GALOIS COHOMOLOGY
GEUNHO GIM

Abstract. This note is based on the 3-hour presentation given in the student seminar on Fall 2013. We will basically follow [HidMFG, Chapter IV] and [MilADT, Chapter I §0, 1, 2].

Contents

1. Group Cohomology 1
2. The main duality theorem 4
3. Local/global case 8
  3.1. Local case 8
  3.2. Global case 10
4. Euler characteristic formula 10
References 11

1. Group Cohomology

Let $G$ be a group and $M$ be a $G$-module (i.e., an abelian group which $G$ acts on). For $G$-modules $M$ and $N$, a $G$-module homomorphism $\alpha : M \to N$ is a group homomorphism satisfying $g \cdot \alpha(m) = \alpha(g \cdot m)$ for $g \in G, m \in M$. If we define the action of $G$ on $\text{Hom}_\mathbb{Z}(M, N)$ by $(g \cdot \phi)(m) = \phi(g^{-1}m)$, then we have $\text{Hom}_G(M, N) = \text{Hom}_\mathbb{Z}(M, N)^G$. We define $G$-Mod to be the category of $G$-modules with $G$-homomorphisms. Note that $G$-Mod is equivalent to the category of modules over the ring $\mathbb{Z}[G]$, $G$-Mod $\cong \mathbb{Z}[G]$-Mod. There are several equivalent ways to construct the cohomology groups.

Construction 1: Extension groups

Note that $G$-Mod has enough injectives. For a $G$-module $M$, we have an injective resolution:

$$0 \to M \xrightarrow{\epsilon} M^0 \xrightarrow{\partial^0} M^1 \xrightarrow{\partial^1} \cdots$$

(exact sequence with injective $M^i$'s for all $i$) and we write this $0 \to M \to (M^\bullet, \partial)$ in short. Given $M, M' \in G$-Mod, and injective resolutions $0 \to M \to (M^\bullet, \partial)$ and $0 \to N \to (N^\bullet, \delta)$, we define

$$\text{Ext}^r_G(M, N) = \{\text{homotopy classes of } \deg r \text{ chain maps } (M^\bullet, \partial) \to (N^\bullet, \delta)\}$$

$$= H^r(\text{Hom}_G(M, N^\bullet), \delta^*)$$

Here $\deg r$ maps $f, g : (M^\bullet, \partial) \to (N^\bullet, \delta)$ are homotopic if there is a $\deg(r-1)$ map $\Delta$ satisfying $f - g = \Delta \delta + \delta \Delta$. We define the $r$-th cohomology group by

$$H^r(G, M) = \text{Ext}^r_G(\mathbb{Z}, M)$$

Date: April 18, 2014.
where $G$ acts on $\mathbb{Z}$ trivially.

**Construction 2 : Right derived functor**

For a $G$-module $M$, we define $M^G = \{m \in M \mid gm = m \text{ for all } g \in G\}$. Since

$$(-)^G = \text{Hom}_\mathbb{Z}(\mathbb{Z}, -)^G = \text{Hom}_G(\mathbb{Z}, -),$$

$(-)^G : G\text{-Mod} \to \text{Ab}$ is a left exact functor. We apply this to an injective resolution

$$0 \to M \to (M^0)^G \xrightarrow{d^0} (M^1)^G \xrightarrow{d^1} \cdots$$

and define

$$H^r(G, M) = \frac{\ker d^r}{\text{im } d^{r-1}}$$

as the right derived functor of $(-)^G$.

**Construction 3 : Cochain complex**

This is the most explicit construction because we can actually see what the elements of the cohomology groups are. We first define

$$C^r(G, M) = \{\phi : G^n \to M\}$$

as the set of set-theoretic maps. Also define the boundary maps $\partial^r : C^r \to C^{r+1}$ by

$$(\partial^r \phi)(g_1, \ldots, g_{r+1}) = g_1 \phi(g_2, \ldots, g_{r+1}) + \sum_{j=1}^{r} (-1)^j \phi(g_1, \ldots, g_j g_{j+1}, \ldots, g_{r+1}) + (-1)^{r+1} \phi(g_1, \ldots, g_r)$$

Now we can define

$$H^r(G, M) = \frac{\ker \partial^r}{\text{im } \partial^{r-1}}$$

as the cohomology group. Note that all three constructions are equivalent. (See for example, [HidMFG, 4.3.1].)

**Example 1.1.**

1. $H^0(G, M) = \text{Hom}_G(\mathbb{Z}, M) = M^G$
2. $H^1(G, M) = \{u : G \to M \mid u(gh) = gu(h) + u(g)\}$
3. If $G$ acts on $M$ trivially, then $H^1(G, M) = \text{Hom}_{\text{group}}(G, M)$.

**Definition 1.2.** Let $H \leq G$ be a subgroup and $M \in H\text{-Mod}$. We define the induced module $\text{Ind}_H^G(M) \in G\text{-Mod}$ by

$$\text{Ind}_H^G(M) = \{\phi : G \to M \mid \phi(hg) = h\phi(g) \text{ for all } h \in H\}$$

and the $G$-action is given by $(g\phi)(m) = \phi(mg)$.

**Definition 1.3.** Let $M \in G\text{-Mod}$ and $M' \in G'\text{-Mod}$. Consider $G \xleftarrow{\alpha} G' \xrightarrow{\beta} M$. The maps $\alpha$ and $\beta$ are called compatible if $\beta(\alpha(g')m) = g'()$ for all $g' \in G'$ and $m \in M$. In this case, there is a natural map between cohomology groups:

$$H^r(G, M) \xrightarrow{[\phi : G^n \to M]} H^r(G', M') \xrightarrow{[\beta \circ \phi \circ (\alpha \times \cdots \times \alpha) : G^n \to M']$$
Example 1.4.  (1) Let $H \leq G$ and $M \in G\text{-}Mod$. Note that $M$ is also an $H$-module by restricting the action of $G$ to $H$. The maps $H \hookrightarrow G$ and $M \xrightarrow{id} M$ are compatible. Thus, we get the restriction map

$$\text{res} : H' (G, M) \longrightarrow H' (H, M)$$

The map $M \xrightarrow{m \mapsto (g \mapsto gm)} \text{Ind}_H^G M$ induces the following commutative diagram.

$$\begin{array}{ccc}
H' (G, M) & \xrightarrow{\text{res}} & H' (H, M) \\
\downarrow & & \searrow \\
H' (G, \text{Ind}_H^G M)
\end{array}$$

where the isomorphism on the right is from Shapiro's lemma.

(2) Let $H \trianglelefteq G$ and $M \in G\text{-}Mod$. Note that $M^H \in (G/H)\text{-}Mod$. The maps $G \twoheadrightarrow G/H$ and $M^H \hookrightarrow M$ are compatible, thus inducing the inflation map

$$\text{inf} : H' (G/H, M^H) \longrightarrow H' (G, M)$$

(3) Suppose the index $(G : H)$ is finite and $M \in G\text{-}Mod$. The map

$$\text{Ind}_H^G M \xrightarrow{\phi \mapsto \sum_{s \in G/H} s \phi (s^{-1})} M$$

defines the corestriction map by the commutative diagram

$$\begin{array}{ccc}
H' (H, M) & \xrightarrow{\text{cor}} & H' (G, M) \\
\downarrow & & \searrow \\
H' (G, \text{Ind}_H^G M)
\end{array}$$

where the isomorphism on the right is from Shapiro’s lemma.

Proposition 1.5. Let $H \leq G$ be a subgroup of a finite group $G$ and $M \in G\text{-}Mod$.

(1) The composition $\text{cor}_{G/H} \circ \text{res}_{G/H} : H' (G, M) \rightarrow H' (G, M)$ is multiplication by $(G : H)$.

(2) $|G|$ kills $H' (G, M)$.

(3) Suppose $H \leq G$, $r > 0$, and we have $H^i (H, M) = 0$ for all $0 < i < r$. Then there is the following inflation-restriction exact sequence

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

Proof. (1) The composition of the maps defined earlier $M \rightarrow \text{Ind}_H^G (M) \rightarrow M$ is multiplication by $(G : H)$.

(2) The map $M \xrightarrow{\phi \mapsto \sum_{s \in G/H} s \phi (s^{-1})} M$ defines the corestriction map.

(3) If $r = 1$, it is clear. For $r > 1$, we use induction. See [MilCFT, p. 69].
Definition 1.6. Let $G$ be a finite group and $M \in G$-$\text{Mod}$. We define Tate cohomology groups as follows:

\[
H^r_T(G, M) = \begin{cases} 
H^r(G, M) & r > 0 \\
M^G/N_G M & r = 0 \\
\ker N_G/I_G M & r = -1 \\
H_{-r-1}(G, M) & r < -1
\end{cases}
\]

where $N_G : M \xrightarrow{m \to \sum_{g \in G} gm} M$ and $I_G M = \sum_{g \in G} (g-1)M$. This connects homology and cohomology.

Example 1.7. $H^{-2}(G, \mathbb{Z}) = G^{ab}$.

Theorem 1.8 (Tate). Let $G$ be a finite group and $C \in G$-$\text{Mod}$. Suppose

1. $H^1(H, C) = 0$
2. $H^2(H, C)$ is cyclic of order $|H|$ for all subgroups $H \leq G$. Then we have

\[
H^r_T(G, Z) \xrightarrow{\gamma} H^{r+2}_T(G, C)
\]

where $[\gamma]$ is a generator of $H^2(G, C)$. (Note that the isomorphism depends on the choice of $\gamma$.)

In general, if $M \in G$-$\text{Mod}$ is torsion-free, then we have

\[
H^r_T(G, M) \xrightarrow{\cup \gamma} H^{r+2}_T(G, M \otimes_{\mathbb{Z}} C)
\]

Proof. Use dimension-shifting. See [MilCFT, p. 81].

2. The main duality theorem

Let $G$ be a profinite group and $M$ be a discrete $G$-module (i.e., $M$ has discrete topology and the action $G \times M \to M$ is continuous.) This is equivalent to say that $M = \bigcup_{U \leq G} M^U$. We define the continous cochain complex $C^n_{\text{ct}}(G, M) = \{ \phi : G^n \to M, \text{ continuous} \}$ and by using this, define $H^r_{\text{ct}}(G, M)$. Note that for $\phi \in C^n_{\text{ct}}(G, M)$, we have $G^n = \bigcup_{\text{finite}} \phi^{-1}(m_i)$ by compactness. Thus, $\phi$ is locally constant and factors through

\[
\begin{array}{ccc}
G^n & \xrightarrow{\phi} & M \\
& (G/U)^n & \nearrow \\
& & (G/U)^n
\end{array}
\]

for some open $U \leq G$. Therefore we have

\[
H^r_{\text{ct}}(G, M) \cong \lim_{U \leq G \text{ open}} H^r(G/U, M^U)
\]

where the limit is over $\inf_{U/V} : H^r(G/U, M^U) \to H^r(G/V, M^V)$ for $V \leq U \leq G$ open subgroups. From now on, $G$-$\text{Mod}$ means the category of discrete $G$-modules (which has enough injectives) and $H^\bullet = H^\bullet_{\text{ct}}$. 


**Definition 2.1.** Suppose $C \in G\text{-Mod}$ and we have

$$\text{inv}_U : H^2(U, C) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

for all open subgroups $U \leq G$ (called the invariant map relative to $U$). $(G, C)$ is called a class formation if

1. $H^1(U, C) = 0$ for all open $U \leq G$
2. for all open $V \leq U \leq G$, we have

$$H^2(U, C) \xrightarrow{\text{res}} H^2(V, C)$$

\[\xymatrix{ \mathbb{Q}/\mathbb{Z} \ar[r]^{(U:V)} & \mathbb{Q}/\mathbb{Z} }\]

**Theorem 2.2.** Let $(G, C)$ be a class formation. Then, there is a map

$$\text{rec}_G : C^G \rightarrow G^{ab}$$

called the reciprocity map such that $\text{im}(\text{rec}_G) \subseteq G^{ab}$ is dense and $\ker(\text{rec}_G) = \bigcap_{U \leq G} N_{G/U} C^U$ where

$$N_{G/U} : C^U \xrightarrow{x \mapsto \sum_{g \in G/U} gx} C^G.$$

**Proof.** Let $V \leq U \leq G$. From the inflation-restriction exact sequence

$$0 \rightarrow H^1(U/V, C^V) \xrightarrow{\text{inf}} H^1(U, C) \xrightarrow{\text{res}} H^1(V, C)$$

we have $H^1(U, C) = 0$ and $H^1(V, C) = 0$ by assumption (1), thus $H^1(U/V, C^V) = 0$. From assumption (2),

$$\xymatrix{ 0 \ar[r] & H^2(U/V, C^V) \ar[r]^-{\text{inf}} & H^2(U, C) \ar[r]^-{\text{res}} & H^2(V, C) \ar[d]^-{\text{inv}_U} \ar[r]^-{\text{inv}_V} & \mathbb{Q}/\mathbb{Z} \ar[r]^-{(U:V)} & \mathbb{Q}/\mathbb{Z} \ar[r] & 0 }$$

we get $\text{inv}_{U/V} := H^2(U/V, C^V) \xrightarrow{u_{U/V}} \mathbb{Q}/\mathbb{Z}$ where $H^2(U/V, C^V) = \langle u_{U/V} \rangle$.

Now we apply Tate's theorem to $G/U$ to get

$$H^{-2}_T(G/U, \mathbb{Z}) \xrightarrow{\sim} H^0_T(G/U, C^U)$$

Now we define $\text{rec}_G : C_G \rightarrow G^{ab} = \varprojlim (G/U)^{ab}$ by using these maps. Then we get $\ker(\text{rec}_G) = \bigcap_{U \leq G} N_{G/U} C^U$ and $\text{im}(\text{rec}_G)$ is dense in $G^{ab}$. \[\square\]
Example 2.3 (trivial example). Suppose \( G = \langle \sigma \rangle \cong \hat{\mathbb{Z}} \) and \( G \curvearrowright C = \mathbb{Z} \) trivially. Let \( U \leq G \) be an open subgroup. By using the fact that \( H^r(G, \mathbb{Q}) = \lim_{U \leq G \text{ open}} H^r(G/U, \mathbb{Q}) \) is a torsion group for \( r > 0 \) and \( \mathbb{Q} \xrightarrow{\times n} \mathbb{Q} \), we get \( H^r(G, \mathbb{Q}) \xrightarrow{\times n} H^r(G, \mathbb{Q}) \) and \( H^r(G, \mathbb{Q}) = 0 \) for all \( r > 0 \). By applying \( H^* (U, -) \) to the exact sequence

\[
0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0
\]

we can define

\[
\text{inv}_U : H^2(U, \mathbb{Z}) \xrightarrow{\sim} H^1(U, \mathbb{Q}/\mathbb{Z}) = \text{Hom}_\text{ct}(U, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}
\]

and \( H^1(U, \mathbb{Z}) = \text{Hom}_\text{ct}(U, \mathbb{Z}) = 0 \) since the image of a continuous map from \( U \) is a compact subgroup of \( \mathbb{Z} \). Therefore, \((G, \mathbb{Z})\) is a class formation.

If \((G : U) = m\), then we have

\[
\frac{C^G/N_{G/U}C^U}{\mathbb{Z}/m\mathbb{Z}} \xrightarrow{\sim} (G/U)^{ab}
\]

and \( \text{rec}_G : C^G(= Z^G = \hat{\mathbb{Z}}) \hookrightarrow G^{ab} = \hat{\mathbb{Z}} \).

Definition 2.4. Let \( M \) be an abelian group. We define \( M^* = \text{Hom}_\mathbb{Z}(M, \mathbb{Q}/\mathbb{Z}) \). (If \( M \) is a torsion group, then this is the Pontryagin dual of \( M \).)

Definition 2.5. Let \( M \in G\text{-Mod} \) and \((G, C)\) be a class formation. We have the following Ext pairing:

\[
\text{Ext}_G^r(M, C) \times \text{Ext}_G^{2-r}(\mathbb{Z}, M) \longrightarrow \text{Ext}_G^2(\mathbb{Z}, C)
\]

\[
H^2-r(G, M) \quad H^2(G, C) \xrightarrow{\text{inv}_G} \mathbb{Q}/\mathbb{Z}
\]

where the map is the composition of chain maps. We define

\[
\alpha_r(G, M) : \text{Ext}_G^r(M, C) \to H^{2-r}(G, M)^*
\]

by using the Ext pairing.

Example 2.6. Let \( M = \mathbb{Z} \) and \( G \curvearrowright M \) trivially. Then, we have \( \text{Ext}_G^r(M, C) = H^r(G, C) \).

1. \((r = 0)\) \( \alpha^0(G, Z) : H^0(G, C)(= C^G) \longrightarrow H^2(G, \mathbb{Z})(= \text{Hom}_\text{ct}(G, \mathbb{Q}/\mathbb{Z})^* = G^{ab}) \)

   and we have \( \alpha^0(G, Z) = \text{rec}_G \).

2. \((r = 1)\) \( \alpha^1(G, Z) : H^1(G, C)(= 0) \xrightarrow{\sim} H^1(G, \mathbb{Z})^* = 0 \)

   since \( H^1(G, \mathbb{Z}) = \text{Hom}_\text{ct}(G, \mathbb{Z}) = 0 \).

3. \((r = 2)\) \( \alpha^2(G, Z) : H^2(G, C) \xrightarrow{\sim} H^0(G, \mathbb{Z})^* = \mathbb{Z}^* = \mathbb{Q}/\mathbb{Z} \)

   and we have \( \alpha^2(G, Z) = \text{inv}_G \).

Example 2.7. Let \( M = \mathbb{Z}/m\mathbb{Z} \) and \( G \curvearrowright M \) trivially. By using the exact sequence \( 0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0 \), we get the following:
\[ \begin{align*}
(1) \ (r = 0) \\
\alpha^0(G, \mathbb{Z} / m\mathbb{Z}) & : \text{Ext}_G^0(\mathbb{Z} / m\mathbb{Z}, C) \longrightarrow H^2(G, \mathbb{Z} / m\mathbb{Z})^* \\
\downarrow & \\
C^G[m] & \longrightarrow G^{ab}[m]
\end{align*} \]

and the composition is \( \text{rec}_G : C^G[m] \rightarrow G^{ab}[m] \).

(2) \ (r = 1)
\[ \begin{align*}
\alpha^1(G, \mathbb{Z} / m\mathbb{Z}) & : \text{Ext}_G^1(\mathbb{Z} / m\mathbb{Z}, C) \longrightarrow H^1(G, \mathbb{Z} / m\mathbb{Z})^* \\
\downarrow & \\
C^G / mC^G & \longrightarrow G^{ab} / mG^{ab}
\end{align*} \]

and we have \( \alpha^1(G, \mathbb{Z} / m\mathbb{Z}) = \text{rec}_G : C^G / mC^G \rightarrow G^{ab} / mG^{ab} \).

(3) \ (r = 2)
\[ \begin{align*}
\alpha^2(G, \mathbb{Z} / m\mathbb{Z}) & : \text{Ext}_G^2(\mathbb{Z} / m\mathbb{Z}, C) \longrightarrow H^0(G, \mathbb{Z} / m\mathbb{Z})^* \\
\downarrow & \\
H^2(G, C)[m] & \longrightarrow 1 \mathbb{Z} / \mathbb{Z}
\end{align*} \]

and we have \( \alpha^2(G, \mathbb{Z} / m\mathbb{Z}) = \text{inv}_G |_{H^2(G, C)[m]} \).

**Theorem 2.8 (Main Theorem : Tate).** Let \((G, C)\) be a class formation and \(M \in \text{G-Mod}\) be a finitely generated \(G\)-module. Then,

1. \( \alpha^r(G, M) : \text{Ext}_G^r(M, C) \longrightarrow H^{2-r}(G, M)^* \) is bijective for \( r \geq 2 \).
2. \( \alpha^1(G, M) \) is bijective for torsion-free \( M \).
3. \( \text{Ext}_G^r(M, C) = 0 \) and for torsion-free \( M \) and \( r \geq 3 \).
4. If \( \alpha^1(U, \mathbb{Z} / m\mathbb{Z}) \) is bijective for all open \( U \leq G \) and \( m \geq 1 \), then \( \alpha^1(G, M) \) is bijective.
5. If \( \alpha^0(U, \mathbb{Z} / m\mathbb{Z}) \) is bijective for all open \( U \leq G \) and \( m \geq 1 \), then \( \alpha^0(G, M) \) is bijective for finite \( M \).

**Sketch of proof.**

**Step 1:** \( \text{Ext}_G^r(M, C) = 0 \) for \( r \geq 4 \) and \( \text{Ext}_G^3(M, C) = 0 \) for torsion-free \( M \). (Thus, for large \( r \), we have \( \alpha^r(G, M) : 0 \longrightarrow 0 \).

**Step 2:** Show this when \( G \rhd M \) trivially. It is enough to show for \( M = \mathbb{Z}, \mathbb{Z} / m\mathbb{Z} \).

**Step 3:** General case. Since \( M = \bigcup_U M_U \) is finitely generated, \( M = M_U \) for some open \( U \leq G \).

Define \( \pi : Z[G/U] \xrightarrow{\bigoplus a_g \mapsto \bigoplus a_g} \mathbb{Z} \) and
\[ M = \text{Hom}_Z(Z, M) \xrightarrow{\alpha^*} \text{Hom}_Z(Z[G/U], M) =: I \rightarrow S = \text{coker} \pi^* \]

We get the following diagram:
\[ \begin{array}{cccccccc}
\cdots & \longrightarrow & \text{Ext}_G^r(S, C) & \longrightarrow & \text{Ext}_G^r(I, C) & \longrightarrow & \text{Ext}_G^r(M, C) & \longrightarrow & \text{Ext}_G^{r+1}(S, C) & \longrightarrow & \cdots \\
& & \downarrow \alpha^r(G, S) & & \downarrow \alpha^r(U, M) & & \downarrow \alpha^r(G, M) & & \downarrow \alpha^{r+1}(G, S) & \\
\cdots & \longrightarrow & H^{2-r}(G, S)^* & \longrightarrow & H^{2-r}(G, I)^* & \longrightarrow & H^{2-r}(G, M)^* & \longrightarrow & H^{1-r}(G, S)^* & \longrightarrow & \cdots \\
\end{array} \]
where we have

$$\alpha'(U, M) : \text{Ext}_G^r(I, C) \cong \text{Ext}_U^r(M, C) \rightarrow H^{2-r}(U, M)^* \cong H^{2-r}(G, I)^*$$

We know that \(\alpha'(U, M)\) is an isomorphism because \(U \sim M\) trivially. We can use the five lemma to show the general case.

Detailed proof can be found in [MilADT, p. 21] or [HidMFG, p. 208]. \(\square\)

3. Local/global case

3.1. Local case. Let \(K/Q_p\) be a finite extension and \(G = \text{Gal}(\bar{K}/K)\) (fix \(K\)), \(G \sim C = \bar{K}^\times\). For \(L/K\) finite, we write \(H^2(L/K) = H^2(\text{Gal}(L/K), L^\times)\). We have the following exact sequence:

$$1 \rightarrow U_{K^{\text{un}}} \rightarrow (K^{\text{un}})^\times \rightarrow \mathbf{Z} \rightarrow 0$$

where \(K^{\text{un}}\) is the maximal unramified extension and \(U_{K^{\text{un}}} = \mathcal{O}^\times_{K^{\text{un}}}\). Note that \(H^2_r(\text{Gal}(L/K), U_r) = 0\) for a finite unramified extension \(L/K\) and all \(r\), thus \(H^2_r(\text{Gal}(K^{\text{un}}/K), U_r) = 0\). We define

$$\text{inv}_G = \text{inv}_K : H^2(G, C) = H^2(\bar{K}/K) \xrightarrow{\text{inf}} H^2(K^{\text{un}}/K) \xrightarrow{\sim} H^2(\text{Gal}(K^{\text{un}}/K), \mathbf{Z}) \xrightarrow{\sim} H^1(\text{Gal}(K^{\text{un}}/K), Q/\mathbf{Z})$$

where

$$\text{inf} : H^2(K^{\text{un}}/K) = H^2(\text{Gal}(\bar{K}/K)/\text{Gal}(K^{\text{un}}/K), (\bar{K}^\times)^{\text{Gal}(K^{\text{un}}/K)}) \xrightarrow{\sim} H^2(\text{Gal}(\bar{K}/K), \bar{K}^\times)$$

For open \(U \leq G\), we have \(U = \text{Gal}(\bar{K}/L) = \text{Gal}(L/K)\) for some \(L/K\) finite. Thus we can define

$$\text{inv}_U = \text{inv}_L : H^2(U, C) = H^2(L/K) \xrightarrow{\sim} Q/\mathbf{Z}$$

similarly. Also note that \(H^1(U, \bar{K}^\times)\) by Hilbert theorem 90. Consider the following:

$$\begin{array}{c}
0 \longrightarrow H^2(L/K) \xrightarrow{\rho_{\bar{K}/L}} H^2(\bar{K}/K) \xrightarrow{\text{res}} H^2(\mathcal{L}/L) \\
\downarrow \quad \downarrow \text{inv}_K \quad \downarrow \text{inv}_L \\
0 \longrightarrow \frac{1}{[L:K]} \mathbf{Z}/\mathbf{Z} \xrightarrow{\text{[L:K]}} Q/\mathbf{Z} \xrightarrow{[L:K] = (G:U)} Q/\mathbf{Z}
\end{array}$$

This shows that \((G, \bar{K}^\times)\) is a class formation. By Tate’s theorem, there is a map

$$\text{rec}_G : (\bar{K}^\times)^G = K^\times \hookrightarrow G_{ab} = \text{Gal}(K_{ab}/K)$$

and in fact, we have \(\bar{K}^\times \cong \text{Gal}(K_{ab}/K)\).

**Theorem 3.1** (nonarchimedean case). Let \((G, C) = (\text{Gal}(\bar{K}/K), \bar{K}^\times)\) be a class formation and \(M\) be a finitely generated \(G\)-module. Then,

1. \(\alpha'(G, M) : H^r(G, \text{Hom}(M, \bar{K}^\times)) \xrightarrow{\sim} \text{Ext}_G^r(M, \bar{K}^\times) \rightarrow H^{2-r}(G, M)^*\) is bijective for \(r \geq 1\).
2. \(\alpha^0(G, M) : \text{Hom}_G(M, \bar{K}^\times) \rightarrow H^2(G, M)^*\) is bijective for finite \(M\).
3. For finite \(M\), \(H^r(G, M)\) is finite for \(r = 0, 1, 2\) and zero otherwise.

(This is also true for function field case if we use \(K_{\text{sep}}/K\) and if \(\langle |M|, \text{char } K \rangle = 1\).)
Proof. (1), (2) Let \( I = \text{Gal}(\overline{K}/K^\text{un}) \). We have the following commutative diagram:

\[
\begin{array}{ccccccc}
1 & \rightarrow & O^\times_{\overline{K}} & \rightarrow & K^\times & \rightarrow & \mathbb{Z} & \rightarrow & 0 \\
\downarrow & & \downarrow^\text{rec}_G & & \downarrow & & \downarrow & & \\
1 & \rightarrow & \mathbb{P}^\text{ab} & \rightarrow & G^\text{ab} & \rightarrow & \hat{\mathbb{Z}} & \rightarrow & 0
\end{array}
\]

Tensoring \( \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \) gives

\[
\alpha^1(G, \mathbb{Z}/m\mathbb{Z}) : K^\times/(K^\times)^m \xrightarrow{\sim} G^\text{ab}/(G^\text{ab})^m
\]

and applying \( \text{Hom}_G(\mathbb{Z}/m\mathbb{Z}, \mathbb{K}^\times) \) and \( \text{Hom}_G(\mathbb{Z}/m\mathbb{Z}, -) \) gives

\[
\alpha^0(G, \mathbb{Z}/m\mathbb{Z}) : \mu_m(K^\times) \xrightarrow{\sim} G^\text{ab}[m]
\]

\[
\text{Hom}_G(\mathbb{Z}/m\mathbb{Z}, \mathbb{K}^\times)
\]

Therefore \( \alpha^1(G, M) \) is bijective and so is \( \alpha^0(G, M) \) for finite \( M \) by Theorem 2.8. (3) Note that \( H^r(G, M) = 0 \) for \( r > 2 \) by duality. Since

\[
\alpha^0(G, M) : \text{Hom}_G(M, \overline{K}^\times) \xrightarrow{\sim} H^2(G, M)^*
\]

and \( \text{Hom}_G(M, \overline{K}^\times) \) is finite, \( H^2(G, M) \) is finite. Also, \( H^0(G, M) = M^G \) is finite. Apply \( (-)^G \) to

\[
1 \rightarrow \mu_m \rightarrow \overline{K}^\times \xrightarrow{m} \overline{K}^\times \rightarrow 1
\]

and get

\[
1 \rightarrow \mu_m(K) \rightarrow K^\times \xrightarrow{m} K^\times \rightarrow H^1(G, \mu_m) \rightarrow H^1(G, \overline{K}^\times) = 0 \rightarrow \cdots
\]

From this, we have

\[
H^1(G, \mu_m) \cong K^\times/(K^\times)^m,
\]

which is finite.

Choose \( m \) such that \( mM = 0 \). Take a finite extension \( L/K \) satisfying \( \mu_m \subseteq L \) and \( M^U = M \) for \( U = \text{Gal}(\overline{K}/L) \). Then, \( M = \prod_{\text{finite} \atop n|m} \mu_n \) as a \( U \)-module. We have

\[
0 \rightarrow H^1(G/U, M) \xrightarrow{\text{inf}} H^1(G, M) \xrightarrow{\text{res}} H^1(U, M)
\]

Here \( H^1(G/U, M) \) is finite because \( G/U \) and \( M \) are finite, and \( H^1(U, M) = \oplus H^1(U, \mu_n) \) is also finite by previous argument. Therefore, \( H^1(G, M) \) is finite. \qed

**Theorem 3.2** (archimedean case). (1) Let \( G = \text{Gal}(C/R) \), \( C = \mathbb{C}^\times \) and \( M \) be a finitely generated \( G \)-module. Then,

\[
H^r_t(G, \text{Hom}_Z(M, \mathbb{C}^\times)) \times \mathbb{Z}^\times \rightarrow H^2(G, \mathbb{C}^\times) \xrightarrow{\sim} \frac{1}{2} \mathbb{Z}/\mathbb{Z}
\]

is a perfect pairing for all \( r \in \mathbb{Z} \).

(2) Let \( K = R \) or \( C \), and \( H = \text{Gal}(C/K) \). Let \( M \) be a finite \( H \)-module. Then,

\[
|M|^{[K:R]} = \frac{|H^0(H, M)| \cdot |H^0(H, \text{Hom}_Z(M, \mathbb{C}^\times))|}{|H^1(H, M)|}
\]

Proof. See [MilADT, p. 35]. \qed
3.2. **Global case.** Let $K$ be a number field, $G = \text{Gal}(\overline{K}/K)$ and $C = \lim_{L/K \text{ finite}} C_L$. $(G, C)$ is a class formation, but it is too big.

**Definition 3.3.** Let $P$ be a set of prime numbers. For a $G$-module $C$, $(G, C)$ is called a $P$-class formation if for all open $U \leq G$, there is a map $\text{inv}_U : H^2(U, C) \to \mathbb{Q}/\mathbb{Z}$ such that

1. $H^1(U, C) = 0$
2. for open $V \leq U \leq G$, we have the following commutative diagram

\[
\begin{array}{ccc}
0 & \longrightarrow & H^2(U/V, C) \\
& & \downarrow \text{inv}_U \\
0 & \longrightarrow & H^2(U, C) \quad \text{res} \quad H^2(V, C) \\
& & \downarrow \text{inv}_V \\
& & H^2(U/V, C) \\
\end{array}
\]

(3) for $l \in P$, we have

\[
\text{inv}_U[l] : H^2(U, C)[l\infty] \overset{\sim}{\longrightarrow} (\mathbb{Q}/\mathbb{Z})[l\infty]
\]

between $l$-primary parts.

Let $P$ be a finite set of primes of $\mathbb{Q}$ including $\infty$ and $S$ be the set of primes of $K$ above $P$. Let $K^S/K$ be the maximal unramified extension outside $S$ and $G_S = \text{Gal}(K^S/K)$. For a finite extension $F/K$ inside $K^S$, let $\Sigma$ be the set of primes above $S$. Define $O_F^S = F \cap (\prod_{p \notin \Sigma} \mathcal{O}_{F, p})$, $C_{F,S} = F^\times \cap (O_F^S)^\times$ and $C_S = \lim_{F} C_{F,S}$. Then, $(G_S, C_S)$ is a $P$-class formation.

**Theorem 3.4.** Let $(G_S, C_S)$ be the $P$-class formation defined above and $M$ be a finitely generated $G_S$-module. Suppose $l \in P$. Then,

1. $\alpha^r(G_S, M)[l] : \text{Ext}_G^r(M, C_S)[l\infty] \longrightarrow H^{2-r}(G_S, M)^*[l\infty]$ is bijective for all $r \geq 1$.
2. Let $M$ be finite, and $F/K$ be a totally imaginary extension. Suppose $\text{Gal}(K_S/F) \trianglelefteq M, \mu_{|M|}$ trivially, and $|M|\mathcal{O}_F = \mathcal{O}_S = \lim_{F} O_F^S$. Then, there is the following exact sequence:

\[
\text{Hom}(M, D_S(F)) \overset{N_{F/K}}{\longrightarrow} \text{Hom}_{G_S}(M, C_S) \overset{\alpha^0(G_S, M)}{\longrightarrow} H^2(G_S, M)^* \longrightarrow 0
\]

where $D_S(F)$ is the identity component of $C_F(S) = C_F/U_{F,S}$ where $U_{F,S} = \prod_{l \in P} (\mathcal{O}_F \otimes Z)l^\times$.

**Proof.** See [MilADT, p. 52].

\[\square\]

4. **Euler characteristic formula**

**Definition 4.1** (Local case). Let $K/Q_p$ be a finite extension and $G = \text{Gal}(\overline{K}/K)$. Let $M$ be a finite $G$-module. Then we define the Euler characteristic of $M$ by

\[
\chi(M) = \chi(G, M) = \frac{|H^0(G, M)| \cdot |H^2(G, M)|}{|H^1(G, M)|}
\]

**Theorem 4.2.** $\chi(M) = \frac{1}{\mathcal{O}_K : |M|\mathcal{O}_K}$
Remark 4.3. If \( M \) has \( l \)-power order for a prime \( l \), then \( H^j(G, M) \) is a \( \mathbb{Z}_l \)-module of finite length for all \( j \). We have
\[
\log_l \chi(M) = \sum_{j=0}^{2} (-1)^j \log_l |H^j(G, M)| = \sum_{j=0}^{\infty} (-1)^j \text{length}_{\mathbb{Z}_l} H^j(G, M)
\]
\((H^j(G, M) = 0 \text{ for } j \neq 0, 1, 2)\) and
\[
\log_l \left( \frac{1}{\mathcal{O}_K : |M|_{\mathcal{O}_K}} \right) = \begin{cases} 
0 & l \neq p \\
-|K : Q_p| \text{length}_{\mathbb{Z}_p} M & l = p
\end{cases}
\]

proof of Theorem 4.2. See [HidMFG, p. 228].

Definition 4.4 (Global case). Let \( K/\mathbb{Q} \) be a finite extension and \( G_S = \text{Gal}(K^S/K) \). Let \( M \) be a finite \( G_S \)-module and assume that \( |M|_{\mathcal{O}_S} = \mathcal{O}_S \). Then we define
\[
\chi(M) = \chi(G_S, M) = \frac{|H^0(G_S, M)| \cdot |H^2(G_S, M)|}{|H^1(G_S, M)|}
\]

Remark 4.5. It is NOT true that we have \( H^r(G_S, M) = 0 \) for \( r \geq 3 \) like in local case.

Theorem 4.6. \( \chi(M) = \prod_{v: \text{arch}} \frac{|H^0(G_v, M)|}{|M|_v} \) where \( G_v = \text{Gal}(K_v/K_0) \) and \( |M|_v = |M|_{[K_v:R]} \).

Proof. See [MilADT, p. 67].

References