Basics of Group Cohomology

Shubhrajit Bhattacharya
Chennai Mathematical Institute
shubhrajit@cmi.ac.in

Contents

Group Cohomology

G-modules

Let G be a group, written multiplicatively and A be an abelian group, written additively. We say that G acts on A if there is a group homomorphism

$$\rho : G \longrightarrow \text{Aut}(A)$$

Definition 1. *An abelian group A is said to be a G-module if G acts on A.*

But, then how it is a module and what is even the base ring here? Well, to answer that, consider the set $\mathbb{Z}[G]$ of formal sums of the form

$$\sum_{g\in G} n_g g \quad n_g \in \mathbb{Z}$$

The sum and product on the set $\mathbb{Z}[G]$ is defined as follows

$$\sum_{g\in G} n_g g + \sum_{g\in G} m_g g = \sum_{g\in G}(n_g + m_g)g$$
$$\left(\sum_{g\in G} n_g g\right)\cdot\left(\sum_{g\in G} m_g g\right) = \sum_{\substack{g\in G\\ h\in G}} n_g m_h (gh)$$

Thus the ring structure in $\mathbb{Z}[G]$ is clear. We define the left-multiplication with elements from A by elements from $\mathbb{Z}[G]$ as follows

$$\left(\sum_{g\in G} n_g g\right) a = \sum_{g\in G} n_g (ga)$$

ga is the action of g on a. Since A is an *abelian* group, $\sum_{g\in G} n_g(ga) \in A$. This makes A into a $\mathbb{Z}[G]$-module.

Definition 2 (**G-module homomorphism**)**.** *Let M, N be G-modules. A G-module homomorphism is a group homomorphism $\varphi : M \longrightarrow N$ such that $\varphi(gm) = g\varphi(m)$ for all $m \in M$.*

here gm denotes the action of g on m and $g\varphi(m)$ denotes the action of g on $\varphi(m)$. For a G-module A, let A^G be the abelian group of G-invariant points, *i.e.*

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

It can be easily verified that if $f : A \longrightarrow B$ is a G-module homomorphism then, then f restricted to A^G maps to B^G and hence we get a group homomorphism $f : A^G \longrightarrow B^G$. The assignment $A \mapsto A^G$ defines a functor from the category of G-modules to the category of abelian groups. This functor is *left exact* but not *right exact*, *i.e.* for any shot exact sequence of G-modules

$$0 \longrightarrow A \longrightarrow A' \longrightarrow A'' \longrightarrow 0$$

Then the following sequence is also exact

$$0 \longrightarrow A^G \longrightarrow (A')^G \longrightarrow (A'')^G$$

But, not necessarily the map $(A')^G \longrightarrow (A'')^G$ is not necessarily surjective. An example is as follows, consider the short exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0$$

of $\mathbb{Z}/p\mathbb{Z}$-modules, where $\mathbb{Z}/p\mathbb{Z}$ acts on the middle factor by the rule $g(a) = a(1+pg)$. Then the map $(\mathbb{Z}/p^2\mathbb{Z})^{\mathbb{Z}/p\mathbb{Z}} \longrightarrow (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}/p\mathbb{Z}}$ is the 0 map but $(\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}/p\mathbb{Z}}$ is non-trivial. Therefore this functor is not *right exact*.

Injective G-modules

Definition 3 (**Injective G-module**). *A G-module M is said to be injective if for every inclusion $A \subset B$ of G-modules and G-module homomorphism $\varphi : A \longrightarrow M$, there exists a G-module homomorphism $\psi : B \longrightarrow M$ such that $\psi|_A = \varphi$.*

We prove the key theorem here.

Theorem 1. *Every G-module A can be embedded into an injective G-module.*

Proof. We will need the following two lemmas:

Lemma 1. *Let G be the trivial group. Then every abelian group is a G-module. An abelian group A is injective if and only if A is divisible, i.e. the map $x \mapsto nx$ is surjective for all $n \in \mathbb{N}$.*

Proof. Let A be injective. Let, if possible, A be not divisible. Then, there exists $n > 1$ and $y \in A$ such that $nx \neq y$ for any $x \in A$. Consider the map $\mathbb{Z} \longrightarrow A$ given by $m \mapsto my$. Then this is a G-module homomorphism as it is a group homomorphism. But since $y \neq nx$ for all $x \in A$, the map $(m \mapsto my)$ can't be extended to $\frac{1}{n}\mathbb{Z}$, but $\mathbb{Z} \subset \frac{1}{n}\mathbb{Z}$ is an inclusion of abelian groups. A contradiction!

Conversely suppose, A is divisible, *i.e.* the map $x \mapsto nx$ is surjective for all $n \in \mathbb{N}$. Let $M \subset N$ be an inclusion of abelian groups and $\varphi : M \longrightarrow A$ be a group homomorphism. Then consider the set S of pairs (M', φ') where $M \subset M' \subset N$ and $\varphi' : M' \longrightarrow A$ a group homomorphism such that $\varphi|_A = \varphi$. This set is nonempty since $(M, \varphi) \in S$. We define a partial order on S, as follows, we say that

$$(M_1, \varphi_1) \leq (M_2, \varphi_2)$$

if $M_1 \subset M_2$ and $\varphi_2|_{M_1} = \varphi_1$. For any chain in S of the form $(M_i, \varphi_i)_{i \in I}$ for some indexing set I. We get a map $\boldsymbol{\varphi} : \bigcup_{i \in I} M_i \longrightarrow A$ given by $a (\in M_i) \mapsto \varphi_1(a)$. Then we get that $\left(\bigcup_{i \in I} M_i, \boldsymbol{\varphi}\right)$ is an upper bound for the chain $(M_i, \varphi_i)_{i \in I}$. The Zorn's lemma applies and we get a maximal element $(\mathcal{M}, \psi)$. We claim that $\mathcal{M} = N$. Suppose the contrary. Then choose $h \in N \setminus \mathcal{M}$ and consider the subgroup $\langle h \rangle$ of N. If $\mathcal{M} \cap \langle h \rangle = \emptyset$ then the sum $\mathcal{M} \oplus \langle h \rangle$ is a larger subgroup of N than $\mathcal{M}$ and we can extend ψ to $\mathcal{M} \oplus \langle h \rangle$ by defining ψ at h arbitrarily and extending by linearity.

Now, let $\mathcal{M} \cap \langle h \rangle \neq \emptyset$. Take $nh \in \mathcal{M} \cap \langle h \rangle$ so that n is minimal. Then $\psi(nh)$ makes sense as $nh \in \mathcal{M}$. Since A is divisible, there exists $g \in A$ so that $ng = \psi(nh)$. By defining $\psi(h) := g$, we get an extension of ψ to $\mathcal{M} \oplus \langle h \rangle$. This is a contradiction to the maximality of $(\mathcal{M}, \psi)$. Therefore $N = \mathcal{M}$. □

Lemma 2. *Every abelian group A can be embedded inside an injective abelian group.*

Proof. Consider the abelian group $\mathbb{Q}/\mathbb{Z}$. This is clearly divisible and hence injective by *lemma 1*. Consider the abelian group A. Let $a \in A$ be a nonzero element. Consider the subgroup $\langle a \rangle \subset A$. Then define a map $\varphi_a : \langle a \rangle \longrightarrow \mathbb{Q}/\mathbb{Z}$ by the following rule

$$\varphi_a(a) = \begin{cases} 1 & \text{when } a \text{ has infinite order} \\ \frac{1}{n} & \text{when order of } a \text{ is } n \in \mathbb{N} \end{cases}$$

Since $\mathbb{Q}/\mathbb{Z}$ is injective, there exists $\psi_a : A \longrightarrow \mathbb{Q}/\mathbb{Z}$ which extends φ_a. By the universal property of product in a category, this collection $\{\psi_a\}_{a \in A \setminus \{0\}}$ defines a unique map

$$\psi : A \longrightarrow \prod_{a \in A \setminus \{0\}} \mathbb{Q}/\mathbb{Z}$$

By definition $\psi_a(a) = 0$ if and only if $a = 0$. Thus ψ is an injective map. Thus we get an embedding of A into $\prod_{a \in A \setminus \{0\}} \mathbb{Q}/\mathbb{Z}$, which is an injective and hence divisible group. □

By *lemma 5* and *lemma 6* we get that the abelian group A can be embedded into a divisible group B. Using that we can embed A into $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], B)$ and $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], B)$ is an injective G-module. □

Following *theorem 1*, we embed A into an injective G-module I_0, then embed I^0/A to a G-module I^1 and continue the process. We get a long exact sequence

$$0 \longrightarrow A \longrightarrow I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \longrightarrow \cdots$$

Definition 4 (Injective resolution). *The exact sequence obtained above is called an injective resolution of A.*

Starting with an *injective resolution* of A and then taking the G-invariant functor, we get a *cochain complex*

$$0 \longrightarrow (I^0)^G \xrightarrow{d^0} (I^1)^G \xrightarrow{d^1} (I^2)^G \xrightarrow{d^2} \cdots$$

i.e., $d^{(i+1)} \circ d^i = 0$ or, in other words, $\mathrm{im}(d^i) \subseteq \ker(d^{(i+1)})$. By definition, d^{-1} is the 0-map $0 \longrightarrow (I^0)^G$. Then, we define the i^{th} cohomology group as follows

$$H^i(G, A) \coloneqq \frac{\ker(d^i)}{\mathrm{im}(d^{(i-1)})} \quad \forall\, i \geq 0$$

By definition, we can see that $H^0(G, A) = A^G = \{a \in A : ga = a \;\forall\, g \in G\}$. Let M, N be two G-modules and let $\mathrm{Hom}_G(M, N)$ be the group of all G-module maps $f : M \longrightarrow N$. Let $\varphi \in \mathrm{Hom}_G(M, N)$. Take two injective resolutions

$$0 \longrightarrow M \longrightarrow I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \longrightarrow \cdots$$
$$0 \longrightarrow N \longrightarrow J^0 \xrightarrow{d^0} J^1 \xrightarrow{d^1} J^2 \longrightarrow \cdots$$

Note the abuse of notations: we have used d^i for both the injective resolutions even though they are not the same!

Then, by *theorem 1*, we get the following commutative diagram

$$\begin{array}{ccccccccccc}
0 & \longrightarrow & M & \longrightarrow & I^0 & \xrightarrow{d^0} & I^1 & \xrightarrow{d^1} & I^2 & \xrightarrow{d^2} & \cdots \\
 & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \\
0 & \longrightarrow & N & \longrightarrow & J^0 & \xrightarrow{d^0} & J^1 & \xrightarrow{d^1} & J^2 & \xrightarrow{d^2} & \cdots
\end{array}$$

Figure 1

Now, taking the G-invariant functor, the vertical arrows in *figure 8* induce maps

$$H^i(\varphi) : H^i(G, M) \longrightarrow H^i(G, N)$$

between cohomology groups.

Right derived functors

The following is a pretty straightforward observation

Proposition 1. *For a fixed choice of injective resolutions for M and N, the maps on cohomology groups, i.e., $H^i(\varphi) : H^i(G, M) \longrightarrow H^i(G, N)$ do not depend on the choice of the maps φ_i's.*

Proof. It's enough to prove that if $\varphi = 0$, then $H^i(\varphi) = 0$ for all i regardless of the choice of φ_i's. We construct maps $g_i : I^{(i+1)} \longrightarrow J^i$, with the convention that g^{-1} is the 0-map, such that $\varphi_i = g_i \circ d^i + d^{(i-1)} \circ g_{i-1}$. We construct it inductively given the existence of φ_{i-1}, g_{i-1} and the injectivity of J_i's. Suppose that we have constructed g_{i-1}. We now have the following diagram:

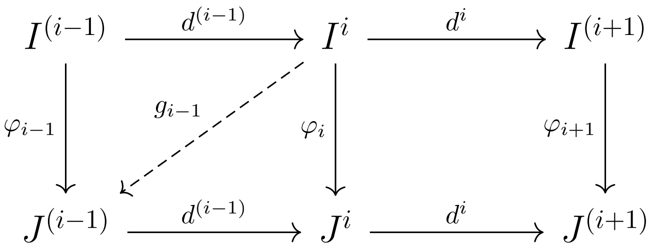

Figure 2

In $\varphi_i = g_i \circ d^i + d^{(i-1)} \circ g_{i-1}$, d^i is the map $I^i \longrightarrow I^{(i+1)}$ and $d^{(i-1)}$ is the map $J^{(i-1)} \longrightarrow J^i$. We have the inclusion of G-modules $\mathrm{im}(d^i) \subseteq I^{(i+1)}$. We define the map $\tilde{g}_i : \mathrm{im}(d^i) \longrightarrow J^i$ as follows: Let $a \in \mathrm{im}(d^i)$ Then there exists $b \in I^i$ such that $a = d^i(b)$. Then

$$\tilde{g}_i(a) \coloneqq \varphi_i(b) - d^{(i-1)}(g_{i-1}(b))$$

We claim that this map is well defined. Let $b_1, b_2 \in I^i$ such that $d^i(b_1) = a = d^i(b_2)$. Since $d(b_1 - b_2) = 0$, $b_1 - b_2 \in \ker(d^i) = \mathrm{im}(d^{(i-1)})$. There exists $b_\circ \in I^{(i-1)}$, such that $d^{(i-1)}(b_\circ) = b_1 - b_2$. Then we must prove

$$\begin{aligned} \varphi_i(b_1) - d_{i-1}(g^{(i-1)}(b_1)) &= \varphi_i(b_2) - d^{(i-1)}(g^{(i-1)}(b_2)) \\ \iff \varphi_i(b_1 - b_2) &= d^{(i-1)}(g_{i-1}(b_1 - b_2)) \\ \iff \varphi_i(d^{(i-1)}(b_\circ)) &= d^{(i-1)}(g_{i-1}(d^{(i-1)}(b_\circ))) \qquad (\dagger) \end{aligned}$$

Hence it's equivalent to show $(\dagger)$. By induction hypothesis, $\varphi_{i-1} = g_{i-1} \circ d^{(i-1)} + d^{(i-2)} \circ g_{i-2}$. Then

$$\begin{aligned} \varphi_{i-1}(b_\circ) &= g_{i-1} \circ d^{(i-1)}(b_\circ) + d^{(i-2)} \circ g_{i-2}(b_\circ) \\ \implies d^{(i-1)}(\varphi_{i-1}(b_\circ)) &= d^{(i-1)}(g_{i-1} \circ d^{(i-1)}(b_\circ) + d^{(i-2)} \circ g_{i-2}(b_\circ)) \\ &= d^{(i-1)}(g_{i-1}(d^{(i-1)}(b_\circ))) \qquad (\ddagger) \\ & \qquad (\text{since } d^{(i-1)} \circ d^{(i-2)} = 0) \end{aligned}$$

Since *figure 1* is commutative, we get that

$$\varphi_i(d^{(i-1)}(b_\circ)) = d^{(i-1)}(\varphi_{i-1}(b_\circ)) \qquad (\spadesuit)$$

Comparing $(\spadesuit)$ and $(\ddagger)$ we get $(\dagger)$. The base case is $g_{-1} = 0$, thus we have constructed a map $\tilde{g}_i : \mathrm{im}(d^i) \longrightarrow J^i$. Since J^i is an injective G-module and $\mathrm{im}(d^i) \subseteq I^{(i+1)}$ is an inclusion of G-modules, there exists $g_i : I^{(i+1)} \longrightarrow J^i$ such that $g_i|_{\mathrm{im}(d^i)} \equiv \tilde{g}_i$. This g_i is the desired map as we can easily verify the relation $\varphi_i = g_i \circ d^i + d^{(i-1)} \circ g_{i-1}$. This completes the induction step and hence the proof of existence of such collection of maps $\{g_i\}_{i \geq -1}$. From these maps we can conclude that $H^i(\varphi)$ are all 0-maps. Hence $H^i(\varphi)$ is dependent only on φ. The following *noncommutative* diagram sums up the construction

$$\begin{array}{cccccccccc}
0 & \longrightarrow & M & \longrightarrow & I^0 & \xrightarrow{d^0} & I^1 & \xrightarrow{d^1} & I^2 & \xrightarrow{d^2} \\
 & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi_0} & \overset{g_0}{\swarrow} & \downarrow{\scriptstyle \varphi_1} & \overset{g_1}{\swarrow} & \downarrow{\scriptstyle \varphi_2} & \\
0 & \longrightarrow & N & \longrightarrow & J^0 & \xrightarrow{d^0} & J^1 & \xrightarrow{d^1} & J^2 & \xrightarrow{d^2}
\end{array}$$

Figure 3

□

Definition 5 (Cochain homotopy). *The maps g_i, constructed above, are called cochain homotopy.*

We make a wonderful observation. Let $M = N$ and $\varphi : M \longrightarrow N$ be the identity map. Then $H^i(\varphi)$ are the canonical induced maps $H^i(\varphi) : H^i(G, M) \longrightarrow H^i(G, N) = H^i(G, M)$. This shows that $H^i(G, M)$ are unique up to isomorphism and independent of the choice of injective resolution. Similarly, the maps $H^i(\varphi)$ are also independent of the choice of injective resolution and the maps φ_i's. Hence H^i defines a functor from the category $\boldsymbol{G}$-**Mod** of G-modules to the category **Ab** of *abelian* groups.

Definition 6 (Right derived functors). *The functors H^i from $\boldsymbol{G}$-**Mod** to **Ab** are called the right derived functors of the G-invariant functor.*

Proposition 2 (Short to Long Exact Sequence in Cohomolgy). *Given any short exact sequence*

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$

There is a corresponding long exact sequence

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(G, M) & \longrightarrow & \cdots & \longrightarrow & H^i(G, M'') & \xrightarrow{\delta_i} & H^{i+1}(G, M) \\
 & & & & & & & & \downarrow \\
 & & \longleftarrow & \cdots & \longleftarrow & H^{i+1}(G, M'') & \longleftarrow & & H^{i+1}(G, M')
\end{array}$$

Figure 4

The maps δ_i are called the connecting homomorphism.

Proof. The proof is based on the following lemma, the so-called snake lemma

Lemma 3 (Snake lemma). *For any commutative diagram with exact rows, as below,*

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M & \longrightarrow & M' & \longrightarrow & M'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_0} & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \\
0 & \longrightarrow & N & \longrightarrow & N' & \longrightarrow & N'' & \longrightarrow & 0
\end{array}$$

Figure 5

there exists a canonical map $\delta : \ker(f_2) \longrightarrow \operatorname{coker}(f_0)$ *forming the following long exact sequence*

$$0 \longrightarrow \ker(f_0) \longrightarrow \ker(f_1) \longrightarrow \ker(f_2) \xrightarrow{\delta} \operatorname{coker}(f_0) \longrightarrow \operatorname{coker}(f_1)\operatorname{coker}(f_2) \longrightarrow 0$$

Proof. We just sketch how to define the map δ. Let $x \in \ker(f_2) \subseteq M''$. Exactness of the upper row tells us the map $M' \longrightarrow M''$ is surjective. Choose $y \in M'$ so that the image of y in M'' is x. Then we push y to N' via f_1. Again exactness tells us that there is a preimage of $f_1(y)$ in N. Thus we get δ. The independence on the choice of y can be proved likewise we did earlier using the exactness of commutativity of *figure 12*. □

we can use the snake lemma to finish the proof. □

Proposition 3. *Let M be an injective G-module. Then $H^i(G, M) = 0$ for all $i \geq 1$.*

Proof. Since M is injective itself, we can take $I^0 = M$. Thus we get the following injective resolution for M

$$0 \longrightarrow M \longrightarrow M \longrightarrow 0 \longrightarrow 0 \longrightarrow \cdots$$

Since $H^i(G, M)$ are independent of the choice of the injective resolution, we get that $H^i(G, M) = 0$ for all $i \geq 1$. □

Definition 7 (**Acyclic module**)**.** *Let M be a G-module. Then M is said to be acyclic if $H^i(G, M) = 0$ for all $i \geq 1$.*

Proposition 3 shows us that an injective module is acyclic. We note the existence of a simple injective resolution in case of an injective module. It turns out that we can replace injective resolution in the definition by an acyclic resolution for the purposes of doing a computation. We state the following proposition in this regard

Proposition 4. *Let*

$$0 \longrightarrow M \longrightarrow M_0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow \cdots$$

be an exact sequence of G-modules with each M_i acyclic. Consider the cochain complex obtained by applying the G-invariant functor

$$0 \longrightarrow (M_0)^G \longrightarrow (M_1)^G \longrightarrow (M_2)^G \longrightarrow \cdots$$

The cohomology groups of this cochain complex coincides with the cohomology groups $H^i(G, M)$.

Two important consequences of the long exact sequence

(•) Let

$$0 \longrightarrow M \longrightarrow M' \longrightarrow M'' \longrightarrow 0$$

be an exact sequence of G-modules and $H^1(G, M) = 0$, then

$$0 \longrightarrow M^G \longrightarrow (M')^G \longrightarrow (M'')^G \longrightarrow 0$$

is also an exact sequence.

(••) Let M' be acyclic in the short exact sequence above. Then the *connecting homomorphisms* δ_i are isomorphisms

$$H^i(G, M'') \overset{\delta_i}{\cong} H^{i+1}(G, M)$$

Cohomology of finite groups

Observe that if G is the one element group, then any G-module is acyclic. This is because starting with any injective resolution of M, taking G-invariant does not the affect the exactenss and hence the cohomology groups are all trivial. In fact, G-modules are precisely the *abelian* groups. Thus every abelian group, thought as a G-module for the trivial group G, is acyclic.

Let G be any group and $H \leq G$ be any subgroup. Let M be an H-module. Then it is a natural question to ask if we can somehow upgrade M to get a G-module. We know that M is actually a $\mathbb{Z}[H]$-module for the group ring $\mathbb{Z}[H]$. Also, H being a subgroup, $\mathbb{Z}[G]$ is also a $\mathbb{Z}[H]$-module. Then we take the tensor product $M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$. Clearly this becomes a $\mathbb{Z}[G]$-module over the group ring $\mathbb{Z}[G]$ and hence a G-module.

Definition 8 (Induction). *Let M be an H-module for some subgroup $H \leq G$ of a group G. We define the induction of M from H to G, denoted by $\mathrm{Ind}_H^G(M)$, is defined to be*

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

We may also identify $\mathrm{Ind}_H^G(M)$ with the set of maps $\phi : G \longrightarrow M$ such that $\phi(gh) = h \cdot \phi(g)$ for all $h \in H$ and $g \in G$. The action of G on $\mathrm{Ind}_H^G(M)$ is given by $g \cdot \phi(g') = \phi(gg')$. $\mathbb{Z}[G]$ contains a copy of G inside it. Let $[g] \in \mathbb{Z}[G]$ be the image of $g \in G$ in $\mathbb{Z}[G]$. The element $m \otimes [g] \in M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$ corresponds to the map $\varphi_{m,g} : G \longrightarrow M$ given by

$$\varphi_{m,g}(g') = \begin{cases} (gg') \cdot m & gg' \in H \\ 0 & gg' \notin H \end{cases} \qquad \forall\, g' \in G$$

Theorem 2 (**Shapiro's lemma**). *Let H be a subgroup of G and N is an H-module. There is a canonical isomorphism*

$$H^i(G, \mathrm{Ind}_H^G(N)) \longrightarrow H^i(H, N)$$

In particular, N is acyclic if and only if $\mathrm{Ind}_H^G(N)$ is acyclic.

Proof. We only sketch the key points of the proof.

1. It is easy to check that

$$H^0(G, \mathrm{Ind}_H^G(N)) = (\mathrm{Ind}_H^G(N))^G = N^H = H^0(H, N)$$

2. The functor Ind_H^G from ***H*-Mod** to ***G*-Mod** is both right and left exact, *i.e.*, for every injective $\mathbb{Z}[H]$-module map $\varphi : A \longrightarrow B$, the induced map

$$\varphi \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G] : A \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G] \longrightarrow B \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$$

given by $a \otimes [g] \mapsto \varphi(a) \otimes [g]$ is also injective. In face, $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module.

3. If I is an injective H-module then $\mathrm{Ind}_H^G(I)$ is an injective G-module. For proving this we need the following lemma

Lemma 4. *Let H be a subgroup of G, let M be a G-module, and let N be an H-module. Then there are natural isomorphisms*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \cong \mathrm{Hom}_H(M, N)$$
$$\mathrm{Hom}_G(\mathrm{Ind}_H^G(N), M) \cong \mathrm{Hom}_H(N, M)$$

Proof. Wherever in the proof I put a '$\cdot$', I mean group action and only juxtaposition means product in either group or module. First we consider the case $M = N$. Then the identity map $M \longrightarrow N = M$ corresponds to the following maps:

$\Phi : \mathrm{Ind}_H^G(M) \longrightarrow M$ given by

$$\sum_{g \in G} m_g \otimes [g] \longmapsto \sum_{g \in G} g \cdot m_g$$

$\Psi : M \longrightarrow \mathrm{Ind}_H^G(M)$ given by

$$m \longmapsto \sum_i (g_i \cdot m) \otimes [g_i^{-1}]$$

where the sum is taken over a set distinct representatives g_i of left cosets of H in G, given that $[G : H] < \infty$. The map Ψ doesn't depend on the choice of g_i's and hence

$$\Psi(g \cdot m) = \Psi\left(\sum_i (gg_i \cdot m) \otimes [(gg_i)^{-1}]\right)[g] = \Psi(m)[g]$$

Therefore Ψ is clearly compatible with G-action.

Now, let N be any H-module. Let $\varphi \in \mathrm{Hom}_H(M, N)$. Then we get a map

$$\varphi \otimes \mathbb{Z}[G] : \mathrm{Ind}_H^G(M) \longrightarrow \mathrm{Ind}_H^G(N)$$

given by $m \otimes [g] \mapsto \varphi(m) \otimes [g]$. Therefore

$$(\varphi \otimes \mathbb{Z}[G]) \circ \Psi : M \longrightarrow \mathrm{Ind}_H^G(N)$$

is the required map in $\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N))$. This gives a map

$$\mathrm{Hom}_H(M, N) \longrightarrow \mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N))$$

We have similar maps, as Φ and Ψ,

$$\tilde{\Phi} : \mathrm{Ind}_H^G(N) \longrightarrow N$$
$$\tilde{\Psi} : N \longrightarrow \mathrm{Ind}_H^G(N)$$

Let $\tilde{\varphi} \in \mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N))$. Then, for any $m \in M$, $\tilde{\varphi}(m) \in \mathrm{Ind}_H^G(N)$ can be identified with a map $\phi : G \longrightarrow N$. Now, compose with the map $\tilde{\Phi}$ to get the map which takes ϕ to $\phi(e) \in N$. Thus we get a map

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \longrightarrow \mathrm{Hom}_H(M, N)$$

On the other hand, let $\psi \in \mathrm{Hom}_H(N, M)$. This induces the map

$$\psi \otimes \mathbb{Z}[G] : \mathrm{Ind}_H^G(N) \longrightarrow \mathrm{Ind}_H^G(M)$$

Then $\Phi \circ (\psi \otimes \mathbb{Z}[G])$ is the required map in $\mathrm{Hom}_G(\mathrm{Ind}_H^G(N), M)$. Hence we get a map

$$\mathrm{Hom}_H(N, M) \longrightarrow \mathrm{Hom}_G(\mathrm{Ind}_H^G(N), M)$$

On the other hand, let $\tilde{\psi} \in \mathrm{Hom}_G(\mathrm{Ind}_H^G(N), M)$. We have a map

$$\tilde{\Psi} : N \longrightarrow \mathrm{Ind}_H^G(N)$$

Using this we get a map (evaluating on $n \otimes [e]$) $N \longrightarrow M$. This completes the proof. $\square$

Using these three steps we can establish the proof of *Shapiro's lemma.* □

Definition 9 (**Induced G-module**). *A G-module is said to be induced it there exists and abelian group, i.e., a $\{1\}$-module, such that $M = \mathrm{Ind}_1^G(N) \cong M \otimes_{\mathbb{Z}} \mathbb{Z}[G]$.*

Corollary 1. *Induced G-modules are acyclic.*

Proof. There exists a $\{1\}$-module (*i.e.*, an abelian group) N so that $M = \mathrm{Ind}_1^G(N)$. By *Shapiro's lemma*,

$$H^i(G, M) = H^i(G, \mathrm{Ind}_1^G(N)) \cong H^i(\{1\}, N) = 0 \qquad \forall\, i > 0$$

Hence M is acyclic. □

Corollary 2. *Let L/K be a Galois extension, then L naturally is a G-module for $G = \mathrm{Gal}(L/K)$. We have*

$$H^i(\mathrm{Gal}(L/K), L) = 0 \qquad \forall\, i > 0$$

Proof. According to the *normal basis theorem*, there exists $\alpha \in L$ such that

$$\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$$

is a K-basis of L as a K-vector space. Consider the map $K \otimes_{\mathbb{Z}} \mathbb{Z}[G] \longrightarrow L$ given by $k \otimes [\sigma] \mapsto k\sigma(\alpha)$. Since every element of L can be uniquely written as $\sum_{\sigma \in G} k_\sigma \sigma(\alpha)$ for $k_\sigma \in K$, we get that $L \cong K \otimes_{\mathbb{Z}} \mathbb{Z}[G] \cong \mathrm{Ind}_1^G(K)$. By *corollary 3*, we are done. □

Definition 10. *For any cochain complex $(A^\bullet, d^\bullet)$, the elements of A^i are called i-cochains, elements of $\ker(d^i)$ are called i-cocycles and elements of $\mathrm{im}(d^{(i-1)})$ are called i-coboundaries.*

The first cohomology group $H^1(G, M)$

We give a description of $H^1(G, M)$ for a G-module M that is useful for computational purposes. Let

$$C^1(G, M) := \{\varphi : G \longrightarrow M\}$$

be the 1-cochains,

$$Z^1(G, M) := \{\varphi \in C^1(G, M) : \varphi(gh) = g \cdot \varphi(h) + \varphi(g)\}$$

be the 1-cocycles or the crossed homomorphisms and

$$B^1(G, M) := \{\varphi \in C^1(G, M) : \exists\, m \in M, \varphi(g) = g \cdot m - m\ \forall\, g \in G\}$$

be the 1-boundaries. Then

$$H^1(G, M) = \frac{Z^1(G, M)}{B^1(G, M)}$$

The second cohomology group $H^2(G, M)$

A 2-cocycle is a map $f : G \times G \longrightarrow M$ satisfying

$$g_1 \cdot f(g_2, g_3) - f(g_1 g_2, g_3) + f(g_1, g_2 g_3) - f(g_1, g_2) = 0$$

for all $g_1, g_2, g_3 \in G$. It classifies the short exact sequences

$$1 \longrightarrow M \longrightarrow E \longrightarrow G \longrightarrow 1$$

for a fixed action of G on M.

Extended functoriality

Let M be a G-module and M' be a G'-module. Suppose that $\alpha : G' \longrightarrow G$ be a given group homomorphism. Let $\beta : M \longrightarrow M'$ be an abelian group homomorphism such that $\beta(\alpha(g) \cdot m) = g \cdot \beta(m)$ for all $m \in M, g \in G'$. This gives a canonical homomorphism

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

Below are some principal examples of *extended functoriality*

(1) The cohomology groups don't seem to carry a nontrivial G-action, because we compute them by taking G-invariants. This can be reinterpreted in terms of extended functoriality: let $\alpha : G \longrightarrow G$ be the conjugation by some fixed h,*i.e.*, $g \mapsto h^{-1}gh$ and let $\beta : M \longrightarrow M$ be the map $m \mapsto h \cdot m$. Then the induced homomorphisms $H^i(G, M) \longrightarrow H^i(G.M)$ are all identity maps.

(2) [Restriction map] Let $H \leq G$ be a subgroup of G and M a G-module. Then M is also an H-module. Let M' be the same M but the G-action forgot except H. Then we get the restriction map

$$\text{Res} : H^i(G, M) \longrightarrow H^i(H, M)$$

This can be obtained in another way using the map $M \longrightarrow \text{Ind}_H^G(M)$ given by $m \mapsto \sum_i (g_i \cdot m) \otimes [g_i^{-1}]$. Then we get the following by *Shapiro's lemma*

$$H^i(G, M) \longrightarrow H^i(G, \text{Ind}_H^G(M)) \xrightarrow{\sim} H^i(H, M)$$

(3) [Corestriction map] Let M be a G-module and consider the map $\text{Ind}_H^G(M) \longrightarrow M$ given by $m \otimes [g] \mapsto g \cdot m$. This gives, applying *Shapiro's lemma*, the following so-called corestriction map

$$\text{Cor} : H^i(H, M) \xrightarrow{\sim} H^i(\text{Ind}_H^G(M), M) \longrightarrow H^i(G, M)$$

(4) The composition Cor ∘ Res is given by

$$m \mapsto \sum_i (g_i \cdot m) \otimes [g_i^{-1}] \mapsto \sum_i m = [G : H]m$$

Thus the composition Cor∘Res : $M \longrightarrow M$ is the multiplication by the index $[G : H]$.

Consequence. Let H be the trivial group. Then $H^i(H, M) = 0$ for all $i > 0$. In this case the composition Cor ∘ Res is multiplication by $[G : H] = |G|$ map, *i.e.*, $m \mapsto |G|m$. Thus every cohomology group $H^i(G, M)$ is annihilated by $|G|$. Therefore M is a torsion module but not necessarily finite. In particular, when M is finitely generated, $H^i(G, M)$ are finitely generated and being annihilated by $|G|$, we get that $H^i(G, M)$ are all finite.

(5) [Inflation map] Let $H \trianglelefteq G$ be a normal subgroup. Let $\alpha : G \longrightarrow G/H$ be the natural projection and $\beta : M^H \hookrightarrow M$ be the injection. Clearly G/H acts on M^H and hence M^H is a G/H-module. Then we get canonical homomorphism, the inflation homomorphism

$$\text{Inf} : H^i(G/H, M^H) \longrightarrow H^i(G, M)$$

Galois Cohomology

Galois cohomology is group cohomology with Galois groups. For this, we need to know about a certain kind of topology on Galois groups and profinite groups.

Profinite groups

A profinite group is a topological group which is Hausdorff and compact, and which admits a basis of neighborhoods of the identity consisting of normal subgroups. More explicitly, a profinite group is a group G plus a collection of subgroups of G of finite index designated as open subgroups, such that the intersection of two open subgroups is open, but the intersection of all of the open subgroups is trivial.

Definition 11 (**Profinite group**). *A Profinite group is a topological group which is the inverse limit of finite groups, each given the discrete topology.*

A profinite group is compact and totally disconnected. The converse is also true.

Proposition 5. *A compact totally disconnected topological group G is profinite.*

Proof. Since G is totally disconnected and compact, the open sets of G form a base of neighbourhoods of 1, the identity of G. Let U be an open subgroup of G. Consider the left cosets gU for $g \in G$. This is an open cover of G. Since G is compact, there are finitely many $g_1U, g_2U, \ldots, g_kU$ such that $G = \cup g_jU$. Then $[G : U] < \infty$. Therefore the conjugates gUg^{-1} for $g \in G$ are finite in number and their intersection V is both open and normal in G. Thus, we get a base of neighbourhoods of 1 which are normal subgroups of G. Consider the inverse limit

$$\varprojlim G/V$$

taken over the quotients G/V where V runs through the base of normal neighbourhoods of 1. The map $G \longrightarrow \varprojlim G/V$ is injective, continuous, and its image is dense; a compactness argument then shows that it is an isomorphism. Hence G is profinite. □

The most interesting and important example for us is any Galois group. Let L/K be a Galois extension, finite or infinite, the $\mathrm{Gal}(L/K)$ is a profinite group, in the following way:

By, construction, $\mathrm{Gal}(L/K)$ is the inverse limit of the Galois groups $\mathrm{Gal}(L_j/K)$ for finite Galois extensions $K \subseteq L_j \subseteq L$. Since each $\mathrm{Gal}(L_j/K)$ is finite and equipped with discrete topology, we get that $\mathrm{Gal}(L/K)$ is finite. For example

$$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim \mathrm{Gal}(K/\mathbb{Q}) \quad \forall\, K/\mathbb{Q},\, [K:\mathbb{Q}] < \infty$$

$$G_{\mathbb{F}_q} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) = \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$$

The profinite topology, *i.e.*, the topology on a Galois group induced by the inverse limit is special and is called the *Krüll topology.* We recall a theorem from the theory of topological groups

Theorem 3. *Let G be a topological group and $\mathcal{N}$ be a base of neighbourhoods of 1. Then the following are true*

- **(a)** *for all $N_1, N_2 \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $1 \in N' \subseteq N_1 \cap N_2$;*
- **(b)** *for all $N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $N'N' \subset \mathcal{N}$;*
- **(c)** *for all $N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $N' \subset N^{-1} = \{n^{-1} : n \in N\}$*
- **(d)** *for all $N \in \mathcal{N}$ and all $g \in G$, there exists an $N' \in \mathcal{N}$ such that $N' \subset gNg^{-1}$*
- **(e)** *for all $g \in G$, the set $\{gN : N \in \mathcal{N}\}$ is a base of neighbourhoods of g.*

*Conversely, if G is a group and $\mathcal{N}$ is a nonempty set of subsets of G satisfying **(a), (b), (c)** and **(d)**, then there is a (unique) topology on G for which **(e)** holds.*

Proof. Milne, Fields and Galois Theory, *proposition 7.2* □

Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$. Let $S \subset L$ be a finite set. The consider the set

$$G(S) := \{\sigma \in G : \sigma(s) = s \;\forall\, s \in S\}$$

This is a subgroup of G. We claim the following:

Proposition 6. *There is a unique structure of a topological group on G for which the sets $G(S)$ form an open neighbourhood base of* 1. *For this topology, the sets $G(S)$ with S G-stable form a neighbourhood base of 1 consisting of open normal subgroups.*

Proof. It is easy to see that for two finite subsets S_1, S_2 of L, $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$, $S_1 \cup S_2$ is finite. Hence (a) in *theorem 27* is true. Also, (b) and (c) are true since $G(S)$ is a subgroup of G. We now show that (d) is true as well. Let S be a finite subset of L. Then $K(S)/K$ is a finite extension. Then there are only finitely many K-homomorphisms $K(S) \longrightarrow L$. Since $\sigma|_{K(S)} = \tau|_{K(S)}$ implies $\sigma(S) = \tau(S)$, the set $\overline{S} := \cup_{\sigma \in G} \sigma S$ is finite. Now, $\sigma(\overline{S}) = \overline{S}$ for all $\sigma \in G$. Thus $G(\overline{S}) \trianglelefteq G$ and hence $\sigma G(\overline{S})\sigma^{-1} = G(\overline{S}) \subset G(S)$. Hence by *theorem 27*, there exists a unique topology on G such that $\{G(S) : S \subset L, |S| < \infty\}$ is a base of neighbourhoods of 1. □

Definition 12 (Krüll topology). *The topology generated by the base of neighbourhoods of 1, namely $G(S)$ for finite $S \subset L$, is called the Krüll topology on* $\mathrm{Gal}(L/K)$*.*

If L/K is a Galois extension, but not necessarily finite, we make $G = \mathrm{Gal}(L/K)$ into a profinite group by declaring that the open subgroups of G are precisely $\mathrm{Gal}(L/M)$ for all finite subextensions M of L.

Theorem 4 (Generalized Galois correspondence). *Let L/K be a Galois extension (not necessarily finite) and let $G = \mathrm{Gal}(L/K)$. There is a 1-1 correspondence between Galois subextensions $L/M/K$ and normal closed subgroups H given by*

$$H \longmapsto \mathrm{Fix}(H) \qquad M \longmapsto \mathrm{Gal}(L/M)$$

Proof. N. Jacobson, *Basic Algebra II*, *Theorem 8.16.* □

Cohomology of profinite groups

One can do group cohomology for groups which are profinite, not just finite, but one has to be a bit careful: these groups only make sense when you carry along the profinite topology.

Definition 13. *If G is profinite, by a G-module we mean a topological abelian group M with a continuous G-action on M. In particular, we say M is discrete if it has the discrete topology; that implies that the stabilizer of any element of M is open, and that M is the union of M^H over all open subgroups H of G. Canonical example:* $G = \mathrm{Gal}(L/K)$ *acting on L^*, even if L is not finite.*

The category of discrete G-modules has enough injectives, so we can find injective resolutions for M with discrete injective G-modules and define cohomology groups for any discrete G-module. The main point is that we can compute them from their finite quotients.

Proposition 7. *Let M be a discrete G-module for a profinite group G. The cohomology groups $H^i(G, M)$ are the direct limit of $H^i(G/H, M^H)$ for normal subgroups H and the direct limit is taken with respect to the inflation homomorphism*

$$\mathrm{Inf} : H^i(G/H, M^H) \longrightarrow H^i(G, M)$$

Proof. Milne, *Class Field Theory*, Proposition II.4.4. □

We have talked about the *inflation homomorphism* before as an example of *extended functoriality*. We give a formal definition below.

Definition 14 (Inflation homomorphism). *Let $H_2 \subseteq H_1 \subseteq G$ be inclusions of subgroups of finite index. Then we have the inflation homomorphism*

$$\mathrm{Inf} : H^i(G/H_1, M^{H_1}) \longrightarrow H^i(G/H_2, M^{H_2})$$

Via these maps, the groups $H^i(G/H, M^H)$ form an inverse system and *proposition 17* tells us that $H^i(G, M)$ is the direct limit of this system.

Hilbert's theorem 90 and some applications

Theorem 5 (Hilbert's Satz 90). *Let L/K be a finite Galois extension of fields with Galois group $G = \mathrm{Gal}(L/K)$. Let $L^\times$ be the multiplicative group of nonzero elements of L. Then $H^1(G, L^\times) = 0$. Moreover, $H^1(G_K, \overline{K}^\times) = 1$, wheher $G_K = \mathrm{Gal}(\overline{K}/K)$ is the absolute Galois group of K.*

Proof. We have to show that all 1-cocycles are 1-coboundaries. We denote the action of the elements of G on L by x^g for $g \in G, x \in L^\times$. Also, we assume that G is written multiplicatively. Then

$$H^1(G, L^\times) = \frac{Z^1(G, L^\times)}{B^1(G, L^\times)}$$

where

$$Z^1(G, L^\times) = \{f : G \longrightarrow L^\times : f(gh) = f(g)^h f(h) \text{ for all } g, h \in G\}$$
$$B^1(G, L^\times) = \{f : G \longrightarrow L^\times : f(g) = x(x^g)^{-1}\,\forall\, g \in G \text{ for some } x \in L^\times\}$$

Let $f \in Z^1(G, L^\times)$. Then the maps $\varphi_g : L^\times \longrightarrow L$ given by $x \mapsto x^g f(g)$ is an automorphism of L. By linear independence of automorphisms we get that

$$\sum_{g \in G} \varphi_g \not\equiv 0$$

Then there exists $x \in L$ such that

$$y = \sum_{g \in G} x^g f(g) \neq 0$$

Now, for any $h \in G$, we get that

$$y^h = \sum_{g \in G} x^{gh} f(g) = \sum_{g \in G} x^{gh} f(gh)(f(h))^{-1} = y(f(h))^{-1}$$

Then, $f \in B^1(G, L^\times)$. This shows that every 1-cocycle is a 1-coboundary and hence $H^1(G, L^\times) = 0$.

Now, the cohomology group $H^1(G_K, \overline{K}^\times)$ is, by definition, the following direct limit

$$H^1(G_K, \overline{K}^\times) = \varinjlim H^1(G_K/H, (\overline{K}^\times)^H)$$

Where the direct limit is taken through all open normal subgroups H of G and with respect to the inflation homomorphisms. For any such open normal subgroup H, $G_K/H \cong \mathrm{Gal}(L_H/K)$ and $(\overline{K}^\times)^H = L_H$ for some finite extension L_H/K. Thus by Hilbert's theorem 90 for finite extensions, we get that $H^1(G_K, \overline{K}^\times) = 1$ since $H^1(G_K/H, (\overline{K}^\times)^H) = 1$ for all open normal subgroups H of G_K. □

Corollary 3 (**The classical version of Hilbert's theorem 90**). *Let L/K be a finite cyclic extension (i.e., a Galosi extension with cyclic Galois group) and let σ be a generator of the Galois group $G = \mathrm{Gal}(L/K)$. Let $\alpha \in L$ be some element such that $\mathbf{N}_{L/K}(\alpha) = 1$. Then there exists $\beta \in L$ such that $\alpha = \beta/\sigma(\beta)$.*

Proof. Exercise. Hint: Use the fact that $\mathbf{N}_{L/K}(\alpha) = 1 \iff \alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha) = 1$, where $n = [L : K]$ and imitate the proof of **Theorem 5**. □

Corollary 4 (**Additive Hilbert's theorem 90**). *Let L/K be a finite cyclic extension and σ be a generator of the Galois group $\mathrm{Gal}(L/K)$. Let $\alpha \in L$ be such that $\mathbf{Tr}_{L/K}(\alpha) = 0$. Then there exists $\beta \in L$ such that $\alpha = \beta - \sigma(\beta)$.*

Proof. Exercise. Hint: Use the fact that $\mathbf{Tr}_{L/K}(\alpha) = 0 \iff \sum_{j=0}^{n-1} \sigma^j(\alpha) = 0$, where $n = [L : K]$. Now, try to define $\beta \in L$ explicitly. □

To demonstrate an application, we prove **Exercise 1.12.** from Silverman's AEC.

Problem.
(a) Let V/K be an affine variety. Prove that

$$K[V] = \{f \in \overline{K}[V] : f^\sigma = f \ \forall\, \sigma \in G_K\}$$

(b) Prove that

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n(\overline{K}) : P^\sigma = P \ \forall\, \sigma \in G_K\}$$

(c) Let $\phi : V_1 \longrightarrow V_2$ be a rational map of projective varieties. Prove that ϕ is defined over K if and only if $\phi^\sigma = \phi$ for all $\sigma \in G_K$.

Solution. Since $K[V] = K[X]/I(V/K)$, any $f \in K[V]$ is represented by a polynomial in $K[X]$. Then it's clear that $f^\sigma = f$ for all $\sigma \in G_K$. Therefore

$$K[V] \subset \{f \in \overline{K}[V] : f^\sigma = f \;\forall\, \sigma \in G_K\}$$

Let $F \in \overline{K}[X]$ such that $F \equiv f \pmod{I(V)}$, where f is some element of $\overline{K}[V]$ fixed by all $\sigma \in G_K$. Since $F \in \overline{K}[X]$, F^σ is not necessarily the same as F. The map $\sigma \mapsto F^\sigma - F$ is non-trivial. For any $\sigma, \tau \in G_K$, we get that

$$F^{\sigma\tau} - F = F^{\sigma\tau} - F^\sigma + F^\sigma - F = (F^\tau - F)^\sigma + (F^\sigma - F)$$

Also, $F^\sigma \equiv f^\sigma = f \equiv F \pmod{I(V)}$. Thus $F^\sigma - F \in I(V)$ for all $\sigma \in G_K$. This shows that the map $\sigma \mapsto F^\sigma - F$ is a 1-cocycle $G_K \longrightarrow I(V)$. Therefore, if we write

$$F(X) = \sum_\alpha a_\alpha X^\alpha$$

for $a_\alpha \in \overline{K}^+$, we get a 1-cocycle $G_K \longrightarrow \overline{K}^+$ and by $B.2.5a$, $H^1(G_K, \overline{K}^+) = 0$, thus they are 1-coboundaries. Thus there exists $G \in I(V)$ such that

$$\sigma \mapsto F^\sigma - F \equiv \sigma \mapsto G^\sigma - G \qquad \text{(for all } \sigma \in G_K)$$

This shows that

$$(F - G)^\sigma - (F - G) = 0 \;\forall\, \sigma \in G_K$$

Thus $F - G \in K[X]$. This shows that $f \in K[V]$. This completes the proof.

(b) Let

$$P \in \{\mathbb{P}^n(\overline{K}) : P^\sigma = P \;\forall\, \sigma \in G_K\}$$

and $P = [x_0 : x_1 : \cdots : x_n]$ be a homogeneous coordinate for $P \in \mathbb{P}^n(\overline{K})$. Since $P^\sigma = P$ as homogeneous coordinates, there exists $\lambda_\sigma \in \overline{K}^\times$ such that $x_i^\sigma = \lambda_\sigma x_i$ for $i = 0, 1, \ldots, n$. We claim that $\sigma \mapsto \lambda_\sigma$ is a 1-cocycle $G_K \longrightarrow \overline{K}^\times$. Indeed, for $\sigma, \tau \in G_K$, $x_i^{\sigma\tau} = \lambda_{\sigma\tau} x_i$. Also, $x_i^{\sigma\tau} = (x_i^\sigma)^\tau = \lambda_\tau x_i$ and $(x_i^\sigma)^\tau = (\lambda_\sigma x_i)^\tau = \lambda_\sigma^\tau x_i^\tau = \lambda_\sigma^\tau \lambda_\tau x_i$. Since $x_i \neq 0$ for at least one $0 \leq i \leq n$, we get that

$$\lambda_{\sigma\tau} = \lambda_\sigma^\tau \lambda_\tau \quad \forall\, \sigma, \tau \in G_K$$

By Hilbert's theorem 90, we get that there exists $\alpha \in \overline{K}^\times$ such that $\lambda_\sigma = \alpha^\sigma/\alpha$ for all $\sigma \in G_K$. Therefore, we get $x_i^\sigma = \alpha^\sigma/\alpha x_i$ or $(\beta x_i)^\sigma = \beta x_i$ for all $\sigma \in G_K$. Thus $\alpha x_i \in K$ for all $\sigma \in G_K$, where $\beta = \alpha^{-1}$. This shows that

$$P = P^\sigma = [\beta x_0 : \beta x_1 : \cdots : \beta x_n] \in \mathbb{P}^n(K)$$

Therefore $\{\mathbb{P}^n(\overline{K}) : P^\sigma = P \, \forall \, \sigma \in G_K\} \subset \mathbb{P}^n(K)$. The other inclusion is clear. This completes the proof.

(c) Let $V_1, V_2 \subset \mathbb{P}^n$ be two projective varieties over K and $\phi : V_1 \longrightarrow V_2$ be a rational map. Then there are functions $f_0, f_1, \ldots, f_n \in \overline{K}(V_1)$ such that f_j are defined for all points $P \in V_1$. If $\phi^\sigma = \phi$ for all $\sigma \in G_K$, then we get that for any P in V_1, we get that

$$[f_0^\sigma(P) : f_1^\sigma(P) : \cdots : f_n^\sigma(P)] = [f_0(P) : f_1(P) : \cdots : f_n(P)]$$

By part (b), there exists $\lambda \in \overline{K}^\times$ such that

$$(\lambda f_j)^\sigma = \lambda f_j \quad \forall \, \sigma \in G_K, 0 \leq j \leq n$$

Hence by part (a) $\lambda f_j \in K(V_1)$. This completes the proof.

References & Further Reading

[1] *The Arithmetic of Elliptic Curves*, Joseph H. Silverman

[2] *Local Fields*, J.-P. Serre

[3] *Galois Cohomology*, J.-P. Serre

[4] *Central Simple Algebras and Galois Cohomology*, Gille & Szamuely

[5] *Modular Forms and Galois Cohomolgy*, Haruzo Hida

[6] *Cohomology of Number Fields*, Jürgen Neukirch

[7] *Galois Cohomology of Elliptic Curves*, Coates & Sujatha

[8] *Galois Cohomology and Class Field Theory*, David Harari

[9] *An Introduction to Galois Cohomology and its Applications*, Grégory Berhuy