Group (and Galois) Cohomology

Let G be a finite group, and let M be an abelian group on which G acts.

Goal: $H^0(G, M)$ and $H^1(G, M)$

$M \circlearrowleft G$, makes M into a G-module, $\sigma \in G$ we write $\sigma \cdot m = \sigma(m) = m^\sigma$

NOTE: G is a profinite group w/ a prof. topology and we require the action of G on M to be continuous w.r.t the prof. top. on G and the discrete top. on M.

examples $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts on $\mathbb{C}$, $\mathbb{C}^\times$

$\{1, c\}$ acts (trivially) on $\mathbb{R}$, $\mathbb{R}^\times$

ex L/k finite Galois ext'n of (number) fields

then $G = \mathrm{Gal}(L/k)$ acts on L, $L^\times$, $\mathcal{O}_L$, $\mathcal{O}_L^\times$

ex $\overline{K}/K$, μ_m m-th roots of unity $\subset \overline{k}^\times$, then $\mathrm{Gal}(\overline{k}/k)$ acts on μ_m.

(note: $\overline{\mathbb{R}} = \mathbb{C}$, $\mathrm{Gal}(\overline{\mathbb{R}}/\mathbb{R}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$.)

ex $\overline{K}/K$, E/K ell. curve, $E[n] = \{P \in E(\overline{k}) : [n]P = \mathcal{O}\}$ $\circlearrowleft \mathrm{Gal}(\overline{k}/k)$

$\mathrm{Gal}(\overline{k}/k)$ acts on $T_\mu(k) = \varprojlim \mu_n$ (Tate module)

on $T(E) = \varprojlim E[n]$

on $T_p(E) = \varprojlim E[p^n]$

M is a G-module :

- $e \in G$ ident. , $e \cdot m = e(m) = m$.
- $\sigma \in G$, $\sigma \cdot (m+m') = \sigma \cdot m + \sigma \cdot m'$
- $(\sigma\tau) \cdot m = \sigma(\tau(m))$ NOTE! LEFT-MODULES!

$\sigma, \tau \in G$

A G-module hom. b/w G-modules M, N is $\phi : M \longrightarrow N$ is a hom.

s.t. $\sigma \cdot (\phi(m)) = \phi(\sigma \cdot m)$

for all $m \in M$, $\sigma \in G$.

Of interest:

M^G = largest submodule of M where G acts trivially.

$= \{ m \in M : \sigma \cdot m = m \quad \forall \sigma \in G \}$

ex $E/\mathbb{Q}$, $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $E[n]^G = E(\mathbb{Q})[n]$.

$E[n]$ = $E(\overline{\mathbb{Q}})[n]$

ex $G = \mathrm{Gal}(L/K)$, $L^G = K$, $\mu_n(L)^G = \mu_n(K)$.

$$\mathcal{O}_L^G = \mathcal{O}_K$$

Now let P, M, N be G-modules and let

$$0 \longrightarrow P \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

be an exact seq. of G-modules : $\begin{cases} \cdot \alpha, \beta \text{ are } G\text{-mod. hom.} \\ \cdot \alpha \text{ is injective , } \beta \text{ is surjective.} \\ \cdot \operatorname{Im}\alpha = \operatorname{Ker}\beta . \end{cases}$

and apply G-invariance:

$$0 \longrightarrow P^G \xrightarrow{\alpha'} M^G \xrightarrow{\beta'} N^G \quad \text{where } \alpha' = \alpha|_{P^G} , \ \beta' = \beta|_{M^G}$$

Q: Is this still exact?

- α' injective? α is injective, and $\alpha' = \alpha|_{P^G}$ is also injective.
- $\operatorname{Im}\alpha' = \operatorname{Ker}\beta'$?

$$0 \longrightarrow P^G \xrightarrow{\alpha'} M^G \xrightarrow{\beta'} N^G$$

- $\operatorname{Im}\alpha' = \ker\beta'$?

Note: $\ker(\beta') = \ker(\beta|_{M^G}) = \ker\beta \cap M^G$

- $\operatorname{Im}(\alpha') = \operatorname{Im}(\alpha) \cap M^G$?

$\operatorname{Im}(\alpha') \subseteq \operatorname{Im}(\alpha) \cap M^G$ ✓

$\exists\ m \in \operatorname{Im}(\alpha) \cap M^G \Rightarrow \exists\ p \in P$ s.t. $\alpha(p) = m$.

Now let $\sigma \in G$, $\sigma(\alpha(p)) = \sigma(m) = m$ ($m \in M^G$)

$\sigma(\alpha(p)) = \alpha(\sigma(p)) = m$

$\alpha(p) = m$

$+\ \alpha$ inj $\Rightarrow p = \sigma(p)$

$\Rightarrow p \in P^G$.

$\Rightarrow m \in \operatorname{Im}(\alpha')$

$\operatorname{Im}(\alpha) = \ker(\beta) \Rightarrow \operatorname{Im}(\alpha) \cap M^G = \ker(\beta) \cap M^G$ ✓

$\operatorname{Im}(\alpha') \qquad\qquad \ker(\beta')$

WARNING! $0 \to P^G \to M^G \xrightarrow{\beta'} N^G$ is

NOT necessarily exact on the right!

β' is NOT nec. surjective!

ex

$$1 \to \{\pm 1\} \to \mathbb{C}^\times \xrightarrow{z \mapsto z^2} \mathbb{C}^\times \to 1 \quad \text{e.s.}$$

exact seq. of G-modules.

take G-invariants:

$$1 \to \{\pm 1\} \to \mathbb{R}^\times \xrightarrow{x \mapsto x^2} \mathbb{R}^\times \to ? \to \dots$$

not surjective!

GOAL: Fix short G-sequences !!

Def. Let M be a G-module.

- $H^0(G,M) = M^G = \{ m \in M : \sigma \cdot m = m \quad \forall \sigma \in G \}$
- Group of 1-cochains: $C^1(G,M) = \{ \text{maps } \phi : G \to M \}$ — if G is profinite, req. maps to be continuous!
- Group of 1-cocycles: $Z^1(G,M) = \{ \phi \in C^1(G,M) : \phi(\sigma\tau) = \phi(\sigma) + \sigma \cdot \phi(\tau) \quad \forall \sigma, \tau \in G \}$ "twisted" homomorphisms
- Group of 1-coboundaries: $B^1(G,M) = \{ \phi \in C^1(G,M) : \text{there is a fixed } m \in M \text{ s.t. } \phi(\sigma) = \sigma \cdot m - m \quad \forall \sigma \in G \}$

Lemma $B^1(G,M) \subseteq Z^1(G,M)$

Pf. Let $m \in M$, $\phi : G \to M$, $\phi(\sigma) = \sigma \cdot m - m$.

Then if $\sigma, \tau \in G$, $\phi(\sigma\tau) = (\sigma\tau) \cdot m - m = (\sigma\tau)m - \sigma m + \sigma m - m$

$= \sigma(\tau \cdot m - m) + \sigma \cdot m - m$

$= \phi(\sigma) + \sigma \cdot (\phi(\tau))$ ∎

Def $H^0(G,M) = M^G$ (0-th cohomology gp)

$H^1(G,M) = Z^1(G,M)/B^1(G,M)$. (1-st cohom. gp)

Remarks

- If G acts trivially on M:
  - $M^G = M$, $H^0(G,M) = M$
  - $B^1(G,M) = 0$ b/c $\sigma \cdot m = m$ $\forall m \in M$, $\forall \sigma \in G$
  - $\phi(\sigma\tau) = \phi(\sigma) + \sigma\phi(\tau) = \phi(\sigma) + \phi(\tau)$ is a hom.
    $\Rightarrow Z^1(G,M) = \mathrm{Hom}(G,M)$
  - $H^1(G,M) = Z^1/B^1 \cong \mathrm{Hom}(G,M)$.

Example $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$

- $H^0(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{R}^\times) = (\mathbb{R}^\times)^G = \mathbb{R}^\times$
- $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{R}^\times) = \mathrm{Hom}(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{R}^\times)$

  φ — $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts trivially on $\mathbb{R}^\times$

  $\phi: G \to \mathbb{R}^\times$ hom., $\phi(\sigma) \in \mathbb{R}^\times$ of order 2 $\Rightarrow \phi(\sigma) = \pm 1$.

  $\mathrm{Hom}(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{R}^\times) = \mathrm{Hom}(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \{\pm 1\}) \cong \mathbb{Z}/2\mathbb{Z}$

  $(c \longmapsto \pm 1)$

$\Rightarrow H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mu_2) = H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{R}^\times) \cong \mathbb{Z}/2\mathbb{Z}$.

example

- $H^0(Gal(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) = (\mathbb{C}^\times)^G = \mathbb{R}^\times$

- $H^1(Gal(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times)$

  - $B^1(G, \mathbb{C}^\times)$ $\quad \phi : G \to \mathbb{C}^\times$, $\alpha \in \mathbb{C}^\times$, $\phi(\sigma) = \dfrac{\sigma(\alpha)}{\alpha}$

$$\phi(c) = \frac{c(\alpha)}{\alpha} = \frac{\overline{\alpha}}{\alpha} = \begin{cases} 1 & \text{if } \alpha \in \mathbb{R}^\times \\ \frac{a-bi}{a+bi} & \text{if } \alpha = a+bi \notin \mathbb{R}^\times \end{cases}$$

  - $Z^1(G, \mathbb{C}^\times)$ $\quad \phi : G \to \mathbb{C}^\times$ s.t. $\phi(\sigma\tau) = \phi(\sigma) \cdot \sigma(\phi(\tau))$

Let $\phi(c) = \beta$ then $\begin{cases} \phi(c^2) = \phi(c) \cdot c(\phi(c)) = \beta \cdot \overline{\beta} = N(\beta) = a^2+b^2 \text{ if } \beta = a+bi. \\ \phi''(1) \end{cases}$

$$\phi(1) = \phi(1 \cdot 1) = \phi(1) \cdot 1 \cdot (\phi(1)) = \phi(1)^2$$

$$\Rightarrow \phi(1) = 1 = N(\beta)$$

$\phi(c) = \beta$ w $N(\beta) = 1$

$\phi(1) = 1$

$Z^1(G, \mathbb{C}^\times) = B^1(G, \mathbb{C}^\times)$

Suppose $\beta \in \mathbb{C}^\times$ w/ $N(\beta) = 1$, then $\beta = e^{\gamma \pi i}$ (want $\beta = \frac{\alpha}{\overline{\alpha}}$)

$\because \overline{\sigma(\alpha)} = \alpha$

and if $\alpha = e^{\theta \pi i}$, then $\overline{\alpha} = e^{-\theta \pi i} \Rightarrow \frac{\alpha}{\overline{\alpha}} = e^{-2\theta \pi i}$

Thus $\alpha = e^{-\frac{\gamma}{2} \pi i}$ satisfies $\frac{\alpha}{\overline{\alpha}} = \beta$

Thus $\phi : G \to \mathbb{C}^\times$, $\phi(c) = \beta$, $N(\beta) = 1$ $\longrightarrow$ $\phi(c) = \frac{c(\alpha)}{\alpha}$ a coboundary!

$\phi(1) = 1$

$Z^1 \subseteq B^1$, we know $B^1 \subseteq Z^1$ $\rightarrow$ $Z^1 = B^1$ $\Rightarrow$ $H^1(G, \mathbb{C}^\times) = 0$.

$\|$

$\mathrm{Gal}(\mathbb{C}/\mathbb{R})$

Thm (Hilbert's Theorem 90)

Let K be a field. Then:

(a) $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^+) = 0$.

(b) $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^\times) = 0$. (Thm. 90)

(c) $H^1(\mathrm{Gal}(\overline{K}/K), \mu_m) \cong K^\times/(K^\times)^m$ (if $\mathrm{char}\, K = 0$ or $\mathrm{char}\, K \nmid m$).

Thm Let $0 \longrightarrow P \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$ be an exact sequence of G-modules. Then there is an exact seq.

$$0 \longrightarrow \underbrace{H^0(G,P)}_{=P^G} \longrightarrow \underbrace{H^0(G,M)}_{=M^G} \longrightarrow \underbrace{H^0(G,N)}_{=N^G} \xrightarrow{\delta} H^1(G,P) \longrightarrow H^1(G,M) \longrightarrow H^1(G,N)$$

where $\delta : H^0(G,N) \longrightarrow H^1(G,P)$ is defined as follows:

δ {
- Let $n \in H^0(G,N) = N^G$ and let $m \in M$ s.t. $\beta(m) = n$ (β is surj.)
- and define $\phi : G \longrightarrow P$ by $\phi(\sigma) = \sigma \cdot m - m$
- Then $\phi \in Z^1(G,P)$ and $\delta(n) := [\phi] \in H^1(G,P)$.

Remarks

$$0 \longrightarrow P \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

- In def. of δ, $\underset{\shortparallel}{\operatorname{Im}(\alpha)} \subseteq M$, $P \cong \ker(\beta)$.
  P
- δ is well defined $\phi : G \to P$, $\phi(\sigma) = \sigma m - m$ where $\beta(m) = n$, $n \in N^G$
  $\in P$?

$$\beta(\sigma \cdot m - m) = \beta(\sigma m) - \beta(m) = \sigma(\beta(m)) - \beta(m) = \sigma(n) - n = 0$$

$\Rightarrow \phi(\sigma) \in \ker\beta \cong P \subseteq M$.

- ϕ is NOT a nec. a coboundary b/c $m \in M$ but not nec in P!
- ϕ is a 1-cocycle as in the proof of $B' \subseteq Z'$
- Proof of Thm is "diagram chasing", skip.

Application: $H^1(\mathrm{Gal}(\bar{k}/k), \mu_m) \cong k^\times/(k^\times)^m$ $\left(\begin{array}{l}\text{if } \mathrm{char}\, k = 0 \\ \mathrm{char}\, k \nmid m.\end{array}\right)$

Pf. $1 \to \mu_m \to \bar{k}^\times \xrightarrow{z \mapsto z^m} \bar{k}^\times \to 1$

short exact seq. of $\mathrm{Gal}(\bar{k}/k)$-modules. Take cohomology:

$$1 \to k^\times \cap \mu_m \to k^\times \xrightarrow{x \mapsto x^m} k^\times \to H^1(G_{\bar{k}/k}, \mu_m) \to H^1(G_{\bar{k}/k}, \bar{k}^\times) \to \cdots$$

Image = ker

$H^1(G_{\bar{k}/k}, \bar{k}^\times) = 0$ (Thm 90)

$$1 \to k^\times/(k^\times)^m \to H^1(G_{\bar{k}/k}, \mu_m) \to 0$$

$\Rightarrow$ $\cong$ ▨

ex $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), \mu_2) \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{R}^\times/(\mathbb{R}^\times)^2$

example Let us "fix"

$$1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{R}^\times \xrightarrow{x \mapsto x^2} \mathbb{R}^\times \longrightarrow ??$$

Start: $1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{C}^\times \xrightarrow{z \mapsto z^2} \mathbb{C}^\times \longrightarrow 1$ exact, $G = Gal(\mathbb{C}/\mathbb{R})$

Coho: $1 \longrightarrow H^0(G, \{\pm 1\}) \longrightarrow H^0(G, \mathbb{C}^\times) \longrightarrow H^0(G, \mathbb{C}^\times) \xrightarrow{=} \mathbb{R}^\times$

($H^0(G, \{\pm 1\}) = \{\pm 1\}$, $H^0(G, \mathbb{C}^\times) = \mathbb{R}^\times$)

$$\xrightarrow{\delta} H^1(G, \{\pm 1\}) \longrightarrow H^1(G, \mathbb{C}^\times) \longrightarrow H^1(G, \mathbb{C}^\times)$$

($H^1(G, \{\pm 1\}) \xrightarrow{\sim} \mathbb{R}^\times/(\mathbb{R}^\times)^2$, $H^1(G, \mathbb{C}^\times) = 0$, $H^1(G, \mathbb{C}^\times) = 0$)

Get: $1 \longrightarrow \{\pm 1\} \longrightarrow \mathbb{R}^\times \xrightarrow{x \mapsto x^2} \mathbb{R}^\times \longrightarrow \mathbb{R}^\times/(\mathbb{R}^\times)^2 \longrightarrow 1$

ex E/k an ell. curve, w/ $E[m] \subseteq E(k)$.

Exact: $0 \to E[m] \longrightarrow E \xrightarrow{[m]} E \longrightarrow 0$ $\quad E = E(\bar{k})$

Tate cohom: $G = Gal(\bar{k}/k)$

$$0 \to E[m] \longrightarrow E(k) \longrightarrow E(k)$$

$$\xrightarrow{\delta} H^1(G_{\bar{k}/k}, E[m]) \longrightarrow H^1(G_{\bar{k}/k}, E) \longrightarrow H^1(G_{\bar{k}/k}, E)$$

$$\| \text{ll}$$

$$\mathrm{Hom}_{\mathrm{cont}}(G_{\bar{k}/k}, E[m])$$

What is δ? Let $P \in E^G = E(k)$, $Q \in E(\bar{k})$ s.t. $[m]Q = P$

Then $\delta(P) : G_{\bar{k}/k} \longrightarrow E[m]$

$$\sigma \longmapsto \sigma(Q) - Q$$

so... $\delta(P) = k(P, \cdot)$

the Kummer pairing!

Restriction - Inflation

Let $H \subseteq G$ be a subgp. Then, $H^1(G,M) \xrightarrow{\text{Res}} H^1(H,M)$ (Restriction)

$$[\phi] \longmapsto [\phi|_H]$$

If $H \triangleleft G$ is normal, then M^H is a G/H-module

$\sigma H \cdot m = \sigma(m)$ b/c $(\sigma h)m = \sigma(h \cdot m) = \sigma m$ $\quad m \in M^H$, $h \in H$.

If $[\phi] \in H^1(G/H, M^H)$ via

$$G \longrightarrow G/H \xrightarrow{\phi} M^H \subseteq M$$

$\Rightarrow [\phi] \in H^1(G,M)$ get (Inflation)

$$H^1(G/H, M^H) \xrightarrow{\text{Inf}} H^1(G,M)$$

Thm There is an exact sequence:

$$0 \longrightarrow H^1(G/H, M^H) \xrightarrow{\inf} H^1(G, M) \xrightarrow{\text{res}} H^1(H, M)$$

ex $G = \mathrm{Gal}(\overline{k}/k)$, L/k is finite

then $H = \mathrm{Gal}(\overline{k}/L) \subseteq G$ is a subgp.

and if L/k is Galois then $H \lhd G$ and

$$G/H = G_{\overline{k}/k} \Big/ \mathrm{Gal}(\overline{k}/L) \cong \mathrm{Gal}(L/k)$$

Thus there is an exact sequence:

$$0 \to H^1(\mathrm{Gal}(L/k), M^{G_{\overline{k}/L}}) \xrightarrow{\inf} H^1(\mathrm{Gal}(\overline{k}/k), M) \xrightarrow{\text{res}} H^1(\mathrm{Gal}(\overline{k}/L), M)$$