Vol. X, N<u>o</u> 2 Jun (2002)
Matemáticas: 85–91

**Matemáticas:
Enseñanza Universitaria**

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, $\Re$ is the maximal ideal in B and $\overline{L}=B/\Re$ is the residue class field. Let ν_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 σ is a wildly ramified automorphism of L if

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

for all x $\in$ B.

Note that if σ is wildly ramified then $(\sigma-1)B \subset \Re^2$ and σ^n is wildly ramified for all integers n. Therefore, the first ramification group of $\Re$ contains the group $G =< \sigma >$. Now we give a result that explores this property.

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

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 unramied; V/T is totally and tamely ramified and, therefore, the extension L/V is totally ramified and $p|e(L/V)$. Moreover if

$$\vartheta_0 = \{\sigma \in G(L/K); (\sigma-1)B \subset \Re\}$$
$$\vartheta_1 = \{\sigma \in G(L/K); (\sigma-1)B \subset \Re^2\}$$

then $T = L^{\vartheta_0}$ ([8], 3-5-4) and $V = L^{\vartheta_1}$ ([8], 3-6-8).
Now, σ 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, σ 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 $\sigma \in Aut(L)$ is wildly ramified, we define the integer $i(\sigma)$ by

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

where π 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 π. Moreover we can show that $i(\sigma^\mu)$ depends only on $0(\mu)$, where $p^{0(\mu)}$ is the highest power of p dividing μ.
On the other hand, from [4], Theorem 1 we have that, for all $n > 0$,

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

so $i(\sigma^{p^r}) = (\sum_{k=1}^{k=n-r} p^{r+k} m_{r+k}) + i(\sigma^{p^n})$ for all $0 \leq r \leq n-1$, where $i(\sigma^{p^{r-1}}) = p^r m_r + i(\sigma^{p^r})$ for all $1 \leq r \leq n$. Wherever convenient we abbreviate and write $i(\mu)$ for $i(\sigma^{p^\mu})$.

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*

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

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

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

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

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 $\operatorname{Card}(A_k) = \varphi(p)p^{n-(k+1)}$. Then we have,

$$\begin{aligned}
\left[\sum_{\mu=1}^{\mu=p^n-1} \frac{i(\mu)+1}{p^n}\right] &= \left[\varphi(p)\sum_{j=1}^{n} \frac{i(\sigma^{p^{j-1}})+1}{p^j}\right]\left[\varphi(p)\left(\sum_{j=1}^{n}\left(\frac{\sum_{k=j}^{n} p^k m_k}{p^j}\right)\right) + \right. \\
&\quad \left. \frac{i(\sigma^{p^n})}{p^n}\left(\sum_{k=0}^{n-1} p^k\right) + 1 - \frac{1}{p^n}\right] \\
&= \left[\varphi(p)\left(\sum_{j=1}^{n}\left(\sum_{k=0}^{j-1} p^k\right)m_j\right) + \frac{i(\sigma^{p^n})}{p^n}\left(\sum_{k=0}^{n-1} p^k\right) + \right. \\
&\quad \left. 1 - \frac{1}{p^n}\right]
\end{aligned}$$

On the other hand,

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

where $\mu_k^{(j-1)}$ 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

$$\begin{aligned}
\sum_{\mu=1}^{p^n-1} \frac{i(\mu)+1}{p^n} &= \varphi(p)\Big(\sum_{j=1}^{n}\Big(\sum_{k=0}^{j-1} p^k\Big)m_j\Big) + \frac{i(\sigma^{p^n})}{p^n}\sum_{k=0}^{n-1} p^k \\
&= \sum_{j=1}^{n}\sum_{k=1}^{\varphi(p)p^{n-j}} \frac{i(\sigma^{p^{j-1}})}{p^n}.
\end{aligned}$$

On the other hand, since $1 \leq \mu_k^{(j-1)} \leq p^n - 1$, then

$$\begin{aligned}\sum_{\mu=1}^{p^n-1}\left[\frac{i(\mu)+\mu}{p^n}\right] &= \sum_{j=1}^{n}\sum_{k=1}^{\varphi(p)p^{n-j}}\left[\frac{i(\sigma^{p^{j-1}})+\mu_k^{(j-1)}}{p^n}\right]\\ &= \sum_{j=1}^{n}\sum_{k=1}^{\varphi(p)p^{n-j}}\left[\frac{i(\sigma^{p^{j-1}})}{p^n}\right].\end{aligned}$$

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 $p^n \nmid i(\sigma^{p^n})$, then $i(\sigma^{p^n}) = p^n s + t$ with $0 \leq t \leq p^n - 1$. Therefore,

$$\left[\tfrac{i(\sigma^{p^n})}{p^n}(p^n-1)+\tfrac{p^n-1}{p^n}\right] = s(p^n-1)+(t+1)+\left[-\tfrac{(t+1)}{p^n}\right].$$

If $t = p^n - 1$, then

$$\left[\tfrac{i(\sigma^{p^n})}{p^n}(p^n-1)+\tfrac{p^n-1}{p^n}\right] = i(\sigma^{p^n}) - s.$$

If $t < p^n - 1$, then

$$\left[\tfrac{i(\sigma^{p^n})}{p^n}(p^n-1)+\tfrac{p^n-1}{p^n}\right] = sp^n - s + t + 1 - 1 - \left[\tfrac{t+1}{p^n}\right] = i(\sigma^{p^n}) - s.$$

Therefore

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

On the other hand,

$$\begin{aligned}
\sum_{\mu=1}^{p^n-1}\left[\frac{i(\mu)+\mu}{p^n}\right] &= \sum_{\mu=1}^{p^n-1}\left[\frac{\sum_{k=1}^{n-0(\mu)} p^{0(\mu)+k}m_{0(\mu)+k}}{p^n}+\frac{i(\sigma^{p^n})+\mu}{p^n}\right]\\
&= \sum_{\mu=1}^{p^n-(t+1)}\left[\frac{\sum_{k=1}^{n-0(\mu)} p^{0(\mu)+k}m_{0(\mu)+k}}{p^n}+s+\frac{(t+\mu)}{p^n}\right]\\
&+ \sum_{\mu=p^n-t}^{p^n-1}\left[\frac{\sum_{k=1}^{n-0(\mu)} p^{0(\mu)+k}m_{0(\mu)+k}}{p^n}+s+\frac{(t+\mu)}{p^n}\right]\\
&= \sum_{\mu=1}^{p^n-(t+1)}\left[\frac{\sum_{k=1}^{n-0(\mu)} p^{0(\mu)+k}m_{0(\mu)+k}}{p^n}\right]+(p^n-(t+1))s\\
&+ \sum_{\mu=p^n-t}^{p^n-1}\left[\frac{\sum_{k=1}^{n-0(\mu)} p^{0(\mu)+k}m_{0(\mu)+k}}{p^n}\right]+t(s+1)\\
&= \sum_{\mu=1}^{p^n-1}(\left[\frac{\sum_{k=1}^{n-0(\mu)} p^{0(\mu)+k}m_{0(\mu)+k}}{p^n}\right])+i(\sigma^{p^n})-s\\
&= \sum_{\mu=1}^{p^n-1}\varphi(p)(\sum_{j=1}^{n}(\sum_{k=0}^{j-1}p^k)m_j)+i(\sigma^{p^n})-s.
\end{aligned}$$

□

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 ϕ be a set of prime ideals of B containing exactly one divisor $\Re$ of each prime ideal $\wp$ of A. Then*

$$H^i(G,B)\cong\bigoplus_{\Re\in\phi}H^i(G_{\Re},\widehat{B_{\Re}}),$$

where $G_{\Re}$ is the decomposition group of $\Re$ in L/K and $\widehat{B_{\Re}}$, is the integer ring of the $\Re$-adic completation $\widehat{L_{\Re}}$ 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

$$H^i(G_{\Re}, \widehat{B_{\Re}}) \cong H^i(G_p, R_p),$$

where G_p is a p-Sylow subgroup of $G_{\Re}$ and $R_p = \widehat{B_{\Re}}^{H_p}$, with $H_p \cong G_{\Re}/G_p$ and by [9], Proposition 3-2-1 we have

$$H^0(G_p, R_p) \cong \widehat{A_{\wp}}/SR_p.$$

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

$$o(H^0(G_p, R_p)) = o(\widehat{A_{\wp}}/\mathcal{A}^{(D)}) = N_{\widehat{K_{\wp}}/\mathbb{Q}_p}(\mathcal{A}^{(D)}) = (N_{\widehat{K_{\wp}}/\mathbb{Q}_p}(\mathcal{A}))^{(D)} = p^{f.(D)},$$

where f is the residual degree of $\widehat{K_{\wp}}/B_p$. On the other hand, by Theorem 2.2,

$$\begin{aligned} o(H^1(G_p, R_p)) &= \prod_{j=1}^{p^n-1} o(\widehat{A_{\wp}}/\pi^{j^*}\widehat{A_{\wp}}) = \prod_{j=1}^{p^n-1} o(\widehat{A_{\wp}}/\mathcal{A}^{j^*}) \\ &= \prod_{j=1}^{p^n-1} p^{f.j^*} \\ &= p^{f.\sum_{j=1}^{p^n-1} j^*}. \end{aligned}$$

Now, by Corollary 2.1, $F/\widehat{K_{\wp}}$, (where $F = \widehat{L_{\Re}}^{H_p}$) is totally ramified, and by ([7], Lema 2.)

$$(D) = \nu_{\widehat{K_{\wp}}}(SR_p) = \left[\frac{\nu_F(\mathfrak{D}_{F/\widehat{K_{\wp}}})}{p^n}\right].$$

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

$$\nu_F(\mathfrak{D}_{F/\widehat{K_{\wp}}}) = \sum_{j=1}^{p^n-1} i(j) + 1,$$

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

[1] A. Garzón, M. Suárez. *Reducción de un problema de cohomología local.* Revista de Ciencias. Universidad del Valle Vol 10, 1995.

[2] G. Januz. *Algebraic Number Fields.* Academic Press, 1973.

[3] S. Lang. *Algebraic Number Theory.* Addison Wesley, 1970.

[4] S. Sen. *On Automorphisms of Local Fields.* Annals of Mathematics, Vol 90, 1969.

[5] J. P. Serre. *Corps Locaux.* Herman, París 1968.

[6] M. F. Suárez. *Galois Cohomology in Dedekind Domains.* Mathematics Departament Cornell, Ph.D. thesis, 1975.

[7] M. F. Suárez. *Cohomología local de las extensiones cíclicas de grado primo.* Revista Colombiana de Matemáticas, Números 3-4, 1985.

[8] E. Weiss. *Algebraic Number Theory.* Academic Press, 1963.

[9] E. Weiss. *Cohomology of Groups.* Academic Press, 1967.

[10] I. Yokoi. *A note on the Galois cohomology group on the ring integers in an algebraic number field.* Proc. Japan Acad, 40, 1964.

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