A very short Introduction to Galois Cohomology

Adrian Baumann

Heinrich-Heine-Universität Düsseldorf

GRK2240 Retreat 2024

Group Cohomology

Let G be a group and M be a G-module (i.e. M is an abelian group on which G acts associatively). Then we can define the so-called *cohomology groups* of G with coefficients in M, $\mathrm{H}^i(G, M)$:

Definition (i-th Cohomology Group)

Let the maps $\mathrm{C}^i(G, M) := \{f \colon G^i \to M\}$ denote the G-module of *inhomogenous i-cochains*. We obtain *coboundary homomorphisms* $d^{i+1} \colon \mathrm{C}^i(G, M) \to \mathrm{C}^{i+1}(G, M)$ by

$$d^{i+1}(f)(g_1, \dots, g_{i+1}) = g_1.f(g_2, \dots, g_i) + \sum_{k=1}^{i} (-1)^k f(g_1, \dots, g_k g_{k+1}, \dots, g_{i+1}) + (-1)^{i+1} f(g_1, \dots, g_i)$$

with the property $d^{i+1} \circ d^i = 0$. Let $\mathrm{Z}^i(G, M) := \ker(d^{i+1})$ and $\mathrm{B}^i(G, M) := \mathrm{im}(d^i)$ (with $\mathrm{B}^0 := 0$). Then we define the i-th cohomology group as

$$\mathrm{H}^i(G, M) := \mathrm{Z}^i(G, M)/\mathrm{B}^i(G, M).$$

Group Cohomology

Those cohomology groups are functors on the category of G-modules (which are also functorial in G) with the following useful properties:

- $\mathrm{H}^0(G, M) = M^G = \{m \in M \mid \forall g \in G : g.m = m\}$.
- $$\mathrm{H}^1(G, M) = \frac{\{f : G \to M \mid f(g_1 g_2) = f(g_1) + g_1.f(g_2)\}}{\{f : G \to M \mid \exists m \in M : f(g) = g.m - m\}}.$$
  In particular, if G acts trivially on M, we have $\mathrm{H}^1(G, M) = \mathrm{Hom}(G, M)$.
- $\mathrm{H}^2(G, M)$ classifies the *Group Extensions* of the form
  $$0 \to M \to E \to G \to 0.$$
- A short exact sequence of G-modules
  $$0 \to L \to M \to N \to 0$$
  becomes a long exact sequence
  $$\begin{aligned} 0 &\to \mathrm{H}^0(G, L) \to \mathrm{H}^0(G, M) \to \mathrm{H}^0(G, N) \\ &\to \mathrm{H}^1(G, L) \to \mathrm{H}^1(G, M) \to \mathrm{H}^1(G, N) \to \dots \end{aligned}$$

Application to Galois Groups

Now let F be a field and denote by F_s its separable closure.
Then we denote its *absolute Galois group* by

$$G_F = \mathrm{Gal}(F_s/F) = \mathrm{Aut}_F(F_s).$$

Let further be $\mu_m \subseteq F_s^\times$ the group of m-th roots of unity (e.g. $\{+1, -1\} = \mu_2$). The operation of a $\sigma \in G_F$ on μ_m results in a permutation given by mapping one primitive m-th root to another.
To make things easier, we will assume that the characteristic of F does not divide m.

Remark

For the rest of the talk, we will actually consider *continuous* cohomology groups, meaning that we take $C^i(G, M)$ to be the G-module made up of only the continuous maps from G^i to M.

Application to Galois Groups

If we now take the short exact sequence of G_F-modules

$$1 \to \mu_m \to F_s^\times \xrightarrow{x \mapsto x^m} F_s^\times \to 1,$$

we obtain as part of the long exact sequence

$$\begin{array}{ccccccc} \mathrm{H}^0(G_F, F_s^\times) & \xrightarrow{(\ )^m} & \mathrm{H}^0(G_F, F_s^\times) & \xrightarrow{\delta} & \mathrm{H}^1(G_F, \mu_m) & \longrightarrow & \mathrm{H}^1(G_F, F_s^\times). \\ \| & & \| & & & & \| \\ F^\times & & F^\times & & & & 0 \end{array}$$

Kummer Theory

Thus we obtain that $F^\times$ maps surjectively onto $\mathrm{H}^1(G_F, \mu_m)$ and its kernel are the elements that are m-th powers in $F^\times$.
In other words, we get an isomorphism

$$F^\times/(F^\times)^m \xrightarrow{\sim} \mathrm{H}^1(G_F, \mu_m)$$

which is induced by the *connecting homomorphism* δ.
If we furthermore have the scenario that $\mu_m \subseteq F^\times$, we know that G_F acts trivially on μ_m. As a result, $\mathrm{H}^1(G_F, \mu_m) \simeq \mathrm{Hom}(G_F, \mu_m)$ and we can explicitly compute δ by the following means:
For $a \in F^\times$, let $\alpha \in F_s$ such that $\alpha^m = a$ and $\sigma \in G_F$. Then

$$\delta(a) = \left(\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}\right).$$

The Cup Product

Definition (Cup Product)

$$\cup\colon \mathrm{H}^i(G,M)\otimes_{\mathbb{Z}}\mathrm{H}^j(G,N)\to \mathrm{H}^{i+j}(G,M\otimes_{\mathbb{Z}}N)$$
$$[f_1]\otimes[f_2]\mapsto \big[(g_1,\dots,g_{i+j})\mapsto(-1)^{ij}f_1(g_1,\dots,g_i)\otimes g_1\dots g_i.f_2(g_{i+1},\dots,g_{i+j})\big]\,,$$

where $M\otimes_{\mathbb{Z}}N$ is equipped with the componentwise operation of G.

This has some useful properties, in particular that it is associative and distributive and furthermore graded-commutative in the following way:
If $\alpha\colon M\otimes N\to N\otimes M$ is given by $m\otimes n\mapsto n\otimes m$, then we have for $\varphi_1\in\mathrm{H}^i(G,M),\varphi_2\in\mathrm{H}^j(G,N)$:

$$\varphi_1\cup\varphi_2=(-1)^{ij}\alpha_*(\varphi_1\cup\varphi_2)$$

The Galois Symbol

Since μ_m is a $\mathbb{Z}$-module (by being an abelian group), we can consider

$$\mu_m^{\otimes n} = \mu_m \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mu_m$$

and by this get

$$\begin{array}{ccc} \mathrm{H}^1(G_F, \mu_m) \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} & \mathrm{H}^1(G_F, \mu_m) & \longrightarrow \mathrm{H}^n(G_F, \mu_m^{\otimes n}). \\ \| & \| & \\ F^\times/(F^\times)^m & F^\times/(F^\times)^m & \end{array}$$

The Galois Symbol

Induced by this, we obtain

$$\delta^n : F^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} F^\times \to \mathrm{H}^n(G_F, \mu_m^{\otimes n}).$$

For this δ^n, we have the following result:

Proposition (Tate)

Let $a_1, \ldots, a_n \in F^\times$ such that $a_i + a_j = 1$ for some $1 \leq i < j \leq n$. Then

$$\delta^n(a_1 \otimes \cdots \otimes a_n) = 0.$$

We will now sketch the proof.

The Galois Symbol

Lemma (1)

Let L/F be a finite separable field extension. Then we have the commuting diagrams

$$
\begin{array}{ccc}
F^\times & \xrightarrow{\delta_F} & H^1(G_F, \mu_m) \\
\big\downarrow & & \big\downarrow {\scriptstyle Res_L^F} \\
L^\times & \xrightarrow{\delta_L} & H^1(G_L, \mu_m)
\end{array}
\quad \text{and} \quad
\begin{array}{ccc}
L^\times & \xrightarrow{\delta_L} & H^1(G_L, \mu_m) \\
{\scriptstyle N_{L/K}} \big\downarrow & & \big\downarrow {\scriptstyle Cor_F^L} \\
F^\times & \xrightarrow{\delta_F} & H^1(G_F, \mu_m)
\end{array}
$$

Lemma (2)

For $f_1 \in H^1(G_F, \mu_m)$, $f_2 \in H^1(G_L, \mu_m)$:

$$f_1 \cup Cor_F^L(f_2) = Cor_F^L(Res_L^F(f_1) \cup f_2)$$

Proof of the proposition

Let $a_1, \ldots, a_n \in F^\times$ such that $a_i + a_j = 1$ for some $i \neq j$.

- Reduce to $n = 2$ and consider $a \otimes (1 - a)$.
- Take an irreducible factorisation $X^m - a = \prod f_l(X)$ with $f_l \in F[X]$.
- Let $\alpha_l \in F_s$ be roots of the f_l and $F_l := F(\alpha_l)$. We obtain

$$1 - a = \prod_l f_l(1) = \prod_l \mathrm{N}_{F_l/F}(1 - \alpha_l).$$

- Since δ^2 is a group homomorphism, we obtain

$$\delta^2(a \otimes (1 - a)) = \sum_l \delta^2(a \otimes \mathrm{N}_{F_l/F}(1 - \alpha_l)).$$

Proof of the proposition

As a result, we get:

$$
\begin{aligned}
\delta^2(a \otimes \mathrm{N}_{F_l/F}(1-\alpha_l)) &= \delta_F(a) \cup \delta_F(\mathrm{N}_{F_l/F}(1-\alpha_l)) && \text{by definition of } \delta^n \\
&= \delta_F(a) \cup \mathrm{Cor}_F^{F_l}(\delta_{F_l}(1-\alpha_l)) && \text{by Lemma (1)} \\
&= \mathrm{Cor}_F^{F_l}(\mathrm{Res}_{F_l}^{F}(\delta_F(a)) \cup \delta_{F_l}(1-\alpha_l)) && \text{by Lemma (2)} \\
&= \mathrm{Cor}_F^{F_l}(\delta_{F_l}(a) \cup \delta_{F_l}(1-\alpha_l)) && \text{by Lemma (1)} \\
&= \mathrm{Cor}_F^{F_l}(0 \cup \delta_{F_l}(1-\alpha_l)) && \text{since } a = \alpha_l^m \text{ in } F_l \\
&= 0 && \text{by distributivity of } \cup
\end{aligned}
$$

This proves the proposition.

The Galois Symbol

The previous proposition motivates the following definition:

Definition

We define the *n-th Milnor K-group* as

$$K_n^M(F) = (F^\times)^{\otimes n} / \langle [a_1, \dots, a_n] \mid a_i + a_j = 1 \text{ for some } i \neq j \rangle.$$

By convention, we set

$$K_0^M(F) = \mathbb{Z} \text{ and } K_1^M(F) = F^\times.$$

Due to the proposition, δ^n factors through $K_n^M(F)$ by

Definition

$$h_{F,m}^n : K_n^M(F) \to \mathrm{H}^n(G_F, \mu_m^{\otimes n}),$$

which we call the *Galois-Symbol*.

The Galois Symbol

Question

What statements can we make about the Galois-Symbol?