A note on Galois cohomology of algebraic integers (Abstract)

Takashi Ono
The Johns Hopkins University
October 10, 2008

1 $H^1(\mathfrak{g}, \mathcal{O}_k)$

Let $k/\mathbb{Q}$ be a finite Galois extension of degree $d$. Let $\mathfrak{g} = \text{Gal}(k/\mathbb{Q})$. Let $\mathcal{O}_k$ be the ring of integers of $k$. We want to express the the number $h_k = |H^1(\mathfrak{g}, \mathcal{O}_k)|$ in terms of the number of solutions of certain system of congruences over the finite ring $\mathbb{Z}/d\mathbb{Z}$.

To be more precise, let us express an element $\xi \in \mathcal{O}_k$ as

$$\xi = x_1\omega_1 + \cdots + x_d\omega_d = \Omega x, \quad \Omega = (\omega_1, \cdots, \omega_d),$$

with

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \in \mathbb{Z}^d.$$

Then

$$^\sigma \xi = ^\sigma \Omega x, \quad \sigma \in \mathfrak{g}.$$

If we define a unimodular matrix $A_\sigma$ by

$$^\sigma \Omega = \Omega A_\sigma,$$

(2)
then, we have
\[ A_{\sigma\tau} = A_{\sigma}A_{\tau}, \quad \sigma, \tau \in g. \]
In other words,
\[ A: \sigma \mapsto A_{\sigma} \in GL_d(\mathbb{Z}) \quad (3) \]
is an integral representation of the Galois group \( g \) of degree \( d = [k : Q] \).

We obtain the following

**Theorem 1** Notations being as above, let \( \nu_k \) be the number of solutions \( x \in \mathbb{Z}^d \) of the congruence \( A_{\sigma}x \equiv x \mod d \forall \sigma \in g \), then \( dh = \nu_k \).

To prove Th.1, the set which is defined naively by
\[ \Xi_k = \{ \xi \in \mathcal{O}_k; \quad ^{\sigma}\xi \equiv \xi \mod d, \forall \sigma \in g \} \quad (4) \]
plays a basic role. This is a \( \mathbb{Z} \)-module in \( \mathcal{O}_k \), containing \( \mathbb{Z} \) and is \( g \)-stable.

For each \( \xi \in \Xi_k \) and \( \sigma \in g \), we see that the element \( t(\xi)_{\sigma} = (\xi - ^{\sigma}\xi)/d \) induces a homomorphism \( t \) of \( \Xi_k \) onto the group of 1-cocycles for \( (g, \mathcal{O}_k) \) so that
\[ \Xi_k/\mathbb{Z} \approx Z^1(g, \mathcal{O}_k). \quad (5) \]

### 2 System \((g, (G, M))\)

As in 1, let \( K/Q \) be a finite Galois extension with the Galois group \( g \). As the group \( G \) we take the additive group of the ring \( \mathcal{O}_k \) and as the \( G \)-module \( M \), we consider the direct sum \( M = \mathcal{O}_k + \mathcal{O}_k = (\mathcal{O}_k)^2 \). With the natural actions of \( G \) on \( M \) and \( g \) on \( (G, M) \), we obtain a **system** \((g, (G, M))\) (cf. T. Ono, Gauss sums and Poincaré sums(a sketch), Appendix 3, Nippon-Hyoronsha, Tokyo, 2008). The action of \( G \) on \( M \) may be written in matrices like
\[ g \circ x = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 + tx_2 \\ x_2 \end{pmatrix}. \]

Hence we can use matrices
\[ C_{\sigma} = \begin{pmatrix} 1 & t_{\sigma} \\ 0 & 1 \end{pmatrix}, \quad \sigma \in g \]
as a cocycle \( \in Z^1(g, \mathcal{O}_k) \). In view of (5), we can write
\[ C_{\sigma} = A(\xi) .^{\sigma} A(\xi)^{-1} \quad \text{for some} \quad \xi \in \Xi_k. \quad (6) \]
where the matrix

\[
A(\xi) = \begin{bmatrix} 1 & \xi/d \\ 0 & 1 \end{bmatrix}.
\]

For the cocycle \( C \), we associate a \( \mathbb{Z} \)-module

\[
M_C = \{ x \in M; \ C_\sigma x = x, \ \sigma \in \mathfrak{g} \}.
\]

and its submodule

\[
P_C = \{ y = p_C(x), \ x \in M \},
\]

where

\[
p_C(x) = \sum \tau C_\tau x.
\]

We know that the quotient \( M_C/P_C \) depends only on the cohomology class \( \gamma = [C] \) and is identified with the module \( \bar{H}^0(\mathfrak{g}, O_k)\gamma \). The determination of the index \( i_\gamma(\mathfrak{g}, M) = [M_C : P_C] \) is a basic theme inspired by Poincaré. In this context, we obtain the following

**Theorem 2** Notations being as above, we find

\[
i_\gamma(\mathfrak{g}, M) = |\bar{H}^0(\mathfrak{g}, A(\xi)^{-1} M)|.
\]