

LA MÁXIMA EXTENSIÓN ABELIANA DE UN CUERPO LOCAL COMO UNA EXTENSIÓN KUMMERIANA, II : CÁLCULO EXPLÍCITO DE ALGUNAS BASES

por

Víctor Samuel ALBIS GONZÁLEZ

Dedicado al profesor Henri Yerly

§ 1. *Introducción.* En esta segunda parte seguiremos usando la notación introducida en la primera ([1]), en la cual hemos expresado la máxima extensión abeliana L_a/L de un cuerpo local L/\mathbb{Q}_p en la forma $L_q(\sqrt[q]{\beta}) = L_a$, $\beta \in L^{\times} \text{ mód } L^{\times q}$, $\text{Gal}(L_a/L_q) \approx \mu_q = \text{grupo de las raíces } q\text{-ésimas de } 1 \text{ contenidas en } L$, donde q es la potencia de p máxima con esta propiedad. Recordemos que los $\beta \in L^{\times} \text{ mód } L^{\times q}$ que satisfacen la anterior propiedad (la cual hemos denominado P) fueron determinados en los teoremas 5 y 6 de [1] pero que, sin embargo, en el caso en que $L(\sqrt[q]{\zeta_q})/L$, donde ζ_q es una raíz primitiva q -ésima de L , ramificase totalmente [1 ; teorema 6], un conocimiento explícito de los β que cumplían P requería un conocimiento también explícito de las bases cuya existencia se demostraba en los teorema 1 y 2 de [1]. Es, pues, nuestro propósito explicitar algunas de estas bases, en especial cuando $L = \mathbb{Q}_p(\zeta_q)$. Para ello será necesario servirnos de algunas relaciones entre los símbolos locales y la ley de reciprocidad potencial. Para las correspondientes definiciones y resultados, y sus demostraciones, remitimos

a [5 : chapter 13] y [2].

PROPOSICIÓN 1. Sea dado $\varepsilon \in \mathbb{Q}(\zeta_q)$, $\varepsilon \equiv 1 \pmod{\pi}$, donde $\pi = 1 - \zeta_q$. Entonces :

$$a) \left(\frac{\zeta_q}{\varepsilon} \right) = (\varepsilon, \zeta_q)$$

donde el miembro izquierdo representa al símbolo de reciprocidad potencial [5: pág. 243] y $(-, -)$ el símbolo local sobre $\mathbb{Q}_p(\zeta_q)$ con respecto a las potencias q -ésimas.

$$b) \left(\frac{\zeta_q}{\varepsilon} \right) = \zeta_q^{[|N\mathbb{Q}(\zeta_q)/\mathbb{Q}| - 1]/q}$$

donde $N\mathbb{Q}(\zeta_q)/\mathbb{Q}$ designa la norma.

$$c) \left(\frac{\pi}{\varepsilon} \right) = \beta \begin{cases} [\mathbb{T}\mathbb{Q}(\zeta_q)/\mathbb{Q}(\log \varepsilon)]/q & \text{si } p \neq 2 \\ \zeta_q^{(1+q/2)[\mathbb{T}\mathbb{Q}(\zeta_q)/\mathbb{Q}(\log \varepsilon)]/q} & \text{si } p = 2 \end{cases}$$

donde $\mathbb{T}\mathbb{Q}(\zeta_q)/\mathbb{Q}$ designa la traza y \log el logaritmo p -ádico. (b) y (d) son las llamadas fórmulas explícitas de la reciprocidad.

El caso, repetimos, en el cual estamos interesados es aquél en que $L(\sqrt[q]{\zeta_q})/L$ ramifica totalmente y en él los β requeridos pueden bien ser unidades o bien parámetros uniformizadores de L . Pero estos últimos se determinan una vez que se ha escogido un parámetro uniformizador π que cumpla $(\pi, \zeta_q) = 1$. Por lo tanto, podemos limitar nuestros cálculos a las unidades de L , y como $N_{L/\mathbb{Q}_p(\zeta_q)}(U_L) \subseteq U_{\mathbb{Q}_p(\zeta_q)}$, podemos siempre utilizar la siguiente

PROPOSICIÓN 2. Sean dados $\mathbb{Q}_p(\zeta_q) \subseteq L$. Entonces $\beta \in L^\times \pmod{L^{\times q}}$ sa-

tisface la propiedad P si, y sólo si, $\mathbb{Q}_p(\zeta_q)(\sqrt[q]{\beta})/\mathbb{Q}_p(\zeta_q)$, donde $\beta = N_L/\mathbb{Q}_p(\zeta_p)(\beta)$, satisface P con respecto al cuerpo $\mathbb{Q}_p(\zeta_q)$.

Además, podemos limitarnos únicamente a las unidades principales, pues $U_L = \mu_q^* \times U_{L,1}$ (μ_q^* es el grupo de las raíces de 1 contenidas en L y de orden primo con p) y $(\eta_1, \zeta_q) = 1$ si $\eta \in \mu_q^* \subset L^{\times q}$. La dificultad de los cálculos, sin embargo, puede ser tremenda. En consecuencia, el siguiente resultado puede ser útil si sólo queremos exhibir un $\beta \in L^{\times} \text{mód } L^{\times q}$ que satisfaga P .

PROPOSICIÓN 3. Sean $\mathbb{Q}_p(\zeta_q)$ y $\beta \in U_{L,1}$. Entonces

a) $L(\sqrt[q]{\beta}) = L(\sqrt[q]{\varepsilon})$ para algún $\varepsilon \equiv 1 \pmod{\pi}$, $\varepsilon \in \mathbb{Q}(\zeta_q)$ y $(\beta, \zeta_q) = (\varepsilon, \zeta_q)$, donde $\pi = 1 - \zeta_q$.

b) Las siguientes afirmaciones son equivalentes:

(I) $L(\sqrt[q]{\beta})/L$ satisface P

(II) $|N_L/\mathbb{Q}_p(\varepsilon)| \not\equiv 1 \pmod{pq}$

(III) $T_L/\mathbb{Q}_p(\varepsilon) \not\equiv 0 \pmod{pq}$

Democión. b) sigue de a) usando la proposición 1 y el hecho de que

$N_L/\mathbb{Q}_p(\varepsilon) = N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}(\varepsilon)$ si $\varepsilon \in \mathbb{Q}(\zeta_q)$ (de igual modo para la traza), pues $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ ramifica totalmente en p [5 : págs. 77 y 99]. Demostremos a): tomando $\varepsilon \in \mathbb{Q}(\zeta_q)$ tal que $\beta \varepsilon^{-1} \equiv 1 \pmod{L^m}$ para m suficientemente grande, obtenemos $L(\sqrt[q]{\beta}) = L(\sqrt[q]{\varepsilon})$ [5 : pág. 226] y $(\beta \varepsilon^{-1}, \zeta_q) = 1$ (por continuidad, todos los elementos suficientemente cercanos a 1 son normas), es decir, $(\beta, \zeta_q) = (\varepsilon, \zeta_q)$.

§ 2. Cálculo explícito de algunas bases.

LEMA 1. [3: pág. 49] $\gamma \in \mathbb{Q}_2^{\times 2}$ si, y sólo si, $\gamma \equiv 1 \pmod{8}$.

PROPOSICIÓN 4. $\mathbb{Q}_2(\sqrt{\beta})/\mathbb{Q}_2$ satisface la condición P si, y sólo si,

$\beta = -1, -2, 6, 3 \pmod{\mathbb{Q}_2^{\times 2}}$. Además, si $\pi = 2$ entonces $\pi = 2$, $\alpha_0 = 1 - \pi^2 = -3$ y $\alpha_1 = 1 - \pi = -1$ forman una base de \mathbb{Q}_2^{\times} mód $\mathbb{Q}_2^{\times 2}$ que cumple las condiciones del teorema 2 en [1].

Demostración: En efecto, como $-3 \not\equiv 1 \pmod{8}$ y $-3 \equiv 1 \pmod{4}$, sigue, respectivamente, que $-3 \notin \mathbb{Q}_2^{\times 2}$ (por el lema 1) y que $\mathbb{Q}_2(\sqrt{-3})/\mathbb{Q}_2$ es inramificado (puesto que en $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ el primo 2 no ramifica). Por otro lado, usando la ley suplementaria de la reciprocidad (proposición 1, a), obtenemos las siguientes relaciones

$$(2, 2)_2 = 1 ; \quad (2, -3)_2 = -1 ; \quad (2, -1)_2 = 1 ;$$

$$(-3, -3)_2 = 1 ; \quad (-3, -1)_2 = 1 ; \quad (-1, -1)_2 = -1 ;$$

de modo que $\{2, 3, -1\}$ es una base de \mathbb{Q}_2^{\times} mód $\mathbb{Q}_2^{\times 2}$ que cumple las condiciones requeridas. Finalmente, si

$$\beta = 2^m (-3)^{b_0} (-1)^{b_1} \pmod{\mathbb{Q}_2^{\times 2}},$$

entonces $b_1 = 1$ si, y sólo si, $\beta = 6, -2, 3, -1 \pmod{\mathbb{Q}_2^{\times 2}}$, y la proposición resulta entonces del teorema 6, b), en [1].

COROLARIO 1. Sea dada $L(\sqrt{-1})/L$ totalmente ramificada. Si β es una unidad en L , entonces $L(\sqrt{\beta})/L$ satisface la propiedad P si, y sólo si, $N_{L/\mathbb{Q}_2}(\beta) = -1, -2, 3, 6 \pmod{\mathbb{Q}_2^{\times 2}}$.

Demostración: Resulta inmediatamente de $(N_{L/\mathbb{Q}_2}(\beta), -1) = (\beta, -1)$.

COROLARIO 2. Sean dadas $L = \mathbb{Q}_2(\sqrt{\beta})$, $\beta = \pm 3, \pm 6 \pmod{\mathbb{Q}_2^{\times 2}}$. Entonces $L(\sqrt{-1})/L$ ramifica totalmente si $\beta = \pm 2, \pm 3, \pm 6 \pmod{\mathbb{Q}_2^{\times 2}}$. Además, se tiene :

a) Si $\beta = \pm 2, -3, \pm 6 \pmod{\mathbb{Q}_2^{\times 2}}$ y $\varepsilon = \eta + \xi\sqrt{\beta}$, $\eta, \xi \in \mathbb{Z}_p$ es una uni-

dad de L , entonces la extensión $L(\sqrt{\varepsilon})/L$ satisface P si, y sólo si, $\eta^2 + \beta \xi^2 \equiv -1, -2, 3, 6 \pmod{\mathbb{Q}_2^{\times 2}}$.

b) Si $\beta = \pm 3 \pmod{\mathbb{Q}_2^{\times 2}}$, estamos en la situación del teorema 5 en [1].

Demarcación : Del diagrama

$$\mathbb{Q}_2(\sqrt{\beta}, \sqrt{-1}) = L(\sqrt{-1})$$

$$L = \mathbb{Q}_2(\sqrt{\beta})$$

$$\mathbb{Q}_2(\sqrt{-\beta})$$

$$\mathbb{Q}_2(\sqrt{-1})$$

$$\mathbb{Q}_2$$

y observando que :

i) Para $\beta = \pm 2, \pm 6, \pm 3 \pmod{\mathbb{Q}_2^{\times 2}}$ la extensión $\mathbb{Q}_2(\sqrt{\beta})/\mathbb{Q}_2$ ramifica totalmente ; y

$$\text{ii) } \text{Gal}(L(\sqrt{-1})/\mathbb{Q}_2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

dedúcese que $L(\sqrt{-1})/L$ ramifica totalmente sólo cuando $\beta \neq 3 \pmod{\mathbb{Q}_2^{\times 2}}$.

El resto sigue del corolario 1 observando que $N_{L/\mathbb{Q}_2}(\eta + \xi\sqrt{\beta}) = \eta^2 + \xi^2\beta$.

Nuestro caso siguiente es $L = \mathbb{Q}_2(\zeta_4) = \mathbb{Q}_2(\sqrt{-1})$. Para calcular una base de $L^{\times} \pmod{L^{\times 4}}$ usamos el siguiente lema :

LEMA 2. (Eisenstein - Gauss) [6 : pág. 96]. Sea dada $L = \mathbb{Q}_2(i)$. Entonces

$$(\varepsilon, i) = i^{(\alpha-1)/2} \quad \text{y} \quad (\varepsilon, \pi) = i^{-[(\alpha-1)+\beta]/4}$$

si $\varepsilon = \alpha + \beta i \equiv 1 \pmod{\pi^3}$, $\pi = 1-i$.

PROPOSICIÓN 7. Si $\varepsilon = 1 + \beta i \pmod{\pi^3}$, $\pi = 1-i$, entonces

PROPOSICIÓN 5. Sea dada $L = \mathbb{Q}_2(i)$. Entonces

$$\pi = 1-i, \alpha_0, \alpha_1 = i, \alpha_2 = 7-6i,$$

donde α_0 es cualquier elemento 4-primario de L , forman una base de $L^\times \bmod L^{\times 4}$ que cumple las condiciones del teorema.

Demostración: Como $g = q' = 1$ (véase el teorema 1 en [1]), podemos tomar $\alpha_1 = i$ y α_0 arbitrario y 4-primario. Determinamos ahora $\alpha_2 = \alpha + \beta i$, $\alpha, \beta \in \mathbb{Z}$ (podemos tomar $\alpha, \beta \in \mathbb{Z}$ pues éste es denso en \mathbb{Z}_2) según las condiciones

$$(\alpha_2, i) = i^{(\alpha-1)/2} = i^{-1}; (\alpha_2, \pi) = i^{-[(\alpha-1)+\beta]/4} = 1$$

y

$$\alpha + \beta i = 1 - 2(1+i)(\eta + \xi i), \eta, \xi \in \mathbb{Z}.$$

Una solución de este sistema de ecuaciones está dado por $\alpha = 7, \beta = -6, \eta = 0$ y $\xi = 3$.

Consideremos ahora $L = \mathbb{Q}_3(\zeta_3)$. Aquí usamos el

LEMA 3. (Eisenstein) [6: pág. 96]. Sean dados $L = \mathbb{Q}_3(\zeta_3)$ y $\pi = 1-\zeta_3$.

Entonces

$$(\varepsilon, \zeta_3) = \zeta_3^{-[(\alpha-1)+\beta]/3} \quad y \quad (\varepsilon, \pi) = \zeta_3^{(\alpha-1)/3}$$

si $\varepsilon = \alpha + \beta \zeta_3 \equiv 1 \pmod 3$.

PROPOSICIÓN 6. Sea dada $L = \mathbb{Q}_3(\zeta_3)$. Entonces $\pi, \alpha_0 = 1-\pi^3, \alpha_1 = 1-\pi, \alpha_2 = 4-3\pi$, donde $\pi = 1-\zeta_3$, forman una base de $L^\times \bmod L^{\times 3}$ que cumple las condiciones del teorema 1 en [1].

Demostración: Sirviéndose del lema 3, la demostración prosigue como en la proposición 5, observando ahora que $1-\pi^3$ es 3-primario [5: pág. 353].

Observación. A la luz de la proposición 1, c), el método usado en la anterior proposición podría usarse para determinar α_2 en el caso $p > 3$, y obtener así $p^3 \varphi(p)$ extensiones de $L = \mathbb{Q}_p(\zeta_p)$ que cumplen P , a saber, aquellas definidas por

$$\beta = \pi^m (1-\pi^p)^{\alpha_0} (1-\pi)^{\alpha_1} \alpha_2^2 \pmod{L^{\times p}},$$

donde $\alpha_2 \not\equiv 0 \pmod{p}$. Queremos anotar aquí que usando las fórmulas explícitas de reciprocidad (proposición 1, b) y c), y a fin de encontrar un α_2 que satisfaga

$(\alpha_1, \alpha_2) = (\zeta_p, \alpha_2) = \zeta_p$ y $(\pi, \alpha_2) = 1$, debemos necesariamente tener que $\log \varepsilon \notin \mathbb{Q}_p$, donde $\varepsilon \equiv 1 \pmod{\pi}$, $\pi = 1 - \zeta_q$; esto evidentemente dificulta la tarea.

Podríamos preguntarnos si la muy canónica base $\pi = 1 - \zeta_p$, $\alpha_0 = 1 - \pi^p$, $\alpha_1 = 1 - \pi$, $\alpha_\nu = 1 - \pi^\nu$, $\nu = 2, \dots, p-1$ de $L^\times \pmod{L^{\times p}}$, $L = \mathbb{Q}_p(\zeta_p)$, satisface las condiciones requeridas. Desafortunadamente, éste no es el caso. En efecto, usando las siguientes propiedades [4 : pág. 353],

an i) $L(\sqrt[p]{\alpha_0})/L$ es inramificada;

an ii) $(\alpha_\nu, \alpha_\mu) = (\alpha_\nu, \alpha_{\nu+\mu})(\alpha_{\nu+\mu}, \alpha_\mu)(\alpha_{\nu+\mu}, \pi)^\mu$, donde $\alpha_\nu = 1 - \pi^\nu$, $\nu = 1, 2, p-1$, y, por supuesto, $\alpha_0 = \alpha_p$;

an iii) si $\nu+\mu \geq p+1$, entonces $(\alpha, \beta) = 1$ cuando $\alpha \in U_{L, \nu}$, $\beta \in U_{L, \mu}$;

an iv) $(\alpha_\nu, \pi) = \begin{cases} \zeta_p & \text{si } \nu = p \\ 1 & \text{en el caso contrario,} \end{cases}$

vemos fácilmente que para $p=3$, $(\alpha_1, \alpha_2) = 1 \neq \zeta_3$, de modo que la condición (iv) del teorema 1 en [1] no subsiste. Sin embargo, no debe sorprendernos el hecho de que para el primo 2 las cosas marchen, como lo vimos en la proposición 4. Nuestro siguiente ejemplo es $L = \mathbb{Q}_2(\sqrt{-3})$. En este caso demostramos la

PROPOSICIÓN 7. Si $L = \mathbb{Q}_2(\sqrt{-3})$, entonces $\pi = 2$, $\alpha_0, \alpha_1 = -1$ y $\alpha_2 =$

$2 + \sqrt{-3}$, donde α_0 es cualquier elemento 2-primario de L , forman una base, del tipo requerido, de $L^\times \bmod L^{\times 2}$.

Demostración: Como $\mathbb{Q}_2(\sqrt{-3})/\mathbb{Q}_2$ es inramificada (proposición 4), 2 es aún un parámetro uniformizador de $\mathbb{Q}_2(\sqrt{-3})$. Sabemos también que $g = q' = 1$, por el corolario 2,a), proposición 4. Sea entonces α_0 cualquier elemento 2-primario de L , y tomemos $\pi = 2$, $\alpha_1 = -1$. Queremos determinar α_2 de tal manera que α_2 de tal manera que $(\pi, \alpha_2) = 1$ y $(\alpha_1, \alpha_2) = -1$.
 $(\alpha + \beta\sqrt{-3}, 2) = (\alpha^2 + 3\beta^2, 2)_2$ y $(\alpha + \beta\sqrt{-3}, -1) = (\alpha^2 + 3\beta^2, -1)_2$
(los miembros derechos se calculan sobre \mathbb{Q}_2), podemos verificar que $\alpha_2 = 2 + \sqrt{-3}$ satisface ambas condiciones.

Veamos ahora cómo se calculan bases del tipo requerido si $L = \mathbb{Q}_2(\sqrt{\beta})$, $\beta = \pm 2, \pm 6$ ($\bmod \mathbb{Q}_2^{\times 2}$). En todos estos casos, $q' = g = 1$, de modo que tomamos $\alpha_1 = -1$; obviamente, $L(\sqrt{-3})/L$ es inramificada, pudiéndose tomar de nuevo $\alpha_0 = -3$. En seguida escogemos π de tal manera que $(\pi, -1) = (N_{L/\mathbb{Q}_2}(\pi), -1) = 1$ (esto es fácil por tanteo o de cualquier otra manera). Sólo falta determinar una unidad α'_2 tal que $(-1, \alpha'_2) = -1$ y $(\pi, \alpha'_2) = (\alpha_0, \alpha'_2) = 1$. Valiéndonos de la relación $(\alpha'_2, -1) = (N_{L/\mathbb{Q}_2}(\alpha_2), -1)_2$, es fácil determinar α'_2 en forma tal que $(\alpha'_2, -1) = (-1, \alpha'_2) = -1$; como siempre se tiene $(\alpha'_2, \alpha_0) = 1$, el único hecho que falta es decidir si $(\alpha'_2, \pi) = 1$ o no. Si por acaso $(\alpha'_2, \pi) = -1$, entonces $\alpha_2 = -3\alpha'_2$ se encargará de lo que queremos, pues $(\alpha_2, \pi) = (-3, \pi)(\alpha'_2, \pi) = (-1)(-1) = 1$. Tomemos, por ejemplo, $L = \mathbb{Q}_2(\sqrt{2})$. En este caso, podemos de terminar

$\pi = 4 + 3\sqrt{2}$, $\alpha_0 = -3$, $\alpha_1 = -1$, $\alpha'_2 = 1 + \sqrt{2}$,
tal como se ha indicado arriba. Ahora bien, $(4 + 3\sqrt{2}, 1 + \sqrt{2}) = 1 \Leftrightarrow 4 + 3\sqrt{2}$

Res es una norma proveniente de $\mathbb{Q}_2(\sqrt{2}, \sqrt{1+\sqrt{2}}) \Leftrightarrow 4+3\sqrt{2} = (\alpha + \beta\sqrt{2})^2 - (\eta + \xi\sqrt{2})^2$ ($1+\sqrt{2}$), $\alpha, \beta, \eta, \xi \in \mathbb{Z}_2$ \Leftrightarrow el sistema de ecuaciones diofánticas

$$\alpha^2 + 2\beta^2 - \eta^2 - 2\xi^2 - 4\eta\xi = 4$$

$$2\alpha\beta - 2\eta\xi - \eta^2 - 2\xi^2 = 3$$

tiene solución en \mathbb{Z}_2 . Este parece ser difícil. Por eso usamos el siguiente sistema

$$\alpha^2 + 2\beta^2 + 3\eta^2 + 6\xi^2 + 12\eta\xi = 4$$

$$2\alpha\beta + 3\eta^2 + 6\xi^2 + 6\eta\xi = 3,$$

el cual, por un razonamiento análogo al anterior, tiene solución si, y sólo si,

$$(4+3\sqrt{2}, -3(1+\sqrt{2})) = 1.$$

Por tanto, encontramos $\alpha = 1, \beta = 0, \xi = 0, \eta = 1$. De modo que hemos demostrado la

PROPOSICIÓN 8. Si $L = \mathbb{Q}_2(\sqrt{2})$, entonces $\pi = 4+3\sqrt{2}, \alpha_0 = -3, \alpha_1 =$

-1 y $\alpha_2 = -3(1+\sqrt{2})$ forman una base de L^\times mód $L^{\times 2}$ que satisface las condiciones requeridas.

COROLARIO. El sistema de ecuaciones diofánticas

$$\alpha^2 + 2\beta^2 - \eta^2 - 2\xi^2 - 4\eta\xi = 4$$

$$2\alpha\beta - 2\eta\xi - \eta^2 - 2\xi^2 = 3$$

no tiene soluciones enteras.

Observación. Este corolario pone de manifiesto nuevamente la estrecha relación que existe entre la ley de reciprocidad y las formas normicas [2 : capítulo II].

BIBLIOGRAFÍA

1. Albis-González, Víctor S., *The maximal abelian extension of a local field as a*

2. Artin, E. und Hasse, H., *Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n -ten Potenzreste im Körper der l^n -ten Einheitswurzeln*, Abh. Math. Sem. Univ. Hamburg, 6 (1928), 146-162.
3. Borevich, Z. I. and Shafarevich, I. R., *Number theory*, Academic Press, New York, 1965.
4. Cassels, J. W. S. and Frolich, A., eds., *Algebraic number theory*, Thompson Book Co., Washington, D. C., 1967.
5. Goldstein, L. J., *Analytic number theory*, Prentice-Hall, Inc., Englewood Cliffs, 1971.
6. Hasse, H., *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II : Reziprozitätsgesetz*, B. G. Teubner, Berlin, 1930.

Departamento de Matemáticas y Estadística

Universidad Nacional de Colombia

Ciudad Universitaria

Bogotá 6, D. E., Colombia, S. A.

(Recibido en noviembre de 1973).