Garzón Rojas, Álvaro
An application of localization to Galois cohomology
Escuela Regional de Matemáticas
Cali, Colombia

Available in: http://www.redalyc.org/articulo.oa?id=46810207
An application of localization to Galois cohomology

Álvaro Garzón Rojas.

Abstract

We use a localization theorem and a characterization of the first group of cohomology $H^1(G, B)$ to give a new proof that the groups of cohomology $H^i(G, B)$ of finite cyclic extensions of number fields have same order for all integers $i$. This result was proved by H. Yokoy in [10] by using the theorem on existence of a normal basis.

Keywords: Localizations theorems, Galois cohomology, theorem of Yokoi.

1. Introduction

Let $K$ be a number field with integer ring $A$, $L$ be a finite cyclic extension of $K$ with Galois group $G$ and $B$ the integer closure of $A$ in $L$. By using a localization technique, we give in this paper a proof of the following theorem of Yokoi:

Theorem 1.1. ([10], Theorem 1) Let $L$, $K$, $G$ and $B$ be as above. Then

$$o(H^i(G, B)) = o(H^j(G, B))$$

for all integers $i$, $j$.

For this, first we treat some facts about automorphism of local fields to give a characterization of $H^1(G, B)$, and then we use a localization theorem to reduce the cohomology at local case.

2. About automorphisms of local fields

By a local field we mean a complete field with respect to a discrete valuation with perfect residue class field. In this section we suppose that $L$ is a local field, $B$ is its ring of integers, $\mathfrak{R}$ is the maximal ideal in $B$ and $\overline{L} = B/\mathfrak{R}$ is the residue class field. Let $\nu_L$ be the order function defined on $L$ and let $p$ denote the characteristic of the residual class field $\overline{L}$.

Definition 2.1. We say that $\sigma$ is a wildly ramified automorphism of $L$ if

$$\nu_L(\sigma - 1)x > 1$$

for all $x \in B$. 
Note that if $\sigma$ is wildly ramified then $(\sigma - 1)B \subset \mathbb{R}^2$ and $\sigma^n$ is wildly ramified for all integers $n$. Therefore, the first ramification group of $\mathbb{R}$ contains the group $G = \langle \sigma \rangle$. Now we give a result that explores this property.

**Theorem 2.1.** Let $\sigma \in \text{Aut}(L)$ be a finite order automorphism and let $K = L^G$. Then $\sigma$ is wildly ramified if and only if $[L : K] = p^n$, where $p = \text{Char}(K)$

**Demostración.** Since $L/K$ is finite, then $L/K$ contains a unique maximal unramified subfield $T$ (i.e., $e(T/K) = 1$) ([8], 3-2-10) and a unique maximal tamely ramified subfield $V$ (i.e., $p \nmid e(V/K)$) ([8], 3-4-7) such that the extension $T/K$ is unramified; $V/T$ is totally and tamely ramified and, therefore, the extension $L/V$ is totally ramified and $p|e(L/V)$. Moreover if

$$\vartheta_0 = \{\sigma \in G(L/K); (\sigma - 1)B \subset \mathbb{R}\}$$

$$\vartheta_1 = \{\sigma \in G(L/K); (\sigma - 1)B \subset \mathbb{R}^2\}$$

then $T = L^{\vartheta_0}$ ([8], 3-5-4) and $V = L^{\vartheta_1}$ ([8], 3-6-8). Now, $\sigma$ is wildly ramified if and only if $G = \vartheta_1$, which occurs if and only if $K = T = V$, which in turn is equivalent to $[L : K] = p^n$ for some $n$. □

Observe that the proof of the Theorem 2.1 gives an interesting property of the extension $L/K$. More precisely we have:

**Corollary 2.1.** Let $L$, $\sigma$ and $K$ as in the Theorem 2.1. Then $[L : K] = p^n$ if and only if $L/K$ is totally ramified.

**Definition 2.2.** If $\sigma \in \text{Aut}(L)$ is wildly ramified, we define the integer $i(\sigma)$ by

$$i(\sigma) = \nu_L((\sigma - 1)\pi/\pi);$$

where $\pi$ is a prime element $L$. For any integer $n$, $i(\sigma^n)$ is defined exactly as above (i.e. $i(\sigma^n) = \nu_L((\sigma^n - 1)\pi/\pi)$).

**Remark 2.1.** Since $L$ is complete, then, by [4], §1, $i(\sigma)$ does not depend on the choice of $\pi$. Moreover we can show that $i(\sigma^n)$ depends only on $0(\mu)$, where $p^{\mu(\nu)}$ is the highest power of $p$ dividing $\mu$.

On the other hand, from [4], Theorem 1 we have that, for all $n > 0$,

$$i(\sigma^{p^n-1}) \equiv i(\sigma^{p^n}) \mod (p^n),$$

so $i(\sigma^{p^n}) = (\sum_{k=1}^{n-1} \sigma^{\mu(k)} + \sigma^{\mu(k)})$ for all $0 \leq r \leq n - 1$, where $i(\sigma^{p^n-1}) = p^r \mu_n + i(\sigma^{p^n})$ for all $1 \leq r \leq n$. Wherever convenient we abbreviate and write $i(\mu)$ for $i(\sigma^{p^n})$. 
The following theorem uses the properties mentioned above to give a characterization of $H^1(G, B)$.

**Theorem 2.2.** ([4], Theorem 2) Suppose $\sigma \in Aut(L)$ has order $p^n$. Let $K = L^{<\sigma>}$ and let $A$ be its integer ring. Then

$$H^1(G, B) \cong \bigoplus_{\mu = 1}^{p^n-1} A/\pi^{\mu} A,$$

where $\mu = [(\mu + i(\mu))/p^n]$ ( $[x]$ denotes the greatest integer less than $x$) and $\pi$ is a prime element in $A$.

The following result shows an interesting fact about the numbers $\mu^*$, which will be used in the next section to prove the main theorem.

**Theorem 2.3.** $\sum_{\mu = 1}^{p^n-1} \frac{i(\mu)+1}{p^n} = \sum_{\mu = 1}^{p^n-1} \frac{i(\mu)+\mu}{p^n}$

**Demostración.** If $A_k = \{ \mu \in \mathbb{Z} : 1 \leq \mu \leq p^n-1; \mu = p^k s, \text{ with } (s, p) = 1 \}$, then it can be proved that $\text{Card}(A_k) = \varphi(p)p^{n-(k+1)}$. Then we have,

$$\sum_{\mu = 1}^{p^n-1} \frac{i(\mu)+1}{p^n} = \left[ \varphi(p) \sum_{j=1}^{n} \frac{i(\sigma^{p^j})+1}{p^n} \right] \left[ \varphi(p) \left( \sum_{j=1}^{n} \frac{\sum_{kp^{j-1}}^{p^{j-1}}} {p^n} (\sum_{k=0}^{n-1} p^k) \right) + 1 - \frac{1}{p^{n}} \right] = \left[ \varphi(p) \left( \sum_{j=1}^{n} (\sum_{k=0}^{n-1} p^k) m_j \right) + \frac{i(\sigma^{p^n})}{p^n} (\sum_{k=0}^{n-1} p^k) + 1 - \frac{1}{p^{n}} \right]$$

On the other hand,

$$\sum_{\mu = 1}^{p^n-1} \frac{i(\mu)+\mu}{p^n} = \sum_{j=1}^{n} \left( \sum_{k=1}^{j} \frac{i(\sigma^{p^j})+\mu}{p^n} \right)$$

where $\mu_{j-1}$ is the $k^{th}$ element of $A_{j-1}$.

We now consider two cases:

**Case 1.** If $p^n | i(\sigma^{p^n})$, we have

$$\sum_{\mu = 1}^{p^n-1} \frac{i(\mu)+1}{p^n} = \varphi(p) \left( \sum_{j=1}^{n} \left( \sum_{k=0}^{j-1} p^k \right) m_j \right) + \frac{i(\sigma^{p^n})}{p^n} \sum_{k=0}^{n-1} p^k$$

$$= \sum_{j=1}^{n} \sum_{k=0}^{j-1} \frac{i(\sigma^{p^j})}{p^n}.$$
On the other hand, since \(1 \leq \mu_k^{(j-1)} \leq p^n - 1\), then
\[
\sum_{\mu=1}^{p^n-1} \left[ \varphi(\mu) + \mu \right] = \sum_{j=1}^{n} \sum_{k=1}^{\varphi(p)p^{n-j}} \left[ \varphi(\mu^{(j-1)}) + \mu^{(j-1)} - \mu_k^{(j-1)} \right]
\]
\[
= \sum_{j=1}^{n} \sum_{k=1}^{\varphi(p)p^{n-j}} \left[ \varphi(\mu^{(j-1)}) + \mu^{(j-1)} \right].
\]
Therefore
\[
\left[ \sum_{\mu=1}^{p^n-1} \frac{i(\mu) + 1}{p^n} \right] = \sum_{\mu=1}^{p^n-1} \left[ \frac{i(\mu) + \mu}{p^n} \right].
\]

**Case 2.** If \(p^n \nmid i(\sigma^n)\), then \(i(\sigma^n) = p^n s + t\) with \(0 \leq t \leq p^n - 1\).
Therefore,
\[
\left[ \frac{i(\sigma^n)}{p^n} (p^n - 1) + \frac{p^n - 1}{p^n} \right] = s(p^n - 1) + (t + 1) + \left[ -\frac{t+1}{p^n} \right].
\]
If \(t = p^n - 1\), then
\[
\left[ \frac{i(\sigma^n)}{p^n} (p^n - 1) + \frac{p^n - 1}{p^n} \right] = i(\sigma^n) - s.
\]
If \(t < p^n - 1\), then
\[
\left[ \frac{i(\sigma^n)}{p^n} (p^n - 1) + \frac{p^n - 1}{p^n} \right] = sp^n - s + t + 1 - \left[ \frac{t+1}{p^n} \right] = i(\sigma^n) - s.
\]
Therefore
\[
\left[ \sum_{\mu=1}^{p^n-1} \frac{i(\mu) + 1}{p^n} \right] = \sum_{\mu=1}^{p^n-1} \varphi(p)(\sum_{j=1}^{n} \mu^{(j-1)} m_j) + i(\sigma^n) - s.
\]
On the other hand,
\[
\sum_{\mu=1}^{p^n-1} \left[ \frac{i(\mu) + \mu}{p^n} \right] = \sum_{\mu=1}^{p^n-1} \left[ \frac{\sum_{k=1}^{\sigma^{n-0(\mu)}} p^{0(\mu) + k} m_0(\mu) + k}{p^n} + \frac{i(\sigma^{p^n}) + \mu}{p^n} \right] \\
= \sum_{\mu=1}^{p^n-(t+1)} \left[ \frac{\sum_{k=1}^{\sigma^{n-0(\mu)}} p^{0(\mu) + k} m_0(\mu) + k}{p^n} + \frac{(t+\mu)}{p^n} \right] \\
+ \sum_{\mu=p^n-t}^{p^n-1} \left[ \frac{\sum_{k=1}^{\sigma^{n-0(\mu)}} p^{0(\mu) + k} m_0(\mu) + k}{p^n} + \frac{(t+\mu)}{p^n} \right] \\
= \sum_{\mu=1}^{p^n-(t+1)} \left[ \frac{\sum_{k=1}^{\sigma^{n-0(\mu)}} p^{0(\mu) + k} m_0(\mu) + k}{p^n} \right] + (p^n-(t+1))s \\
+ \sum_{\mu=p^n-t}^{p^n-1} \left[ \frac{\sum_{k=1}^{\sigma^{n-0(\mu)}} p^{0(\mu) + k} m_0(\mu) + k}{p^n} \right] + t(s+1) \\
= \sum_{\mu=1}^{p^n-1} \left[ \frac{\sum_{k=1}^{\sigma^{n-0(\mu)}} p^{0(\mu) + k} m_0(\mu) + k}{p^n} \right] + i(\sigma^{p^n}) - s \\
= \sum_{\mu=1}^{p^n-1} \phi(p) \left( \sum_{j=1}^{n} \left( \sum_{k=0}^{j-1} p^k m_j \right) \right) + i(\sigma^{p^n}) - s.
\]

3. Main theorem.

To prove the main result we use the following theorem of localization which reduces the proof to the local case.

**Theorem 3.1.** ([6], Theorem 1.16) Let \( \phi \) be a set of prime ideals of \( B \) containing exactly one divisor \( \mathfrak{R} \) of each prime ideal \( \mathfrak{p} \) of \( A \). Then
\[
H^i(G, B) \cong \bigoplus_{\mathfrak{R} \in \phi} H^i(G_{\mathfrak{R}, \widehat{B}_{\mathfrak{R}}}),
\]
where \( G_{\mathfrak{R}} \) is the decomposition group of \( \mathfrak{R} \) in \( L/K \) and \( \widehat{B}_{\mathfrak{R}} \) is the integral ring of the \( \mathfrak{R} \)-adic completion \( \widehat{L}_{\mathfrak{R}} \) of \( L \).

**Proof of Theorem 1.1.** In [1] we proved that, with the same hypothesis of Theorem 3.1, we have an isomorphism of groups of cohomology.
\[ H^i(G_R, \widehat{B}_R) \cong H^i(G_p, R_p), \]

where \( G_p \) is a \( p \)-Sylow subgroup of \( G_R \) and \( R_p = B_R \overline{H_p} \), with \( H_p \cong G_R/G_p \) and by [9], Proposition 3-2-1 we have

\[ H^0(G_p, R_p) \cong A_p/\text{SR}_p. \]

On the other hand, if \( A = \pi\widehat{A}_p \) denotes the maximal ideal of \( \widehat{A}_p \), then \( \text{SR}_p = A^{(D)} \), where \( (D) \) is the order of \( \text{SR}_p \) in \( K_p \). Therefore, by ([5], Chap I, §5) and ([3], Chap I, §7) we have:

\[ o(H^0(G_p, R_p)) = o(\widehat{A}_p/A^{(D)}) = N_{K_p/K_p}(A^{(D)}) = (N_{K_p/K_p}(A))^{(D)} = p^{f(D)}, \]

where \( f \) is the residual degree of \( K_p/B_p \). On the other hand, by Theorem 2.2,

\[ o(H^1(G_p, R_p)) = \prod_{j=1}^{p^n-1} o(\widehat{A}_p/\pi^{j^*} \widehat{A}_p) = \prod_{j=1}^{p^n-1} o(\widehat{A}_p/A^{j^*}) = \prod_{j=1}^{p^n-1} p^{j^*} = p^{\sum_{j=1}^{p^n-1} j^*}. \]

Now, by Corollary 2.1, \( F/K_p \) (where \( F = L_R \overline{H_p} \)) is totally ramified, and by ([7], Lema 2.)

\[ (D) = \nu_{K_p}(\text{SR}_p) = \left[ \frac{\nu_F(D_{F/K_p})}{p^n} \right]. \]

Moreover, from ([5], Chap II, Proposition 4.)

\[ \nu_F(D_{F/K_p}) = \sum_{j=1}^{p^n-1} i(j) + 1, \]

and thus

\[ (D) = \left[ \sum_{j=1}^{p^n-1} \frac{i(j) + 1}{p^n} \right]. \]

Now, by Theorem 2.3 we have \((D) = \sum_{j=1}^{p^n-1} (j) \) (\( (j) \) as in Theorem 2.2) and then,

\[ o(H^1(G_p, R_p)) = o(H^0(G_p, R_p)). \]

Now, using Theorem 3.1 and the fact that \( L/K \) is cyclic, we finally conclude that the cohomology groups have the same order.
References


Dirección del autor: Álvaro Garzón Rojas. Departamento de Matemáticas, Universidad del Valle, Cali, Colombia, A.A 25360, e-mail: alvarogr@mafida.univalle.edu.co.