$ is the algebraic closure of k. The union of all separable extensions $k \subset B \subset \overline{k}$ is the separable closure of k. For a perfect field (eg. in characteristic zero, finite fields) the separable and algebraic closure coincide. For a general field of characteristic $p \neq 0$ we are required to make the distinction.

These fields can alternatively be characterised as the direct limit of all algebraic/separable extensions of k ordered by inclusion. In preparation for sections 4 and 5 we record this as a proposition.

Proposition 1.4. *Let K be a Galois extension of K. Let L be an intermediate, finite Galois extension of k (i.e. $k \subset L \subset K$). The collection $\{L_i\}_{i\in\Lambda}$ (where Λ is an indexing set) of all intermediate, finite, Galois extensions form a direct system with respect to inclusion and $K \simeq \varinjlim L_i$.*

Proof. Given two intermediate finite Galois extensions, say L_i and L_j, their composite L_iL_j is again a finite Galois extension contained in K. In light of this, it is clear that the collection $\{L_i\}_{i\in\Lambda}$ form a direct system.

For each $L_i \subset K$ we have an inclusion map $\phi_i : L_i \hookrightarrow K$. These maps are obviously compatible with the inclusion maps $L_i \hookrightarrow L_j$ where $L_i \subset L_j$. These maps are group homorphisms when K and the $\{L_i\}_{i\in\Lambda}$ are considered groups with addition. An analagous observation is true for $K^\times$and $\{L_i^\times\}_{i\in\Lambda}$ with multiplication.

Therefore, it remains to show that the induced homorphism $\phi : \varinjlim L \to K$ is bijective. For any $\alpha \in K$ we have a finite extension $k(\alpha)$ which is contained in an intermediate finite Galois extension of k by theorem 1.1. That $ker(\phi) = 0$ is clear since each ϕ_i has trivial kernel. □

2. GROUP COHOMOLOGY

2.1. G-MODULES.

Definition 2.1. Let G be a group. Then it's integral ring, denoted $\mathbb{Z}[G]$, is a $\mathbb{Z}$ vector space with basis elements indexed by elements in G and with multiplication defined by

$$mg \cdot nh = (mn) \cdot gh \text{ for } m, n \in \mathbb{Z}\text{and } g, h \in G$$

Suppose A is a left $\mathbb{Z}[G]$ module. Then the elements of the form $1g \in \mathbb{Z}[G]$ give rise to a group action of G on A. Conversely any group action of G on A can be extended to make A into a $\mathbb{Z}[G]$ module. So any $\mathbb{Z}[G]$ module is completely characterised by a group action of G on A. With this in mind we make the following definition.

Definition 2.2. We call a left $\mathbb{Z}[G]$-module a left G-module. Similarly we call a right $\mathbb{Z}[G]$-module a right G-module.

Before proceeding we clarify some notation and terminology. A left G-module can be made into a right G-module by taking $a \cdot g = g^{-1} \cdot a$ but by a G-module we will always mean a left G-module. By a G-homomorphism or G equivariant map we mean a module homomorphism betwee two G-modules.

For the remainder of this section we will let A be a G-module.

Definition 2.3. Let $Hom(A, B)$ denote the group of group homomorphisms from A to B. We will let $Hom_G(A, B)$ denote the G-module of G equivariant maps from A to B.

In definition 2.3 $Hom(A, B)$ is also a G-module with multiplication defined by $(g \cdot \phi)(a) = g \cdot \phi(g^{-1} \cdot a)$ though the maps ϕ may not be G-linear. In particular, we have $Hom_G(A, B) \subset Hom(A, B)$ as a submodule.

Definition 2.4. For any G-module A, the set of elements invariant under the action of G is denoted A^G.

A^G is a subgroup of A and is also a submodule since it is obviously closed under multiplication by G. We record two special cases of fixed submodules as propositions, the proofs of which are trivial.

Proposition 2.1. $Hom_G(A, B) \simeq (Hom(A, B))^G$

Proposition 2.2. *If we regard $\mathbb{Z}$ as a G-module on which G acts trivially then $Hom_G(\mathbb{Z}, A) \simeq (Hom(\mathbb{Z}, A))^G \simeq A^G$.*

An important observation is that the association $A \to A^G$ behaves functorially.

Proposition 2.3. *If*

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

is exact then the sequence

$$0 \to A^G \xrightarrow{f|_{A^G}} B^G \xrightarrow{g|_{B^G}} C^G$$

defined by taking the restrictions of f and g to $A^G$and B^G is also exact.

Proof. Since $Hom(\mathbb{Z}, -)$ is left exact on the category of abelian groups, we know that (permitting an abuse of notation) the sequence

$$0 \to Hom(\mathbb{Z}, A) \xrightarrow{f} Hom(\mathbb{Z}, B) \xrightarrow{g} Hom(\mathbb{Z}, C)$$

is exact. By proposition 2.2 $Hom(\mathbb{Z}, A) \simeq A^G$ for any A-module. □

Definition 2.5. If X is any abelian group then $Hom(\mathbb{Z}[G], X)$ can be made into a G-module with multiplication given by $(g \cdot \phi)(b) = \phi(g \cdot b)$ for $b \in \mathbb{Z}[G]$. A G-module that is isomorphic to $Hom(\mathbb{Z}[G], X)$ for some abelian group X is called a co-induced G-module.

Proposition 2.4. *Every G-module can be embedded into the co-induced G-module $Hom(\mathbb{Z}[G], A)$.*

Proof. For any $a \in A$ let $\phi_a \in Hom(\mathbb{Z}[G], A)$ be the map defined by $\phi_a(g) = g \cdot a$. It's clear that $h \cdot \phi_a(g) = \phi_a(h \cdot g)$ and that $a \mapsto \phi_a$ is injective (evaluate at $1 \in \mathbb{Z}[G]$). Since A is abelian it's easy to see that $\phi_{a+b}(g) = g \cdot (a + b) = g \cdot a + g \cdot b = \phi_a(g) + \phi_a(g)$. □

2.2. THE STANDARD COMPLEX AND GROUP COHOMOLOGY.

Definition 2.6. Let $P_q = \mathbb{Z}[G^{q+1}]$ i.e. the integral ring of the group $G \times \cdots \times G$ $(q+1)$ times. P_q is a G-module where G acts on the basis elements of P_q in the following way,

$$g(g_0, \cdots, g_q) = (gg_0, \cdots, gg_q)$$

Definition 2.7. Let $\delta_q : P_q \to P_{q-1}$ be the G-homomorphism defined by

$$\delta_q(g_0, \cdots, g_q) = \sum_{j=0}^{q} (-1)^j (g_0, \cdots g_{j-1}, g_{j+1}, \cdots, g_q)$$

If we treat $\mathbb{Z}$ as a G-module on which G acts trivially, let $\delta_0 : P_0 \to \mathbb{Z}$ be the G-homomorphism which sends every generator $g \in \mathbb{Z}[G]$ to $1 \in \mathbb{Z}$.

Proposition 2.5. *The following sequence is exact and is called the standard complex.*

$$\cdots \xrightarrow{\delta_3} P_2 \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} \mathbb{Z} \to 0 \tag{2.1}$$

Proof. For $q \geq 1$ it is a well known fact that $\delta_{q-1}\delta_q = 0$ ([13] §1.1), hence $Im(\delta_q) \subseteq Ker(\delta_{q-1})$. For the reverse inclusion define $h_q : P_{q-1} \to P_q$ on the generators by

$$h_q(g_0, \cdots, g_{q-1}) = (e, g_0, \cdots, g_{q-1})$$

Then it's easy to check that $\delta_{q+1}h_{q+1} + h_q\delta_q = id[P_q]$ so that if $a \in Ker(\delta_q)$ then $a = \delta_{q+1}h_{q+1}$. □

By proposition 2.3 we see that the association $A \to A^G$ is a left-exact covariant functor. We observe without proof that the category of G-modules is abelian and has enough injectives. It therefore makes sense to talk about the right derived functor of A^G. For our purposes we make the following definition,

Definition 2.8. A cohomological extension of A^G is a sequence of functors $H^q(G, A)$ for $q \geq 0$ such that the following properties hold

- $H^0(G, A) = A^G$
- If $q \geq 1$ and A is co-induced then $H^q(G, A) = 0$.

- There exists a collection of boundary homomorphisms $d_q : H^q(G, C) \to H^{q+1}(G, A)$ with the following property; if $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is an exact sequence then

$$\cdots \to H^q(G, A) \to H^q(G, B) \to H^q(G, C) \xrightarrow{d_q} H^{q+1}(G, A) \to \cdots \tag{2.2}$$

  is exact.

Theorem 2.1. *There exists only one cohomological extension of the functor A^G.*

Proof. We first show existence. Recall the standard complex

$$\cdots \xrightarrow{\delta_3} P_2 \xrightarrow{\delta_2} P_1 \xrightarrow{\delta_1} P_0 \xrightarrow{\delta_0} \mathbb{Z} \to 0$$

Let $\mathcal{C}$ be the complex formed by applying $Hom_G(-, A)$ to the standard complex. More specifically one obtains

$$0 \to Hom_G(\mathbb{Z}, A) \xrightarrow{\delta_0} Hom_G(P_0, A) \xrightarrow{\delta_1} Hom_G(P_1, A) \xrightarrow{\delta_2} \cdots \tag{2.3}$$

where we permit an abuse of notation by letting the δ_i's in 2.3 denote the maps induced by the maps defined in definition 2.7. For $q \geq 1$ let $H^q(\mathcal{C}) \simeq \frac{Ker(\delta_q)}{Im(\delta_{q-1})}$ be the q-th cohomlogy group of 2.3. Note that $Im(\delta_0) \subset Hom(P_0, A)$ are the maps which take every $g \in G$ to some fixed $a \in A^G$. This map will be zero iff $a = 0$ hence the sequence $0 \to Hom_G(\mathbb{Z}, A) \xrightarrow{\delta_o} Hom(P_0, A)$ is exact. Therefore we would obtain the same $H^q(\mathcal{C})$ if we were to calculate the cohomology of

$$0 \to Hom_G(P_0, A) \xrightarrow{\delta_1} Hom_G(P_1, A) \xrightarrow{\delta_2} \cdots$$

As such, we adopt the convention of defining the 0-th cohomology group to be $H^0(\mathcal{C}) = Hom_G(\mathbb{Z}, A)$ which is just A^G by proposition 2.2.

We claim that the $H^q(\mathcal{C})$ satisfy the properties of a cohomological extension. We have observed that $H^0(\mathcal{C}) = Hom_G(\mathbb{Z}, A) \simeq A^G$. The existence of the boundary homomorphism d_q follows from the fact that the the category of G-modules is abelian ([13] §6.1 Proposition 6.9).

Consider the case where A is co-induced, say $A \simeq Hom(\mathbb{Z}[G], X)$ where X is an abelian group. Then for any G-module B we claim that

$$Hom_G(B, A) \simeq Hom(B, X)$$

If $\varphi \in Hom_G(B, A)$ then let $\lambda : Hom_G(B, A) \to Hom(B, X)$ be defined by $\lambda(\varphi)(b) = \varphi(b)(1)$. Then λ is clearly linear and

$$g \cdot \lambda(\varphi)(b) = \lambda(\varphi)(gb) = \varphi(g \cdot b)(1) = g \cdot (\varphi(b))(1)$$

where by $g \cdot \varphi$ we mean the action of G on $Hom(B, X)$. If $\lambda(\varphi) = 0$ then for all $b \in B$, $\varphi(b)(1) = 0$ so $\varphi(b)$ is the zero map. In particular $\varphi : B \to A$ is the zero map, so λ is injective. For surjectivity suppose

$\pi \in Hom(B, X)$ and define $\pi_b : \mathbb{Z}[G] \to X$ by $\pi_b(g) = \pi(gb)$. To see that $\pi_b \in Hom(\mathbb{Z}[G], X)$ we compute

$$\pi_b(mg_1 + ng_2) = \pi((mg_1 + ng_2)b) = \pi(mg_1 b) + \pi(ng_2 b) = \pi_b(mg_1) + \pi_b(ng_2)$$

A similar computation

$$\pi_{gb_1+b_2}(g') = \pi(g'(gb_1 + b_2)) = \pi_{gb_1}(g') + \pi_{gb_2}(g')$$

indicates that $\varphi : b \mapsto \pi_b$ is a G-module homomorphism with $\lambda(\varphi)(b) = \pi_b(1) = \pi(b)$; hence the claim.

In this case the complex $\mathcal{C}$ would be

$$0 \to Hom(\mathbb{Z}, X) \xrightarrow{\delta_0} Hom(P_0, X) \xrightarrow{\delta_1} Hom(P_1, X) \xrightarrow{\delta_2} \cdots$$

which is exact at every position because the P_i are free as abelian groups. This establishes the existence of at least one cohomological extension.

For uniqueness consider the G-module $\tilde{A} = Hom_G(\mathbb{Z}[G], A)$. By proposition 2.4 we have an exact sequence

$$0 \to A \to \tilde{A} \to \frac{\tilde{A}}{A} \to 0$$

Since $\tilde{A}$ was coinduced the sequence 2.2 becomes

$$0 \to H^q(G, \frac{\tilde{A}}{A}) \xrightarrow{d_q} H^q(G, A) \to 0$$

so the homomorphisms $d_q : H^q(G, \frac{\tilde{A}}{A}) \to H^{q+1}(G, A)$ are in fact isomorphisms for all $q \geq 1$. In particular we have a formula for $H^1(G, A)$

$$H^1(G, A) \simeq CoKer(H^0(G, \tilde{A}) \to H^0(G, \frac{\tilde{A}}{A}))$$

Since all potentail constructions must agree for $q = 0$ we can now inductively and uniquely define all cohomology groups. □

Note that the construction in theorem 2.1 can be repeated using any free resolution of the G-module $\mathbb{Z}$. The Standard complex is a convenient choice.

2.3. COHOMOLOGY IN LOW DIMENSIONS.

Proposition 2.6. *Let $f \in Hom_G(P_q, A)$ i.e $f : G^{q+1} \to A$ s.t. $f(gg_0, gg_1 \cdots, gg_i) = gf(g_0, \cdots, g_i)$. Then f is completely determined by its values on elements of the form $(1, g_1, g_1g_2, \cdots, g_1 \cdots g_q)$.*

Proof. Given $(g_0, g_1, \cdots, g_i)$ let $g_0' = g_0^{-1}$, $g_1 = g_0^{-1}g_1$, $g_2' = g_1^{-1}g_2$ etc. then

$$f(g_0, g_1, \cdots, g_q) = g_0 f(1, g_1', g_1'g_2', \cdots g_1' \cdots g_q')$$

□

So any $f \in Hom_G(P_q, A)$ can be thought of as a map from $G^q \to A$ by factoring out the first coordinate. Let $\phi(g_1, \cdots, g_q) = f(1, g_1, g_1g_2, \cdots, g_1 \cdots g_q)$. Then if we denote $\phi \circ \delta_{q+1} : P_{q+1} \to P_q \to A$ by $\delta\phi$ then we have

$$\delta\phi(g_1, \cdots, g_{q+1}) = g_1\phi(g_2, \cdots, g_{q+1}) + \sum_{j=1}^{q}(-1)^j \phi(g_1, \cdots, g_j, g_{j+1}, \cdots, g_{q+1}) + (-1)^{q+1}\phi(g_1, \cdots, g_q) \tag{2.4}$$

From 2.4 we can deduce the following useful propositions.

Proposition 2.7. *A 1-cocycle is a map $f : G \to A$ satisfying the following identity*

$$f(gg') = g \cdot f(g') + f(g) \tag{2.5}$$

Moreover f is a coboundary if there exists an $a \in A$ s.t.

$$f(g) = g \cdot a - a \tag{2.6}$$

Proposition 2.8. *A 2-cocyle is a map $f : G \times G \to A$ satisfying the following identity*

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

Proposition 2.9. *If G acts trivially on A then $H^1(G, A) = Hom(G, A)$.*

Proof. Apply proposition 2.7 so $f(gg') = f(g) + f(g')$. □

2.4. **COMPATIBLE MAPS.** Let $f : G \to G'$ be a group homomorphism and let A, A' be G, G' modules respectively. Then one can make A' into a G module by letting $g \cdot a' = f(g) \cdot a'$ for $g \in G$ and $a' \in A'$. Let $g : A' \to A$ be a homomorphism of abelian groups. We say f and g are compatible maps if g is a G-homomorphism when we treat A' as a G-module. More specifically if $\tilde{g} \in G$ and $a' \in A'$ then

$$g(f(\tilde{g}) \cdot a') = \tilde{g} \cdot g(a')$$

By a small abuse of notation we can define $f : \mathbb{Z}[G^{q+1}] \to \mathbb{Z}[G'^{q+1}]$ by letting f act coordinate wise. If $\phi \in Hom_{G'}(\mathbb{Z}[G'^{q+1}], A')$ then $g \circ \phi \circ f \in Hom_G(\mathbb{Z}[G^{q+1}], A)$ thus the pair (f, g) induce a map between

the standard complexes of (G, A) and (G', A'). To see that this map extends to a well defined map on the homology groups we verify that the following diagram commutes

$$\begin{array}{ccc} Hom_G(\mathbb{Z}[G^{q+1}], A) & \xrightarrow{\delta_q} & Hom_G(\mathbb{Z}[G^q], A) \\ \uparrow_{(f,g)} & & \uparrow_{(f,g)} \\ Hom_{G'}(\mathbb{Z}[G'^{q+1}, A') & \xrightarrow{\delta'_q} & Hom_{G'}(\mathbb{Z}[G'^{q}, A') \end{array} \tag{2.7}$$

In 2.7 we abuse notation by letting (f, g) denote the appropriate homomorphisms for any q. If $\phi \in Hom_{G'}(\mathbb{Z}[G'^{q+1}], A')$ such that $\delta'_q(\phi) = 0$ then, since g is a homomorphism of abelian groups, one has

$$\begin{aligned} \delta_q \circ (g \circ \phi \circ f) =& \sum_{j=0}^{q} (-1)^q (g \circ \phi \circ f)(g_0, \cdots, g_{j-1}, g_{j+1}, \cdots, g_q) \\ =& g\left(\sum_{j=0}^{q} (-1)^j \phi(f(g_0), \cdots, f(g_{j-1}), f(g_{j+1}), \cdots, f(g_q)) \right) \\ =& 0 \end{aligned}$$

For the cohomology group H^0 one notes that $g(A'^G) \subset A^G$, hence there is a homomorphism $H^0(G', A') \xrightarrow{(f,g)} H^0(G, A)$. We now have a sequence of maps

$$(f, g) : H^q(G', A') \to H^q(G, A) \; q \geq 0$$

The map (f, g) is induced by f and g.

2.5. **INFLATION AND RESTRICTION.**

Definition 2.9. Let $H \subset G$ be a subgroup of G and let $f : H \hookrightarrow G$ be the inclusion map. Then f and the identity map on A are compatible. The induced homomorphism

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

is called the restricition homomorphism.

Definition 2.10. Let $H \subset G$ be a normal subgroup of G. Then the group $A^H \subset A$ is a $\frac{G}{H}$-module and the homomorphisms $G \to \frac{G}{H}$ and $A^H \hookrightarrow A$ are compatible. The induced homomorphism

$$Inf : H^q(\frac{G}{H}, A^H) \to H^q(G, A)$$

is called the inflation homomorphism.

Proposition 2.10. *For any $t \in G$ let $f_t : G \to G$ be the inner automorphism $s \mapsto tst^{-1}$. Let $g_t : A \to A$ be the map $a \mapsto t^{-1}a$ which is a homorphism of abelian groups. Then these two maps are compatible and the induced map $(f_t, g_t) : H^q(G, A) \to H^q(G, A)$ is equal to the identity.*

Proof. It's easy to see that the maps are compatible. To show that (f_t, g_t) is the identity we proceed by induction on q with the case $q = 0$ being trivial.

Let $\tilde{A}$ be a co-induced module in which A is embedded (cf. proposition 2.4). Let $B = \frac{\tilde{A}}{A}$ so one has an exact sequence

$$0 \to A \to \tilde{A} \to B \to 0$$

Therefore the following diagram has exact rows

$$\begin{array}{ccccc} H^q(G,B) & \xrightarrow{d_q} & H^{q+1}(G,A) & \to & 0 \\ \downarrow{\scriptstyle (f_t,g_t)} & & \downarrow{\scriptstyle (f_t,g_t)} & & \\ H^q(G,B) & \xrightarrow{d_q} & H^{q+1}(G,A) & \to & 0 \end{array}$$

Since $(f_t, g_t) : H^q(G, B) \to H^q(G, B)$ is the identity by assumption and the d_q are surjective it follows that

$$(f_t, g_t) : H^{q+1}(G, A) \to H^{q+1}(G, A)$$

is the identity. □

Proposition 2.11. *Let $H \subset G$ be a normal subgroup. Then the following sequence is exact,*

$$0 \to H^1(\frac{G}{H}, A^H) \xrightarrow{Inf} H^1(G, A) \xrightarrow{Res} H^1(H, A)$$

Proof. We first show exactness at $H^1(\frac{G}{H}, A^H)$. Let $f : \frac{G}{H} \to A^H$ be a cocycle equivalent to zero in $H^1(G, A)$. Then by equation 2.6 there exists an $a \in A$ s.t. for all $g \in G$, $Inf(f)(g) = ga - a$. For f to be a coboundary in $H^1(\frac{G}{H}, A^H)$ it suffices to show that $a \in A^H$. We know $Inf(f)(g)$ depends only on g modulo H so for any $h \in H$, $Inf(f)(gh) = Inf(f)(g)$. In particular $ga - a = gha - a$ hence $ha = a$ and so $a \in A^H$.

Next we show $Res \circ Inf = 0$. Let $f \in Im(Inf)$ so there exists an f' such that $f : G \to \frac{G}{H} \xrightarrow{f'} A^H \to A$. For $Res(f) = 0$ we need $f(h) = 0$ for any $h \in H$. We know $f(g)$ only depends on g modulo H. In particular if $h \in H$ and $1 \in G$ is the identity then

$$f(h) = f(1) = f(1 \cdot 1) = 1 \cdot f(1) + f(1)$$

so $f(1) = 0$ and therefore $f(h) = 0$.

It remains to show $Ker(Res) \subset Im(Inf)$. Let $f : G \to A$ be a cocyle s.t. $Res(f) = 0$ i.e. there exists an $a \in A$ s.t. for all $h \in H$, $f(h) = ha - a$. We want to show that f is the inflation of a map from $\frac{G}{H} \to A^H$. Recalling that H^1 is a quotient group, WLOG we can subtract f from the coboundary $\lambda : G \to A$ defined by $\lambda(g) = ga - a$. Therfore we may assume $f(h) = 0$, for all $h \in H$.

If $h \in H$ and $g \in G$ then by equation 2.5 $f(gh) = f(g) + gf(h)$ and so $f(gh) = f(g)$. Hence, f passes to a well defined map on $\frac{G}{H}$. It remains to show that the range of f is contained in A^H.

H is normal i.e. $gH = Hg$ so $f(gh) = f(hg)$. Using this fact and applying 2.5 again we have

$$\begin{aligned} f(g) = f(hg) =& hf(g) + f(h) \\ =& hf(g) \end{aligned}$$

which implies $f(g) \in A^H$. □

Proposition 2.12. *Let $q > 1$ and suppose that $H^i(H, A) = 0$ for all $1 \leq i \leq q - 1$. Then the following sequence is exact:*

$$0 \to H^q(\frac{G}{H}, A^H) \xrightarrow{Inf} H^q(G, A) \xrightarrow{Res} H^q(H, A)$$

Proof. Having established the result for $q = 1$ in proposition 2.11, we proceed by strong induction on q. Let $\tilde{A} = Hom(\mathbb{Z}[G], A)$ be the canonical co-induced module of A of proposition 2.4 and let $B = \frac{\tilde{A}}{A}$. We have an exact sequence

$$0 \to A \to \tilde{A} \to B \to 0 \tag{2.8}$$

We can write $\mathbb{Z}[G] = \oplus_{\sigma \in \frac{G}{H}} \mathbb{Z}[H] \cdot \sigma$ i.e. $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$ module. One has a $\mathbb{Z}$-bilinear map from $\mathbb{Z}[H] \times \mathbb{Z}[\frac{G}{H}] \to \mathbb{Z}[G]$ which factors to a map $\mathbb{Z}[H] \otimes \mathbb{Z}[\frac{G}{H}] \to \mathbb{Z}[G]$. In particular, we can write $\mathbb{Z}[G] = \mathbb{Z}[H] \otimes_{\mathbb{Z}} M$ where M is some abelian group. Therefore

$$\tilde{A} = Hom(\mathbb{Z}[G], A) = Hom(\mathbb{Z}[H] \otimes M, A) = Hom(\mathbb{Z}[H], Hom(M, A))$$

Note that $\tilde{A}$ is co-induced as an H module. We also have two other important observations. Firstly, since $H^1(G, A) = 0$ by hypothesis, theorem 2.1 implies we have an exact sequence

$$0 \to A^H \to \tilde{A}^H \to B^H \to 0 \tag{2.9}$$

Secondly, $\tilde{A}^H = Hom(\mathbb{Z}[\frac{G}{H}], A)$ is a co-induced $\frac{G}{H}$ module.

We can combine 2.8 and 2.9 to get a diagram

$$\begin{array}{ccccccc} 0 & \to & H^{q-1}(\frac{G}{H}, B^H) & \to & H^{q-1}(G,B) & \to & H^{q-1}(H,B) \\ & & \downarrow d_{q-1} & & \downarrow d_{q-1} & & \downarrow d_{q-1} \\ 0 & \to & H^q(\frac{G}{H}, A^H) & \to & H^q(G,A) & \to & H^q(H,A) \end{array} \tag{2.10}$$

The fact that it is commutative follows from properties of the connecting homomorphisms d_{q-1}, an explicit description of which can be found in [13] §6.1. As we have noted, $\tilde{A}$ is co-induced as a G module and as an H module. Moreover $\tilde{A}^H$ is coinduced as a $\frac{G}{H}$ module. So the rows above and below the diagram are zero, indicating that the maps d_{q-1} are in fact isomorphisms. As such, the theorem will follow if the top row of 2.10 is exact.

If $1 \leq i \leq q-1$ then $H^i(H, \tilde{A}) = 0$ since $\tilde{A}$ is a co-induced H module. Moreover we have assumed that $H^i(H, A) = 0$, so applying $H^i(H, -)$ to sequence 2.8 indicates that $H^i(H, C) = 0$ for $1 \leq i \leq q-2$. In particular C satisfies the strong induction hypothesis (for $q-1$ in place of q), and therefore the top row of 2.10 is exact. □

2.6. **CUP PRODUCTS.** We state as a theorem the basic properties of the cup product though we will omit the tedious proof. We will however describe the cup product explicitly in terms of cocycles.

It's worth noting that the cup product factors through the tensor product of $H^p(G, A)$ and $H^q(G, B)$ however the convention is to write the cup product in terms of the cartesian product. For the remainder of this thesis all tensor products are over $\mathbb{Z}$ unless otherwise indicated.

Theorem 2.2. *Let G be a finite group, $p, q \geq 0$ integers and let A, B be G-modules. Then there exists one and only one family of homomorphisms*

$$H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

denoted $(a \times b) \to a \cup b$ satisfying the following properties

(i) These homomorphisms are functorial in A and B i.e. the cup product is a morphism of functors when considered as a covariant bifunctor in (A, B).

(ii) For $p = q = 0$ they are induced by the product

$$A^G \otimes B^G \to (A \otimes B)^G$$

(iii) If $0 \to A \to A' \to A'' \to 0$ is exact and if $0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$ is exact then for all $a'' \in H^q(G, A'')$ and $b \in H^q(G, B)$ one has

$$(d_p a'') \cup b = d_{p+q}(a'' \cup b) \in H^{p+q+1}(G, A \otimes B)$$

(iv) If $0 \to B \to B' \to B'' \to 0$ *is exact and if* $0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$ *is exact then for* $a \in H^q(G, A)$ *and* $b'' \in H^q(G, B'')$ *one has*

$$a \cup (d_q b'') = (-1) d_{p+q}(a \cup b'') \in H^{p+q+1}(G, A \otimes B)$$

Proof. [5] §4.7 □

Consider 2.1, the standard resolution. Let $\varphi_{p,q} : P_{p+q} \to P_p \otimes P_q$ be the map

$$(g_0, g_1, \cdots, g_{p+q}) = (g_0, \cdots, g_p) \otimes (g_p, \cdots, g_{p+q})$$

Then for all p, q we have

$$\varphi_{p,q} \circ \delta_{p+q} = (\delta_{p+1} \otimes 1) \circ \varphi_{p+1,q} + (-1)^p (1 \otimes \delta_{q+1}) \circ \varphi_{p,q+1} \tag{2.11}$$

$$(\delta_0 \otimes \delta_0) \circ \varphi_{0,0} = \delta_0 \tag{2.12}$$

Let $f \in Hom_G(P_p, A)$ and $g \in Hom_G(P_q, B)$ be cocycles and define $f \cup g \in Hom_G(P_{p+q}, A \otimes B)$ by

$$f \cup g = (f \otimes g) \circ \varphi_{p,q} \tag{2.13}$$

Then 2.11 and 2.12 imply that

$$(f \cup g) \circ \delta_{p+q} = (f \circ \delta_{p+1}) \cup g + (-1)^p f \cup (g \circ \delta_{q+1}) \tag{2.14}$$

Equation 2.14 indicates that if f and g are cocycles then so too is $f \cup g$. It can be shown that the product 2.13 is independent of the choices of f and g modulo a coboundary. Thus we have a well defined homomorphism

$$H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

3. APPLICATIONS OF GROUP COHOMOLOGY TO GALOIS THEORY

For this section we will let let K be a finite Galois extension of k with $G = Gal(\frac{K}{k})$.

3.1. **ACTIONS OF GALOIS GROUPS.** We can treat K with addition as a G-module by letting $g \cdot c = g(c)$ where $g \in G$ and $c \in K$.

Proposition 3.1. *If by* K *we mean* K *with addition then* $H^q(G, K) = 0$ *for all* $q \geq 1$.

Proof. We will show that $K \simeq Hom(\mathbb{Z}[G], K)$ by proving two statements.

(1) $Hom(\mathbb{Z}[G], K) \simeq \mathbb{Z}[G] \otimes K$
(2) $\mathbb{Z}[G] \otimes K \simeq K$

We give $\mathbb{Z}[G] \otimes K$ a G module structure by $g \cdot (h \otimes x) = gh \otimes x$ for $g, h \in G$ and $x \in K$.

For statement (1) let $\varphi \in Hom(\mathbb{Z}[G], K)$ and consider $\lambda(\varphi) = \sum_{s \in G} s \otimes \varphi(s) \in \mathbb{Z}[G] \otimes K$. λ is clearly a G-module homorphism. For any given element $s \otimes x$ we have the map φ with $\varphi(s) = x$ and $\varphi(s') = 0$ for $s' \neq s$. Observe that for such a φ, $\lambda(\varphi) = s \otimes \varphi(s)$ so λ is surjective. To see the map is injective note that each $1s \in \mathbb{Z}[G]$ is linearly independent over $\mathbb{Z}$ so if $\sum_{s \in G} s \otimes \varphi(s) = 0$ then each $\varphi(s) = 0$ i.e. $\varphi = 0$.

For statement (2) let K be an n-dimensional vector space over k. We can choose a normal basis for K i.e. there exists some $x \in K$ such that if $\{\beta_i\}_{i=1}^n = G$ the set $\{\beta_i(x)\}_{i=1}^n$ is a basis for K. With this basis we can represent any element of K as an n-tuple $(k_1, \cdots, k_n)$.

Consider the map $\mathbb{Z}[G] \otimes K \to K$ given by

$$g \otimes (k_1, \cdots, k_n) \mapsto k_1 g\beta_1(x) + \cdots + k_n g\beta_n(x) \tag{3.1}$$

This map is clearly a G-module homorphism. The set $\{g\beta_i\}_{i=1}^n$ is linearly independent so if equation 3.1 is zero we must have $(k_1, \cdots, k_n) = 0$ or of course $g \in \mathbb{Z}[G]$ is the zero element. Hence the map is injective. The map is clearly surjective by considering the image $1 \otimes (k_1, \cdots, k_n)$ for any $(k_1, \cdots, k_n) \in K$.

We have established that K is coinduced, hence its cohomology groups are trivial for $q \geq 1$. □

In light of proposition 3.1 we are nearly always concerned with the G module $K^\times$. For the remainder of this section by $H^q(G, K)$ we will mean the module $K^\times$ with group operation given by field multiplication and G action given by $g \cdot c = g(c)$ for $g \in G$, $c \in K^\times$.

Proposition 3.2. $H^1(G, K) = 0$

Remark 3.1. Throughout this proof we will let $\cdot$ denote field multiplication in $K^\times$

Proof. Let $\psi \in: G \to K^\times$ be a 1-cocycle and fix some $s \in G$ and $c \in K^\times$. Consider the following element in K

$$b = \sum_{t \in G} \psi(t) \cdot t(c) \tag{3.2}$$

Since automorphisms are linearly independent ([4], Chapter 5, §10) and each $\psi(t)$ is nonzero we deduce that $b \neq 0$. Applying s to b gives

$$s(b) = \sum_{t \in G} s(\psi(t)) \cdot s(t(c)) \tag{3.3}$$

By equation 2.5 we know $\psi(st) = s(\psi(t)) \cdot \psi(s)$ hence $\psi(t) = s^{-1}(\psi(st) \cdot \psi(s)^{-1})$. Substituting this into 3.3 gives

$$s(b) = \sum_{t \in G} \psi(st) \cdot \psi(s)^{-1} \cdot s(t(c)) = \psi(s)^{-1} \sum_{t \in G} \psi(st) \cdot st(c) \tag{3.4}$$

But the map $t \mapsto st$ is a bijection on G so summing over $st \in G$ is the same as summing over $t \in G$. Equation 3.4 becomes

$$s(b) = \psi(s)^{-1} \cdot b$$

hence $\psi(s) = s(b)^{-1} \cdot b = s(b^{-1}) \cdot (b^{-1})^{-1}$ which is just equation 2.6 in multiplicative notation. □

3.2. HILBERT'S THEOREM 90.

Theorem 3.1. *(Hilbert's Theorem 90): Suppose G is cyclic, $s \in G$ is a generator and $x \in K^\times$. Then x has norm equal to 1 if and only if there exists $y \in K^\times$ such that $x = ys(y)^{-1}$.*

Proof. Suppose $x = ys(y)^{-1} = ys(y^{-1})$ and let $N_{K/k}$ denote the norm on K/k. Suppose $|G| = n$. Then since s is a generator

$$N_{K/k}(x) = xs(x)s^2(x) \cdots s^{n-1}(x) = ys(y)^{-1}[s(y)s^2(y)^{-1}][s^2(y)s(y)^{-2}] \cdots [s^{n-1}(y)s(y)^{-(n-1)}] = yy^{-1} = 1$$

Conversely suppose that $N_{K/k}(x) = 1$. Define $\psi : G \to K$ by

$$\psi(s^l) = \prod_{i=0}^{l-1} s^i(x),\ l \geq 1$$

This is well defined since the norm $\prod_{i=0}^{n-1} s^i(x) = 1$.

$$\psi(s^l s^r) = \psi(s^{l+r}) = \left[\prod_{i=0}^{l-1} s^i(0)\right] \left[\prod_{i=l}^{l+r-1} s^i(x)\right] = \psi(s^l)s^l(\psi(s^r))$$

which shows that ψ is a cocycle. By proposition 3.2 there exists a $b \in K^\times$ such that $\psi(s^i) = s^i(b)b^{-1}$for all $i \geq 1$. In particular for $i = 1$, $x = \psi(x) = \frac{s(b)}{b} = \frac{b^{-1}}{s(b^{-1})}$. □

The proof of theorem 3.1 depends crucially on proposition 3.2. Using proposition 3.1 we automatically get a variation of Hilbert 90 in additive form.

Theorem 3.2. *Suppose G is cyclic, $s \in G$ is a generator and $x \in K$. Then x has trace equal to 0 if and only if there exists a $y \in K$ such that $x = y - s(y)$.*

3.3. **ARTIN-SCHREIER THEORY.** For the purposes of this subsection, suppose that $char(k) = p \neq 0$.

Theorem 3.3. *(Artin-Schreir):*

1. *Let K be a cyclic extension of k of degree p. Then there exists $a, \alpha \in K$ such that $K = k(\alpha)$ and $\alpha^p - \alpha - a = 0$.*
2. *Conversely, given $a \in k$, $f(X) = X^p - X - a \in k[X]$ has either all roots in k or is irreducible. If $f(X)$ is irreducible and if α is a root then $k(\alpha)$ is the splitting field of f and the Galois group is cyclic of degree p.*

Proof. We start with 1. Since K is cyclic of degree p and each element of $Gal(\frac{K}{k})$ fixes -1 we have $Tr_{K/k}(-1) = 0$. Let $s \in G$ be a generator, then theorem 3.2 tells us there exists $\alpha \in K$ such that $-1 = \alpha - s(\alpha)$ which implies $s(\alpha) = \alpha + 1$. Hence $s^i(\alpha) = \alpha + i$ for the integers $i \in \{0, 1, \cdots, p-1\}$. So α has p-distinct conjugates which implies

$$[k(\alpha) : k] \geq p \text{ therefore } K = k(\alpha)$$

Moreover

$$s(\alpha^p - \alpha) = s(\alpha)^p - s(\alpha) = (\alpha + 1)^p - (\alpha + 1) = \alpha^p - \alpha \tag{3.5}$$

So $\alpha^p - \alpha$ is fixed by G and so $\exists a \in k$ such that $a = \alpha^p - \alpha$. This finishes the proof part 1.

Now suppose $a \in k$. A similar computation to 3.5 shows that if α is a root of $f(X) = X^p - X - a \in k[X]$ then so too is $\alpha + i$ for $i \in \{1, \cdots, p-1\}$. Hence if one root lies in k so do all roots.

Next, assume no roots of f lie in k. We claim f is irreducible.

Assume one could write

$$f(X) = g(X)h(X) \text{ where } 1 \leq deg(g) < p \tag{3.6}$$

Since $f(X) = \prod_{i=1}^{p}(X - \alpha - i)$ we know that g must be a product over certain integers of the monomials $(X - \alpha - i)$. Let $deg(g) = d$. Then the coefficient of X^{d-1} of g would be $(-d\alpha + j)$ for some integer j. But we've assumed $d \neq 0$ and that the coefficients of g lie in k, thus $\alpha \in k$, giving the required contradiction.

In particular f splits over $k(\alpha)$, so $k(\alpha)$ is the splitting field for f. f has no repeated roots so $|Gal(\frac{K}{k})| = [K : k] = deg(f) = p$, hence $Gal(\frac{K}{k})$ is a cyclic group of order p. □

For the remainder of this subsection let K be the separable closure of k. Using the tools of group cohomology we aim to describe the group $Hom(G, \frac{\mathbb{Z}}{p\mathbb{Z}})$ entirely in terms of the base field k. We will need a few simple results first.

Lemma 3.1. *The map $\mathcal{P} : K \to K$ defined by $x \mapsto x^p - x$ is a surjective G-homomorphism.*

Proof. That $\mathcal{P}$ is a G-homomorphism is obvious. For surjectivity, let $a \in K$ and consider the polynomial $f(X) = X^p - X - a \in K[X]$. We know from theorem 3.3 that this polynomial is separable with splitting field given by adoining one root, say α. In particular $k(\alpha)$ is a separable extension hence $k(\alpha) \subset K$. □

Theorem 3.4. $Hom(G, \frac{\mathbb{Z}}{p\mathbb{Z}}) = \frac{\mathcal{P}(k)}{k}$.

Proof. As we saw in the proof 3.3 we know that the solutions to the equation $X^p - X = 0$ are $0, 1, \cdots, p-1$. Hence $ker(\mathcal{P}) \simeq \frac{\mathbb{Z}}{p\mathbb{Z}}$. Therefore one has an exact sequence

$$0 \to \frac{\mathbb{Z}}{p\mathbb{Z}} \to K \xrightarrow{\mathcal{P}} K \to 0 \tag{3.7}$$

Taking cohomology groups and noting that $K^G = k$ 3.7 gives an exact sequence,

$$0 \to H^0(G, \frac{\mathbb{Z}}{p\mathbb{Z}}) \to H^0(G, K) \xrightarrow{\mathcal{P}} H^0(G, K) \xrightarrow{d_0} H^1(G, \frac{\mathbb{Z}}{p\mathbb{Z}}) \to H^1(G, K) \to \cdots$$

since $ker(\mathcal{P}) \subset k$ the action G on $ker(\mathcal{P})$ is trivial. This fact, along with propositions 3.2 and 2.9 gives an exact sequence

$$k \xrightarrow{\mathcal{P}} k \xrightarrow{d_0} Hom(G, \frac{\mathbb{Z}}{p\mathbb{Z}}) \to 0$$

□

We remarked that the solutions to the equation $X^p - X = 0$ are $0, 1, \cdots, p$. This is a restatement of Fermat's little theorem.

3.4. BRAUER GROUPS.

Definition 3.1. Let K be a separable closure of k. We call $H^2(G, K)$ the Brauer group of k.

We state without proof that $H^2(G, K)$ is isomorphic to the Brauer group defined on the classes of central simple algebras over k. The Brauer group can be thought of as the projective limit of the groups $H^2(G, K)$ where K is any Galois extension of k. In preparation for this result we need the following proposition.

Proposition 3.3. *Let L be a Galois extension of k containing the Galois extension K of k, i.e. $L \supset K \supset k$. Let $G = Gal(L/k)$, $H = Gal(L/K)$. Then there is an exact sequence*

$$0 \to H^2(\frac{G}{H}, K^\times) \xrightarrow{Inf} H^2(G, L^\times) \xrightarrow{Res} H^2(H, L^\times)$$

Proof. By proposition 3.2 we know that $H^1(H, L^\times) = 0$ so the above is just an application of proposition 2.12 with $q = 2$. □

4. PROFINITE GROUPS

Definition 4.1. A topological group if called profinite if $G \simeq \varprojlim_{i\in\Lambda} G_i$ and each G_i is finite and discrete.

Theorem 4.1. *A topological group G is profinite if and only if it is Hausdorff, compact and totally disconnected.*

If $U \subset G$ is an open normal subgroup of G we will see that the quotient $\frac{G}{U}$ is a discrete finite group. G is the projective limit of these quotient groups. It is possible for a profinite group to be the limit of different projective systems, in particular the groups $\frac{G}{U}$ may form a different projective system to the groups denoted G_i in definition 4.1. However the groups G_i and $\frac{G}{U}$ both 'topologically generate' G in a sense that will be made precise in the next subsection and in lemma 4.4.

For section 4 and section 5 let G be a profinite group and $\underline{\mathrm{S}} = \{U \subset G | U \text{is an open normal subgroup}\}$. For convenience we write $\varprojlim \frac{G}{U}$ in place of $\varprojlim_{U\in\underline{\mathrm{S}}} \frac{G}{U}$ whenever it is obvious from the context that we are taking the projective limit over $\underline{\mathrm{S}}$.

4.1. PROOF OF THEOREM 4.1.

Lemma 4.1. *Let X be a compact, Hausdorff space. For any $x \in X$ let $\{U_q\}_{q\in Q}$ be the collection of compact, open sets containing x (where Q is an indexing set). Then $A = \bigcap_{q\in Q} U_q$ is connected.*

Proof. Observe that each U_q is compact and therefore closed so A is closed.

Suppose that $A = U \bigcup V$ where U, V are disjoint and clopen. Since X is compact Hausdorff it is necessarily a normal topological space so there exists $U \subset U'$ and $V \subset V'$ such that U', V' are open and disjoint. Since $A \subset U' \bigcup V'$ we know that $(X\backslash(U' \bigcup V')) \bigcap A = \emptyset$.

Moreover, the set $X\backslash(U' \bigcup V')$ is closed (hence compact) and is a subset of $X\backslash A = \bigcup_{q\in Q} X\backslash U_q$. In particular, the collection $\{X\backslash U_q\}_{q\in Q}$ form an open cover of $X\backslash(U' \bigcup V')$. Take a finite subcover $\{X\backslash U_q\}_{q\in Q'}$ then

$$X\backslash(U' \bigcup V') \subset \bigcup_{q\in Q'} X\backslash U_q = X\backslash \bigcap_{q\in Q'} U_q \text{ hence } \bigcap_{q\in Q'} U_q \subset U' \bigcap V' \tag{4.1}$$

Let $B = \bigcap_{q\in Q'} U_q$ then B is open and compact. So $x \in B$ and $B = (B \bigcup U') \bigcup (B \bigcup V')$. Suppose $x \in B \bigcap U'$ then since $B \bigcap U'$ is open and compact $A \subset B \bigcap U' \subset U'$ so that $A \bigcap V \subset A \bigcap V' = \emptyset$. □

Lemma 4.2. *Let G be a compact, Hausdorff and totally disconnected topological group. Then every neighbourhood of $1 \in G$ contains an open normal subgroup of finite index.*

Proof. Let $\{U_q\}_{q\in Q}$ be the collection of all compact, open neighbourhoods of 1 (where Q is an indexing set). Since the connnected component of $1 \in G$ is just $\{1\}$, by lemma 4.1 $\{1\} = \bigcap_{q\in Q} U_q$. Let U be a neighborhood of 1. Then $G\backslash U$ (complement) is closed (hence compact) and

$$G\backslash U \subset G\backslash\{1\} = G\backslash \bigcap_{q\in Q} U_q = \bigcup_{q\in Q} G\backslash U_q$$

so the collection $\{G\backslash U_q\}_{q\in Q}$ form an open cover of $G\backslash U$. Let $\{G\backslash U_q\}_{q\in Q'}$ be a finite subcover. Let $A = \bigcap_{q\in Q'} U_q$. We have that A is compact, open and a computation similar to equation 4.1 implies that $A \subset U$. Let $F = (G\backslash A)\bigcap A^2$. A^2 is compact (hence closed) and $G\backslash A$ is closed so F is closed.

Choose a symmetric neighborhood of 1, denoted V, such that $V \subset A$ and $AV\bigcap F = \emptyset$. Then since $AV \subset A^2$ we have $AV \subset A$ so for all $n \geq 0$, $AV^n \subset A$. Let $J = \bigcup_{n\geq 0} V^n \subset A$. Then J is an open subgroup contained in A. Since G is compact, J has finitely many cosets in G (note the cosets of J are open and cover G). We can then define an open normal subgroup with finite index contained in $J \subset A \subset U$

$$H = \bigcap_{x\in G} xJx^{-1} = \bigcap_{x\in \frac{G}{K}} xJx^{-1}$$

i.e. H is the intersection of the finitely many conugate subgroups of J. □

Lemma 4.3. *Let $\{X_{ij}, h_{ij}\}$ be a projective system of topological spaces. Let X be a topological space along with a set of compatible surjective maps $h_i : X \to X_i$ (i.e. $h_i = h_{ij} \circ h_j$). Then the image of X under the induced map $h : X \to \varprojlim X_i$ is dense in $\varprojlim X_i$.*

Proof. Consider open set that is part of the basis for the product topology on $\varprojlim X_i$

$$V = \varprojlim X_i \bigcap (\prod_{i\neq i_1,\cdots i_n} X_i \times U_{i_1} \times \cdots \times U_{i_n}) \text{ where the } U_{i_j} \text{are open for } 1 \leq j \leq n.$$

Let $i_0 > i_j$ for $j = 1, \cdots, n$ and let $(x_i)_{i\in\Lambda} \in V$ with x_{i_j} corresponding to the i_j coordinate. Then since $(x_i)_{i\in\Lambda} \in \varprojlim X_i$ we have $h_{i_j i_0}(x_{i_0}) = x_{i_j}$. Choose $y \in X$ such that $h_{i_0}(y) = x_{i_0}$ then $h(y) \in V$. □

We now proceed with the proof of theorem 4.1. First let G be compact, Hausdorff and totally disconnected. By lemma 4.2 the set $\underline{S}$ forms a neighbourhood basis for $1 \in G$. For each pair $U, V \in \underline{S}$ with $U \subset V$ consider the inclusion map passed into the quotient

$$\varphi_{U,V} : \frac{G}{U} \to \frac{G}{V}$$

We claim that $\{\frac{G}{U}, \varphi_{U,V} | U, V \in \underline{\mathrm{S}}\}$ is a projective system of topological groups. Indeed if $U \subset V \subset W$ then the map $\frac{G}{U} \to \frac{G}{W}$ is the same as the composition $\frac{G}{U} \to \frac{G}{V} \to \frac{G}{W}$ and clearly the inclusion $U \hookrightarrow U$ induces the identity map on $\frac{G}{U}$. If $U, V \in \underline{\mathrm{S}}$ then $U \bigcap V \subset U$, $U \bigcap V \subset V$ and $U \bigcap V$ is clearly open and normal. Moreover each $\frac{G}{U}$ is finite with the discrete topology. Ordering $\underline{\mathrm{S}}$ by reverse inclusion makes $\underline{\mathrm{S}}$ into a directed, partially ordered set (in the sense of appendix 5).

The projections $\varphi_U : G \to \frac{G}{U}$ are compatible with the $\varphi_{U,V}$ in the sense that if $U \subset V$ then $\varphi_V = \varphi_{U,V} \circ \varphi_U$. Hence we can define a map $\varphi : G \to \varprojlim \frac{G}{U}$. Clearly φ is a group homorphism and we further claim that φ is an isomorphism of topological groups.

If $\varphi(g) = 1$ then $g \in U$ for all $U \in \underline{\mathrm{S}}$ so $g \in \bigcap_{U \in \underline{\mathrm{S}}} U = \{1\}$ by the computations in lemma 4.2 and 4.1. $\varphi(G)$ is compact and dense (that later due to lemma 4.3). $\varprojlim \frac{G}{U}$ is Hausdorff since each $\frac{G}{U}$ is and $\varprojlim \frac{G}{U}$ is a subspace of the product space $\prod \frac{G}{U}$. Therefore the compact set $\varphi(G)$ is closed i.e. $\varphi(G) = \varprojlim \frac{G}{U}$. For continuity it suffices to show that the composite map

$$G \xrightarrow{\varphi} \varprojlim \frac{G}{U} \subset \prod_{\underline{\mathrm{S}}} \frac{G}{U} \xrightarrow{\pi_U} \frac{G}{U}$$

is continuous. This follows from the fact that $(\pi_U \circ \varphi)^{-1}\{1_{\frac{G}{U}}\} = U$ is open in G while lemma 4.2 tells us that $1_{\frac{G}{U}}$ is a basis of open neghbourhoods of the identity in $\frac{G}{U}$.

Conversely suppose that $G = \varprojlim G_i$ is a profinite group. We wish to show that G is compact, Hausdorff and totally disconnected. First we claim that $\varprojlim G_i \subset \prod_{i \in \Lambda} G_i$ has the subspace topology induced from $\prod_{i \in \Lambda} G_i$. Let $\pi_j : \prod_{i \in \Lambda} G_i \to G_j$ and $\mu_j : \varprojlim G_i \to G_j$ be the canonical projections for some fixed $j \in \Lambda$. Then $\prod_{i \in \Lambda} G_i$ and $\varprojlim G_i$ have the initial topology given by the π_j and μ_j respectively. Since $\mu_j = \pi_j|_{\varprojlim G_i}$ the claim follows.

Next it's clear that $\varprojlim G_i \subset \bigcap_{i \in \Lambda} \pi_i^{-1}(\mu_i(\varprojlim G_i))$. For the reverse inclusion suppose $(g_i) \in \prod_{i \in \Lambda} G_i$ and $g_i = \mu_i(h_i)$ for $(h_i) \in \varprojlim G_i$. Then by definition of μ_i, for each $i \in \Lambda$ we have $h_i = g_i$ which implies$(g_i) \in \varprojlim G_i$. Hence $\varprojlim G_i = \bigcap_{i \in \Lambda} \pi_i^{-1}(\mu_i(\varprojlim G_i))$.

Each $\mu_i(\varprojlim G_i)$ is closed since G_i is discrete. Therefore $\varprojlim G_i$ is closed. Since the product space $\prod_{i \in \Lambda} G_i$ is compact, Hausdorff and totally disconnected it follows that $\varprojlim G_i$ is as well.

Remark 4.1. Let $\underline{\mathrm{T}} \subset \underline{\mathrm{S}}$ be a collection of open normal subgroups of G that form a basis of open neighborhoods of 1. Then our construction of G indicates that $\varprojlim_{U \in \underline{\mathrm{T}}} \frac{G}{U} \simeq \varprojlim_{U \in \underline{\mathrm{S}}} \frac{G}{U} \simeq G$. In detail, since $\bigcap_{U \in \underline{\mathrm{T}}} U = \{1\}$ the map $G \to \varprojlim_{U \in \underline{\mathrm{T}}} \frac{G}{U}$ is injective with dense image i.e. bijective. It's continuous since the $\underline{\mathrm{T}}$ form a basis for the topology at $1 \in G$.

4.2. **SUBGROUPS OF PROFINITE GROUPS.** The construction in the previous subsection demonstrated that a profinite group can be written as the projective limit of the quotients of its open normal subgroups. In fact we loose little information by thinking of all profinite groups in this way.

Lemma 4.4. *Let $G = \varprojlim G_i$ be a profinite group with $i \in \Lambda$. Then*

$$\underline{T} = \{Ker(G \to G_i) \,|i \in \Lambda\}$$

is a basis of open neighborhoods of $1 \in G$.

Proof. Since each G_i is finite $\{1_i\} \subset G_i$ is a basis of open neighborhoods in G_i. Hence the neighborhoods of $1 \in G$ of the form

$$(\prod_{i \neq i_1,\cdots,i_n} G_i \times \{1_{i_1}\} \times \cdots \{1_{i_n}\}) \bigcap G = \bigcap_{i=i_1,\cdots,i_n} ker(G \to G_i)$$

are a basis of open neighborhoods of $1 \in G$. Choose $i_0 > i_1, \cdots, i_n$ then

$$ker(G \to G_{i_0}) \subset \bigcap_{i=i_1,\cdots,i_n} ker(G \to G_i)$$

□

In particular we can always write $G = \varprojlim_{U \in \underline{S}} \frac{G}{U}$ so lemma 4.4 confirms that the kernels of the projection maps (in this case the open normal subgroups) form a neighborhood basis for $1 \in G$.

Proposition 4.1. *Let $H \subset G$ be a closed subgroup of a profinite group G. Then H is profinite and if $G = \varprojlim \frac{G}{U}$ then*

$$H = \varprojlim \frac{HU}{U} = \varprojlim \frac{H}{H \bigcap U} \tag{4.2}$$

Proof. H is compact, Hausdorff and totally disconnected; therefore it is profinite. Each $\frac{H}{H \bigcap U}$ is finite, hence $\varprojlim \frac{H}{H \bigcap U}$ is profinite; in particular it is a projective system of topological spaces. The projection maps $\pi : H \to \frac{H}{H \bigcap U}$ are continuous and as was noted in the proof of theorem 4.1 they are compatible with the projective system $\{\frac{H}{H \bigcap U} | U \in \underline{S}\}$. By lemma 4.3 under the map

$$H \to \varprojlim \frac{H}{H \bigcap U}$$

H has dense image. Moreover, each $H \bigcap U$ is closed (because each U is closed) so $\frac{H}{H \bigcap U}$ is Hausdorff. This fact along with the compactness of H implies that this map is is a homeomorphism. □

Proposition 4.2. *If $H \subset G$ is a closed normal subgroup then $\frac{G}{H}$ is profinite with $\frac{G}{H} = \varprojlim \frac{G}{HU}$ where $U \in \underline{S}$.*

Proof. $\frac{G}{H}$ is compact and each $\frac{G}{HU}$ is discrete and finite. As in proposition 4.1 we have a collection of projection maps $\frac{G}{H} \to \frac{G}{HU}$ that are compatible with the projective system $\{\frac{G}{HU} | U \in \underline{S}\}$. Another application of lemma 4.3 tells us that $G \to \varprojlim \frac{G}{HU}$ is a homeomorphism. □

Proposition 4.3. *If $\{G_i\}_{i\in\Lambda}$ is a collection of profinite groups then $\prod_{i\in\Lambda} G_i$ is profinite.*

Proof. The product is compact, Hausdorff and totally disconnected. □

Proposition 4.4. *If $\{G_i\}_{i\in\Lambda}$ is a projective system of profinite groups then $\varprojlim G_i$ profinite.*

Proof. Note that $\prod_{i\in\Lambda} G_i$ is compact, Hausdorff and totally disconnected. Moreover $\varprojlim G_i$ is a projective limit of compact spaces so it is again compact ([2] Chapter 1, §9.6). Hence it is a closed subset of $\prod_{i\in\Lambda} G_i$ so it must also be Hausdorff and totally disconnected. □

To tackle the main theorem in this subsection we need a simple variation on lemma 4.3.

Lemma 4.5. *Let $\{S_i\}_{i\in\Lambda}$ be a decreasing filtration of closed subgroups of G. Then the $\{\frac{G}{S_i}\}$ form a projective system by inclusion and if $S = \bigcap S_i$ then the maps $\frac{G}{S} \to \frac{G}{S_i}$ are compatible with the system. In particular the map*

$$\frac{G}{S} \to \varprojlim \frac{G}{S_i}$$

is a homeomorphism.

Proof. If $x \in G$ is equivalent to the identity in $\frac{G}{S}$ then since $S \subset S_i$ for all $i \in \Lambda$, so x will be the equivalent to the identity in $\frac{G}{S_i}$. The map has dense image by lemma 4.3 and since G is compact so too is $\frac{G}{S}$. Each S_i is closed so $\frac{G}{S_i}$ is Hausdorff which implies $\varprojlim \frac{G}{S_i}$ is Hausdorff. This is enough to establish that the image of $\frac{G}{S}$ is equal to its closure and that the map is a homeomorphism. □

Theorem 4.2. *Let $K \subset H \subset G$ be closed subgroups of G. Then there exists a continuous section $\sigma : \frac{G}{H} \to \frac{G}{K}$ i.e. if $\pi : \frac{G}{K} \hookrightarrow \frac{G}{H}$ is the inclusion map passed to the quotient then $\pi \circ \sigma = id_{\frac{G}{H}}$.*

It's worth noting that by proposition 4.1, we could restate theorem 4.2 with K and H as profinite subgroups instead of closed subgroups.

Proof. We divide the proof into two parts.

First suppose that $\frac{H}{K}$ is finite.

H, K are closed so $H\backslash K$ (complement) is open in the subspace topology of H. Since K is of finite index in H we can write

$$K = \bigcap_{g \in \frac{H}{K} \backslash \{1\}} L_g(H\backslash K) \text{ where } L_g \text{is left translation by } g \in G$$

which is open in H. By proposition 4.1 H and K are profinite with $\{1\} \subset K \subset H$ so by lemma 4.2 there exists an open normal subgroup of H contained in K. Proposition 4.1 and lemma 4.4 let us choose an open normal subgroup of H of the form $H \bigcap U$ where $U \in \underline{\mathrm{S}}$.

Since U is finite index in G, UH is also finite index in G. Let $\{x_1, \cdots, x_n\} \subset G$ be representatives of the cosets UH in G so that

$$G = \bigcup_{i=1}^{n} x_i UH \tag{4.3}$$

$$\text{hence } \frac{G}{H} = \bigcup_{i=1}^{n} x_i (\frac{UH}{H}) \tag{4.4}$$

where the unions are disjoint and the x_i in 4.4 refer to the coset in $\frac{G}{H}$ of x_i.

Since $K \subset H$ we have inclusion maps $x_i UK \to x_i UH$ where elements of $x_i UK$ that are equal modulo K are equal modulo H. Therefore we have well defined homomorphisms $\pi_i : x_i \frac{UK}{K} \to x_i \frac{UH}{H}$. We claim that these maps are in fact homeomorphisms then one can let $s = \bigcup_{i=1}^{n} \pi_i^{-1}$.

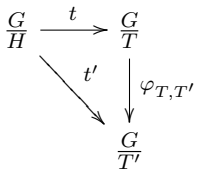
For sujectivity consider an element $x_i uh \in x_i UH$ where $u \in U$ and $h \in H$. Modulo H this element is equivalent to $x_i uhh^{-1} = xue \in x_i UK$ hence $x_i \frac{uh}{H} = \pi_i(\frac{x_i u}{K})$. The domain of π_i is a quotient space so for continuity it will suffice to establish that $\tilde{\pi_i} : x_i UK \to x_i \frac{UK}{K} \to x_i \frac{UH}{H}$ is continuous. But $\tilde{\pi_i}$ can be written as $x_i UK \hookrightarrow x_i UH \to x_i \frac{UH}{H}$which is a composition of continuous maps. For injectivity we only need to consider the case where $\pi_i(x_i u_1) = \pi_i(x_i u_2)$. If so then $x_i u_1 u_2^{-1} x_i^{-1} \in H$ but since U is normal $x_i u_1 u_2^{-1} x_i^{-1} \in U$ i.e. $x_i u_1 u_2^{-1} x_i^{-1} \in H \bigcap U \subset K$. Hence $x_i u_1 = x_i u_2$ are equal modulo K. To finish observe that UH is Hausdorff and H is closed so $\frac{UH}{H}$ is Hausdorff. Also the $x_i \frac{UK}{K}$ are compact (since U and K both are) which implies π_i is a homeomorphism.

Now suppose there is no restriction on $\frac{H}{K}$.

Define a set $A := \{(T, t) : K \subset T \subset H, \text{T is closed and } t : \frac{G}{H} \to \frac{G}{T} \text{is a continuous section}\}$. Note that $(H, id_{\frac{G}{H}}) \in A$ so A is nonempty. Define a partial order on A by $(T, t) \geq (T', t')$ iff $T \subset T'$ and the

following diagram commutes

(4.5)



where $\varphi_{T,T'}$ are the maps induced by the inclusion maps $T \hookrightarrow T'$. Let $\{(T_\alpha, t_\alpha)|\alpha \in B\}$ be a chain: Let $T = \bigcap_{\alpha\in B} T_\alpha$then by lemma 4.5 the φ induce a homeomorphism $\frac{G}{T} \to \varprojlim \frac{G}{T_\alpha}$. Diagram 4.5 indicates that the sections $t_\alpha : \frac{G}{H} \to \frac{G}{T_\alpha}$ induce a continuous map on the limit, denoted $t : \frac{G}{H} \to \frac{G}{T}$. Since each t_α is a section, t is a section. Thus (T, t) is an upper bound on the chain and by Zorn's lemma there exists a maximal element $K \subset \bar{T} \subset H \subset G$. We clearly want to to show that $\bar{T} = K$.

We claim that $\bar{T}$ is contained in any open subset U with $K \subset U$. Let $S = U \bigcap \bar{T}$. Then $S \subset \bar{T}$ is relatively open and is relatively closed since it is a subgroup. By the finite case there exists a section

$$t' : \frac{G}{\bar{T}} \to \frac{G}{S}$$

so that $(s, t' \circ \bar{t}) \in A$ with $(S, t' \circ \bar{t}) \geq (\bar{T}, \bar{t})$. Hence $S = \bar{T}$ and so $U \subset \bar{T}$. By equation 4.2 we have $H = \bar{T}$. □

4.3. SUBGROUP INDEX AND SYLOW THEOREMS.

Definition 4.2. A supernatural number is a formal product

$$n = \prod p^{n_p}$$

where the product is taken over all primes and n_p is an integer such that $n_p \geq 0$ or $n_p = +\infty$.

If m, n are supernatrual numbers with $m = \prod p^{m_p}$ and $n = \prod p^{n_p}$ then we say "m divides n" or write $m|n$ if $0 \leq m_p \leq n_p$ for all p.

Definition 4.3. Let $\{n_i\}_{i\in\Lambda}$ be a family of supernatural numbers. We have the following operations

(1) $\prod n_i = \prod p^{n_p}$ where $n_p = \sum n_{i_p}$
(2) $\gcd\{n_i\} = \prod p^{n_p}$ where $n_p = min\{n_{i_p}\}$
(3) $\mathrm{lcm}\{n_i\} = \prod p^{n_p}$ where $n_p = max\{n_{i_p}\}$

Definition 4.4. Let $H \subset G$ be a closed subgroup. The index $(G : H) := \mathrm{lcm}\{(\frac{G}{U} : \frac{H}{H\bigcap U})|\, U \in \underline{S}\}$. This is equal to $\mathrm{lcm}\{(G : HU)\}$.

Note we also have $(G : H) = \mathrm{lcm}\{(G : V)|V \text{is open and } H \subset V\}$.

Definition 4.5. The order of G (denoted $\#G$) is defined as $\#G := (G:1) = \text{lcm}\{|\frac{G}{U}| U \in \underline{S}\}$

Proposition 4.5. *If $K \subset H \subset G$ with K, H closed then*

$$(G:K) = (G:H)(H:K)$$

Proof. Note that $H \bigcap \underline{S}$ is a basis around the identity of open normal subgroups of H. Therefore

$$\begin{aligned}(H:K) =& \text{lcm}\{(\frac{H}{H\bigcap U} : \frac{K(H\bigcap U)}{H\bigcap U}|U \in \underline{S})\} \\ =& \text{lcm}\{(\frac{HU}{U} : \frac{KU}{U})|U \in \underline{S}\}\end{aligned}$$

For each $U \in \underline{S}$ we know that $\frac{G}{U}$ is a finite group by the proof of 4.2 so

$$(\frac{G}{U} : \frac{KU}{U}) = (\frac{G}{U} : \frac{HU}{U})(\frac{HU}{U} : \frac{KU}{U})$$

Taking the lcm over all choices of $U \in \underline{S}$ proves the result. □

Definition 4.6. A profinite group G is a pro p-group if its order is a power of p.

Since $\#G$=lcm$\{|\frac{G}{U}| : U \in \underline{S}\}$ and $G = \varprojlim_{U\in\underline{S}} \frac{G}{U}$, by a pro p-group we mean a projective limit of p-groups.

Definition 4.7. A closed subgroup $H \subset G$ is called a Sylow p-subgroup if H is a pro p-group and $gcd\{(G:H), p\} = 1$ i.e. $(G:H)$ is coprime to p.

Theorem 4.3. *(the profinite Sylow theorems)*

1. *For every prime p there exists a closed subgroup $H \subset G$ such that H is a Sylow p-subgroup of G.*
2. *Any two Sylow p-subgroups of G are conjugate.*
3. *Every pro p-sugroup is contained in a Sylow p-subgroup*
4. *If $h : G_1 \to G_2$ is a continuous surjective homomorphism of profinite groups then the image of a Sylow p-subgroup is a Sylow p-subgroup.*
5. *$\#G = \prod_p \#G_p$ where G_p is a Sylow p-subgroup of G.*

Proof. For part 1. let $P(U)$ be the set of all Sylow p-subgroups of $\frac{G}{U}$. If $U \subset U'$ are in $\underline{S}$ the map $\varphi_{U,U'} : \frac{G}{U} \to \frac{G}{U'}$ is a homomorphism of finite groups and therefore induces a map $P(U) \to P(U')$. As was noted in subsection 4.1 for any two $U, V \in \underline{S}$ we have $U\bigcap V \in \underline{S}$ with $U \subset U\bigcap V$ and $V \subset U\bigcap V$. It's then clear that if $\underline{S}$ is ordered by reverse inclusion then $\{P(U)| U \in \underline{S}\}$ is a projective system of sets, each of which is finite and nonempty. In particular

$$\varprojlim P(U) \neq \emptyset$$

Let $\{H_U\} \in \varprojlim P(U)$. Then $\{H_U\}$ is a projective and surjective system of Sylow p-subgroups. Let $H = \varprojlim H_U$. It's clear that H is a pro p-group (since each H_U is a p-group) and that

$$(G : H) = \text{lcm}\{(\frac{G}{U} : \frac{H}{H \bigcap U})\} = \text{lcm}\{(\frac{G}{U} : H_U)\}$$

is prime to p since each $(\frac{G}{U} : H_U)$ is prime to p.

For part 2. let H, H' be Sylow p subgroups. Then for every $U \in \underline{\text{S}}$ consider $H_U = \frac{HU}{U}$ and $H_{U'} = \frac{HU'}{U'}$. Since the subgroups $H \bigcap U \subset H$ are a basis of open neighborhoods of 1 consisting of open normal subgroups, by proposition 4.1 we can write $H = \varprojlim \frac{H}{H \bigcap U}$. By definition $\#H = lcm\{\frac{H}{H \bigcap U} | \, U \in \underline{\text{S}}\} = lcm\{\frac{HU}{U} | \, U \in \underline{\text{S}}\}$. Since H is a pro p-group so too is each $\frac{HU}{U}$. Moreover $(G : H) = lcm(\frac{G}{U} : \frac{HU}{U})$ is coprime to p so each $(\frac{G}{U} : \frac{HU}{U})$ is coprime to p. In particular $\frac{HU}{U} \subset \frac{G}{U}$ is a Sylow p-subgroup.

Define $Q(U) = \{\sigma_U \in \frac{G}{U} | \sigma_U H_U \sigma_U^{-1} = H_{U'}\}$. As in part 1. if $U, V \in \underline{\text{S}}$ with $U \subset V$ and $\varphi_{U,V} : \frac{G}{U} \to \frac{G}{V}$ then we have a map $Q(U) \to Q(V)$. This makes $\{Q(U) | U \in \underline{\text{S}}\}$ into a projective system and since each $Q(U)$ is nonempty so too is $\varprojlim Q(U)$. Take $\sigma \in \varprojlim Q(U)$ with $\sigma = \{\sigma_U\}$. Since $H = \varprojlim \frac{HU}{U}$ we have for each $U \in \underline{\text{S}}$, $\sigma_U H_U \sigma_U^{-1} = H_{U'}$ thus $\sigma H \sigma^{-1} = H'$.

For part 3. we adopt the notation of part 1. by letting H be a pro p-group and defining

$$R(U) = \{\tilde{H}_U \in P(U) | \, H_U \subset \tilde{H}_U \text{ and } \tilde{H}_U \text{is a Sylow } p\text{-subgroup}\}$$

Using the analagous process to part 1. we see that $\{R(U) | U \in \underline{\text{S}}\}$ is a projective system of non-empty finite sets. Let $\{\tilde{H}_U\} \in \varprojlim R(U)$ and let $\tilde{H} = \varprojlim \tilde{H}_U$ then it's clear that $H \subset \tilde{H}$ and that $\tilde{H}$ is a Sylow p-subgroup.

For part 4. let $h : G_1 \to G_2$ be a surjective homomorphism of profinite groups. Let $U \subset G_2$ be an open normal subgroup. We then have a surjective homomorphism of finite groups

$$\frac{G_1}{h^{-1}(U)} \to \frac{G_2}{U}$$

If $H \subset G$ is a Sylow p-subgroup then $H_{h^{-1}(U)} \subset \frac{G_1}{h^{-1}(U)}$ is a Sylow p-subgroup of $\frac{G_1}{h^{-1}(U)}$ using the same argument given in part 2. The image of $H_{h^{-1}(U)}$ is a Sylow p-subgroup of $\frac{G_2}{U}$. Taking the limit over all open normal subgroups of G_2 gives the result.

Part 5. is an obvious consequence of the corresponding result for the finite groups $\frac{G}{U}$ and the definition of $\#G$. $\square$

5. COHOMOLOGY OF PROFINITE GROUPS

5.1. DISCRETE G-MODULES.

Definition 5.1. Let G be a profinite group and A an abelian group with the discrete topology. We say A is a discrete G-module if there exists a continuous action $m : G \times A \to A$ such that

(1) $(gh)a = g(ha)$
(2) $g(a + b) = ga + gb$
(3) $1a = a$ where $1 \in G$ is the identity

For the remainder of this section let A be a discrete G-module.

If G is a finite group then the above definition coincides with the usual definition of G module since a 'finite profinite' group is discrete.

Definition 5.2. For $a \in A$ let $U_a = \{g \in G | \, ga = a\}$ be the stabilizer of a.

Proposition 5.1. *Let A be G-module with the discrete topology. Then the following are equivalent*

(1) *$m : G \times A \to A$ is continuous*
(2) *For each $a \in A$, $U_a \subset G$ is open.*
(3) *$A = \bigcup A^U$ where the union is taken over all $U \subset G$ such that U is an open subgroup.*

Proof. $1 \Rightarrow 2$. The map $g \mapsto ga$ is continuous since it is the restriction of the multiplication map to the open set $G \times \{a\}$. U_a is the inverse image of the open set $\{a\} \subset A$ under this map.

$2 \Rightarrow 3$. For any $a \in A$ assume U_a is an open subgroup. Then $a \in A^{U_a}$ so $A = \bigcup A^U$ where U is an open subgroup of A.

$3 \Rightarrow 1$. We only need to show that the inverse image of a singleton $a \in A$ is open. Suppose $gb = a$. By assumption $b \in A^U$ for some $U \subset G$ therefore $gUb = a$ i.e. $g \times b \in gU \times \{b\} \subset m^{-1}(a)$ where $gU \times \{b\}$ is an open set. □

5.2. COHOMOLOGY USING HOMOGENEOUS CO-CHAINS.

Definition 5.3. Let $C^q(G, A) = \{x : G^{q+1} \to A | \, x\text{is continuous and } x\text{is a } G\text{module homomorphism}\}$. When given a group structure through pointwise addition $C^q(G, A)$ is the group of homogeneous q-cochains.

Define a group homomorphism $\delta_{q+1} : C^q(G,A) \to C^{q+1}(G,A)$ by

$$\delta_{q+1}x(g_0,\cdots,g_{q+1}) = \sum_{j=0}^{q+1}(-1)^j x(g_0,\cdots,g_{j-1},g_{j+1},\cdots,g_{q+1})$$

We know that $\delta_{q+1}\circ\delta_q = 0$ ([13]§1.1) hence we can form the cochain complex

$$0 \to C^0(G,A) \xrightarrow{\delta_1} C^1(G,A) \xrightarrow{\delta_2} C^2(G,A) \xrightarrow{\delta_3} \cdots \tag{5.1}$$

We will denote 5.1 by $C(G,A)$ and for $q \geq 1$ define $H^q(G,A) \simeq \frac{Ker(\delta_{q+1})}{Im(\delta_q)}$ as the q-th cohomology group of $C(G,A)$. We will deal with $H^0(G,A)$ in a later subsection.

5.3. COHOMOLOGY USING NON-HOMOGENEOUS COCHAINS.

Definition 5.4. Let $\tilde{C}^q(G,A) = \{x : G^q \to A | \, x\text{is continuous}\}$. When given a group structure through pointwise addition $\tilde{C}^q(G,A)$ is the group of non-homgeneous q-cochains.

Definition 5.5. Define a group homomorphism $\tilde{\delta}_{q+1} : \tilde{C}^q(G,A) \to \tilde{C}^{q+1}(G,A)$ by

(5.2)

$$(\tilde{\delta}_{q+1}x)(g_1,\cdots,g_{q+1}) = g_1x(g_2,\cdots,g_{q+1}) + \left[\sum_{j=1}^{q}(-1)^j x(g_1,\cdots,g_jg_{j+1},\cdots,g_{q+1})\right] + (-1)^{q+1}x(g_1,\cdots,g_q)$$

Once again we know that $\tilde{\delta}_{q+1}\circ\tilde{\delta}_q = 0$ ([13]§1.1) so we can form the cochain complex

$$0 \to \tilde{C}^0(G,A) \xrightarrow{\tilde{\delta}_1} \tilde{C}^1(G,A) \xrightarrow{\tilde{\delta}_2} \tilde{C}^2(G,A) \to \cdots \tag{5.3}$$

We denote 5.3 by $\tilde{C}(G,A)$ and define $H^q(G,A) \simeq \frac{Ker(\tilde{\delta}_{q+1})}{Im(\tilde{\delta}_q)}$ as the q-th cohomology group of $\tilde{C}(G,A)$.

It seems as though we have given two conflicting definitions of $H^q(G,A)$, however both constructions are equivalent.

Proposition 5.2. *5.1 and 5.3 are isomorphic complexes with a pair of inverse homomorphisms given by*

$$\varphi_q : C^q(G,A) \to \tilde{C}^q(G,A)$$

$$\varphi_q(x)(g_1,\cdots,g_q) = x(1,g_1,g_1g_2,\cdots,g_1g_2\cdots g_q)$$

$$\psi_q : \tilde{C}^q(G,A) \to C(G,A)$$

$$\psi_q(y)(g_0,g_1,\cdots,g_q) = y(g_0^{-1}g_1,g_1^{-1}g_2,\cdots,g_{q-1}^{-1}g_q)$$

Proof. The proof is a tedious computation so will be omitted. □

5.4. **FURTHER RESULTS ON THE COHOMOLOGY OF PROFINITE GROUPS.** We begin this section by informally comparing the three equivalent constructions of group cohomology we have given. The justification for our work is the content of theorem 5.1 which shows how the cohomology of a profinite group can be understood in terms of the cohomology of the constituent finite groups.

In low dimensions the two equivalent constructions of sections 5.2 and 5.3 admit the same descriptions given in section 2.3. We note that the construction in 2.3 reduces to the construction given in this section as any map from $\mathbb{Z}[G^i]$ is completely determined by it's action on the elements of G^i.

Firstly we note that by desrcribing $H^0(G,A)$ as maps from singletons to A we can associate $H^0(G,A)$ with a submodule of A. In particular an element is in this submodule if and only if it belongs to $ker(\tilde{\delta}_1)$ i.e.

$$ga - a = 0$$

hence $H^0(G,A) = A^G$ as expected. We can use 5.2 to describe the cocycles of $H^1(G,A)$ as the maps $x : G \to A$ satisfying

$$x(g_1g_2) = g_1x(g_2) + x(g_1)$$

and the coboundaries as maps for which there there exists an $a \in A$ such that

$$x(g) = ga - a$$

This is hardly surprising given that 5.2 and 2.4 are identical.

In the language of Grothendieck, all three constructions are cohomological functors and are characterized by $H^0(G,A) = A^G$ and $H^q(G,A) = 0$ if A is an injective object. In the category of both G-modules and discrete G-modules the later criterion is satisfied precisely when A is co-induced. Theorem 2.1 attempts to make this characterisation somewhat less abstract.

In the category of discrete G-modules we also have notions of compatible maps as in section 2.4. The only extra criterion is that a map $f : G \to G'$ must be a continuous homomorphism of profinite groups (afterall any group homomorphism $g : A' \to A$ between discrete G-modules is obviously continuous). If $g : A' \to A$ then by the same construction we can consider

$$\begin{array}{ccc} \tilde{C}^q(G,A) & \xrightarrow{\tilde{\delta}_{q+1}} & \tilde{C}^{q+1}(G,A) \\ \uparrow_{(f,g)} & & \uparrow_{(f,g)} \\ \tilde{C}^q(G',A') & \xrightarrow{\tilde{\delta}_{q+1}} & \tilde{C}^{q+1}(G',A') \end{array}$$

This induces a morphism which we denote by a small abuse of notation

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

Let Λ be a directed partially ordered set. Let $(G_i,\varphi_{ij})_{i,j\in\Lambda;i\leq j}$ be a projective system of profinite groups and $(A_i,\psi_{ij})_{i,j\in\Lambda;i\leq j}$ a direct system of discrete G-modues. Suppose each A_i is a G_i module and that the maps

$$\varphi_{ij}: G_j \to G_i \,\text{and}\, \psi_{ij}: A_i \to A_j$$

are compatible. Then for each q we obtain a map

$$(\varphi_{ij},\psi_{ij}): H^q(G_i,A_i) \to H^q(G_j,A_j)$$

where $i \leq j$. We want to make these maps into a direct system which will then allow us to express the cohomology groups of $G = \varprojlim G_i$ and $A = \varinjlim A_i$ in terms of the groups $H^q(G_i,A_i)$. We will need to verify several claims first.

First we verify that $\{C^q(G_i,A_i):(\varphi_i,\psi_i)\}$ is a direct system. Let $i,j,k \in \Lambda$ such that $i \leq j \leq k$. Since $\{A_i,\psi_i\}$and $\{G_i,\varphi_i\}$ are direct/projective systems respectively there exist morphisms $\varphi_{ik} = \varphi_{ij}\circ\varphi_{jk}$ and $\psi_{ik} = \psi_{jk}\circ\psi_{ij}$ where by hypothesis all these maps are compatible. Calculating (φ_{ik},ψ_{ik}) gives

$$(\varphi_{ik},\psi_{ik}): \tilde{C}^q(G_i,A_i) \to \tilde{C}^q(G_k,A_k)$$

$$(\varphi_{ik},\psi_{ik}): x \mapsto \psi_{ik}\circ x\circ\varphi_{ik} = \psi_{jk}\circ\psi_{ij}\circ x\circ\varphi_{ij}\circ\varphi_{jk}$$

Hence $(\varphi_{ik},\psi_{ik}) = (\varphi_{jk},\psi_{jk})\circ(\varphi_{ij},\psi_{ij})$.

Proposition 5.3. *A is a G-module*

Proof. Let $a \in A$. This is an equivalence class in $\bigoplus_{i\in\Lambda} A_i$ so take $a = \psi_i(a_i)$ where ψ_i is the restriction of the canonical projection map to the factor A_i. Define

$$ga = \psi_i(\varphi_i(g)a_i)$$

where $\varphi_i : G \to G_i$ is the restriction of the canonical projection map $\prod_{j\in\Lambda} G_j \to G_i$ to G. It's clear that this will make A into a G-module provided it is well defined for a different representative of a. Suppose $j \in \Lambda$ with $i \leq j$ and $a_j = \psi_{ij}(a_i) \in A_j$. We clearly have $\psi_j(a_j) = \psi_j(\psi_{ij}(a_i)) = a$. Since $\varphi_i(g) = \varphi_{ij}(\varphi_j(g))$ and the maps φ_{ij} and ψ_{ij} are compatible we have

$$\psi_{ij}(\varphi_i(g)a_i) = \varphi_j(g)\psi_{ij}(a_i) = \varphi_j(g)a_j$$

$$\psi_j(\varphi_j(g)a_j) = \psi_j(\psi_{ij}(\varphi_i(g)a_i) = \psi_i(\varphi_i(g)a_i) = ga$$

□

Corollary 5.1. *The canonical maps $\varphi_i : G \to G_i$ and $\psi_i : A_i \to A$ are compatible maps.*

Theorem 5.1. $H^q(G, A) = \varinjlim H^q(G_i, A_i)$

Proof. Throughout we will denote $\delta_{q+1} : \tilde{C}^q(G_i, A_i) \to \tilde{C}^{q+1}(G_i, A_i)$ by $\tilde{\delta}^i_{q+1}$. Consider the following exact sequence

$$0 \to Im(\tilde{\delta}^i_q) \to Ker(\tilde{\delta}^i_{q+1}) \to H^q(G_i, A_i) \to 0$$

Then since $\varinjlim$ is an exact functor in the category of abelian groups we have

$$0 \to \varinjlim Im(\tilde{\delta}^i_q) \to \varinjlim Ker(\tilde{\delta}^i_q) \to \varinjlim H^q(G_i, A_i) \to 0$$

So it will suffice to find an isomorphism $\alpha : \varinjlim \tilde{C}^q(G_i, A_i) \to \tilde{C}^q(G, A)$ that commutes with the boundary maps $\tilde{\delta}^i_q$ on $\tilde{C}(G_i, A_i)$. For each $i \in \Lambda$ define

$$\alpha_i : \tilde{C}^q(G_i, A_i) \to \tilde{C}^q(G, A)$$

$$\alpha_i : x_i \mapsto \psi_i \circ x_i \circ \varphi_i$$

To simplify notation we will use α_i to denote this homomorphism regardless of the dimension (i.e. the value of q). We first check that α is a homomorphism on $\varinjlim \tilde{C}^q(G_i, A_i)$ i.e. for $i \leq j$, $\alpha_i = \alpha_j \circ (\varphi_{ij}, \psi_{ij})$. Since $\varphi_{ij} \circ \varphi_j = \varphi_i$ and $\psi_j \circ \psi_{ij} = \psi_i$

$$\alpha_i(x_i) = \psi_i \circ x_i \circ \varphi_i = \psi_j \circ \psi_{ij} \circ x_i \circ \varphi_{ij} \circ \varphi_j = \psi_j \circ (\varphi_{ij}, \psi_{ij})(x_i) \circ \varphi_j = \alpha_j \circ (\varphi_{ij}, \psi_{ij})(x_i)$$

Therefore the α_i extend to a well defined homomorphism on $\varinjlim \tilde{C}^q(G_i, A_i)$. Next we claim that $\alpha_i(\tilde{\delta}^i_{q+1} \circ x_i) = \tilde{\delta}_{q+1} \circ \alpha_i(x_i)$. Calculating $\alpha_i(\tilde{\delta}^i_{q+1} \circ x_i)$ gives

$$\begin{aligned}\alpha_i(\tilde{\delta}^i_{q+1} \circ x_i)(g_1, \cdots, g_{q+1}) =& \psi_i(\varphi_i(g_1))\psi_i(x(\varphi_i(g_2), \cdots, \varphi_i(g_{q+1}))+ \\ & \sum_{j=1}^{q}(-1)^q \psi_i(x(\varphi_i(g_1), \cdots, \varphi_i(g_{j-1}), \varphi_i(g_{j+1}), \cdots, \varphi_i(g_{q+1}))+ \\ & (-1)^{q+1}\psi_i(x(\varphi_i(g_1), \cdots, \varphi_i(g_q))\end{aligned}$$

Since corollary 5.1 indicates $\psi_i(\varphi_i(g)) = g$, the claim follows.

It remains to show that α is a bijection. We will deal with injectivity first. Let $x \in \varinjlim \tilde{C}^q(G_i, A_i)$ and suppose $\alpha(x) = 0$. We need to find an $x_i \in \tilde{C}^q(G_i, A_i)$ such that $\alpha_i(x_i) = \alpha(x)$ and $x_i = 0$. Pick some $i_o \in \Lambda$ and let $\alpha(x) = \alpha_{i_o}(x_{i_o})$. Then for $i \geq i_o$ let $x_i = \psi_{i_o i} \circ x_{i_o}$. Then clearly $\alpha_i(x_i) = 0$. Define the

following set

$$X_i = \{g_i = (g_{i_1}, \cdots, g_{i_q}) \in G_i^q | \, x_i(g_i) \neq 0\}$$

We will be done if we can show that for some $i \geq i_o$, $X_i = \emptyset$. Since each x_i is continuous, G_i^q is compact and A_i is discrete we deduce that X_i is finite. In particular $X_i \subset G_i^q$ is compact. On the other hand for $j \geq i \geq i_o$ we have $\varphi_{ij}(X_j) \subset X_i$ since for $g_j \in X_j$,

$$0 \neq x_j(g_j) = \psi_{ij} \circ x_i \circ \varphi_{ij}(g_j)$$

Hence $x_i(\varphi_{ij}(g_j)) \neq 0$. In particular we can now form a projective system of compact topological spaces.

$$\{X_i, \varphi_{ij} | i, j \geq i_o\}$$

If $g = (g_1, \cdots, g_q) \in \varprojlim_{i \geq i_o} X_i \subset G^q$ then clearly $\alpha(x) \neq 0$. By assumption $\alpha(x) = 0$, therefore $\varprojlim_{i \geq i_0} X_i = \emptyset$. By a standard result in topology([2]Chapter 1, §9.6) there must exist an $i \geq i_0$ such that $X_i = \emptyset$.

For surjectivity let $x : G^q \to A$ be a continuous map. We will need to show that there is a continuous map $x_i : G_i^q \to A$ such that $x = \psi_i \circ x_i \circ \varphi_i$ for some $i \in \Lambda$. A is discrete and the image of G^q under x is compact so x can only take on finitely many values, say

$$x(G^q) = \{a_1, \cdots, a_n\} = \{\psi_{i_1}(a_{i_1}), \cdots, \psi_{i_n}(a_{i_n})\} \subset A$$

For each pair $i_k i_l$ with $1 \leq k, l \leq n$ we know there exists an i such that $i_k \leq i$ and $i_l \leq i$ since Λ is a directed set. In particulr there exists an i_N such that $i_N \geq i_k$ for all $1 \leq k \leq n$. We can then write $x(G^q) \subset \psi_{i_N}(A_{i_N})$.

Next we claim there exists an open normal subgroup U_N of G such that x is constant on the cosets U_N^q in G^q. Take $ker(x) \subset G^q$ which is open and normal. In particular it's projections onto G will all be open and normal. Let U_1 be the intersection of these subgroups. Then U_1 is certainly open and normal and $U_N^q \subset ker(x)$. So x is constant on the cosets of U_N^q.

By lemma 4.4 there exists a $j \geq i_N$ such that for the open normal subgroup $\{1\} \subset G_j$ we have $\varphi_j^{-1}(1) = U \subset U_N$. Then x factors through $\frac{G^q}{U^q}$ i.e. if $\varphi_j : G^q \to \frac{G^q}{U^q} \simeq G_j^q$ is the natural projection map we have the following commutative diagram

$$\begin{array}{ccc} G^q & \xrightarrow{\varphi_j} & \frac{G^q}{U^q} \simeq G_j^q \\ & \searrow^{x} & \downarrow{\scriptstyle \bar{x}} \\ & & A \end{array}$$

where $\bar{x}(gU^q) = x(g)$ for $g \in G^q$. It's not difficult to see $\bar{x}$ will define a map $\bar{x_j} : G_j^q \to A_j$ such that $\bar{x} = \psi_j \circ \bar{x}_j$. Then $\alpha_j(\bar{x}_j) = \psi_j \circ \bar{x_j} \circ \varphi_j = \bar{x} \circ \varphi_j = x$. □

We close this section with some remarks. First, we remark that theorem 2.2 (the cup product) can be restated with G a profinite group ([12], Chapter 3,§6). We note that if A and B are discrete G-modules then $A \otimes B$ is again discrete with an action of G given by $g(a \otimes b) = ga \otimes gb$. Indeed, it's easy to see that $A \otimes B = \bigcup (A \otimes B)^U$ where the union is taken over all $U \subset G$ such that U is an open subgroup of G.

Finally we return to the prototypical example of a profinite group. Let k be a field and K a Galois extension of k with $G = Gal(\frac{K}{k})$. Give G the Krull topology so by theorem 1.3 and theorem 4.1 we know that G is a profinite group. Consider an open, normal subgroup $U \subset G$. Theorem 1.2 indicates that K^U is a normal extension of G. Since U is open it contains an open neighborhood about the identity of the form $U_A = Gal(\frac{K}{A})$ where $k \subset A \subset K$ and A is a finite extension of K. In particular $K^U \subset K^{U_A} = A$ where $K^{U_A} = A$ since K also is a Galois extension of A by corollary 1.2. In particular U is the Galois group of a finite extension of k.

One can now write $G = \varprojlim \frac{G}{U} = \varprojlim_{i \in \Lambda} Gal(\frac{K}{A_i})$ where the limit runs over all finite Galois extensions of k with $k \subset A_i \subset K$. In this case the set Λ is ordered by reverse inclusion i.e. $Gal(\frac{K}{A_i}) \subset Gal(\frac{K}{A_j})$ iff $A_j \subset A_i$, as one would expect.

By proposition 1.4 we can write $A = \varprojlim_{i \in \Lambda} L_i$ where $k \subset L_i \subset K$ and the L_i are finite Galois extensions of k. Of course we are now ordering the fields by standard inclusion. If $L_i \subset L_j$ then the maps $Gal(\frac{K}{A_j}) \to Gal(\frac{K}{A_i})$ and the inclusion map $L_i \hookrightarrow L_j$ are clearly compatible. In light of theorem 5.1 we can write

$$H^q(G, K) = \varinjlim H^q(G_i, L_i)$$

6. APPLICATIONS OF GALOIS COHOMOLOGY TO DUALITY THEOREMS

In this section we discuss several applications of Galois cohomology to duality theorems in number theory. The significance of these results, as well some of the details of their constructions, require results from class field theory (often abbreviated to CFT). A thorough treatment of what we need from CFT and other areas would lead us too far astray, so we will either omit or provide sketches of most of the proofs in this section.

Unless otherwise stated let $G = Gal(\frac{\overline{\mathbb{Q}_p}}{\mathbb{Q}_p})$ where $\mathbb{Q}_p$ is the field of p-adic numbers and $\overline{\mathbb{Q}_p}$ is an algebraic closure of $\mathbb{Q}_p$. Let μ_p be the p-th roots of unity, μ_{p^∞} the union of all p-th power roots of unity and μ the set of all roots of unity. We will state as a fact that as an abelian group $\mu \simeq \frac{\mathbb{Q}}{\mathbb{Z}}$. Let A be a discrete G-module and $A' = Hom(A, \mu)$, (known as the twisted Pontryagin dual). We also state that we have a map $A \otimes_{\mathbb{Z}} A' \to \mu$ and that $A'' \simeq A$.

6.1. **TATE LOCAL DUALITY.** Let $0 \leq i \leq 2$ and consider the cup product

$$H^i(G, A) \times H^{2-i}(G, A') \to H^2(G, \mu) \simeq \frac{\mathbb{Q}}{\mathbb{Z}}$$

That $H^2(G, \mu) \simeq \frac{\mathbb{Q}}{\mathbb{Z}}$ is a gem from CFT. For each fixed $\phi \in H^i(G, A)$ and any $\gamma \in H^{2-i}(G, A')$ the map $\gamma \mapsto \phi \cup \gamma$ induces a homorphism $H^i(G, A) \to H^2(G, \mu)$ and simarly for a fixed $\gamma \in H^{2-i}(G, A')$ and any $\phi \in H^i(G, A)$ the map $\phi \mapsto \phi \cup \gamma$ induces a homorphism $H^{2-i}(G, A') \to H^2(G, \mu)$. In particular we have maps

$$H^i(G, A) \to Hom(H^{2-i}(G, A'), \frac{\mathbb{Q}}{\mathbb{Z}}) \simeq Hom(H^{2-i}(G, A'), \mu) \simeq H^{2-i}(G, A')' \tag{6.1}$$

$$H^{2-i}(G, A') \to Hom(H^i(G, A), \frac{\mathbb{Q}}{\mathbb{Z}}) \simeq Hom(H^i(G, A), \mu) \simeq H^{2-i}(G, A)' \tag{6.2}$$

For the pair $H^i(G, A)$ and $H^{2-i}(G, A')$ to be in duality we mean the homorphisms 6.1 and 6.2 are injective. Alternatively one can say the pairing is dual.

Theorem 6.1. *(Tate 1962): Let A be a discrete, finite G-module. Then for any integer $0 \leq i \leq 2$ the cup product gives a duality between the finite groups $H^i(G, A)$ and $H^{2-i}(G, A')$.*

$$H^i(G, A) \times H^{2-i}(G, A') \to H^2(G, \mu) \simeq \frac{\mathbb{Q}}{\mathbb{Z}}$$

We claim without proof three important results when A is a free $\mathbb{Z}$ module (see [6], Chapter X,§1 and [11])

(1) When $i = 0$ the image of $H^2(G,A')$ under the map $H^2(G, A') \to Hom(H^0(G, A), \mu) \simeq H^0(G, A)'$ is exactly the torsion submodule of $H^0(G, A)$.
(2) When $i = 1$ the pairing is dual
(3) When $i = 2$ the map $H^2(G, A') \to Hom(H^0(G, A), \mu)$ is surjective.

Remark 6.1. For the proof of theorem 6.1 we make a convenient change of notation; $H^q(A) = H^q(G, A)$.

Proof. Since A is finite we can form a G-module by taking the elements of A as a basis for a vector space over $\mathbb{Z}$. If we let M denote this G-module then M is a free $\mathbb{Z}$-module and there is a surjective map $M \to A$ given by $1a \mapsto a$. If N is the kernel of this map then we have an exact sequence

$$0 \to N \to M \to A \to 0 \tag{6.3}$$

Since μ is an injective object in the category of discrete G-modules the functor $Hom(\cdot, \mu)$ is exact. Hence we have another exact sequence

$$0 \to A' \to M' \to N' \to 0 \tag{6.4}$$

Taking cohomology we have exact sequences

$$H^1(A') \to H^1(M') \to H^1(N') \to H^2(A') \to H^2(M') \to H^2(N') \tag{6.5}$$

$$H^1(A) \leftarrow H^1(M) \leftarrow H^1(N) \leftarrow H^0(A) \leftarrow H^0(M) \leftarrow H^0(N) \tag{6.6}$$

where we have deliberately written the cohomology sequence 6.6 from right to left. This is because if one applies $Hom(\cdot, \mu)$ to 6.6 we have a morphism of sequences given by the cup product,

$$\begin{array}{ccccccccccccc} H^1(A') & \to & H^1(M') & \to & H^1(N') & \to & H^2(A') & \to & H^2(M') & \to & H^2(N') & \to & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ H^1(A)' & \to & H^1(M)' & \to & H^1(N)' & \to & H^0(A)' & \to & H^0(M)' & \to & H^0(N)' & \to & 0 \end{array}$$

M and N are free over $\mathbb{Z}$ so the maps $H^1(M') \to H^1(M)'$ and $H^1(N') \to H^1(N)'$ are injective and the maps $H^2(M') \to H^0(M)'$ and $H^2(N') \to H^0(N)'$ are surjective. The 5-lemma implies the result for the case $i = 2$. The case $i = 0$ follows from replacing A with A' and noting that $A'' \simeq A$.

For the case $i = 1$ we first outline why the group $H^1(G, A)$ is finite. For each $a \in A$ let $U_a \subset G$ be the stablizer. This is open by 5.1 so $\bigcap_{a \in A} U_a$ is open since A is finite. In particular there exists an open normal subgroup $G_L \subset \bigcap_{a \in A} U_a \subset G$ which by lemma 4.2 and the remarks at the end of section 5.4 corresponds to a finite Galois extension of $\mathbb{Q}_p$, denoted L. Since $\frac{G}{G_L}$ is finite (again using lemma 4.2) we have that $H^1(\frac{G}{G^L}, A^{G_L})$ is finite. Moreover $H^1(G_L, A) = Hom(G_L, A)$ by proposition 2.9 and $Hom(G_L, A)$ can by shown to be finite using CFT (see [6], Chapter X, Theorem 2.1). Since the inflation-restriction sequence

$$0 \to H^1(\frac{G}{G_L}, A^{G_L}) \xrightarrow{Inf} H^1(G, A) \xrightarrow{Res} H^1(G_L, A)$$

is exact by proposition 2.11 we conclude that $H^1(G, A)$ is finite.

Using a similar construction to the case $i = 0$ we form a commutative diagram with exact rows,

$$\begin{array}{ccccccccccccc} H^1(N) & \to & H^1(M) & \to & H^1(A) & \to & H^2(N) & \to & H^2(M) & \to & H^2(A) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ H^1(N')' & \to & H^1(M')' & \to & H^1(A')' & \to & H^0(N')' & \to & H^0(M')' & \to & H^0(A')' \end{array}$$

The cup product gives maps from the top row into the torsion part of the bottom row. The result can again be established using the 5-lemma. □

6.2. **LOCAL FIELDS.** Let l and p be distinct primes. Let $G = Gal(\frac{\overline{\mathbb{Q}_l}}{\mathbb{Q}_l})$ and let $\mathbb{F}_l$ be the finite field with l elements. Let $I_l \subset G$ be the inertia subgroup. Let M a free $\mathbb{Z}_p$ module equipped with a G-action. We have $\frac{G}{I_l} \simeq Gal(\frac{\overline{\mathbb{F}_l}}{\mathbb{F}_l})$ so M^{I_l} is naturally a $Gal(\frac{\overline{\mathbb{F}_l}}{\mathbb{F}_l})$ module. For convenience let $\tilde{G} = Gal(\frac{\overline{\mathbb{F}_l}}{\mathbb{F}_l})$ for the remainder of this subsection

By proposition 2.11 we have an exaxt sequence,

$$0 \to H^1(\tilde{G}, M^{I_l}) \xrightarrow{Inf} H^1(G, M) \xrightarrow{Res} H^1(I_l, M)$$

We define

$$\begin{aligned} H^1_{nr}(G, M) &= Im(H^1(\tilde{G}, M^{I_l}) \xrightarrow{Inf} H^1(G, M)) \\ &= Ker(H^1(G, M) \xrightarrow{Res} H^1(I_l, M)) \end{aligned}$$

Let $M^*(1) = Hom(M, \mu_{p^\infty})$. Consider the cup product pairing

$$H^1(G, M) \times H^1(G, M^*(1)) \to H^2(G, M \otimes_{\mathbb{Z}_p} M^*(1))$$

We have a natural map $M \otimes_{\mathbb{Z}_p} M^*(1) \xrightarrow{det.} \mu_{p^\infty} \simeq \mathbb{Q}_p(1)$ and under the inv. map $H^2(G, \frac{\mathbb{Q}_p(1)}{\mathbb{Z}_p}) \simeq \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$. For any subgroup $A \subset H^1(G, M)$ we can define $A^\perp = \{\gamma \in H^1(G, M^*(1)) \mid \text{for all } \phi \in A,\ \phi \cup \gamma = 0\}$ i.e. the orthogonal complement to A.

Theorem 6.2. *Under the cup product pairing*

$$H^1(G, M) \times H^1(G, M^*(1)) \to H^2(G, \frac{\mathbb{Q}_p(1)}{\mathbb{Z}_p}) \simeq \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$$

with $H^1_{nr}(G, M)^\perp = H^1_{nr}(G, M^*(1))$.

Proof. See [10] §1.2 □

6.3. **ELLIPTIC CURVES.** Let $G = Gal(\frac{\overline{\mathbb{Q}_p}}{\mathbb{Q}_p})$. Let E be an elliptic curve over $\mathbb{Q}$. We can embed $\mathbb{Q}$ into $\mathbb{Q}_p$ which can then be embedded into $\overline{\mathbb{Q}_p}$. So it makes sense to talk of rational points on E with values in $\overline{\mathbb{Q}_p}$. Let $E(\overline{\mathbb{Q}_p})$ denote the set $\overline{\mathbb{Q}_p}$-rational points of E. It's a well known fact from the arithmetic of elliptic curves that $E(\overline{\mathbb{Q}_p})$ can be equipped with the structure of an abelian group.

Let $E(\overline{\mathbb{Q}_p})_{p^n}$ denote the $\overline{\mathbb{Q}_p}$-rational points on E that are p^n torsion i.e. $\sum_{p^n} a = a + \cdots + a$, p^n times is equal to $\underline{\infty}$. We can define a surjective group homorphism from $E(\overline{\mathbb{Q}_p})$ to $E(\overline{\mathbb{Q}_p})$ by $\theta : a \mapsto \sum_{p^n} a$, the kernel of which if clearly $E(\overline{\mathbb{Q}_p})_{p^n}$. This gives an exact sequence

$$0 \to E(\overline{\mathbb{Q}_p})_{p^n} \to E(\overline{\mathbb{Q}_p}) \xrightarrow{\theta} E(\overline{\mathbb{Q}_p}) \to 0$$

We have an action of G on $E(\overline{\mathbb{Q}_p})$ i.e. $g \in G$ acts coordinate wise. Since G is a Galois extension, the fixed subfield of G is $\mathbb{Q}_p$, therefore $E(\overline{\mathbb{Q}_p})^G = E(\mathbb{Q}_p)$. Passing to cohomology we obtain an exact sequence

$$0 \to E(\mathbb{Q}_p)_{p^n} \to E(\mathbb{Q}_p) \xrightarrow{\theta} E(\mathbb{Q}_p) \xrightarrow{d} H^1(G, E(\overline{\mathbb{Q}_p})_{p^n}) \to H^1(G, E(\overline{\mathbb{Q}_p})) \xrightarrow{\theta} H^1(G, E(\overline{\mathbb{Q}_p})) \to \cdots \tag{6.7}$$

where by $H^1(G, E(\overline{\mathbb{Q}_p})) \xrightarrow{\theta} H^1(G, E(\overline{\mathbb{Q}_p}))$ we mean the map induced by θ. The boundary homorphism $E(\mathbb{Q}_p) \xrightarrow{d} H^1(G, E(\overline{\mathbb{Q}_p})_{p^n})$ has kernel $p^n E(\mathbb{Q}_p)$ hence we can define a map on the quotient.

Definition 6.1. The boundary homorphism d induces an injective map

$$\overline{d} : \frac{E(\mathbb{Q}_p)}{p^n E(\mathbb{Q}_p)} \hookrightarrow H^1(G, E(\overline{\mathbb{Q}_p})_{p^n})$$

called the Kummer homomorphism.

We can consider the image $\overline{d}(\frac{E(\mathbb{Q}_p)}{p^n E(\mathbb{Q}_p)}) \subset H^1(G, E(\overline{\mathbb{Q}_p})_{p^n})$. We have $E(\overline{\mathbb{Q}_p})_{p^n} \simeq Hom(E(\overline{\mathbb{Q}_p})_{p^n}, \mu_{p^n})$ and in fact under the Weil pairing $E(\overline{\mathbb{Q}_p})^*_{p^n}(1) \simeq E(\overline{\mathbb{Q}_p})_{p^n}$.

Theorem 6.3. *Under the cup product pairing*

$$H^1(G, E(\overline{\mathbb{Q}_p})_{p^n}) \times H^1(G, E(\overline{\mathbb{Q}_p})_{p^n}) \to H^2(G, \mu_{p^n}) \simeq \frac{\mathbb{Z}}{p^n \mathbb{Z}}$$

We have

$$\overline{d}(\frac{E[\mathbb{Q}_p]}{p^n E[\mathbb{Q}_p]})^{\perp} = \overline{d}(\frac{E(\mathbb{Q}_p)}{p^n E(\mathbb{Q}_p)})$$

.

6.4. **P-ADIC REPRESENTATIONS.** Let V a be an m-dimensional representation of G i.e. ,V is an m-dimensional vector space over $\mathbb{Q}_p$ along with a homorphism $G \to GL(V)$. In particular, G acts on V via linear transformations.

Definition 6.2. Let B_{cris} be Fontane's ring of p-adic periods. Define a map $id \otimes 1 : V \to V \otimes B_{cris}$ by $v \mapsto v \otimes 1$. We define $H^1_f(G, V) \subset H^1(G, V)$ by

$$H^1_f(G, V) = Ker(H^1(G, V) \xrightarrow{id \otimes 1} H^1(G, V \otimes B_{cris}))$$

Let $\mathbb{Q}_p(1) = (\varprojlim \mu_{p^n}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $V^*(1) = Hom(V, \mathbb{Q}_p(1))$

Theorem 6.4. *Under the cup product pairing*

$$H^1(G,V) \times H^1(G,V^*(1)) \to H^2(G,\mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$$

we have $H^1_f(G,V)^\perp = H^1_f(G,V^*(1))$

References

[1] J. Beachy and W. Blair. *Abstract Algebra*. Waveland Press, 2006.

[2] Bourbaki. *General Topology*. Hermann, Publishers in Arts and Science Addison-Wesley Publishing Company, 1966.

[3] Bourbaki. *Commutative Algebra*. Hermann, Publishers in Arta and Science Addison-Wesley Publishing Company, 1972.

[4] Bourbaki. *Algebra*. Hermann, Publishers in Arts and Science Addison-Wesley Publishing Company, 1981.

[5] J.W.S. Cassels A. Frolich, editor. *Algebraic Number Theory*. Academic Press, 1967.

[6] S. Lang. *Topics in Cohomology of Groups*. Springer, 1991.

[7] S. Lang. *Algebra*. Springer, 2002.

[8] M.F. Atiyah I.G. Macdonald. *Introduction to Commutative Algebra*. Westview Press, 1969.

[9] S. MacLane. *Homology*. Springer, 1963.

[10] J.S. Milne. *Arithmetic Duality Theorems*. Academic Press, 1986.

[11] T. Nakayama. Cohomology of class field theory and tensor product modules i. *The Annals of Mathematics*, 65:255–267, 1957.

[12] L. Ribes. *Introduction to Profinite Groups and Galois Cohomology*. Queen's University, 1970.

[13] J.J. Rotman. *An Introduction to Homological Algebra*. Springer, 2009.

[14] J.P. Serre. *Local Fields*. Springer, 1979.

[15] J.P. Serre. *Galois Cohomology*. Springer, 1997.

[16] J. Tate. Daulity theorems in galois cohomology over number fields. In *Proceedings of the International Congress of Mathematics*, 1962.

[17] L.C. Washington. Galois cohomology. In *Modular Forms and Fermat's Last Theorem*, 1997.

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

[19] S.H. Weintraub. *Galois Theory*. Springer, 2006.

7. APPENDICES

APPENDIX 1: MODULES. Throughout let Λ be an indexing set and A a ring with unit.

Definition 7.1. A left A-module is an abelian group M with the group operation written additively and a multiplication map $A \times M \to M$ with the following properties

For $a, b \in A$ and $m, n \in M$

(1) $a(m+n) = am + an$
(2) $(a+b)m = am + bm$
(3) $(ab)m = a(bm)$
(4) $1m = m$

Henceforth we will simply say an A-module in place of a left A-module.

Definition 7.2. A submodule $M' \subset M$ is a subgroup that is closed under multiplication by elements of A.

Definition 7.3. If M and N are A-modules then a module homorphism $f : M \to N$ is a homomorphism of abelian groups such that for all $a \in A$ and $m \in M$, $f(am) = af(m)$. One sometimes calls such maps A-linear.

We let $Hom(M, N)$ denote the set of all A-module homorphisms from M to N. It is an A-module under pointwise addition and multiplication.

Proposition 7.1. *If $f : M \to N$ is an A-module homomorphism then $f(M) \simeq \frac{M}{ker(f)}$.*

Proof. The statement is self evident given the corresponding result for groups and rings. □

Definition 7.4. If $\{M_i\}_{i\in\Lambda}$is a set of A-modules then we define the direct product as the set $\prod_{i\in\Lambda} M_i$ with addition and multiplication defined pointwise i.e. for all $i \in \Lambda$

- $(x_i) + (y_i) = (x_i + y_i)$
- $a(x_i) = (ax_i)$

Definition 7.5. If $\{M_i\}_{i\in\Lambda}$ is a set of A-modules then we define the direct sum $\oplus_{i\in\Lambda} M_i$ as the set of all elements of the cartesian product $(x_i)_{i\in\Lambda} \in \prod_{i\in\Lambda} M_i$ such that all but finitely many of the $(x_i)_{i\in\Lambda}$ are zero.

If $x \in M$ then the set of all finite sums of the form $\sum_{a\in A} ax$ is clearly a submodule of M, denoted Ax. It is the smallest such submodule containing x and we say x generates Ax. For any arbitrary set $\{x_i\}_{i\in\Lambda} \subset M$ the set of all finite sums of the form $\sum_{i\in\Lambda} a_i x_i$ is the smallest submodule containing $\{x_i\}_{i\in\Lambda}$. The x_i are called generators and in general an element of this submodule will not have a unique representation of the form $\sum_{i\in\Lambda} a_i x_i$.

Definition 7.6. If there exists a finite set $\{x_i\} \subset M$ such that $\sum a_i x_i = M$ then we say M is finitely generated.

Definition 7.7. We say M is a free module if $M \simeq \oplus_{i\in\Lambda} A_i$ where for each $i \in \Lambda$, $A_i \simeq A$.

Proposition 7.2. *M is finitely generated $\iff$ there exists a positive integer $n > 0$ such that M is isomorphic to some quotient of $\oplus_{i=1}^n A_i$.*

Proof. First suppose M is finitely generated with with generators $\{x_i\}_{i=1}^n$. Then we can define a surjective module homomorphism $\pi : \oplus_{i=1}^n A_i \to M$ (where $A_i \simeq A$) by mapping $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i x_i$. By proposition 7.1 we have $M \simeq \frac{\oplus_{i=1}^n A_i}{ker\{\pi\}}$.

Conversely suppose the $M \simeq \frac{\oplus_{i=1}^n A}{I}$ for some ideal I. Since the finite subset of $\oplus_{i=1}^n A$ consisting of all zero entries except for the i-th position generates $\oplus_{i=1}^n A_i$ and their image under the projection map in M will act as a finite set of generators. □

Proposition 7.3. *Let M be finitely generated with generators $\{x_i\}_{i=1}^n$, $I \subset A$ an ideal and $\phi : M \to M$ a module endomorphism such that $\phi(M) \subset I \cdot M$. Then ϕ satisfies and equation of the form*

$$\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0 \tag{7.1}$$

where the $\{a_i\}_{i=1}^n \subset I$.

Remark 7.1. For any $a \in A$ and $j \in I$, $aj \in I$ so $I \cdot M$ is a submodule of M.

Proof. Since the $\{x_i\}_{i=1}^n$ generate M we can write $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ where the $a_{ij} \in I$. In particular $\phi(x_i) - \sum_{j=1}^n a_{ij}x_j = 0$ so if we write multiplication in M using finite dimensional matricies then

$$(\delta_{ij}\phi - a_{ij}) \begin{matrix} x_1 \\ \vdots \\ x_n \end{matrix} = 0$$

We can consider the entries of $(\delta_{ij}\phi - a_{ij})$ as elements of the endomorphism ring $End(M)$ so it makes sense to multiply on the left by the adjoint of $(\delta_{ij}\phi - a_{ij})$. This implies that $det(\delta_{ij}\phi - a_{ij})$ anhilates every generator of M. Expanding the determinant out in powers of ϕ gives an equation of the form 7.1. □

Theorem 7.1. *(Nakayama's lemma): Let $J(A)$ be the Jacobson's radical of A. Let M be finitely generated and $I \subset A$ an ideal such that $I \subset J(A)$. Then $I \cdot M = M \Rightarrow M = 0$.*

Proof. Since $I \cdot M = M$ we can take the endomorphism ϕ from propostion 7.3 to be the identity. Then equation 7.1 reads

$$1 + a_1 + \cdots + a_n = 0$$

In particular there is an element $x = 1 + a_1 + \cdots + a_n \in A$ such that $x \cdot M = 0$. Moreover $x \equiv 1 \ mod \ I$ with $I \subset J(A)$ so x is a unit and hence $x^{-1}(x \cdot M) = (x^{-1}x) \cdot M = M = 0$. □

APPENDIX 2: EXACT SEQUENCES.

Definition 7.8. A sequence $\{M_i, f_i\}_{i\in\Lambda}$ of A-modules and A-module homomorphisms with $f_i : M_{i-1} \to M_i$

$$\cdots \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_{i+2}} \cdots \tag{7.2}$$

is exact at M_i if $Im(f_i) = Ker(f_{i+1})$. The sequence $\{M_i, f_i\}_{i\in\Lambda}$ is called an exact sequence if it is exact at each M_i.

Proposition 7.4. *If i is the inclusion map and π is the projection map*

- $0 \xrightarrow{i} M \xrightarrow{f} N$ *is exact* $\iff$ *f is injective*
- $M \xrightarrow{f} N \xrightarrow{\pi} 0$ *is exact* $\iff$ *f is surjective*

Henceforth we will not label the inclusion of the zero ring or the projection onto the zero ring.

Definition 7.9. An exact sequence of the form $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is called a short exact sequence. An exact sequence of the form in equation 7.2 is called a long exact sequence.

In the case of 7.9 f is clearly injective and g is surjective.

If a sequence of the form 7.2 is exact at M_i then we can insert a short exact sequence at M_i in the following way; replace M_i with $0 \to im(f_i) \to M_i \to ker(f_i) \to 0$. As such we nearly always focus our attention on short exact sequences.

Theorem 7.2. *The sequence*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{7.3}$$

is a short exact sequence iff for any A-module (denoted N) the following sequences are exact

$$0 \to Hom(M'', N) \xrightarrow{\bar{g}} Hom(M, N) \xrightarrow{\bar{f}} Hom(M', N) \tag{7.4}$$

$$0 \to Hom(N, M') \xrightarrow{\underline{\mathrm{f}}} Hom(N, M) \xrightarrow{\mathrm{g}} Hom(N, M'') \tag{7.5}$$

where $\bar{f}(\phi) = \phi \circ f$ *and* $\underline{\mathrm{f}}(\phi) = f \circ \phi$ *where the compositions makes sense.* $\bar{g}$ *and* g *are defined similarly.*

Proof. Firstly suppose that 7.3 is exact i.e. f and g are injective and surjective respectively. We will show that equation 7.4 is exact. Showing that sequence 7.5 is exact is similar. Firstly if $\phi \in Ker(\bar{g}) \subset Hom(M'', N)$ then $\phi \circ g = 0$. Since g is surjective we know that $ker(\phi) = M''$ i.e. $\phi = 0$ and thus $\bar{g}$ is injective. Next if $\phi \in Im(\bar{g}) \subset Hom(M, N)$ then $\phi = \gamma \circ g$ for some $\gamma \in Hom(M'', N)$. Since $g \circ f = 0$ we deduce that $\bar{f}(\phi) = g \circ \phi = g \circ f \circ \gamma = 0$ hence $Im(\bar{g}) \subset Ker(\bar{f})$. If $\phi \in Ker(\bar{f}) \subset Hom(M, N)$ then $\phi \circ f = 0$ so $Im(f) \subset Ker(\phi)$. Since $Im(f) = Ker(g)$ there is a well defined map from $\frac{M}{Im(f)} = \frac{M}{ker(g)} = M''$ to N. If this map is denoted by $\gamma \in Hom(M'', N)$ then $\phi = \gamma \circ g$ so $Ker(\bar{f}) \subset Im(\bar{g})$. This establishes that $Ker(\bar{f}) = Im(\bar{g})$ so the sequence 7.4 is exact. Note that we did not require that f is injective to establish that 7.4 was exact, however it is required for establishing that 7.5 is exact.

For the converse we need to show that f is injective, g is surjective and that $Im(f) = Ker(g)$. In 7.5 let $N = Ker(f)$ and consider the function $i \in Hom(N, M')$ where i is the inclusion map. Then $\underline{f}(i) = 0$ and since $\underline{f}$ is injective this implies $i = 0$ so $Ker(f) = 0$. Next we show that $Im(f) = Ker(g)$. First, if we let $N = Ker(g)$ and $i \in Hom(N, M)$ be the inclusion map then $i \in Ker(\underline{g})$. Since 7.5 is exact there exists a $\phi \in Hom(N, M')$ such that $i = f \circ \phi$. In particular $Ker(g) = Im(i) \subset Im(f)$. Let $N = Im(f)$ and let $\pi \subset Hom(M, N)$ be the projection map $\pi : M \to \frac{M}{Im(f)}$. Then $\overline{f}(\pi) = 0$ so there exists $\gamma \in Hom(M'', N)$ such that $\pi = \gamma \circ g$. So $Ker(g) \subset Ker(\pi) = Im(f)$. All that remains to establish is that g is surjective. Let $N = Im(g)$ and $\pi : M'' \to \frac{M''}{Im(g)}$. Then $\overline{g}(\pi) = 0$ hence $\pi = 0$ since 7.4 is exact. □

APPENDIX 3: TENSOR PRODUCTS. Let M, N and P be A-modules.

Definition 7.10. A function $f : M \times N \to P$ is A-bilinear if for each fixed $m \in M$ the map $n \mapsto f(m, n)$ is A-linear and for each fixed $n \in N$ the map $m \mapsto f(m, n)$ is A-linear.

Theorem 7.3. *There exists an A-module (denoted* $M \otimes N$*) and a unique A-bilinear mapping* $t : M \times N \to M \otimes N$ *with the following property*

- For every P and every A-bilinear map $\phi : M \times N \to P$ there exists a unique A-linear map ϕ' such that $\phi = \phi' \circ t$.
- If $(M \otimes N)'$ and t' satisfy the above requirements of the theorem then there exists a unique isomorphism $j{:}M \otimes N \to (M \otimes N)'$ such that $j \circ t = t'$

Proof. First we show existence. Let $\tilde{A}$ denote the free A-module with basis indexed by $M \times N$. Consider the submodule $\tilde{B} \subset \tilde{A}$ generated by all elements of the form

$$(m + m', n) - (m, n) - (m', n)$$

$$(m, n + n') - (m, n) - (m, n')$$

$$(am, n) - a \cdot (m, n)$$

$$(m, an) - a \cdot (m, n)$$

Let $M \otimes N = \frac{\tilde{A}}{\tilde{B}}$. We claim this A-module has the desired properties. Let $m \otimes n$ denote the image of $(m, n) \in \tilde{A}$ in $M \otimes N$. Consider the map $t : M \times N \to M \otimes N$ defined by $(m, n) \mapsto m \otimes n$, then it is obvious from the definition of $\tilde{B}$ that the following properties hold,

$$(m + m') \otimes n = m \otimes n + m' \otimes n$$

$$m \otimes (n + n') = m \otimes n + m \otimes n'$$

$$a(m \otimes n) = (am \otimes n) = (m \otimes an)$$

so that t is A-bilinear. Since the $m \otimes n$ generate $M \otimes N$, t is also surjective. To see that $M \otimes N$ and t satisfies the required property note that any A-bilinear map $\phi : M \times N \to P$ is zero on the generators of $\tilde{B}$. Since ϕ extends to an A-module homorphism $\tilde{\phi} : \tilde{A} \to P$ and $\tilde{B} \subset Ker(\tilde{\phi})$, there is a well definied A-module homomorphism $\phi' : M \otimes N \to P$. In particular $\phi'(m \otimes n) = \phi(m, n)$ which means $\phi = \phi' \circ t$.

To see that our choice of $M \otimes N$ is unique consider $(M \otimes N)'$ and t' satisfying the requirements of the theorem. Then it's not hard to see that that the A-bilinear map $t' : M \times N \to (M \otimes N)$ induces an A-module homorphism $(M \otimes N)' \to M \otimes N$ and that $t : M \times N \to M \otimes N$ induces the inverse map $M \otimes N \to (M \otimes N)'$. □

Proposition 7.5. (1) $M \otimes N \simeq N \otimes M$

(2) $(M \otimes N) \otimes P \simeq M \otimes (N \otimes P)$

(3) $(M \oplus N) \otimes P \simeq (M \otimes P) \oplus (N \otimes P)$

(4) $A \otimes M \simeq M$

Proof. Properties 1. and 2. are obvious and tedious so will omit their proof. For 3. the map $(m, n) \otimes p \mapsto (m \otimes p, n \otimes p)$ is a well defined isomorphism between $(M \oplus N) \otimes P$ and $(M \otimes P) \oplus (N \otimes P)$. For property 4. we define an A-module homorphism $a \otimes m \mapsto am$. This map is injective since $am = 0$ implies $a \otimes m = a(1 \otimes m) = 1 \otimes am = 1 \otimes 0 = 0$. $1 \otimes m \mapsto m$ so the map is obviously surjective. □

Lemma 7.1. $Hom(M \otimes N, P) \simeq Hom(M, Hom(N, P))$

Proof. Let $\phi : M \times N \to P$ be an A-bilinear map. Then for a fixed $m \in M$, $n \mapsto \phi(m,n) \in P$ is an A-module homomorphism thus inducing a map $m \mapsto \phi(m,\cdot) \in Hom(N,P)$. Similarly any $\phi \in Hom(M, Hom(N,P))$ induces a map $(m,n) \mapsto \phi_m(n)$ which is A-bilinear since ϕ is a module homomorphism. It's easy to see that ϕ in the later case is just a bilinear map from $M \times N \to P$ for which m has been fixed. Any bilinear map from $M \times N \to P$ corresponds to an element of $Hom(M \otimes N, P)$, while it is obvious that the bijection just described is an A-module homorphism. □

Theorem 7.4. *Let*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{7.6}$$

be an exact sequence and let N be any A-module. Then the following sequence is exact

$$M' \otimes N \xrightarrow{f\bar{\otimes}1} M \otimes N \xrightarrow{g\bar{\otimes}1} M'' \otimes N \to 0 \tag{7.7}$$

where $f \otimes 1$ denotes $m' \otimes n \mapsto f(m') \otimes n$.

Proof. We will apply a variation of theorem 7.2. Note that in the proof of the theorem we did not required f being injective to show that equation 7.4 was exact and similarly we did not need equation 7.5 exact to show that g was surjective. So if P is any A-module then

$$0 \to Hom(M'', Hom(N,P)) \xrightarrow{g\bar{\otimes}1} Hom(M, Hom(N,P)) \xrightarrow{f\bar{\otimes}1} Hom(M', Hom(N,P))$$

is exact. We use lemma 7.1 to deduce that

$$0 \to Hom(M'' \otimes N, P) \to Hom(M \otimes N, P) \to Hom(M' \otimes N, P)$$

is exact where the homorphisms are defined using the same procedure as in the proof of lemma 7.1 but we neglect labels for notational convenience. Using the variation of 7.2 described at the start of the proof we deduce that 7.7 is exact. □

APPENDIX 4: DIRECT LIMITS.

Definition 7.11. A directed set is a partially ordered set Λ where for all $i, j \in \Lambda$ there exists $k \in \Lambda$ such that $i \leq k$ and $j \leq k$.

Definition 7.12. A direct system of A-modules over the directed set Λ is a collection of A-modules $\{M_i\}_{i \in \Lambda}$ and a collection of A-module homomorphisms $\{\mu_{ij}\}_{i,j \in \Lambda\, i \leq j}$ where $\mu_{ij} : M_i \to M_j$ and the following conditions are satisfied,

- μ_{ii} is the identity on M_i for all $i \in \Lambda$
- $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ for $i \leq j \leq k$

We will assume that $\{M_i\}_{i\in\Lambda}$, $\{\mu_{ij}\}_{i,j\in\Lambda\, i\leq j}$ (also written $\{M_i,\mu_{ij}\}_{i,j\in\Lambda}$) is a direct system for the remainder of this appendix

Definition 7.13. Let $N=\oplus_{i\in\Lambda}M_i$ and identitfy each module M_i by inclusion with it's canonical image in N. Let $\tilde{N}\subset N$ be the submodule generated by the set $\{m_i-\mu_{ij}(m_i)|\ x_i\in M_i\ i\leq j\}$, let $\mu: N\to\frac{N}{\tilde{N}}$ be the projection onto the quotient module and let $\mu_i=\mu|_{M_i}: M_i\to\frac{N}{\tilde{N}}$ be the restriction of μ to each M_i.

We call the set $M=\varinjlim M_i=\frac{N}{\tilde{N}}$ along with the projections μ_i the direct limit of the direct system.

Proposition 7.6. *$\mu_i=\mu_j\circ\mu_{ij}$ where $i\leq j$*

Proof. From definition 7.13 for all $x_i\in M_i$ we have $x_i-\mu_{ij}(x_i)\in\tilde{N}$ which means that in M, $\mu_i(x_i)=\mu_j(\mu_{ij}(x_i))$. □

Proposition 7.7. *Every element of M can be written in the form $\mu_i(x_i)$ for some $i\in\Lambda$. Moreover If $\mu_i(x_i)=0$ then $\mu_{ij}(x_i)=0$ for some j with $j\geq i$.*

Proof. Every element of M is the image of something in $\oplus_{i\in\Lambda}M_i$ under the quotient map so every element of M is of the form

$$m=\sum_{a=1}^{n}\mu_{i_a}(x_{i_a}) \tag{7.8}$$

Since the $\{M_i\}_{i\in\Lambda}$ are a direct system and 7.8 is a finite sum we can find an element $J\in\Lambda$ such that $i_a\leq J$ for $1\leq a\leq n$. Then applying proposition 7.6 gives

$$m=\sum_{a=1}^{n}\mu_J(\mu_{i_aJ}(x_i))$$

For the second part of the proposition note that if $\mu_i(x_i)=0$ then $x_i\in\tilde{N}$ as defined in definition 7.13. In particular we can write $x_i=\sum_{a=1}^{n}(x_{i_a}-\mu_{i_aj_a}(x_{i_a}))\in\oplus_{i\in\Lambda}M_i$. Let $J\in\Lambda$ be chosen such that $i_a\leq J$ for $1\leq a\leq n$. Then we can express x_i under the image of μ_{iJ} as

$$\mu_{iJ}(x_i)=\sum_{a=1}^{n}\mu_{i_aJ}(x_{i_a})-\mu_{j_aJ}(\mu_{i_aj_a}(x_{i_a}))=\sum_{a=1}^{n}\mu_{i_aJ}(x_i)-\mu_{i_aJ}(x_i)=0$$

□

Theorem 7.5. *Let N be any A-module and for each $i\in\Lambda$ let $\alpha_i: M_i\to N$ be an A-module homorphism such that $\alpha_i=\alpha_j\circ\mu_{ij}$. Let $M=\varinjlim M_i$. Then there exists a unique homorphism $\alpha: M\to N$ such that $\alpha_i=\alpha\circ\mu_i$.*

Proof. According to proposition 7.7 we can write any element of M as $\mu_i(x_i)$ for some $i \in \Lambda$. Define α by $\mu_i(x_i) \mapsto \alpha_i(x_i)$. If $\mu_i(x_i) = \mu_j(x_j)$ for some $i \leq j$ then $\mu_i(x_i) = \mu_j(\mu_{ij}(x_i)) = \mu_j(x_j)$ therefore,

$$\alpha(\mu_i(x_i)) = \alpha_i(x_i) = \alpha_j(\mu_{ij}(x_i)) = \alpha(\mu_j(\mu_{ij}(x_i))) = \alpha(\mu_j(x_j))$$

so that α is well defined. It's also clear that $\alpha_i = \alpha \circ \mu_i$ from the definition of α. If $\beta : M \to N$ is another homorphism with the property that $\alpha_i = \beta \circ \mu_i$ for any $\mu(x_i) \in M$ we have must necessarily have $\alpha(\mu_i(x_i)) = \alpha_i(\mu_i(x_i)) = \beta(\mu_i(x_i))$ i.e. $\alpha = \beta$. □

Definition 7.14. If $\{M_i, \mu_{ij}\}_{i,j\in\Lambda}$ and $\{N_i, \nu_{ij}\}_{i,j\in\Lambda}$ are direct systems with $M = \varinjlim M_i$ and $N = \varinjlim N_i$ then a homorphism ϕ from $M \to N$ is a family of homorphisms $\phi_i : M_i \to N_i$ such that $\phi_j \circ \mu_{ij} = \nu_{ij} \circ \phi_i$ for $i \leq j$.

Proposition 7.8. *With the notation used in definition 7.14, ϕ gives rise to a unique homorphism $\phi : M \to N$ defined by $\phi(\mu_i(x_i)) = \nu_i(\phi_i(x_i))$.*

Proof. ϕ is clearly unique and is a homorphism, but it is not obvious that it is well defined. Let $\mu_i(x_i) = \mu_j(x_j)$ then $\mu_i(x_i) = \mu_j(\mu_{ij}(x_i)) = \mu_j(x_j)$ which gives

$$\phi(\mu_i(x_i)) = \phi_i(x_i) = \phi_j(\mu_{ij}(x_i)) = \phi(\mu_j(\mu_{ij}(x_i))) = \phi(\mu_j(x_j))$$

□

Proposition 7.9. *Using the notation of definition 7.14 with $\{P_i, \eta_{ij}\}_{i,j\in\Lambda}$ being a third direct system with $P = \varinjlim P_i$ then a sequence of direct systems*

$$M \xrightarrow{f} N \xrightarrow{g} P \tag{7.9}$$

is exact at N if the corresponding homorphisms f_i and g_i are exact for each sequence $M_i \xrightarrow{f_i} N_i \xrightarrow{g_i} P_i$.

Proof. This follows easily by representing f and g as homorphisms on M_i,N_i and P_i □

Corollary 7.1. *The functor $\varinjlim$ as functor from the category of direct systems of modules to the category of modules is an exact covariant functor.*

Theorem 7.6. *Let $\{M_i, \mu_{ij}\}_{i,j\in\Lambda}$ be a direct system and let N be any A-module. Let $P = \varinjlim(M_i \otimes N)$ be the direct limit of the direct system $\{M_i \otimes N, \mu_{ij} \otimes 1\}_{i,j\in\Lambda}$. Let $\{\mu_i \otimes 1 : M_i \otimes N \to M \otimes N\}_{i\in\Lambda}$ be a collection of homorphism defining a homorphism on the direct limit $\psi : P \to M \otimes N$. Then ψ is an isomorphism.*

Proof. Consider the collection of A-bilinear mappings $\pi_i : M_i \times N \to M_i \otimes N$. This collection leads in a natural way to a homorphism on the direct limits $M \times N$ and $P = \varinjlim(M_i \otimes N)$; let's denote it $\pi : M \times N \to P$. Moreover

$$\pi((\mu_i \times 1)(x_i + y_i, n)) = \pi_i(x_i + y_i, n) = x_i \otimes n + y_i \otimes n = \pi((\mu_i \times 1)(x_i, n)) + \pi((\mu_i \times 1)(x_i, n))$$

so π is A-bilinear. As such π induces an A-module homorphism $\phi : M \otimes N \to P$ and it's easy to see that $\phi = \psi^{-1}$. □

APPENDIX 5: PROJECTIVE LIMITS.

Remark 7.2. Projective limits are also known as inverse limits. We present a limited selection of the basic properties.

Remark 7.3. It is typical to insist a directed set is a set in which every two points share an upper bound. We can alternately define directed sets to be sets in which every two points have a lower bound. For our purposes when we say directed set in relation to projective limits we will mean every two points have a lower bound.

Definition 7.15. Let Λ be a directed set. A projective system is a collection of modules $\{M_i\}_{i\in\Lambda}$and homorphisms $\mu_{ij} : M_j \to M_i$ with the following properties

- $\mu_{ii} = id_{M_i}$
- $\mu_{ik} = \mu_{ij} \circ \mu_{jk}$ for $i \leq j \leq k$

We will assume that $\{M_i\}_{i\in\Lambda}$ and $\{\mu_{ij}\}_{i,j\in\Lambda\, i\leq j}$ (also written $\{M_i, \mu_{ij}\}_{i,j\in\Lambda}$) is a projective system for the remainder of this appendix.

Definition 7.16. The projective limit of $\{M_i, \mu_{ij}\}_{i,j\in\Lambda}$ is the module

$$\varprojlim M_i = \{(m_i) \in \prod_{i\in\Lambda} M_i | \, \mu_{ij}(m_i) = m_j \text{ for all } i \leq j\}$$

The projection maps $\mu_i : M_i \to \varprojlim M_i$ are the restrictions of the canonical projection maps on $\prod_{i\in\Lambda} M_i$.

Proposition 7.10. $\mu_i = \mu_i \circ \mu_{ij}$

Proof. Trivial □

Theorem 7.7. *Let N be any A-module and suppose there is a collection of maps $\alpha_i : N \to M_i$ with $\alpha_i = \mu_{ij} \circ \alpha_j$. Let $M = \varprojlim M_i$. Then there is a unique map $\alpha : N \to M$ such that $\alpha_i = \mu_i \circ \alpha$.*

Proof. For $n \in M$ define $\alpha(n) = (\alpha_i(n))$ then clearly $\alpha_i = \mu_i \circ \alpha$ and α is unique. □

Remark 7.4. It's possible to formulate the same construction in many categories. One could let the M_i be topological spaces and the μ_{ij} continuous functions. Alternatively the M_i could be groups and the μ_{ij} group homomorphisms.