COHOMOLOGY THEORY OF GALOIS GROUPS

HARUZO HIDA

Contents

1. Extension of Modules 2
1.1. Extension groups 2
1.2. Extension functors 5
1.3. Cohomology groups of complexes 8
1.4. Higher extension groups 10
2. Group Cohomology Theory 15
2.1. Cohomology of finite groups 16
2.2. Tate cohomology groups 20
2.3. Continuous cohomology for profinite groups 23
2.4. Inflation and restriction sequences 30
3. Duality in Galois Cohomology 33
3.1. Class formation and duality of cohomology groups 34
3.2. Global duality theorems 40
3.3. Tate-Shafarevich groups 44
3.4. Local Euler characteristic formula 51
3.5. Global Euler characteristic formula 54
4. Appendix: Categories and Functors 57
4.1. Categories 57
4.2. Functors 58
4.3. Representability 58
4.4. Abelian categories 61
References 63

In this notes, we first describe general theory of forming cohomology groups out of an abelian category and a left exact functor. Then we apply the theory to the category of discrete Galois modules and study resulting Galois cohomology groups. At the end, we would like to give a full proof of the Tate duality theorems and the Euler characteristic formulas of Galois cohomology groups, which were essential in the proof of Fermat's last theorem by A. Wiles.

Date: March 27, 2009.

The author is partially supported by the following NSF grant: DMS 0753991.

1. Extension of Modules

In this section, we describe basics of the theory of module extension functors, and we relate it to group cohomology in the following section.

1.1. **Extension groups.**

We fix a ring Λ with identity, which may not be commutative. We consider the category of Λ–modules Λ–MOD. Thus the objects of Λ–MOD are Λ–modules, and $\mathrm{Hom}_\Lambda(M,N)$ for two Λ–modules M and N is the abelian group of all Λ–linear maps from M into N.

When Λ is a topological ring, we would rather like to consider only Λ–modules with continuous action, that is, continuous Λ–modules, or we might want to impose further restrictions, like compactness or discreteness, to the Λ–modules we study. The totality of such Λ–modules makes a subcategory of Λ–MOD, whose set of morphisms is made of continuous Λ-linear maps. To accommodate such subcategories in an algebraic way without referring topology, we consider subcategories $\mathcal{C}$ of Λ–MOD satisfying a set of conditions enough to define extension functors. First of all, since $\mathcal{C}$ is a subcategory of Λ–MOD,

- Objects of $\mathcal{C}$ are made of a collection $Ob(\mathcal{C})$ of Λ–modules;
- We have a set of $\mathcal{C}$–morphisms: $\mathrm{Hom}_\mathcal{C}(M,N) \subset \mathrm{Hom}_\Lambda(M,N)$ for $M,N \in Ob(\mathcal{C})$;
- The identity map $\mathrm{id}_M : M \to M$ is in $\mathrm{Hom}_\mathcal{C}(M,M)$ for each object M;
- $g \circ f \in \mathrm{Hom}_\mathcal{C}(M,L)$ for $f \in \mathrm{Hom}_\mathcal{C}(M,N)$ and $g \in \mathrm{Hom}_\mathcal{C}(N,L)$.

We impose $\mathcal{C}$ the following four conditions for our purpose:

(C1) The set $\mathrm{Hom}_\mathcal{C}(X,Y) \subset \mathrm{Hom}_\Lambda(X,Y)$ is a subgroup;
(C2) If $f : X \to Y$ be a morphism in $\mathcal{C}$, $\mathrm{Ker}(f)$ and $\mathrm{Coker}(f)$ are both inside $\mathcal{C}$;
(C3) If X and Y are in $\mathcal{C}$, then the direct product $X \times Y$ is in $\mathcal{C}$;
(C4) The zero module $\{0\}$ is in $\mathcal{C}$.

These conditions guarantee that $\mathcal{C}$ is an abelian category (see 4.4 for formal definitions of abelian categories). Hereafter we fix such a category $\mathcal{C}$ and work only in $\mathcal{C}$. We call Λ–linear map: $X \to Y$ for objects X and Y in $\mathcal{C}$ a *$\mathcal{C}$–morphism* if it is in $\mathrm{Hom}_\mathcal{C}(X,Y)$. Similarly an isomorphism which is also a $\mathcal{C}$–morphism is called a $\mathcal{C}$–isomorphism.

For a given pair of Λ–modules M and N in $\mathcal{C}$, we would like to know all Λ–modules E in $\mathcal{C}$ which fit into the following exact sequence in $\mathcal{C}$:

$$0 \longrightarrow N \xrightarrow{\iota_N} E \xrightarrow{\pi_M} M \longrightarrow 0.$$

We call such E an extension in $\mathcal{C}$ of Λ–module M by N. Two extensions E and E' are called isomorphic if we have a $\mathcal{C}$–isomorphism $\xi : E \cong E'$ making the following diagram commutative:

$$\begin{tikzcd} N \arrow[r, hook] \arrow[d, equal] & E \arrow[r, two heads] \arrow[d, "\xi"'] & M \arrow[d, equal] \\ N \arrow[r, hook] & E' \arrow[r, two heads] & M. \end{tikzcd}$$

We write $E(M,N) = E_\mathcal{C}(M,N)$ for the set of all isomorphism classes of extensions of M by N. When $\mathcal{C} = \Lambda$–MOD, we write $E_\Lambda(M,N)$ for $E_\mathcal{C}(M,N)$. Note that $M \oplus N \in E(M,N)$; so, $E(M,N) \neq \emptyset$. An extension E is called split, if we have a $\mathcal{C}$–morphism $\iota_M : M \to E$ such that $\pi_M \circ \iota_M = \mathrm{id}_M$. Then $E \cong M \oplus N$ by $e \mapsto \iota_M(\pi_M(e)) \oplus (e - \iota_M(\pi_M(e))$. The map ι_M is called a section of π_M. This shows the class $M \oplus N \in E(M,N)$ is the unique split extension class. If we have a projection $\pi_N : E \to N$ such that $\pi_N \circ \iota_N = \mathrm{id}_N$, then again $E \cong M \oplus N$ by $e \mapsto (e - \iota_N(\pi_N(e))) \oplus \iota_N(\pi_N(e))$, because $\mathrm{Ker}(\pi_N) \cong M$ by π_M in this case.

If $\Lambda = \mathbb{Z}$ and $M = N = \mathbb{Z}/p\mathbb{Z}$ for a prime p, then we have at least two extensions: $(\mathbb{Z}/p\mathbb{Z})^2$ and $\mathbb{Z}/p^2\mathbb{Z}$ in $E_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$.

Now we would like to study how $E(M,N)$ changes if we change M and N by their homomorphic image (or source). For a given $\mathcal{C}$–morphism $M \xrightarrow{\varphi} X$ and $N \xrightarrow{\phi} X$, the fiber product $T = M \times_X N$ is a Λ–module in $\mathcal{C}$ with the following property:

(FP1) We have two projections

$$\alpha : T \to M \quad \text{and} \quad \beta : T \to N$$

in $\mathcal{C}$ making the following diagram commutative:

$$\begin{tikzcd} M \times_X N \arrow[r, "\alpha"] \arrow[d, "\beta"'] & M \arrow[d, "\varphi"] \\ N \arrow[r, "\phi"'] & X; \end{tikzcd}$$

(FP2) If the following diagram in $\mathcal{C}$ is commutative:

$$\begin{tikzcd} Y \arrow[r, "\alpha'"] \arrow[d, "\beta'"'] & M \arrow[d, "\varphi"] \\ N \arrow[r, "\phi"'] & X, \end{tikzcd}$$

then there exist a unique $\mathcal{C}$–morphism $\gamma : Y \to M \times_X N$ such that $\alpha' = \alpha \circ \gamma$ and $\beta' = \beta \circ \gamma$.

If two fiber products T and T' exist in $\mathcal{C}$, then we have $\gamma : T' \to T$ and $\gamma' : T \to T'$ satisfying (FP2) for $Y = T'$ and $Y = T$, respectively. Then id_T and $\gamma \circ \gamma' : T \to T$ satisfy (PF2) for $Y = T$, and by the uniqueness, $\gamma \circ \gamma' = \mathrm{id}_T$. Similarly, $\gamma' \circ \gamma = \mathrm{id}_{T'}$ and hence $T \cong T'$. Thus the fiber product of M and N is unique in $\mathcal{C}$ up to isomorphisms if it exists. It is easy to see that

$$M \times_X N = \big\{(m,n) \in M \times N \big| \varphi(m) = \phi(n)\big\}$$

satisfies the property (FP1-2) for $\mathcal{C} = \Lambda$–MOD and the two projections $\alpha : M \times_X N \to M$ and $\beta : M \times_X N \to N$ taking (m,n) to m and n respectively. For this choice, $\gamma(y)$ is given by $(\alpha'(y), \beta'(y)) \in M \times_X N$. Thus fiber products exist in Λ–MOD. If further φ and ϕ are $\mathcal{C}$–morphisms, then by the existence of $M \times N$ in $\mathcal{C}$, the above $M \times_X N$ in Λ–MOD is actually the kernel of $(\alpha - \beta) \circ (\varphi \oplus \phi)$, which is therefore a member of $\mathcal{C}$. This shows the existence of the fiber product in $\mathcal{C}$. In functorial terms, the fiber product represents the functor:

$$Y \mapsto \{(\alpha', \beta') \in \mathrm{Hom}_{\mathcal{C}}(Y, M \times N) | \varphi \circ \alpha' = \phi \circ \beta'\}$$

from $\mathcal{C}$ to $SETS$.

Let $N \hookrightarrow E \twoheadrightarrow M$ be an extension in $\mathcal{C}$. For a $\mathcal{C}$–morphism $\varphi : M' \to M$, we look at the fiber product $E' = E \times_M M'$. Let $\pi' : E' \to M'$ be the projection. Since $\pi : E \to M$ is a surjection, for each $m' \in M'$, we find $e \in E$ such that $\pi(e) = \varphi(m')$. By definition, $\pi'(e, m') = m'$, and π' is a surjection. Then

$$\begin{aligned}\mathrm{Ker}(\pi') &= \{(e,m') \in E \times_M M' | \pi'(m) = 0\} \\ &= \{(e,m') \in E \times M' | \pi(e) = \pi'(m) = 0\} = \mathrm{Ker}(\pi) = \mathrm{Im}(\iota_N) \cong N.\end{aligned}$$

Thus we get an extension $N \hookrightarrow E' \twoheadrightarrow M'$ in $E(M', N)$. Namely we have $E(\varphi, N) : E(M, N) \to E(M', N)$ taking

$$N \hookrightarrow E \twoheadrightarrow M \quad \text{to} \quad N \hookrightarrow E' = E \times_M M' \twoheadrightarrow M'.$$

Note that for two $\mathcal{C}$–morphisms: $M'' \xrightarrow{\varphi'} M' \xrightarrow{\varphi} M$, it is easy to check that

$$E' \times_{M'} M'' = (E \times_M M') \times_{M'} M'' \cong E \times_{M, \varphi\circ\varphi'} M''.$$

This shows that

$$E(\varphi', N) \circ E(\varphi, N) = E(\varphi \circ \varphi', N);$$

so, the functor $M \mapsto E(M, N)$ for a fixed N is a contravariant functor.

Suppose we have two $\mathcal{C}$–morphisms $\varphi : X \to M$ and $\phi : X \to N$. We define a fiber sum (or push-out) $S = M \oplus_X N$ under X by the following conditions:

(FS1) We have two inclusions $\alpha : M \to S$ and $\beta : N \to S$ in $\mathcal{C}$ making the following diagram commutative:

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[d, "\phi"'] & M \arrow[d, "\alpha"] \\ N \arrow[r, "\beta"'] & S; \end{tikzcd}$$

(FS2) If the following diagram in $\mathcal{C}$ is commutative:

$$\begin{tikzcd} X \arrow[r, "\varphi"] \arrow[d, "\phi"'] & M \arrow[d, "\alpha'"] \\ N \arrow[r, "\beta'"'] & Y, \end{tikzcd}$$

then there exists a unique morphism $\gamma : S \to Y$ such that $\alpha' = \gamma \circ \alpha$ and $\beta' = \gamma \circ \beta$.

In the same way as in the case of fiber products, the fiber sum is unique up to isomorphisms if it exists. We define $S = M \oplus_X N$ to be the quotient of $M \times N$ by the Λ–submodule generated by $\varphi(x) - \phi(x)$ for all $x \in X$ (that is, the cokernel of $\varphi - \phi : X \to M \times N$). The inclusions α and β are induced by the inclusions $M \hookrightarrow M \oplus N$ and $N \hookrightarrow M \oplus N$.

If $N \hookrightarrow E \twoheadrightarrow M$ is an extension in $\mathcal{C}$, then for $\phi : N \to N'$, it is easy to check that $N' \backslash (N' \oplus_N E) \cong M$ and $N' \hookrightarrow N' \oplus_N E \twoheadrightarrow M$ is an extension in $\mathcal{C}$. The association

$N \hookrightarrow E \twoheadrightarrow M \mapsto N' \hookrightarrow N' \oplus_N E \twoheadrightarrow M$ gives rise to a map $E(M, \phi) : E(M, N) \to E(M, N')$. From the above argument, we get the following fact:

Theorem 1.1. *The association $(M, N) \mapsto E_{\mathcal{C}}(M, N)$ is a functor from $\mathcal{C} \times \mathcal{C}$ into the category $SETS$ of sets, contravariant with respect to the left variable and covariant with respect to the right variable. This means that for morphisms $M'' \xrightarrow{\varphi'} M' \xrightarrow{\varphi} M$ and $N \xrightarrow{\phi} N' \xrightarrow{\phi'} N''$ in $\mathcal{C}$, $E(\varphi', N) \circ E(\varphi, N) = E(\varphi \circ \varphi', N)$ and $E(M, \phi') \circ E(M, \phi) = E(M, \phi' \circ \phi)$.*

Exercises.

(1) Compute $E_{\mathbb{Z}}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ for a prime p;
(2) Compute $E_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$;
(3) Show the existence and the uniqueness of the fiber sum $M \oplus_X N$ in $\mathcal{C}$;
(4) Give a detailed proof of Theorem 1.1.

1.2. **Extension functors.** We would like to find a mechanical way of computing the extension groups. An object I in $\mathcal{C}$ is called *$\mathcal{C}$–injective* if for every $\mathcal{C}$–morphism $\varphi : M \to I$ and every injective $\mathcal{C}$–morphism $i : M \hookrightarrow N$, there exists a $\mathcal{C}$–linear map $\phi : N \to I$ extending φ, that is, the following diagram is commutative:

$$\begin{tikzcd} M \arrow[r, hook] \arrow[d, "\varphi"'] & N \arrow[dl, "\exists\phi"] \\ I. & \end{tikzcd}$$

An *injective presentation* of N is an exact sequence $N \hookrightarrow I \overset{\pi}{\twoheadrightarrow} S$ for a $\mathcal{C}$–injective module I. We always assume

(EI) $\mathcal{C}$ has enough injectives, that is, for a given N in $\mathcal{C}$, an injective presentation exists in $\mathcal{C}$.

Then we apply the covariant functor $* \mapsto \mathrm{Hom}_{\mathcal{C}}(M, *)$ to the above sequence, getting the following exact sequence:

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{C}}(M, N) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(M, I) \xrightarrow{\pi_*} \mathrm{Hom}_{\mathcal{C}}(M, S). \tag{1.1}$$

Then we define $\mathrm{Ext}^1_{\mathcal{C}}(M, N) = \mathrm{Coker}(\pi_*)$.

We claim that the cokernel $\mathrm{Coker}(\pi_*)$ is independent of the choice of the injective presentation. To show this, we pick a $\mathcal{C}$–morphism $\phi : N \to N'$, and let $N' \xrightarrow{i'} I' \xrightarrow{\pi'} S'$ be an injective presentation of N'. Then we have the following commutative diagram:

$$\begin{tikzcd} N \arrow[r, hook] \arrow[d, "i' \circ \phi"'] & I \arrow[dl, "\exists\phi_1"] \\ I'. & \end{tikzcd}$$

The $\mathcal{C}$–injectivity of I' implies that $i' \circ \phi$ extends to $\phi_1 : I \to I'$. We call ϕ_1 a lift of ϕ. Then ϕ_1 induces a $\mathcal{C}$–morphism $\phi_2 : S \to S'$, making the following diagram commutative:

$$\begin{tikzcd}
N \arrow[r] \arrow[d, "\phi"'] & I \arrow[r, "\pi"] \arrow[d, "\phi_1"'] & S \arrow[d, "\phi_2"'] \\
N' \arrow[r] & I' \arrow[r, "\pi'"] & S'.
\end{tikzcd}$$

From this, we get another commutative diagram:

$$\begin{tikzcd}
0 \to \mathrm{Hom}_{\mathcal{C}}(M,N) \arrow[r] \arrow[d, "\phi_*"'] & \mathrm{Hom}_{\mathcal{C}}(M,I) \arrow[r, "\pi_*"] \arrow[d, "\phi_{1,*}"'] & \mathrm{Hom}_{\mathcal{C}}(M,S) \arrow[d, "\phi_{2,*}"'] \\
0 \to \mathrm{Hom}_{\mathcal{C}}(M,N') \arrow[r] & \mathrm{Hom}_{\mathcal{C}}(M,I') \arrow[r, "\pi'_*"] & \mathrm{Hom}_{\mathcal{C}}(M,S').
\end{tikzcd}$$

Suppose now that we have two lifts $\phi_1, \phi'_1 : I \to I'$ of ϕ. Then $\phi_1 - \phi'_1|_N = \phi - \phi = 0$. Thus $\phi_1 - \phi'_1 = \tau \circ \pi$ for a $\mathcal{C}$–morphism $\tau : S \to I'$, and hence, $(\phi_2 - \phi'_2)_* = \pi'_* \circ \tau_*$. This implies that the morphisms of $\mathrm{Coker}(\pi_*)$ into $\mathrm{Coker}(\pi'_*)$ induced by ϕ_2 and ϕ'_2 are equal, which we write as ϕ_*. We apply the above argument to $\phi = \mathrm{id}_N : N = N$ and its inverse ϕ'. Then $\phi_* \circ \phi'_* = \mathrm{id}_{\mathrm{Coker}(\pi'_*)}$ and $\phi'_* \circ \phi_* = \mathrm{id}_{\mathrm{Coker}(\pi_*)}$ showing $\mathrm{Coker}(\pi_*) \cong \mathrm{Coker}(\pi'_*)$ canonically.

We fix an injective presentation $N \hookrightarrow I \xrightarrow{\pi} S$ for each N in $\mathcal{C}$ and define the functor $(M,N) \mapsto \mathrm{Ext}^1_{\mathcal{C}}(M,N) = \mathrm{Coker}(\pi_*)$. This functor is defined on $\mathcal{C}$ and has values in AB. The above argument shows that the association $\mathcal{C} \to AB$ given by $N \mapsto \mathrm{Ext}^1_{\mathcal{C}}(M,N)$ is a covariant functor, that is, $\phi_* = \mathrm{Ext}^1_{\mathcal{C}}(M,\phi) : \mathrm{Ext}^1_{\mathcal{C}}(M,N) \to \mathrm{Ext}^1_{\mathcal{C}}(M,N')$ satisfies

$$\mathrm{Ext}^1_{\mathcal{C}}(M,\phi') \circ \mathrm{Ext}^1_{\mathcal{C}}(M,\phi) = \mathrm{Ext}^1_{\mathcal{C}}(M,\phi' \circ \phi) \tag{1.2}$$

for two $\mathcal{C}$–morphisms $N \xrightarrow{\phi} N' \xrightarrow{\phi'} N''$.

Let $\varphi : M' \to M$ be a $\mathcal{C}$–morphism. This induces

$$\varphi^*_X = \mathrm{Hom}(\varphi, X) : \mathrm{Hom}_{\mathcal{C}}(M,X) \to \mathrm{Hom}_{\mathcal{C}}(M',X)$$

given by $\phi \mapsto \phi \circ \varphi$, and we have the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Hom}(M,N) \arrow[r] \arrow[d, "\varphi^*_N"'] & \mathrm{Hom}(M,I) \arrow[r] \arrow[d, "\varphi^*_I"'] & \mathrm{Hom}(M,S) \arrow[r] \arrow[d, "\varphi^*_S"] & \mathrm{Ext}^1(M,N) \arrow[d, "\mathrm{Ext}(\varphi,N)"] \\
\mathrm{Hom}(M',N) \arrow[r] & \mathrm{Hom}(M',I) \arrow[r] & \mathrm{Hom}(M',S) \arrow[r] & \mathrm{Ext}^1(M',N).
\end{tikzcd}$$

It is easy to check

$$\mathrm{Ext}^1(\varphi',N) \circ \mathrm{Ext}^1(\varphi,N) = \mathrm{Ext}^1(\varphi \circ \varphi',N) \tag{1.3}$$

for two $\mathcal{C}$–morphisms $M'' \xrightarrow{\varphi'} M' \xrightarrow{\varphi} M$.

Thus the functor $(M,N) \mapsto \mathrm{Ext}^1_{\mathcal{C}}(M,N)$ is contravariant with respect to M and covariant with respect to N.

We now claim

Theorem 1.2. *We have an isomorphism $\iota(M,N) : E_{\mathcal{C}}(M,N) \cong \mathrm{Ext}^1_{\mathcal{C}}(M,N)$ such that $\iota(M',N) \circ E(\varphi,N) = \mathrm{Ext}^1_{\mathcal{C}}(\varphi,N) \circ \iota(M,N)$ for each $\mathcal{C}$–morphism $\varphi : M' \to M$ and $\iota(M,N') \circ E_{\mathcal{C}}(M,\phi) = \mathrm{Ext}^1_{\mathcal{C}}(M,\phi) \circ \iota(M,N)$ for each $\mathcal{C}$–morphism $\phi : N \to N'$. In other words, the system of isomorphisms $\iota(M,N)$ gives an isomorphism between two functors $E_{\mathcal{C}}$ and $\mathrm{Ext}^1_{\mathcal{C}}$. In particular, the set $E_{\mathcal{C}}(M,N)$ has a natural structure of an abelian group.*

Proof. We pick an extension $N \overset{\alpha}{\hookrightarrow} E \twoheadrightarrow M \in E_{\mathcal{C}}(M,N)$. We look at the following diagram:

$$\begin{tikzcd}
N \arrow[r, hook] \arrow[d] & E \arrow[dl, "\exists\alpha_*"] \\
I,
\end{tikzcd}$$

which induces the following commutative diagram:

$$\begin{tikzcd}
N \arrow[r, hook] \arrow[d, equal] & E \arrow[r, two heads] \arrow[d, "\alpha_*"'] & M \arrow[d, "\alpha_{*,M}"] \\
N \arrow[r, hook] & I \arrow[r, two heads, "\pi"] & S.
\end{tikzcd}$$

Now we associate the class of $[\alpha_{*.M}] \in \mathrm{Coker}(\pi_*)$ to the extension $N \overset{\alpha}{\hookrightarrow} E \twoheadrightarrow M$. If we have another lift $\alpha'_* : E \to I$ making the first diagram commutative, then $\alpha'_* - \alpha_* = 0$ on N, and hence it factors through $E/N = M$. This shows that $[\alpha_{*,M}] = [\alpha'_{*,M}]$, getting $\iota(M,N) : E(M,N) \to \mathrm{Ext}^1_{\mathcal{C}}(M,N)$.

We now construct the inverse of ι. We start from $[\alpha] \in \mathrm{Coker}(\pi_*)$ for $\alpha : M \to S = I/N$. We put $E = I \times_S M$. Then we get an extension $N \hookrightarrow E \twoheadrightarrow M$. If $[\alpha] = [\alpha']$, then there exists $\tau : M \to I$ such that $\pi\tau = \alpha - \alpha'$. We then define $I \times_{S,\alpha} M \cong I \times_{S,\alpha'} M$ by $(i,m) \mapsto (i - \tau(m), m)$. Thus we get a well defined map $\iota'(M,N) : \mathrm{Ext}^1(M,N) \to E(M,N)$. It is easy to check by following the definition that $\iota(M,N) \circ \iota'(M,N) = \mathrm{id}_{\mathrm{Ext}}$ and $\iota'(M,N) \circ \iota(M,N) = \mathrm{id}_E$. We leave the reader to check the functoriality of ι. □

There is one more way of constructing $E(M,N)$ using projective presentations. A Λ–module P in $\mathcal{C}$ is called *$\mathcal{C}$–projective* if any $\mathcal{C}$–morphism $\alpha : P \to N$ can be extended to $\alpha_E : P \to E$ for each surjective $\mathcal{C}$–morphism $\pi : E \twoheadrightarrow N$ so that $\pi\alpha_E = \alpha$, that is, the following diagram is commutative:

$$\begin{tikzcd}
 & P \arrow[dl, "\exists\alpha_E"'] \arrow[d, "\alpha"] \\
E \arrow[r, two heads] & N.
\end{tikzcd}$$

Thus the notion of $\mathcal{C}$–projective modules is the dual of that of $\mathcal{C}$–injective Λ–modules, in the sense that we have reversed the direction of arrows in the definition, and injectivity of arrows is replaced by surjectivity. Any Λ–free module is Λ–*MOD*–projective. A *projective presentation* of Λ–module M in $\mathcal{C}$ is an exact sequence $T \overset{\iota}{\hookrightarrow} P \twoheadrightarrow M$ with $\mathcal{C}$–projective P. For the moment, we assume

(EP) $\mathcal{C}$ has enough projective, that is, for each $M \in \mathcal{C}$, there exists a $\mathcal{C}$–projective presentation of M.

As we will see, sometimes (EP) may not be satisfied even if (EI) holds for $\mathcal{C}$. Then applying the functor $X \mapsto \mathrm{Hom}_{\mathcal{C}}(X, N)$, we get an exact sequence:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(M, N) \to \mathrm{Hom}_{\mathcal{C}}(P, N) \xrightarrow{\iota^*} \mathrm{Hom}_{\mathcal{C}}(T, N).$$

Then we can show that $\mathrm{Coker}(\iota^*)$ is independent of the choice of the presentation (just reversing the arrows in the proof in the case of injective presentations) and is isomorphic to $E_{\mathcal{C}}(M, N)$. One can find details in [HAL] Chapter III.

Exercises.

(1) Show (1.1) is exact;

(2) Give a detailed proof for (1.2) and (1.3).

(3) Give a detailed proof of Theorem 1.2;

(4) Show that the addition on $E(M, N) = E_{\Lambda-MOD}(M, N)$ is given actually by the following procedure: Let $N \hookrightarrow E \twoheadrightarrow M$ and $N \hookrightarrow E' \twoheadrightarrow M$ be two extensions in $E(M, N)$. Let $\triangle_M$: $M \to M \oplus M$ be the diagonal map $(\triangle_M\ (a) = a \oplus a)$ and $\nabla_N : N \oplus N \to N$ be the summation $(\nabla_N(n \oplus n') = n + n')$. Then the sum of the two extension is given by
$$E(\triangle_M, \nabla_N)(N \oplus N \hookrightarrow E \oplus E' \twoheadrightarrow M \oplus M).$$

(5) Define $\mathrm{Ext}^1_{\mathcal{C}}(M, N)$ by $\mathrm{Coker}(\iota^*)$ using projective presentation $T \overset{\iota}{\hookrightarrow} P \twoheadrightarrow M$, and prove the counterpart of Theorem 1.2 in this setting. Further show that the additive structure of $E(M, N)$ is independent of the choice of either an injective presentation of N or a projective presentation of M.

1.3. **Cohomology groups of complexes.** A *graded module* in $\mathcal{C}$ is an infinite direct sum $M^\bullet = \bigoplus_{j\in\mathbb{Z}} M_j$ of Λ–modules M_j in $\mathcal{C}$. We suppose either $M_j = 0$ for $j < -N$ or $M_j = 0$ for $j > N$ with sufficiently large N. A $\mathcal{C}$–morphism $f : M^\bullet \to N^\bullet$ of graded modules in $\mathcal{C}$ is called a morphism of *degree* k if $f(M_j) \subset N_{j+k}$ for all j. If there is a $\mathcal{C}$–endomorphism $\partial : M^\bullet \to M^\bullet$ of degree 1 with $\partial \circ \partial = 0$, we call the pair $(M^\bullet, \partial)$ a *complex* in $\mathcal{C}$. A *$\mathcal{C}$–chain map* $f : (M^\bullet, \partial) \to (N^\bullet, \delta)$ of degree r is a $\mathcal{C}$–morphism of degree r such that $f \circ \partial = \delta \circ f$. For a given complex $(M^\bullet, \partial)$, we define its cohomology group $H^\bullet(M^\bullet, \partial)$ by

$$H^q(M^\bullet, \partial) = \frac{\mathrm{Ker}(\partial : M_q \to M_{q+1})}{\mathrm{Im}(\partial : M_{q-1} \to M_q)}.$$

Any chain map $f : (M^\bullet, \partial) \to (N^\bullet, \delta)$ of degree r induces a linear map $[f] : H^q(M^\bullet, \partial) \to H^{q+r}(N^\bullet, \delta)$.

Lemma 1.3. *Suppose the following diagram is commutative with two exact rows made of Λ–modules:*

$$\begin{tikzcd}
 & M \arrow[r, "a"] \arrow[d, "d"'] & L \arrow[r, "b"] \arrow[d, "d'"'] & N \arrow[r] \arrow[d, "d''"] & 0 \\
0 \arrow[r] & M' \arrow[r, "a'"] & L' \arrow[r, "b'"] & N'. &
\end{tikzcd}$$

Then there exists a Λ*–linear map* $\delta : \mathrm{Ker}(d'') \to \mathrm{Coker}(d)$*, and the following sequence is exact:*

$$\mathrm{Ker}(d) \to \mathrm{Ker}(d') \to \mathrm{Ker}(d'') \xrightarrow{\delta} \mathrm{Coker}(d) \to \mathrm{Coker}(d') \to \mathrm{Coker}(d'').$$

This lemma is often called the snake lemma.

Proof. By the exactness of the first row and commutativity, the maps a and b induce $\mathrm{Ker}(d) \xrightarrow{a} \mathrm{Ker}(d') \xrightarrow{b} \mathrm{Ker}(d'')$. Similarly, a' and b' induce $\mathrm{Coker}(d) \xrightarrow{a'} \mathrm{Coker}(d') \xrightarrow{b'} \mathrm{Coker}(d'')$. It is easy to check that they are exact at the middle terms (see Exercise 1).

Now let us define $\delta : \mathrm{Ker}(d'') \to \mathrm{Coker}(d)$. Pick $x \in \mathrm{Ker}(d'')$. By the surjectivity of b, we have $y \in L$ such that $a(y) = x$. The choice of y is unique modulo $\mathrm{Im}(a)$. Then we apply d' to y getting $d'(y) \in L'$. Thus $d'(y)$ is unique modulo $\mathrm{Im}(d' \circ a) = \mathrm{Im}(a' \circ d)$. Apply b' to $d'(y)$, getting $b'(d'(y)) = d''(b(y)) = d''(x) = 0$ because $x \in \mathrm{Ker}(d'')$. Thus $b'(d'(y)) \in \mathrm{Im}(a')$; so, we take $z \in M'$ with $a'(z) = b'(d'(y))$. The element $z \in M'$ is unique modulo ${a'}^{-1}(\mathrm{Im}(a' \circ d)) = \mathrm{Im}(d)$, determining a unique class $[z] \in \mathrm{Coker}(d)$. Then define $\delta(x) = [z]$.

We check the exactness of the sequence at $\mathrm{Ker}(d'')$. By definition, if $x \in \mathrm{Ker}(d'') \cap b(\mathrm{Ker}(d'))$, then $y \in \mathrm{Ker}(d')$; so, $d'(y) = 0$. This shows that $\delta \circ b = 0$. Suppose that $\delta(x) = 0$. Then $z \in \mathrm{Im}(d)$; so, we can choose $t \in M$ so that $z = d(t)$. Since we can change y modulo $\mathrm{Im}(a)$, we replace y by $y' = y - a(t)$. Then $d'(y') = d'(y - a(t)) = d'(y) - d'(a(t)) = d'(y) - a'(d(t)) = 0$. This shows $y' \in \mathrm{Ker}(d')$ and hence $x = b(y') \in \mathrm{Im}(b : \mathrm{Ker}(d') \to \mathrm{Ker}(d''))$.

We check the exactness at $\mathrm{Coker}(d)$. Since $a'(z) = d'(y)$, $a' \circ \delta = 0$. Suppose $a'([s]) = 0$ for $s \in M'$. Then $a'(s) = d'(y')$ for $y' \in L$. Then for $x' = b(y')$, we see $d''(x') = d''(b(y')) = b'(d'(y')) = b'(a'(s)) = 0$. Thus $x' \in \mathrm{Ker}(d'')$. Then by definition, $\delta(x') = [s]$. This finishes the proof. □

Proposition 1.4. *Let* $0 \to (M^\bullet, d) \xrightarrow{a} (L^\bullet, d') \xrightarrow{b} (N^\bullet, d'') \to 0$ *be an exact sequence of* $\mathcal{C}$*–chain maps of degree* 0*. Then we have a connection map* $\delta_q : H^q(N^\bullet, d'') \to H^{q+1}(M^\bullet, d)$ *for each* q *and a long exact sequence:*

$$H^q(M^\bullet, d) \xrightarrow{[a]_q} H^q(L^\bullet, d') \xrightarrow{[b]_q} H^q(N^\bullet, d'')$$
$$\xrightarrow{\delta_q} H^{q+1}(M^\bullet, d) \xrightarrow{[a]_{q+1}} H^{q+1}(L^\bullet, d') \xrightarrow{[b]_{q+1}} H^{q+1}(N^\bullet, d'').$$

Proof. Because of the exactness of the complexes, we have the following commutative diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & M_q \arrow[r, "a_q"] \arrow[d, "d_q"] & L_q \arrow[r, "b_q"] \arrow[d, "d'_q"'] & N_q \arrow[r] \arrow[d, "d''_q"] & 0 \\
0 \arrow[r] & M_{q+1} \arrow[r, "a_{q+1}"] & L_{q+1} \arrow[r, "b_{q+1}"] & N_{q+1} \arrow[r] & 0.
\end{tikzcd}$$

This yields another commutative diagram with exact rows:

$$\begin{tikzcd}
 M_q/\operatorname{Im}(d_{q-1}) \arrow[r, "{[a_q]}"] \arrow[d, "{[d_q]}"'] & L_q/\operatorname{Im}(d'_{q-1}) \arrow[r, "{[b_q]}"] \arrow[d, "{[d'_q]}"'] & N_q/\operatorname{Im}(d''_{q-1}) \arrow[r] \arrow[d, "{[d''_q]}"'] & 0 \\
0 \arrow[r] & \operatorname{Ker}(d_{q+1}) \arrow[r, "{[a_{q+1}]}"] & \operatorname{Ker}(d'_{q+1}) \arrow[r, "{[b_{q+1}]}"] & \operatorname{Ker}(d''_{q+1}).
\end{tikzcd}$$

The exactness of the first row comes from the snake lemma applied to cokernels of differential maps of the first diagram for degree $q-1$. The exactness of the second row comes from the snake lemma applied to the kernels of the first diagram at degree $q+1$. Note that the kernels of the vertical maps of the second diagram are the cohomology groups of degree q, and the cokernels are those of degree $q+1$. Now apply the snake lemma to the second diagram, we get the long exact sequence and the connection map δ_q. □

We consider the following condition:

(CN) *The connection map δ is a $\mathcal{C}$–morphism as long as the diagram in the lemma is in $\mathcal{C}$.*

We remark that in the above proof, we have not used the condition (CN), since the condition is always valid for the target category AB of the cohomology functors.

1.4. **Higher extension groups.** Two degree r $\mathcal{C}$–chain maps $f, g : (M^\bullet, \partial) \to (N^\bullet, \delta)$ are called *homotopy equivalent* if there exists a $\mathcal{C}$–morphism $\Delta : M^\bullet \to N^\bullet$ of degree $r-1$ such that $f - g = \delta \circ \Delta + \Delta \circ \partial$. We write $f \sim g$ if f and g are homotopy equivalent. This is an equivalence relation, and we have the identity of cohomology maps $[f] = [g]$ if $f \sim g$.

For a given Λ–module M in $\mathcal{C}$, a *$\mathcal{C}$–resolution* of M is an exact sequence in $\mathcal{C}$:

$$0 \to M \xrightarrow{\varepsilon} M_0 \xrightarrow{\partial_0} M_1 \xrightarrow{\partial_1} M_2 \to \cdots \to M_j \xrightarrow{\partial_j} M_{j+1} \to \cdots .$$

Thus we may put $M^\bullet = \bigoplus_{j=0}^{\infty} M_j$ (regarding $M_j = 0$ if $j < 0$), and $\partial : M^\bullet \to M^\bullet$ is a differential map making $M^\bullet$ a $\mathcal{C}$–complex. We sometimes write the resolution as $0 \to M \xrightarrow{\varepsilon} (M^\bullet, \partial)$, and ε is called the *augmentation* map.

An *injective* resolution of M is a resolution $0 \to M \xrightarrow{\varepsilon_M} (M^\bullet, \partial)$ with $\mathcal{C}$–injective M_j for all j. Since $\mathcal{C}$ has enough injectives, we have an injective presentation $\varepsilon_M : M \hookrightarrow M_0$. Suppose we have an exact sequence: $0 \to M \xrightarrow{\varepsilon_M} M_0 \to \cdots \xrightarrow{\partial_{j-1}} M_j$. Then taking an injective presentation $0 \to \operatorname{Coker}(\partial_{j-1}) \xrightarrow{f} M_{j+1}$ and defining $\partial_j : M_j \to M_{j+1}$ by the composite $\partial_j : M_j \twoheadrightarrow \operatorname{Coker}(\partial_{j-1}) \xrightarrow{f} M_{j+1}$, we see that $0 \to M \xrightarrow{\varepsilon_M} M_0 \to \cdots \to M_j \xrightarrow{\partial_j} M_{j+1}$ is exact. Thus under (EI), we always have a $\mathcal{C}$–injective resolution of a given M in $\mathcal{C}$.

For two Λ–modules M and N in $\mathcal{C}$, we take a $\mathcal{C}$–resolution $0 \to M \xrightarrow{\varepsilon_M} (M^\bullet, \partial)$ and an injective $\mathcal{C}$–resolution $0 \to N \xrightarrow{\varepsilon_N} (N^\bullet, \delta)$ and consider the group made of homotopy classes of degree r $\mathcal{C}$–chain maps from $(M^\bullet, \partial)$ into $(N^\bullet, \delta)$, which we write $\mathrm{Ext}^r_{\mathcal{C}}(M, N)$.

Proposition 1.5. *The abelian group* $\mathrm{Ext}^r_{\mathcal{C}}(M, N)$ *does not depend on the choice of the resolution* $(M^\bullet, \partial)$ *and the injective resolution* $(N^\bullet, \delta)$*. Moreover we have* $\mathrm{Ext}^0_{\mathcal{C}}(M, N) \cong \mathrm{Hom}_{\mathcal{C}}(M, N)$ *and* $\mathrm{Ext}^1_{\mathcal{C}}(M, N) \cong E_{\mathcal{C}}(M, N)$*.*

Proof. Let $\varphi : M \to N$ be a $\mathcal{C}$–morphism. Then we have the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, "\varphi"'] & M_0 \arrow[d, "\exists\varphi_0"'] \\
0 \arrow[r] & N \arrow[r, "\varepsilon_N"'] & N_0 .
\end{tikzcd}$$

We claim the existence of a $\mathcal{C}$–morphism φ_0 making the above diagram commutative. This follows from the $\mathcal{C}$–injectivity of N_0 applied to $\varepsilon_N \circ \varphi : M \to N_0$. Then φ_0 induces a $\mathcal{C}$–morphism: $\mathrm{Coker}(\varepsilon_M) \to \mathrm{Coker}(\varepsilon_N)$, which is still written as φ_0. Then we have the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Coker}(\varepsilon_M) \arrow[r] \arrow[d, "\varphi_0"'] & M_1 \arrow[d, "\exists\varphi_1"'] \\
0 \arrow[r] & \mathrm{Coker}(\varepsilon_N) \arrow[r, "\delta_0"'] & N_1 .
\end{tikzcd}$$

The existence of a $\mathcal{C}$–morphism φ_1 making the above diagram commutative again follows from the injectivity of N_1 applied to $\delta_0 \circ \varphi_0$. Repeating the above process, we get a $\mathcal{C}$–chain map of degree 0: $\varphi^\bullet : M^\bullet \to N^\bullet$, which we call a lift of φ. Suppose that we have two lifts $\varphi^\bullet$ and $\varphi'^\bullet$. Then $\varphi_0 - \varphi'_0 = 0$ on $\mathrm{Im}(\varepsilon_M)$, and hence $\varphi_0 - \varphi'_0$ factors through $\mathrm{Coker}(\varepsilon_M) \cong \mathrm{Im}(\partial_0)$. Thus we have the following commutative diagram by the injectivity of N_0:

$$\begin{tikzcd}
\mathrm{Im}(\partial_0) \arrow[r, hook] \arrow[d, "\varphi_0 - \varphi'_0"'] & M_1 \arrow[dl, "\exists\Delta_1"] \\
N_0 . &
\end{tikzcd}$$

We put here $\Delta_0 : M_0 \to N_1 = \{0\}$ to be the zero map. Thus we have the homotopy relation:

$$\varphi_0 - \varphi'_0 = \Delta_1 \circ \partial_0 + \delta_{-1} \circ \Delta_0.$$

Suppose now by induction on j that we have $\Delta_k : M_k \to N_{k-1}$ for $k \le j$ such that

$$\varphi_{k-1} - \varphi'_{k-1} = \Delta_k \circ \partial_{k-1} + \delta_{k-2} \circ \Delta_{k-1}$$

for all $k \le j$. Then we look at

$$\varphi_j - \varphi'_j - \delta_{j-1} \circ \Delta_j : M_j \to N_j.$$

Note that

$$\begin{aligned}
(\varphi_j - \varphi'_j - \delta_{j-1} \circ \Delta_j) \circ \partial_{j-1} &= \delta_{j-1} \circ (\varphi_j - \varphi'_j) - \delta_{j-1} \circ \Delta_j \circ \partial_{j-1} \\
&= \delta_{j-1} j \circ (\varphi_j - \varphi'_j) - \delta_{j-1} \circ (\varphi_j - \varphi'_j - \delta_{j-1} \circ \Delta_j) = 0.
\end{aligned}$$

Thus $\phi = \varphi_j - \varphi'_j - \delta_{j-1} \circ \Delta_j$ factors through $\mathrm{Coker}(\partial_{j-1}) = \mathrm{Im}(\partial_j)$ and we have another commutative diagram by the injectivity of N_j:

$$\begin{tikzcd}
\mathrm{Im}(\partial_j) \arrow[r, hook] \arrow[d, "\phi"'] & M_{j+1} \arrow[dl, "\exists\Delta_{j+1}"] \\
N_j. &
\end{tikzcd}$$

This shows that $\varphi^\bullet - \varphi'^\bullet = \delta \circ \Delta + \Delta \circ \partial$ and $\varphi^\bullet \sim \varphi'^\bullet$. Namely we have a well defined map: $\mathrm{Hom}_{\mathcal{C}}(M, N) \to \mathrm{Ext}^0_{\mathcal{C}}(M, N)$. Since $M \subset M_0$ and $N \subset N_0$, this map is injective. On the other hand, if $\varphi^\bullet : M^\bullet \to N^\bullet$ is a chain map, φ_0 induces a $\mathcal{C}$–morphism $\varphi : M = \mathrm{Ker}(\partial_0) \to \mathrm{Ker}(\delta_0) = N$, which gives rise to the original $\varphi^\bullet$ via the above construction (up to homotopy). This shows that $\mathrm{Ext}^0_{\mathcal{C}}(M, N) \cong \mathrm{Hom}_{\mathcal{C}}(M, N)$ canonically.

Now we look at $\mathrm{Ext}^r_{\mathcal{C}}(M, N)$, which is made of homotopy equivalence classes of $\mathcal{C}$–chain maps of degree r from $M^\bullet$ into $N^\bullet$. We now define $N[r]^\bullet = \bigoplus_{j=-r}^{\infty} N[r]_j$ for $N[r]_j = N_{j+r}$. Then each degree r chain map: $M^\bullet \to N^\bullet$ can be regarded as a degree 0 chain map: $M^\bullet \to N[r]^\bullet$, and by the same computation above,

$$\mathrm{Ext}^r_{\mathcal{C}}(M, N) = H^r(\mathrm{Hom}_{\mathcal{C}}(M, N^\bullet), \delta_*). \tag{1.4}$$

We repeat the beginning of the argument: We have the following diagram:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\varepsilon_M"] \arrow[d, "\varphi"'] & M_0 \arrow[d, "\exists\varphi_0"'] \\
& N_{r-1} = N[r]_{-1} \arrow[r, "\delta_{r-1}"] & N[r]_0 = N_r.
\end{tikzcd}$$

Pick $\varphi \in \mathrm{Hom}_{\mathcal{C}}(M, N_r)$ with $\delta_r \circ \varphi = 0$ (because φ has to be a part of the chain map). We start constructing a lift $\varphi_j : M_j \to N[r]_j$. If we change φ by $\varphi + \delta_{r-1} \circ \phi$ for $\phi \in \mathrm{Hom}_{\mathcal{C}}(M, N_{r-1})$, the outcome is homotopy equivalent to the original lift (by definition), and we get

$$\mathrm{Ext}^r_{\mathcal{C}}(M, N) = \frac{\mathrm{Ker}(\delta_{r,*} : \mathrm{Hom}_{\mathcal{C}}(M, N_r) \to \mathrm{Hom}_{\mathcal{C}}(M, N_{r+1}))}{\delta_{r-1,*}(\mathrm{Hom}_{\mathcal{C}}(M, N_{r-1}))}.$$

Thus we need to show that $H^\bullet(\mathrm{Hom}_{\mathcal{C}}(M, N^\bullet), \delta_*)$ is independent of the choice of the resolution $N^\bullet$. We take another resolution $N'^\bullet$. Then applying the above argument, replacing $(M^\bullet, N^\bullet, \varphi : M \to N)$ by $(N^\bullet, N'^\bullet, \mathrm{id} : N \to N)$, we have a lift $\iota : N^\bullet \to N'^\bullet$ whose homotopy class is uniquely determined. Thus we have a unique map: $[\iota] : H^\bullet(\mathrm{Hom}_{\mathcal{C}}(M, N^\bullet)) \to H^\bullet(\mathrm{Hom}_{\mathcal{C}}(M, N'^\bullet))$. Reversing this operation, we get $[\iota'] : H^\bullet(\mathrm{Hom}_{\mathcal{C}}(M, N'^\bullet)) \to H^\bullet(\mathrm{Hom}_{\mathcal{C}}(M, N^\bullet))$. By the uniqueness of the lift up to homotopy, we find that $[\iota] \circ [\iota'] = [\mathrm{id}_{N'}]$ and $[\iota'] \circ [\iota] = [\mathrm{id}_N]$. This shows the two cohomology groups are canonically isomorphic.

Since we have shown that $\mathrm{Ext}^r_{\mathcal{C}}(M, N)$ is independent of the choice of $M^\bullet$, we can take the trivial resolution: $0 \to M \overset{\varepsilon_M}{\cong} M \to 0$. Then using this, it is easy to see that $\mathrm{Ext}^1_{\mathcal{C}}(M, N) = \mathrm{Coker}(\delta_{0,*})$ for $\delta_{0,*} : \mathrm{Hom}_{\mathcal{C}}(M, N_0) \to \mathrm{Hom}_{\mathcal{C}}(M, \mathrm{Im}(\delta_0))$. Since $N \hookrightarrow N_0 \twoheadrightarrow \mathrm{Im}(\delta_0)$ is an injective presentation, we see from Theorem 1.2 that $\mathrm{Ext}^1_{\mathcal{C}}(M, N) \cong E_{\mathcal{C}}(M, N)$ canonically. □

The proof of the above proposition shows

Corollary 1.6. *Let $M, N \in \mathcal{C}$ and $0 \to M \to M^\bullet$ (resp. $0 \to N \to N^\bullet$) be a resolution in $\mathcal{C}$ (resp. a $\mathcal{C}$–injective chain complex with augmentation from N). Here $N^\bullet$ may or may not be a resolution. Then for every morphism $\varphi : M \to N$, there is a chain map in $\mathcal{C}^\bullet$ $\varphi^\bullet : M^\bullet \to N^\bullet$ such that φ_0 induces φ. The lift $\varphi^\bullet$ is unique up to homotopy equivalence.*

There is another consequence:

Corollary 1.7. *If N is a $\mathcal{C}$–injective module, then $\mathrm{Ext}^r_{\mathcal{C}}(M, N) = 0$ for all M in $\mathcal{C}$ if $r > 0$.*

This follows from the fact that $0 \to N \xrightarrow{\mathrm{id}} N \to 0$ is a $\mathcal{C}$–injective resolution of N.

Let L be a third Λ–module in $\mathcal{C}$. We take a $\mathcal{C}$–injective resolution $0 \to L \to (L^\bullet, d)$. If $g : N^\bullet \to L^\bullet$ is a $\mathcal{C}$–chain map of degree s, then

$$g \circ (\Delta \circ \partial + \delta \circ \Delta) = g \circ \Delta \circ \partial + g \circ \delta \circ \Delta = (g \circ \Delta) \circ \partial + d \circ (g \circ \Delta).$$

Thus g preserves homotopy equivalence. Thus $g \circ f : M^\bullet \to L^\bullet$ for a chain map $f : M^\bullet \to N^\bullet$ of degree r defines a homotopy class in $\mathrm{Ext}^{r+s}_{\mathcal{C}}(M, L)$, which depends only on classes $[f] \in \mathrm{Ext}^r_{\mathcal{C}}(M, N)$ and $[g] \in \mathrm{Ext}^s_{\mathcal{C}}(N, L)$. Thus we have

Corollary 1.8. *The composition of chain maps induces a bilinear form*

$$\mathrm{Ext}^r_{\mathcal{C}}(M, N) \times \mathrm{Ext}^s_{\mathcal{C}}(N, L) \to \mathrm{Ext}^{r+s}_{\mathcal{C}}(M, L).$$

Proposition 1.9. *Let $0 \to N \xrightarrow{a} E \xrightarrow{b} L \to 0$ be an exact sequence in $\mathcal{C}$. Then we have connection maps: $\mathrm{Ext}^r_{\mathcal{C}}(M, L) \to \mathrm{Ext}^r_{\mathcal{C}}(M, N)$ and the following long exact sequence:*

$$\begin{aligned} &\mathrm{Ext}^r_{\mathcal{C}}(M, N) \to \mathrm{Ext}^r_{\mathcal{C}}(M, E) \to \mathrm{Ext}^r_{\mathcal{C}}(M, L) \\ &\qquad\qquad \to \mathrm{Ext}^{r+1}_{\mathcal{C}}(M, N) \to \mathrm{Ext}^{r+1}_{\mathcal{C}}(M, E) \to \mathrm{Ext}^{r+1}_{\mathcal{C}}(M, L). \end{aligned}$$

Proof. Let $0 \to (N^\bullet, \delta)$ and $0 \to (L^\bullet, d)$ be $\mathcal{C}$–injective resolutions of N and L respectively. Just as a graded module, we put $E^\bullet = \bigoplus_{j=0}^{\infty} (N_j \oplus L_j)$ and we like to create a differential $\partial : E^\bullet \to E^\bullet$ so that $0 \to E \to (E^\bullet, \partial)$ is an injective resolution of E. If we can do this, we will have an exact sequence of complexes:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(M, N^\bullet) \to \mathrm{Hom}_{\mathcal{C}}(M, E^\bullet) \to \mathrm{Hom}_{\mathcal{C}}(M, L^\bullet) \to 0,$$

and then by Proposition 1.4, we have the desired long exact sequence from (1.4) in the proof of Proposition 1.5, because $\mathrm{Ext}^r_{\mathcal{C}}(M, N) = H^r(\mathrm{Hom}_{\mathcal{C}}(M, N^\bullet))$.

We start from the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, hook] \arrow[d, "\varepsilon_N"'] & E \arrow[dl, "\exists\varepsilon'"] \\
 & N_0. &
\end{tikzcd}$$

The existence of $\varepsilon' : E \to N_0$ follows from the $\mathcal{C}$–injectivity of N_0. Then we define $\varepsilon_E : E \to E_0 = N_0 \oplus L_0$ by $\varepsilon_E(e) = \varepsilon'(e) \oplus \varepsilon_L(b(e))$. If $\varepsilon_E(e) = 0$, then $\varepsilon_L(b(e)) = 0$, and hence $e \in \mathrm{Im}(a)$, because $\varepsilon_L : L \to L_0$ is injective. Writing $e = a(n)$, we then see

$0 = \varepsilon'(e) = \varepsilon'(a(n)) = \varepsilon_N(n)$ and hence $n = 0$ by the injectivity of ε_N. This shows $e = a(n) = 0$. Thus ε_E is injective. We suppose that we have constructed an exact sequence:

$$0 \to E \xrightarrow{\varepsilon_E} E_0 \xrightarrow{\partial_0} E_1 \to \cdots \to E_j$$

so that the following diagram is commutative up to $k \le j$:

$$\begin{tikzcd}
N_{k-1} \arrow[r, hook] \arrow[d, "\delta_{k-1}"'] & E_{k-1} = N_{k-1} \oplus L_{k-1} \arrow[r, two heads] \arrow[d, "\partial_{k-1}"'] & L_{k-1} \arrow[d, "d_{k-1}"] \\
N_k \arrow[r, hook] & E_k = N_k \oplus L_k \arrow[r, two heads] & L_k.
\end{tikzcd}\tag{1.5}$$

Then we have the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Coker}(\delta_{j-1}) \arrow[r, hook] \arrow[d, "\delta_j"'] & \operatorname{Coker}(\partial_{j-1}) \arrow[dl, "\exists\partial'"'] \\
 & N_{j+1}. &
\end{tikzcd}$$

We claim that the first row is exact. To see this, we apply the snake lemma to (1.5) for $k = j-1$, which shows that the natural map: $\operatorname{Im}(\partial_{j-1}) = \operatorname{Coker}(\partial_{j-2}) \to \operatorname{Coker}(d_{j-2}) = \operatorname{Im}(d_{j-1})$ is surjective. Again applying the snake lemma to:

$$\begin{tikzcd}
\operatorname{Im}(\delta_{j-1}) \arrow[r] \arrow[d, "\cap"'] & \operatorname{Im}(\partial_{j-1}) \arrow[r] \arrow[d, "\cap"'] & \operatorname{Im}(d_{j-1}) \arrow[r] \arrow[d, "\cap"'] & 0 \\
N_j \arrow[r] & E_j \arrow[r] & L_j, &
\end{tikzcd}$$

we get the desired injectivity. Then the existence of ∂' follows from the $\mathcal{C}$–injectivity of N_{j+1}, and as before, we define $\partial_j : E_j \twoheadrightarrow \operatorname{Coker}(\partial_{j-1}) \to E_{j+1}$ by $\partial_j(x) = \partial'(x) \oplus d_j(b_j(x))$ for $b_j : E_j \to L_j$. We can check similarly as in the case of ε_L that ∂_j as a map from $\operatorname{Coker}(\partial_{j-1})$ to E_{j+1} is injective. This shows that $E_{j-1} \xrightarrow{\partial_{j-1}} E_j \xrightarrow{\partial_j} E_{j+1}$ is exact. Thus by induction on j, we get the desired $\mathcal{C}$–injective resolution $0 \to E \to E^\bullet$. □

Remark 1.1. In the above proof of Corollary 1.8, we have lifted a given exact sequence $0 \to N \to E \xrightarrow{b} L \to 0$ in $\mathcal{C}$ to an exact sequence of injective resolutions: $0 \to N^\bullet \to E^\bullet \to L^\bullet \to 0$. Although we have used the surjectivity of b to do that, actually we can lift an exact sequence $0 \to N \to E \xrightarrow{b} L$ to an exact sequence of complexes: $0 \to N^\bullet \to E^\bullet \to L^\bullet$ in the following way: The above proof applied to $0 \to \operatorname{Im}(b) \to L \to L/\operatorname{Im}(b) \to 0$ tells us that we can choose an injective resolution $L^\bullet$ so that any given injective resolution $\operatorname{Im}(b)^\bullet$ of $\operatorname{Im}(b)$ is embedded into $L^\bullet$. Then applying again the above proof to $0 \to N \to E \to \operatorname{Im}(b) \to 0$, we get an exact sequence $0 \to N^\bullet \to E^\bullet \to \operatorname{Im}(b)^\bullet \to 0$. Combinig with $\operatorname{Im}(b)^\bullet \hookrightarrow L^\bullet$, we get the desired exact sequence: $0 \to N^\bullet \to E^\bullet \to L^\bullet$.

We have used an injective resolution of N to define $\operatorname{Ext}^r_{\mathcal{C}}(M, N)$, and then it turns out $\operatorname{Ext}^r_{\mathcal{C}}(M, N) = H^r(\operatorname{Hom}_{\mathcal{C}}(M, N^\bullet), \delta_*)$. We can instead use a dual version (basically reversing all arrows in the above construction and use a projective resolution of

M). Suppose here that $\mathcal{C}$ has enough projectives. A projective resolution of M is an exact sequence of $\mathcal{C}$–projective modules M_j:

$$\cdots \to M_j \xrightarrow{\partial_j} M_{j-1} \to \cdots \to M_0 \xrightarrow{\pi_M} M \to 0.$$

Then we consider the reversed complex:

$$\mathrm{Hom}_{\mathcal{C}}(M^\bullet, N) = \bigoplus_{j=0}^{\infty} \mathrm{Hom}_{\mathcal{C}}(M_j, N)$$

with differentials $\partial_j^* : \mathrm{Hom}_{\mathcal{C}}(M_{j-1}, N) \to \mathrm{Hom}_{\mathcal{C}}(M_j, N)$ given by sending a map $(\phi : M_{j-1} \to N)$ to $(\phi\partial_j : M_j \to N)$. Then it turns out that

$$\text{(DF)} \qquad \mathrm{Ext}^r_{\mathcal{C}}(M, N) \cong H^r(\mathrm{Hom}_{\mathcal{C}}(M^\bullet, N), \partial^*).$$

Actually this definition of the extension modules is more standard (see [HAL] IV.7-8, for example). The extension module $\mathrm{Ext}^1_{\mathcal{C}}(M, N)$ is also related to the classification of r–extensions, where an r–extension is an exact sequence:

$$0 \to N \to E_r \to E_{r-1} \to \cdots \to E_1 \to M \to 0$$

in $\mathcal{C}$, but the description is not as straightforward as in the case of $r = 0, 1$ (see [HAL] IV.9).

The dual version of Proposition 1.9 is given as follows:

Proposition 1.10. *We suppose* (EP) *. Let*

$$0 \to M \xrightarrow{a} E \xrightarrow{b} L \to 0$$

be an exact sequence in $\mathcal{C}$*. Then we have connection maps:* $\mathrm{Ext}^r_{\mathcal{C}}(M, N) \to \mathrm{Ext}^r_{\mathcal{C}}(L, N)$ *and the following long exact sequence:*

$$\begin{aligned} &\mathrm{Ext}^r_{\mathcal{C}}(L, N) \to \mathrm{Ext}^r_{\mathcal{C}}(E, N) \to \mathrm{Ext}^r_{\mathcal{C}}(M, N) \\ &\qquad \to \mathrm{Ext}^{r+1}_{\mathcal{C}}(L, N) \to \mathrm{Ext}^{r+1}_{\mathcal{C}}(E, N) \to \mathrm{Ext}^{r+1}_{\mathcal{C}}(M, N). \end{aligned}$$

The proof is just a reverse (dual) of that of Proposition 1.9; so, we leave it to the reader (Exercise 1).

The last remark in this section is that we can realize $\mathrm{Ext}^r_{\mathcal{C}}(M, N)$ as a set of r–extension classes as already remarked. This construction extends to any category $\mathcal{C}$ satisfying (C1–4) and the existence of long exact sequence is known in this general case (cf. [HAL] IV.9). Thus actually, the condition (EI) (or (EP)) is not necessary to have a theory of $\mathrm{Ext}_{\mathcal{C}}$.

Exercises.

(1) Give a detailed proof of Proposition 1.10.

2. Group Cohomology Theory

In this section, we study basic properties of group cohomology theory.

2.1. **Cohomology of finite groups.** Let G be a group. For any given commutative ring A with identity, we define the group algebra $A[G]$ by the set of all formal A–linear combinations $\sum_{g\in G} a_g g$ of group elements $g \in G$. The product of the two elements in $A[G]$ is given by:

$$\sum_{g\in G} a_g g \cdot \sum_{h\in G} b_h h = \sum_{g,h\in G} a_g b_h gh.$$

Then $A[G]$ is an A–algebra, whose identity is given by the identity of G. When G is finite, for each $A[G]$–module M, we define $H^r_A(G, M) = \mathrm{Ext}^r_{A[G]}(A, M)$, where on A, G acts trivially, that is, $ga = a$ for all $a \in A$ and $g \in G$. Later we will extend this definition to infinite G in a various way. For the moment, we assume that G is finite.

To compute the cohomology group explicitly, we construct a standard projective resolution of A: Let $A_n = A[\overbrace{G \times G \times \cdots \times G}^{n+1}]$ and regard A_n as a $A[G]$–module by $g(g_0, \cdots , g_n) = (gg_0, \ldots , gg_n)$. Then we define $\partial_n : A_n \to A_{n-1}$ by $\partial_n(g_0, \ldots , g_n) = \sum_{j=0}^{n} (-1)^j (g_0, \ldots , \widehat{g}_j, \ldots , g_n)$, where $\widehat{g}_j$ indicates g_j to be removed. Since any element of A_n is a formal linear combination of $(g_0, \ldots , g_n)$, we extend ∂_n to the whole A_n linearly. By definition, it is obvious that $\partial_{n-1} \circ \partial_n = 0$. Since A_n is an $A[G]$–free module with base $(1, g_1, \ldots , g_n)$, A_n is $A[G]$–projective.

We define $\pi_A : A_0 \to A$ by $\pi_A(\sum_g a_g g) = \sum_g a_g$. We claim now that $\cdots \to A_n \to \cdots \to A_0 \xrightarrow{\pi_A} A \to 0$ is exact. To show this, we now define A–linear maps $\Delta_n : A_n \to A_{n+1}$ by $\Delta_n(g_0, \ldots , g_n) = (1, g_0, \ldots , g_n)$. Then it is a matter of computation that

$$\partial\Delta + \Delta\partial = \mathrm{id}_{A^\bullet} . \tag{2.1}$$

for the complex $A^\bullet = \bigoplus_{n=0}^{\infty} A_n$. Thus the identity map is homotopy equivalent to the 0–map in the category A–$MOD^\bullet$ (not in $A[G]$–$MOD^\bullet$), and hence the identity map of $H^r(A^\bullet, \partial)$ is the zero-map if $r > 0$. This shows that

$$H^0(A^\bullet, \partial) = A \quad \text{and} \quad H^r(A^\bullet, \partial) = 0 \quad \text{if } r > 0$$

and that $A^\bullet \to A \to 0$ is a $A[G]$–projective resolution.

We can always regard M as $\mathbb{Z}[G]$–module. Thus we also have $H^r_{\mathbb{Z}}(G, M)$.

Proposition 2.1. *For each $A[G]$–module M, we have a canonical isomorphism:*

$$H^r_A(G, M) \cong H^r_{\mathbb{Z}}(G, M).$$

Proof. By (DF) in 1.4, we have $H^r_A(G, M) = H^r(\mathrm{Hom}_{A[G]^\bullet}(A^\bullet, M), \partial^*)$. Since $A^\bullet = \mathbb{Z}^\bullet \otimes_{\mathbb{Z}} A$ by definition, we have (see Exercise 2-3)

$$\mathrm{Hom}_{\mathbb{Z}[G]^\bullet}(\mathbb{Z}^\bullet, M) \cong \mathrm{Hom}_{A[G]}(\mathbb{Z}^\bullet \otimes_{\mathbb{Z}} A, M \otimes_A A) = \mathrm{Hom}_{A[G]}(A^\bullet, M).$$

The first isomorphism is given by associating to $f : \mathbb{Z}_n \to M$ a linear map $f_A : \mathbb{Z}_n \otimes_A A \to M \otimes_A A = M$ such that $f_A(z \otimes a) = af(z)$. Using the $\mathbb{Z}[G]$–freeness of $\mathbb{Z}_n$, it is easy to check that $f \mapsto f_A$ is an isomorphism. This shows that

$$H^r_A(G, M) = H^r(\mathrm{Hom}_{A[G]^\bullet}(A^\bullet, M)) = H^r(\mathrm{Hom}_{\mathbb{Z}[G]^\bullet}(\mathbb{Z}^\bullet, M)) = H^r_{\mathbb{Z}}(G, M),$$

as desired. □

Thus, there is no need to specify the base ring A in the definition of $H^r_A(G,M)$; so, we write just $H^r(G,M)$ for this module (although we need to keep in mind that the definition $H^r(G,M) = \mathrm{Ext}^r_{A[G]}(A,M)$ works only for $A[G]$–modules M).

Corollary 2.2. *If G is a finite group and M is a finite G–module, then $H^r(G,M)$ is a finite module.*

Proof. Let A be the center of $\mathrm{End}_{\mathbb{Z}[G]}(M)$, which is a finite ring. Then M is an $A[G]$–module. The standard resolution $A^\bullet \to A \to 0$ is made of finite modules. Then each component of the complex $\mathrm{Hom}_{A[G]^\bullet}(A^\bullet, M)$ is again a finite module. Thus $H^r(G,M) = H^r(\mathrm{Hom}_{A[G]^\bullet}(A^\bullet, M), \partial^*)$ is a finite module. □

There is another standard projective resolution $\underline{A}^\bullet$ of A in $A[G]$–MOD (which is called the standard inhomogeneous resolution) given as follows: We put $\underline{A}_n = A_n$ but let G act (inhomogeneously) on $\underline{A}_n$, which is a bit different from the homogeneous action on A_n, by

$$g(g_0, \dots, g_n) = (gg_0, g_1, \dots, g_n).$$

Then again $\underline{A}_n$ is a $A[G]$ free module with basis $[g_1, \dots, g_n] = (1, g_1, \dots, g_n)$. In particular, $\underline{A}_0$ is the rank one free $A[G]$ module generated by $[\ ] = (1)$. Define the differential $\underline{\partial}_n : \underline{A}_n \to \underline{A}_{n-1}$ by

$$\underline{\partial}_n([g_1, \dots, g_n]) = g_1[g_2, \dots, g_n] \\ + \sum_{j=1}^{n-1} (-1)^j [g_1, \dots, \overset{j}{g_j g_{j+1}}, \dots, g_n] + (-1)^n [g_1, \dots, g_{n-1}].$$

The augmentation: $\underline{A}_0 \to A$ is given by the degree map π_A as in the case of homogeneous chain complex (this is all right, because $\underline{A}_0 = A_0$ as $A[G]$–module, that is, the homogeneous and inhomogeneous actions are the same at degree 0). Again we have $\mathrm{id}_{\underline{A}^\bullet} = \underline{\partial\Delta} + \underline{\Delta\partial}$ for the following A–linear maps:

$$\underline{\Delta}_{-1}(1) = [\ ], \quad \underline{\Delta}_n((x_0, x_1, \dots, x_n)) = [x_0, x_1, \dots, x_n].$$

This shows that $\underline{A}^\bullet$ is a projective resolution of A in $A[G]$–MOD.

Since $\phi \in \mathrm{Hom}_{A[G]}(\underline{A}_n, M)$ for an $A[G]$–module M is determined by its values at the base $\{[x_1, \dots, x_n]\}$, we can identify $\mathrm{Hom}_{A[G]}(\underline{A}_n, M)$ with the space $C_n(M)$ of all functions $\phi : \overbrace{G \times G \times \cdots \times G}^{n} \to M$. Thus by evaluation at the standard base,

$$(\mathrm{Hom}_{A[G]^\bullet}(\underline{A}^\bullet, M), \underline{\partial}^*) \cong (C^\bullet(M) = \bigoplus_{n \geq 0} C_n(M), \delta),$$

where

$$\delta_{n-1}(\phi)(x_1, \dots, x_n) = x_1\phi(x_2, \dots, x_n) \\ + \sum_{j=1}^{n-1} (-1)^j \phi(x_1, \dots, x_j x_{j+1}, \dots, x_n) + (-1)^n \phi(x_1, \dots, x_{n-1}).$$

We call a function ϕ an *n–cocycle* (resp. *n–coboundary*) if $\delta_n(\phi) = 0$ (resp. $\phi = \delta_{n-1}(\psi)$). From this, we find

$$u \in \mathrm{Ker}(\delta_1) \iff u(gh) = gu(h) + u(g)$$

for all $g, h \in G$ and

$$\delta_0(m)(g) = (g-1)m$$

for some $m \in M$. Thus for a finite group G

$$H^0(G,M) = \{m \in M | gm = m \ \forall g \in G\}, \tag{2.2}$$

$$H^1(G,M) = \frac{\{u : G \to M | u(gh) = gu(h) + u(g)\}}{\{g \mapsto (g-1)m | m \in M\}}.$$

In particular, for A with the trivial G–action,

$$H^1(G,A) = \mathrm{Hom}_{gp}(G,A).$$

When G is a finite cyclic group generated by g, we have a very simple projective resolution of $\mathbb{Z}$: We define $C_n = \mathbb{Z}[G]$ for all n. Then we define $\partial_{2n} : C_{2n+1} \to C_{2n}$ by $\partial_{2n}(x) = (g-1)x$ and $\partial_{2n-1} : C_{2n} \to C_{2n-1}$ by $\partial_{2n-1}(x) = N_G x = \sum_{h \in G} hx$. We leave the reader to check that $C^\bullet$ with augmentation $C_0 \to \mathbb{Z}$ given by $\sum_h a_h h \mapsto \sum_h a_h$ is a resolution. From this, we get

Proposition 2.3. *Suppose that G is a finite cyclic group generated by g. Then*

$$H^{2n}(G,M) \cong M^G/N_G M \quad \textit{and} \quad H^{2n-1}(G,M) = \mathrm{Ker}(N_G : M \to M)/(g-1)M$$

for all $n > 0$.

Remark 2.1. If G is a topological (possibly infinite) group, that is, the multiplication: $(g,h) \mapsto gh$ and the inverse $g \mapsto g^{-1}$ are supposed to be continuous, we can think of continuous G–modules M. That is, a G–module M with a topology given, and we require the action $G \times M \to M$ given by $(g,m) \mapsto gm$ is continuous. Then we can define a subcomplex $C^\bullet_{ct}(M) \subset C^\bullet(M)$ by requiring continuity to elements in $C^\bullet(M)$. Obviously the differential δ sends $C^\bullet_{ct}(M)$ into itself, giving rise to a differential of $C^\bullet_{ct}(M)$. The continuous cohomology $H^\bullet_{ct}(G,M)$ is defined by $H^\bullet(C^\bullet_{ct}(M),\delta)$. By definition, the inclusion $C^\bullet_{ct}(M) \hookrightarrow C^\bullet(M)$ induces a canonical map $H^\bullet_{ct}(G,M) \to H^\bullet(G,M)$. Here note that this map of the two cohomology groups may not be injective and may not be surjective either. Suppose that G is a profinite group topologically generated by an element g of infinite order and that M is a discrete G–module. Then we claim

$$H^1_{ct}(G,M) \cong M/(g-1)M. \tag{2.3}$$

Let us prove the claim. For each continuous 1–cocycle $u : G \to M$, we see easily that $u(g^n) = (1 + g + \cdots + g^{n-1})u(g)$ for $0 < n \in \mathbb{Z}$ and $u(g^{-1}) = -g^{-1}u(g)$. Thus for a given $x \in M$, we define a map $u : H = \{g^n | n \in \mathbb{Z}\} \to M$ by the above formula. We can easily check that u is a 1–cocycle of H and is continuous under the topology on H induced by G, if M is discrete. Thus by continuity, u extends to a 1–cocycle on G. Then $u \mapsto u(g)$ induces the isomorphism (2.3). We will see later that $H^2_{ct}(G,M) = 0$

if G is a profinite group topologically generated by an element g of infinite order and M is a discrete G–module.

Let U be a subgroup of G of finite index. We consider the following isomorphism for $\mathbb{Z}[U]$–module M:

$$\eta : \mathrm{Hom}_{\mathbb{Z}[G]^\bullet}(\mathbb{Z}^\bullet, \mathrm{Hom}_{\mathbb{Z}[U]}(\mathbb{Z}[G], M)) \cong \mathrm{Hom}_{\mathbb{Z}[U]^\bullet}(\mathbb{Z}^\bullet, M). \tag{2.4}$$

The isomorphism η is given by the equation $\eta(\varphi)(x) = (\varphi(x))(1)$ (Exercise 5). The module $\mathrm{Hom}_{\mathbb{Z}[U]}(\mathbb{Z}[G], M)$ is considered to be a $\mathbb{Z}[G]$–module by $g\varphi(x) = \varphi(xg)$. Then $\mathbb{Z}^\bullet$ is also a $\mathbb{Z}[U]$–projective resolution of $\mathbb{Z}$, because $\mathbb{Z}[G]$ is a $\mathbb{Z}[U]$–free module. We have

$$H^\bullet(G, \mathrm{Hom}_{\mathbb{Z}[U]}(\mathbb{Z}[G], M)) \cong H^\bullet(\mathrm{Hom}_{\mathbb{Z}[U]^\bullet}(\mathbb{Z}^\bullet, M)) = H^\bullet(U, M). \tag{2.5}$$

Choosing a coset decomposition $G = \bigsqcup_{\xi\in\Xi} U\xi$, we see that $\mathbb{Z}[G]$ is a $\mathbb{Z}[U]$–free module with basis Ξ. We consider a linear map $\theta : \mathrm{Hom}_{\mathbb{Z}[U]}(\mathbb{Z}[G], M) \to M$ given by $\varphi \mapsto \sum_{\xi\in\Xi} \xi^{-1}\varphi(\xi)$. The map θ is well defined independent of the choice of Ξ because $(u\xi)^{-1}\varphi(u\xi) = \xi^{-1}u^{-1}\varphi(u\xi) = \xi^{-1}\varphi(\xi)$ for all $u \in U$. For each $g \in G$, $\xi g = u_g\xi_g$ for $u_g \in U$ and $\xi_g \in \Xi$. The map: $\xi \mapsto \xi_g$ is a permutation on Ξ. Then we have

$$\begin{aligned}\theta(g\varphi) = \sum_\xi \xi^{-1}\varphi(\xi g) = \sum_\xi \xi^{-1}u_g\varphi(\xi_g)&\\ &= \sum_\xi (u_g^{-1}\xi)^{-1}\varphi(\xi_g) = \sum_\xi (\xi_g g^{-1})^{-1}\varphi(\xi_g) = g\theta(\varphi).\end{aligned}$$

This shows that θ is a morphism of $\mathbb{Z}[G]$–module. In particular, we have a linear map:

$$trf_{G/U} : H^\bullet(U, M) = H^\bullet(G, \mathrm{Hom}_{\mathbb{Z}[U]}(\mathbb{Z}[G], M)) \xrightarrow{H^\bullet(\theta)} H^\bullet(G, M), \tag{2.6}$$

which is called the *transfer* map. We define the restriction map $res_{G/U} : H^\bullet(G, M) \to H^\bullet(U, M)$ by restricting the G–cocycle to H.

Proposition 2.4. *We have $trf_{G/U} \circ res_{G/U}(x) = [G : U]x$. In particular, we have*

1. *If M is finite and $|G|$ and $|M|$ are mutually prime, them $H^q(G, M) = 0$ for $q > 0$.*
2. *If $res_{G/U}(x) = 0$ for p-Sylow subgroups U for each prime factor p of $|G|$, then $x = 0$ in $H^q(G, M)$ ($q > 0$).*

Proof. The identity that $trf_{G/U} \circ res_{G/U}(x) = [G : U]x$ follows easily from the fact that $\theta \circ res$ is the scalar multiplication by $[G : U]$. We write $g = |G| = \prod_p p^{e(p)}$. Then for $g^{(p)} = g/p^{e(p)}$, $g^{(p)}x = trf_{G/U} \circ res_{G/U}(x) = 0$ for a p–Sylow subgroup U. Since the greatest common divisor of $\{g^{(p)}\}_p$ is 1, we can find integers m_p such that $\sum_p m_p g^{(p)} = 1$, and hence $x = \sum_p m_p g^{(p)} x = 0$, which shows (2). As for (1), take U to be the trivial subgroup made of the identity. Then the multiplication by $|G|$ is an automorphism on cocycles, since $|G|$ is prime to $|M|$. The cohomology of trivial group vanishes for positive degree, because $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$ is a projective resolution of $\mathbb{Z}$. Thus $res_{G/U}(x) = 0$, and hence $0 = trf_{G/U} \circ res_{G/U}(x) = |G|x$ implies $x = 0$. This shows (1). □

Exercises.

(1) Give a detailed proof of (2.1).
(2) For any A–module M, show $M \otimes_A A \cong M$ canonically.
(3) For any $\mathbb{Z}[G]$–free module X and any $A[G]$–module M, show

$$\mathrm{Hom}_{\mathbb{Z}[G]}(X, M) \otimes_A A = \mathrm{Hom}_{A[G]}(X \otimes_{\mathbb{Z}} A, M).$$

(4) Define $\varphi^\bullet : A^\bullet \to \underline{A}^\bullet$ and $\psi^\bullet : \underline{A}^\bullet \to A^\bullet$ by

$$\varphi_n((g_1, \dots, g_n)) = [g_1, g_1^{-1}g_2, \dots, g_{n-1}^{-1}g_n]$$

and

$$\psi_n([g_1, \dots, g_n]) = (g_1, g_1g_2, \dots, g_1g_2\cdots g_n).$$

Show that they are chain maps, $\varphi^\bullet \circ \psi^\bullet = \mathrm{id}_{\underline{A}^\bullet}$ and $\psi^\bullet \circ \varphi^\bullet = \mathrm{id}_{A^\bullet}$.
(5) Prove (2.4).

2.2. **Tate cohomology groups.** Now we would like to define the Tate cohomology group for finite G, which is a modification of the usual cohomology groups but allows negative degree. We choose a $\mathbb{Z}[G]$–free (so projective) resolution $(C^\bullet, \partial) \xrightarrow{\mathbf{e}} \mathbb{Z}$. For example $C^\bullet = \mathbb{Z}^\bullet$ satisfies this condition. We suppose that C_n is free of finite rank over $\mathbb{Z}[G]$ (and hence is free of finite rank over $\mathbb{Z}$). We write $\widehat{C}_n = \mathrm{Hom}_{\mathbb{Z}}(C_n, \mathbb{Z})$ and make it into a G–module by $g\phi(x) = \phi(g^{-1}x)$. Since C_n is $\mathbb{Z}[G]$–free, take a base $u_1, \dots, u_r$ over $\mathbb{Z}[G]$. Then $\{gu_j | g \in G\}$ is a $\mathbb{Z}$–base of C_n. We take the dual base $\widehat{gu}_j$ of $\widehat{C}_n$ so that $\widehat{gu_i}(hu_j)$ is 1 or 0 according as $g = h$, $i = j$ or not. This shows that $\widehat{C}_n$ is $\mathbb{Z}[G]$–free of finite rank. We have the transpose $\partial_p^t : \widehat{C}_{p-1} \to \widehat{C}_p$ of the differential $\partial_p : C_p \to C_{p-1}$. We now connect $(C^\bullet, \partial) \xrightarrow{\mathbf{e}} \mathbb{Z} \xrightarrow{{}^t\mathbf{e}} (\widehat{C}^\bullet, \partial^t)$ as follows: Define

$$(\widetilde{C}_p, \delta_p) = \begin{cases} (C_p, \partial_p) & \text{if } p > 0 \\ (C_0, {}^t\mathbf{e} \circ \mathbf{e}) & \text{if } p = 0 \\ (\widehat{C}_{p+1}, \partial^t_{-p}) & \text{if } p < 0. \end{cases}$$

It is easy to check that $(\widetilde{C}^\bullet, \delta)$ gives a long exact sequence of $\mathbb{Z}[G]$–free modules (Exercise 1). We then define

$$H_T^\bullet(G, M) = H^\bullet((\mathrm{Hom}_{\mathbb{Z}[G]^\bullet}(\widetilde{C}^\bullet, M), \delta^*)). \tag{2.7}$$

The above cohomology group is independent of the choice of the free resolution by the argument (based on $\mathbb{Z}[G]$–projectivity of $\widetilde{C}_n$ for all n) given in the previous section.

Theorem 2.5. *We have*

$$H_T^q(G, M) = \begin{cases} H^q(G, M) & \textit{if } q > 0 \\ M^G/N_G M & \textit{if } q = 0 \\ \mathrm{Ker}(N_G)/D_G M & \textit{if } q = -1, \end{cases}$$

where the norm map $N_G : M \to M$ is given by $N_G(m) = \sum_{g\in G} gm$ and $D_G M = \sum_{g\in G}(g-1)M$. Moreover $H_T^{-2}(G,\mathbb{Z}) = G^{ab}$, where G^{ab} is the maximal abelian quotient of G.

Proof. The assertion for $q > 0$ follows from the definition, because $(\widetilde{C}_n, \delta_n) = (C_n, \partial_n)$ for $n > 0$. Since $C_1 \xrightarrow{\partial_0} C_0 \xrightarrow{\mathbf{e}} \mathbb{Z} \to 0$ is exact, we have another exact sequence:

$$\widetilde{C}_{-2} \xleftarrow{\delta_{-2}} \widetilde{C}_{-1} \xleftarrow{{}^t\mathbf{e}} \mathbb{Z} \leftarrow 0.$$

Note that $M \otimes_{\mathbb{Z}[G]} C_n \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\widehat{C}_n, M)$ by $\nu : m\otimes c \mapsto (\phi \mapsto \sum_{g\in G}\phi(gc)gm)$ for $\phi \in \widehat{C}_n = \mathrm{Hom}_{\mathbb{Z}}(C_n,\mathbb{Z})$ (Exercise 2). Then we have the following commutative diagram:

$$\begin{tikzcd} {} \arrow[r, "\delta_{-2}"] & \mathrm{Hom}_{\mathbb{Z}[G]}(\widehat{C}_0, M) \arrow[r, "{}^t\mathbf{e}^*"] & \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \arrow[r, "\mathbf{e}^*"] & \mathrm{Hom}_{\mathbb{Z}[G]}(C_0, M) \arrow[r, "\delta_0"] & {} \\
{} \arrow[r, "\mathrm{id}\otimes\partial_1"] & M \otimes_{\mathbb{Z}[G]} C_0 \arrow[u, "\wr"] \arrow[r, "\mathrm{id}\otimes\mathbf{e}"'] & M \otimes_{\mathbb{Z}[G]} \mathbb{Z} \arrow[u, "\nu"] \arrow[r] & 0, \arrow[u, "0"'] & \end{tikzcd}$$

where the lower sequence is exact and $\nu(m\otimes n) = \sum_{g\in G} ngm$ is the one defined above. Note that $M\otimes_{\mathbb{Z}[G]}\mathbb{Z} = M/D_G M$ and $\mathrm{Hom}_{Z[G]}(\mathbb{Z}, M) = M^G$. This shows that $H_T^0(G,M) = M^G/N_G M$ and $H_T^{-1}(G,M) = \mathrm{Ker}(N_G)/D_G M$. To compute $H_T^{-2}(G,M)$, we use inhomogeneous standard projective resolution $\underline{\mathbb{Z}}^\bullet \twoheadrightarrow \mathbb{Z}$. Note that $\mathrm{id}\otimes\partial_0(m\otimes g) = (g-1)m$. Thus if $M = \mathbb{Z}$, $\mathrm{id}\otimes\partial_0$ is the zero map. Then

$$H_T^{-2}(G,\mathbb{Z}) = \frac{\mathrm{Ker}(\mathrm{id}\otimes\partial_0 : \mathbb{Z}\otimes_{\mathbb{Z}[G]}\mathbb{Z}[G^2] \to \mathbb{Z})}{\langle [g]-[hg]+[h]\rangle_{g,h\in G}} = \frac{\mathbb{Z}[G]}{\langle [g]-[hg]+[h]\rangle} \cong G^{ab}$$

by $\sum_{g\in G} n_g[g] \mapsto \prod_{g\in G} g^{n_g} \mod (G,G)$, because $[g]-[hg]+[h]$ is sent to the commutator (g,h) by this map. □

Since the Tate cohomology is computed by using any free (finite rank) resolution, when G is cyclic, we can take the special resolution in Proposition 2.3. Then one verifies that Proposition 2.3 is still valid for $H_T^q(G,M)$ (including negative q) in place of $H^q(G,M)$.

Theorem 2.6. *Let M be a G–module for a finite group G. Suppose that there exists an index $k \in \mathbb{Z}$ such that $H_T^k(U,M) = H_T^{k+1}(U,M) = 0$ for all subgroups U of G. Then $H_T^q(U,M) = 0$ for all subgroups U and q.*

Proof. First suppose that $k = 1$. By Proposition 2.4, we may assume that G has a prime power order. Thus G is a nilpotent group. We have a proper normal subgroup H of G such that G/H is cyclic. We proceed by induction of the order of G. By assumption, $H^q(H,M) = 0$ for $q = 1,2$. We have the restriction-inflation exact sequence (Theorem 2.15):

$$0 \to H^q(G/H, M^H) \to H^q(G,M) \to H^q(H,M)$$

for $q = 1,2$. By induction of the order of G, the vanishing of H^q $(q = 1,2)$ for subgroups of G is equivalent to that for subgroups of the cyclic G/H. Thus we may assume that G is cyclic. Then the assertion for $q = 1, 2$ follows from Proposition 2.3. To treat the general case, take an injective presentation $M \hookrightarrow I \twoheadrightarrow S$ of $\mathbb{Z}[G]$–modules. As we will see later, we may assume that I is $\mathbb{Z}[U]$–injective for all U. Then by long exact sequence and the vanishing $H^q(U, I) = 0$ for all $q > 0$, we have $H^{q-1}(U, S) \cong H^q(U, M)$. Thus we can bring the higher "q" case down to $q = 1, 2$ replacing M by S. This shows the case $k > 0$. We can instead use the projective presentation: $T \hookrightarrow P \twoheadrightarrow M$. Then $H^q_T(U, M) \cong H^{q+1}_T(U, T)$. Since the Tate cohomology is defined by using projective resolution, this shift of degree is valid for all degree q including negative ones. By this, again we can bring the "$q \leq 0$" case into the "$q = 1, 2$" case. □

Theorem 2.7 (J. Tate). *Suppose that G is a finite group. If for a G–module C and for all subgroups U of G,*

(1) $H^1(U, C) = 0$ *and*
(2) $H^2(U, C)$ *is a cyclic group of order* $|U|$,

then for all subgroup U of G, $H^k(U, \mathbb{Z}) \cong H^{k+2}(U, C)$ for all $k > 0$.

Actually, this theorem can be generalized to torsion-free G–module M under the assumption of the theorem as follows:

$$H^k(U, M) \cong H^{k+2}(U, M \otimes_{\mathbb{Z}} C)$$

for all $k > 0$. For the proof of this generalized version, see [CLC] IX.8.

Proof. We first assume, shifting the degree by 1, that $H^0_T(U, M) = 0$ for all subgroup U of G and $H^1(U, M)$ is a cyclic group of order $|U|$. Let $z \in H^1(G, M) = \mathrm{Ext}^1_{\mathbb{Z}[G]}(\mathbb{Z}, M)$ be a generator. Thus we have the corresponding extension: $M \hookrightarrow \overline{M} \twoheadrightarrow \mathbb{Z}$ of $\mathbb{Z}[G]$–modules. The associated long exact sequence is: $\cdots \to H^0_T(U, M) \to H^0_T(U, \overline{M}) \to H^0_T(U, \mathbb{Z}) \to \cdots$. Note that $H^0_T(U, \mathbb{Z}) = \mathbb{Z}/|U|\mathbb{Z}$. We write its generator as 1_U. By the definition of $\overline{M}$, $\delta(1_U) = z_U$ is a generator of $H^1(U, M)$. Thus the connecting map $\delta : H^0_T(U, \mathbb{Z}) \to H^1(U, M)$ is an isomorphism. Since $H^1(U, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(U, \mathbb{Z}) = 0$ because $|U| < \infty$, we have $H^1(U, \overline{M}) = H^0_T(U, \overline{M}) = 0$. This shows, by the theorem just before this one, that $H^q_T(U, \overline{M}) = 0$ for all q. Thus $H^k(U, \mathbb{Z}) \cong H^{k+1}(U, M)$.

To prove the theorem, we take an injective presentation $C \hookrightarrow I \twoheadrightarrow S$. We may assume that I remains $\mathbb{Z}[U]$–injective. Since $H^q_T(U, I) = \mathrm{Ext}^q_{\mathbb{Z}[U]}(\mathbb{Z}, I) = 0$, by the cohomology exact sequence: $H^q_T(U, S) \cong H^{q+1}(U, C)$. Thus by the assumption, $H^0_T(U, S) = 0$ for all subgroup $U \subset G$, and $H^1(U, S)$ is cyclic of order $|U|$. Applying the above argument to $M = S$, we get

$$H^k(U, \mathbb{Z}) \cong H^{k+1}(U, S) \cong H^{k+2}(U, C),$$

which is what we wanted. □

Exercises.

(1) Prove $\widetilde{C}_{n-1} \xrightarrow{\delta_{n-1}} \widetilde{C}_n \xrightarrow{\delta_n} \widetilde{C}_{n+1}$ is exact for all $n \in \mathbb{Z}$ if $(C^\bullet, \partial) \twoheadrightarrow \mathbb{Z}$ is a $\mathbb{Z}[G]$–free resolution such that $\mathrm{rank}_{\mathbb{Z}} C_n < \infty$ for all $n \geq 0$.

(2) Show that $M \otimes_{\mathbb{Z}[G]} C_n \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\widehat{C}_n, M)$ by $\nu : m \otimes c \mapsto (\phi \mapsto \sum_{g \in G} \phi(gc)gm)$ for $\phi \in \widehat{C}_n = \mathrm{Hom}_{\mathbb{Z}}(C_n, \mathbb{Z})$.

2.3. **Continuous cohomology for profinite groups.** We fix a profinite group G. Let $\mathcal{C}$ be the category of discrete G–modules. Discrete G–modules M means that M has a discrete topology and that it has a continuous action of G. The morphisms of the category $\mathcal{C}$ are homomorphisms of $\mathbb{Z}[G]$–modules, because continuity under discrete topology does not impose any restrictions. Thus $\mathrm{Coker}(f)$ and $\mathrm{Ker}(f)$ for a morphism $f : M \to N$ in $\mathcal{C}$ are again objects in $\mathcal{C}$ (see Exercise 1). Therefore $\mathcal{C}$ is an abelian category.

Let $\mathcal{U}$ be the system of neighborhoods of $1 \in G$ made of normal open subgroups. Then it is easy to check:

$$M \text{ is a discrete } G\text{–module} \iff M = \bigcup_{U \in \mathcal{U}} M^U, \tag{2.8}$$

where $M^U = \{m \in M | gm = m \ \forall g \in U\}$. From this, $A[G]$ is not an object of $\mathcal{C}$ (see Exercise 3) if G is infinite, hence there is no $A[G]$–free modules in $\mathcal{C}$ if G is infinite. This shows basically no $A[G]$–projective modules in $\mathcal{C}$. However, for the space $C(G/U, I)$ of all functions $\phi : G/U \to I$, $I_G = \bigcup_{U \in \mathcal{U}} C(G/U, I)$ for any injective $\mathbb{Z}$–module I is actually $\mathcal{C}$–injective (see Proposition 2.8). Here we let G act on I_G by $g\phi(h) = \phi(hg)$. In this way, one can prove that $\mathcal{C}$ has enough injectives (see Proposition 2.8). We define $H^q_{\mathcal{C}}(G, M) = \mathrm{Ext}^q_{\mathcal{C}}(\mathbb{Z}, M)$. By definition,

$$H^0_{\mathcal{C}}(G, M) = \mathrm{Ext}^0_{\mathcal{C}}(\mathbb{Z}, M) = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \cong M^G \tag{2.9}$$

by $\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M) \ni \phi \mapsto \phi(1) \in M^G$.

The above fact (2.9) and (1.4) tell us that for a $\mathcal{C}$–injective resolution $M \hookrightarrow (M^\bullet, \partial)$,

$$H^\bullet(G, M) = H^\bullet(H^0(G, M^\bullet), \partial). \tag{2.10}$$

Since each member M_j of $M^\bullet$ is an object of $\mathcal{C}$, for open normal subgroups $U \subset G$, $M^\bullet = \bigcup_{U \in \mathcal{U}} (M^\bullet)^U$.

Let I be a $\mathcal{C}$–injective module. Then for each G/U–modules $M \subset N$, regarding them as G–modules via the projection: $G \to G/U$, any $\mathcal{C}$–morphism $i : M \to I$ can be extended to a $\mathcal{C}$–morphism $j : N \to I$. Since $j(n) = j(un) = uj(n)$ for $\forall n \in N$ and $\forall u \in U$, j has values in I^U. Similarly i has values in I^U. Thus we have found that any morphism $i : M \to I^U$ can be extended to $j : N \to I^U$. Thus we have

$$I^U \text{ is } \mathbb{Z}[G/U]\text{–injective if } I \text{ is } \mathcal{C}\text{–injective.} \tag{2.11}$$

Now start from an injective system $(I_U, \iota_{U,V} : I_U \to I_V)_{U,V \in \mathcal{U}}$ of $\mathbb{Z}[G/U]$–injective modules I_U. Then we claim

$$I = \varinjlim_{U \in \mathcal{U}} I_U \text{ is } \mathcal{C}\text{–injective if the maps } \iota_{U,V} \text{ are all injective.} \tag{2.12}$$

Let us prove this: Let $M \subset N$ be an inclusion in $\mathcal{C}$ with a $\mathcal{C}$–morphism $\alpha : M \to I$. Then $M^U \subset N^U$ and $\alpha_U : M^U \to I$. First suppose that M^U is finitely generated as a $\mathbb{Z}[G]$–module. Then $\mathrm{Im}(\alpha_U) \subset I_{V(U)}$ for sufficiently small $V = V(U) \in \mathcal{U}$. We may assume that $V(U) \subset U$. Then by the $\mathbb{Z}[G/V]$–injectivity of I_V, α_U extends to $\beta_U : N^U \to I_V$. If $U' \subset U$, we have the corresponding $V' = V(U') \subset V = V(U)$ as above. Then the following diagram is commutative:

$$\begin{tikzcd}
N^U \arrow[r, "\subset"] & N^{U'} \arrow[r, "\beta_{U'}"] & I_{V'} \\
M^U \arrow[u, "\cup"] \arrow[r, "\subset"'] & M^{U'} \arrow[u, "\cup"] \arrow[r, "\alpha_{U'}"] & I_{V'}. \arrow[u, "\|"']
\end{tikzcd}$$

Applying above argument to $N^{U'}$, we may assume that $\beta_U : N^U \to I_{V(U)}$ satisfies $\iota_{V(U),V(U')}\beta_U = \beta_{U'}$. Then taking an injective limit of β_U, we get an extension $\beta : N \to I$ of α. In general, the module M can be written as a union of $M = \bigcup_j M_j$ such that M_j^U is a $\mathbb{Z}[G/U]$–module of finite type. Then first we apply the above argument to each M_j, and then taking the limit of extensions of α to N, we can extend α to N. This shows the claim. □

Let J be a $\mathbb{Z}$–module and Λ be a ring (possibly non-commutative). Write ? for an indeterminate object in Λ–MOD. Then we have an isomorphism of functors $\eta_? : \mathrm{Hom}_\Lambda(?, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, J)) \to \mathrm{Hom}_{\mathbb{Z}}(?, J)$ given by $\eta_A(\varphi)(a) = \varphi(a)(1)$ (Exercise 4). Suppose that J is $\mathbb{Z}$–injective (any divisible module is $\mathbb{Z}$–injective). We would like to prove that $I = \mathrm{Hom}_{\mathbb{Z}}(\Lambda, J)$ is Λ–injective, where $\lambda \in \Lambda$ acts on $\phi : \Lambda \to J$ by $\lambda\phi(x) = \phi(x\lambda)$. Let $M \subset N$ be Λ–modules. For all $\alpha : M \to I$, $\alpha \in \mathrm{Hom}_\Lambda(M, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, J)) \cong \mathrm{Hom}_{\mathbb{Z}}(M, J)$. By the $\mathbb{Z}$–injectivity, we can extend $\eta_M(\alpha) : M \to J$ to $\beta' : N \to J$. Then for β such that $\eta_N(\beta) = \beta'$, $\beta : N \to I$ is an extension of α.

We take $J = \mathbb{Q}/\mathbb{Z}$. Then any cyclic $\mathbb{Z}$–module $\langle a \rangle$ generated by a has a homomorphism $\phi_a : \langle a \rangle \to J$ such that $\phi_a(a) \neq 0$. For example, if the order of a is an integer N, we just define $\phi(ma) = \frac{m}{N} \mod \mathbb{Z}$. If the order of a is infinite, we just take any $x \neq 0$ in J and put $\phi(ma) = mx$. For any given Λ–module M and $m \in M$, we have a non-zero map $\phi_m : \langle m \rangle \to J$, which extends to a linear map $\Phi_m : M \to J$ by the $\mathbb{Z}$–injectivity of J. Then $\eta_M^{-1}(\Phi_m) = \varphi_m : M \to I$ is a Λ–linear map with $\varphi_m(m) \neq 0$. We define $\iota_M : M \to I_M = \prod_{0 \neq m \in M} I_m$ by $\iota_M(x) = \prod_m \varphi_m(x)$, where $I_m = I$. Obviously the product $\prod_{0 \neq m \in M} I_m$ is an injective module, and hence we get an injective presentation of M in Λ–MOD.

Proposition 2.8. *The category Λ–MOD has enough injectives.*

Let $M \in \mathcal{C}$. We apply the above argument to $\Lambda_U = \mathbb{Z}[G/U]$ for M^U. We have an injective presentation of Λ_U–module

$$0 \to M^U \hookrightarrow I_{M^U} = \prod_{m \in M - \{0\}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], J).$$

If $V \subset U$, then we have a projection $\pi_{V,U} : G/V \to G/U$ which induces a ring homomorphism $\pi_{V,U} : \mathbb{Z}[G/V] \to \mathbb{Z}[G/U]$, which is a surjection. Then by pull-back, we have an inclusion $i_{U,V} = \pi_{V,U}^* : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], J) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/V], J)$, which is an injection. Then we can define $\iota_{U,V} : I_{M^U} \hookrightarrow I_{M^V}$ so that $\iota_{U,V}$ coincides with $i_{U,V}$ on the component $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], J)$ indexed by $m \in M^U$ and outside such components, the map is just a zero map. Plainly, we have a commutative diagram:

$$\begin{tikzcd} M^U \arrow[r] \arrow[d] & I_{M^U} \arrow[d] \\ M^V \arrow[r] & I_{M^V}. \end{tikzcd}$$

Taking the injective limit with respect to $U \in \mathcal{U}$, we get an injective presentation:

$$\iota_M = \varinjlim_U \iota_{M^U} : M \hookrightarrow \varinjlim_U I_{M^U} = I_M.$$

We note here that the above module I_M is divisible by definition.

Corollary 2.9. *The category of discrete G–modules $\mathcal{C}$ has enough injectives. Moreover, for each object $M \in \mathcal{C}$, we have an injective resolution $M \hookrightarrow M^\bullet$ such that $M^\bullet$ is divisible and is given by $\bigcup_{U\in\mathcal{U}} M^\bullet_U$ for an injective resolution $M^\bullet_U$ of M^U in $\mathbb{Z}[G/U]$–MOD. In particular, this shows*

$$H^\bullet_{\mathcal{C}}(G, M) \cong \varinjlim_{U\in\mathcal{U}} H^\bullet(G/U, M^U) \cong H^\bullet_{ct}(G, M).$$

Proof. We first prove the first identity. Pick $\mathbb{Z}[G/U]$–injective resolution $M^U \hookrightarrow I^\bullet_U$ of M^U for each $U \in \mathcal{U}$. If $V \subset U$, we have a lift $i^\bullet_{U,V} : I^\bullet_U \to I^\bullet_V$ of the inclusion: $M^U \hookrightarrow M^V$, which is unique modulo homotopy equivalence. Thus $i^\bullet_{U,V}$ induces a unique map of cohomology groups, called the *inflation map* $inf_{U/V} : H^\bullet(G/U, M^U) \to H^\bullet(G/V, M^V)$ independently of the resolution. Thus $\varinjlim_{U\in\mathcal{U}} H^\bullet(G/U, M^U)$ is well defined. In particular, the explicit resolution constructed just above the corollary, we call it the standard injective resolution, identifies it with $H^\bullet_{\mathcal{C}}(G, M)$.

At finite group level, we can compute $H^\bullet(G/U, M^U)$ by using the inhomogeneous standard projective resolution of $\underline{\mathbb{Z}}^\bullet_U$ in $\mathbb{Z}[G/U]$–MOD. Again for $V \subset U$, the projection $G/V \twoheadrightarrow G/U$ induces a surjection $\underline{\mathbb{Z}}^\bullet_V \twoheadrightarrow \underline{\mathbb{Z}}^\bullet_U$. This shows the injective system $(H^\bullet(G/U, M^U))_{U\in\mathcal{U}}$ induced by this projection of the projective resolutions coincides with that induced by the standard injective resolutions. For any continuous map $\phi : G^n \to M$, $G^n = \bigcup_{m\in M} \phi^{-1}(m)$. Since M is discrete, $\phi^{-1}(m)$ is an open set. By the compactness of G^n, there is finitely many $m_i \in M$ such that $G^n = \bigcup_{m_i} \phi^{-1}(m_i)$. Thus ϕ is locally constant, and therefore, there exists a small $U \in \mathcal{U}$ such that ϕ factors through $(G/U)^n$. Thus any continuous cocycle or coboundary can be regarded as a cocycle or coboundary of G/U for sufficiently small U. This shows that $H^\bullet_{ct}(G, M) = \varinjlim_{U\in\mathcal{U}} H^\bullet(G/U, M)$. □

Corollary 2.10. *Let G be a profinite group topologically generated by an element g of infinite order. Let M be a torsion discrete G–module. Then we have $H^2_{ct}(G, M) = 0$.*

Proof. By the assumption, $G = \varprojlim_n G_n$ for cyclic groups G_n with $|G_n| \to \infty$ as $n \to \infty$. Let K_n be the kernel of the projection $G \twoheadrightarrow G_n$. By Proposition 2.3, we have $H^2(G_n, M) \cong M^{G_n}/N_{G_n}M$. We can check easily from the proof of Proposition 2.3, for $m > n$,

$$inf_{m,n} : H^2(G_n, M^{K_n}) = M^G/N_{G_n}M^{K_n} \to M^G/N_{G_m}M^{K_m} = H^2(G_m, M^{K_m})$$

is induced by the norm map given by $N_{K_n/K_m}(x) = \sum_{\gamma \in K_n/K_m} \gamma x = (K_n : K_m)x$ for $x \in M^G$. Since G is torsion-free, if a prime p divides $|G_n|$ for some n, then for any given $N > 0$, we can find $M \gg 0$ such that $p^N | (K_n : K_M)$. This shows that for a given n and $x \in M^G$, $N_{K_n/K_m}(x) = 0$ for sufficiently large $m > n$, since M is a torsion module. Thus $H^2_{ct}(G, M) = \varinjlim_n H^2(G_n, M^{K_n}) = 0$. □

We have from Proposition 1.9

Corollary 2.11. *Let $0 \to M \to N \to L \to 0$ be an exact sequence of discrete G–modules. Then we have a long exact sequence:*

$$\begin{aligned} &H^q_{ct}(G, M) \to H^q_{ct}(G, N) \to H^q_{ct}(G, L) \\ &\qquad\qquad\qquad \xrightarrow{\delta} H^{q+1}_{ct}(G, M) \to H^{q+1}_{ct}(G, N) \to H^{q+1}_{ct}(G, L). \end{aligned}$$

Remark 2.2. Corollary 2.9 shows

$$\mathrm{Ext}^\bullet_{\mathcal{C}}(\mathbb{Z}, M) = H^\bullet_{\mathcal{C}}(G, M) \cong \varinjlim_{U \in \mathcal{U}} H^\bullet(G/U, M^U) = \varinjlim_{U \in \mathcal{U}} \mathrm{Ext}^\bullet_{\mathbb{Z}[G/U]}(\mathbb{Z}, M^U).$$

The exactly the same argument gives a slightly general result:

$$\mathrm{Ext}_{\mathcal{C}}(N, M) \cong \varinjlim_{U \in \mathcal{U}} \mathrm{Ext}_{\mathbb{Z}[G/U]}(N, M^U)$$

for any discrete G–module N of finite type. Here U runs over all open normal subgroups of G fixing N element by element. Since N is of finite type, there exists an open normal subgroup of G fixing N.

For open subgroups $V \subset U$ of G, we can think of the category of discrete U–modules $\mathcal{C}_U$. Each U–module M can be regarded naturally a V–module. Let $M \hookrightarrow M^\bullet_V$ be a $\mathcal{C}_V$–injective resolution. We have a lift $i^\bullet : M^\bullet_U \to M^\bullet_V$ of the identity $\mathrm{id} : M \to M$, which is unique up to homotopy. The induced map of cohomology group $H^\bullet(\mathrm{id}) : H^\bullet_{ct}(U, M) \to H^\bullet_{ct}(V, M)$ is called the restriction map and written as $res_{U/V}$. As usual, $res_{U/V}$ does not depends on the choice of the resolution, coincides with the restriction map defined in the previous subsection and satisfies $res_{V/W} \circ res_{U/V} = res_{U/W}$ (Exercise 5).

If M and N are G–modules, then $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ is again a G–module by $g\phi(m) = g\phi(g^{-1}m)$. Then by definition, $\mathrm{Hom}_{\mathbb{Z}}(M, N)^G = \mathrm{Hom}_{\mathbb{Z}[G]}(M, N)$. Even if $M, N \in \mathcal{C}$, $\mathrm{Hom}(M, N)$ may not be in $\mathcal{C}$. We remedy this by definining

$$Hom(M, N) = \bigcup_{U \in \mathcal{U}} \mathrm{Hom}_{\mathbb{Z}}(M, N)^U,$$

which is a discrete G–module by (2.8). When M is finitely generated over $\mathbb{Z}$, then the image of its generator under $\phi \in \mathrm{Hom}_{\mathbb{Z}}(M, N)$ falls in N^U for some small $U \in \mathcal{U}$. Therefore in this case, $Hom(M, N) = \mathrm{Hom}_{\mathbb{Z}}(M, N)$.

Proposition 2.12. *Let $\langle\ ,\ \rangle : M\times N \to P$ be a bilinear pairing of discrete G–modules. Suppose that $\langle gm, gn\rangle = g\langle m, n\rangle$ for all $g \in G$ and that N is finitely generated as a $\mathbb{Z}[G]$–module. There are canonical morphisms:*

$$H^r_{ct}(G, M) \to H^r_{ct}(G, Hom(N, P)) \to \mathrm{Ext}^r_{\mathcal{C}}(N, P).$$

If one of the following three conditions is satisfied:

(1) *N is $\mathbb{Z}$–free of finite rank;*
(2) *P is divisible;*
(3) *P is a p–divisible (discrete) $\mathbb{Z}_p[G]$–module for a prime p,*

then

$$H^r_{ct}(G, Hom(N, P)) \cong \mathrm{Ext}^r_{\mathcal{C}}(N, P).$$

Proof. The first morphism is induced by the natural map: $M \to \mathrm{Hom}(N, P)$ which is in turn induced by the pairing. To see the second, we first assume that N is $\mathbb{Z}$–free of finite rank. For any $\mathcal{C}$–injective I, we claim that $Hom(N, I)$ is $\mathcal{C}$–injective, as long as N is $\mathbb{Z}$–free of finite rank. By our assumption on N, we have $\mathrm{Hom}_{\mathbb{Z}}(N, I) = Hom(N, I)$. We have a canonical isomorphism (Exercise 4):

$$\mathrm{Hom}_{\mathbb{Z}[G]}(M, Hom(N, I)) \cong \mathrm{Hom}_{\mathbb{Z}[G]}(M \otimes_{\mathbb{Z}} N, I).$$

Since N is torsion-free, it is $\mathbb{Z}$–flat, and hence $M \mapsto M\otimes_{\mathbb{Z}} N$ preserves exact sequence. Note that I is $\mathcal{C}$–injective if and only if $M \mapsto \mathrm{Hom}_{\mathbb{Z}[G]}(M, I) = \mathrm{Hom}_{\mathcal{C}}(M, I)$ preserves exact sequences. Thus the composite functor

$$M \mapsto M \otimes_{\mathbb{Z}} N \mapsto \mathrm{Hom}_{\mathcal{C}}(M \otimes_{\mathbb{Z}} N, I) = \mathrm{Hom}_{\mathbb{Z}[G]}(M, Hom(N, I))$$

preserves exact sequence. This shows that $Hom(N, I)$ is $\mathcal{C}$–injective, as long as N is $\mathbb{Z}$–free of finite rank.

We continue to assume that N is $\mathbb{Z}$–free of finite rank. Thus we may assume $N \cong \mathbb{Z}^n$. Then $Hom(N, I) = I^n$. Thus for an injective resolution $P \hookrightarrow P^\bullet$, $Hom(N, P^\bullet) \cong (P^\bullet)^n$ and hence $Hom(N, P) \hookrightarrow Hom(N, P^\bullet)$ is an injective resolution of $Hom(N, P)$. We choose another $\mathcal{C}$–injective resolution: $Hom(N, P) \hookrightarrow Hom(N, P)^\bullet$, which could be different from $Hom(N, P^\bullet)$. Since P_j is $\mathcal{C}$–injective, $Hom(N, P_j)$ is $\mathcal{C}$–injective. Thus we have lifts

$$i^\bullet : Hom(N, P)^\bullet \to Hom(N, P^\bullet) \quad\text{and}\quad j^\bullet : Hom(N, P^\bullet) \to Hom(N, P)^\bullet$$

of $\mathrm{id} : Hom(N, P) \to Hom(N, P)$, which are unique up to homotopy and are mutually an inverse of each other. Then we have

$$\begin{aligned} H^\bullet(i) : H^\bullet(G, Hom(N, P)) &= H^\bullet(\mathrm{Hom}_{\mathcal{C}}(\mathbb{Z}, Hom(N, P^\bullet))) \\ &\cong H^\bullet(Hom_{\mathcal{C}}(N, P^\bullet)) = \mathrm{Ext}^\bullet_{\mathcal{C}}(N, P), \end{aligned}$$

which is the desired isomorphism.

For a general N, to create the desired map: $H^q_{ct}(G, Hom(N, P)) \to \mathrm{Ext}^q_{\mathcal{C}}(N, P)$, we need to study double complexes, which yield an appropriate spectral sequence giving rise to the map (see [ADT] 0.3). Here we avoid the use of the spectral sequence, and we instead consider the category $\mathcal{C}^\bullet$ of complexes made of objects in $\mathcal{C}$. Since $\mathcal{C}$ is an abelian category with enough injectives, so is $\mathcal{C}^\bullet$. For any object X in $\mathcal{C}$, we take a $\mathcal{C}^\bullet$–injective resolution $Hom(X,P^\bullet)^\bullet$ of the complex $Hom(X,P^\bullet)$ in $\mathcal{C}^\bullet$: Write ∂ for the differential of $Hom(X,P^\bullet)^\bullet$ coming from inner $P^\bullet$ and δ for the outer one. We then define a new complex $HOM(X,P)^\bullet$ by putting $HOM(X,P)_\ell = \bigoplus_{j+k=\ell} Hom(X,P_j)_k$. The new differential Δ_ℓ is given by $\delta_k + (-1)^k\partial_j$ on $Hom(X,P_j)_k$. It is easy to check that $\Delta \circ \Delta = 0$. Then the projection $p : HOM(X,P)^\bullet = Hom(X,P^\bullet)^\bullet \twoheadrightarrow Hom(X,P^\bullet)$ is a morphism of complexes: $HOM(X,P)^\bullet \to Hom(X,P^\bullet)$ up to sign, and inclusion $i : Hom(X,P)^\bullet \hookrightarrow HOM(X,P)^\bullet$ is also a morphism in $\mathcal{C}^\bullet$. Then the composite $p \circ i$ for $X = N$ is the desired map.

To show the above construction is compatible with the one we gave for $\mathbb{Z}$–free N, we take a presentation $N_1 \hookrightarrow N_0 \twoheadrightarrow N$ of $\mathbb{Z}[G]$–modules with $\mathbb{Z}$–free N_j $(j = 0,1)$ (of finite rank). This is possible if N is of finite type over $\mathbb{Z}[G]$ because generators of N is fixed by an open normal subgroup U. Then we look at the exact sequence in $\mathcal{C}^\bullet$:

$$0 \longrightarrow Hom(N,P^\bullet) \longrightarrow Hom(N_0,P^\bullet) \longrightarrow Hom(N_1,P^\bullet).$$

We take an injective resolution in $\mathcal{C}^\bullet$ of each term of the above sequence so that the following diagram is commutative:

$$\begin{tikzcd}
0 \arrow[r] & Hom(N,P^\bullet)^\bullet \arrow[r] \arrow[d] & Hom(N_0,P^\bullet)^\bullet \arrow[r] \arrow[d] & Hom(N_1,P^\bullet)^\bullet \arrow[d] \\
0 \arrow[r] & Hom(N,P^\bullet) \arrow[r] & Hom(N_0,P^\bullet) \arrow[r] & Hom(N_1,P^\bullet).
\end{tikzcd}$$

The argument in Remark 1.1 applied to $\mathcal{C}^\bullet$ (in place of $\mathcal{C}$ there) shows the existence of such $\mathcal{C}^\bullet$–injective resolutions. Since homotopy equivalence with respect to δ (or ∂) gives rise to that with respect to Δ, we have the following commutative diagram (unique up to homotopy equivalence):

$$\begin{tikzcd}
0 \arrow[r] & Hom(N,P)^\bullet \arrow[r] \arrow[d] & Hom(N_0,P)^\bullet \arrow[r] \arrow[d] & Hom(N_1,P)^\bullet \arrow[d] \\
0 \arrow[r] & HOM(N,P)^\bullet \arrow[r] \arrow[d] & HOM(N_0,P)^\bullet \arrow[r] \arrow[d] & HOM(N_1,P)^\bullet \arrow[d] \\
0 \arrow[r] & Hom(N,P^\bullet) \arrow[r] & Hom(N_0,P^\bullet) \arrow[r] & Hom(N_1,P^\bullet).
\end{tikzcd}$$

Removing the middle sequence, we know that the right two vertical maps are lifts of the identities of $Hom(N_j,P)$. Thus the map at the extreme left is induced by the lifts of the identity for $\mathbb{Z}$–free N_j. Thus our construction is compatible with the one for $\mathbb{Z}$–free G–modules, and the map is unique up to homotopy.

Suppose $0 \to Hom(N,P) \to Hom(N_0,P) \to Hom(N_1,P) \to 0$ is exact. Thus, writing $H^\bullet(X)$ (resp. $E^\bullet(X)$) for $H^\bullet(G, Hom(X,P))$ (resp. $\mathrm{Ext}^\bullet_{\mathcal{C}}(X,P)$), we have a following commutative diagram of long exact sequences:

$$\begin{tikzcd}
H^{r-1}(N_0) \arrow[r] \arrow[d, "\wr"'] & H^{r-1}(N_1) \arrow[r] \arrow[d, "\wr"'] & H^r(N) \arrow[r] \arrow[d] & H^r(N_0) \arrow[r] \arrow[d, "\wr"'] & H^r(N_1) \arrow[d, "\wr"'] \\
E^{r-1}(N_0) \arrow[r] & E^{r-1}(N_1) \arrow[r] & E^r(N) \arrow[r] & E^r(N_0) \arrow[r] & E^r(N_1).
\end{tikzcd}$$

Then by the five lemma (see [BCM] Exercise I.1.4.b), $H^r(G, \mathit{Hom}(N,P))$ is isomorphic to $\mathrm{Ext}^r_{\mathcal{C}}(N,P)$. In particular, under the assumptions (2) or (3), we have the desired isomorphism. □

We record here a by-product of the above proof:

Lemma 2.13. *Let N be a discrete $\mathbb{Z}[G]$–module, which is free of finite rank over $\mathbb{Z}$. Then for a $\mathcal{C}$–injective module I, $\mathit{Hom}(N,I) = \mathit{Hom}_{\mathbb{Z}}(N,I)$ is $\mathcal{C}$–injective, and for an arbitrary discrete $\mathbb{Z}[G]$–module P and its $\mathcal{C}$–injective resolution $P \hookrightarrow P^\bullet$, $\mathit{Hom}(N,P) \hookrightarrow \mathit{Hom}(N,P^\bullet)$ is a $\mathcal{C}$–injective resolution of* $\mathrm{Hom}(N,P) = \mathit{Hom}(N,P)$*.*

Here is a definition-proposition of the cup-product pairing:

Corollary 2.14. *Let the notation and the assumption be as in the proposition. Then we have a pairing*

$$\langle\ ,\ \rangle : H^r_{ct}(G,M) \times H^s_{ct}(G,N) \to H^{r+s}_{ct}(G,P)$$

induced by the pairing: $M \times N \to P$.

Proof. We consider the following diagram:

$$\begin{tikzcd}
H^r_{ct}(G,M) \arrow[d] & \times & H^s_{ct}(G,N) \arrow[r] \arrow[d, "\wr"'] & H^{r+s}_{ct}(G,P) \arrow[d, "\wr"'] \\
\mathrm{Ext}^r_{\mathcal{C}}(N,P) & \times & \mathrm{Ext}^s_{\mathcal{C}}(\mathbb{Z},N) \arrow[r] & \mathrm{Ext}^{r+s}_{\mathcal{C}}(\mathbb{Z},P).
\end{tikzcd}$$

The bottom row is the extension pairing in Corollary 1.8. Then we define the desired pairing just insisting on making the above diagram commutative. □

The pairing in Corollary 2.14 is called the cup product pairing .

Exercises.

(1) For an exact sequence of $\mathbb{Z}[G]$–modules: $0 \to M \to N \to L \to 0$, if two left (or right) terms of the sequence are in $\mathcal{C}$, show that the remaining term is again in $\mathcal{C}$. Find an example of exact sequence as above with M and L are discrete modules, but N is not discrete (the maps has to be continuous).

(2) Prove (2.8).

(3) Show that $A[G]$ is not in $\mathcal{C}$ if G is infinite.

(4) Define a morphism of functors $\eta_? : \mathrm{Hom}_\Lambda(?, \mathrm{Hom}_{\mathbb{Z}}(\Lambda, J)) \to \mathrm{Hom}_{\mathbb{Z}}(?, J)$ by $\eta_A(\varphi)(a) = \varphi(a)(1)$. Show that this is an isomorphism.

(5) Show that $res_{U/V}$ is independent of the choice of resolutions and $res_{V/W} \circ res_{U/V} = res_{U/W}$.

(6) Suppose that N is $\mathbb{Z}$–free of finite rank. Write down the map of Proposition 2.12: $H^1(G, Hom(N, P)) \to \mathrm{Ext}^1_{\mathcal{C}}(N, P)$ explicitly, associating to an inhomogeneous 1–cocycle $c : G \to Hom(N, P)$ an extension $P \hookrightarrow M \twoheadrightarrow N$ in $\mathcal{C}$.

2.4. **Inflation and restriction sequences.** Let $U \triangleleft G$ be a closed normal subgroup. For an inhomogeneous q–cocycle $u : U^q \to M$ and $g \in G$, ${}^g u : (g_1, \ldots, g_q) \mapsto gu(g^{-1}g_1g, \ldots, g^{-1}g_qg)$ is again a q–cocycle of U, and the cohomology class of ${}^g u$ is equal to that of u if $g \in U$, as easily verified by computation. Thus the quotient group G/U acts on $H^q(U, M)$ by $[u] \mapsto [{}^g u]$. We now prove

Theorem 2.15. *Let $U \triangleleft G$ be a closed normal subgroup, and suppose that $H^q_{ct}(U, M) = 0$ for all $q = 1, 2, \ldots, p-1$. Then the following sequence is exact:*

$$0 \to H^p_{ct}(G/U, M^U) \xrightarrow{inf_{G/U}} H^p_{ct}(G, M) \xrightarrow{res_{G/U}} H^0(G/U, H^p_{ct}(U, M)) \xrightarrow{trans_{G/U}} H^{p+1}_{ct}(G/U, M^U).$$

We shall give a definition of the *transgression* $trans_{G/U}$, due to Hochschild and Serre, in the following proof of the theorem.

Proof. We only prove the theorem for open subgroups U. The general case is left to the reader (who needs to check continuity of cocycles in the proof below applied to a closed subgroup U in place of open U). When $p = 1$, we use the inhomogeneous cochains. Thus for a profinite group X and a discrete X–module N

$$H^1_{ct}(X, N) = \frac{\{c : X \to N : \text{continuous} | c(gh) = gc(h) + c(g)\ \forall g, h \in X\}}{\{g \mapsto (g-1)x | x \in N\}}. \tag{2.13}$$

For the projection $\pi : G \to G/U$, $inf_{G/U}(c) = c \circ \pi$ and $res_{G/U} c = c|_U$. For these two maps, it is easy to show the exactness by a simple computation (Exercise 1).

We now prove the exactness at $H^0(G/U, H^1_{ct}(U, M))$. Let $c : U \to M$ be a cocycle representing a class $[c]$ in $H^0(G/U, H^1_{ct}(U, M))$. Then $gc(g^{-1}ug) - c(u) = (u-1)a(g)$ for a function $a : G \to M$, because $g[c] = [c]$. If $g \in U$, by cocycle relation, we see

$$gc(g^{-1}ug) - c(u) = c(ug) + gc(g^{-1}) - c(u) = uc(g) - c(g) = (u-1)c(g).$$

Thus we may take the function a to be c on U and hence may assume that $a(u) = c(u)$ for all $u \in U$. Then we have

$$ga(g^{-1}ug) - a(u) = (u-1)a(g).$$

Let F be the space of continuous functions $f : U \to M$. Then we make F into a G–module by the following G–action: $gf(u) = gf(g^{-1}ug)$. Note that $(g-1)f(u) = gf(g^{-1}ug) - f(u)$. But $\delta(g \mapsto (g-1)f) = 0$ for the differential $\delta : C_1(G, F) \to C_2(G, F)$ of inhomogeneous cochains, and by applying δ to $ga(g^{-1}ug) - a(u) = (u-1)a(g)$, we have

$$\begin{aligned} 0 &= \delta(x \mapsto (x-1)a(u)) = \delta(x \mapsto (u-1)a(x))(g, h) \\ &= g(g^{-1}ug - 1)a(h) - (u-1)a(gh) + (u-1)a(g) = (u-1)(ga(h) - a(gh) + a(g)). \end{aligned}$$

Now we put $b(g,h) = \delta_1(a)(g,h) = ga(h) - a(gh) + a(g)$. Then the above equation becomes:

$$(u-1)b(g,h) = 0.$$

Thus the 2–cocycle $b : G \times G \to M$ actually has values in M^U.

Note that

$$\begin{aligned}(u-1)(ua(g)+a(u)) &= u(ga(g^{-1}ug) - a(u)) + ua(u) - a(u)\\ &= uga(g^{-1}ug) - a(u) = (u-1)a(ug).\end{aligned}$$

Thus fixing a complete representative set R for $U\backslash G$ so that $1 \in R$, we may normalize a so that $a(ug) = ua(g) + a(u)$ for all $u \in U$ and all $g \in R$. Since $a|_U$ is a 1–cocycle, by computation, we conclude that $a(ug) = ua(g) + a(u)$ for all $u \in U$ and all $g \in G$ (not just in R). Then for all $u \in U$ and $g, h \in G$, we see $b(u,g) = 0$, and 2–cocycle relation is

$$ub(g,h) - b(ug,h) + b(u,gh) - b(u,g) = 0.$$

This shows that $b(g,h) = ub(g,h) = b(ug,h)$. Similarly, we can show $b(g,uh) = b(g,h)$. Thus b factors through G/U.

If $a' : G \to M$ satisfies the same properties as a, that is, $ga'(g^{-1}ug) - a'(u) = (u-1)a'(g)$ and $a' = c$ on U, then

$$(u-1)(a(g) - a'(g)) = ga(g^{-1}ug) - a(u) - (ga'(g^{-1}ug) - a'(u)) = 0,$$

because $a = c = a'$ on U. This shows that $d(g) = a(g) - a'(g) \in M^U$. Then $b - b' = \delta(d) \in \mathrm{Im}(C_1(G/U, M^U) \xrightarrow{\delta} C_2(G/U, M^U))$, and hence we have the identity of the cohomology classes:

$$[b] = [b'] \in H^2(G/U, M^U)$$

for $b' = \delta(a')$. We then define $trans_{G/U}([c])$ by the cohomology class of $[b]$ in $H^2(G/U, M^U)$.

Suppose that $trans_{G/U}([c]) = 0$. Then choosing a 1–cochain $d : G/U \to M^U$ such that $\delta(d) = b$, we see that $a' = a - d$ agrees with c on U and $\delta(a') = 0$; so, a' is a 1–cocycle of G inducing c. This shows

$$\mathrm{Ker}(trans_{G/U}) \supset \mathrm{Im}(res_{G/U}).$$

By definition, if $c \in \mathrm{Im}(res_{G/U})$, we take a to be the 1–cocycle of G restricting c on U. Thus, $\mathrm{Im}(res_{G/U}) \supset \mathrm{Ker}(trans_{G/U})$. This proves the desired exactness for degree 1 cohomology groups.

We now prove the result in general by induction on p. We take a $\mathcal{C}$–injective presentation:

$$0 \to M \to I \to S \to 0.$$

Then by the long exact sequence of cohomology groups, the following sequence:

$$\begin{aligned}H^{p-1}_{\mathcal{C}}(G,M) \to H^{p-1}_{\mathcal{C}}(G,I) \to H^{p-1}_{\mathcal{C}}(G,S)&\\ \to H^{p}_{\mathcal{C}}(G,M) \to H^{p}_{\mathcal{C}}(G,I) \to H^{p}_{\mathcal{C}}(G,S)&\end{aligned}$$

is exact. Since I is $\mathcal{C}$–injective, $H^j_{\mathcal{C}}(G, I) = \mathrm{Ext}^j_{\mathcal{C}}(\mathbb{Z}, I) = 0$. This shows the isomorphism: $H^{p-1}_{\mathcal{C}}(G, S) \cong H^p_{\mathcal{C}}(G, M)$. We may take

$$I = I_M = \prod_{m \in M - \{0\}} Hom(\mathbb{Z}[G], \mathbb{Q}/\mathbb{Z}).$$

Since $\mathbb{Z}[U]^r \cong \mathbb{Z}[G]$ as right U–modules by using a coset decomposition $G = \bigsqcup g_i U$, I_M is again $\mathcal{C}_U$–injective. Thus again using the long exact sequence:

$$H^{p-1}_{\mathcal{C}}(U, S) \cong H^p_{\mathcal{C}}(U, M)$$

as G/U–modules. Since $H^q_{\mathcal{C}}(U, M) = 0$ if $0 < q < p$, $H^q_{\mathcal{C}}(U, S) = 0$ if $0 < q < p - 1$. By taking U–invariant, we get another exact sequence:

$$0 \to M^U \to I^U \to S^U \to H^1_{\mathcal{C}}(U, M) = 0.$$

Note that I^U is $\mathbb{Z}[G/U]$–injective (2.11). Thus again by the long exact sequence, we get

$$H^{p-1}(G/U, S^U) \cong H^p(G/U, M^U).$$

Then applying induction hypothesis to S in place of M, we get an exact sequence:

$$0 \longrightarrow H^{p-1}(G/U, S^U) \longrightarrow H^{p-1}_{ct}(G, S) \longrightarrow H^0(G/U, H^{p-1}_{ct}(U, S)) \longrightarrow H^p(G/U, S^U),$$

which gives rise to the desired sequence by the three isomorphisms as above. □

We can prove a similar theorem for extension groups:

Theorem 2.16. *Let U be a closed normal subgroup of G. We write $\mathcal{C}_G$ for the categroy of discrete G–modules. Let M be a discrete G/U–module and N be a discrete G–module. If $H^q_{ct}(U, N) = 0$ for all integer q with $1 \le q \le p$, then we have for all q as above*

$$\mathrm{Ext}^q_{\mathcal{C}_G}(M, N) \cong \mathrm{Ext}^q_{\mathcal{C}_{G/U}}(M, N^U).$$

If M is finite of order a prime power ℓ^r and $p > 1$, we can ease the requirement to have the above equality of extension groups to the following weaker condition: $H^q_{ct}(U, N) = 0$ for all integer q with $1 \le q \le p - 1$ and $H^p_{ct}(U, N)[\ell^\infty] = 0$, where "$[\ell^\infty]$" indicates the ℓ–torsion part.

Proof. We claim to have the following exact sequence:

$$0 \to \mathrm{Ext}^1_{\mathcal{C}_{G/U}}(M, N^U) \xrightarrow{inf} \mathrm{Ext}^1_{\mathcal{C}_G}(M, N) \xrightarrow{\delta} \mathrm{Hom}_{\mathcal{C}_G}(M, H^1(U, N)). \tag{2.14}$$

To see this, we consider the extension class $e : N^U \hookrightarrow Y_U \twoheadrightarrow M$ of G/U–modules. Then the class of e can be extended to $inf(e) : N \hookrightarrow (N \oplus_{N^U} Y_U) \twoheadrightarrow M$, which is an extension of M by N, where $N \oplus_{N^U} Y_U$ is the fiber sum of $N^U \hookrightarrow N$ and Y_U over N (see Theorem 1.1). Since e is a sub-sequence of $inf(e)$, if $inf(e) = 0$, we have $e = 0$. Thus inf is an injection. For each extension class $E : N \hookrightarrow Y \twoheadrightarrow M$ in $\mathrm{Ext}^1_{\mathcal{C}_G}(M, N)$, we have a long exact sequences of cohomology groups:

$$0 \longrightarrow N^U \longrightarrow Y^U \longrightarrow M \xrightarrow{\delta_E} H^1_{ct}(U, N).$$

We assign to E the map δ_E. By definition, $\delta_E = 0 \iff E = inf(e)$ for $e : N^U \hookrightarrow Y^U \twoheadrightarrow M$. This shows the exactness of the claimed sequence. Thus we get the desired identity for $p = 1$.

We now prove the general case by induction on $p > 1$. We now take an injective presentation: $N \hookrightarrow I \twoheadrightarrow S$ in $\mathcal{C}_G$. As explained above, we may assume that

$$0 \to N^U \longrightarrow I^U \longrightarrow S^U \longrightarrow H^1(U, N) = 0$$

is an $\mathcal{C}_{G/U}$–injective presentation. Then via long exact sequence of extension groups and group cohomology, we have the following identity:

$$\mathrm{Ext}^q_{\mathcal{C}_G}(M, N) \cong \mathrm{Ext}^{q-1}_{\mathcal{C}_G}(M, S), \quad \mathrm{Ext}^q_{\mathcal{C}_{G/U}}(M, N^U) \cong \mathrm{Ext}^{q-1}_{\mathcal{C}_{G/U}}(M, S^U)$$
$$\text{and} \quad H^p_{ct}(U, N) = H^{p-1}_{ct}(U, S).$$

From this and the induction assumption applied to S, the desired result follows.

Now assume $|M| = \ell^r$ for a prime ℓ. We first check the last assertion when $p = 2$. We have the following exact sequence:

$$0 \longrightarrow \mathrm{Ext}^1_{\mathcal{C}_{G/U}}(M, S^U) \longrightarrow \mathrm{Ext}^1_{\mathcal{C}_G}(M, S)$$
$$\longrightarrow \mathrm{Hom}_{\mathcal{C}_G}(M, H^1_{ct}(U, S)) = \mathrm{Hom}_{\mathcal{C}_G}(M, H^1_{ct}(U, S)[\ell^\infty]) = 0,$$

and also we have

$$\mathrm{Ext}^1_{\mathcal{C}_{G/U}}(M, S^U) \cong \mathrm{Ext}^2_{\mathcal{C}_{G/U}}(M, N^U) \quad \text{and} \quad \mathrm{Ext}^1_{\mathcal{C}_G}(M, S^U) \cong \mathrm{Ext}^2_{\mathcal{C}_G}(M, N).$$

This shows the assertion when $p = 2$. Then we use this to the beginning step of the induction on p. By using the injective presentation: $N \hookrightarrow I \twoheadrightarrow S$, we can reduce the validity of the assertion to the case where $p = 2$, because the top degree vanishing of the ℓ–torsion part goes down to degree 2 and those total vanishing of degree $< p$ assures the vanishing of H^1. The details are left to the reader. □

Exercises.

(1) Show the exactness of

$$0 \longrightarrow H^1(G/U, M^U) \xrightarrow{inf_{G/U}} H^1_{ct}(G, M) \xrightarrow{res_{G/U}} H^0(G/U, H^1_{ct}(U, M)).$$

(2) Show that each closed subgroup of a profinite group G is an intersection of open normal subgroups containing the subgroup;

(3) Give a detailed proof of the last assertion of Theorem 2.16.

3. Duality in Galois Cohomology

In this section, we describe in detail the duality theory of Galois cohomology group due to J. Tate and G. Poitou. Our exposition follows basically that of Milne [ADT] Chapter I, but in many places, it is slightly more elementary.

3.1. Class formation and duality of cohomology groups.

Consider a profinite group G, a discrete G–module C and a family of isomorphisms $inv_U : H^2_{ct}(U, C) \xrightarrow{\simeq} \mathbb{Q}/\mathbb{Z}$ indexed by open subgroups U of G. Such a system is called a *class formation* if

(CF1) $H^1_{ct}(U, C) = 0$ for all open subgroup U of G;

(CF2) For all pairs of open subgroups $V \subset U \subset G$, the diagram

$$\begin{tikzcd} H^2_{ct}(U,C) \arrow[r, "res_{U/V}"] \arrow[d, "inv_U"'] & H^2_{ct}(V,C) \arrow[d, "inv_V"] \\ \mathbb{Q}/\mathbb{Z} \arrow[r, "x\mapsto nx"] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

commutes, where $n = (U : V)$.

The map inv_U is called the "invariant" with respect to U.

Theorem 3.1. *Let (G, C) be a class formation and $G^{ab} = \varprojlim_{U\in\mathcal{U}}(G/U)^{ab}$ is the maximal continuous abelian quotient of G. Then there exists a canonical map $rec_G : C^G \to G^{ab}$ (called the reciprocity map), whose image is dense in G^{ab} and whose kernel is the intersection $\bigcap_{U\in\mathcal{U}} N_{G/U}C^U$, where $N_{G/U} : C^U \to C^G$ is the map given by $N_{G/U}(x) = \sum_{g\in G/U} gx$.*

Proof. Let $V \subset U$ with $n = (U : V)$ be two members of $\mathcal{U}$. We have the following commutative diagram:

$$\begin{tikzcd} 0 \arrow[r] & H^2_{ct}(U/V,C^V) \arrow[r] \arrow[d, "inv_{U/V}"'] & H^2_{ct}(U,C) \arrow[r, "res_{U/V}"] \arrow[d, "inv_U", "\wr"'] & H^2_{ct}(V,C) \arrow[d, "inv_V", "\wr"'] & \\ 0 \arrow[r] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r, "n"'] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0. \end{tikzcd}$$

Since the last two vertical arrows are isomorphisms, the first one is an isomorphism:

$$inv_{U/V} : H^2(U/V, C^V) \cong \frac{1}{(U:V)}\mathbb{Z}/\mathbb{Z}. \tag{3.1}$$

We have the inflation-restriction exact sequence:

$$0 \to H^1(U/V, C^V) \to H^1_{ct}(U, C) \to H^1_{ct}(V, C),$$

which tells us that $H^1(U/V, C^V) = 0$. Then applying Theorem 2.5 and Theorem 2.7 to G/U for $k = -2$, we get the following commutative diagram:

$$\begin{tikzcd} H_T^{-2}(G/U,\mathbb{Z}) \arrow[r, "\simeq"] \arrow[d, "\wr"'] & H_T^0(G/U,\mathbb{Z}) \arrow[d, "\wr"'] \\ (G/U)^{ab} \arrow[r, "rec_{G/U}^{-1}"'] & C^G/N_{G/U}C^U. \end{tikzcd}$$

Taking the projective limit with respect to $U \in \mathcal{U}$, we get an injective map

$$rec_G : C^G/\bigcap_{U\in\mathcal{U}} N_{G/U}(C^U) \hookrightarrow \varprojlim_U C^G/N_{G/U}(C^U) \cong \varprojlim_U (G/U)^{ab} = G^{ab}$$

as desired. □

Let M be a (discrete) G–module which is of finite type as a $\mathbb{Z}$–module. Then by Proposition 2.12, we have a natural map

$$H^r_{ct}(G, \mathrm{Hom}_{\mathbb{Z}}(M, C)) \longrightarrow \mathrm{Ext}^r_{\mathcal{C}}(M, C).$$

This is an isomorphism if M is $\mathbb{Z}$–torsion-free or C is divisible. We also have the cup product pairing:

$$\begin{tikzcd}
H^r_{ct}(G, \mathrm{Hom}_{\mathbb{Z}}(M, C)) \arrow[d] & \times & H^{2-r}_{ct}(G, M) \arrow[d, "\wr"'] \arrow[r] & H^2_{ct}(G, C) \cong \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\
\mathrm{Ext}^r_{\mathcal{C}}(M, C) & \times & \mathrm{Ext}^{2-r}_{\mathcal{C}}(\mathbb{Z}, M) \arrow[r] & \mathrm{Ext}^2_{\mathcal{C}}(\mathbb{Z}, C),
\end{tikzcd}$$

where we agree to define the negative degree cohomology groups and the negative degree extension groups to be zero. For any discrete module M, we put $M^* = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$, which is called the Pontryagin dual module. We have $(M^*)^* \cong M$ canonically. When M is a finite module, $M^* \cong M$ as abelian groups (but may not be as G–modules). By the above pairing, we have the following canonical morphisms:

$$\alpha^r_G(M) : \mathrm{Ext}^r_{\mathcal{C}}(M, C) \to H^{2-r}_{ct}(G, M)^*. \tag{3.2}$$

Here negative degree cohomology groups and extension groups are defined to be 0. It is known that

$$i : H^2_{ct}(G, \mathbb{Z}) \cong \mathrm{Hom}_{ct}(G, \mathbb{Q}/\mathbb{Z}) \tag{3.3}$$

in the following way: the cup product pairing associated to $C \otimes_{\mathbb{Z}} \mathbb{Z} \cong C$:

$$\langle\ ,\ \rangle : H^0_{ct}(G, C) \times H^2_{ct}(G, \mathbb{Z}) \to H^2_{ct}(G, C) = \mathbb{Q}/\mathbb{Z}$$

is given by $\langle c, x\rangle = i(x)(rec_G(c))$ (see [CLC] XI.3). Then, in particular, $\alpha^0_G(\mathbb{Z})$ is the reciprocity map rec_G.

Theorem 3.2 (J. Tate)**.** *Let (G, C) be a class formation and M be a discrete $\mathbb{Z}[G]$–module of finite type. Then we have*

1. *The map $\alpha^r_G(M)$ is bijective for all $r \geq 2$, $\alpha^1_G(M)$ is bijective if M is torsion-free, and $\mathrm{Ext}^r_{\mathcal{C}}(M, C) = 0$ if $r \geq 3$;*
2. *The map $\alpha^1_G(M)$ is bijective if $\alpha^1_U(\mathbb{Z}/m\mathbb{Z})$ is bijective for all $U \in \mathcal{U}$ and all $m \in \mathbb{Z}$ (including $m = 0$);*
3. *The map $\alpha^0_G(M)$ is bijective for all finite M if $\alpha^0_U(\mathbb{Z}/m\mathbb{Z})$ is bijective for all $U \in \mathcal{U}$ and $m \in \mathbb{Z}$ (including $m = 0$).*

Proof. We first claim

$$\mathrm{Ext}^r_{\mathcal{C}}(M, C) = 0 \text{ for } r \geq 4, \text{ and if } M \text{ is torsion-free } \mathrm{Ext}^3_{\mathcal{C}}(M, C) = 0. \tag{3.4}$$

We take a generator $u_1, \dots, u_r$ of M over $\mathbb{Z}[G]$. Since $M \in \mathcal{C}$, $M = \bigcup_{U \in \mathcal{U}} M^U$ and hence, we find a small open normal subgroup U such that $u_j \in M^U$ for all j, that is, M is a G/U–module. Then we consider $\mathbb{Z}[G]$–linear map $\pi : P = \mathbb{Z}[G/U]^r \twoheadrightarrow M$ given by $(x_1, \dots, x_r) \mapsto \sum_{j=1}^r x_j u_j$. Since G/U is a finite group, P is a $\mathbb{Z}$–module of finite rank. Thus M is a $\mathbb{Z}$–module of finite type, and $Q = \mathrm{Ker}(\pi)$ is a $\mathbb{Z}$–free module of finite type. If we know the claim for $\mathbb{Z}$–free $\mathbb{Z}[G]$–modules of finite type, writing down the long exact sequence attached to $Q \hookrightarrow P \twoheadrightarrow M$:

$$\mathrm{Ext}^{r-1}_{\mathcal{C}}(Q, C) \to \mathrm{Ext}^r_{\mathcal{C}}(M, C) \to \mathrm{Ext}^r_{\mathcal{C}}(P, C),$$

we see that $\mathrm{Ext}^r(M,C)=0$ if $r\geq 4$. Thus we may and will assume that M is $\mathbb{Z}$–free.

Let $\widehat{M}=\mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$. Then by $\mathbb{Z}$–freeness, $\widehat{M}\otimes_{\mathbb{Z}}C\cong \mathrm{Hom}_{\mathbb{Z}}(M,C)$ via $\phi\otimes c\mapsto (m\mapsto \phi(m)c)$. Then by Proposition 2.12, we have

$$\mathrm{Ext}^r_{\mathcal{C}}(M,C)\cong H^r_{ct}(G,\mathrm{Hom}_{\mathbb{Z}}(M,C))\cong H^r_{ct}(G,\widehat{M}\otimes_{\mathbb{Z}}C).$$

We have from Corollary 2.9 that

$$H^r_{ct}(G,\widehat{M}\otimes_{\mathbb{Z}}C)=\varinjlim_{U\in\mathcal{U},\widehat{M}^U=\widehat{M}} H^r(G/U,M\otimes_{\mathbb{Z}}C^U).$$

By the remark after Theorem 2.7, we have

$$H^{r-2}(G/U,\widehat{M})\cong H^r(G/U,\widehat{M}\otimes_{\mathbb{Z}}C^U)$$

for all $r\geq 3$. Write $u_{U/V}$ for the generator of $H^2(U/V,C^V)$ with $inv_{U/V}(u_{U/V})=\frac{1}{(U:V)}$. Then we see $inf_{U/V}(u_{G/U})=(U:V)u_{G/V}$ by (CF2). Since the cup product commutes with inflation map (by definition) and the horizontal map of the following diagram sends $x\in H^{r-2}(G/U,\widehat{M})$ to the cup product $x\cup u_{G/U}$, we can check by (CF2) that the following diagram commutes:

$$\begin{tikzcd}
H^{r-2}(G/U,\widehat{M}) \arrow[r, "\simeq"] \arrow[d, "(U:V)inf_{U/V}"'] & H^r(G/U,\widehat{M}\otimes_{\mathbb{Z}}C^U) \arrow[d, "inf_{U/V}"] \\
H^{r-2}(G/V,\widehat{M}) \arrow[r, "\simeq"] & H^r(G/V,\widehat{M}\otimes_{\mathbb{Z}}C^V).
\end{tikzcd}$$

Since $H^r(\{1_G\},X)=0$ for all $r>0$, by Proposition 2.4 applied to $\{1_{G/U}\}\subset G/U$, we see that the index $(G:U)$ kills $H^r(G/U,X)$ for all G/U–modules X. In particular, $H^{r-2}(G/U,\widehat{M})$ is torsion if $r>2$. Thus $\varinjlim_{U\in\mathcal{U}} H^{r-2}(G/U,\widehat{M})$ with respect to $(U:V)inf_{U/V}$ vanishes if $r>2$. This shows the vanishing of $H^r_{ct}(G,\widehat{M}\otimes_{\mathbb{Z}}C)=\mathrm{Ext}^r_{\mathcal{C}}(M,C)$ for $r>2$ as claimed.

Now we suppose that $M=\mathbb{Z}$. Then $\alpha^2_G(\mathbb{Z})$ is the invariant map inv_G by definition, because $H^0_{ct}(G,\mathbb{Z})^*=\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z},\mathbb{Q}/\mathbb{Z})=\mathbb{Q}/\mathbb{Z}$. To study α^0, we look at the following exact sequence: $0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}\to 0$. Since $H^q(G/U,V)$ is killed by $(G:U)$, if V is a vector space over $\mathbb{Q}$, $H^q(G/U,V)=0$. Thus by the cohomology long exact sequence, we get

$$\mathrm{Hom}_{ct}(G,\mathbb{Q}/\mathbb{Z})=H^1_{ct}(G,\mathbb{Q}/\mathbb{Z})\cong H^2_{ct}(G,\mathbb{Z}).$$

Then $\alpha^0_G(\mathbb{Z}):C^G=\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z},C)\to\mathrm{Hom}_{ct}(G,\mathbb{Q}/\mathbb{Z})^*=G^{ab}$ is the reciprocity map. As for $\alpha^1_G(\mathbb{Z}):\mathrm{Ext}^1_{\mathcal{C}}(\mathbb{Z},C)=H^1_{ct}(G,C)\to H^1_{ct}(G,\mathbb{Z})^*$, by our assumption $H^1_{ct}(G,C)=0$. We need to show $H^1_{ct}(G,\mathbb{Z})=\mathrm{Hom}_{ct}(G,\mathbb{Z})=0$. Let $\phi:G\to\mathbb{Z}$ be a continuous homomorphism. Since G is compact, $\phi(G)$ is a compact subgroup of $\mathbb{Z}$. Since $\mathbb{Z}$ is discrete and torsion-free, it has only one compact subgroup, that is, $\{0\}$.

Next we suppose that $M=\mathbb{Z}/m\mathbb{Z}$. For any $\mathbb{Z}$–module X, we write $X[m]=\{x\in X|mx=0\}$. Note that $H^1_{ct}(G,\mathbb{Z})=\mathrm{Hom}_{ct}(G,\mathbb{Z})=\{0\}$ because $\mathbb{Z}$ has only one compact subgroup $\{0\}$. We get from the long exact sequence attached to $0\to\mathbb{Z}\xrightarrow{x\mapsto mx}\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}\to 0$ a short exact sequence:

$$0=H^1_{ct}(G,\mathbb{Z})\to H^1_{ct}(G,\mathbb{Z}/m\mathbb{Z})\to H^2_{ct}(G,\mathbb{Z})[m]=\mathrm{Hom}_{\mathbb{Z}}(G^{ab},\mathbb{Z}/m\mathbb{Z})\to 0.$$

This shows that $H^1_{ct}(G,\mathbb{Z}/m\mathbb{Z})^* = G^{ab}/mG^{ab}$. Similarly, we get from Proposition 1.10 the following exact sequence:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(\mathbb{Z}, C) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \to \mathrm{Ext}^1(\mathbb{Z}/m\mathbb{Z}, C) \to \mathrm{Ext}^1_{\mathcal{C}}(\mathbb{Z}, C)[m] \to 0.$$

Note that $\mathrm{Hom}_{\mathcal{C}}(\mathbb{Z}, C) \cong C^G$ and $\mathrm{Ext}^1_{\mathcal{C}}(\mathbb{Z}, C) = H^1_{ct}(G, C) = 0$ by (CF1). This shows that $\mathrm{Ext}^1_{\mathcal{C}}(\mathbb{Z}/m\mathbb{Z}, C) = C^G/mC^G$. Then

$$\alpha^1_G(\mathbb{Z}/m\mathbb{Z}) : C^G/mC^G \to \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Z}/m\mathbb{Z})^* = G^{ab}/mG^{ab}$$

is induced by rec_G. Since $\mathrm{Ext}^1_{\mathcal{C}}(\mathbb{Z}, C) = 0$, again by long exact sequence:

$$\begin{aligned}0 = \mathrm{Ext}^1_{\mathcal{C}}(\mathbb{Z}, C) \to \mathrm{Ext}^2_{\mathcal{C}}(\mathbb{Z}/m\mathbb{Z}, C) \to \mathrm{Ext}^2_{\mathcal{C}}(\mathbb{Z}, C)[m]& \\ = H^2_{ct}(G, C)[m] = \mathbb{Q}/\mathbb{Z}[m],&\end{aligned}$$

the map $\alpha^2_G(\mathbb{Z}/m\mathbb{Z}) : \mathbb{Q}/\mathbb{Z}[m] \to H^0_{ct}(G, \mathbb{Z}/m\mathbb{Z})^* = \frac{1}{m}\mathbb{Z}/\mathbb{Z}$ is an isomorphism induced by inv_G. As we have seen, $\mathrm{Ext}^3_{\mathcal{C}}(\mathbb{Z}, M) = 0$. Then by the long exact sequence, we get a short exact sequence:

$$0 \to \mathrm{Ext}^2_{\mathcal{C}}(\mathbb{Z}, C) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \to \mathrm{Ext}^3_{\mathcal{C}}(\mathbb{Z}/m\mathbb{Z}, C) \to \mathrm{Ext}^3_{\mathcal{C}}(\mathbb{Z}, C) = 0.$$

Since $\mathrm{Ext}^2_{\mathcal{C}}(\mathbb{Z}, C) = H^2_{ct}(G, C) = \mathbb{Q}/\mathbb{Z}$, $\mathrm{Ext}^2_{\mathcal{C}}(\mathbb{Z}, C) \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} = 0$, and hence

$$\mathrm{Ext}_{\mathcal{C}}(\mathbb{Z}/m\mathbb{Z}, C) = 0.$$

Thus the theorem is valid for any M on which G acts trivially.

Now we treat general M. We take $U \in \mathcal{U}$ such that $M^U = M$. Then M is a module over the finite group G/U. Let $\pi : \mathbb{Z}[G/U] \to \mathbb{Z}$ be the augmentation: $\pi(\sum_{g \in G/U} a_g g) = \sum_{g \in G/U} a_g$. Then $0 \to M = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M) \xrightarrow{\pi^*} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], M) = I$ is an injection with cokernel S. For an injective resolution $M \hookrightarrow M^\bullet$, we see that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], M^\bullet)$ is a $\mathcal{C}$–injective resolution of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], M)$ (Lemma 2.13). Then we have the following version of Shapiro's lemma (see Exercise 5 of 2.1):

$$\mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], M^\bullet)) = \mathrm{Hom}_{\mathbb{Z}[U]}(\mathbb{Z}, M^\bullet).$$

This shows that

$$H^\bullet_{ct}(G, I) = H^\bullet_{ct}(U, M).$$

Since $\mathbb{Z}[G/U] \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], \mathbb{Z})$ as $\mathbb{Z}[G]$–modules, we have $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], M) \cong \mathbb{Z}[G/U] \otimes_{\mathbb{Z}} M$. Then, taking a $\mathcal{C}$–injective resolution $C \hookrightarrow C^\bullet$, we have

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], M), C^\bullet) \cong \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[G/U] \otimes_{\mathbb{Z}} M, C^\bullet)& \\ = \mathrm{Hom}_{\mathbb{Z}[U]}(M, C^\bullet),&\end{aligned} \tag{3.5}$$

which is induced by $\phi \mapsto (m \mapsto \phi(1 \otimes m))$. Write $\mathcal{C}_U$ for the category of discrete U–modules. Then the $\mathcal{C}$–injective resolution of C constructed in 2.3 is also a $\mathcal{C}_U$–injective resolution, we get

$$\begin{aligned}\mathrm{Ext}^\bullet_{\mathcal{C}}(I, C) = H^\bullet(\mathrm{Hom}_{\mathbb{Z}[G]}(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], M), C^\bullet))& \\ \cong H^\bullet(\mathrm{Hom}_{\mathbb{Z}[U]}(M, C^\bullet)) = \mathrm{Ext}^\bullet_{\mathcal{C}_U}(M, C).&\end{aligned}$$

Now we get, writing $E^q_U(X)$ for $\mathrm{Ext}_{\mathcal{C}_U}(X,C)$ and $H^q_U(X)$ for $H^q_{ct}(U,X)$, the following commutative diagram:

$$\begin{tikzcd}
{} \arrow[r] & E^r_G(S) \arrow[r] \arrow[d, "\alpha^r_G(S)"'] & E^r_U(M) \arrow[r] \arrow[d, "\alpha^r_U(M)"'] & E^r_G(M) \arrow[r] \arrow[d, "\alpha^r_G(M)"'] & E^{r+1}_G(S) \arrow[r] \arrow[d, "\alpha^{r+1}_G(S)"] & {} \\
{} \arrow[r] & H^{2-r}_G(S) \arrow[r] & H^{2-r}_U(M) \arrow[r] & H^{2-r}_G(M) \arrow[r] & H^{1-r}_G(S) \arrow[r] & {}.
\end{tikzcd}$$

We first apply this to $r=3$ and we get from (3.4):

$$\begin{tikzcd}
E^3_U(M) \arrow[r] \arrow[d, "\alpha^3_U(M)", "\wr"'] & E^3_G(M) \arrow[r] \arrow[d, "\alpha^3_G(M)"'] & E^4_G(S) \arrow[d, "\alpha^4_U(S)", "\wr"'] \\
H^{-1}_U(M)=0 \arrow[r] & H^{-1}_G(M)=0 \arrow[r] & H^{-2}_G(S)=0.
\end{tikzcd}$$

This shows that $\alpha^3_G(M)$ is the zero map as desired. Now we apply the diagram to $r=2$.

$$\begin{tikzcd}
{} \arrow[r] & E^2_U(M) \arrow[r] \arrow[d, "\alpha^2_U(M)", "\wr"'] & E^2_G(M) \arrow[r] \arrow[d, "\alpha^2_G(M)"'] & E^3_G(S) \arrow[r] \arrow[d, "\alpha^3_G(S)", "\wr"'] & E^3_U(M) \arrow[r] \arrow[d, "\alpha^3_U(M)", "\wr"'] & 0 \\
{} \arrow[r] & H^0_U(M) \arrow[r] & H^0_G(M) \arrow[r] & H^{-1}_G(S)=0 \arrow[r] & H^{-1}_U(M)=0 \arrow[r] & 0.
\end{tikzcd}$$

Then by the five lemma (see [BCM] Exercise I.1.4.b), $\alpha^2_G(M)$ is surjective. Applying this to S in place of M, we see that $\alpha^2_G(S)$ is surjective, getting the following commutative diagram:

$$\begin{tikzcd}
{} \arrow[r] & E^2_G(S) \arrow[r] \arrow[d, "\alpha^2_G(S)"'] & E^2_U(M) \arrow[r] \arrow[d, "\alpha^2_U(M)", "\wr"'] & E^2_G(M) \arrow[r] \arrow[d, "\alpha^2_G(M)"] & E^3_G(S) \arrow[r] \arrow[d, "\alpha^3_G(S)", "\wr"'] & 0 \\
{} \arrow[r] & H^0_G(S) \arrow[r] & H^0_U(M) \arrow[r] & H^0_G(M) \arrow[r] & H^{-1}_G(M) \arrow[r, equal] & 0.
\end{tikzcd}$$

Again by the five lemma, $\alpha^2_G(M)$ is an isomorphism. If M is torsion-free, we see that I and S are both torsion-free. Then the same argument for $r=1$ shows that $\alpha^1_G(M)$ is an isomorphism. This shows (1). As for (2), under the assumption, we do not need to assume that M is torsion-free for $\alpha^1_G(M)$ to be an isomorphism. The same reasoning is valid for $\alpha^0_G(M)$ under the assumption of (3). □

Example 3.1. Let K be a finite extension of $\mathbb{Q}_p$. We fix an algebraic closure $\overline{K}$ of K and put $G=\mathrm{Gal}(\overline{K}/K)$. Then G is a profinite group. Let $C=\overline{K}^\times$. Then by the local class field theory and Hilbert's theorem 90 (Exercises 3-4), it is known that (G,C) is a class formation. Since C is divisible (that is, for any $a\in\overline{K}^\times$ and $0<n\in\mathbb{Z}$ $\sqrt[n]{a}\in\overline{K}^\times$), by Proposition 2.12,

$$\mathrm{Ext}^r_{\mathcal{C}}(M,C)\cong H^r_{ct}(G,Hom(M,C)).$$

Thus the cup product pairing:

$$H^r_{ct}(G,Hom(M,C))\times H^{2-r}_{ct}(G,M)\to H^2_{ct}(G,C)\cong\mathbb{Q}/\mathbb{Z}$$

gives the duality. In this case, the exact statement of the duality is as follows:

Theorem 3.3 (J. Tate)**.** *Let M be a finitely generated discrete $\mathbb{Z}[G]$–module. Then $\alpha^r_G(M) : H^r_{ct}(G, Hom(M, \overline{K}^\times)) \to H^{2-r}_{ct}(G, M)^*$ is an isomorphism for all $r \geq 1$. If M is finite, then $\alpha^0_G(M) : \mathrm{Hom}_{\mathbb{Z}[G]}(M, \overline{K}^\times) \cong H^2_{ct}(G, M)^*$. If M is finite, all cohomology groups introduced above are finite and vanish except for the degrees* $0, 1, 2$.

Proof. Let R be the p–adic integer ring of K. Let I be the inertia subgroup of G. Let I_{ab} be the image of I in G^{ab}. By the local class field theory, we have the following commutative diagram with exact rows:

$$\begin{tikzcd}
1 \to R^\times \arrow[r] \arrow[d, "\wr"'] & K^\times \arrow[r, "v"] \arrow[d, "rec_G"'] & \mathbb{Z} \arrow[r] \arrow[d, "\cap"] & 0 \\
1 \to I_{ab} \arrow[r] & G^{ab} \arrow[r] & \widehat{\mathbb{Z}} \arrow[r] & 0.
\end{tikzcd}$$

The quotient $G^{ab}/I_{ab} = \mathrm{Gal}(\overline{\mathbb{F}}_p/k)$ for the residue field k of K, which is generated by the Frobenius automorphism and is isomorphic to $\widehat{\mathbb{Z}}$. We already have $\alpha^0_G(\mathbb{Z}/m\mathbb{Z}) : \mu_m(K) \to G^{ab}[m]$ and $\alpha^1_G(\mathbb{Z}/m\mathbb{Z}) : K^\times/(K^\times)^m \cong G^{ab}/(G^{ab})^m$ for all positive integer m, where $\mu_m(K)$ is the subgroup of m–th roots of unity in K. Since $\widehat{\mathbb{Z}}$ is $\mathbb{Z}$–flat, after tensoring $\mathbb{Z}/m\mathbb{Z}$ over $\mathbb{Z}$, the two rows are still exact. This combined with the snake lemma shows that $\alpha^1_G(\mathbb{Z}/m\mathbb{Z})$ is an isomorphism. Similarly, by applying $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, *)$ to the above diagram, we see that $\alpha^0_G(\mathbb{Z}/m\mathbb{Z})$ is an isomorphism. Thus from Theorem 3.2, we know that $\alpha^j_G(M)$ is an isomorphism as described above. When M is finite, by what we have proven, $H^r_{ct}(G, M) = 0$ if $r > 2$. By the duality we proved, we only need to prove the finiteness of H^0_{ct} and H^1_{ct}. The finiteness of H^0_{ct} is obvious. To see the finiteness for H^1_{ct}, we use the following exact sequence:

$$1 \to \mu_m \to \overline{K}^\times \xrightarrow{x \mapsto x^m} \overline{K}^\times \to 1.$$

From this we get the following exact sequence:

$$1 \to \mu_m(K) \to K^\times \xrightarrow{x \mapsto x^m} K^\times \to H^1_{ct}(G, \mu_m) \to H^1_{ct}(G, \overline{K}^\times) = 0.$$

The vanishing of $H^1_{ct}(G, \overline{K}^\times)$ follows from the Hilbert theorem 90 (Exercises 3-4). This shows

$$H^1_{ct}(G, \mu_m) \cong K^\times/(K^\times)^m,$$

which is finite. In general, we pick m so that $mM = 0$. Then we take a finite Galois extension L of K such that $\mu_m(L) = \mu_m$ and $M^U = M$ for $U = \mathrm{Gal}(\overline{K}/L)$. Then M is a finite product of copies of μ_n for $n|m$ as U–modules, and hence $H^1_{ct}(U, M)$ is finite. By the inflation-restriction sequence, we get an exact sequence:

$$0 \to H^1(G/U, M) \to H^1_{ct}(G, M) \to H^1_{ct}(U, M).$$

Since $H^1(G/U, M)$ is finite (Corollary 2.2), $H^1_{ct}(G, M)$ is finite. □

Example 3.2. We have a result analogous to Theorem 3.3 for archimedean local fields: Since $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, we can directly compute $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), M)$ for finite modules M over $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, and we leave the reader to prove the following theorem (Exercise 2):

Theorem 3.4. *Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, and let M be a finite G–module. Then we have*

1. *The cup product defines a perfect Pontryagin pairing:*
$$H^r_T(G, \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^\times)) \times H^{2-r}_T(G, M) \cong \frac{1}{2}\mathbb{Z}/\mathbb{Z}$$
for all $r \in \mathbb{Z}$;
2. *Let $K = \mathbb{R}$ or $\mathbb{C}$, and put $H = \mathrm{Gal}(\mathbb{C}/K)$. When $K = \mathbb{R}$, we put $|M|_K = |M|$ (the order of M) and when $K = \mathbb{C}$, we write $|M|_K$ for $|M|^2$. Then we have*
$$\frac{|H^0(H, M)| \cdot |H^0(H, \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{C}^\times))|}{|H^1(H, M)|} = |M|_K.$$

Exercises.

1. Prove (3.5).
2. Prove Theorem 3.4.
3. Prove for a finite Galois extension K/F, $H^1(\mathrm{Gal}(K/F), K^\times) = 0$, where $K^\times$ is the multiplicative group of the field K (Hilbert's theorem 90).
4. Prove for the separable algebraic closure K_s of K,
$$H^1_{ct}(\mathrm{Gal}(K_s/K), K_s^\times) = 0.$$
5. Prove for a finite Galois extension K/F, $H^q(\mathrm{Gal}(K/F), K) = 0$ for all $q > 0$, where K is the additive group of the field K. Hint: Show first the existence of a normal base of K/F.

3.2. **Global duality theorems.** We now look into the global case. Let $K/\mathbb{Q}$ be a finite extension. If we put $G = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $C = C_K = \varinjlim_{L/K} L^\times_{\mathbb{A}}/L^\times$, then by global class field theory, (G, C) is a class formation. However the module C and G are too big to compute cohomology. Thus in this case, we need to restrict ramification to a finite set, to get a reasonable theory. This can be done as follows: Let S be a finite set of places of $\mathbb{Q}$ including the archimedean place and Σ be the set of places of K above S. Let K^S/K be the maximal algebraic extension unramified outside S. We write $\mathrm{G} = \mathrm{G}_S = \mathrm{Gal}(K^S/K)$. We write $O^S = O^S_K$ for the ring of S–integers; in other words, for each prime ideal $\mathfrak{p} \in \Sigma$, we take a power $\mathfrak{p}^h$ for the class number h of K and write its generator as $\omega_{\mathfrak{p}}$: $\mathfrak{p}^h = (\omega_{\mathfrak{p}})$. Then
$$O^S_K = O_K[\frac{1}{\omega_{\mathfrak{p}}}]_{\mathfrak{p}\in\Sigma}.$$

We can rewrite this ring as

$$(3.6)\quad \begin{aligned} O^S_K &= K \cap \bigcap_{\mathfrak{p}\notin\Sigma} O_{K,\mathfrak{p}} \\ &= \left\{\alpha \in O_K \middle| (\alpha) = \frac{\mathfrak{a}}{\mathfrak{b}} \text{ with } \mathfrak{a} \subset O_K \text{ and } \mathfrak{b} \text{ is a product of prime ideals in } \Sigma\right\}, \end{aligned}$$

where O_K is the integer ring of K and $O_{K,\mathfrak{p}}$ is the $\mathfrak{p}$–adic completion of O_K.

We ease slightly the definition of class formation as follows: Consider a profinite group G, a discrete G–module C and a family of injections $inv_U : H^2_{ct}(U, C) \hookrightarrow \mathbb{Q}/\mathbb{Z}$

indexed by open subgroups U of G. Such a system is called an *S–class formation* if the following three conditions are satisfied

(cf1) $H^1_{ct}(U,C)=0$ for all open subgroups U of G;

(cf2) For all pairs of open subgroups $V\subset U\subset G$, the diagram

$$\begin{tikzcd} H^2_{ct}(U,C) \arrow[r, "res_{U/V}"] \arrow[d, "inv_U"'] & H^2_{ct}(V,C) \arrow[d, "inv_V"] \\ \mathbb{Q}/\mathbb{Z} \arrow[r, "x\mapsto nx"] & \mathbb{Q}/\mathbb{Z} \end{tikzcd}$$

commutes, where $n=(U:V)$.

(cf3) For all pairs of open subgroups $V\subset U\subset G$ with V normal in U, the induced map: $inv_{U/V}:H^2_{ct}(U/V,C^V)\to\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is a surjective isomorphism for $n=(U:V)$;

Just restricting to the ℓ–primary parts the proof of Theorem 3.2, we immediately get

Theorem 3.5. *Let (G,C) be an S–class formation and M be a discrete $\mathbb{Z}[G]$–module of finite type. Let $\ell\in S$. Then we have*

1. *The map $\alpha^r_G(M)[\ell]:\mathrm{Ext}^r_{\mathcal{C}}(M,C)[\ell^\infty]\to H^{2-r}_{ct}(G,M)^*[\ell^\infty]$ is bijective for all $r\geq 2$, $\alpha^1_G(M)[\ell]$ is bijective if M is torsion-free, and $\mathrm{Ext}^r_{\mathcal{C}}(M,C)=0$ if $r\geq 3$;*
2. *The map $\alpha^1_G(M)[\ell]$ is bijective if $\alpha^1_U(\mathbb{Z}/\ell^m\mathbb{Z})$ is bijective for all $U\in\mathcal{U}$ and all $m\in\mathbb{Z}$;*
3. *The map $\alpha^0_G(M)$ is bijective for all finite ℓ–primary M if $\alpha^0_U(\mathbb{Z}/\ell^m\mathbb{Z})$ is bijective for all $U\in\mathcal{U}$ and $m\in\mathbb{Z}$.*

We write for any finite extension F/K inside K^S

$$F^\times_S=\prod_{\ell\in S}F^\times_\ell=\left\{a\in F^\times_{\mathbb{A}}\middle|a_\ell=1\ \forall\ell\notin S\right\},$$

where $F_{\mathbb{A}}=F\otimes_{\mathbb{Q}}\mathbb{A}$ and $F_\ell=F\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$. We also put $E_{F,S}=(O^S_F)^\times$, $C_{F,S}=F^\times_S/E_{F,S}$ and $C_S=\varinjlim_F C_{F,S}$, where F runs over all finite extensions of K inside K^S. Then naturally C_S is a discrete G–module. We want to prove

Theorem 3.6 (Tate)**.** *The couple (G_S,C_S) forms an S–class formation, and $C^{\mathrm{G}}_S\cong K^\times_{\mathbb{A}}/U_{K,S}K^\times$, where $U_{K,S}=\prod_{\ell\notin S}O^\times_{K,\ell}$ for $O_{K,\ell}=O_K\otimes_{\mathbb{Z}}\mathbb{Z}_\ell$.*

If $\ell\in S$, K^S contains $K(\mu_{\ell^\infty})$, and hence its maximal ℓ–profinite quotient is an infinite group. This shows, by (cf2-3), that inv_U induces a surjective isomorphism of ℓ–primary parts for $\ell\in S$: $H^2_{ct}(U,C)\cong\mathbb{Q}_\ell/\mathbb{Z}_\ell$ for all open subgroups $U\subset\mathrm{G}$.

Proof. We follow the treatment of Milne in [ADT] I.4. We know from class field theory ([**?**] Section 11) that (G,C) is a class formation for $G=\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $C=C_K=\varinjlim_L L^\times_{\mathbb{A}}/L^\times$, where L runs over all finite extensions of K inside $\overline{\mathbb{Q}}$. Let $\mathfrak{H}=\mathrm{Gal}(\overline{\mathbb{Q}}/K^S)$ and $\pi:G\to\mathrm{G}$ be the projection (thus $\mathfrak{H}=\mathrm{Ker}(\pi)$). By the inflation-restriction sequence (Theorem 2.15) with respect to $\mathfrak{H}$ and G, we verify easily (cf1,2,3) for (G, C_S) if we can prove $H^r(\mathrm{G}, C_S) \cong H^r(\mathrm{G}, C^{\mathfrak{H}})$ for all $r > 0$.

We now prove $H^r(\mathrm{G}, C_S) \cong H^r(\mathrm{G}, C^{\mathfrak{H}})$ for all $r > 0$. Let $Cl(O_F^S)$ be the ideal class group of the Dedekind domain O_S^F. We note the following (natural) exact sequence (Exercise 1):

$$1 \longrightarrow C_{F,S} \longrightarrow F_{\mathbb{A}}^\times / U_{F,S} F^\times \longrightarrow Cl(O_F^S) \longrightarrow 1. \tag{3.7}$$

By the principal ideal theorem ([CFT] XIII.4), we have

$$\varinjlim_F Cl(O_F^S) = \{1\}$$

and hence

$$\varinjlim_F C_{F,S} \cong \varinjlim_F F_{\mathbb{A}}^\times / U_{F,S} F^\times, \tag{$*$}$$

where F runs finite extensions of K inside K^S. Let $U_S = \varinjlim_F U_{F,S}$. Then by the Hilbert theorem 90 (Exercise 2-3 of the previous subsection), we get the following exact sequence:

$$0 \to (K^S)^\times \to (\varinjlim_{L \subset \overline{\mathbb{Q}}} L_{\mathbb{A}}^\times)^{\mathfrak{H}} = (\varinjlim_{F \subset K^S} F_{\mathbb{A}}^\times) \to C_K^{\mathfrak{H}} \to H^1(\mathfrak{H}, \overline{\mathbb{Q}}^\times) = 0.$$

Thus

$$C_K^{\mathfrak{H}} = \varinjlim_F F_{\mathbb{A}}^\times / F^\times.$$

After taking injective limit of (3.7) with respect to $F \subset K^S$, we have from $(*)$ that $C_S \cong C_K^{\mathfrak{H}} / U_S$, which shows the exactness of

$$1 \longrightarrow U_S \longrightarrow C_K^{\mathfrak{H}} \longrightarrow C_S \longrightarrow 1. \tag{3.8}$$

By the long exact sequence (Corollary 2.11) of the above short one, we only need to prove $H^q(\mathrm{G}, U_S) = 0$ for all $q > 0$. Since $H^q(\mathrm{G}, U_S) = \varinjlim_F H^q(\mathrm{Gal}(F/K), U_{F,S})$ by Corollary 2.9, we only need to prove $H^q(\mathrm{Gal}(F/K), U_{F,S}) = 0$ for all finite extensions F/K in K^S.

By projecting down cocycles to components, we see easily for finite extensions F/K that $H^q(\mathrm{Gal}(F/K), U_{F,S})$ injects into $\prod_{\mathfrak{p} \nmid p \in S} H^q(\mathrm{Gal}(F/K), \prod_{\mathfrak{P}|\mathfrak{p}} O_{F,\mathfrak{P}}^\times)$. Here the lower case $\mathfrak{p}$ indicates prime ideals of K and capital $\mathfrak{P}$ indicates those of F. Note that $\prod_{\mathfrak{P}|\mathfrak{p}} O_{F,\mathfrak{P}}^\times \cong \mathrm{Hom}_{\mathbb{Z}[D]}(\mathbb{Z}[\mathrm{Gal}(F/K)], O_{F,\mathfrak{P}}^\times)$ for the decomposition group D of $\mathfrak{P}$ in $\mathrm{Gal}(F/K)$. Thus by Shapiro's lemma Lemma 2.5,

$$H^q(\mathrm{Gal}(F/K), \prod_{\mathfrak{P}|\mathfrak{p}} O_{F,\mathfrak{P}}^\times) \cong H^q(D, O_{F,\mathfrak{P}}^\times).$$

Since $\mathfrak{P}$ is unramified over $\mathfrak{p}$, $O_{\mathfrak{P}}^\times \cong \mathbb{F}_q^\times \times L$ as D–modules, where $\mathbb{F}_q$ is the residue field of $O_{\mathfrak{P}}$, and $L = 1 + \mathfrak{P} O_{\mathfrak{P}}$. Since $D \cong \mathrm{Gal}(\mathbb{F}_q/\mathbb{F})$ for the residue field $\mathbb{F}$ of $O_{\mathfrak{p}}$, it is easy to see from Proposition 2.3 that $H^q(D, \mathbb{F}_q^\times) = 0$. By Exercise 5 of the previous subsection, $H^q(D, \mathbb{F}_q) = 0$. Since $1 + \mathfrak{P}^n O_{\mathfrak{P}} / 1 + \mathfrak{P}^{n+1} O_{\mathfrak{P}}$ is isomorphic to $\mathbb{F}_q$ as D–module and $1 + \mathfrak{P}^n O_{\mathfrak{P}} \cong O_{\mathfrak{P}}$ as D–modules for n sufficiently large (by $\mathfrak{P}$–adic logarithm), we see from Corollary 2.11, $H^q(D, 1 + \mathfrak{P} O_{\mathfrak{P}}) = H^q(D, O_{\mathfrak{P}})$. By taking a normal base of $O_{\mathfrak{P}}$ over $O_{\mathfrak{p}}$, which lifts a normal base of $\mathbb{F}_q/\mathbb{F}$, we see that $O_{\mathfrak{P}} \cong O_{\mathfrak{p}}[D]$ as D–modules, which is $O_{\mathfrak{p}}[D]$–projective. This shows $H^q(D, O_{\mathfrak{P}}) = 0$. Thus we conclude $H^q(D, O_{\mathfrak{P}}^{\times}) = 0$ and hence $H^q(\mathrm{Gal}(F/K), U_{F,S}) = 0$ as desired. □

We have shown the following fact in the above proof of Theorem 3.6:

Lemma 3.7. *If F/K is a finite Galois extension of number fields and if F/K is unramified at a prime ideal $\mathfrak{p}$ of K, then*

$$H^q(\mathrm{Gal}(F/K), \prod_{\mathfrak{P}|\mathfrak{p}} O_{F,\mathfrak{P}}^{\times}) = 0 \quad \text{and} \quad H^q(D, O_{F,\mathfrak{P}}^{\times}) = 0$$

for the decomposition group $D \subset \mathrm{Gal}(F/K)$ of $\mathfrak{P}/\mathfrak{p}$.

To state the exact duality statement, we first study the reciprocity map $rec_S : C_S \to \mathrm{G}_S^{ab}$. By global class field theory, we have the following exact sequence:

$$1 \longrightarrow D_K \longrightarrow K_{\mathbb{A}}^{\times}/K^{\times} \xrightarrow{rec} G^{ab} \longrightarrow 1,$$

where D_K is the identity connected component of $K_{\mathbb{A}}^{\times}/K^{\times}$ and is the maximal divisible subgroup of $K_{\mathbb{A}}^{\times}/K^{\times}$ (see [CFT] VII, IX). Since U_S is totally disconnected, by (3.8), the kernel $\mathrm{Ker}(rec_{S,K})$ of the induced reciprocity map $rec_{S,K} : K_{\mathbb{A}}^{\times}/K^{\times}U_{K,S} \to \mathrm{G}^{ab}$ is the image of D_K. Thus we see $D_K U_{K,S}/U_{K,S} \cong \mathrm{Ker}(rec_{S,K})$, which shows that $\mathrm{Ker}(rec_{S,K})$ is divisible.

Corollary 3.8. *Let the notation and the assumption be as in the theorem. Let M be a discrete G_S–module of finite type, and let $\ell \in S$. Then*

1. *The map $\alpha_{\mathrm{G}}^r(M)[\ell] : \mathrm{Ext}_{\mathcal{C}}^r(M, C_S)[\ell^{\infty}] \to H_{ct}^{2-r}(\mathrm{G}, M)^*[\ell^{\infty}]$ is bijective for all $r \geq 1$.*
2. *Suppose that M is a finite module. Let F be a finite totally imaginary Galois extension of K inside K^S such that $\mathrm{Gal}(K^S/F)$ acts trivially on M and $\mu_{|M|}$. Then if $|M|O_S = O_S$, we have the following exact sequence:*

$$\mathrm{Hom}(M, \mathrm{Ker}(rec_{S,F})) \xrightarrow{N_{F/K}} \mathrm{Hom}_{\mathrm{G}}(M, C_S) \xrightarrow{\alpha_{\mathrm{G}}^0(M)} H_{ct}^2(\mathrm{G}_S, M)^* \longrightarrow 0.$$

Proof. For the first assertion, by Theorems 3.5 and 3.6, we need to prove that $\alpha_{\mathrm{G}}^1(\mathbb{Z}/\ell^m\mathbb{Z})$ is an isomorphism for all m. We get from the long exact sequence attached to $0 \to \mathbb{Z} \xrightarrow{x \mapsto \ell^m x} \mathbb{Z} \to \mathbb{Z}/\ell^m\mathbb{Z} \to 0$ a short exact sequence:

$$0 = H_{ct}^1(\mathrm{G}, \mathbb{Z}) \to H_{ct}^1(\mathrm{G}, \mathbb{Z}/\ell^m\mathbb{Z}) \to H_{ct}^2(\mathrm{G}, \mathbb{Z})[\ell^m] = \mathrm{Hom}_{\mathbb{Z}}(\mathrm{G}^{ab}, \mathbb{Z}/\ell^m\mathbb{Z}) \to 0.$$

This shows that $H_{ct}^1(\mathrm{G}, \mathbb{Z}/\ell^m\mathbb{Z})^* = \mathrm{G}^{ab}/\ell^m\mathrm{G}^{ab}$. Similarly, we get from Proposition 1.10 the following exact sequence:

$$0 \to \mathrm{Hom}_{\mathcal{C}}(\mathbb{Z}, C_S) \otimes_{\mathbb{Z}} \mathbb{Z}/\ell^m\mathbb{Z} \to \mathrm{Ext}_{\mathcal{C}}^1(\mathbb{Z}/\ell^m\mathbb{Z}, C_S) \to \mathrm{Ext}_{\mathcal{C}}^1(\mathbb{Z}, C_S)[\ell^m] \to 0.$$

Note that $\mathrm{Hom}_{\mathcal{C}}(\mathbb{Z}, C_S) \cong C_S^{\mathrm{G}}$ and $\mathrm{Ext}_{\mathcal{C}}^1(\mathbb{Z}, C_S) = H_{ct}^1(\mathrm{G}, C_S) = 0$ by (cf1). This shows that $\mathrm{Ext}_{\mathcal{C}}^1(\mathbb{Z}/\ell^m\mathbb{Z}, C_S) = C_S^{\mathrm{G}}/mC_S^{\mathrm{G}}$. Since $\mathrm{Ker}(rec_{S,K})$ is divisible, $C_S^{\mathrm{G}}/mC_S^{\mathrm{G}} \cong C_K^G/mC_K^G$ for $G = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$. Then $\alpha_{\mathrm{G}}^1(\mathbb{Z}/\ell^m\mathbb{Z}) : C_S^{\mathrm{G}}/\ell^m C_S^{\mathrm{G}} \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{G}, \mathbb{Z}/\ell^m\mathbb{Z})^* = \mathrm{G}^{ab}/m\mathrm{G}^{ab}$ is induced by rec_G and hence is an isomorphism (Theorem 3.1).

We now prove the second assertion. When $M = \mathbb{Z}/m\mathbb{Z}$ or $\mathbb{Z}$, α^0_{G} is just a reciprocity map: $C_S^{\mathrm{G}}/mC_S^{\mathrm{G}} \to \mathrm{G}^{ab}/m\mathrm{G}^{ab}$, and the assertion is clear from the argument preceding the corollary. As in the proof of Theorem 3.2, we take an open normal subgroup $U = \mathrm{Gal}(K^S/F) \subset \mathrm{G}$ fixing M element by element, and for the augmentation $\pi : \mathbb{Z}[\mathrm{G}/U] \twoheadrightarrow \mathbb{Z}$, we consider a presentation:

$$0 \to M = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, M) \xrightarrow{\pi^*} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[\mathrm{G}/U], M) = I \twoheadrightarrow N \to 0.$$

Then we have the following commutative diagram:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{C}}(N, C_S) \arrow[r] \arrow[d, "\alpha^0_{\mathrm{G}}(N)"'] & \mathrm{Hom}_{\mathcal{C}_U}(M, C_S) \arrow[r] \arrow[d, "\alpha^0_U(M)"'] & \mathrm{Hom}_{\mathcal{C}}(M, C_S) \arrow[r] \arrow[d, "\alpha^0_{\mathrm{G}}(M)"] & \cdots \arrow[d, "\wr"] \\
H^2_{ct}(\mathrm{G}, N)^* \arrow[r] & H^2_{ct}(U, M)^* \arrow[r] & H^2_{ct}(\mathrm{G}, M)^* \arrow[r] & \cdots .
\end{tikzcd}$$

All vertical maps are surjective, and they are isomorphisms after left three terms. Thus we get the following exact sequence:

$$\mathrm{Ker}(\alpha^0_{\mathrm{G}}(N)) \longrightarrow \mathrm{Ker}(\alpha^0_U(M)) \xrightarrow{N_{F/K}} \mathrm{Ker}(\alpha^0_{\mathrm{G}}(M)) \longrightarrow 0.$$

By the argument for trivial G–modules, we see

$$\mathrm{Ker}(\alpha^0_U(M)) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \mathrm{Ker}(rec_{S,F})).$$

Thus the kernel $\mathrm{Ker}(\alpha^0_{\mathrm{G}}(M))$ is the image of $\mathrm{Hom}_{\mathbb{Z}}(M, \mathrm{Ker}(rec_{S,F}))$ under the norm map. □

Exercises.

(1) Show that the sequence (3.7) is exact.

3.3. **Tate-Shafarevich groups.** Let S and K be as in the previous subsection. We fix a prime $p \in S$. We suppose the M is a finite discrete G_S–module with p–power order. Let $\Sigma = \Sigma_K$ be the set of places of K which induce places in S of $\mathbb{Q}$. For each $v \in \Sigma$, we write K_v (resp. $\overline{K_v}$) for the completion of K at v (resp. the algebraic closure of K_v), and let $D_v \subset \mathrm{G}$ be the decomposition group at v. When $v = \mathfrak{p}$ is a finite place, we put $H^r_{ct}(K_v, M) = H^r_{ct}(\mathrm{Gal}(\overline{K}_v/K_v), M)$; when v is a real place, we put $H^r_{ct}(K_v, M) = H^r_T(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), M)$ the Tate cohomology; and when v is a complex place, we just put $H^r_{ct}(K_v, M) = \{0\}$. We define

$$(W) \qquad W^r_S(K, M) = \mathrm{Ker}(\beta = \beta^r_S(M) : H^r_{ct}(\mathrm{G}_S, M) \to \prod_{v \in \Sigma} H^r_{ct}(K_v, M)),$$

where the map β is the product over $v \in \Sigma$ of the composites $\beta_v : H^r_{ct}(\mathrm{G}, M) \xrightarrow{res} H^r_{ct}(D_v, M) \xrightarrow{inf} H^r_{ct}(K_v, M)$. The terminology "Tate-Shafarevich group" is often used to indicate $W^r_S(K, M)$ when M is related to abelian varieties (or elliptic curves) defined over number fields. Here we call $W^r_S(K, M)$ for general M the Tate-Shafarevich groups, a bit abusing the language.

We then define $M^*(1) = \mathrm{Hom}_{\mathbb{Z}}(M, \mu_{p^\infty})$ as a G–module, where $\mu_{p^\infty} = \bigcup_\alpha \mu_{p^\alpha}$. Then $(M^*(1))^*(1) \cong M$ canonically. Note that $M^*(1) \cong \mathrm{Hom}_{\mathbb{Z}}(M, \overline{K}^\times)$ as D_v–modules. Then by the duality theorems: 3.3, 3.4 and 3.8 (1), we have the dual map of β

$$\gamma_S^r(M) = \beta^* : \prod_{v\in\Sigma} H^r_{ct}(K_v, M^*(1)) \to H^{2-r}_{ct}(\mathrm{G}_S, M)^*.$$

Theorem 3.9 (J. Tate, 1962)**.** *Let S be finite set of places of $\mathbb{Q}$ including the infinite place. Let K be a number field and Σ be the set of places of K above S. Fix a prime $p \in S$, and let M be a discrete finite G_S–module with p–power order. Then we have*

(1) *The Tate–Shafarevich groups $\text{Ш}^1_S(K, M)$ and $\text{Ш}^2_S(K, M^*(1))$ are finite, and there exists a canonical perfect pairing:*

$$\text{Ш}^1_S(K, M) \times \text{Ш}^2_S(K, M^*(1)) \to \mathbb{Q}_p/\mathbb{Z}_p$$

inducing Pontryagin duality between the two groups;

(2) *The map $\beta^0_S(M)$ is injective, $\gamma^2_S(M)$ is surjective, and we have the identity $\mathrm{Im}(\beta^r_S(M)) = \mathrm{Ker}(\gamma^r_S(M))$ for all $r = 0, 1, 2$;*

(3) *The map $\beta^r_S(M)$ induces a surjective isomorphism for all $r \geq 3$:*

$$H^r(\mathrm{G}_S, M) \cong \prod_{v\in\Sigma(\mathbb{R})} H^r_{ct}(K_v, M),$$

where $\Sigma(\mathbb{R})$ is the set of real places of K;

(4) *We have the following exact sequence:*

$$\begin{tikzcd}
0 \arrow[r] & H^0_{ct}(\mathrm{G}_S, M) \arrow[r, "\beta^0"] & \prod_{v\in\Sigma} H^0_{ct}(K_v, M) \arrow[r, "\gamma^0"] & H^2_{ct}(\mathrm{G}_S, M^*(1))^* \arrow[d] \\
& H^1_{ct}(\mathrm{G}_S, M^*(1)) \arrow[d] & \prod_{v\in\Sigma} H^1_{ct}(K_v, M) \arrow[l, "\gamma^1"'] & H^1_{ct}(\mathrm{G}_S, M) \arrow[l, "\beta^1"'] \\
& H^2_{ct}(\mathrm{G}_S, M) \arrow[r, "\beta^2"] & \prod_{v\in\Sigma} H^2_{ct}(K_v, M) \arrow[r, "\gamma^2"] & H^0_{ct}(\mathrm{G}_S, M^*(1))^* \arrow[r] & 0;
\end{tikzcd}$$

(5) *Let Σ_f be the subset of finite places in Σ. Let $B_v \subset H^1(K_v, M)$ be a submodule for each finite place $v \in \Sigma_f$, and let $B_v^\perp \subset H^1_{ct}(K_v, M^*(1))$ be the orthogonal complement of B_v under the pairing of Theorems 3.3 and 3.4. Suppose that $p > 2$ Then we have the following exact sequence:*

$$\begin{aligned}
0 \to H^1_B(K, M) \to H^1_{ct}(\mathrm{G}_S, M) \to \prod_{v\in\Sigma_f} H^1_{ct}(K_v, M)/B_v \to H^1_{B^\perp}(K, M^*(1))^* \\
\to H^2_{ct}(\mathrm{G}_S, M) \to \prod_{v\in\Sigma_f} H^2_{ct}(K_v, M) \to H^0_{ct}(\mathrm{G}_S, M^*(1))^* \to 0,
\end{aligned}$$

where

$$H^1_{B^\perp}(K, M^*(1)) = \beta^1_S(M^*(1))^{-1}(\prod_{v\in\Sigma_f} B_v^\perp) \text{ and } H^1_B(K, M) = \beta^1_S(M)^{-1}(\prod_{v\in\Sigma_f} B_v).$$

Proof. We again follow the treatment of Milne [ADT] I.4. We first treat the finiteness of $W^1_S(K,M)$. We only need to prove that $H^1_{ct}(\mathrm{G}_S,M)$ is finite. By the inflation-restriction sequence (and finiteness of M), we may assume that G acts trivially on M. Then $H^1_{ct}(\mathrm{G}_S,M)=\mathrm{Hom}_{ct}(\mathrm{G},M)$, which is finite by global class field theory (because S is a finite set). After proving the duality between $W^1_S(K,M)$ and $W^2_S(K,M^*(1))$, the finiteness of $W^2_S(K,M^*(1))$ follows from that of $W^1_S(K,M)$. The duality in question follows from the exact sequence of (4), because $W^2_S(K,M^*(1))=\mathrm{Coker}(\gamma^1_S(M))$.

We now prove the exact sequence of (4): Let $J_S=\varinjlim_F F_S^\times$ and $E_S=\varinjlim_F (O_F^S)^\times$, where F runs over all finite extensions of K inside K^S. Then by (3.7) and (3.8), we have the following short exact sequence of discrete G–modules:

$$0\to E_S\to J_S\to C_S\to 0.$$

Then we apply Proposition 1.9 to this sequence and get the following long exact sequence:

$$\begin{aligned}(3.9)\quad \cdots\to \mathrm{Ext}^0_{\mathcal{C}}(M^*(1),E_S)&\to \mathrm{Ext}^0_{\mathcal{C}}(M^*(1),J_S)\to \mathrm{Ext}^0_{\mathcal{C}}(M^*(1),C_S)\\ \to \mathrm{Ext}^1_{\mathcal{C}}(M^*(1),E_S)&\to \mathrm{Ext}^1_{\mathcal{C}}(M^*(1),J_S)\to \mathrm{Ext}^1_{\mathcal{C}}(M^*(1),C_S)\\ \to \mathrm{Ext}^2_{\mathcal{C}}(M^*(1),E_S)&\to \mathrm{Ext}^2_{\mathcal{C}}(M^*(1),J_S)\to \mathrm{Ext}^2_{\mathcal{C}}(M^*(1),C_S)\to\cdots.\end{aligned}$$

We shall look into one by one the term of the above exact sequence and relate it with the corresponding term of the exact sequence of (4).

Since $\mathrm{Hom}_{\mathcal{C}}(X,Y)=H^0(\mathrm{G},\mathrm{Hom}_{\mathbb{Z}}(X,Y))$ for discrete G–modules X and Y, we see

$$\begin{aligned}\mathrm{Hom}_{\mathcal{C}}(M^*(1),E_S)&=\mathrm{Hom}_{\mathcal{C}}(\mathrm{Hom}_{\mathbb{Z}}(M,\mu_{p^\infty}),\mu_{p^\infty})\\ &=H^0(\mathrm{G},\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(M,\mu_{p^\infty}),\mu_{p^\infty}))=H^0(\mathrm{G},M).\end{aligned}$$

Take a totally complex (finite) Galois extension $F_{/K}$ inside K^S such that $\mathrm{Gal}(K^S/F)$ fixes $M^*(1)$ element by element. Then

$$\mathrm{Hom}_{\mathcal{C}}(M^*(1),J_S)=\mathrm{Hom}_{\mathbb{Z}[\mathrm{Gal}(F/K)]}(M^*(1),F_S^\times).$$

Then $F_S^\times=\prod_{\mathfrak{p}\in\Sigma}\prod_{\mathfrak{P}|\mathfrak{p}}F_{\mathfrak{P}}^\times$ and $\prod_{\mathfrak{P}|\mathfrak{p}}F_{\mathfrak{P}}^\times\cong\mathrm{Hom}_{\mathbb{Z}[D]}(\mathbb{Z}[\mathrm{Gal}(F/K)],F_{\mathfrak{P}}^\times)$, where D is the decomposition group of $\mathfrak{P}/\mathfrak{p}$. Shapiro's lemma Lemma 2.5 can be stated as:

$$\begin{aligned}(3.10)\quad \mathrm{Hom}_{\mathbb{Z}[H']}(\rho',\mathrm{Ind}_H^{H'}\chi)&=H^0_{ct}(H',\mathrm{Hom}_{\mathbb{Z}}(\rho',\mathrm{Ind}_H^{H'}\chi))\\ &\cong H^0_{ct}(H,\mathrm{Hom}_{\mathbb{Z}}(\rho'|_H,\chi))=\mathrm{Hom}_{\mathbb{Z}[H]}(\rho'|_H,\chi),\end{aligned}$$

Then we have

$$\mathrm{Hom}_{\mathcal{C}}(M^*(1),\mathrm{Hom}_{\mathbb{Z}[D]}(\mathbb{Z}[\mathrm{Gal}(F/K)],F_{\mathfrak{P}}^\times))\cong\mathrm{Hom}_{\mathbb{Z}[D]}(M^*(1),F_{\mathfrak{P}}^\times).$$

Since M is of p–power order, we have

$$\mathrm{Hom}_{\mathbb{Z}[D]}(M^*(1),F_{\mathfrak{P}}^\times)\cong\mathrm{Hom}_{\mathbb{Z}[D]}(M^*(1),\mu_{p^\infty})\cong H^0_{ct}(\mathrm{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}}),M).$$

By Lemma 3.10 which follows this proof, we can replace $\mathrm{Hom}_{\mathcal{C}}$ in the above argument by $\mathrm{Ext}^1_{\mathcal{C}}$, and we get

$$(3.11)\qquad \mathrm{Ext}^1_{\mathcal{C}}(M^*(1),J_S)\cong\prod_{v\in\Sigma}H^1_{ct}(K_v,M).$$

We now look into the terms of (3.9) involving E_S. Since we find in K^S any ℓ–th root of elements of $(O_F^S)^\times$ for $\ell \in S$, E_S is in particular p–divisible. Then by Proposition 2.12, we have

$$\mathrm{Ext}^q_{\mathcal{C}}(M^*(1), E_S) \cong H^q(\mathrm{G}, Hom(M^*(1), E_S)) \cong H^q(\mathrm{G}, M)$$

for all $q \geq 0$.

Replacing terms of (3.9) by the cohomology groups we have identified, we get the exactness of the following sequence:

$$\begin{tikzcd}
0 \to H^0_{ct}(\mathrm{G}_S, M) \arrow[r, "\beta^0"] & \prod_{v\in\Sigma} H^0_{ct}(K_v, M) \arrow[r, "\gamma^0"] & H^2_{ct}(\mathrm{G}_S, M^*(1))^* \arrow[d] \\
H^1_{ct}(\mathrm{G}_S, M^*(1)) \arrow[d] & \prod_{v\in\Sigma} H^1_{ct}(K_v, M) \arrow[l, "\gamma^1"'] & H^1_{ct}(\mathrm{G}_S, M) \arrow[l, "\beta^1"'] \\
H^2_{ct}(\mathrm{G}_S, M) & &
\end{tikzcd}$$

Replacing M by $M^*(1)$ and taking the Pontryagin dual (Corollary 3.8 (1)) of the first four terms of the above sequence, we get another exact sequence:

$$H^1_{ct}(\mathrm{G}_S, M^*(1)) \longrightarrow H^2_{ct}(\mathrm{G}_S, M) \xrightarrow{\beta^2} \prod_{v\in\Sigma} H^2_{ct}(K_v, M) \longrightarrow H^0_{ct}(\mathrm{G}_S, M^*(1))^* \longrightarrow 0.$$

This is the last five terms of the exact sequence in (4), and hence we have finished the proof of (4).

By Lemma 3.10 for $q \geq 2$, we have

$$\begin{aligned}
(3.12) \quad \cdots \to H^1_{ct}(\mathrm{G}, M) \to \prod_{v\in\Sigma} H^1_{ct}(K_v, M) \to H^1_{ct}(\mathrm{G}, M^*(1))^* \\
\to H^2_{ct}(\mathrm{G}, M) \to \prod_{v\in\Sigma} H^2_{ct}(K_v, M) \to H^0_{ct}(\mathrm{G}, M^*(1))^* \\
\to H^3_{ct}(\mathrm{G}, M) \to \prod_{v\in\Sigma(\mathbb{R})} H^3_{ct}(\mathrm{Gal}(\overline{K}_v/K_v), M) \to 0;
\end{aligned}$$

and

$$(3.13) \qquad H^q_{ct}(\mathrm{G}, M) \cong \prod_{v\in\Sigma(\mathbb{R})} H^q_{ct}(K_v, M) \quad \text{for all } q > 3.$$

The map: $\prod_{v\in\Sigma} H^2_{ct}(K_v, M) \to H^0_{ct}(\mathrm{G}, M^*(1))^*$ is surjective, because it is a dual of the injection: $H^0(\mathrm{G}, M) \hookrightarrow \prod_{v\in\Sigma} H^0(K_v, M)$. Thus (3.13) holds even for $q = 3$. This proves (1), (2), (3) and (4).

We now prove the last exact sequence (5). Since p is odd, $H^1(K_v, M) = 0$ if v is an archimedean place. We write down the last six terms of the exact sequence in (4):

$$\begin{aligned}
(3.14) \quad \cdots \to H^1_{ct}(\mathrm{G}, M) \to \prod_{v\in\Sigma_f} H^1_{ct}(K_v, M) \\
\to H^1_{ct}(\mathrm{G}, M^*(1))^* \to H^2_{ct}(\mathrm{G}, M) \to \prod_{v\in\Sigma_f} H^2_{ct}(K_v, M) \to H^0_{ct}(\mathrm{G}, M^*(1))^* \to 0.
\end{aligned}$$

We write simply $H^1_{ct}(M)$ for $H^1_{ct}(\mathrm{G}, M)$. From this, we get the following commutative diagram:

$$\begin{tikzcd}
 & \prod_{v\in\Sigma_f} B_v \arrow[r, phantom, "\cong"] \arrow[d] & \prod_{v\in\Sigma_f}\left(\frac{H^1_{ct}(K_v,M^*(1))}{B_v^{\perp}}\right)^* \arrow[d] & \\
H^1_{ct}(M) \arrow[r] \arrow[d, equal] & \prod_{v\in\Sigma_f} H^1_{ct}(K_v, M) \arrow[r] \arrow[d] & H^1_{ct}(M^*(1))^* \arrow[r] \arrow[d] & H^2_{ct}(M) \arrow[d, equal] \\
H^1_{ct}(M) \arrow[r] & \prod_{v\in\Sigma_f} \frac{H^1_{ct}(K_v,M)}{B_v} \arrow[r] & H^1_B(\mathrm{G}, M^*(1))^* \arrow[r] & H^2_{ct}(M),
\end{tikzcd}$$

in which middle line and all columns are exact. Then the desired exact sequence follows from a simple diagram chasing. □

We now need to prove the following lemma:

Lemma 3.10. *Let the notation be as in Theorem 3.9. Then we have*

$$\mathrm{Ext}^q_{\mathcal{C}}(M^*(1), J_S) \cong \prod_{v\in\Sigma} H^q_{ct}(K_v, M) \quad \textit{for all } q \geq 0.$$

Proof. The case $q = 0$ has been shown in the proof of the above theorem. So we may assume that $q \geq 1$. Let X be a G–module of finite type. For the category $\mathcal{C}$ of discrete G–modules, we note that

$$\mathrm{Ext}^\bullet_{\mathcal{C}}(X, J_S) = \varinjlim_{F\subset K^S} \mathrm{Ext}^\bullet_{\mathbb{Z}[\mathrm{Gal}(F/K)]}(X, J_S^{\mathrm{Gal}(K^S/F)}) = \varinjlim_{F\subset K^S} \mathrm{Ext}^\bullet_{\mathbb{Z}[\mathrm{Gal}(F/K)]}(X, F_S^\times), \tag{3.15}$$

where F runs over all finite Galois extensions of K inside K^S such that $\mathrm{Gal}(K^S/F)$ acts trivially on X. This follows from Remark 2.2. Let $v \in S$ and write $G = G_v = \mathrm{Gal}(\overline{K}_v/K_v)$ and $H = \mathrm{Gal}(\overline{F}_w/F_w)$ for a place w of F over v. We consider the extension group $Ext^r_{Gal(F/K)}(X, I)$ for $I = \prod_{w|v} F_w^\times \cong \mathrm{Ind}_D^{\mathrm{Gal}(F/K)} P^H$ with $P = \overline{K}_v^\times$, where $D = G/H$ is the decomposition group of the place w. We take a resolution $X^\bullet \twoheadrightarrow X$ of free $\mathrm{Gal}(F/K)$–modules. Then $X^\bullet \twoheadrightarrow X$ is also a free resolution of D–modules. Then we have

$$\mathrm{Ext}^q_{Gal(F/K)}(X, I) = H^q(\mathrm{Hom}_{\mathrm{Gal}(F/K)}(X^\bullet, I)) \cong H^q(\mathrm{Hom}_D(X^\bullet, P^H)) = \mathrm{Ext}^q_D(X, P^H).$$

The middle isomorphism follows from the Shapiro's lemma (see (2.4)).

Now suppose $q = 1$. By Hilbert's theorem 90, we have the vanishing: $H^1(H, P) = 0$. Thus from Theorem 2.16, we get $\mathrm{Ext}^1_D(X, P^H) \cong \mathrm{Ext}^1_G(X, P^H)$. Thus we get by (3.15)

$$\mathrm{Ext}^1_{\mathcal{C}}(X, J_S) \cong \prod_{v\in\Sigma} \mathrm{Ext}^1_{G_v}(X, \overline{K}_v^\times).$$

By Proposition 2.12, we have

$$\mathrm{Ext}^1_{\mathcal{C}_{G_v}}(X, \overline{K}_v^\times) \cong H^1_{ct}(K_v, X^*(1)).$$

This shows the assertion for $q = 1$.

We now treat the case $q = 2$. We now change the notation and write D for the decomposition group of v in G_S. Write $D = G/H$. Then H is a closed normal subgroup of G but is not open. Let U be an open normal subgroup of G. Since the pair (HU, P) satisfies the axiom of class formation (see Example 3.1), by (CF2), we have

$$H^2_{ct}(H, P)[p^\infty] = \varinjlim_U H^2(H/U \cap H, P^{UH})[p^\infty]$$
$$= \varinjlim_U H^2(HU/U, P^U)[p^\infty] = \varinjlim_U \frac{1}{[HU : U]}\mathbb{Z}_p/\mathbb{Z}_p,$$

where U runs over open normal subgroups of H, $[p^\infty]$ indicates p–torsion part, and the last limit is taken with respect to the map $i_{U,V} : \frac{1}{[HU:U]}\mathbb{Z}_p/\mathbb{Z}_p \to \frac{1}{[HV:V]}\mathbb{Z}_p/\mathbb{Z}_p$ given by

$$i_{U,V}(x) = [UH : VH]x.$$

Since $p \in S$, for any given p–power p^r, we find $V \subset U$ such that $p^r | [HU : HV]$. Thus the last injective limit in the above equation vanishes, and hence

$$H^2_{ct}(H, P)[p^\infty] = 0 \text{ for } q = 2 \text{ and } H^1_{ct}(H, P) = 0$$

by Hilbert's theorem 90. We write $\mathcal{C}_G$ (resp. $\mathcal{C}_D$) for the category of discrete G–modules (resp. discrete D–modules).

Let $P \hookrightarrow I \twoheadrightarrow S$ be a $\mathcal{C}_G$–injective presentation chosen so that $P^H \hookrightarrow I^H \twoheadrightarrow S^H$ is an $\mathcal{C}_D$–injective presentation (as chosen in the proof of Theorem 2.16). We recall the exact sequence (2.14) in the proof of Theorem 2.16:

$$0 \longrightarrow \mathrm{Ext}^1_{\mathcal{C}_D}(X, S^H) \xrightarrow{inf} \mathrm{Ext}^1_{\mathcal{C}_G}(X, S) \xrightarrow{\delta} \mathrm{Hom}_{\mathcal{C}_G}(X, H^1(H, S)).$$

Since we have $H^2_{ct}(H, P) \cong H^1_{ct}(H, S)$, we have $H^1_{ct}(H, S)[p^\infty] \cong H^2_{ct}(H, P)[p^\infty] = 0$. Since we have also

$$\mathrm{Ext}^q_{\mathcal{C}_G}(X, P) \cong \mathrm{Ext}^{q-1}_{\mathcal{C}_G}(X, S) \text{ and } \mathrm{Ext}^q_{\mathcal{C}_D}(X, P^H) \cong \mathrm{Ext}^{q-1}_{\mathcal{C}_G}(X, S^H),$$

if X is of p-power order, we have

$$\mathrm{Hom}_{\mathcal{C}_G}(X, H^1(H, S)) = \mathrm{Hom}_{\mathcal{C}_G}(X, H^1(H, S)[p^\infty]) = 0.$$

Thus, we get

$$\mathrm{Ext}^2_{\mathcal{C}_D}(X, P^H) \cong \mathrm{Ext}^2_{\mathcal{C}_G}(X, P^H),$$

and by Proposition 2.12, we have shown the desired assertion.

For $q > 2$, we need to work more. Let $\mu \subset \overline{K}_v^\times = P$ be the group of all roots of unity. We decompose $\mu = \mu_{p^\infty} \times \mu^{(p)}$. We put $Q = \mu^{(p)} \backslash P$. Note that

$$\mathrm{Ext}^q_{\mathcal{C}_G}(X, \mu^{(p)}) = \varinjlim_{p \nmid N} \mathrm{Ext}^q_{\mathcal{C}_G}(X, \mu_N),$$

and hence $\mathrm{Ext}^q_{\mathcal{C}_G}(X, \mu_N)$ is killed by N, because the multiplication by N on μ_N factors through the trivial group 0. Thus $\mathrm{Ext}^q_{\mathcal{C}_G}(X, \mu^{(p)})$ is a prime-to-p torsion module. If

X is of p–power torsion, $\mathrm{Ext}^q_{\mathcal{C}_G}(X,\mu^{(p)})$ is a p–power torsion, and hence we conclude $\mathrm{Ext}^q_{\mathcal{C}_G}(X,\mu^{(p)})=0$. This applied to the (extension) long exact sequence shows

$$\mathrm{Ext}^q_{\mathcal{C}_G}(X,P)\cong\mathrm{Ext}^q_{\mathcal{C}_G}(X,Q). \tag{3.16}$$

We also have an exact sequence $0\to H^0(H,\mu^{(p)})\to P^H\xrightarrow{\pi}Q^H\to H^1_{ct}(H,\mu^{(p)})$. Thus $Q^H/\operatorname{Im}(\pi)$ is prime-to–p torsion. This shows that $\mathrm{Ext}^q_{\mathcal{C}_D}(X,Q^H/\operatorname{Im}(\pi))=0$ for all q if X is p–torsion, and hence

$$\mathrm{Ext}^q_{\mathcal{C}_D}(X,Q^H)\cong\mathrm{Ext}^q_{\mathcal{C}_D}(X,\operatorname{Im}(\pi))\ \text{ and }\ \mathrm{Ext}^q_{\mathcal{C}_D}(X,\operatorname{Im}(\pi))\cong\mathrm{Ext}^q_{\mathcal{C}_D}(X,P^H).$$

Thus we get, if X is a p–torsion D–module,

$$\mathrm{Ext}^q_{\mathcal{C}_D}(X,P^H)\cong\mathrm{Ext}^q_{\mathcal{C}_D}(X,Q^H). \tag{3.17}$$

From the cohomology long exact sequence, we have the following exact sequence:

$$H^q_{ct}(H,P)\longrightarrow H^q_{ct}(H,Q)\longrightarrow H^q_{ct}(H,\mu^{(p)}).$$

This shows that $H^q_{ct}(H,Q)$ is p–torsion-free and is a torsion module for $q=1$ and $q>2$ by the local duality theorem. For $q=2$, by the above result, $H^2_{ct}(H,P)$ is p–torsion-free and is torsion, the same result holds.

$$H^q_{ct}(H,Q)[p^\infty]=0 \text{ and } H^q_{ct}(H,Q) \text{ is a torsion module for all } q. \tag{3.18}$$

In 2.3, to make an injective presentation: $Y\hookrightarrow I_Y\twoheadrightarrow S_Y$ for a given module Y, we used the product of injective modules: $\mathrm{Hom}_{\mathbb{Z}}(Y,\mathbb{Q}/\mathbb{Z})$. If $y\mapsto Ny$ is an automorphism of Y for all integer N prime to p, we can also use $\mathbb{Q}_p/\mathbb{Z}_p$ in place $\mathbb{Q}/\mathbb{Z}$, because for any given $y\in Y$, we have a homomorphism $\phi_y:Y\to\mathbb{Q}_p/\mathbb{Z}_p$ with $\phi_y(y)\neq 0$ (this fails when y is a prime-to-p torsion element). Thus we may assume that we have an injective presentaion $Q\hookrightarrow I\twoheadrightarrow S$ such that

(1) I is a p–torsion module (and hence so is S);
(2) I^H is an injective D–module.

By $H^1_{ct}(H,Q)[p^\infty]=0$ combined with p–torsion of S^H, we have the exact sequence:

$$0\longrightarrow Q^H\longrightarrow I^H\longrightarrow S^H\longrightarrow 0.$$

From this, we get, for any p–torsion D–module X,

$$\mathrm{Ext}^q_{\mathcal{C}_G}(X,Q)\cong\mathrm{Ext}^{q-1}_{\mathcal{C}_G}(X,S),\quad \mathrm{Ext}^q_{\mathcal{C}_D}(X,Q^H)\cong\mathrm{Ext}^{q-1}_{\mathcal{C}_G}(X,S^H)$$
$$\text{and } H^q_{ct}(H,Q)\cong H^{q-1}_{ct}(H,S),$$

and moreover S is a p–torsion module. Then by an argument similar to the proof of Theorem 2.16, we get

$$\mathrm{Ext}^q_{\mathcal{C}_G}(X,Q)\cong\mathrm{Ext}^q_{\mathcal{C}_D}(X,Q^H).$$

This combined with (3.16) and (3.17) shows

$$\mathrm{Ext}^q_{\mathcal{C}_G}(X,P)\cong\mathrm{Ext}^q_{\mathcal{C}_D}(X,P^H),$$

as long as X is a p–torsion finite module. Then Proposition 2.12 tells us

$$\mathrm{Ext}^q_{\mathcal{C}_G}(X,P)\cong H^q_{ct}(G,X^*(1)).$$

From this, we conclude the desired assertion. □

3.4. **Local Euler characteristic formula.** Let $K/\mathbb{Q}_p$ be a finite extension for a prime p. Let $|\ |_K$ be the p–adic absolute value normalized so that $|p|_K = [O_K : pO_K]^{-1}$ for the p–adic integer ring O_K of K. We would like to prove the following theorem in this subsection:

Theorem 3.11 (J. Tate, 1962)**.** *Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$ and M be a finite (discrete) G–module. Then we have*

$$\frac{|H^0_{ct}(G,M)|\cdot|H^2_{ct}(G,M)|}{|H^1_{ct}(G,M)|} = \frac{|H^0_{ct}(G,M)|\cdot|H^0_{ct}(G,M^*(1))|}{|H^1_{ct}(G,M)|} = \big||M|\big|_K.$$

Proof. In the proof, we simply write $H^q(M)$ for $H^q_{ct}(G,M)$. Since $M = \oplus_\ell M[\ell^\infty]$ for primes ℓ, we may assume that M has an ℓ–power order for a prime ℓ. Then $H^q(M)$ is a $\mathbb{Z}_\ell$–module of finite length. Here length(M) is the length of the Jordan-Hölder sequence of the $\mathbb{Z}_\ell$–module M. Thus $|M| = \ell^{\mathrm{length}(M)}$.

We define the local Euler characteristic of M by

$$\chi(M) = \chi(G,M) = \sum_{j=0}^{2}(-1)^j \,\mathrm{length}(H^j(M))$$

$$\chi'(M) = \chi'(G,M) = \log_p(\big||M|\big|_K) = \begin{cases}[K:\mathbb{Q}_p]\,\mathrm{length}_{\mathbb{Z}_p} M & \text{if } \ell = p,\\ 0 & \text{if } \ell \neq p.\end{cases}$$

Note that the left-hand-side of the formula is just $p^{\chi(M)}$ and the right-hand-side is $p^{\chi'(M)}$; so, we need to prove that $\chi(M) = \chi'(M)$. Let K/L be a finite extension, and write $H = \mathrm{Gal}(\overline{\mathbb{Q}}_p/L)$. By Shapiro's lemma Lemma 2.5,

$$H^q_{ct}(G,M) \cong H^q_{ct}(H, \mathrm{Ind}_G^H M),$$

where $\mathrm{Ind}_G^H M = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}[H], M)$. Since

$$|\,\mathrm{Ind}_G^H M| = |M|^{[K:L]},$$

we have

$$\chi(G,M) = \chi(H, \mathrm{Ind}_G^H M). \tag{3.19}$$

It is easy to see that $\chi'(N) = \chi'(M) + \chi'(L)$ if $0 \to M \to N \to L \to 0$ is an exact sequence of finite G–modules. Thus $\chi'(M) = \chi'(M^{ss})$, where $M^{ss} = \oplus_{j=1}^{\infty} M_j/M_{j-1}$ for a Jordan-Hölder sequence $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ of $\mathbb{Z}_\ell[G]$–modules.

We see easily that if

$$0 \to E_1 \to E_2 \to \cdots \to E_n \to 0$$

is an exact sequence of finite $\mathbb{Z}_\ell$–modules,

$$\prod_j |E_j|^{(-1)^j} = 1 \iff \sum_j (-1)^j \,\mathrm{length}(E_j) = 0. \tag{3.20}$$

If $0 \to M \to N \to L \to 0$ is an exact sequence of finite $\mathbb{Z}_\ell[G]$–modules, we have a long exact sequence:

$$\begin{aligned} 0 \to H^0(M) \to H^0(N) \to H^0(L) & \\ \to H^1(M) \to H^1(N) \to H^1(L) & \to H^2(M) \to H^2(N) \to H^2(L) \to 0. \end{aligned}$$

The sequence is of finite length, since $H^q(M) = 0$ if $q > 2$, and all cohomology groups are finite $\mathbb{Z}_\ell$–modules, both by Theorem 3.3. Then by (3.20), we see $\chi(N) = \chi(M) + \chi(L)$ and therefore $\chi(M) = \chi(M^{ss})$. Since M^{ss} is a $\mathbb{F}[G]$–module for $\mathbb{F} = \mathbb{Z}/\ell\mathbb{Z}$, we may assume that M itself is a $\mathbb{F}[G]$–module. Thus hereafter, we assume that all G–modules are $\mathbb{F}[G]$–modules, and we regard χ and χ' as functions on the Grothendieck group $R_\mathbb{F}(G)$ with values in $\mathbb{Z}$. Thus we need to check the formula for a set of generators of $R_\mathbb{F}(G) \otimes_\mathbb{Z} \mathbb{Q}$.

We first check the formula for the trivial $\mathbb{F} = \mathbb{Z}/\ell\mathbb{Z}$. We see

$$\dim_\mathbb{F} H^0(G, \mathbb{F}) = 1 \quad \text{and} \quad \dim_\mathbb{F} H^2(G, \mathbb{F}) = \dim_\mathbb{F} H^0(G, \mu_\ell) = \dim_\mathbb{F} \mu_\ell(K),$$

where $\mu_\ell(K) = \{z \in K | z^\ell = 1\}$. On the other hand, by local class field theory,

$$(3.21)\quad H^1_{ct}(G, \mathbb{F}) = \mathrm{Hom}_{ct}(G^{ab}, \mathbb{F}) \cong K^\times/(K^\times)^\ell \;\text{ and }\; H^1_{ct}(G, \kappa) \cong \big(K^\times/(K^\times)^\ell\big) \otimes_\mathbb{F} \kappa$$

for a finite extension $\kappa/\mathbb{F}$. Since $K^\times \cong O^\times \times \mathbb{Z}$ for the p–adic integer ring O of K and $O^\times \cong O \times \mu_\ell(K)$ up to prime-to-ℓ torsion,

$$H^1_{ct}(G, \mathbb{F}) \cong \begin{cases} \mathbb{Z}/\ell\mathbb{Z} \oplus \mu_\ell(K) & \text{if } \ell \neq p, \\ O/pO \oplus \mathbb{Z}/p\mathbb{Z} \oplus \mu_p(K) & \text{if } \ell = p. \end{cases}$$

This shows the formula holds for $\mathbb{Z}/\ell\mathbb{Z}$ and hence for any trivial G–module. By the duality (Theorem 3.3), the formula also holds for $M = \mu_\ell = \mathbb{F}^*(1)$.

We take a finite Galois extension F/K such that $\mathrm{Gal}(\overline{\mathbb{Q}}_p/F)$ acts trivially on M. Write $\overline{G} = \mathrm{Gal}(F/K)$. Then by a well known result of E. Artin (cf. [MFG] Corollary 2.11), $R_\mathbb{F}(\overline{G}) \otimes_\mathbb{Z} \mathbb{Q}$ is generated by $\mathrm{Ind}_{\overline{H}}^{\overline{G}} \rho$ for cyclic subgroups $\overline{H}$ of order prime to ℓ and characters $\rho : \overline{H} \to \kappa^\times$ for a finite extension $\kappa/\mathbb{F}$. Thus we may assume that $M = \mathrm{Ind}_{\overline{H}}^{\overline{G}} \rho$. Then by (3.19), we only need to check the Euler characteristic formula for ρ (or for the one dimensional module $V = V(\rho)$ on which $\overline{H}$ acts via ρ). Thus replacing K by the fixed field $\overline{H}$, we may assume that $M = V(\rho)$ is one dimensional over a finite extension κ of $\mathbb{F}$ and that F/K is cyclic of degree prime to ℓ. Then $H^q(\overline{G}, M) = 0$ for all $q > 0$, and for $G' = \mathrm{Gal}(\overline{\mathbb{Q}}_p/F)$, by the inflation and restriction sequence, we have

$$H^q(G, M) \cong H^0(\overline{G}, H^q(G', M)) \quad \text{for } q = 0, 1, 2,$$

and we note

$$H^q(G', M) = \begin{cases} \kappa & \text{if } q = 0 \\ H^1_{ct}(G', \kappa) = \{F^\times/(F^\times)^\ell\} \otimes_\mathbb{F} \kappa & \text{if } q = 1 \\ H^2_{ct}(G', \kappa) = H^0(G', \kappa^*(1)) = \mu_p(F) \otimes_\mathbb{F} \kappa & \text{if } q = 2. \end{cases}$$

Thus writing ρ–eigenspace of $\kappa[\overline{G}]$–module X as $X[\rho]$, we see

$$\chi(G,M)=\dim_{\mathbb{F}}\kappa[\rho]-\dim_{\mathbb{F}}\{(F^\times/(F^\times)^\ell)\otimes_{\mathbb{F}}\kappa\}[\rho]+\dim_{\mathbb{F}}(\mu_\ell(F)\otimes_{\mathbb{F}}\kappa)[\rho],$$

because $H^0(\overline{G},H^q(G',M))\cong H^q(G',M)[\rho]$ by the definition of the action of $\overline{G}$ on cohomology groups of G' (one can check it by using inhomogeneous continuous cochains). Since we have already checked the result for $M=\mathbb{F}$ and $M=\mu_\ell$, we may assume that ρ is neither the trivial character nor the cyclotomic character. Therefore $\kappa[\rho]=(\mu_p(F)\otimes_{\mathbb{F}}\kappa)[\rho]=0$, because the action of the Galois group on κ is trivial and on μ_p is via the cyclotomic character.

We treat the case where $\ell=p$, leaving the case where $\ell\neq p$ to the reader as an exercise. Then

$$\chi(G,M)=-\dim_{\mathbb{F}}\left(\{(F^\times/(F^\times)^p)\otimes_{\mathbb{F}}\kappa\}[\rho]\right).$$

Thus we need to show that

$$[K:\mathbb{Q}_p]\dim_{\mathbb{F}}M=\dim_{\mathbb{F}}\left(\{(F^\times/(F^\times)^p)\otimes_{\mathbb{F}}\kappa\}[\rho]\right),$$

because $\big|\big|M\big|\big|_K=p^{-[K:\mathbb{Q}_p]\dim_{\mathbb{F}}M}$. Writing the additive valuation of F as $v:F^\times\twoheadrightarrow\mathbb{Z}$, we have an exact sequence:

$$1\to U/\mu\to F^\times/\mu\xrightarrow{v}\mathbb{Z}\to 0,$$

where $U=O_F^\times$ and μ is the maximal torsion-subgroup of $F^\times$. Then the above exact sequence is torsion-free, and after tensoring κ, we still have an exact sequence:

$$0\to(U/\mu)\otimes_{\mathbb{Z}}\kappa\to(F^\times/\mu)\otimes_{\mathbb{Z}}\kappa\xrightarrow{v}\kappa\to 0.$$

Taking the ρ–isotypical component (after tensoring κ), we get

$$\{(U/U^p)\otimes_{\mathbb{F}}\kappa\}[\rho]\cong\{(U/\mu)\otimes_{\mathbb{Z}}\kappa\}[\rho]\cong\{(F^\times/\mu)\otimes_{\mathbb{Z}}\kappa\}[\rho].$$

Now we want to lift the representation ρ to characteristic 0 representation $\widetilde{\rho}$. For that, we take a unique unramified extension L of $\mathbb{Q}_p$ of degree $\dim_{\mathbb{F}}\kappa$. Let W be the p–adic integer ring of L. Then we have $W/(p)\cong\kappa$ and hence, $W^\times\cong(1+pW)\times\kappa^\times$. Using this isomorphism, we may think ρ as having values in $W^\times$ (and also in L). This new character, we write as $\widetilde{\rho}:\overline{G}\to W^\times$, which is called the Teichmüller lift of ρ.

Since (U/μ) is torsion-free and the order of $\overline{G}$ is prime to p,

$$\dim_{\mathbb{F}}\{(U/\mu)\otimes_{\mathbb{Z}}\kappa\}[\rho]=\operatorname{rank}_{\mathbb{Z}_p}\{(U/\mu)\otimes_{\mathbb{Z}}W\}[\widetilde{\rho}]$$

for the unique Teichmüller lift $\widetilde{\rho}$ of ρ. By p–adic logarithm, $(U/\mu)\otimes_{\mathbb{Z}}\mathbb{Q}\cong F$ as $\overline{G}$–modules; so, by the normal base theorem $F\cong K[\overline{G}]\cong(\mathbb{Q}_p[\overline{G}])^{[K:\mathbb{Q}_p]}$ as $\overline{G}$–modules. This shows that

$$[K:\mathbb{Q}_p]\dim_{\mathbb{F}}M=[K:\mathbb{Q}_p]\dim_{\mathbb{F}}\rho=\dim_{\mathbb{F}}\left(\{(F^\times/(F^\times)^p)\otimes_{\mathbb{F}}\kappa\}[\rho]\right)$$

as desired.

The case where $\ell\neq p$ can be treated similarly (it is much easier than the case where $\ell=p$) and is left to the reader (Exercise 1). □

Exercises.

(1) Give a detailed proof of Theorem 3.4 when $|M|$ is prime to p.
(2) Prove (3.19).

3.5. **Global Euler characteristic formula.** We use the notation introduced in 3.2 and 3.3. Let M be a finite G_S–module with ℓ–power order for $\ell \in S$. We define the global Euler characteristic of M by

$$\chi(M) = \chi(\mathrm{G}_S, M) = \sum_{q=0}^{2} (-1)^q \operatorname{length}_{\mathbb{Z}_\ell} H^q_{ct}(\mathrm{G}_S, M). \tag{3.22}$$

We would like to prove

Theorem 3.12 (J. Tate, 1965)**.** *Let Σ_∞ be the set of archimedean places of K. We have*

$$\chi(\mathrm{G}_S, M) = \sum_{v \in \Sigma_\infty} \left(\operatorname{length}_{\mathbb{Z}_\ell} H^0(\mathrm{Gal}(\overline{K}_v/K_v), M) - [K_v : \mathbb{R}] \operatorname{length}_{\mathbb{Z}_\ell} M \right).$$

Proof. We follow the proof of Milne given in [ADT] I.5. Let $\varphi(M)$ be the difference of the above formula, and write $\chi(M) = \chi(\mathrm{G}_S, M)$. Thus we need to prove

$$\varphi(M) = 0.$$

We shall prove the theorem here assuming $\ell > 2$. We give a sketch of a proof for $\ell = 2$ later (see Remark 3.1). For simplicity, we write $H^q(M)$ (resp. $H^q_v(M))$) for the cohomology group $H^q_{ct}(\mathrm{G}, M)$ (resp. $H^q(\mathrm{Gal}(\overline{K}_v/K_v), M)$). By Theorem 3.9 (3),

$$H^q(M) \cong \prod_{v \in \Sigma_\infty} H^q_v(M)$$

for $q \geq 3$. Thus if $\ell > 2$, $H^q(M) = 0$ for all $q \geq 3$ (see Proposition 2.4). For each short exact sequence: $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$ of finite $\mathbb{Z}_\ell[\mathrm{G}_S]$–modules, we have the long exact sequence:

$$\begin{aligned} 0 \to H^0(L) \xrightarrow{\alpha_1} H^0(M) \xrightarrow{\beta_1} H^0(N) \to \cdots \\ \to H^2(L) \xrightarrow{\alpha_4} H^2(M) \xrightarrow{\beta_4} H^2(N) \to 0. \end{aligned} \tag{3.23}$$

Thus if $\ell > 2$, $\chi(L) + \chi(N) = \chi(M)$ and hence $\varphi(L) + \varphi(N) = \varphi(M)$, because $M \mapsto \operatorname{length}_{\mathbb{Z}_\ell} H^0_v(M)$ for $v \in \Sigma_\infty$ and $M \mapsto \operatorname{length}_{\mathbb{Z}_\ell} M$ are both additive (on the Grothendieck group $R_{\mathbb{F}}(\mathrm{G})$).

Therefore χ and φ factor through the Grothendieck group $R_{\mathbb{F}}(\mathrm{G})$ for $\mathbb{F} = \mathbb{Z}/\ell\mathbb{Z}$ and have values in $\mathbb{Q}$. By Theorem 3.9 (1) and Theorem 3.3, all the terms of the exact sequence of Theorem 3.9 (4) are finite. Then by (3.20), we get

$$\chi(M) + \chi(M^*(1)) = \sum_{v \in \Sigma} \chi_v(G_v, M),$$

where $\chi_v(G_v, M)$ is the local Euler characteristic

$$\chi(G_v, M) = \sum_{q=0}^{2} (-1)^q \operatorname{length}_{\mathbb{Z}_\ell} H^q_{ct}(G_v, M)$$

defined for $G_v = \mathrm{Gal}(\overline{K}_v/K_v)$. Thus by Theorem 3.4 (2) and Theorem 3.11,

$$\sum_{v\in\Sigma}\chi_v(G_v, M) = \log_\ell\left(\prod_{v\in\Sigma}\big||M|\big|_{K_v}\right).$$

Since $\big||M|\big|_{K_v} = 1$ for $v \notin \Sigma$, by the product formula:

$$\prod_{v\in\Sigma}\big||M|\big|_{K_v} = \prod_{v}\big||M|\big|_{K_v} = 1,$$

we know that

$$\chi(M) + \chi(M^*(1)) = 0 \quad \text{and} \quad \varphi(M) + \varphi(M^*(1)) = 0.$$

We now prove that $\varphi(M) = \varphi(M^*(1))$, which will finish the proof. We take a finite Galois extension F/K such that $\mathfrak{H} = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ acts trivially on M and μ_ℓ. We write $\overline{G} = \mathrm{Gal}(F/K)$. By the same argument as in the proof of Theorem 3.11, we may assume that F/K is cyclic of degree prime to ℓ. The field F is totally imaginary; so, by Theorem 3.9 (3), $H^q_F(M) = H^q_{ct}(\mathfrak{H}, M) = 0$ if $q \geq 3$. Since $H^q_F(M)$ is a finite $\mathbb{Z}_\ell[\overline{G}]$–module (see the definition of the action just above Theorem 2.15). Thus $[M] \mapsto \sum_{q=0}^{2}(-1)^q[H^q_F(M)]$ defines an additive endomorphism χ' of $R_{\mathbb{F}}(\overline{G})$ for $\mathbb{F} = \mathbb{Z}/\ell\mathbb{Z}$. Similarly, $[M] \mapsto [M^*] = [\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{F})]$ defines an involution of $R_{\mathbb{F}}(\overline{G})$. We claim the following facts:

$$\chi'(M^*(1)) = [M^*] \cdot \chi'(\mu_\ell); \tag{1}$$
$$[M] \cdot [\mathbb{F}[\overline{G}]] = \dim_{\mathbb{F}}(M)[\mathbb{F}[\overline{G}]]. \tag{2}$$

Here $[M] \cdot [N] = [M \otimes_{\mathbb{F}} N]$ and $\overline{G}$ acts diagonally on $M \otimes_{\mathbb{F}} N$. Since $\mathfrak{H} = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ acts trivially on μ_ℓ and M, we see that $M \otimes_{\mathbb{F}} \mu_\ell \cong \mu_\ell^{\dim M}$ as $\mathfrak{H}$–modules. The action of $\overline{G}$ is given by $\sigma u(h) = \sigma(u(\sigma^{-1}h\sigma))$ for cocycle $u : \mathfrak{H}^q \to M$ and $\sigma \in$ G. Fixing a base of M, write the action of $\sigma \in \overline{G}$ on M as a matrix form $\rho_M(\sigma)$. We identify the two $\mathbb{F}$–vector spaces M and $\mu_\ell^{\dim M}$ via this base. Thus the matrix $\rho_M(\sigma)$ still acts on $\mu_\ell^{\dim M}$. Then $\overline{G}$ acts on $\mu_\ell^{\dim M}$ by $\sigma v = \rho_M(\sigma)\omega(\sigma)v$ for the (mod ℓ) Teichmüller character ω. From this, it is clear that

$$H^q_F(\mu_\ell \otimes_{\mathbb{F}} M) = H^q_F(\mu_\ell) \otimes_{\mathbb{F}} M$$

as $\overline{G}$–modules. This shows the first statement. The second follows from the isomorphism:

$$M^\circ \otimes_{\mathbb{F}} \mathbb{F}[\overline{G}] \cong M \otimes_{\mathbb{F}} \mathbb{F}[\overline{G}]$$

given by $m \otimes \sigma \mapsto \sigma m \otimes \sigma$, where M° is the trivial $\overline{G}$–module with $M^\circ \cong M$ as $\mathbb{F}$–vector spaces.

We define $\theta : R_{\mathbb{F}}(\overline{G}) \to \mathbb{Z}$ by $\theta([M]) = \dim_{\mathbb{F}} H^0(\overline{G}, M)$. Since $|\overline{G}|$ is prime to ℓ, $M \mapsto H^0(\overline{G}, M)$ preserves short exact sequences of $\mathbb{F}[\overline{G}]$–modules, and hence θ extends to a homomorphism of $R_{\mathbb{F}}(\overline{G})$ into $\mathbb{Z}$. Since $|\overline{G}|$ is prime to ℓ, $H^q(\overline{G}, M) = 0$ for all $q > 0$, and hence, by the inflation and restriction sequence Theorem 2.15,

$H^q(M) \cong H^0(\overline{G}, H^q_F(M))$. Thus $\chi(M) = \theta(\chi'([M]))$. Then from the above two claims and $\mathbb{F}[\overline{G}] \cong \mathbb{F}[\overline{G}]^*$ as $\mathbb{F}[\overline{G}]$–modules, we find

$$\chi'(M^*(1)) \cdot [\mathbb{F}[\overline{G}]^*] = [M^*] \cdot [\mathbb{F}[\overline{G}]] \cdot \chi'(\mu_\ell) = \dim_{\mathbb{F}}(M)[\mathbb{F}[\overline{G}]^*] \cdot \chi'(\mu_\ell).$$

Since $\dim_{\mathbb{F}} M = \dim_{\mathbb{F}} M^*(1)$, the right-hand-side of the above formula is the same even if we replace M in the left-hand-side by $M^*(1)$. Thus this shows that $\chi(M) = \chi(M^*(1))$, which implies $\varphi(M) = \varphi(M^*(1))$. This finishes the proof. □

Remark 3.1. When $\ell = 2$, the above argument works well except for the fact that $\ell > 2$ is used to show the additivity of φ with respect to short exact sequences. Thus we need to modify the proof of $\varphi(M) = \varphi(N) + \varphi(L)$ for short exact sequences $0 \to L \xrightarrow{\alpha} M \xrightarrow{\beta} N \to 0$. By definition, we have

$$\varphi(M) = \chi(M) - \sum_{v \in \Sigma_\infty} \left(\mathrm{length}_{\mathbb{Z}_\ell} H^0(\mathrm{Gal}(\overline{K}_v/K_v), M) - [K_v : \mathbb{R}]\,\mathrm{length}_{\mathbb{Z}_\ell} M\right).$$

Then we truncate the long exact sequence associated to the short exact sequence as follows:

$$(3.24) \quad 0 \to H^0(L) \xrightarrow{\alpha_1} H^0(M) \xrightarrow{\beta_1} H^0(N) \to \cdots$$
$$\to H^4(L) \xrightarrow{\alpha_4} H^4(M) \xrightarrow{\beta_4} H^4(N) \xrightarrow{\delta} \mathrm{Ker}(H^5(L) \xrightarrow{\alpha_5} H^5(M)) \to 0.$$

By Theorem 3.9 (3),

$$H^q(\mathrm{G}_S, M) \cong \prod_{v \in \Sigma_\infty} H^q_v(M)$$

for $q \geq 3$. Thus we have

$$\mathrm{Ker}(H^5(L) \xrightarrow{\alpha_5} H^5(M)) \cong \prod_{v \in \Sigma_\infty} C_v$$

for $C_v = \mathrm{Ker}(H^5_v(L) \xrightarrow{\alpha_{5,v}} H^5_v(M))$. Since $\mathrm{Gal}(\overline{K}_v/K_v)$ is cyclic of order 1 or 2, it is easy to see from Proposition 2.3 that

$$\mathrm{length}(H^3(\mathrm{G}_S, M)) = \mathrm{length}(H^4(\mathrm{G}_S, M)).$$

Thus by (3.24) (and (3.20)), we get

$$\chi(L) + \chi(N) = \chi(M) + \sum_{v \in \Sigma_\infty} \mathrm{length}(C_v),$$

and hence,

$$\varphi(L) + \varphi(N) - X(L) - X(N) = \varphi(M) - X(M)$$
$$+ \sum_{v \in \Sigma_\infty} \left(\mathrm{length}(C_v) - \mathrm{length}(H^0_v(L)) + \mathrm{length}(H^0_v(M)) - \mathrm{length}(H^0_v(N))\right),$$

where $X(M) = \sum_{v \in \Sigma_\infty} [K_v : \mathbb{R}]\,\mathrm{length}_{\mathbb{Z}_\ell} M$. Since $X(L) + X(N) = X(M)$, we need to prove the vanishing of

$$\left(\mathrm{length}(C_v) - \mathrm{length}(H^0_v(L)) + \mathrm{length}(H^0_v(M)) - \mathrm{length}(H^0_v(N))\right).$$

Again by the periodicity of cohomology groups of cyclic groups: Proposition 2.3, we see

$$C_v \cong \mathrm{Ker}(H^1_v(L) \xrightarrow{\alpha_{1,v}} H^1_v(M)).$$

We look at the local truncated exact sequence:

$$0 \to H^0_v(L) \to H^0_v(M) \to H^0_v(N) \to C_v \to 0,$$

which shows

$$\mathrm{length}(C_v) = \mathrm{length}(H^0_v(L)) - \mathrm{length}(H^0_v(M)) + \mathrm{length}(H^0_v(N))$$

as desired.

4. Appendix: Categories and Functors

In this section, we describe briefly the theory of categories to supply basics for our later study of Extension groups.

4.1. **Categories.** A *category* $\mathcal{C}$ consists of two data: objects of $\mathcal{C}$ and morphisms of $\mathcal{C}$. For any two objects X and Y of $\mathcal{C}$, we have a set $\mathrm{Hom}_{\mathcal{C}}(X,Y)$ of morphisms satisfying the following three rules:

(ct1) *For three objects X, Y, Z, there is a composition map:*

$$\mathrm{Hom}_{\mathcal{C}}(Y,Z) \times \mathrm{Hom}_{\mathcal{C}}(X,Y) \to \mathrm{Hom}_{\mathcal{C}}(X,Z) : (g,f) \mapsto g \circ f;$$

(ct2) *(Associativity). For three morphisms: $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$, we have $h \circ (g \circ f) = (h \circ g) \circ f$;*

(ct3) *For each object X, there is a specific element $1_X \in \mathrm{Hom}_{\mathcal{C}}(X,X)$ such that $1_X \circ f = f$ and $g \circ 1_X = g$ for all $f : Y \to X$ and $g : X \to Z$.*

For two objects X and Y in $\mathcal{C}$, we write $X \cong Y$ if there exist morphisms $f : X \to Y$ and $g : Y \to X$ such that $f \circ g = 1_Y$ and $g \circ f = 1_X$.

Example 4.1. Table of some categories used in this book:

Category	Objects	Morphisms
$SETS$	sets	maps between sets
AB	Abelian groups	group homomorphisms
ALG	Algebras	Algebra homomorphisms
A–ALG	A–algebras	A–algebra homomorphisms
$CL_{\mathcal{O}}$	pro-artinian $A \in \mathcal{O}$–ALG with $A/\mathfrak{m}_A = \mathcal{O}/\mathfrak{m}$	morphisms of local $\mathcal{O}$–algebras
A–MOD	A–modules	A–linear maps
G–$\mathcal{MOD}$	discrete G–modules for a profinite group G	continuous G–linear maps

A category $\mathcal{C}'$ is a *subcategory* of $\mathcal{C}$ if the following two conditions are satisfied:

(i) Each object of $\mathcal{C}'$ is an object of $\mathcal{C}$ and $\mathrm{Hom}_{\mathcal{C}'}(X,Y) \subset \mathrm{Hom}_{\mathcal{C}}(X,Y)$;

(ii) The composition of morphisms is the same in $\mathcal{C}$ and $\mathcal{C}'$.

A subcategory $\mathcal{C}'$ is called a *full* subcategory of $\mathcal{C}$ if $\mathrm{Hom}_{\mathcal{C}'}(X,Y) = \mathrm{Hom}_{\mathcal{C}}(X,Y)$ for any two objects X and Y in $\mathcal{C}'$.

4.2. **Functors.** A *covariant* (resp. *contravariant*) *functor* $F : \mathcal{C} \to \mathcal{C}'$ is a rule associating an object $F(X)$ of $\mathcal{C}'$ and a morphism $F(f) \in \mathrm{Hom}_{\mathcal{C}'}(F(X), F(Y))$ (resp. $F(f) \in \mathrm{Hom}_{\mathcal{C}'}(F(Y), F(X))$) to each object X of $\mathcal{C}$ and each morphism $f \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$ satisfying

$$\text{(F)} \quad F(f \circ h) = F(f) \circ F(h) \quad (\text{resp.} \quad F(f \circ h) = F(h) \circ F(f)) \qquad \text{and} \quad F(1_X) = 1_{F(X)}.$$

Example 4.2. Let G be a profinite group. Then the category G–$\mathcal{MOD}$ of discrete G–modules consists of discrete modules with continuous G–action and continuous G–linear maps. Then the association of the G–invariant submodule to each object in the category:

$$M \mapsto H^0(G,M) = \{m \in M \big| gm = m \ \forall g \in G\}$$

is a covariant functor from G–$\mathcal{MOD}$ into AB. Each G–linear homomorphism $\phi : M \to N$ induces $\phi^G : M^G \to N^G$ by G–linearity, which satisfies (F).

A *morphism* f between two contravariant functors F, $G : \mathcal{C} \to \mathcal{C}'$ is a system of morphisms $\{\phi(X) \in \mathrm{Hom}_{\mathcal{C}'}(F(X), G(X))\}_{X \in \mathcal{C}}$ making the following diagram commutative for all $u \in \mathrm{Hom}_{\mathcal{C}}(X,Y)$:

(4.1)
$$\begin{tikzcd}
F(Y) \arrow[r, "F(u)"] \arrow[d, "\phi(Y)"'] & F(X) \arrow[d, "\phi(X)"] \\
G(Y) \arrow[r, "G(u)"'] & G(X).
\end{tikzcd}$$

Thus we can define the category of contravariant functors $CTF(\mathcal{C},\mathcal{C}')$ using the above definition of morphisms between functors. Similarly, we can define the category $COF(\mathcal{C},\mathcal{C}')$ of covariant functors by reversing the direction of morphisms $F(u)$ and $G(u)$. We write $\mathrm{id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ for the identity functor taking each object X to X and each morphism ϕ to ϕ. When we have two functors $F : \mathcal{C} \to \mathcal{C}'$ and $G : \mathcal{C}' \to \mathcal{C}$ such that $G \circ F \cong \mathrm{id}_{\mathcal{C}}$ and $F \circ G \cong \mathrm{id}_{\mathcal{C}'}$ (in the categories $COF(\mathcal{C},\mathcal{C})$ and $COF(\mathcal{C}',\mathcal{C}')$, respectively) for each object Y of $\mathcal{C}$ and X of $\mathcal{C}'$, we say that the two categories are equivalent. When a functor $F : \mathcal{C} \to \mathcal{C}'$ gives an equivalence of $\mathcal{C}$ to a full subcategory of $\mathcal{C}'$, we call F *fully faithful*.

4.3. **Representability.** Fix a category $\mathcal{C}$. For each object X in $\mathcal{C}$, we associate a contravariant functor $\underline{X} : \mathcal{C} \to SETS$ by

$$\underline{X}(S) = \mathrm{Hom}_{\mathcal{C}}(S,X).$$

For each morphism $\phi : T \to S$, $\underline{X}(\phi) : \underline{X}(S) \to \underline{X}(T)$ is given by

$$\underline{X}(\phi) : (S \xrightarrow{\eta} X) \mapsto \eta \circ \phi \in \mathrm{Hom}_{\mathcal{C}}(T,X) = \underline{X}(T).$$

If $f : X \to Y$ be a morphism in $\mathcal{C}$, we have $\iota(f) \in \mathrm{Hom}_{CTF}(\underline{X}, \underline{Y})$ given by

$$\iota(f)(S)(\phi : S \to X) = f \circ \phi.$$

We leave the reader the task of verifying $\iota(f \circ g) = \iota(f) \circ \iota(g)$.

Lemma 4.1 (Unicity-lemma)**.** *The above functor: $\mathcal{C} \to CTF$ given by $X \mapsto \underline{X}$ is fully faithful.*

Proof. We only need to prove $\mathrm{Hom}_{\mathcal{C}}(X, Y) \cong \mathrm{Hom}_{CTF}(\underline{X}, \underline{Y})$ functorially. Here the word "*functorial*" means that the isomorphism commutes with composition of the morphisms. If this is true, $\underline{X} \cong \underline{Y}$ implies $X \cong Y$, and thus the functor ι gives rise to an equivalence of $\mathcal{C}$ with a full subcategory of CTF. The morphism $\iota : \mathrm{Hom}_{\mathcal{C}}(X, Y) \to \mathrm{Hom}_{CTF}(\underline{X}, \underline{Y})$ is given by $f \mapsto \iota(f)$. We define the inverse $\pi : \mathrm{Hom}_{CTF}(\underline{X}, \underline{Y}) \to \mathrm{Hom}_{\mathcal{C}}(X, Y)$ of ι by

$$F \mapsto F(X)(1_X) \in \underline{Y}(X) = \mathrm{Hom}_{\mathcal{C}}(X, Y),$$

where $F(X) : \underline{X}(X) \to \underline{Y}(X)$ by definition. We compute

$$\pi(\iota(f)) = \iota(f)(X)(1_X) = f \circ 1_X = f.$$

Thus $\pi \circ \iota$ is the identity map.

We shall show $\iota(\pi(F)) = F$. We put $f = F(X)(1_X) = \pi(F)$. If $S \xrightarrow{\phi} X \in \underline{X}(S)$ is a morphism, then the following diagram is commutative:

$$\begin{tikzcd}
 & & 1_X \arrow[r, mapsto] & F(X)(1_X) & = & f \\
\xi \arrow[dd] & \in & \underline{X}(X) \arrow[r, "F(X)"] \arrow[dd, "\underline{X}(\phi)"] & \underline{Y}(X) \arrow[dd, "\underline{Y}(\phi)"'] & \ni & \eta \arrow[dd] \\
 & & & & & \\
\xi \circ \phi & \in & \underline{X}(S) \arrow[r, "F(S)"] & \underline{Y}(S) & \ni & \eta \circ \phi,
\end{tikzcd} \tag{4.2}$$

Then we have

$$\iota(\pi(F))(S)(\phi) = \iota(f)(S) \circ \phi = f \circ \phi = F(X)(1_X) \circ \phi = F(S)(1_X \circ \phi) = F(S)(\phi).$$

This shows $\iota \circ \pi$ is the identity map. Since ι is compatible with composition, π has to be compatible with composition. □

Let $\mathcal{C}$ be a category. We consider the functors $\iota : \mathcal{C} \to CTF(\mathcal{C}, SETS)$ and $\iota' : \mathcal{C} \to COF(\mathcal{C}, SETS)$ given by $\iota(X)(S) = \underline{X}(S) = \mathrm{Hom}_{\mathcal{C}}(S, X)$ and $\iota'(X)(S) = \overline{X}(S) = \mathrm{Hom}_{\mathcal{C}}(X, S)$, which can be checked to be fully faithful by the same argument as above (reversing appropriate arrows). If $F \in COF(\mathcal{C}, SETS)$ (resp. $F \in CTF(\mathcal{C}, SETS)$) and we find $X \in \mathcal{C}$ such that $I : \overline{X} \cong F$ (resp. $I : \underline{X} \cong F$), F is called *representable* by X. Then for $S \xrightarrow{\phi} X \in \underline{X}(S)$ (resp. $X \xrightarrow{\phi} S \in \overline{X}(S)$), the following diagrams are commutative:

$$\begin{tikzcd}
& & 1_X \arrow[r, mapsto] & I(X)(1_X) & = & \xi \\
1_X \arrow[d] & \in & \underline{X}(X) \arrow[r, "I(X)"] \arrow[d, "\underline{X}(\phi)"] & F(X) \arrow[d, "F(\phi)"'] & \ni & \xi \arrow[d] \\
\phi & \in & \underline{X}(S) \arrow[r, "I(S)"] & F(S) & \ni & F(\phi)(\xi) \\
& & \phi \arrow[r, mapsto] & F(\phi)(\xi),
\end{tikzcd} \tag{4.3}$$

$$\begin{tikzcd}
& & 1_X \arrow[r, mapsto] & I(X)(1_X) & = & \xi \\
1_X \arrow[d] & \in & \overline{X}(X) \arrow[r, "I(X)"] \arrow[d, "\overline{X}(\phi)"] & F(X) \arrow[d, "F(\phi)"'] & \ni & \xi \arrow[d] \\
\phi & \in & \overline{X}(S) \arrow[r, "I(S)"] & F(S) & \ni & F(\phi)(\xi) \\
& & \phi \arrow[r, mapsto] & F(\phi)(\xi),
\end{tikzcd} \tag{4.4}$$

Start from an element $\eta \in F(S)$. The above diagram tells us that there exists a unique ϕ such that η is given by $F(\phi)(\xi)$ for $\xi = I(X)(1_X)$. Therefore each η is a specialization under a unique ϕ of the universal object ξ. If there is another ξ' which is universal in the above sense, then there exist $\phi : X \to X$ such that $F(\phi)(\xi) = \xi'$ and $\phi' : X \to X$ such that $F(\phi')(\xi') = \xi$. Both ϕ and ϕ' are unique under the above requirement. By the uniqueness, $\phi \circ \phi' = \phi' \circ \phi = 1_X$, because, for example, $\alpha = 1_X$ and $\alpha = \phi \circ \phi'$ both satisfy $F(\alpha)(\xi') = \xi'$. Thus ξ is determined up to automorphisms of X.

If $\underline{X} \cong \underline{Y}$ in $CTF(\mathcal{C}, SETS)$, then we have

$$f \in \mathrm{Hom}_{CTF}(X, Y) \cong \mathrm{Hom}_{\mathcal{C}}(X, Y) \quad \text{and} \quad g \in \mathrm{Hom}_{CTF}(Y, X) \cong \mathrm{Hom}_{\mathcal{C}}(Y, X)$$

such that $f \circ g = 1_{\underline{Y}}$ and $g \circ f = 1_{\underline{X}}$. This implies $X \cong Y$. That is,

$$X \cong Y \iff \underline{X} \cong \underline{Y}$$

Similarly we have

$$X \cong Y \iff \overline{X} \cong \overline{Y}.$$

Example 4.3. Let $\mathcal{O}$ be a valuation ring finite flat over $\mathbb{Z}_p$. We consider the Galois group $\mathrm{G} = \mathrm{G}_p = \mathrm{Gal}(\mathbb{Q}^{(p,\infty)}/\mathbb{Q})$ (unramified outside p and ∞). We fix a Galois representation $\overline{\rho} : \mathrm{G} \to GL_2(\mathbb{F})$ for the residue field $\mathbb{F}$ of $\mathcal{O}$ and define the following covariant functor $\mathcal{F} : CL_{\mathcal{O}} \to SETS$ by

$$\mathcal{F}(A) = \left\{\rho : \mathrm{G} \to GL_2(A) \middle| \rho \mod \mathfrak{m}_A = \overline{\rho}\right\} / \approx, \tag{4.5}$$

where "$\approx$" is the strict equivalence, that is, conjugation by $\widehat{GL}_2(A) = 1_2 + M_2(\mathfrak{m}_A)$. Each element $\rho \in \mathcal{F}(A)$ is of course supposed to be a continuous representation. For any morphism $\alpha \in \mathrm{Hom}_{CL}(A, B)$, we define $\mathcal{F}(\alpha) : \mathcal{F}(A) \to \mathcal{F}(B)$ by $\mathcal{F}(\alpha)(\rho) = \alpha \circ \rho$. In this way, $\mathcal{F}$ forms a covariant functor. Under the absolute irreducibility of $\overline{\rho}$, Mazur's theorem tells us that there exists a universal couple (R, ϱ) made of $\varrho : \mathrm{G} \to GL_2(R) \in \mathcal{F}(R)$ with $R \in CL_{\mathcal{O}}$ such that

$$\mathcal{F}(A) \cong \mathrm{Hom}_{CL}(R, A) \ \text{ via } \rho \mapsto \alpha \iff \alpha \circ \varrho \approx \rho.$$

This shows that the covariant functor $\mathcal{F}$ is representable by $R \in CL_{\mathcal{O}}$, and the universal object in $\mathcal{F}(R)$ is given by ϱ.

We pick a character $\phi : \mathrm{G} \to \mathcal{O}^{\times}$ such that $\phi \mod \mathfrak{m}_{\mathcal{O}} = \det(\overline{\rho})$. Then we can think of the following three subfunctors of $\mathcal{F}$:

$$\begin{aligned} \mathcal{F}^{\phi}(A) &= \{\rho \in \mathcal{F}(A) \big| \det(\rho) = \phi\} \\ \mathcal{F}^{ord}(A) &= \{\rho \in \mathcal{F}(A) \big| \rho \text{ is } p\text{–ordinary}\} \\ \mathcal{F}^{ord,\phi}(A) &= \mathcal{F}^{ord}(A) \cap \mathcal{F}^{\phi}(A), \end{aligned} \tag{4.6}$$

where we regard ϕ as a character with valued in $A^{\times}$ projecting the original ϕ down to A by the structure morphism $\mathcal{O} \to A$. Here we recall that ρ is called p–ordinary if $\rho|_{D_p} \cong \left(\begin{smallmatrix} \mathbf{e} & * \\ 0 & \delta \end{smallmatrix}\right)$ with unramified δ. Of course, the last two functors have meaning only when $\overline{\rho}$ is p–ordinary. Let $CNL_{\mathcal{O}}$ be the subcategory of $CL_{\mathcal{O}}$ made of noetherian local $\mathcal{O}$–algebras. Under the absolute irreducibility of $\overline{\rho}$, $\mathcal{F}^{\phi}$ is representable in $CL_{\mathcal{O}}$ and even in $CNL_{\mathcal{O}}$, and $\mathcal{F}^{ord}$ and $\mathcal{F}^{ord,\phi}$ are also representable in $CNL_{\mathcal{O}}$ if $\overline{\rho}$ is absolutely irreducible and regular

4.4. **Abelian categories.** If one can equip $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ with a functorial addition making it into an abelian group, $\mathcal{C}$ is called an *additive* category. An abelian category $\mathcal{C}$ is an additive category which has a (functorial) notion of cokernel, kernel and image. For example, A–MOD, AB, G–$\mathcal{MOD}$ etc. are abelian categories.

Let us recall the formal definition of additive and abelian categories in the following paragraphs. Let $\{0\}$ be a set made of a single element "0". We consider the covariant functor $F_0 : \mathcal{C} \to SETS$ given by $F_0(Y) = \{0\}$ for all $Y \in \mathcal{C}$ and $F_0(\phi) = 1_{\{0\}}$ for any morphism ϕ in $\mathcal{C}$. If F_0 is representable by an object $X_0 \in \mathcal{C}$, X_0 is called an *initial* object. Thus, for each $X \in \mathcal{C}$, $F_0(X) = \{0\} = \mathrm{Hom}_{\mathcal{C}}(X_0, X)$ is made of a unique element i. In other words, for each $X \in \mathcal{C}$, there is a unique morphism $i : X_0 \to X$ such that $F_0(i) = 1_{\{0\}}$.

We can also consider the contravariant functor $F^0 : \mathcal{C} \to SETS$ given by $F^0(Y) = \{0\}$ for all $Y \in \mathcal{C}$ and $F^0(\phi) = 1_{\{0\}}$ for any morphism ϕ in $\mathcal{C}$. If F^0 is representable by $X^0 \in \mathcal{C}$, X^0 is called a *final* object of $\mathcal{C}$. Thus, for each $X \in \mathcal{C}$, there is a unique morphism $p : X \to X^0$ such that $F^0(p) = 1_{\{0\}}$. By definition, we have a unique morphism $e : X_0 \to X^0$ such that $e = p \circ i$.

We consider the following condition:

(Ab0) *$\mathcal{C}$ has an initial and a final object which are isomorphic under e.*

If $\mathcal{C}$ satisfies (Ab0), we identify the initial and the final object by e and call it the zero-object $\mathbf{0} = \mathbf{0}_{\mathcal{C}}$. We write ${}_X\mathbf{0}$ (resp. $\mathbf{0}_X$) for the unique element in $\mathrm{Hom}_{\mathcal{C}}(\mathbf{0}, X)$ (resp. $\mathrm{Hom}_{\mathcal{C}}(X, \mathbf{0})$). We assume that (Ab0) holds. Then we have a unique $\mathbf{0}_{X,Y} \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$ given by $\mathbf{0}_{X,Y} = \mathbf{0}_Y \circ {}_X\mathbf{0}$, which is called the *zero-map.*

For two objects $X, Y \in \mathcal{C}$, we consider the covariant functor $\underline{X \oplus Y} : \mathcal{C} \to SETS$ defined by $Z \mapsto \mathrm{Hom}_{\mathcal{C}}(X, Z) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z)$. If this functor is representable by an object, we call the object the *direct sum* of X and Y, and write it as $X \oplus Y$. In other words, there exists $\iota_X : X \to X \oplus Y$ and $\iota_Y : Y \to X \oplus Y$ such that the map

$\mathrm{Hom}_{\mathcal{C}}(X \oplus Y, Z) \ni f \mapsto (f \circ \iota_X, f \circ \iota_Y) \in \mathrm{Hom}_{\mathcal{C}}(X, Z) \times \mathrm{Hom}_{\mathcal{C}}(Y, Z)$ is bijective for all Z, that is, (ι_X, ι_Y) is the universal object. The morphism $\iota_X : X \to X \oplus Y$ is called the *inclusion* of X into $X \oplus Y$.

Similarly we consider the contravariant functor $\overline{X \times Y} : \mathcal{C} \to SETS$ defined by $Z \mapsto \mathrm{Hom}_{\mathcal{C}}(Z, X) \times \mathrm{Hom}_{\mathcal{C}}(Z, Y)$. If this functor is representable by an object, we call the object the *direct product* of X and Y, and write it as $X \times Y$. In other words, there exists $\pi_X : X \times Y \to X$ and $\pi_Y : X \times Y \to Y$ such that the map $\mathrm{Hom}_{\mathcal{C}}(Z, X \times Y) \ni f \mapsto (\pi_X \circ f, \pi_Y \circ f) \in \mathrm{Hom}_{\mathcal{C}}(Z, X) \times \mathrm{Hom}_{\mathcal{C}}(Z, Y)$ is bijective for all Z, that is, (π_X, π_Y) is the universal object. The morphism $\pi_X : X \times Y \to X$ is called the *projection* of $X \times Y$ onto X.

We have a unique morphism $\theta : X \oplus Y \to X \times Y$ such that

$$\pi_X \circ \theta \circ \iota_X = 1_X, \pi_X \circ \theta \circ \iota_Y = \mathbf{0}_{Y,X},\ \pi_Y \circ \theta \circ \iota_X = \mathbf{0}_{X,Y},\ \pi_Y \circ \theta \circ \iota_Y = 1_Y.$$

We consider the following condition:

(Ab1) *For any two objects $X, Y \in \mathcal{C}$, there exist $X \oplus Y$ and $X \times Y$ in $\mathcal{C}$, and $\theta : X \oplus Y \cong X \times Y$.*

Suppose (Ab1). Let

$$\triangle_X\colon X \to X \times X = X \oplus X \quad (\text{resp. } \nabla_X : X \times X = X \oplus X \to X)$$

be the morphism corresponding to $(1_X, 1_X)$. For $f, g \in \mathrm{Hom}_{\mathcal{C}}(X, Y)$, let $(f, g) : X \times X \to Y \times Y$ be the corresponding morphism. And we define

$$f + g : X \to Y \in \mathrm{Hom}_{\mathcal{C}}(X, Y) \ \text{ by } \ \nabla_Y \circ (f, g) \circ \triangle_X\ .$$

We then have

$$(f + g) + h = f + (g + h) \quad \text{and} \quad \mathbf{0}_{X,Y} + f = f + \mathbf{0}_{X,Y} = f.$$

We consider the following condition:

(Ab2) *$Hom_{\mathcal{C}}(X, Y)$ is an abelian group under "+" with identity $\mathbf{0}_{X,Y}$.*

A category satisfying (Ab0-2) is called an *additive* category.

Suppose that $\mathcal{C}$ is an additive category. For the category $\mathcal{C}$ to form an abelian category, $\mathcal{C}$ need to have "kernel", "cokernel" and "image" of morphisms. Here an object $K \in \mathcal{C}$ with $i : K \to X$ is called a *kernel* of $f : X \to Y$ if

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{C}}(Z, K) \xrightarrow{\underline{i}} \mathrm{Hom}_{\mathcal{C}}(Z, X) \xrightarrow{\underline{f}} \mathrm{Hom}_{\mathcal{C}}(Z, Y)$$

is an exact sequence in AB for all Z, where $\underline{f}(\phi) = f \circ \phi$. Similarly $p : Y \to C$ is called a *cokernel* of p if

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{C}}(C, Z) \xrightarrow{\overline{p}} \mathrm{Hom}_{\mathcal{C}}(Y, Z) \xrightarrow{\overline{f}} \mathrm{Hom}_{\mathcal{C}}(X, Z)$$

is exact for all $Z \in \mathcal{C}$, where $\overline{f}(\phi) = \phi \circ f$. If $Y \xrightarrow{p} C$ is a cokernel of $X \xrightarrow{f} Y$, $I = \mathrm{Im}(f)$ is defined to be the kernel of p. Thus we have $j : I \to Y$. Similarly, the cokernel of $K \xrightarrow{i} X$ is defined to be the *coimage* of f, and we write $q : X \to L$ for the canonical map. Looking into the following two exact sequences:

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{C}}(L, Y) \xrightarrow{\overline{q}} \mathrm{Hom}_{\mathcal{C}}(X, Y) \xrightarrow{\overline{i}} \mathrm{Hom}_{\mathcal{C}}(K, Y) \tag{4.7}$$

$$0 \longrightarrow \mathrm{Hom}_{\mathcal{C}}(L, I) \xrightarrow{\underline{j}} \mathrm{Hom}_{\mathcal{C}}(L, Y) \xrightarrow{\underline{p}} \mathrm{Hom}_{\mathcal{C}}(L, C), \tag{4.8}$$

we claim to have a unique $\tau : L \to I$ such that $f = j \circ \tau \circ q$. In fact, $\underline{f} \circ \underline{i} = \mathbf{0}$ implies $f \circ i = \mathbf{0} \Leftrightarrow f \in \mathrm{Ker}(\overline{i})$ by the unicity-lemma. This shows that $f = g \circ q \in \mathrm{Im}(\overline{q})$ for $g \in \mathrm{Hom}_{\mathcal{C}}(L, Y)$ by the exactness of (4.7). By $\overline{f} \circ \overline{p} = \mathbf{0}$, we similarly have $p \circ f = \mathbf{0}$ and hence, $\overline{q}(p \circ g) = p \circ g \circ q = \mathbf{0}$. By the injectivity of $\overline{q}$, we have $\underline{p}(g) = p \circ g = \mathbf{0} \Leftrightarrow g \in \mathrm{Ker}(\underline{p}) = \mathrm{Im}(\underline{j})$, and hence $g = j \circ \tau$ for $\tau \in \mathrm{Hom}_{\mathcal{C}}(L, I)$. This shows the claim.

An additive category $\mathcal{C}$ is called *abelian* if the following two conditions are satisfied:

(Ab3) *For every morphism $X \xrightarrow{f} Y$ in $\mathcal{C}$, its kernel and cokernel exist in $\mathcal{C}$;*
(Ab4) *The morphism $\tau : L \to I$ as above is an isomorphism.*

Suppose now that $\mathcal{C}$ is an abelian category. Then $\overline{X}(Y) = \mathrm{Hom}_{\mathcal{C}}(X, Y)$ is an abelian group. That is $\overline{X} \in COF(\mathcal{C}, AB)$. A sequence $F \to G \to H$ of functors in $COF(\mathcal{C}, AB)$ is called exact if $F(X) \to G(X) \to H(X)$ is exact for all X in $\mathcal{C}$. If $X \xrightarrow{\alpha} Y$ is a morphism in $\mathcal{C}$, then $X \xrightarrow{\alpha} Y \to \mathrm{Coker}(\alpha) \to 0$ is exact. Then by definition and the unicity-lemma, we see

$$0 \longrightarrow \overline{\mathrm{Coker}(\alpha)} \longrightarrow \overline{Y} \xrightarrow{\overline{\alpha}} \overline{X}$$

is exact in $COF(\mathcal{C}, AB)$. That is $\overline{\mathrm{Coker}(\alpha)} = Ker(\overline{\alpha})$. Then we see

$$\begin{aligned} (4.9) \quad 0 \to \overline{X} \xrightarrow{\overline{\alpha}} \overline{Y} \to \overline{\beta}\overline{Z} \text{ is exact } &\iff \overline{\mathrm{Coker}(\beta)} = \mathrm{Ker}(\overline{\beta}) \cong \overline{X} \text{ via } \overline{\alpha} \\ &\iff \mathrm{Coker}(\beta) \cong X \text{ via } \alpha \text{ by the unicity-lemma} \\ &\iff Z \xrightarrow{\beta} Y \xrightarrow{\alpha} X \to 0 \text{ is exact.} \end{aligned}$$

A similar assertion also holds for $\underline{X}$.

References

[ADT] J. S. Milne, *Arithmetic Duality Theorem*, Perspectives in Math. **1**, Academic Press, 1986 (available at `http://www.jmilne.org/math/`)

[BCM] N. Bourbaki, *Commutative algebra*, Hermann, Paris, 1961-89

[CFT] E. Artin and J. Tate, *Class Field Theory*, Benjamin, 1968 (errata at `http://www.ams.org/bookpages/chel-366/errata.pdf`)

[CLC] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962

[HAL] P. J. Hilton and U. Stammback, *A Course in Homological Algebra*, Graduate Text in Math. **4**, Springer, Berlin-Heiderberg-New York-Tokyo, 1970

[MFG] H. Hida, *Modular Forms and Galois Cohomology*, Cambridge Studies in Advanced Mathematics **69**, Cambridge University Press, Cambridge, England, 2000.