Profinite Cohomology and Galois Cohomology

Suo-Jun (Stan) Tan

1 Topological groups

Definition 1.1. A topological group G is a group with a topology such that the multiplication map

$$\begin{aligned} m : G \times G &\to G \\ (g_1, g_2) &\mapsto g_1 g_2 \end{aligned}$$

and the inversion map

$$\begin{aligned} i : G &\to G \\ g &\mapsto g^{-1} \end{aligned}$$

are continuous.

We leave to the reader to verify the basic facts.

Proposition 1.2. *Suppose G is a topological group. Let H be a subgroup of G and N be a normal subgroup of G.*

(a) If H is open, then H is closed.

(b) If H is closed and has finite index in G, then H is open.

(c) Suppose G is compact. Then, H is closed and has finite index if and only if H is open.

(d) The quotient group G/N is Hausdorff if and only if N is closed.

(e) The quotient space G/H is discrete if and only if H is open.

(f) $\overline{H} = \bigcap_{e \in U \text{ open sets}} UH.$

Definition 1.3. (Inverse limit and Direct limit) Let I be directed index set, that is for all $i, j \in I$, there exists $k \in I$ such that $i, j \leq k$.

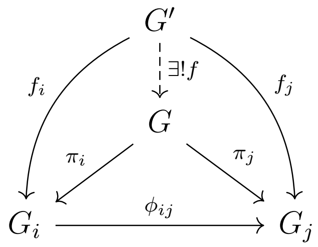
(a) We say (G_i, ϕ_{ij}) is an inverse system of groups over I if for $i \geq j$, we have a group homomorphism

$$\phi_{ij} : G_i \to G_j.$$

An inverse limit

$$G := \lim_{\leftarrow} G_i$$

is a group with a group homomorphism $\pi_i : G \to G_i$ such that for any group G' with group homomorphisms $f_i : G' \to G_i$ and $f_j = \phi_{ij} \circ f_i$, there exists a unique group homomorphism $f : G' \to G$ such that the following diagram is commutative:



.

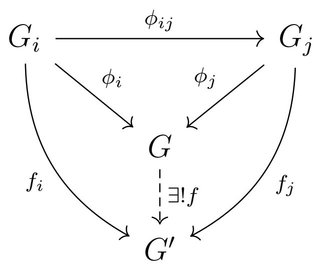
(b) We say (G_i, ϕ_{ij}) is an inverse system of groups over I if for $i \leq j$, we have a group homomorphism

$$\phi_{ij} : G_i \to G_j.$$

A direct limit

$$G := \lim_{\rightarrow} G_i$$

is a group with a group homomorphism $\phi_i : G \to G_i$ such that for any group G' with group homomorphisms $f_i : G_i \to G'$ and $f_j = \phi_{ij} \circ f_i$, there exists a unique group homomorphism $f : G \to G'$ such that the following diagram is commutative:



.

Proposition 1.4. *Suppose (G_i, ϕ_{ij}) is an inverse system of topological groups. Then, the inverse limit $G := \lim_{\leftrightarrow} G_i$ can be identified as a closed subspace of the direct product $\prod G_i$. In fact,*

$$G = \left\{ (g_i) \in \prod G_i : \phi_{ij}(g_i) = g_j \text{ for } i \geq j \right\}.$$

Definition 1.5. (**Profinite group**) A profinite group G is an inverse limit of finite groups with discrete topology.

Theorem 1.6. *A topological group G is profinite if and only if G is compact, Hausdorff and totally disconnected.*

Proposition 1.7. *Suppose G is a profinite group and H be a subgroup. Let $\mathcal{U}$ be the set of all open normal subgroups in G. Then,*

(a) $\bigcap_{N \in \mathcal{U}} N = \{1\}$

(b) $G \cong \varprojlim_{N \in \mathcal{U}} G/N$.

Example 1.8. Suppose L/K is a Galois extension (possibly infinite). Then, the Galois group

$$\mathrm{Gal}(L/K) = \varprojlim_{E/K \text{ finite Galois}} \mathrm{Gal}(E/K)$$

is a profinite group.

Example 1.9. The p-adic integers $\mathbb{Z}_p$ is an inverse limit of $\mathbb{Z}/p^k\mathbb{Z}$,

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^k\mathbb{Z}$$

with natural quotient maps $\mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^{m-1}\mathbb{Z}$.

Example 1.10. The profinite completion of $\mathbb{Z}$ is defined as

$$\widehat{\mathbb{Z}} := \varprojlim \mathbb{Z}/n\mathbb{Z}$$

with the group homomorphisms $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$.

2 Topological G-module

Definition 2.1. Let G be a topological group. A topological G-module A is an abelian topological group such that the G-action on A

$$\begin{aligned} \pi : G \times A &\to A \\ (g, a) &\mapsto g \cdot a \end{aligned}$$

is continuous.

For the remaining of the talk, we assume that A has *discrete topology.* We say that A is a discrete G-module if it is a topological G-module for the discrete topology on A.

Proposition 2.2. *Let G be a compact group and A be a G-module with the discrete topology. Then the following are equivalent:*

(i) A is a discrete G-module

(ii) The stabilizer G_a of $a \in A$ is open in G.

(iii) Let $\mathcal{U}$ be the set of all normal subgroups in G. Then,

$$A = \bigcup_{N \in \mathcal{U}} A^N.$$

Proof. For (i) ⇒ (ii), note that the set

$$\pi^{-1}(a) \cap \big(G \times \{a\}\big) = G_a \times \{a\}$$

is open in $G \times A$. Hence, G_a is open in G.

For (ii) ⇒ (iii), since G is compact and G_a is open, we know that G_a has finite index and hence has only finitely many conjugates, by Orbit-stabilizer theorem. Consider

$$N := \bigcap_{g \in G} g G_a g^{-1}.$$

This is a finite intersection of open subgroups and thus is open in G. Furthermore, we have $a \in A^N$.

For (iii) ⇒ (i), suppose $a \in A^N$ for some open normal subgroup N. Let $b \in A$ be an element in the G-orbit of a. Then, there exists $g \in G$ such that $g \cdot b = a$ and

$$N_g \times \{b\} \subseteq \pi^{-1}(a)$$

is open in $\pi^{-1}(a)$. □

3 Cohomology of a topological group G with coefficients in a discrete G-module

In this section, we assume G is a topological group and A is a discrete G-module. Consider the cochain complex consisting of continuous cochains

$$C^n(G, A) := \{f : G^n \to A | f \text{ is continuous}\}.$$

Remark 3.1. Note that we have the coboundary maps:

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

as usual. Since $d^n(f)$ involves addition in A and the G-action in A, this is well-defined. Furthermore, if $\alpha : A \to B$ is a homomorphism of discrete G-modules, then one easily checks that $\alpha \circ f$ is continuous and the induced map

$$\alpha^n : C^n(G, A) \to C^n(G, B)$$
$$f \mapsto \alpha \circ f$$

commutes with d^n and hence we have maps on cohomology groups

$$\alpha^n : H^n(G, A) \to H^n(G, B).$$

Lemma 3.2. *Let G be a topological group and consider a short exact sequence*

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

of discrete G-modules. Then for every $n \geq 0$, we have the short exact sequence

$$0 \to C^n(G, A) \xrightarrow{\alpha^n} C^n(G, B) \xrightarrow{\beta^n} C^n(G, C) \to 0.$$

Proof. It is easy to see that both α^n and β^n are well-defined. Also, injectivity of α^n follows because α is injective. The exactness also follow easily. It remains to check surjectivity: let $f : G^n \to C$ be a continuous function. For each c, define $U_c = f^{-1}(c)$. Since C is discrete, U_c is open and

$$G^n = \bigcup_{c \in \mathrm{Im}(f)} U_c.$$

Since β is surjective, there exists $b_c \in B$ such that $\beta(b_c) = c$. Now, define

$$h : G^n \to B$$
$$U_c \mapsto b_c.$$

Note that $h^{-1}(b_c) = f^{-1}(c) = U_c$ and hence h is continuous. Also, $\beta^n(f) = h$ and this proves surjectivity of β^n. □

The following corollary then follows easily.

Corollary 3.3. *Every short exact sequence*

$$0 \to A \to B \to C \to 0$$

of discrete G-modules induces a long exact sequence of cohomology groups

$$0 \to H^0(G, A) \xrightarrow{\alpha^0} H^0(G, B) \xrightarrow{\beta^0} H^0(G, C) \xrightarrow{\delta^0} H^1(G, A) \xrightarrow{\alpha^1} \ldots$$

4 Profinite Cohomology

In this section, we further assume that G is profinite. Recall for N normal in G, we have the inflation maps

$$\mathrm{Inf} : H^n(G/N, A^N) \to H^n(G, A)$$

induced by $G \to G/N$ and $A^N \hookrightarrow A$. Furthermore, for $N_3 \subseteq N_2 \subseteq N_1$ normal in G, we have

$$\begin{array}{ccc} H^n(G/N_1, A^{N_1}) & \xrightarrow{\mathrm{Inf}} & H^n(G/N_2, A^{N_2}) \\ & \searrow^{\mathrm{Inf}} & \downarrow{\scriptstyle \mathrm{Inf}} \\ & & H^n(G/N_3, A^{N_3}). \end{array}$$

Now, if we identify

$$G = \varprojlim_{N \text{ open normal}} G/N,$$

then the inflation maps give us a direct system of $H^n(G/N, A^N)$.

Theorem 4.1. *Let G be a profinite group and A be a discrete G-module. Then for $n \geq 0$,*

$$H^n(G, A) \cong \varinjlim_{N \text{ open normal}} H^n(G/N, A^N)$$

where the direct system is given by inflation maps. Furthermore, these isomorphisms are natural in A.

Proof. We show that

$$\varinjlim_{N \text{ open normal}} C^n(G/N, A^N) \xrightarrow{\cong} C^n(G, A)$$

and the maps $C^n(G/N_1, A^{N_1}) \to C^n(G/N_2, A^{N_2})$ are given by composing with the quotient maps $\left(G/N_2\right)^n \to \left(G/N_1\right)^n$.

Each element in $\varinjlim_{N \text{open normal}} C^n(G/N, A^N)$ is represented by a cochain $f \in C^n(G/N, A^N$ for some normal subgroup N. We define

$$\tilde{f} : G^n \to A$$

to be the composite of the quotient map $G^n \to \left(G/N\right)^n$ and f. So this defines a group homomorphism

$$\begin{aligned} \phi : \varinjlim_{N \text{ open normal}} C^n(G/N, A^N) &\to C^n(G, A) \\ f &\mapsto \tilde{f}. \end{aligned}$$

Injectivity of ϕ follows from the definition. Now we show that ϕ is surjective. Suppose $g : G^n \to A$ is a continuous cochain. Since G^n is compact and A is discrete, the image $\mathrm{Im}(g)$ is a finite set. For each $a \in \mathrm{Im}(g)$, $g^{-1}(a)$ is open and hence contains an n-fold product of open subgroups, each of which contains an open normal subgroup. Take the intersection of all these open normal subgroups and denote it as N_a. Then, we obviously have

$$g(N_a) = a$$

for each $a \in \operatorname{Im}(g)$. Define

$$N := \bigcap_{a \in \operatorname{Im}(g)} N_a.$$

Since this is a finite intersection of open normal subgroups, N is open and normal. Furthermore, note that $\operatorname{Im}(g) \subset A^N$ and so $g : G^n \to A$ factors through

$$\begin{array}{ccccc} G^n & \xrightarrow{\quad g \quad} & A^N & \hookrightarrow & A \\ & \searrow & \nearrow_{g'} & & \\ & (G/N)^n & & & \end{array}$$

and hence $\phi(g') = g$.

To finish the proof, it remains to prove the isomorphism ϕ is natural in A. This follows because inflation maps on cochains are natural: let $\alpha : A \to B$ be a homomorphism of discrete G-modules. For $N_2 \subset N_1$ normal in G, we have

$$\begin{array}{ccc} C^n(G/N_1, A^{N_1}) & \xrightarrow{\text{Inf}} & C^n(G/N_2, A^{N_2}) \\ \downarrow{\scriptstyle \alpha^n} & & \downarrow{\scriptstyle \alpha^n} \\ C^n(G/N_1, B^{N_1}) & \xrightarrow{\text{Inf}} & C^n(G/N_2, B^{N_2}) \end{array}.$$

□

Corollary 4.2. *Suppose G is profinite and A is a discrete G-module. Then,*

$$H^0(G, A) = A^G$$

and $H^n(G, A)$ is torsion for all $n > 0$.

Proof. This statement is true for all cohomology groups in the direct system. The corollary follows from the fact that the direct system of torsion groups is again torsion. □

If G is a profinite group (in particular Hausdorff and compact), then a subgroup H is profinite if and only if H is closed. We end the section by including the inflaction-restriction sequence without proof.

Theorem 4.3. ***(Inflation-Restriction)*** *Let H be a closed normal subgroup of a profinite group G and A be a discrete G-module. If $H^i(H, A) = 0$, for all $1 \le i \le n$, then we have the exact sequence*

$$0 \to H^n(G/H, A^H) \xrightarrow{Inf} H^n(G, A) \xrightarrow{Res} H^n(G, A).$$

5 Galois Cohomology

We specialise in the case where $G = \mathrm{Gal}(L/K)$ is the Galois group of a field extension L/K. Recall that the Galois group $\mathrm{Gal}(L/K)$ is a profinite group with basic open sets $\mathrm{Gal}(L/E)$ around 1 for $[E : K] < \infty$. We then have

$$\mathrm{Gal}(L/K) \cong \lim_{E/K \text{ finite Galois}} \mathrm{Gal}(E/K).$$

where each $\mathrm{Gal}(E/K)$ is endowed with the discrete topology. Refer to: `https://docs.wixstatic.com/ugd/67035f_5cf35ba026c84241ad274ef8a648d540.pdf`.

Notice that L and $L^\times$ are discrete G-modules. In fact, for $0 \neq \alpha \in L$, the stabiliser of α in G is

$$G_\alpha = \mathrm{Gal}(L/K(\alpha))$$

which is open in G because $K(\alpha)$ is a finite extension over K.

Theorem 5.1. ***(Hilbert's 90)*** *Suppose L/K is Galois with $G = Gal(L/K)$. Then,*

$$H^1(G, L^\times) = 0.$$

Proof. Since G is a profinite group and $L^\times$ is a discrete G-module, we have

$$H^1(G, L^\times) \cong \varinjlim_{E/K \text{ finite Galois}} H^1(\mathrm{Gal}(E/K), E^\times).$$

Therefore, we may assume L/K is finite. Written multiplicatively, a crossed homomorphism $f : G \to L^\times$ is a map such that

$$f(\sigma\tau) = \sigma(f(\tau)) \cdot f(\sigma)$$

and a principal homomorphism $g : G \to L^\times$ is a map for which there exists $b \in L^\times$ such that

$$g(\sigma) = \frac{\sigma(b)}{b}$$

for all $\sigma, \tau \in G$. Our goal is to show that every crossed homomorphism is principal.

Given a crossed homomorphism f, the independence of characters implies that the sum

$$\sum_{\tau \in G} f(\tau)\tau \neq 0$$

is not identically 0. Therefore, pick $\alpha \in L^\times$ such that

$$\sum_{\tau \in G} f(\tau)\tau(\alpha) = b \in L^\times.$$

Then, for every $\sigma \in G$,

$$\begin{aligned}
\sigma^{-1}(b) &= \sum_{\tau \in G} \sigma^{-1}(f(\tau)) \cdot \sigma^{-1}(\tau(\alpha)) \\
&= \sum_{\gamma \in G} \sigma^{-1}(f(\sigma\gamma)) \cdot \gamma(\alpha) \\
&= \sum_{\gamma \in G} \sigma^{-1}(\sigma(f(\gamma))f(\sigma)) \cdot \gamma(\gamma) \\
&= \sigma^{-1}(f(\sigma))b
\end{aligned}$$

and thus

$$f(\sigma) = \frac{\sigma(b)}{b}$$

as required. $\square$

Corollary 5.2. *Let L/K be a finite cyclic extension with $Gal(L/K) = \langle\sigma\rangle$. Then,*

$$ker(N_{L/K}) = \left\{\alpha \in L^\times : \alpha = \frac{\sigma(\beta)}{\beta} \text{ for some } \beta \in L^\times\right\}.$$

Proof. Recall that the augmentation ideal $\ker(N_{L/K}) = I_G = \langle\sigma - 1\rangle$ as an ideal in $\mathbb{Z}[G]$. Then,

$$0 = H^1(G, L^\times) = H^{-1}(G, L^\times) = \ker(N_{L/K}) \big/ I_G L^\times.$$

$\square$

We also have an additive version of Hilbert's 90:

Theorem 5.3. *Let L/K be a Galois extension with $G = Gal(L/K)$. Then,*

$$H^n(Gal(L/K), L) = 0$$

for all $n \geq 1$.

Proof. Just as before, we may assume L/K is finite. By the normal basis theorem, there exists $\alpha \in L^\times$ such that $\{\sigma(\alpha) : \sigma \in G\}$ is a K-basis for L. Consider the map:

$$\varphi : \mathrm{Ind}^G(K) = \mathbb{Z}[G] \otimes_{\mathbb{Z}} K \to L$$
$$\sum_i \sigma_i \otimes x_i \mapsto \sum_i \sigma_i(\alpha) x_i.$$

One easily sees that this is G-module homomorphism. It is surjective by the choice of α and it is injective by the independence of characters. This shows that L is an induced G-module and thus

$$H^n(G, L) = 0$$

for all $n \geq 1$. $\square$

As a conseuquence of Hilbert's 90, we have the inflation-restriction sequence for Galois extension.

Corollary 5.4. *Suppose $K \subset L \subset M$ is a tower of Galois extensions. Then, the sequence*

$$0 \to H^2(Gal(L/K), L^\times) \xrightarrow{Inf} H^2(Gal(M/K), M^\times) \xrightarrow{Res} H^2(Gal(M/L), M^\times)$$

is exact.

In particular, if $M = K^{sep}$ is a separable closure of K with $G_K = \mathrm{Gal}(K^{sep}/K)$, then we have the following:

Corollary 5.5. *Suppose L/K is Galois. Then, the sequence*

$$0 \to H^2(Gal(L/K), L^\times) \xrightarrow{Inf} H^2(G_K, (K^{sep})^\times) \xrightarrow{Res} H^2(G_L, (K^{sep})^\times)$$

is exact.

Example 5.6. For $K = \mathbb{F}_q$ a finite field where q is a p-power, we show that

$$H^2(G_K, (K^{sep})^\times) = 0.$$

In fact, for each $n \geq 1$, the field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is cyclic of order n and

$$H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) = \widehat{H}^0(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) = \mathbb{F}_q^\times/N(\mathbb{F}_{q^n}^\times).$$

We show that the norm map is surjective. Let ζ be a primitive $(q^n - 1)$-st root of unity. Then,

$$N(\zeta) = \zeta^{\frac{q^n-1}{q-1}}$$

which is a primitive $(q-1)$-st root of unity. This immediately shows that $H^2(\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q), \mathbb{F}_{q^n}^\times) = 0$ and hence

$$H^2(G_K, (K^{sep})^\times) = 0.$$

References

[1] Romyar Sharifi, *Group and Galois Cohomology.* `http://math.ucla.edu/~sharifi/lecnotes.html`.