Revista Colombiana de Matemáticas
Vol. XIX (1985), págs. 251-261

COHOMOLOGIA LOCAL DE LAS EXTENSIONES CICLICAS DE GRADO PRIMO

por

Marco Fidel SUAREZ R.

RESUMEN. Se utiliza un teorema de localización de cohomología para demostrar un teorema de Hideo Yokoi sobre cohomología de extensiones cíclicas de grado primo de cuerpos numéricos. Para ello, se reduce el teorema al caso local y se calculan explícitamente los grupos de cohomología de dimensión 0 y -1, mostrando que son isomorfos.

ABSTRACT. In this paper we use a theorem of localization of cohomology to prove a theorem of Hideo Yokoi on the cohomology of a cyclic extension of number fields of primer degree. We reduce this theorem to the local case and compute explicity the cohomology groups of dimensions 0 and -1, observing that they are isomorphic.

§1. <u>Introducción</u>. Sean K y L cuerpos numéricos, L extensión finita de K con grupo de Galois G, A y B los respectivos anillos de enteros de K y L. En [6] H. Yokoi consideró a B como $\mathbb{Z}[G]$ módulo y en particular demostró

TEOREMA 1. *Si* K *y* L *son extensiones normales de* $\mathbb{Q}$ *y* L/K *es cíclica de grado primo* p, *entonces todos los grupos de cohomología de* B *con respecto a* L/K *son isomorfos entre sí; en otras palabras* $H^i(G,B) \cong H^j(G,B)$, *para cualquier par de enteros* i *y* j *(ver* [4]).

En el presente artículo demostraremos este resultado utilizando el siguiente teorema de localización ([3]).

TEOREMA 2. *Si* Φ *es un conjunto de ideales primos de* L *que contienen exactamente un divisor* q *de cada ideal primo* $\mathcal{P}$ *de* K, *entonces para cualquier entero* i

$$H^i(G,B) \simeq \oplus\, H^i(G_q,\hat{B}_q) \quad (q \in \Phi)$$

donde $\hat{B}_q$ *es el anillo de enteros de la completación* q-*ádica* $\hat{L}_q$ *de* L *y* G_q *es el grupo de descomposición de* q *en* L/K.

En la situación particular del Teorema 1, tenemos el siguiente corolario del Teorema 2.

COROLARIO. *Si* K *y* L *son extensiones normales de* $\mathbb{Q}$ *y* L/K *es cíclica de grado primo* p, *entonces* $H^i(G,B) \simeq H^i(G_q,\hat{B}_q)$ *para todo entero* i *donde* q *es un ideal primo en* L *que divide a* p.

Demostración. Si $\mathcal{P}$ es cualquier ideal primo en K y $\mathcal{P} \cap \mathbb{Z} \neq p$, sea q un ideal primo de L que divide a $\mathcal{P}$; la característica del cuerpo residual $\bar{K}_{\mathcal{P}}$, siendo distinta de p, no divide el índice de ramificación de q sobre $\mathcal{P}$; por lo tanto, la extensión local $L_q/K_{\mathcal{P}}$ es suavemente ramificada (ver [1] I,§5 pág.21) y $H^i(G_q,\hat{B}_q) = 0$ para todo entero i

([3],Cor.1). El resultado del Corolario es entonces consecuencia del Teorema 2. ▲

OBSERVACIONES. Consideramos pertinentes las siguientes observaciones:

(i) El corolario anterior reduce el Teorema 1 al caso de extensiones locales.

(ii) Como G es un grupo cíclico, sabemos ([4], 3-2-1) que para todo entero i y todo G-módulo B

$$H^i(G,B) \simeq H^{i+2}(G,B).$$

Según estas observaciones podemos simplificar el Teorema 1 en la forma siguiente:

TEOREMA 3. *Si* K *es una extensión normal de* $\mathbb{Q}_p$, L/K *es una extensión cíclica de grado* p, A *(resp.*B*) es el anillo de enteros de* K *(resp.*L*) y* G *el grupo de Galois de* L/K, *entonces* $H^0(G,B) \simeq H^{-1}(G,B)$.

Observemos que en caso de que L/K sea suavemente ramificada el resultado es trivial pues todo grupo de cohomología es 0. Por lo tanto podemos suponer que L/K es *totalmente ramificada y fuertemente ramificada.*

§2. Cálculo de los grupos de cohomología $H^0(G,B)$ y $H^{-1}(G,B)$.

A continuación, procederemos a calcular los dos grupos de cohomología anteriores mediante algunos lemas auxiliares.

LEMA 1. *En las mismas condiciones del Teorema 3, el conjunto* SB *de las trazas de los elementos de* B, *constituye un ideal entero de* K, *el cual divide a* $\mathcal{D}$, *"el diferente" de la extensión* ([1], 1, §4, pág. 16).

Demostración. Sea $\mathfrak{A}$ = SB; afirmamos que $\mathfrak{A}^{-1} = \mathcal{D}^{-1} \cap K$. En efecto, $\alpha \in \mathfrak{A}^{-1}$ si y sólo si $\alpha \in K$ y para todo $b \in B$, $\alpha S(b) \in A$, si y sólo si $\alpha \in K$ y $S(\alpha b) \in A$ para todo $b \in B$, si y sólo si $\alpha \in K$ y $\alpha \in \mathcal{D}^{-1}$. De lo anterior concluímos que $\mathfrak{A}^{-1} B \subset \mathcal{D}^{-1}$ y $\mathcal{D} \subset \mathfrak{A}B$, es decir $\mathfrak{A} | \mathcal{D}$. ▲

LEMA 2. *Si* $r = v_K(\mathfrak{A})$, $v = v_L(\mathcal{D})$ *donde* v_K *y* v_L *son las valuaciones de* K *y* L *respectivamente, entonces* $v = re+t$, $0 \leqslant t < e$ (e *es el índice de ramificación de la extensión* L/K), *es decir,* $[v/e] = r$ ([ ] *es la función parte entera*).

Demostración. Según el Lema 1, $v \geqslant re$. Si fuera $(r+1)e \leqslant v$ entonces tendríamos $\mathcal{D} \subset P^{r+1}B$ (P el ideal maximal de K) de lo cual $\mathcal{D} \subset q^{(r+1)e}$ (q el idel maximal de L); pero entonces $q^{-(r+1)e} \subset \mathcal{D}^{-1}$, lo cual implicaría

$$q^{-(r+1)e} \cap K \subset \mathcal{D}^{-1} \cap K = \mathfrak{A}^{-1}.$$

Por otra parte, $P^{-(r+1)} \subset q^{-(r+1)e} \cap K$ y en consecuencia $P^{-(r+1)} \subset \mathfrak{A}^{-1} = P^{-r}$, lo cual es absurdo. ▲

En las mismas condiciones del Teorema 3, si σ es un generador del grupo G, definimos el *número de ramificación* de L/K por $N(\sigma) = v_L \frac{(\sigma-1)\pi}{\pi} = i(\sigma)-1$ ($i(\sigma)$ definido en [2], IV, §1) donde π es un elemento primo en L. Es fácil ver que $N(\sigma)$ no depende del primo π.

PROPOSICION. *En las condiciones del Teorema 3,*

$i(\sigma^{\nu}) = i(\sigma)$ *para todo* ν *tal que* $1 < \nu \leqslant p-1$.

Demostración. Siendo L/K fuertemente ramificada, entonces $i(\sigma) > 1$ ([5], 3-6-8) e inductivamente puede demostrarse que, para $1 < \nu \leqslant p-1$,

$$v_L(\sigma^{\nu}-1)\pi = v_L[(\sigma-1)(\sigma^{\nu-1}+\sigma^{\nu-2}+\ldots+\sigma+1)]\pi$$

$$= v_L(\sigma-1)\pi. \quad \blacktriangle$$

LEMA 3. *Si* $s = N(\sigma) - [N(\sigma)/p]$ *y* $n = [K:\mathbb{Q}_p]$, *entonces*

$$H^{o}(G,B) \simeq \mathbb{Z}/p\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p\mathbb{Z} \text{ (ns/ek veces)}$$

donde e_K *es el índice de ramificación de* p *en* K.

Demostración. Tenemos $v = v_L(\mathcal{D}) = \sum_{\nu=1}^{p-1} i(\sigma^{\nu}) = (p-1)(N(\sigma)+1)$ ([2],Prop.4, IV,§1). Sea $N(\sigma) = pm+t$, $0 \leqslant t < p$; si tomamos $r = p-(t+1)$, entonces también $0 \leqslant r < p$, y sustituyendo en la fórmula para v tendremos

$$v = (p-1)(pm+t+1) = p((p-1)m+t)+r$$

$$= p(N(\sigma)-m)+r = p(N(\sigma)-[N(\sigma)/p])+r = ps+r.$$

De acuerdo con el Lema 2 y la suposición de que L/K es una extensión totalmente ramificada (e = p) concluímos que SB = $\mathcal{P}^s$. Por otra parte, $H^{o}(G,B) \simeq A/SB$ ([4], 1-5-6); luego $H^{o}(G,B) \simeq A/\mathcal{P}^s$, de donde

$$\#H^{o}(G,B) = \operatorname{card}(A/\mathcal{P}^s) = N_{K/\mathbb{Q}p}(\mathcal{P}^s) = (N_{K/\mathbb{Q}p}(\mathcal{P}))^s = p^{ns/e_K}$$

pues $n/e_k = [\bar{K}:\bar{\mathbb{Q}}_p]$ (grado residual); puesto que $p = \#G$ anula $H^{o}(G,B)$ ([4], 3-1-6), se tiene el resultado del Lema 3. $\blacktriangle$

Ahora construiremos una base para B sobre A.

LEMA 4. *Para cada* j, $1 \leqslant j \leqslant p-1$ *existe* $x_j \in B$ *tal que* $v_L(x_j) = j$ *y* $v_L(\sigma-1)x_j = j+N(\sigma)$.

Demostración. Si π es un elemento primo en L, sea $x_j = \prod_{i=0}^{j-1} \sigma^i(\pi)$ para $1 \leqslant j \leqslant p-1$, es claro que $v_L(x_j) = j$. Además, $\sigma x_j/x_j = \sigma^j\pi/\pi$ implica que $(\sigma-1)x_j/x_j = (\sigma^j-1)\pi/\pi$. Ahora bien, $v_L(\sigma^j-1)\pi/\pi = N(\sigma)$ (según la proposición). Por lo tanto $v_L \frac{(\sigma-1)x_j}{x_j} = N(\sigma)$, y entonces

$$v_L(\sigma-1)x_j = v_L(x_j)+N(\sigma) = j+N(\sigma). \quad \blacktriangle$$

LEMA 5. *El conjunto* $\{1 = x_o, x_1, \ldots, x_{p-1}\}$, *constituye una base para* B *sobre* A.

Demostración. Los elementos del anterior conjunto son representantes de todas las distintas coclases de $v_L(K^*)$ en $v_L(L^*)$ ([5], cap.I, 6); además siendo L/K totalmente ramificada $[\bar{L}:\bar{K}] \doteq 1$, entonces dicho conjunto es linealmente independiente sobre A ([5], 1-6-3).

Si π es un primo fijo en B, afirmamos que $B = A+\pi B$. En efecto, si $\alpha \in B$ entonces $\bar{\alpha} = \bar{a}_1 \cdot \bar{1}$, donde $\bar{a}_1 \in \bar{K}$ es la coclase de cierto $a_1 \in A$, y $\bar{\alpha}$ y $\bar{1}$ son las coclases respectivas de α y 1 en $\bar{L}$. Entonces

$$\alpha = a_1 + \pi\alpha_o, \text{ con } \alpha_o \in B.$$

Puesto que $\pi B = \sigma(\pi)B = \sigma^2(\pi)B = \ldots = \sigma^{p-1}(\pi)B$ tendremos

$$B = A+\pi(A+\pi B) = A+\pi(A+\sigma(\pi)B)$$

$$= A+\pi A+\pi\sigma(\pi)B = x_oA+x_1A+x_2B = \ldots$$

$$= x_oA+x_1A+x_2A+\ldots+x_{p-1}A+\pi^pB.$$

En otras palabras, para todo $\alpha \in B$.

$$\alpha = \sum_{j=0}^{p-1} c_j x_j + \pi^p b, \text{ para algunos } b \in B,\ c_j \in A;$$

pero $\pi^p B = \pi_o B$, siendo π_o un primo en A; entonces

$$\alpha = \sum_{j=0}^{p-1} a_j^{(o)} x_j + \pi_o \alpha_1; \quad \alpha_1 \in B,\ a_j^{(o)}, s \in A;$$

así mismo

$$\alpha_1 = \sum_{j=0}^{p-1} a_j^{(1)} x_j + \pi_o \alpha_2.$$

Obtenemos entonces una sucesión $\alpha_1, \alpha_2, \ldots$, en B tal que $\alpha_n = \sum_{j=0}^{p-1} a_j^{(n)} x_j + \pi_o \alpha_{n+1}$; además, para j fijo, $\{a_j^{(n)}\}$ es una sucesión en A.

Consideremos la serie $\sum_{n=0}^{\infty} a_j^{(n)} \pi_o^n$; puesto que $a_j^{(n)} \in A$, esta serie converge ([5],1-7) hacia un $a_j \in A$. Por la construcción de la sucesión $\alpha_1, \alpha_2, \ldots$, tenemos

$$\alpha = \sum_{k=0}^{n-1} \left(\sum_{j=0}^{p-1} a_j^{(k)} x_j \right) \pi_o^k + \pi_o^n \alpha_n, \quad \text{para todo } n \in \mathbb{N},$$

y haciendo tender n a infinito obtenemos $\alpha = \sum_{j=0}^{p-1} a_j x_j$, tal como queríamos demostrar.

LEMA 6. *El conjunto* $\{y_1, y_2, \ldots, y_{p-1}\}$ *donde para todo* j, $1 \leqslant j \leqslant p-1$, $y_j = (\sigma-1)x_j$, *es una base de* $(\sigma-1)B$ *sobre* A.

Demostración. Según el lema anterior basta demostrar su independencia lineal. Supongamos que tenemos $\sum_{j=1}^{p-1} a_j y_j = 0$, donde los $a_j \in A$ no son todos cero. Podemos suponer que por lo menos un a_j es una unidad de A. Sea j_o

el menor subíndice tal que a_{j_o} es una unidad, entonces $v_L(a_{j_o}y_{j_o}) = j_o+N(\sigma)$; pero

$$a_{j_o}y_{j_o} = -\sum_{j\neq j_o} a_j y_j$$

y para $j < j_o$,

$$v_L(a_j y_j) = j+N(\sigma)+v_L(a_j) = j+pv_K(a_j)+N(\sigma) \geqslant j_o+N(\sigma);$$

también para $j > j_o$, $v_L(a_j y_j) \geqslant j+N(\sigma) > j_o+N(\sigma)$; por lo tanto

$$v_L(a_{j_o}y_{j_o}) \geqslant \min_{j\neq j_o} \{v_L(a_j y_j)\} > j_o+N(\sigma),$$

lo cual es una contradicción. ▲

Observemos que $H^{-1}(G,B) \simeq B_S/(\sigma-1)B$ ([4],3-2-1); en consecuencia, a fin de calcular este grupo de cohomología debemos estudiar ahora B_S, el cual consiste de los elementos de B cuya traza es cero. Debemos tener en cuenta además que $B_S = B \cap (\sigma-1)L$. En efecto, $B_S \subset B \cap L_S$, pero $L_S = (\sigma-1)L$, porque $H^{-1}(G,L^+) = 0$ ([4],3-1-4).

LEMA 7. *El conjunto* $\{y_j/\pi_o^{(j)}\}_{j=1}^{p-1}$ *donde* π_o *es un primo en* A *y* $(j) = [j+N(\sigma)/p]$ ([ ] *función parte entera*) *es una base de* B_S *sobre* A.

Demostración. Observemos en primer lugar que para $1 \leqslant j \leqslant p-1$,

$$v_L(y_j/\pi_o^{(j)}) = j+N(\sigma)-p\left[\frac{j+N(\sigma)}{p}\right] > 0.$$

Dado $\alpha \in B_S$, de acuerdo con observaciones anteriores

$$\alpha = \sum_{j=1}^{p-1} q_j y_j, \text{ donde los } q_j \in K.$$

Los números enteros $v_L(q_j y_j) = pv_K(q_j)+j+N(\sigma)$ son distintos entre sí, y puesto que $v_L(\sigma) \geqslant 0$, para todo $1 \leqslant j \leqslant p-1$, entonces $v_L(q_j y_j) \geqslant 0$; es decir,

$$pv_K(q_j) \geqslant -j-N(\sigma),$$

de donde

$$v_K(q_j) \geqslant -\frac{j+N(\sigma)}{p}.$$

Si para cada $1 \leqslant j \leqslant p$, escribimos

$$q_j = b_j/\pi_o^{(j)} \quad \text{con } b_j \in K$$

entonces

$$v_K(b_j) = v_K(q_j)+(j) \geqslant \left[\frac{j+N(\sigma)}{p}\right] - \frac{j+N(\sigma)}{p};$$

de aquí se concluye que para $1 \leqslant j \leqslant p-1$, $v_K(b_j) \geqslant 0$; en otras palabras,

$$\alpha = \sum_{j=1}^{p-1} b_j \frac{y_j}{\pi_o^{(j)}}, \text{ con los } b_j \in A. \quad ▲$$

PROPOSICION. $\sum_{j=1}^{p-1} \left[\frac{j+N(\sigma)}{p}\right] = N(\sigma) - \left[\frac{N(\sigma)}{p}\right] = s$ (*ver Lema 3*).

Demostración. Supongamos en primer lugar que $p|N(\sigma)$, entonces

$$\sum_{j=1}^{p-1} \left[\frac{j+N(\sigma)}{p}\right] = (p-1)\frac{N(\sigma)}{p} = s.$$

Si por el contrario, $p \nmid N(\sigma)$, sea $N(\sigma) = pm+t$, $0 < t < p$; entonces

$$\sum_{j=1}^{p-1} \left[\frac{j+N(\sigma)}{p}\right] = \sum_{j=1}^{p-(t+1)} \left[\frac{N(\sigma)}{p}\right] + \sum_{j=p-t}^{p-1} \left[\frac{j+N(\sigma)}{p}\right] =$$

$$= (p-t-1)m + t(m+1) = N(\sigma)-m = N(\sigma) - \frac{N(\sigma)}{p} = s.$$

LEMA 8. $H^{-1}(G,B) \simeq \mathbb{Z}/p\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p\mathbb{Z}$ (ns/e_k *veces*).

Demostración.

$$H^{-1}(G,B) \simeq \frac{B_s}{(\sigma-1)B} \simeq (\bigoplus_{p-1}^{p-1} Ay_j/\pi_o^{(j)})/(\bigoplus_{j-1}^{p-1} Ay_j)$$

$$\simeq \bigoplus_{j=1}^{p-1} \frac{Ay_j/\pi_o^{(j)}}{Ay_j} \simeq \bigoplus_{j=1}^{p-1} \frac{A}{\pi_o^{(j)}A} .$$

Por otra parte,

$$\mathrm{Ord}(H^{-1}(G,B)) = \prod_{j=1}^{p-1} \mathrm{Ord}(\frac{A}{\pi_o^{(j)}A}) = \prod_{j=1}^{p-1} N_{K/\mathbb{Q}_p}(\pi_o^{(j)})$$

$$= \prod_{j=1}^{p-1} (N_{K/\mathbb{Q}_p}(\pi_o))^{(j)} = \prod_{j=1}^{p-1} p^{n(j)/e_k}$$

$$= p^{\frac{n}{e_k}\sum_{j=1}^{p-1}(j)} = p^{ns/e_k}$$

y el hecho de que p anula $H^{-1}(G,B)$ completa la demostración del Lema 8. ▲

BIBLIOGRAFIA

[1] Cassels, J.W.S. and Frolich, A., *Algebraic Number Theory*, Thompson, 1967.

[2] Serre, J.P., *Corps Locaux*, Hermann, 1968.

[3] Suárez, M.F., *Localization of the Cohomology of a Finite Galois Group in a Dedekind Domain*, Rev.Col. de Matemáticas, Vol. X (1976), 51-55.

[4] Weiss, E., *Cohomology of Groups*, Academic Press, 1969.

[5] Weiss, E., *Algebraic Number Theory*, McGraw-Hill, 1963.
[6] Yokoi, H., *On the Galois Cohomology Group of the Ring of Integers in an Algebraic Number Field*, Acta Arithmetica VIII (1963).

Departamento de Matemáticas
Universidad del Valle
Apartado áereo 2188
CALI, Colombia.

(Recibido en Octubre de 1984).