<table>
<thead>
<tr>
<th>著者</th>
<th>Ono Takashi</th>
</tr>
</thead>
<tbody>
<tr>
<td>ご飯名</td>
<td>未定</td>
</tr>
<tr>
<td>ご飯名</td>
<td>未定</td>
</tr>
<tr>
<td>出所</td>
<td>Interdisciplinary Information Sciences</td>
</tr>
<tr>
<td>出所</td>
<td>未定</td>
</tr>
<tr>
<td>タイムライン</td>
<td>未定</td>
</tr>
<tr>
<td>タイムライン</td>
<td>未定</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10097/48325">http://hdl.handle.net/10097/48325</a></td>
</tr>
<tr>
<td>doi</td>
<td>10.4036/iis.2010.1</td>
</tr>
</tbody>
</table>
A Note on Galois Cohomology of Algebraic Integers

Takashi ONO

Department of Mathematics, The Johns Hopkins University, Baltimore, Maryland, 21218, U.S.A.

Received January 7, 2009; final version accepted March 6, 2009

We consider an admissible system \((g, (G, M))\) where \(g\) is the group of a Galois extension \(k/Q\) of number fields, \(G\) the ring \(O_k\) of integers of \(k\) and \(M = (O_k)^2\). The cohomology group \(H^1(g, O_k)\) is nicely described by a naive submodule \(\Xi_k\) of \(O_k\) and the Poincare’ index \(i_j(g, M)\), \(j \in H^1(g, O_k)\), for the system \((g, (G, M))\), can be expressed in terms of \(\Xi_k\).

KEYWORDS: Galois extension, number fields, ring of integers, cohomology, system

1. The module \(\Xi_k\)

Let \(k/Q\) be a finite Galois extension. Denote by \(g\) the Galois group \(\text{Gal}(k/Q)\) and by \(d\) the degree \(|g| = [k : Q]\). Let \(O_k\) be the ring of integers in \(k\). We set

\[
\Xi_k = \{\xi \in O_k; \quad ^g\xi \equiv \xi \mod d, \quad \forall \sigma \in g.\}
\]

(1)

This is a \(Z\)-module in \(O_k\). It contains \(Z\) and \(dO_k\), and is \(g\)-stable as is easily seen. The definition implies that

\[
\Xi_k/dO_k = (O_k/dO_k)^g,
\]

(2)

where, for any \(g\)-module \(M\), \(M^g\) denotes the subset of elements of \(M\) invariant under the action of \(g\).

For each \(\xi \in \Xi_k\) and \(\sigma \in g\), we can define an element \(t(\xi)_\sigma\) in \(O_k\) by

\[
t(\xi)_\sigma = t(\xi)_\sigma = (\xi - ^\sigma\xi)/d.
\]

(3)

As the group \(g\) acts on the additive group of the ring \(O_k\), we may speak of the first cohomology group \(H^1(g, O_k) = Z^1(g, O_k)/B^1(g, O_k)\). In view of (3), we have

\[
t(\sigma) = t_\sigma + ^\sigma t_t\tag{4}
\]

and hence a homomorphism

\[
t : \Xi_k \rightarrow Z^1(g, O_k), \quad \text{defined by} \quad t(\xi)_\sigma = (\xi - ^\sigma\xi)/d.
\]

(5)

**Proposition 1.** The map \(t\) in (5) induces an isomorphism

\[
\Xi_k/Z \cong Z^1(g, O_k).
\]

(6)

**Proof.** (i) \(\ker t = Z\). In fact,

\[
\xi \in \ker t \iff t(\xi) = 0 \iff \xi - ^\sigma\xi = 0, \quad \sigma \in g \iff \xi \in O_k \cap Q = Z.
\]

(ii) \(t\) is surjective. Let \(u\) be any cocycle in \(Z^1(g, O_k)\). We will find a \(\xi \in \Xi_k\) so that \(u = t(\xi)\). Let us try the following element

\[
\xi = \sum_{\tau \in \sigma} u_\tau \in O_k.
\]

It is not obvious at this moment that \(\xi \in \Xi_k\) but the following argument implies it. In fact, we have

\[
(\xi - ^\sigma\xi)/d = \left(\sum_{\tau} u_\tau - \sum_{\tau} ^\sigma u_\tau\right) / d = \left(\sum_{\tau} u_{\sigma\tau} - \sum_{\tau} ^\sigma u_\tau\right) / d = \left(\sum_{\tau} u_\sigma\right) / d = u_\sigma
\]

which shows that our \(\xi \in \Xi_k\) and \(u = t(\xi)\).

\(\square\)

From Proposition 1 we have the relation:
\[ \Theta_k / \mathbb{L} \supset \Xi_k / \mathbb{L} \cong \mathbb{Z}^1 (g, \Theta_k). \] (7)

Let \( H \) be the subgroup of \( \Xi_k / \mathbb{L} \) corresponding to the coboundary group:
\[ B^1 (g, \Theta_k) = \{ v \in \mathbb{Z}^1 (g, \Theta_k); \eta = \eta - v, \eta \in \Theta_k \}. \] (8)

Denoting by \([\xi]\) the class of \( \xi \in \Theta_k \) modulo \( \mathbb{L} \), we have, for \( \xi \in \Xi_k \),
\[ [\xi] \in H \iff t(\xi) = (\xi - \eta) / d = \eta - \eta, \eta \in \Theta_k \iff \xi - d\eta = \eta(\xi - d\eta) \iff \xi - d\eta \in \mathbb{L}. \]

In other words,
\[ H = d(\Theta_k / \mathbb{L}) = (\mathbb{L} + d\Theta_k) / \mathbb{L}. \] (9)

By (6), (7), (8), (9), we obtain

**Proposition 2.** Let \( k / \mathbb{Q} \) be a finite Galois extension of degree \( d \) with the Galois group \( g \) and let \( \Xi_k \) be the module given by (1). Then we have
\[ H^1 (g, \Theta_k) \cong \Xi_k / (\mathbb{L} + d\Theta_k). \]

We note here an obvious relation:
\[ \Theta_k / d\Theta_k \cong (\mathbb{L} / d\mathbb{L})^d. \] (10)

In connection with the cohomology group \( H^1 (g, \Theta_k) \), we will study the \( g \)-fixed points of the finite module \( \Theta_k / d\Theta_k \). Let us look at the sequence of modules:
\[ \Theta_k \supset \Xi_k \supset \mathbb{L} + d\Theta_k \supset d\Theta_k \] (11)

We already know structures of several portions of (11). By (10), we have
\[ (\Theta_k : d\Theta_k) = d^d, \] (12)
by (2)
\[ (\Xi_k : d\Theta_k) = |(\Theta_k / d\Theta_k)^g|, \] (13)
by Proposition 2
\[ (\Xi_k : \mathbb{L} + d\Theta_k) = |H^1 (g, \Theta_k)|. \] (14)

Combining (12), (13), (14) with the obvious isomorphism
\[ (\mathbb{L} + d\Theta_k) / d\Theta_k \cong \mathbb{L} / d\mathbb{L}, \]
we obtain

**Theorem 1.** Let \( k / \mathbb{Q} \) be a finite Galois extension of degree \( d \) with the Galois group \( g \). Then we have
\[ |H^1 (g, \Theta_k)| = |(\Theta_k / d\Theta_k)^g|/d. \]

**2. The module \((\Theta_k / d\Theta_k)^g\)**

Notations being as before, let us express an element \( \xi \in \Theta_k \) as
\[ \xi = x_1 \omega_1 + \cdots + x_d \omega_d = \Xi x, \quad \Omega = (\omega_1, \ldots, \omega_d). \] (15)

where \( \{\omega_i\} \) being a \( \mathbb{Z} \)-basis of \( \Theta_k \) with
\[ x = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \in \mathbb{Z}^d. \]

Then
\[ \sigma \xi = \sigma \Xi x, \quad \sigma \in g. \]
If we define a unimodular matrix \( A_\sigma \) by
\[ \sigma \Omega = \Omega A_\sigma, \] (16)
then, we have
\[ A_{\sigma T} = A_{\sigma}A_{T}, \quad \sigma, \tau \in \mathfrak{g}. \]

In other words,
\[ A : \quad \sigma \mapsto A_{\sigma} \in GL_d(\mathbb{Z}) \tag{17} \]
is an integral representation of the Galois group \( \mathfrak{g} \) of degree \( d = \lbrack k : \mathbb{Q} \rbrack \).

As for the base change \( \Omega \to \Omega' \) afforded by \( \Omega' = \Omega T, T \in GL_d(\mathbb{Z}) \), let \( A'_\sigma \) be the matrix for the new basis. One then finds
\[ A'_\sigma = T^{-1}A_\sigma T, \]
so \( A' \) is \( \mathbb{Z} \)-equivalent to \( A : A' \sim A \).

Let \( \xi = \Omega x \) be the relation in (15). We want to translate the condition \( \xi \in \mathbb{Z}_k \) in terms of one for \( x \in \mathbb{Z}^d \). Now follow the following sequence of equivalences
\[ \xi \in \mathbb{Z}_k \iff ^{\sigma}\xi \equiv \xi \pmod{(d)} \iff ^{\sigma}\Omega x \equiv \Omega x (d) \iff \Omega A_\sigma x \equiv \Omega x (d) \iff (A_\sigma - I)x \equiv 0 (d). \]

Therefore we obtain the following theorem:

**Theorem 2.** Notations being as above, we have
\[ |(\Theta_k/d\Theta_k)^\mathfrak{g}| = |(x \in \mathbb{Z}^d/d\mathbb{Z}^d; (A_\sigma - I)x \equiv 0 \mod d)|. \]

3. Case \( d = 2 \)

Let us study here a special case where \( d = \lbrack g \rbrack = \lbrack k : \mathbb{Q} \rbrack = 2 \). Let \( \sigma \) be the generator of \( \mathfrak{g} \). As we know there is an \( \Omega \) of the form \( \Omega = (1, \omega) \). [In general, it is true that 1 can appear in a basis of \( \mathcal{O}_k \) for any number field \( k \).] Then the matrix \( A_\sigma, \sigma \neq 1 \), satisfying (16) must be of the form
\[ \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix}. \tag{18} \]

Furthermore it is easy to check that the parity of \( b \) in (18) is unchanged by the base change \( \Omega = (1, \omega) \to \Omega' = (1, \omega') \). We shall call the parity of \( b \) simply the parity of the quadratic field \( k \). Let us set \( p(k) = 1 \) or 2 according as the parity is odd or even. Theorem 1 and Theorem 2, with elementary facts on quadratic fields, imply the following

**Proposition 3.** Let \( k/\mathbb{Q} \) be a quadratic field. Then
\[ p(k) = |H^1(\mathfrak{g}, \mathcal{O}_k)| = \frac{1}{2}|H^0(\mathfrak{g}, \mathcal{O}_k/2\mathcal{O}_k)|. \]

4. The system \((\mathfrak{g}, (G, M))\)

To begin with let us introduce a simple general setting
\[ (\mathfrak{g}, (G, M)) \]
where \( G \) is a group, \( M \) a left \( G \)-module and \( \mathfrak{g} \) is a finite group acting on \( (G, M) \) naturally. Namely, we assume that \( G \) is a left \( \mathfrak{g} \)-group, \( M \) is a left \( \mathfrak{g} \)-module so that
\[ ^{\sigma}sx = ^{\sigma}s\mathfrak{x}, \quad \sigma \in \mathfrak{g}, s \in G, x \in M. \]

For a cocycle \( C \) with values in \( G \), we associate a subgroup \( M_C \) of \( M \) by
\[ M_C = \{x \in M; C_\sigma x = x, \quad \sigma \in \mathfrak{g}\}. \tag{19} \]

We consider also a subgroup of \( M_C \) given by
\[ P_C = \{y = p_C(x), \quad x \in M\} \tag{20} \]
where
\[ p_C(x) = \sum_{\tau \in \mathfrak{g}} C_{\tau}^{-1}x. \tag{21} \]

One verifies that the structure of the module \( M_C/P_C \) depends only on the cohomology class \( \gamma = [C] \in H^1(\mathfrak{g}, G) \). If we put \( C = 1 \) in (19), (20) then we have \( M_1 = M^0, P_1 = N(M) \) hence \( M_1/P_1 = \tilde{H}^0(\mathfrak{g}, M), \) the Tate cohomology group. For a general \( \gamma = [C] \in H^1(\mathfrak{g}, G), \) we have a right to make identification.
\[ M_C/P_C = \hat{H}^1(g, M) \]

and call this the Tate group twisted by \( \gamma \). Furthermore, we shall put

\[ i_\gamma(g, M) = [M_C : P_C], \quad \gamma = [C] \in H^1(g, G). \] (22)

The determination of the index \( i_\gamma(g, M) \) is a theme inspired by Poincaré. (See [1], Appendix 3 (in English) and references there.)

Now let \( k/Q \) be a finite Galois extension with the Galois group \( g \). As for the group \( G \) and the module \( M \), we set

\[ G = \{ g = (t_i), \quad t \in O_k \}, \quad M = \{ x = (x_i), \quad x_1, x_2 \in O_k \}. \]

With the natural action of \( G \) on \( M \) and those of \( g \) on each of \( g \) and \( M \), we obtain an admissible system \((g, (G, M))\). The action of \( G \) on \( M \) is the matrix multiplication: \( g \circ x = (t_i)x = (t_i + x) \). For our Galois actions, the relation \( \sigma (t \circ x) = (\sigma t) \circ (\sigma x) \) is trivial. We can use matrices \( C_\sigma = (c_{i,j})_\sigma \in Z^1(g, G) \). Instead of additive relation (4), we have this, a multiplicative one: \( C_{\sigma \tau} = C_\sigma \tau \). Since any cocycle \( t \in Z^1(g, O_k) \) is of the form \( t_\sigma = t(\xi) = (\xi - \xi)/d \) for some \( \xi \in \mathbb{Z}_k \) by (6), we can write

\[ C_\sigma = A(\xi) \cdot \sigma A(\xi)^{-1} \] (23)

with the matrix

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

Along with (19), (20), for the cocycle \( C \), we associate a \( Z \)-module \( M_C \) by

\[ M_C = \{ x \in M, \quad C_\sigma x = x, \quad \sigma \in g \}. \] (24)

We have also a submodule of \( M_C \) given by

\[ P_C = \{ y = p_C(x), \quad x \in M \} \] (25)

where \( p_C(x) = \sum \tau C_\tau^\tau x \).

We know that the quotient \( M_C/P_C \) depends only on the cohomology class \( \gamma = [t] = [t(\xi)] \in H^1(g, O_k) \) and is identified with the module \( \hat{H}^1(g, M) \). Finally we set index \( i_\gamma(g, M) = [M_C : P_C] \).

In what follows, when a \( \xi \in \mathbb{Z}_k \) is fixed, we set simply \( A = A(\xi) \).

(i) \( M_C \). For \( x \in M \),

\[ x \in M_C \iff C_\sigma^\tau x = x \iff A^\sigma A^{-1} \tau x = x \iff A^{-1} x = (A^{-1} \tau x). \]

Hence we have

\[ A^{-1}M_C = \{ A^{-1} x \in A^{-1} M \cap (Q^2) \}. \]

In other words,

\[ A^{-1}M_C = (A^{-1} M)^\sigma. \] (26)

(ii) \( P_C \). By (20), we find

\[ A^{-1}P_C = \left\{ A^{-1} \sum \tau C_\tau^\tau x \right\} = \left\{ \sum \tau (A^{-1} \tau x) \right\} = \{ Tr(A^{-1} x), \quad x \in M \}. \]

In other words,

\[ A^{-1}P_C = Tr(A^{-1} M). \] (27)

By (24), (25) we obtain

**Theorem 3.** Let \( k/Q \) be a finite Galois extension with the Galois group \( g \). Let \( M = (O_k)^2 \). For a cocycle class \( \gamma = [C] \in H^1(g, O_k) \) corresponding to an element \( \xi \in \mathbb{Z}_k \) by (6), we have \( i_\gamma(g, M) = |\hat{H}^1(g, A(\xi)^{-1} M)| \).

REFERENCES